Ransomware

Incident Response Playbook
Suitable for all (private and public) organizations
Developed by: Olumuyiwa Olufunmilola Agunbiade

Version history

Version	Update Date	Updated By	Reason for Update
1.0	01/03/2024	Olumuyiwa Agunbiade	Initial Draft

Purpose

To guide <ORGANIZATION NAME> in responding to a ransomware incident.

How to Use This Playbook

The steps in this playbook should be followed sequentially where appropriate. With many steps in the Containment, Eradication, and Recovery steps, some overlap may occur and is expected.

Preparation

Note: Preparation steps should primarily be completed prior to an event or incident. If the playbook is being accessed during an event or incident you may proceed to Preparation Step 4b.

1. Determine the members of the Cybersecurity Incident Response Team (CSIRT).
    a. The core CSIRT members should be comprised of individuals responsible for cybersecurity only.
        i. This may include some members of Information Technology roles, depending on the organization size.
        ii. The limited size of the core CSIRT is to assist with confidentiality and efficiency.
        iii. The core CSIRT may be activated often to investigate security events that may or may not result in an incident.
    b. Assign roles and responsibilities to each member.
2. Determine extended CSIRT members.
    a. This will often be Legal, Compliance, Public Relations, and Executive Leadership.
3. Define escalation paths.
    a. Incidents may start as events, or as a lower impact/severity and then increase as more information is gathered. Establishing an escalation path is critical to success.
4. Evaluate and secure critical system backups.
    a. Backups should be secured prior to any incident.
    b. During the initial stages of any incident, evaluate and confirm that backups are secure and not impacted by the incident.

Identification

1. Isolate infected systems ASAP.
    a. DO NOT power off machines, as forensic artifacts may be lost.
    b. Preserve the system(s) for further forensic investigation including log review, MFT analysis, deep malware scans, etc.
        i. These steps should be performed during the Identification phase to guide the investigation.
2. Investigate malware to determine if it's running under a user context.
    a. If so, disable this account (or accounts if multiple are in use) until the investigation is complete.
3. Analyze the malware to determine characteristics that may be used to contain the outbreak.
    a. If available, use a sandboxed malware analysis system to perform analysis.
        i. **Note:** Network connectivity should not be present for this sandbox system except in very rare circumstances. Network activity from malware may be used to alert an attacker of your investigation.
        ii. Observe any attempts at network connectivity, note these as Indicators of Compromise (IoCs)
        iii. Observe any files created or modified by the malware, note these as IoCs.
        iv. Note where the malware was located on the infected system, note this as an IoC.
        v. Preserve a copy of the malware file(s) in a password protected zip file.

   b. Use the PowerShell "Get-FileHash" cmdlet to get the SHA-256 hash value of the malware file(s).
      i. This hash may also be used to search for community information regarding this malware (i.e.VirusTotal, Hybrid-Analysis, CISCO Talos, etc.)
      ii. Additional hash values (SHA1, MD5, etc.) may be gathered to better suit your security tools.
      iii. Note these hash values as IoCs.
   c. Use all IoCs discovered to search any available tools in the environment to locate additional infected hosts.
4. Use all information and IoCs available to search for the initial point of entry.
   a. Determine the first appearance of the malware.
   b. Determine the user first impacted by the malware.
   c. Investigate all available log files to determine the initial date and point of infection.
   d. Analyze all possible vectors for infection.
      i. Focus on known delivery methods discovered during malware analysis (email, PDF, website, packaged software, etc.).
5. Once the ransomware variant is identified, perform research to determine Tactics, Techniques, and Procedures (TTPs) associated with this variant and/or threat-actor.
   a. Determine if data exfiltration and extortion is common.
   b. Determine attacker toolkit if possible.

Containment

1. Use the information about the initial point of entry gathered in the previous phase to close any possible gaps.
   a. Examples: Firewall configuration changes, email blocking rules, user education, etc.
2. Once the IoCs discovered in the Identification phase have been used to find any additional hosts that may be infected, isolate these devices as well.
3. Add IoCs (such as hash value) to endpoint protection.
   a. Set to block and alert upon detection.
4. Submit hash value to community sources to aid in future detection.
   a. **NOTE:** Clear this process with legal/compliance representatives during each incident, as each malware situation will be different.
5. Implement any temporary network rules, procedures and segmentation required to contain the malware.
6. If additional accounts have been discovered to be involved or compromised, disable those accounts.

Eradication

1. Preserve artifacts, systems, and relevant backups according to the sensitivity and scale of the incident. These may be important for future forensics.
   a. If rebuilding or replacing physical systems, preserve physical hard disks, solid state drives, or forensically sound images of those storage drives.
   b. If rebuilding or replacing virtual machines, preserve a copy, full (independent) snapshot, or a backup of the system.
2. Preserve any volatile data that may have been collected during the identification and containment phases.
   a. This may include log files, backups, malware samples, memory images, etc.

3. Once all relevant data, equipment, and/or systems have been preserved replace or rebuild systems accordingly.

Recovery

1. Restore impacted systems from a clean backup, taken prior to infection if these backups are available.
2. For systems not restorable from backup, rebuild the machines from a known good image or from bare metal.
3. Remediate any vulnerabilities and gaps identified during the investigation.
4. Reset passwords for all impacted accounts and/or create replacement accounts and leave the impacted accounts disabled permanently.
5. Continue to monitor for malicious activity related to this incident for an extended period.
    a. Alerts should be configured to aid in quick detection and response.
6. If data-exfiltration and extortion were determined to be part of this attack, work with legal counsel to determine next steps.

Lessons Learned

1. Conduct a meeting after the incident to discuss the following:
    a. What things went well during the investigation?
    b. What things did not go well during the investigation?
    c. What vulnerabilities or gaps in the organization's security status were identified?
        i. How will these be remediated?
    d. What further steps or actions would have been helpful in preventing the incident?
    e. Do modifications need to be made to any of the following:
        i. Network segmentation
        ii. Firewall configuration
        iii. Application security
        iv. Operating System and/or Application patching procedures
        v. Employee, IT, or CSIRT training
2. Create and distribute an incident report to relevant parties.
    a. A primary, and more technical, report should be completed for the CSIRT.
    b. An executive summary should be completed and presented to the management team.

QUESTION & ANSWER?