LetsDefend

Official incident report

Event ID: 92

Rule Name: SOC145 - Ransomware 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:
92

Event Date and Time:
May, 23, 2021, 07:32 PM

Rule:
SOC145 - Ransomware Detected

Level:
Security Analyst

Source Hostname:
MarkPRD

File name:
ab.exe

File Hash:
0b486fe0503524cfe4726a4022fa6a68

File size:
775.50 Kb

Device Action:
Allowed

Network Information Details

Destination Address:
172.16.17.88 internal

Source Address:
61.177.172.87 external from virustotal.com >> the connected IPs

External / Internal Attack:

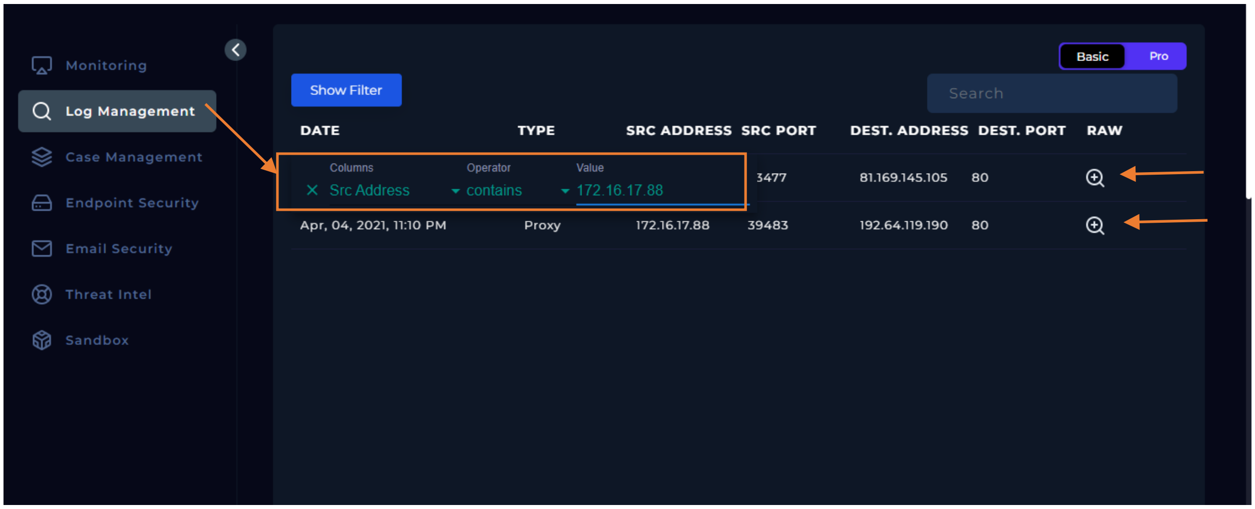
Based on the event details, the attack appears to be **external**.

Analysis:

Log Management

We'll proceed by entering the destination IP address and reviewing the results.

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



Columns: Src Address
Operator: contains
Value: 172.16.17.88

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
			3477	81.169.145.105	80	
Apr, 04, 2021, 11:10 PM	Proxy	172.16.17.88	39483	192.64.119.190	80	

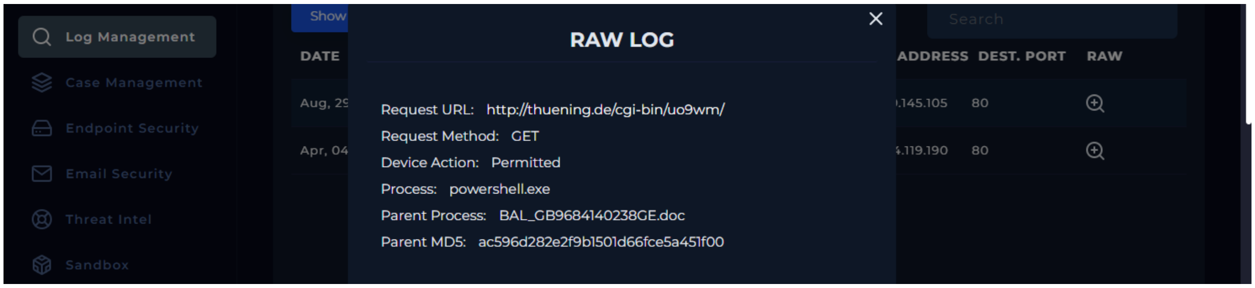
2 Logs records for the destination IP.

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

We will explain all of them step by step

Log Analysis

- **Log1:**



RAW LOG

```
Request URL:   http://thuening.de/cgi-bin/uo9wm/
Request Method:   GET
Device Action:   Permitted
Process:   powershell.exe
Parent Process:   BAL_GB9684140238GE.doc
Parent MD5:   ac596d282e2f9b1501d66fce5a451f00
```

- **Request URL:** http://thuening.de/cgi-bin/uo9wm/
  - This indicates that a request was made to a specific location on a website (http://thuening.de) with a script or program called "uo9wm" likely running on the server.
- **Request Method:** GET
  - This tells us the type of request made. "GET" is the most common method used to retrieve information from a web server.
- **Device Action:** Permitted
  - This suggests that the device's security system allowed this action to proceed.
- **Process:** powershell.exe
  - This indicates that the program responsible for making the request was the Windows PowerShell scripting tool.
- **Parent Process:** BAL_GB9684140238GE.doc
  - This is potentially the name of the document or script that triggered the PowerShell execution. However, ".doc" typically refers to Microsoft Word files, and PowerShell scripts usually have a ".ps1" extension. This might be a file name misinterpreted by the logging system, or it could be a custom script embedded within a Word document (less likely).
- **Parent Process MD5:** ac596d282e2f9b1501d66fce5a451f00
  - This is a unique identifier (hash) generated for the parent process. This value can be used to identify the specific file or script that launched PowerShell.

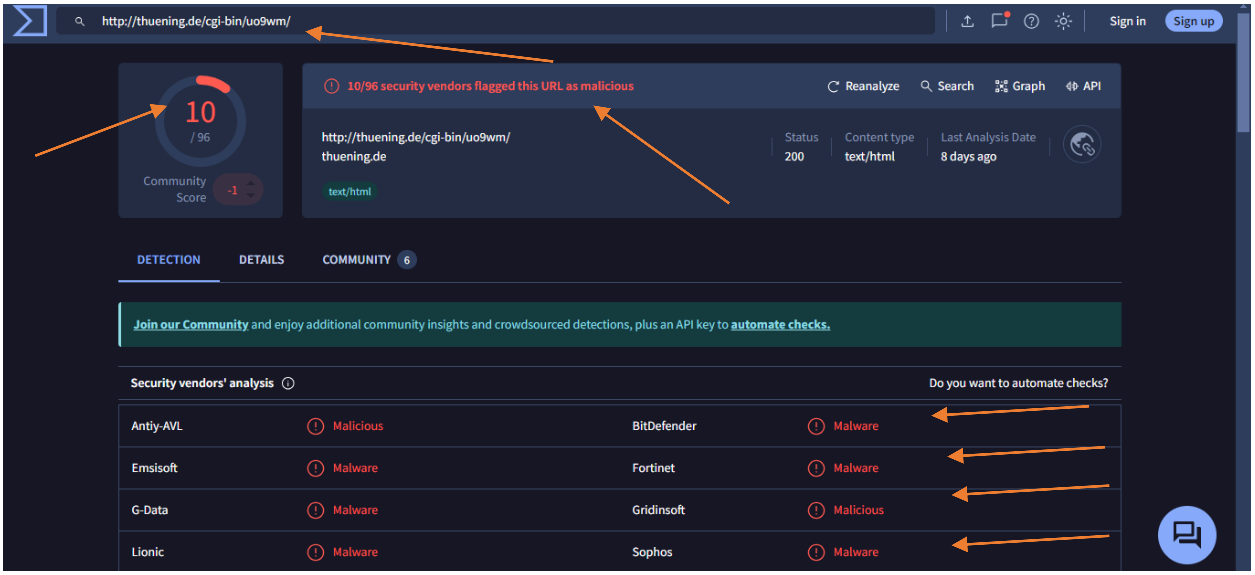
Summary: This log suggests that a script or macro within a document (possibly named BAL_GB9684140238GE.doc) executed PowerShell and made a request to a website (http://thuening.de/cgi-bin/uo9wm/).

- **Checking The Request URL: http://thuening.de/cgi-bin/uo9wm/ on Virus Total**

  Out of 96 security vendors analyzed, 10 flagged the URL as malicious.

  Vendors reporting malicious activity: Antiy-AVL, BitDefender, Emsisoft, Fortinet, G-Data, Gridinsoft, Lionic, Sophos, VIPRE, Webroot

Check the attached photo



10/96 security vendors flagged this URL as malicious

http://thuening.de/cgi-bin/uo9wm/
thuening.de
text/html

Status 200
Content type text/html
Last Analysis Date 8 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	BitDefender	Malware
Emsisoft	Malware	Fortinet	Malware
G-Data	Malware	Gridinsoft	Malicious
Lionic	Malware	Sophos	Malware

[The reference link]()

- ## Checking The Parent MD5: ac596d282e2f9b1501d66fce5a451f00 on Virus Total

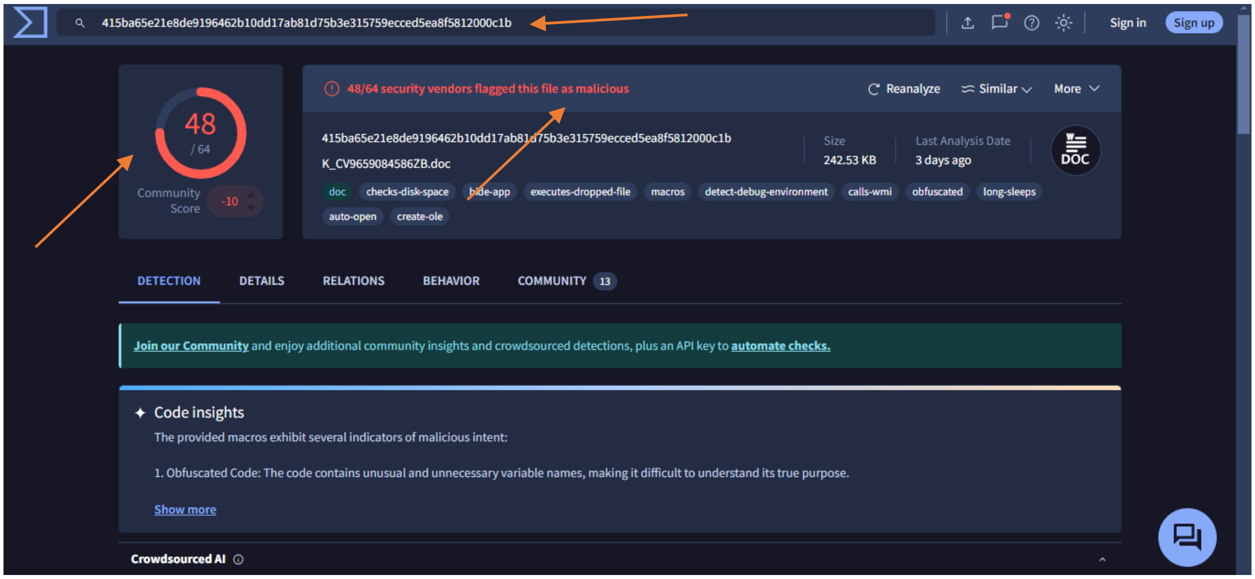
Professional Analysis of File Scan Results

Key Finding: Nearly three-quarters (48 out of 64) of analyzed security vendors flagged the file as malicious.

Details:

- **Malicious Classifications:**
  - Several vendors identified the file as a downloader associated with the Emotet malware (e.g., AhnLab-V3, BitDefender, ESET-NOD32).
  - Other classifications included Trojan, Trojan-Downloader, and Script (indicating suspicious behavior).
- **Suspicious Classifications:**
  - Some vendors flagged the file as suspicious, requiring further investigation (e.g., Acronis, AliCloud).

Check the attached photo



415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b

48 / 64

Community Score -10

48/64 security vendors flagged this file as malicious

415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b

K_CV9659084586ZB.doc

Size 242.53 KB

Last Analysis Date 3 days ago

doc · checks-disk-space · hide-app · executes-dropped-file · macros · detect-debug-environment · calls-wmi · obfuscated · long-sleeps · auto-open · create-ole

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

✦ Code insights

The provided macros exhibit several indicators of malicious intent:

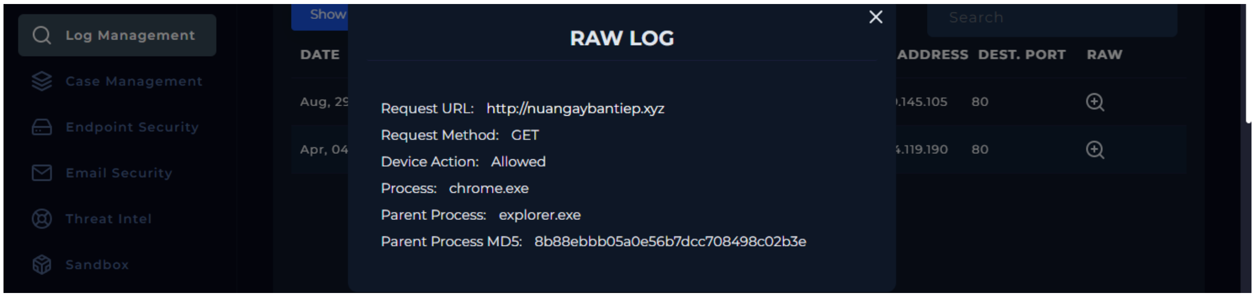
1. Obfuscated Code: The code contains unusual and unnecessary variable names, making it difficult to understand its true purpose.

Show more

Crowdsourced AI

[The reference link]

- **Log2:**

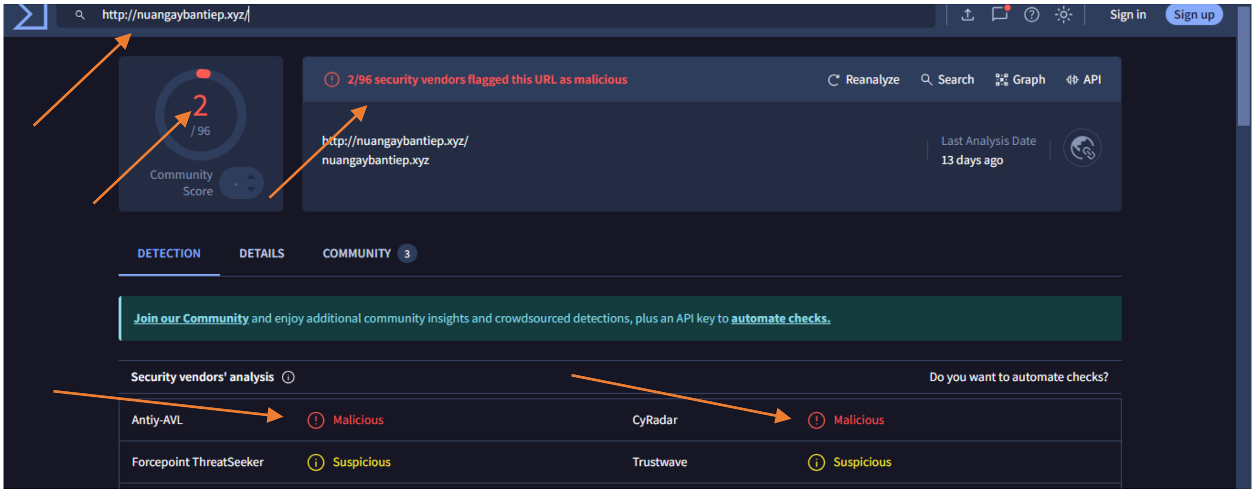


```
Request URL:   http://nuangaybantiep.xyz
Request Method:   GET
Device Action:   Allowed
Process:   chrome.exe
Parent Process:   explorer.exe
Parent Process MD5:   8b88ebbb05a0e56b7dcc708498c02b3e
```

- **Request URL:** http://nuangaybantiep.xyz
  - This indicates that a request was made to a website called "http://nuangaybantiep.xyz".
- **Request Method:** GET
  - Similar to Log 1, this is a "GET" request to retrieve information.
- **Device Action:** Allowed
  - This device's security system also allowed this action.
- **Process:** chrome.exe
  - This indicates that the program making the request was the Google Chrome web browser.
- **Parent Process:** explorer.exe
  - This is the default Windows file explorer process. Chrome is likely launched through explorer.exe when a user clicks a link in a folder or on the desktop.
- **Parent Process MD5:** 8b88ebbb05a0e56b7dcc708498c02b3e
  - This is the unique identifier (hash) for explorer.exe.

Summary: This log simply shows that the Chrome browser made a request to the website "http://nuangaybantiep.xyz" likely by clicking a link.

- **Checking The Request URL: http://nuangaybantiep.xyz on Virus Total**



http://nuangaybantiep.xyz/

2/96 security vendors flagged this URL as malicious

http://nuangaybantiep.xyz/
nuangaybantiep.xyz

Last Analysis Date
13 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Antiy-AVL	Malicious	CyRadar	Malicious
Forcepoint ThreatSeeker	Suspicious	Trustwave	Suspicious

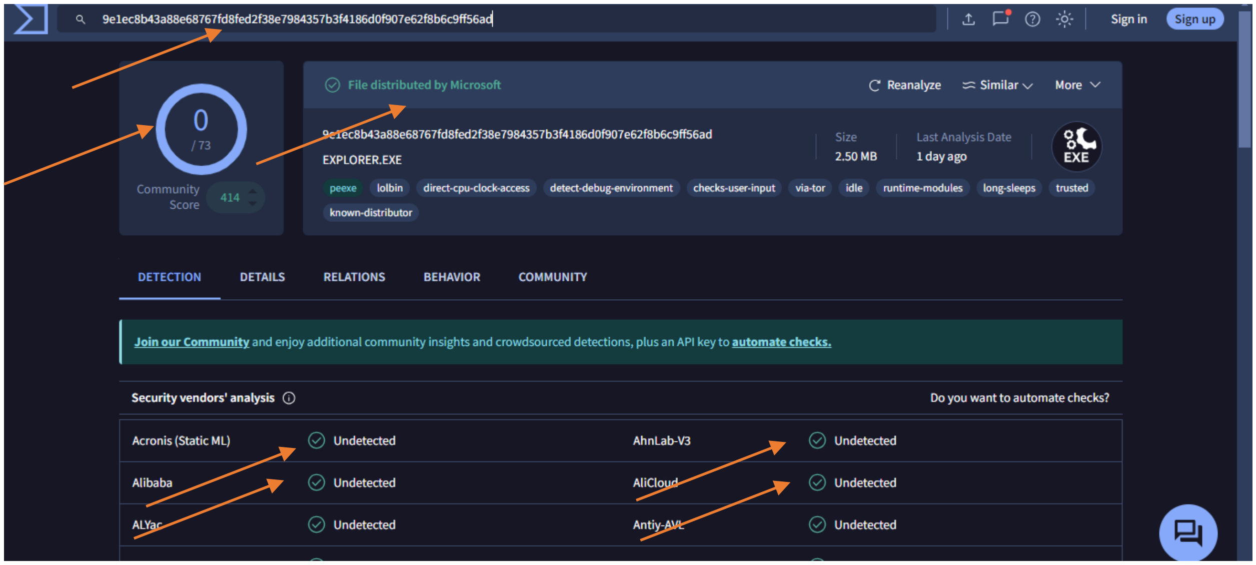
Out of 96 security vendors analyzed, only 2 flagged the URL as malicious.

Vendors reporting malicious activity: Antiy-AVL, CyRadar

Additional findings: Forcepoint ThreatSeeker and Trustwave classified the URL as suspicious.

- **About Parent Process MD5:** 8b88ebbb05a0e56b7dcc708498c02b3e

It`s clear



9e1ec8b43a88e68767fd8fed2f38e7984357b3f4186d0f907e62f8b6c9ff56ad

File distributed by Microsoft

9e1ec8b43a88e68767fd8fed2f38e7984357b3f4186d0f907e62f8b6c9ff56ad
EXPLORER.EXE

Size
2.50 MB

Last Analysis Date
1 day ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected

Summary of Log Analysis

Suspicious Activity Detected (Log 1):

- A script or macro within a document (potentially named BAL_GB9684140238GE.doc) executed PowerShell.
- PowerShell made a request to a website flagged as malicious by 10 out of 96 security vendors (http://thuening.de/cgi-bin/uo9wm/).

Recommendation:

- Investigate the document (BAL_GB9684140238GE.doc) and consider quarantining it if the source is unknown.
- Scan the system for malware using a reputable antivirus program.

Normal Activity (Log 2):

- The Chrome browser made a request to the website "http://nuangaybantiep.xyz," likely by clicking a link.
- Only 2 out of 96 security vendors flagged this URL as malicious, with additional vendors classifying it as suspicious.

Recommendation:

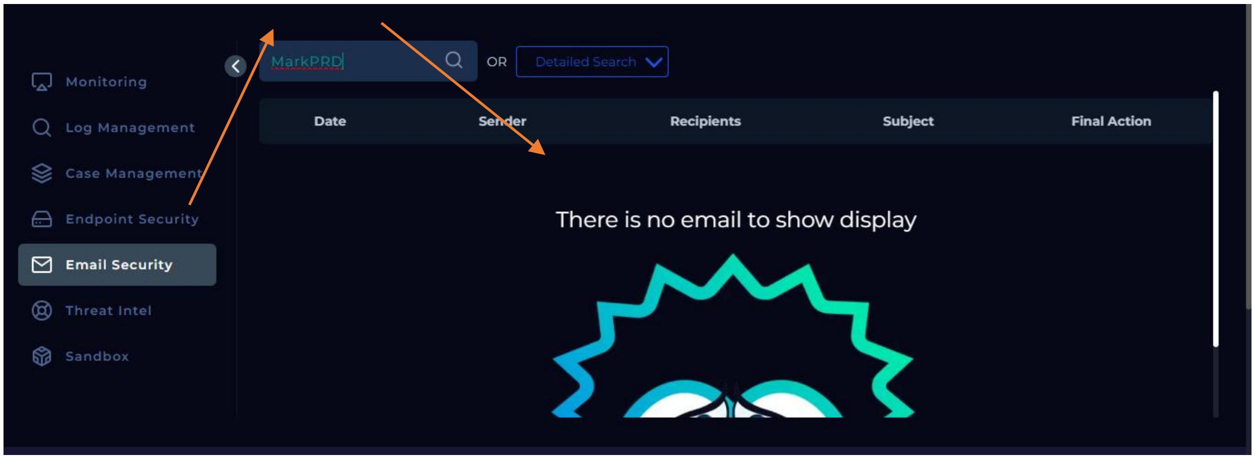
- Exercise caution when visiting unfamiliar websites (like ".xyz" domains).

Additional Notes:

- The attached photos were not included in this summary. However, you can reference them for detailed vendor classifications if needed.

Overall, the log analysis suggests potential malware activity in Log 1. Further investigation and security measures are recommended.

Email Security:



MarkPRD

Date	Sender	Recipients	Subject	Final Action

There is no email to show display

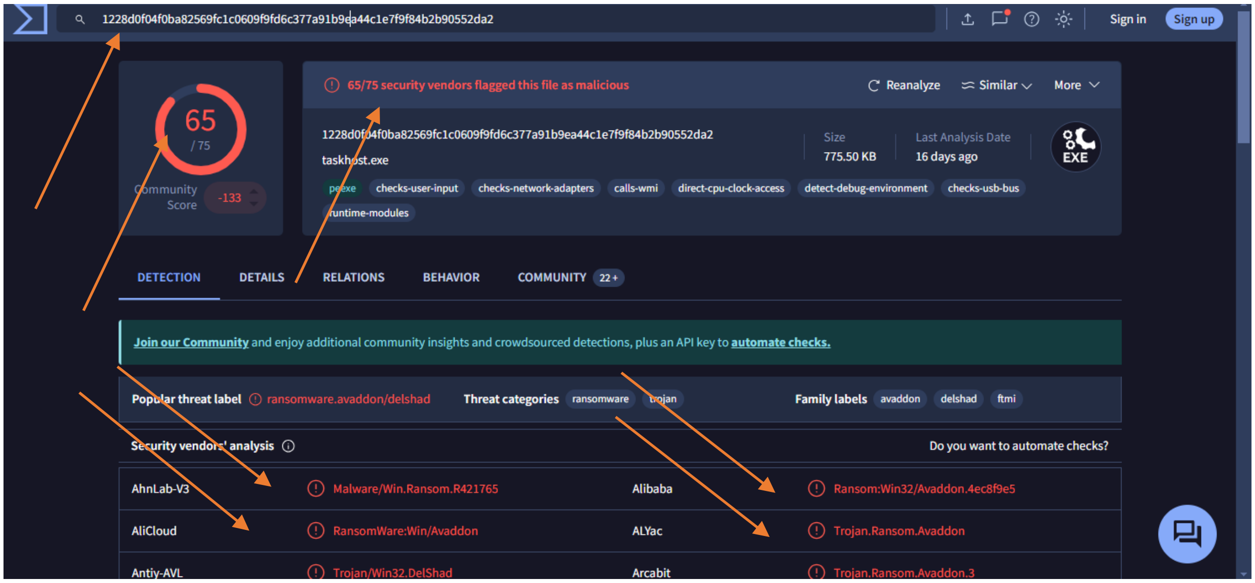
Despite entering the source host name in the email security section, no emails have been sent, indicating that the attack was not executed

Detection:

Threat Intelligence Results

File Hash Analysis on VirusTotal

Check the attached photo



1228d0f04f0ba82569fc1c0609f9fd6c377a91b9ea44c1e7f9f84b2b90552da2

65 / 75

Community Score -133

65/75 security vendors flagged this file as malicious

1228d0f04f0ba82569fc1c0609f9fd6c377a91b9ea44c1e7f9f84b2b90552da2

taskhost.exe

peexe checks-user-input checks-network-adapters calls-wmi direct-cpu-clock-access detect-debug-environment checks-usb-bus runtime-modules

Size 775.50 KB

Last Analysis Date 16 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ransomware.avaddon/delshad

Threat categories ransomware trojan

Family labels avaddon delshad ftmi

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win.Ransom.R421765	Alibaba	Ransom:Win32/Avaddon.4ec8f9e5
AliCloud	RansomWare:Win/Avaddon	ALYac	Trojan.Ransom.Avaddon
Antiy-AVL	Trojan/Win32.DelShad	Arcabit	Trojan.Ransom.Avaddon.3

VirusTotal Analysis:

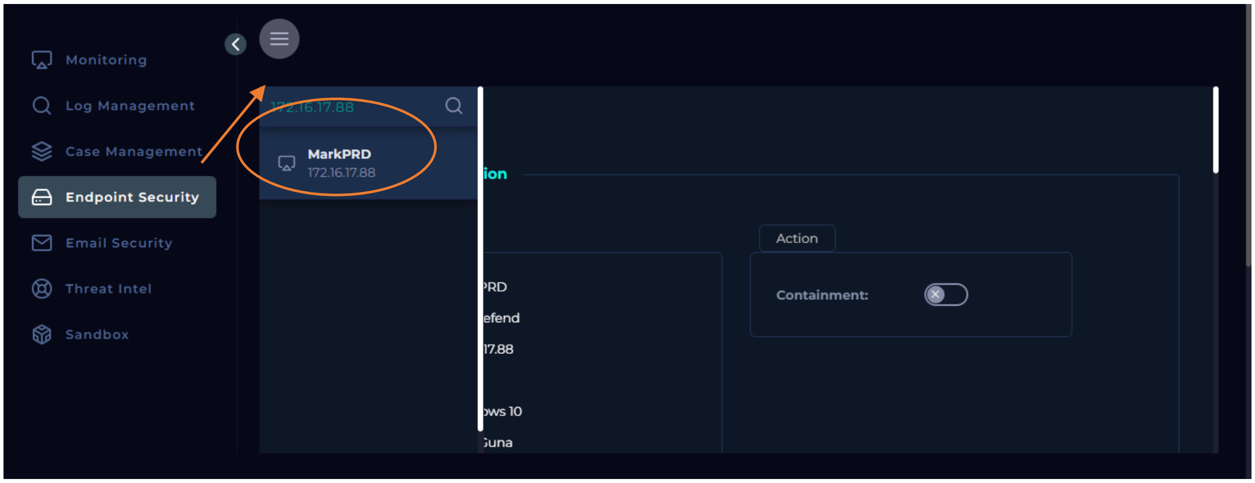
- **Classification:** Malicious (flagged by 65 out of 75 security vendors)
- **Primary Threat:** Ransomware (identified by several vendors as Avaddon or a variant)
- **Additional Detections:** Trojan, Generic Malware

Details:

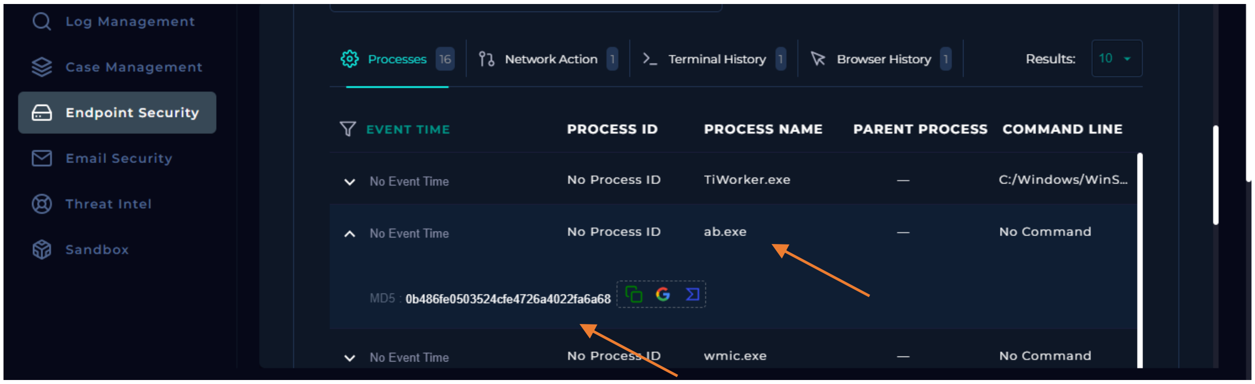
- Multiple vendors identified the file as a variant of the Avaddon ransomware, known for encrypting user data and demanding a ransom for decryption.
- Other vendors detected generic malicious behavior or Trojans, which can also be harmful.

Reference link for hash file

Endpoint Security:

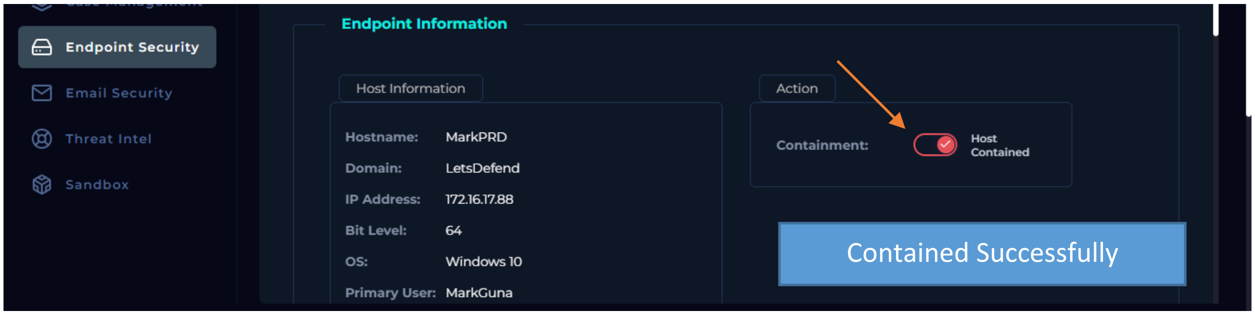


We must carefully review the following section, paying particular attention to the processes involved.



EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
No Event Time	No Process ID	TiWorker.exe	—	C:/Windows/WinS...
No Event Time	No Process ID	ab.exe	—	No Command
MD5 : 0b486fe0503524cfe4726a4022fa6a68				
No Event Time	No Process ID	wmic.exe	—	No Command

The executable file 'ab.exe' was executed on the system, which has subsequently been compromised. The file's hash matches the one in the alert details. To prevent further damage, the device must be isolated immediately.



Endpoint Information

Host Information

Hostname: MarkPRD
Domain: LetsDefend
IP Address: 172.16.17.88
Bit Level: 64
OS: Windows 10
Primary User: MarkGuna

Action

Containment: Host Contained

Conclusion:

Alert Name: SOC145 - Ransomware Detected
Event Date and Time: May 23, 2021, 07:32 PM

The investigation into Event ID 92, flagged under Rule SOC145 as a ransomware detection, reveals a critical security incident requiring immediate action.

Summary of Findings:

1. **Malicious File Identification:**
   - The file `ab.exe`, identified with a hash matching known ransomware signatures, has been classified as a variant of Avaddon ransomware by numerous security vendors. This confirms its role in the attack.
2. **Suspicious Activity:**
   - **Log 1**: PowerShell execution from a document (potentially `BAL_GB9684140238GE.doc`) made a request to a URL (`http://thuening.de/cgi-bin/uo9wm/`) flagged as malicious by 10 out of 96 security vendors. This indicates a high likelihood of ransomware deployment.
   - **Log 2**: Activity involving the Chrome browser and URL (`http://nuangaybantiep.xyz`) was flagged by only 2 vendors as malicious, suggesting that the primary concern is the ransomware-related activity observed in Log 1.
3. **VirusTotal Analysis:**
   - The file `ab.exe` was flagged as malicious by 65 out of 75 security vendors, confirming its association with ransomware. This supports the initial threat assessment and emphasizes the urgency of response.
4. **Email Security Check:**
   - No related email activity was detected, indicating that the attack vector was likely endpoint compromise.

Recommended Actions:

1. **Immediate Containment:**
   - Isolate the affected endpoint to prevent further damage and spread of the ransomware. This is crucial to stopping ongoing malicious activity.
2. **Detailed Investigation:**
   - Examine the document `BAL_GB9684140238GE.doc` and its associated processes. Quarantine the document and conduct a thorough scan for additional malicious artifacts.
3. **System-Wide Scanning:**
   - Execute a full system scan with up-to-date antivirus tools across all potentially affected systems to ensure complete malware removal.
4. **Enhance Security Measures:**

    - Strengthen security protocols, with a focus on improving email defenses, macro security, and endpoint protection to mitigate similar threats in the future.

Final Note:

The ransomware detected in this alert presents a serious threat. Immediate isolation of the compromised system, combined with comprehensive investigation and enhanced security measures, is essential to minimize impact and prevent future incidents. Swift action on these recommendations will be vital in securing our network.