



Cyber Defense in a Post APT 1 World

Nick Essner
SOC/CIRT Strategic Solutions
Mandiant, a FireEye Company

We Live the Headlines

**Bloomberg
Businessweek**

**Evernote Says Cyber Breach
Which Cost Millions Wasn't
From China** -- *BusinessWeek*, May 2013

THE WALL STREET JOURNAL

**Fed Acknowledges
Cybersecurity Breach**
- *Wall St. Journal*, Feb 2013

**LivingSocial Hack Exposes
Data for 50 Million Customers**

- *New York Times*, April 2013

**3.6 Million Social Security Numbers
Hacked in South Carolina**

- *The State Newspaper*, Oct 2012

**Hacking of US media
is 'widespread
phenomenon'**

- *Wired*, Feb 2013

The New York Times

**Hackers in China Attacked the
Times for Last 4 Months**

- *New York Times*, Jan 2013

**2.4 Million People At Risk Over
Schnucks Credit Card Breach**

- *St. Louis Today*, Apr 2013

**NASDAQ Confirms a
Breach in Network**

- *Wall Street Journal*, Feb 2011

COMPUTERWORLD

**Intel Confirms
'Sophisticated'
Attacks in January**

- *Computerworld*, Feb 2010

**Sony PlayStation
Suffers Massive
Data Breach**

- *Reuters*, April 2011

The New York Times

RSA Faces Angry Users After Breach

- *New York Times*, June 2011

The New York Times
**Cyberattack on Saudi Oil Firm
Disquiets U.S.**

- *New York Times*, Oct 2012

Mandiant In the News

The New York Times
"All the News That's Fit to Print"
 TUESDAY, FEBRUARY 19, 2013
Reprinted With Permission

International

China's Army Seen as Tied to Hacking Against U.S.

Report Traces Attacks to Military Office's Doorstep — Power Grid Is a Target

BY MICHAEL HAYDEN
 MICHAEL HAYDEN, a former director of the CIA and national security adviser, is shown in a video recording of a news conference. He is wearing a suit and glasses and is speaking into a microphone. The background is a news studio with a large screen displaying a map of China.

On the evening of Feb. 17, 2013, a Chinese military officer in a dark uniform was seen in a video recording of a news conference. He is wearing a suit and glasses and is speaking into a microphone. The background is a news studio with a large screen displaying a map of China.

...the United States, the Chinese military has been seen in a video recording of a news conference. He is wearing a suit and glasses and is speaking into a microphone. The background is a news studio with a large screen displaying a map of China.

...the United States, the Chinese military has been seen in a video recording of a news conference. He is wearing a suit and glasses and is speaking into a microphone. The background is a news studio with a large screen displaying a map of China.

The New York Times
"All the News That's Fit to Print"
 THURSDAY, JANUARY 31, 2013
Reprinted With Permission

International

Hackers in China Attacked the Times for Last 4 Months

Computer Assaults Tied to Reporting on Premier

By NICOLE PERLBOTH

For the last four months, Chinese hackers have persistently attacked the New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

After surreptitiously tracking the intruders to study their movements and help erect better defenses to block them, The Times and computer security experts have expelled the attackers and kept them from breaking back in.

The timing of the attacks coincided with the reporting for a Times investigation, published online on Oct. 25, that found that the ter, had accumulated a for billion dollars through bus

source, experts said, is that the attacks started from the same university computers used by the Chinese military to attack United States military contractors in the past.

Security experts found evidence that the hackers stole the corporate passwords for every Times employee and used those to gain access to the personal computers of 25 employees, most of them outside The Times's newsroom. Experts found no evidence that the intruders used the passwords to seek information that was not related to the reporting on the Wen family.

No customer data was stolen from The Times, security experts said.

Asked about evidence that indicated the hacking originated in China, and possibly the military, China's Ministry of National Defense said, "China's laws prohibit any action including hacking that damages Internet security." It added that "to accuse the Chinese military of launching cyberattacks without solid proof is unprofessional

2008, Chinese hackers began targeting Western journalists as part of an effort to identify and intimidate their sources and contacts, and to anticipate stories that might damage the reputations of Chinese leaders.

In a December intelligence report for clients, Mandiant said that over the course of several investigations it found evidence that Chinese hackers had stolen e-mails, contacts and files from more than 30 journalists and executives at Western news organizations, and had maintained a "short list" of journalists whose accounts they repeatedly attacked.

While computer security experts say China is more active and persistent, it is not alone in using computer attacks for a variety of national purposes, including corporate espionage. The United States, Israel, Russia and Iran, among others, are suspected of developing and deploying cyberweapons.

The United States and Israel have never publicly acknowledged it, but evidence indicates they're releasing a sophisticated computer program that attacked and destroyed a nuclear power plant in Iran.

CBS
NIGHTLINE
GLOBAL HACK ATTACKS
NEW EFFORT TO FIGHT RISING CYBER THER

Grady Summers
 MANDIANT

REUTERS
By Jim Price
Reuters.com

Mandiant goes viral after China hacking report

February 22, 2013

Reuters' Cybersecurity company Mandiant Corp won plaudits from its peers and made four-page news around the world this week when it published a report that purportedly traced a series of cyberattacks on U.S. companies to a Shanghai-based unit of the Chinese army.

But some hackers have turned the tables on the cyber-expert by creating malicious versions of its 76-page report that were infected with computer viruses. They emailed the tainted reports to their victims this week in a bid to weaken Mandiant's name.

Though the episode was embarrassing, the company said its systems were not breached. "Mandiant has not been compromised," the company said in its corporate blog.

Mandiant was founded in 2004 by Ivan Mandia, a former U.S. Air Force cyber-forensics investigator who co-authored an influential textbook on the subject. The company made its name by automating processes used to investigate computer breaches.

Mandiant was largely unknown outside the computer security industry until Monday, when it flogged the People's Liberation Army's Shanghai-based Unit 61398 as the most likely driving force behind a Chinese hacking group known as APT1.

China's Defense Ministry issued a flat denial of the accusations and called them "unprofessional." But Mandiant won kudos for the unprecedented level of detail in its report, including the location of a building in Shanghai's Pudong financial hub from which Mandiant said the unit had stolen "hundreds of terabytes of data from at least 40 organizations across a diverse set of industries beginning as early as 2005."

Other security companies that have published reports on cyberattacks have shied away from so clearly identifying their perpetrators.

"It was a wonderful report," said Michael Hayden, a former director of the CIA and national security adviser, who is now with the Clarendon Group. "Empirically, it's about time."

The report did not identify the victims of APT1 or Mandiant's customers, though the company says it has worked for about 40 percent of the Fortune 500.

When asked why he had decided to go public with this report, Mandia, 42, told Reuters: "There is mounting frustration in the private sector. Tolerance is shrinking. We also have a bunch of employed folks who are 80-hour a week but don't get paid and said, 'Let's just this out.'"

The report comes ahead of next week's annual RSA Conference on security in San Francisco, where Mandiant will showcase its products to help companies identify security breaches.

FO THE RECORD?

Mandiant says it begins investigations by installing software that has developed that searches for infections by looking for evidence of hacker leave behind. It refers to those digital signatures as indicators of compromise, or IOC.

The proprietary database of those indicators makes up a critical part of the "tactical sauce" that automates the investigation process and, Mandiant says, enables investigators to root out attackers faster than rivals.

The company has thousands of IOCs in its database, which it constantly replenishes.

"We tend not to take the small jobs. We take the big ones — the ones you would love to read about in the paper, but we leave them out of the paper," said Mandiant's chief security officer, Richard Blyden.

Some investors have speculated that Mandiant is preparing for an initial public offering in the next year or so. On Friday, it named Mel Wesley to the post of chief financial officer. Wesley was CFO of publicist need OBJECT, which was sold to Silverline Technology in December for about \$1 billion.

Mandia, who raised \$70 million by selling stock to Silicon Valley venture capitalist firm Visiter Parkers, Caufield & Biers and One Equity Partners, the private investment arm of Zhongshan Capital & Co. said he is in no rush to go public. "I do not believe we need more capital," he said.

Tim Screen, a partner with Kleiner Perkins, declined to say if an IPO was in the works, but told Reuters: "There are certainly of the

U.S. security firm ties hacking attacks to Chinese military unit based in Shanghai
LIVE CNN

CHINA'S HACK ATTACK
140+
U.S. COMPANIES AND GROUPS

Grady Summers
 MANDIANT CORPORATION VP

Bloomberg Businessweek
Technology
Hacked? Who Ya Gonna Call?

► Mandiant is the go-to responder for cyber-espionage attacks
 ► "It's a reputational thing. They play well with law enforcement"

The brand-new operations center of cybersecurity firm Mandiant is deceptively tranquil. Rooms in the third-floor office, overlooking a lagoon in Redwood City, Calif., are playfully named after locations on the Starship Enterprise from *Star Trek*, including a kitchen called 10-Forward.

In one large central control room, dubbed the Bridge, a dozen security analysts peer quietly at their computer monitors, looking for anomalous activity on the computer networks of Mandiant's hundreds of corporate clients around the world. A large computer display on the wall shows an image of the earth, seen from space, that highlights in-bound and outbound network activity in each country. Mandiant monitors the entire planet, yet a printout taped to the

who have written negative stories about the country or its government. After detecting the breaches, papers included the *Times* and *Post* contacted Mandiant, a 9-year-old Alexandria (Va.)-based company with a reputation among industry insiders for technical proficiency and large egos. It also has a budding business on the front lines of U.S. companies' intensifying war with international cyberpirates.

In a wave of cyberattacks beginning in 2009, dubbed Operation Aurora by security firm McAfee, sophisticated hackers based in China breached the corporate networks of Google, Yahoo!, Juniper Networks, Adobe Systems, and dozens of other prominent technology companies and tried to

Experts in Advanced Targeted Threats

- **Expert Responders for Critical Security Incidents**

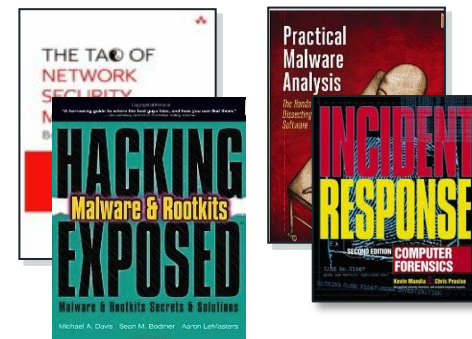
- Incident responders to the biggest breaches
- We train the FBI & Secret Service
- Our consultants wrote the book (literally) on incident response
- Clients include more than 40% of Fortune 100

- **Our Products Are Based on Our Experience**

- Built to find and stop advanced attackers
- We use our own products in our investigations
- SC Magazine 2012 & 2013 “**Best Security Company**”

- **Global Reach & Presence**

- 2000+ employees
- Offices in global regions: Asia-Pacific-Japan, Australia/NZ, Americas, Europe & META.



Overview

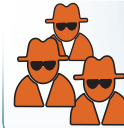
- The Who
- The How
- What Led to APT1 Report
- 1 Year Later
- APT1 Report Lessons Learned



The Who

Targeted Attacks Routinely Bypass Preventive Defenses

Advanced Persistent Threat (APT)



Advanced Targeted Attacks

Commodity Threats

Worms & Bots

TRADITIONAL PREVENTIVE SOLUTIONS
"Next-Gen" Prevention

100%

Of Victims Had Up-To-Date Anti-Virus Signatures

63%

Of Companies Learned They Were Breached from an External Entity

46%

Of Compromised Systems Had No Malware on Them











100%

Of Breaches Involved Use of Stolen Credentials

Source: Mandiant M-Trends 2012 and 2013



Breaking Down the Threat

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Network Attack
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat	Credit Card Theft	Website Defacements	Destroy Critical Infrastructure
Targeted					
Character	Automated	Persistent	Opportunistic	Conspicuous	Conflict Driven

The How

Targeted Threat: Lifecycle Technique



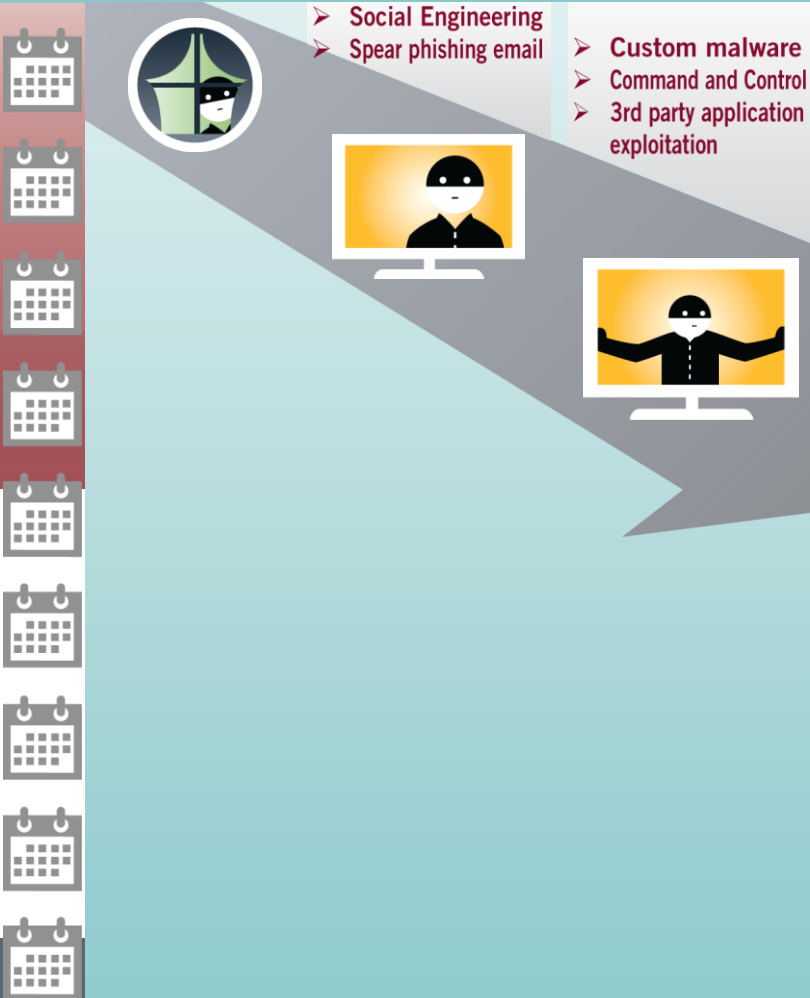
Targeted Threat: Lifecycle Technique



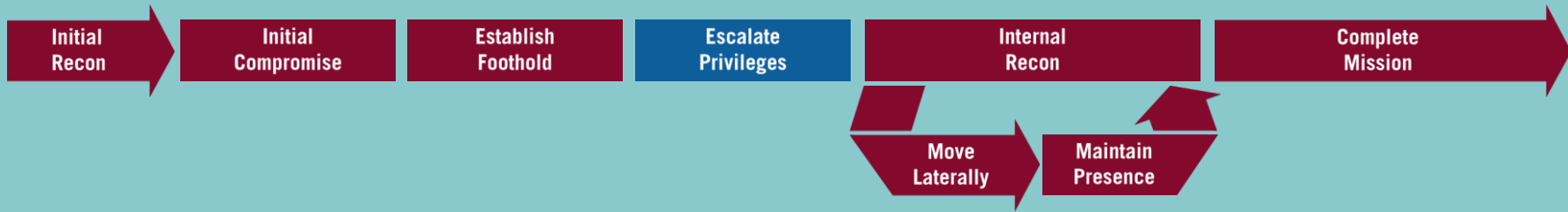
- Social Engineering
- Spear phishing email



Targeted Threat: Lifecycle Technique



Targeted Threat: Lifecycle Technique



- Social Engineering
- Spear phishing email



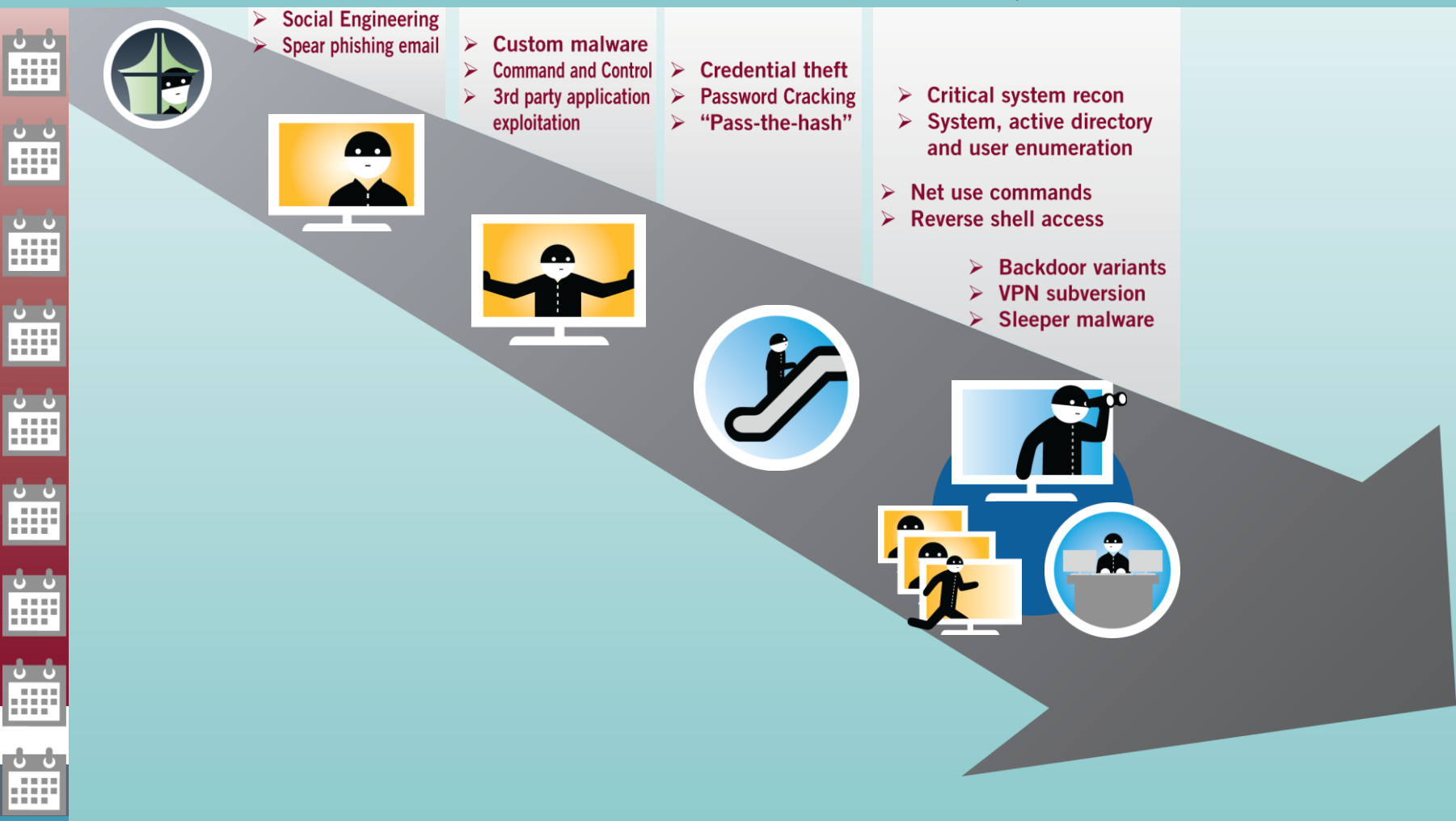
- Custom malware
- Command and Control
- 3rd party application exploitation



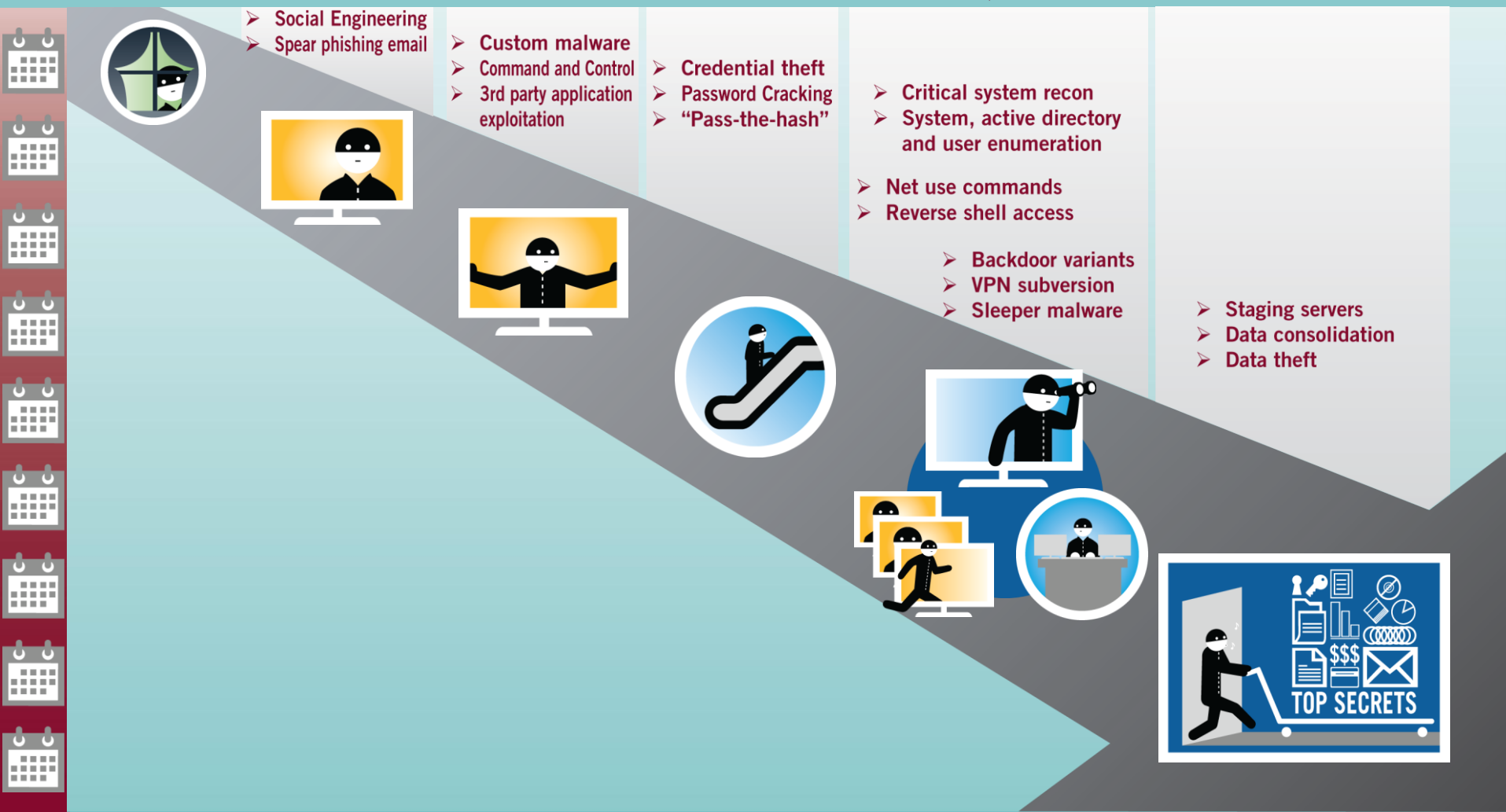
- Credential theft
- Password Cracking
- "Pass-the-hash"



Targeted Threat: Lifecycle Technique



Targeted Threat: Lifecycle Technique



The What

Cyber Espionage “Real World” Examples



PRC J-31



PRC Loong-1



US F-35



US MQ-9

Goophone "clone"



Data Theft: A Lot More than R&D

- Chinese cyber theft of weapons and trade secrets makes front page news...but there's more to the story
- China wants to understand how US/Global businesses work—down to the board room minutes and executives' emails

WHAT MAKES THE HEADLINES...

Compromised U.S. DoD weapons systems:⁵

- » PAC-3
- » F-35
- » THAAD
- » Navy's Aegis ballistic-missile defense system
- » F/A-18
- » V-22 Osprey
- » Black Hawk helicopter
- » Littoral combat ship

AND WHAT DOESN'T:

China-based APT data theft of a broader nature:

- » Executive emails
- » Business processes
- » Negotiations plans
- » Budgetary information
- » Organizational charts
- » Meeting minutes
- » Human resources records
- » Programs & initiatives

China's Response

“It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence.”

- Chinese Defense Ministry, January 2013

Timeline

2013 TIMELINE OF EVENTS — APT1 AND APT12



APT1 Report

18 Feb 2013: Mandiant Released APT1 Intelligence Report

- Linked APT1 to PLA unit 61398
- 5 minute video of APT1 in action

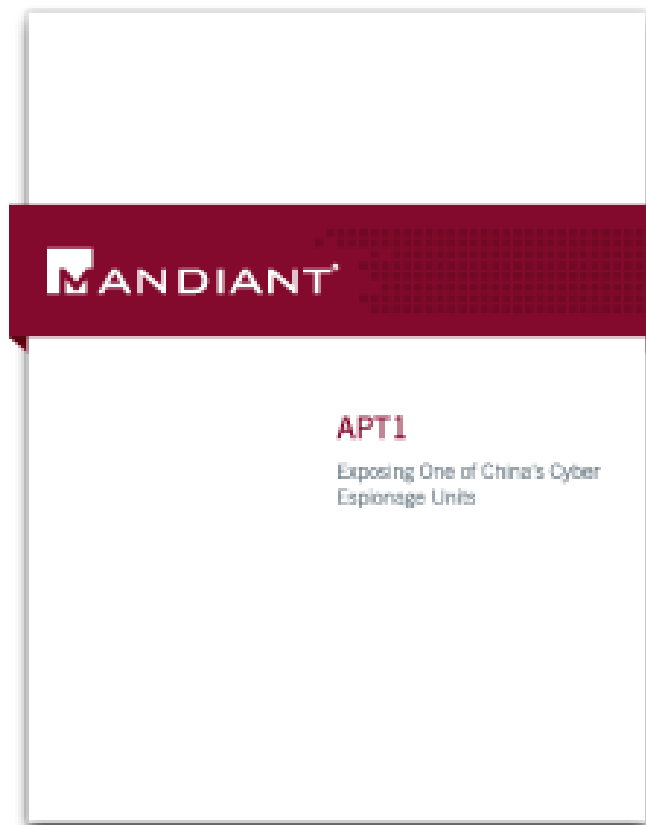
Released 3000+ Actionable

Indicators of Compromise (IOCs)

- OpenIOC format
- Malware reports
- IPs/domain names
- MD5s
- SSL Certificates

Attribution Included:

- Technical data from 140+ intrusions
- Persona and Infrastructure registration
- PLA and PRC Documents
- China Telecom information



Accuracy

20 Feb 2013: CNN video of PLA chasing CNN vehicle at building location

(<https://www.youtube.com/watch?v=yG2ezzLHSD0>)



“I read the Mandiant report. I've also read other reports, classified out of Intelligence, and I think the Mandiant report, which is now unclassified, it's public, is essentially correct”

-- Sen Feinstein, Chairwoman of Senate Intelligence Committee

APT1 – Reaction

- **Monday 2/18 – Business as Usual**
- **Report released at 10 PM EST**
- **Tuesday 2/19 – Action Plan Invoked**
 - Domains parked
 - WHOIS registry changed
 - Backdoor/tools removed
 - Staging/working directories cleared
 - New backdoors implanted
- **PRC Reaction:**
 - High-level public statements
 - Unusual military presence



20 Feb 2013: PLA guard at MUCD 61398

“There is still no internationally clear, unified definition of what consists of a 'hacking attack'. There is no legal evidence behind the report subjectively inducing that the everyday gathering of online (information) is online spying.”

-- 20 Feb 2013, PLA Defense Ministry



One Year After the APT1 Report:



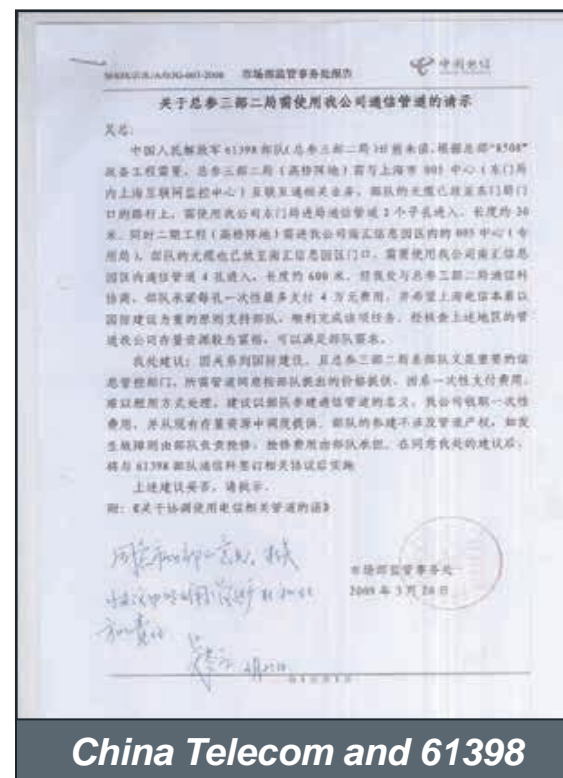
Impact on APTs

■ Short-Term Impacts

- Unreleased Indicators **did not** change
- NYT coverage **did not** stop intrusions...
- But APT1 Report did
- **ALL** APT groups acted in coordination following APT1 Report

■ Long-Term Impacts:

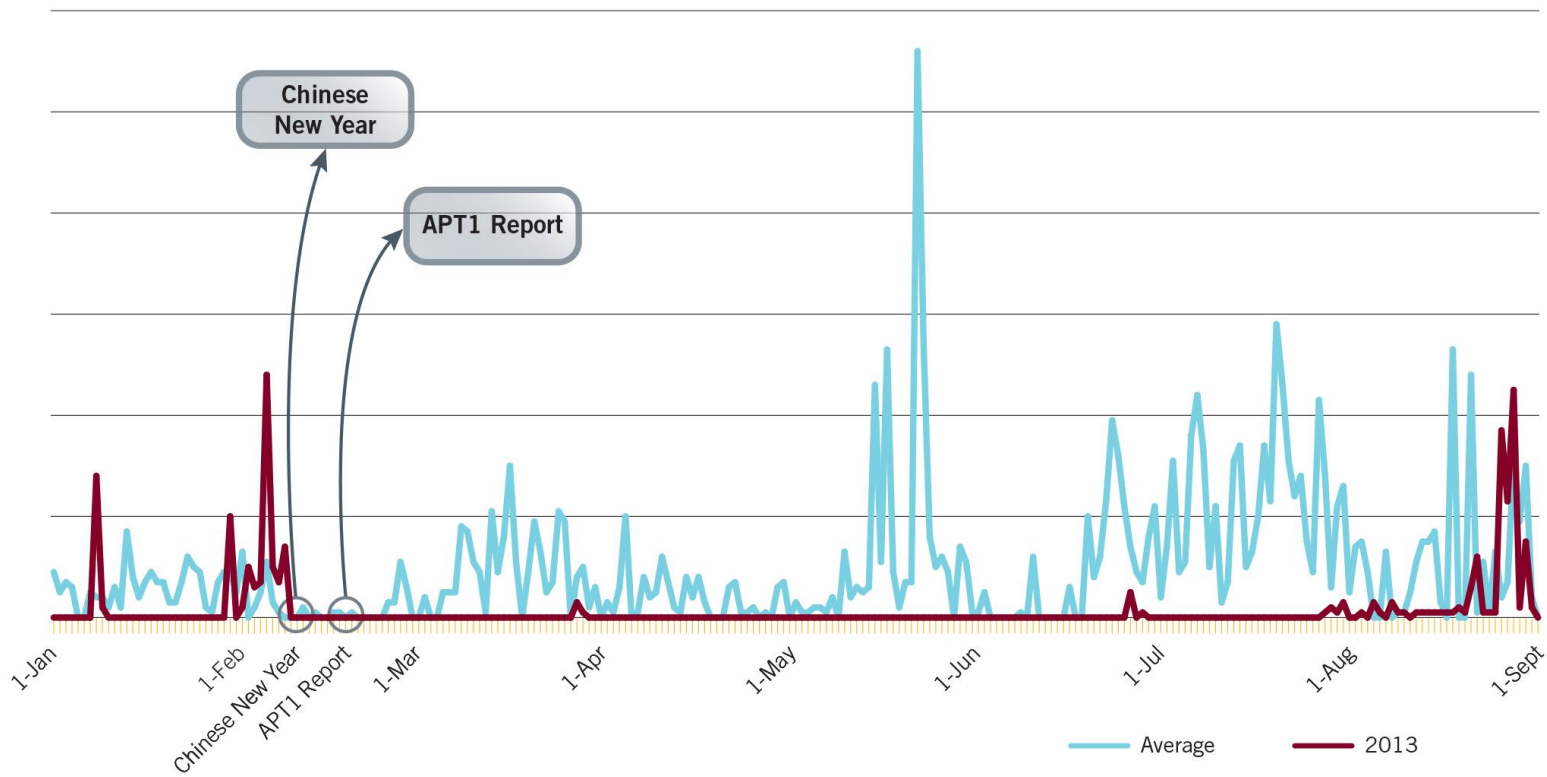
- All groups resumed normal activity levels
- No changes in targeting
- No changes in TTPs



Mandiant learned significant lessons about the nature of APT groups as a collective entity following the APT1 Report. Mandiant considers the uniform actions of ALL suspected China-based groups after the report confirms our attribution as well as speak to the level of Chinese coordination and control.

APT1 Reacts

NUMBER OF APT1'S 2013 C2 SESSIONS COMPARED TO BASELINE ACTIVITY FROM 2010-12

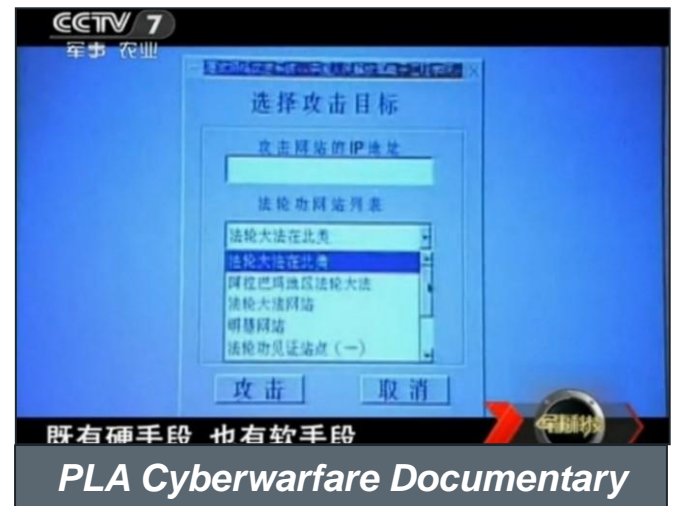


Lessons Learned

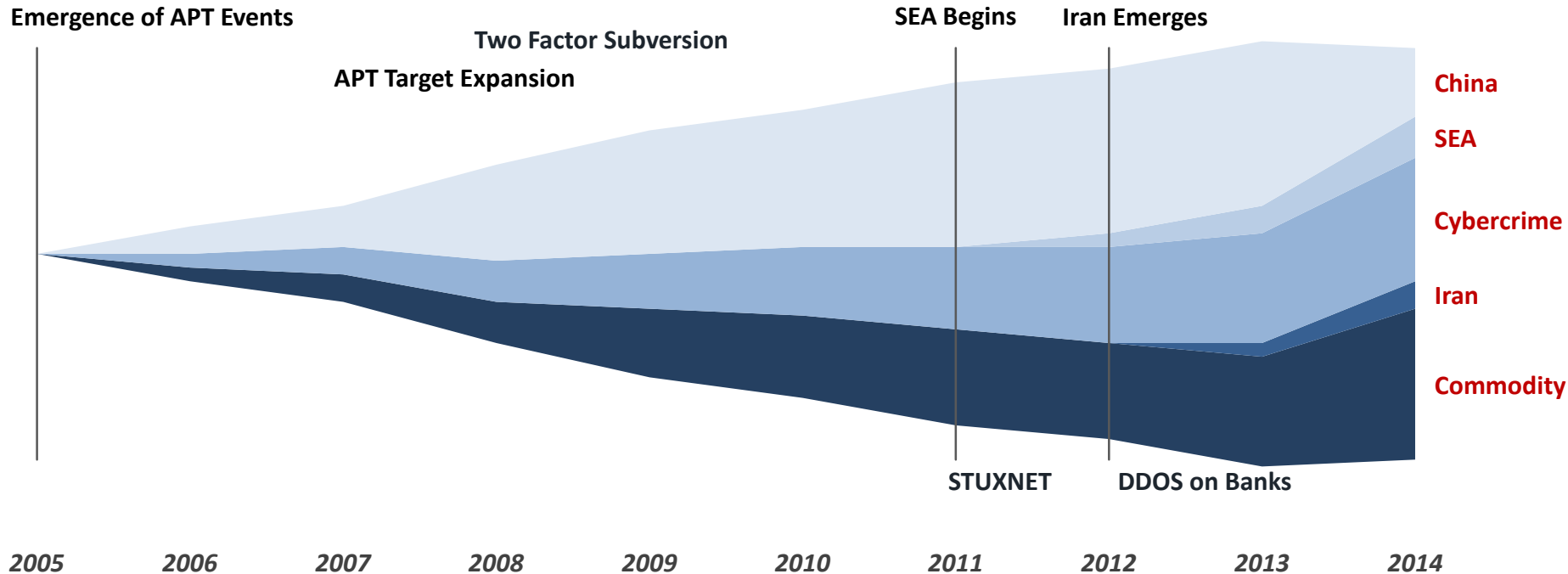
- **What Did We Learn?**
 - APTs respond to a command structure
 - APTs follow media coverage
 - APT “Re-Tool” time is short
 - Only adjust disclosed portions
- **What Does It Mean?**
 - Public disclosures = difficult detection
 - APTs are resilient
 - APTs are not going away
 - “Public shaming” ≠ intrusion response
 - CCP role is critical
 - PRC/PLA beliefs are applicable to APTs



Unit 61398 Office Location



Threat Landscape

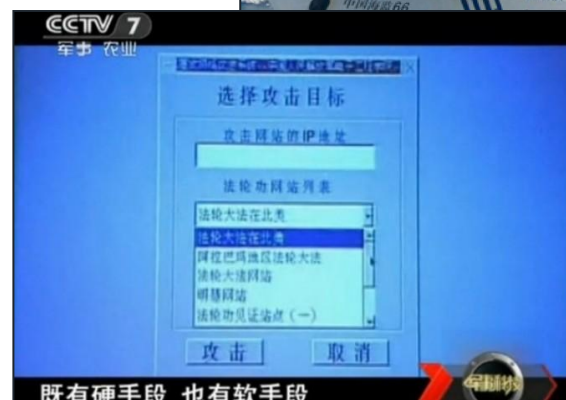


The Asian region faces an active cybercriminal element, encounters frequent hacktivist events tied to international issues as well as country conflicts, and has various nations possessing cyber capabilities. APT threats are the most significant cyber threat to the region based on the importance of the Pacific to the PRC.



Implications

- **Activity Likely to Worsen:**
 - All trends are upward
 - Geopolitical situation is key driver
- **Intrusions Matter:**
 - Data theft rapidly synthesized
 - Used for actionable gains
 - Intrusion effects are cumulative
- **Expected APT Actions:**
 - Valid access and trusted partners
 - Maintenance activity
 - Specific networks, users, data
 - APTs at targets that matter



Lessons Learned

Key Trends



Increased sophistication of network reconnaissance using custom tools and targeting specific systems.

Attackers targeting outsourced service providers and business partners



The use of publicly-available malware is on the rise, creating challenges for enterprise security teams.

Mandiant observed an increasing number of APT attacks which were discovered during the M&A process.



Increase in targeted attackers using strategic web compromise attacks.

In 2012, 38% of targeted companies continued to be a target after successful remediation.



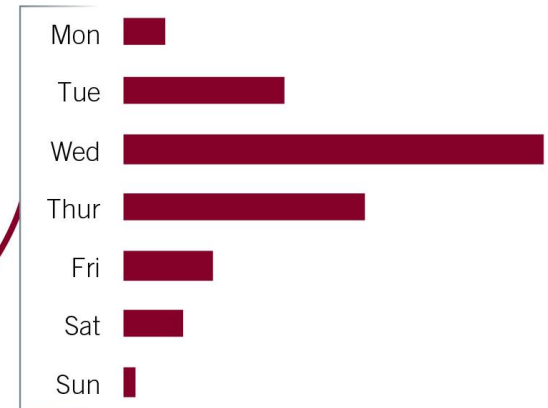
Still Phishing



44%

of observed phishing emails were IT related, often attempting to impersonate the targeted company's IT department

93% of phishing emails were sent on weekdays



Undetected Presence



229

median number of days that threat groups were present on a victim's network before detection



14 days less than 2012

Longest Presence: 2,287 days

Increasingly Agile Attackers

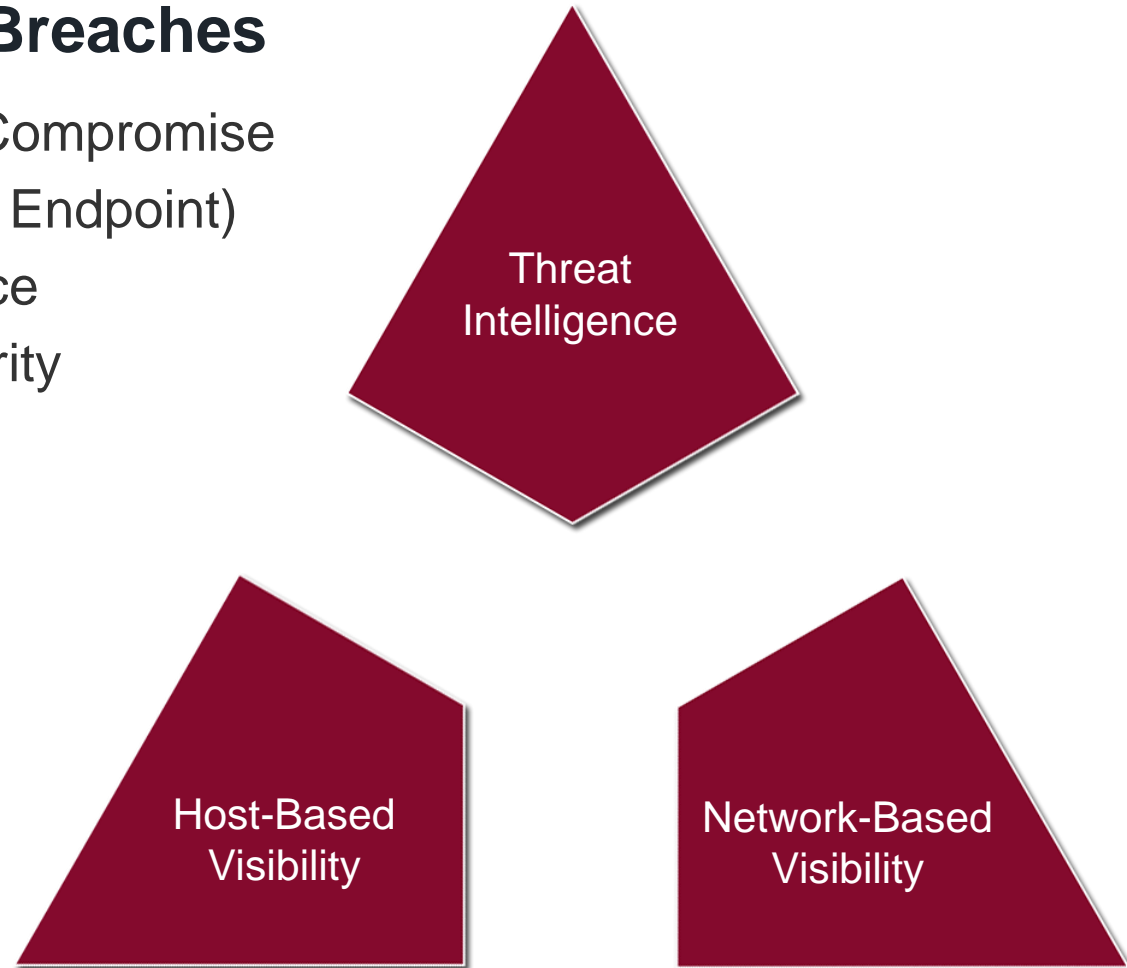
Examples from recent investigations:

- Extensive reconnaissance of victims
- Deep knowledge of victim networks (sometimes better than the organization's own network team)
- Aggressively fighting remediation
- Shifted work schedule to victim's 9-to-5 to counter activity in real time
- Switched to controlling victim PCs via VPN when proxy servers were blocked
- Completely upgraded tools and infrastructure in a two day window
- Attacker will find the path of least resistance
- Adversary will only expose their deepest competencies as a last resort

New Security Paradigm

Organizations Must Seek to Eliminate the Consequences and Impact of Security Breaches

- Ability to Operate Through Compromise
- Holistic Visibility (Network & Endpoint)
- Actionable Threat Intelligence
- Shift to Threat Centric Security



Preventing APT compromises

What's effective?

- **Fast detection and response** is a more effective approach than trying to stop it
- Visibility into network AND endpoints!
- SIGNATURE BASED DETECTION IS DEAD (well, mostly)
- Intelligence is king
- The basics still apply: general system hygiene is important
- Removing admin rights for general users
- Whitelisting
- Privileged access management / IAM improvements
- Proxy “speed bump”
- Virtualize the browser/app/PC



Intelligence is King

- Indicators of Compromise (IOC)
- Intel Mixology
 1. “Tier 1” - Commodity (C2, sinkhole, open source, etc)
 2. “Tier 2” – APT, State Sponsored. “Top Shelf”
 3. Sharing – Partners, Co-opetition, Industry, Government
- Apply Threat Intel operationally to event data at **speed & scale**
- Security Intel vs Threat Intel
 - Structured vs Unstructured



M-Trends 2014



Download the
Full Report
www.mandiant.com





Contact Information:

Nick Essner
SOC/CIRT Strategic Solutions
nick.essner@mandiant.com

