

ICS Malware

What is ICS Malware?

ICS malware is malicious software specifically designed to target Industrial Control Systems (ICS) by interacting with Operational Technology (OT) devices and ICS-specific communication protocols. It must meet three key criteria:

- ICS-capable** – Can navigate, alter, or extract data from OT networks and interact with PLCs.
- Designed with Malicious Intent** – Created for nefarious purposes, not just repurposed benign software.
- Result in Adverse Effects on OT Environment** – Leads to unauthorized access, process manipulation, or physical/operational disruption.

Types of ICS Malware

Our paper examines two types of ICS malware: **high-impact ICS malware** and **ICS ransomware**.

Malware Name	Year Discovered	MITRE ATT&CK ID	Involved APT	Targeted Industries	Targeted ICS Components	Exploited ICS Communication Protocols
1 Stuxnet	2010	S0603	Equation Group (USA, Israel)	nuclear/CS	Siemens PLCs	Siemens Protocols
2 Havex (Backdoor/OTnet)	2013	S0093	Dragonfly / Energetic Bear (Russia)	energy, aviation pharmaceutical, defense, petrochemical	OPC Servers	OPC
3 BlackEnergy2	2016	S0089	Sandworm (Russia)	ICS/SCADA companies, energy, railway, mining	Modbus	Modbus
4 Industroyer (CrasChverdo)	2016	S0604	Sandworm (Russia)	power grid	Siemens S700 IEC devices	IEC-101 IEC-104 IEC-61850 OPC
5 Triton (Trin, Netkan)	2017	S1009	TEMP/Velox (Russia)	petrochemical	Tridation	Tridation
6 Industroyer2	2022	S1072	Sandworm (Russia)	power grid	IEC-104 controllers	IEC-104
7 Pipedream (incontroller)	2022	S1045	Chernovite (Russia)	ICS/SCADA systems	Schneider Electric's Triconex Safety Instrumented System (SIS) controllers	OPC UA Modbus COCOSYS
8 CosmicEnergy	2023	NA	Russia-linked red teaming group	power grid	IEC-104 devices	IEC-104
9 Fluxnet	2024	S1187	Blackjack group (linked to Ukraine intelligence services)	critical infrastructure including: airports, water treatment, gas pipelines	M-Bus Industrial sensors	M-Bus
10 FrostyDroop (Buddiem)	2024	NA	Russia-linked APT	wide range of ICS & critical infrastructure	EMCO controllers/PLCs	Modbus TCP

Table I. High-impact ICS malware strains discovered to-date

Malware Name	Year Discovered	MITRE ATT&CK ID	Involved APT	Targeted Industries	Targeted ICS Components	Exploited ICS Communication Protocols
1 WannaCry	2017	S0366	APT28 (North Korea)	many industries including healthcare, manufacturing, financial services, government	SMB service in production/OT systems	[SMB]
2 NotPetya (EvPhet, GoldenEye, Palnare, NetWin)	2017	S0368	Sandworm Team (Russia)	many industries including pharmaceutical shipping, energy, gas/oil	SMB service in production/OT systems	[SMB, DHCP, VTLIM]
3 BadRabbit (ElamirPalya, ExPhet)	2017	S0606	Sandworm Team (Russia)	transportation, government services, media outlets	SMB service in production/OT systems	[SMB]
4 LockerGoga	2019	S0372	FIN6 (North Korea)	industrial and manufacturing firms	PLC and servers in production/OT systems	
5 REvil (Sodin, Sodinokibi)	2019	0496	Gold Southfield (Russia)	aluminum automotive, automotive, manufacturing	encrypts files/data used by OT components	[SMB, HTTP]
6 EKANS	2020	S0605	Unknown (likely Iranian or Iranian-linked nation state)	energy, healthcare, automotive, manufacturing	various ICS-related processes (e.g., GE Proficy data historian, Honeywell HUI/Win)	

Table II. ICS ransomware strains discovered to-date

MITRE ATT&CK Framework and Navigator Tool

What is MITRE ATT&CK?

MITRE ATT&CK is a **framework for modeling and analyzing adversary behaviors** in cyber threats and attacks. It consists of **Tactics, Techniques, and Procedures (TTPs)** that describe how cyber adversaries operate. The framework includes:

- TTP Matrices** – Organized visual representations of attack techniques across different environments.
- Threat Intelligence Repository** – Data on real-world APT groups, malware, and attack campaigns.
- Open-Source Tools** – Such as MITRE ATT&CK Navigator for visualization and Top ATT&CK Techniques Calculator for prioritizing security defenses.

What is MITRE ATT&CK Navigator?

MITRE ATT&CK Navigator is an open source tool built on the concept of MITRE ATT&CK matrices, and specifically designed to facilitate visualization and analysis of complex adversary behaviors. In particular, Navigator can be used to:

- Visually codify the TTPs deployed in the course of an actual attack or a potential threat,
- Compare and contrast TTPs deployed by (e.g.) different APTs or different malware strains,
- Help cyber defenders identify the best defenses against each particular attack/threat, etc.

Novel Methodolgy for Ranking/Prioritization of Mitigation and Detection Techniques

What is our Novel Methodology?

The novel methodology in the paper is designed to rank and prioritize mitigation and detection techniques against ICS malware using the MITRE ATT&CK framework. It follows these key steps:

- Identify Common Adversary Techniques** – Using MITRE ATT&CK Navigator, the study maps techniques used by ICS malware strains.
- Map Mitigation & Detection Strategies** – Each adversary technique is linked to recommended MITRE mitigation and detection strategies.
- Assign Effectiveness Scores** – A scoring formula evaluates how well each mitigation or detection strategy defends against multiple attack techniques.
- Prioritize Defenses** – Strategies with higher scores are considered more effective and should be implemented first.

Figure 3. Parameters and formulas for calculation of 'mitigation/detection effectiveness score' against a specific group of attacks

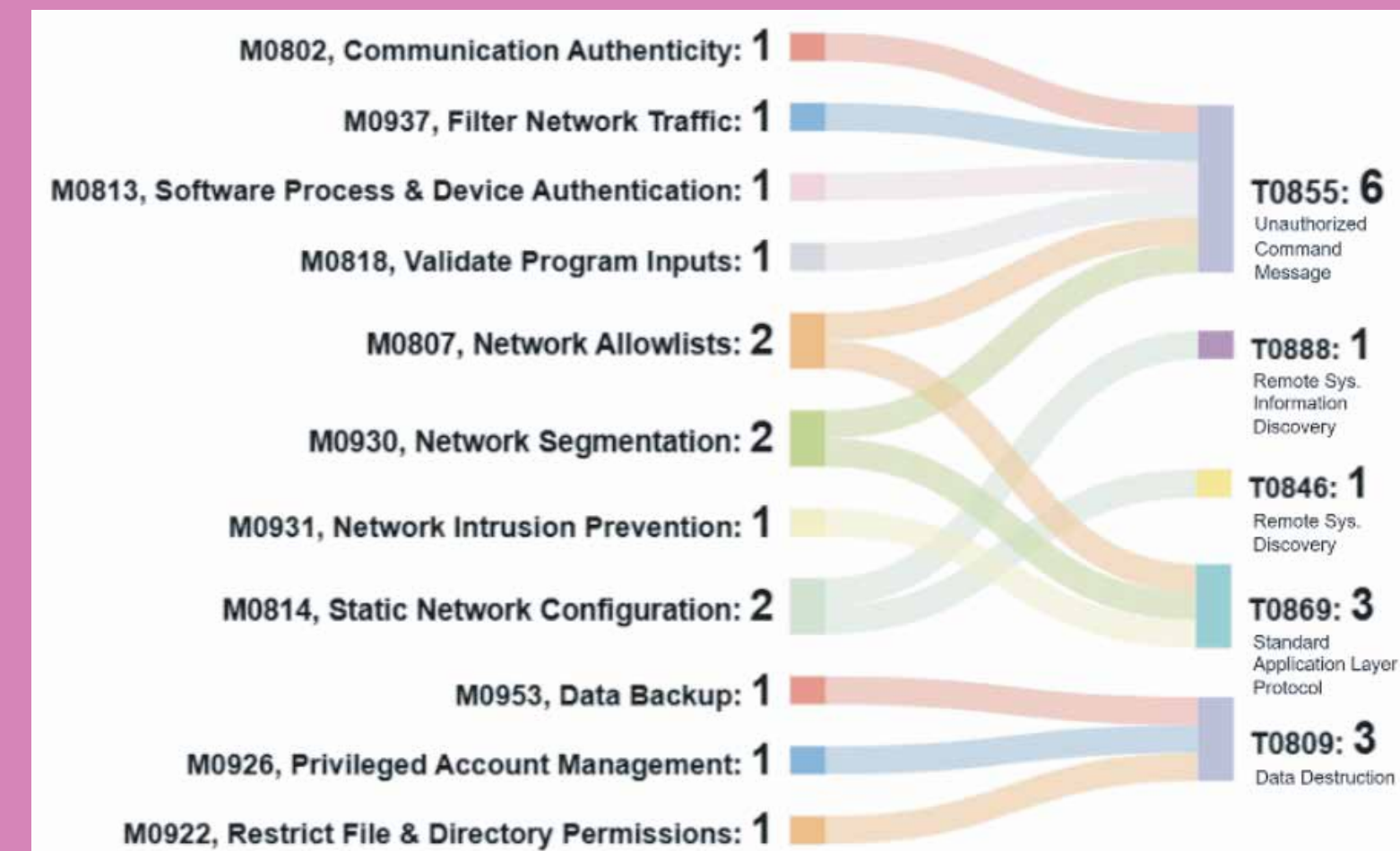
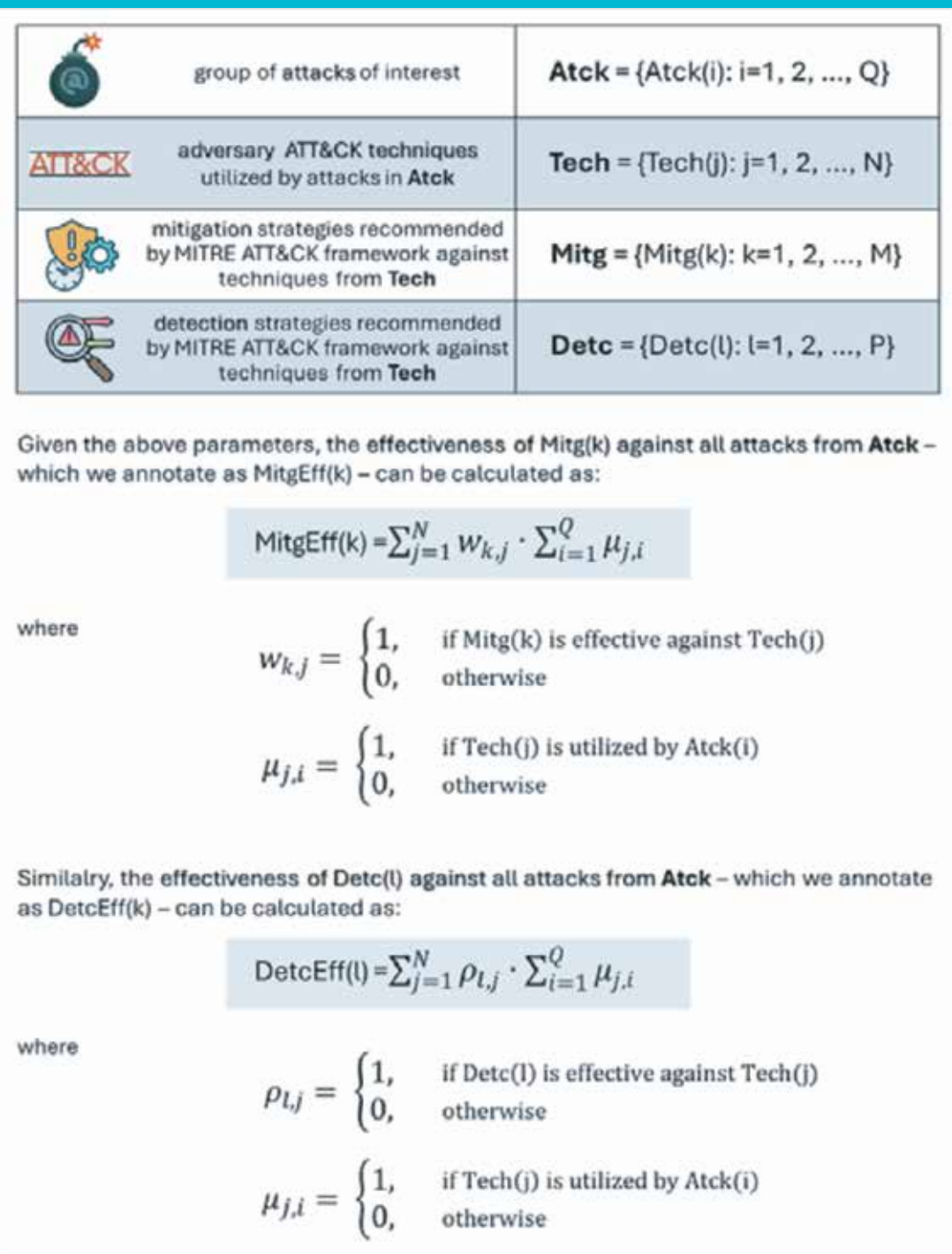


Figure 5. **Mitigation** techniques mapped to top 5 adversary techniques in **High-Impact ICS malware**

MITRE ATT&CK Mitigation Technique	Effectiveness Score
M0807, Network Allowlists	10
M0930, Network Segmentation	10
M0814, Static Network Configuration	9
M0937, Filter Network Traffic	6
M0802, Communication Authenticity	6
M0813, Software Process & Device Authentication	6
M0818, Validate Program Inputs	6
M0931, Network Intrusion Prevention	4
M0953, Data Backup	4
M0926, Privileged Account Management	4
M0922, Restrict File & Directory Permissions	4

Table V. **Mitigation** strategies and their effectiveness scores against **High-Impact ICS malware**

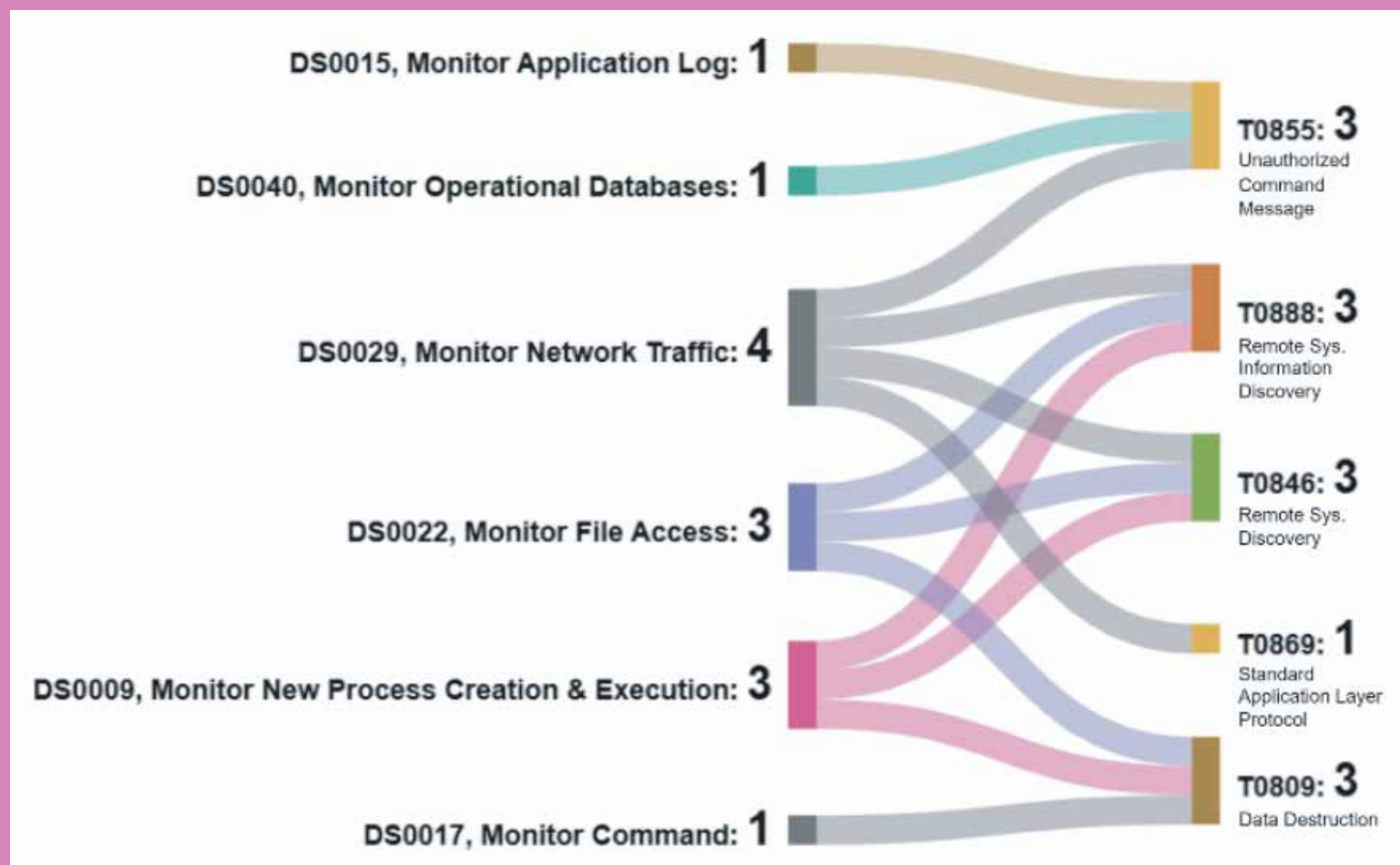


Figure 6. **Detection** techniques mapped to top 5 adversary techniques in **High-Impact ICS malware**

MITRE ATT&CK Detection Technique	Effectiveness Score
DS0029, Monitor Network Traffic	19
DS0022, Monitor File Access	13
DS0009, Monitor New Process Creation & Execut.	13
DS0015, Monitor Application Log	6
DS0040, Monitor Operational Databases	6
DS0017, Monitor Command Execution	4

Table VI. **Detection** strategies and their effectiveness scores against **High-Impact ICS malware**

Summary of Research Findings

RQ1: Most Prevalent Adversary Techniques in Two Groups of ICS Malware

Using MITRE Navigator and data from the MITRE ATT&CK repository, we created TTP-matrix representations for each ICS malware strain (Tables I & II). From these, we derived:

- A combined TTP matrix for 10 high-impact ICS malware strains (Figure 1).
- A combined TTP matrix for 6 ICS ransomware strains (Figure 2).

The **high-impact ICS malware strains** employ a wide range of techniques, though five key techniques are used by 40% or more of them (Table III).

ICS ransomware strains, in contrast, use fewer and different techniques (Table IV). Most cause Loss of Productivity and Revenue, aligning with ransomware's financial motives. Meanwhile, high-impact ICS malware has a broader and more severe impact, including Loss of Safety and Manipulation of Control.

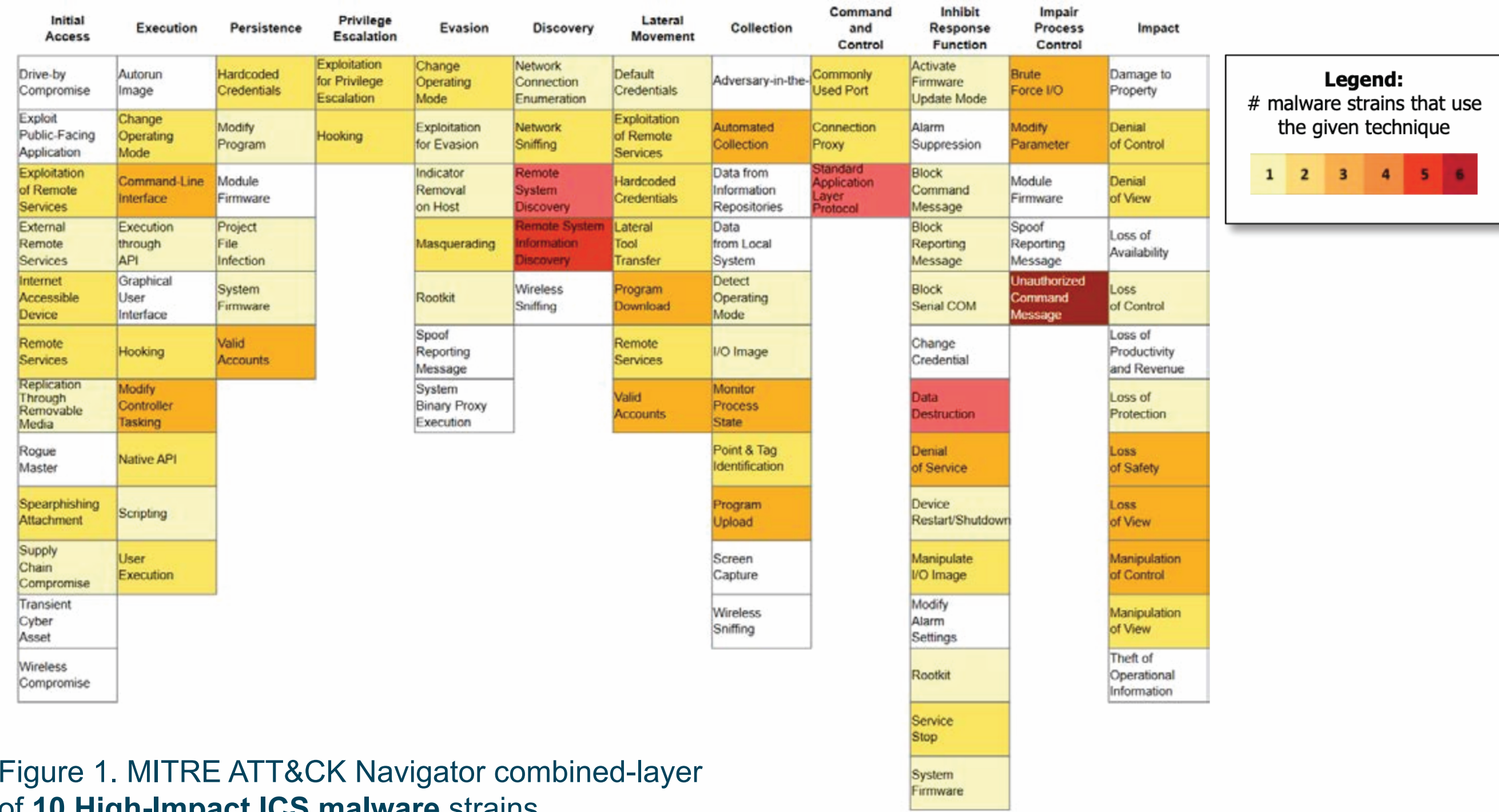


Figure 1. MITRE ATT&CK Navigator combined-layer of 10 High-Impact ICS malware strains

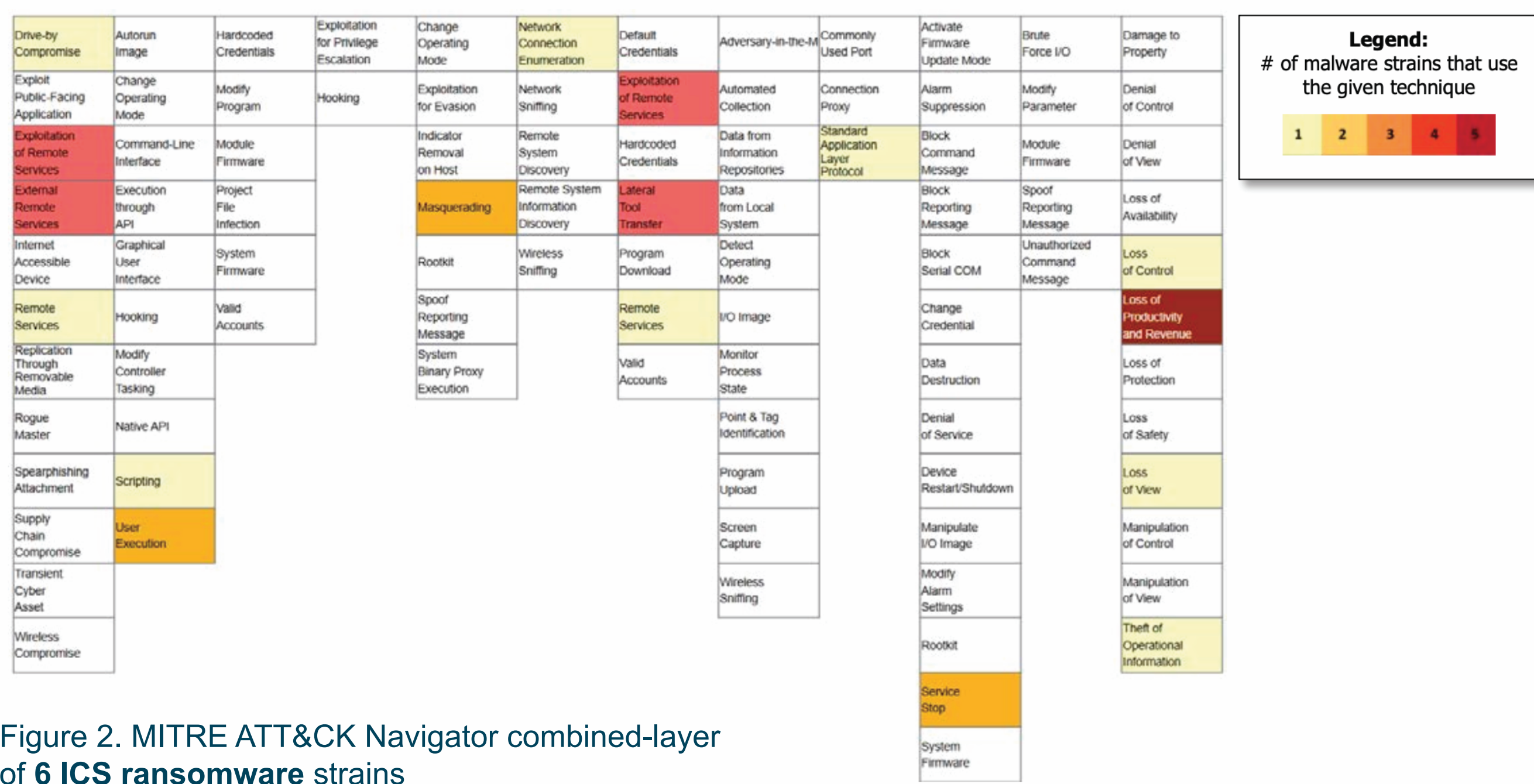


Figure 2. MITRE ATT&CK Navigator combined-layer of 6 ICS ransomware strains

Table III. Top 5 MITRE ATT&CK techniques most commonly deployed by **High-Impact ICS malware** strains

MITRE ATT&CK Technique	[%] of high-impact ICS malware strains deploying given technique
[T0855] Unauthorized Command Message	60% (6/10)
[T0888] Remote System Information Discovery	50% (5/10)
[T0846] Remote System Discovery	40% (4/10)
[T0869] Standard Application Layer Protocol	40% (4/10)
[T0809] Data Destruction	40% (4/10)

Table IV. Top 4 MITRE ATT&CK techniques most commonly deployed by **ICS ransomware** strains

MITRE ATT&CK Technique	[%] of ICS ransomware strains deploying given technique
[T0828] Loss of Productivity and Revenue	83.3% (5/6)
[T0866] Exploitation of Remote Services	50% (3/6)
[T0822] External Remote Services	50% (3/6)
[T0867] Lateral Tool Transfer	50% (3/6)

RQ2: Critical Mitigation and Detection Strategies Against High-Impact ICS Malware

After identifying the top 5 adversary techniques used by high-impact ICS malware (Table III), the next step was to determine the most effective mitigation strategies against these techniques. Using the our novel methodology, we followed these steps:

- Identify common adversary techniques (Table III).
- Identify relevant mitigation strategies from the MITRE ATT&CK framework.
- Map mitigation strategies to adversary techniques (Figure 4).
- Calculate effectiveness scores using our scoring formula (Figure 3).

The top strategies—Network Allowlisting, Network Segmentation, and Static Network Configuration—highlight the critical role of network-based defenses in protecting ICS environments.

We used the same process for detection strategies, and found Monitor Network Traffic to be the most effective (Table VI), again emphasizing the importance of network monitoring for detecting ICS threats.

RQ3: Critical Mitigation and Detection Strategies Against ICS Ransomware

Applying the same methodology to ICS ransomware strains (Table II), we identified and ranked effective MITRE ATT&CK mitigation and detection strategies (Tables VII & VIII).

For mitigation, Network Segmentation and Limit Access to Resources Over Network were among the most effective strategies, alongside Disable or Remove Feature or Program and Data Backup, which is particularly crucial for ransomware defense (Table VII).

For detection, Monitor Network Traffic was again the top strategy (Table VIII), reinforcing the importance of network monitoring in securing ICS/OT environments against both high-impact ICS malware and ICS ransomware.

MITRE ATT&CK Mitigation Technique	Effectiveness Score
M0930, Network Segmentation	6
M0935, Limit Access to Resource Over Network	6
M0842, Disable or Remove Feature or Program	6
M0953, Data Backup	5
M0948, Application Isolation and Sandboxing	3
M0950, Exploit Protection	3
M0826, Privileged Account Management	3
M0919, Threat Intelligence Program	3
M0851, Update Software	3
M0916, Vulnerability Scanning	3
M0936, Account Use Policies	3
M0932, Multi-Factor Authentication	3
M0927, Password Policies	3
M0918, User Account Management	3
M0931, Network Intrusion Prevention	3

Table VII. **Mitigation** strategies and their effectiveness scores against **ICS ransomware**

MITRE ATT&CK Detection Technique	Effectiveness Score
DS0029, Monitor Network Traffic	9
DS0015, Monitor Application Log	6
DS0028, Monitor Logon Session	3
DS0017, Monitor Command Execution	3
DS0022, Monitor File Creation	3
DS0033, Monitor Network Share Access	3
DS0009, Monitor Process Creation	3

Table VIII. **Detection** strategies and their effectiveness scores against **ICS ransomware**