Incident Response Don’ts and Do’s

The following are considerations for an organization experiencing a cybersecurity incident.

CONSIDER NOT DOING THE FOLLOWING:

- Unplug or Power Off Any Network Devices. A common misconception is that devices affected by ransomware should be immediately powered off. Doing so can cause the unintentional loss of valuable forensic artifacts.
- Wipe and/or Restore Devices. Another common mistake is to immediately begin restoring critical network infrastructure from existing backups. Most often, critical systems, such as domain controllers, contain the most valuable forensic evidence. Restoring from backups can involve the wiping or cleaning of the encrypted device, which results in the loss of forensic artifacts. Additionally, the restored backups may still contain vulnerabilities that can lead to re-encryption if appropriate security measures – such as endpoint monitoring – are not put into place before restoration.
- Contact the Attackers. Leave communication with the attackers, if any, to the experts. Unilateral communication without experts consulting can give threat actors leverage that could be used against your organization.
- Pay the Ransom Right Away. Ransom payments are sometimes required – however, it is illegal to make payments to some Bitcoin (BTC) wallet addresses. Prior to payment, the BTC wallet addresses should be checked against a federally maintained blacklist of sanctioned wallets. Additionally, some older ransomware variants have publicly available decryption keys, and decryption of your files may be free.
- Notification of the Incident. Wait for the completion of the forensic investigation, which will inform the legal assessment of whether a notification of the incident is required.
- Run an Anti-Virus (A/V) Scan. Counterintuitively, running an A/V scan can result in the deletion of forensic artifacts valuable to a forensic investigation. For example, some of the malware involved in the attack can be reverse engineered to determine whether it was capable of accessing or acquiring data.

CONSIDER DOING THE FOLLOWING PROCEDURES:

- Unplug the Network Cable. This will disconnect the internal network from the internet, cutting off any unauthorized access to the network.
- Isolate/Segregate the Network. If possible, move the entire network into an isolated VLAN (virtual local area network). This provides added security against unauthorized access and prevents the further spread of malware to outside devices.
- Preserve Firewall, Network, System Logs, RDP Logs and Corporate Email Logs. All available logs should be pulled and preserved to prevent their loss due to rollover.
- Consideration of Creating Full Disk Forensic Images. Consideration of forensically obtaining full disk images of affected devices should be made prior to restoration.
- Initiate a Global Password Reset. Initiate a password reset for all users on the network. This will cut off any potential threat actor persistence as the network is brought back online.

Incident Response Don’ts and Do’s

- Take a Screenshot of or Otherwise Preserve the Ransom Note. The ransom note, much like a fingerprint, provides insight into the variant of the ransomware. The type of variant at play informs many aspects of an incident response. Ransom notes often appear on the infected servers as an HTML or .txt file.
- Map the Network and Create an Inventory of Devices. Having a network inventory prepared will increase the ability of forensic experts to respond and remediate the ransomware.
- Deploy an Endpoint Detection and Response (EDR) Tool. EDR tools are capable of identifying, isolating, and terminating malicious code on the network and will prevent encryption during the forensic collection and remediation process.
- Identify Viable Backups. Identify if there are backups that have not been encrypted by the ransomware. Determine the process for restoring the backups, but do not begin restoration without first consulting legal experts and a forensic investigation team.
- Assess Risk Impact. Gain an understanding of what sensitive data (e.g., customer, vendor or employee PII/PHI or trade secret) may have been impacted by incident. Legal counsel may need to be involved to determine legal and/or compliance risk based on incident and potential access to sensitive data.
- Document Incident. Detailed notes of observations by name, date and time regarding initial detection of incident and any related response to the identification of the incident inclusive of:
- Locations of every device that appears to be infected
- Contact information for all witnesses to the incident

By following these DON’Ts and DO’s, evidence can be properly collected and preserved in a forensically sound manner. By properly collecting and preserving evidence, there should be an opportunity to address the following questions:

- When did the attacker get inside?
- What did the attacker do when they got inside?
- What critical information did the attacker access?
- What did the attacker take (if anything)?