Confidence in a connected world.

Symantec Report on the Underground Economy
July 07–June 08
Published November 2008

Executive Summary

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.

Advertisers on underground channels attempt to capture attention for their messages using techniques such as capitalization, multi-colored text, ASCII flares,[2] and repeated sales pitches across multiple lines (similar to blanketing a wall with the same advertising poster). Typical advertisements list the available

---

[1] http://www.symantec.com/norton/cybercrime/definition.jsp
[2] An ASCII flare is a text graphic that only uses the 128 basic ASCII characters.

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

items, prices, and other details such as payment options, contact information, and qualifiers to describe their 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.

Many of the goods and services advertised on underground economy servers form a self-sustaining marketplace. For example, 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, the profits can also help build an underground economy business as profits from one exploit can be reinvested and used to hire developers for other scams, used to purchase new malicious code or new phishing toolkits, and so on.

Figure 1. Underground economy channel screenshot
Source: Symantec Corporation

The data collected for software piracy includes information on game and application software being pirated, the complete instances of each file, and the location of the users posting the files; video and music data were 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 piracy and file sharing on the Internet as a whole.

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.[3] 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 highly organized and cohesive groups. 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.

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.[4]

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 automated teller machine (ATM) 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.

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.

[3] 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
[4] http://www.wired.com/politics/onlinerights/news/2007/01/72581

Governments have become more sophisticated in their awareness of cybercrime, and specific legislation has been developed at various national and international levels to combat online fraud. As with crime anywhere, the online underground economy will continue to be a struggle between 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 United States Secret Service left for subsequent visitors to the ShadowCrew forum after it was shut down in 2004 (figure 2).

Figure 2. Screenshot of United States Secret Service posting on ShadowCrew forum
Source: web.archive.org[5]

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. Of the categories advertised on underground economy servers observed by Symantec, credit card information 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.[6] It was also the most requested category, making up 24 percent of all goods requested.

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[7]
Source: Symantec Corporation

Credit card information may rank high because there are many ways it can be obtained and used for fraud. This includes phishing schemes, monitoring merchant card authorizations, the use of magnetic stripe skimming devices, or breaking into databases and other data breaches that expose sensitive information.[8] Another explanation may simply be that there is a 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.[9] 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.

Credit card information may be in such demand because using 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.

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 because criminals would require a PIN for the card. Also, most ATMs have security cameras, which may deter criminals from using this medium. In addition, withdrawing currency from a bank account has the advantage of a more immediate financial reward than with online purchases, which would need to be sold to realize a purely financial reward.

---

[7] 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.
[8] Magnetic stripe skimming devices are small machines designed to scan and retain data contained in the magnetic stripes on credit and debit cards.
[9] http://www.bis.org/publ/cpss82p2.pdf, Table 7

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. Since many bank accounts can only be cashed out 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 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).

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 is then used in attempted fraudulent acts such as online purchases. One estimate put the cost of phishing attacks at $2.1 billion for United States consumers and businesses in 2007.[10]

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.

Symantec estimates the value of total advertised goods on observed underground economy servers at over $276 million for the reporting period, with credit card information accounting for 59 percent of that total. 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.

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 a median value for credit card fraud and an average bulk purchase size for credit cards, the potential worth of all credit cards advertised during this reporting period would be $5.3 billion.[11] Similarly, for bank account credentials, extrapolating the value using the average advertised balance of nearly $40,000, all bank accounts advertised in underground economy servers during this reporting period would be worth $1.7 billion.[12]

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.[13]

[10] 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
[11] Discussed in "Unique samples of sensitive information" in the main Symantec *Report on the Underground Economy*.
[12] Discussed in "Goods and services advertised by category" in the main Symantec *Report on the Underground Economy*.
[13] http://www.computerweekly.com/Articles/2008/08/07/231773/tjx-indictments-reveal-global-crime-underworld-for-id-theft-and.htm

Value of total advertised goods—top advertisers

While 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, there are some very active participants, groups, and organizations in the underground economy. 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.[14]

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. The value of total advertised goods does not include the usage of items such as credit card purchases or cashing out bank accounts. For this, Symantec calculated the potential worth of the goods by using the median value for credit card fraud as mentioned above.[15] As such, the potential worth of all credit cards from the top 10 most active advertisers during this reporting period would be $16.3 million, while bank accounts advertised would be worth $2 million, for a total of $18.3 million (table 2).[16]

During this reporting period, Symantec observed 69,130 distinct active advertisers on underground economy servers and 44,321,095 total messages posted.[17] The top 10 most active advertisers accounted for 11 percent of the total messages posted. Of the total messages posted, just over one percent were distinct. 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.

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 2. Value of total advertised goods—advertisers[18]
Source: Symantec Corporation

[14] http://yahoo.businessweek.com/magazine/content/05_22/b3935001_mz001.htm
[15] Discussed in "Goods and services advertised by category" in the main Symantec *Report on the Underground Economy*.
[16] This value does not take into account invalid or canceled credit cards.
[17] This does not take into account advertisers that may be using more than one nickname.
[18] The potential worth measures the use of credit card information and bank account credentials.

Malicious tools

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.

Tools 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. A botnet can persistently produce many other goods and services; it can be rented out for specific attacks or on a periodic basis; and it can be upgraded to create new sources of revenue.

Exploits are another effective malicious tool. 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. 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). 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.

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.

Spam and phishing tools and related goods and services marketed on underground economy servers were also 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 often 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 kit 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. Scammers may also acquire domain names by using stolen currency and credit cards to buy from 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.
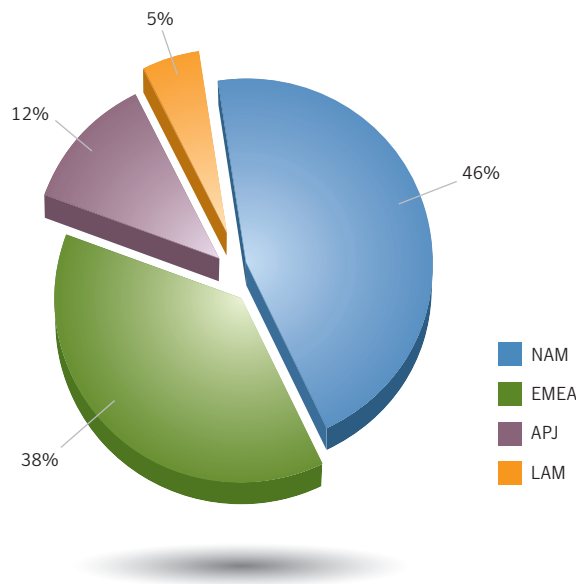
Scam hosters are often implicitly privy to the results of phishing campaigns because they host the data and can monitor phishing activity, and some advertisements stipulate profit-sharing for the scam hoster in any phishing operation. It is likely that other advertisers take advantage of this implicit arrangement. This makes scam hosting a very lucrative activity because the hoster can also resell goods produced from a successful scam.

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, participants on underground economy servers operate from around the world and are not restricted to "normal" business hours. Although users of underground economy servers do most of their business electronically and the geographic location of the server may not be of any consequence to those involved, it may shed light on possible safe havens of underground economy servers.

During this reporting period, North America (NAM) had the largest number of underground economy servers, hosting 46 percent of the total (figure 3); Europe, the Middle East, and Africa (EMEA) 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.[19]

Figure 3. Regional distribution of servers[20]
Source: Symantec Corporation

One possible reason for the lower percentages in LAM and APJ is that users in these regions may not be as familiar with IRC servers and are using other mechanisms for fraud, such as bulletin board systems or other instant messaging clients.[21] 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. Symantec has also observed that users in NAM may be less likely to use or create a Web forum for fraud and opt for IRC servers instead, due to the precedence of legal action.

Another possible reason is that some countries play a more active role in controlling 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 when other communication tools are used. 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, participants in LAM and APJ may prefer to join these well established servers rather than going to the effort of starting and promoting their own.

File instances of pirated software by category

This discussion assesses the total number of file instances observed in the software categories delineated by Symantec.[22] 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 pirated software by a significant margin, accounting for 49 percent of all file instances observed (figure 4). 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.[23] In comparison, retail sales in the United States of software other than games were an estimated $3.3 billion in 2007.[24] Another study worked out the 2007 total to be an average of nine games sold every second of every day.[25]

---

[21] See section 5.1 of http://honeyblog.org/archives/147-Technical-Report-Studying-Malicious-Websites-and-the-Underground-Economy-on-the-Chinese-Web.html
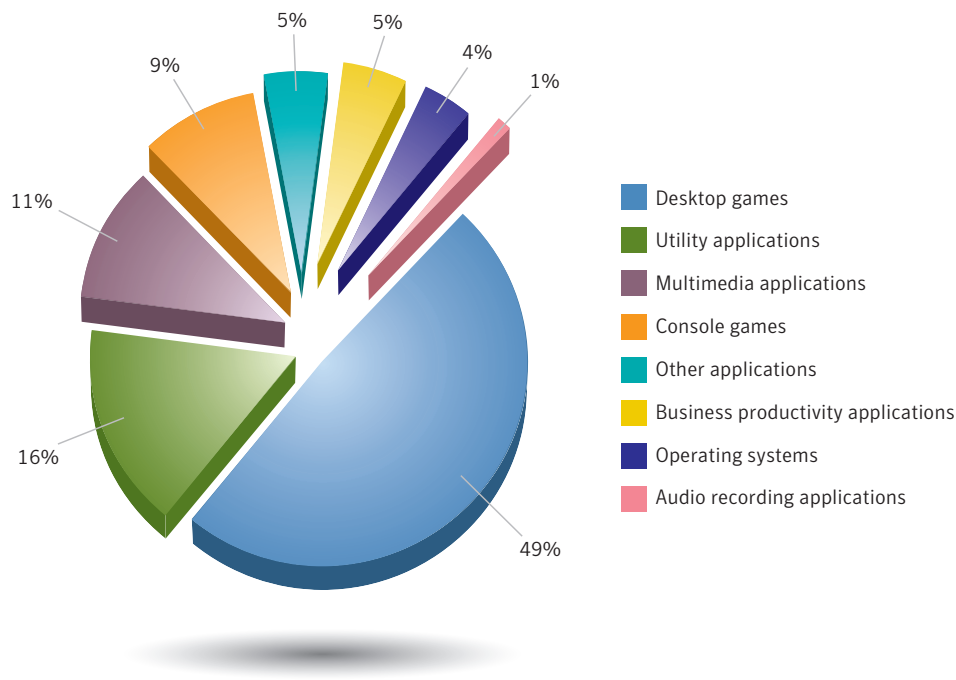[22] Please see Symantec *Report on the Underground Economy*, Appendix B—Methodologies for a full description of the software categories.
[23] http://www.theesa.com/facts/pdfs/ESA_EF_2008.pdf
[24] http://www.eweek.com/c/a/Windows/US-Software-Market-Posts-Best-Performance-in-7-Years/
[25] http://www.theesa.com/newsroom/release_detail.asp?releaseID=8

Figure 4. 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.[26] 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 to download a new file.

The third most pirated software 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 any other category (table 3).[27] 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 for pirated goods.

---

[26] Often defined as anything outside of an operating system or application suite, Symantec defines utility software as applications such as CD-writing applications, data compression tools, media players, etc.
[27] MSRP = Manufacturers' suggested retail price

Considering that nearly 60 percent of the file instances observed were in the two game categories, the majority of 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.[28]

Financial effect of software piracy 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 instances 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 to industries of the piracy could be much greater, even though there may be fewer file instances for such categories.

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 uploads observed by Symantec was $83.4 million (which, it should be noted, is only what 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.[29]

On a category basis, observed file 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 file instances observed by Symantec (table 3). This is far more than all of the other categories combined and is likely due to the high prices of multimedia software.

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 3. Approximate dollar values of software file instances observed
Source: Symantec Corporation

---

[28] http://www.siia.net/press/releases/2-AntiPiracy_YIR_2007.pdf
[29] http://www.itwire.com/content/view/12171/53/

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. This is because the files were valued at an average of $50, far less than either of the top two ranked categories by value.[30] Thus, despite a much larger volume of instances, the cost of desktop game piracy is much less than the estimated $53 million value of multimedia software piracy.

[30] http://www.gamepro.com/article/features/141348/are-60-games-here-to-stay/

Highlights

Goods and services

- During this reporting period, the category of credit card information accounted for 31 percent of all advertisements for sale; it was also the most requested category with 24 percent of the total requested advertisements.

- Bank account credentials were the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 18 percent of all items; prices for bank account credentials ranged from $10 to $1,000, depending on the balance and location of the account.

- Symantec observed 44,752 unique samples of sensitive information publicly posted on underground economy servers, accounting for 10 percent of the total distinct messages.

- Credit card information was the most common unique sample posted on underground economy servers during the reporting period, accounting for 56 percent of the total.

- The potential value of total advertised goods observed by Symantec was over $276 million for the reporting period; this value measured how much advertisers would make if they liquidated their inventory and was determined using the advertised prices of the goods and services.

- The top category for potential value of advertised goods and services was credit card information, which accounted for 59 percent of the total.

- The potential worth of credit card information and bank account credentials on underground economy servers during this reporting period was $7 billion; the worth accounted for use of the goods and was determined using the average values for credit card fraud and bank account balances.

- Online currency accounts were the most popular method of payment during this reporting period, accounting for 63 percent of the total.

Malicious Tools

- The highest priced attack tool, on average, during this reporting period was botnets, which sold for an average of $225.

- Phishing scam hosting services were offered for an average price of $10 with prices ranging from $2 to $80.

- The average price of a keystroke logger advertised on the underground economy was $23.

- 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.

Advertisers

- Symantec observed 69,130 distinct active advertisers and over 44 million total messages posted on underground economy servers during this reporting period.

- The top 10 most active advertisers accounted for 11 percent of the total messages posted; six of the top 10 had credit card information as their top category for sale.

- The most active advertiser posted messages for a wide array of goods and services that covered 15 countries from around the world.

- The potential value of total advertised goods observed for the 10 most active advertisers was over $575,000 for the reporting period.

- The potential worth of credit card information and bank account credentials on underground economy servers for the 10 most active advertisers was $18.3 million.

Servers and channels

- Ninety-eight percent of underground economy servers have lifespans of less than six months.

- 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 smallest underground economy servers had only five channels and 40 users.

- The NAM region had the largest number of underground economy servers, hosting 46 percent of the total, followed by EMEA with 38 percent.

- The United States hosted 41 percent of the total observed underground economy servers worldwide, while Romania had the second highest percentage at 13 percent of the total.

Software Piracy

- Desktop games were the most pirated software, accounting for 49 percent of all file instances observed.

- Individual MSRP prices of software ranged from $20 to $8,000, and the median average cost per file instance for all of the categories was $50.

- The total approximate value of all categorized file instances observed by Symantec was $83.4 million.

- Multimedia software accounted for approximately $53 million of the total; the MSRP shelf values ranged between $40 and $8,000, and an average cost of $1,300—the highest median of all categories.

- The top country by number of file instances was the United States, with 19 percent of the total; the United Kingdom ranked second with seven percent.

- For users by country, the rank and percentages were also the United States first, with 19 percent, and the United Kingdom in second, with seven percent.

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