Showing Off Their SCILz: Sandworm Disrupts Power in Ukraine Using Novel Attack Against OT

Daniel Kapellmann Zafra
Information Operations (IO)
Team Lead and Cyber-Physical
SME (OT/ICS)

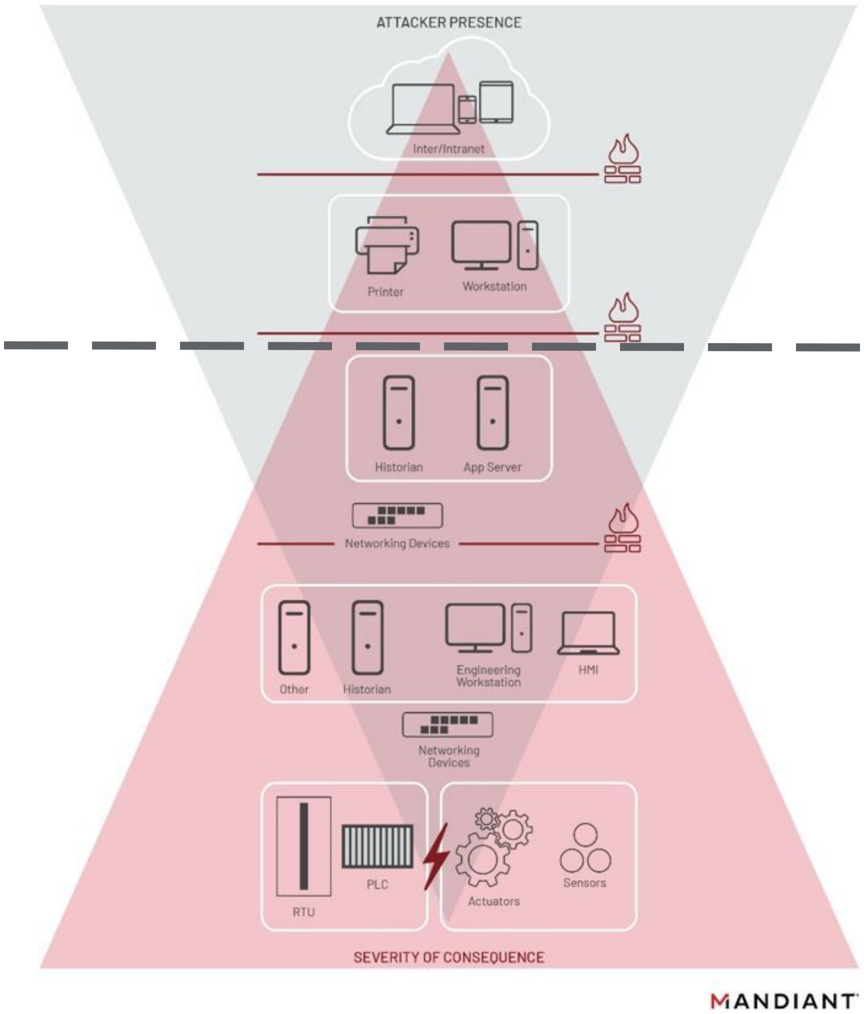
kapellmann@google.com
www.kapell.tech

March 2024

Daniel Kapellmann Zafra

Security Engineering Manager, Google Mandiant
Cyber Physical and Information Operations
@Kapellmann, www.kapell.tech

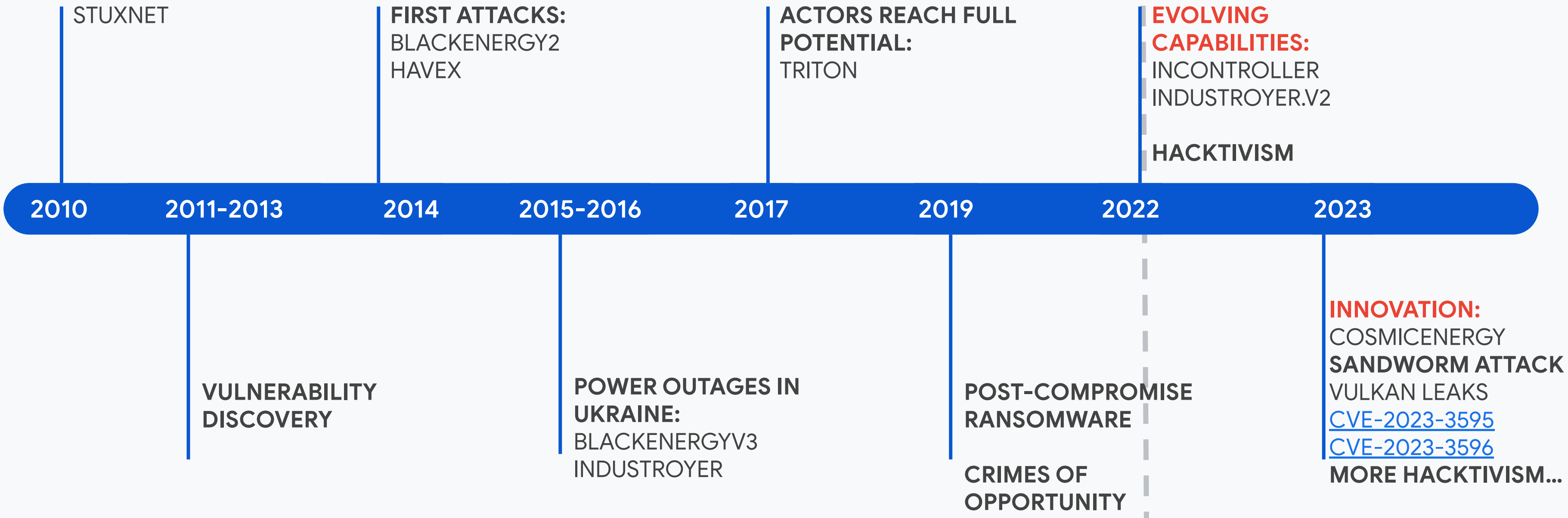
Photo by Pixabay



Information Technology

Operational Technology

Evolution of Threats to OT



2010

STUXNET

2011-2013

VULNERABILITY DISCOVERY

2014

FIRST ATTACKS:
BLACKENERGY2
HAVEX

2015-2016

POWER OUTAGES IN UKRAINE:
BLACKENERGYV3
INDUSTROYER

2017

ACTORS REACH FULL POTENTIAL:
TRITON

2019

POST-COMPROMISE RANSOMWARE

CRIMES OF OPPORTUNITY

2022

EVOLVING CAPABILITIES:
INCONTROLLER
INDUSTROYER.V2

HACKTIVISM

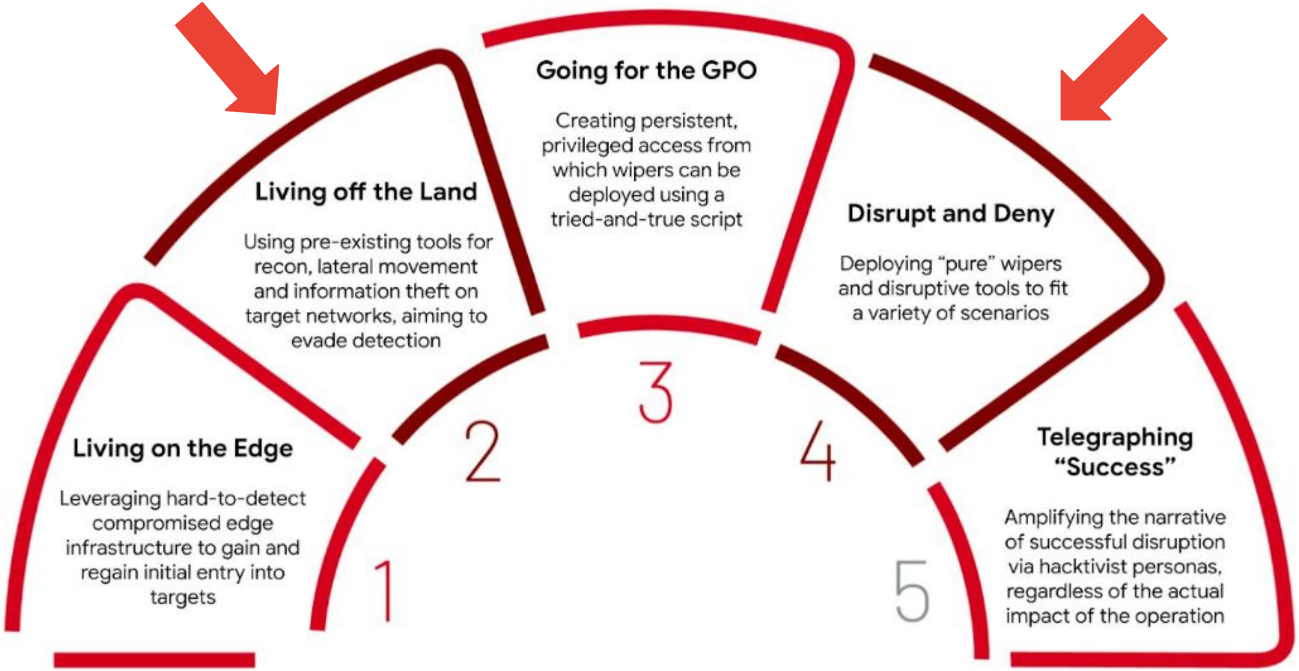
2023

INNOVATION:
COSMICENERGY
SANDWORM ATTACK
VULKAN LEAKS
CVE-2023-3595
CVE-2023-3596
MORE HACKTIVISM...

Sandworm Team... Again

Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology

Sandworm’s Disruptive Playbook



Living on the Edge

Leveraging hard-to-detect compromised edge infrastructure to gain and regain initial entry into targets

Living off the Land

Using pre-existing tools for recon, lateral movement and information theft on target networks, aiming to evade detection

Going for the GPO

Creating persistent, privileged access from which wipers can be deployed using a tried-and-true script

Disrupt and Deny

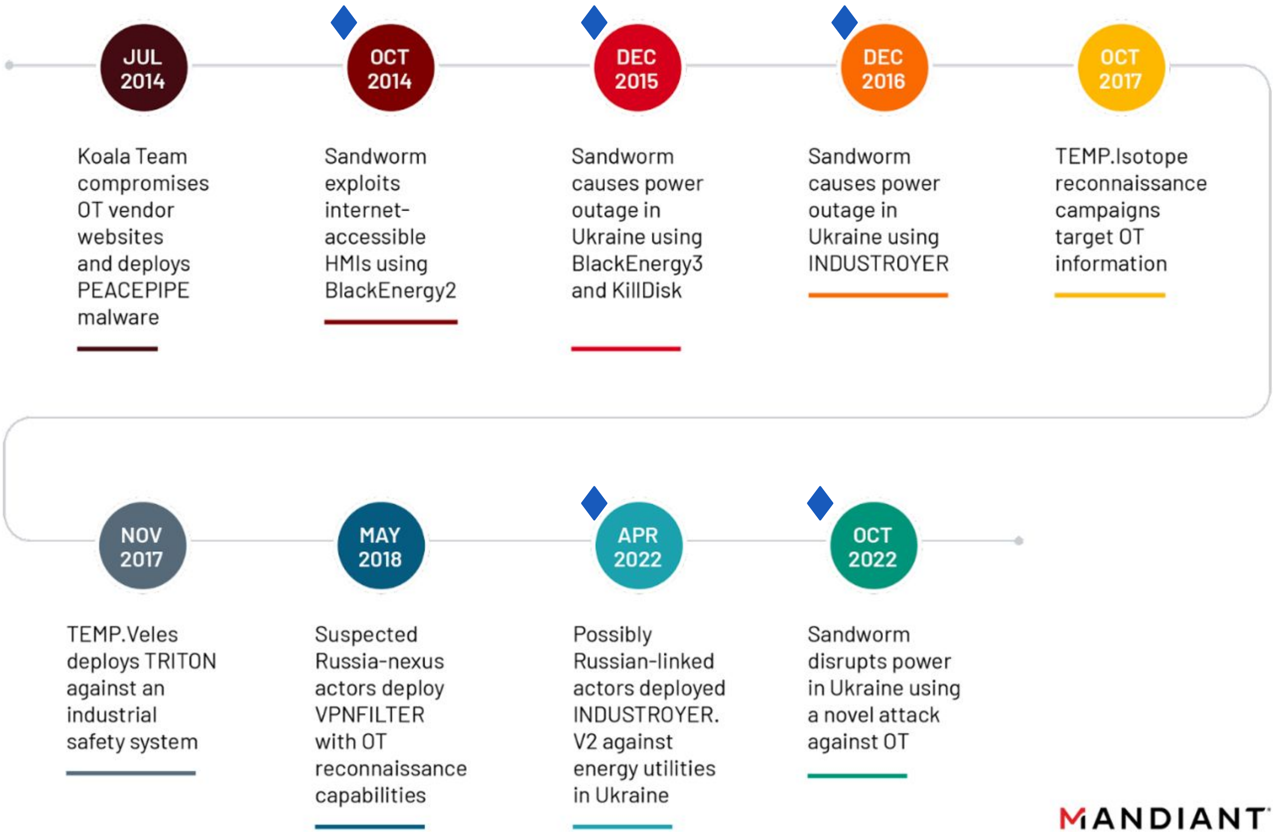
Deploying “pure” wipers and disruptive tools to fit a variety of scenarios

Telegraphing “Success”

Amplifying the narrative of successful disruption via hacktivist personas, regardless of the actual impact of the operation

MANDIANT

2014 — 2022 HISTORICAL RUSSIA-NEXUS ACTIVITY IMPACTING OT



JUL 2014
Koala Team compromises OT vendor websites and deploys PEACEPIPE malware

OCT 2014
Sandworm exploits internet-accessible HMIs using BlackEnergy2

DEC 2015
Sandworm causes power outage in Ukraine using BlackEnergy3 and KillDisk

DEC 2016
Sandworm causes power outage in Ukraine using INDUSTROYER

OCT 2017
TEMP.Isotope reconnaissance campaigns target OT information

NOV 2017
TEMP.Veles deploys TRITON against an industrial safety system

MAY 2018
Suspected Russia-nexus actors deploy VPNFILTER with OT reconnaissance capabilities

APR 2022
Possibly Russian-linked actors deployed INDUSTROYER. V2 against energy utilities in Ukraine

OCT 2022
Sandworm disrupts power in Ukraine using a novel attack against OT

Disrupted Power in Ukraine... Again

Photo by Jack Finnigan on Unsplash

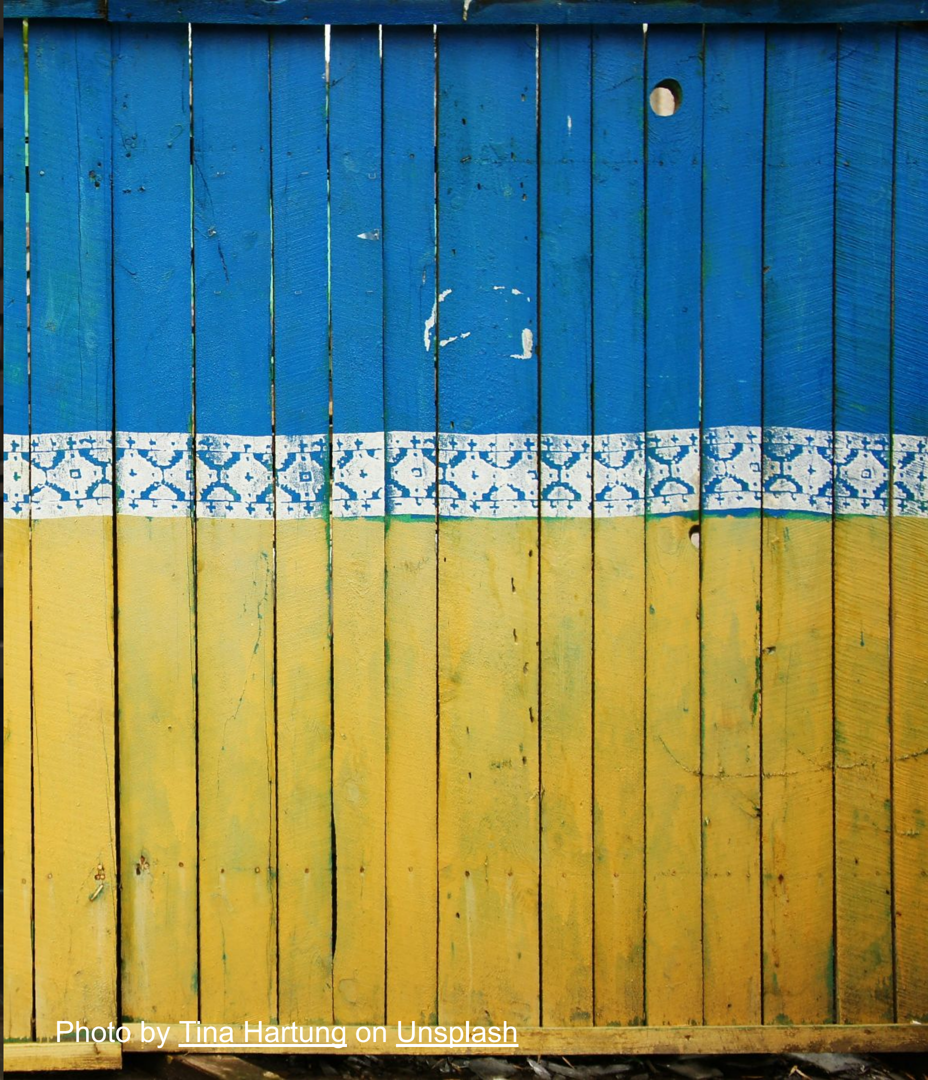


Photo by Tina Hartung on Unsplash

Sandworm’s Novel Attack Against OT

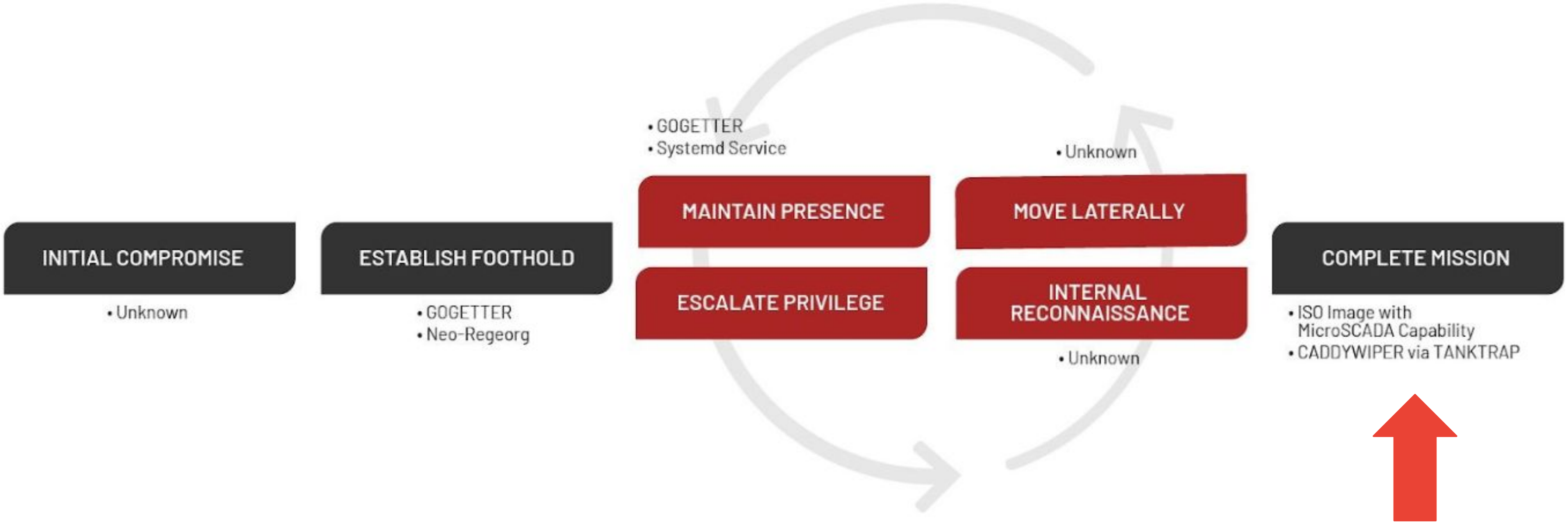
- Multi-event cyber attack impacted OT
- OT-level living-off-the-land (LotL) to trip substation circuit breakers
- Caused power outage coinciding with missile strikes on critical infrastructure
- Visibly growing maturity of Russia’s offensive OT arsenal

Photo by Rodion Kutsaiev on Unsplash

Attack Lifecycle

June-July 2022

October 2022



INITIAL COMPROMISE
- Unknown

ESTABLISH FOOTHOLD
- GOGETTER
- Neo-Regeorg

MAINTAIN PRESENCE
- GOGETTER
- Systemd Service

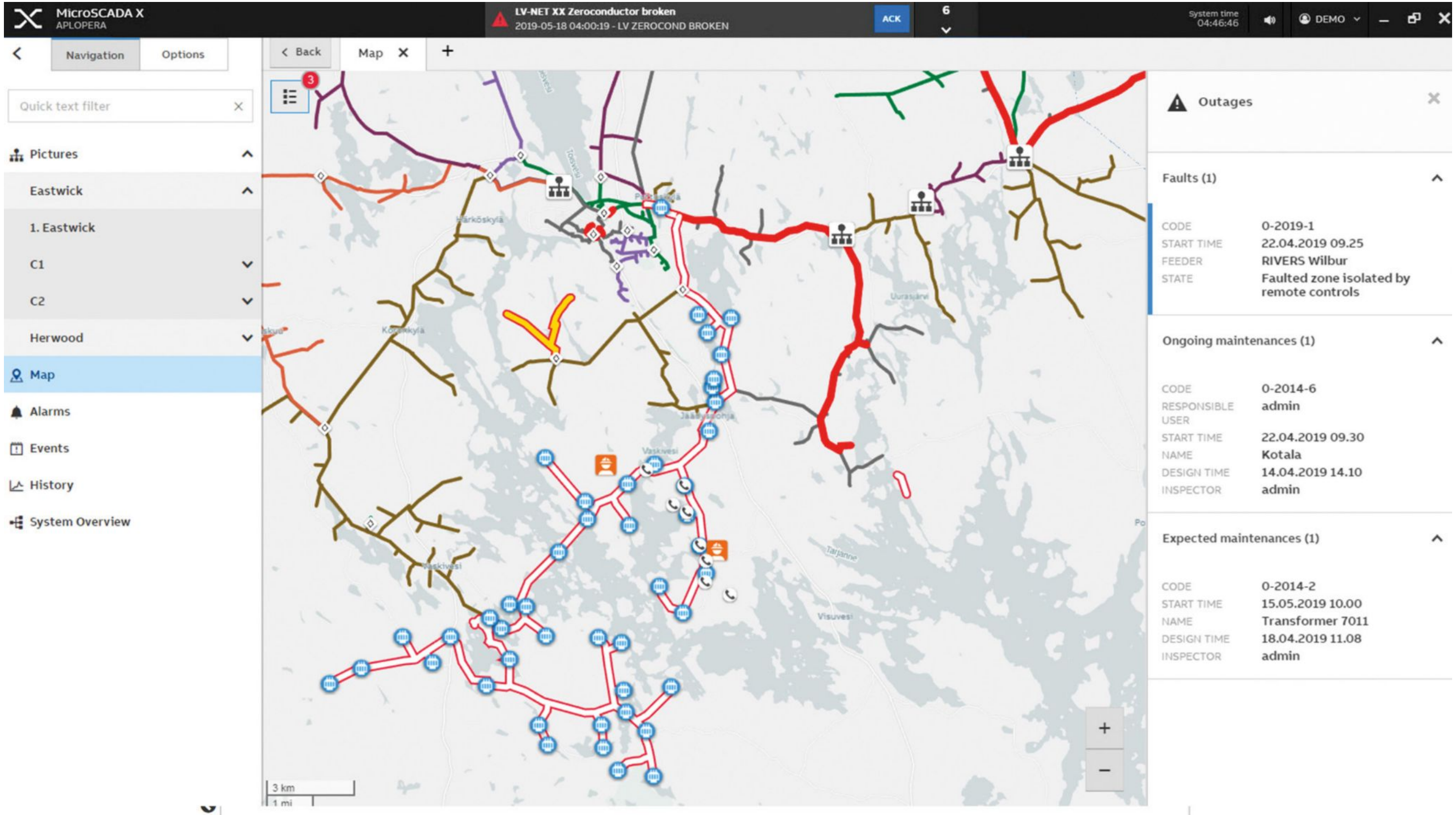
ESCALATE PRIVILEGE

MOVE LATERALLY
- Unknown

INTERNAL RECONNAISSANCE
- Unknown

COMPLETE MISSION
- ISO Image with MicroSCADA Capability
- CADDYWIPER via TANKTRAP

MicroSCADA



LV-NET XX Zeroconductor broken
2019-05-18 04:00:19 - LV ZEROCOND BROKEN

Outages

Faults (1)

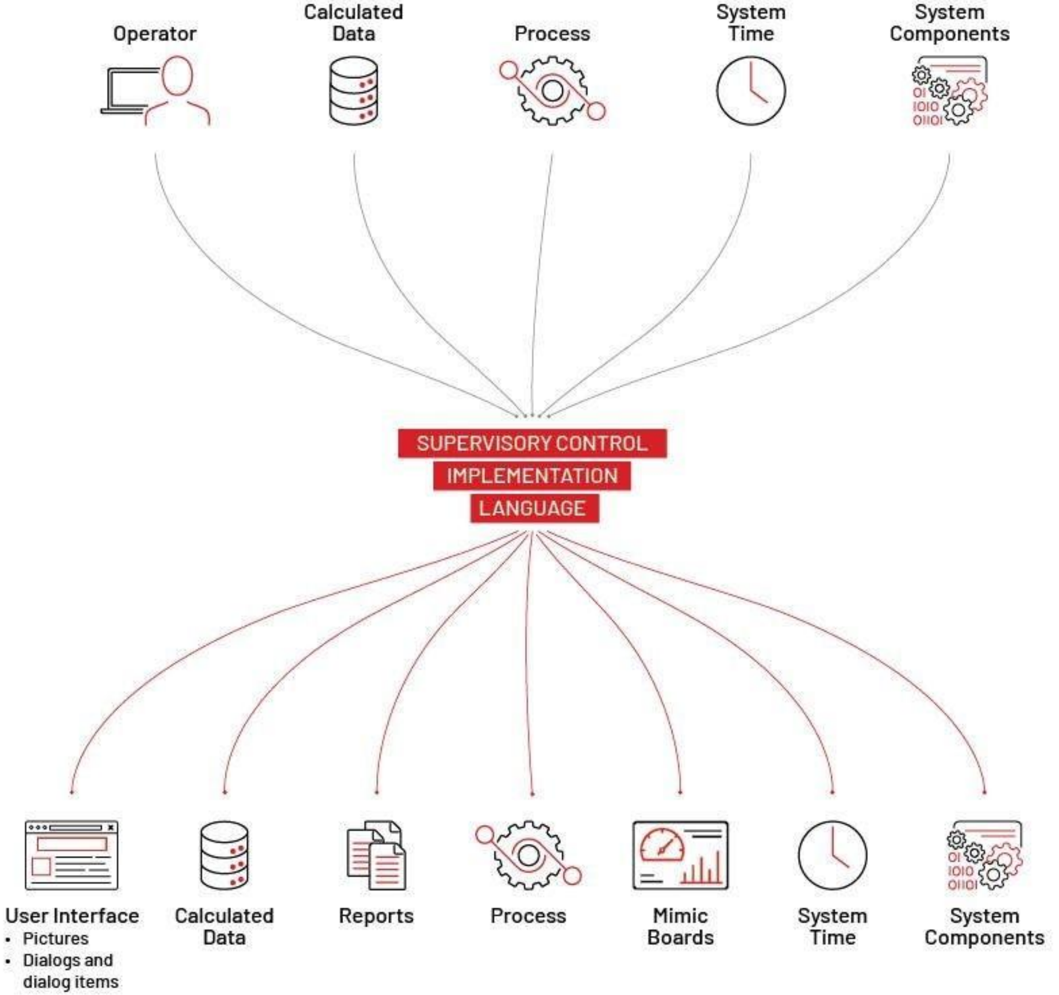
CODE	0-2019-1
START TIME	22.04.2019 09.25
FEEDER	RIVERS Wilbur
STATE	Faulted zone isolated by remote controls

Ongoing maintenances (1)

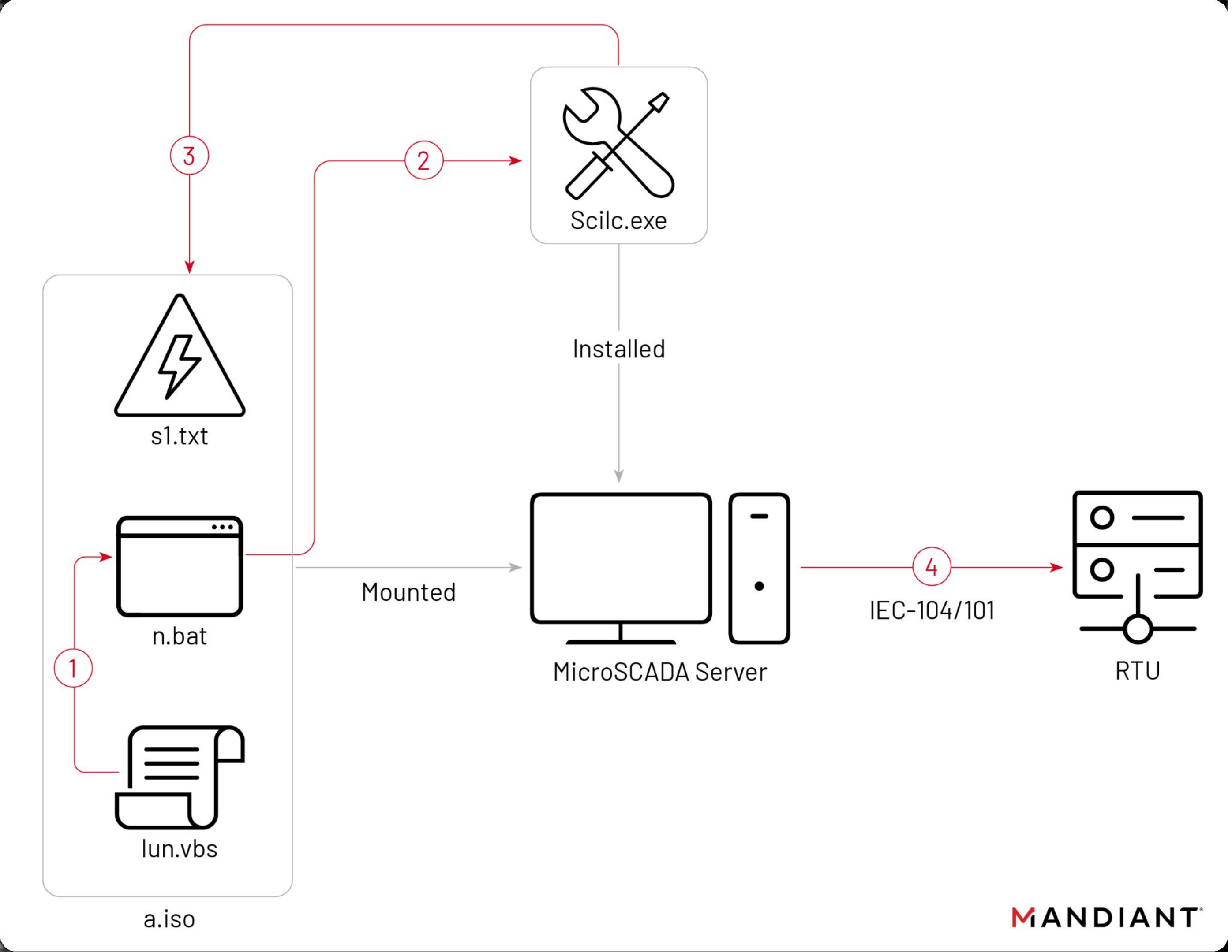
CODE	0-2014-6
RESPONSIBLE USER	admin
START TIME	22.04.2019 09.30
NAME	Kotala
DESIGN TIME	14.04.2019 14.10
INSPECTOR	admin

Expected maintenances (1)

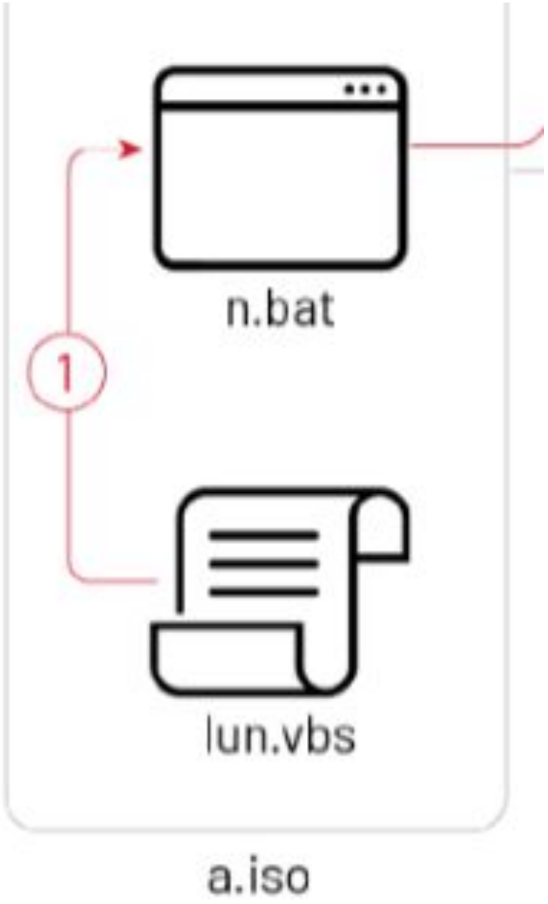
CODE	0-2014-2
START TIME	15.05.2019 10.00
NAME	Transformer 7011
DESIGN TIME	18.04.2019 11.08
INSPECTOR	admin



Supervisory Control Implementation Language (SCIL)



Used ISO image to execute scilc.exe within End-of-Life MicroSCADA to switch off substations



‘A.iso was used as a virtual CD-ROM on the hypervisor where the victim’s substation MicroSCADA instance was running.’

OT Living-off-the-Land

- Using LotL tools, the actor:
  - Decreased time and resources to conduct the attack.
  - Decreased likelihood of detection.
  - Handled legacy proprietary OT protocols without open source implementations or extensive documentation.

Photo by Adele Payman on Unsplash

Showing off their SCILz

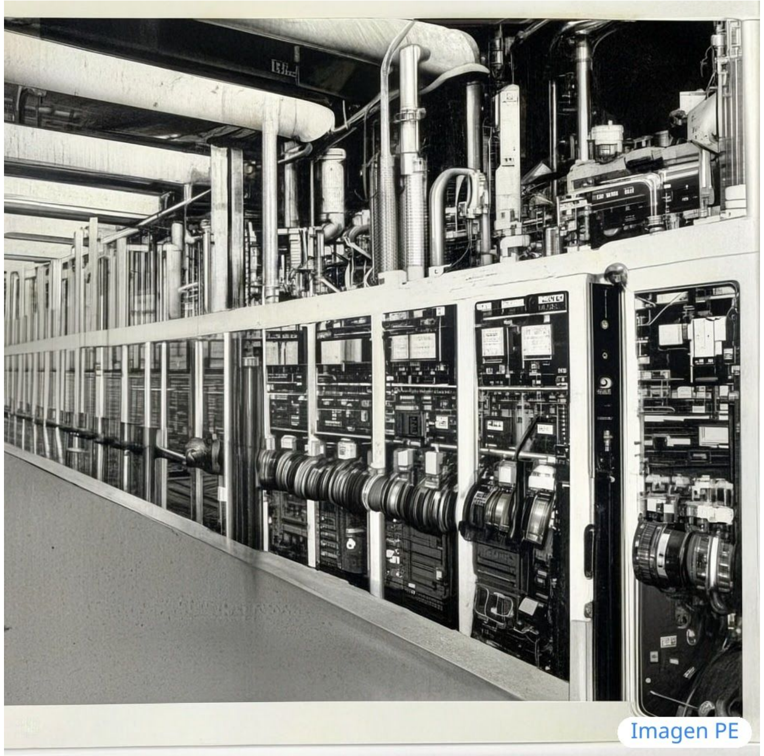
The Attack Required SCILz

Substation Operations

- Equipment hierarchy
- Control Logic
- Communication protocols

MicroSCADA System

- Architecture
- Vulnerabilities
- SCIL Language



More SCILz...

Prerequisites for successful SCIL programming

- Process Knowledge
- Experience with SCIL and MicroSCADA API
- Development & Test Environment

The script must include:

- Device Identification
- Execution Trigger
- Instructions/Commands

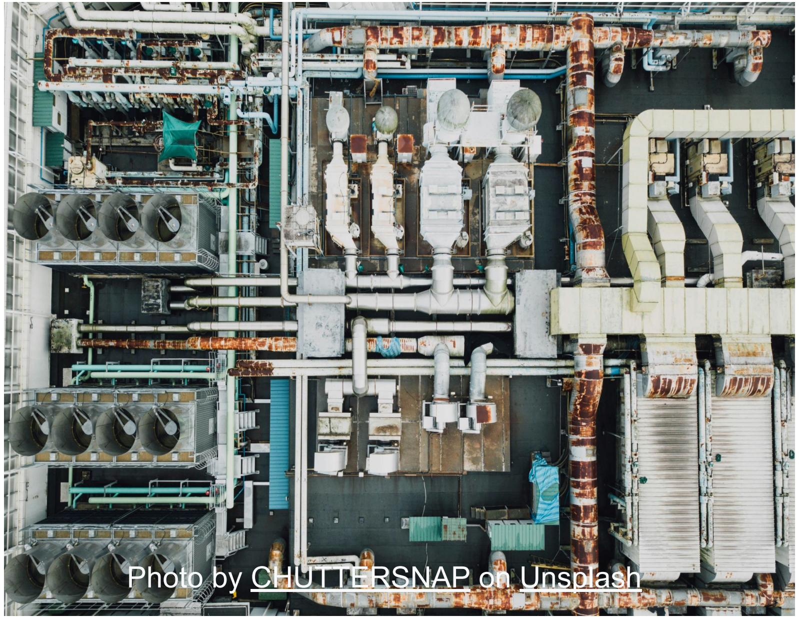


Photo by CHUTTERSNAP on Unsplash

Sophistication & Scope of the Attack

Single vs. Coordinated

Cascading Effects

Time-Based Logic

But we will never know...

SANDWORM: Then vs. Now

The attack suggests growing maturity of Russia's offensive OT arsenal, including an ability to r**ecognize novel OT threat vectors, develop new capabilities, and leverage different types of OT infrastructure** to execute attacks.

Pre Invasion

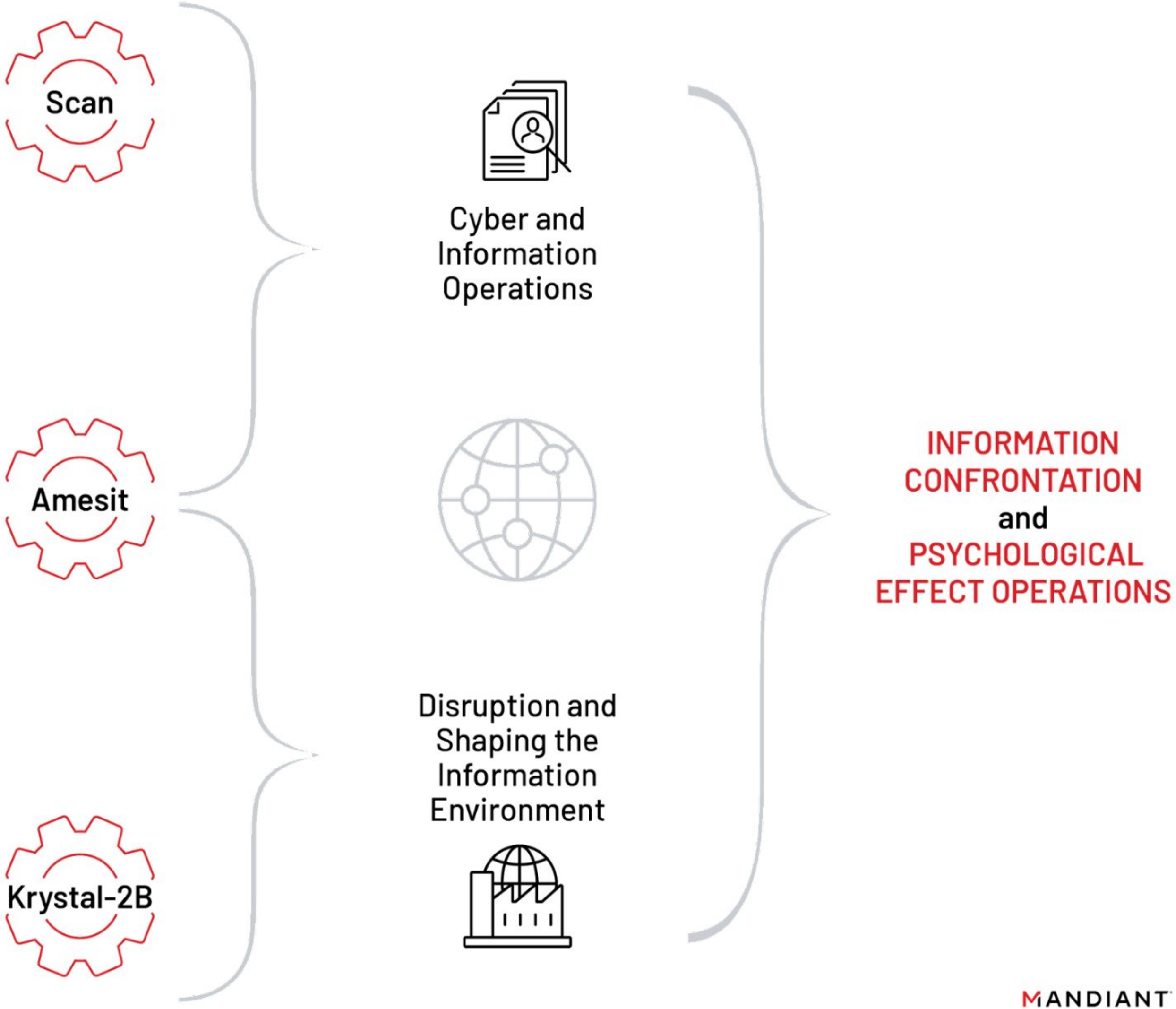
- Highly custom tooling, often tailored to specific operations and has minute details taken into consideration

Post Invasion

- Fast paced op-tempo that continues to evolve over time.
- Move towards lower equity tooling that favors reusability.

Development of Capabilities

Vulkan Leaks



Scan

Amesit

Krystal-2B

Cyber and Information Operations

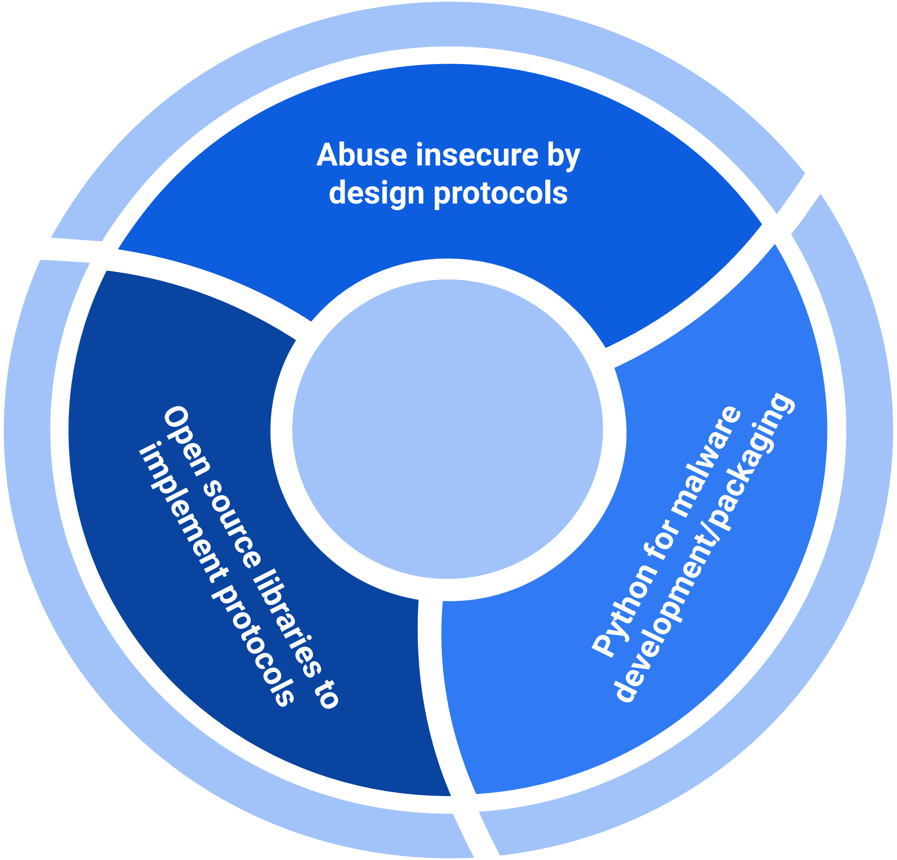
Disruption and Shaping the Information Environment

INFORMATION CONFRONTATION and PSYCHOLOGICAL EFFECT OPERATIONS

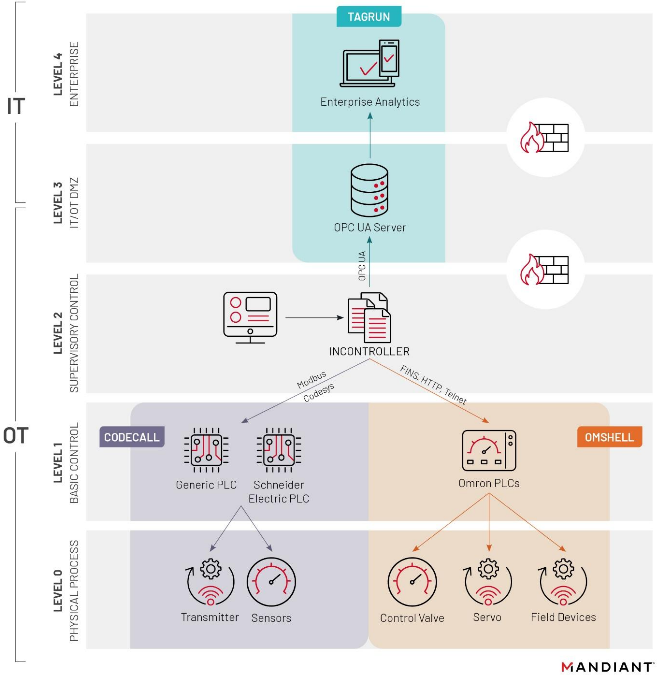
- Rail Systems: Manipulating speed of trains, creating unauthorized track transfers, causing car traffic barriers to fail, and causing combined heat and power (CHP) units to fail, with the objective of causing train collisions and accidents.

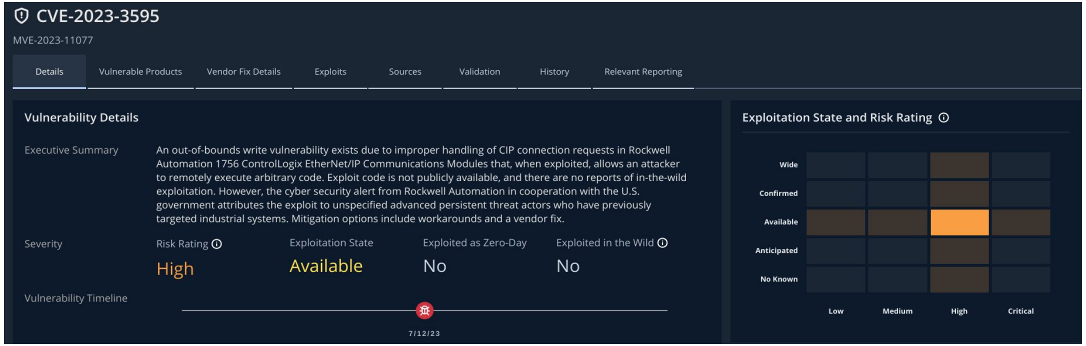
- Pipeline systems: Closing valves, shutting down pumps, overfilling tanks, spilling materials, and causing pump cavitation and overheating.

Modular OT capabilities for every occasion…


Abuse insecure by design protocols
Python for malware development/packaging
Open source libraries to implement protocols

Development of OT malware





CVE-2023-3595

MVE-2023-11077

Vulnerability Details

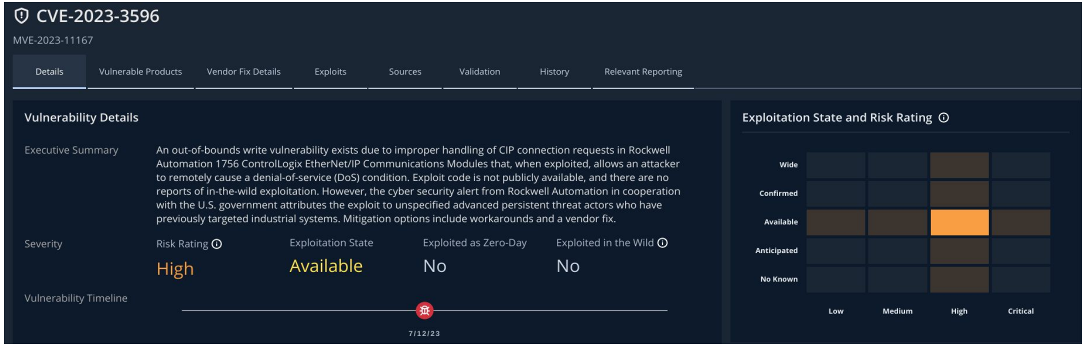
Executive Summary: An out-of-bounds write vulnerability exists due to improper handling of CIP connection requests in Rockwell Automation 1756 ControlLogix EtherNet/IP Communications Modules that, when exploited, allows an attacker to remotely execute arbitrary code. Exploit code is not publicly available, and there are no reports of in-the-wild exploitation. However, the cyber security alert from Rockwell Automation in cooperation with the U.S. government attributes the exploit to unspecified advanced persistent threat actors who have previously targeted industrial systems. Mitigation options include workarounds and a vendor fix.

Severity

Risk Rating	Exploitation State	Exploited as Zero-Day	Exploited in the Wild
High	Available	No	No

Vulnerability Timeline: 7/12/23

Exploitation State and Risk Rating



CVE-2023-3596

MVE-2023-11167

Vulnerability Details

Executive Summary: An out-of-bounds write vulnerability exists due to improper handling of CIP connection requests in Rockwell Automation 1756 ControlLogix EtherNet/IP Communications Modules that, when exploited, allows an attacker to remotely cause a denial-of-service (DoS) condition. Exploit code is not publicly available, and there are no reports of in-the-wild exploitation. However, the cyber security alert from Rockwell Automation in cooperation with the U.S. government attributes the exploit to unspecified advanced persistent threat actors who have previously targeted industrial systems. Mitigation options include workarounds and a vendor fix.

Severity

Risk Rating	Exploitation State	Exploited as Zero-Day	Exploited in the Wild
High	Available	No	No

Vulnerability Timeline: 7/12/23

Exploitation State and Risk Rating

Other examples include INDUSTROYER, INDUSTROYER.V2 and COSMICENERGY...

Main Takeaways

- Growing maturity of Russia’s offensive OT arsenal. Able to **recognize novel OT threat vectors, develop capabilities, and leverage OT infrastructure** to execute attacks.
- We expect future OT attacks to become more efficient, modular, and use LotL resources.
- An attacker with such skills can adapt similar techniques to other SCADA systems.
- Defenders need to match attacker's understanding of systems, protocols, and languages to monitor and detect anomalies.
- Sandworm will be back again...

Photo by Clem Onojeghuo on Unsplash

Recommendations

The attack represents an immediate threat to critical infrastructure environments leveraging the MicroSCADA supervisory control system. We suggest some general steps to harden SCADA systems:

- Disabling unnecessary services and features
- Implement MFA everywhere feasible
- Disable Auto run
- Patch when possible - dependent on availability requirements
- Use Role-Based Access Control to ensure permissions are set properly for accounts based on what they need to do - operator, admin, engineer, or otherwise.
- Enable robust application logging for MicroSCADA and aggregate logs in a central location
- Identify similar applications other than those using SCIL that have similar capabilities
- Collaborate with your vendors to understand similar attack paths to target their systems

Some hunting candy...

```
rule M_Hunting_MicroSCADA_SCILC_Program_Execution_Strings
{
     meta:
          author = "Mandiant"
          date = "2023-02-13"
          description = "Searching for files containing strings associated
with execution of the MicroSCADA Supervisory Control Implementation Language
(SCIL) scilc.exe binary."
          disclaimer = "This rule is for hunting purposes only and has not
been tested to run in a production environment."

     strings:
          $s = "scilc.exe -do" nocase ascii wide

     condition:
          filesize < 1MB and
          all of them
}
```

Blog: Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology

```
rule M_Methodology_MicroSCADA_Path_Strings
{
     meta:
          author = "Mandiant"
          date = "2023-02-27"
          description = "Searching for files containing references to
MicroSCADA filesystem path containing native MicroSCADA binaries and
resources."
          disclaimer = "This rule is for hunting purposes only and has not
been tested to run in a production environment."

     strings:
          $s1 = "sc\\prog\\exec" nocase ascii wide

     condition:
          filesize < 1MB and
          $s1
}
```

Thank you!

kapellmann@google.com
www.kapell.tech
@Kapellmann