Browse This: Oryon C Portable & WhiteHat Aviator

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

Please take a moment as you read this *toolsmith* to honor those lost in the Oso, WA, landslide disaster and those who have lost loved ones, friends, and homes. *Pro Civitas et Patria*.[1]

Prerequisites/dependencies

—Windows for Oryon C Portable

—Mac OS X or Windows for WhiteHat Aviator

Spring is upon us and with April comes a focus on Security and Cloud Computing in the *ISSA Journal,* and as such a focus on security-centric, Chromium-based web browsers in *toolsmith*. It also freaks me out just a bit to say this but with April also comes the **90th consecutive *toolsmith***. I sure hope you enjoy reading it as much as I do writing it; it's been a fabulous seven year plus journey so far.

Those of you who enjoy the benefits of rich web content, fast load times, and flexible browser extensibility have likely tried or use the Chrome browser. What you may not be aware of is that there are other Chromium-based browsers that are built with a bit more attention to privacy than might be expected from Chrome proper.

Full disclosure right up front: as a reminder, I work for Microsoft, and the one thing this article won't be is any kind of a knock on Google Chrome privacy posture or a browser comparison beyond these two Chromium variants. There are plenty of other battles to fight than one in the Browser Wars. We will, however, have a usability and features-based discussion on Oryon C Portable, an OSINT-focused browser built on the SRWare Iron version 31.0.1700.0 of Chromium, and WhiteHat Aviator, also Chromium based. Note that Chromium, no matter the variant, includes sandboxing, which has obvious security advantages.[2]

Oryon C Portable is a web browser designed to assist researchers in conducting open source intelligence (OSINT) investigations with more than 70 pre-installed tools, while WhiteHat Aviator describes itself as the "best and easiest way to bank, shop, browse, and use social networks while stopping viruses, advertisers, hackers, and cyber-crooks."

According to Marcin Meller of OSINT Insight,[3] the next version of Oryon C will be named Oryon C OSINT Framework and will be based on their own build of Chromium. They've made some changes to the tool sets and information sources. While there will be a few new interesting solutions, they also managed to reduce features that proved to be unnecessary. The browser will be lighter, clearer, and more effective, and the new version will offer a cross-platform support including Windows, Linux, and Mac OS X along with a special edition of Oryon F based on the Mozilla source code, specifically for Firefox enthusiasts. These new releases should appear online sometime this summer at the latest. Marcin says that thanks to great feedback from users, including some excellent OSINT specialists, they are highly motivated to make Oryon an even more solid and powerful tool. The active users are the strength of this project; thus, Marcin invites everyone to share their experiences and support Oryon.

When I pinged Jeremiah Grossman, now WhiteHat's CEO, he reminded me that Robert 'RSnake' Hansen, VP of WhiteHat labs, leads the Aviator project.[4] Ah, the fond memories of April Fools' Day past (five years ago now) and the birth of the Application Security Specialist (ASS) certification.[5] Jeremiah is the master of April Fools' mayhem. It's not often that you get the opportunity for a photo opp with both Jeremiah and RSnake, but if you're wearing your ASS shirt at the BlueHat conference, you just might.

Figure 1 – Robert, Russ, and Jeremiah

[1] *For State and Country* – Washington State Guard.

[2] http://www.chromium.org/developers/design-documents/sandbox/Sandbox-FAQ.

[3] http://osintinsight.com/oryon.php.

[4] https://www.whitehatsec.com/aviator/.

[5] http://www.asscert.com/.

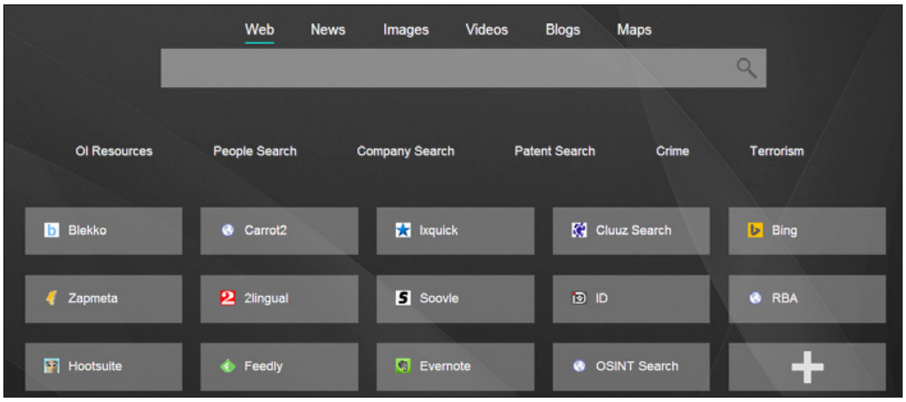


Figure 2 – Revel in the OSINT majesty

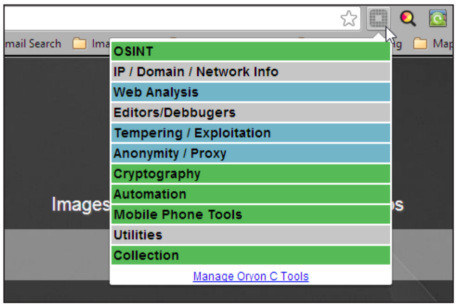


Figure 3 – Enable Oryon tool families

Robert filled me in in the Aviator project: "WhiteHat Aviator started off being a more private and secure browsing option for our own internal users. It has morphed into being a consumer product (Mac and Windows) that has additional and originally unforeseen merits. For instance, it is significantly faster due to having no ads and by virtue of making Flash and Java "click-to-play" options. Users on GoGo inflight wireless love it because it makes the web usable over latent connections, not to mention it uses less power on your laptop. We are giving the browser away for free for now, and all users who download it will be grandfathered in, but in the future we will charge for the browser to ensure that our interests are aligned with the user and to help pay for development without requiring us to steal personal information from our users. ;-) We will quite possibly be the first browser with tech-support!"

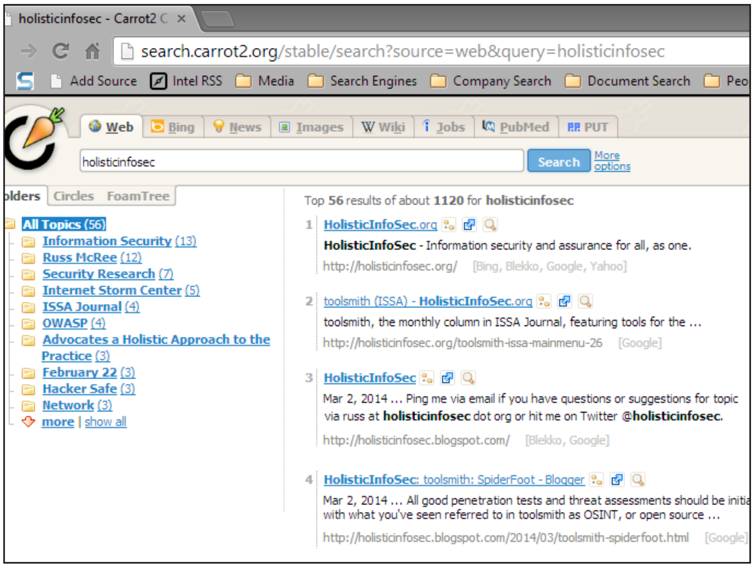
Both of the browsers offer the added benefit of enhanced privacy but serve rather different purposes, so let's explore each for their strengths.

Oryon C Portable

OSINT fans rejoice; there's a browser dedicated to your cause! Oryon includes more than 70 pre-installed tools, more than 600 links to specialized sources of information and online investigative tools, additional privacy protection features, and a ready-to-use OPML file containing a sorted collection of information sources specific to OSINT, intelligence, infosec, defense, and more. Oryon C Portable is also quite literally…portable. You can run it from all sorts of USB and optical media. I'll pause for a second so you can take in all the glorious OSINT power at your fingertips as seen in figure 2.

You can manage the Oryon C tools from the, yep, you guessed it, the Oryon C tools button. As you do so you'll see the related button appear on the toolbar and a popup notice that the extension has been enabled. From the same tools button as seen in figure 3 you can open the full tools menu to create extensions groups and search/sort your extensions.

There are so many tools to explore that it's hard to discuss them all, but I'll mention a few of my favorites. Do keep in mind that you may find part of the feature set using Polish as Oryon C is developed by Mediaquest in Poland. The IP Geolocator uses Google Maps and MaxMind to zoom in on the location of IP addresses you enter in the form field. Fresh Start is a cross-browser session manager that allows you to save a session and reimport it or recover if it's crashed. I love Split Screen as it lets you conduct two sessions side by side for comparison. Wappalyzer is a browser extension that uncovers the technology used on websites including content management systems, eCommerce platforms, web servers, JavaScript frameworks, analytics tools, and many more. Want to spoof your user-agent? Rhetorical question; yes, you do. Make use of the Chrome UA Spoofer. Don't hesitate to dive into the hyperlinks folders as that represents an entire other level of exploration. The All in one Web Searcher aggregates results from a plethora of search results in one UI as seen in figure 4.



Top **56** results of about **1120** for **holisticinfosec**

1 HolisticInfoSec.org
HolisticInfoSec - Information security and assurance for all, as one.
http://holisticinfosec.org/ [Bing, Blekko, Google, Yahoo]

2 toolsmith (ISSA) - HolisticInfoSec.org
toolsmith, the monthly column in ISSA Journal, featuring tools for the …
http://holisticinfosec.org/toolsmith-issa-mainmenu-26 [Google]

3 HolisticInfoSec
Mar 2, 2014 … Ping me via email if you have questions or suggestions for topic via russ at **holisticinfosec** dot org or hit me on Twitter **@holisticinfosec**.
http://holisticinfosec.blogspot.com/ [Blekko, Google]

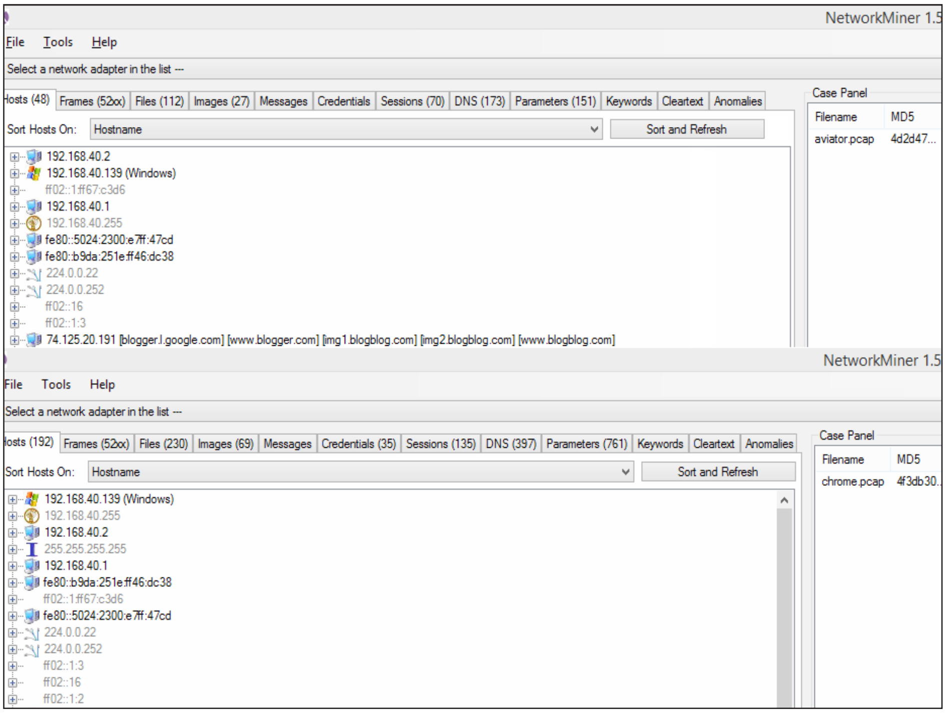
4 HolisticInfoSec: toolsmith: SpiderFoot - Blogger
Mar 2, 2014 … All good penetration tests and threat assessments should be initia
with what you've seen referred to in toolsmith as OSINT, or open source …
http://holisticinfosec.blogspot.com/2014/03/toolsmith-spiderfoot.html [Google]

Figure 4 – All in one Web Searcher results

Oryon C = playtime for OSINT nerds, and I proudly count myself as one. I literally spent hours experimenting with Oryon and am certain to spend many more similarly. At least I can count it as time towards work. ;-)

WhiteHat Aviator

For Aviator I thought I'd conduct an interesting study, albeit not following optimal scientific standards.



```
Filename      MD5
aviator.pcap  4d2d47...

192.168.40.2
192.168.40.139 (Windows)
ff02::1:ff67:c3d6
192.168.40.1
192.168.40.255
fe80::5024:2300:e7ff:47cd
fe80::b9da:251e:ff46:dc38
224.0.0.22
224.0.0.252
ff02::16
ff02::1:3
74.125.20.191 [blogger.l.google.com] [www.blogger.com] [img1.blogblog.com] [img2.blogblog.com] [www.blogblog.com]
```

```
Filename      MD5
chrome.pcap   4f3db30...

192.168.40.139 (Windows)
192.168.40.255
192.168.40.2
255.255.255.255
192.168.40.1
fe80::b9da:251e:ff46:dc38
ff02::1:ff67:c3d6
fe80::5024:2300:e7ff:47cd
224.0.0.22
224.0.0.252
ff02::1:3
ff02::16
ff02::1:2
```

Figure 5 – Comparing the differences between Aviator and Chrome browser session network traffic

On a Windows 7 virtual machine I conducted default installations of Aviator and Chrome and made no setting changes. With no other applications running, and no processes generating any network traffic, I executed the following:

Step 1

1. Started Wireshark
2. Initiated a capture on the active interface
3. Started Aviator
4. Browsed to http://holisticinfosec.blogspot.com
5. Terminated Aviator
6. Stopped Wireshark with 5250 frames captured

Step 2

1. Started Wireshark
2. Initiated a capture on the active interface
3. Started Chrome
4. Browsed to http://holisticinfosec.blogspot.com
5. Terminated Chrome
6. Stopped Wireshark with 5250 frames captured

Step 3

1. Opened aviator.pcap in NetworkMiner 1.5 and sorted by Hostname
2. Opened chrome.pcap in NetworkMiner 1.5 and sorted by Hostname
3. Compared results

The results were revealing to be sure. I'm glad to share the captures for your own comparisons; just ping me via email or Twitter if you'd like copies. Notice in figure 5 the significant differences between counts specific to hosts, files, images, credentials, sessions, DNS, and Parameters.

These differences between default configurations of Aviator and Chrome are achieved as follows:

- Aviator's privacy and security safeguards are preconfigured, active, and enabled by default
- Aviator eliminates hidden tracking and uses the Disconnect extension to block privacy-destroying tracking from advertisers and social media companies
- WhiteHat is not partnering with advertisers or selling click data
- Unwanted access is prevented as Aviator blocks internal address space to prevent malicious web pages from hitting your websites, routers, and firewalls

It's reasonable to ascertain that those with an affinity for strong default privacy settings will favor WhiteHat Aviator, given the data noted in figure 5 and settings provided out of the gate.

In conclusion

These are a couple of fabulous browser for your OSINT and privacy/security pleasure. They're so easy to install and use (I didn't even include an installation section, no need) that I strongly recommend that you do so immediately.

Take note, readers! July's *ISSA Journal* will be entirely focused on the Practical Use of Infosec Tools. Rather than put up what is usually just me going on about infosec tools, you should too! Send articles or abstracts to editor at issa dot org.

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

Cheers…until next month.

Acknowledgements

—Marcin Meller, OSINT Insight

—Robert 'RSnake' Hansen, VP WhiteHat Labs, Advanced Technology Group

About the Author

Russ McRee manages the Threat Intelligence & Engineering team 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 at holisticinfosec dot org or @holisticinfosec.