



**SECURITY
DAYS**

DEMO. ESET THREAT INTELLIGENCE - BŪKITE VEIKSMO FILMO HEROJUS

Lukas Apynis - Baltimax kibernetinio
saugumo inžinierius, ESET ekspertas

Rugsėjo 5 d. 2024

KIBERNETINIO SAUGUMO KONFERENCIJA

esd.eset.lt

KAIP GAUTI KIBERNETINIŲ GRĖSMIŲ ŽVALGYBOS INFORMACIJĄ?



FORMOS

Duomenys, ataskaitos, konsultacijos.



ŠALTINIAI

OSINT, MITRE ATT&CK[®], komerciniai grėsmių kanalai, forumai ir ataskaitos.



NEMOKAMI IR MOKAMI

Nemokami: užima daug laiko, nėra išsamūs.

Mokami: gamintojas viskuo pasirūpina.



THREAT INTELLIGENCE

The latest intelligence from the top industry experts

REGIONAL CENTERS

- BRATISLAVA
- 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 CENTERS

- BRATISLAVA
- BUENOS AIRES
- SINGAPORE
- PRAGUE
- KOSICE
- KRAKOW
- MONTREAL
- ZILINA
- IAȘI
- BRNO
- TAUNTON





ESET THREAT RESEARCH

Recognized research & discoveries serving cybersecurity

800+

Technology professionals

12

Research & Development
centers worldwide

300k+

Unique, new malware samples
detected every day

1 billion+

People worldwide protected

DASHBOARD

18 ALL REPORTS

18 APT REPORTS

10 SAMPLE REPORTS DEMO

5 BOTNET REPORTS DEMO

2 CERTIFICATE REPORTS DEMO

4 PHISHING REPORTS DEMO

11 TARGETED REPORTS DEMO

YARA RULESETS DEMO

YARA MATCHES DEMO

TAXII FEEDS

MISP

Dashboard

WeLiveSecurity Feed

2024-08-02 11:30

▶ **AI and automation reducing breach costs – Week in security with Tony Anscombe**

Organizations that leveraged AI and automation in security prevention cut the cost of a data breach by \$2.22 million compared to those that didn't deploy these technologies

2024-07-31 09:00

▶ **The cyberthreat that drives businesses towards cyber risk insurance**

Many smaller organizations are turning to cyber risk insurance, both to protect against the cost of a cyber incident and to use the extensive post-incident services that insurers provide

2024-07-26 11:57

▶ **Telegram for Android hit by a zero-day exploit – Week in security with Tony Anscombe**

Attackers abusing the "EvilVideo" vulnerability could share malicious Android payloads via Telegram channels, groups, and chats, all while making them appear as legitimate multimedia files

2024-07-29 09:00

▶ **Beware of fake AI tools masking very real malware threats**

Ever attuned to the latest trends, cybercriminals distribute malicious tools that pose as ChatGPT, Midjourney and other generative AI assistants

Podcasts

2024-06-10 09:05

▶ **APT Activity Report Q4 2023-Q1 2024: I-SOON, FishMonger, and MuddyWater**

The I-SOON data leak has allowed us to identify FishMonger, a group notorious for the cyberattacks against Hong Kong universities back in 2019, as I-SOON. This contractor also developed a platform for tracking gambling activity, linking the ...

2024-01-31 10:00

▶ **Threat Report H2 2023: ChatGPT, the MOVEit hack, and Pandora**

In 2023, ESET detected over 675,000 attempts to access malicious domains abusing the popularity of ChatGPT; some offer bring-your-own-key web apps that can steal OpenAI API keys. Apart from AI, in H2 the C10p ransomware gang exploited MOVEi...

2023-12-18 09:00

▶ **Neanderthals, Mammoths and Telekopye**

In this episode, ESET researchers Radek Jizba and Jakub Souček talk about the dynamics within and between various Neanderthal groups, the techniques that this horde of scammers uses to find the best Mammoths, and especially about ...

2023-09-12 08:00

▶ **Threat Report H1 2023: Sextortion, usury and brute-force**

In H1 2023, intrusion vectors were closing left and right. This forced many cybercriminals to search for alternative ways to compromise devices of their victims. While some of the attackers tried revisiting old routes such as brute-forcing MS SQ...

Posts from @ESETresearch

Follow



ESET Research @ESETresearch · Jul 31

Replying to @ESETresearch

To find out more, read the full #ESETThreatReport: welivesecurity.com/en/eset-resear... 3/3



welivesecurity.com
ESET Threat Report H1 2024
A view of the H1 2024 threat landscape as

4



ESET Research @ESETresearch · Jul 31

Replying to @ESETresearch

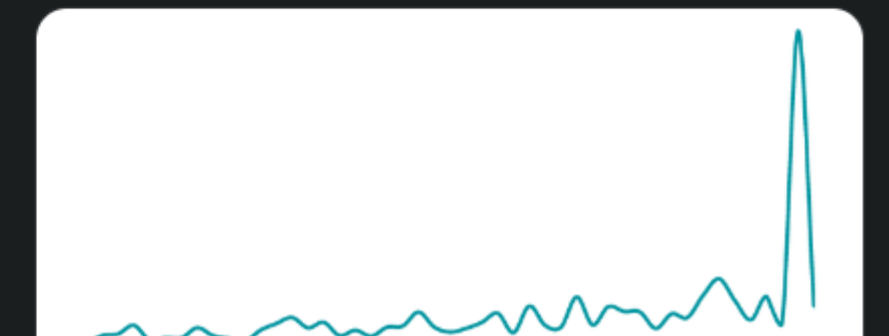
Although we have observed two notable LockBit campaigns in H1 2024, these were the result of non-LockBit gangs using the LockBit builder leaked in September 2022. 2/3

4



ESET Research @ESETresearch · Jul 31

#ESETResearch telemetry corroborates that the #LockBit gang, formerly the leading #ransomware threat, has been struggling to survive ever since Operation Chronos, a global disruption conducted by law enforcement in February 2024. 1/3



Last Reports

NAME	STATUS	REPORT TYPE
[REDACTED]	✔ Published	APT Report
[REDACTED]	✔ Published	APT Report
[REDACTED]	✔ Published	APT Report
[REDACTED]	✔ Published	APT Report
[REDACTED]	✔ Published	APT Report

Submit Feedback

COLLAPSE

- 18 DASHBOARD
 - 18 ALL REPORTS
 - 18 APT REPORTS
 - 10 SAMPLE REPORTS DEMO
 - 5 BOTNET REPORTS DEMO
 - 2 CERTIFICATE REPORTS DEMO
 - 4 PHISHING REPORTS DEMO
 - 11 TARGETED REPORTS DEMO
 - YARA RULESETS DEMO
 - YARA MATCHES DEMO
 - TAXII FEEDS
 - MISP
- [Submit Feedback](#)
- COLLAPSE

Dashboard

WeLiveSecurity Feed

- 2024-08-02 11:30

[AI and automation reducing breach costs – Week in security with Tony Anscombe](#)

Organizations that leveraged AI and automation in security prevention cut the cost of a data breach by \$2.22 million compared to those that didn't deploy these technologies
- 2024-07-31 09:00

[The cyberthreat that drives businesses towards cyber risk insurance](#)

Many smaller organizations are turning to cyber risk insurance, both to protect against the cost of a cyber incident and to use the extensive post-incident services that insurers provide
- 2024-07-26 11:57

[Telegram for Android hit by a zero-day exploit – Week in security with Tony Anscombe](#)

Attackers abusing the "EviVideo" vulnerability could share malicious Android payloads via Telegram channels, groups, and chats, all while making them appear as legitimate multimedia files
- 2024-07-29 09:00

[Beware of fake AI tools masking very real malware threats](#)

Ever attuned to the latest trends, cybercriminals distribute malicious tools that pose as ChatGPT, Midjourney and other generative AI assistants

Podcasts

- 2024-06-10 09:05

[APT Activity Report Q4 2023-Q1 2024: I-SOON, FishMonger, and MuddyWater](#)

The I-SOON data leak has allowed us to identify FishMonger, a group notorious for the cyberattacks against Hong Kong universities back in 2019, as I-SOON. This contractor also developed a platform for tracking gambling activity, linking the ...
- 2024-01-31 10:00

[Threat Report H2 2023: ChatGPT, the MOVEit hack, and Pandora](#)

In 2023, ESET detected over 675,000 attempts to access malicious domains abusing the popularity of ChatGPT; some offer bring-your-own-key web apps that can steal OpenAI API keys. Apart from AI, in H2 the ClOp ransomware gang exploited MOVEi...
- 2023-12-18 09:00

[Neanderthals, Mammoths and Telekopye](#)

In this episode, ESET researchers Radek Jizba and Jakub Souček talk about the dynamics within and between various Neanderthal groups, the techniques that this horde of scammers uses to find the best Mammoths, and especially about ...
- 2023-09-12 08:00

[Threat Report H1 2023: Sextortion, usury and brute-force](#)

In H1 2023, intrusion vectors were closing left and right. This forced many cybercriminals to search for alternative ways to compromise devices of their victims. While some of the attackers tried revisiting old routes such as brute-forcing MS SQ...

Last Reports

NAME	STATUS	REPORT TYPE
[REDACTED]	✓ Published	APT Report
[REDACTED]	✓ Published	APT Report
[REDACTED]	✓ Published	APT Report
[REDACTED]	✓ Published	APT Report
[REDACTED]	✓ Published	APT Report


Posts from @ESETresearch

Follow

- ESET Research** @ESETresearch · Jul 31

Replying to @ESETresearch

To find out more, read the full #ESETThreatReport: [welivesecurity.com/en/eset-resear...](#) 3/3



welivesecurity.com
ESET Threat Report H1 2024
A view of the H1 2024 threat landscape as

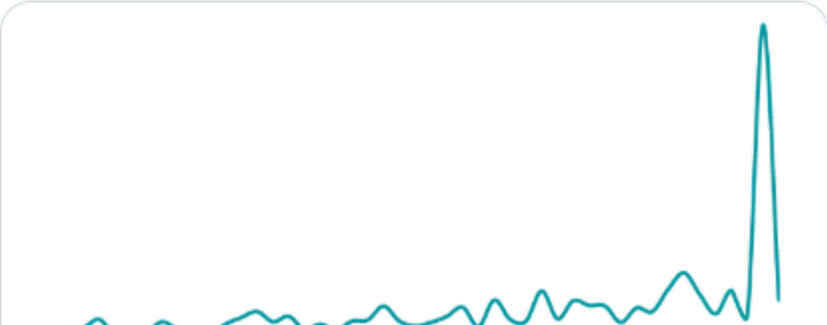
4
- ESET Research** @ESETresearch · Jul 31

Replying to @ESETresearch

Although we have observed two notable LockBit campaigns in H1 2024, these were the result of non-LockBit gangs using the LockBit builder leaked in September 2022. 2/3

4
- ESET Research** @ESETresearch · Jul 31

#ESETresearch telemetry corroborates that the #LockBit gang, formerly the leading #ransomware threat, has been struggling to survive ever since Operation Chronos, a global disruption conducted by law enforcement in February 2024. 1/3



- 18 DASHBOARD
- 18 ALL REPORTS
- 18 APT REPORTS
- 10 SAMPLE REPORTS DEMO
- 5 BOTNET REPORTS DEMO
- 2 CERTIFICATE REPORTS DEMO
- 4 PHISHING REPORTS DEMO
- 11 TARGETED REPORTS DEMO
- YARA RULESETS DEMO
- YARA MATCHES DEMO
- TAXII FEEDS
- MISP

Dashboard

WeLiveSecurity

- [security with Tony](#)
- 2024-06-10 09:05
AI and Anscor
Organic growth of a data technology
- 2024-01-31 10:00
The cyber threats
Many scammers against that insist
- 2024-09-12 08:00
Telegram Anscor
Attacker payload legitim
- 2024-06-10 09:05
Beware
Ever attack as Chat

	STATUS	REPORT TYPE
2024-06-10 09:05	✓ Published	APT Report
2024-01-31 10:00	✓ Published	APT Report
2023-12-18 09:00	✓ Published	APT Report
2023-09-12 08:00	✓ Published	APT Report
2023-09-12 08:00	✓ Published	APT Report

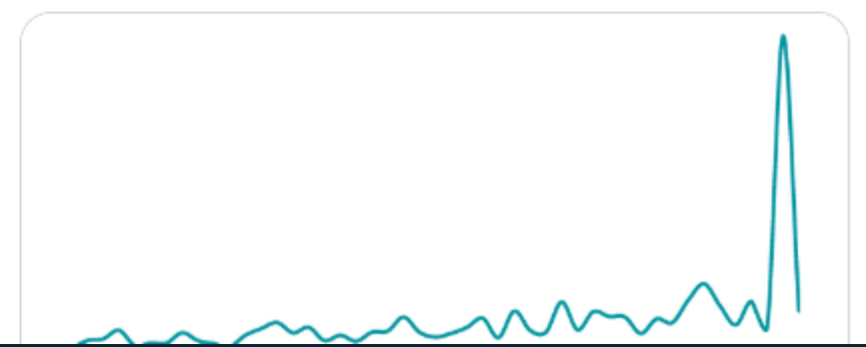
Podcasts

- 2024-06-10 09:05
APT Activity Report Q4 2023-Q1 2024: I-SOON, FishMonger, and MuddyWater
The I-SOON data leak has allowed us to identify FishMonger, a group notorious for the cyberattacks against Hong Kong universities back in 2019, as I-SOON. This contractor also developed a platform for tracking gambling activity, linking the ...
- 2024-01-31 10:00
Threat Report H2 2023: ChatGPT, the MOVEit hack, and Pandora
In 2023, ESET detected over 675,000 attempts to access malicious domains abusing the popularity of ChatGPT; some offer bring-your-own-key web apps that can steal OpenAI API keys. Apart from AI, in H2 the CIOp ransomware gang exploited MOVEi...
- 2023-12-18 09:00
Neanderthals, Mammoths and Telekopye
In this episode, ESET researchers Radek Jizba and Jakub Souček talk about the dynamics within and between various Neanderthal groups, the techniques that this horde of scammers uses to find the best Mammoths, and especially about ...
- 2023-09-12 08:00
Threat Report H1 2023: Sextortion, usury and brute-force
In H1 2023, intrusion vectors were closing left and right. This forced many cybercriminals to search for alternative ways to compromise devices of their victims. While some of the attackers tried revisiting old routes such as brute-forcing MS SQ...

Posts from @ESETresearch

Follow

- ESET Research** @ESETresearch · Jul 31
 Replying to @ESETresearch
 To find out more, read the full #ESETThreatReport: [welivesecurity.com/en/eset-resear...](#) 3/3
- welivesecurity.com
 ESET Threat Report H1 2024
 A view of the H1 2024 threat landscape as
- ESET Research** @ESETresearch · Jul 31
 Replying to @ESETresearch
 Although we have observed two notable LockBit campaigns in H1 2024, these were the result of non-LockBit gangs using the LockBit builder leaked in September 2022. 2/3
- ESET Research** @ESETresearch · Jul 31
 #ESETresearch telemetry corroborates that the #LockBit gang, formerly the leading #ransomware threat, has been struggling to survive ever since Operation Chronos, a global disruption conducted by law enforcement in February 2024. 1/3





DUOMENYS



GREITIS



TIKSLUMAS

KODĖL SVARBI KIBERNETINIŲ GRĖSMIŲ ŽVALGYBA?



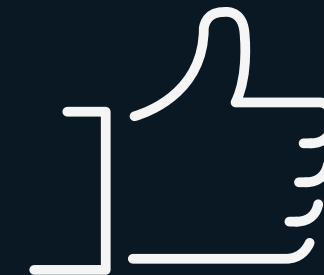
PREVENCIJA

Padedą išvengti įsilaužimų,
konfidencialių duomenų
praradimo.



INCIDENTŲ TYRIMAS

Įvykus įsilaužimui, padeda
ištirti incidento detales.



KITI PRIVALUMAI

Suteikia žinių. Mažina riziką.

Executive summary	3
--------------------------	----------

Targeted countries and verticals	4
---	----------

China-aligned groups	5
-----------------------------	----------

Mustang Panda	6
---------------	---

FishMonger	6
------------	---

TA410	7
-------	---

GRAF	7
------	---

MirrorFace	8
------------	---

GALLIUM	8
---------	---

DigitalRecyclers	8
------------------	---

TheWizards	8
------------	---

PerplexedGoblin	8
-----------------	---

Worok	9
-------	---

India-aligned groups	10
-----------------------------	-----------

Donot Team	11
------------	----

Iran-aligned groups	12
----------------------------	-----------

MuddyWater	13
------------	----

OilRig	13
--------	----

Middle Eastern groups	14
------------------------------	-----------

POLONIUM	15
----------	----

North Korea-aligned groups	16
-----------------------------------	-----------

Andariel	17
----------	----

Lazarus	17
---------	----

ScarCruft	17
-----------	----

Kimsuky	18
---------	----

Konni	18
-------	----

Russia-aligned groups	19
------------------------------	-----------

Sandworm	20
----------	----

Gamaredon	20
-----------	----

Turla	21
-------	----

Sednit	21
--------	----

Other	22
--------------	-----------

SturgeonPhisher	23
-----------------	----

Winter Vivern	23
---------------	----

About ESET	24
-------------------	-----------



THREAT INTELLIGENCE

- ✓ SIEMs – Security Information and Event Management
- ✓ SOARs – Security Orchestration, Automation and Response
- ✓ TIPs – Threat Intelligence Platforms

TAXII Feeds

 **Available: APT IoC** Active

This feed consists of APT information produced by ESET research. In general, the feed is an export from the ESET internal MISP server. All the data that is shared is also explained in greater detail in APT reports. The APT feed is also part of APT reports offering, but the feed can also be purchased separately.

 **Available: Botnet - C&C** Inactive

This feed is a subset of a botnet feed and provides information about links of Command and Control (CnC) servers and associated data. Thus the name CC feed.

 **Available: Botnet - Target** Inactive

This feed is a subset of a botnet feed and provides information about the targets.

 **Available: Botnet feed** Inactive

Based on ESET's proprietary botnet tracker network, Botnet feed features three types of sub-feeds – botnet, C&C and targets. Data provided includes items such as detection, hash, last alive, files downloaded, IP addresses, protocols, targets and other information.

 **Available: Domain feed** Inactive

Block domains which are considered malicious including domain name, IP address, and the date associated with them. The feed ranks domains based on their severity, which lets you adjust your response accordingly, for example to only block high-severity domains.

 **Available: IP feed** Inactive

This feed shares IPs considered to be malicious and the data associated with them. The structure of the data is very similar to that used for the domain and URL feeds. The main use-case here is to understand which malicious IPs are currently prevalent in the wild, block those IPs which are of high severity, spot those that are less severe, and investigate further, based on additional data, to see if they have already caused harm.

 **Available: Malicious file feed** Inactive

Understand which malicious files are being seen in the wild. Features domains which are considered malicious, including domain name, IP address, detection of file downloaded from URL and detection of the file which was trying to access the URL. This feed comprises shared hashes of malicious executable files and associated data.

 **Available: URL feed** Inactive

Similar to Domain feed, the URL feed looks at specific addresses. It includes detailed information on data related to the URL, as well as information about the domains which host them. All the information is filtered to show only high confidence results and includes human-readable information on why the URL was flagged.



THREAT INTELLIGENCE

Coming soon: Android infostealer feed

Inactive

Feed could be viewed as sub-set of Android threats. It contain targeted information about current and prevalent Android infostealer samples and associated data. Provided data helps you understand which Android infostealer families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Coming soon: Android threats feed

Inactive

This feed provides real-time information on the currently prevalent Android threats, as well as their characteristics and IOCs. The feed helps you understand which Android threats are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Coming soon: Cryptoscam feed

Inactive

Feed could be viewed as sub-set of scam domains and URLs. It contain targeted information about current and prevalent crypto scam domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. Crypto scams refer to any fraudulent practice in the cryptocurrency space aimed at tricking individuals into investing or giving away assets or sensitive information.

Coming soon: Malicious email attachments feed

Inactive

Email still remain as one of top attack vectors for adversaries. Feed contain information about current and prevalent malicious email attachments and associated data. The feed is created from ESET telemetry sources focused on email scanning (both client and server) near real-time, deduplication happens every 24 hours.

Coming soon: Phishing URL feed

Inactive

Feed contain information about current and prevalent phishing URLs and associated data. The feed is created from all ESET phishing URL sources near real-time, deduplication happens every 24 hours. Phishing URL redirect recipients to a fake website and coerce them into divulging sensitive data, such as login credentials or financial information. The website will look deceptively familiar and legit, but its aim is to misuse your trust by "fishing" for personal information a malicious actor can use for nefarious purposes.

Coming soon: Ransomware feed

Inactive

Ransomware is a type of cryptovirological malware that permanently block access to the victim's personal data unless a ransom is paid. The feed contain information about current and prevalent ransomware samples and associated data. Provided data helps you understand which ransomware families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Coming soon: Scam URL feed

Inactiv

The feed contain information about current and prevalent scam URLs and associated data. It includes, but is not limited to fraudulent electronic shops, investment scams, dating and cryptocurrency scam. The feed is created from all ESET URL sources near real-time, deduplication happens every 24 hours.

Coming soon: SMS scam feed

Inactive

Feed contain targeted information about current and prevalent sms scam domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. As SMS scam could be seen fake mobile text messages to steal personal information and money and commit fraud.



THREAT INTELLIGENCE

Coming soon: Android infostealer feed

Inactive

Feed could be viewed as sub-set of Android threats. It contain targeted information about current and prevalent Android infostealer samples and associated data. Provided data helps you understand which Android infostealer families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Coming soon: Android threats feed

Inactive

This feed provides real-time information on the currently prevalent Android threats, as well as their characteristics and IOCs. The feed helps you understand which Android threats are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Coming soon: Cryptoscam feed

Inactive

Feed could be viewed as sub-set of scam domains and URLs. It contain targeted information about current and prevalent crypto scam domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. Crypto scams refer to any fraudulent practice in the cryptocurrency space aimed at tricking individuals into investing or giving away assets or sensitive information.

Coming soon: Malicious email attachments feed

Inactive

Email still remain as one of top attack vectors for adversaries. Feed contain information about current and prevalent malicious email attachments and associated data. The feed is created from ESET telemetry sources focused on email scanning (both client and server) near real-time, deduplication happens every 24 hours.

Coming soon: Phishing URL feed

Inactive

Feed contain information about current and prevalent phishing URLs and associated data. The feed is created from all ESET phishing URL sources near real-time, deduplication happens every 24 hours. Phishing URL redirect recipients to a fake website and coerce them into divulging sensitive data, such as login credentials or financial information. The website will look deceptively familiar and legit, but its aim is to misuse your trust by "fishing" for personal information a malicious actor can use for nefarious purposes.

Coming soon: Ransomware feed

Inactive

Ransomware is a type of cryptovirological malware that permanently block access to the victim's personal data unless a ransom is paid. The feed contain information about current and prevalent ransomware samples and associated data. Provided data helps you understand which ransomware families are being seen in the wild and enables you to proactively block them before they can cause any harm. The feed is created from ESET telemetry sources near real-time, deduplication happens every 24 hours.

Coming soon: Scam URL feed

Inactiv

The feed contain information about current and prevalent scam URLs and associated data. It includes, but is not limited to fraudulent electronic shops, investment scams, dating and cryptocurrency scam. The feed is created from all ESET URL sources near real-time, deduplication happens every 24 hours.

Coming soon: SMS scam feed

Inactive

Feed contain targeted information about current and prevalent sms scam domains and URLs and associated data. The feed is created from all ESET domain and URL sources near real-time, deduplication happens every 24 hours. As SMS scam could be seen fake mobile text messages to steal personal information and money and commit fraud.



THREAT INTELLIGENCE



MISP



My Events

Org Events



Enter v

<input type="checkbox"/>		Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Info
<input type="checkbox"/>		ESET		ESET Threat Actor	ESET Technical Analysis tlp:amber+strict			2024-	APT- Rebuilding a zero-day -
				Attack Pattern					
				Dynamic API Resolution - T1027.007					
				System Owner/User Discovery - T1033					
				Exfiltration Over C2 Channel - T1041					
				Scheduled Task - T1053.005					
				Web Protocols - T1071.001					
				File and Directory Discovery - T1083					
				Indirect Command Execution - T1202					
				Exploitation for Client Execution - T1203					
				Malicious Link - T1204.001					
				Rundll32 - T1218.011					
				Component Object Model Hijacking - T1546.015					
				Component Object Model - T1559.001					
				Symmetric Cryptography - T1573.001					
				Domains - T1583.001					
				Web Services - T1583.006					
				Cloud Accounts - T1585.003					
				Upload Malware - T1608.001					



THREAT INTELLIGENCE

ESET Threat Intelligence reports

TLP: AMBER+STRICT



Digital Security
Progress. Protected.

WELIVESECURITY.COM PUBLICATION

Phishing targeting Polish
SMBs continues via
ModiLoader

Tags	#Attr.	#Corr.	Date	Info
ESET			2024-	APT- Rebuilding a zero-day -
Technical Analysis				
tlp:amber+strict				

The image shows a text editor window with a dark blue background. The top half of the window contains several lines of obfuscated batch script code, with characters like '+' and '%' frequently used to break words. Below this, there is a section of base64-encoded data. A red box highlights the text 'Batch script' and 'ModiLoader binary' within the code. At the bottom of the code block, there is a line that reads '-----BEGIN X509 CRL-----'.

Figure 4. File with .cmd extension containing heavily obfuscated batch script (top) that decodes base64-encoded ModLoader binary (bottom)

#Attr.	#Corr.	Date	Info
		2024-	APT- Rebuilding a zero-day -

Analysis
t

PUBLICATION

Phishing targeting Polish SMBs continues via ModLoader



THREAT INTELLIGENCE

Victimology / Business verticals

Aerospace, military, and defense companies.

Infection vector

N/A

Post-compromise activity

N/A

IoCs

Operation In(ter)ception

Date	2021-04-07 00:08:38
MD5	2CBE0BEA035DB9240CEB338CF9EA7FE6
SHA-1	9A8B7F11104156F0DF4F07827EC12E5C2300C4EE
SHA-256	40B6CBCC594D3696952E90FA15CCD733EBC2777554092E8C15694334274E5B90
Filename	c.exe
Description	Stage 1 loader.
C&C	https://kehot.com[.]ar/Pubs/menus.jpg https://www.meisami[.]net/css/search.css https://www.sfaonweb[.]com/pdf/{A76E7D01-6BAF-4FE4-98E0-.pdf https://amon-werbeartikel[.]de/Media/Uploaded/chrisen.png
Detection	Win64/Interception.G
PE compilation timestamp	2020-02-04 18:01:33 (Timestomped)

Loader

ysis
t

#Attr.	#Corr.	Date	Info
		2024-	APT- Rebuilding a zero-day -

Enter v



THREAT INTELLIGENCE

Victimology / Business verticals

Aerospace, military, and defense companies.

Infection vector

N/A

Post-compromise activity

N/A

IoCs

Operation In(ter)ception

Date	2021-04-07 00:08:38
MD5	2CBE0BEA035DB9240CEB338CF9EA7FE6
SHA-1	9A8B7F11104156F0DF4F07827EC12E5C2300C4EE
SHA-256	40B6CBCC594D3696952E90FA15CCD733EBC2777554092E8C15694334274E5B90
Filename	c.exe
Description	Stage 1 loader.
C&C	https://kehot.com[.]ar/Pubs/menus.jpg https://www.meisami[.]net/css/search.css https://www.sfaonweb[.]com/pdf/{A76E7D01-6BAF-4FE4-98E0-.pdf https://amon-werbeartikel[.]de/Media/Uploaded/chrisen.png
Detection	Win64/Interception.G
PE compilation timestamp	2020-02-04 18:01:33 (Timestomped)

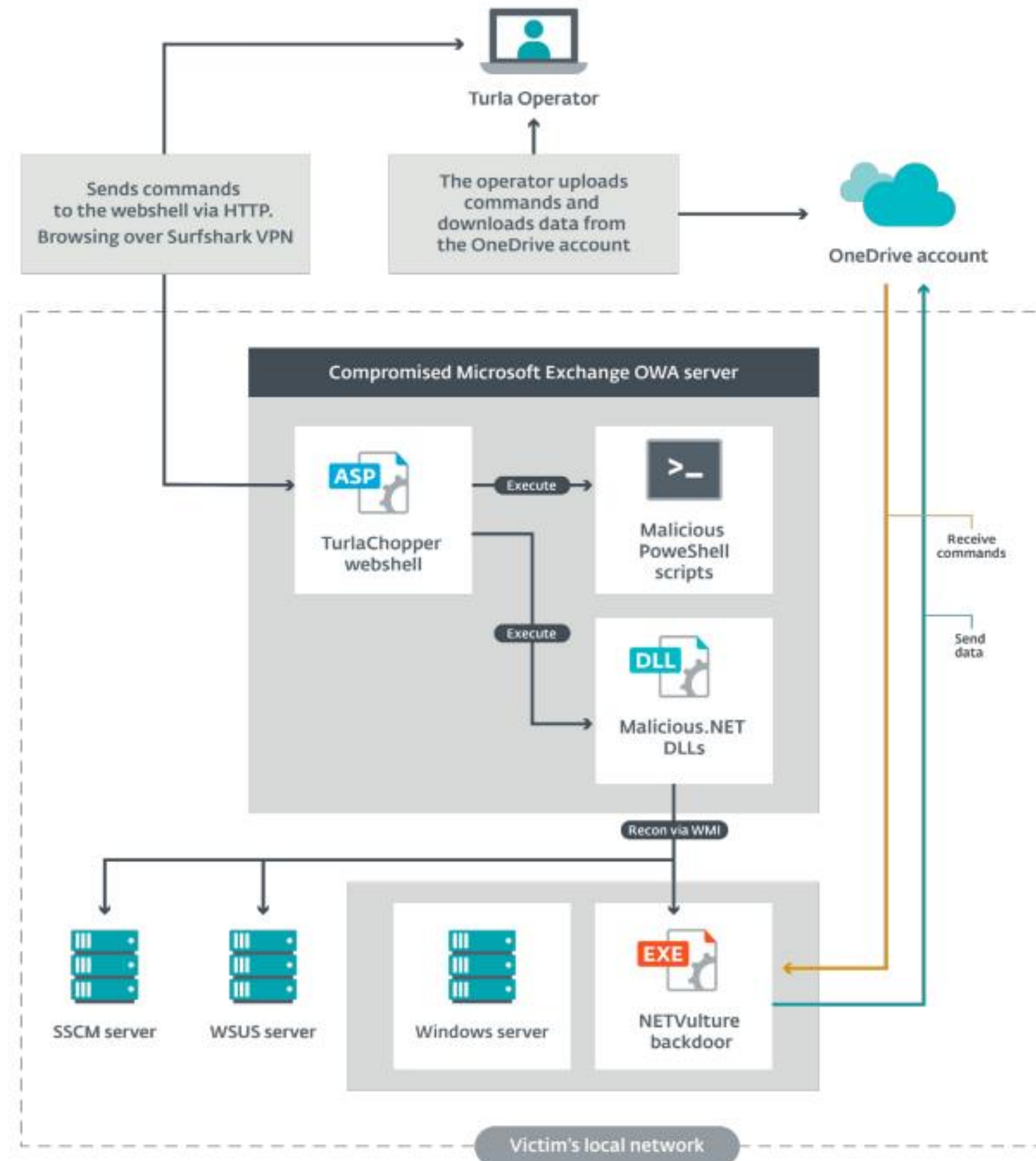


Figure 3. Overview of TurlaChopper and NETVulture usage



3 ESET Threat Intelligence reports

TLP: AMBER+STRICT

Victimology / Business verticals

Aerospace, military, and defense companies.

Infection vector

N/A

Post-compromise activity

N/A

IoCs

Operation In(ter)ception

Date	2021-04-07 00:08:38
MD5	2CBE0BEA035DB9240CEB338CF9EA7FE6
SHA-1	9A8B7F11104156F0DF4F07827EC12E5C2300C4EE
SHA-256	40B6CBCC594D3696952E90FA15CCD733EBC2777554092E8C15694334274E5B9
Filename	c.exe
Description	Stage 1 loader.
C&C	https://kehot.com[.]ar/Pubs/menus.jpg https://www.meisami[.]net/css/search.css https://www.sfaonweb[.]com/pdf/{A76E7D01-6BAF-4FE4-98E0-.pdf https://amon-werbeartikel[.]de/Media/Uploaded/chrisen.png
Detection	Win64/Interception.G
PE compilation timestamp	2020-02-04 18:01:33 (Timestamped)

CAMPAIGNS

In general, all campaigns followed a similar scenario. The targeted company received an email message with a business offer that could be as simple as "Please provide your best price offer for the attached order no. 2405073", as can be seen in Figure 2.

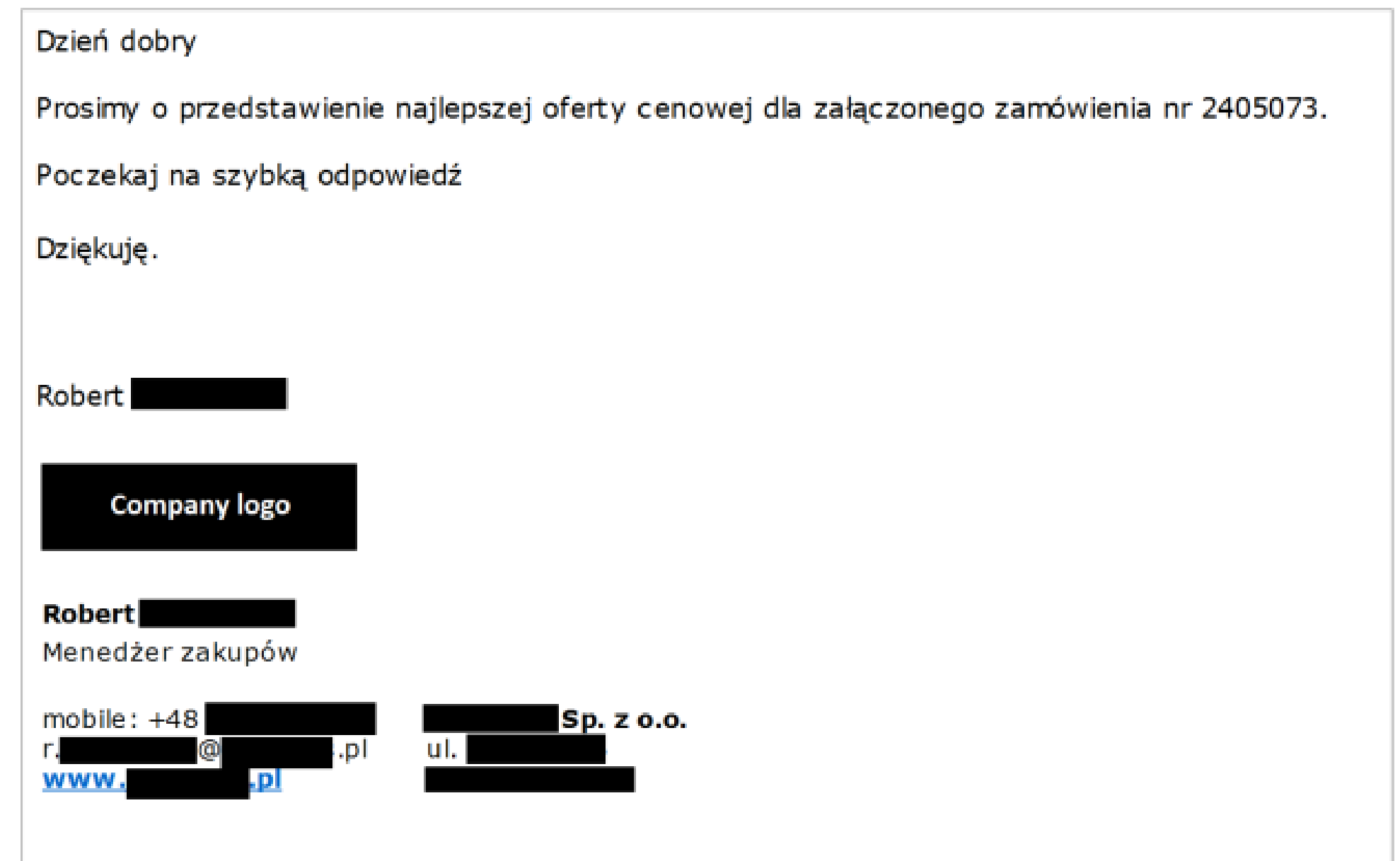


Figure 2. Example of a phishing email containing ModLoader in the attachment



[Redacted]	Countries	First seen	Last seen
[Redacted]	Ukraine	2023-01	2023-[Redacted]
[Redacted]	Ukraine	2023-04	2023-[Redacted]
[Redacted]	Poland	2023-05	2023-[Redacted]
[Redacted]	Ukraine	2023-06	2023-[Redacted]
[Redacted]	Ukraine	2023-08	2023-[Redacted]
[Redacted]	Ukraine	2023-09	2024-[Redacted]
[Redacted]	Poland, Lithuania	2023-09	2024-[Redacted]

The targeted company received an email message with a subject line: "de your best price offer for the attached order no. 2405073",

nowej dla załączonego zamówienia nr 2405073.

Starting from 2023-09, when the new [Redacted] was released, two main clusters reusing the same public key surfaced, as shown in Table 4. The first, [Redacted], is targeting only Ukraine, and the second, [Redacted], seems to have switched from targeting Poland to Lithuania.

As this cluster targeted Poland with lure related to the Polish parliamentary election in 2023-10, it might have switched to target the upcoming Lithuanian presidential election in 2024-05.

file containing ModLoader in the attachment



THREAT INTELLIGENCE

3 ESET Threat Intelligence reports



Countries	First seen
Ukraine	2023-01
Ukraine	2023-04
Poland	2023-05
Ukraine	2023-06
Ukraine	2023-08
Ukraine	2023-09
Poland, Lithuania	2023-09

Starting from 2023-09, when the new [redacted] was released, two main clusters reusing key surfaced, as shown in Table 4. The first, [redacted], is targeting the second, [redacted], seems to have switched from targeting Poland. As this cluster targeted Poland with lure related to the Polish parliamentary election in 2023-10 switched to target the upcoming Lithuanian presidential election in 2024-05.



How can ESET AI Advisor assist you today?

How has the Lazarus group evolved its cyber-attack strategies in the past year?

What cyber defense measures are effective against APT10's recent activities?

What are the emerging threats from APT groups in the healthcare sector?

Which APT groups are known for conducting cyber warfare, and what are their latest operations?

Ask anything regarding APT reports or WeLiveSecurity

Responses are generated by AI. Verify for accuracy.

ESET Research: Spy group exploits WPS Office zero day; analysis uncovers a second vulnerability

- South Korea-aligned advanced persistent threat group APT-C-60 weaponized a remote code execution vulnerability in WPS Office for Windows (CVE-2024-7262) in order to target East Asian countries. ESET Research discovered the vulnerability and provides a root cause analysis, along with a description of its weaponization.
- A strange spreadsheet document referencing one of the group’s many downloader components pointed to APT-C-60.
- The exploit is deceptive enough to trick users into clicking on a legitimate-looking spreadsheet while also being very effective and reliable. The choice of the MHTML file format allowed the attackers to turn a code execution vulnerability into a remote one.
- While analyzing the vulnerability, ESET Research discovered another way to exploit it (CVE-2024-7263).
- Following our coordinated vulnerability disclosure policy, as Kingsoft acknowledged and patched both vulnerabilities, we provide a detailed analysis.

Cluster	Target	Start Date
[REDACTED]	Ukraine	2023-09
[REDACTED]	Poland, Lithuania	2023-09

Starting from 2023-09, when the new [REDACTED] was released, two main clusters reusing key surfaced, as shown in Table 4. The first, [REDACTED], is targeting the second, [REDACTED], seems to have switched from targeting Poland. As this cluster targeted Poland with lure related to the Polish parliamentary election in 2023-10 switched to target the upcoming Lithuanian presidential election in 2024-05.



SET AI Advisor assist you today?

its ear?

What cyber defense measures are effective against APT10's recent activities?

What are the emerging threats from APT groups in the healthcare sector?

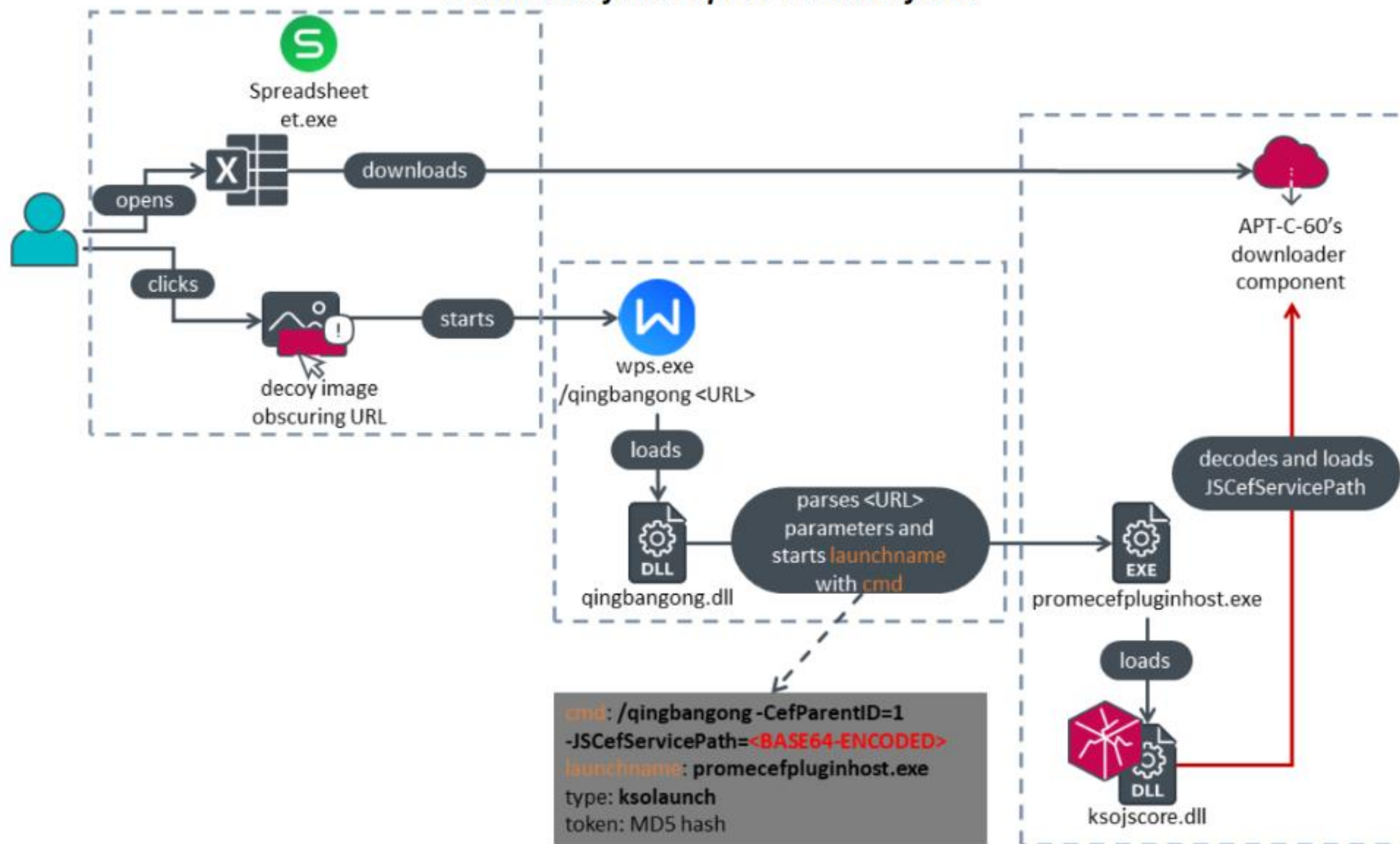
Which APT groups are known for conducting cyber warfare, and what are their latest operations?

Ask anything regarding APT reports or WeLiveSecurity ➤

ESET Research: Spy group exploits WPS Office zero day; analysis uncovers a second vulnerability

- South Korea-aligned advanced vulnerability in WPS Office for Research discovered the vulne weaponization.
- A strange spreadsheet docume to APT-C-60.
- The exploit is deceptive enoug being very effective and reliable execution vulnerability into a r
- While analyzing the vulnerabili
- Following our coordinated vul vulnerabilities, we provide a de

Overview of the exploit's control flow.



```

cmd: /qingbangong -CefParentID=1
-JSCefServicePath=<BASE64-ENCODED>
launchname: promecefpluginhost.exe
type: ksolaunch
token: MD5 hash
  
```

Starting from 2023-09, when the new key surfaced, as shown in Table 4. The first, the second,

As this cluster targeted Poland with lure switched to target the upcoming Lithuanian

THREAT INTELLIGENCE

Pateikiama realiuoju laiku ESET ekspertų sukaupta pasaulinė informacija apie tikslines atakas, pažangias nuolatinės grėsmes, nulinės dienos ir botnetų veiklą.

- ✓ **JSON and STIX v2.0/2.1 formats**
- ✓ **Domain feed**
- ✓ **Via TAXII server, updated several times within one hour**
- ✓ **URL feed**
 - IBM QRadar
 - Anomali
 - MS Azure Sentinel
 - OpenCTI
 - ThreatQuotient
- ✓ **Indicators of Compromise (IoCs)**
- ✓ **Malicious files feed**
- ✓ **Out-of-the-box integrations with Threat Intelligence Platforms**
- ✓ **IP feed**
- ✓ **APT feed**
- ✓ **Botnet feed**

Activity Reports Premium

- ✔ Reports cover threat actors we track
- ✔ Activity Summary reports
- ✔ Technical Analysis reports
- ✔ IOCs available via MISP, STIX/TAXII
- ✔ YARA rules
- ✔ MITRE ATT&CK mapping
- ✔ WLS pre-publication access
- ✔ Retrospective intelligence
- ✔ Access to analysts

Activity Summary reports

- 2x per month
- Describing the latest activities, campaigns of various threat actors
- Targets
- Infection vectors
- Post-compromise activity
- IOCs, network indicators with details
- YARA rules

Technical Analysis reports

- 1+ per month
- In-depth threat analysis describing recent campaign
- Focus on toolset (tools, malware)
- YARA rules, Snort rules
- MITRE ATT&CK mappings
- Recommendations on how to protect the infrastructure
- Remediation advice where applicable



Bendraukime 



lukas@eset.lt

www.eset.lt