



Network Investigations – The Current Flavor of the Month

William L. Farwell, CFE, SCERS, EnCE
Director, Forensic & Dispute Services
National Practice Leader Computer Forensics
Analytic and Forensic Technology
Deloitte Financial Advisory Services LLP

August 9, 2007

Audit • Tax • Consulting • Financial Advisory •

Investigative Steps

Volatile Data Collection – Onsite

- Must be performed with minimal invasiveness
 - Must be performed as early in the process as possible
 - Must be preserved for further or future analysis
 - Must be performed using a repeatable process to prevent inconsistencies
- Memory dump – DCFL version of DD command:
(dcfldd.exe if=\\.\physicalmemory of="c:\forensic images\image.dd"
hashlog="c:\forensic images\image.dd.md5")
 - System Date & Time
 - Active Processes
 - Suspect Process Memory Dumps
 - Active Services

Investigative Steps

Volatile Data Collection – Onsite

- Open Ports
- Active Sockets (“fport” - maps back to executables)
- Open Files
- Scheduled Jobs
- Logged on Users
- NetBIOS Name Table Cache
- Internal Routing Tables
- Arp Cache
- Encrypted Volumes & RAM Disks

Investigative Steps

Forensic Analysis - Laboratory

- Date/time analysis
- Mapped network shares
- Existing user accounts
- Event logs
- Prefetch examination
- Signature Analysis
- Hash analysis – comparison of compromised computer against others in system
- Review of registry (autostart locations)

Investigative Steps

Forensic Analysis – Laboratory

- Packed files – comparison to autostart locations
- Spyware/Anti-virus scans
- File permissions – what is running as System
- System virtualization/Stand alone machine
 - What is running?
 - What network connections are open?
 - You may have to map suspect domains to virtual host machine

Malware Static Analysis

- Identify Packed Files or Suspect Executable
- Visual Inspection Hex Viewer
 - “MZ” “PE” in header – Windows Portable Executable
 - “MEW” – free executable packing program from Northfox
 - “UPX” – Ultimate Packer for eXecutables
- Tools
 - Virus Scan to identify malware
 - <http://virusscan.jotti.org/>
 - <http://www.virustotal.com/>
 - PeiD utility – detect pack version
 - Your favorite disassembler
 - UnMEW.exe or UPX to unpack executable
 - Linux Emulator like “Cygwin” - Linux API emulation for Windows
 - Text extractor utilities: Strings (Linux), Bintext
 - Looking for domains, IP addresses, user names, etc.

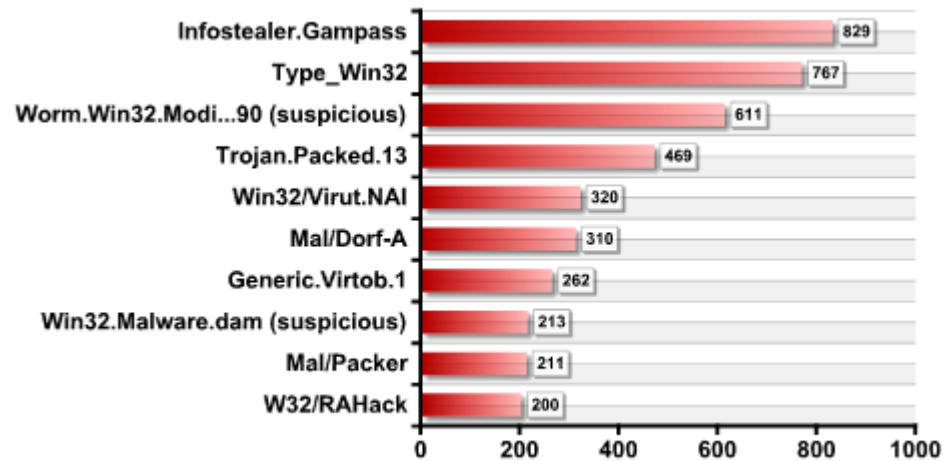
Malware Dynamic Analysis

- Copy the suspect file to a safe environment (Stand alone machine or Virtual machine) Not on a production System!!
- Sample Tool List
 - Dependency Walker – allows you to walk through dependent modules in a Windows binary (www.dependencywalker.com)
 - InCtrl5 – is a before and after utility used to document changes to the disk and registry after a program execution (<http://www.pcmag.com/article2/0,4149,9882,00.asp>)
 - Regmon & Filemon (www.sysinternals.com)
 - Process Explorer (www.sysinternals.com)
 - Port Monitors – TCPView (www.sysinternals.com)
 - Packet Capture - Ethereal (www.ethereal.com)

Malware Static Analysis

Top 10 of Infected Files (Last 24 Hours)

This image shows the list of the most popular infected files received within the last 24 hours.





Questions & Answers

Contact info

- William L. Farwell, CFE, SCRES, EnCE
Director, Forensic & Dispute Services
Analytic and Forensic Technology
Deloitte Financial Advisory Services LLP
617-437-3956
wfarwell@deloitte.com

The information contained in this publication is for general purposes only and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by Deloitte Financial Advisory Services to the reader. This material may not be applicable or suitable for, the reader's specific circumstances or needs. Therefore, the information should not be used as a substitute for consultation with professional accounting, tax, or other competent advisors. Please contact a local Deloitte Financial Advisory Services professional before taking any action based upon this information.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. Deloitte Touche Tohmatsu is an organization of member firms around the world devoted to excellence in providing professional services and advice, focused on client service through a global strategy executed locally in nearly 140 countries. With access to the deep intellectual capital of approximately 150,000 people worldwide, Deloitte delivers services in four professional areas — audit, tax, consulting, and financial advisory services — and serves more than 80 percent of the world’s largest companies, as well as large national enterprises, public institutions, locally important clients, and successful, fast-growing global companies. Services are not provided by the Deloitte Touche Tohmatsu Verein, and, for regulatory and other reasons, certain member firms do not provide services in all four professional areas.

As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other’s acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names “Deloitte,” “Deloitte & Touche,” “Deloitte Touche Tohmatsu,” or other related names.

In the United States, Deloitte & Touche USA LLP is the U.S. member firm of Deloitte Touche Tohmatsu and services are provided by the subsidiaries of Deloitte & Touche USA LLP (Deloitte & Touche LLP, Deloitte Consulting LLP, Deloitte Financial Advisory Services LLP, Deloitte Tax LLP, and their subsidiaries), and not by Deloitte & Touche USA LLP. The subsidiaries of the U.S. member firm are among the nation’s leading professional services firms, providing audit, tax, consulting, and financial advisory services through nearly 40,000 people in more than 90 cities. Known as employers of choice for innovative human resources programs, they are dedicated to helping their clients and their people excel. For more information, please visit the U.S. member firm’s Web site at www.deloitte.com

Deloitte.

A member firm of
Deloitte Touche Tohmatsu