Hewlett Packard Enterprise

Business white paper

Ransomware: Holding data hostage

Coping with the growing threat

Table of contents

Cybercriminals are continuing to refine and evolve their toolsets and methods of corruption in their quest to stay ahead of law enforcement and security experts. Corporations across all industries have suffered losses from advanced threats stealing intellectual property and customer data. But one specialized form of malware has been on the rise that does not steal the information—it holds it hostage. This rising threat is called ransomware.

Ransomware is designed to restrict users from accessing data on their own systems, while perpetrators demand payment (a ransom) to remove the restriction. This is accomplished by either encrypting data or by blocking access to resources.

This paper's intent is to increase awareness of the growing ransomware problem, and to offer recommendations on how to identify it within your environment, prevent it from propagating further, and remove it from compromised systems.

Background

The first widely known ransomware appeared in 1989 and was called the AIDS Trojan (also known as Aids Info Disk or PC Cyborg Trojan). This malware worked by hiding directories and encrypting the names of files on the local disk drive; it would then prompt the user for payment of a "license renewal" (ransom) to restore the infected host back to its original state. Encryption mechanisms for ransomware were rudimentary at first. By 1996, however, much stronger public-key encryption was found in some variants. Ransomware continued to mature, leveraging increasingly complex encryption schemes. By 2008, some instances of 1024-bit RSA keys were reported, and today, 2048- or 4096-bit keys are not uncommon (the higher the bit strength, the harder it is to crack).

The potential for monetary gain by cybercriminals, combined with the difficulty of removal, has led to the further proliferation of ransomware at the global level. The advent of Bitcoin and other cryptocurrency has inadvertently furthered propagation by making it easier to collect ransom, while protecting the anonymity of perpetrators. In fact, ZDNet conducted research in late 2013 that involved the tracking of four Bitcoin addresses identified as being associated with "CryptoLocker" attacks. Over just two months (between October 15 and December 18), they identified about $27 million in transactions. Although this study was limited to only those four accounts, it demonstrates just how lucrative ransomware attacks can be.

Recent advancements in ransomware not only have increased the complexity of the encryption mechanisms, but the methods of deployment are now utilizing nontraditional attack vectors, as well. Rather than infecting a host through a phishing email, variants have been identified that first gain access through a vulnerability exploitation, and then leverage a variety of tools (including common utilities and open-source software) to find, encrypt, and/or delete files and backups. This advancing complexity makes it difficult to defend against and, when coupled with the relative ease of payment, it's no wonder ransomware attacks are on the rise.[1]

[1] Source: McAfee Labs: Threats Report, March 2016.

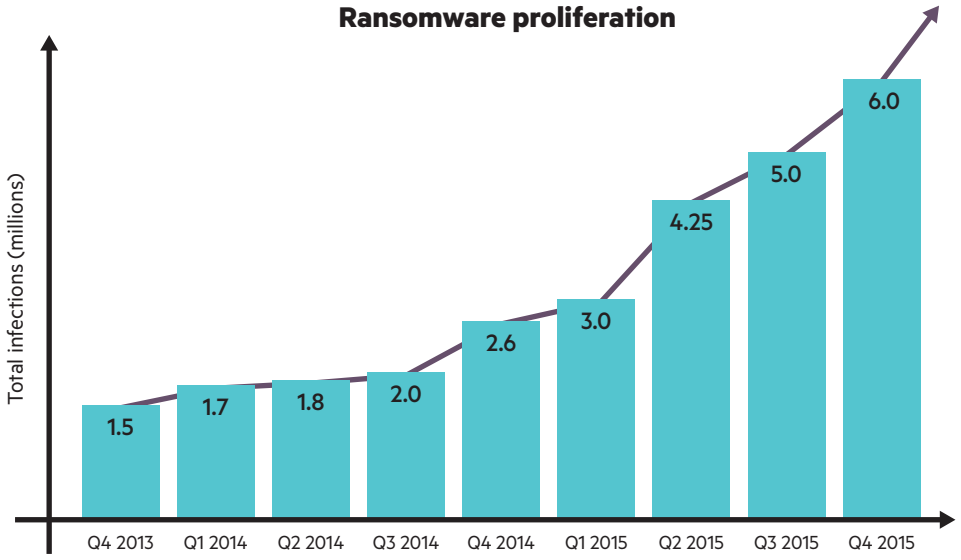

Figure 1: Recent rise in ransomware attacks

Impact of ransomware

As previously noted, ransomware is primarily used to extort money from victims by infecting computers and rendering them unusable until ransom is paid to have data restored. The extortion amount often varies; however, it typically starts at a few hundred dollars and can exceed several thousand dollars. It should be stressed that payment of the ransom does not guarantee the recovery of the encrypted files, nor does it guarantee a reinfection won't occur.

Between April 2014 and June 2015, the CryptoWall strain of ransomware cost Americans over $18 million, according to the FBIs Internet Crime Complaint Center (IC3). This figure includes money spent not only on ransoms, but also on network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and/or the purchase of credit monitoring services for employees or customers.

Most recently, we have seen numerous healthcare organizations targeted. A ransomware attack on one U.S. healthcare organization debilitated 10 hospitals in Maryland and Washington, and impacted 30,000 staff, 6,000 physicians, and countless patients. In February 2016, a ransomware attack on a medical center in Los Angeles, California, crippled the hospital's infrastructure, and prevented staff from accessing critical systems and data. A ransom of 40 Bitcoins (roughly $17,000) was paid to restore order, but in many cases, order cannot be restored, even after paying the ransom.

How ransomware works

The operational cycle of ransomware is similar to 'typical' malware; however, it does have unique aspects when systems are infected. Similar to traditional malware, attackers need a delivery mechanism to get their malicious code (payload) onto a targeted system. Not-so-similar to traditional malware, ransomware has Execution and Demand phases to hold the compromised system hostage and to provide instructions for ransom payment.

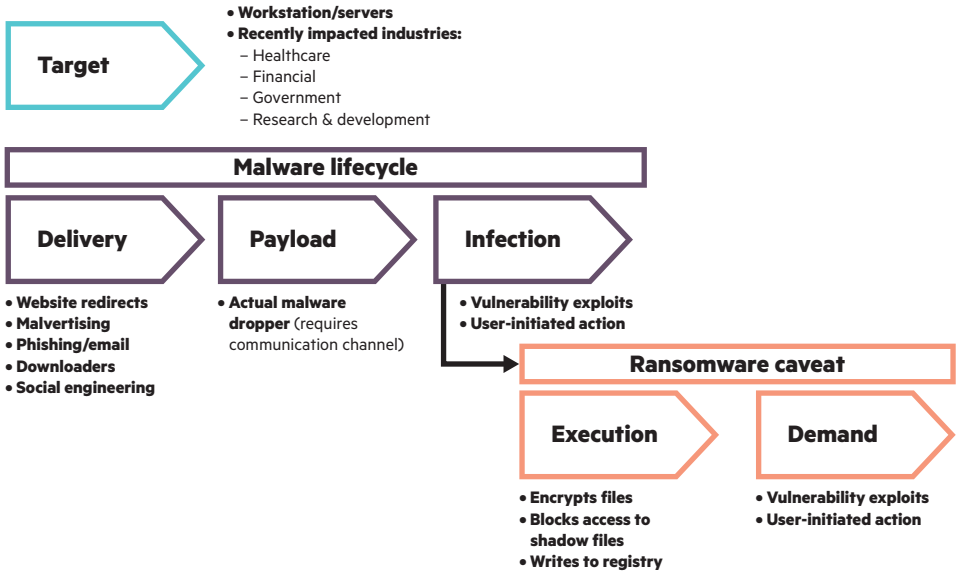

Figure 2: Malware/ransomware operational cycle

Target—Adversaries have previously targeted consumers and, while they still do, they are beginning to target small to medium-sized businesses. These organizations are considered easy targets because they frequently have fewer resources available to properly secure and monitor their environments. Unfortunately, many small businesses often have no capacity to absorb these losses, and frequently end up paying the ransom.

Delivery—Most ransomware is downloaded by users who unwittingly visit a malicious or compromised website through an email attachment, a phishing link, or as a payload from another malware program. Malvertising, or the use of online advertising to spread malware, is another means for delivery, and very difficult to prevent. The advertisement that triggers delivery is legitimate and is substituted by a malicious link after the ad begins to run. Some instances of ransomware delivery are through orchestrated efforts that include exploiting specific vulnerabilities on the target host. Once compromised, various techniques similar to "traditional" hacking are then used to establish a foothold, and elevate privileges in order to ensure the eventual infection.

Payload—The payload is either the actual malicious code or a "dropper." Droppers are small files that are easily downloaded without raising suspicion, and automatically download subsequent ransomware executable(s). A dropper can be as simple as an intentionally corrupted Microsoft Word document, or other attachment in a phishing email. Whether ransomware code or a dropper is the payload, the end result is the same: malware that holds the host hostage and demands a ransom will be transferred to the target.

Infection—Once the payload has been loaded on the target system, it starts infecting immediately, or it is activated by a communication path to a "command and control" server. This communications channel is used to exchange encryption keys, establish contact with the victim, and provide payment details for the ransom. In most cases, payment and command and control communications are handled through "The onion router" (Tor) network. Tor directs Internet traffic through a free, worldwide, volunteer network that effectively conceals the attacker's location and activity.

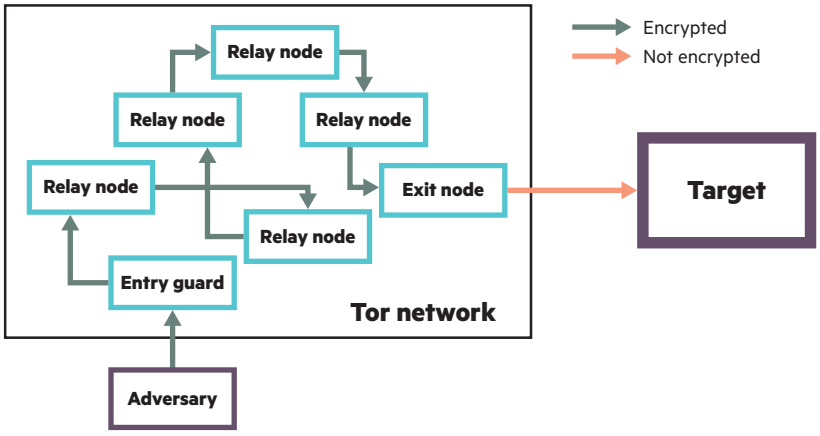

Figure 3: Tor network

Execution—Once activated, the ransomware program will begin its execution. While execution of various strains of ransomware differ, most types of malware maintain a predefined, embedded list of file extensions to search for. Ransomware programs will search all system drives (including mapped network drives), and include any attached removable-storage media. This action can have profound effects on the network as a whole, as it can lead to encrypting backups, network locations, and any files stored on removable media. When the ransomware locates specified files to hold hostage, it creates temporary files, encrypts the original files into those temporary files, and then overwrites the original files with encrypted versions.

Other Tricks—To be successful, ransomware needs to remain undetected. Along with the encryption and "ransom letter" aspects of the malware, the majority of ransomware uses Windows system files (svchost.exe and explorer.exe) to reduce the host's defenses, and some even make use of vssadmin.exe to delete existing Windows shadow volume copies (backup files). More complex variants will change registry settings to prevent warnings regarding non-SSL and non-HTTPS connections, and will disable Windows repair attempts upon startup. Other tactics deployed involve attempts to disable anti-malware programs, the use of rootkits (malicious software designed to enable unauthorized access), and infecting Windows registries to have malware load at boot up, even in Safe Mode.

Demand—Once the encryption process is completed, the ransomware generally displays an on-screen notice that varies, based on the specific ransomware used. In all cases, it indicates the files have been locked and a "ransom fee" will need to be paid by a certain time to decrypt the files. One such example for "CryptoLocker" demands 1 Bitcoin to restore the filesystem:

Examples of ransomware

CryptoLocker—TorrentLocker, CryptoWall
TorrentLocker and CryptoWall are two of the more persistent and popular ransomware variants of CryptoLocker. They appear to be targeting the small and medium-sized business (SMB) market, and are known for initiating spam campaigns in the early morning hours of the time zone associated with the intended victims. They also rely heavily on social engineering tactics tailored at business units by using keywords, such as résumé, orders, or invoice in the subject line of spam emails, attempting to appear legitimate.

TorrentLocker appears to be region-specific with the social engineering based on the victim's country (Australia, Italy, and Turkey have been focused), and its attacks are based on notices from postal services, telecommunication and utility companies, and governmental elements.

CryptoWall seems to have no specific geographically targeted region and recently has been coupled with spyware (Fareit) to steal credentials stored in the system's FTP clients, web browsers, email clients, and Bitcoin wallets. In addition to the primary objective of holding the host hostage, this allows the cybercriminal to steal victims' information that can later be resold.

These ransomware variants also employ methods to avoid security controls. They use "fast flux," which is a Domain Name System (DNS) technique that uses an ever-changing network of compromised hosts, acting as proxies to redirect traffic and bypass antispam and other web filters. They also use compromised websites to hide their redirections, and some TorrentLocker variants use self-destruction mechanisms that remove ransomware executables to keep code from authorities.

VirLock
VirLock is often bundled with other malware and is generally delivered, either by a botnet or through the use of social engineering. VirLock locks the screen of the affected computer, while disabling processes Windows requires for operation (explorer.exe and taskmgr.exe), and will check the physical location of the machine in order to present a tailored message to the user. Currently, VirLock is directed primarily at the United States, followed by China and Australia.

Of significance is that VirLock is a polymorphic worm with file infecting capabilities, which allow it to spread on its own. A single infected file can initiate the process, making it difficult to clean a system completely. Once started, the infected file will substitute a decrypted host file in the same directory where it was executed, and will run the substitute file to make the user believe all is well. The use of the dummy file may serve two purposes—code recycling and polymorphism.

Besides being polymorphic, VirLock creates and modifies registry entries to avoid detection, and also contains a custom hacker package that uses random application program interface (API) calls. The ransomware continuously changes the hacker package to avoid detection. VirLock also uses two layers of encryption, the first is exclusive disjunction (XOR), and the second is a combination of Rotate on Left (ROL) and XOR.

Locky

Locky is a new strain of ransomware with an attack vector similar to Dridex, which is a type of banking-oriented malware. Locky is normally delivered via a Microsoft Word document (posing as an invoice), containing embedded macros that establish connection with the attacker's server.

Most ransomware programs generate the encryption key locally and transmit copies to the attacker. Unlike other ransomware, Locky uses connections to "command and control" servers for encryption key exchange. Locky encrypts local files as well as unmapped network drives, and will delete all the shadow volume copies on the machine to prevent its restoration. Locky also creates a temporary "svchost.exe" process while it encrypts files to avoid detection. It will then delete itself from the system once the infection/encryption process is complete.

More than half of the systems targeted by Locky have been in the United States, with other affected countries including Canada and Australia.

KeRanger

KeRanger is the first example of a fully functional Apple Mac OS X ransomware, and the first Mac OS X malware distributed with a signed software update from a legitimate developer. Analysis of the software suggest it is a ported version of the Linux.Encoder ransomware, making it the first cross-platform ransomware. One main adaptation the KeRanger authors made to the Mac version was to sign the malware with a legitimate code signing key, issued by Apple for the Mac App Store, which means it is whitelisted by the Mac Gatekeeper service.

Samas/Samsam

Samas/Samsam is similar to other advanced ransomware, as it employs elusive code to deter detection and information-stealing malware (Derusbi/Bladabindi) to gather credentials, in addition to the primary objective of the hostage/ransom aspect. What differentiates Samas/Samsam from the others is twofold: the method of infection and its targeting of backup files.

Attackers are employing more advanced methods to hunt for and identify ways to get to the targeted hosts. According to Microsoft, Samas/Samsam infection "starts with a pen-testing/attack server, searching for potential vulnerable networks to exploit with the help of a publicly available tool named reGeorg, which is used for tunneling. Java-based vulnerabilities were also observed to have been utilized."

Samas/Samsam targets and deletes backup files as well, which makes recovering from the infection that much more difficult. Having ransomware delete backup files may sound fairly trivial; however, many backup files are protected from deletion by the operating system. Samas/Samsam will halt those processes protecting the backups first, then delete the files.

Samas/Samsam has been mostly found in North America, with a few instances in Europe.

Cerber

Recently, a new file-encrypting program called "Cerber" has raised ransomware to a new level. Cerber is being sold "as a Service" on a private Russian forum, which makes it available to low-level criminals who might not have the coding skills or resources to create their own ransomware. As with other ransomware, the program encrypts file contents and file names and alters the original extensions. It will also scan for and encrypt available network shares, even if they are not mapped to a drive letter on the host. Another, rather eerie characteristic of Cerber, is the use of audio that speaks a message stating that your computer's files were encrypted.

Ransomware prevention and removal

Although ransomware can be a powerful and effective extortion tool for cybercriminals, there are numerous ways to prevent it and to minimize the impact of an infection. Conducting effective security awareness training, monitoring networks and systems, timely security patching, and employing a robust backup and recovery program are some of the best ways to protect and recover from a ransomware attack. Listed below are several additional, more-detailed techniques to aid in the prevention and removal of ransomware.

Prevention

Awareness—Since most ransomware enters a system via some type of social-engineering attack, user awareness is a critical step in prevention. As with all training and awareness programs, it requires an ongoing effort to stay ahead of changing ransomware tactics. This may require a significant cultural change to prevent users from opening untrusted email attachments and clicking on hyperlinks embedded in emails.

Patching—According to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), as many as 85 percent of all targeted attacks can be prevented by applying a security patch. Maintaining current patch levels for all operating systems, software, anti-virus, and other security programs will greatly reduce the chance of infection.

File management—In a shared environment, exchanging files is routine. Since the distribution of ransomware often depends on this file exchange, it is imperative to have a policy that provides for the transfer of such documents in a safe and secure manner. As an example, using digital signatures for document exchange may reduce the chances of infection.

Email security—Technical controls related to email security will go a long way in reducing the potential for ransomware infection. Effective techniques include employing anti-spam and anti-phishing filters, blocking emails that contain hyperlinks, and quarantining images and attachments.

Disable unnecessary services—Ransomware and other malware leverage legitimate operating system processes and services in one form or another. Since every system is different, there is no "silver bullet" as to which services should be enabled or disabled. The information technology (IT) department should determine which services are deemed unnecessary, prior to disabling them. Additional permissions can also be levied upon "risky" services that are required for system operation.

Software restrictions—Many ransomware variants copy, alter, and run critical system files (executables) in different locations for a variety of reasons. To stop this, policies in the Group Policy Object (GPO) that prevent executables from running in specific locations (such as ProgramData, AppData, and Temp) can be created.

Good housekeeping—The removal of all drives and devices when not in use will reduce the potential of spreading the ransomware. This includes mapped network drives, physical USB drives or memory sticks, smartphones, cameras, and anything else that can be logically written to.

Block IP addresses—Tor gateways are the primary means for some ransomware to communicate with their command and control servers. Blocking these gateways will impede this capability. It should be noted that some cybercriminals have changed tactics and are now using redirected web sites; however, it is still a best practice to block known malicious IP addresses in an operational business environment.

Robust monitoring capabilities—Employing host and network monitoring tools and establishing an effective security information and event management (SIEM) program can help identify malicious activity. Robust monitoring aids in quickly detecting instances where ransomware uses command and control servers, or when malicious code spreads from host to host.

Removal
Back up data—Removing ransomware after it has done its work is difficult, and often the only option left (aside from paying the ransom) is to rebuild the infected system and restore data from known-good back-up medium (such as tape, disk, and so forth).

The primary technical control is to ensure that data and systems are backed up on a regular basis. While it is possible some backups may contain ransomware, the following steps should be taken to avoid and reduce this likelihood:

- Backups should be conducted on a regular basis and maintained for a specified period of time.
- Backups should be write-protected after being stored offline and offsite,
- Backups should employ versioning to ensure known-good media are available from a point in time prior to the infection.
- Backups should be tested regularly to validate the integrity and ability to restore the data.
- Backups should be checked regularly with anti-virus scans.

Have a plan—Being caught off guard is not a good position to be in when facing a ransomware infection. If your organization's security policies do not include provisions for dealing with this type of attack, please work with your leadership team to develop and test a response plan. Understanding how ransomware works is the first step in determining which security controls are required to prevent and/or eradicate it.

Response
Knowing how to identify, prevent, and recover from a ransomware attack is important. However, the timing of the response in the first few hours after an attack is critical. If faced with a ransomware situation:

- It is not advisable to remit payment of any demands, but refer to your company's relevant policies regarding ransomware for guidance.
- It is advisable to disconnect infected hosts from the network if a compromise is suspected.
- It is advisable to deploy or enlist incident response and digital forensic teams for their ability to respond to any such situation professionally and efficiently.
- It is advisable to notify the authorities and record all information on these attacks; this will assist in building up the intelligence available for all those who may be targeted.

Learn more at
hpe.com/us/en/services/consulting/security.html

Appendix A—Glossary

Application program interface (API) calls—API calls are specified operations that applications use to perform tasks on the underlying operating system.

As a Service—Consumption-based delivery of computing services. In this case, Software as a Service, refers to paying a third party for the use of their software.

Attack vector—Methods used by hackers to gain information, leverage permissions, and exploit vulnerabilities for the purpose of accessing computing resources.

Bitcoin—A Bitcoin is a form of digital currency.

Bladabindi—Malware that infects Windows hosts to create backdoors and gain remote access to personal or other sensitive information.

Botnet—A botnet is a number of Internet-connected computers communicating with other similar machines in which components, located on networked computers, communicate and coordinate their actions by command and control or by passing messages to one another.

Command and control server—Command and control (C&C) infrastructure consists of servers and other technical infrastructure used to control malware in general, and, in particular, botnets. Command and control servers may be either directly controlled by the malware operators, or themselves run on hardware compromised by malware.

Cybercriminal—A cybercriminal is an individual who commits cybercrimes, where he/she makes use of the computer, either as a tool, target, or as both. Cybercriminals often work in organized groups. Some cybercriminal groups are reportedly supported by nation states.

Derusbi—A popular remote access Trojan (RAT) used by hackers to steal logon credentials for Windows-based applications.

Digital currency/cryptocurrency—A digital form of currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

Domain Name System (DNS)—A protocol for the naming of and communication among hosts on a network.

Dridex—Malware used by attackers to steal banking credentials and other personal information on the target system.

Dropper—A dropper is a program (malware component) that has been designed to "install" some sort of malware (virus, backdoor, and so forth) to a target system. The malware code can be contained within the dropper (single-stage) in such a way as to avoid detection by virus scanners, or the dropper may download the malware to the target machine once activated (two stage).

Dynamic-Link Library (DLL) file—An executable file that allows programs to share code and other resources necessary to perform particular tasks. Microsoft Windows provides DLL files that contain functions and resources that allow Windows-based programs to operate in the Windows environment.

Exclusive disjunction (XOR)—A symmetric encryption technique that uses the mathematical "exclusive or" operator to encrypt bit strings. XOR is typically used as a component of more complex encryption schemes.

Fareit—Malware that retrieves stored website passwords from browsers including Chrome, Firefox, Internet Explorer, and Opera and posts them to specified websites. It also tries to steal stored account information, like server names, port numbers, login IDs, and passwords from numerous FTP clients or cloud storage programs.

File Transfer Protocol (FTP) client—A program used to transfer files to and from remote hosts.

Gatekeeper service—A program that only allows downloading of approved apps to Apple Mac platforms.

Group Policy Object (GPO)—A feature of the Windows operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications, and users' settings in an active directory environment.

Macro—A single instruction that expands automatically into a set of instructions to perform a particular task.

Malware—An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

Open-source software—Computer software with its source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose. Open-source software may be developed in a collaborative public manner.

Payload—In computer security, payload refers to the part of malware that performs a malicious action. In the analysis of malicious software such as worms, viruses, and Trojans, it refers to the software's harmful results.

Phishing attacks—The act of sending an email to a user, falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. Phishing email will typically direct users to visit a website where they are asked to update personal information, such as a password, credit card, Social Security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and will capture and steal any information the user enters on the page.

Polymorphic—A virus that changes its virus signature (that is, its binary pattern) every time it replicates and infects a new file in order to keep from being detected by an antivirus program.

Public key encryption—A cryptographic system that uses two keys; a public key known to everyone, and a private or secret key known only to the recipient of the message.

Ransomware—Malware designed to restrict users from accessing data on their systems, while demanding payment (a ransom) to remove the restriction. This is accomplished by either encrypting data or by blocking access to resources.

Rootkit—A collection of software designed to enable access to a computer or areas of software that would not otherwise be allowed.

Rotate on left (ROL)—An encryption technique that uses the bitwise "rotate" operator to encrypt bit strings by rearranging the original bits. ROL is typically used as a component of more complex encryption schemes.

RSA encryption—Created by RSA Security, one of the first encryption schemes to successfully use public-key encryption algorithms. The strength of RSA encryption is referenced by the "bit strength" of the keys used to encrypt and decrypt data.

Security information and event management (SIEM)—A collection and correlation program to identify security issues on networks and hosts. A SIEM works by parsing log files from numerous sources and identified patterns that indicate malicious activity.

Safe mode—An alternate, administrative-level Windows environment used to debug or recover from problems with the operating system.

Social engineering attacks—Techniques such as to appeal to vanity, appeal to authority and appeal to greed are often used in social engineering attacks. Many social engineering exploits simply rely on people's willingness to be helpful. Popular types of social engineering attacks include:

- Baiting: Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.
- Phishing: Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.
- Spear phishing: Spear phishing is like phishing, but tailored for a specific individual or organization.
- Pretexting: Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data to confirm the identity of the recipient.
- Scareware: Scareware involves tricking victims into thinking their computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

Shadow volume copies—(Also known as volume snapshot service, volume shadow copy service or VSS) is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use.

Symmetric cryptography—An encryption algorithm where the same key is used for both encryption and decryption. The key must be kept secret, and is shared by the message sender and recipient.

The onion router (Tor)—Free software for enabling anonymous communication. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user, this includes visits to websites, online posts, instant messages, and other communication forms.

Trojan—A malicious computer program that misrepresents itself to appear useful, routine, or interesting to persuade a victim to install it.

United States Computer Emergency Readiness Team (US-CERT)—An organization within the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). US-CERT is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. The division brings advanced network and digital media analysis expertise to bear on malicious activity targeting the networks within the United States and abroad.

Vulnerability exploitation—A software vulnerability is a security flaw, glitch, or weakness found in software or in an operating system that can lead to security concerns. An exploit is a code purposely created by attackers to abuse or target a software vulnerability. This code is typically incorporated into malware. Once the exploit code is successfully executed, the malware drops a copy of itself into the vulnerable system.

Windows registry—A database that stores information about the Windows operating system and applications. Registry files are used to start, configure, and/or control Windows functions and programs.

Windows system files—Executables on the Microsoft Windows platform used to run and support the operating system. Service host, or svchost.exe, is a generic process used to run Dynamic Link Library files; Explorer, or explorer.exe, is main graphical user interface for Windows; Volume Shadow copy Service, or vssadmin, manages and protects shadow volumes (backups); Task Manager, or taskmgr.exe, is used to schedule and start Windows programs or processes.

Appendix B—References

The following references provide additional information on ransomware. Reference to these sites does not constitute an endorsement of their product and/or services.

Federal Bureau of Investigation (**www.fbi.gov**)

Information Systems Audit and Control Association (ISACA), (**www.isaca.org**)

International Information Systems Security Certification Consortium (ISC)[2], (**www.isc2.org**)

McAfee—Intel Security (**www.mcafee.com**)

Microsoft (**www.microsoft.com**)

SANS (**www.sans.org**)

U.S. Cert (**www.us-cert.gov**)

Wikipedia (**www.wikipedia.com**)

ZDNet (**www.zdnet.com**)

Sign up for updates

Hewlett Packard Enterprise

4AA6-5578ENW, May 2016