APT1

“APT1 is a Chinese threat group that has been attributed to the 2nd Bureau of the People’s Liberation Army (PLA) General Staff Department’s (GSD) 3rd Department, commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398” (Mitre Att&ck, 2021).

**Techniques**

There was 20+ techniques used by APT1, so I chose a few that interested me most.

* Account Discovery: Local Account
  + Used commands **net localgroup**, **net user**,and **net group** to find accounts on victim’s system.
* Email Collection: Local Email Collection
  + Used GETMAIL and MAPIGET to steal emails. They were extracted from archived Outlook .pst files.
* Establish Accounts: Email Accounts
  + Created email accounts for use in social engineering, phishing, and registered domains.
* Phishing: Spearphishing Attachment
  + Sent spearphishing emails containing malicious attachments.
* Remote Services: Remote Desktop Protocol
  + Used RDP during operations, possibly to gain information from users’ computers, steal login credentials, and observe employee computer activities.
* Other included:
  + Acquire Infrastructure: Domains, Acquire Infrastructure: Domains, Automated Collection, Data from Local System, Process Discovery, System Network Configuration Discovery, Network Share Discovery, and more.

**Software**

APT1 used software like BISCUIT, Cachedump, CALENDAR, GLOOXMAIL, gsecdump, ipconfig, Lslsass, Mimikatz, Net, Pass-The Hash Toolkit, PoisonIvy, PsExec, pwdump, Seasalt, Tasklist, WEBC2, and xCmd.

**Application**

Besides the obvious, the techniques utilized by APT1 can be used to further compromise an organization by predicting its future actions. It is impossible for the organization to start from scratch and change their habits entirely. The most they can do is patch their vulnerabilities and protect themselves from future attacks.

APT1 can also use the information learned from previous victims to enhance their skills, making them smarter and harder to detect. For example, they can home in on their spear phishing skills, making their emails even more difficult to decipher from the real thing. They can also further enhance their social engineering skills, making it easier to manipulate victims into sharing information.

There are several other steps APT1 can take to better prepare themselves for future attacks, but I hope they will be stopped long before then (which seems impossible, unfortunately).

References

MITRE ATT&CK®. (2021, May 26). *APT1*. <https://attack.mitre.org/groups/G0006/>