
NT KONF
25. – 27.
SEPTEMBER
2023
PORTOROŽ
NT KONF
NT KONFERENCA

Neprebojna podjetja:
Zakaj se nekaterih ne da enostavno pohekat?

Milan Gabor, Viris

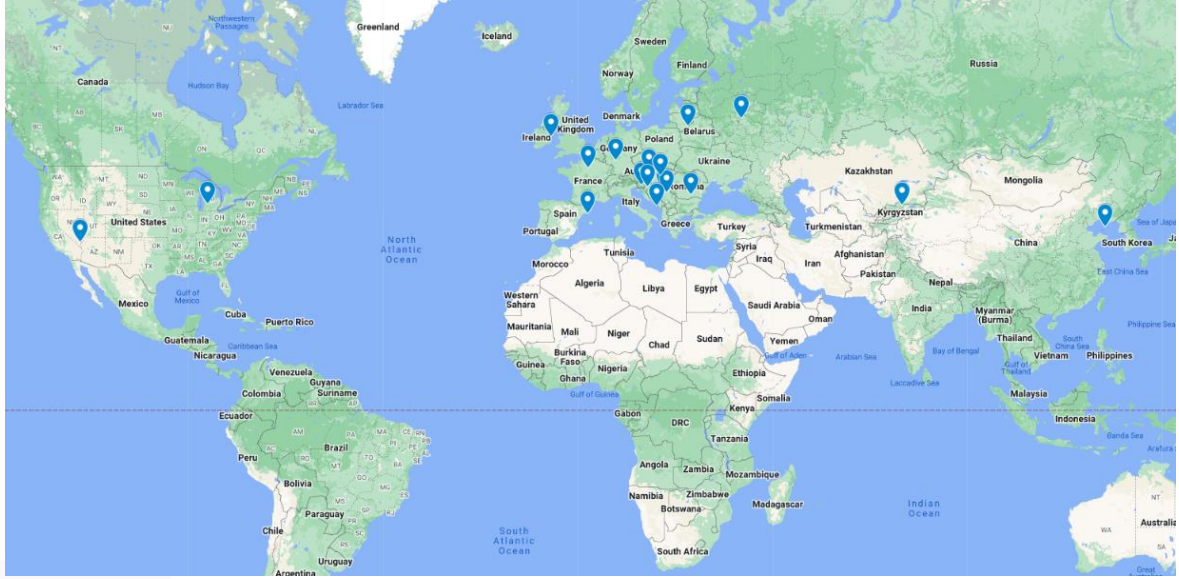
Milan Gabor

Etični heker

Viris – deklica za vse ;)

OWASP Maribor/BSides Ljubljana

Stvari iz prakse

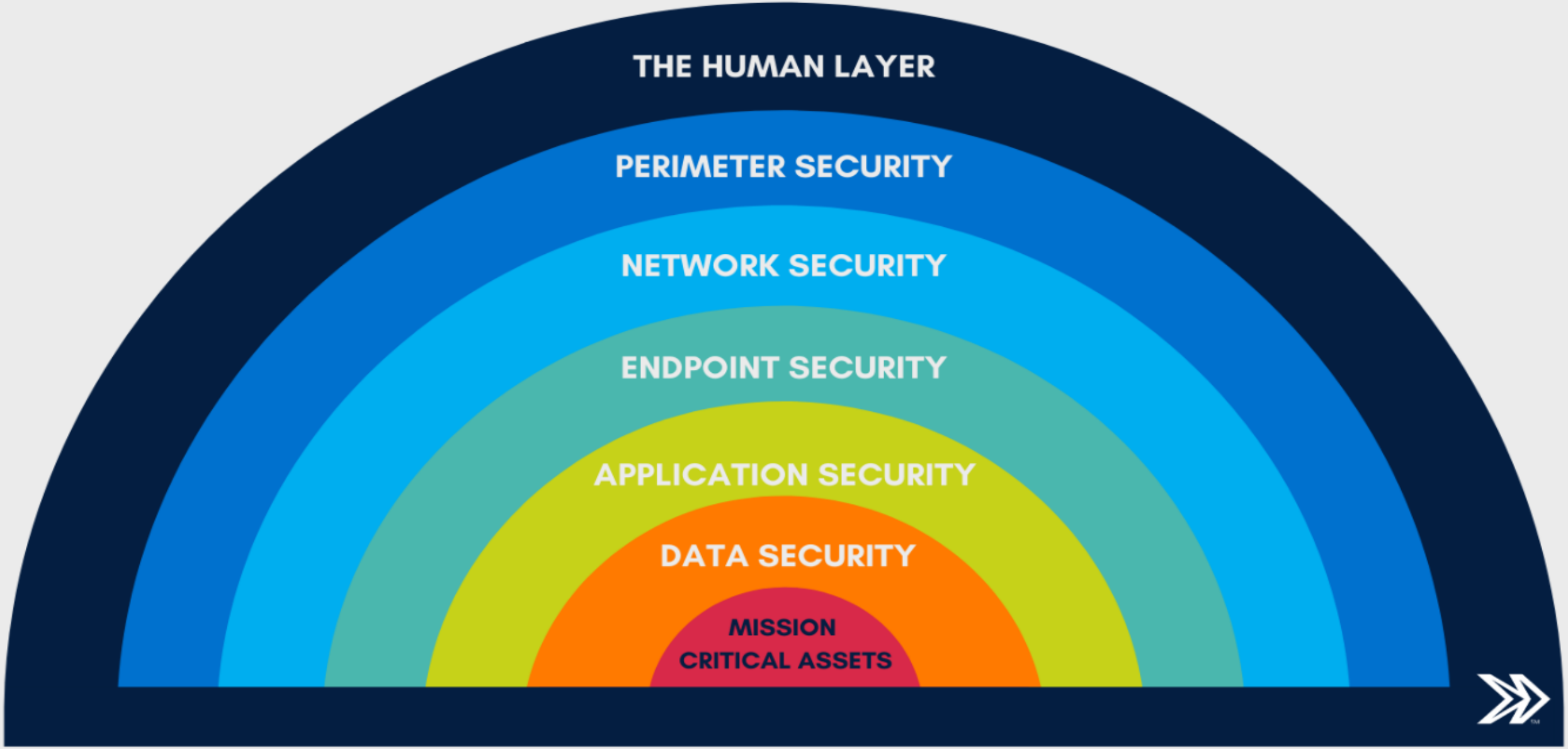


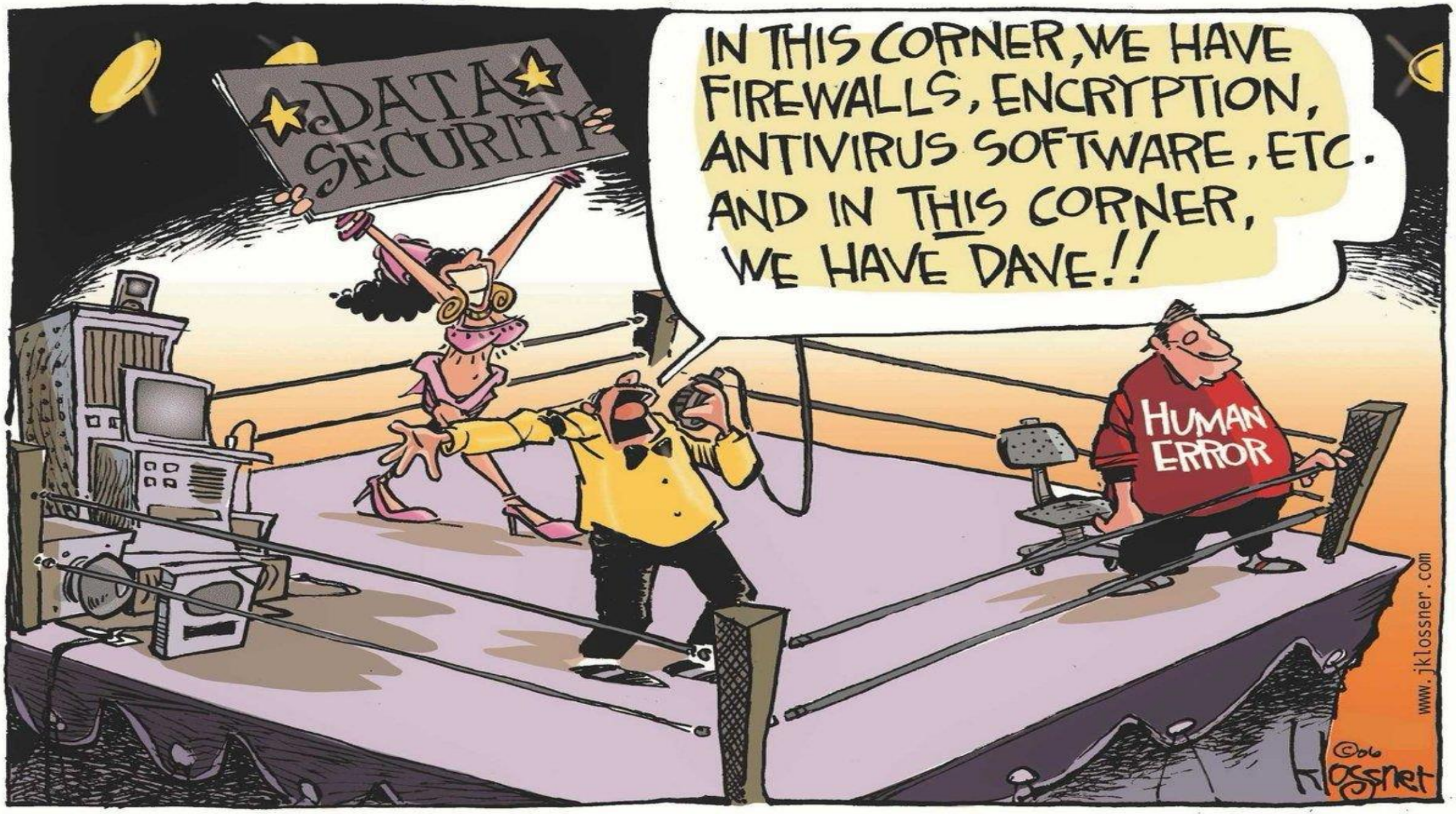

MYTH
VS
REALITY

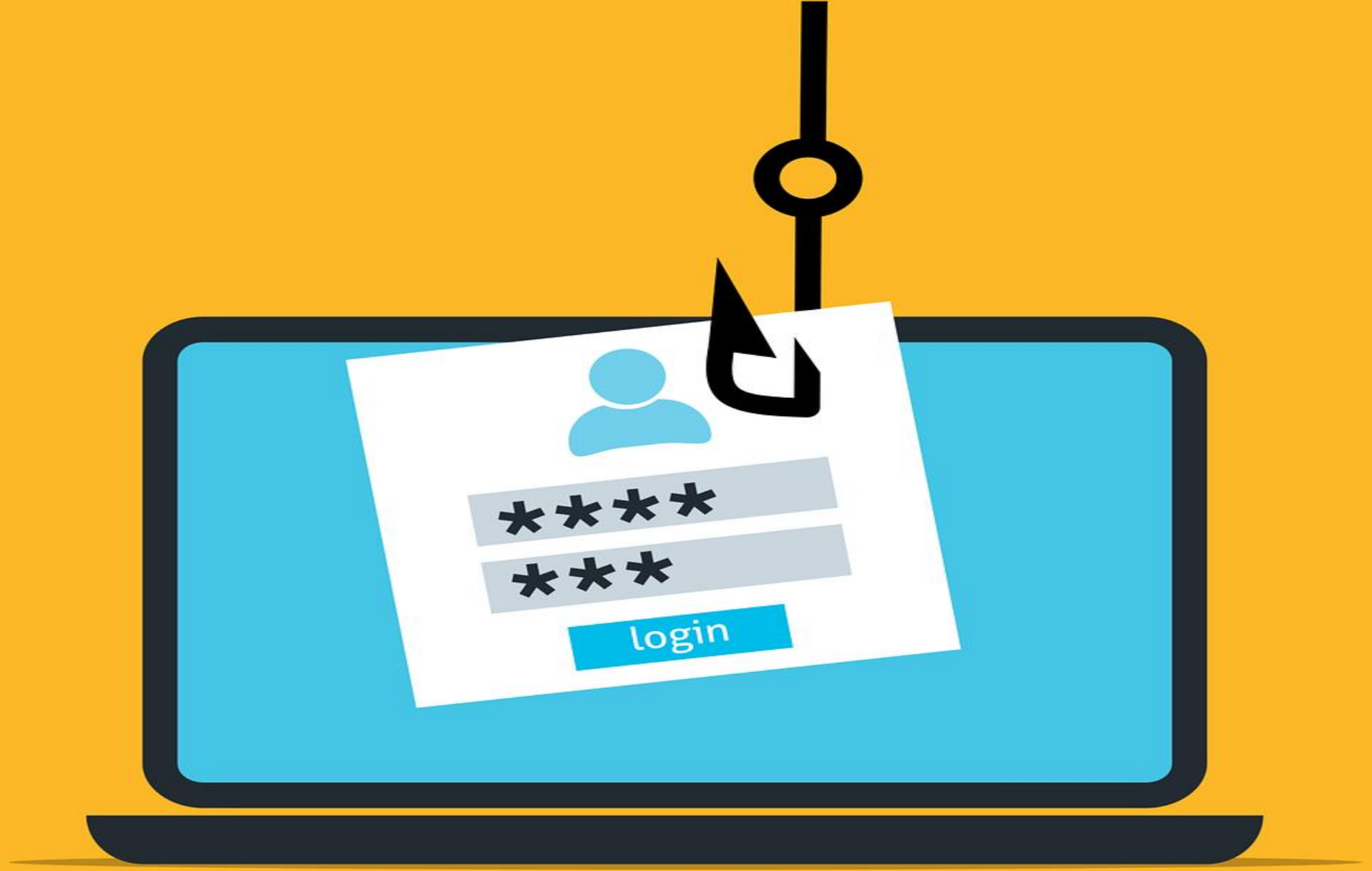

"THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO'VE BEEN HACKED, AND THOSE WHO DON'T KNOW THEY'VE BEEN HACKED."
-JAMES COMEY, FORMER FBI DIRECTOR
197 days
Average time to identify a breach
69 days
Average time after detection to full recovery
$4.45Million
Average cost of a data breach in 2023 (2% YoY increase)
$1.76Million
Average savings for organizations that use security AI and automation extensively compared to the ones that don't
Source: IBM (2023), Ponemon Institute (2023
COURE
NEVER LET A COMPUTER KNOW YOU'RE IN A HURRY

Ljudje

THE 7 LAYERS OF CYBERSECURITY




DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
©06 Klossner
www.jklossner.com

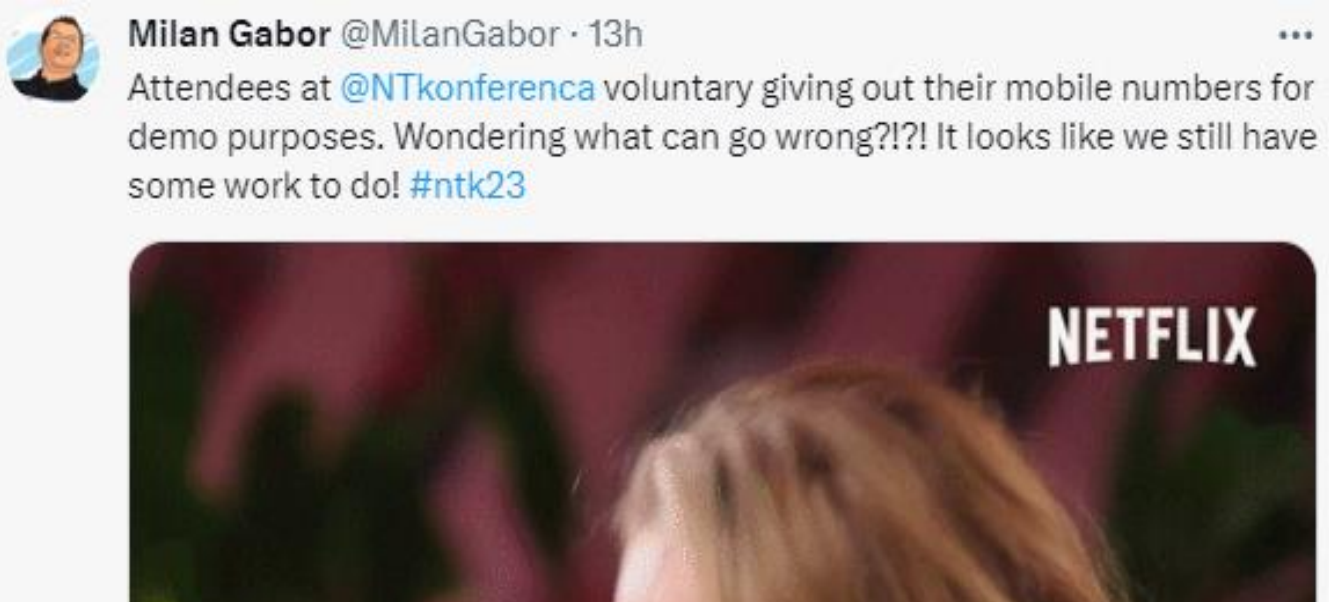

****
***
login

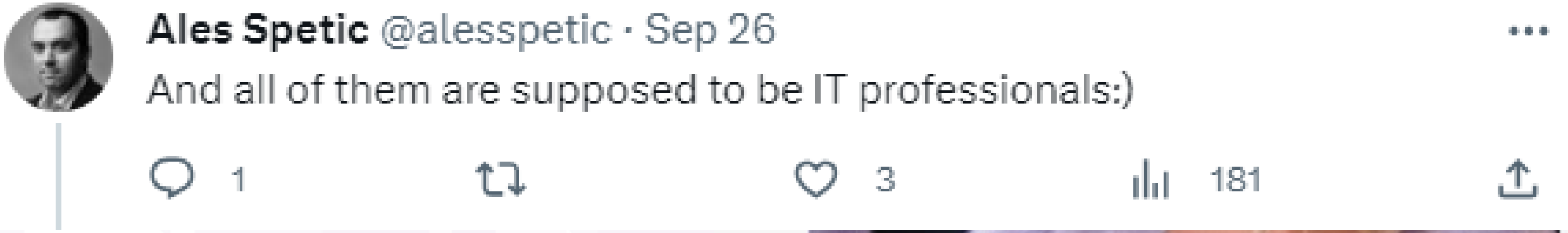
Informacijski pooblaščenec (v nadaljevanju IP) uvodoma pojasnjuje, da sodijo t.i. tehnike ribarjenja podatkov (angl. phishing; več o tem na naši spletni strani: **https://www.ip-rs.si/varstvo-osebnih-podatkov/informacijske-tehnologije-in-osebni-podatki/varstvo-osebnih-podatkov-na-internetu/#c412**) med precej nevarne in učinkovite načine socialnega inženiringa za izvabljanje podatkov, kot so uporabniška imena in gesla, ter posledično nepooblaščene vstope v informacijske sisteme, zato so prizadevanja, ki jih izvajajo organizacije za ozaveščanje svojih zaposlenih o nevarnostih ribarjenja podatkov načeloma legitimne. Seveda pa se pri tem porajajo vprašanja glede smiselnosti, učinkovitosti in transparentnosti ter - kot tudi sami opozarjate – etičnih in moralnih vidikov *preverjanja* zaposlenih glede prepoznavanja t.i. phishing sporočil, sporna je lahko tudi sama zakonitost izvedbe preverjanja, kar pa je zelo odvisno od konkretnih okoliščin primera, samo zakonitost (obdelave osebnih podatkov) pri takšnih preverjanjih pa se lahko preveri le v okviru inšpekcijskega postopka.

IP meni, da *preverjanje* (pre)poznavanja phishing sporočil s strani zaposlenih načeloma ni najbolj primerno, saj lahko vodi v nezaželene odzive in slabo počutje zaposlenih, zlasti če so npr. izpostavljeni kot tisti, ki niso prepoznali lažnega sporočila, zato priporočamo, da se organizacije vzdržijo tovrstnih preverjanj in raje izhajajo iz predpostavke, da je tudi naša organizacija lahko dojemljiva za napade z ribarjenjem podatkov in da je pri tovrstnih napadih veliko bolj kot merjenje stopnje ranljivosti pomembno ustrezno ozaveščanje. Dejstvo je, da so tovrstni napadi na varnost organizacije relativno učinkoviti in izmeriti stopnjo učinkovitosti teh napadov v naši organizaciji najbrž ni primarni in ključni namen organizacije, temveč bi morala biti čim večja odpornost organizacije na take napade, ki je v primeru phishing napadov praktično samo ustrezna ozaveščenost zaposlenih.

Še sveže!

Nore ideje!

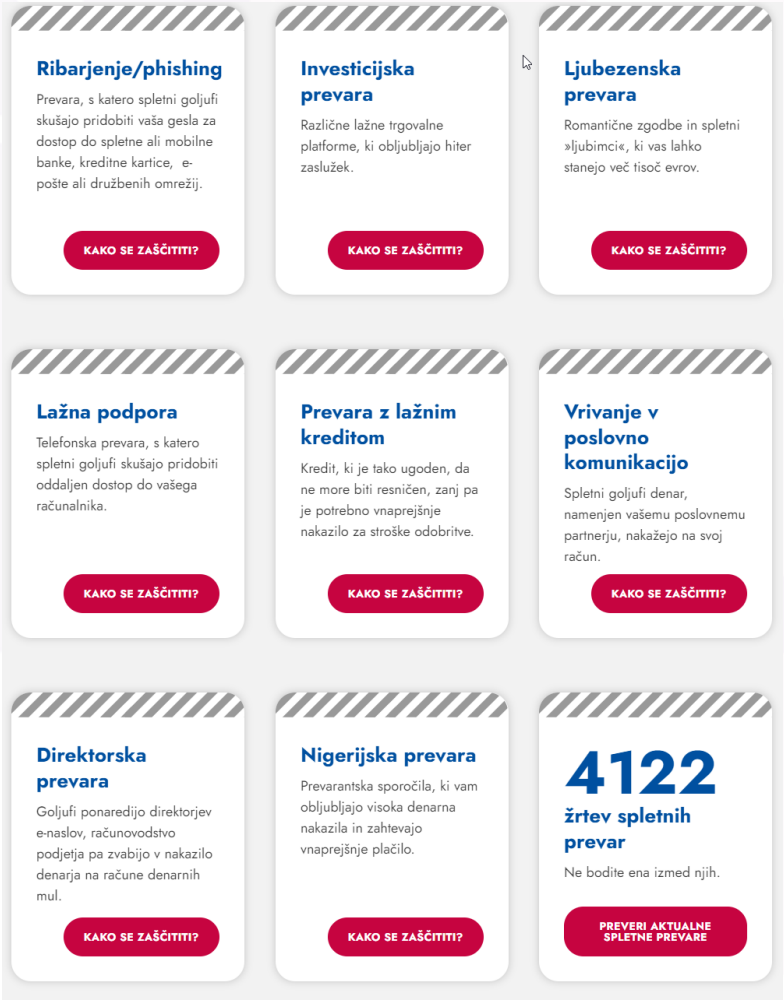


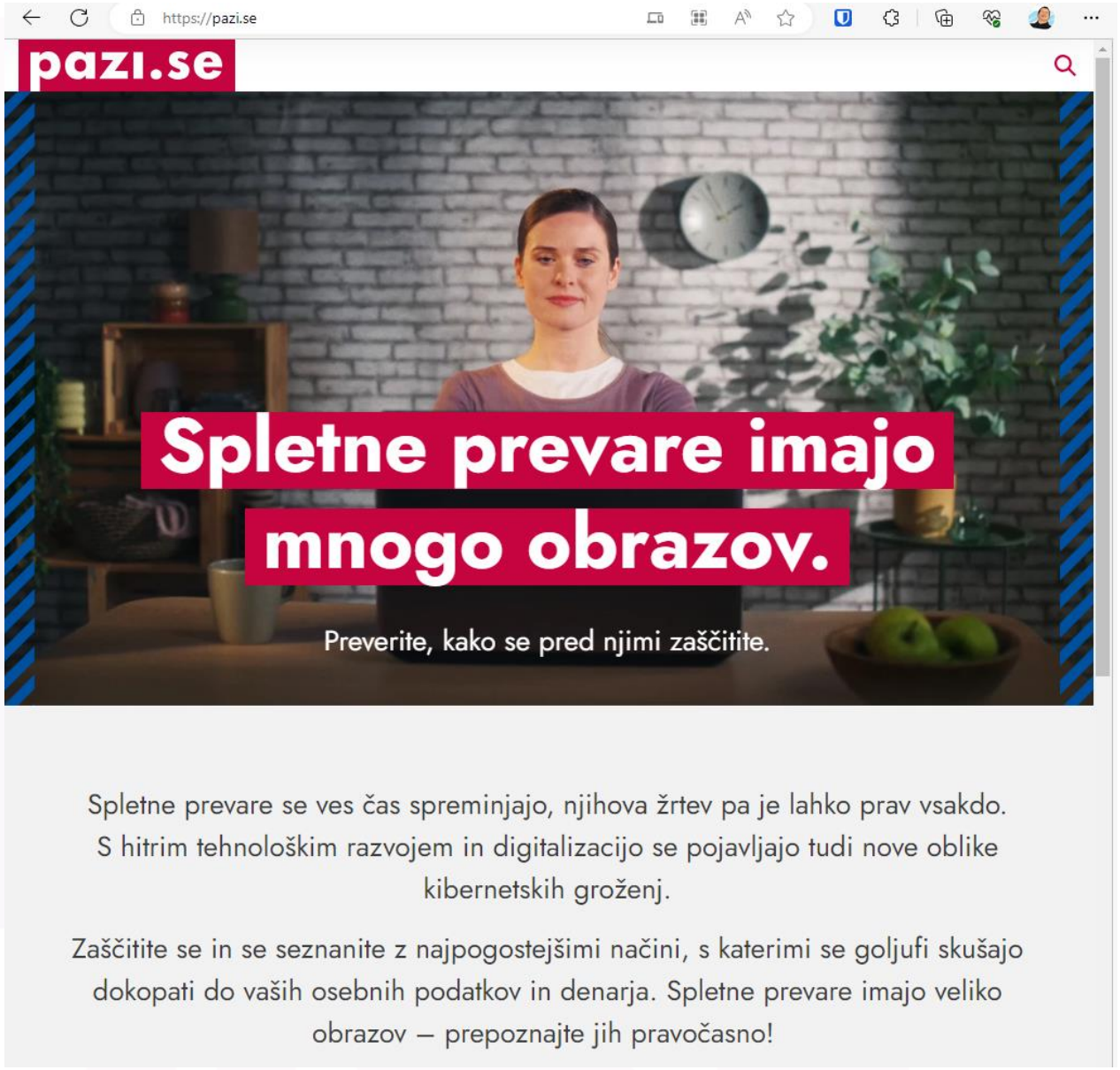


NT KONF
NT KONFERENCA

Preventiva vs kurativa

- https://pazi.se/



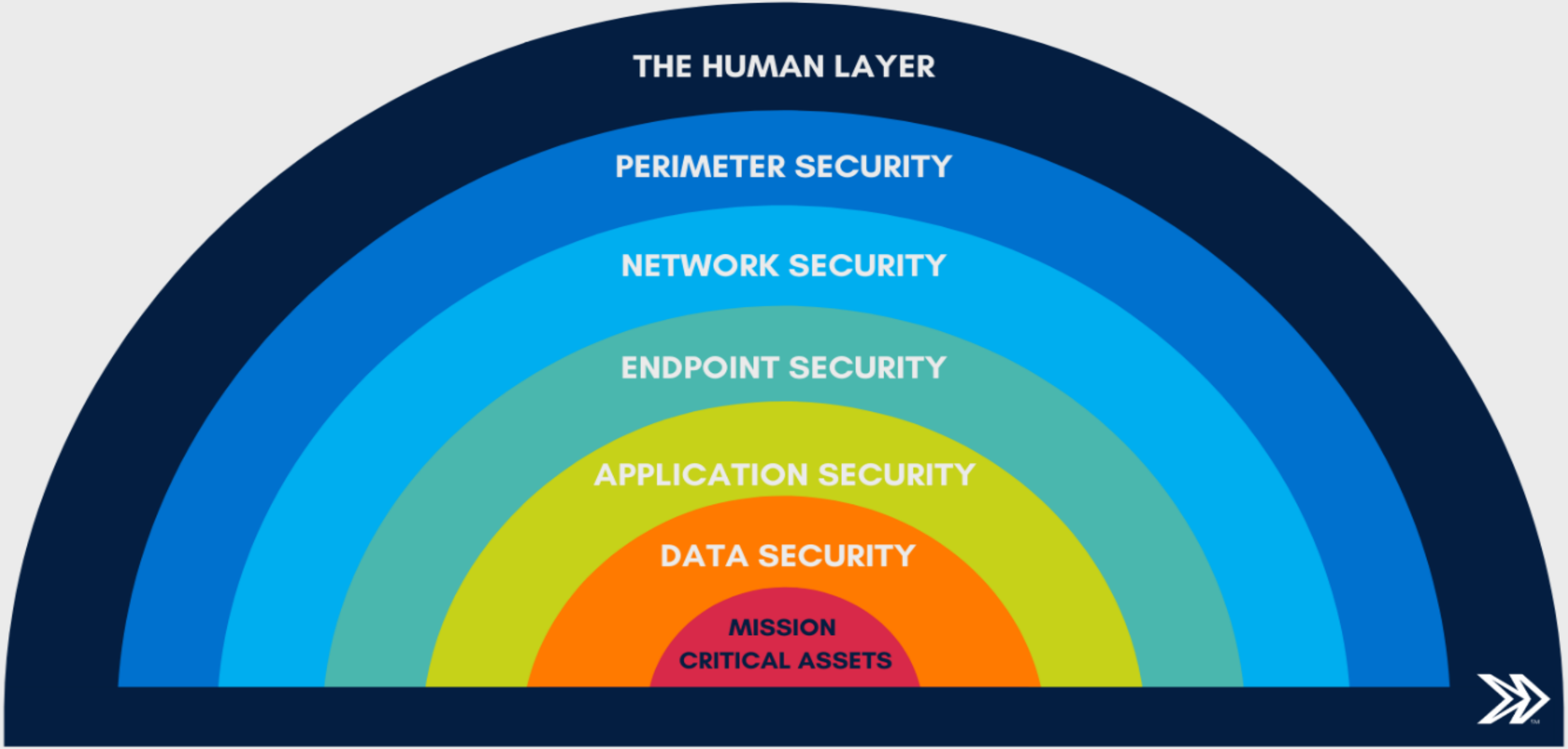


NT KONF
NT KONFERENCA

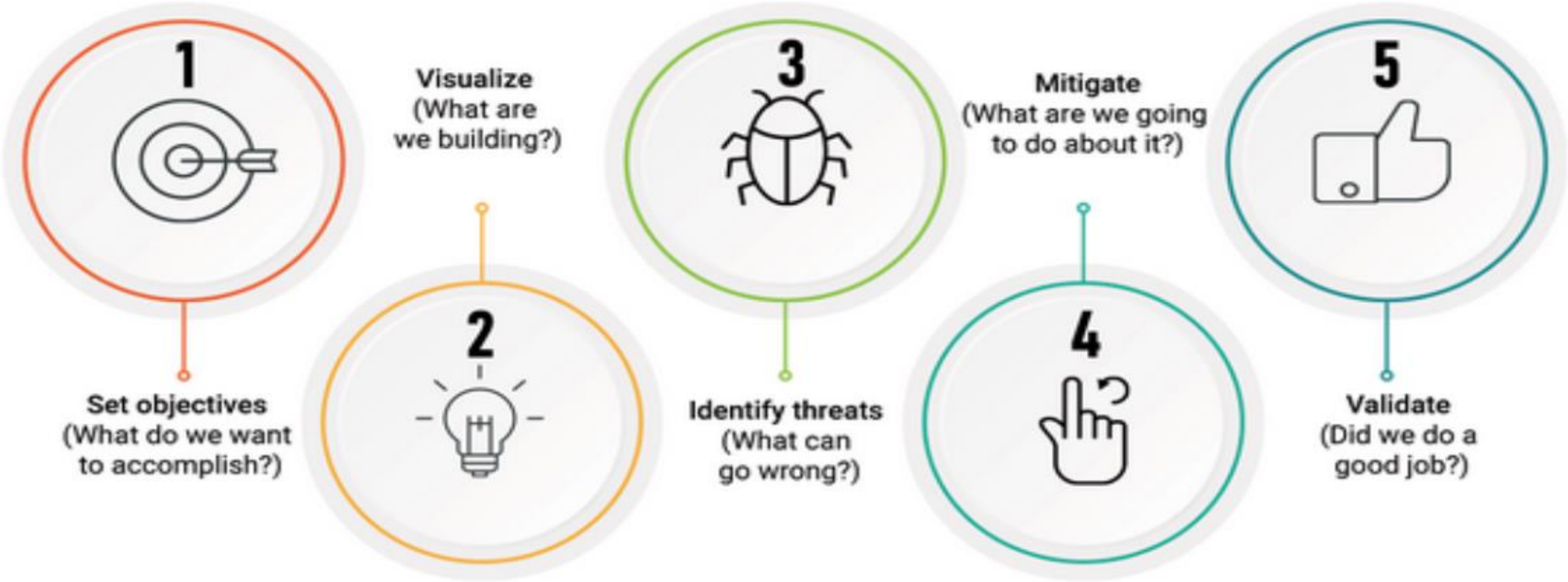
#ntk23

Neprebojna področja ???

THE 7 LAYERS OF CYBERSECURITY



5 KEY STEPS OF THREAT MODELING PROCESS



DREAD Methodology

DAMAGE	Impact of an Attack
REPRODUCIBILITY	How Easily the Attack can be Reproduced?
EXPLOITABILITY	How Easy it is to Launch the Attack
AFFECTED USERS	How Many Users will be Impacted
DISCOVERABILITY	How easily the vulnerability can be found


SIEM

Tudi meni kdaj postane vroče!

Description	Key	Type	Event Definition	Timestamp
Illuminate:Events:4;Logons from different countries in time window: polona - card(source_geo_country)=2.0	polona	Event	*63d7975934c7497f53fcec7f*	2023-03-21 20:57:15
Illuminate:Events:4;Logons from different countries in time window: polona - card(source_geo_country)=2.0	polona	Event	*63d7975934c7497f53fcec7f*	2023-03-21 16:57:15
Illuminate:Events:4;Logons from different countries in time window: polona - card(source_geo_country)=2.0	polona	Event	*63d7975934c7497f53fcec7f*	2023-03-21 12:57:15
Illuminate:Events:4;Logons from different countries in time window: polona - card(source_geo_country)=2.0	polona	Event	*63d7975934c7497f53fcec7f*	2023-03-21 08:57:15

ID
01GW1JR8HJDJA9DT3Y1BGFESR2

Priority
Normal

Timestamp
2023-03-21 08:57:15

Event Definition
63d7975934c7497f53fcec7f (Filter & Aggregation)

Aggregation time range
2023-03-20 08:57:15 — 2023-03-21 08:57:15

Event Key
polona

Additional Fields
- **user_name** polona

Group-By Fields
- **user_name** polona

Novi T2 IP rangi

Odgovori | Preišči to temo...

Novi T2 IP rangi

Napisal/-a **borutz** » 27. Mar 2023 ob 23:29

Pozdrav,

Opazil sem, da je t2 začel dodeljevati naročnikom nove sklope ip adres. Nekatere od teh pokaže kot da so iz Irana, zato imajo marsikateri uporabniki ki delajo od doma preko vpn v podjetja ki se grejo tudi country blocking velike probleme. Je bilo kje kakšno obvestilo, nameravajo te countrye "prekategorizirati", je še kak drug sklop teh naslovov za katere ne vemo?  Verjetno marsikomu tudi ki ni v podjetju ne dela kakšna stvar v sami Sloveniji zaradi tega ...blink..... 

Re: Novi T2 IP rangi

Napisal/-a **mikrohard** » 27. Mar 2023 ob 23:45

IP-ji se non-stop preprodajajo in sčasoma tudi geoip storitve posodobijo bazo. Dejansko lahko tudi sam takim storitvam javiš napako. Verjamem pa, da zna biti zoprno.

Pod kontrolo?

- Kje imamo kaj?
- A tudi diskovje imamo?
- A nismo to odklopili že lani?
- Kaj imamo odprto?
- Kaj sploh imamo?

- Inventory?

2023-09-25T12:54:19.283384

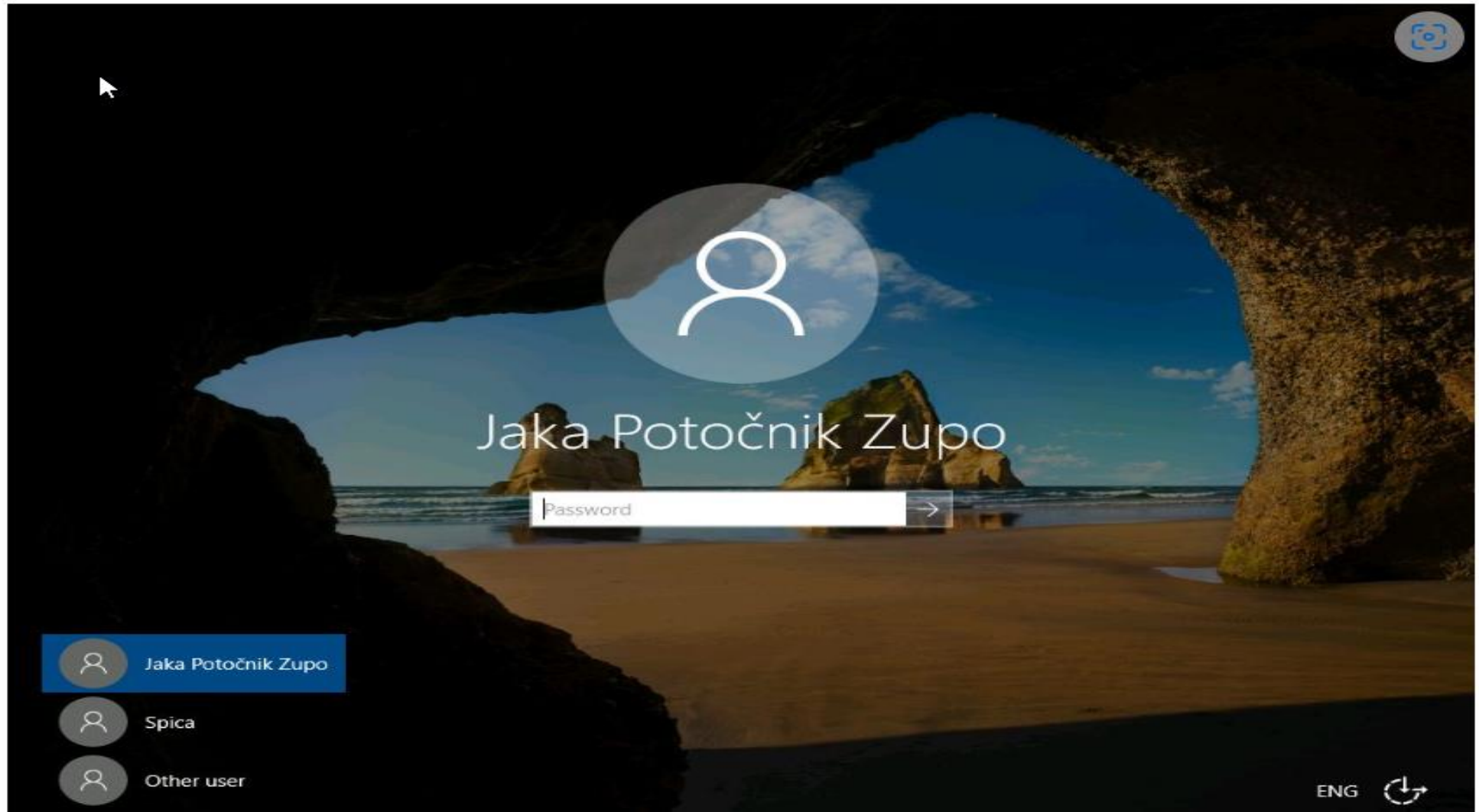
SSL Certificate

Issued By:
|- Common Name:
ZALSQL02.zaloker.local

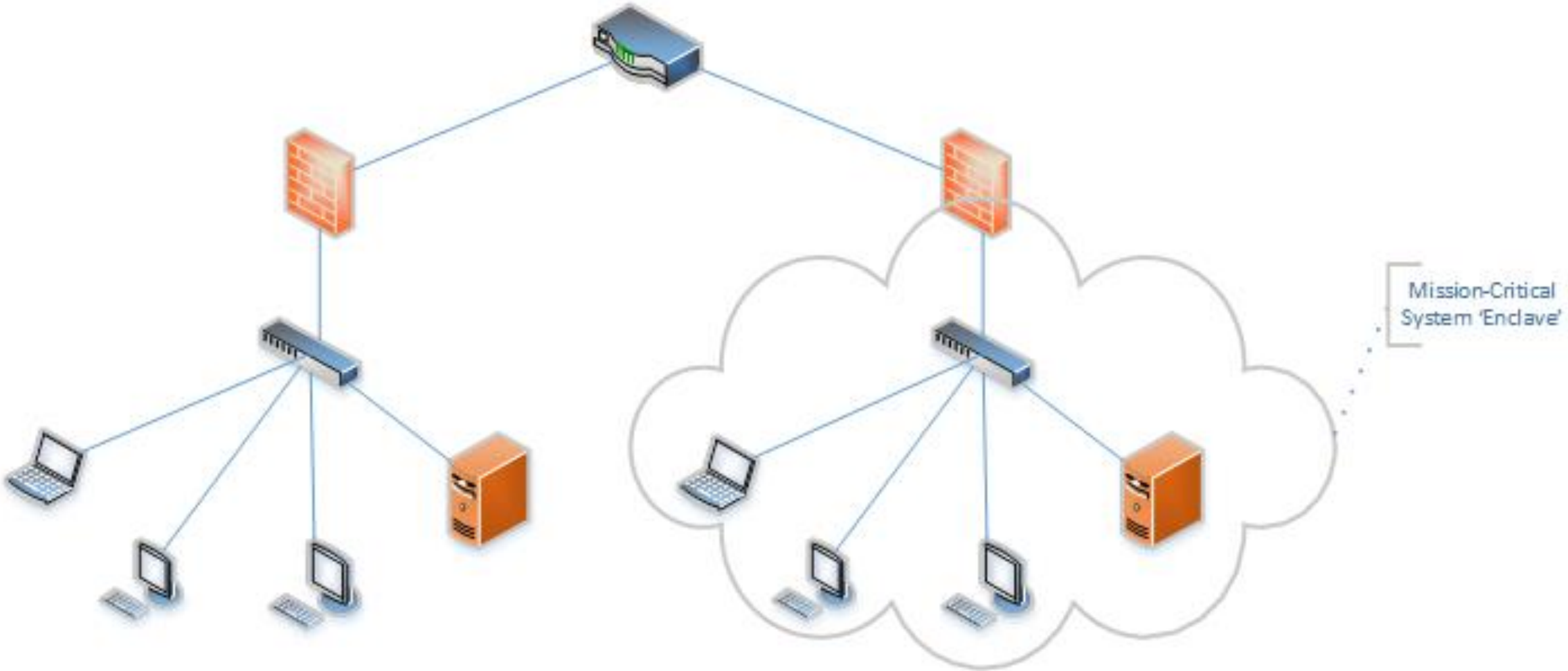
Issued To:
|- Common Name:
ZALSQL02.zaloker.local

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607)
  OS Build: 10.0.14393
  Target Name: ZALOKER
  NetBIOS Domain Name: ZALOKER
  NetBIOS Computer N...
```



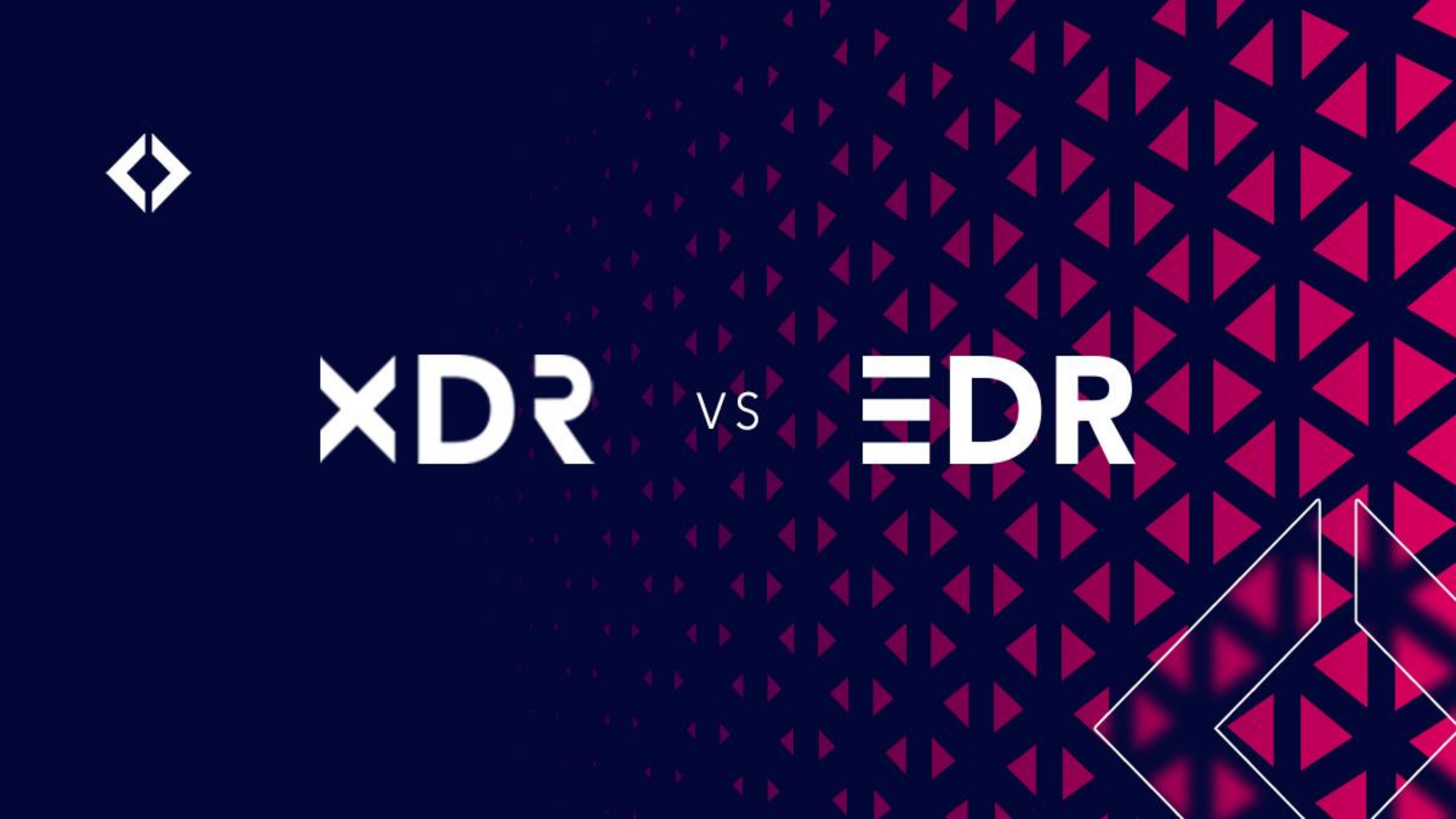
Omrežna segmentacija in izolacija




UNKNOWN

Preparing to configure Windows
Don't turn off your computer

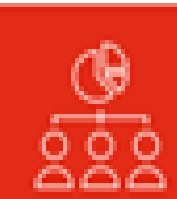
Your PC will restart several times


XDR
VS
EDR

Microsoft Security Defaults – A Step in the Right Direction, but Customers Should Do More

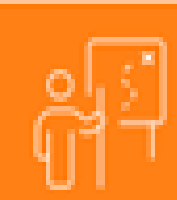
Redna testiranja!

Incident Response Plan Framework



1. Determine key stakeholders

2. Identify critical assets

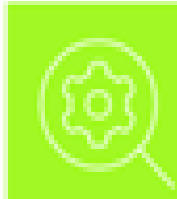


3. Run table-top exercises

4. Deploy protection tools

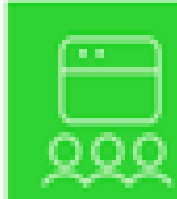
5. Ensure maximum visibility

6. Implement access control

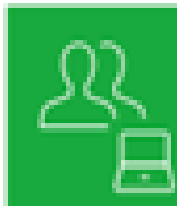


7. Invest in investigation tools

8. Establish response actions



9. Conduct awareness training



10. Hire a managed security service


Za ~~NTK~~/Viris Challenge coin!
10.10.2023

You reposted

Jeff Woolsey ☮
@WSV_GUY

PLEASE RT: IMPORTANT

We are 2 WEEKS away from End of Support for Windows Server 2012/2012R2 (on October 10, 2023) and we're receiving numerous questions about Active Directory Domain Controllers like upgrading & best practices.

This thread is for you.

5:34 PM · Sep 26, 2023 · **3,990** Views

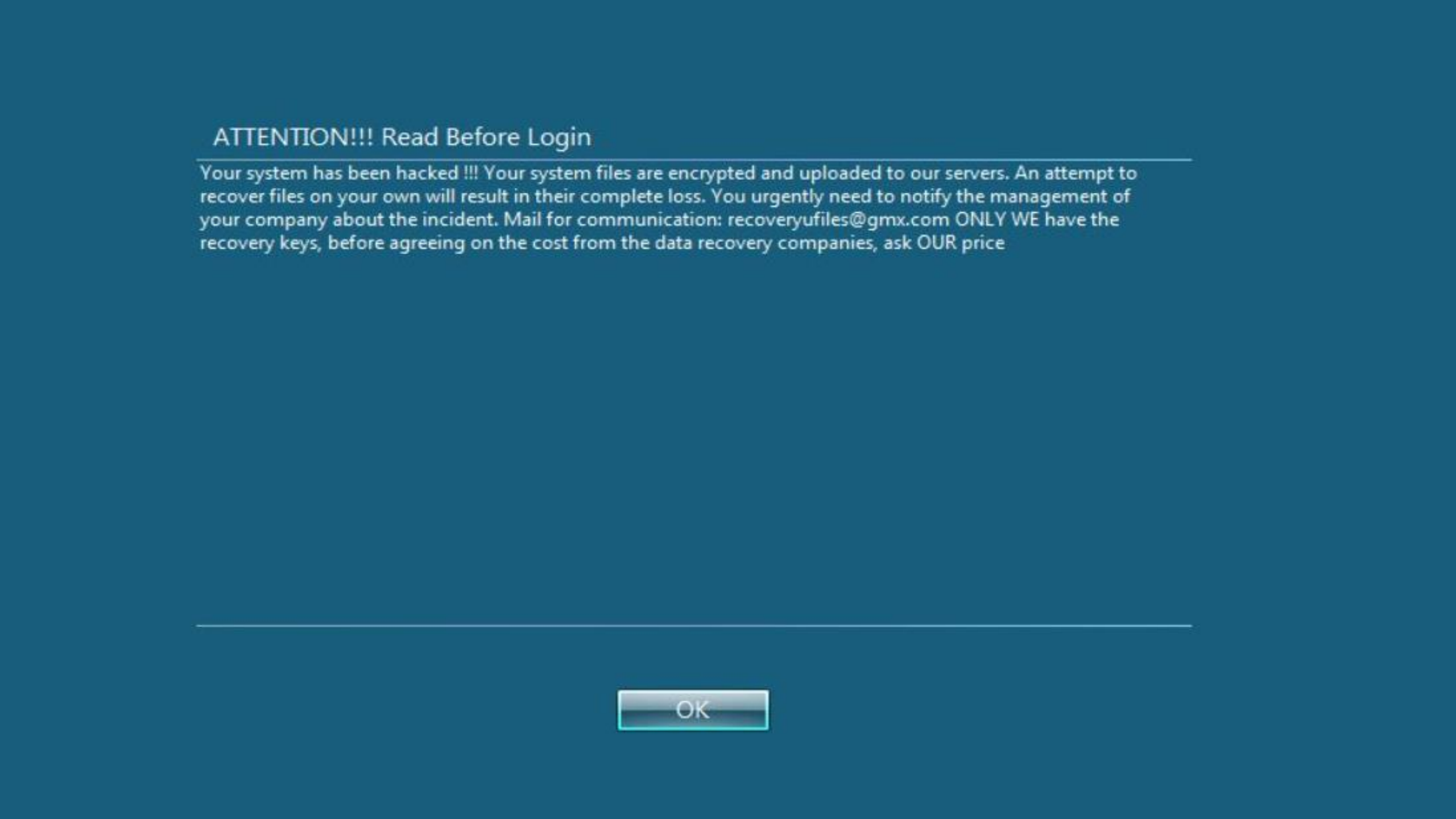
You reposted

Steve Thomas #M365 #Purview #MSIntune
@madvirtualizer

Starting in #Windows11, version 22H2 with KB5030310, Windows passwordless experience is a security policy that promotes a user experience without passwords on Microsoft Entra joined devices.

learn.microsoft.com
Windows passwordless experience - Windows Security
Learn how Windows passwordless experience enables your organization to move away from passwords.

7:49 PM · Sep 26, 2023 · **924** Views


ATTENTION!!! Read Before Login
Your system has been hacked !!! Your system files are encrypted and uploaded to our servers. An attempt to recover files on your own will result in their complete loss. You urgently need to notify the management of your company about the incident. Mail for communication: recoveryufiles@gmx.com ONLY WE have the recovery keys, before agreeing on the cost from the data recovery companies, ask OUR price
OK

```
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Sep 26 20:28:48 2023
  ..                                  D        0  Thu Jul  6 22:04:25 2023
  JrzKqrUw.exe                        A    56320  Sat Sep  2 12:25:42 2023
  lCGlouuf.exe                        A        0  Fri Aug 25 19:30:31 2023
  TeHwYoBI.exe                        A        0  Tue Sep 19 07:55:47 2023
  eQtuGONg.exe                        A    56320  Sat Sep  2 12:28:49 2023
  AvFFaIQj.exe                        A        0  Fri Sep  1 05:03:18 2023
  WdKJSATD.exe                        A    56320  Tue Sep 26 14:40:53 2023
  WZpsAIst.exe                        A        0  Sat Aug  5 03:23:17 2023
  ._.DS_Store                        AH     4096  Fri Jul  7 00:51:47 2023
  RBLQDwoR.exe                        A        0  Tue Sep 19 07:57:34 2023
  GDmjxlMt.exe                        A        0  Fri Sep  1 05:05:04 2023
  nlfsYDkE.exe                        A        0  Fri Aug 25 19:28:44 2023
  ghmYtMSi.exe                        A        0  Thu Sep  7 19:48:23 2023
  BgEPMOFH.exe                        A        0  Thu Sep  7 19:50:12 2023
  NHJRPWFb.exe                        A        0  Sat Aug  5 03:25:03 2023
  .DS_Store                          AH     6148  Fri Jul  7 00:52:04 2023
  PdRViLqd.exe                        A        0  Fri Sep 15 07:20:56 2023

                15054340 blocks of size 1024. 9671076 blocks available
smb: \>
```

Open **Ports**

19	21	22	23	25	53	81	110	123	135	143
443	445	465	993	995	1024	1029	1099	1153	1177	1200
1234	1311	1400	1433	1471	1521	1599	1604	1723	1741	1800
1801	1830	1883	1900	1911	1925	1935	1962	2000	2002	2006
2008	2018	2022	2053	2067	2068	2081	2082	2086	2087	2095
2121	2154	2181	2201	2202	2222	2323	2332	2345	2351	2375
2379	2382	2404	2443	2455	2480	2550	2569	2628	2761	2762
3000	3001	3050	3054	3060	3070	3076	3081	3085	3092	3103
3104	3108	3110	3117	3128	3200	3260	3268	3269	3299	3301
3306	3310	3352	3388	3389	3404	3460	3541	3542	3551	3560
3567	3568	3689	3749	3792	4000	4022	4040	4063	4064	4117

Telekom Slovenije d.d.

Slovenia, Lendava

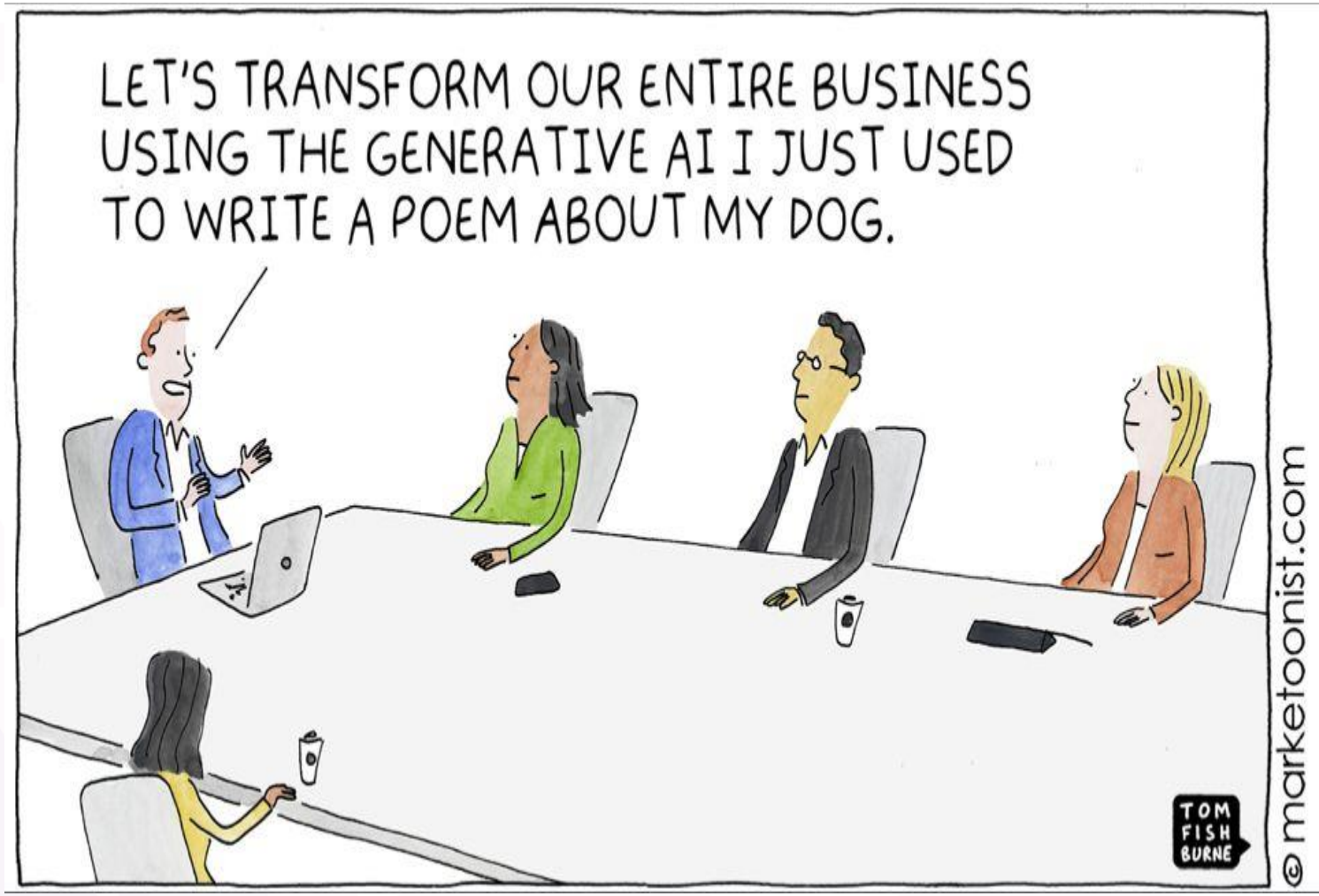
compromised

```
MAC Address: 00:27:22:23:49:8F
Alternate IP Address: 169.254.73.143
Alternate MAC Address: 00:27:22:22:49:8F
Hostname: HACKED-ROUTER-HELP-SOS-VULN-EDB-39701
Product: LAP
Version: XM.ar7240.v5.3.7782.110114.1442
```

Biti up2date!

UI, AI, ChatGPT

- AI je trenutno vroč
- Uporaben
- Pameten
- Kaj pa slabosti?



Nevarnosti

Security

Hackers are increasingly using ChatGPT lures to spread malware on Facebook

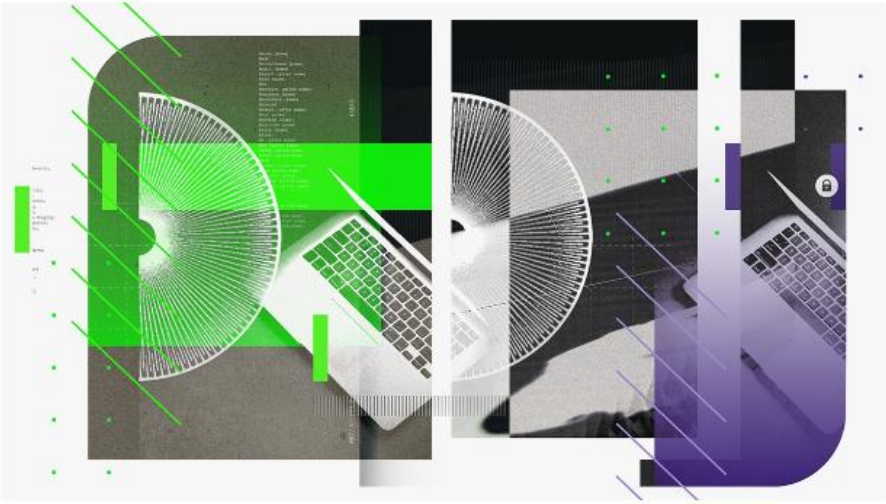
That's according to Facebook's parent company Meta, which said in a report out Wednesday that malware posing as ChatGPT was on the rise across its platforms. The company said that since March 2023, its security teams have uncovered 10 malware families using ChatGPT (and similar themes) to deliver malicious software to users' devices.

Meta says that attackers distributing the DuckTail malware have increasingly turned to these AI-themed lures in an attempt to compromise businesses with access to Facebook ad accounts. DuckTail, which has targeted Facebook users since 2021, steals browser cookies and hijacks logged-in Facebook sessions to steal information from the victim's Facebook account, including account information, location data and two-factor authentication codes. The malware also allows the threat actor to hijack any Facebook Business account that the victim has access to.

The New Risks ChatGPT Poses to Cybersecurity

by Jim Chilton

April 21, 2023



Skizzomat

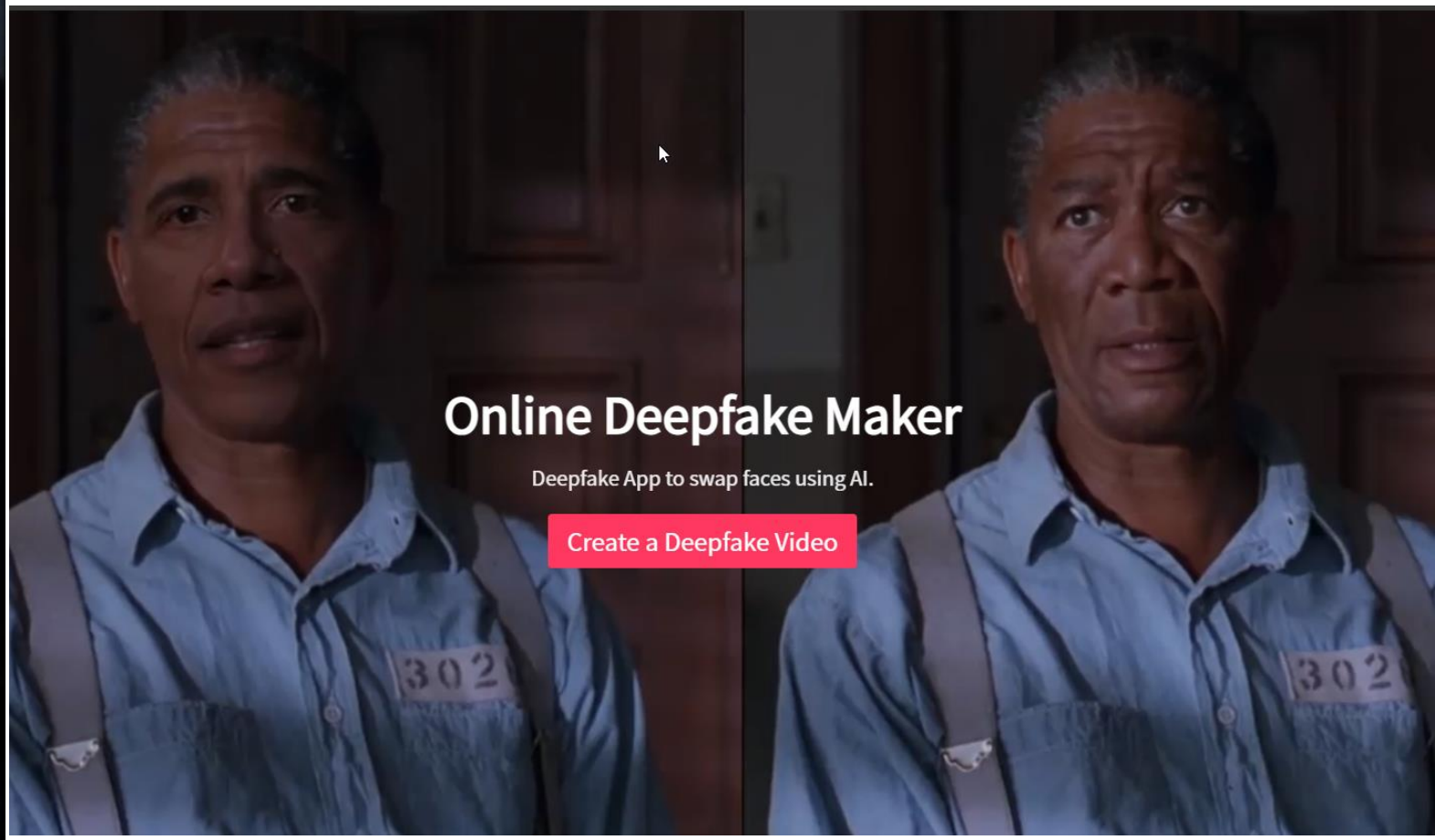
Summary. The FBI's 2021 Internet Crime Report found that phishing is the most common IT threat in America. From a hacker's perspective, ChatGPT is a game changer, affording hackers from all over the globe a near fluency in English to bolster their phishing campaigns.... **more**

https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecurity

Izzivi

- AI phishing
  - Napadalci uporabljajo za napredne in realistične phishing e-maile
  - Taktična uporaba za kreiranje dezinformacij in teorij zarot
- Pisanje škodljive kode
- Zbiranje informacij in graditev velikih baz podatkov
- Povečanja površine napada
  - Mogoče zbira osebne podatke iz sporočil ali datotek
- Napad na ljudi
  - Pretveza za kakšno škodljivo kodo, ki se pretvarja, da je ChatGPT aplikacija


GENERATED BY A.I.


Online Deepfake Maker
Deepfake App to swap faces using AI.
Create a Deepfake Video
302
302

PRIVACY FOCUSED • CRYPTO PAYMENTS • NO LIMITS

GPT Alternative For BlackHat

Get Started →

Using AI for extracting Usernames, Emails, Phone Numbers, and Personal Names from large datasets

Extracting relevant information from large blobs of text, such as text files, PDFs, Excel spreadsheets, JSON files, can be a time-consuming and frustrating task. Everyone in OSINT will most likely acknowledge this since processing and exploiting the collected data in an OSINT investigation is one of most time consuming tasks on average.

Within Open-Source Intelligence (OSINT) we very often collect large amounts of data in the form of text. During investigations there often is a need to extract valuable information from the text that can be used to pivot or help answer research questions.

Not every OSINT investigator feels comfortable extracting usernames, emails, phone numbers and personal names from data. They may have collected the data in various formats which make them think they need specialised software or specific knowledge to extract these key data points.

One could think of crafting Python or Bash scripts alongside with Regular Expression to iterate over your collected data and extract what you need. And yes this is a way to achieve these goals.

[P2O Vancouver 2023] SharePoint Pre-Auth RCE chain (CVE-2023–29357 & CVE-2023–24955)

September 25, 2023 · 18 min · Nguyễn Tiến Giang (Jang)

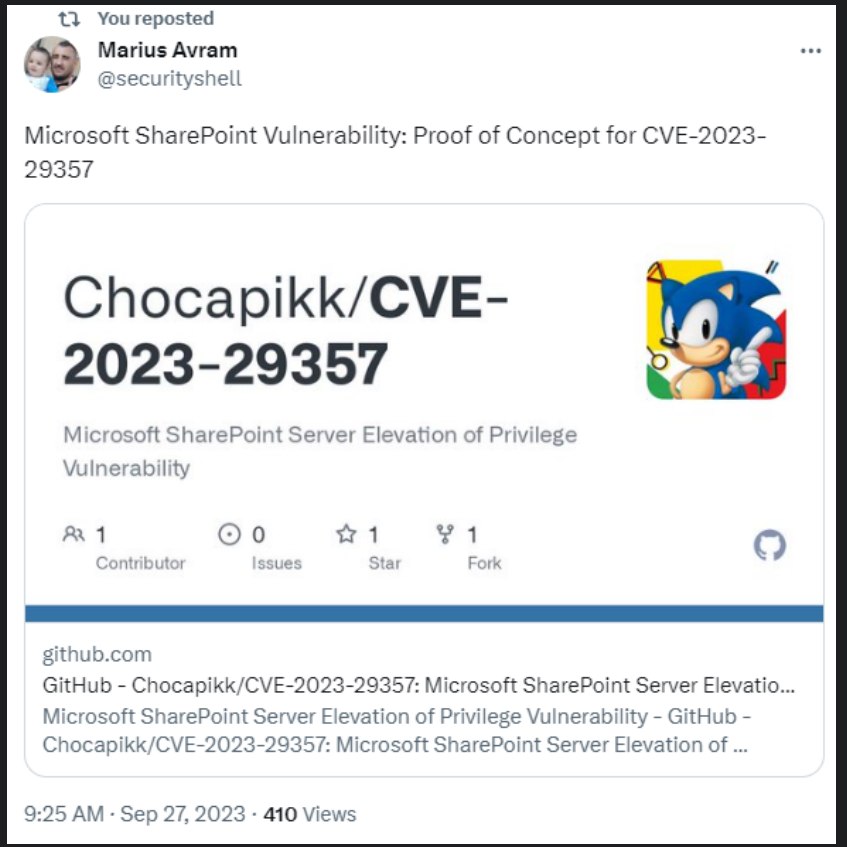
▶ Table of Contents

Brief

I may have achieved successful exploitation of a SharePoint target during Pwn2Own Vancouver 2023. While the live demonstration lasted only approximately 30 seconds, it is noteworthy that the process of discovering and crafting the exploit chain consumed nearly a year of meticulous effort and research to complete the full exploit chain.

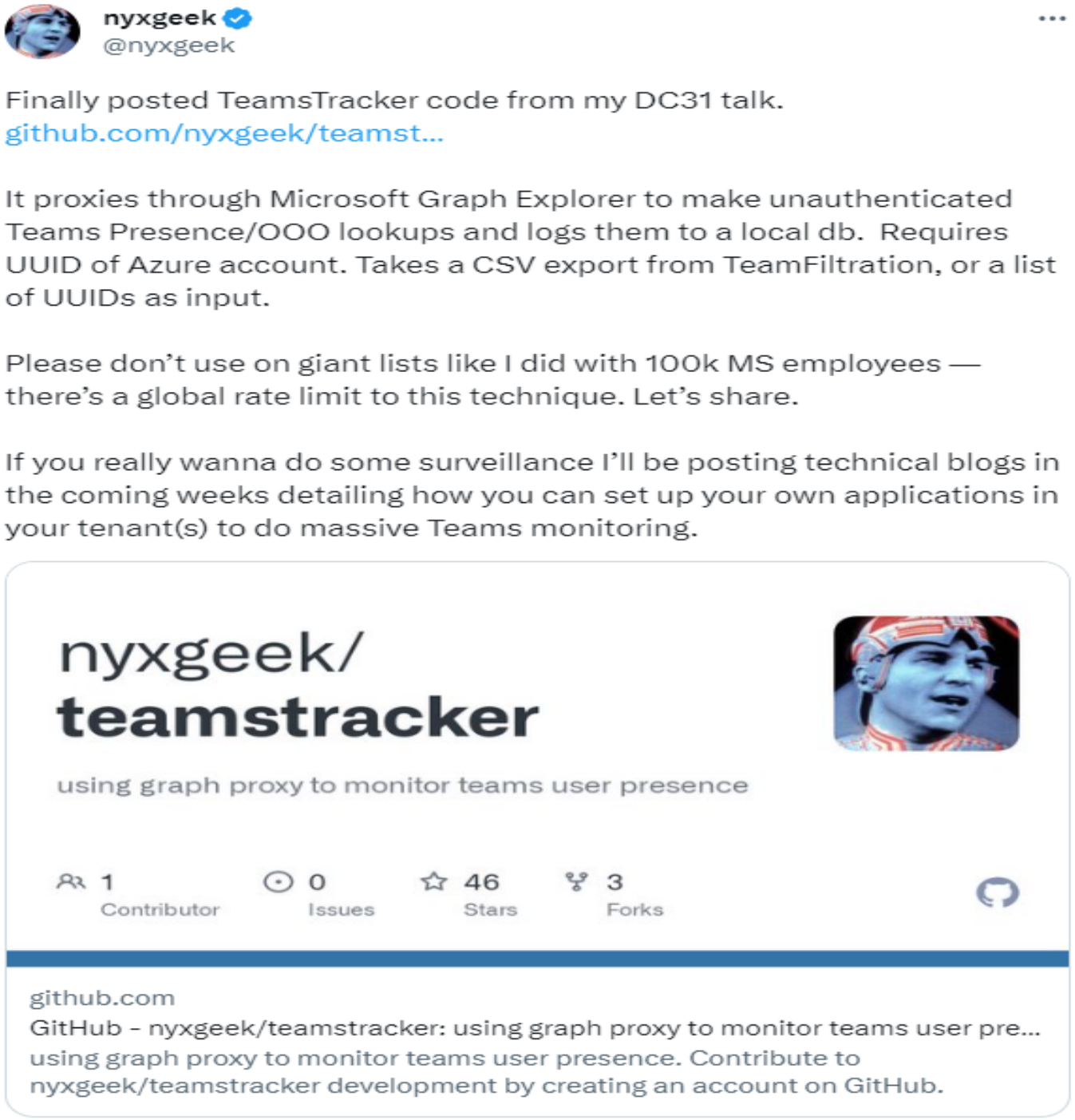
This exploit chain leverages two vulnerabilities to achieve pre-auth remote code execution (RCE) on the SharePoint server:

1. Authentication Bypass – An unauthenticated attacker can impersonate as any SharePoint user by spoofing valid JSON Web Tokens (JWTs), using the `none` signing algorithm to subvert signature validation checks when verifying JWT tokens used for OAuth authentication. This vulnerability has been found right after I started this project for two days.
2. Code Injection – A SharePoint user with `Sharepoint Owners` permission can inject arbitrary code by replacing `/BusinessDataMetadataCatalog/BDCMetadata.bdcm` file in the web root directory to cause compilation of the injected code into an assembly that is subsequently executed by SharePoint. This vulnerability was found on Feb 2022.



DEF CON letos

- No auth status za vse uporabnike clouda
- Fix v manj kot dnevu
- Kdo ima to prav nastavljeno?

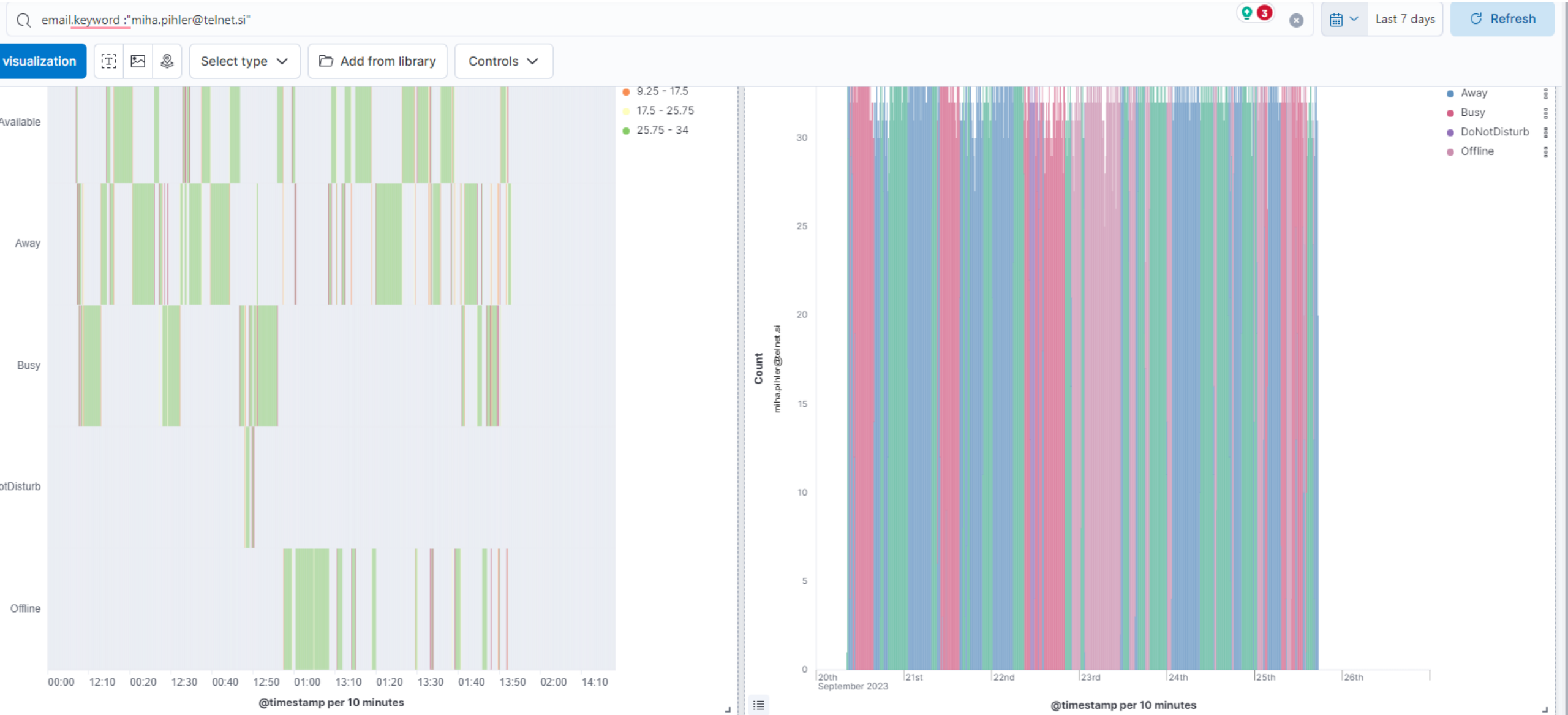


miha.pihler@telnet.si

Get information

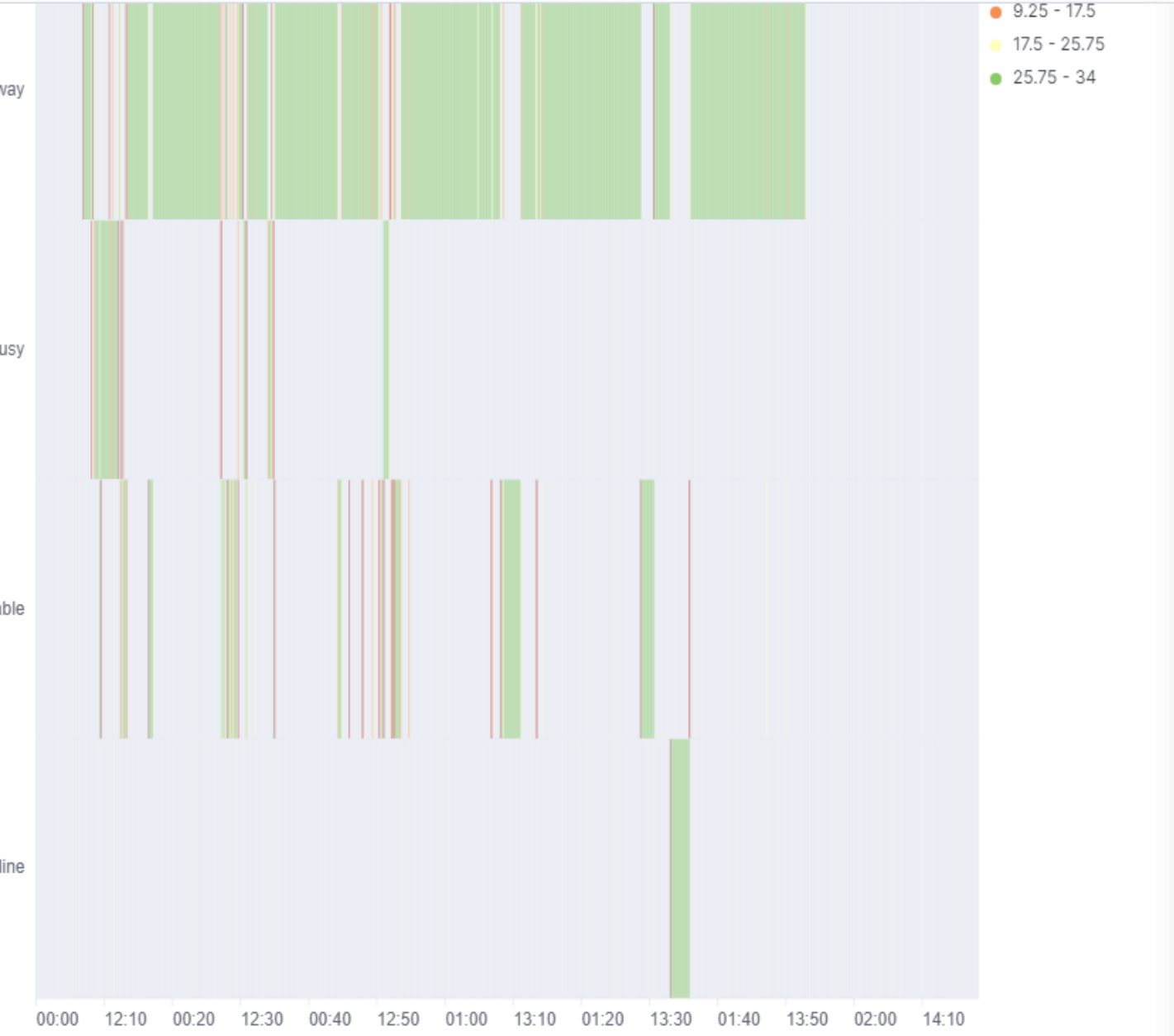
Property	Value
Default domain	mikeji.onmicrosoft.com
Tenant name	mikeji.onmicrosoft.com
Tenant brand	Mikeji d.o.o.
Tenant id	26ccaba3-4ded-4b54-9a38-17c078a69449
Tenant region	EU
Seamless single sign-on (SSSO)	enabled
Uses Azure AD Connect cloud sync	N/A
Certificate-based authentication (CBA)	N/A
User name	miha.pihler@telnet.si
User id	0af1f3f8-534a-4c9f-8dcd-1d28d1d4e6b5
Teams status	Busy
Verified domains	10

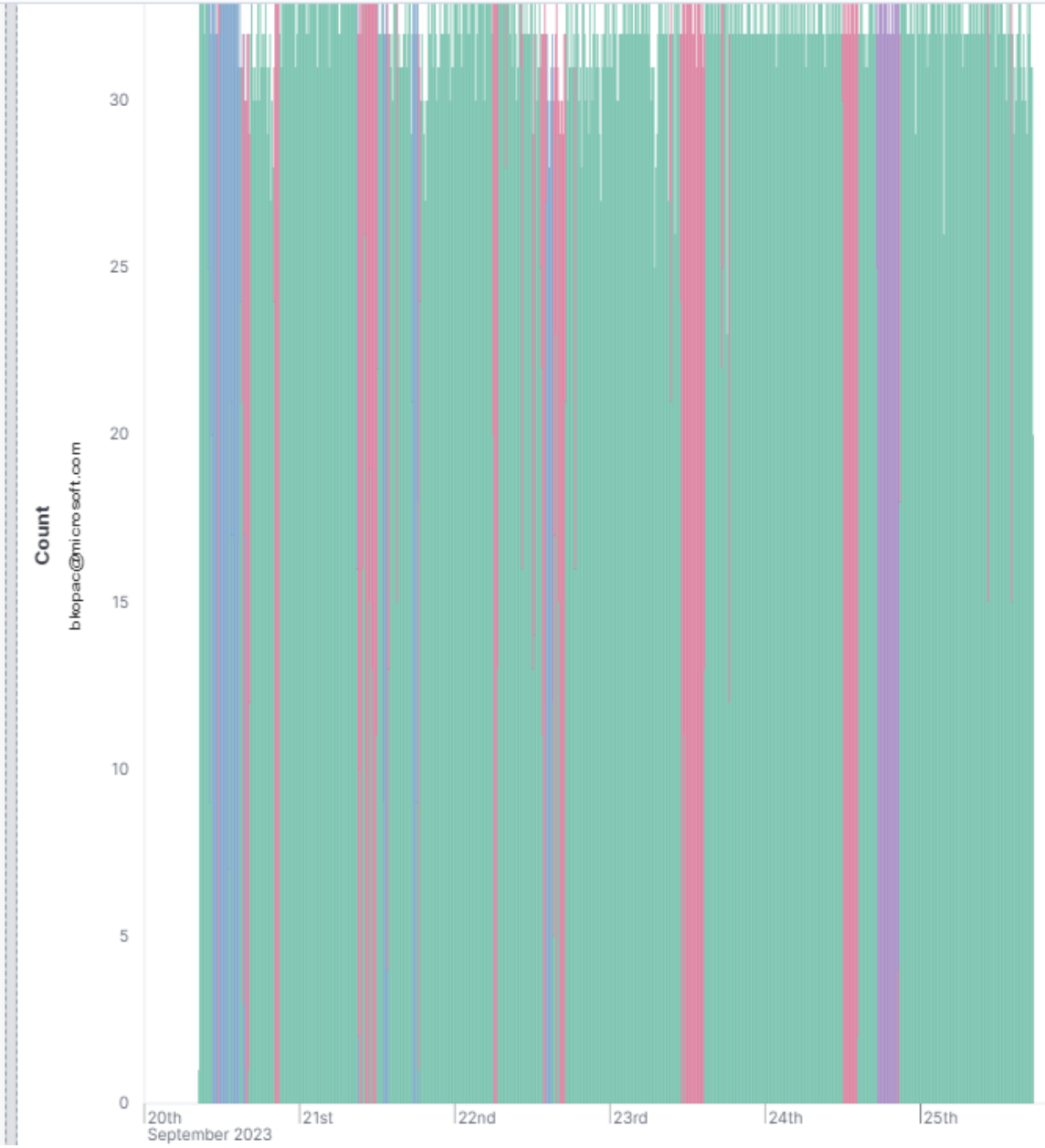
Naredimo nekaj uporabnega



email.keyword :"bkopac@microsoft.com"

visualization | Select type | Add from library | Controls



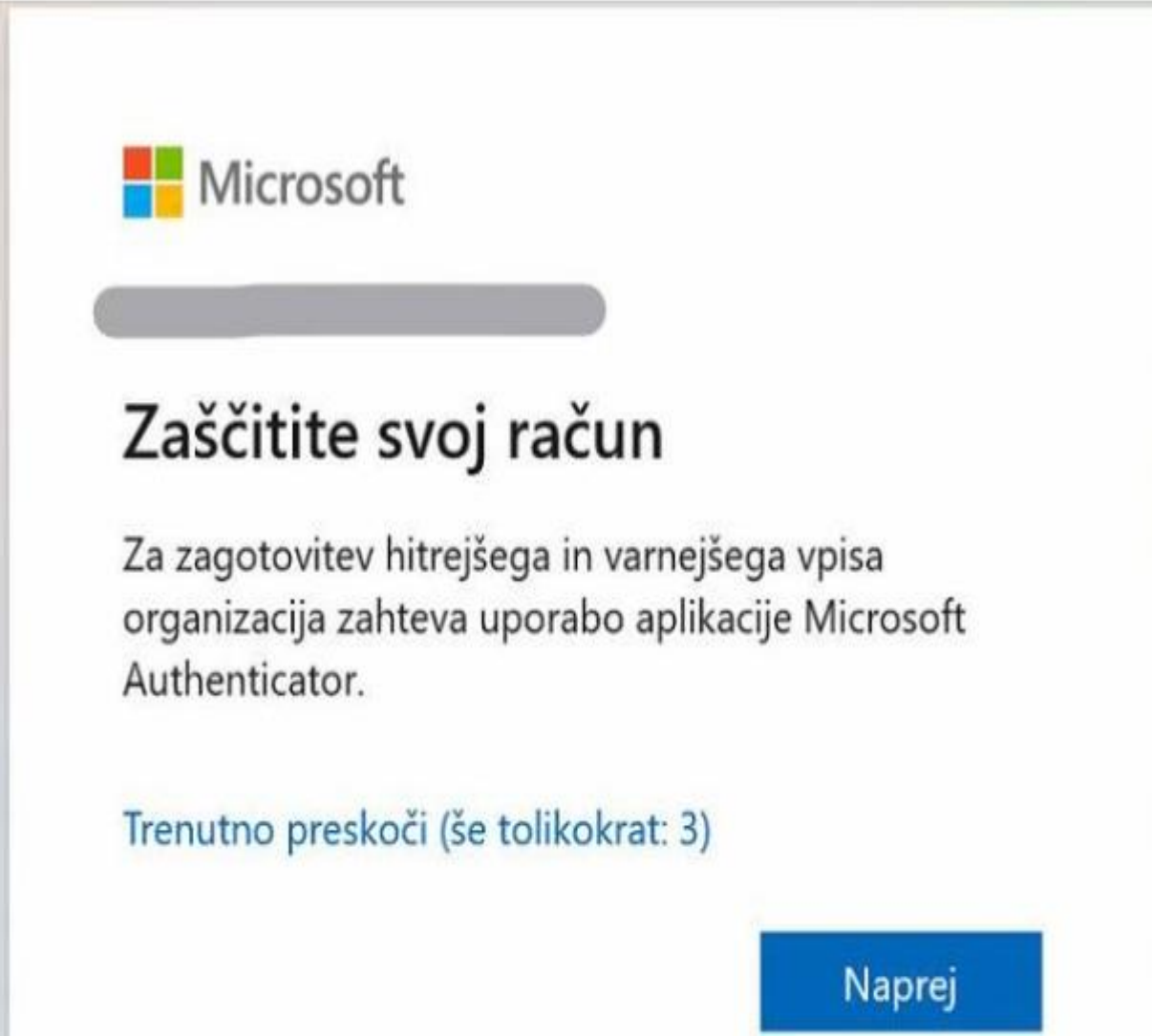


Gesla


NEWGROUNDS
deviantART
friendste
YouTube
facebook
twitter
wasab
Club
flickr
FARK

Andrej Pico Pirman
Top contributor · September 19 at 4:14 PM ·

Faaak, kot Alice v čudežni deželi se počutim, ko spet in spet iščem fakin' Security Defaults v Azure, ki so spet na drugem mestu, vidim, da so izklopljeni...pa MS Avtentikator je tudi na Disabled... ampak fakin' faker pofakan spet random teži uporabnikom... fakin' čist nč več ne zastopim, pe če sem že kdaj vmes mal zastopu, sem pozabu, ker mi res, ampak fakin' RES ni nč jasno! Kje in kaj moram še izklopit, da bo nehal težit?



Top comments

Miha Pihler Admin Group expert +1
Morda zato, ker je Microsoft napovedal, da bo zahteval Autheticator.
We're enabling a stronger form of multifactor authentication beginning September 15, 2023 ....
Morda je pa namesto, da narediš disable bolje, da narediš enroll 😉.
21
1w Like Reply Share

Luka Cajnkar
Miha Pihler amen. 😀
1w Like Reply Share

Andrej Pico Pirman Author Top contributor
Miha Pihler, jp, to je to ocitno. Ampak po moji logiki bi pricakoval, da bodo vklopili to nastavitev, ne pa, da je izklopljena in forsirana na nivoju izven moje kontrole.
6d Like Reply Share

Andrej Gorenc
Razumem tezavo. Ni problem kaj bi mi vklopili. Bolj je dejstvo da morajo uporabniki najprej sprejeti za svoje nov nacin. Je pa neizbezno.
Good luck 🍀
1w Like Reply Share

Miha Pihler Admin Group expert +1
Andrej Gorenc Če so sprejeli da morajo imeti bančno aplikacijo, da potrdijo plačilo vsakič ko kaj kupujo na netu ... 😀 ... bo tole mali kašelj 😀. A ne 😀.
2
6d Like Reply Share

Hash!

```
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 192.168.10.11 for name hackingloop
[SMB] NTLMv2-SSP Client   : 192.168.10.11
[SMB] NTLMv2-SSP Username : braveheart-PC\braveheart
[SMB] NTLMv2-SSP Hash     : braveheart::braveheart-PC:1122334455667788:8B16D628D
5DB625453295E98C807BC98:0101000000000000C2EB23861421D501FC4BF44DB133F2B600000000
02000A0053004D0042003100320001000A0053004D0042003100320004000A0053004D00420031003
32000300 0A0053004D0042003100320005000A0053004D0042003100320008003000300000000000
0000010000000020000 0B8717060 5484E044883D16E75676402607BE4D02D722B71E052756590B4D
1B560A0010000000000000000000000000000090020006300690066007300 2F0068006100
63006B0069006E0067006C006F006F00700000000000000000000
[SMB] Requested Share     : \\HACKINGLOOP\IPC$
[*] [LLMNR]  Poisoned answer sent to 192.168.10.11 for name hackingloop
[*] Skipping previously captured hash for braveheart-PC\braveheart
[SMB] Requested Share     : \\HACKINGLOOP\IPC$
[*] [LLMNR]  Poisoned answer sent to 192.168.10.6 for name wpad
```

https://www.hackingloops.com/wp-content/uploads/2019/06/hash-captured.png

2020

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tm years	100tn years	7qd years

HIVE SYSTEMS

> Learn how we made this table at hivesystems.io/password

ABBA

I HAVE A DREAM


```
[*] [LLMNR]  Poisoned answer sent to 192.168.100.101 for name fielshare
[SMB] NTLMv2-SSP Client   : 192.168.100.101
[SMB] NTLMv2-SSP Username : AIUK\user2
[SMB] NTLMv2-SSP Hash     : user2::AIUK:1122334455667788:B48729A91322323BD4283DD8C4A4F267:0101000
0000000009F8506E2C4BCD101F5B6DBEBD68390A900000000002000A0073006D0062003100320001001400530045005200
560045005200320030003000380004001600730060062003100320020E006C006F00630061006C0003002C00530045005
200560045005200320030003000380002E0073006D0062003100320020E006C006F00630061006C000500160073006D0062
00310032002E006C006F00630061006C0008003000300000000000000000000000000020000043BD1E3E6C201D3D989B389
B5952622F2CDF272A83DDD0084F2145B78F2119930A001000000000000000000000000000000000000000009001C0063006900
660073002F006600690065006C007300680061007200650000000000000000
[SMB] Requested Share     : \\FIELSHARE\IPC$
[*] [LLMNR]  Poisoned answer sent to 192.168.100.101 for name fielshare
[*] Skipping previously captured hash for AIUK\user2
[SMB] Requested Share     : \\FIELSHARE\IPC$
```

```
[+] Listening for events ...
[*] [MDNS] Poisoned answer sent to 192.168.27.1    for name infinitelogins.local
[*] [LLMNR]  Poisoned answer sent to 192.168.27.1 for name infinitelogins
[*] [MDNS] Poisoned answer sent to 192.168.27.1    for name infinitelogins.local
[*] [MDNS] Poisoned answer sent to 192.168.27.1    for name infinitelogins.local
[*] [LLMNR]  Poisoned answer sent to 192.168.27.1 for name infinitelogins
[*] [MDNS] Poisoned answer sent to 192.168.27.1    for name infinitelogins.local
[SMB] NTLMv2-SSP Client   : 192.168.
[SMB] NTLMv2-SSP Username : DESKTOP-NGRA9AJ\Harley
[SMB] NTLMv2-SSP Hash     : Harley::DESKTOP-NGRA9AJ:
0049004E002D005000520048003400390032005200510041004600
0000000000000000000000000000090026006300690066007300 2F
[*] [MDNS] Poisoned answer sent to 192.168.27.1    for name infinitelogins.local
[*] [LLMNR]  Poisoned answer sent to 192.168.27.1 for name infinitelogins
```

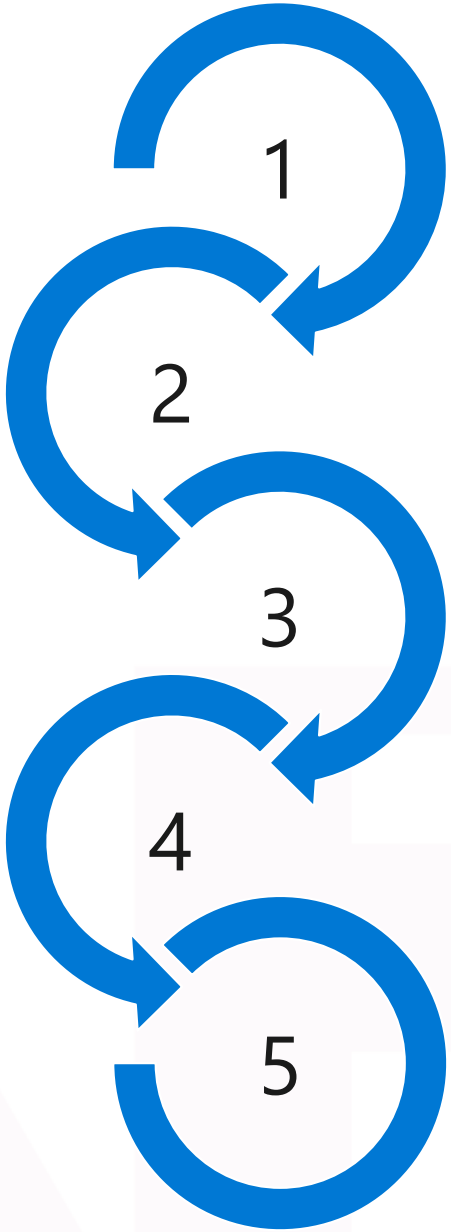
```
[+] Listening for events...
[SMBv2] NTLMv2-SSP Client   : 10.0.2.9
[SMBv2] NTLMv2-SSP Username : user-PC\user
[SMBv2] NTLMv2-SSP Hash     : user::user-PC:7f46c1e57e7e802f:BF3050D9AB89C7E37CE633D3F32381A8:01010
000000000000C0653150DE09D2013E26C02F535CAE9300000000020008005300 4D0042003300010001E00570049004E002D00
500052004800340039003200520051004100460056000400140053004D0042003300 2E006C006F00630061006C000300340
0570049004E002D00500052004800340039003200520051004100460056002E0053004D00420033002E006C006F00630061
006C000500140053004D00420033002E006C006F00630061006C000700800C0653150DE09D2010600040002000000080003
00030000000000000000100000000020000 06BFB9F83143C040E0B997605A5E0E1085042A6BCF2A78ACED01E37A5EC9197C7
0A0010000000000000000000000000000000000000009001A0063006900660073002F00310030002E0030002E0032002E00350
0000000000000000000000000
[*] [LLMNR]  Poisoned answer sent to 10.0.2.9 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.9 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.9 for name wpad
Challenge 2: 01cd445c3c5e6dec
Challenge 2: 01cd445c3c5e6dec
[*] [LLMNR]  Poisoned answer sent to 10.0.2.9 for name wpad
Challenge 2: 32d768bbe23eb829
Challenge 2: 32d768bbe23eb829
[*] [LLMNR]  Poisoned answer sent to 10.0.2.9 for name wpad
```

Hashcatcher

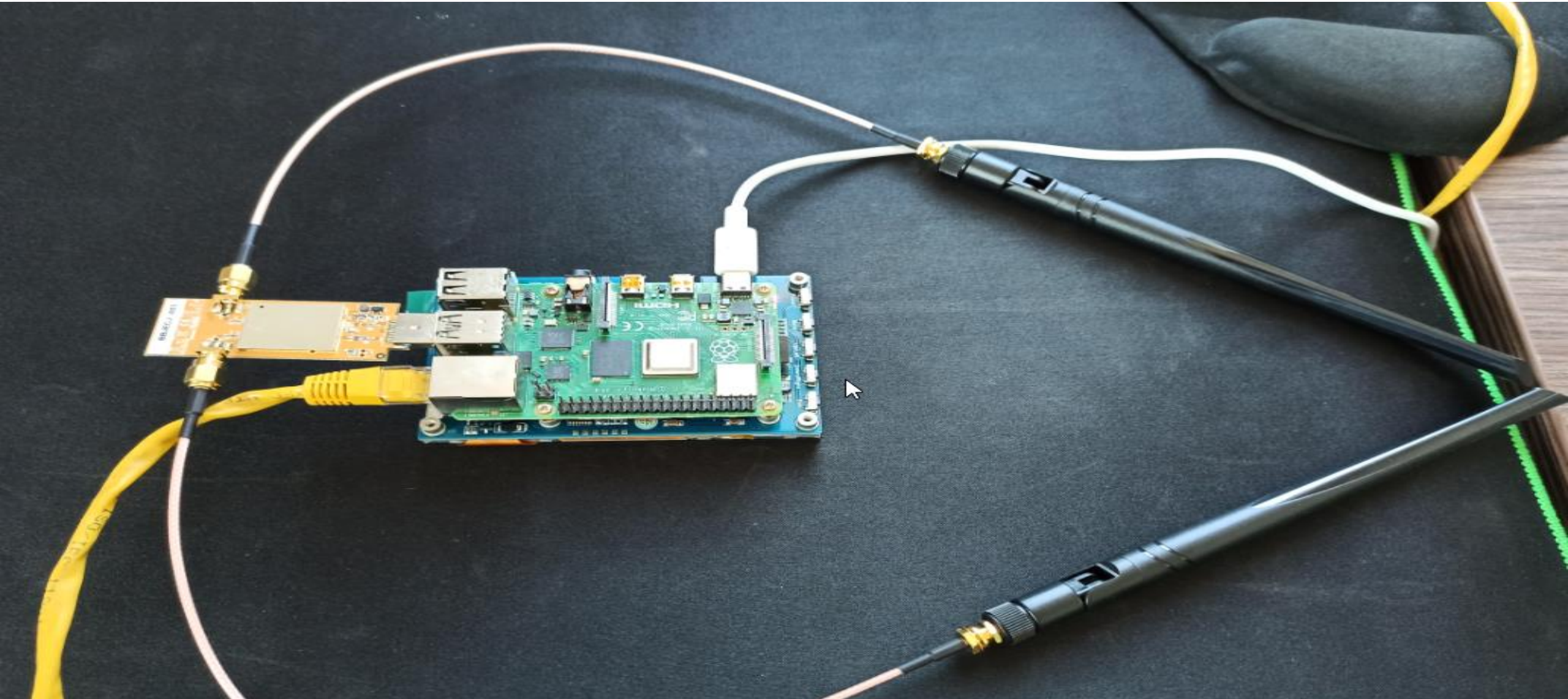
- 1 Responder
- 1 Hostpad
- 1 Dnsmasq
- 1 Dhcpd
- 1 Hashtopolis
- X Hashcat
- 1 Raspberry PI
- 1 Alfa WiFI card

Workflow

- Nastavi nekaj najpogostejših imen točk
- Uporabi Mana napad (glej WiFi probe pakete)
- Ko se nekdo poveže, mu nastavi nastavitve
- Porini mu wpad.dat za proxy nastavitve
- Ko nekaj zahteva - jok brate moraš se avtencirat
- Ko se poskuša avtenticirat – dobiš hashe
- Zmaga odvisna od kvalitete gesla!

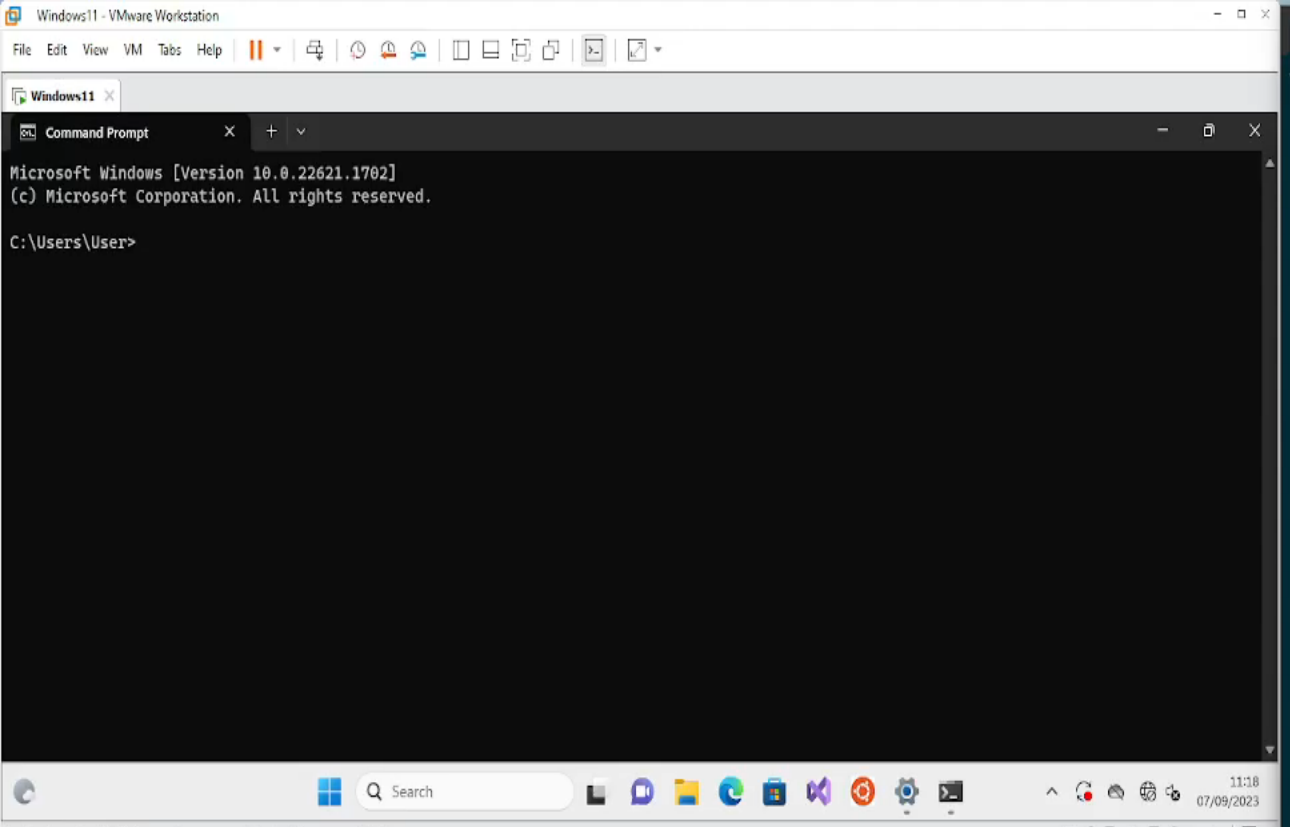


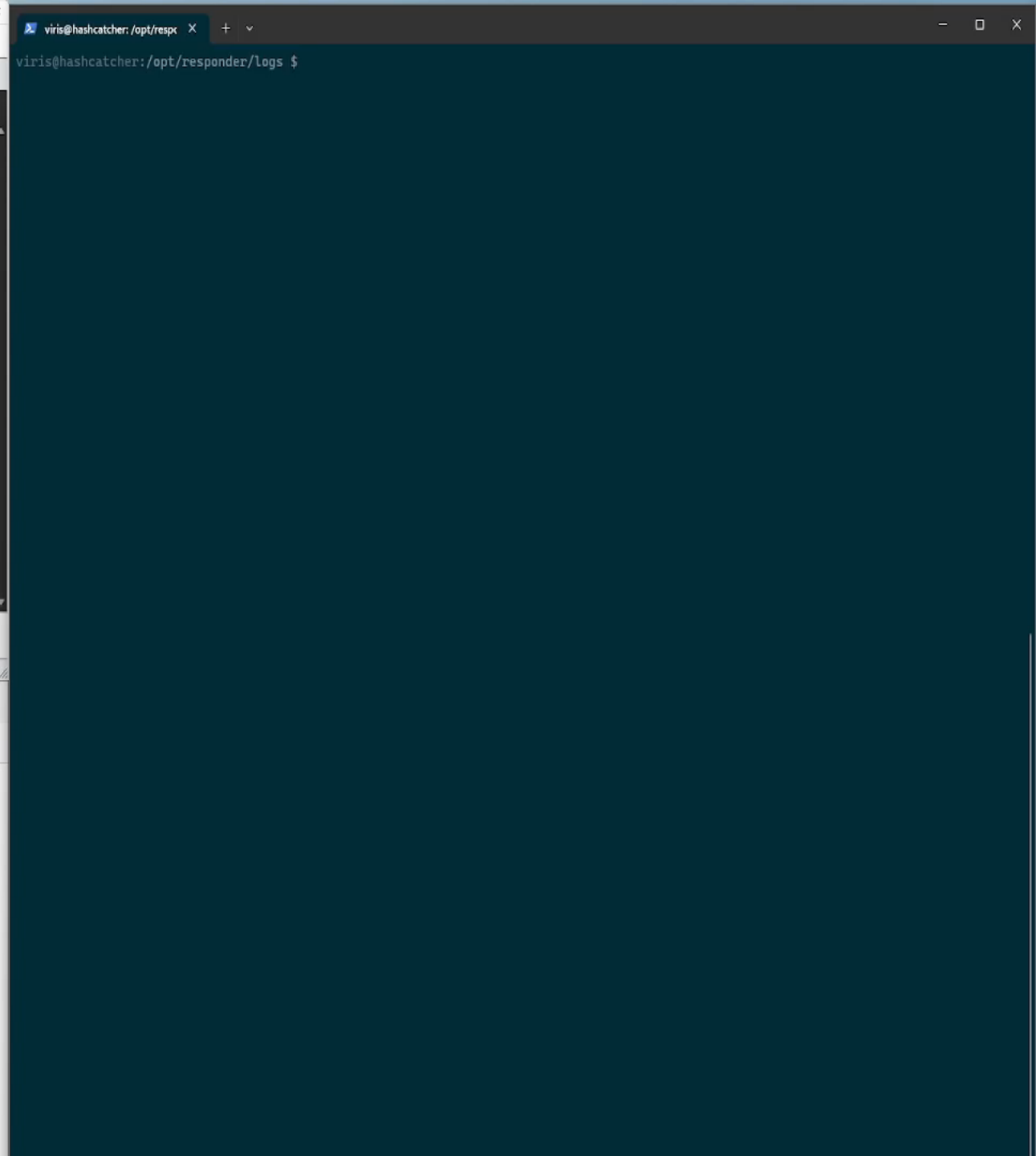
Prototip

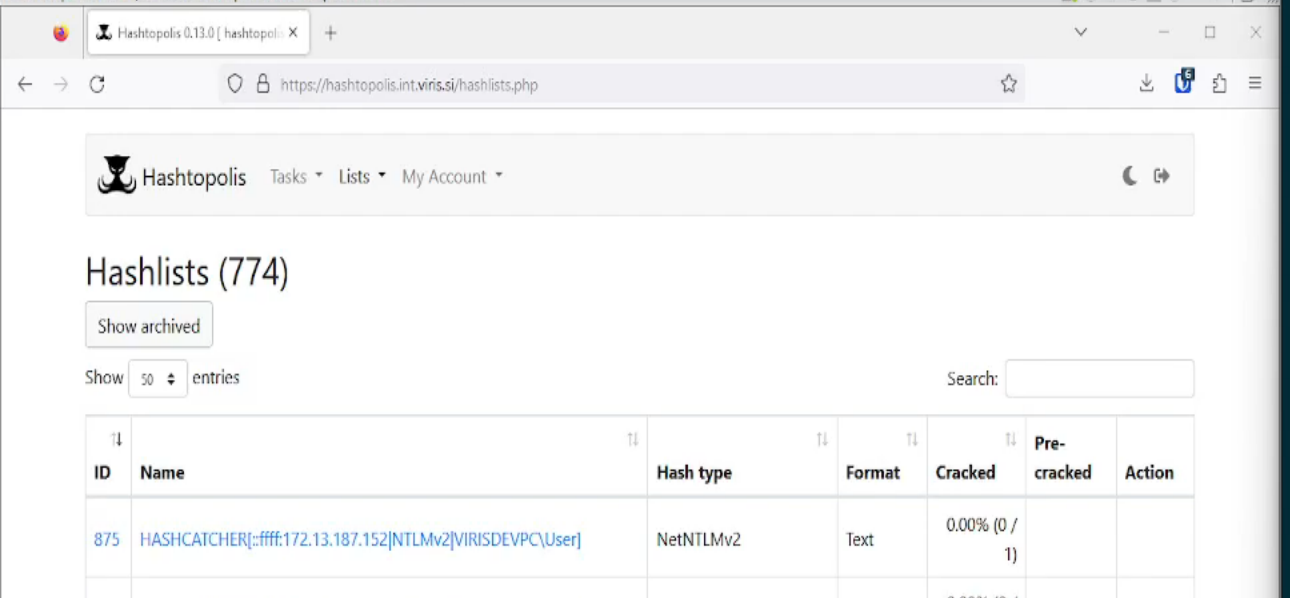


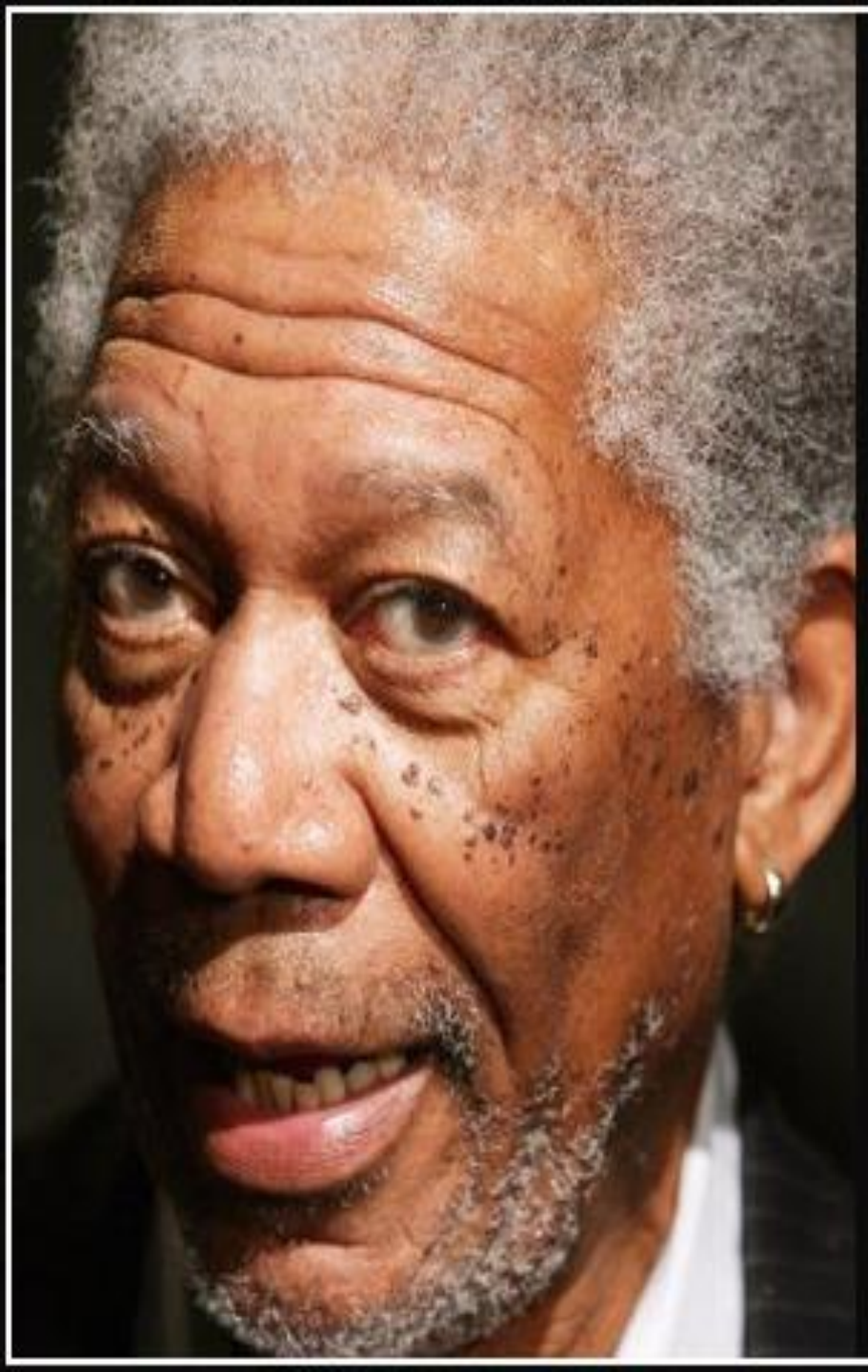
Končna verzija

ALFA
NETWORK


Windows11 - VMware Workstation
File Edit View VM Tabs Help
Windows11
Command Prompt
Microsoft Windows [Version 10.0.22621.1702]
(c) Microsoft Corporation. All rights reserved.
C:\Users\User>
Search
11:18
07/09/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


viris@hashcatcher: /opt/respc
viris@hashcatcher:/opt/responder/logs $

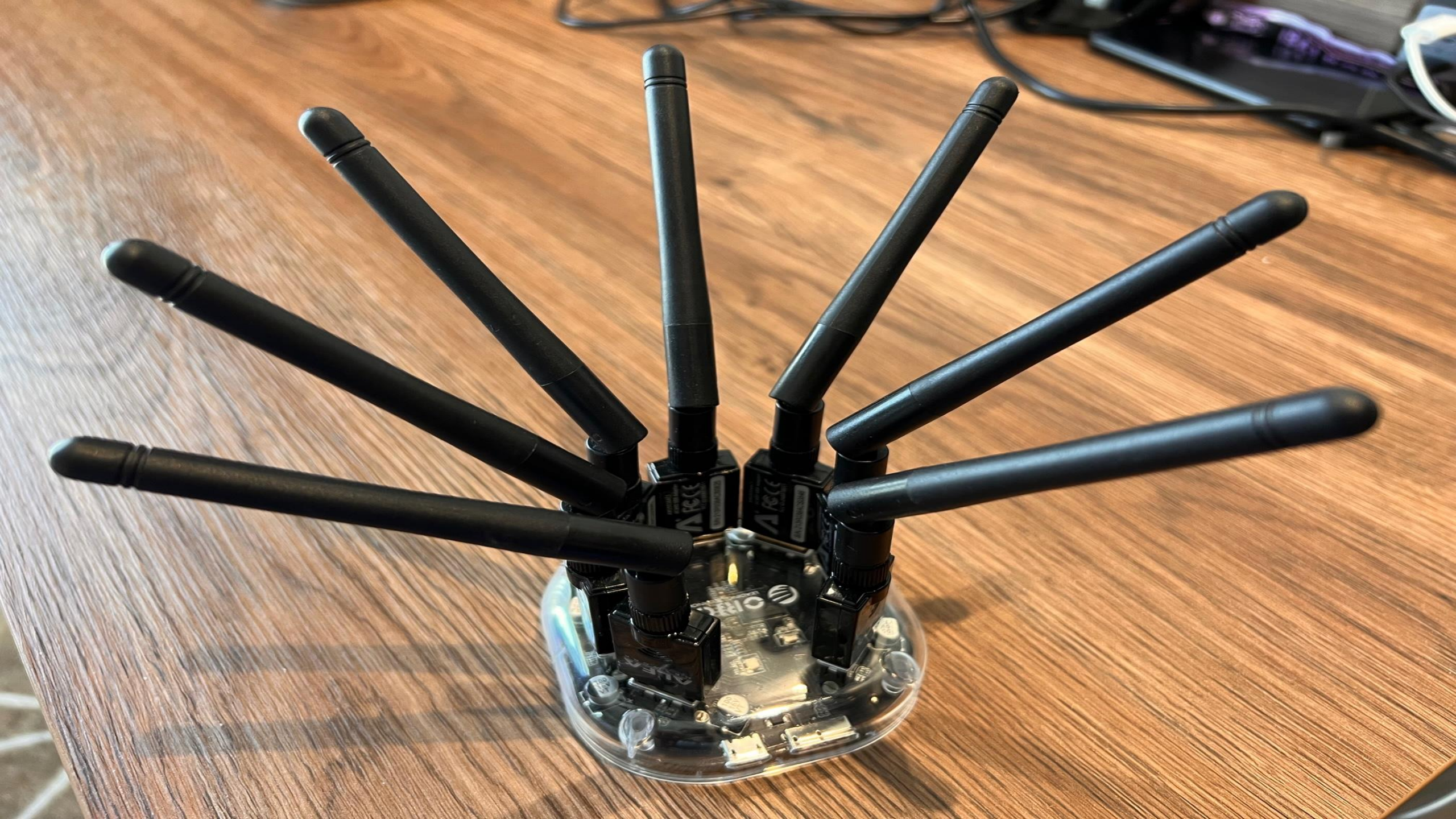

Hashtopolis 0.13.0 [hashtopoli
https://hashtopolis.int.viris.si/hashlists.php
Hashtopolis
Tasks
Lists
My Account
Hashlists (774)
Show archived
Show 50 entries
Search:
ID
Name
Hash type
Format
Cracked
Pre-cracked
Action
875
HASHCATCHER[::ffff:172.13.187.152|NTLMv2|VIRISDEVPC\User]
NetNTLMv2
Text
0.00% (0 / 1)



If you're not living on the edge then you're taking up a little too much space.

— Morgan Freeman —

AZ QUOTES




FINISH

TOP 10 EMERGING CYBER-SECURITY THREATS FOR 2030

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Povzetek

- Ne pozabite na uporabnike!
- Kvalitetna gesla in MFA
- Imejte stvari, sisteme in aplikacije pod kontrolo
- Posodabljajte sisteme – vse! Brez izjem!
- Sledite stvarem/novostim!
- Bodite proaktivni!

Vprašanje/a?

Twitter (X) - **@MilanGabor**

COMING SOON TO A THEATER NEAR YOU

NT KONF

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ

This is not school, but we love to get grades.
Please fill out our questoineers and leave us your feedback.
You may even win some cool rewards.

NT KONF

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ