SeeShells

Case Study #3 Writeup

Background Information:

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 workstations.

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 leading 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.

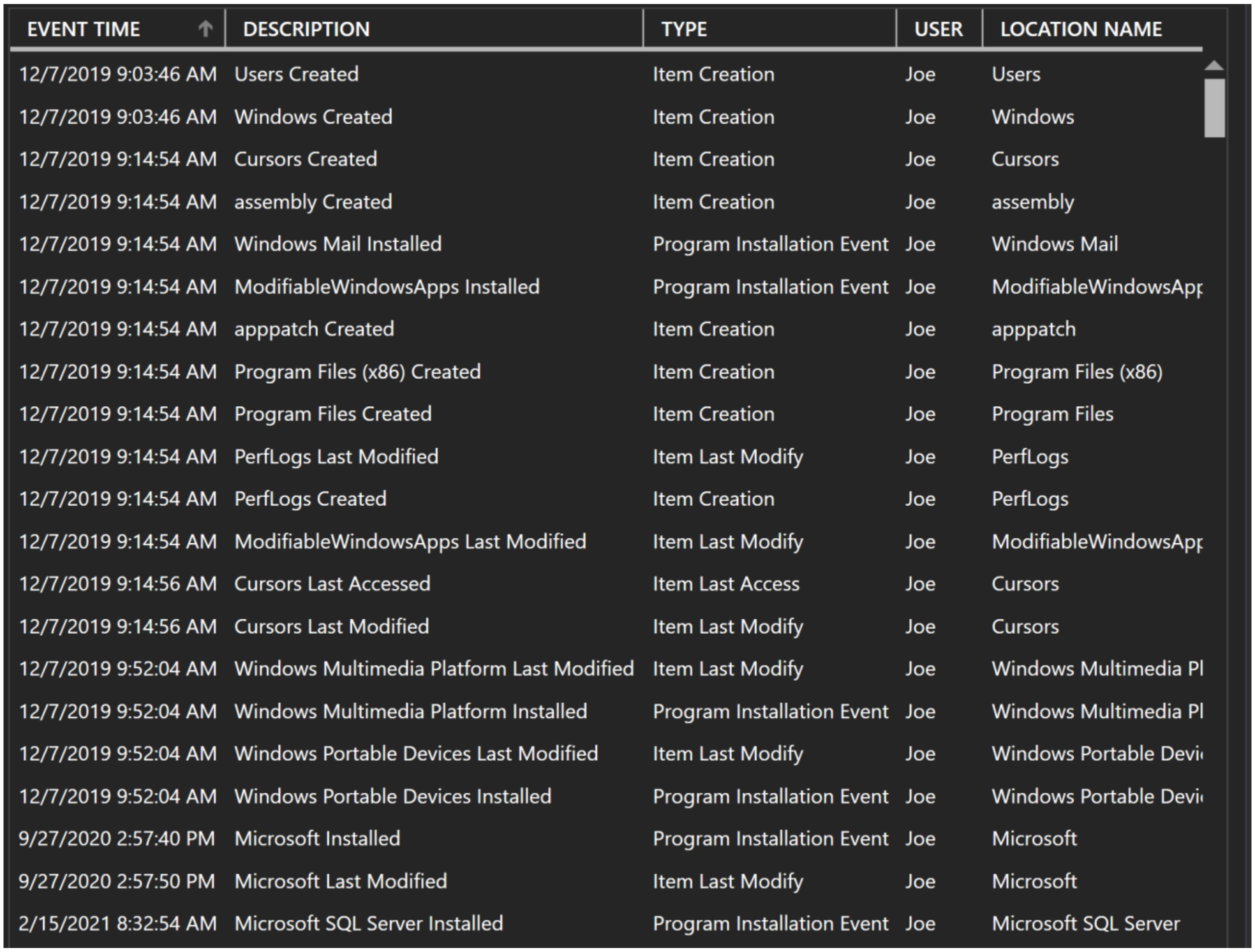
The Compromise Assessment

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

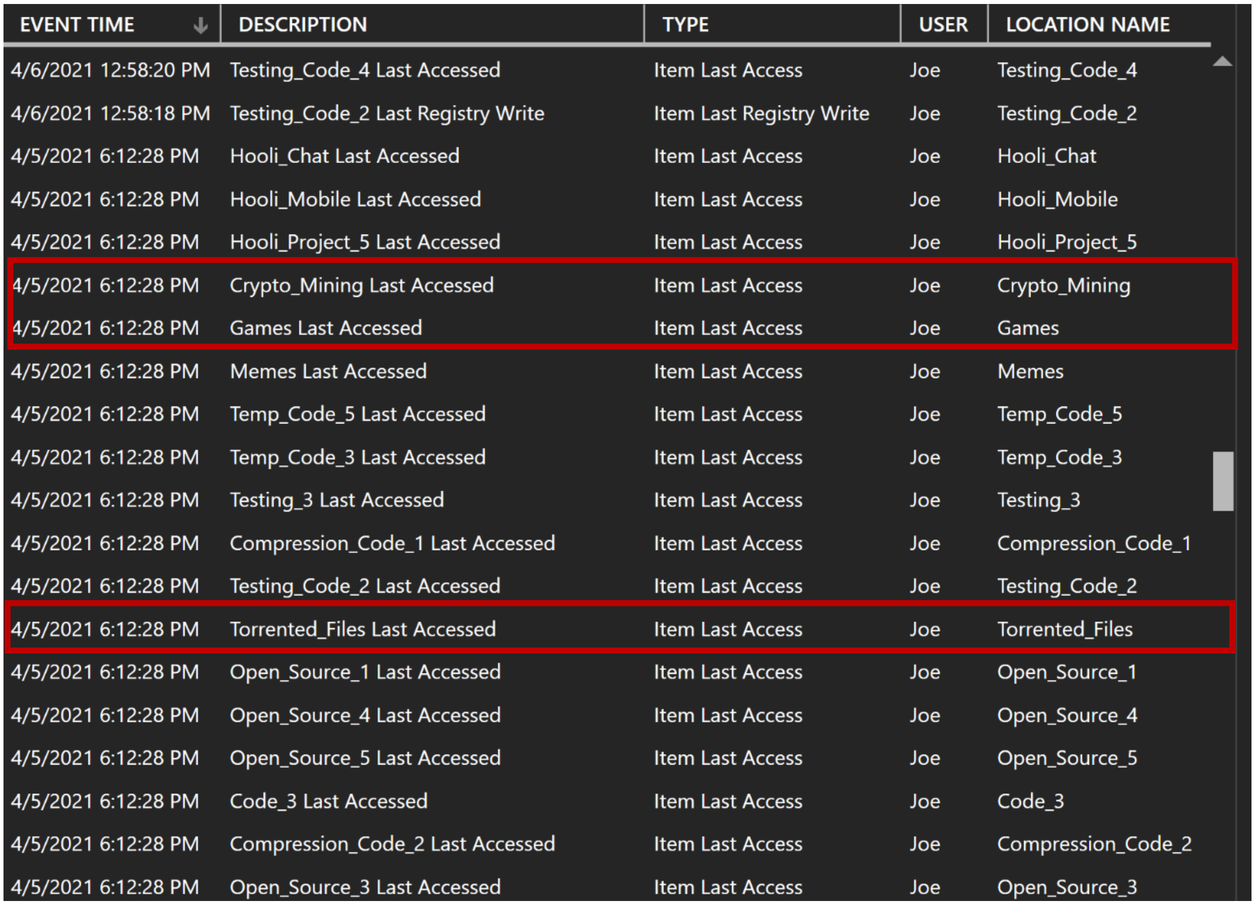
Looking at the events table we can see events in chronological order by clicking on the 'Event Time' header. We can view events in ascending or descending order by clicking the header multiple times.



EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME
12/7/2019 9:03:46 AM	Users Created	Item Creation	Joe	Users
12/7/2019 9:03:46 AM	Windows Created	Item Creation	Joe	Windows
12/7/2019 9:14:54 AM	Cursors Created	Item Creation	Joe	Cursors
12/7/2019 9:14:54 AM	assembly Created	Item Creation	Joe	assembly
12/7/2019 9:14:54 AM	Windows Mail Installed	Program Installation Event	Joe	Windows Mail
12/7/2019 9:14:54 AM	ModifiableWindowsApps Installed	Program Installation Event	Joe	ModifiableWindowsApp
12/7/2019 9:14:54 AM	apppatch Created	Item Creation	Joe	apppatch
12/7/2019 9:14:54 AM	Program Files (x86) Created	Item Creation	Joe	Program Files (x86)
12/7/2019 9:14:54 AM	Program Files Created	Item Creation	Joe	Program Files
12/7/2019 9:14:54 AM	PerfLogs Last Modified	Item Last Modify	Joe	PerfLogs
12/7/2019 9:14:54 AM	PerfLogs Created	Item Creation	Joe	PerfLogs
12/7/2019 9:14:54 AM	ModifiableWindowsApps Last Modified	Item Last Modify	Joe	ModifiableWindowsApp
12/7/2019 9:14:56 AM	Cursors Last Accessed	Item Last Access	Joe	Cursors
12/7/2019 9:14:56 AM	Cursors Last Modified	Item Last Modify	Joe	Cursors
12/7/2019 9:52:04 AM	Windows Multimedia Platform Last Modified	Item Last Modify	Joe	Windows Multimedia Pl
12/7/2019 9:52:04 AM	Windows Multimedia Platform Installed	Program Installation Event	Joe	Windows Multimedia Pl
12/7/2019 9:52:04 AM	Windows Portable Devices Last Modified	Item Last Modify	Joe	Windows Portable Devi
12/7/2019 9:52:04 AM	Windows Portable Devices Installed	Program Installation Event	Joe	Windows Portable Devi
9/27/2020 2:57:40 PM	Microsoft Installed	Program Installation Event	Joe	Microsoft
9/27/2020 2:57:50 PM	Microsoft Last Modified	Item Last Modify	Joe	Microsoft
2/15/2021 8:32:54 AM	Microsoft SQL Server Installed	Program Installation Event	Joe	Microsoft SQL Server

Figure 1. Showing the "Events" tab

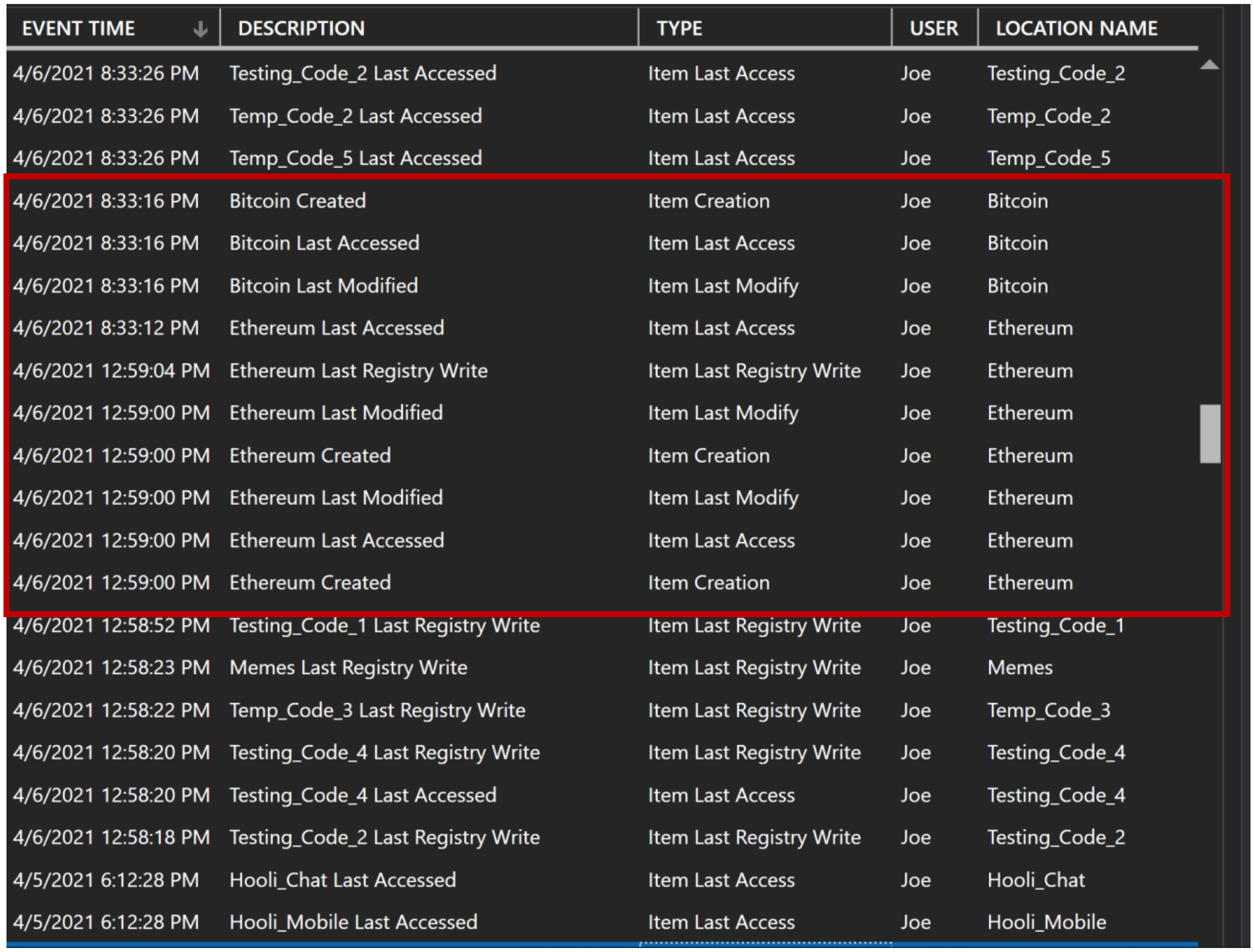
Looking at events that occurred on the 04/05/2021, we three files that potentially go against the company's workstation policy, "Crypto_Mining", "Games", and "Torrented_Files" though so far there's nothing we know of that's inside those folders.



EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME
4/6/2021 12:58:20 PM	Testing_Code_4 Last Accessed	Item Last Access	Joe	Testing_Code_4
4/6/2021 12:58:18 PM	Testing_Code_2 Last Registry Write	Item Last Registry Write	Joe	Testing_Code_2
4/5/2021 6:12:28 PM	Hooli_Chat Last Accessed	Item Last Access	Joe	Hooli_Chat
4/5/2021 6:12:28 PM	Hooli_Mobile Last Accessed	Item Last Access	Joe	Hooli_Mobile
4/5/2021 6:12:28 PM	Hooli_Project_5 Last Accessed	Item Last Access	Joe	Hooli_Project_5
4/5/2021 6:12:28 PM	Crypto_Mining Last Accessed	Item Last Access	Joe	Crypto_Mining
4/5/2021 6:12:28 PM	Games Last Accessed	Item Last Access	Joe	Games
4/5/2021 6:12:28 PM	Memes Last Accessed	Item Last Access	Joe	Memes
4/5/2021 6:12:28 PM	Temp_Code_5 Last Accessed	Item Last Access	Joe	Temp_Code_5
4/5/2021 6:12:28 PM	Temp_Code_3 Last Accessed	Item Last Access	Joe	Temp_Code_3
4/5/2021 6:12:28 PM	Testing_3 Last Accessed	Item Last Access	Joe	Testing_3
4/5/2021 6:12:28 PM	Compression_Code_1 Last Accessed	Item Last Access	Joe	Compression_Code_1
4/5/2021 6:12:28 PM	Testing_Code_2 Last Accessed	Item Last Access	Joe	Testing_Code_2
4/5/2021 6:12:28 PM	Torrented_Files Last Accessed	Item Last Access	Joe	Torrented_Files
4/5/2021 6:12:28 PM	Open_Source_1 Last Accessed	Item Last Access	Joe	Open_Source_1
4/5/2021 6:12:28 PM	Open_Source_4 Last Accessed	Item Last Access	Joe	Open_Source_4
4/5/2021 6:12:28 PM	Open_Source_5 Last Accessed	Item Last Access	Joe	Open_Source_5
4/5/2021 6:12:28 PM	Code_3 Last Accessed	Item Last Access	Joe	Code_3
4/5/2021 6:12:28 PM	Compression_Code_2 Last Accessed	Item Last Access	Joe	Compression_Code_2
4/5/2021 6:12:28 PM	Open_Source_3 Last Accessed	Item Last Access	Joe	Open_Source_3

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.



EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME
4/6/2021 8:33:26 PM	Testing_Code_2 Last Accessed	Item Last Access	Joe	Testing_Code_2
4/6/2021 8:33:26 PM	Temp_Code_2 Last Accessed	Item Last Access	Joe	Temp_Code_2
4/6/2021 8:33:26 PM	Temp_Code_5 Last Accessed	Item Last Access	Joe	Temp_Code_5
4/6/2021 8:33:16 PM	Bitcoin Created	Item Creation	Joe	Bitcoin
4/6/2021 8:33:16 PM	Bitcoin Last Accessed	Item Last Access	Joe	Bitcoin
4/6/2021 8:33:16 PM	Bitcoin Last Modified	Item Last Modify	Joe	Bitcoin
4/6/2021 8:33:12 PM	Ethereum Last Accessed	Item Last Access	Joe	Ethereum
4/6/2021 12:59:04 PM	Ethereum Last Registry Write	Item Last Registry Write	Joe	Ethereum
4/6/2021 12:59:00 PM	Ethereum Last Modified	Item Last Modify	Joe	Ethereum
4/6/2021 12:59:00 PM	Ethereum Created	Item Creation	Joe	Ethereum
4/6/2021 12:59:00 PM	Ethereum Last Modified	Item Last Modify	Joe	Ethereum
4/6/2021 12:59:00 PM	Ethereum Last Accessed	Item Last Access	Joe	Ethereum
4/6/2021 12:59:00 PM	Ethereum Created	Item Creation	Joe	Ethereum
4/6/2021 12:58:52 PM	Testing_Code_1 Last Registry Write	Item Last Registry Write	Joe	Testing_Code_1
4/6/2021 12:58:23 PM	Memes Last Registry Write	Item Last Registry Write	Joe	Memes
4/6/2021 12:58:22 PM	Temp_Code_3 Last Registry Write	Item Last Registry Write	Joe	Temp_Code_3
4/6/2021 12:58:20 PM	Testing_Code_4 Last Registry Write	Item Last Registry Write	Joe	Testing_Code_4
4/6/2021 12:58:20 PM	Testing_Code_4 Last Accessed	Item Last Access	Joe	Testing_Code_4
4/6/2021 12:58:18 PM	Testing_Code_2 Last Registry Write	Item Last Registry Write	Joe	Testing_Code_2
4/5/2021 6:12:28 PM	Hooli_Chat Last Accessed	Item Last Access	Joe	Hooli_Chat
4/5/2021 6:12:28 PM	Hooli_Mobile Last Accessed	Item Last Access	Joe	Hooli_Mobile

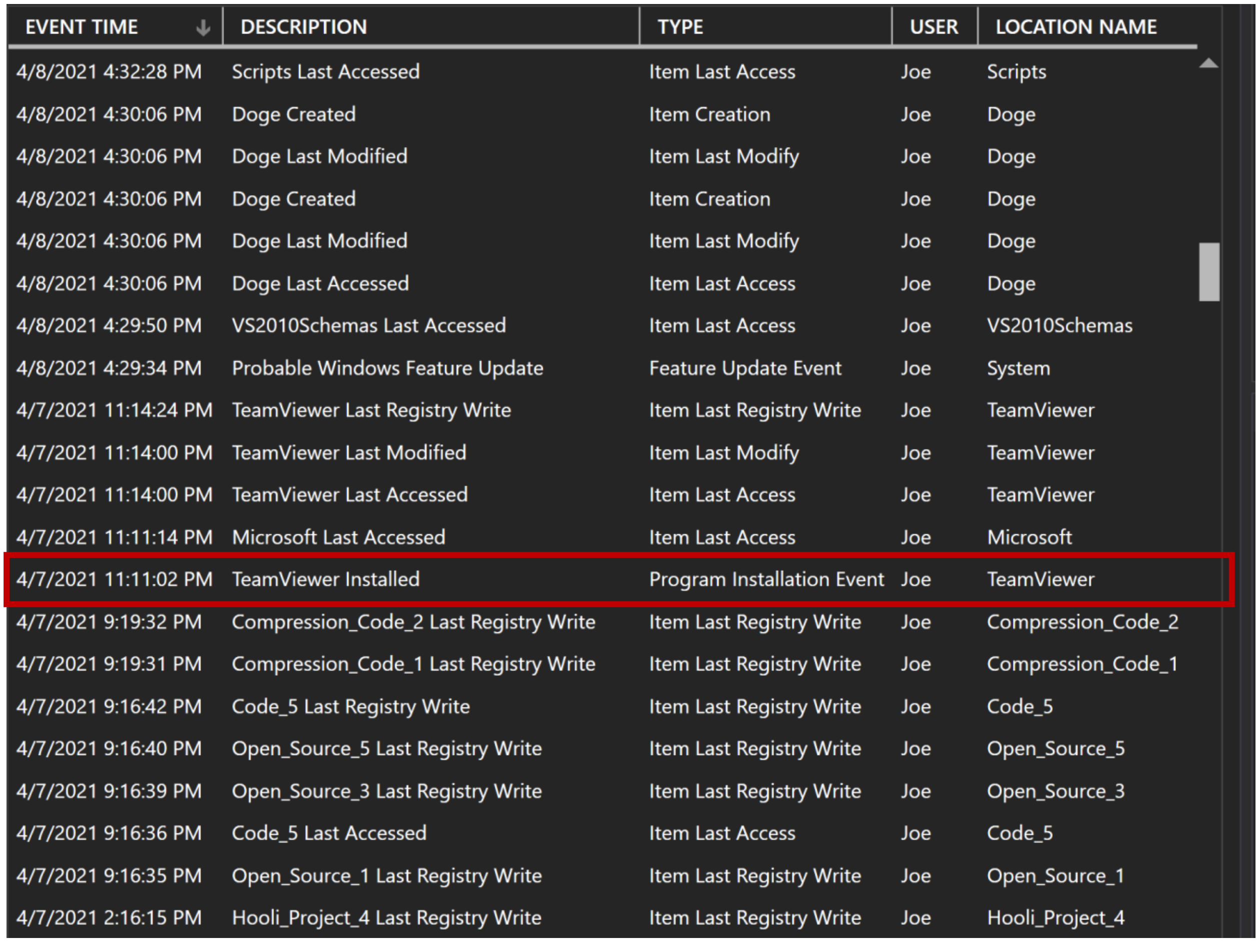
Figure 3. Showing definitive proof of policy breaking activities

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, any unapproved application causes an accidental deletion or overwriting of important folders and files could potentialy 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

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

ways and it is currently not known how TeamViewer has been used.



EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME
4/8/2021 4:32:28 PM	Scripts Last Accessed	Item Last Access	Joe	Scripts
4/8/2021 4:30:06 PM	Doge Created	Item Creation	Joe	Doge
4/8/2021 4:30:06 PM	Doge Last Modified	Item Last Modify	Joe	Doge
4/8/2021 4:30:06 PM	Doge Created	Item Creation	Joe	Doge
4/8/2021 4:30:06 PM	Doge Last Modified	Item Last Modify	Joe	Doge
4/8/2021 4:30:06 PM	Doge Last Accessed	Item Last Access	Joe	Doge
4/8/2021 4:29:50 PM	VS2010Schemas Last Accessed	Item Last Access	Joe	VS2010Schemas
4/8/2021 4:29:34 PM	Probable Windows Feature Update	Feature Update Event	Joe	System
4/7/2021 11:14:24 PM	TeamViewer Last Registry Write	Item Last Registry Write	Joe	TeamViewer
4/7/2021 11:14:00 PM	TeamViewer Last Modified	Item Last Modify	Joe	TeamViewer
4/7/2021 11:14:00 PM	TeamViewer Last Accessed	Item Last Access	Joe	TeamViewer
4/7/2021 11:11:14 PM	Microsoft Last Accessed	Item Last Access	Joe	Microsoft
4/7/2021 11:11:02 PM	TeamViewer Installed	Program Installation Event	Joe	TeamViewer
4/7/2021 9:19:32 PM	Compression_Code_2 Last Registry Write	Item Last Registry Write	Joe	Compression_Code_2
4/7/2021 9:19:31 PM	Compression_Code_1 Last Registry Write	Item Last Registry Write	Joe	Compression_Code_1
4/7/2021 9:16:42 PM	Code_5 Last Registry Write	Item Last Registry Write	Joe	Code_5
4/7/2021 9:16:40 PM	Open_Source_5 Last Registry Write	Item Last Registry Write	Joe	Open_Source_5
4/7/2021 9:16:39 PM	Open_Source_3 Last Registry Write	Item Last Registry Write	Joe	Open_Source_3
4/7/2021 9:16:36 PM	Code_5 Last Accessed	Item Last Access	Joe	Code_5
4/7/2021 9:16:35 PM	Open_Source_1 Last Registry Write	Item Last Registry Write	Joe	Open_Source_1
4/7/2021 2:16:15 PM	Hooli_Project_4 Last Registry Write	Item Last Registry Write	Joe	Hooli_Project_4

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

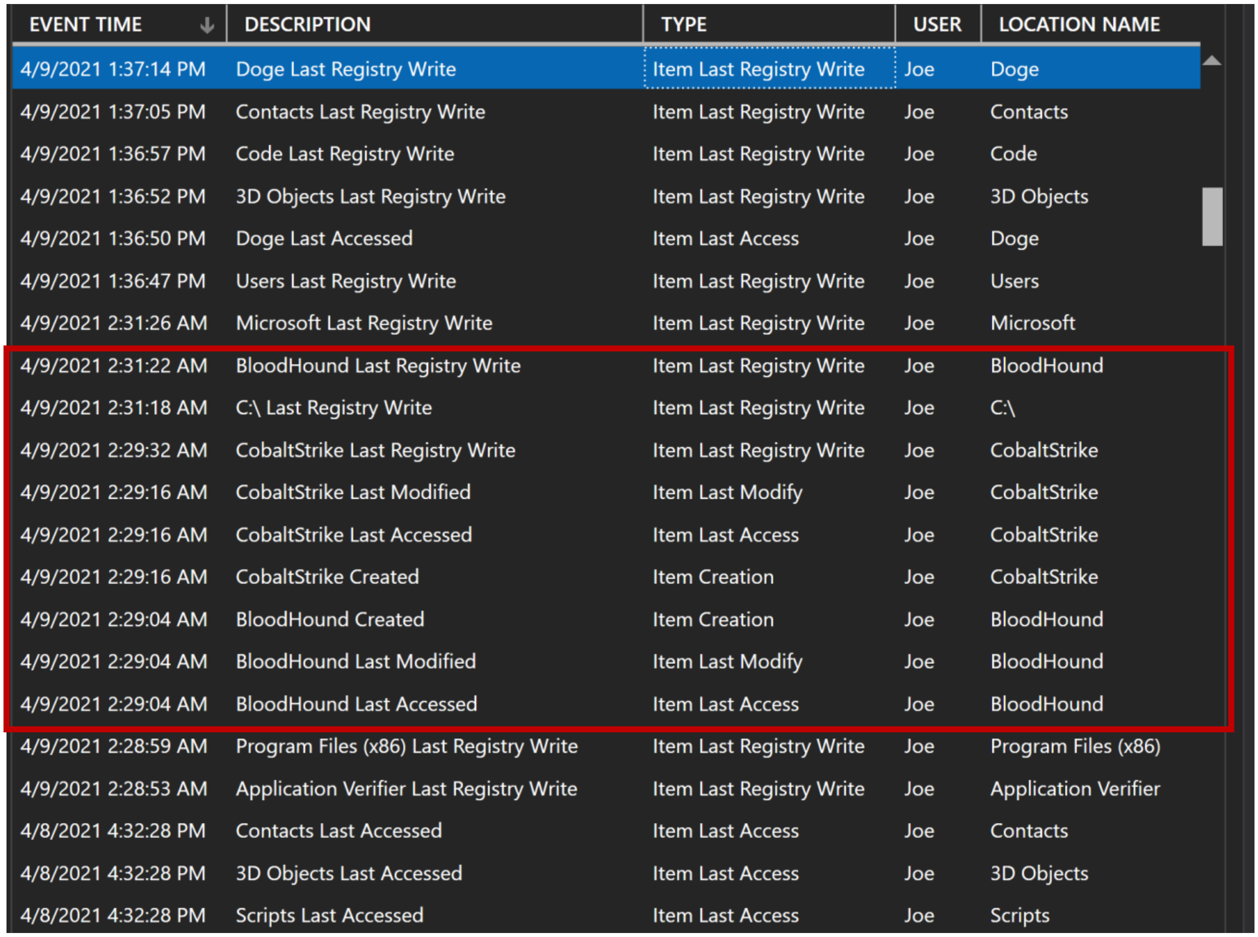
First Signs of Threat Actor Activity

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.” This needs to be reported to the client.

[2] https://www.cobaltstrike.com/

[3] https://github.com/BloodHoundAD/BloodHound

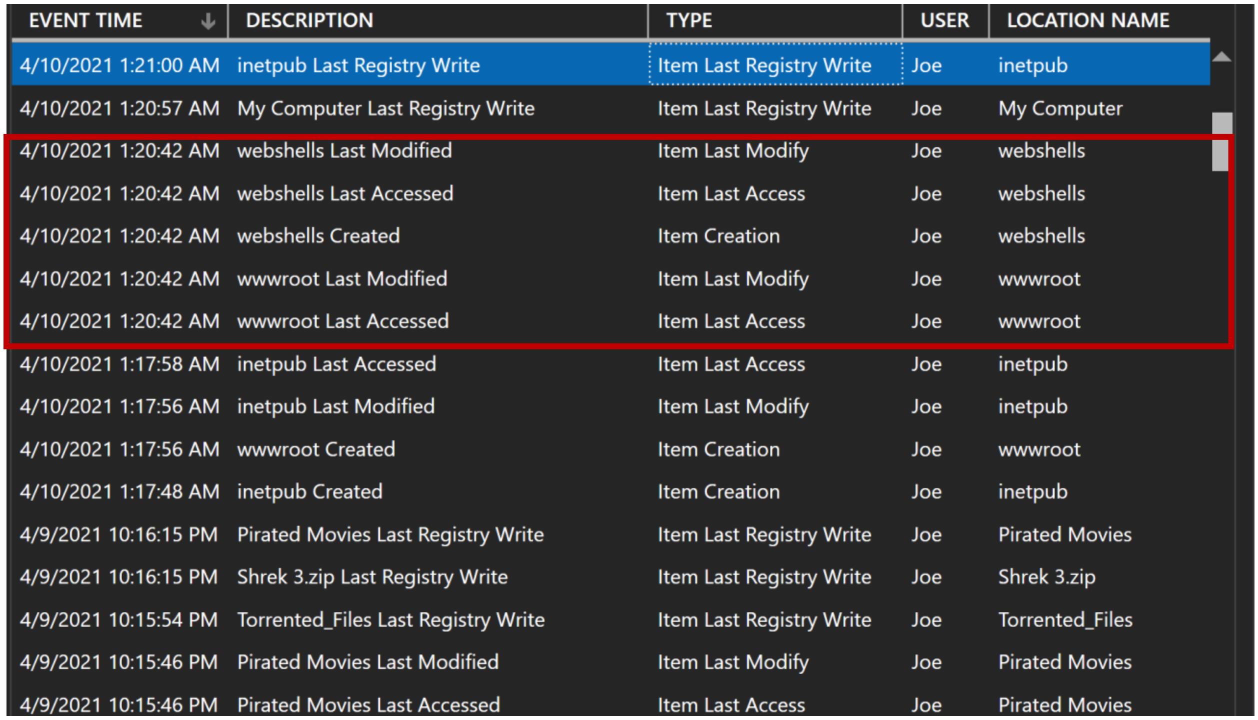


EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME
4/9/2021 1:37:14 PM	Doge Last Registry Write	Item Last Registry Write	Joe	Doge
4/9/2021 1:37:05 PM	Contacts Last Registry Write	Item Last Registry Write	Joe	Contacts
4/9/2021 1:36:57 PM	Code Last Registry Write	Item Last Registry Write	Joe	Code
4/9/2021 1:36:52 PM	3D Objects Last Registry Write	Item Last Registry Write	Joe	3D Objects
4/9/2021 1:36:50 PM	Doge Last Accessed	Item Last Access	Joe	Doge
4/9/2021 1:36:47 PM	Users Last Registry Write	Item Last Registry Write	Joe	Users
4/9/2021 2:31:26 AM	Microsoft Last Registry Write	Item Last Registry Write	Joe	Microsoft
4/9/2021 2:31:22 AM	BloodHound Last Registry Write	Item Last Registry Write	Joe	BloodHound
4/9/2021 2:31:18 AM	C:\ Last Registry Write	Item Last Registry Write	Joe	C:\
4/9/2021 2:29:32 AM	CobaltStrike Last Registry Write	Item Last Registry Write	Joe	CobaltStrike
4/9/2021 2:29:16 AM	CobaltStrike Last Modified	Item Last Modify	Joe	CobaltStrike
4/9/2021 2:29:16 AM	CobaltStrike Last Accessed	Item Last Access	Joe	CobaltStrike
4/9/2021 2:29:16 AM	CobaltStrike Created	Item Creation	Joe	CobaltStrike
4/9/2021 2:29:04 AM	BloodHound Created	Item Creation	Joe	BloodHound
4/9/2021 2:29:04 AM	BloodHound Last Modified	Item Last Modify	Joe	BloodHound
4/9/2021 2:29:04 AM	BloodHound Last Accessed	Item Last Access	Joe	BloodHound
4/9/2021 2:28:59 AM	Program Files (x86) Last Registry Write	Item Last Registry Write	Joe	Program Files (x86)
4/9/2021 2:28:53 AM	Application Verifier Last Registry Write	Item Last Registry Write	Joe	Application Verifier
4/8/2021 4:32:28 PM	Contacts Last Accessed	Item Last Access	Joe	Contacts
4/8/2021 4:32:28 PM	3D Objects Last Accessed	Item Last Access	Joe	3D Objects
4/8/2021 4:32:28 PM	Scripts Last Accessed	Item Last Access	Joe	Scripts

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.



EVENT TIME	DESCRIPTION	TYPE	USER	LOCATION NAME
4/10/2021 1:21:00 AM	inetpub Last Registry Write	Item Last Registry Write	Joe	inetpub
4/10/2021 1:20:57 AM	My Computer Last Registry Write	Item Last Registry Write	Joe	My Computer
4/10/2021 1:20:42 AM	webshells Last Modified	Item Last Modify	Joe	webshells
4/10/2021 1:20:42 AM	webshells Last Accessed	Item Last Access	Joe	webshells
4/10/2021 1:20:42 AM	webshells Created	Item Creation	Joe	webshells
4/10/2021 1:20:42 AM	wwwroot Last Modified	Item Last Modify	Joe	wwwroot
4/10/2021 1:20:42 AM	wwwroot Last Accessed	Item Last Access	Joe	wwwroot
4/10/2021 1:17:58 AM	inetpub Last Accessed	Item Last Access	Joe	inetpub
4/10/2021 1:17:56 AM	inetpub Last Modified	Item Last Modify	Joe	inetpub
4/10/2021 1:17:56 AM	wwwroot Created	Item Creation	Joe	wwwroot
4/10/2021 1:17:48 AM	inetpub Created	Item Creation	Joe	inetpub
4/9/2021 10:16:15 PM	Pirated Movies Last Registry Write	Item Last Registry Write	Joe	Pirated Movies
4/9/2021 10:16:15 PM	Shrek 3.zip Last Registry Write	Item Last Registry Write	Joe	Shrek 3.zip
4/9/2021 10:15:54 PM	Torrented_Files Last Registry Write	Item Last Registry Write	Joe	Torrented_Files
4/9/2021 10:15:46 PM	Pirated Movies Last Modified	Item Last Modify	Joe	Pirated Movies
4/9/2021 10:15:46 PM	Pirated Movies Last Accessed	Item Last Access	Joe	Pirated Movies

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 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