Introduction

Ransomware is a type of malware that is created to encrypt the files on a device and/or network, which in turn makes those files useless and stops the original owner from accessing the data within them, and can even extend to fully affecting the device itself [1]. At that point the attackers will normally demand a ransom in order for the original owners to be able to decrypt their files. These attackers may also have exfiltrated data and may threaten to sell or leak the information that they stole if the ransom that they demanded is not paid [1].

These kinds of attacks occur similarly to any other type of malware, as delivery methods for most of them are extremely similar if not exactly the same. From phishing to exploitation, ransomware may eventually find its way into a system on the network [1]. Most ransomware campaigns have several stages, from initial access to data exfiltration, and finally to the point of where the infected systems are encrypted and the ransom note/information is activated.

Table of Contents

Introduction 1

Initial Access 2

Ransomware Prevention 3

- Employee Education 3
- Reducing the Attack Surface 3
- Evaluate Service Providers and Third Parties 4
- Map the Network 4

Asset Management 4
Prevention is a Many Step Process 4
Responding to a Ransomware Incident 5
Detection 5
Analysis 5
Containment & Eradication 6
Recovery 7
Lessons Learned 7
Record of Changes 8
References 8

Initial Access

Ransomware can end up on a system in a multitude of ways, but the biggest ways are phishing and exploitation [1]. Phishing has multiple different sub-definitions which define specific instances of phishing, like spear phishing. Initial access can also be gained from using sold credentials online. Some threat actors are known for only purchasing remote access to a company's infrastructure and then infiltrating them that way.

Once inside the network, a myriad of tools will be deployed to check for privilege escalation attempts, look for data, extract data, and attempt to spread to more systems within the network [1]. Some of these actions are automated, but sometimes they are done manually by the attackers.

A proper incident response plan is needed to understand the attack in its entirety, what stage it is at, what tools are being used, how to respond, and more [1]. A normal incident response plan has six stages; preparation, identification, containment, eradication, recovery, and review/lessons learned [1]. These usually start as a generalized open framework, and can be redeveloped and altered to fit specific scenarios, like phishing, ransomware, and insider threats.

Ransomware Prevention

Preventing the infection in the first place is important, as preventing a ransomware threat is a lot cheaper in the long run than responding to a ransomware threat. Rapid7 goes over how it's important to reduce the attack surface so that attackers have less to target, and so that the security teams can apply the proper security layers to help reduce the overall risk [1].

Employee Education

Ransomware prevention goes hand-in-hand with employee education since a significant portion of ransomware attacks involve phishing. No matter how good a company's firewalls or internal security is, it can't always stop an unknowing employee. Emails are where most phishing contact will come through, so it is important to train employees on dangers of email and what to look for. Things like external senders, suspicious attachments, and strange links are all great topics to cover [1].

Reducing the Attack Surface

This can come in many forms, but is normally left up to the security team. Things like regular vulnerability scanning, routine patching, making sure devices are correctly configured, and using best practices for hardware and software can all be done to ensure better coverage of the attack surfaces. CISA specifically recommends other things like disabling or blocking the SMB protocol outbound, as it is used by attackers to spread malware across the network [2].

Other things that can be done to reduce the attack surface are:

- Ensure antivirus is up to date
- Use application directory whitelisting on all assets
- Implement an intrusion detection or prevention system
- Have a user awareness and training program
- Filter email traffic
- Disable Microsoft Office macro scripts ability to run for users
- Use multi-factor authentication for all services possible
- Use the principle of least privilege when available
- Secure against pass-the-hash attacks
- Audit user accounts regularly

[2]

Evaluate Service Providers and Third Parties

A few of the biggest infections occurred due to a third-party provider being compromised, so ensuring that third parties are properly audited and that they aren't exempt for any of the company's security policies or detections is important [2]. Sometimes these kind of incidents are extremely hard for a company to avoid, but best practices can be followed to ensure the third-party company is doing their due diligence.

Map the Network

Part of being prepared for a ransomware incident means having a readily available map of the network for the responders. Identify which assets are located where, with information like IP addresses, VLANs, data flows, and more to ensure the responders have what they need [2]. There should be both physical and logical maps of these networks created. This also helps to assess whether the networks are properly segmented or not to contain malware spread.

Asset Management

Tracking who owns what asset and where in the organization can be extremely beneficial to not only responders, but to other IT staff as well. Data, software, and physical machines can all be tracked with asset management. Highlighting specific devices in the network as critical as well can help the company in finding what procedures are necessary to secure, support, and restore them in case of an incident [2].

Prevention is a Many Step Process

There are tons of different things that can be done to reduce the attack surface and prevent the infection of ransomware, the above covered specific areas of it, but here are quite a few more:

- Secure domain controllers
- Set up logging on all systems and log management
- Restrict Powershell/CMD usage

- Create baselines and analyze network activity

[2]

Responding to a Ransomware Incident

Detection

Detection is the first phase of starting the incident response process. Determining whether a system is impacted or not, allows the process to begin [2]. Once an incident has been detected and is potentially suspected to be ransomware, that system needs to be isolated straight away. If it is multiple systems or a subnet, the affected part of the network needs to be taken completely offline and disconnected from any potential servers and switches to ensure the ransomware doesn't continue to traverse the network [2]. If the subnet cannot be taken down, manually remove all ethernet and/or WiFi capabilities from the affected systems; this could be as easy as unplugging the ethernet cable, or as difficult as pulling out the WiFi card. If the devices can't be disconnected from the network in any of the previous methods, they should be powered down.

Threat actors have been known to look at the company's activity and communications to see if they have been detected. Once all of their live connections have been knocked offline, they'll most likely assume that their activity has been detected. Ensure that all responders are using approved secure methods of communication in order to keep the threat actors out of the loop. If the threat actors notice activity and think that they've been detected, they may attempt to move more quickly through the network in order to maintain their access within the organization, or they may flip the switch and activate the ransomware prematurely if it has been caught before activation [2].

Analysis

Once the initial detection of the incident has begun and the affected machines have been addressed, it is time for the phase of analysis. Multiple people will be doing different things at this point. There should be responsible parties triaging the impacted systems to ensure they are restored and recovered, while other parties will be creating documentation and reviewing the initial analysis that occurred during the detection phase [2]. In addition to them, the stakeholders will be contacted and briefed, and the incident response procedures to looping in management and senior leaders at the company will be followed [2].

Now that the analysis phase has been reached, questions need to be answered to help find the necessary response. First and foremost, the type of ransomware needs to be determined. The following things can all help determine the type of ransomware:

- Finding any messages or files left behind
- Analyzing the files or messages
- File renaming scheme or type of encryption used
- Whether file corruption or encryption was used
- Icons utilized
- Files targeted
- And many more items

[3]

Determining the type of ransomware can be tricky, but there are also services that can be utilized in order to help. The next step is analyzing the scope. Find what systems are affected, identifying the markers that show a system as being infected help with this process. Scanning the network for indicators of compromise, checking similar systems, looking for C2 communication and more can all assist in this process [3]. Next the type of data affected needs to be found out, as it can assist in the response as well. “Did the ransomware only target databases or excel files?” is an example of a question whose answer can be searched for. Once the scope has been determined and the ransomware type has been identified, the containment phase can start.

Containment & Eradication

At this point it is time to contain the damage, and prevent further damage from occurring [4]. In the beginning a type of “short-term” containment was done to prevent the ransomware from spreading to other areas of the network, this phase will be more in-depth than that. Forensic imaging of the affected machines needs to be done, along with snapshots of VMs, drive cloning, and further documentation and evidence collection [4]. System logs, network captures, firewall alerts, and everything else to do with this process should be collected and fully documented.

Before wiping the devices, evaluate the backups available for them and test to see if any of them are viable to see if the files can be recovered. If not, reach out to federal law enforcement to see if there are any decryptors available for the type of ransomware on the systems [2]. Ensure the proper steps have been performed to fully contain the version of ransomware that is present, as there are tons of approved guidelines present online.

A ransomware attack isn't limited to just ransomware, data exfiltration could have occurred, and other corporate accounts could be turned into opportunities for the attackers to get back into the system. Identify all of the potentially impacted user accounts and the associated data, and have them change their passwords and prepare public notification of the data lost if needed [2]. At this point, if the decision has been reached to wipe the machines, this can be done as well.

Since proper indicators of compromise have been identified for the specific ransomware strain, it is possible to ensure that there is no continuing infection. This is a part of the eradication stage, ensuring that nothing persists by monitoring for IOCs across the network that was identified within scope, along with the exterior networks to it [2]. Once this is done, systems can be rebuilt.

Recovery

This is when it is time to redeploy and systems that were affected to get them back up and running in the production environment. Prioritization can occur, to ensure that more necessary systems are rebuilt and redeployed first. The systems being deployed need to be patched against the vulnerability that was used to exploit them (if that is how the attack occurred) [4]. Not only the initial cause of the intrusion needs to be patched, but everything else on the systems as well [4]. Complete a final review of the systems to ensure they are operating fully, have been backed up, patched, and have all protections enabled before signing off on them.

At this point, all the parties affected by the breach should be notified as well. Every other task begun through this should be completed, like changing user passwords, and deploying machines [5].

Lessons Learned

After the previous phases have occurred it is time to review everything that occurred before, during, and after the incident to see what went well, what went badly, went can be improved upon, and more [11]. Thorough documentation was to be taken throughout the entirety of the incident, which helps a lot when it comes to reviewing different areas of the response. When identifying weaknesses, vulnerabilities, and areas to improve a remediation plan always needs to be put into place to ensure that these areas have a way to track the improvement status.

All areas are open for review; from looking at the network segmentation, to firewall configuration, all the way to employee or CSIRT training [11]. Once all the incident has been

reviewed and everything has been combed over, a report should be created regarding the incident to distribute to the "relevant parties" [11]. The CSIRT will get a primary report which is more technical in nature, but an executive summary report should be provided to the management team.

Record of Changes

Version #	Date Revised	Author	Revision Description
1.0	3/23/2022	Evan Read	Created the document.
1.1	3/27/2022	Evan Read	Updated the table of contents and created section headers according to research performed. Finalized document.

References

[1]
Rapid7, "Ransomware Playbook Introduction 3," 2021. Accessed: Mar. 27, 2022. [Online]. Available: https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-insightidr-ransomware-playbook.pdf

[2]
CISA, "RANSOMWARE GUIDE," Sep. 2020. Accessed: Mar. 31, 2022. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

[3]
C. CounterActive, "Playbook: Ransomware," *GitHub*, Nov. 15, 2019. https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-ransomware.md (accessed Mar. 31, 2022).

[4]
University of Toronto, "Short Incident Response Playbook for Ransomware | Information Security and Enterprise Architecture," *University of Toronto: Information Security and*

Enterprise Architecture. https://isea.utoronto.ca/policies-procedures/guidelines-2/short-incident-response-playbook-for-ransomware/ (accessed Mar. 31, 2022).

[5]

Cyber Readiness Institute, "Ransomware Playbook How to prepare for, respond to, and recover from a ransomware attack," 2020. Accessed: Mar. 31, 2022. [Online]. Available: https://cyberreadinessinstitute.org/wp-content/uploads/20-CRI-Ransomware-Playbook.pdf

[6]

H. Maskill, "Insure Your Future: The Ransomware Response Playbook," *www.securityinfowatch.com*. https://www.securityinfowatch.com/cybersecurity/article/21238473/insure-your-future-the-ransomware-response-playbook (accessed Apr. 01, 2022).

[7]

CrowdStrike, "Incident Response [Beginner's Guide] | CrowdStrike," *crowdstrike.com*, May 06, 2021. https://www.crowdstrike.com/cybersecurity-101/incident-response/ (accessed Mar. 31, 2022).

[8]

A. Pugh, "Ransomware Incident Response Playbook," *Tandem*, Sep. 14, 2021. https://tandem.app/blog/ransomware-incident-response-playbook (accessed Apr. 01, 2022).

[9]

CREST, "Cyber Security Incident Response Guide." Accessed: Mar. 31, 2022. [Online]. Available: https://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide-1.pdf

[10]

Palo Alto Networks, "Ransomware Playbook - Manual | Cortex XSOAR," *xsoar.pan.dev*. https://xsoar.pan.dev/docs/reference/playbooks/playbook3 (accessed Apr. 01, 2022).

[11]

FRSecure, "Ransomware Response Playbook | FRSecure," *frsecure.com*, Aug. 24, 2021. https://frsecure.com/ransomware-response-playbook/ (accessed Apr. 01, 2022).