Incident Response Playbook - Ransomware Infection

Metadata

ID	IR-001
Language	EN
Title	Incident Response Playbook - Ransomware Infection
Last Modified	2021-04-18
Status	Draft
Created	2020-12-20

Content

Description

Ransomware attacks can be characterized by infecting large segments of an existing network and encrypting data on server and client systems without the possibility for the legitimate users to get access to this data. The decryption key/mechanism will then be presented to the legitimate user by the attacker in exchange for a more or less reasonable amount of money, most likely in the form of digital currency like bitcoin. The attacker will leave information on the encrypted system on how to contact them for payment and retrieving the decryption methods.
Ransomware became one of the most lucrative cyberattacks in the recent years and is often spread with phishing campaigns against end users or by exploiting unpatched vulnerabilities in external facing systems. Most times the attackers have had deep system access for a long time before the actual encryption of data.
In the event of a ransomware-attack fast response is critical since this could stop ongoing encryption and lateral movement. Most times a hard organization-wide shutdown can't be avoided, but the recovery time can highly depend upon the maturity of the incident response program of the organization.
Ransomware events are most likely only the end of an ongoing infiltration of a network. In many cases the attackers will already mapped your network and gathered credentials long before. Even the extortion of data over a long time span is not uncommon nowadays.
Ransomware in particular is still mostly focused on Windows based systems and domains. The recommendations in this playbook aim to be universal but may sometimes be specific to Windows systems.

Safeguards

These Safeguards are designed to limit the spread and/or impact of a potential ransomware infection. Since ransomware infections often come with wide-spread network compromise the safeguards are also focused on this part.

Mature Patch Management

When preparing for cyberattacks in general it is highly advised to implement available patches in a safe and fast manner. This way known vulnerabilities can be tackled and the exploitation of these can be stopped.
It is important to keep in mind that not only all available components including network components (routers, switches, etc), servers, endpoints and appliances including security appliances need to be in focus. Also patches need to be tested for the internal use and then applied to the systems in focus within a reasonable time frame depending on the criticality of the issues being fixed.
Components that are not longer supported by the vendor or an active community should not be used or only used with great care and additional and appropriate safeguards.

Endpoint Protection

Endpoint protection is about blocking unauthorized changes to a system and to stop the execution of malicious code.
This is normally done with (next-gen) anti-virus software that should always be kept up to date. For systems without support for such software application and execution whitelist could be used.
Endpoint protection need to span on server and client systems and should be configured to alert in a centralized and immediate manner.

Network segmentation

Network segmentation is about separating the network in multiple network zones that house systems of similar use. A very basic separation could be a three tier network architecture with Client-Zone, Server-Zone and DMZ for Server with external accessibility (internet).
The aim of network segmentation is to limit, control and log the network traffic between the different network zones. When this is properly implemented it could be possible to limit the access from the Client-Zone to the Server-Zone to the necessary ports (Web, Mail, ERP...) and block all other access.
The more granular and restrictive a network segmentation is built the better, but it also gets more troubling to manage. A good configuration management is key to achieve this.
Network segmentation can for example be achieved with multiple firewall-interfaces, other means of VLAN or ACLs on managed switches. When creating a network segmentation the different network segments should be thoroughly planned and involve all available systems (including Virtual Machines and Networks).

Backup Strategy

Once any malware has successfully rendered data or systems unusable the most common approach to recovery would be replaying the systems or information from a valid backup.
The backup should follow some criteria to ensure usability in the case of an incident:

- Backups should be regularly and stored off-site or at least offline to ensure that they can't be reached by a potential attacker that has infiltrated the network

- Backup-Server should not be included in the domain and use dedicated accounts to hinder attackers that have acquired a valid domain admin account.
- Backups should be done on a regular basis according to the criticality of the data to the business. For some data it may be required to only lose some minutes or hours in the event of data loss and for other information days or weeks may be fine.
- Replaying backups should be tested from time to time to ensure that the process is working and that data can be restored within a reasonable time frame.

Restrict Administrative Accounts

Before actually deploying ransomware attackers often try to scope and move through the infected network to increase the potential damage that could be done. For this domain-wide administrative accounts are a lucrative target.
Make sure that all administrators have a low privileged user account for their daily tasks and only switch to their administrative account when absolutely necessary. Administrative accounts should also follow the least-privilege principle and domain administrators should be used even more limited. Another point to remember is to use dedicated accounts for services and not use administrative accounts when possible. Other means are Microsoft LAPS.

Security Appliances - Firewalls / IDS / Mail Security

The market offers a huge amount of security appliances for each and every need out there. To protect from ransomware the following are the most crucial:

- Firewall / IDS: Firewalls and IDS have the possibility to block communication to C&C servers and potential downloads of Malware.
- E-Mail Security: Mails including malicious attachments or links are a common tool for attackers. Make sure to have a proper configured spam filter in place and block incoming mails with executable attachments including office documents and content of archive files. Links within mails should be checked as well.
- Managed Endpoint Protection: The endpoint protection solution should be central managed to have a unified view on alerts and the possibility to roll out measures to all devices simultaneously.
- Web-Proxy: Implementing a web-proxy for all connections terminating outside the organizational network can help to monitor and restrict outgoing traffic. Furthermore, Malware which is not proxy-aware could be hindered. For servers internet connectivity should be monitored and restricted even more and a custom proxy could be used.

Endpoint Hardening

Malware infections often start from one host and later spread through the network. Therefore, the protection of all endpoints is crucial. Make sure to limit access and available services to reduce the attack surface.

- Use endpoint hardening checklists offered by the CIS or other organizations to reduce the attack surface
- Remove old and unpatched systems from the network
- Disable SMBv1, Disable SNMP version 1 and 2, disable Windows script host, disable office macros or restrict them further if disabling is not an option
- Restrict internet access where possible. Server should not have internet access in general. If they need to reach certain services only enable FW rules or access lists. Clients in general require internet access

but mostly only for a few services/protocols (Mail, HTTP). Other services can often be restricted. (Like FTP, SSH, RPC...)

- Also make sure to restrict communication within the domain. Not each workstation needs to reach everything in the domain and vice versa.
- Disable USB storage if possible.
- Enable Windows Applocker or other whitelisting technology.
- Enable Microsoft Defender controller folder access.
- Enable Sysmon logging.
- Disable Windows Scripting Host (WSH).

Vulnerability Management

Define and implement a mature vulnerability management process to constantly keep track of vulnerabilities in your network and remediate them accordingly. Known vendors are Tenable, Qualys etc.

Restrict access to Management Interfaces

Management interfaces of all kind are prone to being abused by an attacker. Make sure to properly secure them (MFA) or disable external access all together.
Common management interfaces exists for Web Apps, Network components like firewalls and switches and appliances as well as IoT devices.

Awareness Trainings

Uses are still the number one vulnerability in every infrastructure no matter the size. To tackle this make sure to not give them to many right and properly train your users to identify malicious activity and properly react and notify to it.

VPN

VPN when not properly secured offer an easy way for an attacker to infiltrate a network. Make sure to protect your VPN with current encryption methods, client-certificates and multi-factor authentication. Make as many services available through the VPN but not the internet to reduce your external perimeter. For Site2Site VPNs with third parties make sure that they only reach the needed targets and always configure with least privileges principle in mind.
Also make sure to properly monitor and log authentication requests to find anomalies.

Preparation

Network orchestration tools

When dealing with ransomware attacks it is helpful to have a hardware and software inventory as well as the possibility to roll out patches and software, make configuration changes and populate software to systems in the network. For example to schedule certain scans or patch for known vulnerabilities.

IoC scans for network traffic and hosts

During the analysis of ransomware certain indicators of compromise will be found. It is crucial to be able to scan the network traffic (netflow, IDS, Firewall) as well as the hosts (THOR, YARA) for these indicators in a central manner.

Network segmentation and quarantine

A strict network segmentation enables the possibility to isolate and quarantine certain systems and segments that seem to be infected without having to pull the plug.

Central Log management

For analysis of incidents log data is key. Since attackers do know this as well they often seek to destroy or manipulate log data. A central, secured log service can help for later investigation of the incident, impact and attack methods used. Best utilized is a central log service when all log data is synchronized with a central timeserver and uses a common log format. Central log server should be properly secured to keep attackers at bay and store the data for some time in the past to enable thorough investigations (30 - 90 days considering priority). Logs should be collected for network data (at least netflow), for internal traffic as well as external traffic. DNS requests. System security logs. Authentication logs. Service logs for important services.

Enhance your logging

There are different ways to further increase logging to identify access to critical data. For example with the Windows last access timestamp that can be enabled for certain folders and file shares or WMI Trace Logs. Comparable means are available for other systems as well. Also make sure to properly size your log files to stop them from fast log rotating. Windows and Linux system log sizes can be adjusted. (This is crucial for important server systems like file shares, management systems, domain controller etc. and the central system and security log files)

Network and business knowledge

You will need a in depth knowledge about your network and you core business processes in order to remediate in the proper priority and reasonable timeframe.
This includes but is not limited to:

- Used OS and software
- Used Domain-Policies
- Logging mechanisms
- Prioritized list of business processes
- Prioritized lists of users

Mock Incidents

Training the worst case is crucial for a timely reaction in this certain event. Make sure to properly train all the steps that go into remediating security incidents from time to time.
This involves testing back-ups and how fast you can roll back as well as organizational process like hire additional experts.

Ransom payment policy

As an organization you should have a policy if at all and under which circumstances you are willing to negotiate a possible ransom payment. As always I do condemn paying the ransom in any case, but I do also understand that this is not always an option.

Upfront decisions

There are certain decision that should be made upfront including but not limited to:

- When to pull the plug
- Critical business path and involved systems
- Who can make which decisions
- 3rd party support at hand for forensic analysis, IT support (rebuilding systems and networks), public communication, legal advice...
- If and when to pay a ransom

User and service desk awareness

Ransomware impact often get to know first by the end users of systems and services therefore it is important that these users and the service desk (first level support) where the users will raise their problems are properly trained to detect the signs of system compromise and ransomware infections and that they know where and how to escalate these issues to enable fast first response.

Insurance

Since cyber incidents as any other incidents can cause serious damage and inflict unknown costs it is possible to insure the residual risk for cyber incidents. It is not always the best option, but it should at least be known that this is a possibility.

Detection / Discovery

Detecting Ransomware is normally quite easy since it is a "loud" attack event in its nature. Ransomware events that were successful can most times be identified by:

Ransomware notes

Ransomware notes often come in the form of human-readable text files that include information about what happened (encryption) and how to retrieve the original files (payment). Sometimes also screen backgrounds are changed or new programs are deployed that open up automatically and inform about the ransom.

Encrypted Files

When successful ransomware attacks will encrypt many files on the infected systems, overwriting the original files. The encryption focuses on data that has value speaking of databases and documents and not log files or executables. The encrypted files can be identified by their new file ending which is most likely cryptic or because the file can't be opened and read as normal as before.

Unusual high load

When the encryption is ongoing the system may see unusual high load. For example with high CPU usage, high Disk(I/O) usage and unusual many file and folder access calls. This can be monitored through many tools and should be investigated further.

Anti-virus or IDS Events

Events of your security appliances should be thoroughly monitored and investigated. For ransomware events look out for privilege escalation attempts, widespread use of one account through many systems, unusual administrative account usage (shell usage, WMI, etc.) and blocked execution of unknown software that occurs on multiple systems.

Beacon file monitoring

Many security appliances nowadays use custom deployed beacon files to watch whether they get accessed or changed later on and alert in this case. When such an event occurred on a single system make sure to investigate the access and see whether this was unintentional user behaviour or something malicious. When such alerting occurs in a short time span on multiple systems this is nearly always a good indicator for a ransomware infection.

User reports

In most cases the users will be the first to notice the impact of a successful ransomware infection. In these cases some systems may not be working as expected or information can no longer be retrieved. When such user reports come in make sure to investigate them and look for other indicators of ransomware. Therefore, it is important to properly train your first level support desk to handle these reports and first-hand investigation in a safe and timely manner.

Network traffic

When searching for hints to ransomware infection one normally does not have to rely on network traffic since other indicators may be more present. When searching through traffic logs make sure to watch out for unusual DNS Traffic, direct connections to IP-addresses and not domains, unusual protocols and unusual ports as well as combinations of those. Also look out for internal connections originating from few systems to many others and clarify that these do not present a "normal" behaviour like administrative tasks.

Abused Accounts

Admin and user accounts running havoc and being utilized at unusual times or for unusual action can be a sign of malicious activity in general.

Unusual Executables or Processes (that launch on boot)

Executables files that pop up on one or more systems without any reasonable explanation as well as new auto-start entries are usually a bad sign.

Documentation

Starting with the discovery phase it is crucial to create and continue a documentation of the planned and carried out actions as well as additional information and sightings belonging to the case. This way it is easily possible to on-board new members to the case, hand over to third parties and will be from great value for potential later involvement of authorities. Furthermore, this way improvement to the incident response processes and infrastructure can be easily derived later on.

Containment / Mitigation

Containment of a ransomware threat should better be done too broad then to little. Include at least all systems that show symptoms and incorporate all possible information you can get from the analysis steps.

When containing the infection it can sometime be more effective to focus on the systems that are not infected or show no signs of infection and make sure that they can't get infected later on.

Reset or lock compromised accounts

All accounts that were compromised should be locked and reset before any further use. Make sure to also change the password for all services using the same credentials. Check for abuse of the accounts that are infected.

Secure uninfected systems

For wide-reaching infections it is often more usable to first ignore the obviously infected systems and make sure to secure the non-infected systems. This can be done by starting controlled shutdowns or properly separate the systems.

Encapsulation of infected subnets/systems

When your network is structured in multiple subnets it may be possible to stop the ongoing infection with disconnecting all subnets that show signs of infections. All other systems still have to be monitored very closely to watch out for other corrupted systems.

Pausing of infected or potential infected VMs

Pause (not shutdown) Virtual Machines that show signs of an active infection. This way they may be analysed later without potential data loss.

Shutdown of infected or potential infected Systems (Non-VM)

Shutdown all systems that show signs of infection and are not virtualized. When this is no option at least disconnect the network.

Disconnect shared drives

Normally when isolating systems that includes all network traffic so shared drives should be already among them but since file shares normally do hold precious data one can not stress that enough!

Restrict or disable internet connection for infected segments

For infected systems or network segments the internet connection should be disabled and also internal connections should be strongly restricted to ensure no further spreading is possible and all C&C connectivity is blocked.

Check Back-Up availability

Make sure to check whether back-ups were affected by destruction, manipulation or encryption. Take proper care to secure them and make sure that they will stay unaffected. In the simplest case by taking the back-up off-network.

Secure needed data

Make sure to first care about data that may be overwritten due to log rotation or other means. Export this data to have it available for the analysis. For example logs of firewalls and IDS systems as well as server and clients that can't be paused or shut down are prone to lose data due to overwriting mechanism.

Communication internal and external

Prepare your communication for employees and external sources because you will likely be running a limited network for the next couple of days or even weeks. External communication is also crucial when PII is suspect to be disclosed.

Documentation

Keep in mind to document all actions that were done.

Analysis

Analysis of such incidents should be conducted by a properly trained person. This documentation can only help to provide the most basics steps and give you some kind of guideline.
For analysis steps always make sure to not tamper with the information. Make copies of the original data and work with them. Only mount file systems as read-only to not change any data. Take extra care with live malware and commands/scripts to not infected clean systems.

Determine the Ransomware/Malware type

Ransomware is often reused by their actors in multiple attacks against different targets. Thus allowing to define certain characteristics that are often similar or even the same between different attacks using the same ransomware-software. This information can help through the whole response process. It is therefore crucial to identify the ransomware family. Besides information about the attack some ransomware families are known to have used weak encryption methods or faulty implementation thus allowing for decryption of the encrypted data.
There are several ways to determine the ransomware type. In most events it is sufficient to read through the notes that are dropped by the attacker providing additional information about the attack on how to retrieve the data/make the payment. These notes are either placed in every folder/ the desktop/ opened by itself or visible as a changed background picture. Another indicator may be the file ending of the encrypted files or the encrypted file itself (metadata etc...).
Use normal search engines to identify the ransomware family with the above information or use specialized web services like NoMoreRansom or ID-Ransomware that will take an encrypted file and/or the ransomware note to automatically determine the ransomware type. In many cases this is sufficient. If not you may seek help from professional security providers or ask in the BleepingComputer forum. When you have identified the ransomware family search for already conducted analysis reports and gather the following information:

- Decryption chances: Is it possible to decrypt the encrypted files without paying the ransom? What experiences have others made after paying the ransom? Are all files targeted? Is the whole file encrypted or only some information (may help with large files like databases which could be recovered if only the metadata was destroyed) ?
- Indicators of compromise: What are common attack, persistence and lateral movement vectors used by the actors? Other indicators like network traffic to specific domains etc. . This information can be used to scan and locate and remediate the infection. Where are the executable dropped by the ransomware, are they still there? If so make sure to leave them in place for later analysis.

Determine the attack vector

Try to track down the root of the initial infection through time-lining of infected systems or by statements from employees. Where this is not feasible try to track down the most potential targets and work from there. Common root causes can be:

- Phishing Mails: Mails with malicious links or files attached are one of the most common infection paths. These link often lead to faked pages that try to trick the user into downloading files or entering credentials that will then later be exploited. E.g. VPN Logins. With this you have to rely heavily on user feedback. Make sure to create a culture that supports employees to admin errors otherwise they will not call out to you in respect of the feared consequences.
- Attached removable media: Untrained users may attach non-trusted media or devices to their company systems. This way unknown and untrusted software could be placed or executed on these systems.
- Vulnerable systems: Unpatched, unmanaged or obsolete system pose a great threat and are often targeted by attackers. In focus lay system that are externally facing but this is not limited to them. Every vulnerable system can help the attackers to strengthen their foothold in the infrastructure. System that are often available to attackers and are prone to being exploited are for example VPN gateways, Firewalls, Mail server, Web- and application server, PBX systems, FTP server.
- Unusual events in general: Make sure to also review all unusual events that occurred in the last several weeks or even months and check for possible connections. For example loss of hardware, burglaries, technology partners that were attacked or even employees that were terminated in bad standing can have a context to a malware outbreak way after. The target is to identify the system where the attacker started to iterate the network and gather more information since this will most likely be a system infected very early and close to the attack vector itself if it is not the system posing the attack vector.

Gather information about the malware that was deployed and their damage potential

Try to get a sample from the active malware that was executed on the environment. Normally ransomware comes with various droppers, exploit kits, scanners and so on resulting in multiple binaries that we need to search for. Use the collected IoC from the ransomware family and search for executables in known locations. Other possibilities include reviewing last run software (prefetch, amcache/shimcache), system event logs, MFT timelines, auto start mechanisms (registry auto start keys, autostart folder, tasks, services, CRON jobs, bashrc etc...) and malware search tools like THOR, Rootkit Removal Tools, multiple antivirus suites to identify unknown malware binaries.
Identified malware can be analysed through sandboxes or static analysis measure up to reverse engineering to find out what functionalities the malware had and what other damage may be done which is currently unknown.
Through this means it may be possible to identify system which may not be corrupted or at least not by automatic measures.

Determine the scope of the attack

To properly plan the extent of later recovery and eradication measures it is crucial to identify the scope of the attack. What system were infected for sure, what system may be infected and which system may be untouched. This has to be properly checked of course.
Use automatic tools to scan the network for all identified IoCs. This can include checking for network traffic in central network components (firewalls, proxies, core switches). Other means are YARA or THOR rules or additional policies for the endpoint protection with the help of the vendor.

Another important point is to identify affected data. This should focus on data that is damaged in the form of encryption but also data that may be copied without permission from the systems. When there is no DRM or Data Loss prevention in place this can be a very hard task to identify. Try to scope out the amount of outgoing traffic to known domains of the attackers and from which system it was sent. Starting with this search for manual executed commands or database queries. If you can't further pivot the data that may be corrupted on a system you must assume the worst case. Identify stolen data is crucial since the attacker will try to threaten you with realizing stolen data. This is almost always a very hard task to do and depends heavily on the system to identify such actions in the first place.
Also make sure to check for exposure/disclosure of PII since then you not only have to properly inform all affected persons and the data protection officers but also have to make sure what other measures were in place to secure PII and if they may be breached as well. (Encryption in rest etc.)
Check whether backups were affected and how far the traces of the attack go to identify which backups may be safe. Determine which services are effected and which may be used with limited impact.

Timeline

Creating a timeline of events will help you take different information in a reasonable structure and will enable new clues that evolve through the interaction of different information. Make sure to check that the time zones of different events match your timeline.

Check for backdoors

The attackers will most likely try to preserve a foothold in your infrastructure through so-called backdoors. These have to persist on the file system and need a way of communication with the attacker. Monitor for traffic to unusual domains or IPs from systems that normally don't have active network activity. Restrict all systems to only the network traffic that is needed for the services on the system. Also check for beacon traffic occurring in certain patterns.
Another way is the use of backdoor or rootkit removal tools like Kaspersky TDSSKiller.

Documentation

Keep in mind to document all actions that you conducted as well as the results.

Remediation

Close the attack vector

It is crucial to identify the attack vector and lateral movement techniques used and properly close them. Otherwise, the same vulnerabilities could be exploited again by the same or other attackers in very short time. When the attack vector could not be identified properly you have to make sure to properly increase overall it-security to enhance monitoring and implement safeguards for all identified techniques the attackers have used or abused.

Patching

Make sure to patch all your systems including networking devices. Start with former infected systems and those which are on the network perimeter. Then go for security appliances and servers, prioritizing by with business criticality. Afterwards care for clients and everything else.

IoC search the whole infrastructure

Use the identified IoC's and scan your whole infrastructure to identify infected or otherwise compromised systems.

Remove backdoors and other malware from the systems

Use the knowledge about the identified attack methods to clean all systems from backdoors/Trojans that might AutoStart and other executable programs that might get executed by untrained personal.

Adjust Firewall / IDS / AV

Adjust your security appliances like firewalls, IDS/IPS and endpoint protection systems to identify the known indicators from the attack and be prepared for new outbreaks of malware beacons that were missed beforehand.

Documentation

Keep in mind to document all actions that were done.

Recovery

Recovery can be started after the remediation efforts are done or beforehand in a completely new network zone that has initially no ties to the infected network. When needed the infected systems can be continued to be used with great care and connectivity to other systems should be limited to known good services and protocols. (For example with firewall rules)

Rebuild or cleanse infected systems in a new network zone

Infected systems should be rebuilt from scratch with hardened blueprints in a new network zone without or with very limited connectivity to the infected network. When an analysis of the incident was conducted it sometimes can be possible to cleanse infected systems with known IOCs and not rebuilding them from scratch. But in most cases this will pose a great residual risk.

Rebuild the domain

When domain controller and or domain administrative account were compromised it is often necessary to build a new domain (tree) since trying to clean up the old domain can be tricky. If you want to do this, check for backup accounts, reset all accounts, reset the golden ticket as described by Microsoft (when windows AD) check group policies and even then you may have forgotten something.

Recover data from known good backups

After the systems have been rebuilt, the data from the last known good backup can be restored if available.

Pay the ransom (if no other way can be found)

Decide whether to pay the ransom or not. There are known trusted services to support with this endeavour if necessary.

Address collateral damage

Ransomware and measures to control the incident can result in collateral damage to systems, production and personal. Make sure to properly address these parts as well and make use of the created documentation to identify them.

Ensure that network traffic is back to normal

After a major incident you will spin up system by system and service by service. During this time and afterwards it could be a good invest to monitor the network traffic and search for anything that does not look like it belongs there. Heavy inter-machine communication. External traffic from internal system using unusual protocols, etc. . This becomes even more crucial when you want to include some "old" systems and not rebuild literally everything.

Documentation

As always keep in mind to document all actions that were done.

Post Morten

Review your created documentation and conduct lessons learned sessions to improve the overall process of incident handling as well as overall IT security.

Review the incident response process

Enhance the response process for later incidents by collecting what went good and what not. Identify steps that needed more preparation and use the advice that was given by any involved parties throughout the response.

Discuss security enhancements

During the investigation of an incident many measures and potentials for enhancement will come to light. Keep track of them through the incident handling process and discuss them afterwards with deciders and colleagues to see which will fit your organization best and provide the most use for your overall IT-Security.

Conduct external reviews

To help further harden your infrastructure think about external review opportunities like penetration tests or security audits.

Determine Incident cost

Regarding insurance but also regarding your own controlling it will be necessary to communicate a total number of efforts and damages done because of the security incident. This includes potential losses because your systems were halted and such.
But this is also crucial for you ongoing risk analysis and cost-benefit analysis regarding security invests in the future.