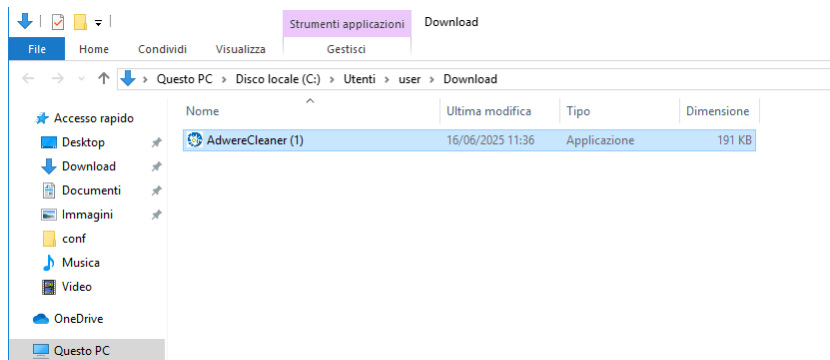


Esercizio 1: Malware analysis

Download del file

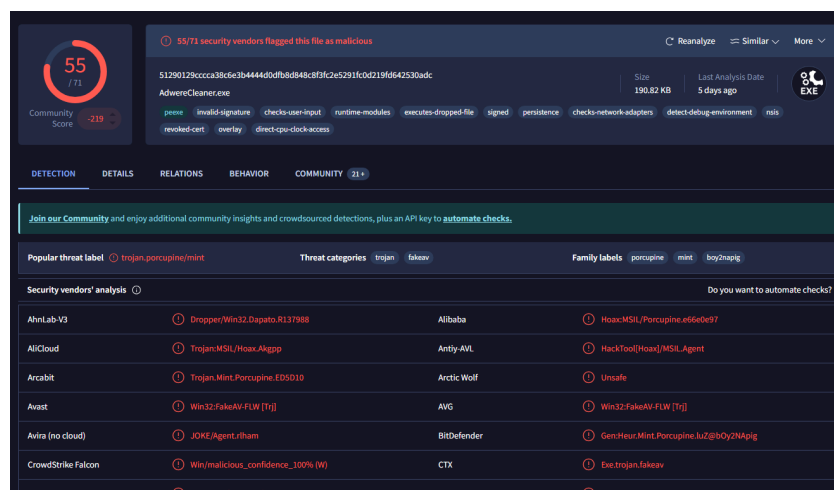
Il file è stato scaricato dal link GitHub fornito dall'esercizio. Per consentire il download, è stato necessario disattivare temporaneamente le protezioni di Google Chrome. Il file è stato salvato all'interno della VM Win10 con snapshot pre-esecuzione e connessa in NAT, per evitare rischi di compromissione sia del sistema principale sia della VM.



Analisi statica

A. Analisi su Virustotal

Prima di aprire il malware faremo un'analisi statica veloce su virustotal.

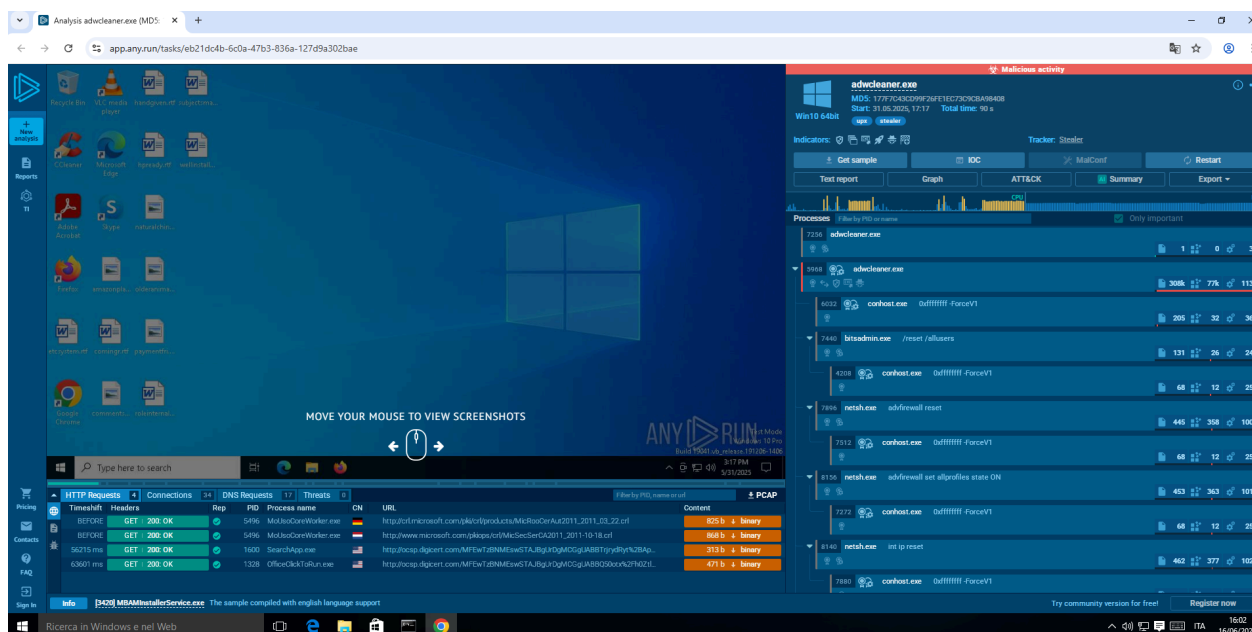


Questa scansione veloce indica che questo file viene segnalato da 55 antivirus come un FakeAV e Trojan, appartenente alla famiglia Porcupine ovvero al gruppo di trojan creati e progettati per ingannare gli utenti e far loro credere che il pc sia infetto.

L'hash MD5 del file è 248AADD395FFA7FFB1670392A9398454.

B. Analisi su ANY.RUN

Diamo il nostro file in pasto ad ANY.RUN e vediamo il report.



Nella parte in alto a destra della schermata è ben visibile e in rosso la dicitura "Malicious activity". Questo ci conferma che ANY.RUN ha rilevato comportamenti malevoli in tempo reale, già durante i primi istanti di esecuzione.

Nel pannello centrale a destra si osserva una catena di processi figli (come gli innumerevoli "conhost.exe" o "advfirewall reset") che hanno eseguito manipolazioni dirette delle impostazioni di rete e firewall, probabilmente per assicurarsi che la comunicazione esterna fosse consentita e per rimuovere eventuali blocchi o restrizioni imposte da protezioni preesistenti.

Nella parte inferiore si vedono alcune richieste GET con risposta 200 OK associate a processi interni come ad esempio "SearchApp.exe" o "MoUsoCoreWorker.exe"

In conclusione, il malware si installa e agisce subito in profondità, toccando rete, firewall e componenti di sistema tendendo al ripristino di connessioni, modificando le policy firewall e IP reset.

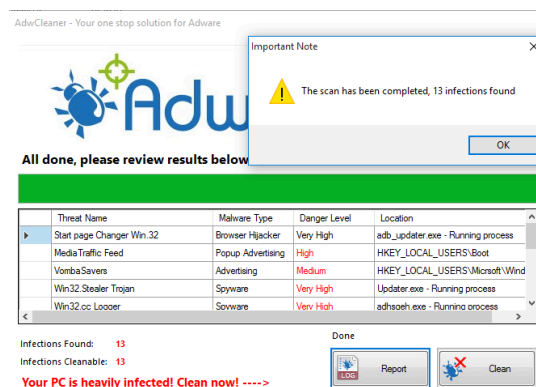
Analisi dinamica

A. Apriamo il malware



Avviamo il rogue av e noteremo una finestra di benvenuto di un'applicazione antivirus che invita a premere sul tasto "Scan".

Naturalmente ci fidiamo, click su Scan e attendiamo la fine del processo.



Il risultato mostra che la nostra VM ha ben 13 Malware con vari livelli di pericolo che vanno dal medio al molto alto. Prima di procedere oltre facciamo una ricerca veloce nel web per informarci sulle attività di questi malware che si fingono antivirus e su quale strumento da usare per analizzare.

Rogue security software

15 languages

Article Talk

Read Edit View history Tools

From Wikipedia, the free encyclopedia

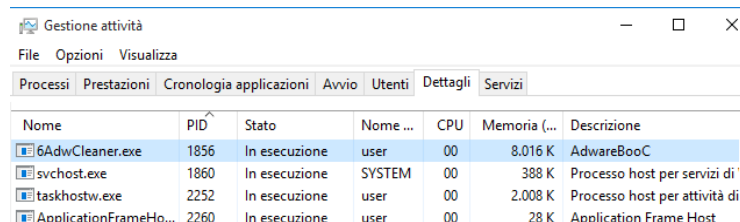
Rogue security software is a form of [malicious software](#) and [internet fraud](#) that misleads users into believing there is a [virus](#) on their computer and aims to convince them to pay for a fake [malware](#) removal tool that actually installs malware on their computer.^[1] It is a form of [scareware](#) that manipulates users through fear, and a form of [ransomware](#).^[2] Rogue security software has been a serious security threat in desktop computing since 2008.^[3] An early example that gained infamy was [SpySheriff](#) and its clones,^[4] such as Nava Shield.

With the rise of cyber-criminals and a black market with thousands of organizations and individuals trading exploits, malware, virtual assets, and credentials, rogue security software has become one of the most lucrative criminal operations.

I fake antivirus sono software dannosi che si fingono programmi di sicurezza per ingannare l'utente, facendo credere che il dispositivo sia infetto. In realtà, è proprio tentando di rimuovere il falso virus che il malware si attiva.

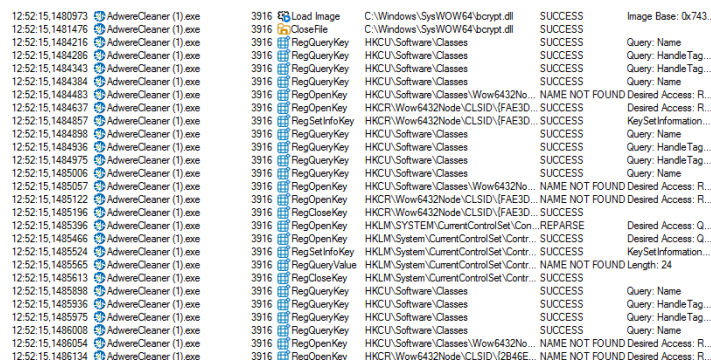
B. Analisi con Procmon

Passiamo all'analisi dei processi utilizzando Process Monitor e cerchiamo quello che ci interessa, per scoprire quale apriremo il task manager.



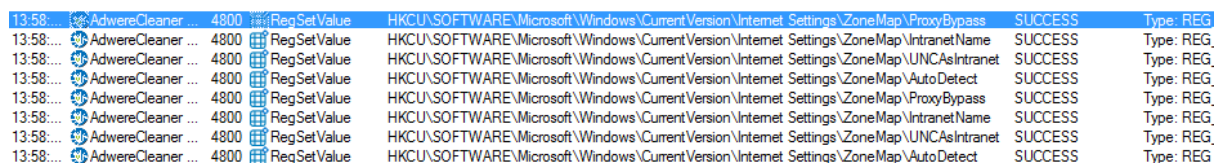
Nome	PID	Stato	Nome ...	CPU	Memoria (...)	Descrizione
6AdwCleaner.exe	1856	In esecuzione	user	00	8,016 K	AdwareBooC
svchost.exe	1860	In esecuzione	SYSTEM	00	388 K	Processo host per servizi di
taskhostw.exe	2252	In esecuzione	user	00	2,008 K	Processo host per attività di
ApplicationFrameHo...	2260	In esecuzione	user	00	28 K	Application Frame Host

Identificato il processo col nome di “6AdwCleaner.exe” con PID “1856”, torniamo su Procmon e lo cerchiamo con lo strumento “Find”.



12:52:15,1480973	6AdwCleaner (1).exe	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS	Image Base: 0x743...
12:52:15,1481476	6AdwCleaner (1).exe	CloseFile	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS	
12:52:15,1484216	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:52:15,1484286	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:52:15,1484343	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:52:15,1484384	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:52:15,1484483	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes\Wow6432No...	NAME NOT FOUND	Desired Access: R...
12:52:15,1484637	6AdwCleaner (1).exe	RegOpenKey	HKCR\Wow6432Node\CLSID\{FAE3D...	SUCCESS	Desired Access: R...
12:52:15,1484857	6AdwCleaner (1).exe	RegSetInfoKey	HKCR\Wow6432Node\CLSID\{FAE3D...	SUCCESS	KeySetInformation...
12:52:15,1484898	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:52:15,1484936	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:52:15,1484975	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:52:15,1485006	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:52:15,1485057	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes\Wow6432No...	NAME NOT FOUND	Desired Access: R...
12:52:15,1485122	6AdwCleaner (1).exe	RegOpenKey	HKCR\Wow6432Node\CLSID\{FAE3D...	NAME NOT FOUND	Desired Access: R...
12:52:15,1485196	6AdwCleaner (1).exe	RegOpenKey	HKCR\Wow6432Node\CLSID\{FAE3D...	SUCCESS	Desired Access: R...
12:52:15,1485396	6AdwCleaner (1).exe	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
12:52:15,1485466	6AdwCleaner (1).exe	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
12:52:15,1485524	6AdwCleaner (1).exe	RegSetInfoKey	HKLM\SYSTEM\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
12:52:15,1485565	6AdwCleaner (1).exe	RegSetInfoKey	HKLM\SYSTEM\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
12:52:15,1485613	6AdwCleaner (1).exe	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	SUCCESS	NAME NOT FOUND Length: 24
12:52:15,1485898	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:52:15,1485936	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:52:15,1485975	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:52:15,1486008	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:52:15,1486054	6AdwCleaner (1).exe	RegOpenKey	HKCU\Software\Classes\Wow6432No...	NAME NOT FOUND	Desired Access: R...
12:52:15,1486134	6AdwCleaner (1).exe	RegOpenKey	HKCR\Wow6432Node\CLSID\{2B46E...	NAME NOT FOUND	Desired Access: R...

Poichè il malware esegue un elevato numero di processi andremo ad usare il filtro “Operation is RegSetValue” per cercare operazioni di modifica delle chiavi di registro.



13:58:...	6AdwCleaner ...	4800	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG
13:58:...	6AdwCleaner ...	4800	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG
13:58:...	6AdwCleaner ...	4800	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG
13:58:...	6AdwCleaner ...	4800	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG
13:58:...	6AdwCleaner ...	4800	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG
13:58:...	6AdwCleaner ...	4800	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG
13:58:...	6AdwCleaner ...	4800	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG
13:58:...	6AdwCleaner ...	4800	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG

Anche in questo caso ci sono molti processi completati con successo, il più preoccupante è il primo in cui cerca di modificare anche le regole del proxy intercettando il traffico e probabilmente bypassare i controlli e registri sulle connessioni effettuate.

Altre operazioni che il malware svolge sono quelle di apertura e chiusura di file e directory, probabilmente modificando anche loro. Proviamo ad usare un altro filtro “Operation is WriteFile”.

```

13:58:... AdwareCleaner ... 4800 WriteFile C:\Users\user\AppData\Local\6AdwCleaner.exe
13:58:... AdwareCleaner ... 4800 WriteFile C:\Users\user\AppData\Local\6AdwCleaner.exe
13:58:... AdwareCleaner ... 4800 WriteFile C:\Users\user\AppData\Local\6AdwCleaner.exe
13:58:... AdwareCleaner ... 4800 WriteFile C:\Users\user\AppData\Local\6AdwCleaner.exe
13:58:... AdwareCleaner ... 4800 WriteFile C:\Users\user\AppData\Local\6AdwCleaner.exe
13:58:... AdwareCleaner ... 4800 WriteFile C:\Users\user\AppData\Local\6AdwCleaner.exe
13:58:... AdwareCleaner ... 4800 WriteFile C:\Users\user\AppData\Local\6AdwCleaner.exe
13:58:... AdwareCleaner ... 4800 WriteFile C:\Users\user\AppData\Local\6AdwCleaner.exe

```

In effetti sta scrivendo dei file locali, molto preoccupante.

C. Analisi con Wireshark

Passiamo all'analisi di rete con Wireshark per verificare eventuali connessioni svolte dal malware, apriamo il terminale come amministratore e lanciamo il comando <netstat -abno>.

```

TCP    10.0.2.15:50355    142.250.180.170:443    ESTABLISHED    4444
TCP    10.0.2.15:50356    142.250.180.170:443    ESTABLISHED    4444

```

Abbiamo trovato 2 connessioni stabilite sulla porta 443 all'IP 140.250.180.170.

Installiamo Wireshark 3.2.7 (versioni più aggiornate non vengono eseguite per colpa di un file .dll mancante) e lo apriamo catturando il traffico di rete. Diamo un filtro "tcp.port==443" perché come abbiamo visto prima la connessione avviene su quella porta.

No.	Time	Source	Destination	Protocol	Length	Info
145	93.798007	fd00::d0ac:e833:8260:6d49	2a00:1450:4002:c02:154	TCP	86	49585 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1440 WS=256 SACK_PERM=1
146	93.798498	2a00:1450:4002:c02:154	fd00::d0ac:e833:8260:6d49	TCP	74	443 → 49585 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
252	93.966279	fd00::d0ac:e833:8260:6d49	2a00:1450:4002:411:2003	TCP	86	49586 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1440 WS=256 SACK_PERM=1
254	93.966496	2a00:1450:4002:411:2003	fd00::d0ac:e833:8260:6d49	TCP	74	443 → 49586 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
270	94.012873	fd00::d0ac:e833:8260:6d49	2a00:1450:4002:415:200a	TCP	86	49587 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1440 WS=256 SACK_PERM=1
271	94.013196	2a00:1450:4002:415:200a	fd00::d0ac:e833:8260:6d49	TCP	74	443 → 49587 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
286	94.099126	10.0.2.15	142.251.168.84	TCP	60	49588 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=256 SACK_PERM=1
311	94.137944	142.251.168.84	10.0.2.15	TCP	60	443 → 49588 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460
312	94.137984	10.0.2.15	142.251.168.84	TCP	54	49588 → 443 [ACK] Seq=1 Ack=3 Win=64240 Len=0
313	94.138218	10.0.2.15	142.251.168.84	TLSv1.3	1815	Client Hello
314	94.138345	142.251.168.84	10.0.2.15	TCP	60	443 → 49588 [ACK] Seq=1 Ack=1461 Win=65535 Len=0
315	94.138758	142.251.168.84	10.0.2.15	TCP	60	443 → 49588 [ACK] Seq=1 Ack=1762 Win=65535 Len=0
319	94.177456	142.251.168.84	10.0.2.15	TLSv1.3	1466	Server Hello, Change Cipher Spec
320	94.177762	142.251.168.84	10.0.2.15	TCP	1466	443 → 49588 [PSH, ACK] Seq=1413 Ack=1762 Win=65535 Len=1412 [TCP segment of a reassembled PDU]
321	94.177776	10.0.2.15	142.251.168.84	TCP	54	49588 → 443 [ACK] Seq=1762 Ack=2825 Win=64240 Len=0
322	94.178381	142.251.168.84	10.0.2.15	TCP	1466	443 → 49588 [PSH, ACK] Seq=2825 Ack=1762 Win=65535 Len=1412 [TCP segment of a reassembled PDU]
323	94.178530	142.251.168.84	10.0.2.15	TLSv1.3	1204	Application Data
324	94.178542	10.0.2.15	142.251.168.84	TCP	54	49588 → 443 [ACK] Seq=1762 Ack=5387 Win=64240 Len=0
325	94.179676	10.0.2.15	142.251.168.84	TLSv1.3	128	Change Cipher Spec, Application Data

Potremo osservare un tentativo di connessione a più indirizzi remoti su porta 443 (che fa riferimento al servizio HTTPS), in più alcune connessioni IPv6 sono state immediatamente rifiutate (RST/ACK) probabilmente dal firewall di Windows.

Il contenuto delle comunicazioni non è visibile a causa della cifratura, ma il comportamento suggerisce un possibile uso di canali HTTPS ad esempio per il download di payload aggiuntivi.

Indicatori di compromissione

Tutte queste analisi hanno portato a numerosi indicatori di compromissione e in ordine abbiamo:

- File drop sospetto, ovvero “6AdwCleaner.exe”, generato all’esecuzione del file principale.
 - Processo figlio “conhost.exe” eseguito più volte per manipolare file di sistema e chiavi di registro.
 - Comandi malevoli come “advfirewall reset” per forzare il reset della configurazione del firewall di windows.
 - Connessioni HTTP/GET sulla porta 443 verso domini sospetti usando processi apparentemente innocui come “SearchApp.exe”
-

Conclusioni

L’analisi del file, inizialmente apparentemente legittimo, ha rivelato un comportamento malevolo riconducibile a un malware progettato per compromettere il sistema e manipolare impostazioni di rete e sicurezza.

Questo malware non solo compromette la privacy dell’utente ma potrebbe potenzialmente aprire backdoor per attività successive.

Questo esercizio dimostra l’importanza di adottare un approccio metodico all’analisi malware, utilizzando analisi statiche, dinamiche e di monitoraggio del traffico di rete per sviluppare efficaci strategie di rilevamento e mitigazione.

Pertanto, si deve passare alla rimozione immediata del file insieme ai relativi processi e il tempestivo isolamento del sistema compromesso per poi passare all’analisi retroattiva degli IoC riportati.
