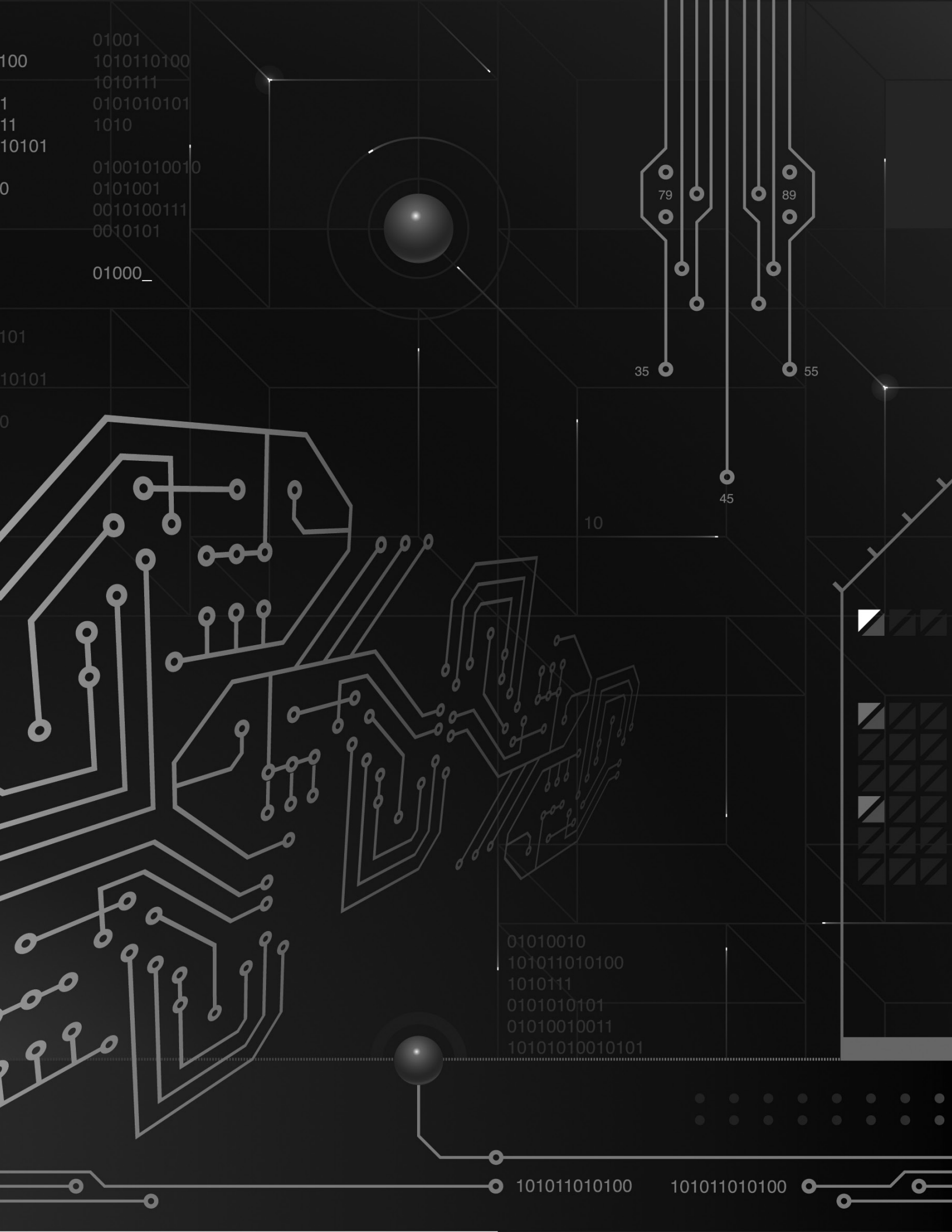
A REPORT BY THE
BUSINESS SOFTWARE ALLIANCE
OCTOBER 2009

BSA®
BUSINESS SOFTWARE ALLIANCE

Software Piracy on the Internet: A Threat To Your Security


01001
100
1010110100
1010111
1
0101010101
11
1010
10101
01001010010
0
0101001
0010100111
0010101
01000_
101
10101
0
79
89
35
55
45
10
01010010
101011010100
1010111
0101010101
01010010011
10101010010101
101011010100
101011010100

Contents

CHARTS AND ILLUSTRATIONS

Foreword

For the second year, the Business Software Alliance (BSA) has produced the Internet Piracy Report, an overview of the scale and serious negative impacts of online software piracy, including a retrospective look at the past year's notable enforcement actions, and a resource for those who wish to avoid the pitfalls of illegal software on the Internet. Overall, this year's report makes it clear that software piracy is as pervasive as the Internet itself, exposing users of illicit goods to a host of risks while at the same time harming the economy. Individuals who, mistakenly or otherwise, turn to auction sites and peer-to-peer networks to acquire or transfer illegal software expose themselves to everything from malware and identity theft to criminal prosecution.

Among the notable cases highlighted in this year's report is that of Tommy Rushing, recently sentenced to three years in federal prison for copyright infringement linked to four for-profit Web sites that offered pirated copies of Adobe and Macromedia software. Likewise, Timothy Dunaway was sentenced to 41 months in prison for selling counterfeit computer software through 40 different Web sites. Outside of the US, a District Court in Taiwan sentenced two individuals to six months' imprisonment for illegal duplication of software, while Hungarian authorities raided the country's largest illegal software distribution company and seized approximately 250 terabytes of illegal content stored on 43 computer servers. The largest case in the world was in China, where the government shut down and convicted the leaders of tomatolei.com, a Web site offering free downloads of massive quantities of illegal software originally published by Adobe, Autodesk, Microsoft, and Symantec.

Alongside enforcement, this year's Internet Piracy Report also highlights how BSA works proactively to educate users about the dangers of online piracy. Pirated products often fail to function properly, or worse still, they are capable of infecting users' PCs with malware that has the potential to cause serious damage. According to some reports, indiscriminate use of peer-to-peer file-sharing networks has led to the disclosure of sensitive government and personal information including FBI surveillance photos and Social Security numbers.

Consumers can often protect themselves just by using common sense and trusting their instincts. Software security updates, trust marks, and a little homework can make a big difference, too. But the best advice is simply to be aware that illegal software is all too common online, and it is best avoided.

Finally, on behalf of millions of people who work in the software industry and related fields worldwide, we at BSA say thank you to those in law enforcement and private industry who are on the front lines in the fight against Internet piracy. Every Internet user in the world ultimately depends on them to help keep the software industry — and society at large — vibrant, innovative and healthy.

ROBERT HOLLEYMAN
President and CEO
Business Software Alliance

Introduction

On any given day, nearly 1.7 billion people around the world use the Internet.[1] Software and computers have become indispensable tools in our businesses, schools, and personal lives.

However, no technology or tool is without risk, and wherever people gather, there are bound to be criminal elements on the fringe of the crowd. The Internet is no different. Almost daily it seems we hear about a new virus spreading through millions of computers; or about companies and government agencies losing sensitive data of employees, customers, and citizens; or in one recent case, about peer-to-peer (P2P) network use exposing confidential witness lists in a high-profile trial of a mafia hit man.

As complex as the technology used to create and develop the Internet is, so too is the network of online criminals and their cyber arsenal of viruses, trojans, and other forms of malware used to dupe unsuspecting consumers and even steal their identities. Internet threats are a clear and present danger to society, as the potential economic rewards for criminals are enormous and the curtain of anonymity behind which they can hide is equally heavy.

Internet threats now go far beyond e-mail spam and swindles of gullible consumers. Today, public and private organizations are dealing with massive onslaughts of malware and inappropriate content. For example, the US Federal Trade Commission (FTC) recently shut down a notorious rogue Internet service provider that was operating under various names and dedicated exclusively to recruiting, knowingly hosting, and participating in the distribution of spam, child pornography, and other harmful electronic content including spyware, viruses, and Trojan horses. According to the FTC, the service provider even established a forum to facilitate communication between criminals.[2] The complexity of such nefarious organizations far transcends the stereotype of a lone individual distributing inappropriate content.

The Internet Theft Resource Center estimates that in 2008, 35 million data records were breached in the United States alone, the majority of which were neither encrypted nor protected by a password.[3] This sad state of affairs shows that security practices and awareness remain low among many Internet users, making it possible for hackers to continue to prey on individuals and organizations. Even as technology providers and users work to close the obvious security holes, the "bad guys" continue to roll out new threats.[4]

What many people may not realize is the connection between Internet security threats and Internet-based software piracy. This is the second edition of a report on this subject first issued by the Business Software Alliance (BSA) in 2008. The report includes descriptions and facts about the various Internet security threats that are related to unlicensed software use; case studies from recent experience; and perhaps most importantly, additional information and steps consumers can take to be an informed and protected Internet user.

On behalf of the leadership of the global software industry, BSA has spent more than 20 years defending the value of intellectual property and pursuing software pirates. Over the past decade, this mission has expanded

to include cracking down on those who offer illegal software via P2P networks, auction sites, and other kinds of Internet-based channels.

Worldwide, roughly 41 percent of all software installed on personal computers is obtained illegally, with foregone revenues to the software industry totaling $53 billion. These are funds that could have been invested in new jobs and next-generation solutions to society's needs. Software piracy affects more than just the software industry since for every $1 of PC software sold, there is another $3 to $4 of revenues lost to local IT support and distribution services.[5]

This report also demonstrates how software piracy — far from being an innocent, victimless crime — exposes users to unacceptable levels of cyber-security risk, including the threat of costly identity theft or allowing one's computer to become a tool in further criminal activity.

The Many Forms of Internet Software Piracy

Before the rise of the Internet, unauthorized copying of software generally required the physical exchange of disks or other hard media through the mail or on the streets. But as technology has advanced and high-speed Internet connections have spread around the world, software piracy has moved from the streets to the Internet.

Generally, Internet software piracy refers to the use of the Internet to:

- Provide access to downloadable copies of pirated software;
- Advertise and market pirated software that is delivered through the mail; or
- Offer and transmit codes or other technologies to circumvent anti-copying security features.

The process can be as evasive as any other illegal activity. Buyers may be directed to one Web site to select and pay for a software program, and then receive instructions to go to another Web site to download the product. This circuitous process makes the pirate less vulnerable to detection.

Internet-based software scams can occur through numerous channels:

AUCTION SITES: Online auction sites are among the most popular destinations on the Web, with millions of people logging on to buy and sell a vast array of products. The most widely recognized auction sites are eBay, UBid, Mercadolibre in Latin America, Taobao and Eachnet in China, and QXL in Europe. Yahoo! operates heavily used sites in Japan, Hong Kong, Singapore, and Taiwan. While many legitimate products are sold on auction sites, the sites are also subject to abuse, especially when it comes to software sales.

PEER-TO-PEER (P2P): Peer-to-peer technology connects individual computer users to each other directly, without a central point of management. To access a P2P network, users download and install a P2P client application. Millions of individuals have P2P programs installed on their computers, enabling them to search for files on each other's computers and download the files they want, including software, music, movies, and television programs. Popular P2P protocols include BitTorrent, eDonkey, Gnutella, and FastTrack. P2P applications include eMule, Kazaa, BearShare, and Limewire. Currently, the most popular protocol worldwide is BitTorrent. BitTorrent indexing and tracker sites facilitate obtaining and sharing illegal copies of software online. In Europe, the Middle East, and Australia, P2P traffic consumes anywhere between 49 percent and 89 percent of all Internet traffic in the day. At night, it can spike up to an astonishing 95 percent.[6]

BUSINESS-TO-BUSINESS (B2B) SITES: Business-to-Business (B2B) Web sites enable bulk or large-scale distribution of products for a low price. Counterfeit software is often sold by distribution sellers on these sites.

SOCIAL NETWORKING SITES: According to Web-security firm Sophos, social networking Web sites such as Facebook, Twitter, and MySpace will soon become "the most insidious places on the Internet, where users are most likely to face cyber attacks and digital annoyances." In a recent report, the firm says security experts are becoming increasingly concerned about malicious attacks originating from social networking sites, as well as the risks of users revealing sensitive personal or corporate data online.[7]

OTHER WEB SITES: Some Internet software scams are conducted via Web sites that offer advertising, such as

According to a report in *The Washington Post*, the indiscriminate use of a P2P networks has led to the disclosure of sensitive government and personal information, including FBI surveillance photos of a suspected mafia hit man, confidential witness lists in the man's trial, Social Security numbers, names of individuals in the witness protection program, and lists of people with HIV. The information is often exposed inadvertently by people who download P2P software to share music or other files, perhaps not realizing that the software also makes the contents of their computers available to others. According to the testimony of one Internet security company executive before the US House of Representatives Oversight and Government Reform Committee, "This is not information you want to have out there."

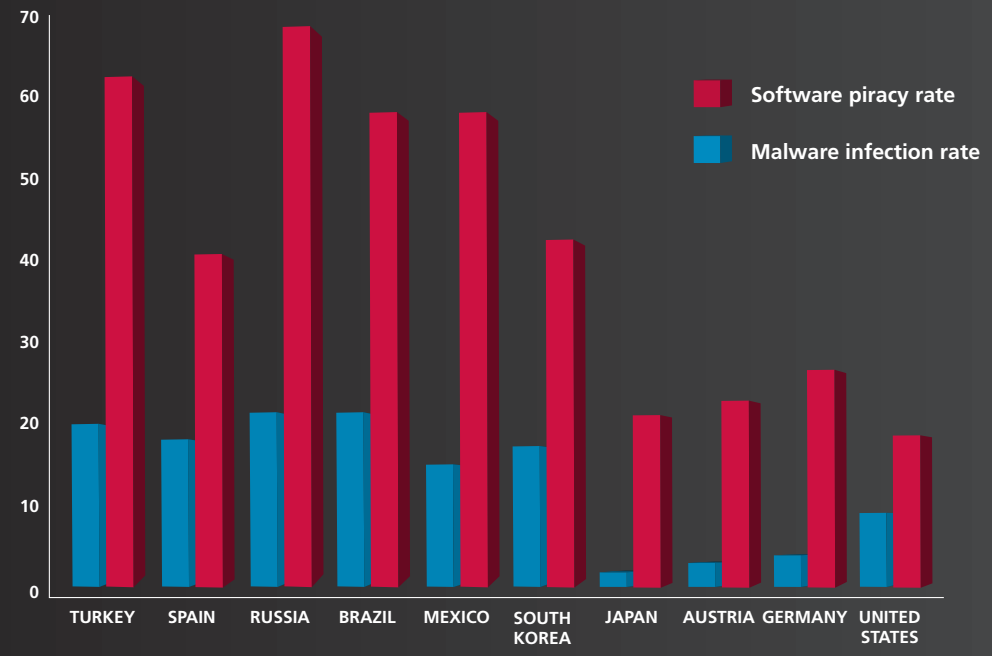
Brian Krebs and Ellen Nakashima, "File Sharing Leaks Sensitive Federal Data, Lawmakers Are Told," *The Washington Post*, July 30, 2009

craigslist, Google, and Yahoo!. iOffer.com describes itself as an online "trading community" without auctions or listing fees. Other scams occur via "cyber lockers" or one-click file-hosting sites such as RapidShare, Megaupload, and Hotfile, where users can upload their content, receive a Web link for it, and then provide that link to others via direct e-mails or ads on other Web sites. Finding and stopping software piracy on such Web sites is becoming more difficult as the number of Internet domain names and overseas-based Web sites proliferates. Some Internet observers have proposed allowing domain name registrars to block information about who controls any given site, which would make it even more difficult to protect consumers from fraud.

BOTNETS: Botnets illustrate how the worlds of software piracy and cyber crime are merging. They are both a contributor to software piracy and one of its most alarming side effects. In simple terms, "bot" is short for robot, a piece of software code programmed to conduct repetitive tasks, while "net" is short for network. In the cyber-crime context, cyber criminals and/or their accomplices ("bot herders") send out "bots" through various techniques, including e-mail spam and malicious code ("malware") added to pirated software. The bots and malware infect ordinary consumers' computers, which then become remotely controlled "zombies." The compromised zombie computers can then be tied together in a botnet and exploited remotely by the cyber criminals to carry out a variety of illegal activities. According to the FBI, more than 1 million computers have become ensnared in botnets.[8] "And the owners often have no idea that it's happening," says Dave Marcus, security research and communications manager with McAfee Avert Labs.[9]

OLDER FORMS OF INTERNET PIRACY: Several older forms of Internet-based piracy are still seen but have been largely supplanted by the more efficient techniques described above. These techniques include Internet Relay Chat (IRC), which are locations on the Internet for real-time, multi-user, interactive conversations; File Transfer Protocol (FTP), a standard computer language that allows disparate computers to exchange and store files quickly and easily; and newsgroups, established Internet discussion groups that operate like a public e-mail inbox.

Rate of Software Piracy vs. Malware Infection

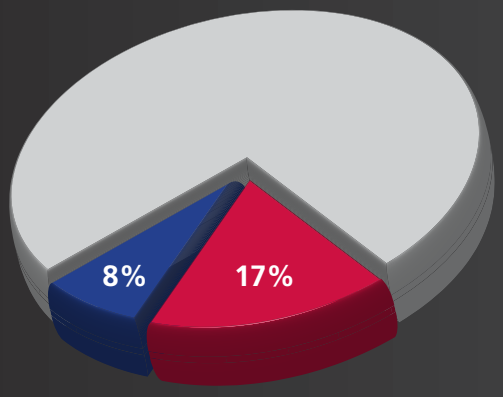


MARKETS WITH HIGH SOFTWARE PIRACY RATES OFTEN HAVE HIGH MALWARE INFECTION RATES[12,13]

SOURCES: SIXTH ANNUAL BSA AND IDC GLOBAL PIRACY STUDY; MICROSOFT SECURITY INTELLIGENCE REPORT VOL. 6

Software Piracy Web Sites* Also Spread Malware

SAMPLE OF 98 UNIQUE WEB SITES



8% OF SITES OFFER MALICIOUS OR POTENTIALLY UNWANTED SOFTWARE

17% OF SITES HAVE MULTIPLE INSTANCES OF MALICIOUS OR POTENTIALLY UNWANTED SOFTWARE

* SITES OFFER ACCESS TO PIRATED SOFTWARE AND PIRACY-RELATED TOOLS.

SOURCE: IDC, RISKS OF OBTAINING AND USING PIRATED SOFTWARE, 2006 SOURCE: IDC STUDY, RISKS OF OBTAINING AND USING PIRATED SOFTWARE, 2006

The Correlation between Malware and Piracy

Globally, there is significant evidence to link software piracy with the frequency of malware attacks. While this correlation has not been measured with precision, the evidence from industry sources suggests that markets with high software piracy rates also have a tendency to experience high rates of malware infection (see diagram on page 10).

Security threats such as viruses, worms, trojans, and spyware are often designed to exploit vulnerabilities in common software products, forcing software developers to constantly develop patches and other fixes to keep emerging malware at bay. Those who use pirated, unlicensed software are typically unable to access or download essential patches and critical updates that ensure their systems remain as secure as possible, and are therefore more susceptible to attack over the long term. Moreover, once infected, consumers are often forced to turn to experts to repair the damage done by the malware, often negating any savings from having acquired and used the products illegally.

One needs only to look at the 2008-2009 spread of the "Downadup" virus, also known as the "Conficker worm." The sleeper virus implanted itself on at least 8 million computers worldwide, and while its exact purpose was unknown, it appeared to give hackers the ability to steal financial and personal information. Security investigators are now describing it as one of the most serious infections they have ever seen. An expert at security firm Symantec showed that the virus spread rapidly in geographic areas with the highest piracy rates, bearing out the correlation between lax handling of software and computers, and security threats that affect millions of people.[14]

Another study from IDC also shows that malware and pirated software frequently co-exist on certain Web sites that offer access to pirated software and piracy-related tools (see diagram on page 10). At least a quarter of such sites were found to be rife with trojans and other security threats that are imbedded into downloaded products or distributed through other means to infect visitors' computers.

The Risks to Consumers

Internet commerce is largely unrestricted, self-regulated, and anonymous. Consumers should proceed with caution when purchasing and using software from unknown vendors online. Using illegal software can put one's personal information, financial security, and even reputation at risk. At the very least, it can lead to software incompatibility and viruses, drive up maintenance costs, and leave users without technical support or security updates. At worst, it can cost ordinary consumers hundreds or thousands of dollars and lost time due to identity theft and the exposure of personal information.

The statistics on risks to consumers are ominous. According to a survey conducted by Forrester Research on behalf of BSA, one in five US consumers who purchased software online in 2006 experienced problems. Of those who had problems:

- 53% received software that wasn't what they ordered;
- 36% reported that the software did not work;
- 14% immediately realized the software was pirated; and
- 12% never received the product.[10]

The risks to consumers also include:

- Not receiving upgrades, technical support, manuals or appropriate documentation;
- Receiving an incomplete, altered, or trial version of the software;
- Allowing criminals access to sensitive personal and financial information; and
- Infecting the consumer's computer with viruses or tools for remote-controlled cyber crime.

A 2006 report by the IDC research firm revealed that 25 percent of Web sites offering access to pirated software and piracy-related tools were distributing malicious code that could undermine IT security and performance. In some cases, the Web sites exploited vulnerabilities in the users' computers to install the unwanted software automatically.[11]

BSA Investigations of Internet Software Piracy

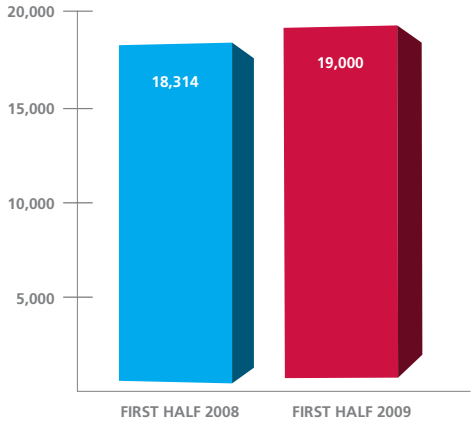
The software industry has worked to combat Internet-based software scams for more than a decade. The centerpiece of BSA's efforts is the Online Auction Tracking System (OATS), a proprietary tool that monitors auction sites and BitTorrent networks (described above) on a continuous basis, while another tool monitors other P2P activity. These systems identify thousands of cases of suspicious activity each day in countries where scanning is permitted by law. BSA then analyzes each case to determine whether it merits further action.

Once BSA has identified offerings of illegal software via various Web sites and P2P networks, it may issue "takedown" notices to the Internet Service Providers (ISPs), asking them to remove the pirated software. In the first half of 2009, BSA stepped up its efforts in this area and issued almost 2.4 million takedown notices related to P2P and BitTorrent file sharing, an increase of more than 200 percent over the same period in 2008.

In 2007, BSA launched an in-house Internet "crawler" to strike further up the BitTorrent supply chain, in addition to the notices sent at the "demand" level where permitted by law. In the first half of 2009, BSA more than doubled its impact with this tool compared to Q1 of 2008, requesting the removal of almost 103,000 torrent files from nine of the largest BitTorrent index sites worldwide. These torrent files were being used by nearly 2.9 million individuals to download software with a retail value of more than $974 million.

When BSA finds suspicious software being offered on auction sites, it issues takedown requests to the auction site providers to remove those listings. During the first half of 2009, BSA has expanded its efforts in this area as well, requesting auction-site providers to shut down more than 19,000 auctions offering about 128,000 products worth a combined $55 million.

Number of Online Software Auctions Removed Due to BSA Requests



BSA CONTINUES TO EXPAND ITS ABILITY TO REQUEST TAKEDOWNS OF SUSPICIOUS ONLINE SOFTWARE AUCTIONS. REMOVALS INCREASED 4% FROM 2008 TO 2009.

SOURCE: BSA DATA

Enforcement Action

When necessary and appropriate, BSA files civil lawsuits to try to stop Internet-based piracy, sometimes referring cases to the US Justice Department (DOJ) for criminal prosecution. Such cases may bring about very serious consequences. Federally prosecuted copyright infringement cases can result in fines of up to $250,000 and, in some cases, jail time.

Over the past decade, BSA, its member companies, and outside partners have provided significant assistance to the Justice Department on hundreds of prosecutions of criminals who were operating for-profit and not-for-profit online software scams. Several of these cases resulted in prison sentences of anywhere between six and nine years, and millions of dollars in restitution.

The following are highlights of several notable Internet piracy cases.

United States

VIRGINIA: In April 2009, Gregory Fair pleaded guilty to one count of criminal copyright infringement and one count of mail fraud before the US District Court for the District of Columbia. From 2001 through 2008, Fair sold a large volume of counterfeit Adobe software on the eBay auction site using multiple user IDs. The combined retail value of this software was at least $1 million. Fair agreed to forfeit the proceeds, including $144,000 in cash, one BMW 525i, one Hummer H2, one Mercedes CL600 and one 1969 Pontiac GTO.

WISCONSIN: In February 2009, Kelly Garcia of Dubuque, Iowa, was sentenced in the Western District of Wisconsin to six months in prison for copyright infringement. In March 2003, Garcia advertised the sale of software products by e-mail offers, including more than 25 products of BSA member companies. After an undercover investigation conducted by BSA, the case was referred to the US DOJ. In November 2003, federal agents searched Garcia's home and discovered she had received approximately $85,000 in proceeds from illegally selling copyright-protected software.

MISSISSIPPI: In May 2008, Mark Anderson was sentenced in the Southern District of Mississippi to 24 months of incarceration plus three years of suspended supervisory release for copyright infringement. While operating the Web site oemcdshop.com, Anderson offered unlicensed copies of more than 31 BSA member-company products. As part of his sentencing, he was ordered to pay restitution in the amount of approximately $46,000.

Asia Pacific

JAPAN: In July 2009, BSA settled a case with an architect who was making illegal copies of Autodesk products and selling the pirated software on Yahoo! Japan's auction site. The seller agreed to pay damages and submit the full list of customers who purchased the software.

TAIWAN: In July 2009, a court in Taiwan sentenced two individuals to six months imprisonment and a criminal fine for illegal duplication of software. The Web site, XYZ Information Workshop, had been operating since 2002, providing unlicensed software products for sale over

the Internet. BSA assisted the government's Intellectual Property Rights Protection Team with the investigation. As part of a 2007 raid, approximately 80,000 copies of CD-Rs were seized in addition to two servers and 19 CD burners. The CD-Rs inspected contained 2,877 copies of BSA members' software, including products by Adobe, Altium, Apple, Autodesk, Bentley, McAfee, Microsoft, PTC, Siemens, Dassault Systemes SolidWorks, Sybase, Symantec, and The Mathworks.

Europe, Middle East and Africa

HUNGARY: In April 2009, the Hungarian National Investigation Authority against Organized Crime raided the country's largest illegal software distribution company, ColdFusion Kft (aka Spamfusion). During the raid, the authorities seized approximately 250 terabytes of illegal content stored on 43 computer servers. Internet traffic in Hungary dropped by 10 percent after the raid, illustrating the far-reaching impact of online software piracy on the Internet. BSA supported the National Investigation Office with the case starting in 2007.

UNITED KINGDOM: In September 2008, Richard Clark of Wolverhampton was stopped from selling counterfeit copies of Adobe, Corel, and Quark software from his Web site, RJ-Software. He agreed to terminate sales of the counterfeit software and pay damages for the distribution of 24 batches of fake software disks. Clark cooperated with the investigation and named a computer maker in Manchester as the source of the illegal goods.

RUSSIA: In April 2008, BSA supported Russian law enforcement with an investigation of a major warez site called ftpwelt.com. For a monthly subscription, users were able to download software programs of BSA members. The two Web site operators were brothers aged 16 and 20. Both were sentenced to prison terms.

Enforcement Case Studies

CASE STUDY: Tommy Rushing

In December 2008, US District Judge Sam Sparks in Austin, Texas, sentenced Thomas "Tommy" Rushing to three years in federal prison, three years of supervised released following jail time, and a $10,000 fine for copyright infringement. Rushing's 2006 Porsche Cayenne Turbo, valued at approximately $40,000, a high-definition television, and computer equipment were also seized as part of the sentencing.

Rushing, of Wichita Falls, Texas, was a college track star at the University of Texas. Beginning in his sophomore year in January 2004, he operated four for-profit Web sites that offered pirated copies of Adobe and Macromedia software. Claiming it was "backup" software, Rushing and his partners offered individuals the opportunity to download the software from his Web site or purchase both the download and CD. Rushing would then burn the software on a CD-R and mail it to unsuspecting customers. Between early 2006 and September 2007, Rushing and his partners sold an estimated retail value of $2.5 million in illegal software.

BSA was responsible for providing the US Department of Justice (DOJ) with evidence that led to Rushing's conviction.

Video excerpts from an interview with Tommy Rushing can be viewed online at **www.bsa.org/faces**.

CASE STUDY: Timothy Dunaway

In early 2009, Timothy Dunaway of Wichita Falls, Texas, was sentenced to 41 months in prison by US District Court Judge Reed O'Conner for selling counterfeit computer software through the Internet. Dunaway was sentenced to two years of supervised release, ordered to pay $810,000 in restitution, and forfeit a Ferrari 348 TB and Rolex watch. From July 2004 through May 2008, Dunaway operated approximately 40 Web sites that sold a large volume of downloadable counterfeit software. He operated computer servers in Austria and Malaysia; US and foreign law enforcement agents cooperated in the investigation. Dunaway purchased advertising for his Web site on major Internet search engines and processed more than $800,000 through credit-card merchant accounts under his control. The software sold by Dunaway had a combined retail value of more than $1 million.

CASE STUDY: Matthew Miller

In August 2009, BSA announced that its members won a $210,563 judgment in the US District Court for the Northern District of California against Matthew Miller of Newark, Del., who sold illegal copies of software through an Internet auction site. Software programs published by Adobe, Autodesk, and Microsoft were at the center of the case, which stemmed from a 2008 investigation by BSA. US District Judge Susan Illston awarded the plaintiffs $195,000 in statutory damages and an additional $15,563 for filing costs and attorneys' fees. Miller was barred from committing future acts of copyright infringement involving Adobe, Autodesk, and Microsoft software products, and was ordered to immediately destroy any and all infringing copies of such software in his possession or control. According to legal documents filed on behalf of BSA member companies, the defendant "admitted he had 'downloaded software, burned and copied CDs, and sold about 200 to outsiders for $8.00 to $12.00.'" Records in the case also describe how Miller used the popular iOffer Web site to sell unlicensed copies of BSA member software. In one particular instance, Miller was accused of offering approximately $12,000 worth of software to an undercover investigator for just $52, with an agreed price of $45 after some haggling.

CASE STUDY: Tomatolei

Established in early 2004, tomatolei.com is a China-based Web site offering free downloads of illegal software originally published by Adobe, Autodesk, Microsoft, and Symantec. BSA supported Chinese law enforcement with this case, filing a complaint in June 2008 against tomatolei.com to the National Copyright Administration (NCA) and the Ministry of Public Security (MPS) on behalf of its member companies. In August of that same year, Suzhou Public Security Bureau arrested the Webmaster of tomatolei.com, impounded approximately $266,000 belonging to the suspect, and found evidence linking him to large-scale reproduction of counterfeit CDs. Chengdu Gongruan Network Technology Co., Ltd., which runs the tomatolei.com Web site, together with the four defendants, were convicted in August 2009 of criminal liability for copyright infringement associated with unauthorized reproduction and distribution of PC software.

The verdicts marked the end of China's largest online software piracy syndicate and a milestone in the nation's efforts to crack down on Internet piracy. It also demonstrates the joint efforts and achievements of the Chinese government, its enforcement agencies, and the international software industry in fighting large-scale Internet piracy.

Government Policy

As described throughout this report, online software piracy presents serious and immediate threats to software users, software developers and service providers, and society at large. Online piracy also has serious negative effects on other copyright-based industries such as music and motion pictures. While the vast majority of individuals and businesses use software, computers, and the Internet legally, too many people treat the illicit acquisition of copyrighted works online as a minor offense — or even as their right. The truth is, those people are breaking well-established laws, causing severe and widespread damage.

In recent years, governments in many countries have witnessed lively debates over the appropriate policy responses to counter online piracy. BSA members approach the debate with two objectives in mind:

- To effectively deter illicit downloading, uploading, providing, and using of licensed content; and
- To ensure that existing technologies function as designed; that innovation and the development of new technologies is not obstructed; and that users' enjoyment of software, computers, and the Internet is not diminished.

BSA members believe the following principles can help governments strike the right balance between these two objectives:

- Some anti-piracy content identification and filtering technologies may play a useful role in deterring piracy in some limited cases, but they are not a silver-bullet solution to piracy. The current voluntary, industry-led approach to developing anti-piracy technologies continues to be effective, and mandated use of any such technologies is not justified.
- In appropriate circumstances, BSA supports:
  - Automated educational notification mechanisms for alleged online infringers and a requirement for ISPs to preserve evidence of repeated infringements, such as a user's IP address to enable appropriate enforcement actions — subject to appropriate safeguards — including those governing privacy.
  - The imposition of appropriate sanctions, including blocking a user, blocking a site, and the suspension or termination of Internet service for individual repeat offenders, provided that such sanctions shall be based on either breach of contract (i.e., the terms of the subscriber's contract with the service provider), or a decision by an administrative or judicial entity, provided such entity gives all parties an opportunity to be heard and to present evidence, and that the decision can be appealed before an impartial court. Before an order becomes final, parties should have the opportunity to have the order stayed pending an appeal.
  - Contractual mechanisms are a helpful and efficient way of dealing with online piracy and should be encouraged and widely implemented.

- When developing steps to address online content piracy, the following should also be given due consideration:
  - The voluntary development and use of anti-piracy content identification and filtering technologies should continue unimpeded; this self-regulatory approach is an effective way to address piracy. The specific technologies themselves should be developed through voluntary processes open to all affected stakeholders, and the results should be based on consensus of the participants.
  - In specific cases where anti-piracy content identification and filtering technology is used, it should be demonstrated to be robust, renewable, interoperable, free of unintended consequences for existing systems, and meet any other relevant criteria necessary to ensure that users' experience will not be degraded, and the development and deployment of new technologies will not be impeded.
  - Where it is determined that it is necessary to empower national judicial or administrative entities to require the use of anti-piracy content identification and filtering technologies, such entities shall impose the requirement as a remedy on a case-by-case basis, in view of the specific facts presented, and after all affected stakeholders have had an opportunity to assess the impacts of such technologies, and after identified issues have been comprehensively addressed.
- BSA opposes:
  - The termination of ISP services or any other sanctions or penalties imposed on alleged infringers without due process and, at a minimum, a right of appeal to a judicial authority, except when such penalties are imposed as a result of a breach of contract with the service provider.
  - Imposition of broad anti-piracy content identification and filtering technological requirements applicable to all Internet users, or all computers and software used to access the Internet, by legislation, administrative fiat, or adjudication.

BSA Partnerships and Educational Outreach

Beyond enforcement actions, BSA also works with various organizations to gain an even deeper understanding of Internet piracy and to educate the public about the risks of purchasing software from questionable Internet sources.

NATIONAL COMPUTER FORENSICS TRAINING ALLIANCE (NCFTA): In February 2005, BSA began a sponsorship of a dedicated cyber forensics analyst at the National Computer Forensics Training Alliance (NCFTA). The NCFTA provides a neutral collaborative venue where critical, confidential information about cyber crime — including software piracy — can be shared discreetly. It is also an environment where resources can be shared among industry, academia, and law enforcement. The partnership has provided BSA with valuable data on cyber security and software piracy.

US IPR TRAINING COORDINATION GROUP (IPR TCG): BSA works closely with the US State Department's Bureau of International Narcotics and Law Enforcement Affairs (INL) and Bureau of Economic, Energy and Business Affairs (EEB), which co-chair the Intellectual Property Rights Training Coordination Group (IPR TCG). Founded in 1998, the IPR TCG is comprised of US government agencies and industry associations that provide education, training, and technical assistance to foreign officials and policymakers. The departments of Justice and Commerce, US Trade Representative (USTR), FBI, US Customs and Border Protection, US Patent and Trademark Office, US Agency for International Development, and Copyright Office all participate in the IPR TCG. Private sector partners include the International Intellectual Property Alliance (IIPA), US Chamber of Commerce, International Anti-Counterfeiting Coalition, and other industry organizations.

SMALL BUSINESS ADMINISTRATION (SBA): In 2007, in an attempt to help American small businesses avoid the risks of software piracy, the US Small Business Administration (SBA) and BSA partnered for a multi-year education program called "Smart About Software: Software Strategies for Small Businesses." By using the tools and tips for responsible management available at www.smartaboutsoftware.org, small businesses can learn to protect themselves from the legal and financial consequences of using unlicensed software. In March 2008, the SBA and BSA hosted a free Webinar for small businesses to discuss software license management and how it fits into a comprehensive business plan. It is estimated that the partnership will educate as many as 100,000 small businesses through the national SBA network.

BETTER BUSINESS BUREAU: In 2003, BSA joined forces with the Council of Better Business Bureaus (CBBB) to educate consumers about the risks of purchasing software on auction sites. Together, the two organizations have reached an estimated 6 million consumers through outreach efforts including media tours, direct mail, television and radio advertising, and online initiatives.

LOOKSTOOGOODTOBETRUE.COM: This Web site was developed and is maintained by a joint federal law enforcement and industry task force, including the US Postal Inspection Service and the FBI. The Web site was built with the goal of educating consumers and preventing them from being affected by Internet fraud. BSA was recently accepted as a new member of the task force and will lend its expertise and resources to the group's efforts.

"DON'T GET DUPED": All computer users should have a basic understanding of how to protect themselves from Internet dangers. The "Don't Get Duped" Web site found at www.bsacybersafety.com was created to help educate consumers on these dangers and offer them a forum through which to tell their stories about how they were duped into purchasing illegal software online. Over

the past several years, nearly 400 consumers have written to BSA to share their experience. More than 30 percent of complaints involved eBay.

For example, many consumers have complained about receiving software that was obviously pirated, oftentimes on store-bought CD-Rs with handwritten titles, no registration keys, and no manuals. In one such case, a Texas consumer who paid $155 on eBay for Adobe Photoshop CS — software that normally retails for about $650 — learned that the seller's account was cancelled a few days later. After numerous e-mail complaints to the seller, which were not answered, he was instructed by eBay to wait 10 days from the auction close and then file a complaint with PayPal. PayPal was able to contact the seller, and the man eventually received the software in the mail. But that was not the end of the story. "It was easy to tell it was pirated," he said. "It was in a thin case with just a CD-R and only a handwritten note on the disc itself about what it was. When I opened the package and saw that it was pirated, I immediately e-mailed him requesting my money back." The consumer never got his money back.

More stories about consumers who were duped are posted on **www.bsacybersafety.com**.

B4USURF: In Asia, BSA manages a cyber safety and ethics campaign (www.b4usurf.org) aimed at influencing youths ages 10–18. The centerpiece of the initiative is a Web site with resources for educators, youths, and parents. For example, the site includes lesson plans and tips for teachers based on input from teachers in Singapore. Over time, BSA hopes to encourage education officials to incorporate Internet-focused ethics, security, and safety units in the curriculum of many nations. To date, the campaign has focused on Singapore, Malaysia, China, Taiwan, the Philippines, Hong Kong and India.

B4UCOPY: In a continuation of the BSA's efforts to educate youth and higher-education students about the potential risks they face online and the importance of respecting intellectual property, BSA introduced B4UCopy, a program designed to raise overall student awareness of copyright issues and to encourage responsible behavior online. BSA selected Young Minds Inspired (YMI), an in-school curriculum-based program creator, to assist in the design of the comprehensive program and curricula which includes lesson plans and teacher guides for grades 3 through 12. The curricula are available on two BSA Web sites created for parents/guardians and educators at www.b4ucopy.com/kids (grades 3-8) and www.b4ucopy.com/teens (grades 9-12). In conjunction with the curricula, the main Web site (www.b4ucopy.com) includes materials to educate college students about cyber safety and cyber ethics. BSA also introduced a B4UCopy video specifically targeting college students. This video includes interviews with college students and offers tips to help students be smart about piracy and using digital media. Due to the success of the North America effort, the Web site has been translated into both Spanish (www.pienseantesdecopiar.com) and Portuguese (www.penseantesdecopiar.com) for use in Latin America.

EDUCATIONAL RESOURCES: In April 2008, BSA unveiled "Faces of Internet Piracy," a revealing look at the true stories of people affected by online piracy. BSA toured the country interviewing software pirates from all walks of life, including an Austin, Texas, college track star (See "Case Study: Tommy Rushing," above); a Richmond Hills, Ga., grandmother; a Lakeland, Fla., entrepreneur; a Wichita Falls, Texas, software programmer; and a New Milford, Conn., college student. The BSA Web page (www.bsa.org/faces) features videos of the pirates telling their personal stories, along with tips for consumers on how to avoid online piracy.

The Larger Internet Crime Puzzle

Online software scams are one piece of the larger Internet crime puzzle. The Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center (NW3C), receives Internet-related criminal complaints on an ongoing basis and refers cases to the appropriate local, state, federal, or international agency for possible investigation and prosecution.

In 2008, IC3 processed 275,284 complaints spanning the spectrum of Internet crime from auction fraud, non-delivery, and credit/debit card fraud, computer intrusions, spam/unsolicited e-mail, and child pornography. From the submissions, IC3 referred 72,940 complaints to the appropriate law enforcement agencies. The total dollar loss from all referred cases of fraud was $264.6 million, with a median dollar loss of $931 per complaint.

For more information, visit **www.ic3.gov**.

What Consumers Can Do to Protect Themselves

As described throughout this report, consumers who buy software from questionable sources online or engage with Web sites of dubious credibility face serious risk of identity theft or having their computers involved in cyber crime, among many other hassles. Armed with the right information, however, consumers can avoid online software piracy scams and protect their personal well-being and privacy. The following is a list of key tips for consumers:

TRUST YOUR INSTINCTS. When you buy software from the original publishers, brand-name sources, or other online sources that offer security features, you are much more likely to get a safe, legitimate product than when you buy from anonymous, unprofessional sources. Check the online seller's price against the estimated retail value of the software. Be wary of compilations of software titles from different publishers on a single disk or CD. This is a sure sign that the software has been pirated and possibly altered. Remember, whether the product is being sold as new or used, if a price for software seems "too good to be true," it probably is.

USE SOFTWARE SECURITY UPDATES. Take advantage of free software updates from the original publishers, which often contain "patches" to fix security flaws that have been discovered by the publishers themselves. Also, install antivirus software and make sure it is activated.

LOOK FOR A "TRUST MARK." Look for a "trust mark" from a reputable organization to make sure the online retailer is reliable and has a proven track record of satisfying customers. If in doubt, conduct Web searches about the Web site in order to determine its legitimacy. You may also check for a Better Business Bureau report at **www.bbb.org**.

DO YOUR HOMEWORK. Most legitimate retail sites will have sections for feedback comments by other users, so check the seller's rating and see what comments others have posted. Most legitimate sellers will have responses from other users, and if they are reputable and reliable, nearly all should be positive.

MAKE SURE IT'S AUTHENTIC. Be suspicious of software products that do not include proof of authenticity such as original disks, manuals, licensing, service policies, and warranties. Beware of products that do not look genuine, such as those with handwritten labels.

BEWARE OF BACK-UPS. Take care to avoid sellers offering to make "back-up" copies. This is a clear indication that the software is illegal. Also be sure to check the software version. Many people receive educational or promotional versions of software when they have been told they were purchasing a full or standard version.

GET THE SELLER'S ADDRESS, IF POSSIBLE. Remember that if you cannot contact the seller after making a purchase, you may have no recourse if the product turns out to be pirated. BSA receives numerous reports about sellers who became impossible to reach as soon as the payment was finalized. If the vendor is unfamiliar to you, look for an online and offline customer support contact. A legitimate transaction should involve ongoing transparency and communication between buyer and seller

UNDERSTAND THE TRANSACTION TERMS. Make sure you get a clear explanation of the merchant's policies concerning returns and refunds, shipping costs, and security and privacy protection before you complete the transaction. Check the Web site's privacy policies to understand what personal information is being requested, as well as how your information will be used and protected.

ENSURE SECURE PAYMENT. Before you give your payment information, check that the Internet connections you are using are secure. Most Internet browsers will display a padlock icon when you are using a secure site, you can check the Web site address in the address bar. If the connection is secure, the site address will be preceded by https:// instead of http://. Heed any pop-up boxes that warn you about an invalid "security certificate."

HOW TO REPORT SUSPECTED SOFTWARE PIRACY

Consumers have a key role to play as sentinels of possible Internet fraud. Individuals who believe they may have information about software piracy — or who have become victims of such fraud — are encouraged to file a confidential report at **www.nopiracy.com** or call 1-888-NO-PIRACY. Consumers are also able to file a confidential report at **www.bsacybersafety.com**.

Through BSA's "Know it, Report it, Reward it" program, individuals who provide qualified reports of software piracy are eligible to receive up to $1 million in cash rewards.

Know it. Report it. Reward it.

Conclusion

Software piracy may be tempting to those who are not familiar with the risks. But far from being an innocent, victimless crime, software piracy exposes users to unacceptable levels of cyber-security risk, including the threat of costly identity theft. It also undermines the value of intellectual property, which is one of the key drivers of innovation and the way millions of people earn a living.

In today's increasingly interconnected global economy, the Internet has opened incredible new frontiers for communicating, shopping, learning, and simply having fun. At the same time, the Internet's global reach, anonymity, and speed can be used for harmful purposes as well as benign ones. As long as the Internet remains a central front in the war on software piracy and related crimes, BSA will continue to raise awareness of the problem and focus its resources on pushing back the enemy.

For more information from BSA on online software piracy or other important IT topics, visit **www.bsa.org**.

Endnotes

1 Miniwatts Marketing Group, Internet World Stats (Web site); 30 June 2009; http://www.internetworldstats.com/stats.htm

2 FTC Press Release; FTC Shuts Down Notorious Rogue Internet Service Provider, 3FN Service Specializes in Hosting Spam-Spewing Botnets, Phishing Web sites, Child Pornography, and Other Illegal, Malicious Web Content; FTC Press Release; 4 June 2009; http://www.ftc.gov/opa/2009/06/3fn.shtm

3 ITRC ; ITRC 2009 Consumer Awareness Survey: The Need for "Secure Payment Agent" (SPA); 23 September 2009; http://www.idtheftcenter.org/artman2/publish/lib_survey/SPA_White_Paper_printer.shtml

4 IT-Director.com; Ignorance is not Bliss; 19 January 2009; http://www.it-director.com/business/security/content.php?cid=11015

5 IDC; Sixth Annual BSA and IDC Global Software Piracy Study; May 2009

6 Paul Mah, IT News Digest on Tech Republic.com; Majority of Internet bandwidth consumed by P2P services; 28 November 2007; http://blogs.techrepublic.com.com/tech-news/?p=1651

7 Euractive.com Report; Facebook: A new battleground for cyber-crime; 27 July 2009; http://www.euractiv.com/en/infosociety/facebook-new-battleground-cyber-crime/article-184380

8 FBI Press Release; Over 1 Million Potential Victims of Botnet Cyber Crime; 13 June 2007

9 BSA; Online Software Scams: A Threat to your Security; October 2008; http://www.bsa.org/files/Internet_Piracy_Report.pdf

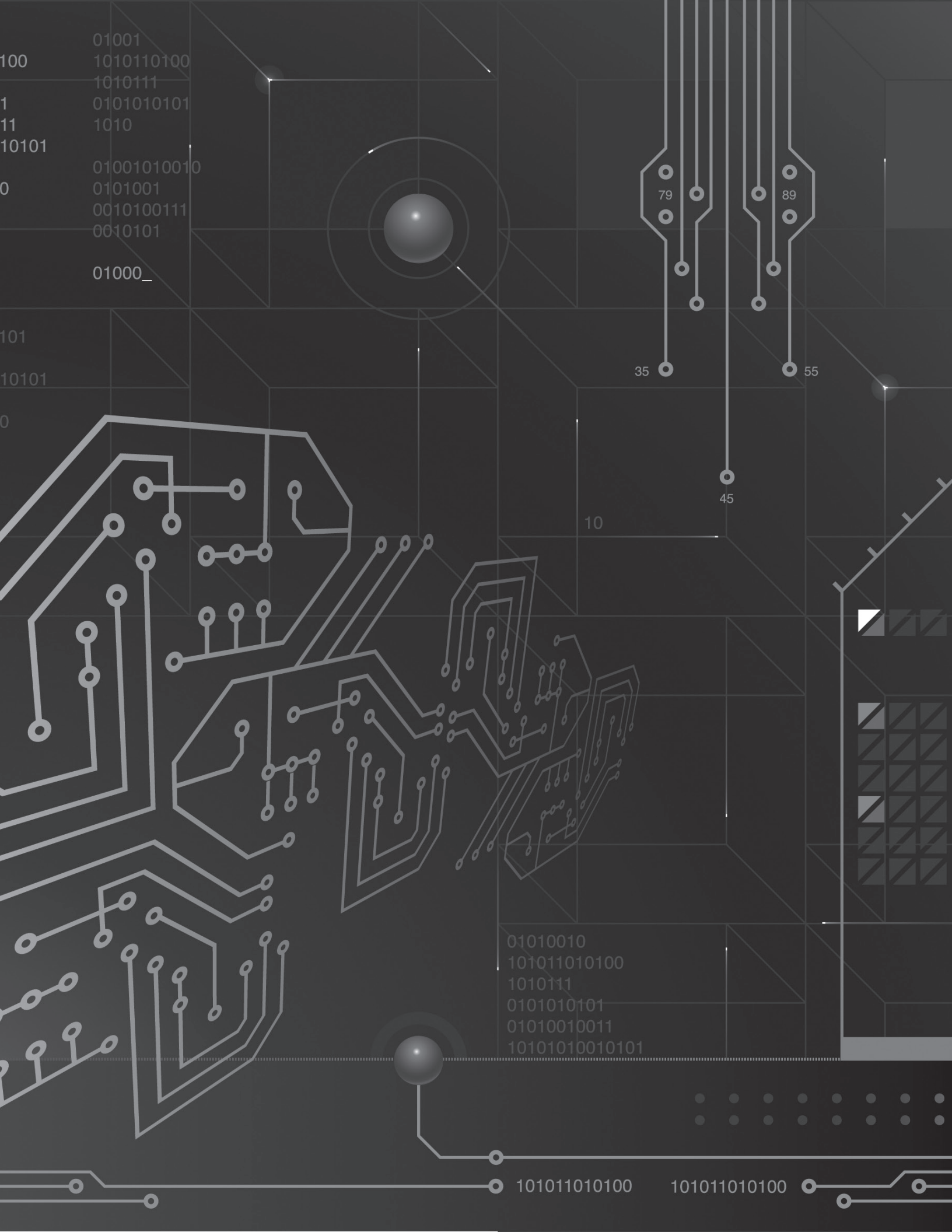
10 BSA Press Release; National Survey Reveals Consumers Concerned About Safety and Security of Online Shopping; 15 November 2006; http://www.bsacybersafety.com/news/2006-concerned-online-shopping.cfm

11 IDC; The Risks of Obtaining and Using Pirated Software; October 2006

12 Microsoft Security Intelligence Report Volume 6; April 2009; http://www.microsoft.com/security/portal/Threat/SIR.aspx

13 BSA; Sixth Annual BSA and IDC Global Piracy Study; May 2009; http://global.bsa.org/globalpiracy2008/images/GlobalStudy2008_CoverDL.jpg

14 Symantec Security Blog; January 2009; http://www.symantec.com/connect/blogs/downadup-geo-location-fingerprinting-and-piracy


01001
100
1010110100
1010111
1
0101010101
11
1010
10101
01001010010
0
0101001
0010100111
0010101
01000_
101
10101
0
79
89
35
55
45
10
01010010
101011010100
1010111
0101010101
01010010011
10101010010101
101011010100
101011010100

BUSINESS SOFTWARE ALLIANCE
1150 18th Street, NW
Suite 700
Washington, DC 20036
T. +1 202 872 5500
F. +1 202 872 5501
www.bsa.org

BSA ASIA-PACIFIC
300 Beach Road
#25-08 The Concourse
Singapore 199555
T +65 6292 2072
F +65 6292 6369

BSA EUROPE-MIDDLE EAST-AFRICA
2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom
T +44 [0] 20 7340 6080