Official incident report

Event ID: 92

Rule Name: SOC146 - Phishing Mail Detected - Excel 4.0 Macros

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:
93

Event Date and Time:
Jun, 13, 2021, 02:13 PM

Rule:
SOC146 - Phishing Mail Detected - Excel 4.0 Macros

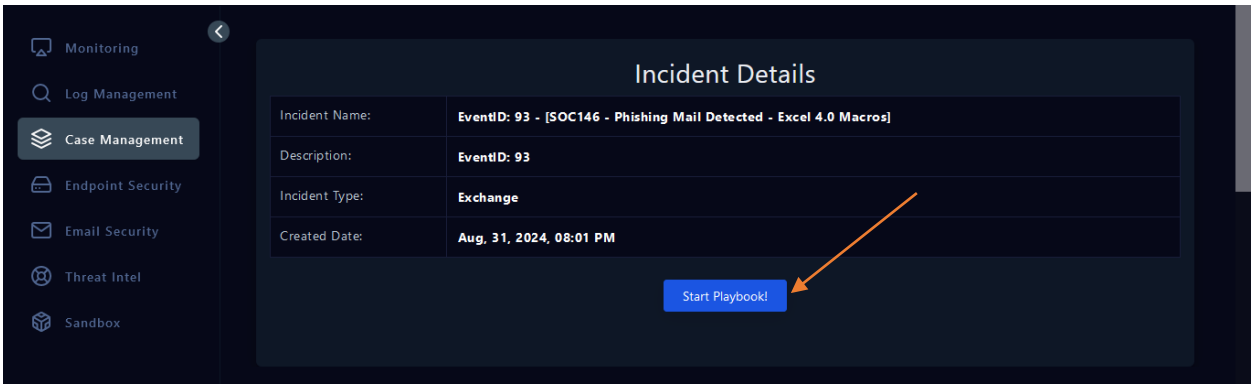
Level:
Security Analyst

Network Information Details

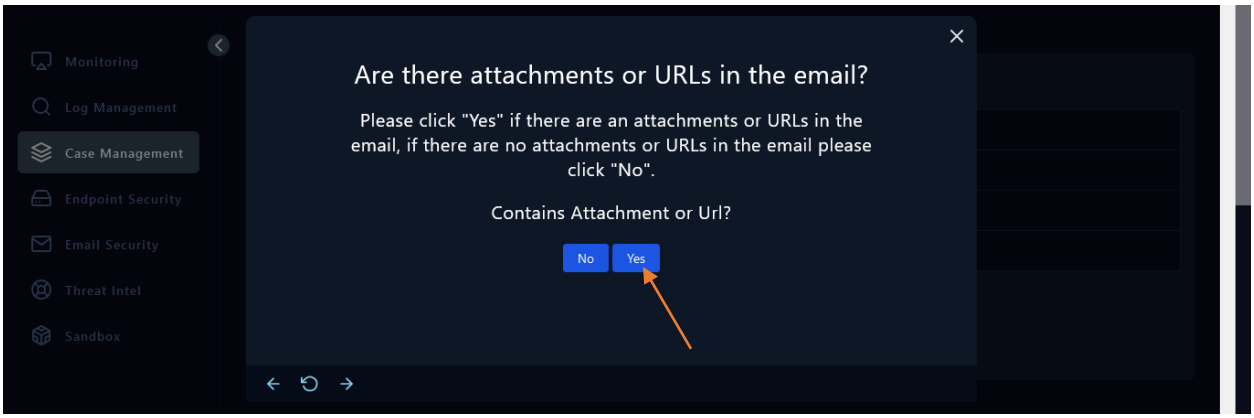
Source Address: trenton@tritowncomputers.com

SMTP Address:
24.213.228.54

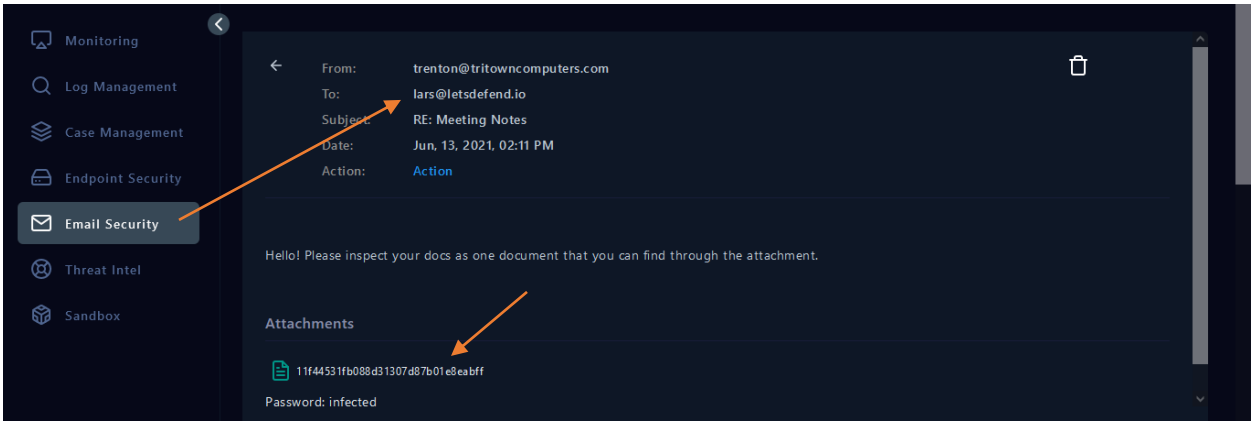
Let’s start the playbook:



Playbook Inquiry: Are there attachments or URLs in the email?



We will confirm by selecting 'Yes.' To validate this, we'll access the email security system and input the targeted email to demonstrate the containment process.

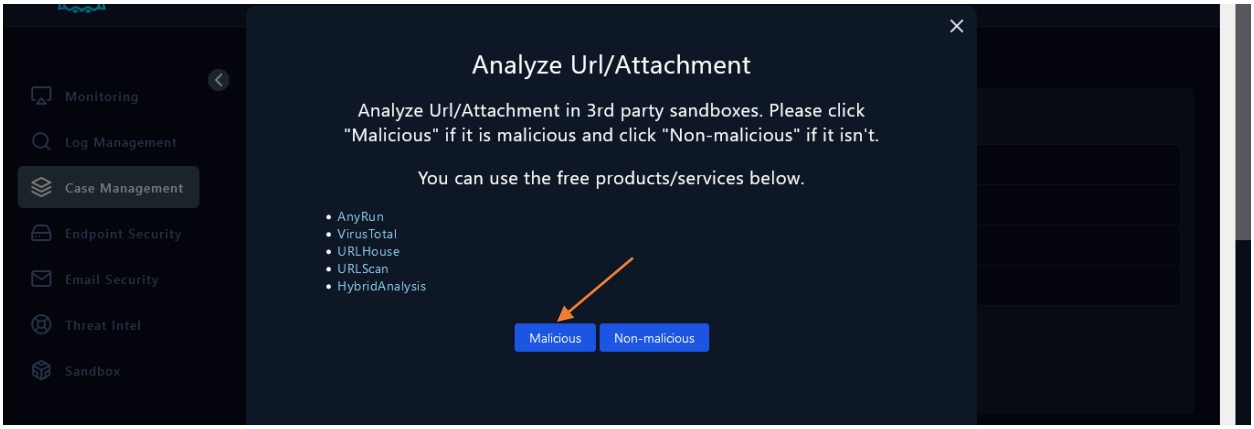


The attached file, named '11f44531fb088d31307d87b01e8eabff,' represents the containment evidence.

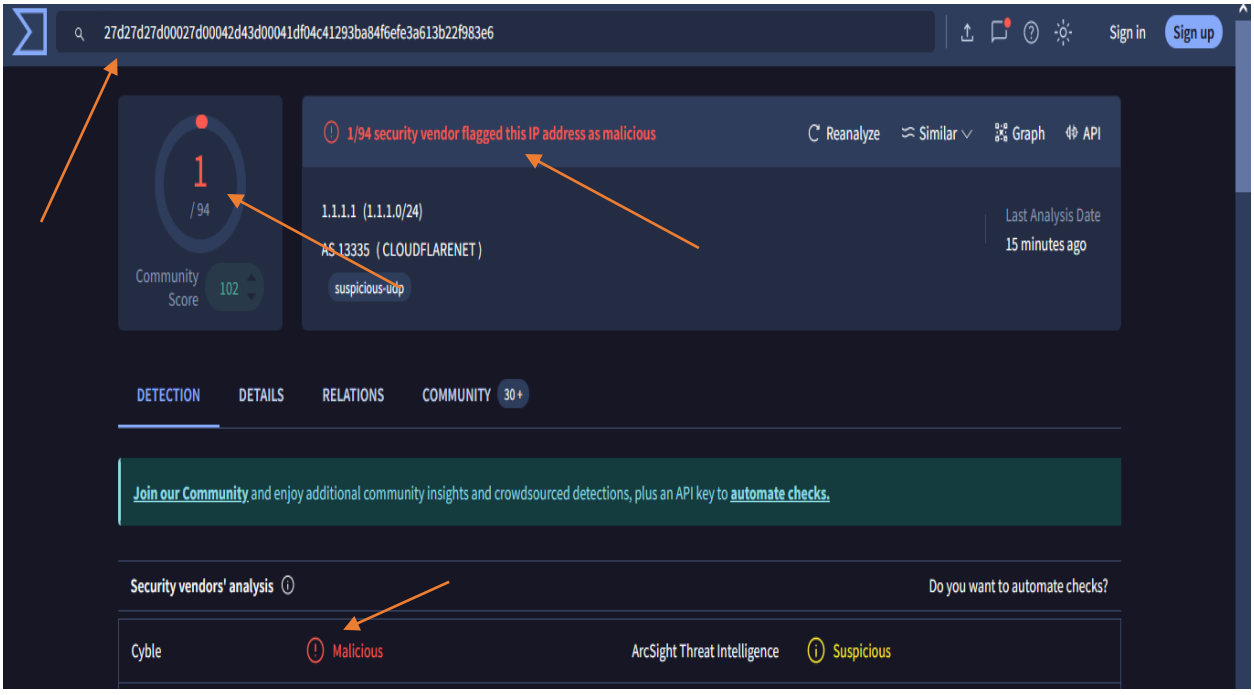
Detection:

Threat Intelligence Results

Playbook Inquiry: Analyze Url/Attachment. Analyze Url/Attachment in 3rd party sandboxes. Please click "Malicious" if it is malicious and click "Non-malicious" if it isn't.

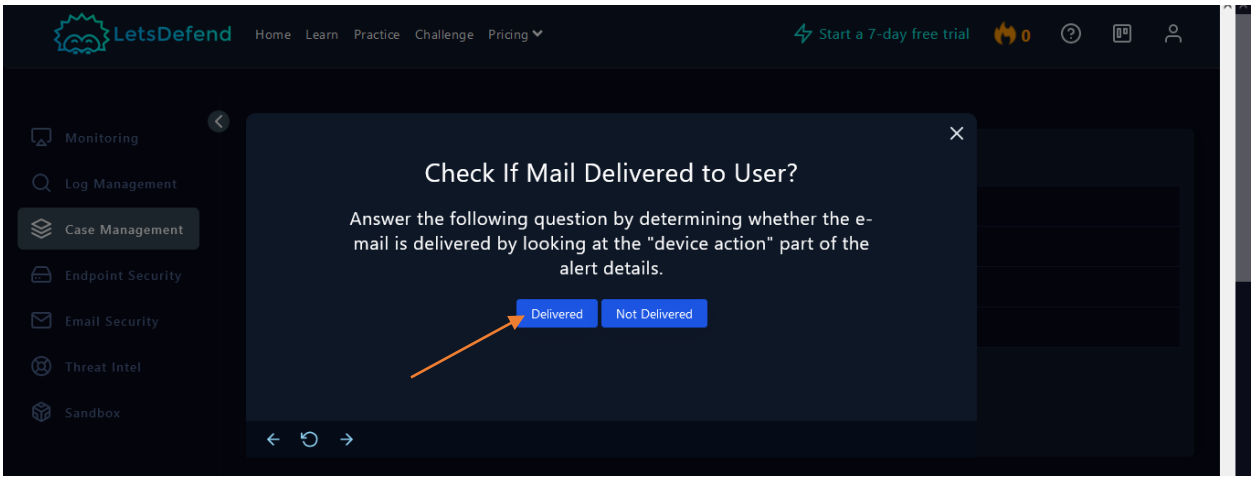


We will classify the file as Malicious based on our analysis from Virus Total Please refer to the attached photo for details

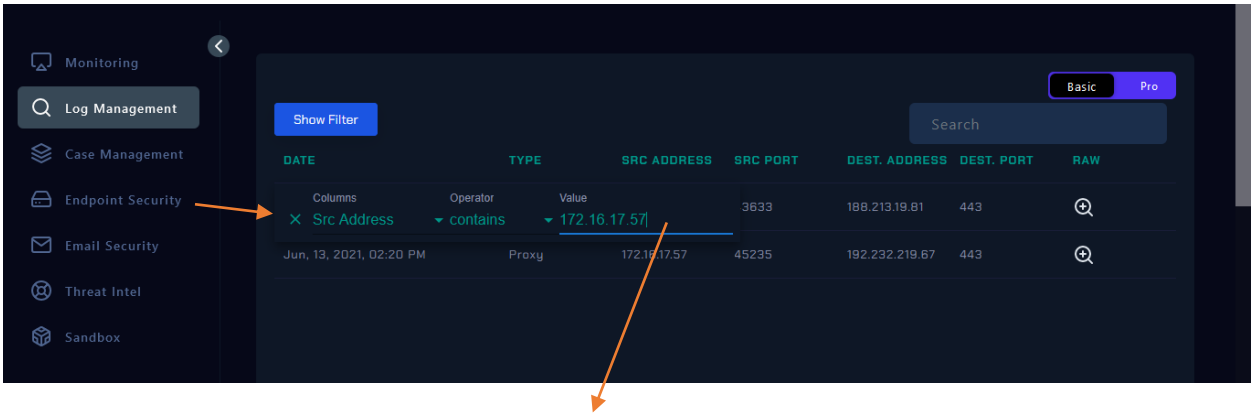


Analysis:

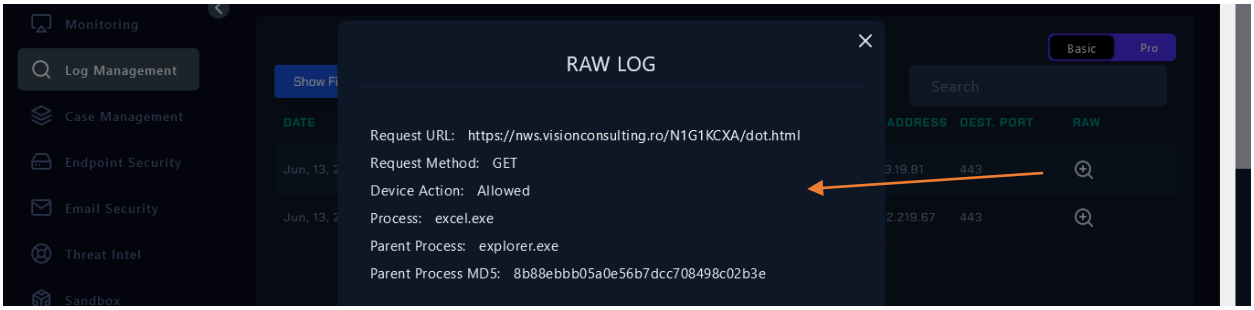
Playbook Inquiry: Check If Mail Delivered to User?



We will select 'Delivered' based on our log management analysis, with a detailed explanation provided for each log entry.



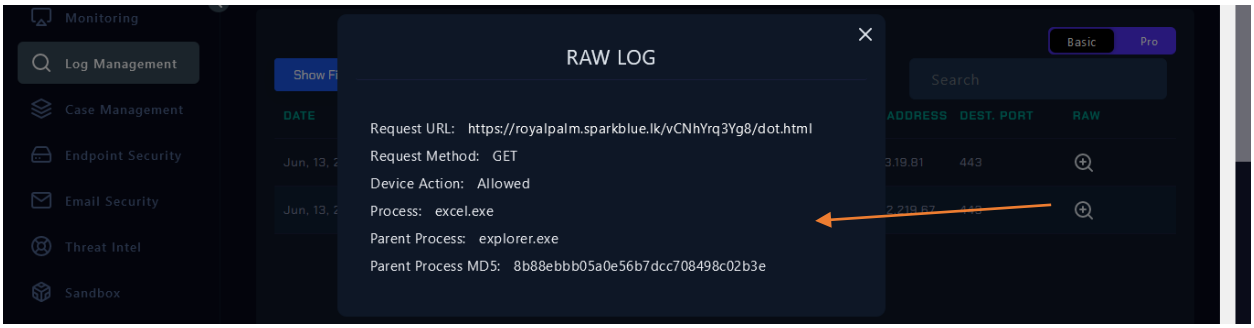
The IP address we identified corresponds to **Lars' device**, as confirmed through Endpoint Security.



Log 1:

- **Request URL:** `https://nws.visionconsulting.ro/N1G1KCXA/dot.html`
- **Request Method:** GET
- **Device Action:** Allowed
- **Process:** `excel.exe`
- **Parent Process:** `explorer.exe`
- **Parent Process MD5:** `8b88ebbb05a0e56b7dcc708498c02b3e`

Explanation: This log shows that an HTTP GET request was made to the URL `https://nws.visionconsulting.ro/N1G1KCXA/dot.html`. The request was processed by the `excel.exe` application, which was launched by `explorer.exe`. The action was allowed, indicating that the request was permitted by the security system.

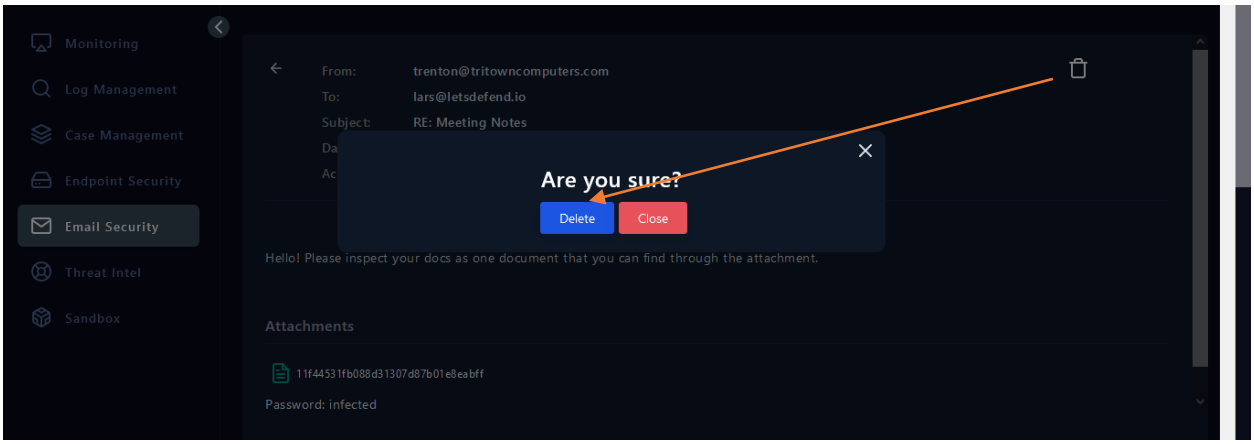


Log 2:

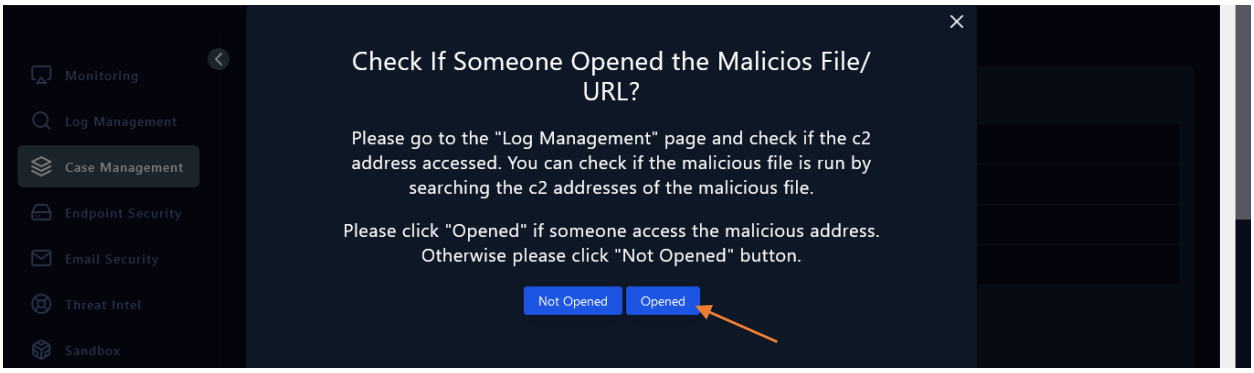
- **Request URL:** `https://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html`
- **Request Method:** GET
- **Device Action:** Allowed
- **Process:** `excel.exe`
- **Parent Process:** `explorer.exe`
- **Parent Process MD5:** `8b88ebbb05a0e56b7dcc708498c02b3e`

Explanation: This log entry records an HTTP GET request to the URL `https://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html`. Similar to the first log, the request was made by `excel.exe` and initiated by `explorer.exe`. The request was allowed by the device, which suggests that it was not blocked or flagged by the security system.

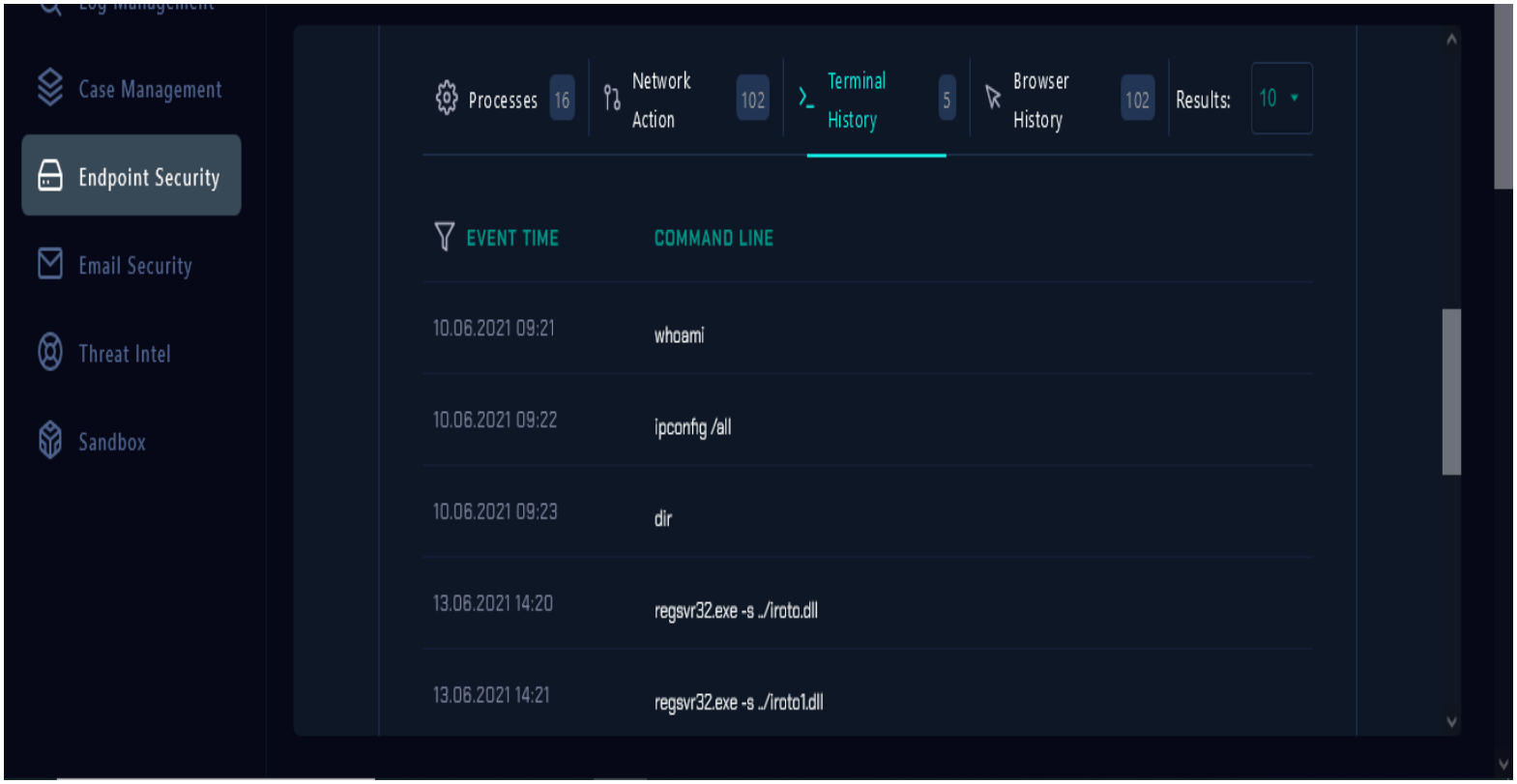
Playbook Order: Delete Email from Recipient!



Playbook Order: Check If Someone Opened the Malicios File/URL?



We will classify the file as 'Opened' based on the log management history. Additionally, we will verify this by reviewing the Terminal History section in Endpoint Security for further confirmation.



The attacker utilized the following commands from the Terminal History section. I will provide an explanation of the purpose and usage of each command.

Terminal History 1:

- **Date/Time:** 10.06.2021 09:21
- **Command:** `whoami`

Explanation: This command displays the username of the currently logged-in user, providing information about the user account under which the commands are being executed.

Terminal History 2:

- **Date/Time:** 10.06.2021 09:22
- **Command:** `ipconfig /all`

Explanation: This command retrieves and displays detailed network configuration information for all network interfaces on the system, including IP addresses, subnet masks, and default gateways.

Terminal History 3:

- **Date/Time:** 10.06.2021 09:23
- **Command:** `dir`

Explanation: This command lists the files and directories in the current directory, providing an overview of the contents and structure of the directory.

Terminal History 4:

- **Date/Time:** 13.06.2021 14:20
- **Command:** `regsvr32.exe -s ../iroto.dll`

Explanation: This command silently registers the `iroto.dll` dynamic link library (DLL) with the system, making its functionality available to other applications.

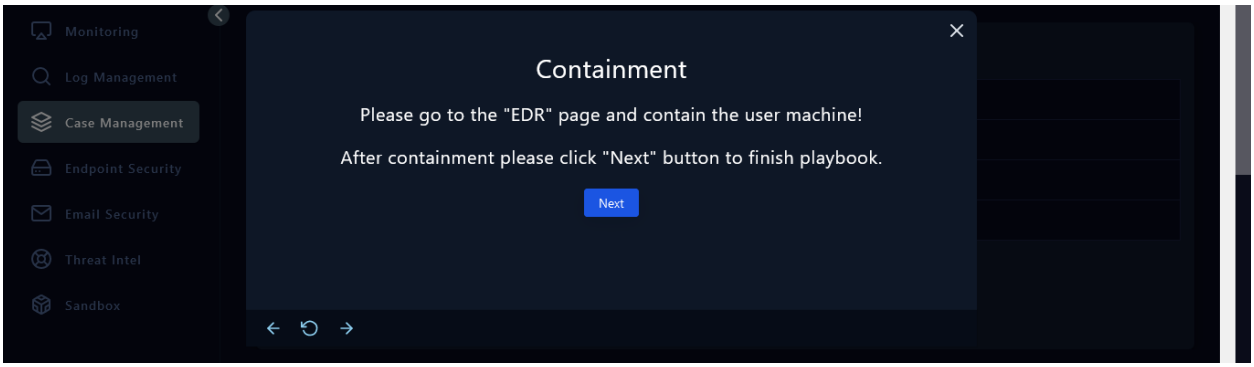
Terminal History 5:

- **Date/Time:** 13.06.2021 14:21
- **Command:** `regsvr32.exe -s ../iroto1.dll`

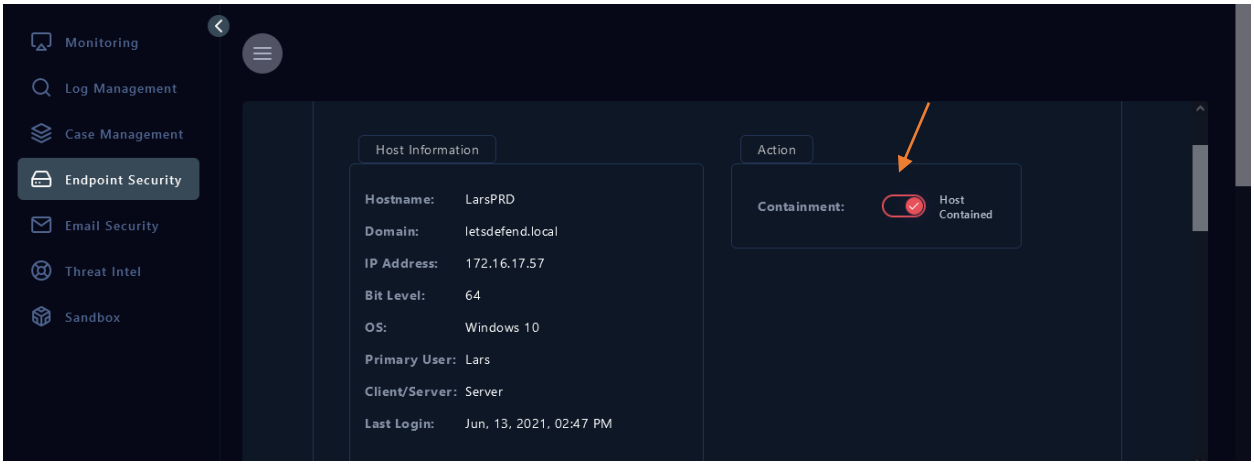
Explanation: Similar to the previous command, this command silently registers the `iroto1.dll` DLL with the system, indicating the attacker may be deploying or configuring additional components.

The commands executed in the Terminal History provide insight into the attacker's actions. The use of `whoami` and `ipconfig /all` indicates an attempt to gather system and network information. The `dir` command suggests a check of the directory contents, while the registration of `iroto.dll` and `iroto1.dll` indicates the installation of potentially malicious components. These activities collectively point to a reconnaissance phase followed by the deployment of payloads, highlighting a targeted attempt to compromise and manipulate the system.

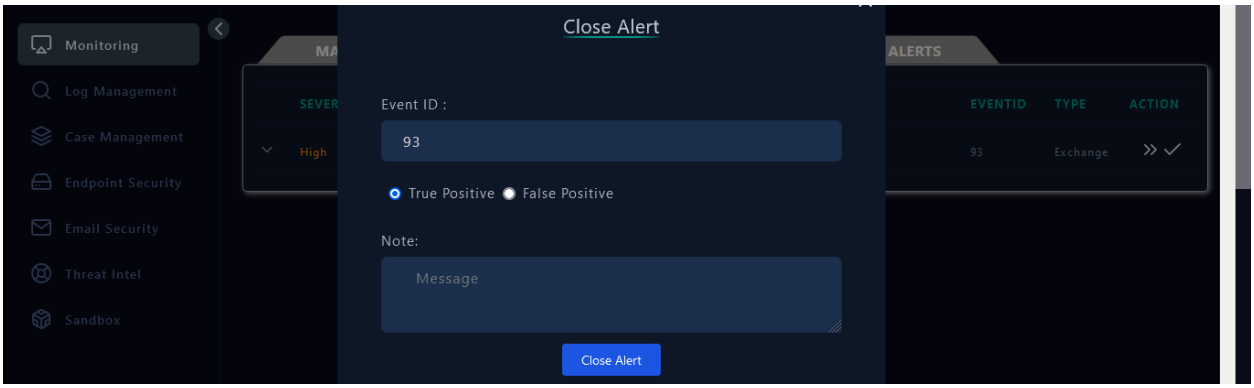
Playbook Order: Containment. Please go to the "EDR" page and contain the user machine!



Based on our previous analysis, we need to contain the device as it has already been compromised.



Containment has been successfully achieved.



We have confirmed the alert as a True Positive and have resolved it accordingly.

Conclusion

On June 13, 2021, at 2:13 PM, Event ID 93 triggered an alert under Rule SOC146, identifying a phishing email utilizing Excel 4.0 Macros. Our investigation into the incident revealed critical details about the attack, allowing us to take decisive action.

Event Summary: The phishing email originated from `trenton@tritowncomputers.com` with an SMTP address of `24.213.228.54`. The attached file, named `11f44531fb088d31307d87b01e8eabff`, was flagged as malicious based on our analysis with VirusTotal, confirming it contained harmful elements. To verify this, we examined the email security system, where the attachment served as the primary evidence of containment.

Network and Log Analysis: We assessed the logs related to the email's impact:

- **Log 1:** An HTTP GET request was made to `https://nws.visionconsulting.ro/N1G1KCXA/dot.html`, processed by `excel.exe` and launched by `explorer.exe`. This log confirmed that the request was permitted by the security system, indicating no immediate blocking or alerts at the time.
- **Log 2:** Similarly, an HTTP GET request to `https://royalpalm.sparkblue.lk/vCNhYrq3Yg8/dot.html` was also handled by `excel.exe` under `explorer.exe`. The lack of any blockage suggests that the system allowed the potentially malicious content without interference.

The analysis of these logs affirmed that the email was delivered to the user, and the file was opened, as indicated by our log management history. Further verification through the Terminal History section provided additional insights into the attacker's actions.

Terminal History Insights:

- **Commands Executed:**
  - **`whoami`** (June 10, 2021, 09:21): Revealed the user account details.
  - **`ipconfig /all`** (June 10, 2021, 09:22): Provided comprehensive network configuration.
  - **`dir`** (June 10, 2021, 09:23): Listed directory contents.
  - **`regsvr32.exe -s ../iroto.dll`** (June 13, 2021, 14:20): Silently registered the `iroto.dll` DLL, indicating the deployment of a potentially malicious component.
  - **`regsvr32.exe -s ../iroto1.dll`** (June 13, 2021, 14:21): Registered another DLL, suggesting further deployment of malicious components.

These commands reveal a deliberate reconnaissance phase followed by the installation of malicious payloads. The use of system commands for gathering information and deploying components signifies a sophisticated attack aimed at compromising the system.

Containment and Resolution: Given the evidence and our findings, we proceeded with containment measures. The device was identified as compromised based on our analysis, and we successfully executed containment procedures. The alert was confirmed as a True Positive, and the incident has been resolved accordingly.

Our thorough investigation and effective response have ensured that the threat was managed and mitigated, safeguarding the integrity of our network and systems. The incident underscores the importance of vigilant monitoring and prompt action in cybersecurity operations.