

Policing Bad Behavior in New Internet Markets  
David Bateman, K&L Gates

16<sup>th</sup> Annual Seattle Conference on New Developments in Technology Law  
December 13, 2007

As commerce and social interaction have moved to the Internet, criminals have followed. A significant portion of Americans get their news, do their banking and search for their soul mates online. It should be no surprise that these new avenues of human interaction have been infiltrated by scammers of all types.

Internet criminals, like their brick-and-mortar predecessors, are opportunists. Like viruses, they morph and mutate to take advantage of new services, new technologies, and new user behaviors. And because they can harness the power of technology and the immense penetration of the Internet, they can react immediately and globally to seize opportunities.

For example, two weeks after Hurricane Katrina, the FBI's cybercrime division reported the creation of more than 2000 websites dedicated to collecting money for hurricane relief, with the vast majority designed to defraud their on-line visitors.<sup>1</sup> Similar scams were apparent in the aftermath of the Asian tsunami in 2004 and are likely being developed after last week's Bangladesh cyclone. And as tax time approaches, consumers need to be wary of "Internal Revenue Service" phishing scams.<sup>2</sup>

Most new products and services are attacked almost immediately. Hackers and phishers are always looking for new opportunities and are not deterred by technological protection. For example, the immense popularity of social networking sites made them immediate and valuable target for phishers and spammers. Crackers have succeeded in decoding even immensely sophisticated Digital Rights Management technology, most recently publishing a key for unrestricted access to AACS-restricted HD DVD content.<sup>3</sup> Hackers were also quick to unlock the Apple iPhone, competing for honors among their community.

Moreover, even the best technology cannot prevent fraud if humans willingly supply sensitive information to charlatans. Much of the criminal Internet activity involves social engineering and plain old trickery. Phishing and its variants -- "spear phishing," "vishing" and "smishing" -- are all premised upon luring a human user into a false sense of confidence. The classic Nigerian 419 scam requires almost no technology; today's emails from deposed Nigerian princes simply replace the letters and faxes of

---

<sup>1</sup> See "Online scams emerge in Katrina's wake," CNET News.com, September 1, 2005.

<sup>2</sup> See, e.g., IRS Publication IR-2006-116, July 19, 2006, "Electronic Federal Tax Payment System Cited in New Email Scam."

<sup>3</sup> See <http://www.drmwatch.com/standards/article.php/3653281>

yesterday. That scam, like others, persists primarily because humans are the weak link in the Internet ecosystem, not because of technological advances.

It is impossible to identify or categorize all of the scams, frauds, hacks and bad behavior that occur on the Internet. It is probably fair to say that every Internet-based activity is tested for vulnerabilities and is exploited to the extent that it is profitable. Hackers are numerous and talented. As Internet activity expands into more walks of life, fraud will inevitably follow. Some of the more recent and interesting activities occurring on the Internet, and the scams related to them, are discussed in more detail below.

## **BOTNETS**

A botnet is the workhorse of the cybervillian's operation. By using vast armies of infected computers to do his bidding, a scammer can exponentially scale his activities while shielding his operation from detection. "Bot masters" who create and control these armies rent them to spammers, scammers and miscreants of all kinds, for several hours or several days.

A botnet is simply a collection of robots, or "bots," which are controlled remotely as a group. After becoming infected with botnet malware, compromised computers (or "zombies") report back to a command-and-control server, through which their instructor ("bot-herder" or "bot-master") provides instructions. Industry analysts estimate that there are at between 75 million and 150 million infected computers worldwide, and that number is growing.<sup>4</sup>

A large botnet may control over one million machines.<sup>5</sup> The newest and most notorious botnet – propagated by the "Storm" worm – is believed to control up to 50 million compromised computers.<sup>6</sup> Storm first appeared in late 2006, as an email attachment with a holiday greeting or a news report about imminent war. By 2007, Storm was distributed through e-card greetings, and most recently through MP3 attachments. Since July, e-mail management company Postini alone has blocked nearly 1.5 billion copies of Storm.<sup>7</sup>

Botnets can be used for almost any type of illegal activity. Spamming is a common function; botnets are responsible for between 50% and 80% of all spam sent on the Internet.<sup>8</sup> Botnets are also used to distribute spyware and to conduct denial-of-service attacks. And they are incredibly efficient at self-propagating, replicating themselves and spreading their payload to vulnerable or unsuspecting victims. Botnet operators enjoy

---

<sup>4</sup> "FireEye CEO Ashar Aziz: Battling the Zombie Hordes," by Jack M. Germain, *TechNewsWorld*, September 25, 2007; "Attack of the Zombie Computers Is Growing Threat," by Josh Markoff, *New York Times*, January 7, 2007.

<sup>5</sup> "Dutch Botnet Suspects Ran 1.5 Million Machines," by Gregg Keizer, *TechWeb Technology News*.

<sup>6</sup> "Worm 'Storm' gathers strength", by Kevin Speiss, *Neo Seeker*, September 7, 2007.

<sup>7</sup> "Spam-spitting Storm virus, a year old, is as tricky as ever," by Jon Swartz, *USA TODAY*, November 19, 2007.

<sup>8</sup> "Spam Slayer: Slaying Spam-Spewing Zombie PCs," by Tom Spring, *PC World*, June 20, 2005.

anonymity by controlling the botnets remotely. Investigators tracing back nefarious activity dead end at an infected home PC, not at the botmaster's control server.

The creation of botnets, and their use for cybercrime, is addressed by a number of existing laws. Fundamentally, obtaining unauthorized access to computers is a violation of the federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. It is likely also a violation of numerous state statutes aimed at computer protection, including:

- State Computer Crimes Statutes
  - Arkansas Code Annotated § 5-41-103;
  - Cal. Penal Code § 502;
  - 11 Delaware Code § 2738;
  - Hawaii Revised Statutes Annotated §§ 708-891;
  - 720 Illinois Compiled Statutes 5/16D-5;
  - Louisiana Revised Statutes 14:73.5;
  - North Dakota Century Code 12.1-06.1-08;
  - South Dakota Codified Laws § 37-24-36;
  - Virginia Code Annotated § 18.2-152.3;
  - West Virginia Code § 61-3C-4

Although Congress has yet to pass a federal spyware bill, the use of botnets is also governed by numerous state spyware statutes, including Washington's Computer Spyware statute (R.C.W. Ch. 19.270), and California's Consumer Protection Against Computer Spyware Act ("CPACSA")

The following recent enforcement actions reflect the criminal nature of botmaster activity:

Los Angeles Bot Master Pleads Guilty. A California man agreed to plead guilty to infecting as many as 250,000 personal computers with software used to steal user names and passwords for EBay Inc.'s PayPal online payment service. John Schiefer, 26, of Los Angeles will admit to four felony counts, including accessing protected computers to conduct fraud, according to a statement by the U.S. attorney's office in Los Angeles. He faces as much as 60 years in prison and a fine of \$1.75 million, according to the statement.<sup>9</sup>

FBI's Operation Bot Roast Nets Three. According to its June 2007 announcement,<sup>10</sup> the FBI's "Operation Bot Roast" identified over 1 million compromised computers, and resulted in the charging or arrest of three individuals:

---

<sup>9</sup> "Los Angeles botmaster pleads guilty, faces 60 years in prison, \$1.75 million fine," Frank Washkuch, Jr., *SC Magazine*, November 12, 2007.

<sup>10</sup> June 2007 announcement. FBI Press Release, June 13, 2007, at <http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm>

- James C. Brewer of Arlington, Texas, is alleged to have operated a botnet that infected Chicago area hospitals. This botnet infected tens of thousands of computers worldwide.
- Jason Michael Downey of Covington, Kentucky, was charged with using botnets to send a high volume of traffic to intended recipients to cause damage by impairing the availability of such systems. He was sentenced to a year in prison, three years of supervised release and more than \$21,000 in restitution for running a botnet of up to 6,000 infected PCs.
- Robert Alan Soloway of Seattle, Washington, is alleged to have used a large botnet network and spammed tens of millions of unsolicited email messages to advertise his website from which he offered services and products.

Botmaster Sentenced to 57 Months. Jeanson James Ancheta was sentenced to 57 months in prison in 2006 for creating a zombie network of hundreds of thousands of PCs that he rented out to hackers to send spam campaigns and launch DoS attacks. He was also ordered to pay \$15,000 to the military organizations whose computers were hit by his attacks. According to prosecutors, some of the computers attacked were at the Weapons Division of the U.S. Naval Air Warfare Center in China Lake, Calif., and at the U.S. Department of Defense.<sup>11</sup>

California Arrest of Botmaster. In October, 2007, a California man was arrested for allegedly attacking organizations, including the anti-phishing community CastleCops, with botnets. Greg King, 21, of Fairfield, was been charged with four counts of electronic transmission of codes to cause damage to protected computers, according to U.S. Attorney McGregor Scott of the Eastern District of California. King, allegedly controlled more than 7,000 servers as part of his botnet, and faces a maximum sentence of 10 years in prison and a \$250,000 fine.<sup>12</sup>

### **ABUSE OF SOCIAL NETWORKING SITES**

The rise and enormous popularity of social networking sites has made them an attractive target for Internet villains. MySpace alone has more than 200 million subscribers, and is one of the Internet's most popular sites. Sixty one percent of teenagers 13 to 17 have a personal profile on sites such as MySpace, Friendster, or Xanga.<sup>13</sup>

---

<sup>11</sup> "Botmaster Ancheta gets 57 months in jail," by Rene Milman, SC Magazine, May 9, 2006.

<sup>12</sup> "Man Arrested For Using Botnet To Launch DoS Attacks," by Sharon Gaudin, InformationWeek, October 4, 2007.

<sup>13</sup> National Center for Missing and Exploited Children, May 2006 Press Release, quoted at <http://blogs.zdnet.com/ITFacts/?p=10900>

Abuse of social networking services ranges across the spectrum. Because they provide a platform that combines communications functions with the revelation of personal information, these new services may be abused to inflict personal harm or to conduct cyberbullying.<sup>14</sup>

Social networking sites also contain a vast pool of consumers who are prime targets for commercial advertisements. Legitimate advertisers have recognized this market -- social network ad spending in the U.S. is predicted to be \$875 million in 2007, with potential to reach \$2 billion by 2010.<sup>15</sup> It is no wonder that Internet peddlers of mortgages, pharmaceuticals and porn have scrambled to get in on the action.

The social networking sites not only provide a captive audience of hundreds of millions of potential buyers, but they also provide robust and free delivery mechanisms. Each of the social networking services connects its member through internal communications systems, whether bulletin board posts, groups, email, IM, or mobile phone deliveries. By getting access to these systems, spammers and scammers can distribute their promotions at negligible cost.

As reflected in the cases described below, spammers have been quick to blast social networking subscribers with their offerings. Although network administrators are on constant watch, abusers create multiple profiles and use those profiles to either generate traffic or to post links that will take a visitor to sites that will secretly download adware and spyware.<sup>16</sup>

Similarly, because of their vast customer base, social networking sites have become a favorite target for phishing. Not surprisingly, because the sites are primarily social and teenage subscribers are not likely to have valuable financial information, phishing in the social networking space is generally not geared directly to obtaining banking or other financial records. Rather, phishers attempt get passwords for account access in order to use the account to promote their products.

In a recent attack, phishers circulated emails and postings to the “friends” of compromised accounts, enticing the recipients with a Macy’s gift card offer. Upon opening the offer, the recipient was redirected to a phony login page, at which the phishers collected MySpace login credentials.<sup>17</sup> Similarly, Internet watchers have reported phishing at Facebook, Friendster and Orkut. The social nature of the networking sites makes it easy to imbue phishing messages with a sense of trust;

---

<sup>14</sup> See, e.g., “States Fault My Space on Predator Issues,” by Brad Stone, *New York Times*, May 15, 2007; “Mom: MySpace Hoax Led to Daughter’s Suicide,” *FoxNews.com*, November 16, 2007.

<sup>15</sup> “Social network ad spending in the US could top \$2 billion by 2010”, by Steve O’Hear, November 2, 2007, <http://blogs.zdnet.com/social/?p=8>

<sup>16</sup> “Social-networking sites a ‘hotbed’ for spyware,” by Aric Hesseldahl, *MSNBC*, August 18, 2006. <http://www.msnbc.msn.com/id/14413906/>

<sup>17</sup> “MySpace Overcome By Severe Phishing ‘Epidemic’,” by Steve Fink, *WCBSTV.COM* Nov 9, 2007

according to an Indiana University study, 72% of individuals who received phishing messages spoofed to come from their social network acquaintances were fooled. In contrast, only 15% of the recipients were fooled when the messages came from an unknown party.

According to an interview with an anonymous phisher,<sup>18</sup> the basic phishing operation begins with the creation of a credible fake login site that resembles the login page of the network. That phishing site is used to capture the logon credentials of users, which is then transmitted to the phisher. The phisher then uses the captured contact information or the compromised accounts to send advertising, profiting from commissions on sales.

The phisher may also access a victim's email, Paypal and eBay accounts using captured logon credentials, relying on the fact that many people use the same credentials on multiple sites.

The social networking sites are fighting back, with some success.

MySpace Inc. v. TheGlobe.com Inc., (No. CV 06-3391, C.D.Cal.) On February 28, 2007, the court granted summary judgment in favor of MySpace on several of its claims against the defendant. The lawsuit, which was filed by June 2006, contended that The Globe had violated California and federal law by sending 400,000 unsolicited email messages to MySpace users, in violation of the CAN-SPAM Act and the California Business & Professions Code Section 17529.5. The Court held that "e-messages" sent between MySpace.com account holders qualify as e-mail under state and federal anti-spam statutes, and that MySpace.com was an "Internet access provider" eligible to invoke the CAN-SPAM Act's civil remedies. The Court also ruled that the terms of service, which called for liquidated damages of \$50 per unauthorized commercial e-message to MySpace users, were enforceable.

Facebook Inc. v. ConnectU LLC (No. 07-01389, N.D. Cal. (2007)). Facebook sued competitor social networking site for harvesting email addresses. The Court held that harvesting e-mail addresses from a social networking site likely violates provisions of California Penal Code section 502 and may constitute misappropriation.

MySpace, Inc. v. Optinrealbig.com and Scott Richter, (No 07-0496GHK, C.D.Cal.). MySpace alleges that between July and December 2006, Richter and his associates arranged for millions of spam "bulletins" to be sent from MySpace users' accounts without their knowledge.<sup>19</sup> According to the lawsuit, Richter either phished MySpace accounts himself or acquired a list of phished accounts to launch spam campaigns. The campaigns promote websites offering products and services such as ringtones and polo shirts, according to MySpace's filing. Motion to compel arbitration granted August 13, 2007.

---

<sup>18</sup> Phishing Social Network Sites, <http://ha.ckers.org/blog/20070508/phishing-social-networking-sites/>

<sup>19</sup> "MySpace sues 'Spam King' Richter," by Caroline McCarthy, *CNET News.com*, January 22, 2007.

## AD BASED REVENUE PRODUCTS AND SERVICES

More than ever, advertising revenue is driving the Internet. Internet advertising in the U.S. was approximately \$10 billion during the first half of 2007,<sup>20</sup> and third quarter results were up 25% over the same period last year.<sup>21</sup> Online businesses have come to recognize advertisement spending as their principal revenue source.

Fueled by pay-per-click advertising, Internet sites can now offer powerful and free services to their customers. ESPN.com, Yahoo! email, and Google's search engine all have one commonality – they provide free services supported by ad revenue. Indeed, the extent of ad-supported free offerings is quite remarkable – Microsoft's Office Live Service will provide registrants with a free domain name, free hosting, free email accounts and free software use. From bloggers generating revenue from Google AdSense to sophisticated entertainment sites such as YouTube, entrepreneurs are creating innovative online businesses that are funded by advertising revenue. Underlying this model is a simple value proposition – an entity will provide free or subsidized content or services in exchange for the customer's willingness to see ads.

With so much money in play, it is not surprising that individuals and businesses devote a great deal of attention to how to illicitly capitalize on this growing section of the economy. Yet to the extent they enrich themselves, they destroy the value proposition that underlies this segment of the industry.

One familiar example of illicit behavior is “click fraud.” Given that enormous revenues are generated through pay-per-click advertising, it is obvious and predictable that scammers would create methods of generating clicks to maximize commissions. Click fraud can be as simple as one person creating a webpage, becoming an ad network affiliate, and clicking on those ads to generate commissions. On a much larger scale, the use of scripts and botnets can magnify the fraud. Some estimates assert that by 2008, click fraud will cost online advertisers \$1.6 billion, and waste up to 70% of advertising budgets.<sup>22</sup> Both Yahoo! and Google have settled lawsuits relating to click fraud on their advertising networks.

Another interesting development is “stealware.” Stealware is software that modifies affiliate tracking codes or replaces affiliate cookies on a user's computer - resulting in a hijacking of advertising commissions going to another person or company. Most affiliate programs credit commissions based on the affiliate software interpreting cookies on the users' computer. Cookies include information such as login information, user preferences, shopping cart sessions and referral information such as an affiliate ID.

Stealware overwrites these cookies and other affiliate tracking data with data of its own. Thus, advertising commissions properly destined for an advertising partner are

---

<sup>20</sup> IAB Internet Advertising Revenue Report (2007)

<sup>21</sup> IAB Press Release, November 12, 2007

<sup>22</sup> Clickfraud.com, November 21, 2007

redirected to the company controlling the stealware. Stealware can also engage in "cookie stuffing," placing hundreds of cookies of other merchants' affiliate programs on a user's computer. If that user then visits those sites and makes a purchase, the stealware-powered affiliate receives the commissions.

Other examples of undercutting the ad revenue value proposition are much more subtle and perhaps more sophisticated. Adware, for example, may undercut the fundamental ad-driven revenue model by siphoning off ad revenues from their intended destination. For example, some adware replaces website banner ads with ads of its own, thereby depriving the website content provider of the revenue necessary to continue providing that content. Other adware may analyze a user's search engine request, displaying pop-up ads of its own rather than the advertised links that pay for the search engine's operation.

Recent case law demonstrates that courts appear to be willing to protect the ad revenue value proposition, in part by enforcing the Terms of Use under which subscribers agree to accept free content.

A September 2007 decision in *Southwest Airlines Co. v. BoardFirst LLC*, (No. 3:06cv0891, N.D. Tex., 9/12/07) pointedly supported Southwest's right to control the manner in which its customers interacted with its website and advertising. After Southwest implemented a policy allowing online access for priority seating, defendant BoardFirst built its business around charging Southwest travelers \$5 to conduct the login and obtain the seating on their behalf. Although BoardFirst was acting with the traveler's express permission, it was violating provisions of Southwest's Terms of Use, including a provision that prohibited use of the website for commercial purposes. The Court embraced Southwest's argument that BoardFirst's access to the Southwest site necessarily diverted visits by the travelers themselves, and thereby deprived Southwest of "valuable selling and advertising opportunities," such as the ability to sell more tickets or to cross-sell hotel and car reservations.

Similarly, the October 16, 2007 decision in *Ticketmaster v. RMG Technologies* (CV07-2534ABC, C.D. Cal. ), affirmed Ticketmaster's right to control access to its site based on its Terms of Use. In that instance, defendant had created an application that permitted users to make thousands of automated ticket requests, thereby circumventing Ticketmaster's control systems and allegedly preventing ordinary consumers from obtaining tickets to events. After examining whether defendant's system were "automatic devices" prohibited by Ticketmaster's Terms of Use, the court issued a preliminary injunction enjoining the use of defendant's application.

## IDENTIFYING THE THREATS TO DEVELOPING PRODUCTS AND SERVICES GLOSSARY

**Spyware:** software installed without the user's informed consent that is used to collect and transmit information about the user or the user's computer use. Spyware can be designed for many nefarious purposes, including collecting a user's keystrokes, examining a user's Internet search pattern, and searching a user's hard drive for data.

**Adware:** software installed on a user's computer (either with or without informed consent) that plays, displays, or downloads advertising material. Because it can identify and respond to a user's search inquiry or computer use, the advertising that is displayed is often referred to as "contextual advertising."

**Drive-by download:** a download of software – often spyware, a computer virus or other malware – that occurs without the user's knowledge. Drive-by downloads may happen by visiting a website, viewing an e-mail message or by clicking on a deceptive popup window.

**Botnet:** a network or army of robots, or "bots," which are controlled remotely as a group. After becoming infected with botnet malware, compromised computers (or "zombies") report back to a command-and-control server, through which their instructor ("bot-herder" or "bot-master") provides instructions.

**Phishing:** an attempt to acquire personal or financial information, such as passwords, credit card numbers or banking information, by impersonating a legitimate and trustworthy entity, or by other means of social engineering.

**Spear phishing:** a phishing attempt that targets a particular organization or group, usually impersonating a trustworthy member of that organization or group. For example, spear phishers may impersonate the IT group or HR department of a particular agency or company.

**Vishing:** "Voice Phishing" or "vishing" is the practice of using telephone services as part of a phishing scheme. Recognizing the public's growing skepticism about providing information online and a historical trust in landline telephone services, phishers incorporate telephone calls or responses into their scheme, often using Voice over IP (VoIP) telephony.

**Smishing:** Phishing using SMS (short message service) to send messages to mobile phones. SMS messages may include URL links to phishing websites, email addresses or other malware.

**Pharming:** or "DNS poisoning" is a technological means of providing falsified DNS results to redirect traffic destined for legitimate websites. The falsified DNS result, akin to a false phonebook entry, unwittingly lead a user's computer to a malicious website of the hacker's choosing.