

# Case Study #3 Writeup

## Table Of Contents

<b>Situation</b>	<b>2</b>
<b>The Compromise Assessment</b>	<b>4</b>
Pre-Assessment Observations	4
Initial Findings	4
First Signs of Threat Actor Activity	8
Further Signs of Threat Actor Activity	9
<b>Conclusion</b>	<b>11</b>

## 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.

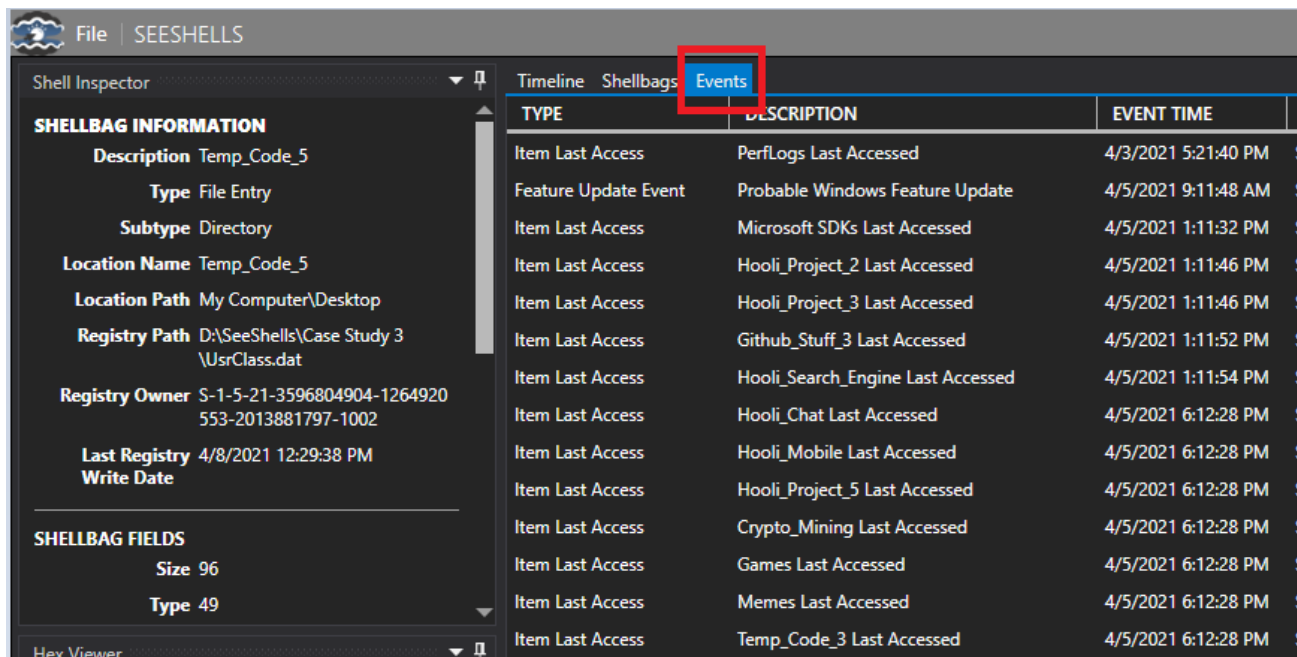


Figure 1. Showing the “Events” tab

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.

The screenshot displays the SEESHELLS Shell Inspector interface. The 'Events' tab is active, showing a list of file system events. The 'Item Last Access' section on the left highlights the 'Crypto\_Mining' directory, showing its description, type (File Entry), subtype (Directory), location name, and path. The 'SHELLBAG EVIDENCE' section shows the 'SHELLBAG INFORMATION' for the 'Crypto\_Mining' directory, including its description, type, subtype, location name, and path. The 'Hex Viewer' section at the bottom left shows a hex dump of the file system data. The main event log table on the right lists various file system events, including 'Item Last Access' for 'Crypto\_Mining', 'Games', and 'Torrented\_Files', all occurring on 4/5/2021 at 6:12:28 PM. The events are filtered by the user 'S-1-5-21-3596804904-1264920553-201388179'.

TYPE	DESCRIPTION	EVENT TIME	USER
Item Last Access	Hooli_Search_Engine Last Accessed	4/5/2021 1:11:54 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Hooli_Chat Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Hooli_Mobile Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Hooli_Project_5 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Crypto_Mining Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Games Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Memes Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Temp_Code_3 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Temp_Code_5 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Testing_3 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Testing_Code_1 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Testing_Code_2 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Torrented_Files Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Compression_Code_1 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Open_Source_1 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Open_Source_4 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Open_Source_5 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Code_3 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Compression_Code_2 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Open_Source_3 Last Accessed	4/5/2021 6:12:28 PM	S-1-5-21-3596804904-1264920553-201388179
Item Last Registry Write	Testing_Code_2 Last Registry Write	4/6/2021 8:58:18 AM	S-1-5-21-3596804904-1264920553-201388179
Item Last Registry Write	Testing_Code_4 Last Registry Write	4/6/2021 8:58:20 AM	S-1-5-21-3596804904-1264920553-201388179
Item Last Registry Write	Temp_Code_3 Last Registry Write	4/6/2021 8:58:22 AM	S-1-5-21-3596804904-1264920553-201388179
Item Last Registry Write	Memes Last Registry Write	4/6/2021 8:58:23 AM	S-1-5-21-3596804904-1264920553-201388179
Item Last Registry Write	Testing_Code_1 Last Registry Write	4/6/2021 8:58:52 AM	S-1-5-21-3596804904-1264920553-201388179
Item Last Registry Write	Ethereum Last Registry Write	4/6/2021 8:59:04 AM	S-1-5-21-3596804904-1264920553-201388179
Item Last Access	Testing_Code_4 Last Accessed	4/6/2021 12:58:20 PM	S-1-5-21-3596804904-1264920553-201388179
Item Creation	Ethereum Created	4/6/2021 12:59:00 PM	S-1-5-21-3596804904-1264920553-201388179

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.

File | SEESH-HELLS

Shell Inspector

Item Last Access

Description

Ethereum Last Accessed

Event Time

4/6/2021 12:59:00 PM

User

S-1-5-21-359680490-4-1264920553-2013881797-1002

Location Name

Ethereum

Location Path

My Computer\C:\Users\Joe\Desktop\Crypto\_Mining

SHELLBAG EVIDENCE

SHELLBAG INFORMATION

Description

Ethereum

Type

File Entry

Hex Viewer

00 01 02 03 04 05 06 07

0x00 5A 00 31 00 00 00 00 Z . 1

0x08 86 52 60 67 10 00 45 74 . R `

0x10 68 65 72 65 75 6D 00 00 h e x

0x18 42 00 09 00 04 00 EF BE B .

0x20 86 52 60 67 86 52 60 67 . R `

0x28 2E 00 00 00 CB F6 00 00 . . .

0x30 00 00 03 00 00 00 00 . . .

0x38 00 00 00 00 00 00 00 . . .

0x40 00 00 39 80 64 00 45 00 . @

0x48 74 00 68 00 65 00 72 00 t . h

0x50 65 00 75 00 6D 00 00 00 e . u

0x58 18 00 00 00 . . .

0x60

0x68

0x70

0x78

0x80

Timeline Shellbags Events

TYPE

DESCRIPTION

EVENT TIME

USER

U

Item Last Access

Compression\_Code\_2 Last Accessed

4/5/2021 6:12:28 PM

S-1-5-21-359680490-1264920553-2013881797-1002

C

Item Last Access

Open\_Source\_3 Last Accessed

4/5/2021 6:12:28 PM

S-1-5-21-359680490-1264920553-2013881797-1002

O

Item Last Registry Write

Testing\_Code\_2 Last Registry Write

4/6/2021 8:58:18 AM

S-1-5-21-359680490-1264920553-2013881797-1002

T

Item Last Registry Write

Testing\_Code\_4 Last Registry Write

4/6/2021 8:58:20 AM

S-1-5-21-359680490-1264920553-2013881797-1002

T

Item Last Registry Write

Temp\_Code\_3 Last Registry Write

4/6/2021 8:58:22 AM

S-1-5-21-359680490-1264920553-2013881797-1002

T

Item Last Registry Write

Memes Last Registry Write

4/6/2021 8:58:23 AM

S-1-5-21-359680490-1264920553-2013881797-1002

M

Item Last Registry Write

Testing\_Code\_1 Last Registry Write

4/6/2021 8:58:52 AM

S-1-5-21-359680490-1264920553-2013881797-1002

T

Item Last Registry Write

Ethereum Last Registry Write

4/6/2021 8:59:04 AM

S-1-5-21-359680490-1264920553-2013881797-1002

E

Item Last Access

Testing\_Code\_4 Last Accessed

4/6/2021 12:58:20 PM

S-1-5-21-359680490-1264920553-2013881797-1002

T

Item Creation

Ethereum Created

4/6/2021 12:59:00 PM

S-1-5-21-359680490-1264920553-2013881797-1002

E

Item Last Access

Ethereum Last Accessed

4/6/2021 12:59:00 PM

S-1-5-21-359680490-1264920553-2013881797-1002

E

Item Last Modify

Ethereum Last Modified

4/6/2021 12:59:00 PM

S-1-5-21-359680490-1264920553-2013881797-1002

E

Item Creation

Ethereum Created

4/6/2021 12:59:00 PM

S-1-5-21-359680490-1264920553-2013881797-1002

E

Item Last Modify

Ethereum Last Modified

4/6/2021 12:59:00 PM

S-1-5-21-359680490-1264920553-2013881797-1002

E

Item Last Registry Write

Bitcoin Last Registry Write

4/6/2021 4:33:39 PM

S-1-5-21-359680490-1264920553-2013881797-1002

B

Item Last Registry Write

Games Last Registry Write

4/6/2021 4:33:52 PM

S-1-5-21-359680490-1264920553-2013881797-1002

G

Item Last Registry Write

Cyberpunk 2077 Last Registry Write

4/6/2021 4:33:52 PM

S-1-5-21-359680490-1264920553-2013881797-1002

C

Item Last Registry Write

Testing\_Code\_5 Last Registry Write

4/6/2021 4:33:56 PM

S-1-5-21-359680490-1264920553-2013881797-1002

T

Item Last Registry Write

Testing\_1 Last Registry Write

4/6/2021 4:33:59 PM

S-1-5-21-359680490-1264920553-2013881797-1002

T

Item Last Registry Write

Temp\_Code\_4 Last Registry Write

4/6/2021 4:35:37 PM

S-1-5-21-359680490-1264920553-2013881797-1002

T

Item Last Registry Write

Hooli\_Mobile Last Registry Write

4/6/2021 4:35:49 PM

S-1-5-21-359680490-1264920553-2013881797-1002

H

Item Last Registry Write

Compression\_Research Last Registry Write

4/6/2021 4:44:21 PM

S-1-5-21-359680490-1264920553-2013881797-1002

C

Item Last Registry Write

Plaid\_Pepper Last Registry Write

4/6/2021 4:44:21 PM

S-1-5-21-359680490-1264920553-2013881797-1002

P

Item Last Access

Ethereum Last Accessed

4/6/2021 8:33:12 PM

S-1-5-21-359680490-1264920553-2013881797-1002

E

Item Creation

Bitcoin Created

4/6/2021 8:33:16 PM

S-1-5-21-359680490-1264920553-2013881797-1002

B

Item Last Access

Bitcoin Last Accessed

4/6/2021 8:33:16 PM

S-1-5-21-359680490-1264920553-2013881797-1002

B

Item Last Modify

Bitcoin Last Modified

4/6/2021 8:33:16 PM

S-1-5-21-359680490-1264920553-2013881797-1002

B

Item Last Access

Program Files Last Accessed

4/6/2021 8:33:26 PM

S-1-5-21-359680490-1264920553-2013881797-1002

P

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<sup>1</sup>, “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*

<sup>1</sup> <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<sup>2</sup>, “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<sup>3</sup>, “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.”

---

<sup>2</sup> <https://www.cobaltstrike.com/>

<sup>3</sup> <https://github.com/BloodHoundAD/BloodHound>



The screenshot displays the Windows Security Event Viewer interface. The left-hand pane shows the 'Item Last Access' details for the event 'BloodHound Last Accessed'. The event occurred on 4/9/2021 at 2:29:04 AM, performed by user S-1-5-21-3596804904-1264920553-2013881797-1002, and the location was 'BloodHound'. The location path is listed as 'My Computer\C:\Program Files (x86)\Microsoft'. The right-hand pane shows a list of events, including 'Item Last Registry Write' for 'Microsoft Last Registry Write' and 'Item Last Access' for 'BloodHound Last Accessed'. The bottom pane shows a hex viewer with the text '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.

File SEESHELLS		Timeline Shellbags Events			
Shell Inspector		TYPE	DESCRIPTION	EVENT TIME	USER
		Item Last Access	Shrek 3.zip Last Accessed	4/9/2021 10:12:06 PM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	Pirated Movies Last Accessed	4/9/2021 10:15:46 PM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Modify	Pirated Movies Last Modified	4/9/2021 10:15:46 PM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	Pirated Movies Created	4/9/2021 10:15:46 PM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	inetpub Created	4/10/2021 1:17:48 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Modify	inetpub Last Modified	4/10/2021 1:17:56 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	wwwroot Created	4/10/2021 1:17:56 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	inetpub Last Accessed	4/10/2021 1:17:58 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Modify	webshells Last Modified	4/10/2021 1:20:42 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	wwwroot Last Accessed	4/10/2021 1:20:42 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Modify	wwwroot Last Modified	4/10/2021 1:20:42 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	webshells Created	4/10/2021 1:20:42 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	webshells Last Accessed	4/10/2021 1:20:42 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	IIS Express Last Accessed	4/18/2021 2:20:48 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	Microsoft SQL Server Last Accessed	4/18/2021 2:22:14 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	ModifiableWindowsApps Last Accessed	4/18/2021 2:22:14 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	Windows Multimedia Platform Last Accessed	4/18/2021 2:22:14 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Access	Windows Portable Devices Last Accessed	4/18/2021 2:22:44 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	Desktop Created	4/18/2021 2:24:08 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	Documents Created	4/18/2021 2:24:08 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Modify	Users Last Modified	4/18/2021 2:24:08 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	Joe Created	4/18/2021 2:24:08 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	Contacts Created	4/18/2021 2:24:24 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Modify	Contacts Last Modified	4/18/2021 2:24:24 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Creation	3D Objects Created	4/18/2021 2:24:24 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Modify	3D Objects Last Modified	4/18/2021 2:24:24 AM	S-1-5-21-3596804904-1264920553-2013881797-1002
		Item Last Modify	Documents Last Modified	4/18/2021 2:24:24 AM	S-1-5-21-3596804904-1264920553-2013881797-1002

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