VIAVIS střežíme podstatné

CACIO

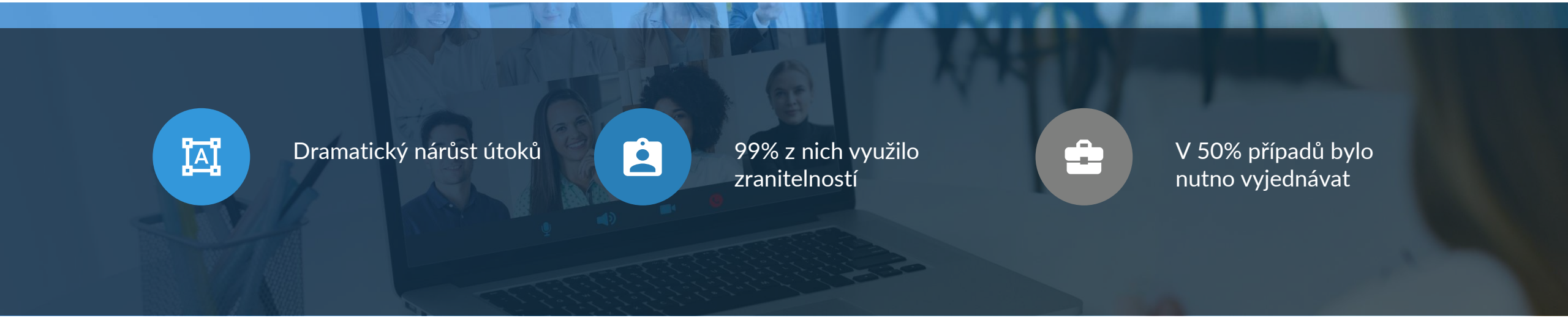
S hackery se nevyjednává?

Vladimír Lazecký

Jan Bonczek

Úrodný rok 2021

Naše zkušenost – bez nároku na generalizaci



Dramatický nárůst útoků

99% z nich využilo zranitelností

V 50% případů bylo nutno vyjednávat

V čem jsou útočníci dobří

Exploitace a obcházení AV

Jsou dobří ve zneužívaní zranitelností a v tom jak obejít AV.

Eskalace privilegií

Jsou velice dobří v tom jak získat domain admin přístup.

Mazání záloh

Zaměřují se na mazání a šifrování záloh.

Rychlost

Vše zvládnou velice rychle.

Příklad první

Magistrát města Olomouc

Kyberútok na olomoucký magistrát, agendy úřadů jsou mimo provoz

7.4.2021

Michal Kovář Daniela Tauberová

Datové systémy olomouckého magistrátu napadli ve středu ráno hackeři. Kybernetický útok byl podle radnice velmi silný a navíc přišel v den, kdy chodí na úřad více lidí. Agendy byly po celý den mimo provoz.

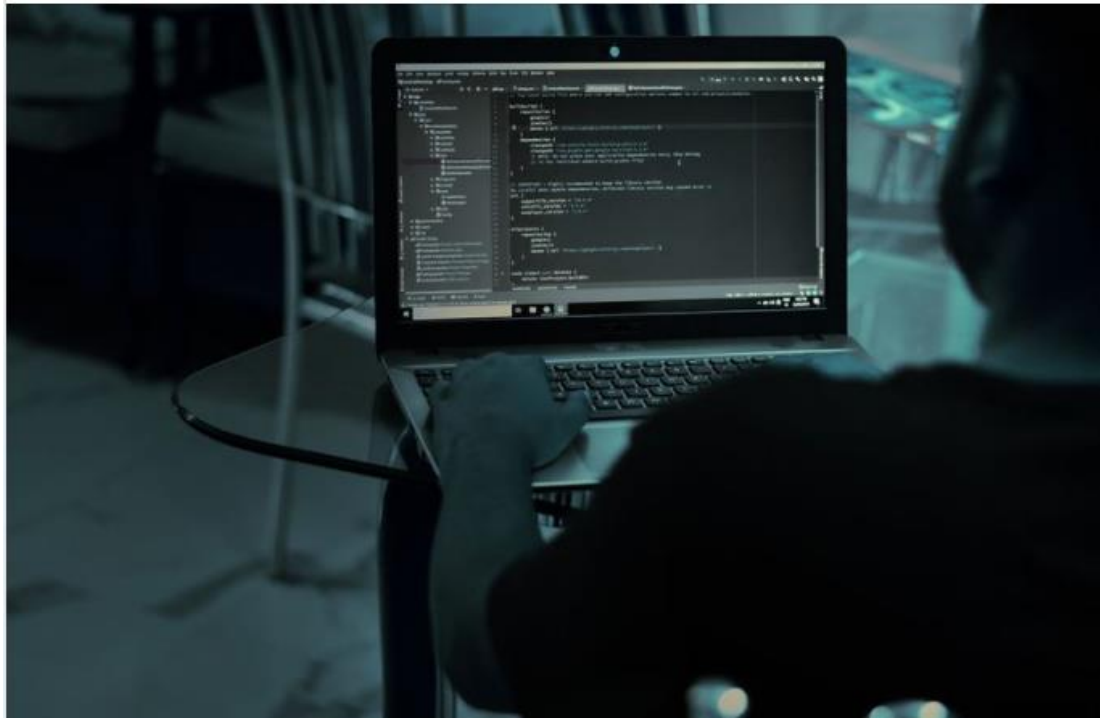
Budova olomouckého magistrátu v Hynaisově ulici | Foto: DENÍK

Magistrát města Olomouc

Statutární město Olomouc
26. dubna v 16:39 ·

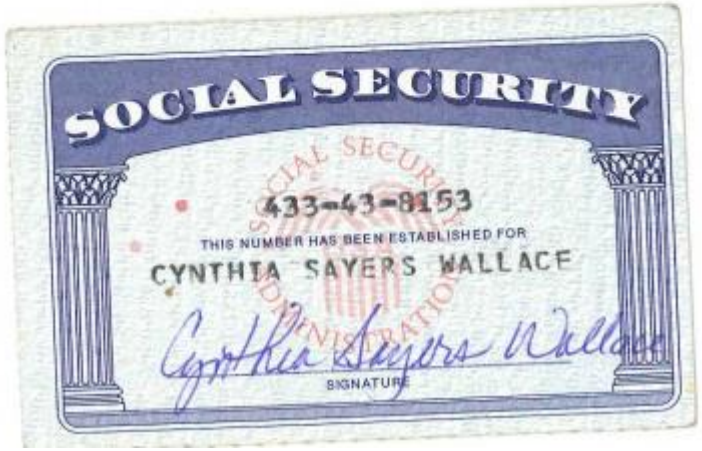
1️⃣Magistrát funguje. 2️⃣Hackeři znovu útočili
👉Dva a půl týdne od začátku kybernetického útoku jsou veřejnosti k dispozici služby téměř všech agend magistrátu. Výjimkou je zatím živnostenský úřad, ale na zprovoznění jeho agendy se intenzivně pracuje. V případě některých odborů, jako je majetkoprávní, stavební, životního prostředí, dopravy či místní zeleně a odpadového hospodářství, zatím neběží plnohodnotně softwarová podpora. Vyřizování příslušné žádosti může proto být v některých případech zdlouhavější. IT specialisté pracují na tom, aby bylo fungování magistrátní digitální infrastruktury a všech speciálních aplikací každým dnem lepší, rychlejší a bezpečnější.

👉O víkendu došlo také k útoku na webové stránky města, kdy stejná hackerská skupina cíleně útočila na webové servery s cílem eliminovat jejich dostupnost. IT tým útok rychle odhalil, provedl protiopatření, a preventivně příslušné servery odstavil. Webové portály budou zatím omezeny co do funkčnosti. Podle odborníků se jednalo o jiný typ útoku – tzv. DDoS, k němuž se ale hlásí stejná skupina útočníků – dle jejího vyjádření jde o mstu za obnovení infrastruktury vlastními silami, aniž by město útočníkům platilo požadované výkupné.



Ilustrační obrázek. Zdroj: Avaddon home page na Darknet

CEO TAX, SOCIAL SECURITY NUMBER + DRIVER LICENSE

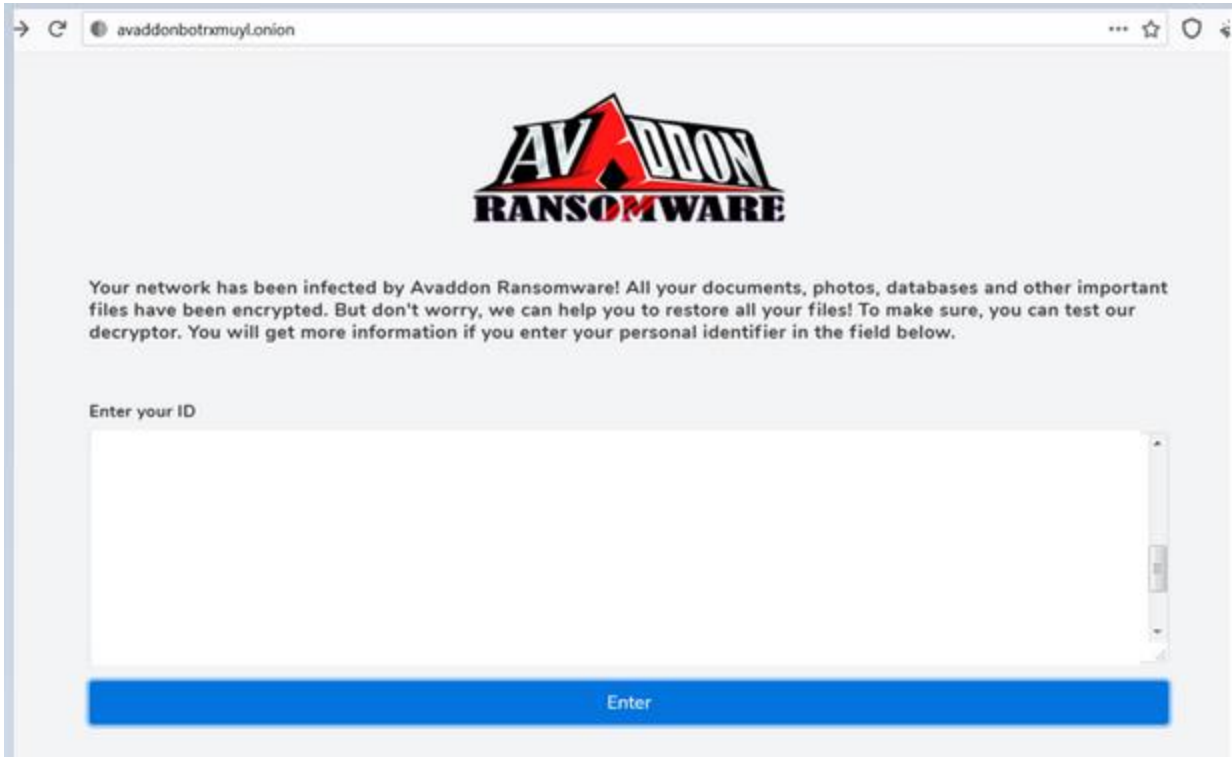


Ejercicio: 2018

		iento	Contrapartid:	Comentario	Debe	Haber	Saldo
		TERIORAMIENTO PARCELA (1296242CG7819N0000XX)					
			27	69100010015 DETERIORAMIENTO TERRENOS I BIENES NATURA		71860,84	-71860,84
			27	79100010015 REVERSION TERRENOS Y BIENES NATURALES	5282,18		-66578,66
			29	Cierre contabilidad 2017	66.578,66		
		tos ...			71.860,84	71.860,84	
		TERIORAMIENTO PARCELA (1296248CG7819N0000UX)					
			27	69100010015 DETERIORAMIENTO TERRENOS I BIENES NATURA		51462,94	-51462,94
			27	79100010015 REVERSION TERRENOS Y BIENES NATURALES	3585,94		-47877
			29	Cierre contabilidad 2017	47.877,00		
		tos ...			51.462,94	51.462,94	
		TERIORAMIENTO PARCELA (1296249CG7819N0000HX)					
			27	69100010015 DETERIORAMIENTO TERRENOS I BIENES NATURA		51223,86	-51223,86
			27	79100010015 REVERSION TERRENOS Y BIENES NATURALES	3566,57		-47657,29
	31/12/2017		29	Cierre contabilidad 2017	47.657,29		
		Suma Movimientos ...			51.223,86	51.223,86	
291000000158		DETERIORAMIENTO PARCELA (1296250CG7819N00000ZX)					
	01/01/2017		27	69100010015 DETERIORAMIENTO TERRENOS I BIENES NATURA		51974,89	-51974,89
	31/12/2017		27	79100010015 REVERSION TERRENOS Y BIENES NATURALES	3547,22		-48427,67
	31/12/2017		29	Cierre contabilidad 2017	48.427,67		
		Suma Movimientos ...			51.974,89	51.974,89	
291000000159		DETERIORAMIENTO PARCELA (1296241CG7819N0000DX)					
	01/01/2017		27	69100010015 DETERIORAMIENTO TERRENOS I BIENES NATURA		69967,28	-69967,28
	31/12/2017		27	79100010015 REVERSION TERRENOS Y BIENES NATURALES	5062,88		-64904,4
	31/12/2017		29	Cierre contabilidad 2017	64.904,40		
		Suma Movimientos ...			69.967,28	69.967,28	
291000000160		DETERIORAMIENTO PARCELA (1296243CG7819N0000IX)					
	01/01/2017		27	69100010016 DETERIORAMIENTO TERRENOS I BIENES NATURA		73987,61	-73987,61

Vyjednávání s útočníky

```
--------===    Your network has been infected!    ===--------

*****************    DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED    *****************

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

You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!

The only way to restore your files is to buy our special software. Only we can give you this software and only we c
restore your files!

We have also downloaded a lot of private data from your network.

If you do not contact as in a 3 days we will post information about your breach on our public news website
(avaddongun7rngel.onion) and after 7 days the whole downloaded info.

You can get more information on our page, which is located in a Tor hidden network.


How to get to our page

--------------------------------------------------------------------------------
|
|  1. Download Tor browser - https://www.torproject.org/
|
|  2. Install Tor browser
|
|  3. Open link in Tor browser - avaddonbotrxmuyl.onion
|
|  4. Follow the instructions on this page
|
--------------------------------------------------------------------------------

Your ID:
```



Zdroj: Avaddon

Jak to dopadlo

Windows zašifrované

Windows zašifrované. Linuxy přežily.

Výkupné nezaplaceno

Požadováno 100 000 dolarů.

Následovaly DDoS

Jako pomsta za nezaplacení následoval dlouhotrvající DDoS.

Napadení webového serveru

Exploitace a smazání.

Zveřejnění dat

Byla zveřejněna ukradená data.

Příklad druhý

Centrální konzole AV

Endpoint Protection - Dashboard

Overview / Endpoint Protection Dashboard

He
Central

Recent threat graphs

Sophos generated | Admin generated

As an MTR customer, these graphs are for information only for all devices with an MTR assigned license. Our MTR team will contact you if you need to take action.

Time created	Priority	Name	User	Device
Oct 16, 2021 7:20 AM	High	CryptoGuard	Frank Castle	Win7-desktop-3
Oct 16, 2021 6:32 AM	Medium	PrivGuard	Frank Castle	Win7-desktop-3
Oct 16, 2021 5:46 AM	Medium	CodeCave	Frank Castle	Win7-desktop-3
Oct 16, 2021 1:49 AM	Medium	ATK/Shellter-B	Frank Castle	Win7-desktop-3
Oct 16, 2021 12:56 AM	Medium	HeapHeapProtect	Frank Castle	Win7-desktop-3

Threat Analysis Center - CryptoGuard

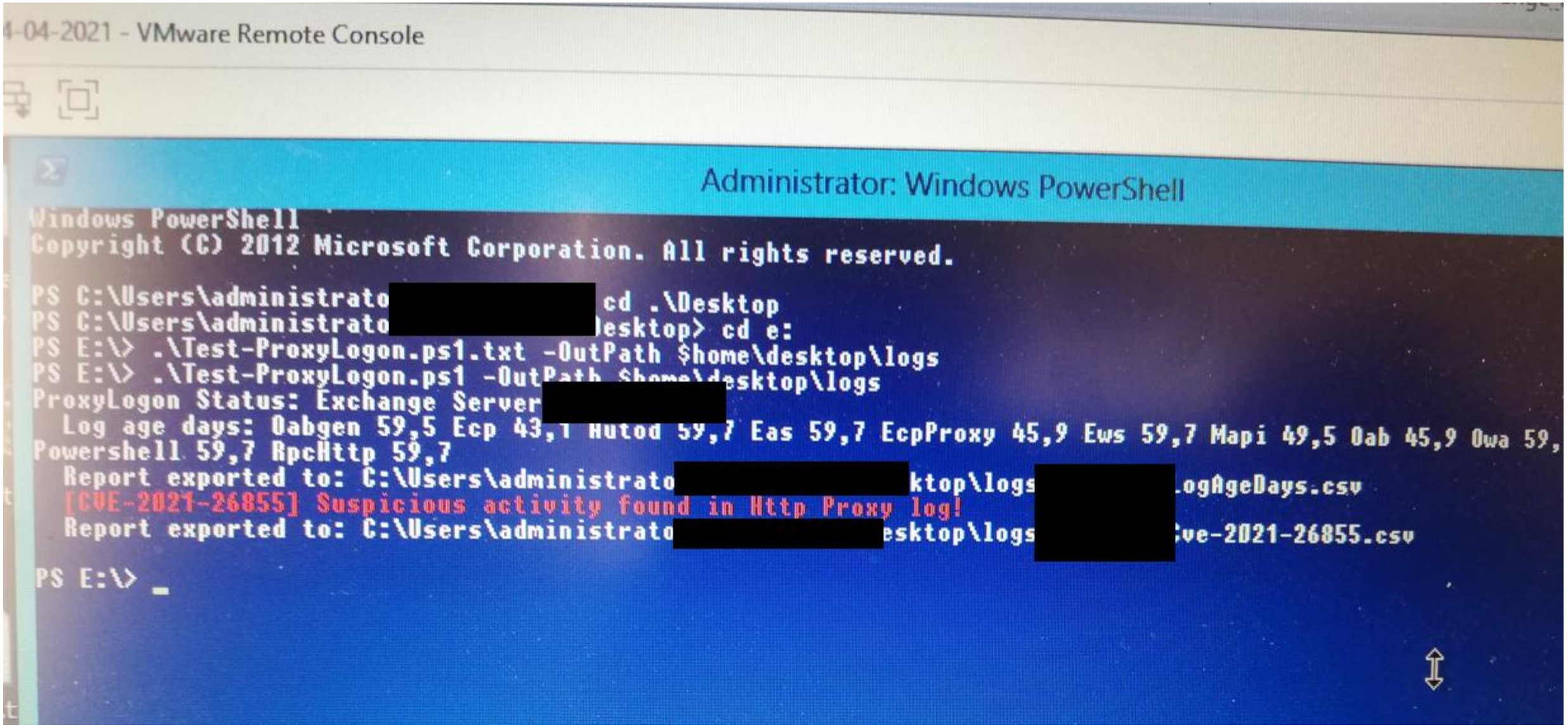
Overview / Threat Analysis Center Dashboard / Threat Graphs / CryptoGuard

Help
Central Demo Sophos In

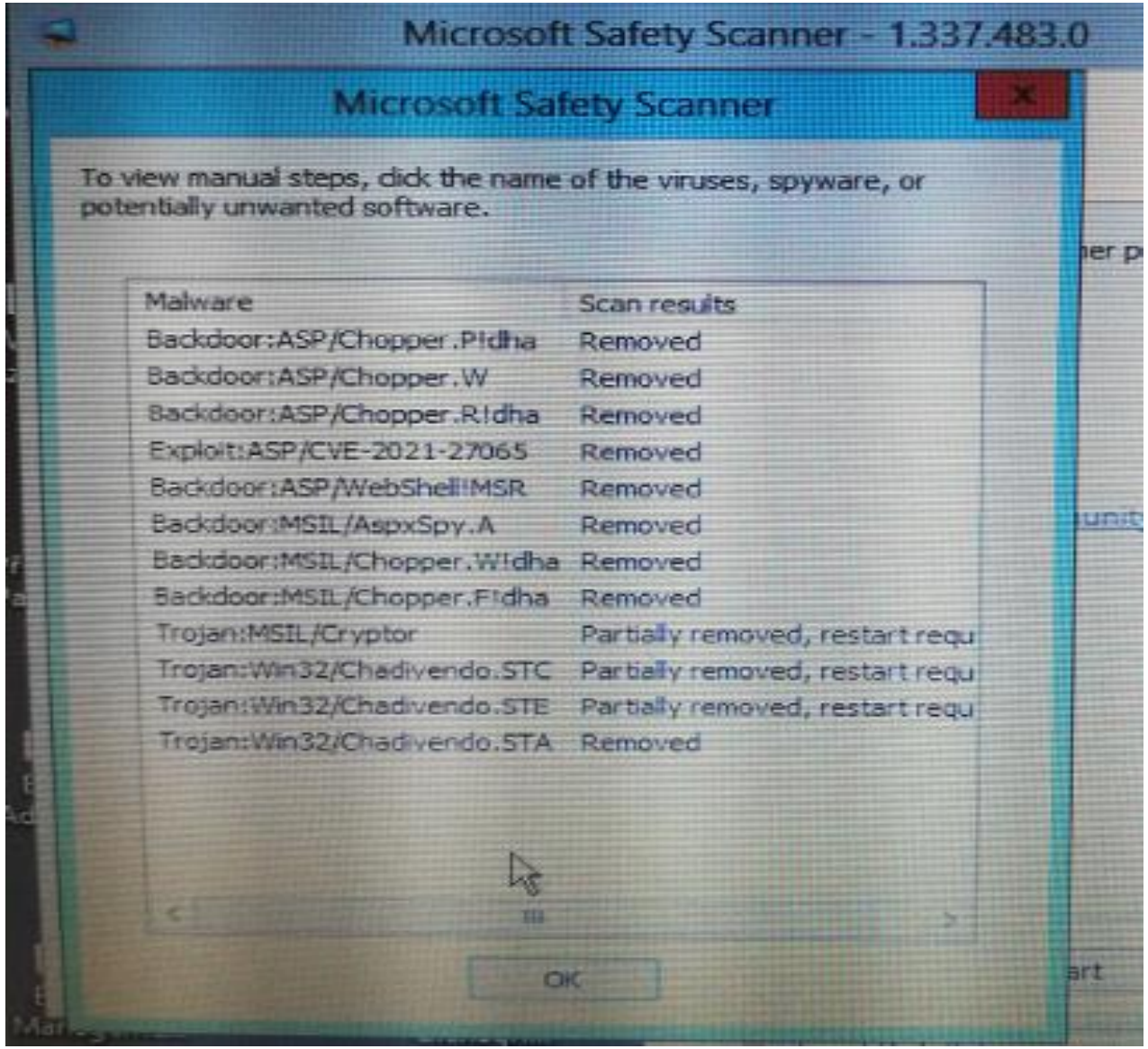
Summary

Suggested next steps

Analýza OS


4-04-2021 - VMware Remote Console
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.
PS C:\Users\administrato [redacted] cd .\Desktop
PS C:\Users\administrato [redacted] esktop> cd e:
PS E:\> .\Test-ProxyLogon.ps1.txt -OutPath $home\desktop\logs
PS E:\> .\Test-ProxyLogon.ps1 -Out[redacted]esktop\logs
ProxyLogon Status: Exchange Server [redacted]
Log age days: Oabgen 59,5 Ecp 43,1 Hutod 59,7 Eas 59,7 EcpProxy 45,9 Ews 59,7 Mapi 49,5 Oab 45,9 Owa 59,
Powershell 59,7 RpcHttp 59,7
Report exported to: C:\Users\administrato [redacted] ktop\logs [redacted] .ogAgeDays.csv
[CVE-2021-26855] Suspicious activity found in Http Proxy log!
Report exported to: C:\Users\administrato [redacted] esktop\logs [redacted] Cve-2021-26855.csv
PS E:\> _

Analýza OS


Microsoft Safety Scanner - 1.337.483.0
Microsoft Safety Scanner
To view manual steps, dick the name of the viruses, spyware, or potentially unwanted software.
Malware
Scan results
Backdoor:ASP/Chopper.P!dha
Removed
Backdoor:ASP/Chopper.W
Removed
Backdoor:ASP/Chopper.R!dha
Removed
Exploit:ASP/CVE-2021-27065
Removed
Backdoor:ASP/WebShell!MSR
Removed
Backdoor:MSIL/AspxSpy.A
Removed
Backdoor:MSIL/Chopper.W!dha
Removed
Backdoor:MSIL/Chopper.F!dha
Removed
Trojan:MSIL/Cryptor
Partially removed, restart requ
Trojan:Win32/Chadivendo.STC
Partially removed, restart requ
Trojan:Win32/Chadivendo.STE
Partially removed, restart requ
Trojan:Win32/Chadivendo.STA
Removed
OK

Analýza komunikace

Jak to dopadlo

Vše zašifrované

Windows zašifrované. Linuxy smazané.

Technologická síť přežila

Uživatelská doména posloužila jako honeypot.

Zaplacení výkupného

Zaplaceno 1,5 BTC.

Existovala druhá lokalita

V době útoku byla téměř připravena nová serverovna.

18 TB dat

V době útoku nebyly dostupné SSD.

Co s tím?

Důsledná segmentace

Přístup všude jen na základě nutného minima.

Řídit vzdálené přístupy

Více faktorová autentizace je „must have“.

Zálohy

Co je doma, to se počítá.

Za všechno může uživatel?

Platí i pro IT. Bez kvalitních lidí na IT pozici to nepůjde.

Útoky z pohledu managementu

Uspěl management?

- Formální/reálná připravenost
- Zvyšování časového stresu
- Řešení nepodstatných problémů

Veselé příhody z natáčení

- „Jak dlouho budeme obnovovat? Hmm, to raději zaplatíme...“
- „Může za to informatika, potrestáme je. Zkrátíme jim rozpočet…“
- „Tak dáme zálohy do cloudu, nemůže se nic stát… “
- Poslední vlna útoku

Workshop – jak zvládnout kyber útok

Simulace reálného útoku

Tým managementu a tým IT

Reakce na jednotlivé fáze a vlny útoku

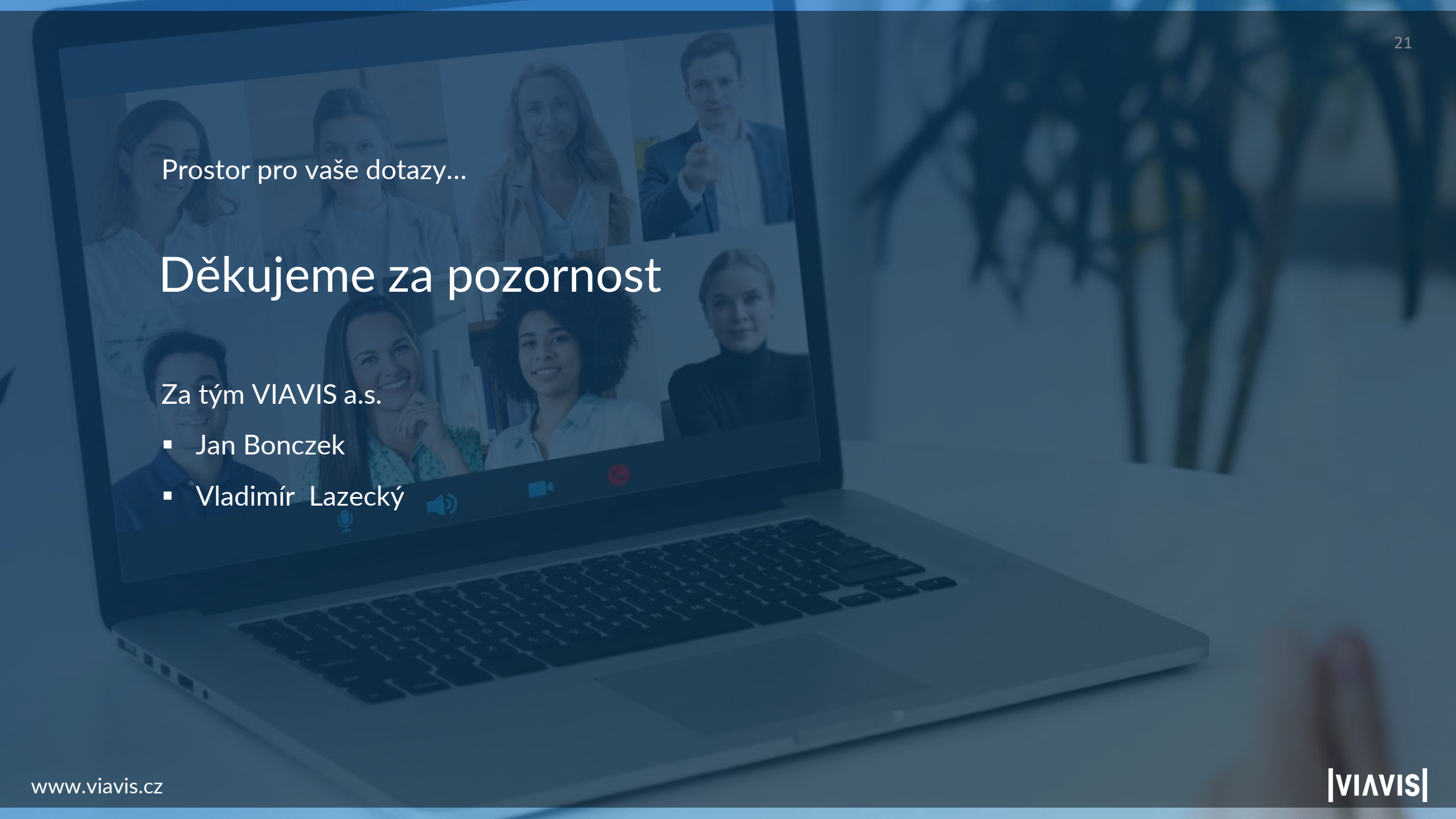
Co si odnesete

Jak řešit situace, o kterých se nedočtete

Ukázka pro CACIO

14.4.2022

Registrace: jan.heisler@cacio.cz



Prostor pro vaše dotazy…

Děkujeme za pozornost

Za tým VIAVIS a.s.

- Jan Bonczek
- Vladimír Lazecký