3-2019

Peeling back the (onion) layers of the Dark Web

Singapore Management University

Peeling back the (onion) layers of the Dark Web

29 Mar 2019

Manoeuvring the minefield of risk and exposure

When Finnish courts sentenced the administrator of trading site *Sipulikanava* – "The Onion Channel" in English – to 40 months in prison last month, it raised concerns and discussions about the Dark Web again. The 45-year-old man in question was arrested for hosting a website which enabled the trading of illegal drugs, a shutdown of which echoed that of the fate of other similar illegal Dark Web marketplaces AlphaBay and Silk Road.

What exactly is the Dark Web? Do users, organisations and businesses understand this platform and know what is really there?

"Dark Web is an encrypted platform which is not accessible through traditional search engines," explains **Mikko Niemela**, CEO of Cyber Intelligence House (CIH), a Singapore-based company which specialises in the detection and monitoring of cyber exposure from the Dark and Deep Web. "The anonymity that the Dark Web allows, using a combination of routing and encryption, has made it a go-to place for discussing, planning and hosting illegal activities including drug trafficking, weapon trading, criminal, terrorist and cyber attacks which expose personal data."

While access to the Dark Web is not a crime in most jurisdictions, the anonymity it provides makes it a source of concern for authoritarian states. "The challenge that the Dark Web poses," Niemela elaborates, "is that it does not have an index and its nature is such that pages are taken down without any data trail left unlike in the normal internet space, which makes the security risk stakes higher than ever."

As a company dedicated to assessing and mitigating the cyber exposure of organisations and individuals, CIH built its own search engine to trawl through the Dark Web with a system in place to archive all the data and analyse the chatter, which is critical when it comes to investigating cyber breach occurrences.

KEEPING COMPANY INFORMATION SAFE FROM THE DARK WEB

Speaking to *Perspectives@SMU*, Niemela adds that companies in general do not know much about cyber exposure or what has to be done to mitigate threats. From his experience of assessing over 6000 organisations, he says it is imperative for companies to know and understand their exposure levels. This is particularly so with rapid digital transformation and the increasing complexity of networks, which is creating expanded attack surfaces and endless virtual entry points.

Once a breach occurs, it is safe to assume that fraud will follow within days, months or even years, as in the case of the Yahoo in September 2016, which was believed to have started as far back as 2013. When asked if companies are actively addressing this knowledge gap, Niemela laments that they are "not doing much".

In fact, he points out that most companies are less than steadfast when it comes to data safety. "Many assume that buying a preventative solution is enough, but in reality equal emphasis must also be put on monitoring and response", he points out.

The fundamentals of cybersecurity, Niemelma says, are understanding:

- What is the most critical information on which the survival of the company depends?

- Where is this information located – including the number of copies of this critical information that has been stored, including in desktops, laptops, cloud, USB sticks etc.?
- How many people have access to this critical information?
- What needs to be done to shore up these vulnerabilities?

“Companies and their employees should be trained to understand these fundamentals,” Niemela advises, adding that it has been found that more than 80 percent of cyber attacks against organisations happened through targeted employees. Therefore it is important for employees to be educated on the risk factors of sharing information, passwords etc.

CIH created a proprietary global scoring system called Cyber Exposure Index (CEI) which evaluates exposure of listed companies based on the signs of disclosure of sensitive information, leaked credentials and hacker-group activity tracked in the Dark and Deep Web. This index helps companies mitigate potential data breaches by identifying existing threats and loopholes within their organisations. “It also helps investors compare the risk levels between companies to make more informed decisions to grow their investment portfolios,” Niemela adds.

IT IS NOT ALL BAD

While it is true that the Dark Web is a hub of illegal activities for cybercriminals, a lesser-known fact is that the anonymous Dark Web browsers such as TOR and EPIC can also be used to access regular websites and is also used for legal purposes. With the anonymity and the ability to access sites that Chrome or Explorer cannot, the Dark Web is also used for investigative journalism and whistleblowing, testing of new internet services, or where marketers can also tap into the relatively unguarded nature of discussion on forums to discover unmet demands of consumers.

At the end of the day, there is no ignoring the dangers the Dark Web, the increased threats of data breaches, and also the magnitude of the impact. The issue about understanding the Dark Web and cyber exposure really boils down to: What data has already been exposed in the Dark Web? Who has access to it? What can be done to mitigate further exposure?

Follow us on Twitter (@sgsmuperspectiv) or like us on Facebook (https://www.facebook.com/PerspectivesAtSMU)