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

mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

In late 2022, Mandiant responded to a disruptive cyber physical incident in which the Russia-linked threat actor Sandworm targeted a Ukrainian critical infrastructure organization. This incident was a multi-event cyber attack that leveraged a novel technique for impacting industrial control systems (ICS) / operational technology (OT). The actor first used OT-level living off the land (LotL) techniques to likely trip the victim's substation circuit breakers, causing an unplanned power outage that coincided with mass missile strikes on critical infrastructure across Ukraine. Sandworm later conducted a second disruptive event by deploying a new variant of CADDYWIPER in the victim's IT environment.

This attack represents the latest evolution in Russia's cyber physical attack capability, which has been increasingly visible since Russia's invasion of Ukraine. The techniques leveraged during the incident suggest a growing maturity of Russia's offensive OT arsenal, including an ability to recognize novel OT threat vectors, develop new capabilities, and leverage different types of OT infrastructure to execute attacks. By using LotL techniques, the actor likely decreased the time and resources required to conduct its cyber physical attack. While Mandiant was unable to determine the initial intrusion point, our analysis suggests the OT component of this attack may have been developed in as little as two months. This indicates that the threat actor is likely capable of quickly developing similar capabilities against other OT systems from different original equipment manufacturers (OEMs) leveraged across the world.

We initially tracked this activity as UNC3810 before merging the cluster with Sandworm. Sandworm is a full-spectrum threat actor that has carried out espionage, influence and attack operations in support of Russia's Main Intelligence Directorate (GRU) since at least 2009. The group's long-standing center focus has been Ukraine, where it has carried out a campaign of disruptive and destructive attacks over the past decade using wiper malware, including during Russia's re-invasion in 2022. Beyond Ukraine, the group continues to sustain espionage operations that are global in scope and illustrative of the Russian military's far-reaching ambitions and interests in other regions. Government indictments have linked the group to the Main Center for Special Technologies (also known as GTsST and Military Unit 74455). Given Sandworm's global threat activity and novel OT capabilties, we urge OT asset owners to take action to mitigate this threat. We include a range of detections, hunting and hardening guidance, MITRE ATT&CK mappings and more in the appendices of this blog post.

If you need support responding to related activity, please contact Mandiant Consulting. Further analysis of Sandworm threat activity is available as part of Mandiant Advantage Threat Intelligence.

Incident Summary

Based on our analysis, the intrusion began on, or prior to, June 2022 and culminated in two disruptive events on October 10 and 12, 2022. While we were unable to identify the initial access vector into the IT environment, Sandworm gained access to the OT environment through a hypervisor that hosted a supervisory control and data acquisition (SCADA) management instance for the victim's substation environment. Based on evidence of lateral movement, the attacker potentially had access to the SCADA system for up to three months.

On October 10, the actor leveraged an optical disc (ISO) image named "a.iso" to execute a native MicroSCADA binary in a likely attempt to execute malicious control commands to switch off substations. The ISO file contained at least the following:

- "lun.vbs", which runs n.bat
- "n.bat", which likely runs the native scilc.exe utility
- "s1.txt", which likely contains the unauthorized MicroSCADA commands

Based on a September 23 timestamp of "lun.vbs", there was potentially a two-month time period from when the attacker gained initial access to the SCADA system to when they developed the OT capability. Although we were not able to fully recover the ICS command execution implemented by the binary, we are aware that the attack resulted in an unscheduled power outage. Figure 1 contains a visualization of the execution chain resulting in the disruptive OT event.

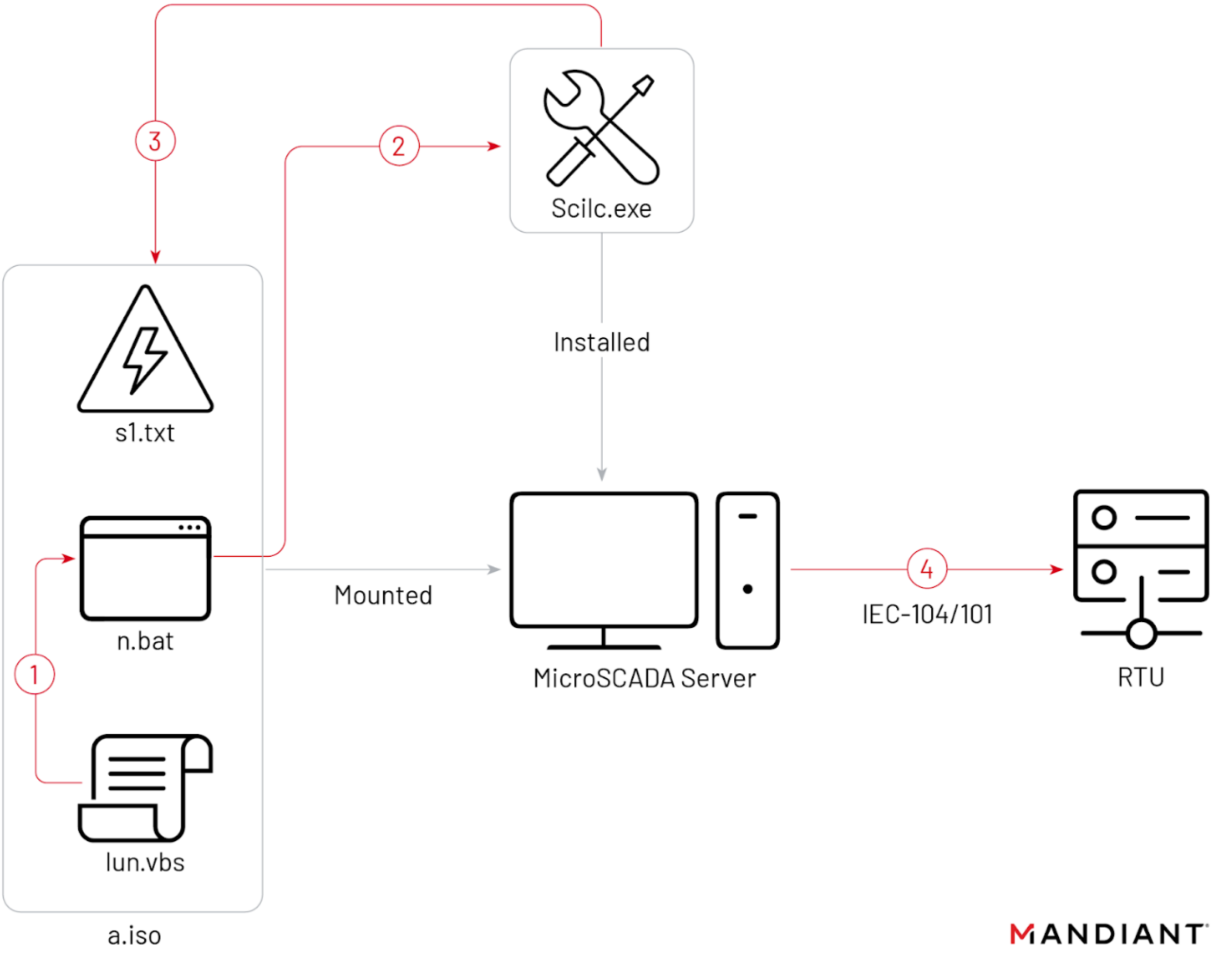


Figure 1: Execution chain of disruptive OT event

Two days after the OT event, Sandworm deployed a new variant of CADDYWIPER in the victim’s IT environment to cause further disruption and potentially to remove forensic artifacts. However, we note that the wiper deployment was limited to the victim’s IT environment and did not impact the hypervisor or the SCADA virtual machine. This is unusual since the threat actor had removed other forensic artifacts from the SCADA system in a possible attempt to cover their tracks, which would have been enhanced by the wiper activity. This could indicate a lack of coordination across different individuals or operational subteams involved in the attack.

A deeper dive on the attack lifecycle and OT capability can be found in the Technical Analysis section of the blog post.

Sandworm’s Threat Activity Reveals Insights into Russia’s Offensive Cyber Capabilities

Sandworm’s substation attack reveals notable insights into Russia’s continued investment in OT-oriented offensive cyber capabilities and overall approach to attacking OT systems. This incident and last year’s INDUSTROYER.V2 incident both show efforts to streamline OT attack capabilities through simplified deployment features. We observed the same efforts in our analysis of a series of documents detailing project requirements to enhance Russian offensive cyber capabilities.

Similarly, the evolution of suspected GRU-sponsored OT attacks shows a decrease in the scope of disruptive activities per attack. The 2015 and 2016 Ukraine blackout events each featured several discrete disruptive events against the OT environment (e.g., disabling UPS systems, bricking serial-to-ethernet converters, conducting a DoS attack against a SIPROTEC relay, wiping OT systems, etc.). By comparison, the INDUSTROYER.V2 incidents lacked many of those same disruptive components and the malware did not feature the wiper module from the original INDUSTROYER. Likewise, Sandworm's activity in the OT network appears streamlined to only executing unauthorized ICS command messages, with the wiper activity limited to the IT environment. While this shift likely reflects the increased tempo of wartime cyber operations, it also reveals the GRU's priority objectives in OT attacks.

Sandworm's use of a native Living off the Land binary (LotLBin) to disrupt an OT environment shows a significant shift in techniques. Using tools that are more lightweight and generic than those observed in prior OT incidents, the actor likely decreased the time and resources required to conduct a cyber physical attack. LotLBin techniques also make it difficult for defenders to detect threat activity as they need to not only remain vigilant for new files introduced to their environments, but also for modifications to files already present within their installed OT applications and services. As outlined in recent research detailing the GRU's disruptive playbook, we have observed Sandworm adopting LotL tactics across its wider operations to similarly increase the speed and scale at which it can operate while minimizing the odds of detection.

While we lack sufficient evidence to assess a possible link, we note that the timing of the attack overlaps with Russian kinetic operations. Sandworm potentially developed the disruptive capability as early as three weeks prior to the OT event, suggesting the attacker may have been waiting for a specific moment to deploy the capability. The eventual execution of the attack coincided with the start of a multi-day set of coordinated missile strikes on critical infrastructure across several Ukrainian cities, including the city in which the victim was located.

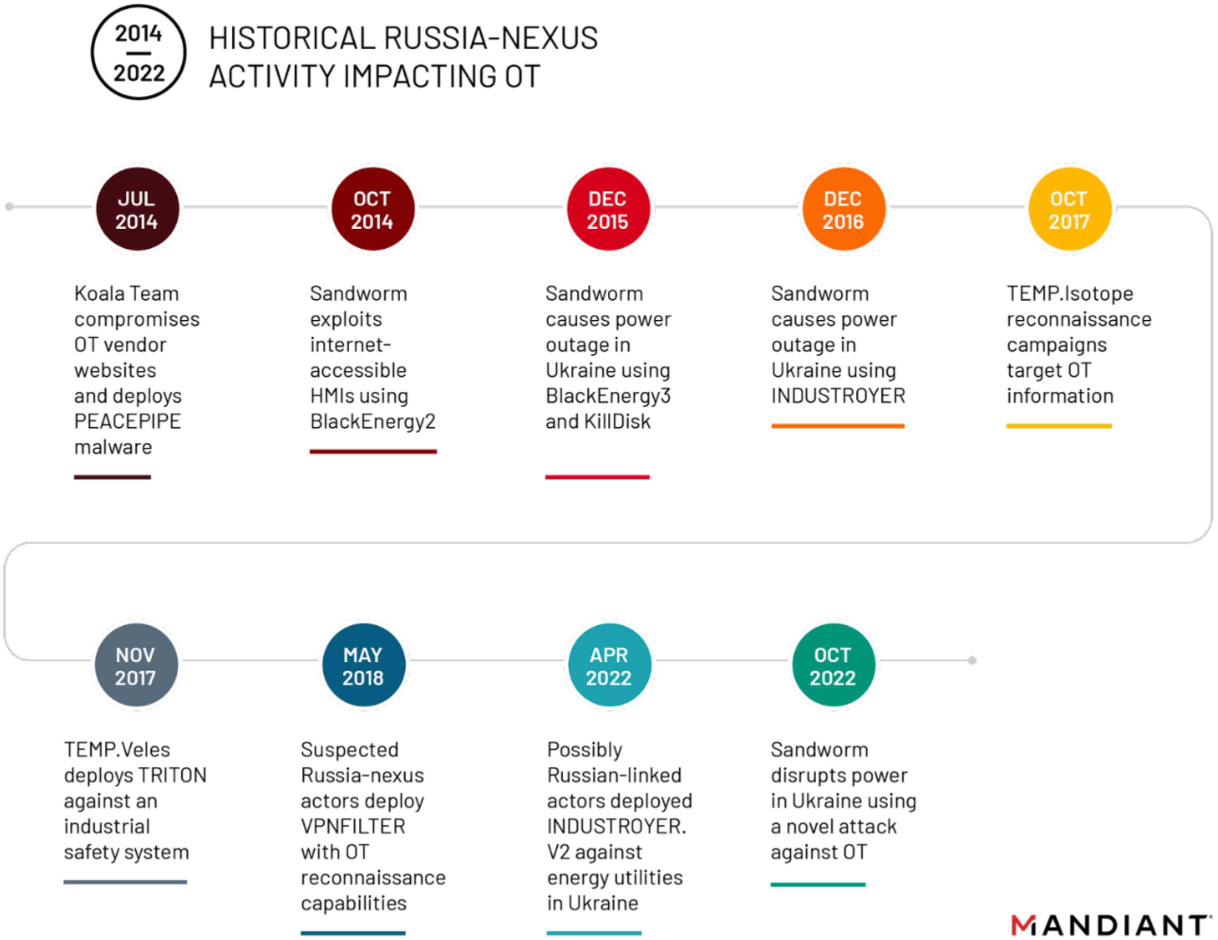

2014
2022
HISTORICAL RUSSIA-NEXUS ACTIVITY IMPACTING OT
JUL 2014
Koala Team compromises OT vendor websites and deploys PEACEPIPE malware
OCT 2014
Sandworm exploits internet-accessible HMIs using BlackEnergy2
DEC 2015
Sandworm causes power outage in Ukraine using BlackEnergy3 and KillDisk
DEC 2016
Sandworm 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
MANDIANT

Figure 2: Historical Russia-nexus activity impacting OT

Outlook

This attack represents an immediate threat to Ukrainian critical infrastructure environments leveraging the MicroSCADA supervisory control system. Given Sandworm's global threat activity and the worldwide deployment of MicroSCADA products, asset owners globally should take action to mitigate their tactics, techniques, and procedures against IT and OT systems. Furthermore, our analysis of the activity suggests Russia would be capable of developing similar capabilities against other SCADA systems and programming languages beyond MicroSCADA and SCIL. We urge asset owners to review and implement the following recommendations to mitigate and detect this activity.

Acknowledgements

This research was made possible thanks to the hard work of many people not listed on the byline. Mandiant would like to acknowledge the Security Service of Ukraine (SBU) for their continued partnership and contributions to this report as well as their on-going collaboration. This incident response engagement was funded through the UK’s Ukraine Cyber Programme (cross-government Conflict, Stability and Security Fund) and delivered by the United Kingdom’s Foreign, Commonwealth and Development Office.

Technical Analysis: Sandworm Attack Against Ukrainian Substations

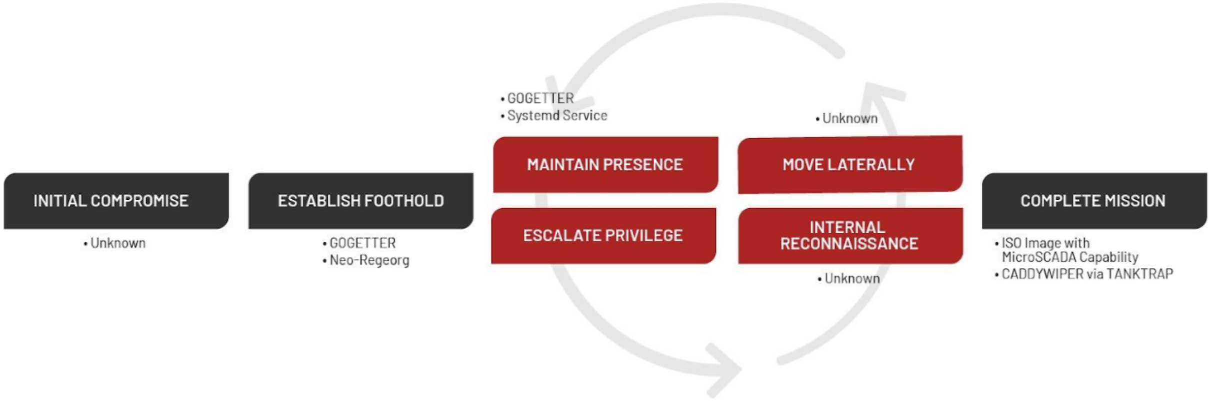
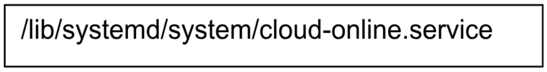


Figure 3: Incident targeted attack lifecycle

Initial Compromise and Maintaining Presence

At this time, it is unknown how Sandworm gained initial access to the victim. Sandworm was first observed in the victim's environment in June 2022, when the actor deployed the Neo-REGEORG webshell on an internet-facing server. This is consistent with the group's prior activity scanning and exploiting internet facing servers for initial access. Roughly one month later, Sandworm deployed GOGETTER, which is a tunneler written in Golang that proxies communications for its command and control (C2) server using the open-source library Yamux over TLS.

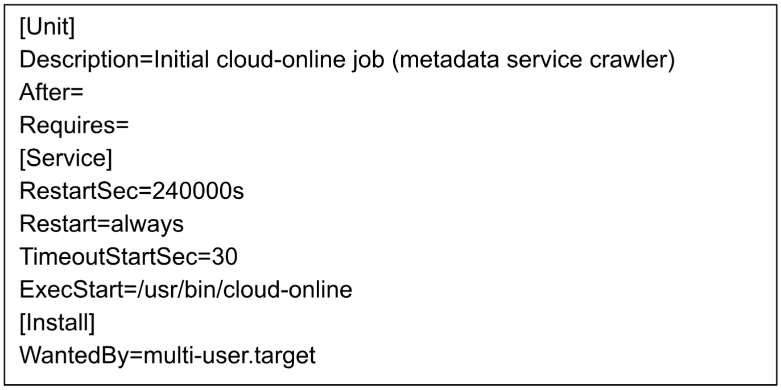
When leveraging GOGETTER, Sandworm utilized a Systemd service unit to maintain persistence on systems. A Systemd service unit allows for a program to be run under certain conditions, and in this case, it was used to execute the GOGETTER binary on reboot.



```
/lib/systemd/system/cloud-online.service
```

Figure 4: Sandworm GOGETTER Systemd configuration location

The Systemd configuration file leveraged by Sandworm enabled the group to maintain persistence on systems. The value "WantedBy" defines when the program should be run; in the configuration used by Sandworm, the setting "multi-user.target" means that the program will be run when the host has reached a state when it will accept users logging on, for example after successful power on. This enables GOGETTER to maintain persistence across reboots. The "ExecStart" value specifies the path of the program to be run, which in this case was GOGETTER.



```
[Unit]
Description=Initial cloud-online job (metadata service crawler)
After=
Requires=
[Service]
RestartSec=240000s
Restart=always
TimeoutStartSec=30
ExecStart=/usr/bin/cloud-online
[Install]
WantedBy=multi-user.target
```

Figure 5: Sandworm GOGETTER Systemd configuration

When deploying GOGETTER, Mandiant observed Sandworm leverage Systemd service units designed to masquerade as legitimate or seemingly legitimate services.

Lateral Movement to SCADA Hypervisor and OT Attack Execution

Sandworm utilized a novel technique to impact the OT environment by executing code within an End-of-Life (EOL) MicroSCADA control system and issuing commands that impacted the victim’s connected substations. Table 1 summarizes the malicious files containing the new OT capability. We note that given the attacker’s use of anti-forensics techniques, we were not able to recover all the artifacts from the intrusion.

Filename	Hash	Purpose
a.iso	Unknown	Contains attacker’s files
lun.vbs	26e2a41f26ab885bf409982cb823ffd1	Runs n.bat
n.bat	Unknown	Likely runs native scilc.exe utility
s1.txt	Unknown	Likely contains SCIL commands

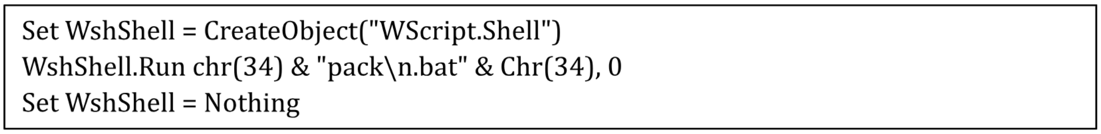
Table 1: Malicious OT files

To impact the OT systems, Sandworm accessed the hypervisor that hosted a SCADA management instance for the victim’s substation environment and leveraged an ISO image named "a.iso" as a virtual CD-ROM. The system was configured to permit inserted CD-ROMs to autorun. The ISO file, at minimum, contained the following files: "lun.vbs" and "n.bat" as both files are referenced within the D volume and therefore contained within “a.iso”. The inserted ISO led to at least the following command lines execution:

- wscript.exe "d:\pack\lun.vbs"

- cmd /c "D:\pack\n.bat"

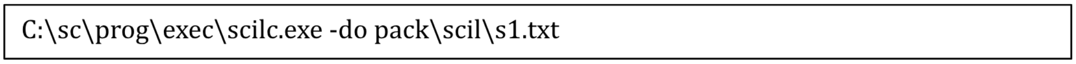
Based on forensic analysis, we believe “lun.vbs” contents are the following (Figure 6):



```
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run chr(34) & "pack\n.bat" & Chr(34), 0
Set WshShell = Nothing
```

Figure 6: “lun.vbs” contents

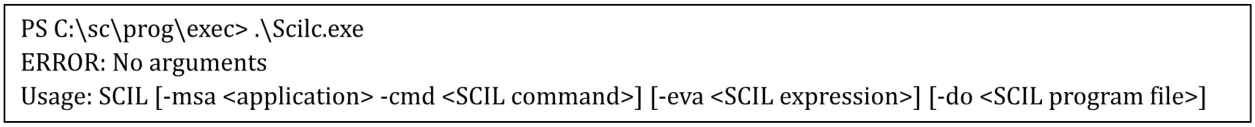
The contents in Figure 6 indicate that “lun.vbs” executes “n.bat”. Additional fragments recovered include text consistent with Windows command line execution (Figure 7). This fragment was identified by analyzing images from the host. Reconstruction of the host’s anti-virus logs indicates “lun.vbs” and “n.bat” were executed in close time proximity. Because of this and the reference to the attacker’s ISO folder path, we believe that the command fragment in Figure 7 is likely the contents of “n.bat”.



```
C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt
```

Figure 7: Command fragment

The syntax of the command fragment includes “scilc.exe”, a native utility that is part of the MicroSCADA software suite. The utility is located in the “\sc\prog\exec” folder within the MicroSCADA installation directory, amongst other utilities, libraries, and resources used by MicroSCADA. The impacted MicroSCADA system was running an EOL software version that allowed default access to the SCIL-API. The “-do” flag specifies a SCIL program file to execute (Figure 8). Lastly, the command supplies a file named “s1.txt” in the "pack\scil\" folder of the attacker's ISO. We assess "pack\scil\s1.txt" is likely a file containing SCIL commands the attackers executed in MicroSCADA. This file was unrecoverable at the time of analysis.



```
PS C:\sc\prog\exec> .\Scilc.exe
ERROR: No arguments
Usage: SCIL [-msa <application> -cmd <SCIL command>] [-eva <SCIL expression>] [-do <SCIL program file>]
```

Figure 8: Scilc.exe usage example

According to Hitachi Energy’s documentation, SCIL is a high level programming language designed for MicroSCADA control systems and can operate the system and its features (Figure 9). SCIL programs are generally text-based statements that can be composed of commands, objects, variables, calls to predefined functions, and expressions. There are several methods in which SCIL programs can execute, such as an engineer/operator clicking a button or image within the MicroSCADA system, scheduled or process derived changes, or in this case manual execution.

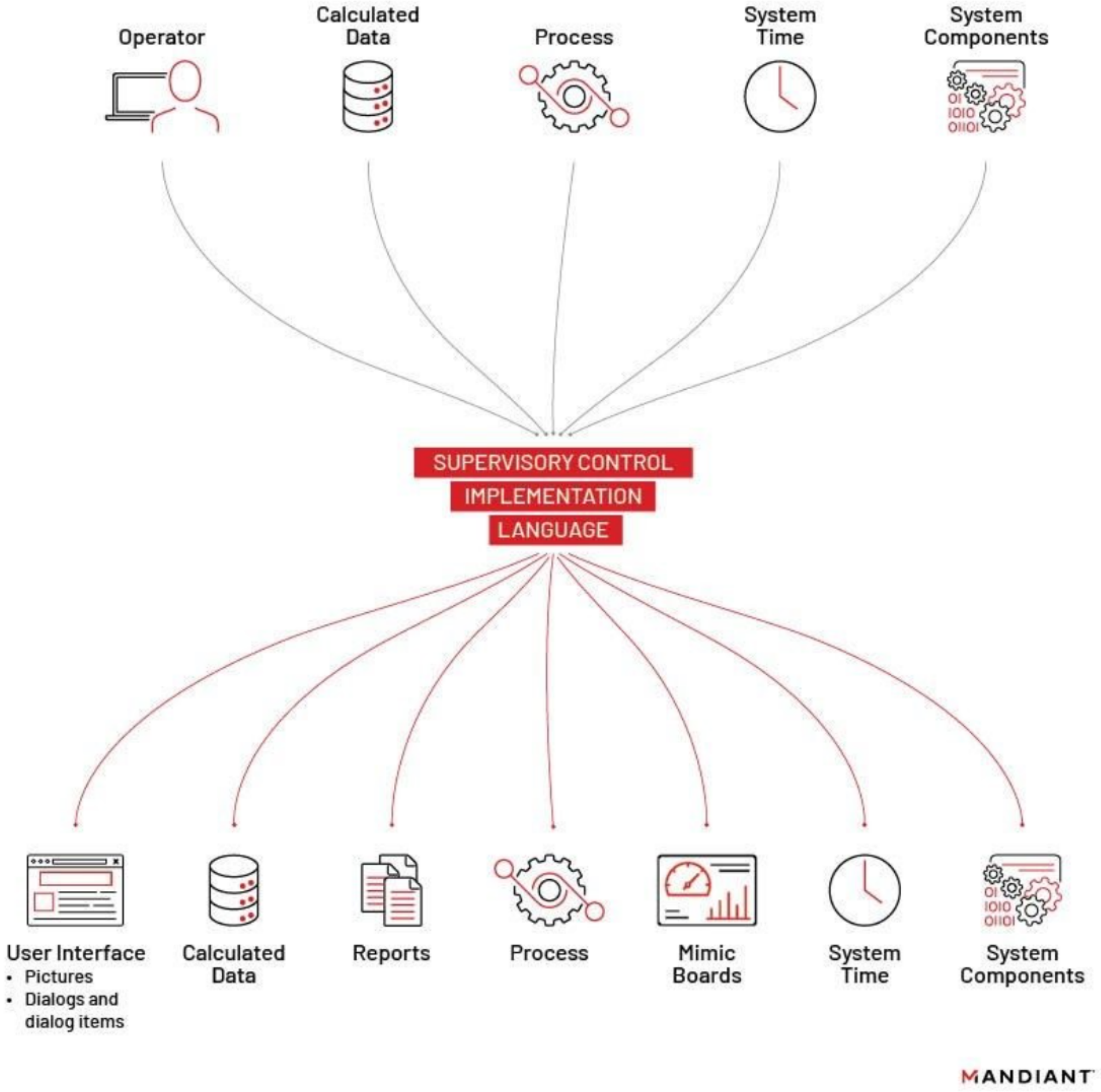


Figure 9: SCIL overview

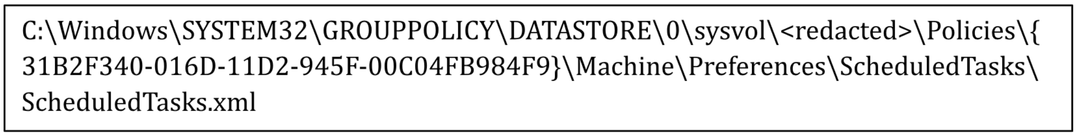
While we were unable to identify the SCIL commands executed, we believe they were probably commands to open circuit breakers in the victim's substation environments. The SCIL commands would have caused the MicroSCADA server to relay the commands to the substation RTUs via either the IEC-60870-5-104 protocol for TCP/IP connections or the IEC-60870-5-101 protocol for serial connections.

Sandworm Deployed New CADDYWIPER Variant to Further Disrupt the Victim's IT Environment

Two days following the OT activity, Sandworm deployed a new variant of CADDYWIPER throughout the IT environment. This CADDYWIPER variant, compiled in October 2022, contains some minor functionality improvements that allow threat actors to resolve functions at runtime. We have observed CADDYWIPER deployed across several verticals in Ukraine, including the government and financial sectors, throughout Russia's invasion of Ukraine.

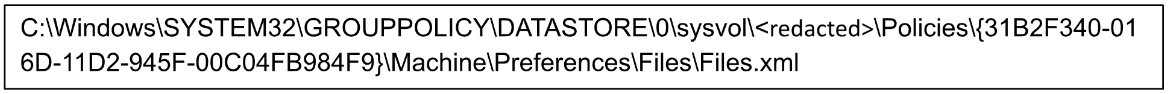
CADDYWIPER is a disruptive wiper written in C that is focused on making data irrecoverable and causing maximum damage within an environment. CADDYWIPER will attempt to wipe all files before proceeding to wipe any mapped drives. It will then attempt to wipe the physical drive partition itself. Notably, CADDYWIPER has been the most frequently used disruptive tool against Ukrainian entities during the war and has seen consistent operational use since March 2022, based on public reporting. We have observed Sandworm utilize CADDYWIPER in disruptive operations across multiple intrusions.

Sandworm deployed CADDYWIPER in this operation via two Group Policy Objects (GPO) from a Domain Controller using TANKTRAP. TANKTRAP is a utility written in PowerShell that utilizes Windows group policy to spread and launch a wiper. We have observed TANKTRAP being used with other disruptive tools including NEARMISS, SDELETE, PARTYTICKET, and CADDYWIPER. These group policies contained instructions to copy a file from a server to the local hard drive and to schedule a task to run the copied file at a particular time.



```
C:\Windows\SYSTEM32\GROUPPOLICY\DATASTORE\0\sysvol\<redacted>\Policies\{
31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Preferences\ScheduledTasks\
ScheduledTasks.xml
```

Figure 10: Sandworm TANKTRAP GPO 1



```
C:\Windows\SYSTEM32\GROUPPOLICY\DATASTORE\0\sysvol\<redacted>\Policies\{31B2F340-01
6D-11D2-945F-00C04FB984F9}\Machine\Preferences\Files\Files.xml
```

Figure 11: Sandworm TANKTRAP GPO 2

Both TANKTRAP GPOs deployed CADDYWIPER from a staged directory to systems as msserver.exe. CADDYWIPER was then executed as a scheduled task at a predetermined time.

Item	Value
Task Name	qAWZe
Legacy Task Name	QcWBX
Command to Run	C:\Windows\msserver.exe
Trigger	Run at 2022-10-12 16:50:40

Table 2: Sandworm TANKTRAP GPO 1 Scheduled Task

Item	Value
Task Name	QJKWt
Legacy Task Name	zJMwY
Command to Run	C:\Windows\msserver.exe
Trigger	Run at 2022-10-12 17:15:59

Table 3: Sandworm TANKTRAP GPO 2 Scheduled Task

Appendix A: Discovery and Hardening Guidance

In this incident, the attacker leveraged an EOL version of the MicroSCADA supervisory control system. The SCIL-API interface in MicroSCADA has been disabled-by-default since the release of MicroSCADA 9.4 in 2014. If required to continue using the interface, asset owners can refer to MRK511518 MicroSCADA X Cyber Security Deployment Guideline on how to harden the MicroSCADA. Please contact the Hitachi Energy MicroSCADA support team to obtain the documentation.

We note that the MicroSCADA control system became a Hitachi Energy product in 2022 after a divestiture from ABB. Asset owners should reference both vendors in asset inventories and manual asset inspections to determine if the product is present in any OT environments.

Harden MicroSCADA and other SCADA management hosts:

- Update MicroSCADA to supported versions.
- Configure MicroSCADA to require authentication and establish a least privilege design for user permissions.
- Establish robust network segmentation between MicroSCADA hosts and IT networks.
- Enable robust application logging for MicroSCADA and aggregate logs to a central location.
- If/where feasible, configure the base system in “read-only” mode and ensure no external SCIL-API programs (such as scilc.exe) are allowed.
- Consult with OEMs for installed SCADA software to identify similar methods of code execution within their software and to obtain guidance on mitigations.

Monitor MicroSCADA systems and other SCADA management systems for:

- Command-line execution of MicroSCADA “Scilc.exe” binary and other native MicroSCADA binaries that may be leveraged to execute unauthorized SCIL program/commands.
- Network traffic and process related telemetry to/from host(s) operating the MicroSCADA software. Investigate anomalous activity and correlate findings with process telemetry.
- Files transferred or moved onto MicroSCADA hosts.
- Newly created files with MicroSCADA or SCIL programming language references.
- Unauthorized changes in MicroSCADA system configuration and data.

Appendix B: Indicators of Compromise (IOCs)

Indicator	Description
82.180.150[.]197	Source IP address for requests to Neo-REGEORG
176.119.195[.]113	Source IP address for requests to Neo-REGEORG
176.119.195[.]115	Source IP address for requests to Neo-REGEORG
185.220.101[.]58	Source IP address for requests to Neo-REGEORG
190.2.145[.]24	C2 for GOGETTER
Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0	User agent for requests to Neo-REGEORG
Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0	User agent for requests to Neo-REGEORG

Table 4: Network IOCs

File Name	MD5 Hash	Type

Functions.php	3290cd8f948b8b15a3c53f8e7190f9b0	Neo-REGEORG
cloud-online	cea123ebf54b9d4f8811a47134528f12	GOGETTER
lun.vbs	26e2a41f26ab885bf409982cb823ffd1	Runs n.bat
n.bat	UNKNOWN	Likely runs scilc.exe
a.iso	UNKNOWN	Likely contains attacker files
msserver.exe / lhh.exe	b2557692a63e119af0a106add54950e6	CADDYWIPER
Files.xml	Not Applicable	Part of TANKTRAP Group Policy; File Copy
ScheduledTasks.xml	61c245a073bdb08158a3c9ad0219dc23	Part of TANKTRAP Group Policy; Task
ScheduledTasks.xml	82ab2c7e4d52bb2629aff200a4dc6630	Part of TANKTRAP Group Policy; Task
s1.txt	UNKNOWN	Likely contains SCIL commands

Table 5: Endpoint IOCs

Appendix C: YARA Rules

```
rule M_Methodology_MicroSCADA_SCILC_Strings

{

     meta:

          author = "Mandiant"

          date = "2023-02-13"

          description = "Searching for files containing strings associated
with 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:

          $s1 = "scilc.exe" ascii wide

          $s2 = "Scilc.exe" ascii wide

          $s3 = "SCILC.exe" ascii wide

          $s4 = "SCILC.EXE" ascii wide

     condition:

          filesize < 1MB and

          any of them

}
```

```
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

}
```

```
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

}
```

```
rule M_Hunting_VBS_Batch_Launcher_Strings
{
     meta:
          author = "Mandiant"
          date = "2023-02-13"
          description = "Searching for VBS files used to launch a batch
script."
          disclaimer = "This rule is for hunting purposes only and has not
been tested to run in a production environment."
     strings:
          $s1 = "CreateObject(\"WScript.Shell\")" ascii
          $s2 = "WshShell.Run chr(34) &" ascii
          $s3 = "& Chr(34), 0" ascii
          $s4 = "Set WshShell = Nothing" ascii
          $s5 = ".bat" ascii

     condition:
          filesize < 400 and
          all of them
}
```

```
rule M_Hunting_APT_Webshell_PHP_NEOREGEORG

{

     meta:

          author = "Mandiant"

          description = "Searching for REGEORG webshells."

          disclaimer = "This rule is for hunting purposes only and has not
been tested to run in a production environment."

     strings:

          $php = "<?php" nocase

          $regeorg1 = {24 72 61 77 50 6f 73 74 44 61 74 61 20 3d 20 66 69 6c
65 5f 67 65 74 5f 63 6f 6e 74 65 6e 74 73 28 22 70 68 70 3a 2f 2f 69 6e 70
75 74 22 29 3b}

          $regeorg2 = {20 24 77 72 69 74 65 42 75 66 66 20 3d 20 24 5f 53 45
53 53 49 4f 4e 5b 24 77 72 69 74 65 62 75 66 5d 3b}

          $regeorg3 = {20 75 73 6c 65 65 70 28 35 30 30 30 30 29 3b}

          $regeorg4 = {20 24 61 72 68 5f 6b 65 79 20 3d 20 70 72 65 67 5f 72
65 70 6c 61 63 65 28 24 72 78 5f 68 74 74 70 2c 20 27 27 2c 20 24 6b 65 79
29 3b}

          $regeorg5 = {20 24 72 75 6e 6e 69 6e 67 20 3d 20 24 5f 53 45 53 53
49 4f 4e 5b 24 72 75 6e 5d 3b}

          $regeorg6 = {20 24 72 78 5f 68 74 74 70 20 3d 20 27 2f 5c 41 48 54
54 50 5f 2f 27 3b}

     condition:

          (5 of ($regeorg*)) and

          $php

}
```

```
rule M_Hunting_GOGETTER_SystemdConfiguration_1
{
     meta:
          author = "Mandiant"
          description = "Searching for Systemd Unit Configuration Files but with some known filenames observed with GOGETTER"
          disclaimer = "This rule is for hunting purposes only and has not been tested to run in a production environment."
     strings:
          $a1 = "[Install]" ascii fullword
          $a2 = "[Service]" ascii fullword
          $a3 = "[Unit]" ascii fullword
          $v1 = "Description=" ascii
          $v2 = "ExecStart=" ascii
          $v3 = "Restart=" ascii
          $v4 = "RestartSec=" ascii
          $v5 = "WantedBy=" ascii
          $f1 = "fail2ban-settings" ascii fullword
          $f2 = "system-sockets" ascii fullword
          $f3 = "oratredb" ascii fullword
          $f4 = "cloud-online" ascii fullword
     condition:
          filesize < 1MB and (3 of ($a*)) and (3 of ($v*)) and (1 of ($f*))
}
```

Appendix D: SIGMA and YARA-L Rules

```
title: MicroSCADA SCILC Command Execution

description: Identification of Events or Host Commands that are related to
the MicroSCADA SCILC programming language and specifically command execution

author: Mandiant

date: 2023/02/27

logsource:

    product: windows

    service: security

detection:

    selection:

        NewProcessName|endswith:

            - \scilc.exe

        CommandLine|contains:

            - -do

    condition: selection

falsepositives:

    - Red Team

level: High

tags:

    - attack.execution

    - attack.T1059
```

```
rule M_YARAL_Methodology_ProcessExec_SCILC_Do_1

{

    meta:

        author = "Mandiant"

        description = "YARA-L rule hunting for instances of process
execution of the scilc.exe process with -do parameters. This is intended to
be a hunting rule. Analysts would need to verify the legitimacy of the file
passed in the -do parameter."

        severity = "Low"

        reference = "
https://cloud.google.com/chronicle/docs/detection/yara-l-2-0-overview"

    events:

        $e.metadata.event_type = "PROCESS_LAUNCH"

        $e.target.process.command_line = /\s+\-do\s+[^\-\s]+/ nocase

        $e.target.process.file.full_path = /scilc\.exe$/ nocase

    condition:

        $e

}
```

Appendix E: MITRE ATT&CK for ICS Mapping

Tactic	Technique	Procedure
Initial Access	**T0847:** Replication Through Removable Media	Sandworm accessed a hypervisor that hosted a SCADA management instance for the victim’s substation environment and leveraged an ISO image named "a.iso" as a logical CD-ROM inserted into the CD-ROM drive of the SCADA virtual machine. The system was configured to permit inserted CD-ROMs to autorun.

Execution	**T0807:** Command-Line Interface	Sandworm leveraged malicious files that led to at least the following command lines execution: • *wscript.exe "d:\pack\lun.vbs"* • *cmd /c "D:\pack\n.bat"* Additional fragments recovered include text consistent with Windows command line execution: *C:\sc\prog\exec\scilc.exe -do pack\scil\s1.txt*
Execution	**T0871:** Execution Through API	Sandworm utilized the native MicroSCADA “scilc.exe” binary to execute an external SCIL program via the SCIL-API.
Execution	**T0853:** Scripting	Sandworm leveraged Visual Basic Scripts, such as “lun.vbs”. The contents of “lun.vbs” include the following: *Set WshShell = CreateObject(“WScript.Shell”)* *WshShell.Run chr(34) & “pack\n.bat” & Chr(34), 0* *Set WshShell = Nothing*
Evasion	**T0872:** Indicator Removal on Host	Sandworm deployed CADDYWIPER malware and deleted files to remove forensic artifacts.
Inhibit Response Function	**T0809:** Data Destruction	Sandworm deployed CADDYWIPER to wipe all files, any mapped drives, and the physical drive partition of impacted systems. The actor deleted files related to the OT capability.
Impair Process Control	**T0855:** Unauthorized Command Message	Sandworm utilized “scilc.exe” to execute unauthorized SCIL commands that would have caused the MicroSCADA server to relay the commands to the substation RTUs via either the IEC-60870-5-104 protocol for TCP/IP connections or the IEC-68750-5-101 protocol for serial connections.
Impact	**T0831:** Manipulation of Control	Sandworm caused a manipulation of control of the power distribution system via unauthorized SCIL commands. These were likely commands to open circuit breakers in the victim’s substation environments.

Table 6: MITRE ATT&CK for ICS mapping

Appendix F: Validation Content

VID	Title
A106-441	Malicious File Transfer - REGEORG.NEO, Download, Variant #1
A106-442	Malicious File Transfer - Sandworm, GOGETTER, Download, Variant #5
A106-443	Web Shell Activity - REGEORG.NEO, Initial Connection, Variant #1
A106-440	Malicious File Transfer - CADDYWIPER, Download, Variant #6
A106-438	Host CLI - Sandworm, GOGETTER, Systemd Service
A106-446	Host CLI - Sandworm, CADDYWIPER, Scheduled Task, Variant #2
A106-439	Host CLI - Sandworm, CADDYWIPER, Scheduled Task, Variant #1
A106-437	Protected Theater - CADDYWIPER, Execution, Variant #2
S100-280	Malicious Activity Scenario - Sandworm Disrupts Power Using a Novel Attack Against Operational Technology Systems