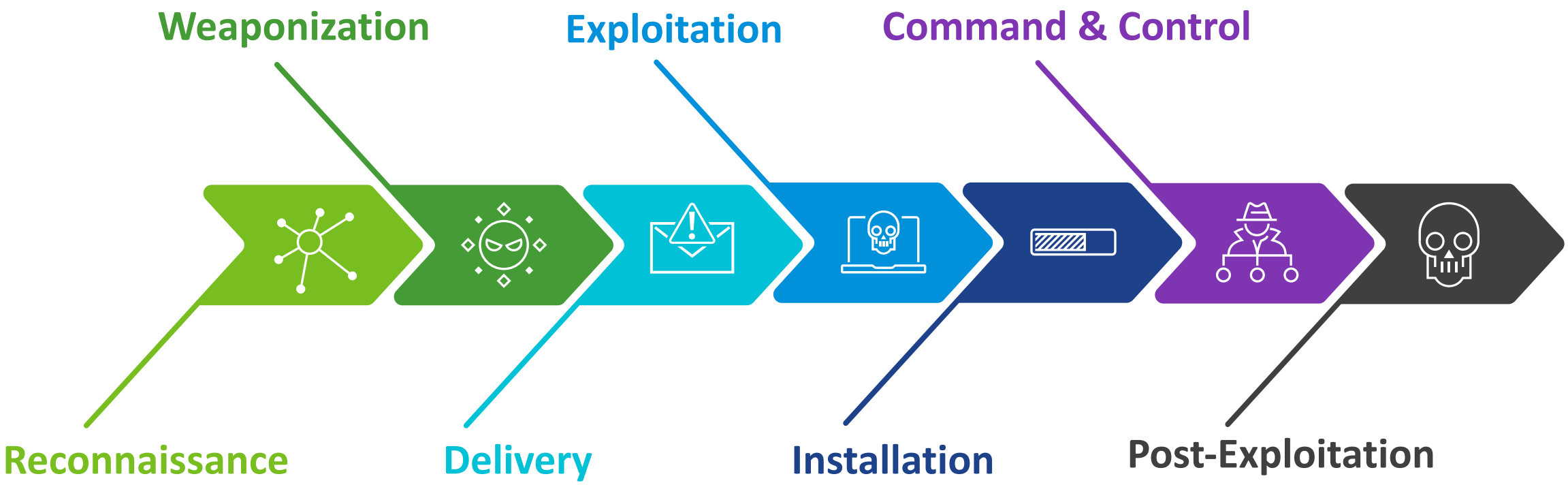
Scenari di attacchi avanzati:

Le best practice per una protezione avanzata

Kill Chain
A Red Team Perspective



certego

Kill Chain
A Red Team Perspective


Domain, subdomain, harvesting e-mail addr., …


Exploit, payload, backdoor, …

Preparation


Hours to Months


E-mail, SMS, USB, …


Exploit a vulnerability to execute code on target machine


Installing malware on the asset

Intrusion


Seconds


Command channel for remote manipulation of target's system


Exfiltration, gathering information, …

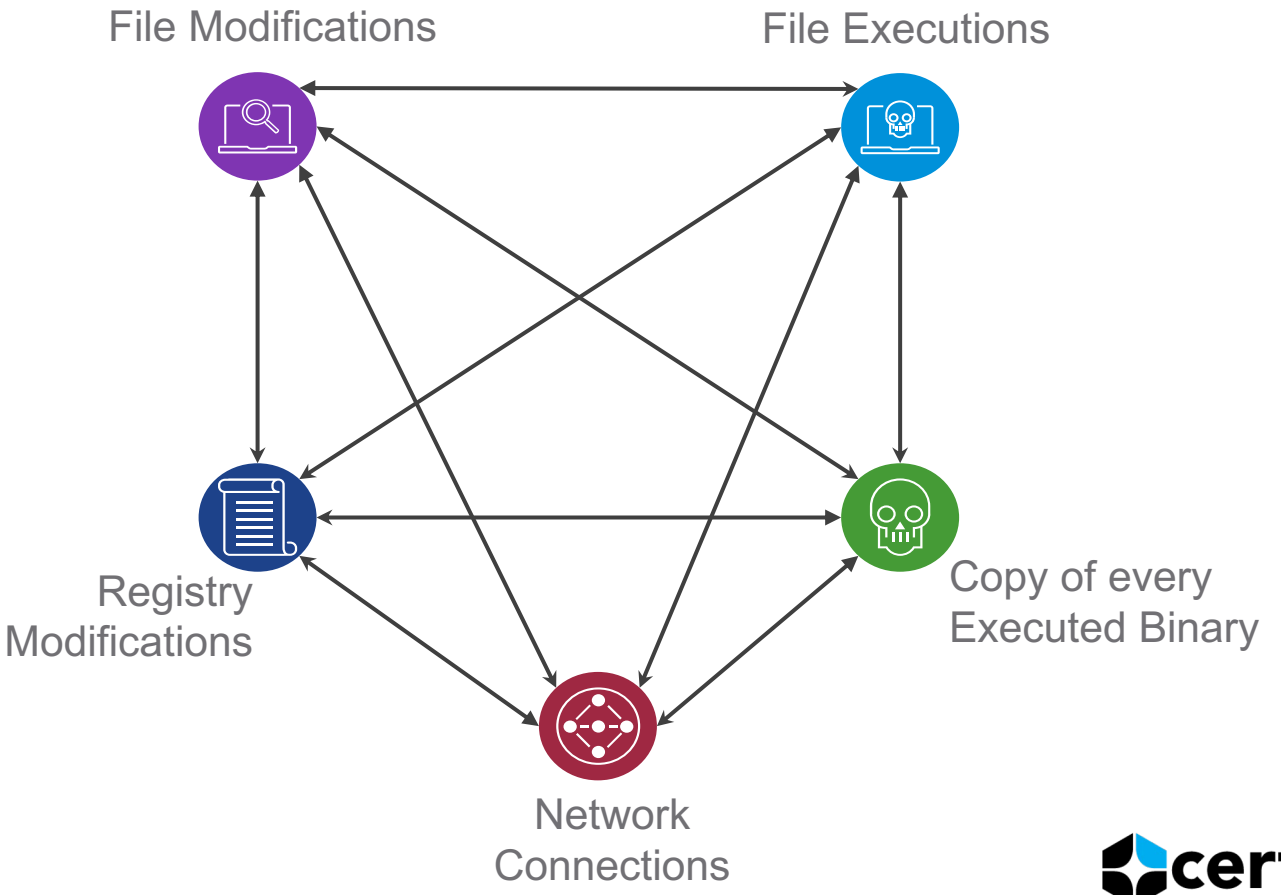
Active Breach


Hours to Years

certego

Endpoint Detection & Response

- Process Analysis & Timeline
- Continuous Monitoring
- Custom Signatures
- Scalable
- Response capabilities

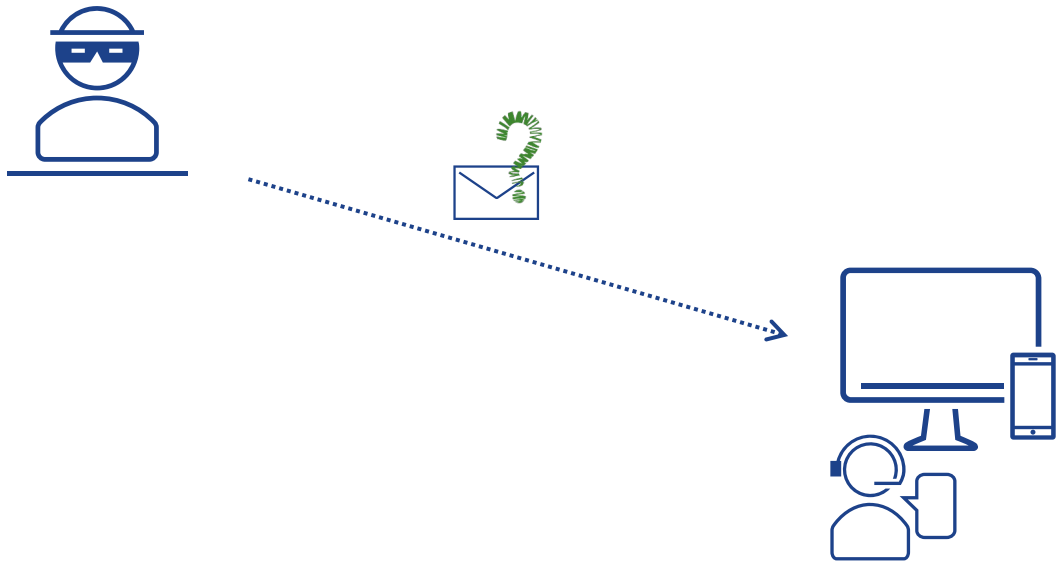


certego

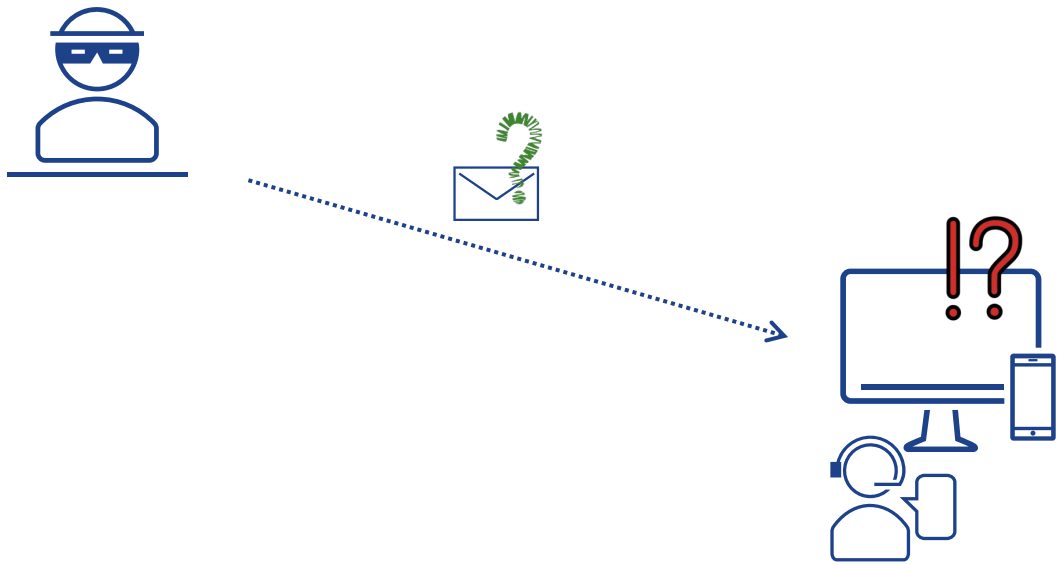
Real world scenario

certego

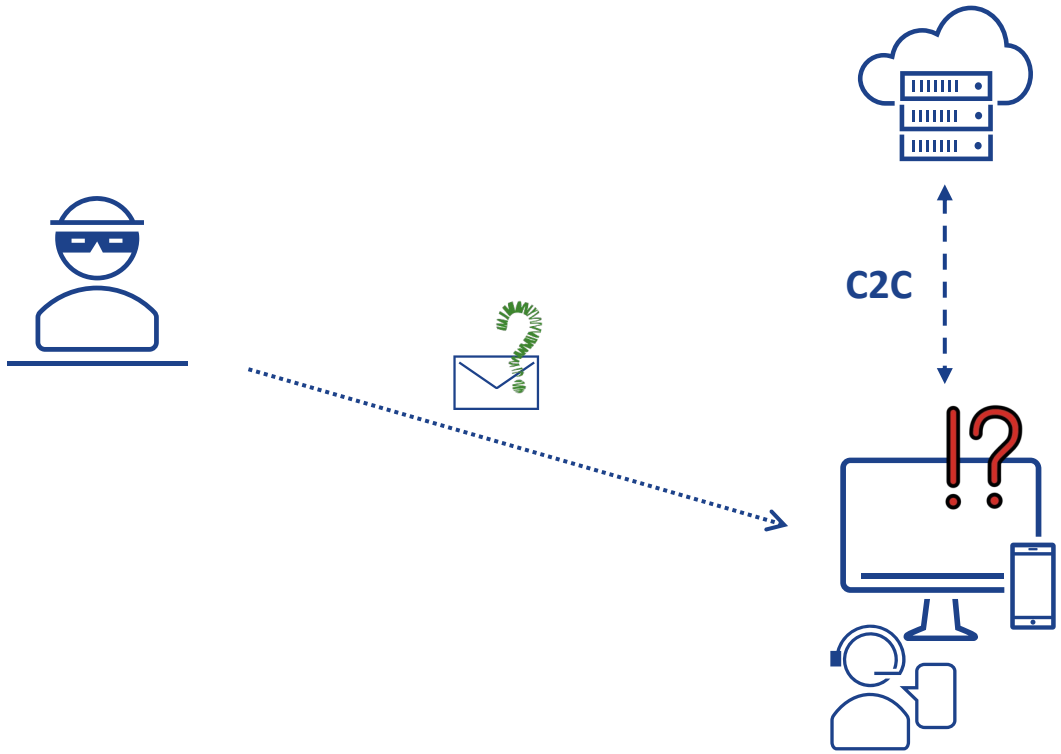
Real world scenario



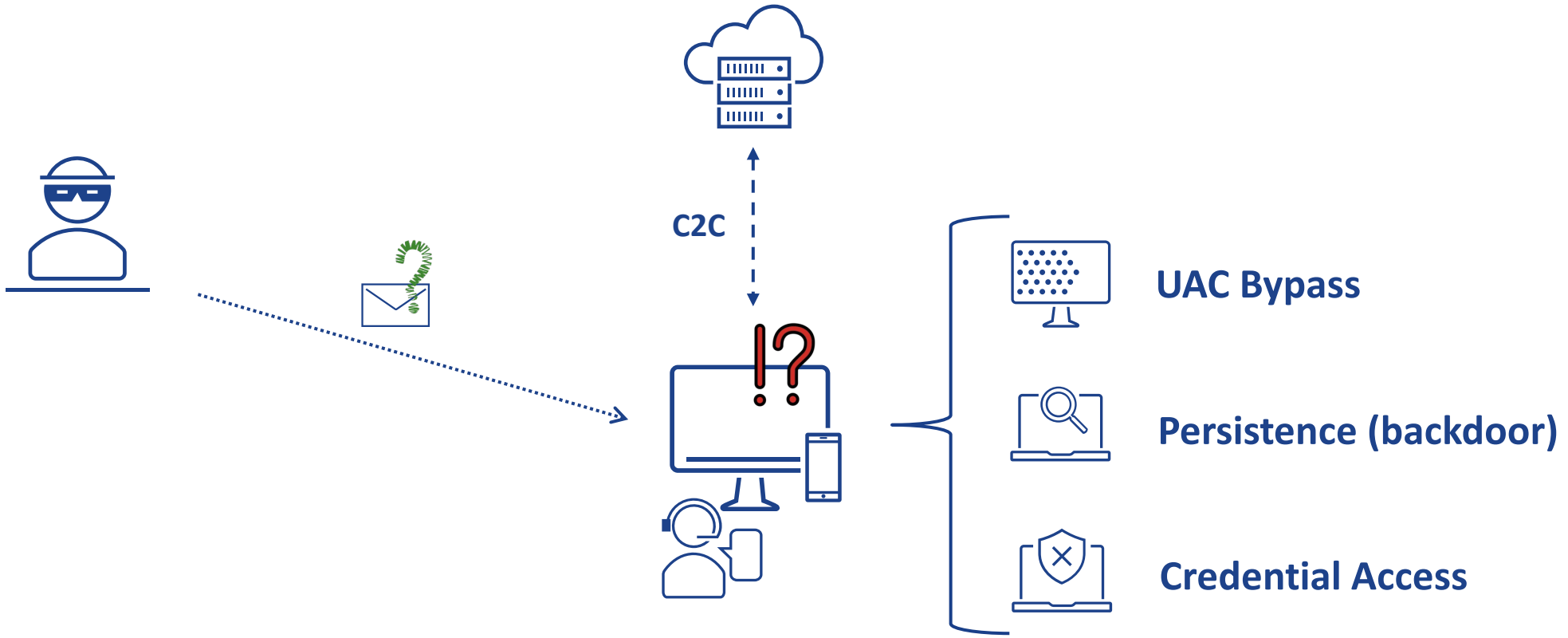
Real world scenario



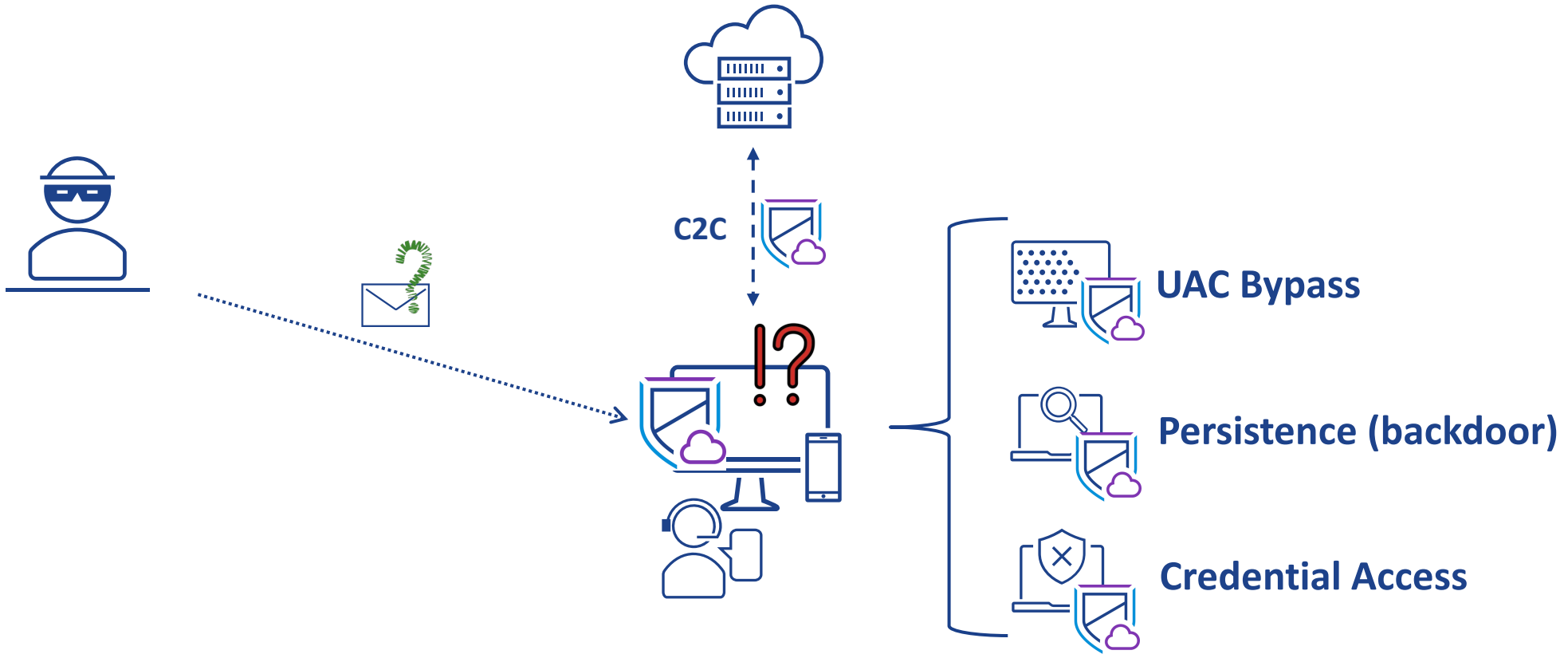
Real world scenario



Real world scenario

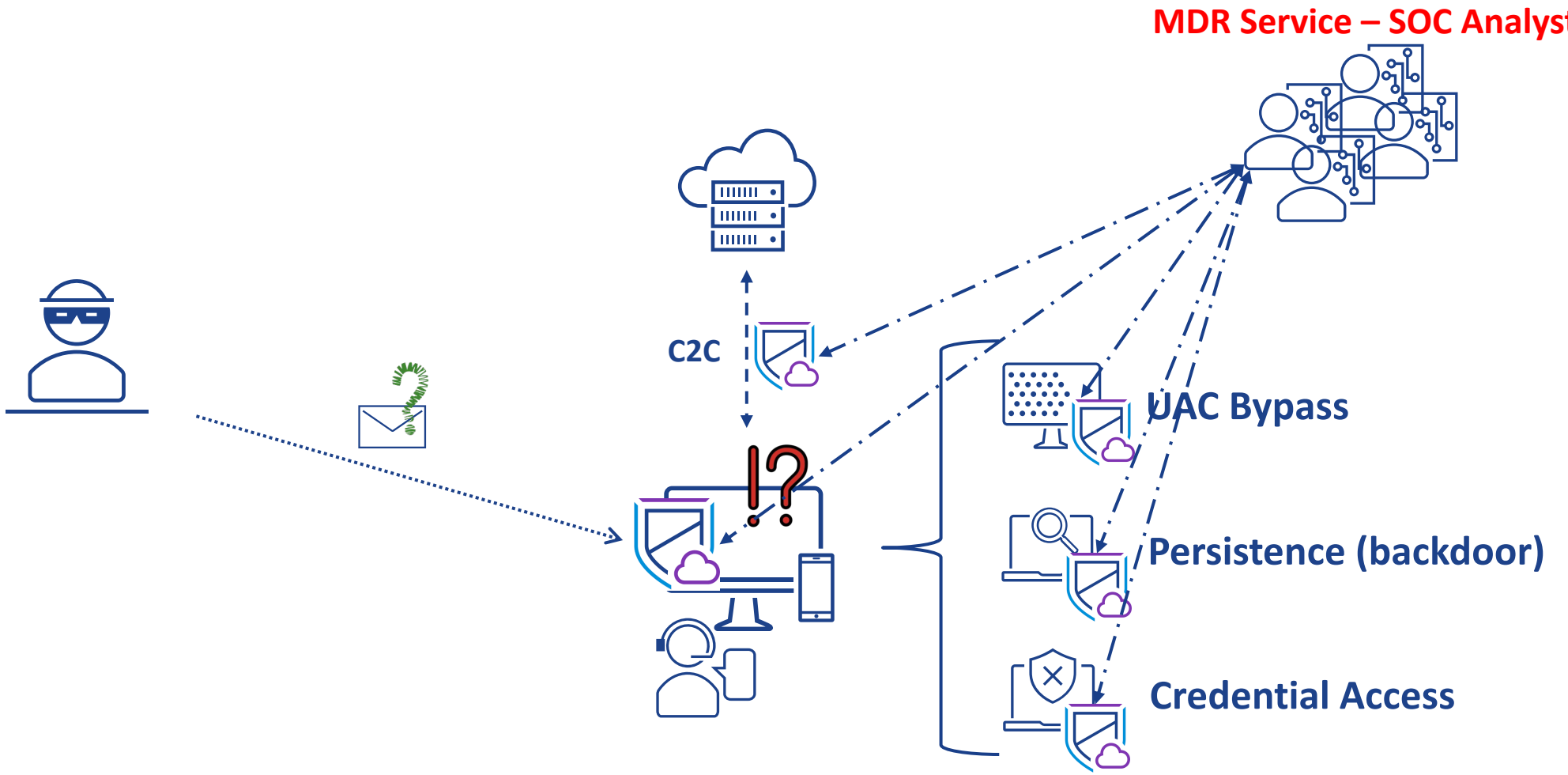


Real world scenario

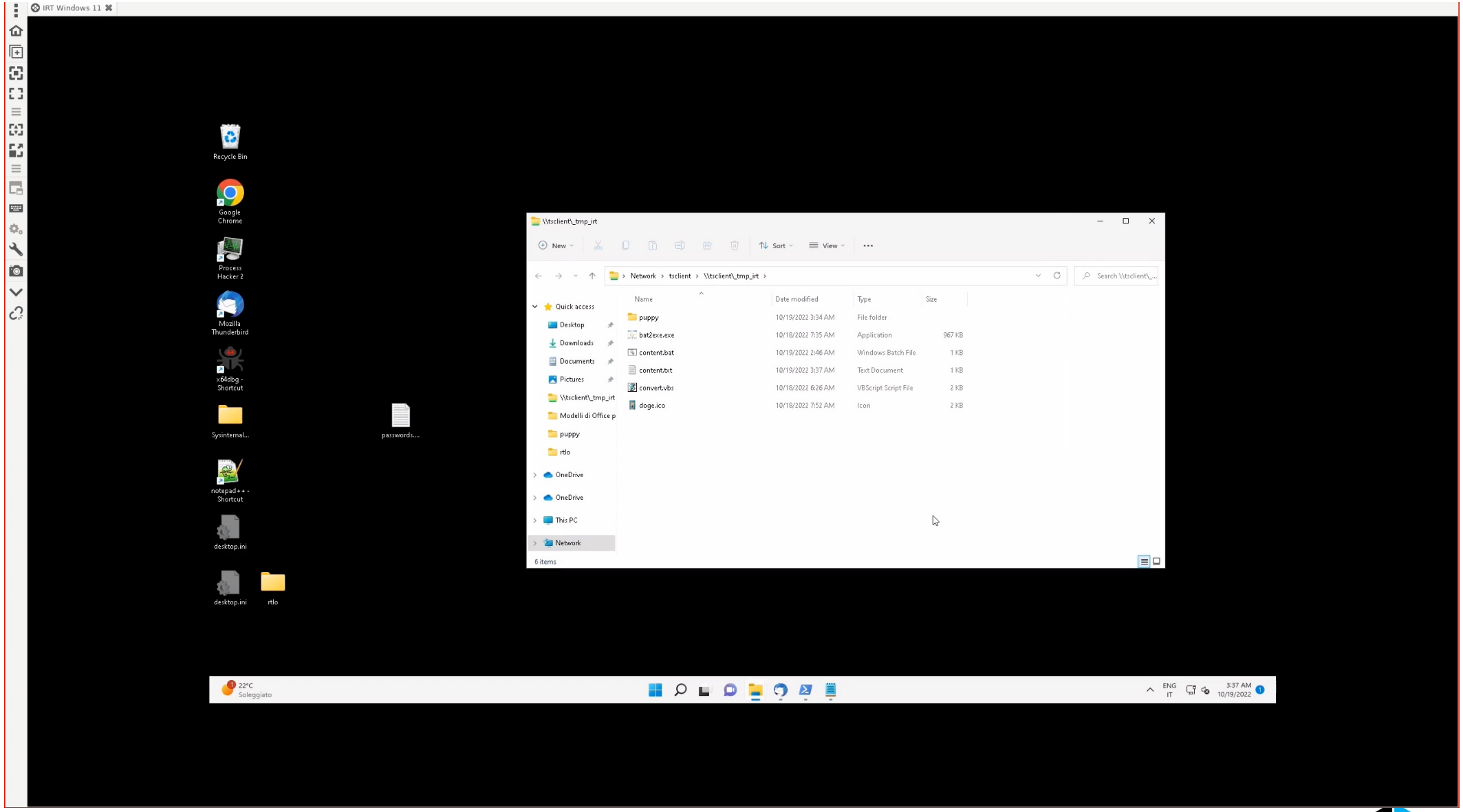


certego

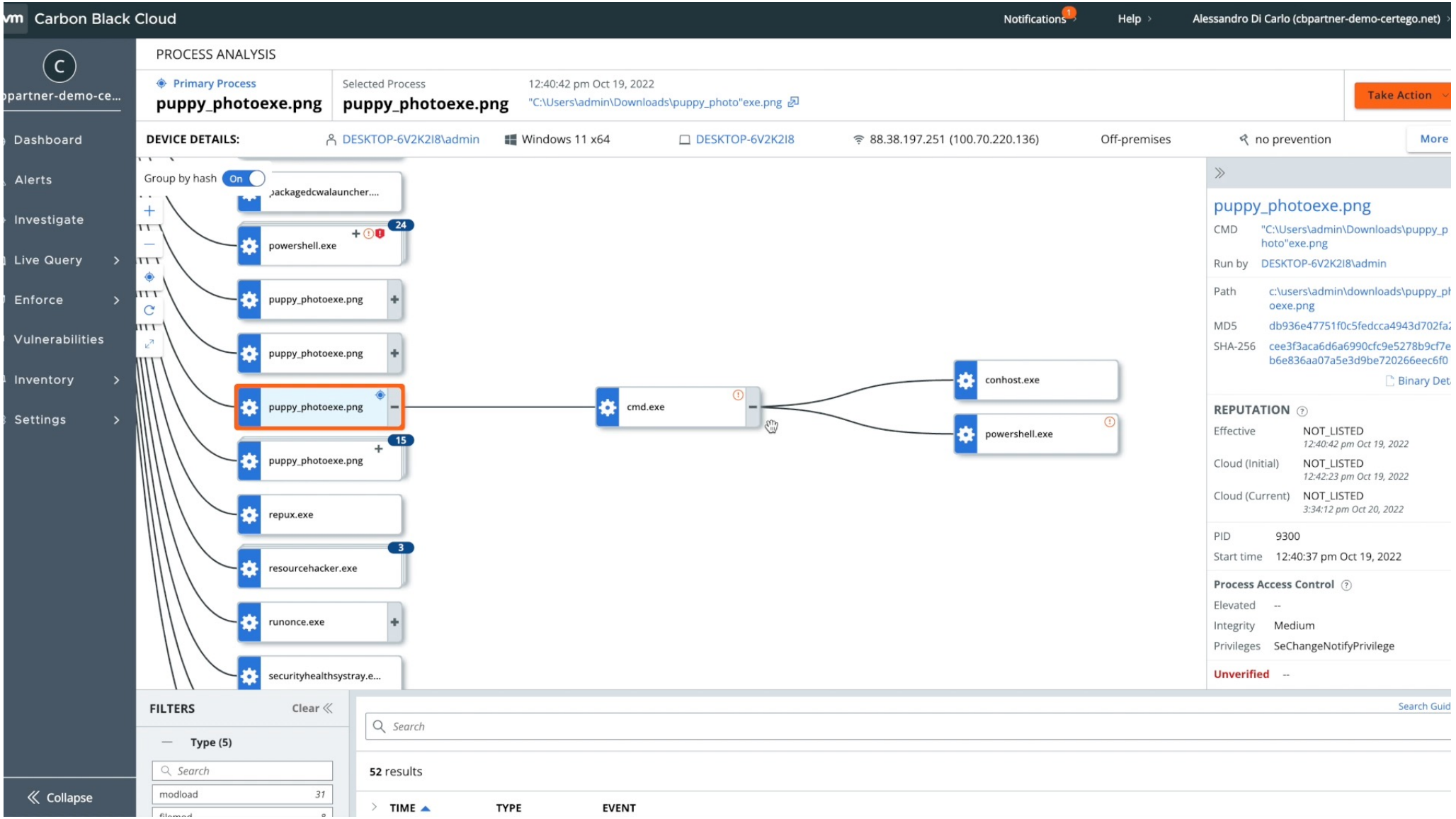
Real world scenario



Delivery and execution – Red Team perspective



Delivery and execution – Blue Team perspective

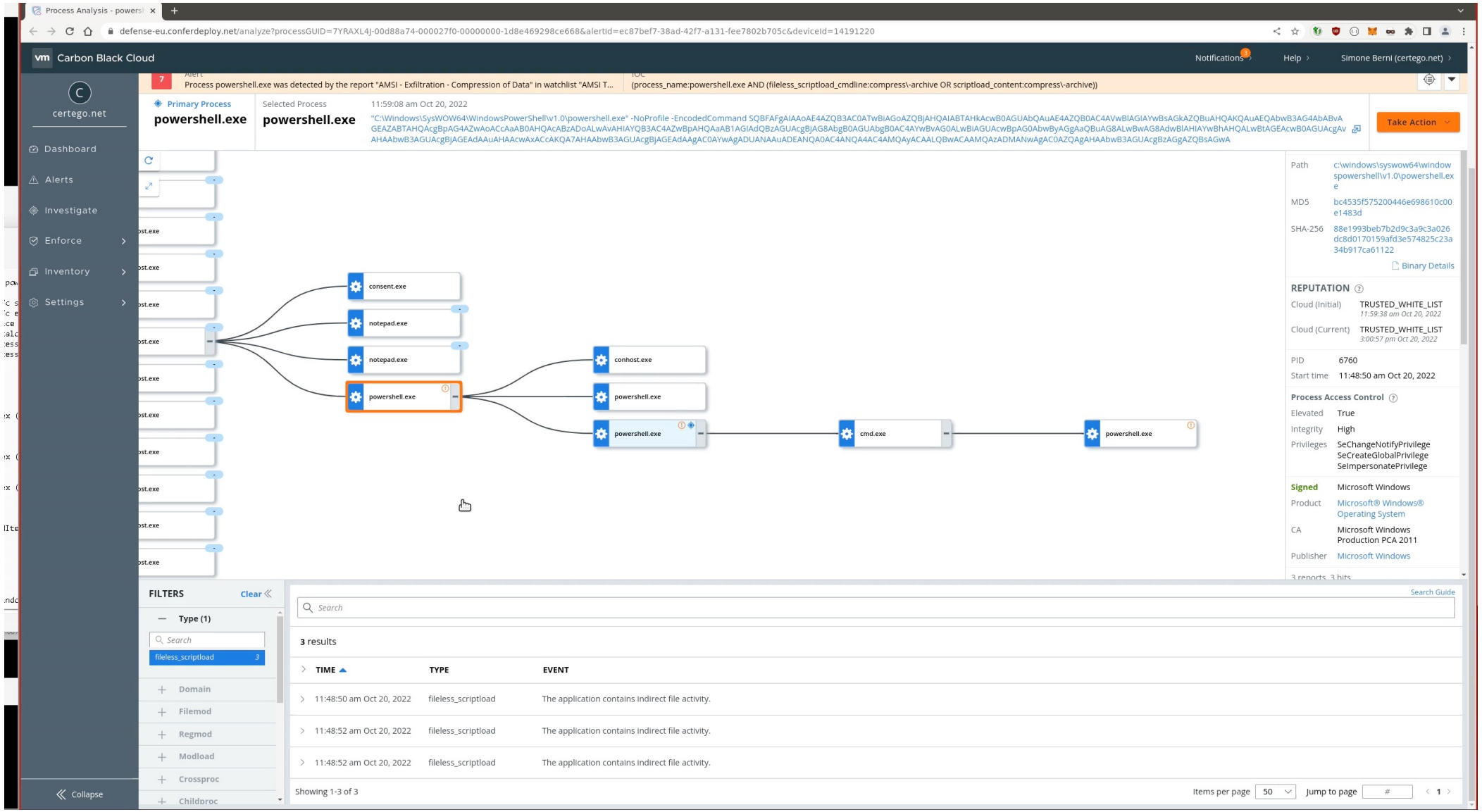


Credential Access - Red Team perspective

```
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>
```

certego

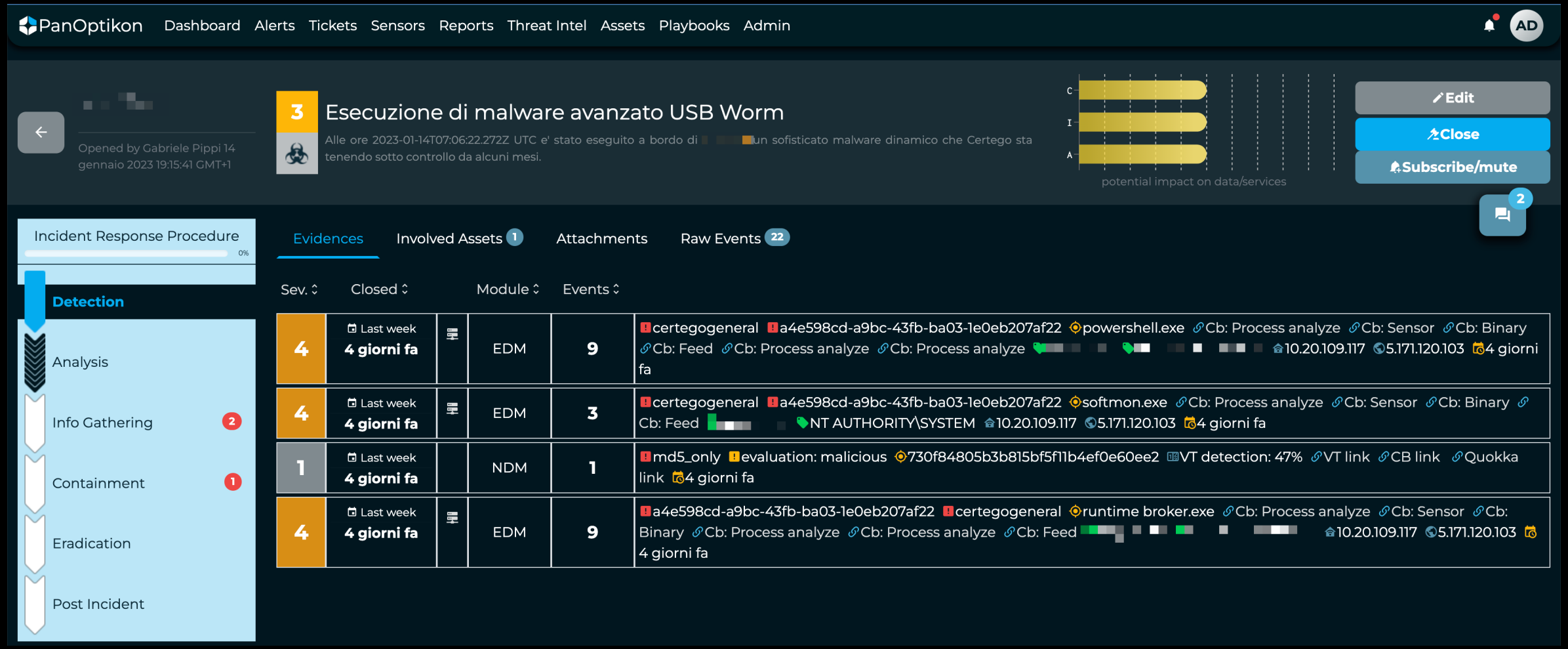
Credential Access - Blue Team perspective



PanOptikon®

Overview

certego


PanOptikon
Dashboard
Alerts
Tickets
Sensors
Reports
Threat Intel
Assets
Playbooks
Admin
AD
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
2
Incident Response Procedure
0%
Detection
Analysis
Info Gathering 2
Containment 1
Eradication
Post Incident
Evidences
Involved Assets 1
Attachments
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 fa
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 5.171.120.103 4 giorni fa
1 Last week 4 giorni fa NDM 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

certego

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.

Edit
Close
Subscribe/mute

2

Incident Response Procedure 0%

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

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'incona 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

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.

certego

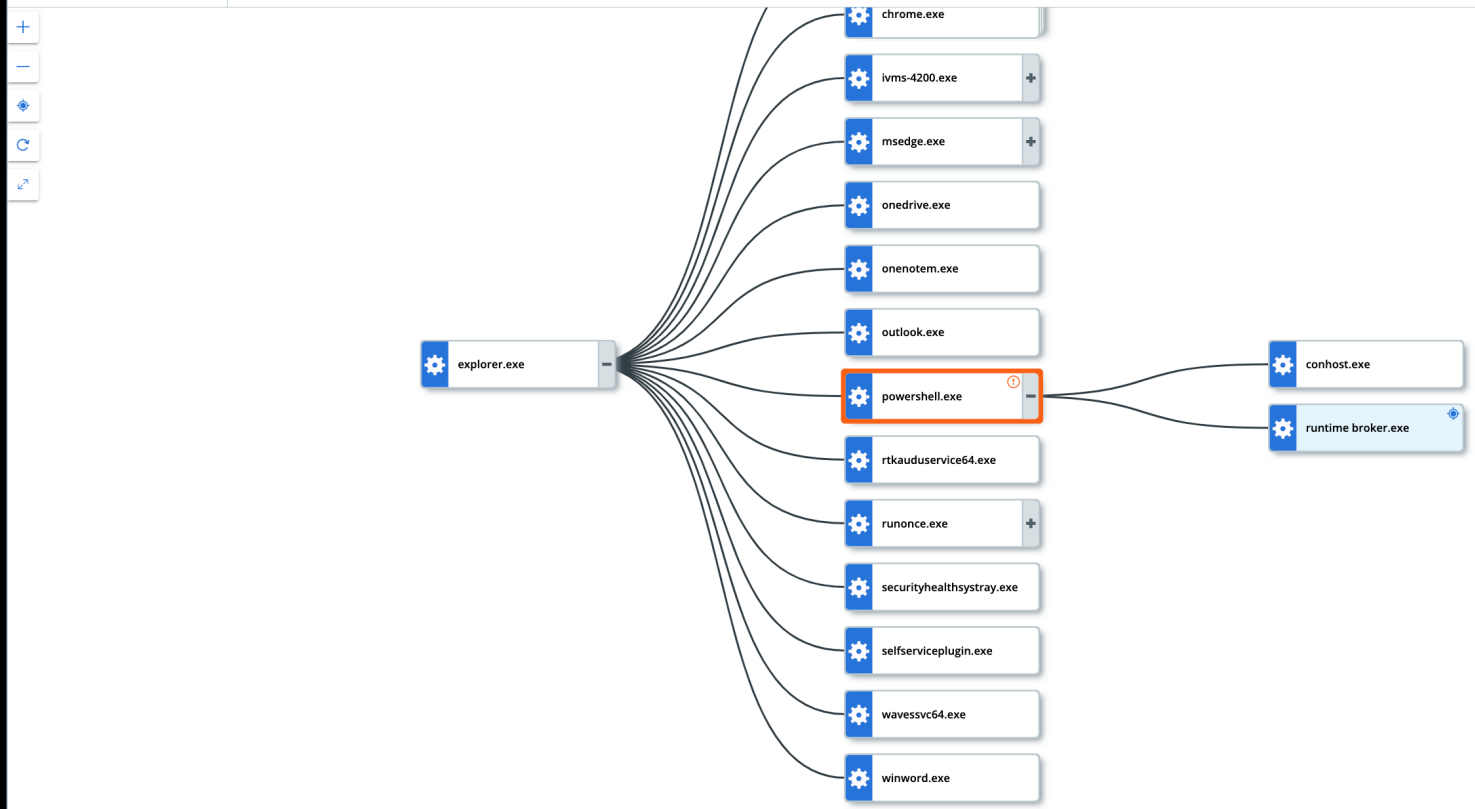
PROCESS ANALYSIS

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

netconn	3
modload	203
filemod	30
regmod	27
crossproc	21
scriptload	7

Search Guide

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)

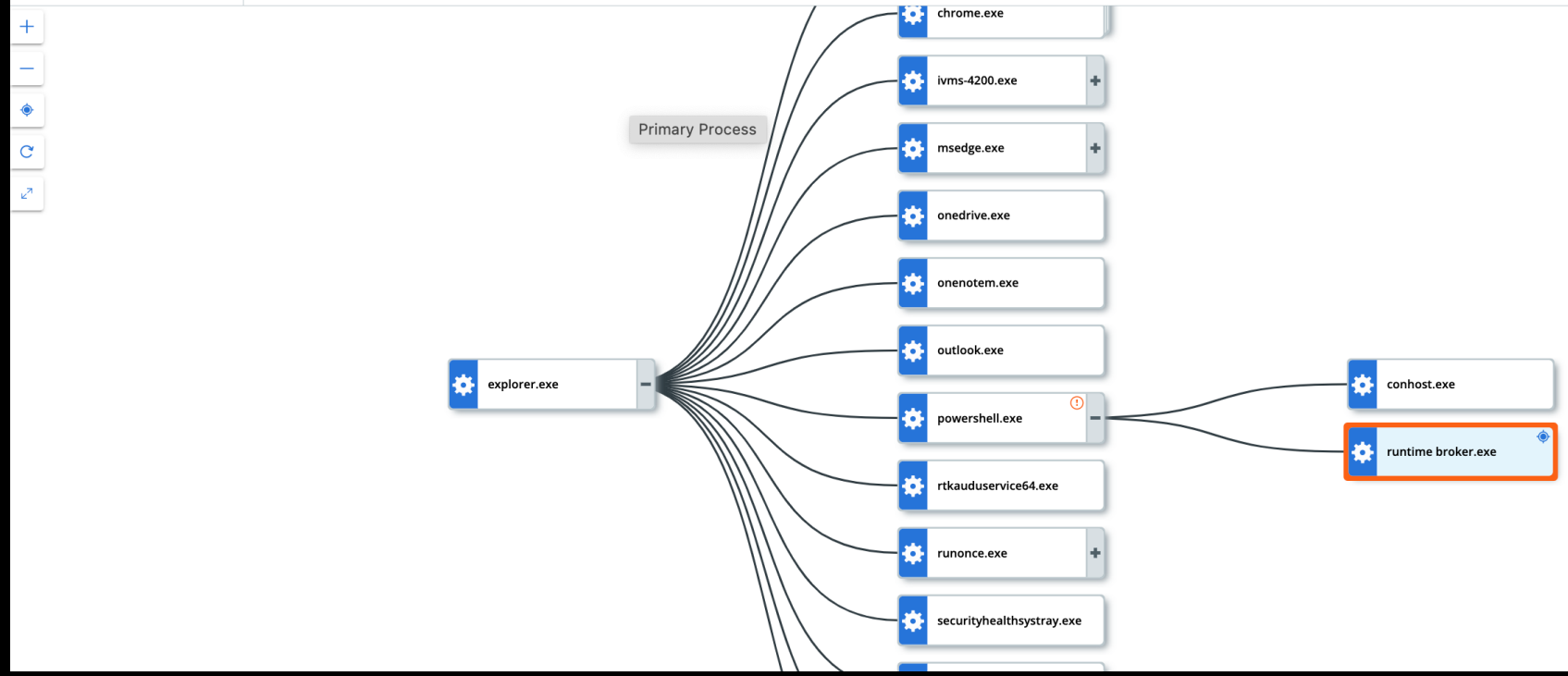
certego

PROCESS ANALYSIS

Primary Process
runtime broker.exe

Selected Process
runtime broker.exe
9:53:03 am Jan 2, 2023
"C:\Users\ \AppData\Local\Temp\Runtime Broker.exe"

Take Action



runtime broker.exe

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

Run by

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

MD5 730f84805b3b815bf5f11b4ef0e60ee2

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

CERTEGO S.R.L.

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