HTCIA2015
Registry Analysis

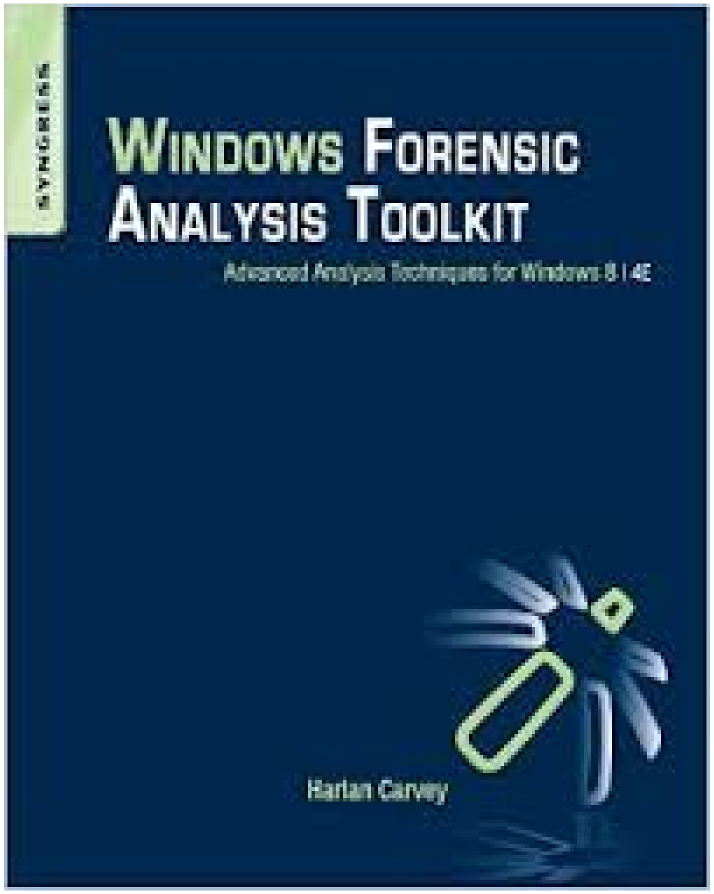
H. Carvey

Sr. Infosec Researcher, CTU-SO

Introduction

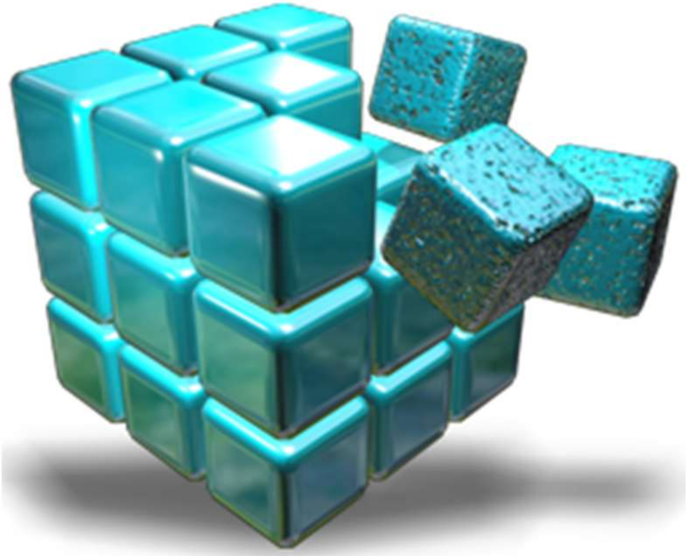
- Sr Infosec Researcher @ DSWRX CTU-SO team
- Former Marine Officer
- Infosec since ‘89, DFIR since ’00
- Prolific author (books, blog)

- Let’s talk about Registry Analysis…


SYNGRESS
WINDOWS FORENSIC ANALYSIS TOOLKIT
Advanced Analysis Techniques for Windows 8 | 4E
Harlan Carvey

Registry Analysis

- What is it?
- Why does it matter?
- Why bother?



By The Numbers…

- Why does *ANY* of this matter?

- Annual Security reports
  - % external notification
  - Median days to detection

- M-Trends 2015
  - 69%
  - 205
  - Longest persistence: 2,982 days (8+ yrs)

- TrustWave GSR 2015
  - 81%
  - 86 days

- What does this mean?

First Steps

- There’s a wealth of data within the Registry that can help us fill in gaps in analysis
- Time stamped data => Log file

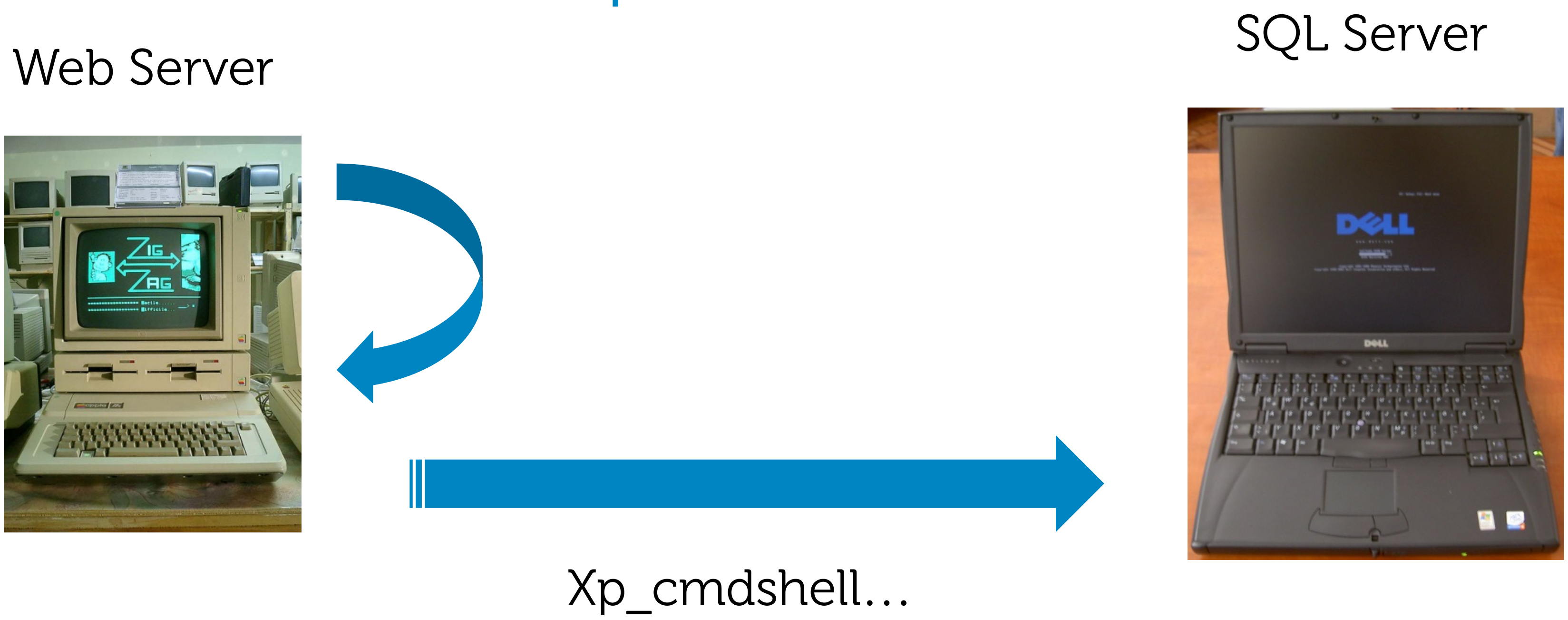
Registry Analysis – Why?

- Artifact Categories
  - Program execution
  - Lateral Movement
  - Malware (not associated with malware persistence)
  - User Activity
  - User Access To Files
- Can help obviate anti-forensics activities…

Registry Analysis – How?

- How do we “do” Registry Analysis?

Ex: Web Shell Loopback



Web Server

SQL Server

Xp_cmdshell…

- Threat actor had RDP access to both systems
- Installed web shell on web server
- Accessed web shell in IE, “hxxp://localhost/a.aspx”
- Created a user account on the SQL Server

Ex: Poison Ivy

Ex: Admin Cleanup

Ex: PCI

- Intruder had accessed employee’s home system, found that the employee accessed corp infrastructure via RDP
- Intruder accessed corp infrastructure via RDP/Term Services
- Total of 25 systems accessed; we knew:
  - Searches executed
  - Applications launched
  - Files accessed
- Demonstrated to PCI council that files containing PCI data had not been accessed
- Client received much reduced fine, didn’t have to notify

Ex: Remote Access

- Question of Remote Access via Terminal Services
- Analysis of the System Registry hive indicated that Terminal Services were not set to run/launch at startup

Things To Watch For…

- Unicode
  - RLO
  - 0xa0 (not space) vs 0x20 (space)

- Deleted keys/values

Questions?

Harlan Carvey

Work: hcarvey@secureworks.com

Not work: keydet89@yahoo.com

Dell SecureWorks