Advanced Persistent Threats

Jill Sopko, Senior Security Researcher
Who Am I?

• 15 years in DOD, US Intelligence
  – Left in 2017
• Bachelors degree in Political Science (National Security Policy)
• Master of Business Administration
• Master of Science in Homeland Security
• Currently a Sr Security Research at NetScout
Definition of APT

• Advanced
  – Not necessarily sophisticated
  – “Advanced” speaks to the resources available to the Actors ($)

• Persistent
  – Actors have available time
  – Actors have other tools

• Threat
  – Nations & States (China, Russia, Iran, DPRK)
  – Hacktivists (Anonymous, WikiLeaks, LulzSec)
  – Criminal Organizations (Spider Groups)
  – For-Profit Actors (FIN groups)
  – Terrorists (ISIL)
Overview of APT Motivations

- Intellectual Property Theft: Generally economic in nature
- Intelligence Gathering—Operational: Military advantage
- Intelligence Gathering—Strategic: Upper hand in negotiations
- Profit: Want to make money (may be sanctioned, or not)
- Ideology: Fighting for/against a cause
- Destruction: Want to burn it all down
- Power Projection: Sends a political message
China: Planned Advancement

- Intelligence Gathering & Intellectual Property Theft
- Individual Targets:
  - Governments / Diplomats / Military
  - Corporations esp. Defense Contractors
  - Universities / R&D / Centers of Excellence
- Technology Targets:
  - Aviation
  - Internet Connectivity
  - Energy / Petrochem
  - Next Gen Tech
  - Agriculture
South China Sea: Islands VS Rocks

Credit: Katie Park / NPR
India and Pakistan

INDIA
- Near Abroad
  - Pakistan
  - China
  - Sri Lanka
  - Myanmar
  - Bangladesh
  - United States
- Nuclear & Missile Technology
- Telecom & IT Technology
- Oil & Gas
- Activists within India
- Embassies around the world

PAKISTAN
- Near Abroad
  - Pakistan
  - China
  - United States
  - Occasionally the Middle East
- Nuclear & Missile Technology
- Transportation & Logistics
- Embassies around the world
- Internal dissent
Tension in South Asia
Iran: In Depth

Joint Comprehensive Plan of Action (JCPOA)
Iran: A Tail of Many Kittens

- OilRig
- Mabna Institute/Silent Librarian
- Charming Kittens
- Domestic Kittens

U.S. RQ-170 SENTINEL
- Aircraft type: Low observable, unmanned aircraft system (UAS)
- Operating altitude: 15,940 m
- Material: Composite
- Manufacturer: Lockheed Martin

Ali Khamenei in 2017

7th President of Iran
Post-Soviet Region: Geopolitical Positioning

- Intelligence Gathering
- Extension of Kinetic War
- Control of Former USSR Nations
- Influence Adversary States
- Silence Activists and Dissidents

5 Stages of Election Meddling
1. Amplify suspicions and divisions
2. Steal sensitive data
3. Leak stolen data via ‘hacktivists’
4. Whitewash leaked data via professional media
5. Secret collusion between a candidate and foreign state to synchronize election efforts

Finish Institute of International Affairs, 2017
Russian Disinformation Campaign

EUvsDisinfo.eu

Criminals commit less crime after they have been shot! That’s why I say #BlueLives Matter

"F*ck this flag. F*ck this country!" #BLM were shouting at "peaceful" protests to Trump’s rally in Wisconsin
North Korea Overview

- Power Projection: Destructive attack on Sony, South Korean banks and media outlets
- Revenue Generation: Feb 2016 cyber theft of $81M from the Bangladeshi central bank account at the Federal Reserve in New York
- Intellectual Property: Defense, missile tech, bio-med engineering (See Stolen Pencils)
- Intelligence: Dec 2016, South Korean military cyber command
DPRK & Software Revenue

- Apps & Games = Revenue Generation
- Appropriation of content
- Likely IP theft
What to do?

1. 2-Factor is better than 1-Factor
2. Keep passwords long and strong, but useable
3. PATCH & UPDATE
4. Watch your IoT, BYOD
5. Access controls
6. Train them, then test them
7. Consider insider threats
8. Sharing is caring
9. Physical security
10. Collect, Monitor, & Plan
Thank You.

Jill Sopko
jsopko@netscout.com