**Technical Analysis of Evil Twin Wi-Fi Attacks with Captive Portals Using Airgeddon**

Vasile Mihai Glodici CS4

**Introduction**

As wireless networks become commonplace, attackers use their inherent vulnerabilities to compromise user data. Evil Twin Wi-Fi attacks, which include the creation of a fake access point (AP) that imitates a genuine one, constitute a serious network security risk. This article examines the technical aspects of conducting Evil Twin Wi-Fi attacks with Airgeddon, a versatile tool that automates the deployment of rogue APs and captive websites. Additionally, the report investigates various strategies to counteract these threats.

The PVI applies the Body of Knowledge topic Wi-Fi Security and Hacking, where Airgeddon is covered. I've chosen to investigate more alternatives and scripts before settling on the Captive Portal attack. This approach eliminated the time-consuming requirement of decrypting the hashed password, as clients entered the password in plain text.

**Main Question**

What is the technical process of conducting an Evil Twin Wi-Fi attack with a captive portal using Airgeddon, and how can users and organizations protect themselves from these attacks?

**Sub questions**

1. How does the Airgeddon tool simplify the deployment of malicious APs and captive portals?
2. Which wireless network flaws are exploited during an Evil Twin Wi-Fi attack?
3. How can users and organizations detect the presence of rogue APs within their network?
4. What are the most effective methods for defending wireless networks from Evil Twin Wi-Fi attacks?

**Time Allocation**

Initial Research, tool testing, vulnerability analysis, and report writing needed a total of 24 hours for this research report. The allocation of time is as follows:

1. Initial Investigation of PVI Choice: 3 hours
2. tool testing and vulnerability analysis: 9 hours
3. Troubleshooting: 5 hours
4. report writing: 7 hours.

**DOT Framework Usage**

The Design, Operate, and Transfer (DOT) framework will be used to analyse the phases of an Evil Twin Wi-Fi attack utilizing Airgeddon. This method gives a detailed description of the attack, including the design of the malicious AP, its operation, and the exfiltration of gathered data.

1. Design: entails the configuration of the malicious AP, the selection of target networks, the cloning of their settings, and the creation of a fake captive site.
2. Operate: by capturing user data via the rogue AP and exploiting captive portals to collect credentials and other sensitive information.
3. Transfer: The exfiltration of the gathered password to a remote server or storage location

**Demo**

\*Video demonstration is attached\*

https://youtu.be/4G22bh986r8

Several technical steps are required in executing an Evil Twin Wi-Fi attack with Airgeddon:

1. Connect to the attacker's machine two wireless adapters capable of monitor mode and packet injection.
2. Scan for surrounding wireless networks with Airgeddon and select a network to clone.
3. Enable monitor mode on one of the wireless adapters and utilize Airgeddon to collect the WPA/WPA2 handshake from the target network. This is required in order to create a rogue AP with same encryption settings.
4. Configure the second wireless adapter to emulate the target network's SSID, encryption, and settings to construct a rogue AP.
5. Construct a fake captive portal that resembles the target network's login screen to deceive people into entering their credentials.
6. Operate the rogue AP and captive portal, capturing user credentials and data as users login.
7. Transfer the acquired information to a remote server or storage location for further analysis or malicious usage.

**Setup**

1. The first target computer is a virtual machine running Ubuntu 20.04 with a third network adapter attached.
2. The second and third target machines are an iOS device and an Android phone to demonstrate the versatility of the attack across different operation systems.
3. The target Wi-Fi access point is my personal 2.4GHz mobile hotspot.

**Some Errors encountered and fixes:**

VirtualBox was initially utilized but was later replaced with VMWare because my Wi-Fi USBs were not being detected/cloned reliably.

Unrecognized Wi-Fi sticks are solved by plugging them in after machine startup and driver update.

Because the previous script's use of "Fluxion" rendered the hardware unidentifiable, snapshots were utilized to return to previously functioning system states.

**Answers to Main Question and Subquestions:**

1. Airgeddon automates steps of the process of constructing rogue APs and captive portals, therefore making it more efficient and user-friendly for attackers. steps taken using the Airgeddon script are:
   * Automated scanning of surrounding wireless networks for target network identification using the Aircrack-ng suite
   * Capturing WPA/WPA2 handshakes to clone the encryption settings of the target network.
   * Creation of rogue APs with cloned SSIDs, encryption, and settings.
   * Creation of rogue APs with cloned SSIDs, encryption, and settings.
   * Deauthenticating users from original AP.
   * Hosting a fake captive portal that prompts for the login of the target network.
2. During an Evil Twin Wi-Fi attack employing Airgeddon, the tool targets the following vulnerabilities in wireless networks:
   * Weak, easily duplicated or cracked encryption protocols (e.g., WEP, WPA and WPA2)
   * Insufficient awareness, which causes users to connect to rogue APs and provide credentials to captive portals.
3. Users and organizations can identify rogue APs and captive sites established by Airgeddon using the following strategies:
   * Employ network monitoring technologies such as WIPS or IDS to detect unwanted access points.
   * Train users to identify phishing and social engineering techniques used by captive portals.
   * Train users to identify phishing and social engineering techniques used by captive portals.
4. Solutions to reduce the threats presented by Wi-Fi attacks utilizing Airgeddon by Evil Twins include:
   * Deploying a wireless honeypot to divert attackers and collect intelligence on their approaches.
   * Conducting regular security audits and penetration tests to discover and address any network vulnerabilities.
   * Developing a thorough security awareness program that emphasizes the dangers of connecting to untrusted networks and how to recognize potential Evil Twin WiFi attacks.

**Conclusion**

Airgeddon enables Evil Twin Wi-Fi attacks with captive portals by exploiting wireless network vulnerabilities in order to social engineer users and collect sensitive information. By adopting the DOT architecture and understanding each phase of an attack, individuals and organizations may limit risk and defend networks effectively. These options include implementing strong encryption (e.g., WPA3), altering default configurations, updating firmware, and educating users on the potential threats posed by malicious Access Points.