Cyber Crime

A Technical Desk Reference

CENTER FOR INTERNET SECURITY®

For additional copies or to download this document, please visit:

http://msisac.cisecurity.org/resources/guides

The mission of the Center for Internet Security is to enhance the security readiness and response of public and private sector entities, with a commitment to excellence through collaboration.

CIS comprises four program divisions:

Integrated Intelligence Center
The mission of the Integrated Intelligence Center is to facilitate trusted relationships with government and private sector entities to develop and disseminate comprehensive, coordinated intelligence products that help improve the security posture of all partners.

Multi-State Information Sharing and Analysis Center
The mission of the MS-ISAC is to improve the overall cyber security posture of state, local, territorial and tribal governments. Collaboration and information sharing among members, private sector partners and the U.S. Department of Homeland Security are the keys to success.

Security Benchmarks
The mission of the division is to establish and promote the use of consensus-based best practice standards to raise the level of security and privacy in Internet-connected systems, and to ensure the integrity of the public and private Internet-based functions and transactions on which society increasingly depends.

Trusted Purchasing Alliance
The mission of the Trusted Purchasing Alliance (TPA) is to serve state, local, territorial and tribal governments and related not-for-profit entities in achieving a greater cyber security posture through trusted expert guidance and cost-effective procurement. The Alliance builds public and private partnerships and works to enhance collaboration that improves the nation's cyber security.

CYBER CRIME

Technical Desk Reference

Table of Contents:

Introduction

This guide is intended as a desk reference to provide a basic introduction to the cyber crime that state, local, tribal, and territorial (SLTT) governments encounter. The information in this report is provided to further the reader's understanding of reports issued by the Center for Internet Security (CIS) relating to cyber threats and attacks, and raise the reader's awareness of the malicious actors, motivations, malware, and fraud schemes. The information in this guide is divided into cyber crime categories and sorted alphabetically within those categories. For the purposes of this guide the terms 'actor' and 'hacker' are used interchangeably.

Botnets

DNSChanger is malware and a botnet that alters a computer's domain name service (DNS) settings, redirecting infected computers to domains maintained by the malicious actors and used to promote fake and dangerous products.

AKA: none

Malware type: botnet for the purposes of spyware and DNS redirect fraud

Objective: financial fraud through click fraud

Primary Actors: organized cyber criminal groups

Propagation & Exploit: through Tidserv, and downloading freeware and shareware

Activity/Payload: modified search results and the Internet browsing experience, disabled programs and prevented online access to programs that could detect the DNSChanger malware

Variants: none

Attribution & History: The DNSChanger malware made international headlines on 8 November 2011, when the FBI, National Aeronautics and Space Administration-Office of the Inspector General (NASA-OIG), and Estonian Police arrested the 'Rove Digital' group of cyber criminals in Operation Ghost Click. The Rove Digital actors ran the DNSChanger malware. As part of the arrest an independent group, the DNSChanger Working Group (DCWG), began hosting the malicious domains to allow infected computers the opportunity to remove the malware. By court order this activity ended on 9 July 2012, however, infections still occur and not all computers infected prior to 8 November 2011 were appropriately cleaned. Detailed information regarding detecting and remediating DNSChanger is available on the DCWG website at www.dcwg.org.

Worth noting: N/A

Ponmocup – please see the section on Trojans.

Exploit Kits

The **Blackhole Exploit Kit** (Blackhole) is one of the most widely used kits currently in existence, largely due to the speed with which the creator is able to include exploits for newly announced vulnerabilities, allowing actors to compromise computers with the new vulnerabilities before a patch is available. (This section derives the majority of its information from the MS-ISAC SOC report on Blackhole, September 2012, http://msisac.cisecurity.org/resources/reports/documents/BlackHole2.0WhitePaper.pdf.)

AKA: none

Malware type: exploit kit

Objective: installation of additional malware

Primary Actors: lone hackers and organized cyber criminal groups

Propagation & Exploit: iframes with redirects on compromised websites, spam email, poisoned search engine results; identifies and takes advantage of vulnerabilities in web browsers, and browser plug-ins, including Java, PDF, and Adobe vulnerabilities

Activity/Payload: delivery of ZeuS, Zeroaccess, Cridex, FakeAV malware, although it is capable of distributing any malware

Variants: Version 2.0, released in September 2012, focused on preventing detection, as well as providing support for Windows 8 and mobile platforms. Easily identified vulnerabilities and exploits that may draw user attention were removed from this version. The previous uniform resource locator (URL) naming scheming involving “{letter}.php” was removed and the new exploit pages follow realistic looking URL naming schemes (i.e. /news/index.php). This change defeated the common method of identifying infected machines by looking for traffic to a URL ending with “{letter}.php.” Version 2 also included a method for generating dynamic domain names, which are only valid for the unique victim for a very short time frame, thus defeating blacklisting efforts.

Attribution & History: Blackhole originated in September 2010, and researchers believe a Russian actor, possibly using the alias ‘Paunch,’ created it. Per Trend Micro’s 2012 analysis, Blackhole has been the most popular exploit kit since 2011.

Worth noting: Blackhole is available to rent via hosting websites. Renters can pay for small time blocks or lengthier sessions ranging from a few hours to weeks.

Frauds

Doxing is the identification of someone through Internet resources, generally for malicious purposes.

Risk of occurrence: low-medium risk for agency personnel named in controversial news stories, low risk for agency executives and law enforcement officers, very low risk for all other agency personnel

Impact: medium-high potential impact if the dox reveals the information of sensitive or controversial personnel such as elected officials or undercover law enforcement officers.

Objective: the public dissemination of the victim's PII, including home addresses, family members' information, and financial information. Hacktivist groups dox government officials in response to perceived injustices with the objective of embarrassing the victim, or providing the information so others may target the victim for malicious activity.

Primary Actors: hacktivists

Worth noting: Organized cyber criminal groups and criminals may take advantage of information released during doxing incidents but are not known to conduct the activity themselves.

False Emergency Broadcasts through television and radio stations, and emergency sirens, have the potential to seriously jeopardize a population and may suddenly overwhelm responders before the responders are aware of an incident.

Risk of occurrence: low probability of occurrence

Impact: potential for a high impact, including loss of life if malicious actors coordinated a realistic broadcast over multiple methods

Objective: prank; it is possible that other actors, including terrorists, could use this fraud technique for malicious purposes

Primary Actors: lone hackers

Worth noting: While all known examples of fake emergency broadcasts are obvious pranks and/or unrelated to an emergency, citizens responded to these incidents by calling their local government agencies. A coordinated false broadcast that conveyed realistic information poses a risk to SLTT government agencies and the populations they serve. An attack that included the use of multiple methods, such as a simultaneous television, radio, and siren broadcast, social media site or messaging program, and the website defacement of a local news station, could result in mass panic.

False and Unsubstantiated Hacking Claims are a favorite technique of hacktivists and unskilled hackers. Unsubstantiated claims of successful hacks occur when the victim denies or does not confirm the breach, and the hacktivists does not publish evidence or publishes evidence that does not clearly originate from the victim's internal network, to support their claim of success. Hacktivists substantiate false claims with information already available due to previous compromises, information the victim purposely released, or fabricated information.

Risk of occurrence: low-medium risk that an agency will be targeted by hacktivists, with an increasing risk for larger agencies, law enforcement agencies, and agencies named in controversial news stories

Impact: low impact to operations, low-medium potential impact to personnel and reputation

Objective: to gain credibility in the hacker community, expose purported evidence of injustice, achieve social or economic goals, and/or embarrass targets.

Primary Actors: lone hackers, script kiddies, hacktivists, terrorists

Worth noting: N/A

The **tech call scam** is a fairly common scam that appears to move around the country by area code. Actors call victims and claim to work for a well-known computer or Internet security company. They then claim the victim's computer is attacking the actor's computer and the actor wants to "help" the victim stop the attacks. Other variations include instances where the actor claims to be a researcher who discovered that the victim's computer is infected with malware or where the actor claims the victim is due for a software upgrade.

Risk of occurrence: medium probability of occurrence

Impact: fairly minimal as the goal is often the installation of the malware and/or the immediate monetary theft, both of which are easy to remediate.

Objective: The caller will attempt to install a remote access Trojan (RAT), fakeAV, or other malware on the victim's computer to allow for further infections, and may attempt to convince the victim to pay for something, compromising the victim's PII and stealing their money.

Primary Actors: Organized cyber criminal groups

Worth Noting: The scam indiscriminately targets home, business, and government computer users.

Telephone Denial of Service (TDOS) attacks overload the telephone network, preventing legitimate telephone calls from being placed or received. Attacks against SLTT emergency lines, primarily at public safety answering points (PSAP) such as 9-1-1 centers, but also including utility department emergency numbers and other emergency numbers, are increasing.

Risk of occurrence: low risk of TDOS occurring_

Impact: low impact during the majority of TDOS events, however, a TDOS against a PSAP could endanger emergency responders and citizens if the TDOS prevents them from contacting the PSAP. Potential for high dollar loss if the TDOS is used to prevent the detection of financial fraud.

Objective: There are three known variants of this fraud, each with slightly different objectives.

- Direct financial gain: These calls may target the employee at work or the organization where the employee works or worked. The attacks begin with a variant of the payday loan scam, in which callers harass their victims about repayment of a payday loan the victim purportedly took out. In these cases the callers claim the department employee took out a payday loan and the callers demand the department repay the loan on behalf of their employee. Many of the victims claim they never applied for or received a payday loan. The TDOS occurs after the initial demand for money.

- Indirect financial gain: The second variant of the TDOS occurs during financial fraud schemes. In this case the victim of the financial fraud is the recipient of a TDOS attack, preventing the financial institution from confirming a suspicious wire transfer or Automated Clearing House (ACH) transaction. When the financial institution is unable to confirm the transaction, the transaction occurs, and the TDOS prevents the victim from learning about the transaction until it is too late to recover the money. For this reason, TDOS victims should immediately contact their financial institution to cancel any pending transactions, in addition to implementing other TDOS countermeasures.

- Unknown cause: Some TDOS incidents, particularly those targeting PSAPs and emergency telephone lines do not involve a demand for money or any other obvious benefit. The objective of these attacks is currently unknown.

Primary Actors: lone hackers, organized cyber criminal groups, and sometimes hacktivists

Worth Noting: N/A

SWATting occurs when an actor places a prank 9-1-1 call, to trick emergency responders into responding to a fake incident. The fake incident typically requires a full-scale response, such as a hostage situation, bomb, plane crash, or terrorist attack.

Risk of occurrence: low probability of occurrence

Impact: potential high impact event to both the individuals targeted and the first responders

Objective: embarrassment for the victims, "enjoyment" of watching the response

Primary Actors: lone hackers, hacktivists, non-cyber actors

Worth Noting: The victims are the emergency responders as well as the victim to whom they respond. In some incidents, the calls indicate that the victim is a hostage taker or terrorist, resulting in the victim's arrest before an investigation determines that the incident involved SWATting. Malicious actors may target SLTT government agencies with incidents that pertain to their area of responsibility, such as a phone call about a case of extreme abuse against a child to a social services department. Law enforcement personnel may be individually targeted by SWATting incidents as a form of revenge.

- While prank phone calls are not new, SWATting can involve spoofing, social engineering, Voice over Internet Protocol (VoIP), and phone network compromises. Spoofing software allows the caller to enter fictitious caller ID. Social engineering is the ability to find and use information to manipulate people into performing actions or divulging confidential information. VoIP is the transmission of voice communications over Internet Protocol (IP), i.e. telephone calls over the Internet.

Point of sale (POS) compromises are increasingly common in the commercial sector but remain rare in the government sector. They could target SLTT government agency locations where fees and other monetary transactions are processed. The POS is the location where money transfers from the buyer to the seller.

Risk of occurrence: very low probability of occurrence

Impact: potential medium impact to citizens affected and low impact on the affected agency

Objective: financial fraud

Primary Actors: insiders and organized cyber criminal groups

Worth Noting: Compromises can include physical tampering with pinpads or cash registers, complicit employees, or computer viruses. The compromise may affect the cash register or the computer that processes the credit card payments, and may target debit cards and pin numbers or credit card information. When multiple victims share a single financial commonality, a POS compromise is the most likely culprit.

Keyloggers

ZeuS and **SpyEye** are advanced keylogger programs with modular designs, supported by botnets, and containing sophisticated techniques to defeat many common computer and financial institution security measures. Due to the similarities between ZeuS and SpyEye and the joint history since 2010, these programs are described together in this desk reference.

- Both are capable of using web injects, which inject new information into web pages; injects are site-specific code and lists of injects are available for free and for sale. Injects can take the form of malicious fields, which ask financial institution customers for additional information, such as a debit card or pin number, or date of birth, and display inaccurate bank balances and transaction records, hiding the fraudulent transactions.

- In 2010, rumors abounded that the ZeuS author turned his code over to the SpyEye creator, implying that ZeuS would disappear. Despite this, new updates to ZeuS continued to appear in 2012, suggesting the ZeuS author or someone else continued to update the software.

- As of 2012, SpyEye copied the ZeuS functionality enabling it to hide transactions even after a user logged out and logged back into their account.

AKA: Zbot

Malware type: keylogger, botnet, worm

Objective: financial fraud

Primary Actors: lone hackers, nation-states, organized cyber criminal groups

Propagation & Exploit: exploit kits like Blackhole, drive-by-downloads, phishing emails, and social media and networking sites. In June 2013, Trend Micro researchers discovered a worm variant that arrives through a malicious portable document format (PDF) file and is capable of spreading through removable media by hiding a copy of itself in a hidden folder on the removable media.

Activity/Payload: modules include web injects, mobile platform, transmission of screen shots to defeat on-screen keyboards, and:

- Instant communication to defeat two-factor authentication is available via the Jabber messaging software.

- ZeuS includes functionality that allows the malware to accurately manipulate the bank account balances displayed to the user, effectively hiding malicious activity.

- The backconnect module allows malicious actors to initiate financial transactions from the infected computer, to defeat financial institutions rules that require IP address verification for transactions.

- A 2011 modification allows ZeuS to check to see if it is being analyzed on a test platform.

Variants: multiple

- A March 2013 McAfee report identified ZeuS as responsible for approximately 57% of all botnet infections in 2013 and in May 2013, Trend Micro reported an increase in the number of detected ZeuS variants, which they predict will continue through at least June 2013.

- The Gameover ZeuS variant, like ZeroAccess, uses P2P functionality to hide its communications. The Gameover crew used distributed denial of service (DDoS) attacks to target the financial institution and prevent immediate actions to stop the monetary transfers. In a 2012 variant of the fraud, the Gameover crew immediately used the money to purchase high-value and easily hidden merchandise, notably precious stones and watches, which they transported out of the United States using mules (actors who intentionally transfer goods on behalf of another party).

Attribution & History: The creator of ZeuS possibly uses the alias “Umbro” or “Monstr.”

Worth noting:

- ZeuS is credited for introducing the modular design concept to malware, which allows malicious actors to purchase only the functionality they require.

- The May 2013 extradition of suspected SpyEye developer Hazma Bendelladj from Thailand will likely affect the keylogger market, possibly allowing another keylogger to become dominant, although ZeuS will likely remain a major keylogger threat. (Due to the similarities between ZeuS and SpyEye, SpyEye is not separately discussed in this paper.)

- **Citadel,** a by-product of ZeuS, is used as financial fraud malware and to install other malware, including the Reveton ransomware. According to a McAfee report on Citadel, the creators of Citadel withdrew the program from the open crimeware markets. Along with the fall 2012-early 2013 shift toward European targets, McAfee believes that some Citadel variants are targeting local governments and large private enterprises for the purpose of espionage, which may provide the reason for Citadel disappearing from the crimeware markets. In late May-early June 2013 the FBI and Microsoft announced the disruption of a large Citadel operation, which may diminish the Citadel threat during the 2013 summer months.

Trojans

Carberp is a financially motivated Trojan designed as a competitor to ZeuS.

AKA: none

Malware type: Trojan horse

Objective: financial fraud

Primary Actors: lone hackers

Propagation & Exploit: drive-by download

Activity/Payload: modifies the MBR to avoid antivirus detection and opens a back door on the compromised computer

Variants: none, yet

Attribution & History: first appeared in 2010 and targeted primarily Ukrainian and Russian bank customers.

Worth noting: In late June 2013 researchers found the Carberp source code available for sale, indicating a possible increase in infections is forthcoming during the latter half of 2013. The source code was soon thereafter posted for free, possibly due to the addition of code that will open a backdoor when the person who downloaded it attempted to study or use the Carberp code.

The Security Service of Ukraine (SBU) and the Russian Federal Security Service (FSB) announced the arrest of the gang controlling Carberp in April 2013.

Hiloti is the generic name for a family of Trojan horses that first appeared in 2009 with the primary purposes of downloading additional malware.

AKA: Vundo, Zefarch

Malware type: Trojan horse

Objective: installation of additional malware

Primary Actors: lone hackers

Propagation & Exploit: social engineering, file sharing networks, and other malware

Activity/Payload: search engine poisoning and uses web injects to modify webpages displayed to the user

Variants: multiple

Attribution & History: Hiloti first appeared in August 2009.

Worth noting: N/A

Ponmocup is a Trojan horse and botnet that first appeared in 2009.

AKA: Changeup, Swisyn

Malware type: Trojan horse and botnet

Objective: installation of additional malware (pay-per-install scheme)

Primary Actors: lone hackers

Propagation & Exploit: drive-by downloads, possibly other methods

Activity/Payload: modifies the Windows Hosts file, downloads additional malware

Variants: multiple

Attribution & History: Ponmocup first appeared in August 2009.

Worth noting: Ponmocup employs polymorphism to dynamically generate the links from which it will attempt to download files and has several uniquely modified bytes, which result in constant new file hashes, defeating antivirus protections that rely on file hashes.

Sykipot is malware routinely used by nation-state actors during spear phishing campaigns.

AKA: none

Malware type: Trojan horse

Objective: full system/network access to collect sensitive information

Primary Actors: nation-states

Propagation & Exploit: propagation through links in spear phishing emails with links to malicious files and/or attachments of malicious files; exploits multiple vulnerabilities in Microsoft Excel and Internet Explorer, and Adobe Reader and Flash Player. Exploits have previously included zero-days.

Activity/Payload: provides a backdoor into the network so attackers may issue custom commands and located and exfiltrate sensitive information

Variants: none

Attribution & History: Nation-state actors are suspected to have used Sykipot in targeted spear phishing campaigns since 2007 and possibly 2006.

Worth noting: Known targets in identified Sykipot campaigns include defense contractors, telecommunications, computer hardware, commercial airports, chemical sector, energy sector, and government agencies, including SLTT governments. The spear phishing emails are generally highly targeted, and recipients are often high-rank executives.

Tidserv is a financially motived Trojan horse that uses a rootkit to hide itself.

AKA: TDSS, TDL, Alureon

Malware type: Trojan horse and rootkit

Objective: financial fraud

Primary Actors: lone hackers

Propagation & Exploit: through malicious links to infected or malicious websites, in illegally and peer-to-peer shared files, and accidental drive-by downloads

Activity/Payload: Tidserv profit schemes often involve click fraud and pay-per-install scenarios, which include the display of advertisements and redirecting search results. Tidserv may open a backdoor into the compromised computer.

Variants: multiple

Attribution & History: First reported in September 2008.

Worth noting: Tidserv may affect the Master Boot Record (MBR) to ensure that it can interfere with the loading of the operating system.

ZeroAccess is a Trojan horse with a modular architecture, allowing for Peer-to-Peer (P2P) communication, the creation of backdoors, the installation of fake anti-virus software, and search engine redirections, spambot, and click fraud functions. (This section derives the majority of its information from the MS-ISAC SOC report on ZeroAccess, September 2012, http://msisac.cisecurity.org/resources/reports/documents/ZeroAccess3WhitePaper.pdf.)

AKA: max++, Sirefef

Malware type: Trojan horse with user-mode root kit functionality, forms a botnet

Objective: financial fraud

Primary Actors: lone hackers and organized cyber criminal groups

Propagation & Exploit: execution of a malicious (Trojanized) program or file, or exploit kit

Activity/Payload: ZeroAccess infects the services.exe and explorer.exe processes through a malicious dynamically linked library (DLL) file, and conducts all of its activities through these processes. It installs backdoors, and fakeAV, and facilitates click fraud (it monitors user's searches to provide advertisements from the command and control (C2) server). The traffic redirection feature captures file transfer protocol (FTP) credentials. It creates a hidden folder to store files, and runs as a user-mode rootkit. ZeroAccess may also be used to mine Bitcoins (a popular form of online currency).

Variants: none.

Attribution & History: ZeroAccess first appeared around July 2011. Previous versions of ZeroAccess infected the Windows kernel, affectively hiding itself. Key files were stored in a hidden, encrypted file, which also included a backup copy of ZeroAccess to allow for re-infection, as necessary. The older version of ZeroAccess also provided self-defense through a bait process. If another program attempts to open this process, ZeroAccess injects code into the program, terminating it, and changes the program's permissions so that it could not be executed.

Worth noting: Requests to the C2 servers are disguised as hypertext transfer protocol (HTTP) traffic to a randomly generated domain name. The P2P communication feature decentralizes distribution, which makes it difficult for law enforcement and cyber security groups to track.

Worms

Conficker is a worm that infects a network, primarily through flaws in services or hosts on the network.

AKA: Downadup, Downup, Kido

Malware type: worm and botnet

Primary Actors: lone hacker and organized cyber criminal groups

Objective: spam generation, installation of financial fraud malware and fakeAV

Propagation & Exploit: flaws in Windows, and dictionary attacks against administrator passwords

- Conficker.A exploited a just-patched Windows vulnerability but the variants expanded to exploit multiple vulnerabilities.

Activity/Payload:

- In 2009, Conficker received a fair amount of news coverage due to a report that the worm would update itself on April 1, 2009. The update did not occur but Microsoft estimated there were still seven million infected machines on April 1, 2012.

- Conficker.A propagates by brute-forcing commonly used network passwords and through removable media.

- Conficker.E downloaded Waledact (spam generating and financial fraud malware), and successfully accomplished Conficker.A's objective of downloading the fakeAV product, SpywareProtect 2009.

Variants: Conficker includes five variants, .A, .B, .C, .D, and .E, with .E released in April 2009. The Conficker Working Group uses an alternate variant naming scheme that identifies Conficker.C as Conficker.B++, Conficker.D as Conficker.C and Conficker.E as Conficker.D.

- Every day Conficker.A and .B dynamically generate a new list of C2 domains from which the computer was supposed to receive files. The Conficker Working Group sinkholed all possible C2 domains before the malicious actors behind Conficker could use them, thus preventing the infected computers from receiving instructions. In response, Conficker.D generated a much larger pool of possible domains, with computers trying to connect with a C2 on one of 500 domains per day. Additionally, Conficker.D included P2P communication infrastructure.

Attribution & History: Conficker was first detected in November 2008.

Worth noting: Automated removal of Conficker is difficult because Conficker disables Windows system security services, third party firewalls, and anti-virus products, and blocks access to computer security sites, which prevents users from downloading removal tools.

Scams

Internet Scams continue to target individuals, companies, and SLTT government agencies. With the inclusion of social networking information these scams can appear incredibly realistic. The following are newer variants that target SLTT agencies, although the standard scams are still practiced and highly successful. In all of these scams, information gathered from social media websites provide key details that convince the victims that the malicious actor is providing accurate information and should be trusted.

The **Domain Registration Scam** is a common scam targeting SLTT agencies; it involves a letter or email from a domain registration company, generally located in China, that claims someone is trying to register a domain similar to the one the SLTT agency uses. The letter asks for the recipient to respond as to whether this registration violates any brand or trademark concerns and offers the recipient the opportunity to register the Chinese domains themselves, in order to protect their name. The scam is that the SLTT agency does not need Chinese domains and the registration fee is higher than market rate, generally around $15-20 per registration with the letter suggesting 5-10 registrations.

Risk of occurrence: high probability of occurrence

Impact: low impact event

Objective: financial fraud

Primary Actors: foreign non-cyber actors

Worth Noting: N/A

Scams on Classified Ad sites affect SLTT governments, commonly through the posting of falsified hiring notices or exams that the advertisement claims are necessary to apply for open SLTT government positions.

Risk of occurrence: low-medium probability of occurrence

Impact: low impact event for the government agency, potential medium impact event on the victims, especially if they are targeted for future malicious activity

Objective: financial fraud and collection of PII

Primary Actors: lone hackers, organized cyber criminal groups, non-cyber actors

Worth Noting: These scams may result in falsified employment where the “employee” unwittingly becomes part of additional illegal activity.

In the **Purchase Order Scam** there are two victims, the company the scammers pretend to be (Agency A) and the company being scammed (Company B). The scammers create a purchase order that appears to come from Agency A. They send the purchase order to Company B, with a request to purchase thousands of dollars in supplies for shipment to another location, generally overseas. Company B fulfills the order and ships the goods. When Company B does not receive payment, Company B contacts Agency A demanding payment, and at some point the scam is discovered.

Risk of occurrence: low probability of occurrence

Impact: low impact event affecting Company A's reputation and Company B's finances

Objective: financial fraud

Primary Actors: organized cyber criminal groups, non-cyber actors

Worth Noting: The scam may involve fake websites and other supporting documentation to provide authenticity to the purchase order request.

Debt Collection and **Payday Loan Scams** target victims, claiming the victim owes the malicious actor several thousand dollars. The malicious actors are known to call the victim at work, and may harass co-workers or other employees, and threaten physical violence. The malicious actors may also show up at the work place, or could threaten or attempt to include police involvement.

Risk of occurrence: low probability of occurrence

Impact: potential medium-high impact on personnel at the affected agency, as collectors include threats of physical violence

Objective: financial fraud

Primary Actors: lone hackers, organized cyber criminal groups, non-cyber actors

Worth Noting: In some cases the victim did apply for a payday loan or has defaulted on a debt, but in many cases the victims have no prior contact with scammers and have no debts nor applied for a loan.

SLTT government senior executives can be victims of **Social Networking Scams** where fake profiles are created in the name of the executive. Malicious actors have used fake social networking site profiles of public figures to trick residents into sending money to fake charities or to post misleading information about the SLTT government.

Risk of occurrence: low probability of occurrence

Impact: event impact depends on the success and purpose of the false profile with fake charities resulting in limited impacts on the government agency and individual victim and misleading information potentially resulting in high impacts on the government and individual victims

Objective: financial fraud

Primary Actors: unknown

Worth Noting: N/A

Actors and Motivations

Discussions of cyber crime actors generally classify the actors into several categories: script kiddies, insiders, hacktivists, lone hackers, organized cyber criminal groups, nation-state hackers, and terrorists. Different organizations define the groups based on their internal needs and experiences, which is why the classification names vary, but no matter the name, SLTT governments are at risk from these groups.

Script kiddies are unskilled hackers. They act out of interest and a desire for recognition and rely on scripts, programs, or very simple techniques. Script kiddies are known for defacing websites but may also attempt other simple malicious activity. The term “script kiddie” is considered derogatory.

While **insiders** may or may not have significant hacking skills but their access to sensitive networks poses a significant threat. Insider cases include the theft of information for industrial espionage purposes, blackmail and extortion by disgruntled employees, destruction of data, and the illicit use of equipment for alternative purposes, such as running a botnet. Any employee could be an insider, regardless of age, income, position, computer/cyber skills, or network access. Insiders can pose a significant threat to SLTT governments.

The **hacktivist** believes in a specific ideology and associates with others with that same ideology, however, some hacktivist groups are geographically affiliated. Together they form groups to conduct operations for the purpose of drawing attention to their ideology or to achieving some set goal, such as stopping an activity or embarrassing a person or entity. The majority of hacktivists do not use sophisticated techniques, but this does not negate the hacktivist threat to SLTT governments, or the hacktivists ability to cause significant damage or embarrassment to their targets.

The **lone hacker** is someone who generally acts out of interest, a desire for recognition, or for financial profit. Hackers-for-hire (professional, independent actors who hire out their services) also fall within this category. Individual hackers may be extremely skilled and pose a significant risk to SLTT governments, or they may be script kiddies, hackers without any skills who pose a minimal risk to SLTT governments.

Organized cyber criminal groups are criminal syndicates formed to conduct cyber crime. These groups may be referred to as transnational cyber criminals in other documents. They groups have a strong hierarchy, distinct divisions of labor, and may employ members to fulfill specific needs on a one-time basis, not unlike traditional organized crime organizations. They conduct large-scale cyber crime schemes such as running ZeuS botnets and auction fraud. Organized cyber criminal groups may pose an unintentional threat to SLTT governments if the government is accidentally affected by the group's activity through indiscriminant infection techniques, such as malvertising. A small subset of organized cyber criminal groups target government agencies, primarily for financial fraud.

Nation-state hackers who conduct computer network exploitation (CNE) for the purpose of foreign espionage currently pose a significant threat to SLTT governments. Nation-state hackers, sometimes referred to as Advanced Persistent Threat (APT) actors, attempt to steal secrets from United States entities in order to advance their own country's development. The hackers may be members of a foreign military, government, or consultants, and seek to achieve long-term, deep compromises of the organizations they target. SLTT governments may be compromised due to contractual negotiations for projects, insight into new technology (i.e. plans for the new laboratory which is receiving government tax incentives), for political or economic purposes, as a pivot point for another compromise, or accidentally. Nation-state actors pose the highest, consistent cyber threat to state and territorial governments, and currently an unknown level of risk to local and tribal governments.

Skilled hackers belonging to traditional **terrorism organizations** are currently rare, but will likely become a more significant threat within the next 1-3 years as the current group of web defacers gains a broader skill set. Terrorist hackers are likely to target critical infrastructure and government operations in computer network attacks (CNA) with the intent to create as much harm as possible. Iranian hackers and members of some hacktivists groups can also be considered e-terrorists or e-jihadists, the terms used to refer to hackers who act on behalf of or for a terrorist organization. Terrorist organizations have professed the intent to conduct cyber attacks against SLTT governments, and certain terrorist organizations have demonstrated the capability to successfully attack critical infrastructure. There is not, as of yet, a clear indication of the risk to SLTT governments by terrorists.

Definitions

Exploit kits combine the delivery of malicious payloads with methods to search for and exploit vulnerabilities. The kits allow unskilled malicious actors to easily attack and compromise computers and websites. Kit vendors may rent or sell the kits and provide updates incorporating the latest vulnerabilities and malware.

Fake Antivirus (fakeAV) software, is a form of scareware. FakeAV may use a pop-up message, spam email, links on social networking sites, or compromised websites to install or convince the user to install the fakeAV. Commonly fakeAV convinces a user that they have a virus or other malware on their computer so that the user purposefully downloads the fakeAV to clean the computer. This can occur through "scans" of the computer listing numerous fictitious threats needing immediate attention, fake "reboots" (a series of images are displayed making it appear the computer is rebooting) resulting in "system error messages," "stuck" screens (images that show the Blue Screen of Death), real reboots that result in icons and desktops "disappearing" (images of the desktop without any icons are displayed), or the malware may prevent legitimate applications from running, triggering legitimate warnings.

FakeAV charges the user a fee for the "antivirus" software; in an effort to appear legitimate many fakeAV programs have official looking websites, offer users the opportunity to purchase varying levels of "protection," and may even provide live support to answer customer questions and call centers to cold call users. Aside from simply losing money, users who pay with their credit cards may compromise their personally identifiable information (PII) and be exposed to additional fraud. An unwary user may pay for the fakeAV with their government credit card, creating an opportunity to identify fakeAV installations by working with the finance department to spot unusual credit card charges. Installations paid for by government cards may also expose the government agency to additional financial fraud; credit cards used in these schemes should be immediately cancelled.

Keystroke loggers (a.k.a. keyloggers) are malware that record all keys typed on a computer. Keyloggers send this information "home," which provides malicious actors with login names, passwords, and other sensitive information. While keyloggers can be used for espionage and other purposes, the majority of incidents involving keyloggers are related to financial fraud. Losses range from a few thousand to millions of dollars in a single incident. Small businesses and government agencies, including schools, are primary targets, although malicious actors also target personal retirement and investment accounts.

Keylogger financial fraud generally involves what initially appears to be a legitimate automated clearinghouse or wire transfer from the victim's bank account to one or more other entities. The financial trail may include a United States-based destination but will typically lead overseas; Russia, China, and the Ukraine are common destinations. The malicious actors frequently access the compromised account through a proxy server or another victim's computer to prevent attribution. Financial institutions may be able to recall transfers if the transfers are reported to the financial institution before the overseas actors retrieve the funds, which can occur within hours of the transfer.

Of note, some financial fraud groups modify the victim's information with the financial firm so that confirmation telephone calls are redirected to the malicious actors. In a similar variant, the victim is overwhelmed by telephone calls containing white noise or recorded sounds, preventing the bank from confirming the transaction.

Other password stealers with similar functionality as the keyloggers discussed below include Ice IX, Citadel, and Carberp. Variations on standard keyloggers include Man-in-the-Browser (MitB) malware, which only collects data entered into a web browser, and Man-in-the-Mobile (MitMo), which only collects short messaging service (SMS) traffic from smartphones.

Polymorphic code is programming code that mutates each time the code is run. This results in polymorphic malware that appears different each time it is run, although the capabilities of the malware do not change, allowing the malware to defeat traditional signature-based malware detection methods.

Ransomware is malware that locks a computer and demands a ransom in exchange for the password. In 2012, Reveton, a common version of ransomware, claimed to originate with police departments or the Federal Bureau of Investigation (FBI) and claimed the user committed illegal activity for which they had to pay a fine. The ransomware claimed that once the user paid the fine their computer would be unlocked. In May 2013, Total Defense discovered malware that combined the effects of fakeAV with ransomware, resulting in malware that attempts to trick users into purchasing fake antivirus, and if that fails, locks the user's computer and demands a ransom to release the system.

Rootkits are stealth malware designed to hide other malware while remaining hidden themselves. User-mode rootkits can overwrite the memory of a targeted application, while kernel-mode rootkits add code to or replace the code of core operating system functionality. In both cases, this parasitic technique helps hide the rootkit from traditional antivirus programs.

Scareware is malware that intends to scare the user into taking further action, generally installing software, that is malware in disguise, or paying a fine.

Summary

Cyber crime encompasses a broad array of actors and actions. Appropriate security, precautions, and monitoring will significantly decrease the potential of being victimized. If an incident does occur, SLTT governments should notify the CIS SOC immediately, and law enforcement officials when appropriate. (The CIS report an incident form is located here http://msisac.cisecurity.org/about/incidents/.) A quick response, a little luck, and the preservation of evidence to uncover the extent of the damage can turn a potentially significant event into a minor disturbance.

For additional copies or to download this document, please visit:

http://msisac.cisecurity.org/resources/guides