PURDUE UNIVERSITY

DEPARTMENT OF COMPUTER & INFORMATION TECHNOLOGY

CERIAS tm

Anti-Forensics

LOCKHEED MARTIN

San Diego

September 15th, 2005

Dr. Marcus K. Rogers

AGENDA

- What is anti-forensics
- Countering anti-forensics
- Looking ahead
- Conclusions

ANTI-FORENSICS (AF)

- Various definitions
  - Attempts to negatively effect the existence, amount and/or quality of evidence from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct.
- Digital evidence (DE) is not immune to this
- The volatility of DE and the reliance on tools makes cyber forensics very vulnerable to AF
- Issue for all the Digital Forensics Communities
  - LE, Private Sector, Military/Intelligence

ANTI-FORENSICS (AF)

- Conferences are talking about this
  - Black Hat Briefings USA 2005

  - E-Crime and Computer Evidence Conference -2005 Monaco

ANTI-FORENSICS (AF)

- Categories
  - Data hiding
  - Artifact wiping
  - Trail obfuscation
  - Attacks against the CF process/tools **

CATEGORIES

- Data hiding
  - Nothing new here!
  - Rootkits have been around for quite some time
  - Attempt to hide data in unusual places
    - Memory
    - Slack space
    - Hidden directories
    - Modifying metadata
    - Bad blocks
    - Alternate Data Streams
    - Hidden partitions
  - Data Encryption
  - Steganography
    - No one is sure how big a problem this is
    - Mixed results on identifying stego

CATEGORIES

- Artifact wiping
  - Disk cleaners
    - Effective but obvious that it was used
  - Free space and memory cleaners
    - Less obvious
    - Most don't work properly and leave signatures behind (Geiger, 2005 - DFRWS)
    - Nothing really new
  - Prophylactic
    - Not producing any artifiacts/reminants
      - No writes to the disk

CATEGORIES

- Trail obfuscation
  - Where is the source located
  - Who is the source
    - Log cleaners
    - Spoofing
    - Misinformation
    - Backbone hoping
    - Zombied accounts
    - Trojan commands
      - PS, LS, etc.
  - Not new either!

CATEGORIES

- Attacks against the CF Process/tools
  - Houston we have a problem!
  - Relatively new
  - Victim of our own success in making CF standardized and public
  - Vendor & Tool dependency has made us very vulnerable!
  - Relative immaturity of the discipline has not helped
  - Focus area for the computer underground because of its relative ease

CF Process/tools

- Multiphase approach
  - Crime scene identification/control
  - Evidence identification
  - **Evidence preservation & collection**
  - Evidence transportation
  - **Examination and Analysis**
    - Interpretation
  - Report and Presentation

CF Process/tools

- Evidence Preservation & Collection
  - Some novel attacks discussed but few so far have been documented in the "wild"
    - Bad blocks
    - Odd disk sectors
    - Altering the HDA or DCO at the drive level
  - This CF process is very tool centric
    - EnCase, FTK, DD, or other integrated device
  - Attacks seek to prevent the creation of bitstream images or prevent integrity checking
    - Image appears to be +4 Terabytes
    - Hashes never match
- For the most part it is obvious that something is amiss

CF Process/tools

- Examination & Analysis
  - Can be a much more subtle attack
  - Relies on vulnerabilities of the examination and analysis tools
  - Assumption is most LE and CF practitioners are "tool monkeys" who don't understand what is happening under the hood
  - Documented attacks against
    - FTK, EnCase, iLook, WinHex, TCT, Sleuthkit, etc.
      - Compression bombs
      - Nested directories
      - Altering the MFT and inodes
      - File signature altering, hash fooling
  - The more automated the tool the more susceptible it is to attack!

Countering AF

- Anti-Anti- Forensics
  - Understand what the tools are doing or supposed to do
  - Error logging on tools
  - Don't automate everything by default
- Funded research on AF
  - Most research is to date is grass roots and ad hoc
- Focus research on the Windows world as opposed to *NIX
  - Majority of LE and Private sector cases involve Windows OS
    - Academic research has tended to be *NIX centric as it is better understood, relatively open, and documented
- Don't publish all of our tricks??

Looking Ahead

- Anti-forensics is here to stay
- We are now in an arms race of sorts
- Data wiping tools (free space etc.) will get better
- Attacks will get more subtle
- Unfortunately tools will get more automated, more levels of abstraction
  - Data mining, Expert systems, Evidence aggregation tools, AI
- Data mining and evidence aggregation are needed due to the increasing storage capacities and thus increase in volume of data
- SOPs give the other side intelligence to use against us

Conclusion

- Most anti-forensics techniques are not new
- Most are obvious
- Increased attention by the underground
- More research is needed
- More information sharing within the community is needed
- Better training for practitioners
- Vendors need to listen to the community better
- This issue is here to stay!

Further Reading

Butler, G. H. J. (2005). *Rootkits: Subverting the windows kernel*: Addison Wesley Professional.

Foster, J., & Liu, V. (2005). Catch me, if you can... Retrieved Sept 5th, 2005, from www.metasploit.com/projects/ antiforensics/BH2005-Catch_Me_If_You_Can.ppt

Geiger, M. (2005, August 18th). *Evaluating commercial counter-foreniscs tools.* Paper presented at the DFRWS, New Orleans.

Grugq. (2005). The art of defiling. *Blackhat Briefings* Retrieved Sept 9, 2005, from www.blackhat.com/presentations/ bh-asia-03/bh-asia-03-grugq/bh-asia-03-grugq.pdf

Mcleod, S. (2005). Smart anti-forensics. Retrieved June 1, 2005, from http://members.ozemail.com.au/~steven.mcleod/SMART_Anti_Forensics.pdf

Peikari, A. C. C. (2004). *Security warrior*: O'Reilly.

Peron, C., & Legary, M. (n.d.). Digital anti-forensics: Emerging trends in data transformation techniques. Retrieved Sept 1, 2005, from www.seccuris.com/documents/papers/Seccuris-Antiforensics.pdf

PURDUE UNIVERSITY

DEPARTMENT OF COMPUTER & INFORMATION TECHNOLOGY

CERIAS tm

Contact Information

Marc Rogers PhD, CISSP, CCCI
Associate Professor
Computer & Information Technology
Center for Education and Research in Information Assurance & Security (CERIAS)
Purdue University
http://www.cyberforensics.purdue.edu
rogersmk@purdue.edu
765-494-2561