UNCLASSIFIED

Working with Law Enforcement
SANS Forensics Summit

July 2009
CS Jennifer Kolde
jennifer.kolde@ic.fbi.gov

UNCLASSIFIED
Panelist Bio

• Computer Scientist (CS) with San Diego FBI National Security Cyber Squad
  – Cyber-counterterrorism / cyber-counterintelligence
• SME in support of Agent investigations
  – Forensics, malware analysis, traffic analysis…
• 11 years in IT / security, primarily for US Navy
  – Computer / network security, incident response, forensics, malware analysis
• 2 yrs SANS instructor / Director of GIAC
Discussion Question

• What are the major challenges that Law Enforcement digital investigators now face or will face in the near future?
  – Increasingly sophisticated tools and techniques make intrusions more difficult to detect
  – Insufficient forensic evidence and / or skills to fully determine “what happened”
Low Risk / High Reward

- McAfee / Purdue CERIAS, “Unsecured Economies” Survey:
  - Companies estimated they lost $4.6 billion worth of intellectual property last year alone
  - Spent ~$600 million repairing damage from data breaches

- Heartland Payment Systems’
  - Breach cost $12.6 million to date (as of May 2009)
  - Does not include cost of new end-to-end encryption

- How do you measure “national security” losses?


Source: Network World, “Security breach cost Heartland $12.6M so far”,

UNCLASSIFIED
Tools and Techniques: Examples

• Heartland:
  – “The sniffer malware that surreptitiously siphoned tons of payment card data…hid in an unallocated portion of a server’s disk…hidden so well that it eluded two different teams of forensic investigators…”

• Conficker:
  – Digitally signed and encrypted binaries
  – 250 -> over 50,000 random callback locations
  – P2P capabilities
  – Ongoing development to thwart analysis / containment

Source: Storefrontbacktalk, “Heartland Sniffer Hid In Unallocated Portion of Disk”, 28 January 2009

http://mtc.sri.com/Conficker and “Conficker C Analysis”, 4 April 2009,
http://mtc.sri.com/Conficker/addendumC/index.html
Additional Threats

• Memory-only malware?
• BIOS-based malware?
• Attacks against virtual machines?
• Network devices?
• PDAs / smartphones?
• Other?
Insufficient Evidence

• Everyone wants to know *what happened*?
  – Reporting requirements
  – Legal / regulatory liability
  – Damage assessment

• Consistent problems:
  – Insufficient logging (not logged, not retained)
  – Evidence not collected (memory)
  – Lack of skills and / or tools to analyze…
    • Databases, network devices, smart phones…
Challenges

• Network defenders need to:
  – Be alert to highly sophisticated threats
    • The Cuckoo’s Egg
  – Ensure enough data is collected and retained

• First responders need to:
  – Collect all potential sources of evidence

• Forensic analysts need to:
  – Think outside the box, look for evidence in non-traditional locations, expand skill set to address emerging threats