Cyberthreat Environment

Matthew Devost  
mgd@fusionX.com  
July 2010
About the presenter

• Currently
  – President & CEO – FusionX, LLC
  – Adjunct Professor at Georgetown since 2002
  – Special Advisor to multiple official entities

• Previously
  – Founder, President of CEO of Terrorism Research Center (1996-2008)
  – President of Total Intelligence Solutions
  – SAIC, iDEFENSE, iSIGHT, Counterpane, and SDI
About this presentation

• Focus on overall environment and non-observables
  – Assuming state-actors – why are they here?
• Not for attribution or public disclosure
• No discussion of particular countries, but happy to handle in Q&A
Criminal Hacking

• Attribution on criminal elements is often initially incorrect
• Use of “neutral space”
• Pirated software base in developing and newly developed nations allows for convenient obfuscation of actual actors
Patriotic Hacking

• Amateur and mildly sophisticated
• Utilization of known vulnerabilities
• Primarily focused on targets of opportunity with some direct targeting
• Not controlled by State governments, but tolerated and in some instances “inspired” by State propaganda
Dissident monitoring and identification

• Directed intrusion to monitor equipment outside government’s official jurisdiction
• Internet as extension of government surveillance capabilities
Intellectual Property Theft

• Direct intrusion or targeting to steal IP
• Gain marketplace advantage
• Decrease effective lifecycle or emerging technologies (especially true to DIB)
Social Network Exploitation

- Exploitation of social network aspects of legitimate entities (not social networks like Facebook, although that happens too)
- Save Darfur case study
- Educational environment implications
Political Intelligence/National Security

- Strategic insight into Foreign Policy or those shaping the dialogue
- Think tanks, political parties and individuals associated with those entities or official government agencies
Strategic Penetration...

• ....for future exploitation
• Penetrate and maintain access
• Targeting of critical infrastructure
• Minimize observable patterns or traffic
• Placement of backdoors
• Compromise source code (to determine future access nexus)
Discrepancy in Adversary Capabilities

• A Team versus B Team
• Target escalation
• Compromise maintenance
Emerging Concerns

• Unstructured Hacker gets lucky
• Displaced Terrorist organizations
• Politically motivated criminals (non-terrorist)
• International terrorist organizations
  — Finance as a primary target
Educational environment

- Human element
- Social Network Exploitation
- Neutral space
- Bandwidth rich attack platforms
- Links to government agencies
- Insight into foreign policy
- Fraud or fraud monetization
- Early state companies (e.g. Facebook)
Questions/Comments
Contact Information

Matt Devost
703-626-0272
mgd@fusionX.com

Twitter: @mattdevost
Facebook: http://www.facebook.com/devost
Skype: mattdevost