LetsDefend

Official incident report

Event ID: 61

Rule Name: SOC126 - Suspicious New Autorun Value Detected

Made By

LinkedIn: Engineer.Ahmed Mansour

Link: https://www.linkedin.com/in/ahmed-mansour-5631b5323/

Github link: https://github.com/AhmedMansour93

Table of contents

Event Details

Event ID:
61

Event Date and Time:
Feb, 14, 2021, 06:40 PM

Rule:
SOC126 - Suspicious New Autorun Value Detected

Level:
Security Analyst

Hostname:
KatharinePRD

Process Name:
OliwciaPrivInstaller.exe

File Hash:
436fa243bbfed63a99b8e9f866cd80e5

File Size:
348.00 Kb

Device Action:
Cleaned

Network Information Details

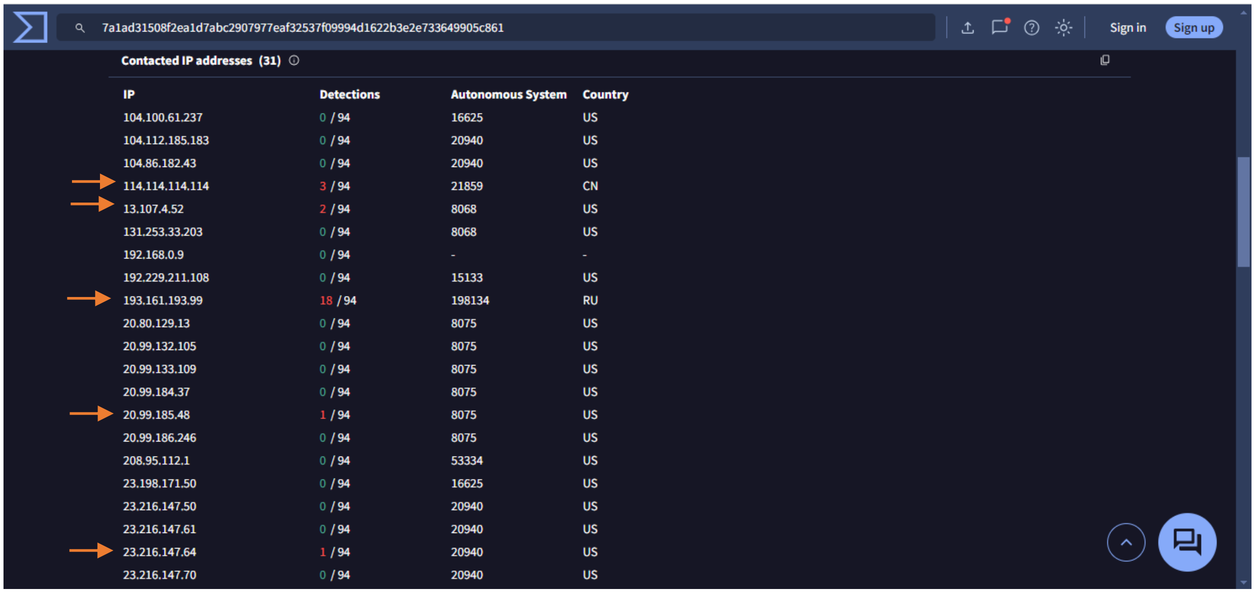
Destination IP Address:

This IP address (172.16.15.78) is part of the private IP range (172.16.0.0 to 172.31.255.255), indicating that it belongs to your organization's internal network. Traffic directed to this address remains within the local network, suggesting that the device associated with this IP is located within your internal environment.

Source IP Addresses:

- 114.114.114.114 (External)
- 13.107.4.52 (External)
- 193.161.193.99 (External)
- 20.99.185.48 (External)
- 23.216.147.64 (External)
- 8.8.8.8 (External)

All of these IP addresses are public and originate from outside your organization's network. The presence of these external IPs indicates that the source of the traffic, or potential threats, is from external entities on the internet, targeting the internal device at 172.16.15.78. These IP addresses are flagged as potentially malicious, suggesting potential hostile intent or suspicious activity directed toward your network.



7a1ad31508f2ea1d7abc2907977eaf32537f09994d1622b3e2e733649905c861
Sign in
Sign up

Contacted IP addresses (31)

IP	Detections	Autonomous System	Country
104.100.61.237	0 / 94	16625	US
104.112.185.183	0 / 94	20940	US
104.86.182.43	0 / 94	20940	US
114.114.114.114	3 / 94	21859	CN
13.107.4.52	2 / 94	8068	US
131.253.33.203	0 / 94	8068	US
192.168.0.9	0 / 94	-	-
192.229.211.108	0 / 94	15133	US
193.161.193.99	18 / 94	198134	RU
20.80.129.13	0 / 94	8075	US
20.99.132.105	0 / 94	8075	US
20.99.133.109	0 / 94	8075	US
20.99.184.37	0 / 94	8075	US
20.99.185.48	1 / 94	8075	US
20.99.186.246	0 / 94	8075	US
208.95.112.1	0 / 94	53334	US
23.198.171.50	0 / 94	16625	US
23.216.147.50	0 / 94	20940	US
23.216.147.61	0 / 94	20940	US
23.216.147.64	1 / 94	20940	US
23.216.147.70	0 / 94	20940	US

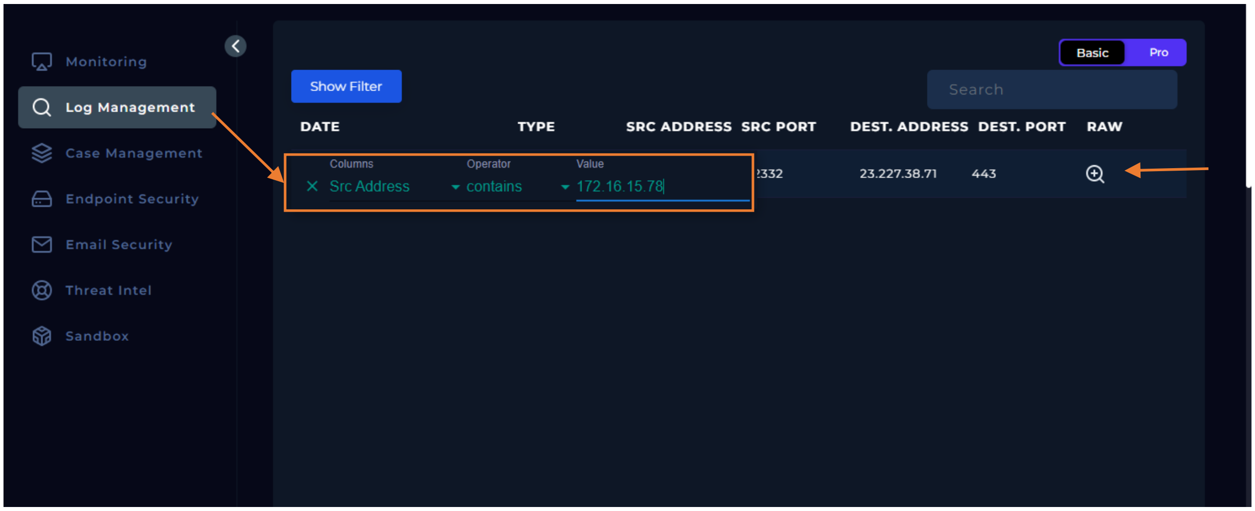
- **The attack is external / the results from Virustotal**
- **Reference results. Relation section (Connected IPs)**

Analysis:

Log Management

We'll proceed by entering the destination IP address from the alert and reviewing the results. Based on the time and date of the attack. The search will be choosing the Source IP because the Destination IP in the alert Names as Source Address.

Please refer to the attached image for further details regarding the attack.



Columns: Src Address
Operator: contains
Value: 172.16.15.78

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
			332	23.227.38.71	443	🔍

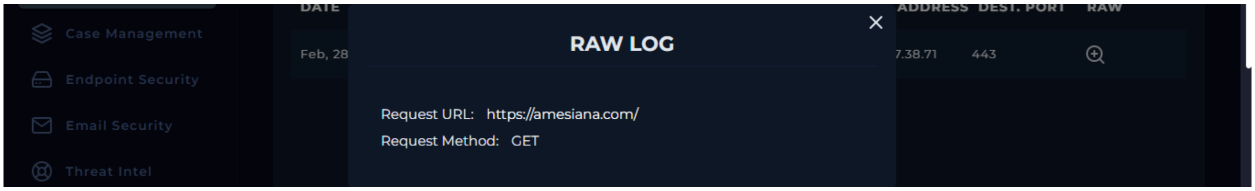
1 Log records for the destination IP regarding to our alert date and time.

Please refer to the attached image for further details regarding the attack.

We will explain the log step by step

Log Analysis

- **Log1:**

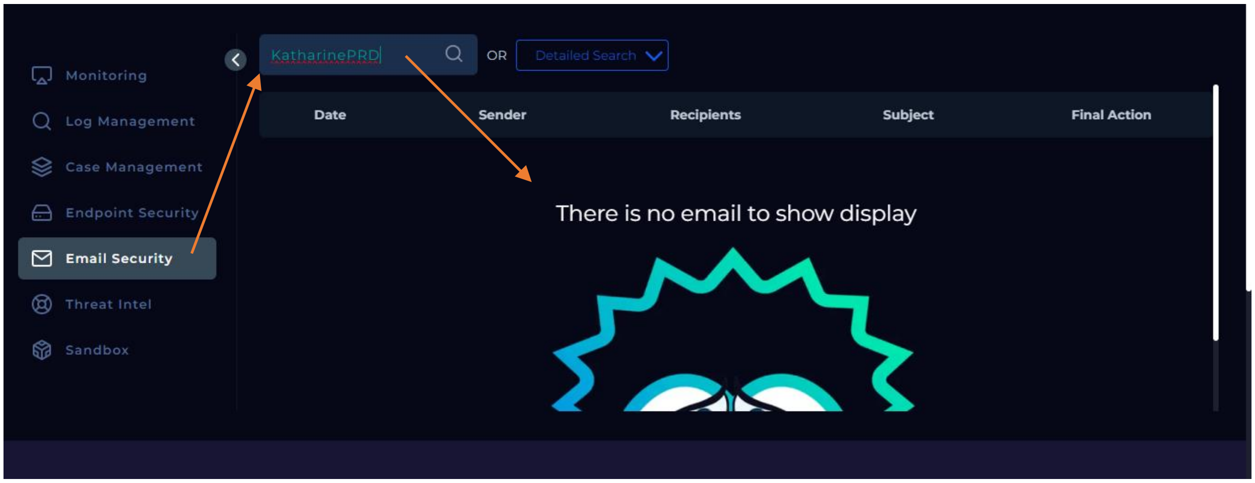


```
Request URL:   https://amesiana.com/
Request Method:   GET
```

This log captures a web request made to the URL `https://amesiana.com/` using the HTTP method `GET`. Here's a breakdown of the key components:

1. **Request URL: `https://amesiana.com/`**
   - This is the URL or web address to which the request is being made. In this case, it is a website named `amesiana.com`. The request is being sent over HTTPS, meaning it is a secure connection using SSL/TLS encryption.
2. **Request Method: GET**
   - The HTTP method `GET` indicates that the request is asking to retrieve data from the server. In other words, the client (e.g., a browser or application) is requesting to download a web page or resource from `https://amesiana.com/`. No data is being sent in the body of the request, as `GET` is primarily used for fetching resources (e.g., HTML pages, images, or scripts).

Email Security:



KatharinePRD

Date	Sender	Recipients	Subject	Final Action

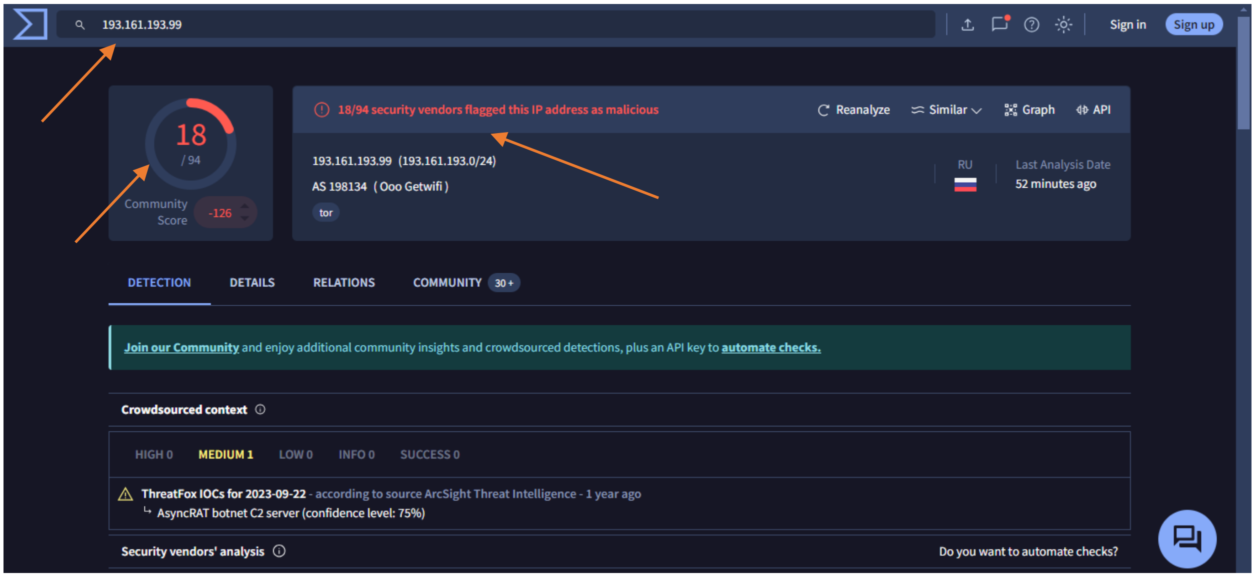
There is no email to show display

- Despite entering the source host name in the email security section, no emails have been sent, indicating that the attack was not executed.

Detection:

Threat Intelligence Results

We will conduct a comprehensive scan of the source IP address using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



18/94 security vendors flagged this IP address as malicious

193.161.193.99 (193.161.193.0/24)
AS 198134 (Ooo Getwifi)
tor

RU

Last Analysis Date
52 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

⚠ ThreatFox IOCs for 2023-09-22 - according to source ArcSight Threat Intelligence - 1 year ago
↳ AsyncRAT botnet C2 server (confidence level: 75%)

Security vendors' analysis

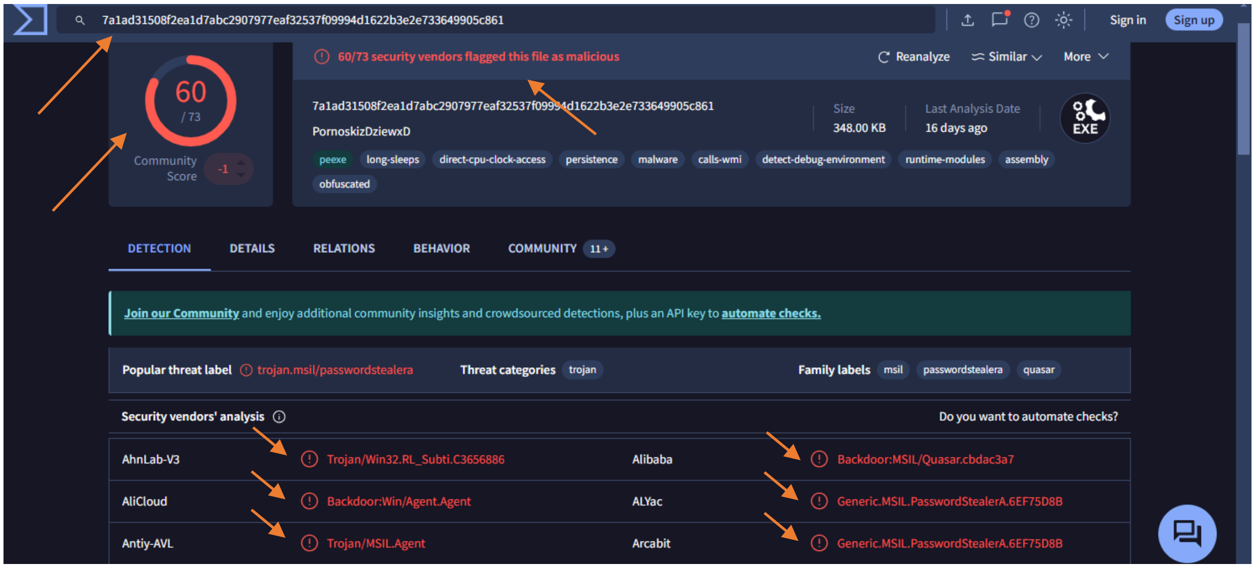
Do you want to automate checks?

VirusTotal Results for Attacker IP: 67.68.210.95

Out of 94 security vendors, 18 flagged this IP address as malicious:

- **alphaMountain.ai**: Malicious
- **Antiy-AVL**: Malicious
- **ArcSight Threat Intelligence**: Malware
- **BitDefender**: Malware
- **Certego**: Malicious
- **CRDF**: Malicious
- **Criminal IP**: Malicious
- **CyRadar**: Malicious
- **ESET**: Malware
- **Forcepoint ThreatSeeker**: Malicious
- **Fortinet**: Malware
- **G-Data**: Malware
- **Kaspersky**: Malware
- **Webroot**: Malicious
- **Reference result.**
- **The Traffic is Malicious**

We will conduct a comprehensive scan File Hash using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



7a1ad31508f2ea1d7abc2907977eaf32537f09994d1622b3e2e733649905c861

60/73 security vendors flagged this file as malicious

7a1ad31508f2ea1d7abc2907977eaf32537f09994d1622b3e2e733649905c861
PornoskizDziewxD

Size 348.00 KB

Last Analysis Date 16 days ago

peexe long-sleeps direct-cpu-clock-access persistence malware calls-wmi detect-debug-environment runtime-modules assembly obfuscated

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.msil/passwordstealera Threat categories trojan Family labels msil passwordstealera quasar

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.RL_Subti.C3656886	Alibaba	Backdoor:MSIL/Quasar.cbdac3a7
AliCloud	Backdoor:Win/Agent.Agent	ALYac	Generic.MSIL.PasswordStealerA.6EF75D8B
Antiy-AVL	Trojan/MSIL.Agent	Arcabit	Generic.MSIL.PasswordStealerA.6EF75D8B

VirusTotal Results for File Hash: 436fa243bbfed63a99b8e9f866cd80e5

Out of 73 security vendors, 60 flagged this file as malicious.

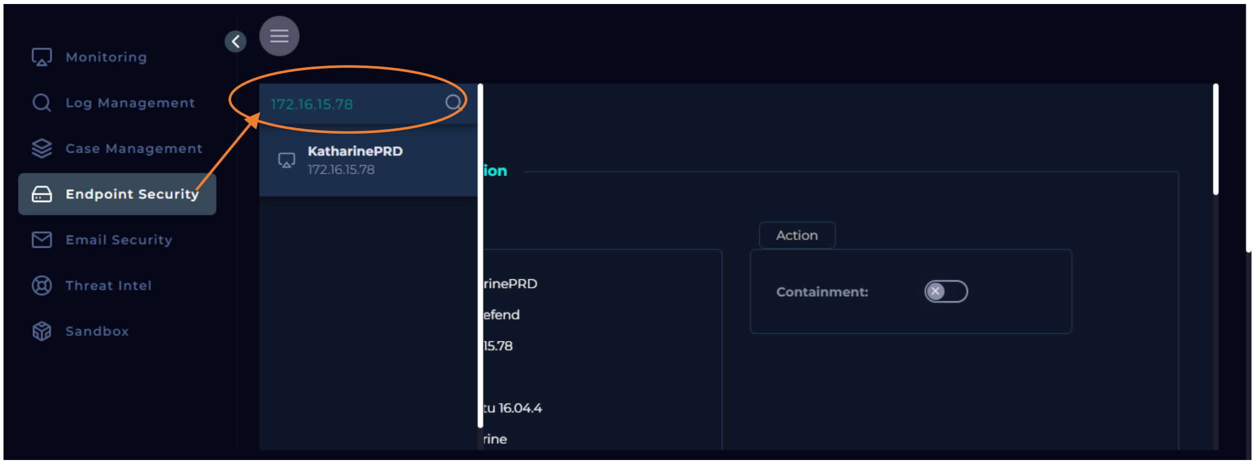
Popular threat label: trojan.msil/passwordstealera

Security vendors' analysis:

- **AhnLab-V3**: Trojan/Win32.RL_Subti.C3656886
- **Alibaba**: Backdoor/Quasar.cbdac3a7
- **AliCloud**: Backdoor/Agent.Agent
- **ALYac**: Generic.MSIL.PasswordStealerA.6EF75D8B
- **Antiy-AVL**: Trojan/MSIL.Agent
- **Arcabit**: Generic.MSIL.PasswordStealerA.6EF75D8B
- **Avast**: MSIL[Trj]
- **AVG**: MSIL[Trj]

- **Reference result.**
- **The File is Trojan.**

Endpoint Security:



172.16.15.78

KatharinePRD
172.16.15.78

ion

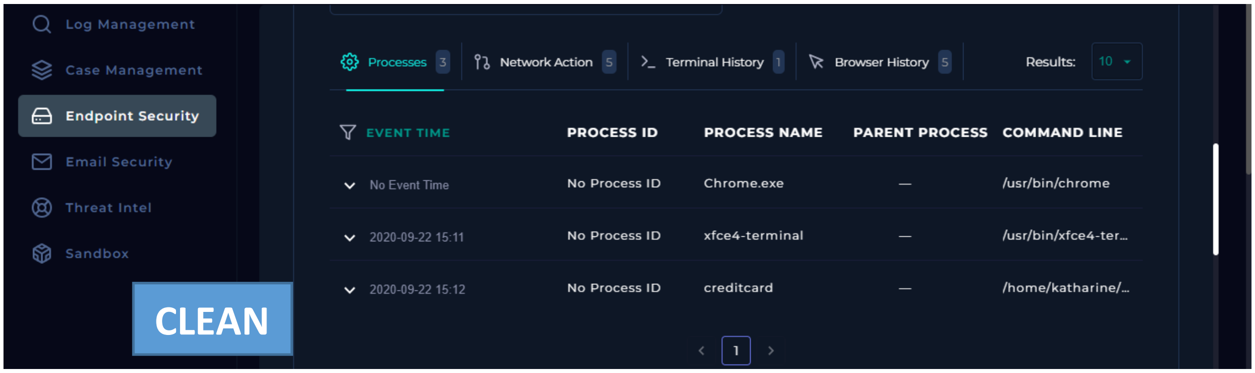
Action

Containment: ☒

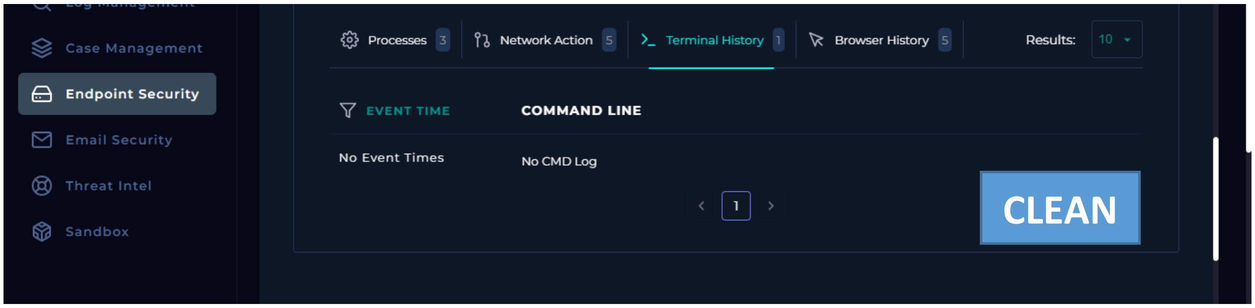
rinePRD
efend
15.78
tu 16.04.4
rine

After thoroughly reviewing the processes section from the endpoint, as well as verifying all other relevant sections within the Endpoint Security system, we confirmed that no malicious commands were installed or executed. The system appears to be secure and free from any suspicious activities.

Please refer to the attached images for the detailed process records and terminal logs for further reference.



EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
No Event Time	No Process ID	Chrome.exe	—	/usr/bin/chrome
2020-09-22 15:11	No Process ID	xfce4-terminal	—	/usr/bin/xfce4-ter...
2020-09-22 15:12	No Process ID	creditcard	—	/home/katharine/...



EVENT TIME	COMMAND LINE
No Event Times	No CMD Log

Conclusion:

The incident reported under **Event ID: 61**, with the rule **SOC126 - Suspicious New Autorun Value Detected**, was carefully analyzed and resolved. The event occurred on **February 14, 2021, at 06:40 PM** on the host **KatharinePRD**, with the malicious process **OliwciaPrivInstaller.exe** being detected. The process hash, identified as **436fa243bbfed63a99b8e9f866cd80e5**, was flagged by 60 out of 73 security vendors on VirusTotal as associated with the **trojan.msil/passwordstealera** malware family. The file size was **348.00 KB**, and Endpoint Security confirmed that the device action taken was successful, resulting in the process being cleaned.

In terms of network analysis, the **destination IP address 172.16.15.78**, belonging to the internal network, received suspicious traffic from multiple external IP addresses. These public source IP addresses, including **114.114.114.114**, **13.107.4.52**, **193.161.193.99**, and others, were flagged by threat intelligence as potentially malicious. VirusTotal scanning further confirmed that the source IP **67.68.210.95** was flagged by 18 security vendors as malicious, reinforcing the suspicion of an external threat attempting to target the internal device at **172.16.15.78**.

Upon reviewing the logs, one of the suspicious activities involved a **GET request** to the URL **https://amesiana.com/**, which was detected in the logs. The request method **GET** indicates an attempt to retrieve data from this website, which, given the context of the attack, suggests a potential attempt to exfiltrate or communicate with a malicious domain. However, no data was sent from the internal system, as indicated by the absence of any **POST** requests or outbound data transfer logs.

The **Email Security** section was also scrutinized, revealing that no emails had been sent from the affected host, confirming that the malicious process did not execute any outbound email communication as part of its payload.

Endpoint Security's review of all related sections confirmed that no further malicious commands were installed or executed, aside from the initial detection of the trojan-infected executable. The thorough investigation of system processes, coupled with terminal logs, showed that the system is now secure, and no residual malicious activity was found.

Based on the collected evidence, this attack was determined to be external, originating from a range of suspicious IPs, and intended to compromise internal systems through the **OliwciaPrivInstaller.exe** process. The swift response, combined with effective device cleaning and process removal, mitigated the risk of further compromise. Additionally, network traffic analysis and VirusTotal results confirmed that both the IP addresses and file hash were associated with malicious activity, thereby validating the security team’s decision to contain and clean the system.