NSIGHT SERIES

May 2020 — Issue 5

The Decline of the Dark Web

How Mobile Solutions have Disrupted the Dark Web

The dark web is in decline. Once the preferred means for anonymizing users' online activity, the dark web has now been supplanted by encrypted mobile applications and alternate solutions. Similarly, aggressive law enforcement actions have shuttered many of the dark web's largest forums, making it a much more fleeting and much less secure destination for criminal activity. As a result, the number of users accessing dark web sites has dropped.

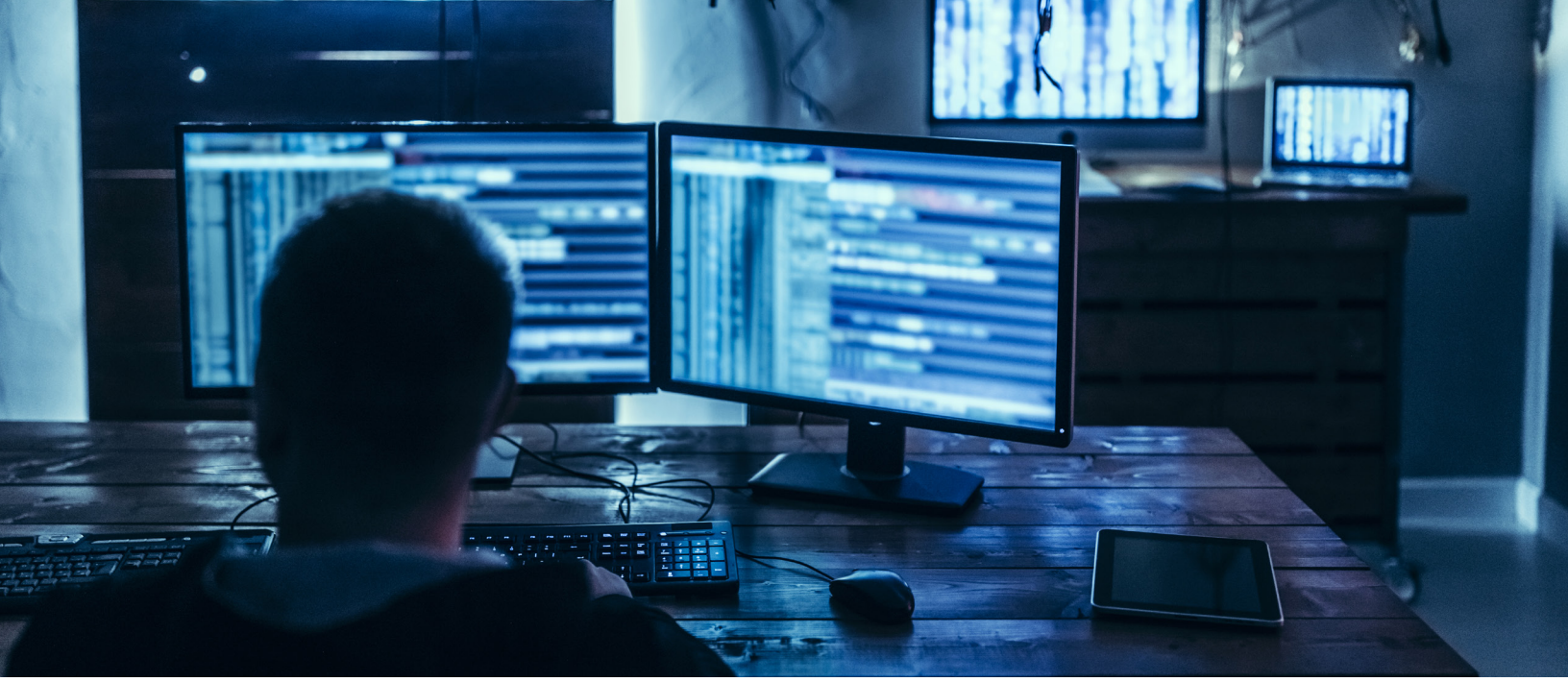
Instead, many users are connecting through the dark web via mobile applications on Android and iOS, rather than to the dark web via standard browsers, to obfuscate their internet traffic. Indeed, the number of users accessing the Tor network has increased, even as the number of users accessing hidden service sites—the "dark" part of the dark web—has dropped. Moreover, encrypted applications like Telegram, Signal, and Wickr.me have lowered the barrier to entry for secure communication and illicit transactions. As a result, just like many other industries, the dark web has been disrupted by technological innovation and aggressive competition, triggering a gradual decline and turning the so-called invisible internet even more opaque.

What is The Dark Web?

The "dark web" refers to parts of the internet that require the use of special tools or routing protocols to access. By comparison, the clear or surface web does not require any special tools to access (think, espn.com or cnn.com). A traditional web browser, unless specially configured, cannot connect users to a dark web "hidden service" site. These sites rely on specific encryption and routing protocols to protect users' identities.

Dark web platforms such as The Onion Router (Tor), I2P, Freenet, and Zeronet, attempt to anonymize users' digital fingerprint so that technical attributes like IP addresses are not easily available to entities with intent to track users' online activity. This emphasis on anonymity was designed to keep the dark web free from oversight, free from censorship, and open to anyone in any location. The developers of Tor, the most popular dark web platform, promote it as a tool to combat oppression and connect people who might not otherwise have open access to the internet. A substantial percentage of Tor users come from countries like Iran, China, and Russia, where governments have restricted the content its citizens can access. Major news outlets, sites like Facebook, and even U.S. federal agencies maintain websites on the dark web so its users can securely communicate from countries where free speech is controlled.

However, the lack of oversight has earned the dark web a reputation as a haven for criminals looking to sell drugs, stolen identities, and other illicit services. Illegal transactions



largely occur on dark web markets, which make up some of Tor's most popular hidden service sites. These markets are populated by hundreds of vendors and buyers, all of whom have learned how to operate specialized programs that keep their identities hidden. To operate on a dark web market, a user must create an account which is usually linked to a secure dark web email address. They can then buy and sell content using cryptocurrency, provided they've established a crypto wallet and obtained digital funds without linking them to their personal information. If a user attempts to acquire illegal goods from these markets without practicing proper operational security, they risk compromising not only their funds, but also their identity.

A lack of oversight has also made it difficult for developers to create and promote dark web resources. Due to its criminal connotation, clear web sites are reluctant to post content that links its viewers to potentially illicit hidden service sites on the dark web. Resources dedicated to the dark web are routinely targeted by law enforcement entities and shut down, so anyone interested in learning about how to operate on the dark web will need to look through community forums, archived pages, and posts on social media.

Unlike many popular clear web services, security patches, updates, and improvements to Tor are released slowly and sporadically, as the organization responsible for the browser, the Tor Project, has a limited number of resources. The anonymous nature of Tor makes identifying and implementing fixes for issues difficult. For example, The Tor Project recently released an update that patched a major vulnerability that had been taking hidden service sites offline for years. The bug was so well-known by the time it was addressed that a free-to-use dark web denial-of-service (DOS) tool meant to exploit the bug had been available on Github for four years.

Feeling Around in The Dark Web

The lack of centralized information, coupled with a lack of trust in fellow dark web users, has made it difficult for the dark web community to collectively evolve, or create a set of tools equivalent to those on the clear web. While the dark web has a few options for search engines, none are particularly effective. There are dozens of social media sites that prioritize privacy being offered, but none has gained enough notoriety to attract a wide user base. This, in turn, means they aren't advertised in community forums, and ultimately have little chance of attracting a wider user base in the future. Marketplaces and community forums have maintained their popularity on the dark web primarily because they offer the illicit goods and services without content censorship that could not easily be found elsewhere.

Even the dark web's most visited markets are having trouble staying active as law enforcement entities around the world begin to dedicate substantial resources towards conducting effective cyber investigations. From original marketplaces like Silk Road, to recent marketplaces like

Alphabay and Dream Market, hidden service sites offering illegal content are routinely targeted and taken down as soon as they gain prominence. Many markets that attempt to fill the vacuum have "exit scammed"—a fraudulent practice wherein market admins or other actors appear to be running a market or providing a service but are in fact stealing users' cryptocurrency before shutting down their site—before they are caught by law enforcement. The constant uncertainty, high level of risk, and lack of continuity make dark web markets less attractive each year. Secure communication platforms on mobile devices, however, present an interesting alternative.

The Rise in Alternate Solutions

Mobile devices are simplifying how users access web-based services. Smartphone owners have a connection to the internet in their pockets at all times, and this connection is available to millions of people that don't have access to a standard computer or home internet service. There are approximately 3.5 billion smartphone users worldwide as of 2020, and it's estimated that around sixty percent of annual web traffic now comes from mobile devices. People are able to share more of their lives from more places than ever, and that's put a renewed emphasis on securing users' privacy.

In an environment where Tor and the dark web once offered some control over the information users shared over the internet, secure messaging apps have begun to gain traction. Platforms like Signal, Telegram, and Whatsapp all offer options to encrypt communications between users and prevent unintended parties from intercepting content. While the user has less control over configurations on mobile devices than they would through Tor on a standard computer, these apps allow anyone with a smartphone to create secure accounts quickly and with little effort.

Just as with Tor on the dark web, mobile platforms that were developed to facilitate free speech are gradually being co-opted by groups with criminal intent. Apps like Telegram have been targeted by extremist groups who have graduated from the dark web to mobile services in order to expand their reach to a larger audience. Telegram, intentionally or not, has become a platform where radical users can connect and spread extremist ideology. Thanks to its privacy-focused infrastructure, these users are able to create closed groups and channels full of encrypted content that can only be accessed by invitation. They can also create public channels to broadcast read-only messages as a supplement to recruitment and indoctrination campaigns.

Groups ranging from Islamic extremists like IS and Al Qaeda to white supremacists and neo-nazis have migrated from hidden service sites on Tor to groups and channels on Telegram. Instead of targeting only users technically proficient enough to avoid compromising themselves on the dark web, these extremists now have access to 200 million active monthly users through an easily downloadable smartphone app. Users looking for stronger privacy features can try apps like Signal and Wickr, which offer end-to-end encryption and require little to no verifiable personal information. These also offer users the ability to create self-destructing messages so that any incriminating conversations are inaccessible to law enforcement. These messaging apps are a popular supplement for vendors of illicit goods who want to talk directly to customers or conduct business outside of Tor's dark web markets.

The Tor Project is working to adapt to this new mobile-focused environment. The organization recently released an app for the Android mobile operating system and recommends the Orbot app for users on an iOS device. These apps allow users to not only visit hidden service sites from their smartphone, but also lets them route their clear web traffic through Tor's relays in order to obscure some of their technical indicators. Documentation published by the IS-linked Electronic Horizons Foundation encourages its followers to browse Facebook and Twitter through Tor's mobile app but directs its users to a list of secure messaging apps for group communication. High-profile white supremacist terrorist groups like the Atomwaffen Division (AWD) maintain a hidden service site but, because most of the community operates on apps like Telegram, their messages often need to be reposted in popular white supremacist channels on the app. The group was recently subjected to internal fracturing in part because the original members of AWD did not establish presence on Telegram before a splinter group in the organization laid claim to the official channel.

The Decline of the Dark Web

Due to the relative difficulty associated with creating, maintaining, and marketing a hidden service site on the Tor network, traditional utilization of sites on the dark web will continue to decrease. The dark web's reputation as a haven of criminal activity will ensure it remains a target for law enforcement. Law enforcement take downs of popular dark web markets and resources will prevent an increase in hidden service site usage. Users looking for platforms that advocate privacy and free speech will increasingly transition to secure messaging apps and mobile services. There they can easily secure their communications and browsing with encrypted messaging apps and mobile optimized versions of Tor. These mobile platforms are also available to millions of users worldwide who do not have access to standard computers with a Tor browser.

The massive number of smartphone users, the ability to download and operate mobile apps with relative ease, and the security offered by content encryption are just a few notable reasons why the dark web is in decline. In response to this disruption, the Tor Project and other dark web services have released mobile solutions of their own, but they're still only partial measures. The most sensitive or illicit activity is increasingly occurring on end-to-end encrypted mobile applications. As a result, the dark web, once an unpoliced and assumedly anonymous bastion for illegal activity, is today on its way to dying a slow death in favor of simpler, more accessible mobile solutions.

About Ntrepid

Ntrepid's suite of managed attribution products enable organizations to safely conduct their online activities. We are dedicated to understanding the challenges our customers face in order to build environments to facilitate secure operations in the most hostile network environments and against the most sophisticated opponents. We are proud to support Fortune 500 companies in the financial and healthcare sectors and customers across the national security community.

Contact us to learn more about the full spectrum of Ntrepid solutions.

www.ntrepidcorp.com
1.800.921.2414
solutions@ntrepidcorp.com

Ntrepid's Nsight Series analyzes emerging trends, challenges, and technologies that impact your online operations—all from the perspective of better managing your online attribution.

NTREPID®