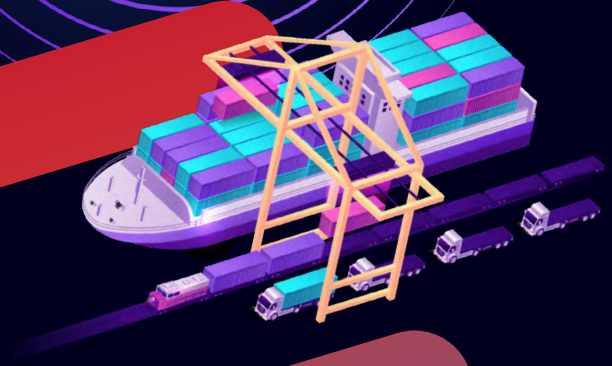
SCADAfence

White Paper

HACK THE PORT



MARITIME
& CONTROL SYSTEMS
CYBERSECURITY CON

April 2022

Hack The Port Introduction

Hack The Port 2022 is a competition sponsored by U.S. Cyber Command, the NSA, and the Maryland Innovation & Security Institute (MISI), that simulated a real-world attempt to compromise the security of a functional maritime port in the United States. The competition took place in Florida during March, 2022.

The competition organizers invited "red teams" to try to Hack The Port, that is, to seriously compromise the security of the technological infrastructure of the port, and "blue teams" to act as defenders. The competition included six scenarios, encompassing all aspects and possible risks of a real-world industrial port.

The red teams were allowed to use any means that real-world threat actors would employ in their attempt to breach the networks, including phishing, metasploit, DDOS attacks and others.

This whitepaper will outline the findings and the results of the exercise, and it details the success of SCADAfence in successfully defending the port against the attacks.

The Attack Scenarios

The Gantry Crane

An industrial port's gantry crane is a large overhead crane that sits astride the port and is used for loading and unloading containers on ships, and for installing engines and other heavy equipment used in ship building and repair. The cranes are controlled and operated via a computer with specialized software. This attack scenario invited red team participants to attempt a breach of the crane's control system and gain enough access to allow them to disrupt the crane's movement and to lower a ship's engine directly into the ocean.

The Water Filtration System

The water filtration system at a major port is responsible for providing clean water to shipboard personnel, and the entire port. The goal of this challenge was to sabotage the water filtration system by accessing the devices that control the machinery, and trick it into adding an incorrect ratio of additives into the water. A key part of this challenge was to prevent the system's detectors from discovering the changes.

The Ship Board Network

This scenario challenged red teams to access the bridge control systems of the actual vessels as they attempted to dock at the port and shut down the ship's propellers, thereby halting the ship and in effect, causing gridlock at the port.

The Ballast Control

This challenge also required accessing a ship's bridge control systems. In this scenario, red teams attempted to gain access to the ship's ballast control system and cause the HMIs to incorrectly indicate that the system is pumping water even though it is not.

The Surveillance System

Like any major industrial facility, Hack The Port's organizers included a surveillance system in their port, consisting of cameras which record digital footage to be saved for later review when needed. Red teams were challenged to shut down this network and to make sure no data was preserved that might implicate the threat actors later.

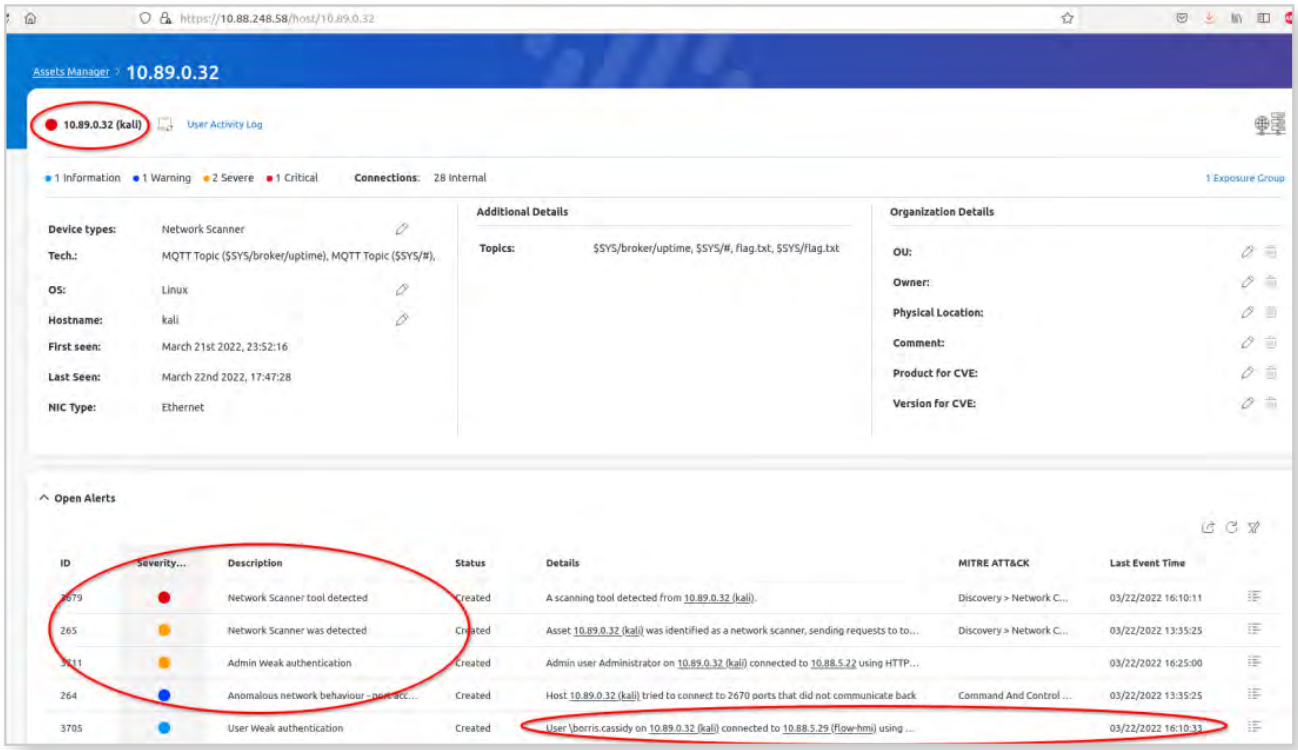
The Access Control System

Secure ID cards issued to each worker at a port is a critical aspect of maritime security. Ensuring that each person has the exact level of access to restricted areas helps keep the area secure. This challenge required red teams to gain access to the gate control systems and to card readers, and to allow unauthorized entry into the port.

The Red-Teams' Attacks - Detected by SCADAfence

Scanning the Network

As expected, the red teams began each scenario with reconnaissance of the network.[1] This begins with a scan to gather information in order to obtain the following: An inventory of devices attached to the network, services that run on those devices, device types, IP addresses, open ports, the manufacturer names, and what OS software the devices were running. They then used this information to correlate those devices with known vulnerabilities, and continued looking for anything else they could find, in order to gain further network access.



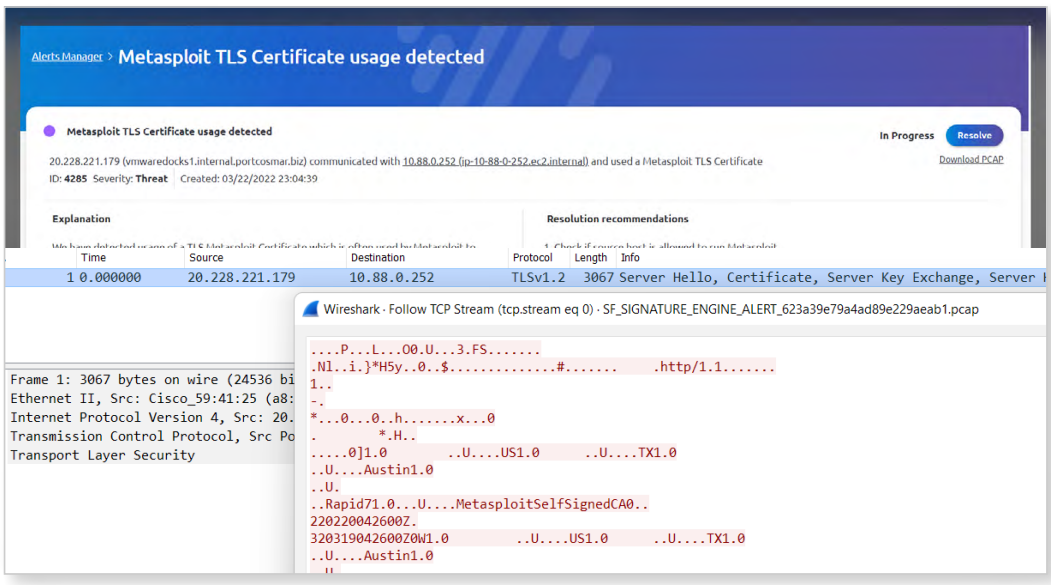
Host view10.89.0.32 scanning the network

[1] Reconnaissance is the first step of the kill-chain:
- https://collaborate.mitre.org/attackics/index.php/Discovery
- https://attack.mitre.org/tactics/TA0043/
- https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

SCADAfence

Metasploit Certificate Usage

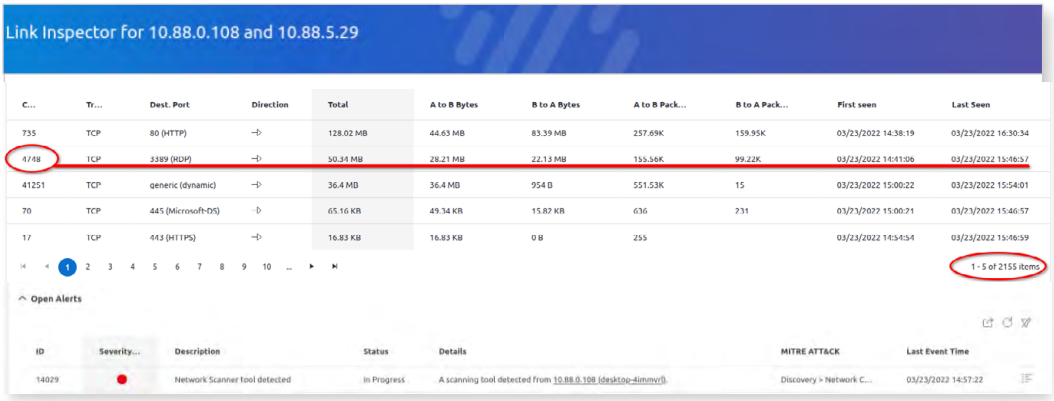
During a routine scan, one of the first things the SCADAfence Platform detected was a self-signed Metasploit certificate. A certificate signed by the Metasploit Framework, instead of a certificate signed by a trusted company such as DigiCert or GoDaddy. This indicates unauthorized or malicious activity being sent through the network. Specifically, it was issued by a router with an IP address of[c][d] 10.88.0.252 (NAT).



Detecting a Metasploit Certificate Usage. Every alert includes the PCAP file to help further investigate the issue.

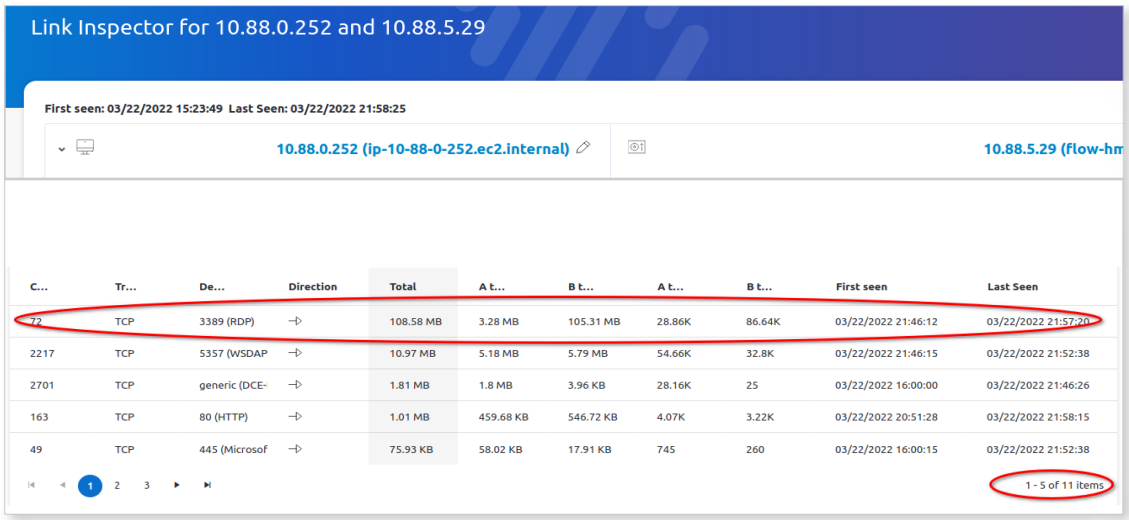
Attempted Attack Via RDP (Remote Desktop Protocol)

The SCADAfence Platform detected that attackers tried over 4,700 times to establish a connection with the FLOW-HMI machine. They were eventually able to create a successful RDP session.



An alert showing a successful RDP connection to the FLOW-HMI

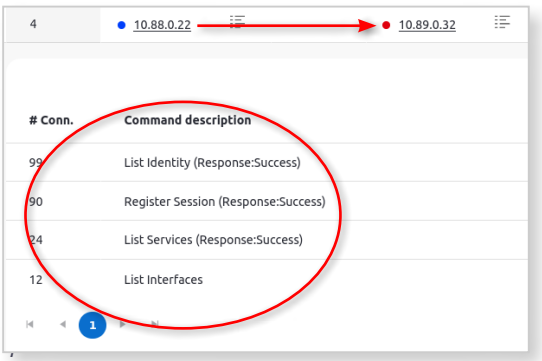
Several other successful RDP sessions on 10.88.5.29 from known malicious actors (10.88.0.252, 10.88.0.106) that happened on the same day, were not preceded by targeted scans or bruteforce login attempts, and were therefore not reported.

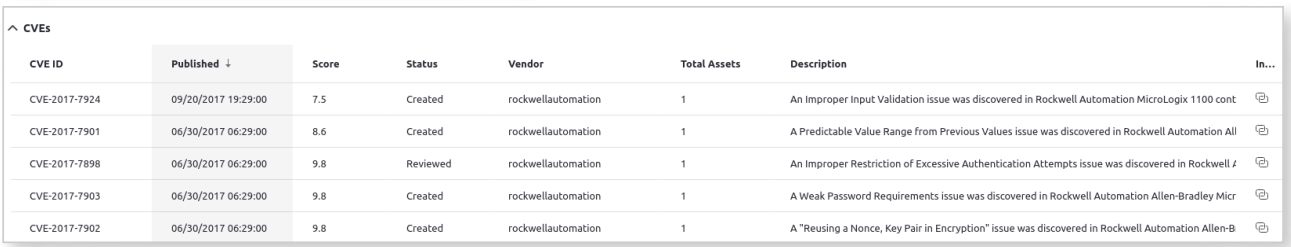


Link inspector showing a successful RDP connection to the FLOW-HMI

Successful PLC Scan Using Allen-Bradley ENIP

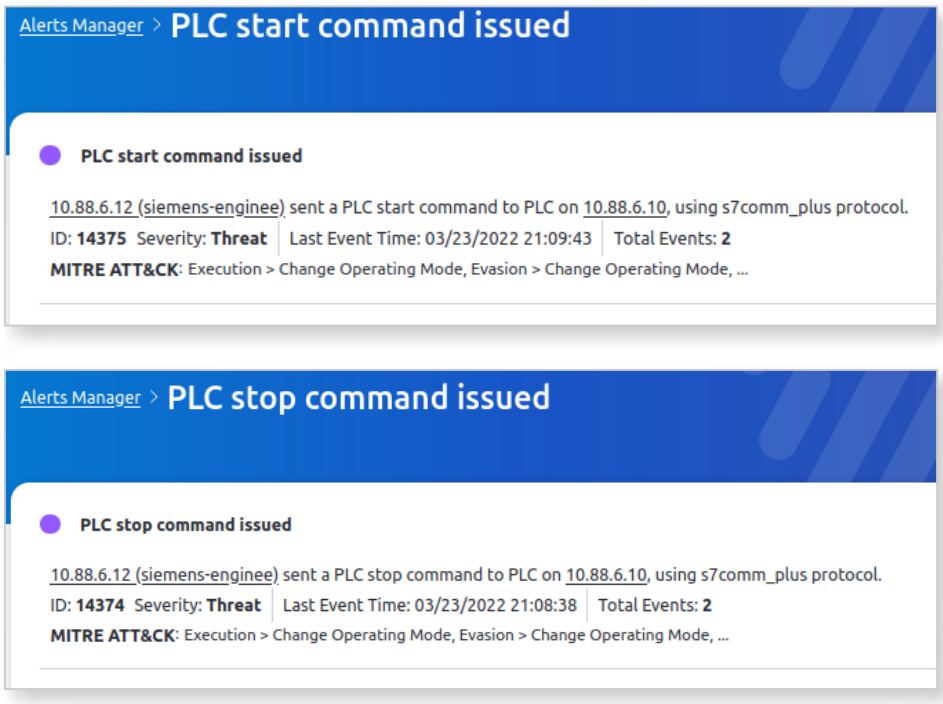
In another attempted attack, The SCADAfence Platform, caught red team attackers attempting to use Allen-Bradley's ENIP protocol to retrieve details from a PLC. The SCADAfence Platform was able to detect that the attackers successfully acquired details such as the identity of a device, the model name, the session details and additional information from the PLC.





Starting and Stopping a PLC

One of the most significant attacks the SCADAfence Platform was able to detect was an actual start/stop commands sent to a PLC. After gaining access to the PLC, the threat actors maintained their attack on the compromised device sending commands to change the device's operating mode.
Had this been a real-world attack, the threat actors could have used PLC start/stop commands to launch attacks with potentially lethal consequences.



Engineering station 10.88.6.12 sent a PLC stop & start commands to PLC 10.88.6.10

SCADAfence

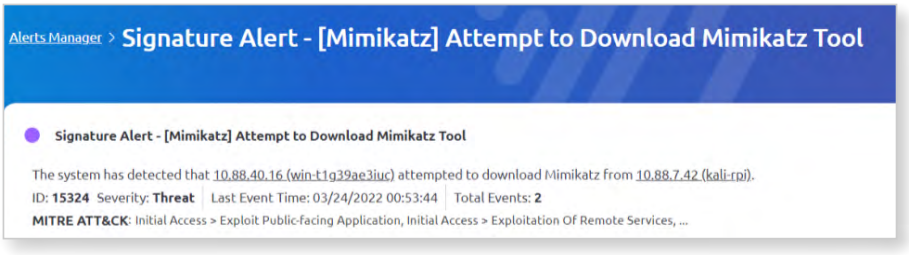
Downloading Mimikatz on a Compromised Domain Controller

One important way threat actors launch significant attacks is by first gaining a foothold in a network, then using that entry point to penetrate further into the network where they can work undetected. The SCADAfence Platform detected one of the most significant attacks of the Hack the Port event using this technique.

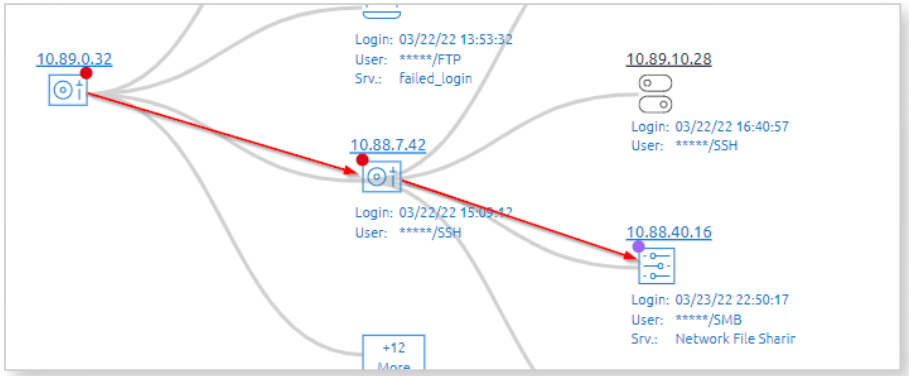
The Red Team attackers initial breach was a successful brute-force attack which they used as a launching point, and then, using compromised SSH access they continued through an intermediary device to then access a domain controller.

From that point, the attackers attempted to download Mimikatz onto a compromised domain controller in order to steal passwords (hashes) and other sensitive information. The SCADAfence Platform was able to detect the download.

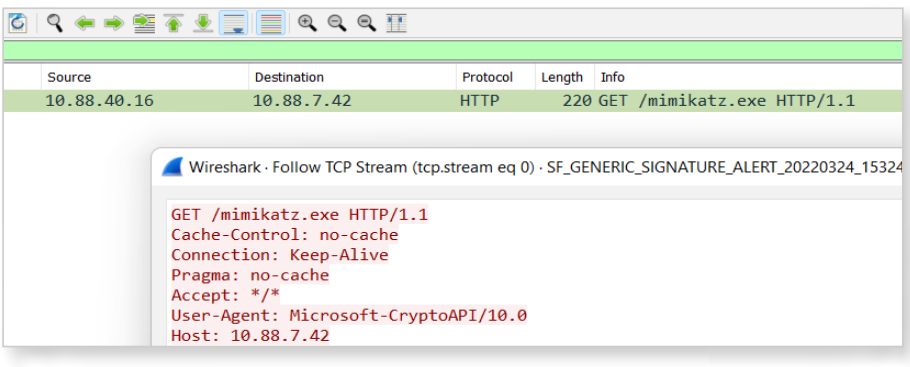
In a real world scenario the attackers would have been able to use the information they gathered to compromise other devices on the network.



Detecting the attempt to download the Mimikatz tool



Mapping the attacker's path to the domain controller



Attached Pcap showing http download of Mimikatz executable

SCADAfence

Connecting to the TIA Portal

Among the most important devices that control the workings of an industrial port, (or any other computer controlled manufacturing or production environment) are the HMI's and operator / engineering stations.

Gaining access to these and the PLCs by which they are controlled, is among the top prizes for a threat actor. During the Hack the Port event, the SCADAfence Platform detected an external connection to port 8888. Port 8888 is used for the integrated configuration web application of Siemens TIA Administrator (TIA Portal).

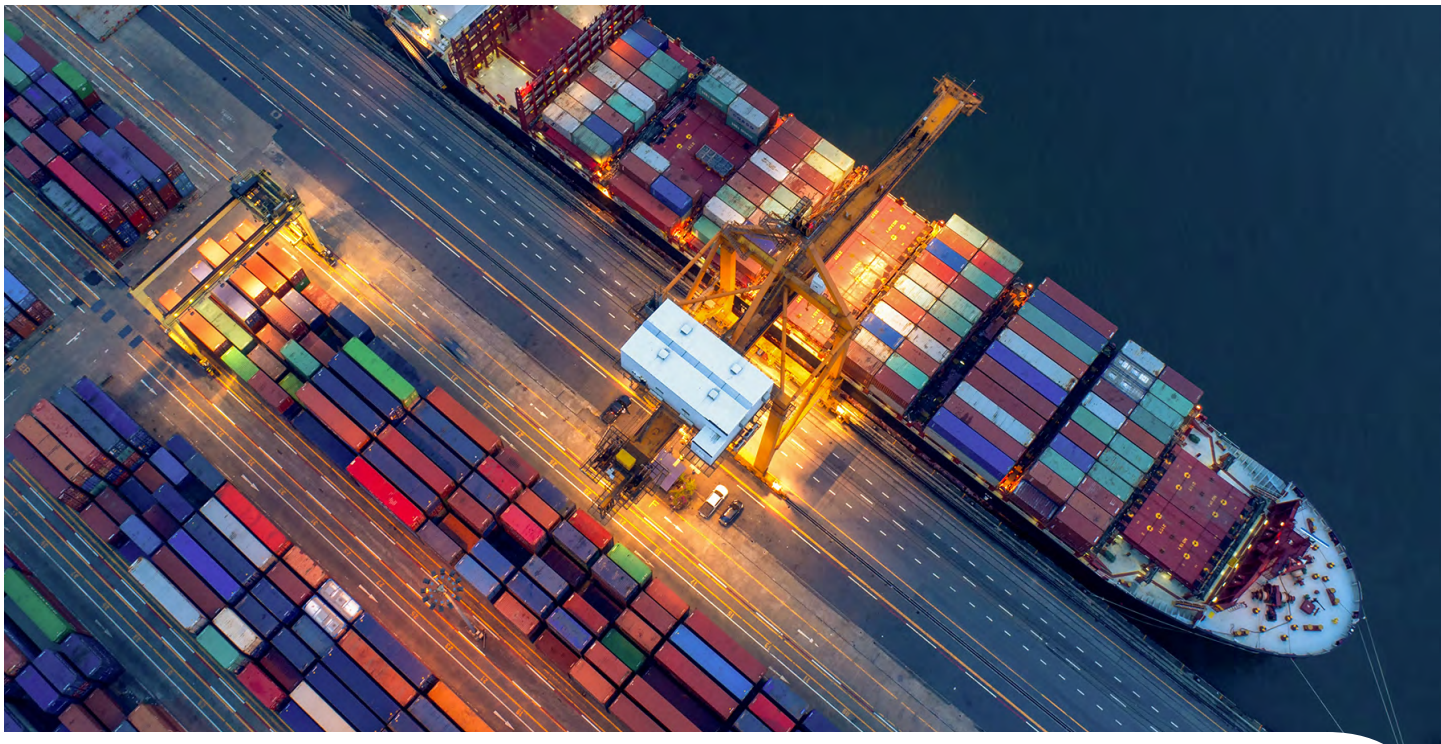
This indicated that the threat actors were attempting to gain access to the PLC. Again, the two-way communication detected by the Platform, indicated that they had successfully established this connection and the PLC was compromised.

In a real-world breach of this nature, threat actors could use this access to reprogram the PLC and to have full control of the PLC.

Link Inspector for 10.88.0.108 and 10.88.5.29

Conve...	Trans...	Dest. Port	Direction	Total ↓	A to B Bytes	B to A Bytes	A to B Packets	B to A Packets	First seen
1314	TCP	3389 (RDP)	→	4.89 GB	334.05 MB	4.56 GB	2.84M	4.37M	03/23/2022 18:18:16
4973	TCP	8888 (DDI-TCP-1)	→	1.43 GB	206.33 MB	1.22 GB	993.92K	1.13M	03/22/2022 13:51:25

A connection is established to TCP port 8888, which is one of TIA Portal ports, advised by Siemens to be restricted for local user access

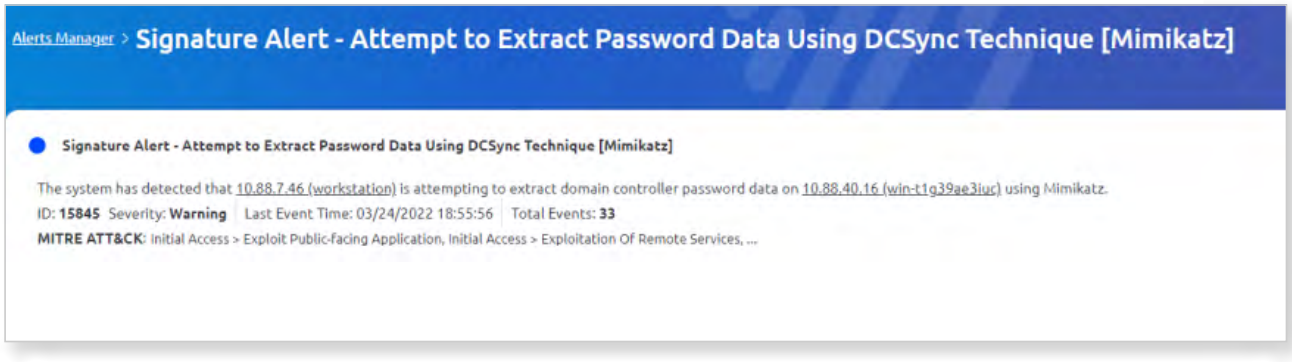


DCSync Attack

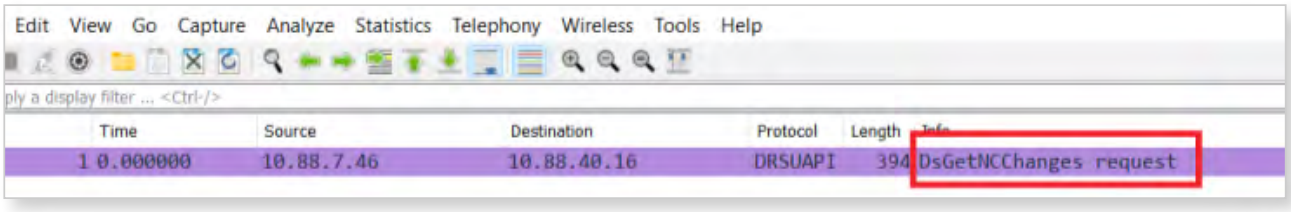
Hack the Port included a number of Raspberry PI devices with notable vulnerabilities. Most red teams were able to gain a foothold into the Raspberry PI network and use it as a jump point to gain deeper access into the network, by using one or more intermediary devices.

In this case, the Raspberry PI network was compromised in order to launch a DCSync attack against a domain controller.

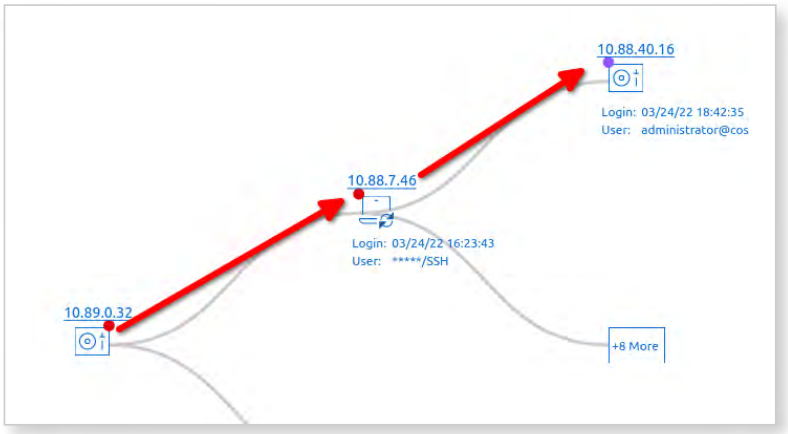
The attacker first compromised the Raspberry PI and used that as a jump point to access an HMI via SSH, before finally attacking the domain controller. The attackers used their control to extract information from the domain controller using the SMB protocol.



An alert showing the DCSync attack



The attached PCAP shows the DCSync attack



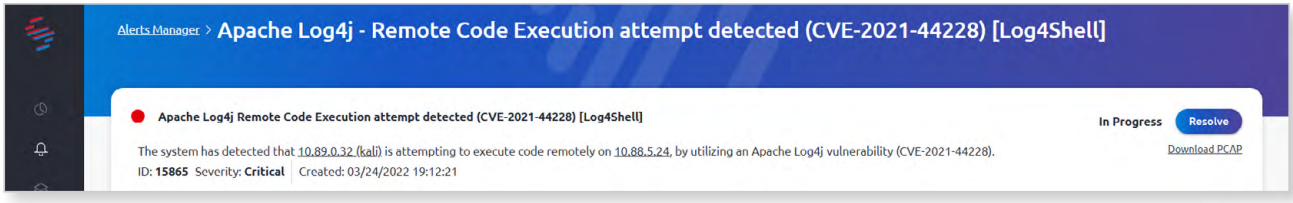
The attacker's path to the domain controller

SCADAfence

Log4J Strikes Back

A major vulnerability was identified in open source logging library Apache Log4J at the end of 2021. SCADAfence added support for the Log4J vulnerability immediately after the attack was discovered. At Hack The Port, the red team used this known vulnerability to stage an attack, hoping that it wouldn't be discovered.

The target of this attack was an IO-link ENIP adapter, AL1970. The SCADAfence Platform immediately detected the attempt to use the Log4J vulnerability in order to execute code remotely on the device.



An alert showing the Log4J attack

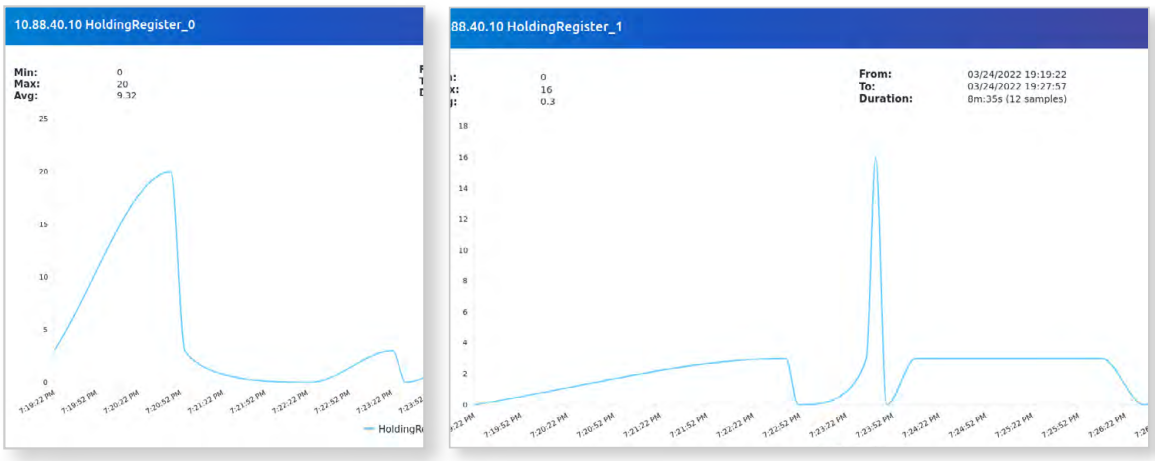
The attached PCAP showing IP 192.168.0.32 is attacking 10.88.5.24 using the Log4j / Log4Shell vulnerability

SCADAfence

Value Analysis Changes from A Compromised Domain Controller

One of the most vital features of the SCADAfence Platform, the value Level feature, goes beyond basic OT command level detection, and retrieves actual OT variable values that were sent to the PLC.

During the Hack the Port event, the SCADAfence Platform detected value level changes that originated in a compromised domain controller. Unexpected changes in values indicate a breach, and in a real world scenario can indicate a major attack. In this case, the attacker changed the values in the PLC via the Modbus protocol, to a significantly higher value in order to disrupt both the PLC and connected machinery/sensors. The attacker's intent was to cause damage by having harmful additives dumped into the water supply.



The SCADAfence Platform Value detects changes on a PLC, done from a compromised domain controller via the Modbus protocol.

Conv...	Source IP	Src Hostname	Dest. IP	Dest Hostn...	Protocol
2	10.88.40.16	win-t1g39ae3iuc	10.88.40.10		Modbus/TCP

# Conn.	Command description	Last Seen
11	Request: Function 0x3: Read Holding Registers	03/24/2022 19:27:44
44	Request: Function 0x10: Write Multiple Registers	03/24/2022 19:28:27

1 - 2 of 2 items

Conv...	Source IP	Src Hostname	Dest. IP	Dest Hostn...	Protocol
2	10.88.40.10		10.88.40.16	win-t1g39ae3iuc	Modbus/TCP

# Conn.	Command description	Last Seen
11	Response: Function 0x3: Read Holding Registers	03/24/2022 19:27:44
44	Response: Function 0x10: Write Multiple Registers	03/24/2022 19:28:27

An alert showing the value level changes on the PLC

SCADAfence

Detecting All New Red Team Scenarios

As one of the red teams completed working on the attack scenario, another red team took it in turn. The SCADAfence Platform was able to detect the change due to new IP addresses being added to the network. The same IP address being used by a new device potentially indicated that a device that was using the IP has left the scene and a new device entered, taking the same IP and thus triggering a corresponding event.

Scenario changes were detected via IP/MAC correlation

SCADAfence

Conclusion: The SCADAfence Platform Demonstrates Its Superiority

The SCADAfence Platform succeeded in detecting the widest variety of attempted red team attacks against the fictional port. From untrusted x.509 certificates and DCSync attacks to unauthorized PLC start/stop commands and others, the SCADAfence Platform generated alerts to breaches on their network, without a large number of distracting false positives.

> *the SCADAfence blue team provided the most comprehensive reporting details for the entire blue team channel, with the fewest false positives.*

the.storyteller 03/29/2022
first of all please make sure your whole team knows you provided the most comprehensive reporting details for the entire BLUE team channel

The SCADAfence team is congratulated by the Hack The Port event organizers

In real world scenarios, the SCADAfence Platform's ability to detect cyber security breaches and generate accurate alerts would have protected the port from experiencing a major security incident, as it does today with many industrial ports around the world.

This case study is a perfect example.

SCADAfence

About SCADAfence

SCADAfence is the global technology leader in OT cyber security. The solution enables organizations with large-scale OT networks to embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. The non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and user experience. The SCADAfence solution seamlessly integrates OT security within existing security operations, bridging the IT/OT convergence gap. SCADAfence delivers security and visibility to some of the world's most complex OT networks, including the largest manufacturing facility in Europe. SCADAfence enables organizations in manufacturing, building management and in critical infrastructure industries to operate securely, reliably and efficiently as they go through the digital transformation journey. To learn more go to www.scadafence.com

Our offices
Headquarters: Tel Aviv
Regional: New York, Munich, Tokyo

Contact us: info@scadafence.com
www.scadafence.com

SCADAfence