



Redline: APT1 and You – We’re All Owned



Redline

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

Prerequisites/dependencies

Windows OS and .NET 4

Embrace this simple fact, we’re all owned. Maybe you aren’t right now, but you probably were at some point or will be in the future. “Assume compromise” is a stance I’ve long embraced; if you haven’t climbed aboard this one-way train to reality, I suggest you buy a ticket. If headlines over the last few years weren’t convincing enough, Mandiant’s *APT1, Exposing One of China’s Cyber Espionage Units*¹ report should serve as your re-education. As richly detailed, comprehensive, and well-written as it is, this report is groundbreaking in the extent of insights on our enemy it elucidates, but not necessarily as a general concept. Our adversary has been amongst us for many, many years and the problem will get much worse before it gets better. They are all up in your grill, people; your ability to defend yourself and your organizations, and to hunt freely and aggressively is the new world order. I am reminded, courtesy of my friend TJ O’Connor, of a most relevant Patton quote: “a violently executed plan today is better than a perfect plan expected next week.” Be ready to execute. *Toolsmith* has spent six and half years hoping to enable you, dear reader, to execute; take the mission to heart now more than ever.

I’ve covered Mandiant tools before for good reason: Red Curtain in 2007,² Memoryze in 2009,³ and Highlighter in 2011.⁴ I stand accused of being a fanboy⁵ and hereby render myself guilty. If you’ve read the APT1 report you should have taken immediate note of the use of Redline and Indicators of Compromise (IOCs) in Appendix G.

Outreach to Richard Bejtlich, Mandiant’s CSO, quickly established goals and direction: “Mandiant hopes that our free Redline tool will help incident responders find intruders on their network. Combining indicators from the APT1 report with Redline’s capabilities gives responders the ability to look for interesting activity on endpoints, all for free.” Well in keeping with the *toolsmith*’s love of free and open source tools, this conversation led to an immediate connection with

Ted Wilson, Redline’s developer, who kindly offered his perspective:

Working side by side with the folks here at Mandiant, who are out there on the front lines every day, is definitely what has driven Redline’s success to date. Having direct access to those with firsthand experience investigating current attack methodologies allows us stay ahead of a very fast moving and quickly evolving threat landscape. We are in an exciting time for computer security, and I look forward to seeing Redline help new users dive headfirst into computer security awareness.

Redline has a number of impressive features planned for the near future, focusing first on expanding the breadth of live response data Redline can analyze. Some highlights from the next Redline release (v1.8) include full file system and registry analysis capabilities, as well as additional filtering and analysis tools around the always popular Timeline feature. Further out, we hope to leverage that additional data to provide expanded capabilities that help both the novice and the expert investigators alike.

Mandiant’s Lucas Zaichkowsky, who will have presented on Redline at RSA by the time you read this, sums up Redline’s use cases succinctly:

1. Memory analysis from a live system or memory image file. Great for malware analysis.
2. Collect and review a plethora of forensic data from hosts in order to investigate an incident. This is commonly referred to as a Live IR collector.
3. Create an IOC search collector to run against hosts to see if any IOCs match.

He went further to indicate that while the second scenario is the most common use case, in light of current events (APT1), the third use case has a huge spotlight on it right now. This is where we’ll focus this discussion to utilize the APT1 IOC files and produce a collector to analyze an APT1 victim.

Installation and preparation

Mandiant provides quite a bit of material regarding preparation and use of Redline including an extensive user guide⁶ and two webinars⁷ well worth taking the time to watch. Specific

1 http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

2 <http://holisticinforesec.org/toolsmith/docs/december2007.pdf>

3 <http://holisticinforesec.org/toolsmith/docs/february2009.pdf>

4 <http://holisticinforesec.org/toolsmith/pdf/october2011.pdf>

5 <https://www.mandiant.com/blog/highlighter-super-users-series-post-2/>

6 http://www.mandiant.com/library/Redline1.7_UserGuide.pdf

7 <http://www.mandiant.com/events/webinar/tools-of-engagement-redline-weve-got-the-tool-if-youve-got-the-time> & <http://www.mandiant.com/events/webinar/tools-of-engagement-redline>

to this conversation, however, with attention to APT1 IOCs we must prepare Redline for a targeted *Analysis Session*. The concept here is simple: install Redline on an analysis workstation and prepare a collector for deployment to suspect systems.

To begin, download the entire *Digital Appendix & Indicators*⁸ archive associated with the APT1 report.

Wesley McGrew (McGrew Security) put together a great blog post⁹ regarding matching APT1 malware names to publicly available malware samples from VirusShare¹⁰ (which is now *the* malware sample repository). I’ll analyze a compromised host with one of these samples, but first let’s set up Redline.

I organize my Redline file hierarchy under `\tools\redline` with individual directories for *audits*, *collectors*, *IOCs*, and *sessions*. I copied *Appendix G (Digital) – IOCs* from the above mentioned download to APT1 under `\tools\redline\IOCs`.

Open Redline, and select *Create a Comprehensive Collector* under *Collect Data*. Select *Edit Your Script* and enable *Strings* under *Process Listing and Driver Enumeration*, and be sure to check *Acquire Memory Image* as seen in figure 1.

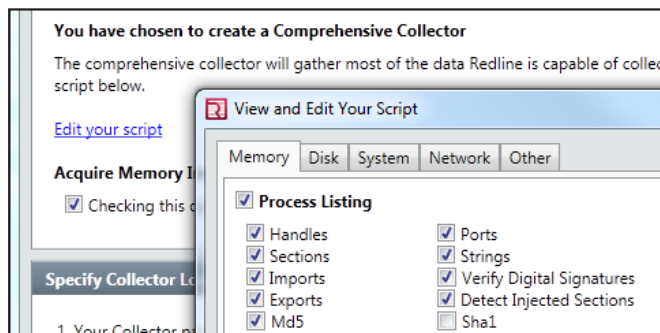


Figure 1 – Redline script configuration

I saved the collector as *APT1comprehensive*. These steps will add a lot of time to the collection process but will pay dividends during analysis. You have the option to build an *IOC Search Collector* but by default this leaves out most of the acquisition parameters selected under *Comprehensive Collector*. You can (and should) also add analysis inclusive of the IOCs after acquisition during the *Analyze Data* phase.

Redline, IOCs, and a live sample

I grabbed the binary `034374db2d35cf9da6558f54cec8a455` from VirusShare, described in Wesley’s post as a match for BISCUIT malware. BISCUIT is defined in *Appendix C – The Malware Arsenal* from *Digital Appendix & Indicators* as a backdoor with all the expected functionality including gathering system information, file download and upload, create or kill processes, spawn a shell, and enumerate users.

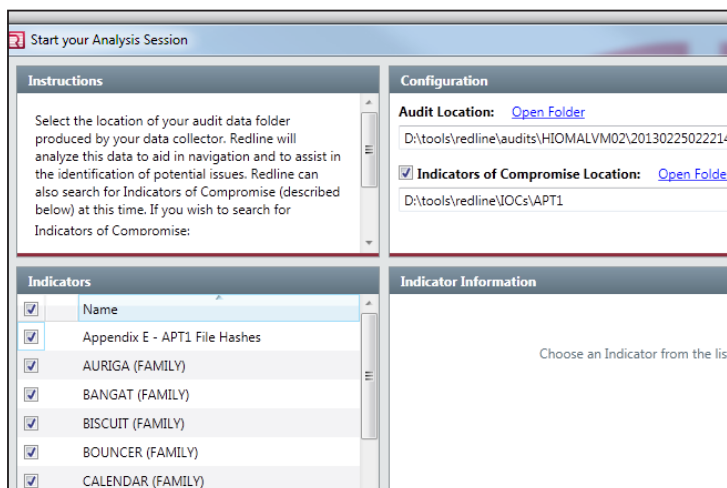


Figure 2 – Analyze collector results with Redline

I renamed the binary `gc.exe`, dropped it in `C:\WINDOWS\system32`, and executed it on a virtualized lab victim. I rebooted the VM for good measure to ensure that our little friend from the Far East achieved persistence, then copied the collector created above to the VM and ran *RunRedlineAudit.bat*. If you’re following along at home, this is a good time for a meal, walking the dog, and watching *The Walking Dead* episode you DVR’d (it’ll be awhile if you enabled strings, as advised). Now sated, exercised, and your zombie fix pulsing through your bloodstream, return to your victim system and copy back the contents of the audits folder from the collector’s file hierarchy to your Redline analysis station, select *From a Collector* under *Analyze Data*, and choose the copied audit as seen in figure 2.

Specify where you’d like to save your Analysis Session (`D:\tools\redline\sessions` if you’re following my logic). Let Redline crunch a bit and you will be rewarded with instant IOC goodness. Right out of the gate the report details indicated that “2 out of my 47 Indicators of Compromise have hit against this session.”

Sweet, we see a file hash hit and a BISCUIT family hit as seen in figure 3 (next page).

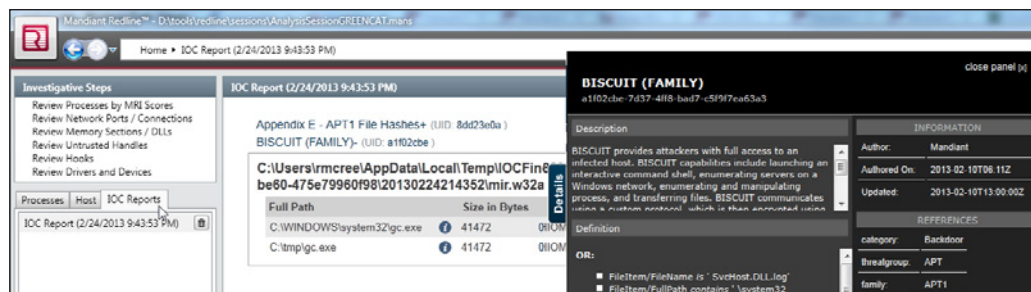
Your results will also be written out to HTML automatically. See *Report Location* at the bottom of the Redline UI. Note that the BISCUIT family hit is identified via UID `a1f02cbe`. Search `a1f02cbe` under your IOCs repository and you should see a result such as `D:\tools\redline\IOCs\APT1\a1f02cbe-7d37-4ff8-bad7-c5f9f7ea63a3.ioc`.

Open the `.ioc` in your preferred editor and you’ll get a feel for what generates the hits. The most direct markup match is:

```
<IndicatorItem id="c9032003-14c2-4437-a0e8-ab5a54f975f3" condition="is">
<Context document="FormItem" search="FormItem/Md5sum" type="mir" />
<Content type="md5">034374db2d35cf9da6558f54cec8a455</Content>
</IndicatorItem>
```

8 http://intelreport.mandiant.com/Mandiant_APT1_Report_Appendix.zip.
 9 <http://www.mcgresecurity.com/2013/02/19/rough-mapping-of-mandiant-apt1-malware-names-to-available-samples/>.
 10 <http://virusshare.com/>.

Figure 3 – 2 IOC hits against the Session



In the Redline UI, remember to click the little blue button with the embedded “i” (information) associated with IOC hit for highlights on the specific IndicatorItem that triggered the hit for you and displays full metadata specific to the file, process, or other indicator.

But wait, there’s more. Even without defined, parameterized IOC definitions, you can still find other solid indicators on your own. I drilled into the *Processes* tab, and selected *gc.exe*, expanded the selection, and clicked *Strings*. Having studied *Appendix D – FQDNs*, and checked out the *PacketStash APT1.rules*¹¹ file for Suricata and Snort (thanks, Snorby Labs), I went hunting (CTRL-F in the Redline UI) for strings matches to the known FQDNs. I found 11 matches for *purpledaily.com* and 28 for *newsnet.net* as seen in figure 4.

Great! If I have alert `udp $HOME_NET any -> $EXTERNAL_NET 53 (msg:"[SC] Known APT1 domain (purpledaily.com)"; content:"|0b|purpledaily|03|com|00|"...snipped enabled on my sensors, I should see all the other systems that may be pwned with this sample.`

Be advised that the latest version of Redline (1.7 as this was written) includes powerful, time-related filtering options including *Field Filters*, *TimeWrinkle*, and *TimeCrunch*. Explore

¹¹ <https://github.com/packetstash/packetstash-rules/blob/master/APT1/apt1.rules>.

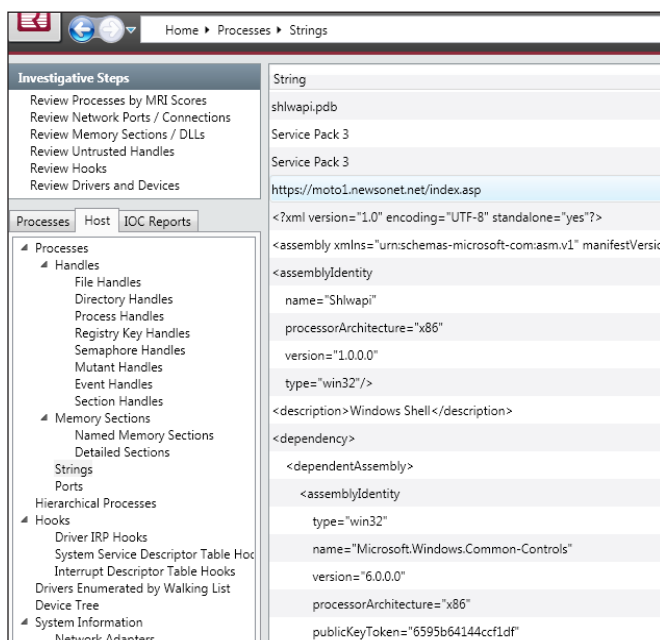


Figure 4 – Strings yields matches too

them as you seek out APT1 attributes. There are lots of options for analysis. Read the *Redline Users Guide* before beginning so as to be fully informed. :)

In conclusion

I’m feeling overly dramatic right now. Ten years now

I’ve been waiting for what many of us have known or suspected all along to be blown wide open. APT1, presidential decrees, and “it’s not us,” oh my. Mandiant has offered both the fodder and the ammunition you need to explore and inform, so awake! I’ll close with a bit of the Bard (Ariel, from *The Tempest*):

*While you here do snoring lie,
Open-ey’d Conspiracy
His time doth take.
If of life you keep a care,
Shake off slumber, and beware.
Awake, awake!*

I am calling you to action and begging of your wariness; your paranoia is warranted. If in doubt of the integrity of a system, hunt! There are entire network ranges that you may realize you don’t need to allow access to or from your network. Solution? Ye olde *deny* statement (thanks for reminding me, TJ). Time for action; use exemplary tools such as Redline to your advantage, where advantages are few.

Ping me via email if you have questions or suggestions for topic via russ@holisticinfosec.org or hit me on Twitter @holisticinfosec.

Cheers...until next month.

Acknowledgements

To the good folks at Mandiant:

—Ted Wilson, Redline developer

—Richard Bejtlich, CSO

—Kevin Kin and Lucas Zaichkowsky, Sales Engineers

About the Author

Russ McRee manages the Security Analytics team (security incident management, penetration testing, monitoring) for Microsoft’s Online Services Security & Compliance organization. In addition to toolsmith, he’s written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ@holisticinfosec.org or @holisticinfosec.