HARMONY IoT

Cyber Of Things

The Top 10

Wireless Threats Around Your Office

October 29th, 2019

By ORCHESTRA

1. Misconfigured APs

Corporate access points configured with weak encryption schemes, or host encrypted and unencrypted networks side by side pose a major security risk. Attackers can easily crack weak encryption schemes to retrieve the original Wi-Fi password using publicly available tools such as Aircrack-ng, or connect to an unencrypted network and exploit one of the many public vulnerabilities in wireless routers today (e.g. CVE-2019-15260) to gain full control over the access point and all data passing through it.

2. Rogue APs

A malicious insider, a bribed cleaning lady or just a clueless employee could connect an unauthorized access point to the corporate network. This unmanaged access point has none of the organization's security policies installed, and if it is not properly secured attackers could circumvent your corporate security and gain full access to your corporate network by connecting to that insecure access point.

3. Insecure Enterprise IoT

More and more devices are becoming "smart" and "connected". These devices are unmanaged and unmonitored by your IT and Security teams, but are connected to your corporate network. Many of these devices are open to wireless connections to allow for easy interactions such as printing documents or casting screens, but this behavior also makes them insecure bridges into your secured corporate network. Attackers can connect to your office printer or your smart TV and use it as a pivot to your corporate network, thus bypassing your corporate security, like the case of the Vegas casino database theft of late 2018.

4. Suspicious Devices

Wireless hackers use specialized wireless equipment to conduct their attacks and increase their chances for successful exploitation: from powerful external antennas such as the Alfa and Panda, to miniature easy-to-hide computers such as the Raspberry Pie and ESP32, to tactical wireless attack platforms or "dropboxes" such as the Hak5 Pineapple or the PwnieExpress Pwn Plug.

5. Insecure Connections

Since wireless attacks are probabilistic and require physical proximity to the target, attackers will look for the place with the biggest concentration of corporate devices to stage their attack. Those places are your headquarters and branches. That is why it is critical to ensure on-premise corporate devices connect only to corporate networks. Connections to external networks or mobile hotspots can circumvent corporate security policies and critical cyber-security defenses. Connections to public networks is even worse because it allows attackers to connect to these networks as well and exploit your corporate and employee devices, gain full control over them and then use them as a stepping stone to infiltrate the corporate network once they connect back.

6. Wireless Network Hacking

Attackers will try everything in their toolbox to try and get access to your corporate network. This includes trying to repeatedly guess your wireless password, using the power of the cloud to try and crack it, circumventing the password all together by brute-forcing the WPS pin code or even spoofing the MAC address to bypass whitelist access restrictions, all using publicly available tools such as Kismet, CloudCracker, Reaver and MacChanger respectively.

7. Man in the Middle Attacks

The most popular Wi-Fi attacks revolve around getting a victim device to connect to the attacker's network. Once that's done - it's game over for the victim: the attacker is now able to listen in on all communications performed by the victim and also inject new traffic such as malware infection. The easiest way to accomplish this is by faking an existing network used by the victim. This could be an exact clone of the network he is currently connected to or one he has connected to in the past. Once that's done, the attacker can jam his current connection and force him to connect to his malicious fake network. These attacks come in many varieties including the "Karma" attack, "Evil Twin" attack and the "Known Beacons" attack and can all be performed using open-source tools.

8. Remote Code Execution Attacks

The holy grail of all attacks - the ability to run any code remotely on a victim device. From laptops and smartphones to wearables and other IoT devices - they all have wireless chips inside of them, which allows them to connect to and host wireless networks. The firmware running on these chips can be vulnerable to zero-click wireless attacks, meaning all an attacker has to do is send a single packet out into the air (within range of the victim device), and once picked up it will exploit a vulnerability in the firmware which will allow the attacker to run any piece of code on the victim device - gaining full remote control over it. Recent examples of such vulnerabilities, with publicly available code, include the "Broadpwn", "Qualpwn" and Marvell vulnerabilities targeting the Broadcom, Qualcomm and Marvell Wi-Fi chips respectively, which together cover the vast majority of the Wi-Fi chips market share.

9. Surveillance Devices

Most surveillance devices today have moved away from using old-school radio transmissions or locally store the collected material, and now support Wi-Fi to stream the collected data in real time straight to the attacker's machine. Thanks to advances in computer technology these devices are now extremely small, require very little power and are laughably cheap. They are also available for purchase on-line and are delivered world-wide, making their use much more common, allowing attackers to easily leak sensitive data from within corporate facilities while completely bypassing all corporate network protections.

10. PCI Compliance

Not complying with key industry standards such as PCI can cause significant damage to an organization. Apart from the clear security threat, incompliance could result in financial penalties, legal actions and revenue loss. A major part of security standards such as PCI has to do with wireless technologies. Therefore, It is best to make sure you have systems in place to ensure the deployment and enforcement of these compliance policies.