The Dark Net

A primary source of threat intelligence is the **dark web**. Here is a summary of what you learned today:

Terminology:

Please note: The Internet and the World Wide Web are NOT synonymous. They are two different animals!

- The **Internet** is an electronic communications network that connects computer networks and organizational computer facilities around the world.

- The **World Wide Web** is actually a layer that sits on top of the Internet and uses Internet technology. The WWW is a global collection of documents and other resources, linked by hyperlinks and URIs. **Web** resources are accessed using HTTP or HTTPS, which are application-level, by means of a software application called a web browser.

- The Clearnet is another term for the World Wide Web

- The Deep Web— any part of the World Wide Web that is not indexed by a search engine. This includes pages that require registration, pages that block search indexing, unlinked pages, pages using nonstandard DNS, and content encoded in a nonstandard manner. It is still part of the Clearnet.

- The Dark Net—a network established as an overlay to the Internet infrastructure by software, such as The Onion Router (TOR), Freenet, or I2P, that acts to anonymize usage and prevent a third party from knowing about the existence of the network or analyzing any activity taking place over the network. Onion routing, for instance, uses multiple layers of encryption and relays between nodes to achieve this anonymity.

- The Dark Web— sites, content, and services accessible ***only*** over a dark net. While there are dark web search engines, many sites are hidden from them. Access to a dark web site via its URL is often only available via "word of mouth" bulletin boards.

Safety Tips

The Dark Net is a very interesting place, but it can also be very dangerous. There are unscrupulous people of the very WORST kind trolling the Dark Net. You can browse the Dark Net with confidence if you take the necessary precautions to stay SAFE!

1. Turn on your VPN! I use PIA (Private Internet Access), but there are other reliable products. ProtonVPN is very good. There are others, just make sure you investigate them first.

The Dark Net

2. LEARN before you browse! I use the TOR browser (The Onion Router), and I'm very happy with it. Once you launch the browser, you will want to click the onion in the upper left-hand corner and READ EVERYTHING!. There is also some useful information that you can find on the OSINT Framework (https://osintframework.com). If you use the TOR browser, there are a lot of resources there to learn just about anything.

3. Make sure you are setting your browsers security setting to "Safest." In some situations, such as if you want to access the OSINT framework from the Dark Net, you may need to use "Safer" instead of "Safest," but when you are just browsing, ALWAYS use "Safest." You can access the security settings by clicking the little shield to the right of the address bar.

4. Do not EVER provide your true contact details and name to ANYONE on the Dark Net. It is very dangerous to do that! You can establish a Dark Net email account and use that for Dark Net communications. I realize some of you will want to check out Facebook's Dark Net Onion site- do it safely!

5. You will know if you are on an onion site because there will be an onion where you will see a lock on a Clearnet site. You can click that little onion for additional information.

6. If you want to find The Hidden Wiki, you can access it here: http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

7. DO NOT DO NOT DO NOT DO NOT DO ANYTHING ILLEGAL! Do not do anything that you wouldn't want your mother or grandmother to know about! You are UNITED STATES AIRMAN! Keep us proud of you!

8. If you have questions, please ASK!

donna.schwartz.1@us.af.mil
228-256-9111