Scavare in un *dump* di RAM

Caos globale: aeroporti, ospedali e grandi organizzazioni vengono messi in ginocchio da improvvisi BSOD (schermi blu). Un computer del controllo del traffico aereo mostra segni di malware, mostrando messaggi minacciosi che incitano la gente a scendere in piazza.

Username & Host name

Obiettivo: trovare il nome dell'utente e il nome del computer.

Per trovare l'utente sono stati analizzati i *link file* (LNK FILE) tra gli artefatti del sistema operativo, di cui si riporta un'anteprima di seguito:

Linked Path	Target File Created Date/Time
C:\Users\award\Desktop	04/02/2025 21:18:51.000
C:\Users\award\Downloads	04/02/2025 21:18:51.000
C:\Users\award\Documents	04/02/2025 21:18:51.000
C:\Users\award	04/02/2025 21:18:51.000
C:\Users\award\AppData\Roaming\Microsoft\...	04/02/2025 21:20:11.000
C:\Users\award\AppData\Roaming\Microsoft\...	04/02/2025 21:20:11.000
C:\Users\award\AppData\Local\Packages\Mic...	05/02/2025 19:46:22.000
C:\Users\award\WP_TSO-ATC-CT412.JPG	05/02/2025 19:47:04.000

Figura 1 - LNK File

Dall'immagine precedente è evidente come un utente sia sicuramente "award".

Al fine di rinvenire, invece, il nome del computer in analisi sono stati analizzati i log degli eventi Windows. Sono stati presi in considerazione gli User Event:

Created Date/Time	Event Description Summary	Logon Type	Subject Username	Subject Domain Name
22/07/2025 18:50:48.482	An account was successfully logged on.	5-Service	TSO-ATC-CT412$	KTSO.AERO
22/07/2025 18:50:48.510	An account was successfully logged on.	5-Service	TSO-ATC-CT412$	KTSO.AERO
22/07/2025 18:50:48.587	An account was successfully logged on.	5-Service	TSO-ATC-CT412$	KTSO.AERO

Figura 2 - User Event

Analizzando nello specifico uno degli eventi presenti è evidente come il nome dell'host sia `<Computer>TSO-ATC-CT412</Computer>`.

Figura 3 - User Event - computer name

Locker

Obiettivo: trovare il nome del file eseguibile del malware.

All'interno del dump di memoria sono state recuperate quattro e-mail. Si vuole evidenziare il messaggio di posta elettronica inviato da *Information Technology Department* `<ktso.sec@mailforce.net>`, nel quale l'utente viene esortato a scaricare un file ed eseguirlo immediatamente:

From: Information Technology Department <ktso.sec@mailforce.net>
Sent: 22/07/2025 16:42:39.000
To: alex.ward67@posteo.us
Subject: URGENT: Corporate software update

REQUIRES IMMEDIATE ATTENTION AND ACTION

We wish to draw your immediate attention to an emerging global incident currently affecting numerous Windows-based computer systems across various industries and locations worldwide. Specifically, Windows machines are experiencing critical instability, resulting in frequent occurrences of the Blue Screen of Death (BSOD), an error state rendering affected systems temporarily unusable, with potential risks including significant operational downtime and data loss.

In response to this critical situation, our Information Technology Department has conducted a thorough assessment and has urgently identified and prepared an internal software update designed explicitly to mitigate this vulnerability. This software update is essential in safeguarding your workstation and ensuring the continued stability, security, and integrity of our organizational systems.

Mandatory Action Required:
It is imperative that you install the provided software update at your earliest convenience—ideally immediately upon receipt of this notification. Prompt compliance will significantly reduce the likelihood of your workstation being compromised by the current global BSOD event.

Software Update Installation Procedure:
1. Download the necessary update using this one-time link: https://limewire.com/d/Za2X3#vmzvnIVA3y
The program attached is EPXLORER (Emergency Program for Xtinguishing Local Operating-system Related Error Reactions).

2. Save epxlorer.exe to any folder on your computer. Verify that the executable is 1 111 552 bytes in size.

3. Immediately run epxlorer.exe.

Figura 4 - E-mail phishing

La mail rappresenta un chiaro tentativo di phishing. Al fine di controllare che il malware sia effettivamente il programma EPXLORER, è stata analizzata la navigazione web, cercano come keyword il link presente all'interno della mail:

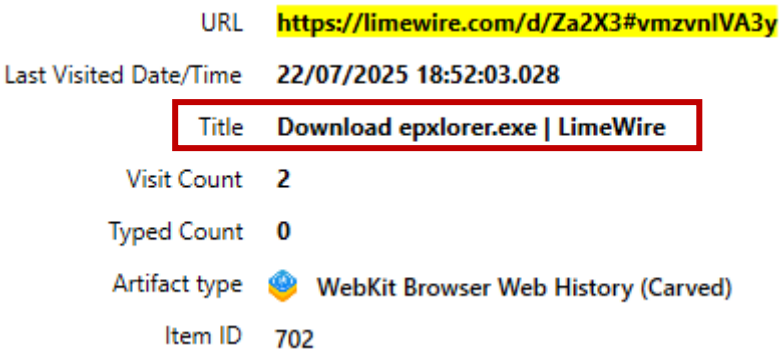


Figura 5 - Link visitato e file scaricato

Per conferma è stato analizzato anche il nodo "Malware Finder" presente nello strumento software forense *Magnet Axiom Examine* ed in effetti è stato rinvenuto l'eseguibile **`EPXLORER.EXE`:**

Process ID	Process Name	Address	Vad Tag
9920	epxlorer.exe	52428800	VadS
9920	epxlorer.exe	90767360	VadS
9920	epxlorer.exe	162660352	VadS

Figura 6 - Nome del file eseguibile del malware

Infezione

Obiettivo: trovare l'indirizzo di posta elettronica della persona che ha diffuso il malware.

Già precedentemente riportato: `<ktso.sec@mailforce.net>`.

Hash MD5 + Telegram API server

Obiettivo: trovare il valore di hash del file eseguibile e il server API Telegram ospitato dall'attaccante e utilizzato dal malware.

Come prima cosa viene analizzato l'artefatto *FileScan*, al fine di visualizzare l'Offset relativo al file, al fine di estrarlo dal dump di memoria:

File Path	Permissions	File Name	Location	Artifact type
\Device\HarddiskVolume3\Users\award\Downloads\...	-W-rw-	epxlorer.exe435568.crdownload	File Offset 253476805414416	Files (filescan)
\Device\HarddiskVolume3\Users\award\Downloads\...	R--r-d	epxlorer.exe	File Offset 253476805407216	Files (filescan)

Figura 7 - Offset epxlorer.exe

È stata dunque scaricata la repository di Volatility3, al fine di estrarre il file di interesse:

```
python vol.py -f "Y:\PCIX16x8\Gaia\BelkaCTF_7_CASE250722_KTSOAERO.mem"
                windows.dumpfiles --virtaddr 253476805407216
```

```
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0xe6892af1f1f0  epxlorer.exe    file.0xe6892af1f1f0.0xe6892ae60750.DataSectionObject.epxlorer.exe.dat
ImageSectionObject      0xe6892af1f1f0  epxlorer.exe    file.0xe6892af1f1f0.0xe6892acfa080.ImageSectionObject.epxlorer.exe.img
```

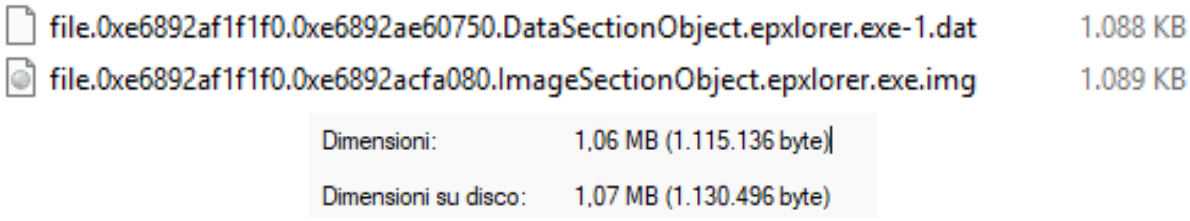


Figura 8 - Comando per estrarre il file eseguibile e file estratti

Dall'analisi precedentemente riportata, l'attaccante scriveva di verificare che il file fosse della seguente dimensione:

. Verify that the executable is 1 111 552 bytes in size.

Figura 9 - Stralcio di e-mail di phishing

Come è possibile vedere dalla Figura 8 nessuno dei due file ha la dimensione desiderata. Volatility, infatti spesso aggiunge blocchi di zeri alla fine. Dunque, prima di calcolare l'hash del file, è necessario ridurlo a *1,111,552 byte*.

È stato dunque aperto il file in un editor HEX[1], al fine di selezionare solo la parte di file interessata:

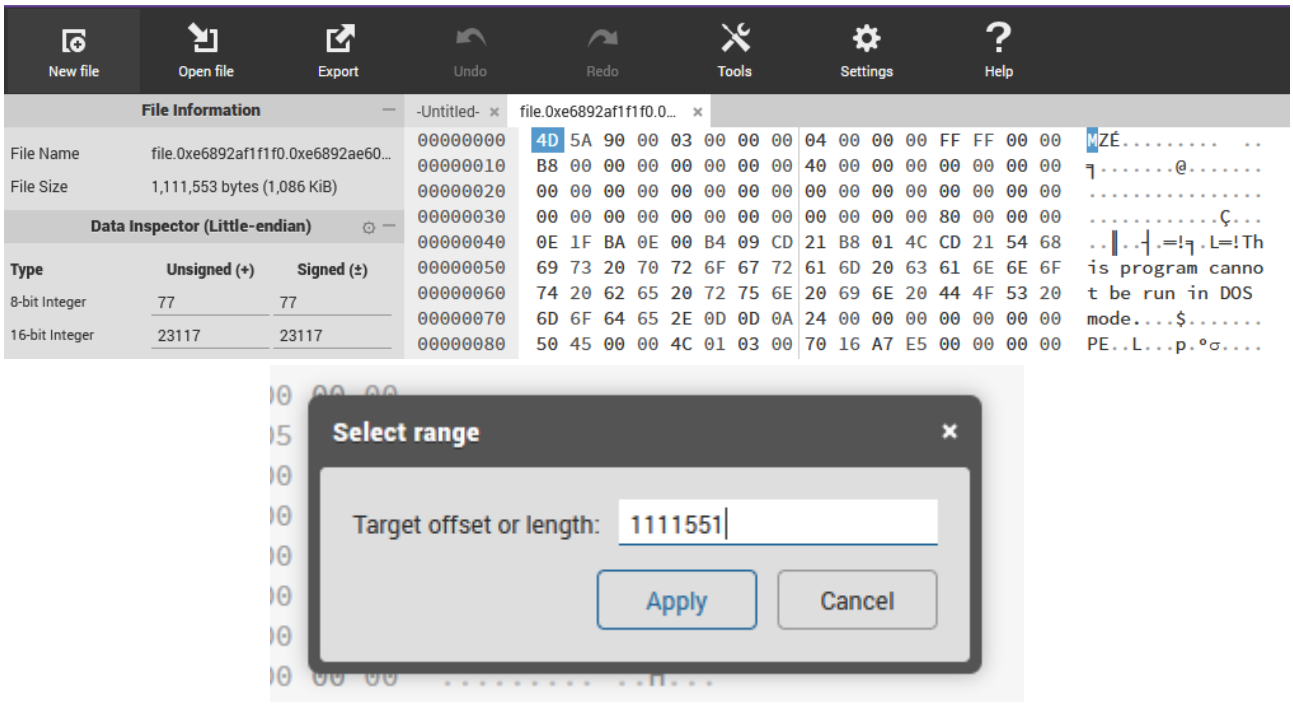


Figura 10 - HexEditor per modificare la dimensione del file

Dopo aver effettuato questo passaggio, è stato calcolato il valore di hash, con algoritmo MD5: **`75ea94b54420c39dcd3d8ce574ba9d34`**.

Figura 11 - Calcolo Hash MD5

Il malware analizzato è un *assembly Mono/.NET*. Poiché le applicazioni .NET non vengono compilate direttamente in codice macchina nativo, ma in bytecode intermedio (CIL/MSIL), esse sono generalmente decompilabili in una forma molto vicina al codice sorgente originale. Per questo motivo si procede ad analizzare il file tramite ***JetBrains dotPeek*** *(nota: è possibile utilizzare altri strumenti di analisi analoghi)*, ottenendo una rappresentazione del codice ad alto livello prossima al sorgente originale.

[1] https://hexed.it/

Analizzando il codice si nota la classe Form1 contenente le informazioni che stavamo cercando:

```
public class Form1 : Form
{
    private const string AppName = "melok";
    private readonly string telegram_api_key;
    private readonly string admin_telegram_id = "7474460026";
    private readonly string custom_api_url = "https://api-telegram-org.ctf.do/";
    private TelegramBotClient botClient;
    private Label label1;
    private bool NoClose = true;
    private IContainer components;
```

Figura 12 – api_url

Alla luce di quanto appena riportato, è possibile affermare che l'indirizzo web dell'API del malware è ***https://api-telegram-org.ctf.do/***.

API del bot Telegram

Obiettivo: trovare API del bot Telegram codificata nell'eseguibile del malware.

Il token del bot di Telegram è crittografato. Nella prima parte del codice di Form1() è possibile visionare l'algoritmo di decifratura del token:

```
int[] numArray = new int[46]
{
  16 ...,
  23,
  104,
  28,
  6,
  16 ...,
  105,
  20,
  16 ...,
  30,
  28,
  119,
  105,
```

[…]

```
int index1 = 0;
StringBuilder stringBuilder = new StringBuilder();
string str = "(&^%4&^%$*&6";
for (int index2 = 0; index2 < numArray.Length; ++index2)
{
  char ch = (char) ((uint) numArray[index2] ^ (uint) str[index1]);
  stringBuilder.Append(ch);
  index1 = (index1 + 1) % str.Length;
}
```

Per comodità di esecuzione viene riscritto l'algoritmo di decrittazione della chiave API utilizzando Python:

```
num_array = [
    16, 23, 104, 28, 6, 16, 105, 20, 16, 30, 28, 119, 105, 96,
    41, 78, 92, 75, 6, 77, 19, 27, 117, 123, 126, 69, 40, 99,
    120, 71, 48, 81, 78, 126, 74, 65, 68, 116, 60, 113, 13,
    110, 58, 111, 64, 127
]
```

```python
s = "(&^%4&^%$*&6"

index1 = 0
result = []

for n in num_array:
    ch = chr(n ^ ord(s[index1]))
    result.append(ch)
    index1 = (index1 + 1) % len(s)

token = "".join(result)
print(token)
```

Figura 13 - Riscrizione del codice in Python

```
Y:\PCIX16x8\Gaia\cf test>py "descrittazione API.py"
8169267144:AAFwkhmXh71SMVcvFLantjTlwlRbT9HdJdU
```

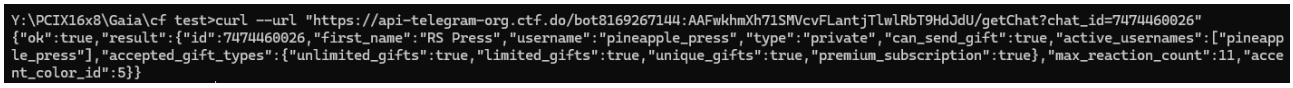
Figura 14 - API decifrata

Numero di telefono

Obiettivo: scoprire il numero di telefono dell'operatore malware.

Dall'analisi precedentemente svolta è stato rinvenuto l'`admin_id_telegram`: 7474460026. È stato quindi utilizzato il metodo ***`getChat`*** per reperire le informazioni dell'account in oggetto:

```
curl --url "https://api-telegram-
org.ctf.do/bot8169267144:AAFwkhmXh71SMVcvFLantjTlwlRbT9HdJdU/getChat?chat_id=747
4460026"
```




```
"id":7474460026,"first_name":"RS
Press","username":"pineapple_press","type":"private"
```

Figura 15 - curl per info account

Cercando lo username su Telegram, si visualizza un account avente numero di telefono **+995 568 988 280.**