In "The Deep Dark Web," a research and intelligence report, John Kuhn explains how the term "Deep Web" has become a place that contains more content than the standard web everyone uses, most of it for nefarious reasons. In this report, he gives a high-level overview of two networks that dominate the hidden spaces of the dark web:

- Tor

The Deep Dark Web

by John Kuhn, Senior Threat Researcher, IBM

Abstract

In "The Deep Dark Web," a research and intelligence report, John Kuhn explains how the term Deep Web has become a place that contains more content than the standard web everyone uses, most of it for nefarious reasons. In this report, he gives a high-level overview of two networks that dominate the hidden spaces of the dark web:
• I2P

Tor

Originally developed by the U.S. Navy to provide secure communications, Tor has come to be used by criminal elements active in the selling of illegal drugs, weapons, pornography, and other contraband. A peer-to-peer network, Tor makes possible the creation of hidden sites catering to activists and criminals. It also provides exit node proxies that enable users to access its sites anonymously.

One of the most active sites on Tor was Silk Road, which specialized in offering contraband for sale, using Bitcoin, and using national postal services for delivery. Because of its popularity, Silk Road came under increasing attention of law enforcement and was eventually shut down. Replacements appeared, however, and eventually the site moved from Tor to I2P.

I2P

I2P is also an encrypted peer-to-peer network, although technologically it functions differently. I2P offers such services as email, web browsing, blogging, and real-time chatting. Sites on I2P are known as eepsites. Silk Road was reborn on I2P as Silk Road Reloaded and now uses, in addition to Bitcoin, other crypto-currencies such as Darkcoin, Dogecoin, and Anoncoin.

Criminals have been somewhat slow to move to I2P, probably because of its greater complexity, though the network is expected to attract more criminals as it becomes more popular. For the time being, Tor remains the criminal's dark web of choice.

In summary

Kuhn explains that it's imperative to understand what the dark web might contain when it pertains to your company or brand. Organizations should prevent access to the dark web from within their networks. These hidden networks not only provide access to illegal products, they may also open your infrastructure to attack. You should use security software to block access from your network to the dark web and configure your firewall to prevent attacks originating there. Given the illegal character of many of the sites they host, it is best to employ an experienced, professional service.

Download this important threat alert.

© Copyright IBM Corporation 2015
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)