Join the Discussion
Connect

NetWitness Investigator

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

Prerequisites

Windows operating system (XP/2003 or later)

As I write this month's column I'm on a plane returning from the 22nd Annual FIRST Conference in Miami. As always, in addition to a collection of the world's finest computer incident response teams, there was a select number of vendors. I will be honest when I admit that I typically avoid conference vendor booths unless the swag is really good, but some of my favorites were in attendance, including Mandiant and Secunia. When I noticed the NetWitness booth I was reminded of the suggestions I'd heard suggesting NetWitness Investigator as a *toolsmith* topic. During Robert Rounsavall's FIRST presentation, "Forensics considerations in next generation cloud environments," he made mention of the fact that the Terremark teams make use of NetWitness offerings on their high throughput network capture platforms. Incident responders, network analysts, and security engineers typically can't get enough of good network capture tools; the reminder triggered by the NetWitness booth presence clearly indicated that the time had come.

Specifically, NetWitness Investigator is part of a suite of products offered by NetWitness that are designed to capture network traffic and use the resulting data for business and security problem analysis. Others include Administrator, Decoder, Concentrator, Broker, Informer, and the NwConsole. Most NetWitness applications are commercial offerings, but Investigator is freely available and quite useful.

Installing and configuring NetWitness Investigator

Installation is point-and-click simple. Accept defaults or modify installation paths as you see fit. You will need to register the Computer ID generated for the host on which you're installing that is generated as part of the license key. Provide a valid email address; you'll be sent a link to activate your installation for first use.

Keep in mind that by default NetWitness Investigator does phone home for new updates and will reach out to the NetWitness web service to offer you the most recent FAQs, news and community posts in the Welcome Page.[1] If you prefer otherwise select *Edit*, then *Options*, and uncheck *Automatically Check for Updates* as well as *Allow Investigator to Reach Internet*.

If you don't have WinPcap installed you will be prompted to do so; WinPcap 4.1.1 is bundled with the installation package.

Under *View* be sure to enable the *Capture Bar* as it will present a Capture icon and Collection selector at the bottom of the NetWitness Investigator UI.

You can also pre-define the interface from which you'd like to capture via the *Options* menu as described above.

Using NetWitness Investigator

The NetWitness Investigator (NI) Welcome Page provides useful FAQ; read it as you get underway.

NI allows you to either capture data directly from the host network interfaces, including wireless adapters, or import network captures from other sources and its use is built around Collections. The free version of NI doesn't offer *Remote Collections* as they are specific to retrieving data gathered by other NetWitness commercial offerings. That said you can create *Local Collections*.

Ctrl + L will pull up the new Local Collection UI; you can also click *Collection*, then *New Local Collection* from the menu bar or click the create icon from the Collection toolbar.

I called my collection *bredolab* (you'll learn why shortly) and will refer to it hereafter.

Once you create a collection right-click it, then connect to it.

You know have two options, *capture* or *import*.

Capture

To capture, use the *Capture Bar*, select the already-created Collection or create a new by collecting the Capture icon first. Once you click the Capture icon, NI will cap-

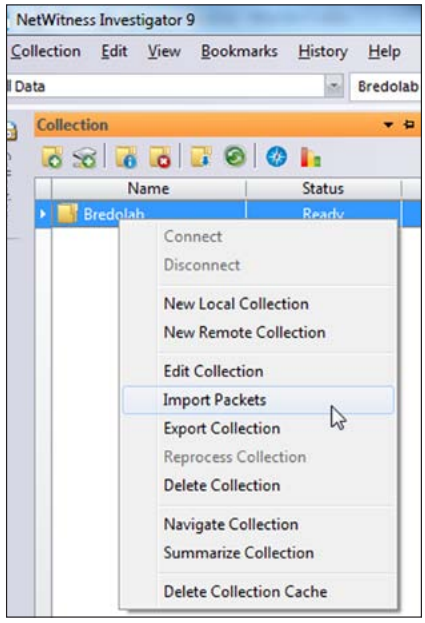

Figure 1 – Configuring NetWitness Investigator.

1 NetWitness® Investigator User Guide, p. 22.

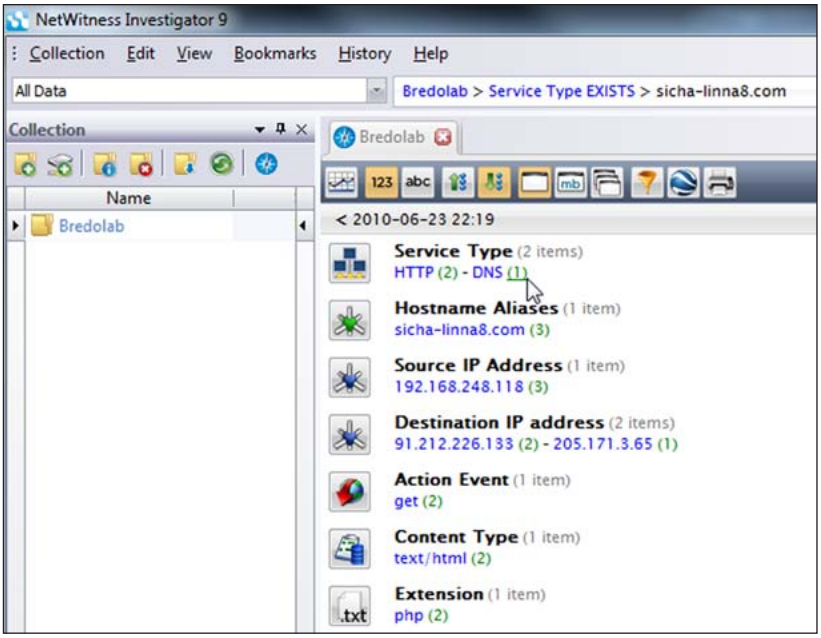

Figure 2 –Bredolab sample collection navigation.

ture network data until you click the Capture icon again to halt the process.

Import

Right-click the already-created Collection to add data via the *Import Packets* options (Figure 1).

Select a PCAP file from your local file system, and click *Open*.

I worked primarily with imported PCAPs, though testing NI's capture capability proved successful. I did find that in resource-limited virtual environments capturing network traffic with NI causes fairly significant VM grind.

As I was testing NI in the *toolsmith* lab, a golden opportunity to put it though its motions presented itself via the SANS ISC Diary.[2] The Lenovo support site had been discovered to be compromised and propagating the Bredolab Trojan[3] via an embedded IFRAME.[4] As I had literally just been to the Lenovo site to update my laptop BIOS (I had not experienced the malicious behavior), I was pleased with the near real-time relevance and the opportunity to check NI against a new sample. The CyberInsecure article[5] called out the exact malware URL that the IFRAME pointed to (hxxp://volgo-marun.cn/pek/exe.exe) so I grabbed it immediately via my malware sandbox VM. After firing up Wireshark on my VM server, I executed exe.exe (great name) and captured the resulting traffic. I imported the resulting `bredolab.pcap` (email me if you'd like a copy) into NI and compared results against details provided in the Lenovo compromise article. While this is a really small PCAP it serves well in exemplifying NI features.

Claim: The malware "receives commands from C&C server with domain sicha-linna8.com."

Validation: Check. Right out of the gate we can see sicha-linna8.com as part of the *Collection Navigation* view, under *Hostname Aliases* (Figure 2).

Left-click the Hostname Alias result to drill into it.

Right-click it to evoke bonus functionality such as SANS IP History, SamSpade, and CentralOps.

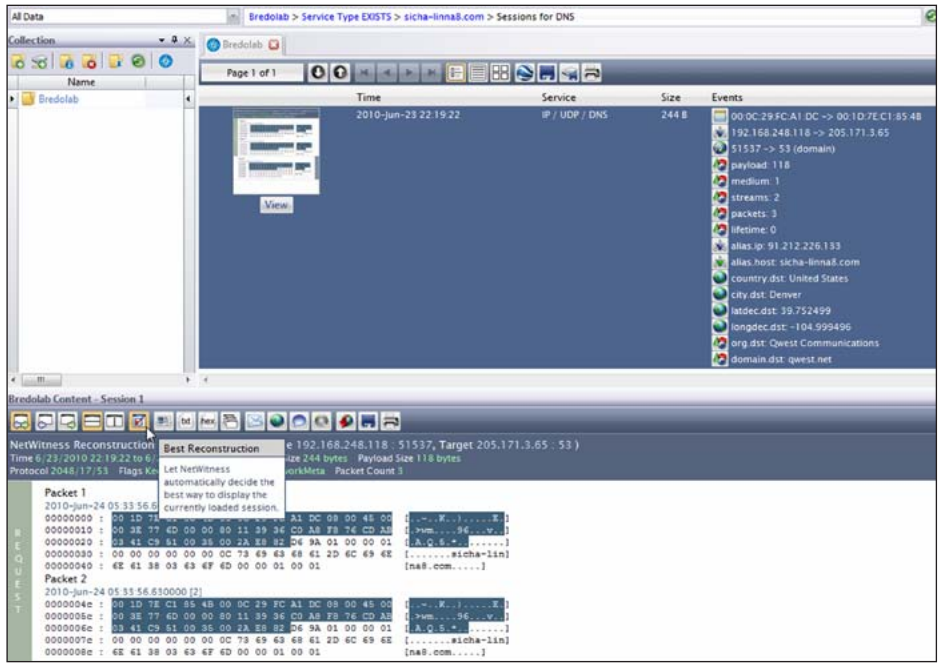

Figure 3 – DNS session content.

Drilling in the Hostname Alias entry reduces the *Service Type* findings to just HTTP and DNS traffic which is useful as they are the primary services of interest with this sample. As seen in Figure 3, we can drill further into the single referenced DNS session. The resulting *Session* view, using the *Hybrid* option, shows us both a thumbnail view and session

2 http://isc.sans.edu/diary.html?storyid=9049.

3 http://www.virustotal.com/analisis/ca4727bf9c5ec08807452fa5e549989012842ddc665034e135da1cddb3526a3e-1277396819.

4 http://blog.bkis.com/en/lenovo-download-site-infected-with-bredolab-botnet.

5 http://cyberinsecure.com/lenovo-support-website-loads-malicious-iframe-infects-visitors-with-trojan.

Figure 4 – Google Earth view of DNS request domain location.

details. Further *Content* options are presented in the lower pane with additional functionality such as, were it relevant, rebuilding instant messaging (IM) and audio, as well as mail and web content reconstruction. The *Best Reconstruction* option is tidy; it organizes into the three packets for the DNS session represented as the two request packets (as hex) and the response from server.

You can make use of Google Earth as well, if installed. But be sure to default your private IP addresses to your local latitude and longitude. As if we hadn't already imagined or determined it so, sicha-linna8.com is attributed to the Russian Federation (RU).

Click the Google Earth icon in the Session view.

Satellite imagery does a fair job of bearing that out, although unless I'm mistaken, Figure 4's reference pointer looks to be more like China.

Figure 5 – Hello, I'm a bot.

Now, I'm just being silly here, but again NI justifies my being so with its capabilities.

As mentioned above, the malware "receives commands from C&C server." Hmm, that sounds like a bot. Duh, ok Russ, prove it. Navigate back to the Collection summary via the URL window, scroll down to the *Querystring* reference and click [open]. See, I told you so.

That would be the HTTP GET equivalent of calling home to the mothership and requesting mission orders. As if `action=bot` and `action=report` weren't enough for you, the fact that the *Filename* reference in Figure 5 is also `controller.php` really helps you reach a reasonable conclusion.

By the way, Trend Micro's Bredolab summary (not specific to this sample) will give a good understanding of its behavioral attributes, but there should be no surprises.

There are endless additional features including the use of breadcrumbs to help you leave a trail as you navigate through large captures, excellent reporting capabilities, as well as the ability export sessions to a file (PCAP, CSV, XML, HTML, etc.) or a new or different collection.

If you click *Help*, you'll be offered the 168 page *NetWitness Investigator User Guide*, which will do this tool far more justice than I have. Consider it required reading before going too far down the rabbit hole on your own.

In conclusion

There's much more that I could have covered for you regarding NetWitness Investigator, would time and space have allowed it, but hopefully this effort will get you cracking with this tool if you haven't already partaken.

NetWitness Investigator is really slick and I'm pleased enough with it to declare it a candidate for the 2010 Toolsmith Tool of the Year to be decided no later than January 2011.

Check it out for yourself and let me know what you think.

Cheers…until next month.

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@holisticinfosec.org.