

Case Study #2 Writeup

Table of Contents

Situation	2
The Investigation	3
Pre-Investigative Observations	3
Setting up Timeline Filters in SeeShells	3
Initial Findings	4
Further Investigations	6
Patterns Within this Investigation	9
Conclusion	11

Situation

Arasaka is a global conglomerate whose subsidiaries span across several industry types, including defense, investment banking, manufacturing, private security, and biotechnology. As a cyber security analyst working within their security department, you are responsible for learning about any potential threats, investigating breaches, and investigating any reports. On 03/26/2021 you have received a report that an employee within the company accidentally clicked a phishing link, and inputted their username/password combination for their VNC client access (a remote desktop application) into a fake website. The employee mentioned that they initially clicked the phishing link on 03/21/2021 and inputted their username/password combination on that same day. They thought it was a legitimate email until they noticed the email's domain is not one that is affiliated with Arasaka. You were able to receive the computer's ShellBag information as part of the investigation. Are you able to figure out any patterns of unusual activity? And if so, what was done (what tools were used, what information was found, etc.)?

The Investigation

Pre-Investigative Observations

One of the first things to note is that the company utilizes VNC to allow their workers to remotely access their work computer. The worker potentially had their VNC credentials compromised so if a threat actor was able to capture those credentials, they would have full access to the computer as the employee.

Another thing to note is the currently known timeline. The employee initially clicked the phishing link and inputted their username/password combination on 03/21/2021 and the current day is 03/26/2021.

Setting up Timeline Filters in SeeShells

Within SeeShells we can filter out ShellBag events that happened outside of the interested timeline. To do this, go to the bottom left and next to Hex Viewer, click **Filter Controls** and edit the dates. A screenshot of what the timeline looks like with the timeline filters is shown below:

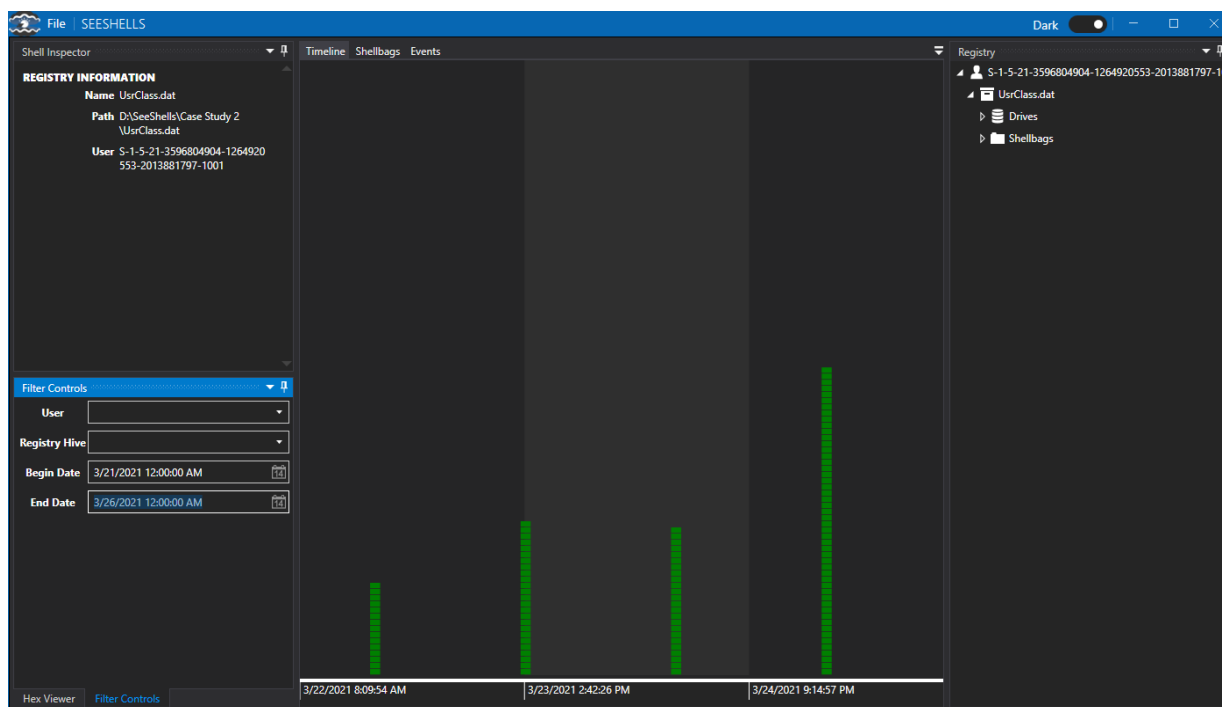


Figure 1. Timeline view with the timestamp filters

Initial Findings

Utilizing the Events view, there seems to be no ShellBag activity that happens the day the employee clicked the phishing link (03/21/2020). The following day there seems to be no immediate signs of intrusion as well. However going into Tuesday, 03/23/2020 at around 2 AM, there is a directory that was created onto the system named mimikatz_trunk. According to Offensive Security¹, “Mimikatz is a great post-exploitation tool written by Benjamin Delpy (gentilkiwi). After the initial exploitation phase, attackers may want to get a firmer foothold on the computer/network. Doing so often requires a set of complementary tools. Mimikatz is an attempt to bundle together some of the most useful tasks that attackers will want to perform.” On the left side is SeeShell’s Inspector view which allows us to take a closer look into individual Shell items.

¹ <https://www.offensive-security.com/metasploit-unleashed/mimikatz/>

Looking into that newly created directory, it appears that it was placed under a different directory named Applications.

Timeline Shellbags Events				
TYPE	DESCRIPTION	EVENT TIME	↑	USER
Item Last Registry Write	Military_Vehicle_5 Last Registry Write	3/19/2021 2:09:30 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Military_Vehicle_13 Last Registry Write	3/19/2021 2:09:32 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Weapon_Design_3 Last Registry Write	3/19/2021 2:09:36 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Weapon_Design_4 Last Registry Write	3/19/2021 2:09:38 PM		S-1-5-21-3596804904-126
Item Last Access	Pictures Last Accessed	3/19/2021 6:08:58 PM		S-1-5-21-3596804904-126
Item Last Access	Military_Vehicle_15 Last Accessed	3/19/2021 6:09:36 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Military_Vehicle_6 Last Registry Write	3/22/2021 8:09:54 AM		S-1-5-21-3596804904-126
Item Last Registry Write	Weapon_Design_2 Last Registry Write	3/22/2021 8:09:57 AM		S-1-5-21-3596804904-126
Item Last Access	Windows Defender Last Accessed	3/22/2021 12:09:54 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Military_Vehicle_8 Last Registry Write	3/22/2021 2:18:04 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Military_Vehicle_12 Last Registry Write	3/22/2021 2:18:05 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Military_Vehicle_15 Last Registry Write	3/22/2021 2:18:07 PM		S-1-5-21-3596804904-126
Item Last Registry Write	OneDrive Last Registry Write	3/22/2021 2:18:11 PM		S-1-5-21-3596804904-126
Item Last Modify	Applications Last Modified	3/23/2021 2:03:48 AM		S-1-5-21-3596804904-126
Item Last Access	Applications Last Accessed	3/23/2021 2:03:48 AM		S-1-5-21-3596804904-126
Item Creation	Applications Created	3/23/2021 2:03:48 AM		S-1-5-21-3596804904-126
Item Creation	Applications Created	3/23/2021 2:03:48 AM		S-1-5-21-3596804904-126
Item Creation	mimikatz_trunk Created	3/23/2021 2:18:14 AM		S-1-5-21-3596804904-126
Item Creation	mimikatz_trunk Created	3/23/2021 2:18:14 AM		S-1-5-21-3596804904-126
Item Last Access	mimikatz_trunk Last Accessed	3/23/2021 2:18:14 AM		S-1-5-21-3596804904-126
Item Last Modify	mimikatz_trunk Last Modified	3/23/2021 2:18:14 AM		S-1-5-21-3596804904-126
Item Last Registry Write	IISExpress Last Registry Write	3/23/2021 12:32:21 PM		S-1-5-21-3596804904-126
Item Last Registry Write	config Last Registry Write	3/23/2021 12:32:21 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Templates Last Registry Write	3/23/2021 12:32:26 PM		S-1-5-21-3596804904-126
Item Last Registry Write	Visual Studio 2019 Last Registry Write	3/23/2021 12:32:27 PM		S-1-5-21-3596804904-126

Figure 2. The Applications directory being made and mimikatz_trunk being access right after

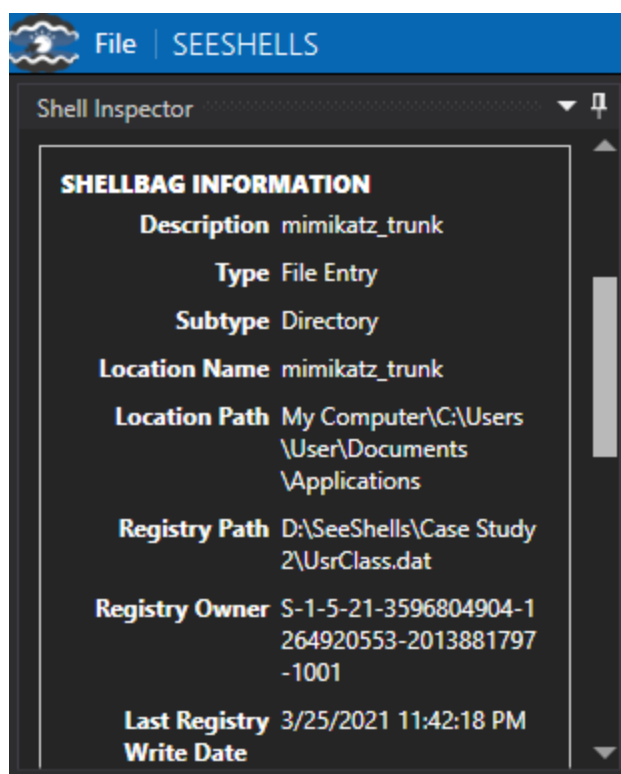


Figure 3. Looking at the Inspector view to see where it was downloaded

On the same day at 10 PM, we see the same suspicious mimikatz folder being accessed, along with other user accounts on the system.

Further Investigations

The following day (03/24/2021), we see there's similar activity that happens at approximately the same time at 2AM. The same mimikatz folder was accessed, and a new directory inside it was created named Accounts. Within this directory, there were a couple folders that were created, the names resemble a couple other users. Since mimikatz is a credential harvesting tool, these directories possibly contain the user's password hashes or files within those accounts. From an investigative standpoint, it can be assumed that those users are compromised.

Location Path My Computer\C:\Users\	Item Last Registry Write	V Last Registry Write	3/23/2021 10:27:51 PM	S-1-5-21-3596804904-1264920553-2013881797-1001	V
\User\Documents	Item Last Registry Write	JoshR Last Registry Write	3/23/2021 10:33:42 PM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR
\Applications	Item Last Access	Accounts Last Accessed	3/24/2021 2:02:18 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	Accounts
\mimikatz_trunk	Item Last Modify	Accounts Last Modified	3/24/2021 2:02:18 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	Accounts
\Accounts	Item Creation	Accounts Created	3/24/2021 2:02:18 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	Accounts
Registry Path D:\SeeShells\Case Study	Item Creation	Accounts Created	3/24/2021 2:02:18 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	Accounts
2\UsrClass.dat	Item Last Modify	mimikatz_trunk Last Modified	3/24/2021 2:02:30 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	mimikatz
Registry Owner S-1-5-21-3596804904-1	Item Creation	V Created	3/24/2021 2:27:44 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	V
264920553-2013881797	Item Last Modify	V Last Modified	3/24/2021 2:27:44 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	V
-1001	Item Creation	V Created	3/24/2021 2:27:44 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	V
Last Registry 3/25/2021 11:42:20 PM	Item Last Access	V Last Accessed	3/24/2021 2:27:44 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	V
	Item Last Modify	V Last Modified	3/24/2021 2:27:44 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	V
Filter Controls	Item Creation	JoshR Created	3/24/2021 2:33:36 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR
User	Item Last Modify	JoshR Last Modified	3/24/2021 2:33:36 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR
Registry Hive	Item Creation	JoshR Created	3/24/2021 2:33:36 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR
Begin Date 3/21/2021 12:00:00 AM	Item Last Access	JoshR Last Accessed	3/24/2021 2:33:36 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR
End Date 3/26/2021 12:00:00 AM	Item Last Modify	JoshR Last Modified	3/24/2021 2:33:36 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR

Figure 4. User accounts V and JoshR were likely compromised utilizing mimikatz

Soon after, a new directory under the initial Applications directory was created named WinPEAS. This is the Windows Privilege Escalation Awesome Scripts tool, essentially it is utilized as a post-exploitation tool to do further reconnaissance on the system, and to find any potential weaknesses to exploit on the system.

Item Creation	JoshR Created	3/24/2021 2:33:36 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR
Item Last Access	JoshR Last Accessed	3/24/2021 2:33:36 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR
Item Last Modify	JoshR Last Modified	3/24/2021 2:33:36 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	JoshR
Item Last Modify	Accounts Last Modified	3/24/2021 2:33:38 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	Accounts
Item Last Modify	WinPEAS Last Modified	3/24/2021 2:34:04 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	WinPEAS
Item Last Access	WinPEAS Last Accessed	3/24/2021 2:34:04 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	WinPEAS
Item Creation	WinPEAS Created	3/24/2021 2:34:04 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	WinPEAS
Item Creation	WinPEAS Created	3/24/2021 2:34:04 AM	S-1-5-21-3596804904-1264920553-2013881797-1001	WinPEAS
Item Last Registry Write	Documents Last Registry Write	3/24/2021 2:44:12 PM	S-1-5-21-3596804904-1264920553-2013881797-1001	Documents
Item Last Registry Write	Users Last Registry Write	3/24/2021 2:44:25 PM	S-1-5-21-3596804904-1264920553-2013881797-1001	Users
Item Last Registry Write	Documents Last Registry Write	3/24/2021 2:44:29 PM	S-1-5-21-3596804904-1264920553-2013881797-1001	Documents

Figure 5. The WinPEAS folder being created

The attacker then accesses a couple directories, namely the Documents and Users directories. There is no further activity that happens around this time.

The same day (03/24/2020) at around 10 PM, we see activity happening revolving around the WinPEAS folder - a directory was created within it named Network findings.

Following, a directory named BloodHound was created. BloodHound is another post-exploitation tool that it utilized to view Windows Active Directory relations within different accounts and systems. By utilizing these relations, attackers utilize this information to move laterally around the network. Another tool was downloaded on the system afterwards named PowerView which is a Windows Powershell tool to do further attacks on the system. Last, nmap - a network mapping tool was also downloaded onto the system. We can assume that the attacker downloaded these tools onto the system to do further enumeration on the computer after getting initial access.

TYPE	DESCRIPTION	EVENT
Item Last Access	Applications Last Accessed	3/24/2020
Item Last Registry Write	WinPEAS Last Registry Write	3/24/2020
Item Last Registry Write	WinPEAS findings Last Registry Write	3/24/2020
Item Last Registry Write	Networking findings Last Registry Write	3/24/2020
Item Last Registry Write	BloodHound Last Registry Write	3/24/2020
Item Last Registry Write	BloodHound findings Last Registry Write	3/24/2020
Item Last Registry Write	PowerView Last Registry Write	3/24/2020
Item Last Registry Write	nmap Last Registry Write	3/24/2020
Item Last Registry Write	network map Last Registry Write	3/24/2020
Item Last Modify	WinPEAS findings Last Modified	3/25/2020
Item Last Access	WinPEAS findings Last Accessed	3/25/2020
Item Creation	WinPEAS findings Created	3/25/2020
Item Last Modify	WinPEAS findings Last Modified	3/25/2020
Item Creation	WinPEAS findings Created	3/25/2020
Item Last Modify	WinPEAS Last Modified	3/25/2020
Item Creation	BloodHound Created	3/25/2020

Figure 6. WinPEAS, BloodHound, and nmap folders being created

Patterns Within this Investigation

By utilizing SeeShells to analyze the ShellBag artifacts, there is an observable pattern. At around 2 AM and 10 PM system time there is activity that revolves around the Applications directory. Within that directory are files that are potentially named after the tools that are installed inside of it.

On 03/26/2021, a folder named exfil was created which we can assume is files that are being staged for exfiltration. Utilizing the file view on the right side of SeeShells, we can easily see how the file system looks like - including what's inside that exfil folder.

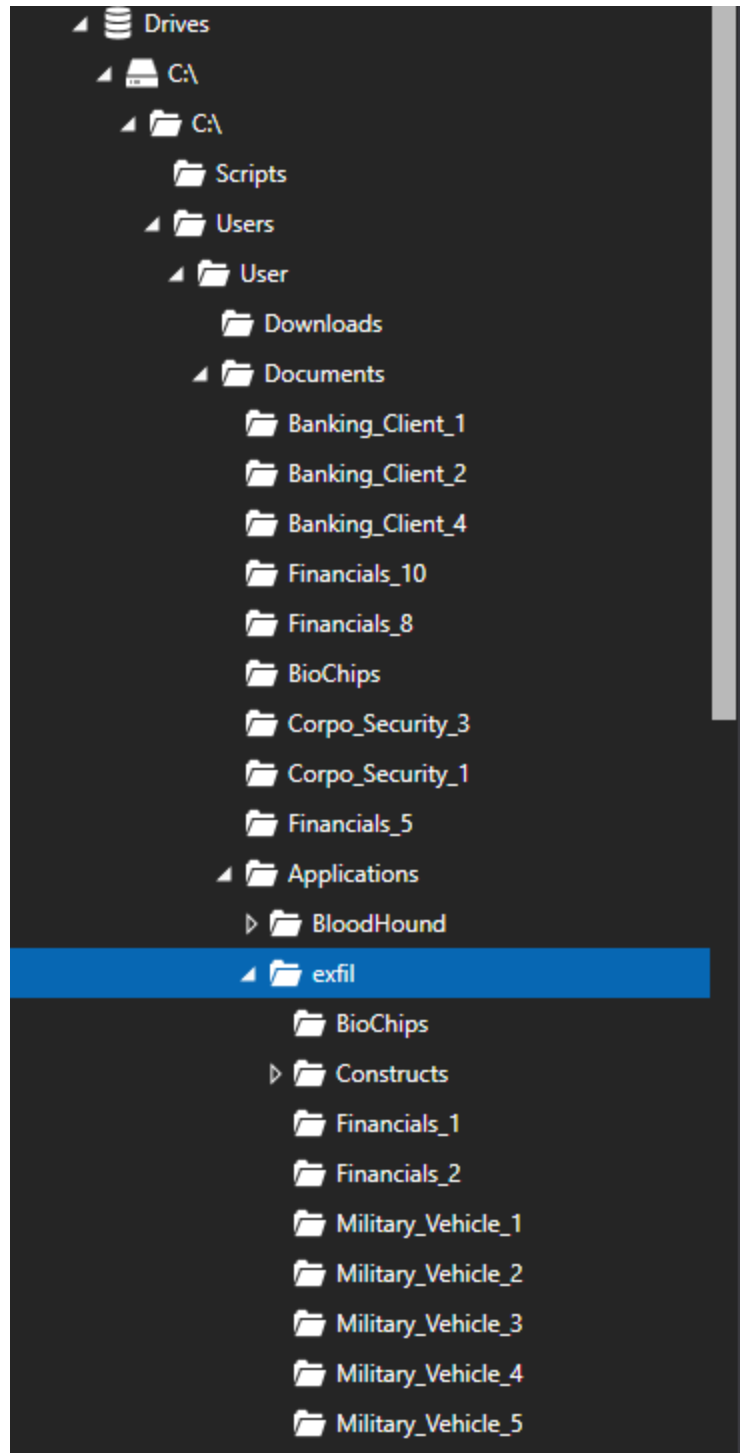


Figure 7. Contents inside the exfil folder

Conclusion

There is suspicious activity that falls within the timeline of events. It is likely the attacker created a directory named `Applications` to disguise it as a normal folder. Within that are subdirectories with names of post-exploitation tools - BloodHound, mimikatz, nmap, PowerView, and WinPEAS. It is likely that the attacker ran all of these tools and utilized it to gather information on how to move laterally around the network.

Furthermore, on 03/26/2021, there is evidence of a folder named `exfil` being created which is files that the attacker potentially exfiltrated. The following is a list folders that were likely exfiltrated outside the network environment:

- `Constructs`
- `Financials_1`
- `Financials_2`
- `Military_Vehicle_1`
- `Military_Vehicle_2`
- `Military_Vehicle_3`
- `Military_Vehicle_4`
- `Military_Vehicle_5`