NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems

Summary

Over recent months, cyber actors have demonstrated their continued willingness to conduct malicious cyber activity against Critical Infrastructure (CI) by exploiting Internet-accessible Operational Technology (OT) assets [1]. Due to the increase in adversary capabilities and activity, the criticality to U.S. national security and way of life, and the vulnerability of OT systems, civilian infrastructure makes attractive targets for foreign powers attempting to do harm to US interests or retaliate for perceived US aggression. OT assets are critical to the Department of Defense (DoD) mission and underpin essential National Security Systems (NSS) and services, as well as the Defense Industrial Base (DIB) and other critical infrastructure. At this time of heightened tensions, it is critical that asset owners and operators of critical infrastructure take the following immediate steps to ensure resilience and safety of US systems should a time of crisis emerge in the near term. The National Security Agency along with the Cybersecurity and Infrastructure Security Agency recommend that all DoD, NSS, DIB, and U.S. Critical Infrastructure facilities take immediate actions to secure their OT assets.

Internet-accessible OT assets are becoming more prevalent across the 16 US CI Sectors as companies increase remote operations and monitoring, accommodate a decentralized workforce, and expand outsourcing of key skill areas such as Instrumentation & Control, OT asset management/maintenance, and in some cases, process operations and maintenance. Legacy OT assets that were not designed to defend against malicious cyber activities, combined with readily available information that identifies OT assets connected via the Internet (e.g., Shodan[1] [2], Kamerka [3]), are creating a "perfect storm" of 1) easy access to unsecured assets, 2) use of common, open-source information about devices, and 3) an extensive list of exploits deployable via common exploit frameworks [4] (e.g., Metasploit[2] [5], Core Impact[3] [6], and Immunity Canvas[4] [7]). Observed cyber threat activities can be mapped to the MITRE[5] Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK[6]) for Industrial Controls Systems (ICS) framework [8]. It is important to note that while the behavior may not be technically advanced, it is still a serious threat because the potential impact to critical assets is so high.

Recently Observed Tactics, Techniques, and Procedures

- Spear phishing [T1192] to obtain initial access to the organization's information technology (IT) network before pivoting to the OT network.
- Deployment of commodity ransomware to Encrypt Data for Impact [T1486] on both networks.
- Connecting to *Internet Accessible* PLCs [T883] requiring no authentication for initial access.
- Utilizing *Commonly Used Ports* [T885] and *Standard Application Layer Protocols* [T869], to communicate with controllers and download modified control logic.
- Use of vendor engineering software and *Program Downloads* [T843].
- Modifying *Control Logic* [T833] and *Parameters* [T836] on PLCs.

[1] Shodan is a registered trademark of Shodan Limited Liability Company.
[2] Metasploit is a registered trademark of Rapid7 Limited Liability Company.
[3] Core Impact is a registered trademark of Help/Systems, Limited Liability Company.
[4] Canvas is a registered trademark of Immunity Products, Limited Liability Company.
[5] MITRE is a registered trademark of The MITRE Corporation.
[6] ATT&CK is a registered trademark of The MITRE Corporation.

Impacts

- Impacting a Loss of Availability [T826] on the OT network.
- Partial Loss of View [T829] for human operators.
- Resulting in Loss of Productivity and Revenue [T828].
- Adversary Manipulation of Control [T831] and disruption to physical processes.

Recommendations

Have a Resilience Plan for OT

Since the Ukraine cyberattack of 2015 organizations must assume in their planning of not only a malfunctioning or inoperative control system, but a control system that is actively acting contrary to the safe and reliable operation of the process. Organizations need an OT resilience plan that allows them to:

- Immediately disconnect systems from the Internet that do not need Internet connectivity for safe and reliable operations. Ensure that compensating controls are in place where connectivity cannot be removed.
- Plan for continued manual process operations should the ICS become unavailable or need to be deactivated due to hostile takeover.
- Remove additional functionality that could induce risk and attack surface area.
- Identify system and operational dependencies.
- Restore OT devices and services in a timely manner. Assign roles and responsibilities for OT network and device restoration.
- Backup “gold copy” resources, such as firmware, software, ladder logic, service contracts, product licenses, product keys, and configuration information. Verify that all “gold copy” resources are stored off-network and store at least one copy in a locked tamperproof environment (e.g., locked safe).
- Test and validate data backups and processes in the event of data loss due to malicious cyber activity.

Exercise your Incident Response Plan

In a state of heightened tensions and additional risk and exposure, it is critical to have a well-exercised incident response plan that is developed before an incident.

- Conduct a tabletop exercise including, executive personnel, to test your existing incident response plan.
- Be sure to include your public affairs and legal teams in your exercise in addition to your IT, OT and executive management.
- Discuss key decisions points in the response plan and identify who has the authority to make key decisions under what circumstances.
- Ensure your plan takes into account a scenario inclusive of the TTPs above and where the control system is actively operating counter to safe and reliable operations.
- Partner with third-parties for support. Review service contracts and government services for emergency incident response and recovery support.

Harden Your Network

Remote connectivity to OT networks and devices provides a known path that can be exploited by cyber actors, External exposure should be reduced as much as possible.

- Remove access from networks, such as non-US IP addresses if applicable, that do not have legitimate business reasons to communicate with the system.
- Use publicly available tools, such as Shodan[1] to discover Internet-accessible OT devices. Take corrective actions to eliminate or mitigate Internet-accessible connections immediately. Best practices include:
    - Fully patch all Internet-accessible systems.

  - Segment networks to protect PLCs and workstations from direct exposure to the Internet. Implement secure network architectures utilizing demilitarized zones (DMZs), firewalls, jump servers, and/or one-way communication diodes.
  - Ensure all communications to remote devices use a virtual private network (VPN) with strong encryption further secured with multifactor authentication.
    - Check and validate the legitimate business need for such access.
  - Filter network traffic to only allow Internet Protocol (IP) addresses that are known to need access, and use geo-blocking where appropriate.
  - Connect remote PLCs and workstations to network intrusion detection systems where feasible.
    - Capture and review access logs from these systems.
  - Encrypt network traffic preferably using NIAP-validated VPN products and/or CNSSP- or NIST-approved algorithms when supported by OT system components to prevent sniffing and man-in-the-middle tactics. Available at: https://niap-ccevs.org.

- Use the validated inventory to investigate which OT devices are Internet-accessible.
- Use the validated inventory to identify OT devices that connect to business, telecommunications, or wireless networks.
- Secure all required and approved remote access and user accounts.
  - Prohibit the use of default passwords on all devices, including controllers and OT equipment.
  - Remove, disable, or rename any default system accounts wherever possible, especially those with elevated privileges or remote access.
  - Enforce a strong password security policy (e.g., length, complexity).
  - Require users to change passwords periodically, when possible.
  - Enforce or plan to implement two-factor authentication for all remote connections.
- Harden or disable unnecessary features and services (e.g., discovery services, remote management services, remote desktop services, simulation, training, etc.).

Create an Accurate "As-operated" OT Network Map Immediately

An accurate and detailed OT infrastructure map provides the foundation for sustainable cyber-risk reduction.

- Document and validate an accurate "as-operated" OT network map.
  - Use vendor-provided tools and procedures to identify OT assets.
  - Use publically available tools, such as Wireshark[7] [9], NetworkMiner [10], GRASSMARLIN [11], and/or other passive network mapping tools.
  - Physically walk down to check and verify the OT infrastructure map.
- Create an asset inventory.
  - Include OT devices assigned an Internet Protocol (IP) address.
  - Include software and firmware versions.
  - Include process logic and OT programs.
  - Include removable media.
  - Include standby and spare equipment.
- Identify all communication protocols used across the OT networks.
  - Use vendor-provided tools and procedures to identify OT communications.
  - Use publically available tools, such as Wireshark[7] [9], NetworkMiner [10], GRASSMARLIN [11], and/or other passive network mapping tools.
- Investigate all unauthorized OT communications.
- Catalog all external connections to and from the OT networks.
  - Include all business, vendor, and other remote access connections.
  - Review service contracts to identify all remote connections used for third-party services.

[7] Wireshark is a registered trademark of Wireshark Foundation, Inc.

Understand and Evaluate Cyber-risk on "As-operated" OT Assets

Informed risk awareness can be developed using a variety of readily available resources, many of which include specific guidance and mitigations.

- Use the validated asset inventory to investigate and determine specific risk(s) associated with existing OT devices and OT system software.
  - Vendor-specific cybersecurity and technical advisories.
  - Department of Homeland Security - Cybersecurity and Infrastructure Security Agency Advisories [12]. Available at https://us-cert.cisa.gov/ics/advisories.
  - Department of Homeland Security – Cybersecurity and Infrastructure Security Agency Cyber Security Evaluation Tool [13]. Available at https://us-cert.gov/ncas/current-activity/2019/11/04/cset-version-92-now-available.
  - MITRE[5] Common Vulnerabilities and Exposures (CVE[8]) for both Information Technology and OT devices and system software [14]. Available at https://cve.mitre.org.
  - National Institute of Standards and Technology – National Vulnerability Database [15]. Available at https://nvd.nist.gov.
- Implement mitigations for each relevant known vulnerability, whenever possible (e.g., apply software patches, enable recommended security controls, etc.).
- Audit and identify all OT network services (e.g., system discovery, alerts, reports, timings, synchronization, command, and control) that are being used.
  - Use vendor provided programming and/or diagnostic tools and procedures.

Implement a Continuous and Vigilant System Monitoring Program

A vigilant monitoring program enables system anomaly detection, including many malicious cyber tactics like "living off the land" techniques within OT systems.

- Log and review all authorized external access connections for misuse or unusual activity.
- Monitor for unauthorized controller change attempts.
  - Implement integrity checks of controller process logic against a known good baseline.
  - Where possible, ensure process controllers are prevented from remaining in remote program mode while in operation.
  - Lock or limit set points in control processes to reduce the consequences of unauthorized controller access.

Works Cited

[1] Lyngaas, S. Israeli official confirms attempted cyberattack on water systems. Cyberscoop, 28 May, 2020. [Online] Available at: https://www.cyberscoop.com/israel-cyberattacks-water-iran-yigal-unna
[2] Shodan. [Online] Available at: https://shodan.io
[3] Kamerka. [Online] Available at: https://github.com/woj-ciech/kamerka
[4] Fireeye (2020).Monitoring ICS Cyber Operation Tools and Software Exploit Modules to Anticipate Future Threats. [Online] Available at: https://www.fireeye.com/blog/threat-research/2020/03/monitoring-ics-cyber-operation-tools-and-software-exploit-modules.html
[5] Metasploit. [Online] Available at: https://metasploit.com
[6] Core Impact. [Online] Available at: https://coresecurity.com/products/core-impact
[7] Immunity CANVAS. [Online] Available at: https://immunityinc.com/products/canvas
[8] MITRE ATT&CK for Industrial Control Systems. [Online] Available at: https://collaborate.mitre.org/attackics/index.php/Main_Page
[9] Wireshark. [Online] Available at: https://www.wireshark.org
[10] NetworkMiner. [Online] Available at: https://netresec.com/?page=Networkminer
[11] GRASSMARLIN. [Online] Available at: https://github.com/nsacyber/GRASSMARLIN
[12] Department of Homeland Security - Cybersecurity and Infrastructure Security Agency Advisories. [Online] Available at: https://us-cert.cisa.gov/ics/advisories
[13] Department of Homeland Security - Cybersecurity and Infrastructure Security Agency Cyber Security Evaluation Tool. [Online] Available at: https://us-cert.gov/ncas/current-activity/2019/11/04/cset-version-92-now-available
[14] MITRE Common Vulnerabilities and Exposures. [Online] Available at: https://cve.mitre.org

[8] CVE is a registered trademark of The MITRE Corporation.

[15] National Institute of Standards and Technology National Vulnerability Database. [Online] Available at https://nvd.nist.gov

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact

NSA Cybersecurity

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov

DHS Cybersecurity & Infrastructure Security Agency

CISA encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- CISAServiceDesk@cisa.dhs.gov

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found at http://www.us-cert.gov/.

CISA strives to make this report a valuable tool for our partners and welcomes feedback on how this publication could be improved. You can help by answering a few short questions about this report at the following URL: https://www.us-cert.gov/forms/feedback.