MITRE | SOLVING PROBLEMS FOR A SAFER WORLD

BIRD Project Review Workshop

Marie Collins, Adam Hahn

Jan, 24, 2022

Established

1958

Today We Operate Six FFRDCs

National Security Engineering Center

Center for Advanced Aviation System Development

Homeland Security Systems Engineering and Development Institute

CMS Alliance to Modernize Healthcare

Center for Enterprise Modernization

National Cybersecurity FFRDC

MITRE

Mission-Driven

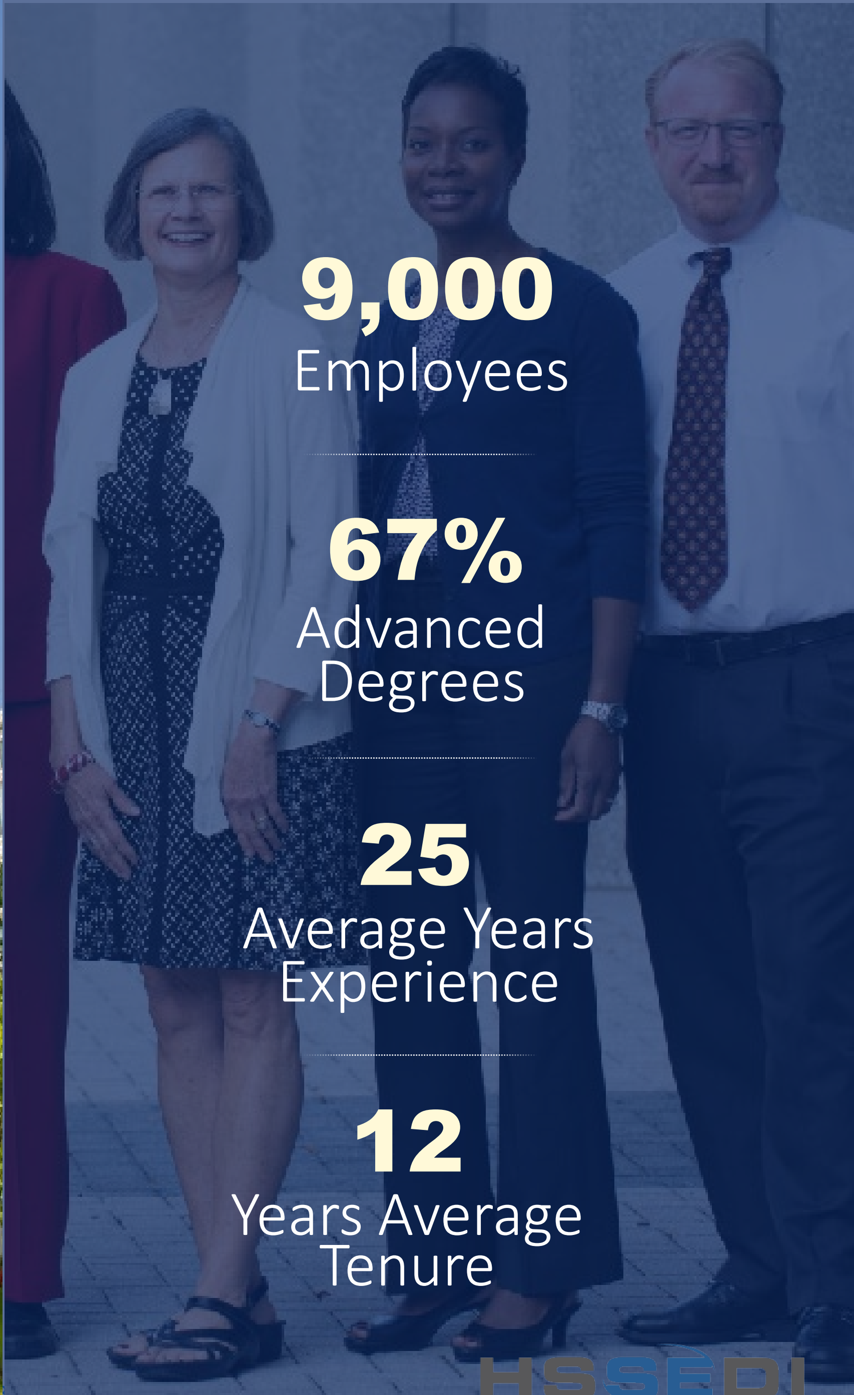
Objective Insight

Unique Vantage Point

Technical Know-How

Pioneering Together

Serve the Public Interest



9,000
Employees

67%
Advanced Degrees

25
Average Years Experience

12
Years Average Tenure

MITRE Tasking

Task 4 – Multi-Level Threat Intelligence Knowledge Base

1. MITRE will deliver ATT&CK for ICS training materials

2. MITRE will deliver ATT&CK for ICS based adversarial models, using known ICS attack vectors and TTPs, and aligned with the unique architectures and devices supporting SCADA/EMS applications. The proposed adversarial models will also inform automated techniques for attack detection and threat hunting.

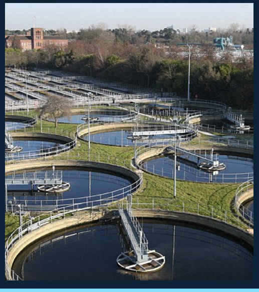
3. MITRE will deliver ATT&CK for ICS based adversarial models to support the assessment of the proposed cyber resiliency techniques, including proposed physics-based device designs and machine learning based techniques.

What is ATT&CK® for ICS?

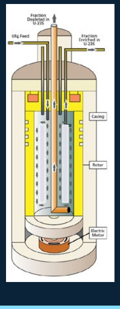
A knowledge base of adversary behavior

- *Based on real-world observations*
- *Free, open, and globally accessible*
- *A common language*
- *Community-driven*

Maroochy Water Services (2000)

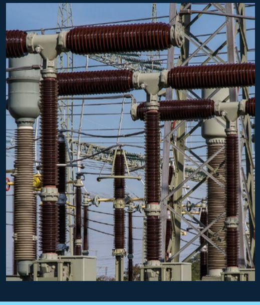


Stuxnet (2011)

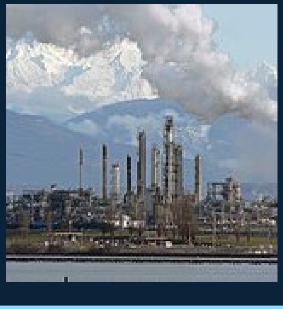


BlackEnergy3 (2015)

Industroyer (2016)



Triton (2017)



Tactics

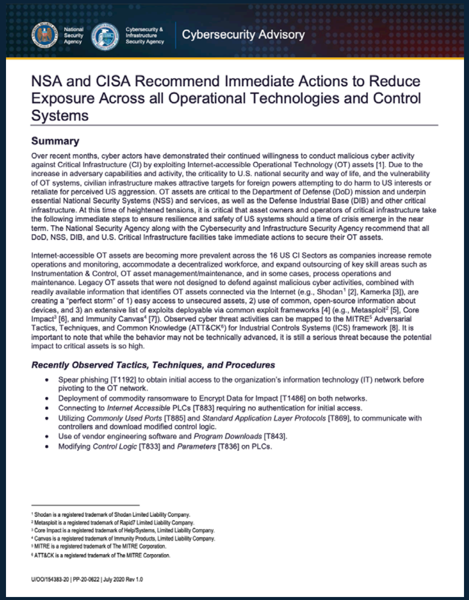
Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
External Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Internet Accessible Device	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Remote Services	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Replication Through Removable Media	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Rogue Master							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Spearphishing Attachment									Rootkit		Manipulation of View
Supply Chain Compromise									Service Stop		Theft of Operational Information
Wireless Compromise									System Firmware		

MITRE

ATT&CK for ICS Adoption

Government



National Security Agency | Cybersecurity & Infrastructure Security Agency | Cybersecurity Advisory

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

Summary

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

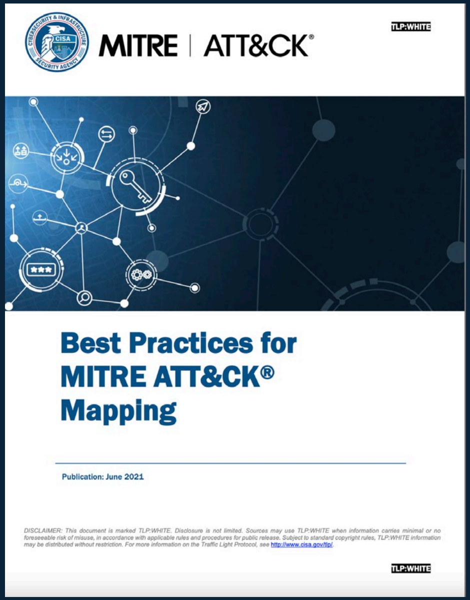
Internet-accessible OT assets are becoming more prevalent across the 16 US CI Sectors as companies increase remote operations and monitoring, accommodate a decentralized workforce, and expand outsourcing of key skill areas such as Instrumentation & Control, OT asset management/maintenance, and in some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

Recently Observed Tactics, Techniques, and Procedures

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

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

U/OO/154383-20 | PP-20-0622 | July 2020 Rev 1.0



MITRE | ATT&CK®

TLP:WHITE

Best Practices for MITRE ATT&CK® Mapping

Publication: June 2021

DISCLAIMER: This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

TLP:WHITE

Industry

SANS / DRAGOS

MITRE ATT&CK for ICS Webinar

April 2, 2020

Robert M. Lee
Dragos CEO

Austin Scott
Dragos ICS Penetration Testing Principal

DRAGOS

ADDRESSING THE MITRE ATT&CK FOR ICS MATRIX

How CyberX Protects Against IoT/ICS Threats Described in

FORESCOUT

From Events to TTPs:
Maturing OT Incident Response with MITRE ATT&CK® for ICS

by Forescout Research Labs

INDUSTRIAL DEFENDER

MITRE ATT&CK for ICS Detection Methods

CyberSecurity

FILLING THE GAP WITH MITRE ATT&CK FOR ICS

FELIX RODER, SECURITY ANALYST

ARMIS

HOW ARMIS SUPPORTS THE MITRE ATT&CK™ FOR ICS MATRIX

Grantek and ThreatGEN Cybersecurity Webinar: ICS ATT&CK

Creating a More Cost-Effective Risk Mitigation Strategy

March 5, 2020

GRANTEK

THREATGEN

Isaac Guevara
ICS Network/Cybersecurity Specialist, Grantek

Clint Bodungen
Founder & CEO, ThreatGEN

Technology Transfer at MITRE

- While serving our government sponsors, MITRE develops intellectual property which would be of great value to the government and the nation if it were readily available

- Because product development is not part of our mission, in many cases MITRE must transfer IP to commercial organizations that can undertake the technical, business, and manufacturing activities necessary to bring products incorporating the technology to market.

- 3 Approaches to transfer of MITRE IP
  – Transfer to government program
  – Transfer into public domain (publishing or open source licensing)
  – Transfer directly to a commercial company

External Impact

Broad Industry Impact through Security Standards Initiatives

- ATT&CK for ICS
- ATT&CK for Mobile
- Common Weakness Enumeration (CWE) – Top 25 and expansion to hardware
- Common Vulnerability Enumeration (CVE)
- Software Supply Chain System of Trust and Software Bill of Materials (SBOM)

Government-Wide Impacts

NIST Guidance

- Cyber Resiliency Engineering
- Information Security Continuous Monitoring
- Identity Proofing Templates and Authentication guidance
- Privacy Engineering

External Capability Delivery

- Security Automation Framework saf.mitre.org
- Medical Device Innovation Sandbox and BioHacking Village

Major Vendor Impacts

- Microsoft adoption of WinKIM
- Intel collaboration to expand CWE to hardware
- Cross Domain Unstructured Data Exchange (CDUX) at major cloud providers

International Cyber Capacity Building

Many Recent Patents