WiFi Pineapple

Hak5.org - $99

WiFi Pineapple Mark V
WiFi Pineapple

- Dual removable antennas.
- Support for USB mobile broadband modems.

Pro Kit:
- Battery power for long-term placement.
- Weatherized storage.
WiFi Pineapple

- Enhanceable through “infusions”, community written modules. Also expandable with external storage and modules.

- The WiFi Pineapple does many things, but what we’re interested in is Karma.
Basics:

● The device in your pocket looks for networks. It’s doing it right now. It’s not finding those networks, so it will try again in a little while.

● Depending on device settings, it might automatically connect if it finds a network.
That device is essentially saying “Hello? ‘ATTwifi’, are you there?” “Hello? ‘Linksys’, are you there?”, “Hello? ‘It burns when IP’, are you there?” and so on.

We will show you more towards the end of this presentation.
...now for the fun part!

Karma says, “Yes! I’m that network you’re looking for!” and voila, the device is now connecting to the device/machine running Karma.
Karma

Why This Is Bad:

- Attacker can intercept all of your wireless traffic.
- Could be changing web pages, capturing your banking credentials, etc.
- ...however, Karma (normally) only works on open networks.
Karma

Considerations:

● The attack doesn’t have to take place anywhere near the SSID.

● In fact, it’s easier if it’s somewhere else.

● For example: a coffee house or airport.
Pineapple Demo

Pineapples are yummy!
Do you need a Pineapple? No, but they are cool!

The Pineapple code is completely open-source. That said, you don’t need it to use Karma or the other Pineapple attacks.
Pentoo + HostAPd-Karma

- Pentoo, a Gentoo Linux-based distribution for penetration testing, has a pre-patched version of HostAPd with Karma built in.
- Two new command line flags: -R and -A:
  - -R activates Karma.
  - -A logs the connection attempts.
LootBooty

- Released by PuNk1nPo0p at DEFCON 21.

- Just a small patch to FreeRADIUS!

- Allows acquisition of cleartext passwords from vulnerable devices.
LootBooty

How It Works:

● Creates a rogue access point with a certain SSID.

● When a device in range tries to connect, LootBooty jumps in and says, “Talk to me! I’m totally ‘SuperSecureCorporateWiFi!’”
How It Works, Cont’d:

- During authentication, LootBooty says, “I don’t understand your encryption. Use EAP-GTC instead. I need your password in cleartext.”
- ...a vulnerable device will say, “Okay!”
- LootBooty will then log that password.
What’s EAP-GTC?

- Extensible Authentication Protocol - Generic Token Card.
- Designed by Cisco for generic authentication using a one time password.
- Unfortunately, vulnerable devices allow fallback to this protocol.
eap_rlm_mschapv2.c:

PW_MSCHAP2_SUCCESS);

data->code = PW_EAP_MSCHAPV2_SUCCESS;

} else if (inst->send_error) {
    pairmove2(&response, &handler->request->reply->vps,
    PW_MSCHAP_ERROR);
    data->code = PW_EAP_MSCHAPV2_FAILURE;
} else if (rcode == RLM_MODULE_FAIL) {
    pairmove2(&response, &handler->request->reply->vps,
    PW_MSCHAP2_SUCCESS);
    data->code = PW_EAP_MSCHAPV2_SUCCESS;
} else {
    eap_ds->request->code = PW_EAP_MSCHAPV2_SUCCESS;
    return 1;
}

rlm_pap.c:

fail:

RDEBUG("No password configured for the user. Cannot
do authentication");

return RLM_MODULE_FAIL;

+ return RLM_MODULE_OK;

} else {
    vp = NULL;

...that’s it!
Vulnerable versions of Android:

- Depends on the carrier/manufacturer’s code, specifically the wireless supplicant.

- Anthony’s Verizon Samsung Galaxy SIII, running Android 4.3 *is* vulnerable. …but it *wasn’t* before the last update!
Vulnerable versions of iOS:

- 6, 7, at least. Likely older versions, too.

- Prompts on invalid certificates.

- Easy enough to bypass with a valid cert: it doesn’t matter whose it is!
Vulnerable Desktop OSes:

- Windows doesn’t implement EAP-GTC. (Add-on supplicants might be vulnerable.)
- OS X prompts on invalid certs, but will connect if the user accepts anyway.
- Linux, like Android, will depend on which wireless supplicant is used.
Why This Is Bad:

- Is your wireless network password your Active Directory password?
- What else is it used for? Payroll info, maybe?
- How extensive is your organization’s Single Sign On structure?
LootBooty

Demo time!
An enterprising hacker just might combine these attacks.

The end result? A rogue access point that answers WPA2 Enterprise connection requests from any SSID and captures credentials in cleartext.
How We Did It:

- Modified HostAPd-Karma to answer WPA2 Enterprise requests.
- The patched FreeRADIUS from LootBooty still downgrades to EAP-GTC and captures passwords.
- With some work, we’d just need HostAPd.
KarmaBooty

- Demo? We can’t...

- We don’t have a way to limit the area of effect on the attack.
How Do We Stop This?

For Device Manufacturers:

- EAP-GTC shouldn’t be a fallback.
- Only use EAP-GTC when specifically requested.
- Ideally, require authentication every time a device connects to the network. This would really, really annoy people, though.
For Network Administrators:

- Use EAP-TLS!
- Yes, this means that everyone needs certificates. (But you could self-sign.)
- Wireless network passwords shouldn’t be the same as Active Directory passwords. (No Single Sign On. It’s a bad idea.)
For End Users:

- Don’t auto-connect to wireless networks. (Yes, it’s annoying, but it might just save your password!)

- Don’t click past certificate verification boxes. **Read them!**
Fixing It Boils Down To...

CERTS!
Questions?

No WiFis were harmed in the making of this production.

Questions later?
abolan at unomaha dot edu
ccox at unomaha dot edu