Cyber Threat Intelligence
w budowaniu odporności organizacji

Bartosz Różalski

senior product manager ESET \ DAGMA

Digital Security
Progress. Protected.

Bartosz Różalski

senior product manager ESET

@ rozalski.b@dagma.pl LinkedIn

“

If it is written in Python,
it’s probably machine learning.

If it is written in PowerPoint,
it's probably AI.

”

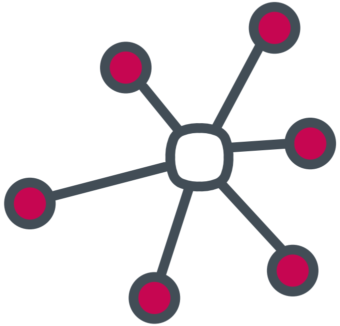
Curt Simon Harlinghausen

MOŻLIWE UŻYCIE SZTUCZNEJ INTELIGENCJI

1. Ochrona zainfekowane węzły w infrastrukturze przestępczej
2. Tworzenie fałszywych alarmów
3. Mechanizmy samozniszczenia w złośliwym oprogramowaniu
4. Imitowanie ruchu sieciowego naśladujące wzorce legalny połączeń
5. Wyszukiwanie najskuteczniejszych technik ataku
6. Wykrywanie nowych podatności dnia-zero

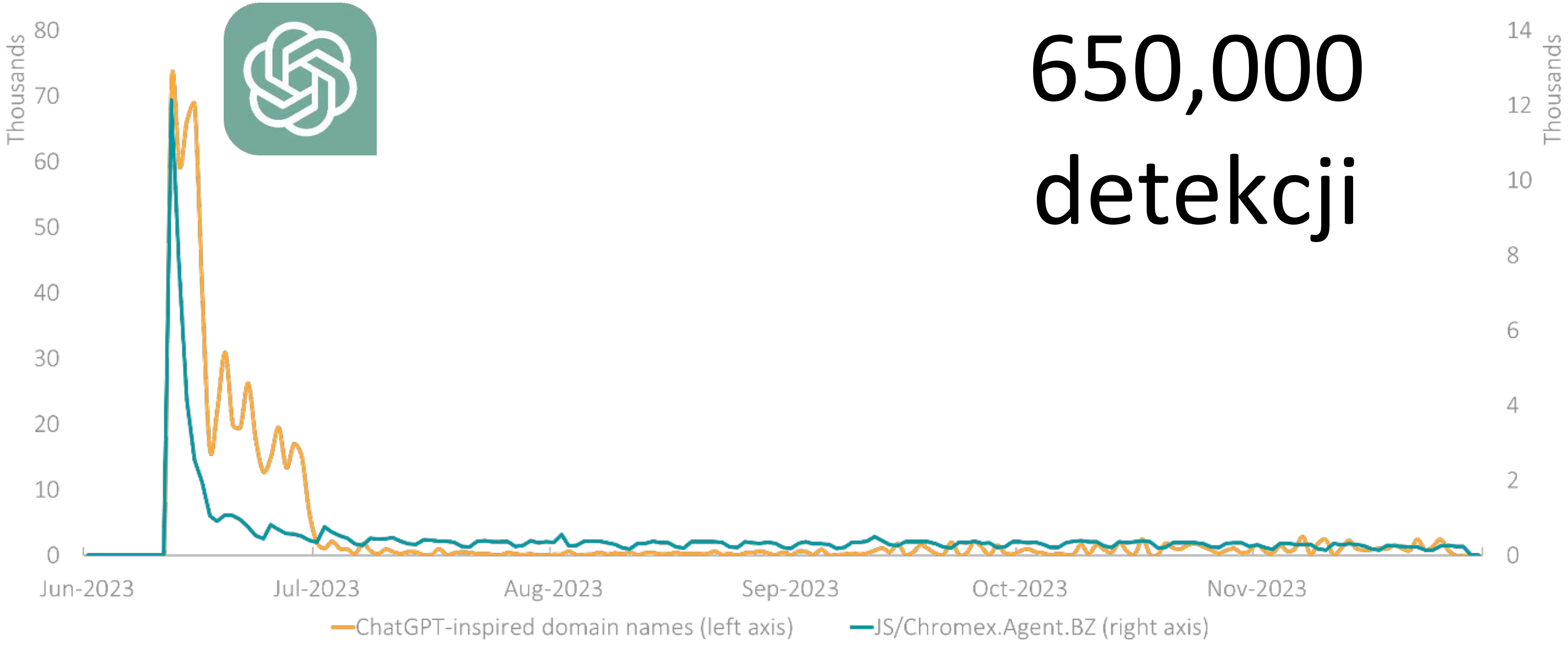
OBSERWOWANE DZIAŁANIA CYBERPRZESTĘPCZYCH

1. Generowanie i ulepszanie malware
2. Unikanie detekcji systemów zabezpieczających
3. Tworzenie deepfake
4. Tworzenie i udoskonalanie kampanii phishingowych



ChatGPT (jako przynęta)

Złośliwe domeny używające „ChatGPT”...



650,000 detekcji

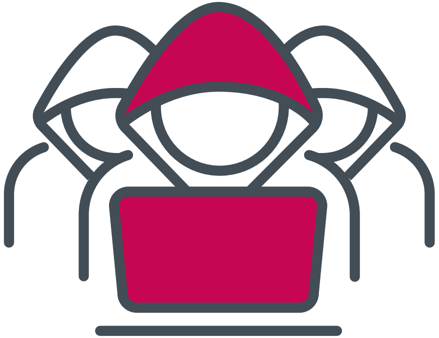
- **Detections of malicious ChatGPT-inspired domain names and JS/Chromex.Agent.BZ** in H2 2023, seven-day moving average

CYBER THREAT INTELLIGENCE

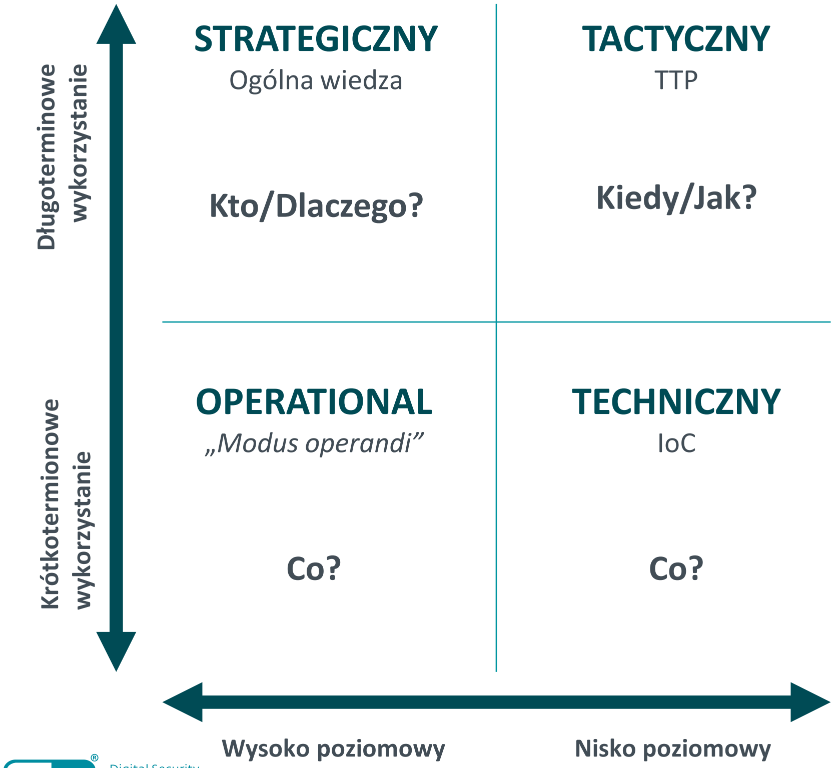
KTO STOI ZA KAMPANIAMI?

JAK PRZEBIEGAJĄ?

CO I KTO JEST ICH CELEM?



RODZAJE ORAZ ADRESACI CTI



Długoterminowe wykorzystanie

Krótkotermionowe wykorzystanie

STRATEGICZNY

Ogólna wiedza

Kto/Dlaczego?

TACTYCZNY

TTP

Kiedy/Jak?

OPERATIONAL

„Modus operandi”

Co?

TECHNICZNY

IoC

Co?

Wysoko poziomowy

Nisko poziomowy

- Zespół SOC, NOC,CSRIT
- Zespół DFIR
- Red team/ Blue team
- Zespół administratorów IT
- Zespół zarządzania podatnościami
- Zespół Threat Huntingu
- Zespół PR
- Zespół GRC
- Działy biznesowe
- C-level

WYBRANE ŹRÓDŁA DANYCH DLA CTI

- ISAC
- CERT/CSRIT
- Baza podatności CVE
- CISA, ENISA, MITRE
- Informacje z własnej infrastukrtury (np. honeypoty, sandboxy)
- Dark web
- Media branżowe
- Raporty dostawców CTI

● **HEADQUARTERS**

Bratislava

● **REGIONAL CENTERS**

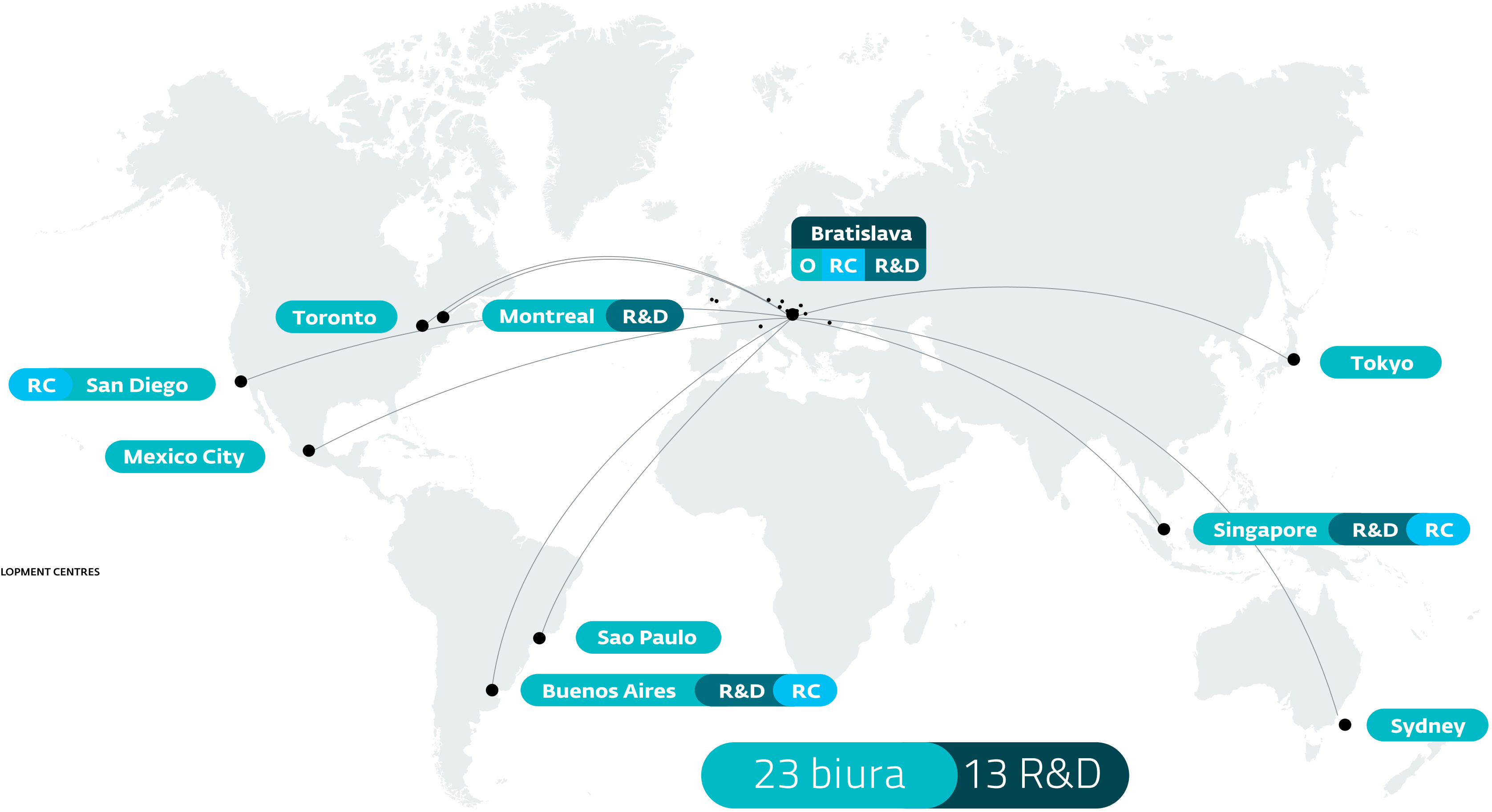
San Diego
Buenos Aires
Singapore

● **OFFICES**

Prague
Jablonec nad Nisou
Sao Paulo
Jena
Krakow
Sydney
Taunton
Bournemouth
Toronto
Montreal
Iași
Mexico City
Zilina
Brno
Tokyo
Milan

● **RESEARCH AND DEVELOPMENT CENTRES**

Bratislava
San Diego
Buenos Aires
Singapore
Prague
Košice
Krakow
Montreal
Zilina
Iași
Brno
Taunton



23 biura 13 R&D

Sandworm uses a ne
version of ArguePat
attack targets in Uk

Europe's quest
independence – and how
cyber-risks come into play

Soaring energy prices and increased geopolitical tensions amid the Russian invasion of Ukraine bring a sharp focus on European energy security

André Lameiras James Shepperd

29 Mar 2022 - 11:30AM

Industroyer: A cyber-wea
that brought down a p
grid

five year

welivesecurity BY eset

HermeticWiper: New data-wiping malware hits Ukraine

undreds of computers in Ukraine compromised just ho
umber of Ukrainian websites

Editor

b 2022 - 10:32AM

Critical infrastru
cyberattack for
you mi

vesecurity BY eset

CaddyWiper: New wiper malware discovered in Ukraine

third time in as many weeks that ESET researchers have spotted previously
aim at Ukrainian organizations

pause

100 days of war in
How the conflict is
out in cyberspace

It's been 100 days since Russia invaded Ukraine, and we
the conflict

welivesecurity BY eset

Menu

Industroyer2: Industro
reloaded

This ICS-capable malware targets a Ukrainian energy company

ESET Research

12 Apr 2022 - 11:28AM

welivesecurity BY eset

Menu

I see what you did there: A look at the CloudMensis macOS spyware

Previously unknown macOS malware uses cloud storage as its C&C channel and to exfiltrate documents, keystrokes, and screen captures from compromised Macs

Marc-Etienne M.Léveillé

19 Jul 2022 - 11:30AM

orga
BY eset

Digital Security
Progress. Protected.

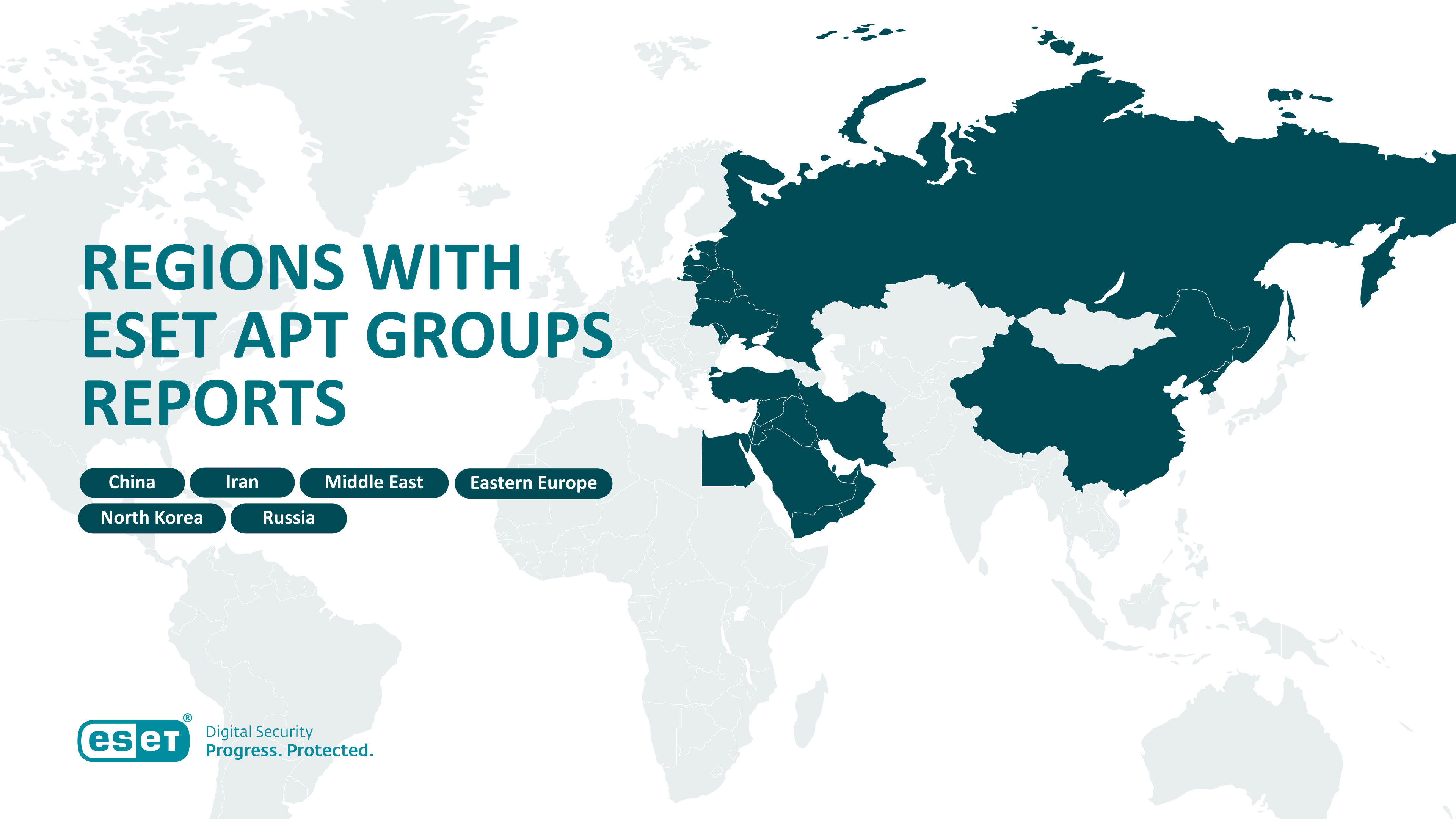
APT Activity Report

GOVERNMENT ESPIONAGE AND UNPATCHED VULNERABILITIES

April 2023 – September 2023

(eset):research

REGIONS WITH ESET APT GROUPS REPORTS



China

Iran

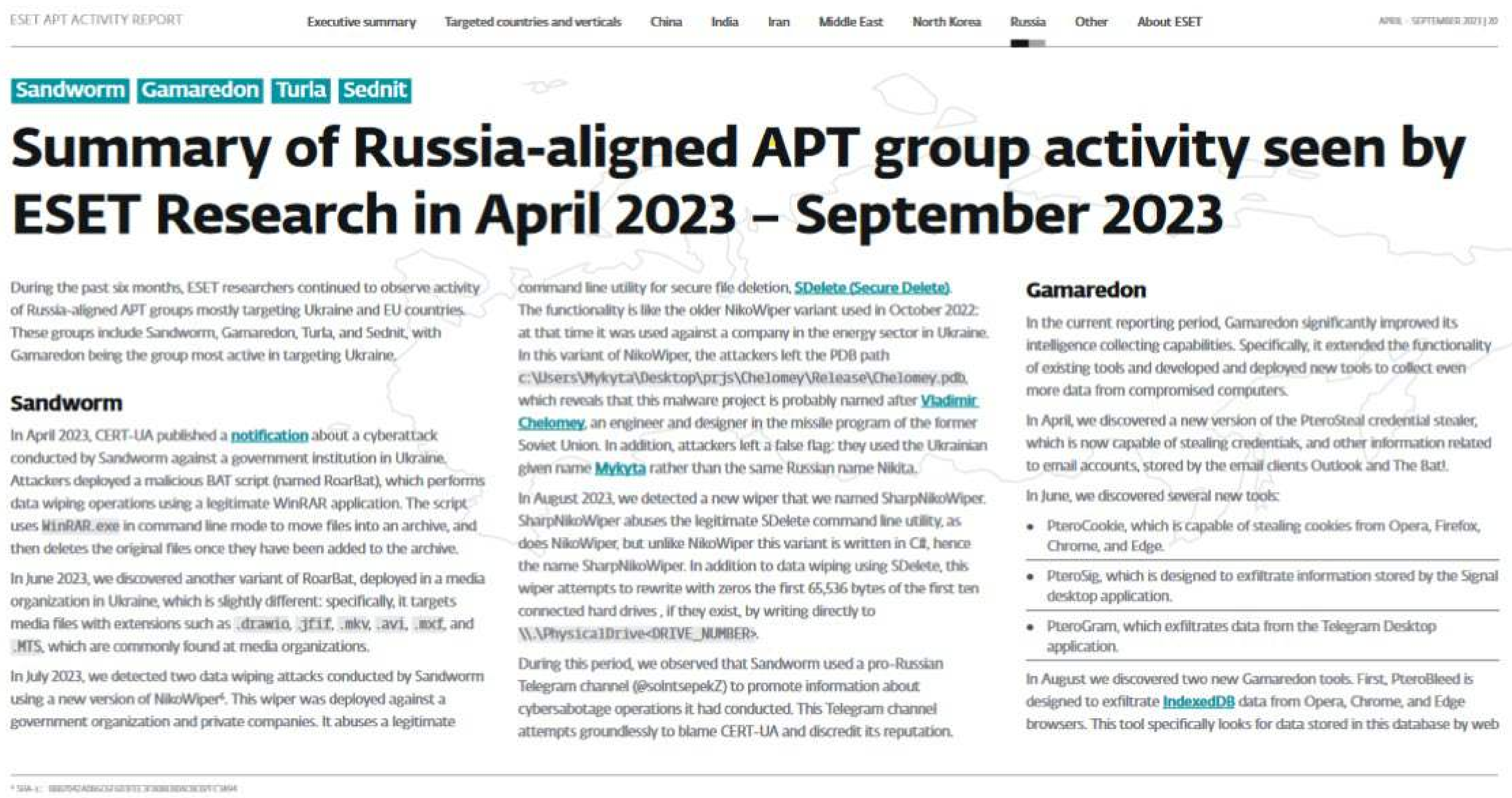
Middle East

Eastern Europe

North Korea

Russia

Digital Security
Progress. Protected.



ESET APT ACTIVITY REPORT | Executive summary | Targeted countries and verticals | China | India | Iran | Middle East | North Korea | Russia | Other | About ESET | APRIL – SEPTEMBER 2023 | 20

Sandworm Gamaredon Turla Sednit

Summary of Russia-aligned APT group activity seen by ESET Research in April 2023 – September 2023

During the past six months, ESET researchers continued to observe activity of Russia-aligned APT groups mostly targeting Ukraine and EU countries. These groups include Sandworm, Gamaredon, Turla, and Sednit, with Gamaredon being the group most active in targeting Ukraine.

Sandworm

In April 2023, CERT-UA published a notification about a cyberattack conducted by Sandworm against a government institution in Ukraine. Attackers deployed a malicious BAT script (named RoarBat), which performs data wiping operations using a legitimate WinRAR application. The script uses `WinRAR.exe` in command line mode to move files into an archive, and then deletes the original files once they have been added to the archive.

In June 2023, we discovered another variant of RoarBat, deployed in a media organization in Ukraine, which is slightly different: specifically, it targets media files with extensions such as `.drawio`, `.jfif`, `.mkv`, `.avi`, `.mxf`, and `.MTS`, which are commonly found at media organizations.

In July 2023, we detected two data wiping attacks conducted by Sandworm using a new version of NikoWiper[4]. This wiper was deployed against a government organization and private companies. It abuses a legitimate command line utility for secure file deletion, SDelete (Secure Delete). The functionality is like the older NikoWiper variant used in October 2022: at that time it was used against a company in the energy sector in Ukraine. In this variant of NikoWiper, the attackers left the PDB path `C:\Users\Mykyta\Desktop\prjs\Chelomey\Release\Chelomey.pdb`, which reveals that this malware project is probably named after Vladimir Chelomey, an engineer and designer in the missile program of the former Soviet Union. In addition, attackers left a false flag: they used the Ukrainian given name Mykyta rather than the same Russian name Nikita.

In August 2023, we detected a new wiper that we named SharpNikoWiper. SharpNikoWiper abuses the legitimate SDelete command line utility, as does NikoWiper, but unlike NikoWiper this variant is written in C#, hence the name SharpNikoWiper. In addition to data wiping using SDelete, this wiper attempts to rewrite with zeros the first 65,536 bytes of the first ten connected hard drives , if they exist, by writing directly to `\\.\PhysicalDrive<DRIVE_NUMBER>`.

During this period, we observed that Sandworm used a pro-Russian Telegram channel (@solntsepekZ) to promote information about cybersabotage operations it had conducted. This Telegram channel attempts groundlessly to blame CERT-UA and discredit its reputation.

Gamaredon

In the current reporting period, Gamaredon significantly improved its intelligence collecting capabilities. Specifically, it extended the functionality of existing tools and developed and deployed new tools to collect even more data from compromised computers.

In April, we discovered a new version of the PteroSteal credential stealer, which is now capable of stealing credentials, and other information related to email accounts, stored by the email clients Outlook and The Bat!.

In June, we discovered several new tools:

- PteroCookie, which is capable of stealing cookies from Opera, Firefox, Chrome, and Edge.
- PteroSig, which is designed to exfiltrate information stored by the Signal desktop application.
- PteroGram, which exfiltrates data from the Telegram Desktop application.

In August we discovered two new Gamaredon tools. First, PteroBleed is designed to exfiltrate IndexedDB data from Opera, Chrome, and Edge browsers. This tool specifically looks for data stored in this database by web

[4] SHA-1: [illegible]

ESET: APT Activity Report April 2023 – September 2023

https://www.eset.com/fileadmin/ESET/INT/B2B_Resource_centrum/Reports/ESET_APT_Activity_Report_Q2_2023-Q3_2023.pdf

ESET THREAT INTELLIGENCE

ESET udostępnia **informacje i dane** w podstaci Data Feeds.

Format **JSON i STIX** v2.0

TAXII serwer, updatowany kilkukrotnie każdej godziny

Indicators of Compromise (**IoCs**)

Gotowe integracje z platformami Threat Intelligence Platforms

Botnet Feed

Domain Feed

URL Feed

Malicious Files Feed

IP Feed

APT Feed

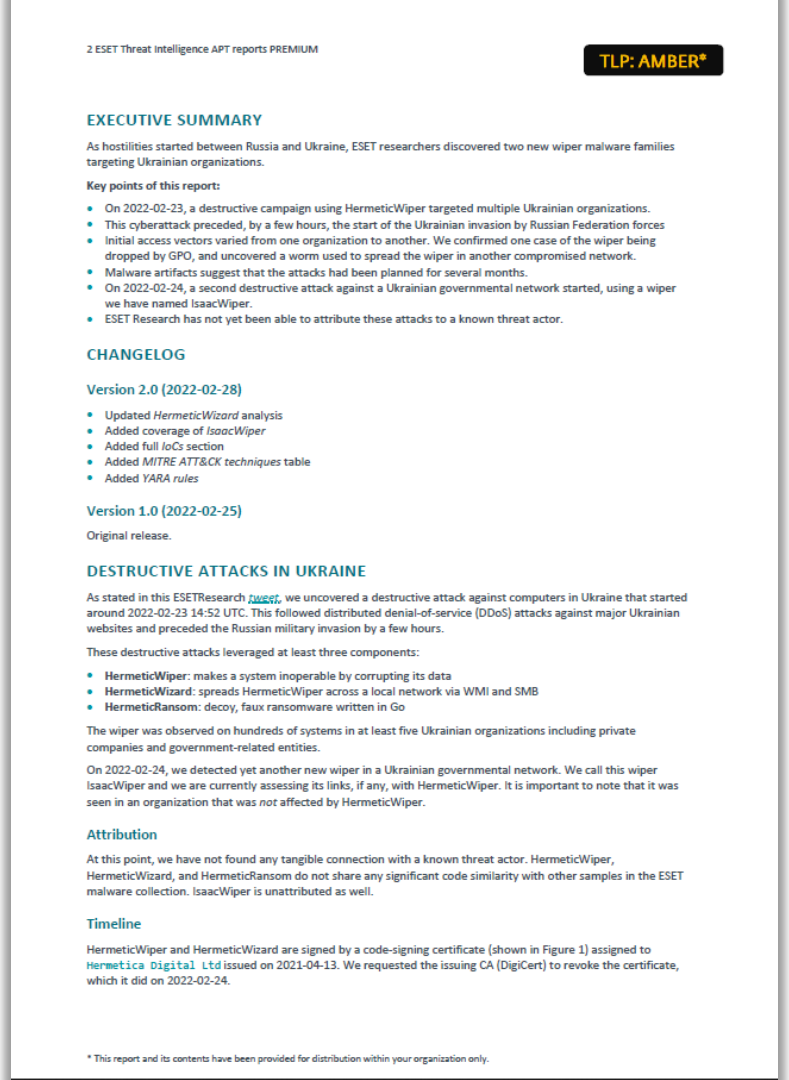
MONTHLY DIGEST

MONTHLY OVERVIEW

ACTIVITY SUMMARY

TECHNICAL ANALYSIS

Hello Zebrocy, my old friend



TLP: AMBER*

EXECUTIVE SUMMARY

As hostilities started between Russia and Ukraine, ESET researchers discovered two new wiper malware families targeting Ukrainian organizations.

Key points of this report:

- On 2022-02-23, a destructive campaign using HermeticWiper targeted multiple Ukrainian organizations.
- This cyberattack preceded, by a few hours, the start of the Ukrainian invasion by Russian Federation forces
- Initial access vectors varied from one organization to another. We confirmed one case of the wiper being dropped by GPO, and uncovered a worm used to spread the wiper in another compromised network.
- Malware artifacts suggest that the attacks had been planned for several months.
- On 2022-02-24, a second destructive attack against a Ukrainian governmental network started, using a wiper we have named IsaacWiper.
- ESET Research has not yet been able to attribute these attacks to a known threat actor.

CHANGELOG

Version 2.0 (2022-02-28)

- Updated *HermeticWizard* analysis
- Added coverage of *IsaacWiper*
- Added full *IoCs* section
- Added *MITRE ATT&CK techniques* table
- Added *YARA rules*

Version 1.0 (2022-02-25)

Original release.

DESTRUCTIVE ATTACKS IN UKRAINE

As stated in this ESETResearch *tweet*, we uncovered a destructive attack against computers in Ukraine that started around 2022-02-23 14:52 UTC. This followed distributed denial-of-service (DDoS) attacks against major Ukrainian websites and preceded the Russian military invasion by a few hours.

These destructive attacks leveraged at least three components:

- **HermeticWiper**: makes a system inoperable by corrupting its data
- **HermeticWizard**: spreads HermeticWiper across a local network via WMI and SMB
- **HermeticRansom**: decoy, faux ransomware written in Go

The wiper was observed on hundreds of systems in at least five Ukrainian organizations including private companies and government-related entities.

On 2022-02-24, we detected yet another new wiper in a Ukrainian governmental network. We call this wiper IsaacWiper and we are currently assessing its links, if any, with HermeticWiper. It is important to note that it was seen in an organization that was *not* affected by HermeticWiper.

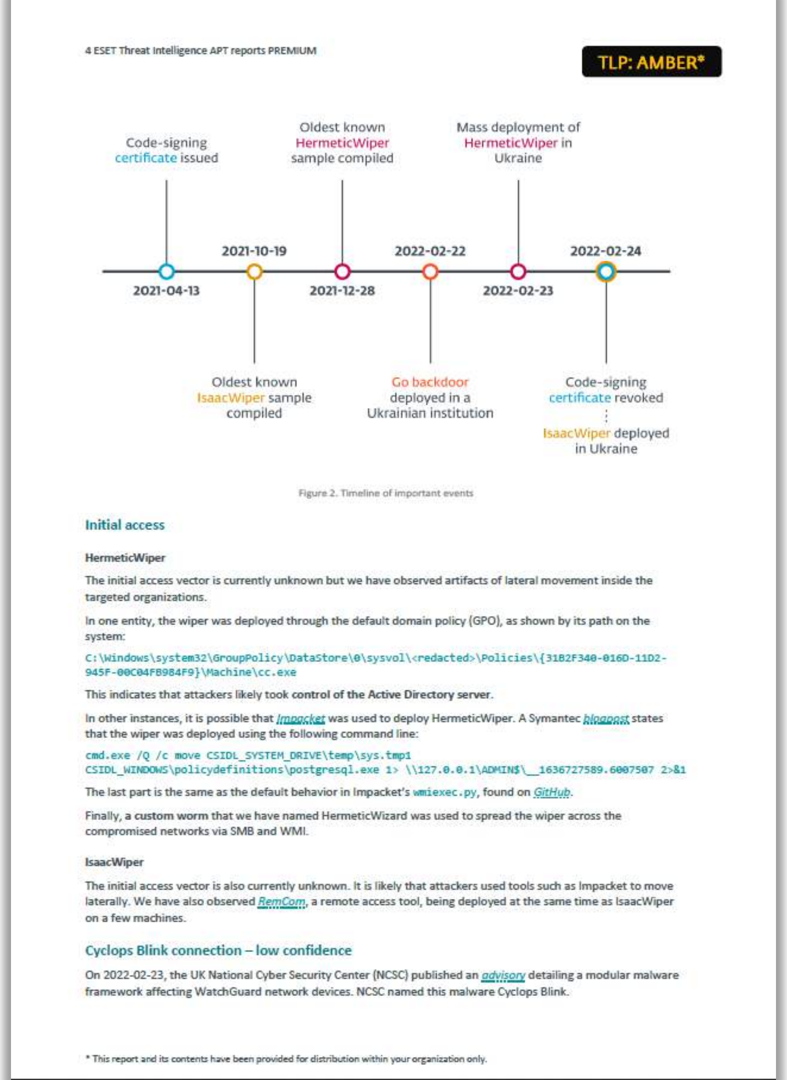
Attribution

At this point, we have not found any tangible connection with a known threat actor. HermeticWiper, HermeticWizard, and HermeticRansom do not share any significant code similarity with other samples in the ESET malware collection. IsaacWiper is unattributed as well.

Timeline

HermeticWiper and HermeticWizard are signed by a code-signing certificate (shown in Figure 1) assigned to `Hermetica Digital Ltd` issued on 2021-04-13. We requested the issuing CA (DigiCert) to revoke the certificate, which it did on 2022-02-24.

* This report and its contents have been provided for distribution within your organization only.



TLP: AMBER*

Code-signing certificate issued
2021-04-13
2021-10-19
Oldest known IsaacWiper sample compiled
Oldest known HermeticWiper sample compiled
2021-12-28
2022-02-22
Go backdoor deployed in a Ukrainian institution
Mass deployment of HermeticWiper in Ukraine
2022-02-23
2022-02-24
Code-signing certificate revoked
IsaacWiper deployed in Ukraine

Figure 2. Timeline of important events

Initial access

HermeticWiper

The initial access vector is currently unknown but we have observed artifacts of lateral movement inside the targeted organizations.

In one entity, the wiper was deployed through the default domain policy (GPO), as shown by its path on the system:

```
C:\Windows\system32\GroupPolicy\DataStore\0\sysvol\<redacted>\Policies\{31B2F340-016D-11D2-
945F-00C04FB984F9}\Machine\cc.exe
```

This indicates that attackers likely took **control of the Active Directory server**.

In other instances, it is possible that *Impacket* was used to deploy HermeticWiper. A Symantec *blogpost* states that the wiper was deployed using the following command line:

```
cmd.exe /Q /c move CSIDL_SYSTEM_DRIVE\temp\sys.tmp1
CSIDL_WINDOWS\policydefinitions\postgresql.exe 1> \\127.0.0.1\ADMIN$\__1636727589.6007507 2>&1
```

The last part is the same as the default behavior in Impacket's `wmiexec.py`, found on *GitHub*.

Finally, **a custom worm** that we have named HermeticWizard was used to spread the wiper across the compromised networks via SMB and WMI.

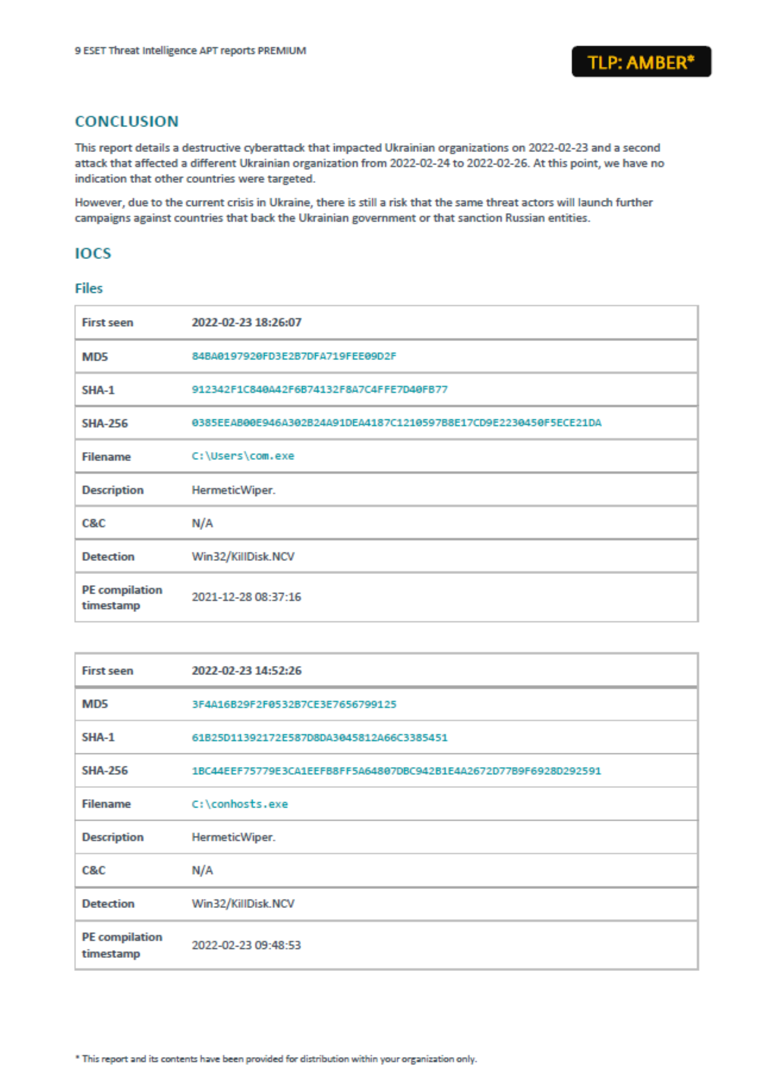
IsaacWiper

The initial access vector is also currently unknown. It is likely that attackers used tools such as Impacket to move laterally. We have also observed *RemCom*, a remote access tool, being deployed at the same time as IsaacWiper on a few machines.

Cyclops Blink connection – low confidence

On 2022-02-23, the UK National Cyber Security Center (NCSC) published an *advisory* detailing a modular malware framework affecting WatchGuard network devices. NCSC named this malware Cyclops Blink.

* This report and its contents have been provided for distribution within your organization only.



CONCLUSION

This report details a destructive cyberattack that impacted Ukrainian organizations on 2022-02-23 and a second attack that affected a different Ukrainian organization from 2022-02-24 to 2022-02-26. At this point, we have no indication that other countries were targeted.

However, due to the current crisis in Ukraine, there is still a risk that the same threat actors will launch further campaigns against countries that back the Ukrainian government or that sanction Russian entities.

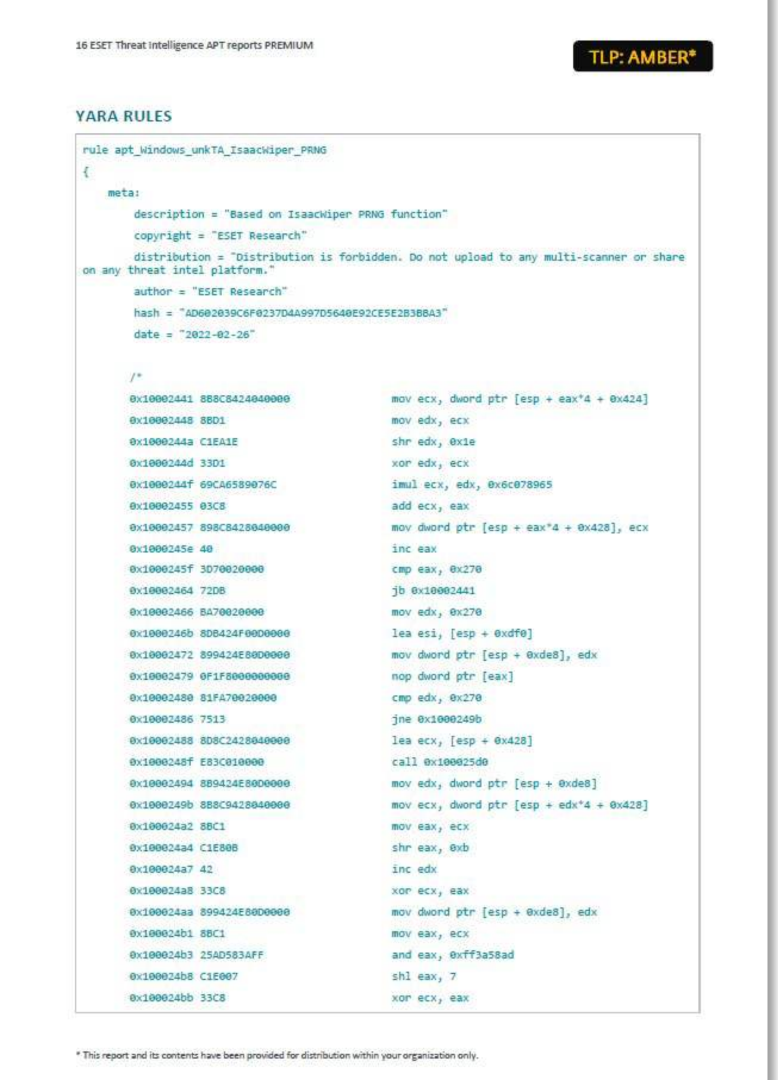
IOCS

Files

First seen	**2022-02-23 18:26:07**
MD5	`84BA0197920FD3E2B7DFA719FEE09D2F`
SHA-1	`912342F1C840A42F6B74132F8A7C4FFE7D40FB77`
SHA-256	`0385EEAB00E946A302B24A91DEA4187C1210597B8E17CD9E2230450F5ECE21DA`
Filename	`C:\Users\com.exe`
Description	HermeticWiper.
C&C	N/A
Detection	Win32/KillDisk.NCV
PE compilation timestamp	2021-12-28 08:37:16

First seen	**2022-02-23 14:52:26**
MD5	`3F4A16B29F2F0532B7CE3E7656799125`
SHA-1	`61B25D11392172E587D8DA3045812A66C3385451`
SHA-256	`1BC44EEF75779E3CA1EEFB8FF5A64807DBC942B1E4A2672D77B9F6928D292591`
Filename	`C:\conhosts.exe`
Description	HermeticWiper.
C&C	N/A
Detection	Win32/KillDisk.NCV
PE compilation timestamp	2022-02-23 09:48:53

* This report and its contents have been provided for distribution within your organization only.



YARA RULES

```
rule apt_Windows_unkTA_IsaacWiper_PRNG
{
    meta:
        description = "Based on IsaacWiper PRNG function"
        copyright = "ESET Research"
        distribution = "Distribution is forbidden. Do not upload to any multi-scanner or share
on any threat intel platform."
        author = "ESET Research"
        hash = "AD602039C6F0237D4A997D5640E92CE5E2B3BBA3"
        date = "2022-02-26"

        /*
        0x10002441 8B8C8424040000               mov ecx, dword ptr [esp + eax*4 + 0x424]
        0x10002448 8BD1                         mov edx, ecx
        0x1000244a C1EA1E                       shr edx, 0x1e
        0x1000244d 33D1                         xor edx, ecx
        0x1000244f 69CA6589076C                 imul ecx, edx, 0x6c078965
        0x10002455 03C8                         add ecx, eax
        0x10002457 898C8428040000               mov dword ptr [esp + eax*4 + 0x428], ecx
        0x1000245e 40                           inc eax
        0x1000245f 3D70020000                   cmp eax, 0x270
        0x10002464 72DB                         jb 0x10002441
        0x10002466 BA70020000                   mov edx, 0x270
        0x1000246b 8DB424F00D0000               lea esi, [esp + 0xdf0]
        0x10002472 899424E80D0000               mov dword ptr [esp + 0xde8], edx
        0x10002479 0F1F8000000000               nop dword ptr [eax]
        0x10002480 81FA70020000                 cmp edx, 0x270
        0x10002486 7513                         jne 0x1000249b
        0x10002488 8D8C2428040000               lea ecx, [esp + 0x428]
        0x1000248f E83C010000                   call 0x100025d0
        0x10002494 8B9424E80D0000               mov edx, dword ptr [esp + 0xde8]
        0x1000249b 8B8C9428040000               mov ecx, dword ptr [esp + edx*4 + 0x428]
        0x100024a2 8BC1                         mov eax, ecx
        0x100024a4 C1E80B                       shr eax, 0xb
        0x100024a7 42                           inc edx
        0x100024a8 33C8                         xor ecx, eax
        0x100024aa 899424E80D0000               mov dword ptr [esp + 0xde8], edx
        0x100024b1 8BC1                         mov eax, ecx
        0x100024b3 25AD583AFF                   and eax, 0xff3a58ad
        0x100024b8 C1E007                       shl eax, 7
        0x100024bb 33C8                         xor ecx, eax
```

* This report and its contents have been provided for distribution within your organization only.

SED CLOUD &
PENTERA
FORTIN
OME
eset
PROTECT
ELITE
All-in-one prevention, detection & response com
enterprise-grade XDR with complete multilayere