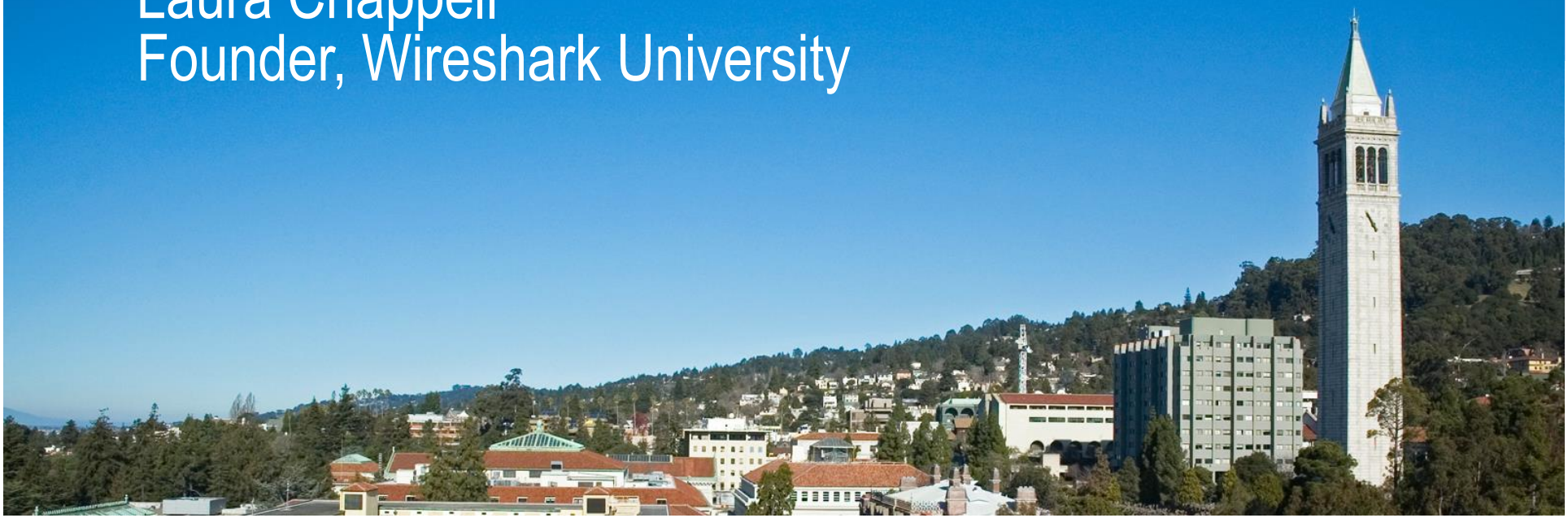
SHARKFEST '13

Wireshark Developer and User Conference

SEC-7

Wireshark Network Forensics

Laura Chappell
Founder, Wireshark University



How *not* to lock your bike…

wireshark.org Attack (Today)

- >40,000 SYNs/second
- Client Symptoms – no connection
- Client Trace File - SYN, backoff, SYN
- Server Trace File – SYN, SYN, SYN…
- Signature of Attack – Let's look inside the SYNs
- Something looks familiar here…

DDoS: Banking Sector

Since September 2012, hackers have launched major disruptive DDoS attacks that temporarily took down the online banking sites of many major U.S. banks, such as Bank of America, Citi, PNC, Capital One, Fifth Third Bank, Wells Fargo, U.S. Bancorp, BB&T and HSBC. The hackers claimed to be a group called Izz ad-Din al-Qassam Cyber Fighters and preannounced the banks it was going to attack on Pastebin, another online site. The group promised in early January 2013 to continue its attacks against U.S. banks. The Obama administration says it is the work of the Iranian government.

- Gartner 29 January 2013 ID:G00237376

Operation Ababil

- **Source:** Qassam Cyber Fighters [some question this]
- **Named targets**: U.S. Bancorp, J.P. Morgan Chase, Bank of America, PNC Financial Services and SunTrust Bank
- **DNS Top-Level Hits**: Almost 1.8 million/second
- **DDoS Hit Level**: 70 Gbps
- Used **itsoknoproblembro**

itsoknoproblembro

- **Infected hosts**: brobots
- **C&C**: Uses "push" technology
- **Infection**:
  - *itsoknoproblembro* PHP scripts
  - Awstats, WordPress, Joomla, Plesk
    - Joomla Blue Stork Theme (Template)
  - stcp.php, stpf.php, rp.php, and indx.php
- **Great write-up**: Prolexic-Threat-Advisory-Itsoknoproblembro_12.29.12.pdf

itsoknoproblembro

- “Junk packets” with all “A”s in payload
  - UDP/TCP 53
  - TCP/UDP 80
- DNS on UDP 53 payload of 8 or more “A”s
- DNS on UDP 53 packet size of 500 bytes or more
- TCP/UDP on port 80 with a payload of numerous “A”s

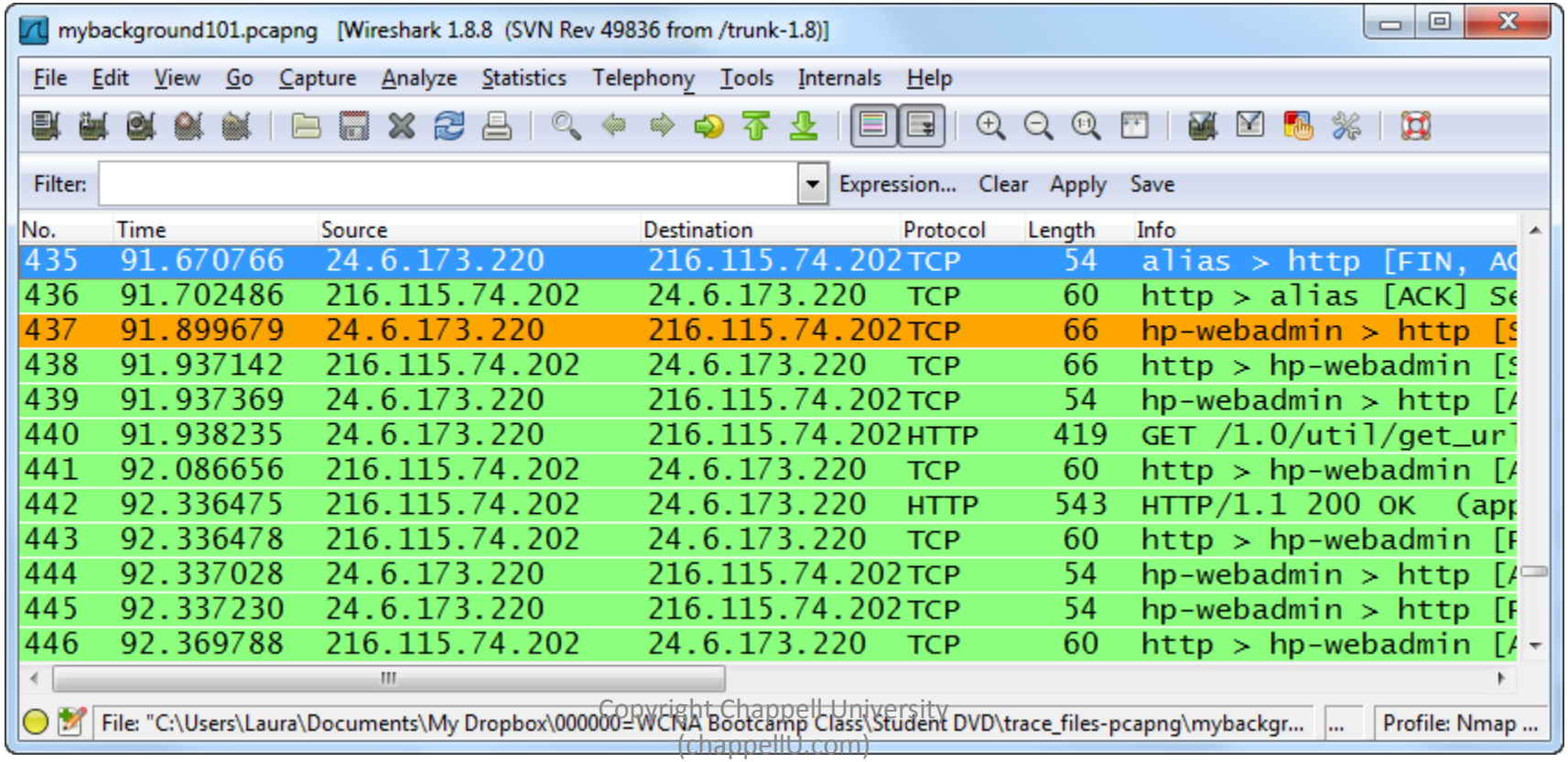
Join HTCIA

- Why are you waiting?
- Set up your LE contacts now.
- Get inside info on breaches/trends/resources.

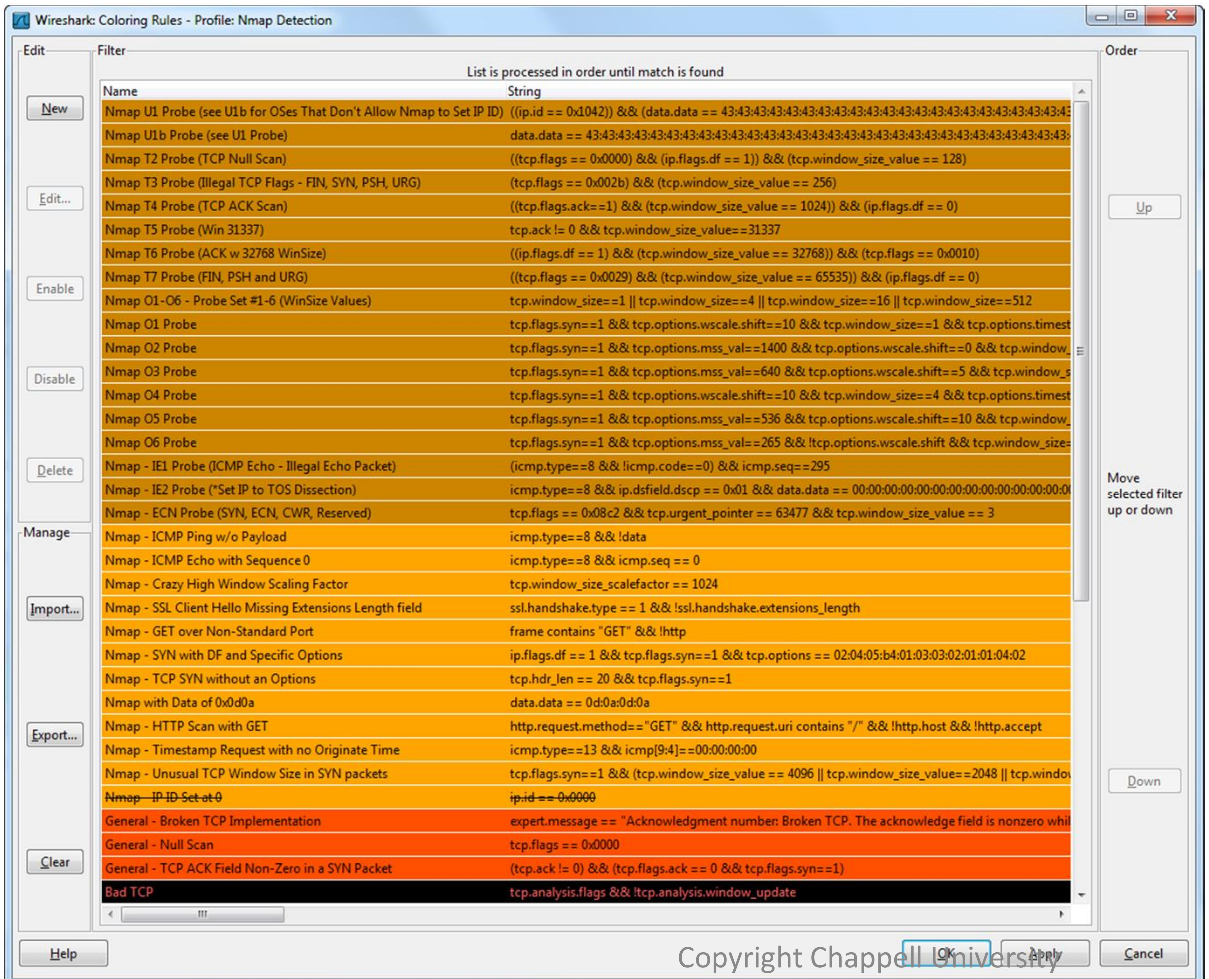
Baselines, Baselines, Baselines

Å Create them NOW!

Å Wireshark 101 Book – Chapter 0



Sample Security Profile bit.ly/nmapcolors



DDoS DNS Reflection Attack

Response Packet


```
⊞ User Datagram Protocol, Src Port: 16 (16), Dst Port: domain (53)
⊟ Domain Name System (response)
    Transaction ID: 0x03b8
  ⊞ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 13
    Additional RRs: 1
  ⊟ Queries
    ⊟ ripe.net: type ANY, class IN
        Name: ripe.net
        Type: ANY (Request for all records)
        Class: IN (0x0001)
  ⊞ Answers
  ⊟ Authoritative nameservers
    ⊞ net: type NS, class IN, ns k.gtld-servers.net
    ⊞ net: type NS, class IN, ns l.gtld-servers.net
    ⊞ net: type NS, class IN, ns m.gtld-servers.net
    ⊞ net: type NS, class IN, ns a.gtld-servers.net
    ⊞ net: type NS, class IN, ns b.gtld-servers.net
    ⊞ net: type NS, class IN, ns c.gtld-servers.net
    ⊞ net: type NS, class IN, ns d.gtld-servers.net
    ⊞ net: type NS, class IN, ns e.gtld-servers.net
    ⊞ net: type NS, class IN, ns f.gtld-servers.net
    ⊞ net: type NS, class IN, ns g.gtld-servers.net
    ⊞ net: type NS, class IN, ns h.gtld-servers.net
    ⊞ net: type NS, class IN, ns i.gtld-servers.net
    ⊞ net: type NS, class IN, ns j.gtld-servers.net
  ⊞ Additional records
```

TA13-141A: Washington, DC Radio Station Web Site Compromises

05/20/2013 05:59 PM EDT

Original release date: May 20, 2013 | Last revised: May 21, 2013

Systems Affected

- Microsoft Windows systems running Adobe Reader, Acrobat, or Oracle Java

Overview

On May 16, 2013, US-CERT was notified that both www.federalnewsradio[.]com and www.wtop[.]com had been compromised to redirect Internet Explorer users to an exploit kit. As of May 17, 2013, US-CERT analysis confirms that no malicious code remains on either site.

Description

The compromised websites were modified to contain a hidden iframe referencing a JavaScript file on a dynamic-DNS host. The file returned from this site was identified as the Fiesta Exploit Kit. The exploit kit script uses one of several known vulnerabilities to attempt to download an executable:

- CVE-2009-0927: Stack-based buffer overflow in Adobe Reader and Adobe Acrobat
- CVE-2010-0188: Unspecified vulnerability in Adobe Reader and Acrobat
- CVE-2013-0422: Multiple vulnerabilities in Oracle Java 7 before Update 11

Any systems visiting running vulnerable versions of Adobe Reader or Acrobat or Oracle Java may have been compromised.

Impact

The exploit kit, once successful, delivers and executes a known variant of the ZeroAccess Trojan. Additionally, according to open source reporting, the malware also downloads and installs a variant of FakeAV/Kazy malware.

The ZeroAccess Trojan attempts to beacon to one of two hardcoded command-and-control addresses, 194[.]165[.]17[.]3 and 209[.]68[.]32[.]176. The beaconing occurs using an HTTP GET using the Opera/10 user-agent string.

After beaconing, the malware then downloads a custom Microsoft Cabinet file and the malware uses port UDP/16464 to connect to the peer-to-peer network. This cabinet file contains several lists of IP addresses, as well as a fake flash installer.

- Target IP Addresses known
- User-agent string known
- UDP Port known

Security Profile Elements

- Unusual TCP flags
- Peer-to-peer SYNs
- DNS containing for ANY (DNS reflection)
- DNS with repeating As
- HTTP with repeating As
- UDP Port 16464
- User-Agent Opera/10
- IP Addresses 194.165.17.3, 209.68.32.176

When the Traces are Huge!

- **Extract DNS info**

  tshark –r monsterfile.pcapng -R dns
  -w dns.pcapng

- **Extract HTTP Host info**

  tshark –r monsterfile.pcapng -R http.host
  -T fields -e ip.src -e ip.dst -e http.host
  > httphosts.txt

When the Traces are Huge!

- **Extract GETs and POSTs**
  tshark -r monsterfile.pcapng
  -R "http.request.method contains "GET" or
  http.request.method contains "POST""
  -w httpGETPOST.pcapng
- **…and Get Responses**
  tshark -r monsterfile.pcapng
  -R "http.request.method contains "GET"
  or http.request.method contains "POST"
  or http.response.code"
  -w httpGETPOSTresponse.pcapng

When the Traces are Huge!

- **Extract Connections**

  tshark -r monsterfile.pcapng
  -R “tcp.flags.syn==1"
  -w tcpsyns.pcapng

- **Extract .exe**

  tshark -r monsterfile.pcapng
  -R "frame matches "**[.]**exe""
  -w exe.pcapng

When the Traces are Huge!

- **Extract packets based on Country Code**

  tshark -r monsterfile.pcapng
  -R "http.host matches """(?i)[.](ru|cn)$"""
  -w httphostrucn.pcapng

- **Extract .exe**

  tshark -r monsterfile.pcapng
  -R "frame matches
  """(?i)(join|admin|password)""" -w
  keyword1.pcapng

Wrap Up Checklist

- Join HTCIA
- Baseline your traffic
- Start building your security profile
- Batch file Tshark extractions
- Grab bit.ly/nmapcolors
- Also…
  - www.wiresharktraining.com/sharkfest2013.html (C)
  - www.wiresharktraining.com/gerald.html (V)