



# Alternate Data Streams

How Files can be Hidden on Your System



# Who am I

- George Pauwels
  - Technical Instructor – New Horizons
    - CISSP, CEH, SCNS, Security+
    - MCSE, MCSA, MCT
    - CCNA, CCENT
    - Linux+, Network+, A+
  - 20 years IT Experience



# Review of the Hacker Process

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks



# What are Alternate Data Streams?

- Fork – additional data associated with a file system object - metadata.
- Files systems that support ADS:
  - Microsoft's NTFS
  - Apple's Hierarchical File System
  - Novell's Novell Storage Services and Netware File System
  - Solaris' UFS (Solaris 9 and later) and ZFS
  - Veritas Software's Veritas File System

# What Kind of Metadata?

- Apple's uses for forks
  - store GUI info like icons, menu items and dialog boxes
  - Splitting word processing document into content and presentation
  - Postscript fonts
- Novell uses their forks to:
  - store NDS information
  - allow Mac clients to attach to NetWare Servers



# Why do Alternate Data Streams Exist?

- What was Microsoft thinking?
  - Same thing they think every night...How to take over the world.
  - Introduced with Windows NT 3.1
  - Trying to be all things to all vendors
  - File Attributes – Hidden Files, System Files, Access permissions



# What Dangers do ADS Pose?

- Users may never know the presence of files on their computers.
- Computer viruses can hide in ADS
- Data can be lost in ADS
- Crackers can hide root kits behind files



# How do ADS' Work?

- Demo - 1: Text Files



# How do ADS' Work?

- Demo - 2: Program Files



# How do I know they are there?

- LADS - [www.heysoft.de/Frames/f\\_sw\\_la\\_en.htm](http://www.heysoft.de/Frames/f_sw_la_en.htm)
- CrucialADS – [www.crucialsecurity.com](http://www.crucialsecurity.com)
- LNS (List NTFS Streams) Ntsecurity .nu
- Microsoft TechNet – Streams – M Russinovich
- Vista – DIR /R
- Host Intrusion Detection/Prevention Systems
- Checksums



# How do ADS' Work?

- Demo - 3: Multiple Files



# How do ADS' Work?

- Demo – 4: Thumb Drives / I-Pods



# Should I be concerned?

- Some Malware uses ADS
  - Mailbot.AZ
- PreVista dir will not find ADS
- Windows Explorer will not reveal ADS
- SFC.exe (System File Check) will not find ADS
- Laptops in Airports



# Tell-Tail Signs

- Time and date stamp
  - Attribute Magic (<http://www.elwinsoft.com/atm.html>)
  - File Tweak (<http://www.febooti.com/products/filetweak/>)



# How do I get rid of ADS?

- ADS Spy - (  
<http://www.spywareinfo.com/~merijn/downloads.html>)
- Copy your NTFS partition to a FAT partition



## For more Information...

- [http://en.wikipedia.org/wiki/Fork\\_\(filesystem\)](http://en.wikipedia.org/wiki/Fork_(filesystem))
- [www.microsoft.com/technet/sysinternals/fileanddisk/streams.msp](http://www.microsoft.com/technet/sysinternals/fileanddisk/streams.msp)
- [http://images.globalknowledge.com/www/images/whitepaperpdf/WP\\_DS\\_Palmgren1.pdf](http://images.globalknowledge.com/www/images/whitepaperpdf/WP_DS_Palmgren1.pdf)