Corporation in the Middle

Lee Brotherston
@synackpse
MITM vs Everything Else
Detection
This is probably not the site you are looking for!

You attempted to reach 66.185.85.55, but instead you actually reached a server identifying itself as google.com. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of 66.185.85.55.

You should not proceed, especially if you have never seen this warning before for this site.

Proceed anyway  Back to safety

Help me understand
Parse Error

Unexpected Response: "<?xml version="1.0"?><catalog><item id="xv101">..."
An important message about your Rogers Internet Service

In the past 48 hours, our records show your household has reached 75% of the 120 GB monthly usage allowance provided with your Rogers Internet Extreme service.

You will receive another notification when you reach 100% of your monthly usage allowance.

I acknowledge that I have received this message

Please do not send me this message in the future

You will continue to receive notifications if you reach 75% of your monthly usage allowance in the future.

You will no longer receive a notification when you reach 75% of your monthly usage allowance.

Welcome to SecTor – Canada’s Premier IT Security Conference!

Security Training October 20.

Illuminating the Black Art of Security. Now entering its 8th year, SecTor has built a reputation of bringing together experts from around the world to share their latest research and techniques involving underground threats and corporate defences. The conference provides an unmatched opportunity for IT professionals and managers to connect with their peers and learn.

2014 Keynote Speaker
Ray Boisvert

New Era Risk Management: Using Information to Predict, Understand and Mitigate Organizational Threats
How, what, why, when?
Capture all the Packets
PCAP Tools

- tcpdump
- wireshark
- tshark
- mergecap
- tcpsplice
- tcptrace
- captcp
- ntop
- pcapdiff
- tcpflow
SYN
SYN/ACK
ACK
HTTP Request
HTTP Response (Header & Data)
More Data……
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Content-Script-Type: text/javascript
Connection: close
Cache-Control: no-store, no-cache, must-revalidate, max-age=0
Expires: -1
Pragma: no-cache

Fun with Firewalls
Content of messages

36. Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public.

–Telecommunications Act (S.C. 1993, c. 38)
But wait, there's more....
HTTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Content-Script-Type: text/HTML
Connection: close
Tests
RetentionPolicy

```
rewrite ^(.*)$ /index.php;
```
OoB Indexing

rewrite ^(.*)$ /index.php;
+ /etc/hosts
+ .htaccess
Document Format

<html>
<head>
<title>Oh Hai</title>
</head>
<!doctype html>
<html>
<head>
<title>Oh Hai</title>
</head>
</html>
Mapping the Network
Traceroute

... ish
<table>
<thead>
<tr>
<th>2</th>
<th>7.40.72.1</th>
<th>2</th>
<th>7.40.72.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>209.148.241.61</td>
<td>3</td>
<td>209.148.241.61</td>
</tr>
<tr>
<td>4</td>
<td>66.185.81.221</td>
<td>4</td>
<td>*</td>
</tr>
<tr>
<td>5</td>
<td>69.63.251.242</td>
<td>5</td>
<td>*</td>
</tr>
<tr>
<td>6</td>
<td>69.63.249.26</td>
<td>6</td>
<td>69.63.249.26</td>
</tr>
<tr>
<td>7</td>
<td>*</td>
<td>7</td>
<td>*</td>
</tr>
</tbody>
</table>
for i in `jot 65535 1`
do
tcptraceroute -f4 -m5 host $i
done >> $i.log
<table>
<thead>
<tr>
<th></th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>7.11.164.41</td>
</tr>
<tr>
<td>3</td>
<td>66.185.90.37</td>
</tr>
<tr>
<td>4</td>
<td>209.148.224.205</td>
</tr>
<tr>
<td>5</td>
<td>209.148.224.242</td>
</tr>
<tr>
<td>6</td>
<td>4.31.208.129</td>
</tr>
<tr>
<td>7</td>
<td>209.148.228.218</td>
</tr>
<tr>
<td>8</td>
<td>209.148.224.254</td>
</tr>
<tr>
<td>9</td>
<td>4.31.208.129</td>
</tr>
</tbody>
</table>
Intercept Portscanning

nmap -sS --ttl 64 host
Which Interface?
scapy

```
sendp(Ether(dst="02:1f:ba:20:4b:d2",
          src="10:2f:33:fe:b2:11")/
        IP(src="99.243.151.125",
           dst="95.85.52.23",
           ttl=(1,30),
           options=IPOption(\x07))/
       TCP(sport=3125, dport=80,
            flags="S"), iface="en1")
```
So, that network...
Client

SYN

SYN/ACK

ACK

TTL = 1

TTL = 2

TTL = 3

RST/PSH/ACK

Server
What?
Hints in Scripts


extWebServer = "http://64.71.255.194";
intWebServer = "http://172.19.11.72";

displayUrl = "http://www.perftech.com/console/original.html";
Notification Solutions

In 2001, PerfTech designed and developed both the software and hardware to create a comprehensive in-browser notification solution called Bulletin System. Continuous upgrades and new features make Bulletin System the fastest, most scalable, robust, and reliable subscriber notification solution of its kind. No other browser-based messaging solution has been proven to meet the time-critical subscriber communication needs and performance that Bulletin System delivers to its ISP customers worldwide every day.

Sample in-browser notification solutions include:

**Bandwidth Usage**

- Customized data usage alerts
- Subscriber notification preferences
- Tier or incremental upgrade activation

Avoid bill shock, keep subscribers informed, and add revenue through upgrades.

**Service Notifications**

- Planned maintenance outages
- Modem upgrade campaigns
- Educational “how-to” information

Avoid subscriber frustration when changes to the network are necessary and increase profit by reducing call center load.

**Billing Alerts and Account Status**
production and delivery.

Security and Community

- Virus alerts and outbound spam containment
- Copyright infringement notifications
- EAS weather/Amber alerts from automated feeds

Immediately alert subscribers to security threats that impact their devices and the network; save cost related to mandatory notices; offer optional local alerts.

Subscriber Retention

- Welcome or transition messaging for new subscribers
- Guides to information on the ISP’s portal
- Online surveys to obtain feedback

Keep subscribers engaged, reduce churn, and drive traffic to your portal.

Revenue Extenders

- Search-enhancement monetization, not using DNS
- Network-based parental control packages
- Third-party advertising for subsidized access

Add revenue through PerfTech packages that incorporate added functionality with flagship in-browser messaging.
Why So Bothered?
Why Metadata Matters

They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.

They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.

They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

Attribution: EFF 30C3 -Through Prism Darkly
GET / HTTP/1.1
Host: squarelemon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:25.0) Gecko/20100101 Firefox/25.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _pk_ses.4.9b83=*  
Connection: keep-alive
If-Modified-Since: Fri, 18 Oct 2013 14:45:41 GMT
Cache-Control: max-age=0
What could possibly go wrong?
Apparently Comcast will straight up inject HTML/CSS/JS into unsecure pages to advertise to you. What. The. Fuck.

South Beach, San Francisco
Comcast is pleased to introduce a new communications vehicle!

Comcast will implement a new communications vehicle that will provide direct, timely information to our valuable subscribers. These "bulletins" will appear on your screen as you browse, but they will not overlay or interfere with your browsing activity. The subject matter of the bulletins will vary covering topics such as virus alerts, maintenance notifications, service enhancements, weather alerts, community alerts, etc.

You can be assured these bulletins are from Comcast because of the "key" symbol that appears in the upper right corner. The 4-digit code is unique to your account and matches the last 4-digits that appear on your cable modem address (found on the bottom of your cable modem).

Each bulletin may contain buttons that allow you to perform a variety of tasks. Some of these buttons may include:

- Close (to close the bulletin)
I learnt Stuff!
“Never attribute to malice that which is adequately explained by stupidity Enhancing Shareholder Value.”

– Hanlon’s Brotherston’s Razor
"Type a quote here."
Perftech Upgrades Its Growing Roster of Internet Providers to Smart Bulletins; In-browser Messaging Beta Personal for 15M Subscriber Accounts

(San Antonio, TX January 15, 2014) — To kick off the new year, Perftech Inc., who supplies the leading in-browser, subscriber communications solution to Internet Service Providers (ISPs), completed upgrading its entire roster of customers to the newest customization features of its Bulletin System messaging platform, featuring Smart Bulletins™. Perftech’s roster includes half of the top 10 U.S. cable Internet providers, as well as other cable and telecom providers in the U.S., Canada, the Caribbean, and Europe. In addition to Perftech’s adding new customers in 2013, several large, existing customers ordered system expansions to accommodate growth and acquisitions, while upgrading software and hardware.

Smart Bulletins give ISPs a higher level of interaction with subscribers, make customer support easier, and improve subscriber response. They let the provider deliver a detailed, personalized message with options for follow-on actions, while respecting personal preferences previously indicated. Typically, ISPs use Smart Bulletins to give subscribers a heads up regarding some aspect of their service, whether it relates to individual data usage, specific equipment they use, or a tailored promotion. Smart Bulletins know who the subscriber is, details of their service plan, opt-out preferences, and other information derived from interactive responses and/or back-office applications. Automated bulletins are personalized dynamically, thanks to interaction with the product’s extensive, internal database. A Smart Bulletin also knows when it has displayed on the screen, all interactions that have resulted, and if it should display a reminder or a sequential message, if at all. “When subscribers receive generic alerts that may or may not pertain to them, and that keep popping up over and over, they become annoyed,” stated Jane Christ, Perftech Sales VP. “Subscribers are left with a negative perception of the ISP’s service. With Smart Bulletins, this doesn’t happen. The customized message is always relevant, respects subscriber preferences, and has been received by ISP customers and subscribers alike.”

About Perftech
Perftech enables ISPs to forge a responsive relationship with their subscribers through proactive communications. The company’s patented Bulletin System allows ISPs to deliver interactive, time-critical messages directly to targeted subscribers’ browsers on any device, in wired, wireless, or mobile environments. Privately held, Perftech is headquartered in San Antonio.
Internet provider subscriber communications system

Redirecting device environment

Distribution Hub

Cisco uBR

Ethernet

Redirecting device

I/F downstream to customer (up to 4)

Upstream from customer (up to 24)

Uo-converter

Modulated R/F to customer

Combiners

Other CATV channels

Coax

Fiber

Laser Transceivers

Fiber

Neighborhood Distribution

Fiber

Fiber

Neighborhood Node

Laser Transceivers

Coax

Home

Cable Modem

PC

Redirecting Device

Sample Software Block Diagram

HTTP Engine

Mgmt Engine

Address Manager

TCP

UDP

GRE

IP Protocol

Ethernet Driver
Internet advertising method and system using Web page US 8005717 B2

1. Start
2. Search for advertisement location
3. Identify space information
4. Does advertising content exist? (Decision)
   - Yes: Edit web page
   - No: Display web page
5. End
<table>
<thead>
<tr>
<th></th>
<th>IP Address</th>
<th></th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>31.55.164.187</td>
<td>6</td>
<td>31.55.164.187</td>
</tr>
<tr>
<td>7</td>
<td>31.55.164.107</td>
<td>7</td>
<td>31.55.164.107</td>
</tr>
<tr>
<td>8</td>
<td>109.159.248.69</td>
<td>8</td>
<td>109.159.248.104</td>
</tr>
<tr>
<td>9</td>
<td>109.159.248.10</td>
<td>9</td>
<td>109.159.248.142</td>
</tr>
<tr>
<td>10</td>
<td>62.172.103.187</td>
<td>10</td>
<td>194.71.107.15</td>
</tr>
</tbody>
</table>

Great Firewall of Cameron
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>98.0.3.14</td>
<td>4</td>
<td>98.0.3.14</td>
</tr>
<tr>
<td>5</td>
<td>98.0.3.3</td>
<td>5</td>
<td>98.0.3.3</td>
</tr>
<tr>
<td>8</td>
<td>64.86.79.97</td>
<td>8</td>
<td>64.86.79.97</td>
</tr>
<tr>
<td>9</td>
<td>64.86.79.2</td>
<td>9</td>
<td>64.86.79.2</td>
</tr>
</tbody>
</table>

RoadRunner via Marriott
Thank you!

Lee Brotherston
@synackpse