



**SECURITY
DAYS**

KIBERNETINIO SAUGUMO INCIDENTO TYRIMAS: DETEKTYVĖ ESET



LUKAS APYNIS

„Baltimax“ vyresnysis
kibernetinio saugumo
inžinierius, ESET ekspertas

**Jie turi taktikas, o mes - aptikimo
ir reagavimo priemonės**



Cybersecurity
Progress. Protected.

Šiandienos istorijos



BlackBasta – Oh Shift, kà jie padarè?



BlackPasta



Cybersecurity
Progress. Protected.

PRIEŠISTORĖ



**Savarankiškai
prižiūrėjo savo
saugumą**

Viskas susiklostė ne
taip, kaip tikėjosi



**Failų šifravimo
ataka**

Užšifruoti failai



**Norėjo, kad mes
ištirtume**

Skamba įdomiai



Tapo SOC klientu

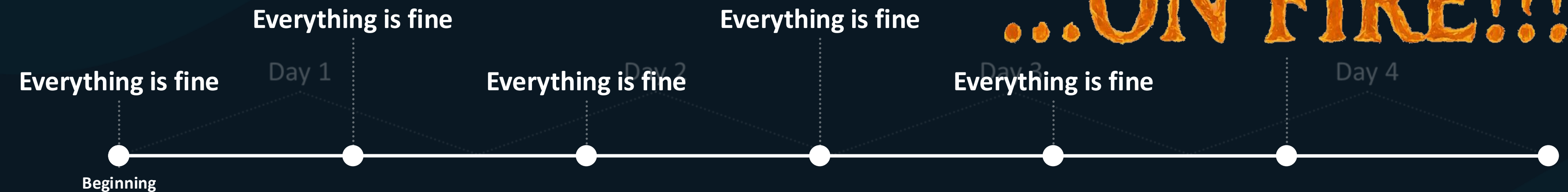
Aktyvi stebėseną,
grėsmių paieška ir
užkardymas

Paskutinės dienos chronologija



Everything is...

...**ON FIRE!!!!**



Paskutinės dienos chronologija

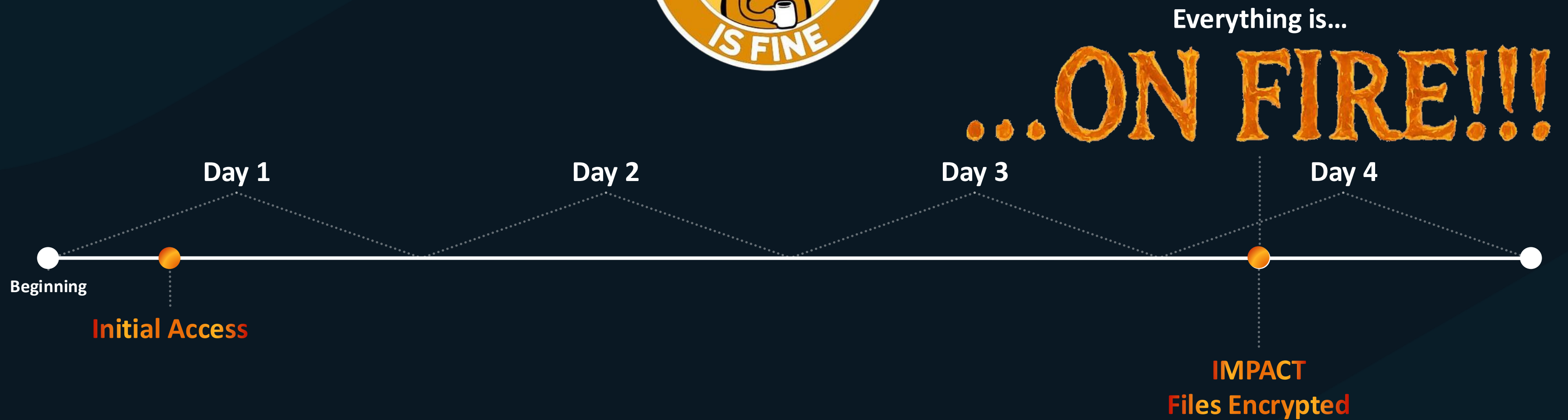


Everything is...

...**ON FIRE!!!**



Paskutinės dienos chronologija



Pirminė prieiga - RDS

- Piktadarys prisijungia prie RDS ir pasirenka programą
- Jam parodoma programa
- 5 kartus paspaudžia klavišą „Shift“
- Paspaudžia nuorodą...
- Valdymo skydas (iš tikrųjų - „explorer.exe“)
- Paleidžia „iexplorer“, „cmd“ ir pan....





Work Resources

RemoteApp and Desktop Connection

[Help](#)

Domain\user name:

Password:

Security

Warning: By logging in to this web page, you confirm that this computer complies with your organization's security policy.

[Sign in](#)

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.



Work Resources

RemoteApp and Desktop Connection

RemoteApp and Desktops

Help

Sign out

Current folder: /



Calculator

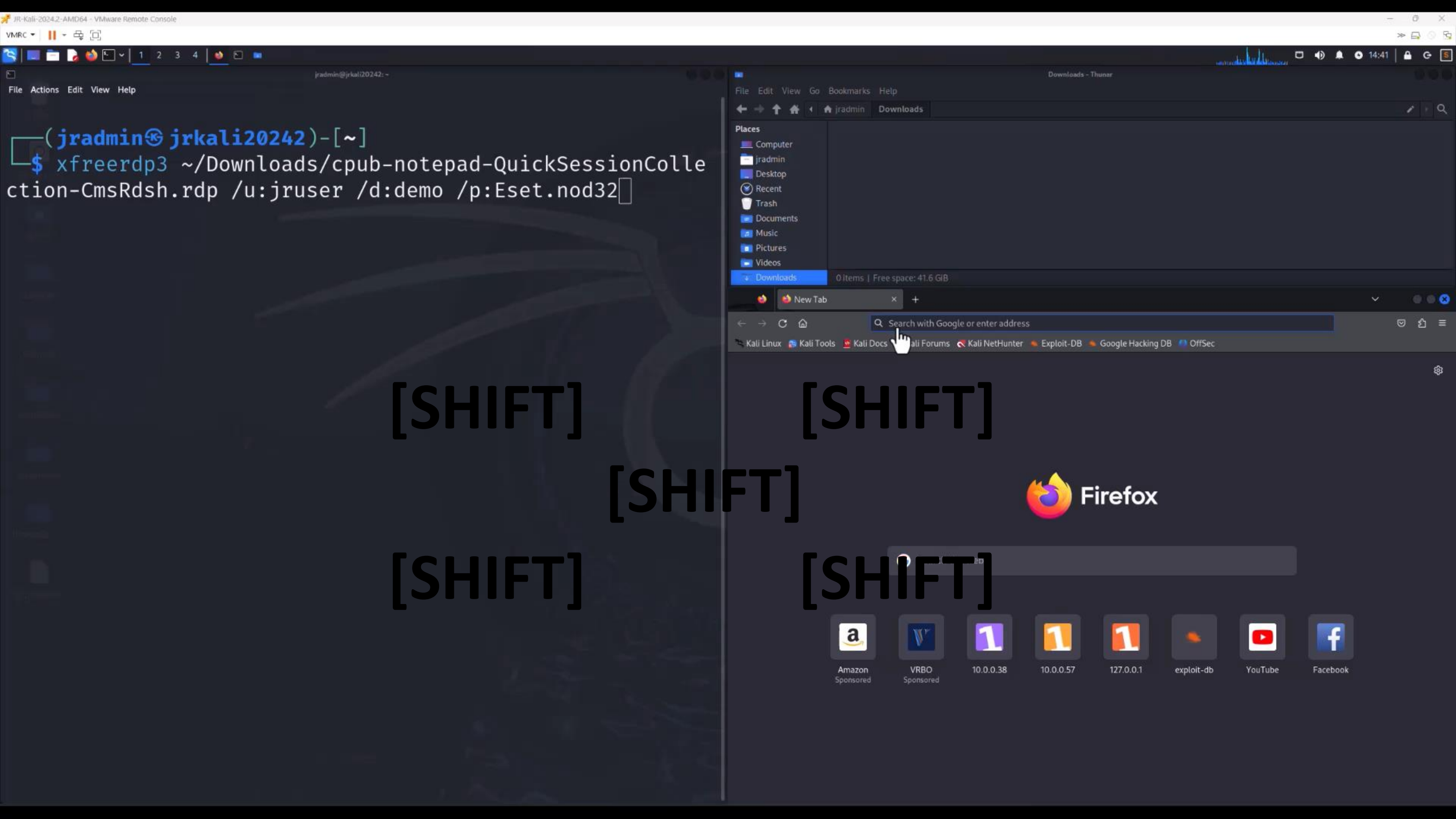


notepad



Paint

Notepad



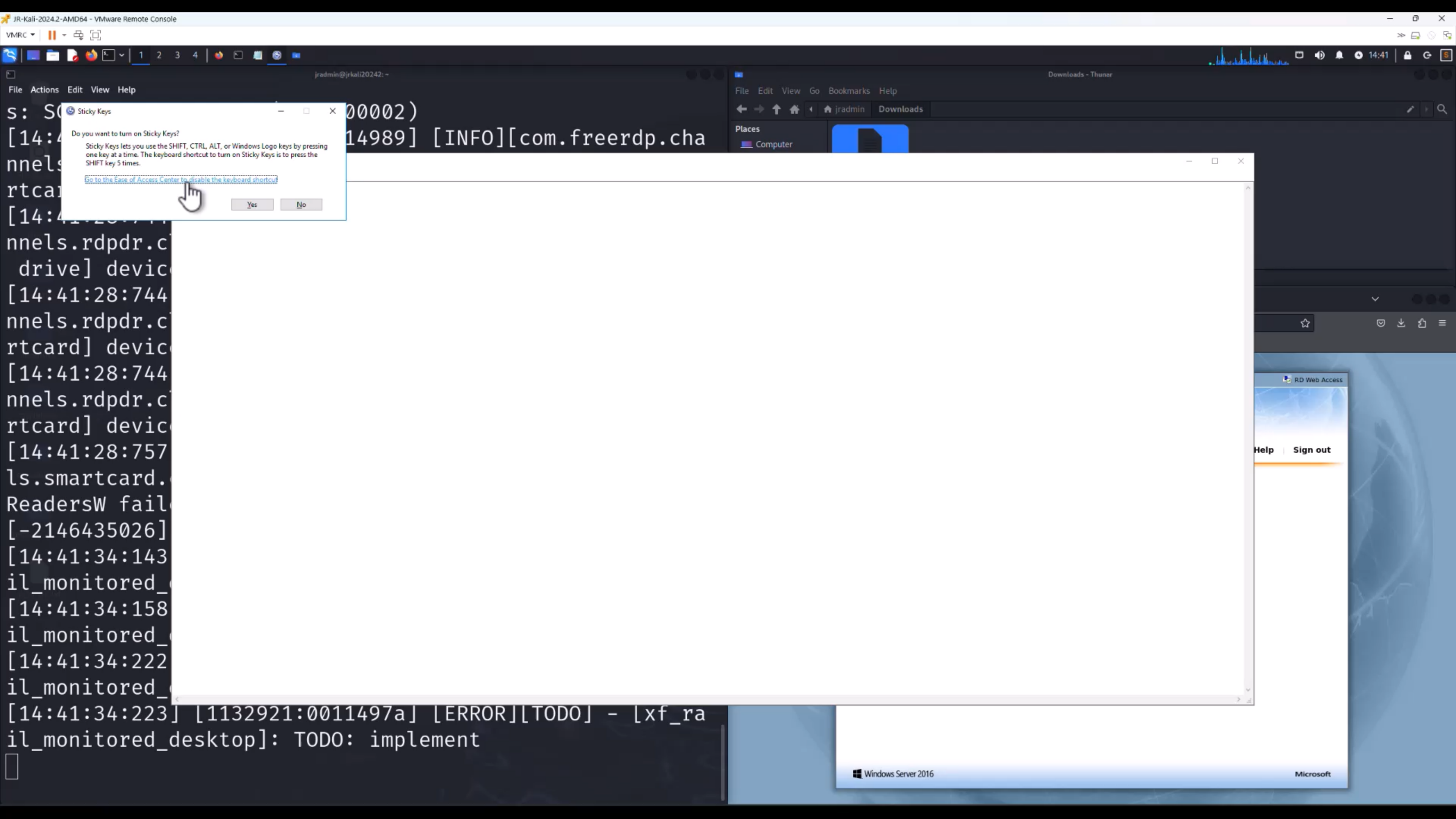
[SHIFT]

[SHIFT]

[SHIFT]

[SHIFT]

[SHIFT]



s: S000002)
[14:41:28:744] [INFO][com.freerdp.cha

Sticky Keys

Do you want to turn on Sticky Keys?

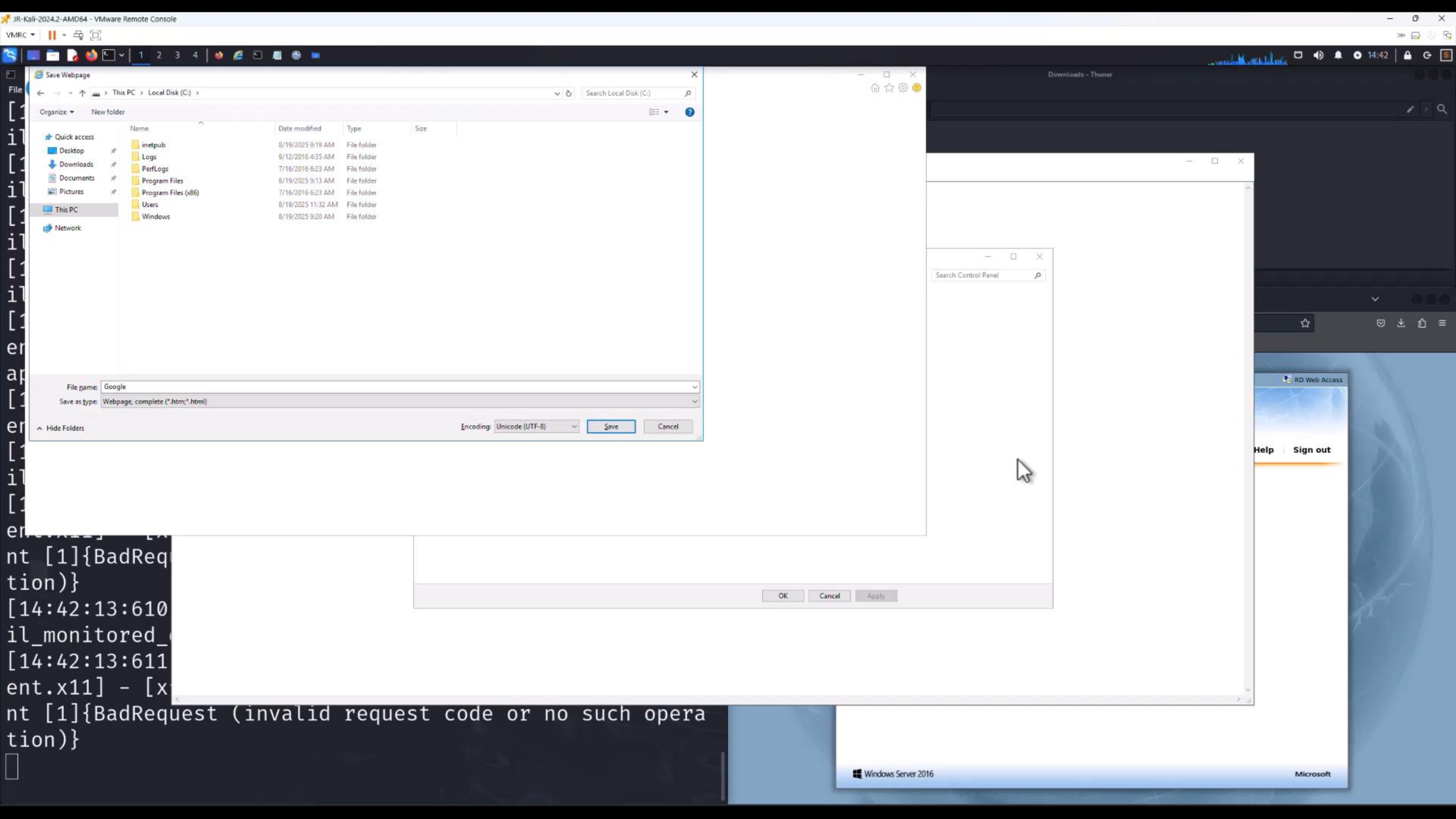
Sticky Keys lets you use the SHIFT, CTRL, ALT, or Windows Logo keys by pressing one key at a time. The keyboard shortcut to turn on Sticky Keys is to press the SHIFT key 5 times.

[Go to the Ease of Access Center to disable the keyboard shortcut](#)

Yes

No

nnels.rdpdr.c
drive] device
[14:41:28:744
nnels.rdpdr.c
rtcard] device
[14:41:28:744
nnels.rdpdr.c
rtcard] device
[14:41:28:757
ls.smartcard.
ReadersW fail
[-2146435026]
[14:41:34:143
il_monitored_
[14:41:34:158
il_monitored_
[14:41:34:222
il_monitored_
[14:41:34:223] [1132921:0011497a] [ERROR][TODO] - [xf_ra
il_monitored_desktop]: TODO: implement



Initial Access - RDS

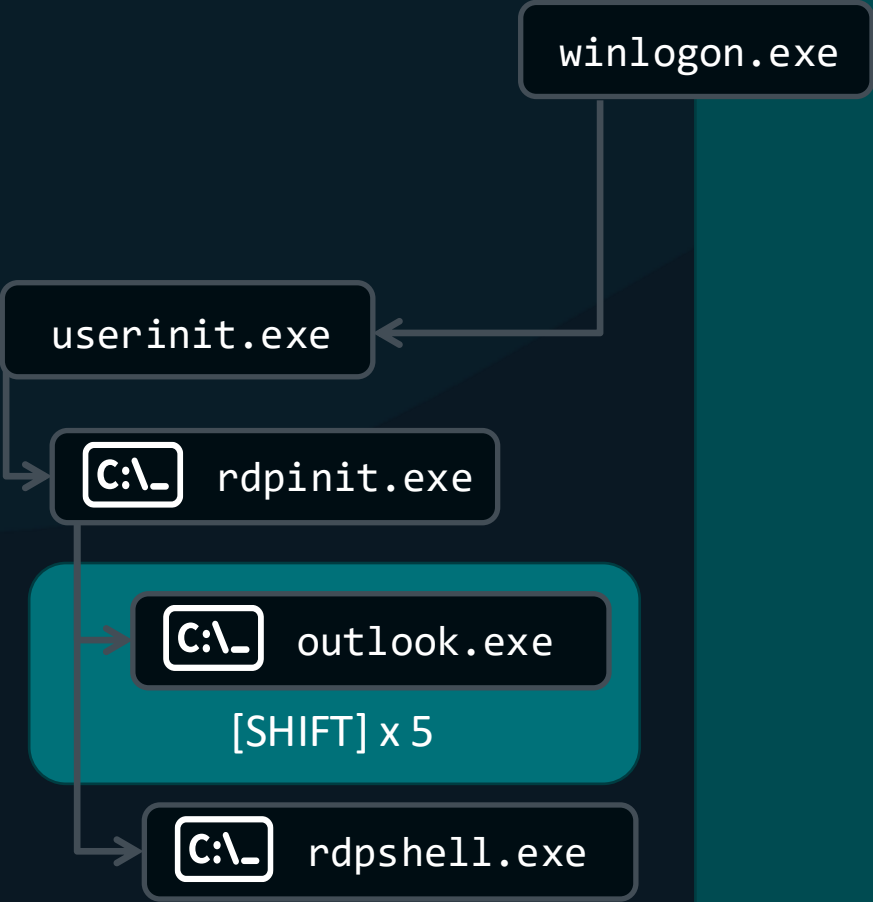
RDS Launching Apps

Sticky Keys Launched

Control Panel Explorer

Initial Access - RDS

RDS Launching Apps

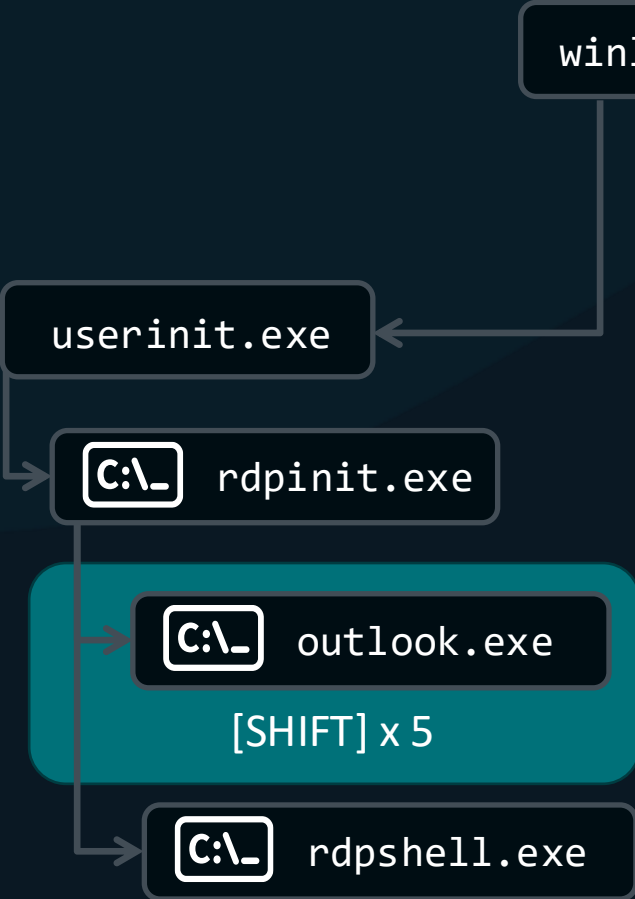


Sticky Keys Launched

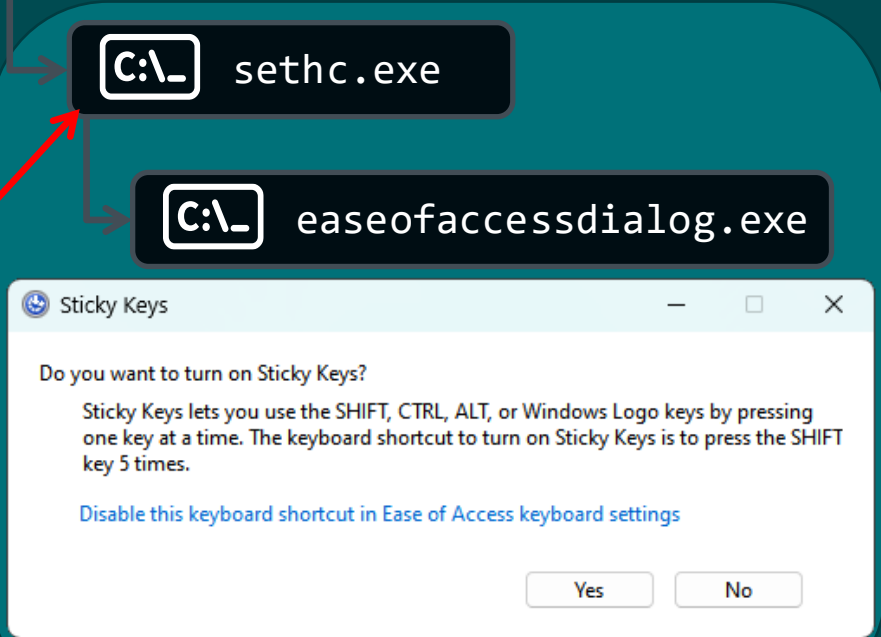
Control Panel Explorer

Initial Access - RDS

RDS Launching Apps



Sticky Keys Launched



Control Panel Explorer

Initial Access - RDS

RDS Launching Apps

Sticky Keys Launched

Control Panel Explorer



Pirminė prieiga - RDS

RDS Launching Apps

Sticky Keys Launched

Control Panel Explorer



Jie turi prieigą... Ką jie veikia?

Žvalgyba - PowerShell...

- systeminfo.exe
- tasklist.exe
- Failed Command: powershell.exe '-c "[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain();'=LDAP://'.; <snip>"
- nltest.exe /domain_trusts
- whoami.exe
- ipconfig.exe
- ping.exe
- Procexp64.exe

Failų perdavimas - naudojami keli įrankiai...

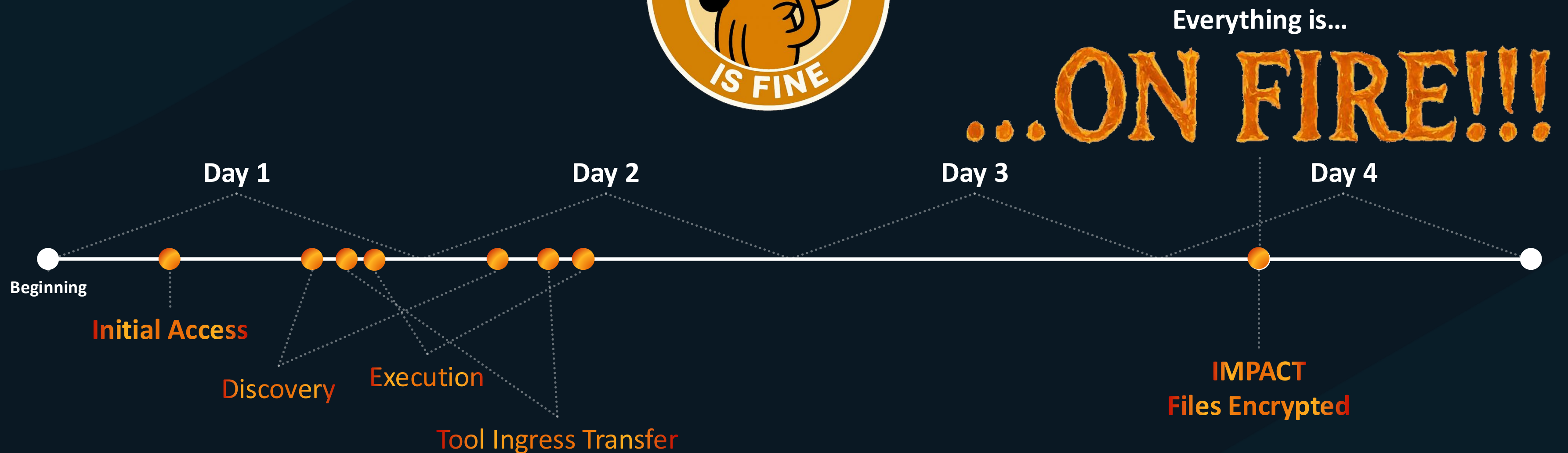
- Internet Explorer, MS Edge, Chrome
 - URL/Urlik.AAF
 - Win64/GenKryptik.GTKR
 - MSIL/Riskware.BloodHound.D
 - MSIL/Riskware.Rubeus.A
 - Hash blocked by ESET LiveGuard
- PowerShell Invoke-WebRequest (used alias "iwr")
 - Win64/CobaltStrike.Agent.B
- Certutil.exe
 - Win32/Rozena.SA
- Explorer.exe (copy paste via RDP)
 - Win64/Kryptik.EEY

Dvi dienas buvo užblokuota daugybė veiksmų

Threat Name – Day 1	Count
Suspicious	5
URL/Urlik.AAF	1
URL/Urlik.C	1
URL/Urlik.E	1
Win64/GenKryptik.GTKR	1
Win64/Kryptik.EEY	5
Win64/Kryptik.EFH	1
Renamed PowerShell Execution [D0411]	19
Total	34

Threat Name – Day 2	Count
Hash blocked by ESET LiveGuard	2
Generik.GXUDDTG	2
MSIL/HackTool.SharpShares.A	1
MSIL/Riskware.BloodHound.D	6
MSIL/Riskware.Rubeus.A	3
Suspicious	14
Win32/GenCBL.EQQ	2
Win32/Rozena.SA	2
Win64/CobaltStrike.Agent.B	2
Win64/CobaltStrike.Artifact.Z	1
Win64/CobaltStrike.Beacon.A	2
Win64/GenKryptik.GTCZ	2
Win64/GenKryptik.GTOS	2
Win64/Kryptik.EEY	2
Win64/Kryptik.EFH	7
Win64/Kryptik.EFK	5
Win64/Kryptik.EFP	2
Renamed PowerShell Execution [D0411]	4
Total	62

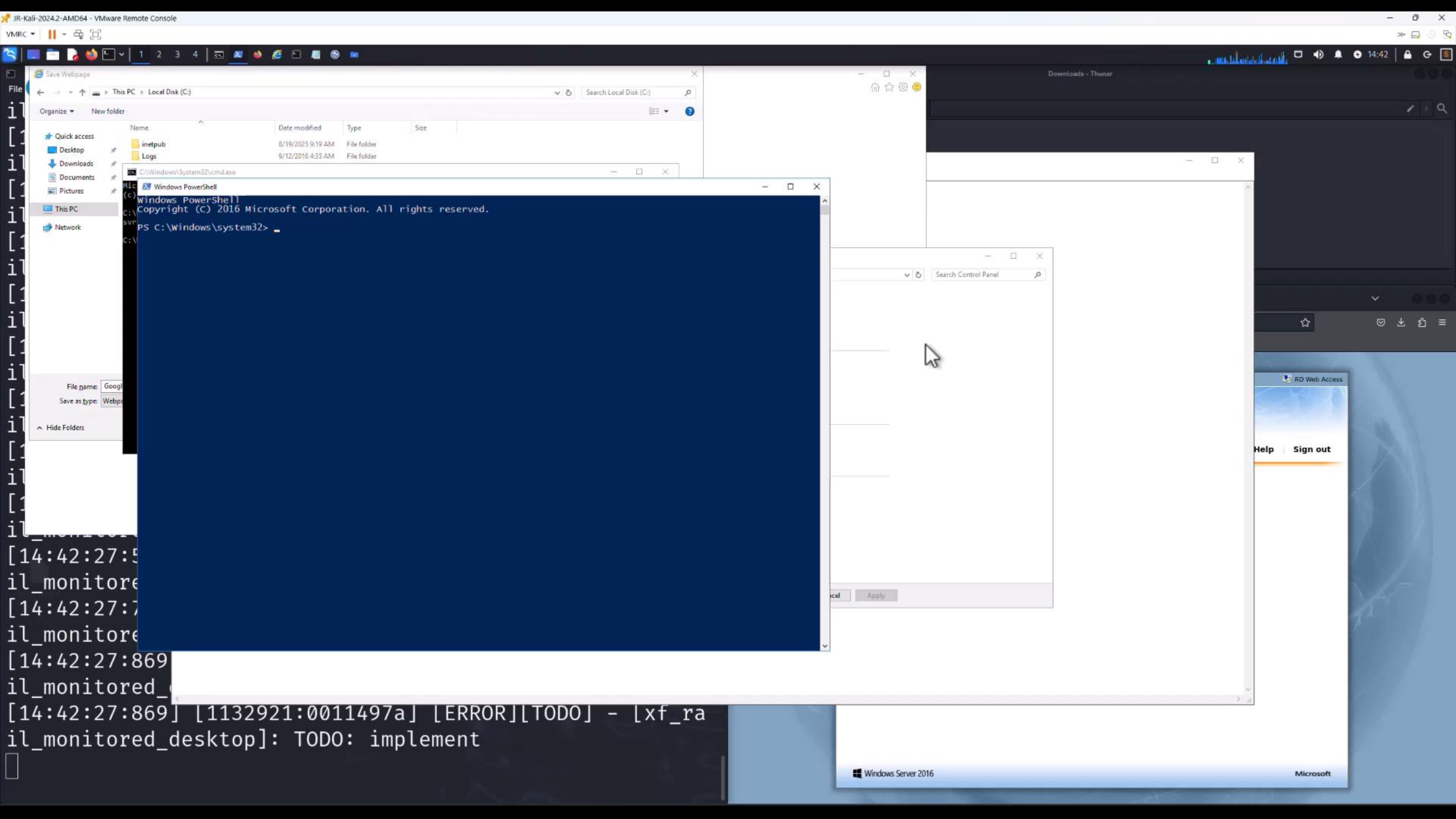
Paskutinės dienos chronologija



Jei visi jų įrankiai buvo užblokuoti, kaip jiems pavyko apeiti „ESET“ ir paleisti išpirkos reikalaujančią programą?

- ✓ Jiems to atlikti nepavyko
- ✓ Jie atidarė PDF failą, pavadintą „Company Passwords.PDF“
- ✓ Atsisakė to įrenginio ir prisijungė per RDP prie neapsaugoto serverio
- ✓ Be to, per RDP prisijungė prie 127.0.0.1





File Explorer

This PC > Local Disk (C:)

Search Local Disk (C:)

Organize New folder

Name	Date modified	Type	Size
inetpub	8/19/2025 9:19 AM	File folder	
Logs	9/12/2016 4:35 AM	File folder	

File name: Google
Save as type: Webpage
Hide Folders

Windows PowerShell

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32>

Search Control Panel

Cancel Apply

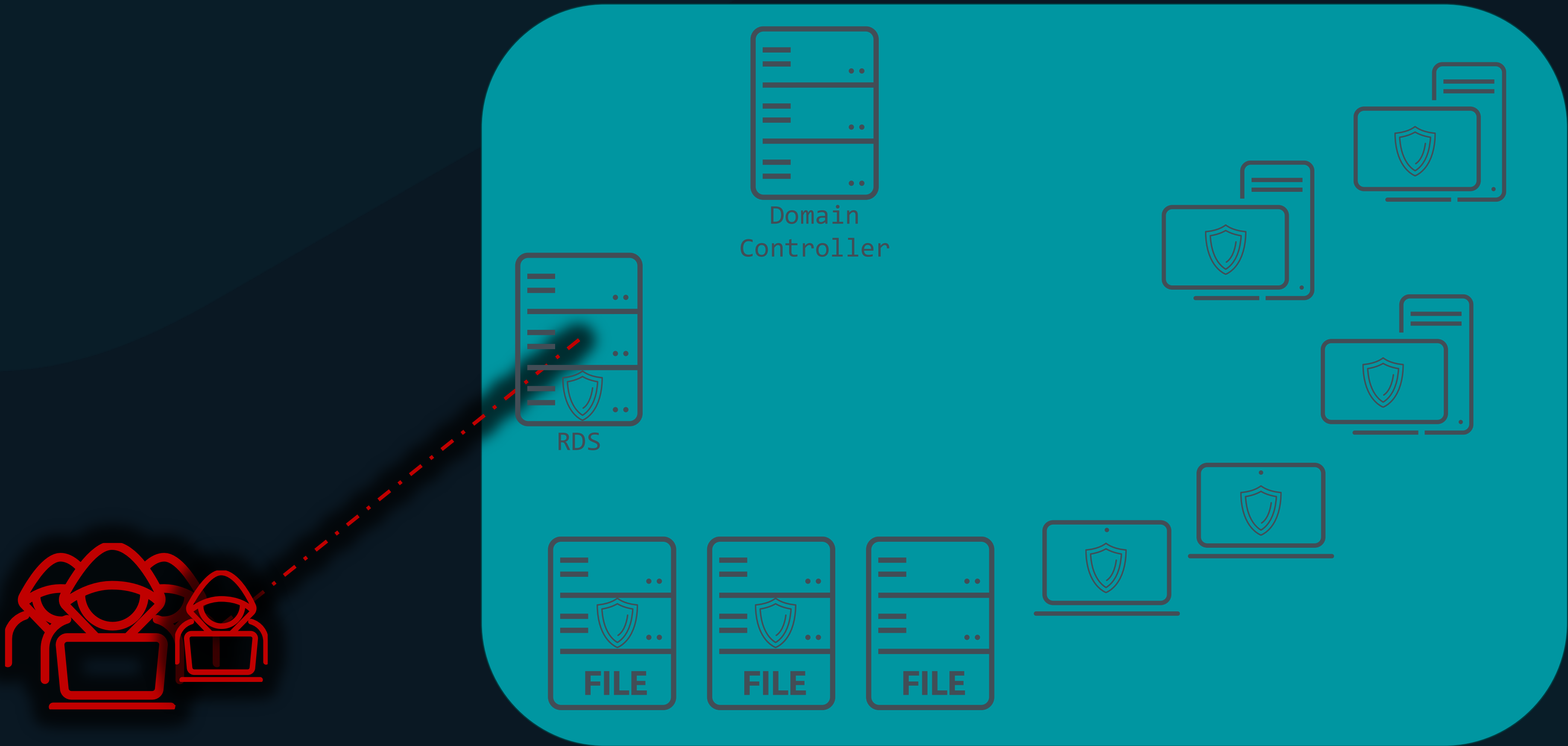
RD Web Access

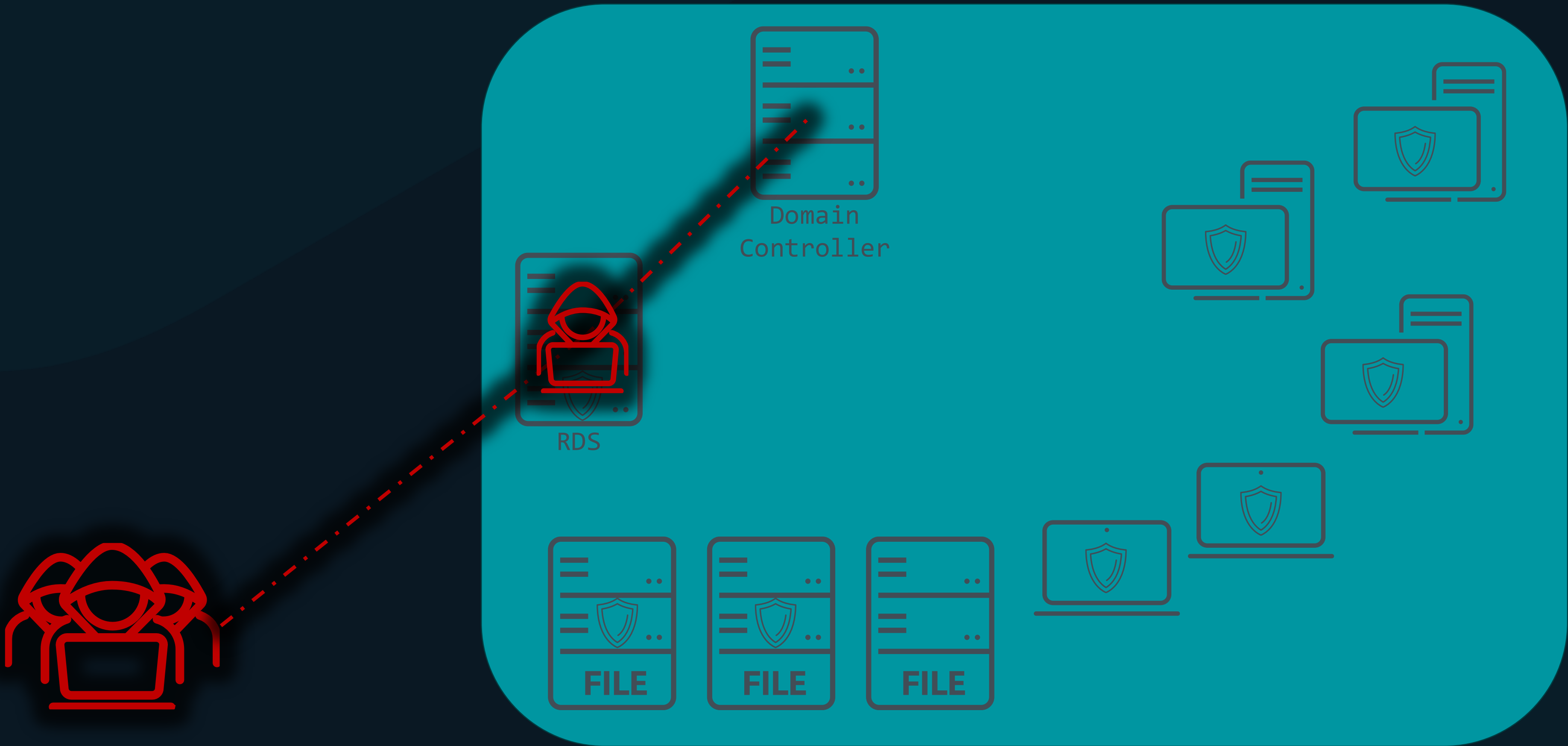
Help Sign out

[14:42:27:5]
il_monitored
[14:42:27:7]
il_monitored
[14:42:27:869]
il_monitored
[14:42:27:869] [1132921:0011497a] [ERROR][TODO] - [xf_ra
il_monitored_desktop]: TODO: implement

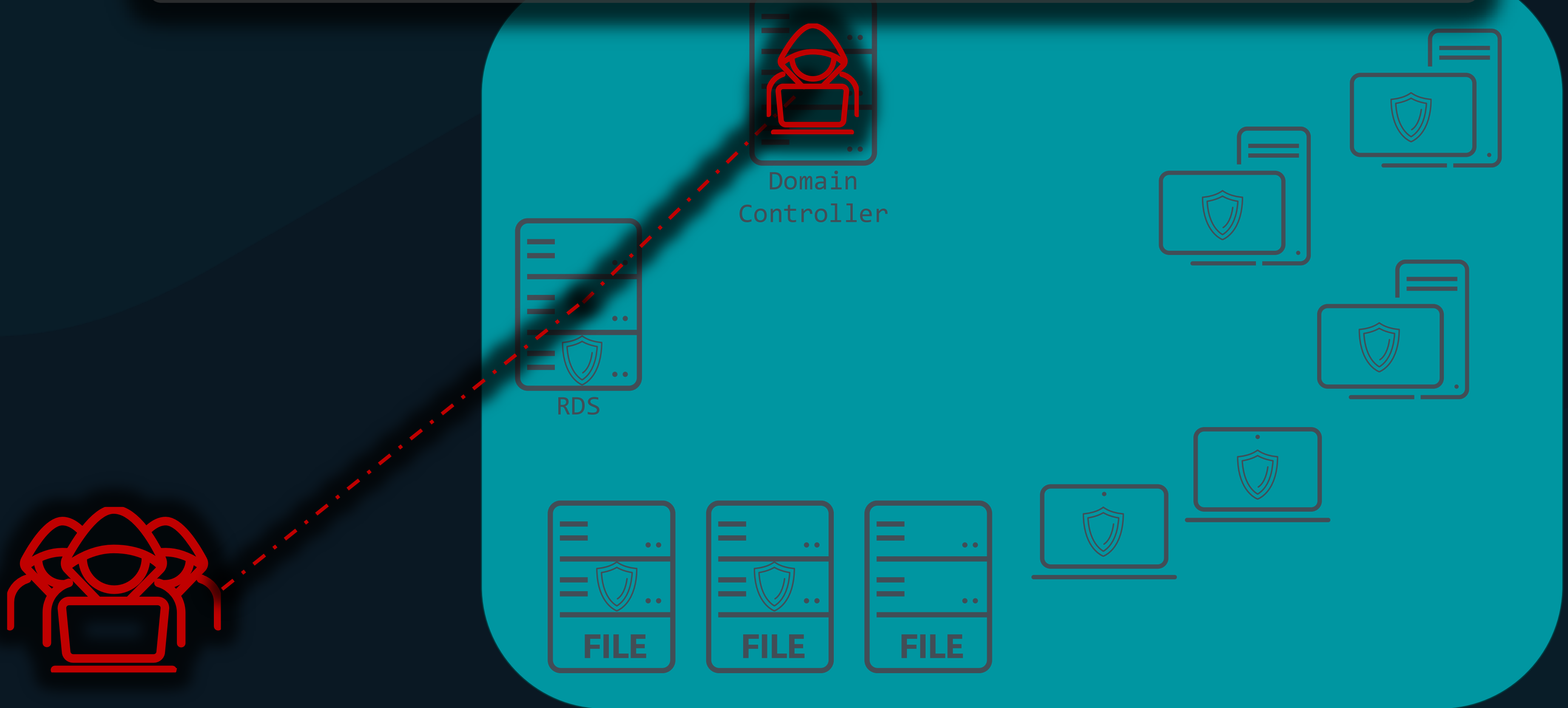
Windows Server 2016

Microsoft

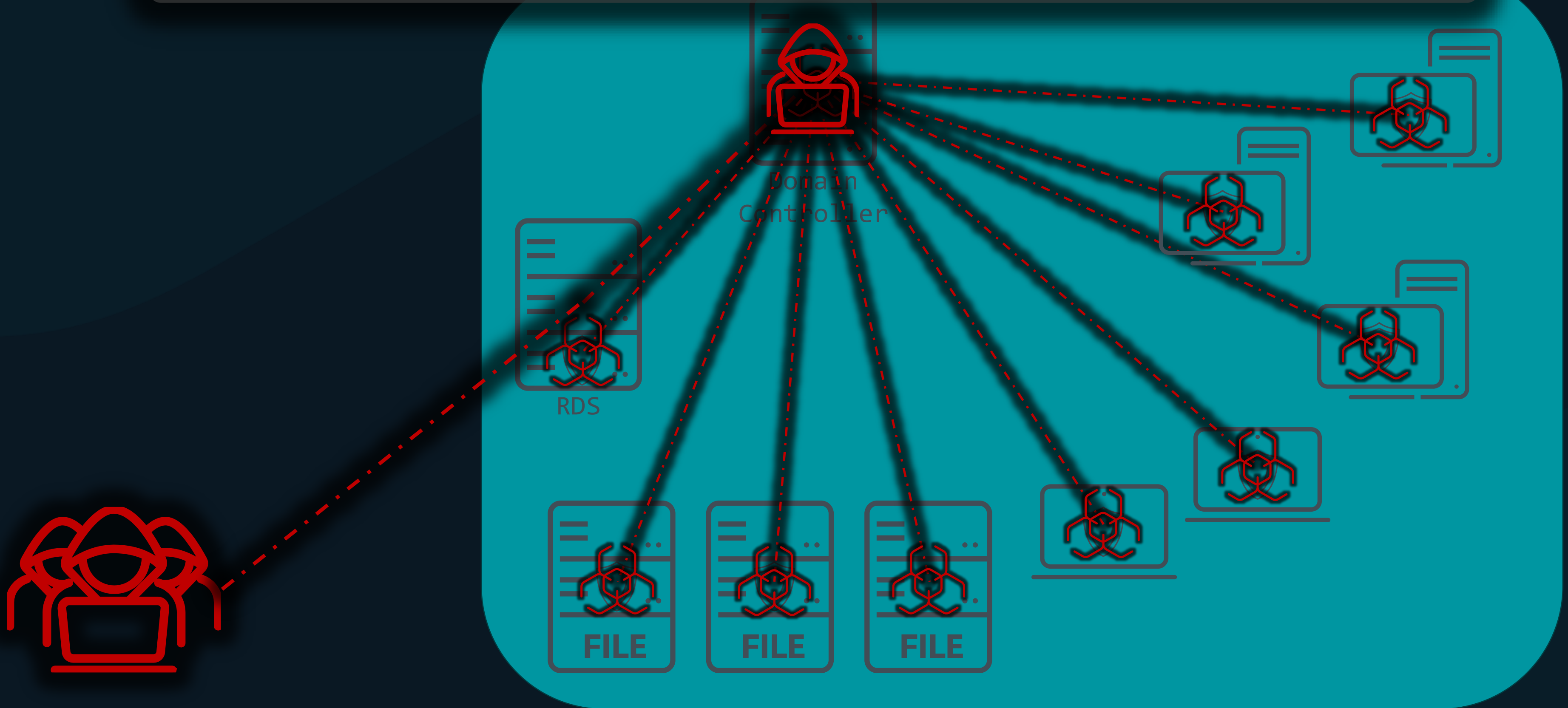




WMI:> %WINDIR%\syswow64\rundll32.exe c:\windows\COMPANY_c.dll,VisibleEntry



WMI:> %WINDIR%\syswow64\rundll32.exe c:\windows\COMPANY_c.dll,VisibleEntry





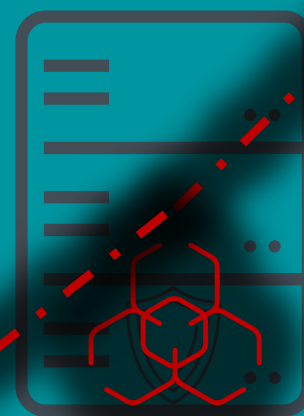
LiveGuard Advanced with Inspect



```
WMI:> %WINDIR%\syswow64\rundll32.exe c:\windows\COMPANY_c.dll,VisibleEntry
```



```
syswow64\rundll32.exe c:\windows\COMPANY_c.dll,VisibleEntry
```



RDS



Domain
Controller



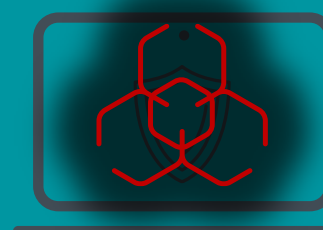
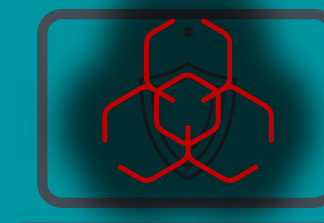
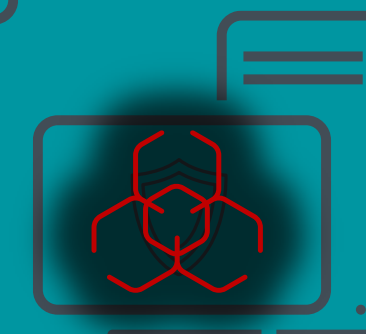
FILE



FILE



FILE





LiveGuard Advanced with Inspect

3 min

`c:\windows\COMPANY_c.dll,VisibleEntry`



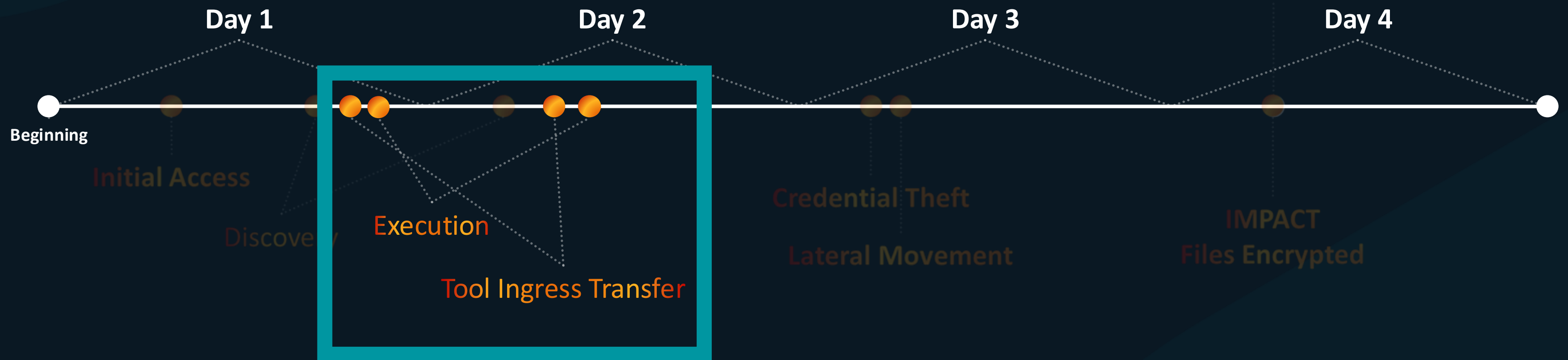
Paskutinės dienos chronologija



Paskutinės dienos chronologija



Everything is...
...ON FIRE!!!!



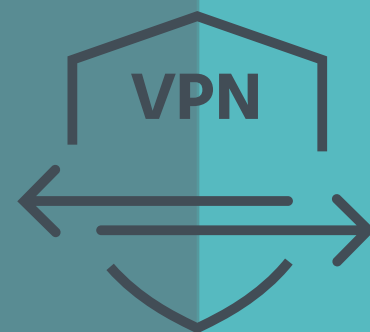
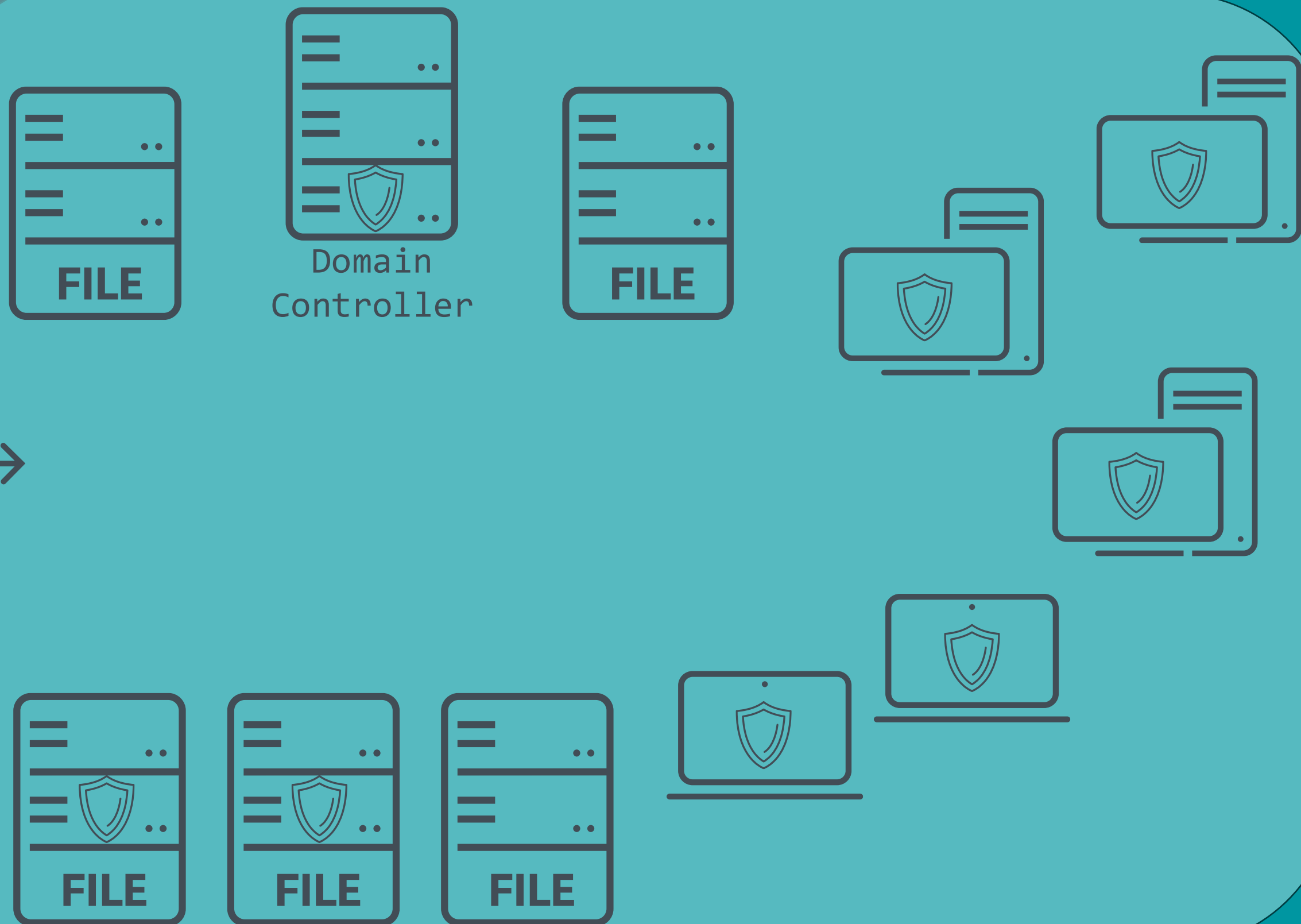
Išmoktos pamokos

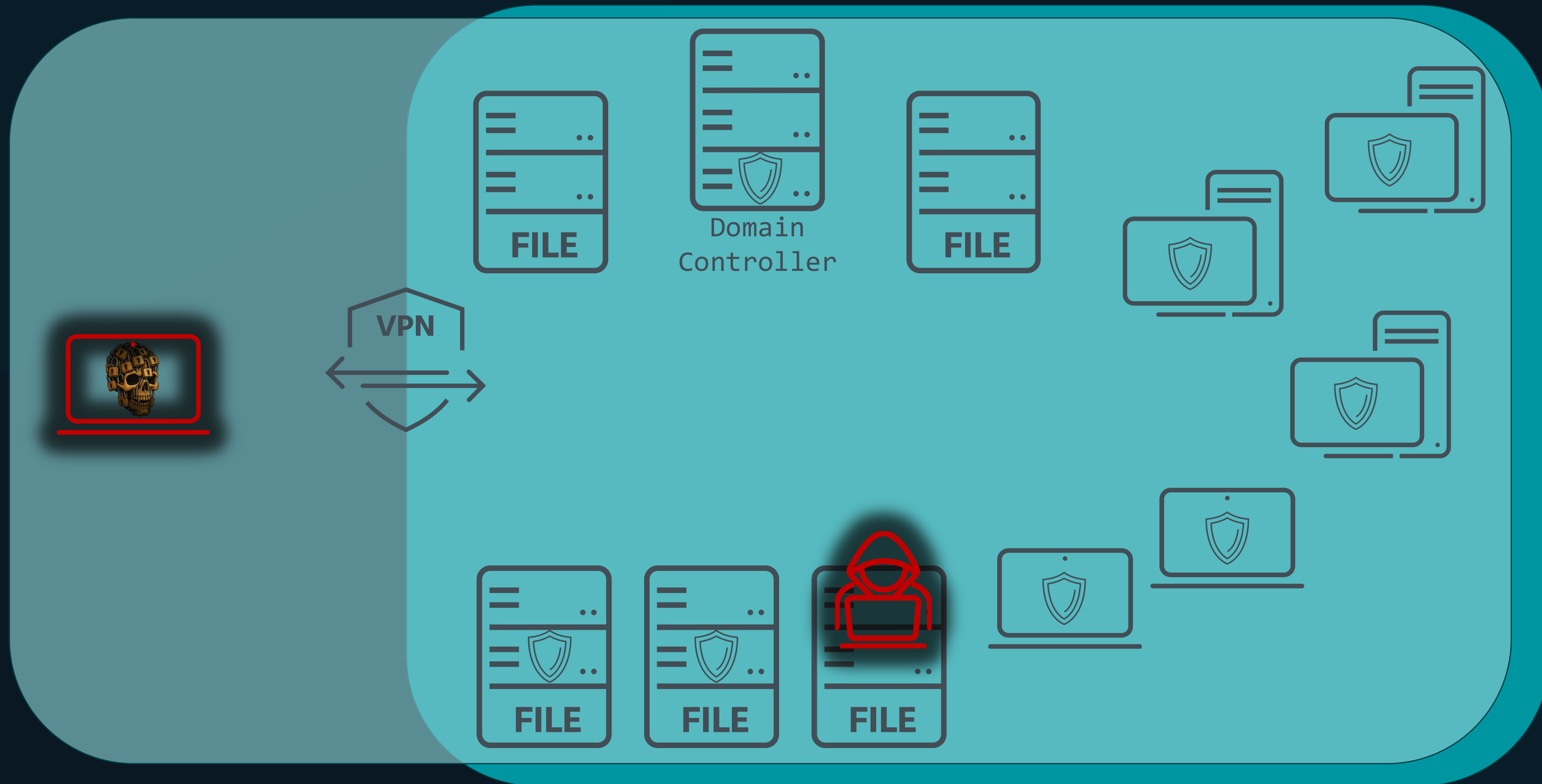
- ✔ Dviejų veiksmų autentifikavimas (2FA) būtų užblokavęs pradinį prisijungimą
- ✔ Numatytas EDR/XDR taisyklių rinkinys ir antivirusinė programa yra veiksmingos priemonės, padedančios užkirsti kelią įsilaužėliams
- ✔ Jei tai būtų stebėję kibernetinio saugumo ekspertai, tai būtų sustabdyta jau pirmą dieną
- ✔ Būtų buvę naudinga įdiegti ESET programą visuose įrenginiuose

„DeadLock“ - kova dël pergalès

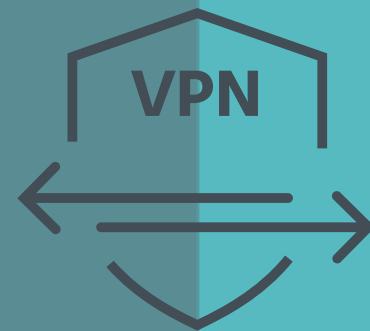
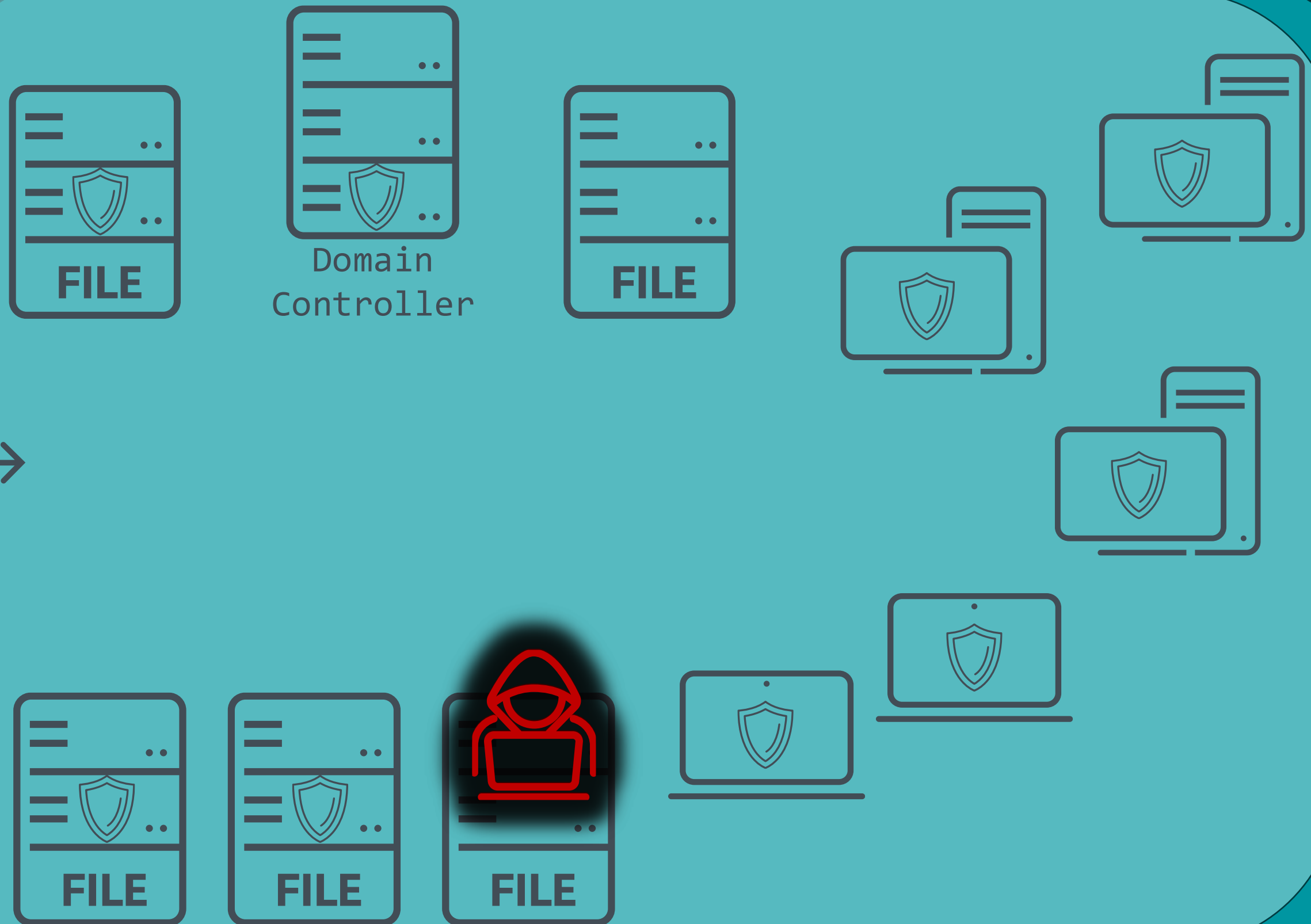


Cybersecurity
Progress. Protected.

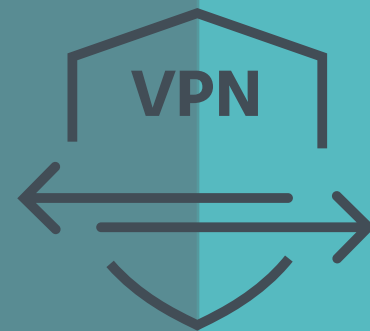




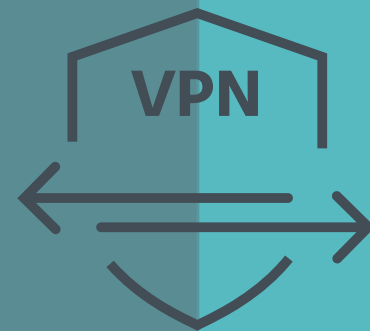
Išpirkos^{reik}reikalaujantis virusas per SMB



Išpirkos^{reik}reikalaujantis virusas per SMB



Išpirkos^{reik}reikalaujantis virusas per SMB





Kovos chronologija

Encryption failed...
BLOCKED AGAIN?!?!

Lateral Movement
from Rogue to
Unprotected device

Blocked by IDS/IPS

Hour 1

Hour 3

Hour 5

Hour 7

Hour 9

Hour 11

Beginning

Impacket

Hour 2

Hour 4

Blocked by IDS/IPS
Ransomware Over
SMB

Hour 8

Hour 10

TCP Port Scanning

Lateral Movement
Via PSEXEC RDP

EDR Killer Appears
EXE & Driver

Blocked by IDS/IPS

TCP Port Scanning
From unprotected host

Initial Access
Rogue Device on
Fortigate SSLVPN



Kovos chronologija

Move to another device...
Try again...

Lateral Movement
from Rogue to
Unprotected device

Blocked by IDS/IPS

EDR Killer Appears
EXE & Driver
Lateral Movement
Via PSEXEC RDP
Ransomware Over
SMB

Beginning

Impacket

TCP Port Scanning

Initial Access

Rogue Device on
Fortigate SSLVPN

Blocked by IDS/IPS

TCP Port Scanning
From unprotected host

Lateral Movement
Via PSEXEC RDP
Ransomware Over
SMB

EDR Killer Appears
EXE & Driver

Blocked by IDS/IPS

Ransomware Over
SMB



Kovos chronologija

...WHY NO WORK?!?!

It should work.

It no work.

Lateral Movement
from Rogue to
Unprotected device

EDR Killer Appears

EXE & Driver

Lateral Movement
Via PSEXEC RDP

Ransomware Over
SMB

Blocked by IDS/IPS

Blocked by IDS/IPS

Beginning

Impacket

TCP Port Scanning

Initial Access

Rogue Device on
Fortigate SSLVPN

Blocked by IDS/IPS

Lateral Movement
Via PSEXEC RDP

EDR Killer Appears
EXE & Driver

TCP Port Scanning
From unprotected host

Blocked by IDS/IPS
Ransomware Over
SMB

Hour 9

Hour 11

Hour 10

Hour 8

Hour 7

Hour 5

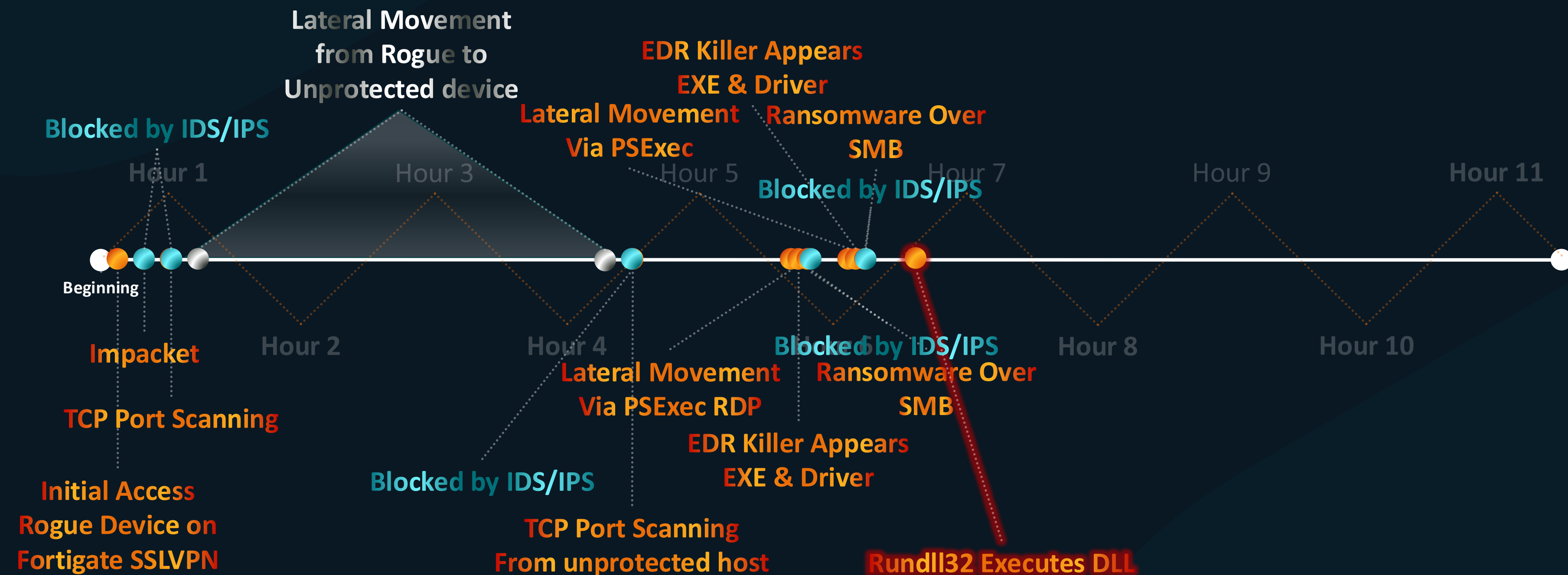
Hour 3

Hour 1



Kovos chronologija

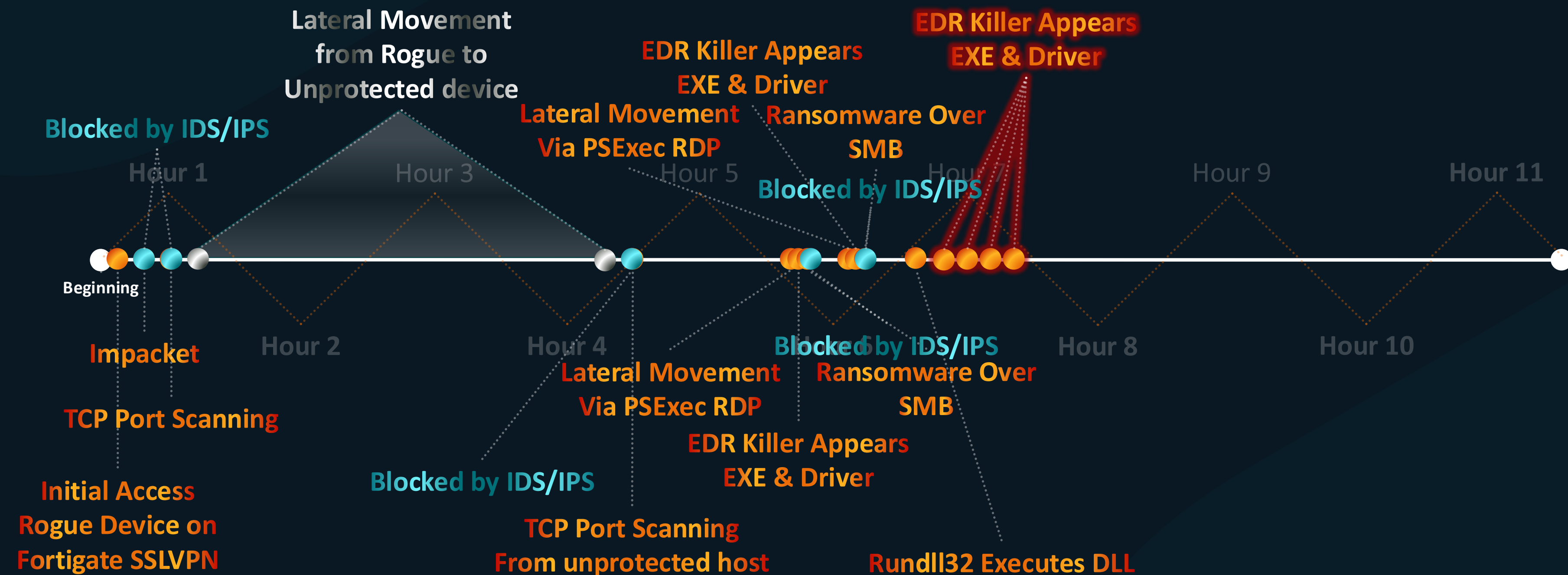
Time to change tactics. No longer use EXE or SMB. Just RunDll32 and my DLL.





Kovos chronologija

Lets try my EDR Killer
some more.

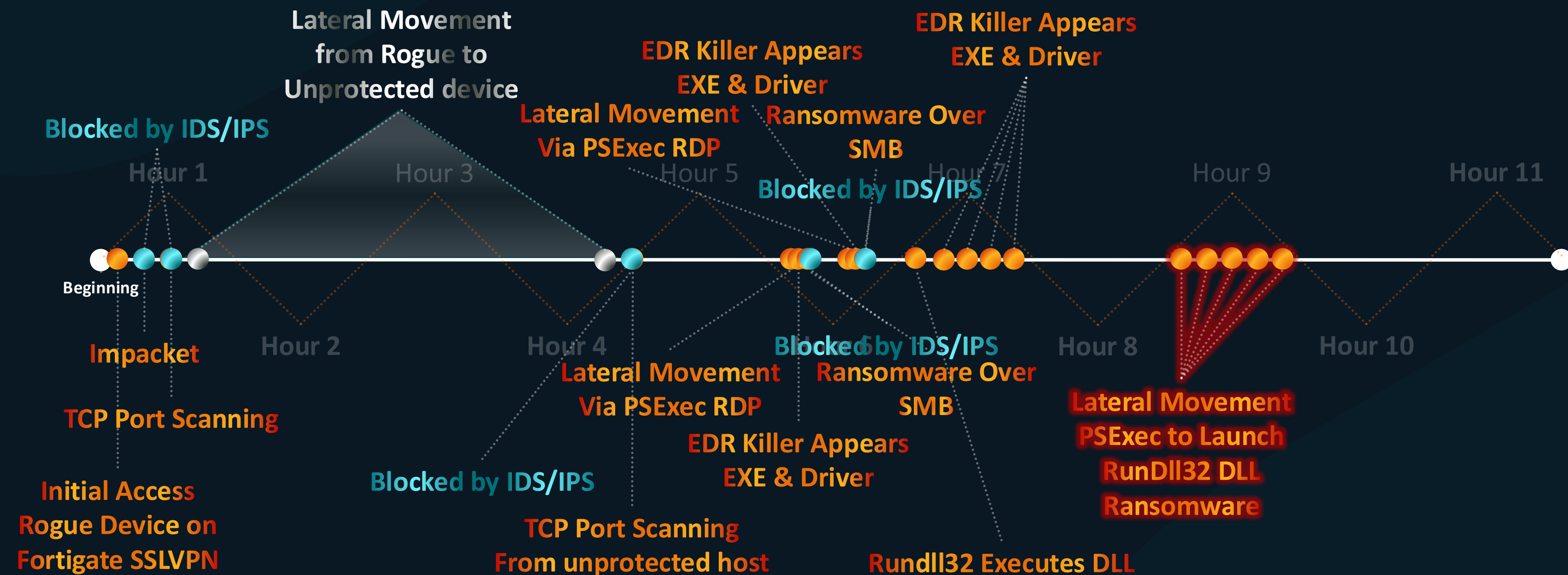




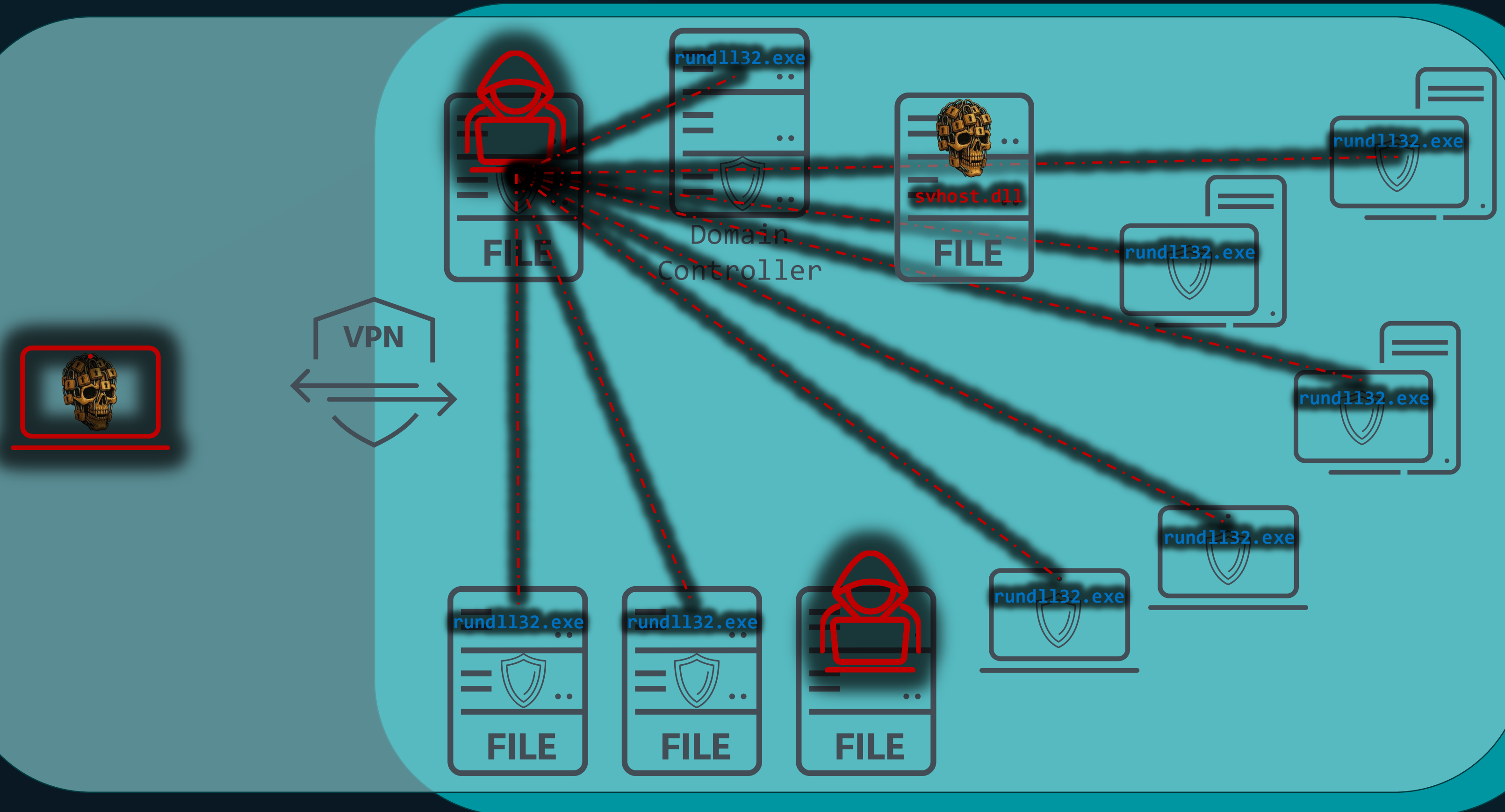
Kovos chronologija

Skrew it.

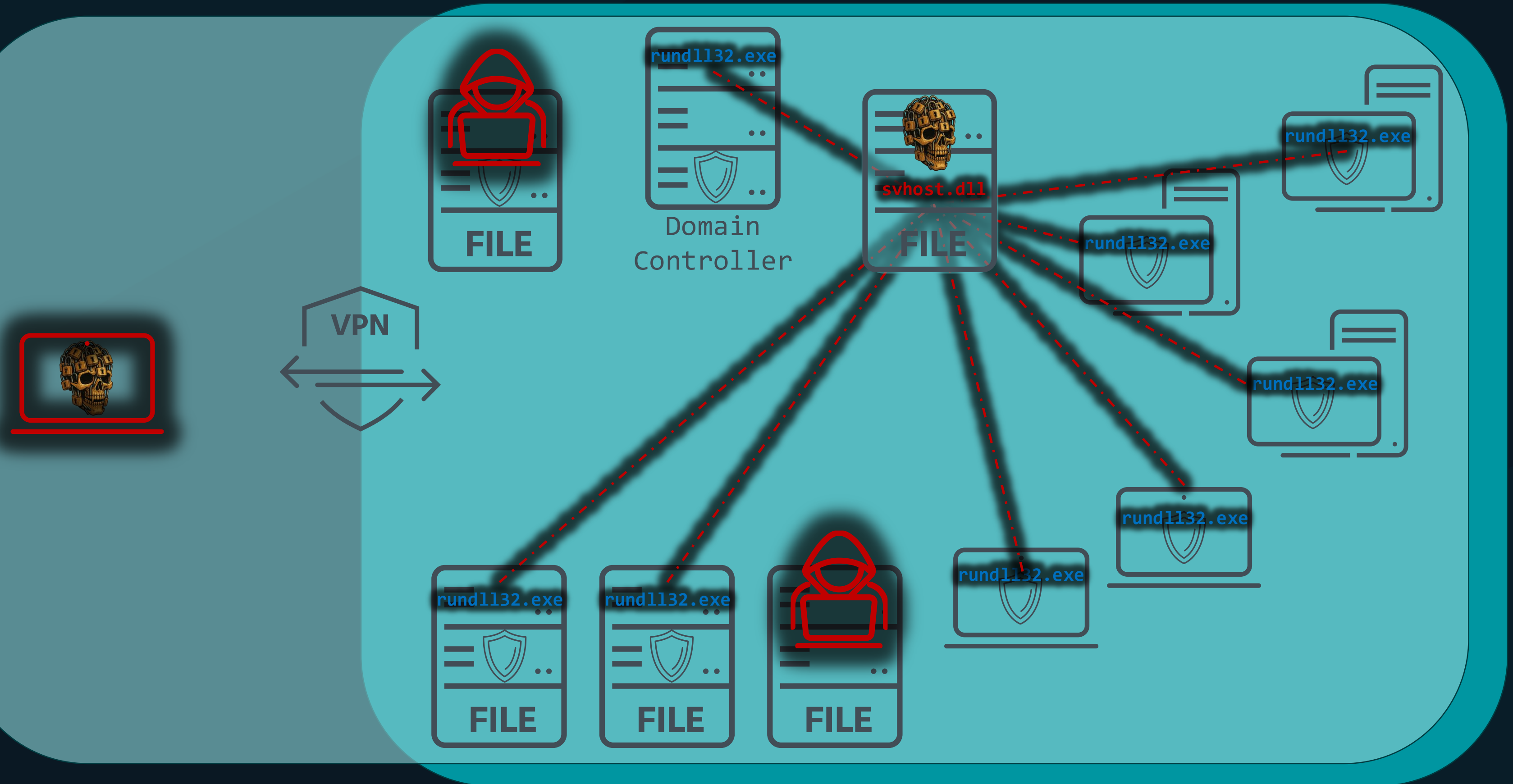
PSExec to launch my DLL on
remote machines.



Ransomware RunDll32 Using C\$



Ransomware RunDll32 Using C\$



Ransomware RunDll32 Using C\$



PsExec:>

%WINDIR%\syswow64\rundll32.exe

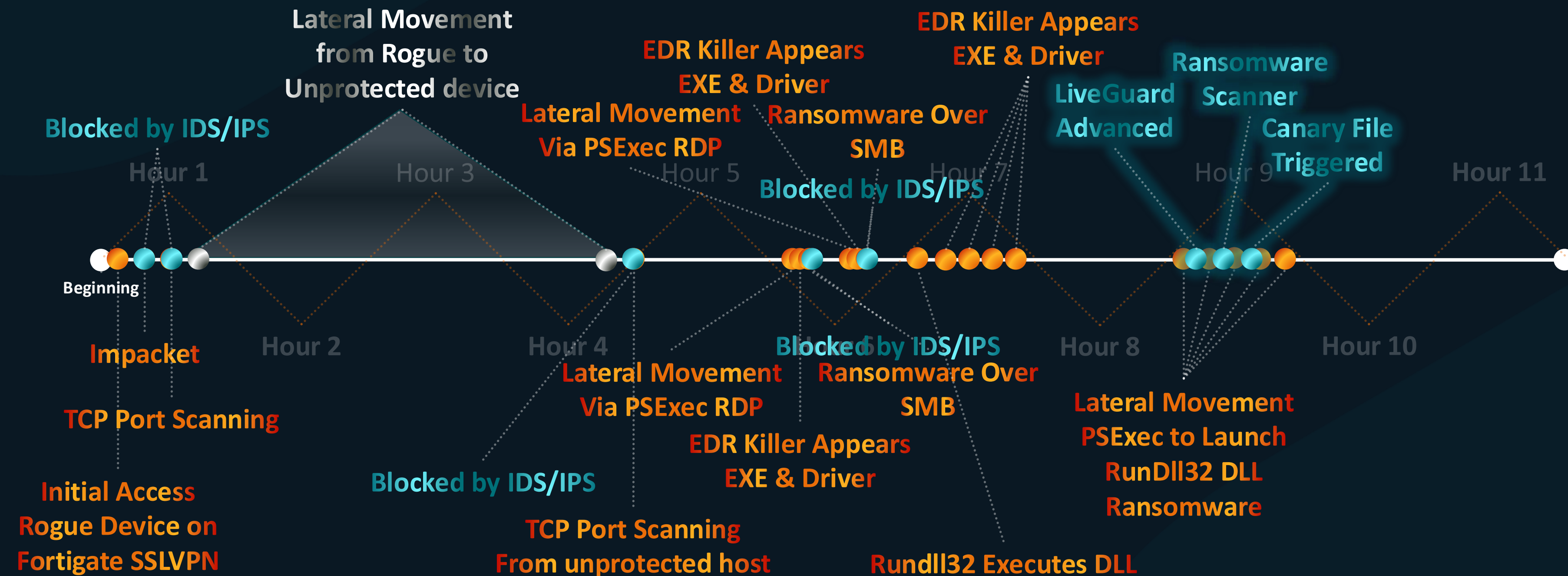
\\192.168.1.200\c\$\Windows\SoftwareDistribution\svhost.dll,ZwExecuteTh





Kovos chronologija

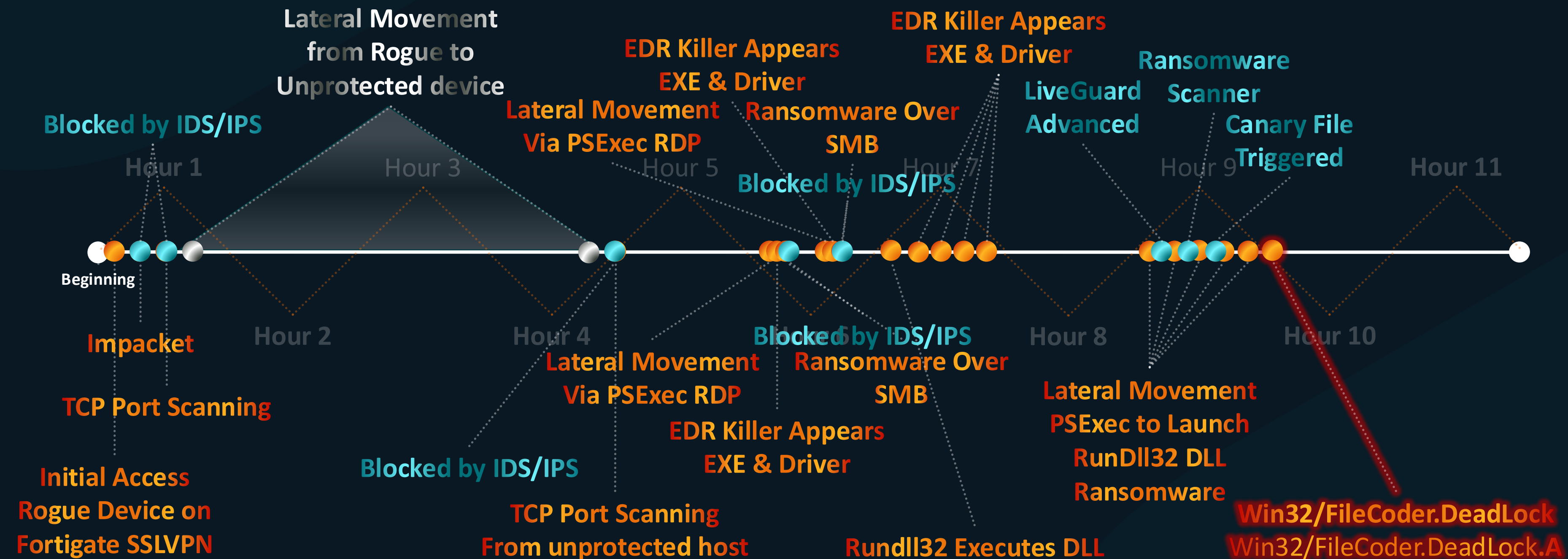
Wait... My DLL stopped
before it was finished.





Kovos chronologija

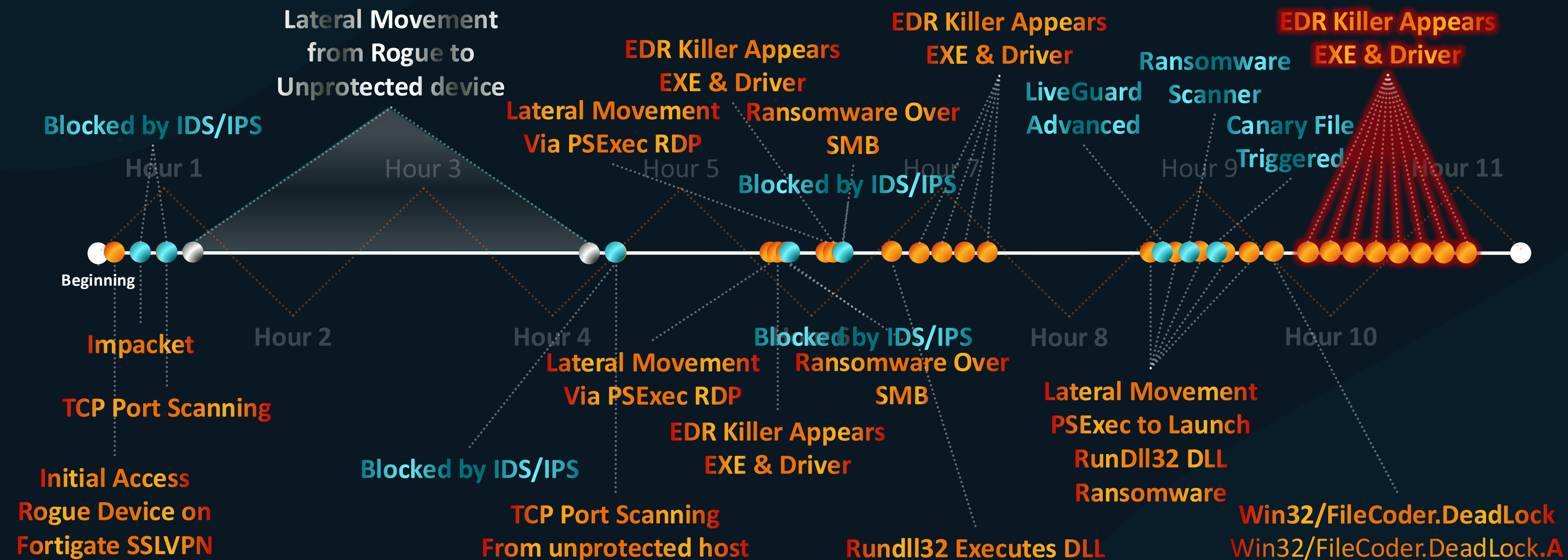
Seems to have worked on some devices. But something is now deleting my DLL and my EXE





Kovos chronologija

Back to trying to get my
EDR Killer working.



Išvados

- ✔ 2FA galėjo užblokuoti pradinį prisijungimą
- ✔ ESET tinklo atakų apsaugos funkcija sėkmingai užblokavo atakas
- ✔ Jei ekspertai būtų stebėję, to būtų buvę galima išvengti
- ✔ Būtų buvę naudinga užtikrinti, kad ESET būtų įdiegtas visuose įrenginiuose
- ✔ Būtina atnaujinti savo VPN programas
- ✔ Naudokite 2FA VPN sprendime



Pabaigai



- ✓ 2FA prisijungiant iš išorės = prevencija
- ✓ Nesaugomi įrenginiai = čia slepiasi įsibrovėlis
- ✓ Neapsaugotas VPN = vartai į tinklą
- ✓ RDP/RDS/SSH = bus išnaudojamas programišių
- ✓ Jei niekas nestebi ir nereaguoja = blogai
- ✓ „Hands On“ veikla:
 - ~~!= Malware~~
 - == Malicious Human logged into network

lukas@eset.it



Bendraukime:



Cybersecurity
Progress. Protected.