IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

RANSOMWARE RESPONSE

March 8, 2022

The Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends responding to ransomware by using the following checklist provided in a Joint CISA and Multi-State Information Sharing and Analysis Center (MS-ISAC) Ransomware Guide. This information will take you through the response process from detection to containment and eradication. Be sure to move through the first three steps in sequence.

DETECTION AND ANALYSIS

1. Determine which systems were impacted, and immediately isolate them.

If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.

If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.

After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.

Please Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

3. Triage impacted systems for restoration and recovery.

Identify and prioritize critical systems for restoration and confirm the nature of data housed on impacted systems.

Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.

Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

> *Remember: The Joint CISA MS-ISAC Ransomware guide states, "Paying ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, MS-ISAC, and other federal law enforcement do not recommend paying ransom. In addition, attackers have begun following their ransom demands to decrypt the data with a follow-on extortion demand to keep data private."*

4. Consult with your incident response team to develop and document an initial understanding of what has occurred based on initial analysis.

5. Engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.

CONTAINMENT AND ERADICATION

If no initial mitigation actions appear possible:

6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected).

Take care to preserve evidence that is highly volatile in nature - or limited in retention - to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

For more information or to seek additional help, contact us at email here.

> *We understand attacks can severely impact business processes and leave organizations without the data needed to operate and deliver mission-critical services. To continue taking steps and mitigating the ransomware incident, please see the Ransomware Guide for more information.*