

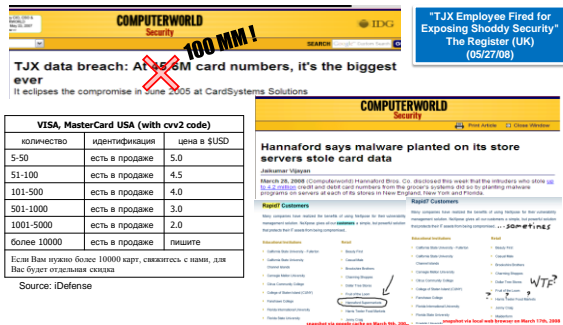
How to Stop Serious Threats from Evading Detection

Chris Lawrence
Senior Systems Engineer
chris.lawrence@netwitness.com

What We Will Be Discussing Today

- Advanced Persistent Threats and the Gaps in the Threat Management Lifecycle
- How to Improve Network Security Monitoring
 - Three Case Studies
- Final Thoughts and Conclusions
- Q&A

Companies Are Being Slammed



COMPUTERWORLD Security

TJX data breach: At least 6M card numbers, it's the biggest ever
It eclipses the compromise in June 2005 at CardSystems Solutions

TJX Employee Fined for Exposing Shoddy Security*
The Register (UK) (05/27/08)

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

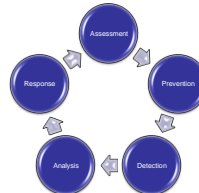
Если Вам нужно более 10000 карт, свяжитесь с нами, для Вас будет отдельная оценка

Source: IDDefense

Hannaford says malware planted on its store servers stole card data
Jalisco/Maple

March 26, 2008 (Computerworld) Hannaford Bros. Co. disclosed this week that the intruders who stole 400,000 credit and debit card numbers from the grocer's servers did so by creating malware programs on servers at each of its stores in five English, New York and Florida.

Problems in the Threat Management Lifecycle



- Advanced Persistent Threats continue to evade point solutions
- Insider threats also cannot be underestimated – particularly in multinational organizations
- Results: Breaches in data privacy and enormous data loss issues

- Each stage in the threat management lifecycle offers an opportunity to stop an attack from becoming a disaster
- At each stage it is critical that your InfoSec staff is equipped with the right visibility and tools needed to understand the scope and context of the problem



Network Visibility Gaps Are Critical



- Unfortunately, “defense-in-depth” has been built upon a series of point solutions offering incomplete capabilities:
 - Signature based detection
 - Zone segmentation
 - Access controls
 - Packet filtering
 - Content monitoring
- This approach leaves many potential gaps in your network visibility, exploited by your top adversaries today:
 - Application attacks
 - Zero-day threats
 - Data loss events
 - Designer malware

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

Threat Lifecycle Scorecard

- Threat assessment misses key issues
- Exfiltration prevention fails
- Malware detection only catches pieces or fails entirely
- Analysis requires the correlation of hard to obtain data
- Incident resolution and remediation requires more input and more resources
- **Gaps, Errors, and Inefficiency**

Bottom line: There are many gaps in network visibility, and these are the very gaps being exploited by your top adversaries today.

Organizations Must Close the Gaps



- For the remainder of this presentation we will discuss how to:
 - Introduce new network visibility and bridge gaps in typical layered security environments
 - Increase efficiency in the security cycle
 - Enhance and leverage the capabilities of the current layered security model

Case Studies

What is Needed?

- A new kind of network monitoring for incident responders / investigators, threat analysts, auditors and others
- Reconstruction of network events to provide live threat intelligence into advanced persistent threats
- 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?

Technology Requirements for Next Generation Network Monitoring

Infrastructure

- Live, promiscuous full packet capture
- Session reassembly
- Port agnostic processing and data modeling
- Real-time metadata indexing across the OSI stack
- Focus on application layer

Data Modeling



Analytics



Automated analysis



Interactive research

SDK

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
- When thinking about "drive-bys", stay alert for:
 - cross-site scripting
 - zero-size IFRAMES
 - malicious downloads (i.e. "exe" and obfuscated JavaScript)
 - non-standard traffic appearing over various ports
 - abnormal traffic to foreign locations
 - clear text authentication

An Initial Problem Area...

Copyright 2008 NetWitness Corporation 13

- It is important to fuse conceptual problem areas and target high risk adversary trends
- In this case, the existence of a notorious DYNDNS is particularly concerning...

Other Problem Areas

Copyright 2008 NetWitness Corporation 14

- 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 real evidence...

Moving Quickly from Alerts to Results

Copyright 2008 NetWitness Corporation 15

Through fusion between alert queries, the metadata model, and a 3rd party reputation service, we can now see a "drillable" alert with full data behind the content and context of the Dynamic DNS activity

Drilling into the Details

Copyright 2008 NetWitness Corporation 16

- Drilling into the dyndns alert reveals the source IP of all dynamic DNS requests
- Most likely an "owned" internal machine
- Need to understand pathology for damage control and assessment

Isolating the Source of the Problem and Knowing the Malware Pathology

Inspection shows .exe file enumeration downloads, non-standard port activity at the top (8090), and top destination China... all abnormal. Take a look at .exe downloads.

Copyright 2008 NetWitness Corporation 17

Discovering the Index Case (Patient 0)

- Viewing Session Content – Chinese HTTP error page?
- Obscured JavaScript?
- How did this get on my network?

Copyright 2008 NetWitness Corporation 18

The Original Drive By...

- Perform a content search for "cb.js"
- Someone visited Chinese Academy of Sciences webpage that was compromised... hence launched the JavaScript infecting the visiting host.
- What is this malware DOING and what has it done, now that it's on my network

Copyright 2008 NetWitness Corporation 19

Discovering the Malware's Signature

- Let's go back to our starting point...
- Top Destination was China and TCP 8090 have the highest number of sessions (vs. HTTP, HTTPS)?
- Probably will be a good idea to look more closely at these sessions...

Copyright 2008 NetWitness Corporation 20

Uncovering Covert Channels and Beacon Trojans

Remember port 8090?
 • Non-descript sessions destined to China – do not decode to known protocol – non-standard traffic
 • Regular 366 Byte beaoning... looks to be empty, but not appropriate

Copyright 2008 NetWitness Corporation 21

Google Earth mapping of RED traffic represents beacon to Chinese IP

Copyright 2008 NetWitness Corporation 22

Summary of Example #1

- Thousands of compromised, sites exist using this same attack trend
- Live Threat Intelligence highlights key areas of concern --- live DYNDNS, PROXY, HAXTOR, BOTS, DARKNET..etc.
- From Informer, you can navigate instantly to application and content detail showing the Dynamic DNS activity in detail
- Focusing on source IP address shows file download enumeration (1.exe,2.exe) , non-standard port activity(8090), and top destination China... all abnormal.
- Drilling in cb.js as potential culprit, turns out top be an obfuscated JavaScript that among other things initiated the exe downloads, and installed the Beacon Trojan.
- Further search for cb.js shows that user visiting a compromised site caused the infection.
- Additionally the non-standard activity showed beaoning malware periodically sending 366 Byte sessions to server located in China.
- In this case system was quarantined prior to any known data loss

Copyright 2008 NetWitness Corporation 23

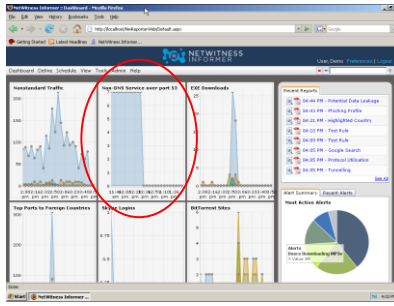
Example #2: Beacon Trojan

- 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? Doesn't my IDS platform do this?
- NetWitness
 - Holds the **ONLY US Patent for session-based port-agnostic service identification in a network security system**

Copyright 2008 NetWitness Corporation 24

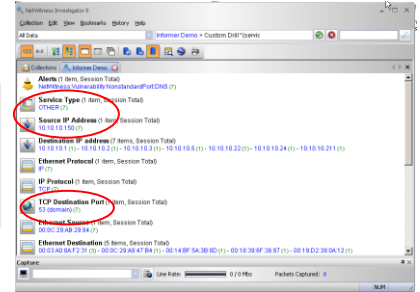
Using Active Threat Intelligence

- 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.

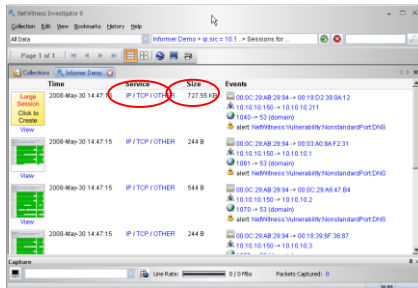


Port Agnostic Session Analysis

7 total sessions over port 53 with unknown service. ... must take a closer look at the sessions



Non-Standard Traffic

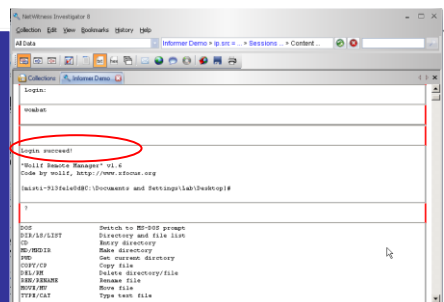


Very small sessions followed by big session... Too big to be plain DNS, and zone transfer is not TCP.. Take a look at payload

Command Shell Traffic

Payload shows command and control software being controlled over port 53. What is it doing? Look at 10.10.10.150 originating IP

(note: data altered to protect privacy)



Inappropriate Binaries on Our Network!

FTP of various binaries with malicious names (sniff, scan, kill). Outbound PUT shows concern.

Copyright 2008 NetWitness Corporation 29

Exfiltrated Data?

Looks like file exfiltrate.rar FTP'd out. Most likely, compromised data

(note: IP addresses changed for confidentiality reasons)

Copyright 2008 NetWitness Corporation 30

Summary

- Non-standard traffic is a good sign of something bad that many technologies do not identify well, if at all.
- Live intelligence chart illustrates a spike in traffic over port 53 that is NOT DNS
- Inspection of suspect sessions show large session over port tcp/53 containing malicious command and control data
- Further inspection shows outbound FTP upload from host of "exfiltrate.rar", most likely compressed data being leaked
- In this case host was quarantined and cleaned.

Copyright 2008 NetWitness Corporation 31

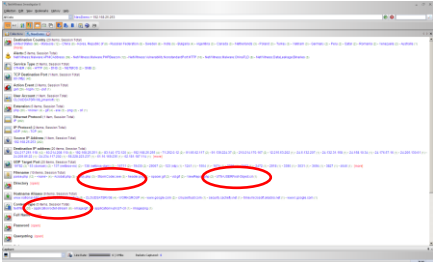
Example #3: BBB SpearPhishing

- 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?

Copyright 2008 NetWitness Corporation 32

NETWITNESS
TOTAL NETWORK KNOWLEDGE

Malicious Downloads



Downloads of 3 unidentified binary streams, SSL certificate list (.crl) and stormcodec.exe? What is going on?

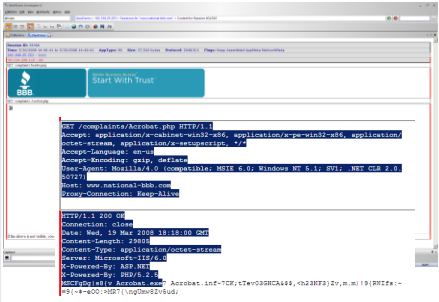
Take a closer look at www.national-bbb.com activity

Copyright 2008 NetWitness Corporation 37

NETWITNESS
TOTAL NETWORK KNOWLEDGE

Many Sites Are Not What They Seem

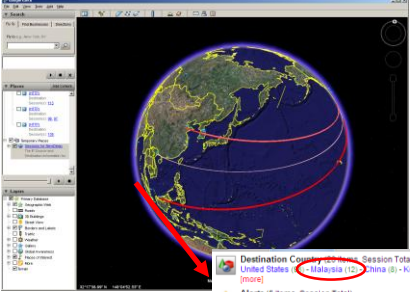
- Looks similar to actual BBB site, but has an embedded link to download an "Adobe" product.
- Appears that user clicked thru from content download – probably the unidentified binary streams....
- Infected with something? Yes.
- Now what? ... Google Earth It!



Copyright 2008 NetWitness Corporation 38

NETWITNESS
TOTAL NETWORK KNOWLEDGE

Google Earth GeoIP Fun



High Volume Traffic to Malaysia? Need more detail...

Destination Country (23 Items, Session Total)
United States (8) - Malaysia (11) - China (8) - Korea, Republic of (8) - Russian Federation (more)

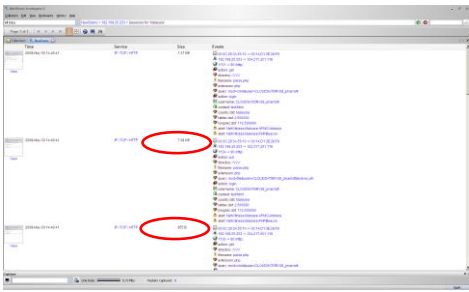
Alerts (5 Items, Session Total)
NetWitness Malware APNICAddress (3) - NetWitness Malware PHPBeacon (1) - NetWitness

Service Type (5 Items, Session Total)
OTHER (16) - HTTP (3) - DNS (2) - NETBIOS (2) - SMB (2)

Copyright 2008 NetWitness Corporation 39

NETWITNESS
TOTAL NETWORK KNOWLEDGE

Another Kind of "Invisible" Beacon Trojan Discovered!

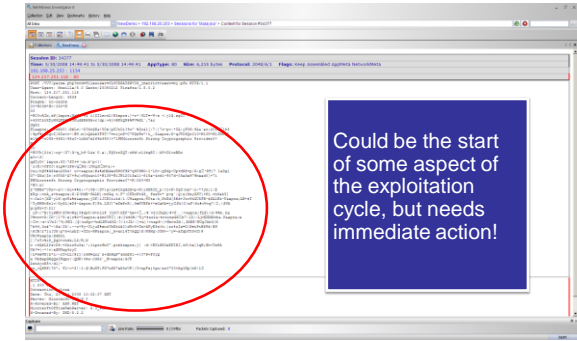


Periodic PHP Beacon HTTP POST to Malaysian Server – usually empty at 955 Bytes – until...

Copyright 2008 NetWitness Corporation 40



Encrypted Blob Post to Malaysia – Data Exfiltration?



Summary

- Salesforce.com gets owned
- Insider gets BBB Phishing email with malicious link, and clicks it and accepts malware masquerading as “Adobe.exe” from server located in China
- Malware is loaded
 - Downloads SSL Certificate List
 - Initiates PHP Beacon to Malaysian IP
 - Exfiltrated data (in this case it was keystrokes) are either obfuscated or encrypted (SSL) when shipped back to the beacon address in Malaysia.
- In this case ~7KB data was transferred via beacon before compromised system was taken offline.



Conclusions

- Advanced persistent threats evade your current processes and security technologies
- Network forensics techniques, next generation security monitoring and active threat intelligence processes are required to improve visibility and accelerate the incident response cycle
- Security professionals can dramatically increase the effectiveness of their security programs by using the approaches described today



Please download Investigator Freeware
<http://download.netwitness.com>

For a copy of this presentation, please email me:

chris.lawrence@netwitness.com