Achievement Unlocked

Chinese Cyber Espionage Evolves to Support Higher Level Missions

Nalani Fraser and Kelli Vanderlee
Redline Drawn

- Decline in Chinese cyber espionage activity beginning in mid 2014

- Observed Chinese cyber threat activity from 2013-2015
  - High volume
  - Majority in US
  - IP theft
Chinese Cyber Espionage in 2019 is Significantly Different

- Tempo
- Active Groups
- Geographic focus
- Industries targeted most frequently
- TTPs
- Goals
Chinese Domestic Context

- Growing, aging, urbanizing population
- Slowing economic growth
  - Made in China 2025
  - Belt and Road Initiative (BRI)
Belt and Road Initiative
Chinese Military Restructuring Timeline

- **Early 2014**: PLA reform discussions
- **September 2015**: Official announcement at military parade in Beijing
- **December 2015**: SSF establishment ceremony
- **February 2016**: Chinese Military Commission officially replaced the military region system
- **April 2017**: Even further reorganization; entire PLA was streamlined
Restructuring of Cyber Forces
Former People’s Liberation Army (PLA)

- PLA, General Staff Department’s (GSD) 3rd department
  - 12 operational bureaus, each with distinct mission

- APT1 (2nd Bureau; MUCD Unit 61398)
  - Political, economic, military intelligence
  - Feb 2013: Mandiant report
  - Early 2015: Last known activity

- APT2 (reportedly 12th Bureau; Unit 61486)
  - Satellite communications and space-related surveillance
  - Early 2014: Last known activity
Technical Reconnaissance Bureaus (TRBs)

- Under the former PLA, each service/military region maintained its own TRB
  - Responsible for signals intelligence & cyber espionage

- Unclear how the TRBs have been incorporated into the SSF
  - Indications that they have been transferred into the SSF?

- Naikon Team (suspected Unit 78020)
  - Government and military targeting in ASEAN countries
  - Late 2016: suspected Naikon Team observed with ASEAN lure doc
TRB Incorporation?

- Tonto Team (possibly Unit 65017)
  - Shenyang Military Region Technical Reconnaissance Bureau
  - Targeting of South Korea, Russia, and Japan

- Suspected Tonto with same targeting pattern:
  - Early 2016: suspected Tonto targeting South Korea
  - Mid 2017: suspected Tonto targeting Russia
    - (possible pause in activity)
  - Early 2018: suspected Tonto targeting South Korea
## Ministry of State Security (MSS)

- Responsible for domestic counter-intelligence, non-military intelligence, political / diplomatic security
- Reportedly has taken on more robust role. Possible MSS reorganization in 2018.

<table>
<thead>
<tr>
<th>APT3</th>
<th>APT10</th>
<th>APT26</th>
</tr>
</thead>
</table>
| **Boyusec, an MSS contractor**  
  Stole satellite mobile device technology  
  Nov 2017:  
  US DOJ indicted 3 members  
  De-registered website  
  Last observed activity | **Huaying Haitai Science and Technology Development Company, associated with MSS**  
  Oct 2018: last observed activity  
  Dec 2018: US DOJ indicted 2 members | **Associated with the Jiangsu Ministry of State Security (JSSD), foreign intelligence arm of MSS**  
  Mid 2017: last observed  
  Oct 2018: US DOJ indicted 2 members  
  Conspiring to steal aviation technology |
Sept 2015: Official announcement of SSF

PLA reform discussions

ACTIVE NETWORK COMPROMISES CONDUCTED BY CHINA BASED GROUPS BY MONTH
February 2013-June 2019
Threat Groups: Who is Most Active?

<table>
<thead>
<tr>
<th>TOP TARGETED CHINESE THREAT GROUP ACTIVITY (2016-2019)</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT41</td>
</tr>
<tr>
<td>APT40 (Periscope)</td>
</tr>
<tr>
<td>APT10 (Menupass)</td>
</tr>
<tr>
<td>APT19 (Codoso)</td>
</tr>
<tr>
<td>Group using TOYSNAKE</td>
</tr>
<tr>
<td>Group using DOORJAM/WARP</td>
</tr>
<tr>
<td>Group targeting Mongolian orgs</td>
</tr>
<tr>
<td>APT12 (Calc)</td>
</tr>
<tr>
<td>Tonto Team</td>
</tr>
<tr>
<td>ASEAN related targeting</td>
</tr>
</tbody>
</table>
Geographic Focus

- Observed cyber threat activity focused in Asia Pacific
- Most frequently targeted countries:
  1. United States
  2. South Korea
  3. Hong Kong
  4. Germany
  5. Japan
  6. India
  7. Taiwan
Industries Most Frequently Targeted

1. Telecommunications
2. Government
3. High Tech
4. Media & Entertainment
Telecommunications Targeting

- Targeting observed across the telecommunications ecosystem
- SMS and call record data exfiltrated
- Increased operational maturity
Primary motivation: maintain regional supremacy

Secondary motivation: Chinese economic ambitions (BRI)

FireEye anticipates more aggressive efforts to influence public opinion in the future
Asia Pacific

- Prominent actors, campaigns:
  - APT41
  - Mongolian targeting
  - ASEAN targeting

Observed Chinese Activity in the Asia Pacific, Jan 2016-Aug 2019

- East Asia
- Southeast Asia
- South Asia
- Oceania
- Central Asia

Top 5 Sectors Targeted by Chinese Activity in the Asia Pacific, Jan 2016-Aug 2019

- Government
- Telecommunications
- Media and Entertainment
- High Tech
- Transportation
Europe

Prominent actors:
- APT10
- APT41
- APT40

Observed Chinese Activity in Europe, Jan 2016-Aug 2019

Top 5 Sectors Affected by Chinese Activity in Europe, Jan 2016 - Aug 2019

- Chemicals and Materials
- Retail
- Government
- Telecommunications
- Legal and Professional Services
Americas

- 3rd party compromise
- Military and dual use IP
- PII collection
- Prominent actors, campaigns:
  - APT19
  - DOORJAM / WARP phishing campaign
  - APT40
  - APT41
TTPs: Shifts in Use of Public Malware

- Use of Poison Ivy declined
- Use of Chinese specific malware declined
- Shift towards more broadly used malware
### TTPs: Malware Platform Compatibility

<table>
<thead>
<tr>
<th>Windows / Linux</th>
<th>Windows / Mac OS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2011-2015</strong></td>
<td><strong>2015-2019</strong></td>
</tr>
<tr>
<td>• ASPXSPY (public webshell)</td>
<td>• TERA (backdoor)</td>
</tr>
<tr>
<td>• MIMIKATZ (public credtheft)</td>
<td>• NETWIRE (public backdoor)</td>
</tr>
<tr>
<td>• CMDSOCKS (tunneler)</td>
<td>• ICEFOX.OSX (backdoor - available on forums)</td>
</tr>
<tr>
<td>• PHOTO (backdoor)</td>
<td>• CAKECLOG (tunneler)</td>
</tr>
<tr>
<td>• MESSAGETAP (dataminer)</td>
<td>• TERA (backdoor)</td>
</tr>
<tr>
<td>• PHOTO (backdoor)</td>
<td></td>
</tr>
<tr>
<td>• QUICKFLOOD (disruption)</td>
<td></td>
</tr>
<tr>
<td>• CAKECLOG (tunneler)</td>
<td></td>
</tr>
</tbody>
</table>

- Use of malware with multi-platform capabilities increased
- Some of this is due to use of publicly available tools
Rise in modular malware cases, mostly attributed to APT41

Other actors consistent:
- APT10, dissident targeting in South East Asia
TTPs: Malware Executed in Memory

- “Fileless persistence”
- Malware runs in memory and is not saved to disk
- Evades antivirus

### Chinese Espionage Memory-Only Malware Incidents

<table>
<thead>
<tr>
<th>Year</th>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-2015</td>
<td>HIGHNOON</td>
</tr>
<tr>
<td></td>
<td>ROCKETSHP</td>
</tr>
<tr>
<td></td>
<td>HELLWOOD</td>
</tr>
<tr>
<td></td>
<td>TOWTRUCK</td>
</tr>
<tr>
<td></td>
<td>SAFERSING</td>
</tr>
<tr>
<td></td>
<td>COMBATBOOT</td>
</tr>
<tr>
<td></td>
<td>LOSTCAUSE</td>
</tr>
<tr>
<td></td>
<td>QUICKBALL</td>
</tr>
<tr>
<td></td>
<td>UPCONTROL</td>
</tr>
<tr>
<td>2015-2019</td>
<td>TOWTRUCK</td>
</tr>
<tr>
<td></td>
<td>RABBITPUNCH</td>
</tr>
<tr>
<td></td>
<td>FRONTSHELL</td>
</tr>
<tr>
<td></td>
<td>FOCUSFJORD</td>
</tr>
<tr>
<td></td>
<td>EVORA</td>
</tr>
<tr>
<td></td>
<td>Poison Ivy</td>
</tr>
<tr>
<td></td>
<td>TSCOOKIE</td>
</tr>
<tr>
<td></td>
<td>LITRECOLA</td>
</tr>
</tbody>
</table>

©2019 FireEye
TTPs: Confirmed Initial Infection Vectors

- Continued reliance on spear-phishing
- Decrease in 0-day use
In June 2018, a utility to update ASUS computers was compromised

- Kaspersky reported more than 50,000 systems installed the malicious update

Guardrail #1:

- Utilized MAC address whitelisting to limit download & execution of 2nd stage malware (APT41 POISONPLUG)

Guard rail #2:

- POISONPLUG sample matches C: drive volume serial number to limit execution to 1 system

Google Docs (embedded C&C command)
Goals: Data Theft

- PII was the most commonly observed type of data stolen
- IT data was stolen as well
- Military application IP theft continues
- No direct evidence of theft of IP with purely commercial applications
IP Theft by Other Means?

- APT26 and Insiders (2010-2015)

Risks to Foreign Business Operations in China:

- Reviewing Hardware & Software
- Limiting VPNs
- Censoring Content
- Influencing Corporate Leadership
- Remote & In-Person Access
- Data Acquisition & Information Sharing
- Weak Protection Clauses
Chinese Cyber Espionage in 2019

- Tempo: normalizing
- Active Groups: APT41, APT40, APT19, new activity sets
- Geographic focus: Asia, but still globally diverse
- Industries targeted most frequently: Telecommunications
- TTPs: stealthy, more sophisticated
- Goals: aligned with top state political and defense priorities
Technologies in Development Hint at Future Capabilities

Mapping Technology Advancements Against Stages in the Intelligence Lifecycle:

**PLANNING:**
- Data Science & Machine Learning
  - Facilitates pattern recognition to improve tradecraft techniques identifying foreign individuals for social engineering or intelligence recruitment

**COLLECTIONS:**
- 5G
  - Vulnerabilities can potentially be built into Chinese 5G products to allow state-sponsored cyber espionage actors to eavesdrop, steal information, and conduct network exploitation at a later date
  - Increased speed and capacity; less latency, expands potential capabilities to capture large quantities of data
  - Increased connectivity of more devices

**ANALYSIS & EXPLOITATION:**
- Quantum Computing, Data Science, & Machine Learning
  - Quantum Computing: Could increase cyber espionage actor's ability to decrypt intercepted or stolen data protected with encryption
  - Data Science & Machine Learning: Improved data access and analysis allows Chinese analytical intelligence services to operationalize collected information with greater speed and efficiency
  - Improved data access and analysis allows traditional espionage actors to operationalize collected information with greater speed and efficiency

**INTELLIGENCE TRADECRAFT:**
- Quantum Computing could increase the integrity of secure Chinese communication networks
Questions?