SeeShells

Case Study #2 Writeup

Background Information:

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 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 input 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.)?

What we know:

- 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.
- 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.

What we need to find out:

- Is there any suspicious activity around the date of the incident?
- What tools were used?
- What information is the attacker interested in?

Guide:

Within SeeShells we can filter out ShellBag events that happened outside of the timeline we are interested in. To do this, go to the 'Global Event Filters' panel and edit the start dates. The phishing link was clicked on 3/21/2021, so this is a good start date. We are also going to put the end date as the 'current day' – 3/26/2021. A screenshot of what the timeline looks like with the timeline filters is shown below:

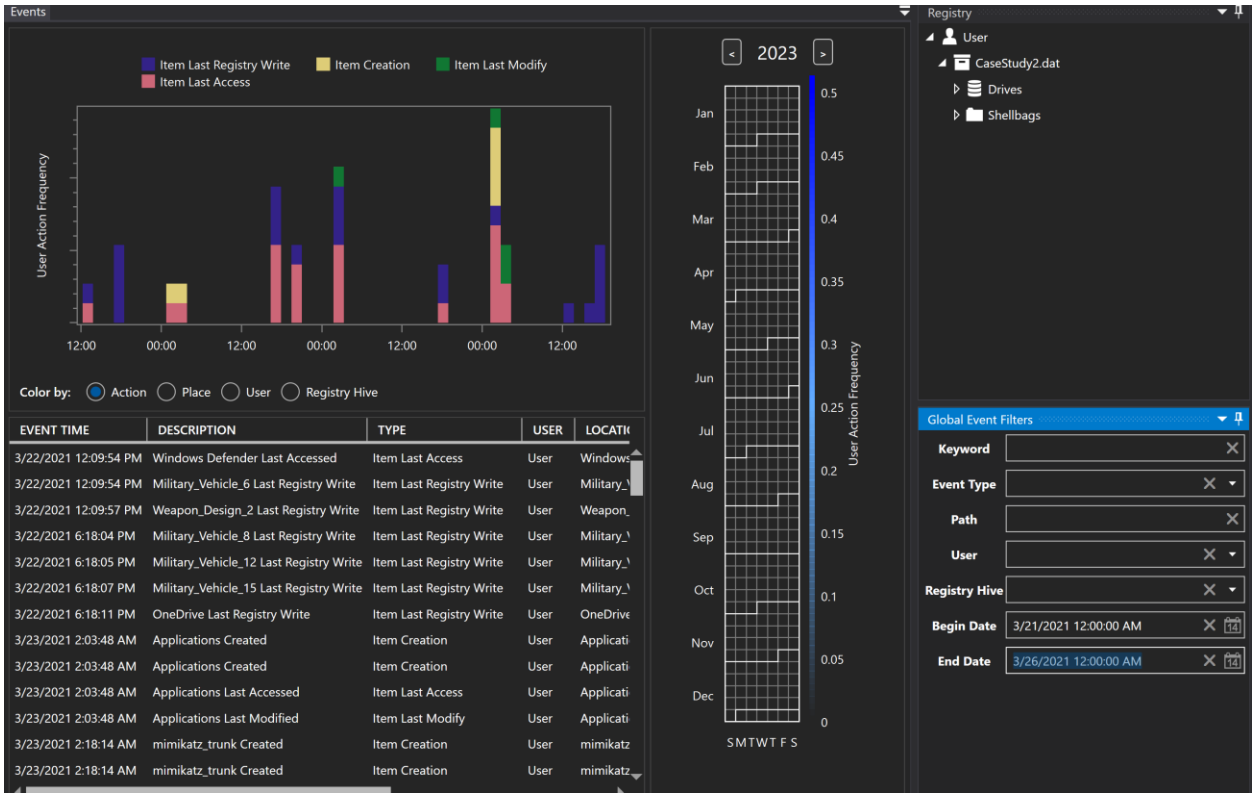


Figure 1. Timeline view with the timestamp filters

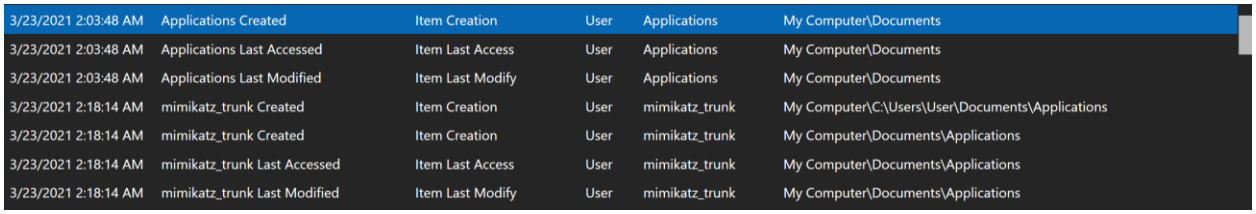
Initial Findings

Looking at the timeline view, there seems to be no ShellBag activity that happens the day the employee clicked the phishing link (03/21/2021). 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 Security[1], "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

[1] https://www.offensive-security.com/metasploit-unleashed/mimikatz/

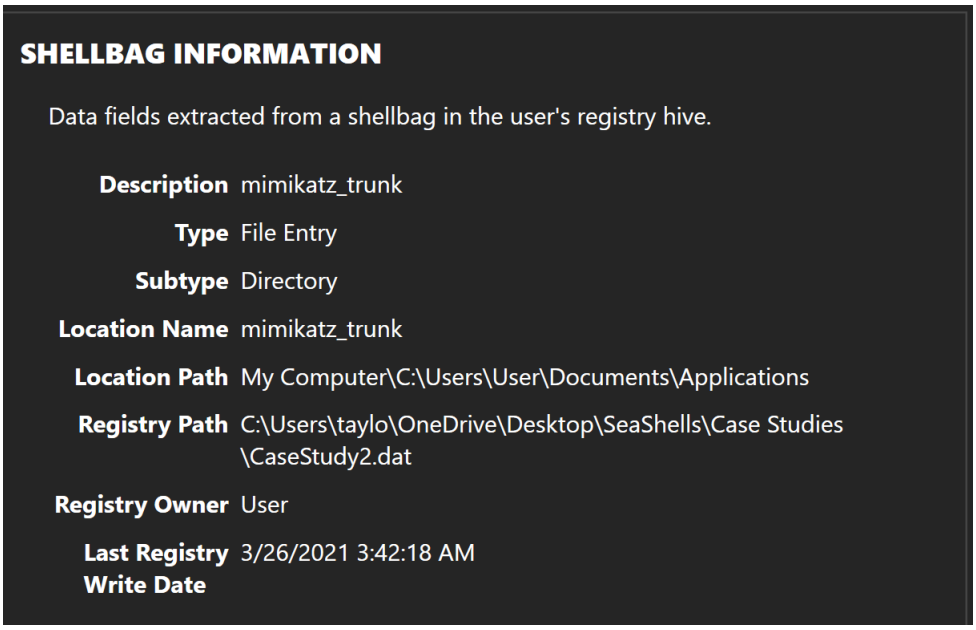
requires a set of complementary tools. Mimikatz is an attempt to bundle together some of the most useful tasks that attackers will want to perform." On the left side is SeeShell's Inspector view which allows us to take a closer look into individual Shell items.

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



3/23/2021 2:03:48 AM	Applications Created	Item Creation	User	Applications	My Computer\Documents
3/23/2021 2:03:48 AM	Applications Last Accessed	Item Last Access	User	Applications	My Computer\Documents
3/23/2021 2:03:48 AM	Applications Last Modified	Item Last Modify	User	Applications	My Computer\Documents
3/23/2021 2:18:14 AM	mimikatz_trunk Created	Item Creation	User	mimikatz_trunk	My Computer\C:\Users\User\Documents\Applications
3/23/2021 2:18:14 AM	mimikatz_trunk Created	Item Creation	User	mimikatz_trunk	My Computer\Documents\Applications
3/23/2021 2:18:14 AM	mimikatz_trunk Last Accessed	Item Last Access	User	mimikatz_trunk	My Computer\Documents\Applications
3/23/2021 2:18:14 AM	mimikatz_trunk Last Modified	Item Last Modify	User	mimikatz_trunk	My Computer\Documents\Applications

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



SHELLBAG INFORMATION

Data fields extracted from a shellbag in the user's registry hive.

Description	mimikatz_trunk
Type	File Entry
Subtype	Directory
Location Name	mimikatz_trunk
Location Path	My Computer\C:\Users\User\Documents\Applications
Registry Path	C:\Users\taylo\OneDrive\Desktop\SeaShells\Case Studies \CaseStudy2.dat
Registry Owner	User
Last Registry Write Date	3/26/2021 3:42:18 AM

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

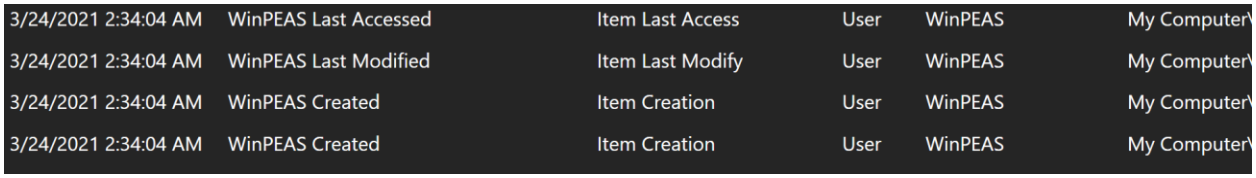
The following day (03/24/2021), we see there's similar activity that happens at approximately the same time at 2AM. The same mimikatz folder was accessed, and a new directory inside it was created named Accounts. Within this directory, there were a couple folders that were created, the names resemble 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.

3/24/2021 2:27:44 AM	V Last Accessed	Item Last Access	User	V	My Computer\
3/24/2021 2:27:44 AM	V Last Modified	Item Last Modify	User	V	My Computer\
3/24/2021 2:27:44 AM	V Created	Item Creation	User	V	My Computer\
3/24/2021 2:27:44 AM	V Last Modified	Item Last Modify	User	V	My Computer\
3/24/2021 2:27:44 AM	V Created	Item Creation	User	V	My Computer\
3/24/2021 2:27:51 AM	V Last Registry Write	Item Last Registry Write	User	V	My Computer\
3/24/2021 2:33:36 AM	JoshR Last Modified	Item Last Modify	User	JoshR	My Computer\
3/24/2021 2:33:36 AM	JoshR Created	Item Creation	User	JoshR	My Computer\
3/24/2021 2:33:36 AM	JoshR Last Accessed	Item Last Access	User	JoshR	My Computer\
3/24/2021 2:33:36 AM	JoshR Last Modified	Item Last Modify	User	JoshR	My Computer\
3/24/2021 2:33:36 AM	JoshR Created	Item Creation	User	JoshR	My Computer\
3/24/2021 2:33:38 AM	Accounts Last Modified	Item Last Modify	User	Accounts	My Computer\
3/24/2021 2:33:42 AM	JoshR Last Registry Write	Item Last Registry Write	User	JoshR	My Computer\

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.



3/24/2021 2:34:04 AM	WinPEAS Last Accessed	Item Last Access	User	WinPEAS	My Computer\
3/24/2021 2:34:04 AM	WinPEAS Last Modified	Item Last Modify	User	WinPEAS	My Computer\
3/24/2021 2:34:04 AM	WinPEAS Created	Item Creation	User	WinPEAS	My Computer\
3/24/2021 2:34:04 AM	WinPEAS Created	Item Creation	User	WinPEAS	My Computer\

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.

3/25/2021 2:08:52 AM	WinPEAS Last Registry Write	Item Last Registry Write	User	WinPEAS	My Computer\
3/25/2021 2:08:52 AM	WinPEAS findings Last Registry Write	Item Last Registry Write	User	WinPEAS findings	My Computer\
3/25/2021 2:18:24 AM	Networking findings Last Registry Write	Item Last Registry Write	User	Networking findings	My Computer\
3/25/2021 2:18:39 AM	BloodHound Last Registry Write	Item Last Registry Write	User	BloodHound	My Computer\
3/25/2021 2:18:39 AM	BloodHound findings Last Registry Write	Item Last Registry Write	User	BloodHound findings	My Computer\
3/25/2021 2:35:40 AM	PowerView Last Registry Write	Item Last Registry Write	User	PowerView	My Computer\
3/25/2021 2:58:59 AM	nmap Last Registry Write	Item Last Registry Write	User	nmap	My Computer\
3/25/2021 2:58:59 AM	network map Last Registry Write	Item Last Registry Write	User	network map	My Computer\

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.

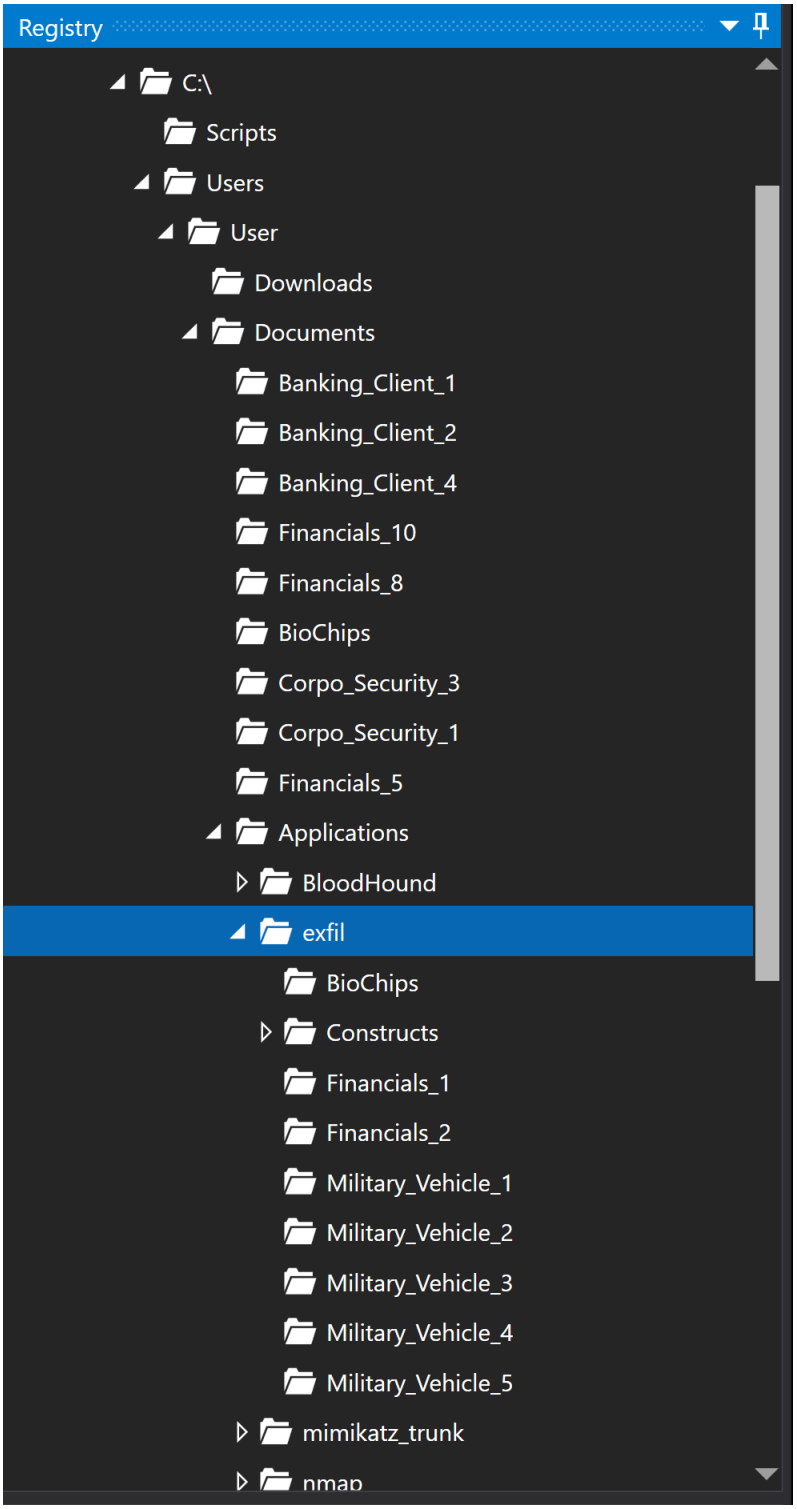


Figure 7. Contents inside the exfil folder

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