Case Study #3 Writeup

Table Of Contents

Situation

You are currently working as a cybersecurity consultant for a large security firm that does security services for Fortune 500 and Global 500 companies. These services include penetration testing/red teaming services, digital forensics and incident response services. Recently, the technology giant Hooli decided to contract your company to do a compromise assessment on a few of their work stations.

For background, Hooli develops hardware and software - their search engine “Hooli Search” is the most used search engine in the world. They also create mobile phones, and have vastly popular cloud computing services that also power their Hooli Chat servers and Hooli Exchange Mail servers. To continue their innovation and being the lead company in technology, they plan on acquiring smaller start-up companies that rival them.

Hooli say they apply best security practices on their work environment - everyone must physically be at their computer to access it, no remote work allowed. In addition, employees are supposed to only use their workstations for work related things only. Before they acquire another startup and integrate their workstations onto the corporate network environment, they want to do a compromise assessment on their own machines to ensure good cyber hygiene (a compromise assessment is designed to find weaknesses in the company’s network/practice, unknown security breaches, and any past or ongoing attackers on the network). You have been assigned to this engagement and have been tasked to look through a specific workstation. For this, you were given the ShellBags artifacts among other things - can you find anything worth bringing up to the client?

The scope of this engagement with Hooli is any activity happening between 04/05/2021 through 04/10/2021.

The Compromise Assessment

Pre-Assessment Observations

This engagement is a compromise assessment: we currently do not know if there are any attackers on this workstation. Along with looking for any past or current unauthorized access that would compromise the confidentiality of this system, we should look for any bad practices that could also help improve the client's security posture.

Initial Findings

Looking at the "Events" tab we could see events in chronological order which would help looking at activities that happened within the scope of the engagement.

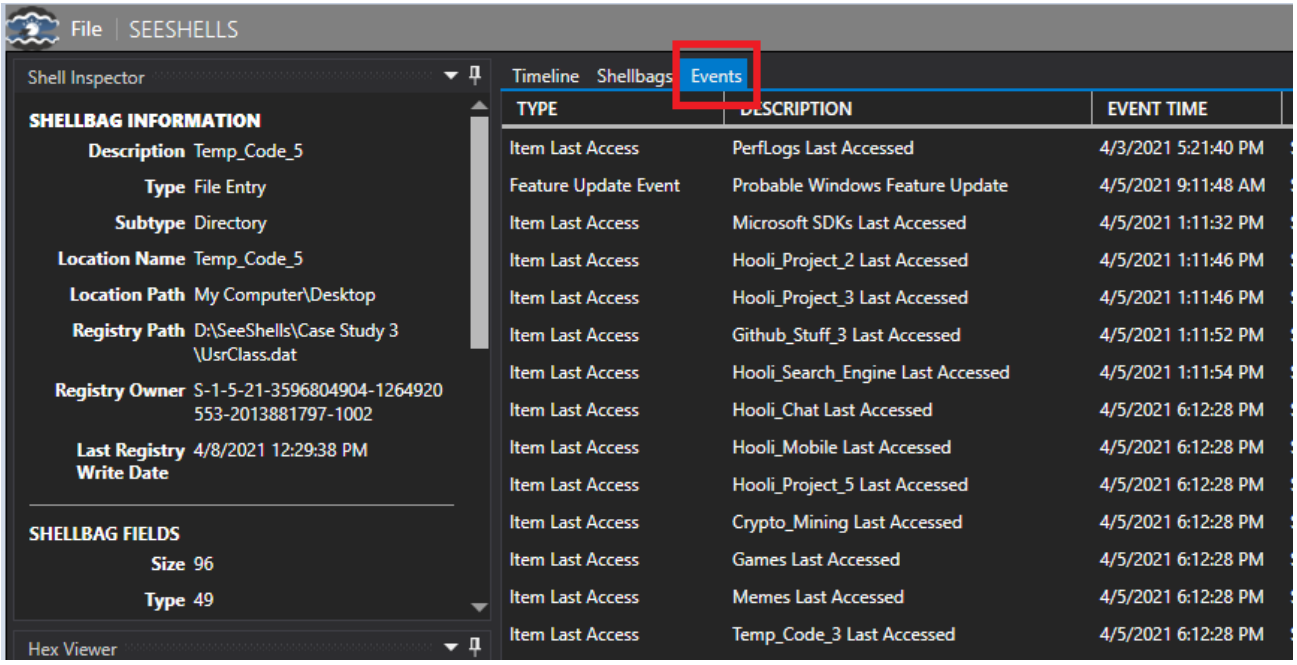

Figure 1. Showing the "Events" tab

Looking at events that occurred on the 04/05/2021, we three files that potentially go against the company's workstation policy, "Crypto_Mining", "Games", and "Torrented_Files" though so far there's nothing we know of that's inside those folders.

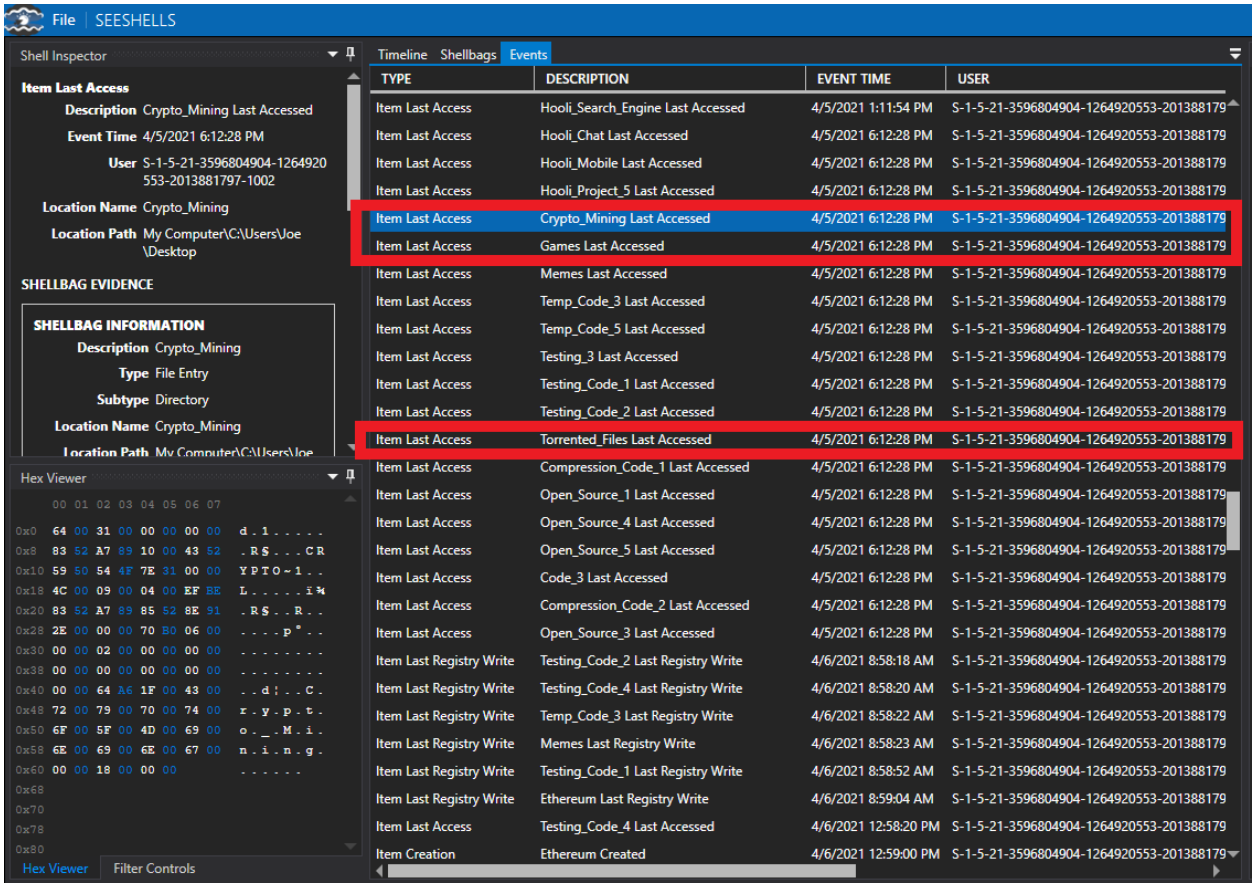

Figure 2. Showing proof of potentially policy breaking activity

The following day (04/06/2021), we see the user creating a couple directories under the "Crypto_Mining" directory, these two folders are named "Ethereum" and "Bitcoin" - it can be assumed that this employee is using his work computer to farm these crypto currencies. In addition, the employee also downloads games on his work computer.

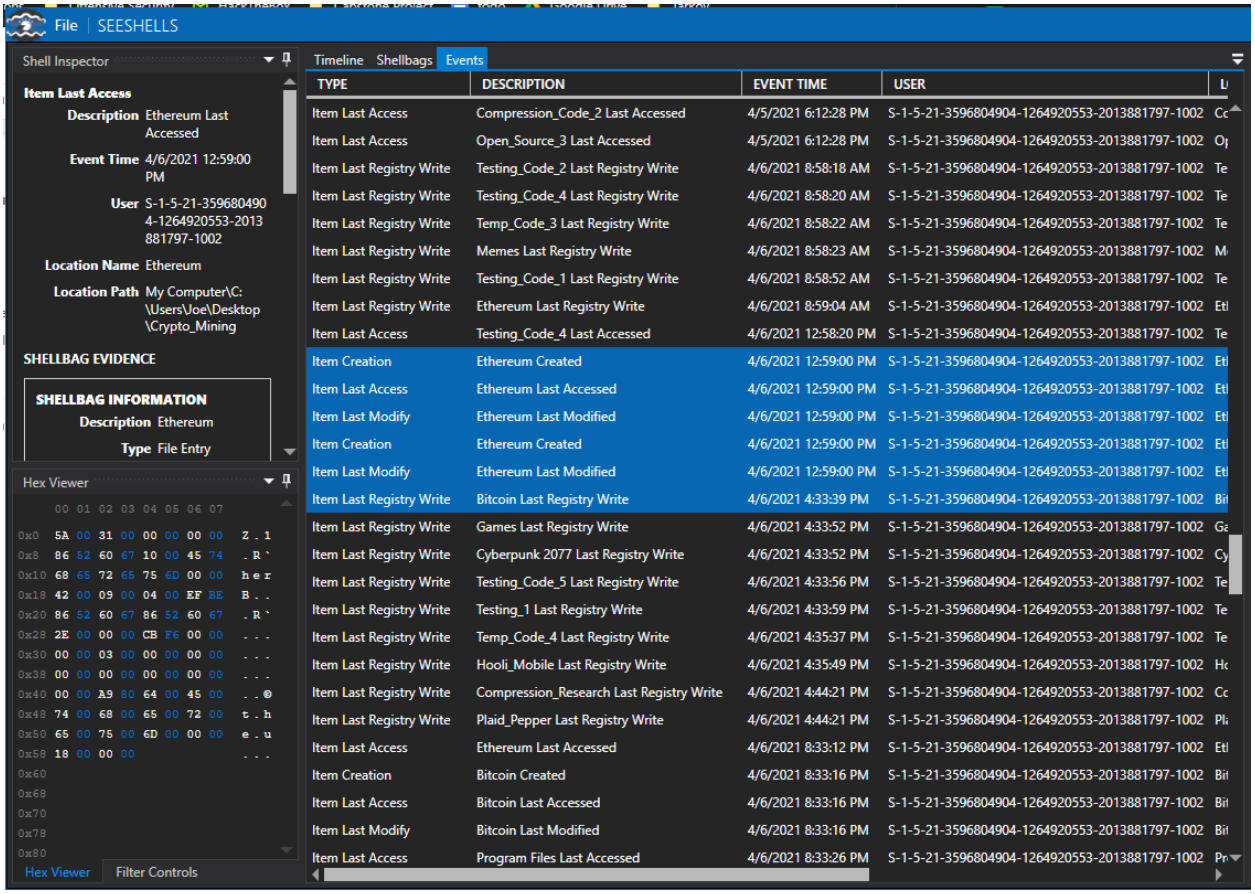

Figure 3. Showing definitive proof of policy breaking activities

For security best practices, workstations that are owned by the company should only be used for work-related purposes. This includes only having applications and processes running that are approved by the company's System Administrators. Having unwanted and unnecessary applications running runs the risk that the computer could have its integrity, and availability compromised. For instance, if any unapproved application causes the modification of important folders and files, that is a loss of integrity of the filesystem. Furthermore, if any unapproved application causes an accidental deletion or overwrite of important folders and files, that will result in a loss of availability. Since these applications and processes that were found are not part of the company's policy, it should be reported to the client.

On 04/07/2021 there is a “Program Installation Event” with the description that says “TeamViewer Installed.” According to the TeamViewer website[1], “The TeamViewer remote connectivity cloud platform enables secure remote access to any device, across platforms, from anywhere, anytime.” Having any type of remote connection is against the company’s policy so it is worth noting. TeamViewer does have legitimate uses, but it also could be used in malicious ways and it is currently not known how TeamViewer has been used.

Timeline Shellbags Events

TYPE	DESCRIPTION	EVENT TIME
Item Last Access	Program Files (x86) Last Accessed	4/7/2021 2:16:02 PM
Item Last Registry Write	Open_Source_1 Last Registry Write	4/7/2021 5:16:35 PM
Item Last Registry Write	Open_Source_3 Last Registry Write	4/7/2021 5:16:39 PM
Item Last Registry Write	Open_Source_5 Last Registry Write	4/7/2021 5:16:40 PM
Item Last Registry Write	Code_5 Last Registry Write	4/7/2021 5:16:42 PM
Item Last Registry Write	Compression_Code_1 Last Registry Write	4/7/2021 5:19:31 PM
Item Last Registry Write	Compression_Code_2 Last Registry Write	4/7/2021 5:19:32 PM
Item Last Registry Write	TeamViewer Last Registry Write	4/7/2021 7:14:24 PM
Item Last Access	Code_5 Last Accessed	4/7/2021 9:16:36 PM
Program Installation Event	TeamViewer Installed	4/7/2021 11:11:02 PM
Item Last Access	Microsoft Last Accessed	4/7/2021 11:11:14 PM
Item Last Access	TeamViewer Last Accessed	4/7/2021 11:14:00 PM
Item Last Modify	TeamViewer Last Modified	4/7/2021 11:14:00 PM

Figure 4. Evidence of TeamViewer being installed on 04/07/2021

[1] https://www.teamviewer.com/en-us/

First Signs of Threat Actor Activity

The following day we see a couple things. The first being another directory under “Crypto_Mining” was created that was named “Doge”. However during the nighttime we see some signs of malicious activities. A folder named “CobaltStrike” was created and accessed. Later, another folder named “BloodHound” was created.

Both of these tools are red teaming tools that need to be brought up to the client. According to CobaltStrike’s website[2], “Cobalt Strike gives you a post-exploitation agent and covert channels to emulate a quiet long-term embedded actor in your customer’s network.” BloodHound is also a post-exploitation tool used to graph out relationships within the Active Directory environment, according to BloodHound’s github page[3], “BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify.”

[2] https://www.cobaltstrike.com/
[3] https://github.com/BloodHoundAD/BloodHound

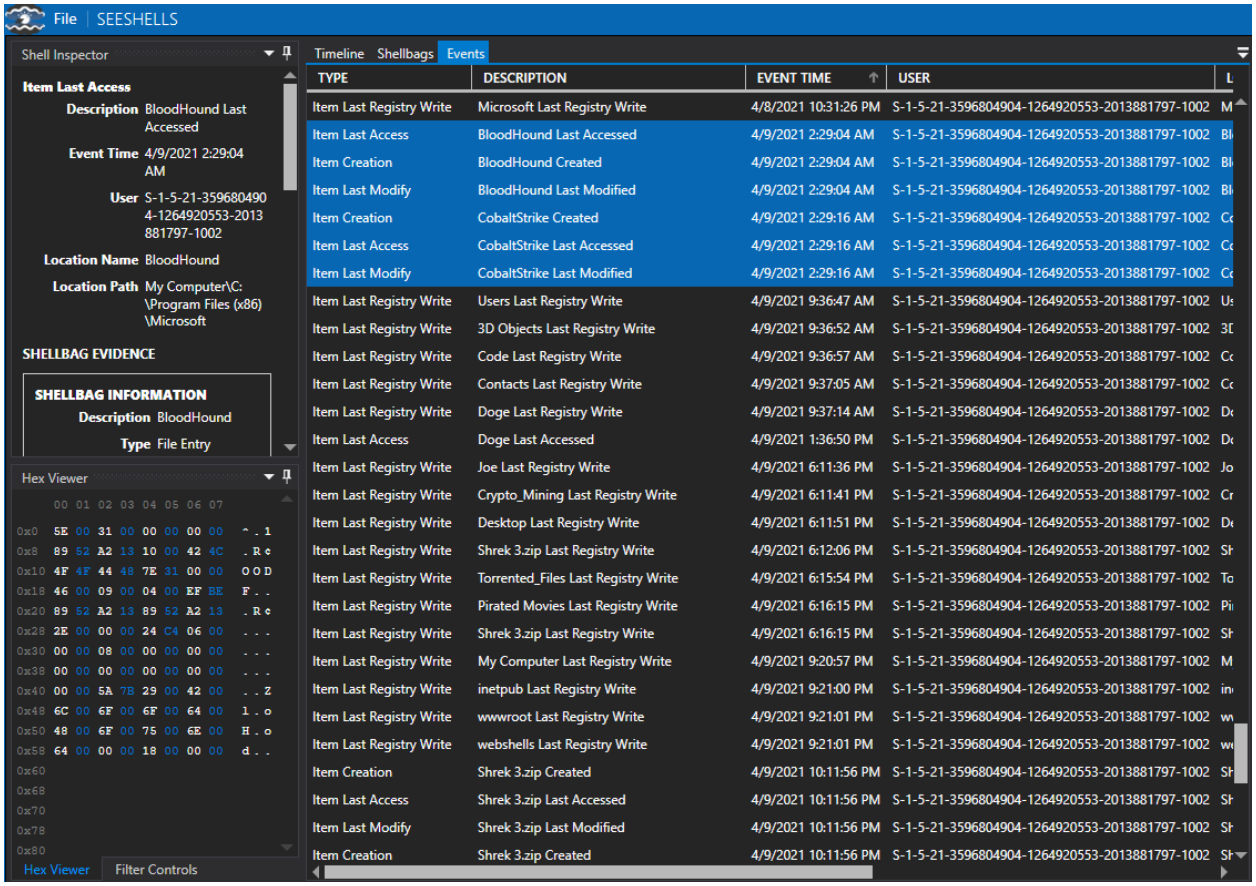

Figure 5. Finding evidence of BloodHound and CobaltStrike

Further Signs of Threat Actor Activity

On 04/10/2021, under the Windows IIS (the Windows web application) root folder, there was a folder named “webshells” that was created. Webshells are malicious web-based shells that enable remote access to a web server by allowing the execution of commands. This is sometimes used by malicious actors to achieve persistence on the network.

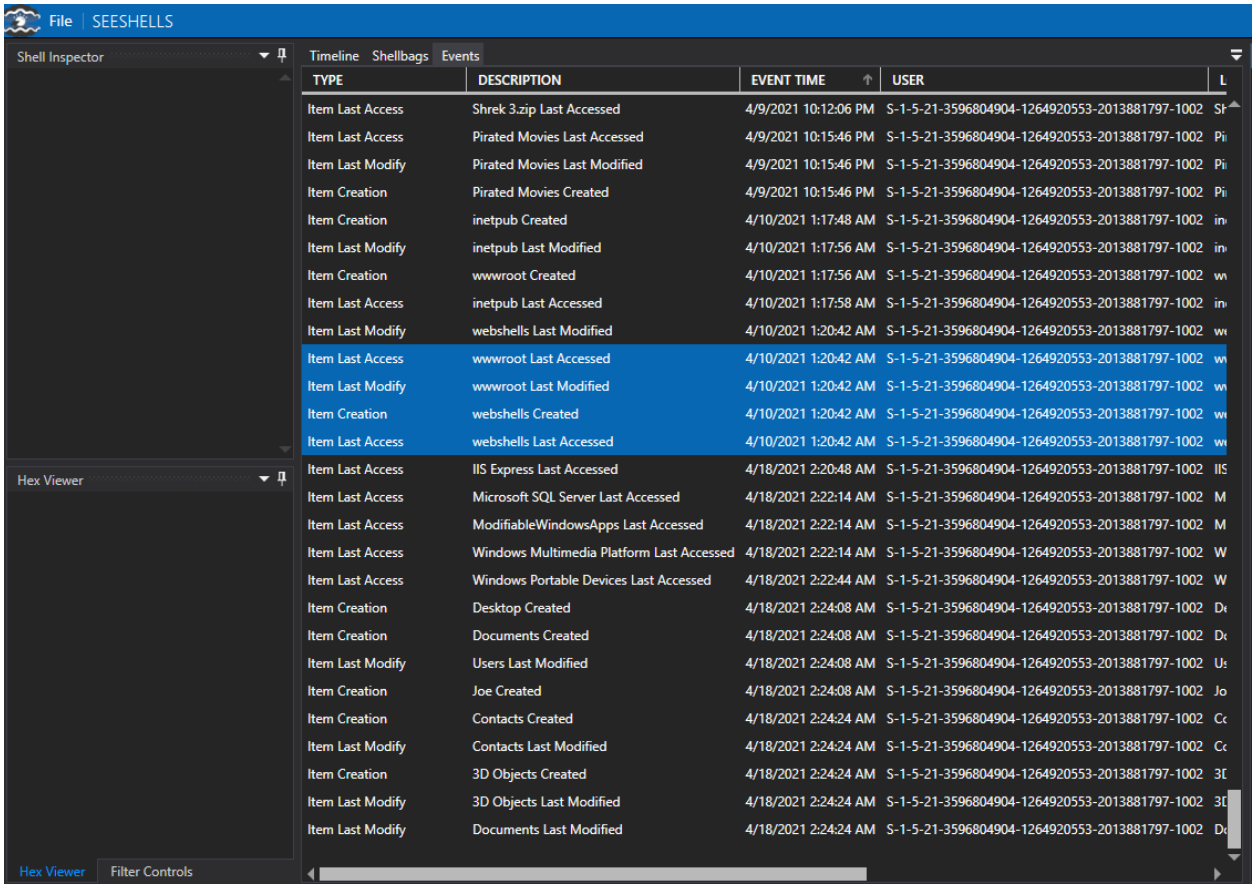

Figure 6. Finding the “webshells” directory

Conclusion

As for the security posture of this particular workstation, there are a few things that are out of company policy. Namely the cryptocurrency mining, the video games, and the torrented files. Furthermore, there are signs that there is current unauthorized access going on starting from when TeamViewer was installed. There are post exploitation tools that were being used on this system - namely CobaltStrike and BloodHound. The system also needs to be investigated for the use of webshells within the Hooli's web servers. The following is a list of directories that are out of policy or are suspicious:

- Crypto_Mining
    - Bitcoin
    - Ethereum
    - Dogecoin
- Video_Games
    - Cyberpunk 2077
    - League of Legends
- Torrented_Files
    - Shrek 3.zip
    - Witcher 3
- TeamViewer (installation)
- CobaltStrike
- BloodHound
- webshells