Ransomware Response Guide

IBM INCIDENT RESPONSE SERVICES

RELEASE DATE: MAY 2016

Copyright

The methodologies and processes used in the conduct of this engagement are considered proprietary intellectual property of IBM, and may not be disclosed without written permission from IBM. IBM authorizes you to copy this report for the purposes of disseminating information within your organization or any regulatory agency.

Disclaimer

New technology, configuration changes, software upgrades and routine maintenance, among other items, can create new and unknown security exposures. Moreover, computer "hackers" and other third parties continue to employ increasingly sophisticated techniques and tools, resulting in ever-growing challenges to network and computer system security. The Report and the recommendations contained herein do not constitute any representation or warranty by IBM about the security of a company's network and/or computer systems including, but not limited to, any representation that a company's computer systems are safe from intrusions, viruses, or any other security exposures.

Table of Contents

Executive Summary

Background

If you are currently experiencing a ransomware incident, immediately review the containment section on page 17.

The document is intended to be a guide for organizations faced with a ransomware[1] infection. This guide is split into several sections, with the most critical and time-sensitive being in the initial response section. **If you are currently experiencing a ransomware incident, it is highly recommended you immediately review the containment section below**, and return to this section at a later time for an overall background of ransomware.

For the purpose of this guide, the terms 'version' and 'variant' are used with different meaning. The term version refers to the same malware program which encompasses newer or older versions of the same program with varying features. The term variant is used to describe a 'family' of ransomware. For example, there are several different variants of ransomware that encrypt a user's files and then demand a ransom. These variants are commonly written by different people, known by different names by anti-virus companies, and function differently with the same overall goal.

In the past several months, IBM Security's Emergency Response Services (IBM) organization has seen an increased number of customers who have reported being a victim of ransomware. Ransomware is commonly received by the victim through unsolicited email from an unknown sender as an attachment and/or injected into a user's browser session through a web browser vulnerability, such as many of the recent Adobe Flash vulnerabilities that have been published in 2015.[2] Early in 2016, a new approach was used to deploy yet another ransomware variant; this one is known as SamSam or SamAs. This new threat uses known vulnerabilities (mainly in JBoss at this time). These vulnerabilities are exploited by threat actors using tools to compromise systems and plant "webshells" or "backdoors" (remote access Trojans (RATs)) to allow further compromise of the victim's systems and network infrastructure. Once this has been achieved, the ransomware payload/package is deployed to all targeted Windows systems. The attacker uses PSEXEC to deliver the ransomware to each target system. Once delivered it is detonated, starting the encryption of files that match the 'hit' list.

[1] *https://en.wikipedia.org/wiki/Ransomware* — "a type of malicious software designed to block access to a computer system until a sum of money is paid."

[2] *https://helpx.adobe.com/security.html#flashplayer*

As of the start of 2016, there are now numerous different variants of ransomware in use. Some are very efficient and highly successful in rendering files inaccessible unless a ransom is paid, while other variants attempt to accomplish the same goal, but implement the encryption process poorly. Depending on the variant and version of the ransomware, this poor implementation may allow a user to decrypt their files without paying a ransom.

However, this is generally becoming less likely as the implementation and key management technique has significantly improved.

When a computer becomes infected with ransomware, the malware typically generates a very small amount of external network traffic. Upon infection, most versions/variants of ransomware utilize a Domain Generation Algorithm (DGA)[3] to randomize the DNS request that it makes to the command & control (C&C) server. This makes blacklisting the known domains much harder since the malware will use the DGA to generate thousands of randomized domain names, where one may be a legitimate domain used to connect to the C&C server. This initial contact with the C&C server is to enroll the computer with the C&C server and to obtain the public encryption key(s) it then uses to encrypt all the user's files. Therefore, a memory dump or network traffic capture will do very little to help gain the necessary information to restore the files since the private key that is needed to decrypt the files never exists on the victim computer.

In the case of SamSam, there is no key-exchange as the public key (used to encrypt files) is included in the deployed package. However, as SamSam is introduced via traditional hacking activities, other indicators of compromise should be visible and acted upon.

[3] *https://en.wikipedia.org/wiki/DGA*

Most ransomware target files commonly created and utilized by users, not operating system files.

Most ransomware target files commonly created and utilized by users, not operating system files. The targeted files vary from variant to variant of ransomware, and in some cases in different versions of the same ransomware variant, but they typically include, but are not limited to:

- Microsoft Office files (.doc, .docx, .xls, .xlsx, .ppt, .pptx, .rtf)
- Open Office files (.odt, .ods, .odp)
- Adobe PDF files
- Popular image files (.JPG, .PNG, raw camera files, etc.)
- Text files (.txt, .RTF, etc.)
- Database file (.sql, .dba, .mdb, .odb,. db3, .sqlite3, etc.)
- Compressed file (.zip, .rar, .7z, etc.)
- Mail files (.pst)
- Key files (.pem, .crt, etc.)

To demonstrate the breadth of the files encrypted by one variant of ransomware, over 150 different extensions are targeted for encryption. Depending on the variant and version of the ransomware, additional file extensions may be targeted.

The decision to pay a ransom in hopes of getting the data back is a complicated one. IBM does not have a position on paying a ransom to decrypt files. Any decision to pay a ransom should be based on a risk vs. benefit analysis and with the understanding that while many users have reported success in getting their files back after paying a ransom, there are no guarantees that if a ransom is paid, an organization will receive the necessary keys to decrypt the affected files. IBM recommends an organization first consider their internal backup infrastructure as a way to recover important files before considering paying a ransom. If backups are not available, then the relevant stakeholders within the organization should be involved in any decision to pay a ransom.

The widespread success of ransomware is largely due to the fact that ransomware does not require administrative privileges like other malware. Instead, it relies and preys specifically on the permissions a victim user has on their assigned computer and within an organization, to encrypt the files that the specific user has access to, either locally on their own computer and/or across the organization's network on corporate file share servers.

Incident Lifecycle

This document describes responding to a ransomware incident using the National Institute of Standards and Technology (NIST) Incident Response Life Cycle, as described in the NIST Computer Security Incident Handling Guide[4].

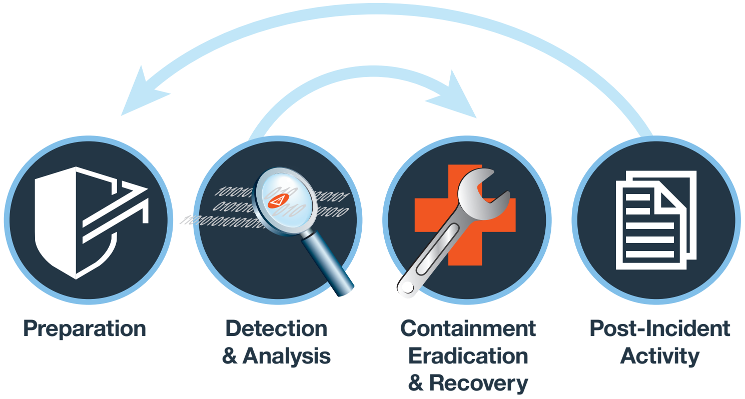


Figure 1. Incident Response Life Cycle

Preparation

This phase involves preparing an organization for the types of events and incidents they are likely going to encounter. Detailing all aspects of incident response is beyond the purpose of this document, but the following recommendations are provided as steps an organization can take to help prepare for and prevent a ransomware incident. Because of the quick evolution of ransomware, IBM notes that the preparation phase of the NIST Incident Response Life Cycle is the most important. Once malicious ransomware files have been detected, it is likely too late and your files have been encrypted. It is important to utilize a defense-in-depth strategy; several preparatory prongs are essential in confronting ransomware and ensuring it never has the opportunity to infect your environment.

[4] *http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911736*

END-USER EDUCATION

Proactive end-user education and training continue to be critical in helping to prevent ransomware and malware incidents in general as it is not uncommon for end-users to be the first to encounter a security incident. Because of this, it is highly recommended to have periodic training for end-users on the types of threats they are likely going to encounter and what actions they should or should not take on an information system while performing their jobs. Ultimately, a security conscious workforce is a rare cultural asset which only serves as a cost-effective multiplier for the security posture of the organization.

RECOGNIZING A RANSOMWARE EVENT

When executed, ransomware creates several telltale signs that an information system has been compromised (see Detection section). End users should know how and who to contact to quickly report anomalies. For example, if an employee stumbles across a file that has been encrypted by ransomware, or the HTML/TXT file most leave behind to inform the user of payment instructions, has that employee been educated to the behavior of ransomware, what that message means, and who they should report that to immediately to help minimize the overall impact to the organization? If end users are unable to recognize a security event and report it via proper channels, the organization may never become aware that a security event has ever occurred.

E-MAIL AS AN INFECTION VECTOR

Consider performing periodic unannounced mock phishing exercises where the users receive emails or attachments that simulate malicious behavior. During such campaigns, generating metrics on the number of users clicking on suspicious attachments or links is essential to demonstrate improvement. A successful campaign requires generating a baseline of the number of users clicking on suspicious attachments or links, followed by educating the workforce, and then a follow up campaign to quantify the increased awareness within the organization.

The common file formats (extensions) used in emails for malicious attachments include: ZIP, RAR, JS, PDF, DOC, XLS, CHM, HTML. Often double-extensions — sometimes with lots of padding via spaces — are used to hide the ‘real’ file format and make the victim believe the file is safe to open. Often those email attachments that are .ZIP or .RAR files will contain malicious .JS, .DOC, .XLS, .HTML, .PDF files.

MACROS AS AN INFECTION VECTOR

Ransomware is also commonly distributed as an Office Word document which contains a macro. Once the user opens the document they are encouraged to "enable the macro to see more information". Once this is done, the macro will fetch an additional payload that can circumvent traditional security tools by downloading data that is encrypted and then decrypt it on the infected computer, thus bypassing security tool inspection during transit. Distributing malware via macros is a very old technique, dating back to at least the mid-1990's, and probably one that many security programs do not address since it has not been popular in years. This legacy attack method and lack of knowledge by users may lead to them to enable a macro on a weaponized Office document merely because they do not understand the risks involved and have not been informed of the dangers.

STRIP/PROHIBIT ATTACHMENTS WITH EXECUTABLES FROM EMAIL

Most organizations configure their email servers to prohibit the sending or receiving of emails with executable files as an attachment. It is also fairly common for attackers to send an email with a ZIP archive attachment that contains executable malware. Organizations often configure their email gateways to scan inside of ZIP archive attachment, but not to strip/remove the executables. If the anti-virus scan does not detect the executable as a threat, then it will eventually make it to the user's mailbox and to the endpoint.

When possible, it is recommended to configure the email server to strip any executable file, including files within archives (that are not password protected) that have an EXE, COM or SCR extension and since 2016, also consider stripping .JS extensions. These files should be stripped before allowing delivery to the user's mailbox.

Depending on what security tools are in place within an organization, the organization may also consider automatically quarantining Office document attachments that contain macros because that is also a common distribution method. Some organizations have taken this a step further and quarantine all attachments, regardless of type and then hold them for approval and release to the end-recipient.

For some organizations, a better solution for Office documents is to white-list trusted macros (signed) and block all others; in cases where new business document macros need to be whitelisted, this should be change-managed to ensure that a full audit trail exists (to minimize the risk of this being misused by malicious insiders).

New versions of ransomware are appearing each day and often go undetected by popular corporate antivirus products for several days.

MAINTAIN CURRENT ANTIVIRUS AND/OR ENDPOINT PROTECTION

Endpoint antivirus solutions should never be relied up as the only protection mechanism for threat, but they are the most common initial detection mechanism. It is recommended that organizations ensure their antivirus solutions are updated with the latest virus definitions to maximize their effectiveness. Ransomware is constantly evolving and changing in an effort to avoid detection. New versions are appearing each day and often go undetected by popular corporate antivirus products for several days.

Organizations should consider using different antivirus products for different purposes, i.e. one antivirus product for the desktops, a different one for servers and another for the email gateway. This strategy can provide maximum coverage for emerging threats that may not be detected by one of the antivirus solutions, but may be detected by one of the others.

Consider additional endpoint protection solutions such as IBM Security Trusteer APEX Advanced Malware Protection[5] or endpoint integrity solutions such as Carbon Black which do not rely on signatures, but rather behavior and trusted applications.

RESTRICT EXECUTION OF PROGRAMS FROM TEMP FOLDERS

Malware commonly uses temp folders as the initial execution point and ransomware is no different. When possible, it is recommended to use Group Policy Objects (GPO) or Software Restriction Policies (SRP)[6] to restrict the execution of any program from generic temp folders and from within temp folders in a user's profile, such as "`c:\users\<user>\appdata\temp`".

For example, when most ransomware is initially executed, it tries to copy the malicious payload to the user's temp folder to continue the execution chain. If that were to be blocked, the initial malware infection would be blocked.

A more robust solution is to utilize AppLocker to disable executables being launched from not only temporary folders but also other non-standard folders, such as in %AppData% or %LocalAppData%, which most commercial/professional software should not use. Many ransomware and other malware will use these folders.

[5] *http://www-03.ibm.com/software/products/en/trusteer-apex-adv-malware*

[6] *https://technet.microsoft.com/en-us/library/cc759648%28v=ws.10%29.aspx*

MAINTAIN AN AGGRESSIVE AND CURRENT PATCH MANAGEMENT POLICY

Ransomware (and malware in general) often uses zero-day7 vulnerabilities to further their campaign. This attack vector is also one that may not be monitored as heavily as incoming email messages. Threat intelligence reveals that many different versions of malware, including ransomware are quick to implement zero-day vulnerabilities in an attempt to increase their revenue.

Organizations should adopt an aggressive patch management policy, especially with browser vulnerabilities such as Adobe Flash and Java that are used by a large population of employees. Patches should be applied in a timely basis. IBM notes that the recent Adobe patches for ransomware are to be applied "as soon as possible" and Adobe defines this time period as "within 72 hours."[8]

INCREASE DNS VISIBILITY, SINKHOLE & WEB FILTERING CAPABILITIES

In the case of ransomware, initial DNS resolution by the malware relies on the domain generation algorithm (DGA). This makes blocking known bad domains much more difficult since it has the ability to generate and use thousands of different domain names to reach the command & control server.

Nevertheless, having good visibility into the corporate domain names server(s) (DNS) can be extremely helpful when working on an incident and for providing an early warning system. Being able to search and monitor the DNS requests that are happening provides the ability to see patterns, such as frequent DGA style DNS requests. Organizations should also consider implementing a DNS sinkhole[9] capability rather than outright blocking specified IPs or domains at the egress gateway. Using a sinkhole allows the organization to redirect domains (and IPs) to a specific internal server that can provide advisories to users who attempt to go to blocked sites. The sinkhole also provides real-time notification capability of when computers are attempting to go to specific sites.

Organizations should consider implementing a reputation-based web filtering capability. Keeping track of blacklisted IPs, domains and sites in general is a never-ending job. Next-generation firewalls and proxies rely on real-time reputation feeds that crowd source intelligence information and help protect organizations by implementing known bad destinations quickly, providing rapid blocking capabilities when sites have been discovered as having malicious content.

[7] *https://en.wikipedia.org/wiki/Zero-day_%28computing%29*

[8] *https://helpx.adobe.com/security/severity-ratings.html*

[9] *https://en.wikipedia.org/wiki/DNS_sinkhole*

ENFORCE LEAST PRIVILEGE METHODOLOGY

Since ransomware targets common user files on the local system as well as network shares, it is recommended by IBM Security's Emergency Response Services team that organizations use the least privilege methodology and only grant the permissions necessary into folders each user may require in order to perform their daily job. Since an infected computer operates with the permissions of the user currently logged on, it can only traverse and encrypt files it has read & write access to. If a user does not require read/write access to various network shares, consider removing, at a minimum, write permissions from the locations that are not required to be accessed by users for a routine business need.

CONSIDER DISABLING FLASH

Adobe's Flash has been a well-documented infection vector for ransomware. In July, Mozilla took the unusual step of blocking Flash by default due to the mounting security flaws in Flash. Because of the risk posed by Flash, IBM's Emergecny Response Services recommends that organizations consider disabling Flash within the organization by default. Should a business case exist for select users to use Flash, said uses may benefit from additional safeguards (e.g. dedicated high risk network segmented from the organization). While disabling Flash won't remove all risk from Internet activity, it will decrease the number of well-used infection vectors open to attackers.

CONSIDER DISABLING WINDOWS SCRIPTING HOST

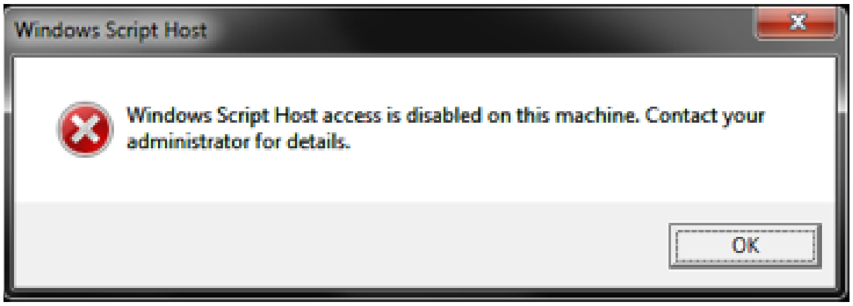
The use of JavaScript or VBScript by ransomware (and other malware) has been increasing over the last few years. This has been used by the malware authors because Windows Scripting Host (WSH) is enabled on all Windows systems by default.

However, many organizations do not use it, or use it sparingly. This allows a large attack vector for the ransomware authors to use and abuse, leading to a high chance of the malware-dropper script being successful and starting the ransomware ball rolling to its file-encrypted conclusion.

This can be centrally prevented via Group Policy. Create the following registry key and value:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings\Enabled and set the 'Value data' field of Enabled to '0' (That is a zero without the quotes).

This will effectively de-fang any ransomware or other malware that attempts to use JavaScript or VBScript to infect a system. Iinstead of happily executing the script, the following will be shown to the user:



Windows Script Host access is disabled on this machine. Contact your administrator for details.

Figure 2. Windows Script Host disabled message.

This warning message box is preferable to your users seeing a ransom note, because by then it is too late. Just note that disabling WSH will prevent users from running any scripts (including VBScript and JScript scripts) that rely on WSH.

HAVING A PLAN

Responding to ransomware or other types of malware may require a cross-functional response within the organization. Having a clearly defined, up-to-date incident response plan with pre-defined roles and responsibilities is an essential preparatory step which enables the organization to have an organized response process should ransomware be detected.

Responding to ransomware or other types of malware may require a cross-functional response within the organization.

Detection

The manner in which an organization realizes they have been a victim of ransomware may vary. The most time-sensitive issue is to identify any and all systems that have (or may have) been infected with ransomware. The reason for this is to help minimize the risk to the organization by isolating the infected systems. It also helps stop any encryption process that may still be underway, thus reducing the damage to the organization and the effort necessary to restore the organization to normal business.

Keep in mind as you read the scenarios below that just because an organization identifies one host that is infected or is responsible for encrypting files, that does not mean that others are not affected. If one host within an organization is infected, there is a high chance there are multiple hosts infected because the same vulnerability may exist within the entire enterprise. Most ransomware will not re-encrypt files that are already encrypted. Therefore, if you identify an infected host that is responsible for encrypting files, especially on a network share, monitor the shares very closely after you take the infected host offline in case there are other hosts that are infected and continue the encryption process.

SCENARIO ONE – A NETWORK USER ATTEMPTS TO ACCESS A FILE ON A NETWORK SHARE AND FINDS IT IS ENCRYPTED

This first example presents the most potential risk to the organization. In this case, there is an infected computer somewhere on the network. The user using the computer has access to a network share(s) and the ransomware, which is operating with the user's permissions, is going through all the network share and files to which the user has access.

If the organization is large, the number of files the user can access could be several hundred thousand, which could take days for the ransomware to encrypt. This delay can contribute to the fact that the victim computer never displays a message since it is still going through all the files and network shares to which the user has access.

In this case, it is extremely important and time sensitive to determine the victim computer. This is most commonly achieved by looking at the ownership permissions of the files that have been encrypted and/or looking at the ownership permissions of the new file that was created in each folder notifying users that the files have been encrypted. This new file will commonly inherit the user's permissions that ransomware was executing under, causing the file's owner to be listed as the user account that initially became infected with the ransomware.

SCENARIO TWO – USER ATTEMPTS TO ACCESS A LOCAL FILE AND FINDS IT IS ENCRYPTED

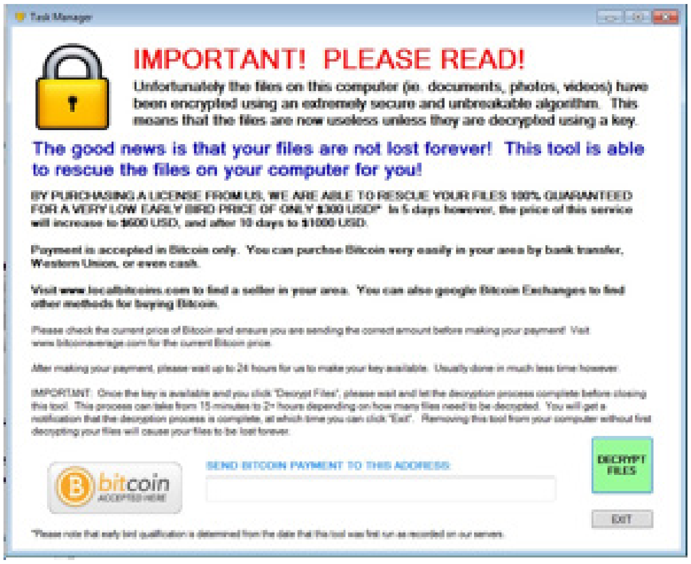
The second possible scenario is when a computer becomes infected and a user finds files on the local system that are encrypted and inaccessible, but they have not yet received a pop-up message. In this scenario, it is likely that the encryption process is currently in progress and the user just happened to try and access a file that has been encrypted, but the ransomware has not completed its malicious activity. Most variants of malware leave a text file or HTML file in each folder they encrypt that informs the user the files have been encrypted and are being held ransom.

In this case, the victim computer should be shut off immediately since the likelihood is that the malicious process is currently active and still going through the various folders on the local (and possibly network) drives and rendering them inaccessible. The system should be turned off immediately and IT security staff should be notified. The system should not be turned back on otherwise the encryption process will continue and may complete, rendering all user files inaccessible.

SCENARIO THREE – USER RECEIVED POP-UP MESSAGE ON THEIR COMPUTER

In this last scenario, a victim computer (or computers) within the organization will silently become infected and begin encrypting all the user's local files as well as all the files the user may have access to on network shares.

Once the encryption process is complete, a message will pop-up on the infected computer notifying the user their files have been encrypted and providing a method to pay the ransom. The text of a message displayed to the user may vary and look similar or different than the example shown below.



IMPORTANT! PLEASE READ!

Unfortunately the files on this computer (ie. documents, photos, videos) have been encrypted using an extremely secure and unbreakable algorithm. This means that the files are now useless unless they are decrypted using a key.

The good news is that your files are not lost forever! This tool is able to rescue the files on your computer for you!

BY PURCHASING A LICENSE FROM US, WE ARE ABLE TO RESCUE YOUR FILES 100% GUARANTEED FOR A VERY LOW EARLY BIRD PRICE OF ONLY $300 USD!* In 5 days however, the price of this service will increase to $600 USD, and after 10 days to $1000 USD.

Payment is accepted in Bitcoin only. You can purchase Bitcoin very easily in your area by bank transfer, Western Union, or even cash.

Visit www.localbitcoins.com to find a seller in your area. You can also google Bitcoin Exchanges to find other methods for buying Bitcoin.

Please check the current price of Bitcoin and ensure you are sending the correct amount before making your payment! Visit www.bitcoinaverage.com for the current Bitcoin price.

After making your payment, please wait up to 24 hours for us to make your key available. Usually done in much less time however.

IMPORTANT: Once the key is available and you click "Decrypt Files", please wait and let the decryption process complete before closing this tool. This process can take from 15 minutes to 2+ hours depending on how many files need to be decrypted. You will get a notification that the decryption process is complete, at which time you can click "Exit". Removing this tool from your computer without first decrypting your files will cause your files to be lost forever.

SEND BITCOIN PAYMENT TO THIS ADDRESS:

*Please note that early bird qualification is determined from the date that this tool was first run as recorded on our servers.

Figure 3. Sample Ransomware end-user pop-up message.

Each variant of ransomware can have a different message that is displayed to the user and/or the message text itself may vary. The message displayed on the infected computer is very helpful in determining with which variant of ransomware the victim computer is infected. Any displayed messages should be captured by taking a screenshot or photo with a mobile device. We will discuss the importance of determining the ransomware variant in a later section.

The Analysis phase largely focuses on two areas: 1) identifying the specific variant of ransomware and 2) determining how the malware entered the organization.

Analysis

The Analysis phase largely focuses on two areas: 1) identifying the specific variant of ransomware and 2) determining how the malware entered the organization.

MALWARE IDENTIFICATION

When embarking on the Analysis phase of the incident, it is essential to identify the specific variant of ransomware within your environment. Because there are many varieties of ransomware with new ones emerging on an all too frequent basis and each with their own unique capabilities, understanding which variant of ransomware is a prerequisite before advancing to the Containment phase. Some versions of ransomware, such as SamSam, have the capability to leverage lateral movement while other variants may not have this capability. The capabilities of the ransomware will greatly influence your later containment steps.

Determining the variant can be tricky and IBM recommends the organization seek internal subject matter experts or external professional assistance, such as a security services provider, in helping determine the variant.

ROOT CAUSE ANALYSIS

An abridged level of root cause analysis (RCA) should be done to help an organization understand how the ransomware was introduced into their environment. While a formal root cause analysis can wait until the Post-Incident Activity, an abridged RCA will aid in the organization when the Containment phase is entered. Without this analysis, the infection cycle will likely repeat itself. It is also important to do the RCA before the recovery phase, since an organization could expend a large amount of time and effort recovering files only to have them encrypted again shortly thereafter.

There are two common ways ransomware arrives in an organization— via an unsolicited email with an attachment or via web browser vulnerabilities, such as the recent Flash vulnerability that was implemented into the Angler exploit kit. If an employee received an unsolicited email that contained ransomware, there is a high re-infection. If it is determined that the ransomware was received via email, a search across the organization's email store should be quickly conducted to identify other, possibly unopened, emails sitting in employee's mailboxes. These emails should be immediately extracted and purged.

Web browser vulnerabilities are a little more complicated and harder to determine, but the RCA will likely rely on the organization's patch management infrastructure. A proper analysis would help identify what initial website caused the infection, thus providing the organization the ability to block access to that site by all other employees and helping to reduce the chance of future similar incidents. The organization should keep in mind that while blocking the identified malicious site is a first step, it may not be an adequate compensating control since employees who are mobile will not be blocked by the organization's firewall rules while they are not on the organization's local area network (LAN).

A more recent method is that ransomware is introduced by hackers exploiting known vulnerabilities in JBoss and then installing webshells or backdoors to allow them to manually deploy ransomware to identified systems.

IBM recommends using internal incident response subject matter experts (SMEs) or an external third party SME to assist in a proper root cause analysis.

Containment

Once a system has been identified as potentially having ransomware, the potentially infected computer should be immediately removed from your networks (including WiFi), and either shut down, or ideally hibernated (to assist in forensic and sample analysis) in order to minimize the risk of the ransomware continuing the encryption process.

Failure to quickly isolate the system from the network may contribute to the incident by allowing the malware to continue to encrypt files on the local system and/or network shares, thus increasing the recovery efforts the organization will need to take.

LAST RESORT CONTAINMENT

If the organization *cannot quickly determine* the source of the ransomware and encryption process, as a last resort the organization should consider taking the file share(s) offline to help minimize the risk and impact to the business. The file server(s) do not need to be shut down, but all access to the file shares should be terminated (remove the share, restrict by network or host-based firewall ACL, etc.). It is not recommended to change permissions on the files within a share in an attempt to restrict access since depending on the number of files, permission propagation could take hours and would allow the encryption process to continue during this time.

If you use CIFS/SMB on other operating systems, including UNIX, Linux, etc. remember to protect these too. This will greatly reduce the chance of these shares being encrypted because to the ransomware they will appear to be Windows shares.

Eradication

This phase involves removing the ransomware from the infected systems. IBM recommends that any system that has been identified as being infected with ransomware should be rebuilt from a trusted source. Additionally, the RCA may reveal that the ransomware came into the organization through email or other mechanisms to which other users have access. If the RCA revealed the malware initially arrived through an email, the organization should search and purge all existing messages still within the mail store. An organization should consider isolating any systems that received the email and/or opened the email until is it verified that the ransomware was not executed on those systems.

If the RCA revealed that the ransomware arrived via a web browser exploit, those sites should be blocked and monitored. The organization should then assess the need to update/remove any vulnerable browser components.

Passwords for affected users should be changed as a precaution.

Recovery

Once an organization has contained the ransomware and identified the root cause of the infection, there are several considerations an organization should examine when beginning the recovery phase. It is very important the organization determine which hosts are infected and the root cause of the infection before beginning the recovery process.

RESTORE FROM BACKUP

IBM recommends an organization initially rely on their internal backup infrastructure to restore the affected files, before any other option is considered. This requires that a backup process already exists for the data affected and an analysis must be done on the frequency and completeness of the backups to ensure the affected data will be completely restored.

An organization should keep in mind that if a network share was involved in the encryption there may be a chance that several of the last backups may contain partially encrypted files. For example, if an organization's file share is backed up daily, but a victim computer becomes infected and takes five days to encrypt everything on the file share before it notifies the user or someone discovers the infection, the last five backups are going to contain files that have initially been encrypted.

The best solution is to have a good backup process — one that utilizes industry best practices, such as ensuring that not only local backups are done, but that backups are also archived to removable media (tapes, optical disks or removable hard disks). Simply relying on local disk images, replication, and other local network backups may not be sufficient, as these can be encrypted by ransomware too, or the backup could be taken after the files were encrypted by the ransomware.

RANSOMWARE VARIANT CAPABILITIES

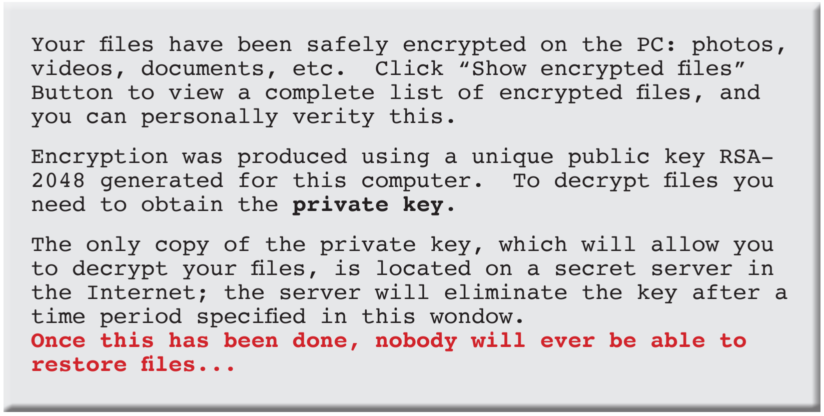
While, ideally, you have identified the ransomware variant in the Analysis phase, knowing the variant and version of ransomware may help in the recovery phase by determining if the encryption process used by the ransomware is reversible without having to pay the ransom. Many variants of ransomware accomplish the goal of securely encrypting your files, while others do not. Determining the variant of ransomware that your organization has been infected with, will potentially provide an alternate recovery option if a restore from backup is not possible.

Contact Information for IBM Incident Response Services

North America:
24x7 Hotline: 1-888-241-9812

Europe, Middle East, Africa, Asia-Pacific:
France (+33) 157327272
Spain (+34) 910507799
Portugal (+351) 213665622
Finland (+358) 972522099
Germany (+49) 69380791120
Netherlands (+31) 707709351
Latvia (+371) 66163849
Italy (+39) 299953631
UK (+44) 2036844872
Denmark (+45) 43314987
Sweden (+46) 850252313
Norway (+47) 23024798
Switzerland (+41) 227614228
Poland (+48) 223062234
UAE (+971) 4 80004442417
Australia (+61) 1888637539

Bear in mind that the stated encryption used by the ransomware may not be accurate. For example, IBM has observed that the original version of TeslaCrypt actually used AES Symmetric encryption, even though it states that is uses RSA Asymmetric (PKI) keys.This is clearly shown in the following screen shot from a TeslaCrypt infection.



```
Your files have been safely encrypted on the PC: photos,
videos, documents, etc.  Click “Show encrypted files”
Button to view a complete list of encrypted files, and
you can personally verity this.

Encryption was produced using a unique public key RSA-
2048 generated for this computer.  To decrypt files you
need to obtain the private key.

The only copy of the private key, which will allow you
to decrypt your files, is located on a secret server in
the Internet; the server will eliminate the key after a
time period specified in this wondow.
Once this has been done, nobody will ever be able to
restore files...
```

Figure 4. Sample screen shot from infection incident.

PAYING THE RANSOM

Organizations may be faced with a decision of paying the ransom in order to recover important files that cannot be recovered by other methods. As mentioned above, each organization should consider this option carefully and only after all other recovery options have been exhausted. An organization considering this option should involve all the relevant stakeholders within the organization in the decision process and consider all possible outcomes.

The ideal solution is one where the data can be recovered, via backups or other data stores. This is preferable to paying up, as otherwise you are validating the ransomware author’s business model and proving that it was a good business decision for them to make. Furthermore, it will only encourage more bad actors to take advantage of a particular situation.

Post-Incident Activity

Post-incident activity should include reviewing lessons learned during the incident response, what detection and security controls may or may not have been in place to help detect and prevent a similar incident in the future. Each organization is different and the recommendations presented in the preparation phase of this document may or may not apply to a particular organization. Therefore, it is extremely important that the organization discuss the incident findings for the purpose of learning new techniques to respond, detect, analyze or prevent similar incidents in the future.