Covering Your Tracks: Ncrypt and Ncovert

Simple Nomad

Hacker – NMRC

Sr. Security Analyst - BindView

Stealth and Covert Communications

- What is it
- Why use it
- Examples in existence
  - File encryptors/decryptors (GPG, etc)
  - File system encryption (CFS, NTFS encryption, etc)
  - Steganography (Outguess, etc)
  - Covert network (Loki2, etc)

Goals for Project

- Defeat network and workstation forensics
- Simple and clean install/compile (no extra libraries)
- Leverage existing technology

Ncovert - Overview

- Freeware
- No extra libraries required, uses standard C
- Uses Initial Sequence Number (ISN) as the data field
- Anonymous sending
- Can bypass most firewalls

Ncovert – How it works

- Sender sends SYN packet with data in ISN to public server, forges source IP as receiver's IP
- Public server receives SYN, sends SYN/ACK to receiver's machine
- Receiver's machine sniffs packet and gets data, the OS sends a RST to public server
- Repeated until all data is sent

Ncovert – Pros and Cons

- Pro
  - Anonymous sending
  - If sniffing in path to forged source IP, anonymous receiving
  - Careful planning can bypass most firewall rules
- Con
  - Slow, as reliable as UDP
  - Plaintext transmission, must encrypt data first (use Ncrypt)
  - Needs multiple "triggers"

Ncovert - Live Demo

BINDVIEW Insight at Work

Ncrypt - Overview

- Freeware
- No extra libraries required, uses standard C
- Symmetric file encryption/decryption
- Choice of three encryption algorithms
- Optional wiping of files, with wiping also getting file slack
- Choice of two wiping techniques
- Additional secure coding

Ncrypt – Crypto Used

- Encryption algorithms
  - Rijndael (AES)
  - Serpent
  - Twofish
- SHA-1 hashing of passphrase
- Random data stream generation - ISAAC

Ncrypt - Wipe Fu

- Peter Gutmann's 1996 defacto standard from "Secure Deletion of Data from Magnetic and Solid-State Memory"
- 4 passes of random data, 27 passes of specific bit patterns, 4 more passes of random data, 35 passes total
- Anti-forensics aimed for defeating TLAs
- Probably overkill by today's standards for disk drives

BINDVIEW Insight at Work

Ncrypt – Wipe Fu

- NSA-developed National Industrial Security Program Operating Manual (NISPOM) aka DoD 5220.22-M; subsection 8-306
- A pass of a character, a pass with that character's bits flipped, and a verified pass with random data, 3 passes total
- There is no "wipe 7 times" U.S. Government standard to be found
- Not for TOP SECRET, which is significant in itself

BINDVIEW Insight at Work

Ncrypt – Secure Coding

- Plaintext passphrase wiped from memory after converted to a SHA-1 hash
- SHA-1 hash wiped from memory after crypto key is made
- If root, memory locked from paging

BINDVIEW Insight at Work

Ncrypt – Target Users

- Non-root users e.g. shell account on an ISP
- Human rights worker
- Security professional
- Privacy advocate
- Black hat

Ncrypt - Live Demo

Resources

- Ncrypt - http://ncrypt.sourceforge.net/
- Ncovert - http://www.nmrc.org/project/ncovert/
- National Industrial Security Program Operating Manual (DoD 5220.22-M), Dept. of Defense, 1995 - http://www.dss.mil/isec/nispom_195.htm
- “Secure Deletion of Data from Magnetic and Solid-State Memory” , Peter Gutmann, 1996 - http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

BINDVIEW Insight at Work

Questions

- thegnome@nmrc.org
- Loveless@bindview.com