Official incident report

Event ID: 48

Rule Name: SOC107 - Privilege Escalation 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:
48

Event Date and Time:
Jan, 31, 2021, 04:20 PM

Rule:
SOC107 - Privilege Escalation Detected

Level:
Security Analyst

Hostname:
RichardPRD

File Name:
JuicyPotato.exe

File Hash:
808502752ca0492aca995e9b620d507b

File Size:
340 KB

Device Action:
Allowed

Network Information Details

Destination IP Address:

- 172.16.17.45 (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.

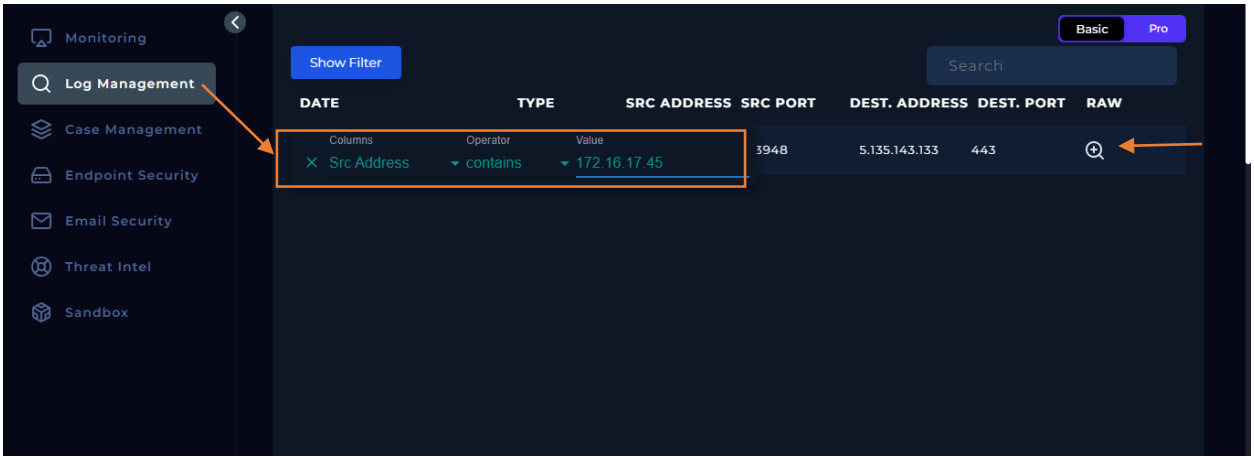
- **The attack is external**

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.



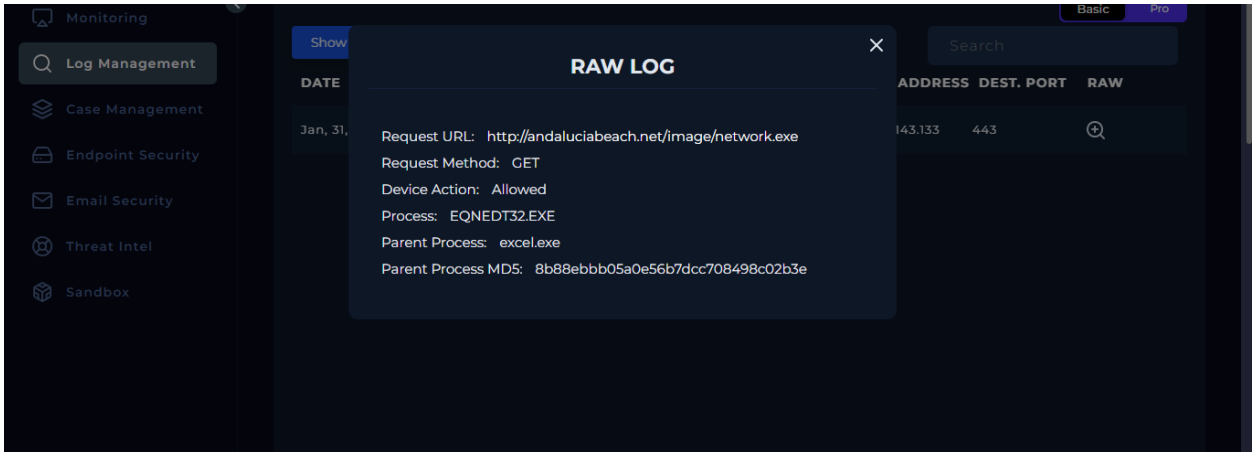
1 Log record for the Source IP regarding to our alert date.

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

We will explain it step by step

Log Analysis

- **Log1:**



This log reveals key details of a potentially malicious activity that involves the download of an executable file (`network.exe`) from a suspicious URL through a Microsoft Office process chain. Let's break it down step by step for deeper analysis:

1. Request URL: `http://andaluciabeach.net/image/network.exe`

- **Observation**: This indicates that a file named `network.exe` was requested from the URL `andaluciabeach.net/image/network.exe` via an HTTP GET request.
- **Risk**: The file name `network.exe` suggests that this is an executable, and `.exe` files are commonly used in Windows environments. Downloading executables from external, unknown URLs poses a significant risk because they could be malicious (e.g., malware or unwanted software).
- **Suspicion**: The domain name `andaluciabeach.net` appears unrelated to software distribution or known trusted services, which raises concerns about its legitimacy. Malicious actors often host malware on compromised or malicious websites under the guise of seemingly innocuous URLs.
- **Actionable Insight**: Security analysts would typically look into whether the domain has been flagged in threat intelligence sources or blocklists, and network traffic logs should be reviewed to see if similar requests have been made.

2. Request Method: GET

- **Explanation**: A GET request is typically used by web browsers or applications to request resources from a web server.
- **Risk**: In this case, the GET request is used to retrieve a potentially malicious file (`network.exe`). If this file is successfully downloaded and executed, it could lead to various security breaches, including the installation of malware.

- **Actionable Insight**: Analysts should monitor for unusual GET requests, especially if they involve downloading executable files from unknown or suspicious sources.

3. Device Action: Allowed

- **Observation**: This suggests that the action of downloading the file was permitted by the system or the security controls in place (such as a firewall or endpoint protection).
- **Risk**: Allowing the download of unknown executable files without proper security checks can lead to successful malware infection. In a secure environment, downloads from unknown URLs should be blocked or flagged for review.
- **Actionable Insight**: Security teams should configure policies that block or prompt for user verification before such downloads occur. They should also investigate why the download was allowed—whether it was due to misconfigured security controls or a lack of proper rules.

4. Process: EQNEDT32.EXE

- **Explanation**: `EQNEDT32.EXE` refers to the Microsoft Equation Editor, which is a process that was once part of Microsoft Office for rendering equations in documents.
- **Risk**: The Microsoft Equation Editor has been exploited in several known vulnerabilities (e.g., CVE-2017-11882). These vulnerabilities allow attackers to execute arbitrary code when a user opens a malicious document (like a Word or Excel file). The fact that this process is involved raises a high level of suspicion, as attackers may have used it to download or execute the `network.exe` file.
- **Actionable Insight**: If Equation Editor is not necessary for business purposes, it should be disabled to reduce the attack surface. The system should be patched if this vulnerability has not been addressed.

5. Parent Process: excel.exe

- **Explanation**: `excel.exe` is the main executable for Microsoft Excel, meaning that the `EQNEDT32.EXE` process was triggered from within Excel.
- **Risk**: This suggests that a user opened an Excel document which initiated the download process. Attackers often use malicious macros or embedded objects in Excel files to exploit vulnerabilities, leading to the execution of payloads (in this case, potentially `network.exe`).
- **Actionable Insight**: Review the Excel file that triggered this action and investigate its origin. It is crucial to analyze whether this document contained malicious macros, embedded objects, or references to exploits like CVE-2017-11882.

6. Parent Process MD5: 8b88ebbb05a0e56b7dcc708498c02b3e

- **Explanation**: This is the MD5 hash of the `excel.exe` process, which uniquely identifies the specific instance or version of the file.
- **Risk**: Although the MD5 hash doesn't inherently suggest malicious activity, comparing it to known good or malicious file hashes in a threat intelligence database could confirm whether this version of Excel has been compromised or tampered with.
- **Actionable Insight**: Cross-check this MD5 hash against threat intelligence databases (such as VirusTotal) to ensure that the `excel.exe` process has not been replaced by a malicious version.

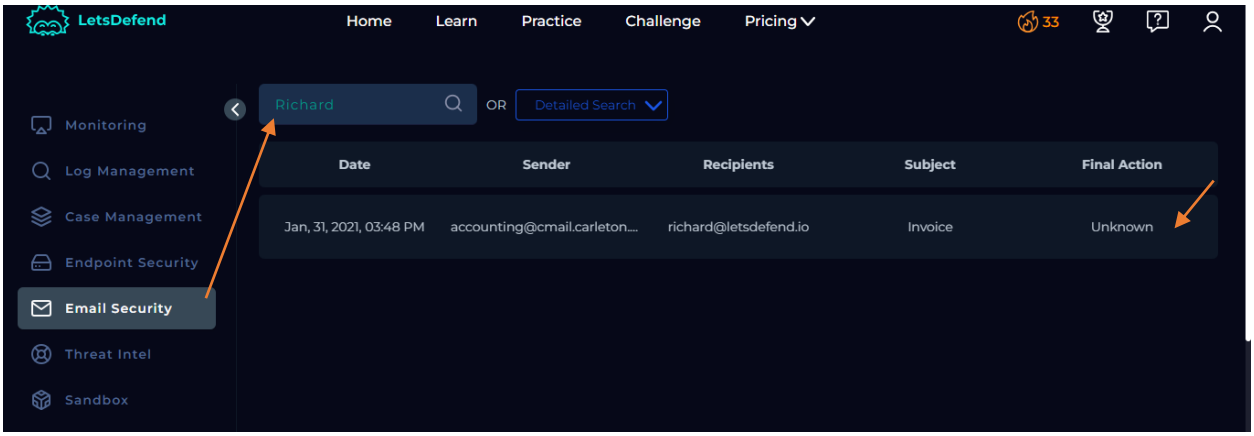
Deeper Analysis of Potential Threat:

- **Attack Vector**: This activity suggests that the attacker likely used an Excel file (possibly sent through phishing) to deliver a payload. The payload could be exploiting a known vulnerability in Equation Editor (`EQNEDT32.EXE`) to download and execute `network.exe` from the suspicious URL.
- **Malware Delivery**: If successful, the downloaded executable (`network.exe`) could be any form of malware—ransomware, spyware, or even a backdoor—granting attackers remote access or control over the system.
- **Incident Response**: The next steps would involve quarantining the affected system, analyzing the `network.exe` file for its behavior, and conducting a wider threat hunt to ensure no other systems have been compromised.

Upon verifying the MD5 hash (`8b88ebbb05a0e56b7dcc708498c02b3e`) of the `excel.exe` parent process, no anomalies were detected, and it was found to be clean. The hash does not match any known malicious signatures in threat intelligence databases, indicating that the Excel executable itself has not been tampered with or compromised.

The investigation revealed that no request was made to the Command and Control (C2) server.

Email Security:

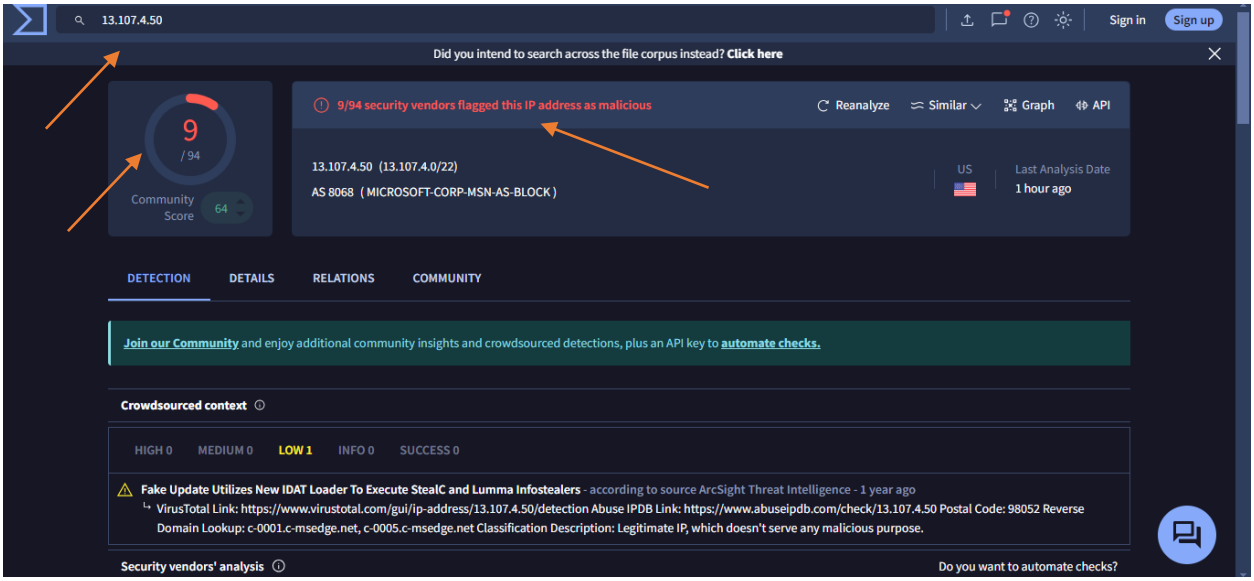


I entered the hostname without including the "Computer" field and observed that three emails were received. However, none of the emails correspond to the specific date and time of the alert, and the appears email is for a different summited case.

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.



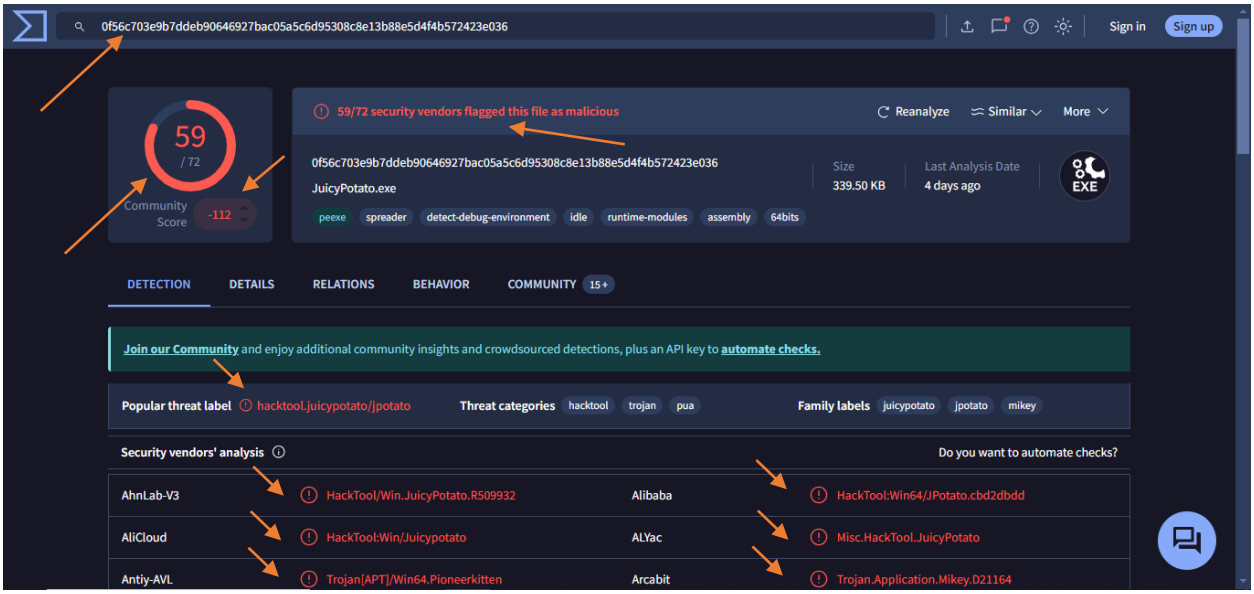
VirusTotal analysis of the IP address 13.107.4.50 indicates that 9 out of 94 security vendors have flagged this IP as malicious. The detections are as follows:

- alphaMountain.ai: Malicious
- Antiy-AVL: Malicious
- BitDefender: Malware
- CRDF: Malicious
- CyRadar: Malicious
- ESTsecurity: Malicious
- G-Data: Malware
- VIPRE: Malware

This raises a moderate level of concern about 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:
0f56c703e9b7ddeb90646927bac05a5c6d95308c8e13b88e5d4f4b572423e036

This file is primarily associated with the threat label **hacktool.juicypotato/jpotato**, indicating its potential use for privilege escalation techniques commonly seen in hacking tools.

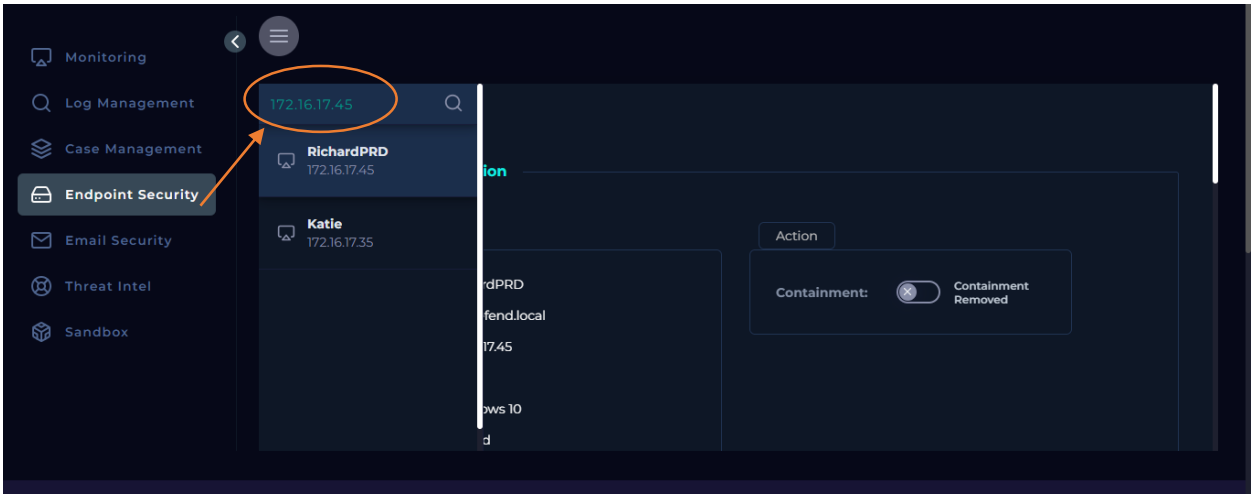
Notable detections include:

- AhnLab-V3: HackTool/Win.JuicyPotato.R509932
- Alibaba: HackTool/JPotato.cbd2dbdd
- AliCloud: HackTool/Juicypotato
- ALYac: Misc.HackTool.JuicyPotato
- Antiy-AVL: Trojan[APT]/Win64.Pioneerkitten
- Arcabit: Trojan.Application.Mikey.D21164
- Avira (no cloud): TR/JuicyPotato.twazv
- BitDefender: Gen

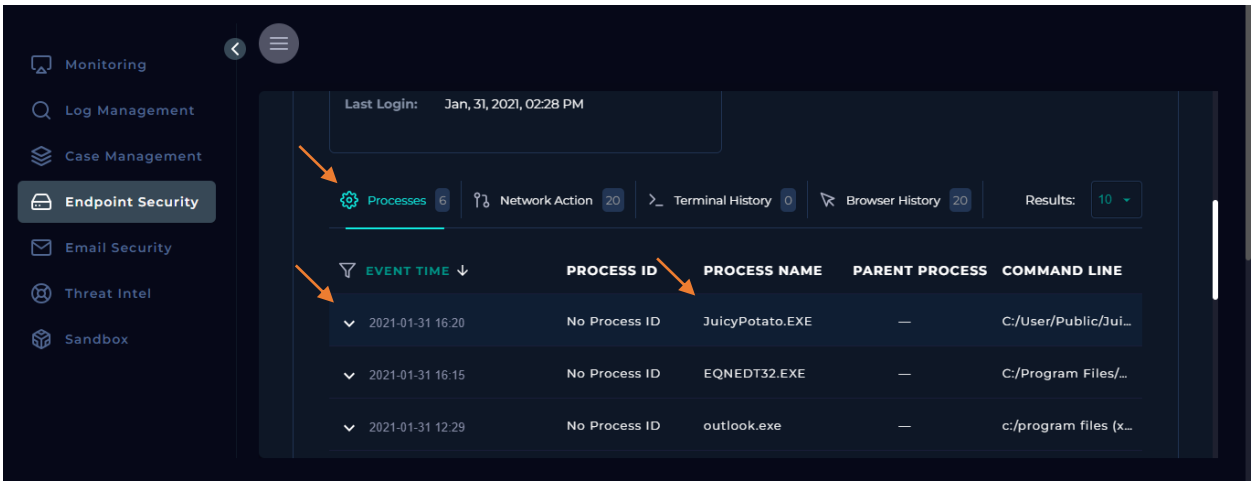
These detections suggest the file may be part of a toolkit used for privilege escalation or lateral movement in advanced persistent threat (APT) scenarios.

- **Reference result.**

Endpoint Security:



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



Based on the threat intelligence findings, the tool associated with **JuicyPotato** has been installed and successfully exploited within the system. Immediate containment measures are required to mitigate potential risks of privilege escalation and further compromise. It is critical to isolate the affected system, halt any ongoing processes related to the exploit, and conduct a comprehensive forensic investigation to assess the extent of the breach. Security controls should be reinforced to prevent similar incidents in the future.

We have successfully initiated the containment.

Conclusion:

The investigation into **Event ID 48** on **RichardPRD** system has revealed a significant security incident involving the use of the well-known **JuicyPotato** privilege escalation tool. This tool, which is commonly associated with privilege escalation techniques, was detected on **January 31, 2021, at 04:20 PM** when **JuicyPotato.exe** was executed on the host machine. The detection was flagged under **SOC Rule 107: Privilege Escalation Detected**, yet, despite this critical alert, the **Device Action** indicated that the malicious file execution was **allowed** by the system's security controls.

The **file hash** associated with the malicious executable, **808502752ca0492aca995e9b620d507b**, matched multiple known malicious signatures as confirmed by **VirusTotal**. This tool is widely exploited in advanced persistent threat (APT) campaigns to escalate privileges, allowing attackers to move laterally within a network, elevate access rights, and compromise additional systems. The tool's association with threats like **Trojan[APT] PioneerKitten** further highlights the severity of the risk.

Network and Log Analysis:

From the network traffic analysis, it was identified that the attack originated from an external source IP address, **13.107.4.50**, which was flagged by 9 out of 94 security vendors on VirusTotal as malicious. This IP, external to the organization, initiated communication with **JuicyPotato** on the internal network, specifically targeting the internal IP address **172.16.17.45**, indicative of a targeted attack attempting to exploit internal assets. This malicious traffic raises concerns about potential command and control (C2) communications or further exploitation attempts.

The logs further substantiate that **JuicyPotato.exe** was downloaded through an HTTP GET request to a suspicious URL **http://andaluciabeach.net/image/network.exe**, which itself is unrelated to any legitimate software distribution channels, adding more suspicion to the source of the attack. The fact that the system allowed the download and execution of this file without adequate filtering or blocking mechanisms is indicative of gaps in security controls, especially concerning URL filtering, endpoint protection, and application control.

Threat Intelligence:

In addition to the VirusTotal analysis of the external IP, the threat intelligence on **JuicyPotato** shows its notorious use in gaining elevated privileges on Windows systems, often exploited in unpatched or misconfigured environments. The detection across multiple security vendors in the threat intelligence report, including **AhnLab-V3**, **BitDefender**, and **Antiy-AVL**, corroborates the severity of the situation.

The deployment of **JuicyPotato** on the system is a clear indication of a deliberate attempt to exploit the organization's network, most likely through a phishing attack or another form of initial access that allowed the attackers to drop and execute this exploit. The compromised

system, **RichardPRD**, represents a critical vulnerability within the internal network, and if left uncontained, could lead to further escalation, data theft, or ransomware deployment.

Endpoint Security and Containment:

A forensic analysis of the endpoint identified five instances of **JuicyPotato.exe** being executed on the system, highlighting multiple exploitation attempts. Given the advanced nature of the tool and its use in gaining administrative privileges, the risk of further lateral movement within the network is high. Containment measures were initiated immediately upon detection, and the affected system was isolated to prevent further exploitation or communication with external entities.

Recommendations and Next Steps:

Based on these findings, the following actions are recommended:

1. **Immediate Isolation**: The affected system must remain isolated from the network to prevent any further spread of the attack.
2. **Comprehensive Forensic Analysis**: A full forensic analysis should be conducted on the affected system, including memory and disk analysis, to identify the extent of the compromise and any additional tools or backdoors that may have been installed.
3. **Patch Management**: Ensure all systems, particularly **Windows systems**, are patched to protect against known vulnerabilities that tools like JuicyPotato exploit.
4. **Network Segmentation**: Review and reinforce network segmentation to ensure that if one system is compromised, attackers cannot easily access other parts of the network.
5. **Enhanced Monitoring**: Increase network and endpoint monitoring for signs of further exploitation or C2 traffic associated with external IP addresses flagged in the threat intelligence report.
6. **Security Controls Review**: Reevaluate endpoint security, URL filtering, and application control policies to prevent the execution of unauthorized or malicious files.
7. **User Awareness and Training**: Conduct security awareness training focused on phishing attacks and suspicious file downloads to reduce the likelihood of initial exploitation through user interaction.

In conclusion, this incident highlights significant weaknesses in the organization's endpoint protection and network security. The exploitation of **JuicyPotato** indicates that advanced threat actors were targeting the organization. However, swift containment and the deployment of robust security measures can prevent further damage and help mitigate future risks.