Tracing crime on the Dark Web

It's the section of the internet that is unknown to the vast majority of people. The Dark Web is a network of websites and servers that use encryption in an attempt to keep their activities secret. It isn't indexed by search engines but it's where fraudsters buy drugs, guns, credit card details and personal information. In fact, when researchers at King's College, London, looked at the contents of nearly 3,000 sites on the Dark Web, they discovered that 57 per cent were hosting illicit material.

The Dark Web is accessed via special browsers such as TOR, an open source protocol with a suite of plugins that has been built on top of Mozilla's Firefox web browser. The source and destination of web traffic are anonymised by passing an IP address through a network of other, encrypted IP addresses.

While the Silk Road, one of the best-known aspects of the Dark Web, is used by drug dealers and their clients, financial data is one of the most common forms of personal information sold and bought by fraudsters on Dark Web generally, while login details are also highly sought after. These can be used to access sensitive information on corporate sites as well as personal bank accounts. Information ends up on the Dark Web through sources such as data breaches, phishing or skimming and illegal activity by an individual within the organisation itself.

Information is being stolen to order

Demand for this essential information means that increasingly it is being stolen to order so that it can be traded on platforms on the dark web. Every aspect of an individual's life is currently available to buy for just £820, according to recent research by virtual private network review site Top10VPN.com.

Raw information on a credit card's magnetic strip is available for somewhere between 20 and 80 US dollars or "doughnuts" in the fraudsters' parlance.

Around the world law enforcement agencies are trying a range of new approaches in order to catch the Dark Web fraudsters and to close down their trading platforms. Hansa was, for a while, a popular platform which featured more than 24,000 listings for drug products.

Closing down Dark Web sites

In order to remove it Dutch Investigators identified the two people that they believed were behind Hansa and took over their accounts to gain control of the site itself. They then amended its codes so that they could identify those who were trading on it and take action against them. AlphaBay was the largest criminal marketplace on the dark web until it was removed by a Europol-coordinated operation of police forces from a number of countries in 2017. As well as providing over a quarter of million listings for illegal drugs and toxic chemicals police also found over 100,000 listings for fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools.

In the three years that it existed AlphaBay handled transactions valued at more than $1billion. The creator and administrator was a Canadian citizen living in Thailand. When the site was taken down, millions of dollars' worth of cryptocurrencies were frozen and seized.

Coordinated law enforcement

Europol now has a coordinated law enforcement approach which aims to tackle crime on the Dark Web alongside law enforcement agencies from across EU Member States. The US military's Defense Advanced Research Projects Agency (DARPA) is building a special search engine called Memex that can combat sex trafficking on dark web.

The Dark Web might be evolving and the demand that it is creating for stolen sensitive data growing but the practices required to keep it at bay are well established. The assumption must be that an organisation will be the target of an attack which will lead to information about it being offered on the dark web.

As hacking incidents affecting blue-chip companies have become more common and widely reported, an increasing number of reputable brands have found themselves reacting to claims that consumer information hacked from their systems is now available to fraudsters on the Dark Web.

Last year, following a cyberattack on British Airways, it was reported that the credit card details of 380,000 of its customers could have been on sale on the Dark Web. The information, which was thought to include the security CVV codes for customer credit cards, could have been worth as much as £20million. In 2016 a BBC investigation revealed that phone numbers, emails, passwords and dates of birth of o2 customers was being traded on the Dark Web.

Monitoring the Dark Web – expertise required

To prevent their data being traded on this sinister version of the internet, organisations need to ensure that they have appropriate controls and monitoring measures in place. A layered approach should include anti-cyberattack technology alongside staff training and awareness campaigns.

Given its lawlessness, complexity and lack of transparency, monitoring the Dark Web requires expertise and experience. It is often difficult for organisations due to a lack of highly skilled resources and skillset they typically have available. Instead, companies would be better served by working closely with a technology provider who can provide the relevant support along with assistance in closely monitoring the Dark Web for relevant data using specialist tools and techniques.

Muthmainur Rahman
Senior Managing Director
+971 (0) 58 562 4020
muthmainur.rahman@fticonsulting.com

FTI CONSULTING™

EXPERTS WITH IMPACT

0633-01/19