Cyber@UC Meeting 68

Advanced Persistent Threats

If You’re New!

- Join our Slack: cyberatuc.slack.com **(URL changed!)**
- **SIGN IN!** *(Slackbot will post the link in #general every Wed@6:30)*
- Feel free to get involved with one of our committees:

  Content *Finance* *Public Affairs* *Outreach* *Recruitment*
- Ongoing Projects:
  - Research lab!

Announcements

- **September 18th** NSA visit with an **Enigma Machine**
  - Deli Food!
  - Vicki Baker Will talk about NSA Scholarships
- **US Bank visit** *Friday Sept 28th 2pm*
- **Rockwell Security Seminar**
  - September 20th 9am-3pm
  - Nippert Stadium

Public Affairs

Useful videos and weekly livestreams on **YouTube**:

youtube.com/channel/UCWcJuk7A_1nDj4m-cHWvIFw

Follow us for club updates and cybersecurity news:

- **Twitter:** @CyberAtUC
- **Facebook:** @CyberAtUC
- **Instagram:** @CyberAtUC

For more info: cyberatuc.org

Weekly Content

Mobile Spyware Developer mSpy leak

- Develops SaaS that claims to help customers spy on kid’s and partner’s phones
- Leaked millions of sensitive records:
  - Passwords, call logs, sms, contacts, notes, username, private key, and location data
- < 2 weeks ago there was an online database that allowed up to the minute querying of mSpy records for customer transactions and collected data
  - No authentication required
- This is not the first time mSpy has been breached

U.S. charges North Korean over WannaCry

- Park Jin Hyok has been charged, works for North Korean Military Intelligence Agency Reconnaissance General Bureau (RGB)
- Also known as Pak Jin Hek, linked to Lazarus Group
    - Lazarus is tied to WannaCry and an attempt to steal 1 Billion $ from Bangladesh Bank
- First time we have announced a suspect in a North Korean hack
    - Remember the Sony hack

Tor Zero-day

- Tor Browser zero-day could reveal your identity and site history
- Shared by Zerodium, an infamous exploit vendor, acquire zero-days and then report them to clients with countermeasures
- Offered $1 million for zero-day in Tor Browser earlier this year
- Vulnerability in NoScript plugin pre-installed in Firefox bundled with the Tor software
- NoScript is a free extension meant to block malicious JavaScript, Java, Flash, etc.
- Changing a content-type header to JSON allows the running of any JavaScript on a victim
- Tor 8.0 is patched

Recommended Reading

https://thehackernews.com/2018/09/cohan-hoax-bomb-threats.html

https://krebsonsecurity.com/2018/09/leader-of-ddos-for-hire-gang-pleads-guilty-to-bomb-threats/

https://www.welivesecurity.com/2018/09/07/british-airways-card-details-stolen/

https://thehackernews.com/2018/09/british-airways-data-breach.html

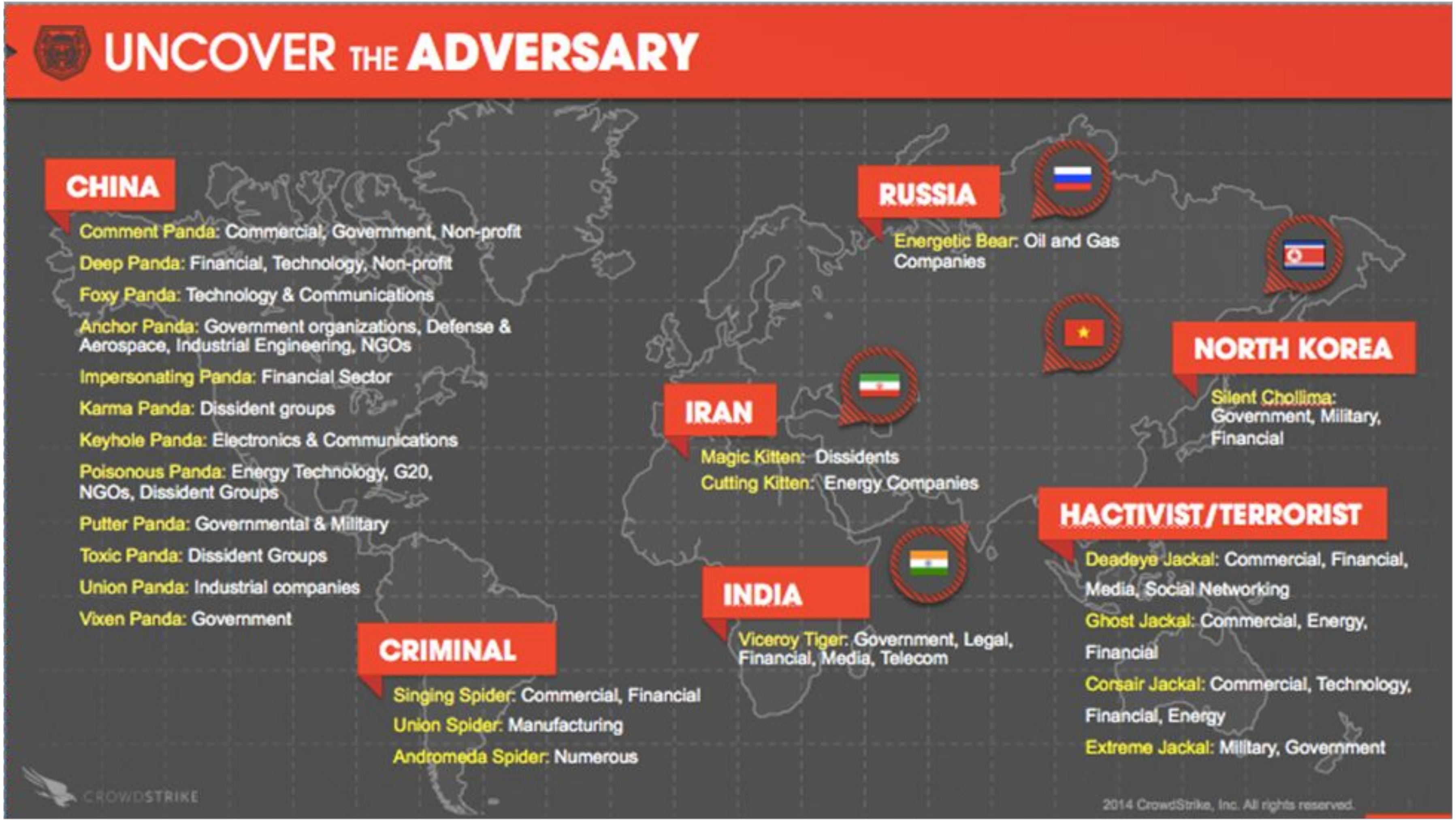
https://www.welivesecurity.com/2018/09/10/apple-top-grossing-app-mac-app-store-grabbing-private-user-data/

https://thehackernews.com/2018/09/mac-adware-removal[illegible]ml

APT

What is an APT?

- Advanced Persistent Threat
- Stealthy, persistent hacker group
  - Often larger or more advanced the other hackers
  - More likely to make use of zero day exploits
- Have an agenda/target
- Often refers to government sponsored groups
- Common Targets:
  - Governments
  - Corporations
  - Financial Institutions



UNCOVER THE ADVERSARY

CHINA

- **Comment Panda:** Commercial, Government, Non-profit
- **Deep Panda:** Financial, Technology, Non-profit
- **Foxy Panda:** Technology & Communications
- **Anchor Panda:** Government organizations, Defense & Aerospace, Industrial Engineering, NGOs
- **Impersonating Panda:** Financial Sector
- **Karma Panda:** Dissident groups
- **Keyhole Panda:** Electronics & Communications
- **Poisonous Panda:** Energy Technology, G20, NGOs, Dissident Groups
- **Putter Panda:** Governmental & Military
- **Toxic Panda:** Dissident Groups
- **Union Panda:** Industrial companies
- **Vixen Panda:** Government

CRIMINAL

- **Singing Spider:** Commercial, Financial
- **Union Spider:** Manufacturing
- **Andromeda Spider:** Numerous

RUSSIA

- **Energetic Bear:** Oil and Gas Companies

IRAN

- **Magic Kitten:** Dissidents
- **Cutting Kitten:** Energy Companies

INDIA

- **Viceroy Tiger:** Government, Legal, Financial, Media, Telecom

NORTH KOREA

- **Silent Chollima:** Government, Military, Financial

HACTIVIST/TERRORIST

- **Deadeye Jackal:** Commercial, Financial, Media, Social Networking
- **Ghost Jackal:** Commercial, Energy, Financial
- **Corsair Jackal:** Commercial, Technology, Financial, Energy
- **Extreme Jackal:** Military, Government

CROWDSTRIKE

Breakout Session

- Break into groups
- Each group gets a copy of summarized reports
- Look for trends/similarities and any other standout information
- Look into and discuss those points as a group
- Put together a list of those things
- Reconvene and discuss findings