BeEF

If You Tolerate This

Your Child Processes Will Be Next

Bart Leppens

whoami

Bart Leppens

- BeEF developer (since may 2012)
- Ported BeEF Bind shellcode to Linux
- Smashing the stack for FUN

@bmantra

In

Disclaimer

- The views and opinions expressed here are my own and **do not necessarily represent** those of my employer
- My employer has absolutely **nothing** to do with anything related to BeEF
- I’m **not** speaking in the representation of my company

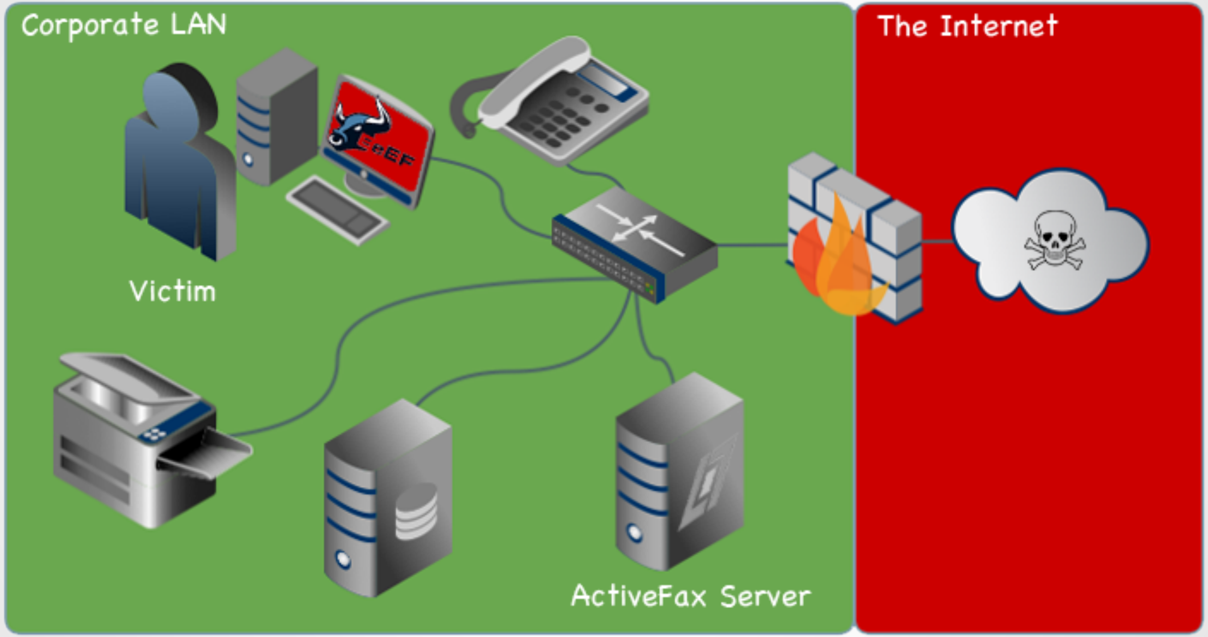
What the talk?

- BeEF: Browser Exploitation Framework
- IPC: Inter-Protocol Communication
- IPE: Inter-Protocol Exploitation
- BeEF Bind Shellcode
- Binding shells with BeEF

BeEF: Browser Exploitation Framework

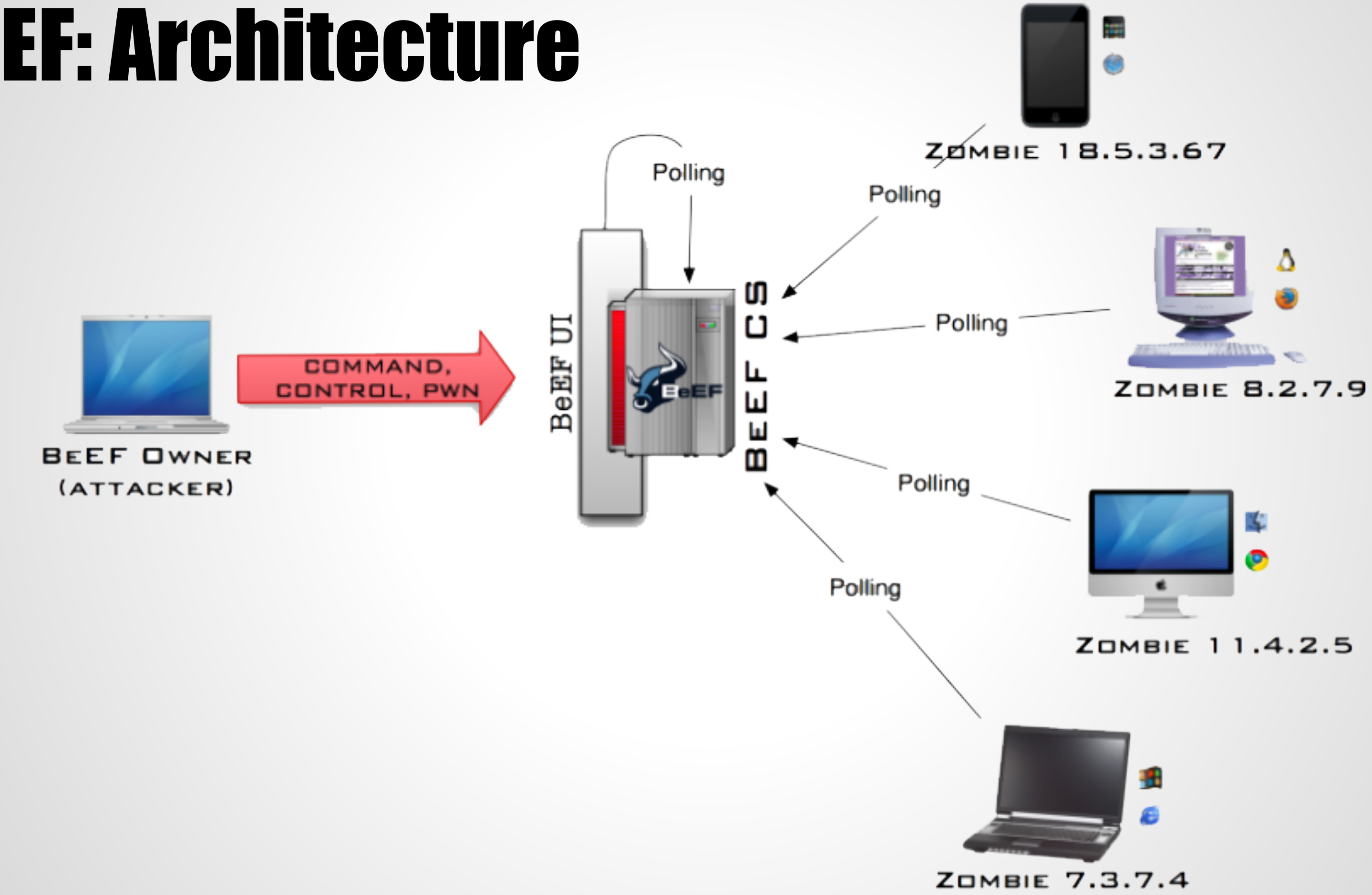
- Professional security tool
- Focus on client side attack vectors
- Real attack scenarios
- v1.0 by Wade Alcorn

BeEF: Sesame Magic Browser



"Internal server vulnerabilities are sitting there bored and lonely"
- Michele Orru` // "ActiveFax, you look very bored" - Bart Leppens

BeEF: Architecture



BeEF: A Whole Lot Of Modules

- Many different purposes
  - Information gathering
  - Social Engineering
  - Network Discovery
  - ...
- Easy to extend with your own modules
- Complex scenarios with RestFul API

BeEF: DEMO

IPC: Inter-Protocol Communication

- Initial research by Wade Alcorn in 2006/2007
- “Tolerant” protocol implementation that does not drop the client connection after N errors
- A properly encoded POST request can be send to the target:
  - HTTP Headers are parsed as BAD COMMANDS
  - HTTP request body is parsed as VALID COMMANDS (or as SHELLCODE)

IPC: Limitations

- Some ports are banned by the Browser (e.g. 21,25,110,..)
- Content-Type: text/plain or multipart/form-data
- Doesn’t work well with binary protocols => often not that tolerant

IPC: ActiveFax Server

- Extended research done by Michele Orru` & myself
- Widely used Fax solution
- Manual suggest port 3000 for RAW socket
- Protocol is very tolerant
- Commands are formatted as: @Fxxx data@

IPC: ActiveFax Server (example message)

Sender...................... Bart Leppens, +1 11 112233-25
Recipient 1............... OWASP Belgium, Fax: 016 123456
Subject..................... IPC is cool
Priority..................... Very High

```
@F101 Bart Leppens@@F110 +1 11 112233-25@
@F201 OWASP Belgium@@F211 016 123456@
@F307 IPC is cool@
@F301 1@
```

IPC: ActiveFax Server (XHR)

```
var xhr = new XMLHttpRequest();
var uri = "http://x.x.x.x:3000/";
xhr.open("POST", uri, true);
xhr.setRequestHeader("Content-Type", "text/plain");
var post_body = "@F101 Bart Leppens@@F110 +1 11 112233-25@@F201 OWASP Belgium@@F211 016 123456@@F307 IPC is cool@@F301 1@";
xhr.send(post_body);
```

IPC: ActiveFax Server (XHR)

```
POST / HTTP/1.1
Host: 127.0.0.1:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:24.0) Gecko/20100101 Firefox/24.0
..
Content-Type: text/plain; charset=UTF-8
Cache-Control: no-cache


@F101 Bart Leppens@@F110 +1 11 112233-25@@F201 OWASP Belgium@@F211 016 123456@@F307 IPC is cool@@F301 1@
```

IPC: ActiveFax Server (Demo)

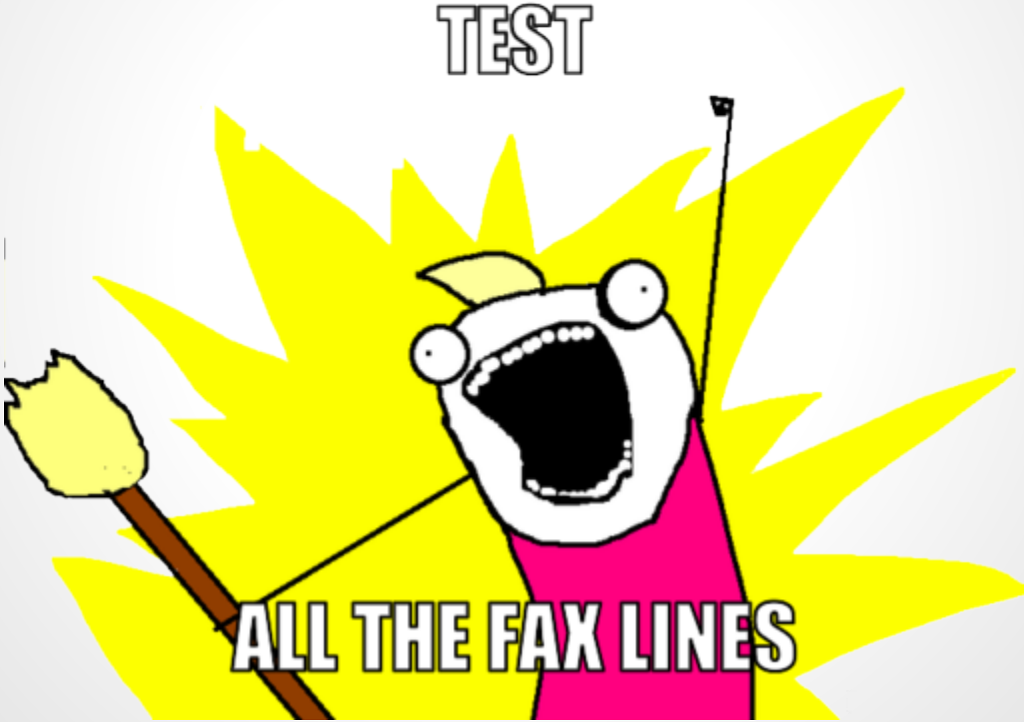
IPC: ActiveFax Server (Time-out)

The ActiveFax RAW socket takes 60 seconds to time-out.

We can fix that! 2 seconds is more then enough to send a FAX over a LAN network:

```
xhr = new XMLHttpRequest();
..
xhr.send(post_body);
setTimeout(function(){xhr.abort()}, 2000);
```

IPC: ActiveFax Server (Faster Demo)



IPE: Inter-Protocol Exploitation

- Research by Wade Alcorn (extension of IPC)
- Extended research in 2012 by Michele Orru`
  - QualCOMM WorldMail IMAP 3.0
- More research in 2013 by Michele & myself
  - ActiveFax Server

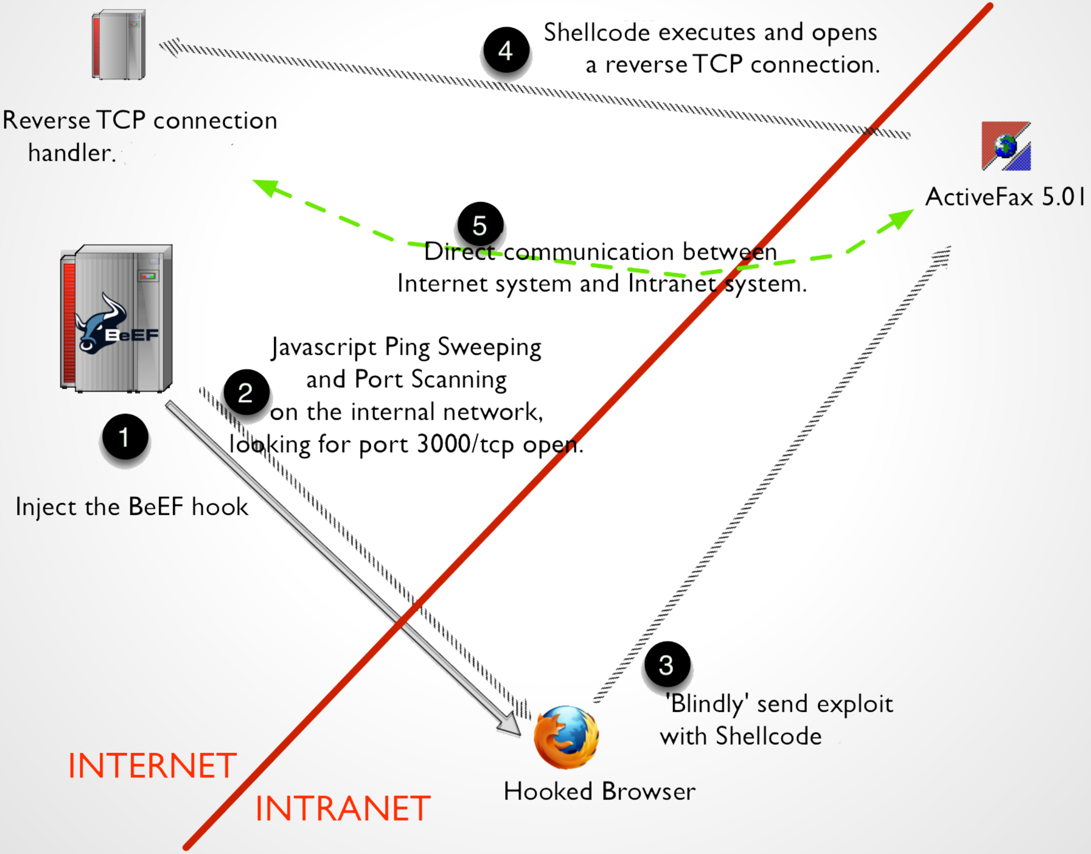
IPE: Inter-Protocol Exploitation

- Need to send binary data
  - sendAsBinary (FF, Chrome)
- Same restrictions: tolerance, blocked ports
- More restrictions: header space, bad chars

IPE: ActiveFax 5.01 RAW Server Exploit

- bug found by Craig Freyman
- @F506 crashes after 1024 bytes
- Many bad characters:
  - 0x00 -> 0x19
  - 0x40 (@)
- PoC modified to use IPE

IPE: ActiveFax (Metasploit Reverse shell)



4 Shellcode executes and opens a reverse TCP connection.

Reverse TCP connection handler.

ActiveFax 5.01

5 Direct communication between Internet system and Intranet system.

Javascript Ping Sweeping and Port Scanning on the internal network, looking for port 3000/tcp open.

2

1 Inject the BeEF hook

3 'Blindly' send exploit with Shellcode

Hooked Browser

INTERNET

INTRANET

IPE: ActiveFax (Demo)

BeEF Bind Shellcode

- Shellcode written by Ty Miller (Win32)
- Allows communication from the browser to a shell
    - Commands are proxied back and forth through the browser to cmd.exe
    - Stage is delivered through the browser as well

BeEF Bind Shellcode: The Stager

- Stager listens on a specified port for HTTP requests
- Ignores HTTP headers and looks for the egg “cmd=” which marks the start of our 2nd stage (or any stage you like)
- Allocate executable memory + copy
- Jump into the stage shellcode

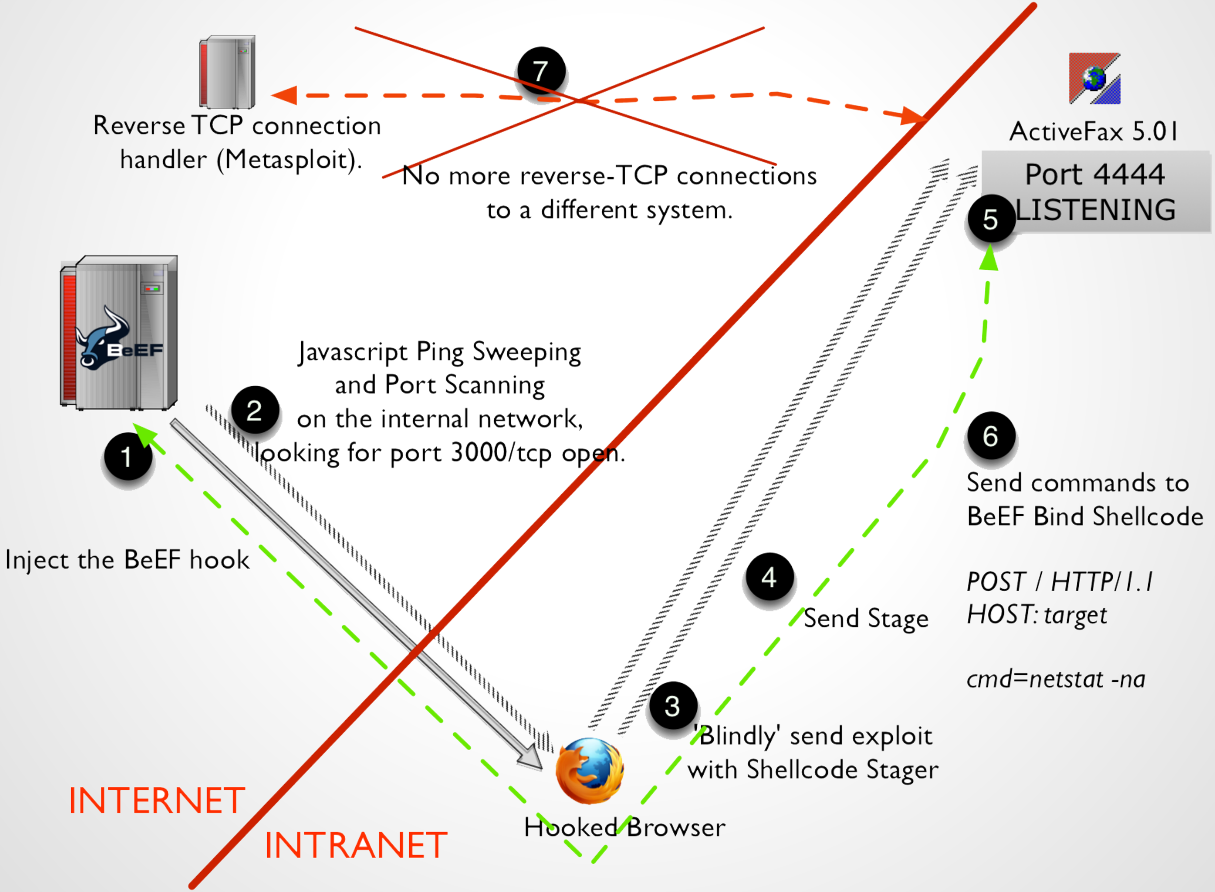
BeEF Bind Shellcode: The Stage

- Stage listens on a specified port for HTTP requests as well
- Ignores HTTP headers and looks for “cmd=” which marks the start of our command
- Requests are proxied back and forth from the browser to a “cmd.exe” childprocess
- Access-Control-Allow-Origin: *

BeEF Bind Shellcode:

- Ported to Linux x86 and Linux x64
  - stager and stage
- Can also be used compiled with RCE vulns
- Metasploit modules are available for easily encoding and removal of bad characters

IPE: ActiveFax (BeEF Bind + BeEF)

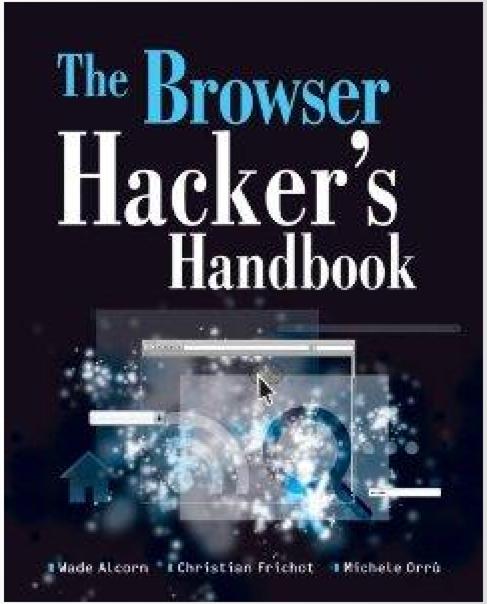


7
Reverse TCP connection handler (Metasploit).
No more reverse-TCP connections to a different system.
ActiveFax 5.01
Port 4444 LISTENING
5
BeEF
2
Javascript Ping Sweeping and Port Scanning on the internal network, looking for port 3000/tcp open.
1
Inject the BeEF hook
6
Send commands to BeEF Bind Shellcode
POST / HTTP/1.1
HOST: target
cmd=netstat -na
4
Send Stage
3
'Blindly' send exploit with Shellcode Stager
INTERNET
INTRANET
Hooked Browser

IPE: ActiveFax (Demo)

For those who can’t get enough

- Browser Hackers Handbook
  - Chapter 10: Attacking Networks
  - out march 2014
  - 50% of revenues will be used for the BeEF project (testing infrastructure, etc..)



Thanks to

- OWASP Belgium
- (ISC)2
- The other BeEF guys
- My wife for lending her laptop

Questions