MS-ISAC

MS-ISAC Security Primer

The Deep Web

March 2017, SP2017-0918

The Internet is comprised of two sections, the searchable Internet, sometimes called the “surface web” or “clearnet,” and another network known as the “deep web.” The surface web can be accessed using standard web browsers such as Mozilla Firefox, Microsoft’s Internet Explorer or Edge, and Google’s Chrome. The deep web is made up of a collection of web pages that cannot be, or are not, indexed by search engines like Google.

Similar to the surface web, the deep web contains unlinked pages,[1] dynamic content pages,[2] and limited-access or private pages.[3] Some pages associated with the deep web are part of the deep web because they do not use common top-level domains (TLDs), such as .com, .gov, and .edu, and as such, they are not crawled and indexed by search engines. To view content on these unindexed pages, users may need to use specific software like Tor or tor2web. Other websites are part of the deep web because they are dynamic content pages, with data and content supplied by databases. This information changes constantly and is dependent on the user, so search engines cannot crawl or index it.

Many individuals who are interested in the deep web focus on the existence of unlinked pages and pages with limited access, as malicious actors commonly use these pages to communicate about, sell, and/or distribute illegal content or items, or discuss sensitive or banned topics. The most direct way to find these pages is to receive a link to the page by someone who already knows about the page.

Cyber professionals often interchange the terms “deep web” and “dark web.” The dark web is a part of the deep web. The dark web relies on connections made between trusted peers and requires specialized software, tools, or equipment to access. Examples of dark web networks include Tor (f.k.a. The Onion Router), Freenet, and the Invisible Internet Project (I2P). Just like the surface web, activity on the dark web may or may not be illegal.

RECOMMENDATIONS:

- Be aware of the potential for your computer to be compromised while browsing the deep or dark webs. Use a virtual machine (VM) to reduce the risk of infection or compromise. VMs provide a virtual layer between the system you are using, and the physical network you are operating on, which can act as an additional layer of security and be erased if the VM is infected with malware.
- Do not assume that information posted to the deep or dark webs is secure because it is difficult to locate.
- Do not assume that you cannot be identified, even when using software and visiting websites that promise anonymity.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation’s state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.

[1] Unlinked webpages are created specifically with no inbound or outbound links on them. Unlinked pages are accessed by typing the specific Uniform Resource Locator (URL) into a browser address bar or from a hyperlink shared with the intended viewer.

[2] Standard webpages host unchanging content. Dynamic webpages provide an interactive user experience, with changing content.

[3] A page that requires a user name and password to access.