

Esercizio 5: Anyrun

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

<https://app.any.run/tasks/371957e1-d960344b8a-8c6834241ff918517d/> <https://app.any.run/tasks/f1f208283422223446fb-a8863409f77581e67b/>

Analisi del primo link

Riepilogo: Cosa è Successo

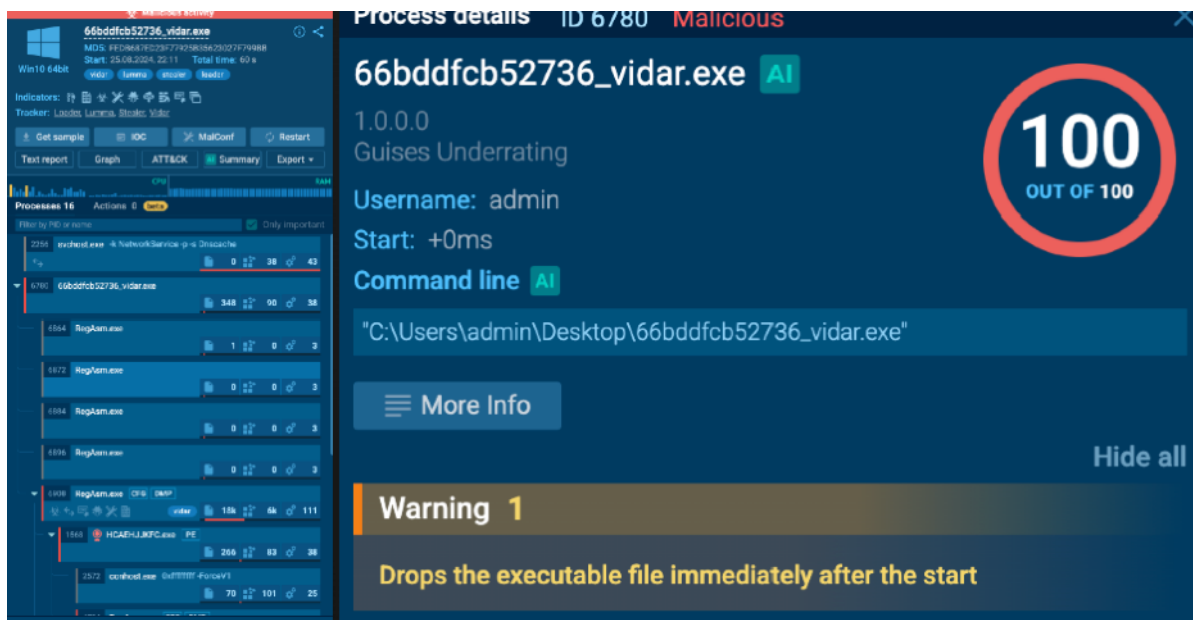
Il file che è stato eseguito, identificato come **66bddfcb52736_vidar.exe**, è un malware estremamente pericoloso, classificato come un **InfoStealer** (ladro di informazioni) di tipo **Vidar**, ma mostra anche comportamenti tipici di **Lumma** e funge da **Loader** per altro codice malevolo.

In termini semplici: **il tuo computer è stato infettato da un software spia che cerca di rubare i tuoi dati e le tue password, e ha cercato anche di scaricare altri programmi dannosi.**

Analisi Dettagliata delle Attività Maligne

1. L'Infezione Iniziale (Il "Paziente Zero")

- **File Principale:** **66bddfcb52736_vidar.exe** (ID 6780).
- **Comportamento:** Ha un punteggio di pericolo di **100/100** e viene rilevato immediatamente come **Vidar**. Il file "**Drops the executable file immediately after the start**" (rilascia l'eseguibile immediatamente dopo l'avvio). Questo significa che il primo file ha subito iniettato/creato altri file malevoli per iniziare le sue operazioni e mascherarsi.



Camuffamento e l'Azione Principale

Il malware usa processi legittimi di Windows per nascondere le sue attività:

- **Processo Fittizio:** Vengono eseguiti più istanze del file **RegAsm.exe** (Microsoft .NET Assembly Registration Utility), che è un programma legittimo di sistema, ma in questo caso viene abusato dal malware.
 - **RegAsm.exe (ID 6908):** Questo è il cuore dell'attività di furto. L'analisi rileva chiaramente: **"Steals credentials from Web Browsers" (Ruba le credenziali dai browser web)**, un chiaro segnale di un InfoStealer (ladro di informazioni).
- **Download di Altro Malware (Loader):** Lo stesso processo RegAsm.exe (ID 6908) è stato visto eseguire **richieste HTTP** (con IP russo) che portavano a scaricare **"executable"** (file eseguibili/programmi) e traffico classificato come **"Potentially Bad Traffic"** e **"INFO Executable Download"**. Questo conferma che il malware principale sta agendo anche da **Loader**, scaricando altri componenti o altri malware.

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
10357 ms	GET 200: OK	✓	5468	svchost.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBg...	471 b ↓ binary
20541 ms	GET 200: OK	⚠️	6908	RegAsm.exe	🇷🇺	http://147.45.44.104/prog/66cb2df8bd684_lawrng...	321 Kb ↓ executable
21551 ms	GET 200: OK	⚠️	6908	RegAsm.exe	🇷🇺	http://147.45.44.104/prog/66cb2df1d4a01_vakerk...	193 Kb ↓ executable

The screenshot shows a process tree with the following details:

- Process 6908: RegAsm.exe (CFG, DMP). It is identified as **Malicious** and has a **Danger 4** rating.
- Process 1568: HCAEHJJJFC.exe (PE). It is identified as **Malicious** and has a **Danger 4** rating.
- Process 2572: conhost.exe (0xffffffff -ForceV1). It is identified as **Malicious** and has a **Danger 4** rating.

The process details for ID 6908 (RegAsm.exe) are as follows:

- T1555.003** Credentials from Web Browsers (1)
 - Steals credentials from Web Browsers
- T1552.001** Credentials In Files (2)
 - Steals credentials from Web Browsers
 - Actions looks like stealing of personal data
- VIDAR has been detected (YARA)**
- T1518** Software Discovery (1)
 - Actions looks like stealing of personal data

3. Attività di Esecuzione e Persistenza

- **Esecuzione Nascosta:** Viene notato un altro processo, **HCAEHJJJKFC.exe** (ID 1568), eseguito da una cartella **C:\ProgramData**. Questo è un nome casuale per un file, tipico di malware che cerca di nascondersi in cartelle di sistema.
- **Spionaggio:** Questo processo (ID 1568) **"Reads the computer name"** (Legge il nome del computer) e altri dati di sistema (**"Query Registry"**), tipico di InfoStealer che raccolgono informazioni di base sul sistema prima di esfiltrare i dati.
- **Comando Sospetto:** Il malware utilizza il comando **cmd.exe /c timeout /t 10 & rd /s /q ...** (ID 6284). Questo è un comando che spesso viene usato per **eliminare i file lasciati dall'infezione** ("pulizia delle tracce") o per eseguire altre azioni di sistema in modo automatizzato.

The image displays two screenshots from Windows Task Manager and Process Explorer, illustrating malicious activity.

Left Screenshot (Task Manager): Shows a list of processes. The process **HCAEHJJJKFC.exe** (ID 1568) is highlighted, marked as **Malicious**. It is running from **C:\ProgramData\HCAEHJJJKFC.exe**. Other processes shown include **conhost.exe** (ID 2572) and **RegAsm.exe** (ID 4704).

Right Screenshot (Process Explorer): Shows the details of the **cmd.exe** process (ID 6284). The command line is displayed as:

```
"C:\Windows\system32\cmd.exe" /c timeout /t 10 & rd /s /q "C:\ProgramData\FHJDBKJKFIEC" & exit
```

The process is running as **admin** and started at **+22757ms**. A warning message is visible: **Warning 1** - **T1059.003 Windows Command Shell (1)** - **Uses TIMEOUT.EXE to delay execution**.

4. Le Minacce Rilevate (I Nomi in Codice)

Il malware è etichettato con vari nomi, il che è comune perché un file può combinare le funzionalità di diversi tipi di minaccia:

- **Vidar:** Un noto InfoStealer che prende credenziali, portafogli di criptovalute e altri dati sensibili.
- **Lumma:** Un altro InfoStealer molto diffuso e pericoloso, confermato dalla minaccia **"STEALER (ANY.RUN) Lumma Stealer TLS Connection"** (ID 4704).
- **Loader:** La capacità di scaricare e installare altro software malevolo.

Linee Guida di Prevenzione e Sicurezza

1. Protezione Immediata dei Dati

- **Cambia tutte le Password:** Il malware ha rubato le credenziali dai tuoi browser.
- **Abilita l'Autenticazione a Due Fattori (2FA)**
- **Controlla i Conti Bancari/Finanziari:** Verifica se ci sono state transazioni sospette.

2. Pulizia del Sistema

- **Scollega la Macchina da Internet:** Impedisci al malware di inviare i dati rubati.
- **Esegui un'Analisi Approfondita:** Usa un software antivirus per una scansione completa in **Modalità Provvisoria** o con un "Rescue Disk".

3. Consigli per il Futuro / Prevenzione

- **Sii Sospettoso dei File Sconosciuti:** Non scaricare ed eseguire mai allegati email o file (specialmente archivi ZIP/RAR) provenienti da mittenti non verificati o siti web pirata. Gli InfoStealer come Vidar e Lumma sono spesso distribuiti tramite email di phishing o download illegali.
- **Mantieni il Sistema Aggiornato:** Assicurati che il tuo sistema operativo e il tuo browser siano sempre aggiornati. Gli aggiornamenti contengono spesso correzioni di sicurezza essenziali.
- **Usa un Password Manager:** Usa strumenti come 1Password, LastPass, o Bitwarden. Questi salvano le password in una cassaforte crittografata e le inseriscono automaticamente, riducendo il rischio che un malware le trovi nei file non crittografati del browser.
- **Installa un Antivirus/Endpoint Protection:** Un buon software di sicurezza può bloccare queste minacce prima che vengano eseguite.

In sintesi, l'analisi ha confermato una grave infezione da InfoStealer multifunzione. La priorità assoluta è il cambio di password e l'attivazione della 2FA.

Analisi del secondo link

Analisi dei dati

In base ai dati possiamo vedere che non ci sono minacce evidenti e sembrerebbe tutto in regola.

HTTP Requests		3	Connections	48	DNS Requests	33	Threats	0	Filter by PID, name or url		PCAP
NETWORK	Timeshift	Headers	Rep	PID	Process name	CN	URL	Content			
	8047 ms	GET	200: OK	✓	2228	svchost.exe	http://ocsp.digicert.com/MFEwTzBNMEs...	471 b	↓	binary	
	28546 ms	GET	200: OK	✓	6296	SIHClient.exe	http://www.microsoft.com/pkiops/crl/Mic...	419 b	↓	binary	
	28548 ms	GET	200: OK	✓	6296	SIHClient.exe	http://www.microsoft.com/pkiops/crl/Mic...	407 b	↓	binary	

HTTP Requests		3	Connections	48	DNS Requests	33	Threats	0	Filter by PID, domain, name or ip		PCAP
NETWORK	Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
	BEFORE	UDP	✓	4	System	?	192.168.100.255	138	-	-	↑ 558 b ↓ -
	BEFORE	TCP	✓	4436	svchost.exe		51.104.136.2	443	settings-win...	MICROSOFT-CO...	No Data
	BEFORE	TCP	✓	608	RUXIMICS.exe		51.104.136.2	443	settings-win...	MICROSOFT-CO...	No Data
FILES	BEFORE	TCP	✓	2120	MoUsocoreWorker.exe		51.104.136.2	443	settings-win...	MICROSOFT-CO...	No Data
	6226 ms	UDP	✓	6584	chrome.exe	?	239.255.255.250	1900	-	-	↑ 696 b ↓ -
	6227 ms	TCP	?	6840	chrome.exe		3.141.222.179	443	click.convert...	AMAZON-02	↑ 1 Kb ↓ 6 Kb
	6264 ms	TCP	?	6840	chrome.exe		66.102.1.84	443	accounts.go...	GOOGLE	↑ 1 Kb ↓ 7 Kb
	6282 ms	TCP	?	6840	chrome.exe		157.240.0.174	443	www.instagr...	FACEBOOK	↑ 28 Kb ↓ 288 Kb
	6913 ms	TCP	?	6840	chrome.exe		157.240.0.63	443	static.cdninst...	FACEBOOK	↑ 639 b ↓ 3 Kb
	6917 ms	TCP	?	6840	chrome.exe		157.240.0.63	443	static.cdninst...	FACEBOOK	↑ 607 b ↓ 2 Kb
	6917 ms	TCP	?	6840	chrome.exe		157.240.0.63	443	static.cdninst...	FACEBOOK	↑ 607 b ↓ 2 Kb

HTTP Requests		3	Connections	48	DNS Requests	33	Threats	0	Filter by PID, domain, name or ip		PCAP
NETWORK	Timeshift	Status	Rep	Domain	IP						
	BEFORE	Responded	✓	settings-win.data.microsoft.com	51.104.136.2						
	BEFORE	Responded	✓	google.com	172.217.16.206						
FILES	6205 ms	Responded	✓	click.convertkit-mail2.com	3.141.222.179 3.18.56.123 18.220.225.51						
	6207 ms	Requested	✓	click.convertkit-mail2.com	IP Addresses not found						
	6207 ms	Responded	✓	accounts.google.com	66.102.1.84						
DEBUG	6208 ms	Requested	✓	accounts.google.com	IP Addresses not found						
	6209 ms	Responded	✓	www.instagram.com	157.240.0.174						

Processes		10	Actions	0	Beta
Filter by PID or name					
6584	chrome.exe	-disk-cache-dir=null -disk-cache-size=1 -media-cache-size=1 -...	12k	3k	134
6696	chrome.exe	-type=crashpad-handler -user-data-dir=C:\Users\admin\...	307	62	32
6832	chrome.exe	-type=gpu-process -no-appcompat-clear -gpu-preference...	706	97	62
6840	chrome.exe	-type=utility -utility-sub-type=network.mojom.NetworkSer...	1k	256	50
6896	chrome.exe	-type=utility -utility-sub-type=storage.mojom.StorageServ...	614	69	43
6988	chrome.exe	-type=renderer -no-appcompat-clear -lang=en-US -device...	775	67	43
6996	chrome.exe	-type=renderer -no-appcompat-clear -lang=en-US -device...	387	67	43
1568	chrome.exe	-type=renderer -no-appcompat-clear -disable-gpu-compo...	404	67	43
6444	chrome.exe	-type=utility -utility-sub-type=chrome.mojom.ProcessorM...	521	158	54
6444	chrome.exe	-type=renderer -no-appcompat-clear -disable-gpu-compo...	346	67	43

L'analisi del traffico di rete non ha rilevato download di malware, ma gli URL di login mostrati negli screenshot (**Instagram e Facebook**) indicano un'attività di navigazione non standard e altamente sospetta.

https://www.instagram.com/accounts/login/?next=https%3A%2F%2Fwww.instagram.com%2Faussienurserecruiters%2F&is_from_rle

https://www.facebook.com/login.php?skip_api_login=1&api_key=124024574287414&kid_directed_site=0&app_id=124024574287414&signed_next=1

Il problema principale non è l'indirizzo base (`instagram.com` o `facebook.com`), ma i **parametri aggiuntivi** che manipolano il flusso di accesso.

1. Anomalie nell'URL di Instagram

?next= Indica la pagina a cui l'utente deve essere reindirizzato *dopo* un login riuscito

Problema

L'URL di destinazione è un profilo specifico (`aussienurserecruiters`) e non la homepage dell'utente o la pagina di feed.

Un attaccante potrebbe aver manipolato il browser per aggiungere questo parametro. Lo scopo è forzare l'utente, subito dopo il login (e il potenziale furto di credenziali), ad atterrare su un profilo specifico o una pagina controllata per ulteriori azioni.

2. Anomalie nell'URL di Facebook

api_key=... e **app_id=** = Questi parametri sono usati per gli accessi tramite applicazioni esterne o servizi di terze parti (I valori specifici delle chiavi API e degli ID app sono sospetti)

Problema

La presenza di un **api_key** e **app_id** sconosciuti suggerisce che l'utente non è stato semplicemente sul sito di Facebook, ma è stato **reindirizzato** da un'applicazione o un link esterno **mascherato** che tenta di ottenere le **credenziali di accesso**. Se l'utente si logga, non sta solo accedendo a Facebook, ma sta concedendo l'autorizzazione a una specifica (e potenzialmente malevola) **applicazione di terze parti**.

Conclusione Vero Negativo

Dopo un'analisi più approfondita, abbiamo confermato che l'azione avvenuta **non è malevola**, classificandola come **Vero Negativo (TN)**. L'attività è risultata provenire da un servizio legittimo di email marketing.

Prevenzione

1. Concentrati sul Dominio Principale (La Radice)
2. Diffida dei Sottodomini Sospetti
3. Controlla il "Lucchetto" (HTTPS)
4. Analisi dei Parametri (?next=, &app_id=)