IBM Security

IBM Security

Inside the Mind of a Hacker

IBM X-Force Command

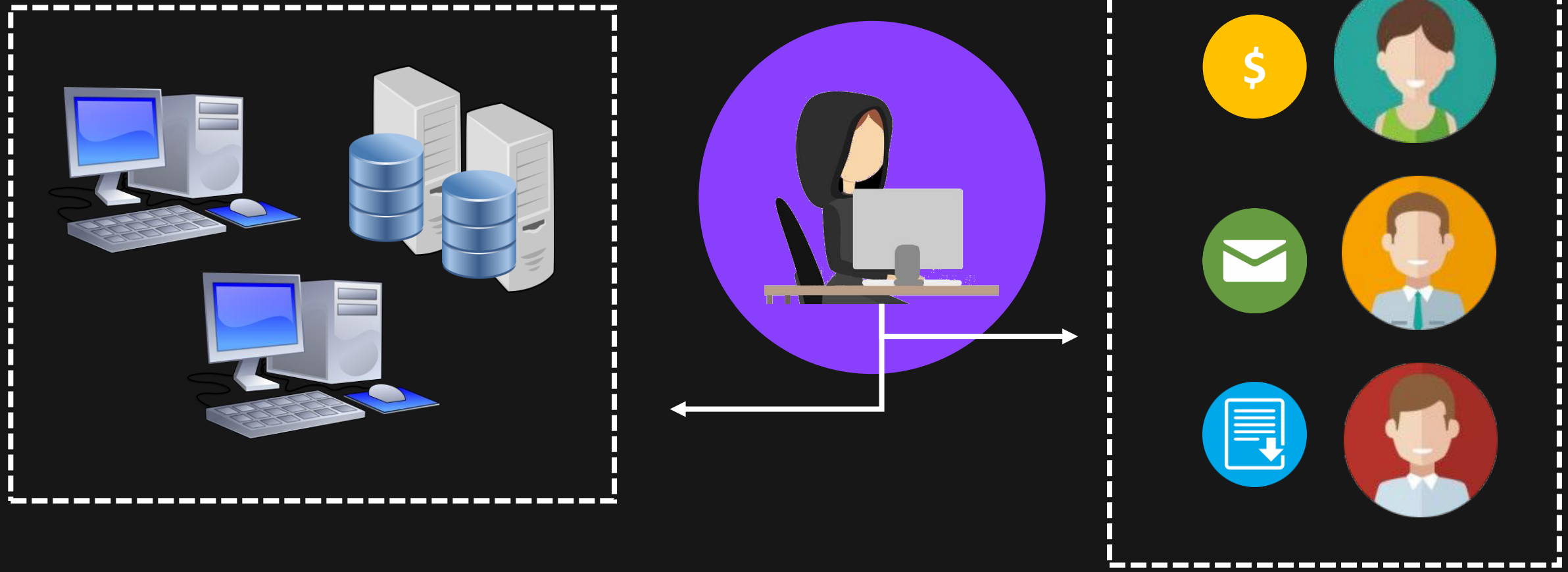
@HayleyBCohen

Executive Security Advisor
X-Force Command
IBM Security

IBM

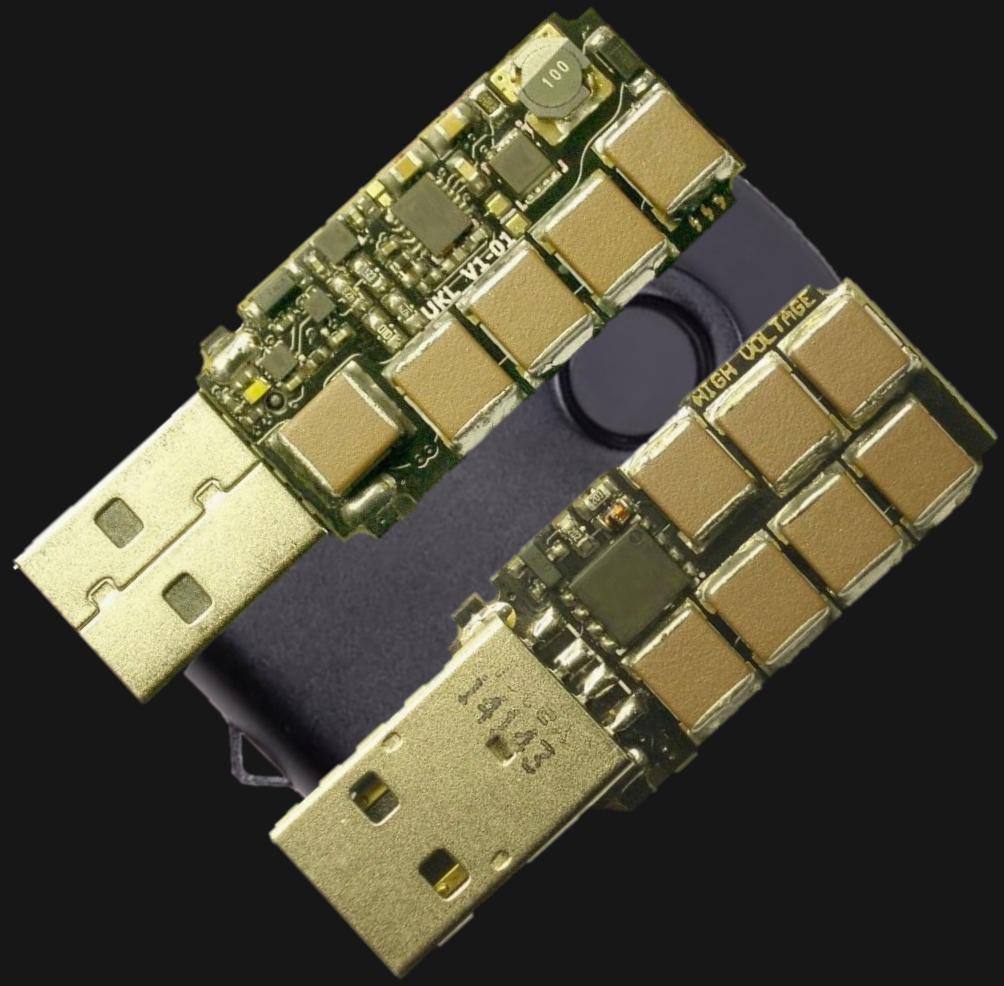
Who We Target

“Defenders don’t focus on people, attackers do”



Malicious USBs

Rubber Ducky

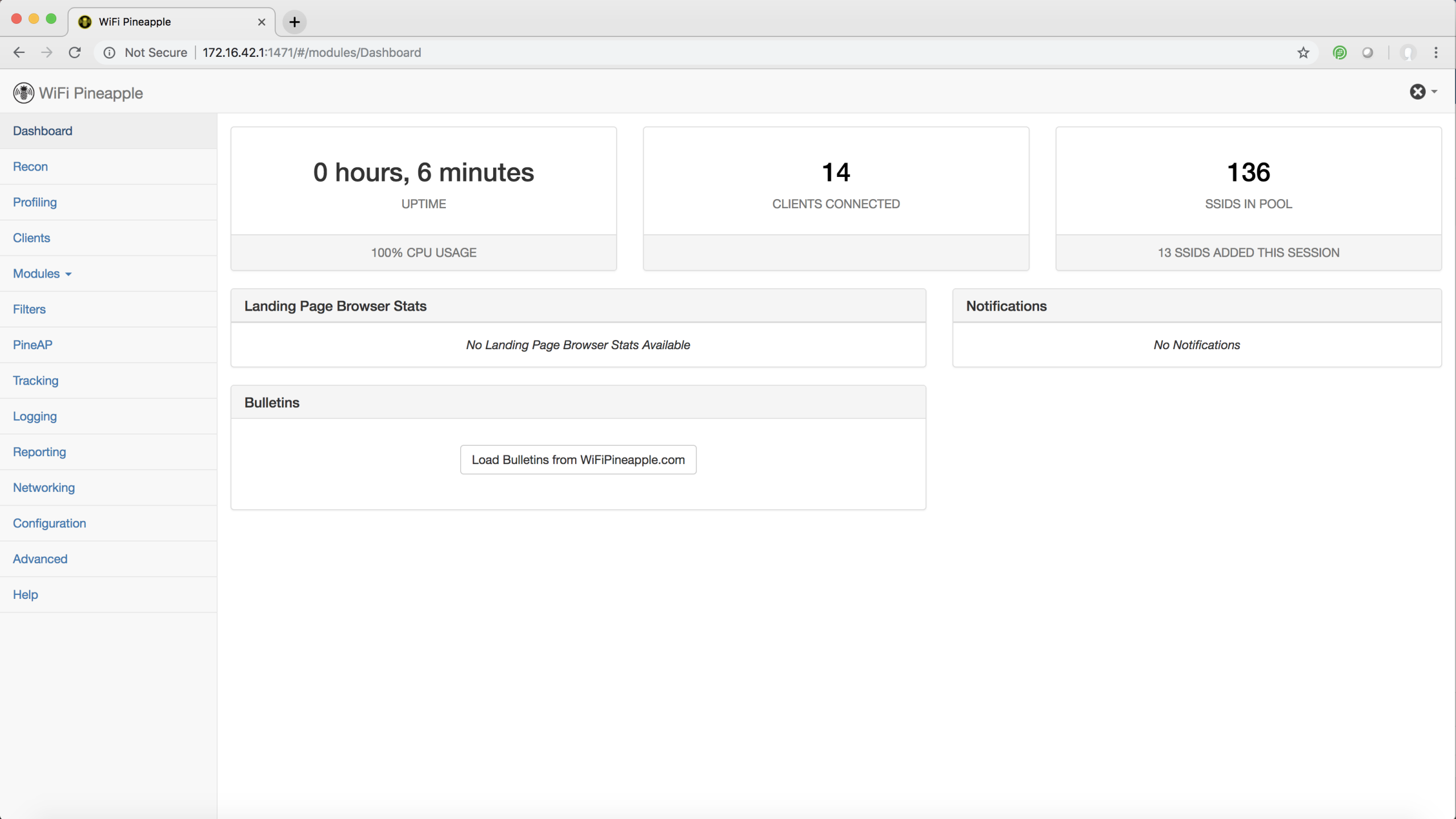


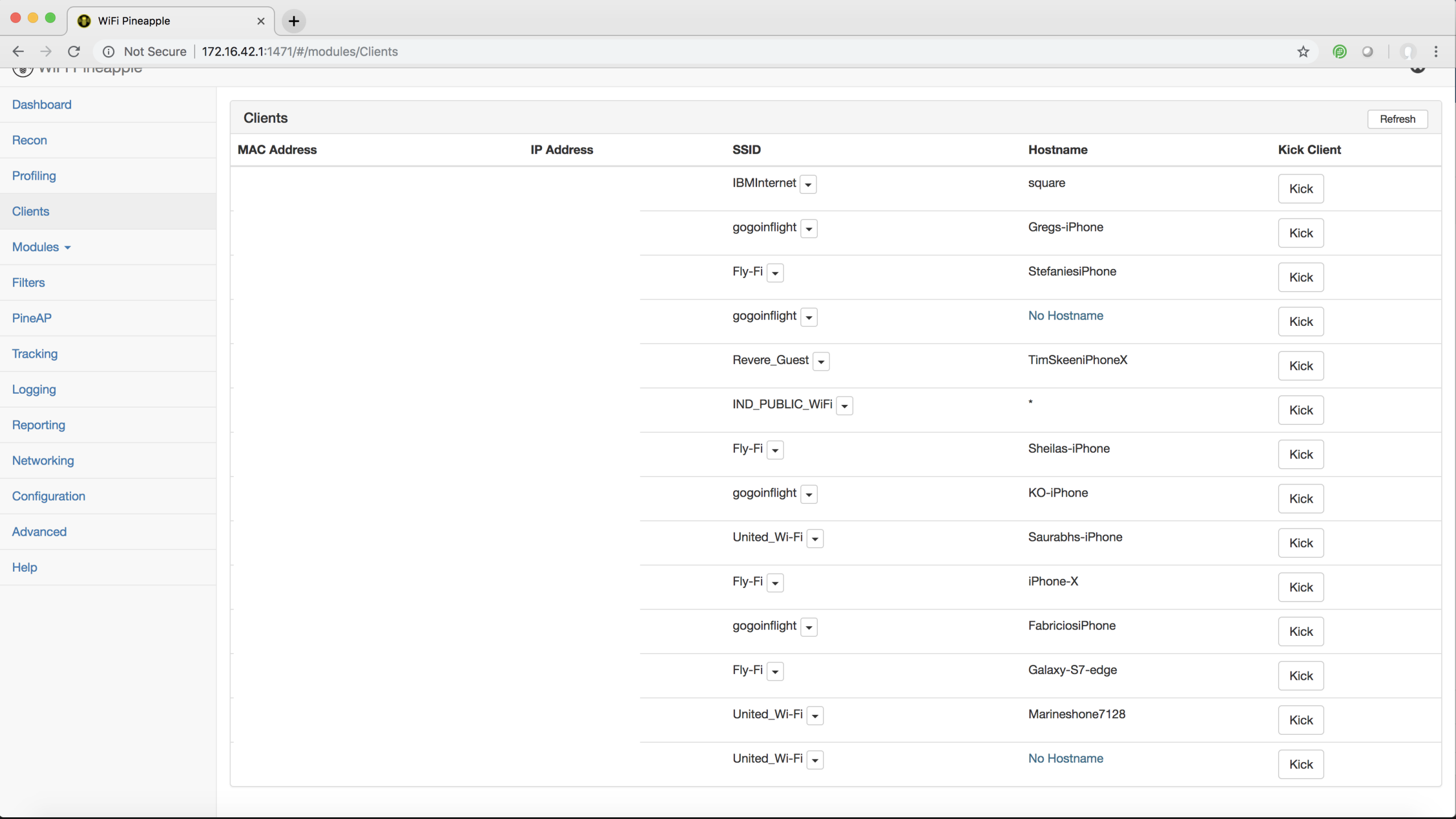
USB Kill

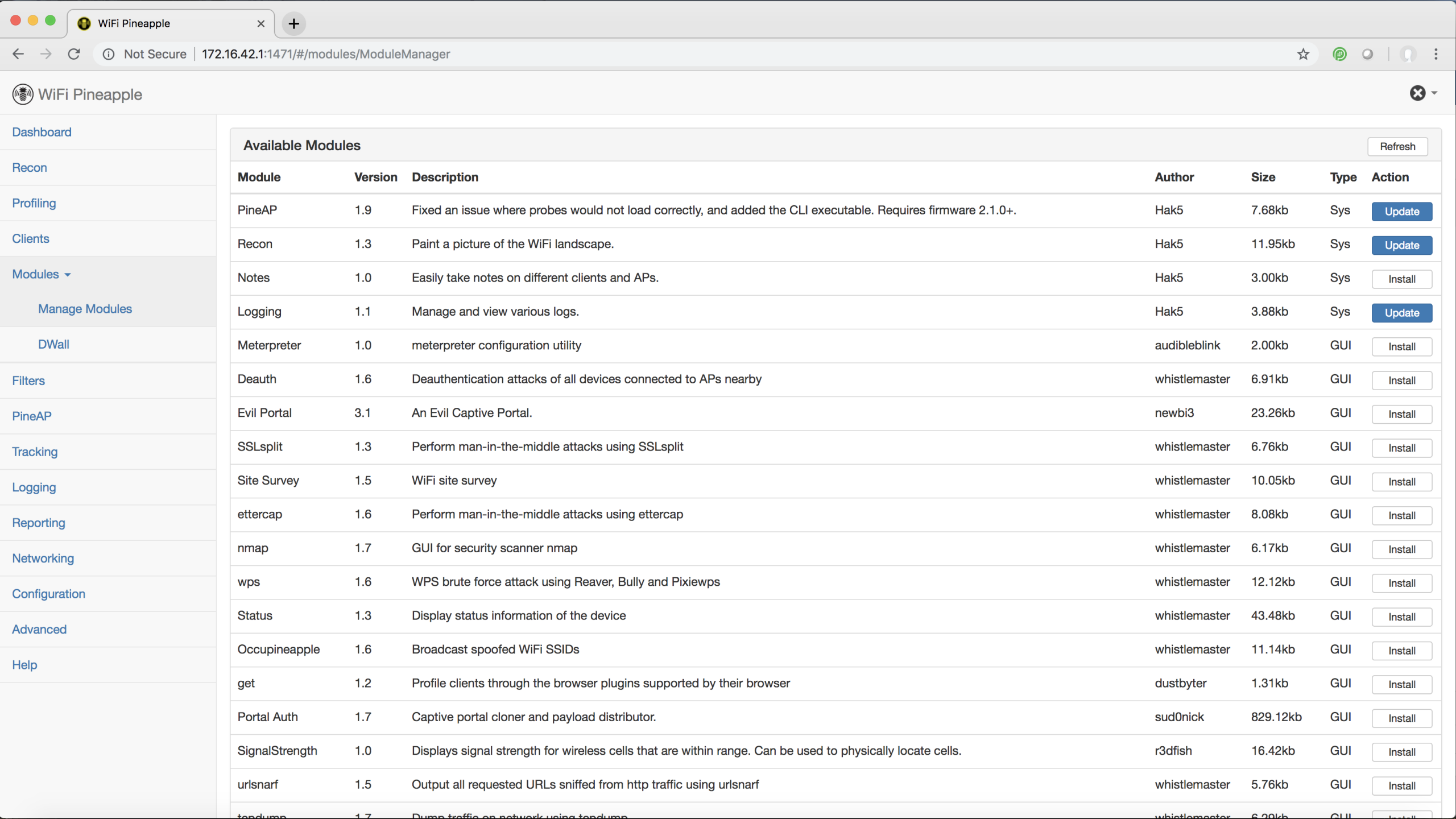
Recommendations

- Implement a corporate USB policy
- Do not plug in USBs if you do not know where they came from
- Do not plug in cords at airports, public places or from strangers
- Plug your charging cords into an outlet, not directly into a port

WiFi Attacks


WiFi Pineapple
Not Secure | 172.16.42.1:1471/#/modules/Dashboard
WiFi Pineapple
Dashboard
Recon
Profiling
Clients
Modules
Filters
PineAP
Tracking
Logging
Reporting
Networking
Configuration
Advanced
Help
0 hours, 6 minutes
UPTIME
100% CPU USAGE
14
CLIENTS CONNECTED
136
SSIDS IN POOL
13 SSIDS ADDED THIS SESSION
Landing Page Browser Stats
No Landing Page Browser Stats Available
Notifications
No Notifications
Bulletins
Load Bulletins from WiFiPineapple.com


WiFi Pineapple
Not Secure | 172.16.42.1:1471/#/modules/Clients
Dashboard
Recon
Profiling
Clients
Modules
Filters
PineAP
Tracking
Logging
Reporting
Networking
Configuration
Advanced
Help
Clients
Refresh
MAC Address
IP Address
SSID
Hostname
Kick Client
IBMInternet
square
Kick
gogoinflight
Gregs-iPhone
Kick
Fly-Fi
StefaniesiPhone
Kick
gogoinflight
No Hostname
Kick
Revere_Guest
TimSkeeniPhoneX
Kick
IND_PUBLIC_WiFi
*
Kick
Fly-Fi
Sheilas-iPhone
Kick
gogoinflight
KO-iPhone
Kick
United_Wi-Fi
Saurabhs-iPhone
Kick
Fly-Fi
iPhone-X
Kick
gogoinflight
FabriciosiPhone
Kick
Fly-Fi
Galaxy-S7-edge
Kick
United_Wi-Fi
Marineshone7128
Kick
United_Wi-Fi
No Hostname
Kick



Module	Version	Description	Author	Size	Type	Action
PineAP	1.9	Fixed an issue where probes would not load correctly, and added the CLI executable. Requires firmware 2.1.0+.	Hak5	7.68kb	Sys	Update
Recon	1.3	Paint a picture of the WiFi landscape.	Hak5	11.95kb	Sys	Update
Notes	1.0	Easily take notes on different clients and APs.	Hak5	3.00kb	Sys	Install
Logging	1.1	Manage and view various logs.	Hak5	3.88kb	Sys	Update
Meterpreter	1.0	meterpreter configuration utility	audibleblink	2.00kb	GUI	Install
Deauth	1.6	Deauthentication attacks of all devices connected to APs nearby	whistlemaster	6.91kb	GUI	Install
Evil Portal	3.1	An Evil Captive Portal.	newbi3	23.26kb	GUI	Install
SSLsplit	1.3	Perform man-in-the-middle attacks using SSLsplit	whistlemaster	6.76kb	GUI	Install
Site Survey	1.5	WiFi site survey	whistlemaster	10.05kb	GUI	Install
ettercap	1.6	Perform man-in-the-middle attacks using ettercap	whistlemaster	8.08kb	GUI	Install
nmap	1.7	GUI for security scanner nmap	whistlemaster	6.17kb	GUI	Install
wps	1.6	WPS brute force attack using Reaver, Bully and Pixiewps	whistlemaster	12.12kb	GUI	Install
Status	1.3	Display status information of the device	whistlemaster	43.48kb	GUI	Install
Occupineapple	1.6	Broadcast spoofed WiFi SSIDs	whistlemaster	11.14kb	GUI	Install
get	1.2	Profile clients through the browser plugins supported by their browser	dustbyter	1.31kb	GUI	Install
Portal Auth	1.7	Captive portal cloner and payload distributor.	sud0nick	829.12kb	GUI	Install
SignalStrength	1.0	Displays signal strength for wireless cells that are within range. Can be used to physically locate cells.	r3dfish	16.42kb	GUI	Install
urlsnarf	1.5	Output all requested URLs sniffed from http traffic using urlsnarf	whistlemaster	5.76kb	GUI	Install
tcpdump	1.7	Dump traffic on network using tcpdump	whistlemaster	6.29kb	GUI	Install

WiFi Pineapple

172.16.42.1:1471/#/modules/DWall

WiFi Pineapple

- Dashboard
- Recon
- Profiling
- Clients
- Modules
  - Manage Modules
  - Deauth
  - DNSspoof
  - DWall
  - SSLsplit
- Filters
- PineAP
- Tracking
- Logging
- Reporting
- Networking
- Configuration
- Advanced
- Help

DWall Settings

DWall is currently running.

Disable | Stop Listening

URLs

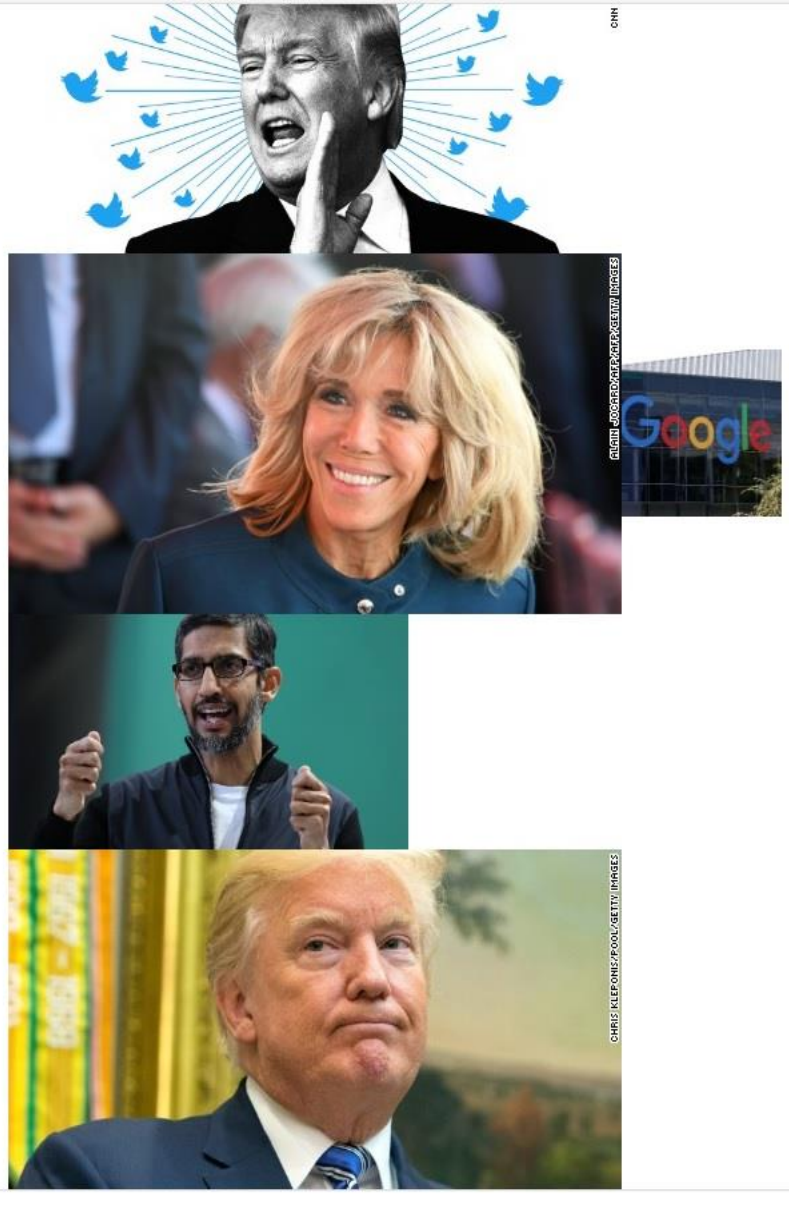
Client	URL
172.16.42.216	http://3.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/1e0aa6c7-e946-4b0b-8eaa-8c1299a122e5
172.16.42.187	http://api.bounceexchange.com/bounce/init1.js? tojQ=function&cts=1502211223961&tzo=240&is_preview=false&website_id=340&resolution=1920x974&ref
172.16.42.216	http://3.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/1e0aa6c7-e946-4b0b-8eaa-8c1299a122e5
172.16.42.187	http://cdn.livefyre.com/libs/fyre.conv/v3.0.0/livefyre.min.js
172.16.42.216	http://3.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/1e0aa6c7-e946-4b0b-8eaa-8c1299a122e5
172.16.42.216	http://3.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/1e0aa6c7-e946-4b0b-8eaa-8c1299a122e5

Cookies

Client	Cookie
172.16.42.187	__qca=P0-2023635121-1459394101055; CNNtosAgreed=true; __gads=ID=4afb73bda193cd2b:T=1459394
172.16.42.187	__qca=P0-2023635121-1459394101055; CNNtosAgreed=true; __gads=ID=4afb73bda193cd2b:T=1459394 optimizelySegments=%7B%22170962340%22%3A%22false%22%2C%22171657961%22%3A%22gc%22 optimizelyBuckets=%7B%7D; gig_hasGmid=ver2; optimizelyEndUserId=oeu1459394093391r0.155884117(
172.16.42.187	__qca=P0-2023635121-1459394101055; CNNtosAgreed=true; __gads=ID=4afb73bda193cd2b:T=1459394 optimizelySegments=%7B%22170962340%22%3A%22false%22%2C%22171657961%22%3A%22gc%22 optimizelyBuckets=%7B%7D; gig_hasGmid=ver2; optimizelyEndUserId=oeu1459394093391r0.155884117(
172.16.42.187	__qca=P0-2023635121-1459394101055; CNNtosAgreed=true; __gads=ID=4afb73bda193cd2b:T=1459394 optimizelySegments=%7B%22170962340%22%3A%22false%22%2C%22171657961%22%3A%22gc%22

Data

Images



Recommendations

- Do not do anything personal or sensitive when connected to public WiFi
- Forget networks after you're done using them
- Turn on 'Ask to Join Networks'
- Use a VPN on your personal and corporate devices

Reconnaissance

Collecting SSID Probes

Probe Request	xfinitywifi	1
Probe Request	Arunima	2
Probe Request	Tufts_Guest	1
Probe Request	IBM	1
Probe Request	JioFi_1019098	1
Probe Request	Deliberant	1
Probe Request	RO2	1
Probe Request	IBM	3
Probe Request	IBM	1
Probe Request	TMobileWingman	1
Probe Request	Sheraton_GUEST	1
Probe Request	Grey Lady WiFi	1
Probe Request	White Elephant	1
Probe Request	Jared Coffin	1
Probe Request	IBM	1
Probe Request	rhome	1
Probe Request	United_Wi-Fi	1
Probe Request	rhome2	1
Probe Request	BAWi-Fi	1
Probe Request	Harvard WiFi Setup	1
Probe Request	IBM	1

Our Target

Probe Request	8C:85:90:48:8D:0B	xfinitywifi	1
Probe Request	8E:1B:7D:A1:ED:8F	Arunima	2
Probe Request	8E:1B:7D:A1:ED:8F	Tufts_Guest	1
Probe Request	8E:1B:7D:A1:ED:8F	IBM	1
Probe Request	8E:1B:7D:A1:ED:8F	JioFi_1019098	1
Probe Request	8E:1B:7D:A1:ED:8F	Deliberant	1
Probe Request	8E:1B:7D:A1:ED:8F	RO2	1
Probe Request	98:01:A7:9A:FA:A3	IBM	3
Probe Request	98:01:A7:A7:10:E3	IBM	1
Probe Request	9E:1D:98:C7:87:35	TMobileWingman	1
Probe Request	9E:63:7C:C1:EE:DF	Sheraton_GUEST	1
Probe Request	9E:63:7C:C1:EE:DF	Grey Lady WiFi	1
Probe Request	9E:63:7C:C1:EE:DF	White Elephant	1
Probe Request	9E:63:7C:C1:EE:DF	Jared Coffin	1
Probe Request	9E:63:7C:C1:EE:DF	IBM	1
Probe Request	9E:63:7C:C1:EE:DF	rhome	1
Probe Request	9E:63:7C:C1:EE:DF	United_Wi-Fi	1
Probe Request	9E:63:7C:C1:EE:DF	rhome2	1
Probe Request	9E:63:7C:C1:EE:DF	BAWi-Fi	1
Probe Request	A6:E1:60:A8:7D:C3	Harvard WiFi Setup	1
Probe Request	A6:E1:60:A8:7D:C3	IBM	1

Immediate Info

Probe Request	9E:63:7C:C1:EE:DF	Sheraton_GUEST	
Probe Request	9E:63:7C:C1:EE:DF	Grey Lady WiFi	1
Probe Request	9E:63:7C:C1:EE:DF	White Elephant	1
Probe Request	9E:63:7C:C1:EE:DF	Jared Coffin	1
Probe Request	9E:63:7C:C1:EE:DF	IBM	1
Probe Request	9E:63:7C:C1:EE:DF	rhome	1
Probe Request	9E:63:7C:C1:EE:DF	United_Wi-Fi	1
Probe Request	9E:63:7C:C1:EE:DF	rhome2	1
Probe Request	9E:63:7C:C1:EE:DF	BAWi-Fi	

Frequent Sheraton Guest?

United FF?

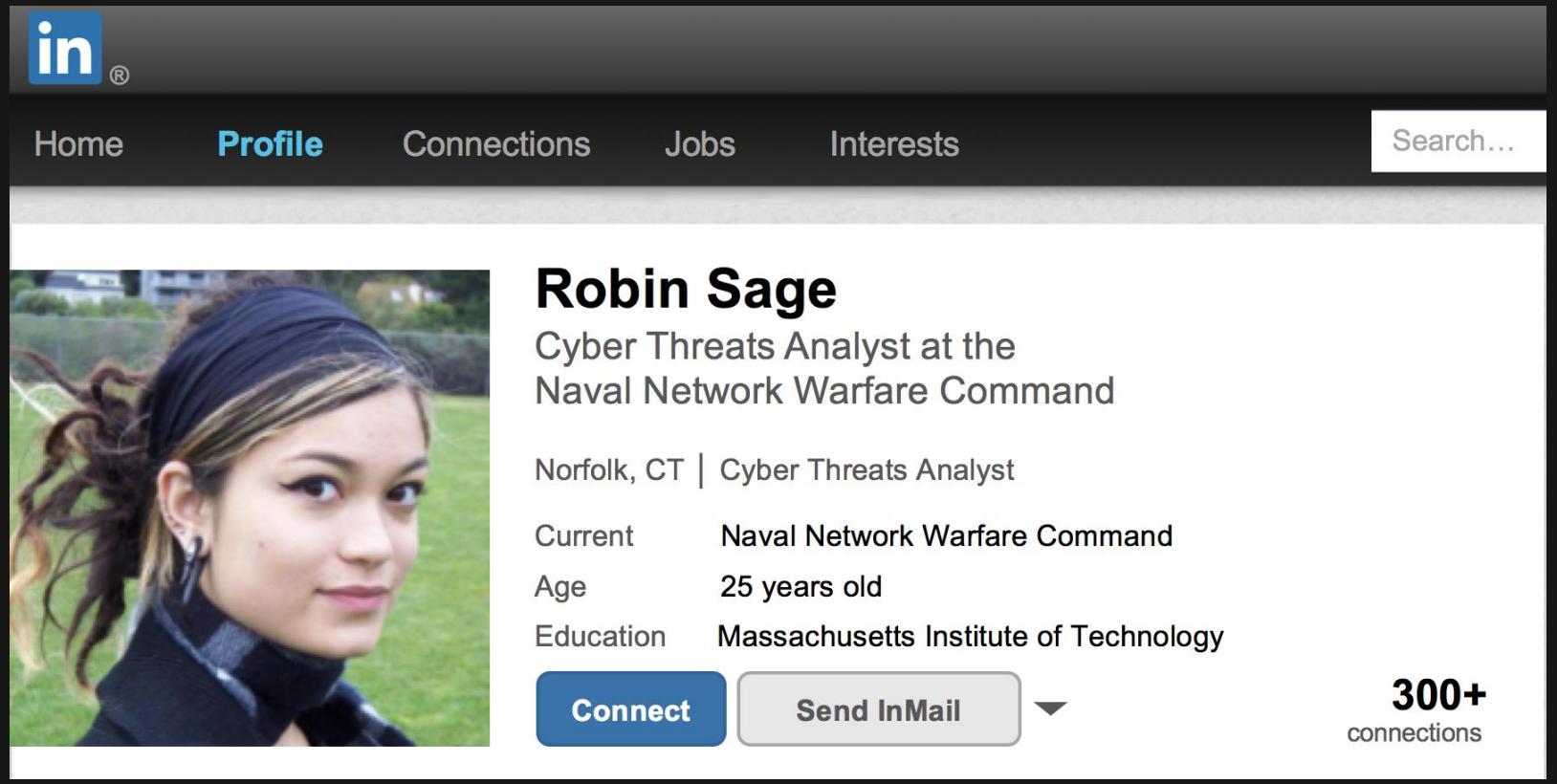
British Airways FF?

Typo Type	Typo	DNS-A	CC-A	DNS-MX	Extn
Character Omission	ww.facebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Omission	www.acebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Omission	www.facbook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Omission	www.facebok.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Omission	www.faceboo.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Omission	www.facebook.cm	46.166.184.99	GB,UNITED KINGDOM		cm
Character Omission	www.faceook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Omission	www.faebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Omission	www.fcebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Omission	wwwfacebook.com	157.240.18.15	US,UNITED STATES		com
Character Repeat	www.faacebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Repeat	www.faccebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Repeat	www.facebbook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Repeat	www.facebookk.com	198.54.117.244			com
Character Repeat	www.faceboook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Repeat	www.faceebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Repeat	www.ffacebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Repeat	wwww.facebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Swap	ww.wfacebook.com	72.52.179.174	US,UNITED STATES	mx156.hostedmxserver.com	com
Character Swap	www.afcebook.com	104.219.168.162			com
Character Swap	www.facbeook.com	104.219.168.162			com
Character Swap	www.faceboko.com	199.59.242.153	CN,CHINA		com
Character Swap	www.faceobok.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Swap	www.faecbook.com		?		com
Character Swap	www.fcaebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Swap	wwwf.acebook.com		?		com
Character Replacement	eww.facebook.com		?		com
Character Replacement	qww.facebook.com		?		com
Character Replacement	wew.facebook.com		?		com
Character Replacement	wqw.facebook.com		?		com
Character Replacement	wwe.facebook.com		?		com
Character Replacement	wwq.facebook.com		?		com
Character Replacement	www.dacebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Replacement	www.facebiok.com	104.219.168.162			com
Character Replacement	www.faceboik.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Replacement	www.facebooj.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Replacement	www.facebool.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Replacement	www.facebopk.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Replacement	www.facebpok.com	104.219.168.162			com
Character Replacement	www.facenook.com		?		com
Character Replacement	www.facevook.com		?		com
Character Replacement	www.facrbook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com
Character Replacement	www.facwbook.com	185.53.178.6		mail.h-email.net	com
Character Replacement	www.favebook.com	157.240.18.15	US,UNITED STATES	smtpin.vvv.facebook.com	com

Recommendations

- Consider purchasing available domains
- Block and monitor TypoSquatted domains
- Check for emails originating from TypoSquatted domains
- Verify you are connected to a legitimate network

Social Engineering



- Haveibeenpwned.com
- Pastebin.com
- Shodan.io
- Censys.io

Recommendations

- Lock down social media accounts
- Be aware of what personal information is publicly available
- Do not reuse passwords, and update passwords frequently
- Do not use the same email for personal, finance, work

You Are the Shield

1. Slow down – Go thru your check list
2. Zero trust - USB sticks, URLs, Cash Machines,
3. Cybersecurity starts at home
4. Turn on 2-F-A, or 3-F-A whenever possible
5. Use different email addresses for account importance
6. Lock down your Social Media accounts
7. Use a webcam cover on your laptop
8. Do a security check on your accounts
9. Do not reuse the same password – 15 characters is the new standard
    - Use Password Phrases
        - Do not mix drinks Worst wedding ever 2017 = Dnmdwwe2017
        - Password Manager (ex. 1Password) (Auto Generate)
10. Use a VPN on corporate and personal devices

IBM Security

IBM Security

Thank you.

@HayleyBCohen

Executive Security Advisor
X-Force Command
IBM Security

IBM