Author: Jack Fitzgerald

Official Incident Report

Date: Jan, 31, 2021, 04:59 PM

Event ID: 44

Rule Name: SOC113 - Suspicious hh.exe Usage

Table of Contents

Alert Details

Severity: Low

Type: Malware

Source Address: 172.16.17.47

Source Hostname: BillPRD

File Name: WinRAR.chm

File Hash: 07694464c25bac4ecdb365e928ffe1ff

File Size: 306 KB

Device Action: Allowed

Based on the information provided in the alert, it appears that a suspicious **executable** has been run on host **172.16.17.47**. The alert is triggered by rule SOC113 - Suspicious hh.exe Usage.

Upon reviewing the alert, it is observed that a file named **WinRAR.chm** with the file hash of **07694464c25bac4ecdb365e928ffe1ff** was executed on host **172.16.17.47**.

The device action is marked **allowed**, indicating that the execution was successfully performed on the host machine.

Overall, it appears that the **hh.exe** usage may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

By investigating the executable **hh.exe**, as well as the file **WinRAR.chm**, along with the MD5 hash of **07694464c25bac4ecdb365e928ffe1ff**, we can determine whether the executable along with the file is malicious or benign.

The Microsoft HTML Help executable (hh.exe), is a legitimate Windows file that displays compiled help files (.chm). It's used for standard help functions, but attackers can abuse it to execute malicious code hidden inside .chm files, often for defense evasion.

https://www.virustotal.com/gui/file/d7e601bce098797f3f76f6cdd6fb49a011b4fb86ea060196c7cf2ec21bb9b5ae

No security vendors flagged this file as malicious

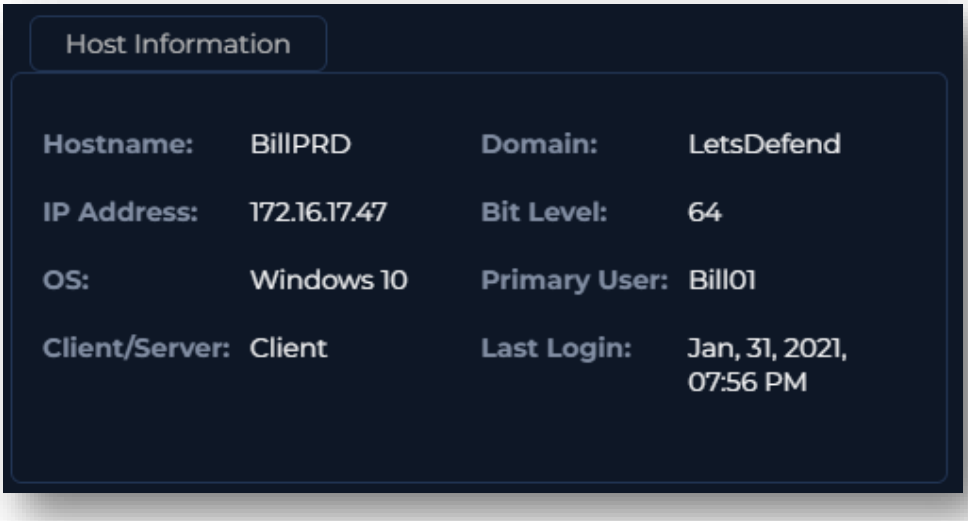
Based on the information provided by **VirusTotal**, it appears that **WinRAR.chm** is legit and has been flagged as benign by all security vendors. **WinRAR** is a trialware file archiver and compression utility for Microsoft Windows.

Now, we can identify which device this alert came from by searching for **172.16.17.47** in Endpoint Security.

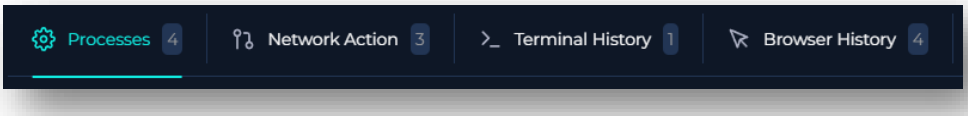
Analysis

The next step is to investigate Endpoint Security, which can provide valuable insights into the commands executed by the user and help us understand the scope and intent of the suspicious activity. In the previous section, we found the device with the IP of **172.16.17.49**, which belongs to Primary User **Bill01**, with hostname **BillPRD**.

We determined some host information from here, such as Hostname, IP Address, OS, Client/Server, Domain, Bit Level, Primary User, and Last Login.

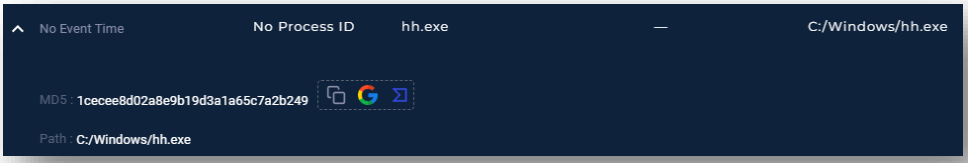


We can also investigate Processes, Network Action, Terminal History, and Browser History.



In Terminal History, we found the command line that was executed **hh.exe c:/program files/winrar/winrar.chm**.

Furthermore, we found the process involved with the alert; however, no event time was identified.



After investigating the Endpoint Security, no suspicious activity was performed, but just to be safe, we investigated the MD5 hash **1cecee8d02a8e9b19d3a1a65c7a2b249** of the process too.

https://www.virustotal.com/gui/file/8ab2f9a4ca87575f03f554aeed6c5e0d7692fa9b5d420008a1521f7f7bd2d0a5

File distributed by Microsoft

Our analysis was correct, **hh.exe** is a **trusted** and **signed** file from known distributor **Microsoft**.

Containment

Based on the information gathered during the investigation, it is highly unlikely that the system has been compromised. There is no need to isolate the system from the network.

Summary

The incident involves a non-compromised system named **BillPRD** with an IP address of **172.16.17.47**. The alert was triggered by the detection of a suspicious **executable** being used, based on the rule SOC113 - Suspicious hh.exe Usage.

Upon further analysis, it was discovered that **hh.exe** is Microsoft HTML Help executable, which is a legitimate Windows file that displays compiled help files (.chm) was not being used maliciously, as identified in Endpoint Security.

The analysis of **BillPRD's** Terminal History and Processes revealed use of **hh.exe** regarding **WinRAR.chm**, both being identified as legitimate and benign, matching the alert creation date, further substantiating the alert's authenticity.

Based on the findings of the incident, no immediate action needs to be taken to isolate the compromised system, and the event was identified as a **False Positive**.

Lessons Learned

- Legitimate processes can appear suspicious, as attackers sometimes abuse them to execute scripts or load malicious files
- Not every uncommon process usage is malicious, context matters
- Detection logic may be too broad, capture many false positives

Remediation Actions

- Refine the detection rule, or create an allow list for known good usage
- Update documentation and SOPs, reducing future investigation times
- Even though this case was benign, monitor future cases as hh.exe could still be abused by an attacker in a different instance

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
n/a	n/a

Artifacts

Value	Comment	Type
07694464c25bac4ecdb365e928ffe1ff	WinRAR.chm	MD5 Hash
1cecee8d02a8e9b19d3a1a65c7a2b249	hh.exe	MD5 Hash

LetsDefend Playbook

n/a