wifi wall

Wireless Security Report

No.1 ▣ May 19, 2019

The next Cyber Attacks after APT

The next Cyber Attacks after APT

Recently we see an increasing number of Single Step Advance Attacks. In a Single Step Advance Attack, the Advance Attacker starts with all the necessary intelligence and privileges needed to access the target and achieves his goal by avoiding unnecessary or lateral movement. For example, by identifying the target and using previously obtained superuser privileges, the Attacker logs into the critical server dump the necessary data and send it out via one of the company's VPN servers. As a result, the attack duration is short, the damage is significant, and there are no traces left behind.

The Attack looks like a legitimate action of IT personnel. A post-attack investigation of the IT team finds they were not involved, and digital forensics do not find evidence of the attacker acts. The zillion event records we expect to see in the logging systems are missing. Even more, there is no evidence that someone deleted the event records and it looks like, event records were not created.

Usually, an ultra-damaging Cyber Attack is carried by APT (Advanced Persistent Threat) over a long period. The Attacker penetrates a machine inside the corporate network, performs orientation and investigation steps, to identify the landing place, the privilege level of the current user, and where can he move forward. In many following steps,

sometimes hundreds and even thousands, the Attacker pushed his malicious agent from station to station, harvesting higher privileges and finally achieving access to the specific server or assets he is looking of targeting. This process can take a few months and even a few years. Many of the most damaging and famous attacks are APT attacks.

As more APT detection and prevention system had been developed and deployed (including the fantastic illusive networks solution, which I was part of bringing it to the market, the Advance Cyber Attackers realize that the lateral movement inside the victim network exposes their acts. The longer they move inside the site and the more stations and servers they "touch" the detection probability increases.

Therefore they searched for a network "zone" that is entirely in the dark. A zone that no event logs exist and yet, the Attacker can harvest superuser privileges quickly and safely. They realized that those high profile IT personnel and corporate executives with superuser permissions travel and use their mobile stations (laptop and phone) from conferences, airports, hotels, etc.

These ultra busy executives need to retain connectivity when traveling and mostly needs a high-speed connection to do their tasks. The 3G/4G connection is not good enough for a video conference or downloading multi-gigabytes presentations via a VPN connection.

Conferences and Airports WiFi networks are the most dangerous networks. They host Rogue Access Points and Evil Twin Access Points that looks exactly like the official WiFi network. There are many publically available Rogue AP kits, that automatically duplicate the WiFi landing page and divert all URLs to a spoofed landing page: "Welcome to JFK WiFi". The only difference between the original splash screen and the spoofed one is malware or trojan horse embedded in the spoofed splash screen. This step is happening much before the VPN client is loaded, making it immune to VPN solutions.

Connecting to these WiFi networks leaves no audit trail and therefore will fail the post-attack investigation.

Attackers load these AP traps in public WiFi and wait. In average they harvest thousands of user's credential, many with high privileges. They know to which corporation network they connect and at any time later can log in and attack.
Recently, a major USA corporation suffered from a Single Step Advanced Attack. Initially, it looked like a senior IT team member logged in the most important server of the company, dump a highly confidential database and upload it encapsulated in encrypted data packets via one of the company VPN servers to an external server. When the Attack was found (a few months after) an investigation was launched. The immediate suspect was an IT team member, but a human investigation found him clear. The digital forensics

found nothing but a legitimate server login record, a connection to the company VPN and regular flow of encrypted data outside, and That was it.

An additional human investigation found that an IT member was called before catching a flight to help and diagnose a problem on the company servers. This superuser could not help before the flight and after landing was rushing to his car in public parking. Additional calls convinced him that the problem could not wait for him to return to the office, he opened his laptop and connected to the parking free WiFi. He was caught by a Rogue AP that hijack the connection, and before routing him to the internet, it captured his user name and password. These were the superuser credentials used later for the Single Step Advanced Attack.

WiFi attacks are becoming an easy step to obtain all the information necessary to carry a Single Step Advance Attack. It replaces the lateral movement inside the victim's network, saves time, and dramatically reduces the attacker exposure. It is shortening the attack time and makes it almost impossible to be detected.

WiFi networks become the Attacker preferred penetration option.