



# NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

## Dark Web: Illicit Activity Thriving on the Underground Internet

April 15, 2016

TLP: WHITE | *The NJCCIC assesses with high confidence that a broad range of criminals, malicious hackers, and violent extremists will increasingly utilize the dark web—the underground Internet only accessible via special software that maintains the anonymity of users—to facilitate illicit activity, which will present threats to public safety as threat actors can securely communicate, conspire, and acquire materials or know-how.* We assess use of the dark web will accelerate amongst traditional criminal enterprises as well as those plotting domestic terrorism attacks or extremists inspired by ISIS and other terror groups. This is due, in part, to the low barriers to entry, low risk of attribution, and ubiquitous availability of illicit goods and services, from heavy weapons and explosives to bank account credentials, fraudulent US passports, and ready-made hacking tools. Though there are legitimate uses of these clandestine networks, such as providing secure communications for political dissidents, oppressed societies, and journalists, a [recent study from King's College](#) found that a majority, 57 percent, of active websites on the dark web are illicit in nature.

- The dark web is a subset of the deep web, a large portion of the Internet that is not indexed and inaccessible via standard search engines. The deep web can be accessed via ordinary web browsers, however, a user must know the address (Uniform Resource Locator or URL) of a site in order to navigate to it, and many sites are password protected. On the other hand, the dark web is only accessible via Tor, the Invisible Internet Project (I2P), Freenet, and several other, less common, networks known as darknets. As with the deep web, users need to know what they are looking for, as most dark web URLs are alphanumeric strings that are unassociated with the site's content, for example, zqtkwi7fexvo6ri.onion. However, some mainstream websites have begun hosting their services on the dark web, providing users with untraceable usability. In October 2014, [Facebook](#) announced they were hosting their social media service directly via the Tor network, with the address of facebookcorewwi.onion/.
- In early 2015, [researchers at King's College](#) scanned and analyzed all active and accessible websites on the Tor network, creating a taxonomy of twelve categories. Of the 2,723 active sites evaluated, 1,547 were classified as illicit with a high degree of confidence, with the most common involving drugs (pharmaceutical and illegal narcotics), illicit finance, and various extremist, pornographic, or violent content. The researchers identified one key differentiator between licit and illicit sites on the dark web: the majority of legitimate sites identify their operators, while the majority of illicit sites do not. Known as [hidden services](#), illicit operators take full advantage of the dark web's anonymity, allowing them to build and maintain servers without an associated Internet Protocol (IP) address, physical address, or identity. Therefore, both parties involved in illicit transactions remain untraceable.
- According to an April 2016 [report from Dell SecureWorks](#), supply and demand for stolen financial and identity data remains strong, in addition to hacker-for-hire services. For example, a counterfeit US passport can be purchased for as low as \$3,000, while an 'identity package' consisting of a Social Security number, driver's license, and utility bill costs only \$90. Hackers can be paid to hack a corporate email account for \$500, or launch a weeklong distributed denial of service attack for \$200 to \$555. Aspiring hackers can also pay for a variety of hacking tutorials for less than \$40, and purchase [Remote Access Trojans](#) (RATs) for less than \$10 or [exploit kits](#) for \$100.

### Recommendations

Organizations may want to consider blocking [Tor exit nodes](#) in order to prevent cyber threats that utilize the dark web to obfuscate the attacker's identity, often used to attack websites or servers. However, the addresses change continuously.

### Contact

For more information, or to request an in-depth briefing on the dark web and the implications on the public and private sector, please contact the NJCCIC at [NJCCIC@cyber.nj.gov](mailto:NJCCIC@cyber.nj.gov).

Traffic Light Protocol: **WHITE** information may be distributed without restriction.