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**

LISA ‘09 | November 4, 2009

Raytheon
Customer Success Is Our Mission
APT in the News

The Washington Times

Chinese hackers prompt Navy college site closure

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

La France touchée par les pirates informatiques chinois

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.

A Broad Problem Affecting Many Nations and Industries

LISA ‘09 November 4, 2009
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
“[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.” **

Are we paying attention

Google Trends: “Your terms - advanced persistent threat - do not have enough search volume to show graphs.”
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.
A “case study”

Bad Guy Searches the USENIX Site.

11/2/2009
Searches Site

11/2/2009
Downloads Agenda

11/3/2009
Adds Trojan to Agenda

11/3/2009
Sends to Selected Attendees

11/4/2009
Bob Opens “Agenda”

11/4/2009
Bob PC starts “Beaconing”

11/5/2009
Bob PC Used to Harvest

LISA ’09
November 4, 2009
A “case study”

Bad Guy downloads the LISA Agenda.

11/2/2009
Searches Site

11/3/2009
Adds Trojan to Agenda

11/2/2009
Downloads Agenda

11/3/2009
Sends to Selected Attendees

11/4/2009
Bob Opens "Agenda"

11/4/2009
Bob PC starts "Beaconing"

11/5/2009
Bob PC Used to Harvest
A more specific example

Bad Guy adds a Trojan to the Agenda PDF.
A more specific example

Bad Guy sends the Trojanized PDF to selected attendees.

11/2/2009
Searches Site

11/3/2009
Adds Trojan to Agenda

11/2/2009
Downloads Agenda

11/3/2009
Sends to Selected Attendees

11/3/2009
Bob Opens "Agenda"

11/4/2009
Bob PC starts "Beaconing"

11/4/2009
Bob PC Used to Harvest

LISA '09
November 4, 2009
A more specific example

Bob opens the Agenda PDF.

Note: This image is not really Bob ;-)
A more specific example

Bob’s PC starts “beaconing” that it is available.
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.
What happens when they are opened

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
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


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.
AV Detection of Malicious PDF Documents has been very poor.

- McAfee-GW-Edition
- AntiVir
- Sophos
- BitDefender
- GData
- Avast
- Symantec
- a-squared
- McAfee
- Ikarus
- McAfee+Artemis
- Kaspersky
- NOD32
- F-Secure
- Microsoft
- TrendMicro
- Fortinet

AV Detection of Malicious PDFs is extremely low across the board.
Common PDF Exploits

<table>
<thead>
<tr>
<th>CVE</th>
<th>Name</th>
<th>First Used</th>
<th>Discovered</th>
<th>Patched</th>
<th>Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-5659</td>
<td>collectEmailInfo() (JS)</td>
<td>1/1/2008</td>
<td>2/6/2008</td>
<td>2/7/2008</td>
<td>37</td>
</tr>
</tbody>
</table>

Days Between First Use and Patch

Occasional Lag to Discovery – Consistent Lag to Remediation
More Than 2 Months from First Known Offensive Use to Patch Availability
What did Bad Guy do to the PDF?

- Object 3 is first to launch, in this case.
- It has an OpenAction to go to Object 2.
- Object 2 fills memory with code that leads to Object 7.
- Object 7 contains the executable that gives you a bad day.
- The red colored areas are indicators you can use to find similar documents.

Automated Tools Are Available To Help Our Bad Guy Insert the Executable
Cool Tool to Help Find Stuff

Yara

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

```yara
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
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

Circles are scaled in proportion to the number of compromised computers found in each country.

THE NEW YORK TIMES

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

APT Tactics, Techniques & Procedures

A-Team
More senior? Malware writers?

B-Team

www.hackedsite1.com
Agent Download & Install
Beaconing & Latching
Command & Control; Agent transfer

www.hackedsite2.com
RDP & Other
Command & Control; Agent transfer
Data transfer

Foothold Host
Stage 0
Infection

Intermediary Host
Stage 1
Generate Intermediaries

Transfer Host
Stage 2
Setup Relay Agents

Data Host
Stage 3
Data Exfiltration

LISA ‘09
November 4, 2009

Customer Success Is Our Mission
### VPN Client Shimming

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

**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

Move

Counter-Move

LISA ‘09  November 4, 2009
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.
Knowledge is Power – Social Engineering Relies on Ignorance

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
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

LISA ‘09  November 4, 2009
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: 17%
- Used non http/s port: 83%

**See Mandiant, Ero Carrera and Peter Silberman, “State Of malware: Explosion of the axis of Evil”**
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)
F-Secure: We’d recommend you’d at least check your company’s gateway logs.

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

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

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Version</th>
<th>Last Update</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>VBA32</td>
<td>3.12.10.10</td>
<td>2009.08.25</td>
<td>suspected of Exploit.Signature</td>
</tr>
</tbody>
</table>

Additional information

File size: 1575940 bytes
MD5: 1d65f1be33c9d72636568c3df24ec780
SHA1: ffb7497f4597137f174339a91dfbf888f9ad278db
SHA256: 2ce516c14b8d9e8ea414d65d565f6bdde69a2a5c00ba711cddaffa5f768f4f2a
TrID: File type identification
      Microsoft PowerPoint document (79.7%)
      Generic OLE2 / Multistream Compound File (20.2%)
      ssdeep: 24576:td069c3cn/Q4/luadE40BSQifE5sa0/EJLUKFQ8htzQ91FqiQIYdY+4gBt6zCh:BoIWJQM9HASFqEeY8Q83n1FU1gb62h
      PEiD: -
      RDS: NSRL Reference Data Set

- See if someone else has already found this problem.

Sharing Malware Identification

LISA ‘09  November 4, 2009
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

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.
- 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
QUESTIONS?

Can I catch an earlier flight?

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

Could you repeat everything after “good afternoon”?

Why did he take so long?
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.