

Esercizio_S10_L5_Studio_IOC

Consegna

Studiare questo link di anyrun e spiegare queste minacce in un piccolo report.

<https://app.any.run/tasks/9a15871843fe-45ce-85b366203dbc2281/>

Svolgimento

Aperto il link ci ritroviamo all'interno di [anyrun](#), un applicativo sandbox online volto al rilevamento, il monitoraggio e la ricerca di minacce informatiche in tempo reale.




Il file che ci viene proposto è visibile nella parte in alto a destra della GUI ed è nominato **Jvczfhe.exe**.



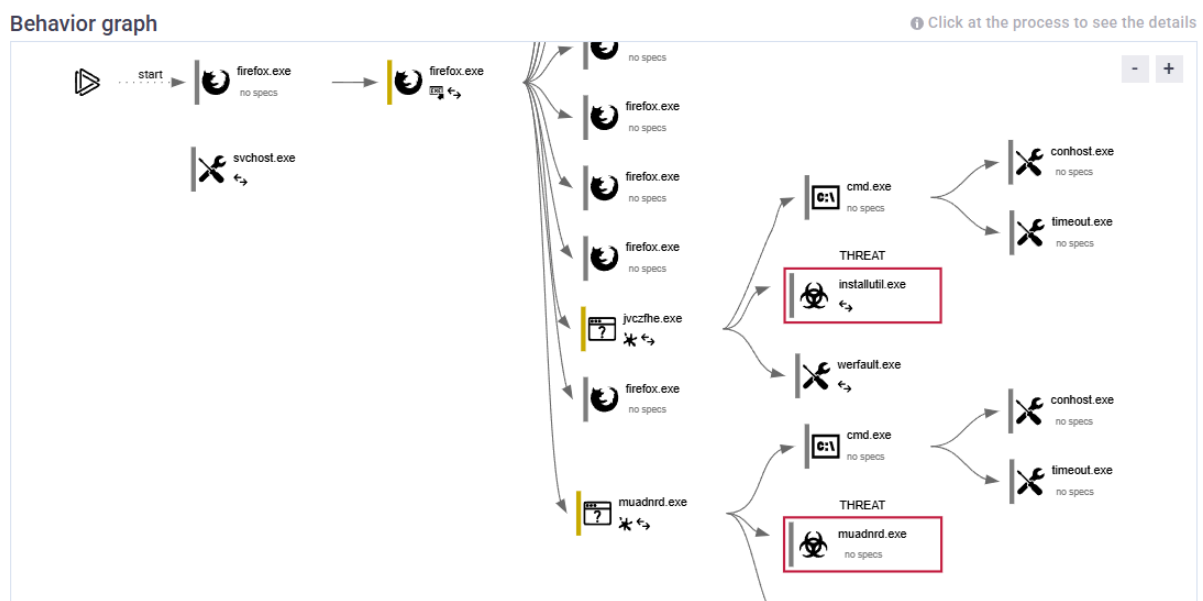
Spostandoci nella sezione text report possiamo notare subito alcune informazioni utili tra le quali i vari hash.

SHA256:
0307EE805DF8B94733598D5C3D62B28678EAEADB1CA3689FA678A3780DD3DF0

General Info

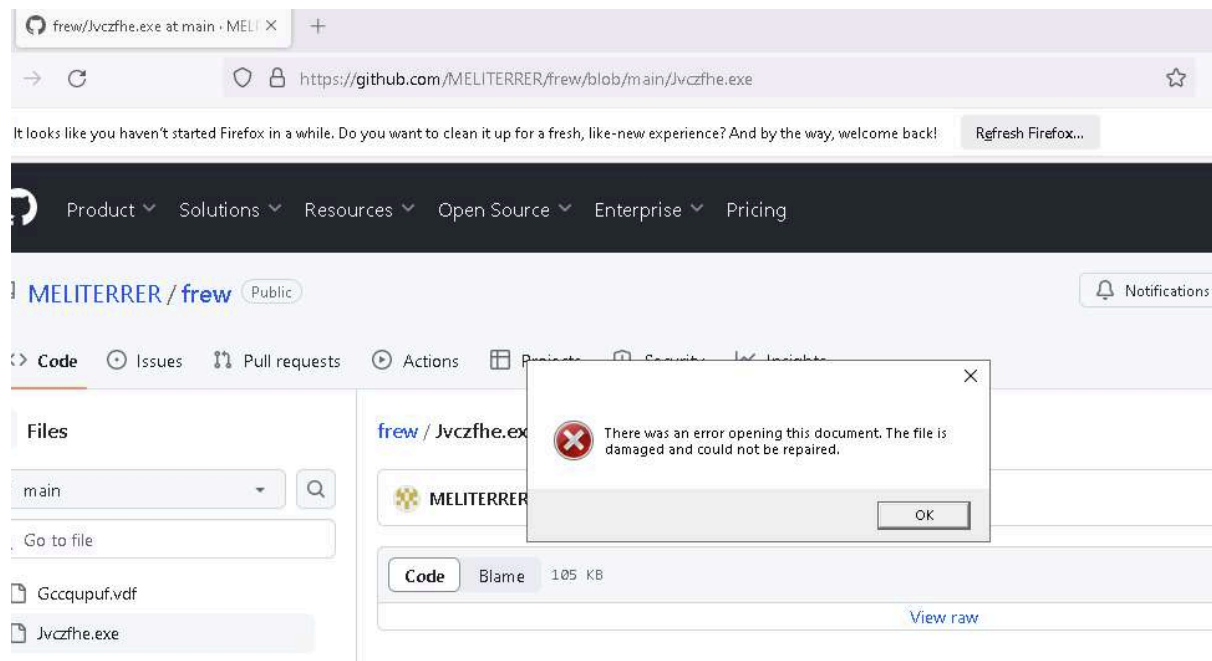
URL:	https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe
Full analysis:	https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281
Verdict:	Malicious activity
Analysis date:	August 25, 2024 at 22:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	github netreactor
Indicators:	  
MD5:	00B5E91B42712471CDFBDB37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62B28678EAEADB1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

Poco più sotto, all'interno della sezione Behaviour graph possiamo trovare la lista dei processi avviati dal presunto malware una volta eseguito:



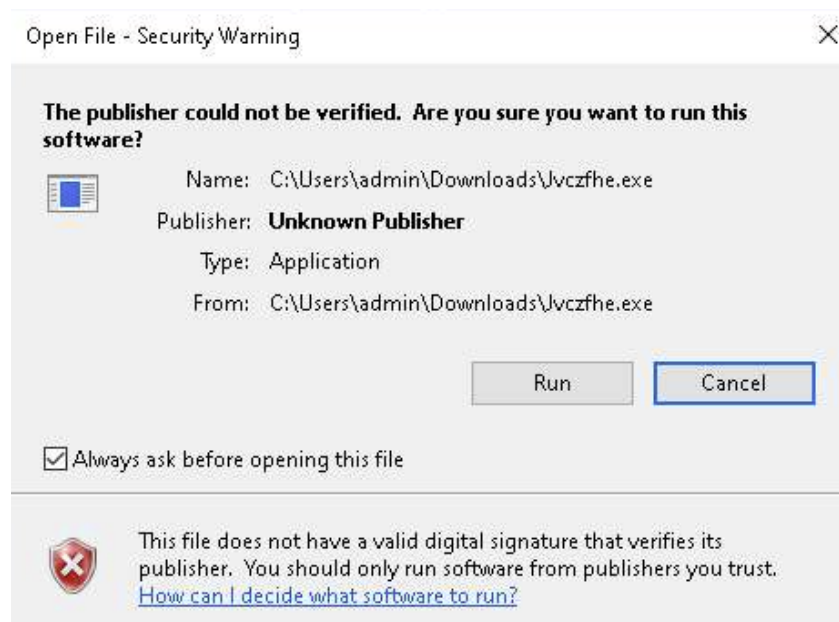
Dal grafico sembra che l'eseguibile, una volta avviato tenti di accedere a processi critici come cmd.exe, che avvia a sua volta avvia conhost.exe e timeout.exe spesso sintomo di malware che utilizzano **Esecuzione Ritardata** a fini di **Offuscamento**; una tattica comune per eludere i sistemi di rilevamento basati sul tempo. Vengono inoltre avviati installutil.exe e werfault.exe, quest'ultimo viene normalmente avviato per registrare problemi in caso di crash delle applicazioni.

Possiamo notare da uno degli screenshots il perchè viene avviato:



Quando si tenta di eseguire il presunto malware un errore viene dato in output che ci comunica che l'eseguibile risulta danneggiato e non può essere riparato.

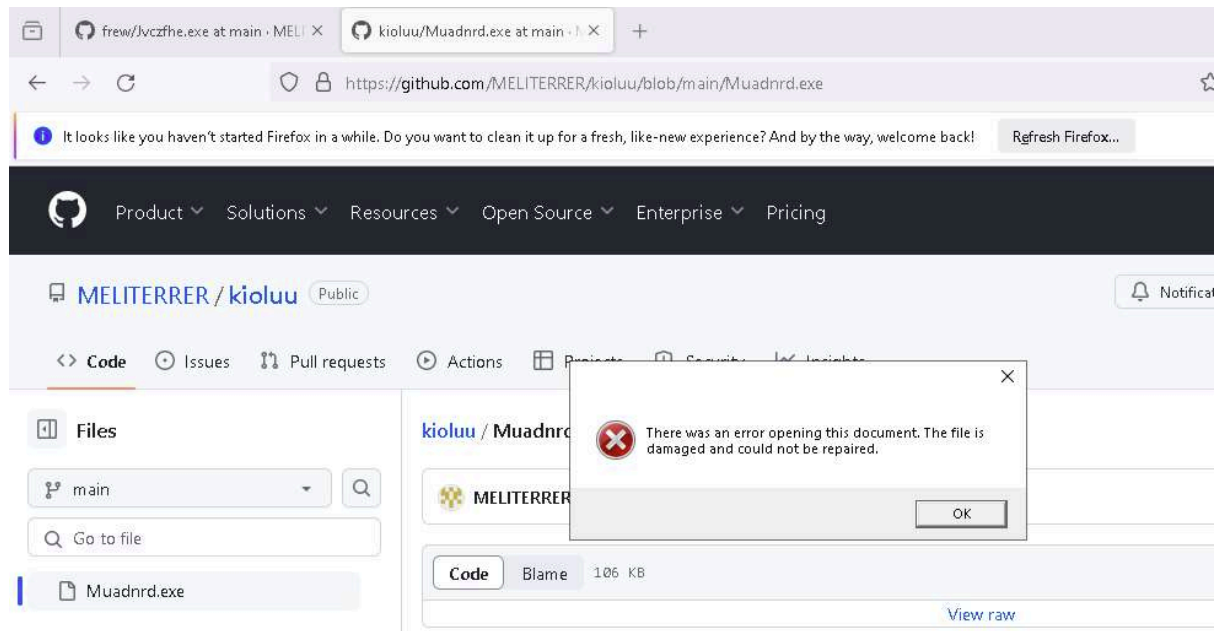
Dagli screenshots si nota altresì un dettaglio molto rilevante ovvero che l'esecuzione del sospetto malware viene richiesta come amministratore:



Ciò dà di fatto pieno potere all'eseguibile qualora l'utente avesse i permessi necessari per eseguirlo.

Notiamo poi che si tenta di scaricare un ulteriore file chiamato **Muadnrd.exe**

Una volta scaricato ed eseguito (anch'esso come admin), notiamo che anche questo restituisce il medesimo errore:



Andando a verificare il comportamento anche di quest'ultimo possiamo notare che presenta le stesse caratteristiche di Jvczfhe.exe: **cmd** → **timeout.exe**



Ulteriori informazioni cruciali possiamo ricavarle dalla sezione **MITRE ATT&CK Matrix**:

Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C
Command and Scripting Interpreter (1/12) Windows Command Shell 4			Masquerading (1/11) Rename Legitimate Utilities 1 Impair Defenses (1/11) Disable Windows Event Logging 2		Query Registry 4 50 System Information Discovery 15			Non-Standard Port 1

Qui possiamo notare alcuni potenziali IOC; Sotto la sezione **Execution** ritroviamo, come indicato in precedenza, che entrambi gli eseguibili hanno avviato cmd.exe, un comportamento sempre molto sospetto soprattutto se si tratta di app non conosciute.

The screenshot shows the 'Techniques details' page for T1059.003, titled '"Windows Command Shell"'. It includes a description of the technique, permissions required (User), data sources (Command, Command Execution, Process, Process Creation), and a list of subtechniques. The subtechniques listed are: 'Uses TIMEOUT.EXE to delay execution (2)' with examples 7520 cmd.exe (1) and 7876 cmd.exe (1); and 'Starts CMD.EXE for commands execution (2)' with examples 7492 Jvczfhe.exe (1) and 7824 Muadnrd.exe (1). A paragraph at the bottom explains that adversaries may abuse the Windows command shell for execution, as it is the primary command prompt on Windows systems and can be used to control almost any aspect of a system.

Techniques details
Get to know what this threat is about

Subtechniques ▼ [T1059.003](#)

"Windows Command Shell"

Permissions required: User

Data sources: Command:
Command Execution, Process:
Process Creation

Adversaries may abuse the Windows command shell for execution. The Windows command shell (`cmd`) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via Remote Services such as SSH.

- Uses TIMEOUT.EXE to delay execution (2)
 - 7520 cmd.exe (1)
 - 7876 cmd.exe (1)
- Starts CMD.EXE for commands execution (2)
 - 7492 Jvczfhe.exe (1)
 - 7824 Muadnrd.exe (1)

Mitre ci fa inoltre notare, all'interno della sezione **Defense Evasion**, che con i privilegi di amministratore l'eseguibile potrebbe facilmente cancellare i log di windows per impedirvi di tracciarne correttamente le azioni:

Adversaries may disable Windows event logging to limit data that can be leveraged for detections and audits

Se andiamo ad analizzare nel dettaglio quanto è successo possiamo notare che il trigger era dato semplicemente dall'azione di firefox che in fase di download scarica il file e gli assegna un nome temporaneo **OOD5yt-b.exe** e successivamente, una volta completato, lo rinomina con il suo nome originale **Jvczfhe.exe**.

In questo caso l>alert è dunque un falso positivo.

La tecnica a cui si fa riferimento è comunque interessante:

MITRE ATT&CK T1036.003

Rename Legitimate Utilities: L'avversario cambia il nome del file sfruttando la fiducia degli utenti o la scarsa accuratezza di alcuni sistemi di monitoraggio.

La sezione ci restituisce però anche quello che è il vero hash del file incriminato **Sha256:**

e6a7aaff54eb6d06acfc6f1dfa21a85b767dbf7ff3e9bdfd2ddbdec86aa9b2

Techniques details

Get to know what this threat is about

Warning (1)

Subtechniques ▼ [T1036.003](#)

"Rename Legitimate Utilities"

Permissions required:

Data sources: File: File Modification, Process: Process Metadata, Command: Command Execution, File: File Metadata

Adversaries may rename legitimate / system utilities to try to evade security mechanisms concerning the usage of those utilities. Security monitoring and control mechanisms may be in place for legitimate utilities adversaries are capable of

Process drops legitimate windows executable (1)

6596 firefox.exe (1)

Filename:	C:\Users\admin\Downloads\OOD5yt-b.exe.part
Md5:	5ec4256e6a2367502a8058f4bc8f4ecc
Sha1:	c6f996570b6f34cb813028c601b9d27bf8df0550
Sha256:	e6a7aaff54eb6d06acfc6f1dfa21a85b767dbf7ff3e9bdf2ddbdeced86aa9b2

Nella sezione **Discovery** ci avvisa inoltre che, avendo così altri privilegi, sarebbe semplice enumerare il sistema e raccogliere tutte le informazioni necessarie per proseguire un attacco.

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.

Andando nel dettaglio notiamo infatti che entrambi gli eseguibili tentano di accedere alla chiave di registro di windows **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing** dove sono contenute le informazioni relative al sistema operativo su cui viene eseguito.

Checks Windows Trust Settings (2)

7492 Jvczfhe.exe (1)

7824 Muadnrd.exe (1)

Reads security settings of Internet Explorer (2)

7492 Jvczfhe.exe (1)

7824 Muadnrd.exe (1)

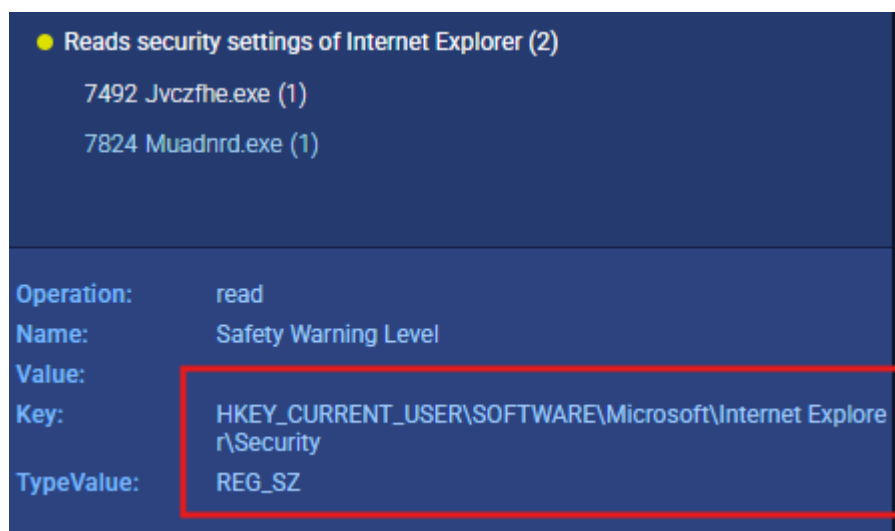
Operation:	read
Name:	State
Value:	146432
Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing
TypeValue:	REG_DWORD

Un'altra chiave critica a cui accedono è

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Security, responsabile delle preferenze di sicurezza dell'utente per Internet Explorer, tra cui:

- livello di restrizione della navigazione;
- abilitazione o disabilitazione di funzionalità potenzialmente rischiose (script, ActiveX, download);
- configurazioni usate da malware o amministratori per abbassare o alzare la sicurezza del browser.

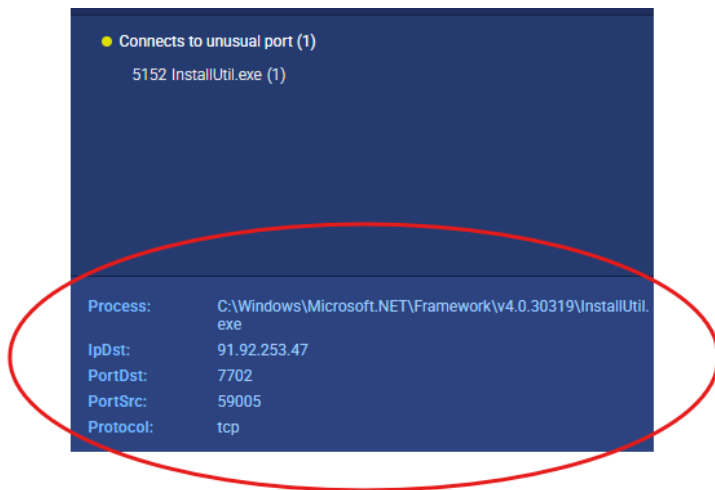
Un malware potrebbe quindi modificare questa chiave per indebolire la **sicurezza** (es. abbassare il livello della zona Internet, abilitare ActiveX non firmati), così da facilitare ulteriori infezioni; **leggere questa chiave può dare indicazioni su tentativi di manipolare la sicurezza del browser.**



Infine nella sezione Command & Control (**C&C**) ci fa porre attenzione **installutil.exe** che può essere sfruttato per una connessione remota ad un potenziale attaccante.

Se andiamo nei dettagli notiamo infatti che l'applicativo ha tentato di configurare una connessione verso **91.92.253.47** sulla porta **7702** ed utilizzando sul sistema target una porta secondaria in modo da non destare alcun sospetto, la porta **59005**.

Tutto ciò è un chiaro indicatore che siamo dinanzi ad un malware che punta ad ottenere una **backdoor** sfruttando un ritardo nell'esecuzione tramite **timeout.exe**.



La connessione punta per l'appunto ad un dominio a dir poco sospetto:
egehgdehjbhjtreduckdns.org

5370	Internet Explorer	23.33.40.102.00	discounthub.openniz.org	Akademi Internet User D.V.	UC	unknown
5152	InstallUtil.exe	91.92.253.47:7702	egehgdehjbhjtreduckdns.org	—	BG	unknown
1356	WinFount.exe	104.900.16.04.443	winfount.safedata.microsoft.com	MICROSOFT CORP. MON. AS BLOCK	US	unknown

Per indagare ulteriormente potrebbe visionare anche Scanners come [Virustotal.com](https://www.virustotal.com):

46/72 security vendors flagged this file as malicious

e6a7aaff54eb6d6ac6cf1dfa21a85b767dbf7f3e9bf02d0bdeced86aa9b2
Jvczhe.exe

Size: 104.95 KB | Last Analysis Date: 7 months ago

peexe invalid-signature signed overlay spreader assembly checks-user-input detect-debug-environment long-sleeps

Popular threat label: trojan.msl/jalapeno | Threat categories: trojan | Family labels: msil, jalapeno, injuke

Security vendors' analysis

Vendor	Detection	Category	GenVariant
Alibaba	Trojan:MSIL/injuke.d4fdac5	ALYac	GenVariant_Jalapeno.17798
Arcabit	Trojan.Jalapeno.D4586	Arctic Wolf	Unsafe
Avast	Win32:PWSX-gen [Trj]	AVG	Win32-PWSX-gen [Trj]
Avira (no cloud)	TR/Kryptik.dbsz	BitDefender	GenVariant_Jalapeno.17798

Che possono darci una prospettiva diversa in base ad altri motori di ricerca malware.

Display grouped sandbox reports	
<div> <div>1</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>1</div> </div>	<div> <div>1</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> </div>
<div> <div>7</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>4</div> </div>	<div> <div>15</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> </div>
<div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> </div>	<div> <div>6</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> </div>

Conclusioni

L'analisi del file **Jvczfhe.exe** mostra un comportamento tipico di **dropper**: una volta avviato con privilegi amministrativi, genera processi sospetti (**cmd.exe**, **timeout.exe**, **installutil.exe**) e tenta di contattare un server remoto (**91.92.253.47:7702**). L'uso di **timeout.exe** evidenzia tattiche di offuscamento basate su ritardo, mentre **installutil.exe** segnala abuso di strumenti legittimi (LOLBins) per eseguire codice.

L'allerta sul file **.part** e "firefox.exe" non indica un travestimento del malware, ma il normale meccanismo del browser durante il download; quindi in questo caso si tratta di un **falso positivo**.

Nel complesso, il malware punta a ottenere una **backdoor** sull'host, con rischio elevato se eseguito come amministratore.