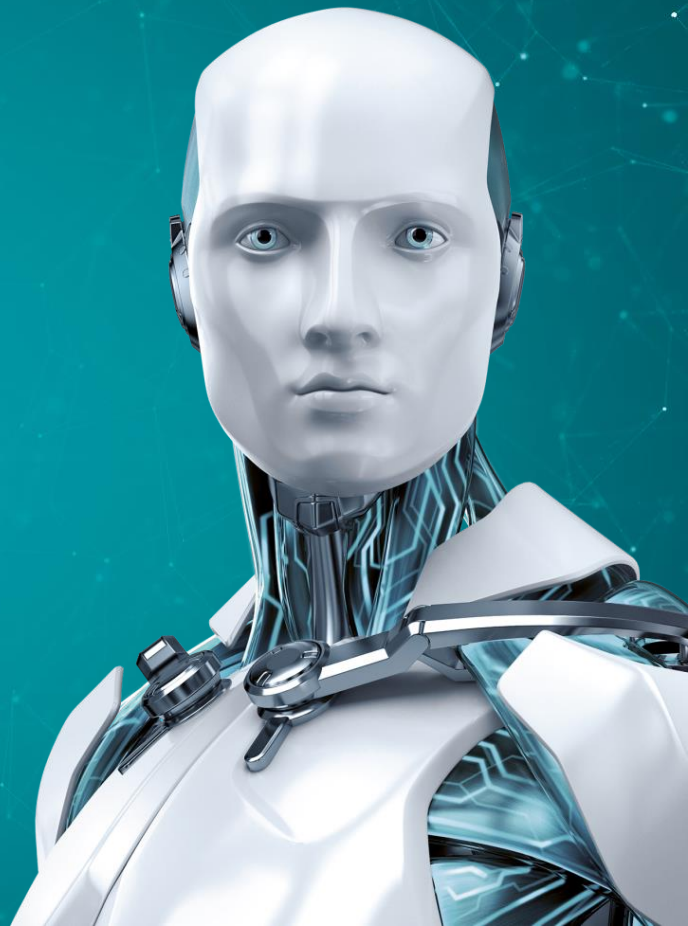
ENJOY SAFER TECHNOLOGY™

ZAUJÍMAVÉ PRÍPADY Z VIRUSLABU

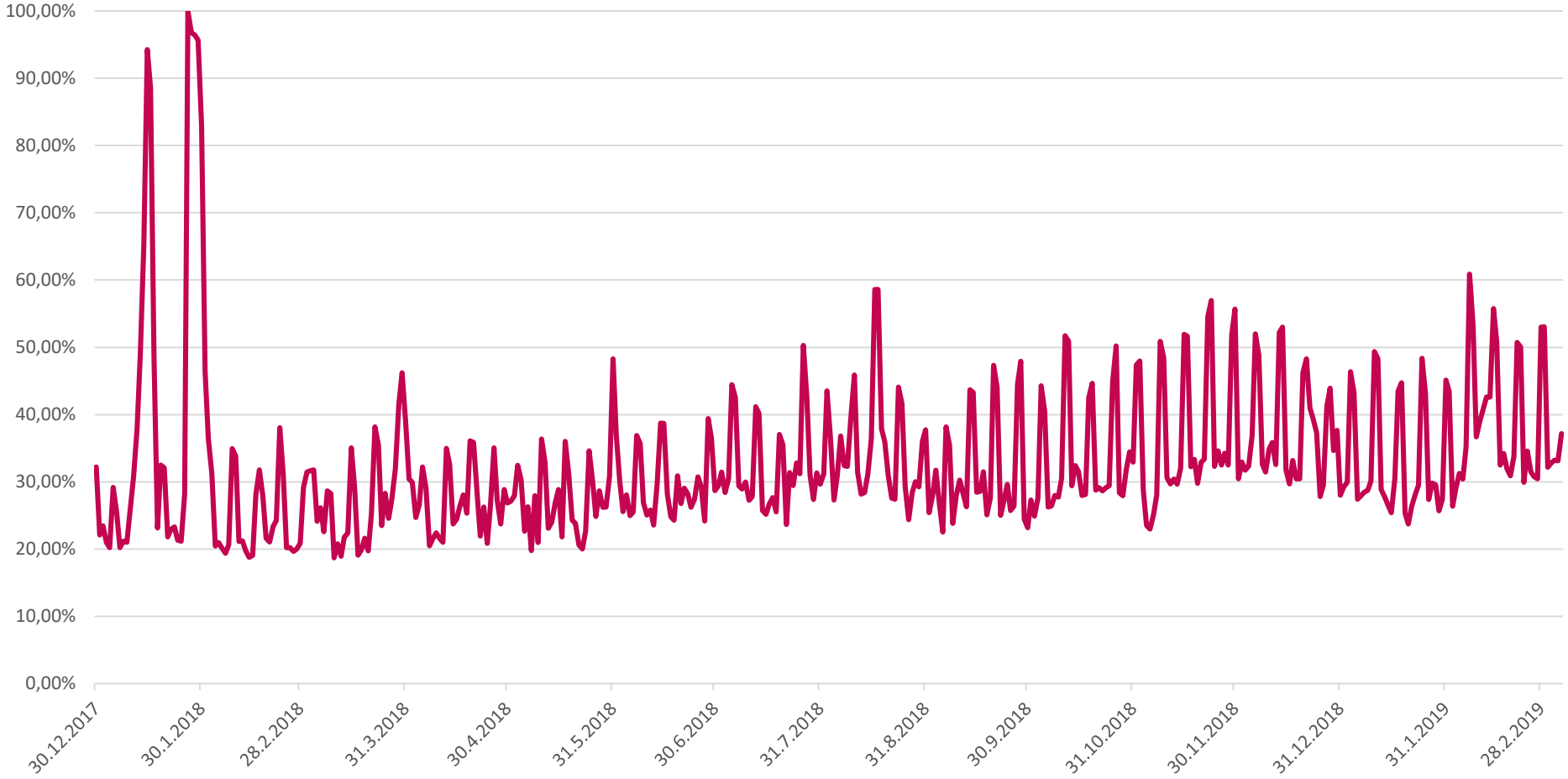
Ondrej Kubovič, ESET Security Awareness Specialist



Spam

...a ransomware

Globálny trend spamu

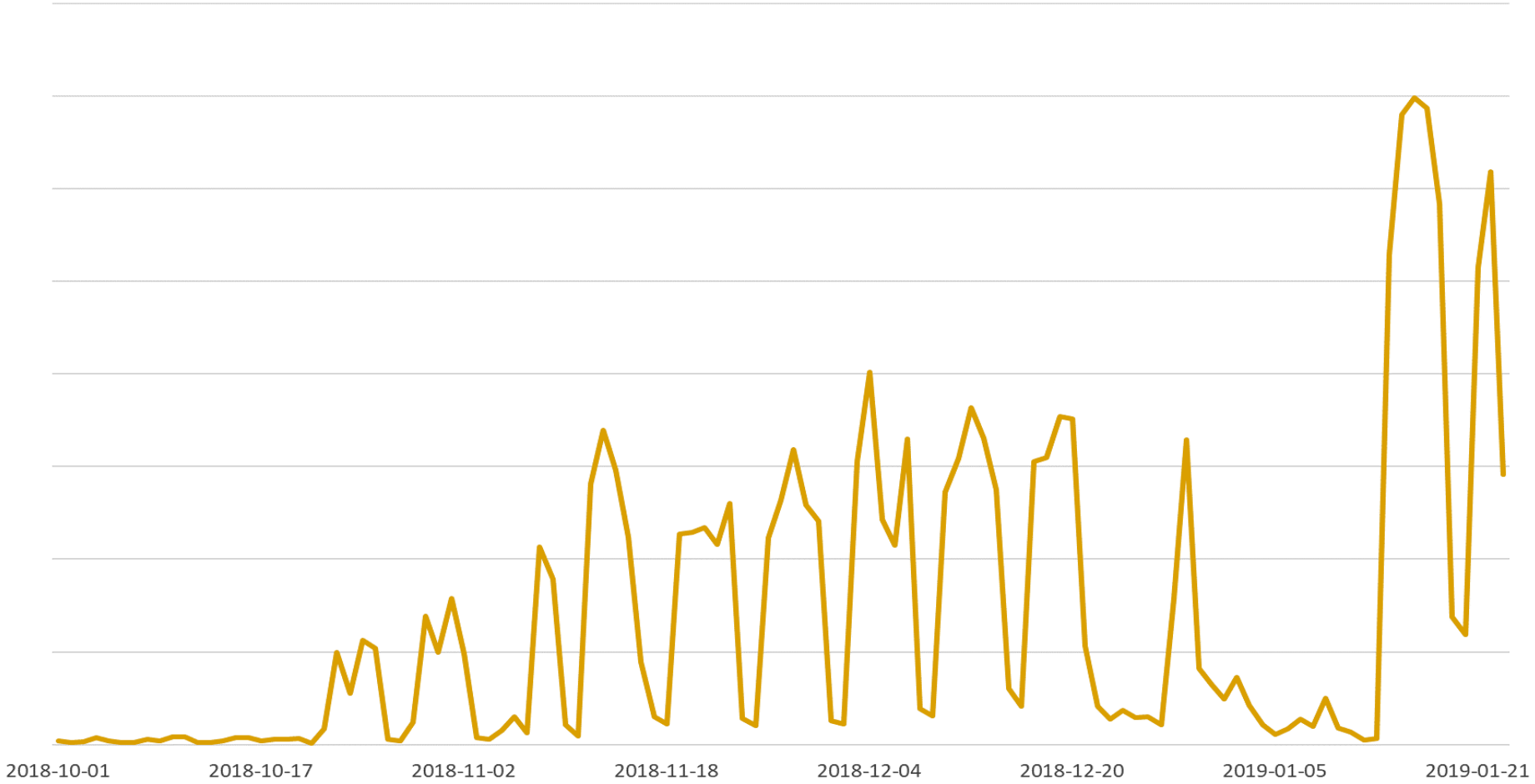


Russia hit by new wave of ransomware spam

Among the increased number of malicious JavaScript email attachments observed in January 2019, ESET researchers have spotted a large wave of ransomware-spreading spam targeting Russian users

Juraj Jánošík 28 Jan 2019 - 02:57PM

Ruská kampaň Nemucod-u



подробности заказа - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

Reply Reply All Forward More

From Кудряшов

Subject **подробности заказа** Detaily objednávky

To

1/18/2019 7:13 AM

Добрый день!

Dobrý deň!

Отправляю подробности заказа. Документ во вложении

Posielam vám detaily o objednávke. Dokument je v prílohe.

Кудряшов Денис

Denis Kudrashev

Менеджер.

Manager

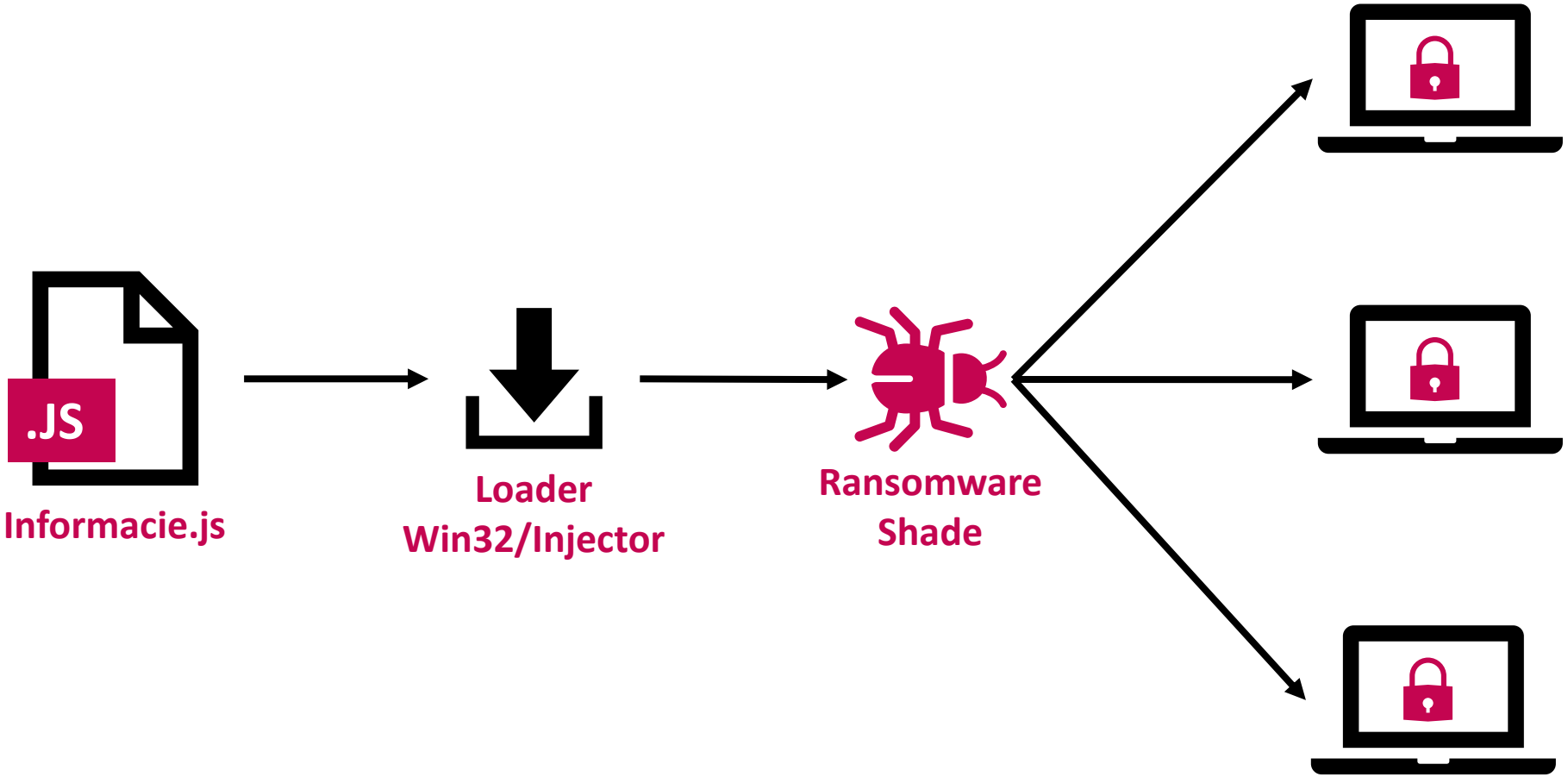
Публичное Акционерное Общество «БИНБАНК»

(495) 755-50-75, 8 800 200-50-75

1 attachment: info.zip 3.2 KB → JavaScript súbor “Информация.js“ = Informacie.js

Save

Shade ransomware



Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
1C75444CDBB110436B9C|0
на электронный адрес pilotpilot088@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке: https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/

All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
1C75444CDBB110436B9C|0
to e-mail address pilotpilot088@gmail.com .
Then you will receive all necessary instructions.
All the attempts of decryption by yourself will result only in irrevocable loss of your data.
If you still want to try to decrypt them by yourself please make a backup at first because
the decryption will become impossible in case of any changes inside the files.
If you did not receive the answer from the aforecited email for more than 48 hours (and only in this case!),
use the feedback form. You can do it by two ways:
1) Download Tor Browser from here:
https://www.torproject.org/download/download-easy.html.en
Install it and type the following address into the address bar:
http://cryptsen7fo43rr6.onion/
Press Enter and then the page with feedback form will be loaded.
2) Go to the one of the following addresses in any browser:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/

“Love you” malspam gets a makeover for massive Japan-targeted campaign

ESET researchers have detected a substantial new wave of the “Love you” malspam campaign, updated to target Japan and spread GandCrab 5.1

Juraj Jánošík 30 Jan 2019 - 02:57PM

:D - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address

From

Subject :D

To

1 attachment: PIC0-5967725682019-jpg.zip 8.6 KB

Yui Aragaki ;) - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address

From

Subject Yui Aragaki ;)

To

1 attachment: PIC0-5302900242019-jpg.zip 7.9 KB

Misia ;) - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From

Reply Reply All Forward More

Subject Misia ;) 8:53 AM

To

1 attachment: PIC0-14310656162019-jpg.zip 7.8 KB Save

Kyary Pamyu Pamyu ;) - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address

From

Subject Kyary Pamyu Pamyu ;)

To

Kyoko Fukada ;) - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address

From

Subject Kyoko Fukada ;)

To

Yuriko Yoshitaka ;) - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From

Reply Reply All Forward More

Subject Yuriko Yoshitaka ;) 1:14 AM

To

**********UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED**********

*****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .XSXEWH

The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.

The server with your key is in a closed network TOR. You can get there by the following ways:

| 0. Download Tor browser - https://www.torproject.org/

| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser: http://gandcrabmfe6mnef.onion/34571e618494ffbb
| 4. Follow the instructions on this page

On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.

ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---
lAQAABonidc2J8EaQjmatZ+R8rFechyrh5A0xwIS6bP01UVIw4RbhB7/Vw6/XSoAUHWa+5scfVrIXVa5BwxIKBt861dzaUPLMyt56Mt8uvNbTIfFASFkqdZaHYHJuN45b6XJAOgJzudgMZ6/25Bpi1xBiF5zFvk55f2VL
HXR8q2OXRs7zDOzoUnkMr9mnVLLCuofmoof/4m8ramT8e8YVzR8VO+C8KYT1SEp/5yk557w147f66Mvc/78NiaiMTiIhYeF4qqIMRx6H1uqKzZlfYIvv2UoSrV4Sj24Wyu/3yDQQpEMCPSJPpYsX/NaMwVW1I3JPlu2fa
QuW4lcp1GWS37HHYDKsAYnq9wxzVwxXABT4oMW1mposDCMUP7/fwcbbj00vQW29sd65pp3jZdlYQKKHG7U5UO7rGldfQ76ZwXu85FqgGyd7rUhhLUeqwtyzRP7d3J1XTJ4duT8xy/aEGntsQ+kNR1igD3LBZ9ZKXE8NZb
---END GANDCRAB KEY---

Ransomware GandCrab v5.1

Je ransomware naozaj na ústupe?

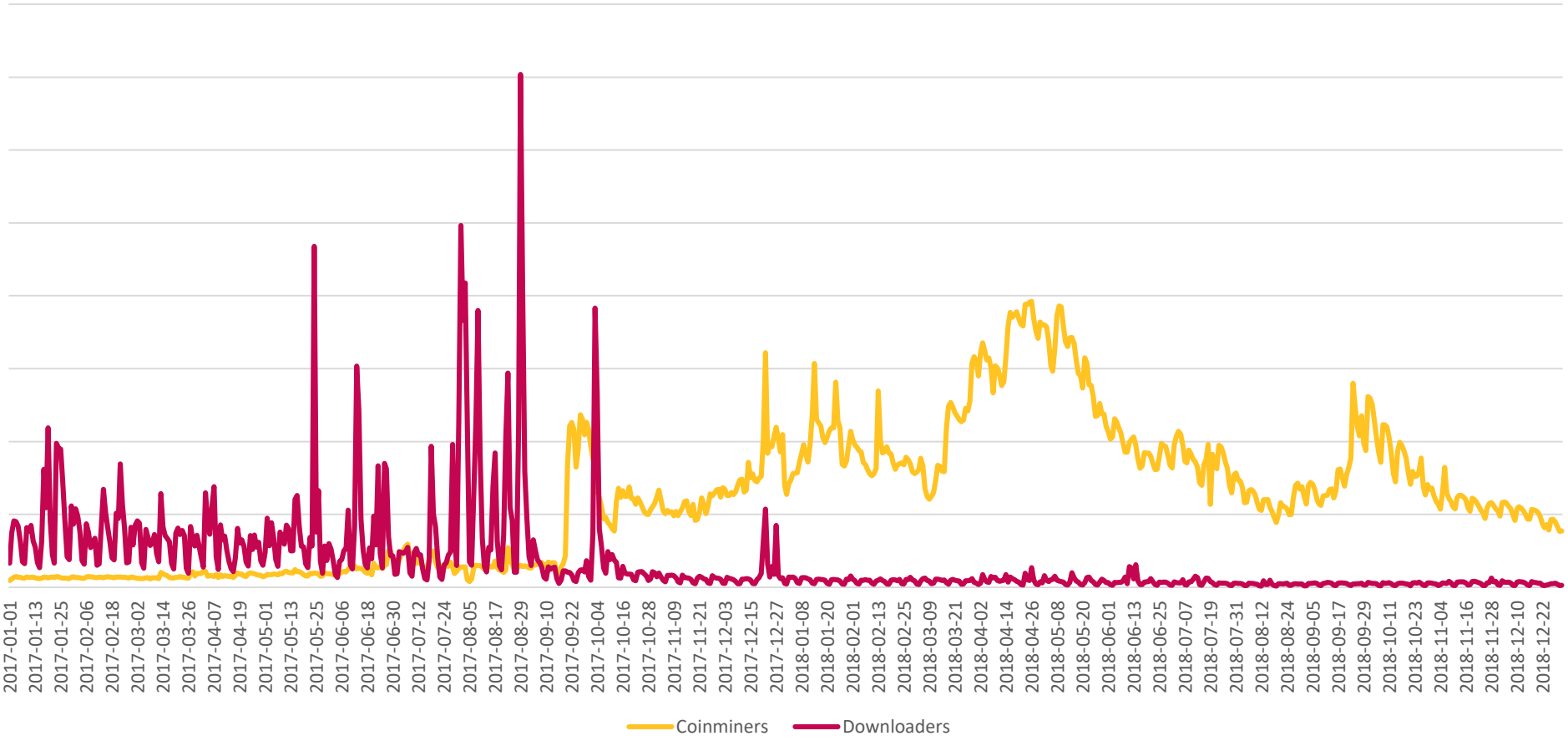
Coinhive cryptocurrency miner to call it a day next week

The service became notorious for its use by ne'er-do-wells looking to make a quick buck by hijacking the processing power of victim machines to generate virtual money

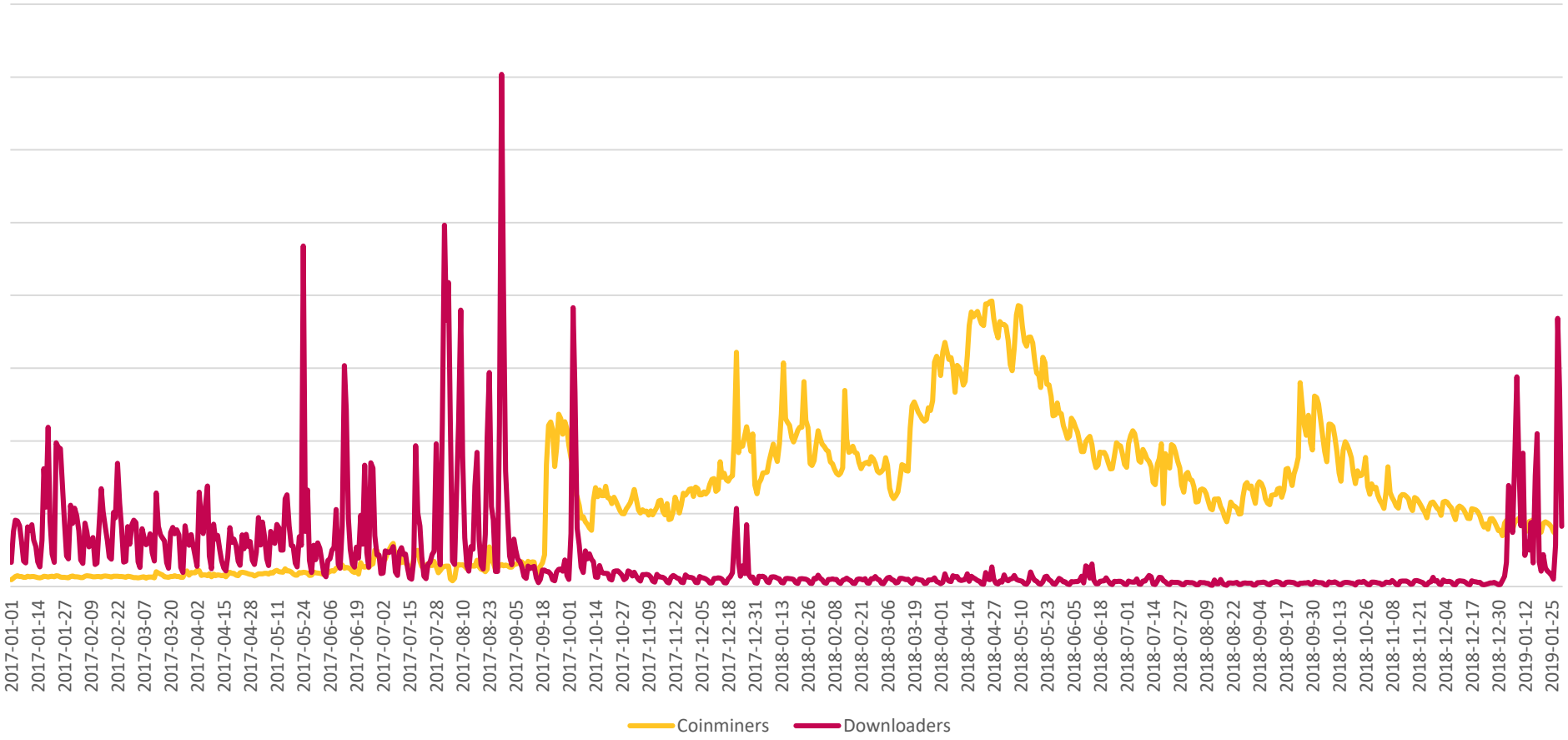
Tomáš Foltýn 28 Feb 2019 - 03:47PM

28. Február 2019

Coinminery vs. Downloadery



Coinminery vs. Downloadery



ESET® DYNAMIC THREAT DEFENSE

Prevent zero-day threats with powerful cloud-based sandboxing

CONTACT SALES

110m+ users worldwide

400k+ business customers

200+ countries & territories

13 global R&D centers

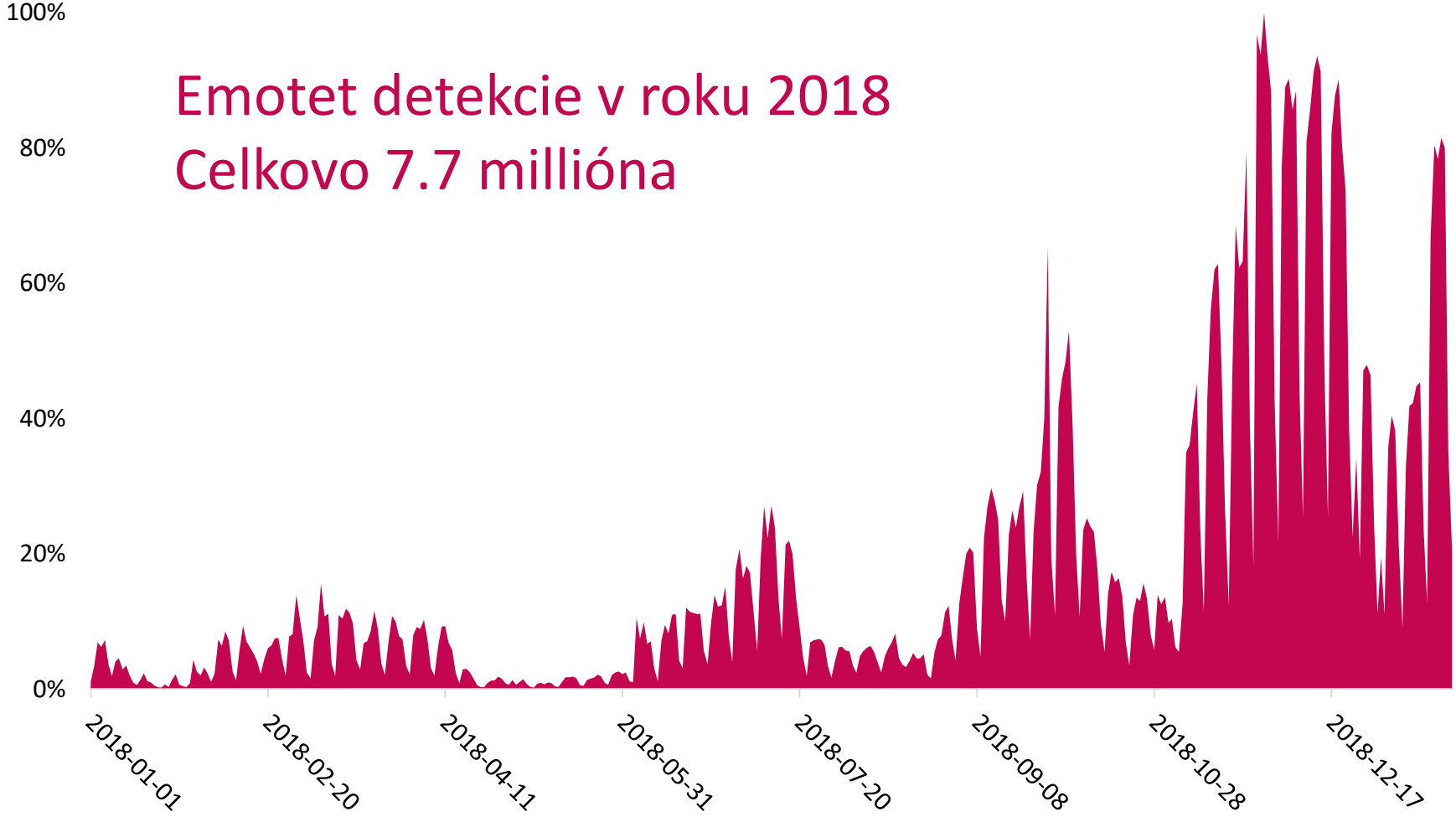
ESET Dynamic Threat Defense

provides another layer of security for ESET products like Mail Security and Endpoint products by utilizing a cloud-based sandboxing technology to detect new, never before seen type of threats. Future proof your company IT security with:

- **Behavior-based Detection**
- **Machine Learning**
- **Zero-day Threats Detection**
- **Cloud Sandbox**

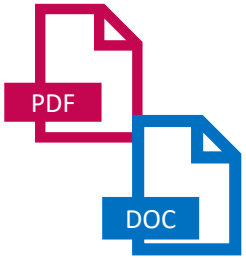
Emotet

Emotet detekcie v roku 2018
Celkovo 7.7 millióna

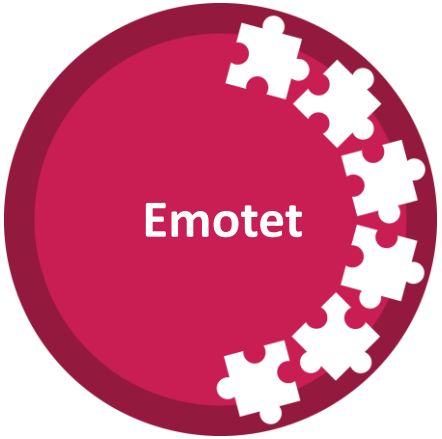


E-mail

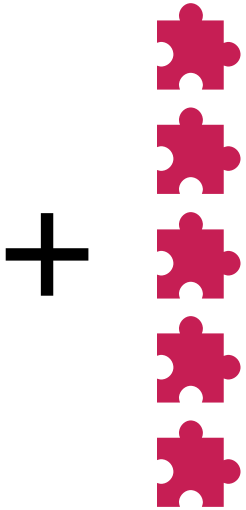
Príloha



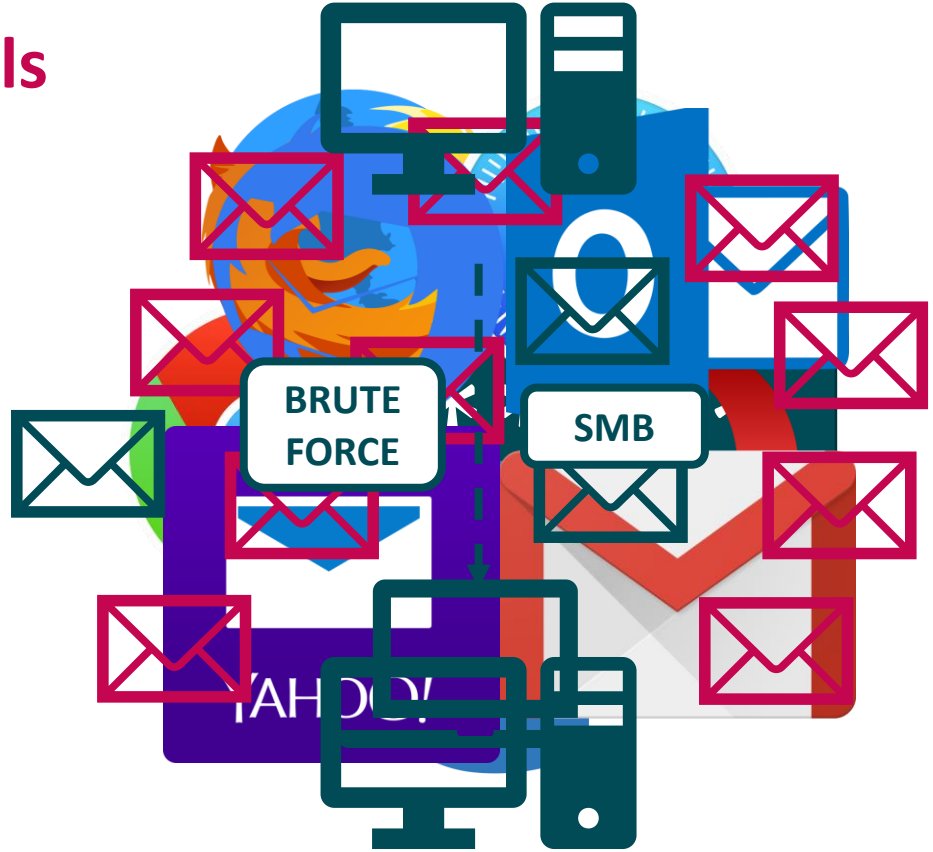
Emotet Agent



Modul

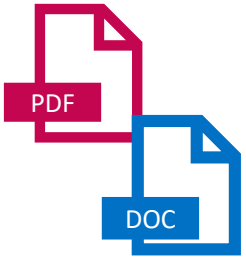


- Password Recovery Tools
- Credential Enumerator
- WebBrowserPassView
- MailPassView alebo Outlook Scraper
- Spammer

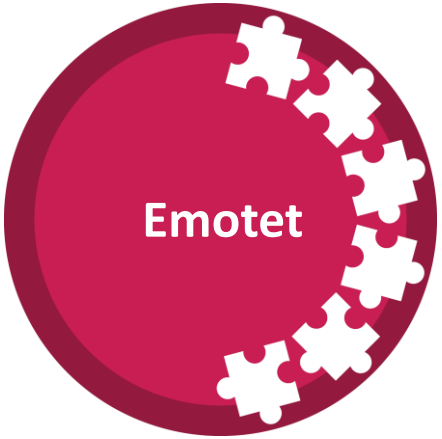


E-mail

Príloha



Emotet Agent



Banking Malware

Gootkit

Nymaim

TrickBot

IcedId

Emotet

ZBot

Ursnif

Qbot

Dridex

Task Manager

File Options View

Processes | Performance | App history | Startup | Users | Details | Services

Name	5% CPU	56% Memory	0% Disk	0% Network	1% GPU	GPU Engine
Background processes (89)						
64-bit Synaptics Pointing Enhan...	0%	0.6 MB	0 MB/s	0 Mbps	0%	
Active Protection System	0%	0.1 MB	0 MB/s	0 Mbps	0%	
Adobe Acrobat Update Service	0%	0.2 MB	0 MB/s	0 Mbps	0%	
Application Frame Host	0%	7.9 MB	0 MB/s	0 Mbps	0%	
Auto Scroll Start Service	0%	0.3 MB	0 MB/s	0 Mbps	0%	
BACK Monitor Application (32 ...	0.1%	6.6 MB	0 MB/s	0 Mbps	0%	
Camera Mute Control Service fo...	0%	0.7 MB	0 MB/s	0 Mbps	0%	
COM Surrogate	0%	1.3 MB	0 MB/s	0 Mbps	0%	
Communications Utility launche...	0%	1.4 MB	0 MB/s	0 Mbps	0%	
Cortana (2)	0%	112.6 MB	0 MB/s	0 Mbps	0%	
CTF Loader	0.4%	1.7 MB	0 MB/s	0 Mbps	0%	
Device Association Framework ...	0%	0 MB	0 MB/s	0 Mbps	0%	
Device Association Framework ...	0%	1.1 MB	0 MB/s	0 Mbps	0%	
ESET Enterprise Inspector Agent	0%	22.0 MB	0 MB/s	0 Mbps	0%	
ESET Main GUI	0%	4.8 MB	0 MB/s	0 Mbps	0%	
ESET Management Agent Modu...	0%	11.1 MB	0 MB/s	0 Mbps	0%	
ESET Service (2)	0%	34.1 MB	0 MB/s	0 Mbps	0%	
f.lux (32 bit)	0%	2.5 MB	0 MB/s	0 Mbps	0%	
Groove Music	0%	0.1 MB	0 MB/s	0 Mbps	0%	

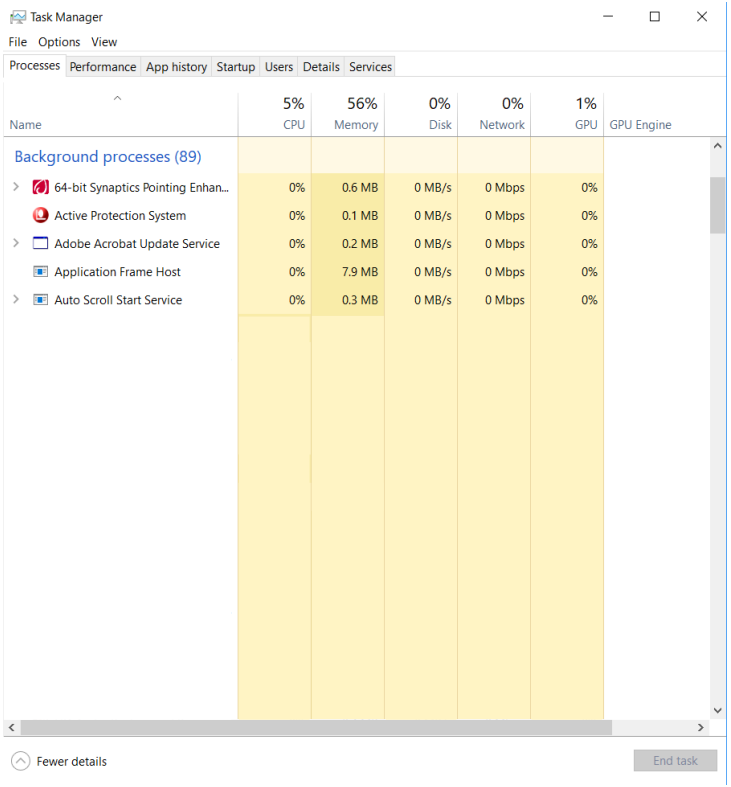
Fewer details | End task

Attacker's C&C

Return telemetry data

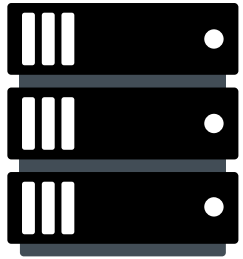
Victim

ESET ENJOY SAFER TECHNOLOGY

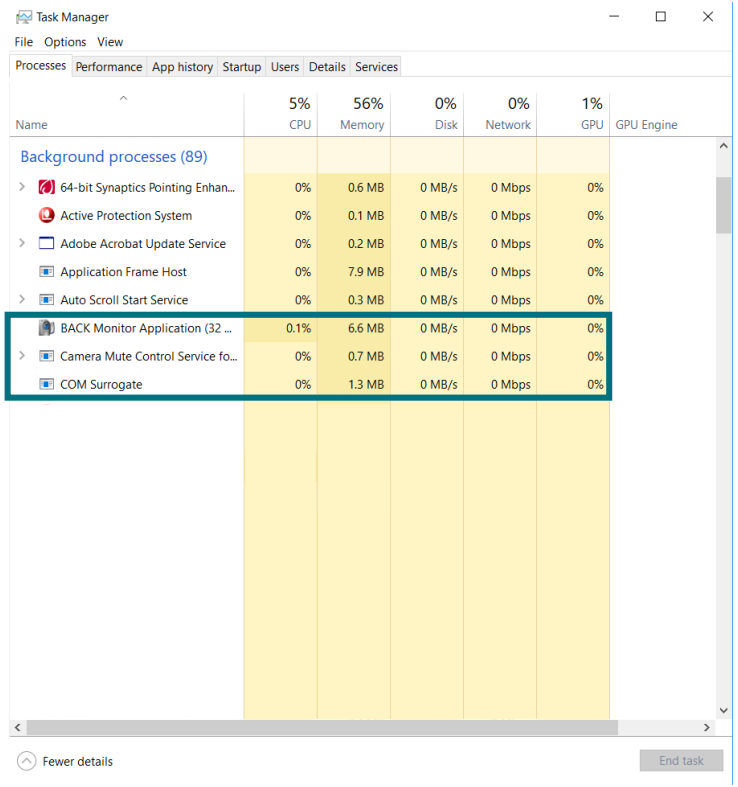


Researcher/ Honeypot

Attacker's C&C

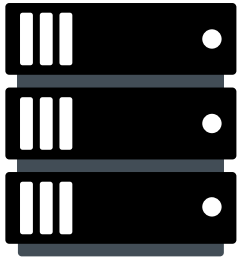


Reti Quit/Sleep Data



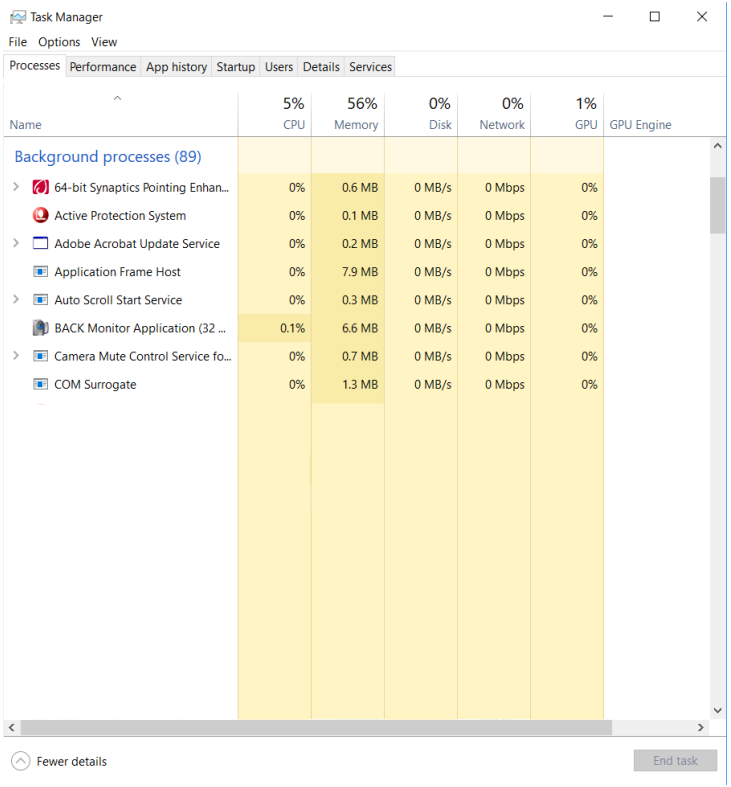
Researcher/ Honeypot

Attacker's C&C



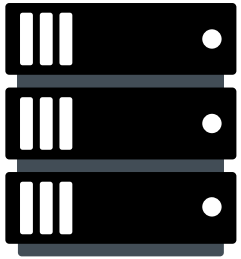
Re Command/ Data
Binary module

A few days later…



Researcher/ Honeypot

Attacker's C&C



Retu Quit/Sleep / Data

Turla

Používa vaša firma MS Outlook?

Turla: In and out of its unique Outlook backdoor

The latest ESET research offers a rare glimpse into the mechanics of a particularly stealthy and resilient backdoor that the Turla cyberespionage group can fully control via PDF files attached to emails

2009

Compilation timestamp (may be faked) of a basic version of the Outlook backdoor. It could only dump email content.

2013

Improvement: the backdoor could execute commands. They are sent by email in XML format.

2013

Last known version targeting The Bat! email client.

2016

Improvement: the commands are now sent as attachments in specially crafted PDF documents.

2017

Improvement: the backdoor is able to build PDF documents to exfiltrate data to the attackers.

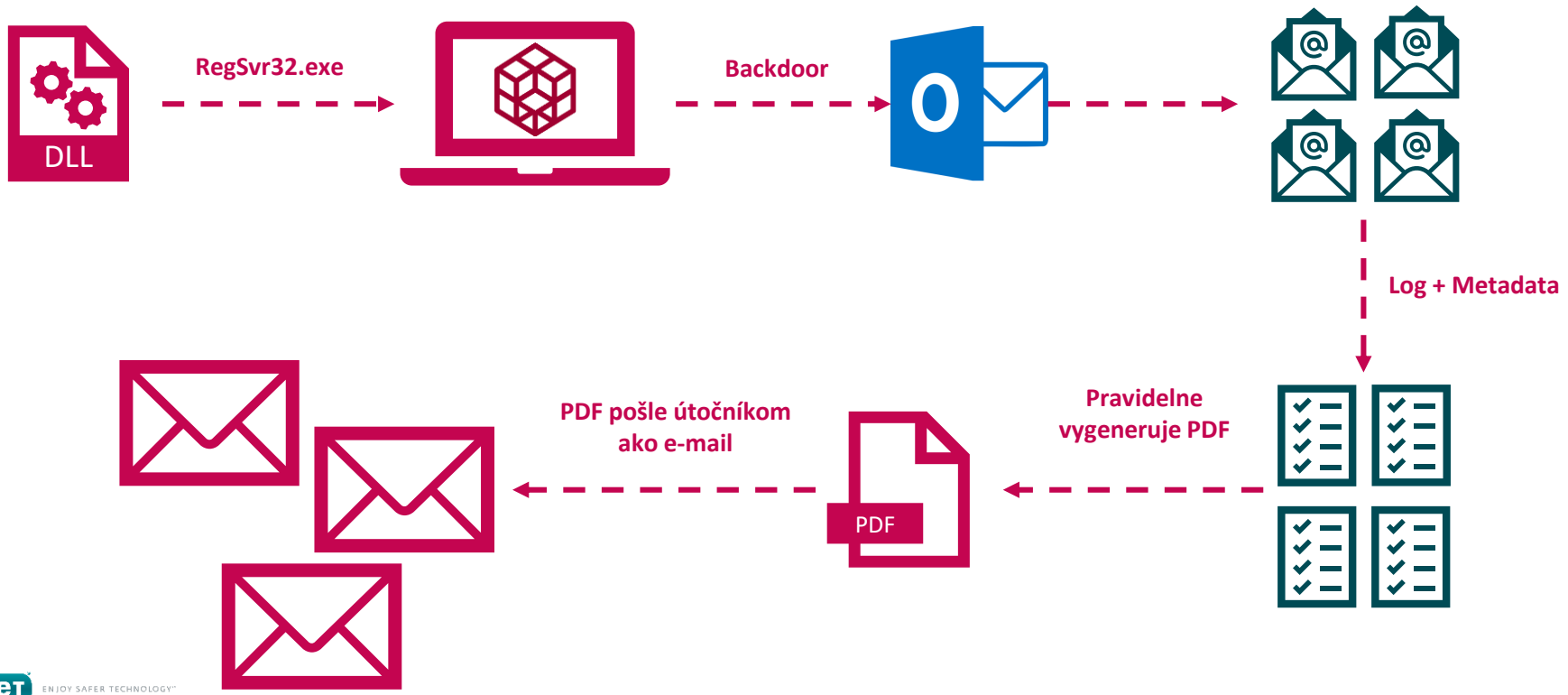
2018 April

Improvement: the backdoor can execute PowerShell commands by leveraging Empire PSInject.

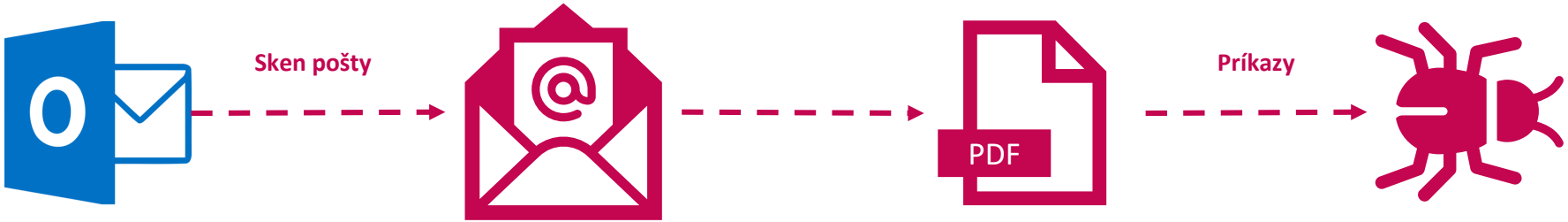
2018 March

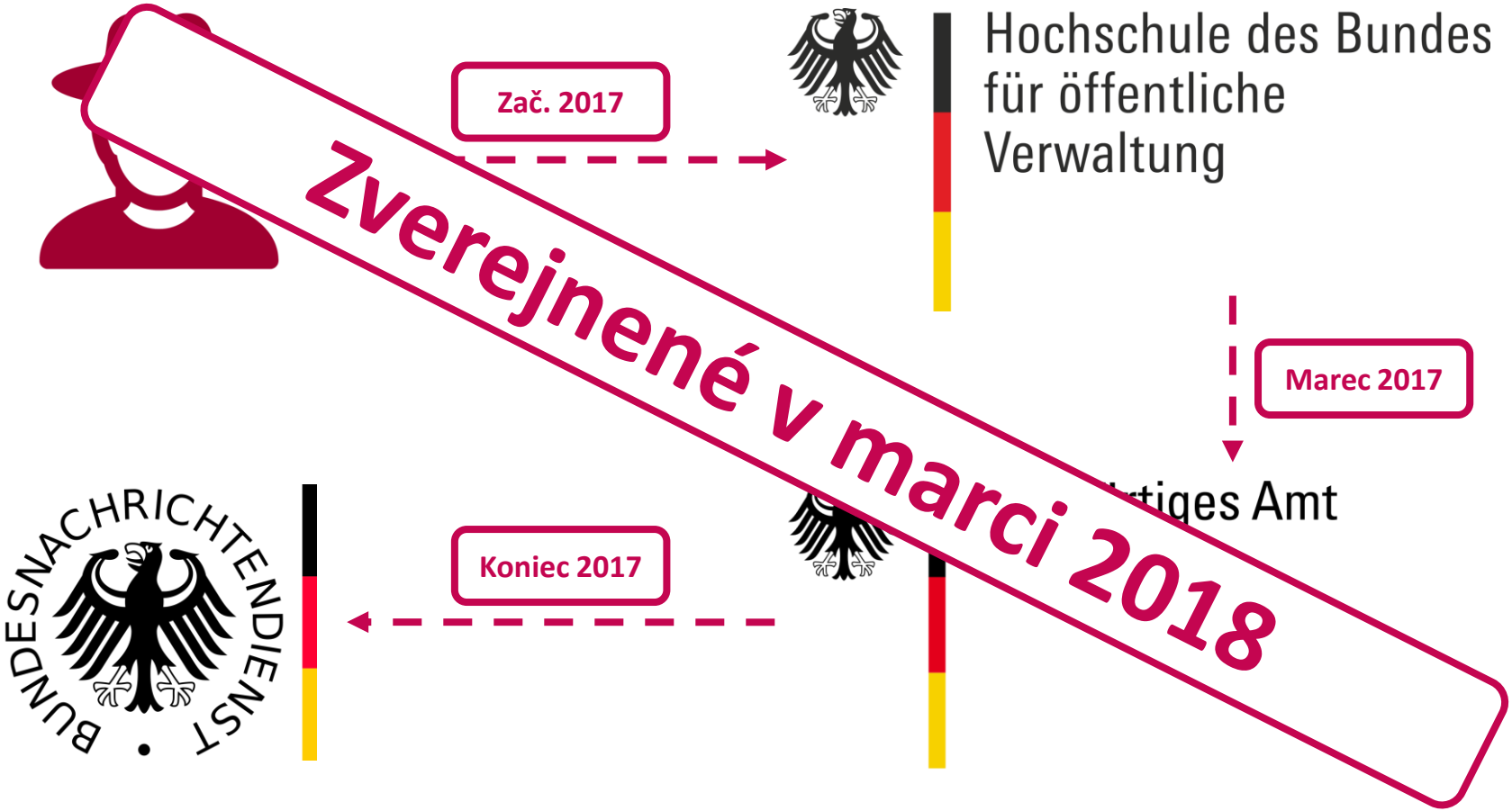
Public announcement of the compromise of the German government.

Exfiltráica dát



Ovládanie a príkazy





Ďalšie ciele

Vlády a ich predstavitelia

Vojenskí predstavitelia a zbrojárske firmy

Diplomati

ESET Research Whitepapers // August 2018

TURLA OUTLOOK BACKDOOR

Analysis of an unusual Turla backdoor

ENJOY SAFER TECHNOLOGY™

ESET® ENTERPRISE INSPECTOR

Uncover the unknown in your network with our EDR solution

CONTACT SALES

110m+ users worldwide

400k+ business customers

200+ countries & territories

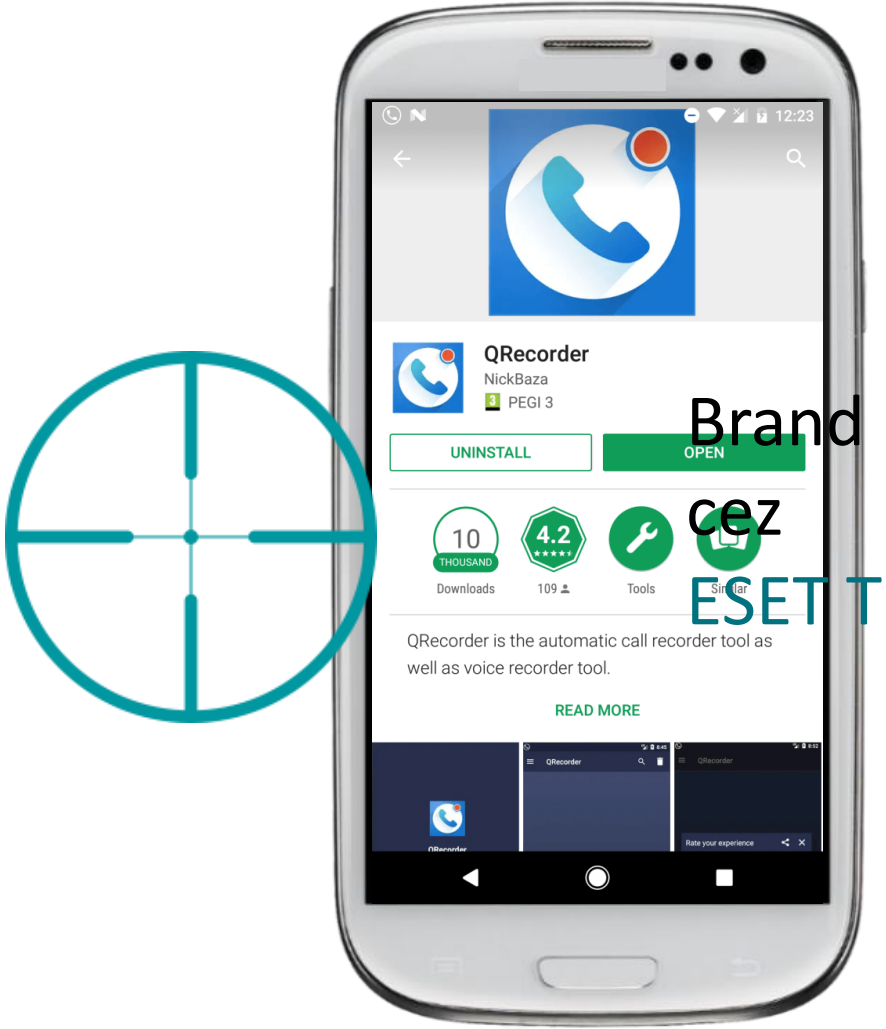
13 global R&D centers

ESET Enterprise Inspector

An Endpoint Detection & Response tool designed to exploit ESET's multilayered Endpoint Protection Platform. All layers send relevant data to ESET Enterprise Inspector, which analyzes vast amounts of real time endpoint data. The result is complete prevention, detection and response solutions for quick analysis and remediation of any security issue in the network enabling organizations to take immediate action to:

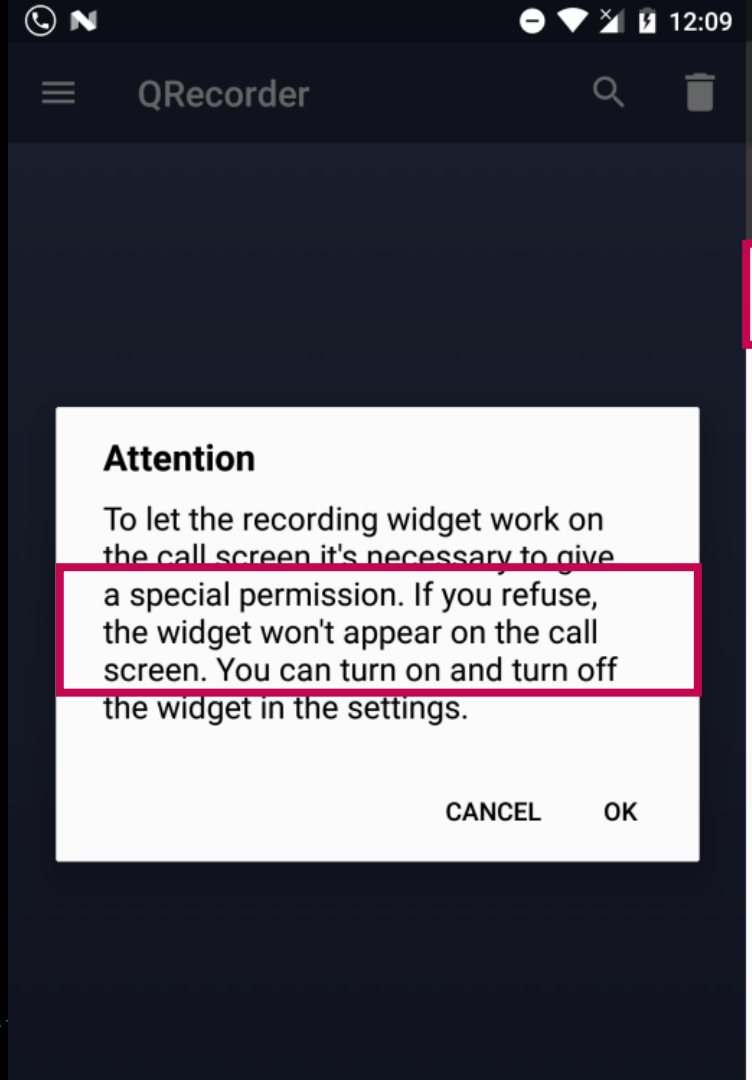
- **Detect advanced persistent threats**
- **Stop file less attacks**
- **Block zero-day threats**
- **Protect against ransomware**
- **Neutralize state-sponsored attacks**

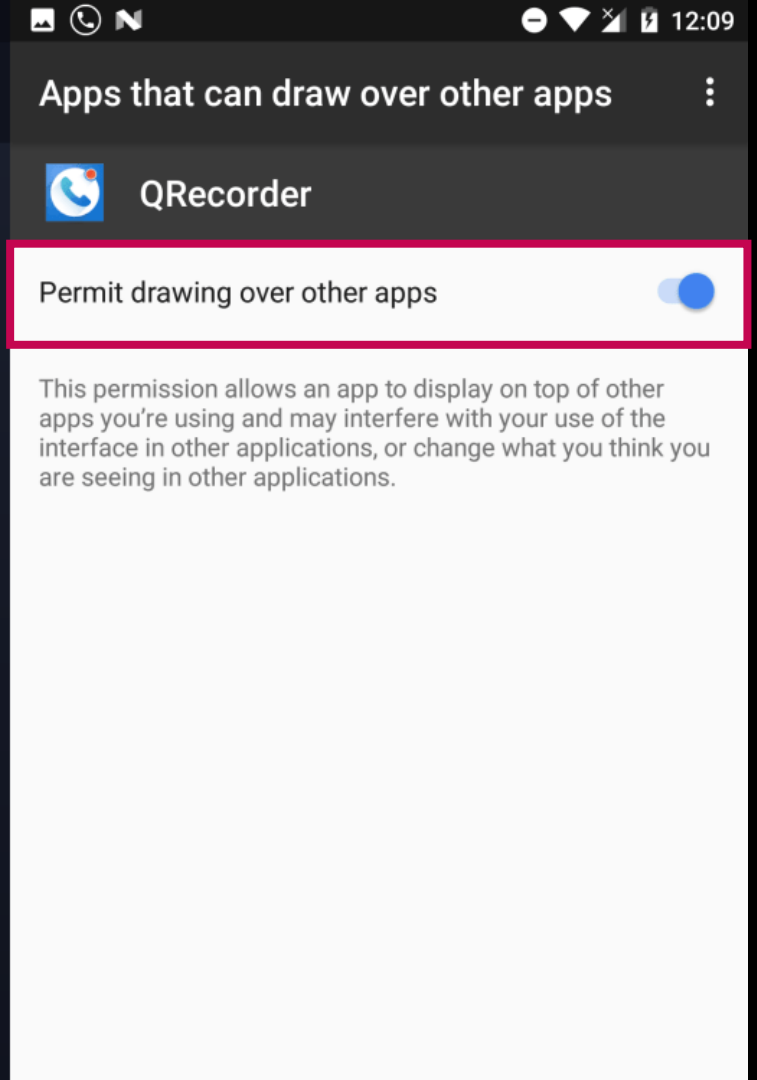
QRecorder

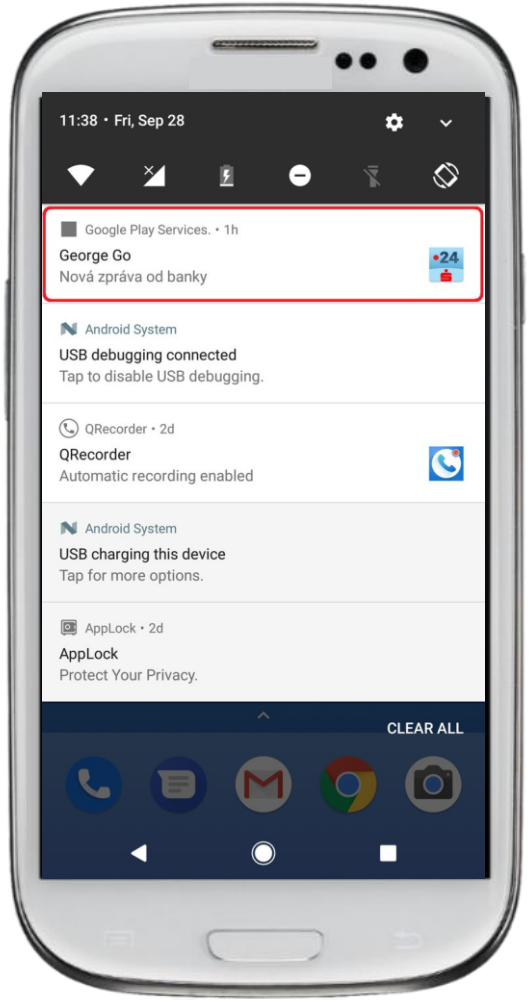


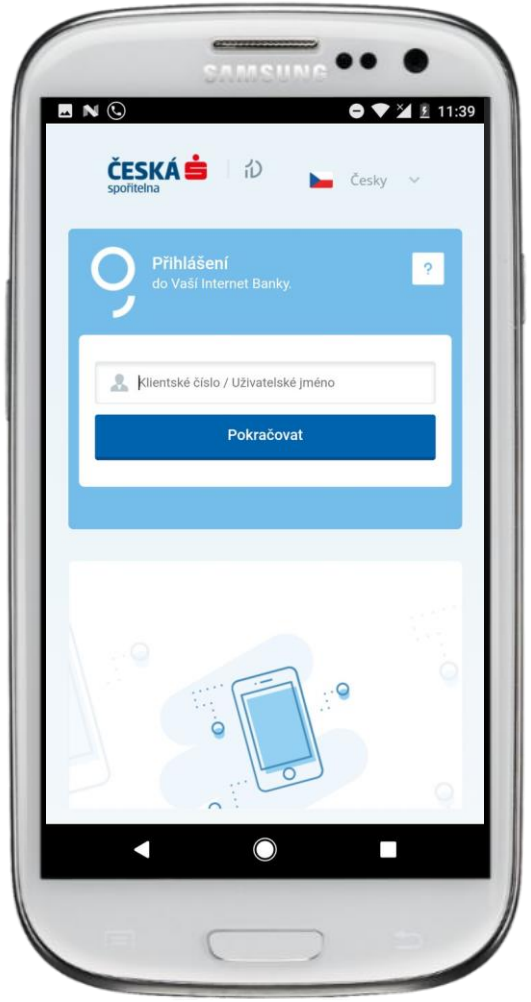
Brand protection servis cez ESET Threat Intelligence

ENJOY SAFER TECHNOLOGY







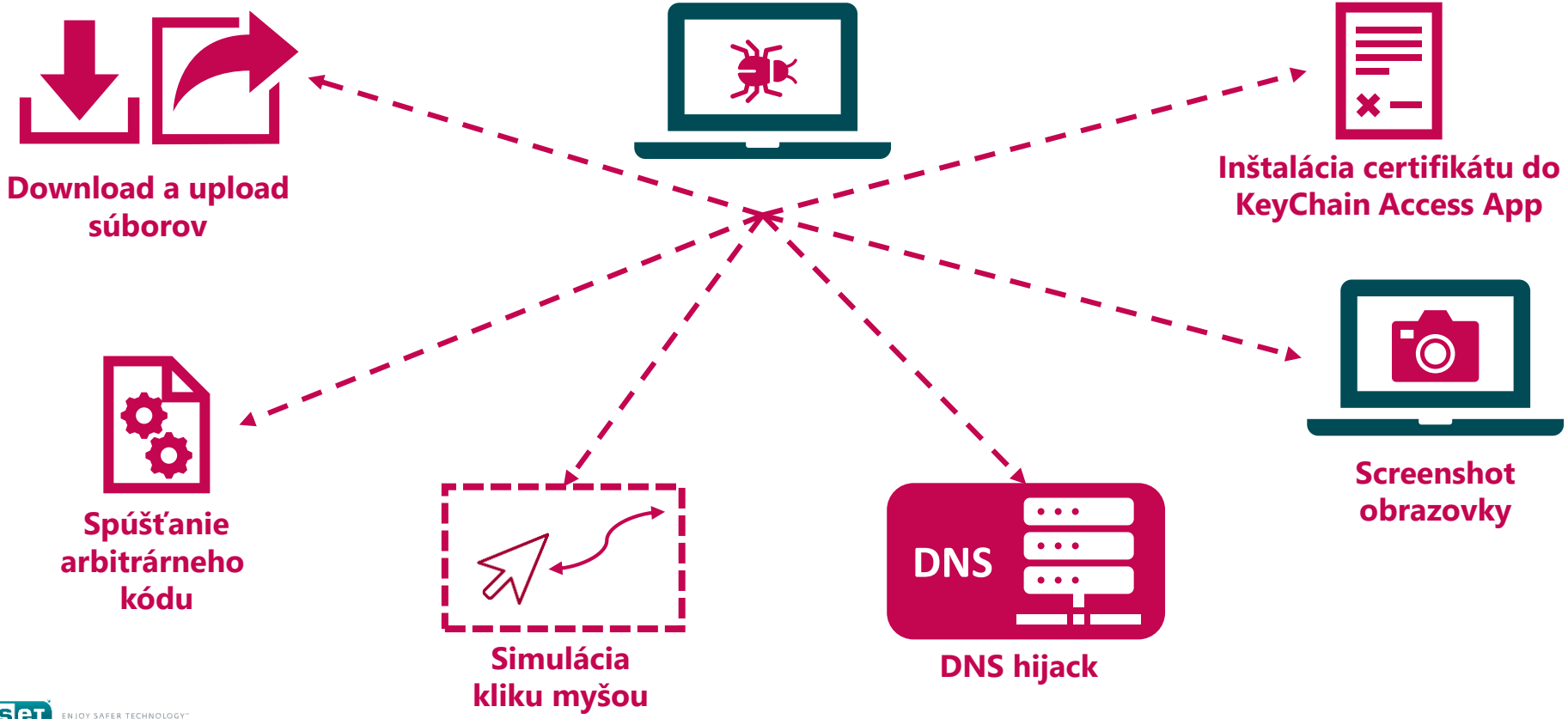


```
="Air Bank" android:name="gjfid.pziovmiq.eefff.Air" android:taskAffinity="cz.airbank.android" android:theme="@andr
l="George Go" android:name="gjfid.pziovmiq.eefff.Csas" android:taskAffinity="cz.csas.georgego" android:theme="@and
l="SERVIS 24" android:name="gjfid.pziovmiq.eefff.Service24" android:taskAffinity="com.cleverlance.csas.servis24" a
="Muj stav" android:name="gjfid.pziovmiq.eefff.Muj" android:taskAffinity="cz.csas.app.mujstav" android:theme="@and
l="ČSOB SmartBanking" android:name="gjfid.pziovmiq.eefff.Csob" android:taskAffinity="cz.csob.smartbanking" android
="Equa bank" android:name="gjfid.pziovmiq.eefff.Equ" android:taskAffinity="cz.equabank.mobilebanking" android:then
="Equa bank" android:name="gjfid.pziovmiq.eefff.Bsc" android:taskAffinity="com.icomvision.bsc.mobilebank" android:
l="mBank CZ" android:name="gjfid.pziovmiq.eefff.Mban" android:taskAffinity="cz.mbank" android:theme="@android:styl
l="Smart Banka" android:name="gjfid.pziovmiq.eefff.Mone" android:taskAffinity="cz.moneta.smartbanka" android:theme
l="Smart Banking" android:name="gjfid.pziovmiq.eefff.Rbap" android:taskAffinity="cz.rb.app.smartphonebanking" andr
l="Fio banka" android:name="gjfid.pziovmiq.eefff.Ulik" android:taskAffinity="cz.ulikeit.fio" android:theme="@andro
="BAWAG PSK" android:name="gjfid.pziovmiq.eefff.Baw" android:taskAffinity="at.bawag.mbanking" android:theme="@andr
="easybank" android:name="gjfid.pziovmiq.eefff.Easyb" android:taskAffinity="at.easybank.mbanking" android:theme="@
l="ING-DiBa" android:name="gjfid.pziovmiq.eefff.Inga" android:taskAffinity="at.ing.diba.client.onlinebanking" andr
="Oberbank" android:name="gjfid.pziovmiq.eefff.Ober" android:taskAffinity="at.oberbank.mbanking" android:theme="@a
="Banking" android:name="gjfid.pziovmiq.eefff.Volk" android:taskAffinity="at.volksbank.volksbankmobile" android:th
="Bank Austria" android:name="gjfid.pziovmiq.eefff.Unic" android:taskAffinity="com.bankaustria.android.olb" androi
="ELBA" android:name="gjfid.pziovmiq.eefff.Raifa" android:taskAffinity="com.isis_papyrus.raiffeisen_pay_eyewdg" an
```

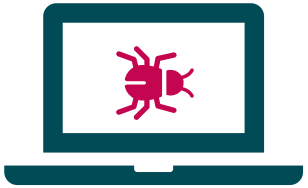
Česká polícia:
Najmenej 5 obetí
2.000.000 CZK

OSX/DNSChanger.A
a.k.a. OSX/MaMi

OSX/DNSChanger.A v1.1.0



OSX/DNSChanger.A v1.1.0



DNS hijack

Inštalácia certifikátu do KeyChain Access

Možný Man-in-The-Middle útok

ESET® ENDPOINT PROTECTION ADVANCED

Complete multilayered protection with remote security management

CONTACT SALES

REQUEST TRIAL

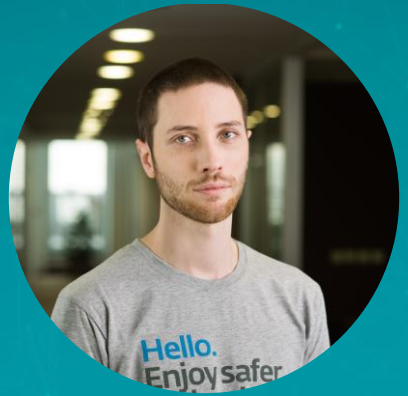
30-days free trial

- On-premise management
- Endpoint security
- File server security

ESET Endpoint Protection Advanced

Multilayered technology, machine learning and human expertise combined with automated security management. Provides:

- **Protection against targeted attacks**
- **Protection against ransomware**
- **Prevention of fileless attacks**
- **Remote management**



Ondrej Kubovič

ESET Špecialista pre digitálnu bezpečnosť

ondrej.kubovic@eset.sk