The Dark Web of deceit

By
GERRY CHNG

The Internet already provides us with so much information, but is there more than meets the eye? Deep within the recesses of the Internet is the Dark Web, where data is encrypted and users remain anonymous. Is it a place for good or for bad?

The Internet. A vast expanse of interconnected systems offering a seemingly endless treasure trove of information.

Usually, search engines are our first resort when we look for information. These search engines trawl the Internet and create sophisticated search indices by applying advanced algorithms. The pages that are found with search engines are known as part of the "Surface Web".

Over the years, those who try to determine the extent of the Internet reveal what we have long suspected: the Surface Web accounts for only one to four per cent of what is out there on the World Wide Web.

Go deep

There are, in fact, much more resources on the Internet that can be accessed only if the URL address is known. Examples of such pages are private corporate resources that are only meant to be accessed by employees or contractors, or simply resources that are not linked in from other pages.

These form what is known as the "Deep Web", the part of the Internet that has not been indexed by search engines.

On its own, the Deep Web is not ill-intentioned. It is what it is: a place that can only be accessed if you know the URL. No special permits or tools are needed to pry it open.


SURFACE WEB
Google
Bing
Wikipedia
Yahoo
Medical records
Legal documents
Academic information
Financial records
Scientific reports
Government reports
DEEP WEB
Intranet
Graphic media
Subscription databases
Multilingual databases
Password-protected pages
Conference proceedings
DARK WEB
Illegal information
Drug trafficking sites
Hacking groups and services
Private communications
TOR-encrypted sites

The Dark Web rises

However, residing within the Deep Web is a much shadier part of the Internet, called the "Dark Web" or "Dark Net".

The physical world equivalent will be the dark alleys that most will wisely not venture unless they are feeling adventurous, or are a familiar part of that community.

The Dark Web is where shady business thrive. Examples include:

- Sales of drugs and illegal items,
- Pornography (particularly child pornography which is illegal in most places with coordinated policing by the Interpol and various governments),
- BitCoin-related financial services,
- Hacking services (see the table "Available for sale in hackers' paradise")
- Pirated software

Accessing the Dark Web

When accessing a page using a conventional browser, the browser follows a direct network route to the destination. Assuming there are no special steps taken to make the connection anonymous (e.g. through VPN or anonymous proxy services), the destination resource is able to know the Internet address one is accessing the service from. Likewise, the user is able to determine the Internet address of the resource he or she is trying to access.

Obviously, this ease of mutual identification does not serve well for the Dark Web community. This part of the Internet is not meant to be directly accessible even with knowing the URL. To protect their own anonymity, such resources are only available to verified members of the community, and through the Tor network.

Tor is a free software that enables anonymous communication. The name is an acronym derived from the original mid-1990s software project, "The Onion Router" which was used to protect the security of US intelligence communications conducted online.

When using a specialised Tor browser, the anonymity of the data transport is achieved by encrypting the payload and routing it through a random list of relay servers distributed throughout the world. Each relay "peels away" one layer of the onion to reveal which relay server to subsequently forward to. Each relay only knows this much, just enough to route the encrypted package along.

This helps to create the cloak of anonymity that operators within the Dark Web seek to make it harder for law enforcers to track them down.

Just like in the physical world, we also do see law enforcement and threat intelligence operators within the Dark Web. Their objective is to gather relevant threat intelligence and perhaps even to avail of its product and services for law enforcement purposes.

The digital black market

The anonymity of the Dark Web creates a perfect environment for different trades to exist with lowered risk of discovery.

A prominent example was the Silk Road digital marketplace, which was allegedly founded and run by Ross William Ulbricht under the pseudonym, "Dread Pirate Roberts". Launched in 2011, Silk Road was an online marketplace for selling illegal drugs, accessible only through the Dark Web. It was shut down in 2013 by the FBI along with the arrest of Ulbricht.

We have also seen the rise of a thriving trade serving the hacker community with a matured

Available For Sale In Hackers' Paradise

Zero-day exploit information	These are hitherto unpublished vulnerabilities in software, which can be sold to individuals or entities for their own purposes. They are called "zero-day exploits" because they are yet to be made known publicly.
Exploit kits	The zero-day exploits can be packaged together into exploit kits that can be sold to either individuals, hacking groups, or other entities for their purposes of breaking into other systems. Usually, such exploit kits combine several capabilities so that there are more than one possible vector in gaining unauthorised access to the victims.
Stolen credit card details	Magnetic stripe information stored on credit cards that are stolen can be sold for the purpose of credit card fraud or duplication of such cards. It is envisioned that this category of malicious activities will disappear soon with the adoption of EMV chips on credit cards.
Stolen personal information	Stolen personal information can be sold and subsequently resold, possibly along with the exploit kits. The information serves as a pool of victims that can be targeted either in general phishing or spear-phishing (a more targeted form of defrauding victims over emails).
Hacking and surveillance services	Sometimes, a buyer does not want to be bothered with the tools and process, and only wants specific outcomes. Such services can also be bought for a price from digital black marketplaces.

supply chain and business models, so much so that the Dark Web has also been referred to as a "hackers' paradise" with products and services such as those shown in the table.

The increasing number and sophistication of tools and services available in the Dark Web has made cyberattacks a stark reality of the digital era. It is no longer possible to assume that with the right preventive measures, one can hope to prevent being a victim of a cyberattack. It all depends on the value of the information that is at stake, and how much the hacker is prepared to invest to get the most relevant or best exploit kit or services.

Enterprises should thus diversify their security expenditure to cover not just preventive measures, but also to ensure that they have the right detection and response capabilities.

What sets apart the digitally responsible organization from the rest is taking the right informed decisions to embrace the opportunities that the digital age brings, while in doing so, recognise the risks and put in the appropriate measures to safeguard the future of the business. ■

Gerry Chng is Partner, Advisory Services, EY. The views reflected in this article are the views of the author and do not necessarily reflect the views of the global EY organisation or its member firms.