How to Defeat a WIFI Pineapple

usenix white paper |

Saving yourself from pineapple wifi attacks

eli brown, jess allen, george greer

**ITC 134 2017**

How to defeat a wi-fi Pineapple

Eli Brown, Jess Allen, George Greer

Seattle Central College



DEFCON 22 PREVIEW: Pineapple Abduction

<https://www.youtube.com/watch?v=9tl-ktPtPKI>

[](https://www.youtube.com/watch?v=9tl-ktPtPKI)

ABSTRACT

Presented to you in this white paper is a description of what a WiFi pineapple is and a how-to for making sure you defend yourself against pineapples.

in this paper, you will learn basic, proper techniques to ensure you don’t unknowingly connect to the WiFi through a pineapple.

Introduction

A WIFI Pineapple Mark V, as it is formally known, is a small, hand-held device that when initial set-up has been performed, can act as a middle-man to an unsuspecting user and the resources they are accessing on the web without them ever knowing.

The Pineapple device uses an attack method known as Karma. Karma works by masking the known WiFi network that a user may have stored in their computer (ie. “Airport Free Wi-Fi”). The user has stored the authentication details of the airport they frequent for easy access when they need to check their email before their flight. The Pineapple device will mask as the network so the user, in actuality, without them knowing, has connected to the known WiFi network through the Pineapple device. Pineapple can now read all the information the user is accessing while using the WiFi network.

Darren Kitchen, the creator of this device, hoped that this would appeal to an initial audience of novice hackers, as his marketing schemes tend to target. However, his main buyers are security professionals. There are many other tools, a lot that are free, available to these professionals so the actual recipients of the Pineapple Mark V are unknown.

Research

WiFi Pineapple works by cloning an active WiFi connection, and “bumping” itself to the top of the list to be the first connected to by the client.

There are certain measures a network operator can take in order to ensure network security is exacted upon their users.

* Ensure you have the highest level of security options set in your internet settings.
* Set up a Remote Authentication Dial-In User Service (RADIUS), which helps by providing a centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use network services.

NOTE: This method works only with Dial Up modems, which are becoming more and more rare

* Universal Threat Management (UTM) is another way to help through controlling the rogue networks from gaining access to the LAN. They are also capable of detecting a pineapple in the area. There have been numerous cases of the UTM finding rogue Pineapples, and kicking users off the network by sending de-authentication frames at the pineapple.

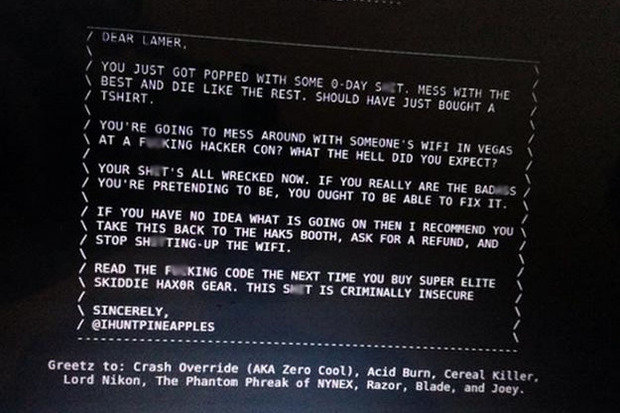
In order to properly protect yourself from this type of attack, you should consider these security measures:

* Keep your software up to date. Most networks won’t screen spyware for you, make sure you are properly protected
* Use anti-virus software and set up a personal firewall.
* On work computers, use the VPN client you are given. Anything you do on that computer will be routed through your employer’s server.
* Make sure any transaction of sensitive data is secure by checking that HTTPS or SSL is on.
* Turn off wireless auto-connect so that you are asked to connect each time.
* At home use an Address Resolution Protocol (ARP). An ARP is used to map MAC address to their respective IPs.
* In public, be sure to not use any insecure (non-password protected) networks unless there are proper security measures taken on your personal machine (ie. Use a VPN, SSL Verification, and use a browser that supports HSTS- meaning it will use HTTPS before it will use HTTP)

Conclusion

Based on the knowledge we have gained through researching the best methods for protecting ourselves from unwanted connections, the most effective thing you can do is always re-authenticate your open internet connections. If you happen to find two versions of a network, one that is password protected, and one that is not, never chose the open connection.

Most places you go these days will have a WiFi password displayed. Always trust the “Secure Network”.



# Bibliography

Authors, M. (n.d.). *RADIUS*. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/RADIUS

*How Does RADIUS Work?* (n.d.). Retrieved from CISCO: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

Team, W. P. (n.d.). *WiFi Pineapple Wiki*. Retrieved from github.com: https://WiFipineapple.github.io/WiFipineapple-wiki/#!index.md