Advanced Persistent Threat (APT):
Sharpening Your Defensive Arsenals

Inno Eroraha, CISSP-ISSAP, CISM, CISA, CHFI, PI
Founder & Chief Strategist
NetSecurity Corporation

Techo Security 2010 Conference (Keynote)

Abstract Condensed

Today's cyber adversaries are highly skilled and sophisticated hackers who are either part of a state-sponsored or organized crime. These "elite" hackers are so advanced that current perimeter security measures do not detect, let alone prevent their attacks. These criminals are paid and spend ample time conducting reconnaissance about their targets, and then customizing their attack (in form of a malicious software) towards the victim. The firewall or perimeter defensive measures do not prevent these attacks and the intrusion detection systems or anti-virus software doesn't detect these intrusions since there are no known signatures. These cyber attackers continue to leverage users' susceptibility to social engineering attacks to infiltrate critical networks. Once inside the network, they fly below the radar and often go undetected while pilfering vital data. Advanced Persistent Threats (APTs) pose a new set of challenges to cyber security personnel and forensics analysts charged with securing critical networks (of government, corporations, or political groups) that may become targets. This presentation addresses APT, why these attacks are successfully bypassing existing security measures, ways to detect APT attacks through real-time network- and memory-forensics techniques, current challenges posed by APT, and steps to build carefully executed defensive measures to thwart these emerging attacks..

Agenda

- What is APT?
- Who is behind APT activities?
- Who are APTs targeting?
- Why should we care?
- Common attacks vectors
- Sharpening your defensive arsenals

The Evolution of Commercial Malware

- Years ago, virus writers used to be script kiddies
  - More interested in attention and bragging rights
  - Motive was to corrupt data and inconvenience users
- These malware were easily detected and stopped
- The cyber attack landscape has changed…

Change in Cyber Landscape

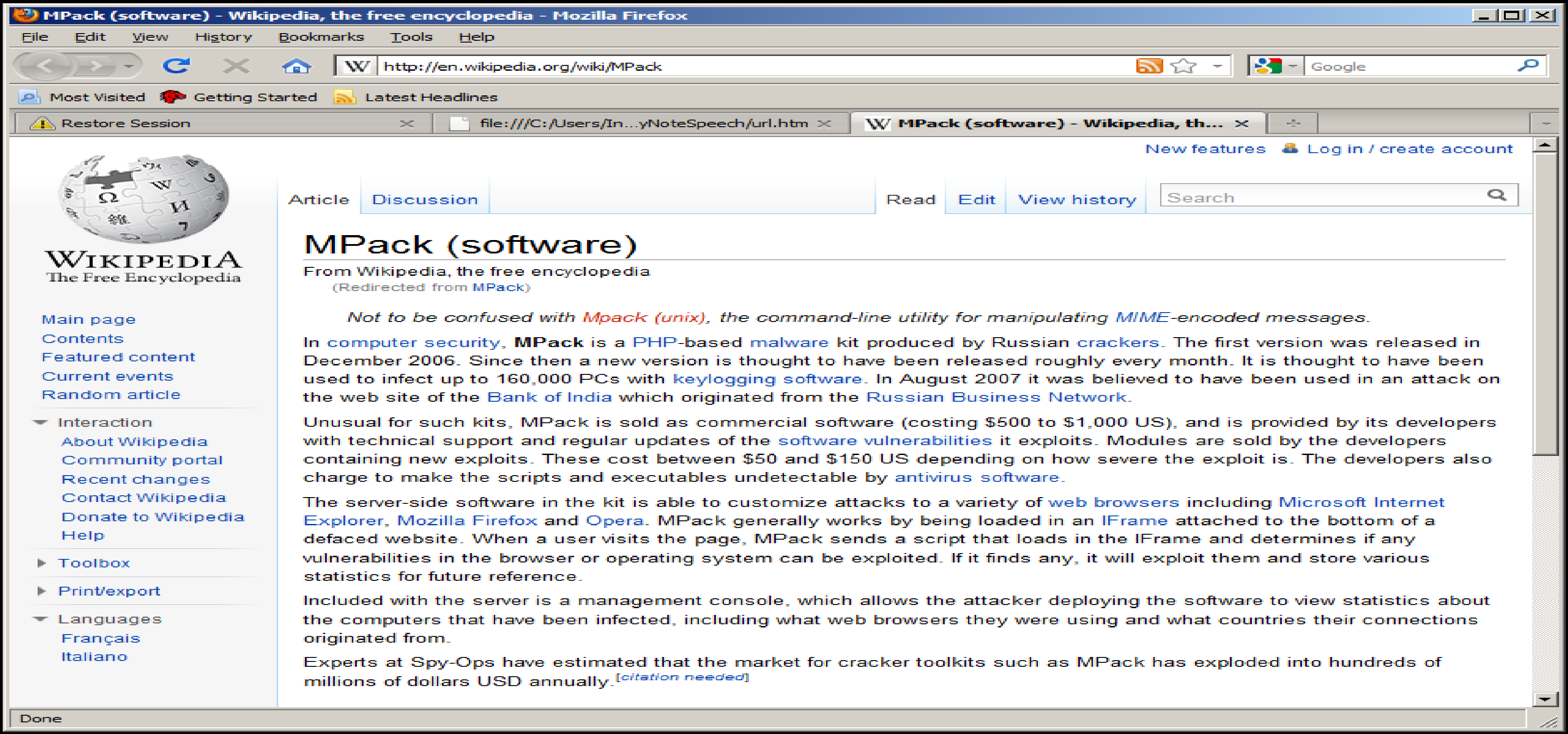
- Organized criminal elements realize the Internet presents a good vehicle to make money
- Recruit skilled programmers to create malicious software
- Not intended to cause disruption but to enable the theft of money and/or data
- Leads to the creation of underground economy
- Attackers keep their zero day exploits secret
- Exploits are used against targets or sold to other attackers
- Hackers no longer disclose their exploits like before

The Underground Economy

- Allows cyber criminals to buy data and software to steal data
- Malware creation tools exist:
  - Examples: MPack is used to launch sophisticated attacks by people with the right programming skills against unsuspecting users
- There is an increase in the number of attacks and compromised systems
- According to AVG Technology, *"During 2008 alone, more than 1.5 million new strains of malware were identified – which translates to tens of thousands of samples arriving in security companies' research labs every day."*

- Cybercrime is a multi-billion dollar industry

Malware Kit – MPack



MPack (software)

From Wikipedia, the free encyclopedia

(Redirected from MPack)

Not to be confused with Mpack (unix), the command-line utility for manipulating MIME-encoded messages.

In computer security, **MPack** is a PHP-based malware kit produced by Russian crackers. The first version was released in December 2006. Since then a new version is thought to have been released roughly every month. It is thought to have been used to infect up to 160,000 PCs with keylogging software. In August 2007 it was believed to have been used in an attack on the web site of the Bank of India which originated from the Russian Business Network.

Unusual for such kits, MPack is sold as commercial software (costing $500 to $1,000 US), and is provided by its developers with technical support and regular updates of the software vulnerabilities it exploits. Modules are sold by the developers containing new exploits. These cost between $50 and $150 US depending on how severe the exploit is. The developers also charge to make the scripts and executables undetectable by antivirus software.

The server-side software in the kit is able to customize attacks to a variety of web browsers including Microsoft Internet Explorer, Mozilla Firefox and Opera. MPack generally works by being loaded in an IFrame attached to the bottom of a defaced website. When a user visits the page, MPack sends a script that loads in the IFrame and determines if any vulnerabilities in the browser or operating system can be exploited. If it finds any, it will exploit them and store various statistics for future reference.

Included with the server is a management console, which allows the attacker deploying the software to view statistics about the computers that have been infected, including what web browsers they were using and what countries their connections originated from.

Experts at Spy-Ops have estimated that the market for cracker toolkits such as MPack has exploded into hundreds of millions of dollars USD annually.[*citation needed*]

What are Cyber Criminals After

- Your Identity
- Confidential Data
- Money
- Defense Intelligence
- Intellectual property (competitive and strategic advantage)
- Infrastructure

Cyber Attack Vectors

- Socially-Engineered Highly-target Email (Spear Phishing)
  - Malicious Attachments (PDF, Word, Excel, CHM, etc.)
  - Malicious Web Links
- Websites ("trusted" and "untrusted") with malicious payloads
    - "Trusted" websites are compromised and used to deliver malicious payloads
      - Example: **U.S. Treasury Web sites hacked, serving malware**
        - **(http://www.computerworld.com/s/article/9176278/US_Treasury_Web_sites_hacked_serving_malware)**
    - Social networks
- Vulnerabilities in web browsers and browser ad-ons (Flash, QuickTime, etc.)
- Vulnerable applications

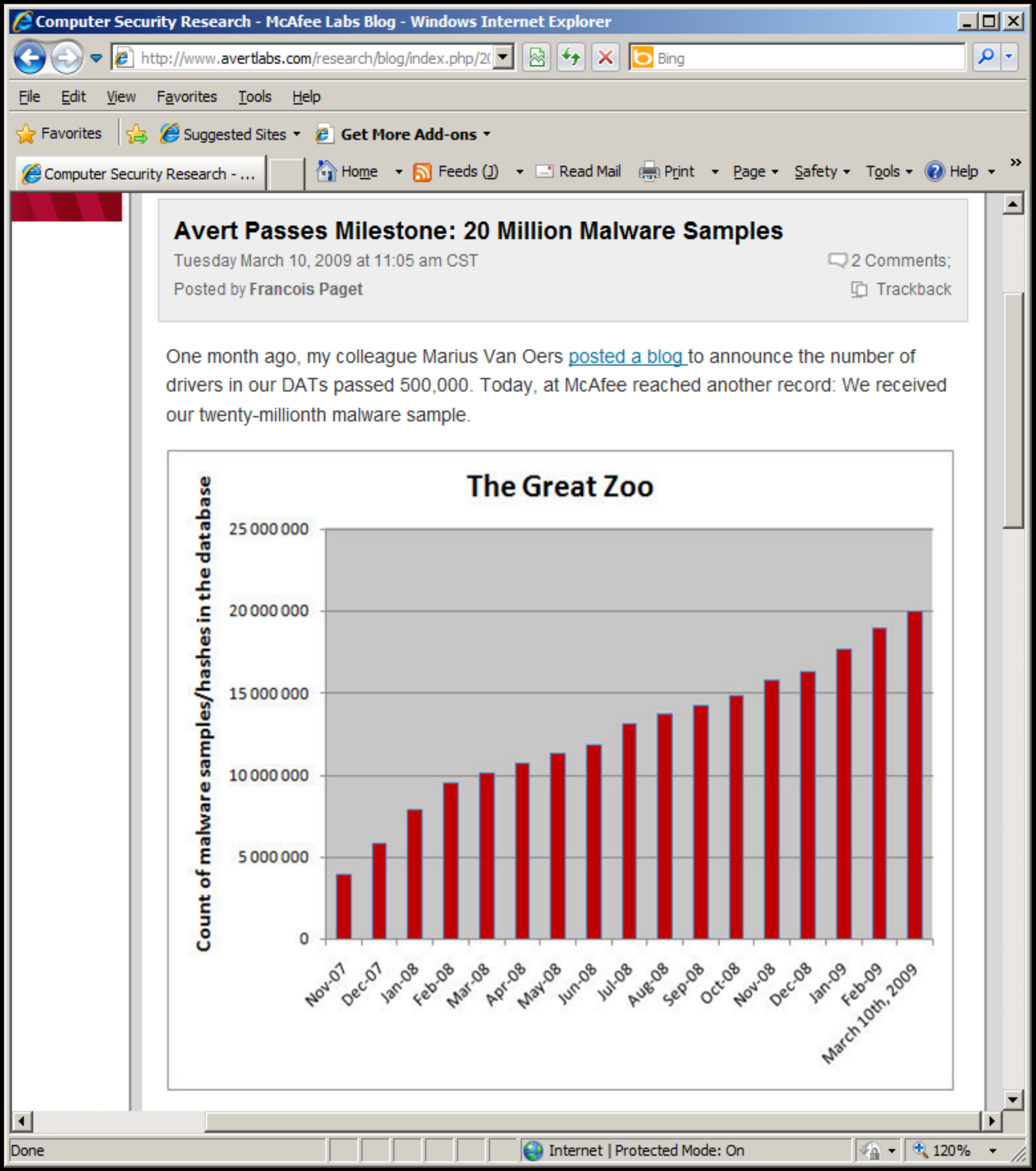
Avoiding Detection

- Cyber criminals want to remain undetected and want to "hang around" the penetrated network for a long time
- Malware Operators avoid their tools being captured by security companies by serving different content based upon the visitor – security vendors can be provided with good code while unpatched browsers can be serviced with bad codes
- Malware are Polymorphic which allows them to change each time

Malware Growth

According to McAfee:

- In about 22 years, from 1986 to March 2008, 10 million malware samples piled up in their collection.
- In just the last 12 months, however, from March 2008 to March 2009, this figure doubled.
- This pace represents 27,000 samples in a day, or 1,100 each hour.



Avert Passes Milestone: 20 Million Malware Samples

Tuesday March 10, 2009 at 11:05 am CST

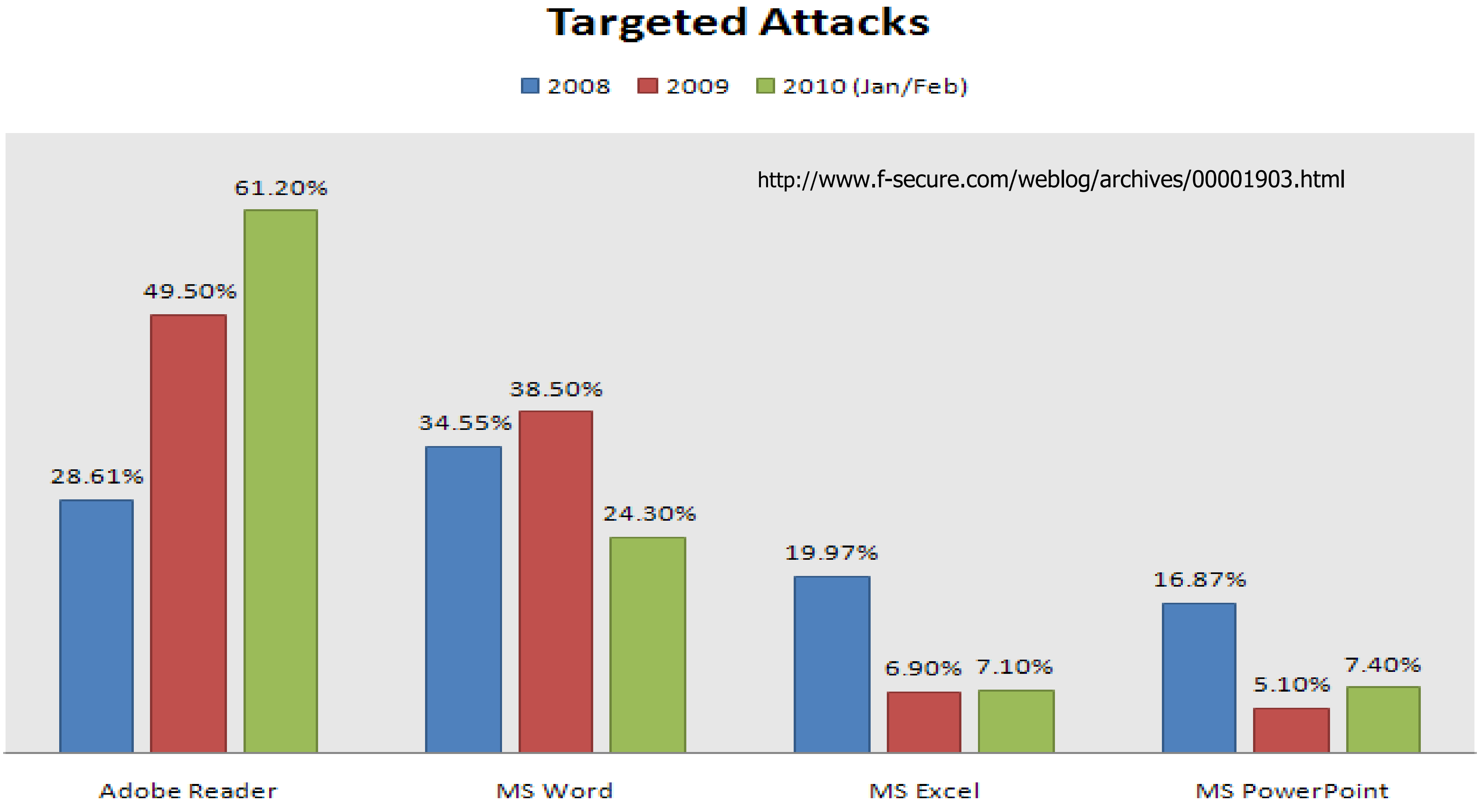
Posted by Francois Paget

2 Comments;

Trackback

One month ago, my colleague Marius Van Oers posted a blog to announce the number of drivers in our DATs passed 500,000. Today, at McAfee reached another record: We received our twenty-millionth malware sample.

Common Attack Vectors



http://www.f-secure.com/weblog/archives/00001903.html

What is Advanced Persistent Threat (APT)?

- **Advanced** – Criminal operators behind the threat utilize the full spectrum of computer intrusion technologies and techniques. While individual components of the attack may not be classed as particularly "advanced" (e.g., malware components generated from commonly available DIY construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

- **Persistent** – Criminal operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a "low-and-slow" approach is usually more successful.

- **Threat** –There is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The criminal operators have a specific objective and are skilled, motivated, organized and well funded.

Source: http://www.damballa.com/knowledge/advanced-persistent-threats.php

Advanced Persistent Threats

- Are posed by hackers sponsored by organized crime, state-sponsored and recruit skilled software programmers to develop malware
- Targets Government entities, defense industrial base, financial institutions, corporations, political groups, and other "high-valued" organizations
- Are low key and stealth attacks, developed to bypass security measures (firewalls, IDS/IPS, anti-virus, etc.)
- Employs web and email as attack vectors to target their victims – through social networks, malicious websites, or **Spear-Phishing** (carefully crafted and spoofed emails)

Advanced Persistent Threats (Contd.)

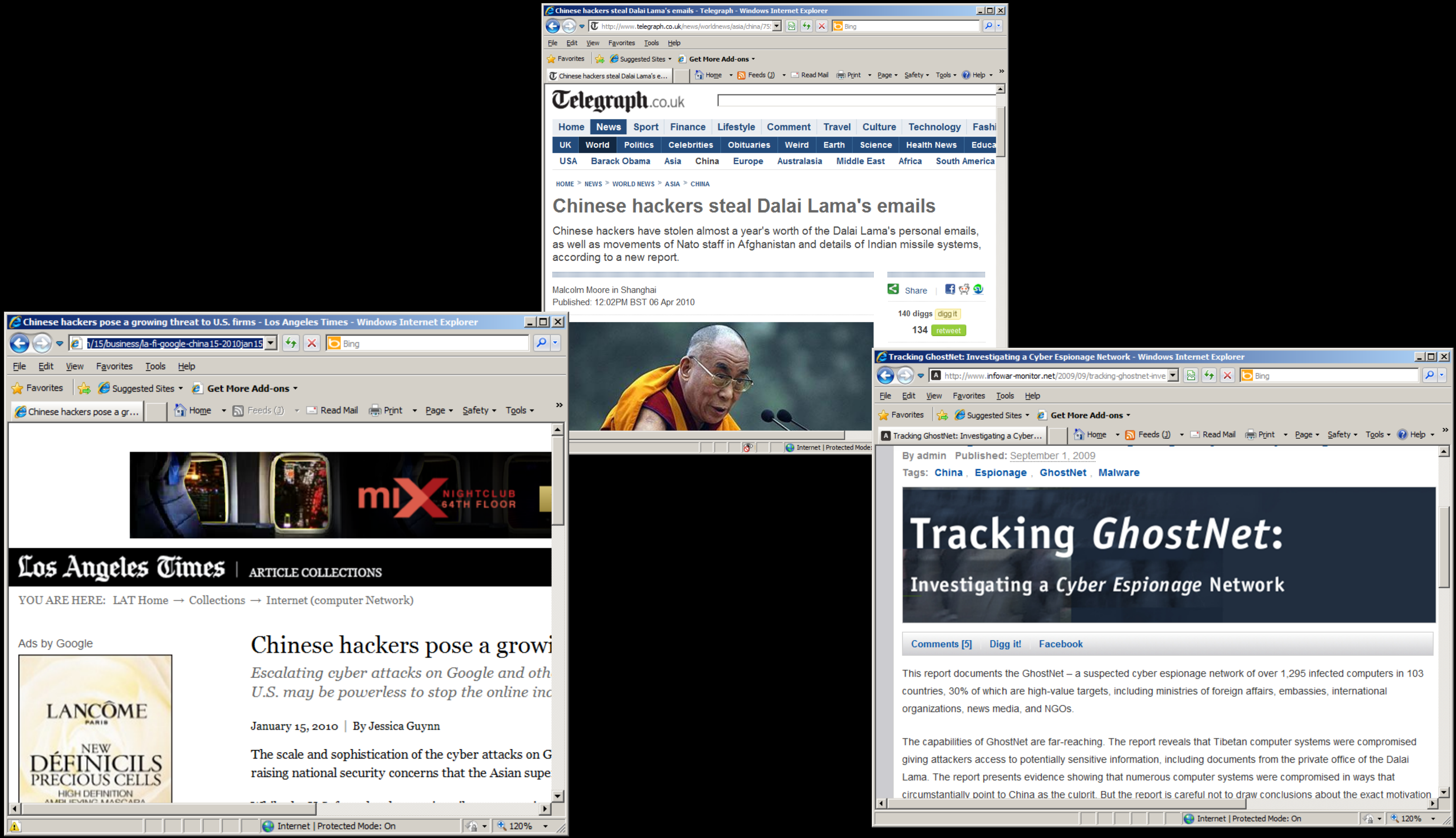
- Takes great skills in proactive incident response, security, forensics, and malware analysis to identify – It is a very complex challenge
- Detection relies upon knowledge of host- and network-based compromise indicators
- Rushing to quick fixes, removing “affected” system, could result in reoccurrence

- Widely Publicized Examples:
  - Google (Operation Aurora)
  - GhostNet

APT Motivation

- Money
- Defense Intelligence
- Intellectual property (competitive and strategic advantage)
- Infrastructure
- Identify Theft

APT in the News


File Edit View Favorites Tools Help
Favorites
Suggested Sites
Get More Add-ons
Home
Feeds (J)
Read Mail
Print
Page
Safety
Tools
Help
Bing
Internet | Protected Mode: On
120%
Home News Sport Finance Lifestyle Comment Travel Culture Technology Fashi
UK World Politics Celebrities Obituaries Weird Earth Science Health News Educa
USA Barack Obama Asia China Europe Australasia Middle East Africa South America
Share
140 diggs digg it
134 retweet
mix NIGHTCLUB 64TH FLOOR
LANCÔME PARIS NEW DÉFINICILS PRECIOUS CELLS HIGH DEFINITION

Chinese hackers steal Dalai Lama's emails - Telegraph - Windows Internet Explorer

http://www.telegraph.co.uk/news/worldnews/asia/china/75

Telegraph.co.uk

HOME > NEWS > WORLD NEWS > ASIA > CHINA

Chinese hackers steal Dalai Lama's emails

Chinese hackers have stolen almost a year's worth of the Dalai Lama's personal emails, as well as movements of Nato staff in Afghanistan and details of Indian missile systems, according to a new report.

Malcolm Moore in Shanghai
Published: 12:02PM BST 06 Apr 2010

Chinese hackers pose a growing threat to U.S. firms - Los Angeles Times - Windows Internet Explorer

/15/business/la-fi-google-china15-2010jan15

Los Angeles Times | ARTICLE COLLECTIONS

YOU ARE HERE: LAT Home → Collections → Internet (computer Network)

Ads by Google

Chinese hackers pose a growi

Escalating cyber attacks on Google and oth
U.S. may be powerless to stop the online inc

January 15, 2010 | By Jessica Guynn

The scale and sophistication of the cyber attacks on G
raising national security concerns that the Asian supe

Tracking GhostNet: Investigating a Cyber Espionage Network - Windows Internet Explorer

http://www.infowar-monitor.net/2009/09/tracking-ghostnet-inve

By admin Published: September 1, 2009

Tags: China , Espionage , GhostNet , Malware

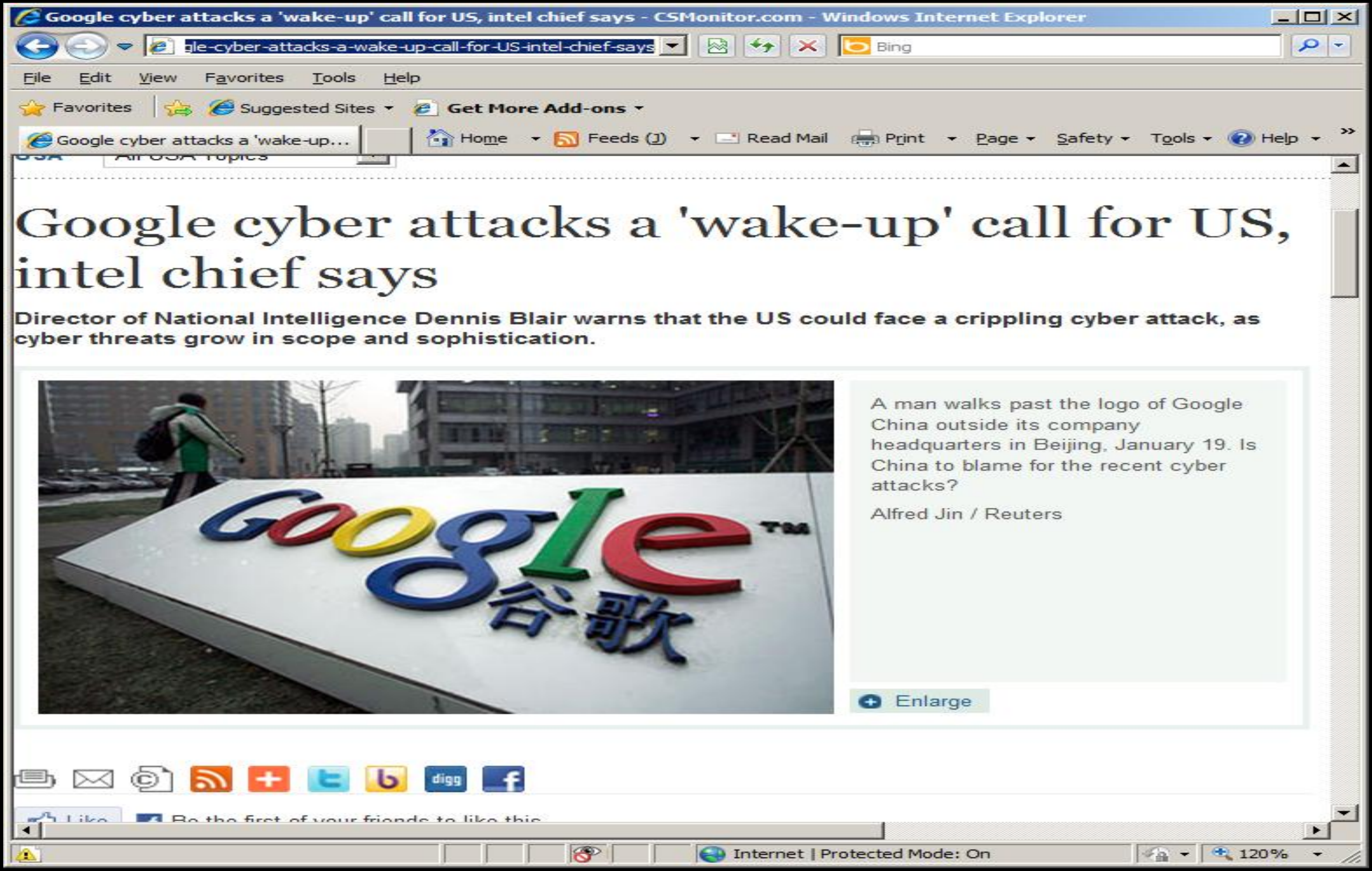
Tracking *GhostNet:*
Investigating a *Cyber Espionage* Network

Comments [5] Digg it! Facebook

This report documents the GhostNet – a suspected cyber espionage network of over 1,295 infected computers in 103 countries, 30% of which are high-value targets, including ministries of foreign affairs, embassies, international organizations, news media, and NGOs.

The capabilities of GhostNet are far-reaching. The report reveals that Tibetan computer systems were compromised giving attackers access to potentially sensitive information, including documents from the private office of the Dalai Lama. The report presents evidence showing that numerous computer systems were compromised in ways that circumstantially point to China as the culprit. But the report is careful not to draw conclusions about the exact motivation

Example APT – Operation Aurora


Google cyber attacks a 'wake-up' call for US, intel chief says - CSMonitor.com - Windows Internet Explorer
gle-cyber-attacks-a-wake-up-call-for-US-intel-chief-says
Bing
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Get More Add-ons
Google cyber attacks a 'wake-up...
Home
Feeds (J)
Read Mail
Print
Page
Safety
Tools
Help
digg
Internet | Protected Mode: On
120%

Google cyber attacks a 'wake-up' call for US, intel chief says

Director of National Intelligence Dennis Blair warns that the US could face a crippling cyber attack, as cyber threats grow in scope and sophistication.

A man walks past the logo of Google China outside its company headquarters in Beijing, January 19. Is China to blame for the recent cyber attacks?

Alfred Jin / Reuters

Enlarge

Example APT – GhostNet

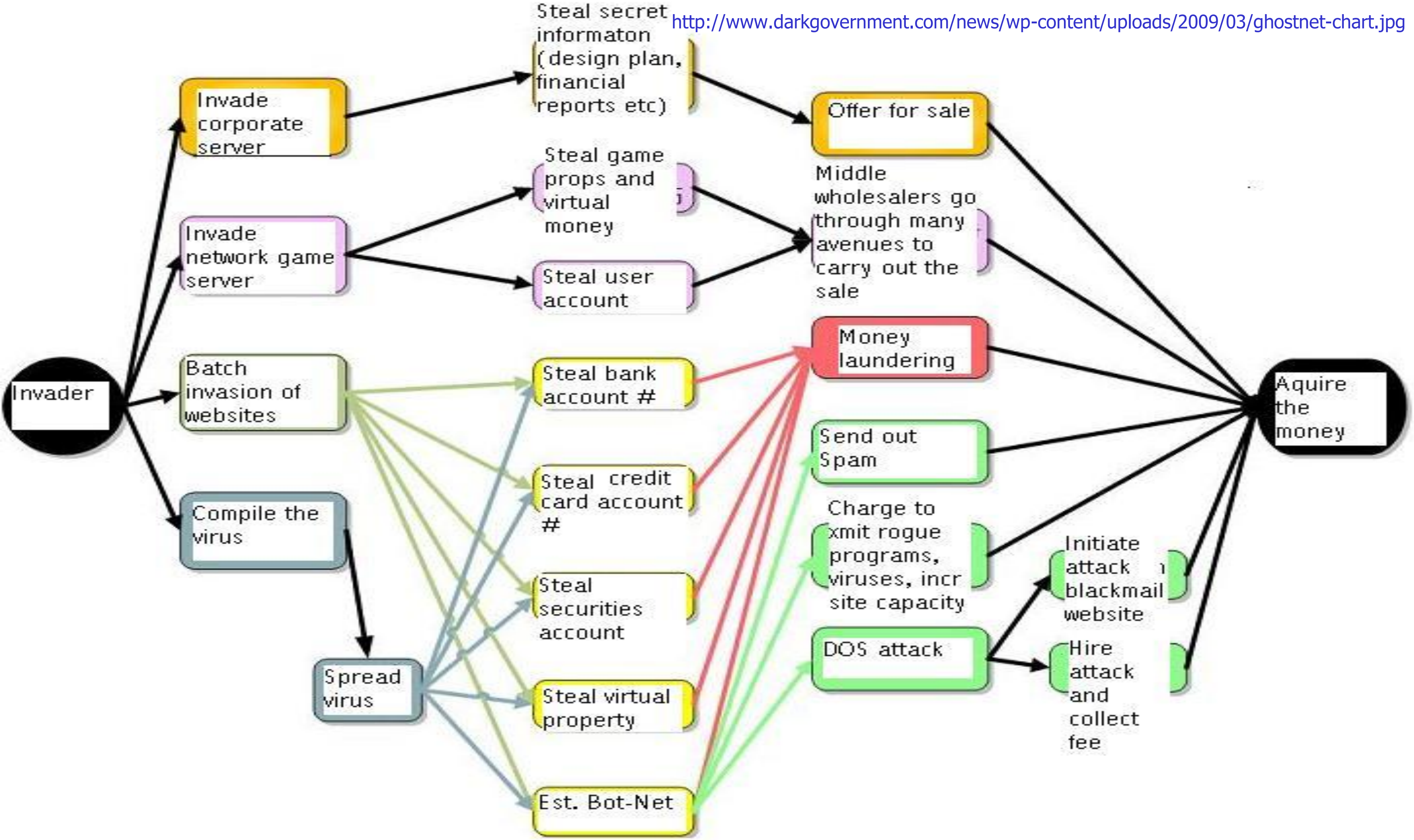
According to a 10-month investigation of alleged Chinese cyber spying against Tibetan institutions, the findings from Information Warfare Monitor show:

- Documented evidence of a cyber espionage network— of GhostNet—infecting at least 1,295 computers in 103 countries, of which close to 30% can be considered as high-value diplomatic, political, economic, and military targets.
- Documented evidence of GhostNet penetration of computer systems containing sensitive and secret information at the private offices of the Dalai Lama and other Tibetan targets.
- Documentation and reverse engineering of the of modus operandi of the GhostNet system—including vectors, targeting, delivery mechanisms, data retrieval and control systems—reveals a covert, difficult-to-detect and elaborate cyber-espionage system capable of taking full control of affected systems.

Source: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

Example APT – GhostNet

http://www.darkgovernment.com/news/wp-content/uploads/2009/03/ghostnet-chart.jpg


Invader
Invade corporate server
Invade network game server
Batch invasion of websites
Compile the virus
Spread virus
Steal secret informaton (design plan, financial reports etc)
Steal game props and virtual money
Steal user account
Steal bank account #
Steal credit card account #
Steal securities account
Steal virtual property
Est. Bot-Net
Offer for sale
Middle wholesalers go through many avenues to carry out the sale
Money laundering
Send out Spam
Charge to xmit rogue programs, viruses, incr site capacity
DOS attack
Initiate attack blackmail website
Hire attack and collect fee
Aquire the money

Source : http://www.darkgovernment.com/news/wp-content/uploads/2009/03/ghostnet-chart.jpg

Other Attack Examples

- Adobe
- **Heartland (SQL Injection?)
- **Oil Companies
  - Marathon Oil
  - ExxonMobil
  - ConocoPhillips

**The FBI told them "proprietary" data had been siphoned from their computers

(http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?articleID=222600139)

Is APT New?

- Are these attacks new?
- Three viewpoints
  - The press/media
  - Marketers wants you to think it's new so they can jam their products down your throats – new buzzword is created
  - Security professionals would debate the "newness" of APTs, especially looking at preventive and defensive measures

Anatomy of APT Malware

- Conduct Reconnaissance on Target
- Compromise System
- Create Backdoors (uses Command and Control [CC] Protocol)
- Install Keyloggers and Multiple CC Channels on Compromised Host
  - Multiple CC Channels allows for PERSITENCE access!!!
- Exfiltrate Data
- Perform Lateral Network Movement
- Maintain Persistence (Survive Reboots)

Detecting APTs

- Network-based indicators
- Host-based indicators
- Infrastructure-level indicators
- Users indicators

Why Current Approaches are Inadequate

- False sense of security
- Vendor influences – slanting the solution towards their offerings

Why are Attacks Occurring?

- People’s weakness
- Computing Habits (Email, Web, Trust, Naivety)
- Internal politics
- Not fully leveraging existing security investment
- Reactive instead of proactive security process
- Thinking current measures would solve the problem
  - Anti-virus
  - IDS/IPS
  - Firewalls

Perimeter defenses are not detecting APTs

Lessons from APT

- Understand the scope and extent of damage before mitigation approaches
- Communicate with involved team properly
- Protect critical assets proactively
- Implement carefully planned remediation strategies to prevent attacks

Current Approaches

- Anti-virus solution
- IDS/IPS
- Expensive Firewalls
- Regulatory Compliance (FISMA, PCI, HIPAA, etc) focus
- No true Defense-in-Depth

Why are these approaches not working?

Sharpening Your Defense Arsenals

- Investigate thoroughly without rushing to mitigation
- Stay educated and get well trained
- Implement Measures
- Identify all points of connections to the network
- Create separate networks with various level of trusts

Defending against APTs

- Awareness Training
  - Based upon various roles – users, SAs, DBAs, Developers, etc.
- Network Seclusion
- Stringent Ingress (Inbound) and Egress (Outbound) Access Control
- Information Sharing

Implement Defensive Measures

- Firewalls with restrictive inbound and outbound rules
- Implement centralized logging
- Log everything centrally and correlate actively
- Implement host-based IDS and network-based IDS and file-integrity checking
- Application Whitelisting

Secure Network Design

- Implement two-factor authentication, even for outbound connections
- Secure network design
  - Network isolation/seclusion
  - Treat every system as untrusted
  - Change Passwords frequently (depending on the criticality of the network)
  - Allow only required services and people
  - Perimeter Defensive Measure
  - Very restrictive firewall rulesets
  - Service and data isolation

Host-Based Security Measures

- Host IDS/IPS
- File integrity checking
- Host baselining
- Proactive host monitoring
- Host assessment
- Secure host configuration
- Application Whitelisting

Application Security

- Use up-to-date applications
- Patch old applications
- Perform code review or application security review
- Sign all emails, if practical!
  - Automatically treat each unsigned emails as suspicious
  - While not 100%, email signing can make phishing attacks less likely to succeed

Application Whitelisting

- Signature-based defenses are capturing a fraction of attacks
- Application Whitelisting may be a solution against advanced threats
- Combine with Host-based IDS/IPS

Network Isolation/Seclusion

- Isolate networks based upon mission
- Enforce strong access control even inside the network

Log Monitoring and Correlation

- Monitor logs vigilantly, looking for compromise indicators
- Correlate logs from other threat feeds
- Correlate logs from various logging devices

Non-Technical Solutions

- Educate people of social engineering
  - Conduct training targeting users based upon their roles
- Educate defenders on threats and how to defend
  - Take courses in forensics, security
  - Non-certification courses are encouraged as they provide problem solving skills

Essential Skillsets for APT Defense

- Incident Response/Handling
- Malware Analysis
- Remote Forensics
- Forensics
- Security Administration
- Log Analysis
- Intrusion Detection
- Reverse Engineering
- Programming
- System/Network Administration

Identify Compromise Indicators

- Windows
- Unix
- Mac OS
- Network Devices
- Mainframes(?)

Establish Policies and Procedures

- Define policies and procedures
- Implement and enforce policies
- Proactively verify for compliance

Identify Information Assets

- Identify organizational assets
- Categorize assets based upon criticality
- Update the assets database proactively

Incident Response Capability

- Develop forensics and incident response plans
- Proactively train incident responders, security analysts, and forensics examiners on new threats

Summary

- Don’t be fooled by vendors proposing to sell you a cure-all solution
- Remember basic protection mechanisms – product alone won’t protect against cyber threats
- Establish an adaptive response strategy

References

- http://www.darkreading.com/database_security/security/attacks/showArticle.jhtml?pgno=2&articleID=222600139
- http://bit.ly/73tuYA
- http://www.dataconnectors.com/events/2009/01Chicago/pres/NetWitness.pdf
- http://event.on24.com/event/19/57/42/rt/1/documents/slidepdf/final_gcnuglannetwitness_webinar_aptfinal.pdf
- Advanced Persistent Threat: What APT Means to Your Enterprise, by Greg Hoglund
- The Advanced Persistent Threat, http://www.usenix.org/event/lisa09/tech/slides/daly.pdf
- PDF Most Common File Type in Targeted Attacks, http://www.f-secure.com/weblog/archives/00001903.html
- http://www.f-secure.com/weblog/archives/Shadows_In_The_Cloud.pdf
- http://www.damballa.com/knowledge/advanced-persistent-threats.php
- Top Ten Cyber Security Menaces for 2008, http://www.sans.org/2008menaces/
- 70 Of Top 100 Web Sites Spread Malware , http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=212901775

RFC/Questions/Feedback

- If you have critical comments/feedback that can enhance this presentation, please send it for a FREE **NetSecurity Forensic Labs T-Shirt** – Limited supply of 10 shirts (as shown) so act fast!

- Direct Comments, Questions, and Feedback to **Inno@NetSecurity.com**