NOVACTF{2023}

Forensic Challenge

Description:

A suspected "threat group" has been targeting the Semiconductor Industry in Taiwan, and "Agent Hunt" has been tasked with investigating their activities. During his investigation, Hunt discovers that the group has been using advanced techniques and tactics, some of which are associated with the MITRE ATT&CK framework.

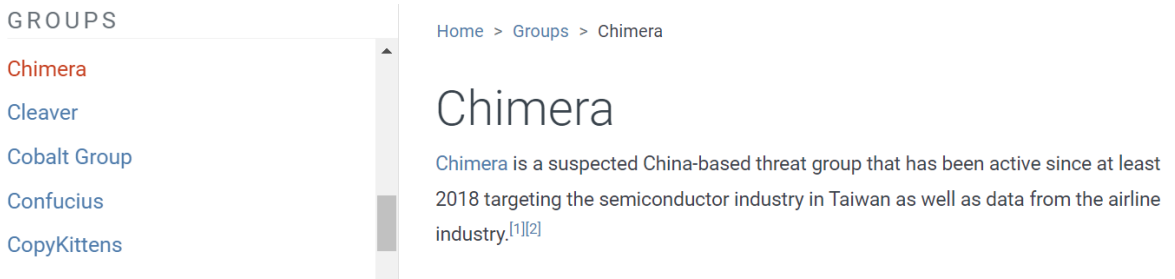
One critical piece of evidence discovered by Hunt is the use of a "tool" that appears to be communicating with a command-and-control channel. This tool is in the format of an "executable" and is likely related to password dumping activities. Hunt believes that this tool could provide valuable insights into the methods and techniques used by the attackers.

However, the investigation is complicated by the fact that the attackers have taken steps to cover their tracks. They are using various evasion techniques, making it difficult for Hunt and his team to trace their activities. Nonetheless, Hunt continues to analyze the evidence he has gathered and seeks to find additional leads that could help him identify the perpetrators.

As the investigation continues, Hunt realizes that Finding the tool is very important to identify the attackers and prevent future attacks on the Semiconductor Industry in Taiwan.Identify the Tool

Approach:

By Searching the Threat Group in MITRE ATT&CK framework we can find the suspected group is Chimera.



Next given hint is use of a "tool" that appears to be communicating with a command and control channel. By searching for tool we can find the resources at the end.

References

1. Cycraft. (2020, April 15). APT Group Chimera - APT Operation Skeleton key Targets Taiwan Semiconductor Vendors. Retrieved August 24, 2020.
2. Jansen, W . (2021, January 12). Abusing cloud services to fly under the radar. Retrieved January 19, 2021.

Link: https://research.nccgroup.com/2021/01/12/abusing-cloud-services-to-fly-under-the-radar/

After opening the resources we can look into any Sort of information we can find for the tool

Privilege escalation (TA0004)

The adversary started a password spraying attack against those domain admin accounts, and successfully got a valid domain admin account this way. In other cases, the adversary moved laterally to another system with a domain admin logged in. We observed the use of Mimikatz on this system and saw the hashes of the logged in domain admin account going through the command and control channel of the adversary. The adversary used a tool called NtdsAudit to dump the password hashes of domain users as well as we observed the following command:

```
msadcs.exe "NTDS.dit" -s "SYSTEM" -p RecordedTV_pdmp.txt --users-csv
RecordedTV_users.csv
```

Note: the adversary renamed ntdsaudit.exe to msadcs.exe.

Another Hint given here is tool is in the format of an "executable" and is likely related to password dumping activities. Actually the Tool used for password dump hashes of domains users is NTdsAudit

and the hint given is tool is the format of executable means (.exe)

so the Flag is NOVA { NTdsAudit.exe}

Another Approach we can find the tool by searching in the page of chimera group for credential Dumping.

Enterprise	T1003	.003	OS Credential Dumping: NTDS	Chimera has gathered the SYSTEM registry and ntds.dit files from target systems.[1] Chimera specifically has used the NtdsAudit tool to dump the password hashes of domain users via `msadcs.exe "NTDS.dit" -s "SYSTEM" -p RecordedTV_pdmp.txt --users-csv RecordedTV_users.csv` and used ntdsutil to copy the Active Directory database.[2]
Enterprise	T1201		Password Policy Discovery	Chimera has used the NtdsAudit utility to collect information related to accounts and passwords.[2]

https://attack.mitre.org/techniques/T1003/003/

And cobalt strike is not the Flag because NtdsAudit.exe is a command-line tool that can be used to extract password hashes from the Active Directory (AD) database, also known as the NTDS.dit file. This file stores the hashes of all user accounts and their respective passwords in a Windows domain. NtdsAudit.exe can be used by an attacker who has administrative privileges on a Windows domain controller to dump these hashes and then attempt to crack them to recover the actual passwords. Credential dumping is a common technique used by attackers to obtain the credentials of legitimate users on a network, which can then be used to escalate privileges, move laterally across the network, and ultimately achieve their objectives. Cobalt Strike is a popular post-exploitation tool that can be used for many purposes, including lateral movement, privilege escalation, and data exfiltration. However, it is not typically used for credential dumping. Instead, attackers often use standalone tools or custom scripts for this purpose. One reason why the Chimera group might not use Cobalt Strike for credential dumping is that it is a well-known and widely used tool, which means that its use may be detected and flagged by security solutions. By using less well-known tools or custom scripts, the group may be able to evade detection and maintain its covert operations for longer periods of time. It’s worth noting that the use of NtdsAudit.exe or any other tool for credential dumping is not inherently malicious. These tools are legitimate system administration and security tools that can be used for legitimate purposes. However, when used by attackers without authorization, they can be extremely effective in compromising network security and stealing sensitive data.