Rising Ransomware Threat To Operational Technology Assets

OVERVIEW

In recent months, ransomware attacks targeting critical infrastructure have demonstrated the rising threat of ransomware to operational technology (OT) assets and control systems.[1]

OT components are often connected to information technology (IT) networks, providing a path for cyber actors to pivot from IT to OT networks.[2] Given the importance of critical infrastructure to national security and America's way of life, accessible OT assets are an attractive target for malicious cyber actors seeking to disrupt critical infrastructure for profit or to further other objectives. As demonstrated by recent cyber incidents, intrusions affecting IT networks can also affect critical operational processes even if the intrusion does not directly impact an OT network.

All organizations are at risk of being targeted by ransomware and have an urgent responsibility to protect against ransomware threats. Critical infrastructure asset owners and operators should adopt a heightened state of awareness and voluntarily implement the recommendations listed in this document, including:

- Identify critical processes that must continue uninterrupted in order to provide essential services;
- Develop and regularly test workarounds or manual controls to ensure that critical processes—and the industrial control system (ICS) networks supporting them—can be isolated and continue operating without access to IT networks, if needed;
- Implement robust network segmentation between IT and OT networks; and
- Ensure backup procedures are implemented and regularly tested and that backups are isolated from network connections.

These steps will help critical infrastructure owners and operators improve their entity's functional resilience by reducing their vulnerability to ransomware and the risk of severe business degradation if affected by ransomware.

PREPARE

- **Determine your critical operational processes' reliance on key IT infrastructure.**
  - Maintain a current asset inventory to assist in determining components and devices that support your operational processes.
  - Understand and evaluate cyber risk on "as-operated" OT assets.
  - Create an accurate "as-operated" OT network map and identify OT and IT network inter-dependencies.

> **Note**: if network segmentation is implemented, critical operational processes may still be dependent on business functions performed by the IT network. It is important to identify and take immediate steps to reduce these co-dependencies.

- **Identify a resilience plan that addresses how to operate if you lose access to or control of the IT and/or OT environment.**
  - Plan for how to continue operations if a control system is malfunctioning, inoperative, or actively acting contrary to the safe and reliable operation of the process.
  - Develop workarounds or manual controls to ensure ICS networks can be isolated if the connection to a compromised IT environment creates risk to the safe and reliable operation of OT processes.
- **Exercise your incident response plan.**
  - Regularly test manual controls so that critical functions can be kept running if OT networks need to be taken offline.

[1] CISA-FBI Joint Cybersecurity Advisory: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks
[2] NSA Cybersecurity Advisory: Stop Malicious Cyber Activity Against Connected Operational Technology

- **Implement regular data backup procedures on both IT and OT networks.**
    - Regularly test backup procedures.
    - Ensure that backups are isolated from network connections that could enable the spread of ransomware.

Note: CISA recommends testing backups by doing a full restore from scratch. This valuable process can help map previously unknown dependencies.

MITIGATE

CISA recommends critical infrastructure organizations apply the following mitigations to defend against potential future threats and prevent severe functional degradation if the organization falls victim to a ransomware attack.

- **Practice good cyber hygiene.** The significant majority of ransomware attacks exploit known vulnerabilities and common security weaknesses.
    - Update software, including operating systems, applications, and firmware, on IT network assets, in a timely manner.
    - Implement application allowlisting.
    - Ensure user and process accounts are limited through account use policies, user account control, and privileged account management.
    - Require multi-factor authentication for access to OT and IT networks.
    - Enable strong spam filters to prevent phishing emails from reaching end users.
- **Implement and ensure robust network segmentation between IT and OT networks.**
- **Implement a continuous and vigilant system monitoring program.**

CISA offers a variety of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By enrolling in these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

See the following resources for more detailed mitigation guidance:

- CISA-NSA Joint Cybersecurity Advisory: Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
- CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC): Joint Ransomware Guide
- CISA-FBI Joint Cybersecurity Advisory: DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks

RESPOND

Remember: paying a ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised and further encourages criminal groups to conduct more attacks. CISA strongly discourages paying ransoms.

Should your organization become a victim of ransomware, CISA strongly recommends implementing your cyber incident response plan by using the following checklist. Be sure to move through the first three steps in sequence. **Note:** CISA recommends including this checklist as a ransomware-specific annex in cyber incident response plans. See the CISA-MS-ISAC Joint Ransomware Guide for more details and a full ransomware response checklist.

1. Determine which systems were impacted and immediately isolate them.
2. If and only if you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.
3. Triage impacted systems for restoration and recovery.
4. Confer with your 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. **Strongly consider requesting assistance from a third-party incident response provider or CISA.**

If no initial mitigation actions appear possible:

6. Take a system image and memory capture of a sample of affected devices. Additionally, collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise. **Note**: take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering.
7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

ADDITIONAL RESOURCES

- The National Security Agency's practical guide, Stop Malicious Cyber Activity Against Connected Operational Technology, assists OT owners and administrators in evaluating risks against their systems and using that knowledge to guide network changes to realistically monitor and detect malicious activity.
- The National Institute of Standards and Technology's Special Publication, SP 800-184: Guide for Cybersecurity Event Recovery, provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning.
- CISA's Joint Cybersecurity Advisory—created with the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom—Technical Approaches to Uncovering and Remediating Malicious Activity, serves as a playbook for incident investigation. It highlights technical approaches to uncovering malicious activity and includes mitigation steps according to best practices.
- Cyber Resilience Review Resource: Service Continuity Management
- See the following CISA resources pages for more information:
  - Industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
  - Ransomware guidance: https://www.cisa.gov/ransomware

REPORTING

- All ransomware incidents are federal crimes and should be reported to law enforcement to help bring these criminals to justice. Ransomware events can be reported to the FBI or the Secret Service. You can find your local FBI field office at https://www.fbi.gov/contact-us/field-offices/ and your local Secret Service office at https://www.secretservice.gov/contact/field-offices.

- CISA is the nation's cyber defense center and is dedicated to helping all organizations prevent cyber intrusions, including ransomware. You can request technical assistance or provide information that can be used to protect other possible victims at https://us-cert.cisa.gov/forms/report.