RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

The Art of Attribution
Identifying and Pursuing your Cyber Adversaries

SESSION ID: ANF-T07B

Dmitri Alperovitch
CrowdStrike, Co-Founder & CTO

ABOUT ME

- Dmitri Alperovitch
  - Co-Founder & CTO, CrowdStrike
  - Former VP Threat Research, McAfee
  - Author of Operation Aurora, Night Dragon, Shady RAT
  - MIT Tech Review's Top 35 Innovator Under 35 for 2013
  - Foreign Policy's Top 100 Leading Global Thinkers for 2013
  - Twitter: @DmitriCyber

CROWDSTRIKE

ORGANIZATIONS
BELIEVE THEY HAVE

A MALWARE PROBLEM

ORGANIZATIONS BELIEVETHEY HAVE

AN ADVERSARY PROBLEM

Importance of Attribution

Executive Briefing

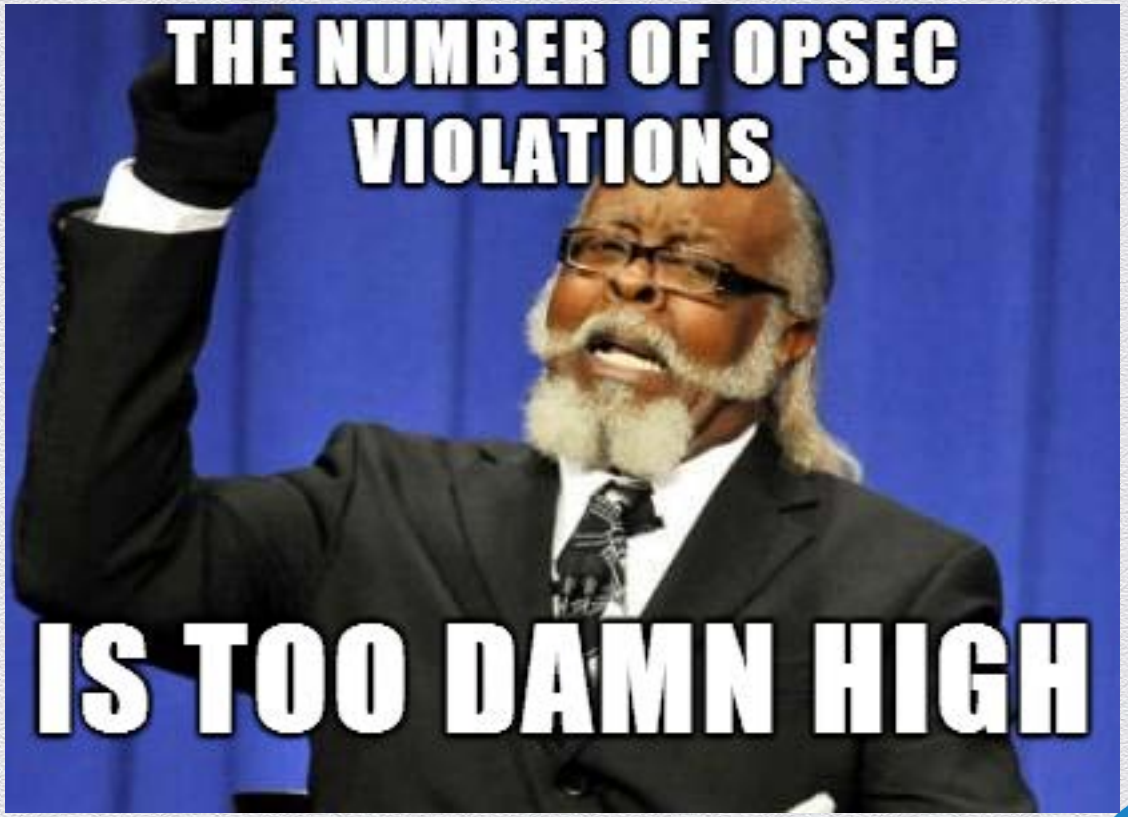
- Attribution: PLA Navy
- Targets:
  - Governments
  - Military / Defense
  - Intelligence
  - NGO
  - Oil
  - Green Energy
  - Shipping

EYES ONLY

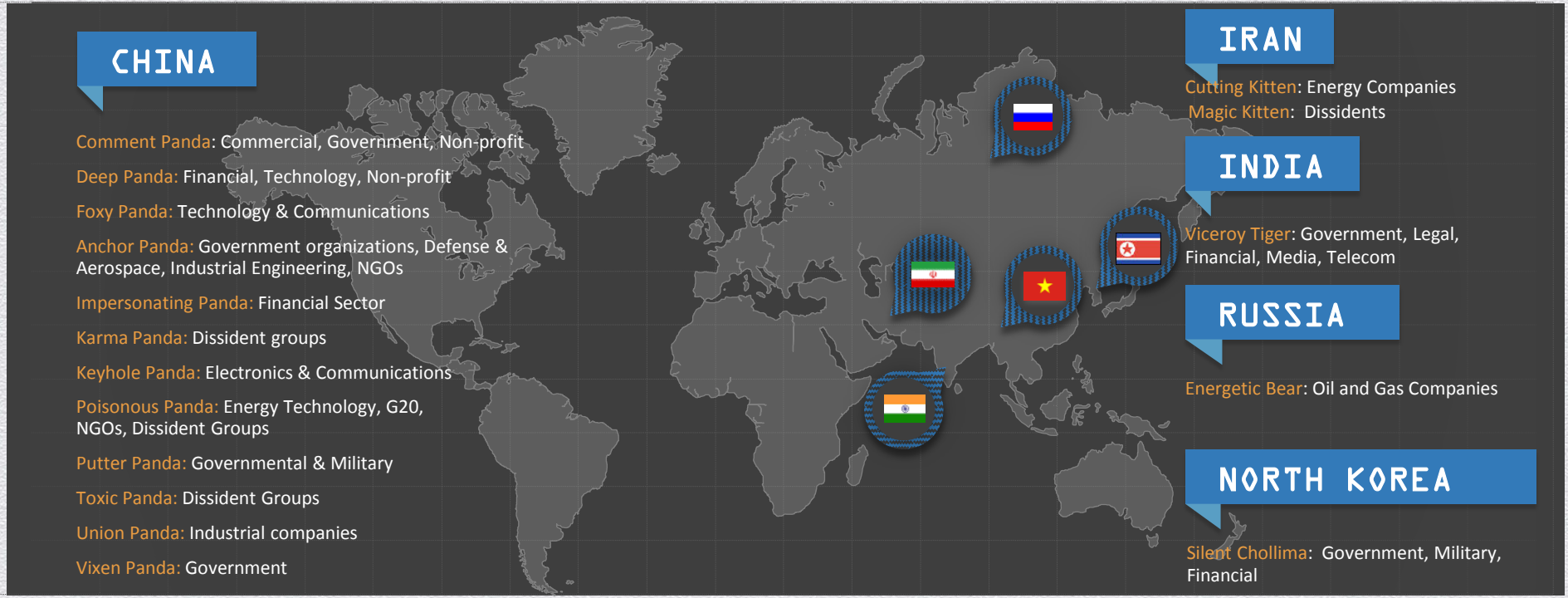

I'M FROM THE GOVERNMENT
AND I'M HERE TO HELP

Attribution is Impossible in Cyberspace

Attribution Paradox



Who are the Adversaries



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

IRAN

Cutting Kitten: Energy Companies

Magic Kitten: Dissidents

INDIA

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

RUSSIA

Energetic Bear: Oil and Gas Companies

NORTH KOREA

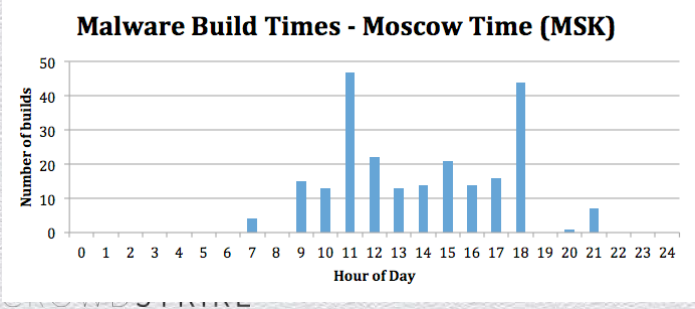
Silent Chollima: Government, Military, Financial

Who are the Adversaries

Who are the Adversaries

Attribution Indicators

- “Human Toolmarks”
- Resource Language
- Timezone information
  - Build times
  - C2 check-in times
  - Mutex names
  - Kernel pool tags
- Tradecraft
- Passwords
- Indicators
- Domain Registration
- IP Ownership
- Code Styles



Conclusion

- Predictive security requires intelligence & attribution
- Know Thy Enemy
- Tailor defense to attacker's capabilities and motivations
- Involve the business in the risk-based decisions!

- Know your Pandas, Bears, Kittens and Tigers!