



A FireEye® Company

The Threat Today

James Nettesheim, Senior Consultant

SECURITY
CONSULTING

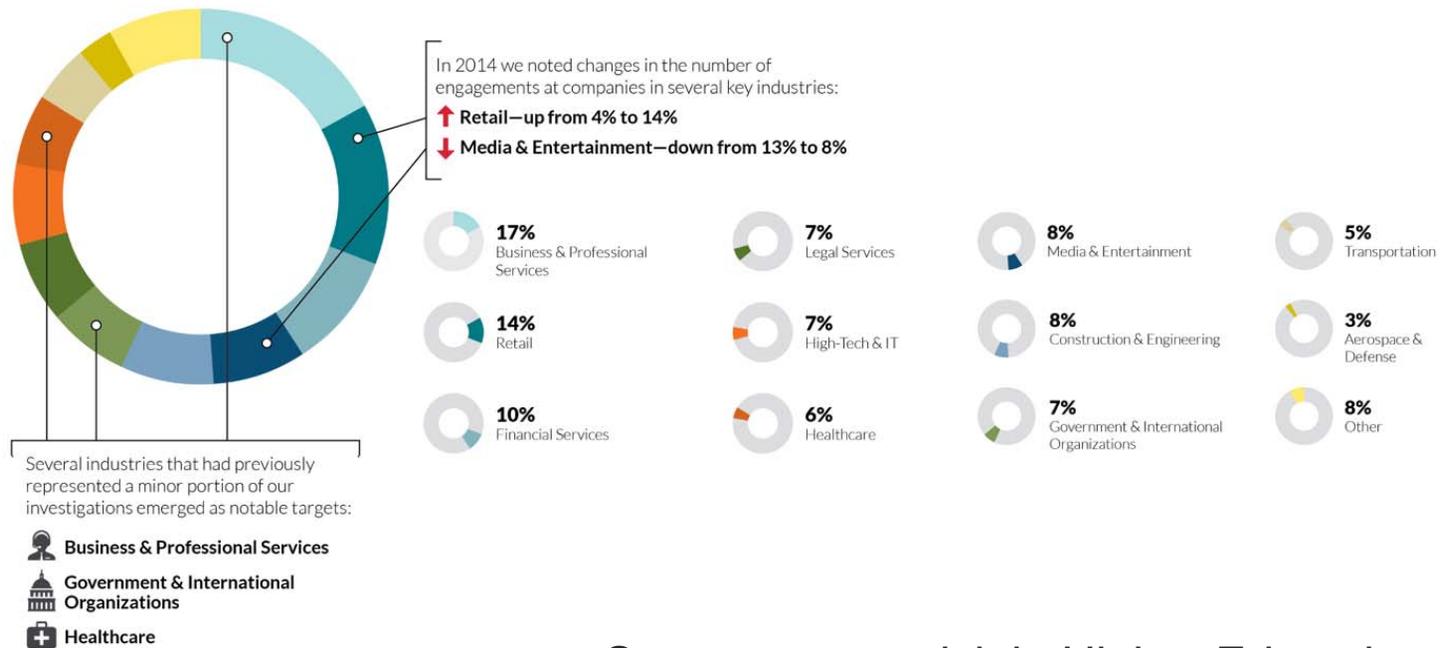
Agenda

- 2014 – By the numbers
- Threat landscape overview
- Attack readiness
- Case study
- Key takeaways/outlook

BY THE NUMBERS

2014

Who's a Target?

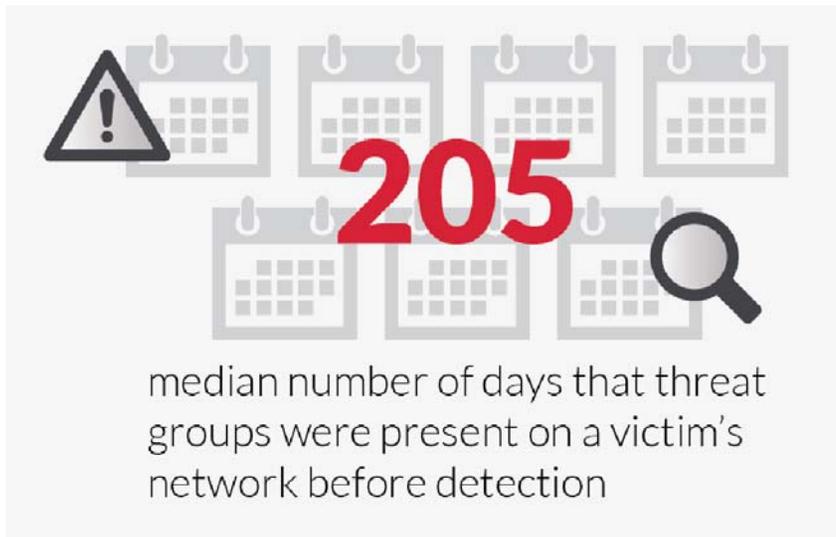


Seen recent uptick in Higher Education

How Compromises Are Being Detected



Dwell Time



↓ 24 days less than 2013

Longest Presence: 2,982 days

APT Phishing



78%

of observed phishing emails were IT or security related, often attempting to impersonate the targeted company's IT department or an anti-virus vendor

72%

of phishing emails were sent on weekdays



THREAT LANDSCAPE

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, PHI, and PII Theft	Website Defacements	Destroy Critical Infrastructure
Targeted					
Character	Automated	Persistent	Financially Motivated	Conspicuous	Conflict Driven

Why Are Targeted Attacks Different?

**It's a "Who,"
Not a "What" ...**

- There's a human at a keyboard
- Highly tailored and customized attacks
- Targeted specifically at you
- Effective at bypassing preventive controls

**They are Professional,
Organized, and Well Funded...**

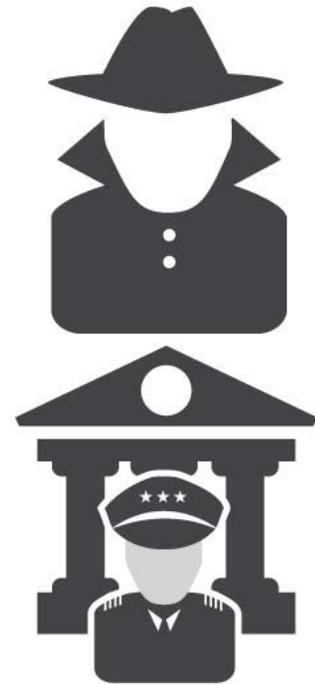
- Can be a nation-state or state-sponsored
- Division of labor for different stages of attack
- Utilize change management processes
- Escalate sophistication of tactics as needed

**If You Kick Them
Out, They Will Return...**

- They have specific objectives
- Their goal is long-term occupation
- Persistence tools ensure ongoing access
- They are relentlessly focused on their objective

Threat Actor Focus

- Cyber criminals
 - Target PII and Financial data
 - Sell information for profit
 - User information for profit
- Advanced Persistent Threats (APT)
 - Target technologies, processes, and expertise
 - Focused on improving domestic industries/abilities
 - More recently targeting PII



ATTACK READINESS

Security Grades by Industry

Industry	Grade Level
Aerospace and Defense	B+
Financial Services	B
High-tech and IT	C+
Retailers	C-
Healthcare	D
Education	F
Government	Depends

Common Observations

- Limited security technology
 - Focus has been more on preventative products (anti-virus, firewalls, etc.)
 - Few detection/response tools
 - Limited understanding of the tools
- Limited security staff
 - Small security teams
 - Often times limited management support
- Reactive security model
 - Very little “hunting” for suspicious activity
 - Immature incident response programs



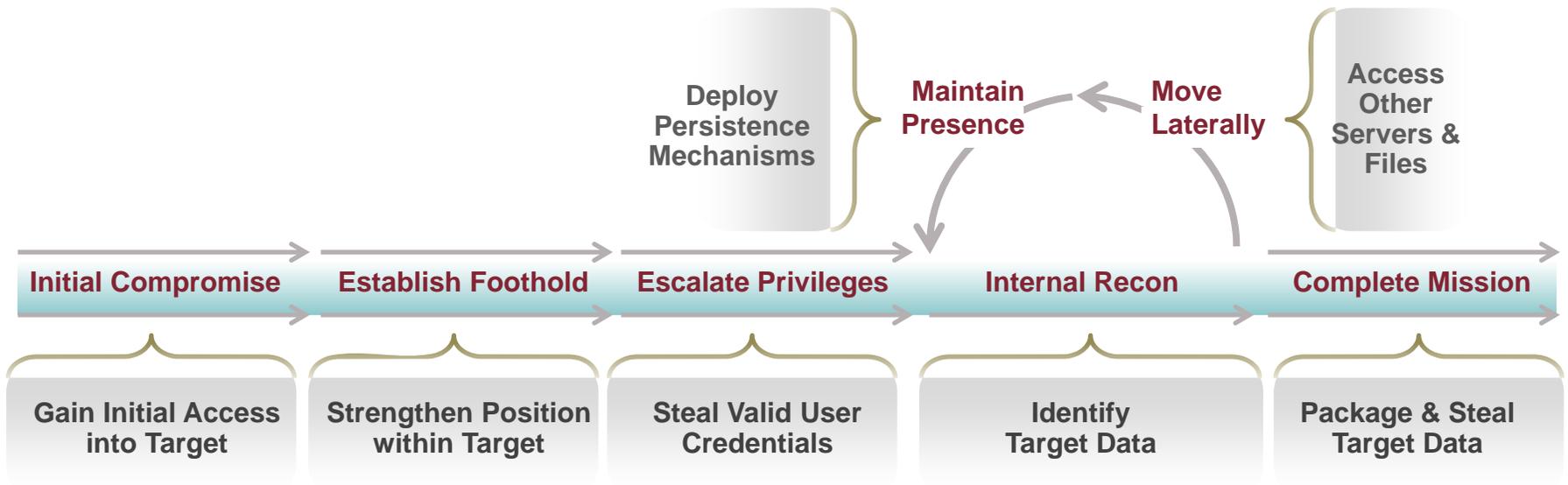
Common Observations

- Historically, security not a priority
 - Starting to improve
- Unique challenges to overcome dependent on industry
 - Peoples' lives at risk
 - Doctors' needs often put first
 - Large remote user base
 - Open Cultures
- Rapid expansion and network interconnectivity
 - Security often an afterthought



ATTACKER TACTICS

Anatomy of Targeted Attacks



Anatomy of Targeted Attacks

- Initial Point of Compromise
 - Vulnerability on external facing servers
 - Single factor remote access (Citrix, VPN, etc)
 - Spear phishing emails to internal users
 - Drive-by downloads
- Establish Foothold / Escalate Privileges
 - Initial focus on installing backdoors
 - Custom backdoors
 - Publically available backdoors
 - Dump passwords on systems
 - Target local admin, domain admin, and database administrator accounts



Anatomy of Targeted Attacks

- Lateral Movement
 - Valid credentials to access additional systems
 - Standard Windows methods
 - RDP, network shares, etc
 - Administrative tools
 - PsExec
- Internal Reconnaissance
 - Network documentation
 - Privileged users
 - Databases containing sensitive data

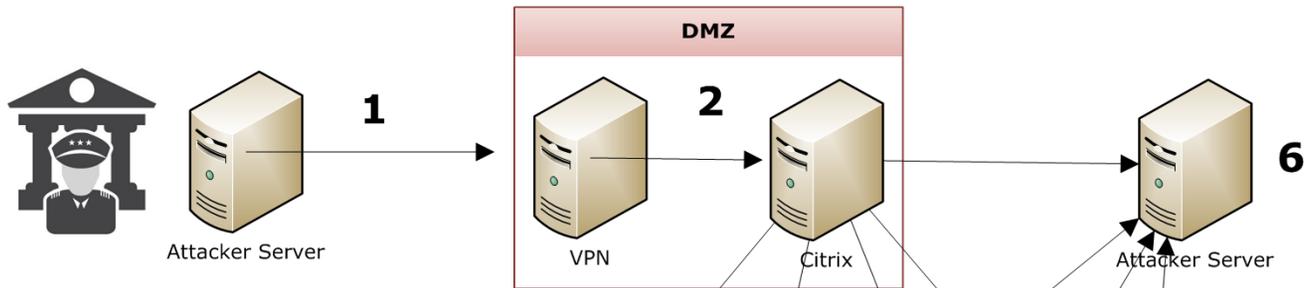


Anatomy of Targeted Attacks

- Maintain persistence
 - Deploy additional backdoors
 - Switch to remote access with legitimate credentials
 - Citrix virtualized environments
 - VPN access
- Complete mission
 - Harvest data
 - Transfer stolen data out of the network



BREACH CASE STUDY



Steps

Step 1: The attacker authenticated to the VPN.

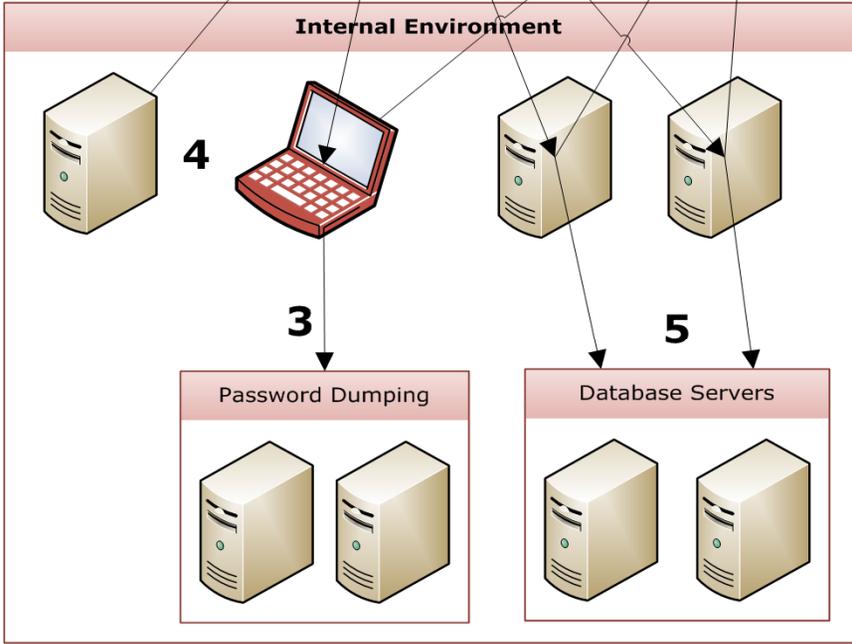
Step 2: The attacker accessed a virtualized Citrix environment.

Step 3: The attacker used a system to dump passwords on over 200 systems.

Step 4: The attacker installed backdoors on six systems.

Step 5: The attacker used two systems to access 75 database servers and harvest PHI data.

Step 6: The attacker transferred files out of the environment to attacker controlled servers.



Damage Assessment

- Attacker was active in the environment for three months
- Compromised approximately 500 systems
 - Only six systems had backdoors
 - Remaining systems related to reconnaissance and data theft
- Obtained password hashes for every user in the environment
- Obtained data for a large number of customers

Post-Containment

- Victim was unable to perform an effective containment strategy due to potential impact to doctors
 - No enterprise wide password reset
 - Could not implement two-factor authentication for remote access
- Attacker authenticated to Citrix using new accounts two weeks after containment event
 - Accessed ~100 systems
 - Dumped passwords from one system

LESSONS LEARNED

Lessons Learned From Breaches

- Identify and secure critical data
 - Data encryption
 - Minimize access
 - Detailed logging and alerting
- Two-factor authentication for external access
 - Token based second factor a must
 - Asset verification
- Network segmentation
 - Reduce the attacker's ability to move throughout the environment

Lessons Learned From Breaches

- Application white-listing on critical systems
 - Domain controllers, email servers, file servers, etc
- Protect privileged accounts
 - Unique passwords for all local administrator accounts
 - Enhanced control over domain administrator accounts and database accounts
- Proactive “hunting” for evidence of compromise
- Enhanced incident response processes
 - Focus on people and processes first
- Implement technology that solves true issues
- Execution trumps strategy

QUESTIONS

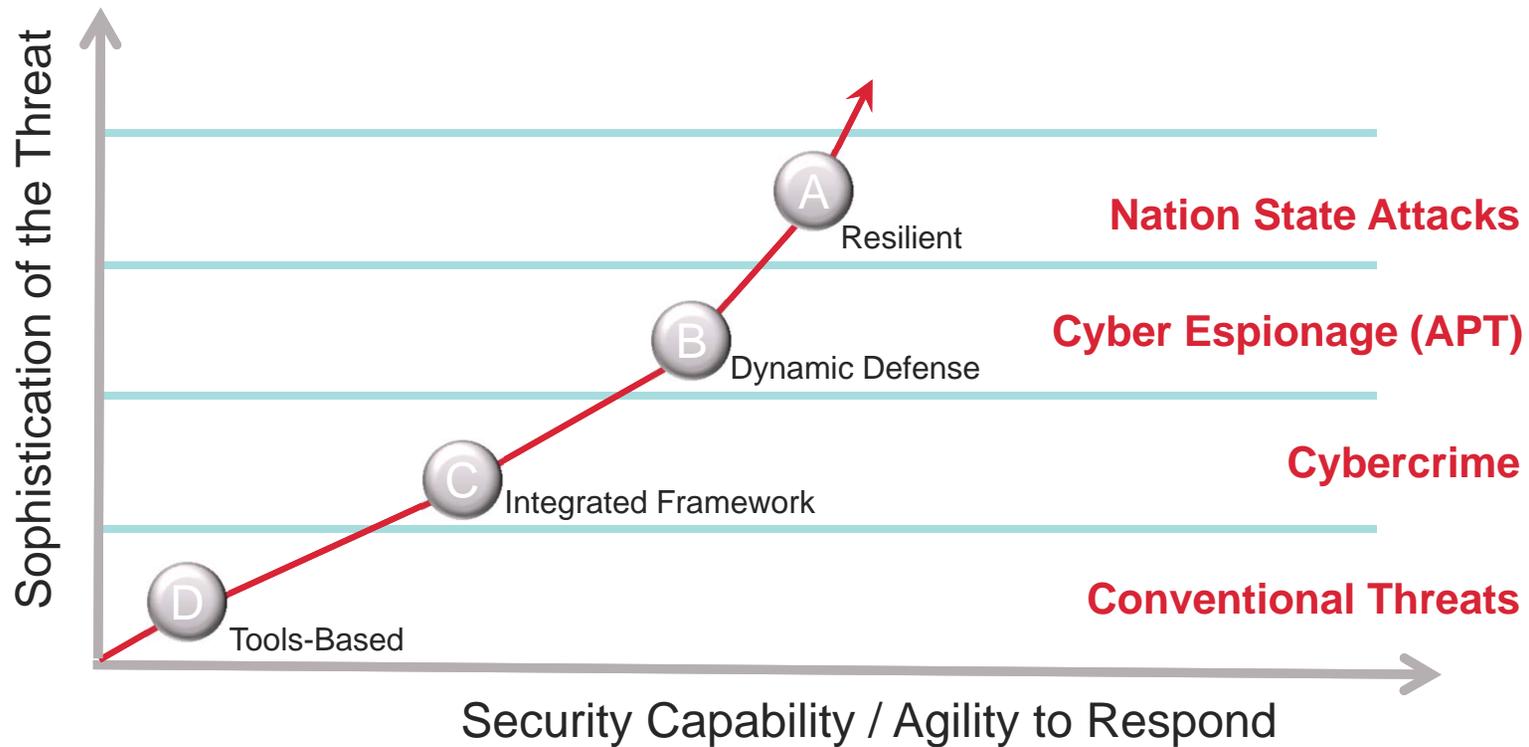
INVESTIGATION LIFECYCLE

Discussions to Have in Advance

- Determine how good you want your cyber security program to be. Fund accordingly.



Discussions to Have in Advance



Discussions to Have in Advance

- Determine how good you want your cyber security program to be. Fund accordingly.
- Assign “One Throat to Choke” for cyber security efforts
- Ensure risk profile aligns with direction set by senior management
- Identify areas for additional help and outside perspective



Rally the Troops

- Where do you need help?
 - Incident Advisors / Investigators
 - Outside Counsel
 - Public Relations
- How much help do you need?
- How quickly can you get help?
 - Secure relationships prior to incident
 - Eliminate negotiations and paperwork during an incident



Limiting the Impact of a Breach

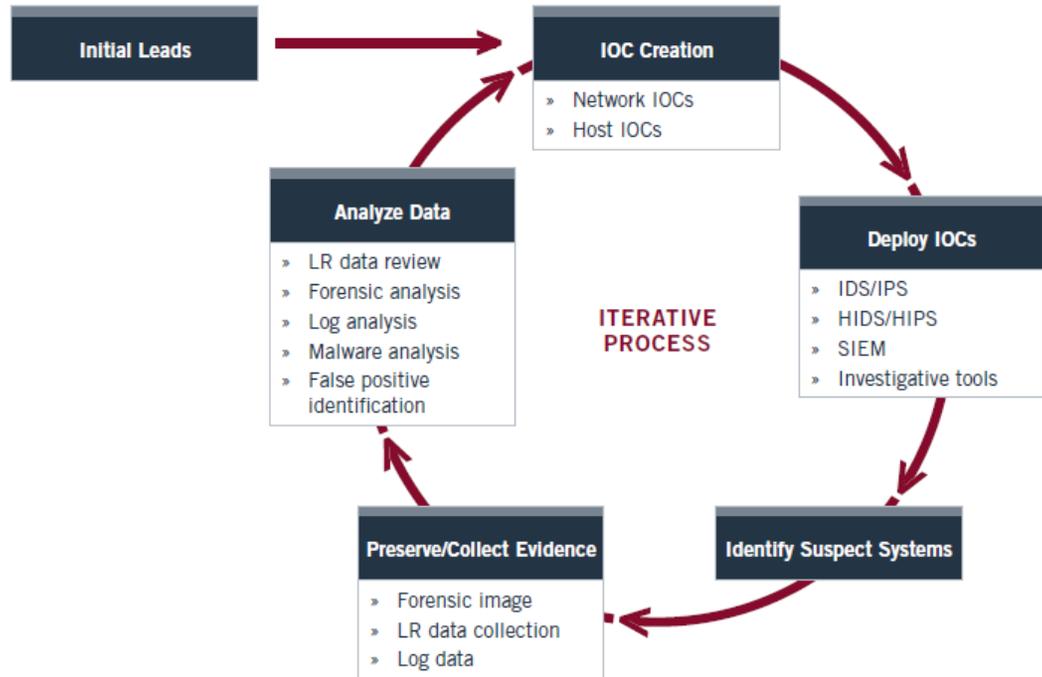
- Educate your people, clients, suppliers, partners about security awareness and attacker profiles / tactics
- Elevate logging and monitoring to gain visibility
- Obtain senior management awareness and support
- Invest in “appropriate practices”
 - Focus on people and process first
 - Implement technology that addresses true issues:
 - Application whitelisting on critical systems
 - Credential management systems
- Recognize that execution trumps strategy



Investigative Approach

Primary Information Sources

- Host inspection (MIR)
- Full network monitoring
- Log analysis (SIEM)
 - Near real-time
 - Historical
- Malware reverse engineering
- System inspection
 - Live response analysis
 - In-depth forensic analysis
 - Memory analysis



Remediation

- Posturing (Pre-remediation)
 - Enhance visibility to aid investigation
 - Increase security controls without affecting the attacker
 - Perform concurrently with the investigation
 - Do not “tip off” attacker
- Remediation
 - Kick the attacker out
 - Execute over a short period of time
 - Remove the attacker and all traces of their intrusion
- Strategic (Long-term)
 - Require significant organizational or architectural alterations



Remediation

Remediating in the Strike Zone

