State of the Hack
Observations from Mandiant Investigations
Background

**Mandiant**
- Based in Washington DC
- Focused on helping organizations recover from security breaches
- Released concrete evidence of hacking by the Chinese PLA
- Significant knowledge of hundreds of threat actors operating across the globe

**Charles Carmakal**
- Managing Director
- Based in Washington DC
- Over 15 years of experience in incident response and ethical hacking

© Mandiant, a FireEye Company. All rights reserved.
Agenda

- Who are the threat actors?
- What are the trends?
- How do we combat advanced attacks?
- Q&A
## Threat Actor Motivations

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance</th>
<th>Data Theft</th>
<th>Cyber Crime</th>
<th>Hacktivism</th>
<th>Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access &amp; Propagation</td>
<td><img src="image" alt="BUY" /></td>
<td>Economic, Political Advantage</td>
<td>Financial Gain</td>
<td>Defamation, Press &amp; Policy</td>
<td>Escalation, Destruction</td>
</tr>
<tr>
<td>Example</td>
<td>Botnets &amp; Spam</td>
<td>Advanced Persistent Threat Groups</td>
<td>Credit Card Theft</td>
<td>Website Defacements</td>
<td>Destroy Infrastructure</td>
</tr>
<tr>
<td>Targeted</td>
<td><img src="image" alt="✗" /></td>
<td><img src="image" alt="✓" /></td>
<td><img src="image" alt="✓" /></td>
<td><img src="image" alt="✓" /></td>
<td><img src="image" alt="✓" /></td>
</tr>
<tr>
<td>Character</td>
<td>Often Automated</td>
<td>Persistent</td>
<td>Frequently Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
</tbody>
</table>
## Threat Actor Motivations

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance</th>
<th>Data Theft</th>
<th>Cyber Crime</th>
<th>Hacktivism</th>
<th>Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
<td>Botnets &amp; Spam</td>
<td>Advanced Persistent Threat Groups</td>
<td>Credit Card Theft</td>
<td>Website Defacements</td>
<td>Destroy Infrastructure</td>
</tr>
<tr>
<td>Targeted</td>
<td>❌</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Character</td>
<td>Often Automated</td>
<td>Persistent</td>
<td>Frequently Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
</tbody>
</table>
THE WORLD TODAY
INDICTMENT OF CHINESE SOLDIERS
US indicts 5 individuals in China’s Unit 61398 for cyber-spying on US firms
Chinese Government Motivations

- The intrusions continue…
- Ongoing attacks to give the Chinese government and domestic enterprises an economic, military, or political advantage
- They are known to compromise entities for the following reasons:
  1. Theft of intellectual property
  2. Mergers, acquisitions, and divestments of foreign companies
  3. Modernization of processes and technologies
  4. Political reasons – political activists, spread of democracy, etc.
- They follow their own rules of engagement.
# Threat Actor Motivations

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance</th>
<th>Data Theft</th>
<th>Cyber Crime</th>
<th>Hacktivism</th>
<th>Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access &amp; Propagation</td>
<td><img src="image1" alt="Image" /></td>
<td><img src="image2" alt="Image" /></td>
<td><img src="image3" alt="Image" /></td>
<td><img src="image4" alt="Image" /></td>
<td><img src="image5" alt="Image" /></td>
</tr>
<tr>
<td>Economic, Political Advantage</td>
<td><img src="image6" alt="Image" /></td>
<td><img src="image7" alt="Image" /></td>
<td><img src="image8" alt="Image" /></td>
<td><img src="image9" alt="Image" /></td>
<td><img src="image10" alt="Image" /></td>
</tr>
<tr>
<td>Financial Gain</td>
<td></td>
<td></td>
<td><img src="image11" alt="Image" /></td>
<td><img src="image12" alt="Image" /></td>
<td>Escalation, Destruction</td>
</tr>
<tr>
<td>Defamation, Press &amp; Policy</td>
<td></td>
<td></td>
<td><img src="image13" alt="Image" /></td>
<td><img src="image14" alt="Image" /></td>
<td></td>
</tr>
<tr>
<td>Escalation, Destruction</td>
<td></td>
<td></td>
<td><img src="image15" alt="Image" /></td>
<td><img src="image16" alt="Image" /></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>Botnets &amp; Spam</th>
<th>Advanced Persistent Threat Groups</th>
<th>Credit Card Theft</th>
<th>Website Defacements</th>
<th>Destroy Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted</td>
<td><img src="image17" alt="Image" /></td>
<td><img src="image18" alt="Image" /></td>
<td><img src="image19" alt="Image" /></td>
<td><img src="image20" alt="Image" /></td>
<td><img src="image21" alt="Image" /></td>
</tr>
<tr>
<td>Character</td>
<td>Often Automated</td>
<td>Persistent</td>
<td>Frequently Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
</tbody>
</table>

© Mandiant, a FireEye Company. All rights reserved.
RUSSIAN ACTIVITY

- **Malware**
  - Evolves and maintains tools for continued long-term use
  - Various data theft techniques

- **Targeting**
  - Georgia and the Caucasus Eastern European governments & militaries
  - Security-related organizations

- **Russian Attributes**
  - Russian language indicators
  - Malware compile times correspond to work day in Moscow’s time zone
POINT OF SALE MALWARE

Ten new POS malware families investigated in 2014

- Backoff POS
- BrutPOS
- Soraya
- Nemanja
- JackPOS
- Decebal
- ChewBacca
- BlackPOS
- Alina
- vSkimmer
## Threat Actor Motivations

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance</th>
<th>Data Theft</th>
<th>Cyber Crime</th>
<th>Hacktivism</th>
<th>Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnets &amp; Spam</td>
<td>Advanced Persistent Threat Groups</td>
<td>Credit Card Theft</td>
<td>Website Defacements</td>
<td>Destroy Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Targeted</td>
<td>❌</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Character</td>
<td>Often Automated</td>
<td>Persistent</td>
<td>Frequently Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
</tbody>
</table>

© Mandiant, a FireEye Company. All rights reserved.
## Threat Actor Motivations

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance</th>
<th>Data Theft</th>
<th>Cyber Crime</th>
<th>Hacktivism</th>
<th>Disruption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Access &amp; Propagation</td>
<td>Economic, Political</td>
<td>Financial Gain</td>
<td>Defamation, Press &amp;</td>
<td>Escalation,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Advantage</td>
<td></td>
<td>Policy</td>
<td>Destruction</td>
</tr>
<tr>
<td>Example</td>
<td>Botnets &amp; Spam</td>
<td>Advanced Persistent</td>
<td>Credit Card Theft</td>
<td>Website Defacements</td>
<td>Destroy Infrastructure</td>
</tr>
<tr>
<td>Targeted</td>
<td>✖</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Character</td>
<td>Often Automated</td>
<td>Persistent</td>
<td>Frequently Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
BY THE NUMBERS
How Compromises Are Being Detected

31% victims discovered the breach internally

69% victims notified by an external entity
Dwell Time

205

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

24 days less than 2013

Longest Presence: 2,982 days
ASSUMPTIONS

- Attacker has domain administrator privileges
- Attacker has hashes or cracked passwords for all domain accounts
- Attacker has additional stolen certificates
- Attacker can freely move
  - VPN to servers
  - VPN to workstations
  - Host to host
- Partner networks may be compromised
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.
STRUGGLING WITH DISCLOSURE
Trend 1: Struggling with Disclosure

- Mandiant worked with over 30 companies that publicly disclosed a compromise
- Many of them learned about the breach from the media.
- The public is asking more informed questions:
  - Attribution
  - Malware
  - Attacker TTPs
- Public speculation starting to affect investigations
Why the Increase in Notifications?

- Mandiant worked an increased number of cases where protected data was lost
  - Cardholder data, Personally identifiable information (PII), and Protected Health Information (PHI)
  - Contractual and legal obligation to notify
- 69% of victims did not self-detect
  - Increased pressure to notify
- More companies willing to notify
  - Companies feel like it’s the right thing to do
  - Being a breach victim is less taboo than in the past
Critical Investigation Questions

- Questions you should have answers to during the investigation
  - How did the attacker gain initial access to the environment?
  - How did the attacker maintain access to the environment?
  - What is the storyline of the attack?
  - What data was stolen from the environment?
  - Have you contained the incident?
The Takeaways

- Breaches are inevitable
  - Have an effective communication strategy available
- Consistent communication is key
  - Based on factual investigative findings
- Public speculation will happen
  - Avoid distracting the investigation
RETAIL IN THE CROSSHAIRS
Trend 2: Retail in the Crosshairs

- Retailers thrust into the spotlight in 2014
- New groups getting into the game
- Small misconfigurations led to greater compromise
Themes of Financial-Motivated Attackers in 2014

- Citrix servers used as an entry point
  - Valid credentials used to authenticate
  - Misconfigurations / lack of network segmentation allowed greater access

- New tools, tactics, and procedures
  - Highly sophisticated malware
  - Publically available tools

- Increased number of attacks against e-commerce in locations that deployed chip-and-PIN technology
  - Attackers shifting focus to lowest hanging fruit
Initial Access To Environment

- Attacker authenticated to a Citrix server
  - Already had legitimate credentials, no failed logons
- Escaped from “jailed” environment to gain additional control over the system
- Misconfiguration in virtual application server resulted in greater access to environment
  - No segmentation
- Same local administrator password on all systems
  - Allowed attacker privileged access to systems
Data Theft

- Attacker used domain controller as pivot point into retail environment
  - The retail domain had a two-way trust with the corporate domain
  - The store registers ran Microsoft Windows XP
  - The store registers were joined to the retail domain
- Deployed card harvesting malware to registers throughout the environment
- Malware wrote stolen track data to temporary MSSQL database
- Attacker queried database to collect stolen track data
- Transferred files off of network using FTP, Citrix, and web servers
THE EVOLVING ATTACK LIFECYCLE
Trend 3: The Evolving Attack Lifecycle

- Threat actors have used stealthy new tactics to move laterally and maintain persistence in victim environments.
**Attack Lifecycle**

Broadcasting Exfiltration

**Hiding Webshells**
Attackers continued to use novel techniques to deploy and hide web-based malware. Mandiant saw several stealthy techniques, including the following:
- Shells planted on servers that used SSL encryption to evade network monitoring
- Single-line “eval” shells embedded in legitimate web pages
- Server configuration files that were modified to load malicious DLLs

**Leveraging WMI and PowerShell**
Attackers increasingly adopted WMI and PowerShell, two powerful built-in components of Windows, to maintain a presence, gather data, and move laterally.

**Hijacking the VPN**
Mandiant witnessed more cases in which attackers successfully gained access to victims’ VPNs than in any prior year.

**Malicious Security Packages**
Attackers took advantage of Windows security package extensibility to load backdoors and password loggers.

**Initial Compromise**

**Establish Foothold**

**Escalate Privileges**

**Internal Recon**

**Complete Mission**

**Plaintext Passwords**
Attackers used recompiled variants of the Mimikatz utility to steal plaintext passwords from memory while evading anti-virus detection.

**Kerberos Attacks**
After gaining domain administrator privileges, attackers used the Kerberos golden ticket attack to authenticate as any privileged account—even after domain password resets.
Hijacking the VPN

- Heartbleed vulnerability
- Single-factor authentication & credential theft
- Bypassing two-factor authentication

Dumping certificates with Mimikatz (Image Source: www.darkoperator.com)
Password Harvesting

“Victims quickly learned that the path from a few infected systems to complete compromise of an Active Directory domain could be incredibly short.”

- Clear-text passwords in memory
- “Golden Ticket” Kerberos attack
- Malicious security packages
COMBATTING TARGETED ATTACKS
Tactical Steps to Reduce the Risk
Effective Ways to Counter Attacks

- Requiring **dual factor authentication** on all remote access (VPN, Citrix, Terminal Services, and webmail)
- Deployment of **application whitelisting technology** to critical assets (domain controllers, mail servers, file servers, etc.)
- **Network compartmentalization** of critical assets and data
- Deployment of **advanced malware detection/prevention** technology at the perimeter (web and email)
- Annual **penetration testing** of environments (internal and external networks, social engineering, and web applications)
- Searching for host and network-based **indicators of compromise** on a periodic basis
- Inventoring **service accounts** and resetting passwords on a periodic basis
- Blocking or requiring “click through” authentication when browsing to **uncategorized websites**
QUESTIONS?

Charles Carmakal
Managing Director
charles.carmakal@mandiant.com
864-735-7242