The documents include several lists of routers and access points, some of which are more than five years old. The first list of devices, titled simply "WiFi Devices" is described in the CherryBlossom user manual :

> CB [CherryBlossom] maintains an information database of wireless network devices in the "WiFi Devices.xls" document. This database contains information about hundreds of network devices, including manufacturer, make, model, version, reference design, FCC ID, network processor, wireless chipset, operating system, default username/password, etc. It also contains firmware analysis information about exact make, model, hardware versions, and firmware versions supported by CB.

In the version of the document WikiLeaks released, some of the information listed in that description is missing, including the firmware versions that CherryBlossom supports. So while it's clear that the CherryBlossom project targeted the following list of routers, it is not clear which have been successfully compromised.

It is, however, never a bad idea to update your home router's firmware, as these devices stand on the front line of your digital security. And if your device is on the list below, perhaps now is an time to flash your firmware. To do so, simply search the internet for your router's make and model with the keyword "firmware," and follow your vendor's instructions.

Routers and access points targeted by CherryBlossom

Again, while it's clear that the CherryBlossom project targeted the following list of routers, it is not clear which have been successfully compromised.

- **3Com:** 3CRWE454A72, 3CRWX120695A, 3CRWX275075A, 3CRTRV10075, 3CRWE41196, 3CRWE454G72, 3CRWE53172, 3CRWE554G72T, 3CRWE554G72TU, 3CRWE675075, 3CRWE725075A-US, 3CRWE754G72-A, 3CRWE754G72-B, 3CRWE825075A-US, 3CRWE875075A-US, 3CRWE91096A, 3CRWE91096A, 3CRWE920G73-US, 3CRWEASY96A, 3CRWEASY96A, 3CRWEASYG73-U, 3CRWX440095A
- **Accton:** WA3101, WA4101, WA5101, WA5201, WA6101, WA6102, WA6102X
- **Aironet/Cisco:** Aironet 1310 Outdoor Access Point /Bridge, Aironet 350 Series Wireless Bridge, 1300 Series Outdoor Access Point/Bridge, Aironet 1200 Series a/b/g Access Point, Aironet 1310 Outdoor Access Point/Bridge, Aironet 350 Series, Aironet 350

Series AP, Cisco Aironet 1400 Series Wireless Bridge, Cisco Aironet 1400 Series Wireless Bridge

- **Allied Telesyn:** AT-WA1004G, AT-WA7500, AT-WL2411
- **Ambit:** (No models specified)
- **AMIT, Inc:** WIS418, WQS418, WUC128
- **ANI Communications:** (No models specified)
- ~~**Apple:** AirPort Express~~
- **Asustek Co:** WL-160g, WL-300, WL-300g, WL-330, WL-330g, WL-500b, WL-500g
- **Belkin:** F5D7230-4
- **Breezecom:** AP-10, AP-10D, BU-DS.11, BU-DS.11D, DS.5800 Base Unit, RB-DS.11, RB-DS.11D, SA-10, SA-10D, SA-40, SA-40D, WB-10, WB-10D
- **Cameo:** WLB-2006_2007, WLB-2203/2204, WLG-2002/2003, WLG-2204/2205
- **D-Link:** AP Manager or D-View SNMP management module?, DCS-2100+, DCS-3220G, DCS-5300G, DCS-5300W, DI-514, DI-524, DI-624, DI-714P+, DI-774, DI-784, DI-824VUP, DP-311P, DP-311U, DPG-2000W, DP-G310, DP-G321, DSM-320, DVC-1100, DWL-1000AP+, DWL-120, DWL-1700AP, DWL-1750, DWL-2100AP, DWL-2200AP, DWL-7000AP, DWL-7100AP, DWL-800AP+, DWL-810+, DWL-G700AP, DWL-G730AP, DWL-G800AP, DWL-G810, DWL-G820
- **Epigram:** (No models specified)
- **Gemtek:** WADB-100G, WHAPC-100GE 11G, WHRTC-100GW, WX-1500, WX-1590, WX-1600, WX-1688, WX-2214, WX-2501, WX-5520A, WX-5520G, WX-5525G, WX-5525R, WX-5541, WX-5545, WX-5551, WX-5555, WX-5800, WX-5801, WX-5803
- **Global Sun:** CM054RT, WL AP 2454 NM0, WL AP 2454 QA0, WL AP 2454 QA3, WL MU 2454 13I0, WL RT 2454 NM0, WL RT 2554 QA0, WL UD 2454 13I0
- **Hsing Tech:** (No models specified)
- **Linksys:** BEFW11S4, WAP11, WAP51AB, WAP54G, WAP55AG,

WCG200, WET54G, WET54GS5, WGA11B, WGA54G, WMA11B, WMLS11B, WPG12, WPG54G, WPS11, WPS54GU2, WRE54G, WRT54G, WRT54GP2, WRT54GS, WRT55AG, WRV54G, WVC11B, WVC54G

- **Motorola:** WR850G
- **Orinoco:** AP-2000 Access Point, AP-2500 Access Point, AP-4000 Tri-Mode Access Point, AP-600 Access Point, Orinoco AP-700, Tsunami MP.11, Tsunami QuickBridge 11, Tsunami QuickBridge 20, Tsunami QuickBridge 60
- **Planet Tec:** WAP-1963A, WAP-4030, WRT-413, WAP-1963, WAP-1966, WAP-4000, WAP-4050, WAP-5000, WAP-5100, WL-U356, WRT-403, WRT-410
- **RPT Int:** (No models specified)
- **Senao:** 5GHz/2.4GHz Dual Band Wireless Access Point, Aries2, Dual Band Wireless Access Point, Long Range Wireless Dongle, Long Range Wireless Outdoor Client Bridge, NL-2511AP PRO PLUS, NL2511SR Plus, NL2511SR Plus(A), NL-2611AP3 PLUS, NL-3054CB3 PLUS, Outdoor Wireless Access Point/Router, Outdoor Wireless Bridge, SL2511SR Plus, Wireless 11g Broadband Router, Wireless Multi-Client Bridge/Access Point
- **US Robotics:** USR5420, USR5430, USR5450, USR8054
- **Z-Com:** XG-1100, XG-2000, XG-3020, XG-580, XG-580Plus, XG-581, XG-582, XI-1450, XI-1500, XI-1510

Within the CherryBlossom release, there are also documents that appear to target seven specific routers for use with "Flytrap." Flytrap is a tool CherryBlossom uses to "beacon over the Internet to a Command & Control server referred to as the CherryTree," according to WikiLeaks.

Flytrap routers

The CherryBlossom documents included firmware flashing instructions labeled "Flytrap" for each of these router models.

- **Belkin:** F5D8231
- **DLink:** DIR130

- **Linksys:** WRT320N, WRT54G, WRT300N, WRT54GL, WRT54GL

There are also two separate lists of devices in the CherryBlossom documents, named "Flytrap — Inventory (1)" and "Flytrap — Inventory (2)." These inventories appear to be lists of equipment used by a particular department within the CherryBlossom project, and many of the devices they list are very old, dating back to 2004. The devices include routers and access points, but also old computers and printers.

While we are listing the devices from those inventories below, it is not immediately clear whether they were targeted or compromised by CherryBlossom. We will update this post as more information becomes available.

Flytrap inventories

The devices listed below may have been used to test Flytrap or other CherryBlossom tools, but that is not immediately clear. We will update this post as more information becomes available.

- **3Com:** SL-1020, SL-1022, WL-525, SL-1020
- **ActionTec:** HWS 01170-01, HWS 01170-01
- **AG Neovo:** F-417, F-417
- **Asus:** WL-500g, WL-500g, WL-530g
- **Belkin:** F5D6130, F5D7231-4, F5D8230-4 v2, F5D6130
- **Buffalo:** WBR2-G54S, WHR-G54S, WZR-RS-G54, WBR2-G54S, WZR-G108
- **Cisco:** AIR-AP350, AIR-BR1310G-A-K9, AIR-PCM352, AIR-AP350
- **Compaq:** Deskpro 2000, iPAQ 3850, Deskpro 2000
- **D-Link:** DWL-1000AP, DWL-1000AP, DWL-650, DWL-G650
- **Dell:** Dimension 2400, Dimension XPS 600r, Inspiron 1100, WRTB-107GD340, Dimension 2400
- **DWL-1000AP:** D-Link
- **Epson:** M/N P954A, M/N P954A
- **Ericsson:** EPDK S10906/2.11, EPDK S10906/2.11
- **Gateway:** Performance 500 (TBR3500), Solo 9500, Performance 500

(TBR3500), Performance 500

- **Gateway Fax Systems:** 90si, 90si
- **HP:** HP Color LaserJet 3500, iPAQ 2215, iPAQ 5450, HP Color LaserJet 3500, iPAQ 5450
- **HyperLink Technologies:** HG2415Y, HG2415Y
- **IBM:** X40, 2378-FZU, X40
- **Intel:** M3AWEB, M3AWEB
- **Intersil:** APDK-EVAL, APDK-EVAL, WorldRadio APDK-EVAL
- **Iosoft:** ChipWeb 2.61, ER22 Development Board, ChipWeb 2.61
- **Linksys:** NSLU2, WAP11, WPC11, WRT54G, WRV54G, WRT54GS, WRT54G v5, WRT54GS v4, NSLU2
- **Microsoft:** NM-500, X09-29306, NM-500
- **Motorola:** WR850Gv2, WR850Gv2, WR850Gv3
- **Netgear:** WG602v2, WG602v2, WGT634U
- **Panasonic:** CF-73, CF-73
- **SMC:** SMC2682W, SMC2735W, SMC2755W, SMC2804WBR, SMC2682W
- **SMC2755W:** SMC
- **Sony:** PCG-FRV37, SPP-A967, PCG-FRV37
- **Sputnik:** 802AI, 802AI
- **U.S. Robotics:** 5461, 5461
- **WAP11:** Linksys
- **Western Digital:** WD1200B008-RNN, WD1200B008-RNN
- **Xircom:** APWE1100, APWE1100
- **Zcomax:** XI-1000, XI-1000