Emerging Threats to Infrastructure

Jorge Orchilles
Security Analyst

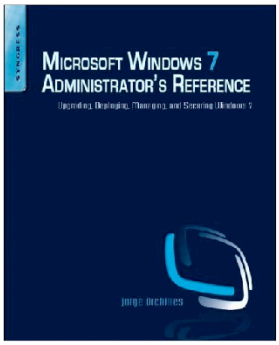
North Central Florida IIA

Titled Emerging Threats to Infrastructure and NOT Advanced Persistent Threat. APT will be highlighted but by definition only refer to attacks coming from China.

Prepared for North Central Florida Institute of Internal Auditors.

About Your Speaker

- Information * for over 8 years
- Security Analyst – Fortune 20
- Consultant by night – Orchilles Consulting
- Master of Science and BBA in Management Information Systems – Florida International University
- Author – Microsoft Windows 7 Administrator's Reference (Syngress)
- Certifications – GCIH, CEH, CICP, CCDA, CSSDS, MCTS, MCP, Security+
- Organizations:
  - VP of South Florida ISSA
  - Hack Miami
  - OWASP
  - InfraGard
  - Miami Electronic Crimes Task Force

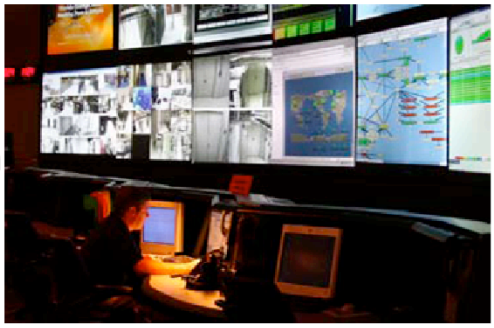


Jorge Orchilles, author of Microsoft Windows 7 Administrator's Reference, holds a Master's of Science in Management Information Systems from Florida International University, is currently a Security Analyst at a Fortune 20 financial institution, and serves as Vice President of the South Florida ISSA Chapter.

Terremark Worldwide (NASDAQ:TMRK) is a leading global provider of IT infrastructure services delivered on the industry's most robust and advanced technology platform. Leveraging data centers in the United States, Europe and Latin America with access to massive and diverse network connectivity, Terremark delivers government and enterprise customers a comprehensive suite of managed solutions including managed hosting, colocation, disaster recovery, security, data storage and cloud computing services. Terremark's Enterprise Cloud computing architecture delivers the agility, scale and economic benefits of cloud computing to mission-critical enterprise and Web 2.0 applications and its DigitalOps® service platform combines end-to-end systems management workflow with a comprehensive customer portal. More information about Terremark Worldwide can be found at http://www.terremark.com.

Security Operations Center (SOC)

- 24/7 monitoring
- IDS/IPS
- Log Aggregation
- Network Analysis
- Deep Packet Inspection
- Managed Firewall
- Network Forensics
- DB Monitoring
- Scanning
- File integrity monitoring
- Compliance reporting



Terremark's Security Operations Center (SOC) is part of Terremark Operations and located in the Network Operations Center in the NAP of the Americas. Our team of skilled security analysts monitor our customers and internal information security 24/7.

The slide points out most of the security solutions we provide.

We offer all of these quality services to customers and are considered a Managed Security Service Provider (MSSP).

Industry Reports

- SANS Top Cyber Security Threat
- Verizon Business 2010 Data Breach Study
- Symantec State of Security Report
- US Cert
- SANS Internet Storm Center – http://isc.sans.org/

Information Security reports are released at different intervals throughout the year depending on the sponsor. Generally these reports are by vendors and show their results. The favored reports are those by vendor neutral entities such as the SANS, US Cert, and Verizon business which deal with actual data breaches:

Verizon: http://newscenter.verizon.com/press-releases/verizon/2009/verizon-business-2009-data.html

SANS Top Security Risk: http://www.sans.org/top-cyber-security-risks/

SANS Internet Storm Center: http://isc.sans.org/

Symantec State of Security Report - http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=sesreport2010

US Cert - http://www.us-cert.gov/

News and Media

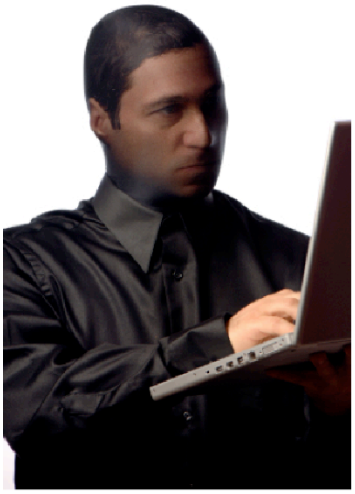
- Resources:
  - Data Loss Database - http://datalossdb.org/
  - PrivacyRights.org
- Some that were reported:
  - Heartland Payment Systems (130+ million – 1/2009)
  - Oklahoma Dept of Human Service (1 million – 4/2009)
  - University of California (160,000 – 5/2009)
  - Network Solutions (573,000 – 7/2009)
  - U.S. Military Veterans Administration (76 million – 10/2009)
  - BlueCross BlueShield of Tennessee (187,000 – 10/2009)
  - Google (1/2010)
    - Many others?
  - Stuxnet (2010)

DataLossDB is a research project aimed at documenting known and reported data loss incidents and data breaches world-wide.

PrivacyRights.org - A nonprofit consumer education and advocacy project whose purpose is to advocate for consumers' **privacy rights in public policy proceedings.**

Agenda

- Know your enemy
  - Who is your enemy?
  - What are they after?
  - How are they attacking?
- Know yourself
  - What are you defending?
  - Who are you defending?
  - How do we defend?



It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle. – Sun Tzu

Sun Tzu:

It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.

Art of War for Security Managers: http://www.elsevier.com/wps/find/bookdescription.cws_home/712202/description#description

To properly analyze emerging threats we need to answer a few questions:

1. Who is attacking? Know your enemy
2. Know what your enemy is after.
3. Know how your enemy is attacking.

Know your enemy

This slide is reserved for a video courtesy of Radware demonstrating hackers in the past and hackers today. In 1988, kids played computer games and figured out how to cheat. It was a lot of fun. Then as they got older they got good grades in school, not because they earned them but because they hacked the school computers. While they were at it they would deface web sites too for bragging rights. Today, today is different. Today hackers want money and they are going after your financial information.

Who is attacking?

- Organized Crime
- Nation-States
- Well Meaning Insider
- Malicious Insider
- Script Kiddies

Miami hacker accused of record credit card theft

A Miami native who is one of the nation's most well-known hackers is charged with stealing 130 million credit card numbers -- a case prosecutors are calling the largest ever.

Police said Albert Gonzalez, 28, launched his career as a hacker cruising Dixie Highway with a laptop to break into the security systems of box stores. (AND OUT

Related Content

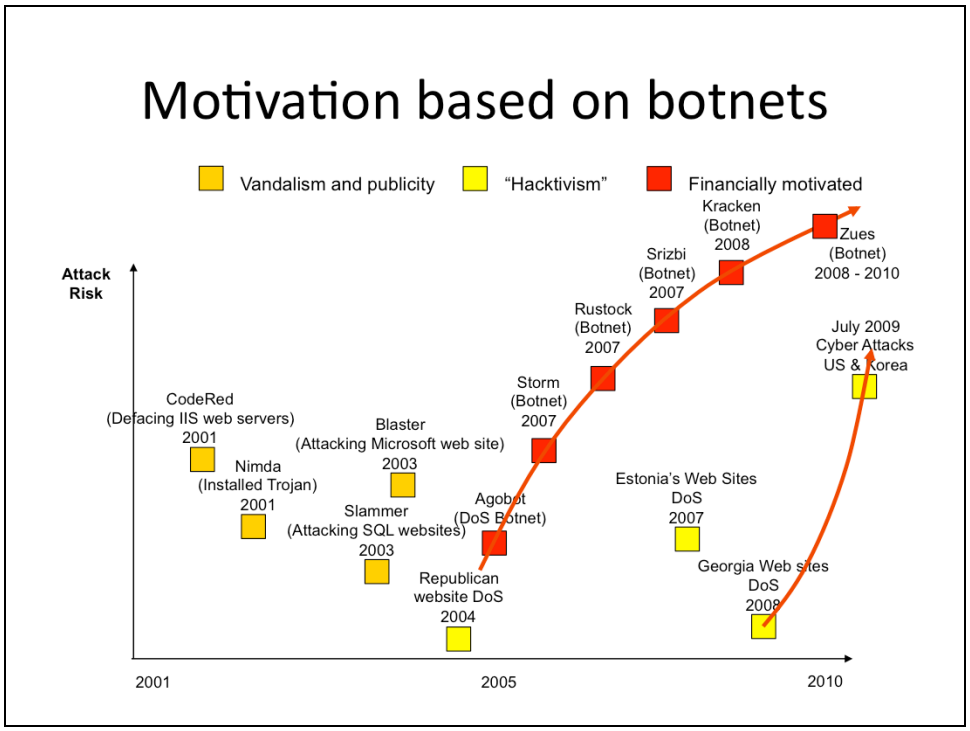
- Complete coverage of Technology

Albert Gonzalez, the Miami cyberthief and former government informant who broke records last year in the largest credit card fraud case in U.S. history, shattered his own mark this week, prosecutors say. The 28-year-old hacker who launched his career cruising Dixie Highway with a laptop to break into the security systems of box stores was indicted Monday in New Jersey in an elaborate scheme to steal more than 130 million credit cards -- reselling them on the worldwide black market.

Known in dark corners of cyberspace as "soupnazi," the Miami native was charged along with two unnamed defendants with targeting customers at convenience store giant 7-Eleven and supermarket chain Hannaford Brothers. The defendants also are accused of infiltrating the computers of a national credit card processing company.

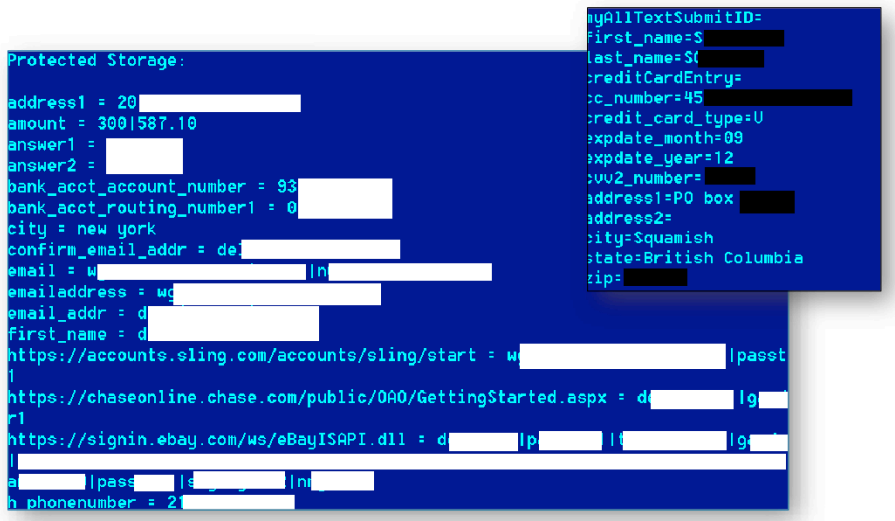
Prosecutors said Gonzalez, who is already in jail awaiting trial in the earlier case, used a sophisticated hacking technique known as "SQL injection" to break into computer systems and steal credit and debit card records, sending the data to California, Illinois, Latvia, the Netherlands and Ukraine.

1. Organized Crime - 90% of records lost in 2008 involved organized crime targeting corporate information according to Symantec
2. Nation-States are now behind some of the most advanced malware we have seen!
3. Well Meaning Insiders – includes laptops and USB flash drives lost with data
4. Malicious Insiders –
5. Script Kiddies and automated attacks is the majority of the attacks your IDS and Anti-virus will see and stop

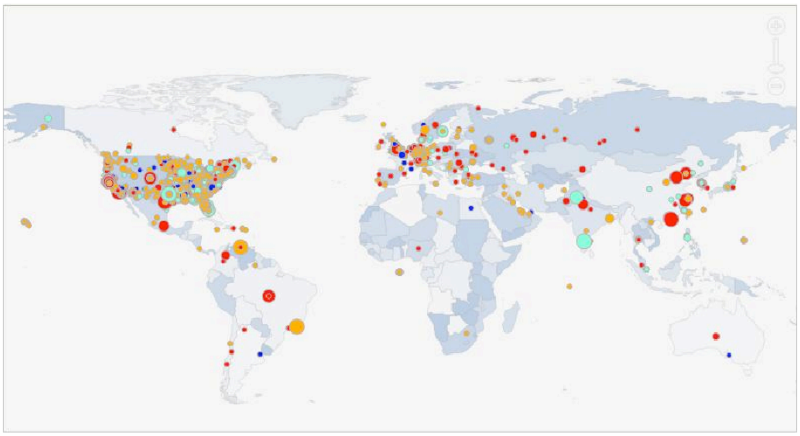


Botnet attacks show a lot about hacker motivation. Back in the early 2000's it was more for vandalism, publicity, and hacktivism. In the late 2000's a trend began to financially motivated attacks. "If my competition is down for 1 day, I get all their business"

Output of Zeus Logs



From where are they attacking?

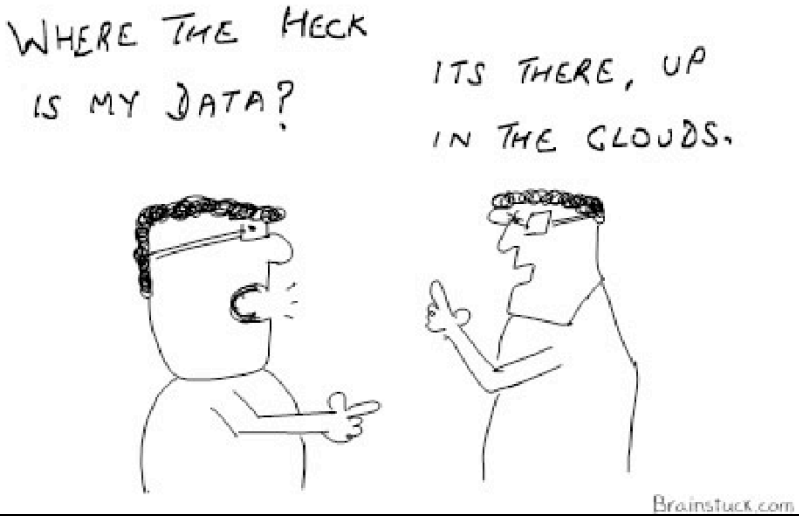


Where the attacks are coming from? Everywhere! Attackers generally do not attack from home, they proxy and bounce from compromised host to compromised host to hide identity.

This is a snapshot of the events in the past 24 hours on Tuesday March 16, 2010

One of the largest problems I see is that not all countries have laws against hacking. The ones that do may not have jurisdiction into countries that do not.

What are they after? What are we defending?



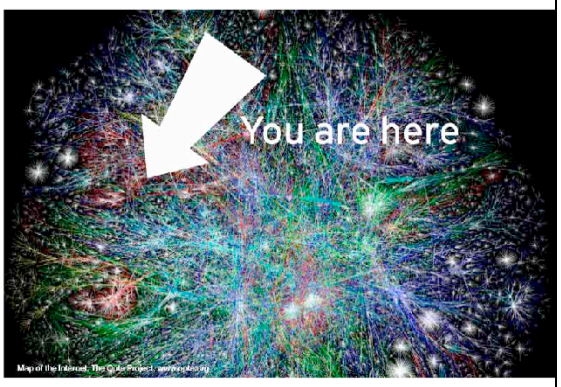
Is anyone evaluating or looking at Cloud Computing? What is one of the main questions when considering this move? Where is my data?

Data is what they attackers of after, whether it is PII, credit card numbers, databases, etc they are after the data. Hacktivism might be after infrastructure to take it down but the biggest concern is loosing data.

Know yourself

- Users
  - They are going to click on EVERYTHING
  - On a mission to explore the entire Internet.
    - The Internet is so massively big and EVIL!

– Security is not a major concern
  - They never get in trouble
  - "It was just a pop-up"
  - They "think" they know when they are being attacked



The weakest link in any security assessment is the user. The user can be socially engineered to do things they shouldn't, click on things they shouldn't and eventually give an attacker access to data that they should not have.

A snapshot of a map of the internet. It is HUGE and many areas are evil!

Anatomy of an Attack

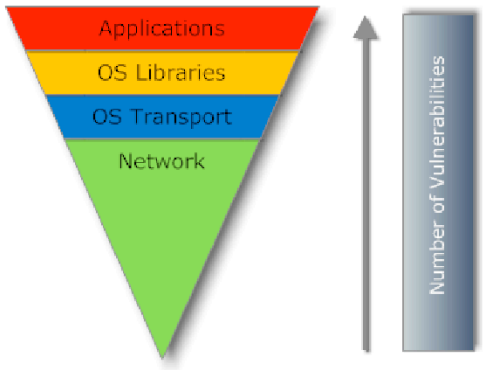
- Reconnaissance\ Information Gathering
  - Social Networks
  - Job Postings
- Scanning
  - Targeted against users
    - Spear Phishing
    - Spam
    - Social Networks
- Exploiting – initial intrusion into network
- Maintaining Access
  - Establish backdoor – outbound connection
  - Obtain user credentials
  - Install various malware
- Privilege escalation/ Lateral Movement/ Data Exfiltration
- Erase tracks

This is how attacks work and have always worked. The methods used within each point is what changes. The SANS SEC504 class that prepares you for the GIAC Certified Incident Handler certification titled Hacker Techniques, Exploits, and Incident Response is based on these main points.

The main method stays the same, the ways of doing each aspect is what changes and emerges and what we will focus on in this presentation.

How are they attacking?

- Application vulnerabilities exceed OS vulnerabilities
  - Adobe Reader 0 day
  - Adobe Flash 0 days
  - Apple QuickTime
  - Microsoft Office
- Growing Malware



Microsoft and other Operating Systems have been diligent about releasing secure code and patches to vulnerabilities in a timely fashion. Users and IT have also been keeping up to date and patching these systems on a regular basis. Therefore, the weakest link becomes the third party applications installed on these systems. Adobe has been extremely bad about patching their vulnerable software and has horrible coding practice with what is speculated to be no concern for security. The same is true for other third party applications and developers.

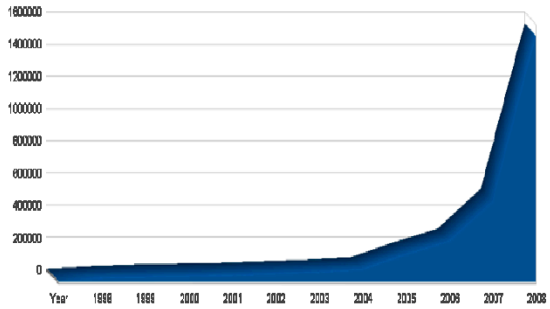
Growing Malware Threat

New threats per day:
~30,000

New signatures per day:

~3,500

Total as of September 1, 2009: 2,739,919



Signature based Anti-Virus and IDS will not catch it all!

Malware is an increasing threat. Over 30,000 new malware variants are released per day. In this presentation we will create 1 more for the purpose of proving this point. The malware will not leave the sandbox/ demo environment.

Anti-virus vendors cannot keep up with the growing threat. The growth is incredible.

How are they attacking?

- Professionally targeted to weakest links
  - Poorly configured Web servers
  - Vulnerable publishing platforms
  - Un-patched Internet-facing databases
- Obfuscated JavaScript code inserted on hacked Web pages
  - Redirects to remote server hosting exploits
  - Serves custom malware based on Windows OS version, browser version, patch level, vulnerable third party apps
  - Fires exploits simultaneously at IE, WinZip, Java, QuickTime, ActiveX controls, even Firefox … until exploit hits target
- Payload: Backdoor Trojans, password stealers, banker Trojans, spam bots
  - This is the work of highly skilled, well-organized cyber criminals

Attackers today are cyber-criminals looking to make money off of your data. Attackers no longer target the OS. They are after applications that contain data that can be used to make money! Threats come from many vectors: physical vectors (floppy disk, USB drives, CD's), Email vectors (spam, web redirection, phishing), Web vectors (drive-by downloads, malicious sites, liability). And they are targeting WEB sites as the weakest links.

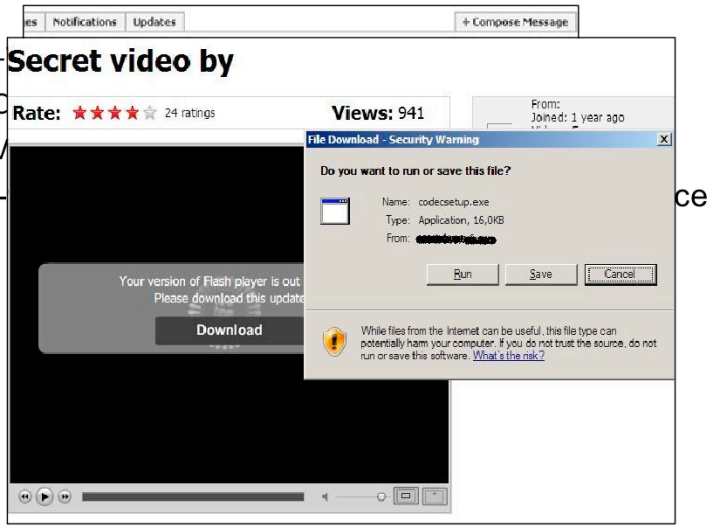
The primary web vulnerabilities, SQL Injections and Cross-site Scripting (XSS) make up 80% of the exploited vulnerabilities. Because of these, your web site could be launching malware, serving malicious content to vulnerable client side applications. If it's poorly configured to keep hackers out, hackers will plant malicious code that proliferates malware to unsuspecting surfers. Not only will your users be hurt but Google will see it and block your website until you clean it, resulting in damage to your business. Vulnerable databases that hold user data can also be hacked. Software that creates a website, like Drupal, WordPress (the most insecure), and others. Your website is vulnerable because of these platforms. Must keep systems updated and patched.

Obfuscated (hidden, obscure) Javascript, hidden in a legitimate website, redirects users connections to another server (in Astonia, Russia). This happens in background without your knowledge. You are fingerprinted, shows apps, OS, patch levels, etc., and an exploit is triggered to target a found vulnerability.

A backdoor trojan is loaded which gives the hacker access to put other things on your system, i.e., banker Trojans (programed with list of 100 banks – when you go to your bank the Trojan kicks in because it's on the list and it captures your info and uploads it to a remote server.

A Facebook Attack In Action

- Net-
  - C
  - V
- Net-



ce

Koobface. A network worm running on Windows systems. There are 60 new variants today since july 2008.

Originally found on facebook but now it's occurring on twitter and myspace. Exploits this trusted site kind of thing.

Here's what it looks like. Notice the redirector says google to add more trust.

You click on the link and it looks like Youtube. Then it tells you that you need to update your flashplayer. If you run it, you get the malware. When you get it, you then start sending the same message to all of your friends and family. **Makes you very popular!!**

Live Demo

- Attacker – BackTrack 4 LiveCD and SET
  - Perform recon on company to obtain email address of IIA presentation participant
  - Create malicious PDF file and configure it to call attacker when opened.
  - Email IIA presentation participant
- Victim
  - Running Windows XP Federal Desktop Core Configuration with all Windows Updates and Anti-Virus signatures
  - *Running Adobe Reader 9.0 latest version is 9.4.0*
  - User is very conscience about security and does not open files from people he/she does not know.
  - Will open IIA presentation because it has very valuable material
- Pray to demo gods!

Shiatata_ga_nai – Chinese for “you can not do anything about it”

How do we let this happen?

- Lack of user awareness
- Poorly protected infrastructure
  - Patch everything, not just OS but applications
- Poorly protected data
- Poorly enforced IT/Security Policy
  - Security tools deployed don't just work

What is Advanced Persistent Threat?

- Term coined by U.S. Air Force for Chinese Related Intrusions
- Attacks conducted by well funded and organized groups
  - Professionals not script kiddies!
- Motivation
  - Economic, Financial, and Political against US government and commercial entities
- Targeted attacks
- Custom Malware
- Constant Aggressor
  - Network Occupation
  - Persistent Access to network
- This is not new! Over 5 years seeing this activity!

Why is APT Successful?

- Victims and targets are not aware of these attacks
  - Good that Google disclosed?
- Information Security Defenses Don't Work!
  - APT evades:
    - Anti-Virus signatures
    - IDS signatures
    - Network appliances (firewall, IPS, etc)
    - Security Operations?
  - APT remains undetected once inside the network!

Case Study: Heartland

- They were PCI Compliant!
- ~ 130 million credit cards compromised
- Notified by 3rd party!
- Attackers had persistent long-term access
- Possible initial entrance through WEP or even open Wireless Access Point.
- Used targeted (custom) malware to propagate
- They were PCI Compliant!!
- Why was the only "early indicator" the resulting fraud? -Anton Chuvakin

Compliance ≠ Security

- Blame TrustWave?
  - No way! Not fair to TrustWave!
- Was compliance or PCI designed to make systems secure?
  - Is that even possible?
- Although Compliance is not Security are more companies more secure now because of compliance?
- Is this even a compliance issue?

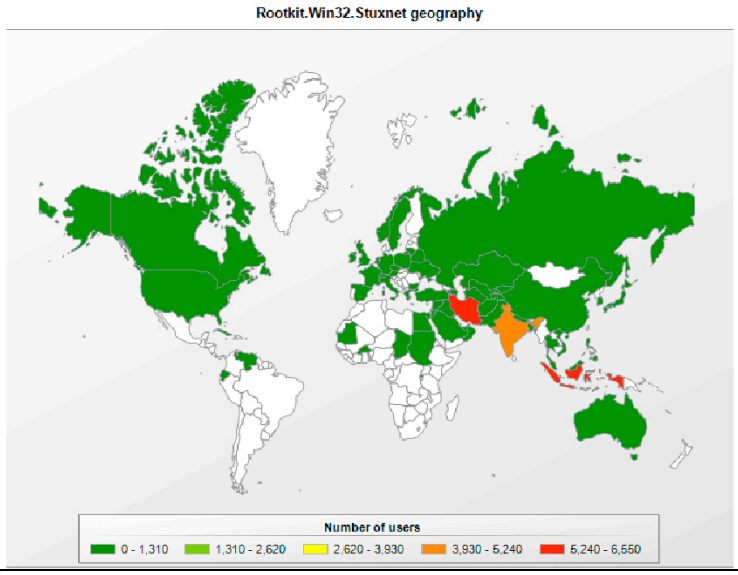
Case Study - Aurora

- Targeted Attacks
- Used Social Engineering
- Followed by 0-day on IE6
- Lots of research, time, and money
- Wasn't just Google! Many, many, others

Case Study - Stuxnet

- Very Targeted!
  - SCADA systems
  - Programmable Logic Controllers
  - Specific models: s7-300 and s7-400
  - Specific configuration in these models
- 4 different attack vectors – 0day, USB
- Uses rootkit and machines become part of botnet
- Lots of research, time, and money (nation-state involvement)
- Difficult to detect - intercepts commands, modifies, and continues to send
- Sloppy

Stuxnet Geographical Distribution



Iran was the most hit by Stuxnet. Many say it was targeting their newest nuclear facility. Analysts found Hebrew in the code but it may have been planted.

Stuxnet vs. Aurora

- Both used 0day attacks which required funded and lots of research
  - Aurora was for IE6
  - Stuxnet was on Windows up to 7!
- Stuxnet was more targeted and advanced in bypassing security tools:
  - Uses signed drivers
  - Uses Rootkit
- Aurora is a trojan while Stuxnet is a worm

Both were targeted and complex.

The Challenge!

- Are you willing to be proactive about security?
- Ask these 5 key questions:
  1. What data is being collected, transacted on, transmitted, or stored, and for what purpose?
  2. How are authentication and authorization being accomplished?
  3. What are the communications channels between each component of the system and do they cross any network boundaries?
  4. Does the solution involve: an Application Service Provider, data in the Cloud, an externally facing service?
  5. Are there any regulatory laws, statutes, and/or compliance that must be met?

You can make a difference!

- Think architecturally about security
- Follow Project Life Cycle process
- Ask the 5 key questions on all projects
- Ensure implementation of requirements
- Grow your security knowledge
- Evangelize information security in your area

Tips for Computer use at Home

- Separate computer for online banking
- Separate compute for the kids
- Set strong administrator passwords
- Use a second limited user account
- Turn the computer off when not using it
- Apply operating system AND application patches
- Don’t use wireless for online banking
- Use a strong password for online banking accounts and do not use this password ANYWHERE else

Conclusion

- You will get compromised!
  - Plan accordingly – incident response planning
- Focus on securing the data and the access to it
- Secure the user environment
  - Patch OS and applications
- User awareness training
  - Not just a form to sign
  - Test the users!

Questions?

Jorge Orchilles
jorge@orchilles.com
Twitter: jorgeorchilles
http://www.orchilles.com