CYBER SECURITY PRIMER

21 January 2011

Albany, Buffalo & New York Divisions

Cyber Crime Executive Briefing

EXECUTIVE SUMMARY:
This primer provides a common language between organization leaders and technical employees protecting networks from cyber threats.

The sections of this document contain a *brief* introduction to cyber threats, appropriate for corporate, Federal, state and local agency leaders; it is not a comprehensive discussion of cyber crime. An enhanced understanding of the cyber crime field can assist leaders to deter, prevent, and respond to cyber threats.

Please feel free to distribute as appropriate.

CYBER CRIME:
Perhaps the most talked about cyber crime is **financial** and **automated clearinghouse (ACH) fraud**, perpetrated through malware like Zeus. Zeus is only one piece of **malware** in the financial fraud arena but it dominated headlines in 2010 as hundreds of businesses reported compromises and significant losses due to the program. When malware like Zeus is installed on a computer, the software begins recording every keystroke through a **keystroke logger** and submits that information back to the criminal. Advanced variations of this type of malware include the abilities to add questions to a bank's login page and the creation of a backdoor into a computer system. Malware like Zeus is particularly dangerous because most antivirus programs have trouble detecting it and it is a "**point-and-click**" program. Consequently, criminals no longer need computer expertise to create malware that can defeat antivirus products. In the fall, information suggested that the creator of Zeus retired and handed his code to a competing program, SpyEye. At this point it remains unclear how or if the Zeus-SpyEye merger will occur, and whether the new malware will be as large a threat in 2011 as Zeus in 2010.

Financial fraud includes mortgage and Ponzi schemes, credit card theft and tax fraud. Identity theft frequently results in financial fraud. **ACH fraud** is fraudulent electronic funds transfer between banks through batch processing (a data handling method in which a large number of requests are processed in the same transaction).

Malware is the catch-all phrase used to describe all types of malicious software, including viruses, Trojans and worms. Like many cyber crime terms, the word is the shortened form of two words, in this case "malicious software." Different types of malware are described in other sections of this paper.

Keystroke loggers (**keyloggers**) are software programs that record every key pressed. Newer versions include the ability to take a picture of the screen (screenshot) after each input, defeating voice recognition software and onscreen keyboards.

Point-and-click software are programs that allow a user to easily accomplish tasks without having advanced computer knowledge. These easy to use programs generally offer self-explanatory menus or toolbars to aid the user.

Spam is one of the cheapest online advertising methods. The high volumes of spam received by businesses can overwhelm email servers and deleting it wastes valuable time. In addition, spam has become a preferred delivery method for **phishing** emails and malware. Online pharmacies, specializing in the illegal distribution of prescription medication routinely employ spam, advertisements for Viagra are the most well known example. These pharmacies exist outside the United States and attempt to exploit high drug prices inside the United States by marketing prescription medications at hugely discounted prices. When customers receive their medication (if they ever do), the medication will most likely be counterfeit, a placebo, or another unrelated substance made to look like the intended medication. Spam-delivered malware may contain viruses, Trojans or worms, and compromise the computer or the entire network. Phishers use spam to cast broad nets in identity theft scams. They frequently target customers of large financial institutions through spam emails that tell the customer their account has been compromised. When the target clicks on the link in the email, they are brought to a website that looks like the institution's website, but is not. When the customer enters their information to login, they are really passing their information to the phishers. **Spear phishing** is a variation of phishing that may be specifically directed to a small group of people. Spear phishers believe in quality over quantity and use research on a small group of people to craft an email specific to the group.

Spam is unsolicited electronic mail, generally email, although it is possible to receive spam faxes. Spammers may send email to known email addresses or may try common emails ("jsmith@abc.com"). Spam costs so little that an extremely small number of positive responses will pay for millions of spam emails. Spam is frequently used to deliver malware and phishing attempts.

Phishing is a variation of the word "fishing," because it is the electronic version of throwing a hook in the water and hoping for a bite. Other forms of phishing include "**spear phishing**" (a targeted phishing attack), "**SMShishing**" (phishing through SMS and text messages) and "**vishing**" (phishing through phone calls). Spear phishing victims may receive an email that contains information about their company, "CEO Killed in Crash," or that appears to come from a friend "Vacation pictures").

The exploitation of trusted Internet resources has long been a cyber crime trend. "**Drive-by downloads**" are one of the more insidious Internet-based malware attacks as they frequently exploit trusted websites and require no action by the user. **Malvertising** is one form of drive-by download. Malvertisers embed malicious code into advertisements on legitimate websites, turning popular websites into malware servers. This is both difficult to block and to detect because the user trusts the website and the advertisements rotate so only a few users to the website receive the malware.

Drive-by downloads are unintended downloads of programs from the Internet. These programs can be malicious in nature. A **drive-by installation** is the actual installation of a program without the user's knowledge.

Malvertising is malicious advertising. Criminals may purchase an advertisement on a website like the New York Times home page and hide malicious code in the ad. All the users who visit that legitimate website and view that advertisement will be infected.

Internet scams involving fake charities raising money for current events, dating and romance schemes, event ticket sales, real estate and time-share sales, and secret shopper or work-at-home opportunities all take advantage of people's trusting nature to repeatedly con money out of the unsuspecting victims. Criminals attempt to sell items, frequently cars and other larger items, they have no intention of delivering and may not even own, using the reputations of online auction and sales websites like eBay and Craigslist to create a level of trust with the purchaser. Work-at-home opportunities are often scams used to hire unsuspecting victims, known as money mules, who help criminals pass money outside of the United States without arousing suspicion. Many of the money mules do not know they are helping criminals. Dating sites can act as recruitment centers for various types of victims, including money mules and romance scams. Standard romance scams involve an overseas scam artist developing a

personal relationship with a United States citizen and then asking that citizen to send money to help the scam artist come to the US or to accept and re-mail packages on the scammers behalf. Large events like the World Cup result in malicious websites selling fake tickets. Disasters around the world create numerous charities that claim to be fundraising for the victims. Fake Wi-Fi access points at public locations use the same trust to convince victims to connect laptops or smartphones to the free access points. These free access points may distribute malware or harvest personal information, logins and passwords.

The increasing use of social networking websites like Facebook and Twitter has spread to the criminal underground, too. These websites can be used to spread malware, gather target information or to disseminate links to malicious websites. Malware designed for social networking websites, like Facebook, Twitter, and LinkedIn, compromise a victim's account and spread the malware to his or her friends, creating an ever-expanding victim network. Koobface, first detected in 2008, is one of the more prolific pieces of social networking malware. Social networking websites are also ideal for targeting victims. Criminals can use the information gained on these websites to identify targets, craft spear phishing emails and to develop other more devious scams such as the **hitman scam**.

The **hitman scam** is an online scam in which the criminal uses personal knowledge to convince the victim of an awful event. In the hitman scam the criminal tells the victim that he, the criminal, has been hired to assassinate the victim. However, the victim seems like a nice guy, and if the victim will pay the criminal, the criminal will not kill him. Variations include requests for money to help out someone traveling or living overseas that has supposedly been injured, arrested or kidnapped.

Scareware is any type of software that tricks the user into anxiety or panic. Rogue security software, like fake antivirus programs, offer the user a solution that will fix the problem that caused the panic. These solutions may require a credit card for purchase (identity theft/financial fraud) or trick the user into downloading malware.

Botnets are large networks of computers around the world. Each bot consists of **zombie** computers, to which the **command and control** (C&C or C2) server can send commands. Most often, the owner of a zombie does not know they are part of the botnet. Botnets are used to send spam, spread malware and handle tasks that require lots of computing power or multiple geographic locations. Many botnet owners rent out their botnets to other criminals.

Rogue security software and fake antivirus programs are different names for the same type of **scareware**. These programs trick the user into downloading them through various ruses meant to frighten the user. Often they use a compromised website to create a pop-up dialog box that warns the user of malicious activity on their computer and offers a solution. When the user clicks in the box to download the fix, they really initiate the malware download. The software may do nothing visible to the user or it may try to look like a real antivirus product and start scans to "fix" the problem. Some fake antivirus programs require the user to pay for the program via credit card and provide realistic looking websites, live help desks, and 1-800 numbers to call. No matter what type of scareware is used, viruses, keystroke loggers, **botnet** infections or identity theft are possible results.

Other online crimes include a rising use of webcams, blackmail, and smart phone vulnerabilities. Malware enables criminals to remotely turn on and monitor webcams, and can disable the indicator light, so the victim is unaware they are being watched. Individual users and companies have reported blackmail and extortion attempts when a criminal holds their data, computer or personal information hostage. These attacks sometimes include the use of ransomware, malware that is specifically written to hold data or computer systems hostages so the criminals can demand a ransom. Numerous demonstrated vulnerabilities in smartphone "apps" are programmed to make expensive phone calls and text messages, monitor the victim's location and steal contact lists and documents off the phone, all without the victim

knowing. Location information, retrieved from smartphone pictures posted to Internet websites, has been gaining attention for the vulnerabilities it may expose.

In July, **Stuxnet** made a large splash in the and **Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA)** world, proving that these simple control systems are also vulnerable to exploits; exploits that could be used to crash trains, shut down power plants or have other catastrophic infrastructure effects. Soon after Stuxnet, the SHODAN search engine became widely known. SHODAN, nicknamed "Google for hackers," is a search engine that allows anyone to locate a server, router or computer connected to the Internet, including vulnerable SCADA systems.

Stuxnet was the first widely publicized worm to attack PCS/SCADA systems. The worm reprogrammed infected computers and exfiltrated data possibly for espionage purposes.

ICS and **SCADA** systems are very simple control computers for monitoring machinery, turning switches on and off, performing load balancing and other simple functions that can be easily automated.

Exploits are software that take advantage of bugs, glitches and vulnerabilities within other programs.

While the above has focused on cyber criminal activity, cyber espionage is a real threat, amply demonstrated over the past several years. Some cyber espionage activity is illegal, however, some practices are completely legal. The term "advanced persistent threat" is often used in cyber espionage discussions because of the long-term intelligence gathering focus by actors who use a full spectrum of techniques. Zeus operators have used its keystroke logger to learn login names and passwords, giving them access to company data. Spear phishing attempts frequently target business leaders, negotiators, lawyers and management to install malware for espionage purposes. Malicious actors use social networking sites to monitor company activity, which is easily accomplished by monitoring posts from several employees in a single company. The recent **Gawker Media** compromise demonstrates the vulnerability of simple passwords and the use of the same login credentials across multiple platforms; within days criminals had used the compromised login credentials to break into other websites.

In mid-December **Gawker Media** was hacked and approximately 1.3 million users' passwords were released into file sharing websites. The compromise spread to other companies because employees often use the same logins and passwords across multiple accounts and Gawker used an outdated encryption method to protect all of the information. One day after the Gawker compromise, criminals had access to multiple Twitter accounts because the Twitter accounts used the same login information.

EMPLOYEE EDUCATION

Educating employees about cyber security can be one of the most difficult security tasks facing any business. Security warnings, even the best ones, inevitably produce glazed eyes and yawns, but security must become a habit because humans are the weakest link in any security network. Everyone remembers to badge in, lock their car doors, and report suspicious activity. Cyber security staples such as deleting suspicious emails unread, surfing only trusted sites and locking a computer when away from it, should be just as reflexive.

Cyber security posters, calendars and toolkits can be used to enhance employees' awareness of cyber security basics are available through a number of links at the bottom of this document. Some of the best basic security precautions include preventing physical access to a computer: locking the workstation when stepping away, disconnecting from the Internet when it is not in use, and keeping data on a server instead of a local machine (i.e. not on the Desktop or in the My Documents folders). Remind users to implement basic security steps through emails, a security banner or website pop-up box and then remind

users again if violations of these precautions occur.

Building strong cyber security practices among employees requires significant work, but taken in small increments it can be managed. Add a new goal each week and explain why each goal is important and what can happen when it is not achieved. (A little Internet research can provide many examples of the risks and costs associated with security lapses.)

To take it a step further, send tests to employees; for example, a "phishing" email loaded with "malware." Creating the malware so that it only displays a funny picture and reports back who opened it is a good way to educate users through example, without harming the network.

Using Internet-based scams and urban legends in weekly emails are a great way to grab attention and educate employees at the same time. Many scams are interesting to read and most people think they would never fall for any them. Decide on the message and then look for a related scam or urban legend that you can work the message into. Multiple websites provide lists of these urban legends and scams, including Snopes.com and UrbanLegendsOnline.com.

October, National Cyber Security Awareness Month, is the perfect time to culminate efforts and join in the national campaigns to promote cyber security awareness. Many of these campaigns include special contests in which employees and their children may participate. There are also many opportunities to tailor or create contests for individual companies including creating a company calendar complete with special company dates, random funny facts and cyber security tips.

THE LANGUAGE OF CYBER CRIME

The following are basic definitions of common cyber crime terms. To learn more about any of these terms, consult technical staff or check trusted websites.

Black lists are lists of malicious websites, domains or IP addresses. System administrators can use these to block malicious activity. **White lists** are lists of known, good websites, domains or IP addresses. (Internet Protocol (IP) addresses are the physical address of any computer on the Internet and look like: 123.123.123.123.)

Black hats are individuals who use their knowledge to commit illegal or immoral cyber activities. **White hats** are those who use their knowledge to aid others. **Grey hats** fall in between the two groups and may conduct illegal acts but are not malicious in their activities whereas black hats are. For instance, a grey hat may discover an exploit but publish the information to the software vendor so that it can be repaired instead of using the information to create malware.

Carding refers to the process of verifying stolen credit card information. **Carders**, the criminals involved in this activity, sell credit card information online and are able to imprint stolen data onto fake credit cards, which may be used on the Internet or in a store without arousing suspicion.

Clickjacking is a technique used to trick Internet users into clicking on a button or link that appears to do one thing but really does something else. **Likejacking** is a similar technique but unique to Facebook, where attackers show the user a web page with two layers. The front layer contains the ruse the user thinks they are clicking on and the back layer contains a "like" button that spreads the spam to others.

Cross-site scripting (XSS) attacks are used to inject code into webpages viewed by others. These attacks bypass client-side security and allow the attacker to steal user information, including sensitive personal data, or to gain elevated privileges to the webpage, which provides access for further attacks.

Denial of Service (DOS) attacks involve one computer sending information to another computer to keep the second computer busy. Generally these attacks are **Distributed DOS** (DDOS) attacks involving hundreds or thousands of computers sending bad information to a website. DDOS attacks can overload websites and company networks, forcing them off the Internet. **Telephony DOS** (TDOS) attacks are similar but the victim is called and hears white noise or random conversation, forcing the employees to constantly answer the phone, keeping the phone lines busy.

DNS cache poisoning tricks a Domain Name Server (DNS) into storing incorrect information regarding a website. A DNS server matches a domain (www.Google.com) to the host IP address, which allows humans to use an easy to remember word (i.e. Google) instead of an IP address (i.e. 123.123.123.123) for web browsing. When the DNS cache is poisoned, the cache believes that the website corresponds to a different IP address and redirects users to a site the attacker controls.

Domain slamming is a trick originating with Internet Service Providers (ISP) and domain registration services where a secondary service provider issues a notice that the victim's service is about to expire and offers to renew the service. In reality, the service was not about to expire and a competing service provider issued the notice to trick the victim into switching service providers.

Domain squatting, also known as **cybersquatting**, takes advantage of brand names. The domain squatter purchases an Internet domain using a well-known term and then offers to resell the domain to the brand owner at an inflated price. **Typosquatting** is a similar technique where the squatter picks a name very similar to a well-known domain and relies on typing mistakes to drive customers to the website.

Hacker is a nickname for a person who attempts to access a website, computer or network without appropriate authority. Traditionally, hackers were programmers who sought to improve programming code by developing new, faster or better ways of accomplishing a task.

Hijacking websites, computers, and networks is a common cyber technique. Criminals may hijack a website, computer or network, preventing the legitimate owners from gaining access. Hijacks may be done as part of blackmail or extortion effort, or for personal reasons.

Intruders are individuals who gain or attempt to gain unauthorized access to or escalated privileges on a website, computer or network.

Meta data is the data that exists within a document but is not seen. Examples include information residing in the track changes feature and document properties. Meta data is harvested by criminals who want to know more about the network or by lawyers for use in a court case.

Nigerian scams or **419 scams** are so named because it is section 419 of the Nigerian criminal code that covers these crimes, which were initially popularized by Nigerian cyber criminals. A variety of these scams exist but they all involve requests for the victim to facilitate the movement of money.

Payload is the data and origination information of data transmitted over a network. In cyber crime, the

payload is the virus or other malicious code transmitted to the victim's computer.

Search Engine Optimization (SEO) is an Internet marketing strategy that involves a variety of techniques, some legal and some not, to move a particular website to the top of the hit list returned by a search engine. Varying studies suggest that most people only visit the first few results in the hits, making SEO an important marketing consideration. Various criminal techniques include manipulating the programming code on a legitimate website to make the criminal's site appear more valuable.

Skimming involves various methods of reading and stealing a debit or credit card's data. Skimming can occur anywhere credit cards are routinely used. Skimming devices are generally small devices that can be hidden by a cashier who swipes a victim's credit card through the device during the legitimate transaction or devices that install over ATMs and other self service credit card scanning points.

Sniffing is when one computer user looks at the network traffic of another computer user, with or without the second user's knowledge.

Spoofing is when a user impersonates another user. Criminals may spoof email addresses or phone numbers so the victim believes the email or phone call originated with a trusted entity.

Spyware is a large class of malicious software that can be installed on a user's computer without their knowledge. The spyware collects information about the user, their browsing habits, or to actively affect the user's computing experience by changing settings or redirecting Internet requests. Keystroke loggers are one form of spyware. **Adware** displays pop-up advertisements on the machine it has infected; it may be spyware if it watches browsing activity to provide directed advertisements.

SQL injection is a form of attack against websites that have forms for the user to complete. SQL is a database query language common among many different database platforms. Normally, the data in these forms is transmitted to a database for storage. In this type of attack the attacker inputs SQL commands into the form and the database provides information instead of storing the data.

Website defacements occur when a intruder gains administrative access to a website and uses that access to change the look or content of the website. The majority of defacements involve changing the home page to display an announcement that the website was hacked and by whom and sometimes include a political or religious message.

Zero day exploits are new exploits that have never been documented by cyber researchers. These exploits cannot be prevented by patching and regular maintenance until after they have been in the "wild." Once the exploit becomes known, software companies will issue software patches.

FURTHER RESOURCES:
Contributors to this paper have valuable cyber security information on their websites. In addition to those resources, the following resources may be useful:

Department of Homeland Security: www.dhs.gov
Stay Safe Online campaign: www.staysafeonline.org
On Guard, Online: www.onguardonline.gov
Looks too Good to be True: www.lookstoogoodtobetrue.com
Internet Crime Complaint Center (IC3): www.ic3.gov

Points of Contact

Multi-State Information Sharing and Analysis Center (MS-ISAC) 31 Tech Valley Drive East Greenbush, NY 12061 (518) 266-3485 7x24 Security Operations Center 1-866-787-4722 www.msisac.org	**FBI Albany** 200 McCarty Ave. Albany, NY 12209 518-465-7551 albany.fbi.gov
NY State Police **Computer Crime Unit** 1220 Washington Ave. Building 22 Albany, NY 12226 518-457-5712 www.troopers.state.ny.us	**New York State Intelligence Center** **630 Columbia Street Ext.** **Latham, NY 12110** **(518)786-2100** **www.troopers.state.ny.us**
NY State Division of Homeland Security and Emergency Services **Office of Homeland Security** 1220 Washington Ave. Building 7A Suite 710 Albany, NY 12242 518-402-2227 www.security.state.ny.us	**NY State Division of Homeland Security and Emergency Services** **Office of Cyber Security** 30 S. Pearl Street P2 Albany, NY 12207 518-474-0865 www.cscic.state.ny.us
FBI Buffalo One FBI Plaza Buffalo, NY 14202 (716) 856-7800 buffalo.fbi.gov	**FBI New York** 26 Federal Plaza, 23rd Floor New York, NY 10278 (212) 384-1000 newyork.fbi.gov
United States Secret Service, Albany 39 N Pearl St # 2 Albany, NY 12207 (518) 436-9600 www.secretservice.gov	

Please send any comments or suggestions to CTICGfeedback@msisac.org.