Privacy Section

The overall privacy of user browsing activities and their associated connections continues to be an increasing concern for organizations. With the events of September 11th and the growing industry regulations (HIPAA, NERC, PCII, etc.) in mind, privacy is not and cannot be an absolute right within an organization, as there needs to be accountability and auditability for user actions. Similarly though, an organization must be able to trust that the user’s outbound web browsing connections cannot be easily intercepted, modified, or otherwise routed through uncontrolled channels for malicious use. To this effect, the team has utilized network packet captures (or pcaps) to discover and access the outbound connections being established by Firefox for comparison against the outbound connections being established by Opera.

A “packet analyzer” or “network protocol analyzer” is computer software that can intercept and log network traffic as it passes across the entire network (or the segmented portions, if quality assurance or security controls have been implemented). “Wireshark is the world’s foremost network protocol analyzer” and “the de facto (and often de jure) standard across many industries and educational institutions” (Wireshark.org), allowing for live network captures or static analysis from previously captures saved to disk (.pcap or .pcapng files). Any outbound network connection, internal or external, encrypted or unencrypted, can be captured and reviewed through Wireshark.

To begin the assessment of outbound connections from Opera and Firefox, the two browsers were installed on the OS X El Capitan 64-bit release (version 10.11.5) of Mac. As no specific version of Opera was mandated and the default Opera configuration performs automatic updates, the latest version was used – “Version: 38.0.2220.31”. To maintain compliance with the Testing Scope (as noted in the Appendix), version 46.0 of Firefox was installed for evaluation. More specifically, the same Security and Stability release of 46.0.1 was utilized to most closely mirror the results that the CIO noted (as mentioned in the Syllabus). To ensure impartial testing moving forward, the automatic updating was disabled in both Firefox and Opera. If the automatic updates were not disabled, Firefox would be updated to the latest version on launch and/or restart, placing the assessment out of scope. As automatic updating is a core feature of many applications today, Opera performs similar checks and updates. These features require one or more outbound connections be made and would not allow for impartial testing if Opera was allowed to make outbound connections for automatic updating while Firefox was prevented from doing so.

After the base outbound connections were captured through Wireshark, the next assessment involved the monitoring of alerts generated through the program “Little Snitch” (as its use by the CIO in the Syllabus generated the initial concern around the difference in outbound connections between Opera and Firefox). As the installation of Little Snitch requires a reboot and then begins interception of connections upon login, it was not installed prior to the Wireshark assessments. Once the installation was performed, each browser was launched and allowed to run for five minutes, as was the case with the Wireshark assessment.

Comparing the outbound connections through these two tools, there is a considerable different noted between Opera and Firefox. Though the HTTP and HTTPS traffic (web requests) intercepted via Little Snitch shows few dissimilarities, analysis of the Wireshark traffic stands out more. The DNS traffic (in essence an Internet telephone book, resolving numbers to names) shows numerous outbound connections not readily visible through Little Snitch. While Firefox makes only three unique calls (two to Google and the third to Mozilla), Opera quickly exceeds this with about nine unique calls (many to Amazon, Facebook, Google, and Opera). Though these are often considered trusted sources, Amazon (Amazon Web Services and CloudFront content delivery network) and Facebook can be associated with ad services, external hosted solutions, and general privacy concerns. As Opera initiated three times more DNS outbound connections in a short five minute window than Firefox, the CIO’s assessment of the connection differences seems to be well founded, and Tiger team recommends Firefox based on these results.