**Advanced Persistent Threats**

Report by – Harsh Sharma

**Who are Advanced Persistent Threats?**

Advanced Persistent Threats often termed as APTs is a group of threat actors who are the most experienced group of threat actors who have access to the state-of-art attack tools and tactics like Cyber, Physical and Deception to exploit the vulnerabilities and get into the companies’ network.

These groups are mainly state sponsored and under some government-funded like APT1 group is backed by 2nd bureau of the People Liberation Army General Staff Departments 3rd Department aka Unit 91398.

There are hundreds of APT groups present in the Cyber World to get the data of the companies, although they have set their areas and criteria. For e.g., APT1 Group targets on sectors like Aerospace, Education, Energy, Finance Industries, Healthcare, Information Technology, Mining, Research and Transportation

List of Countries attacked by APT1:

Belgium, Canada, France, Israel, Japan, Norway, Switzerland, UAE. UK and USA.

**AIM of Advanced Persistent Threats**

1. Establishing and Extending footholds within the information
2. Exfiltration of data
3. Stopping the critical aspects of the mission
4. Making disruptions in the ongoing missions
5. Promoting hacktivism

**Specialties of APTs**

1. Pursues its objectives, repeatedly over extended period
2. Observes the defenders’ efforts and resist them
3. Determined to escalate and maintain the privileges which is needed to execute and pursue the objectives.
4. Have ability to adapt the changes in the implemented security controls at the target.
5. They are very knowledgeable and always one step ahead against the defenders.

**How they are different from other hacker groups?**

1. They take more time in reconnaissance of the network and discover zero-day attacks
2. They make zero-day exploits and malwares that the target cannot detect
3. Social Engineering is heavily used by the APTs and their part of TTPs.

Social engineering is the major technique of APTs, as per Mr. John McAfee,

“Social Engineering has become about 75% of an average hacker’s toolkit and for the most successful hackers, it reaches 90% or more.”

**Life-cycle of APTs**

1. Initial Compromise – Using the art of deception and zero-day exploits to gain the initial access of the system.
2. Establish Foothold – Installing backdoor in the systems to make persistence by installing Remote Access Trojans.
3. Escalate Privileges – Password attacks are done to escalate the privileges.
4. Internal Reconnaissance – Completing the objectives and getting more information for lateral movement
5. Move Laterally - Expanding the access to the system to system, server to server.
6. Maintain Presence – making persistence in the systems
7. Complete Mission Data exfiltration is performed

**TOP 5 APT GROUPS**

1. Lazarus group APT 38
2. Equation group
3. Fancy Bear APT 28
4. Charming Kitten APT 35
5. Elfin APT 33

**Lazarus group APT 38**

Lazarus Group is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau. [The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups, such as Andariel, APT37, APT38, and Kimsuky.

**Equation group**

Equation is a sophisticated threat group that employs multiple remote access tools. The group is known to use zero-day exploits and has developed the capability to overwrite the firmware of hard disk drives.

Equation group is in the Tailored Access Operations (TAO) unit of NSA

**Fancy Bear APT 28**

Fancy Bear, also known as APT 28, Sofacy, or Swallowtail, is a cyberespionage group that is linked to the Russian government. The group has been in operation since 2008, targeting the energy, government, media, aerospace, and defense sectors via phishing campaigns and credential harvesting. Fancy Bear is known to target both computers and mobile devices, running multiple intrusion operations concurrently.

In 2016, Fancy Bear was front and center after they attacked the Democratic National Committee (DNC). The group was also responsible for leaking confidential drug testing information after they attacked the World Anti-Doping Agency (WADA) during the same year. Fancy Bear took credit for the attack and leaked the stolen information on a site named “Fancy Bears”. Despite two very public attacks, Fancy Bear returned to the shadows in 2017. Since that time, the group’s activities have become clandestine, motivated by intelligence gathering.

Between 2017 and 2018, Fancy Bear targeted the following organizations:

* European military
* European government
* A South American country’s government
* An Eastern European embassy
* A prominent international organization

**Charming Kitten APT 35**

The Iranian advanced persistent threat actor and cyberespionage group, APT35, also known as Charming Kitten or Phosphorus, has been making headlines since 2014. During that time, the group launched one of the most sophisticated internet based spying campaigns organized by Iranian threat actors – a campaign conducted via social media.

Since then, the group has not slowed down and has been responsible for several other cyber-attacks around the world. In 2019, APT35 was responsible for targeting several academic institutions in the U.S, France, and the Middle East region. In late 2020, the group targeted medical research organizations in Israel and in the U.S. By 2021, APT35 was abusing Microsoft Exchange Server vulnerabilities that were chained together (Proxy Shell).

As of 2022, APT35 has been observed using new tactics to attack a wide range of targets. Using a new strain of malware, the threat actors were able to use the malware for intelligence collection. The group has also been seen using a new tool called Hyper scrape to quietly extract emails from victim’s mailboxes.

**Elfin APT 33**

The Elfin espionage group (aka APT33) has remained highly active over the past three years, attacking at least 50 organizations in Saudi Arabia, the United States, and a range of other countries.

The group, which first became active in late 2015 or early 2016, specializes in scanning for vulnerable websites and using this to identify potential targets, either for attacks or creation of command and control (C&C) infrastructure. It has compromised a wide range of targets, including governments along with organizations in the research, chemical, engineering, manufacturing, consulting, finance, telecoms, and several other sectors.

**Conclusion**

All the above APT groups mentioned are very dangerous and needs to be stopped but these types of cyber-attacks they made will never be stopped. Companies must take more than sufficient security measures to keep their defence strong. APTs will always find a way to get into the network. Mostly the attacks get occurred due to social engineering and human error. Considering these things can prevent the company from an upcoming attack.