The New Normal

State of the Threat Landscape

Dave Merkel
Chief Technology Officer, FireEye
Introductions

…and some definitions
What Is Threat Intel?
What is an “APT” group, anyway?

Advanced Persistent Threat actors receive direction and support from a national government. Whether their mission is to steal information or cause disruption or destruction, they pursue their objectives tenaciously using a wide range of tools and tactics.

FireEye tracks 25 China-based APT groups and 1 Russia based
## Breaking Down the Threat

<table>
<thead>
<tr>
<th>Objective</th>
<th>Nuisance</th>
<th>Data Theft</th>
<th>Cyber Crime</th>
<th>Hacktivism</th>
<th>Network Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access &amp; Propagation</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Economic, Political Advantage</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Financial Gain</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Defamation, Press &amp; Policy</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
<tr>
<td>Escalation, Destruction</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
<td>![Icon]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>Botnets &amp; Spam</th>
<th>Advanced Persistent Threat</th>
<th>Credit Card Theft</th>
<th>Website Defacements</th>
<th>Destroy Critical Infrastructure</th>
</tr>
</thead>
</table>

| Targeted                      | ❌             | ✓                          | ✓                 | ✓                    | ✓                             |

<table>
<thead>
<tr>
<th>Character</th>
<th>Automated</th>
<th>Persistent</th>
<th>Opportunistic</th>
<th>Conspicuous</th>
<th>Conflict Driven</th>
</tr>
</thead>
</table>
What the heck is a (an)…

• Advanced attack?
• Exploit?
• Zero Day?
• Malware?
• Backdoor?
• C2 Channel?
• Weaponized document?
• Illudium Q-36 Space Modulator?
Here's a sample of what we found in the first report:

97% of organizations in the study were breached during the test period.

>1/4 More than a fourth of all organizations experienced events consistent with tools and tactics employed by known advanced persistent threat (APT) actors.

>1/week Three-fourths of organizations had active command-and-control communications, indicating that attackers had control of the breached systems and were possibly already receiving data from them.

Even after an organization was breached, attackers attempted to compromise the typical organization more than once per week on average.
Real World, Real Threats – January 2015

- 1189 POV Customers
- 67 Countries
- 20+ Industries
- 96% Customers Compromised
- 27% Had APT
## Data by Region

<table>
<thead>
<tr>
<th>Region</th>
<th>Number of PoV Customers</th>
<th>% PoV</th>
</tr>
</thead>
<tbody>
<tr>
<td>N. AMERICA</td>
<td>477</td>
<td>40%</td>
</tr>
<tr>
<td>EMEA</td>
<td>369</td>
<td>31%</td>
</tr>
<tr>
<td>APAC</td>
<td>252</td>
<td>21%</td>
</tr>
<tr>
<td>JAPAN</td>
<td>53</td>
<td>4.5%</td>
</tr>
<tr>
<td>LATAM</td>
<td>36</td>
<td>3%</td>
</tr>
<tr>
<td>ROW</td>
<td>2</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>
Data by Industry

- Financial: 17%
- Government: 17%
- Chemical & Manufacturing: 7%
- High-Tech: 10%
- Consulting: 8%
- Energy: 6%
- Retail: 5%
- Healthcare: 5%
- Others: 26%
- Other: 5%
Average Attack Seen Per Week

- Exploit: 1 Per Week
- Malware Download: 100 Per Week
- Command and Control: 397 Per Week

377 Impacted Hosts Per Week
How Do We Know This Is Happening?

Source: Mandiant M-Trends 2015

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

- **31%** victims discovered the breach internally

- **69%** victims notified by an external entity

24 days less than 2013

Longest Presence: 2,982 days
The Malware Lifespan: Two Hours

Source: FireEye Labs
67% of malware only exists once.

85% of malware disappears after one hour.
Case Study

Russian Sponsored Cyber Attacks – APT28
APT28 Key Findings

- APT28 targets insider information related to governments, militaries, and security organizations that would likely benefit the Russian government.

- APT28 primarily targets Georgia, Eastern Europe, and European security organizations using skillfully engineered malware that was created during normal working hours in Moscow.
APT28 Primary Targets

GEORGIA

APT28 likely seeks to collect intelligence about Georgia’s security and political dynamics by targeting officials working for the Ministry of Internal Affairs and the Ministry of Defense.

EASTERN EUROPE

APT28 has demonstrated interest in Eastern European governments and security organizations. These victims would provide the Russian government with an ability to predict policymaker intentions and gauge its ability to influence public opinion.

SECURITY ORGANIZATIONS

APT28 appeared to target individuals affiliated with European security organizations and global multilateral institutions. The Russian government has long cited European security organizations like NATO and the OSCE as existential threats, particularly during periods of increased tension in Europe.
## Targeting: European Security Organizations

- NATO
- OSCE

<table>
<thead>
<tr>
<th>APT28 Domain</th>
<th>Real Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>nato.nshq[.]in</td>
<td>NATO Special Operations Headquarters (<a href="http://nshq.nato.int">nshq.nato.int</a>)</td>
</tr>
<tr>
<td>natoexhibitionff14[.]com</td>
<td>NATO Future Forces 2014 Exhibition &amp; Conference (<a href="http://natoexhibition.org">natoexhibition.org</a>)</td>
</tr>
<tr>
<td>login-osce[.]org</td>
<td>Organization for Security and Cooperation in Europe (<a href="http://osce.org">osce.org</a>)</td>
</tr>
</tbody>
</table>
Targeting: Defense Attaches

- UK
- Turkey
- China
- Japan
- South Korea
Russian Indicators...

- Systematically updating malware since 2007
- Family of modular backdoors suggests a formal code development environment
- Group creates flexible and lasting platforms indicative of plans for long-term use
- APT28 tailors implants to specific environments
- Malware contains counter-analysis capabilities
- A significant portion of APT28 malware was compiled in a Russian language build environment consistently over six years
- Compile times parallel working hours in Moscow and St Petersburg
Case Study
Cyber Attacks for Market Manipulation – FIN4
## Key Findings

| 100+ TARGETS | FIN4 knows their targets. Their spear phishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies. | FIN4 does not infect their victims with malware, but instead focuses on capturing usernames and passwords to victims’ email accounts, allowing them to view private email correspondence. | FIN4 uses their knowledge to craft convincing phishing lures, most often sent from other victims’ email accounts and through hijacked email threads. These lures appeal to common investor and shareholder concerns, enticing the intended victims into opening the weaponized document and entering their email credentials. | On multiple occasions, FIN4 has targeted several parties involved in a single business deal, to include law firms, consultants, and the public companies involved in negotiations. They also have mechanisms to organize the data they collect and have taken steps to evade detection. |

Since mid-2013, FIN4 has targeted over 100 organizations, all of which are either publicly traded companies or advisory firms that provide services such as investor relations, legal counsel, and investment banking. Approximately two-thirds of the targeted organizations are healthcare and pharmaceutical companies.
Overview

- Financially-motivated threat group
- Active since at least mid-2013
- Targets confidential business information in emails - likely for use in gaining insider trading advantage
- Members appear to include native English speakers and Wall Street insiders
- Demonstrates familiarity with investment terminology, inner workings of public companies
Intelligence Sources

- Mandiant Incident Response Investigations
- FireEye device detections
- FireEye as a Service (FaaS) detections
- Other research
Targets

TARGETED ORGANIZATIONS:
OVER 100 PUBLICLY TRADED COMPANIES AND ADVISORY FIRMS

Publicly Traded Healthcare and Pharmaceutical Companies
68%

Other Publicly Traded Companies
12%

Firms Advising Public Companies on Securities, Legal and M&A Matters
20%

Figure 1: FIN4's Targets
Operations

Would you fall for it?

- Spear phishing emails sent from other victims’ email accounts, and through hijacked email threads
- Uses weaponized documents to capture credentials via malicious VBA macros; malicious URLs to fake OWA sites
- Difficult to detect because of its simplicity. The actors real skill is social engineering.
Case Study
Syrian Conflict
## Key Findings

<table>
<thead>
<tr>
<th>DATA THEFT</th>
<th>VICTIMS</th>
<th>TACTICS AND TECHNIQUES</th>
<th>MALWARE</th>
<th>POTENTIAL SPONSORSHIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
</tr>
</tbody>
</table>

### Data Theft
The threat group stole hundreds of documents and some 31,107 logged Skype chat sessions that included discussions of plans and logistics of the Syrian opposition’s attacks on Assad’s forces.

### Victims
Targeted individuals included armed opposition members, media activists, humanitarian aid workers, and others. The victims are located in Syria, the region and beyond.

### Tactics and Techniques
The threat actors used female Skype avatars to chat with their targets and infect their devices with malware. “She” typically asked her intended victim if he was using Skype on an Android or a computer, in a likely attempt to send malware tailored to the device. The threat group also maintained a seemingly pro-opposition website containing links to malicious downloads and Facebook profiles with malicious links as well. They conducted these operations using servers located outside of Syria.

### Malware
The threat group employed a diverse malware toolset that implied access to development resources. They used both widely available and custom malware to breach their targets, including the DarkComet RAT, a customized keylogger, and tools with different shellcode payloads.

### Potential Sponsorship
While we have only limited indications about the origins of this threat activity, our research revealed multiple references to Lebanon both in the course of examining the malware and in the avatar’s social media use.
# Stolen Data

<table>
<thead>
<tr>
<th>MILITARY INFORMATION</th>
<th>POLITICAL INFORMATION</th>
<th>HUMANITARIAN ACTIVITIES AND FINANCING</th>
<th>REFUGEE PERSONAL INFORMATION</th>
<th>MEDIA AND COMMUNICATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conversations and documents planning military operations</td>
<td>Political strategy discussions</td>
<td>Humanitarian needs assessments</td>
<td>Applications for assistance by refugees to authorities in Turkey</td>
<td>Documents and strategy information pertaining to media releases</td>
</tr>
<tr>
<td>Details on military hardware and positions of fighting groups</td>
<td>Political tracts, manifestos, and alliances within the opposition</td>
<td>Lists of materials for the construction of major refugee camps</td>
<td>Lists of aid recipients, scans of ID cards</td>
<td>Situation reports and lists of casualties</td>
</tr>
<tr>
<td>Names of members of fighting groups and their weapons systems</td>
<td></td>
<td>Humanitarian financial assistance disbursement records</td>
<td></td>
<td>Information about rights abuses</td>
</tr>
</tbody>
</table>
So What?

- For every good guy, there is a bad guy
- Cyber, it’s not just for the big players
- Mobile is a target
- This is the new normal
Case Study

APT 30
Key Findings

1. 10 Year campaign, same infrastructure, including ability to exploit air-gapped networks
2. Collaborative team environment for creation and maintenance of tools
3. Sophisticated target prioritization and structured shift work
4. Focused on “traditional” sensitive information for government espionage
5. Targets “traditional” for containing information responsive to intelligence collection requirements
## Structured Development Process

<table>
<thead>
<tr>
<th>MD5 Hash</th>
<th>Version</th>
<th>Compile Time</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>b4ae0004094b37a40978ef06f311a75e</td>
<td>1.0.0</td>
<td>4 November 2010 03:51</td>
<td>73,728</td>
</tr>
<tr>
<td>37ae58655f5859e60e6e6e249107b87</td>
<td>1.1.0</td>
<td>25 February 2011 02:03</td>
<td>32,768</td>
</tr>
<tr>
<td>8ff473bedbc77df2c49a91167b1abeb</td>
<td>1.2.0</td>
<td>4 May 2011 14:46</td>
<td>49,152</td>
</tr>
<tr>
<td>4154548e1f8e9e7eb39d48a4cd75bcd1</td>
<td>1.2.0</td>
<td>4 May 2011 14:46</td>
<td>17,408</td>
</tr>
<tr>
<td>15304d20221a26a0e413fba4c5729645</td>
<td>1.2.0</td>
<td>16 May 2011 11:03</td>
<td>36,864</td>
</tr>
<tr>
<td>c4dec6d69d8035d81e4f2c86f580e81</td>
<td>1.3.0</td>
<td>26 October 2011 11:21</td>
<td>40,960</td>
</tr>
<tr>
<td>a813eba27b2166620bd75029cc1f04b0</td>
<td>1.3.0</td>
<td>28 June 2012 10:01</td>
<td>86,144</td>
</tr>
<tr>
<td>5b2b07a86c6982789d1d85a78ebd6c54</td>
<td>1.5.10</td>
<td>8 January 2013 01:33</td>
<td>10,518,528</td>
</tr>
<tr>
<td>71f25831681c19ea17b2f2a84a41bbfb</td>
<td>1.6.10</td>
<td>23 April 2013 08:12</td>
<td>57,344</td>
</tr>
<tr>
<td>6ee35da59f92f717e757d4d5b964ecf00</td>
<td>1.9.10</td>
<td>28 August 2014 09:12</td>
<td>57,344</td>
</tr>
</tbody>
</table>
Targeted Regions

Countries with Confirmed APT 30 Targets
- India
- Thailand
- South Korea
- Saudi Arabia
- Malaysia
- United States
- Vietnam

Countries with Likely APT30 Targets
- Nepal
- Indonesia
- Cambodia
- Bhutan
- Brunei
- Japan
- Philippines
- Myanmar
- Singapore
- Laos
Takeaways
OK, so this is kind of obvious…

- Bad guys aren’t going anywhere
- For every good guy, there is a bad guy
- The scope and pace of this activity continues to increase
- A note on destructive attacks
- All is not lost! However…
THE END