THE DARK SIDE

The dark web often conjures up images of shadowy criminal gangs committing online crime

Andrei Barysevich *shines a light on the dark web and how it can be used to stop malware attacks before they happen*

Anything related to hacking and cyber crime has always had a tendency to fall victim to exaggeration and mischaracterisation in the media and popular consciousness. One of the most recent examples is the dark web, which has become something of a catchall phrase but is generally used to conjure images of shadowy criminal gangs gathering to commit crimes online.

The truth is a bit more nuanced, however, and while the concept and practices of the dark web have existed for many years, the phrase itself has become increasingly popular as general awareness of cyber crime grows. Activity by high-profile criminal groups has helped to draw attention to the way these hidden communities are used, most recently seen with The Shadow Broker group, which leaked the NSA toolsets that eventually led to the WannaCry attack.

By understanding the true nature of the dark web, it is possible to use it as a powerful source of threat intelligence. Accessing these hidden communities can provide insight into everything from the theft of commercial data, to potential attacks on governmental and national infrastructure.

Perhaps befitting its secretive purposes, the dark web has often proven to be confusing and hard to define. The concept is frequently conflated with the deep web – a term used to refer to any website not indexed by Google or other search engines. However, this term is too broad and the dark web would best be considered as a specific subset of the deep web.

My favourite way to describe the dark web in non-technical terms is to compare it to a nondescript bar entrance in a dark alley – the kind of place that you won't find in the *Yellow Pages* or Google Maps. If someone knows the secret knock and the password, the door will open to them, but will remain firmly shut and implacable to anyone else. Inside, a selection of shady patrons are waiting to offer illicit goods and services to trusted regulars.

HIDDEN NETWORKS

Similarly, dark web communities cannot be found via search engines, and patrons will generally know exactly what they are looking for. These sites are usually only accessible through networks such as Tor – 'The Onion Router', so named because it uses layer upon layer of encryption to provide anonymity. Data is routed through a large number of servers around the world, and the transmitted information can only be decrypted by the next node in the network. This makes it impossible to decrypt the information and trace the IP of the users to learn their location and identity.

> BY UNDERSTANDING THE DARK WEB, IT IS POSSIBLE TO USE IT AS A SOURCE OF THREAT INTELLIGENCE

Just as with our hypothetical secret bar, these communities frequently use this ironclad anonymity to undertake illegal activity. Many of these practices were brought to light when a landmark international law enforcement investigation in July brought down AlphaBay and Hansa, two of the most prominent marketplaces. Europol reported that more than 250,000 listings for drugs and toxic chemicals were available on AlphaBay alone.

Drugs also made up more than 70 percent of trade on Silk Road, another famous marketplace that was shut down in 2013 by the FBI. Contrary to popular opinion of the lawlessness of the dark web, however, Silk Road and many other marketplaces like it actually have their own terms of service, barring the sale of products such as weapons or child pornography, and services like assassination.

Likewise, while many may think that dark web users are members of crime syndicates and other powerful underworld figures, the average user is much more likely to be a small-timer. Most will only be wannabe hackers that engage in illegal cyber activity occasionally, while others aren't even cyber criminals at all – simply people after something less sinister like stolen Netflix credentials.

SUPPLY AND DEMAND

The sites themselves often resemble mainstream online bulletin boards such as Craigslist, with members posting the products and services they have for sale, or requesting services and connections with others. We generally see these communities take on two distinct forms. The more technical sources are devoted to the development of malicious software and supporting infrastructure, while more commercial marketplaces specialise in the sale of stolen data, financial information, drugs, compromised accounts, *etc*.

A good demonstration of the way these communities operate came when the group calling itself The Shadow Brokers released part of its cache of stolen NSA exploits. We saw individuals quickly dedicate themselves to researching the tools and sharing the information to allow others to use them in malware attacks. For example, a member of a top-tier Russian-speaking criminal community soon analysed the ETERNALBLUE and the DOUBLEPULSAR kernel payload and an in-depth tutorial was produced within three days. The tutorial quickly spread far and wide, and was almost certainly used by the actor behind the recent infamous WannaCry ransomware, as the attack used both of these exploits together.

As expected from a community that has gone to such pains to remain hidden, getting access is far from easy. The first challenge is that in many cases, only existing members can tell a newcomer how to find a particular community. Unlike our shady bar down a dark alley, there is no chance of accidentally stumbling upon one of these communities, and many don't even have names.

Most communities require a "donation" from new members, which can run from $500 to several thousand dollars. More challenging than fronting the money, however, is that a new member also needs to be vouched for by existing ones, which can take anywhere from six months to a full year. Some of the more commercial communities, such as the now-defunct Hansa, require neither fees nor vetting, leading to membership in the thousands and an automated approach closer to eBay.

TREAD CAREFULLY

Once they have gained admittance, researchers still need to be very careful how they operate. Asking too many questions will certainly raise some red flags, and we've also seen cases of researchers accidently revealing too much information, enabling astute hackers to discover their real identities, or the organisations they work for. All but the most experienced researchers are much better off reading and observing, rather than trying to engage directly.

So while the dark web might not be the lawless nightmare that many imagine, these underground communities still thrive on illegal activity – and accessing and understanding them can play a major role in preventing both traditional crime and cyber crime. As seen with the closure of AlphaBay and Hansa, shutting these places down can cut off sources of drugs and other illegal items – although these supplies invariably find new channels before long.

On the cyber side of things, the dark web is an incredibly valuable source of threat intelligence for law enforcement, governments and private enterprises. One of the most useful applications for dark web research is identifying assets or information compromised by a data breach, and in many cases there's a strong chance stolen information will show up on the dark web before the organisation even detects the intrusion itself.

▶

On a national level, Recorded Future researchers were able to prevent the sale of access to the US Election Assistance Commission (EAC) last year after monitoring the dark web and picking up chatter soliciting the sale. After engaging with the Russian-speaking actor to assess the full scope of the access on offer, it discovered the breach appeared to include more than 100 access credentials, including backdoor access to EAC servers via an SQL injection vulnerability. Using these accounts, a threat actor could access sensitive information or even covertly modify or plant malware on the EAC website. Once it was determined how serious the sale was, Recorded Future provided the information to federal law enforcement and assisted with the investigation.

PROACTIVE ACTION

In some cases, it's even possible to identify a potential attack before it happens by analysing threat actor communication. This could be a planned attack on a specific organisation, or new malware or exploits that have not yet been deployed. Spotting these threats ahead of time provides the opportunity for organisations to close vulnerabilities or strengthen technical controls in advance, hopefully mitigating the impact when the attack is launched.

Accessing and navigating the dark web requires a great deal of time and resources – and can be risky to anyone not prepared to deal with the way communities operate. The level of dedication required means that most organisations are best served by partnering with a third party specialising in the field. Taking on an external expert is also the most effective way to turn dark web research into usable intelligence.

Although fascinating, accessing one or two dark web communities is not a guarantee of usable information that can help to improve security. To gain the full picture of the threat landscape, intelligence needs to be drawn from as many sources as possible, combining dark web channels with more mundane and accessible forums and social media. By combining advanced machine learning and experienced human researchers, it is possible to analyse this vast array of data and distil it down to a manageable number of actionable points.

> **EUROPOL REPORTED MORE THAN 250,000 LISTINGS FOR DRUGS AND TOXIC CHEMICALS ON ALPHABAY**

For most, the dark web is likely to remain a murky and half-understood idea of the cyber underworld. However, those that are able to understand the dark web and penetrate its operations can arm themselves with powerful threat intelligence that will enable them to more effectively identity and counter new threats ●

Andrei Barysevich is the Director of Advanced Collection at Recorded Future. He specialises in threat intelligence on highly restrictive criminal communities and he oversees proactive intelligence operations. He was previously an independent e-commerce fraud researcher and a private consultant for the FBI's New York Cybercrime field office.

The dark web is widely considered as a specific subset of the deep web