NMFTA
National Motor Freight
Traffic Association, Inc.

Ransomware
Playbook Template

Version 1.4 – November 8, 2019

Table of Contents

1. Introduction

Ransomware offers a unique and pressing threat to the business. This playbook template is intended to outline a structured and specific approach in response to a ransomware attack that can be customized and tailored for a specific organization. This playbook is not designed to be a standalone document. Rather, it is meant to be integrated with other organizational security countermeasures across the incident response lifecycle and relevant documents including information security policy, breach notification policy and procedure, security operation procedures and incident management documents. Addressing all of these artifacts are outside the scope of this document.

The National Institute of Standards and Technology defines ransomware as a type of malware that attempts to deny access to a user's data usually by encrypting it with a key known only to the hacker who deployed the attack until a ransom is paid.

This document outlines some ideas on how to prepare for and defend against a ransomware attack as well as what to do should one occur.

2. Playbook Methodology

The main goal of this ransomware playbook is to help organizations develop their own playbook to be able to contain, eradicate, and recover from a malicious infection as quickly as possible. The structure of the playbook is based on National Institute of Standards and Technology (NIST) SP 800-61 *Computer Security Event Handling Guide*. This document outlines the NIST recommendations for security incident handling policy, plans, and procedures.

According to Cybersecurity and Infrastructure Security Agency (CISA) United States Computer Emergency Readiness Team (US CERT) the definition of a cybersecurity incident is

"

[…] the act of violating an explicit or implied security policy". This definition relies on the existence of a security policy that, while generally understood, varies among organizations.

- *These include but are not limited to:*
- *attempts (either failed or successful) to gain unauthorized access to a system or its data*
- *unwanted disruption or denial of service*
- *the unauthorized use of a system for the processing or storage of data*
- *changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent*

"[1]

Detecting ransomware will require diligence on behalf of both the systems administrators and users. This playbook will outline Indicators of Compromise (IOC) that will be used to identify infected machines or malicious activity, as well as response actions to take to mitigate the impact of a ransomware attack on the business. Understanding how the infection occurred and what IOCs were observed will help to eradicate the current threat and block instances of recurrence.

[1] https://www.us-cert.gov/government-users/compliance-and-reporting/incident-definition

3. Resilience

Resilience is an organization's ability to prepare for, respond to and rapidly recover from an adverse event. Resilience is a key overarching concept when defending against not only ransomware attacks but also building a strong and robust business process model. A ransomware attack is fundamentally a test of your organization's resilience or, phrased differently, a test of your organizations reliance on specific computer systems. In a medium to large organization, a single workstation being impacted by ransomware is probably not major issue unless the workstation is the one used for payroll or cutting checks. If, however, entire groups of workstations and laptops are affected or entire systems such as freight logistics, warehouse operations, driver communications, pickup/delivery scanning systems, etc. are knocked out, this can become a critical business event.

Take the time to walk through your day to day business operations and identify each and every business process and the systems they use to evaluate the impact on your business if that system were to be unavailable. What is the backup plan? Do you have alternate operating procedures? How do you meet your business operation needs without that piece of equipment or computer system? For example, if your entire server infrastructure is on a specific cloud provider, what do you do if that cloud provider has a major outage? What if the driver tablet/scanner used to record receipt and delivery of freight becomes unavailable? If the answer is that you don't have any alternatives or backup plans then you have a very fragile operation which is very susceptible to major disruption.

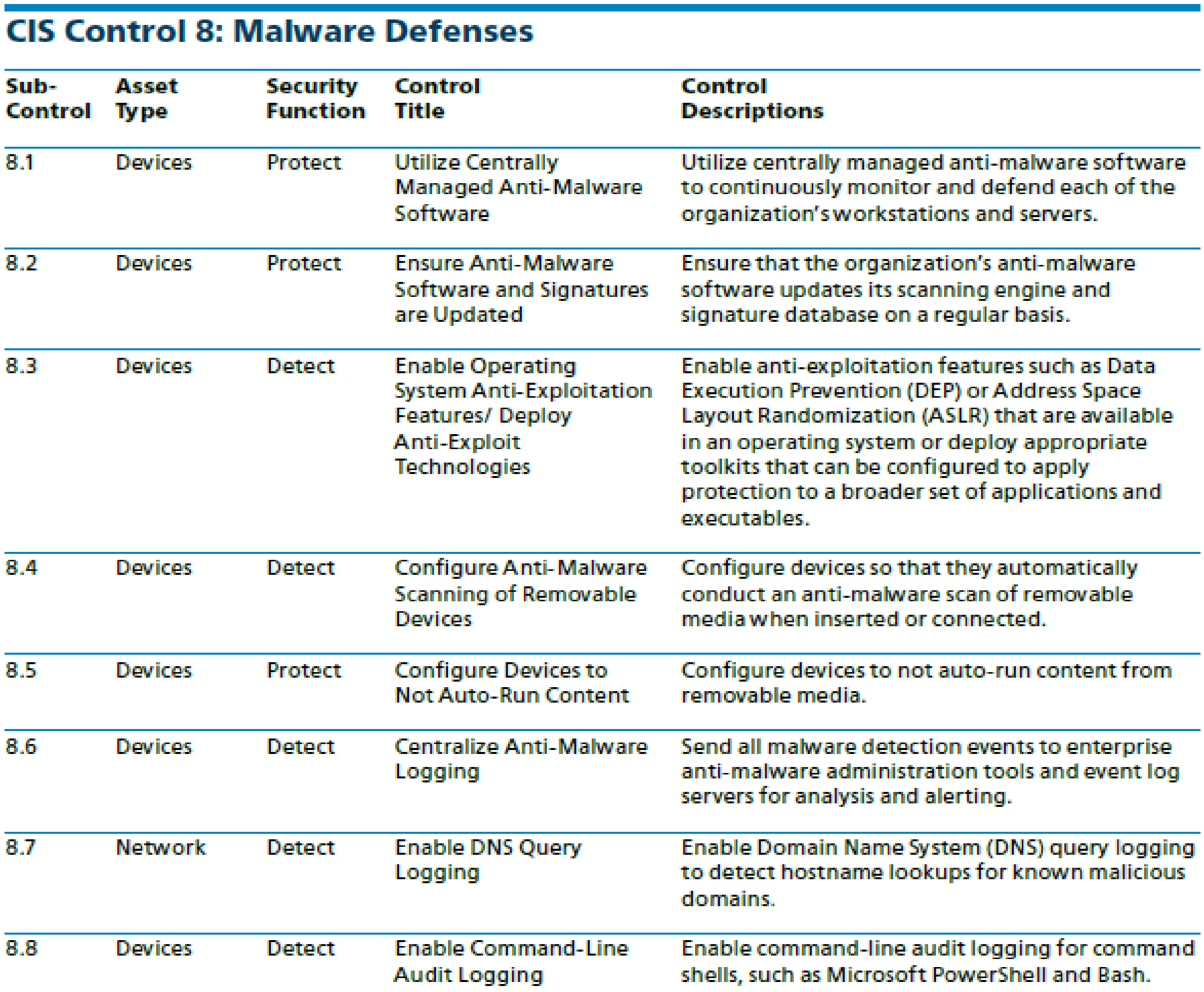
One of key aspects of good resilience is making preparations before an event. For ransomware this means hardening systems and business processes in anticipation of an event. First, harden your environment. The following section goes into more details on some of steps that you can take to harden your environment against a ransomware attack. Then, develop the tools, documentation, processes, and policies before an event takes place so that everyone knows who is responsible for doing what and how to do it. This will help reduce the business impact of the event.

Resilience is a broad and rich area of study and full coverage is outside the scope of this document but it is an area well worth exploring. The U.S. Department of Homeland Security's Cyber Infrastructure and Security Agency offers a free Cyber Resilience Review (CRR) here https://www.us-cert.gov/resources/assessments. Cybersecurity firm Mitre's Cyber Resiliency Engineering Framework can be viewed here https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework.

Some specific lessons learned from the ransomware attack that simultaneously affected 22 Texas municipalities can be found here. To read more about how Lubbock County, TX avoided being the 23rd victim, see this article.

4. Malware Defenses

Good malware defenses help eliminate or reduce the impact of a ransomware event across the enterprise. The starting point is good general cyber hygiene. In order to better protect and detect malware events, risk strategy should be to implement defense in depth in accordance with Center for Internet Security (CIS) Control benchmarks identified below as well as other industry recommendations such as the FireEye white paper on Ransomware Protection and Containment Strategies (Appendix A) and other best practices that are incorporated into network design, configuration, operational procedures and security policies:



CIS Control 8: Malware Defenses

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions
8.1	Devices	Protect	Utilize Centrally Managed Anti-Malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.
8.2	Devices	Protect	Ensure Anti-Malware Software and Signatures are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.
8.3	Devices	Detect	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.
8.4	Devices	Detect	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.
8.5	Devices	Protect	Configure Devices to Not Auto-Run Content	Configure devices to not auto-run content from removable media.
8.6	Devices	Detect	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.
8.7	Network	Detect	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.
8.8	Devices	Detect	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.

In addition to the CIS controls, there are additional steps that should be taken to help reduce risks of ransomware and mitigate the impact.

- Network segmentation between workstations (in most cases workstations do not need to communicate or connect to each other)
- Network segmentation between workstations and production systems
- Regular vulnerability scanning and patching
- Workstation lockdown and configuration (See FireEye report in Appendix A)

- Whitelist and lockdown remote workstation and server access (RDP)
- Map out and document physical network isolation mechanisms
- Maintain a dynamic and frequently updated listing of active network endpoints and ports
- Close all unnecessary network endpoint ports/services and restrict local admin rights
- End user training to learn to recognize the threat that malicious email and USB drives pose to the enterprise
- Please see Appendix B (US Gov - Ransomware Prevention and Response for CISOs) for additional tips and suggestions on how to improve defenses.

The strategy should also include multiple backup and backup storage methods which can be combined to increase the probability that the impact can be minimized to the maximum extent possible. The following are some backup and storage methods:

- Full machine snapshot backups with key data servers backed up every few hours and more static data repositories backed up daily.
- Versioned replication of critical data backup sets between physical sites.
- Weekly rotating offline cold backup sets pulled from the online backups.
- SAN disk storage appliance snapshots including snapshots every two hours for critical server data. These are separate from other backups and are self-contained on the SAN appliance making them very difficult to attack and infect/destroy.
- Standardized offline base images for all workstations and servers allowing for fast wipe and reimaging of all user workstations and servers for faster recovery times.

Cyber Kill Chain

Before an organization can defend and recover from a malware event, it is important to understand how such attacks occur. The Cyber Kill Chain® , developed by Lockheed Martin[2], is a useful construct for analyzing the patterns of an attack and identifying key points in time where an attack can be stopped. The earlier in the chain you are able to contain the attack the less damage will be incurred. In general the cyber kill chain is broken down into seven steps:

Reconnaissance – Performing both active and passive information collection about the target such as networks, architecture, layout, systems, personnel, contractors, etc. The purpose of the reconnaissance is to find vulnerabilities and weaknesses in the defenses of the target to map out the best attack vector.

Weaponization – Developing a weapon (Malware, exploit code, etc.) to use against an identified vulnerability and weakness in the target.

Delivery – Delivering the weapon to the target through email, website drive-by download, or directly accessing systems or networks.

[2] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Exploitation – Compromise the targeted system or machine using the delivered weapon and gaining control of the device. Once a foot hold has been established the attacker may attempt to obtain additional privileges, obtain password hashes, etc. to get enough permissions to persist

Installation – The attacker installs web shells, back doors, or other tools to bypass security mechanisms and obtain persistent remote access. This may also include the installation of malware such as ransomware to be launched at some time in the future.

Command and Control – Remote access tools establish connections to outside command and control servers which allows the attacker to perform actions on the compromised network such as download of encryption keys before encrypting the files in a ransomware attack.

Action on Objectives – The attacker achieves their end goal such as exfiltration of sensitive information or, in the case of a targeted ransomware attack, encrypt computers and wipe out online backups to enable the extortion of the targeted victim. It can also include reinfection during which the attacker activates other types of malware distributed during the initial attack to re-infect machines and/or servers.

The event sequence for a basic ransomware attack to be successful would be as follows:

A. (Reconnaissance) The threat actor identifies a suitable target (you) and begins to collect data about your organization, it's IT networks, and cybersecurity vulnerabilities your organization may be susceptible to
B. (Weaponization) The threat actor develops a piece of malware tailored to your environment. This may be a new piece of malware or a modified version of existing malware
C. (Delivery) A "ransomware" file is delivered, this can occur via:
    - Attachments of web links or files in phishing emails;
    - Malicious Web pages containing embedded files; or
    - Malicious manual or automatic downloads;
D. (Exploitation) Once successfully delivered, the payload is executed on the end device
E. (Installation) Once executed, the file installs malicious software (ransomware) on the machine
F. (Installation) The ransomware then generates a unique key pair to encrypt and decrypt files
G. (Command and Control) The decryption key is uploaded to a secure server in a location the attacker knows
H. (Action or Objective) The malware executes its payload which encrypts your files and data across the local hard disk and ANY mapped network drives or attached external storage including USB hard drives
I. (Action or Objective) Once the files are encrypted, they are inaccessible until the proper decryption key is presented. In certain cases even if the decryption key is obtained it may not always work or result in recovery of the files.

Ransomware attacks are not limited to simple random file access by an unwitting end user and can be part of a larger and more complex targeted cyber-attack. In targeted attacks, threat actors may establish persistence on systems and perform reconnaissance on the network to identify and encrypt/disable online backups and target critical servers to increase the impact of attack.

Ransomware attacks can also be used to mask other malicious activities such as business email compromise (BEC), Personally Identifiable Information (PII) data exfiltration, data modification, wire transfer fraud, data theft, and other criminal activity. In certain cases, such as NotPetya[3], deliberately destructive malware may masquerade as ransomware to hide the true intention of the threat actors.

In the event of a simple "click and run" attack, we can expect that the ransomware would quickly (within seconds) attempt to do all of the following:

- Encrypt local hard disk contents
- Encrypt connected network shared drive contents (user and company file shares and storage including anything mapped as a network drive including SharePoint, accounting systems relying on shared file databases, etc.)
- Encrypt attached USB drives contents (USB backup drives still attached)
- Delete Windows restore points
- Disable Windows recovery
- Attempt to move laterally to infect other workstations and servers via
    - vulnerabilities (e.g. the Eternal Blue [4])
    - hidden administrative network shares (including domain controllers)
    - USB thumb drives
    - Captured or shared credentials[5]

In the event the attackers are resident on the network before the attack, expect them to target online backups and as many servers and workstations as possible before executing the file encryption attack.

5. MITRE ATT&CK

The cyber kill chain does have some limitations and there are additional resources which can be used for threat modelling. The MITRE ATT&CK[6] framework goes much further, not only in defining various steps in the process, but also provides specific examples of types of tools and tactics that are actually being used and by whom, allowing defenders to go much further in their modelling and incident response. The MITRE ATT&CK Enterprise Framework Matrix is available at https://attack.mitre.org/. Additional MITRE ATT&CK resources can be found at https://attack.mitre.org/resources/. The benefit of the MITRE ATT&CK approach as compared to the various frameworks available before is that MITRE ATT&CK is fundamentally based on the attacker mindset and real world tools and tactics. For example, it provides greater detailed information about the reconnaissance phase by listing a large number of 'PRE-ATT&CK' tactics, one of which is highlighted here:

[3] https://www.wired.com/story/petya-ransomware-ukraine/

[4] https://en.wikipedia.org/wiki/EternalBlue

[5] Malware such as Petya used Mimekatz to try to extract credentials from compromised machines to enable lateral movement. https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html

[6] A foundational paper on the subject can be obtained from https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf.

Target Selection	Target selection consists of an iterative process in which an adversary determines a target by first beginning at the strategic level and then narrowing down operationally and tactically until a specific target is chosen. A target may be defined as an entity or object that performs a function considered for possible engagement or other action.

A full list of the PRE-ATT&CK tactics can be found at https://attack.mitre.org/tactics/pre/.

6. Malware Indicators of Compromise (IOC)

Indicators of Compromise are forensic artifacts of a cybersecurity incident that can be identified. This can take the form of malware files, registry entries, modifications of windows scheduler programs, artifacts in memory (e.g. meterpreter shell), log entries, data exfiltration, etc. IOCs are very valuable in forensic investigations to determine the "what, how and who" of a security incident. Most are less than useful for preventing security incidents. You might be able to get file hashes of a certain malware to detect them in a file system but, as attackers have become more sophisticated, they have started generating new and unique signatures for each attack which can bypass many end point, anti-virus and network file security scanners.

The cyber kill chain can provide us with some ideas to identify practical indicators that our systems have been compromised besides the obvious screen message that your machine has been encrypted and instructions on how to pay a ransom in bitcoin.

In order to ransom a computer system, there needs to be communication between the malware and command and control (C&C) servers. Closely monitoring inbound and outbound communication to the internet can provide an early warning. This 'north-south' traffic can be extensive, so looking for specifics can enhance your analyst's effectiveness, e.g. monitoring source and target traffic for communications with known C&C servers or botnets. Additionally, plain text communication over ports which should be encrypted such as 443 (HTTPS) and 22 (SSH) or alternately encrypted traffic over plain ports such as port 80 (HTTP). Finally, actively monitoring your DNS traffic or running all your DNS traffic through a provider that filters for malware can also provide some early indicators that something is not right.

Threat actors are becoming increasingly sophisticated in masking malicious outbound traffic by compromising legitimate system processes. Another point in time of the cyber kill chain that we can monitor for is the encryption process. Regardless of how stealthily the attacker encrypts the contents of an entire hard disk, this action will result in an increase in processor and disk IO utilization. Monitoring side-channels, or physical indicators of the attack, such as resource usage, especially on end user devices like desktop, laptops, and file share servers, can provide early indicators that something is not right.

The active search for these indicators is commonly referred to as threat hunting. The Infosec Institute has at https://resources.infosecinstitute.com/category/enterprise/threat-hunting/iocs-and-artifacts/

Additional resources can be found on the internet at Dark Reading's at https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647 and a LinkedIn article outlining " https://www.linkedin.com/pulse/9-great-sites-ioc-searching-ely-kahn/. The resources available and the IOCs themselves change over time, therefore it is important to keep up to date on the most recent and current sources for IOC. For example, based on actual attacks in the wild, US federal agencies have recently determined that the presence of Trickbot[7] and Emotet[8] are good indicators that a targeted ransomware attack can be imminent.

The best early indicators of ransomware and malware can be identified by knowing your assets and closely monitoring their behavior, performance, processes, and communication.

7. Emergency Network Isolation Procedures

Every organization should have a documented step by step emergency network shutdown process for physically isolating systems and network segments. This process focuses on attempting to save critical systems from damage rather than system up time. Following this procedure will result in loss of system operations and will impact staff and customers, but should be completed as quickly as possible to contain the situation. This is usually something that is designed into a company network at the planning phase as it generally works in opposition to redundancy. Access to this "emergency stop button" should be limited and properly secured. It can be a manual process or something more automated depending on size of the enterprise.

Sample actions could include:

1) Execute a script which powers down switches and routers via PDUs
2) Execute PowerShell management scripts to shut down virtual and physical servers via server management APIs
3) Disconnect the physical uplink connection between core switches and server switches.
4) Physically shut down core switches which connect all workstations to the network thereby isolating all workstations from each other. (Pull the power plugs)
5) Disconnect the firewall(s) from the internet circuit. This will sever the point to point VPN connections as well as stop any exfiltration.
6) Shutdown the specific switches and routers (pull the plug)
7) Shutdown all virtual servers and appliances including the backup system but not the monitoring servers or security appliances required to fight the infection. Shut them down in order of importance. For example:
    a. SQL Servers
    b. Exchange Servers
    c. Backup Appliances
    d. Application Servers

[7] https://attack.mitre.org/software/S0266/
[8] https://attack.mitre.org/software/S0367/

8. Communication Templates

Being able to quickly and effectively communicate with users and customers is essential to any incident response scenario. It is highly recommended that pre-approved communication message templates are created as part of any incident response planning. Being able to use pre-approved message templates can significantly improve the effectiveness of the messaging as well as increase the speed at which the message can be conveyed.

An example company phishing email alert from the security team to the company users can read something like this:

Dear User:

<CompanyName> has encountered a phishing campaign seeking to trick users into /providing user names and passwords/installing malware/installing ransomware. The phishing campaign was limited in its scope and has been contained, however, we recommend preventative action. The email, which resembles the wording and format below, will appear to come from an <CompanyName> employee.

[insert sample of email]

If you receive the email above, do not click on any embedded links or open attachments, instead, delete it from your inbox. You will be advised regarding any additional required actions.

Regards,

<CompanyName> Security Office

Two examples of a customer notifications:

<CompanyName> has not been impacted by the ransomware attacks reported by large companies around the world. Our cybersecurity and IT team is aware of the threats and taking proactive measures to protect our customer and product data.

We confirm that <CompanyName> is experiencing impact from the latest ransomware attack, along with many other reported companies. This affects customers' ability to access _____. We thank you for your continued patience during this time. Our cybersecurity and IT team is taking steps to remedy the issue as quickly as possible. <CompanyName> will provide updates as we move back to operating at full capacity.

9. Playbook

Objective

This playbook has been developed to provide instructions for ransomware incident handling. Ransomware will be detected by technical or non-technical controls implemented across the data environment.

The business objectives for establishing such a playbook are as follows:

- Proactively manage cyber risk by being able to restore data to its last known good configuration
- Position the organization to recover as quickly as possible from a malicious ransomware attack by identifying correct backup actions and versions (free of malware);
- Provide clear guidance and direction that will facilitate the highest degree of data integrity;
- Minimize to the greatest extent possible any disruption to business operations; and
- Preserve evidence to the extent feasible for forensic analysis

Scope and Applicability

All company systems and employees to include contractors working on behalf of the organization.

Response Procedures

There are numerous types of ransomware attacks. Some of the most common types that information security personnel should be aware of include:

- Encryption (traditional Ransomware) - malicious piece of software encrypts data making it unusable by the business
- File modification and deletion – malicious software from a phishing site or user modifies files in the directory and altering the data integrity of business data
- Permission changes – malicious insider creates back door and once inside the domain is assumed to be privileged with administrator access escalation
- Database manipulation – malicious user accesses database data files and executes queries to modify, change or delete data vital to business operations

The procedures for handling these, or similar attacks, will be theoretically the same. Once ransomware is suspected or detected, the priority is to get the infected systems offline as quickly as possible and isolate critical systems from the rest of the network until the situation is fully understood and under control.

The following basic steps from across the phases of detection, analysis and containment should be completed as quickly as possible to mitigate the impact of a ransomware event:

1. User reports incident
2. Get in touch with the user and collect as much information as possible:
    a. Who was affected? (what individual, team, division, etc.);
    b. What happened that triggered the event? (please have user be as detailed as possible)
    c. Where did this occur? (people, systems, data, locations, client facing)
    d. When did this happen? (timestamps and clock data)
    e. Why did this happen? (what actions, precursors lead to the event); and
    f. How did it happen? (ran in background, autorun, click on link or .exe)
3. Have user(s) disconnect device from network, isolate the host, and if necessary turn it off[9]. If possible, collect forensic information from device before turning it off.
4. Notify all the necessary internal parties including the IT Leadership and Senior Business Leadership
5. If the entry point (e.g. phishing email, compromised file, etc.) is identifiable and may have been sent to more than one employee, delete all instances from servers and workstations
6. Collect the IP address, MAC addresses, and computer name of the infected system
7. Isolate physical locations and network segments using established procedure. If it is uncertain that only one location is impacted follow procedures for both locations to safeguard system.
8. Immediately shutdown backup appliances
9. Identify, locate, and secure the latest cold offline backups and determine time gap
10. Look for alerts of indicators of compromise (IOC) that could be related
11. Look in the logs to identify similar IOCs similar across the network (lateral movement)
12. Check logs for suspicious URLs and messages

The steps above must be completed as quickly as possible. As noted they are selected from across three of the phases of incident response: detection, analysis and containment. A more detailed list of actions required to deal with specific ransomware events are detailed below for each relevant stakeholder (team), and in each of the phases (detection, analysis, containment and eradication, recovery, and post-incident) of incident response. The list of actions are not exhaustive and are only a general representation of actions for the specific phase. Each set of actions should be reviewed and adapted as necessary for an actual incident using a tactical mindset.

[9] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf

In the following playbook the names of groups involved have been simplified and may not be representational of your specific company.

End User - An employee of the organization with organization issued computer assets such as laptops, workstations, and cell phones

IT Operations - For the purposes of this document IT Operations team is used in a general way. The specific group names can vary depending on the size of the organization and include groups such as help desk, IT operations staff, etc. and the tasks discussed could be split across multiple teams. In larger organizations, this may include ticketing systems tracking end user requests.

IT Leadership – Depending on the size of the organization this could be a single person or it could be a combination of roles such as a Chief Technology Officer, Chief Information Officer, or Chief Information Security Officer depending on organizational structure and granted authorities.

Senior Business Leadership – This would be the business leadership group who are empowered to make high level decisions impacting the business and communicating with the board of directors. In small organization this could be a single individual or a full management team made up of CEO, CFO, CIO, General Counsel, etc.

Customer Service – The group of company employees which communicated directly with customers by operating the customer service hotline and mailboxes. In larger organizations, this may include customer inquiry ticketing systems.

Detection Phase

During the ransomware incident management detection phase, teams will evaluate a potential ransomware incident.

Detection Phase Roles, Responsibilities, and Actions

End User
During the incident management detection phase, the end user will report suspicious emails, endpoint issues, and system/service disruptions.

Actions for the End User:

- □ Report a suspicious email.
- □ Report suspicious behaviour of an endpoint.
- □ Report a system or service disruption.
- □ Report a pop-up screen preventing access to an endpoint.

IT Operations
During the incident management detection phase, IT support staff will monitor calls and emails. IT Operations staff monitors systems in accordance with established operational policies and procedures using a task tracking system, which outlines daily, weekly, monthly, quarterly, and annual monitoring and compliance items, to maintain a record of the activity by recording observations and attaching supporting logs or other information.

Actions for IT Operations:

- □ Investigate reports as required.
- □ Review a firewall event or series of events.
- □ Review an IDS/IPS event or series of events.
- □ Review suspicious internet connections.
- □ Review an antivirus event or series of events.
- □ Review an anti-malware event or series of events.
- □ Review an email gateway event or series of events
- □ Open a support ticket.
- □ If necessary, generate an incident report and initiate proper processes and notifications.

Analysis Phase

During the ransomware incident management analysis phase, teams will analyze the incident to determine the impact of the threat. Depending on the impact, a number of teams will be involved in the remediation of the ransomware incident, and the notification of the threat will be escalated as appropriate.

Analysis Phase Roles, Responsibilities, and Actions

End User

During the incident management analysis phase, end users will provide information related to the incident as required.

Actions for the End User:

- ☐ Provide information to the IT Operations team, related to the incident.

IT Operations

During the incident management analysis phase, the IT Operations team directly interacts with the end user(s), asks incident-related questions, takes actions, and documents findings. Depending on the nature of the event, the IT Operations team will also analyze appropriate logs, conduct open-source intelligence research, provide technical support, provide incident coordination support, directly interact with the end user, ask incident-related questions, take actions, and document findings in the incident record.

Actions for IT Operations team:

- ☐ Gather answers to incident-related questions.
- ☐ Facilitate end-user notifications.
- ☐ Decide if any local/server data was encrypted.
- ☐ Determine any endpoint exposures and the potential risk implications.
- ☐ Document all connections to the impacted device(s) and the order in which the connections were disabled.
- ☐ Assess organizational exposure for all internet-facing endpoints.
- ☐ Search web proxy logs to identify any outbound command and control traffic.
- ☐ Conduct open-source threat intelligence analysis to identify comparative indicators of compromise (IOCs).
- ☐ Collect and backup firewall, IDS, IPS, email gateway, and system and server logs.
- ☐ Perform IOC search in firewall, IDS, IPS, email gateway, and system and server logs.
- ☐ Determine if any end user devices had attached USB devices; assume that they were compromised.
- ☐ Assess if any servers were impacted and plan remediation if necessary.
- ☐ If practical, obtain memory images from at least one workstation (e.g. Volatility[10], PCILeech[11], etc.) to facilitate forensic analysis by LE. [**NOTE**: If necessary request assistance from US FBI through local field office or other organizations with proper expertise]

[10] https://www.volatilityfoundation.org/
[11] https://github.com/ufrisk/pcileech

IT Leadership

During the incident management analysis phase, the IT Leadership will notify and coordinate with the relevant stakeholders and Senior Business Leadership.

Actions for IT Leadership:

- ☐ Establish priorities for containment, remediation and recovery, if applicable.
- ☐ Publish corporate-wide situational awareness alerts to inform end users of any system outages. Notify end users of any required changes to processes or access points.
- ☐ Coordinate and inform Senior Business Leadership of any incident updates.
- ☐ Determine if third party technical assistance is required.
- ☐ Approve the disaster recovery enactment plan (if applicable).
- ☐ Report any external criminal activities to Senior Business Leadership.
- ☐ Determine if any incident information should be shared with external parties.
- ☐ Notify law enforcement, if approved.

Senior Business Leadership

During the incident management analysis phase, the Senior Business Leadership will direct outside counsel, human resources, and public relations staff to analyze any insider activity and brand or reputational damage. The leadership will also determine the chain of command and incident response leader to manage incident response going forward.

Actions for Senior Business Leadership:

- ☐ Determine the chain of command and overall incident response leader, if applicable.
- ☐ Determine if third party legal assistance is required.
- ☐ Determine if any regulatory, legal, or compliance mandates have been violated or impacted.
- ☐ Determine if any breach notifications are required.
- ☐ Determine if any employee acceptable-use or security policies have been violated.
- ☐ Determine if any employee disciplinary actions are required.
- ☐ Determine if any public reputational or brand damage has occurred.
- ☐ Provide an incident summary/updates to the board of directors.
- ☐ Approve reporting of crime to law enforcement.
- ☐ Approve communication of any incident information with external parties, such as ISACs, federal, or business partners.
- ☐ Approve communication of any alternate access or business processes, activation of hot sites, or outage notification with external parties.

Containment Phase

During the ransomware incident management containment phase, teams will isolate and contain the infected device(s), servers, and storage arrays, and ensure they are not allowed back on the network.

Containment Phase Roles, Responsibilities, and Actions

Customer Service
During the incident management containment phase, Customer Service will maintain communications with any impacted customers.

Actions for the Customer Service team:

- □ Maintain communications with any impacted customers.

Decisions for the Customer Service team:

- ❖ Are any customer communications required?
- ❖ Are any alternate customer access instructions required?

IT Operations
During the incident management containment phase, cybersecurity staff will document all findings in the incident report.

Actions for the IT Operations:

- □ Facilitate end-user notifications as directed by IR leader/ chain of command.
- □ Isolate or disconnect the infected endpoint from the network using established procedure.
- □ Disconnect infrastructure from internet using established procedure.
- □ Isolate systems and subnets as necessary using established procedure.
- □ Create an OS-level image of any endpoint, servers, or storage arrays to preserve evidence and provide an alternate potential source for specific data recovery.
- □ Snapshot virtual servers to create a restore point.
- □ Provide incident coordination support.

Decisions for IT Operations:

- ❖ Which systems and networks need to be isolated?
- ❖ Who needs to be notified of the incident findings?

IT Leadership
During the incident management containment phase, the IT Leadership will evaluate any control weaknesses and make recommendations for remediation.

Actions for IT Leadership:

- □ Review and approve isolation plan.
- □ Provide Senior Business Leadership with incident updates.

Decisions for IT Leadership:

- ❖ Does the organization need to engage 3rd party technical resources to help with containment?
- ❖ Does the organization need to implement any new or update any existing security controls?

Senior Business Leadership
During the incident management containment phase, Senior Business Leadership will determine if any core business function is impacted.

Actions for Senior Business Leadership:

- □ Review isolation plan for business impact.
- □ Take any appropriate actions to inform legal or government agencies.
- □ Assess any brand or reputational damage.
- □ Use a PR campaign to reduce reputational damage as appropriate.

Decisions for Senior Business Leadership:

- ❖ Do any third-parties or government agencies need to be notified?
- ❖ Do customers need to be notified?
- ❖ Do any additional stakeholders need to be notified?
- ❖ Will the incident be disclosed to internal and/or external parties as a malicious incident? If so, when and how frequently should situational updates be issued?

Eradication Phase

During the ransomware incident management eradication phase, teams will restore and reissue endpoints and servers. After an incident has been contained, eradication may be necessary to eliminate components of the incident such as deleting malware and disabling breached user accounts as well as identifying and mitigating all vulnerabilities that were exploited. During eradication, it is important to identify all affected hosts within the organization so that they can be remediated. For some incidents, eradication is either not necessary or is performed during recovery. **Do not rush** to get systems back online but move slowly and cautiously to ensure that all systems are checked, proactively monitored and vetted carefully or else the risk of reinfection is very high. Don't forget about the firmware, e.g. bios, storage controllers, switchers, etc.

Eradication Phase Roles, Responsibilities, and Actions

Customer Service

During the incident management eradication phase, the Customer Service team will maintain communications with impacted customers.

Actions for Customer Service:

- □ Communicate progress and system status to impacted customers

IT Operations

During the incident management eradication phase, IT Operations staff will ensure that all endpoints are clean and restore data and identify defense gaps in the organization.

Actions for IT Operations:

- □ Perform vulnerability assessment and antivirus and anti-malware scans on any endpoints or servers to ensure the threat has been remediated.
- □ Seize endpoints.
- □ Wipe servers and storage as required.
- □ Delete impacted virtual machines.
- □ Identify and remove malware if unable to wipe.
- □ Preserve evidence as best possible.
- □ Maintain communications with any impacted end users.
- □ Change all system passwords once the malware is deleted from the system.

IT Leadership

During the incident management eradication phase, the IT Leadership will develop any control weakness strategies, as appropriate.

Actions for IT Leadership:

- □ Develop and execute eradication plan.
- □ Approve new and updates to existing controls.

Senior Business Leadership

During the incident management eradication phase, Senior Business Leadership will approve the proposed control strategy and allocate any budget or resources to eradicate the malware and restore systems. The Senior Business Leadership will evaluate if any public relations or legal actions need to be taken.

Actions for Senior Business Leadership:

- □ Review eradication plan for business impact.
- □ Allocate budget and resources for eradication.
- □ Determine if any additional stakeholders need to be notified.
- □ Take any appropriate actions to inform legal agencies.
- □ Use a PR campaign to reduce reputational damage as appropriate.

Recovery Phase

During the ransomware incident management recovery phase, teams will enact processes and procedures for the recovery and full restoration of any infected endpoints or servers during the incident. In recovery, administrators restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents.

Recovery Phase Roles, Responsibilities, and Actions

Customer Service
During the incident management recovery phase, the Customer Service team will maintain communications with impacted customers.

Actions for Customer Service:

- ☐ Maintain communications with any impacted customers.

IT Operations
During the incident management eradication phase, IT Operations staff will ensure that all servers and systems are back online and restored. They will also ensure that the incident is fully documented and findings noted.

Actions for IT Operations:

- ☐ Ensure no other systems are impacted. **[IMPORTANT]**
- ☐ Reinitialize firmware using known good versions
- ☐ Change online, network and system passwords.
- ☐ Restore data from backup.
- ☐ Build replacement server.
- ☐ Issue new clean endpoints.
- ☐ Ensure systems are operational and accessible.
- ☐ Document the incident and preserve evidence.
- ☐ Review organizational anti-malware defenses and controls for gaps.

IT Leadership
During the incident management eradication phase, the IT Leadership will evaluate any weaknesses in security controls or policies as appropriate.

Actions for IT Leadership:

- ☐ Review any security policies or controls, as appropriate.

Senior Business Leadership
During the incident management eradication phase, Senior Business Leadership will determine if all relevant paperwork is complete.

Actions for Senior Business Leadership:

- ☐ Ensure appropriate paperwork is filled out about any malicious or accidental insider activity.
- ☐ Ensure all incident reporting requirements have been met.

Post-Incident Phase

During the ransomware incident management post-incident phase, teams will perform root-cause analysis and lessons-learned activities with various teams and stakeholders within the organization.

Post-Incident Phase Roles, Responsibilities, and Actions

Customer Service
During the incident management recovery phase, the Customer Service team will maintain communications with impacted customers.

Actions for Customer Service:

- □ Maintain communications with any impacted customers.

IT Operations
During the incident management post-incident phase, IT Operations staff will support any post-incident activities, as appropriate.

Actions for IT Operations:

- □ Document all findings in an incident report.
- □ Provide input to any post-incident analysis.
- □ Send out ransomware awareness and training.
- □ Participate in any post-incident meetings, as appropriate.

IT Leadership
During the incident management post-incident phase, the IT Leadership will facilitate any post-incident activities.

Actions for IT Leadership:

- □ Conduct and facilitate any post-incident activities.
- □ Facilitate post-incident lessons-learned meeting.
- □ Review and update policies and procedures based on lessons learned.

Senior Business Leadership
During the incident management post-incident phase, Senior Business Leadership will support any post-incident activities, as appropriate.

Actions for Senior Business Leadership:

- □ Participate in any post-incident meetings, as appropriate.
- □ Estimate and document the business impact of the incident.
- □ Generate full incident report for board of directors.