DEFINITION

evil twin attack

Katie Terrell Hanna

What is an evil twin attack?

An evil twin attack is a rogue Wi-Fi access point (AP) that masquerades as a legitimate one, enabling an attacker to gain access to sensitive information without the end user's knowledge. An attacker can easily create an evil twin with a smartphone or other internet-capable device and some easily available software.

How does an evil twin attack work?

Attackers position themselves near a legitimate Wi-Fi network and lets their device discover what service set identifier and radio frequency the legitimate AP uses. They then send out their own radio signal, using the same name as the legitimate AP.

To the end user, the evil twin AP looks like a hotspot with a strong signal.

That's because attackers have not only used the same network name and settings as the "good twin" they are impersonating, but they have also physically positioned themselves near the end user so that the signal is likely to be the strongest within range.

If the end user is tempted by the strong signal and connects manually to the evil twin to access the internet or if the end user's computer automatically chooses the fake AP because it is running in promiscuous mode, the evil twin becomes the end user's wireless AP.

types of malware

Evil twins masquerade as legitimate access points to lure victims so attackers can unleash malware to steal sensitive data, like credit card numbers and login credentials.

This gives the attacker the ability to eavesdrop or intercept sensitive data, such as login credentials, bank account details or credit card information.

This type of attack employs similar protocols to phishing scams, which involve luring users to a fraudulent website with malware waiting to invade their systems.

How to protect your device from evil twins

Evil twin Wi-Fi APs are not a new phenomenon in wireless transmission. Historically, these captive portals have been used by hackers as base station clones or honeypots.

They have also been used by network security professionals to conduct penetration tests with tools such as a Wi-Fi Pineapple.

What is a Honeypot (Cybersecurity)? Hon…

What's different now is that more businesses and consumers are using wireless devices in public places, and it's easier than ever for someone who doesn't have any technical expertise to create an evil twin.

To avoid evil twin attacks through fake Wi-Fi networks, end users should only use public Wi-Fi networks for web browsing and refrain from visiting any sites that require you to reveal sensitive information.

To provide an added layer of cybersecurity for corporate data, employees who use free Wi-Fi hotspots to gain internet access -- for example, at a coffee shop -- should always connect to the internet through a virtual private network.

wi-fi security cheat sheet

Learn differences among Wired Equivalent Privacy, Wi-Fi Protected Access, WPA2 and WPA3 wireless security protocols, and find out if WPA2 can be upgraded to WPA3. See how to defend against the most common wireless network attacks and the importance of staying up to date with Wi-Fi training.

This was last updated in December 2021

Continue Reading About evil twin attack

- Enterprises mull 5G vs. Wi-Fi security with private networks
- 11 common wireless security risks you don't have to take
- Why WPA2-PSK can be a security risk even with an uncracked key
- New WPA3 security protocol simplifies logins, secures IoT
- How to secure your home Wi-Fi network in 7 steps

Related Terms

hypervisor security

Hypervisor security is the process of ensuring the hypervisor -- the software that enables virtualization -- is secure throughout... See complete definition

juice jacking

Juice jacking is a security exploit in which an infected USB charging station is used to compromise devices that connect to it. See complete definition

phishing

Phishing is a fraudulent practice in which an attacker masquerades as a reputable entity or person in an email or other form of ... See complete definition

Dig Deeper on Threats and vulnerabilities

12 types of wireless network attacks and how to prevent them

By: Karen Scarfone

Wireless security: WEP, WPA, WPA2 and WPA3 differences

By: Alissa Irei

WLAN security: Best practices for wireless network security

By: Andrew Froehlich

Wireless access point vs. router: What's the difference?

By: Alissa Irei

NETWORKING CIO ENTERPRISE DESKTOP CLOUD COMPUTING COMPUTER WEEKLY

Networking

Cisco acquires Accedian for Network Assurance portfolio

Cisco expects Accedian to bolster its Network Assurance portfolio for service providers. The product line provides network ...

Evaluate top 5G fixed wireless access benefits

Fixed wireless access, when enabled by 5G, makes wireless network connectivity accessible to users at affordable rates. Learn the...