



**CYBERSECURITY
EXPERTS ON YOUR SIDE**

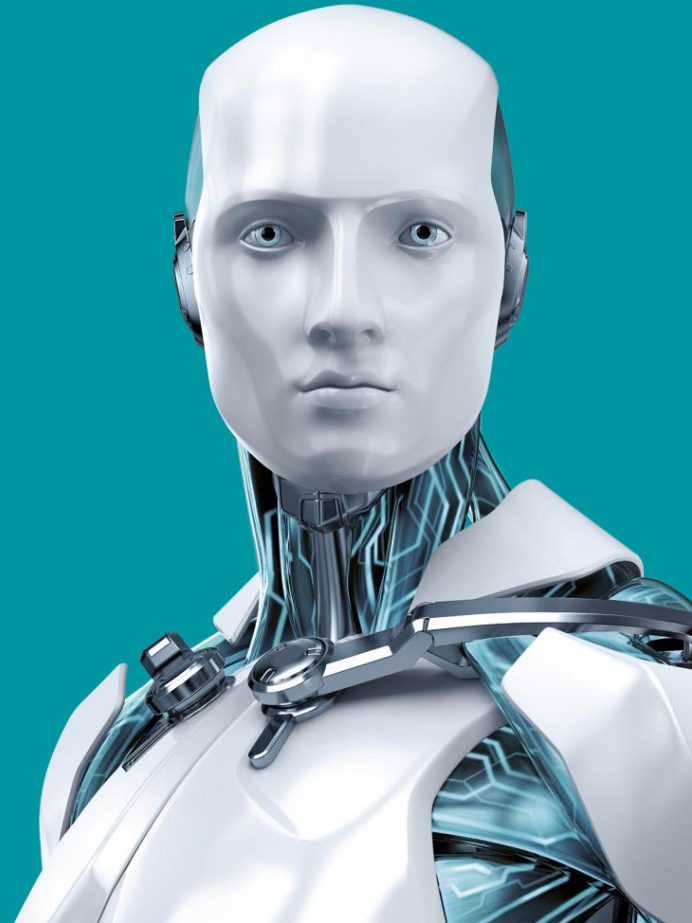
KYBERNETICKÉ ÚTOKY V ČESKU

Evoluce ransomwaru

Václav Zubr
Pre-Sales Engineer



CYBERSECURITY
EXPERTS ON YOUR SIDE

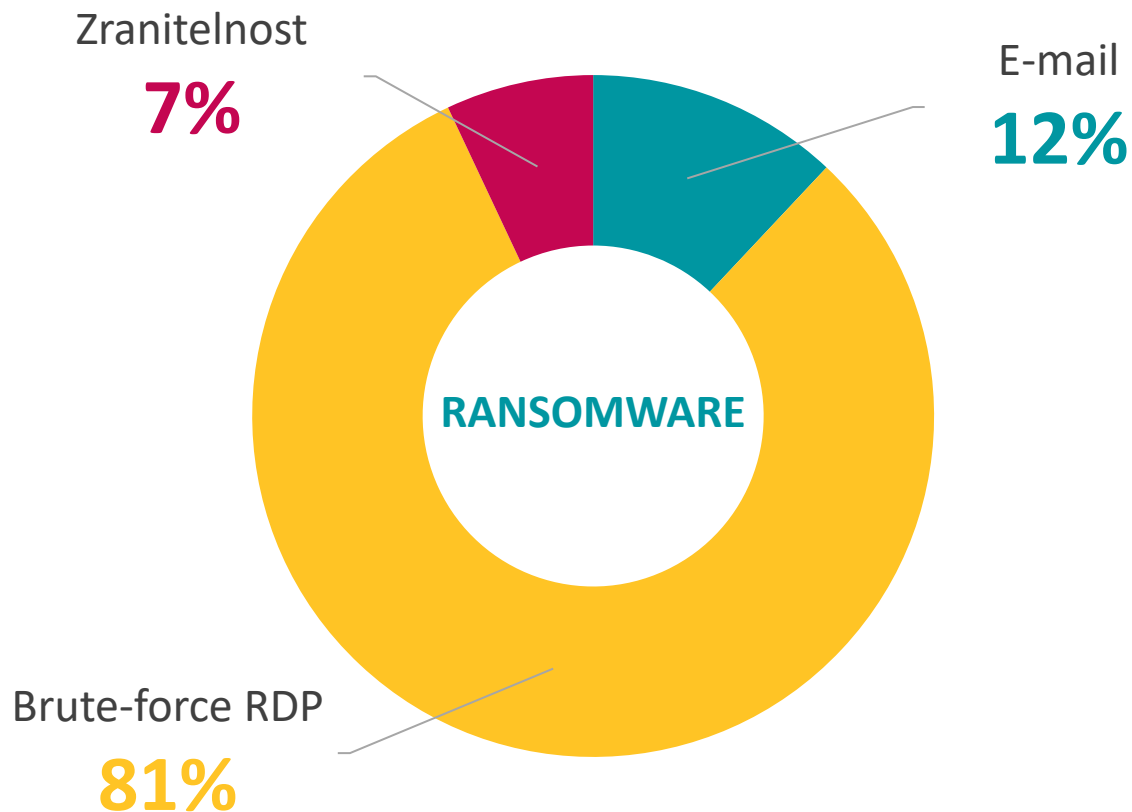


SOFISTIKOVANÉ CÍLENÉ ÚTOKY

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

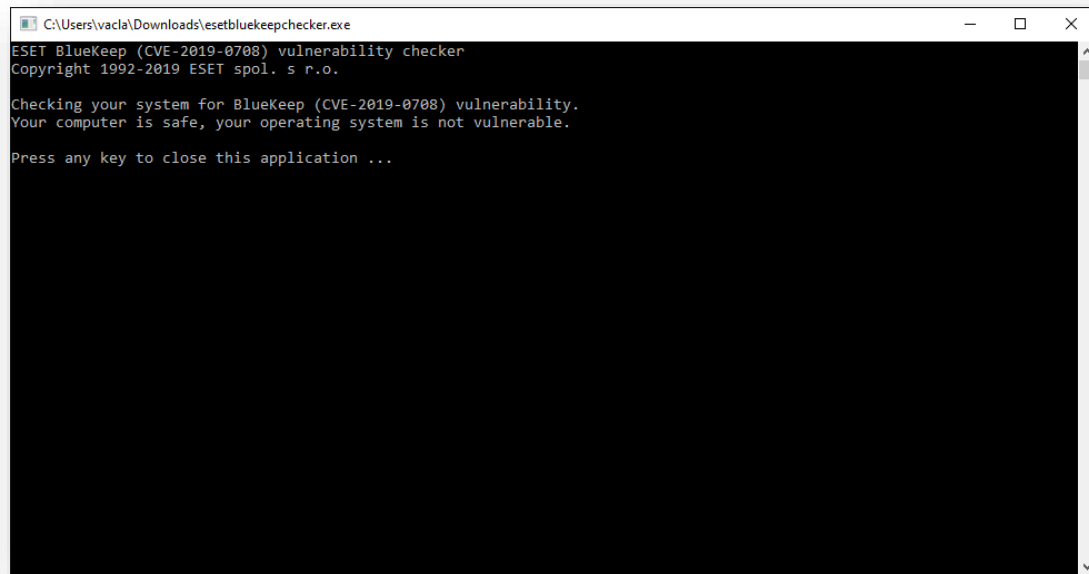
VEKTORY ÚTOKU

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.



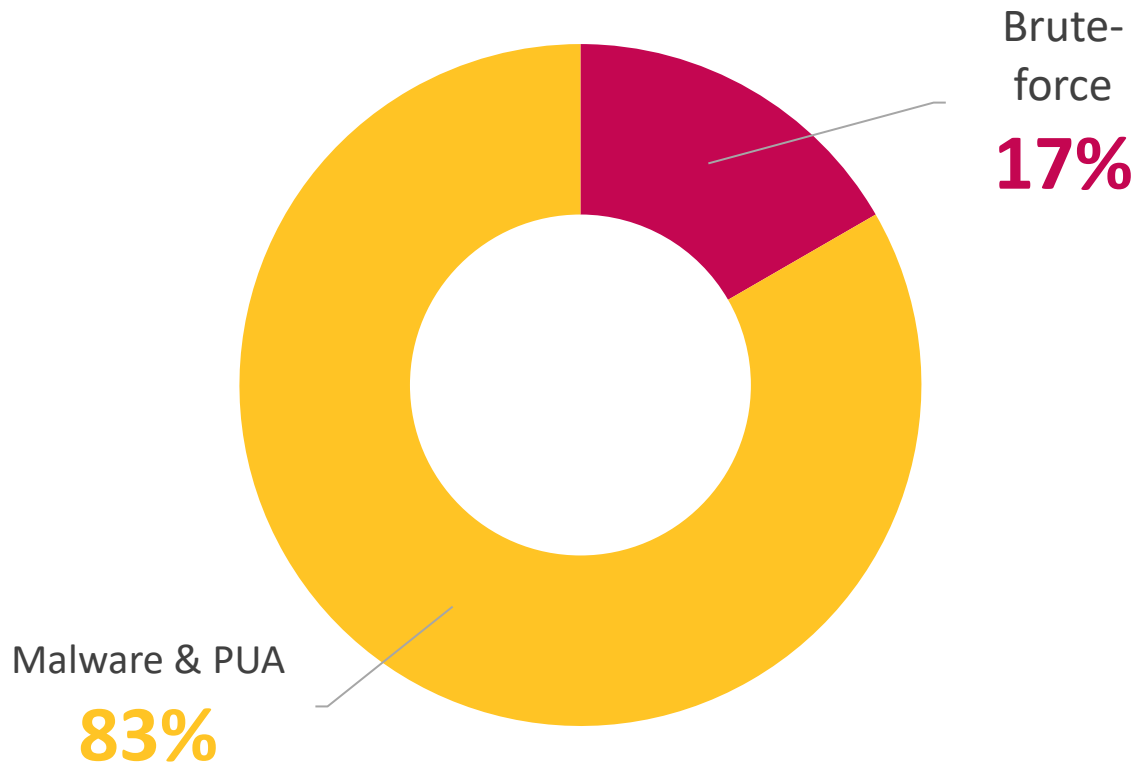
```
C:\Users\vacla\Downloads\esetbluekeepchecker.exe
ESET BlueKeep (CVE-2019-0708) vulnerability checker
Copyright 1992-2019 ESET spol. s r.o.

Checking your system for BlueKeep (CVE-2019-0708) vulnerability.
Your computer is safe, your operating system is not vulnerable.

Press any key to close this application ...
```

CELKOVÉ DETEKCE

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



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



Explore

Downloads

Reports

Pricing

Enterprise Access

My Account

Results

Create Report

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

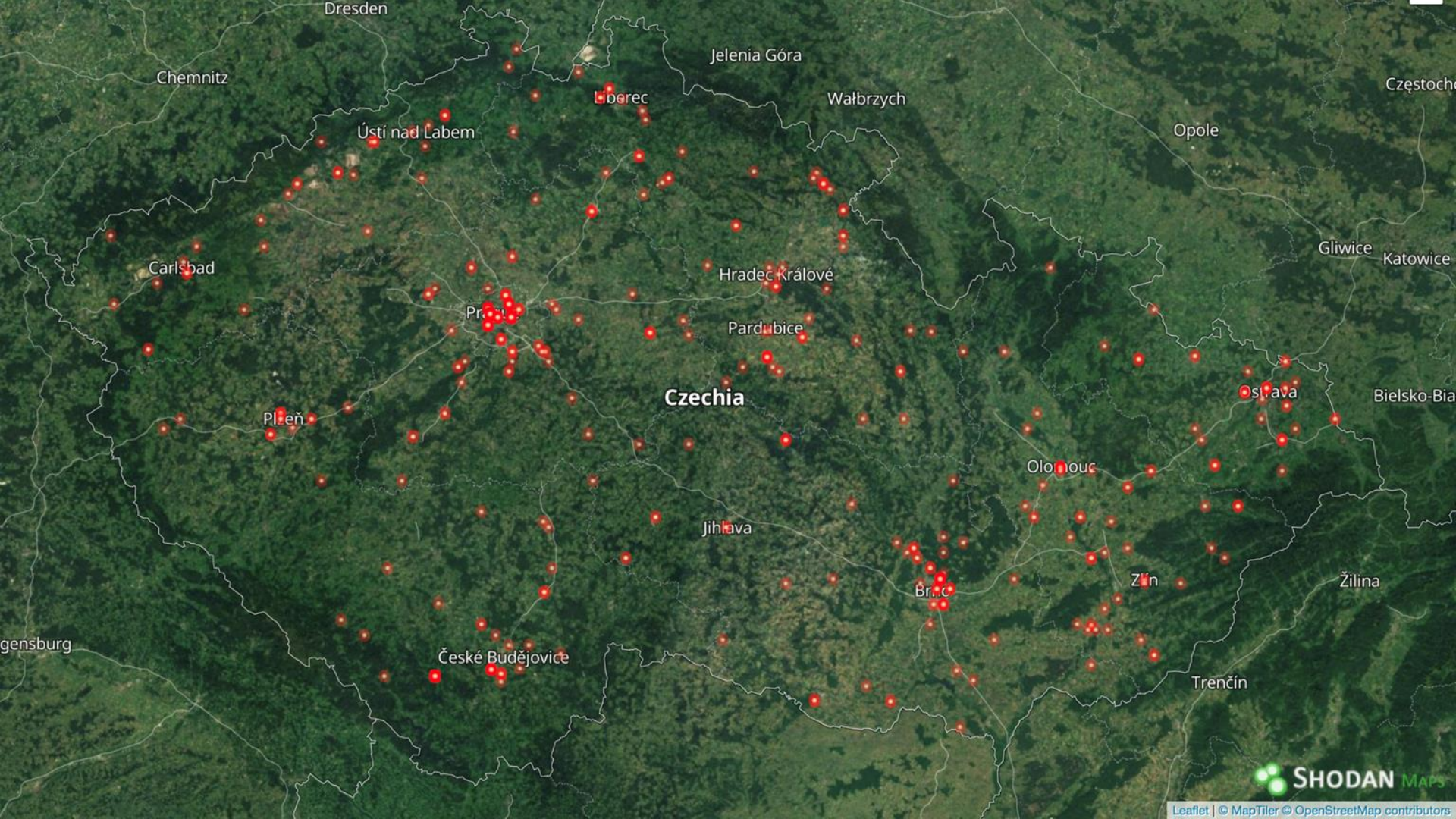
Administrator



Administrator



Administrator



Chemnitz

Dresden

Jelenia Góra

Wałbrzych

Częstocho

Ústí nad Labem

Liberec

Opole

Gliwice

Katowice

Carlsbad

Hradec Králové

Prácheň

Pardubice

Bielsko-Bia

Píseň

Czechia

Ostava

Olomouc

Jihlava

Žilina

gensburg

České Budějovice

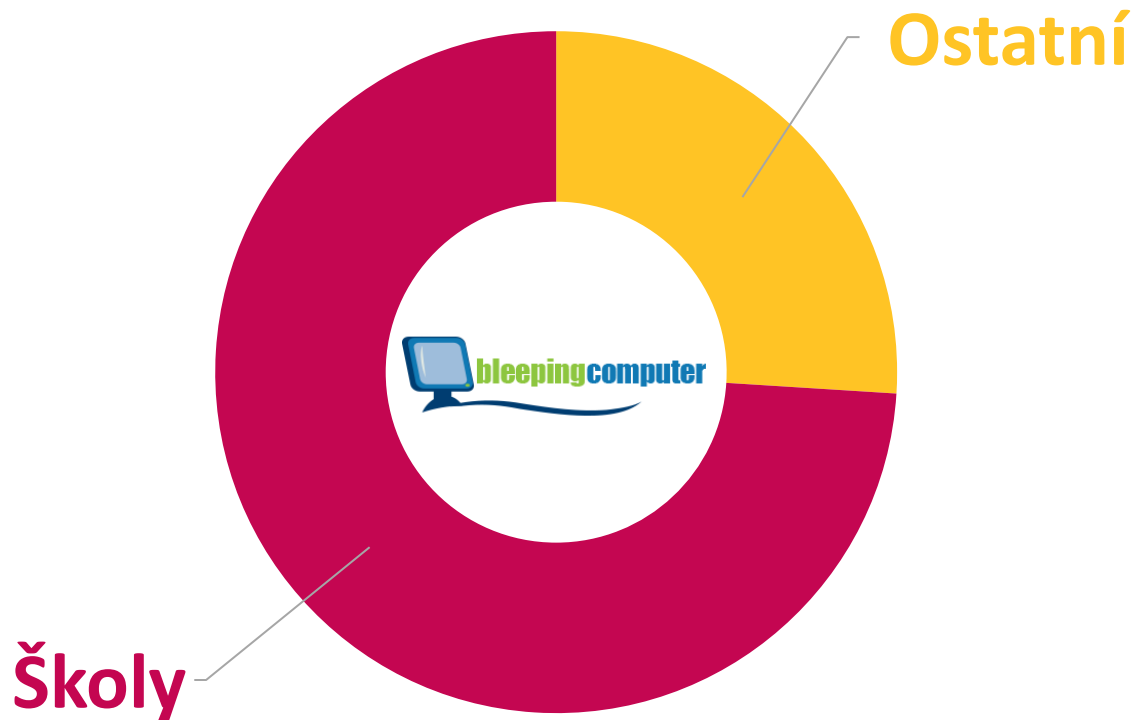
Brno

Zlín

Trenčín

VZDÁLENÝ PŘÍSTUP

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





Home



PayPal



Banks



Shoppo



CC



Services



0

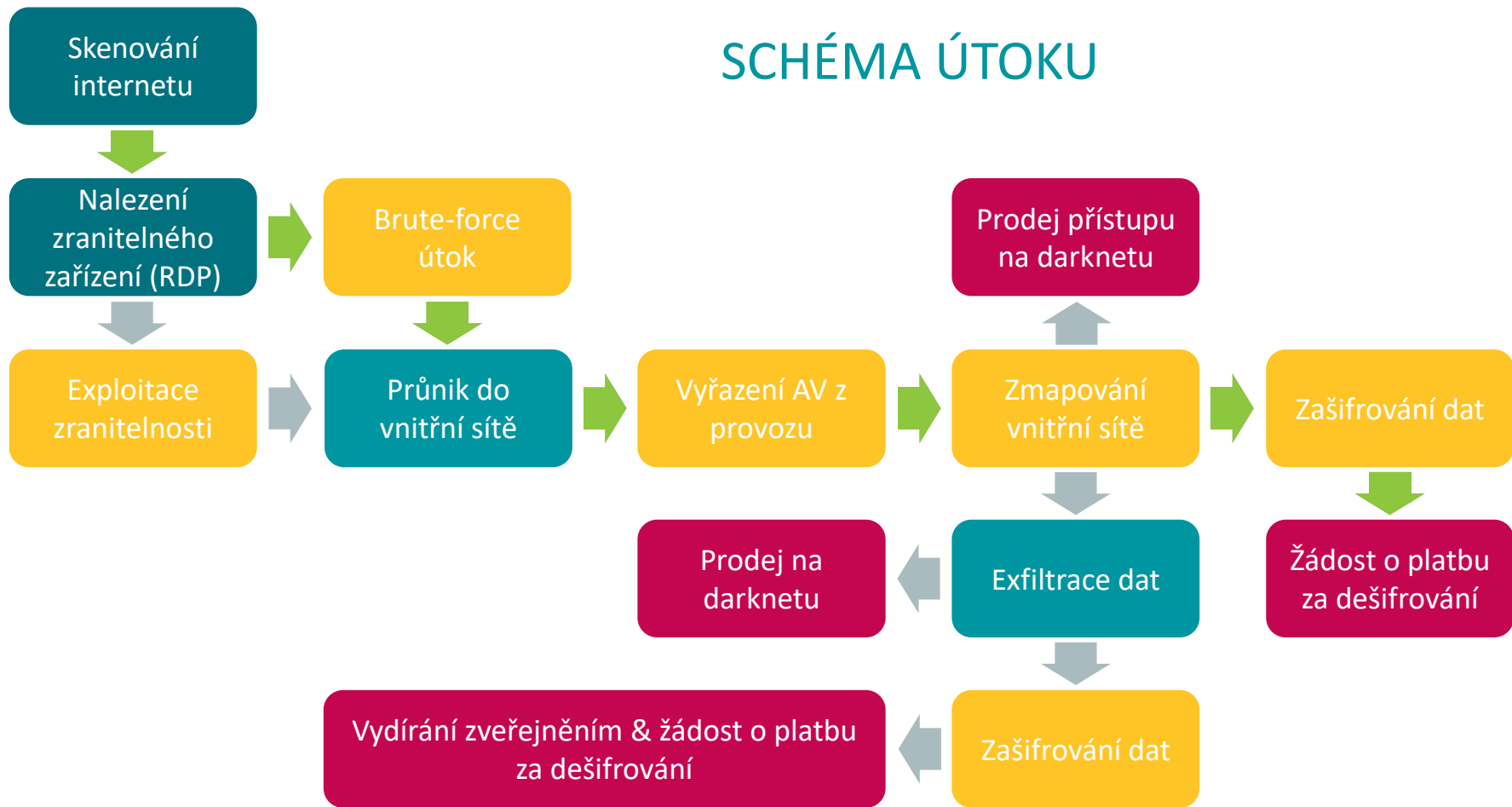


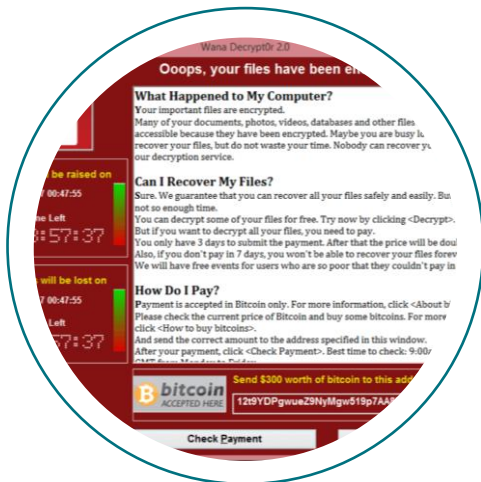
Home / Dedicate (10815)

Q 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 Mortgage 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.


Full dump



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

[United Decorating](#) **Added**

<http://uniteddecorating.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

DETEKCE



UEFI Scanner



Network Attack Protection



Reputation & Cache



In-product Sandbox



Exploit Blocker



Ransomware Shield



Advanced Memory Scanner



Cloud Sandboxing



Botnet Protection

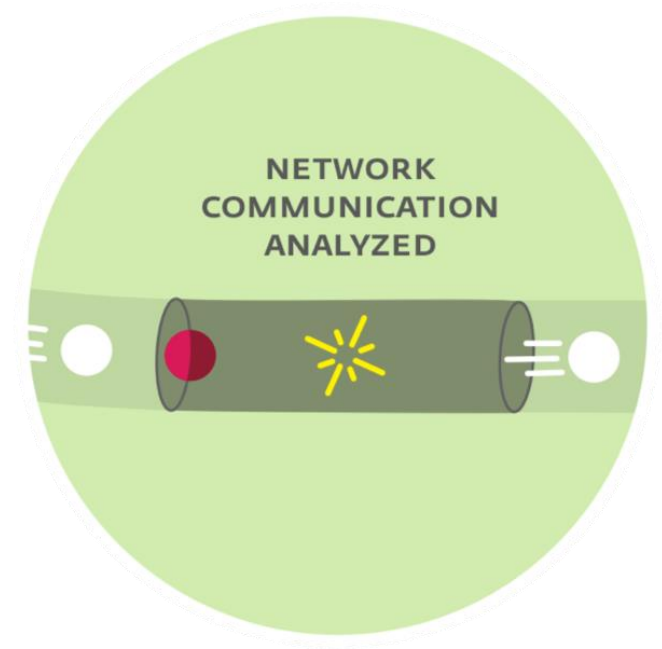


Script Scanner (AMSI)



- PŘED SPUŠTĚNÍM
- PŘI SPUŠTĚNÍ
- PO SPUŠTĚNÍ

NETWORK ATTACK PROTECTION



Wana Decrypt0r 2.0

 **Oops, your files have been encrypted!** English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT+08:00 (UTC+8:00).

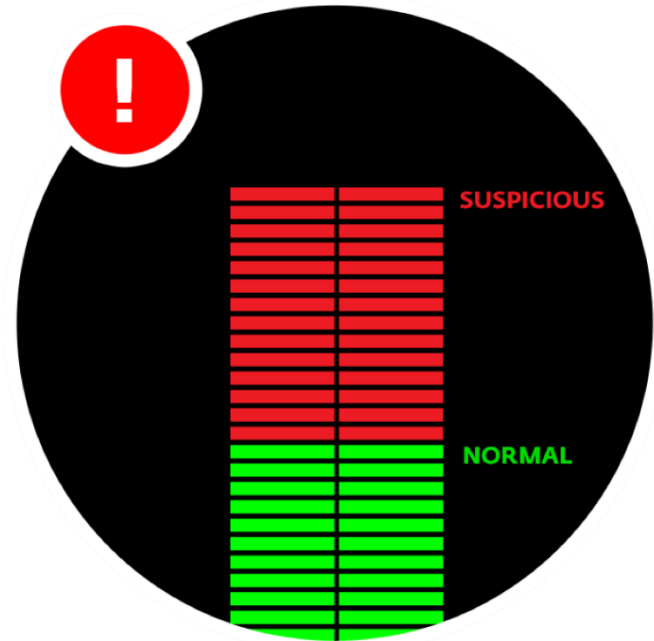
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **Send \$300 worth of bitcoin to this address:**
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

ADVANCED MEMORY SCANNER



RANSOMWARE SHIELD





DNA DETECTIONS



100%

7,7 milionů detekcí malwaru Emotet

80%

3 miliony pokryté jednou DNA detekcí

(25 000 unikátních souborů)

60%

40%

20%

0%

1. 2018

3. 2018

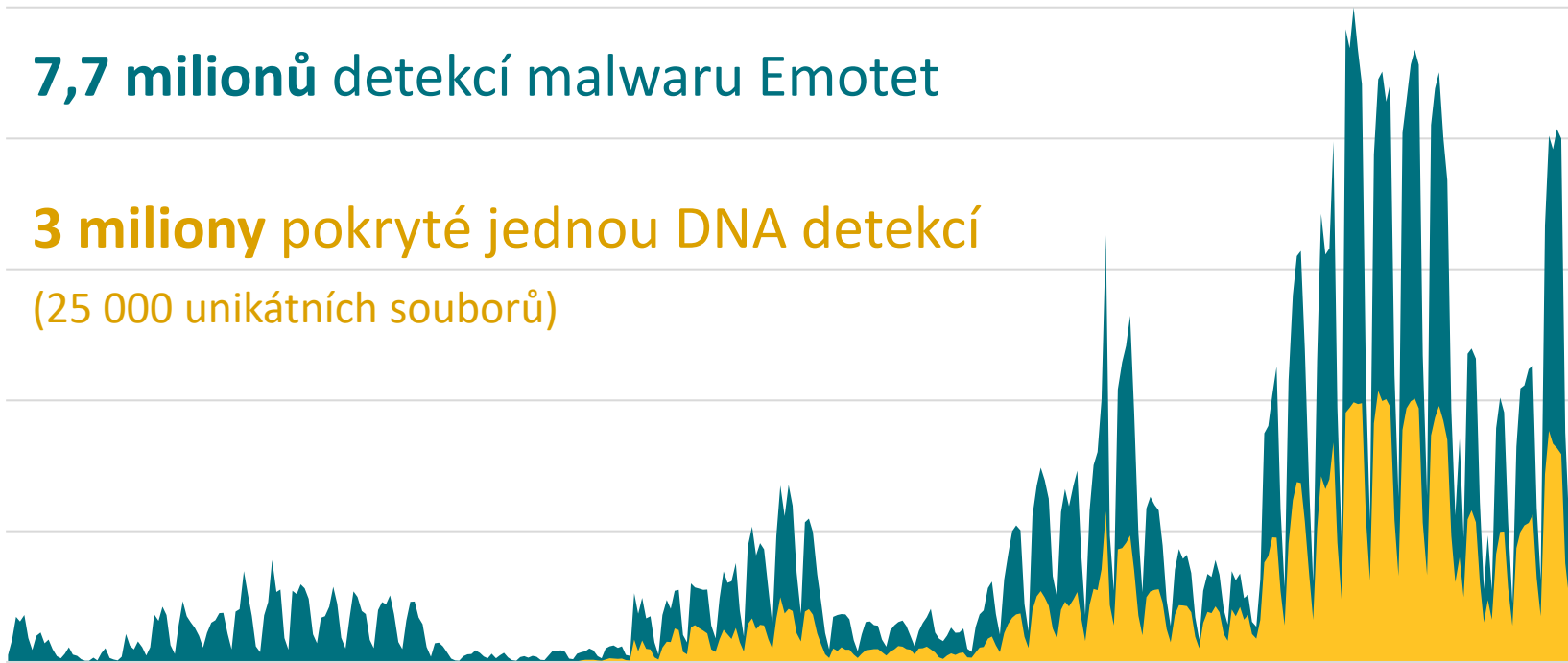
5. 2018

7. 2018

9. 2018

11. 2018

1. 2019





Machine Learning Engine ESET Augur

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
```

NÁSTĚNKA

1
POČÍTAČE

DETEKCE

Přehledy

Úlohy

Instalační balíčky

Politiky

Uživatelé zařízení

Oznámení

2
Stav serveru4
Další

Nová politika

Politiky > Nová politika

Obecné

Nastavení

Přidat

Souhm

ESET Endpoint for Windows

Q Co chcete hledat...

?

DETEKČNÍ JÁDRO

Residentní ochrana souborového systému

Cloudová ochrana

Detekce škodlivého kódu

HIPS

AKTUALIZACE

SÍŤOVÁ OCHRANA

WEB A MAIL

SPRÁVA ZAŘÍZENÍ

NÁSTROJE

UŽIVATELSKÉ ROZHRAŇÍ

DOČASNÁ ZMĚNA NASTAVENÍ

- REZIDENTNÍ OCHRANA S VYUŽITÍM STROJOVÉHO UČENÍ

ŠKODLIVÝ KÓD

	Agresivně	Vyváženě	Mírně	Vypnuto	
<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Hlášení	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>
<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Ochrana	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>

POTENCIÁLNĚ NECHTĚNÉ APLIKACE

	Agresivně	Vyváženě	Mírně	Vypnuto	
<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Hlášení	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="i"/>
<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Ochrana	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="i"/>

PODEZŘELÉ APLIKACE

	Agresivně	Vyváženě	Mírně	Vypnuto	
<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Hlášení	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>
<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Ochrana	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="button" value="i"/>

POTENCIÁLNĚ ZNEUŽITELNÉ APLIKACE

	Agresivně	Vyváženě	Mírně	Vypnuto	
<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Hlášení	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="i"/>
<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/> Ochrana	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="button" value="i"/>

+ 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

PROPERTIES

System Properties

Computer Name Hardware Advanced Remote

Remote Assistance

 Allow Remote Assistance connections to this computer

Advanced...

Remote Desktop

Choose an option, and then specify who can connect.

 Don't allow remote connections to this computer

 Allow remote connections to this computer

 Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)
[Help me choose](#)

Select Users...

OK

Cancel

Apply

 Last installed updates
 Windows Update
 Last checked for updates

 Windows Error Reporting
 Customer Experience Improvem
 IE Enhanced Security Configurati
 Time zone
 Product ID

 Server 2012 R2 Datacenter
 o. Virtual server

 Processors
 Installed memory (RAM)
 Total disk space

Filter

Server Name	ID	Severity	Source	Log	Date ar
WIN-8A4HV84HBGK	8198	Error	Microsoft-Windows-Security-SPP	Application	22. 3. 21
WIN-8A4HV84HBGK	10149	Warning	Microsoft-Windows-Windows Remote Management	System	22. 3. 21
WIN-8A4HV84HBGK	7023	Error	Microsoft-Windows-Service Control Manager	System	22. 3. 21

RDP

Ransomware Deployment Protocol

Whitelistace konkrétních IP
 Restrikce na uživatelské účty
 Nastavení komplexních hesel
 Nastavení zamykání účtů
 Zakázání nebo přejmenování
 účtu Administrator



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



Hospitals in US, Australia hobbled by ransomware

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



South African power company battles ransomware attack

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



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



Buhtrap backdoor and Buran ransomware distributed via major advertising platform

To pay o
attackers
do pay u
away?



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

City
that
Afric
is gra
attac
with
Reut

are
"attack",
partment
(DIR)



**CYBERSECURITY
EXPERTS ON YOUR SIDE**

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