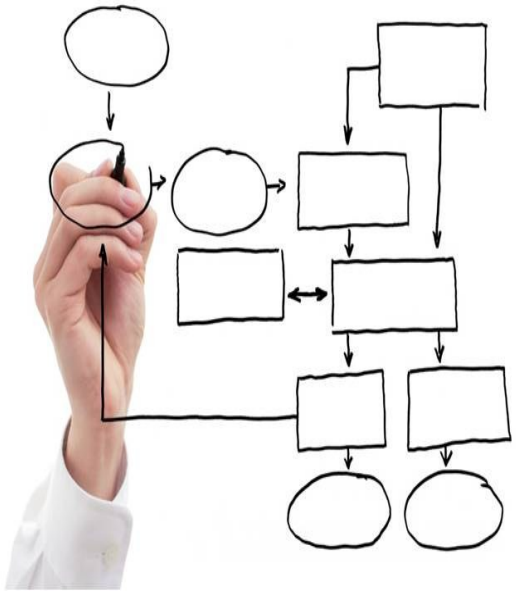
The trends of cyber incidents leading to large scale cyber-crisis

Ilias Chantzos

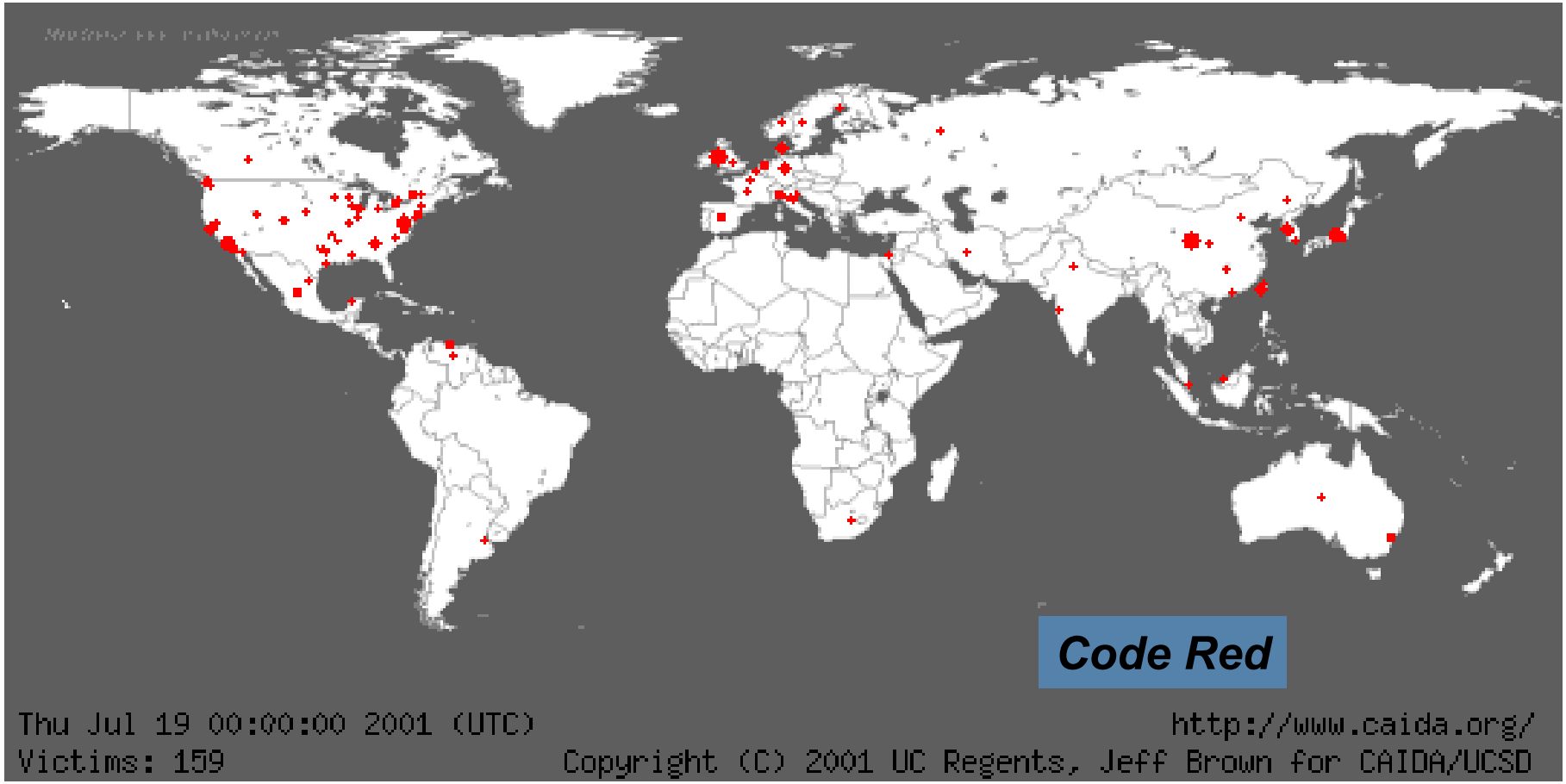
Senior Director Government Affairs EMEA, Global CIP and Privacy Advisor

Agenda for discussion

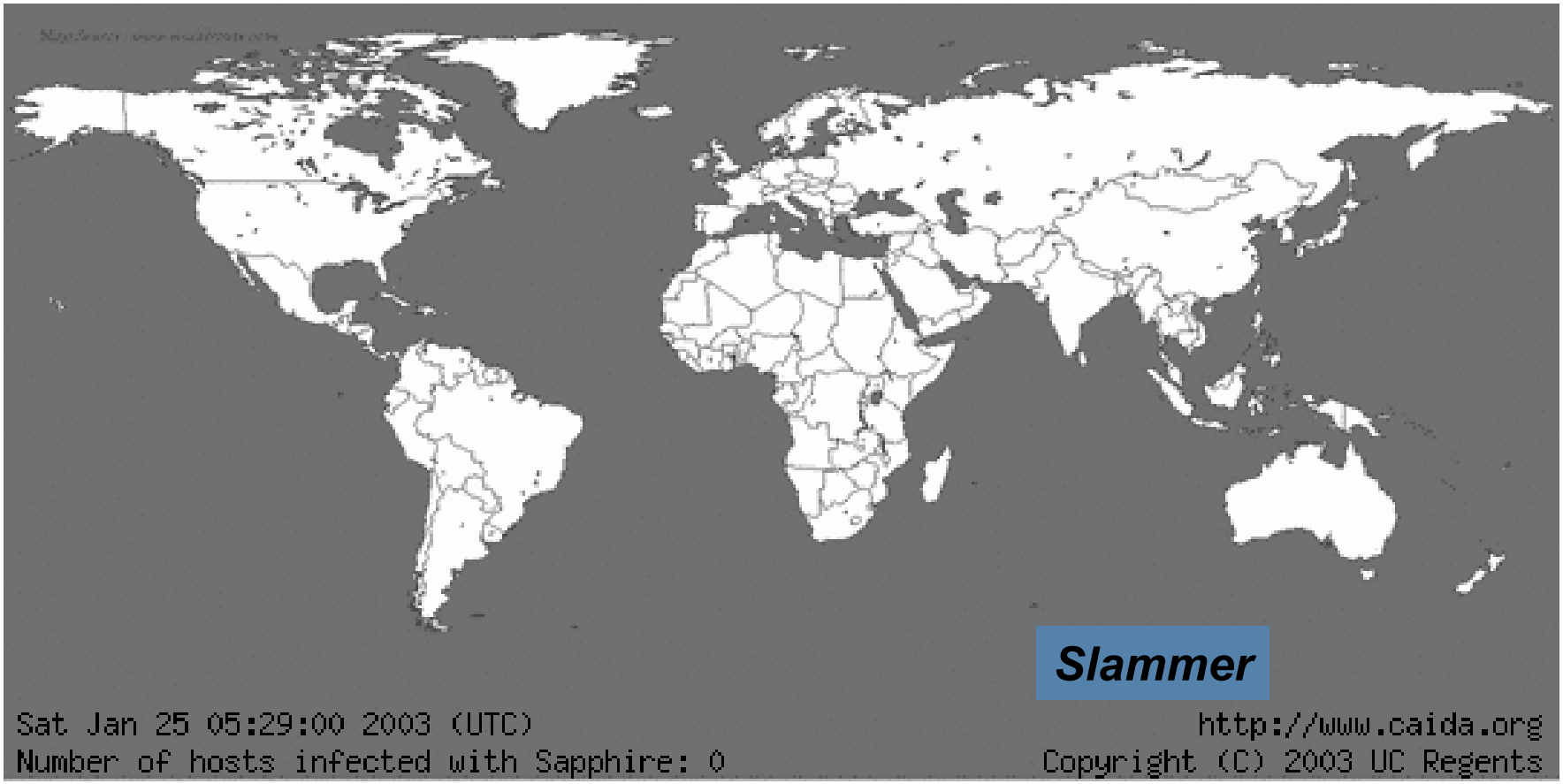
- Do you remember?
- Who is being attacked and how?
- Most recent example
- Political considerations
- Conclusions



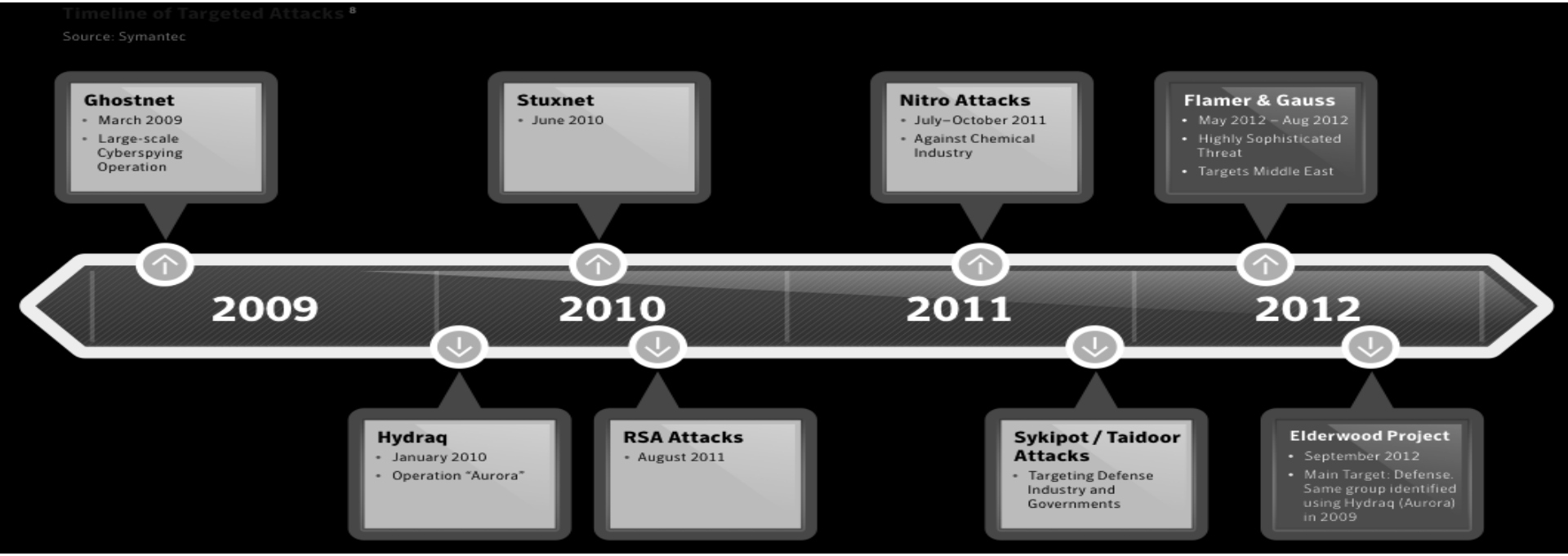
Back in early 2000……Fast Spreading Exploits



Spread Even Faster…



Since then…..


Timeline of Targeted Attacks [8]
Source: Symantec
Ghostnet
• March 2009
• Large-scale Cyberspying Operation
Stuxnet
• June 2010
Nitro Attacks
• July–October 2011
• Against Chemical Industry
Flamer & Gauss
• May 2012 – Aug 2012
• Highly Sophisticated Threat
• Targets Middle East
2009
2010
2011
2012
Hydraq
• January 2010
• Operation "Aurora"
RSA Attacks
• August 2011
Sykipot / Taidoor Attacks
• Targeting Defense Industry and Governments
Elderwood Project
• September 2012
• Main Target: Defense. Same group identified using Hydraq (Aurora) in 2009

The change in the game

- When was the last time you saw mass malware distribution?
- Botnet usage reminiscent of this style of attack
- No longer hacking for fame but for fortune
- The biological bug vs the digital
- Polymorphism
- 1 mutation per 10 victims

Spear

person of interest

Watering Hole Attack

in wait for them

- Targeted Attacks predominantly start as spear phishing attacks
- In 2012, Watering Hole Attacks emerged
  - Popularized by the Elderwood Gang

Effectiveness of Watering Hole Attacks

1 Watering Ho
Attack in 201
Infected
500 Compan

All Within
24
Hours

- Watering Hole attacks are targeted at specific groups
- Can capture a large number of victims in a very short time

Watering Hole Targeted iOS Developers

- The Watering Hole
- The attackers were looking for iOS developers

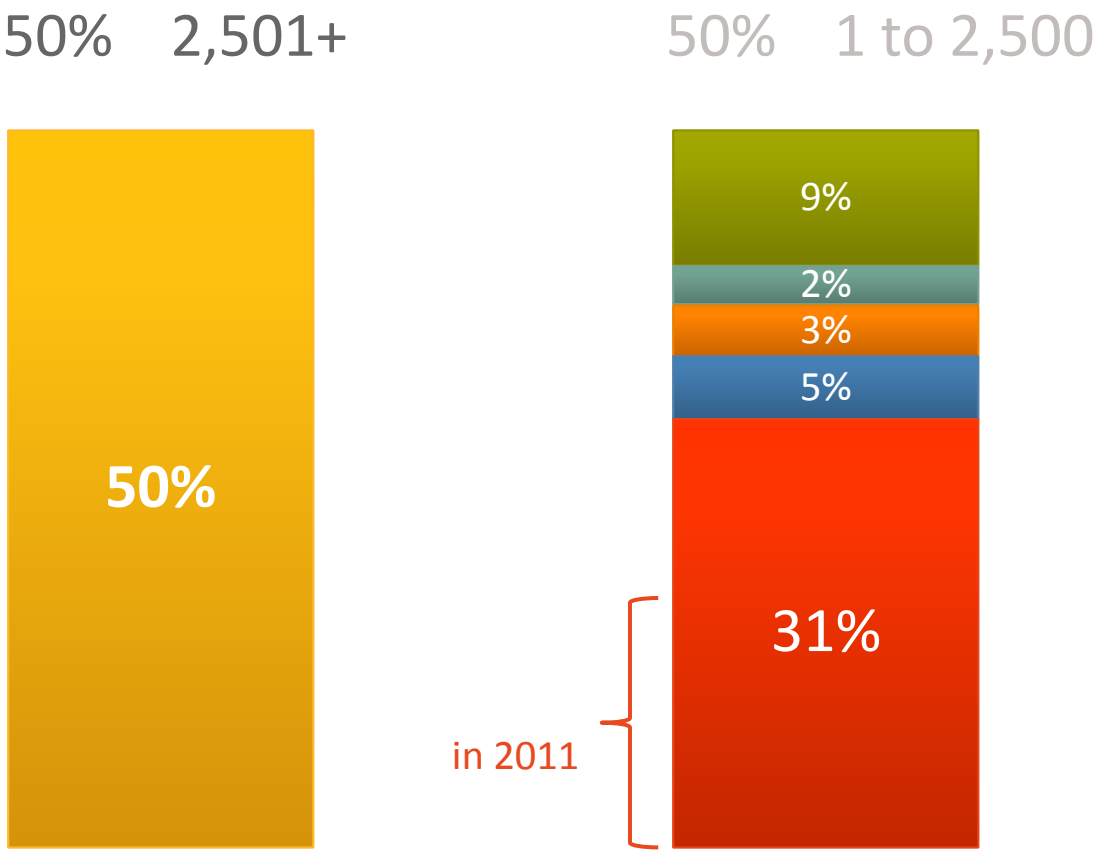
To watch out - Vulnerabilities & Mobile Malware

Platform	Vulnerabilities
Apple iOS	387
Android	13
Blackberry	13
Windows Mobile	2

Device Type	# of Threats
Apple iOS Malware	1
Android Malware	103
Symbian Malware	3
Windows Malware	1

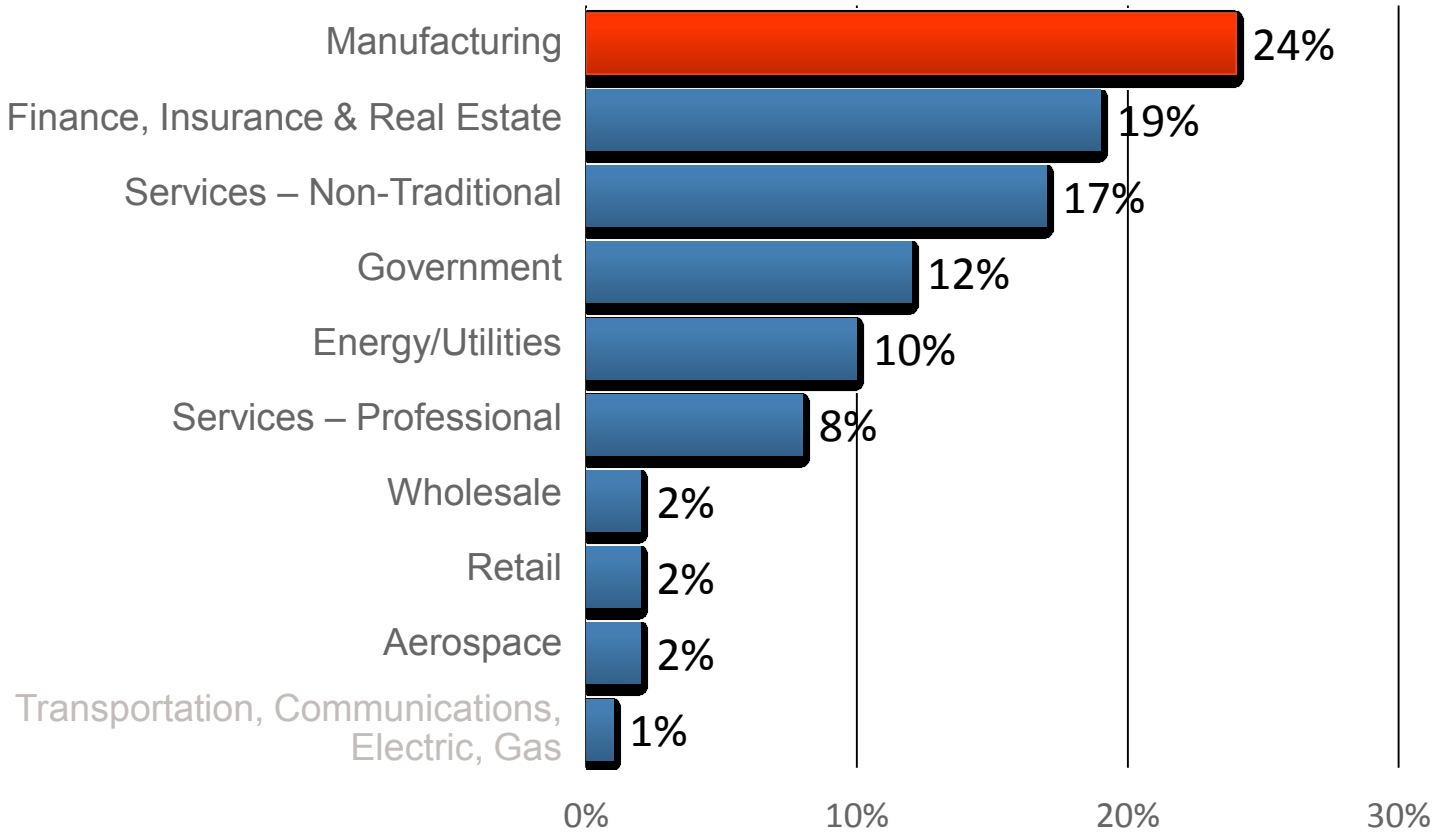
- Today there is no significant link between mobile OS vulnerabilities and exploitation by malware
- In the future that may change

Targeted Attacks by Company Size



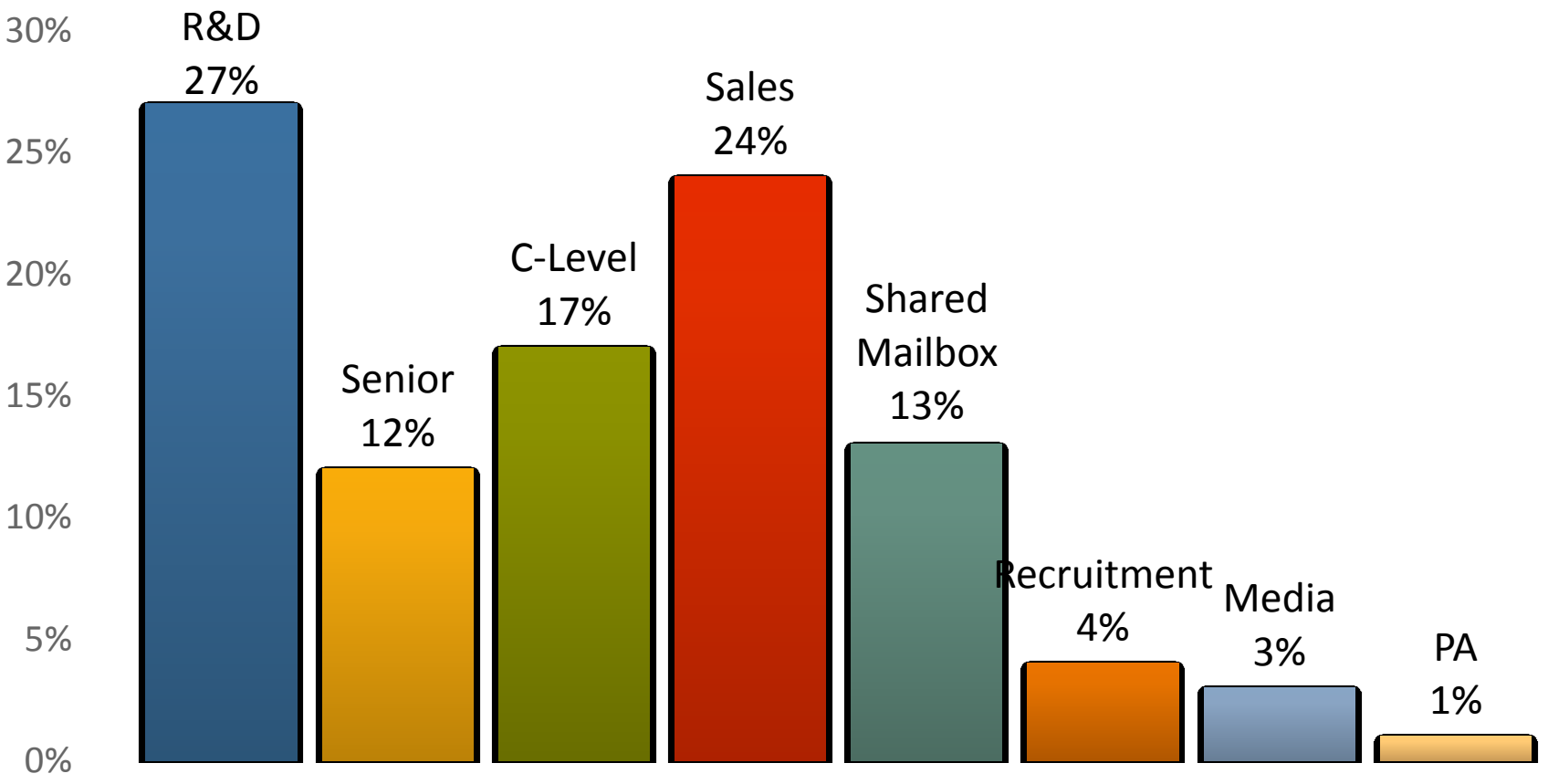
- Greatest growth in 2012 is at companies with <250 employees
- Up 42% in total in comparison to last year

Targeted Attacks by Industry



- Manufacturing moved to top position in 2012
- But all industries are targeted

Targeted Attacks by Job Function

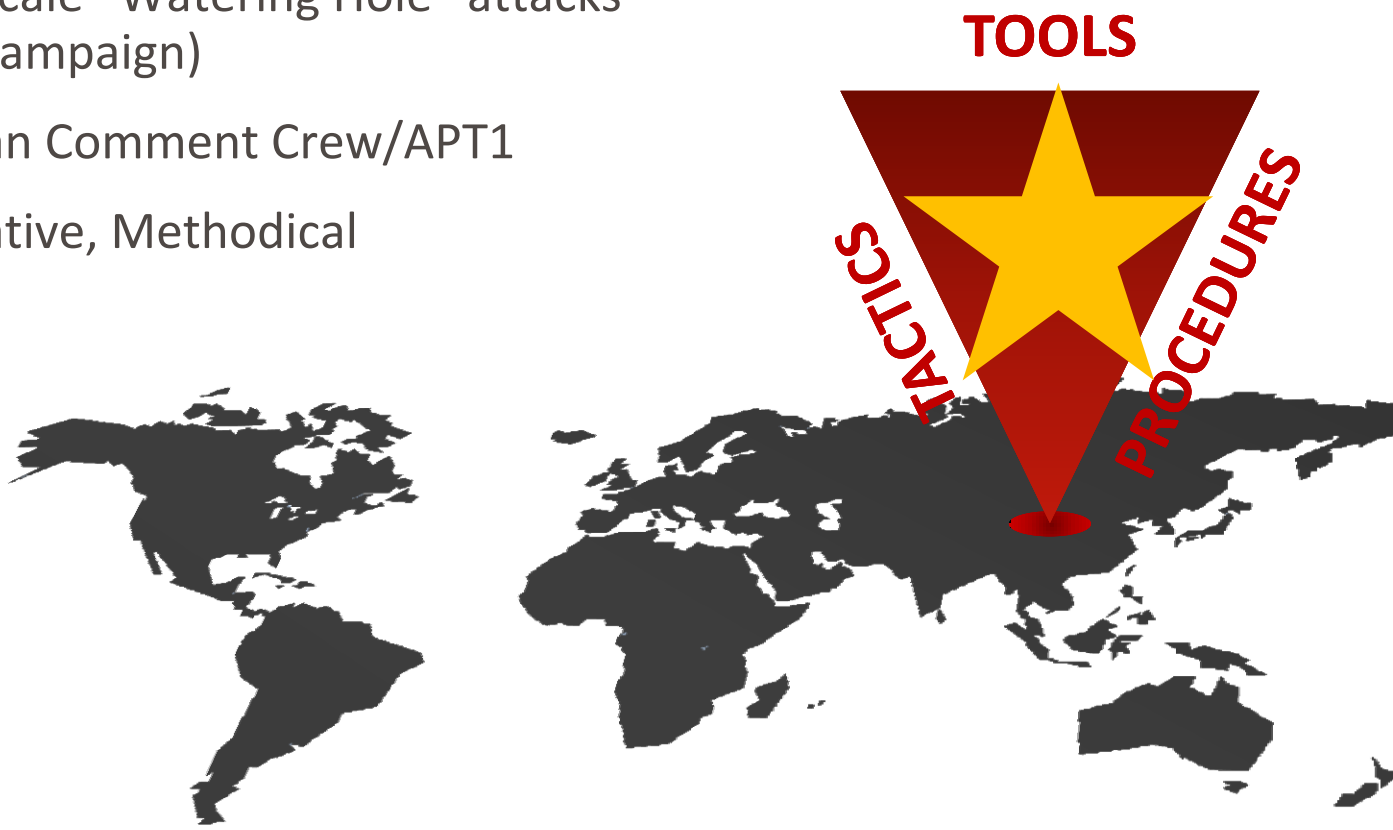


- Attacks may start with the ultimate target but often look opportunistically for any entry into a company

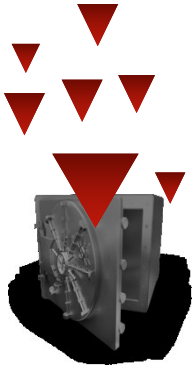
Latest example - Hidden Lynx

Who is the Hidden Lynx group?

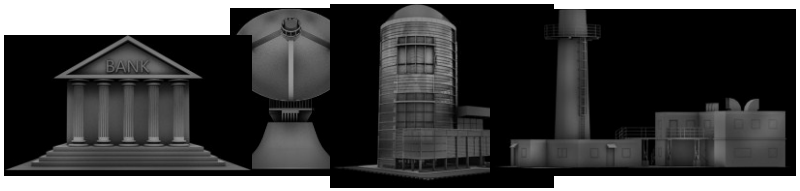
- “Hackers for Hire” established < 2009
- Based in China
- Highly customize tools & access to 0-day exploits
- Pioneered large scale “Watering Hole” attacks (AKA the VOHO Campaign)
- More capable than Comment Crew/APT1
- Proficient, Innovative, Methodical



Characteristics of Hidden Lynx

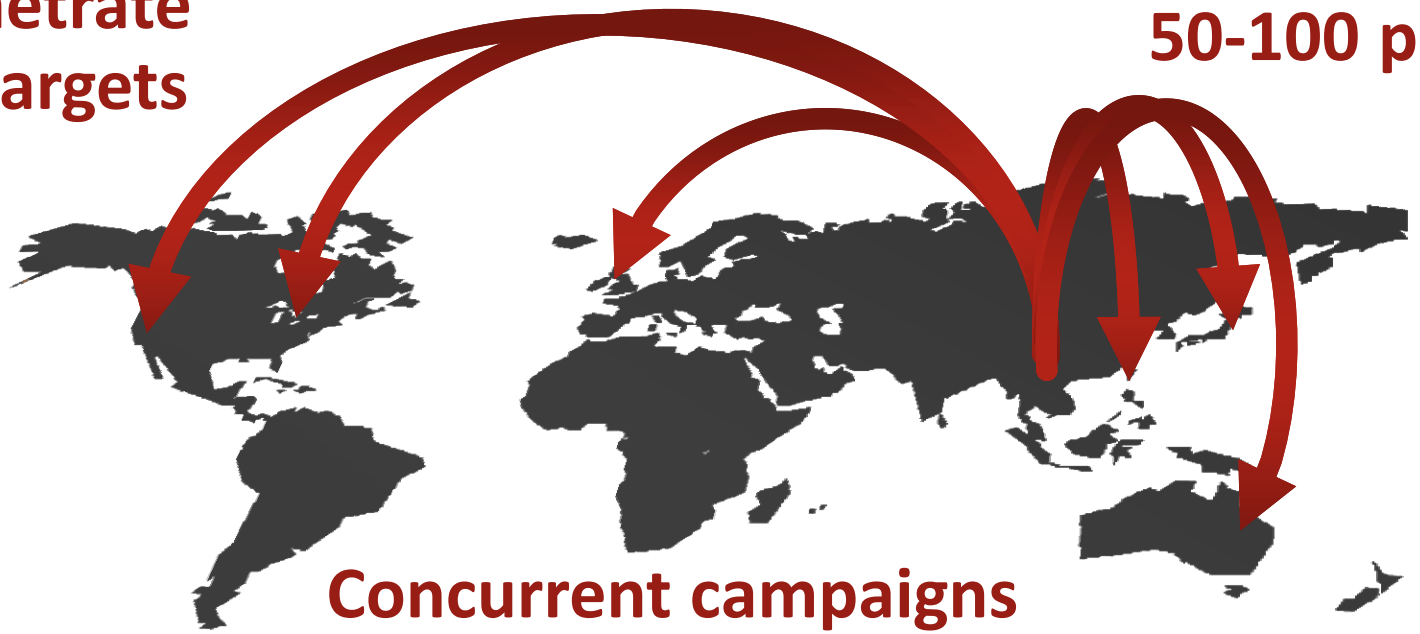


Can penetrate tough targets



Diverse range of targets

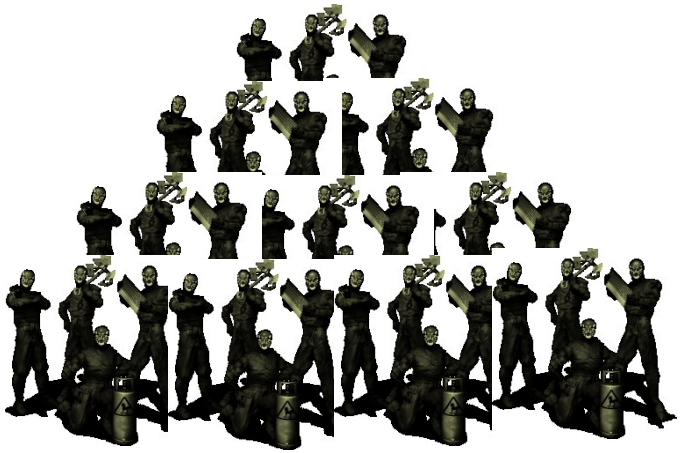
Well resourced 50-100 people



Concurrent campaigns

The Two Sides of Hidden Lynx

Same organization but different teams…



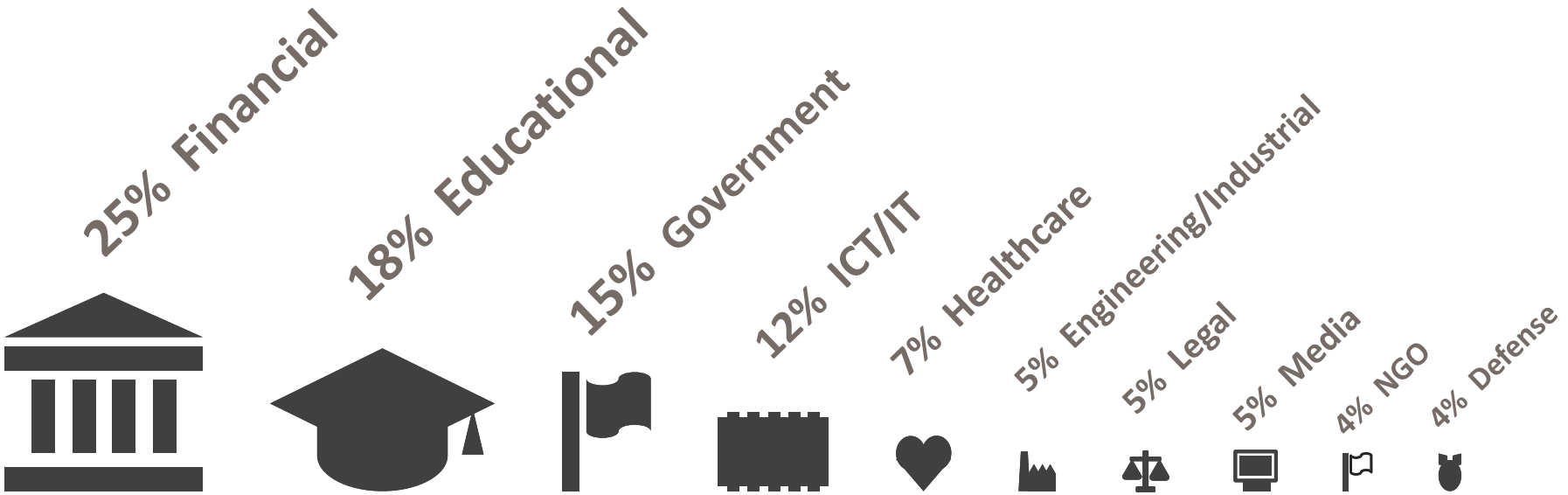
Team Naid

Elite, Precise, Surgical
Uses: Trojan.Naid
Scope: Special operations (small team)
Targets: Information of national interest
Examples: Bit9 attack, Operation Aurora

Team Moudoor

Skilled, Prolific, Indiscriminant
Uses: Backdoor.Moudoor (custom “Gh0st RAT”)
Scope:
Wide scope attacks (large team)
Targets: Financial sector, all levels of government, healthcare, education and legal

Who's Targeted – Verticals

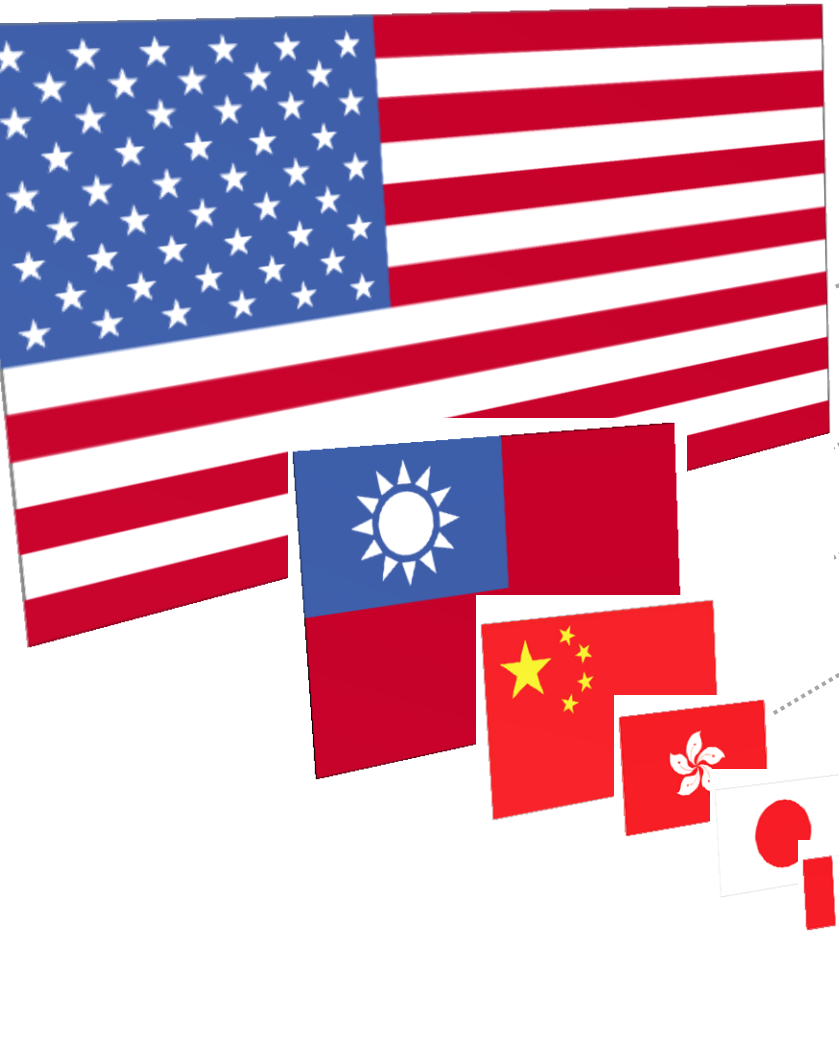


Hundreds of targets

Dozens of campaigns

Direct/Indirect attacks

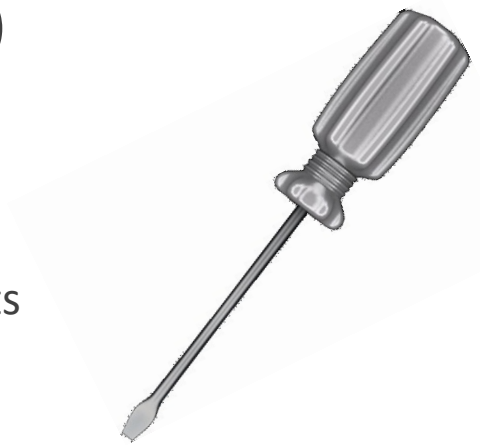
Who's Targeted – Top 10 Countries



- 52.7% USA
- 15.5% Taiwan
- 9% China
- 4% Hong Kong
- 3% Japan
- 2.4% Canada
- 2.2% Germany
- 1.7% Russian Federation
- 1.5% Australia
- 1.5% Republic of Korea

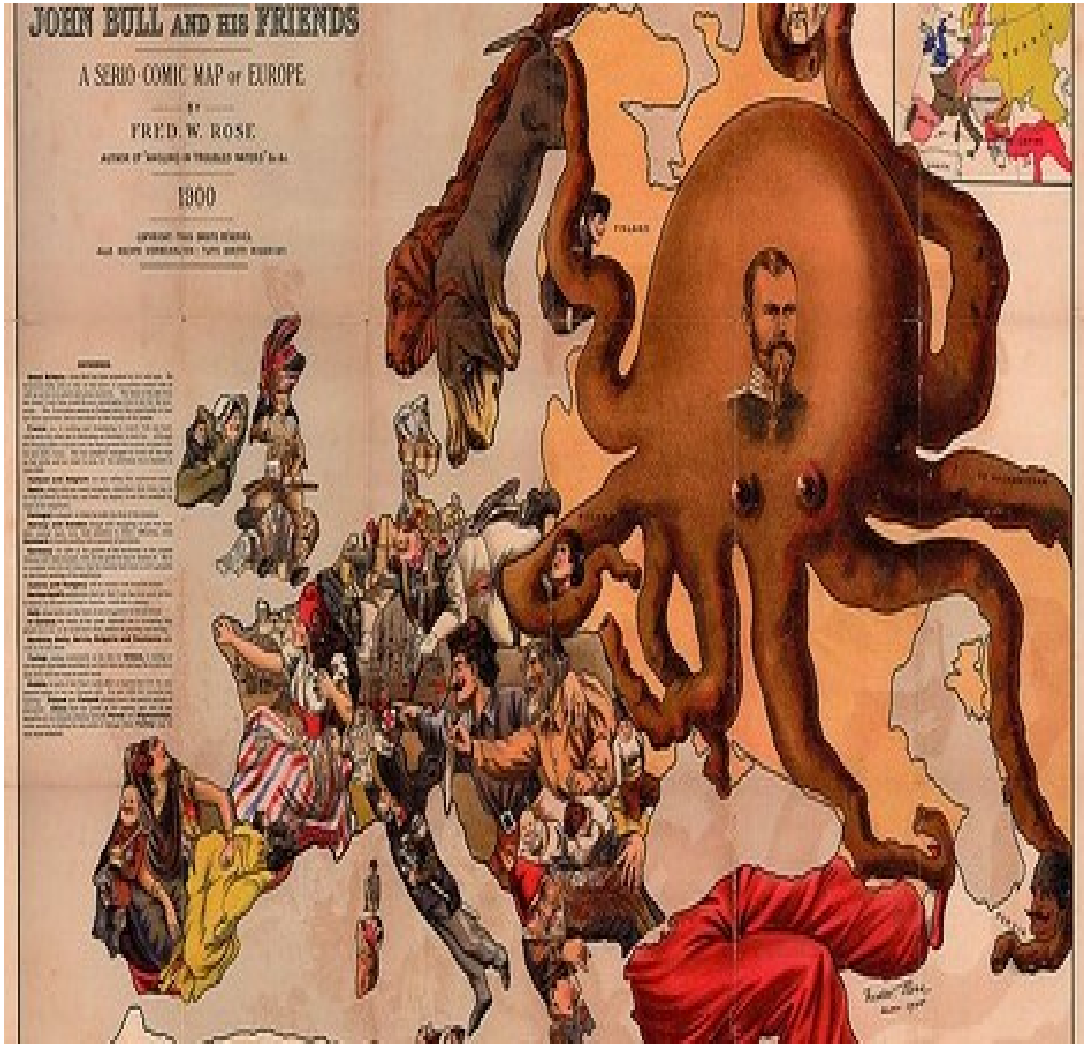
Tools, Tactics and Procedures

- Custom Trojans
- Early adopters of watering hole techniques (VOHO)
- Spear-phishing
- Supply chain attacks
  - Trojanizing driver files in the supply chain to infiltrate final targets
- 0-day and known exploits
  - Since 2011, 5 exploits including 3 0-day exploits
  - Including gaining early access to exploit details (Oracle Java CVE-2013-1493)
- Adaptable and resourceful
  - Stole Bit9 signing certificate to bypass their trust protection model
- Tell-tale characteristics of a professional and skilled gro



Political considerations

- Cyber as a tool for SIGINT
- Cyber as a tool in conflict management
- Asymmetric, deniable, effective
- Political tension and cyber links
- Cyber+CNI= Physical crisis
- Presumed capability and deterrence
- Trust model and PPP



Conclusions

- No agreed definition of large-scale cybercrisis
- Deterrence by denial is likely to prove superior to deterrence by counterstrike
- Militarization of some technologies is inevitable
- Cybersecurity moving towards SIGINT, EW, sabotage and strategic warfare
- Reliance on robotics will extend civilian and military use of cyber
- Combination of targeted and mass-scale likely to evolve
- Financial motivation will remain a prime driver
- Another political tool?

Thank you!

Ilias_chantzos@symantec.com