C11 Online Anonymity: Forensic Analysis of The Onion Router (Tor) Browser Bundle

Darcie Lynn Winkler, BS, 1106 11th Avenue, Apt 4, Huntington, WV 25701; Robert J. Boggs, West Virginia State Police Digital Forensics Unit, 1401 Forensic Science Drive, Huntington, WV 25701; John E. Sammons, MS, 18 Quail Drive, Ona, WV 25545; and Terry Fenger, PhD, 1401 Forensic Science Drive, Huntington, WV 25701*

After attending this presentation, attendees will understand the manner in which The Onion Router (Tor) provides anonymity to its users, some of the vulnerabilities that exist within the software, and a few forensic analysis techniques that are capable of circumventing the secrecy.

This presentation will impact the forensic science community by allowing practicing digital forensic analysts to take away valuable information pertaining to the Tor Browser Bundle (TBB) that may save time in future investigations as attendees will be aware of several methods that will and will not work in the process of gathering pertinent evidence.

Tor is a network of encrypted onion routers that helps to increase the level of anonymity experienced by its users. The security and privacy provided by the TBB was originally intended to protect the communications of the government; however, it is also a facilitator for individuals participating in illicit activities. It was hypothesized that if correct methodology is executed and the data collected is analyzed using pre-existing forensic techniques, then relevant evidence of the browsing history and presence of the TBB may be acquired. To test this, Virtual Machines (VM) were constructed to test four possible scenarios: (1) a machine running only Internet Explorer®; (2) a machine with TBB downloaded but no active use recorded; (3) a machine with TBB downloaded and used to navigate both the internet and Darknet; and, (4) a machine where TBB had been installed, used, then uninstalled. Furthermore, an additional VM was created solely for the purpose of tracking registry changes throughout the course of installing and uninstalling the TBB. It is hoped that beneficial information will become evident by capturing packets while the TBB is navigating to .onion and .com websites, dumping the Random Access Memory (RAM), and comparing versions of the registry from various points of the installation process.

In conclusion, the RAM dump provided several file types from the carved image that linked the web browsing to the TBB and several .onion sites. The registry files demonstrated that deleting Tor does not carry out a full uninstallation, thereby leaving artifacts behind. Lastly, the packet capture proved that Tor traffic is very different in appearance and content than that of a standard web browser.

Each method employed reaped beneficial artifacts proving that the TBB does not provide complete anonymity. These techniques would for the most part only be applicable in a proactive network forensics environment using a remote process to monitor a suspect's activity. Therefore, it is less likely that these methods would be used in a digital forensics lab that receives evidence from a crime scene. Naturally, the digital forensic community will remain persistent in their quest to refine an applicable technique that will adequately gather incriminating evidence from a hard drive subsequent to collection; however, without more advanced technology and abundant resources like those available to government agencies such as the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA), digital analysts will be hard pressed to find a reliable method of breaking through the anonymity provided by the TBB for confiscated hard drives and associated digital evidence.

Anonymity, Forensic Analysis, Tor Browser

Copyright 2015 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS.