AKO VZNIKÁ ESET VÝSKUM ŠKODLIVÉHO KÓDU: ESET TECHNOLÓGIE A INÉ TAJOMSTVÁ

Zuzana Hromcová | Malware Researcher

Digital Security
Progress. Protected.

&

SME KONFERENCIE

ESET research
@ESETresearch · **Follow**

Breaking. **#ESETResearch** d
data wiper malware used in
ESET telemetry shows that it
hundreds of machines in the
follows the DDoS attacks ag
Ukrainian websites earlier to

12:25 PM · Feb 23, 2022

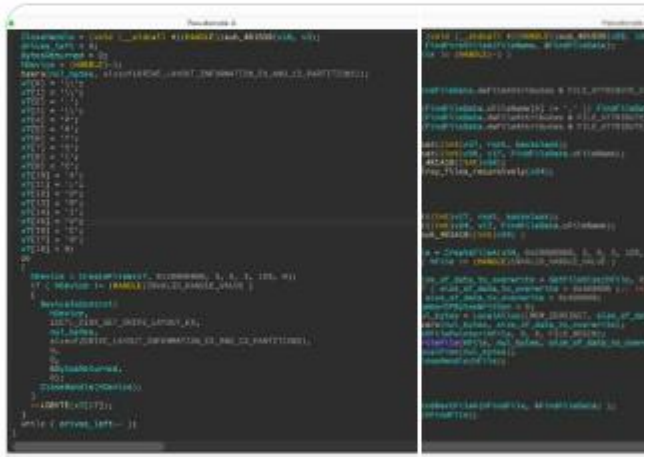
Read the full conversation on Twitter

3.5K Reply Share

Read 65 replies

ESET research
@ESETresearch · **Follow**

#BREAKING **#ESETresearch** warns a
discovery of a 3rd destructive wiper
in Ukraine 🇺🇦. We first observed this
malware we call **#CaddyWiper** toda
9h38 UTC. 1/7



11:22 AM · Mar 14, 2022

Read the full conversation on Twitter

1.3K Reply Share

Read 28 replies

ESET research
@ESETresearch · **Follow**

#BREAKING **#ESETresearch** helped analyze a **#Sandworm** campaign against an energy company in **#Ukraine** 🇺🇦 using **#CaddyWiper** and a new version of the infamous **#Industroyer** malware. **#WarInUkraine**
welivesecurity.com/2022/04/12/ind... 1/5

welivesecurity.com
Industroyer2: Industroyer reloaded | WeLiveS...
ESET researchers have responded to a cyber-incident that affected an energy provider in ...

2:40 AM · Apr 12, 2022

Read the full conversation on Twitter

643 Reply Share

Read 10 replies


welivesecurity BY eset
Crypto malware in patched wallets targeting Android and iOS devices
ESET Research uncovers a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets
Lukas Stefanko
24 Mar 2022 - 01:30PM


welivesecurity BY eset
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


welivesecurity BY eset
Anatomy of native IIS malware
ESET researchers publish a white paper putting IIS web server threats under the microscope
Zuzana Hromcová
Anton Cherepanov
6 Aug 2021 - 02:59PM


welivesecurity BY eset
The dirty dozen of Latin America: From Amavaldo to Zumanek
The grand finale of our series dedicated to demystifying Latin American banking trojans
ESET Research
15 Dec 2021 - 11:30AM


welivesecurity BY eset
Jumping the air gap: 15 years of nation-state effort
ESET researchers studied all the malicious frameworks ever reported publicly that have been used to attack air-gapped networks and are releasing a side-by-side comparison of their most important TTPs
Alexis Dorais-Joncas
Facundo Muñoz
1 Dec 2021 - 11:30AM


welivesecurity BY eset
DoNot Go! Do not respawn!
ESET researchers take a deep look into recent attacks carried out by Donot Team throughout 2020 and 2021, targeting government and military entities in several South Asian countries
Facundo Muñoz
Matías Porolli
18 Jan 2022 - 11:30AM


welivesecurity BY eset
Mustang Panda's Hodur: Old tricks, new Korplug variant
ESET researchers have discovered Hodur, a previously undocumented Korplug variant spread by Mustang Panda, that uses phishing lures referencing current events in Europe, including the invasion of Ukraine
Alexandre Côté Cyr
23 Mar 2022 - 09:00AM


welivesecurity BY eset
Strategic web compromises in the Middle East with a pinch of Candiru
ESET researchers have discovered strategic web compromise (aka watering hole) attacks against high-profile websites in the Middle East
Matthieu Faou
16 Nov 2021 - 04:34PM


welivesecurity BY eset
FamousSparrow: A suspicious hotel guest
Yet another APT group that exploited the ProxyLogon vulnerability in March 2021
Tahseen Bin Taj
Matthieu Faou
23 Sep 2021 - 11:30AM


welivesecurity BY eset
A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity
ESET researchers reveal a detailed profile of TA410: we believe this cyberespionage umbrella group consists of three different teams using different toolsets, including a new version of the FlowCloud espionage backdoor discovered by ESET.
Alexandre Côté Cyr
Matthieu Faou
27 Apr 2022 - 03:00PM


welivesecurity BY eset
BladeHawk group: Android espionage against Kurdish ethnic group
ESET researchers have investigated a mobile espionage campaign that targets the Kurdish ethnic group and has been active since at least March 2020
Lukas Stefanko
7 Sep 2021 - 02:30PM


welivesecurity BY eset
The SideWalk may be as dangerous as the CROSSWALK
Meet SparklingGoblin, a member of the Winnti family
Thibaut Passilly
Mathieu Tartare
24 Aug 2021 - 07:59PM


welivesecurity BY eset
Signed kernel drivers – Unguarded gateway to Windows' core
ESET researchers look at malware that abuses vulnerabilities in kernel drivers and outline mitigation techniques against this type of exploitation
Michal Poslušný
11 Jan 2022 - 11:30AM


welivesecurity BY eset
When "secure" isn't secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops
ESET researchers discover multiple vulnerabilities in various Lenovo laptop models that allow an attacker with admin privileges to expose the user to firmware-level malware
Martin Smolár
19 Apr 2022 - 11:30AM


welivesecurity BY eset
UEFI threats moving to the ESP: Introducing ESPecter bootkit
ESET research discovers a previously undocumented UEFI bootkit with roots going back all the way to at least 2012
Martin Smolár
Anton Cherepanov
5 Oct 2021 - 11:30AM


welivesecurity BY eset
Under the hood of Wslink's multilayered virtual machine
ESET researchers describe the structure of the virtual machine used in samples of Wslink and suggest a possible approach to see through its obfuscation techniques
Vladislav Hrčka
28 Mar 2022 - 11:30AM


welivesecurity BY eset
FontOnLake: Previously unknown malware family targeting Linux
ESET researchers discover a malware family with tools that show signs they're used in targeted attacks
Vladislav Hrčka
7 Oct 2021 - 11:30AM


welivesecurity BY eset
Fake e-shops on the prowl for banking credentials using Android malware
ESET researchers analyzed three malicious applications targeting customers of eight Malaysian banks
Lukas Stefanko
6 Apr 2022 - 11:30AM


welivesecurity BY eset
Watering hole deploys new macOS malware, DazzleSpy, in Asia
Hong Kong pro-democracy radio station website compromised to serve a Safari exploit that installed cyberespionage malware on site visitors' Macs
Marc-Etienne M.Léveillé
Anton Cherepanov
25 Jan 2022 - 11:30AM


welivesecurity BY eset
ESET takes part in global operation to disrupt Zloader botnets
ESET researchers provided technical analysis, statistical information, and known command and control server domain names and IP addresses
Jean-Ian Boutin
Tomáš Procházka
13 Apr 2022 - 06:00PM

SECURITY DAYS

Čo sa skrýva za týmito titulkami?

ESET Digital Security Progress. Protected. & SME KONFERENCIE


welivesecurity BY eset
Crypto malware in patched wallets targeting Android and iOS devices
ESET Research uncovers a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets
Lukas Stefanko
24 Mar 2022 - 01:30PM


welivesecurity BY eset
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


welivesecurity BY eset
Anatomy of native IIS malware
ESET researchers publish a white paper putting IIS web server threats under the microscope
Zuzana Hromcová
Anton Cherepanov
6 Aug 2021 - 02:59PM


welivesecurity BY eset
The dirty dozen of Latin America: From Amavaldo to Zumanek
The grand finale of our series dedicated to demystifying Latin American banking trojans
ESET Research
15 Dec 2021 - 11:30AM


welivesecurity BY eset
Jumping the air gap: 15 years of nation-state effort
ESET researchers studied all the malicious frameworks ever reported publicly that have been used to attack air-gapped networks and are releasing a side-by-side comparison of their most important TTPs
Alexis Dorais-Joncas
Facundo Muñoz
1 Dec 2021 - 11:30AM


welivesecurity BY eset
DoNot Go! Do not respawn!
ESET researchers take a deep look into recent attacks carried out by Donot Team throughout 2020 and 2021, targeting government and military entities in several South Asian countries
Facundo Muñoz
Matías Porolli
18 Jan 2022 - 11:30AM


welivesecurity BY eset
Mustang Panda's Hodur: Old tricks, new Korplug variant
ESET researchers have discovered Hodur, a previously undocumented Korplug variant spread by Mustang Panda, that uses phishing lures referencing current events in Europe, including the invasion of Ukraine
Alexandre Côté Cyr
23 Mar 2022 - 09:00AM


welivesecurity BY eset
Strategic web compromises in the Middle East with a pinch of Candiru
ESET researchers have discovered strategic web compromise (aka watering hole) attacks against high-profile websites in the Middle East
Matthieu Faou


welivesecurity BY eset
FamousSparrow: A suspicious hotel guest
Yet another APT group that exploited the ProxyLogon vulnerability in March 2021
Tahseen Bin Taj
Matthieu Faou
23 Sep 2021 - 11:30AM


welivesecurity BY eset
A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity
ESET researchers reveal a detailed profile of TA410: we believe this cyberespionage umbrella group consists of three different teams using different toolsets, including a new version of the FlowCloud espionage backdoor discovered by ESET.
Alexandre Côté Cyr
Matthieu Faou
27 Apr 2022 - 03:00PM


welivesecurity BY eset
BladeHawk group: Android espionage against Kurdish ethnic group
ESET researchers have investigated a mobile espionage campaign that targets the Kurdish ethnic group and has been active since at least March 2020
Lukas Stefanko
7 Sep 2021 - 02:30PM


welivesecurity BY eset
The SideWalk may be as dangerous as the CROSSWALK
Meet SparklingGoblin, a member of the Winnti family
Thibaut Passilly
Mathieu Tartare
24 Aug 2021 - 07:59PM


welivesecurity BY eset
Signed kernel drivers – Unguarded gateway to Windows' core
ESET researchers look at malware that abuses vulnerabilities in kernel drivers and outline mitigation techniques against this type of exploitation
Michal Poslušný
11 Jan 2022 - 11:30AM


welivesecurity BY eset
When "secure" isn't secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops
ESET researchers discover multiple vulnerabilities in various Lenovo laptop models that allow an attacker with admin privileges to expose the user to firmware-level malware
Martin Smolár
19 Apr 2022 - 11:30AM


welivesecurity BY eset
UEFI threats moving to the ESP: Introducing ESPecter bootkit
ESET research discovers a previously undocumented UEFI bootkit with roots going back all the way to at least 2012
Martin Smolár
Anton Cherepanov
5 Oct 2021 - 11:30AM


welivesecurity BY eset
Under the hood of Wslink's multilayered virtual machine
ESET researchers describe the structure of the virtual machine used in samples of Wslink and suggest a possible approach to see through its obfuscation techniques
Vladislav Hrčka
28 Mar 2022 - 11:30AM


welivesecurity BY eset
FontOnLake: Previously unknown malware family targeting Linux
ESET researchers discover a malware family with tools that show signs they're used in targeted attacks
Vladislav Hrčka
7 Oct 2021 - 11:30AM


welivesecurity BY eset
Fake e-shops on the prowl for banking credentials using Android malware
ESET researchers analyzed three malicious applications targeting customers of eight Malaysian banks
Lukas Stefanko
6 Apr 2022 - 11:30AM


welivesecurity BY eset
Watering hole deploys new macOS malware, DazzleSpy, in Asia
Hong Kong pro-democracy radio station website compromised to serve a Safari exploit that installed cyberespionage malware on site visitors' Macs
Marc-Etienne M.Léveillé
Anton Cherepanov
25 Jan 2022 - 11:30AM


welivesecurity BY eset
ESET takes part in global operation to disrupt Zloader botnets
ESET researchers provided technical analysis, statistical information, and known command and control server domain names and IP addresses
Jean-Ian Boutin
Tomáš Procházka
13 Apr 2022 - 06:00PM

welivesecurity BY ESET

Crypto malware in patched wallets targeting Android and iOS devices

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

Anatomy of native IIS malware

The dirty dozen of Latin America: From Amavaldo to Zumanek

Jumping the air gap: 15 years of nation-state effort

ESET researchers studied all the malicious frameworks ever reported publicly that have been

Signed kernel drivers – Unguarded gateway to Windows' core

ESET researchers look at malware that abuses vulnerabilities in kernel drivers and outline mitigation techniques against this type of exploitation

Michal Poslušný

11 Jan 2022 - 11:30AM

When "secure" isn't secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops

ESET researchers discover multiple vulnerabilities in various Lenovo laptop models that allow an attacker with admin privileges to expose the user to firmware-level malware

Martin Smolár

19 Apr 2022 - 11:30AM

Under the hood of Wslink's multilayered virtual machine

ESET researchers describe the structure of the virtual machine used in samples of Wslink and suggest methods to overcome techniques

Vladislav Hrčka

28 Mar 2022 - 11:30AM

FontOnLake: Previously unknown malware family targeting Linux

ESET researchers discover a malware family with tools that show signs they're used in targeted attacks

Vladislav Hrčka

7 Oct 2021 - 11:30AM

Fake e-shops on the prowl for banking credentials using Android malware

ESET researchers analyzed three malicious applications targeting customers of eight Malaysian banks

Lukas Stefanko

6 Apr 2022 - 11:30AM

Watering hole deploys new macOS malware, DazzleSpy, in Asia

Hong Kong pro-democracy radio station website compromised to serve a Safari exploit that installed cyberespionage malware on site visitors' Macs

Marc-Etienne M.Léveillé Anton Cherepanov

25 Jan 2022 - 11:30AM

ESET takes part in global operation to disrupt Zloader botnets

ESET researchers provided technical analysis, statistical information, and known command and control server domain names and IP addresses

Jean-Ian Boutin Tomáš Procházka

13 Apr 2022 - 06:00PM

SECURITY DAYS

Výskum zraniteľností

Digital Security
Progress. Protected.

&

SME KONFERENCIE


hacked...
SOROS
D-Link
D-Link
D-Link
D-Link


welivesecurity BY eset
Crypto malware in patched wallets targeting Android and iOS devices
ESET Research uncovers a sophisticated scheme that distributes trojanized Android and iOS apps posing as popular cryptocurrency wallets
Lukas Stefanko
24 Mar 2022 - 01:30PM


welivesecurity BY eset
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


welivesecurity BY eset
Anatomy of native IIS malware
ESET researchers publish a white paper putting IIS web server threats under the microscope
Zuzana Hromcová
Anton Cherepanov
6 Aug 2021 - 02:59PM


welivesecurity BY eset
The dirty dozen of Latin America: From Amavaldo to Zumanek
The grand finale of our series dedicated to demystifying Latin American banking trojans
ESET Research
15 Dec 2021 - 11:30AM


welivesecurity BY eset
Jumping the air gap: 15 years of nation-state effort
ESET researchers studied all the malicious frameworks ever reported publicly that have been used to attack air-gapped networks and are releasing a side-by-side comparison of their most important TTPs
Alexis Dorais-Joncas
Facundo Muñoz
1 Dec 2021 - 11:30AM


welivesecurity BY eset
DoNot Go! Do not respawn!
ESET researchers take a deep look into recent attacks carried out by Donot Team throughout 2020 and 2021, targeting government and military entities in several South Asian countries
Facundo Muñoz
Matías Porolli
18 Jan 2022 - 11:30AM


welivesecurity BY eset
Mustang Panda's Hodur: Old tricks, new Korplug variant
ESET researchers have discovered Hodur, a previously undocumented Korplug variant spread by Mustang Panda, that uses phishing lures referencing current events in Europe, including the invasion of Ukraine
Alexandre Côté Cyr
23 Mar 2022 - 09:00AM


welivesecurity BY eset
Strategic web compromises in the Middle East with a pinch of Candiru
ESET researchers have discovered strategic web compromise (aka watering hole) attacks against high-profile websites in the Middle East
Matthieu Faou


welivesecurity BY eset
FamousSparrow: A suspicious hotel guest
Yet another APT group that exploited the ProxyLogon vulnerability in March 2021
Tahseen Bin Taj
Matthieu Faou
23 Sep 2021 - 11:30AM


welivesecurity BY eset
A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity
ESET researchers reveal a detailed profile of TA410: we believe this cyberespionage umbrella group consists of three different teams using different toolsets, including a new version of the FlowCloud espionage backdoor discovered by ESET.
Alexandre Côté Cyr
Matthieu Faou
27 Apr 2022 - 03:00PM


welivesecurity BY eset
BladeHawk group: Android espionage against Kurdish ethnic group
ESET researchers have investigated a mobile espionage campaign that targets the Kurdish ethnic group and has been active since at least March 2020
Lukas Stefanko
7 Sep 2021 - 02:30PM


welivesecurity BY eset
The SideWalk may be as dangerous as the CROSSWALK
Meet SparklingGoblin, a member of the Winnti family
Thibaut Passilly
Mathieu Tartare
24 Aug 2021 - 07:59PM


welivesecurity BY eset
Signed kernel drivers – Unguarded gateway to Windows' core
ESET researchers look at malware that abuses vulnerabilities in kernel drivers and outline mitigation techniques against this type of exploitation
Michal Poslušný
11 Jan 2022 - 11:30AM


welivesecurity BY eset
When "secure" isn't secure at all: High-impact UEFI vulnerabilities discovered in Lenovo consumer laptops
ESET researchers discover multiple vulnerabilities in various Lenovo laptop models that allow an attacker with admin privileges to expose the user to firmware-level malware
Martin Smolár
19 Apr 2022 - 11:30AM


welivesecurity BY eset
UEFI threats moving to the ESP: Introducing ESPecter bootkit
ESET research discovers a previously undocumented UEFI bootkit with roots going back all the way to at least 2012
Martin Smolár
Anton Cherepanov
5 Oct 2021 - 11:30AM


welivesecurity BY eset
Under the hood of Wslink's multilayered virtual machine
ESET researchers describe the structure of the virtual machine used in samples of Wslink and suggest a possible approach to see through its obfuscation techniques
Vladislav Hrčka
28 Mar 2022 - 11:30AM


welivesecurity BY eset
FontOnLake: Previously unknown malware family targeting Linux
ESET researchers discover a malware family with tools that show signs they're used in targeted attacks
Vladislav Hrčka
7 Oct 2021 - 11:30AM


welivesecurity BY eset
Fake e-shops on the prowl for banking credentials using Android malware
ESET researchers analyzed three malicious applications targeting customers of eight Malaysian banks
Lukas Stefanko
6 Apr 2022 - 11:30AM


welivesecurity BY eset
Watering hole deploys new macOS malware, DazzleSpy, in Asia
Hong Kong pro-democracy radio station website compromised to serve a Safari exploit that installed cyberespionage malware on site visitors' Macs
Marc-Etienne M.Léveillé
Anton Cherepanov
25 Jan 2022 - 11:30AM

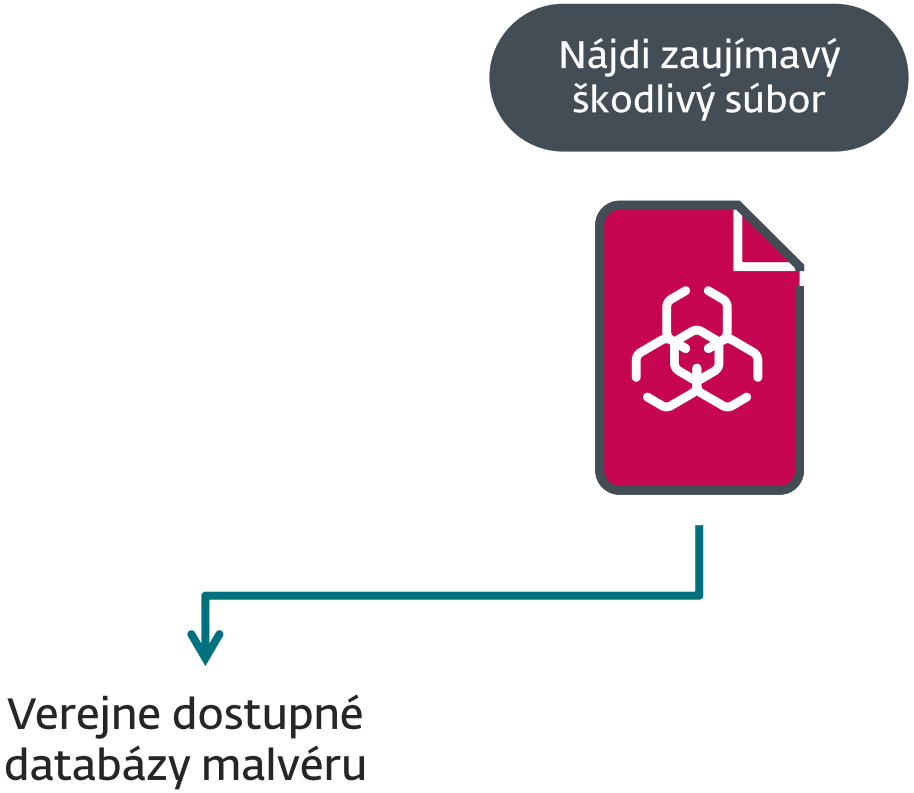

welivesecurity BY eset
ESET takes part in global operation to disrupt Zloader botnets
ESET researchers provided technical analysis, statistical information, and known command and control server domain names and IP addresses
Jean-Ian Boutin
Tomáš Procházka
13 Apr 2022 - 06:00PM

SECURITY DAYS

Výskum škodlivého kódu

Digital Security
Progress. Protected. & SME KONFERENCIE

Výskum škodlivého kódu



VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community

FILE URL SEARCH

Choose file

30 / 62

Community Score

30 security vendors and no sandboxes flagged this file as malicious

48f9471c20316b295704e6f8feb2196dd619799edec5835734fc24051f45c5b7

48f9471c20316b295704e6f8feb2196dd619799edec5835734fc24051f45c5b7.elf

64bits elf

78.17 KB
Size

2022-08-02 09:13:20 UTC
2 months ago

ELF

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

Security Vendors' Analysis

Ad-Aware	Trojan.Linux.GenericKD.40030713	AhnLab-V3	Trojan/Linux.Agent.80048
ALYac	Trojan.Linux.Agent	Antiy-AVL	Trojan/Generic.ASELF.166D
Avast	ELF:Lightning-B [Trj]	AVG	ELF:Lightning-B [Trj]
BitDefender	Trojan.Linux.GenericKD.40030713	Cyren	E64/Lightning.A

Intelligence ▾ Hunting ▾ Graph ▾ API ▾

5 Zuzana Hr…

- Search through corpus
- Threat landscape
- My group profile
- Search modifiers
- Documentation
- Automate searches
- Intelligence consumption

VT ENTERPRISE

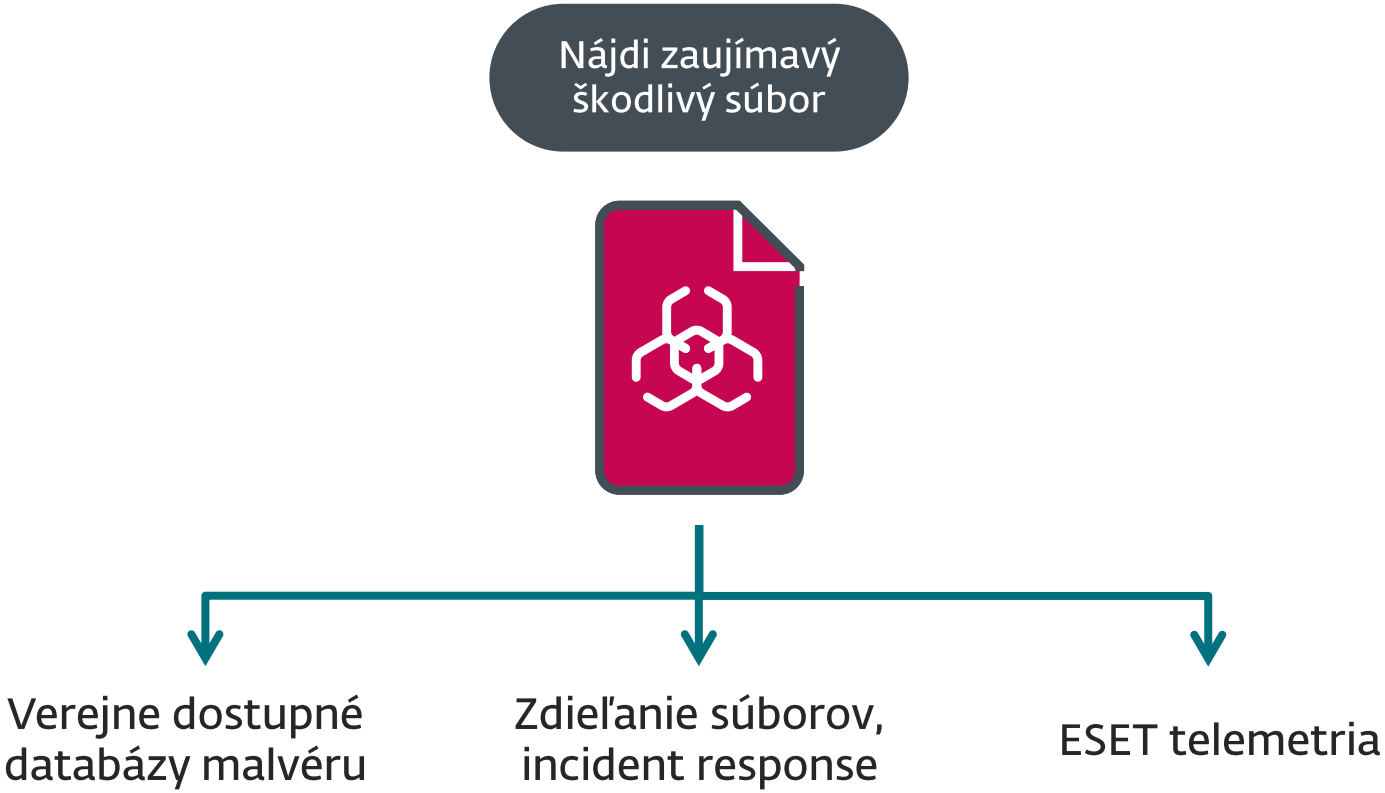
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

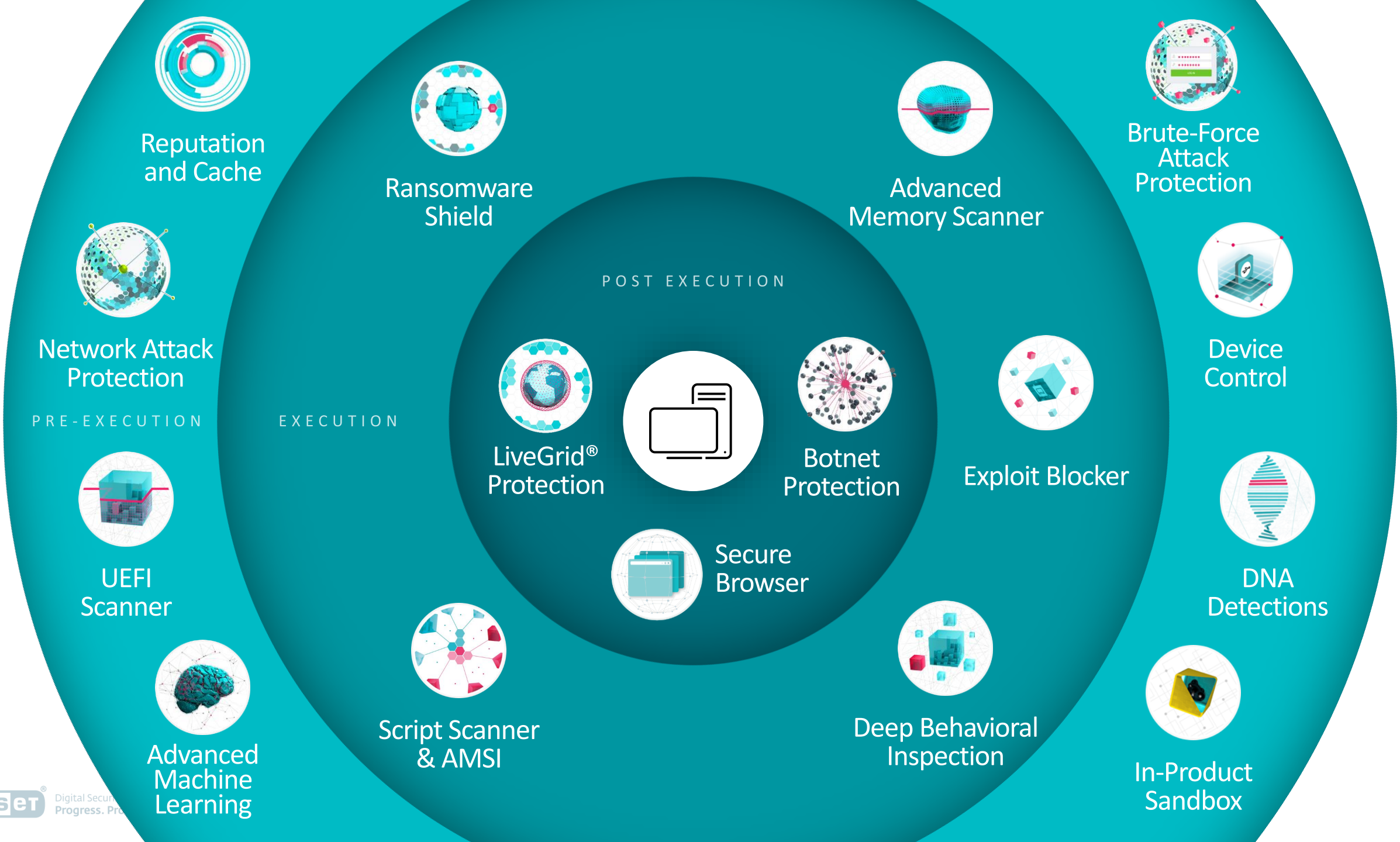
FILE | URL | SEARCH

Choose file

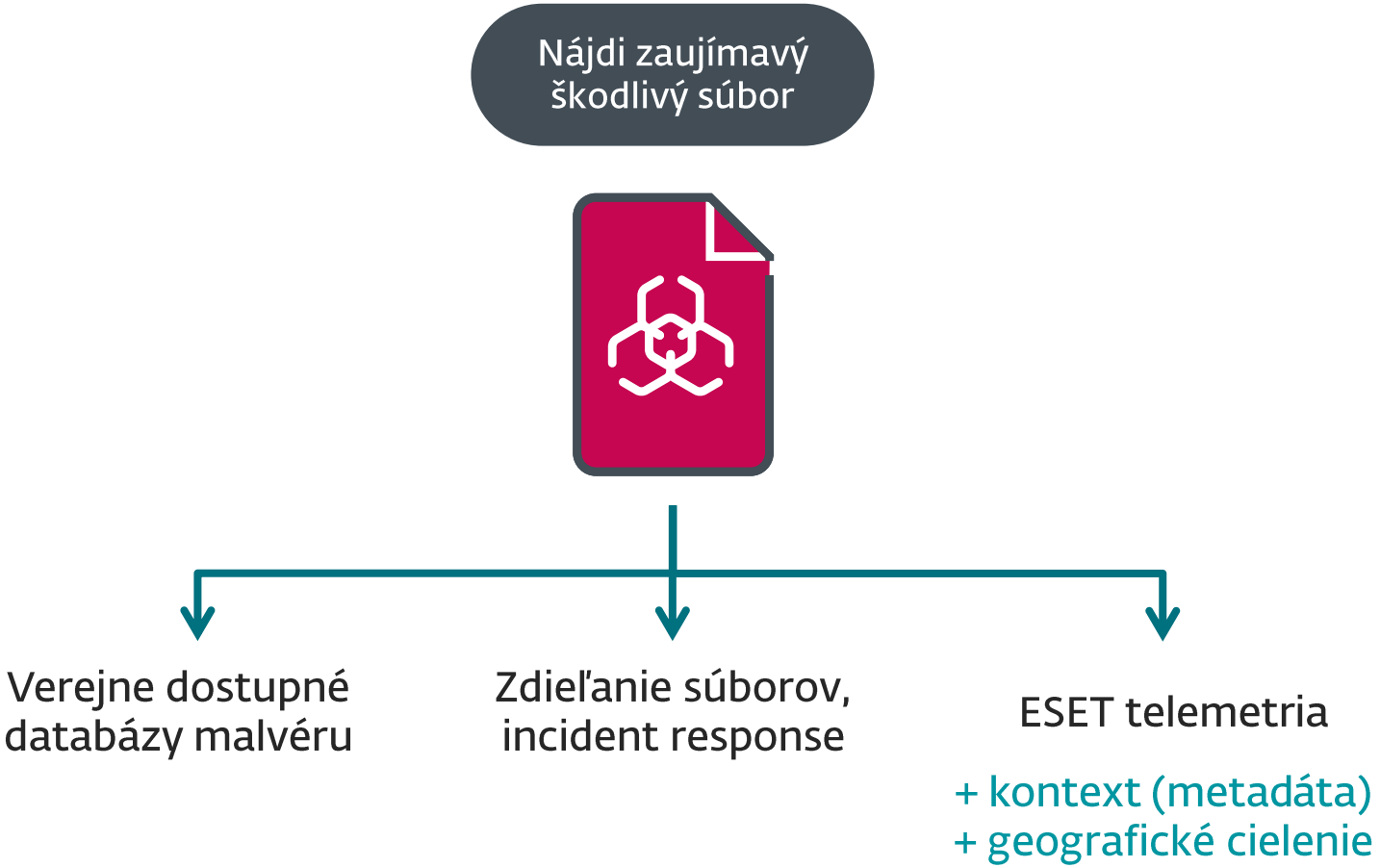
By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of**

Výskum škodlivého kódu



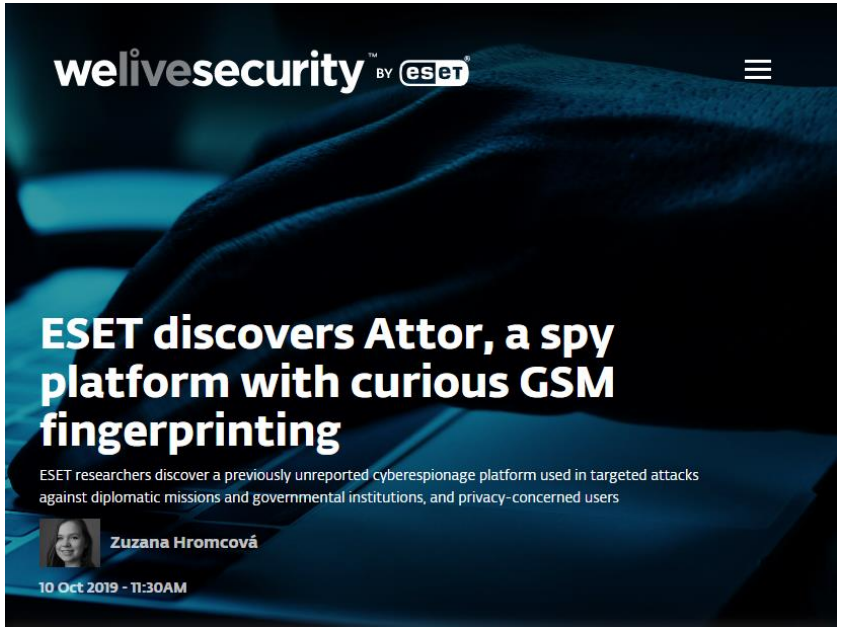

Reputation and Cache
Ransomware Shield
Advanced Memory Scanner
Brute-Force Attack Protection
Network Attack Protection
POST EXECUTION
Device Control
PRE-EXECUTION
EXECUTION
LiveGrid® Protection
Botnet Protection
Exploit Blocker
UEFI Scanner
DNA Detections
Secure Browser
Advanced Machine Learning
Script Scanner & AMSI
Deep Behavioral Inspection
In-Product Sandbox

Výskum škodlivého kódu



Advanced Memory Scanner

HĹBKOVÁ KONTROLA SPRÁVANIA



Script Scanner & AMSI

KONTROLA SKRIPTOV A ROZHRANIE AMSI

welivesecurity BY ESET

Watering hole deploys new macOS malware, DazzleSpy, in Asia

Hong Kong pro-democracy radio station website compromised to serve a Safari exploit that installed cyberespionage malware on site visitors' Macs

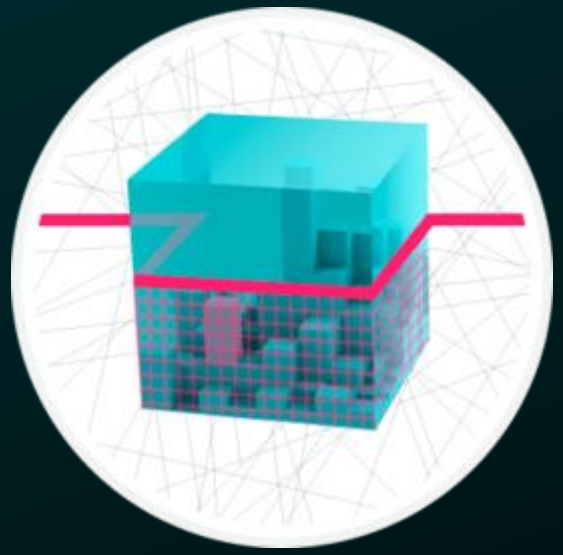
Marc-Etienne M.Léveillé

Anton Cherepanov

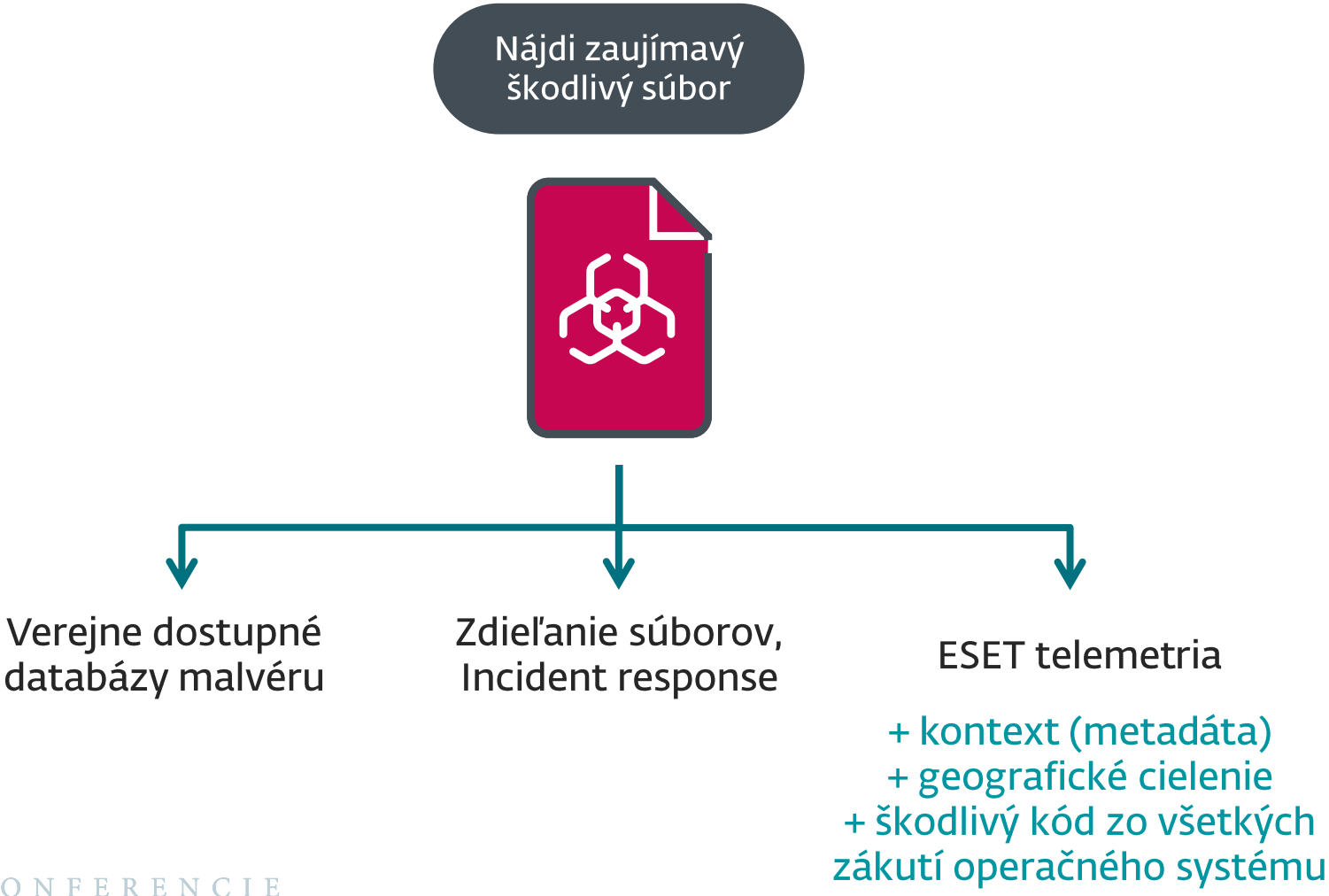
25 Jan 2022 - 11:30AM

UEFI Scanner

KONTROLA UEFI

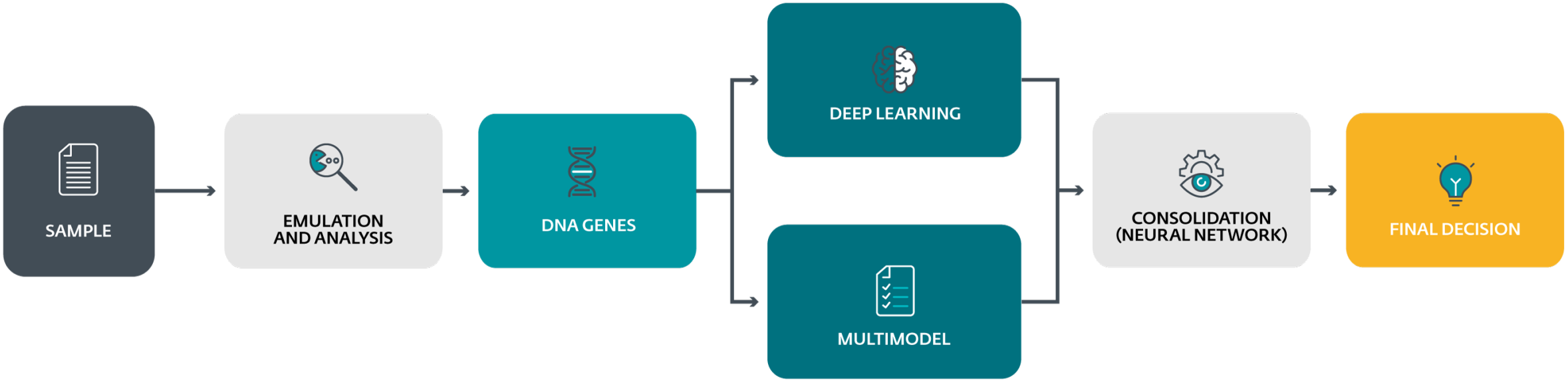


Výskum škodlivého kódu



Advanced Machine Learning

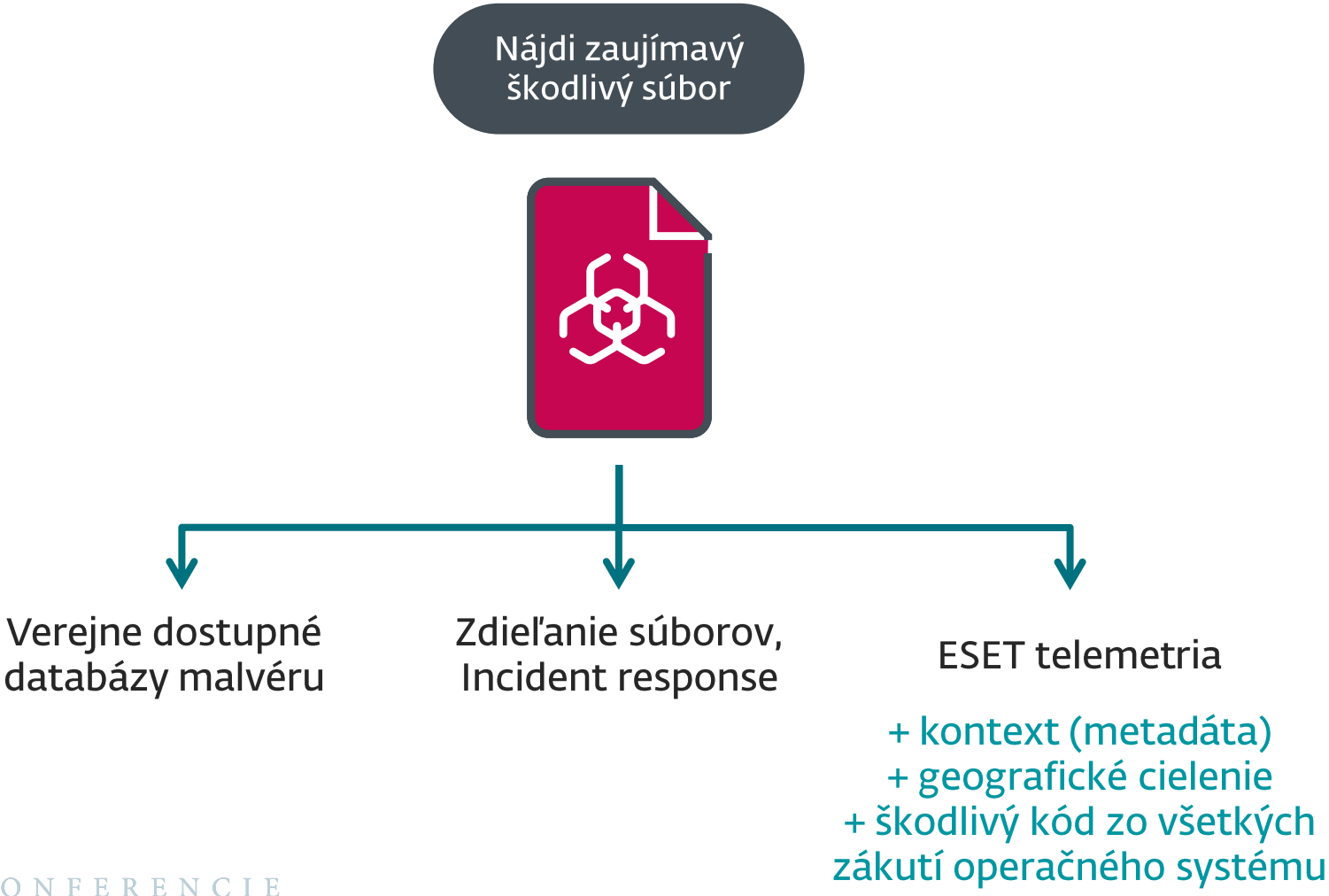
POKROČILÉ STROJOVÉ UČENIE


SAMPLE
EMULATION AND ANALYSIS
DNA GENES
DEEP LEARNING
MULTIMODEL
CONSOLIDATION (NEURAL NETWORK)
FINAL DECISION

Advanced Machine Learning

POKROČILÉ STROJOVÉ UČENIE

Výskum škodlivého kódu



Výskum škodlivého kódu

Under the hood of Wslink's multilayered virtual machine

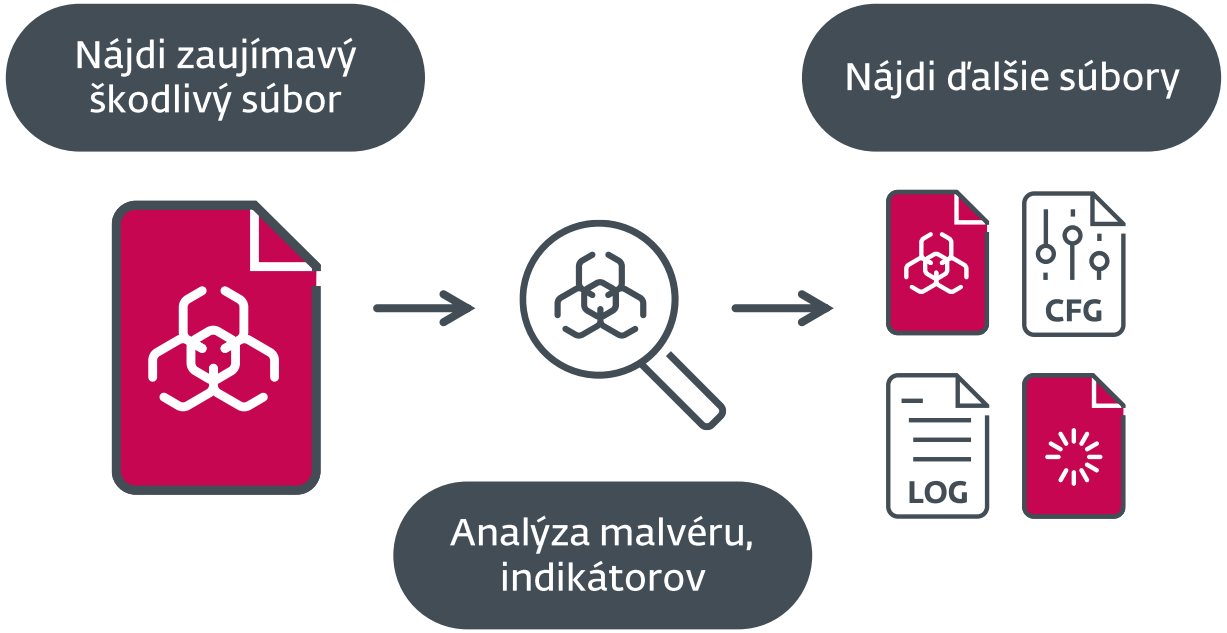
ESET researchers describe the structure of the virtual machine used in samples of Wslink and suggest a possible approach to see through its obfuscation techniques

Vladislav Hrčka

28 Mar 2022 - 11:30AM

Výskum škodlivého kódu

Výskum škodlivého kódu



FamousSparrow: A suspicious hotel guest

Yet another APT group that exploited the ProxyLogon vulnerability in March 2021

 Tahseen Bin Taj

 Matthieu Faou

23 Sep 2021 - 11:30AM

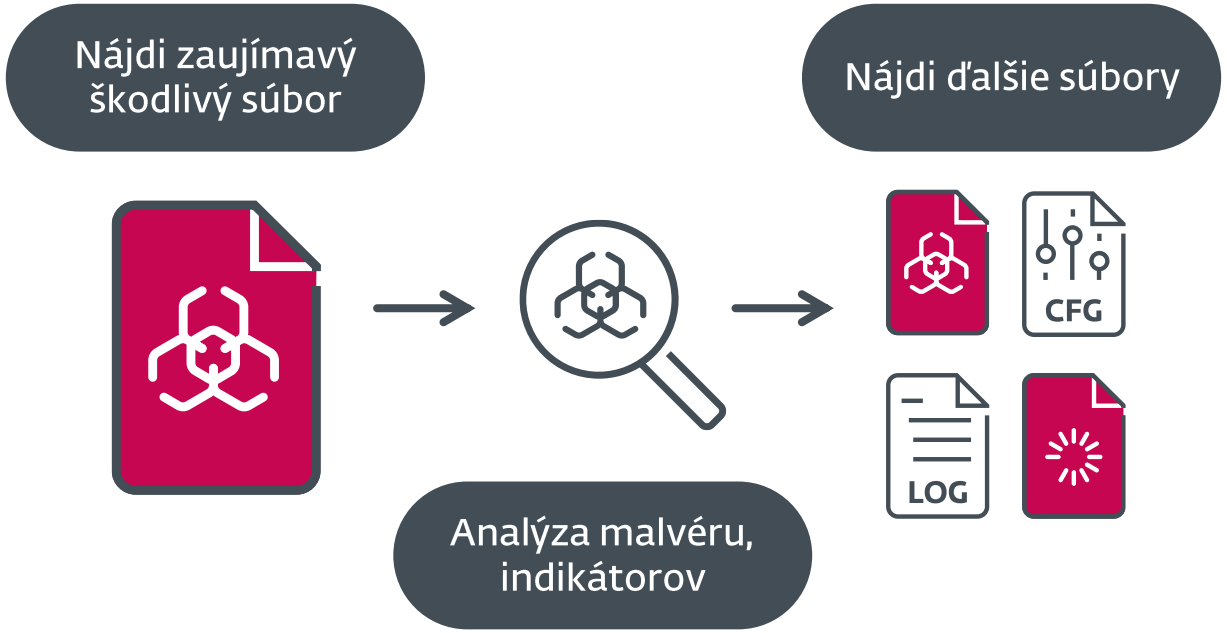
XDSpy: Stealing government secrets since 2011

ESET researchers uncover a new APT group that has been stealing sensitive documents from several governments in Eastern Europe and the Balkans since 2011

Matthieu Faou

2 Oct 2020 - 11:30AM

Výskum škodlivého kódu



ESET DNA Detections

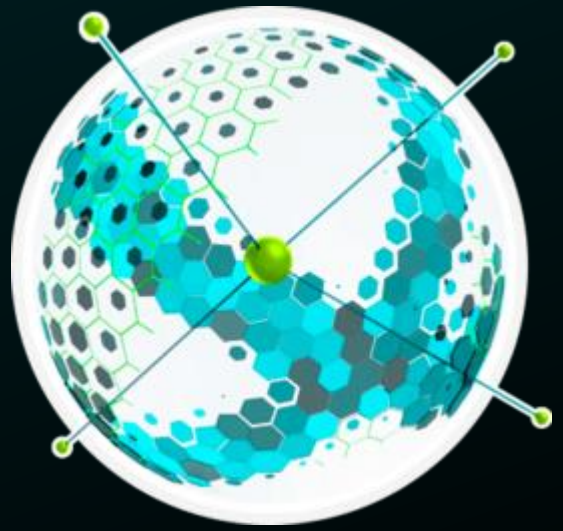
DNA DETEKCIE

Script Scanner & AMSI

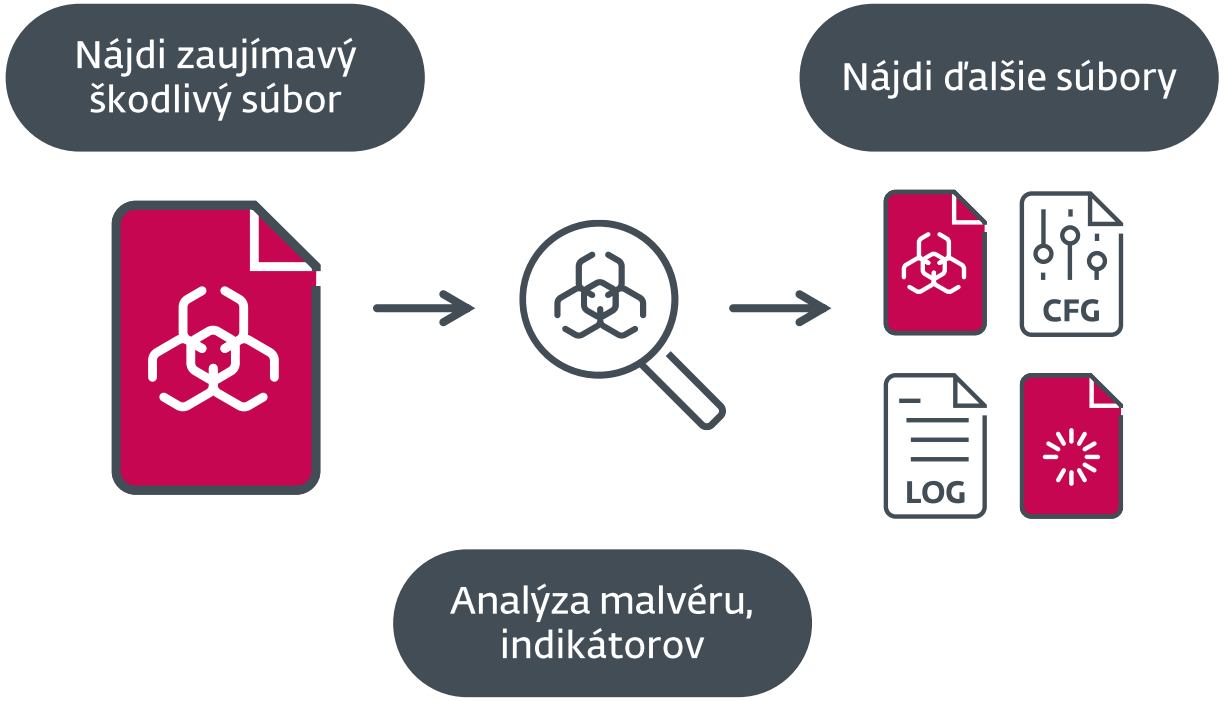
KONTROLA SKRIPTOV

Network Level Protection

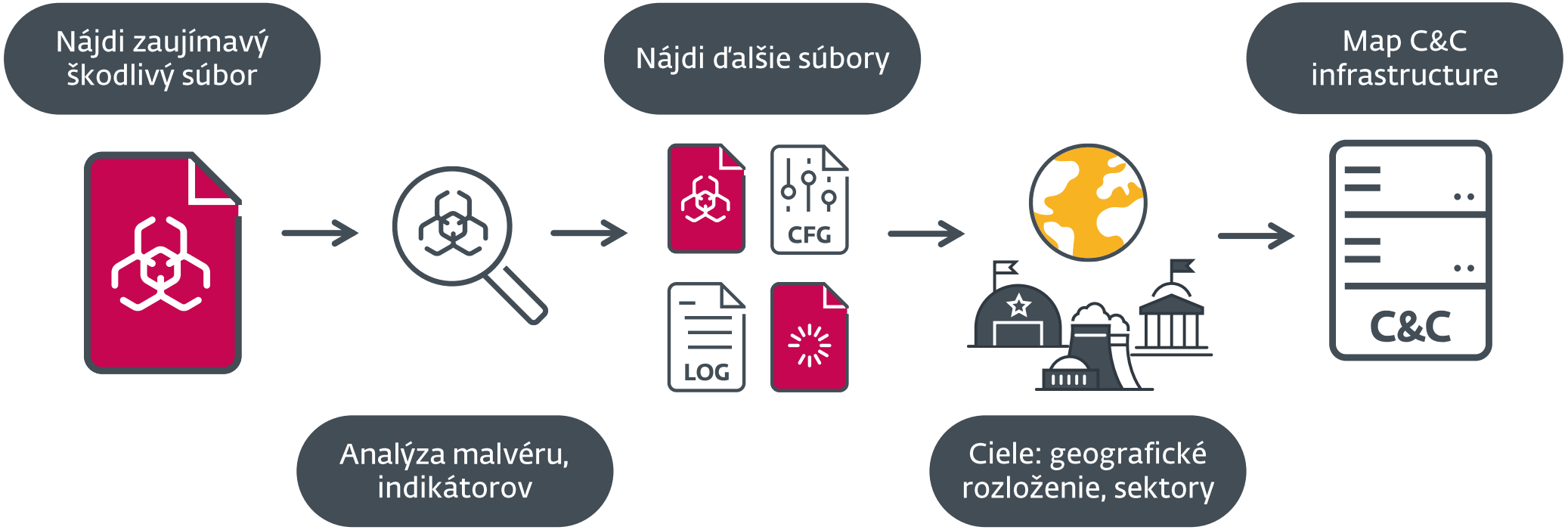
SIEŤOVÁ OCHRANA



Výskum škodlivého kódu

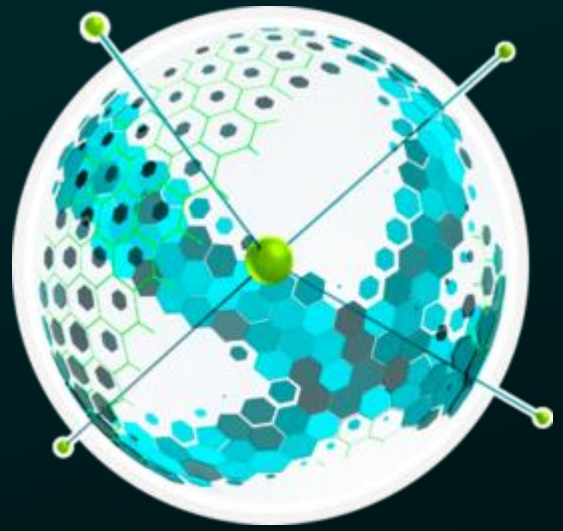


Výskum škodlivého kódu



Network Level Protection

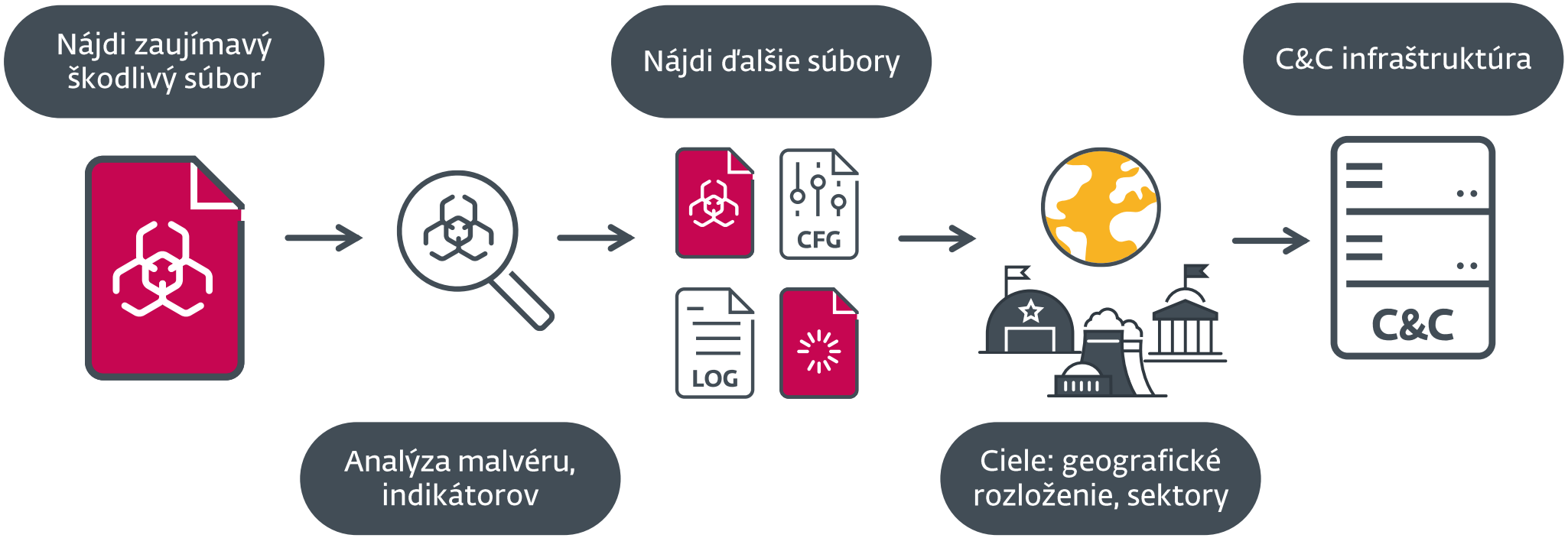
SIEŤOVÁ OCHRANA



LiveGrid® Protection

OCHRANA SYSTÉMOM LIVEGRID

Výskum škodlivého kódu



Výskum škodlivého kódu

A lookback under the TA410 umbrella: Its cyberespionage TTPs and activity

ESET researchers reveal a detailed profile of TA410: we believe this cyberespionage umbrella group consists of three different teams using different toolsets, including a new version of the FlowCloud espionage backdoor discovered by ESET.

 Alexandre Côté Cyr  Matthieu Faou

27 Apr 2022 - 03:00PM

SECURITY DAYS

A čo crimeware?

Digital Security
Progress. Protected.

&

SME KONFERENCIE

Botnet Analyzer

OCHRANA PRED BOTNETMI

The dirty dozen of Latin America: From Amavaldo to Zumanek

The grand finale of our series dedicated to demystifying Latin American banking trojans

(e):r ESET Research

15 Dec 2021 - 11:30AM

ESET takes part in global operation to disrupt Zloader botnets

ESET researchers provided technical analysis, statistical information, and known command and control server domain names and IP addresses

 Jean-Ian Boutin  Tomáš Procházka

13 Apr 2022 - 06:00PM

SECURITY DAYS

A čo ďalej?

Digital Security
Progress. Protected.

&

SME KONFERENCIE

welivesecurity BY eset

Award-winning news, views, and insight
from the ESET **security community**

In English

Menu

Research

Expert content, for researchers by researchers

Research

The dirty dozen of Latin America: From Amavaldo to Zumanek

The grand finale of our series dedicated to demystifying Latin American banking trojans

ESET Research 15 Dec 2021 - 11:30AM

Launching ESET Research Podcast: A peek behind the scenes of ESET discoveries

Press play for the first episode as host Aryeh Goretsky is joined by Zuzana Hromcová to discuss native IIS malware

Roman Kovac 2 Dec 2021 - 11:30AM

Jumping the air gap: 15 years of nation-state effort

ESET researchers studied all the malicious frameworks ever reported

Follow us

Newsletter – Ukraine Crisis section

Email...

Submit

Newslette

Email...

Our exper

ESET research

3,049 Tweets

Following

ESET research

@ESETresearch Follows you

Security research and breaking news straight from ESET Research Labs.

welivesecurity.com/research/ Joined July 2009

31 Following **27.1K** Followers

Followed by Thibaut, AVAR (Association of Anti-Virus Asia Researchers), and 34 others you follow

ESET research @ESETresearch · Jul 19

#ESETresearch uncovers #CloudMensis, spyware for
storage as a way to communicate back and forth its op
@marc_etienne_
welivesecurity.com/2022/07/19/i-s... 1/7

welivesecurity.com
I see what you did there: A look a
ESET uncovers CloudMensis, a

welivesecurity™ BY ESET

UEFI threats moving to the ESP: Introducing ESPecter bootkit

ESET research discovers a previously undocumented UEFI bootkit with roots going back all the way to at least 2012

Martin Smolár

Anton Cherepanov

5 Oct 2021 - 11:30AM

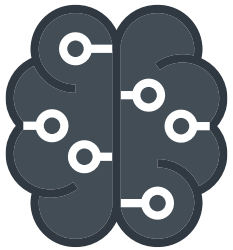
SECURITY DAYS

Čo sa skrýva za ESET výskumom škodlivého kódu?

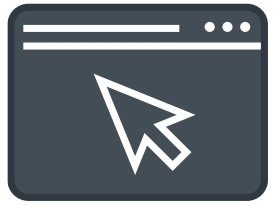
Digital Security
Progress. Protected. & SME KONFERENCIE

ESET
výskumníci

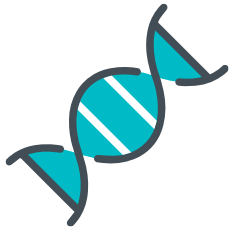
Spolupráca s
partnermi



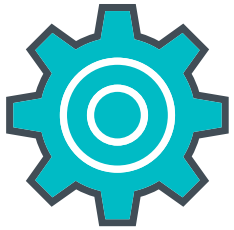
OSINT zdroje



Externé
služby



ESET
technológie



ESET
Interné nástroje

ESET
používatelia

SECURITY DAYS

Ďakujem za pozornosť!

Digital Security
Progress. Protected. & SME KONFERENCIE