THREAT BULLETINS

OT/ICS Defense: Know the Opponent

TLP:WHITE

Sep 22, 2022

On September 22, 2022, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) published a Joint Cybersecurity Advisory (CSA) (AA22-265A) as operational technology/industrial control system (OT/ICS) assets that operate, control, and monitor day-to-day critical infrastructure and industrial processes continue to be an attractive target for malicious cyber actors.

OT/ICS devices and designs are publicly available, often incorporate vulnerable information technology (IT) components, and include external connections and remote access that increase their attack surfaces. In addition, a multitude of tools are readily available to exploit IT and OT systems. As a result of these factors, malicious cyber actors present an increasing risk to ICS networks.

Health-ISAC is sharing this Joint Cybersecurity Advisory which builds on previous NSA and CISA guidance to increase awareness for OT/ICS network defenders seeking to better understand the tactics,

techniques, and procedures (TTPs) observed to be consistent with OT/ICS threat actors.

OT/ICS assets operate, control, and monitor industrial processes throughout critical infrastructure. Traditional ICS assets are difficult to secure due to their design for maximum availability and safety, coupled with their use of decades-old systems that often lack any recent security updates. Newer ICS assets may be able to be configured more securely, but often have an increased attack surface due to incorporating Internet or IT network connectivity to facilitate remote control and operations. The net effect of the convergence of IT and OT platforms has increased the risk of cyber exploitation of control systems.

Today's cyber realm is filled with well-funded malicious cyber actors financed by nation-states, as well as less sophisticated groups, independent hackers, and insider threats. Control systems have been targeted by a variety of these malicious cyber actors in recent years to achieve political gains, economic advantages, and possibly destructive effects. More recently, APT actors have also developed tools for scanning, compromising, and controlling targeted OT devices.

Malicious Actors' Game Plan for Control System Intrusions

Cyber actors typically follow these steps to plan and execute compromises against critical infrastructure control systems:

- Establish intended effect and select a target.
- Collect intelligence about the target system.
- Develop techniques and tools to navigate and manipulate the system.
- Gain initial access to the system.
- Execute techniques and tools to create the intended effect.

Leveraging specific expertise and network knowledge, malicious actors such as nation-state actors can conduct these steps in a coordinated manner, sometimes concurrently and repeatedly, as illustrated by real-world cyber activity.

Establish Intended Effect and Select a Target

Cyber actors, from cybercriminals to state-sponsored APT actors, target critical infrastructure to achieve a variety of objectives. Cybercriminals are financially motivated and target OT/ICS assets for

financial gain (e.g., data extortion or ransomware operations). State-sponsored APT actors target critical infrastructure for political and/or military objectives, such as destabilizing political or economic landscapes or causing psychological or social impacts on a population. The cyber actor selects the target and the intended effect—to disrupt, disable, deny, deceive, and/or destroy—based on these objectives. For example, disabling power grids in strategic locations could destabilize economic landscapes or support broader military campaigns. Disrupting water treatment facilities or threatening to destroy a dam could have psychological or social impacts on a population.

Collect Intelligence about the Target System

- Once the intent and target are established, the actor collects intelligence on the targeted control system. The actor may collect data from multiple sources, including:
- Open-source research: A great deal of information about control systems and their designs is publicly available. For example, solicitation information and employment advertisements may indicate components and—list specific model numbers.
- Insider threats: The actor may also leverage trusted insiders, even unwitting ones, for collecting information. Social engineering often elicits a wealth of information from people looking for a new job or even just trying to help.
- Enterprise networks: The actor may compromise enterprise IT networks and collect and exfiltrate ICS-related information. Procurement documents, engineering specifications, and even configurations may be stored on corporate IT networks.

In addition to OT-specific intelligence, information about IT technologies used in control systems is widely available. Knowledge that was once limited to control system engineers and OT operators has become easily available as IT technologies move into more of the control system environment. Control system vendors, in conjunction with the owner/operator community, have continually optimized and reduced the cost of engineering, operating, and maintaining control systems by incorporating more commodity IT components and technologies in some parts of OT environments. These advancements sometimes can make information about some systems easily available, thereby increasing the risk of cyber exploitation.

Develop Techniques and Tools

Using the intelligence collected about the control system's design, a cyber actor may procure systems that are similar to the target and configure them as mock-up versions for practice purposes. Nation-state actors can easily obtain most control system equipment. Groups with limited means can still often acquire control systems through willing vendors and secondhand resellers.

Access to a mock-up of the target system enables an actor to determine the most effective tools and techniques. A cyber actor can leverage resident system utilities, and available exploitation tools; or, if necessary, develop or purchase custom tools to affect the control system. Utilities that are already on the system can be used to reconfigure settings and may have powerful troubleshooting capabilities.

As the control system community has incorporated commodity IT and modernized OT, the community has simplified the tools, techniques, scripts, and software packages used in control systems. As a result, a multitude of convenient tools are readily available to exploit IT and OT systems.

Actors may also develop custom ICS-focused malware based on their knowledge of the control systems. For example, TRITON malware was designed to target certain versions of Triconex Tricon programmable logic controllers (PLCs) by modifying in-memory firmware to add additional programming. The extra functionality allows an actor to read/modify memory contents and execute custom code, disabling the safety system. APT actors have also developed tools to scan for, compromise, and control certain Schneider Electric PLCs, OMRON Sysmac NEX PLCs, and Open Platform Communications Unified Architecture (OPC UA) servers.

With TTPs in place, a cyber actor is prepared to do virtually anything that a normal system operator can, and potentially much more.

Gain Initial Access to the System

To leverage the techniques and tools that they developed and practiced, cyber actors must first gain access to the targeted system.

Most modern control systems maintain remote access capabilities allowing vendors, integrators, service providers, owners, and operators access to the system. Remote access enables these parties to perform remote monitoring services, diagnose problems remotely, and verify warranty agreements.

However, these access points often have poor security practices, such as using default and maintenance passwords. Malicious cyber actors can leverage these access points as vectors to covertly gain access to the system, exfiltrate data, and launch other cyber activities before an operator realizes there is a problem. Malicious actors can use web-based search platforms, such as Shodan, to identify these exposed access points.

Vendor access to control systems typically use connections that create a bridge between control system networks and external environments. Often unknown to the owner/operator, this bridge provides yet another path for cyber exploitation and allows cyber actors to take advantage of vulnerabilities in other infrastructure to gain access to the control system.

Remote access points and methodologies use a variety of access and communication protocols. Many are nothing more than vendor-provided dial-up modems and network switches protected only by obscurity and passwords. Some are dedicated devices and services that communicate via more secure virtual private networks (VPNs) and encryption. Few, if any, offer robust cybersecurity capabilities to protect the control system access points or prevent the transmission of acquired data outside the relatively secure environment of the isolated control system. This access to an ostensibly closed control system can be used to exploit the network and components.

Execute Techniques and Tools to Create the Intended Effects

Once an actor gains initial access to the targeted OT/ICS system, the actor will execute techniques, tools, and malware to achieve the intended effects on the target system. To disrupt, disable, deny, deceive, and/or destroy the system, the malicious actor often performs, in any order or in combination, the following activities:

- Degrade the operator's ability to monitor the targeted system or degrade the operator’s confidence in the control system’s ability to operate, control, and monitor the targeted system. Functionally, an actor could prevent the operator's display (human-machine interface, or HMI) from being updated and

selectively update or change visualizations on the HMI, as witnessed during the attack on the Ukraine power grid.

- Operate the targeted control system. Functionally, this includes the ability to modify analog and digital values internal to the system (changing alarms and adding or modifying user accounts), or to change output control points — this includes abilities such as altering tap changer output signals, turbine speed demand, and opening and closing breakers.
- Impair the system's ability to report data. Functionally, this is accomplished by degrading or disrupting communications with external communications circuits (e.g., ICCP, HDLC, PLC, VSAT, SCADA radio, other radio frequency mediums), remote terminal units (RTUs) or programmable logic controllers (PLCs), connected business or corporate networks, HMI subnetworks, other remote I/O, and any connected Historian/bulk data storage.
- Deny the operator's ability to control the targeted system. Functionally, this includes the ability to stop, abort, or corrupt the system's operating system (OS) or the supervisory control and data acquisition (SCADA) system's software functionality.
- Enable remote or local reconnaissance on the control system. Functionally, an actor could obtain system configuration information to enable development of a modified system configuration or a custom tool.

Using these techniques, cyber actors could cause various physical consequences. They could open or close breakers, throttle valves, overfill tanks, set turbines to over-speed, or place plants in unsafe operating conditions. Additionally, cyber actors could manipulate the control environment, obscuring operator awareness and obstructing recovery, by locking interfaces and setting monitors to show normal conditions. Actors can even suspend alarm functionality, allowing the system to operate under unsafe conditions without alerting the operator. Even when physical safety systems should prevent catastrophic physical consequences, more limited effects are possible and could be sufficient to meet the actor's intent. In some scenarios though, if an actor simultaneously manipulates multiple parts of the system, the physical safety systems may not be enough. Impacts to the system could be temporary or permanent, potentially even including physical destruction of equipment.

Reference(s)	CISA, Defense, Defense

Recommendations

The complexity of balancing network security with performance, features, ease-of-use, and availability can be overwhelming for owner/operators. This is especially true where system tools and scripts enable ease-of-use and increase availability or functionality of the control network; and when equipment vendors require remote access for warranty compliance, service obligations, and financial/billing functionality. However, with the increase in targeting of OT/ICS by malicious actors, owner/operators should be more cognizant of the risks when making these balancing decisions. Owner/operators should also carefully consider what information about their systems needs to be publicly available and determine if each external connection is truly needed.

System owners and operators cannot prevent a malicious actor from targeting their systems. Understanding that being targeted is not an “if” but a “when” is essential context for making ICS security decisions. By assuming that the system is being targeted and predicting the effects that a malicious actor would intend to cause, owner/operators can employ and prioritize mitigation actions.

However, the variety of available security solutions can also be intimidating, resulting in choice paralysis. In the midst of so many options, owner/operators may be unable to incorporate simple security and administrative strategies that could mitigate many of the common and realistic threats. Fortunately, owner/operators can apply a few straightforward ICS security best practices to counter adversary TTPs including:

- Limiting Exposure of System Information
- Identifying and Securing Remote Access Points
- Restricting Tools and Scripts
- Conducting Regular Security Audits
- Implementing a Dynamic Network Environment

For additional information regarding details on how to action the above please see the full report here.

Sources

OT/ICS Defense: Know the Opponent

Stop Malicious Cyber Activity Against Connected Operational Technology

NSA and CISA Recommend Immediate Actions, Reduce Exposure Across all OT/ICS

Alert ID b2ca2ce7

View Alert

Tags Operational technology (OT), Industrial Control System (ICS)

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**