

# CSE406

## Presentation on Security Tools

---

Group - B2G1  
1705091-92-93-94-95-96

---

01

# ELSA

---

Geo-locating using Access Points

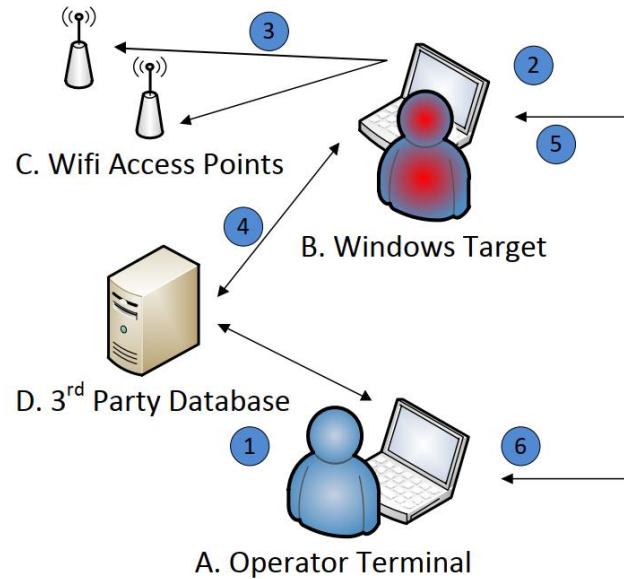
# **Introduction**

ELSA is a tool allegedly used by the U.S. CIA to track people's locations via their WiFi-enabled devices.

# Overview

- ELSA is a software system that geo-locates WiFi-enabled Windows systems.
- ELSA provides this geolocation by recording the details of WiFi access points near the target machine and transmitting metadata to 3<sup>rd</sup> party databases for resolution into latitude and longitude and an accuracy measure.
- These 3<sup>rd</sup> party databases exist to support location services in internet browsers like Chrome, and Firefox according to the w3c specification. ELSA uses HTTPS connections to query these 3rd party services and saves its data into a 128-bit AES encrypted file.

# How ELSA Works



# How ELSA Works

- An operator configures an ELSA implant based on the host environment ( A ).
- An operator deploys the implant to a Windows host, and it begins its collection ( B ).
- The implant begins collecting WiFi access point information based on the schedule set by the operator ( C ).
- If configured to do so, when the target user connects to the internet, the implant will resolve the WiFi data to geolocation via the third-party database ( D ).
- The operator connects to the Windows hosts and downloads the encrypted collection log.
- The operator decrypts the log and performs further analysis on their target.

# **System Description**

As, described before, ELSA is a tool designed to provide COG pattern of life geolocation information. The major component is the windows DLL tool, which is used in the target environment. The minor components are the configuration tool (patcher) and the post-processor (processor), which are used in the deployment, configuration, and operation.

# ELSA File Components

Directory	Filename	Note(s)
server/windows	patcher.exe	Windows Config Tool
server/windows	processor.exe	Windows Decryption Tool
server/windows	tool-x64.dll	Windows x64 implant
server/windows	tool-x86.dll	Windows x86 implant
server/windows	installDllMain.vbs	VBScript file illustrating optional placement of the Elsa task in the Task Scheduler
server/windows	uninstallDllMain.vbs	VBScript file illustrating optional removal of the Elsa task from the Task Scheduler
server/windows	sha1-windows-images.txt	Sha1 hashes of files in the distribution
server/windows	classifications-windows.txt	Classifications of files in the distribution
docs	Elsa User Manual.pdf	This manual

# Installation: Prerequisites

- The operator will only work correctly if everything is installed and executed within the appropriate operating environment.
- ELSA is designed to work on Windows 7 32 bit and 64 bit.
- ELSA tool can be renamed, signed and packed without losing its functionality.
- The dll can be injected inside an existing process which reduces its visibility.
- Third-party databases can be set during ELSA installation. They can be none, Google or Microsoft.

# Installation: DLL Injection

- The ELSA client is designed to be injected into an existing process on the system. It is delivered in the form of a DLL. As such it is essential that the 32-bit and 64-bit versions of the DLL be run on the matching machines.
- ELSA can run in several operational modes that offer flexibility as to its appearance within the system. ELSA can be installed as a service running inside of SvcHost, a scheduler task running inside of Dllhost, a utility running inside of rundll32, or an AppInit DLL running inside of a specified process.

# Installation: DLL Installation

ELSA dll exports routines that can be used to install the tool using **RegSvr32.exe** among other methods. 64-bit version of windows contains two copies of RegSvr32.exe. The first is a 64-bit executable located in **C:\Windows\System32** directory and the second is a 32-bit executable located in the **C:\Windows\SysWOW64** directory. Deploying the 64-bit version of the dll required the 64-bit version of RegSvr32.

# Installation: Configuration

- Resolve geolocation from the target or later. If it is resolved from the target, it may create additional network traffic, although this traffic is designed to look like legitimate browser traffic. Resolving later can result in different result if the WiFi database changes.
- How much space will be allocated for the log file.
- If the WiFi surveys will be saved.

# **Exfiltration**

Currently, Elsa makes no provisions for automatically beaconing or exfiltrating collected data off of the target machine. Therefore, the operator must extract the ELSA log file from the target machine through other means. It is possible to completely delete the log file. Elsa will create a new file if this is the case.

# Processing

Exfiltrated data will be symmetrically encrypted and must be processed using the processor tool. This tool has two main functions:

- Decrypting raw log files generated by ELSA into XML files.
- Resolving lists of wifi access point metadata into geolocations, using the `-l <provider>` flag

# End-to-end Walk-through - 1

```
Directory of C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows

06/13/2012  10:33 AM    <DIR>          .
06/13/2012  10:33 AM    <DIR>          ..
06/13/2012  09:09 AM            2,717 addtask.vbs
06/13/2012  09:09 AM            116,224 patcher.exe
06/13/2012  09:09 AM            270,336 processor.exe
06/13/2012  09:09 AM            453 shal-windows-images.txt
06/13/2012  09:09 AM            109,568 tool-x64.dll
06/13/2012  09:09 AM            86,016 tool-x86.dll
               6 File(s)        695,526 bytes
               2 Dir(s)   196,852,690,944 bytes free
```

# End-to-end Walk-through – 2.1

```
C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows
> patcher.exe -p x64 -o testx64g.dll -W
Enter mode [default is RunDll32]:
Enter target process filename [default is rundll32.exe]:
Enter data file name [default is %SystemRoot%\TEMP\elsa.data]:
%SystemRoot%\TEMP\elsag.data
Enter data file max kb [default is 200]: 202
Enter data file archive seconds [default is 60]: 62
Enter data encryption key file [default is key.bin]:
Create a new application guid [default is no]:
Enter application guid [default is {59553112-3228-49ce-8044-4AB3C63BD46C}]:
Enter seconds between wifi surveys [default is 30]: 32
Enter the seconds to delay the wifi survey after install [default is 30]: 32
Enter the seconds to delay the wifi survey after startup [default is 30]: 32
Enter backoff factor to use when wifi survey are unsuccessful [default is 10]: 13
Enter the wifi rssи threshold [default is 100]: 202
Save all wifi surveys [default is no]:
Enter geolocation provider [default is google]:
Enter the Client Id [default is 5555]: 2234

C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows
> dir
```

# End-to-end Walk-through – 2.2

```
Volume in drive C is OS
Volume Serial Number is 16CB-523E

Directory of C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows

06/13/2012  10:44 AM    <DIR>        .
06/13/2012  10:44 AM    <DIR>        ..
06/13/2012  09:09 AM            2,717 addtask.vbs
06/13/2012  10:33 AM            130 key.bin
06/13/2012  09:09 AM            116,224 patcher.exe
06/13/2012  09:09 AM            270,336 processor.exe
06/13/2012  09:09 AM            453 sha1-windows-images.txt
06/13/2012  10:44 AM            109,568 testx64g.dll
06/13/2012  09:09 AM            109,568 tool-x64.dll
06/13/2012  09:09 AM            86,016 tool-x86.dll
06/13/2012  10:44 AM            512 wizard.config
               8 File(s)       806,919 bytes
               2 Dir(s)   196,851,429,376 bytes free
```

# End-to-end Walk-through – 3

```
C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows
> mkdir indir
C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows
> mkdir outdir
C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows
> processor.exe -k key.bin -i indir -o outdir
key      : key.bin
input    : indir
output   : outdir
mask     : (null)

processing 'indir\elsag.data' done

1 files processed.

C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows
```

# End-to-end Walk-through - 4

```
<?xml version="1.0" encoding="UTF-8"?>
<Log>
  <client>0x2234</client>
  <wifi-ap-list>
    <wifi-ap-entry>
      <timestamp format="UTC">Wed Jun 13 14:42:27 2012</timestamp>
      <flags>0x0</flags>
      <count>12</count>
      <wifi-ap>
        <ssid>BREAD SHOP</ssid>
        <mac>00:03:52:AB:F4:20</mac>
        <rssii>-29</rssii>
      </wifi-ap>
      <wifi-ap>
        <ssid>CableCo</ssid>
        <mac>00:04:E2:C6:3B:DA</mac>
        <rssii>-77</rssii>
      </wifi-ap>
      <wifi-ap>
        <ssid>grace</ssid>
        <mac>00:13:10:C3:26:24</mac>
        <rssii>-73</rssii>
      </wifi-ap>
      <wifi-ap>
        <ssid></ssid>
        <mac>00:14:D1:AE:D3:EC</mac>
        <rssii>-81</rssii>
      </wifi-ap>
      <wifi-ap>
        <ssid></ssid>
        <mac>00:14:D1:AE:D3:FC</mac>
        <rssii>-81</rssii>
      </wifi-ap>
      <ssid>09BX03031164</ssid>
      <mac>00:23:97:33:5D:F1</mac>
      <rssii>-79</rssii>
    </wifi-ap>
    <wifi-ap>
      <ssid>09FY11030962</ssid>
      <mac>00:23:97:C0:9E:11</mac>
      <rssii>-81</rssii>
    </wifi-ap>
    <wifi-ap>
      <ssid>dlink</ssid>
      <mac>1C:AF:F7:DB:0B:B7</mac>
      <rssii>-83</rssii>
    </wifi-ap>
  ...</wifi-ap-list>
</Log>
```

# End-to-end Walk-through – 5

```
C:\Users\user\elsa-v1.0.0-windows\unclassified\server\windows
> processor.exe -i outdir\elsag.data.xml -o relocateg.xml -l google
input      : outdir\ elsag.data.xml
output     : relocateg.xml
provider   : google
processing Wed Jun 13 14:42:27 2012
```

# End-to-end Walk-through – 6

```
<?xml version="1.0" encoding="UTF-8"?>
<Log>
  <geo-list>
    <geo-entry>
      <timestamp format="UTC"> Wed Jun 13 14:42:27 2012</timestamp>
      <accuracy>75</accuracy>
      <provider>google</provider>
      <location>38.123456789, -77.123456789</location>
    </geo-entry>
  </geo-list>
</Log>
```

# Limitations

- ELSA cannot send data to the operator directly through the attacked machine. The operator must use some backdoor or download the data manually by connecting to the target machine.
- The result of the geolocation depends on the quality of the databases used. If the database is not updated periodically, the result may be poor.
- Also, a place with more access points yields a higher accuracy than a place with lower number of access points.

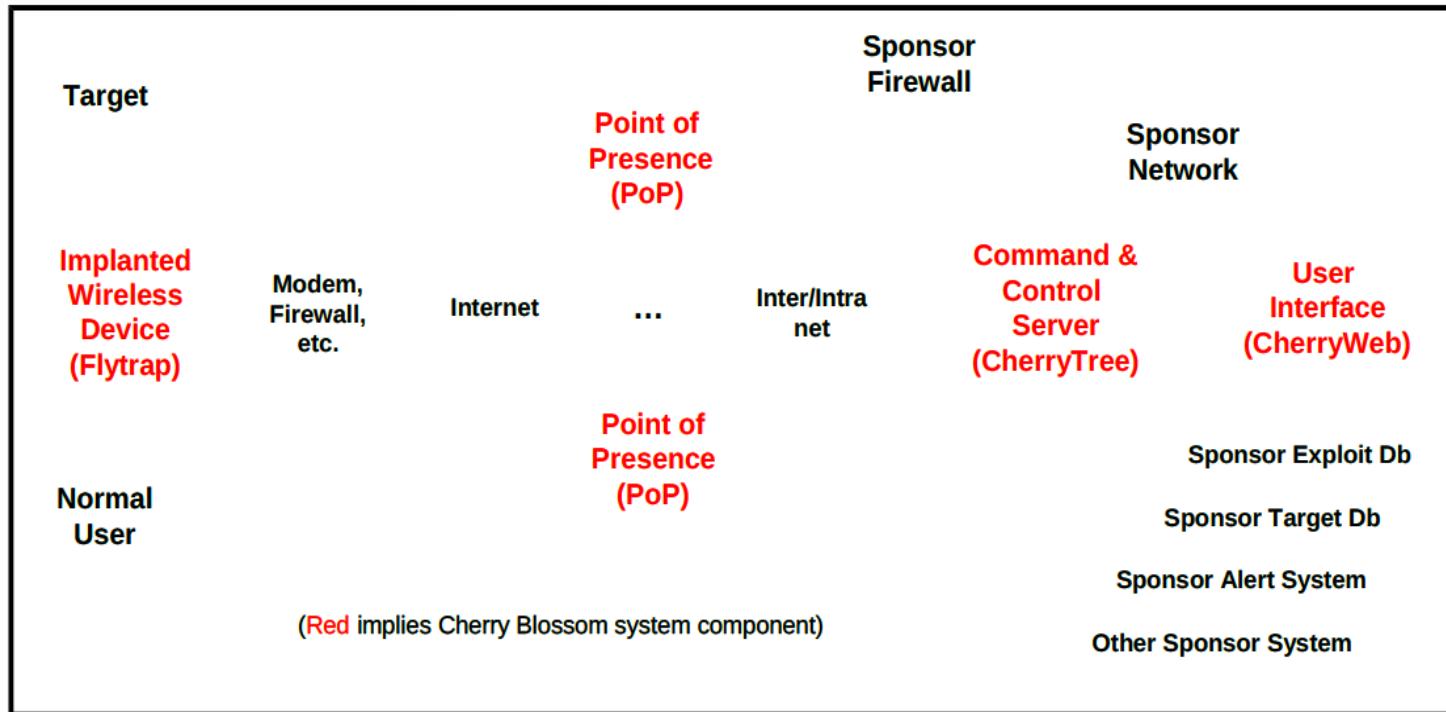
# Cherry Blossom

Performing software exploits by  
compromising wireless devices

# **Introduction**

- The Cherry Blossom (CB) system provides a means of
  - monitoring the internet activity
  - performing software exploits
- Particularly focused on
  - compromising wireless networking devices, such as
    - wireless (802.11) routers
    - access points (APs)

# Cherry Blossom Architecture



# The key component

- *Flytrap*
  - Typically a wireless (802.11/WiFi) device (router/access point)
  - Has been implanted with *CB* firmware

# Tools/techniques for Implanting

- Using the Device's Firmware Upgrade Web Page over a Wireless (WLAN) Link
  - Many wireless devices
    - allow a firmware upgrade over the wireless link
    - can often be implanted without physical access.

# **Tools/techniques for Implanting**

- **Using a Wireless Upgrade Package**
  - some devices do not allow a firmware upgrade over the wireless link
  - To workaround this issue, “Wireless Upgrade Packages” have been created for a few devices of interest

# Tools/techniques for Implanting

- Using the Claymore Tool
  - the *Claymore* tool is a
    - survey,
    - collection, and
    - implant tool for wireless (802.11/WiFi) devices.

# **Tools/techniques for Implanting**

- Using the Device's Firmware Upgrade Web Page over a Wired (LAN) Link**

# What Happens After Implanting?

- Affected device will
  - *Beacon* over the internet to a command & control server referred to as the *CherryTree (CT)*.
  - The *Beacon* contains
    - device status and
    - security information
      - that the *CherryTree* logs to a database.

# What Happens After Implanting?

- In response to the Beacon,
  - The *CherryTree* sends a *Mission* with operator-defined tasking
- An operator can use
  - *CherryWeb (CW)*, a browser-based user interface

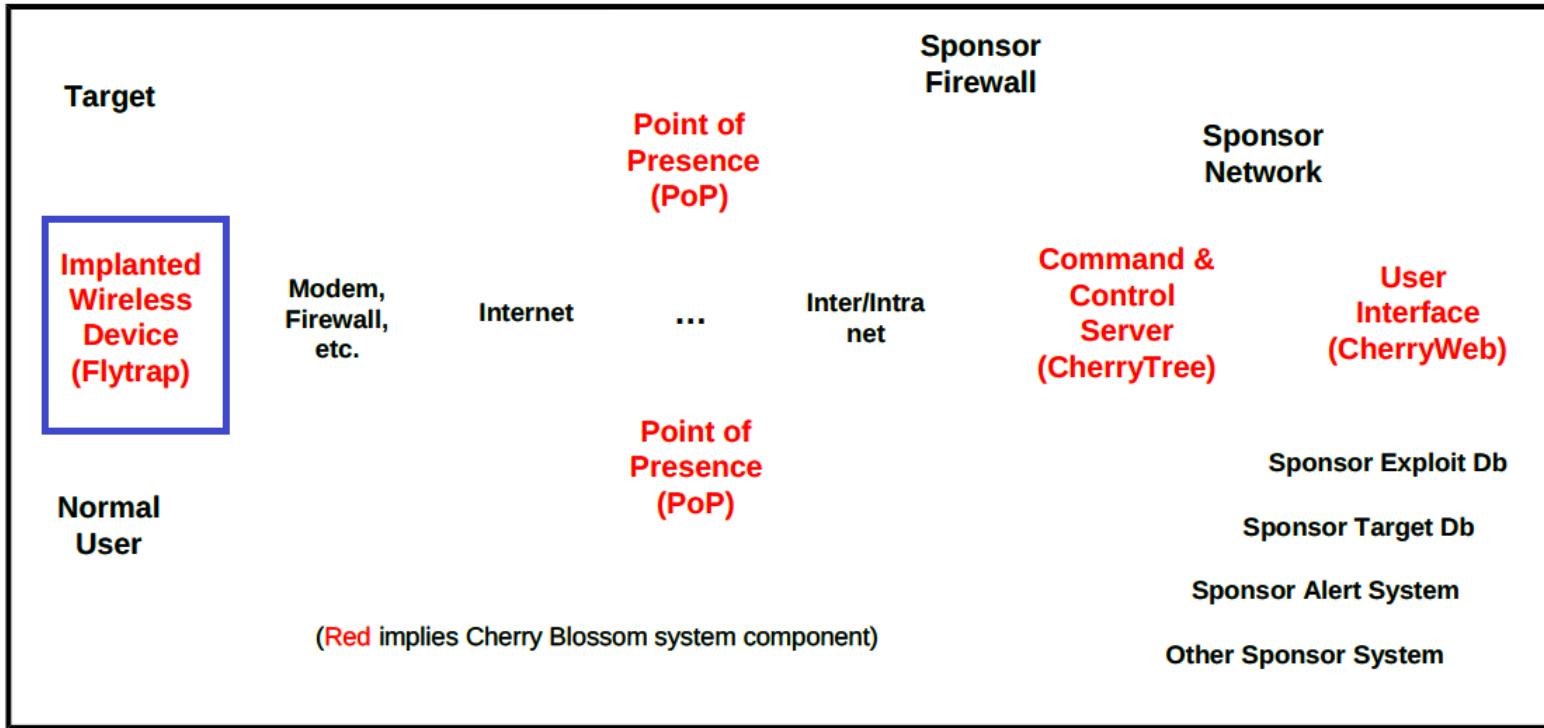
---

# **System Components and Features**

---

# **Claymore**

- **The survey function**
  - Attempts to determine device makes/models/versions in a region of interest.
- **The collection function**
  - Can capture wireless traffic.
- **The implant function**
  - Can perform wireless firmware upgrades
  - Incorporates the exploitation tools



# Flytrap Features

- Beacon
  - A *Flytrap* will periodically send a *Beacon* to report
    - status
    - security settings

# Flytrap Features

- Mission Tasking
  - When a *Flytrap* sends a *Beacon*,
    - the *CT* responds by tasking the Flytrap with a *Mission*.
  - Upon receipt of a *Mission*,
    - a *Flytrap* will begin *Mission* execution

# Flytrap Features

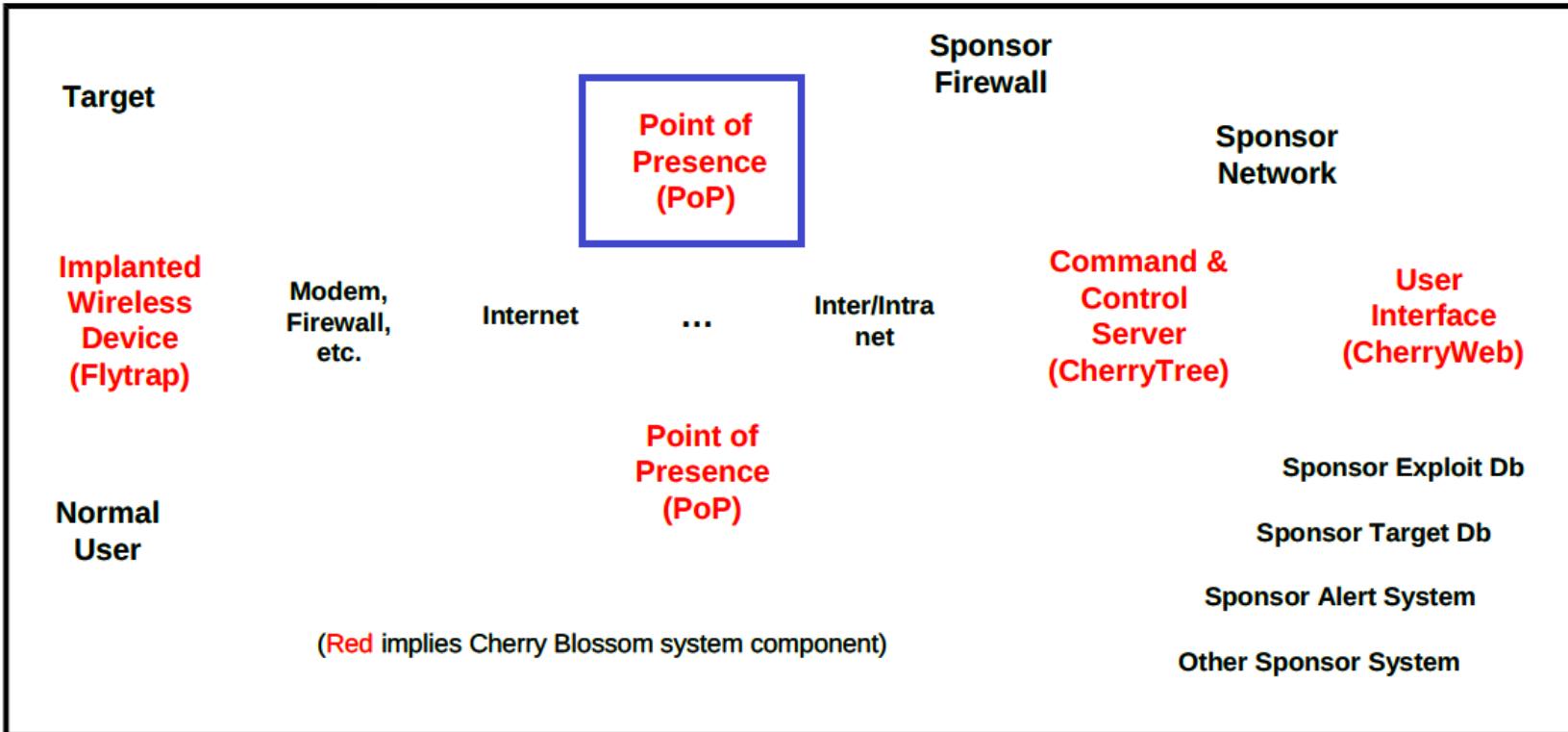
- Target Detection
  - Email addresses
  - Chat usernames
  - MAC addresses
  - VoIP phone numbers

# Flytrap Features

- Target Alerting
  - When a Target is detected, the Flytrap sends an Alert to the CT
  - An Alert generated from a Target detection will contain the MAC address of the client that generated the Target detection, and the time the detection occurred.

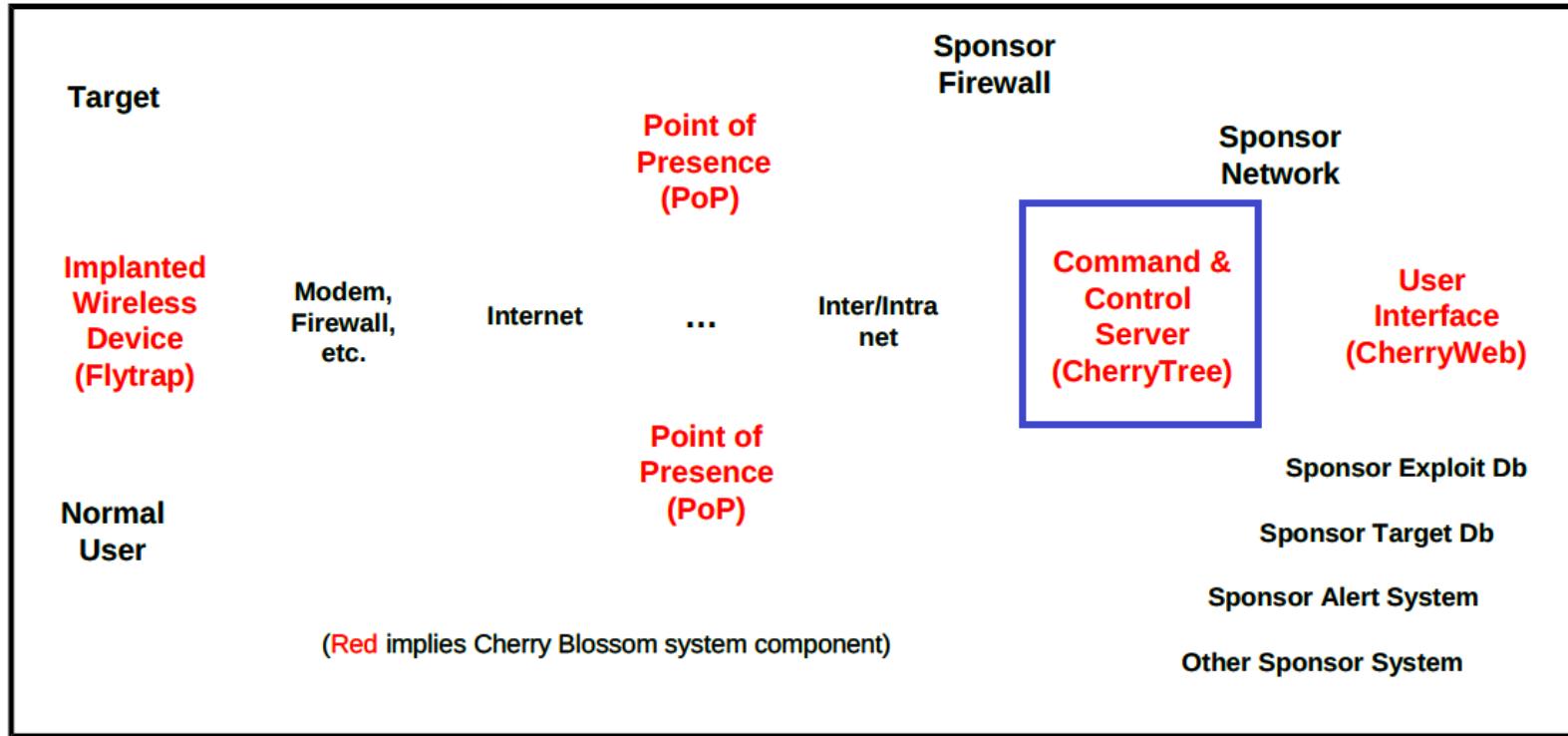
# Flytrap Features

- Target Actions
  - Browser Redirect (Windex)
  - Copy
  - VPN Proxy/Link
- Default Gateway Discovery (DGD)
- Firmware Upgrade Inhibit and Upgrade Alert



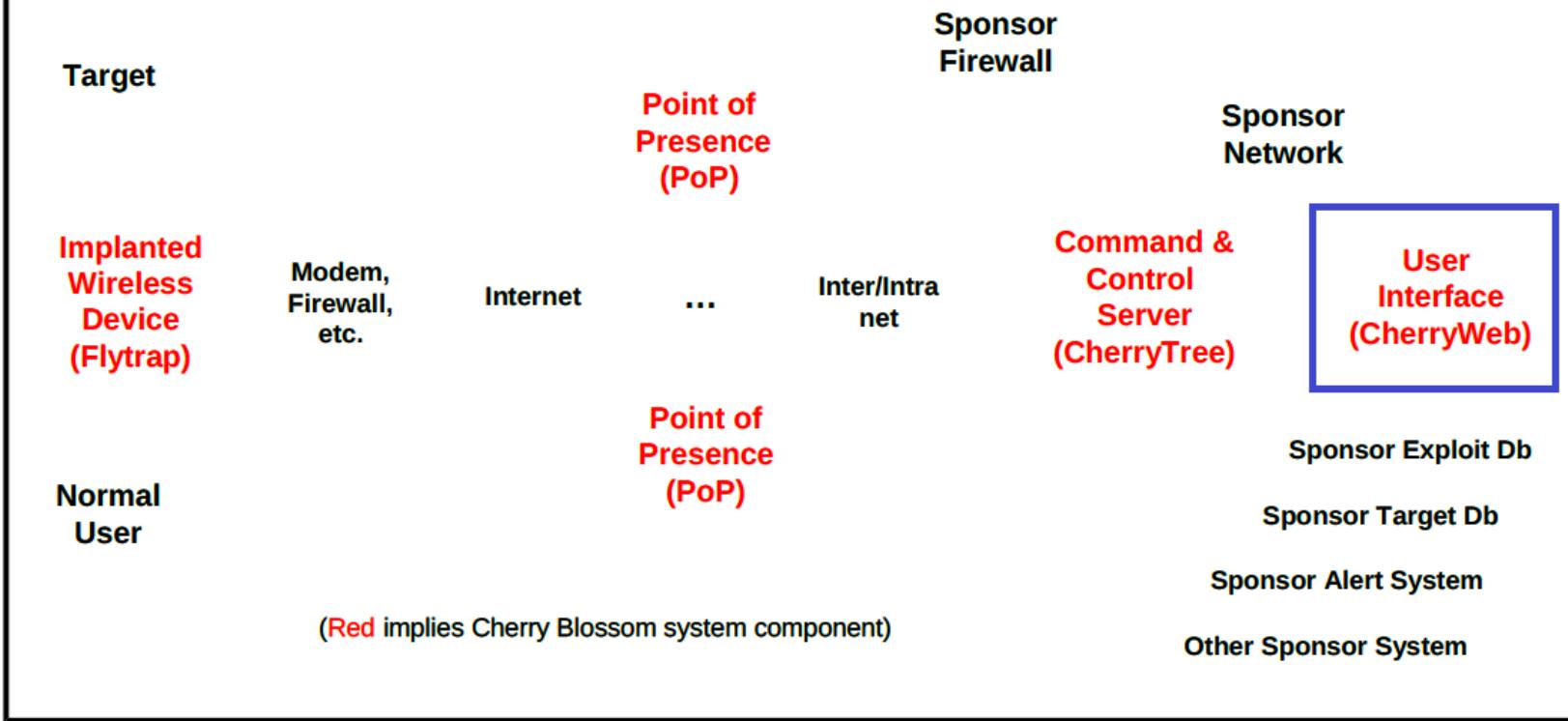
# **Point of Presence (PoP)**

- The *PoP* is a relay that is configured to
  - Properly relay traffic
  - Provide a layer of protection against discovery of the *CT*'s address.



# CherryTree

- **Handling and Persistent Storage of**
  - Beacon Information
  - Alert Information
  - Copy Data
  - Mission



# **CherryWeb**

- **Web Browser User Interface**
- **Display of**
  - Alert Information
  - Flytrap Status
- **Display, Creation, Editing, and Assignment of Missions**

---

# Target Handling

# Target Detection

- Targets are hashed in the Mission
- The Flytrap must
  - parse likely email addresses/chat users/VoIP numbers out of network traffic, and
  - compare the hashes of these emails/chat users/VoIP numbers to the hashed emails/chat users/VoIP numbers in the Mission's Target list.
- Similarly, MAC addresses are also hashed

# Target Tracking

- To monitor a Target and perform Actions
  - a Flytrap must be able to distinguish that Target's network traffic from the network traffic of other users on a per packet basis.
  - MAC address is used for this purpose

# **Target Tracking**

- Each packet of network traffic passing through the Flytrap contains a client MAC address but does not necessarily contain the Target email address/chat user/VoIP number

# **System Operation**

- Implanting a Wireless Device**

There are four methods for getting a Flytrap implant onto a wireless device

- 1.** Use the Device's Firmware Upgrade Web Page over a Wireless (WLAN) Link
- 2.** Use a Wireless Upgrade Package
- 3.** Use the Claymore Tool
- 4.** Use the Device's Firmware Upgrade Web Page over a Wired (LAN) Link

# Preparing for an Initial Beacon

- This is an optional step, but is particularly useful in a supply chain scenario where you want to pre-configure a Flytrap Name/Location/Group/Child Group, and pre-assign a specific Mission to the Flytrap before deployment.

# Create Flytrap

The screenshot shows the Cherry Web interface for creating a new flytrap. On the left, a sidebar menu lists various options under 'Plan' and 'Flytraps'. A red arrow points from the text 'Plan -> Flytraps' to the 'Flytraps' link in the sidebar. Another red oval highlights the 'Create a Flytrap' section in the main content area. A red arrow points from this section to a callout box containing the instructions: 'Enter a Name and a Starter Flytrap from the Plan -> Flytraps page'. The main content area has a title 'Plan Flytraps' and a heading 'Options:'.

**Plan Flytraps**

**Options:**

- **Create a Flytrap**  
Name   
Starter Flytrap Belkin Serial 00:17:3F:40:98:86 Belkin/F5D8231-4/v4/4\_00\_16
- **Edit Flytrap**
- **Delete Flytrap**

Enter a Name and a Starter Flytrap from the Plan -> Flytraps page

Plan ->  
Flytraps

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Current Time: 2010-12-17 18:21:13.241

Figure 6: Cherry Web Plan -> Flytraps Page (Create)

# Add Flytrap

Cherry Blossom  
Version 4.0 (svn 8275)

Overview  
View  
Alerts  
Windex Alerts  
Upgrade Alerts  
Target Activity  
Flytraps  
Deployments  
Missions  
Target Decks  
Copy Data  
VPN Data  
Harvest Data  
Location Data  
Diagnostic Data

Plan  
Flytraps  
Targets  
Target Decks  
Exploits  
Windex  
VPN Link/Proxy

Flytrap Applications  
Mission File  
Execute Command

PoP(s)  
Missions

Assign  
Mission to Flytraps  
Flytrap Kill

Administrator  
Customers  
Permissions  
Users  
Catapult

**Add Flytrap**

- [NewFlytrap](#)

Base Flytrap  
NewFlytrap 00:17:3F:XX:XX:XX Belkin/F5D8231-4/v4/4\_00\_16  (will loose edits if applied)

Name	Location	Group	Child Group
NewFlytrap	SLO		

WLAN MAC = 00:17:3F:XX:XX:XX  
LAN MAC = 00:17:3F:XX:XX:XX

Make/Model/HW/FW = Belkin/F5D8231-4/v4/4\_00\_16

Estimated Initial Beacon Date = 17 Dec 2010

Next Mission = [M Test 1 \(Active\)](#)

M Test 1 (Active)

[Back to Plan Flytraps](#)

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111 Current Time: 2010-12-17 18:22:05.322

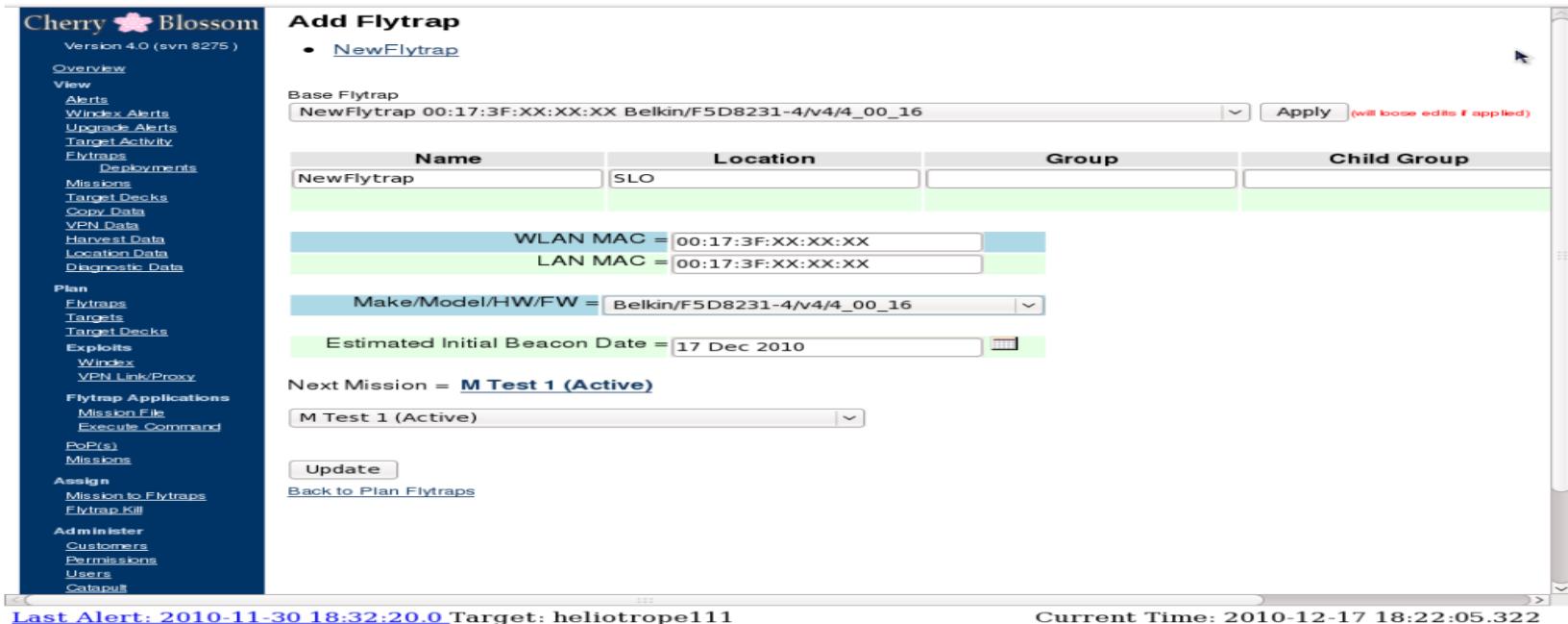


Figure 7: Cherry Web Add Flytrap Page

# Checking Flytrap Status

The screenshot shows the Cherry Blossom web interface. On the left, a sidebar menu lists various options like View, Alerts, Windex, Upgrades, Target Activity, Flytraps, Missions, etc. A red arrow points from the text "View -> Flytraps" to the "Flytraps" link in the sidebar. Another red arrow points from the text "Click on a Flytrap link to see the Flytrap Details page" to a specific row in the main table, which is highlighted with a red oval.

**Flytrap Overview**

Name	Location	In Com	VPN Link	Harvest Data	Current Mission
Belkin Serial 00:17:3F:40:98:86	SLO	No	N/A	View	M Test 1
cb-vpn PoP 192.12.16.81 LAN=00:1D:7E:DC:2A:69	SLO	No	N/A	N/A	cb-vpn 192.12.16
CPE0450_8C:A2 LAN=00:24:A1:7D:8C:A2		No	N/A	N/A	at-35
CPEi775 LAN=00:23:EE:1D:58:6F		No	N/A	N/A	at-35
CPEo450_9E:09 00:21:80:F0:9E:09		No	N/A	N/A	None
CW_1 LAN=00:24:A1:68:41:3A		No	N/A	View	ORT-5.1
CW_2 LAN=00:24:A1:7C:F5:CA		No	N/A	N/A	ORT-5.15
FT3 00:13:10:44:98:AD	SLO	No	Down	N/A	S test zakura VP
J Serial 320N 68:7F:74:29:4B:AA	Scott Office	No	Down	N/A	S test vpnlink glc
Little Bird-750 LAN=00:1E:46:1D:79:02		No	Down	N/A	S test vpnlink glc
M KIT Belkin 00:17:3F:40:01:7C	SLO	Killed	N/A	View	Kill M KIT Belkin
M KIT Linksys WRT300N v2 00:18:39:90:18:C4	SLO	Killed	N/A	View	Kill M KIT Linksys
M KIT WRT54GL 00:25:9C:47:73:F5	SLO	No	N/A	View	M Test 1
SlimBoyFlyTrap 00:25:9C:3B:D3:5B	Firebaugh, CA	No	N/A	View	GlobalShield
SLO flower LAN=00:1E:46:1D:79:14		No	Down	View	S test zakura VP
test planned ft LAN=00:24:A1:00:00:00		No	N/A	N/A	None
00:22:B0:C8:E0:07		No	N/A	N/A	default passive lo
77:77:77:77:77:77		No	N/A	N/A	ORT-5.4
99:99:99:99:99:99	81.3.110.8	No	N/A	N/A	default passive lo
LAN=00:1E:46:1C:DF:42		No	N/A	N/A	default passive lo

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111      Current Time: 2010-12-17 17:46:42.221

Figure 8: CherryWeb View -> Flytraps Page

# Flytrap Details

**Flytrap Information**

**Flytrap Details**

**Mission Information**

**Status Information**

**Security Information**

**Capabilities**

**Collected Data**

**Status History**

**Security History**

The screenshot displays the 'Flytrap Details' page for a device named 'Cherry Blossom'. The page is organized into several sections:

- Flytrap Information:** A sidebar on the left containing links for View, Wireless Alerts, Target Actions, Reports, Beacons, Status, Applications, Scripts, Execute Command, DiffX, and Administer.
- Flytrap Details:** The main content area, which is further divided into tabs:
  - General Information:** Shows details like ID (25), Name (J Serial 320N), Location (Scott Office), and Child Device (Wireless LAN MAC: 68:7F:74:29:4B:AA).
  - Status Information:** Displays current status (Date: 2010-12-13 17:42:55.0, WAN MAC: 68:7F:74:29:4B:AA), LAN IP (192.168.1.1), LAN Netmask Bits (24), and WAN Netmask Bits (0).
  - Beacon IP (Internal):** Shows Max Actions (32), Max Retries (10), Software Uptime (9 Secs), Hardware Uptime (1 Hour 3 Mins 23 Secs), and Password (admin).
  - Mission Management:** Lists SVN Revision (8141), PoP IP Address (24.176.227.182), and Diagnostic (View). It also indicates Catapult Notified (Connection Error).
- Mission Information:** Details the current mission (S-test vpnlink\_global) and its execution status (Executing Since: 2010-12-13 17:42:55.0).
- Security Information:** Lists security parameters including Security Date (2010-12-13 17:42:55.0), Security Type (None), WEP Key Index (1), WEP Key 2 (00000000000000000000000000000000), WEP Key 3 (00000000000000000000000000000000), WEP Key 4 (00000000000000000000000000000000), WPA Pre-Shared Key (00000000000000000000000000000000), WPA Radius Server IP (0.0.0.0), and WPA Crypto Type (TKIP).
- Capabilities:** Lists various capabilities such as Firmware Inhibit (No), VPN Link (Yes), VPN Proxy (Yes), VPN Encryption (Blowfish), VoIP (No), Location (No), and FW Version String (No).
- Collected Data:** Shows data from Windex, Firmware Upgrade Alerts, Diagnostic, Harvest, Corp, and VPN.
- Status History:** A table showing hardware and software uptime, SSID, password, and address for specific dates.
- Security History:** A table showing security history with columns for Date, Security Type, WEP Key Index, WEP Keys, WPA Pre-Shared Key, WPA Radius Key, WPA Radius Server IP, and WPA Crypto Type.

Figure 9: Cherry Web Flytrap Details Page

# Deployed Flytraps

**Cherry Blossom**  
Version 4.0 (svn 8275)

**Deployed Flytraps**

<< < 1 > >>

Name	Wireless LAN MAC	Init. Beacon Received	Init. Beacon Date	Catapult Notified	Last Beacon
M KIT WRT54GL	00:25:9C:47:73:F5	Yes	29 Jun 2010	N/A	SIMPLY
Little Bird-750	LAN=00:1E:46:1D:79:02	Yes	29 Jun 2010	N/A	
(no name)	77:77:77:77:77:77	Yes	30 Jun 2010	N/A	
(no name)	99:99:99:99:99:99	Yes	30 Jun 2010	N/A	8/10/2010
CW_1	LAN=00:24:A1:68:41:3A	Yes	08 Jul 2010	N/A	
SLO flower	LAN=00:1E:46:1D:79:14	Yes	21 Jul 2010	N/A	
FT3	00:13:10:44:98:AD	Yes	22 Jul 2010	N/A	SIMPLY
test planned ft	LAN=00:24:A1:00:00:00	No	22 Jul 2010 (est.)	N/A	
Belkin Serial	00:17:3F:40:98:86	Yes	23 Jul 2010	N/A	SIMPLY
M KIT Belkin	00:17:3F:40:01:7C	Yes	13 Aug 2010	N/A	SIMPLY
(no name)	LAN=00:1E:46:1C:DF:42	Yes	25 Aug 2010	N/A	
CPEi775	LAN=00:23:EE:1D:58:6F	Yes	02 Sep 2010	N/A	
CPE0450 - 8C:A2	LAN=00:24:A1:7D:8C:A2	Yes	03 Sep 2010	N/A	
CPEo450 - 9E:09	00:21:80:F0:9E:09	No	03 Sep 2010 (est.)	N/A	
cb-vpn PoP 192.12.16.81	LAN=00:1D:7E:DC:2A:69	Yes	03 Sep 2010	N/A	SIMPLY
MKIT Linksys WRT300N v2	00:18:39:90:18:C4	Yes	16 Sep 2010	N/A	SIMPLY
J Serial 320N	68:7F:74:29:4B:AA	Yes	03 Dec 2010	Connection Error	SIMPLY
CW_2	LAN=00:24:A1:7C:F5:CA	Yes	04 Oct 2010	N/A	
(no name)	00:22:B0:C8:E0:07	Yes	26 Oct 2010	N/A	
SlimBoyFlyTrap	00:25:9C:3B:D3:5B	Yes	30 Nov 2010	Connection Error	FIREWALL

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Current Time: 2010-12-17 17:47:06.672

Figure 10: Cherry Web View -> Flytraps -> Deployments Page

# The Default Mission

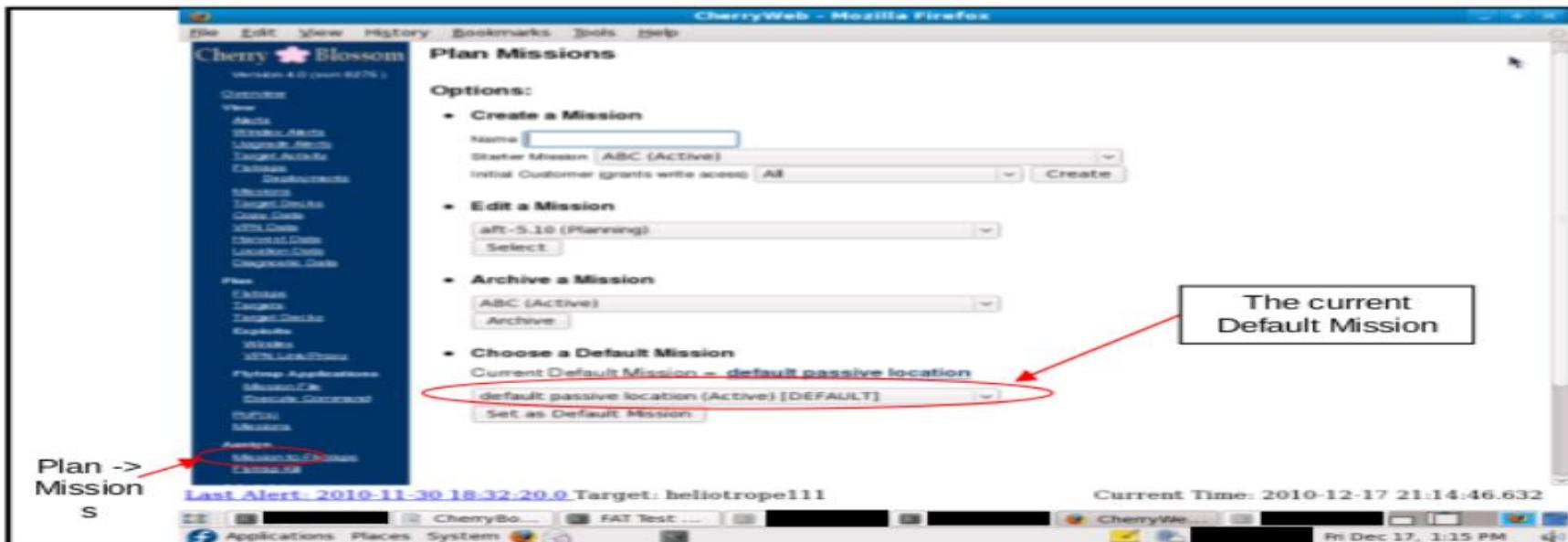


Figure 13: Cherry Web Plan -> Missions Page

# Planning a Mission

- Step 1: Define Targets
- Step 2: Create Target Deck(s)
- Step 3: Define Windex (Browser Redirect) and VPN Link/Proxy Exploits
- Step 4: Define Mission Files (for Application Execution)
- Step 5: Define Execute Commands (for Application Execution)
- Step 6: Define PoPs
- Step 7: Create a New Mission
- Step 8: Edit Operation Ownership of Mission (Mission Workflow 1)
- Step 9: Edit Mission Support Parameters (Mission Workflow 2)
- Step 10: Add Target Decks (Mission Workflow 3)
- Step 11: Override Target Actions (Mission Workflow 4)
- Step 12: Add Mission Files (Mission Workflow 5)
- Step 13: Add Execute Commands (Mission Workflow 6)
- Step 14: Add FW Version Replacement String (Mission Workflow 7)
- Step 15: Add PoPs (Mission Workflow 8)
- Step 16 (Optional): Set Suicide Properties
- Step 17: Review the Mission

# Step 1: Define Targets

The screenshot shows the Cherry Blossom web interface. On the left is a sidebar menu with various options like Overview, View, Alerts, Windex Alerts, Upgrade Alerts, Target Activity, Flytraps, Deployments, Missions, Target Decks, Copy Data, VPN Data, Harvest Data, Location Data, Diagnostic Data, Plan, Flytraps, Targets, Target Decks, Exploits, Windex, VPN Link/Proxy, Flytrap Applications, Mission File, Execute Command, PoC(s), Missions, Assign, Mission to Flytraps, Flytrap Kill, Administer, Customers, Permissions, Users, Catalog, and Windex Connection. A red arrow points from the text "Plan -> Targets" to the "Targets" link in the sidebar.

The main area is titled "Create a Target". It has fields for "Target Type" (set to "email") and "Name" (with a dropdown for "tel: Translation" set to "None"). Below these is a note: "Note: Target names are case insensitive".

A table titled "Targets" lists 24 entries:

ID	Name	Type	Missions
25	00118475766037	VoIP	Missions
190	00:01:02:03:04:05	MAC	Missions
194	00:01:02:03:04:06	MAC	Missions
186	00:0B:97:29:B7:5D	MAC	Missions
187	00:D6:60:CD:7E:B0	MAC	Missions
20	00:0E:0B:2B:41:6D	MAC	Missions
15	00:11:22:33:44:55	MAC	Missions
30	00:12:3F:11:22:33	MAC	Missions
183	00:18:8B:CB:B3:BB	MAC	Missions
184	00:18:8B:CB:B3:BC	MAC	Missions
18	00:1D:7E:DC:2A:69	MAC	Missions
31	00:1E:65:F2:0F:B0	MAC	Missions
7	00:1E:65:F2:DB:D8	MAC	Missions
21	00:21:70:B8:B2:B3	MAC	Missions
17	00:21:86:61:4B:AA	MAC	Missions
2	00:24:7E:DE:9A:BA	MAC	Missions
26	0118475766037	VoIP	Missions
16	11:22:33:44:55:66	MAC	Missions
191	12345678901234567	Chat	Missions
27	18475766037	VoIP	Missions
19	6517553037	VoIP	Missions
29	838475766037	VoIP	Missions
24	8475764548	VoIP	Missions

At the bottom, it says "Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope11" and "Current Time: 2010-12-17 18:23:51.357".

Figure 14: Cherry Web Plan -> Targets Page

# Step 2: Create Target Deck(s)

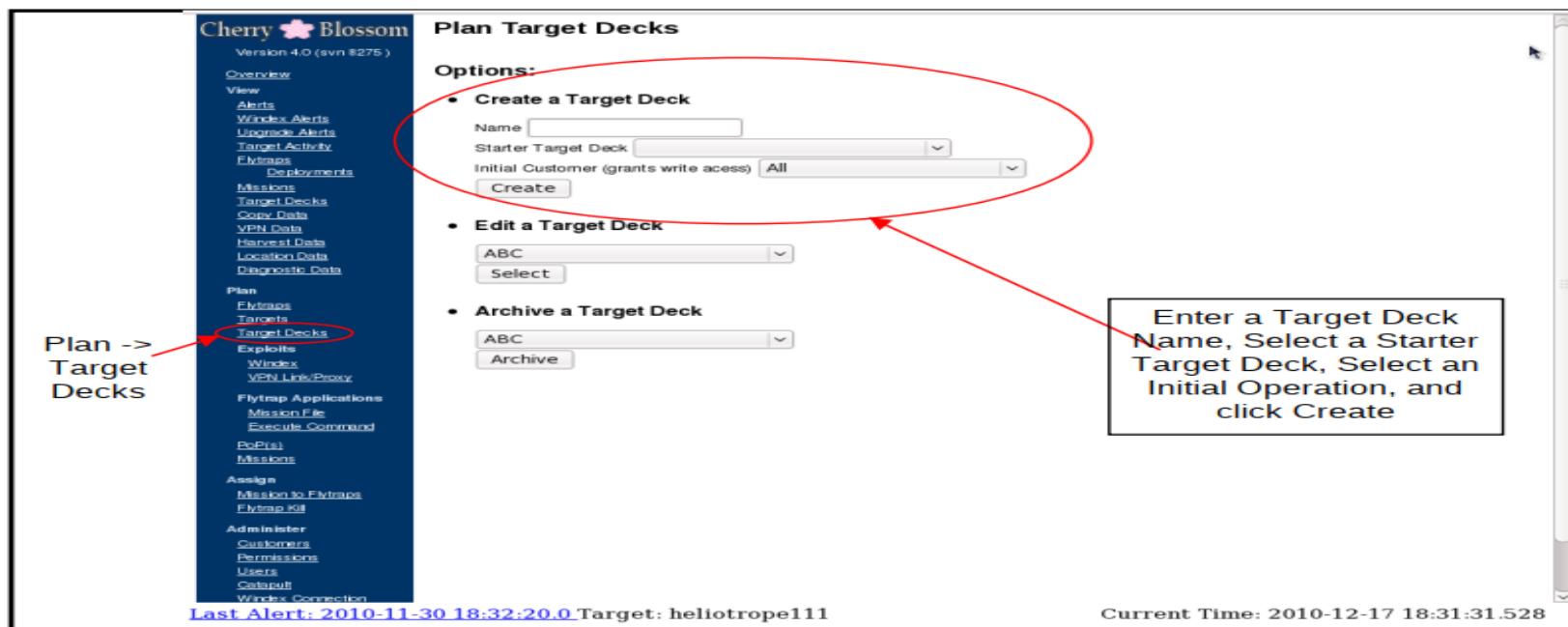


Figure 15: Cherry Web Plan -> Target Decks Page

# Step 3: Define Windex (Browser Redirect) and VPN Link/Proxy Exploits

The screenshot shows the Cherry Blossom web interface. On the left, a sidebar menu lists various sections: Overview, View, Alerts, Windex Alerts, Upgrade Alerts, Target Activity, Flytraps, Deployments, Missions, Target Decks, Copy Data, VPN Data, Historical Data, Location Data, Diagnostic Data, Plan, Flytraps, Targets, Target Decks, Exploits, Windex, and VPN Link/Proxy. A red arrow points from the 'Exploits' link to the 'Windex' link. Below the sidebar, a message says 'Plan -> Exploits -> Windex'. At the bottom of the sidebar, it says 'Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111'. The main content area is titled 'Create a Windex URL' and contains fields for 'Name:' and 'URL:' with a 'Create' button. Below this is a table titled 'Windex URLs' with columns 'Id', 'Name', and 'URL'. The table lists six entries:

Id	Name	URL
3	Random Website ( <a href="#">edit name</a> )	<a href="http://www.camelporn.org">http://www.camelporn.org</a>
4	WFW (website for wankers) ( <a href="#">edit name</a> )	<a href="http://www.wankers..org">http://www.wankers..org</a>
5	ZZZ Website ( <a href="#">edit name</a> )	<a href="http://www.zipnada.org">http://www.zipnada.org</a>
1	asdf website ( <a href="#">edit name</a> )	<a href="http://www.asdf.com">http://www.asdf.com</a>
2	calpoly website ( <a href="#">edit name</a> )	<a href="http://www.calpoly.edu">http://www.calpoly.edu</a>
7	m end-to-end ( <a href="#">edit name</a> )	<a href="http://10.1.1.77:8181?promo_code=1Z45RDJ">http://10.1.1.77:8181?promo_code=1Z45RDJ</a>
6	yyy website ( <a href="#">edit name</a> )	<a href="http://www.Yme.net">http://www.Yme.net</a>

At the bottom right, it says 'Current Time: 2010-12-17 18:41:39.89'.

Figure 21: Cherry Web Plan -> Exploits -> Windex Page

# Step 3: Define Windex (Browser Redirect) and VPN Link/Proxy Exploits

The screenshot shows the Cherry Blossom web interface. On the left, a sidebar menu lists various sections: Overview, View (Alerts, Windex Alerts, Upgrade Alerts, Target Activity, Exploits, Deployments, Missions, Target Decks, Copy Data, VPN Data, Harvest Data, Location Data, Diagnostic Data), Plan (Exploits, Targets, Target Decks, Exploits, Windex, VPN Link/Proxy), Flytrap Applications (Mission File, Execute Command, PoPs), Missions, Assign (Mission to Flytraps, Flytrap Kill), and Administer (Customers, Permissions, Users, Catalog, Windex Connection). A red arrow points from the text "Plan -> Exploits -> VPN Link/Proxy" to the "VPN Link/Proxy" link in the sidebar. The main content area is titled "Add a VPN Server for 'VPN Link' or 'VPN Proxy All' actions". It features input fields for "Proxy Name", "Proxy Address", and "Port" (set to 80), and a "Create" button. Below these is a table titled "VPN Servers" with columns "Id", "Name", "Address", and "Port". The table contains four entries:

Id	Name	Address	Port
4	Fast (edit name)	192.168.1.197	80
2	slo (edit name)	192.12.16.81	80
1	slo dsl (edit name)	70.237.151.14	80
3	zakura vpn (temporary) (edit name)	24.176.227.182	80

At the bottom of the page, there is a "Last Alert" message: "Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111" and a "Current Time" message: "Current Time: 2010-12-17 18:44:34.294".

Figure 22: Cherry Web Plan -> Exploits -> VPN Link/Proxy Page

# Step 4: Define Mission Files (for Application Execution)

The screenshot shows the Cherry Web interface with the following navigation path highlighted:

Plan ->  
Flytrap Applications ->  
Mission File

A red arrow points from the "Mission File" link in the sidebar to the "Mission File" link in the main content area.

**Import Mission File**

Upload a Mission File:  
File:    
File Compatibility: Universal

Upload Action: Retain

**Available Mission File(s)**

File Name	File Compatibility	Download	Last Modified
vpn	Universal	<input type="button" value="download"/>	2010-12-02 22:40:03.0
test.txt	Universal	<input type="button" value="download"/>	2010-07-07 19:27:29.0
max_file_size_is_1010135	Unknown/Unknown/Unknown/Unknown	<input type="button" value="download"/>	2010-07-23 18:53:09.0
max_file_name_length_32_pass	pass	<input type="button" value="download"/>	2010-07-23 18:53:41.0
shellid_GL	Linksys/WRT54G(L)/v4(1)/4_30_11_ETS1	<input type="button" value="download"/>	2010-09-19 20:55:03.0
shellid_300	Linksys/WRT300N/v2/2_00_08	<input type="button" value="download"/>	2010-09-19 22:42:11.0
dumbbellid_belkin	Belkin/F5D8231-4/v4/4_00_16	<input type="button" value="download"/>	2010-11-30 01:45:53.0

<< < 1 > >>

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111 Current Time: 2010-12-17 18:53:45.834

Figure 23: Cherry Web Plan -> Flytrap Applications -> Mission File Page

# Step 5: Define Execute Commands (for Application Execution)

The screenshot shows the Cherry Web interface with a sidebar on the left and a main content area on the right.

**Left Sidebar (Plan -> Flytrap Applications -> Execute Command):**

- Version 4.0 (svn 8275)
- Overview
- View
- Alerts
- Windows Alerts
- MacOSX Alerts
- Target Activity
- Flytraps
- Deployments
- Missions
- Target Decks
- Copy Data
- VPN Data
- Harvest Data
- Location Data
- Diagnostic Data
- Plan
- Flytraps
- Targets
- Target Decks
- Exploits
- Windex
- VPN Link/Prom
- Flytrap Applications

  - Mission File
  - Execute Command** (highlighted with a red oval)
  - PoPs
  - Missions
  - Assign
  - Mission to Flytraps
  - Flytrap Kill

- Administrator
- Customers
- Permissions
- Users
- Catapult

**Main Content Area:**

### Create a new command to execute on a Flytrap

Create a Execute Command:  
Name:   
Execution Compatibility:  (dropdown menu)  
Command: (escaped characters or new lines are not supported)

### Available Mission Command(s)

Name	Command
vpn	vpn u 23232 genREMOTEADDR genREMOTEPORT genCLIENTCSUBN
Universal	
ABC	echo "Hello World!" > /dev/null
Universal	
shellid	shellid -p 12345
Linksys/WRT54G(L)/v4(1)/4_30_11_ETS1	
shellid_GL port 2112	shellid_GL -p 2112
Linksys/WRT54G(L)/v4(1)/4_30_11_ETS1	
echo universal	echo "Fetznrausch" > /tmp/tmp.txt
Universal	
killall GL shellid	killall shellid_GL
Linksys/WRT54G(L)/v4(1)/4_30_11_ETS1	
shellid_300 port 2112	shellid_300 -p 2112
Linksys/WRT300N/v2/2_00_08	
dumbbellid_belkin port 2112	dumbbellid -p 2112
Belkin/F5D8231-4/v4/4_00_16	
nat 80 to 8104	iptables -t nat -R PREROUTING 3 -p tcp -d 192.16.81 --dport 80 -j DNAT
Linksys/WRT54G(L)/v4(1)/4_30_11_ETS1	
nat 8080 to 8104	iptables -t nat -R PREROUTING 4 -p tcp -d 192.16.81 --dport 8080 -j DNAT
Linksys/WRT54G(L)/v4(1)/4_30_11_ETS1	

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111      Current Time: 2010-12-17 18:54:25.776

Figure 24: Cherry Web Plan -> Flytrap Applications -> Execute Command Page

# Step 6: Define PoPs

Cherry Blossom  
Version 4.0 (rev 4876)

File Edit View History Bookmarks Tools Help

Add a PoP (Point of Presence)

Name: URL or IP Address: Port: 80 Create

PoP(s)

ID	Name	Address	Port
1	Edit "this" [edit name]	0.0.0.0	0
3	ZZWankersAway [edit name]	255.255.255.1	2345
2	zakura dev (8080) [edit name]	24.176.227.182	8080

<<< 1 >>>

Last Alert: 2010-11-30 18:32:20.0 Target: heliotropell1

Current Time: 2010-12-17 18:59:27.853

Plan ->  
PoP(s)

Applications Places System

Fri Dec 17, 10:59 AM

Figure 25: Cherry Web Plan -> PoP(s) Page

# Step 7: Create a New Mission

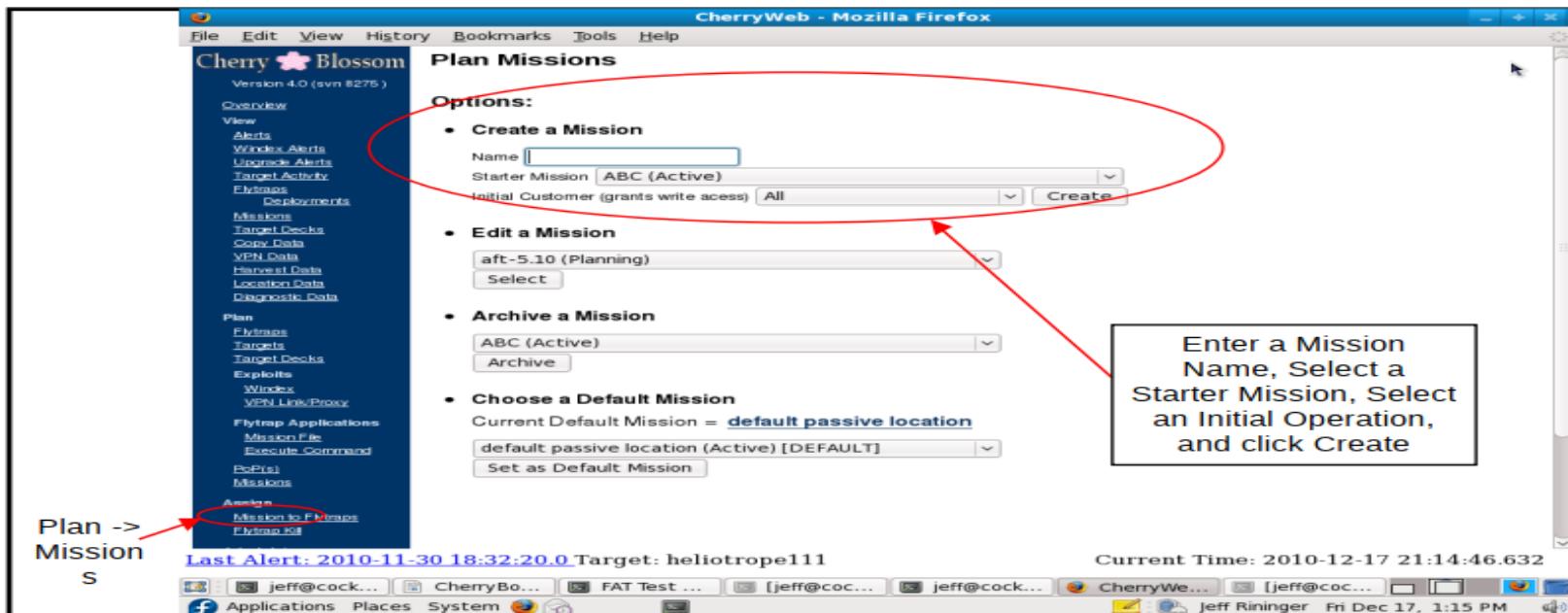


Figure 26: Cherry Web Plan -> Missions Page (Create)

# Step 8: Edit Operation Ownership of Mission (Mission Workflow 1)

Cherry Blossom  
Version 4.0 (svn #275)

**Mission Workflow**

**Mission**  
NewMission

- Customer Ownership
- Support Parameters
- Target Deck(s)
- Target Exploit/Action(s)
- Mission File(s)
- Execute Command(s)
- Firmware Version String(s)
- PoP(s)

- [Suicide Properties](#)
- [Assign Mission to Flytraps](#)

>> Next >>

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Current Time: 2010-12-17 21:16:04.952

Figure 27: Cherry Web Mission Workflow Page

Cherry Blossom  
Version 4.0 (svn #275)

**Customer Ownership** (NewMission)

**Customers**

Create a Customer

Available Customers

Owning Customers

select →  
← deselect

DEFAULT	HarryPotter
	NewCust1
No_data_customer	
Test_3.0.4	
Test_Customer_Id_Crash	
TestCust1	
TestCust2	

Apply Customers

<< Back <<   >> Next >>

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Current Time: 2010-12-17 21:17:33.842

Figure 28: Cherry Web Mission Workflow Operation Ownership Page

# Step 9: Edit Mission Support Parameters (Mission Workflow 2)

Cherry Blossom  
Version 4.0 (svn 8275)

Overview

View

- Alerts
- Windex Alerts
- Upgrade Alerts
- Target Activity
- Flytraps
- Deployments

Missions

- Target Decks
- Copy Data
- VPN Data
- Harvest Data
- Location Data
- Diagnostic Data

Plan

- Flytraps
- Targets
- Target Decks
- Exploits
- Windex
- VPN Link/Proxy

Flytrap Applications

- Mission File
- Execute Command

PoP(s)

- Missions

Assign

- Mission to Flytrap
- Flytrap Kill

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Edit Mission Support Parameters ([NewMission](#))

Mission Name

**Periodic Beacon Parameters**

Interval	Traffic Requirement	Traffic Requirement Timeout	Power Cycle Wait
0 Days 0 Hours 1 Mins 0 Secs	None	N/A Select a Traffic Requirement	0 Days 0 Hours 0 Mins 10 Secs
1 Min to 91 Days			

**Target Monitoring Parameters**

Session Timeout	Target Monitoring
0 Days 0 Hours 5 Mins 0 Secs	No N/A Select Target Moni
30 Secs to 1 Day	

**Filter Parameters**

Port Scanning	Protocol Scanning	Remove AcceptEncoder
Scan All Ports	Scan All Protocols	Yes

Current Time: 2010-12-17 21:18:00.239

Figure 29: Cherry Web Mission Support Parameters Mission Workflow Page

# Step 10: Add Target Decks (Mission Workflow 3)

The screenshot shows the 'Target Deck Assignment' page from the Cherry Blossom version 4.0 interface. The left sidebar contains navigation links for Overview, Alerts, Windex Alerts, Upgrade Alerts, Target Activity, Flytraps, Deployments, Missions, Target Decks, Copy Data, VPN Data, Harvest Data, Location Data, Diagnostic Data, Plan, Flytraps, Targets, Target Decks, Exploits, Windex, VPN Link/Proxy, Flytrap Applications, Mission File, Execute Command, PoP's, Missions, Assign, Mission to Flytraps, and Flytrap Kill. The main content area is titled 'Target Deck Assignment (NewMission)'. It features two lists: 'Available' on the left and 'Selected' on the right. The 'Available' list includes items like 'email-chat', 'M Test MAC CF-52', 'M Test Max Targets', 'M Test Suite 1', 'NewTargetDeck', 'NewTargetDeck1', 'ORT-deck', 'ORT-MAC Deck', 'ORT-VOIP Deck', and 'PTF-Cell'. Below these lists is a message stating '1 Target(s) included from selected decks.' followed by a 'Apply Target Decks' button. Navigation buttons for '<< Back <<' and '>> Next >>' are also present. A vertical scrollbar is visible on the right side of the page.

Cherry Blossom  
Version 4.0 (svn 8275)

Overview  
Alerts  
Windex Alerts  
Upgrade Alerts  
Target Activity  
Flytraps  
Deployments  
Missions  
Target Decks  
Copy Data  
VPN Data  
Harvest Data  
Location Data  
Diagnostic Data

Plan  
Flytraps  
Targets  
Target Decks  
Exploits  
Windex  
VPN Link/Proxy

Flytrap Applications  
Mission File  
Execute Command

PoP's  
Missions

Assign  
Mission to Flytraps  
Flytrap Kill

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Target Deck Assignment ([NewMission](#))

**Target Decks**

[Create a Target Deck](#)

**Available**

- email-chat
- M Test MAC CF-52
- M Test Max Targets
- M Test Suite 1
- NewTargetDeck
- NewTargetDeck1
- ORT-deck
- ORT-MAC Deck
- ORT-VOIP Deck
- PTF-Cell

**Selected**

- ABC

→ select ← deselect

1 Target(s) included from selected decks.

[Apply Target Decks](#)

<< Back <<    >> Next >>

Current Time: 2010-12-17 21:18:33.584

Figure 30: Cherry Web Target Deck Assignment Mission Workflow Page

# Step 11: Override Target Actions (Mission Workflow 4)

The screenshot shows the 'Target Exploit/Action Assignment' page for a mission named 'NewMission'. The left sidebar lists various navigation options under categories like Overview, Missions, Plan, and Assign. The main content area displays a table for target assignment. A single target row is present:

Target Name	Type	Copy Action	Copy Timeout	Windex URL
abc@def.com	Email	Disabled	0 Days 0 Hours 0 Mins 0 Sec to 45 Days 12 Hours 15 Mins	asdf website ( <a href="http://www.asdf.c">http://www.asdf.c</a> ) <a href="#">Add an URL</a>

Below the table, it says 'Total targets for the Mission: 1' and 'Total unique actions for Mission: 1'. There is an 'Apply Actions' button and navigation buttons for '<< Back <<' and '>> Next >>'. At the bottom, a status bar shows 'Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope11' and 'Current Time: 2010-12-17 21:19:19.539'.

**Figure 31: Cherry Web Target Exploit/Action Assignment Mission Workflow Page**

# Step 12: Add Mission Files (Mission Workflow 5)

The screenshot shows the 'Mission File Assignment' page from the Cherry Blossom web interface. The left sidebar contains navigation links for Overview, View (Alerts, Windex Alerts, Upgrade Alerts, Target Activity, Flytraps, Deployments), Missions, Target Decks, Copy Data, VPN Data, Harvest Data, Location Data, Diagnostic Data, Plan (Flytraps, Targets, Target Decks, Exploits, Windex, VPN Link/Proxy), Flytrap Applications (Mission File, Execute Command, PoPs), Missions, Assign (Mission to Flytraps, Flytrap Kill), and a Last Alert message.

The main content area is titled 'Mission Files' and includes a 'Mission File Assignment' sub-header. It features a 'Available' list of files:

- dumbbellid\_belkin (MMV = Belkin/F5D8231-4/v4/4\_00\_16 )
- max\_file\_name\_length\_32\_pass (MMV = Unknown/Unknown/Unknown/Unknown )
- max\_file\_size\_is\_1010135 (MMV = Unknown/Unknown/Unknown/Unknown )
- shellid\_300 (MMV = Linksys/WRT300N/v2/2\_00\_08 )
- shellid\_GL (MMV = Linksys/WRT54G(L)/v4(1)/4\_30\_11\_ETSI )
- test.txt (MMV = Universal )

Below the list are 'select' and 'deselect' buttons with right and left arrow icons. At the bottom are 'Apply Mission Files', '<< Back <<', and '>> Next >>' buttons.

At the bottom of the page, the 'Last Alert' is listed as 'Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111' and the 'Current Time' is '2010-12-17 21:20:58.658'.

Figure 32: Cherry Web Mission File Assignment Mission Workflow Page

# Step 13: Add Execute Commands (Mission Workflow 6)

The screenshot shows the 'Execute Command Assignment' page in the Cherry Blossom web interface. The left sidebar contains navigation links for Overview, View (Alerts, Windex Alerts, Upgrade Alerts, Target Activity, Flytraps, Deployments, Missions, Target Decks, Copy Data, VPN Data, Harvest Data, Location Data, Diagnostic Data), Plan (Flytraps, Targets, Target Decks, Exploits, Windex, VPN Link/Proxy), Flytrap Applications (Mission File, Execute Command, PoPs), Missions, and Assign (Mission to Flytraps, Flytrap KI). The main content area is titled 'Execute Commands' and includes a 'Available' list of commands:

```
ABC (MMV = Universal )
dumbbellid_belkin port 2112 (MMV = Belkin/F5D8231-4/v4/4_00_16 )
echo universal (MMV = Universal )
filter forward allow 8104 for128.18.233.81 (MMV = Linksys/WRT54G(L)/v4(1)/4_30_11_ETSI )
killall GL shellid (MMV = Linksys/WRT54G(L)/v4(1)/4_30_11_ETSI )
nat 80 to 8104 (MMV = Linksys/WRT54G(L)/v4(1)/4_30_11_ETSI )
nat 8080 to 8104 (MMV = Linksys/WRT54G(L)/v4(1)/4_30_11_ETSI )
shellid (MMV = Linksys/WRT54G(L)/v4(1)/4_30_11_ETSI )
shellid_300 port 2112 (MMV = Linksys/WRT300N/v2/2_00_08 )
shellid_GL port 2112 (MMV = Linksys/WRT54G(L)/v4(1)/4_30_11_ETSI )
```

Below the list are 'Apply Execute Commands' and '<< Back <<'/'>> Next >>' buttons. A vertical toolbar on the right provides navigation icons: select (right arrow), deselect (left arrow), move up (up arrow), and move down (down arrow).

At the bottom, a status bar shows 'Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111' and 'Current Time: 2010-12-17 21:22:55.116'.

Figure 33: Cherry Web Execute Command Assignment Mission Workflow Page

## Step 14: Add FW Version Replacement String (Mission Workflow 7)

Cherry Blossom  
Version 4.0 (svn 8275 )

Overview  
View  
Alerts  
Windex Alerts  
Upgrade Alerts  
Target Activity  
Flytraps  
Deployments  
Missions  
Target Decks  
Copy Data  
VPN Data  
Harvest Data  
Location Data  
Diagnostic Data

Plan  
Flytraps  
Targets  
Target Decks  
Exploits  
Windex  
VPN Link/Proxy

Flytrap Applications  
Mission File  
Execute Command

PoPs  
Missions

Assign  
Mission to Flytraps  
Flytrap Kill

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Firmware Version String Replacement ([NewMission](#))

Device MMV	Manufacturer's Original FW Version String	Desired FW Version String
Linksys/WRT54G(L)/v4(1) /4_30_11_ESI	v4.30.11	
Linksys/WRT300N/v2/2_00_08	2.00.08	
Belkin/F5D8231-4/v4/4_00_16	F5D8231-4_WW_4.00.16	

[Update](#)

<< Back <<    >> Next >>

Current Time: 2010-12-17 21:23:42.362



Figure 34: Cherry Web Firmware Version String Replacement Mission Workflow Page

# Step 15: Add PoPs (Mission Workflow 8)

Cherry  Blossom  
Version 5.0-test\_seven (svn 8929M)

[Overview](#)  
[View](#)  
[Alerts](#)  
[Windex Alerts](#)  
[Upgrade Alerts](#)  
[Target Activity](#)  
[Flytraps](#)  
[Deployments](#)  
[Missions](#)  
[Target Decks](#)  
[Copy Data](#)  
[VPN Data](#)  
[Harvest Data](#)  
[Location Data](#)  
[Diagnostic Data](#)  
[Plan](#)  
[Flytraps](#)  
[Targets](#)  
[Target Decks](#)  
[Exploits](#)  
[Windex](#)  
[VPN Link/Proxy](#)  
[Flytrap Applications](#)  
[Mission File](#)

**PoP Assignment (CTMissiontest\_tenn.)**

**PoP(s)**

[Add a PoP](#)

**Available**

test pop one (192.168.1.1:80)  
test pop two (192.168.1.2:80)

**Selected**

toughbook\_test (10.1.1.27:8080)

→ select  
← deselect  
↑ move up  
↓ move down

Use Firmware Default PoP(s) in Mission:  No  Yes

[Apply PoP\(s\)](#)

[<< Back <<](#) [>> Next >>](#)

Last Alert: 2012-07-10 22:58:54.0 Target: snakes@scary.gov

Current Time: 2012-07-17 22:04:21.817

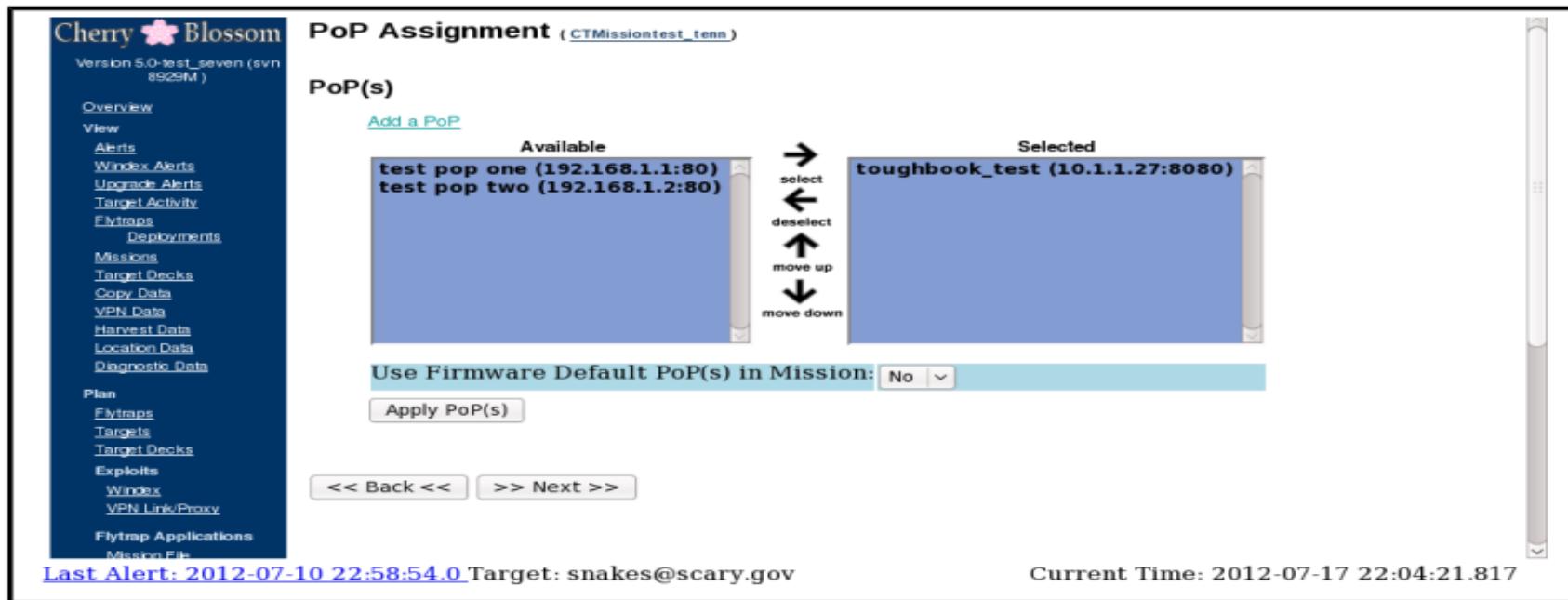


Figure 35: Cherry Web PoP Assignment Mission Workflow Page

# Step 16 (Optional): Set Suicide Properties

The screenshot shows the Cherry Blossom software interface. On the left is a dark sidebar menu with various navigation options. The main area is titled "Suicide Mission Properties" and contains a table with two columns: "Suicide Enabled" and "Suicide Time". The "Suicide Enabled" column has a dropdown menu set to "No". Below the table are "Update" and "Back/Next" buttons. At the bottom of the main area, there are links for "Last Alert" and "Current Time".

**Cherry Blossom**  
Version 4.0 (svn 8275)

[Overview](#)  
[View](#)  
[Alerts](#)  
[Windex Alerts](#)  
[Upgrade Alerts](#)  
[Target Activity](#)  
[Flytraps](#)  
[Deployments](#)  
[Missions](#)  
[Target Decks](#)  
[Copy Data](#)  
[VPN Data](#)  
[Harvest Data](#)  
[Location Data](#)  
[Diagnostic Data](#)

[Plan](#)  
[Flytraps](#)  
[Targets](#)  
[Target Decks](#)  
[Exploits](#)  
[Windex](#)  
[VPN Link/Proxy](#)  
[Flytrap Applications](#)  
[Mission File](#)  
[Execute Command](#)  
[PoPs](#)  
[Missions](#)

[Assign](#)  
[Mission to Flytraps](#)  
[Flytrap Kill](#)

**Suicide Mission Properties** ([NewMission](#))

Suicide Enabled	Suicide Time
No	

[Update](#)

<< Back <<   >> Next >>

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Current Time: 2010-12-17 21:25:41.928

# **Step 17: Review the Mission**

- It is important to review all of the settings for the Mission created
- Necessary changes should be made if needed.

# Assign a Mission to Flytraps

Assign ->  
Mission to Flytraps

Cheny Blossom  
Version 4.0 (swm 8275 )

Overview  
View  
Alerts  
Windows Alerts  
Upgrade Alerts  
Target Activity  
Flytraps  
    Deployments  
Missions  
Target Decks  
Copy Data  
VPN Data  
Harvest Data  
Location Data  
Diagnostic Data

Plan  
Flytraps  
Targets  
Target Decks  
Exploits  
    Windows  
    VPN Link/Proxy

Flytrap  
Applications  
Mission File  
Execute Command  
PoPs  
Missions

Assign  
Mission to Flytraps  
Flytrap Kill

Mission Assignment

Mission: default Harvest frequent beacon (Active) [DEFAULT]

<< < 1 2 3 4 5 > >>

Select	Flytrap	Location	Current Mission	Assigned Mission
<input type="checkbox"/>	Albert-1C:E7:74:00:1E:46:1C:E7:71		Albert T2 Forever	Albert T2 Forever
<input type="checkbox"/>	CB dev server local gw LAN=00:12:17:08:92:E9	greenhouse	Kill CB dev server local gw LAN=00:12:17:08:92:E9	Kill CB dev server local gw LAN=00:12:17:08:92:E9
<input type="checkbox"/>	CB margarita gw LAN=00:1C:F0:C5:1F:65	greenhouse	Kill CB margarita gw LAN=00:1C:F0:C5:1F:65	Kill CB margarita gw LAN=00:1C:F0:C5:1F:65
<input type="checkbox"/>	CW_2 LAN=00:24:A1:7C:F5:CA		test server	test server
<input checked="" type="checkbox"/>	DIR test LAN=00:24:01:42:59:1F		default Harvest frequent beacon	default Harvest frequent beacon
<input type="checkbox"/>	J WRT320N Serial 68:7F:74:29:4B:AA	Lab	M Test 4 Rev. 2	M Test 4 Rev. 2
<input type="checkbox"/>	K Moto 00:0C:10:21:32:01		default	default
<input type="checkbox"/>	M D-link DIR-330 00:1C:F0:F0:6A:3C	SLO	M Test VPN Link	M Test 3 Rev. 2
<input type="checkbox"/>	M KIT Berlin FSD8231-4 v4 00:17:3F:40:01:7C	SLO	S test r7910 web detect copy crash debug 4	M Test 3 Rev. 2
<input type="checkbox"/>	M KIT Linksys WRT300N v2 00:18:39:90:18:C4	SLO	M Test 4 Rev. 2	M Test 3 Rev. 2

<< < 1 2 3 4 5 > >>

Select All

Assign

1. Select Mission
2. Check Flytraps to Assign Mission to
3. Click "Assign" button

Figure 37: Cherry Web Assign -> Mission to Flytraps Page

# Editing Missions

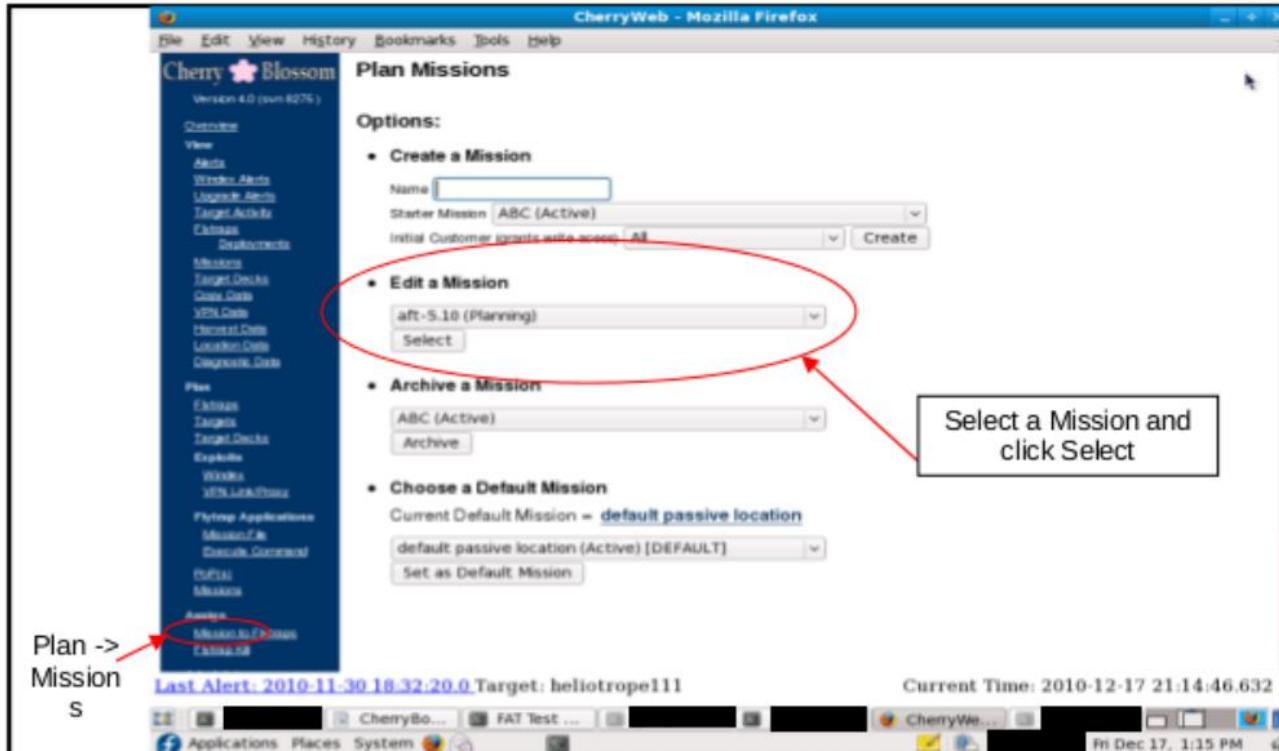


Figure 38: Cherry Web Plan -> Missions Page (Edit)

# Archiving Missions

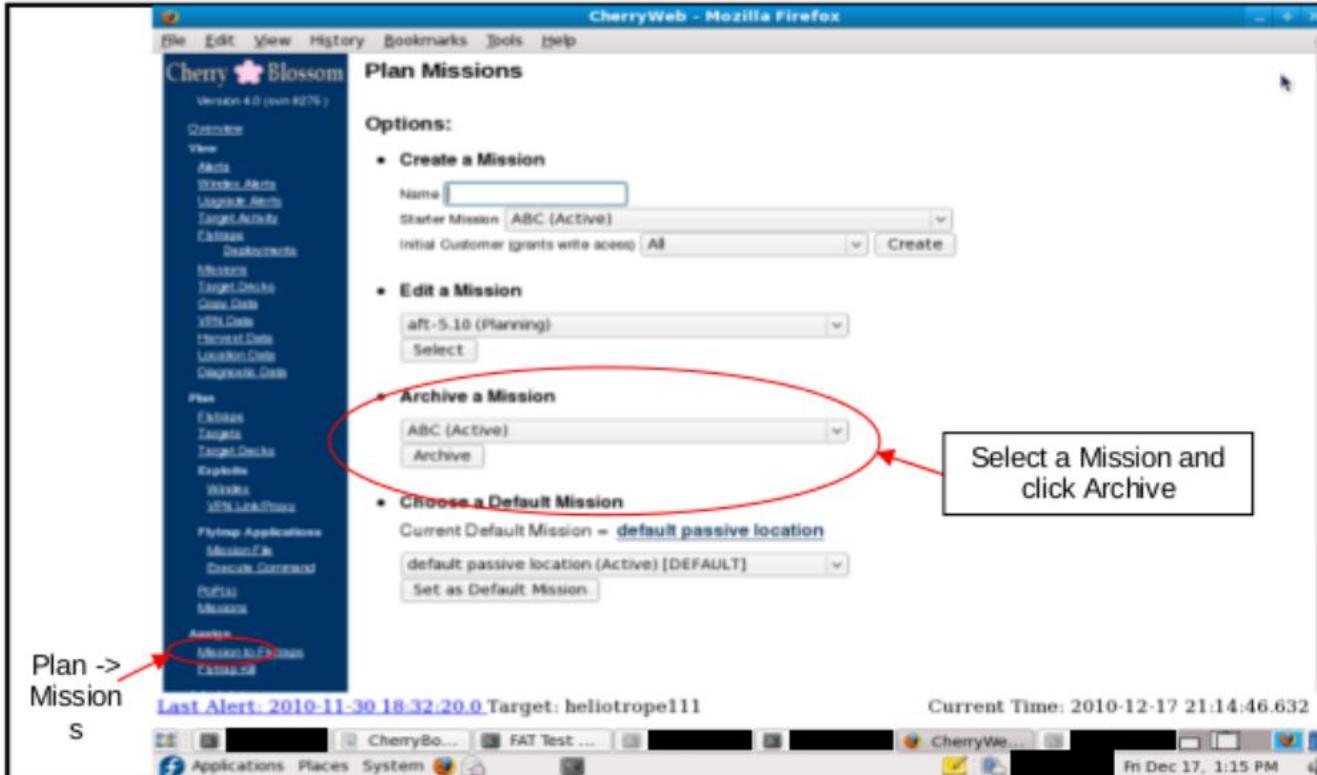


Figure 39: Cherry Web Plan -> Missions Page (Archive)

# **Mission States**

- Planning
- Active
- Archived

# Setting the Default Mission

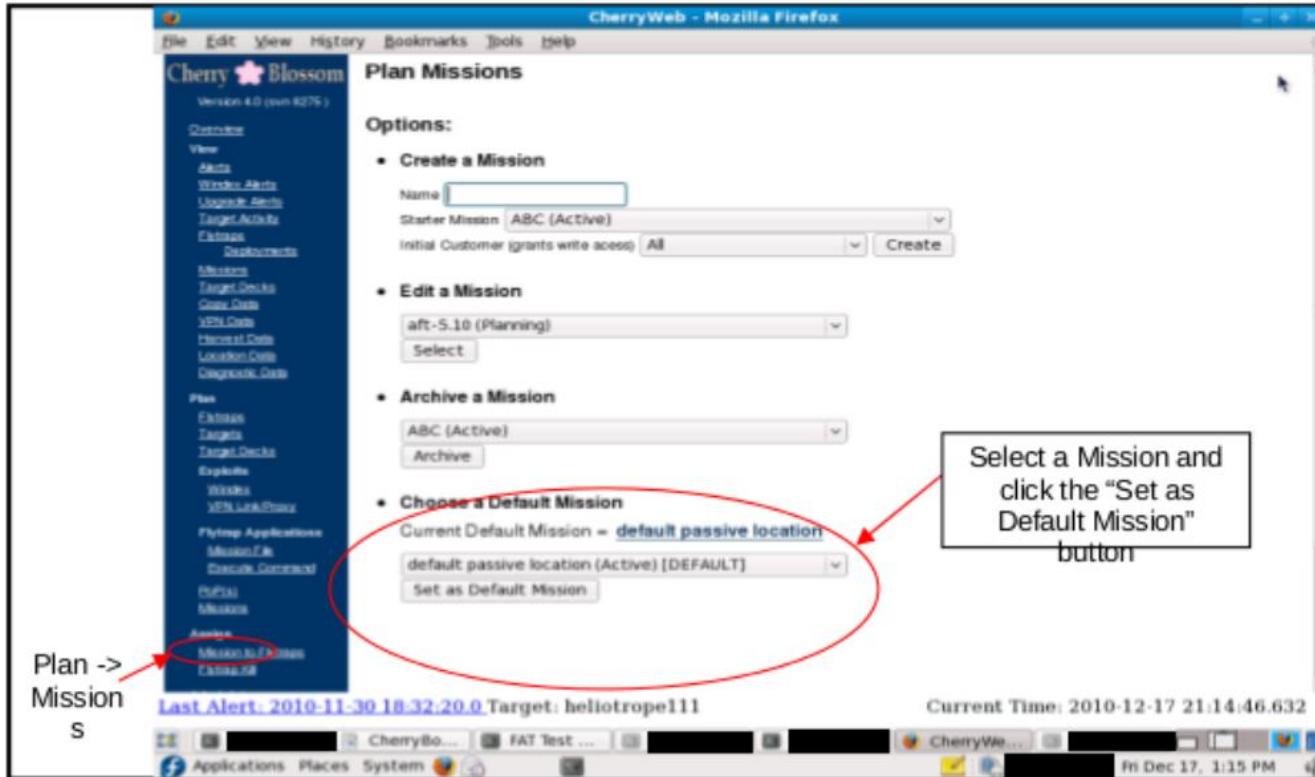


Figure 40: Cherry Web Plan -> Missions Page (Choose Default Mission)

# Editing Target Decks

The screenshot shows the 'Plan Target Decks' page from the Cherry software. On the left is a navigation sidebar with a tree structure:

- Cherry Blossom Version 4.0 (svn 8275)
  - Overview
  - View
    - Alerts
    - Windex Alerts
    - Upgrade Alerts
    - Target Activity
    - Flytraps
    - Deployments
  - Missions
    - Target Decks
    - Copy Data
    - VPN Data
    - Harvest Data
    - Location Data
    - Diagnostic Data
  - Plan
    - Flytraps
    - Targets
    - Target Decks** (highlighted with a red oval)
    - Exploits
    - Windex
    - VPN Link/Proxy
  - Flytrap Applications
    - Mission File
    - Execute Command
    - PoPs
    - Missions
  - Assign
    - Mission to Flytraps
    - Flytrap Kill
  - Administrator
    - Customers
    - Permissions
    - Users
    - Catapult
    - Windex Connection

A red arrow points from the text 'Plan -> Target Decks' to the 'Target Decks' link in the sidebar.

The main content area is titled 'Plan Target Decks' and contains the following sections:

- Options:**
  - Create a Target Deck**: Fields for Name, Starter Target Deck (dropdown), Initial Customer (dropdown), and a 'Create' button.
  - Edit a Target Deck**: A dropdown menu showing 'ABC' with a 'Select' button below it. This section is circled with a red oval and has a red arrow pointing to it from the sidebar.
  - Archive a Target Deck**: A dropdown menu showing 'ABC' with an 'Archive' button below it.

A callout box with a black border and white text says: "Select a Target Deck, and click Select".

At the bottom of the page, there are two status messages: "Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111" and "Current Time: 2010-12-17 18:31:31.528".

Figure 41: Cherry Web Plan -> Target Decks Page (Edit)

# Assign a Kill Mission

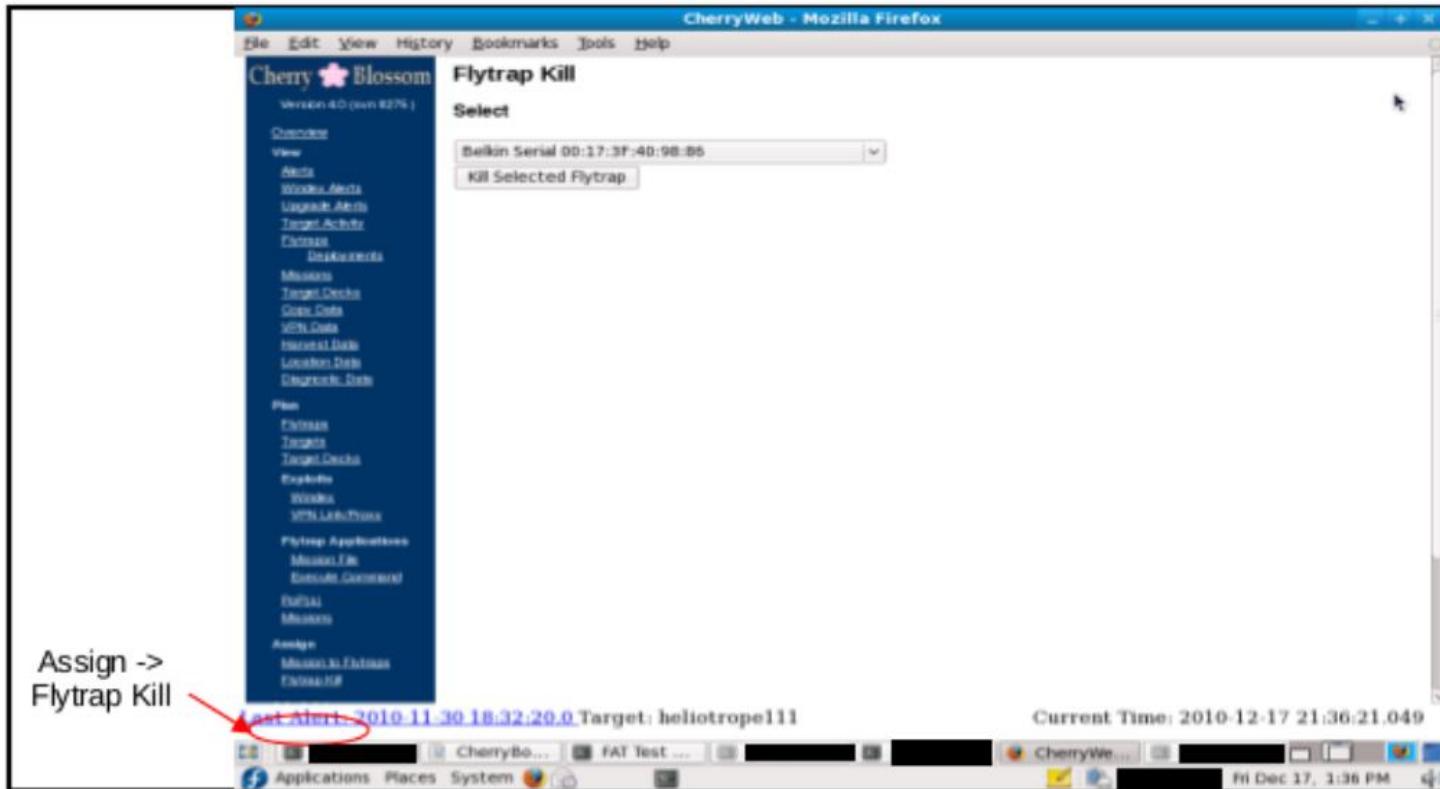


Figure 42: Cherry Web Assign -> Flytrap Kill Page

# Viewing Alerts

The screenshot shows the Cherry Blossom web interface with a sidebar menu on the left and a main content area on the right.

**Left Sidebar (Menu):**

- Cherry Blossom Version 4.0 (svn 8278)
- Customize
- View
  - Alerts (highlighted with a red circle and arrow)
  - Derived Alerts
  - Unpack Alerts
  - Target Alerts
  - Fileless
  - Downloads
  - Memory
  - Target Decks
  - Case Data
  - Windex
  - Execution Data
  - Location Data
  - Diagnostic Data
- Plan
  - Fileless
  - Targets
  - Decks
  - Target Decks
  - Exploits
  - Windex
  - Windex Data
- Fileless Applications
- Message UI
- Execute Command
- HTTP
- Memory
- Assign
- Memory to Database
- External
- Administrator
- Customize
- Remember
- Home
- Logout

**Main Content Area:**

## Alerts

Show Alerts for Derived Targets

<< < 1 2 3 4 5 6 7 > >>

Target	Session	Active	Last Activity	Windex	Alert	Copy Data	Client MAC	Client IP
smith_test2@hotmail.com	No		2010-09-30 18:47:28.0	No Data	00:0D:60:CD:7E:B0	192.	192.168.1.10	192.168.1.10
z100@testing.com	N/A		2010-09-28 18:54:36.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10
smith_test2@hotmail.com	No		2010-09-28 17:51:52.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10
smith_test1@yahoo.com	No		2010-09-28 17:15:13.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10
smith_test2@hotmail.com	No		2010-09-28 17:15:13.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10
abc@def.com	No		2010-09-28 16:29:34.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10
smith_test2@hotmail.com	No		2010-09-28 16:29:34.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10
smith_test3@maktoob.com	No		2010-09-28 16:29:34.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10
00:21:70:B8:B2:B3	No		2010-09-28 16:29:34.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10
smith_test2@hotmail.com	No		2010-09-28 16:29:34.0	No Data	00:21:70:B8:B2:B3	192.	192.168.1.10	192.168.1.10

<< < 1 2 3 4 5 6 7 > >>

Last Alert: 2010-09-17 23:26:20.0 Target: space@test.com      Current Time: 2011-01-03 17:24:51.987

Figure 43: Cherry Web View -> Alerts Page

# Viewing Target Activity

**View -> Target Activity**

Target	Session Active	Name	Location	Client MAC	Alert Actual Date
zakura.test@gmail.com	N/A	CW_2	D8:D3:85:99:1B:C5	2010-10-13 19	
zakura.test@gmail.com	N/A	M KIT Belkin	SLO	00:1E:65:F2:0F:B0	2010-11-29 22
zakura.test@gmail.com	N/A	M KIT Linksys WRT300N v2	SLO	00:1E:65:F2:0F:B0	2010-11-25 01
test@testing.com	N/A	Belkin Serial	SLO	00:24:7E:DE:9A:BA	2010-07-26 16
test@testing.com	N/A	M KIT WRT54GL	SLO	00:1E:65:F2:0F:B0	2010-11-03 21
test002@testing.com	N/A	M KIT Linksys WRT300N v2	SLO	00:1E:65:F2:0F:B0	2010-11-29 17
test001@testing.com	N/A	M KIT Belkin	SLO	00:1E:65:F2:0F:B0	2010-11-30 02
test001@testing.com	N/A	M KIT WRT54GL	SLO	00:1E:65:F2:0F:B0	2010-11-08 21
smith test4@gawab.com	N/A	M KIT Belkin	SLO	00:1E:65:F2:0F:B0	2010-11-29 22
smith test4@gawab.com	N/A	M KIT Linksys WRT300N v2	SLO	00:1E:65:F2:0F:B0	2010-11-25 01
smith test4@gawab.com	N/A	M KIT WRT54GL	SLO	00:1E:65:F2:0F:B0	2010-11-03 19
smith test3@maktoob.com	N/A	M KIT WRT54GL	SLO	00:24:7E:DE:9A:BA	2010-07-23 21
smith test2@hotmail.com	N/A	CW_2	D8:D3:85:99:1B:C5	2010-10-13 19	
smith test2@hotmail.com	N/A	M KIT Belkin	SLO	00:1E:65:F2:0F:B0	2010-11-30 02
smith test2@hotmail.com	N/A	M KIT Linksys WRT300N v2	SLO	00:1E:65:F2:0F:B0	2010-11-29 18
smith test2@hotmail.com	N/A	M KIT WRT54GL	SLO	00:1E:65:F2:0F:B0	2010-11-18 21
smith test2@hotmail.com	N/A	M KIT WRT54GL	SLO	00:24:7E:DE:9A:BA	2010-07-23 21
smith test1@yahoo.com	N/A	CW_1	D8:D3:85:99:1B:D3	2010-10-06 14	
smith test1@yahoo.com	N/A	CW_2	D8:D3:85:99:1B:C5	2010-10-13 19	
smith test1@yahoo.com	N/A	M KIT Belkin	SLO	00:1E:65:F2:0F:B0	2010-11-29 22
smith test1@yahoo.com	No	M KIT Linksys WRT300N v2	SLO	00:1E:65:F2:0F:B0	2010-11-29 19
smith test1@yahoo.com	N/A	M KIT WRT54GL	SLO	00:1E:65:F2:0F:B0	2010-11-19 17
smith test1@yahoo.com	N/A	M KIT WRT54GL	SLO	00:24:7E:DE:9A:BA	2010-07-23 21
heliotropeaim	N/A	M KIT Belkin	SLO	00:1E:65:F2:0F:B0	2010-11-29 22
heliotropeaim	N/A	M KIT Linksys WRT300N v2	SLO	00:1E:65:F2:0F:B0	2010-11-25 01
heliotropeaim	N/A	M KIT WRT54GL	SLO	00:1E:65:F2:0F:B0	2010-11-03 18
heliotropeaim	N/A	M KIT WRT54GL	SLO	00:24:7E:DE:9A:BA	2010-07-23 21
heliotrope111	No	M KIT Belkin	SLO	00:1E:65:F2:0F:B0	2010-11-30 18
heliotrope111	N/A	M KIT Linksys WRT300N v2	SLO	00:1E:65:F2:0F:B0	2010-11-29 18
heliotrope111	N/A	M KIT WRT54GL	SLO	00:1E:65:F2:0F:B0	2010-11-03 18
bethenaaaim	N/A	CW_1	D8:D3:85:99:1B:D3	2010-10-05 19	

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111      Current Time: 2010-12-17 17:46:03.379

Figure 44: Cherry Web View -> Target Activity Page

# Viewing Target Details

The screenshot shows the Cherry Web interface for viewing target details. The left sidebar contains a navigation menu with sections like Overview, View, Alerts, Windex Alerts, Upgrade Alerts, Target Activity, Flytraps, Deployments, Missions, Target Decks, Copy Data, VPN Data, Harvest Data, Location Data, Diagnostic Data, Plan, Flytraps, Targets, Target Decks, Exploits, Windex, VPN Link/Proxy, Flytrap Applications, Mission File, Execute Command, PoPs, Missions, Assign, Mission to Flytraps, Flytrap Kill, and Administrator. The main content area is titled "Target Details" and shows a table for the target "smith\_test2@hotmail.com". The table has columns: Session Active, Name, Location, Client MAC, Start Time, and End Time. The data in the table is as follows:

Session Active	Name	Location	Client MAC	Start Time	End Time
No	00:18:F8:B7:B7:A5		00:15:58:84:08:F4	2010-01-21 01:19:49.0	2010-01-21
No	J WRT320N Serial	Lab	00:0D:60:CD:7E:B0	2010-09-30 18:28:25.0	2010-09-30
No	J WRT320N Serial	Lab	00:21:70:B8:B2:B3	2010-09-28 17:51:52.0	2010-09-28
N/A	M DLink DIR-330	SLO	00:20:E0:67:96:D4	2009-02-26 22:28:35.0	2009-02-26
N/A	M DLink DIR-330	SLO	08:00:46:C3:02:B7	2009-02-26 00:45:30.0	2009-02-26
N/A	M KIT Belkin F5D8231-4 v4	SLO	00:12:3F:11:22:33	2009-10-23 17:42:14.0	2009-10-24
No	M KIT Belkin F5D8231-4 v4	SLO	00:15:58:84:08:F4	2010-01-15 01:17:13.0	2010-01-15
N/A	M KIT Belkin F5D8231-4 v4	SLO	00:1E:65:F2:0F:B0	2010-01-21 02:02:25.0	2010-01-21
N/A	M KIT Belkin F5D8231-4 v4	SLO	08:00:46:C3:02:B7	2009-10-26 19:47:08.0	2009-10-26
N/A	M KIT Linksys WRT300N v2	SLO	00:0B:97:96:FC:69	2010-01-19 21:13:23.0	2010-01-19
N/A	M KIT Linksys WRT300N v2	SLO	00:1E:65:F2:0F:B0	2010-01-19 21:01:42.0	2010-01-19
N/A	M KIT WRT54G v5	SLO	00:0B:97:96:FC:69	2010-01-21 23:22:34.0	2010-01-21
N/A	M KIT WRT54G v5	SLO	00:1E:65:F2:0F:B0	2010-01-21 22:20:14.0	2010-01-21
N/A	SLO flower	SLO	00:1D:7E:DC:2A:69	2010-01-22 18:58:59.0	2010-01-22
N/A	Sunflower seed	remote	00:02:3F:94:08:6C	2009-01-15 22:18:13.0	2009-01-15
N/A	sunflower seed 00:1B:DD:76:A6:40	remote	00:22:5F:35:DF:CE	2009-07-23 19:40:55.0	2009-07-23
N/A	S_FT3	slo	00:11:43:A8:8A:67	2009-09-22 17:43:37.0	2009-09-22
N/A	WRT300N v2 Bad Power	SLO	00:0B:97:96:FC:69	2009-10-21 21:05:20.0	2009-10-21

At the bottom of the page, there are two status messages: "Last Alert: 2010-06-17 23:26:20.0 Target: space@test.com" and "Current Time: 2011-01-03 17:23:55.149".

Figure 45: Cherry Web Target Details Page

# Viewing Copy Data

The screenshot shows the Cherry Blossom web interface with the title "Cherry Blossom" and "Version 4.0 (svn 8275)". On the left, there is a navigation menu with various links such as Overview, View, Alerts, Windex Alerts, Upgrade Alerts, Target Activity, Flytraps, Deployments, Missions, Target Decks, Copy Data (which is circled in red), VPN Data, Harvest Data, Location Data, Diagnostic Data, Plan, Flytraps, Targets, Target Decks, Exploits, Windex, VPN Link/Proxy, Flytrap Applications, Mission File, Execute Command, PoP(s), Missions, Assign, Mission to Flytraps, Flytrap Kill, Administer, Customers, Permissions, Users, and Catsput. Below the navigation menu, the main content area is titled "Copy Data". It contains a table with columns: File, File Size, FlyTrap, Last Modified, Start Time, and a sorting icon. The table lists numerous entries, each representing a download task. The first few rows show entries like "download 0.2 MB SlimBoyFlyTrap 00:25:9C:3B:D3:5B" and "download 0.2 MB SlimBoyFlyTrap 00:25:9C:3B:D3:5B". The last row shows a large file "download 75.2 MB CW\_1 LAN=00:24:A1:68:41:3A". At the bottom of the page, there is a message "Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111" and the current time "Current Time: 2010-12-17 17:48:48.452". A red arrow points from the text "View -> Copy Data" to the "Copy Data" link in the navigation menu.

File	File Size	FlyTrap	Last Modified	Start Time	W
download 0.2 MB	SlimBoyFlyTrap 00:25:9C:3B:D3:5B		2010-11-30 23:52:46.0	2010-11-30 23:26:52.000	
download 0.2 MB	SlimBoyFlyTrap 00:25:9C:3B:D3:5B		2010-11-30 23:26:49.0	2010-11-30 23:08:40.000	
download 24.8 MB	M KIT Belkin 00:17:3F:40:01:7C		2010-11-30 21:08:57.0	2010-11-30 20:44:48.000	
download 1.0 MB	M KIT Belkin 00:17:3F:40:01:7C		2010-11-30 02:11:25.0	2010-11-30 02:03:05.000	
download 0.1 MB	M KIT Belkin 00:17:3F:40:01:7C		2010-11-30 02:02:52.0	2010-11-30 02:00:28.000	
download 7.0 MB	M KIT Belkin 00:17:3F:40:01:7C		2010-11-29 22:25:28.0	2010-11-29 22:01:18.000	
download 1.0 MB	M KIT Linksys WRT300N v2 00:18:39:90:18:C4		2010-11-29 19:18:12.0	2010-11-29 19:10:02.000	
download 4.9 MB	M KIT Linksys WRT300N v2 00:18:39:90:18:C4		2010-11-29 18:01:01.0	2010-11-29 17:47:22.000	
download 12.2 MB	M KIT Linksys WRT300N v2 00:18:39:90:18:C4		2010-11-25 01:40:12.0	2010-11-25 01:19:03.000	
download 2.8 MB	M KIT Linksys WRT300N v2 00:18:39:90:18:C4		2010-11-25 00:18:51.0	2010-11-24 23:54:47.000	
download 0.3 MB	M KIT Linksys WRT300N v2 00:18:39:90:18:C4		2010-11-24 20:03:40.0	2010-11-24 19:39:31.000	
download 0.7 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-13 01:28:47.0	2010-11-13 01:04:56.000	
download 0.3 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-08 21:31:26.0	2010-11-08 21:16:25.000	
download 0.1 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:25:27.0	2010-11-05 21:23:38.000	
download 0.2 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:23:36.0	2010-11-05 21:22:46.000	
download 0.9 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:22:47.0	2010-11-05 21:21:35.000	
download 0.9 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:21:36.0	2010-11-05 21:19:48.000	
download 1.0 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:19:49.0	2010-11-05 21:18:37.000	
download 0.1 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:17:57.0	2010-11-05 21:08:05.000	
download 0.1 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:07:37.0	2010-11-05 21:07:30.000	
download 0.3 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:06:45.0	2010-11-05 21:04:54.000	
download 1.7 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-05 21:04:11.0	2010-11-05 21:00:11.000	
download 1.3 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-03 22:00:26.0	2010-11-03 21:46:31.000	
download 0.1 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-03 20:48:49.0	2010-11-03 20:32:47.000	
download 1.0 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-03 20:32:01.0	2010-11-03 20:26:11.000	
download 0.4 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-03 20:25:45.0	2010-11-03 20:23:28.000	
download 1.9 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-03 20:20:52.0	2010-11-03 20:15:08.000	
download 3.3 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-03 20:01:28.0	2010-11-03 19:43:28.000	
download 9.6 MB	M KIT WRT54GL 00:25:9C:47:73:F5		2010-11-03 18:57:31.0	2010-11-03 18:33:26.000	
download 0.4 MB	CW_1 LAN=00:24:A1:68:41:3A		2010-10-13 22:04:20.0	2010-10-13 22:00:01.0LA	
download 75.2 MB	CW_1 LAN=00:24:A1:68:41:3A		2010-10-13 21:12:55.0	2010-10-13 20:42:31.0LA	

Figure 46: Cherry Web View -> Copy Data Page

# Viewing VPN Data

The screenshot shows the Cherry Blossom web interface. On the left is a vertical navigation menu with a dark blue background. A red arrow points from the text "View -> VPN Data" to the "VPN Data" link in the menu. The main content area has a light gray header bar with the title "VPN Data". Below the header is a toolbar with links: <<< 1 >>>, File, File Size, FlyTrap, Last Modified, Start Time, WLAN MAC, LANMAC, and <<< 1 >>>. Below the toolbar is a link "Back to VPN Data". At the bottom of the page, there is a status bar with "Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111" and "Current Time: 2010-12-17 18:17:43.594".

Cherry Blossom  
Version 4.0 (svn 8275)

View ->  
**VPN Data**

Overview  
View  
Alerts  
Windex Alerts  
Upgrade Alerts  
Target Activity  
Flytraps  
Deployments  
Missions  
Target Decks  
Copy Data  
**VPN Data**  
Harvest Data  
Location Data  
Diagnostic Data

Plan  
Flytraps  
Targets  
Target Decks  
Exploits  
Windex  
VPN Link/Proxy

Flytrap Applications  
Mission File  
Execute Command

PoPs  
Missions

Assign  
Mission to Flytraps  
Flytrap Kit

Administer  
Customers  
Permissions  
Users  
Catapult  
Windex Connection

VPN Data

<<< 1 >>>

[File](#) [File Size](#) [FlyTrap](#) [Last Modified](#) [Start Time](#) ▾ [WLAN MAC](#) [LANMAC](#)

<<< 1 >>>

[Back to VPN Data](#)

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Current Time: 2010-12-17 18:17:43.594

Figure 47: Cherry Web View -> VPN Data Page

# Viewing Harvest Data

View ->  
Harvest Data

The screenshot shows the Cherry Blossom web interface. On the left is a navigation sidebar with various links such as Overview, View, Alerts, Flytraps, Missions, Exploits, Flytrap Applications, Assign, Administer, and Customers. A red arrow points from the text "View -> Harvest Data" to the "Harvest Data" link in the sidebar. The main content area is titled "Harvest Data" and contains a table with 18 rows of data. The columns are labeled "Content", "Filter Origin", "Client MAC", and "FlyTrap". The "Content" column lists "root@localhost.localdomain" repeated 18 times. The "Filter Origin" column lists "Webmail Email 00:0D:60:CD:7E:B0" repeated 18 times. The "Client MAC" column lists "Create Target SlimBoy" repeated 18 times. The "FlyTrap" column lists "Create Target" repeated 18 times. At the bottom of the page, there is a message "Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111" and the current time "Current Time: 2010-12-17 18:18:19.648".

Content	Filter Origin	Client MAC	FlyTrap
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target
root@localhost.localdomain	Webmail Email 00:0D:60:CD:7E:B0	Create Target SlimBoy	Create Target

Figure 48: Cherry Web View -> Harvest Data Page

# Viewing Upgrade Alerts

The screenshot shows the Cherry web interface with a dark blue sidebar on the left and a main content area on the right.

**Left Sidebar (Cherry Blossom Version 4.0 (svn 8275)):**

- Overview**
- View**
- Alerts**
- Windex Alerts**
- Upgrade Alerts** (highlighted with a red arrow)
- Target Activity**
- Flytraps**
- Deployments**
- Missions**
- Target Decks**
- Copy Data**
- VPN Data**
- Harvest Data**
- Location Data**
- Diagnostic Data**
- Plan**
- Flytraps**
- Targets**
- Target Decks**
- Exploits**
- Windex**
- VPN Link/Proxy**
- Flytrap Applications**
- Mission File**
- Execute Command**
- POPs**
- Missions**
- Assign**
- Mission to Flytraps**
- Flytrap Kill**
- Administer**
- Customers**
- Permissions**
- Users**
- Calapult**

**Main Content Area:**

### Firmware Upgrade Alerts

Date	Flytrap	Type	Client MAC	Client IP
2010-11-29 22:30:17.0	M KIT Belkin 00:17:3F:40:01:7C	Upgrade attempted	00:24:7E:DE:9A:BA	192
2010-11-29 22:28:57.0	M KIT Belkin 00:17:3F:40:01:7C	Upgrade page visited	00:24:7E:DE:9A:BA	192
2010-11-29 22:27:10.0	M KIT Belkin 00:17:3F:40:01:7C	Upgrade page visited	00:24:7E:DE:9A:BA	192
2010-11-29 22:25:32.0	M KIT Belkin 00:17:3F:40:01:7C	Upgrade page visited	00:24:7E:DE:9A:BA	192
2010-11-25 01:42:28.0	M KIT Linksys WRT300N v2 00:18:39:90:18:C4	Upgrade page visited	00:1E:65:F2:0F:B0	192
2010-11-25 01:42:23.0	M KIT Linksys WRT300N v2 00:18:39:90:18:C4	Upgrade page visited	00:1E:65:F2:0F:B0	192
2010-11-25 01:40:50.0	M KIT Linksys WRT300N v2 00:18:39:90:18:C4	Upgrade page visited	00:1E:65:F2:0F:B0	192
2010-11-25 01:40:47.0	M KIT Linksys WRT300N v2 00:18:39:90:18:C4	Upgrade page visited	00:1E:65:F2:0F:B0	192
2010-11-25 01:35:30.0	M KIT Linksys WRT300N v2 00:18:39:90:18:C4	Upgrade page visited	00:1E:65:F2:0F:B0	192
2010-11-03 22:06:14.0	M KIT WRT54GL 00:25:9C:47:73:F5	Upgrade page visited	00:1E:65:F2:0F:B0	192
2010-11-03 18:02:05.0	M KIT WRT54GL 00:25:9C:47:73:F5	Upgrade attempted	00:24:7E:DE:9A:BA	192
2010-10-27 17:18:23.0	M KIT Belkin 00:17:3F:40:01:7C	Upgrade attempted	00:24:7E:DE:9A:BA	192
2010-10-27 17:15:06.0	M KIT Belkin 00:17:3F:40:01:7C	Upgrade page visited	00:24:7E:DE:9A:BA	192
2010-10-15 23:27:19.0	FT3 00:13:10:44:98:AD	Upgrade page visited	00:21:86:61:4B:AA	192
2010-10-15 23:27:05.0	FT3 00:13:10:44:98:AD	Upgrade attempted	00:21:86:61:4B:AA	192

**Bottom Status Bar:**

- Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope11
- Current Time: 2010-12-17 17:45:30.277

Figure 49: Cherry Web View -> Upgrade Alerts Page

# Viewing Windex Alert

View -> Windex Alerts

The screenshot shows the Cherry Web interface with a dark blue header and sidebar. The header features the 'Cherry Blossom' logo and 'Version 4.0 (svn 8275)'. The sidebar contains a navigation menu with various links such as Overview, View, Alerts, Windex Alerts (which is highlighted with a red oval), Upgrade Alerts, Target Activity, Flytraps, Deployments, Missions, Target Decks, Copy Data, VPN Data, Harvest Data, Location Data, Diagnostic Data, Plan, Flytraps, Targets, Target Decks, Exploits, Windex, VPN Link Proxy, Flytrap Applications, Mission File, Execute Command, PoPs, Missions, Assign, Mission to Flytraps, Flytrap Kill, Administer, Customers, Permissions, Users, and Chatbot. The main content area is titled 'Windex Alerts' and displays a table of alerts. The table has columns for Target, Receive Time, Windex Status, Updated, Client MAC, and Client IP. The table lists numerous entries, mostly from 2010-11-30, with various status codes like Pending, Unknown, Success, and Redirected. At the bottom of the table, there are '<<< 1 >>>' navigation buttons. Below the table, the text 'Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111' is displayed in blue, and 'Current Time: 2010-12-17 17:44:49.558' is displayed in black.

Target	Receive Time	Windex Status	Updated	Client MAC	Client IP
abc@def.com	2010-11-30 17:20:41.0	Pending	2010-11-30 17:20:01.000:24.7E:DE:9A:BA	192.168	
abc@def.com	2010-11-30 02:12:19.0	Pending	2010-11-30 02:12:19.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-30 02:26:56.0	Unknown	2010-11-30 02:03:47.000:1E:65:F2:0F:B0	192.168	
smith test2@hotmail.com	2010-11-30 01:59:42.0	Unknown	2010-11-30 01:59:59.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-30 01:39:31.0	Unknown	2010-11-30 01:39:37.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-30 01:21:00.0	Success	2010-11-30 01:21:24.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-30 01:14:00.0	Success	2010-11-30 01:14:44.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-30 00:58:54.0	Pending	2010-11-30 00:58:54.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-30 00:05:16.0	Failure	2010-11-30 00:05:52.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-29 23:45:31.0	Pending	2010-11-29 23:45:31.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-29 23:38:17.0	Failure	2010-11-29 23:38:58.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-29 23:33:15.0	Failure	2010-11-29 23:34:12.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-29 23:29:09.0	Unknown	2010-11-29 23:29:46.000:1E:65:F2:0F:B0	192.168	
abc@def.com	2010-11-29 22:01:19.0	Unknown	2010-11-29 22:01:37.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-29 19:09:53.0	Unknown	2010-11-29 19:10:10.000:1E:65:F2:0F:B0	192.168	
smith test2@hotmail.com	2010-11-29 17:46:18.0	Unknown	2010-11-29 17:46:39.000:1E:65:F2:0F:B0	192.168	
abc@def.com	2010-11-24 23:54:48.0	Pending	2010-11-24 23:54:47.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-24 22:13:45.0	Success	2010-11-24 22:14:07.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-24 21:57:07.0	Failure	2010-11-24 21:58:42.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-24 21:21:05.0	Failure	2010-11-24 21:44:58.000:1E:65:F2:0F:B0	192.168	
abc@def.com	2010-11-24 19:39:31.0	Unknown	2010-11-24 19:39:37.000:1E:65:F2:0F:B0	192.168	
abc@def.com	2010-11-13 01:04:56.0	Pending	2010-11-13 01:04:56.000:0B:97:29:B7:D	192.168	
abc@def.com	2010-11-08 21:17:17.0	Redirected	2010-11-08 21:17:31.000:1E:65:F2:0F:B0	192.168	
test@testing.com	2010-11-03 21:46:33.0	Pending	2010-11-03 21:46:33.000:1E:65:F2:0F:B0	192.168	
abc@def.com	2010-11-03 21:45:23.0	Redirected	2010-11-03 21:45:31.000:1E:65:F2:0F:B0	192.168	
test@testing.com	2010-11-03 20:32:51.0	Redirected	2010-11-03 20:33:02.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-03 20:26:06.0	Redirected	2010-11-03 20:26:34.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-03 20:23:24.0	Redirected	2010-11-03 20:24:33.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-03 20:15:03.0	Redirected	2010-11-03 20:15:44.000:1E:65:F2:0F:B0	192.168	
0:1:E:65:F2:0F:B0	2010-11-03 19:43:24.0	Redirected	2010-11-03 19:44:11.000:1E:65:F2:0F:B0	192.168	
abc@def.com	2010-11-03 18:33:28.0	Redirected	2010-11-03 18:34:02.000:1E:65:F2:0F:B0	192.168	

<<< 1 >>>

Last Alert: 2010-11-30 18:32:20.0 Target: heliotrope111

Current Time: 2010-12-17 17:44:49.558

Figure 50: Cherry Web View -> Windex Alerts Page

# Using VPN Link and VPN Proxy

- The Flytrap executes a Mission with a VPN Link Global Action
- The Flytrap executes a Mission with a VPN Proxy All Global Action
- The Flytrap detects a Target with a VPN Link Action
- The Flytrap detects a Target with a VPN Proxy Action



# One-way Transfer (OWT) of Cherry Blossom Data

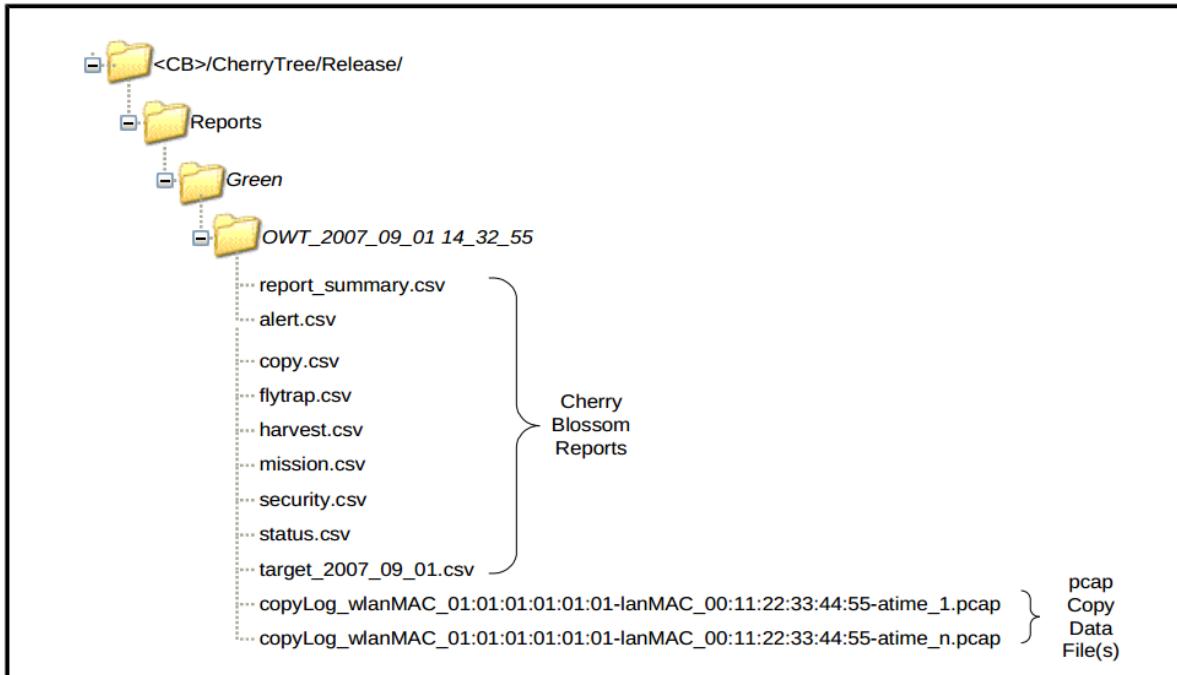


Figure 53: OWT Report Structure

# Generating a OWT Report from Cherry Web

Cherry Blossom  
Version 5.0-test\_seven (svn 8929M)

[Overview](#)  
[View](#)  
[Alerts](#)  
[Windex Alerts](#)  
[Upgrade Alerts](#)  
[Target Activity](#)  
[Flytraps](#)  
[Deployments](#)  
[Missions](#)  
[Target Decks](#)  
[Copy Data](#)  
[VPN Data](#)  
[Harvest Data](#)  
[Location Data](#)  
[Diagnostic Data](#)  
[Plan](#)  
[Flytraps](#)  
[Targets](#)  
[Target Decks](#)  
[Exploits](#)  
[Windex](#)  
[VPN Link/Proxy](#)  
[Flytrap Applications](#)  
[Mission File](#)

**OWT Report Configuration**

Operation:

Start Time:   00:00:00

End Time:   22:05:13

Output Directory:

Last Alert: 2012-07-10 22:58:54.0 Target: snakes@scary.gov      Current Time: 2012-07-17 22:05:34.312

Figure 59: Generating a OWT Report from Cherry Web

# **Some use scenarios and mission use cases**

- Tradeoffs regarding flytrap covertness  
Any flytrap Action that generates traffic might raise suspicion of a vigilant network administrator or Target user. Some cases and their countermeasures are discussed below

- Copy All:  
All network traffic copied. A Network sniffer can detect copy of data (copy data is not encrypted). Copy timeout can be configured to mitigate detection
- Disabling of GZIP encoding:  
if user visits site with GZIP encoding and Mission is configured to strip GZIP encoding, then user will notice slower download from site. This will be more noticeable in flytraps with slow WAN connection
- VPN Proxy:  
a network sniffer could reveal a VPN tunnel that might be suspicious. If a VPN Proxy Action is assigned to a Target, only that Target's traffic is proxied, which mitigates detection.

- Beacon:

Beacons are periodically sent to report status and retrieve new Missions. Beacons are encrypted and wrapped in a covert communication technique. Flytrap can be configured to Beacon only if "Traffic Requirements" is met which will mitigate detection.

- Harvest:

Beacon will contain any email addresses/chat users harvested since the previous Beacon, which will increase the size of the Beacon data. Beacon interval can be configured accordingly.

## Planning of Mission:

Assignment of mission should consider covertness tradeoff. If Environment is likely to be monitored by system administrator then more detectable Actions should be used with caution.

## Slow start:

start with a very “conservative” Mission (no Target Monitoring, no Harvest, long Beacon Interval). As a “comfort level” is achieved on a particular Flytrap, more “liberal” Missions could then be assigned.

# Attack in different cases

- Man In the Middle Attack: The VPN Proxy Action should be used. When the Target is detected, his TCP and UDP traffic will be proxied through the CB-VPN. MITM tool could be run on the CB-VPN to exploit the Target's traffic.
- Suspected target with unknown email/chat address: The Harvest and Copy All features should be used
- Multi user Computer with Target and Non-Target Users: Now we cannot differentiate with MAC address. So expected 'Session Timeout' of Target user can be guessed to approximate which packets are of the Target user.

# System Limitations

- Hardware limitations:  
Most hardwares use about 1-4 MB RAM. And CPU cycles available to Flytrap is low. So Minimal Resource Usage must be done.
- Limited Maximum Number of Targets and Target Actions:  
maximum number of Targets that can be assigned in a Mission is 150, and the maximum number of “unique” Actions that can be assigned is 32.
- Overload of Copy data:  
Under severe loading, the process that performs the Copy Action will drop packets. Upto 10% of downloaded data might be dropped for huge files.

# System Limitations

- Loss of Data in hard reset:  
in Some devices Persistent Data is lost in hard reset. It restores the device back to an initial state (it will return to the Initial Beacon state). Any suicide data is also removed
- Windex Action limitation:  
The Windex Action occurs only on the first HTTP GET request on a root URL, If the Target does not go to a root URL, he will not be exploited.
- Non-Deterministic Beacon Timing:  
Sponsor has no control over when the device is powered-on or connected to the internet. Beacons interval can be configured to some "Traffic requirement". So its timing cannot be known beforehand.

# System Limitations

- Firmware update :  
Successful firmware upgrade will cause the Cherry Blossom implant to be lost.

2 countermeasures of FW update:

- Firmware Upgrade Inhibit :  
user is always presented with a manufacturer's error message when an upgrade is attempted.
- Allow update:  
Some devices have a backdoor upgrade webpage that still allows the device to be upgraded.

**Thank you**