Windows Incident Response

The Windows Incident Response Blog is dedicated to the myriad information surrounding and inherent to the topics of IR and digital analysis of Windows systems. This blog provides information in support of my books; "Windows Forensic Analysis 2/e", "Windows Registry Forensics", "Windows Forensic Analysis Toolkit 3/e", as well as the book I co-authored with Cory Altheide, "Digital Forensics with Open Source Tools".

Monday, February 08, 2010

MFT Analysis

As an aside to timeline analysis, I've been considering the relative confidence levels inherent to certain data sources, something I had discussed with Cory. One of the things we'd discussed was the relative confidence level of file system metadata, specifically the timestamps in the $STANDARD_INFORMATION attribute versus those in the $FILE_NAME attribute. Brian Carrier addresses some specifics along these lines in chapter 12 of his *File System Forensic Analysis* book.

So, I've been looking at the output of tools like Mark Menz's MFTRipper and David Kovar's analyzeMFT.py tools. Based on the information in Brian's book and my chat with Cory, it occurred to me that quite a bit of analysis could be done automatically, using just the MFT and one of the two tools. One thing that could be done is to compare the timestamps in both attributes, as a means of possibly detecting the use of anti-forensics, similar to what Lance described here.

Another thing that could be done is to parse the output of the tools and build a bodyfile using the timestamps from the $FILE_NAME attribute only. However, this would require rebuilding the directory paths from just what's available in the MFT...that is, record numbers, and file references that include the parent record number for the file or folder. That's the part that I got working tonight...I rebuilt the directory paths from the output of David's tool...from there, it's a trivial matter to employ the same code with Mark's tool. And actually, that's the hardest part of the code...the rest is simply extracting timestamps and translating them, as necessary.

Also, I didn't want to miss mentioning that there's a tool for performing temporal analysis of the MFTRipper output from Mark McKinnon over at RedWolf Computer Forensics. I haven't tried it yet, but Mark's stuff is always promising.

Posted by Harlan Carvey at 11:53 PM

Reactions: valuable (1) interesting (0) meh (0)

Recommend this on Google

Labels: analysis, MFT

2 comments:

Phil Rodokanakis said...

Harlan:

I know you're a big Perl guy and I love what you've done with RegRipper. However, I'm sure you're aware that there are several EnScripts that do a pretty good job parsing out MFT records and reporting on the SI and FB Attributes. I'm wondering whether it would be possible to improve on those EnScripts to do the time analysis you describe.

6:40 PM

Pages

- Home
- Little Black Book of Windows Forensic Secrets
- Timelines
- Books
- Malware
- FOSS Tools

Subscribe To WindowsIR

Posts

Comments

WindowsIR Blog List

Linux Sleuthing
Searching for Searches

Microsoft® Malware Protection Center
The evolution of Rovnix: new Virtual File System (VFS)

Hacking Exposed Computer Forensics Blog
Daily Blog #316: Sunday Funday 5/4/14 Winner!

Grand Stream Dreams
Playing Nicely Now: Xplico 1.1.0 & Ubuntu 14.04 LTS

M-unition
An Intel Analyst's Key Takeaways from M-Trends: Beyond the Breach

Another Forensics Blog
What's the Word -

Keydet89 said...

Phil,

I'm sure that's the case.

I don't have EnCase.

6:44 PM

Post a Comment

Links to this post

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Thunderbird! - Parser that is....

Open Security Research
Recap of BYOD Risks

Journey Into Incident Response
Triaging with the RecentFileCache.bcf File

Yogesh Khatri's forensic blog
Search history on windows 8.1 - Part 2

4n6k
Forensics Quickie: Merging VMDKs & Delta/Snapshot Files (2 Solutions)

JL's stuff
Volatility Talk at Upcoming NYC4SEC

Computer Forensics, Malware Analysis & Digital Investigations
EnCase v7 EnScript to quickly provide MD5/SHA1 hash values and entropy of selected files

Forensic Artifacts
ActionVoip – Windows client

Trace Evidence
Analyzing Weaponized RTF Files

Malware Analysis Blog
Podcasts I listen to

Haft of the Spear
You Were Promised Neither Security Nor Privacy

Enterprise Detection & Response
Use of the term "Intelligence" in the RSA 2014 Expo

Digital Forensics Stream
Office 2013: More MRUs

System Forensics | System Forensics
Do not fumble the lateral movement

Digital Forensics Blog
Forensics 4cast Award Nominations

HeX-OR Forensics | Digital Forensics & Information Assurance
Part 6: USB Device Research – Open File Artifacts (LNK Files)

Volatility
Volatility Skills in High Demand!

Offensive Computing - Community Malicious code research and analysis
New Search System, No More Accounts Needed [1]

All things time related....
Visualize the Output

Digital Forensical | Discussion on Digital Forensics and Information Assurance
FIREBrick Build Part 1

fork()
Updates to GPS Utility (Timestamp Features)

dig4n6
VDI-in-a-Box Analysis Results

System Forensics
LastWriteTime and LastAccessTimes via Powershell

Sploited
SANS Forensic Artifact 7: Last Visited MRU

Digital Forensics Solutions
Registry Decoder 1.4 Released and Updated Registry Decoder Live

Blog Archive

► 2014 (12)

► 2013 (64)

► 2012 (73)

- ▶ 2011 (109)
- ▼ 2010 (90)
  - ▶ December (12)
  - ▶ November (5)
  - ▶ October (3)
  - ▶ September (2)
  - ▶ August (3)
  - ▶ July (10)
  - ▶ June (9)
  - ▶ May (5)
  - ▶ April (8)
  - ▶ March (10)
  - ▼ February (15)
    - More on AV write-ups
    - Researching Artifacts
    - IT firm looses...a lot!
    - Fun Analysis Stuff
    - More Links, and a Thanks
    - Links Plus
    - MFT Analysis
    - Timeline Analysis...do we need a standard?
    - Is anyone doing timeline analysis??
    - How Did THAT Get There???
    - Forensic Analysis and Intel Gathering
    - More Thoughts on Timeline Analysis
    - A Conference By Any Other Name...
    - Some New Stuff
    - Forensic Analysis Process/Procedures
  - ▶ January (8)
- ▶ 2009 (166)
- ▶ 2008 (108)
- ▶ 2007 (83)

- ► 2006 (118)
- ► 2005 (163)
- ► 2004 (16)