What is a Wi-Fi-Pineapple?

Have you been a victim a Bad-Karma attack or Man-in-the-Middle Attack, or an evil-twin attack? Maybe you have and don’t know it. With the rise of new technologies in penetration testing you should know how to find out if you have been a victim and how to avoid the perils of cyber snoops. This will be a brief look into one of the newer tools being used, and how to mitigate possible attacks

There only seems to be one true way anyone can defeat it and that’s by not letting it attach to your network via hardline or over Wi-Fi (WPA2-Enterprise or WPA2 Personal (CCMP-AES) with a strong passphrase)… the key thing doesn't give it access. Pineapples love open Wi-Fi -Hotspots like Coffee Shops and Hotels, remember nothing in life is free, basically anywhere easy access can be had with little authentication where bad Karma can be unleashed upon the unexpecting public

KARMA attacks are really based towards a user’s device the “client”. The users device is looking at an SSID and its last known good network was "SCC", which has been cloned to look real and even though the real network “SCC” most likely uses WPA2-Enterprise w/Radius authentication it sends that SSID in the Probe Request message to any AP (and other known networks as well that it has attached to looking to exploit), and the Pineapple is placed somewhere in the network, the rogue AP sees this, and updates the SSID list to be that SSID "SCC" the client sees this, and does the initial association, the authentication sequences for WPA2/WPA2 Enterprise, are never started collecting the information.

So how does one beat this?

Well, something that does help is keeping your client up to date - newer devices don't send out the SSID in the probe request message, it just sends out a broadcast SSID, and then it picks and chooses the appropriate one. if the known good AP is a member of a well-built security network (WPA2 PSK/Enterprise), you’re a little safer but this is typically not the case for most. If your equipment is one on the higher end and of better quality and you have setting that has been tightened up, you’ll have a chance setting up layer of security that can help you out with this, but generally the client management by Windows Mac, Android, iOS, and Linux don't require authentication to be enabled even on known networks.

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. <http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html>

Radius servers and clients, aren’t going to fix/solve a Pineapple Karma attack on its own, but it can keep a pineapple off the wireline controlled by the Radius server, but remember the pineapple doesn't need to be there, it all depends on what the pineapple operator wants to do with the ill-gotten information. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&sqi=2&ved=0ahUKEwjD7f_S2P7RAhVGwVQKHXvWB3MQFgguMAI&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FRADIUS&usg=AFQjCNE3nnh7hcq2HmwhiSyMbfN1cPicpg&sig2=9to5yCszvfJk6-k4yz8sfg&bvm=bv.146094739,d.cGw>

UTM's can help in areas controlled by the network operator to keep rogues off the LAN, and they can also detect and mitigate to some degree a pineapple in the area - I've seen one case where the UTM did detect the rogue AP, and started knocking clients off it by sending de-authentication frames at the pineapple.

General protection measures are recommended

1. keep your software up to date - since the network isn't going to screen spyware for you, make sure your defenses are good.
2. have virus scanning and a personal firewall if you are concerned about your data and your system's integrity
3. when using a work computer, use any VPN client you are given - it never hurts to use it even for default browsing, as it means your traffic will be routed through the network and some level of privacy is being applied.
4. don't do unsecured transactions of sensitive data - always make sure HTTPS or SSL is on when you're sending a credit card, personal info, or other information you want kept private.

So how can I be safe?

* 1. Don't use open Wi-Fi in public areas, or use it very sparingly
  2. If one must, then VPN is an absolute necessity, even if only PPTP - VPN operates at a higher layer than a Pineapple does, so even if your client is (owned/pwned), the VPN will keep the upper layer of the network protocol traffic safe.
  3. SSL verification - a bit of work, but keeping your browser current, and having only trusted SSL certs in your keychain can help - but SSLstrip can defeat this
  4. Use a browser that supports HSTS, meaning that it'll first use HTTPS before falling back to HTTP - most modern browsers do this - Chrome, Safari, Firefox
  5. Turn off wireless auto-connect in the properties so that you are asked to connect each time (but remember, when you want more security you’ll give up convenience)
  6. At home use ARP –a to find your devices to your router Look for a mac address, if the address is different then what you’re connected to, then you may have been attacked especially if there are duplicated SSID listed.

Darren Kitchen who created Wi-Fi Pineapple, SxS2012 aggressively touted this hacking tool. While Kitchen maintained that he sells his project mainly to security professionals, most reputable professionals have plenty of other ways to conduct valid security audits. There are many free products on the Internet that are specifically made for security professionals that do a much better job for legitimate needs of managing Wi-Fi networks. So who exactly is buying Wi-Fi Pineapple? As Kitchen’s marketing seems to target novice hackers instead of security professionals, one has to wonder. At the very least, Wi-Fi Pineapple is a good reminder that you should always protect your communications in Wi-Fi hotspots using a virtual private network like Private Wi-Fi, or else you could be Wi-Fi Pineapple’s Bad Karma victim.