Incident Report: Equifax Breach

Summary:

This report details the attack flow of the 2017 Equifax data breach, which compromised the personal information of approximately 147 million people. The breach was carried out by four members of the Chinese People's Liberation Army (PLA): Wu Zhiyong, Wang Qian, Xu Ke, and Liu Lei, who were indicted by the U.S. Department of Justice for computer fraud, economic espionage, and wire fraud.

Attack Details:

The attack began with the threat actors conducting vulnerability scanning to identify systems with a known vulnerability in the Apache Struts Web Framework (CVE-2017-5638). They discovered that Equifax's online dispute portal was vulnerable and exploited this vulnerability to gain initial access to the network.

After gaining a foothold, the attackers installed a web shell on the online dispute portal server to establish persistence and enable further reconnaissance. Using the web shell, they were able to conduct reconnaissance activities, such as identifying databases containing personally identifiable information (PII) and obtaining valid credentials for these databases.

With valid credentials and knowledge of the network topology, the attackers queried the databases for PII using existing encrypted channels to blend in with normal network traffic. To evade data loss prevention (DLP) systems, they obfuscated the stolen PII before exfiltration.

The stolen data was then split into smaller compressed files for exfiltration. The attackers used a combination of techniques to hide their activities, including multi-hop proxies and the use of standard encrypted web protocols to disguise the data exfiltration as normal network traffic. In total, the attackers utilized approximately 34 servers located in nearly 20 countries to host their multi-hop proxy infrastructure.

After successfully exfiltrating the data, the attackers deleted the compressed files to cover their tracks. They also wiped log files on a daily basis to eliminate records of their activities.