**Operation Soft Cell**

**A Worldwide Campaign Against Telecom Providers**

**Report by – Harsh Sharma**

**Operation SOFTCELL**

In 2018, A huge data leakage attack was occurred on various telecom providers such as AT&T, Vodafone, T-Mobile globally. 100’s GB of data was leaked according to the cyber security professionals of Cybereason.

**Details of the Attack and the Malware**

Firstly, the SOC team of Cybereason detected a malware which was known to them but that malware was highly modified and scripted which did beyond the teams’ expectations and jumped across the networks which made huge data leakage. The main problem was between the air-gapped networks. The data inside in the servers was hidden from outside world which means the data cannot be accessed from outside world. But the malware was connected to the malicious server.

The attackers were successful throughout the attack to gain the data using different tools installed in the servers. The attack was a multi-wave attack because of multiple attacks at the servers. Making it low and slow so it cannot be detected easily. SOFTCELL Operation was active since 2012.

**Impact**

The attack was only meant to obtain the data of very high personalities but ended up in a complete takeover of the network.

The threat actors were attempting to steal all the data stored in their active directory compromising every single Username and password in the organization along with other personally identifiable data such as:

1. Billing Information
2. Call detail records
3. Credentials
4. Email Servers
5. Geo-location of the users

Operation SOFTCELL was an APT Attack associated with Chinese affiliated threat actors such as APT10, APT41 and LuckyMouse.

**Malware and Tools used in the Attack**

The malwares were injected in the servers by using malicious servers.

* According to the Cybereason, Phantom Creator was used to generate a server.
* To stole the credentials modified version of Mimikatz was used.
* Poison IVY was the malware which was injected in the Air-gapped networks
* Web shells were created, so that the tools can be installed in the servers to gain the access and obtain the data.

**Nature of SOFTCELL Operation**

The attack was very slow and low because it was not been detected for several years. The attack was a multi-wave attack which made huge data leakage.