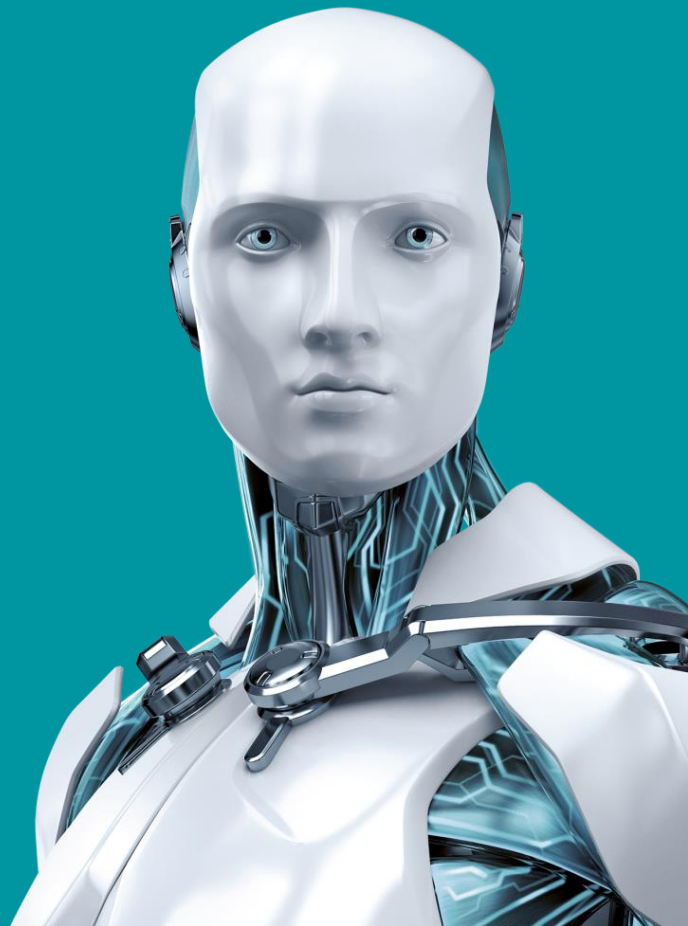
CYBERSECURITY
EXPERTS ON YOUR SIDE

KYBERNETICKÉ ÚTOKY V ČESKU

Evoluce ransomwaru

Václav Zubr
Pre-Sales Engineer

ESET
CYBERSECURITY
EXPERTS ON YOUR SIDE

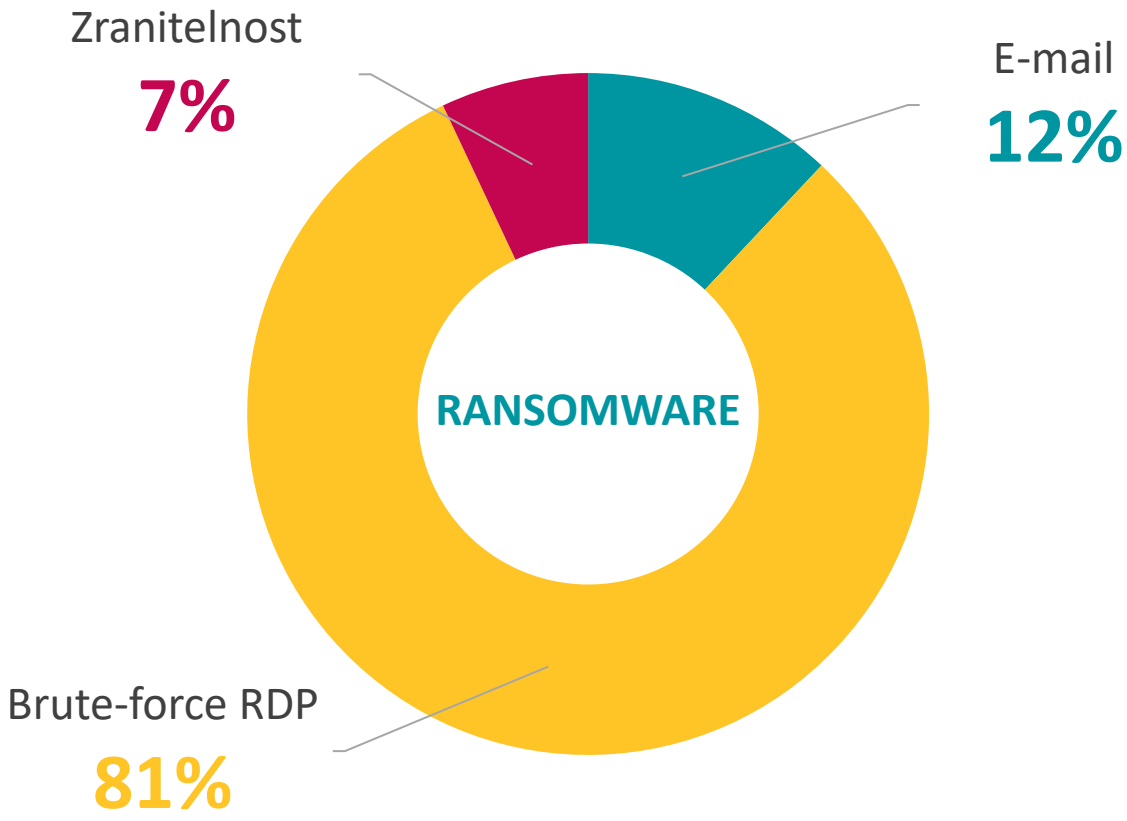


SOFISTIKOVANÉ CÍLENÉ ÚTOKY

1. Hackování, manuální operace
2. Více typů škodlivého kódu
3. Vyřazení AV z provozu
4. Ransomware jako poslední stage

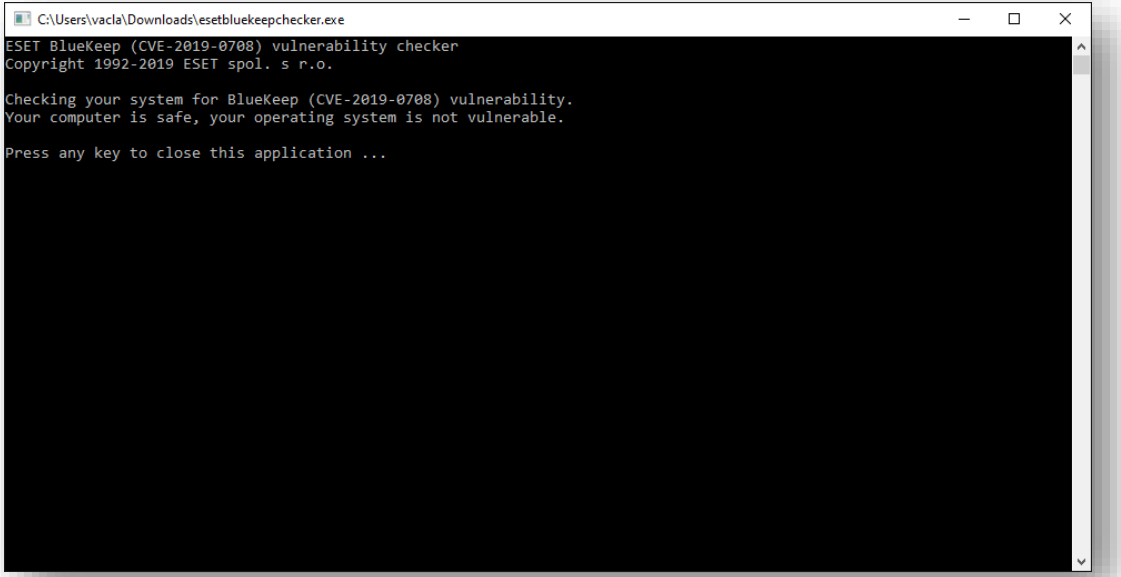
VEKTORY ÚTOKU

Remote Desktop Protokol otevřený do internetu se stal dominantní branou při nákazách šifrovacím kódem.



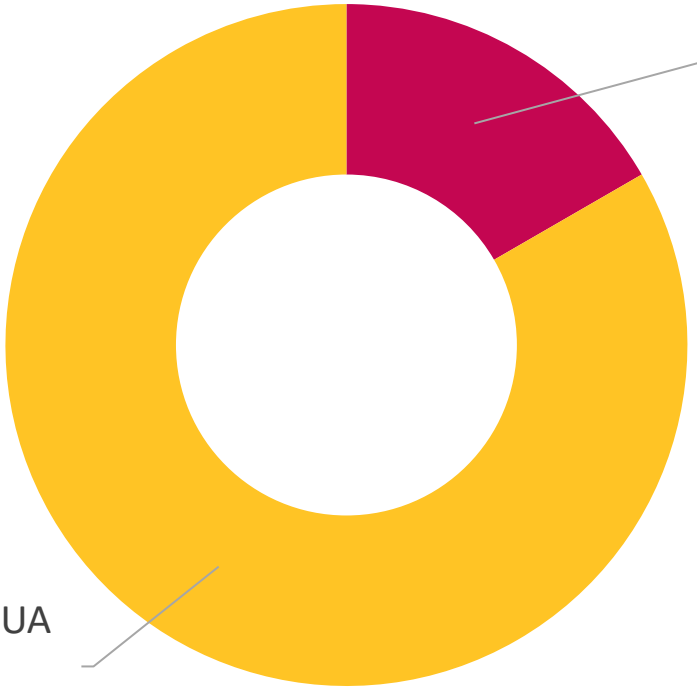
VEKTORY ÚTOKU

Remote Desktop Protokol otevřený do internetu se stal dominantní branou při nákazách šifrovacím kódem.



CELKOVÉ DETEKCE

Veškeré detekce versus součet tří nejvýznamnějších generických detekcí brute-force útoků od začátku roku 2020.



ck of what you have connected to the Internet. Check out Shodan Monitor

Czechia	15,078

TOP CITIES

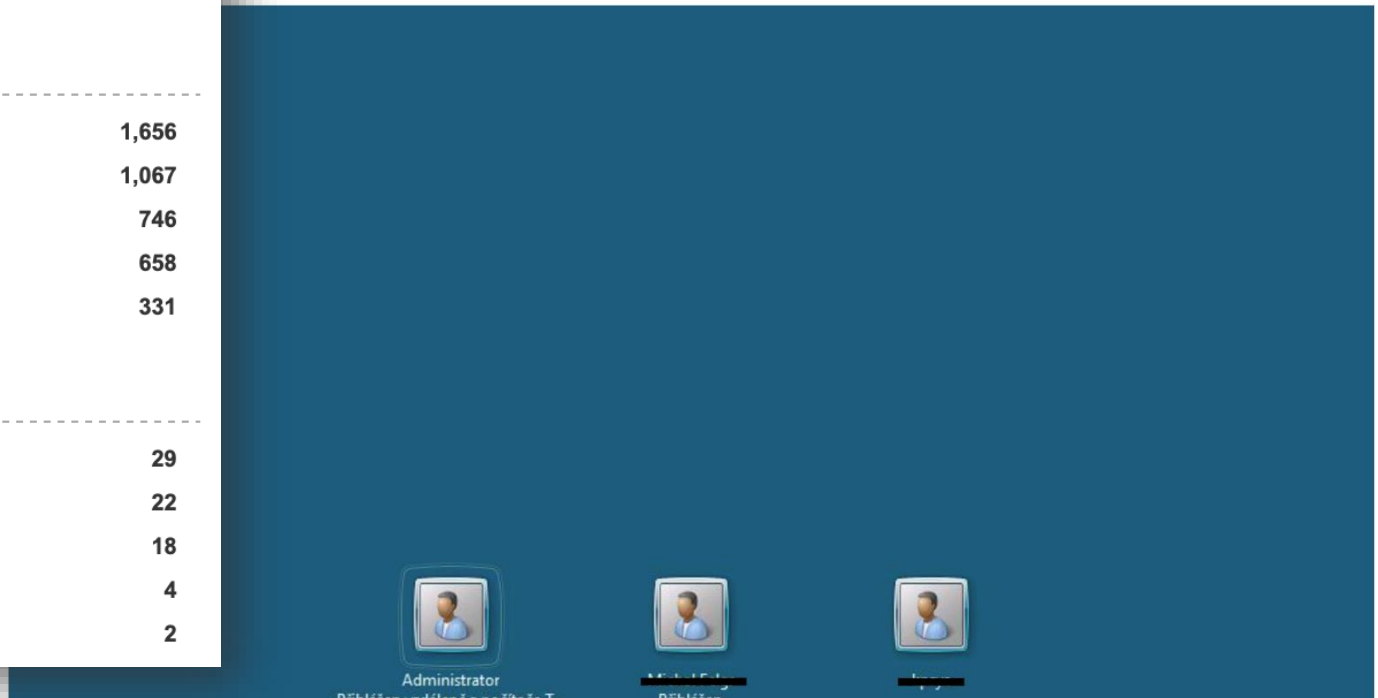
Prague	1,855
Brno	1,455
Ktis	631
Ceske Budejovice	237
Ostrava	146

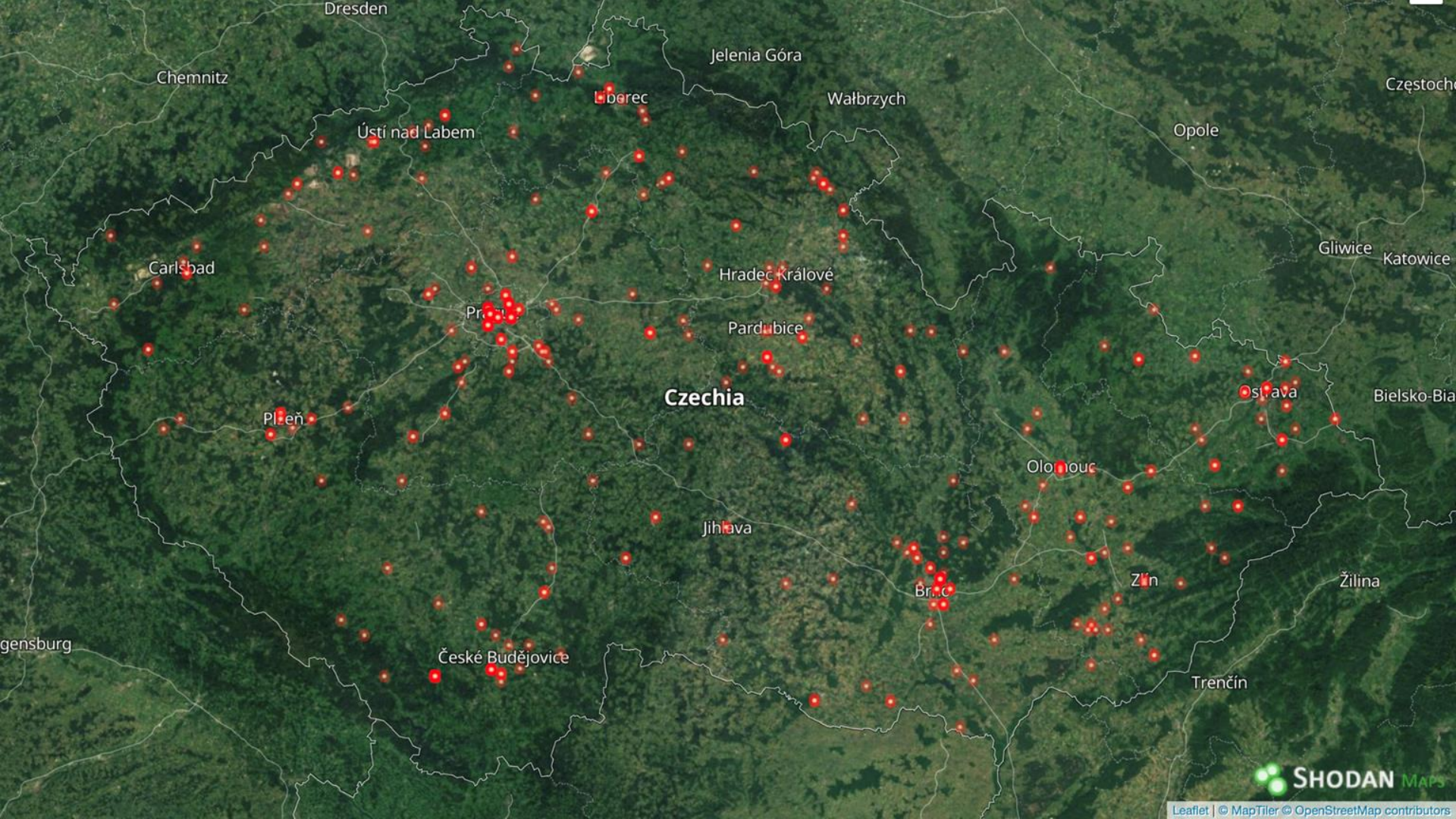
TOP ORGANIZATIONS

SuperNetwork s.r.o.	1,656
O2 Czech Republic	1,067
Brno University of Technology	746
T-Mobile Czech Republic	658
UPC Ceska Republica	331

TOP OPERATING SYSTEMS

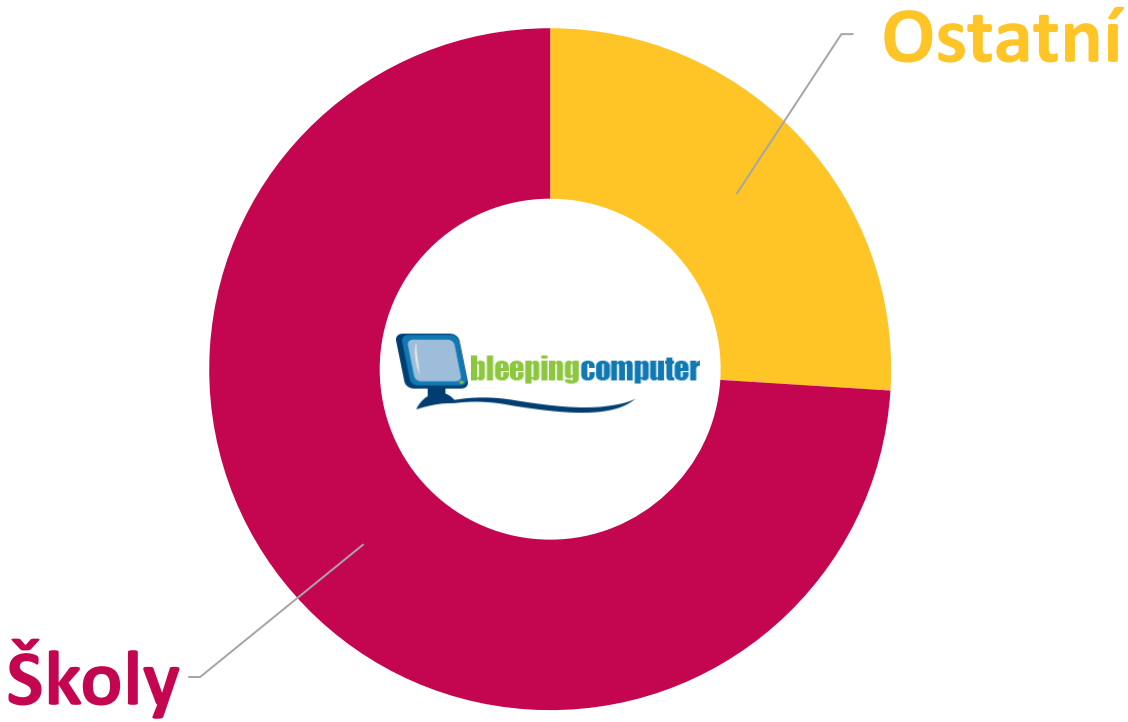
Windows 10 or Server 12	29
Windows 10	22
Windows Server 2008	18
Windows Server 2003	4
Windows XP	2




Dresden
Chemnitz
Jelenia Góra
Liberec
Wałbrzych
Ústí nad Labem
Opole
Częstoch
Gliwice
Katowice
Carlsbad
Hradec Králové
Pardubice
Czechia
Ostrava
Bielsko-Bia
Plzeň
Olomouc
Jihlava
Zlín
Žilina
Brno
gensburg
České Budějovice
Trenčín
SHODAN MAPS
Leaflet | © MapTiler © OpenStreetMap contributors

VZDÁLENÝ PŘÍSTUP

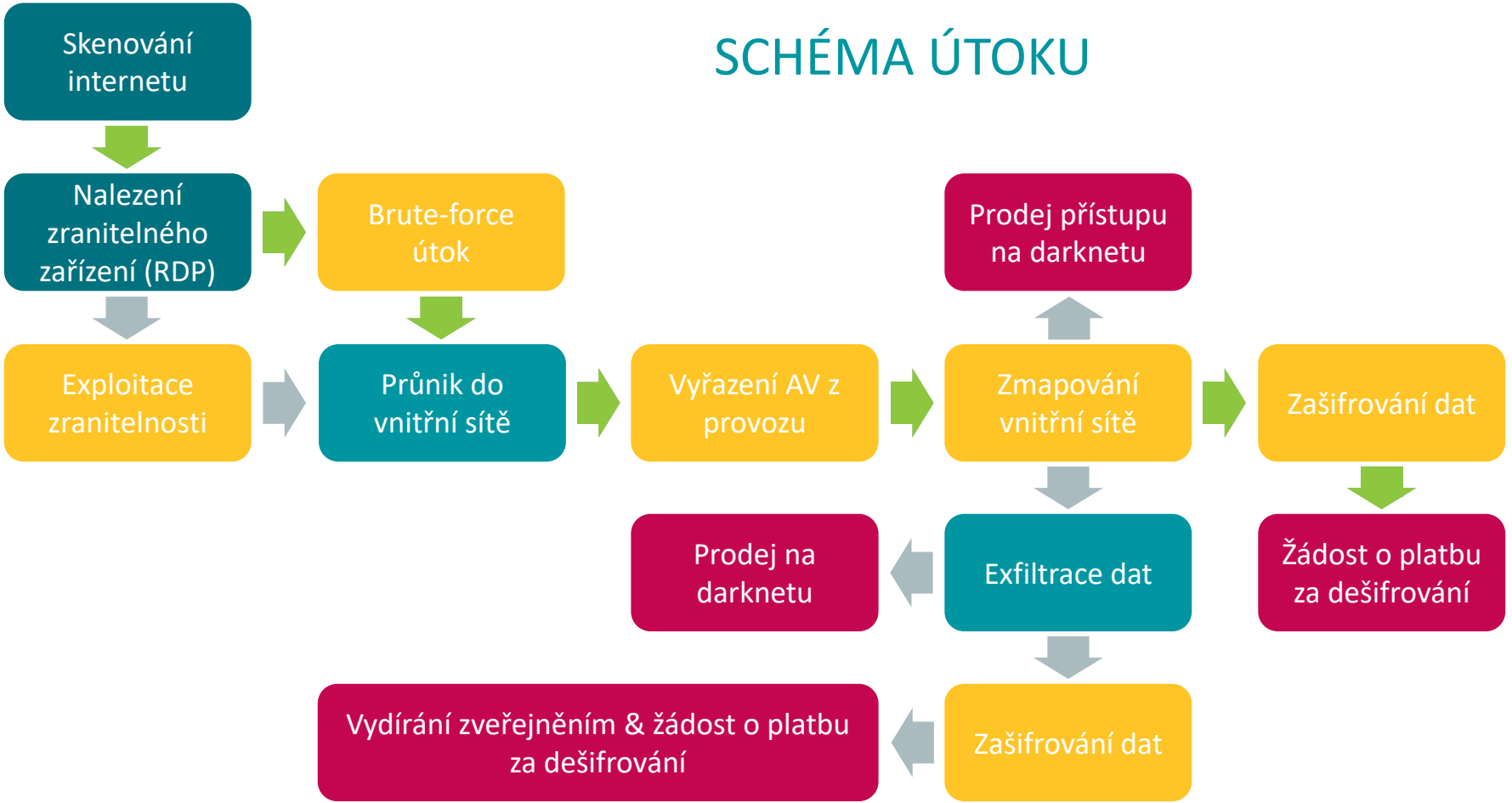
Skoro 75 % všech přístupů přes RDP prodávaných na darknetu míří do škol.



Search

OS / Lang	Ram	CPU / Core / Bits	AV	Browse	Not Used	UP / DL	Root	NAT	Location	Checked	Port	Seller	
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: United States State: California City: Los Angeles Zip: 75007	11-05-2018	3389	Fantasy	+🛒 $4.5
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: Singapore State: Central Singapore Community Development Council City: Singapore Zip: 22042	11-05-2018	3389	iDed	+🛒 $4.5
N/A [N/A]	N/A	N/A CPU Core: N/A Bits OS: N/A	N/A			UP: N/A DL: N/A	no	no	Country: United States State: Florida City: Boca Raton Zip: N/A	11-05-2018	3389	Fantasy	+🛒 $4.5
Windows Server 2012 [English]	4.00 GB	Intel(R) Xeon(R) CPU E5... CPU Core: 2 Bits OS: 64	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 9.84 Mbit/s DL: 14.05 Mbit/s	yes	no	Country: United States State: Arizona City: Scottsdale Zip: 85260	11-05-2018	3389	iDed	+🛒 $6.58
Windows 7 [English]	2.00 GB	Virtual CPU a7769a638... CPU Core: 1 Bits OS: 32	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 74.32 Mbit/s DL: 12.65 Mbit/s	no	no	Country: Hong Kong State: N/A City: N/A Zip: N/A	11-05-2018	3389	iDed	+🛒 $4.5
Windows Server 2012 [English]	1.75 GB	AMD Opteron(tm) Proce... CPU Core: 1 Bits OS: 64	N/A		paypal.com amazon.com wellsfargo.com ebay.com suntrust.com	UP: 10.86 Mbit/s DL: 13.29 Mbit/s	no	yes	Country: United States State: Texas City: San Antonio Zip: 94948	11-05-2018	3389	iDed	+🛒 $4.5

SCHÉMA ÚTOKU



Zašifrování

Prodej na černém trhu

Vydírání zveřejněním

New Clients

United Decorating
Nielsen Bainbridge Group LLC Headquarters
Atlas Machinery
CU Collections
Academy Mortage Corp.
TechnoOrbits
Talon Logistics
Johnson Air Products
Affordacare Urgent Care Clinic
Woods And Woods

Represented here companies do not wish to cooperate with us, and trying to hide our successful attack on their resources. Wait for their databases and private papers here. Follow the news! P.S. We have the second domain: newsmaze.top.

United Decorating Added

http://unitеddecorating.com/Danijel

Article about United Decorating have been locked

Cryptoransomware

admin , 82

Read More

Nielsen Bainbridge Group LLC Headquarters Added

www.nielsenbainbridgegroup.com

Article about Nielsen Bainbridge Group LLC Headquarters have been locked

Cryptoransomware

admin , 67

Read More

Atlas Machinery Added

https://www.atlas-machinery.com/

Article about Atlas Machinery have been locked

Cryptoransomware

admin , 122

Read More

CU Collections Added

http://www.cucollections.com/

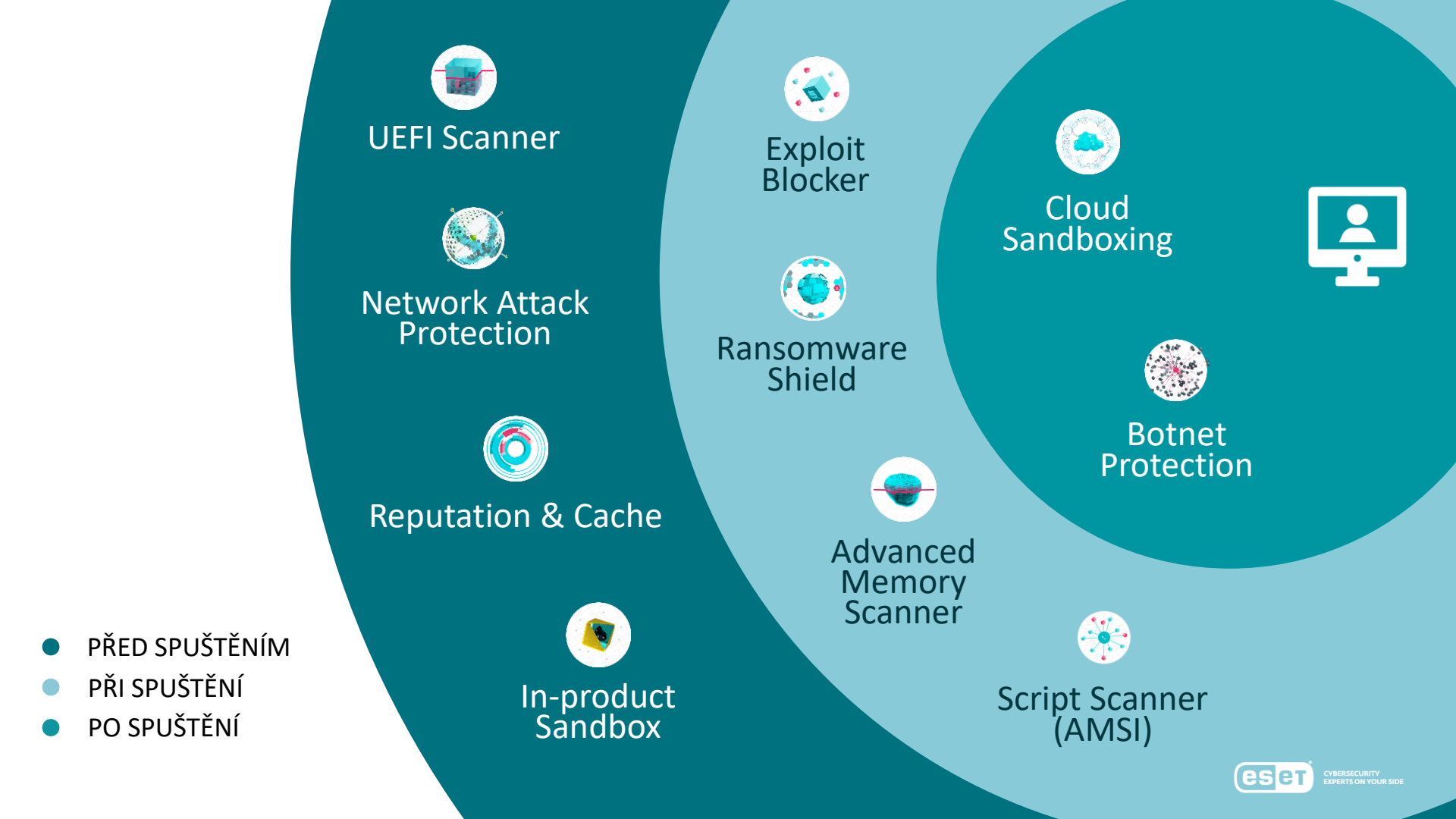
Article about CU Collections have been locked

Cryptoransomware

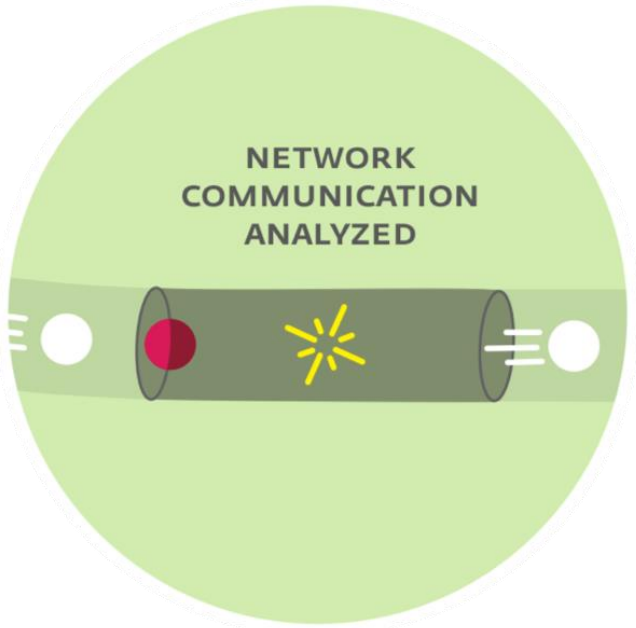
Full dump

Cutrale (oranges)
Busch's Inc.
L&F DISTRIBUTORS (LNF)
City Of Pensacola
Groupe Igrec, igrec.fr
Baker Wotring LLP
Saxbst & Bstco (all passwords)
SALUMIFICIO FRATELLI
BERETTA S.P.A. O
Southwire (US, GA)

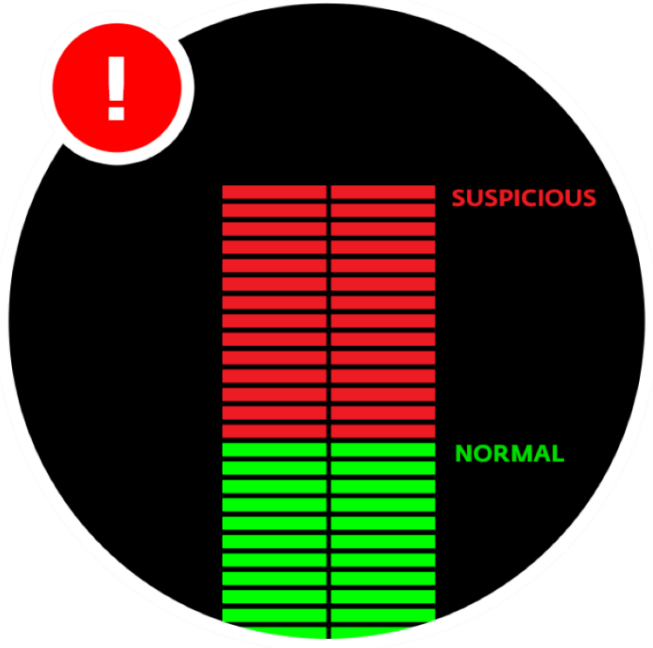
DETEKCE


UEFI Scanner
Network Attack Protection
Reputation & Cache
In-product Sandbox
Exploit Blocker
Ransomware Shield
Advanced Memory Scanner
Cloud Sandboxing
Botnet Protection
Script Scanner (AMSI)
PŘED SPUŠTĚNÍM
PŘI SPUŠTĚNÍ
PO SPUŠTĚNÍ
eset
CYBERSECURITY EXPERTS ON YOUR SIDE

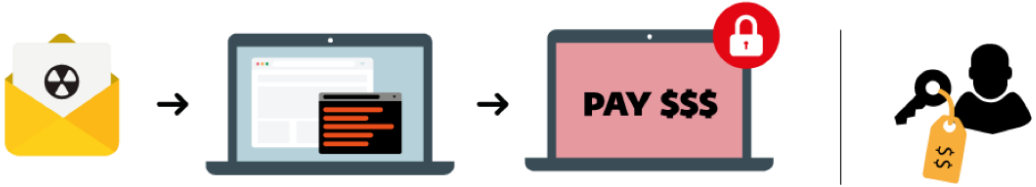
NETWORK ATTACK PROTECTION

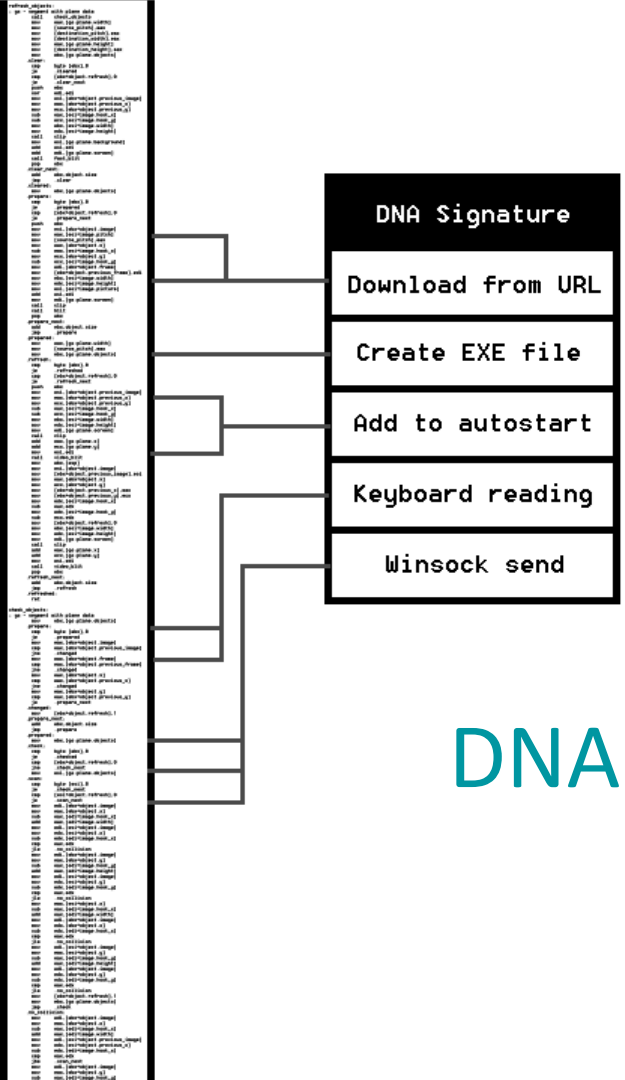


ADVANCED MEMORY SCANNER



RANSOMWARE SHIELD





DNA Signature

Download from URL

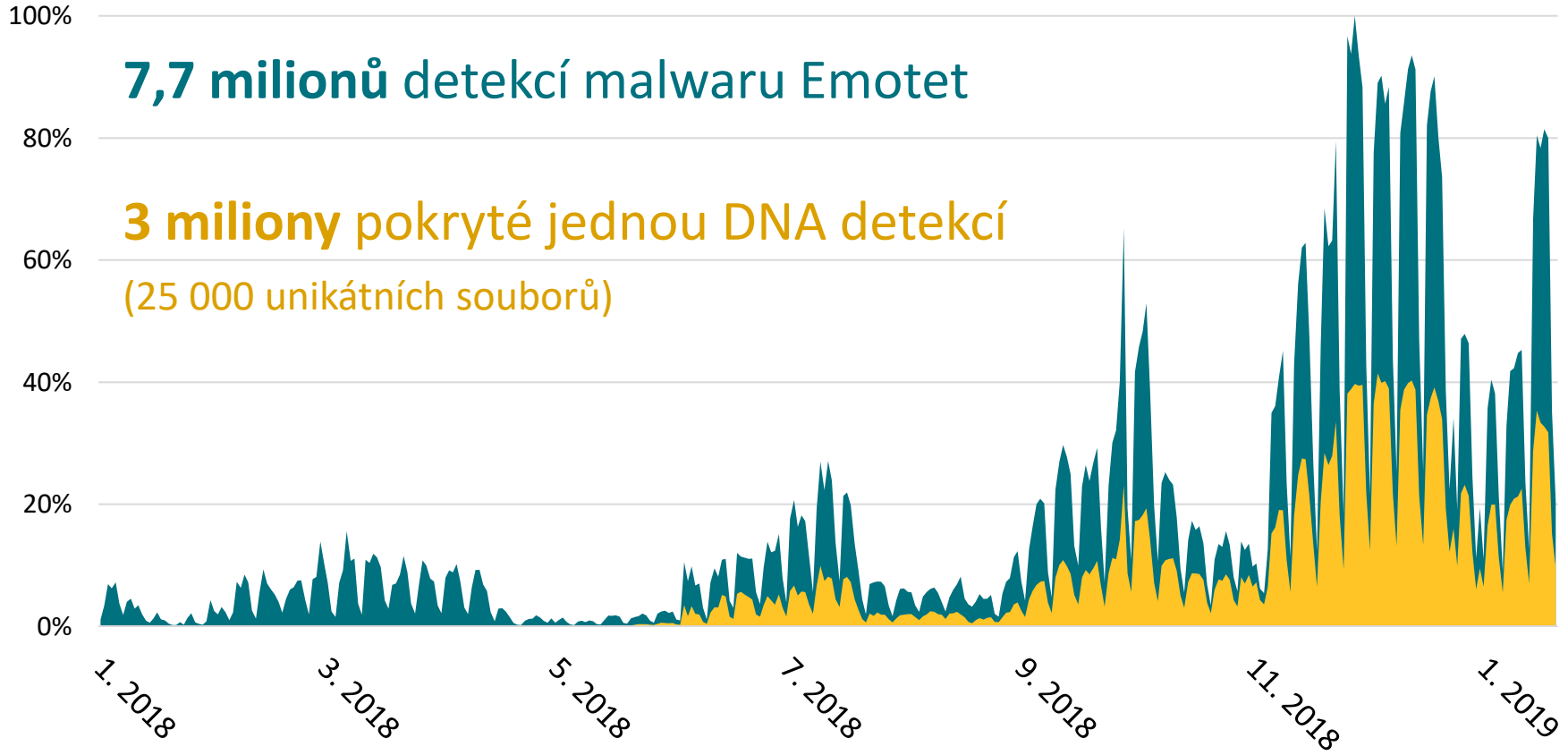
Create EXE file

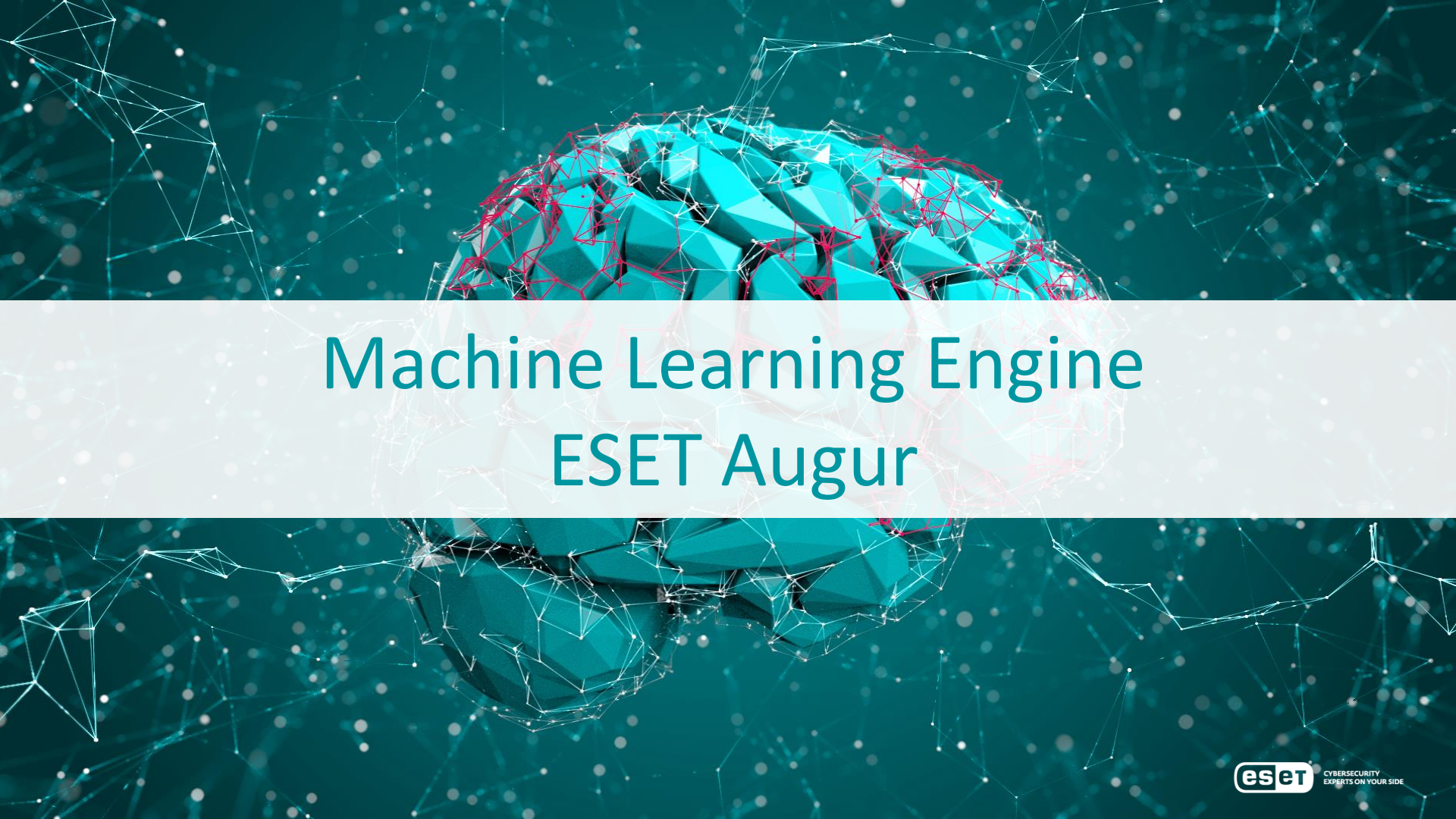
Add to autostart

Keyboard reading

Winsock send

DNA DETECTIONS





Machine Learning Engine
ESET Augur

CYBERSECURITY
EXPERTS ON YOUR SIDE

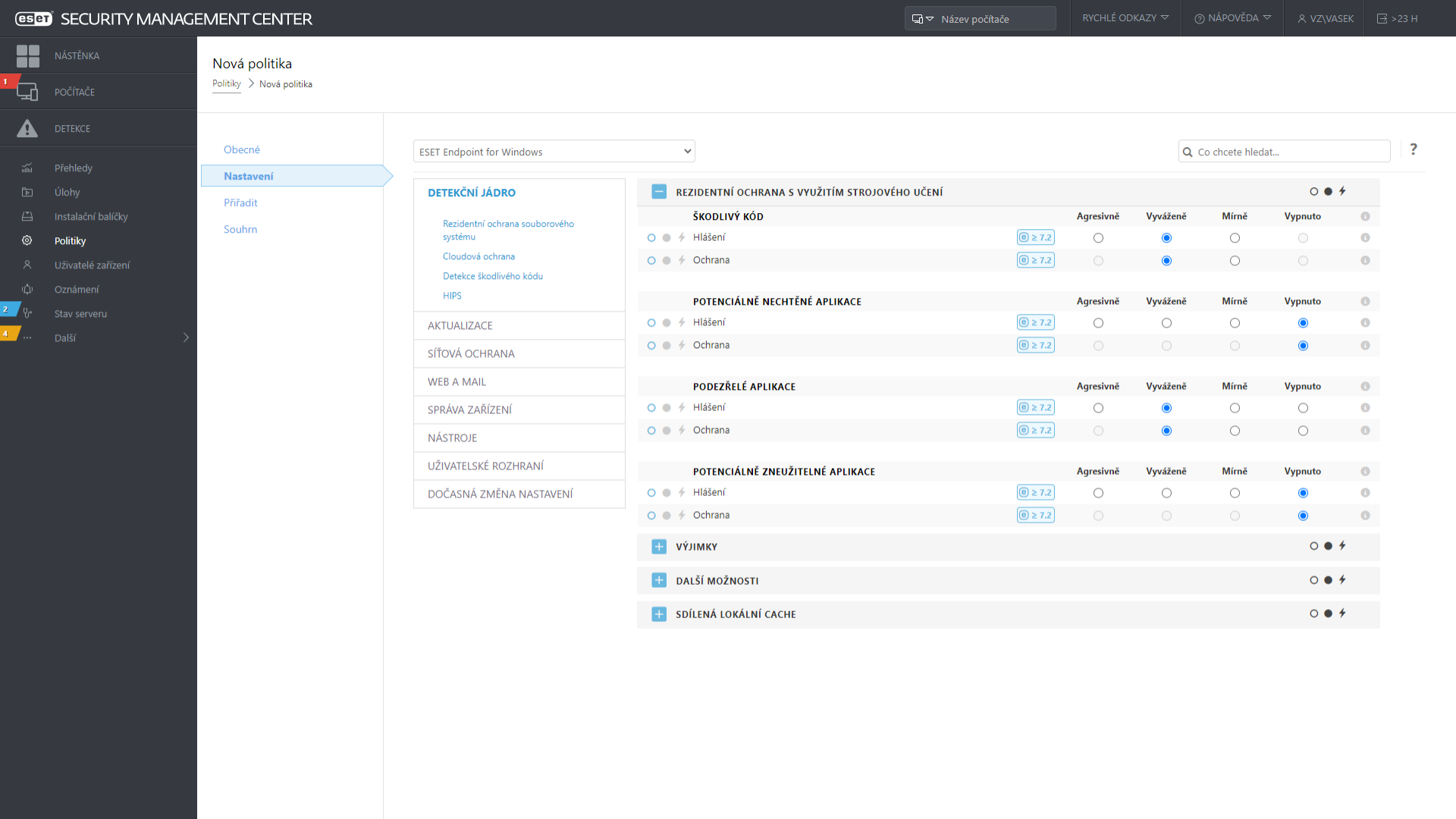
RANSOMWARE VS. ESET AUGUR (březen 2017)

Malware (květen 2017 - červen 2018)	Počet vzorků	Augurem detekováno	Poměr detekce
NotPetya	86	85	**98,8 %**
BadRabbit	20	20	**100 %**
Crysis	30	30	**100 %**
WannaCryptor	67	67	**100 %**

ÚČINNÁ OCHRANA

Občas se o nás tvůrci malwaru z frustrace zmíní i ve svém kódu. Jako zde v případě trojanu Emotet ☺

```
mov     [ebp+var_30], eax
mov     eax, [ebp+var_2C]
mov     [esp+4], eax
mov     dword ptr [esp], 0
mov     eax, [ebp+var_24]
call    eax
sub     esp, 8
mov     [ebp+var_34], eax
mov     eax, [ebp+var_30]
mov     [esp], eax
mov     eax, [ebp+var_28]
call    eax
sub     esp, 4
mov     [ebp+var_38], eax
lea     eax, [ebp+var_54]
mov     [esp+8], eax
mov     eax, [ebp+var_34]
mov     [esp+4], eax
mov     eax, [ebp+var_38]
mov     [esp], eax
call    __Z18_Crypt_DecryptDataPhmS_ ; _Crypt_DecryptData(uchar *,ulong,uchar *)
mov     [ebp+var_3C], eax
mov     eax, [ebp+var_3C]
mov     [ebp+var_40], eax
mov     eax, [ebp+var_40]
call    eax
mov     [ebp+var_44], eax
mov     dword ptr [esp+4], 0 ; pNumArgs
mov     dword ptr [esp], offset CmdLine ; lpCmdLine
call    _CommandLineToArgvW@8 ; CommandLineToArgvW(x,x)
sub     esp, 8
mov     dword ptr [esp+0Ch], 0 ; uType
mov     dword ptr [esp+8], 0 ; lpCaption
mov     dword ptr [esp+4], offset Text ; "ESET Stupid!!!"
mov     dword ptr [esp], 0 ; hWnd
call    _MessageBoxA@16 ; MessageBoxA(x,x,x,x)
sub     esp, 10h
mov     eax, 0
lea     esp, [ebp-0Ch]
pop     ebx
pop     esi
pop     edi
pop     ebp
retn
_VzcsSxdKopTdfCVS endp
```


ESET SECURITY MANAGEMENT CENTER
Název počítače
RYCHLÉ ODKAZY
NÁPOVĚDA
VZ\VASEK
>23 H
NÁSTĚNKA
POČÍTAČE
DETEKCE
Přehledy
Úlohy
Instalační balíčky
Politiky
Uživatelé zařízení
Oznámení
Stav serveru
Další
Nová politika
Politiky
Nová politika
Obecné
Nastavení
Přiřadit
Souhrn
ESET Endpoint for Windows
Co chcete hledat...
DETEKČNÍ JÁDRO
Rezidentní ochrana souborového systému
Cloudová ochrana
Detekce škodlivého kódu
HIPS
AKTUALIZACE
SÍŤOVÁ OCHRANA
WEB A MAIL
SPRÁVA ZAŘÍZENÍ
NÁSTROJE
UŽIVATELSKÉ ROZHRANÍ
DOČASNÁ ZMĚNA NASTAVENÍ
REZIDENTNÍ OCHRANA S VYUŽITÍM STROJOVÉHO UČENÍ
ŠKODLIVÝ KÓD
Agresivně
Vyváženě
Mírně
Vypnuto
Hlášení
≥ 7.2
Ochrana
POTENCIÁLNĚ NECHTĚNÉ APLIKACE
PODEZŘELÉ APLIKACE
POTENCIÁLNĚ ZNEUŽITELNÉ APLIKACE
VÝJIMKY
DALŠÍ MOŽNOSTI
SDÍLENÁ LOKÁLNÍ CACHE

JAK VYZRÁT NAD ÚTOČNÍKY

NADSTAVBOVÉ PRODUKTY

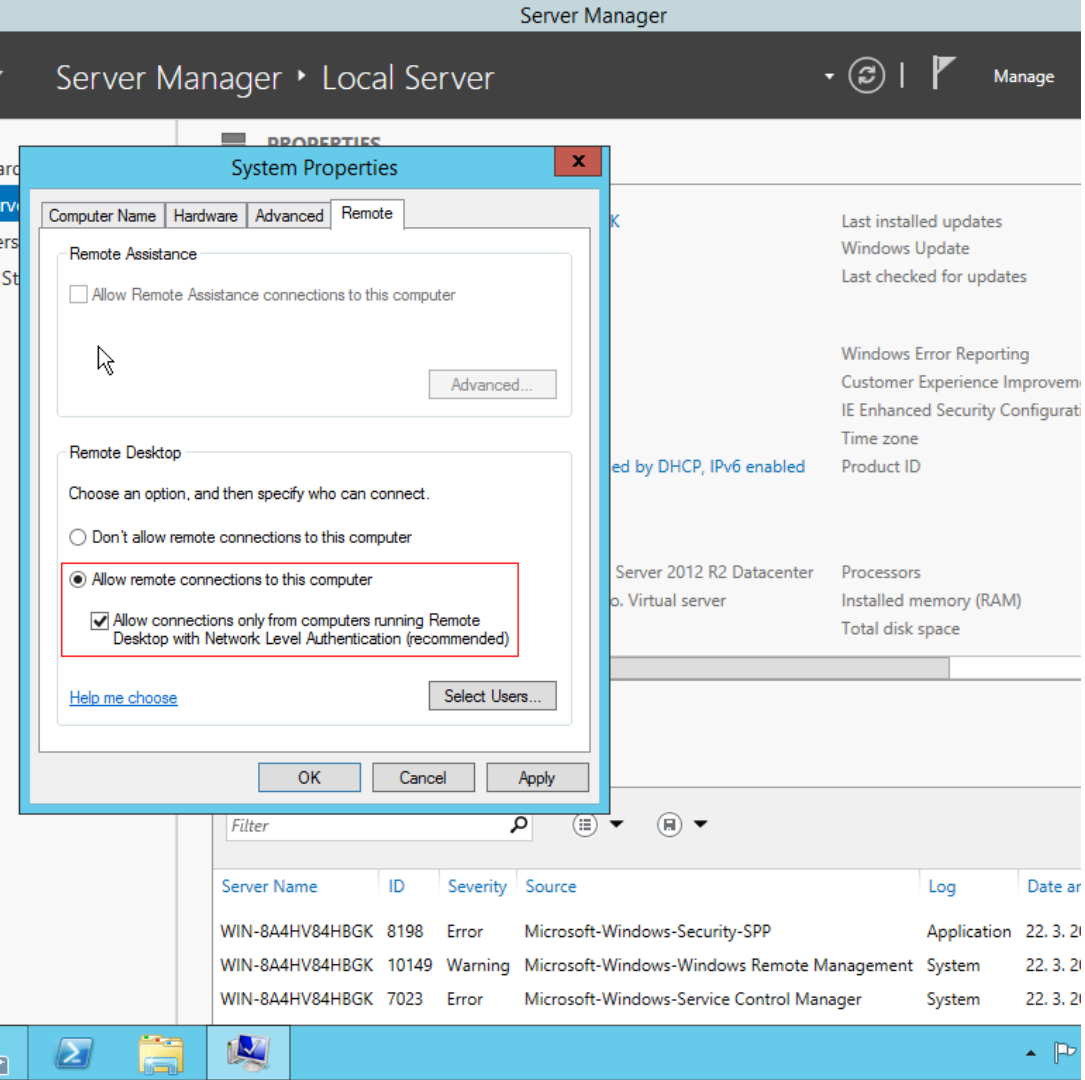
Cloudový sandbox

Endpoint Detection and Response

Dvoufaktorové ověřování

JAK VYZRÁT NAD HACKERY

- Omezit služby vystavené do internetu (VPN)
- Pravidelně patchovat celou infrastrukturu
- Segmentovat síť, používat servisní účty
- Zavést 2FA, sledovat perimetr sítě
- Provádět bezpečnostní monitoring
- Zálohovat, školit zaměstnance



RDP

Ransomware Deployment Protocol

Whitelistace konkrétních IP

Restrikce na uživatelské účty

Nastavení komplexních hesel

Nastavení zamykání účtů

Zakázání nebo přejmenování účtu Administrator

ESET CYBERSECURITY EXPERTS ON YOUR SIDE

welivesecurity BY eset

Two US cities opt to pay $1m to ransomware operators

A few days apart, two cities in Florida cave in to extortionists' demands in hopes of restoring access to municipal computer systems

To pay o
attackers
do pay u
away?

welivesecurity BY eset

Hospitals in US, Australia hobbled by ransomware

The incidents send medical staff back to the days of pen and pape

cks
ll
en

d
re

welivesecurity BY eset

South African power company battles ransomware attack

The power utility appears to be well on track to a swift recovery following an attack that ultimate left some people without electricity

City
that
Afric
is gra
attac
with
Reut

welivesecurity BY eset

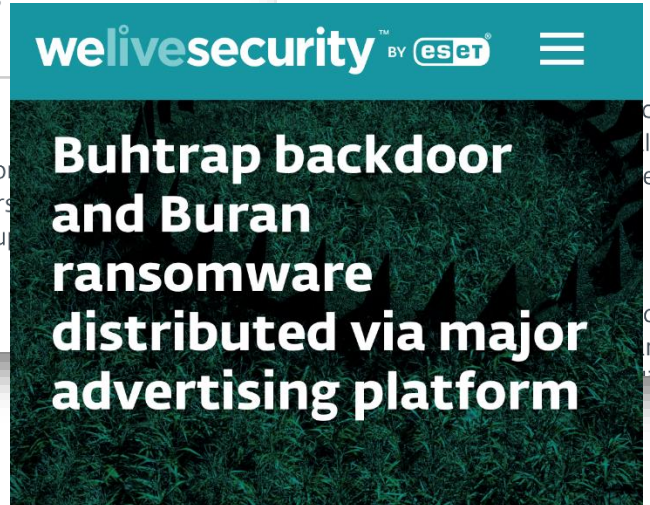
Ransomware wave hits 23 towns in Texas

The attack, which has victimized mostly smaller local governments, is thought to have been unleashed by a single threat actor

t
s are

attack",
rtment
DIR)

welivesecurity BY eset



Buhtrap backdoor and Buran ransomware distributed via major advertising platform

welivesecurity BY eset

Cybersecurity Trends 2020: Technology is getting smarter – are we?

CYBERSECURITY
EXPERTS ON YOUR SIDE

Václav Zubr | Pre-Sales Engineer | vaclav.zubr@eset.cz