
MITRE ATTA&K
Globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.


MITRE
A: Adversarial
T: Tactics
T:Techniques
&
CK: Common Knowledge


ICS TACTICS

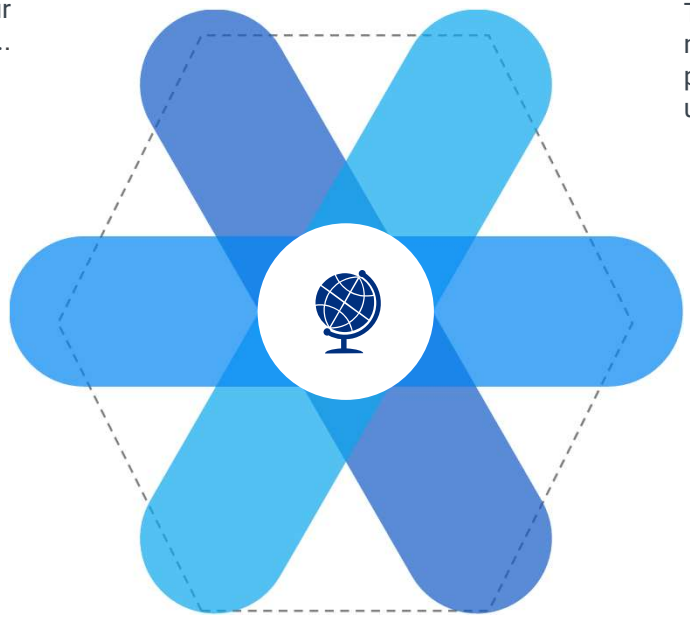
ICS Tactics

Initial Access

The adversary is trying to get into your ICS environment..

Execution

The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way..



Discovery

The adversary is locating information to assess and identify their targets in your environment..

Persistence

The adversary is trying to maintain their foothold in your ICS environment.

Evasion

The adversary is trying to avoid security defenses.

Privilege Escalation

The adversary is trying to gain higher-level permissions.

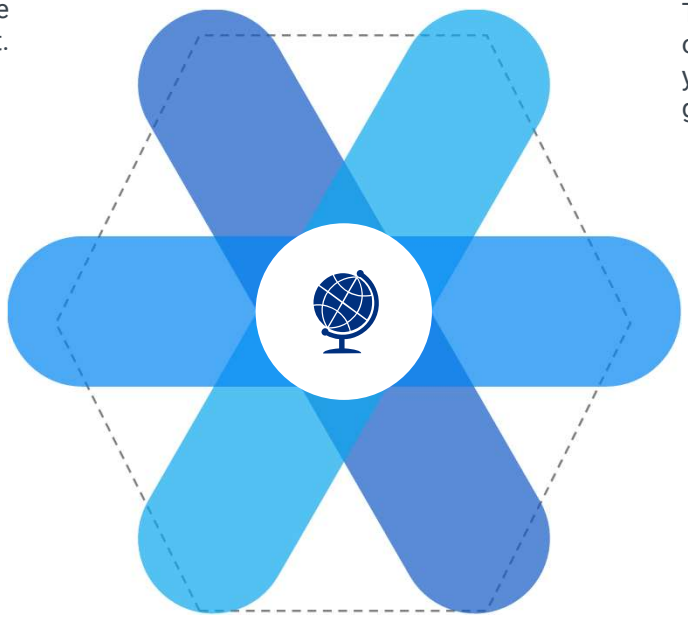
ICS Tactics

Lateral Movement

The adversary is trying to move through your ICS environment.

Collection

The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.



Impact

The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.

Command and Control

The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.

Impair Process Control

The adversary is trying to manipulate, disable, or damage physical control processes..

Inhibit Response Function

The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.

Initial Access

- Initial Access consists of techniques that adversaries may use as entry vectors to gain an initial foothold within an ICS environment.
- These techniques include compromising operational technology assets, IT resources in the OT network, and external remote services and websites.
- They may also target third party entities and users with privileged access.
- In particular, these initial access footholds may include devices and communication mechanisms with access to and privileges in both the IT and OT environments.
- IT resources in the OT environment are also potentially vulnerable to the same attacks as enterprise IT systems.
- Trusted third parties of concern may include vendors, maintenance personnel, engineers, external integrators, and other outside entities involved in expected ICS operations.
- Initial access techniques may also leverage outside devices, such as radios, controllers, or removable media, to remotely interfere with and possibly infect OT operations.

Techniques
Drive by Compromise
Exploit Public-Facing Application
Exploitation of Remote Services
External Remote Services
Internet Accessible Device
Remote Services
Replication Through Removable Media
Rogue master
Spearphishing Attachment
Supply Chain Compromise
Transient Cyber Asset
Wireless Compromise

Execution

- Execution consists of techniques that result in adversary-controlled code running on a local or remote system, device, or other asset.
- This execution may also rely on unknowing end users or the manipulation of device operating modes to run.
- Adversaries may infect remote targets with programmed executables or malicious project files that operate according to specified behavior and may alter expected device behavior in subtle ways.
- Commands for execution may also be issued from command-line interfaces, APIs, GUIs, or other available interfaces.
- Techniques that run malicious code may also be paired with techniques from other tactics, particularly to aid network Discovery and Collection, impact operations, and inhibit response functions.

Techniques
Change Operating Mode
Command-Line Interface
Execution through API
Graphical User Interface
Hooking
Modify Controller Tasking
Native API
Scripting
User Execution

Persistence

- Persistence consists of techniques that adversaries use to maintain access to ICS systems and devices across restarts, changed credentials, and other interruptions that could cut off their access.
- Techniques used for persistence include any access, action, or configuration changes that allow them to secure their ongoing activity and keep their foothold on systems.
- This may include replacing or hijacking legitimate code, firmware, and other project files, or adding startup code and downloading programs onto devices

Techniques
Modify Program
Module Firmware
Project File Infection
System Firmware
Valid Accounts

Privilege Escalation

- The adversary is trying to gain higher-level permissions.
- Privilege escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
- Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.
- Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Techniques
Exploitation for Privilege Escalation
Hooking

Evasion

- Evasion consists of techniques that adversaries use to avoid technical defenses throughout their campaign.
- Techniques used for evasion include removal of indicators of compromise, spoofing communications, and exploiting software vulnerabilities.
- Adversaries may also leverage and abuse trusted devices and processes to hide their activity, possibly by masquerading as master devices or native software.
- Methods of defense evasion for this purpose are often more passive in nature.

Techniques
Change Operating Mode
Exploitation for Evasion
Indicator Removal on Host
Masquerading
Rootkit
Spoof Reporting Message

Discovery

- Discovery consists of techniques that adversaries use to survey your ICS environment and gain knowledge about the internal network, control system devices, and how their processes interact.
- These techniques help adversaries observe the environment and determine next steps for target selection and Lateral Movement.
- They also allow adversaries to explore what they can control and gain insight on interactions between various control system processes.
- Discovery techniques are often an act of progression into the environment which enable the adversary to orient themselves before deciding how to act.
- Adversaries may use discovery techniques that result in collection, to help determine how available resources benefit their current objective.

Techniques
Network Connection Enumeration
Network Sniffing
Remote System Discovery
Remote System Information Discovery
Wireless Sniffing

Lateral Movement

- Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network.
- These techniques abuse default credentials, known accounts, and vulnerable services, and may also leverage dual-homed devices and systems that reside on both the IT and OT networks.
- The adversary uses these techniques to pivot to their next point in the environment, positioning themselves to where they want to be or think they should be.
- Reaching this objective often involves pivoting through multiple systems, devices, and accounts.
- Adversaries may install their own remote tools to accomplish Lateral Movement or leverage default tools, programs, and manufacturer set or other legitimate credentials native to the network, which may be stealthier.

Techniques
Default Credentials
Exploitation of Remote Services
Lateral Tool Transfer
Program Download
Remote Services
Valid Accounts

Collection

- Collection consists of techniques adversaries use to gather domain knowledge and obtain contextual feedback in an ICS environment.
- This tactic is often performed as part of discovery, to compile data on control systems and targets of interest that may be used to follow through on the adversary's objective.
- Examples of these techniques include observing operation states, capturing screenshots, identifying unique device roles, and gathering system and diagram schematics.
- Collection of this data can play a key role in planning, executing, and even revising an ICS-targeted attack.
- Methods of collection depend on the categories of data being targeted, which can include protocol specific, device specific, and process specific configurations and functionality.
- Sensitive floor plans, vendor device manuals, and other references may also be at risk and exposed on the internet or otherwise publicly accessible.

Techniques
Automated Collection
Data from Information Repositories
Detect Operating Mode
I/O Image
Man in the Middle
Monitor Process State
Point & Tag Identification
Program Upload
Screen Capture
Wireless Sniffing

Command and Control

- Command and Control consists of techniques that adversaries use to communicate with and send commands to compromised systems, devices, controllers, and platforms with specialized applications used in ICS environments.
  - Examples of these specialized communication devices include human machine interfaces (HMIs), data historians, SCADA servers, and engineering workstations (EWS).
- Adversaries often seek to use commonly available resources and mimic expected network traffic to avoid detection and suspicion.
  - For instance, commonly used ports and protocols in ICS environments, and even expected IT resources, depending on the target network.
- Command and Control may be established to varying degrees of stealth, often depending on the victim's network structure and defenses.

Techniques
Commonly Used Port
Connection Proxy
Standard Application Layer Protocol

Inhibit Response Function

- Inhibit Response Function consists of techniques that adversaries use to hinder the safeguards put in place for processes and products.
- This may involve the inhibition of safety, protection, quality assurance, or operator intervention functions to disrupt safeguards that aim to prevent the loss of life, destruction of equipment, and disruption of production.
- Adversaries may modify or update system logic, or even outright prevent responses with a denial-of-service.
- As prevention functions are generally dormant, reporting and processing functions can appear fine, but may have been altered to prevent failure responses in dangerous scenarios.
- Unlike evasion, Inhibit Response Function techniques may be more intrusive, such as actively preventing responses to a known dangerous scenario.
- Adversaries may use these techniques to follow through with or provide cover for Impact techniques.

Techniques
Activate Firmware Update Mode
Alarm Suppression
Block Command Message
Block Reporting Message
Block Serial COM
Data Destruction
Denial of Service
Device Restart/Shutdown
Manipulate I/O Image
Modify Alarm Settings
Rootkit
Service Stop
System Firmware

Impair Process Control

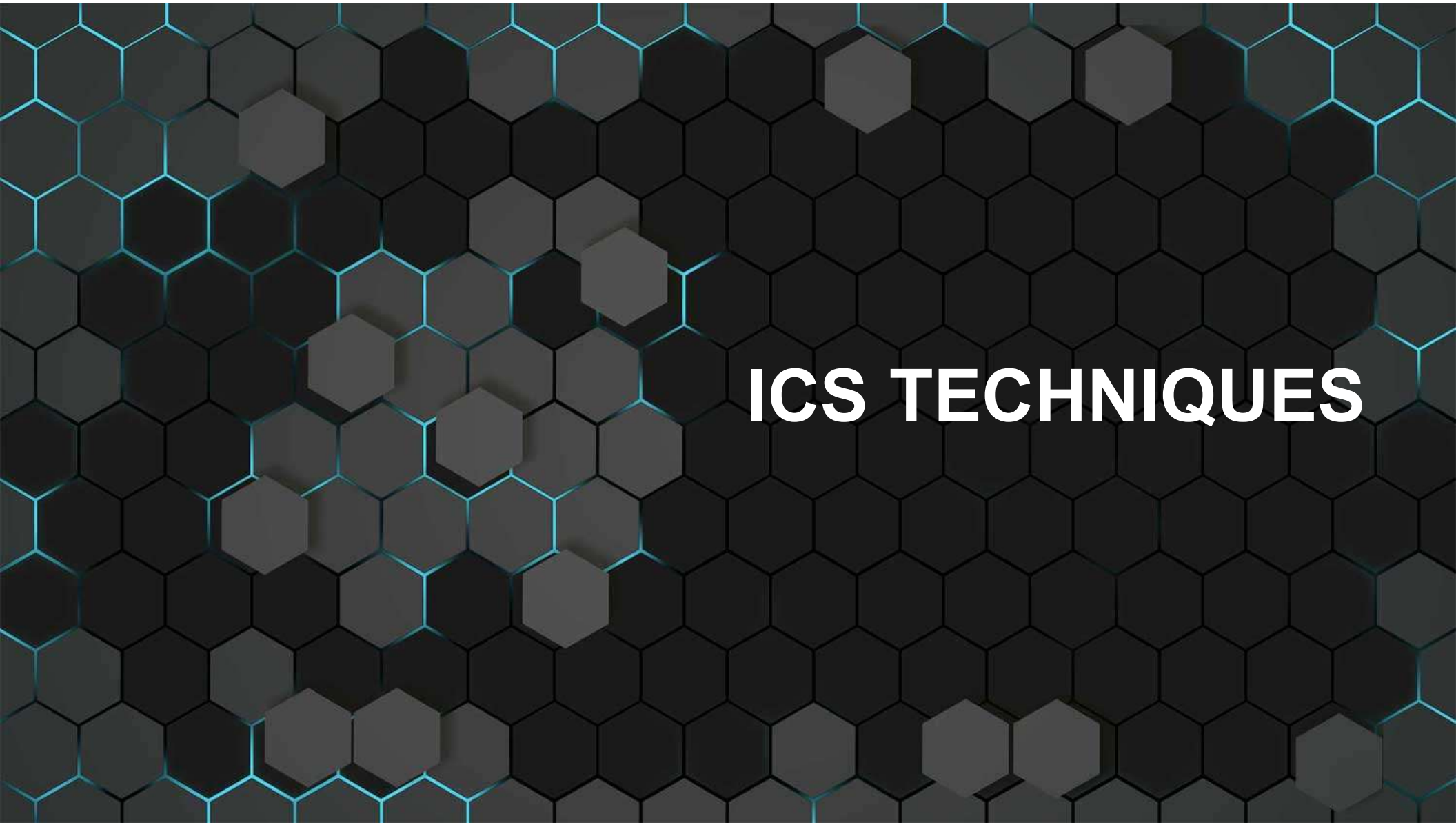
- Impair Process Control consists of techniques that adversaries use to disrupt control logic and cause determinantal effects to processes being controlled in the target environment.
- Targets of interest may include active procedures or parameters that manipulate the physical environment.
- These techniques can also include prevention or manipulation of reporting elements and control logic.
- The direct physical control these techniques exert may also threaten the safety of operators and downstream users, which can prompt response mechanisms.
- Adversaries may follow up with or use Inhibit Response Function techniques in tandem, to assist with the successful abuse of control processes to result in Impact.

Techniques
Brute Force I/O
Modify Parameter
Module Firmware
Spoof Reporting Message
Unauthorized Command Message

Impact

- Impact consists of techniques that adversaries use to disrupt, compromise, destroy, and manipulate the integrity and availability of control system operations, processes, devices, and data.
- These techniques encompass the influence and effects resulting from adversarial efforts to attack the ICS environment or that tangentially impact it.
- Impact techniques can result in more instantaneous disruption to control processes and the operator, or may result in more long term damage or loss to the ICS environment and related operations.
- The adversary may leverage impair process control techniques, which often manifest in more self-revealing impacts on operations, or Inhibit Response Function techniques to hinder safeguards and alarms in order to follow through with and provide cover for Impact.
- In some scenarios, control system processes can appear to function as expected, but may have been altered to benefit the adversary's goal over the course of a longer duration.
- These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

Techniques
Damage to Property
Denial of Control
Denial of View
Loss of Availability
Loss of Control
Loss of Productivity and Revenue
Loss of Protection
Loss of Safety
Loss of View
Manipulation of Control
Manipulation of View
Theft of Operational Information


ICS TECHNIQUES

Activate Firmware Update Mode

- Adversaries may activate firmware update mode on devices to prevent expected response functions from engaging in reaction to an emergency or process malfunction.
- For example, devices such as protection relays may have an operation mode designed for firmware installation.
- This mode may halt process monitoring and related functions to allow new firmware to be loaded.
- A device left in update mode may be placed in an inactive holding state if no firmware is provided to it.
- By entering and leaving a device in this mode, the adversary may deny its usual functionalities.

The **Industroyer** SPIROTEC DoS module places the victim device into \firmware update\ mode. This is a legitimate use case under normal circumstances, but in this case is used the adversary to prevent the SPIROTEC from performing its designed protective functions. As a result the normal safeguards are disabled, leaving an unprotected link in the electric transmission.

IRF

Alarm Suppression

- Adversaries may target protection function alarms to prevent them from notifying operators of critical conditions.

- Disruption of the alarm system does not imply the disruption of the reporting system as a whole.

The method of suppression may greatly depend on the type of alarm in question:

- An alarm raised by a protocol message
- An alarm signaled with I/O
- An alarm bit set in a flag (and read) In ICS environments,

The adversary may have to suppress or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring.

Methods of suppression may involve tampering or altering device displays and logs, modifying in memory code to fixed values, or even tampering with assembly level instruction code.

In the Maroochy Attack, the adversary suppressed alarm reporting to the central computer. Adversaries attempting alarm suppression: prevent outgoing alarms from being raised and prevent incoming alarms from being responded to.

IRF

Automated Collection

Adversaries may automate collection of industrial environment information using tools or scripts.

This automated collection may leverage native control protocols and tools available in the control systems environment.

For example, the OPC protocol may be used to enumerate and gather information.

Access to a system or interface with these native protocols may allow collection and enumeration of other attached, communicating servers and devices.

Backdoor.Oldrea
Using OPC, a component of Backdoor.Oldrea gathers any details about connected devices and sends them back to the C2 for the attackers to analyze.

Industroyer
Industroyer automatically collects protocol object data to learn about control devices in the environment.

CL

Block Command Message

- Adversaries may block a command message from reaching its intended target to prevent command execution.
- In OT networks, command messages are sent to provide instructions to control system devices.
- A blocked command message can inhibit response functions from correcting a disruption or unsafe condition.

Industroyer
In Industroyer the first COM port from the configuration file is used for the actual communication and the two other COM ports are just opened to prevent other processes accessing them. Thus, the IEC 101 payload component is able to take over and maintain control of the RTU device.

Sandworm Team
In the Ukraine 2015 Incident, Sandworm Team blocked command messages by using malicious firmware to render communication devices inoperable

IRF

Block Reporting Message

- Adversaries may block or prevent a reporting message from reaching its intended target.
- In control systems, reporting messages contain telemetry data (e.g., I/O values) pertaining to the current state of equipment and the industrial process.
- By blocking these reporting messages, an adversary can potentially hide their actions from an operator.
- Blocking reporting messages in control systems that manage physical processes may contribute to system impact, causing inhibition of a response function.
- A control system may not be able to respond in a proper or timely manner to an event, such as a dangerous fault, if its corresponding reporting message is blocked.

Industroyer uses the first COM port from the configuration file for the communication and the other two COM ports are opened to prevent other processes accessing them. This may block processes or operators from getting reporting messages from a device.

Sandworm Team
In the Ukraine 2015 Incident, Sandworm Team blocked reporting messages by using malicious firmware to render communication devices inoperable.

IRF

Block Serial COM

- Adversaries may block access to serial COM to prevent instructions or configurations from reaching target devices.
- Serial Communication ports (COM) allow communication with control system devices. Devices can receive command and configuration messages over such serial COM.
- Blocking device serial COM may also block command messages and block reporting messages.
- A serial to Ethernet converter is often connected to a serial COM to facilitate communication between serial and Ethernet devices.
- One approach to blocking a serial COM would be to create and hold open a TCP session with the Ethernet side of the converter.

In Industroyer the first COM port from the configuration file is used for the actual communication and the two other COM ports are just opened to prevent other processes accessing them. Thus, the IEC 101 payload component is able to take over and maintain control of the RTU device.

For example, if there are three serial COM available -- 1, 2 and 3 , the converter might be listening on the corresponding ports 20001, 20002, and 20003. If a TCP/IP connection is opened with one of these ports and held open, then the port will be unavailable for use by another party. One way the adversary could achieve this would be to initiate a TCP session with the serial to Ethernet converter at 10.0.0.1 via Telnet on serial port 1 with the following command: telnet 10.0.0.1 20001.

IRF

Brute Force I/O

- Adversaries may repetitively or successively change I/O point values to perform an action.
- Brute Force I/O may be achieved by changing either a range of I/O point values or a single point value repeatedly to manipulate a process function.
- In the case of brute forcing a range of point values, the adversary may be able to achieve an impact without targeting a specific point.
- In the case where a single point is targeted, the adversary may be able to generate instability on the process function associated with that particular point.
- Adversaries may use Brute Force I/O to cause failures within various industrial processes. These failures could be the result of wear on equipment or damage to downstream equipment.

The Industroyer IEC 104 module has 3 modes available to perform its attack. These modes are range, shift, and sequence.

The range mode operates in 2 stages.

- The first stage of range mode gathers Information Object Addresses (IOA) and sends \select and execute\ packets to switch the state.
- The second stage of range mode has an infinite loop where it will switch the state of all of the previously discovered IOAs.
- Shift mode is similar to range mode, but instead of staying within the same range, it will add a shift value to the default range values

IPC

Change Operating Mode

- Adversaries may change the operating mode of a controller to gain additional access to engineering functions such as program download.
- Programmable controllers typically have several modes of operation that control the state of the user program and control access to the controllers API.
- Operating modes can be physically selected using a key switch on the face of the controller but may also be selected with calls to the controllers API.
- Operating modes and the mechanisms by which they are selected often vary by vendor and product line

EX	EV

Program - This mode must be enabled before changes can be made to a devices program.

Run - Execution of the devices program occurs in this mode. Input and output (values, points, tags, elements, etc.) are monitored and used according to the programs logic.

Remote - Allows for remote changes to a PLCs operation mode.

Stop - The PLC and program is stopped, while in this mode, outputs are forced off.

Reset - Conditions on the PLC are reset to their original states. Warm resets may retain some memory while cold resets will reset all I/O and data registers.

Test / Monitor mode - Similar to run mode, I/O is processed, although this mode allows for monitoring, force set, resets, and more generally tuning or debugging of the system..

Procedure Examples

PLC-Blaster
PLC-Blaster stops the execution of the user program on the target to enable the transfer of its own code. The worm then copies itself to the target and subsequently starts the target PLC again.

Triton
Triton has the ability to halt or run a program through the TriStation protocol. TsHi.py contains instances of halt and run functions being executed

Command-Line Interface

- Adversaries may utilize command-line interfaces (CLIs) to interact with systems and execute commands.
- CLIs provide a means of interacting with computer systems and are a common feature across many types of platforms and devices within control systems environments.
- Adversaries may also use CLIs to install and run new software, including malicious tools that may be installed over the course of an operation.
- CLIs are typically accessed locally, but can also be exposed via services, such as SSH, Telnet, and RDP.
- Commands that are executed in the CLI execute with the current permissions level of the process running the terminal emulator, unless the command specifies a change in permissions context.
- Many controllers have CLI interfaces for management purposes.

The name of the **Industroyer** payload DLL is supplied by the attackers via a command line parameter supplied in one of the main backdoors execute a shell command commands.

Sandworm Team
Sandworm Team uses the MS-SQL server xp_cmdshell command, and PowerShell to execute commands.

Stuxnet
Stuxnet will store and execute SQL code that will extract and execute Stuxnet from the saved CAB file using xp_cmdshell

EX

Commonly Used Port

- Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend in with normal network activity, to avoid more detailed inspection.
- They may use the protocol associated with the port, or a completely different protocol.

TCP:80 (HTTP)
TCP:443 (HTTPS)
TCP/UDP:53 (DNS)
TCP:1024-4999 (OPC on XP/Win2k3)
TCP:49152-65535 (OPC on Vista and later)
TCP:23 (TELNET)
UDP:161 (SNMP)
TCP:502 (MODBUS)
TCP:102 (S7comm/ISO-TSAP)
TCP:20000 (DNP3)
TCP:44818 (Ethernet/IP)

Stuxnet
Stuxnet attempts to contact command and control servers on port 80 to send basic information about the computer it has compromised.

Triton
Triton uses TriStations default UDP port, 1502, to communicate with devices

Connection Proxy

- Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications.
- The definition of a proxy can also be expanded to encompass trust relationships between networks in peer-to-peer, mesh, or trusted connections between networks consisting of hosts or systems that regularly communicate with each other.
- Adversaries could use these types of relationships to manage command and control communications, to reduce the number of simultaneous outbound network connections, to provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion.

Industroyer attempts to connect with a hardcoded internal proxy on TCP 3128 [default Squid proxy]. If established, the backdoor attempts to reach an external C2 server via the internal proxy.

Sandworm Team
Sandworm Team establishes an internal proxy prior to the installation of backdoors within the network

Damage to Property

- Adversaries may cause damage and destruction of property to infrastructure, equipment, and the surrounding environment when attacking control systems.
- Depending on the severity of physical damage and disruption caused to control processes and systems, this technique may result in Loss of Safety.
- Operations that result in Loss of Control may also cause damage to property, which may be directly or indirectly motivated by an adversary seeking to cause impact in the form of Loss of Productivity and Revenue.

- In the Maroochy Attack, 800,000 liters of raw sewage being spilled out into the community. The raw sewage affected local parks, rivers, and even a local hotel.
- A Polish student used a remote controller device to interface with the Lodz city tram system in Poland. Using this remote, the student was able to capture and replay legitimate tram signals. This resulted in damage to impacted trams, people, and the surrounding property.

IM

Data Destruction

- Adversaries may perform data destruction over the course of an operation.
- The adversary may drop or create malware, tools, or other non-native files on a target system to accomplish this, potentially leaving behind traces of malicious activities.
- Such non-native files and other data may be removed over the course of an intrusion to maintain a small footprint or as a standard part of the post-intrusion cleanup process.
- Data destruction may also be used to render operator interfaces unable to respond and to disrupt response functions from occurring as expected.
- An adversary may also destroy data backups.

Industroyer
Industroyer has a destructive wiper that \overwrites all ICS configuration files across the hard drives and all mapped network drives specifically targeting ABB PCM600 configuration files.

KillDisk
KillDisk is able to delete system files to make the system unbootable and targets 35 different types of files for deletion.

IRF

Data from Information Repositories

- Adversaries may target and collect data from information repositories.
- This can include sensitive data such as specifications, schematics, or diagrams of control system layouts, devices, and processes.
- Examples of information repositories include reference databases or local machines in the process environment, as well as workstations and databases in the corporate network that might contain information about the ICS.

In a campaign between 2011 and 2013 against ONG organizations, Chinese state-sponsored actors searched document repositories for specific information such as, system manuals, remote terminal unit (RTU) sites, personnel lists, documents that included the string SCAD*, user credentials, and remote dial-up access information.

CL

Default Credentials

- Adversaries may leverage manufacturer or supplier set default credentials on control system devices.
- These default credentials may have administrative permissions and may be necessary for initial configuration of the device.
- It is general best practice to change the passwords for these accounts as soon as possible, but some manufacturers may have devices that have passwords or usernames that cannot be changed.
- Default credentials are normally documented in an instruction manual that is either packaged with the device, published online through official means, or published online through unofficial means.
- Adversaries may leverage default credentials that have not been properly modified or disabled.

Stuxnet uses a default password hardcoded the WinCC software's database server as one of the mechanisms used to propagate to nearby systems.

LM

Drive by Compromise

- Adversaries may gain access to a system during a drive-by compromise, when a user visits a website as part of a regular browsing session. With this technique, the user's web browser is targeted and exploited simply by visiting the compromised website.
- The adversary may target a specific community, such as trusted third party suppliers or other industry specific groups, which often visit the target website.
- This kind of targeted attack relies on a common interest, and is known as a strategic web compromise or watering hole attack.
- Analysis by DHS and FBI has noted two distinct categories of victims in the Dragonfly campaign on the Western energy sector: staging and intended targets.
  - The adversary targeted the less secure networks of staging targets, including trusted third-party suppliers and related peripheral organizations.
  - Initial access to the intended targets used watering hole attacks to target process control, ICS, and critical infrastructure related trade publications and informational websites.

Watering hole is a computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware.

IA

Procedure Examples-Drive By Compromise

ALLANITE

Leverages watering hole attacks to gain access into electric utilities

OilRig

Has been seen utilizing watering hole attacks to collect credentials which could be used to gain access into ICS networks

TEMP.Veles

Utilizes watering hole websites to target industrial employees.

Dragonfly

Utilized watering hole attacks on energy sector websites by injecting a redirect iframe to deliver Backdoor.Oldrea

Bad Rabbit

Bad Rabbit ransomware spreads through drive-by attacks where insecure websites are compromised..

.

While the target is visiting a legitimate website, a malware dropper is being downloaded from the threat actors infrastructure

Denial of Control

- Adversaries may cause a denial of control to temporarily prevent operators and engineers from interacting with process controls.
- An adversary may attempt to deny process control access to cause a temporary loss of communication with the control device or to prevent operator adjustment of process controls.
- An affected process may still be operating during the period of control loss, but not necessarily in a desired state.

- In the 2017 Dallas Siren incident operators were unable to disable the false alarms from the Office of Emergency Management headquarters.
- In the Maroochy attack, the adversary was able to temporarily shut an investigator out of the network preventing them from issuing any controls
- Industroyer is able to block serial COM channels temporarily causing a denial of control.

IM

Denial of Service

- Adversaries may perform Denial-of-Service (DoS) attacks to disrupt expected device functionality.
- Overwhelming the target device with a high volume of requests in a short time period and sending the target device a request it does not know how to handle.
- Disrupting device state may temporarily render it unresponsive, possibly lasting until a reboot can occur.
- When placed in this state, devices may be unable to send and receive requests, and may not perform expected response functions in reaction to other events in the environment.
- Some ICS devices are particularly sensitive to DoS events, and may become unresponsive in reaction to even a simple ping sweep.

- Adversaries may also attempt to execute a Permanent Denial-of-Service (PDoS) against certain devices, such as in the case of the BrickerBot malware.
- Adversaries may exploit a software vulnerability to cause a denial of service by taking advantage of a programming error in a program, service.
- In the Maroochy attack, the adversary was able to shut an investigator out of the network.

IRF

Procedure Examples

Backdoor.Oldrea
The Backdoor.Oldrea payload has caused multiple common OPC platforms to intermittently crash. This could cause a denial of service effect on applications reliant on OPC communications.

Industroyer
The Industroyer SIPROTEC DoS module exploits the CVE-2015-5374 vulnerability in order to render a Siemens SIPROTEC device unresponsive. Once this vulnerability is successfully exploited, the target device stops responding to any commands until it is rebooted manually. [6] Once the tool is executed it sends specifically crafted packets to port 50,000 of the target IP addresses using UDP. The UDP packet contains the following 18 byte payload: 0x11 49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 9E.

PLC-Blaster
The execution on the PLC can be stopped by violating the cycle time limit. The PLC-Blaster implements an endless loop triggering an error condition within the PLC with the impact of a DoS

Denial of View

- Adversaries may cause a denial of view in attempt to disrupt and prevent operator oversight on the status of an ICS environment.
- This may manifest itself as a temporary communication failure between a device and its control source, where the interface recovers and becomes available once the interference ceases.
- Denying this view may temporarily block and prevent operators from noticing a change in state or anomalous behavior.
- The environment's data and processes may still be operational, but functioning in an unintended or adversarial manner.

Industroyer is able to block serial COM channels temporarily causing a denial of view

In the Maroochy attack, the adversary was able to temporarily shut an investigator out of the network, preventing them from viewing the state of the system.

IM

Detect Operating Mode

- Adversaries may gather information about a PLCs or controllers current operating mode.
- Operating modes dictate what change or maintenance functions can be manipulated and are often controlled by a key switch on the PLC (e.g., run, prog [program], and remote).
- Knowledge of these states may be valuable to an adversary to determine if they are able to reprogram the PLC.
- Some commonly implemented operating modes are Program, Run, Remote, Stop, Reset, Test

Triton contains a file named TS_cnames.py which contains default definitions for program state (TS_progstate). Program state is referenced in TsHi.py.

CL

Device Restart/Shutdown

- Adversaries may forcibly restart or shutdown a device in an ICS environment to disrupt and potentially negatively impact physical processes.
- These functionalities can be executed using interactive device web interfaces, CLIs, and network protocol commands.
- Unexpected restart or shutdown of control system devices may prevent expected response functions happening during critical states.
- A device restart can also be a sign of malicious device modifications, as many updates require a shutdown in order to take effect.

Industroyer
The Industroyer SIPROTEC DoS module exploits the CVE-2015-5374 vulnerability in order to render a Siemens SIPROTEC device unresponsive. While the vulnerability does not directly cause the restart or shutdown of the device, the device must be restarted manually before it can resume operations.

Sandworm Team
In the 2015 attack on the Ukrainian power grid, the Sandworm Team scheduled disconnects of uninterruptable power supply (UPS) systems so that when power was disconnected from the substations, the devices would shut down and service could not be recovered

IRF

Execution through API

Adversaries may attempt to leverage **Application Program Interfaces** (APIs) used for communication between control software and the hardware.

Specific functionality is often coded into APIs which can be called by software to engage specific functions on a device or other software.

Triton leverages a reconstructed TriStation protocol within its framework to trigger APIs related to program download, program allocation, and program changes.

EX

Exploit Public-Facing Application

- Adversaries may leverage weaknesses to exploit internet-facing software for initial access into an industrial network.
  - Internet-facing software may be user applications, underlying networking implementations, an assets operating system, weak defenses, etc.
- Targets of this technique may be intentionally exposed for the purpose of remote management and visibility.
- Publicly exposed applications may be found through online tools that scan the internet for open ports and services.
- Version numbers for the exposed application may provide adversaries an ability to target specific known vulnerabilities.
- Exposed control protocol or remote access ports found in Commonly Used Port may be of interest by adversaries.

Sandworm Team

Sandworm Team actors exploited vulnerabilities in GE's Cimplicity HMI and Advantech/Broadwin WebAccess HMI software which had been directly exposed to the internet

IA

Exploitation for Evasion

- Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to evade detection.
- Vulnerabilities may exist in software that can be used to disable or circumvent security features.
- Adversaries may have prior knowledge through Remote System Information Discovery about security features implemented on control devices.
- There are examples of firmware **RAM/ROM consistency checks on control devices** being targeted by adversaries to enable the installation of malicious System Firmware.

- **Triton** disables a firmware RAM/ROM consistency check after injects a payload (imain.bin) into the firmware memory region.
- Triconex systems include continuous means of detection including checksums for firmware and program integrity, memory and memory reference integrity, and configuration

EV

Exploitation for Privilege Escalation

- Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.
- Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code.
- When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system.
- Vulnerabilities could enable someone to move from unprivileged or user level permissions to system or root permissions depending on the component that is vulnerable.
- This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods.

Triton leverages a previously-unknown vulnerability affecting Tricon MP3008 firmware versions 10.010.4 allows an insecurely-written system call to be exploited to achieve an arbitrary 2-byte write primitive, which is then used to gain supervisor privileges

PE

Exploitation of Remote Services

- Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse.
- A common goal for post-compromise exploitation of remote services is for initial access into and lateral movement throughout the ICS environment to enable access to targeted systems.
- ICS asset owners and operators have been affected by ransomware (or disruptive malware masquerading as ransomware) migrating from enterprise IT to ICS environments: WannaCry, NotPetya, and BadRabbit.
- In each of these cases, self-propagating (wormable) malware initially infected IT networks, but through exploit spread to industrial networks, producing significant impacts.

Bad Rabbit
Bad Rabbit initially infected IT networks, but by means of an exploit spread to industrial networks.

NotPetya
NotPetya initially infected IT networks, but by means of an exploit spread to industrial networks.

Stuxnet
Stuxnet executes malicious SQL commands in the WinCC database server to propagate to remote systems.

WannaCry
WannaCry initially infected IT networks, but by means of an exploit spread to industrial networks

External Remote Services

- Adversaries may leverage external remote services as a point of initial access into your network. Examples are VPNs, Citrix, and other access mechanisms.
- Remote service gateways often manage connections and credential authentication for these services.
- External remote services allow administration of a control system from outside the system. In some cases, this access is enabled directly from the internet..
- The adversary may use these services to gain access to and execute attacks against a control system network.
- Access to valid accounts is often a requirement. Adversaries may begin searching for existing point to point VPN implementations at trusted third party networks or through remote support employee connections where split tunneling is enabled.

Sandworm Team
In the Ukraine 2015 Incident, Sandworm Team harvested VPN worker credentials and used them to remotely log into control system networks

In the **Maroochy Attack**, the adversary was able to gain remote computer access to the system over radio

IA

Graphical User Interface

- Adversaries may attempt to gain access to a machine via a Graphical User Interface (GUI) to enhance execution capabilities.
- Access to a GUI allows a user to interact with a computer in a more visual manner than a CLI.
- If physical access is not an option, then access might be possible via protocols such as VNC on Linux-based and Unix-based operating systems, and RDP on Windows operating systems.
- An adversary can use this access to execute programs and applications on the target machine.

In the **Oldsmar water treatment attack**, adversaries utilized the operator HMI interface through the graphical user interface.
This action led to immediate operator detection as they were able to see the adversary making changes on their screen.

Sandworm Team
In the Ukraine 2015 Incident, Sandworm Team utilized HMI GUIs in the SCADA environment to open breakers

EX

Hooking

- Adversaries may hook into application programming interface (API) functions used by processes to redirect calls for execution and privilege escalation means.
- Windows processes often leverage these API functions to perform tasks that require reusable system resources.
- Windows API functions are typically stored in dynamic-link libraries (DLLs) as exported functions.
- One type of hooking seen in ICS involves redirecting calls to these functions via import address table (IAT) hooking.
- IAT hooking uses modifications to a process IAT, where pointers to imported API functions are stored.

PROCEDURAL EXAMPLES

Stuxnet
Stuxnet modifies the Import Address Tables DLLs to hook specific APIs that are used to open project files.

Triton
Triton's injector, inject.bin, changes the function pointer of the 'get main processor diagnostic data' TriStation command to the address of imain.bin so that it is executed prior to the normal handler.

I/O Image

- Adversaries may seek to capture process values related to the inputs and outputs of a PLC.
- During the scan cycle, a PLC reads the status of all inputs and stores them in an image table.
- The image table is the PLCs internal storage location where values of inputs/outputs for one scan are stored while it executes the user program.
- After the PLC has solved the entire logic program, it updates the output image table.
- The contents of this output image table are written to the corresponding output points in I/O Modules.
- The Input and Output Image tables described above make up the I/O Image on a PLC.

- The collection of the PLCs I/O state could be used to replace values or inform future stages of an attack.

- **Stuxnet** copies the input area of an I/O image into data blocks with a one second interval between copies, forming a 21 second recording of the input area.
- The input area contains information being passed to the PLC from a peripheral. For example, the current state of a valve or the temperature of a device

CL

Indicator Removal on Host

- Adversaries may attempt to remove indicators of their presence on a system in an effort to cover their tracks.
- In cases where an adversary may feel detection is imminent, they may try to overwrite, delete, or cover up changes they have made to the device.

KillDisk deletes application, security, setup, and system event logs from Windows systems.

Triton would reset the controller to the previous state over TriStation and if this failed it would write a dummy program to memory in what was likely an attempt at anti-forensics

EV

Internet Accessible Device

- Adversaries may gain access through systems exposed directly to the internet for remote access rather than through External Remote Services. Internet Accessible Devices are exposed to the internet unintentionally or intentionally without adequate protections.
- This may allow for adversaries to move directly into the control system network. Access onto these devices is accomplished without the use of exploits, these would be represented within the Exploit Public-Facing Application technique.
- These services may be discoverable through the use of online scanning tools.
- In the case of the Bowman dam incident, adversaries leveraged access to the dam control network through a cellular modem. Access to the device was protected by password authentication, although the application was vulnerable to brute forcing.
- In Trend Micros manufacturing deception operations adversaries were detected leveraging direct internet access to an ICS environment through the exposure of operational protocols such as Siemens S7, Omron FINS, and EtherNet/IP, in addition to misconfigured VNC access.

https://www.shodan.io/

IA

Lateral Tool Transfer

- Adversaries may transfer tools or other files from one system to another to stage adversary tools or other files over the course of an operation.
- Copying of files may also be performed laterally between internal victim systems to support Lateral Movement with remote Execution using inherent file sharing protocols such as file sharing over SMB to connected network shares.
- In control systems environments, malware may use SMB and other file sharing protocols to move laterally through industrial networks.

- **Bad Rabbit** can move laterally through industrial networks by means of the SMB service.
- **NotPetya** can move laterally through industrial networks by means of the SMB service.
- **Sandworm Team** used a VBS script to facilitate lateral tool transfer. The VBS script was used to copy ICS-specific payloads with the following command: cscript C:\Backinfo\ufn.vbs C:\Backinfo\101.dll C:\Delta\101.dll
- **Stuxnet** sends an SQL statement that creates a table and inserts a binary value into the table. The binary value is a hex string representation of the main Stuxnet DLL as an executable file and an updated configuration data block.
- **WannaCry** can move laterally through industrial networks by means of the SMB service

LM

Loss of Availability

- Adversaries may attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services.
- Adversaries may leverage malware to delete or encrypt critical data on HMIs, workstations, or databases.

A Conficker infection at a nuclear power plant forced the facility to temporarily shutdown.

In the 2021 Colonial Pipeline ransomware incident, pipeline operations were temporally halted on May 7th and were not fully restarted until May 12th.

IM

Loss of Control

- Adversaries may seek to achieve a sustained loss of control or a runaway condition in which operators cannot issue any commands even if the malicious interference has subsided.
- These targeted attacks affected industrial operations and resulted in breakdowns of control system components and even entire installations.
- As a result of these breakdowns, massive impact resulted in damage and unsafe conditions from the uncontrolled shutdown of a blast furnace.

Industroyer
Industroyer's data wiper component removes the registry \image path\ throughout the system and overwrites all files, rendering the system unusable.

LockerGoga
Some of Norsk Hydro's production systems were impacted by a LockerGoga infection. This resulted in a loss of control which forced the company to switch to manual operations.

IM

Loss of Productivity and Revenue

- Adversaries may cause loss of productivity and revenue through disruption and even damage to the availability and integrity of control system operations, devices, and related processes.
- This technique may manifest as a direct effect of an ICS-targeting attack or tangentially, due to an IT-targeting attack against non-segregated environments.
- In cases where these operations or services are brought to a halt, the loss of productivity may eventually present an impact for the end-users or consumers of products and services.
- The disrupted supply-chain may result in supply shortages and increased prices, among other consequences.

- In the 2021 Colonial Pipeline ransomware incident, the pipeline was unable to transport approximately 2.5 million barrels of fuel per day to the East Coast.
- A ransomware attack on an Australian beverage company resulted in the shutdown of some manufacturing sites, including precautionary halts to protect key systems.
-

IM

Procedure Examples

Bad Rabbit
Several transportation organizations in Ukraine have suffered from being infected by Bad Rabbit, resulting in some computers becoming encrypted, according to media reports.

A **Conficker** infection at a nuclear power plant forced the facility to shutdown and go through security procedures involved with such events, with its staff scanning computer systems and going through all the regular checks and motions before putting the plant back into production.

EKANS infection resulted in a temporary production loss within a Honda manufacturing plant.

LockerGoga
While Norsk Hydro attempted to recover from a LockerGoga infection, most of its 160 manufacturing locations switched to manual (non-IT driven) operations. Manual operations can result in a loss of productivity.

NotPetya disrupted manufacturing facilities supplying vaccines, resulting in a halt of production and the inability to meet demand for specific vaccines.

The **REvil** malware gained access to an organizations network and encrypted sensitive files used by OT equipment.

Ryuk
An enterprise resource planning (ERP) manufacturing server was lost to the Ryuk attack. The manufacturing process had to rely on paper and existing orders to keep the shop floor open.

Loss of Protection

- Adversaries may compromise protective system functions designed to prevent the effects of faults and abnormal conditions.
- This can result in equipment damage, prolonged process disruptions and hazards to personnel.
- Speed is critical in correcting these conditions to limit serious impacts such as Loss of Control and Property Damage.
- Adversaries may target and disable protective system functions as a prerequisite to subsequent attack execution or to allow for future faults and abnormal conditions to go unchecked.
- Detection of a Loss of Protection by operators can result in the shutdown of a process due to strict policies regarding protection systems.

Industroyer contained a module which leveraged a vulnerability in the Siemens SIPROTEC relays to create a Denial of Service against automated protective relays.

IM

Loss of Safety

- Adversaries may compromise safety system functions designed to maintain safe operation of a process when unacceptable or dangerous conditions occur.
- Safety systems are often composed of the same elements as control systems but have the sole purpose of ensuring the process fails in a predetermined safe manner.
- Adversaries may target and disable safety system functions as a prerequisite to subsequent attack execution or to allow for future unsafe conditionals to go unchecked.
- This can cause a Loss of Productivity and Revenue and may meet the technical goals of adversaries seeking to cause process disruptions.

Triton has the capability to reprogram the SIS logic to allow unsafe conditions to persist or reprogram the SIS to allow an unsafe state while using the DCS to create an unsafe state or hazard.

IM

Loss of View

- Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation.
- By causing a sustained reporting or visibility loss, the adversary can effectively hide the present state of operations.
- This loss of view can occur without affecting the physical processes themselves.

Industroyer's data wiper component removes the registry \image path\ throughout the system and overwrites all files, rendering the system unusable.

KillDisk
KillDisk erases the master boot record (MBR) and system logs, leaving the system unusable.

LockerGoga
Some of Norsk Hydro's production systems were impacted by a LockerGoga infection. This resulted in a loss of view which forced the company to switch to manual operations.

IM

Man in the Middle

- Adversaries with privileged network access may seek to modify network traffic in real time using man-in-the-middle (MITM) attacks.
- This type of attack allows the adversary to intercept traffic to and/or from a particular device on the network.
- If a MITM attack is established, then the adversary has the ability to block, log, modify, or inject traffic into the communication stream.
- There are several ways to accomplish this attack, but some of the most-common are Address Resolution Protocol (ARP) poisoning and the use of a proxy.

VPNFilter

The VPNFilter's ssler module configures the device's iptables to redirect all traffic destined for port 80 to its local service listening on port 8888. Any outgoing web requests on port 80 are now intercepted by ssler and can be inspected by the ps module and manipulated before being sent to the legitimate HTTP service

CL

Manipulate I/O Image

- Adversaries may manipulate the I/O image of PLCs through various means to prevent them from functioning as expected.
- Methods of I/O image manipulation may include overriding the I/O table via direct memory manipulation or using the override function used for testing PLC programs.
- One of the unique characteristics of PLCs is their ability to override the status of a physical discrete input or to override the logic driving a physical output coil and force the output to a desired status.

PLC-Blaster
PLC-Blaster may manipulate any outputs of the PLC. Using the POU POKE any value within the process image may be modified.

Stuxnet
When the peripheral output is written to, sequence C intercepts the output and **ensures it is not written to the process image output.**
The output is the instructions the PLC sends to a device to change its operating behavior. By intercepting the peripheral output, Stuxnet prevents an operator from noticing unauthorized commands sent to the peripheral.

IRF

Manipulation of Control

- Adversaries may manipulate physical process control within the industrial environment.
- Methods of manipulating control can include changes to set point values, tags, or other parameters.
- Adversaries may manipulate control systems devices or possibly leverage their own, to communicate with and command physical control processes.
- The duration of manipulation may be temporary or longer sustained, depending on operator detection.

Methods of Manipulation of Control include:

- Man-in-the-middle
- Spoof command message
- Changing setpoints

Industroyer toggles breakers to the open state utilizing unauthorized command messages.

Stuxnet
Stuxnet can reprogram a PLC and change critical parameters in such a way that legitimate commands can be overridden or intercepted. In addition, Stuxnet can apply inappropriate command sequences or parameters to cause damage to property.

IM

Manipulation of View

- Adversaries may attempt to manipulate the information reported back to operators or controllers.
- During this time the process itself could be in a much different state than what is reported.
- Operators may be fooled into doing something that is harmful to the system in a loss of view situation.
- With a manipulated view into the systems, operators may issue inappropriate control sequences that introduce faults or catastrophic failures into the system.
- Business analysis systems can also be provided with inaccurate data leading to bad management decisions.

Industroyer's OPC module can brute force values and will send out a 0x01 status which for the target systems equates to a Primary Variable Out of Limits misdirecting operators from understanding protective relay status.

Stuxnet
Stuxnet manipulates the view of operators replaying process input and manipulating the I/O image to evade detection and inhibit protection functions

IM

Masquerading

- Adversaries may use masquerading to disguise a malicious application or executable as another file, to avoid operator and engineer suspicion.
- By impersonating expected and vendor-relevant files and applications, operators and engineers may not notice the presence of the underlying malicious content and possibly end up running those masquerading as legitimate functions.
- Applications and other files commonly found on Windows systems or in engineering workstations.
- This can be as simple as renaming a file to effectively disguise it in the ICS environment.

EV

Procedure Examples

- **EKANS** masquerades itself as a valid executable with the filename \update.exe. Many valid programs use the process name \update.exe\ to perform background software updates.
- **REvil** searches for whether the Ahnlab autoup.exe service is running on the target system and injects its payload into this existing process.
- **Sandworm Team** transfers executable files as .txt. and then renames them to .exe, likely to avoid detection through extension tracking.
- **Stuxnet** renames s7otbxdx.dll, a dll responsible for handling communications with a PLC. It replaces this dll file with its own version that allows it to intercept any calls that are made to access the PLC.
- **Triton's** injector, inject.bin, masquerades as a standard compiled PowerPC program for the Tricon. Triton was configured to masquerade as trilog.exe, which is the Triconex software for analyzing SIS logs.

Modify Alarm Settings

- Adversaries may modify alarm settings to prevent alerts that may inform operators of their presence or to prevent responses to dangerous and unintended scenarios.
- If an adversary is able to change the reporting settings, certain events could be prevented from being reported.
- This type of modification can also prevent operators or devices from performing actions to keep the system in a safe state.
- In ICS environments, the adversary may have to use Alarm Suppression or contend with multiple alarms and/or alarm propagation to achieve a specific goal to evade detection or prevent intended responses from occurring.

In the Maroochy Attack, the adversary disabled alarms at four pumping stations. This caused alarms to not be reported to the central computer.

IRF

Modify Controller Tasking

- Adversaries may modify the tasking of a controller to allow for the execution of their own programs.
- This can allow an adversary to manipulate the execution flow and behavior of a controller.
- An adversary may modify these associations or create new ones to manipulate the execution flow of a controller.
- Modification of controller tasking can be accomplished using a Program Download in addition to other types of program modification such as online edit and program append.
- Some controller vendors implement tasks with implicit, pre-defined properties whereas others allow for these properties to be formulated explicitly.
- An adversary may associate their program with tasks that have a higher priority or execute associated programs more frequently.

PLC-Blaster
PLC-Blaster's code is stored in OB9999. The original code on the target is untouched. The OB is automatically detected by the PLC and executed.

Stuxnet
Stuxnet infects OB1 so that its malicious code sequence is executed at the start of a cycle. It also infects OB35. OB35 acts as a watchdog, and on certain conditions, it can stop the execution of OB1.

Triton
Triton's \argument-setting\ and inject.bin shellcode are added to the program table on the Tricon so that they are executed by the firmware once each cycle.

EX

Modify Parameter

- Adversaries may modify parameters used to instruct industrial control system devices.
- By modifying system and process critical parameters, the adversary may cause Impact to equipment and/or control processes.
- Modified parameters may be turned into dangerous, out-of-bounds, or unexpected values from typical operations.

- In the Maroochy Attack, Vitek Boden gained remote computer access to the control system and altered data so that whatever function should have occurred at affected pumping stations did not occur or occurred in a different way.
- In the Oldsmar water treatment attack, adversaries raised the sodium hydroxide setpoint value from 100 part-per-million (ppm) to 11,100 ppm, far beyond normal operating levels

IPC

Modify Program

Adversaries may modify or add a program on a controller to affect how it interacts with the physical process, peripheral devices and other hosts on the network.

Modification to controller programs can be accomplished using a Program Download in addition to other types of program modification such as online edit and program append.

Program modification encompasses the addition and modification of instructions and logic contained in Program Organization Units (POU) and similar programming elements found on controllers.

This can include, for example, adding new functions to a controller, modifying the logic in existing functions and making new calls from one function to another..

PLC-Blaster

- PLC-Blaster copies itself to various Program Organization Units (POU) on the target device.
- The POUs include the Data Block, Function, and Function Block.

Stuxnet

- Stuxnet infects PLCs with different code depending on the characteristics of the target system.
- An infection sequence consists of code blocks and data blocks that will be downloaded to the PLC to alter its behavior.

PR

Module Firmware

Adversaries may install malicious or vulnerable firmware onto modular hardware devices. Control system devices often contain modular hardware devices. These devices may have their own set of firmware that is separate from the firmware of the main control system equipment.

An easy point of access for an adversary is the Ethernet card, which may have its own CPU, RAM, and operating system. Exploitation enable the adversary to accomplish additional attacks:

- **Delayed Attack -** The adversary may stage an attack in advance and choose when to launch.
- **Brick the Ethernet Card** - Malicious firmware may be programmed to result in an Ethernet card failure, requiring a factory return.
- **Random Attack or Failure** - The adversary may load malicious firmware onto multiple field devices. Execution of an attack shall be random.

A Field Device Worm –
The adversary may choose to identify all field devices of the same model, with the end goal of performing a device-wide compromise.

Attack Other Cards on the Field Device –
The Ethernet card is most accessible to the adversary and malware. Compromise of the Ethernet card may provide a more direct route to compromising other modules, such as the CPU module.

IPC | PR

Monitor Process State

- Adversaries may gather information about the physical process state.
- This information may be used to gain more information about the process itself or used as a trigger for malicious actions.
- The sources of process state information may vary such as, OPC tags, historian data, specific PLC block information, or network traffic.

Industroyer
Industroyer's OPC and IEC 61850 protocol modules include the ability to send \stVal\ requests to read the status of operational variables.

Stuxnet
Stuxnet examines fields recorded by the DP_RECV monitor to determine if the target system is in a particular state of operation.

CL

Native API

- Adversaries may directly interact with the native OS application programming interface (API) to access system functions.
- Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes.
- These native APIs are leveraged by the OS during system boot as well as carrying out tasks and requests during routine operations.
- Functionality provided by native APIs are often also exposed to user-mode applications via interfaces and libraries.
- For example, functions such as memcpy and direct operations on memory registers can be used to modify user and system memory space.

Procedure Examples

PLC-Blaster
PLC-Blaster uses the system function blocks TCON and TDISCON to initiate and destroy TCP connections to arbitrary systems. Buffers may be sent and received on these connections with TRCV und TSEND system function blocks.

Stuxnet
Stuxnet calls system function blocks which are part of the operating system running on the PLC. They are used to execute system tasks, such as reading the system clock (SFC1) and generating data blocks on the fly.

Triton
Triton's imain.bin payload takes commands from the TsHi.ExplReadRam(Ex), TsHi.ExplWriteRam(Ex) and TsHi.ExplExec functions to perform operations on controller memory and registers using syscalls written in PowerPC shellcode.

EX

Network Connection Enumeration

- Adversaries may perform network connection enumeration to discover information about device communication patterns.
- If an adversary can inspect the state of a network connection with tools, such as Netstat, in conjunction with system firmware, then they can determine the role of certain devices on the network .
- The adversary can also use Network Sniffing to watch network traffic for details about the source, destination, protocol, and content.

- **EKANS** performs a DNS lookup of an internal domain name associated with its target network to identify if it was deployed on the intended system.
- **Industroyer** contains an IEC 61850 module that enumerates all connected network adapters to determine their TCP/IP subnet masks

DI

Network Sniffing

- Network sniffing is the practice of using a network interface on a computer system to monitor or capture information regardless of whether it is the specified destination for the information.
- An adversary may attempt to sniff the traffic to gain information about the target.
- Relatively unimportant information is general communications to and from machines.
- User credentials may be sent over an unencrypted protocol, such as telnet that can be captured and obtained through network packet analysis.
- ARP and Domain Name Service (DNS) poisoning can be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

DI

Procedure Examples

Stuxnet

DP_RECV is the name of a standard function block used by network coprocessors. It is used to receive network frames on the Profibus a standard industrial network bus used for distributed I/O. The original block is copied to FC1869, and then replaced by a malicious block. Each time the function is used to receive a packet, the malicious Stuxnet block takes control: it will call the original DP_RECV in FC1869 and then perform postprocessing on the packet data. The replaced DP_RECV block (later on referred to as the DP_RECV monitor) is meant to monitor data sent by the frequency converter drives to the 315-2 CPU via CP 342-5 Profibus communication modules.

VPNFilter

The VPNFilter packet sniffer looks for basic authentication as well as monitors ICS traffic, and is specific to the TP-LINK R600-VPN. The malware uses a raw socket to look for connections to a pre-specified IP address, only looking at TCP packets that are 150 bytes or larger. Packets that are not on port 502, are scanned for BasicAuth, and that information is logged. This may have allowed credential harvesting from communications between devices accessing a modbus-enabled HMI.

Point & Tag Identification

- Adversaries may collect point and tag values to gain a more comprehensive understanding of the process environment.
- Points may be values such as inputs, memory locations, outputs or other process specific variables.
- Tags are the identifiers given to points for operator convenience. Collecting such tags provides valuable context to environmental points and enables an adversary to map inputs, outputs, and other values to their control processes.

The Backdoor.Oldrea payload has the capability of enumerating OPC tags, in addition to more generic OPC server information.
The server data and tag names can provide information about the names and function of control devices.

CL

Program Download

- Adversaries may perform a program download to transfer a user program to a controller.
- Variations of program download, such as online edit and program append, allow a controller to continue running during the transfer and reconfiguration process without interruption to process control.
- However, before starting a full program download a controller may need to go into a stop state.
- Adversaries may choose to avoid a download all in favor of an online edit or program append to avoid disrupting the physical process.

- An adversary may need to use the technique Detect Operating Mode or Change Operating Mode to make sure the controller is in the proper mode to accept a program download.
- Program download is a high-level term for the suite of vendor-specific API calls used to configure a controllers user program memory space.
- Modify Controller Tasking and Modify Program represent the configuration changes that are transferred to a controller via a program download

LM

Program Upload

- Adversaries may attempt to upload a program from a PLC to gather information about an industrial process.
- Uploading a program may allow them to acquire and study the underlying logic.
- Methods of program upload include vendor software, which enables the user to upload and read a program running on a PLC.
- This software can be used to upload the target program to a workstation, jump box, or an interfacing device.

Triton calls the SafeAppendProgramMod to transfer its payloads to the Tricon. Part of this call includes preforming a program upload.

CL

Project File Infection

- Adversaries may attempt to infect project files with malicious code.
- Using built in functions of the engineering software, adversaries may be able to download an infected program to a PLC in the operating environment enabling further execution and persistence techniques.
- Adversaries may export their own code into project files with conditions to execute at specific intervals.
- Malicious programs allow adversaries control of all aspects of the process enabled by the PLC. Once the project file is downloaded to a PLC the workstation device may be disconnected with the infected project file still executing.

Stuxnet
Stuxnet copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded

PR

Remote Services

- Adversaries may leverage remote services to move between assets and network segments. examples are RDP, SMB, SSH, and other similar mechanisms.
- Remote services could be used to support remote access, data transmission, authentication, name resolution, and other remote functions.
- Further, remote services may be necessary to allow operators and administrators to configure systems within the network from their engineering or management workstations.
- An adversary may use this technique to access devices which may be dual-homed to multiple network segments, and can be used for Program Download or to execute attacks on control devices directly through Valid Accounts.
- Specific remote services (RDP & VNC) may be a precursor to enable Graphical User Interface execution on devices such as HMIs or engineering workstation software.

In the Oldsmar water treatment attack, adversaries gained access to the system through remote access software, allowing for the use of the standard operator HMI interface.

LM | IA

Procedure Examples

Bad Rabbit
Bad Rabbit initially infected IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks.

NotPetya
NotPetya initially infected IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks.

Stuxnet
Stuxnet executes malicious SQL commands in the WinCC database server to propagate to remote systems. The malicious SQL commands include xp_cmdshell, sp_dumpdbilog, and sp_addextendedproc.

WannaCry
WannaCry initially infected IT networks, but by means of an exploit (particularly the SMBv1-targeting MS17-010 vulnerability) spread to industrial networks

Remote System Discovery

- Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for subsequent Lateral Movement or Discovery techniques.
- Functionality could exist within adversary tools to enable this, but utilities available on the operating system or vendor software could also be used.

Backdoor.Oldrea
The Backdoor.Oldrea ICS malware plugin relies on Windows networking (WNet) to discover all the servers, including OPC servers, that are reachable by the compromised machine over the network.

Industroyer
The Industroyer IEC 61850 payload component has the ability to discover relevant devices in the infected host's network subnet by attempting to connect on port 102.

PLC-Blaster
PLC-Blaster scans the network to find other Siemens S7 PLC devices to infect. It locates these devices by checking for a service listening on TCP port 102.

Triton
Triton uses a Python script that is capable of detecting Triconex controllers on the network by sending a specific UDP broadcast packet over port 1502.

DI

Remote System Information Discovery

- An adversary may attempt to get detailed information about remote systems and their peripherals, such as make/model, role, and configuration.
- To aid in targeting and shaping follow-on behaviors. For example, the systems operational role and model information can dictate whether it is a relevant target for the adversary's operational objectives.
- In addition, the systems configuration may be used to scope subsequent technique usage.
- Requests for system information are typically implemented using automation and management protocols and are often automatically requested by vendor software during normal operation.
- This information may be used to tailor management actions, such as program download and system or module firmware. An adversary may leverage this same information by issuing calls directly to the systems API.

DI

Replication Through Removable Media

- Adversaries may move onto systems, such as those separated from the enterprise network, by copying malware to removable media which is inserted into the control systems environment.
- The adversary may rely on unknowing trusted third parties, such as suppliers or contractors with access privileges, to introduce the removable media.
- This technique enables initial access to target devices that never connect to untrusted networks, but are physically accessible.

Operators of the German nuclear power plant, Gundremmingen, discovered malware on a facility computer **not connected to the internet**.

The malware included Conficker and W32.Ramnit, which were also found on eighteen removable disk drives in the facility. The plant has since checked for infection and cleaned up more than 1,000 computers.

An ESET researcher commented that internet disconnection does not guarantee system safety from infection or payload execution.

IA

Procedure Examples

Conficker

- Conficker exploits windows drive shares. Once it has infected a computer, Conficker automatically copies itself to all visible open drive shares on other computers inside the network.

- Nuclear power plant officials suspect someone brought in Conficker by accident on a USB thumb drive, either from home or computers found in the power plant's facility.

Stuxnet

- Stuxnet was able to self-replicate by being spread through removable drives. A willing insider or unknown third party, such as a contractor, may have brought the removable media into the target environment.

- The earliest version of Stuxnet relied on physical installation, infecting target systems when an infected configuration file carried by a USB stick was opened.

Rogue Master

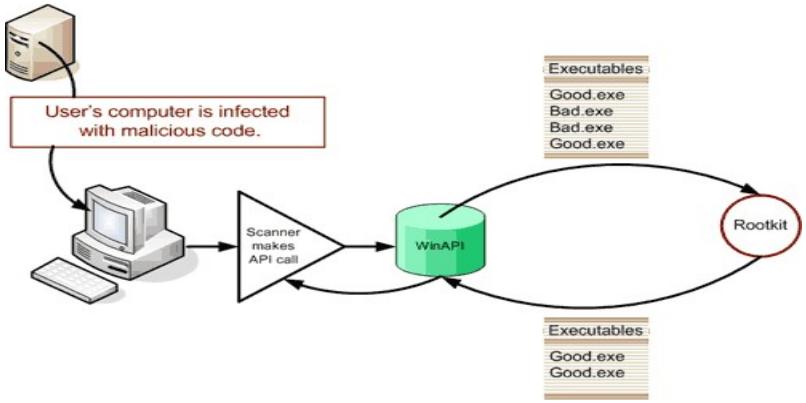
- Adversaries may setup a rogue master to leverage control server functions to communicate with outstations.
- A rogue master can be used to send legitimate control messages to other control system devices, affecting processes in unintended ways.
- It may also be used to disrupt network communications by capturing and receiving the network traffic meant for the actual master.
- Impersonating a master may also allow an adversary to avoid detection.

- In the **Maroochy Attack**, Vitek Boden falsified network addresses in order to send false data and instructions to pumping stations.
- In the case of the 2017 **Dallas Siren incident**, adversaries used a rogue master to send command messages to the 156 distributed sirens across the city, either through a single rogue transmitter with a strong signal, or using many distributed repeaters.

IA

Rootkit

- ❑ Adversaries may deploy rootkits to hide the presence of programs, files, network connections, services, drivers, and other system components.
- ❑ Rootkits are programs that hide the existence of malware by intercepting and modifying operating-system API calls that supply system information.
- ❑ Rootkits or rootkit-enabling functionality may reside at the user or kernel level in the operating system, or lower.



- One of Stuxnet's rootkits is contained entirely in the fake s7otbxdx.dll.
- In order to continue existing undetected on the PLC it needs to account for at least the following situations: read requests for its own malicious code blocks, read requests for infected blocks (OB1, OB35, DP_RECV), and write requests that could overwrite Stuxnets own code.
- Stuxnet contains code to monitor and intercept these types of requests. The rootkit modifies these requests so that Stuxnets PLC code is not discovered or damaged.

IRF EV

Scripting

Adversaries may use scripting languages to execute arbitrary code in the form of a pre-written script or in the form of user-supplied code to an interpreter.

Scripting languages are programming languages that differ from compiled languages, in that scripting languages use an interpreter, instead of a compiler.

These interpreters read and compile **part of the source code** just before it is executed, as opposed to compilers, which compile each and every line of code to an executable file.

Scripting allows software developers to run their code on any system where the interpreter exists. This way, they can distribute one package, instead of precompiling executables for many different systems.

Scripting languages, such as Python, have their interpreters shipped as a default with many Linux distributions.

In addition to being a useful tool for developers and administrators, scripting language interpreters may be abused by the adversary to execute code in the target environment.

Due to the nature of scripting languages, this allows for weaponized code to be deployed to a target easily, and leaves open the possibility of on-the-fly scripting to perform a task.

EX

Procedure Examples

- **APT33** utilized PowerShell scripts to establish command and control and install files for execution.
- **HEXANE** utilizes VBA macros and Powershell scripts such as DanDrop and kl.ps1 tools.
- **OilRig** has embedded a macro within spearphishing attachments that has been made up of both a VBScript and a PowerShell script.
- **REvil** utilizes JavaScript, WScript, and PowerShell scripts to execute. The malicious JavaScript attachment has an obfuscated PowerShell script that executes the malware.
- **Sandworm Team** utilized VBS and batch scripts for file movement and as wrappers for PowerShell execution.
- **Triton** communicates with Triconex controllers using a custom component framework written entirely in Python. The modules that implement the TriStation communication protocol and other supporting components are found in a separate file -- library.zip -- the main script that employs this functionality is compiled into a standalone py2exe Windows executable -- trilog.exe which includes a Python environment.

Screen Capture

- Adversaries may attempt to perform screen capture of devices in the control system environment.
- Screenshots may be taken of workstations, HMIs, or other devices that display environment-relevant process, device, reporting, alarm, or related data.
- These device displays may reveal information regarding the ICS process, layout, control, and related schematics.
- Analysis of screen captures may provide the adversary with an understanding of intended operations and interactions between critical devices.

ALLANITE has been identified to collect and distribute screenshots of ICS systems such as HMIs.

APT33 utilize backdoors capable of capturing screenshots once installed on a system.

CL

Service Stop

- Adversaries may stop or disable services on a system to render those services unavailable to legitimate users.
- Stopping critical services can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.
- Services may not allow for modification of their data stores while running.
- Adversaries may stop services in order to conduct Data Destruction.

EKANS
Before encrypting the process, EKANS first kills the process if its name matches one of the processes defined on the kill-list. EKANS also utilizes netsh commands to implement firewall rules that blocks any remote communication with the device.

Industroyer
Industroyer has the capability to stop a service itself, or to login as a user and stop a service as that user.

KillDisk
KillDisk looks for and terminates two non-standard processes, one of which is an ICS application.

REvil
REvil searches for all processes listed in the prc field within its configuration file and then terminates each process.

IRF

Spearphishing Attachment

Adversaries may use a spearphishing attachment, a variant of spearphishing, as a form of a social engineering attack against specific targets.

Spearphishing attachments are different from other forms of spearphishing in that they employ malware attached to an email.

All forms of spearphishing are electronically delivered and target a specific individual, company, or industry.

In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution and access

A Chinese spearphishing campaign running from December 9, 2011 through February 29, 2012, targeted ONG organizations and their employees. The emails were constructed with a high level of sophistication to convince employees to open the malicious file attachments.

IA

Procedure Examples

Name	Description
ALLANITE	ALLANITE utilized spear phishing to gain access into energy sector environments.
APT33	APT33 sent spear phishing emails containing links to HTML application files, which were embedded with malicious code. APT33 has conducted targeted spear phishing campaigns against U.S. government agencies and private sector companies.
Backdoor.Oldrea	The Backdoor.Oldrea RAT is distributed through a trojanized installer attached to emails.
BlackEnergy	Sandworm Team targeted energy sector organizations in a wide reaching email spearphishing campaign. Adversaries utilized malicious Microsoft Word documents attachments.
Hexane	HEXANE has used malicious documents to drop malware and gain access into an environment.
Lazarus Group	Lazarus Group has been observed targeting organizations using spearphishing documents with embedded malicious payloads. Highly targeted spear phishing campaigns have been conducted against a U.S. electric grid company.
OilRig	OilRig used spearphishing emails with malicious Microsoft Excel spreadsheet attachments.
Sandworm Team	In the Ukraine 2015 incident, Sandworm Team sent spearphishing attachments to three energy distribution companies containing malware to gain access to victim systems.

Spoof Reporting Message

- Adversaries may spoof reporting messages in control system environments for evasion and to impair process control.
- In control systems, reporting messages contain telemetry data (e.g., I/O values) pertaining to the current state of equipment and the industrial process.
- Reporting messages are important for monitoring the normal operation of a system or identifying important events such as deviations from expected values.
- If an adversary has the ability to Spoof Reporting Messages, they can impact the control system in many ways.
- The adversary could also Spoof Reporting Messages to make the defenders and operators think that other errors are occurring in order to distract them from the actual source of a problem.

In the Maroochy Attack, the adversary used a dedicated analog two-way radio system to send false data and instructions to pumping stations and the central computer.

IPC EV

Standard Application Layer Protocol

- Adversaries may establish command and control capabilities over commonly used application layer protocols such as HTTP(S), OPC, RDP, telnet, DNP3, and Modbus.
- These protocols may be used to disguise adversary actions as benign network traffic.
- Standard protocols may be seen on their associated port or in some cases over a non-standard port.

- **BlackEnergy:** Sandworm Team uses HTTP POST request to contact external command and control servers.
- **HEXANE** communicated with command and control over HTTP and DNS.
- **OilRig** communicated with its command and control using HTTP requests.
- **REvil** sends HTTPS POST messages with randomly generated URLs to communicate with a remote server.
- **Triton** can communicate with the implant utilizing the TriStation 'get main processor diagnostic data' command and looks for a specifically crafted packet body from which it extracts a command value and its arguments

Supply Chain Compromise

Adversaries may perform supply chain compromise to gain control systems environment access by means of infected products, software, and workflows.

Supply chain compromise can occur at all stages of the supply chain, from manipulation of development tools and environments to manipulation of developed products and tools distribution mechanisms.

Due to the lack of adherence to standards and overall lesser quality, the counterfeit products may pose a serious safety and operational risk

Yokogawa identified instances in which their customers received counterfeit differential pressure transmitters using the Yokogawa logo. The counterfeit transmitters were nearly indistinguishable with a semblance of functionality and interface that mimics the genuine product.

F-Secure Labs analyzed the approach the adversary used to compromise victim systems with Havex. The adversary planted trojanized software installers available on legitimate ICS/SCADA vendor websites. After being downloaded, this software infected the host computer with a Remote Access Trojan (RAT).

IA

System Firmware

- System firmware on modern assets is often designed with an update feature.
- When available, the firmware update feature enables vendors to remotely patch bugs and perform upgrades.
- An adversary may exploit the firmware update feature on accessible devices to upload malicious or out-of-date firmware.
- Malicious modification of device firmware may provide an adversary with root access to a device, given firmware is one of the lowest programming abstraction layers.

Sandworm Team
In the Ukraine 2015 Incident, Sandworm Team developed and used malicious firmware to render communication devices inoperable.

Triton

- Triton is able to read, write and execute code in memory on the safety controller at an arbitrary address within the devices firmware region.
- This allows the malware to make changes to the running firmware in memory and modify how the device operates.

IRF PR

Theft of Operational Information

- Adversaries may steal operational information on a production environment as a direct mission outcome for personal gain or to inform future operations.
- This information may include design documents, schedules, rotational data, or similar artifacts that provide insight on operations.
- In the Bowman Dam incident, adversaries probed systems for operational data.

ACAD/Medre.A
ACAD/Medre.A can collect AutoCad files with drawings. These drawings may contain operational information.

Duqu
Duqus purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party.

Flame
Flame can collect AutoCAD design data and visio diagrams as well as other documents that may contain operational information.

IM

Transient Cyber Asset

- Adversaries may target devices that are transient across ICS networks and external networks.
- Transient assets are brought into an environment by authorized personnel and do not remain in that environment on a permanent basis.
- Transient assets are commonly needed to support management functions and may be more common in systems where a remotely managed asset is not feasible, external connections for remote access do not exist, or 3rd party contractor/vendor access is required.
- Adversaries may target a transient asset when it is connected to an external network and then leverage its trusted access in another environment to launch an attack.
- Transient assets, in some cases, may not be deployed with a secure configuration leading to weaknesses that could allow an adversary to propagate malicious executable code.

In the **Maroochy attack**, the adversary utilized a computer, possibly stolen, with proprietary engineering software to communicate with a wastewater system.

IA

Unauthorized Command Message

- Adversaries may send unauthorized command messages to instruct control system assets to perform actions outside of their intended functionality, or without the logical preconditions to trigger their expected function.
- If an adversary can send an unauthorized command message to a control system, then it can instruct the control systems device to perform an action outside the normal bounds of the device's actions.

- In the **Maroochy Attack**, the adversary used a dedicated analog two-way radio system to send false data and instructions to pumping stations and the central computer.
- In the **Dallas Siren incident**, adversaries were able to send command messages to activate tornado alarm systems across the city without an impending tornado or other disaster.

Industroyer
Using its protocol payloads, Industroyer sends unauthorized commands to RTUs to change the state of equipment.

Sandworm Team
In the Ukraine 2015 Incident, Sandworm Team issued unauthorized commands to substation breakers after gaining control of operator workstations and accessing a distribution management system (DMS) client application.

IPC

User Execution

- Adversaries may rely on a targeted organizations user interaction for the execution of malicious code.
- User interaction may consist of installing applications, opening email attachments, or granting higher permissions to documents.
- Adversaries may embed malicious code or visual basic code into files such as Microsoft Word and Excel documents or software installers.
- Execution of this code requires that the user enable scripting or write access within the document.
- Embedded code may not always be noticeable to the user especially in cases of trojanized software.

A Chinese spearphishing campaign running from December 9, 2011 through February 29, 2012 delivered malware through spearphishing attachments which required user action to achieve execution

- Execution of **Backdoor.Oldrea** relies on a user opening a trojanized installer attached to an email.
- **Bad Rabbit** is disguised as an Adobe Flash installer. When the file is opened it starts locking the infected computer.
- **REvil** initially executes when the user clicks on a JavaScript file included in the phishing emails .zip attachment. [6]
- **Stuxnet** infects DLL's associated with the WinCC Simatic manager which are responsible for opening project files. If a user opens an uninfected project file using a compromised manager, the file will be infected with Stuxnet code. If an infected project is opened with the Simatic manager, the modified data file will trigger a search for the \xyz.dll\ file. If the \xyz.dll\ file is not found in any of the specified locations, the malicious DLL will be loaded and executed by the manager.

EX

Valid Accounts

- Adversaries may steal the credentials.
- Default credentials for control system devices may be publicly available.
- Compromised credentials may be used to bypass access controls.
- Compromised and default credentials may also grant an adversary increased privilege to specific systems.
- Adversaries may also create accounts, sometimes using predefined account names and passwords, to provide a means of backup access for persistence.
- Adversaries may choose not to use malware or tools, in conjunction with the legitimate access those credentials provide, to make it harder to detect their presence or to control devices and send legitimate commands in an unintended way.

Procedure Examples

- **ALLANITE** utilized credentials collected through phishing and watering hole attacks.
- **BlackEnergy:** Sandworm Team utilizes valid user and administrator credentials, in addition to creating new administrator accounts to maintain presence.
- **HEXANE** has used valid IT accounts to extend their spearphishing campaign within an organization.
- **OilRig** utilized stolen credentials to gain access to victim machines.
- **Sandworm Team** used valid accounts to laterally move through VPN connections and dual-homed systems. In the Ukraine 2015 Incident, Sandworm Team used the credentials of valid accounts to interact with client applications and access employee workstations hosting HMI applications.
- **TEMP.Veles** used valid credentials when laterally moving through RDP jump boxes into the ICS environment.

Wireless Compromise

- Adversaries may perform wireless compromise as a method of gaining communications and unauthorized access to a wireless network.
- Access to a wireless network may be gained through the compromise of a wireless device.
- Adversaries may also utilize radios and other wireless communication devices on the same frequency as the wireless network.

IA

A joint case study on the **Maroochy Shire Water Services** event examined the attack from a cyber security perspective.

The adversary disrupted Maroochy Shire's radio-controlled sewage system by driving around with stolen radio equipment and issuing commands with them. Boden used a **two-way radio to communicate** with and set the frequencies of Maroochy Shire's repeater stations.

Polish student used a modified TV remote controller to gain access to and control over the Lodz city tram system in Poland.

- The remote controller device allowed the student to interface with the trams network to modify track settings and override operator control.
- The adversary may have accomplished this by **aligning the controller to the frequency and amplitude of IR control protocol signals.** The controller then enabled initial access to the network, allowing the capture and replay of tram signals.

Wireless Sniffing

- Adversaries may seek to capture radio frequency (RF) communication used for remote control and reporting in distributed environments.
- RF communication frequencies vary between 3 kHz to 300 GHz, although are commonly between 300 MHz to 6 GHz.
- Some examples of wireless protocols : Wireless HART, Zigbee, WIA-FA, and 700 MHz Public Safety Spectrum.
- Information transmitted over a wireless medium may be captured in-transit whether the sniffing device is the intended destination or not.

- Adversaries may capture RF communications by using specialized hardware, such as software defined radio (SDR), handheld radio, or a computer with radio demodulator tuned to the communication frequency.

In the 2017 Dallas Siren incident, it is suspected that adversaries likely captured wireless command message broadcasts on a 700 MHz frequency during a regular test of the system. These messages were later replayed to trigger the alarm systems.

CL | DI


ICS MITIGATIONS

MITIGATIONS

Access Management

- Access Management technologies can be used to enforce authorization polices and decisions, especially when existing field devices do not provided sufficient capabilities to support user identification and authentication.

Account Use Policies

- Configure features related to account use like login attempt lockouts, specific login times, etc.

Active Directory Configuration

- Configure Active Directory to prevent use of certain techniques; use security identifier (SID) Filtering, etc.

Antivirus/Antimalware

- Use signatures or heuristics to detect malicious software. Within industrial control environments, antivirus/antimalware installations should be limited to assets that are not involved in critical or real-time operations.

Application Developer Guidance

- This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an adversary may be able to take advantage of.

Application Isolation and Sandboxing

- Restrict the execution of code to a virtual environment on or in-transit to an endpoint system.

MITIGATIONS

Audit
Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.

Authorization Enforcement
The device or system should restrict read, manipulate, or execute privileges to only authenticated users who require access based on approved security policies.

Boot Integrity
Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.

Code Signing
Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.

Communication Authenticity
When communicating over an untrusted network, utilize secure network protocols that both authenticate the message sender and can verify its integrity.

Data Backup
Take and store data backups from end user systems and critical servers.

MITIGATIONS

Data Loss Prevention
Data Loss Prevention (DLP) technologies can be used to help identify adversarial attempts to exfiltrate operational information, such as engineering plans, trade secrets, recipes, intellectual property, or process telemetry.

Disable or Remove Feature or Program
Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

Encrypt Network Traffic
Utilize strong cryptographic techniques and protocols to prevent eavesdropping on network communications.

Encrypt Sensitive Information
Protect sensitive data-at-rest with strong encryption.

Execution Prevention
Block execution of code on a system through application control, and/or script blocking.

Exploit Protection
Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.

Filter Network Traffic
Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

MITIGATIONS

Human User Authentication
Require user authentication before allowing access to data or accepting commands to a device.

Limit Access to Resource Over Network
Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.

Limit Hardware Installation
Block users or groups from installing or using unapproved hardware on systems, including USB devices.

Mechanical Protection Layers
Utilize a layered protection design based on physical or mechanical protection systems to prevent damage to property, equipment, human safety, or the environment.

Minimize Wireless Signal Propagation
Wireless signals frequently propagate outside of organizational boundaries, which provide opportunities for adversaries to monitor or gain unauthorized access to the wireless network.

Mitigation Limited or Not Effective
This type of attack technique cannot be easily mitigated with preventative controls since it is based on the abuse of system features.

MITIGATIONS

Multi-factor Authentication
Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.

Network Allowlists
Network allowlists can be implemented through either host-based files or system hosts files to specify what connections (e.g., IP address, MAC address, port, protocol) can be made from a device.

Network Intrusion Prevention
Use intrusion detection signatures to block traffic at network boundaries.

Network Segmentation
Architect sections of the network to isolate critical systems, functions, or resources.

Operating System Configuration
Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.

Operational Information Confidentiality
Deploy mechanisms to protect the confidentiality of information related to operational processes, facility locations, device configurations, programs, or databases that may have information that can be used to infer organizational trade-secrets, recipes, and other intellectual property (IP).

MITIGATIONS

Out-of-Band Communications Channel
Have alternative methods to support communication requirements during communication failures and data integrity attacks.

Password Policies
Set and enforce secure password policies for accounts.

Privileged Account Management
Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.

Redundancy of Service
Redundancy could be provided for both critical ICS devices and services, such as back-up devices or hot-standbys.

Restrict File and Directory Permissions
Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.

Restrict Library Loading
Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.

Restrict Registry Permissions
Restrict the ability to modify certain hives or keys in the Windows Registry.

Restrict Web-Based Content
Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc.

MITIGATIONS

Safety Instrumented Systems
Utilize Safety Instrumented Systems (SIS) to provide an additional layer of protection to hazard scenarios that may cause property damage.

Software Configuration
Implement configuration changes to software (other than the operating system) to mitigate security risks associated with how the software operates.

Software Process and Device Authentication

Require the authentication of devices and software processes where appropriate.

SSL/TLS Inspection
Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.

Static Network Configuration
Configure hosts and devices to use static network configurations when possible, protocols that require dynamic discovery/addressing (e.g., ARP, DHCP, DNS).

Supply Chain Management
Implement a supply chain management program, including policies and procedures to ensure all devices and components originate from a trusted supplier and are tested to verify their integrity.

Threat Intelligence Program
A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.

Update Software
Perform regular software updates to mitigate exploitation risk. Software updates may need to be scheduled around operational down times.

MITIGATIONS

User Account Management
Manage the creation, modification, use, and permissions associated to user accounts.

User Training
Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.

Vulnerability Scanning
Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.

Watchdog Timers
Utilize watchdog timers to ensure devices can quickly detect whether a system is unresponsive.