FINANCIAL COALITION AGAINST CHILD PORNOGRAPHY

TECHNOLOGY CHALLENGES WORKING GROUP REPORT 2008: "TRENDS IN MIGRATION, HOSTING AND PAYMENT FOR COMMERCIAL CHILD PORNOGRAPHY WEBSITES"

Background

The Financial Coalition Against Child Pornography ("Coalition") was formed in 2006 to address the alarming growth of commercial child pornography over the Internet. Its members include leaders in the banking and payments industries, as well as Internet services companies. One of the Coalition's charters is to track and anticipate how the mechanics of commercial child pornography are evolving. To that end, the Coalition's Technology Challenges Working Group ("TCWG") offers the following observations.

Disclaimer

This Report ("Report") was created and written by volunteers on behalf of TCWG and represents the current view of TCWG on the issues addressed as of the date of publication. The content 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. There may be inaccuracies and information that has become outdated since this Report was originally written.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. TCWG 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 an endorsement by such organization or entity.

Complying with all applicable copyright laws is your responsibility. This Report may be freely redistributed in its entirety at no charge provided that any legal notices, including all copyright notices, are not removed. It may not be sold for profit or used in commercial documents without the written permission of TCWG, which may be withheld in TCWG's sole discretion.

Trends in Migration

The central problem for governments and law enforcers attempting to deal with online commercial child pornography ("CCP") is the inherent anonymity of the Internet. Criminals have resourcefully defended their online operations, ultimately enabled by the anonymity of their selected transaction and content medium.

To wit:

- CCP content can be hosted in non-enforcement countries, remote from direct legal recourse, or it can be unwittingly hosted on a system of computing platforms which themselves have been co-opted by technically skilled purveyors of CCP.

- Online payment for viewing CCP is, in effect, anonymous. Although traditional payment providers are banks or bank-like institutions following national banking regulations, TCWG sees a trend toward emerging ("alternate") payment services and financial entities, whose non-bank status entitles them to bypass compliance rules requiring them to know payer and payee identities.

The central problem in detection and prevention of online CCP is that the Internet provides an anonymous space in which cybercriminals can operate with relative impunity and carry out a multitude of crimes, aside from the sale of CCP. Anonymity facilitates online CCP operations in three ways: ease of concealing stored content; criminals' ability to operate rapidly dynamic payment sites ("up today, down tomorrow, up the next day") to avoid detection; and the lack of regulation of emerging alternate payment methods.

Typically the Internet is peppered with child pornography link ("CPL") farms. Some CPL sites have a number of redirects, eventually moving the potential customer to an unrelated domain. When a potential consumer arrives at a site that offers a membership for a fee, a number of things could occur. The host site may offer to take a credit card to pay for the site. At that point an unencrypted web page may be used to document the name, address, phone, and credit card data. The majority of CPL sites that offer memberships transact credit card payments without the use of https technology, thus exposing the consumer to a high degree of risk. The information is vulnerable to exploitation by cybercriminals. TCWG can only assume that the CPL sites choose not to obtain an SSL certificate because they would have to sacrifice some of their anonymity.

Some sites offer CCP material for sale via email confirmations. The customer sends an email to an unknown individual to complete the transaction, sometimes using webmoney transfers or simply using the U.S. mail to send cash. Still other CCP sites offer membership, but redirect the customer to a credit card payment site aggregator. Some of these aggregators offer both secure and insecure transactions. These aggregator sites generally: do not encrypt credit card transactions; and will counterfeit or "spoof" credit card transaction pages to look like legitimate and semi-legitimate third party processors. TCWG has not seen a significant drop in the number of pay for CCP sites, but has seen a decline in successful identification of the CCP sites likely due to stricter enforcement causing those who profit from CCP to go further underground thereby making them more difficult to identify.

Hosting[1]

Hosting Companies

Many hosting companies have become conduits for the storage of CCP. To that end, in most cases, branded URLs or content sites will rotate through scores of potential merchants and payment methods

[1] A **web hosting service** is a type of Internet hosting service that allows individuals and organizations to provide their own websites accessible via the World Wide Web. Web hosts are companies that provide space on a server they own for use by their clients as well as providing Internet connectivity, typically in a data center. See http://en.wikipedia.org/wiki/Web_hosting.

until each is shut down. The branded sites will then establish new accounts and payment methods. In this way, it is possible for an individual site to have had both its content and its payment capabilities removed repeatedly only to pop back up with new hosts and merchants. To the casual observer, it appears that these sites have continued to operate without intervention. To the trained and educated eye, it is clear that these sites have actually been repeatedly disabled only to reappear. The futility of this process can be compared to the "Whack-A-Mole" game that children enjoy in amusement arcades.

Interestingly, "white label" (seemingly harmless) content sites and URLs have an entirely different life cycle. Typically, these URLs are used simply to drive consumers to temporary white label content or the temporary location of branded content. In this respect, these URLs are the "cannon fodder" in the ongoing battle for commercial viability. In fact, it is possible to see 10-20 different URLs appear within days of each other in mass spam campaigns, where all URLs end up housing the same branded content.

Currently many hosting companies are merely focused on reliability and pricing and most have no written policies with regard to illegal content. In some cases their terms of use agreements have language which states that hosting illegal content by their customers could result in termination of service. However, how proactively they enforce these agreements is the key question. Generally speaking, hosts do not screen content, and are dependent on reports that they are hosting CCP before they are willing to take action. TCWG has been advised by one legal expert that hosts that have not consulted a lawyer or someone knowledgeable about the issue often respond to complaints about this material by undertaking their own internal investigation; the same expert asserts that this is a risky and ill-advised practice for the following reasons: a) it should not be the role of the host to "police" content; b) web hosts are not qualified to determine what constitutes CCP; and c) hosts could be in violation of possession laws regarding CCP. Those who have sought legal advice have institutional procedures in place to isolate the material and report it to the National Center for Missing & Exploited Children ("NCMEC").

The first step would be to get the hosting companies to adopt best practices. TCWG research has shown that there is currently no trade organization for web hosts similar to the U.S. Internet Service Providers Association. Such an organization would be helpful in establishing industry standards and could serve as a mechanism for responding to TCWG's concerns.

The following brief list serves to recommend and highlight a minimum level of due diligence for hosting companies with the purpose of eradicating the storage of CCP.

- Child Pornography Policy: Maintain a policy on how to detect and react to the hosting and storage of CCP. The following web host's site has been suggested by a legal expert as one that addresses the CCP issue: http://www.peakinternet.com/legal/aup/. While TCWG is not endorsing this language as a model, it does at least attempt to address the issue.

- Monitoring: Frequent changes in methods, technology, URLs, etc. are clearly deliberate efforts used by criminals to avoid detection. They also go to great lengths to maintain their anonymity. TCWG therefore recommends that hosts search for known CCP sites on a quarterly basis with a goal of weekly review of all known active sites. Spider and bot technology exists to assist in locating the lexicon associated with CCP and images with ease. Once found, these sites should be removed by the host.

- WRT Filtering: Much like Internet Service Providers currently do, when using technology to rid their systems of illegal material, hosts should delete all illicit material from their servers.

- Information Sharing with NCMEC by Nefarious Hosts (e.g., those hosts who store illicit content): Consistent with their policies, hosts are encouraged to share information that they possess with NCMEC regarding persons or companies believed to be engaged in the distribution of CCP.

- Conduct Due Diligence on Customers: Just as banks have been required to adopt "know your customer" policies to avoid being used by drug traffickers and terrorists for money laundering, web hosts should be encouraged, if not required, to conduct due diligence on customers and their content.

Finally, it would behoove the Coalition to consider creating a "blacklist" of hosting companies who are known to either knowingly host CCP or practice willful neglect, and others who are unwilling to follow the five steps of due diligence highlighted above.

Compromised Corporate Servers as CCP Hosts

Holes in a corporate network's security are opened by criminal crews with their malware, who take control of any one remote user hooked up to a network and, in turn, compromise the entire network leaving intellectual property and financial data vulnerable for exploitation by organized crime, or in the case of CCP, allowing crews to deposit onto or distribute from these compromised networks.[2]

Imagine the server of a major corporation, university, or financial institution being taken over and relaying CCP for sale. The clear evidence of ongoing major security breaches makes such a thought not only possible, but likely. The best practice checklist in the Appendix should be shared with CTOs and CIOs of Coalition member institutions.

Online Payment Systems

In the Introduction to the December 2005 "U.S. National Money Laundering Threat Assessment,"[3] ("NMLTA") the U.S. Government stated that "criminals are enjoying new advantages with globalization and the advent of new financial services such as stored value cards and online payment services." The NMLTA identified and assessed thirteen systemic financial threats against the United States and, of those thirteen, two — online payment systems and stored value cards — represented new chapters that would not have appeared in such an NMLTA a few years prior. These new and evolving threats in the financial system, predicated in part as a response to demands from the unbanked, and, in part, in response to the globalization of financial systems and to their reactions to the reality of the Internet, pose potential threats from criminal and other illicit use not only to the U.S. economy, but to the global economy as well.

As the NMLTA asserted, "[n]ew and innovative online payment services are emerging globally in response to market demand from individuals and online merchants… [O]nline merchants, particularly those in sectors with high 'chargeback' rates, are generating demand for new payment methods. There are hundreds of these online payment systems. These markets embrace online payment systems that set their own clearing and settlement terms absent any consumer protection regulations. Typically, transactions through these service providers are considered final with no recourse for individuals who

[2] See http://www.securityfocus.com/brief/691.

[3] See http://www.treas.gov/press/releases/docs/nmls.pdf.

believe they have been defrauded. The consequence, according to federal law enforcement agencies, is that these systems have become favorite payment mechanisms for online perpetrators of fraudulent investment schemes and other illegal activity."[4]

The NMLTA provided an overview of "digital currency services" such as the recently-indicted e-gold, Ltd., as well as other online payment systems. The NMLTA assessed vulnerabilities for these evolving technologies noting that money transmitters are required to register with FinCEN,[5] and are subject to anti-money Laundering ("AML") recordkeeping and reporting requirements, as well as, in general, state licensing requirements. The AML requirements of an online payment system or a digital currency "depends upon its location and the ways in which it participates in or conducts transactions." [6]

These new and evolving payment mechanisms, including two not addressed in the NMLTA — online games such as Entropia Universe, which have their own convertible currencies with links to real-world withdrawal capacities, as well as the advent of mobile banking via cell phone — point out the dramatically altered landscape from the traditional methods of cash, check, and credit card. These new payment mechanisms, especially where coupled with the Internet, can facilitate conventional crime in new ways, or can generate new criminal activities that could not have occurred but for the use of the technologies themselves. The financial flow may be the origination of the criminal proceeds, or the laundering mechanism to move the proceeds, once generated.

Internationally, the 34 nation Financial Action Task Force ("FATF"),[7] in October 2006, released a report[8] that examined the way in which money can be laundered through the exploitation of new payment technologies (prepaid cards, Internet payment systems, mobile payments, and digital precious metals). The report found that, while there is a legitimate market demand for these payment methods, they are highly vulnerable to money laundering and terrorist financing schemes. Specifically, cross-border providers of new payment methods may pose more risk than providers operating exclusively within a particular country. The FATF report recommended continued vigilance by all countries to further assess the impact of evolving technologies on cross-border and domestic regulatory frameworks. However, given the level of corruption or collusion on the part of some foreign governments in various types of criminal activities, strict monitoring and enforcement of financial transactions is unlikely.

PayPal has exhibited an extraordinary level of due diligence as an online payment system and can be a model for others in the industry. Through sound policies, proprietary models, audit/investigative means, and public/private partnerships, PayPal demonstrates a rigor that other online payment systems should emulate in order to thwart payments for child pornography. PayPal's policies and procedures for due diligence are outlined below:

Policy

- PayPal has a zero tolerance policy for the use of its system for any illegal materials and services.

---

4 NMLTA at 25.

5 U.S. Treasury Financial Center.

6 NMLTA at 27.

7 Since its creation, the FATF has spearheaded the international effort to adopt and implement measures designed to counter the use of the global financial system by criminals. It established a series of 40 Recommendations in 1990, revised in 1996 and in 2003, to ensure that they remain up- to-date and relevant to the evolving threat of money laundering.

8 http:www.fatfgafi.org/document/17/0,3343,en_32250379_32237217_37627409_1_1_1_1,00.html.

- The PayPal User Agreement clearly states that any account offering illegal materials and/or services violates the Acceptable Use Policy and will be subject to immediate closure.

Models and Other Detection Tools

- PayPal has proprietary models that are designed specifically for child exploitation.
- PayPal has over 1700 key words in multiple languages built into modeling tools.
- PayPal invests heavily in monitoring and detection tools in the area of child exploitation.
- PayPal employs tools that crawl and spider its system internally and externally on the web looking for violations.
- Key words and modeling techniques are updated weekly.
- PayPal encourages anyone who has information about the potential unlawful use of PayPal to contact the company.

Audit

PayPal engages several vendors that "crawl" the web in search of potential violations associated with its brand.

Investigative Agents, Analysts, and a Global Law Enforcement Operations Team

- PayPal has a team of close to 100 agents globally (in Omaha, Dublin, and Shanghai) who search for, review, and investigate high risk violations, including those related to child exploitation.
- In addition, PayPal has a team of specialized agents who work solely in the area of anti-child exploitation — they have been trained for several years by NCMEC and are regularly tested for subject matter expertise.
- PayPal invests heavily in training and mentoring programs for its investigations team and analysts, including internal and external training, online libraries, and other resources to ensure that PayPal has the most up-to-date reference materials.
- PayPal has a research program where agents research industry trends, news, and events, and explore next generation technology.

Public and Private Partnerships

- PayPal works closely with U.S. Immigration and Customs Enforcement, the FBI, and other regulatory bodies to ensure that it is well-versed on problems with illegal content.
- PayPal has had various representatives from law enforcement as guests to its Global Operations Center in Omaha as part of their Distinguished Speakers Program for training.

- As part of their Global Law Enforcement Operations Team, PayPal has former law enforcement, U.S. Attorneys, and industry professionals who work closely with their counterparts in law enforcement, regulatory agencies, and NGOs to foster communication and to collaborate on investigations.

Conclusion

The migration of CCP payment and web hosting away from traditional financial vehicles and hosting models is a highly challenging trend that not only requires attention but also greater understanding and, as in other aspects of Internet commerce, perhaps greater regulation. The underground economy and the distribution of CCP are dynamic and resilient in the face of the Coalition's best efforts to combat it. As various Internet-related industries mature and enter the community of good corporate citizens, it will be critical for the Coalition to bring them into the fold and encourage them to adopt good policies, such as greater due diligence and some degree of filtering and monitoring of their hosted sites.

APPENDIX: WEB SERVER SECURITY PRACTICE[9]

Web Server Security
1. Remember that default installation of HTTP can lead to DDoS attacks and exposure of confidential information making the server vulnerable to an attack.
2. Use SSL or SSH.
3. Do not run other applications on system. Limit to HTTP and any other services required.
4. Apply latest service packs, updates, and patches.
5. Access Control Issues: restrict user list from accessing web server by utilizing two factor authentication.
6. Conduct a penetration test with associated vulnerability scans to audit the web servers for critical exploitable vulnerabilities.
7. Is change control implemented to reduce overall risk? Are system changes tracked and monitored?
8. Remove any sample CGI programs from the server.
9. Run web application scanner to simulate an attack of the website and determine its security. Run it often during design phase and implement weekly scans to check for new vulnerabilities.
10. Review all logs frequently. All logging should be turned on. If possible one should push all logs to central location to check for trends or similarities between other web servers.
11. Carefully plan and address the security aspects of the deployment of any public web server.[10]
12. Implement appropriate security management practices and controls when maintaining and operating a secure web presence.[11]
13. To ensure the security of the web server and the supporting network infrastructure, the following practices should be implemented: ▪ Organizational-wide information system security policy. ▪ Configuration/change control and management. ▪ Risk assessment and management. ▪ Standardized software configurations that satisfy the information system security policy. ▪ Security awareness and training. ▪ Contingency planning, continuity of operations, and disaster recovery.

[9] World Bank Treasury Technology Risk Checklist 7.3.

[10] As it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage. Organizations are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan that addresses security. Establishing such a plan guides organizations in making the inevitable tradeoff decisions between usability, performance, and risk. Organizations often fail to take into consideration the human resource requirements for both deployment and operational phases of the web server and supporting infrastructure. Organizations should address the following points in a deployment plan:
- Types of personnel required (e.g., system and web administrators, web master, network administrators, information systems security officers [ISSO]);
- Skills and training required by assigned personnel;
- Individual (level of effort required of specific personnel types) and collective manpower (overall level of effort) requirements.

[11] Appropriate management practices are critical to operating and maintaining a secure web server. Security practices entail the identification of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability of information system resources.