CSE406

Presentation on Security Tools

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

01

ELSA

Geo-locating using Access Points

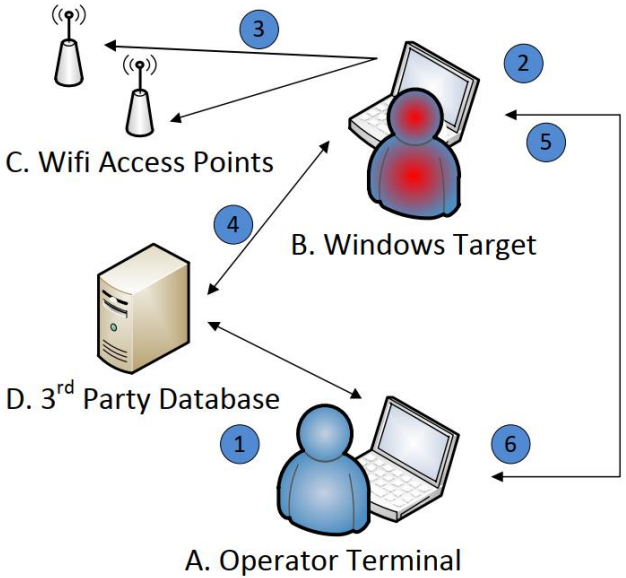
Introduction

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 3rd party databases for resolution into latitude and longitude and an accuracy measure.
- These 3rd 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 sha1-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 rssi 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>
                <rssi>-29</rssi>
            </wifi-ap>
            <wifi-ap>
                <ssid>CableCo</ssid>
                <mac>00:04:E2:C6:3B:DA</mac>
                <rssi>-77</rssi>
            </wifi-ap>
            <wifi-ap>
                <ssid>grace</ssid>
                <mac>00:13:10:C3:26:24</mac>
                <rssi>-73</rssi>
            </wifi-ap>
            <wifi-ap>
                <ssid></ssid>
                <mac>00:14:D1:AE:D3:EC</mac>
                <rssi>-81</rssi>
            </wifi-ap>
            <wifi-ap>
                <ssid></ssid>
                <mac>00:14:D1:AE:D3:FC</mac>
                <rssi>-81</rssi>
            </wifi-ap>
            <wifi-ap>
                <ssid>09BX03031164</ssid>
                <mac>00:23:97:33:5D:F1</mac>
                <rssi>-79</rssi>
            </wifi-ap>
            <wifi-ap>
                <ssid>09FY11030962</ssid>
                <mac>00:23:97:C0:9E:11</mac>
                <rssi>-81</rssi>
            </wifi-ap>
            <wifi-ap>
                <ssid>dlink</ssid>
                <mac>1C:AF:F7:DB:0B:B7</mac>
                <rssi>-83</rssi>
            </wifi-ap>
```

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.

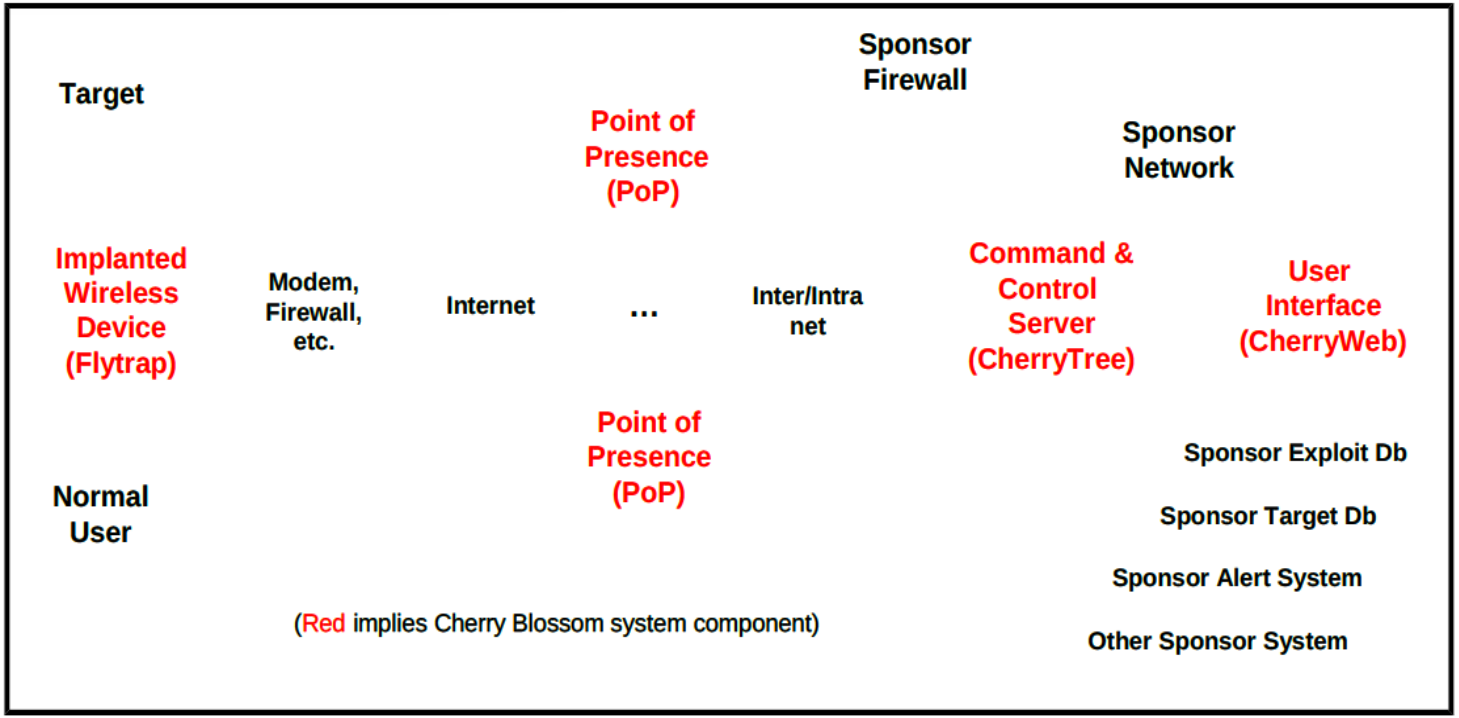
Cherry Blossom

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.

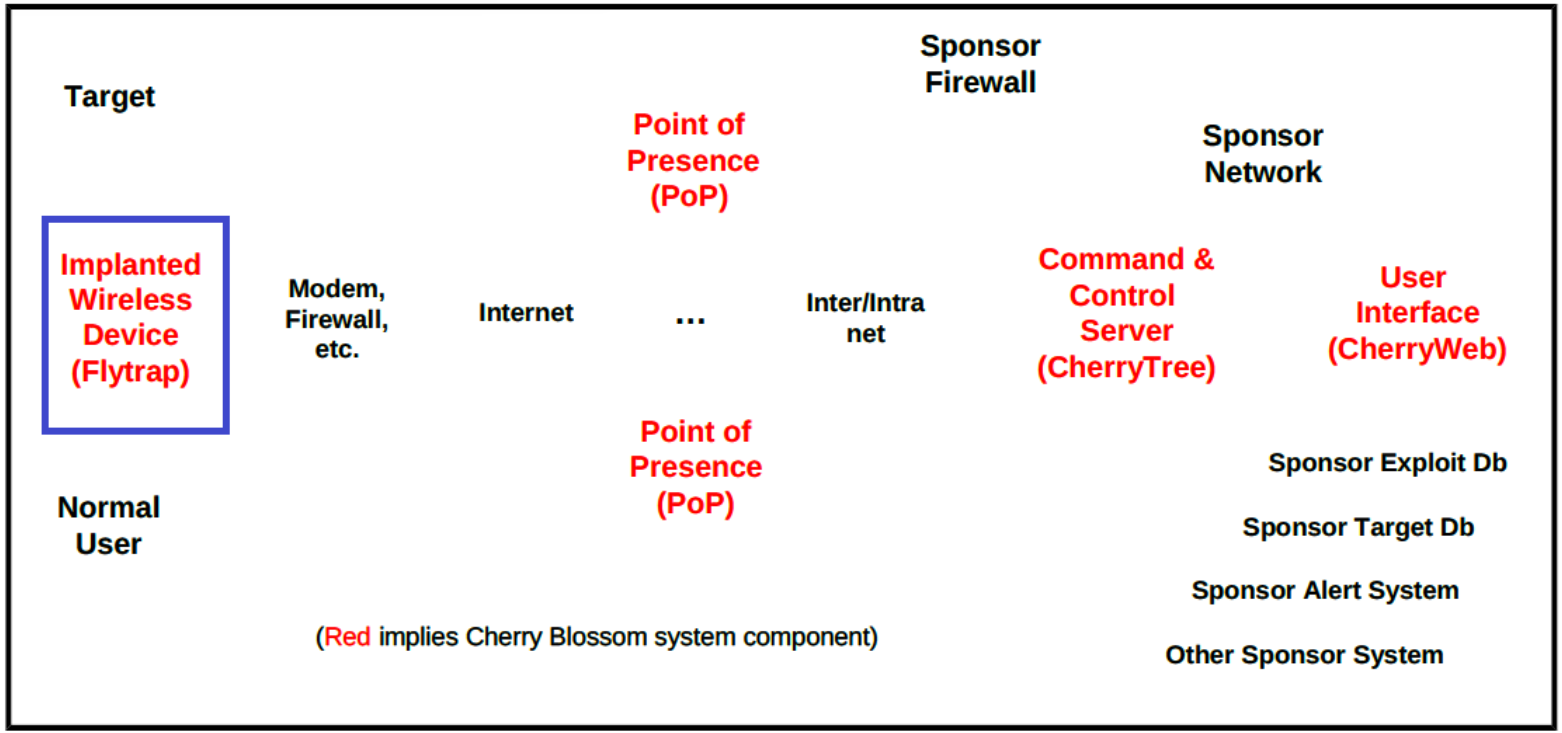
What Happens After Implanting?

- **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


Target
Sponsor Firewall
Point of Presence (PoP)
Sponsor Network
Implanted Wireless Device (Flytrap)
Modem, Firewall, etc.
Internet
...
Inter/Intra net
Command & Control Server (CherryTree)
User Interface (CherryWeb)
Point of Presence (PoP)
Sponsor Exploit Db
Normal User
Sponsor Target Db
Sponsor Alert System
(Red implies Cherry Blossom system component)
Other Sponsor System

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

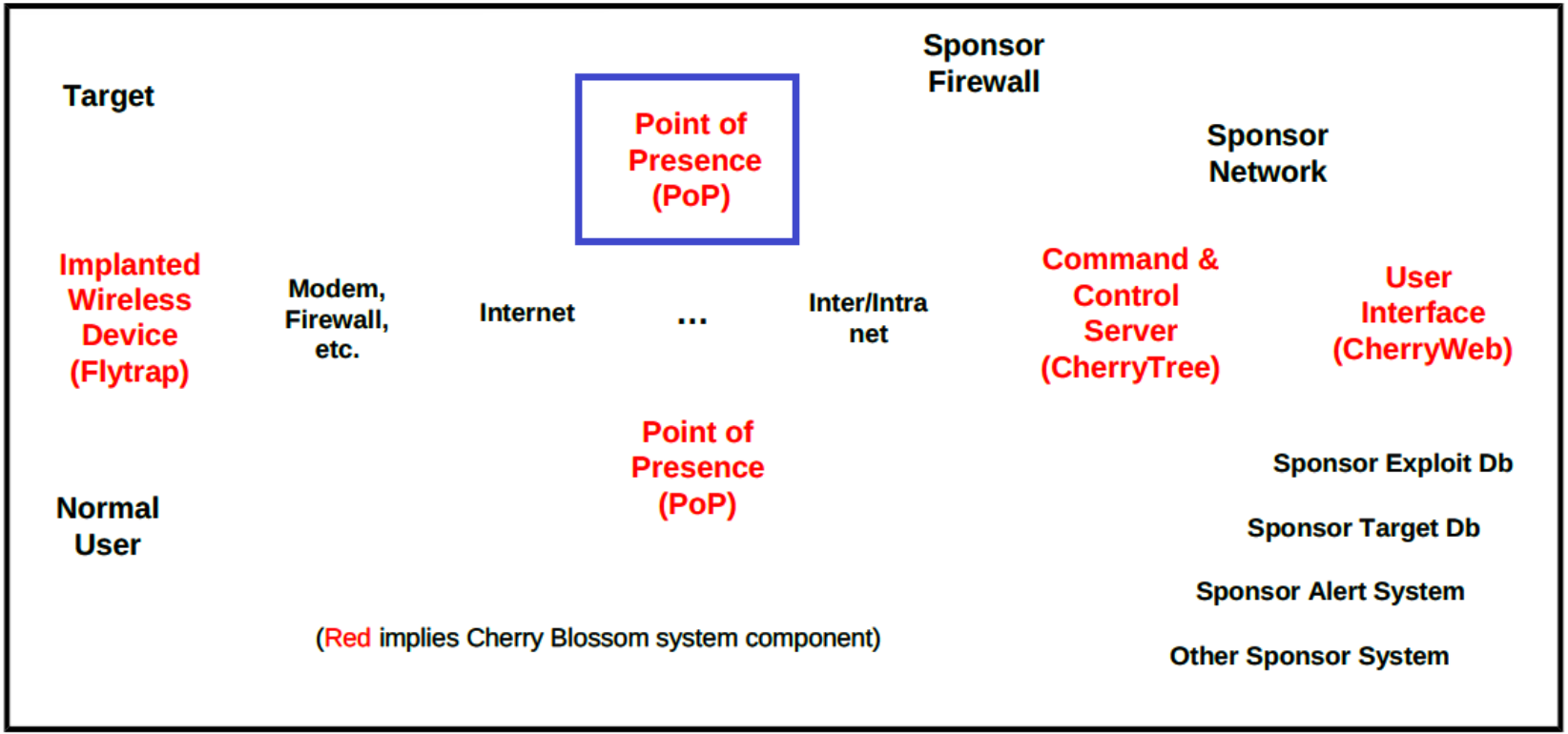
- **Target Detection**
  - Email addresses
  - Chat usernames
  - MAC addresses
  - VoIP phone numbers

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.

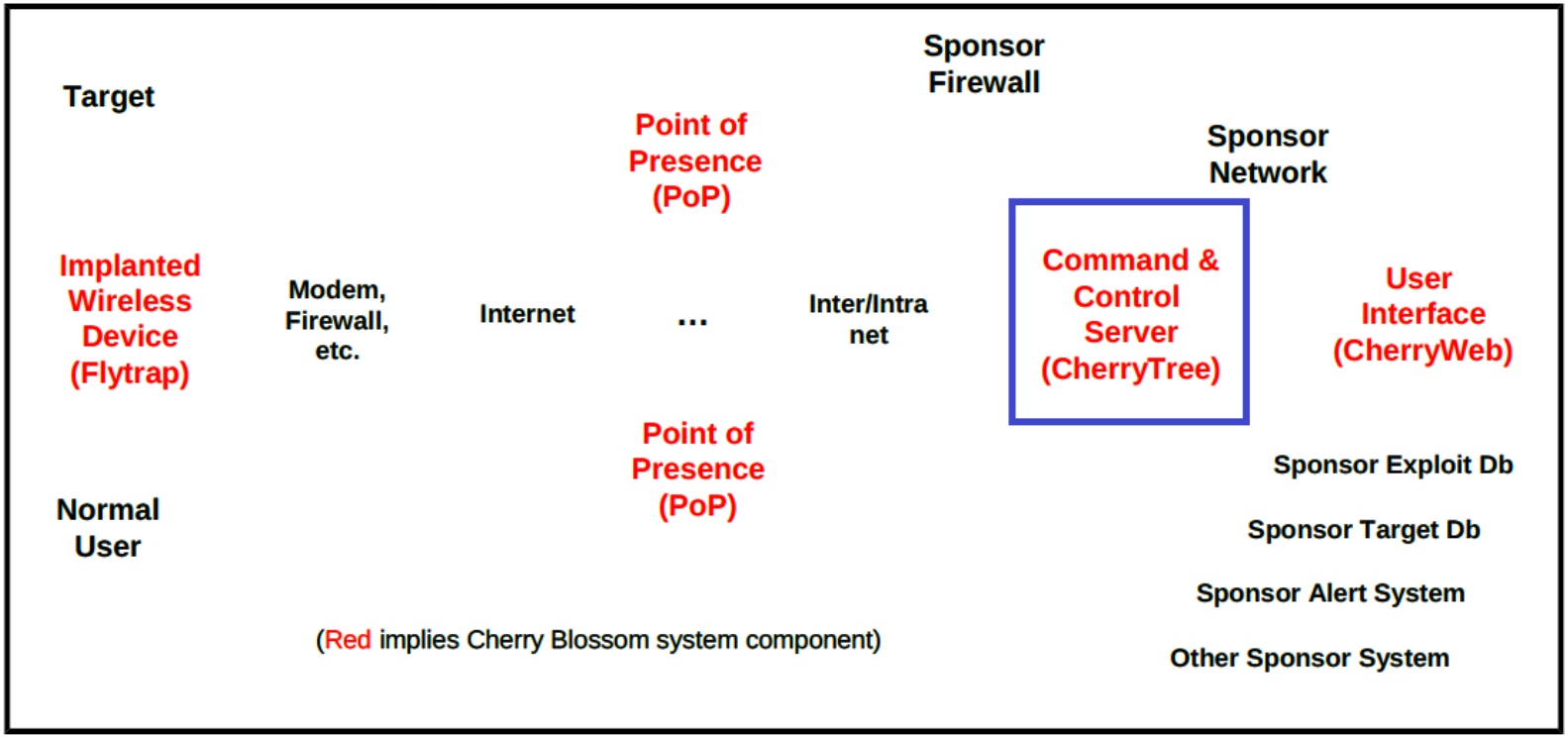
Flytrap Features

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


Target
Sponsor Firewall
Point of Presence (PoP)
Sponsor Network
Implanted Wireless Device (Flytrap)
Modem, Firewall, etc.
Internet
...
Inter/Intra net
Command & Control Server (CherryTree)
User Interface (CherryWeb)
Point of Presence (PoP)
Normal User
Sponsor Exploit Db
Sponsor Target Db
Sponsor Alert System
Other Sponsor System
(Red implies Cherry Blossom system component)

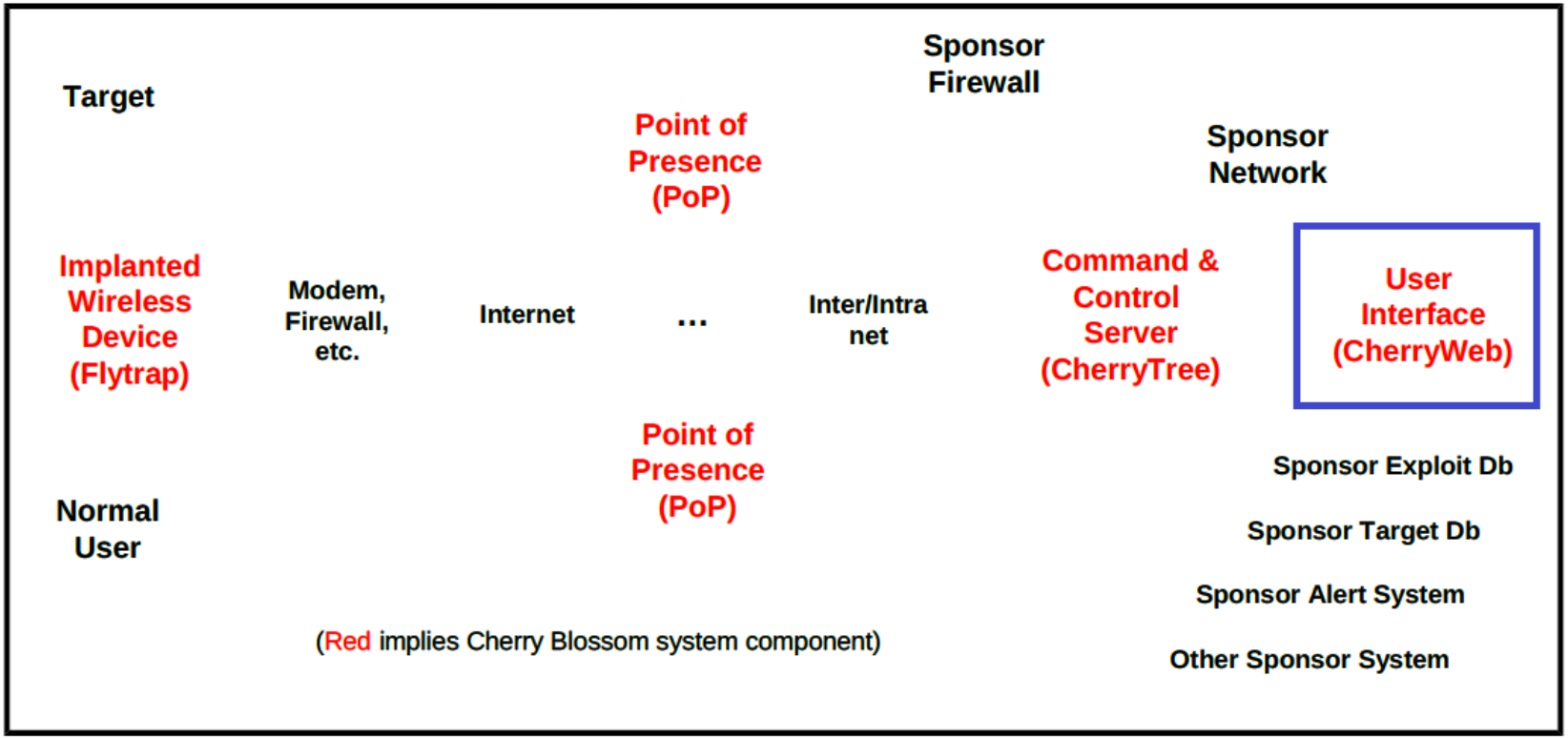
Point of Presence (PoP)

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


Target
Sponsor Firewall
Point of Presence (PoP)
Sponsor Network
Implanted Wireless Device (Flytrap)
Modem, Firewall, etc.
Internet
...
Inter/Intra net
Command & Control Server (CherryTree)
User Interface (CherryWeb)
Point of Presence (PoP)
Normal User
Sponsor Exploit Db
Sponsor Target Db
Sponsor Alert System
Other Sponsor System
(Red implies Cherry Blossom system component)

CherryTree

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


Target
Sponsor Firewall
Point of Presence (PoP)
Sponsor Network
Implanted Wireless Device (Flytrap)
Modem, Firewall, etc.
Internet
...
Inter/Intra net
Command & Control Server (CherryTree)
User Interface (CherryWeb)
Point of Presence (PoP)
Normal User
Sponsor Exploit Db
Sponsor Target Db
Sponsor Alert System
Other Sponsor System
(Red implies Cherry Blossom system component)

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

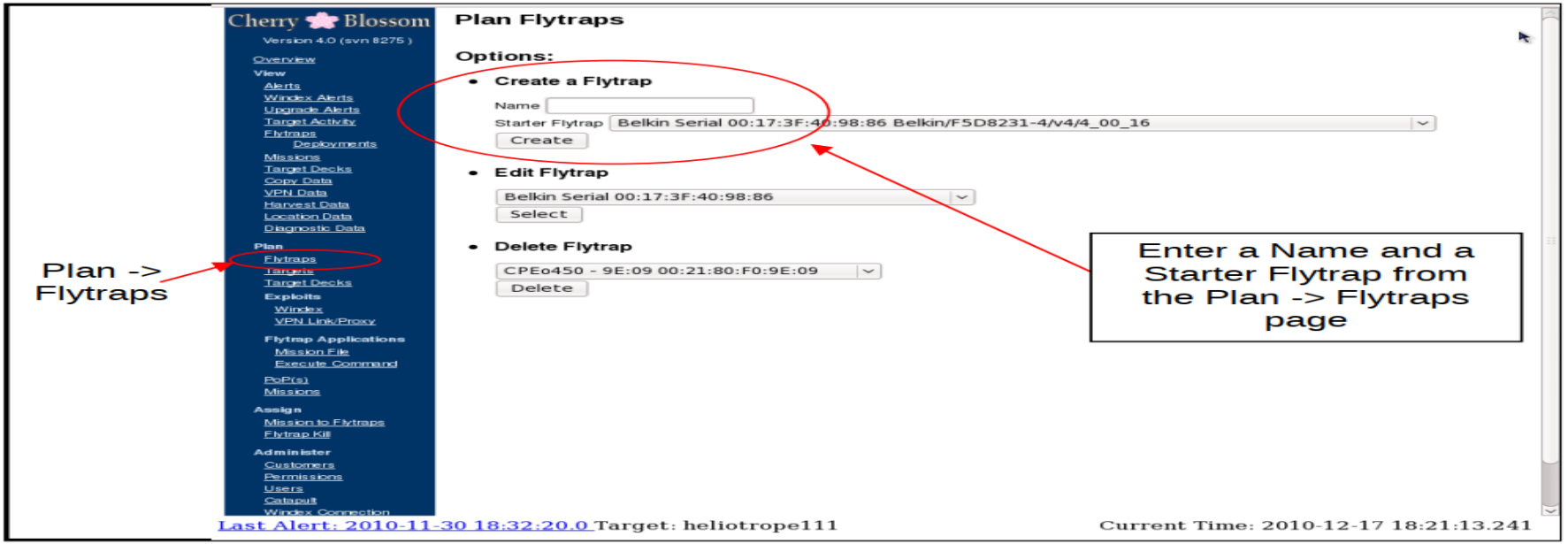


Figure 6: Cherry Web Plan -> Flytraps Page (Create)

Add Flytrap

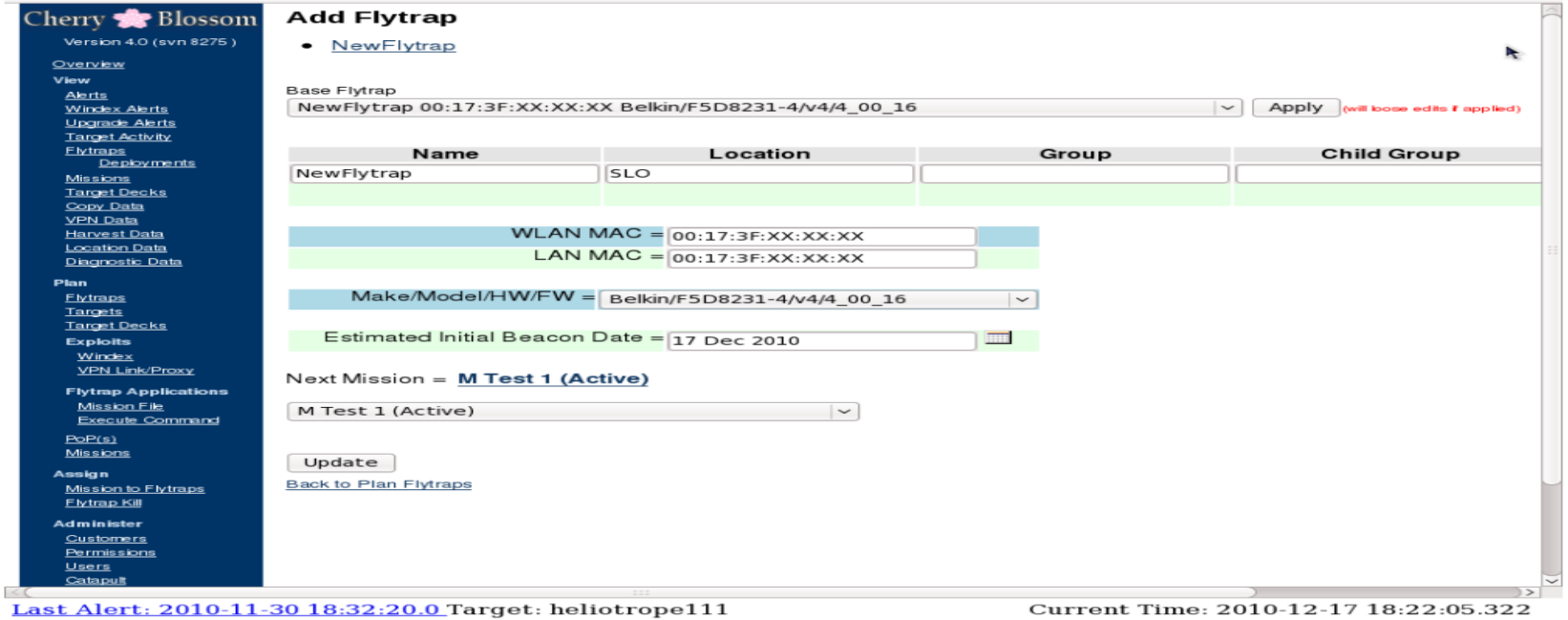


Figure 7: Cherry Web Add Flytrap Page

Checking Flytrap Status

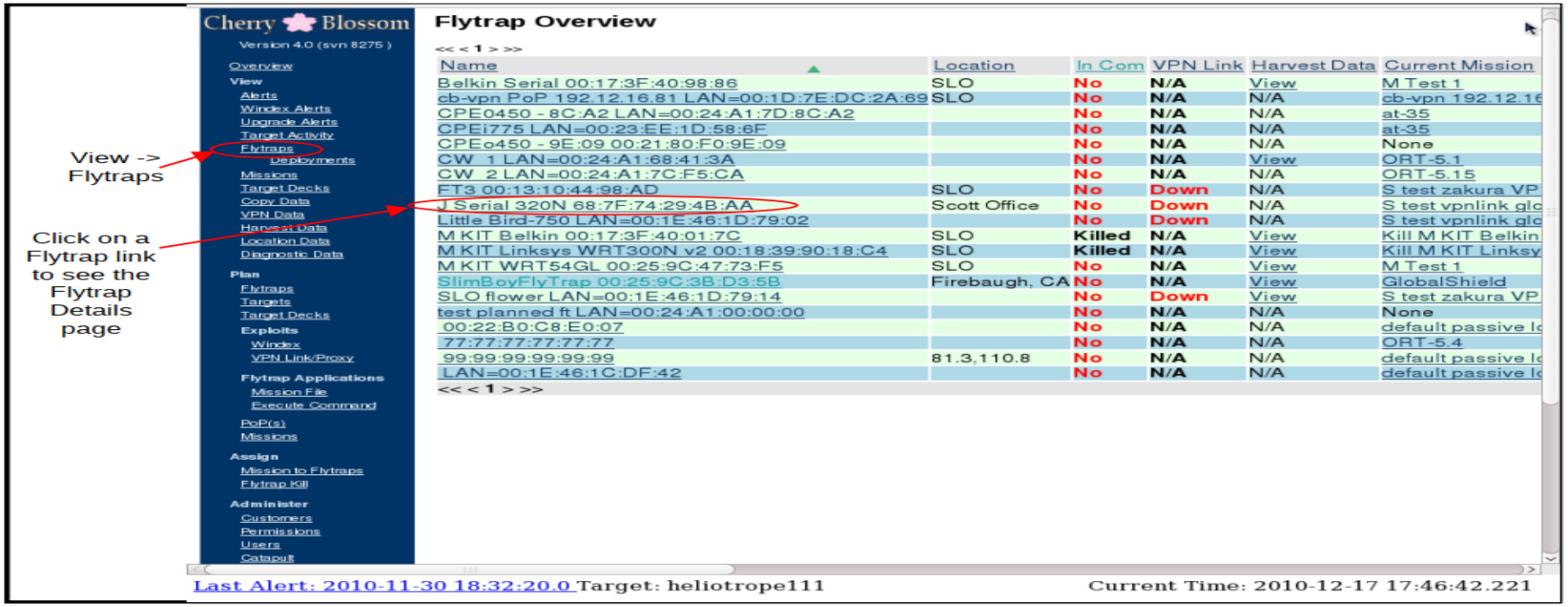


Figure 8: CherryWeb View -> Flytraps Page

Flytrap Details

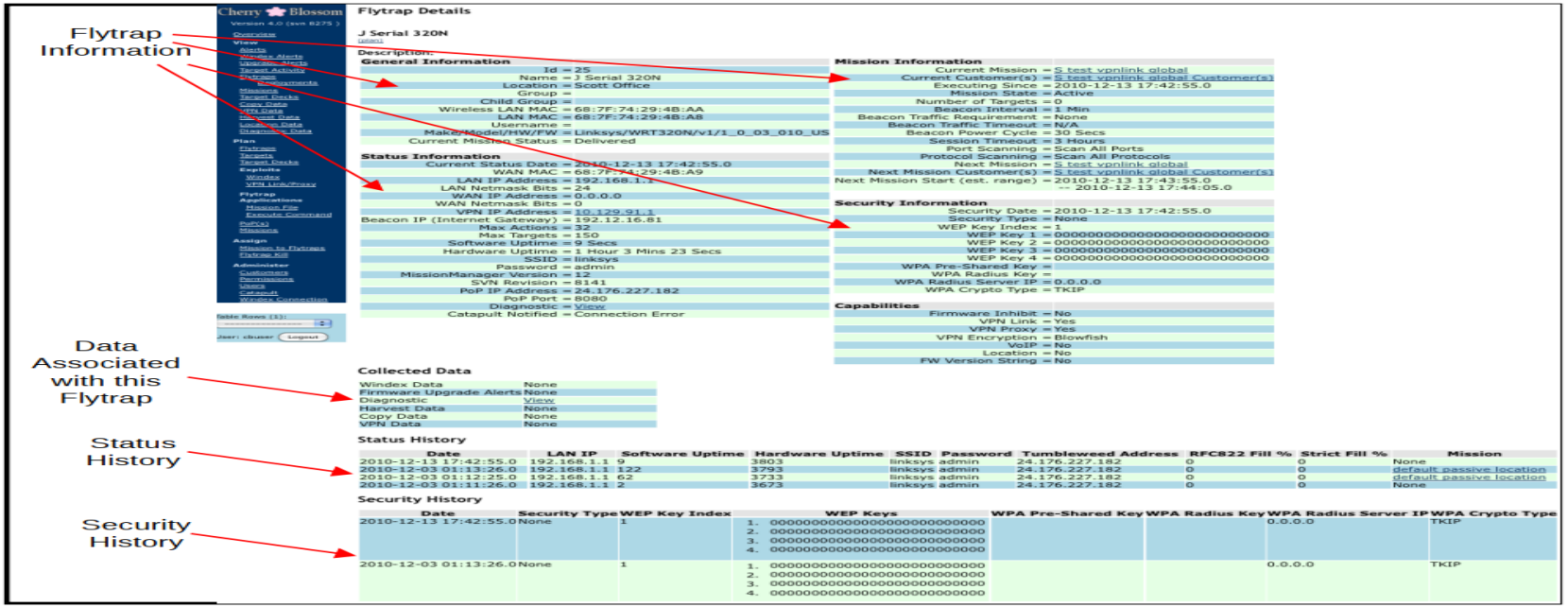


Figure 9: Cherry Web Flytrap Details Page

Deployed Flytraps

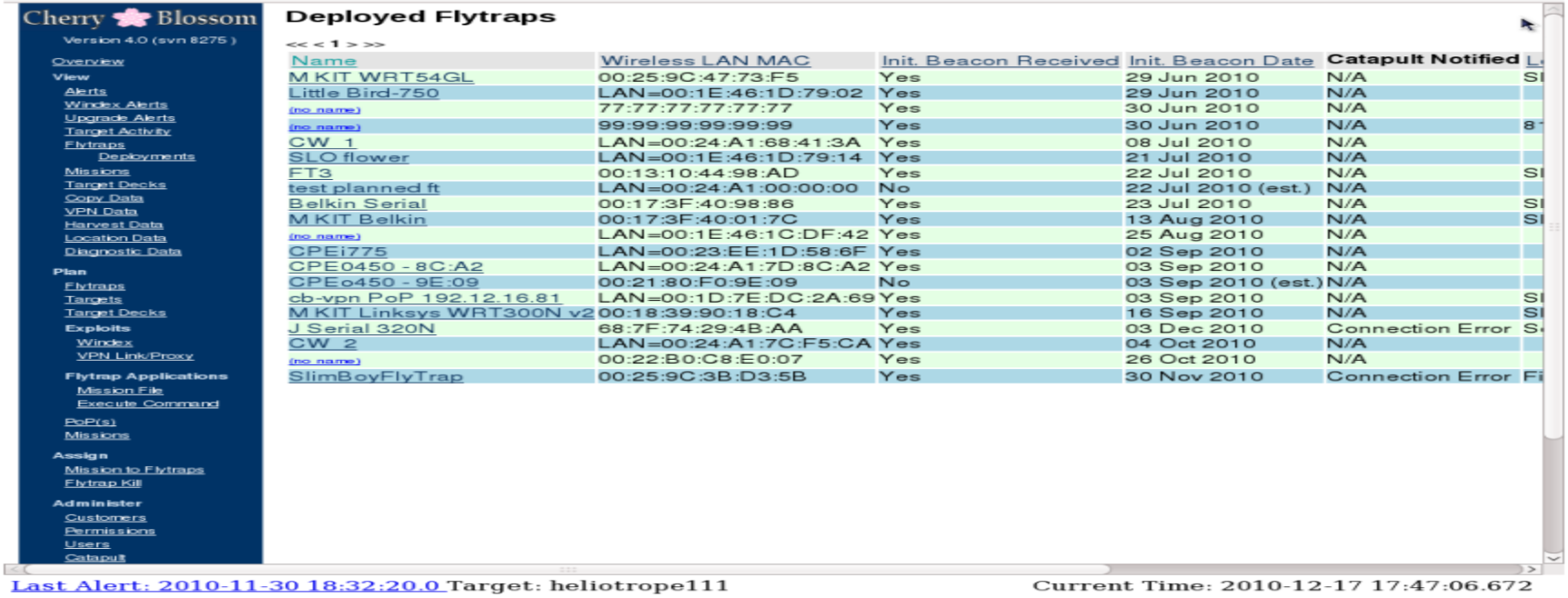


Figure 10: Cherry Web View -> Flytraps -> Deployments Page

The Default Mission

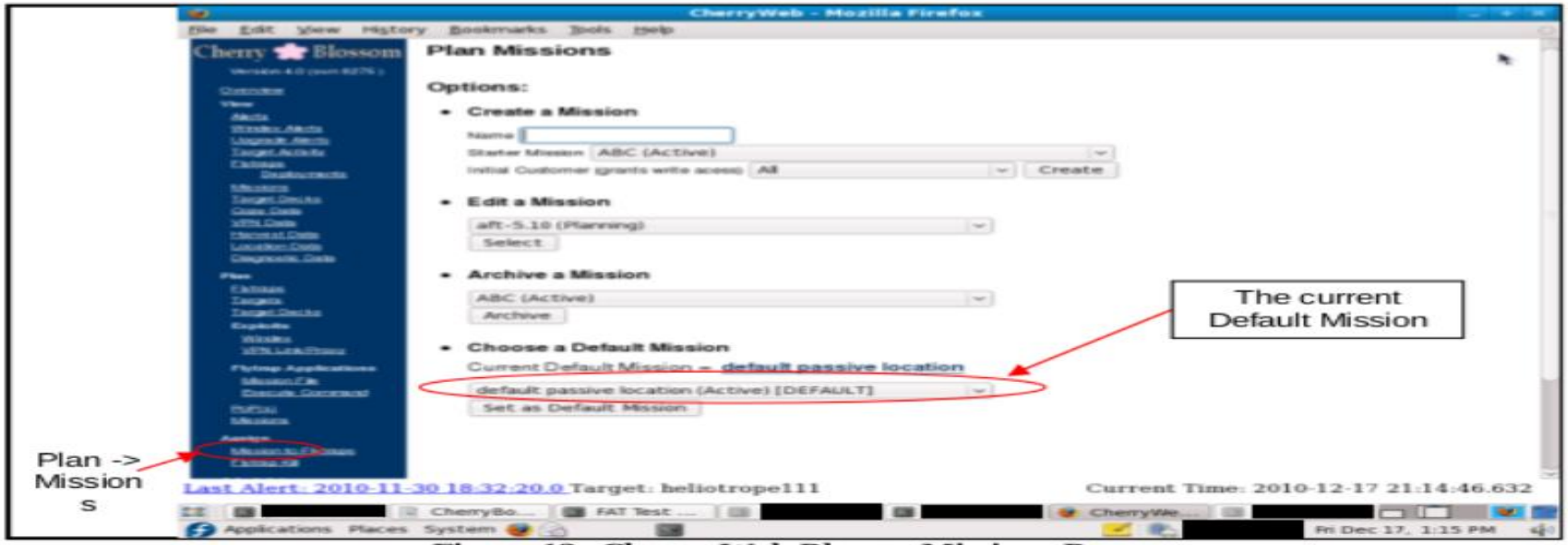


Figure 13: Cherry Web Plan -> Missions Page

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

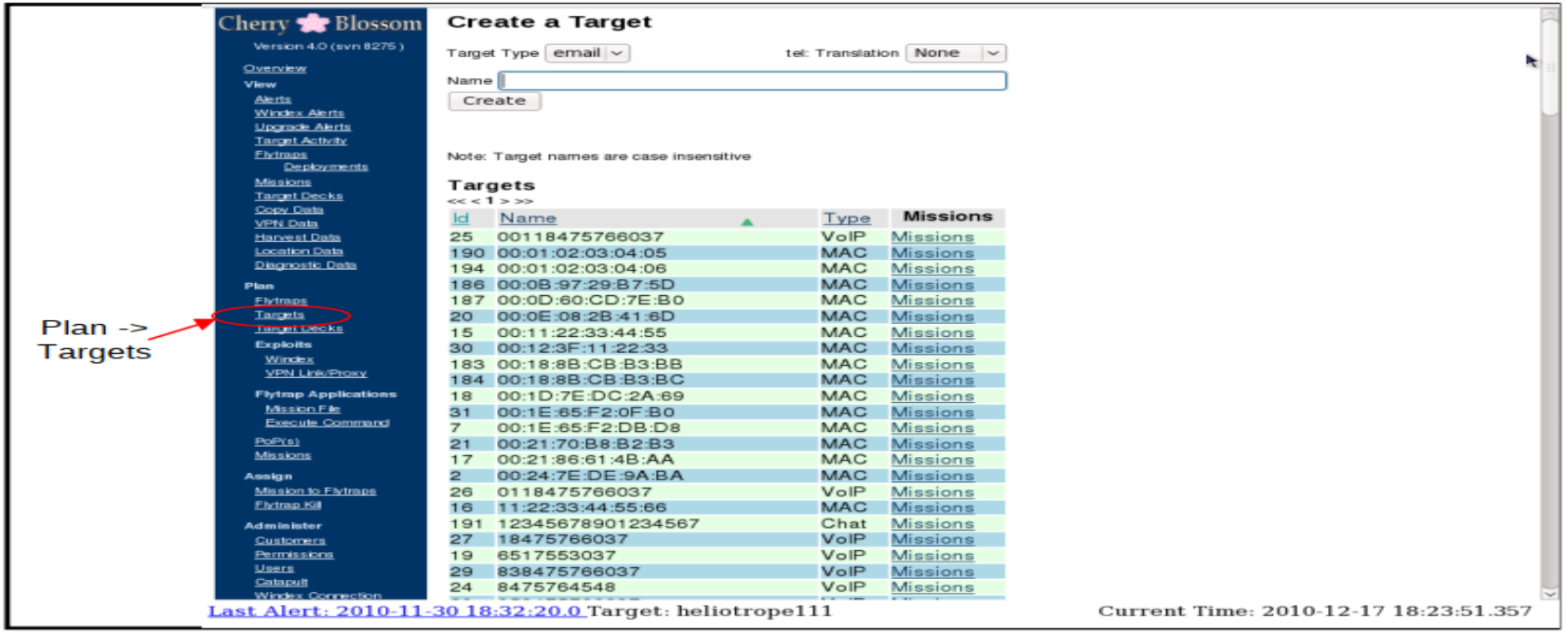


Figure 14: Cherry Web Plan -> Targets Page

Step 2: Create Target Deck(s)

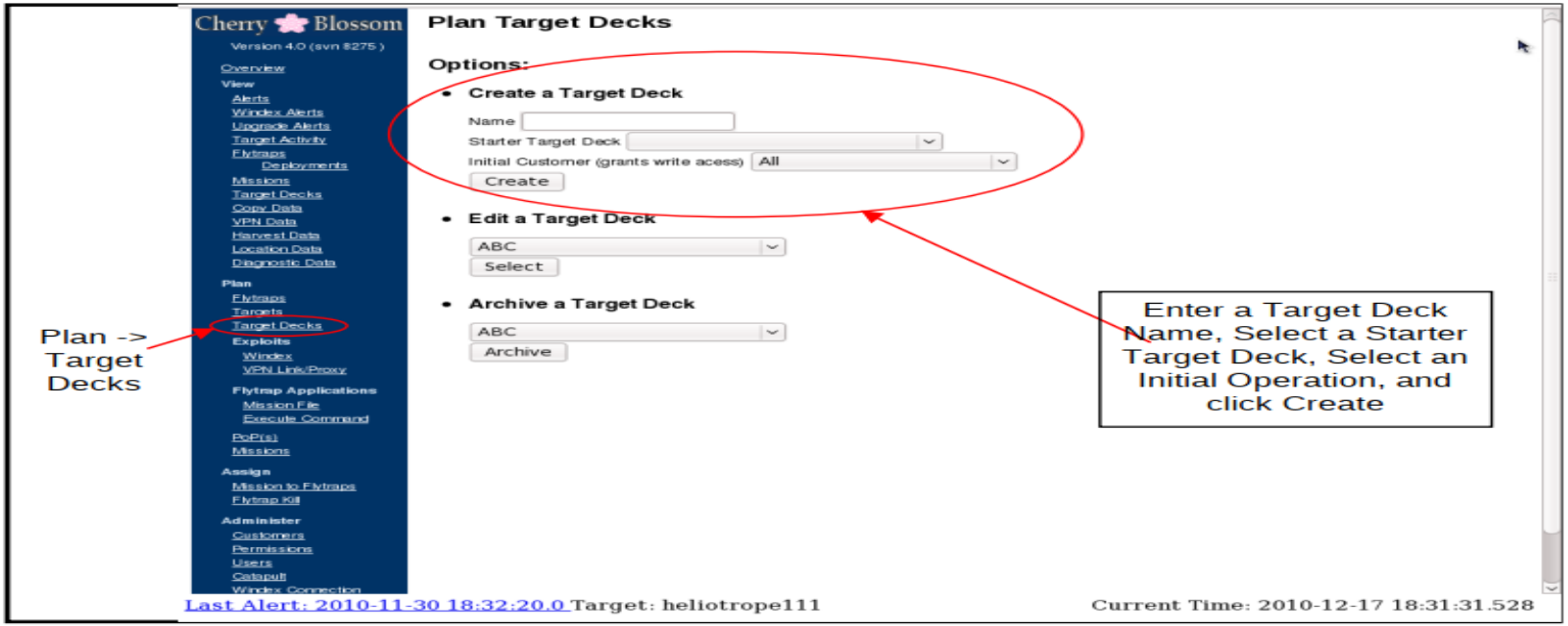


Figure 15: Cherry Web Plan -> Target Decks Page

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

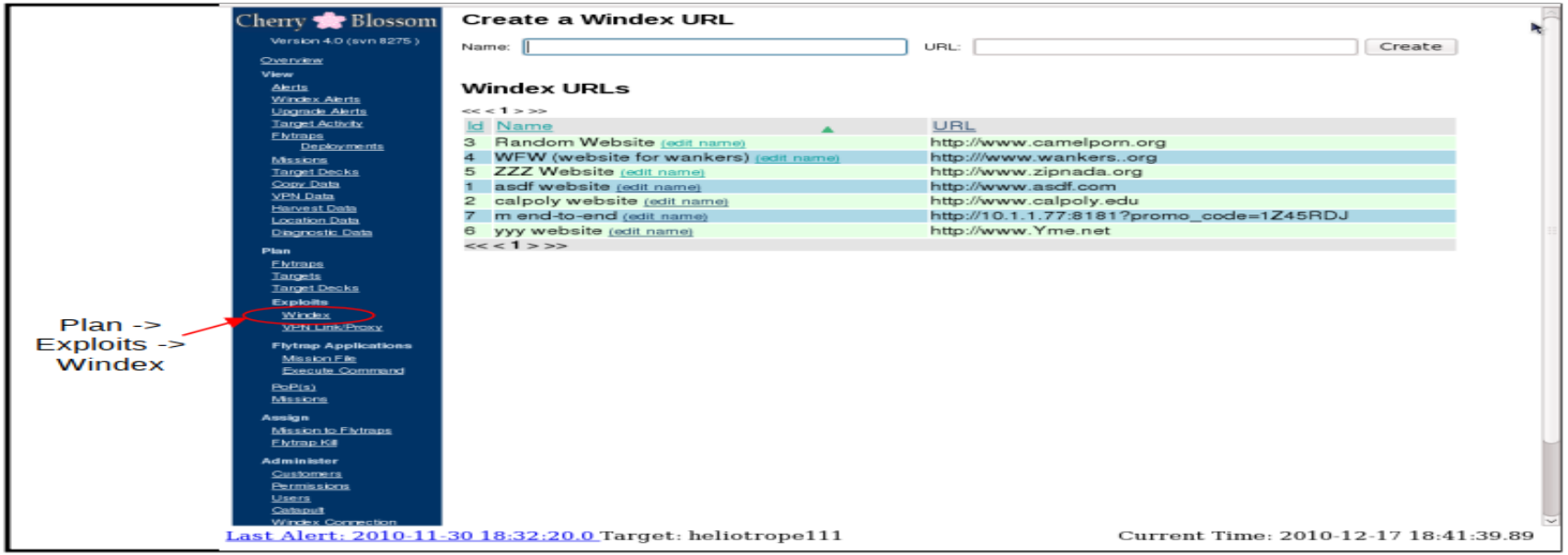


Figure 21: Cherry Web Plan -> Exploits -> Windex Page

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

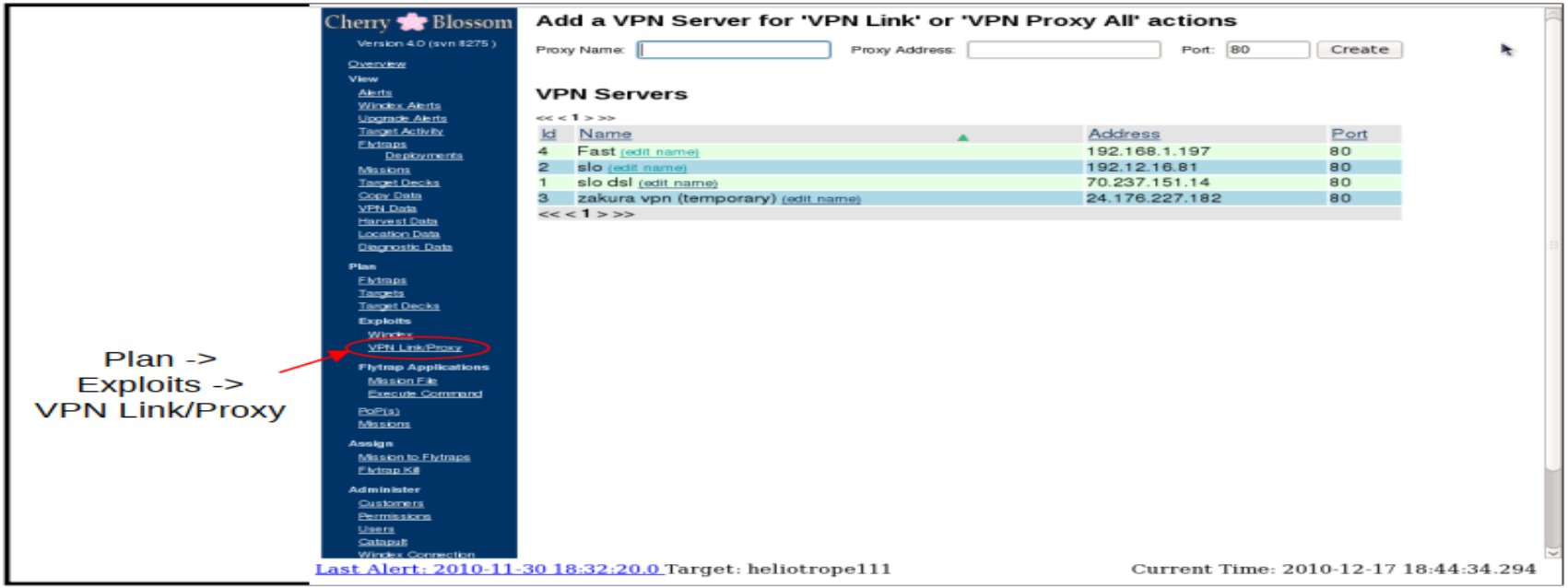


Figure 22: Cherry Web Plan -> Exploits -> VPN Link/Proxy Page

Step 4: Define Mission Files (for Application Execution)

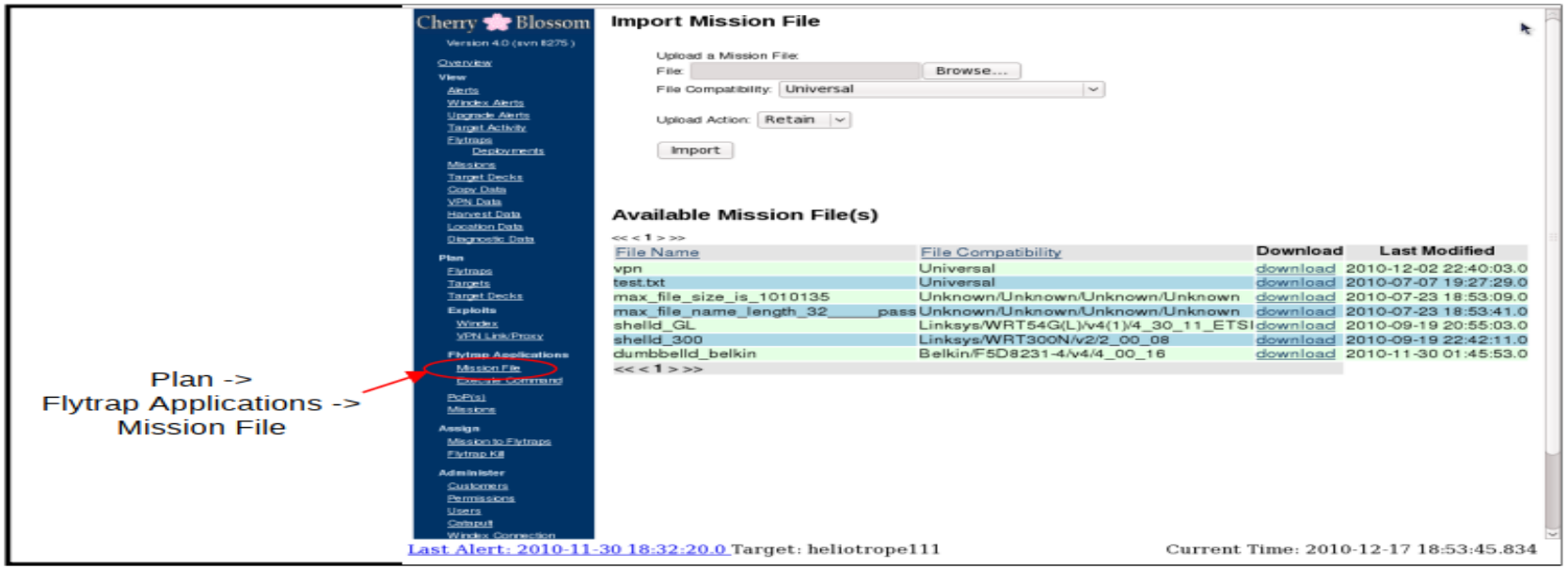


Figure 23: Cherry Web Plan -> Flytrap Applications -> Mission File Page

Step 5: Define Execute Commands (for Application Execution)

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

Step 6: Define PoPs

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

Step 7: Create a New Mission

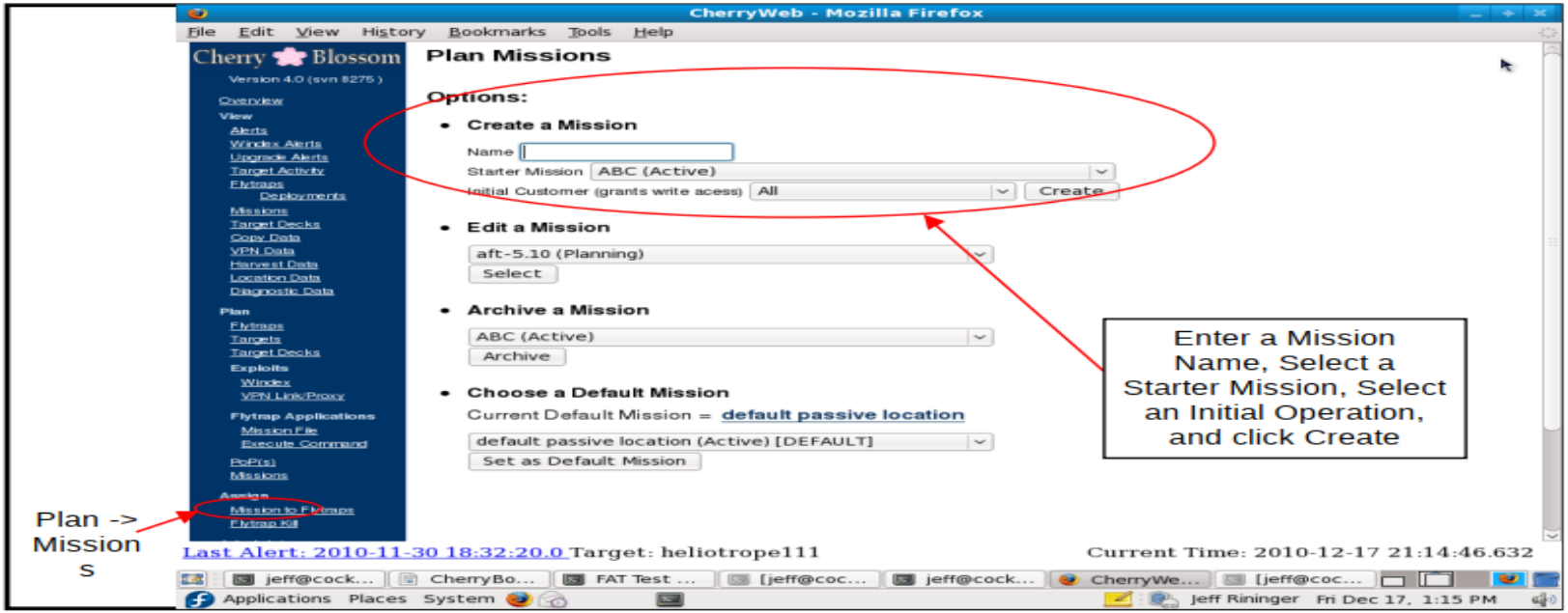


Figure 26: Cherry Web Plan -> Missions Page (Create)

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

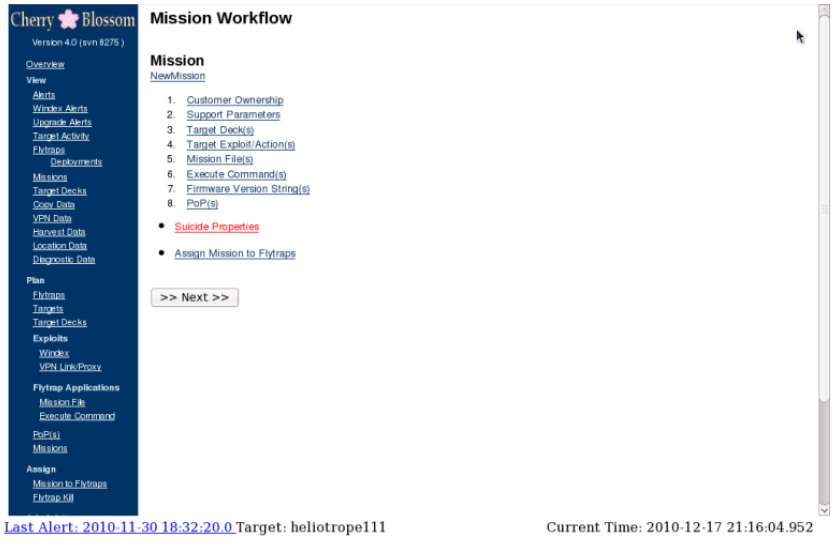


Figure 27: Cherry Web Mission Workflow Page

Figure 28: Cherry Web Mission Workflow Operation Ownership Page

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

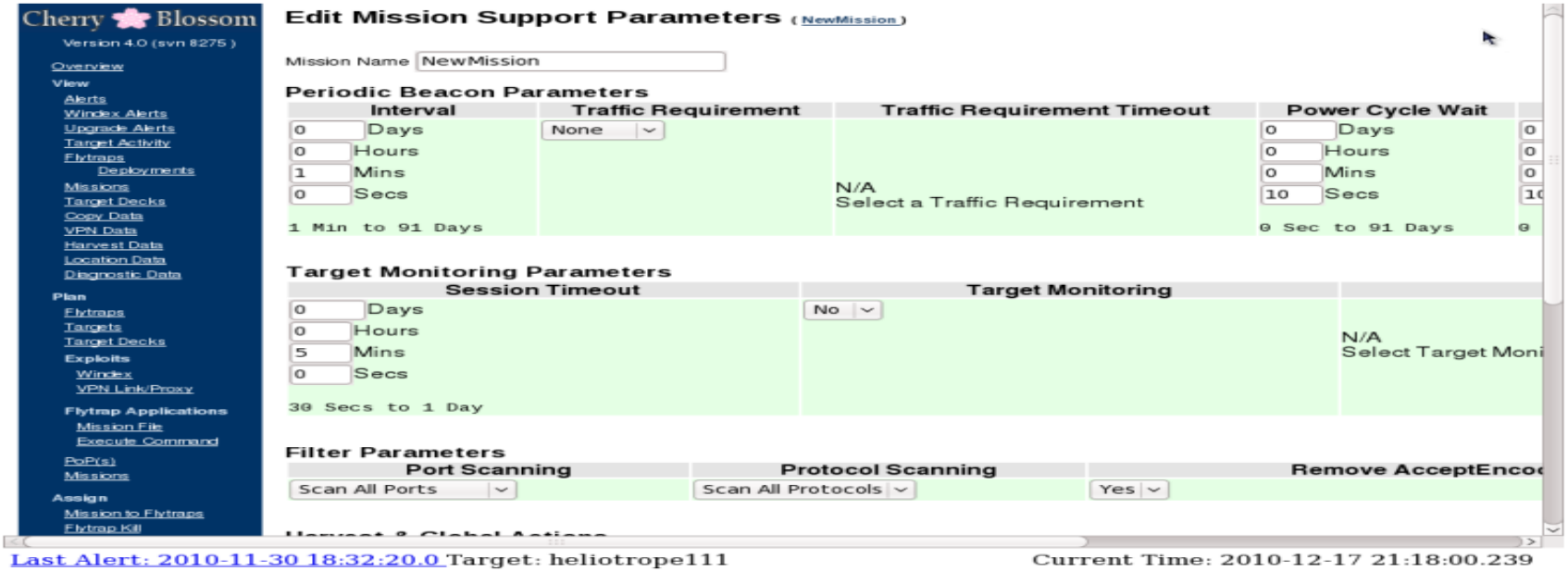


Figure 29: Cherry Web Mission Support Parameters Mission Workflow Page

Step 10: Add Target Decks (Mission Workflow 3)

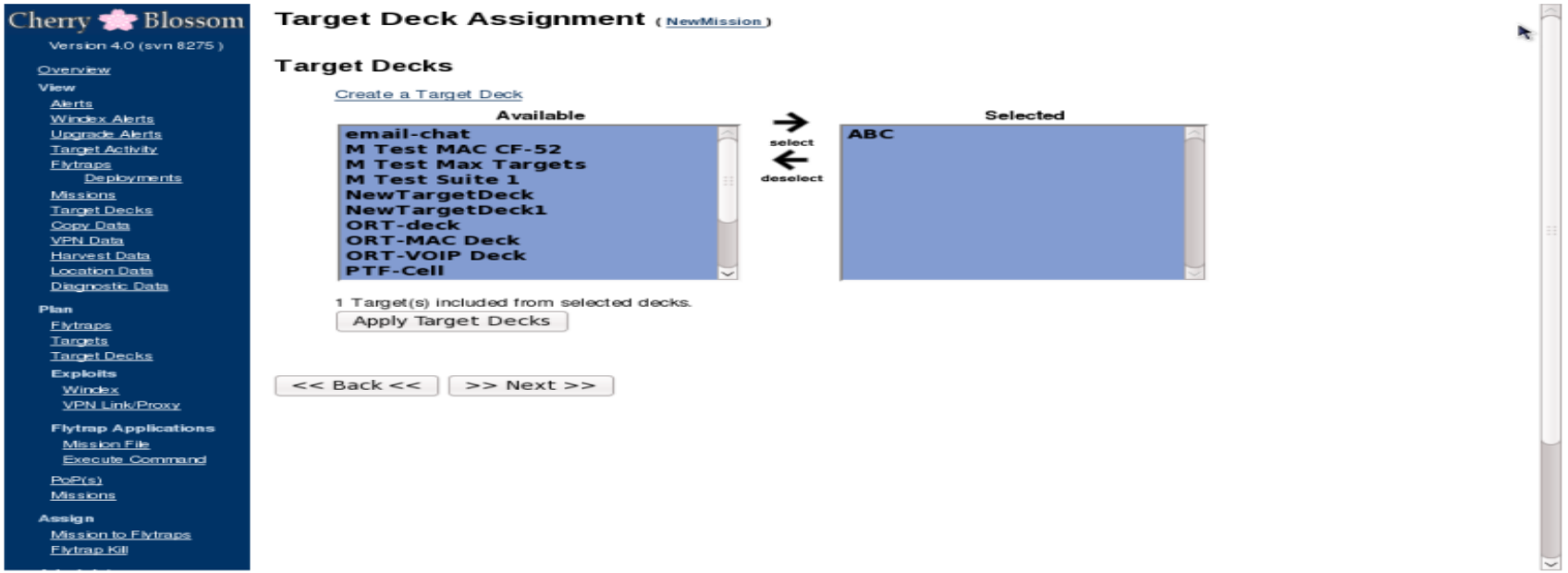


Figure 30: Cherry Web Target Deck Assignment Mission Workflow Page

Step 11: Override Target Actions (Mission Workflow 4)

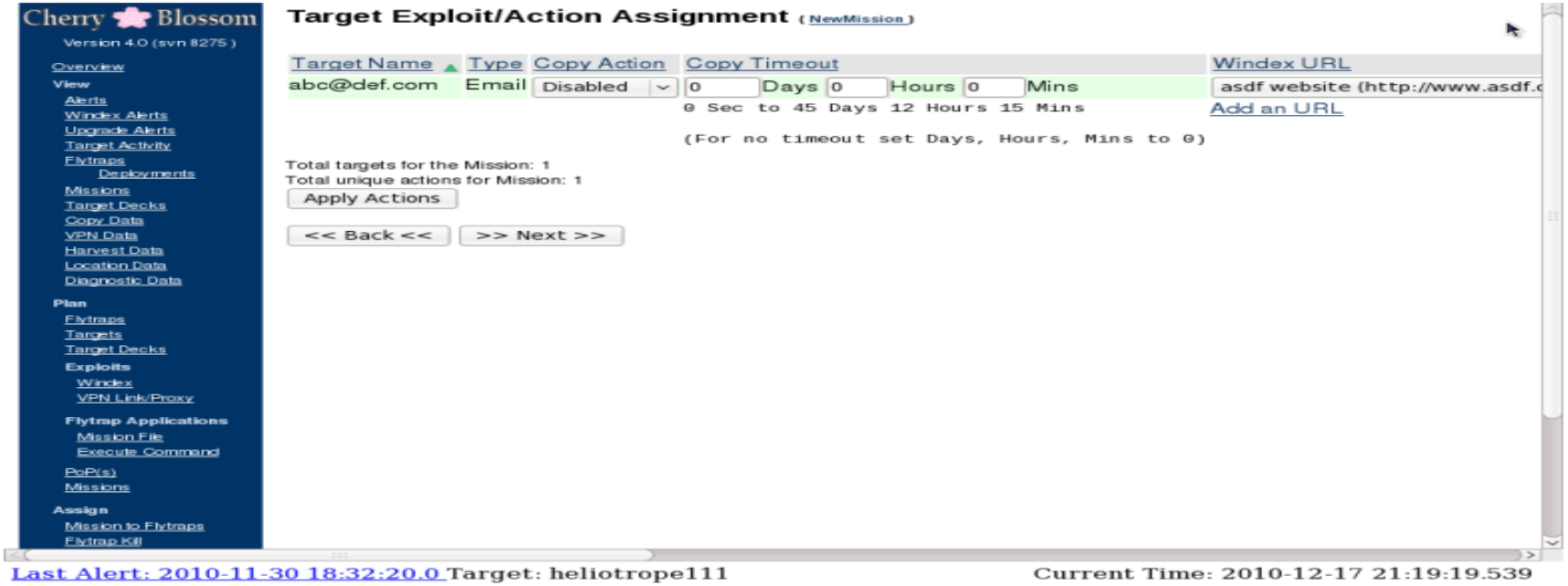


Figure 31: Cherry Web Target Exploit/Action Assignment Mission Workflow Page

Step 12: Add Mission Files (Mission Workflow 5)

Figure 32: Cherry Web Mission File Assignment Mission Workflow Page

Step 13: Add Execute Commands (Mission Workflow 6)

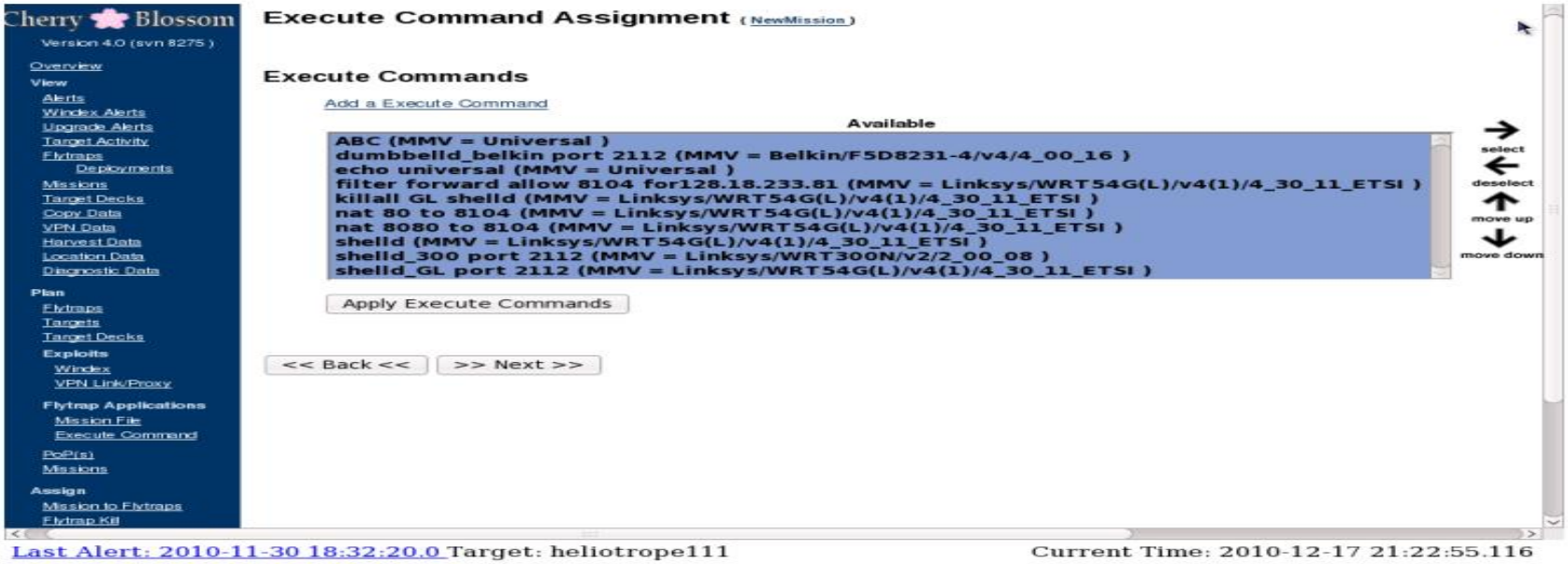


Figure 33: Cherry Web Execute Command Assignment Mission Workflow Page

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

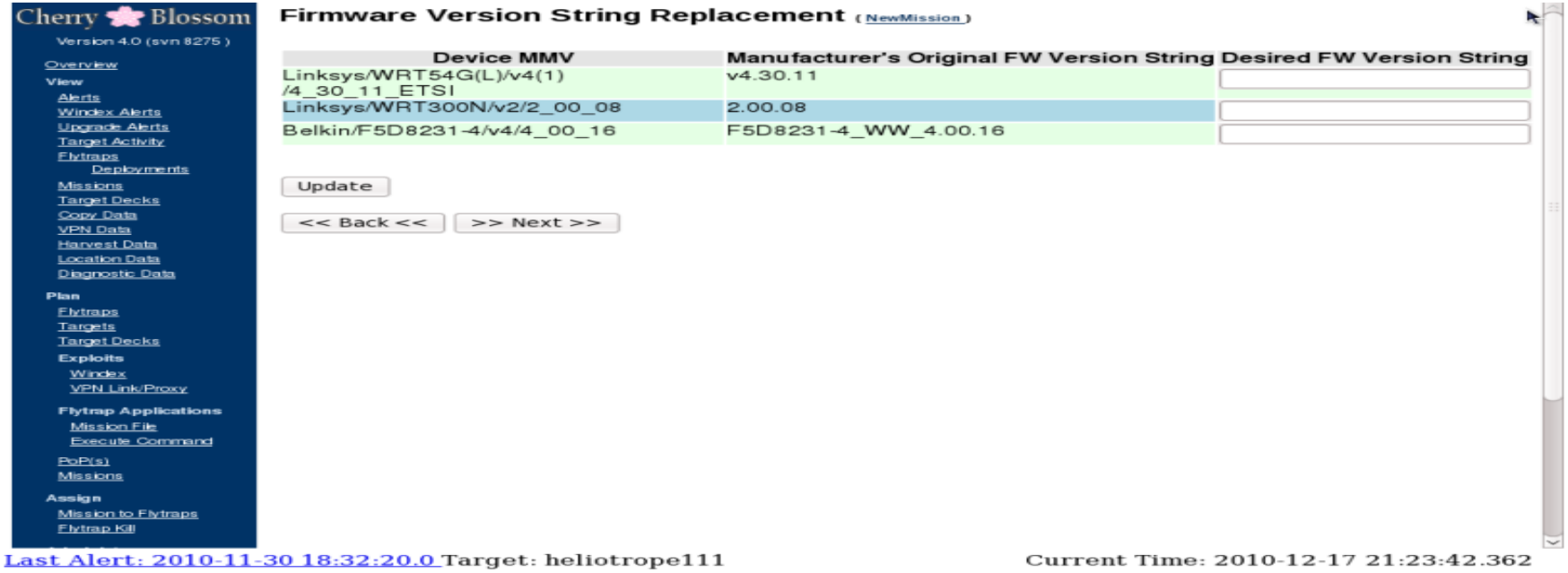


Figure 34: Cherry Web Firmware Version String Replacement Mission Workflow Page

Step 15: Add PoPs (Mission Workflow 8)

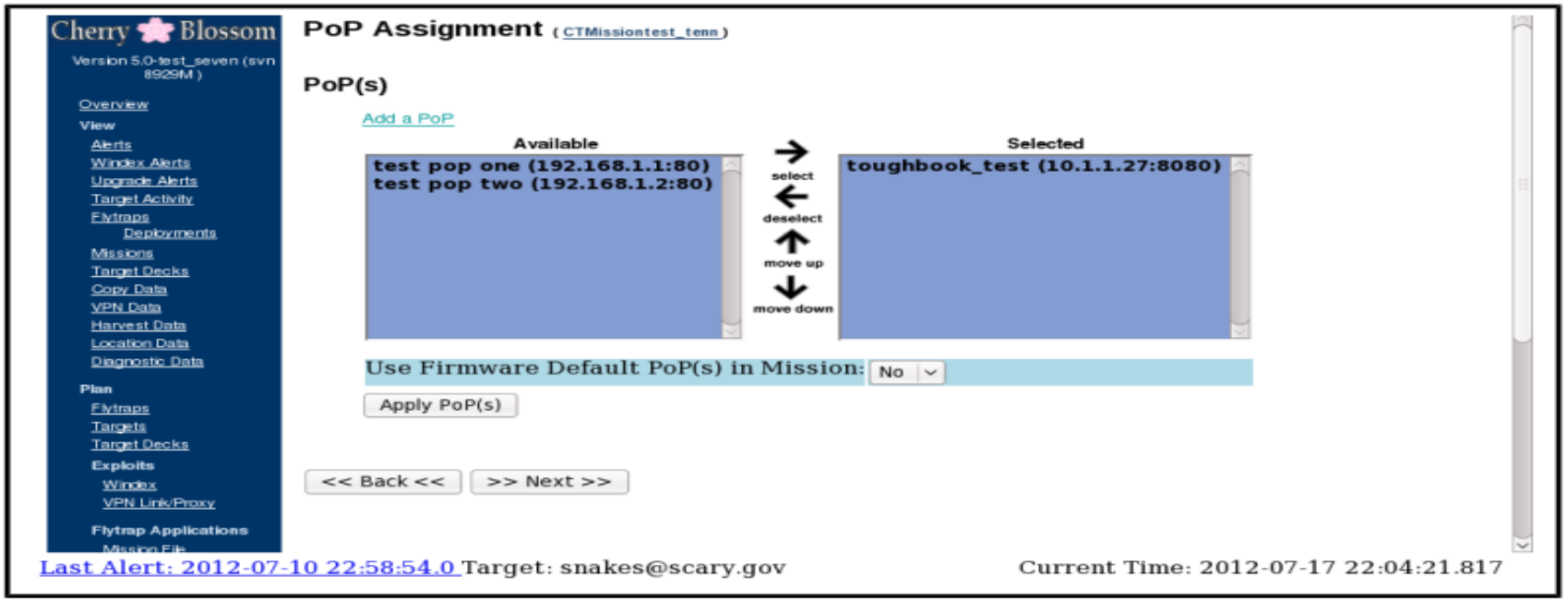


Figure 35: Cherry Web PoP Assignment Mission Workflow Page

Step 16 (Optional): Set Suicide Properties

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

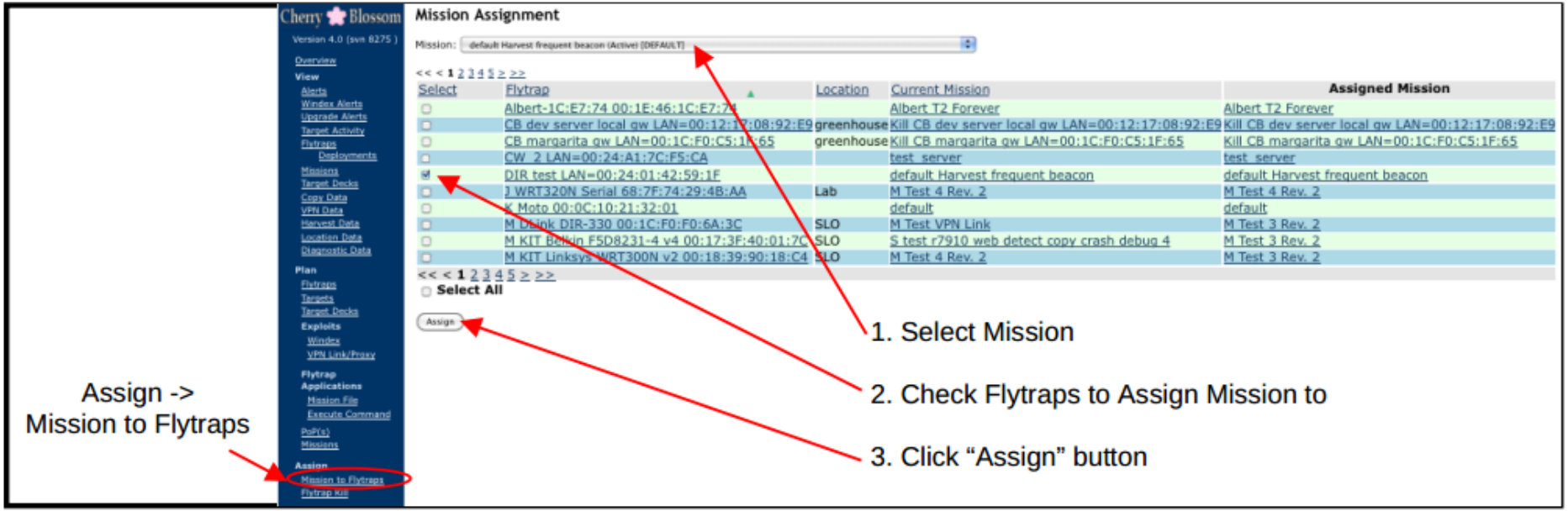


Figure 37: Cherry Web Assign -> Mission to Flytraps Page

Editing Missions

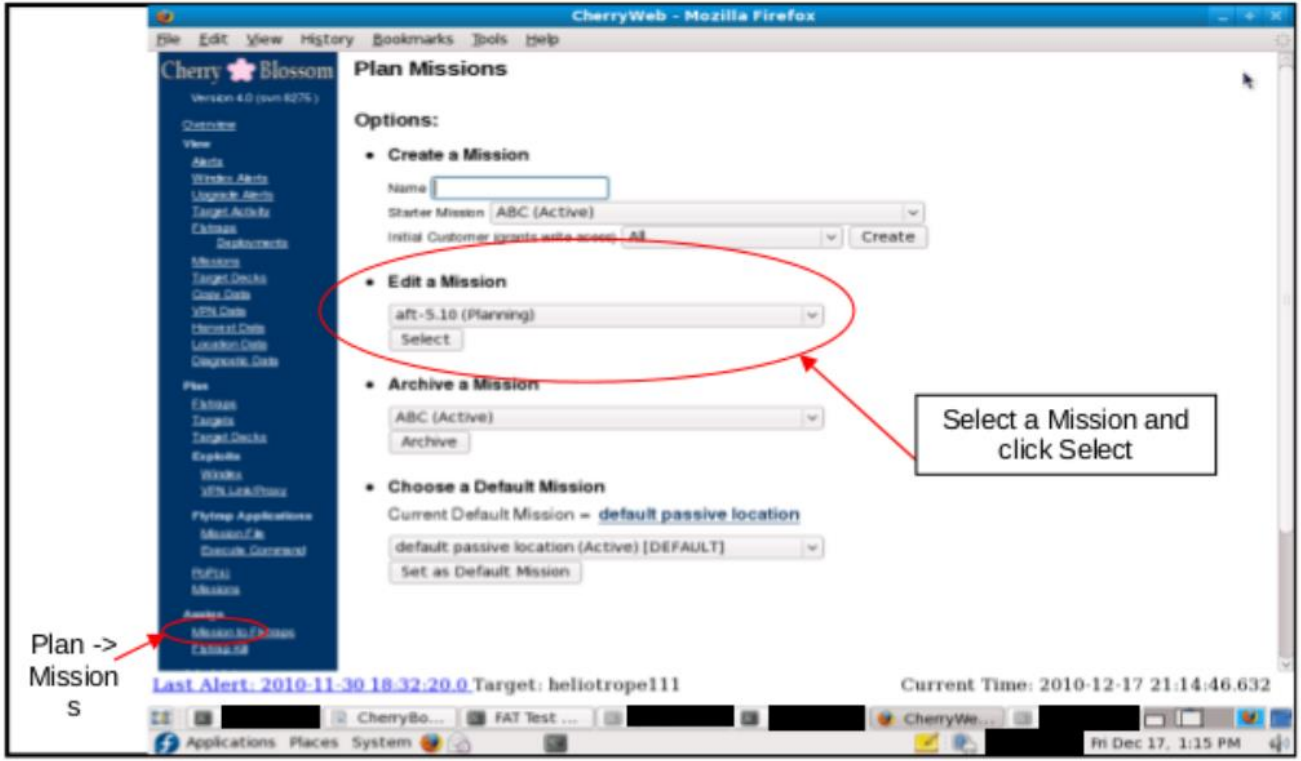


Figure 38: Cherry Web Plan -> Missions Page (Edit)

Archiving Missions

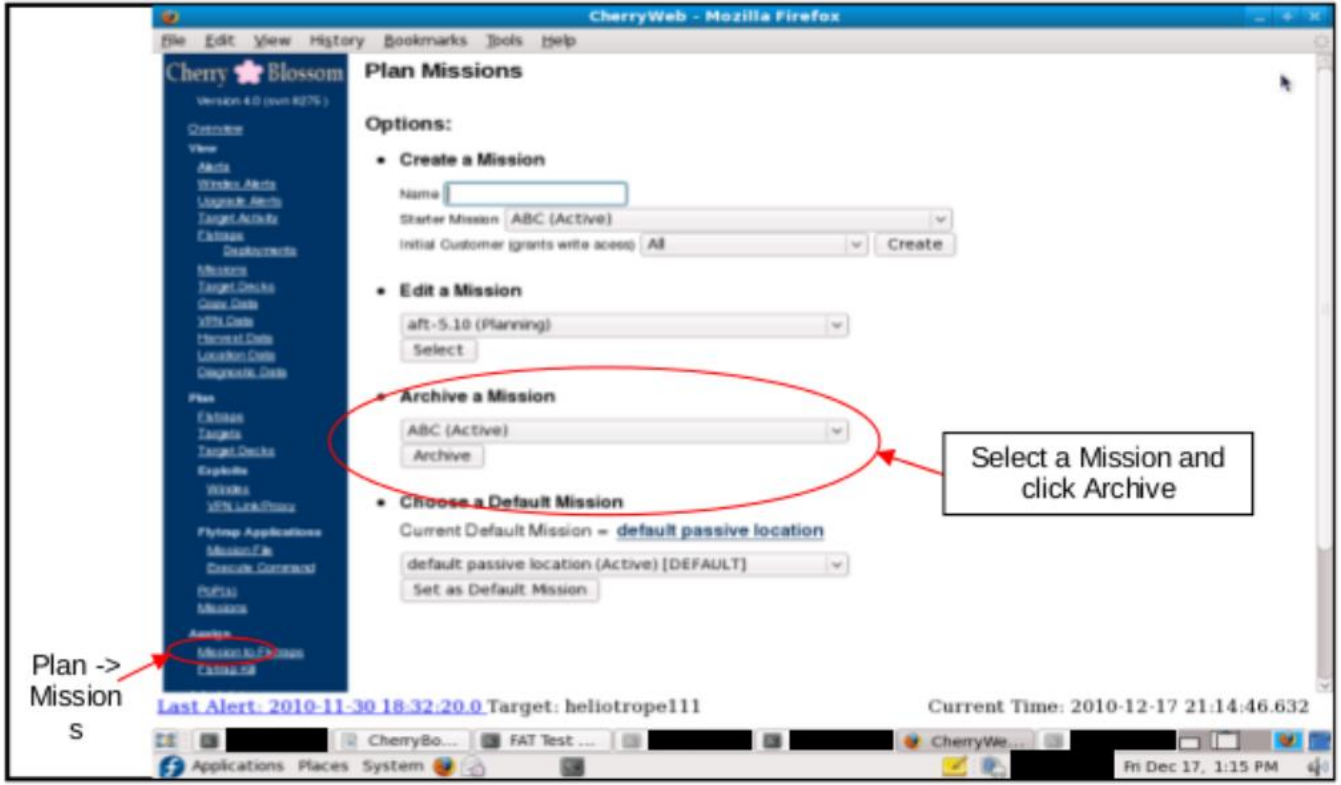


Figure 39: Cherry Web Plan -> Missions Page (Archive)

Mission States

- Planning
- Active
- Archived

Setting the Default Mission

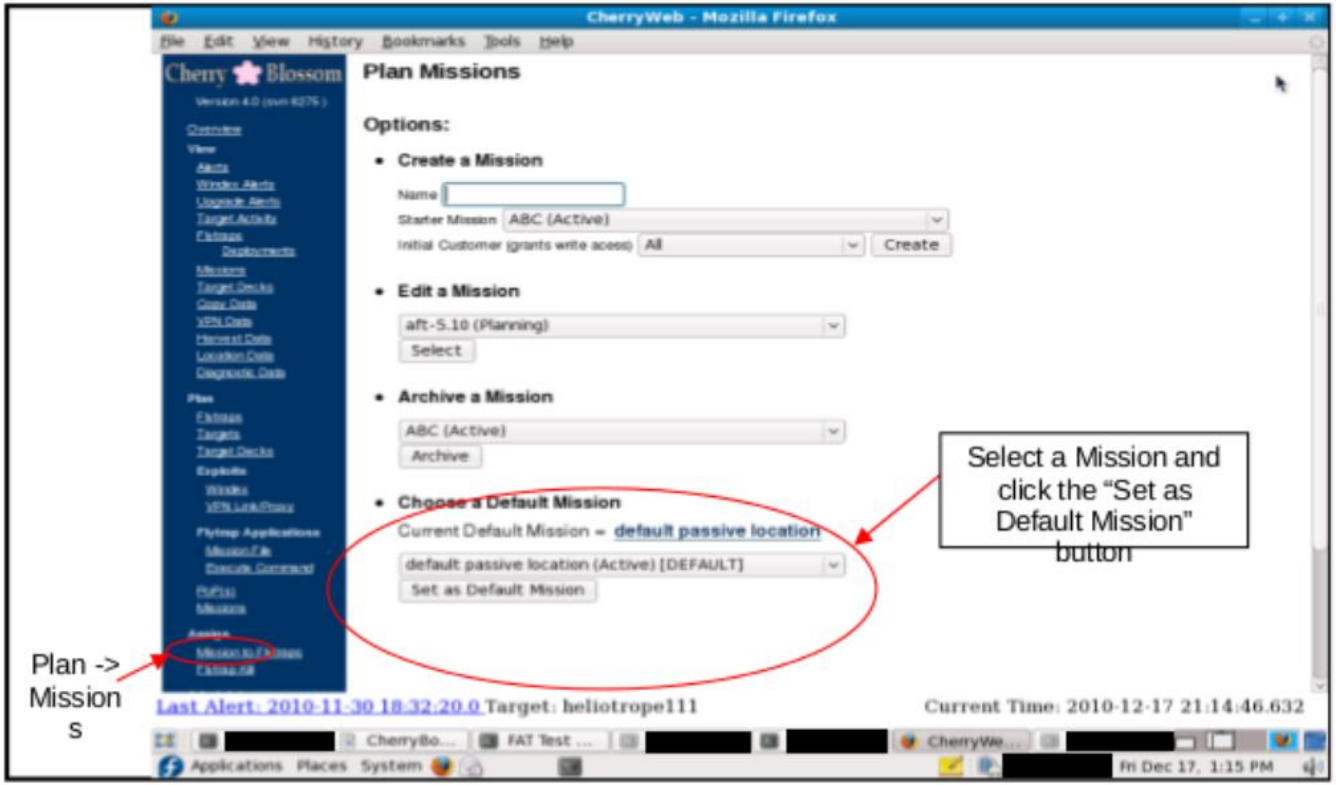


Figure 40: Cherry Web Plan -> Missions Page (Choose Default Mission)

Editing Target Decks

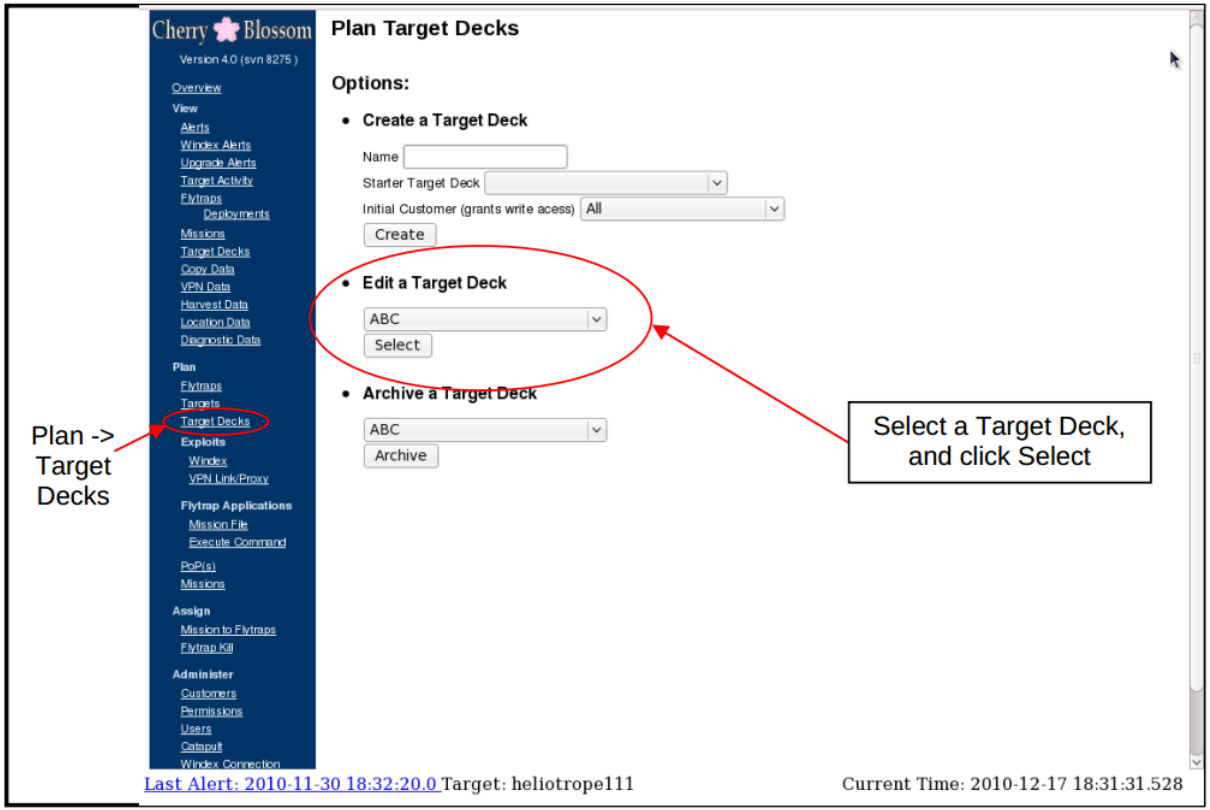


Figure 41: Cherry Web Plan -> Target Decks Page (Edit)

Assign a Kill Mission

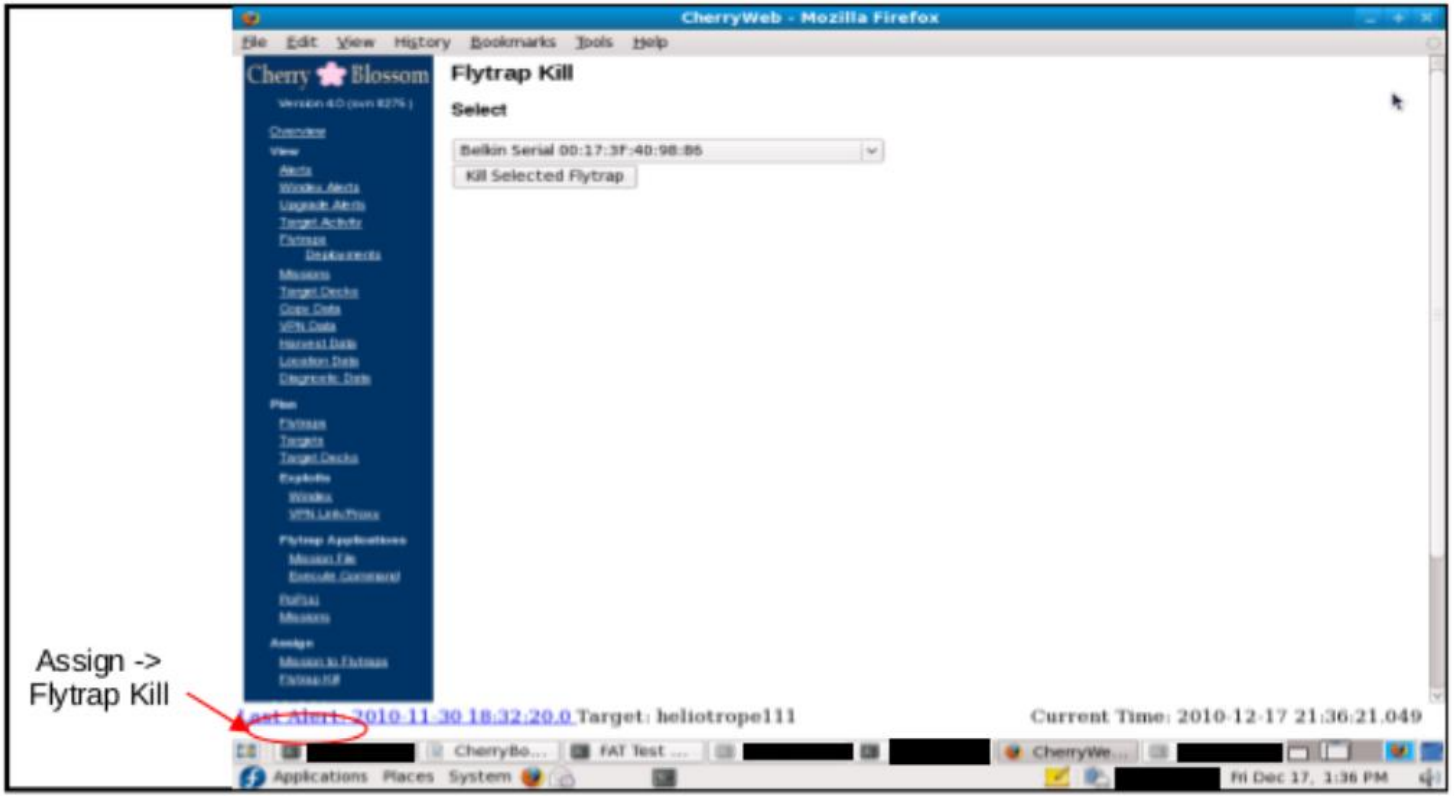


Figure 42: Cherry Web Assign -> Flytrap Kill Page

Viewing Alerts

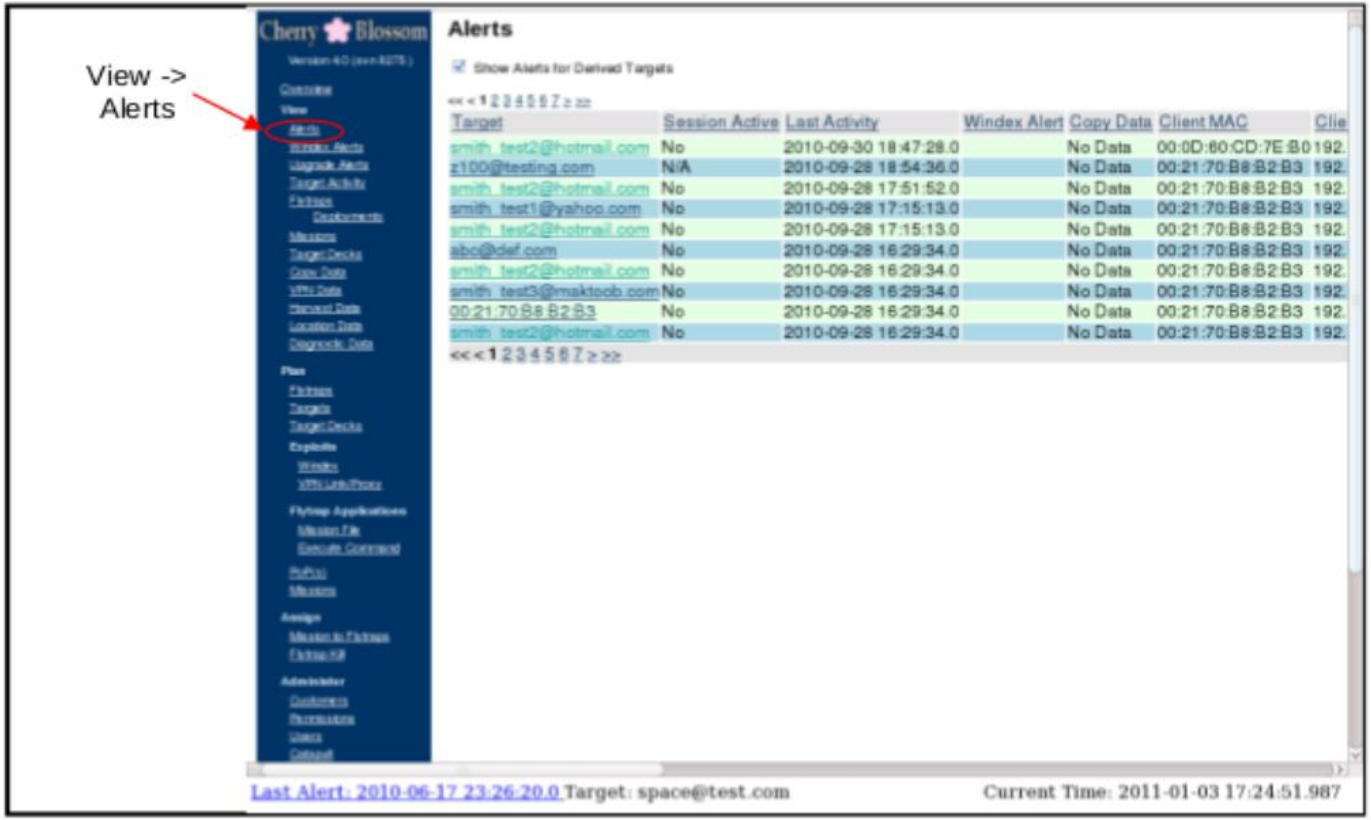


Figure 43: Cherry Web View -> Alerts Page

Viewing Target Activity

View -> Target Activity

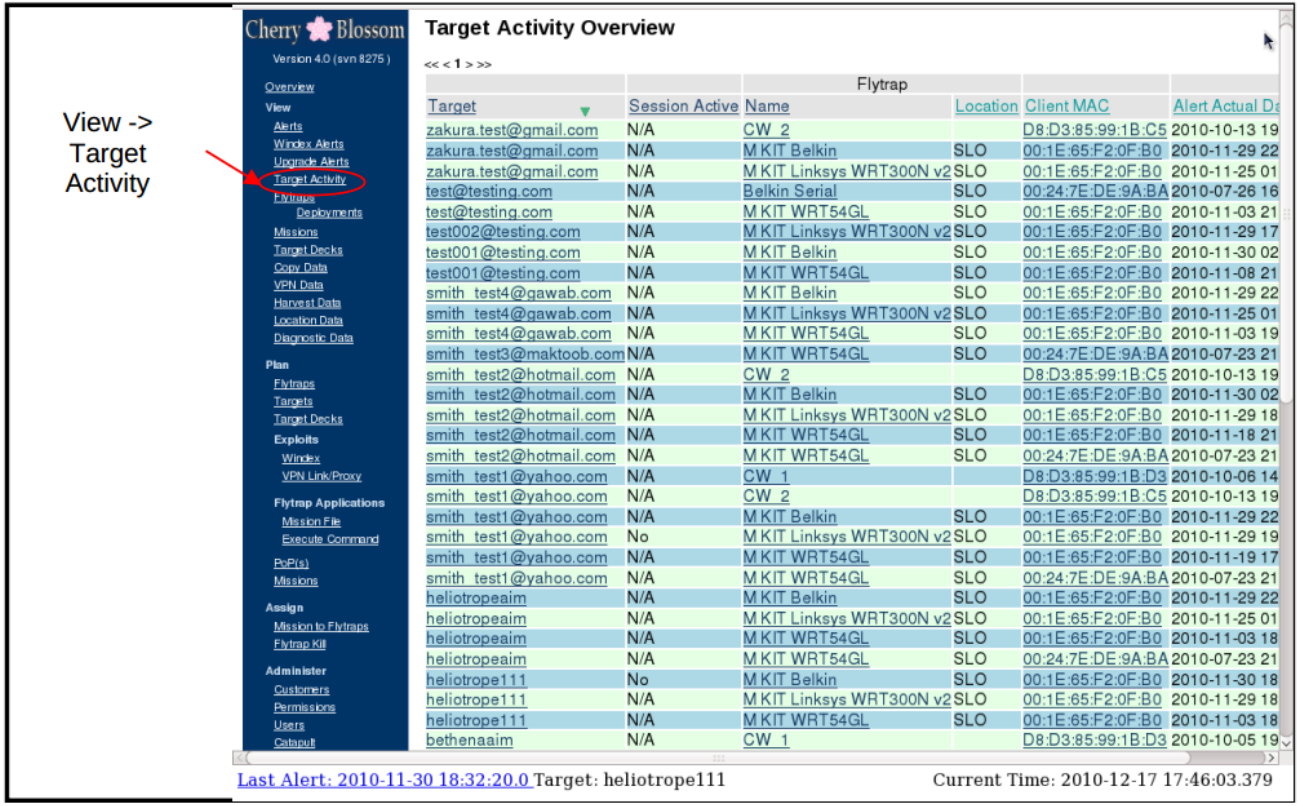


Figure 44: Cherry Web View -> Target Activity Page

Viewing Target Details

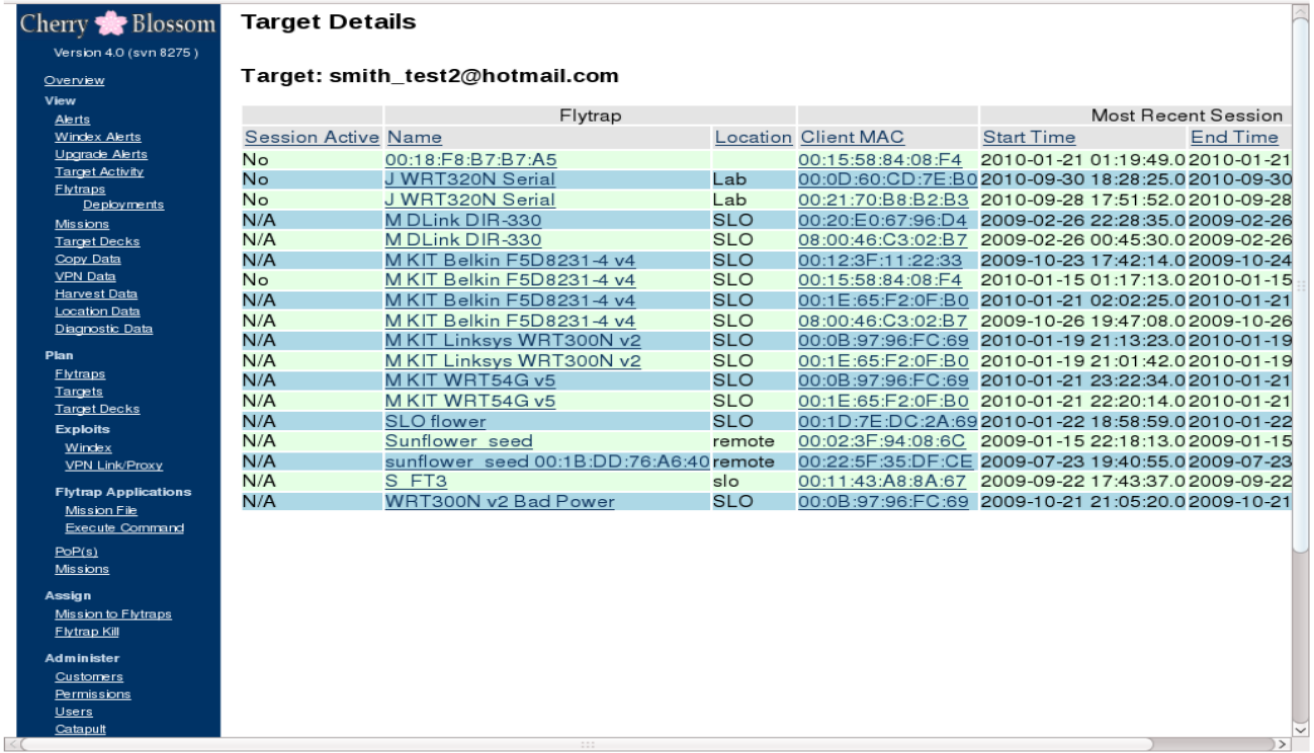


Figure 45: Cherry Web Target Details Page

Viewing Copy Data

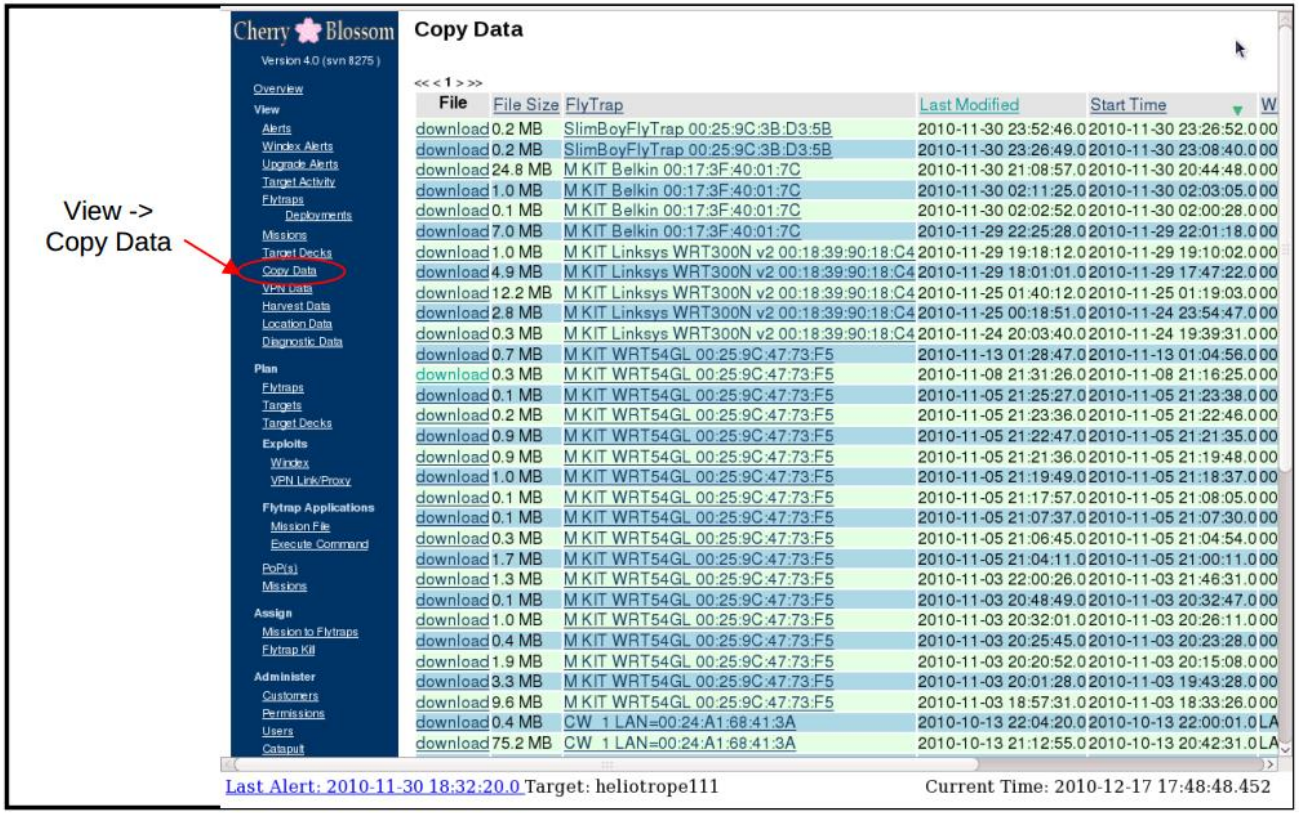


Figure 46: Cherry Web View -> Copy Data Page

Viewing VPN Data

Figure 47: Cherry Web View -> VPN Data Page

Viewing Harvest Data

View -> Harvest Data

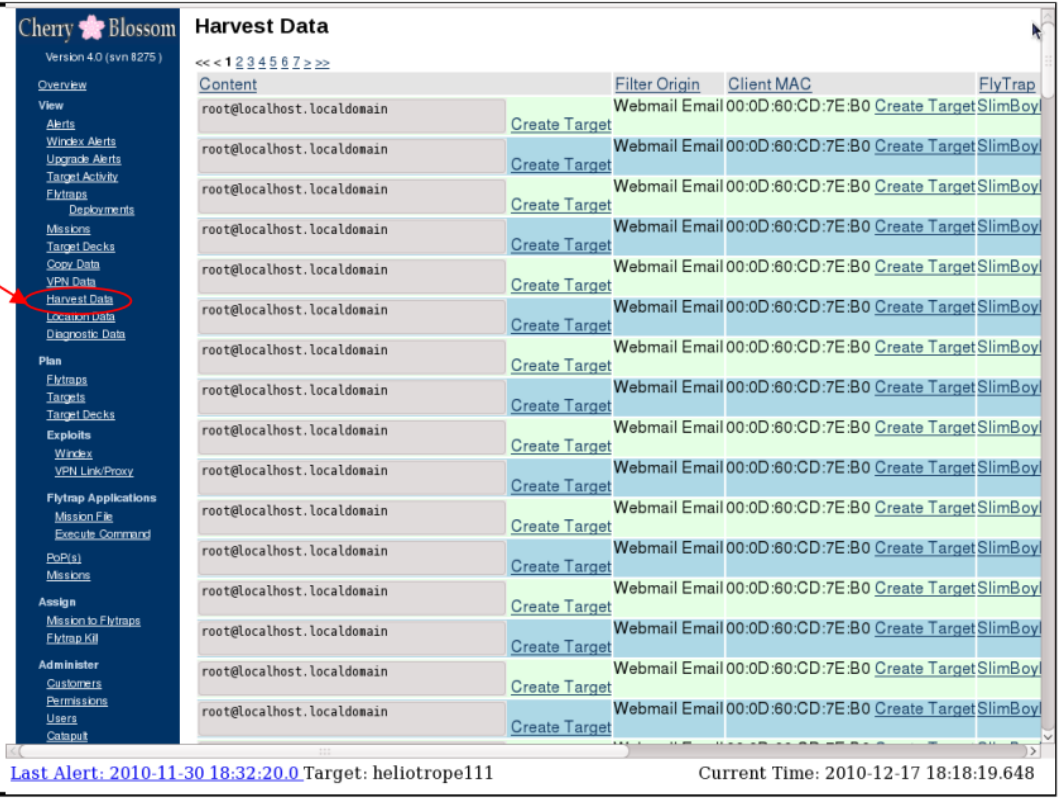


Figure 48: Cherry Web View -> Harvest Data Page

Viewing Upgrade Alerts

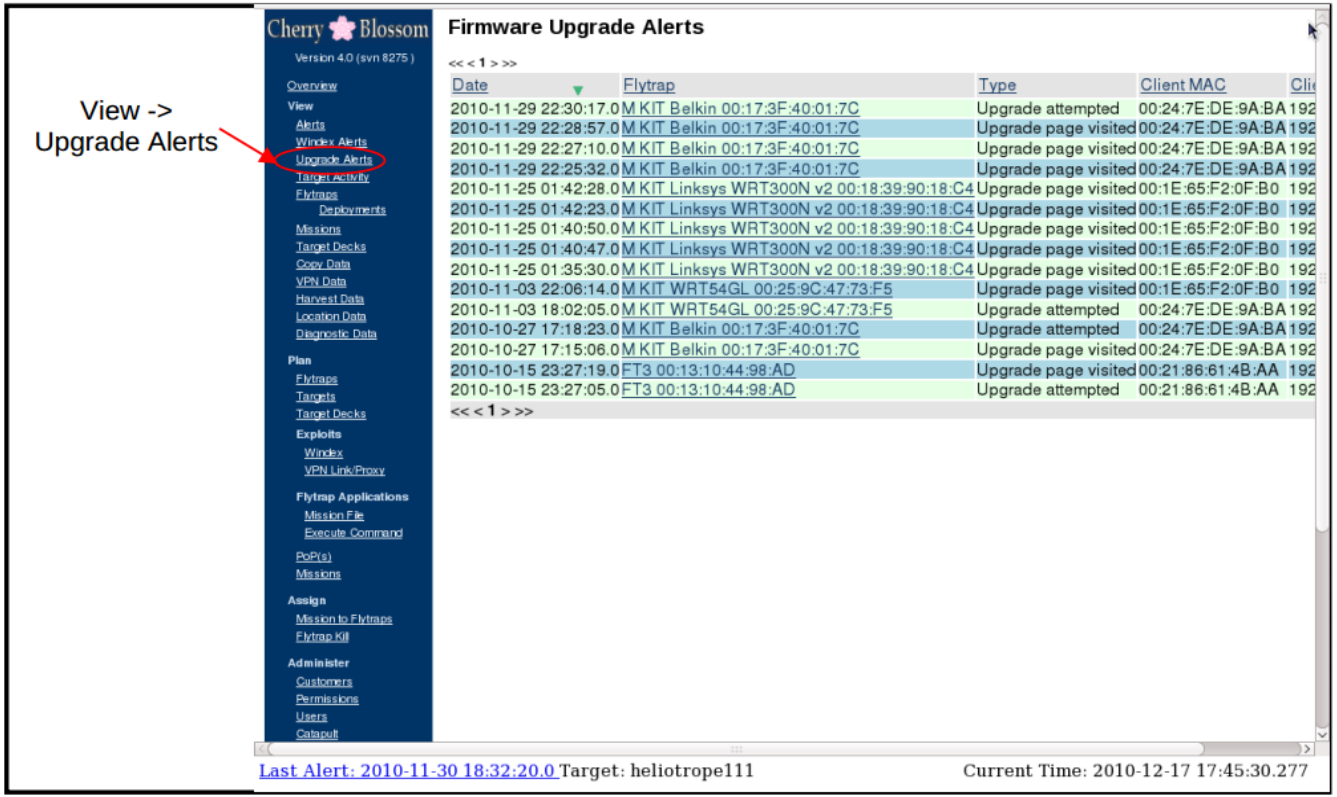


Figure 49: Cherry Web View -> Upgrade Alerts Page

Viewing Windex Alert

View -> Windex Alerts

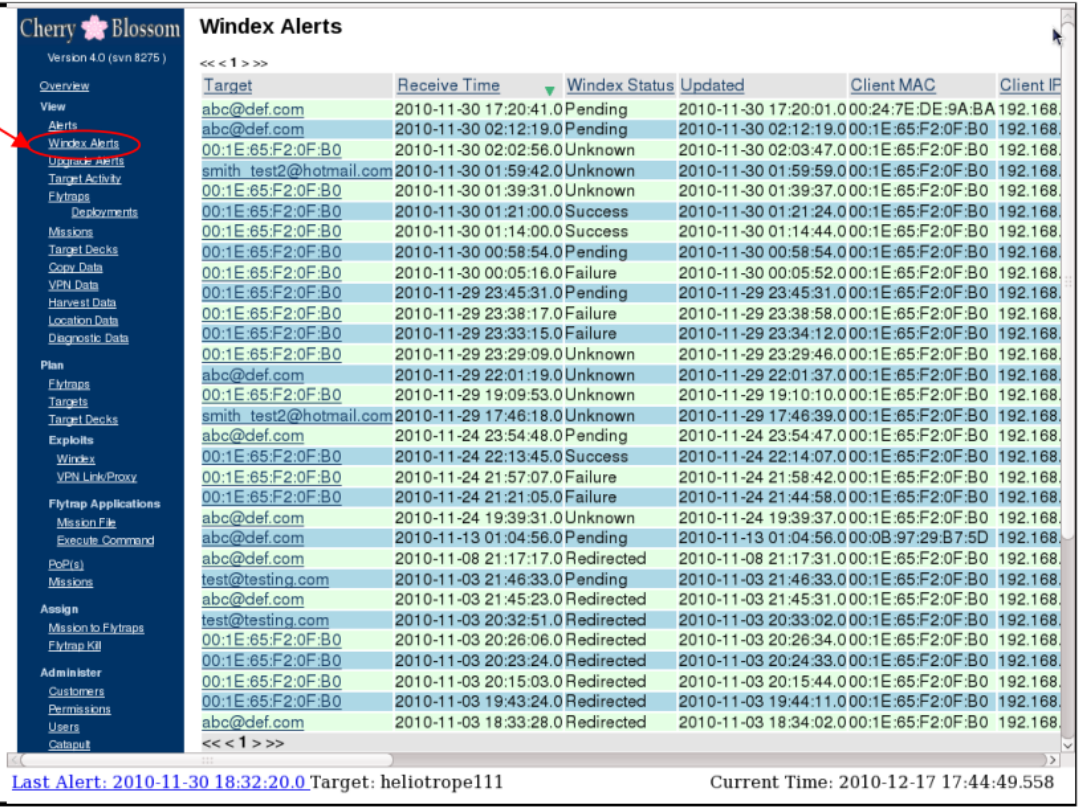


Figure 50: Cherry Web View -> Windex Alerts Page

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

Viewing Flytrap Diagnostic Data

Figure 52: Cherry Web View -> Diagnostic Data Page

One-way Transfer (OWT) of Cherry Blossom Data

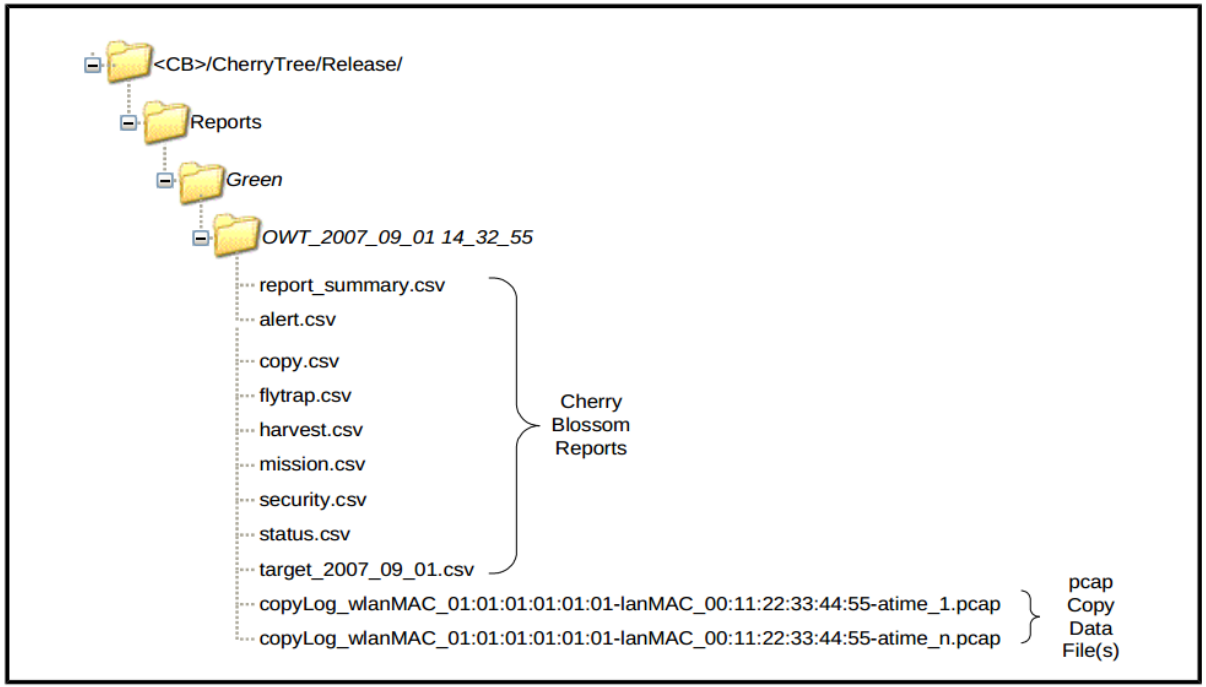


Figure 53: OWT Report Structure

Generating a OWT Report from Cherry Web

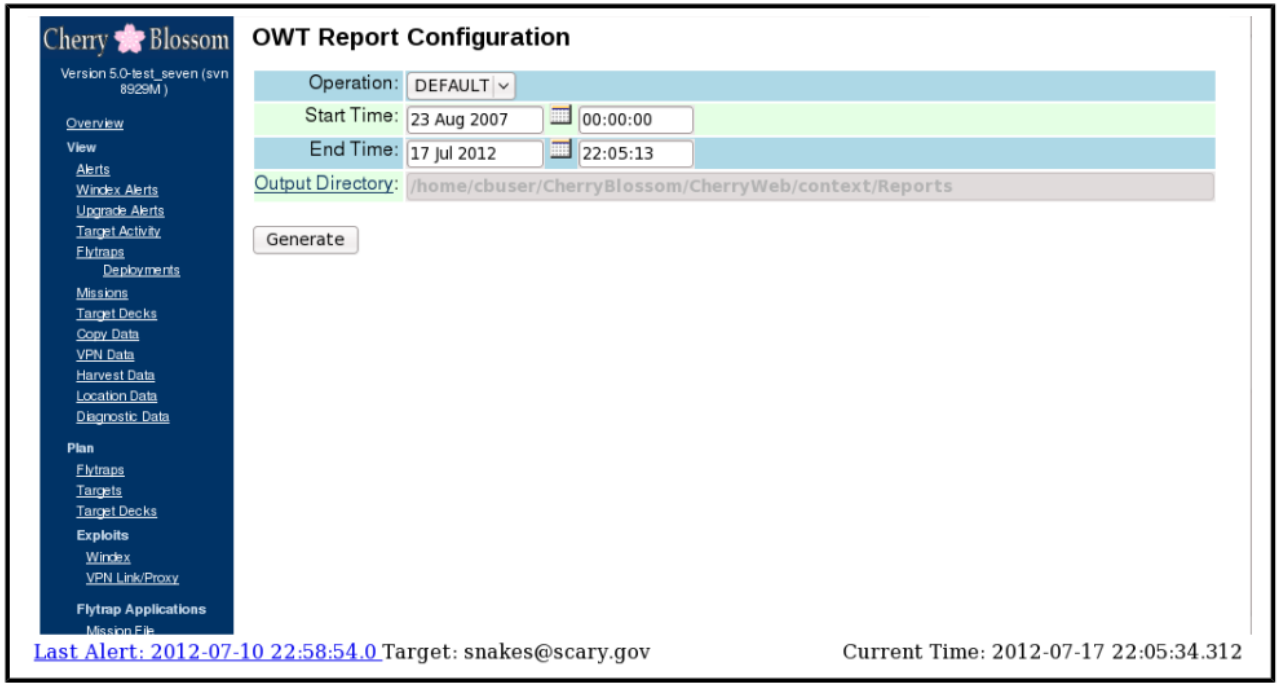


Figure 59: Generating a OWT Report from Cherry Web

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