\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Insert Institution Name>

Ransomware Incident Response Playbook

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Version: 1.0**

**Approved:**

**Approval Authority:**

# Introduction

This playbook is a reference process for handling Ransomware incidents which should be exercised, deployed and governed as part of the incident management function.

## -Playbook Applicability - Ransomware

A ransomware incident involves a piece of malicious software which has been successfully executed on a system. The code could be targeted and bespoke or generic. Ransomware is a specific subset of malware that is designed to block access to a computer system or data on a computer system, usually until a sum of money is paid.

Due to the fact that ransomware is a type of malicious code, this playbook overlaps significantly with the “Malicious Code” playbook.

1. Verify Ransomware
   1. Verify and Contain
      1. Notify IT Admins (Code Red)
      2. Has a Ransomware message appeared on the screen?
         1. Yes🡪take a picture and then remove from network and proceed to Section 2. of this playbook.
         2. No🡪If in the process of encrypting and the message has not appeared, immediately remove from the network
         3. Unsure?🡪If you are unsure of what to do and but believe you have been compromised, remove from the network.
      3. Shared File Location
         1. Check for encrypted files
         2. Disconnect from the backups and the DR sites until Ransomware is contained.
2. Investigate
   1. <Insert your EDR solution> Endpoint Detection and Response (EDR)
      1. Did EDR detect Ransomware
         * 1. Yes🡪Investigate Ransomware in Windows Defender Security Center (If Operating System is 1803 or higher, auto investigation will begin)
           2. No🡪Notify Microsoft that EDR failed to detect Ransomware.
   2. Endpoint Protection Platform (EPP)
      1. Has malicious code been found on systems? (Y/N)
         1. YES🡪we use that code and all tools possible to see if it exists anywhere else on the network.
            1. NO🡪Proceed to (2)
         2. Is the code a potential unwanted application, remote access, or hacker tool?
            1. YES🡪we use the info provided to see if other devices on the network have been exposed.
            2. NO🡪Proceed to (3)
         3. EPP detect Ransomware?
            1. Yes

Was it stopped?

Investigate further to gather more details.

* + - * 1. No

Why it was not detected?

Contact vendor to notify them EPP did not detect Ransomware.

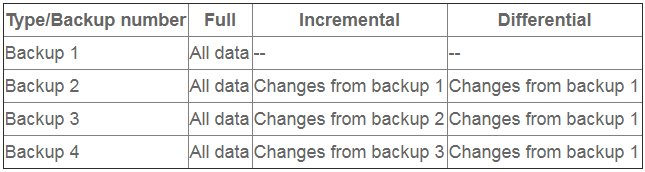
If further investigation provides you hashes or Indicators of Compromise (IOC’s), enter into EPP immediately to stop further propagation.

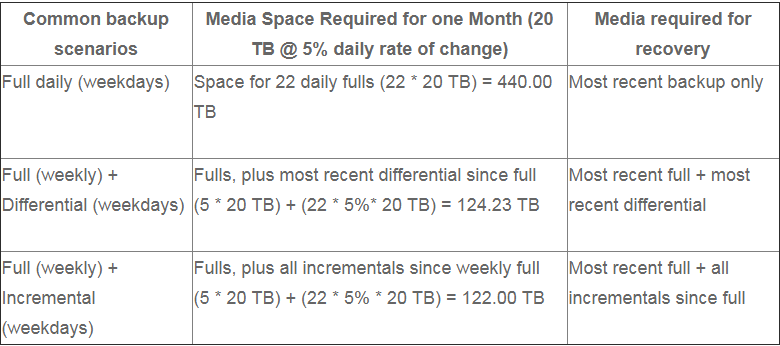
* 1. EDR (Oracle)
     1. Did EDR detect Ransomware?
        1. Yes🡪EDR filters data into Enterprise EDR, follow process found above under 2.a.
        2. No🡪Contact EDR provider and inform them there was no detection.
  2. SIEM/IDS-IPS
     1. Has there been communication with known malicious hosts?
     2. Have there been any offenses created in SIEM?
  3. Identify scope of impact
     1. Internal
        1. How many endpoints were affected?
        2. How many servers were affected?
        3. Were backups affected?
        4. Was Shared folder location affected?
     2. External
        1. Have there been any threats/comments made on Social Media? (Facebook, Twitter, Reddit, etc.)
        2. Communicate with 3rd party vendors.
           1. DHS NCCIC
           2. REN-ISAC
           3. US-CERT
     3. Are there reports of global issues where the company would be collateral damage?
        1. Is this a targeted attack of the company or across the education sector? Or many sectors?

1. Ransomware Verified (DISCONNECT SYSTESMS RIGHT AWAY!) (Physical Connections goes to Wi-Fi once disconnected, make sure to disconnect both!)
   1. Assess Damage
      1. Important Systems or Data
         1. How sensitive is the data stored, processed, or transmitted by the affected systems.
         2. How critical are the services provided by the affected systems?
         3. Do the systems or data being targeted affect a single person, team, business unit, or whole organization?
         4. What other systems are on the same subnet as the affected systems? (Network Segmentation)
      2. Many Systems or Data
         1. Which systems are affected and how sensitive is the data that is stored?
            1. How much data is affected?
         2. How critical are the services provided by the affected systems to the organization?
         3. Is there data availability, integrity, or confidentiality issues?
            1. Where does the data reside and how is it accessed? Local Systems, Network Drives
      3. VPN Users
         1. Disable through ATP
         2. If EDR has been disabled, work with Network Team to terminate VPN session. Then work with Service Desk team to prevent further sessions. Must occur within first 5-10 minutes or else endpoint has been lost.
2. Analyze
   1. Check Appendix and compare to see if Ransomware falls under any of the more commonly known.
   2. Is there any information the Ransomware provides that indicates a specialized targeted function?
   3. Does the ransomware target specific data/system(s)?
   4. Is there any evidence of data being exfiltrated?
   5. How were systems infected?
      1. Phishing?
         1. Was the attack Targeted or an act of War Driving?
      2. Malicious download?
         1. .pdf?
         2. .exe?
      3. Attack Vectors
      4. If Ransomware propagated and affected multiple systems, was it done so automatically or did it require user interaction?
   6. Network
      1. What addresses (IP, Email, Social Media, etc.) is the ransomware communicating with? Command and Control?
      2. What does threat intelligence say about the addresses?
      3. Will this stop services or just slow them down?
      4. Will availability issues cease once Ransomware has been successfully mitigated?
      5. Packet Capture Analysis?
      6. Payload analysis, via EPP?
3. Recovery/Mitigation
   1. Backups? (See Appendix)
      1. Full Backup
      2. Incremental Backup
      3. Differential Backup
      4. Shared Folder
      5. OneDrive
         1. EDR will notify us of the threat and will provide options to recover OneDrive files (Files Restore) to the state prior to the attack.
   2. Search Enterprise for Ransomware Indicators of Compromise (IOC’s)
   3. Implement additional countermeasures as a lesson learned.

APPENDIX A

* Ransomware
  + Crypto Ransomware🡪This ransomware will lock your files by encrypting and then progressively delete them.
  + Locker Ransomware🡪this ransomware works by displaying a warning, allegedly from the FBI, the police or some authority, stating that your system will remain unstable unless a ransom has been paid.
* Methods of Delivery
  + Spam
  + Exploit Kit
  + Malicious Software
  + Malicious Files
* Known Types
  + Bad Rabbit
    - Infected organizations in Russia and Eastern Europe. Was spread through a fake Adobe Flash update on compromised websites. When infected, users were directed to a payment page demanding .05 Bitcoin, which amounted to 285 dollars at the time.
  + Cerber
    - Targeted cloud based Office 365 users and impacted millions using an elaborate phishing campaign. This type of malware emphasizes the growing need for Software as a Service backup in addition to on-premises.
  + Crysis
    - Crysis can encrypt files on fixed, removable, and network drives and it uses strong encryption algorithms and a scheme which makes it hard to crack in a reasonable amount of time. Typically spread via emails containing attachments with double-file extension (test.pdf.exe), which make the filer appear as a non-exe. In addition to emails, it can also be disguised as a legit installer for applications.
  + CryptoLocker
    - One of the most well-known Ransomware attacks in Cryptolocker, which made headlines in 2013. The original Cryptolocker botnet was shut down in 2014, but not before hackers extorted nearly 3 million dollars.
  + CryptoWall
    - Gained notoriety after the downfall of the original CryptoLocker. First appeared in early 2014 and variants have appeared with a variety of names. Distributed via spam or exploit kits.
  + CTB-Locker
    - The hackers behind CTB-Locker outsourced the infection process to partners in exchange for a cut. This is a proven strategy for achieving large volumes of malware infections at a faster rate.
  + GoldenEye
    - Similar to Petya, hackers spread GoldenEye through a massive campaign targeting human resources departments. After the file download, a macro is launched which encrypts files. For each encrypted file, GoldenEye adds a random 8-character extension at the end. Then, the ransomware modifies the user’s hard drive MBR with a custom boot loader.
  + Jigsaw
    - Encrypts and progressively deletes files until a ransom is paid. The ransomware deletes a single file after the first hour, then deletes more and more per hour until the 72 hour mark, when all files are deleted.
  + KeRanger
    - Was discovered on BitTorrent client. Was not widely distributed but, it’s known as the first fully functioning ransomware designed to lock Mac OS X applications.
  + LeChiffre
    - Unlike other variants, hackers must run LeChiffre manually on the compromised system. Cyber criminals automatically scan networks in search of poorly secured remote desktops, logging into them remotely and manually running an instance of the virus.
  + Locky
    - Locky is spread in an email messaged disguised as an invoice. When opened, the invoice is scrambled and the victim is instructed to enable macros to read the document. When macros are enabled, Locky begins encrypting a large array of file types using AES encryption.
  + NotPetya
    - NotPetya, originally claimed to be a variant of Petya, is instead of malware known as wiper, whose sole purpose is destroying data rather than obtaining a ransom.
  + Petya
    - Petya encrypts entire computer systems. Petya overwrites the master boot record, rendering the OS unbootable.
  + Spider
    - Spider is spread via spam emails across Europe. Spider ransomware is hidden in MSoft Word documents that install the malware on a victim’s computer when downloaded. The Word document, which is disguised as a debt collection notice, contains malicious macros. When these macros are executed, the ransomware begins to download and encrypt the victim’s data.
  + TeslaCrypt
    - Uses AES algorithm to encrypt files. It’s typically distributed via the Anger exploit kit specifically attacking Adobe vulnerabilities. Once a vulnerability is exploited, TeslaCrypt installs itself in the MSoft temp folder.
  + TorrentLocker
    - Typically distributed through spam email campaigns and is geographically targeted with email messages delivered to specific regions. TorrentLocker is often referred to as CryptoLocker, and it uses AES algorithm to encrypt file types. It also collects email addresses from the victim’s address book to spread malware beyond the initial infected computer-this process uses TorrentLocker.
  + WannaCry
    - This ransomware hit over 125K organizations in over 150 countries. The ransomware strain, AKA WCry or WanaCrypt0, currently affects Windows machines through MSoft exploit known as EternalBlue.
  + ZCryptor
    - Is a self-propagating malware strain that exhibits worm-like behavior, encrypting files and also infecting external drives and flash drives so it can be distributed to other computers.
* Prevention/Mitigation
  + Education
    - Bi-annual phishing campaign
  + Security
    - Network Segmentation
      * This method pursues the goal of protecting IT infrastructure by restricting the scope of resources an intruder/malware has access to. It presupposes the compartmentalization of data, network assets, and applications into standalone segments while limiting communication between these segments. Therefore, if a Ransomware event were to take place, the infection would be unable to traverse the entire network to encrypt.
    - AV
    - EPP
    - Enhanced Mitigation Experience Toolkit (EMET)
    - Anti-Spam Settings
    - Disablement of Macros
    - Application Whitelisting
  + Maintain Secure Backups
    - Full Backups
      * Full backups copy all data to another set of media, in our case, a tape. (Iron Mountain). Primary advantage to performing a full backup, though it can take much time and space, is that a complete copy of all data is available with a single set of media. This results in a minimal time to restore data, a metric known as Recovery Time Objective (RTO).
    - Incremental Backup
      * Incremental backups will result in copying only the data that has changed since the last backup operation of any type. The modified time stamp on files is typically used and compared to the time stamp of the last backup. The benefit of an incremental backup is that they copy a smaller amount of data than a full, resulting in a faster backup that requires less media to store the backup.
    - Differential Backup
      * Similar to an Incremental backup, it will copy all data changed from the previous backup the first time performed. However, each time afterwards, it will continue to copy all data changed since the previous full backup. Therefore, more data will be stored, though far less than a Full. Time and space falls in the middle of the 3.





APPENDIX B: Do We Pay the Ransom?

For the full article, see details at the Forrester link: <https://www.forrester.com/report/Forresters+Guide+To+Paying+Ransomware/-/E-RES154595>

APPENDIX C: Ransomware Protection Strategies

Attached are recommendations on how to harden your environment to prevent Ransomware.

