SHINE A LIGHT

Ziv Mador *delves into the depths of the DarkWeb and explains why it's important to understand its workings to stay one step ahead of its threat*

The Dark Web has long served as an invaluable tool for facilitating international crime. From firearms and narcotics to violent services for hire, any illegal item or criminal endeavour you can imagine can be found if you know where to look.

As a digital environment, it is also a natural home for all things cyber crime. Closed forums provide cyber criminals with a place to sell stolen data and credentials, purchase malware kits and expertise, and hire specialists to help with attacks.

Many of the prominent underground marketplaces on the Dark Web have been closed thanks to well-executed strikes involving coordinated efforts from international law enforcement. However, it is something of a Hydra. Every time a forum is closed, more will spring forth to replace them. The Dark Web, therefore, remains the premier method for cyber criminals around the world to communicate with each other.

As such, being able to locate these hidden forums and infiltrate their communities is a valuable advantage for organisations targeted by criminals. Shining a light into the dark can reveal both general trends in cyber attacks, and even planned activity targeting specific companies.

The virtual nature of the Dark Web means it facilitates criminal activity on a global scale and a user's physical location has no bearing. Forums are usually divided by language; Russian tends to be the common tongue for closed forums. English, Chinese and Portuguese are also very popular in forums and ads.

One of the most remarkable things about the Dark Web is how organised it is. It can be a surreal experience to browse forums and see an array of criminal services and resources for sale as neatly as though you were on Gumtree or Craigslist. Transactions are usually completed in cryptocurrency, with criminals going through laundering processes to obscure their trail against law enforcement.

The criminal underground has also increasingly become a dark reflection of a legitimate economy. Just as we have supply chains of large companies buying goods and services from smaller suppliers, threat actors specialising in different areas will sell their capabilities and assets to other individuals and groups.

For example, you'll find individuals who are skilled at developing malware, but prefer not to get their hands dirty by directly launching attacks. Instead, they will sell access to malware kits, complete with instructions, enabling other criminals to use them instead. This kind of transaction has had a major impact on the volume and sophistication of cyber attacks, as even relatively unskilled criminals can access powerful malware tools that they could not have developed themselves. Ransomware kits have become one of the most popular commodities, as well as malware that can facilitate more complex attacks such as keyloggers.

Every so often we come across zero-day exploits for sale. These are some of the most premium items on the Dark Web, with for example one Windows zero-day we encountered selling for over $90,000. However, these are fairly rare as most criminals are content with buying cheaper commodity malware since these will get the job done just as adequately.

You will also find huge volumes of data for sale as criminals seek to profit on the loot of previous attacks. For example, some will steal corporate log-in

THE LACK OF LEGAL PROTECTION MEANS INFILTRATING THE DARK WEB CAN TAKE YEARS

credentials and sell them on to other groups that will then execute the full attack.

High-value data assets such as intellectual property can occasionally be found, but the majority of stolen data is sold as a bulk commodity. Databases containing the personally identifiable information (PII) of many millions of citizens are bought and sold on a regular basis, with medical records being particularly popular. These assets are used by other criminal gangs to facilitate fraud, blackmail, and social engineering attacks.

Many criminals also specialise in selling on credit card details acquired through stolen databases or card skimming. Credit card sets are priced based on the accessible funds in the bank account, and the effectiveness of the particular card issuer in identifying and shutting down fraudulent transactions. A fully cloned card that grants bank account access may sell for $200-$800, while credit card numbers and CVCs, which will enable online purchases, can be as cheap as $20.

The virtual nature of the Dark Web means it facilitates criminal activity on a global scale

Alongside datasets, hacking knowledge is also a valuable asset on the Dark Web. Specialists might for example provide guidance on how to exploit a particular vulnerability or avoid a certain security tool.

In 2020, for example, we saw a large amount of information being offered around exploiting companies left vulnerable by the COVID-19 pandemic. This has included malware designed to exploit remote access connections as well as social engineering techniques to fool remote workers by impersonating their IT departments. There has also been a surge in offers of broader efforts such as phishing attacks baiting people with an offer of access to COVID relief money or information about the virus.

As well as being sold on for cash, information is often offered up for free. This is no act of altruism, but rather done as a way of boosting the user's reputation on the forum. Like the physical criminal world, reputation is extremely important on the Dark Web. Building a good reputation will grant the member access to more information on the forum and give them the ability to conduct business with other forum members more easily and on a wider scale.

Taking the first step into the Dark Web is as easy as installing the open-source anonymity Tor browser. The software is completely legal and freely available, having first launched in 2008 as a way of providing individuals with anonymity online. Tor, or 'The Onion Router', takes its name from the onion routing used to hide its users' identities. Communications are encrypted and bounced at random through relays across the world, making it all but impossible to trace users through their IPs. Unfortunately, these capabilities are also perfectly suited for criminals hiding from law enforcement.

After installing the Tor browser, it takes very little effort to find online marketplaces advertising illegal services including stolen data and goods, drugs and counterfeit documents. Despite all the brazen criminality on display, however, this is only the surface of the Dark Web. Security researchers will find little at this level that will be of use in helping organisations defend themselves against attacks.

The most valuable intelligence can only be found within hidden cyber criminal communities, protected by restricted-access forums. I have spent many years as a security researcher navigating these secret networks.

Higher level Dark Web forums could be compared to a mobster's den, or one of the illegal speakeasies of the prohibition era. The owners and occupants are well aware that law enforcement agents will be trying to find a way in to learn their secrets and carry out a bust, so one simply cannot wander in off the street.

While the virtual world offers a much greater level of protection than any physical meeting place, there have been a number of successful raids. In September for example Europol announced the success of operation 'DisrupTOR'. The operation, which involved coordination between multiple law enforcement agencies, saw the arrest of 179 criminals involved in a variety of illegal activities.

While law enforcement will always be the biggest concern, criminal forums are also acutely aware of security researchers trying to learn their secrets and help companies defend against the latest attacks.

Accordingly, just like their physical counterparts, these forums are invitation only and require new

entrants to be vouched for by an existing member. Even finding many forums is impossible without being sent an invitation link.

In addition, forums often operate tiered access based on user reputation. Individuals that are active and seen as contributing to the community will be given more reputation points and afforded more capabilities. Often, new users will not be able to make their own posts without sufficient reputation, for example, and more rep could also enable access to more areas of the forum.

Sharing information is one of the most effective ways of increasing reputation and credibility, and users will often post advice and guidance on areas such as establishing persistence and evading the latest detection tools or developing and using malware.

Just as with officers going undercover to physically infiltrate gangs, individuals working on behalf of law enforcement agencies are afforded a certain level of leeway to establish and maintain their cover. Even then, building reputation in a forum is a slow and painstaking process. For security researchers working on a private basis, the lack of legal protection means infiltrating the Dark Web will usually require years of work. Researchers must be careful to establish reputation without incriminating themselves.

The knowledge and time required to penetrate closed forums means it's something best left to specialists with years of experience behind them. Companies that invest in access to these skills, however, can reap some powerful rewards to help prevent cyber attacks.

Acquiring threat intelligence from Dark Web forums will provide useful insights into the latest developments in cyber criminal activity. When new attack techniques and malware appear, the organisation's security team will have a valuable early warning that will give them time to harden their defences and update their response playbooks.

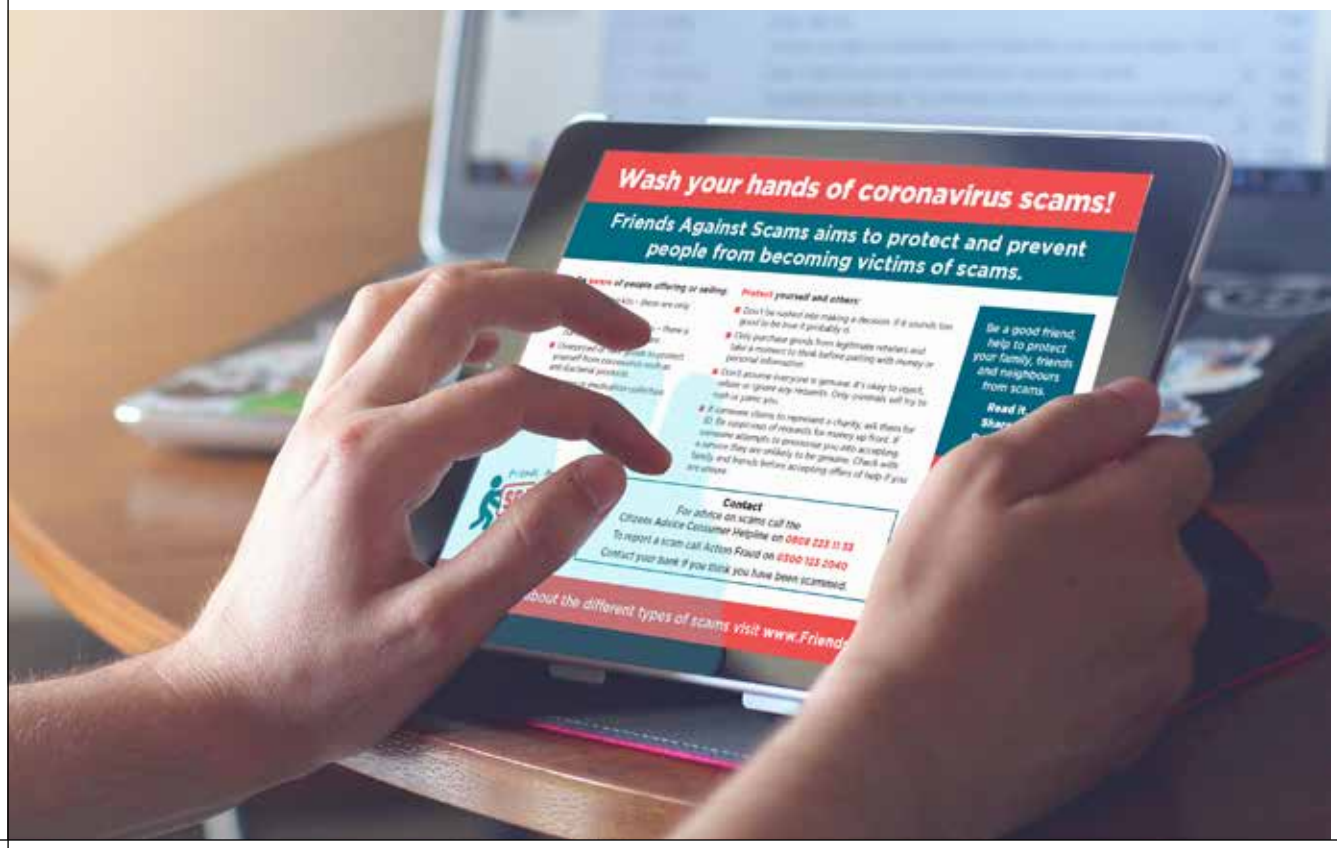
For example, if a new phishing scheme emerges which aims to exploit remote workers by impersonating a popular cloud service provider, the security team will be able to both update email security solutions and improve awareness among staff to help them spot the scam. Similarly, if a new exploit or malware kit is being traded around, the company can ensure that all of its systems have been updated and patched to close the vulnerability.

Alongside this steady supply of general insight into cyber developments, Dark Web intelligence can also provide an early warning of threats against specific companies. Large-scale attack campaigns will often target a number of companies within a specific sector at a time, for example going after a list of universities or healthcare providers. When threat actors use the Dark Web to acquire resources and information for these attacks, companies can be alerted to potential incoming threats and prepare their defences. The largest and most prominent organisations with high-risk profiles will also be able to identify planned attacks targeting them specifically.

Organisations also have much to gain by monitoring the flow of stolen data for sale on the Dark Web. Databases and credentials being advertised as belonging to specific companies are a useful indicator of a breach. When PII is involved, the company will have a better chance of confirming the scope of the breach for customer and regulatory notifications. If credentials are involved, the business may have the opportunity to change passwords before they can be exploited.

Despite being weakened by law enforcement stings, the Dark Web will continue to provide an effective haven for cyber criminals to trade skills, information and stolen assets. However, those that can infiltrate and monitor it can turn these hidden communities against the criminals, helping organisations to identify and mitigate the biggest threats coming their way ●

Ziv Mador, VP Security at Trustwave, manages the global security research team covering research areas such as vulnerability assessment and scanning, analysis of attacks against web servers and web clients, malware reverse engineering, IDS/IPS research, SIEM correlation and reporting, spam and phishing research, threat intelligence and database security research.



National Trading Standards is just one organisation providing advice on Covid scams