THE CHANGING FACE OF CYBERCRIME

NEW INTERNET THREATS CREATE CHALLENGES TO LAW ENFORCEMENT

By Terrence Berg

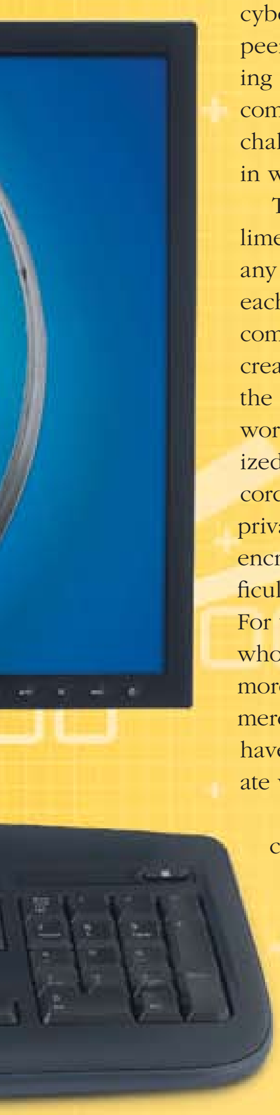
Since 1995, when average Americans first began exploring the Internet, prosecutors and police have been called on to respond to new kinds of crimes in what some called the "Wild West" of cyberspace. Assessing the state of cybercrime more than 10 years later, it's a good news/bad news situation. The good news is that federal, state, and local authorities have taken significant strides in developing their cybercrime-fighting capacities, with numerous prosecutions of Internet predators and online child pornography traders being handled by both local police departments and federal-state task forces across the nation. The bad news is that enforcing the law in cyberspace means adapting to an ever-evolving frontier where new criminal threats are constantly emerging, and law enforcement is still struggling to keep up.

"Cybercrime" generally includes any crime carried out primarily by means of a computer or the Internet. Examples include hacking into or damaging a computer network; accessing and stealing electronic data or trade secrets without authorization; fraud in connection with an Internet auction; "spam" (false or misleading bulk commercial e-mail); e-mail threats of violence or extortion ("cyberstalking"); stealing credit card information through a phony website log-in page ("phishing"); soliciting minors for sexual activity or trading child pornography or other contraband over the Internet; and distributing pirated music, movies, and software via file-sharing networks (or "warez" sites), just to name some of the most common.

In recent years, the face of cybercrime has changed due to the growth of three phenomena: (1) new Internet environments, such as "peer-to-peer" networks and "social networking" sites; (2) organized cybercrime groups; and (3) powerful new "smart" viruses.

THE EVER-CHANGING ENVIRONMENT

Two new modes of Internet communication that have exploded in the last several years illustrate the shifting battlefield of



cybercrime: (1) file-sharing networks, also known as peer-to-peer (or P2P) networks; and (2) social networking websites, such as MySpace.com and Facebook.com. Both of these modes of communication present challenges for investigators and create environments in which certain kinds of illegal activity flourish.

The P2P networks (such as Kazaa, BitTorrent, and limewire) are tailor-made for sharing digital media of any kind; by downloading the P2P client software, each user's designated collection of digital files becomes accessible by every other user, in a privately created network. Both the Department of Justice[1] and the entertainment industry have targeted P2P networks in an effort to combat the rampant unauthorized distribution of software, movies, and music recordings that takes place via such networks.[2] The private networks created by P2P technology are often encrypted and password-protected, making them difficult to discover and resource-intensive to investigate. For this reason, child pornography traders and others who traffic in digital contraband find P2P networks a more effective hiding place than easy-to-search commercial websites or web-based e-mail services that have strict terms of service and are willing to cooperate with law enforcement.

Both MySpace and Facebook allow members to create personal web pages containing personal profiles, photos, video clips, lists of interests, shared posted messages, e-mail accounts, and instant messaging. Members join multiple groups of "friends" who may grant mutual access to each others' sites. Facebook, created by two Harvard students in 2004, grew from zero to over 7.5 million users, nearly all college students, in only two years. Yahoo! has reportedly offered $900 million to purchase Facebook, which according to one report has become the seventh most-trafficked website in the United States.[3] Even more explosive has been MySpace.com, which started in 2003 and is now reported to be the third most-visited site, with over 106 million users and new registrations reported at 230,000 per day. MySpace was bought by Rupert Murdoch's Newscorp for an estimated $327 million in 2005. In August of 2006, Google paid $900 million to Newscorp to become the search engine of MySpace.[4]

Like the Internet chatrooms frequented by child sexual predators, MySpace has already been the forum for some celebrated cases of child solicitation.[5] In June 2006, a Michigan teenager garnered national headlines when she was intercepted by U.S. authorities in Jordan after traveling to meet a Palestinian man she had encountered through her MySpace page.[6] MySpace and Facebook are subject to abuse by child predators just like other Internet forums that offer chatrooms and private chat sessions. Unlike chatrooms, however, the social networking sites promote sharing a vast amount of personal information divulged on a user's MySpace or Facebook page and engender a feeling of trust among "friends" in the social network. These sites are built on the model that people who already know each other will create online "friend" communities by allowing each other access to their sites. However, since "friending" another user is accomplished by nothing more than a click of "offer" and a return-click of "acceptance," with no requirement of verification or due diligence, the circles of "friends" can quickly escalate into worldwide multitudes of defacto strangers, but perhaps with a false sense of security. The sites are powerful network-building tools, but are used increasingly by teenagers and college students with little or no adult supervision.

MySpace has already been victimized by a "cross site-scripting worm," called the "samy worm," which, within 20 hours of its release in October 2005, had altered the profiles of a million MySpace users to include the tagline, "But most of all, Samy is my hero."[7] If that many users' sites could be affected so quickly by a comparatively harmless prank, the potential for greater abuse is obvious and serious. Another worm released through a flaw in Quicktime media player stole 100,000 MySpace passwords, and these accounts were then used to send spam.[8]

What are the consequences of these social networking sites for law enforcement? With millions of users packing these sites with personal information of every type, from family photos and movies to career interests to what used to pass for private gossip among close friends, these sites are gargantuan warehouses of valuable personal identity, consumer preference, personality and family issues, and online usage/habit information that could be exploited if made accessible to those with criminal ends in mind. They are a treasure trove for the Internet child predator or ID thief.

FAST FACTS:

Cybercrime is becoming more complex, better organized, and harder to stop as criminals take advantage of new technologies like social networking websites, "smart" viruses, and foreign-based criminal syndicates.

Aggregating user data in the hands of fewer service providers increases the risk of identity theft and other data compromises because so many users are interlinked.

Both P2P networks and social networking sites represent, on the one hand, the trend of interconnecting and sharing the contents of individual users' data, and on the other hand, the trend of aggregating the personal data of millions of individuals in the control of a small number of service providers. Placing so many "eggs in so few baskets" presents a target-rich environment for those seeking to steal data, and runs the risk that viruses or worms intended either to collect data or damage systems will have devastating multiplier effects because so many users are interlinked. These new technologies are changing at lightning speed, while the law itself is slow to change and law enforcement's resources are challenged as well.

CHANGING PROFILE OF A CYBERCRIMINAL: FROM NERDY LONER TO SYNDICATE MEMBER

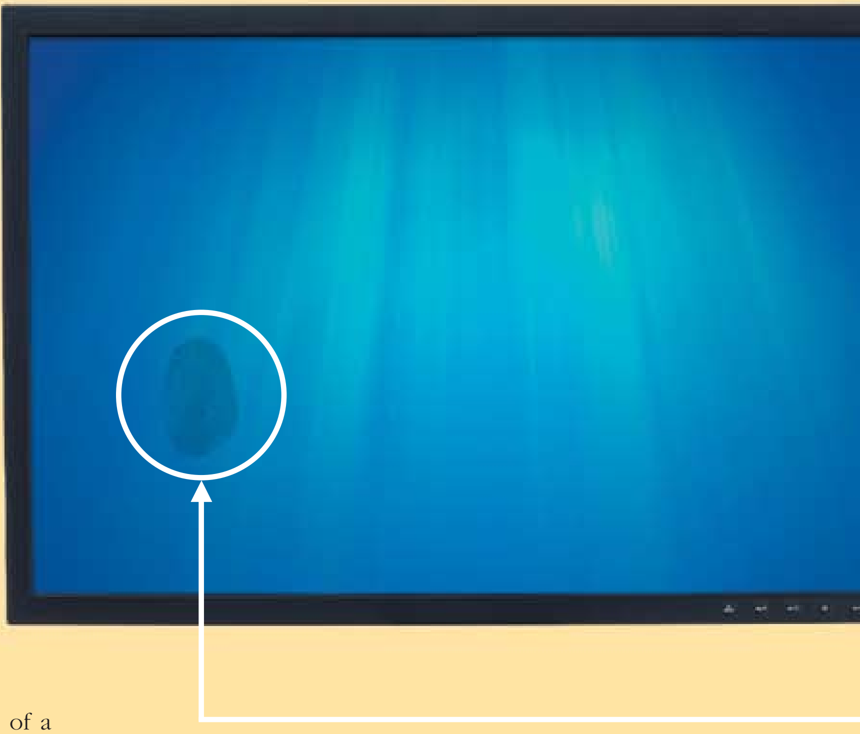
The profile of the typical cybervillain has also matured in dangerous ways. Unlike the lone hacker of the past, cybercriminals today are becoming more organized, profit-driven, group-oriented, and technologically advanced in their craft.

Two kinds of Internet fraud are attracting highly organized criminals: illegal spam—fraudulent bulk commercial e-mail—and phishing—the use of phony financial websites to harvest personal identity and account information. In 2003, Congress passed the CAN-SPAM Act, making mass commercial e-mail campaigns illegal when they involve statutorily defined badges of fraud. Although criminal cases have been successfully prosecuted under CAN-SPAM,[9] the law has not reduced the volume of unwanted spam on the Internet. By December 2006, unsolicited spam e-mail accounted for 90 percent of all e-mail sent on the Internet.[10]

Spammers are turning the Internet's own architecture to their advantage by employing legions of virus-infected computers, known as "botnets" to blast out their spam.[11] Since the spam is routed through networks of infected "robot" or "zombie" computers, it prevents spam recipients from knowing the actual source of the junk e-mail. Although the exact number is unknown, it is estimated that millions of computers across the Internet,[12] from unprotected servers in former Eastern bloc countries to family PCs with "always-on" cable connections, are infected with "bot" viruses. The botvirus causes the computer to "phone in" to a command and control server on a channel that the "bot master" (or "bot herder") uses to issue commands to the waiting army of infected computers. Frequently, operators of bot networks are selling their services to spammers, mailing out spam runs over thousands of infected computers[13] that will provide no trail back to the real spammer. According to a report in the *New York Times,* "botnet programs are present on about 11 percent of the more than 650 million computers attached to the Internet,"[14] and these botnets are compromising as many as 250,000 new computers every day.[15] Organized groups, rather than lone hackers, are responsible for 80 percent of spam, according to Spamhaus, an anti-spam group.[16]

Spammers can spend thousands of dollars on mailing software that will handle millions of messages, insert randomly generated return addresses, and automatically scan the Internet for open proxy computers through which to blast (and mask) the spam.

Unfortunately, botnets can also harvest data from the infected computers. One file generated by a botnet was found to contain a huge amount of financial data: log-in credentials, credit card numbers, and other data pertaining



to hundreds of bank, stock brokerage, e-commerce, and e-mail accounts.[17] Microsoft attorney Aaron Kornblum, a senior attorney for the company's Internet Enforcement Safety team, cited botnets as a major problem in a *PC World* report: "Botnets are really where it's at for serious cybercriminals, because of their concentrated power. That power can be used for all sorts of malicious conduct on the Internet."[18]

Some of the more serious bot masters include organized criminal groups in Russia, according to a recent report in *e-Week,* which cited "a well-organized hacking gang controlling a 70,000-strong-peer-to-peer botnet"[19] that included compromised computers in 166 countries, mainly the United States.[20] As *Wired* writer Scott Berinato put it, "The bot market isn't like the ad hoc street-corner bazaar of cheap handguns. It's more like the narcotics business: a highly organized subculture of people fulfilling specific functions. There are producers, distributors, and customers with varying degrees of criminal involvement."[21]

Theft of financial data through phishing, the creation of a bogus bank or brokerage website link that is then mass e-mailed in the hope that recipients will provide passwords, log-ins, Social Security numbers, or other account information, is also increasing in its sophistication and degree of organization. Again, emerging organized criminal groups have been detected in a recent surge of phishing sites. According to one group that monitors phishing sites, identified scam sites increased by 12,000 to 37,444 from August to October 2006.[22] One criminal organization known as "Rock Phish" (identified by the term "rock" found in subdirectories of its fake sites) is estimated by some security experts to be responsible for between one-third and one-half of all phishing messages sent out in a given day. It has spoofed sites from 44 different businesses in 9 countries, and funnels all stolen financial information to a central server.[23]

The downside of the international nature of these groups is that gathering evidence abroad can be slow and difficult, and the data may be gone by the time the legal process is complete. The upside of their intense profit motive is that it becomes possible to "follow the money." Just as traditional "real world" organized crime requires a sustained and specialized law enforcement response to be successfully investigated and prosecuted, the emergence of foreign-based, highly organized and sophisticated cybercrime syndicates will also necessitate a robust governmental response to be checked. As one network security firm president put it, "We used to call the Internet a sort of Wild West. Now it's more like Chicago in the 1920s with Al Capone."[24]

THE "WEAPONIZATION" OF MALWARE: SMART VIRUSES AUTOMATE THE CRIME

Like the advances in IT generally, the malicious programs used by cybercriminals include more and more automated functions that make crimes easier to commit and more damaging. Spammers, for example, can spend thousands of dollars on mailing software that will handle millions of messages, insert randomly generated return addresses, and automatically scan the Internet for open proxy computers through which to blast (and mask) the spam. Spamming programs also have innovated new ways to evade filters, by embedding the text message in an image that can't be scanned for key words, and also altering a few pixels in each message so that filters using pattern recognition or "fingerprinting" will not see the same signature, even though the message appears identical to the human reader.[25]

Fraudsters interested in the phishing game need not be computer whizzes. For about $1,000, they can download a sophisticated tool kit that will allow them to enter the web address of the site to be spoofed, along with the IP address where the fake site will be hosted, and, *presto,* the software will pull down the image of the legitimate commercial site to the bad guy's server. The link—which actually leads to the bad guy's server—is then e-mailed to unsuspecting victims. Victims see the current website of their legitimate company—but any information they enter goes directly to the bad guy.[26]

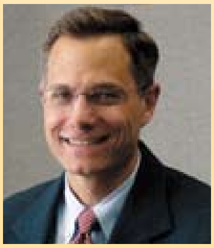
Those trojan viruses employed to dragoon computers into botnets have been found to possess as many functions as a Swiss Army knife. The "spam-thru Trojan," for example, not only will convert your computer into a willing botnet soldier, it also installs its *own* anti-virus scanner, and removes any competing malware from the machine—thereby kicking out the competition.[27] This virus then sends the stats from the infected computer back to a central database and includes access to a list of proxy servers that the infected computer could use to further hide the source of the spam.[28] Another botvirus was programmed to look in "last accessed" files first for valuable personal data.[29] A particularly

New technologies are changing at lightning speed, while the law itself is slow to change and law enforcement's resources are challenged as well.

virulent botvirus called "Rustock.B," linked to several hundred thousand infected computers that were drafted into carrying out a "pump and dump" stock scam, was found to have the ability to *change its own programming* slightly at each infection, thereby making it impossible to be recognized by anti-virus software.[30]

Responding effectively to cybercrime in a changing environment, against more organized criminals using advanced malicious technologies, is a tall order for law enforcement. Fortunately, highly trained agents have scored some victories in even the most complex of cases.[31] The Department of Justice has two major initiatives dedicated to addressing these crimes. To combat child exploitation on the Internet, Project Safe Childhood has provided training and expertise to federal prosecutors throughout the country. In addition, teams of specialized prosecutors called CHIP (Computer Hacking and Intellectual Property) attorneys have been designated in United States Attorney's Offices nationwide to beef up the federal capacity to fight sophisticated cybercrimes such as hacking, Internet fraud, and intellectual property theft. The Detroit U.S. Attorney's Office has deployed both of these teams in its continuing efforts to respond to this growing area of crime. ■

This article represents the author's opinion and views and does not necessarily represent the views of the Department of Justice.



Terrence Berg is the first assistant United States attorney for the Eastern District of Michigan Office of the U.S. Attorney, concentrating in cybercrime, white-collar crime, and intellectual property prosecutions.

FOOTNOTES

[1] In May 2005, "Operation D-Elite," conducted by the Department of Justice, resulted in the takedown of a P2P network called "Elite Torrent," which was using the BitTorrent P2P network to allow over 130,000 members to distribute copyrighted works such as movies, music, and software.

[2] See, e.g., *Metro Goldwyn-Mayer Studios, Inc v Grokster, Ltd,* 545 US ___, 125 S Ct 2764 (2005) (allowing civil action against peer-to-peer style network for intentionally inducing or encouraging the theft of copyrighted materials).

[3] See Facebook entry in wikipedia, online encyclopedia, <http://en.wikipedia.org/wiki/Facebook> (accessed April 29, 2007).

[4] See MySpace entry in wikipedia, online encyclopeida, <http//en.wikipedia.org/wiki/MySpace> (accessed April 29, 2007).

[5] *MySpace Hit with Online Predator Suits,* New York Times (AP), January 19, 2006, <http://nytimes.com/aponline/technology/AP-MySpace-Lawsuit.html> (accessed January 19, 2006).

[6] *Michigan Teen in Seclusion After Overseas MySpace Trip, Lawyer Says,* FOXNEWS.com (AP), June 13, 2006, <http://www.foxnews.com/story/0,2933,199247,00.html> (accessed January 19, 2007).

[7] Robert Vamosi, *MySpace YourVirus,* cnet Reviews, December 7, 2006, <http://reviews.cnet.com/4520-3513_7-6674087-1.html> (accessed May 2, 2007).

[8] *Id.;* see also *Cybercrooks Deliver Trouble: With Filters Working Overtime, Security Experts See No Let Up in '07,* Washington Post, December 27, 2006, at D01. (MySpace accounts hijacked for spam by worm.)

[9] The first criminal prosecution for a violation of CAN-SPAM was brought in the Eastern District of Michigan, *United States v Daniel Lin,* Crim No 04-80863.

[10] *Cybercrooks Deliver Trouble: With Filters Working Overtime, Security Experts See No Let Up in '07,* Washington Post, December 27, 2006, at D01; Brad Stone, *Spam Doubles, Finding New Ways to Deliver Iself,* New York Times, December 6, 2006. (Nine out of 10 e-mails on the Internet are unsolicited junk e-mail.)

[11] *Id.*

[12] John Markoff, *Attack of the Zombie Computers is Growing Threat,* New York Times, January 7, 2007.

[13] *Id.*

[14] *Id.*

[15] Stone, *supra.*

[16] *9 out of 10 e-mails now spam,* CNN.com, November 27, 2006, <http://www.netenigma.com/news/cnn/cnn-11282006-spamemail.pdf> (accessed May 10, 2007).

[17] Markoff, *supra.*

[18] Robert McMillan, *Microsoft Sees Botnets as Top Cyberthreat,* PC World, January 3, 2007.

[19] *Id.*

[20] *Id.*

[21] Scott Berinato, *Attack of the Bots,* Wired.com, <http://www.wired.com/wired/archive/14.11/botnet.html> (accessed May 2, 2007).

[22] Brian Krebs, *Cyber Crime Hits the Big Time in 2006: Experts Say 2007 Will Be Even More Treacherous,* Washington Post, December 22, 2006.

[23] Robert McMillan, *Who or What is 'Rock Phish' and Why Should You Care: Security experts believe that the entity or people behind Rock Phish are the rock stars/innovators of most new evil phishing scams,* PC World, December 12, 2006.

[24] Berinato, *supra,* quoting Keith Laslop of Prolexic.

[25] Stone, *supra;* Ryan Naraine, *Pump and Dump Spam Surge Linked to Russian Bot Herders,* e-Week, November 16, 2006.

[26] Joris Evers, *New Tool Enables Sophisticated Phishing Scams,* CNET News.com, January 10, 2007, <http://news.com.com/2100-1029_3-6149090.html> (accessed May 2, 2007).

[27] Naraine, *supra.*

[28] *Id.*

[29] Markoff, *supra.*

[30] *Cybercrooks Deliver Trouble: With Filters Working Overtime, Security Experts See No Let Up in '07,* Washington Post, December 27, 2006, at D01; Krebs, *supra;* Markoff, *supra.*

[31] *To Catch Crooks in Cyberspace, FBI Goes Global,* Wall Street Journal, November 21, 2006.