Alert (AA20-049A)

More Alerts

Ransomware Impacting Pipeline Operations

Original release date: February 18, 2020 | Last revised: October 24, 2020

Summary

> ***Note:*** *This Activity Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework. See the MITRE ATT&CK for Enterprise and ATT&CK for Industrial Control Systems (ICS) frameworks for all referenced threat actor techniques and mitigations.*

The Cybersecurity and Infrastructure Security Agency (CISA) encourages asset owner operators across all critical infrastructure sectors to review the below threat actor techniques and ensure the corresponding mitigations are applied.

CISA responded to a cyberattack affecting control and communication assets on the operational technology (OT) network of a natural gas compression facility. A cyber threat actor used a *Spearphishing Link* [T1192] to obtain initial access to the organization's information technology (IT) network before pivoting to its OT network. The threat actor then deployed commodity ransomware to *Encrypt Data for Impact* [T1486] on both networks. Specific assets experiencing a *Loss of Availability* [T826] on the OT network included human machine interfaces (HMIs), data historians, and polling servers. Impacted assets were no longer able to read and aggregate real-time operational data reported from low-level OT devices, resulting in a partial *Loss of View* [T829] for human operators. The attack did not impact any programmable logic controllers (PLCs) and at no point did the victim lose control of operations. Although the victim's emergency response plan did not specifically consider cyberattacks, the decision was made to implement a deliberate and controlled shutdown to operations. This lasted approximately two days, resulting in a *Loss of Productivity and Revenue* [T828], after which normal operations resumed. CISA is providing this Alert to help administrators and network defenders protect their organizations against this and similar ransomware attacks.

Technical Details

Network and Assets

- The victim failed to implement robust segmentation between the IT and OT networks, which allowed the adversary to traverse the IT-OT boundary and disable assets on both networks.
- The threat actor used commodity ransomware to compromise Windows-based assets on both the IT and OT networks. Assets impacted on the organization's OT network included HMIs, data historians, and polling servers.
- Because the attack was limited to Windows-based systems, PLCs responsible for directly reading and manipulating physical processes at the facility were not impacted.
- The victim was able to obtain replacement equipment and load last-known-good configurations to facilitate the recovery process.
- All OT assets directly impacted by the attack were limited to a single geographic facility.

Planning and Operations

- At no time did the threat actor obtain the ability to control or manipulate operations. The victim took offline the HMIs that read and control operations at the facility. A separate and geographically distinct central control office was able to maintain visibility but was not instrumented for control of operations.
- The victim's existing emergency response plan focused on threats to physical safety and not cyber incidents. Although the plan called for a full emergency declaration and immediate shutdown, the victim judged the operational impact of the incident as less severe than those anticipated by the plan and decided to implement limited emergency response measures. These included a four-hour transition from operational to shutdown mode combined with increased physical security.
- Although the direct operational impact of the cyberattack was limited to one control facility, geographically distinct compression facilities also had to halt operations because of pipeline transmission dependencies. This resulted in an operational shutdown of the entire pipeline asset lasting approximately two days.
- Although they considered a range of physical emergency scenarios, the victim's emergency response plan did not specifically consider the risk posed by cyberattacks. Consequently, emergency response exercises also failed to provide employees with decision-making experience in dealing with cyberattacks.
- The victim cited gaps in cybersecurity knowledge and the wide range of possible scenarios as reasons for failing to adequately incorporate cybersecurity into emergency response planning.

Mitigations

Asset owner operators across all sectors are encouraged to consider the following mitigations using a risk-based assessment strategy.

Planning and Operational Mitigations

- Ensure the organization's emergency response plan considers the full range of potential impacts that cyberattacks pose to operations, including loss or manipulation of view,

loss or manipulation of control, and loss of safety. In particular, response playbooks should identify criteria to distinguish between events requiring deliberate operational shutdown versus low-risk events that allow for operations to continue.
- Exercise the ability to fail over to alternate control systems, including manual operation while assuming degraded electronic communications. Capture lessons learned in emergency response playbooks.
- Allow employees to gain decision-making experience via tabletop exercises that incorporate loss of visibility and control scenarios. Capture lessons learned in emergency response playbooks.
- Identify single points of failure (technical and human) for operational visibility. Develop and test emergency response playbooks to ensure there are redundant channels that allow visibility into operations when one channel is compromised.
- Implement redundant communication capabilities between geographically separated facilities responsible for the operation of a single pipeline asset. Coordinate planning activities across all such facilities.
- Recognize the physical risks that cyberattacks pose to safety and integrate cybersecurity into the organization's safety training program.
- Ensure the organization's security program and emergency response plan consider third parties with legitimate need for OT network access, including engineers and vendors.

Technical and Architectural Mitigations

- Implement and ensure robust *Network Segmentation* [M1030] between IT and OT networks to limit the ability of adversaries to pivot to the OT network even if the IT network is compromised. Define a demilitarized zone (DMZ) that eliminates unregulated communication between the IT and OT networks.
- Organize OT assets into logical zones by taking into account criticality, consequence, and operational necessity. Define acceptable communication conduits between the zones and deploy security controls to *Filter Network Traffic* [M1037] and monitor communications between zones. Prohibit Industrial Control System (ICS) protocols from traversing the IT network.
- Require *Multi-Factor Authentication* [M1032] to remotely access the OT and IT networks from external sources.
- Implement regular *Data Backup* [M1053] procedures on both the IT and OT networks. Ensure that backups are regularly tested and isolated from network connections that could enable the spread of ransomware.
- Ensure user and process accounts are limited through *Account Use Policies* [M1036], *User Account Control* [M1052], and *Privileged Account Management* [M1026]. Organize access rights based on the principles of least privilege and separation of duties.
- Enable strong spam filters to prevent phishing emails from reaching end users. Implement a *User Training* [M1017] program to discourage users from visiting malicious websites or opening malicious attachments. Filter emails containing executable files from reaching end users.

- *Filter Network Traffic* [M1037] to prohibit ingress and egress communications with known malicious Internet Protocol (IP) addresses. Prevent users from accessing malicious websites using Uniform Resource Locator (URL) blocklist and/or allowlist.
- *Update Software* [M1051], including operating systems, applications, and firmware on IT network assets. Use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program. Consider using a centralized patch management system.
- Set *Antivirus/Antimalware* [M1049] programs to conduct regular scans of IT network assets using up-to-date signatures. Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- Implement *Execution Prevention* [M1038] by disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.
- Implement *Execution Prevention* [M1038] via application allow listing, which only allows systems to execute programs known and permitted by security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Limit *Access to Resources over Network* [M1035], especially by restricting Remote Desktop Protocol (RDP). If after assessing risks RDP is deemed operationally necessary, restrict the originating sources and require *Multi-Factor Authentication* [M1032].

Resources

- CISA Ransomware One-Pager and Technical Document (CISA, 2019)
- CISA Insights: Ransomware Outbreak (CISA, 2019)
- Pipeline Cybersecurity Initiative (CISA, 2018)
- CISA Webinar: Combating Ransomware (CISA, 2018)
- Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018)
- Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (NIST, 2018)
- Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events (NIST, 2018)
- Pipeline Security Guidelines (TSA, 2018)
- NIST SP 800-11: Data Integrity: Recovering from Ransomware and Other Destructive Events (NIST, 2017)
- Guide to Industrial Control Systems (ICS) Security (NIST, 2015)
- Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (DOE, 2014)

Revisions

February 18, 2020: Initial Version

October 23, 2020

TLP:WHITE

This product is provided subject to this Notification and this Privacy & Use policy.

TLP:WHITE