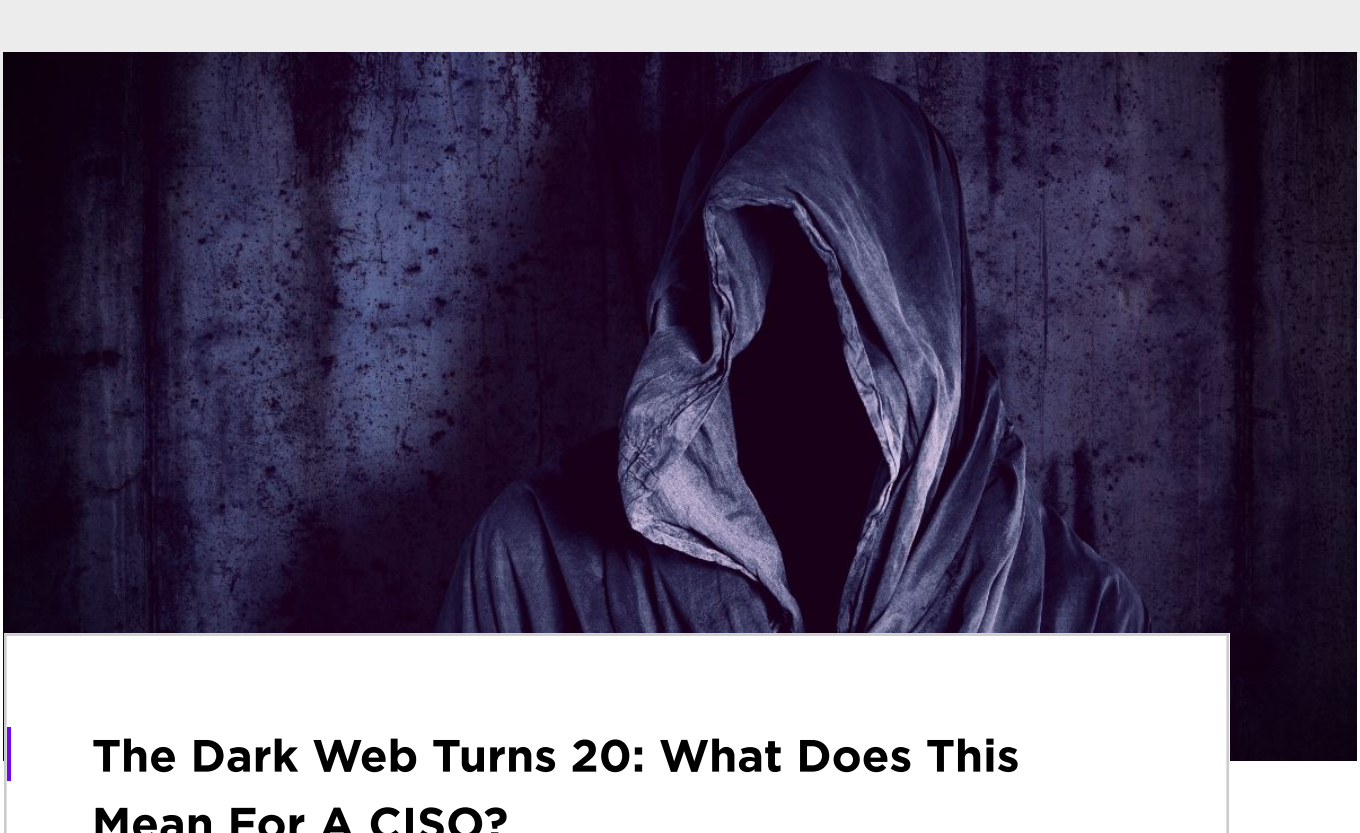

The Dark Web Turns 20: What Does This Mean For A CISO?

April 9, 2020
by Yotam Gutman

Infamous for its illicit trade and now the adopted home of malware authors, purveyors of ransomware and traders in stolen credit card and other misappropriated data, the Dark Web (*aka* Darknet) has been with us now for two decades. While not everything on the Dark Web is shady – there's plenty of traffic hidden from sight that is not only benign, but sometimes in the public good – there's no doubt that it has acquired a reputation as a place that harbors criminals, malcontents, and threat actors who might be planning on attacking your enterprise. In this post, as the Dark Web turns twenty, we review what it is, where it came from, and most importantly, what it means to today's CISOs and their security teams.

How the Dark Web Started 20 Years Ago

The Dark Web (sometimes referred to as the "Darknet") was officially launched 20 years ago, on March 20, 2000 with the release of "Freenet": a peer-to-peer, decentralised network, designed to make it less vulnerable to attack and snooping by authorities and states.

Freenet was the brainchild of Ian Clarke, who developed the concept and the software tools required to support it during his studies at Edinburgh University. For his thesis project, Clarke created "a Distributed, Decentralised Information Storage and Retrieval System", through which he hoped he could provide freedom to communicate without the fear of being tracked online.

Freenet is still available today, and it is still free to use. Freenet was mostly about information sharing (including pornographic and pirated materials), but otherwise the hardcore cybercriminals were at this time still using other platforms for their needs such as imageboards like 4Chan and IRC channels.

Peeling the Onion

On 20 September 2002, the The Onion Router (or TOR) Network was created by computer scientists Roger Dingledine and Nick Mathewson. Surprisingly, this semi-anarchist project was mostly funded by the US Naval Research Laboratory, which wished to facilitate safer communication with intelligence sources around the world. This is a critical point. The TOR network is not inherently evil, nor was it architected with bad intent.

There has always been a need for a network which facilitates a higher level of security communications. This network allows for anonymous sources to be protected in hostile regimes, for example. The adoption of the TOR network by criminals is an unfortunate side-effect, but the value of the network should not be weighed based solely on that as there is also a percentage of legitimate and good activity as well.

In 2004, the Naval Research Laboratory released the code for TOR under a free license, and the Electronic Frontier Foundation (EFF) began funding Dingledine Mathewson and others to continue its development, until they launched "The TOR Project", a non-profit organization to help maintain the network.

The Onion Router is the most popular means by which people today access dark web sites. TOR has several search engines, directories and hidden wikis that users can use to navigate their way around the dark web and find the kind of sites they're looking for. A version of the TOR browser even exists for mobile users.

TOR greatly simplified access to and use of the Dark Web, and this has led to an explosion of sites offering almost any type of service imaginable, especially for contraband and illicit material – both physical and digital content – using a variety of online payment services like Paypal and Western Union.

Cryptocurrencies, Revolutions and the NSA

It wasn't until around 2010 when cybercriminals really took to the platform. Forums like the Silk Road netted millions of dollars for their administrators with the aid of another technological development: cryptocurrencies, particularly Bitcoin (BTC) and, later, Monero. Cryptocurrency enables the anonymous transfer of funds and provides a nearly complete smokescreen for both buyers and sellers.

Later, the Dark Web was used by hacktivists such as the Anonymous collective and Middle Eastern hacktivists involved in the Arab Spring to coordinate attacks on countries, organizations and enterprises.

Darknet users who value their privacy and anonymity also make use of virtual private networks (VPN). The reason for that is to disguise the fact that the user is actually connecting to TOR at all. Without a VPN, even though you may be anonymous, your use of TOR is not. It has been claimed that the NSA tracks the IP addresses of everyone who visits a TOR website, regardless of the content. According to leaks from whistleblower Edward Snowden in 2014, the NSA also collects the IPs of anyone using FreeNet, HotSpotShield, FreeProxies, MegaProxy and Tails. Hence, along with bitcoin, VPNs are part-and-parcel of the darknet user's technology stack.

And What About the Dark Web Today?

Although the FBI took down the Silk Road and hacktivist activities have declined in recent years, the Dark Web is still a haven of illegal activity. Researchers at King's College in London classified the contents of 2,723 dark web sites over a five-week period (2015) and found that 57% hosted illicit material.

As for the rest, it is largely a mixture of political dissidents, journalists, and whistelblowers mixed in with a motley crew of people trading esoteric or borderline-legal goods and services that the participants or community would rather not draw attention to. White hat, grey hat and of course, black hat hackers also all make use of the darknet for sharing techniques, intel and various software kits that could be used for both educational and illegal purposes.

Nevertheless, it is important to note that on any given day, there are only a few thousand illicit Dark Web sites that are active and accessible. It is very dynamic, and if we compare the risk of the Dark Web to the "clearnet", there is no doubt that there are far more threats in the known clearnet than on the Darknet.

How is the Dark Web Relevant to a CISO?

So how is the Dark Web relevant to CISOs and CIOs? The fact that this network exists is in itself no cause for concern. Cybercrime existed before it was fully developed and will continue even if it were to shut down today. Even in that unlikely event, the same traffic would most likely migrate to social media or encrypted messaging apps like Signal, Telegram and WhatsApp.

But in all likelihood, the cybercriminals who are, or might be, relevant to your organization are active on the Dark Web today. Employing proactive threat intelligence from Dark Web sources can provide security teams with additional information that might prove useful for securing your organization against future threats.

Here are some examples of how Dark Web intelligence could be relevant to your security operations:

- Tracking the development and sale of malware and exploit kits
- Monitoring data dumps that could contain your IP
- Finding stolen credentials such as login passwords belonging to your organization
- Discovering vendors on the Dark Web actively selling access to corporate networks and MSPs

Summary

The Dark Web has been around for two decades, and it seems that it will continue to be with us for some time yet; its shape could change, but its function will likely remain the same. It isn't the sort of mythical place some imagine it to be; it is real and won't disappear just by simply looking the other way. But the Dark Web does offer some opportunities: it can provide us with useful intelligence. The SentinelLabs team regularly monitors the Dark Web and provides actionable intelligence for our customers.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Return to Base | The CISO's Guide to Preparing A COVID-19 Exit Strategy
- Our Take: SentinelOne's 2022 MITRE ATT&CK Evaluation Results
- Dealing with Cyberattacks | A Survival Guide for C-Levels & IT Owners
- 22 Cybersecurity Twitter Accounts You Should Follow in 2022
- More Evil Markets | How It's Never Been Easier To Buy Initial Access To Compromised Networks
- 4 Steps Toward Successfully Measuring the Effectiveness of Your Security Controls