Financial Coalition Against Child Pornography Report on Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography

February 1, 2011

Table of Contents

Acknowledgments

The Financial Coalition Against Child Pornography wishes to thank the following organizations and individuals for their contributions to this paper: Heather Accardi of American Express, Eric Olson of Cyveillance, and Melissa Hsieh Nikolic and Cory Louie of Google.

Disclaimer

This report ("Report") was created and written by volunteers on behalf of the Financial Coalition Against Child Pornography (FCACP) and represents the current views of the issues addressed as of the date of publication. The content of the Report is based on the individual input of the contributors, and does not necessarily reflect the opinions or policies of the companies at which the individuals work, nor of any of the FCACP member companies. There may be inaccuracies or information that has become outdated since this Report was originally written.

This Report is for reference only and does not purport to provide specific legal, financial, or business advice. If you require specific advice or counsel, you should consult with a proper professional. **THE FCACP MAKES NO WARRANTIES, EXPRESSED, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS REPORT.** The listing of an organization or entity herein does not imply any sort of endorsement by such organization or entity.

INTRODUCTION

The Financial Coalition Against Child Pornography (FCACP) was formed in 2006 to address the alarming growth of commercial child pornography over the Internet. Its members include leaders in the banking and payment industries, as well as Internet services companies. The FCACP is managed by the National Center for Missing & Exploited Children (NCMEC) and its sister organization, the International Centre for Missing & Exploited Children (ICMEC).[1]

The Internet has enabled instant access to child pornography by thousands and possibly millions of individuals around the world. Consumers are able to use traditional payment tools, such as credit cards, as well as new, alternative payment schemes, to purchase child pornography on the Internet. The mission of the FCACP is to follow the flow of funds and shut down the payments accounts used by these illicit enterprises. The situation with commercial child pornography has changed dramatically since the FCACP became operational in 2006. As one example, there has been a 50% drop in the number of unique commercial child pornography websites reported into the U.S. CyberTipline, a hotline operated by NCMEC. The FCACP views this as a very encouraging sign, even as it works to expand around the world.[2]

But even with these positive trends, the FCACP recognizes that these criminal enterprises are likely to evolve and flourish without sustained pressure from law enforcement and the private sector. Consequently, the FCACP endeavored to collect a brief summary of some of the most current research on trends related to online crime in order to apply those learnings to how the mechanics of commercial child pornography may be evolving.

This report on *Trends in Online Crime and Their Potential Implications in the Fight Against Commercial Child Pornography* ("Report") is divided into three sections:

1. **Online Financial Crimes**, which helps to illustrate means and methods to obtain data and assets illegally to support the child pornography industry.

2. **Social Media**, which highlights some of the risks associated with social media and illustrates how social media can provide the means and methods of potential child pornography industry recruitment of both victims and consumers.

3. **Technical Issues**, which illustrates the means and methods of concealing the origin and real identity of those seeking to exploit children through child pornography.

The intent of this Report is to highlight emerging trends in cybercrime/cybersecurity and to evoke thought and discussion about their potential impact on the child safety arena. Each section delves into examples of activities that have garnered the attention of the researchers and professionals working to combat cybercrime.

[1] A full backgrounder on the FCACP can be found at: http://icmec.org/en_X1/pdf/FCACP_Backgrounder__FINAL_.pdf.

[2] There are active coalitions in Europe and the Asia-Pacific region. For more information, please visit: http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=4355.

Online Financial Crimes

Alternative Payment Systems

The online financial landscape has evolved dramatically with ever-more alternative payment options offering increased privacy, speed, mobility, and anonymity for transactions executed over the Internet. Unfortunately, there is a dramatic downside to this increase in choice, speed, and convenience. With new, small, offshore, and/or unknown parties behind these payment systems, security practices, business ethics, and regulatory oversight of these systems vary widely. As a result, the volume of stolen identities, fraudulent transactions, and pilfered financial and personal information has made financial fraud a reality in the world of e-commerce and on many popular online marketplaces.

For example, credit card crimes continue to rise sharply, but alternative payments – including new Internet, mobile, peer-to-peer (P2P), and other payment methods – represent a troubling new source of losses for large merchants. Fraudsters are actively using non-traditional payment methods, with 29% of large retailers reporting an increase in alternative payments fraud during 2008.[3] As alternative payments increase in popularity with merchants and consumers, it is likely criminals will quickly leverage them as well.

Implications for Commercial Child Pornography and Online Child Safety

As law enforcement and public-private partnerships like the FCACP have disrupted the use of traditional payment forms, such as credit cards, by commercial child pornography enterprises, new and alternative forms of payment offer benefits that the child pornography industry and its customers have been quick to realize.

First, given the basing of many such enterprises in countries with limited legal or regulatory oversight of payment systems, it can be difficult to shut down, investigate, or, in some cases, even successfully contact the operators of these alternative payment systems. These systems also offer increased anonymity for both purchasers and purveyors of illegal content in that many require little or no information about either buyers or sellers utilizing the system. Unlike more established payment systems and services, these outfits are often willing to facilitate payments between parties with no record of, or interest in, *any* information about the parties' identities, legitimacy, or legality. As such, the emerging payment systems offer an appealing transaction option for illicit goods and services, including child sexual abuse images.

Identity Fraud

Based on the *2009 LexisNexis True Cost of Fraud Study,* 1 in 5 merchants experienced an increase in unauthorized transactions associated with identity fraud, which is attributed to depressed economic conditions and increased criminal sophistication in criminal fraud methods.[4]

The *Lexis Nexis Study* also describes the industry sectors that are impacted by identify fraud. Specifically,

[3] LexisNexis, *2009 LexisNexis True Cost of Fraud Study*, research conducted by Javelin Strategy & Research, 11 (on file with the International Centre for Missing & Exploited Children) [hereinafter *LexisNexis Study*].

[4] *Id.* at 24-25.

industry segments with high levels of card-not-present transactions experience a higher prevalence of related fraud.[5] The computer/electronics industry continues to be targeted for fraudulent purchases due to high-value goods with many merchants selling these products online.[6] However, the hotel/travel industry has seen the greatest increase in fraudulent transactions, as the majority of travel arrangements are now being conducted online.[7] Telecommunications fraud has also become an increasing problem, with criminals creating fraudulent new accounts and illegally accessing telecommunications services.[8]

In 2008, 44% of merchants in the online gaming industry reported an increase in fraudulent transactions, and 33% of merchants in the social networking space reported rising identity fraud.[9]

Implications for Commercial Child Pornography and Online Child Safety

Stolen information, including personal credentials and payment details, can be used in a number of ways related to commercial child pornography and threats to online child safety. First, the FCACP has for several years noted an increasing sophistication on the part of child pornography purveyors with regard to screening buyers. An ever increasing number of technical hurdles, including offline (e.g., SMS message) purchase validation and leveraging legitimate website affiliate programs to mask child pornography purchases, have been put in place most likely to flag undercover law enforcement credit card transactions.

As a result, a "legitimate" online identity, account information, and persona are increasingly needed to successfully capture evidence against an online purveyor of child sexual abuse images. Thus, the clean PCs, virtual machines, test credit card accounts, and other tools formerly used by investigators are increasingly ineffective because the child pornography peddlers can recognize a "fake identity."

Meanwhile, child pornography consumers, some of whom may well have few qualms about committing other criminal acts to cover their tracks and protect themselves from discovery, can steal or purchase a real identity and clear the technical hurdles encountered by law enforcement. Put another way, the child pornography peddlers have found a new range of ways to stop the "good guys" from tracking them down, but the "bad guys" have a new avenue to not only purchase the contraband material but also to further obscure their tracks while doing it.

Worst of all, in the event that a later investigation manages to secure the records of those transactions, law enforcement might very well then pursue, arrest, or attempt to prosecute an entirely innocent party whose PC, credit card, or account might have been involved in a child pornography purchase, of which the actual individual is both innocent and genuinely ignorant.

In still another angle on the same issue, it has been reported by law enforcement and others in the Internet security industry that sites purporting to sell child pornography are in fact using existing content as a "lure." The interested consumer may then be convinced to reveal personally identifiable information, such as credit card data, addresses, etc., even though the site operator has no intention of providing any goods or data in return. The site is a pure fake, set up solely to harvest financial and identity data, which can then be sold on the black market or used to make other illicit purchases.

[5] *Id.* at 35.
[6] *Id.*
[7] *Id.* at 38.
[8] *Id.*
[9] *Id.* at 25.

DIGITAL CURRENCY AND VIRTUAL WORLDS

In many online "virtual worlds," digital currency or electronic money has outpaced traditional currency and become the accepted payment norm. Benefits of using a digital currency include the convenience, privacy, and efficiency of Internet-based real-time transactions.

The most common application of digital currency is an Electronic Funds Transfer (EFT) involving bank accounts. "Real" money is exchanged for digital currency and added to the account balance of a digital stored value system.

Many systems will sell currency directly to the end user, thus allowing P2P transactions using digital currency. Other systems only sell currency through digital currency exchangers that apply either a commission or bid/offer spread to transactions. This method offers another layer of privacy and anonymity in a transaction.

As obscure as this may seem to many, there are entirely virtual, and privately controlled, economies, such as Second Life and World of Warcraft, whose currencies have staggering "real dollar" value and are traded on exchanges for legitimate currency. According to Linden Labs, the creator and operator of the Second Life virtual world, in 2009 more than $100 million U.S. Dollars were exchanged on the official Linden currency exchange and user-to-user transactions exceeded half a *billion* U.S. Dollars.[10]

Implications for Commercial Child Pornography and Online Child Safety

While digital currency in and of itself is not necessarily illicit, it can be used for illicit purposes. The speed, scale, and anonymity of these economies are extreme, and they provide a nearly opaque medium for exchanging value between any two parties for any reason. Moreover, they often present legislative, regulatory, and financial quandaries that oversight and law-enforcement bodies may be ill-equipped to address or, in some cases, even determine what jurisdiction, if any, can be applied to a world that exists only inside a computer's memory.

Given that these are privately-operated worlds, tracing the sender or receiver of digital currency transactions, by law enforcement for example, poses many difficulties due to the lack of account or transaction records, the lack of jurisdiction or authority over many transactions, and the difficulty of even knowing how to recognize suspect money flows or actors. Layering transactions across multiple digital currencies and systems compounds the complexity of following the money trail. As such, virtual worlds represent a promising environment for money laundering, paying for contraband such as child pornography and/or any other illicit good or act.

PREPAID CARDS

Certain types of stored value cards may pose challenges as the cards themselves have value that may not be linked to a separate, individualized, external account. Common examples include transit system cards or prepaid telephone cards. If the cards have the ability to be reloaded, they may present a vulnerability

[10] T. Linden, *2009 End of Year Second Life Economy Wrap Up (including Q4 Economy in Detail), at* http://blogs.secondlife.com/community/features/blog/2010/01/19/2009-end-of-year-second-life-economy-wrap-up-including-q4-economy-in-detail (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

that criminals can exploit to launder illicit proceeds from transactions such as the sale of child pornography.

There are two primary types of prepaid cards used today: open system and closed system with varying degrees of anonymity, depending on the ability to reload the cards. Closed system prepaid gift cards are generally only accepted at a single merchant and are completely anonymous with no identification required to purchase. Semi-closed systems allow cards that can be used at a limited number of merchant locations (e.g., within a specified geographic area) and may be issued by a third party. One example is a shopping mall card that can be used at all participating stores within that mall.

Open system prepaid cards link to a database where the balance is recorded. These are also known as network-branded, prepaid credit cards, or prepaid debit cards. These cards are issued by the payment networks, such as American Express, Discover, MasterCard, and Visa, and can be used anywhere the payment network cards are accepted.[11] These cards may be issued as reloadable cards, which generally require customer identification, or as non-reloadable cards, which generally do not require customer identification. These types of cards are generally funded through pooled accounts.

A hybrid example is the payroll card where the employee is issued a card to access a separate account set up by the employer. The employer deposits the employee's wages directly into the account where the employee can access the funds. The employee can also withdraw the funds at an ATM or use the card at stores for purchases. Payroll cards are not anonymous because identifying information about the purchaser/user is captured to some extent, as is generally the case with other general purpose reloadable prepaid products.

Implications for Commercial Child Pornography and Online Child Safety

Based on a 2006 study,[12] Stored Value Cards are attractive to criminals as they are loosely regulated, function as remittance cards, and may provide anonymity. "Prepaid stored value cards are, in many ways, superior to established methods of money laundering and money movement – specifically, the use of money transmitters and bulk cash smuggling – and may replace these methods under certain conditions."[13] Of course, in recent years, prepaid cards have become more regulated.

Any payment option that offers a level of anonymity is an attractive option for sellers and purchasers of commercial child pornography; however, only certain prepaid products do offer anonymity.

MOBILE PAYMENTS

The rise of mobile payments presents lucrative opportunities for financial and identity theft. Many users view their phones simply as a communication device, and fail to consider the wealth of personal information that the phone holds. At least 79% of consumers are using unprotected mobile phones, while

[11] Federal Reserve Bank of New York, *Stored Value Card: An Alternative for the Unbanked?, at* http://www.newyorkfed.org/regional/stored_value_cards.html (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[12] U.S. Department of Justice National Drug Intelligence Center, *Assessment: Prepaid Stored Value Cards: A Potential Alternative to Traditional Money Laundering Methods*, Product No. 2006-R0803-001 (Oct. 31, 2006) (on file with the International Centre for Missing & Exploited Children).

[13] *Id*. at 1.

15% are unsure of their security levels.[14] The prevailing consumer attitude and accessibility of information allow criminals to execute easier attacks on a broader, less sophisticated audience.

In 2008, more than 10% of large merchants saw an increase in mobile payments fraud.[15] At the time of the *LexisNexis Study*, 3% of all merchants accepted mobile payment methods, while payments via mobile phone were accepted by more than 20% of large e-commerce merchants.[16] Illicit activity gains for mobile payments and mobile devices will emerge quickly as the growth of mobile access outpaces established methods.

Implications for Commercial Child Pornography and Online Child Safety

Mobile payments do provide somewhat more "traceability" than some alternative payment methods due to the records that cellular carriers assemble on the purchasers of handsets and service plans. However, these devices are still a potential boon to sellers and buyers of child pornography. The increasingly disposable nature of the handsets and service contracts mean that mobile devices can be used for illicit acts and payments. Increasingly, some of the most powerful "smart phones" can actually be configured to act as web servers, making those same devices a potential host for the illicit content and payment processing, and which literally can be dropped in the nearest river or trash bin at any time to stymie investigative efforts.

[14] Jennifer Hill, *Mobile Phone Payments "Pose Huge Fraud Risk,"* Reuters (May 19, 2008), *at* http://uk.reuters.com/article/idUKNOA94822420080519 (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[15] *LexisNexis Study, supra* note 3, at 27.

[16] *Id.*

Social Media

Social Networks

Social networks have brought together "trusted communities" that transcend geographic and sociologic gaps. Users self-select their contacts and "friends" to share anything from geotagged pictures to innermost thoughts. These websites and services aggregate large amounts of verified information that can be quickly harvested.

Traditional methods of phishing, impersonation, and 419 scams[17] continue to be popular schemes seen by these social communities. The richness of personal details available can result in victimization for identity theft purposes.

Easy access to personal information, either real or fake, has greatly accelerated the ability to find like-minded individuals. While the primary intent is to connect with others, some users may be doing so for malicious purposes such as finding victims or fellow predators. Social networks are also largely unregulated, especially as many services operate outside the United States.

Implications for Commercial Child Pornography and Online Child Safety

With today's technology, people can connect and disseminate information with more speed and anonymity than ever before. Entire personas can be created and maintained online, completely disconnected from the real world.

This has several implications for both the trading of child sexual abuse images online and the broader victimization of children by leveraging the Internet and social networks in particular. First, the wealth of personal information revealed on social networks (especially by the young, and possibly more naïve, users) is fertile potential stalking ground for child predators and abusers.

Second, it is easy to construct a rich, complete, and completely fictitious online persona for illicit purposes, whether offering child pornography or enticing young users into dangerous online and real-world circumstances. This was recently demonstrated quite powerfully in the national-security space by the so-called "Robin Sage" experiment,[18] in which a security researcher created a fictitious intelligence analyst working at a U.S. government agency. Simply by using a copied photo of an attractive young woman, this entirely imaginary person successfully networked with hundreds of military personnel, intelligence officers, journalists, and business people, many of whom revealed highly sensitive information.

Social network users can rely on a "created" persona and digital avatars that need not correspond to anything real. This ephemeral entity can be used for interactions, messages, pictures, videos, currency, gifts, and more – all exchanged quickly without exposing one's real-life identity. In the event of criminal

[17] Additional information on 419 scams is available online at http://www.fbi.gov/scams-safety/fraud/fraud (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[18] Additional information on the "Robin Sage" experiment is available online at http://science.dodlive.mil/2010/07/21/the-dangers-of-friending-strangers-the-robin-sage-experiment/ (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

acts, these layers of anonymity can complicate or even totally eliminate the ability to identify the actual perpetrator.

URL SHORTENERS

Services with character limits including Short Message Service (SMS) and microblogs inadvertently encourage the use of URL shorteners.

With the increased popularity of communication media with character limits, the emerging technology of URL shorteners has fulfilled a real need. URL shortener services concatenate lengthy URLs by redirecting users to the desired link and inadvertently hiding the original URL.

While this technology greatly reduces the character count of a URL, it is also used maliciously to mask harmful links. Because of their prevalence in accepted forms of communication, suspicion has been lowered for shortened and hidden URLs. Popular URL shortener services include "tinyurl.com" and "bit.ly," for which the latter reported 4.2 billion hits on its services alone for May 2010.[19]

Scammers have also leveraged the popularity of URL shorteners. "They intentionally shorten URLs to trick users into clicking them to further their profiteering activities. In [one] particular attack, the URL redirected a user to http://www.{BLOCKED}ryeasy.com where a rogue registry cleaner[[20]] can be downloaded."[21]

Many companies are now providing their own URL shorteners, some of which check for malicious content as an added layer of safety.

Implications for Commercial Child Pornography and Online Child Safety

These URL shortening redirect services have powerful potential for purveyors of child sexual abuse images. As Internet users become more and more accustomed to seeing hyperlinks of which they cannot see the destination until *after* they have clicked them, it is easier to distribute links to child pornography under almost any pretext (e.g., click here to win a prize, download a cool game, see a neat video, etc.). While it might seem overly brazen to simply "spam" the user base with a mislabeled link, it is a "numbers game." Spammers will blast out links to everything from child pornography to bestiality, knowing that for every one million disgusted, repulsed viewers, they may gain a few paying customers. The simple economics of such a tactic make it worthwhile for criminal enterprises.

[19] Beth Snyder Bulik, *URL Shorteners in High Demand with Revenue as Low Priority*, Advertising Age (May 31, 2010), *at* http://adage.com/digital/article?article_id=144153 (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[20] "Registry Cleaners are software utilities that attempt to remove configuration data from the Windows Registry that is no longer in use or that is unwanted on the system. Such data may include information left by software that has not been uninstalled completely from the computer, information that is no longer of use, or settings required for the operation of malware. A registry cleaner scans the registry, and attempts to pick out the unnecessary values in order to delete or repair them." Wikipedia Contributors, *Registry Cleaners*, Wikipedia: The Free Encyclopedia, *at* http://en.wikipedia.org/wiki/Registry_cleaner (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[21] Trend Micro, *Security Spotlight: Spambot Sends Automated Tweets* (Sept. 7, 2009), 2 (on file with the International Centre for Missing & Exploited Children).

MICROBLOG SPAM

Microblogging is a variation on blogging in which users write short posts to a special blog that are subsequently distributed to their friends and other observers via text messaging, instant messaging systems, and email.[22]

The popularity of microblogging has grown dramatically with the launch of new services, web-connected mobile devices, and the social model. Top-followed microblogs are oftentimes representing high-profile individuals and news services, with followers numbering in the 3+ million each.[23] (Even heavily connected, lesser-known microbloggers can reach an audience of hundreds almost instantaneously. Microblogs can be used as a megaphone to blast messages to intended listeners but otherwise appear as daily noise to the bystander.)

Implications for Commercial Child Pornography and Online Child Safety

Coupled with URL shorteners as described above, microblogs are an environment susceptible to spam and malicious content. Similar to abuses of standard blogs, a user can theoretically post a message and shortened URL to an intended audience that then directs to an illicit website, then redirects or removes the URL after a short period of time. This effectively hides any suspicious behavior from risk of exposure.

[22] Akshay Java, Xiodan Song, Tim Finin, Belle Tseng, *Why We Twitter: Understanding Microblogging Usage and Communities* (2007), 1 (on file with the International Centre for Missing & Exploited Children).

[23] *See e.g.*, http://twitaholic.com/.

Technical Issues

As new technologies are introduced, methodologies to use them for the activities of the criminal underworld quickly emerge. The vulnerabilities and even advantages of each invention are typically exploited for financial or personal gain.

Older, reliable methods are not abandoned but rather made more sophisticated by cybercriminals. Examples of ongoing threats include malware, viruses, and botnets which are continually morphing to be even more resilient. Advances in hosting strategies and providers, as well as satellite Internet Service Providers (ISPs), have contributed to more anonymity and stability for each piece of the scam life cycle. Botnets[24] consist of compromised and zombie computers[25] that can span numerous ISPs and countries, which can result in extensive criminal networks that are difficult to trace and take down.

Another key entry point to successful attacks is social engineering. By exploiting the human as the weakest link in the security chain, successfully "spear-phishing" and "whaling" attacks on known or high interest individuals have increased. After access has been gained, technical methods of attack can be used to carry out Advanced Persistent Threats[26] (APTs). APTs generally refer to targeted attacks on business or political victims with specific and long-term goals. They are carried out over a period of time and rely on stealth and gradually increasing access to key systems.

Malware

Malware (malicious software) is designed to secretly access a computer system without the owner's informed consent.[27] The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. While the original intent of malware for unauthorized access to computers has not changed, there has been an increase in sophistication and prevalence.[28] The array of malware variants, distribution techniques and volume of infected machines has increased exponentially. The end goal for a majority of malware appears to be to generate financial gain, gather private information, or add machines to botnets.

[24] "A botnet is a collection of software agents, or robots, that run autonomously and automatically. The term is most commonly associated with [Internet Relay Chat] bots and more recently malicious software, but it can also refer to a network of computers using distributed computing software." Wikipedia Contributors, *Botnet*, Wikipedia: The Free Encyclopedia, *at* http://en.wikipedia.org/wiki/Botnet (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[25] "Zombie computers" are explained in the *Fast Flux Hosting* section below.

[26] "Advanced Persistent Threats (APTs) are a cybercrime category directed at business and political targets. APTs require a high degree of stealthiness over a prolonged duration of operation in order to be successful. The attack objectives therefore typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached." Damballa, *Advanced Persistent Threats*, *at* http://www.damballa.com/knowledge/advanced-persistent-threats.php (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[27] Wikipedia Contributors, *Malware*, Wikipedia: The Free Encyclopedia, *at* http://en.wikipedia.org/wiki/Malware (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[28] *Id*.

Blended malware threats are increasing, where harm to an infected user is maximized, often combining various characteristics to include keylogging, DNS hijacking,[29] and the use of trojan, rootkit, worm, virus, and spyware to steal login credentials and confidential data, as just a few examples.

The ability to download for free or for a fee (up to $1,000 U.S. Dollars) various types of exploit toolkits has made it easier for novice criminals to distribute malware and manage botnets through user-friendly control panels.

Malware has evolved from being distributed through executable files (.exe) in email attachments to other file types in email, such as pdf, jpg, xls, doc, and ppt. In addition, peer-to-peer, other filesharing methods, social networks, and the manipulation of trusted social relationships have emerged as effective malware distribution channels.

One infection method is through drive-by downloads of malware from websites either created to distribute payloads or placed on hacked sites. These websites are often indexed by the major search engines to appear in search results naturally or Search Engine Optimization (SEO) techniques are applied to increase ranking. Additionally the malware can be distributed through online advertising (also known as malvertising), links spammed through email and social networks, or through user comments on other social sites.

Another malware distribution model is fake anti-virus software, or scareware.[30] Users are socially engineered to execute a free scan of their machine and informed that, in order to clean their machine, they need to purchase and download a package, which is actually a rogue anti-virus program that infects their machine and steals their valuables, such as funds or personal details. Fake anti-virus software currently accounts for 15% of all malware detected on the web and these attacks account for 60% of the malware discovered on domains that include trending keywords.[31]

Many zero-day exploits[32]/malware are not detected by anti-virus programs as the malware authors and distributors also check current detection signatures and produce variants of current malware or new malware to remain undetected.

Implications for Commercial Child Pornography and Online Child Safety

Press reports, published security papers, and primary research done by one FCACP Supporter have all revealed direct evidence of a linkage between online child pornography and malware distribution. Awful as it is to most, child pornography presents a nearly ideal distribution "lure" for sites using exploits to install malware on user PCs. Often these users are willing to pay for the content they seek, meaning there is little social engineering required to get them to give up credit card and other information that other

[29] "DNS hijacking or DNS redirection is the practice of redirecting the resolution of Domain Name System (DNS) names to other DNS servers." Wikipedia Contributors, *DNS Hijacking*, Wikipedia: The Free Encyclopedia, *at* http://en.wikipedia.org/wiki/DNS_hijacking (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[30] *See generally* Microsoft Security, *Watch Out for Fake Virus Alerts, at* http://www.microsoft.com/security/antivirus/rogue.aspx (last visited Jan. 10, 2011) (on file with the International Centre for Missing & Exploited Children).

[31] Moheeb Abu Rajab, Lucas Ballard, Panayiotis Mavrommatis, Niels Provos, Xin Zhao, *The Nocebo Effect on the Web: An Analysis of Fake Anti-Virus Distribution* (2010), 1 (on file with the International Centre for Missing & Exploited Children).

[32] "A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack.." Information Security Magazine, *Zero-Day Exploit*, *at* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci955554,00.html (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

users might be suspicious of giving away. Those who are aware of the illegal nature of their interest and suspect that they've been victimized or their PC infected, are least likely to notify anyone or submit their PC to an outside party for service, out of fear it might reveal their nefarious activities.

FAST FLUX HOSTING

Fast Flux Hosting (FFH) can be defined as "the combination of peer-to-peer networking, distributed command and control, web-based load balancing and proxy redirection used to make malware networks more resistant to discovery and counter-measures."[33] Cybercriminals are users of these services because of their need to maintain a high level of anonymity and uptime.

The principles behind FFH, such as Round-Robin DNS and Content Distribution Networks, are employed by legitimate online businesses to maintain continuous website availability and to "distribute the load not only to multiple servers at a single location, but to also distribute these servers over the globe… By using the compromised machines as proxies to route an incoming request to another system (control node/"mothership"), an attacker can build a resilient, robust, one-hop overlay network."[34]

One of the key attributes of FFH is the use of compromised "zombie" machines to replicate the mechanics of load distribution and routing, thus making the actual scam or other malicious site harder to take down.[35] This technique is popular with particular botnets to hide phishing and malicious websites. It is believed that this activity will continue to grow as counter measures against traditional botnets are developed.

Implications for Commercial Child Pornography and Online Child Safety

FFH is a nearly ideal application for hosting child pornography. Why set up or lease dedicated servers to host illegal content when the use of botted nodes and rapidly fluxing Internet Protocol (IP) Addresses can make tracking down the criminal "server" an almost meaningless pursuit? Moreover, in the event that law enforcement were to "kick in the door," in all likelihood the door kicked in, and the PC found, would almost certainly belong to a user who had no idea their machine was involved in something illegal . Yet the user might have a difficult time convincing law enforcement officials or judges they were blameless when the "evidence" is right there on their computer.

Worse still, in the event such a legitimate defense was proven, it exonerates the innocent and thereby creates an entirely new obstacle for law enforcement officials in the pursuit of true criminals: the "my computer did it" defense.

BULLETPROOF HOSTING

The aptly named "Bulletproof Hosting" (BPH) is a method of website hosting with marked improvements for uptime and reliability. A host that provides these exclusive services "promises

[33] Wikipedia Contributors, *Fast Flux*, Wikipedia: The Free Encyclopedia, *at* http://en.wikipedia.org/wiki/Fast_flux (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[34] Thorsten Holz, Christian Gorecki, Konrad Pieck, Felix C. Freiling, *Measuring and Detecting Fast-Flux Service Networks* (2008), 1, 3 (on file with the International Centre for Missing & Exploited Children).

[35] Alper Caglayan, Mike Toothaker, Dan Drapaeau, Dustin Burke, Gerry Eaton, *Behavioral Analysis of Fast Flux Service Networks* (2009), 1 (on file with the International Centre for Missing & Exploited Children).

customers that their websites will not be taken down, regardless of complaints or content."[36] The rise of BPH will make it more difficult for websites with illicit content and activity to be shut down.

BP Hosts use a combination of distributed services to maintain uptime for their customers. Specific tactics they use include:

1. Registering the domain name with a registrar with relaxed enforcement. Depending on the location and enforcement policies, some registrars are used more heavily than others for illicit activities.

2. Sharing and shuffling IP Addresses to minimize downtime if particular IPs are shut down. This ensures "content remains up while being indifferent to the status of particular domains."[37] Instead of relying on one IP, BPH relies on multiple IPs that can keep the content up independent of specific IP shut downs. This methodology is similar to that used for FFH.

3. Using a standardized yet specific naming methodology for name servers (NS) to minimize service interruption. With a redundant infrastructure and IP shuffling, "a handful of illicit NSs can keep hundreds of scam domains operational."[38]

4. Soliciting business and communicating with customers using unmonitored, private media. BP Hosts frequently advertise their services on message boards frequented by their target customer base. From there, email, instant messaging, and other non-public options are used to further business dealings. This allows BPH services to remain largely underground and reduces exposure to enforcement entities.

5. Collecting payment using unregulated payment services to limit scrutiny and preserve anonymity. The use of small payment processors originating from outside the United States is popular due to lax regulatory environments and lessened cooperation with law enforcement agencies.

Implications for Commercial Child Pornography and Online Child Safety

Each methodology described can be used for legitimate purposes; however, when used in combination, they add layers of complexity to nefarious operations. The popularity of BPH will increase as standard hosting methods are more heavily regulated. The success of many phishing campaigns will continue to rely on website uptime, making BPH services invaluable.

[36] Nathaniel Markowitz, Jonathan Brown, Amanda Cummins, Erin Greathouse, Christopher Kanezo, David McIntire, Thomas Saly, Toby Taylor, Louis Ulrich, Desiree Williams, *Bullet Proof Hosting: A Theoretical Model*, Infosec Island (Apr. 23, 2010), *at* https://www.infosecisland.com/blogview/4487-Bullet-Proof-Hosting-A-Theoretical-Model.html (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[37] Nathaniel Markowitz, Jonathan Brown, Amanda Cummins, Erin Greathouse, Christopher Kanezo, David McIntire, Thomas Saly, Toby Taylor, Louis Ulrich, Desiree Williams, *Patterns of Use and Abuse with IP Addresses*, Infosec Island (Jul. 10, 2010), *at* https://www.infosecisland.com/blogview/5068-Patterns-of-Use-and-Abuse-with-IP-Addresses.html (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

[38] Nathaniel Markowitz, Jonathan Brown, Amanda Cummins, Erin Greathouse, Christopher Kanezo, David McIntire, Thomas Saly, Toby Taylor, Louis Ulrich, Desiree Williams, *Name Servers and DNS Infrastructure*, Infosec Island (Jul. 15, 2010), *at* https://www.infosecisland.com/blogview/5456-Name-Servers-and-DNS-Infrastructure.html (last visited Jan. 5, 2011) (on file with the International Centre for Missing & Exploited Children).

BOTNETS

Bot-compromised PCs and botnets will likely maintain and increase their current high volumes and malicious activity, since they offer a profitable area for malware developers. These botnets will continue to innovate the use of technologies such as FF and a range of communication channels, including social networks, encrypted communications, or peer-to-peer networks. These trends will continue to replace previous communication channels through IRC (Internet Relay Chat) and, to a lesser extent, of HTTP communications using plain text.

Botnets are the leading infrastructure for cybercriminals, used for actions from spamming to identity theft. Recent successes in shutting down botnets will force their controllers to switch to alternate, less vulnerable methods of command, including peer-to-peer setups.[39] Unfortunately, there currently is no scalable solution to clean affected machines, which results in a significant monetary loss to personal, professional, educational, and governmental networks.

There may be a trend toward a more distributed and resilient botnet infrastructure that relies much more on peer-to-peer technologies rather than on the centralized hosting model that is prevalent today.[40] By distributing botnets, cybercriminals successfully increase their anonymity and the overall stability of their networks.

Implications for Commercial Child Pornography and Online Child Safety

The availability of botnets has significant potential impact for the child pornography realm. Since a botnet is essentially a vast network of available machines that have been compromised and are open to receiving instructions or tasking, one opportunity is to convert the "botted" machines into Web servers. As noted in the section on *Fast Flux Hosting*, this would allow the child pornography advertiser, seller, or distributor using (or renting the services of) the botnet to constantly shift the machines and IP addresses on which the content is being hosted. By moving the content around machines (e.g., on a timed and automated basis, with the advertising or distribution auto-synched to those timed changes) or by changing the machine/IP to which a fixed domain name is delegated, botnets become a hosting method for illegal content that is nearly impossible to nail down. Not only can the hosting location for content, or the IP for a given rogue domain, shift as often as every few minutes, but the "guilty" machine is almost certainly the PC of a home or business user who has no idea the computer is being used for this illicit purpose. This raises the possibility of law enforcement tracking the content/hosting to an innocent party, and each effort that ends in such a botnet-caused dead-end sadly serves as a disincentive to pursue the next such effort.

[39] McAfee Labs, *2010 Threat Predictions*, 2 (on file with the International Centre for Missing & Exploited Children).

[40] *Id*. at 9.

Conclusion

The landscape of commercial child pornography has changed significantly due to the efforts of law enforcement, the FCACP, and similar private-sector groups.

Ernie Allen, the President and Chief Executive Officer of NCMEC and ICMEC, and FCACP Chairman, recently commented, "The share of commercial child pornography that is on the Internet is substantially smaller than it was just a few years ago. This Coalition has had an enormous impact on the problem, but we are not ready to declare victory."

While the general trends are encouraging, this Report illustrates how the mechanics of commercial child pornography may be evolving. It is for this reason that the FCACP is attempting to stay ahead of this process and is reaching out to additional industry sectors to keep the pressure on. Specifically, the FCACP is developing contacts and learning procedures for acting with registrars, hosting companies, and similar entities as added avenues to make the child pornography business more difficult to run.

Financial Coalition Against Child Pornography Members

AOL
American Express Company
Banco Bradesco
Bank of America
Bank of New York – Mellon
Capital One
Chase Paymentech Solutions
CheckFree
Citigroup
CyberSource-Authorize.Net
Deutsche Bank Americas
Discover Financial Services
Elavon
First Data Corporation
First National Bank of Omaha
Global Payments Inc.
GoDaddy.com, Inc.
Google
Green Dot Corporation
HSBC – North America
JP Morgan Chase
MasterCard
Microsoft
National Processing Company
North American Bancard
PayPal
Premier Bankcard
ProPay Inc.
Standard Chartered Bank
Visa
Wells Fargo
WePay
Western Union
Xoom.com
Yahoo! Inc.