Cyber Security
Current Trends & Emerging Threats

Michael Saylor | Executive Director
Cyber Defense Labs
Michael Saylor, CISM, CISA

Michael (Mike) possesses over 19 years of experience with both domestic and international companies in IT security and Cyber investigations, and IT operations. Specializing in: Technology Risk Management, Enterprise Security, Incident Response, Fraud Investigations, Digital Forensics, Project Management, Training, and Process and Policy Development. He is the Executive Director for Cyber Defense Labs located on the campus of UT Dallas, President Emeritus for the North Texas FBI Infragard, Cyber Crime Committee Member for the North Texas Crime Commission, and the CIO for the Texas Credit Union League. He was also a professor of Computer Science for the Dallas County Community College District where he served as the Chairman of the Technology Advisory Board. He has B.S. in Information Systems, and Masters (2013) Criminal Justice. Michael has worked with local and federal law enforcement in the identification and apprehension of perpetrators committing multi-million dollar fraud, embezzlement, identity theft, hacking, and racketeering crimes.
Recent Trends
  Industry Analysis (2011-2012, some 2013)
Continuing and Emerging Threats
  Continued Convergence
  Drugs, Crime, and Terrorism
Enterprise Best Practices
Recent Trends

Almost all attacks in 2012 had a web component, where data was sent to or received from a target via http or https, and took advantage of a human element (Social Engineering, Phishing, etc).

- Mobile Devices and Mobile Applications
- Hacktivism / Cyber Protests
- Advanced Persistent Threat (APT)
- Lures
  - Social Engineering & Social Media
  - Search Engine Optimization Poisoning
  - Spam and Spear Phishing
Mobile Devices

- 6 Billion Mobile Subscribers on the Planet (end of 2012)
- Mobile Apps increasingly rely on Internet browser
- Little to no patch management for mobile & Poor QA in the AppStore
- Few anti-virus / anti-malware solutions
- 51% of users circumvent or disable device passwords & security controls
- Increasing malicious mobile applications and mobile exploitation
Mobile Devices

Recent attacks include:

- SMShing – SMS texts asking for bank credentials / PIN, or to call 800 number
- Trojan / Malware – key logger, malware propagation (facebook), remote control (e.g. ZitMo & EuroGrabber targeting mobile banking credentials), infecting trusted systems.
Recent Trends

• Malicious Android Apps up 580% (28k)

• Location Services?

• Mobile Threats will impact your organization – eventually!

• CEO’s Phone?
Malware

82% of malware sites are hosted on compromised systems
55% of data-stealing malware is web-based
Hacktivism / Cyber Protests

• Attacks in Response to Geo-Political issues
• Objectives are primarily to disrupt and / or voice the views of a particular group
  – Website defacements
  – Denial of Service attacks (US Banks)
  – Automated exploit attempts
  – Disclosure of sensitive information (The Truth)
Any computer system connected to a communications medium will be compromised given enough time and the appropriate resources. 80% of attacks in 2012 required multi-stage defenses for protection.

**APT Attacks use:**
- Highly Customized Tools and Intrusion Techniques
- Stealthy, Patient attack methods to reduce detection
- Focus on high value targets (Mil, Pol, Eco, Intel)
- Well funded & staffed, supported by Mil or State Intel
- Organizations are targeted for strategic importance
APT Attackers worked with BotNet operators to determine if target systems have already been compromised. Use of polymorphic code that manifests differently on each system it infects. Cyber Criminals are becoming Information Brokers as a result of their Industrial Espionage schemes.
"A Thousand Grains of Sand..."

The Chinese continue to follow ancient book, "The Art of War," which advises the commission of espionage by "a thousand grains of sand"; meaning obtaining small but innumerable pieces of information by vast numbers of people acting as armies of spies sent against the enemy.

This recruitment usually translates to ethnic, 1st generation Chinese immigrants with cultural and familial ties to China. The Chinese government then reciprocates by helping their part-time spies create or proceed with commercial or business ventures in the United States. This is called guanxi. As a result, the Chinese coordinators do not offer money, and they do not accept walk-in cases, which may turn out to be "dangles" (double agents). Most espionage activities are coordinated by the Ministry of State Security (MSS) or the military intelligence arm of the People's Liberation Army (PLA).

Dave Wise, Espionage Author
Espionage

- Mandiant’s 2013 report on Chinese (APT1) attacks on 141 organizations since 2006 (115 were in the U.S.).
- The report presents substantial evidence of Chinese sponsored activities, including photos, forensics, communications, and profiles.
- Soon after Mandiant’s report, the U.S. government publishes a 140 page strategy to combat the theft of U.S. trade secrets.
- The U.S. government initially attempted to halt the attacks on U.S. organizations, but soon resorted to asking China to please stop stealing our stuff.
- China’s response to the Mandiant report was that it was “unprofessional” to publish and make such claims.
According to the U.S. Justice Department, of 20 cases of economic espionage and trade secret criminal cases from January 2009 to January 2013, 16 involved Chinese nationals; i.e. organizations hired foreign nationals to work on national security level projects (DuPont, NASA, Google, Intel, DoD, etc.).

63% of impacted organizations learn they were breached from an external source, like law enforcement.

Organizations are being targeted by more than one attack group, sometimes in succession. In 2012, 38% of targets were attacked again after the original incident was remediated, lodging more than one thousand attempts to regain entry to former victims.

Feb 2013 report (Akamai) shows that 30% of all observed attacks came from China and 13% originated from within the U.S. March 2013 report (Solutionary) states that the majority of attacks on the U.S. are now originating in the U.S.
Longest time period within which APT1 has continued to access a victim’s network:

4 Years, 10 Months

Largest APT1 data theft from a single organization:

6.5 Terabytes over 10 months
In 2012, Exploit Toolkits cost between $40 and $4k.

61% of all malware is based on pre-existing toolkits; upgrades are made to keep them current and provide additional capabilities.

Toolkits used for Targeted Attacks can create custom Blog entries, emails, Instant Messages, and web site templates to entice target organization personnel toward malicious links / content. (Blackhole >100k/day)

Broadcast attacks will use toolkits to automate SQL injection, web tools, or server exploits in an effort to inject a malicious link within target websites.
• Traditional Attacks were loud, high volume attacks typically stopped by threat monitoring tools.
• Today's sniper attacks use specific exploits to get clear shots at the objective.
• The convergence of Social Engineering, Social Profiling, and Geo-Location improve attack success.
• Rogue software (anti-virus, registry cleaner, machine speed improvement, backup software, etc)
  – Increase in MAC Malware (MACDefender)
  – +50% attacks on Social Media sites were Malware

Exploit Toolkits & Malware
Several attacks in 2012 were conducted by luring victims to accept malware or follow a link to an infected site. 92% of all email Spam contained a Link.

There are 6 stages of the attack:

1. **LURE**
   - Two Types: email and web
2. **REDIRECT**
   - Funnels and sends the user to a hidden server.
3. **EXPLOIT KIT**
   - User's system is inspected for an open vulnerability
4. **DROPPER FILE**
   - If vulnerability exists, malware dropper file is delivered
5. **CALL HOME**
   - Calls home for more malware to expand attack
6. **DATA THEFT**
   - Cybercrime reaches out into internal systems for data to steal
Lures

1,760 online visitors per few seconds

1,267,200 visitors a day

One infected visitor share with 130 friends

823,680 Facebook users see scam
Lures – Facebook Specific

• Typo-Squatting
• Fake Facebook Applications
• Hidden Camera Video Lure
• Celebrity Deaths
• Fake Offers & Gifts
• Browser Plugin Scams
• Fake Profile Creeper
• Blog Spam Attack

SOCIAL NETWORKING BY NUMBERS

- Facebook
  - 845M active users per month
  - 483M active users per day
- Twitter
  - 140M active users
  - 340M Tweets a day
- Pinterest
  - 11.7M unique visitors per month
- LinkedIn
  - >150M users
- Google+
  - >100M active users
Top5 Social Engineering Lures
2012 saw an increase in malware infections as a result of SEP.

- Hackers crawling current news headlines, creating related malicious sites and conducting SEP
- Google Images – links to source photo
- Using web analytics to determine what people are searching for
SPAM & Phishing

2012 Symantec Results

• Spam is at 66.8% of all global email
• Phishing attacks are 1 in every 467 emails
• Malware is in 1 out of every 316 emails
• Began to see combination of email and SMS for targeted attacks
Dear Staff,
The new design for our network services such as email and internet have been installed, please proceed to activate its usage on your system using the link below.

http://www.avant.net.br/testes/yourls/activatenow

Thank You
IT Department

Your mailbox has exceeded the size limitation set by your system administrator and you may not be able to send or receive new mail until you re-validate. To re-validate please ClickHere. System Administrator.
Mobile Internet will continue to increase as it eventually takes the place of desktop Internet. The illegal drug organizations are looking to Cyber Crime to facilitate their business and expand their operations. Your organization could be infiltrated by an insider, socially engineered for identities and social profiles, and potentially held hostage with ransomeware.

Localized Nation State attacks on U.S. increase

Emerging Threats

TOP 8 RANSOMWARE-INFECTED COUNTRIES

UNITED STATES 41%
GERMANY 25%
FRANCE 11%
HUNGARY 11%
ITALY 11%
RUSSIA 4%
TAIWAN 2%
AUSTRALIA 4%
Emerging Threats

Terrorists are expected to continue to expand their technical capabilities which may lead to an increase in cyber crime and cyber terrorism.

• Domestic groups funded by foreign States to conduct US-based attacks
• Cyber crime as a funding vehicle for Terrorism
• Cyber as a facilitator / component for a Terrorist attack (Effects-based Operations)
Emerging Threats

- Malware embedded at the hardware / chip level of consumer products will continue to increase.
- Targeted Attacks and APT will continue to increase in number and sophistication.
- Sophistication from APT attacks will trickle down to black market malware toolkits.
- Mobile Phone attacks will increase in volume and type.
- Insider Threat will continue to grow as new technology is introduced, especially non-company devices.
- Thwarting attacks will require multi-stage defenses.
Emerging Threats

- Attackers are increasingly using outsourced service providers (HR, Procurement, IT, Finance, etc.) as a means to gain access to their victims.
- Attackers are using comprehensive reconnaissance (network, physical, social) to help navigate victims’ organization and networks more effectively (e.g. network infrastructure, system administration guides, etc.)
- The use of Mercenary Cyber Commandos (Gangs / Cartels) will grow to support the organizational foot soldiers of Nation State actors.
Blended threats are cybercriminals’ answer to wreaking greater havoc among users. Developments like the reemergence of ransomware or the proliferation of spam campaigns allow the bad guys to profit off stolen data. Whether on desktops or mobile devices, blended threats remained just as prominent.

Emerging Threats

• Growth of the Dark Web / Tor Network

  – Law Enforcement has little understanding of these “off the web” networks, how to access them, and the types of activities being conducted there, including:
    • CrimeWare
    • Child Pornography
    • Trafficking of Drugs, Weapons, Humans
    • Child Exploitation
    • Sex Tourism

  – Without LE involvement and understanding in these networks, criminal activity will grow and evolve, and outpace legislative and procedural response to these crimes.
Emerging Threats

- Sophistication of “Call-Home” tactics of Malware will continue to grow, including the use of Twitter, DNS, VoIP, and other open communication channels for command and control.
- Recent and emerging Malware and Crimeware receive updates / patches and can be armed with various modules.
- Your Social Media Identity is or soon will be valued greater than your Credit Cards.
Best Practice Guidelines

User Education and Awareness
Containment is the new Prevention….Compromise is inevitable
Monitoring Network, Vulnerabilities, and Brand
Anti-Virus, Anti-Malware, Device Control
Encryption

Data Loss Prevention & Monitoring
Removable Media Policy
Mobile Device Policy

Frequent Risk-Based Security Assessments and Updates
Aggressive Patching and Software Polling
Incident Response Procedures

Social Media / Social Networking Policy
References

Mandiant Report – February 2013
Bit9 Cyber Security Report 2012
Symantec Intelligence Reports 2012
Georgia Tech - Emerging Cyber Threats Report 2012
WebSense Threat Report 2012
TrendLabs – Security in the Age of Mobility 2012
Breakthrough Silicon Scanning Discovers Backdoor, University of Cambridge 2012
Kaspersky Labs report on Red October 2013
Tiger Trap, David Wise, 2012
TrendMicro, Peter the Great versus Sun Tzu, 2012
Questions / Contact Info

Questions?

Mike Saylor | Cyber Defense Labs
Msaylor@CyberDefenseLabs.org
972-454-0227

Terry Quan | Cyber Defense Labs
TQuan@CyberDefenseLabs.org
214-563-5235