Threat Analysis – DoD vs Civilian Government

Matthew A Stern
LTC (Retired)
Former Commander, US Army CERT
2d Battalion, 1st Information Operations Command
Currently –
Distinguished Member Technical Staff
General Dynamics – Advanced Information Systems

This briefing is Unclassified

Agenda

- Today’s Cyber Threat
- Exploit Vectors
- DoD Cyber Security Community
- Civilian Government Cyber Security Community
- Growing Commercial Intel Community
- Just my opinion…

Today's Cyber Threat

- Characteristics:
  - Determined, sophisticated, agile and stealthy
  - Not deterred or encumbered by laws or policy
  - Motivated by money, politics, pride, or thrills
  - They are probably better at it than your security staff…
- "For every action, there is an equal and opposite reaction":
  - Anti-virus programs = polymorphic viruses
  - Two factor authentication = exploits against service accounts
  - Locking down ports and protocols = encrypted traffic over port 80
  - Computer forensics = code obfuscation and anti-forensics
  - Trusted Platform Module (TPM) Chip = Remotely deployed BIOS Root kit
  - MD5 Hashing = Evil Twin

Exploit Vectors

- Social engineering and phishing
- Web browsing attacks (compromised commercial websites)
- SQL injection methods against vulnerable websites
- Increasingly sophisticated BotNets
- Stolen credentials and certificates
- Pharming (website redirection)
- DNS Attacks
- Distributed Denial of Service (DDoS)
- Supply chain insertion
- Thumb Drives (U3 Technology)
- BIOS Root kits

DOD Cyber Security Community

- Tools
  - Analytic – Event Correlation, Trends, Patterns
  - Detection (PCAP and forensics are essential)
  - Open source research
- Analyst Training
  - Critical Thinking and reasoning
  - Technical know how
  - Inculcate Intel Oversight to ensure regulatory compliance on collection, dissemination, and storage
- Have a great model to focus Intelligence efforts
  - Priority Intelligence Requirements
  - Wargame threat most probable or dangerous course of action
- Rehearse to validate processes and operational concepts
- Certification
  - Analysts and Operators
  - Organizations (Computer Network Defense – Service Provider)

Civilian Government Cyber Security Community

- Need the same capabilities as DoD
- Analyst Training
  - Key to ensuring privacy is protected
  - Recommend certification program to create “Trusted Agents”
  - Recommend a CND-SP like program to certify organizational processes
    - » Allows cyber security community to use all tools at their disposal
    - » Provides governance to ensure regulatory compliance on collection, dissemination, and storage
- Follow DoD model to focus intelligence support
  - Documents threat detection methodology and procedures
  - Can be used to focus limited resources

Growing Commercial Intel Community

- No restrictions on privacy
- Need to understand the value of
  - commercial cyber “intel” providers
  - Evolving computer security research community of reformed hackers
- Can tailor products to ensure privacy compliance
- Trained and certified analysts can ensure governance

Just my opinion…

- Looking for a technical panacea when is most cases privacy compliance is a “people” problem
- The issues can be mitigated with an accepted program to ensure that cyber security organizations maintain
  - Trained and certified analysts
  - Trained and certified processes
- The DoD CND-SP model is very useful
- Technology will never keep pace with the threat
  - Again – “For every action, there is an equal and opposite reaction” – what’s next?
  - Everyone in this business is trying to build a better mouse trap…That’s a problem when your trying to catch a snake.