Jun 10 2023

NETMANAGEIT

Intelligence Report

COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises

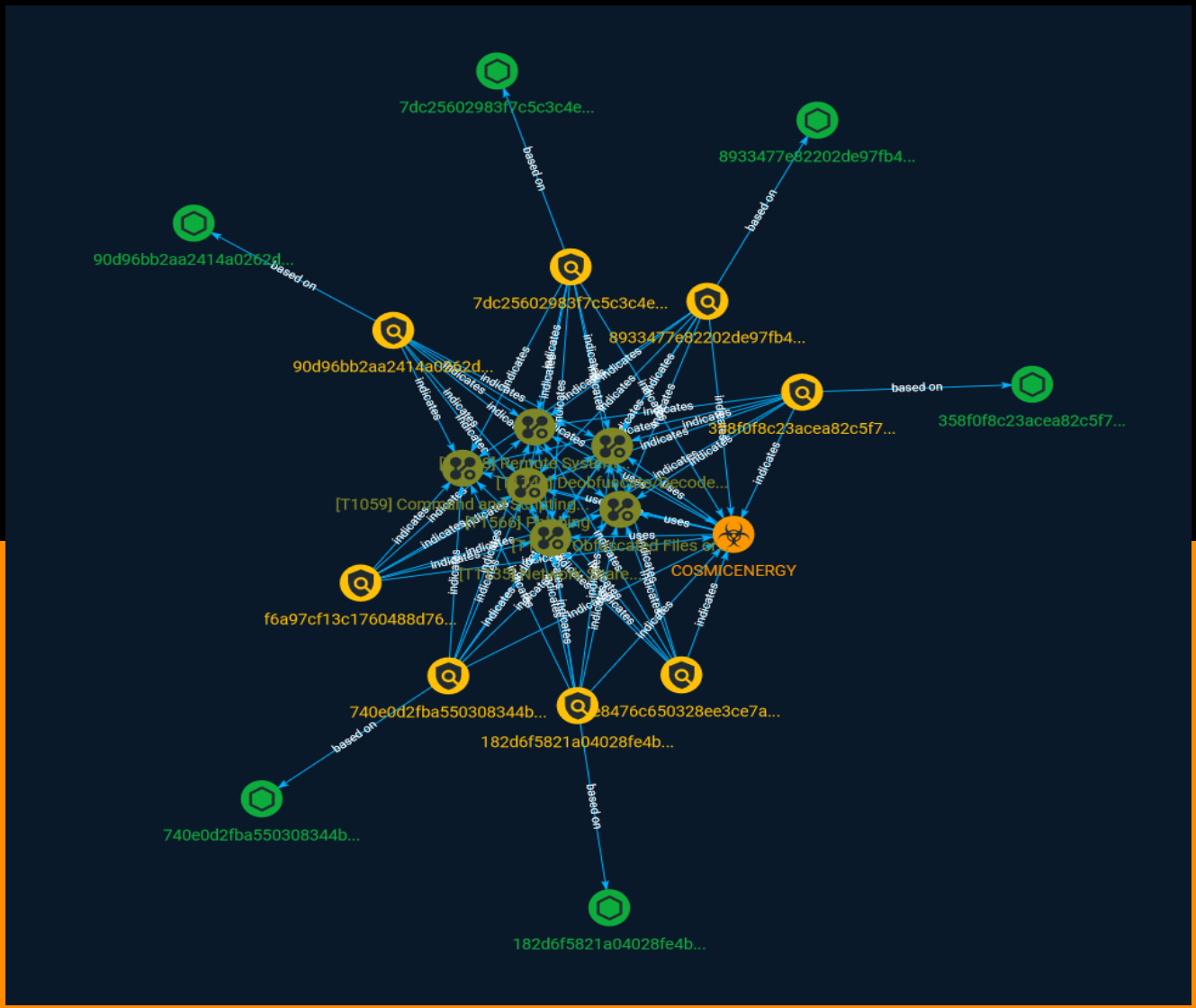

Table of contents

Overview

- Description 3
- Confidence 3

Entities

- Attack-Pattern 4
- Indicator 9
- Malware 13

Observables

- StixFile 14

External References

- External References 15

Overview

Description

Mandiant identified novel operational technology (OT) / industrial control system (ICS)-oriented malware, which we track as COSMICENERGY, uploaded to a public malware scanning utility in December 2021 by a submitter in Russia. The malware is designed to cause electric power disruption by interacting with IEC 60870-5-104 (IEC-104) devices, such as remote terminal units (RTUs), that are commonly leveraged in electric transmission and distribution operations in Europe, the Middle East, and Asia.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Remote System Discovery

ID

T1018

Description

Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or `net view` using [Net](https://attack.mitre.org/software/S0039). Adversaries may also analyze data from local host files (ex: `C:\Windows\System32\Drivers\etc\hosts` or `/etc/hosts`) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment. Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information about systems within a network (e.g. `show cdp neighbors`, `show arp`).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid

detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Command and Scripting Interpreter

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://

attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

Network Share Discovery

ID

T1135

Description

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network. File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the `net view \\\\remotesystem` command. It can also be used to query shared drives on the local system using `net share`. For macOS, the `sharing -l` command lists all shared points used for smb services.

Indicator

Name
358f0f8c23acea82c5f75d6a2de37b6bea7785ed0e32c41109c217c48bf16010
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '358f0f8c23acea82c5f75d6a2de37b6bea7785ed0e32c41109c217c48bf16010']
Name
740e0d2fba550308344b2fb0e5ecfebdd09329bdcfaa909d3357ad4fe5552532
Description
SHA256 of 6eceb78acd1066294d72fe86ed57bf43bc6de6eb
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '740e0d2fba550308344b2fb0e5ecfebdd09329bdcfaa909d3357ad4fe5552532']

Name

7dc25602983f7c5c3c4e81eeb1f2426587b6c1dc6627f20d51007beac840ea2b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7dc25602983f7c5c3c4e81eeb1f2426587b6c1dc6627f20d51007beac840ea2b']

Name

2e8476c650328ee3ce7accf0d24c1aa277f59d82

Description

Searching for PyInstaller files with a custom Python script/module associated with PIEHOP.

Pattern Type

yara

Pattern

rule M_Hunting_PyInstaller_PIEHOP_Module_Strings { meta: author = "Mandiant" date = "2023-04-11" description = "Searching for PyInstaller files with a custom Python script/module associated with PIEHOP." strings: $lib = "iec104_mssql_lib" ascii condition: uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and $lib }

Name

f6a97cf13c1760488d766cd9502b65de954eb047

Description

Searching for strings associated with IEC-104 used in LIGHTWORK.

Pattern Type

yara

Pattern

rule M_Hunting_Disrupt_LIGHTWORK_Strings { meta: author = "Mandiant" description = "Searching for strings associated with IEC-104 used in LIGHTWORK." date = "2023-04-19" strings: $s1 = "Connecting to: %s:%i\n" ascii wide nocase $s2 = "Connected!" ascii wide nocase $s3 = "Send control command C_SC_NA_1" ascii wide nocase $s4 = "Connect failed!" ascii wide nocase $s5 = "Send time sync command" ascii wide nocase $s6 = "Wait ..." ascii wide nocase $s7 = "exit 0" ascii wide nocase condition: filesize < 5MB and uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550 and all of them }

Name

8933477e82202de97fb41f4cbbe6af32596cec70b5b47da022046981c01506a7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8933477e82202de97fb41f4cbbe6af32596cec70b5b47da022046981c01506a7']

Name

182d6f5821a04028fe4b603984b4d33574b7824105142b722e318717a688969e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '182d6f5821a04028fe4b603984b4d33574b7824105142b722e318717a688969e']

Name

90d96bb2aa2414a0262d38cc805122776a9405efece70beeebf3f0bcfc364c2d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90d96bb2aa2414a0262d38cc805122776a9405efece70beeebf3f0bcfc364c2d']

Malware

Name
COSMICENERGY

StixFile

Value
7dc25602983f7c5c3c4e81eeb1f2426587b6c1dc6627f20d51007beac840ea2b
358f0f8c23acea82c5f75d6a2de37b6bea7785ed0e32c41109c217c48bf16010
90d96bb2aa2414a0262d38cc805122776a9405efece70beeebf3f0bcfc364c2d
8933477e82202de97fb41f4cbbe6af32596cec70b5b47da022046981c01506a7
182d6f5821a04028fe4b603984b4d33574b7824105142b722e318717a688969e
740e0d2fba550308344b2fb0e5ecfebdd09329bdcfaa909d3357ad4fe5552532

External References

- https://otx.alienvault.com/pulse/6471304f6bea67d687e380d6
- https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response