MS-ISAC®

Cybercrime Technical Desk Reference

August 31, 2018

This guide is intended as a desk reference for state, local, tribal, and territorial (SLTT) governments in order to provide a basic introduction to recent cybercrime activities. This information is provided to further the reader's understanding of notifications issued by the Multi-State Information Sharing and Analysis Center (MS-ISAC) relating to cyber threats and to raise the reader's awareness of the malicious actors, motivations, malware, and fraud schemes. The information in this desk reference is divided into cybercrime categories and sorted alphabetically within those categories.

Table of Contents

MALWARE

Malware is software designed to perform malicious actions on a machine. Examples of malicious actions include stealing sensitive information, opening unauthorized connections, or downloading additional malware. The format in which malware will be listed is below.

Malware Name (year first observed) information about the malware AKA: other names associated with malware Variants: known malware variants Malware Type: category of malware based on malware capabilities Objective: targeted use of malware Primary Actors: cyber threat actors that use malware Propagation & Exploit: vectors used by malware Activity/Payload: known malware actions Attribution & History: Malware context and analysis

Botnets

Botnet malware opens connections on devices, allowing malicious actors to send instructions to the infected devices using a command and control (C2) server. A botnet infected device is called a zombie and most owners of zombie devices are unaware that their device is infected and being used in a botnet. C2s issue commands to the zombie steal data, or direct it to send spam or help with a distributed denial of service (DDoS) attack, which can result in the IP address or email domain being blacklisted.

Andromeda (2011) uses its modular design to compromise victims. Communication with the C2 is done with encryption and over HTTP protocol.
AKA: Win32/Gamarue
Variants: None
Malware Type: botnet
Objective: financial, credential theft
Primary Actors: cybercriminals
Propagation & Exploit: malspam, malvertisement
Activity/Payload: Andromeda uses several modules including keyloggers, form grabbers, rootkits, and proxy modules. Andromeda can also be loaded with a module that is used to update other malware. It uses RC4 encryption on its HTTP network traffic.
Attribution & History: Andromeda and its modules are available for purchase via underground forums. In 2014, with version 2.8, Andromeda started targeting the payment card industry.

Conficker (2008) infects a network primarily through flaws in services or hosts on the network. It is known to infect out-of-date devices.
AKA: Downadup, Downup, Kido, Downad
Variants: multiple
Malware type: botnet worm
Primary Actors: cybercriminals
Objective: spam generation,
Propagation & Exploit: network
Activity/Payload: Conficker drops a copy of itself into the Recycle Bins of all drives connected to the infected machine's removable and network drives. It executes whenever a user browses an infected network drive. It connects to a server or peer to receive a binary update. The instructions it receives may direct it to propagate, gather personal information, or to download and install additional malware onto the infected machine.

Attribution & History: Conficker was first detected in November 2008 and targets outdated systems. Removal of Conficker is difficult because Conficker disables a number of system services such as Windows Automatic Update, Windows Security Center, Windows Defender, and Windows Error Reporting, as well as third-party firewalls and anti-virus products.

Kelihos (2010) is a peer-to-peer botnet malware that used a hybrid peer-to-peer C2 network in order to decentralize its infrastructure.
AKA: none
Variants: none
Malware Type: botnet
Objective: financial, botnet, credential theft, spam, ransom
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Kelihos was used to carry out spam campaigns, such as pump and dump schemes. It also carried out credential theft, as well as the propagation of ransomware.
Attribution & History: The Kelihos botnet was partially shut down after a U.S. Department of Justice (DOJ) operation ended with the arrest of the operator and the sinkholing of infected devices. At its peak, it had infected over 100,000 devices worldwide.

Mirai (2015) is botnet malware known to compromise insecure, networked Internet of Things (IoT) devices running Linux in order to conduct large-scale DDoS attacks. Mirai is dropped after an exploit has allowed the attacker to gain access to a machine.
AKA: none
Variants: multiple
Malware Type: botnet
Objective: botnet propagation, service disruption
Primary Actors: cybercriminals
Propagation & Exploit: network
Activity/Payload: Mirai scans the Internet looking for known vulnerable IoT devices. Once a device is found, Mirai runs an exploit style package against IoT devices, focusing mainly on default credential brute forcing, as default credentials are a known issue amongst IoT devices.
Attribution & History: Mirai is known for a DDoS attack that resulted in a partial Domain Name System (DNS) infrastructure outage in October 2016, which led to a slowdown in Internet activity across the U.S. After the attack, Mirai source code was posted on hackforums[.]net, leading to multiple users utilizing the Mirai source code to build out additional botnets.

Necurs (2012) is the world's largest spam botnet, with an estimated six million zombies. Its complexity and constant reinvention has kept it as one of the top botnet operations.
AKA: none
Variants: none
Malware Type: backdoor
Objective: financial, botnet, denial of service, ransom, spam
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Necurs performs many activities, including being a spam distributer for the Dridex banking trojan and ransomware. It has a DDoS component and has been involved in pump and dump scams related to low-end penny stocks or obscure cryptocurrencies.
Attribution & History: Necurs is known for its technical complexity. Unlike common botnet malware, Necurs has kernel-mode rootkit capabilities. Its modular architecture allows for versatility and instead of one domain generation algorithm (DGA), as seen in several malware families, Necurs uses 2 DGAs and a hardcoded set of domains for a fallback.

Ponmocup (2006) is a downloader associated with one of the largest and longest running botnets, active since 2006.
AKA: Vundo, Virtumonde
Variants: none
Malware Type: downloader
Objective: botnet propagation, financial
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement
Activity/Payload: Ponmocup is difficult to detect due to its use of different encryption types per infected system. Ponmocup uses one-time domains for installation, which means domains cannot be used for indicators of compromise. The most actively developed plug-in is for advertisement fraud.

Exploit Kits

Exploit kits (EK) are a type of malicious toolkit that cyber threat actors use in order to discover and exploit vulnerabilities in systems for the purpose of spreading malware. These kits usually target commonly insecure or outdated software applications, such as Java, AdobeFlash, and Silverlight, in order to find a route to privilege escalation and further exploitation. The EK landscape started to decline in June 2016 with the disappearance of the Angler EK.

Angler (2013) **-RETIRED-** was one of the most notorious EKs due to its wide distribution and high usage.
AKA: none
Variants: none
Malware Type: exploit kit
Objective: identity theft, credential theft, ransom, botnet
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement
Activity/Payload: Angler was a versatile EK that was able to install malware, collect data, or tie the system to a botnet. It was able to install many types of malware and was one of the first EK to integrate zero-day vulnerabilities. Furthermore, Angler kept a very fluid distribution infrastructure, making it hard to block.
Attribution & History: Angler first arrived in 2013 and was halted on June 7, 2016, with the arrest of the Lurk group. Angler was a Malware-as-a-Service, which allowed non-technical users access to malware campaigns without having the technical knowledge for delivery. Angler was known for its versatility, as demonstrated in April 2015 when it was used to drop over 10 different malware families.

DNSChanger (2007) is malware that was very prolific in the late 2000s and early 2010s, before being dismantled by a FBI takedown. A new variant was identified in December 2016, which acts as an EK targeting routers. Once infected, the routers' DNS records are modified to point to a malicious server. DNSChanger is disseminated via malvertising and uses steganography to obfuscate its initial actions.
AKA: none
Variants: none
Malware Type: exploit kit
Objective: man in the middle, financial
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement
Activity/Payload: Unlike most EKs, DNSChanger does not attack the operating system or browser, but attacks the victim's home or small office (SOHO) router. DNSChanger uses an infected advertisement on a website to redirect the victim to a page infected with DNSChanger. DNSChanger fingerprints the router in order to execute the proper exploit and change DNS settings. Once changed, this allows

cyber threat actors to redirect users to ads controlled by the actors and also conduct man-in-the-middle attacks on all systems behind the compromised router.
Attribution & History: DNSChanger started as a DNS hijacking trojan distributed by drive-by downloads that modified the system's DNS configuration to point to rogue name servers operated by the cyber threat actor. This version of DNSChanger shutdown after a joint operation by the Federal Bureau of Investigation (FBI) and Estonian Police called Operation Ghost Click. DNSChanger resurfaced in December 2016 as an EK.

RIG (2013) attempts to compromise a system by redirecting victims through gates to the EK and exploiting vulnerabilities in JavaScript, Flash, and VBscript. RIG rose to prominence due to the EK reshaping in 2016.
AKA: Goon
Variants: none
Malware Type: exploit kit
Objective: identity theft, credential theft, ransom
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement
Activity/Payload: RIG combines different web technologies, such as JavaScript and Flash, to obfuscate its attack. Furthermore, RIG changes scripts with each attack session making it impossible to detect through hash values. RIG payloads mostly include ransomware.
Attribution & History: The EK had similarities to the Redkit and Dotcache EKs, using a JSON Web Signature (JWS) bypass. RIG's infection rate in 2015 was much lower than Angler's. RIG took advantage of the EK reshaping in 2016 and is considered one of the top EKs in use as of May 2018.

Sundown (2015) is delivered through a malicious iframe. Sundown rose to prominence due to an increase in sophistication after the takedown of Angler.
AKA: none
Variants: none
Malware Type: exploit kit
Objective: identity theft, credential theft, ransom
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement
Activity/Payload: Sundown become more sophisticated by stealing exploits from other EK and using recently expired domains in good standing in order to avoid blacklists. Unlike most EKs that focus on a single exploit on a system after fingerprinting, Sundown executes all exploits on a victim instead of scanning and choosing the proper exploit.
Attribution & History: Sundown became less popular after its source code was leaked in February 2017.

Ransomware

Ransomware is a type of malware that blocks access to a system, device, or file until a ransom is paid. This is achieved when the ransomware encrypts files on the infected system (crypto ransomware), although some variants erase files (wiper), or block access (locker ransomware) to the system using other methods. If the crypto ransom is not paid within a specific time frame, the cyber threat actors will destroy the decryption keys, making decryption impossible. If the wiper ransomware is not paid within a specific time frame, the ransomware generally starts permanently deleting files. Currently, there are opportunistic and strategic forms of ransomware. Check https://www.nomoreransom.org to see if a decryption tool exists for a particular version of ransomware. When uploading a test file to any website ensure the file does not contain sensitive or protected information.

Cerber (2016) is evasive, crypto ransomware that is capable of encrypting files in offline mode and is known for fully renaming files and appending them with a random extension. There are currently six versions of Cerber and it has evolved specifically to evade detection by machine learning algorithms.
AKA: none
Variants: Cerber1, Cerber2, Cerber3, Cerber4, Cerber5, Cerber6
Malware Type: opportunistic crypto ransomware
Objective: financial, ransom, service disruption
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Cerber 6 uses Window's Cryptographic Application Programming Interface (CryptoAPI) for encryption and does not attack the Volume Shadow Copy Service (VSS) copy of an infected computer. The decryption key can be sniffed on a network during the encryption process. Only Cerber1 has a decryptor available.
Attribution & History: Cerber was released in March 2016. It is distributed via a Ransomware-as-a-Service model. Cerber5 and earlier use RSA 512 cipher as well as RC4 encryption. Cerber6 has added several processes focusing on stealth techniques and has gone from implementing RC4/RSA 512 to using CryptoAPI.

Cryptowall (2014) is crypto ransomware that not only encrypts files on the infected machine, but also any connected file shares or drives.
AKA: Cryptorbit, CryptoDefense
Variants: none
Malware Type: opportunistic crypto ransomware
Objective: financial, ransom, service disruption
Primary Actors: cybercriminals
Propagation & Exploit: malspam, dropped, network
Activity/Payload: Cryptowall uses unbreakable AES encryption and deletes all restore points on the machine.
Attribution & History: CryptoWall provides a free single-use decryption service to prove that the key works on hijacked files. (Uploading a file containing sensitive or protected information could result in a data breach) It gained notoriety after CryptoLocker was taken down by Operation Tovar.

CryptXXX (2016) is known for trying to find and encrypt files in shared drives via scanning Server Message Block (SMB) on port 445. Once a file has been encrypted, an extension is attached to the end.
AKA: UltraCryptor
Variants: CryptXXX 1.0, CryptXXX 2.0, CryptXXX 3.0
Malware Type: opportunistic crypto ransomware
Objective: financial, ransom, service disruption
Primary Actors: cybercriminals
Propagation & Exploit: malspam, dropped, network
Activity/Payload: CryptXXX is a virulent crypto ransomware that has the ability to spread across an organization's network through critical vulnerabilities in Windows computers. Current variants encrypt over 175 different file types as well as attacking Windows VSS so that the user cannot use backups.
Attribution & History: CryptXXX was released in April 2016. It was initially part of a malware bundle being pushed out by the Angler EK. The first three variants of CryptXXX have been cracked and free decoders released.

Dharma (2016) is a crypto ransomware from the Crysis/Dharma family that encrypts all files located on the local drives as well as shared network dives. Dharma also deletes all Shadow Copies so that the user cannot restore from them.
AKA: Crysis

Variants: none
Malware Type: strategic crypto ransomware
Objective: financial, ransom
Primary Actors: cybercriminals
Propagation & Exploit: dropped, malspam
Activity/Payload: Dharma uses RC4 encryption.
Attribution & History: The master decryption keys for Dharma have been released.

Locky (2016) is crypto ransomware delivered via the Necurs botnet as well as on social media via malicious image files. Osiris is the 7th generation of Locky, and due to strong encryption, it cannot be decrypted by third-party tools. Locky is currently using a RSA-2048 + AES-128 cipher with electronic code book (ECB) mode to encrypt files.
AKA: none
Variants: .thor, .locky, .bart, .zepto, .perl, .odin, .osiris
Malware Type: opportunistic crypto ransomware
Objective: financial, ransom, service disruption
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Locky is evasive due to its uses of standard Windows components such as scripts and libraries in order to download and execute its payload. It also has obfuscations built in to evade detection when in a virtualized environment. Locky is known to spread across a network as well as across organizational boundaries. Furthermore, it also attacks Windows VSS.
Attribution & History: Locky was released in February 2016. Locky has seven iterations and has used many different distribution methods including EKs, malspam using malicious documents with embedded macros and zipped JavaScript attachments, and through social media. It is considered particularly evasive.

NotPetya (2017) leveraged the EternalBlue exploit and Mimikatz tool to extract credentials to be used with PsExec in order to spread across a network.
AKA: SortaPetya, Petna, ExPetr, Diskcoder
Variants: none
Malware Type: opportunistic wiper ransomware
Objective: data wipe
Primary Actors: nation-state
Propagation & Exploit: dropped, network
Activity/Payload: NotPetya encrypts the Master File Table (MFT) for NTFS partitions and overwrites the Master Boot Record (MBR) with a custom bootloader.
Attribution & History: NotPetya infected machines in over 100 countries and caused billions of dollars in damage. The U.S. attributed the attack to the Russian military. NotPetya is associated with a singular campaign that occurred on June 17, 2017, and no subsequent attacks are known to have occurred.

SamSam (2016) is strategically placed crypto ransomware that tends to affect the SLTT governments and the healthcare industry. The attackers opt for higher dollar amounts and manual control over the attacks instead of the more common opportunistic approach with smaller ransom demands. The targeted entities receive custom ransoms with varying demands.
AKA: Samas, Samsa
Variants: none
Malware Type: strategic crypto ransomware
Objective: financial, ransom, service disruption
Primary Actors: cybercriminals
Propagation & Exploit: dropped

Activity/Payload: SamSam is deployed either by leveraging JexBoss and other Java-based application platforms in order to exploit and install a remote shell on the server or through brute forcing Remote Desktop Protocol (RDP) service passwords. The server is then leveraged to laterally move through the network, infecting Windows machines with SamSam. It also locates and destroys backups.
Attribution & History: SamSam is one of the only types of ransomware that does not use malvertisments or malspam for delivery. The attackers are known for neogitating payment options with the victim.

Virlock (2014) is a polymorphic crypto ransomware virus that is known for its virulence.
AKA: Virul, VirRansom
Variants: none
Malware Type: opportunistic crypto ransomware
Objective: financial, ransom, service disruption
Primary Actors: cybercriminals
Propagation & Exploit: malspam, network
Activity/Payload: Virlock's virulence is due to the virus not only encrypting the files, but also copying the file and making an .exe version that is loaded with the virus. This increases the chances of users spreading the virus.
Attribution & History: The most recent version of Virlock can spread through cloud sync, cloud storage, and collaboration applications.

WannaCry (2017) leverages the EternalBlue exploit that was made public in April 2017 by the ShadowBrokers. It was the first major cryptoworm exploiting EternalBlue.
AKA: WannaCrypt, WanaCrypt0r, WCrypt, WCRY
Variants: none
Malware Type: opportunistic crypto ransomware worm
Objective: financial
Primary Actors: nation-state, cybercriminals
Propagation & Exploit: malspam, network
Activity/Payload: WannaCry uses AES-128 encryption in cipher block chaining (CBC) mode.
Attribution & History: The U.S. government attributed the original WannaCry campaign to North Korea. Subsequent infection campaigns are attributed to the wormability of WannaCry and its use of the EternalBlue exploit against the CVE-2017-0143 vulnerability. WannaCry was rendered incapable of encryption through the use of a "killswitch." Though due to the way proxy servers work, non-updated systems behind a proxy server are still vulnerable.

Trojans

Trojans is malware that try to disguises itself as legitimate software or operations. Trojans try to delete, block, modify, or copy data, or otherwise disrupt the performance of computers. Traditional trojans were incapable of self-replication, though newer trojans have incorporated spreader modules for wormability.

Bedep (2013) comes in a 32- or 64-bit version. Bedep downloads other malware and has been associated with the Ursnif and Fareit trojans.
AKA: Rozena
Variants: none
Malware Type: backdoor
Objective: downloader, botnet
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement
Activity/Payload: Bedep is made up of dynamic-link libraries (.dll) and can be loaded directly in memory by exploit code.

Attribution & History: In December 2016, according BitSight, Bedep was seen in one out of every five Fortune 1000 companies. Bedep has not been in the MS-ISAC Top 10 Malware since September 2016.

CoinMiner (2014) campaigns continue to proliferate since the increased value of cryptocurrencies. CoinMiner has evolved from originally mining bitcoin to now mining Monero.
AKA: none
Variants: multiple
Malware Type: cryptocurrency miner
Objective: financial
Primary Actors: cybercriminals
Propagation & Exploit: malspam, network, dropped
Activity/Payload: CoinMiner's payload is a common application to mine cryptocurrency that the actor is using maliciously and without authorization.
Attribution & History: CoinMiner initially mined bitcoin, but has subsequently changed to mining Monero.

Dridex (2014) leverages macros in Microsoft Office to infect machines.
AKA: Bugat
Variants: Cridex
Malware Type: banking trojan
Objective: financial, credential theft
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Dridex can utilize DNS cache poisoning to direct users from legitimate banking websites to fake ones. Dridex also utilizes keylogging and web injection to steal banking credentials.
Attribution & History: A partial takedown of Dridex occurred in late 2015, which did not affect its distribution.

Emotet (2014) is a modular trojan that downloads or drops banking trojans. Initial infection occurs via malspam emails that contain malicious download links, a PDF with embedded links, or a macro-enabled Word attachment. Emotet incorporates five spreader modules in order to propagate throughout a network. Emotet actors actively update the malware with new features.
AKA: Heodo
Variants: Geodo
Malware Type: infostealer
Objective: malware propagation, credential theft, financial
Primary Actors: cybercriminals
Propagation & Exploit: malspam, network
Activity/Payload: As Emotet evolves in functionality it keeps adding spreader modules. This builds on a recent trend of adding propagation tools and techniques to ransomware that crimeware is adopting.
Attribution & History: Emotet is in the same family of malware as Dridex and was regionally isolated in Europe around Germany. In early-April 2017, a campaign targeted the United Kingdom (UK) before surfacing in the United States in mid-April 2017. Emotet quickly became one of the most prevalent malware affecting SLTT governments.

Fleercivet (2014) opens a hidden Internet Explorer window and injects itself into browser memory processes while setting up a backdoor on the device.
AKA: none
Variants: A, B
Malware Type: backdoor
Objective: spyware, click fraud

Primary Actors: cybercriminals
Propagation & Exploit: malvertisement
Activity/Payload: Fleercivet causes browsers to open hidden windows to websites containing advertisements, allowing the actor to generate advertisement revenue.
Attribution & History: In early 2017, Fleercivet attacked the Chrome browser, social engineering users to download either BrowserMe.exe or Chrome_Font.exe.

Gh0st (2001) is a remote access trojan (RAT) used to control infected endpoints.
AKA: PCRat, GhostRAT
Variants: multiple
Malware Type: RAT
Objective: malware propagation, botnet, espionage
Primary Actors: cybercriminals, nation-state
Propagation & Exploit: dropped
Activity/Payload: Gh0st allows an attacker to take full control of infected systems, log keystrokes, provide live webcam and microphone feeds, and download and upload files.
Attribution & History: Gh0st obfuscates client-server communications and has seen an uptick of activity since 2017. In 2015, Threatlabs released a report stating that nation-state actors were using over 32 variants of Gh0st, although the source code is now openly available and most infections are not related to nation-state activity.

Hancitor (2014) is disseminated via malspam containing a malicious macro attachment and is known to obfuscate itself using PowerShell commands.
AKA: Chanitor, Tordal
Variants: none
Malware Type: downloader
Objective: financial, credential theft
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Hancitor contains a macro script that downloads additional malware.
Attribution & History: In 2018, Hancitor is known to download the ZeuS banking trojan.

Kovter (2014) is a click fraud trojan disseminated via malspam email attachments containing malicious office macros. Kovter is fileless malware that evades detection by hiding in registry keys and using hooks within certain APIs for persistence. Some reports indicate that Kovter infections have received updated instructions from C2 infrastructure to serve as a remote access backdoor.
AKA: none
Variants: none
Malware Type: click fraud
Objective: click fraud, financial
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Kovter is loaded with an encoded resource segment containing configuration settings for the malware. Most IPs stored in Kovter's resource segment are not legitimate C2 addresses. All C2 communication occurs over SSL using port 443.
Attribution & History: Kovter is one of the first fileless malwares that reside in memory and run from the system registry rather than on the disk. This evasion technique is used to evade file-based malware detection products.

Nemucod (2015) is commonly spread through malspam containing malicious attachments that execute heavily obfuscated JavaScript.
AKA: none

Variants: none
Malware Type: downloader
Objective: downloader
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Nemucod delivers Locky, Pony, Emotet, and Ursnif.
Attribution & History: In April 2017, the MS-ISAC noted a Nemucod campaign using the MS-ISAC name to download Emotet.

Pony (2012) is known for its association with the Hancitor downloader and Vawtrak banking malware.
AKA: Fareit, Evil Pony
Variants: none
Malware Type: downloader
Objective: financial, malware propagation, credential theft, DDoS
Primary Actors: cybercriminals
Propagation & Exploit: malspam, dropped
Activity/Payload: Pony has many modular components that can be used, including credential harvesting and DDoS components. Pony is highly associated with Vawtrak.
Attribution & History: In early 2017, malspam campaigns had malicious macro Word documents attached to them that downloaded Hancitor, which then downloaded Pony, which in turn followed up with Vawtrak.

Qakbot (2011) is financial malware designed to target governments and businesses for financial fraud and known for its wormability on a network.
AKA: Qbot; Pinkslipbot; Bzud
Variants: none
Malware type: banking trojan
Primary Actors: cybercriminals
Objective: financial fraud
Propagation & Exploit: malspam, dropped, network
Activity/Payload: Qakbot installs a keylogger to steal user credentials. It monitors network traffic, specifically traffic to online banking websites and can piggyback on a user's active banking session by intercepting authentication tokens, facilitating financial fraud.
Attribution & History: Since February 2018, Qakbot is being spread via Emotet as well as using its own self-spreading capabilities.

Sofacy (2014) is a malicious .dll trojan dropped by specially crafted documents (.rtf, .doc, .docx, .pdf). The trojan is associated with the Russian nation-state group known as Fancy Bear or APT 28.
AKA: Carberp, SofacyCarberp
Variants: none
Malware Type: nation-state
Objective: espionage
Primary Actors: nation-state
Propagation & Exploit: malspam
Activity/Payload: When executed, Sofacy connects to a remote location and gathers computer information to send to the remote attacker. The trojan then downloads and executes malicious files from a remote site.
Attribution & History: The group behind Sofacy is attributed with the Democratic National Committee (DNC) compromise disclosed in 2016. Sofacy is a first-stage tool used by APT 28.

Terdot (2015) is associated with the ZeuS banking trojan.

AKA: Zloader, Terdot.A
Variants: none
Malware Type: downloader
Objective: downloader, financial
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement
Activity/Payload: Terdot mostly downloads the ZeuS banking trojan. It has also implemented credential harvesting features as well as social media account monitoring functionality.
Attribution & History: Terdot avoids attacking computers that have the Russian language pack installed.

Tinba (2012), also known as Tiny Banker, is a banking Trojan, known for its small file size. Tinba uses web injection to collect victim information from login pages and web forms, and is primarily disseminated via spam containing a weaponized PowerPoint file. Tinba is a highly modified version of Zeus.
AKA: Tiny Banker
Variants: none
Malware Type: banking trojan
Objective: financial, credential theft
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement, malspam, downloaded
Activity/Payload: Tinba reads network traffic to determine when a user navigates to a banking website. Tinba then either launchs a form grab, which registers the keystrokes used before HTTPS encryption ensues, or Tinba allows the user to login and capture the company's logo and site formatting to use as a popup to trick the user into submitting further information such as a Social Security Number.
Attribution & History: When Tinba was discovered in 2012, it was the smallest banking trojan by file size.

Upatre (2013) is a downloader that is capable of stealing system information, such as the computer name and the operating system being utilized.
AKA: none
Variants: none
Malware Type: downloader
Objective: malware propagation
Primary Actors: cybercriminals
Propagation & Exploit: malspam
Activity/Payload: Upatre is known for downloading ZeuS, Crilock, Dyreza and Rovnix malware.
Attribution & History: Upatre was first spotted in August 2013, after the fall of the Blackhole EK.

Ursnif (2014) utilizes malspam with JavaScript attachments.
AKA: Gozi, Dreambot
Variants: none
Malware Type: banking trojan
Objective: credential theft
Primary Actors: cybercriminals
Propagation & Exploit: malspam, dropped
Activity/Payload: Ursnif steals banking and credit card data while utilizing keylogging to acquire passwords.
Attribution & History: In 2018, researchers noted the Dark Cloud botnet dropping Ursnif while malspam campaigns were also delivering the malware. Ursnif is also able to detect malware analysis tools and check for virtualization, which makes it difficult to detect.

Vawtrak (2014) is known to use a DGA bundled inside of a compiled codebase to identify its C2 server making it a smaller and more efficient trojan.
AKA: NeverQuest, Snifula
Variants: none
Malware Type: banking trojan
Objective: financial
Primary Actors: cybercriminals
Propagation & Exploit: malspam, dropped
Activity/Payload: Vawtrak modifies the content of a web page and injects rogue forms on bank sites and then sends bank credentials back to a C2 server.
Attribution & History: Vawtrak is most commonly associated with Hancitor malspam emails using malicious Microsoft Office documents. Hancitor retrieves a Pony downloader which in turn downloads Vawtrak.

Virut (2007) is polymorphic malware that mostly infects executable files and has worm-like behavior.
AKA: W32.Virut, Virtob
Variants: none
Malware Type: botnet
Objective: malware propagation
Primary Actors: cybercriminals
Propagation & Exploit: malvertisement, malspam, network
Activity/Payload: Virut spreads by copying itself to hard drives and opening up a back door on the compromised device. It communicates via encrypted IRC.
Attribution & History: Virut is known for obfuscating code immediately following the entry point and the code continues to change over time as it attempts to avoid detection.

WannaMine (2017) is designed to generate Monero cryptocurrency. It is one of the first cryptocurrency miners that has wormability functionality and leverages two separate propagation techniques affecting Windows environments: Mimikatz and EternalBlue. Campaigns have been seen leveraging RDP and recent CVEs for initial infection.
AKA: none
Variants: none
Malware Type: cryptocurrency miner
Objective: financial
Primary Actors: cybercriminals
Propagation & Exploit: dropped, network
Activity/Payload: WannaMine is known to spread across entire networks. Organizations with flat networks are particularly vulnerable to complete saturation.
Attribution & History: WannaMine was discovered at the end of 2017 and was heavily influenced by the WannaCry and NotPetya propagation methods.

ZeuS (2006) is an advanced keylogger with a modular design. Due to the source code being released in 2011, many cybercriminals have built variants or other malware families incorporating both the modular design and coding behind ZeuS.
AKA: Zbot, Zeus Gameover
Variants: Several
Malware Type: banking trojan
Objective: financial, botnet, credential theft
Primary Actors: cybercriminals
Propagation & Exploit: malspam, dropped, malvertisement

Activity/Payload: ZeuS serves two major functions, first creating a botnet and then stealing banking credentials. It steals credentials through website monitoring, injects, and keylogging.
Attribution & History: ZeuS is credited for introducing the modular design concept to malware, which allows malicious actors to purchase only the functionality they require. Since the release of the ZeuS source code in 2011, many other malware variants have adopted parts of its codebase, which means that events classified as ZeuS may actually be other malware using parts of the ZeuS code.

SCAMS

Scams are often fraudulent schemes performed by a malicious individual, group, or organization in an attempt to obtain financials or other valuables through opportunistic aims or strategic targeting of unsuspecting victims. The scammer conducts the scam using one or more components of the Internet and traditionally relies upon confidence tricks, where an individual misrepresents themselves as someone of trustworthiness or legitimacy and dupes or conns the victim into falling to the objective of the scammer. The primary goal in the scam is to gain unauthorized access to assets normally out of reach.

Business Email Compromise (BEC) Scam are scams that attempt to deceive SLTT governments into sending money or personally identifiable information (PII), or that use the government's name to fraudulently obtain material goods. The scam almost always arrives via an email spoofing the name of or originating from the compromised account of a senior official.
Variants: Purchase Order and Vendor Fraud, W-2 and PII Data Theft, Financial Theft, Compromised Email Accounts
AKA: man-in-the-email scam, Business Email Spoofing (BES), Wire Transfer Scam, Money Wiring Scam
Risk of Occurrence: medium - high
Objective: financial fraud
Impact: low – high; depending on dollar value and reputational harm
Primary Actors: cybercriminals
Note: MS-ISAC BEC Security Primer

Domain Registration Scam involves a letter or email from a domain registration company, generally located in a foreign country, claiming another entity is trying to register a domain of like characteristics to the targeted entity. The correspondence will often request the recipient to respond if the registration violates current branding or trademark and offers the recipient the opportunity to register the domain themselves to protect name, brand, trademark, and/or confidentiality. The scam is rooted in the fact that registration of these domains is unnecessary and the registration fees are steeply priced above the going market rate.
AKA: Domain Name Scam
Risk of Occurrence: low
Objective: financial fraud, domain compromise
Impact: low
Primary Actors: cybercriminals

Doxing is the malicious identification and subsequent publication of an individual's PII, or other highly sensitive, private or damaging information that has been gathered through Internet resources by cyber threat actors.
AKA: Doxxing
Risk of Occurrence: medium – high
Objective: Public dissemination of the victims PII, to include home address, family members' information, financials, and any other incriminating information for the purposes of harming the victim.
Impact: medium – high
Primary Actors: hacktivists, cybercriminals

False and Unsubstantiated Claims are when a cyber threat actor claims, on fraudulent and/or unsubstantiated grounds, to have successfully compromised an entity. The actor will either claim credit for another actor's success, claim credit for an attack when the vector was not an attack but an issue internal to the entity or the information was openly posted, or boast of an attack with no evidence or falsified evidence.

AKA: False Claims
Risk of Occurrence: low – medium
Objective: Gain credibility within the cybercriminal and/or hacker community. To expose claimed evidence of racism, sexism, xenophobia, or other purported injustice. Achieve social or economic goals. Embarrass targets of spoken incident.
Impact: low
Primary Actors: hacktivists, terrorists, cybercriminals

False Emergency Broadcasts occur when a malicious actor utilizes television, radio stations, and/or emergency sirens to broadcast fraudulent emergency alerts to achieve mass disruption, chaos, or widespread disruption, consequently overwhelming first responders.
AKA: Fake Emergency Broadcasting
Risk of Occurrence: low
Objective: panic
Impact: low
Primary Actors: hacktivists, cybercriminals

Hoax Extortion happens when a cyber threat actor threatens that they will or have conducted an attack against a target to intimidate the target into paying a set amount. These are hoax claims and the actors do not follow through with the threats.
Variants: Denial of Service, Sextortion, Hitman
AKA: none
Risk of Occurrence: low
Objective: trying to be paid based off of another actor's reputation.
Impact: low
Primary Actors: cybercriminals

Nigerian Letter Scam is a mailed, faxed, or emailed letter, frequently from Nigeria or other parts of Africa, offering the recipient the chance to share in a portion of millions of dollars that the author is trying to transfer illegally out of Nigeria. In some instances, these contacts masquerade as legitimate correspondence from the U.S. Department of State or the U.S. Department of the Treasury. In like cases, the correspondence will claim to have collaboration with the United Nations and the World Bank. The author usually claims to be a ranking government official, encouraging the recipient to send information like blank letterheads, bank names, and account numbers, as well as other identifying information through provided a fax number or website within the letter or email. The schemes themselves violate section 419 of the Nigerian criminal code, hence the label "419" (see below). Scammers have operated out of the U.S. to make the scam more realistic and some scammers around the world have adopted these techniques
AKA: "419"scam, Country code scam, Advance Fee Fraud
Risk of Occurrence: low
Objective: financial fraud, identity theft
Impact: low – high
Primary Actors: cybercriminals

Phishing occurs when malicious actors masquerade as legitimate entities during electronic communication in an attempt to compromise systems and networks or to gain unauthorized access to private, sensitive, or restricted content. Phishing is designed to socially engineer a response from the recipient, such as going to a malicious actor controlled website and entering login credentials. Phishing emails often entail a sense of urgency to exploit time constraints and cloud a victim's initial judgment.
Variants: vishing, smishing, pharming

Risk of Occurrence: high
Objective: financial, fraud, credential theft
Impact: medium – high
Primary Actors: cybercriminals, nation-states

Social Network Profile Scam is when a malicious actor creates a fake social media profile in the name of celebrities, public officials, law enforcement officers, or business executives. The profiles are used to trick or coerce employees, colleges, or constituents into sending money to fraudulent charities or to post misleading and/or incriminating information about the named individual. This scam can also be for satirical or malicious purposes.
AKA: Social Media Scam
Risk of Occurrence: low
Objective: reputation hijacking, financial fraud
Impact: low – medium; severity largely depends upon individual or entity targeted and believability of the fake profile
Primary Actors: hacktivists, cybercriminals

Stranded Traveler Scam is when a cyber threat actor uses a compromised email or social media account to pose as the victim (Victim 1). The actor contacts a relative of Victim 1 and claims that he (Victim 1) is stranded in a foreign country and in urgent need of money, which the relative transfers to the actor. Other variants involve claims of imprisonment, lost passports, and injuries/hospitalizations. Additionally, the actor locks Victim 1 out of their accounts so they cannot tell everyone that they were hacked.
Variants: none
AKA: Grandparent Scam
Risk of Occurrence: low
Objective: financial
Impact: low
Primary Actors: cybercriminals

Swatting is a hoax call to 9-1-1 to draw a response from law enforcement, especially a SWAT team. A malicious actor will place a prank phone call to emergency services, tricking authorities into dispatching a large number of law enforcement officers to a given address. This usually includes reporting of a fake hostage situation, terrorist attack, or bomb threat, or similar emergency.
AKA: SWATting
Risk of Occurrence: low
Objective: Embarrassment or harm of victim; revenge and enjoyment of scammer.
Impact: medium – high; possible injury and death
Primary Actors: cybercriminals

Tech Support Scam is a common scam where cyber threat actors claim to be computer techs from legitimate and reputable companies (i.e., Apple or Microsoft) and attempt to defraud their targeted victim. Actors will either call or send popup messages warning the user the computer in question is malfunctioning or is experiencing an infection. This notice is to convince the user that the system is experiencing problems and usually directs the user to a malicious website to further carry out the fraud attempt. Once persuaded, the actor will attempt to gain remote access to the system and fraudulently tamper to infect the host or diagnose a non-existent problem prompting the user to pay for an unnecessary service.
AKA: Tech Call Scam
Risk of Occurrence: medium
Objective: financial, fraud, credential theft

Impact: low – medium
Primary Actors: cybercriminals
Note: Tech Support Scam Primer

Telephony Denial of Service (TDoS) attack is an attempt to make a telephone system unavailable to the intended user(s) by preventing incoming and/or outgoing calls. This is accomplished when an attacker successfully consumes all available telephone resources, so that there is no unoccupied telephone line.
AKA: Telephone denial-of-service, TDOS
Risk of Occurrence: low
Objective:

- *Direct Financial gain*: Direct targeting of individuals or organizations for scamming or extortion of financial assets. This is the social engineering aspect.
- *Indirect Financial gain:* Denial of services during TDoS attack where wire transfers and transactions cannot be verified (allowing actor to steal financials under radar), or simply denying the target normal operations and up time, damaging individual or company profits.
- *Unknown:* Instances where no money is demanded and no indirect financial gain attempts have been uncovered. Could be hacktivist, or lone hacker play for fun.

Impact: high impact for 911 and other emergency call services.
Primary Actors: cybercriminals, hacktivists
Note: Telephony Denial of Service Attacks Primer

ACTORS AND MOTIVATIONS

Discussions of cybercrime actors generally classify the actors into several categories: cybercriminals, hacktivists, insiders, terrorist organizations, and nation-states. 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. Of note, all the hacking activity discussed in this guide is considered black hat activity by hackers with the intent to perform malicious and illegal actions.

Cyber Threat Actor is a participant (person, group, or organization) in an action or process that is characterized by malice or hostile action (intending harm) toward computers, devices, systems, or networks.

Nation-states actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information. However, not all nation-states have the ability nor pursue sophisticated cyber capabilities and some, while they may have the intent, do not possess the technical competency to achieve such capabilities.
Motivation: espionage, disruption, or destruction
Affiliation: nation-states

Terrorist Organizations are defined by the U.S. Department of State.
Motivation: political or ideological, possibly for financial gain, espionage, or destruction
Affiliation: individuals, organizations, or nation-states

Cybercriminals are largely motivated by profit and represent a long-term, global, and common threat. Cybercriminals may work individually or in groups to achieve their purposes.
Motivation: personal financial gain or reputation enhancement
Affiliation: individuals or with co-collaborators

Hacktivists (a.k.a. Ideologically-Motivated Criminal Hackers) are politically, socially, or ideologically motivated and target victims for publicity or to effect change, which can result in high profile operations.
Motivation: political, social, or ideological
Affiliation: individuals or organizational

Insiders are a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.
Motivation: generally for financial gain or destruction
Affiliation: current or former employee, contractor, or other business partner who has or had authorized access