Wi-Fi Hacking via Drones

Executive Summary:

Drones were invented to render support to military operations. Constant innovation and development have made drone technology more efficient and affordable. As a result, drones are now available for commercial and personal purposes.

Drones are now capable of flying for several hours with multiple pounds of payload fitted with high-definition cameras and other electronic devices. It is being used as an aerial photography tool for photographers, cinematographers, often for entertainment purposes as an aerial projector or light show tool. It is even enabling rescue operations in areas affected by natural calamities.

As per FAA's 2018 - 2038 Airspace Forecast, the number of drones in the USA are expected to rise from 1.1 million to over 2.4 million units in 2022. Being easily available and affordable, drones have become an efficient tool for corporate espionage. Threatening payloads on drones including IoT hacking devices, microphones and spying cameras could breach the security of an organization.

Wi-Fi Networks Are Not Secure

In today's era of cybersecurity, where data protection has become the foremost priority, drone-based attacks have become a treacherous threat for enterprises' Wi-Fi setups.

Business Wi-Fi network setup is considered relatively simple and rudimentary. However, this could also mean that an organisation may choose to set up their devices heedlessly and consequently risk their data to insecure networks. It has been recognized that there are existing vulnerabilities in Wi-Fi security protocols and hardware elements that are released by manufacturers. These include poorly secured administrator access and vulnerable services.

The default configuration of connected devices, factory default passwords, and weak encryption are among some of the most notorious factors that have contributed to attacks not only to the ecosystem of the internet of things (IoT) but also to networks in general.

Moreover, Wireless networks can be viewed as inherently insecure, potentially paying for unauthorized access by strangers, who could pry into transmitted data. While various security protocols have been developed to protect wireless networks the best practice still followed by most of the reputed organizations works the best – this involves limiting their wifi range within the premises of the workplace, thus making it difficult for the attackers to hack a network which is beyond their reach.

Wi-Fi Hacking Drone

The following demonstration shows how an attacker develops and carries the complete network penetration assembly to its victim network range through a quadcopter/Drone, executes malicious scripts and tools on the targeted network and hacks into its wifi, thus, entering its intranet to perform further attacks.

Equipments Used

DJI Phantom 3 Quadcopter | Raspberry Pi 3 | Alfa AWUSO36NH Network Adaptor | Battery Hat | Laptop with Kali Linux | 4G Smartphone

Drone Setup

Raspberry Pi with Kali Linux is mounted on the drone. The Alfa Network adaptor is connected to the USB port of raspberry Pi and attached to the drone's body. A Battery HAT is used to supply 5V, 2A power to Raspberry Pi.

Laptop Setup

A Laptop with Kali Linux OS is the primary machine to execute the attack.

Setting up a Local Network

A 4G smartphone with high speed internet is trained to create a local network through its Hotspot letting the RaspberryPi and Laptop connect to its Wi-Fi hotspot.

Connecting with Raspberry Pi

"Putty" tool is used to create an SSH connection between Raspberry Pi (Drone) and the laptop. Thereby getting access to the R-Pi terminal remotely.

Flight

The drone takes off and lands on the roof or any other blind spot of the target organization.

The Attack

The Attacker runs a Linux based wifi hacking tool "Fluxion" on the terminal of R-Pi through its laptop. Inside, Fluxion attacker selects the network adapter to be utilized for the attack. After selecting Alfa Network adaptor, it displays the list of Wi-Fi signals the network adaptor is currently able to scan. The attacker now selects the Wi-Fi to be hacked. Fluxion will de-authenticate all connected users of the network and capture the Wi-Fi handshake and save it. Flexion now allows the attacker to select a phishing page to be displayed to all the users. Moving ahead, Fluxion prevents the user from reconnecting to the original Access Point and makes a rogue Access Point with the same name as the targeted AP.

The Innocent user at this point will experience no internet connection on the current AP. Moreover, it would also fail at reconnecting to the network. Crippled by failure, clueless users will observe that another Wifi network having the exact same name is showing up under current Wi-Fi networks. The confused user will try to connect to the other rogue Wi-Fi by entering the password/key in its Wi-Fi sign-up phishing page, hoping to reconnect to the lost network.

Fluxion will now compare the key with the captured handshake to check its authenticity. Once the key is verified, the attack is deemed concluded, and the original Wi-Fi is released for other users.

Once the adversary gets the key, it can now assume the role of an insider within intranet and perform further critical attacks compromising organisation's network security.

Conclusion

Some of the most common wireless network attacks are opportunistic in nature. Businesses that fail to secure their Wi-Fi networks leave the door wide open to scammers and hackers who would otherwise look for easier targets. Scammers are happy to take advantage of poor security controls to steal sensitive information from Wi-Fi users and distribute malware. Unsecured Wi-Fi networks are also targeted by sophisticated cybercriminals and organized crime groups to gain a foothold in the network. The attacks can be extremely lucrative.

In one of the easiest ways, the attacker can simply create a hotspot on a smartphone and pair it with a tablet or laptop. The hacker can then easily monitor the traffic of everyone that connects.

Alternatively they can use a router with the same name and password as the one currently in use. This may also have a stronger Wi-Fi signal, which may see more people connect to it but it is an "evil twin" through which man in the middle attacks occur – the interception of data sent over the network. This is one of the most common wireless network attacks and it is surprisingly effective. One study indicated that more than a third of Wi-Fi hotspot users take no precautions when accessing Wi-Fi hotspots and frequently connect to networks that are not secure.

To avoid intrusion of Wi-Fi hacking drones, enterprises need to have a capable security system in place to detect and locate drones and track flight paths accurately. Organizations can leverage video detection technology to monitor the entry of unauthorized drone flights in office campus airspace. Security teams need to constantly monitor high quality live video feeds to prevent drone attacks.

About QA InfoTech

At QA InfoTech we specialize in providing independent software testing and unbiased software quality assurance services to product companies, ranging from the Fortune 500 to start-ups. Established in 2003, with less than five testing experts, QA InfoTech has grown leaps and bounds with its Four QA Centers of Excellence globally; located in the hub of IT activity in India in Noida and Bangalore and our affiliate QA InfoTech Inc. in Michigan and Bentonville, USA.

- 1400+ QA engineers and domain experts
- An ISO 9001:2015, CMMi Level 3, ISO 20000-1:2011 and ISO 27001:2013 compliant company
- Thought Leaders in E2E testing, specifically in Test Automation, Performance Testing, Localization and Accessibility Testing

In 2017, QA InfoTech has been ranked in the top 100 places to work for in India. We are amongst the top 50 Best IT & ITeS Companies To Work For in 2012, 2014, 2015 & 16 in India. For more details, please refer to our blog on this event.

"We assure the highest degree of Excellence and Accuracy in our engagements. Once you have placed your trust with us, rest assured we guarantee an elated peace of mind"

Michigan, USA
32985 Hamilton Court East, Suite 121,
Farmington Hills, MI 48334 U.S.A

Noida, INDIA (HQ)
A-8, Sector 68 Noida, U.P, 201309,
India

USA Phone Number: +1-469-759-7848, +1-248-246-1109

Arkansas, USA
Rain Tree Business Center, 900B South Walton Blvd, Suite 1, Bentonville, Arkansas, 72712, U.S.A

Bengaluru, INDIA
CoWrks, RMZ Ecoworld, Outer Ring Road, Bellandur, Bengaluru, Karnataka 560103, India

For More Details:
Contact Us: info@qainfotech.com || Visit Us: www.qainfotech.com