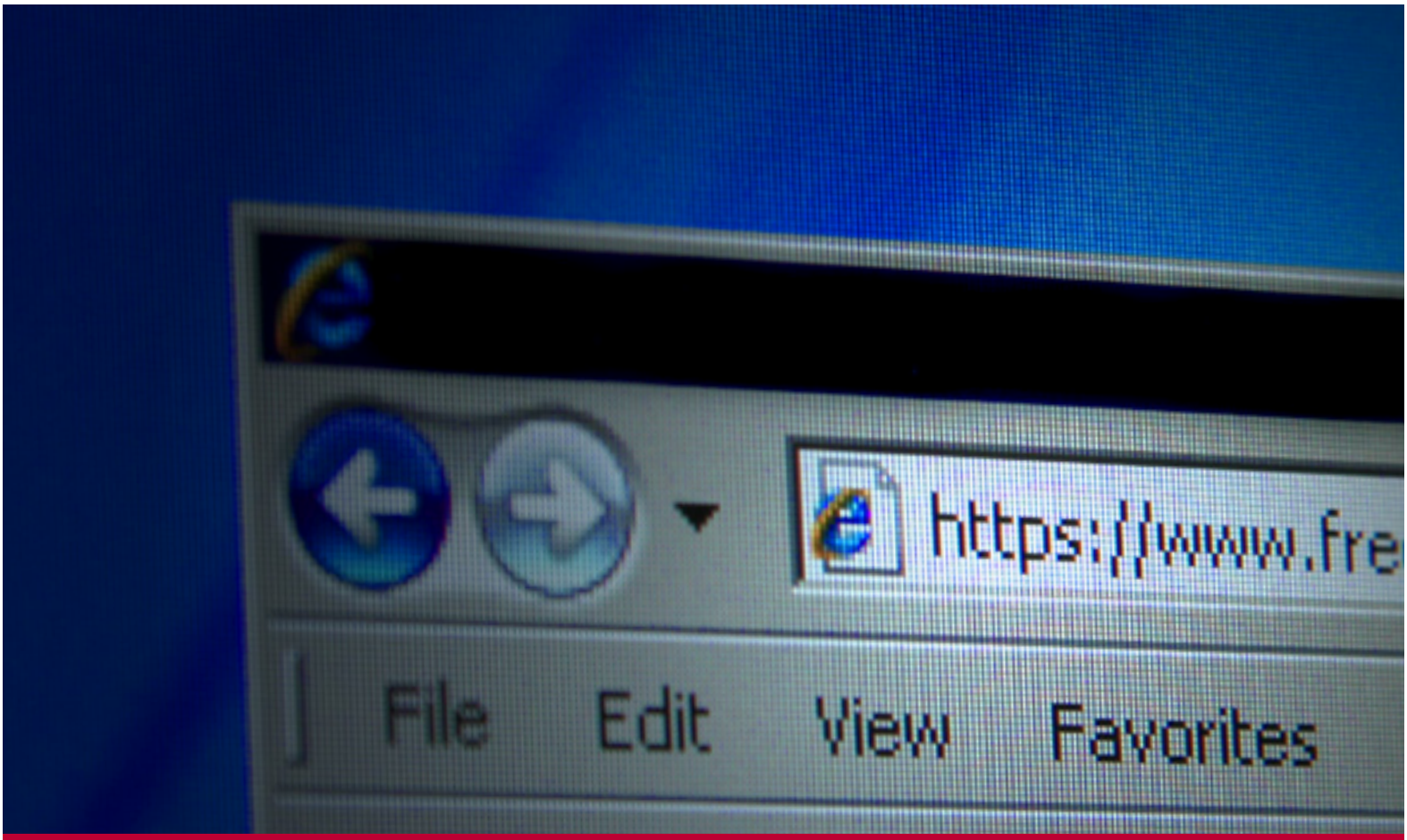


A REPORT BY THE
BUSINESS SOFTWARE ALLIANCE
OCTOBER 2008

BSA®
BUSINESS SOFTWARE ALLIANCE

Online Software Scams: A Threat To Your Security

Contents

Charts and Illustrations

Introduction

An employee of Wagner Resource Group of McLean, Virginia, decided to use his office computer to download music and video files from the Internet using the popular LimeWire peer-to-peer program. Unfortunately, LimeWire is one of many such programs used to exchange pirated copies of music, video, and software, and those often-tainted files can then help cyber criminals accomplish even further misdeeds. In this case, the Wagner employee's action set off a terrible chain reaction, opening up the firm's computers to outsiders and exposing the names, dates of birth, and Social Security numbers of about 2,000 of the firm's clients, including US Supreme Court Justice Stephen Breyer. The company hired by Wagner to help contain the data breach said it found more than a dozen LimeWire users in places as far away as Sri Lanka and Colombia had downloaded the list of personal data from the Wagner network. "This may explain why two weeks ago I got a $9,000 cell phone bill from AT&T," said one of the firm's clients.[1]

A consumer in Texas bought a software product online for a deeply discounted price. But when he received the CD in the mail, he immediately realized there was a problem. "To get the serial number to activate the product, I had to use the keygen.exe software included on the disk," he said. The consumer did some research online and discovered that the keygen.exe application is used to generate CD keys or serial numbers required for software installation or activation. Keygens are available on the Internet and are often packaged with software for distribution by piracy groups. The use of keygens to activate software without purchasing a genuine code is illegal.[2]

On any given day, nearly 1.5 billion people around the world—one in four human beings—may go online to communicate with friends, family, and business associates; shop for a great deal; do research for school; or seek out entertainment. The global number of Internet users grew by more than 300% from 2000 to 2008.[3]

However, there is a darker side to the Internet when it comes to online scams that snare consumers

ALTHOUGH CONSUMERS MAY THINK THEY ARE GETTING A GREAT DEAL WHEN THEY BUY SOFTWARE FROM UNFAMILIAR SOURCES ONLINE, IT IS MORE LIKELY THEY WILL RECEIVE A SUBSTANDARD PRODUCT WITH HIDDEN CYBER SECURITY THREATS THAT MAY EXPOSE THEM TO IDENTITY THEFT AND THE LOSS OF THOUSANDS OF DOLLARS.

attracted by low-priced deals. One of the most widespread online scams involves stolen or unlicensed software programs, i.e., pirated software, offered at discounted prices. Although consumers may think they are getting a great deal, it is more likely they will receive a substandard product with hidden cyber security threats that may expose them to identity theft and the loss of thousands of dollars. As described below, software piracy is conducted via numerous channels in the online world; however, piracy on online auction sites such as eBay is challenging.

Pirated software can also enmesh the unwitting consumer in further criminal activity, as the consumers' computer is effectively converted into a "robot" and exploited remotely by the cyber criminal. Cyber crime is increasingly perpetrated by organized crime syndicates located around the world. "Cyber crime today isn't about computer geeks just having fun at other people's expense," says Rob Clyde, vice president for technology at Symantec. "It's real criminals making real money off of real victims. And it gets more serious by the day."[4]

The widespread theft and distribution of bogus software is also evidence that the value of intellectual property (IP) is under attack around the world. Far too many people are careless in how they handle software and computers, instead of respecting the value and effort that went into them or the dangers of abusing them. Some people behave as though the copying and theft of IP is a victimless crime or that the creators of works such as software, music, films, and books can be stolen from without consequences. People who would not dream of shoplifting a music CD or a package of software from a store will go online to seek out copies of plainly illegal software.

Worldwide, more than one-third of all software installed on personal computers is obtained illegally, with foregone revenues to the software industry totaling nearly $48 billion, monies that could have been invested in new jobs and next-generation solutions to society's needs. The ripple effects also include tax revenues not paid to support community services such as police protection and new schools. A 2008 study found that reducing software piracy in the United States alone by just 10 percentage points over the next four years could generate more than 32,000 new jobs, $41 billion in economic growth, and $7 billion in tax revenues above current projections.[5]

The Business Software Alliance (BSA) has spent more than twenty 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 peer-to-peer (P2P) networks, auction sites, and other kinds of Internet-based channels. The following report describes the scope and nature of the Internet piracy problem, as well as steps that are needed to reduce it, with a special emphasis on auction site scams.

The Many Forms of Software Internet 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 high-speed Internet connections have spread around the world, software piracy has moved from the streets to the Internet.

Generally, Internet 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 roundabout as any other illegal activity. Buyers may be directed to one website to select and pay for a software program, and then receive instructions to go to another website 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 best known auction sites are eBay, UBid, Mercadolibre in Latin America, Taobao in China, and QXL in Europe. Yahoo! operates heavily used sites in Hong Kong and Taiwan. While many legitimate products are sold on auction sites they are also subject to abuse, especially when it comes to software sales (see more details below).

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 networks include BitTorrent, eDonkey, Gnutella, and FastTrack. P2P applications include BitTorrent, eMule, Kazaa, BearShare, and Limewire. In Europe, the Middle East, and Australia, P2P traffic consumes anywhere between 49% and 89% of all Internet traffic in the day. At night, it can spike up to an astonishing 95%.[6]

OTHER WEBSITES: Some Internet software scams are conducted via websites that offer advertising, such as craigslist, Google, and Yahoo!. iOffer.com describes itself as an online "trading community" without auctions or listing fees. Other scams occur via file-hosting sites such as RapidShare, 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 websites. Finding and stopping software piracy on such websites is becoming more difficult as the number of Internet domain names and websites

PEER-TO-PEER (P2P) TECHNOLOGY IS WIDELY USED FOR PIRACY OF INTELLECTUAL PROPERTY. IN SOME PARTS OF THE WORLD, P2P TRAFFIC CONSUMES BETWEEN 49% AND 89% OF ALL INTERNET TRAFFIC DURING THE DAY, AND UP TO 95% AT NIGHT.

based overseas proliferates. Some Internet observers have proposed allowing domain name registrars to block information about who controls the sites, which would make it 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. 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, including hosting files used for additional piracy. According to the FBI, more than 1 million computers have become ensnared in botnets.[7] "And the owners often have no idea that it's happening," says Dave Marcus, security research and communications manager with McAfee Avert Labs.

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.

The Risks to Consumers

Internet commerce is essentially 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, reputation, and financial security at risk. At the very least, it can lead to software incompatibility and viruses, drive up maintenance costs, and leave users without technical support and 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.

"WHEN SOMEONE CAME TO OUR SITE, THEY WOULD MAKE THEIR PURCHASES ONLINE, WITH EITHER A CREDIT CARD OR A DEBIT CARD, WHICH MEANS THAT NOW, THE PERSON YOU ARE BUYING PIRATED SOFTWARE FROM HAS YOUR CREDIT CARD OR DEBIT INFORMATION."

— DANNY FERRER, A CONVICTED SOFTWARE PIRATE WHO IS CURRENTLY SERVING A SIX-YEAR JAIL SENTENCE.

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

- 53% received software that was not what they had ordered;
- 36% reported that the software did not work;
- 14% immediately realized the software was pirated; and
- 12% never received the product.[8]

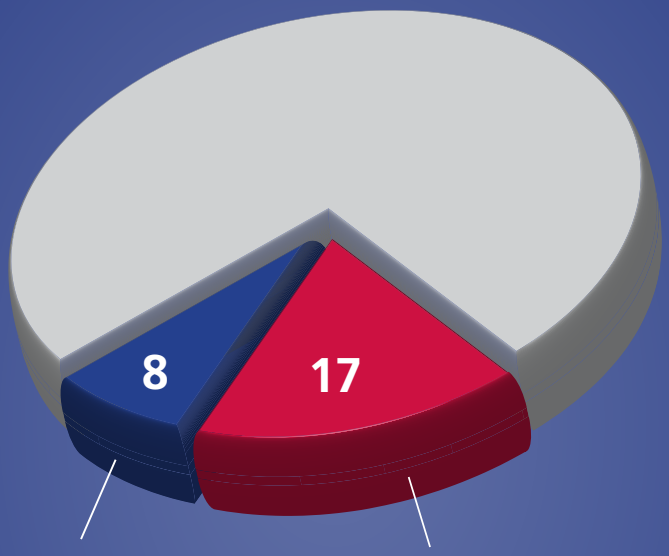
The risks to consumers also include:

- Not receiving upgrades, technical support, manuals or 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% of websites offering access to pirated software and piracy-related tools were distributing malicious code that could undermine IT security and performance. In some cases, the websites exploited vulnerabilities in the users' computers to install the unwanted software automatically.[9]

SOFTWARE PIRACY WEBSITES* ALSO SPREAD MALWARE

SAMPLE OF 98 UNIQUE WEBSITES



Sites with Malicious or Potentially Unwanted Software

Sites with Multiple Instances of Malicious or Potentially Unwanted Software

* SITES OFFER ACCESS TO PIRATED SOFTWARE AND PIRACY-RELATED TOOLS.
SOURCE: IDC STUDY, RISKS OF OBTAINING AND USING PIRATED SOFTWARE, 2006

A Closer Look at Auction Site Piracy

Of the various types of Internet-based piracy, auction site piracy is the most devious because it involves actual sales of software to consumers, as opposed to the other types of piracy that distribute free copies of software to people experienced enough to navigate P2P programs and other esoteric Internet channels.

No software titles are exempt from the threat of auction site piracy. A search of popular auction sites for the best-selling titles produces thousands of results, many with "Buy It Now" options.

While no one has quantified the scope of auction site piracy with a high degree of confidence, estimates have pegged the problem in the range of 50% to 90%. For example, in one 2005 study involving test purchases of more than 115 copies of software purchased from eBay, 39% were counterfeit and 12% came with additional software components that were counterfeit or genuine software that had been tampered with. This data indicated that there was a less than one-in-two chance of buying genuine, licensed software from eBay that had not been tampered with.[10]

Some auction sites provide limited safeguards such as tips for consumers, comments on sellers posted by other site users, and/or Spoof website protection, which is a toolbar that helps alert users when they are on fraudulent sites. But generally speaking, auction site owners disclaim responsibility for the legitimacy of any products sold or transactions made on their sites.

TOP TEN SOFTWARE PUBLISHERS* WITH MOST PRODUCTS AVAILABLE ON eBAY

1. Microsoft
2. Adobe
3. Apple
4. Corel
5. Symantec
6. McAfee
7. Borland
8. Autodesk
9. Solidworks
10. CNC

*AS OF JULY 31, 2008. BSA MEMBERS ONLY.

In the absence of any action by the auction sites themselves to stop software piracy, it is safe to assume the practice will spread as more people around the world go online every day and learn how to buy and sell items on the growing number of auction sites. In short, auction site piracy is unlikely to disappear altogether and is more likely to resemble the carnival "Whack-a-mole" game, disappearing here and reappearing there as software pirates work to evade watchful eyes.

CASE STUDY: eBay

As the world's leading online marketplace, eBay has an interest in ensuring that its online trading platform is trusted. In 2007, eBay had approximately eighty-four million active users worldwide, who traded more than $60 billion worth of goods. Unfortunately, the site is subject to abuse, as noted by *The New York Times*, which called eBay "the center of a new universe of counterfeit with virtually no policing."[1]

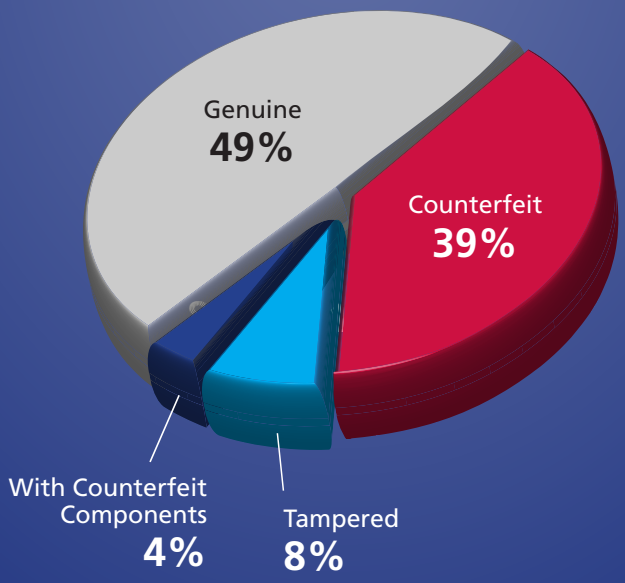
BSA has worked with eBay to fight software piracy for approximately ten years, and eBay has taken a number of steps to combat piracy. For example, eBay prohibits the sale of Original Equipment Manufacturer (OEM) or "bundled" copies of software—software obtained as part of the purchase of a new computer—unless the seller provides it along with the original computer hardware. But eBay does not actually police the listings on its site, and it disclaims any responsibility for doing so.

In another step, eBay created the Verified Rights Owner (VeRO) Program, giving intellectual property owners an avenue for reporting eBay listings that infringe upon their rights. Based upon information provided by rights holders, eBay investigates instances of possible piracy and may remove listings that violate VeRO policies. However, the system still leaves the primary burden of monitoring listings on the rights holders. It is not designed to protect consumers—and its benefits to consumers are limited.

1. "Seeing Fakes, Angry Traders Confront eBay," Katie Hafner, New York Times, January 29, 2006.

eBAY: TEST PURCHASES OF SOFTWARE

SAMPLE OF 115



SOURCE: MICROSOFT LEGAL AND COMPLIANCE TEAM, 2006, CITED IN "THE RISKS OF OBTAINING AND USING PIRATED SOFTWARE," IDC, OCTOBER 2006. TAMPERED INCLUDES BOTH GENUINE SOFTWARE WITH COUNTERFEIT COMPONENTS AND GENUINE SOFTWARE THAT HAS BEEN TAMPERED WITH.

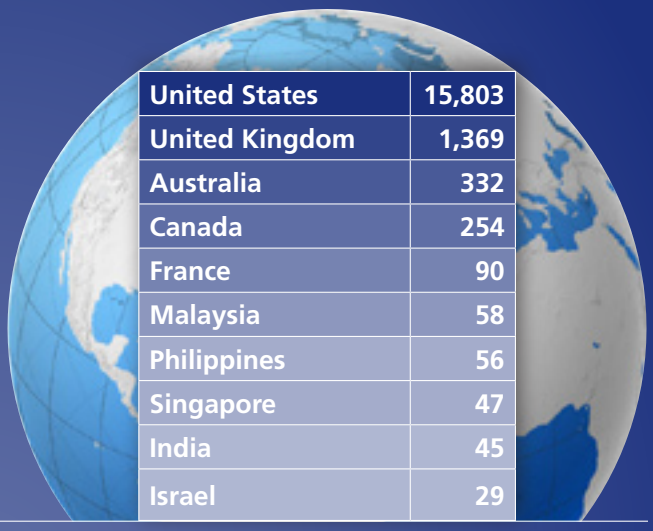
CASE STUDY: iOffer

iOffer was launched in 2001 as an alternative to eBay and other highly competitive auction sites. Unfortunately, it has not been immune to the activities of software pirates, and it also disclaims responsibility for the legitimacy of online transactions conducted on its platform.

In response to concerns about piracy, iOffer established C.O.P.S., the Counter Online Piracy System, which allows verified copyright owners to remove and/or disable access to items that may infringe upon their copyright.

BSA has recently added iOffer to the list of websites that it monitors for illegitimate software transactions and possible takedown notices.

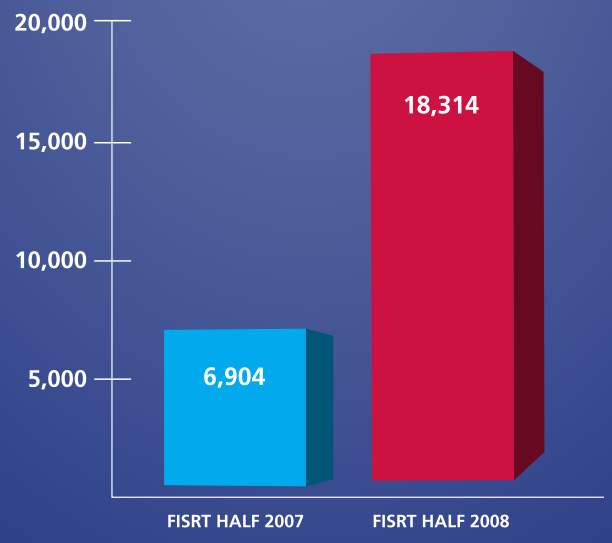
TOP TEN COUNTRIES FOR AUCTION SITE PIRACY TAKEDOWN REQUESTS, FIRST HALF OF 2008



United States	15,803
United Kingdom	1,369
Australia	332
Canada	254
France	90
Malaysia	58
Philippines	56
Singapore	47
India	45
Israel	29

SOURCE: BUSINESS SOFTWARE ALLIANCE

NUMBER OF ONLINE SOFTWARE AUCTIONS REMOVED DUE TO BSA REQUESTS



BSA has expanded its ability to request takedowns of suspicious online software auctions. Removals jumped 265% from 2007 to 2008.

SOURCE: BSA DATA

Investigations of P2P, Website, and Auction Site 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 websites 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 2007, BSA sent 471,694 non-BitTorrent takedown notices to ISPs. In the first half of 2008, BSA stepped up its efforts and issued 782,832 such takedown notices.

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 2008, BSA issued more than 48,000 notices related to BitTorrent files that were being used by 633,000 people to download BSA member software worth an estimated $525 million.

When BSA finds suspicious software being offered on auction sites, it issues takedown requests to the auction site providers to remove those listings. In 2007, BSA requested that auction site providers shut down more than 13,800 online auctions that were offering more than 50,500 individual software products with a total retail value of more than $13.3 million. Nearly two-thirds of the auctions shut down were on US auction sites. During the first half of 2008, BSA has expanded this effort, and requested auction site providers to shut down 18,314 auctions offering 45,000 products worth a combined $22 million.

As the chart on page 11 indicates, the number of auctions removed in the first half of 2008 increased by nearly three-fold compared to the same period in 2007, reflecting BSA's increased efforts to block auction site piracy.

Enforcement Action

When necessary and appropriate, BSA files civil lawsuits to try and stop Internet-based piracy, and sometimes it refers 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 others 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 between six and nine years and millions of dollars in restitution.

The following are highlights of several notable Internet piracy enforcement cases:

United States:

GEORGIA: In July 2008, a Savannah, Georgia, woman, was stopped from selling counterfeit copies of Corel software on eBay. A BSA investigation showed that she had sold more than $212,000 worth of unlicensed software to hundreds of consumers from January to May 2008. A $250,000 civil judgment was entered against her.

PENNSYLVANIA: Jon Crain of Coraopolis, Pennsylvania, operated nearly twenty websites distributing unlicensed copies of Adobe, McAfee, Microsoft, and Symantec software online. He was first targeted by BSA in March 2007 as part of an international legal action against five software pirates. The other offenders were located in the United Kingdom, Austria, and Germany. In many of these cases, BSA was alerted to the illegal activity by reports or complaints from disappointed consumers who were initially attracted by low price deals. BSA sued Crain, and a civil judgment was entered that included a hefty settlement payment and a requirement to remove the unlicensed software from his website.

OREGON: In July 2008, Jeremiah Mondello, a 23-year Oregon man, was sentenced to four years in federal prison for selling more than $1 million worth of pirated software and distributing malware via instant message networks to steal financial data from dozens of consumers. He then used the stolen bank account credentials to set up more than forty online auction accounts in the victims' names and withdraw money from their debit accounts. In addition to the prison sentence, federal investigators also seized computers and $220,000 in cash from Mondello. The government also is entitled to seize his home and surrounding land.

CALIFORNIA: Nathan Peterson ran a Los Angeles-based, for-profit website called www.iBackups.net from which he sold illegal copies of software programs copyrighted by Adobe, Macromedia, Microsoft, Symantec, and others. An investigation conducted by the FBI, with support from BSA, determined that Peterson sold more than $20 million worth of software and pocketed more than $5.4 million.

The DOJ believed that Peterson was "the most prolific online commercial distributor of pirated software ever convicted in the US." He was sentenced to a prison term of 87 months and ordered to pay $5.4 million in restitution.

Asia Pacific:

TAIWAN: In October 2007, the Taiwanese police raided a large Internet pirate site called the XYZ Information Workshop in Kaohsiung and arrested a father and son engaged in piracy. The authorities seized 27 CD burners and more than 80,000 copies of illegal CD-Rs containing business software, games, music, and movies. The estimated retail value of the goods was more than $30,000,000, and the pirates' estimated daily revenue was $3,000. BSA actively assisted the police in this case.

THAILAND: In April 2008, the Bangkok police raided the offices of www.idsoft.org, a website offering counterfeit software by mail. During the raid, the police arrested the 28-year-old pirate who had been operating the website and seized significant evidence including large quantities of supplies needed to make and mail copies of software, as well as 138 CDs containing Adobe, Autodesk, and Microsoft programs.

INDIA: BSA in 2007 carried out civil enforcement action against Hyderabad-based SM Technologies, leading to the seizure of pirated software worth approximately $475,000.

A total of 1,843 CDs were recovered. This was the second time in three years that the same company was raided. In September 2004, BSA filed a criminal complaint against the company, leading to police raids at three locations in Hyderabad. SM Technologies was creating "compilation pirated CDs" with a range of products from Adobe, Autodesk, Microsoft, and Symantec, and selling the pirated software through multiple channels, including the Internet, resellers, and directly to end-users.

Europe, Middle East and Africa:

UKRAINE: In May 2006, a Ukrainian man, Maksym Vysochanskyy, was sentenced to 35 months in prison for his role in selling pirated copies of software from Adobe, Autodesk, Borland, and Microsoft through websites he operated and on eBay. The case was one of the first in the nation to involve an extradition in a prosecution for intellectual property offenses. Authorities from Canada, Lithuania, and Ukraine also took part in the investigation, and the Royal Thai Police collaborated in Vysochanskyy's capture and extradition while he was on a trip there.

RUSSIA: In April 2008, the district court of Izhevsk imposed a criminal verdict on a Russian man who had created an FTP resource on his home computer to sell pirated copies of Adobe and Microsoft products worth more than $15,000. The local police made several test purchases of software from Titov and matched them with the software on his PC.

CASE STUDY: **Danny Ferrer**

Video excerpts from an interview with Danny Ferrer can be viewed online at **www.bsacybersafety.com/video**.

After receiving a tip from BSA, an FBI investigation determined that from late 2002, Danny Ferrer of Lakeland, Florida, was operating for-profit websites selling illegal copies of software published by Adobe and Autodesk. Ferrer sold approximately $20 million worth of copyrighted software products on www.BuysUSA.com at prices substantially below the suggested retail price. For example, software that had a retail value of more than $600 was purchased by BSA from Ferrer for $57. The software products purchased were reproduced on recordable CDs and distributed through the mail. On the CD-R discs, Ferrer included labels that featured trademarks of the legitimate software companies and a serial number that allowed the purchaser to activate and use the product.

Ferrer made more than $4.1 million from his operations, which was used to purchase luxury cars, airplanes, a helicopter, and boats. These items were all confiscated by the FBI, and Ferrer was sentenced in federal court to six years in prison. He also was ordered to pay more than $4.1 million in restitution.

CASE STUDY: **The Robberson Brothers**

In early 2002, BSA began investigating Maurice A. Robberson and his brother, Thomas Robberson, after receiving complaints from software publishers. After reviewing the four reported websites, BSA made undercover purchases and determined that the software sold was pirated. BSA then referred the case to the FBI Washington Field Office, which conducted its own investigation and subsequently shut the operation down in October 2005.

The FBI investigation determined that from late 2002, the Robberson brothers sold more than $5 million of counterfeit software products. In addition to running four for-profit websites, the Robberson brothers were also co-conspirators with Danny Ferrer in the operation of www.BuysUSA.com.

During the operation of the websites, Thomas Robberson grossed more than $150,000 selling software with a retail value of nearly $1 million. Maurice Robberson grossed more than $855,000 selling software with a retail value of nearly $5.6 million.

In March 2008, Maurice Robberson was sentenced to thirty-six months in prison, while his brother Thomas was sentenced to thirty months. Both were also ordered to undergo an additional three years of supervised release and pay restitution.

BSA Partnerships and Educational Outreach

Beyond enforcement actions, BSA also works with various organizations to gain a better 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.

NATIONAL INTELLECTUAL PROPERTY LAW ENFORCEMENT COORDINATION COUNCIL (NIPLECC): NIPLECC is an interagency group responsible for coordinating the United States' domestic and international intellectual property enforcement activities. Members include the director of US Patent and Trademark Office (USPTO); the Assistant Attorney General for the Criminal Division; the Undersecretary of State for Economics, Business and Agricultural Affairs; the Deputy United States Trade Representative; the Commissioner of Customs; and the Under Secretary of Commerce for International Trade. BSA is among the industry associations that have appointed liaisons between their members and the US Commerce Department's Trade Compliance Center.

US IPR TRAINING COORDINATION GROUP: 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.

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 six million consumers through outreach efforts including media tours, direct mail, television and radio advertising, and online initiatives.

"DON'T GET DUPED": BSA's "Don't Get Duped" website offers consumers a forum 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 150 complaints involved eBay.

For example, many consumers have complained about receiving software that was obviously pirated, oftentimes on obviously 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 ten 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 man never got his money back.

More stories about consumers who were duped are posted on BSA's Cyber Safety website, **www.bsacybersafety.com**.

B4USURF: In Asia, BSA manages a cyber safety and ethics campaign (www.b4usurf.org) aimed at influencing youths aged ten to eighteen years old. The centerpiece of the initiative is a website 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, and the Philippines, with India, Hong Kong, and Thailand to be added later.

EDUCATIONAL VIDEO: To help individuals avoid purchasing fraudulent software online, BSA developed a brief educational video, "Software Piracy Exposed: A Dangerous Business for Buyers and Sellers." The video educates consumers about safe online shopping while alerting potential sellers of the serious legal consequences of software piracy. The video includes interviews with Danny Ferrer, a convicted software pirate sentenced to six years in federal prison (see case study); a victim of online auction software fraud; a high-ranking Department of Justice official; a BSA spokesperson; and helpful tips on how to prevent against consumer fraud. The video is available for viewing at **www.bsacybersafety.com**.

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 and refers cases to the appropriate local, state, federal, or international agency for possible investigation and prosecution.

In 2007, IC3 processed more than 219,553 complaints spanning the spectrum of Internet crime from auction site fraud, credit/debit card fraud, computer intrusions, unsolicited e-mail, and child pornography. From the submissions, IC3 referred 90,008 complaints to the appropriate law enforcement agencies. The total dollar loss from all referred cases of fraud was $239.09 million, with a median dollar loss of $680 per complaint. This was an increase from $198.44 million in total reported losses in 2006.

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

Auction Sites Must Do More to Protect Consumers

Given the growing role of auction sites in software piracy and the especially high hurdles in identifying and fighting such piracy, BSA believes auction sites should take the following additional steps to protect consumers:

ASSUME RESPONSIBILITY: To date, auction sites have insisted that piracy on their sites is beyond their ability to police. Although the challenge is certainly broad and complicated, auction sites could do much more to protect consumers by working more closely with the software industry and others to share information and collaborate on best practices.

WARNINGS: Current warnings to sellers and buyers of software—if they exist at all—tend to be buried in hard-to-find areas of auction sites. To have a greater impact, auction sites should post warnings to vendors at the time they list their products and to consumers at the point of bidding. These could take the form of pop-up ads reiterating the risks and penalties of dealing in pirated software.

SLOW IT DOWN: Several of the auction sites offer consumers a "Buy It Now" option, short-cutting the auction process in favor of quick sales at discounted prices. However, the speed of such transactions makes it harder to monitor and catch the scammers. Recognizing that an estimated 50% to 90% of the software on their sites is illegitimate, the auction sites should eliminate the "Buy It Now" option for software sales.

What Consumers Can Do to Protect Themselves

As described throughout this report, consumers face a serious risk of identity theft, having their computers become involved in cyber crime, and many other hassles when buying software from questionable sources online. Armed with the right information, however, consumers can avoid online software piracy scams and protect their personal well-being. The following is a list of tips for consumers:

Use software 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.

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. Also, check the online seller's price against the estimated retail value of the software. Whether the product is being sold as new or used, if a price for software seems "too good to be true," it probably is.

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 website in order to determine its legitimacy. You may also check for a Better Business Bureau report at **www.bbb.org**.

Do your homework.

On auction sites, check the seller's rating or feedback comments by other users. 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.

Steer clear of compilations.

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. When buying more than one software program, be sure that each program is on a separate disk.

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 final.

Keep receipts.

Keep as much information as possible regarding the transaction and the seller. Print out a copy of your order with confirmation numbers and file it for your records. This information will help to build your case if the product turns out to be pirated and further action is needed with the auction site or payment facilitator site.

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 website'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; or you can check the website 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."

Be cautious when dealing with software sellers in other countries.

Many cyber crime rings are based in countries abroad. Moreover, the physical distance, differences in legal systems, and other factors could complicate matters if the transaction goes awry.

Recognize and avoid e-mail spam.

Indicators that an e-mail may be unsolicited spam include senders whose names you do not recognize; typos and odd phrases in the subject line; and prices that seem too good to be true. Delete such messages without opening them, and empty your "trash" folder frequently.

How to Report Suspected Software Piracy and Fraud

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.bsacybersafety.com** or call **1-888-NO-PIRACY**.

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 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 considerable resources on pushing back the enemy.

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

End Notes

1. "Justice Breyer Is Among Victims in Data Breach Caused by File Sharing," Brian Krebs, *The Washington Post*, July 9, 2008.
2. BSA sources.
3. Estimate as of May 31, 2008. Internet World Stats by Miniwatts Marketing Group, http://www.internetworldstats.com/.
4. "The Fight for Cyber Space: High Tech and Law Enforcement Experts on Defeating Today's Cyber Criminals," Business Software Alliance, 2007.
5. "2007 Global Software Piracy Study," IDC, May 2008; "2007 State Piracy Study," IDC, July 2008; "Piracy Reduction Impact Study," IDC, 2008, all available at www.bsa.org.
6. Based on a study of Internet traffic in Europe, the Middle East and Australia from August to September of 2007. "Majority of Internet bandwidth consumed by P2P services," Paul Mah, IT News Digest on Tech Republic.com, November 28, 2007, http://blogs.techrepublic.com.com/tech-news/?p=1651.
7. "Over 1 Million Potential Victims of Botnet Cyber Crime," FBI press release, June 13, 2007.
8. "National Survey Reveals Consumers Concerned About Safety and Security of Online Shopping," BSA press release, November 15, 2006.
9. "The Risks of Obtaining and Using Pirated Software," IDC, October 2006.
10. "The Risks of Obtaining and Using Pirated Software," IDC, October 2006.

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

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
F +44 [0] 20 7340 6090

WWW.BSA.ORG