ZeroAccess analysis with OSForensics

By Russ McRee – ISSA member, Puget Sound (Seattle), USA Chapter

Join the Discussion
Connect

Prerequisites

Windows

Happy New Year: "A New Year's resolution is something that goes in one year and out the other." - Author Unknown

December is the time of year when I post the *Toolsmith Tool of the Year* survey for reader's to vote on their favorite tool of the given year. Please do take a moment to vote.[1] What's nice is that I often receive inquiries from tool developers who would like consideration for coverage in *toolsmith*. David Wren, Managing Director of PassMark Software, caught me at just the right moment as I was topic hunting for this month's column. PassMark, out of Sydney, Australia, has been known for benchmark and diagnostic tools but has recently dipped its tow in the digital forensics pool with OSForensics.[2] I give PassMark props for snappy marketing. OSForensics, "Digital Investigation for a new era" coupled with the triumvirate of Discover, Identify, and Manage makes for a good pitch, but as always we need tools that do as they do, not as they say. So what can we expect from OSForensics? According to David, who provided me with requisite vendor/developer content, the pending 1.1 release of OSForensics, expected in mid-January 2012 will include:

- Inclusion of a tree-view style file system browser (Windows Explorer replacement).
- Indexing and searching of the contents of email attachments. At the moment just the email content and the file names of attachments are indexed.
- Improvements to add search results to a case directly from search history (efficiency improvement).
- Ability to add quick notes to a case. At the moment adding arbitrary notes is a two-step process.
- Improvements in the built-in image viewer. Better quality image scaling and more file properties.
- Minor improvements in the way emails are exported.
- Significant speed improvements in the window's registry browser.
- A bug fix for handling of dates in Spanish language emails.
- Some minor documentation changes.

Existing features include disk imaging, disk image mounting, raw hex view of disk, manual carving, a registry viewer, forensic copy of network files, testing and zeroing of external drives prior to imaging, file hashing, live memory dumping, detection of files with wrong extensions via signatures, case management, reporting, 64bit support, and more.

The OSForensics website has an extensive FAQ as well excellent videos and tutorials.

Please note that there is a Free Edition and a Pro Edition. For this article I tested the 1.0 Pro version of OSForensics.

Integrating additional tools into OSForensics

One of the things I like most about OSForensics is the ability to plug in other tools. There's a great tutorial for enhancing OSForensics with Harlan Carvey's RegRipper[3] that will give you a solid starting point for this activity. Friend and reader Jeff C. expressed interest in rootkit analysis this month, so I'm going to use this opportunity to integrate GMER[4] and RootkitRevealer[5] into OSForensics.

As I ran OSForensics on a Windows XP system from a USB key, I copied GMER and RootkitRevealer to `E:\OSForensics\AppData\SysInfoTools`.

I then navigated to *System Information* in the OSForensics UI, selected *Add List* and created a Rootkit Analysis list, followed *Add* under *Commands* and added the command to execute GMER and RootkitRevealer as seen in Figure 1 (next page).

Keep in mind, you can add any of your preferred tools to OSForensics and their execution as well as their output will be captured as part of OSForensics case management capabilities.

Running OSForensics

For ease of viewing, right-click the menu on the left side of the OSForensics UI and choose "thin buttons" as this will present all options without scrolling.

1 http://holisticinfosec.blogspot.com/2011/12/choose-2011-toolsmith-tool-of-year.html.

2 http://www.osforensics.com/.

3 http://regripper.wordpress.com/.

4 http://www.gmer.net/.

5 http://technet.microsoft.com/en-us/sysinternals/bb897445.

©2012 Information Systems Security Association • www.issa.org • editor@issa.org • Permission for author use only.

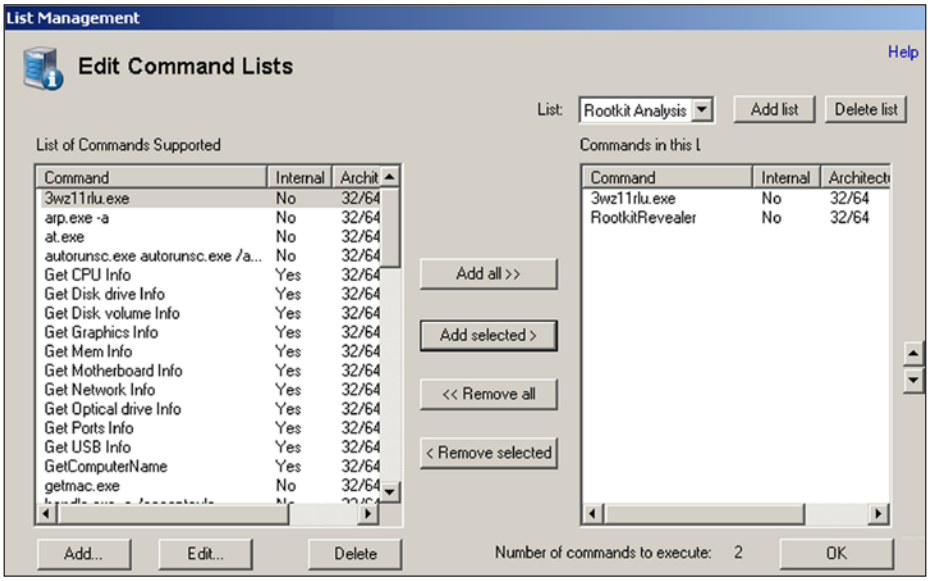

Figure 1 – Rootkit Analysis tools added

One note of interest before diving in: OSForensics allows installation on a base analysis system from which you can then install to USB so as to run it from a USB key as part of your field kit as seen in Figure 2.

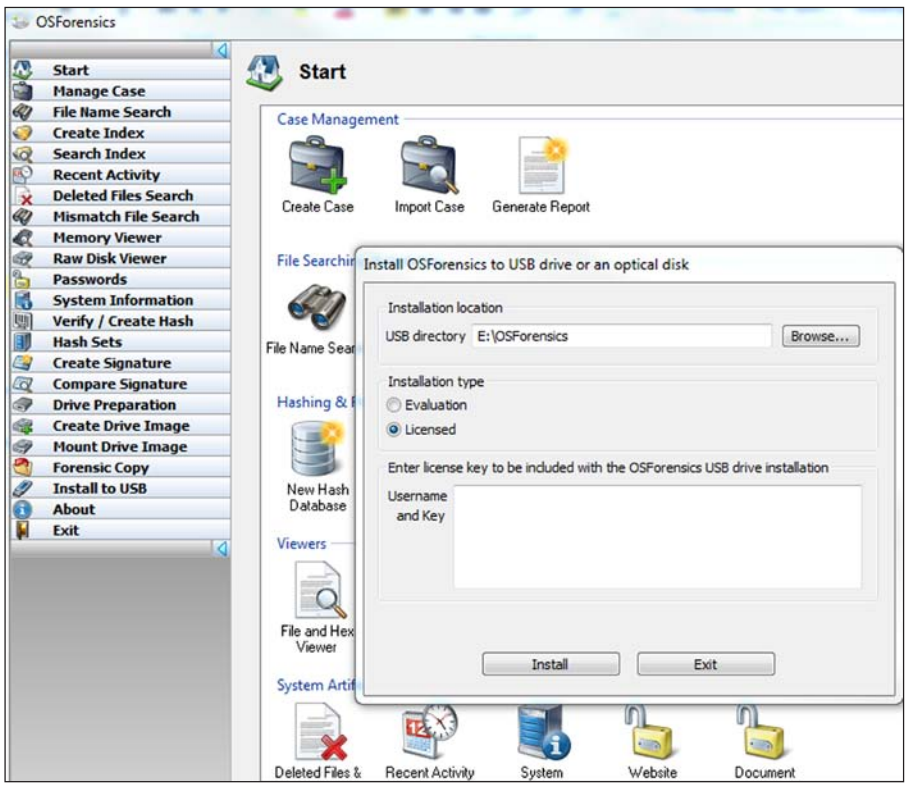

Figure 2 – Install OSForensics to a USB key

Jeff, as part of his expressed interest in rootkit analysis, also provided me with a perfect sample with which to compromise my test system. Nomenclature for this little nugget includes *Jorik* and *Sirefef* but you may now it best as *Zaccess* or *ZeroAccess*. To read a truly in-depth study of ZeroAccess, check out Giuseppe Bonfa's fine work in four parts over at Infosec Resources,[6] as well as a recent update from Pedro Bueno on the ISC Diary.[7] ZeroAccess has been rolled into the BlackHole Exploit Kit and is often used in crimeware bundles for ad clicking.

This particular sample

(MD5: 3E6963E-23A65A38C5D565073816E6BDC)

is VMWare-aware, so I targeted my Windows XP SP 3 system running Windows Steady State and executed QuickTimeUpdate.exe (it only plays a real QuickTime update on TV).

As with any tool of OSForensic's ilk, I started the process by creating a case which is as easy clicking *Start* then *Create Case*. The OSForensics UI is insanely intuitive and simple; if you're one of those who refuses to read manuals, FAQs, and/or tutorials, you'll still get underway in short order. With most forensics-oriented multi-functional tools that include indexing, I always make indexing my second process. Yep, it's as easy as *Create Index*. I infected this system on 12/26/11 at 1630 hours, so a great next step for me was to review *Recent Activity* to see what was noteworthy. Based on a date range-limited search under Recent Activity, I noted a significant spike in events in the 1600 hour. I right-clicked on the resulting histogram for the hour of interest and selected *Show These Files*. The result, as seen in Figure 3, shows all the cookies spawned when ZeroAccess tapped into all its preferred ad channels. All cookies in Figure 3, including those for switchadhub.com, demdex.com, and displayadfeed.com, were created right on the heels of the infection at 1630 hours. These are services malware writers use to track clicks and campaign success.

I had not browsed to any websites and on this host would have done so via a browser other than Internet Explorer; as such this activity as written to `C:\Documents and Settings\LocalService\LocalSettings\Temporary Internet Files\Content.IE5` clearly occurred in the background.

I always take a network capture during malware runtime and the resulting PCAP acquired while analyzing this version of

6 http://resources.infosecinstitute.com/step-by-step-tutorial-on-reverse-engineering-malware-the-zeroaccessmaxsmiscer-crimeware-rootkit/.

7 http://isc.sans.edu/diary.html?storyid=12079.

©2012 Information Systems Security Association • www.issa.org • editor@issa.org • Permission for author use only.

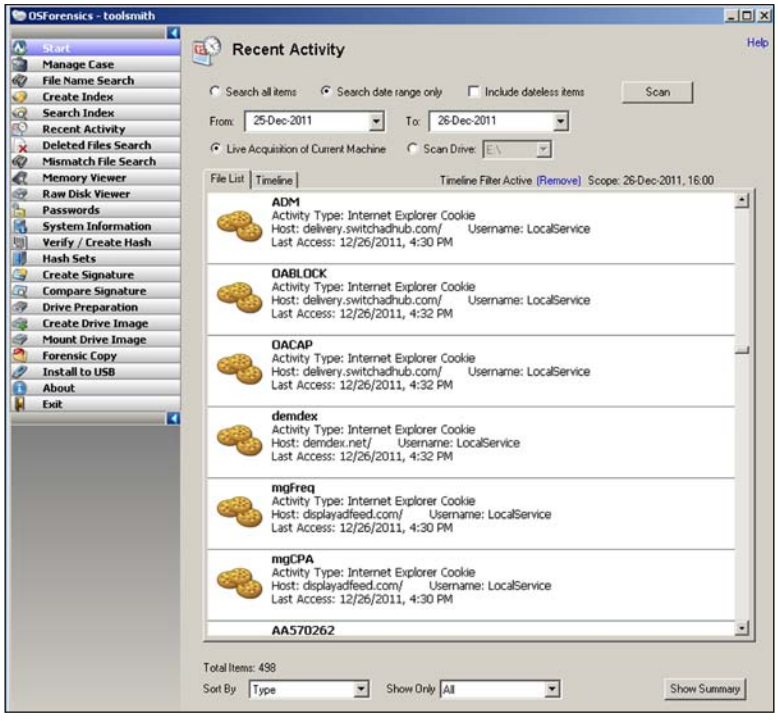

Figure 3 – ZeroAccess' malicious click campaign evidence via OSForensics

ZeroAccess included connections to a well-known malware redirection service at 67.201.62.*. Search "67.201.62" malware and you'll see what I mean.

I then opted to call GMER from OSForensics as discussed earlier during Integration. If you're not familiar, GMER is the defacto standard for rootkit detection. Once a GMER scan is complete, you can choose to dump detected modules as seen in Figure 4 via *Dump* module.

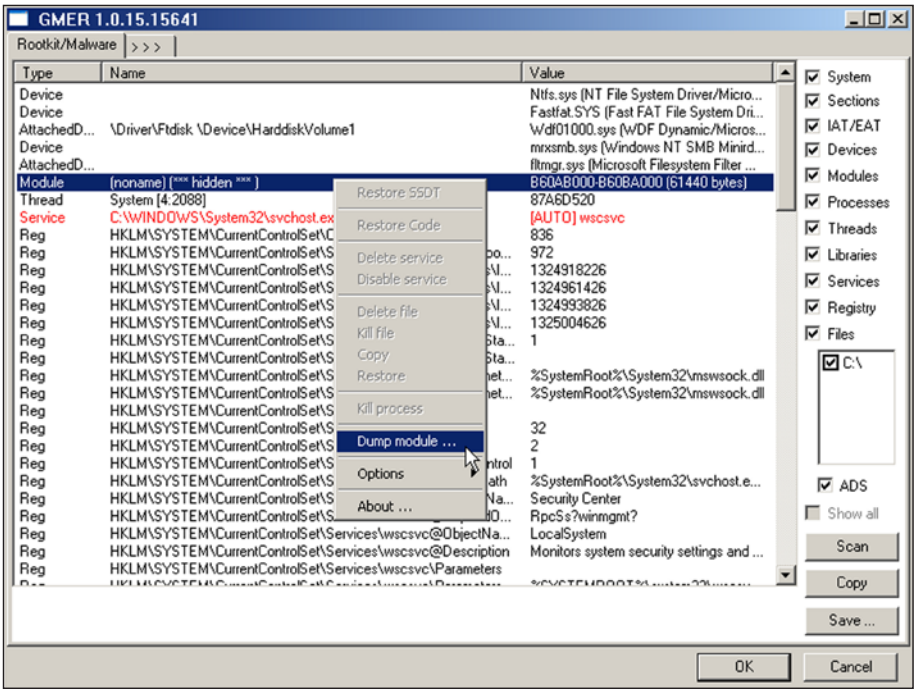

Figure 4 – GMER bags ZeroAccess via OSForensics

I fed the resulting binary file to *VirusTotal* and was rewarded for my efforts with hits for `Gen:Variant.Sirefef.38`, a ZeroAccess variant.

OSForensics features a Memory Viewer from which you can conduct similar activity natively by selecting a given process (one you assume or have determined is malicious); select one of four dump options including *Dump Process Memory Contents*, then click *Dump*. The resulting `.bin` can be fed to VirusTotal or a similar service.

But alas, you will not have made the utmost use of OSForensics if you don't capitalize on *Hash Sets*. I won't get into great detail as to how to do so as again the tutorial videos are excellent. You will want to enable a given hash set by selecting it in the UI then clicking *Make Active*. One of the hash sets PassMark offers via download is a 124kb common keyloggers hash set.[8] You can select a directory via *File Name Search*, then *Search*, then right-click a file of interest (or CTRL-A to select all) and choose *Look Up in Hash Set*. As none of the acquired binaries for ZeroAccess matched the current hash set, I chose to scan my Lurid[9] (the APT) analysis folder to see what matches the hash set had for me. I used the *Sorting* menu in the lower right-hand corner of the UI and set it to *In Hash Sets*; the results are seen Figure 5 (next page).

While OSForensics claimed to have matches, they were only for 0 byte files that all show up with the MD5 hash of D41D8CD98F00B204E9800998ECF8427E. I'll test this further with a known keylogger and determine what a real match looks like. I don't fault OSForensics for this as I likely don't have a sample keylogger whose hash matched the hash set. Trying hash matching against known good system files worked admirably.

I didn't even touch OSForensics password analysis capabilities but will also likely do so in a future blog post. Do check out that feature set via *Passwords* for yourself and share your feedback. Recognize that OSForensics integrates Rainbow Tables so as you can imagine, the possibilities are endless.

Don't forget the expected disk image analysis capabilities coupled with file carving. I tested this briefly (and successfully) only to confirm what I consider a required and standard feature for tools of this nature.

8 http://www.osforensics.com/download.html.

9 http://blog.trendmicro.com/trend-micro-exposes-lurid-apt/.

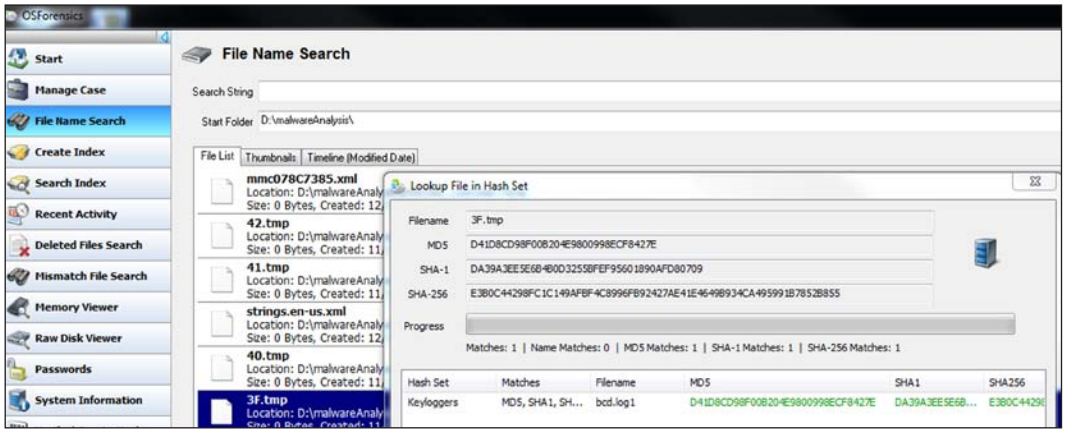

Figure 5 – Keylogger hashset checks

In conclusion

I'll admit I had no expectations for OSForensics as I had no prior experience with it, and to be quite candid, no awareness prior to David contacting me. I always assume some risk when choosing such a tool, given that I could spend hours conducting research and analysis only to find the tool does not meet the standard for *toolsmith* discussion (can you say "emergency topic change"?). Such was not the case with OSForensics. I was pleased with the results, disappointed I didn't have more time to spend on it before writing about it here, but looking forward to making much more use of it in the future. As always, let me know what you think, I'm hopeful you find it as intriguing as I have.

Ping me via email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

Acknowledgements

—David Wren, Managing Director, PassMark Software

About the Author

Russ McRee, GCIH, GCFA, GPEN, CISSP, is team leader and senior security analyst for Microsoft's Online Services Security Incident Management team. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ at holisticinfosec dot org.

©2012 Information Systems Security Association • www.issa.org • editor@issa.org • Permission for author use only.