



Official incident report

Event ID: 31

Rule Name: SOC104 - Malware 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

Official incident report	1
Event ID: 31	1
Rule Name: SOC104 - Malware Detected	1
Table of contents	2
Event Details	3
Network Information Details	4
Analysis	5
Log management	5
Security Email	7
Detection	8
Threat intelligence	8
Endpoint Security	10
Conclusion	14

Event Details

Event ID:

31

Event Date and Time:

Oct, 29, 2020, 07:55 PM

Rule:

SOC104 - Malware Detected

Level:

Security Analyst

Hostname:

JohnComputer

File Name:

Purchase-Order_NO.231101.exe

File Hash:

cdde99520664ac313d43964620019c61

File Size:

616.50 KB

Device Action:

Allowed

Network Information Details

Destination IP Address:

- 172.16.17.82 (Internal)
 - This IP address falls within the private IP range (172.16.0.0 to 172.31.255.255), indicating it belongs to your organization's internal network. Any traffic directed to this address remains within the local network. The device with this IP address is located within your internal environment.

Source IP Address:

- 13.107.4.50 (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 communication or potential interaction is coming from an entity on the internet. Depending on the nature of the observed activity, this external source could represent a legitimate service, a benign connection, or a potential threat.

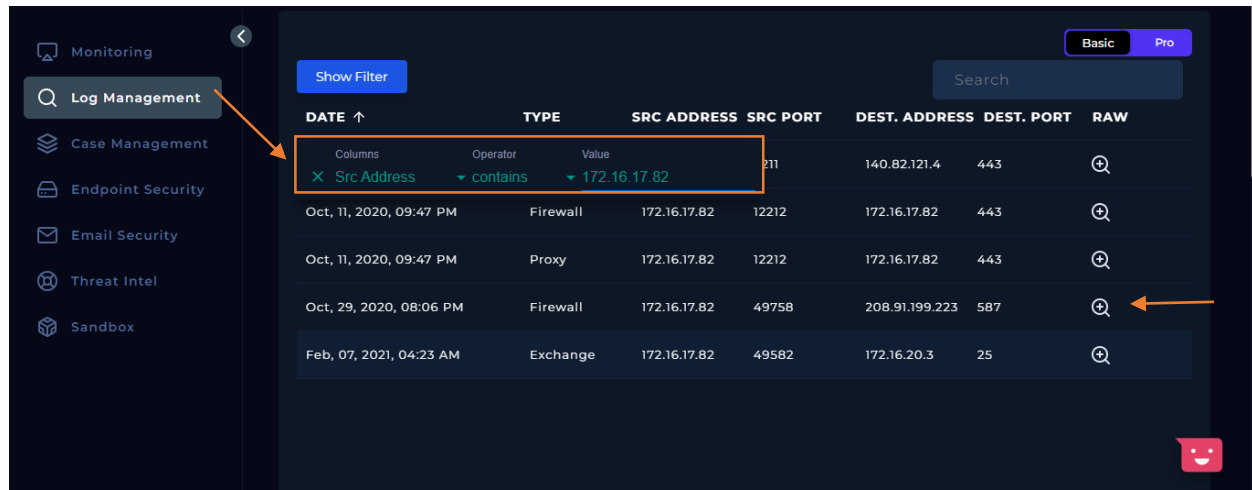
- **The attack is external**

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.



The screenshot shows a security dashboard with a sidebar on the left containing navigation links: Monitoring, Log Management (highlighted with an orange arrow), Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main panel displays a log management interface with a 'Show Filter' button and a search bar. Below these, a table lists log entries with columns: DATE ↑, TYPE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, DEST. PORT, and RAW. A filter is applied to the SRC ADDRESS column, showing 'X Src Address' with a dropdown menu set to 'contains' and the value '172.16.17.82'. The table contains five entries, with the third entry (Oct, 29, 2020, 08:06 PM, Firewall, 172.16.17.82, 49758, 208.91.199.223, 587) highlighted by an orange arrow pointing to its RAW column icon.

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
		Columns	Operator	Value		
		X Src Address	contains	172.16.17.82		
Oct, 11, 2020, 09:47 PM	Firewall	172.16.17.82	12212	172.16.17.82	443	⊕
Oct, 11, 2020, 09:47 PM	Proxy	172.16.17.82	12212	172.16.17.82	443	⊕
Oct, 29, 2020, 08:06 PM	Firewall	172.16.17.82	49758	208.91.199.223	587	⊕
Feb, 07, 2021, 04:23 AM	Exchange	172.16.17.82	49582	172.16.20.3	25	⊕

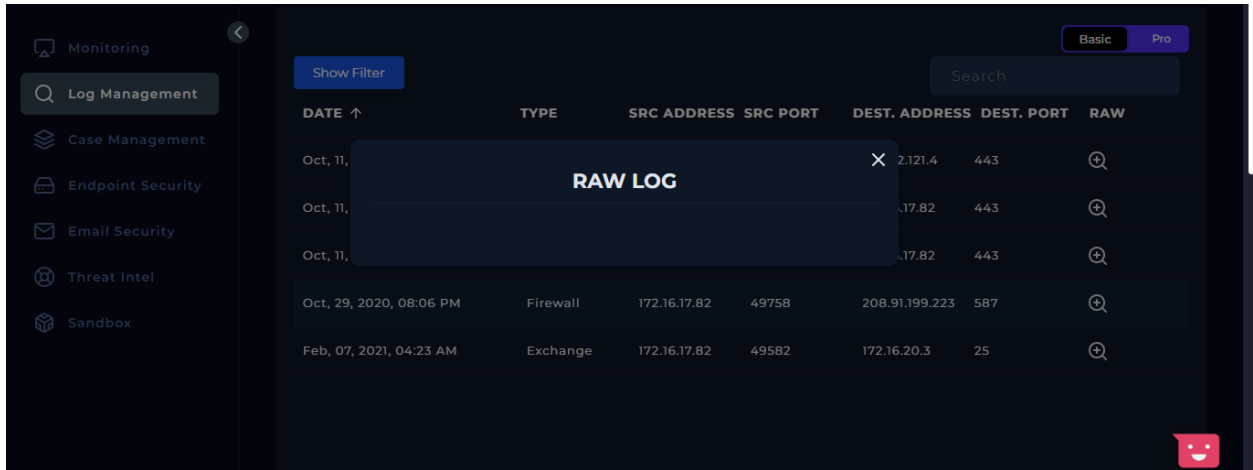
1 Log record for the Source IP regarding to our alert date and time.

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

We will explain it step by step

Log Analysis

- **Log1:**

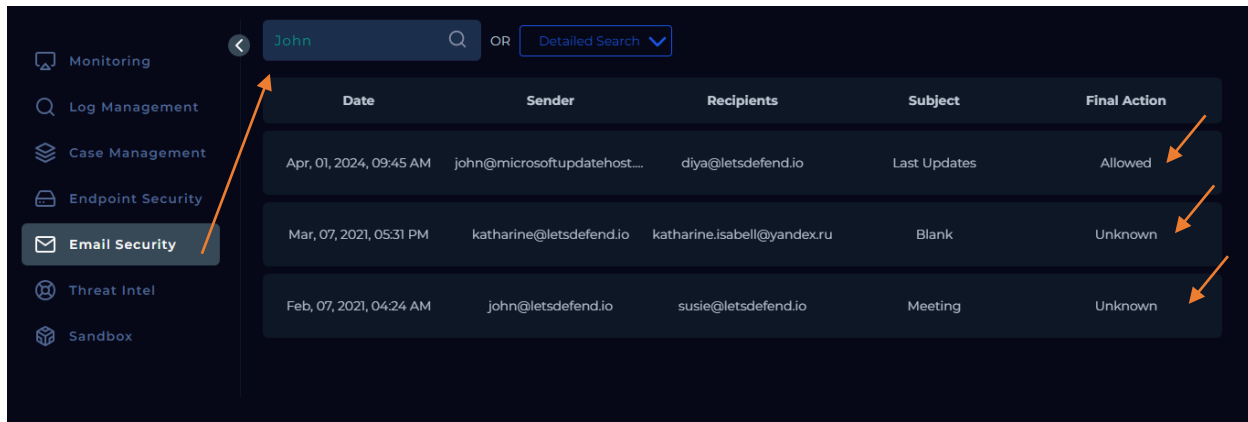


The screenshot shows a security monitoring interface with a sidebar on the left containing menu items: Monitoring, Log Management (selected), Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main area displays a log table with columns: DATE ↑, TYPE, SRC ADDRESS, SRC PORT, DEST. ADDRESS, DEST. PORT, and RAW. A modal window titled 'RAW LOG' is open, obscuring the first three rows of the table. The table contains two visible rows of log data.

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Oct, 11, 2020, 08:06 PM	Firewall	172.16.17.82	49758	208.91.199.223	587	[Icon]
Feb, 07, 2021, 04:23 AM	Exchange	172.16.17.82	49582	172.16.20.3	25	[Icon]

The first log appears to be empty, as the detected malware has erased all the data from the log management system, according to the time and date of the alert.

Email Security:



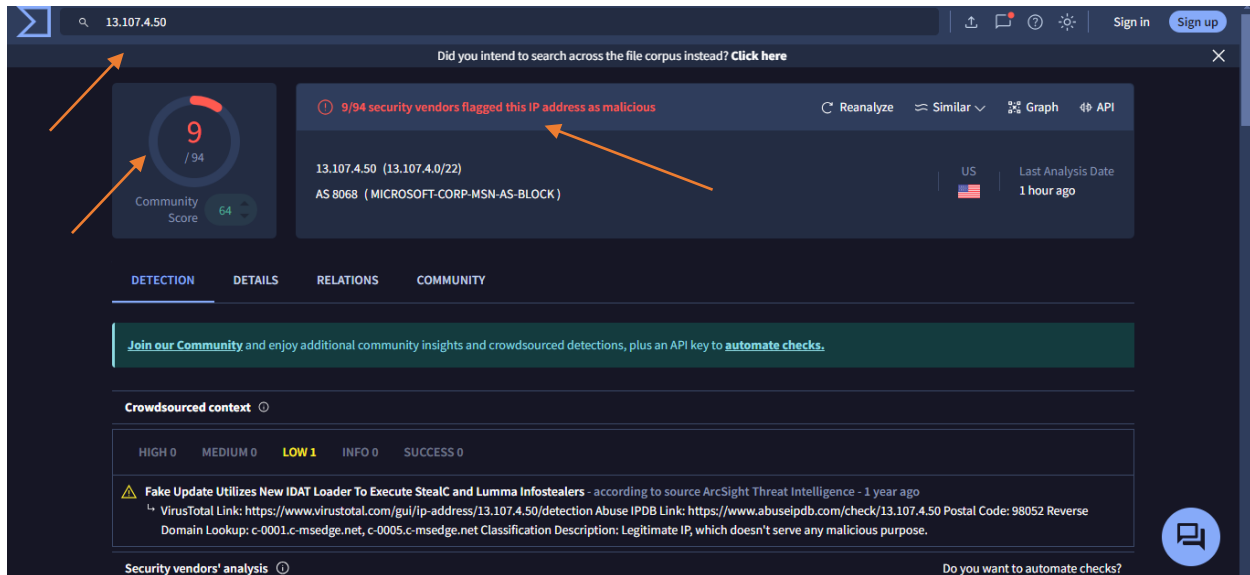
Monitoring	John	OR	Detailed Search	
Log Management				
Case Management				
Endpoint Security				
Email Security				
Threat Intel				
Sandbox				
Date	Sender	Recipients	Subject	Final Action
Apr, 01, 2024, 09:45 AM	john@microsoftupdatehost...	diya@letsdefend.io	Last Updates	Allowed
Mar, 07, 2021, 05:31 PM	katharine@letsdefend.io	katharine.isabell@yandex.ru	Blank	Unknown
Feb, 07, 2021, 04:24 AM	john@letsdefend.io	susie@letsdefend.io	Meeting	Unknown

I entered the hostname without including the "Computer" field and observed that three emails were received. However, none of the emails correspond to the specific date and time of the alert.

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.



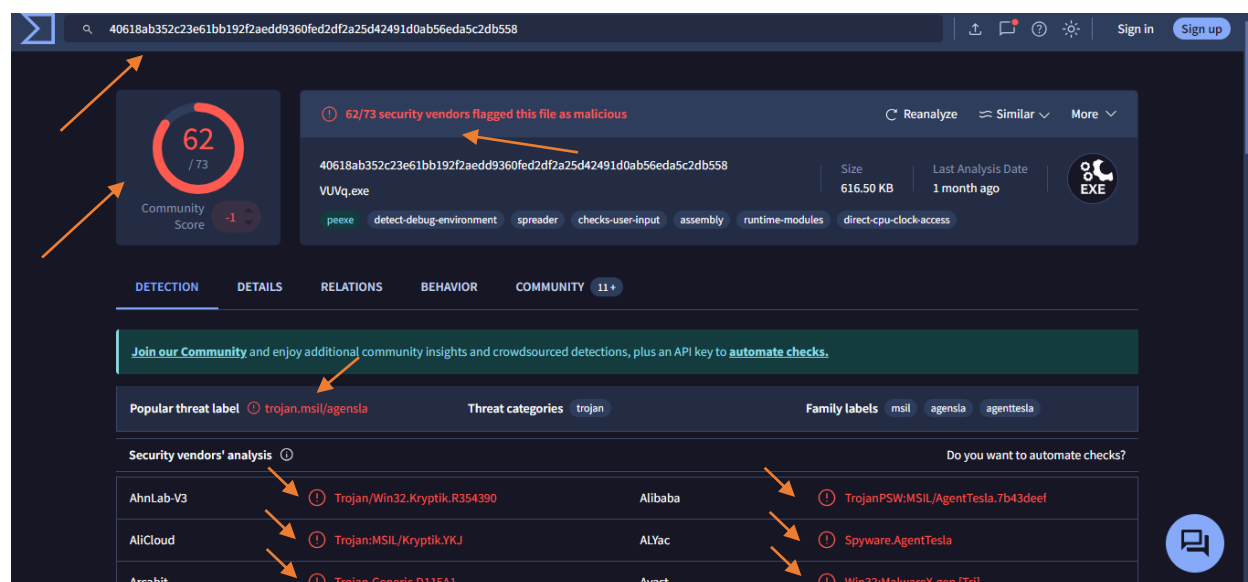
VirusTotal analysis of the source IP address 13.107.4.50 reveals that 9 out of 94 security vendors have flagged this IP as malicious. The detections include the following:

- alphaMountain.ai: Malicious
- Antiy-AVL: Malicious
- BitDefender: Malware
- CRDF: Malicious
- CyRadar: Malicious
- ESTsecurity: 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 File Hash:

40618ab352c23e61bb192f2aedd9360fed2df2a25d42491d0ab56eda5c2db558

VirusTotal analysis of the file hash

40618ab352c23e61bb192f2aedd9360fed2df2a25d42491d0ab56eda5c2db558 reveals that 62 out of 73 security vendors have flagged this file as malicious. The file is primarily associated with the trojan label **trojan.msil/agensla**, indicating a high likelihood of malicious behavior.

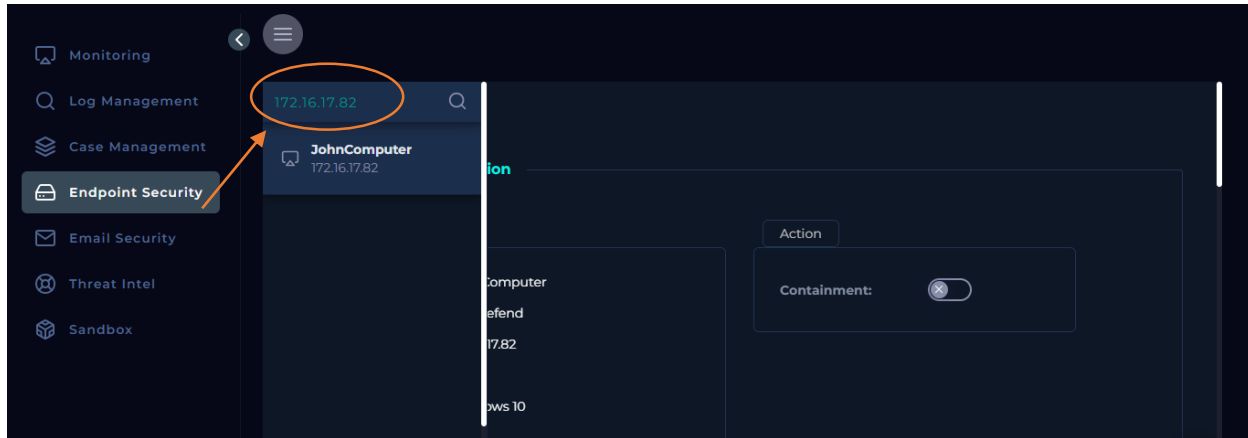
Notable detections include:

- **AhnLab-V3:** Trojan/Win32.Kryptik.R354390
- **Alibaba:** TrojanPSW/AgentTesla.7b43deef
- **AliCloud:** Trojan/Kryptik.YKJ
- **ALYac:** Spyware.AgentTesla
- **Arcabit:** Trojan.Generic.D115A1
- **Avast:** Win32[Trj]
- **AVG:** Win32[Trj]
- **Avira (no cloud):** HEUR/AGEN.1308735

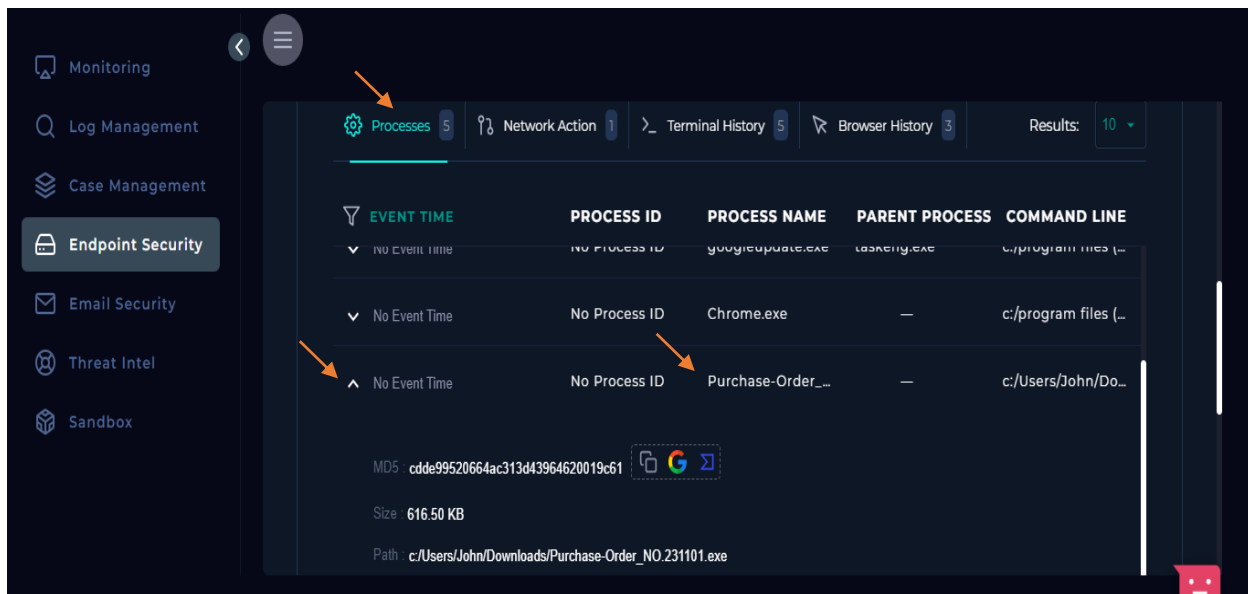
These results indicate that the file is likely a significant threat, with associations to spyware and trojans like **AgentTesla** and **Kryptik**, often used for credential theft and remote access capabilities.

- [Reference result.](#)

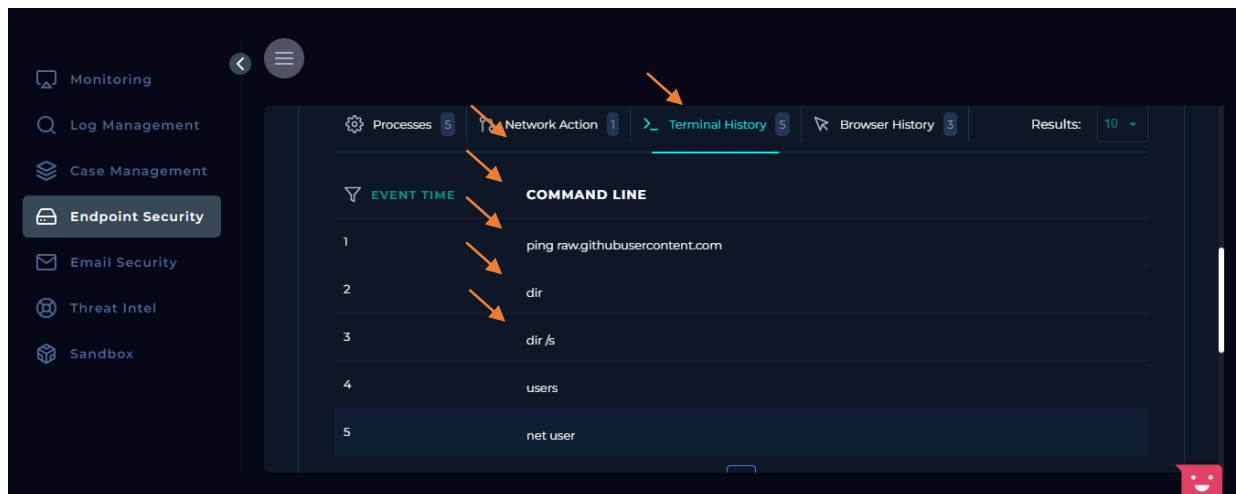
Endpoint Security:



- There are five records in the process history, indicating that the malicious file *Purchase-Order_NO.231101.exe* was installed and executed on the computer. Please refer to the attached image for further details.



- We conducted a thorough review of the 5 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: `ping raw.githubusercontent.com`

The attacker used the `ping` command to check the connectivity between the compromised machine and the domain `raw.githubusercontent.com`, which hosts files for developers using GitHub. By pinging this domain, the attacker is likely verifying if the machine can reach external resources, possibly for downloading malicious scripts or tools from GitHub repositories in subsequent steps.

- **Purpose:** Testing internet connectivity or potentially preparing to download malicious payloads from GitHub.
- **Implication:** This indicates the attacker may be planning to retrieve external files or communicate with an external server.

Record 2: `dir`

The `dir` command is used to list the contents of the current directory. The attacker is inspecting the files and folders on the compromised system.

- **Purpose:** Reconnaissance to gather information about the current directory contents.
- **Implication:** The attacker is trying to understand the file structure and locate valuable or vulnerable files to exploit further.

Record 3: `dir /s`

The `dir /s` command lists all files and directories recursively from the current directory and subdirectories. This is a more thorough scan of the system, allowing the attacker to locate specific files or directories that could be of interest.

- **Purpose:** Performing a deep enumeration of the file system to identify files across the system.
- **Implication:** The attacker is exploring the entire file system, likely looking for sensitive files, credentials, or system configuration files that could be used for further exploitation.

Record 4: `users`

By entering `users`, the attacker is checking for a list of all logged-in users on the system. This is useful for identifying which accounts are available, especially if they are admin accounts or accounts with high privileges.

- **Purpose:** Identifying the user accounts on the compromised system.
- **Implication:** The attacker may be looking to escalate privileges by identifying privileged users, or they could be targeting specific user accounts to compromise further.

Record 5: `net user`

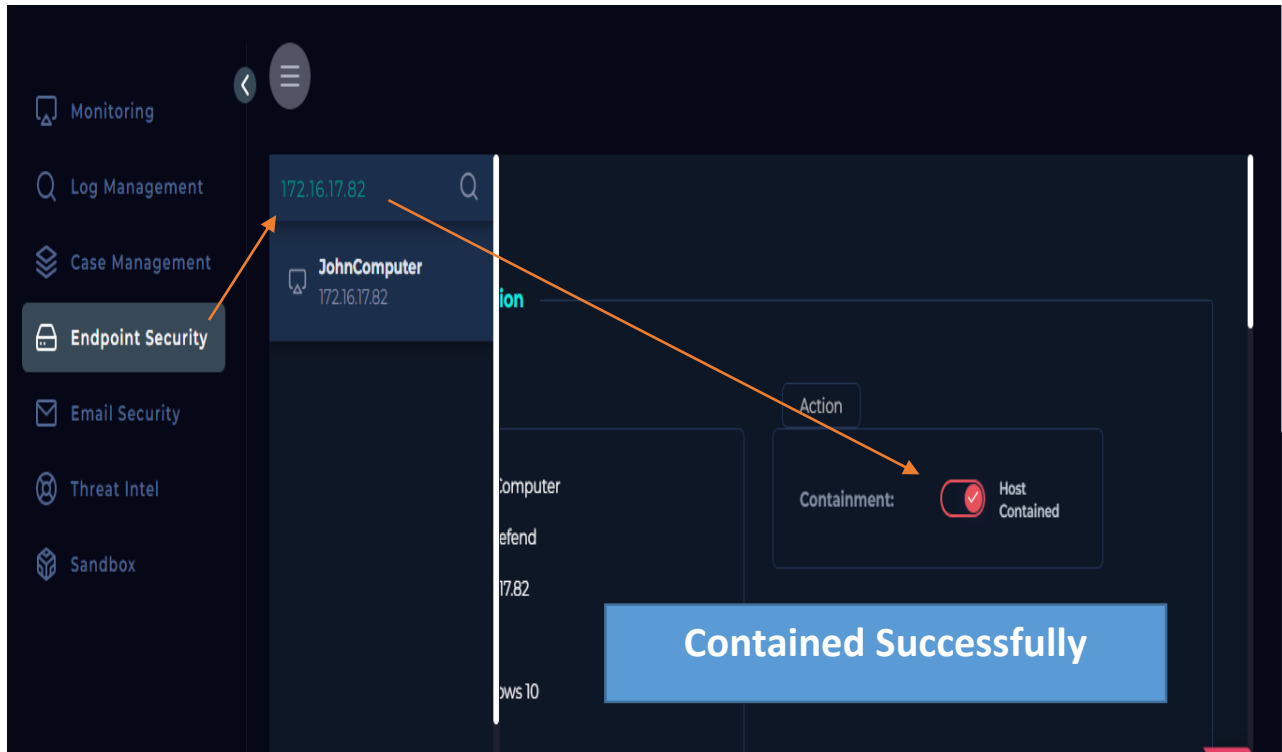
The `net user` command lists all user accounts on the machine, along with details such as when the account was created, the last login, and whether the account is an administrator.

- **Purpose:** Gathering detailed information about all users on the system, including potential admin accounts.
- **Implication:** The attacker is likely trying to identify high-privilege accounts (e.g., administrators) to either gain more control over the system or use these accounts for lateral movement across the network.

Summary of the Attacker's Actions:

1. **Connectivity Check:** The attacker first verified internet access by pinging `raw.githubusercontent.com`, likely to confirm they could download additional payloads or establish communication with external servers.
2. **System Reconnaissance:** They used the `dir` and `dir /s` commands to explore the file system, gaining knowledge about the structure and contents of the compromised machine.
3. **User Account Enumeration:** By running the `users` and `net user` commands, the attacker focused on identifying users, especially administrative ones, possibly with the intent of escalating privileges or gaining further control over the system.

Based on our thorough analysis, it is clear that the system has been compromised, with the attacker conducting reconnaissance and preparing for potential further exploitation. To prevent additional unauthorized access or data loss, immediate containment of the affected machine is critical. We recommend isolating the system from the network, terminating any malicious processes, and initiating a full forensic investigation to assess the scope of the breach and identify remediation steps.



We have successfully initiated the containment.

Conclusion:

In conclusion, the detailed analysis of Event ID 31 highlights the critical importance of prompt detection, response, and containment when dealing with a malware infection within a corporate network. This incident, detected on Oct 29, 2020, involves the execution of a malicious file—*Purchase-Order_NO.231101.exe*—on a system named *JohnComputer*. Our investigation reveals that this file, confirmed to be malicious through extensive threat intelligence and VirusTotal scans, has the potential to cause significant damage by enabling external attackers to gain unauthorized access to the network and engage in malicious activities, including data theft and reconnaissance.

Key Findings

Our analysis identified several key elements that reinforce the need for immediate action and the implementation of stronger defenses against such threats:

1. **File-Based Malware Attack:** The malicious file, *Purchase-Order_NO.231101.exe*, was allowed to run on the system despite its harmful nature. VirusTotal scans confirmed that 62 out of 73 security vendors flagged this file as malicious, associating it with well-known trojans such as **AgentTesla** and **Kryptik**. These trojans are commonly used in attacks aimed at credential theft and remote access, underscoring the threat level posed by this file. The file hash further supported the finding that this executable is part of a broader family of malware capable of exfiltrating sensitive data and allowing remote control of compromised systems.
2. **External Threat Origin:** The network traffic associated with this incident shows that the attack originated from an external IP address, **13.107.4.50**. VirusTotal analysis of this IP revealed that it had been flagged as malicious by several reputable security vendors, further validating the nature of the threat. The external IP connection confirms that the attacker is located outside of the internal network, attempting to exploit vulnerabilities in the targeted system.
3. **Internal Network Targeting:** The destination IP address, **172.16.17.82**, is a private internal IP, suggesting that the attack was specifically directed at an internal asset. This IP belongs to the organization's internal network, which heightens the risk of lateral movement and broader compromise of internal systems. The attacker's ability to reach this system indicates either exploitation of a network vulnerability or the successful execution of a phishing or social engineering attack that allowed the malware to be installed and executed on the endpoint.
4. **Empty Log Data:** A particularly concerning aspect of the incident is the discovery that the malware appears to have erased the log data from the system's log management tools. This tactic is often employed by sophisticated attackers to cover their tracks and make post-incident analysis more challenging. The absence of logs at the time of the alert suggests that the attacker was able to execute the malicious file and gain control of the system before log files could record critical information, indicating a serious compromise of the logging and monitoring systems.

5. **Email Security Observations:** Our examination of the email security systems identified that although three emails were received by the user of *JohnComputer*, none of these emails corresponded with the date and time of the alert. This observation may indicate that the initial infection vector was not email-based, or the attacker successfully bypassed email defenses. Further analysis may be required to confirm the exact method of delivery for the malware, but it is clear that the email system did not provide early warning or prevent the incident.
6. **Terminal History and Attack Progression:** The terminal history from the compromised machine provides valuable insight into the attacker's activities post-exploitation. The attacker engaged in several actions, which included verifying external connectivity, performing reconnaissance, and enumerating user accounts. These steps strongly suggest that the attacker was preparing for further exploitation or escalation, possibly attempting to gain higher privileges or access to additional sensitive data. The use of the `ping`, `dir`, `users`, and `net user` commands is indicative of an attacker probing the environment to gather intelligence on available resources, file structures, and user permissions.

Actions Taken

To mitigate the threat, the following actions have been successfully initiated:

1. **Immediate Containment:** Upon confirming the nature of the malware and the potential scope of the breach, the affected system, *JohnComputer*, was immediately isolated from the network. This step was taken to prevent the attacker from maintaining persistence, communicating with external servers, or moving laterally to other systems within the internal network.
2. **Termination of Malicious Processes:** All known malicious processes associated with *Purchase-Order_NO.231101.exe* were identified and terminated to halt further damage to the system. This involved a comprehensive review of the process history and the active state of the machine.
3. **Forensic Investigation:** A full forensic investigation has been initiated to assess the scope of the breach. This includes a detailed review of file systems, user accounts, network connections, and any additional malicious artifacts that may have been left behind by the attacker. Given the potential for credential theft and data exfiltration, the investigation will prioritize identifying any compromised accounts and mitigating any further risks to internal systems.
4. **Threat Intelligence Updates:** Based on the detection of *AgentTesla* and *Kryptik*, additional threat intelligence rules and indicators of compromise (IOCs) have been updated within the organization's security information and event management (SIEM) system. This ensures that similar threats are identified and responded to more rapidly in the future.
5. **Log Review and Improvement:** The incident revealed a critical weakness in the organization's logging capabilities. The ability of the malware to erase log data suggests the need for more robust logging and monitoring solutions. It is recommended that the organization invest in advanced logging solutions with tamper-resistant capabilities to ensure that logs are protected even in the event of a breach. This will facilitate more effective post-incident analysis in the future.

Recommendations for Future Prevention

To prevent similar incidents from occurring in the future, the following recommendations are proposed:

1. **Enhanced Endpoint Security:** Implement advanced endpoint detection and response (EDR) tools that provide real-time monitoring, behavioral analysis, and automated containment of suspicious activity. This will allow for faster detection and response to malicious activities before they can escalate.
2. **Network Segmentation:** Strengthen network segmentation to limit the spread of malware between internal devices. By isolating critical systems and sensitive data, the organization can reduce the risk of lateral movement within the network, minimizing the potential impact of future attacks.
3. **User Training and Awareness:** Increase user training on the risks of phishing, social engineering, and malicious file downloads. Regular security awareness programs will empower users to recognize and report suspicious emails, files, and activities, serving as an additional layer of defense against malware infections.
4. **Regular Security Audits:** Conduct regular security audits and penetration tests to identify and address vulnerabilities within the network. This proactive approach will help identify weaknesses in defenses before they can be exploited by attackers.

Conclusion

This incident underscores the importance of vigilance and prompt action when dealing with potential malware threats. By identifying the malicious file, isolating the compromised system, and conducting a thorough forensic investigation, the security team has effectively mitigated the immediate threat posed by this attack. Moving forward, the implementation of the recommended measures will strengthen the organization's overall security posture, ensuring that similar incidents are detected and neutralized before they can cause significant harm.