SYMANTEC ENTERPRISE SECURITY

Confidence in a connected world.

Symantec Report on the Underground Economy

July 07–June 08

Published November 2008

Marc Fossi
Executive Editor
Manager, Development
Security Technology and Response

Eric Johnson
Editor
Security Technology and Response

Dean Turner
Director, Global Intelligence Network
Security Technology and Response

Trevor Mack
Associate Editor
Security Technology and Response

Joseph Blackbird
Threat Analyst
Security Technology and Response

David McKinney
Threat Analyst
Security Technology and Response

Mo King Low
Threat Analyst
Security Technology and Response

Téo Adams
Threat Analyst
Security Technology and Response

Marika Pauls Laucht
Threat Analyst
Security Technology and Response

Jesse Gough
Sr. Security Researcher
Security Technology and Response

Published November 2008

Symantec Report on the Underground Economy

Contents

Introduction

The Symantec *Report on the Underground Economy* is a survey of cybercrime activity in the underground economy. It includes a discussion of some of the more notable groups involved, as well as an examination of some of the major advertisers and the most popular goods and services available. It also includes an overview of the servers and channels that have been identified as hosts for trading, and a snapshot of software piracy using a file-sharing protocol in the public domain. This report is meant to be an analysis of certain aspects of the underground economy and is not meant to encompass a survey of Internet cybercrime as a whole. For the underground economy servers observed by Symantec, the period of observation was between July 1, 2007, and June 30, 2008. The software piracy observed by Symantec occurred over a three-month period between July and September, 2008. All prices are in U.S. dollars unless otherwise noted. Also, due to rounding, percentages given may not total exactly 100 percent.

Symantec defines cybercrime as any crime that is committed using a computer, network, or hardware device. The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime. The crime may take place on the computer alone or in addition to other locations.[1] Two of the most common platforms available to participants in the online underground economy are channels on IRC servers and Web-based forums. Both feature discussion groups that participants use to buy and sell fraudulent goods and services. Items sold include credit card data, bank account credentials, email accounts, and just about any other information that can be exploited for profit. Services can include cashiers who can transfer funds from stolen accounts into true currency, phishing and scam page hosting, and job advertisements for roles such as scam developers or phishing partners.

Web-based forums

Web-based forums are a popular means of trading stolen information. Some reasons for this are that posted advertisements are visible to anyone visiting the website until they are removed, most forums are organized chronologically and can be easily searched, and joining is usually open to anyone, often entailing registration with only a username. That said, various forums have differing levels of membership. Some allow members to immediately post advertisements and interact with other members, while other forums restrict member privileges until certain criteria are met. Many forums conduct a peer-review process for potential sellers before they are endorsed. To establish a reputation and prove themselves, potential sellers are often required to provide samples of their goods for validation and verification. Many of the sites often provide a range of active forums, including tutorials, how-to guides, credit card scams, or even specialized venues for goods from specific countries or regions.

[1] http://www.symantec.com/norton/cybercrime/definition.jsp

IRC channels

Channels on Internet relay chat (IRC) servers are also used to advertise and traffic stolen information, and to provide services to facilitate these illegal activities. IRC is an Internet communications protocol with a number of attractive aspects for operators in the underground economy: it offers real-time group communications, requires very little bandwidth, and the IRC client software is freely available across all operating systems.

The majority of IRC servers are set up for legitimate purposes and there are thousands of different channels devoted to many different subjects. Major IRC server networks strive for legitimacy and often monitor and ban inappropriate conduct, whether illegal or not. That being said, there are many public IRC servers available worldwide on which underground economy channels are covertly operated.

Because multiple IRC servers can be connected to form a larger network, there is a wide range in the size of IRC servers and the number of channels on each server. During this reporting period, for example, Symantec observed IRC servers that had as few as five channels to one network with over 28,000 channels.

Users can connect to IRC servers using one of many freely available IRC clients.[2] As with Web forums, users often need only a unique username to join a channel, although some channels are restricted and a user must either be invited by an existing channel user or approved by the channel administrators.

Advertisers on underground channels attempt to capture attention for their messages using techniques such as capitalization, multi-colored text, ASCII flares,[3] and repeated sales pitches across multiple lines (similar to blanketing a wall with the same advertising poster). Typical advertisements list the available items, prices, and other details such as payment options, contact information, and qualifiers to describe the goods such as “100% successful,” “fast,” or “legit” (figure 1). Since these channels are “always open,” advertisers often use scripts to schedule automatic message broadcasts across many servers and channels. Along with selling specific items, advertisements are also posted requesting particular goods and services, such as credit cards from a certain country, or a cashier of a specific gender.

[2] A client is anything that connects to the server that is not a server itself.
[3] An ASCII flare is a text graphic that only uses the 128 basic ASCII characters.

Figure 1. Underground economy channel screenshot
Source: Symantec Corporation

Potential buyers for advertised goods and services will privately contact the sellers to negotiate the deal and finalize payment. The seller will usually then arrange to forward the goods to the buyer upon payment, options for which include using online currency exchange services or the exchange of goods. Many buyers will also use the services of experienced cashiers who will convert the stolen goods, such as bank account credentials, into true currency, either in the form of online currency accounts or through money transfers. This is referred to as a cash out. In exchange for this service, cashiers will charge a fee, which is usually a percentage of the cash-out amount.

Participants on underground economy servers are usually self-policing, reporting rippers to the IRC server administrators and also broadcasting this information on the channels to warn others.[4] Many underground economy servers have channels specifically created by the server administrators as a direct forum to report and list current rippers to avoid. Repeat rippers can be kicked off and banned from the servers. Also, due to the potential legal liability of hosting channels where stolen goods are trafficked, some administrators prevent the creation of channels with names typically associated with illegal activities. That said, although the administrators can ban the creation of these channel names, traders often manipulate the channel names to avoid being blacklisted.

[4] Rippers are vendors on underground economy servers who conduct fraudulent transactions such as not delivering purchased goods, or deliberately selling invalid or fake credit cards.

Along with masking activities at the channel level, participants often use multiple nicknames to obscure their activities, or mask their IP addresses to conceal their true location.[5] They may also use different nicknames to provide a name association with the goods or services being offered, similar to descriptive company names such as A1 Lumber Company. A new nickname can also be used to clear a bad reputation on the servers. Because word-of-mouth and reputation may affect the ability of an advertiser to conduct business, if an advertiser is accused of being a ripper, he or she can simply switch nicknames and start anew.

Software piracy

As part of this survey of the underground economy online, Symantec also examined software piracy activity over a peer-to-peer (P2P) file-sharing protocol. Data was sampled over a three-month period from July to September, 2008. The data collected includes information on application and game software being pirated, the number of instances of each file, and the locations of the users posting the files. Video and music data was not monitored. The data collected represents a snapshot of the software piracy activity that Symantec observed over the specified period and is not meant to be representative of all piracy and file sharing on the Internet.

[5] http://www.securityfocus.com/news/11517

Groups and Organizations

There are a number of groups and organizations that have been active in the trade of fraudulent goods and services in the underground economy. The majority of these groups functioned through a number of Web-based forums devoted to online fraud.[6] While apparently not as profuse as underground economy IRC channels, these forums have been responsible for a sizable amount of the trade in fraudulent goods and services online. Moreover, there have been a number of high-profile prosecutions of the people behind these operations. For these reasons, it is worth examining some of these forums and the operators behind them for insight into fraud in the underground economy.

There has been much speculation and debate as to the level of organization and professionalism of these groups, mainly because of the nature of the forums, which exist primarily to provide a means for participants to collaborate with each other, offer their skills, and buy and sell fraudulent and stolen goods and services. Thus, these forums could be more aptly defined as a loose collection of individuals with a common purpose, rather than as a highly organized and cohesive group. Nonetheless, Symantec research indicates that there is a certain amount of collaboration and organization occurring on these forums, especially at the administrative level. Moreover, considerable evidence exists that organized crime is involved in many cases.

One advantage of a Web forum is in the relative permanence of available content. Advertisements and other messages posted to the forum are readily available, even days or months afterward, making it easier to conduct business and post detailed price lists for goods or services. This is in contrast to IRC channels, where advertisements typically scroll out of view within seconds, especially on very busy channels—requiring advertisements to be periodically repeated in order to remain visible. Symantec observed that some IRC channels with hundreds of users will generate thousands of lines of messages per day. Moreover, the lifespan of IRC channels is typically far shorter, with only a very small percentage remaining active beyond a few months, as discussed in the "IRC Servers and Channels" section of this report.

Another distinction between Web forums and IRC channels is that, in most cases on the forums, participants wishing to be sellers are subject to a peer-review process before they are granted vendor status by administrators.[7] Depending on the types of goods and services offered by the participant, the process can involve providing pre-determined sample packages for verification and validation.[8] Reputation is important and sellers expend no small amount of time and effort to establish their identities. While reputation is also important for participants on IRC channels, Symantec has observed that members there change identities much more often, mostly to evade identification (as well as for other reasons, as discussed in the "Advertisers on Underground Economy Servers" section). That being said, IRC channels are less restrictive, allowing just about anyone to post. This, in turn, would lead to increased traffic since more goods and services on the channels would likely attract more customers. In addition, the seemingly transient nature of IRC channels may also give participants a sense of security and they may think that there is less likelihood of being apprehended. The high-profile arrests of Web-forum operators, such as are described below, may also make IRC channels a more appealing venue for many users.

One reason why forum-based groups have been identified and prosecuted more often than participants on IRC channels, despite the significant amount of fraud occurring on these channels, may be simply because of the use of relatively permanent nicknames—the very thing that helps participants on the forums establish themselves. This, along with the reality that many of these forums blatantly advertise their

[6] An Internet forum is a collection of dated posts that are defined by a topic or purpose. Cf. http://dictionary.zdnet.com/definition/forum.html
[7] http://www.darkoperations.net/shadowcrew/viewtopic.php-t=5103&sid=55dce3a5fefbd4597ef015fbd12bc941.htm
[8] http://www.darkoperations.net/shadowcrew/viewtopic.php-t=2741&sid=55dce3a5fefbd4597ef015fbd12bc941.htm

presence online, would facilitate the tracking of activities on these forums by law enforcement. IRC channels, on the other hand, attempt to operate under the radar for the most part. They are also easier to hide and more transitory than Web forums. Thus, it is possible that there are a comparable number of IRC-based groups, but their more discreet operations may allow them to more easily evade public scrutiny.

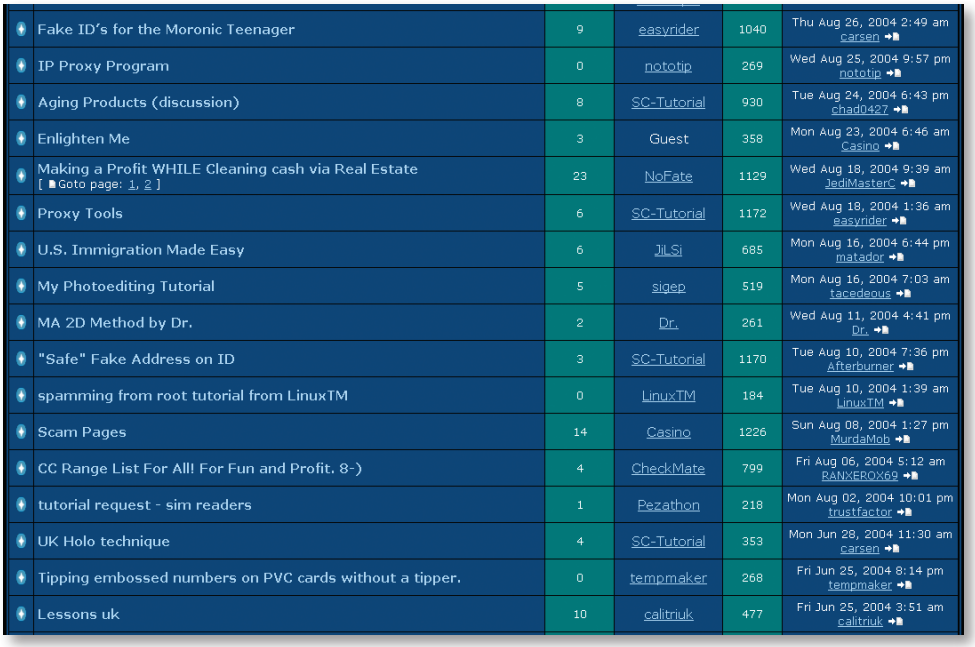
One of the first groups to gain significant notoriety as an active Web forum for online fraud was called ShadowCrew. The genesis of ShadowCrew was in a site called Counterfeitlibrary, which primarily catered to discussions regarding forgery, identity theft, and credit card fraud. In 2002, several members of Counterfeitlibrary decided to launch their own forum, which became the ShadowCrew site. ShadowCrew was active until 2004, when its main operators were arrested as part of Operation Firewall—an 18-month undercover initiative by U.S. and international law enforcement agencies.[9] (Two other Web forums devoted to online fraud, Carderplanet and Darkprofit, were also shut down during Operation Firewall.)

The ShadowCrew forum made little effort to conceal its purpose or activities, which likely contributed to the level of unwanted attention it attracted, and probably its ultimate demise. It was open to public registration and viewable by anyone online. Because of the static nature of a website compared to an IRC channel, forums like ShadowCrew are easy to locate and revisit, which would make them an easier target for law enforcement agencies to monitor.

As with a number of the forums discussed in this report, ShadowCrew offered content in both English and Russian, which is not surprising given that the website had administrators and contacts who resided in Russia.[10] Although there were not necessarily organized ties between users in these countries, it seems to have been a mutually beneficial arrangement. It is likely that, by attracting members from other countries, ShadowCrew was able to expand the availability of cash-out and drop locations. U.S. members of the forum could provide cash-out services to Eastern European users, who in turn seemed to provide specialized services such as card duplications. This would have been an attractive incentive because many banks allow financial accounts to be cashed out only from within the issuing country. There are indications that Russian and Eastern European crime syndicates were involved in many aspects of these operations.[11] This may be because participants in the underground economy in these countries are often able to operate with less fear of apprehension, mainly because of the lack of extradition laws, budget constraints affecting law enforcement, and the backing provided by well-organized crime syndicates.[12]

As with any self-perpetuating economic system, because of the open nature of the ShadowCrew forum, many new participants made use of tutorials and advice posted by others. These tutorials covered a wide range of topics and catered to various skill levels, detailing such fraudulent activity as how to obscure the source of attacks with proxies, how to spam, and how to assume false identities, among others (figure 2). For many participants, tutorial forums such as these were a “must-read” for anyone wanting to get into the underground economy.[13] In addition, some forums required a certain number of posts from members before they could be considered a senior member and given certain privileges, and one participant explained how he fulfilled his quota by posting “how to” articles on various check-cashing scams.[14]

[9] http://www.internetnews.com/security/article.php/3429101
[10] http://www.usdoj.gov/criminal/cybercrime/mantovaniIndict.htm
[11] http://www.wired.com/politics/onlinerights/news/2007/01/72581
[12] http://www.wired.com/politics/onlinerights/news/2007/01/72605
[13] http://www.wired.com/politics/onlinerights/news/2007/01/72581?currentPage=2
[14] http://www.wired.com/politics/onlinerights/news/2007/01/72581?currentPage=2



Fake ID's for the Moronic Teenager	9	easyrider	1040	Thu Aug 26, 2004 2:49 am carsen
IP Proxy Program	0	nototip	269	Wed Aug 25, 2004 9:57 pm nototip
Aging Products (discussion)	8	SC-Tutorial	930	Tue Aug 24, 2004 6:43 pm chad0427
Enlighten Me	3	Guest	358	Mon Aug 23, 2004 6:46 am Casino
Making a Profit WHILE Cleaning cash via Real Estate [Goto page: 1, 2]	23	NoFate	1129	Wed Aug 18, 2004 9:39 am JediMasterC
Proxy Tools	6	SC-Tutorial	1172	Wed Aug 18, 2004 1:36 am easyrider
U.S. Immigration Made Easy	6	JiLSi	685	Mon Aug 16, 2004 6:44 pm matador
My Photoediting Tutorial	5	sigep	519	Mon Aug 16, 2004 7:03 am tacedeous
MA 2D Method by Dr.	2	Dr.	261	Wed Aug 11, 2004 4:41 pm Dr.
"Safe" Fake Address on ID	3	SC-Tutorial	1170	Tue Aug 10, 2004 7:36 pm Afterburner
spamming from root tutorial from LinuxTM	0	LinuxTM	184	Tue Aug 10, 2004 1:39 am LinuxTM
Scam Pages	14	Casino	1226	Sun Aug 08, 2004 1:27 pm MurdaMob
CC Range List For All! For Fun and Profit. 8-)	4	CheckMate	799	Fri Aug 06, 2004 5:12 am RANXEROX69
tutorial request - sim readers	1	Pezathon	218	Mon Aug 02, 2004 10:01 pm trustfactor
UK Holo technique	4	SC-Tutorial	353	Mon Jun 28, 2004 11:30 am carsen
Tipping embossed numbers on PVC cards without a tipper.	0	tempmaker	268	Fri Jun 25, 2004 8:14 pm tempmaker
Lessons uk	10	calitriuk	477	Fri Jun 25, 2004 3:51 am calitriuk

Figure 2. Tutorials section on ShadowCrew
Source: web.archive.org[15]

Several notable ShadowCrew members were active participants in similar sites before and after the ShadowCrew forum was operational. These figures were mostly ShadowCrew moderators and administrators. Online venues such as forums (and IRC channels) generally designate administrators and/or moderators, whose roles are to perform tasks such as managing members and accounts, moderating content and topics, and ensuring the availability of the site.

The creator and original administrator of the ShadowCrew website went by the nickname Kidd. Shortly after establishing the forum, Kidd disappeared from the website, and someone nicknamed Macgyver assumed control. Macgyver was arrested in 2002 with another forum member, El Mariachi, in the state of Washington while allegedly attempting to collect $30,000 worth of merchandise for a Ukrainian known as Big Buyer.[16] This arrest was not generally perceived as a move by law enforcement against ShadowCrew, but rather as an isolated case involving that particular crime.

The last person to assume control of the ShadowCrew forum before it was shut down was known as CumbaJohnny (a.k.a. Segvec, a.k.a. soupnazi). It was later revealed that he was working as a confidential informant for the United States Secret Service and was a key to the success of Operation Firewall.[17] CumbaJohnny was arrested in 2003 on credit card fraud charges and, as part of a plea bargain, agreed to help the authorities.[18] As part of Operation Firewall, CumbaJohnny relocated ShadowCrew's servers to New Jersey and several members were instructed to use an encrypted virtual private network (VPN) connection to conceal the source of their activities.[19] In actuality, the VPN routed their communications and incriminating traffic to a single server that was actively monitored by the Secret Service. The evidence gathered from this allowed the authorities to eventually indict 19 people from ShadowCrew and shut down the site.[20] Although

[15] http://web.archive.org/web/20021001123344/www.shadowcrew.com/forum/viewforum.php?f=4
[16] http://www.wired.com/politics/onlinerights/news/2007/01/72515
[17] http://www.javelinstrategy.com/2008/08/13/albert-cumbajohnny-gonzalez-hacking-ringleader%E2%80%98s-life-as-a-secret-service-mole/
[18] http://www.nytimes.com/2008/08/12/technology/12theft.html
[19] http://www.wired.com/science/discoveries/news/2007/02/72585
[20] http://www.usdoj.gov/opa/pr/2004/October/04_crm_726.htm

forum participants at times doubted the integrity of CumbaJohnny, the majority of the participants were oblivious to his involvement with law enforcement until the website was shut down. The catalyst for the arrests during Operation Firewall came when a hacker nicknamed Ethics, while illegally accessing a telecommunications server, discovered that the Secret Service was monitoring ShadowCrew members.[21] Ethics and another ShadowCrew member brought this to the attention of CumbaJohnny who, in turn, notified the Secret Service that their investigation likely had been compromised.

Notwithstanding his arrangement to provide the Secret Service with criminal intelligence, CumbaJohnny remained active in the underground economy. At the same time he was acting as an informant for U.S. authorities, according to federal prosecutors he was also working with another group outside of ShadowCrew on a range of other sophisticated fraud attacks on large U.S. retail chain stores.[22] Part of the operation was to gain access to systems that processed customer credit cards by "wardriving" and exploiting poorly protected wireless networks.[23] The group then installed a custom sniffer application to seek out and capture credit card data.[24] Schemes such as these highlight the global nature of cybercrime, given that it is likely that this group came together because members in each area could provide the specialized services and supplies to carry out the operation. In this case, the stolen data was usually stored on servers in Latvia and Ukraine until being imprinted on blank ATM cards supplied by contacts in China, and then the cards were shipped back to North America to be used in skimming operations.[25]

CumbaJohnny was arrested in 2008 along with 10 others from the United States, China, Ukraine, Estonia, and Belarus in one of the largest credit card and debit card thefts ever prosecuted in the United States.[26] At the time of his final arrest, authorities were aware of one of his bank accounts containing $1.6 million, in addition to assets such as a luxury vehicle, a Miami condominium, and many high-value consumer electronics.[27]

Another prolific forum that operated in a similar fashion to ShadowCrew and included much of the same type of content was called the Grifters. The inception of the Grifters came about when El Mariachi was arrested in 2003 (during the incident in Washington State, discussed above). To avoid a prison sentence, El Mariachi divulged details of the online forums and promised to participate in a large international sting operation.[28] This led to the creation of the Grifters forum, which was intended from its inception to be used as a sting website by the U.S. Federal Bureau of Investigation (FBI), although it was later abandoned. The Grifters operated from 2003 until 2006, with many members of ShadowCrew joining after that forum was shut down by Operation Firewall in 2004.[29]

[21] http://www.securityfocus.com/news/10271
[22] http://www.nytimes.com/2008/08/12/technology/12theft.html
[23] Wardriving is a term used to refer to the act of using a vehicle and a laptop with a wireless network card to scan for networks in the area.
[24] A sniffer is an application designed to capture specific types of data during transmission.
[25] http://www.nytimes.com/2008/08/12/technology/12theft.html?pagewanted=2&_r=1
[26] http://blog.wired.com/27bstroke6/2008/08/11-charged-in-m.html
[27] http://www.usdoj.gov/criminal/cybercrime/yastremskiyIndict.pdf
[28] http://www.wired.com/politics/onlinerights/news/2007/01/72515
[29] http://blog.wired.com/27bstroke6/files/FBI_Cybercrook.pdf : p. 3

As with most criminal enterprises, and similar to how rippers are exposed and monitored on IRC channels, suspicion on these forums is common and members will use their abilities to hack into computer systems to run background checks on other members. El Mariachi, for example, was frequently suspected of being an informant by his peers because of several inconsistencies in his story, such as not being prosecuted for outstanding warrants.

Another forum of note was called Cardersmarket, which was launched in 2005 by "Iceman" (a.k.a. Max Vision) after he hacked four rival forums and merged the user accounts into his own site. These forums included DarkMarket, TalkCash, ScandanavianCarding, and TheVouched. These forums all provided a means for users to buy, sell, and trade stolen information, with a focus on credit cards. Iceman was arrested for hacking-related crimes targeted at U.S. government agencies in 1998, and in exchange for a lighter sentence, he agreed to work as an informant.[30] Following his release, he worked in the San Francisco area as an information security consultant, while maintaining Cardersmarket. The site remained operational until 2007, when Iceman was arrested for fraud-related charges as a result of his continued involvement.[31] During the operation of Cardersmarket, it was alleged that Iceman sold tens of thousands of stolen credit card numbers through the forum.[32] He also used as many as five different nicknames on the forum, hoping to confuse law enforcement by separating his administrator functions from his illegal activities.[33]

In late 2008, one of the fraudulent credit card trading forums that Iceman had hacked, DarkMarket, was discovered to be an FBI operation. The forum administrator, who was known as Master Splynter, was in fact an undercover FBI agent who had run the site out of government offices since November 2006.[34] Unlike ShadowCrew, where membership was open to anyone, DarkMarket was set up as an invite-only forum for members to meet and trade stolen information such as credit card numbers, full identities, and phishing attacks. The FBI gained access to the website when Master Splynter was invited as an administrator. The FBI shut down the website in 2008 after enough information had been gathered to arrest over 60 people worldwide.[35]

Another forum of note was called CarderPlanet (shut down during Operation Firewall, as mentioned above), which was created in 2002 by a man nicknamed Script, and an accomplice. The operation was apparently conceived at a meeting that Script held in 2001 at a restaurant in Odessa, Ukraine, with 150 other interested people from Eastern Europe.[36] Initially focused on members in Eastern Europe, CarderPlanet eventually added a forum in English to attract North Americans and other English-speaking members in order to expand the geographic area for cashing out cards, and for additional drop locations for stolen goods.[37]

Script was a well-known figure in the underground economy and active in other forums, including ShadowCrew. Script and his associates were known for mass-producing counterfeit credit and debit cards, which they delivered internationally and used to withdraw cash. This was so efficient that, at one point, those working with Script were reportedly earning up to $100,000 a day—significantly more than estimates of earnings on U.S.-based forums.[38]

[30] http://www.securityfocus.com/news/11487
[31] http://www.usdoj.gov/usao/paw/pr/2007_september/2007_09_11_02.html
[32] http://www.usdoj.gov/usao/paw/pr/2007_september/2007_09_11_02.html
[33] http://www.securityfocus.com/news/11487/2
[34] http://blog.wired.com/27bstroke6/2008/10/darkmarket-post.html
[35] http://news.bbc.co.uk/2/hi/uk_news/7675191.stm
[36] http://www.wired.com/politics/onlinerights/news/2007/01/72581
[37] Ibid.
[38] Ibid.

As a result of an investigation led by U.S. authorities, Script was arrested by Russian authorities in 2005. Script was also allegedly connected to a previous arrest at his makeshift card factory, where approximately 8,000 credit cards were seized.[39] These factories were routinely used to create duplicate credit cards using stolen data, which were then shipped worldwide to cashiers for withdrawal, with a percentage of the profit purportedly being sent back to Script and his associates.

Finally, there is the Russian Business Network (RBN), which is an organization that has been associated with a significant percentage of cybercrime in recent years.[40] Some of the activity associated with the RBN has included spam, phishing, and software piracy. Although its activities online have often been highly visible, relatively little is known about who is behind the RBN, though the group appears to have considerable resources at its disposal.

The RBN has been credited for creating approximately half of the phishing incidents that occurred worldwide in 2006, and for hosting websites that are responsible for a large amount of the world's Internet crime.[41] For example, Rock Group, an organization allegedly specializing in phishing, used hosting services provided by the RBN and was estimated to have made $150 million in 2006 from phishing attempts that stole bank credentials.[42] As well, several highly prolific pieces of malicious code have been developed and distributed from within RBN networks, such as the MPack exploit toolkit.[43] Additionally, large bot networks (botnets) using the Peacomm Trojan have relied on systems within the RBN network to be used as control channels.[44] While similar botnets are usually shut down within days or weeks, through the "bulletproof" hosting offered by the RBN, these command-and-control channels were allowed to remain active for up to nine months after their discovery.[45]

Actions such as these, along with many other aspects of the RBN's operation as an Internet service provider (ISP), drew suspicion and criticism from an increasing number of authorities. Many administrators and security professionals took note of the fact that, not only was the RBN a common host for malicious code, phishing scams, and command-and-control servers, but it also failed to respond to abuse reports requesting the removal of malicious content found on its networks. In some cases, while a customer's website would be replaced with a suspended notice, a direct link to the malicious content would still be active. Despite the criticism and contrary to the impressions of the security community, the RBN continued to maintain that it was a legitimate organization that made efforts to respond to reports of abusive users.

In late 2007 the amount of criminal activity being harbored by the RBN drew the attention of mainstream media, eventually pressuring several of the RBN's upstream providers to shut down service to the network.[46] However, only days after the RBN disappeared from the Internet, many researchers noted newly registered networks appearing in China, and much of the former RBN clientele appeared to be associated with this new network. It is believed that this may have been an attempt by the RBN to relocate its operations.[47]

[39] http://www.wired.com/politics/onlinerights/news/2007/01/72581
[40] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2844031.ece
[41] http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html
[42] http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article2844031.ece
[43] https://forums.symantec.com/syment/blog/article?message.uid=305505
[44] http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99
[45] Bulletproof hosting is a term that is used to describe service providers that are difficult to shut down, due to a combination of technical and political barriers. They often reside in jurisdictions that may have lax computer crime laws, fewer resources to investigate offenders, or indifference towards foreign complaints.
[46] Upstream provider is a large ISP that provides Internet access to a smaller ISP.
[47] http://www.scmagazineus.com/Is-this-the-end-of-the-Russian-Business-Network/article/96289/ and http://www.pcworld.com/article/id,139465-page,1-c,privacysecurity/article.html

There is speculation as to whether or not the RBN was directly responsible for all of the alleged activity or if it merely facilitated all of the fraud attributed to it.[48] Either way, the organization was clearly operating in the underground economy. It was not registered as a corporation and did not have its own website. Potential customers could only use its services by having social connections to the individuals running the network.

Although there is a wide variety of individuals and groups active in the underground economy, there does appear to be some correlation between the level of organization and specific regions. For example, various arrests and indictments of underground economy participants suggest that groups in Russia and Eastern Europe are more organized in their operations, with greater ability to mass-produce physical credit and debit cards.[49]

In contrast, groups operating out of North America tend to be loosely organized, often made up of acquaintances who have met in online forums and/or IRC channels and who have chosen to associate with each other. Another notable contrast is that there has been a number of recorded incidents involving undercover law enforcement agents or confidential informants within groups based in North America, whereas Symantec has not observed any publicized incidents of the same in Europe. In some cases, groups operating out of North America have relied on the more professional Eastern European groups to supply them with high-quality fraudulent cards for use in schemes such as magnetic stripe skimming. This arrangement is mutually beneficial to operators in Eastern Europe, who require physical access to U.S. banks or ATMs in order to exploit stolen U.S. card data.

Another trait likened to that of organized crime is that Eastern European groups have been known to use physical violence in repercussions against competitors, which Symantec has not observed elsewhere.[50] The propensity for more serious organized crime to use physical violence may be one reason why law enforcement is more often inclined to attempt to employ confidential informants within groups based in North America. In one case where this tactic was attempted in Eastern Europe, a confidential informant was kidnapped, assaulted, and exposed online as a warning to others in the online underground economy.[51]

Although there is a wide range in the sophistication and capabilities of these groups and organizations, Symantec believes that, on the whole, they will continue to shift away from such a relatively visible Web presence. With so many of these forums and other sites being the target of undercover sting operations, it is likely that the more highly organized groups will attempt to cover their activities and limit their communications to private channels that are not as easily monitored, such as is afforded by the relative anonymity and safety of the IRC channels. These channels are discussed in greater depth in the following sections of this report.

[48] http://www.guardian.co.uk/technology/2007/nov/15/news.crime
[49] http://www.wired.com/politics/onlinerights/news/2007/01/72581
[50] http://blog.wired.com/27bstroke6/2008/08/hacker-reported.html
[51] http://blog.wired.com/27bstroke6/2008/08/hacker-reported.html

Governments have also become more sophisticated in their awareness of cybercrime, and specific legislation at national and international levels has been developed to combat online fraud. As with crime anywhere, the online underground economy will continue to be a struggle between the participants looking to profit from fraud and the various authorities and antifraud organizations trying to shut them down. This is evidenced by the calling card the Secret Service left for subsequent visitors to the ShadowCrew forum after it was shut down in 2004 (figure 3).

Figure 3. Screenshot of United States Secret Service posting on ShadowCrew forum
Source: web.archive.org[52]

[52] http://web.archive.org/web/20041030015234/http://shadowcrew.com/

Goods and Services Advertised

This section of the Symantec *Report on the Underground Economy* examines the goods and services advertised on underground economy servers observed by Symantec between July 1, 2007 and June 30, 2008. The discussion will be broken out into two sections: supply and demand, and malicious tools. The analysis is by distinct messages, which are considered single advertisements for a good or service, though the same ad may appear thousands of times. To qualify as a new message, there must be variations to the message, such as price changes or other alterations in the message.

Supply and demand

The online underground economy observed by Symantec has matured into a global market with the same supply and demand pressures and responses of any other economy.[53] There are a great many channels available to advertisers to market their wares, which they do, and often. Many of the ads are also for requests, seeking cashiers perhaps, or for an effective exploit—demand identifying a need. Like advertising everywhere, messages come loaded with enticements, such as "fresh," "unspammed," and "high balance."[54] Typical contents include what is for sale, the price range, acceptable payment methods, and contact information.

For this report, the analysis of the supply and demand of goods and services has been further broken out into the following topics:

- Goods and services advertised by category
- Goods and services advertised by item
- Unique samples of sensitive information
- Value of total advertised goods

Goods and services advertised by category

Symantec organizes the goods and services advertised on the underground economy into categories (such as credit card information, financial accounts, and so forth). Measuring by category provides insight into supply and demand patterns in the underground economy. (Specific items within these categories are discussed below in "Goods and services advertised by item.")

Of the categories advertised on underground economy servers observed by Symantec, the credit card information category ranked highest during this reporting period, with 31 percent of the total (table 1). This category includes credit card numbers, credit cards with CVV2 numbers, and credit card dumps.[55] It was also the most requested category, making up 24 percent of all goods requested.

[53] Please see the Symantec *Internet Security Threat Report*, Volume XIII Executive Summary (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 12

[54] "Fresh" indicates that the goods are newly acquired, i.e. likely still valid and not canceled, and "unspammed" indicates an email address list that has not been used for spamming. Please see Appendix B—Methodologies and Appendix C—Glossary for explanations of the terms discussed in this section.

[55] Card Verification Value 2 (CVV2) is a three- or four-digit number on the credit card and used for card-not-present transactions, such as Internet or phone purchases. This was created to add an extra layer of security for credit cards and to verify that the person completing the transaction was in fact, in possession of the card (cf. http://www.visa.ca/en/merchant/fraudprevention/cvv2.cfm).; a credit card dump is the information contained within the magnetic stripe on the back of a credit card, which is itself made up of two tracks; while both tracks contain the primary account number and expiration date, only the first track will contain the cardholder name.

Rank for Sale	Rank Requested	Category	Percentage for Sale	Percentage Requested
1	1	Credit card information	31%	24%
2	3	Financial accounts	20%	18%
3	2	Spam and phishing information	19%	21%
4	4	Withdrawal service	7%	13%
5	5	Identity theft information	7%	10%
6	7	Server accounts	5%	4%
7	6	Compromised computers	4%	4%
8	9	Website accounts	3%	2%
9	8	Malicious applications	2%	2%
10	10	Retail accounts	1%	1%

Table 1. Goods and services available for sale, by category[56]
Source: Symantec Corporation

One reason for this ranking may be because there are many ways credit card information can be obtained and used for fraud. This includes phishing schemes, monitoring merchant card authorizations, the use of magnetic stripe skimmers, or breaking into databases and other data breaches that expose sensitive information.[57]

Another reason is the high frequency use of credit cards. For example, the 22 billion credit card transactions in the United States in 2006 represent a growth of eight percent over the previous year.[58] High frequency use and the range of available methods for capturing credit card data would generate more opportunities for theft and compromise and, thus, lead to an increased supply on underground economy servers.

One reason that credit card information is in such demand is because using the fraudulent credit card data for activities such as making online purchases is relatively easy. Online shopping can be easy and fast, and a final sale often requires just credit card information. Someone knowledgeable enough could potentially make many transactions with a stolen card before the suspicious activity is detected and the card is suspended. Once the purchases have been completed and delivered, they can then be fenced for a profit.

People using fraudulent credit cards will try to raise as little suspicion as possible in order to get the maximum use of the card. This is because credit card issuers routinely monitor the card transactions of their clients, looking out for unusual spending patterns, locations and/or amounts as part of their security practices. For example, with card-present transactions, suspicious activities such as consecutive purchases from more than one country will quickly alert the credit card issuer of potential fraud or theft and the card will be suspended. However, this is more difficult to monitor for online stores that have no geographical boundaries, and the same credit card number can be used from multiple locations by multiple people with less likelihood of being detected immediately. In addition, not all online stores verify the billing address of the credit card, and often any location can be provided as the shipping address.

[56] Credit card information includes credit card numbers, credit cards with CVV2, and credit card dumps; financial accounts includes bank account numbers, magnetic stripe skimming devices, online payment services, online currency accounts, and online stock accounts; spam and phishing information includes email addresses, email passwords, scams, and mailers; withdrawal services include cash outs and drops that are used to withdraw money and items from purchases; identity theft includes full identities and Social Security numbers; server accounts are for file transfers and virtual networks; compromised computers includes hacked computers, bot-infected computers, and shells; website accounts include online accounts for access to specific websites such as social networking sites; malicious tools includes Web-based attack tools and malicious code; and retail accounts includes gift cards for online stores and online auction accounts.
[57] Magnetic stripe skimming devices are small machines designed to scan and retain data contained in the magnetic stripes on credit and debit cards.
[58] http://www.bis.org/publ/cpss82p2.pdf : Table 7

To acquire the physical goods, advertisers on the underground economy servers also sell drop locations, and a trusted drop may be used by multiple people.[59] Because many online stores also offer international shipping to compete with other businesses, buyers can easily direct their purchases to secure and untraceable drop locations either close to their physical location for easy retrieval or to an intermediary who will forward the purchase. To the credit card issuer, these transactions may not show up immediately as being suspicious, especially during peak shopping times such as holidays when the number of purchases made increases substantially. This is compounded by the ability of legitimate shoppers to buy gifts online and ship them to a location other than their billing address, often at the expense of the retailers. These factors will hinder the ability of credit card issuers to monitor spending patterns, thereby increasing the opportunity to use fraudulent credit cards.

Given these reasons, credit card issuers may not see these online purchases as fraudulent until well after the transactions have been completed and the goods shipped. Although many major online stores have adopted added security features such as online authentication services and billing address checks, there are still many smaller merchants that may not be taking such security precautions online.[60]

Another factor that contributes to the popularity of credit card information as a category is that it is typically sold in bulk packages on underground economy servers. Not only do advertisers offer discounts for bulk purchases or throw in free numbers with larger purchases, but having an extensive list of cards enables individuals to quickly try a new number if a card number does not work or is suspended. Also, having a larger number of credit cards numbers included should theoretically increase the potential of having active cards in the bulk package.

The second most common category of goods and services advertised was financial accounts, with 20 percent of the total. This category includes bank account credentials, magnetic stripe skimming devices, online payment services, online currency accounts, and online stock trading accounts. This category ranked third for advertised requests, with 18 percent of the total. By far the major contributor to the popularity of the financial accounts category was bank account credentials, which accounted for 18 percent of all goods and services advertised for sale.

Financial accounts are attractive targets because of the opportunity to withdraw currency directly. Although this may involve more steps than using stolen credit card data to make online purchases, the process of cashing out financial accounts can be easier than retrieving cash from credit cards since criminals would require a PIN for the card. Also, most ATMs have security cameras, which may deter criminals from using this method. In addition, withdrawing currency from a bank account has the advantage of a more immediate payout than with online purchases, which would need to be sold to realize a purely financial reward.

To cash out bank accounts, individuals can either use a reliable cashier or can assume the identity of the bank account owner to withdraw funds. Because many bank accounts can be cashed out only from within the issuing country, criminals may prefer the use of cashiers that specialize in extracting currency from these accounts. Such cashiers use a variety of methods to convert the information into true currency, transferring money either through wire transfers or to online currency exchange accounts. They can also hire an intermediary to receive the transfer in person using a fake identity. Symantec observed requests

[59] A drop is either a secure location where goods can be delivered or a bank account through which money can be moved. The drop locations may be an empty residence or an intermediary who will reship the goods to a third location. Criminals often change the billing addresses of credit cards to safe drops that are untraceable.

[60] Online authentication services are multi-level security features provided by credit card issuers for online purchases. Consumers register their credit card with a password, which is then used to complete the online transaction.

on underground economy servers for cashiers in specific locations and of a particular gender (as matching the cashier's gender to the identity of the bank account holder is essential to not raise suspicion when withdrawing funds).

Although the process may take longer than making online purchases, the promised payouts for bank accounts tend to be higher. Symantec observed that the average advertised bank account balance, including both personal and corporate accounts, was much higher than the average advertised credit card limit—nearly $40,000 for the former, compared to just over $4,000 for the latter. Beyond straightforward account cash outs, financial accounts can also be used as intermediary channels to launder money or to fund other online currency accounts that only accept bank transfers for payments.

The third ranked category of advertised goods and services for sale was spam and phishing information, with 19 percent of the total. This category includes email addresses, email account passwords, scams, and mailers. For requests, it ranked second, with 21 percent of the total. Spam can be a serious security concern because it can be used to deliver malicious code and phishing attempts. Phishing is an attempt to trick people into divulging confidential information by mimicking, or spoofing, a specific well-known brand, usually for financial gain. Phishers attempt to obtain personal data such as credit card information, online banking credentials, and other sensitive information, which they then attempt to exploit. One estimate put the cost of phishing attacks at $2.1 billion for U.S. consumers and businesses in 2007.[61]

There are a wide variety of goods and services being advertised on underground economy servers, and many of these goods and services form a self-sustaining marketplace. Spam and phishing attempts are attractive because of their effectiveness in harvesting credit card information and financial accounts. Along with the potential financial gain from the sale of such information, amassing it can also help build an underground economy business. Profits from one exploit can be reinvested and used to hire developers for other scams, or used to purchase new malicious code or new phishing toolkits, and so on.

Email addresses can be used in tandem with mass-mailers for sending out substantial amounts of spam or phishing emails—a process that is usually accomplished using bot-infected computers.[62] A remote attacker can control a large network of compromised computers (a botnet), which can be programmed to automatically distribute spam. The addresses have typically been illegally stolen from hacked databases or harvested from public areas on the Internet, such as social networking sites and public forums, or from personal websites.

Gaining possession of email passwords can allow access to email accounts, which can be used for sending out spam and/or for harvesting additional email addresses from contact lists. Moreover, along with email, many ISPs include free Web space in their account packages, which many people rarely access. Once the ISP accounts are compromised, these free spaces can be used to host phishing sites or malicious code without the knowledge of the victims.

In addition, compromised email accounts will often provide access to additional sensitive personal information such as bank account data, medical or school information, or access to other online accounts (social networking pages, etc.). From there, it is often simple for someone to go online and use the password recovery option offered on most registration sites to have a new password sent via email and gain complete access to these accounts. This danger is compounded by the habit many people have of using the same password for multiple accounts.

[61] http://www.consumerreports.org/cro/electronics-computers/computers-internet/internet-and-other-services/net-threats-9-07/state-of-the-net/0709_state_net.htm
[62] Bots are small programs that are designed to run specific information-gathering functions. Bots can be covertly installed on a user's machine (typically through malicious code such as Trojans) to allow an unauthorized user to remotely control the targeted system through a communication channel, such as IRC, P2P, or HTTP.

Goods and services advertised by item

This metric will assess the goods and services advertised by specific item on underground economy servers, rather than by category, as above. The discussion will highlight the supply and demand trends on the servers and how this influences prices. It will also highlight the specific goods and services by item that influenced the top categories in the previous discussion.

During this reporting period, the most frequently advertised item observed on underground economy servers was bank account credentials (which consists of account numbers and authentication information), with 18 percent of the total (table 2). It was also the top ranked request, accounting for 14 percent of all specifically requested goods and services. As noted in the previous discussion, bank account credentials were the major contributor to the financial accounts category.

The large supply of bank account credentials may be due to a shift toward online banking. In the United States, 44 percent of Internet users perform some degree of online banking. That number is even higher in Canada, where 67 percent of Internet users bank online.[63] The potential increased availability of such sensitive information would likely also result in an increase in attempts to steal banking credentials through phishing attempts or the use of malicious code such as banking Trojans.

Rank for Sale	Rank Requested	Goods and Services	Percentage for Sale	Percentage Requested	Range of Prices
1	1	Bank account credentials	18%	14%	$10–$1,000
2	2	Credit cards with CVV2 numbers	16%	13%	$0.50–$12
3	5	Credit cards	13%	8%	$0.10–$25
4	6	Email addresses	6%	7%	$0.30/MB–$40/MB
5	14	Email passwords	6%	2%	$4–$30
6	3	Full identities	5%	9%	$0.90–$25
7	4	Cash-out services	5%	8%	8%–50% of total value
8	12	Proxies	4%	3%	$0.30–$20
9	8	Scams	3%	6%	$2.50–$100/week for hosting; $5–$20 for design
10	7	Mailers	3%	6%	$1–$25

Table 2. Breakdown of goods and services available for sale and requested[64]
Source: Symantec Corporation

The popularity of bank account credentials during this reporting period may be due to the ease with which this information can be used to withdraw hard currency. For example, in order to take full advantage of the flexibility of a credit card, multiple components are required, such as the credit card number, expiry date, and the CVV2 number. Perhaps more importantly, a PIN number is required in order to withdraw money from a credit card account using ATMs (most of which now have cameras monitoring transactions). On the other hand, compromised financial accounts can be relatively easily cashed out online to secure and untraceable locations using wire transfers or services offered by cashiers—sometimes in less than 15 minutes.

[63] http://www.comscore.com/press/release.asp?press=2318
[64] Descriptions and definitions for the goods and services discussed in this section can be found in Appendix B—Methodologies.

Another reason for the high ranking of bank accounts—both for sale and requested—is that some wire transfer companies, online payment services, and online currency services do not accept credit cards as forms of payment, preferring that clients use bank transfers to fund their online accounts. In addition, as stated in the "Goods and services advertised by category" discussion above, bank accounts advertised on underground economy servers are listed with higher balances on average than advertised credit card limits. The lure of relatively easy money may explain why bank accounts credentials were both the most advertised and the most requested specific item observed on underground economy servers during this reporting period.

The advertised prices for bank account credentials ranged from $10 to $1,000, with prices depending on the amount of funds available, the location, and the type of the account. Corporate accounts were advertised with considerably higher balances and, on average, were offered at more than double the price of personal bank accounts. For example, one particular bank account being advertised for $1,000 purportedly had a balance of $130,000. In addition, EU accounts were advertised at a considerably higher cost than their U.S. counterparts, which may be because EU accounts are rarer than U.S. accounts on underground economy servers. Furthermore, bank account credentials that bundled in additional information such as names, addresses, and dates of birth were advertised at higher prices, presumably because this added information could potentially be used for further identity fraud.

The second most commonly advertised item was credit card numbers accompanied by CVV2 numbers, accounting for 16 percent of all advertised goods.[65] It was also the second most commonly requested good, accounting for 13 percent of the total. CVV2 numbers are not encoded in the magnetic stripe of credit cards, nor permitted to be stored with credit card numbers in any database by merchants or agents.[66] Thus, credit card numbers with their corresponding CVV2 numbers would be especially attractive for fraud, which could explain their popularity as a requested good on underground economy servers.

Merchants at many online sites now require the CVV2 number as part of their authorization process, and the number of sites requiring this authentication is increasing. Thus, anyone trying to conduct a transaction at these sites using a stolen credit card must also possess a valid CVV2 number, which explains the popularity of credit card numbers with associated CVV2 numbers as a specifically advertised and requested item on underground economy servers.

Some advertisers selling credit cards with CVV2 numbers are claiming that they can generate the CVV2 numbers using online tools specifically designed for this purpose. There are many such tools available for download, either for a fee or for free, and most are based on "brute forcing" online merchant accounts. Brute forcing involves illegally hacking into online merchant accounts and then testing credit card-CVV2 number pairs by trying to authorize a small transaction, incrementing the CVV2 number each time until a transaction is successful. Moreover, this will not cost the hacker anything because it is typically the merchant that absorbs any fees for such transactions.[67] Brute-force attacks are possible because there are only a maximum of 1,000 combinations to test with credit card numbers employing a three-digit CVV2 and the process is easily automated.[68] Symantec believes that this is not a feasible method because credit card issuers will suspend the card after a certain number of declined authorizations.

[65] Note that these advertisements explicitly state the inclusion of CVV2 numbers with the credit card credentials for sale.
[66] http://usa.visa.com/download/merchants/rules_for_visa_merchants.pdf
[67] http://www.msnbc.msn.com/id/3078574/
[68] For credit cards with four-digit CVV2 numbers, there would be a maximum of 10,000 CVV2 combinations.

Credit cards with CVV2 numbers are typically sold in bulk, with packages ranging in size from five to 500. For this reporting period, the advertised prices of these ranged from $0.50 to $12. As with bank account credentials, prices often depended on the geographic location of the issuing bank of the credit card. In keeping with supply and demand theories, scarce numbers—such as those from smaller countries such as United Arab Emirates (U.A.E.), Qatar, and Kuwait—were advertised at higher prices than more abundant card sources such as numbers issued from U.S. banks. Along with the countries mentioned, credit cards with CVV2 numbers were advertised from issuing banks from around the world, including Canada, the European Union, India, Barbados, Costa Rica, Malaysia, and Australia. Some bulk amounts and rates for credit cards with CVV2 numbers observed for this reporting period were 100 for $70 ($0.70 each) and 500 for $300 ($0.60 each).

On some servers, there are "`check`" channels that users can join to check the validity of a credit card number, expiration date, and matching CVV2 numbers. Users can enter credit card data into the channel and an IRC bot returns an output of whether the card was approved or not approved. As with the CVV2 checking service, it is likely that the channel operator is illegally hacking into an online merchant account and attempting to authorize a card to test the numbers.[69] If approved, the user knows that the card is both valid and still active. The major disadvantage of this method is that the credit card information is broadcast to everyone in the channel and may be skimmed by another individual. During this reporting period, Symantec observed IRC chat messages that contained credit card authorizations for small donations to charities, which are likely the result of testing the validity of the credit card.[70] Small transactions—such as donations to charities that may not be part of consumers' typical spending habits but are still valid—are often not flagged as suspicious by credit card monitors.

Symantec also observed advertisements for services providing CVV2 number-checking against the corresponding credit card number and expiry date. One example was charging $10 per 1000 credit card numbers for this service. This process is identical to the brute-force method for generating CVV2 numbers stated above, except that only the one CVV2 number is checked using a hacked online merchant account. The advantage of such a checking service is that the information is still kept confidential between the customer and the checking service provider, rather than broadcast on the entire channel.

Credit cards were the third most common specific item advertised for sale on underground economy servers, making up 13 percent of all advertised goods during this reporting period.[71] For requested goods, credit cards ranked fifth, accounting for eight percent of the requested total. Credit cards advertised on the underground economy consist of the credit card number and expiry date, and may also include the name on the card (or business name for corporate cards), billing address, phone number, and PIN. It should be noted that in the previous metric, both credit cards alone and credit cards with CVV2 numbers were the major contributors to the credit card information category. This also shows that credit cards, in general, were the most popular goods advertised on underground economy servers for this reporting period.

One reason that credit cards may not be as popular as bank account credentials or credit card/CVV2 number combinations is that they are typically not as easily exploited. This is due to the time-sensitive nature of stolen credit cards and increased security measures taken by merchants, such as adding authentication service passwords, billing address checks, or requiring the CVV2 number for online

[69] Credit card transactions occur in two steps: authorization, then settlement. In the authorization process, the merchant, through an account provider, sends a request to the credit card issuer to check card validity and credit availability. Once authorized, the funds are set aside from the available credit of the cardholder. The merchant then initiates the settlement through their merchant account provider. The settlement transfers the committed funds from the issuing bank of the credit card to the merchant's account. To prevent suspension of the card, checkers do not allow initiation of the settlement so that no money is transferred from the credit card issuer and hence, no purchase is present on the legitimate cardholders' statements. (cf. http://help.yahoo.com/l/us/yahoo/smallbusiness/store/order/order-21.html)

[70] First noted in Symantec *Internet Security Threat Report*, Volume XII (September 2007): http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf : p. 43

[71] Note that these advertisements do not list that CVV2 numbers are included with the credit card credentials.

purchases. Possibly adding to this deterrence is the extra step of having to fence the goods once purchases have been made in order to realize a profit, as opposed to the more immediate reward of withdrawing funds from financial accounts, as described above.

With high profile data losses and news reports on credit card fraud, people may also be more concerned about fraudulent credit card use and may be monitoring their credit card accounts more carefully, reporting any misuse and canceling their cards quickly. The advent of online banking has also helped people to more easily keep track of any transactions posted to their credit cards. In addition, many credit card issuers have become more vigilant in monitoring all transactions and will immediately contact consumers of any suspicious activities.

Furthermore, consumers who fear identity theft and payment fraud may be moving toward Internet-based payment services and other non-credit card electronic payment services. In a recent US study, 74 percent of online consumers had used an alternative payment method for an online purchase.[72] Non-credit card electronic payment services also accounted for 30 percent of online payments in the United States in 2007, with a volume increase of 34 percent from the previous year.[73] These types of services have become more popular because they do not expose the credit or debit card information that is used to set up the accounts and, as with some credit card issuers, often offer full protection from unauthorized transactions. In addition, they allow people without credit cards to make online purchases.

Nonetheless, even though consumers seem to be moving towards other non-credit card electronic payment services for online payments, credit cards are still the most popular payment method. People may also be using credit cards over other payment options because of the added bonuses sometimes associated with using them, such as flight points, cash back options, travel options, or dividend bonuses. As mentioned in the "Goods and services advertised by category" discussion, above, there were over 22 billion credit card transactions in the United States in 2006. The total value of these transactions was estimated at just under $2 trillion—the equivalent of nearly $6,500 for each person in the United States.[74]

Credit card prices observed on the underground economy servers for the reporting period ranged from $0.10 to $25 per card number. The lower price in the range may be due to a decreased demand for credit cards that do not include the CVV2. This is also shown by the lower requested percentage for this item compared to the sale percentage. Also, this price is lower than credit cards with CVV2 numbers, which is to be expected since credit cards on their own lack the value-added information offered by credit cards and CVV2 numbers together.

Credit cards that also bundled in personal information—such as government-issued identification numbers and authentication service passwords—were offered at higher prices. The location of the issuing bank and the type of card also affected the price of the credit card. Information from regions such as Europe and the Middle East was often offered at higher prices than elsewhere because the supply of credit card information for these regions is rarer. For example, cards from countries such as the United Arab Emirates were the most costly, at an average of $25 each, while cards issued from the United States were the least expensive.

As with other areas of the underground economy, the availability of the item seems to determine its price: an increase in supply will decrease the price of the goods. There are more credit cards in circulation in the United States than in any other country in the world—1.3 billion cards by the end of 2006, which is an

[72] http://www.forrester.com/Research/Document/Excerpt/0,7211,44785,00.html
[73] http://www.businessweek.com/technology/content/nov2007/tc20071120_575440.htm?campaign_id=rss_tech
[74] http://www.bis.org/publ/cpss82p2.pdf : Tables 9 and 9d

average of four credit cards per person.[75] In comparison, there were only 70 million credit cards in circulation in the United Kingdom, an average of one per inhabitant and only five percent of the U.S. total. This correlates with the originating location percentages of credit cards advertised on underground economy servers. Cards issued by institutions based in the United States during this reporting period accounted for 74 percent of the total advertised credit cards observed on underground economy servers, while cards from institutions based in the United Kingdom accounted for 10 percent.

Credit cards are also typically sold in bulk, with lot sizes from as few as 50 credit cards to as many as 2,000. Common bulk amounts and rates observed by Symantec during this reporting period were 50 credit cards for $40 ($0.80 each), 200 credit cards for $150 ($0.75 each), and 2,000 credit cards for $200 ($0.10 each).

The third most common specific item requested during this reporting period was full identities, accounting for nine percent of the requested total. Full identities ranked sixth for advertised goods for sale, accounting for five percent of the total. A full identity can consist of a combination of the following sensitive pieces of information: full name, address, date of birth, phone number(s), government issued identification numbers, driver's license number, mother's maiden name, email addresses, and/or "secret" questions and answers to online account verifications. Since a full identity consists of many components, it may be more difficult to obtain, resulting in fewer full identities advertised for sale and an increase in the demand, given their potential versatility for fraud.

Most people associate identity theft with money because most reported cases involve criminals using the identity for activities such as obtaining credit cards, applying for loans, obtaining expensive medical or pharmaceutical treatments, or even stealing house titles.[76] However, financial identity theft is only one of the many types of identity theft that exists. The Identity Theft Resource Center (ITRC) categorizes identity theft into five major types: financial (the identity is used to obtain goods and services); criminal (the identity is used during a criminal investigation or arrest); commercial (the identity of a business is used to obtain credit); governmental (the identity is used to obtain government-issued documents such as a passport or driver's license); and cloning (the identity is assumed by another and used on a daily basis).[77] Compounding the situation for victims is that it may take months, if not years, to clear up these activities from their credit ratings once these illegal actions are detected.

One reason that would reduce the availability of full identities is that consumers may be taking more protective and preventative measures against identity fraud, such as credit monitoring, avoiding high-risk activities, and reporting suspicious activity immediately. The number of victims of identity fraud in the United States was 8.1 million at the end of 2007, a decrease of four percent from the previous year.[78] That said, even though consumers may be better educated in preventing personal identity fraud, there are still significant data breaches that could lead to identity theft exposing personal information, often on a large scale.[79] Between July 1, 2007 and June 30, 2008, there were nearly 700 reported data breaches worldwide that could lead to identity theft, which resulted in 200 million identities exposed.[80] This is an increase of 83 percent from the previous 12-month period for data breaches.

[75] http://www.bis.org/publ/cpss82p2.pdf : Tables 10 and 10b
[76] http://www.fbi.gov/page2/march08/housestealing_032508.html
[77] http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_100_-_Financial_Identity_Theft_-_The_Beginning_Steps.shtml
[78] http://www.javelinstrategy.com/products/F59339/97/delivery.pdf
[79] An identity is considered to be exposed if personal or financial data related to the identity is made available through the breach. An identity exposed by a data breach might not ever be used for fraudulent activities, though the breach will increase the probability.
[80] http://datalossdb.org/

During this reporting period, prices for full identities ranged from $0.90 to $25. As with other goods, Symantec observed that cost depended on the location of the identity, and that those from the European Union were advertised as the most expensive. The higher prices may be indicative of increased demand and lower supplies of identities from the European Union. The popularity of EU identities may also be due to the flexibility of their use, since citizens there are able to travel and conduct business fairly freely across the region.[81] Full identities were also sold in bulk, with size and price ranges including 10 for $60 ($6 each), 500 for $750 ($1.50 each), and 1,000 for $1,000 ($1 each).

On underground economy servers observed by Symantec during this reporting period, the distribution of sale advertisements are closely matched with requests for goods and services. This follows basic supply and demand principles and seems to suggest that the underground economy is acting as a valid, mature economy. In a competitive market, the pricing of goods and services is a reflection of supply and demand trends; an increase in supply or decrease in demand will drive the prices down, while a decrease in supply or increase in demand will have the opposite effect and prices will increase. The same is true in underground economy servers, as shown by the prices of goods and services. It is expected that as individual goods and services become more popular, the supply will increase and, hence, the prices will drop.

Unique samples of sensitive information

Between July 1, 2007 and June 30, 2008, Symantec monitored 44,752 unique samples of sensitive information publicly posted on underground economy servers, which accounted for 10 percent of the total distinct messages. Sellers often publicly post samples of their goods in the channels on underground economy servers. These samples serve several purposes: to prove that sellers actually have the goods in their possession; to show potential buyers the quality of goods they can expect; to enhance their credibility, and; to allow users to validate the information.[82]

Samples dealing with credit card information, such as CVV2 numbers, credit card numbers, and expiry dates, were the most common unique samples posted on underground economy servers, accounting for 56 percent of the total (table 3). Using the median value of goods and services obtained for credit card fraud of $350 per card, the potential worth of these posted credit cards during the reporting period was $2.9 million.[83] Many of the messages that posted credit card information were queries sent to channels specifically created to check the validity of credit cards using IRC bots, as discussed above in “Goods and services advertised by item.”

[81] http://ec.europa.eu/justice_home/fsj/freetravel/frontiers/fsj_freetravel_schengen_en.htm
[82] Although some information, such as credit card information, was posted multiple times due to different authorization queries, it was counted only once for this metric.
[83] http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf : p. 5

Rank	Sensitive Information	Percentage
1	CVV2 numbers	23%
2	Credit card numbers	18%
3	Credit card expiration dates	15%
4	Addresses	12%
5	Phone numbers	11%
6	Email addresses	6%
7	PINs for credit or debit cards	5%
8	Social security numbers	4%
9	Full names	4%
10	Dates of birth	2%

Table 3. Unique samples of sensitive information
Source: Symantec Corporation

Because the total unique samples of sensitive information accounted for such a relatively high percentage of the total distinct messages, this shows that there is a significant amount and variety of sensitive information to be found in underground economy servers. Since this information is publicly posted on a variety of channels and across multiple server networks, it can quickly become quite widely dispersed because it is visible to anyone on the channels and available for anyone to use. The information also often ends up reposted onto other channels, increasing the exposure. This can significantly increase the difficulty of resolving the fraud for the victims.

Value of total advertised goods

This analysis highlights the potential value if all of the advertisers active on underground economy servers observed by Symantec were to liquidate their assets. As the underground economy matures and operates more like a traditional business model, it is expected that generated revenues will increase. For example, one underground group reportedly made $4.3 million in purchases using stolen credit cards over a two-year period.[84] In another case, the U.S. government sought forfeiture on a condominium, car, and $1,650,000 in cash from a suspect in a data breach in which millions of credit and debit card numbers were stolen.[85]

Symantec calculated the total value of all goods advertised for sale using the price ranges and average bulk sizes determined in the "Goods and services advertised by item" measurement, above. The average purchase price was determined by calculating the average of the price ranges for an individual item. For items typically sold in bulk, Symantec calculated an average bulk purchase size and multiplied that by the average individual price to obtain the average purchase price.[86]

Many advertisers will state a minimum purchase quantity for many of the bulk items because it is not in their best financial interest to sell only one item at a low price, especially since some payment systems charge the seller a fee for each transaction (discussed further in the "Advertisers on Underground Economy Servers" section). Also, buyers may prefer to purchase in bulk because of the discounted prices and, in the case of personal information such as credit cards or financial data, because much of the information is time sensitive in that it may have been reported stolen during the transaction completion time. Symantec also observed sellers that offered free bonus goods for large bulk purchases, either based on quantity bought or amount spent.

[84] http://yahoo.businessweek.com/magazine/content/05_22/b3935001_mz001.htm
[85] http://blog.wired.com/27bstroke6/2008/08/11-charged-in-m.html
[93] This list includes credit cards, CVV2, full identities, proxies, email addresses, and bot-infected computers.

Symantec estimates the value of total advertised goods on observed underground economy servers was over $276 million for the reporting period. The value of credit card information was the highest during this time, accounting for 59 percent of that value (table 4). This is not surprising because credit card information was the highest priced good in the underground economy. In addition, it was the top advertised category of goods advertised for sale.

Rank	Category	Percentage
1	Credit card information	59%
2	Identity theft information	16%
3	Server accounts	10%
4	Financial accounts	8%
5	Spam and phishing information	6%
6	Financial theft tools	<1%
7	Compromised computers	<1%
8	Malicious applications	<1%
9	Website accounts	<1%
10	Online gaming accounts	<1%

Table 4. Value of advertised goods as a percentage of total, by category
Source: Symantec Corporation

Note that this value does not take into account the use of the goods, such as actually maxing out credit cards or cashing out bank accounts, which would be a calculation of the potential worth of the market. Using the median value for credit card fraud from the "Unique samples of sensitive information" discussion and the average bulk purchase size for credit cards, the potential worth of all credit cards advertised during this reporting period would be $5.3 billion.[87] Similarly, for bank account credentials, extrapolating the value using the average advertised balance of nearly $40,000, as discussed in "Goods and services advertised by category," would place the worth of all bank accounts advertised in underground economy servers during this reporting period at $1.7 billion.

These figures are indicative of the value of the underground economy and the potential worth of the market. Although law enforcement agencies have been concentrating their efforts on arresting and indicting those involved in fraud and identity theft, the global nature of these criminal enterprises increases the difficulty of locating their operations and shutting them down. In one large-scale breach, criminals were able to defraud over $10 million through credit and debit card withdrawals.[88] The financial sector has also been responding to such fraud activities by implementing stricter preventative measures, such as the updated Payment Card Industry (PCI) Data Security Standards, which is a set of requirements for enhancing payment account data security such as network requirements, encryption transmission requirements, and maintaining security policies.[89] The updated version will include incorporating best practices and improving reporting requirements.[90]

[87] This value does not take into account invalid or canceled credit cards.
[88] http://www.computerweekly.com/Articles/2008/08/07/231773/tjx-indictments-reveal-global-crime-underworld-for-id-theft-and.htm
[89] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
[90] https://www.pcisecuritystandards.org/pdfs/08-18-08_2.pdf

Malicious tools

This section of the Symantec *Report on the Underground Economy* will examine the various types of malicious tools that were advertised between July 1, 2007 and June 30, 2008 on the observed underground economy servers. Malicious tools serve as a means of producing other goods and services, but are also goods and services in their own right. This ensures a degree of self-sufficiency in the underground economy, as the skills, services, and tools needed to produce more goods and services are advertised and sought out.

Malicious tools enable attackers to gain access to a variety of valuable resources such as identities, credentials, hacked hosts, and other goods and services. Some malicious tools and services are designed to counter security measures such as antivirus software to increase the lifespan of a malicious code sample in the wild. The result is a cycle whereby malicious tools must be continuously developed and used to produce other goods and services. The profits from these goods and services may then be reinvested into the development of new malicious tools and services. The following types of malicious tools will be examined:

- Attack tools
- Spam and phishing tools
- Malicious code
- Exploits

Attack tools

This section will analyze attack kits that are marketed on the underground economy. Attack kits cover a range of tools used to generate income and other goods and services. They range from kits that automatically scan and exploit vulnerabilities to botnets. These tools may be used to provide services such as denial-of-service (DoS) attacks, spamming and phishing campaigns, and finding exploitable websites and servers. They can also be used to generate a number of goods, such as compromised hosts, credentials, personal information, credit card data, and email addresses.

The highest priced attack tool, on average, during this reporting period was botnets, which sold for an average of $225 (table 5). The advertised prices for a botnet ranged from $150 to $300, which are still reasonable prices when considering the revenue-generating potential of a botnet: a botnet can persistently produce many other goods and services; it can be rented out for a specific attacks or on a periodic basis; and it can be upgraded to create new sources of revenue.

Attack Kit Type	Average Price	Price Range
Botnet	$225	$150–$300
Autorooter	$70	$40–$100
SQL injection tools	$63	$15–$150
Shopadmin exploiter	$33	$20–$45
RFI scanner	$26	$5–$100
LFI scanner	$23	$15–$30
XSS scanner	$20	$10–$30

Table 5. Attack kit prices
Source: Symantec Corporation

Botnets are valuable assets because they enable attackers to control a network of compromised computers to perform various actions such as launch DoS attacks, scan for vulnerabilities, and conduct spam or phishing campaigns. Botnets were priced substantially higher than other advertised attack tools—more than three times the second ranked tool—likely due to their versatility, complexity, and the amount of labor involved in building the underlying malicious software and the network.

The botnets advertised included a global network of compromised computers. For example, the botnet in one advertisement claimed to include 2,000 compromised computers. In many cases, what was advertised varied. Whereas some advertisements offered the botnet itself or services offered by the bot network, some just offered the attack tools (including source code) necessary to begin a bot network. Botnet kits include methods of propagation—which could include exploits for client-side and Web application vulnerabilities—as well as social engineering capabilities that attempt to lure unsuspecting users over instant messaging protocols and email. Bot source code is valuable because it allows the buyer to modify the functionality of the botnet and add new propagation mechanisms to expand the network. Encrypted or P2P communication mechanisms can also be added to increase the value and lifespan of the network. Encryption makes it more difficult to analyze and detect traffic associated with the botnet, and P2P capabilities make the network decentralized and more difficult to shut down. Additional bot services may also be added to branch out and increase the potential of the network to generate revenue.

The second most expensive attack tool advertised during this reporting period was autorooters, with an average price of $70. These are automated tools that scan networks for vulnerable computers, which they then attempt to exploit using vulnerabilities in order to compromise as many computers as possible. This can yield shells and servers for use in other malicious activities such as spam, phishing, proxy attacks, and so forth.[91]

The third most expensive item on average during this reporting period was SQL injection attack tools, with an average price of $63. SQL injection is a type of security vulnerability that typically affects Web applications by exploiting improper input validation in database queries. A successful exploit will allow attackers to access, modify, or delete information on the database. SQL injection tools come in different varieties: some scan websites for vulnerabilities and then exploit them, while others include bot-like features or incorporate scanners for other types of vulnerabilities. There are also standalone SQL injection tools that aid with exploitation once an attacker has discovered a vulnerability.

SQL injection is a popular attack method in the underground economy due to its versatility. It can let attackers steal sensitive information stored within the back-end databases of affected websites, which can include user credentials, email addresses, personal information, and credit card numbers. In many cases, SQL injection vulnerabilities can also let attackers bypass authentication and compromise the affected Web application. Website content generated from a database can also be manipulated, potentially allowing an attacker to launch other attacks from the compromised site, such as client-side exploits or the distribution of malicious code. This mode of attack was used in early 2008 as a means of distributing malicious software.[92] Another series of SQL injection attacks were also detected soon after that.[93] In Volume XIII of the Symantec *Internet Security Threat Report*, site-specific Web application vulnerabilities were found to be prevalent, with only a small percentage being patched.[94] This makes Web applications that are vulnerable to methods such as SQL injection attractive targets for stealing information and compromising websites.

[91] A shell provides remote access to a computer, letting users execute operating system commands over the network.
[92] http://www.computerworld.com.au/index.php/id;683627551
[93] http://www.infoworld.com/article/08/05/19/Mass-SQL-injection-attack-targets-Chinese-Web-sites_1.html
[94] Please see the Symantec *Internet Security Threat Report*, Volume XIII (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 38

Interestingly, notorious attack toolkits such as MPack,[95] IcePack,[96] and Neosploit[97] are rarely discussed on the underground economy servers. Because these types of toolkits are high profile and expensive to develop, their developers may be wary of broadcasting the availability of these tools on public underground economy servers, instead preferring a more direct marketing approach. Tools advertised on the underground economy servers are often less complex and require fewer development and maintenance resources than kits such as MPack, IcePack, etc.

Development of the Neosploit kit appears to have stopped recently.[98] Symantec believes that this is because the developers could not generate new revenue at a rate that justified development efforts. There are also advertisements for competing attack tools at a fraction of the price of the Neosploit kit on underground economy servers and through other outlets. This is an interesting development because it may indicate that the demand for mass-marketed and cheaply available attack toolkits may pose a threat to high-priced, professionally developed attack kits.

There is a tendency within the underground economy to specialize in creating and marketing tools that are best suited for producing the most profitable goods and services. Spam, phishing, identity theft, and credit fraud and related activities are among the most advertised and sought after goods and services, and the attack tools discussed are designed to help facilitate these activities. It also means that goods and services outside of these high revenue activities are usually in lower demand and, therefore, tend to be advertised by specialists with particular skills and resources.

This increasing trend towards specialization and outsourcing was highlighted in Volume XIII of the Symantec *Internet Security Threat Report*, whereby the diversity of goods and services within the underground economy creates a demand for specialists in various facets of the market.[99] Each of these activities presents enough of a profit incentive for specialization to pay off. Tools must be developed, used by attackers, and the goods and services they generate must be marketed and traded. An individual who acts as a broker for various goods and services is not necessarily responsible for producing these goods and services or the tools used to generate them. This creates many opportunities throughout the supply and demand chain, which makes it beneficial to engage specialists and to outsource tasks as opposed to being directly involved at every stage. In this manner, the underground economy mirrors the legitimate software industry.

Spam and phishing tools

This section will examine the spam and phishing tools and related goods and services marketed on underground economy servers observed by Symantec during this reporting period. Products include spam software, spam relays, compromised computers to host phishing scams, and content such as phishing scam pages and phishing scam letters. Spam is used to advertise black-market products—such as pharmaceutical drugs, pump-and-dump stock scams, and pornography—and to distribute malicious code and launch phishing attacks that steal credentials, personal information, and credit card numbers.

The highest priced item during this reporting period was for the hosting of phishing scams, which was offered for an average price of $10. Prices for this service ranged from $2 to $80. Scam hosting services are often advertised with guaranteed uptime, and virtual hosts may be included in the scam page service.

[95] https://forums.symantec.com/syment/blog/article?message.uid=305505
[96] http://ddanchev.blogspot.com/2007/07/icepack-malware-kit-in-action.html
[97] https://forums.symantec.com/syment/blog/article?message.uid=314840
[98] http://www.rsa.com/blog/blog_entry.aspx?id=1314
[99] Please see the Symantec *Internet Security Threat Report*, Volume XIII Executive Summary (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 9

Scammers may also acquire domain names by using stolen currency and credit cards to use at domain name registrars. Additionally, some advertisers offer periodic rates for daily, weekly, and monthly hosting. Periodic hosting services range from less than $1 per day to $15 per day.

Scam hosters are often implicitly privy to the results of phishing campaigns because they host the data and can monitor phishing activity, and some advertisements stipulate profit-sharing for the scam hoster in any phishing operation. It is likely that other advertisers take advantage of this implicit arrangement. This makes scam hosting a very lucrative activity because the hoster can also resell goods produced from a successful scam.

Spam and Phishing Type	Average Price	Price Range
Scam hosting	$10	$2–$80
Scam pages	$10	$2–$50
Spam software	$9	$3–$20
Mailers	$7	<$1–$20
Emaill addresses (per MB)	$6	<$1–$40
Scam letters	$6	$1–$10

Table 6. Spam and phishing prices
Source: Symantec Corporation

The second most expensive item was scam pages, which were advertised for an average price of $10. Prices for scam pages ranged from $2 to $50. Scam pages are designed to spoof a legitimate website. At the very minimum, scam pages include the HTML, images, and other content necessary to spoof the targeted site. These scam pages often use actual content from the company targeted by the scam, including images, formatting, and even underlying page code. A scam page could also include back-end scripts for storing credentials and reporting on the progress of the phishing. These pages are meant to be uploaded to a scam host, so scam letters will often link to the hosted scam page. Advertisers market ready-made scam pages for particular websites, but many also offer to design custom pages. The range of prices is based on the complexity of the scam page. For example, whether the scam pages are ready-made, custom designed, or include back-end scripts. Scam pages may also be offered as part of a package deal that includes scam letters, making it cheaper to acquire the scam page and letter in a package rather than separately.

The third ranked spam and phishing tool during this reporting period was spam software, which cost an average of $9. Spam software consists of utilities such as bulk mailers and email address spiders/extractors. One example of this is a sophisticated bulk mailer application that randomizes spam messages to evade spam filters, and which can proxy and relay spam through a network of compromised computers, Simple Mail Transfer Protocol (SMTP) servers, and Web applications. Another example of spam-related software crawls the Web and extracts email addresses from websites. Such harvesters are not illegal, but their main reason for being developed is for the purposes of obtaining email addresses for spamming. Even this software is pirated and sold for a lower price in the underground economy.

Spam and phishing are popular activities in the underground economy because they have a low barrier of entry and a high return on investment. The competitive nature of these services means that goods and services are always available and constantly being updated to evade spam and phishing countermeasures. Increasingly robust countermeasures also mean that spam and phishing campaigns are typically short-lived and success requires a sustained effort. Phishers must increasingly contend with new security products and browser security features that help users determine the authenticity of websites through a combination of visual indicators, heuristics, and whitelisting/blacklisting techniques.[100] Search engine vendors are also starting to track malicious sites that host exploits, malicious code, and phishing scams. Innovations in antiphishing may increase the demand for effective phishing goods and services. If these measures are effective then this will decrease the revenue generated from phishing, affecting the frequency and success of phishing campaigns. However, as spamming and phishing-related goods and services are quite common in the underground economy, this indicates that they continue to be effective malicious tools.

Malicious code

This discussion deals with goods and services related to malicious code that are bought and sold in the underground economy. Because malicious code such as banking Trojans, back doors, and password stealers generate income for attackers, it is natural that these goods are also advertised. Much like the tools discussed already, malicious code is a constantly evolving threat due to effective security countermeasures being implemented by antivirus vendors. The result is a specific demand on underground economy servers for countermeasures to evade security strategies and antivirus software. Along with new malicious code samples that are sold in the underground economy, many of the advertisements offer variants of existing samples that claim to make the malicious code again able to evade antivirus signatures and detection engines.

Volume XIII of the Symantec *Internet Security Threat Report* noted a 136 percent increase in new malicious code threats in the second half of 2007.[101] This trend was attributed to the professionalization of malicious code development and an increased demand for threats engaging in high-profit activities such as the theft of confidential information. This increase in supply can also be correlated to the availability of obfuscation tools that allow new threats to be created for a fraction of the investment required to develop entirely new malicious code samples.

During this reporting period, on average, binders were the most expensive malicious code-related good advertised in the underground economy, with an average price of $27 (table 7). The range of prices observed for binders was from $10 to $100. Often called joiners, binders are programs that allow multiple executables to be combined into a single executable file. This can allow for the creation of hybrid malicious code samples that combine features for multiple malicious code executables. Binders can also allow legitimate or otherwise innocuous programs to be combined with malicious code executables to create Trojan horses. Programs combined in this manner may evade existing antivirus signatures. This is also a less costly activity than investing resources into the development of new malicious code samples.

[100] Whitelisting is the process where administrators and end users maintain a list of trusted websites and access is given to only those trusted sites. Similarly blacklisting consists of a list of websites that have historically been determined to be untrustworthy. Access to these sites is denied while all others are allowed.
[101] Please see the Symantec *Internet Security Threat Report*, Volume XIII (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 45

Malicious Code Tool Type	Average Price	Price Range
Binders	$27	$10–$100
Packers	$24	$4–$100
Trojans	$24	$15–$40
Keystroke loggers/password stealers	$23	$20–$30

Table 7. Malicious code prices
Source: Symantec Corporation

During this reporting period, packers and Trojans were both ranked second, with each averaging $24, although their price ranges were quite different, with packers ranging from $4 to $100, while Trojans ranged in price from $15 to $40.

Packing is a code obfuscation technique that encodes the executable code in a program file. When the program is executed, the code is decoded at runtime. The program code may also be compressed by the packing algorithm, resulting in a smaller executable that requires less bandwidth to be transferred. Packing also makes it difficult to analyze packed programs, as the executable must be unpacked before it can be analyzed. It may also be used to create variants to evade detection by antivirus software. On the low end of the price scale are packing services that are marketed on a per-executable-file basis. Packing programs that employ new algorithms are also advertised. Source code for packer programs is also marketed, which may increase the advertised price.

Packers are also used to create new variants of existing malicious code samples. New packing algorithms are valuable because they must be analyzed and understood by antivirus researchers before effective protections can be developed, which would add time to the lifecycle of malicious code samples. This makes packers a worthwhile investment for attackers because they are also less costly to develop than entirely new malicious code samples.

Trojans were the other second ranked tool observed by Symantec during this reporting period. Trojans typically allow back-door access to compromised computers, although they may be sold on the underground market for a variety of malicious activities.

The average prices for malicious code related goods and services all fall within a similar range. For example, the fourth ranked tool, keystroke loggers and password stealers, averaged only a dollar less than packers and Trojans. The pricing pattern is largely due to the short-lived nature of specific malicious code samples and because many of the malicious code tools advertised on the underground economy require development resources. The development resources invested must be offset by profits generated through malicious activities and sale of goods and services produced by malicious code. The competition between malicious code developers and the antivirus industry results in relatively low prices for goods and services because these goods and services are constantly expiring. Developers try to extend the lifespan of the malicious code samples by obfuscating the code using the various techniques described. Buyers are thus also constantly on the lookout for new malicious code samples and obfuscation programs and services. It should also be noted that most malicious code samples are not traded on the underground economy servers because many malicious code authors wish to remain low-key to increase the time that their samples remain undetected.

Exploits

Exploits constitute vulnerability information and exploit code. They differ from the other categories of attack tools in that they are not automated by nature. When exploits are incorporated into automated tools, they can then be classified as attack tools. This section covers vulnerability information and exploit code that has not been refined into automated tools.

The exploits available in the underground economy are typically tailored to specific market demands. Profitable activities in the underground economy (such as identity theft, credit card fraud, spam, and phishing) require a constant supply of resources (such as compromised personal information, credit card numbers, and hosts) to facilitate spam operations and phishing scams.

Many of these goods and services are produced by attackers who exploit vulnerabilities in Web applications and servers. The market for exploit code and vulnerability information is geared toward attackers and malicious code developers who wish to incorporate fresh exploits into attack toolkits and, therefore, represent a distinct category of their own. It should be noted that some of these vulnerabilities are likely designed to affect specific websites, while others are meant to affect a particular application or product that may be deployed on many different websites or computers. For example, browser vulnerabilities target products that are deployed on many computers, whereas exploits such as shopadmin or remote file includes (RFI) exploits may target either an application that is deployed on multiple sites or they can be site-specific in nature.

The highest ranked exploit during this reporting period was site-specific vulnerabilities in financial sites, which were advertised for an average price of $740, with prices ranging from $100 to $2,999. In some cases, it appears the same vulnerability was advertised at both the low and high ends of the price range. This may indicate that the value of the exploit decreased as it became over-traded, resulting in many attackers exploiting the same vulnerability in the same financial service. Attacks such as these are very noisy and difficult to conduct without detection, increasing the likelihood that the vulnerability will be noticed and patched by the maintainer of the affected website.

Exploits in financial services and online payment sites are the most expensive exploits advertised on the underground economy. Depending on the nature of the underlying vulnerability, an attacker may be able to compromise accounts and perform fraudulent activities such as transferring money. Because individuals in the underground economy need a secure method to obfuscate and conduct transactions, they may rely upon compromised accounts to receive payments. This makes exploits in financial sites such as online banking and payment systems an attractive target for the underground economy.

Exploit Type	Average Price	Price Range
Site-specific vulnerability (financial site)	$740	$100–$2,999
Remote file include exploit (500 links)	$200	$150–$250
Shopadmin (50 exploitable shops)	$150	$100–$200
Browser exploit	$37	$5–$60
Remote file include exploit (100 links)	$34	$20–$50
Remote file include exploit (200 links)	$70	$50–$80
Remote operating system exploit	$9	$8–$10

Table 8. Exploit prices
Source: Symantec Corporation

The next highest priced exploit, on average, is RFI exploits. These are commonly advertised by the number of vulnerable links, which is a URL pointing to a vulnerable Web page, and each link may represent a different website or domain. Multiple links can also affect a single site or domain. Five hundred RFI links sell for an average of $200, with a minimum price of $150 and a maximum price of $250. Two hundred RFI links are advertised for an average price of $70, and range from $50 to $80. One hundred RFI links have an average price of $34 and are offered for $20 to $50.

Buyers only seem to take advantage of bulk pricing if they negotiate below average prices. The average sale price for 500 links is usually higher than a buyer will pay on average for buying a combination of 100 and 200 RFI link bundles. The higher mark-up on 500 RFI link bundles could be indicative of a higher quality product, which could mean that the vulnerabilities are more recent and less likely to be patched. The high price may also deter buyers since the 100 and 200 link bundles are a better deal, which also can result in a longer lifespan for the vulnerabilities in the bundle.

Advertisers have also been observed marketing 10,000 RFI exploits for a price of $50. This may represent a list of unverified exploits that are false, commonly traded, publicly known, or patched. Therefore, the advertised exploits may have little value compared to a list of verified and functioning exploits from a reputable seller at the commonly advertised price.

There are a number of factors driving the demand for RFI vulnerabilities. First, they allow an attacker to run arbitrary code in the context of the Web server hosting the vulnerable Web application. Second, these vulnerabilities are prevalent enough that multiple advertisers can sell lists of vulnerable sites in bulk without any indication that the pool of vulnerabilities has been exhausted. These vulnerabilities are attractive because of the number of sites that are affected, the relative ease of discovering and exploiting RFI vulnerabilities, and their severity. As noted in Volume XIII of the Symantec *Internet Security Threat Report*, there is also a strong possibility that vulnerabilities in websites can remain unpatched for prolonged periods.[102]

Once exploited, an affected website can be compromised in many different ways, which yields a number of goods and services that can be resold. Once compromised, there are many options for reselling the compromised host, such as including it in a bulk list of RFI vulnerabilities. The nature of RFI vulnerabilities also allows options such as installing a C99/R57 shell and selling it, or offering a spam service via a PHP-based mailer that is injected into the vulnerable application.[103] This is because RFI vulnerabilities allow attackers to execute arbitrary PHP scripts that can be hosted from a computer that they control. Any features that can be implemented in PHP can be offered as a service through a computer that is compromised by an RFI vulnerability. Additionally, further attacks may yield user credentials, email addresses, credit card numbers and other personal information depending on the nature of the application. Phishing pages or malicious code may be also be hosted through a compromised application.

The third ranked exploit during this reporting period was shopadmin exploits. These are vulnerabilities in websites with ecommerce capabilities—hence "shop"—that let an attacker gain access to the administrative console of the ecommerce application. These applications are often prone to common vulnerabilities such as RFIs, SQL injection, and cross-site scripting. Shopadmin exploits are commonly advertised in bulk. Fifty shopadmin exploits were advertised for an average price of $150, with prices ranging from $100 to $200.

[102] Please see the Symantec *Internet Security Threat Report*, Volume XIII (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 38

[103] PHP is a widely used Web-scripting language. C99/R57 shells are implemented in PHP and they allow access to computers through a Web interface. They may also be injected into a site that is affected by an RFI vulnerability.

Less commonly, prices for individual shopadmin exploits range from $30 to $80. The prices for individual exploits typically represent private or lesser-known vulnerabilities, in contrast with the bulk offers which are more likely to be commonly traded exploits. The more people with access to information about an exploitable website or online application, the more likely it is that the vulnerability will be patched. In addition, if multiple people have compromised the same application, then the information they have compromised will be less unique. This will likely devalue the data because numerous people will end up selling the same credentials, email addresses, personal information, and credit card numbers.

Online shopping sites are attractive targets because of the amount of sensitive and financial information that is exchanged during online transactions. These sites are also the target of other fraudulent activities, such as manipulating the prices of goods and services for sale. For example, if the transactions are processed automatically, attackers can purchase goods and services for a fraction of the actual prices with a vulnerability exploit that allows them to manipulate prices.

Participants in the underground economy also need to conduct financial transactions so that goods and services can change hands. Therefore, online financial and payment services are also highly sought after assets. These market demands also foster collaboration between different types of attackers and advertisers of varying goods and services. For example, if an exploit developer needs a way of accepting payment for his goods, he may enlist the aid of someone advertising phishing services or compromised credentials for an online payment system. This scenario may also motivate the exploit developer to branch out into different areas to not only fulfill the requirements of his own activities, but to also trade many different types of goods and services. In contrast, there are also likely many advertisers who simply buy and sell services without becoming actively involved in any of the activities needed to produce these goods and services, such as developing attack tools, spamming, phishing, etc. The marketplace is sufficiently complex that an individual may have many roles, ranging from participation in malicious activities that produce the goods and services, to supporting roles that allow the goods and services to be bought and sold.

Due to the cycle of vulnerability disclosure and patching, attackers need a constant supply of new vulnerabilities and exploits so that they can continue producing other goods and services. Exploits become a good and service in their own right. Some individuals in the underground economy are devoted to discovering new vulnerabilities and authoring exploits to be sold or traded for other goods and services.

A number of advertisements are malicious in nature. Some users will attempt to lure buyers into running malicious code or visiting a malicious website that attempts to exploit a vulnerability. This type of attack may even let users steal goods from their victims, depending on whether the goods are stored on the compromised computer. This means that buyers must be aware of fraudulent or malicious advertisements. As with rippers, users who are involved in these activities are reported and ostracized by others in the underground economy once their activities are discovered.

Overall, the exploits on the underground economy servers represent a smaller portion of the goods and services available. There are a number of reasons for this, but primarily, it is because attack tools that automate scanning and exploitation of vulnerabilities are in higher demand than individual exploits and vulnerability information that must be developed into working exploit code. It is also likely that attackers, exploit developers, and malicious code developers represent a smaller demographic. Due to the technical nature of these skills, fewer individuals are adept at conducting attacks, doing security research, or developing exploit code and attack tools.

In comparison, activities such as fraud, spam, and phishing may require fewer technical skills but are also highly profitable due to a larger demand. Skilled exploit and attack toolkit developers are more likely to be found advertising their goods and services in other forums than the underground economy servers. This is because their goods and services take more skill and time to develop. Therefore, they will demand a higher price than what may be offered on the underground economy servers, especially because the exclusivity of information is an inherent property when determining the value of goods such as zero-day exploits.[104] The underground economy servers seem to be more focused on the rapid production of goods and services that can generate quick returns—which means that goods and services are mass-marketed for bulk prices with no guaranteed of exclusivity.

However, it is interesting that a small exploit market is capable of generating a large amount of goods and services. This may mean that exploits are currently undervalued in the market. Security researchers and exploit developers gain higher returns from selling their wares through more discreet and direct channels to buyers who are willing to pay a high price for exclusive and private information. However, the underground economy serves as a dumping ground for vulnerabilities that have little value in other vulnerability markets such as RFI, local file include (LFI), and cross-site scripting (XSS).[105] Exploits for these vulnerabilities have gravitated toward the underground economy servers because they not only suit the interests of individuals within the economy, but also because it represents one of the only viable markets for trading these goods.

[104] A zero-day exploit is one that appears to have been used in the wild prior to being publicly known.
[105] Local file include (LFI) vulnerabilities are specific to Web applications implemented in the PHP programming language. They allow an attacker to specify an arbitrary include path for files that are external to a vulnerable PHP script. They are local because the attacker can only specify a path to a file that exists on the computer hosting the vulnerable application. Cross-site scripting (XSS) vulnerabilities affect Web applications and allow attackers to inject content such as HTML and script code into a vulnerable Web application, which can facilitate various attacks such as theft of cookie-based website credentials, spoofing of content, and injection of exploit code into a legitimate website.

Advertisers on Underground Economy Servers

There are three primary types of traders on underground economy servers: sellers who advertise their goods and services for sale, potential buyers, and requesters who post advertisements for specific items to buy. Sellers advertise their goods and services on many different channels across many IRC server networks by listing available items via public messages.[106] Messages can range from sellers advertising one type of item ("`CCs from 3 to 5$`") to listing out an entire inventory ("`sell: USA fulls = $10 // Inboxmailer = $7 // USA CVV = $2`").[107] Sellers may also include a preferred method of payment and contact details, such as private message, email, or instant message.

Potential buyers who are interested in the goods and services listed in the public messages will privately contact the sellers to negotiate the deal and finalize payment. Payment options for these goods are conducted either through online currency exchange services, wire transfers, online payment services, or the exchange of goods. Unwilling to risk exposure, many buyers will use the services of cashiers who will convert the stolen goods, such as bank account credentials, into true currency, either in the form of online currency accounts or through money transfers. In exchange for the service, cashiers will charge a fee, which is usually a percentage of the cash-out amount.

Requesters send public advertisements on IRC channels when seeking specific goods or services to buy. This approach is different from that of a buyer because the requester is actively broadcasting to the channel with a list of the items that they are seeking, rather than passively waiting for an item to be advertised. Requesters also post job advertisements for positions such as scam developer, phishing partner, or credit card harvester.[108] Some of these job advertisements specifically seek long-term business relationships or partnerships to share in the profit, as well as offers for tutorials on hacking. As with sellers, requesters will list their preferred payment methods or the exchange of goods.

Advertisers on underground economy servers are usually self-policing and will report rippers to the administrators of the IRC servers. They will also broadcast this information across the channels to warn others. Many underground economy servers have ripper channels specifically created by the server administrators as a direct forum to report and list current rippers to avoid. Repeat rippers are often kicked off and banned from the servers.

Advertisers looking to establish a reputation may use the same nickname across many server networks; the more trusted they can become, the more business they can obtain. Criminals may prefer to deal with established vendors with good reputations as these sellers are unlikely to be rippers or disappear from the underground economy. Sellers with reputations for being able to provide the advertised high quality goods, quick delivery, added bonus items, or even who offer replacement policies for invalid goods may have large customer bases with many repeat clients.[109] But, even vendors with good reputations may still have to prove themselves by providing valid goods because one poor transaction may affect their credibility. However, the balance lies between establishing a good reputation and holding onto a nickname for too long; if the advertiser is caught with stolen personal information or laundering money, the authorities may be able to more easily trace one nickname versus many.

[106] Internet relay chat (IRC) is an Internet communications tool for real-time communications, primarily through discussion forums, commonly referred to as channels. Cf. http://www.irchelp.org/irchelp/rfc/chapter1.html

[107] In these examples, "CCs" are credit cards, "fulls" are full identities, "Inboxmailer" is a tool used to send out mass email messages as spam, and "CVV" is the Credit Verification Value 2.

[108] A scam developer is someone who creates a fraudulent scheme in order to steal money from people; a phishing partner is someone who collaborates with others to steal personal information such as credit card numbers or online banking passwords through phishing schemes; a credit card harvester is someone who is able to steal credit card information on a large scale. Please see Appendix C for full descriptions.

[109] http://www.darkoperations.net/shadowcrew/viewtopic.php-t=5103&sid=55dce3a5fefbd4597ef015fbd12bc941.htm

This section of the Symantec *Report on the Underground Economy* will examine the activities and trends of advertisers in the underground economy that Symantec observed between July 1, 2007 and June 30, 2008. The following topics will be discussed:

- Most active advertisers
- Goods and services advertised by category—top advertisers
- Messages by type—top advertisers
- Value of total advertised goods—top advertisers
- Payment systems

Most active advertisers

This discussion will focus on the most active advertisers found on the underground economy servers observed by Symantec during this reporting period. Advertisers will typically post messages across multiple channels and servers to maximize their exposure. Symantec defines the most active advertisers as those with the highest number of posted messages during the reporting period, even though these messages may not be unique. An active advertiser is one that actively posts messages on the servers. If there has been no activity on the server for 30 days or more, then the advertiser is considered to be no longer active. It should be noted that the names listed here are nicknames created by Symantec to negate any identification of the users themselves (who are using nicknames to begin with).

Between July 1, 2007 and June 30, 2008, Symantec observed 69,130 distinct active advertisers on underground economy servers and 44,321,095 total messages posted.[110] The top 10 most active advertisers accounted for 11 percent of the total messages posted. The top 10 most active advertisers accounted for only one percent of the total distinct messages, which shows that the top advertisers are likely using a high quantity of repeated messages to advertise their wares. Unlike traditional storefront businesses, the cost of advertising on underground economy servers is negligible and many advertisers spam across servers to increase their exposure.

During this reporting period, six of the top 10 most active advertisers posted credit card information as their top category (table 9), three listed financial accounts, and one listed spam and phishing. It is not surprising that the primary focus of the top most active advertisers is credit card information since it was also the top most requested category, as discussed in the "Goods and Services Advertised" section, and the advertisers will cater to market pressures on underground economy servers for easier methods to make a profit. Individuals can obtain credit card information through a number of methods such as spam and phishing attacks, monitoring and storing wireless transmissions from merchant authorization terminals, or hacking into merchant or financial databases. These types of methods can often yield a large amount of credit card information; in one large data breach, criminals were able to steal over 94 million credit cards by hacking into a company database through unencrypted wireless transmissions and installing programs to capture credit card information.[111]

[110] This does not take into account advertisers that may be using more than one nickname.
[111] http://www.msnbc.msn.com/id/21454847/

Also, as stated in the "Goods and Services Advertised" section, credit card information can be easy to use, especially for online purchases. Someone with a stolen credit card may be able to quickly complete many transactions online from around the world before any suspicious activity is detected. And since credit card information is sold in bulk amounts, if one card is suspended or invalid, another one is available to be tried.

This continues the trend noted in Volume XIII of the Symantec *Internet Security Threat Report* that advertisers are more focused on supplying goods that allow buyers to make large quantities of money quickly on underground economy servers, rather than on malicious activities that require more time and resources, such as scam pages and email lists for spamming (though these, too, can be lucrative, as discussed in "Malicious tools," above).[112] This trend is likely to continue until obtaining and exploiting such financial information is made more difficult.

Rank	Advertiser	Percentage of Messages	Top Category Advertised
1	Maggie	20%	Credit card information
2	Fergie	14%	Credit card information
3	Tesa	12%	Credit card information
4	Shadow	10%	Credit card information
5	Luna	9%	Credit card information
6	Spooki	8%	Credit card information
7	Expo	7%	Financial accounts
8	Pranda	7%	Financial accounts
9	Pepper	7%	Financial accounts
10	Fintan	6%	Spam and phishing information

Table 9. Top 10 most active advertisers
Source: Symantec Corporation

Goods and services advertised by category—top advertisers

This metric will determine the percentage of goods and services available for sale by category on underground economy servers for each of the top three most active advertisers, and will discuss how supply and demand trends have influenced each category.

The most active advertiser for this reporting period, Maggie, accounted for 20 percent of messages from the top 10 advertisers. Maggie's top advertised category was credit card information, which accounted for 48 percent of her total (figure 4). This is not surprising because the category of credit card information was also the top most requested item observed by Symantec, as shown in the "Goods and Services Advertised" section, and successful participants in the underground economy will cater to market demands. Also, credit card information may be easier to obtain since credit cards are used with such a high frequency, hence exposing the information more readily than that of financial accounts. In the United States alone, there were over 22 billion credit card transactions in 2006,[113] which would provide ample opportunity for people to steal the information and increase the supply on underground economy servers.

[112] Please see the Symantec *Internet Security Threat Report*, Volume XIII (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 19
[113] http://www.bis.org/publ/cpss82p2.pdf : Table 7

The major contributor to Maggie's high percentage of credit card advertising was her specialization in offering credit cards with CVV2 numbers, which accounted for 40 percent of Maggie's total goods advertised for sale. (I.e., 40 percent of Maggie's goods advertised were credit cards with CVV2s, eight percent were credit cards, for 48 percent of her goods.) By specializing, Maggie can concentrate on providing valid CVV2 numbers to buyers rather than dividing up her resources with items that she can purchase from other advertisers.

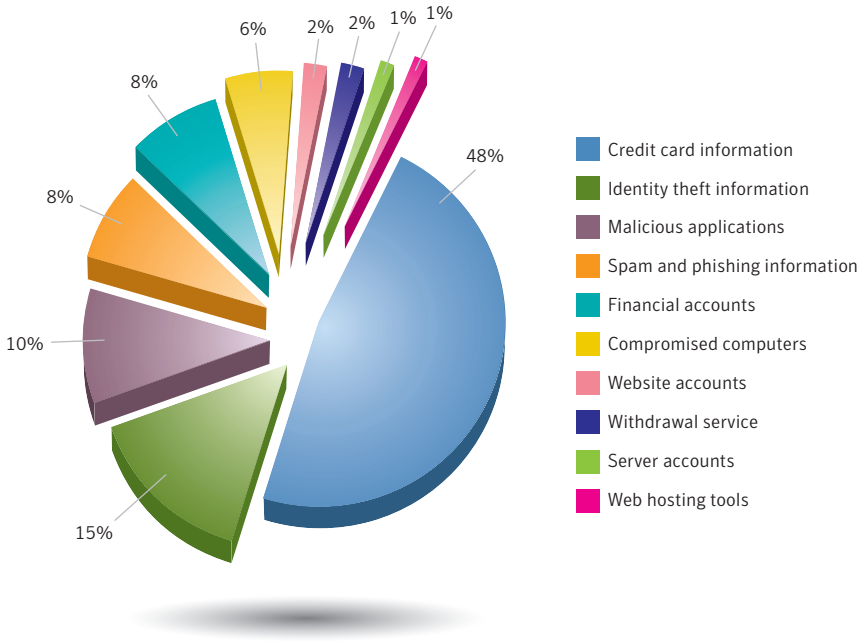


Figure 4. Goods and services advertised for sale by category, user Maggie
Source: Symantec Corporation

Along with credit card information, Maggie offered a wide array of other goods and services during this reporting period, including website accounts and malicious applications. The credit cards advertised for sale by Maggie covered 15 countries, ranging from North America, Europe, the Middle East, and Asia. As stated in the "Goods and Services Advertised" section, information from smaller markets such as Europe and the Middle East often are offered at higher prices than their more popular counterparts because the credit cards are rarer. Also, credit cards with additional information such as CVV2 numbers, billing addresses, or PINs were advertised for more since this added information could enhance the usage potential of the credit card. Many online merchants require either the CVV2 number to complete online purchases or verification of the billing address with the credit card issuer as extra layers of security.

By offering a wide variety of goods and services from around the world, major advertisers can cater to many types of buyers looking for purchases. Maggie was the only advertiser in the top three that also requested goods and services (figure 5). Although Maggie had a wide variety of goods and services, the requested goods and services were for specific items that she did not already possess, such as an exact brand of credit card, cash-out services for a specific country, and specific types of online currency accounts. It may be that Maggie is a middle-market person who brings interested buyers and sellers together since she is asking for specific goods and services. As the top active advertiser, it may be that Maggie is an established vendor with a large loyal customer base that other sellers may want to use to their advantage.

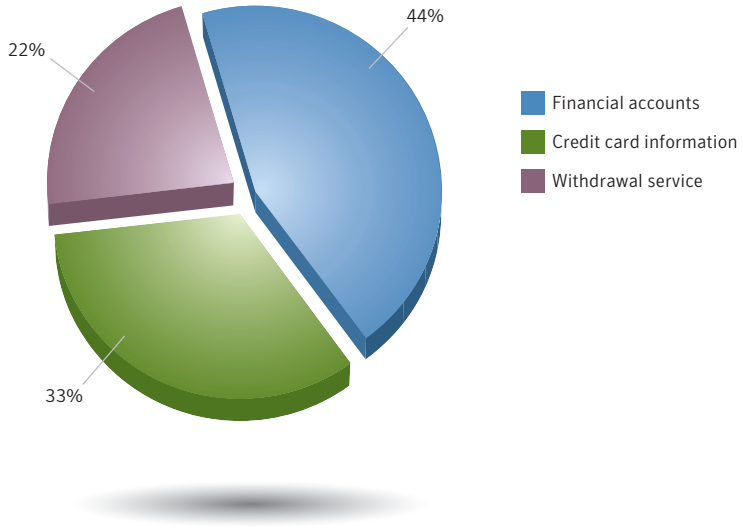


Figure 5. Goods and services requested by category, user Maggie
Source: Symantec Corporation

The second ranked advertiser for total messages during this reporting period was Fergie, who accounted for 14 percent of the messages from the top 10 advertisers. Fergie's top category of goods advertised was credit card information, which accounted for 91 percent of his total (figure 6). Fergie specialized in credit card dumps (with or without PINs) from Canada, the United States, and the European Union.

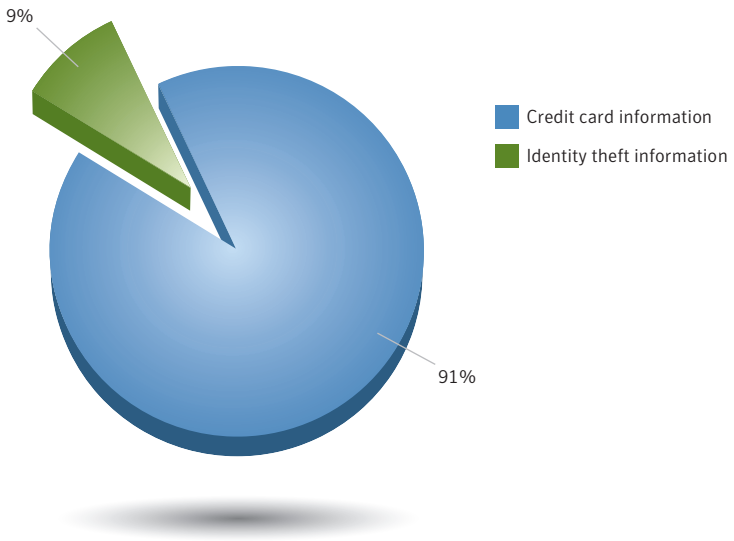


Figure 6. Goods and services advertised for sale by category, user Fergie
Source: Symantec Corporation

In the underground economy, "dump" or "full stripe" are the terms used that refer to the information contained within the magnetic stripe on a credit card, which itself is made up of two tracks. While both tracks contain the primary account number and expiration date, only the first track will contain the cardholder name and CVV.[114] Each credit card issuer will have its own standards for encoding the information in the tracks. Electronic card readers scan this information during transactions and transmit it to the credit card issuer for authorization. If the transmissions are unencrypted (or encrypted with a weak cryptosystem) and have been compromised, these transactions can be monitored either at the merchant's end or during the wireless transmissions to the credit card issuer. The magnetic stripe information on the credit card can then be illicitly recorded and put up for sale in the underground economy. In a recent major data breach, the interception of customer credit card information over wireless transmissions resulted in the theft of over 94 million credit card numbers.[115] It is estimated that between $63 million and $83 million in credit card fraud across 13 countries can be attributed to this single data breach.[116]

Because the PIN number of a credit card is not included in a credit card information dump, PIN numbers are a value-added extra item that can be used to attract buyers because they are required to withdraw currency from the credit card account when using an ATM. The information contained in a credit card dump can be used to commit fraud through the creation of counterfeit credit cards for point-of-sale purchases. The dump is encoded onto a fake credit card and can be used for card-present transactions. Since CVV2 numbers are not stored in the dump and are often required for card-not-present purchases, such as online transactions, some criminals will use online tools specifically designed to generate them.[117] Individuals can then use that information for cash outs or Internet purchases.

[114] The CVV (or CVC) number is encoded on the magnetic strip of the credit card and is used for point-of-sale or card-present transactions.
[115] http://www.msnbc.msn.com/id/21454847/
[116] http://www.securityfocus.com/news/11493
[117] https://forums.symantec.com/syment/blog/article?blog.id=grab_bag&thread.id=100

Advertised CVV2 generators purportedly use a brute-force method on hacked online credit card merchant accounts. Advertisements claim that these generators have the ability to hack into the account in order to authorize small transactions using the credit card number and a list of CVV2 numbers. CVV2 numbers are systematically incremented until a transaction is approved and the valid matching CVV2 number is revealed. For credit cards with three-digit CVV2 numbers, there are only 1,000 possible combinations, so this process can easily be automated. As stated in the "Goods and services advertised by item" discussion, Symantec believes that this is not a feasible method because credit card issuers will suspend the card after a certain number of declined authorizations. Because the credit card issuer generates the CVV2 number by encrypting the credit card number and expiration date with secret bank keys, only those with access to these keys may be able to generate the CVV2 numbers. As a precaution to this, many credit card issuers will have multiple keys for the credit cards that they issue.

Ripley ranked as the third most active advertiser, accounting for 12 percent of all messages from the top 10 advertisers. As with the top two advertisers, the top category of goods for sale by Ripley was credit card information, which accounted for 28 percent of his total (figure 7). Ripley also offered a wide variety of other goods and services, varying from full identities to proxies to credit cards with CVV2 numbers. The top four categories advertised by Ripley—credit card information, identity theft, spam and phishing, and financial accounts—are reflective of the goods and services advertised for sale on the underground economy servers overall. These four accounted for 80 percent of Ripley's advertisements and accounted for 78 percent of the overall total as stated in the "Goods and Services Advertised" section.

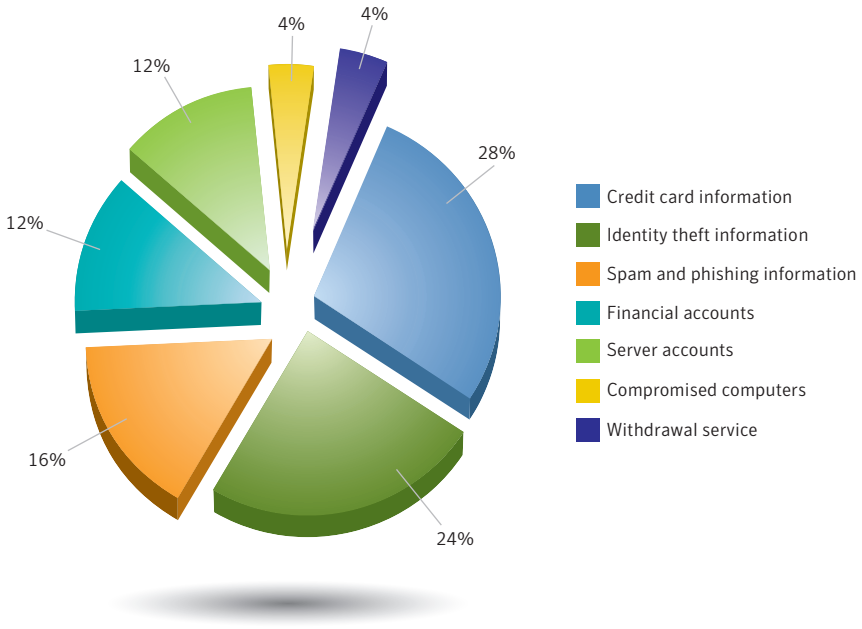


Figure 7. Goods and services advertised for sale by category, user Ripley
Source: Symantec Corporation

The distribution of the types of goods and services from the top most active advertisers follows closely with the top goods and services advertised by category. This is not surprising as most economies will cater to the demand trends of their consumers. Also, the top most active advertisers show that there are a wide variety of types of advertisers on underground economy servers, much like the different types of business in the retail sector. Some are like a large discount store, offering a wide array of goods and services, and some are similar to boutiques that specialize in one type of commodity.

Messages by type—top advertisers

Not all messages posted on underground economy servers are advertisements for goods and services. There are various types of posted messages, including some that contain sensitive information, advertisements for other servers and/or channels, and miscellaneous chat messages with other members. This metric will determine the types of distinct messages the top three advertisers posted on underground economy servers. The types of messages will give some insight into what sort of advertisers are participating in the chat rooms and also an indication of the market itself.

Between July 1, 2007 and June 30, 2008, the top distinct message type for Maggie was sensitive information, accounting for 48 percent of her total (figure 8). As discussed above in "Goods and services advertised by category," advertisers publicly post sensitive information such as credit card numbers, names, and addresses on underground economy servers for a number of reasons: to prove that they actually have the goods; to show potential buyers the quality of goods they can expect from the vendor; and to allow the buyer to validate the information before purchasing.

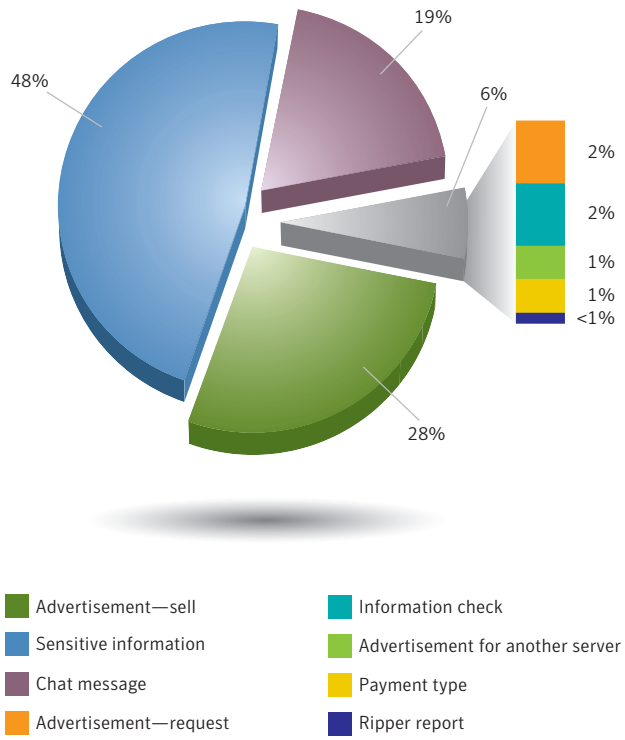


Figure 8. Types of unique messages, user Maggie
Source: Symantec Corporation

In Maggie's case, information related to identity theft—including names, addresses, phone numbers, dates of birth, and emails—accounted for 51 percent of her posted messages (figure 9). Credit card information—including credit card numbers, expiration dates, and CVV2 numbers—accounted for 33 percent, while online account information—including usernames, account numbers, passwords, and secret questions—accounted for 16 percent. Posting such sensitive information shows other members (i.e., potential customers) the type and quality of goods available. Even though some vendors may have a good reputation in the channels for quality goods, potential customers may still require proof of quality before agreeing to any transaction.

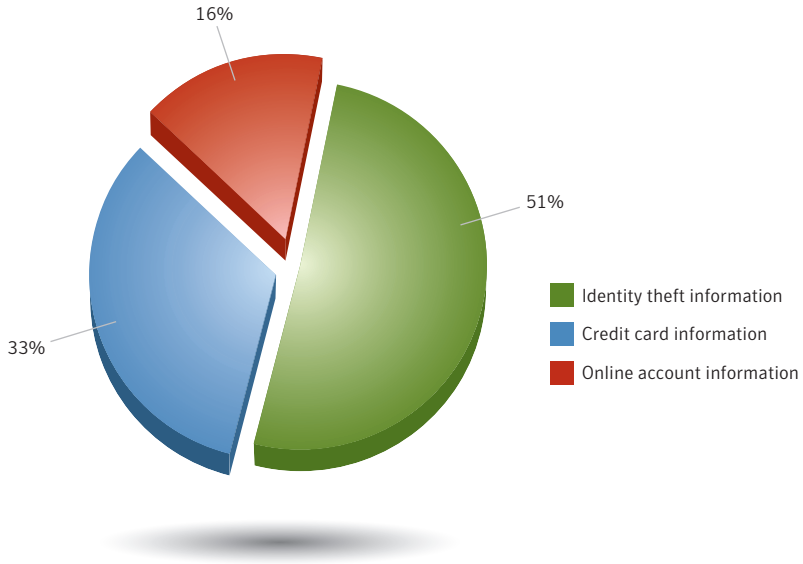


Figure 9. Types of sensitive information posted, user Maggie
Source: Symantec Corporation

During this reporting period, the top types of unique messages posted by the second most active advertiser, Fergie, were sale advertisements and chat messages, both accounting for 48 percent of his total (figure 10). A majority of the chat messages used the "`!seen`" command, which determines the last time a nickname was seen on the server. Since reputation and contacts are important on underground economy servers, Fergie may be using this command to find previous clients, either to purchase goods and services or to offer specific users something that he has for sale.

In the underground economy, buyers have no recourse to obtain refunds for unsatisfactory goods or services, apart from broadcasting to ripper channels; therefore, reputations and trusted contacts are that much more important. This is especially true within an economy based on illegal activity, because advertisers depend in large part on word-of-mouth and referrals in order to gain new business and build a good reputation. Buyers may be hesitant to conduct business with an unknown advertiser since it can be difficult to determine the advertiser's true intention—he or she may be a ripper or even someone from law enforcement posing as an advertiser. With a solid reputation behind the advertiser, buyers may be more trusting to part with more of their money.

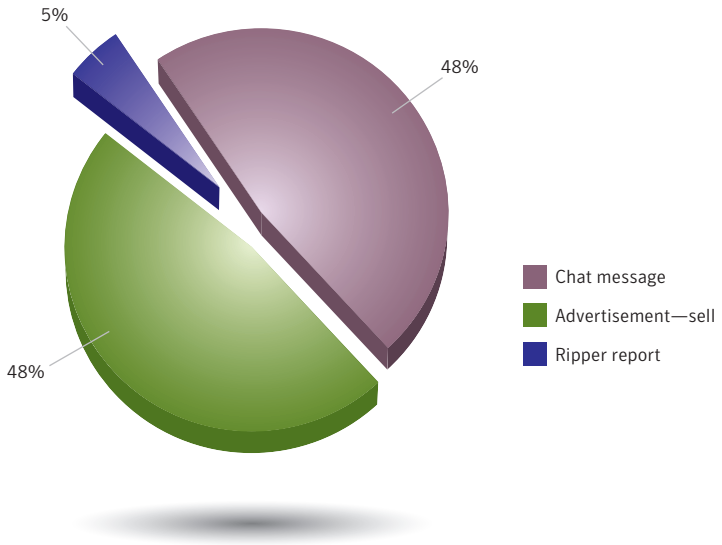


Figure 10. Types of unique messages, user Fergie
Source: Symantec Corporation

During this reporting period, the top type of unique message for Ripley, the third most active advertiser, was administrator messages, which accounted for 95 percent of his total (figure 11). This shows that Ripley is likely a services administrator on a server, since most of the messages were uptime and load average reports.[118] Many administrators use the uptime command to monitor the amount of activity on a server because it allows them to track the performance of the servers.[119] In this case, Ripley also acted as an intermediary, posting advertisements for not only his own goods, but also those of other users.

[118] Uptime measures in days how long a computer system has been up and operational since its last reboot. Load average is the moving average of the number of processes a computer is performing at any time (cf. http://www.linuxjournal.com/article/9001).
[119] In UNIX, the uptime command gives an output of time, uptime, number of users, and the 1-, 5-, and 15-minute load averages.

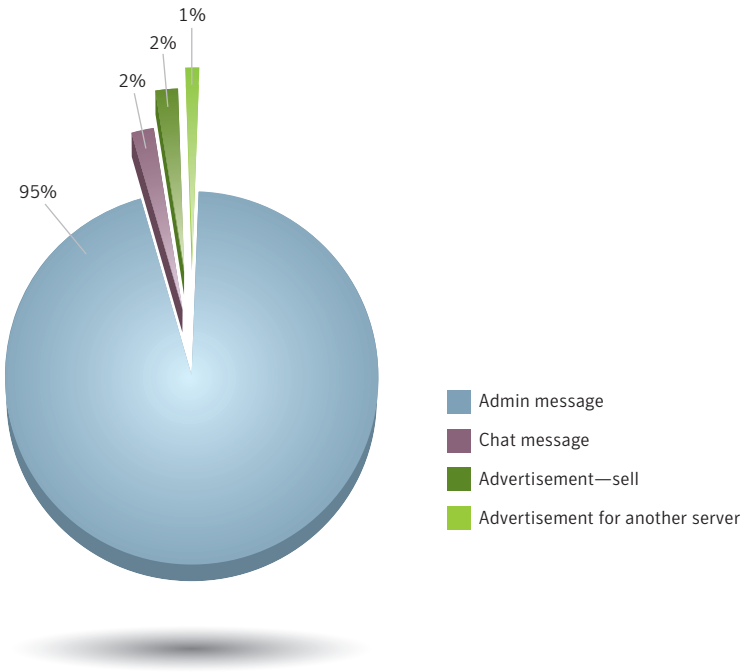


Figure 11. Types of unique messages, user Ripley
Source: Symantec Corporation

Value of total advertised goods—top advertisers

This metric will investigate the potential value of the underground economy for each of the top most active advertisers by estimating the amount each advertiser could potentially gross if he or she was to liquidate all of the goods advertised. As discussed in the "Goods and Services Advertised" section, the underground economy is potentially worth a great deal of money. For example, one illegal organization that specialized in trafficking stolen information reportedly made more than $4.3 million in purchases using stolen credit cards over a two-year period.[120] The potential value of the underground economy may be difficult to pinpoint because the number of advertisers participating in the underground economy and the number of goods sold are constantly changing.

Symantec calculated the total value of all goods advertised for sale by the top most active advertisers using the price ranges and average bulk sizes determined in the "Goods and Services Advertised" section. The average purchase price was determined by calculating the average of the price ranges for an individual item. For items typically sold in bulk, Symantec calculated an average bulk purchase size and multiplied that by the average individual price to obtain the average purchase price.[121]

Many advertisers will state a minimum purchase quantity for many of the low-priced bulk items they advertise because it is not in their best financial interest to sell only one item, especially since the most popular payment systems charge the seller a fee for each transaction. This is similar to wholesale distributors who require a minimum dollar amount for each purchase order. This ensures that they can keep prices low by increasing their average dollar sale amount.

[120] http://yahoo.businessweek.com/magazine/content/05_22/b3935001_mz001.htm
[121] This list includes credit cards, CVV2, full identities, proxies, email addresses, and bot-infected computers.

Buyers may also prefer to purchase in bulk because of the discounted prices. In the case of personal information, such as credit card or financial data, buyers may make bulk purchases to ensure that at least some of their purchase is still usable because of the time-sensitive nature of the information, since the goods may have been reported stolen during the transaction completion time. In addition, the goods may not be exclusively sold to one buyer and hence, more than one person may be using that information concurrently. This would effectively shorten the lifespan of the valid goods by increasing the likelihood of detection.

On the active servers observed during this report period, Symantec estimates that the value of the total advertised goods for the top 10 most active advertisers was over $575,000. The majority of the goods offered by these advertisers was made up of credit card information and identity theft items, which were the top two most expensive goods advertised for sale. In addition, it should be noted that the top three advertisers for this metric accounted for two-thirds of the total value of advertised goods listed above.

The value of total advertised goods does not include the usage of items such as credit card purchases or cashing out bank accounts. The potential worth of the goods can be calculated by using the median value for credit card fraud, the average bulk purchase size for credit cards, and the average advertised balance of nearly $40,000 for bank accounts. (Please see "Goods and services advertised by category" for more discussion around this.) As such, the potential worth from the top 10 most active advertisers during this reporting period of all credit cards advertised would be $16.3 million, while bank accounts advertised would be worth $2 million, for a total of $18.3 million (table 10).[122]

During this reporting period, Maggie had the highest value of total advertised goods, accounting for 25 percent of the top 10 total (table 10). This is not surprising because Maggie also had the most advertised goods and services, with 27 percent of the total for the top 10 most active advertisers. As stated in the "Goods and services advertised by category—top advertisers" metric, 63 percent of the goods offered by Maggie was made up of credit card and identity theft information, which were the most costly items advertised. The large number of credit card information and bank account credentials advertised by Maggie establishes her potential worth on the underground economy at $6.4 million.

Rank	Advertiser	Percentage of Advertised Goods, Top 10	Percentage of Goods and Services, Top 10	Value of Goods	Potential Worth
1	Maggie	25%	27%	$144,448	$6.4 million
2	Spooki	22%	15%	$128,459	$3.3 million
3	Luna	19%	18%	$108,798	$3.2 million
4	Shadow	14%	11%	$80,309	$1.7 million
5	Expo	9%	12%	$52,599	$2.0 million
6	Ripley	8%	6%	$10,728	$0.9 million
7	Fergie	1%	3%	$5,523	Not applicable
8	Fintan	1%	3%	$5,262	$0.4 million
9	Pepper	1%	2%	$4,040	$0.3 million
10	Pranda	<1%	4%	$2,185	Not applicable

Table 10. Value of total advertised goods—advertisers[123]
Source: Symantec Corporation

[122] This value does not take into account invalid or canceled credit cards.
[123] The potential worth measures the use of credit card information and bank account credentials.

The second ranked advertiser for value of total advertised goods during this reporting period was Spooki, who accounted for 22 percent of the top 10 total. Luna ranked third, with 19 percent of the top 10 total value of advertised goods. Like Maggie, a large proportion of the goods advertised for sale by both Spooki and Luna was in the credit card information or identity theft categories, accounting for 48 and 57 percent of their totals, respectively. Also, both Spooki and Luna offered a wide variety of goods in many categories.

All of the top three in this metric had credit cards as their top good advertised for sale, which was also the most expensive item listed. Credit cards are often sold in bulk packages that can include as many as 2,000 credit cards. Because of these bulk purchases, the value of the goods advertised can become very high.

Payment systems

Most payments for goods and services on underground economy servers are completed without physical interaction because members use electronic payment systems such as transfers from online currency accounts, wire transfer payments, online payment services, or the trade of goods and services. Since the transactions are electronic, advertisers can receive their payment instantly. Similar to traditional retail transactions, some advertisers prefer certain types of payments on underground economy servers and will not accept others. This metric will determine the most popular payment systems used on underground economy servers and discuss the reasons for such popularity.

Between July 1, 2007 and June 30, 2007, online currency accounts were the most popular method of payment, accounting for 63 percent of the total (table 11). Online currency accounts exchange true currency, such as U.S. dollars or Euros, into electronic currency that can be based on metals, such as gold or silver, or electronic money. As such, these e-currencies may not be affected by inflation or other fluctuations commonly associated with true currencies. The advantages of online currency accounts are that, in addition to immediate payments, the service is offered worldwide, there are no charge-backs on the payment (making them final and non-reversible once the transaction is processed by the online payment company), and the fees are charged to the vendor so the buyer does not incur a fee. By absorbing the transaction fee, the vendor may be able to attract more buyers who are seeking bargains. This is similar to the marketing technique that online stores use to attract more customers by offering free shipping with purchases.

In addition, some online currency companies do not require proof of identity to open an account, only requiring a valid email address, and users could use a proxy server to mask their IP address.[124] It is also possible to have more than one online currency account from the same company and there are no age restrictions in obtaining an account.[125] Unlike wire transfer companies and banks, online currency companies are not government regulated and are not required to monitor either their customers or suspicious transactions.[126] These reasons make online currency accounts an attractive payment system for criminals using false names for their illegal transactions. At the end of the reporting period, there were over five million online currency accounts.[127]

[124] http://www.wired.com/science/discoveries/news/2006/12/72278
[125] http://www.irishoffice.com/docs2/egold_info.htm
[126] http://www.businessweek.com/magazine/content/06_02/b3966094.htm
[127] https://www.e-gold.com/stats.html

Due to recent events involving three owners of an online electronic currency service pleading guilty to money laundering charges, some of these types of companies have begun to investigate all accounts and have suspended the creation of all new accounts.[128] Advertisers on underground economy servers, fearing the publicity and in-depth investigations, may move away from these types of payment systems in the future.

Rank	Payment System	Percentage
1	Online currency account	63%
2	Trade of goods and services	24%
3	Online payment service	9%
4	Wire transfer service	3%

Table 11. Payment systems used on underground economy servers
Source: Symantec Corporation

Trading goods and services was the second most popular payment system this reporting period, accounting for 24 percent of the total. Unlike online currency accounts and payment services, there is neither a medium of exchange nor a middle-person or company for such types of transactions, resulting in less of either an electronic or paper trail. Using the trade system, both buyer and seller can receive goods and services that they are lacking. For example, an advertiser who can easily obtain stolen credit card information can trade for goods that are difficult for the advertiser to produce, such as an online scam page or Web-based attack tool.

Online payment services ranked as the third most popular payment system, accounting for nine percent of the total. Two main reasons that online payment services are popular in the underground economy are because the buyer absorbs the fee (so the seller gets a full payment), and sellers can use credit and debit cards to fund the accounts. Because profit drives the underground economy, sellers can use stolen credit cards to load up their online payment services accounts and then use the accounts to purchase more goods from other sellers. Also, buyers may be using stolen online payment services accounts that may have been compromised or obtained through phishing attempts.

[128] Please see http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering and http://www.usdoj.gov/opa/pr/2007/April/07_crm_301.html

IRC Servers and Channels

This section of the Symantec *Report on the Underground Economy* analyzes the location, lifespan, and nature of the active underground economy IRC servers observed by Symantec between July 1, 2007 and June 30, 2008. IRC stands for Internet relay chat, and is an Internet communications tool that is based on several different protocols to facilitate real-time communications for users. Communication occurs primarily in discussion forums, called channels, where users' messages are visible to every other user in that channel, although private messaging is also possible. Channels are hosted on IRC servers, and multiple channels can exist on any given server.

In addition, IRC servers can be connected to other IRC servers to expand into a broader network, which then provides larger bandwidth and processing capacities. For example, some networks consist of more than 50 servers. This in turn supports larger numbers of users and channels. The majority of traffic occurring on IRC servers is legitimate and spans a wide variety of topics ranging from politics to pets. Currently, the largest IRC network available is dedicated to games-related discussions.[129] While IRC is a popular tool in the underground economy, other communication methods such as bulletin board systems, instant messaging applications, or Web forums (as discussed above in "Groups and Organizations") are also used to sell contraband goods and services.

An IRC server is considered to be active on the underground economy if it hosts one or more active underground economy channels. It should be noted that, even though an IRC server may be hosting an underground economy channel, many of the other channels on the server may be legitimate. The proprietors of these servers may not be concerned about illicit activity occurring therein as long as it follows the IRC etiquette and does not disrupt the server.[130] In other cases, some IRC servers are dedicated to underground economy activity and the administrator will be fully aware and supportive of the intended purpose. As well, some dedicated underground economy servers may exist on compromised computers where the proprietor of the actual computer will be unaware that the server even exists.

Users log on to IRC servers using client applications and then create or join existing channels. By default, the first user in a channel becomes the channel operator and is able to perform some administration functions on that channel such as changing topics or ejecting other users.[131] Some operators use IRC bots to keep channels active and maintain their administrative privileges.[132] IRC bots are scripts that appear as regular users and can perform a variety of automated tasks. While they typically handle administrative tasks, they can also post advertisements, launch attacks against disruptive users, or provide services for regular users, such as checking weather conditions or dictionary definitions.

There are several modes available for users and/or channels that dictate various restrictions, privileges, or attributes. For instance, the "invite only" channel mode permits a new user into the channel only by invitation from an existing user. This sort of exclusivity may benefit participants of the underground economy by ensuring that only sellers and buyers with a proven track record are allowed into certain channels. If the members of that channel only invite reputable users there would be less concern with rippers in the channel. Reputable users may also be less likely to flood the channel with excessive messages or otherwise disrupt communication in the channel. The moderators of the channel would have less work keeping the channel in order.

[129] http://searchirc.com/
[130] http://www.livinginternet.com/r/ru_chatq.htm
[131] An IRC operator is a user who has access to IRC commands that can be used to administrate channels, servers, and networks. The level of privileges for operators can differ, so an operator that can administrate a channel may not necessarily be able to administrate the server.
[132] For a description of IRC bots, please see Appendix C—Glossary.

Another example is a "moderated" channel, which allows only those users who have the "operator" or "voice status" modes attributed to them to post messages in the channel.[133] The benefit of this is similar to that of the "invite only" mode. If "voice status" is granted only to reputable users there is a smaller chance of disruptive behavior occurring in the channel. Unlike "invite only" mode, unprivileged users can still access the channel and may respond to advertisements using private messages.

When a new server becomes available on the underground economy, users are made aware of its location primarily by word-of-mouth. As discussed previously in the "Messages by type—top advertisers" section, users may post public or private IRC messages containing information about new servers or announcing that previously shut down servers are active again. Information about these servers is also spread through other Web forums, email, or instant messaging. This can be particularly important for new underground economy servers that have just been created because a lack of interest early in their lifespan may cause them to be quickly abandoned.

Underground economy channels can be very broad in their focus or quite specific. For example, some channels are dedicated to specific brands of credit cards or bank names, while others are used specifically for data verification. These verification channels would contain an IRC bot that receives user-submitted commands and automatically authenticates the validity of credit cards, as described in "Goods and Services Advertised," above. Another example of specialization is a ripper channel, in which buyers and sellers report on and monitor rippers. This process serves as a form of self-policing in underground economy servers in as much that users can be made aware of disruptive users and privileged users can kick and ban repeat offenders from their channels.

This section of the Symantec *Report on the Underground Economy* will discuss the following topics:

- IRC server lifespans
- IRC servers by region

IRC server lifespans

Due to the inherent illegality of the underground economy and the risks involved of being caught, online fraud activities have evolved into rapidly adaptable mechanisms; as such, the location and lifespans of underground economy servers are primarily driven by convenience.[134] The lifespan of each server is calculated by tracking the days between when an active underground economy channel first appears on the server and when there are no longer any underground economy channels active on the server. The first person to join a channel generally creates it and becomes the operator. In addition, the channel closes when the last person in that channel leaves. Thus, IRC server administrators often situate IRC bots with operator status in their channels to avoid closing the channel and to block malicious users from taking over the channel by achieving operator status. It should be noted that some servers were active for the entire reporting period and may have existed prior to or afterward.

[133] Channels can be configured to restrict users from posting messages unless they have been granted voice status by an administrator of the channel. Users are, however, permitted to send private messages to specific users in the channel.
[134] For a discussion of evolving adaptability of malicious activity online, please see the Symantec *Internet Security Threat Report*, Volume XIII (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

During this reporting period, the median average observed server lifespan was 10 days. Thirty-six percent of the servers observed by Symantec were active for less than one week (figure 12), 41 percent were active between one week and one month, and 21 percent were active for a period of one month to six months. Given that the percentage of observed servers in these three categories amounts to 98 percent of the total and only two percent lasted longer than six months, the average lifespan for the vast majority of underground economy servers is considered relatively short, at six months or less.

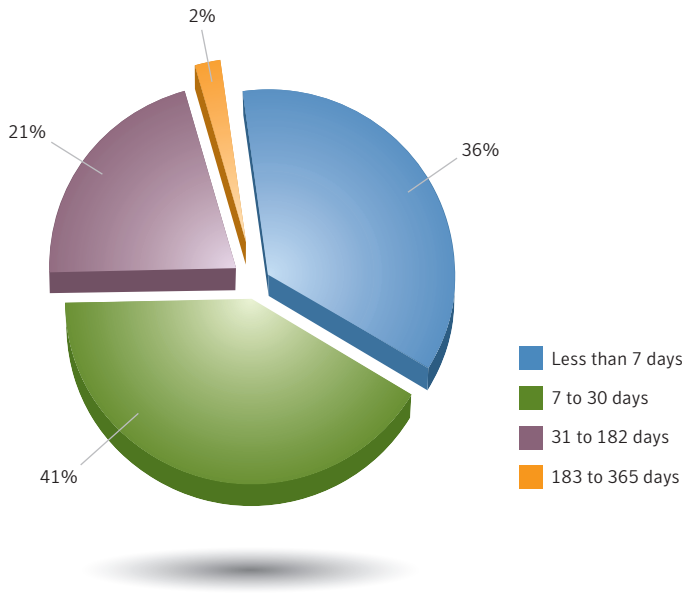


Figure 12. Average server lifespans by days
Source: Symantec Corporation

There are a number of reasons why the average lifespan of an underground economy server is so short. One factor that would reduce the average lifespan is when underground economy servers are located on compromised computers. As the popularity and traffic on one of these servers increases, it is more difficult to hide its presence, and the owner or administrator of the computer is more likely to discover the unauthorized activity and promptly shut down the server. Thus, servers that are active for longer than one month tend to be hosted on large IRC networks with a large volume of users, where there is less likelihood of the server being shut down.

Another explanation for the reduced lifespans is that proprietors of legitimate IRC servers are actively protecting themselves against illicit activity occurring on their servers, using techniques such as "channel juping" or blacklisting.[135] For example, if a user on a server tries to create or join a channel called "`creditcardsales`," and that name has been blacklisted by the administrators, the channel may be automatically closed and the user may be automatically banned from the server. Such mitigation tactics are limited, though, by the ability of users to easily modify channel names to circumvent the blacklist—changing "`creditcardsales`" to "`credit_card_sales`," for example. Channels are also created

[135] Juping is a means of blocking channels; a blacklist is a list of blocked channels, addresses, etc. maintained by administrators. It should be noted that networked servers are considered to be a single server in this metric.

using generic or non-suggestive names to obscure the intended topic. For well-established or invite only channels that rely on word-of-mouth promotion, the channel names may not be an important factor for conducting business.

Another reason is from a lack of interest or use—if a dedicated underground economy server does not attract enough users there will be little incentive to keep it active. While there can be an advantage to having a dedicated underground economy server because of a lower chance of exposure to law enforcement agencies, promoting it without exposing information to unwanted parties can be difficult and could result in a small number of users. That said, once a fraud-related IRC server becomes too exposed or widely known, it is often shut down by the IRC server administrators or abandoned by its users due to the legal liability of hosting illegal trafficking forums and an increased probability of being caught. A lack of advertising could also affect server lifespans and, furthermore, potential users might not be interested in devoting time to a server with fewer available goods or potential buyers than on the larger underground economy servers.

Underground economy servers with lifespans longer than six months are thus mainly made up of large, global networks of servers where detection and mitigation are more difficult. During this reporting period, the majority of the servers in these larger networks observed by Symantec were located in Europe, Middle East and Africa (EMEA) and North America (NAM). Typically housed on legitimate and public networks, these underground economy servers employ multiple computers in multiple regions to better handle large numbers of users, to ensure continuous uptime of the servers, and to provide regionalized services. One of the largest and most popular IRC networks consists of 26 servers in North America and 20 servers in Europe.

Hosting fraud-related servers on large networks is attractive because the heavy traffic makes it inherently difficult to monitor and police so many channels and thus reduces the chance of detection. One of the largest IRC server networks observed by Symantec had approximately 28,000 channels and 90,000 users at one point. In contrast, one of the smaller underground economy servers had only five channels and 40 users.

These types of large networks also incorporate server redundancy measures so that if one computer fails or is down for maintenance, the users on that server are immediately transferred to another computer that is still running. If a server is only hosted on a single computer, its lifespan will be directly affected if the computer goes down for some reason. Sellers may be inclined to participate on more reliable servers so that they can find and keep repeat buyers. Likewise, buyers would be able to continue purchasing from known or trusted sellers without needing to track them down across servers. Because of this, and the factors mentioned above, large-scale server networks are the most popular choice for users setting up underground economy channels. In this way, they may be regarded as safe havens for conducting business in the underground economy.

Participants in the underground economy recognize that the mechanisms must be rapidly adaptable because of the risks associated with discovery. Therefore, the short lifespans of the majority of servers may be an accepted aspect of participation. This would likely have a greater effect on newer participants attempting to establish a reputation. Established participants often have access to exclusive, invite only channels on more secure servers and would therefore be less concerned with having to deal with potential server and channel closures. Like legitimate economies, such impediments would affect the bottom line of less established participants more than experienced traders.

IRC servers by region

The regional location of underground economy servers is diverse. When these servers are shut down, users will start new servers or relocate to the most convenient server at that time. As a result, the geographic locations of underground economy servers are constantly changing. As well, people on underground economy servers operate from around the world and are not restricted to "normal" business hours. In one recent case of a high-profile breach and theft of over 46.5 million credit cards, the 11 people that were indicted came from across the globe, including the United States, Estonia, Ukraine, China, and Belarus. They operated distribution rings out of Ukraine, China, Belarus, the Philippines, and Thailand.[136]

This metric will determine the location of underground economy servers observed by Symantec during this reporting period and their distribution globally. Although the location of the server is typically not of any consequence to those involved because users of underground economy servers do most of their business electronically, it may shed light on possible safe havens of underground economy servers. The percentage of servers in each region as well as the top three countries hosting servers will be discussed.

During this reporting period, North America had the largest number of underground economy servers, hosting 46 percent of the total (figure 13); Europe, the Middle East and Africa ranked second with 38 percent; Asia-Pacific/Japan (APJ) had 12 percent; and Latin America (LAM) had five percent. These percentages are similar to those of the regional distribution of IRC networks in general and may indicate that the prevalence of underground economy servers in each region is relative to the total number of IRC servers in those regions.[137]

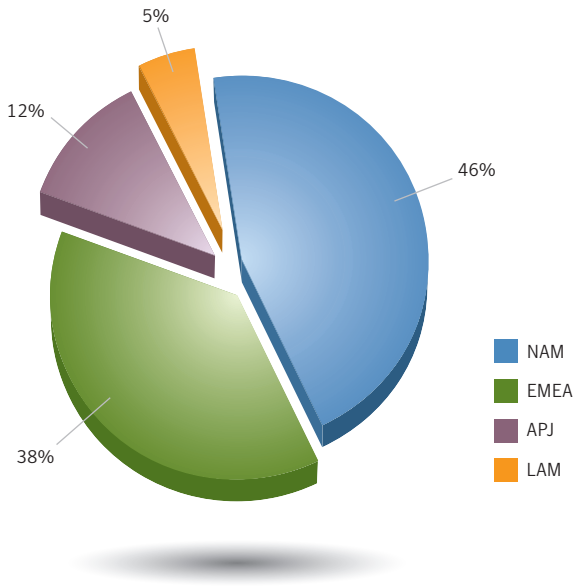


Figure 13. Regional distribution of servers
Source: Symantec Corporation

[136] http://www.securityfocus.com/news/11530
[137] http://searchirc.com/networks

One possible reason for the lower percentages in LAM and APJ is that in some countries such as China, users may not be as familiar with IRC servers and could be carrying out the majority of their underground economy communications and transactions using bulletin board systems or other instant messaging clients.[138] Additionally, there may be fewer efforts in APJ and LAM to shut down bulletin boards and forums, and users there may be more likely to rely on such existing underground methods of communication. An example of this is the numerous sting operations targeting Web forums, as discussed in "Groups and Organizations," above. Therefore, due to the precedence of legal action, users in North America and Europe may be less likely to use or create an underground economy Web forum and opt for IRC servers instead.

Another possible reason is that some countries actively attempt to control Internet content and usage as a way of limiting the influences from outside the country. Monitoring and controlling content may be more challenging on IRC servers than on other communication tools. As a result, these countries may attempt to restrict IRC access when possible, which would lead to difficulties in hosting IRC servers and reaching potential users. In addition, due to the existence of many large-scale, public IRC server networks in the NAM and EMEA regions, users in other regions may have little incentive to start their own servers. In other words, the users in LAM and APJ may prefer to participate in trade on these well-established servers rather than put out the effort of starting and promoting their own.

On a per country basis, the largest contributing country by a significant margin was the United States, which hosted 41 percent of the total observed servers worldwide (table 12). One explanation for such a large percentage of servers is that there are over 75 million broadband Internet users in the United States.[139] Also, some major IRC server networks have large proportions of their servers located in the United States. Considering that there is also a large amount of cybercrime that occurs in the United States, it is not surprising that this country accounts for the largest percentage of underground economy servers.[140] For instance, Symantec has observed that the United States ranks first for percentage of hosted phishing websites.[141] These websites are frequently used by criminals to acquire goods to be sold in the underground economy. As stated above, the regional distribution of underground economy servers appears to be relative to the total servers in each region. Considering that NAM consists of a smaller number of countries than other regions, in addition to the above information, it makes sense that the United States accounts for the majority of underground economy servers.

[138] See section 5.1 of http://honeyblog.org/archives/147-Technical-Report-Studying-Malicious-Websites-and-the-Underground-Economy-on-the-Chinese-Web.html
[139] http://point-topic.com
[140] See any of: http://www.circleid.com/posts/us_slammed_major_host_cybercrime/, http://www.usatoday.com/tech/news/computersecurity/infotheft/2006-10-11-cybercrime-hacker-forums_x.htm, or http://voices.washingtonpost.com/securityfix/2008/08/report_slams_us_host_as_major.html
[141] Please see the Symantec *Internet Security Threat Report*, Volume XIII (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 68

Rank	Country	Percentage of Servers	Region
1	United States	41%	NAM
2	Romania	13%	EMEA
3	Germany	11%	EMEA
4	United Kingdom	6%	EMEA
5	Canada	5%	NAM
6	Australia	4%	APJ
7	Brazil	3%	LAM
8	South Korea	2%	APJ
9	Netherlands	2%	EMEA
10	Sweden	2%	EMEA

Table 12. Top countries by number of underground economy servers
Source: Symantec Corporation

Romania had the second highest percentage of underground economy servers, accounting for 13 percent of the total. This may be a result of a strong pattern of cybercrime that has emerged in Romania recently.[142] Romania has suffered from slow economic growth in recent years, resulting in a lack of employment opportunities. A well-established tradition of computer skills in the country combined with such employment hardships may contribute to the temptations of cybercrime.[143] Media reports suggest that fraud and corruption are serious problems in Romania and cybercrime continues to be a factor in both of these issues.[144] This may explain the high percentage of underground economy servers there because those carrying out identity theft may be compelled to create their own servers to subsequently sell the goods. This is supported by previous Symantec analysis that showed Romania emerging as the largest host of phishing websites in EMEA, an indication of the amount of Internet-fraud related activity occurring there.[145]

While there is a large amount of cybercrime occurring in both the United States and Romania, the difference in the number of broadband users may explain why there is such a large gap in the percentages of underground economy servers in each country. The fact that Romania, with approximately 2.25 million broadband Internet users compared to the 75 million broadband Internet users in the United States, was still host to 13 percent of the global underground economy servers indicates that there is a higher than expected level of illicit trade occurring there. A smaller number of broadband users would normally indicate that there is a smaller potential for users to access the Internet—let alone host or participate in the underground economy—so the relatively high percentage of underground economy activity in Romania may be cause for concern.

[142] http://www.cbsnews.com/stories/2003/10/20/tech/main578965.shtml
[143] http://news.bbc.co.uk/2/hi/technology/3344721.stm
[144] See http://bucharest.usembassy.gov/US_Citizen_Services/Visiting_Living/Corruption.html or http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9110222
[145] Symantec *Internet Security Threat Report*, Volume XIII Executive Summary (April 2008): http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf : p. 10

Germany had nearly the same percentage of underground economy servers as Romania, with 11 percent of the total observed by Symantec. In past years, Germany was the largest host of phishing websites in EMEA, however it ranked third in 2007. Despite the drop, the history of phishing activity indicates that there is still a significant amount of Internet-fraud related activity occurring there. There is also a strong computer infrastructure in Germany, and it also ranks in the top five countries worldwide for the number of broadband users.[146] However, Germany still has 50 million fewer users than the United States, which may explain why the percentage of underground economy servers there is significantly less than in the United States, despite ranking high in this metric. On the other hand, the proportionally high levels of underground economy servers hosted in Germany may be interesting for similar reasons to those for Romania's ranking; that is, there exists a relatively modest number of broadband users compared to a relatively high percentage of global underground economy servers hosted within the country.

The United States, Romania, and other top-ranking countries in this metric may all be perceived as regional safe havens for underground economy servers inasmuch that, unless a channel becomes very popular, it may go largely unnoticed. That is to say that, despite law enforcement efforts to monitor or close underground economy servers, the immense volume of legitimate IRC activity in some regions may provide opportunities for the servers to go unnoticed. Similarly, large-scale public IRC server networks would be appealing for the same reason because users may be more willing to use a channel on one of these servers instead of a channel on a server with fewer people in a different region.

[146] http://point-topic.com

Software Piracy

This section of the Symantec *Report on the Underground Economy* examines software piracy over a public-domain peer-to-peer (P2P) file-sharing protocol that was observed by Symantec across a three-month period between July and September, 2008. For the purpose of this report, a user is deemed to be a single IP address from which one or more files are being uploaded, and a file instance refers to a complete instance of software that is available for download. Because this metric only measures software piracy occurring over one P2P protocol, regions where other file distribution methods may be more popular—such as other P2P protocols, FTP, or the duplication and distribution of physical media such as CD-ROMs—will be under-represented here. In determining the potential costs of piracy in each category, the manufacturers' suggested retail price (MSRP) of the software is used wherever possible to approximate the value of each file.

This section will look at the following topics:

- File instances by category
- Financial effect on business sectors
- File instances by country
- Users by country

File instances by category

This section of the Symantec *Report on the Underground Economy* assesses the total number of file instances observed in the software categories delineated by Symantec.[147] Measuring the number of file instances in each category provides insight into the popularity of piracy in these software categories, and may also indicate which business sectors are most affected by piracy. It may also provide insight into the motivations of people pirating software. For example, users may be more motivated to download software that has a high retail sales price. Another factor could be the geographical variance in software release dates, particularly for games; users wanting access to a game as soon as possible could resort to piracy in the absence of a commercially available version in their region. In addition to these reasons, some people may be pirating software for the purpose of creating and selling physical counterfeits.

During this reporting period, desktop computer games were the most uploaded software by a significant margin, accounting for 49 percent of all file instances observed (figure 14). The high percentage of desktop game files indicates that software in this category is both readily available and a popular target of piracy. Given the steadily increasing popularity of electronics games, this is not surprising. Retail sales of desktop games reached $9.5 billion in the United States alone in 2007, a 28 percent increase from 2006.[148] In comparison, retail sales in the United States of software other than games were an estimated $3.3 billion in 2007.[149] Another study worked out the 2007 total to be an average of nine games sold every second of every day.[150]

Another possible explanation for the large number of desktop game files is that their popularity often relies on their entertainment and replay value.[151] People may quickly move from game to game, and thus increase the demand for new titles. Desktop games are also much easier to pirate than console games, which are often released on proprietary media formats, as discussed further below.

[147] Please see Appendix B—Methodologies for a full description of the software categories.
[148] http://www.theesa.com/facts/pdfs/ESA_EF_2008.pdf
[149] http://www.eweek.com/c/a/Windows/US-Software-Market-Posts-Best-Performance-in-7-Years/
[150] http://www.theesa.com/newsroom/release_detail.asp?releaseID=8
[151] http://www.economy-point.org/r/replay-value.html

Software such as business, multimedia, and utility applications would have greater longevity because they are intended for continuous use and not for entertainment purposes. Considering this and the smaller percentages in other categories, the majority of users may be pirating software primarily for recreational purposes rather than for business use.

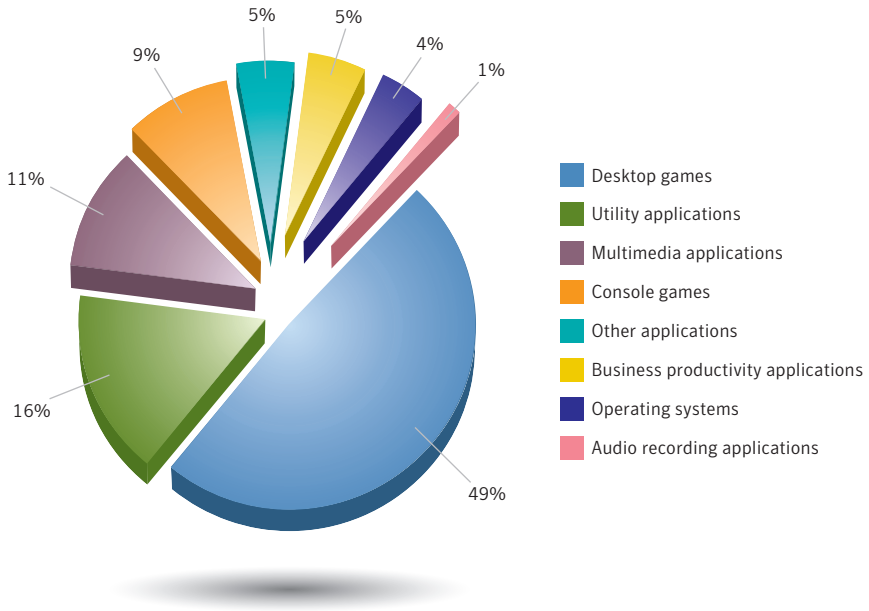


Figure 14. Number of file instances per category
Source: Symantec Corporation

The second ranked category of file instances observed during this reporting period was utility applications, with 16 percent of the total.[152] This is not surprising given the prevalence of computers in most regions of the world and the large number of utility applications available in the marketplace. Furthermore, a high number of utility applications will likely lead to a greater number of new versions and updates, especially given that many such smaller applications tend to go through many version releases. There are several possible reasons for the frequency of updates and versions for smaller applications. Small companies may not have the research and development or quality assurance resources necessary to ensure that each release is error free. Also, smaller companies with only one or two smaller applications will likely be able to dedicate more time to developing and marketing those products. Each new version of an application that is released would generate an opportunity for piracy of a new file.

The third most pirated software category was multimedia productivity applications (such as photo editors, 3D animation editors, HTML editors, etc.), with 11 percent of the total. One explanation for the piracy of this category is cost: the median MSRP for multimedia software is estimated to be $1,300—more than twice the median MSRP of any other category (table 13). Casual users of the software or hobbyists may not be willing to pay this much for software. Moreover, regional differences in pricing and income may also be a factor; for instance, in some countries $1,300 is more than the average annual household income. People in such regions may be less inclined to spend money on software, thus increasing the demand and inclination for pirated goods.

[152] Often defined as anything outside of an OS or application suite, Symantec defines utility software as applications such as CD writing applications, data compression tools, media players, etc.

Considering that nearly 60 percent of the file instances observed were in the two game categories, the majority of the files appear to be uploaded by users pirating software for recreational purposes, indicating that these users are more likely to pirate software than businesses. According to one study, however, applications in the utility and multimedia categories are the most frequently pirated software by businesses, indicating that businesses may still represent a considerable portion of the users observed.[153]

Financial effect on business sectors

While measuring by the number of file instances shows the popularity of pirating games, measuring by the potential market value of the files gives a different picture because the retail costs for different categories vary widely. Given the significant development time and labor that goes into the production of some software such as operating systems or application suites, the potential cost of the piracy to industries could be much greater, even though there may be fewer file instances for such categories. Anti-piracy measures that are integrated into software may have an effect on this as well. Some operating systems and software suites require users to validate the authenticity of the software with the company before certain features can be accessed or updates can be acquired. This validation is often performed after a serial number or product key has been used, and is essentially another layer of protection. Users are required to actively validate authenticity over the Internet or by telephone. Furthermore, some of this software is also configured to stop working after a specific number of days if it is not validated. Defeating these protection measures can be very time consuming and may discourage some users from pirating software if a viable workaround is not available.

During this reporting period, there were far more file instances crowded into the lower-value end of the scale. While individual MSRP prices ranged from $20 to $8,000, the average cost per file for all the categories was just $50. In total, the approximate U.S. retail value of all file instances observed by Symantec was $83.4 million (which, it should be noted, is only what that Symantec observed being pirated via one P2P protocol during a brief period). The annual global cost to businesses of software piracy likely dwarfs this figure, and one 2007 study puts the cost at nearly $40 billion.[154]

On a category basis, observed instances of multimedia software accounted for fully two-thirds of the $83.4 million total. Although the volume of file instances for multimedia software was only 11 percent, it accounts for over $53 million of the total estimated value of all software piracy observed by Symantec (table 13). This is far more than all the other categories combined and is likely due to the high prices of multimedia software, discussed above.

Although multimedia software companies have been at the vanguard of copyright protection, users have often kept pace with “cracks” that enable them to get around such protections. Thus, efforts to shore up copyright protection through techniques such as digital rights management (DRM) have had mixed results and in some cases limited success.[155] Some of the skills used to crack software protection can be useful in locating and exploiting vulnerabilities. As a result, the individuals who crack pirated software may also be involved in other aspects of the underground economy such as compromising computers or gaining unauthorized access to e-commerce websites. As mentioned above, protection methods that require additional validation to extend usage times or access certain content and updates may be more effective than traditional methods because they require more effort to bypass. In certain cases, the resulting negative reaction from consumers regarding attempts to implement DRM has compelled companies to

[153] http://www.siia.net/press/releases/2-AntiPiracy_YIR_2007.pdf
[154] http://www.itwire.com/content/view/12171/53/
[155] DRM refers to techniques for controlling the usage of digital media or devices. Cf. http://www.webopedia.com/TERM/D/DRM.html

shy away from implementing such restrictions. With the potential of file-sharing protocols, many companies are rethinking their approach to longstanding publishing and distribution models to adapt to the challenges posed by illegal file sharing.[156]

Rank	Category	Approximate Value	Percentage of Total Value of Categories	Price Range of Software	Percentage of File Instances
1	Multimedia applications	$53,098,000	65%	$40–$8,000	11%
2	Business productivity applications	$8,671,000	11%	$400–$700	5%
3	Desktop games	$8,062,000	10%	$50	49%
4	Audio recording applications	$2,992,000	4%	$250–$700	1%
5	Utility applications	$2,573,000	3%	$20–$230	16%
6	Operating systems	$2,237,000	3%	$100–$220	4%
7	Other applications	$2,152,000	3%	$30–$600	5%
8	Console games	$1,286,000	0%	$35–$60	9%

Table 13. Approximate dollar values of software file instances observed[157]
Source: Symantec Corporation

Business software, which includes applications such as accounting and word processing tools, was the second ranked category in dollar value, with an estimated $8.67 million of the total. Like multimedia, this category made up much less of the volume than desktop games, with only five percent of the file instances observed by Symantec, but its high median price of $680 lifts its ranking in this measurement.

For the third ranked category, desktop games, the inverse was true. Although the volume of desktop games far exceeded any other, with 49 percent, the estimated total value for this category was just over $8 million because the files were valued at an average of $50, far less than either of the top two ranked categories by value.[158] Thus, despite a much larger volume of file instances, the cost of desktop game piracy is much less than the estimated $53 million value of multimedia software piracy.

File instances by country

Measuring the file instances by location will provide insight into where software piracy is most prominent and where specific categories are most freely uploaded. The top 10 countries by total number of file instances and the top three countries in each category are examined here. Determining the countries from which pirated software is being distributed was measured using the location of users uploading files. It should be noted however, that users can obfuscate their true locations through the use of network proxies. In these cases, the locations observed will be those of the proxy computer and not the actual user.

During this reporting period, the top ranked country by number of file instances was the United States, with 19 percent of the total—nearly three times higher than any other country (table 14). One reason that may explain this is that the United States also has the most broadband users in the world, with over 75 million users.[159] The potential for software piracy over the Internet may be more prevalent in countries with well established Internet communities and a large number of broadband users. Broadband access

[156] http://www.buzzle.com/articles/fairuse4m-cracks-open-copy-protected-downloads.html
[157] Please see Appendix B—Methodologies for descriptions of the software categories
[158] http://www.gamepro.com/article/features/141348/are-60-games-here-to-stay/
[159] http://point-topic.com

facilitates faster data transfer rates due to high bandwidth capabilities. File sizes of pirated software are often quite large, some being over four gigabytes, making downloading over a slower connection difficult, if not impossible.

Rank	Country	Percentage
1	United States	19%
2	United Kingdom	7%
3	Canada	6%
4	Spain	5%
5	Brazil	5%
6	Poland	5%
7	France	4%
8	Sweden	3%
9	Netherlands	3%
10	Australia	2%

Table 14. Top countries by total file instances
Source: Symantec Corporation

The United Kingdom ranked second for total number of file instances with seven percent, followed closely by Canada with six percent. Like the United States, the United Kingdom and Canada both have well-established Internet infrastructures and high broadband penetration.[160] Because the United Kingdom and Canada also rank in the top three in most of the software categories, discussed below, it appears that there is no categorical bias to piracy activity occurring in these countries. That is to say that the rankings of these countries are due to a relatively consistently high number of file instances in each category as opposed to an extremely high number in a single category and lower numbers in the others.

The top countries by total file instances all rank in the top 25 countries by number of broadband Internet users.[161] This could indicate that countries with a large number of broadband users also have a large number of users pirating software. However, China has the second highest number of broadband users in the world, but only ranks 34th for number of file instances, with only one percent of the total observed by Symantec during this reporting period. Therefore, there is a strong possibility that while countries with the largest number of people pirating software typically have a large number of broadband users, the reverse may not be true. One possible reason for this is that physically pirated or counterfeit software is more popular than Internet piracy in some regions. For example, one syndicate of counterfeiters in Asia reportedly sold more than $500 million in pirated software before the operation was shut down.[162]

The possession of physical products may also be preferable for users in some regions. This would be especially true of countries where digital distribution methods have not entered the mainstream. This can occur in regions with low broadband penetration. For example, broadband users in the United States represent 26 percent of the U.S. population, while broadband users in China represent only six percent of that country's population. Users without broadband access may be more inclined to acquire pirated software in other ways, such as physical counterfeit copies. Alternatively, users in these countries may

[160] http://www.point-topic.com
[161] http://www.point-topic.com
[162] http://losangeles.fbi.gov/pressrel/2007/la072307.htm

prefer using other methods of file sharing, such as FTP. Some countries have less enforcement against file-sharing websites or services. As a result, pirated content over HTTP and FTP may be more readily available in these countries.

The high rankings for the United States, United Kingdom, and Canada for total file instances may also indicate a lack of availability of pirated software in languages other than English. Of the instances observed, only two specified that the software was available in a language other than English. This may also indicate that users pirating software in other languages prefer to use websites and trackers specific to their region or language. When a non-English speaking country accounts for a large percent of pirated software in a specific category, it may be an indication that the desirability of that software transcends the language preference of the users.

For desktop games, the top three ranked countries were the United States with 14 percent, Poland with eight percent, and Brazil with seven percent (table 15). The rank of the United States is not surprising given the high broadband penetration there, as mentioned, and that game files are typically quite large so users without broadband connections may be less inclined to download them.

Because this is the only category in which Poland and Brazil rank in the top three, the majority of software being pirated in these two countries may constitute desktop games. A lack of availability of desktop games available in Polish or Portuguese may be the reason for this, leading users to opt for the English versions over other available language versions. Another possible reason for Poland and Brazil ranking high in this category is the regional variance of game releases.[163] For example, someone in Poland wanting to play the latest video game may be inclined to acquire a pirated copy of the game if it is released earlier in North America than in Europe.

Rank	Country	Percentage
1	United States	14%
2	Poland	8%
3	Brazil	7%

Table 15. File instances of desktop games, top three countries
Source: Symantec Corporation

For console games, Spain ranked first by a significant margin with 44 percent, followed by France and the United States with just six percent and five percent, respectively (table 16). Spain's high rank is assumed to be primarily due to a judicial ruling that permits modifying console hardware to play media formats other than the proprietary formats most manufacturers employ for their games, which is illegal in most countries.[164] These modifications can also override security measures built into the software. Thus, people in Spain may be less concerned about legal liability when modifying game consoles to play pirated games. Furthermore, a lack of legal liability may mean that acquiring modification chips and having them installed is easier in Spain than in other countries, thus reducing the difficulty of using pirated console games.

[163] http://www.vgreleases.com
[164] Because publicly available media writing devices and software often cannot write data in the propriety formats used by most console game units, users must burn the games onto a standard media format such as a DVD. To play these DVDs then requires altering the console hardware and firmware by installing a modifier chip and loading third-party firmware. Cf. http://www.xbox-hq.com/html/article871.html

Rank	Country	Percentage
1	Spain	44%
2	France	6%
3	United States	5%

Table 16. File instances of console games, top three countries
Source: Symantec Corporation

The business productivity category is the second category in which Spain ranked first—again by a significant margin—with 32 percent, compared to the eight percent that France and the United States each had in the second and third rank (table 17). The frequency of pirated business software in Spain over elsewhere could be due to pricing trends; software often costs significantly more in some countries than in others, and one popular software suite costs nearly twice as much in Spain as it does in the United States. As a result, the appeal of pirated business software may be higher in a country like Spain. One study found that approximately 40 percent of Spanish software distributors are linked to the distribution of illegal software.[165]

Rank	Country	Percentage
1	Spain	32%
2	France	8%
3	United States	8%

Table 17. File instances of business software, top three countries
Source: Symantec Corporation

In all of the remaining categories—utility, multimedia, operating systems, and audio recording applications—the top three ranked countries were the United States, United Kingdom, and Canada, in that order (table 18). The consistency of these rankings is assumed to primarily be a reflection of regional language and broadband usage patterns, as discussed earlier. This ranking pattern may also indicate that there is no regional special interest for applications in these categories, unlike business software piracy in Spain, for example.

Rank	Top Country	Percentage: Utility Applications	Percentage: Multimedia Applications	Percentage: Operating Systems	Percentage: Audio Recording Applications
1	United States	25%	27%	25%	27%
2	United Kingdom	9%	8%	7%	8%
3	Canada	7%	7%	5%	6%

Table 18. File instances of remaining categories, top three countries
Source: Symantec Corporation

[165] http://www.iipa.com/rbc/2007/2007SPEC301SPAIN.pdf

Users by country

The location of users is used to determine the countries with the highest number of users providing files for download. Users are only counted once regardless of the number of files they are providing.

During this reporting period, the United States had the largest number of users, with 19 percent of the total (table 19). There were nearly three times as many users in the United States than there were in the United Kingdom, which was ranked second with seven percent. The third largest number of users was from Canada, making up six percent of the total.

These results emphasize the significant number of users located in the United States. While most of the countries in the top 10 were within a few percentage points of each other, the United States had significantly more users than any other country. This could explain why the United States ranked first with a significant percentage of the total file instances observed, because a large number of users should correlate to a large volume of file instances. The country rankings by user, in fact, are nearly identical to the country by number of file instances measure, and the related percentages are very similar. The only difference in rank between the two measurements is with Brazil and Spain, which swap places at fourth and fifth on the two charts with just slight variations in their totals.

Rank by Percentage	Country	Percentage	Rank by Total File Instances
1	United States	19%	1
2	United Kingdom	7%	2
3	Canada	6%	3
4	Brazil	5%	5
5	Spain	5%	4
6	Poland	5%	6
7	France	4%	7
8	Sweden	3%	8
9	Netherlands	3%	9
10	Australia	2%	10

Table 19. Top 10 countries by number of users
Source: Symantec Corporation

File instances per user ranged from five to 267 files and the median number of file instances per users was seven. This indicates that the percentage of users sharing a large number of files is substantially low. Considering this and the rankings above, the number of file instances per user has far less of an effect on the number of file instances per country than does the number of users.

As the popularity of P2P file sharing grows and more people use it for piracy, the regional distribution of users and file instances will likely increase and shift. This may result in regional user bases that come to more closely mimic regional broadband usage. This may be especially true of countries such as China, where broadband usage is already high but the penetration is low, meaning there is a large potential for broadband growth. Furthermore, because there is no cost to users for downloading the software, aside from ISP traffic fees where they exist, an increase in the number of users and a more even regional distribution could adversely affect counterfeiting operations. This presents an interesting situation; as "free" piracy becomes more feasible for users around the world, legitimate software producers will still be financially affected; however, people who profit from the sale and production of physical counterfeit will also be financially affected. The negative effect on counterfeit sales could very well force some counterfeiting operations to go out of business.

Appendix A—Protection and Mitigation

There are a number of general measures that enterprises, administrators, and end users can employ to protect against fraud-related activities. Organizations should monitor all network-connected computers for signs of malicious activity including bot activity and potential security breaches, ensuring that any infected computers are removed from the network and disinfected as soon as possible. Organizations should employ defense-in-depth strategies. Defense-in-depth emphasizes multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection methodology. Defense-in-depth should include the deployment of antivirus, firewalls, and intrusion detection systems, among other security measures.

Administrators should update antivirus definitions regularly and ensure that all desktop, laptop, and server computers are updated with all necessary security patches from their operating system vendor. As compromised computers can be a threat to other systems, Symantec also recommends that enterprises notify their ISPs of any potentially malicious activity, such as bots. Symantec recommends that organizations perform both ingress and egress filtering on all network traffic to ensure that malicious activity and unauthorized communications are not taking place. Organizations should also filter out potentially malicious email attachments to reduce exposure to enterprises and end users.

Identity fraud mitigation

To reduce the likelihood of identity theft, organizations that store personal information should take the necessary steps to protect data transmitted over the Internet or to limit the exposure of confidential information stored on their computers by successful intrusions. This should include the development, implementation, and enforcement of secure policy requiring that all sensitive data is strongly encrypted and educating users on the proper procedures for using such programs. Encrypting sensitive data that is stored in databases will limit an attacker's ability to view and/or use the data. However, this step will require that sufficient computing resources be made available, as encrypting and decrypting the data for business use consumes processing cycles on servers. Furthermore, encrypting stored data will not protect against man-in-the-middle attacks that intercept data before it is encrypted. A man-in-the-middle attack is a form of attack in which a third party intercepts communications between two computers. The third party captures the data, but still relays it to the intended destination to avoid detection. This can allow the attacker to intercept communications on a secure or encrypted channel. As a result, data should always be transmitted through secure channels such as SSH, SSL, and IP Sec.

Organizations should also enforce compliance to information storage and transmission standards such as the PCI standard.[166] Policies should be put in place and enforced that ensure that computers containing sensitive information are kept in secure locations and are accessed only by authorized individuals. Sensitive data should not be stored on mobile devices that could be easily misplaced or stolen. This step should be part of a broader security policy that organizations should develop and implement in order to ensure that any sensitive data is protected from unauthorized access. Security processes and systems should be regularly tested to ensure their integrity.

To help prevent fraud, credit card issuers and banks could take more secure measures to verify and authenticate users. The Federal Financial Institutions Examination Council (FFIEC) requires banks in the United States to implement appropriate risk mitigation strategies, which may include upgrading to layered

[166] https://www.pcisecuritystandards.org/

security or to a multi-factor authentication (MFA) security system for online banking.[167] Multi-factor authentication depends on two or more of the following categories of factors for a user: something they have (bank card, smart card), something they know (password, PIN), and something they are (retinal scan, fingerprint). For example, online banking is considered to be a single-factor authentication since the user logon ID is not considered secret, while banking at an ATM is multi-factor. By instituting effective multi-factor authentication and multi-level security systems, banks and credit card issuers can make it more difficult for criminals to exploit stolen financial information. Also, security features such as Smart Card-based credit cards using the EMV standard for security verification,[168] one-time use credit card numbers, or an embedded security token in a credit card that generates one-time pass codes,[169] can make it more difficult for criminals to obtain and use financial information.

Consumers could also take more security precautions to ensure that their information will not be compromised. When conducting higher-risk Internet activities, such as online banking or purchases, consumers should do so only on their own computers and not on public computers such as those in Internet cafés or libraries. If consumers do use public computers, they should ensure that the cache is cleared and cookies are deleted after use. Further, they should not store passwords or bank card numbers on their computers. They should also avoid following links from emails as these may be links to spoofed websites. Instead, they should manually type in the URL of the website. Also, consumers should be aware of the amount of personal information that they post on the Internet, as this information can be used in malicious activities such as phishing scams or email harvesting schemes.

Phishing mitigation

Symantec recommends that enterprise users protect themselves against phishing threats by filtering email at the server level through the mail transfer agent (MTA). Although this will likely remain the primary point of filtering for phishing, organizations can also use IP-based filtering upstream, as well as HTTP filtering. DNS block lists also offer protection against potential phishing emails.[170] Organizations should also consider using domain-level or email authentication in order to verify the actual origin of an email message. This can protect against phishers who are spoofing email domains.[171]

To protect against potential phishing activity, organizations should educate their end users about phishing.[172] They should also keep their employees notified of the latest phishing attacks and how to avoid falling victim to them, as well as provide a means to report suspected phishing sites.[173] Symantec also advises that users never view, open, or execute any email attachment unless the attachment is expected and comes from a known and trusted source, and unless the purpose of the attachment is known. Also, users should be suspicious of any email that is not directly addressed to their email address.

By creating and enforcing policies that identify and restrict applications that can access the network, organizations can minimize the effect of malicious activity, and hence, minimize the effect on day-to-day operations.

[167] http://www.ffiec.gov/pdf/authentication_guidance.pdf
[168] EMV is a standard for authenticating credit and debit card payments. The name originates from the initial letters of Europay, MasterCard and VISA, who together developed the standard. Cf. http://www.emvco.com/about.asp
[169] http://www.incard.com/products.html
[170] A DNS block list (sometimes referred to as a black list) is simply a list of IP addresses that are known to send unwanted email traffic. It is used by email software to either allow or reject email coming from IP addresses on the list.
[171] Spoofing refers to instances where phishers forge the "From:" line of an email message using the domain of the entity they are targeting with the phishing attempt.
[172] For instance, the United States Federal Trade Commission has published some basic guidelines on how to avoid phishing. They are available at: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.htm
[173] A good resource for information on the latest phishing threats can be found at: http://www.antiphishing.org

Organizations can also employ Web-server log monitoring to track if and when complete downloads of their websites, logos, and images are occurring. Such activity may indicate that someone is attempting to use the legitimate website to create an illegitimate website for phishing. Organizations can detect phishing attacks that use spoofing by monitoring non-deliverable email addresses or bounced email that is returned to non-existent users. They should also monitor the purchasing of cousin domain names by other entities to identify purchases that could be used to spoof their corporate domains.[174] So-called typo domains[175] and homographic domains[176] should also be monitored as this may indicate potential phishing websites. This can be done with the help of companies that specialize in domain monitoring; some registrars also provide this service.

New security products and browser security features help users determine the authenticity of websites through a combination of visual indicators, heuristics, and whitelisting/blacklisting techniques. The use of antiphishing toolbars and components in Web browsers can also help protect users from phishing attacks; search engine vendors track malicious sites that host exploits, malcode, and phishing scams. These measures notify the user if a Web page being visited does not appear to be legitimate. This way, even if a phishing email reaches a user's inbox, the user can still be alerted to the potential threat. End users should use an antiphishing solution. As some phishing attacks may use spyware and/or keystroke logging applications, end users should use antivirus software, antispam software, firewalls, toolbar blockers, and other software detection methods. Symantec also advises end users to never disclose any sensitive personal or financial information until they can confirm that any request for such information is legitimate.

Users should review bank, credit card, and credit information frequently as this can provide information on any irregular activities. For further information, the Internet Fraud Complaint Center (IFCC) has also released a set of guidelines on how to avoid Internet-related scams.[177] Additionally, network administrators can review Web proxy logs to determine if any users have visited known phishing sites.

Vulnerability mitigation

Administrators can use a number of measures to protect against the effects of vulnerabilities. They should employ a good asset management system to track what assets are deployed on the network and to determine which ones may be affected by the discovery of new vulnerabilities. Vulnerability management technologies should also be used to detect known vulnerabilities in deployed assets. Administrators should monitor vulnerability mailing lists and security websites to keep abreast of new vulnerabilities in Web applications.

Symantec recommends that administrators employ vulnerability assessment services, a vulnerability management solution, and vulnerability assessment tools to evaluate the security posture of the enterprise. These measures should be incorporated into infrastructure change management processes. Unpatched vulnerabilities should be identified by administrators, and assessed and mitigated according to the risk they present. Where possible, problematic applications with many unpatched vulnerabilities should be removed or isolated. Intrusion protection software (IPS) systems can aid in detecting known attacks against such applications. Event management should also be integrated into the enterprise infrastructure to aid in policy compliance.

[174] "Cousin domains" refers to domain names that include some of the key words of an organization's domain or brand name; for example, for the corporate domain "bigbank.com", cousin domains could include "bigbank-alerts.com", "big-bank-security.com", and so on.
[175] Typo domains are domain names that use common misspellings of a legitimate domain name, for example the domain "symatnec.com" would be a typo domain for "symantec.com".
[176] A homographic domain name uses numbers that look similar to letters in the domain name, for example the character for the number "1" can look like the letter "l".
[177] http://www.fbi.gov/majcases/fraud/internetschemes.htm

When deploying applications, administrators should ensure that secure, up-to-date versions are used, and that applications are properly configured to avoid the exploitation of latent vulnerabilities. Symantec recommends the use of secure shared components that have been audited for common Web application vulnerabilities. As much as possible, enterprises are advised to avoid deploying products that are not regularly maintained or that are not supported by the vendor.

Website administrators can reduce their exposure to site-specific vulnerabilities by conducting a security audit for common vulnerabilities affecting their sites. Web application code should be audited prior to being released to production systems. When developing Web applications, organizations should investigate the availability and applicability of secure libraries to perform validation of user-supplied input. Secure development practices and threat modeling should also be employed when developing Web-based applications. Web-application firewalls may also detect and prevent exploitation of Web-based vulnerabilities on production sites.

To protect against successful exploitation of Web browser vulnerabilities, Symantec advises users and administrators to upgrade all browsers to the latest, patched versions. Symantec recommends that organizations educate users to be extremely cautious about visiting unknown or untrusted websites and viewing or following links in unsolicited emails. Administrators should also deploy Web proxies in order to block potentially malicious script code. While attacks are likely to originate from websites that are trusted as well as those that are not, Web browser security features can help reduce exposure to browser plug-in exploits, as can whitelisting. Specifically, administrators and end users should actively maintain a whitelist of trusted websites, and should disable individual plug-ins and scripting capabilities for all other sites. This will not prevent exploitation attempts from whitelisted sites, but may aid in preventing exploits from all other sites. Only plug-ins that have been audited and certified should be installed on workstations throughout the organization.

For zero-day vulnerabilities, Symantec recommends that administrators deploy network and host-based IDS/IPS systems as well as regularly updated antivirus software. Security vendors may provide rapid response to recently discovered zero-day vulnerabilities in the wild by developing and implementing new or updated IDS/IPS and antivirus signatures before a patch has been released by the affected vendor. Behavior-blocking solutions and heuristic signatures may also provide protection against zero-day vulnerabilities.

Organizations can also implement a whitelist policy at the network perimeter to regulate outgoing access by end users. Content filtering may also be employed to strip potentially malicious content from trusted and untrusted sites. Antivirus and host-based IDS and IPS solutions at the desktop level also provide a layer of protection against attacks that originate from the Web. IPS technologies can prevent exploitation of some browser plug-in vulnerabilities through signature- or behavior-based approaches. In addition, some IPS systems may provide further protection against memory corruption vulnerabilities in the form of address space layout randomization (ASLR), and by making memory segments non-executable.[178] These measures may complicate the exploitation of such vulnerabilities and make it more difficult for attack payloads to execute; however, this security measure may not protect all applications by default. Antivirus software may also aid in protecting organizations from browser plug-in exploits through heuristic signatures.

[178] Address space layout randomization is a security measure to complicate exploitation of some classes of vulnerabilities by randomizing the layout of process address space to make it less predictable to attackers.

Enterprises should subscribe to a vulnerability alerting service to be notified of new vulnerabilities. They should also manage their Web-based assets carefully. If they are developing Web applications in-house, developers should be educated about secure development practices, such as the Security Development Lifecycle and threat modeling.[179] If possible, all Web applications should be audited for security prior to deployment and only those applications that have been certified should be deployed. Web application security solutions and a number of products and services are available to detect and prevent attacks against these applications.

Individual Web users should also exercise caution when browsing the Web. Since these attacks can result in hijacking of open sessions, users should make sure to log out of websites when their session is complete. Users should also be wary of visiting untrusted or unfamiliar sites. Scripting and active content can also be disabled when casually browsing the Web.

Malicious code mitigation

Symantec recommends that certain best security practices always be followed to protect against malicious code infection. Administrators should keep patch levels up to date, especially on computers that host public services and applications—such as HTTP , FTP , SMTP , and DNS servers—and that are accessible through a firewall or placed in a DMZ. Email servers should be configured to only allow file attachment types that are required for business needs and to block email that appears to come from within the company, but that actually originates from external sources. Additionally, Symantec recommends that ingress and egress filtering be put in place on perimeter devices to prevent unwanted activity.

To limit the propagation of threats through removable drives, administrators should ensure that all such devices are scanned for viruses when they are connected to a computer. If removable drives are not needed, endpoint security and policy can prevent computers from recognizing these drives when they are attached. Additionally, policy and user education should be implemented to prevent users from attaching unauthorized devices to computers within the enterprise.

Administrators should ensure that all email attachments are scanned at the gateway to limit the propagation of email-borne threats. Additionally, all executable files originating from external sources, such as email attachments or downloaded from websites should be treated as suspicious. All executable files should be checked by antivirus scanners using the most current definitions.

For threats that use the CIFS protocol to propagate, all shares should be protected with strong passwords, and only users who require the resources should be given access to them. If other users do not need to write to a share, they should only be given “read” permissions. This will prevent malicious code from copying itself to the shared directory or modifying shared files. Finally, CIFS shares should not be exposed to the Internet. Blocking TCP port 445 at the network boundary will help to protect against threats that propagate using CIFS.

Enterprises should take measures to prevent P2P clients from being installed on any computers on the network. They should also block any ports used by these applications at the network boundary. End users who download files from P2P networks should scan all such files with a regularly updated antivirus product.

[179] The Security Development Lifecycle is a development paradigm that incorporates security at every stage from the initial architecture to programming, and in the quality assurance/testing phases. Threat modeling is a security auditing methodology that involves formally identifying and mapping out all possible attack vectors for an application.

Appendix B—Methodologies

Goods and Services Advertised

This section is based on data that is gathered by proprietary Symantec technologies that observe activity on underground economy servers and collect data. Underground economy servers are typically chat servers on which stolen data, such as identities, credit card numbers, access to compromised computers, and email accounts are bought and sold. Each server is observed by recording communications that take place on its channels, which typically includes advertisements for stolen data. This data is used to derive the data presented in this metric. It should be noted that this discussion is not meant to be representative of Internet-wide activity; rather, it is intended as a snapshot of the activity that Symantec monitored during this period.

Goods and services advertised by category

The following list shows the categories used for this metric and the goods and services included in each category:

- **Compromised computers:** Includes goods associated with compromised computers such as hacked computers, bot-infected computers, and shells.
- **Credit card information:** Includes goods that pertain to credit cards such as credit card numbers, CVV2, and credit card dumps.
- **Financial accounts:** Includes goods associated with financial services such as bank account numbers, magnetic stripe skimming devices, online payment services, online currency accounts, and online stock accounts.
- **Identity theft information:** Includes goods that can be used in identity theft such as full identities and Social Security numbers.
- **Malicious applications:** Includes Web-based attack tools and malicious code.
- **Retail accounts:** Includes accounts from retail services such as gift cards for online stores and online auction accounts.
- **Server accounts:** Includes accounts for file transfers and virtual networks.
- **Spam and phishing information:** Includes goods that can be used for spam and phishing such as email addresses, email passwords, scams, and mailers.
- **Website accounts:** Includes online accounts to specific websites such as social networking sites.
- **Withdrawal service:** Includes services such as cash out and drops that are used to withdraw money and items from purchases.

Goods and services advertised by item

Description of goods and services advertised on underground economy servers may vary from vendor to vendor. The following list shows typical goods and services that are found on these servers and general descriptions of each:

- **Bank account credentials:** Bank account credentials may consist of name, bank account number (including transit and branch number), address, and phone number. Online banking logins and passwords are often sold as a separate item.
- **Cash out:** Cash out is a service where purchases are converted into true currency. This could be in the form of online currency accounts or through money transfer systems and typically, the requester is charged a percentage of the cash-out value as a fee.
- **CVV2 Number:** Credit Verification Value 2 (CVV2) is a three- or four-digit number on the back of the credit card and used for card-not-present transactions such as Internet or phone purchases. It is also known as the Card Validation Code 2 (CVC2), Card Identification Digits (CID), or Card Verification Value (CVV). This was created to add an extra layer of security for credit cards and to verify that the person completing the transaction was in fact, in possession of the card. This value differs from the CVV, which is encoded on the magnetic strip of the credit card and used for point-of-sale or in-person transactions.
- **Credit cards:** Credit cards may include name, credit card number, PIN, billing address, phone number, and company name (for a corporate card). Credit cards with CVV2 are often advertised as a separate item.
- **Email addresses:** These consist of lists of email addresses used for spam or phishing activities. The sizes of lists sold can range from 1 MB to 150 MB. There can be as many as 40,000 email addresses in each MB of data sold.
- **Email passwords:** These can include account information for emails including user IDs, email address and password. In addition, the account will contain personal information and email addresses in the contact list.
- **Full identities:** Full identities may consist of name, address, date of birth, phone number, and Social Security number. It may also include extras such as driver's license number, mother's maiden name, email address, or "secret" questions/answers.
- **Mailers:** A mailer is an application that is used to send out mass emails (spam) for phishing attacks. Examples of this are worms and viruses.
- **Proxies:** Proxy services provide access to a software agent, often a firewall mechanism, which performs a function or operation on behalf of another application or system while hiding the details involved, allowing attackers to obscure their path and make tracing back to the source difficult or impossible. This can involve sending email from the proxy, or connecting to the proxy and then out to an underground IRC server to sell credit cards or other stolen goods.
- **Scams:** Vendors sell malicious Web pages that pose as legitimate pages for phishing scams. They also offer services for hosting the pages, usually priced per week, given the transitory lifespan of many phishing sites.

Unique samples of sensitive information

To evaluate this metric, Symantec determines the number of unique samples of sensitive personal information being posted on the servers. The occurrences of each type of sensitive information (below) is calculated as a percentage of the total. Personal information includes:

- Full name
- Credit card number
- Expiry date
- CVV2
- PIN for credit and debit cards
- Social Security number
- Home address
- Phone number
- Email address
- Date of birth

Value of total advertised goods

Symantec determines the value of all goods advertised based on the average purchase price for each good and service. This was determined by calculating the average of the price ranges for an individual item. For items typically sold in bulk, Symantec calculated an average bulk purchase size and multiplied that by the average individual price to obtain the average purchase price. This list of bulk items includes credit cards, CVV2, full identities, proxies, email addresses, and bot-infected computers. Only distinct messages are used to determine the total value of advertised goods.

The potential worth of the market takes into account the use of the goods, such as using the credit cards or cashing out bank accounts. This value was calculated using the median value for credit card fraud, the average bulk purchase size for credit cards, and the average advertised balance of bank accounts advertised in underground economy servers during this reporting period.

Malicious tools

To develop the metrics for malicious tools, Symantec has analyzed the price data for a number of commonly advertised goods and services. Since the focus of this section is pricing data for goods and services, only those goods and services for which pricing information is available are discussed.

Advertisers on Underground Economy Servers

Most active advertisers

Symantec determined the most active advertisers as those with the highest number of posted messages during the reporting period, even though these messages may not be unique. An active advertiser is determined as one that has been actively posting messages on the servers. If the advertiser is no longer actively posting messages for 30 days, it is assumed that after such time the advertiser is no longer active on the server. It is important to note that the real user names have been changed to prevent identification.

Goods and services advertised by category—top advertisers

This metric will determine the percentage of goods and services available for sale by category on underground economy servers for each of the top three most active advertisers from unique messages. The categories are defined in "Goods and Services Advertised" methodology.

Messages by type—top advertisers

This metric will determine the types of unique messages the top three most active advertisers posted on underground economy servers. The following list shows the types of messages posted on underground economy servers and general descriptions of each:

- **Advertisement—sell:** The goods and services for sale by the user.
- **Advertisement—request:** The goods and services the user is seeking to purchase.
- **Advertisement for another server:** Posts by the user to promote other channels, servers, or services outside of the current channel.
- **Chat message:** Personalized messages sent to other users. Often these messages do not include any information on goods and services.
- **Information check:** These messages are used to find out more information about goods that the advertiser may have or check if the information is accurate and valid. Examples of this may include trying to find a CVV2 for a credit card number or checking if a credit card number is valid.
- **Payment type:** Messages that are posted to inform potential buyers of the payment systems that the advertiser accepts.
- **Ripper report:** Channel broadcasts about suspected rippers. Often this will include what the ripper is accused of and how much the advertiser has lost.

- **Sensitive information:** Posted messages with sensitive information for others on the channel. Advertisers publicly post sensitive information on underground economy servers to prove that the seller actually has the goods, to show potential buyers the quality of goods they can expect from the vendor, and to allow the buyer to validate the information before purchasing. Categories of sensitive information are:
  - **Credit card information,** including credit card numbers, expiration dates, and CVV2 numbers.
  - **Online account information,** including usernames, account numbers, passwords, and secret questions.
  - **Identity theft information,** including names, addresses, phone numbers, email addresses, Social Security numbers, and dates of birth.

Value of total advertised goods—top advertisers

Using the top 10 most active advertisers, Symantec determines the value of all goods advertised by advertiser, based on the average price associated with each good and service and average bulk purchase size as determined in the "Goods and Services Advertised" section. Only distinct messages are used to determine the total value of advertised goods.

The potential worth of the top 10 most active advertisers takes into account the use of the goods, such as using the credit cards or cashing out bank accounts. This value was determined using the same methods as in "Goods and Services Advertised" section.

Payment systems

Symantec determines the most popular payment systems used on underground economy servers by calculating the usage of each as a percentage of the total. Only distinct messages are considered. Note that not all advertisers report payment systems in their messages. If an advertiser listed more than one type of payment system in the message, each type was counted once.

IRC Servers and Channels

IRC server lifespans

The lifespans of all servers observed by Symantec and determined as being active during the reporting period are considered. The lifespan of some of the servers extends beyond the 12-month reporting period and, as such, their lifespans will be longer than 365 days. A server is considered to be active if it has one or more active underground economy channels. The lifespan of each server is calculated by determining the number of days between the first time the server is observed to have an active underground economy channel and the last time the server is observed to have an active underground economy channel.

IRC servers by region

Geographic locations of underground economy servers are constantly changing due to the nature of these servers, which are often hosted as channels on public IRC servers. This metric determines the geographic location of the underground economy servers and their distribution worldwide.

Software Piracy

For the purpose of this report, an instance of a particular file that is available for download refers to a complete file or a complete compilation of files. A user refers to a single IP address from which files are made available for download.

The files discussed are separated into the following categories:

- **Audio recording applications:** Includes music production software, sound editors, software synthesizers and sequencers.
- **Business productivity applications:** Includes word processing and spreadsheets.
- **Console games:** Includes video games for game consoles and handheld gaming devices.
- **Desktop games:** Includes video games for desktop computers.
- **Multimedia productivity applications:** Includes photo editors, 3D animation editors, and HTML editors.
- **Operating systems:** Includes operating systems for all platforms.
- **Utility applications:** Includes CD writing applications, data compression tools, and media players.
- **Other software:** Includes GPS navigators and language trainers.

In determining the potential costs of piracy in each category, where possible the manufacturers' suggested retail price (MSRP) of the software is used to approximate the value of each file. If an MSRP is unavailable, similar software with an available MSRP is used, or else the file is excluded. For example, all desktop games were given an MSRP of $50 and console games ranged from $35 to $60 depending on the console system. The estimated value of each file is then multiplied by total file instances observed and totaled to approximate the value of the category.

Appendix C—Glossary

Attack kits	Attack kits cover a range of tools used to generate income and other goods and services. They range from kits that automatically scan and exploit vulnerabilities to botnets. These tools may be used to provide services such as denial-of-service attacks, spamming and phishing campaigns, and finding exploitable websites and servers.
ATM	An automated teller machine (ATM) is a computerized device that allows customers to complete financial transactions such as deposits and withdrawals without the need for a bank teller.
Autorooters	Automated tools that scan networks for vulnerable computers, which they then attempt to exploit using vulnerabilities in order to compromise as many computers as possible.
Back door	A way to access a computer system that circumvents computer security measures.
Binder	A program that allows multiple executables to be combined into a single executable file.
Blacklisting	Maintaining a list of items such as websites, IRC channels, or email addresses that have historically been determined to be untrustworthy. Access to these items is denied while all others are allowed.
Bot-infected computers or bots	Programs that are covertly installed on a user's machine to allow an unauthorized user to remotely control the targeted system through a communication channel, such as IRC, P2P, or HTTP
Botnet	A large number of compromised computers usually under the control of a botherder (who is someone that controls the bots on the network).
Brute-force attack	An attack where all possible options are systematically tried to reveal a solution. This type of attack is often related to password or encryption key recovery.
C99/R57 shell	Shells that are implemented in the PHP Web-scripting language and which allow access to computers through a Web interface. They may also be injected into a site that is affected by an RFI vulnerability.
Cashiers	People who convert stolen goods, such as bank account credentials, into true currency, either in the form of online currency accounts or through money transfers. In exchange for the service, cashiers will charge a fee, which is usually a percentage of the cash-out amount.
Cash out	A term used on underground economy servers where purchases are converted into true currency. This could be in the form of online currency accounts or through money transfer systems.
Channel juping	A means of blocking the creation of channels by the IRC server administrators.
Channels	Group discussion forums in IRC servers. Each channel is specified by a name and usually a description or main topic of the channel is given.
Check channel	A channel that users can join to check the validity of a credit card number, expiration date, and matching CVV2 numbers. This service is automated by an IRC bot.
Crack	A method for modifying software or files to remove security and protection features.

Credit card dumps	Information contained within the magnetic stripe on a credit card, which is made up of two tracks. Both tracks contain the primary account number and expiration date; the first track will contain the cardholder name and CVV. Each credit card issuer will have their own standards for encoding the information in the tracks.
Cross-site scripting (XSS) vulnerabilities	Vulnerabilities that affect Web applications and allow attackers to inject content such as HTML and script code into a vulnerable Web application, which can facilitate various attacks such as theft of cookie-based website credentials, spoofing of content, and injection of exploit code into a legitimate website.
CVV	A number which is encoded on the magnetic strip of the credit card and is used to authorize point-of-sale or in-person transactions.
CVV2	The three- or four-digit number on the credit card and used, along with the credit card number for not-in-person transactions such as Internet or phone purchases. It is also known as the Card Validation Code 2 (CVC2), Card Identification Digits (CID), or the Card Verification Value (CVV).
Denial-of-Service (DoS) attack	An attack that attempts to keep the user from being able to access a particular computer resource (for example a website or Internet service).
Digital rights management (DRM)	Techniques for controlling the usage of digital media or devices.
Drop	A secure location where goods or cash can be delivered or a bank account through which money can be moved. The drop locations may be an empty apartment or some other scouted location. Criminals often change the billing addresses of credit cards and bank accounts to safe drops that are untraceable. Bank account drops are a convenient way to cash out bank accounts, credit cards, or other online financial accounts. Services for drops can often be accompanied by cashier services.
Exploit	A program or technique that takes advantage of a vulnerability in software and that can be used for breaking security, or otherwise attacking a host over the network.
File transfer protocol (FTP)	A protocol used to transfer files through a network.
Fresh	Describes that the goods are newly acquired, i.e. likely still valid and not canceled.
Full stripe	The information contained within the magnetic stripe on a credit card, which itself is made up of two tracks. While both tracks contain the primary account number and expiration date, only the first track will contain the cardholder name and CVV. Each credit card issuer will have their own standards for encoding the information in the tracks.
Hacker	A computer programmer who attempts to gain unauthorized access computer systems.
Internet relay chat (IRC)	An Internet communications protocol for real-time communications, primarily through group communication forums, commonly referred to as channels.
IRC bots	Scripts that appear to users in the servers as another user. They typically perform administrative functions when the channel administrators are not present or they perform automated functions such as nickname registering or maintaining channel logs.

Joiner	A program that allows multiple executables to be combined into a single executable file.
Local file include (LFI)	Vulnerabilities that are specific to Web applications implemented in the PHP programming language. They allow an attacker to specify an arbitrary include path for files that are external to a vulnerable PHP script. They are local because the attacker can only specify a path to a file that exists on the computer hosting the vulnerable application.
Magnetic stripe skimming devices	Small devices designed to scan and retain data contained in the magnetic stripes on credit and debit cards.
Mailer	An application that is used to send out mass emails (spam) for phishing attempts. Examples of mailers include worms and viruses.
Metadata	Data that provides context for the files. For example, digital music metadata can include the song title, artist name, and genre.
Online authentication services	A multi-level security feature provided by credit card issuers for online purchases. Consumers register their credit card and select a password which is used to complete the online transaction.
Online currency accounts	Online currency accounts exchange true currency, such as U.S. dollars or Euros, into electronic currency that can be based on metals, such as gold or silver, or electronic money. As such, these e-currencies may not be affected by inflation or other fluctuations commonly associated with true currencies.
Online stock accounts	An account held with an online stock brokerage company that facilitates self-directed investors to buy and sell securities such as stocks, bonds, and mutual funds via the Internet.
Packers	A component used to reduce file executable sizes and, in the case of malicious code, can be used as a code obfuscation technique that encodes the executable code in a program file. Executables that are packed must be unpacked before they can be analyzed.
Peer	Any computer that is actively participating in a network.
Peer-to-peer (P2P) network	A network where resources are shared among clients, such as files, without the requirement for a centralized server.
Phishing	An attempt by a third party to solicit confidential information from an individual, group, or organization by mimicking, or spoofing, a specific well-known brand, usually for financial gain.
PHP	A Web-scripting language and interpreter used mainly with Linux.
Personal Identification Number (PIN)	A secret numeric password used to authenticate the user, typically for debit or credit cards.
Proxy	Proxy services provide access to a software agent, often a firewall mechanism, which performs a function or operation on behalf of another application or system while hiding the details involved, allowing attackers to obscure their path and make tracing back to the source difficult or impossible. This can involve sending email from the proxy or connecting to the proxy and then out to an underground IRC server to sell credit cards or other stolen goods.

Remote file include (RFI)	Vulnerabilities that are specific to Web applications implemented in the PHP programming language. They allow an attacker to specify an arbitrary include path for files that are external to a vulnerable PHP script. They are "remote" because the attacker can specify a path that points to a remote computer that is under their control.
Ripper	A vendor on underground economy servers who conducts fraudulent transactions, such as not delivering purchased goods, or who deliberately sells invalid or fake goods.
Scams	An attempt to defraud a person or organization. In the case of phishing scams, the scammer is attempting to acquire sensitive information such as usernames, credit card numbers, or bank account credentials.
Shopadmin	A term used in the underground economy to describe administrative access to online shopping applications. A shopadmin exploit is an exploit that allows for the administrative compromise of such an application.
Simple Mail transfer Protocol (SMTP)	A protocol designed to facilitate the delivery of email messages across the Internet.
Spam	Junk or unsolicited email sent by a third party.
SQL injection	A type of security vulnerability that typically affects Web applications by exploiting improper input validation in database queries. A successful exploit will allow attackers to access, modify, or delete information in the database.
Trojan	Computer code designed to appear as something beneficial, but which in reality delivers malicious code without the user's knowledge.
Underground economy servers	Black market forums used by criminals and criminal organizations to advertise and traffic stolen information, and provide services to facilitate illegal activities.
Unspammed email list	An email address list that has not been previously used for spamming.
Whitelisting	A process where administrators and end users maintain a list of trusted items and access is given to only those trusted items. Examples include websites, IRC channels, and email addresses.
Wire transfer	A method of transferring money from one institution to another, usually through electronic means.
Withdrawal service	Withdrawal services are cash out and drops that are used to withdraw money and items from purchases.
Zero-day exploits	A vulnerability that has been exploited in the wild prior to being publicly known.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

11/08 14525717