

Bezpečnosť ako služba: keď nemocnica spí, MDR bdie

Július Selecký
Solution Architect



Digital Security
Progress. Protected.



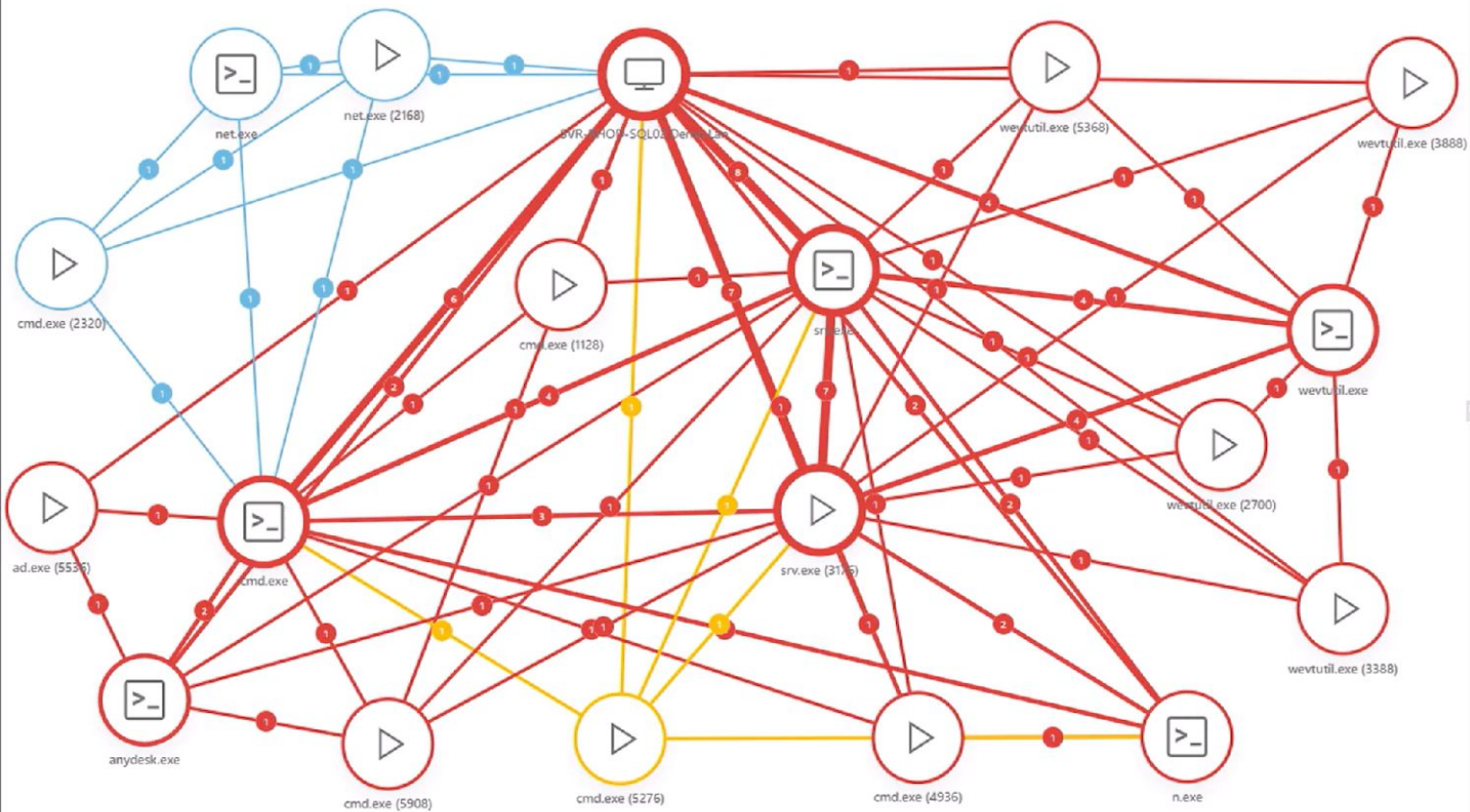
Koľko administrátorov
nekontroluje konzolu
kybernetickej bezpečnosti
každý týždeň?

75 %

75 %

[BACK](#)

Anomalous Event Log Clearing - svr-rhod-sql02.demo.lan

[Incident graph](#) [Timeline](#) [Detections](#) [Computers](#) [Executables](#) [Processes](#)[Incident](#) [Timeline](#)

Anomalous Event Log Clearing - svr-rhod-sql02.demo.lan

Status Resolved**Severity** High**Assignee** None**Tags** [Select tags](#)**Description**

MDR observed a pattern of events where an adversary attempts to clear Windows Event logs on a specific host using the wevtutil.exe utility. The wevtutil.exe utility is a legitimate Windows command-line tool used for managing event logs. However, its misuse to clear event logs can indicate malicious intent, as adversaries often attempt to erase their tracks and evade detection by removing any evidence of their activities. Host has experienced multiple attempts to clear Windows Event logs using wevtutil.exe with distinct command lines. Windows Event log channels that are most often deleted by adversaries are: System, Application and Security.

It is important to note that while clearing event logs using wevtutil.exe may not always be indicative of malicious activity, multiple attempts, especially with different command lines, raise significant concerns.

Threat indicators (10)**Antivirus** Malware: Win64/Rozena.BY**Rule** Clearing event logs [B1001]**Mitre att&ck™ techniques**[T1070.001 - Indicator Removal: Clear Windows Event Logs](#)[View more](#)**Computers (1)**svr-rhod-sql02.demo.lan[View more](#)**Executables (6)**srv.exewevtutil.exe[View more](#)



DASHBOARDS



DEVICES



INCIDENTS



VULNERABILITIES



Patch Management



Indicators



Reports



Tasks



Installers



Policies



Notifications



Status Overview



ESET Solutions



More

< BACK

Incidents >

🔗 eu_w10

i Overview

🔗 Incident Visualization

⚠️ Indicators (11)

💻 Affected Computers (2)

📄 Affected Executables (4)

👤 Affected Identities (2)

📅 Incident Timeline

Overview



Compromised Identities, Lateral Movement, and Ransomware Activity Detected

| | |
|--------------|---------------------------------------|
| Severity | 🔴 High |
| Status | ESET |
| Assignee | John Doe |
| Time created | 2 days ago - Dec 1. 2024, 10:11:11 AM |
| Last update | 3 min ago - Dec 3. 2024, 10:11:11 AM |
| Author | 🔄 In progress |
| Tags | Needs more investigation |



Company impact

| | |
|-------------|---|
| Computers | 2 |
| Identities | 2 |
| Processes | 5 |
| Executables | 4 |



Comments

+ Add comment



Description

On Desktop-D561G, rundll32.exe executed with an unusual command line, and wslservice.exe **made an HTTP request to <https://api.github.com>**, while taskhostw.exe accessed **LSASS**, suggesting credential dumping. **XDR correlation with EntralD** revealed identity **anomalies—John.Doe@company.com** had multiple failed logins before a successful RDP session from an **unusual external IP (45.33.XX.XX)**, followed by psexec.exe execution on **Server-X123**, indicating **lateral movement**. Meanwhile, **svc-backup@company.com** was flagged in **EntralD for rare administrative actions**, correlating with shadow copy deletion and log clearing, suggesting **potential service account compromise**. The combination of **compromised identities, endpoint tampering, and credential theft** suggests an **ongoing ransomware attempt or unauthorized persistence**, requiring immediate containment.



MITRE ATT&CK techniques

1. Initial Access > Execution



ČAS VENUJTE
REÁLNYM
HROZBÁM, NIE
ZBYTOČNÉMU
ŠUMU.



Základom je svetová špička v prevencii – ESET PROTECT

Pred útokom

Reputation
and cache

Network Attack
Protection

UEFI Scanner

Advanced
Machine Learning

Brute-Force Attack
Protection

Device Control

DNA Detections

In-Product Sandbox

Počas útoku

Ransomware
Shield

Ransomware
Remediation

Script Scanner
& AMSI

Advanced
Memory Scanner

Exploit Blocker

Deep Behavioral
Inspection

Po útoku

LiveGrid®
Protection

Secure Browser

Botnet Protection





Sila riešenia
ESET Inspect

Hlboký prehľad o tom
Čo, Kde a **Ako**
prebiehajú hrozby a útoky




Poznatky
ESET odborníkov

Špičkoví bezpečnostní
výskumníci ESET zabezpečujú
nepretržitú **24/7**
reakciu na hrozby




ESET MDR

Najlepšie hodnotená
spravovaná bezpečnosť, **ktorá**
vás chráni



11

Total number of devices




8

Ok



1


Attention required



2

Security risks

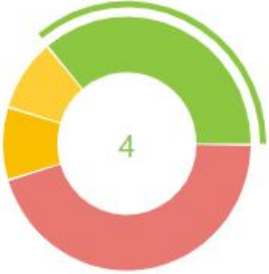
Device status



Desktops

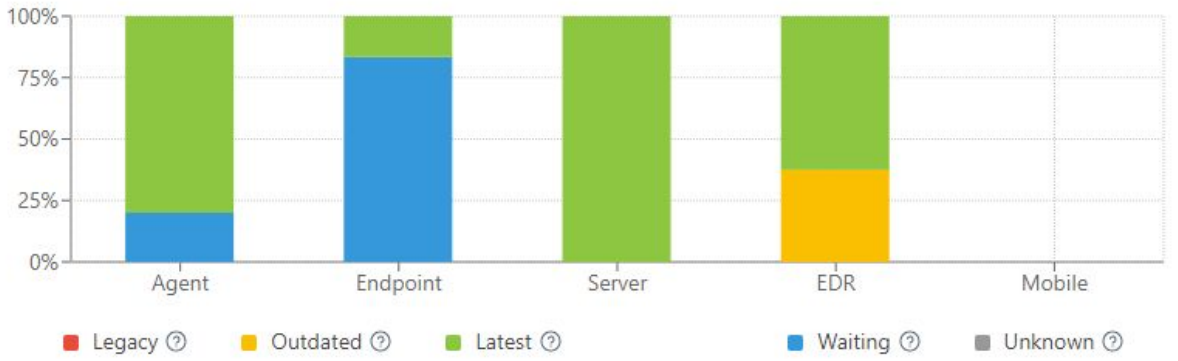
| | |
|--------------------|----------|
| Ok | 4 |
| Attention required | 1 |
| Security risk | 1 |
| Total | 6 |

Connection status




| | |
|----------|---|
| 1 day | 4 |
| 3 days | 1 |
| 7 days | 1 |
| > 7 days | 5 |

Component version status



| Component | Legacy | Outdated | Latest | Waiting | Unknown |
|-----------|--------|----------|--------|---------|---------|
| Agent | 0% | 0% | 75% | 25% | 0% |
| Endpoint | 0% | 0% | 10% | 85% | 5% |
| Server | 0% | 0% | 100% | 0% | 0% |
| EDR | 0% | 35% | 65% | 0% | 0% |
| Mobile | 0% | 0% | 0% | 0% | 100% |

Management status



10
Managed & Protected

11

0

0

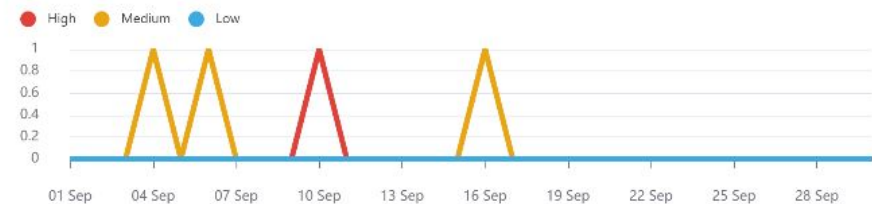
RSS feed

ESET Support News

September 23rd, 2024

[ESET Inspect version 2.3 has been released](#)

ESET Inspect version 2.3 has been released.



**Čas na detekciu a reakciu je
rozhodujúci**

Čas na detekciu a reakciu (MTTR)



Zhrnutie

- 1 Nemáte čas ani rozpočet na vlastné monitorovanie prostredia
- 2 Ak nikto nemonitoruje prostredie, neviete, že sa niečo deje. Nezachytený útok sa môže rozvinúť do niečoho horšieho – napríklad ransomvéru
- 3 ESET má čas aj know-how na nepretržité monitorovanie vášho prostredia

Ďakujem za pozornosť



Digital Security
Progress. Protected.