radware

UNDERSTANDING THE DARKNET/DARK WEB AND ITS IMPACT ON CYBERSECURITY

The darknet. It's a very real concern for today's businesses. In recent years, it has redefined the art of hacking and, in the process, dramatically expanded the threat landscape that organizations now face. It's important to understand what the darknet is, why you should care, how it has forever altered cyberattacks and how your organization can protect itself from the dangers lurking within.

WHAT IS THE DARKNET?

Not to be confused with the deep web, the dark web/darknet is a collection of thousands of websites that can't be accessed via normal means and aren't indexed by search engines like Google or Yahoo.

Simply put, the darknet is an overlay of networks that requires specific tools and software in order to gain access. The history of the darknet predates the 1980s, and the term was originally used to describe computers on ARPANET that were hidden and programmed to receive messages but which did not respond to or acknowledge anything, thus remaining invisible, or in the dark. Since then, "darknet" has evolved into an umbrella term that describes the portions of the internet purposefully not open to public view or hidden networks whose architecture is superimposed on that of the internet.

Ironically, the darknet's evolution can be traced somewhat to the U.S. military. The most common way to access the darknet is through tools such as the Tor network. The network routing capabilities that the Tor network uses were developed in the mid-1990s by mathematicians and computer scientists at the U.S. Naval Research Laboratory with the purpose of protecting U.S. intelligence communications online.

USE AND ACCESS

Uses of the darknet are nearly as wide and as diverse as the internet: everything from email and social media to hosting and sharing files, news websites and e-commerce. Accessing it requires specific software, configurations or authorization, often using nonstandard communication protocols and ports. Currently, two of the most popular ways to access the darknet are via two overlay networks. The first is the aforementioned Tor; the second is called I2P.

Tor, which stands for "onion router" or "onion routing," is designed primarily to keep users anonymous. Just like the layers of an onion, data is stored within multiple layers of encryption. Each layer reveals the next relay until the final layer sends the data to its destination. Information is sent bidirectionally, so data is being sent back and

forth via the same tunnel. On any given day, over one million users are active on the Tor network.

I2P, which stands for the Invisible Internet Project, is designed for user-to-user file sharing. It takes data and encapsulates it within multiple layers. Just like a clove of garlic, information is bunched together with other people's information to prevent depacking and inspection, and it sends that data via a unidirectional tunnel.

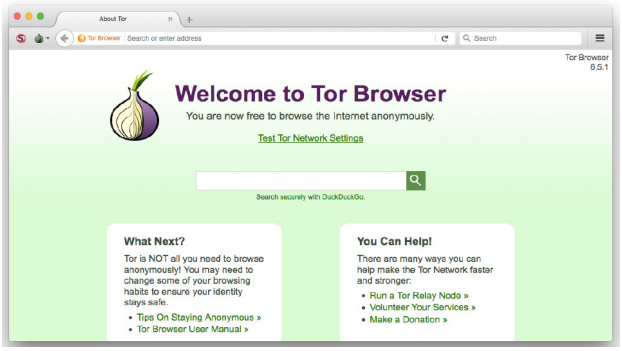

Figure 1: The Tor browser

WHAT'S OUT THERE?

As mentioned previously, the darknet provides news, e-commerce sites, and email and hosting services. While many of the services are innocent and are simply alternatives to what can be found on the internet, a portion of the darknet is highly nefarious and tied to illicit activities due to its surreptitious nature. As a result, since the 1990s, cybercriminals have found a "digital home" on the darknet as a way to communicate, coordinate and, most recently, monetize the art of cyberattacks to a wide range of non-technical novices.

One of the most popular services are email services, which have seen a dramatic increase in recent years that parallels the increased popularity of ransomware. Cyberattackers will often use these email services to execute their campaigns to remain hidden from authorities.

Hosting services are yet another. Similar to the cloud computing environments that enterprises might use as part of their IT infrastructure, darknet hosting services are leveraged by cybercriminals and hackers to host websites or e-commerce marketplaces that sell distributed denial-of-service (DDoS) tools and services. These hosting services are typically very unstable as they can be "taken down" by law enforcement or vigilante hackers for political, ideological or moral reasons.

Forums also exist to allow hackers and criminals to have independent discussions for the purpose of knowledge exchanging, including organizing and coordinating DDoS campaigns (such as those planned by Anonymous) and/or exchanging cyberattack best practices. These forums come with a variety of technical options and languages and can be associated with particular threat actors/ groups, hacktivists, attack vectors, etc.

Lastly, just like the real internet, darknet search engines exist to allow users to easily locate and navigate these various forums, sites and e-commerce stores. Examples of these search engines include Candle and Torch.

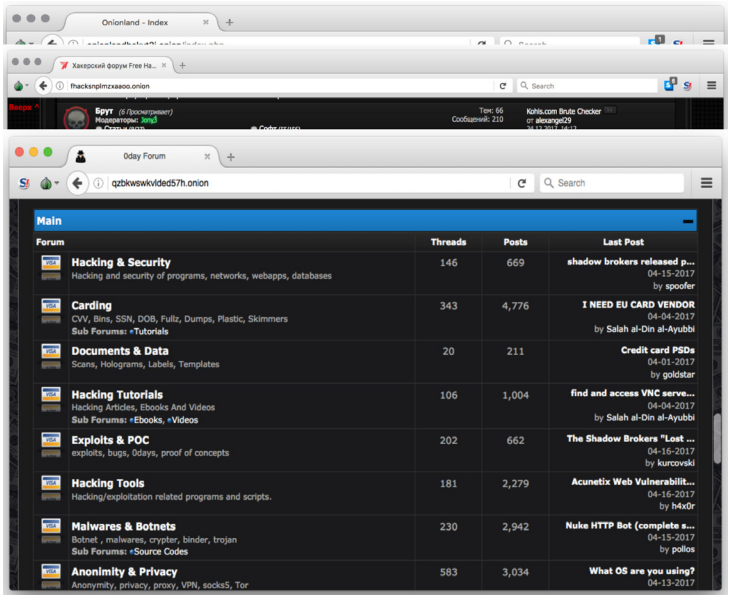

Figure 2: An example of one DDoS forum that can be found on the darknet

A DIGITAL STORE

Perhaps more than any other service usage, e-commerce sites on the darknet have exploded in popularity in recent years due to the rise of DDoS as a service and stresser services, resulting in huge profit margins for entrepreneurial hackers. Everything from DDoS attack tools and botnet rentals to "contracting" the services of a hacker are now available on the darknet.

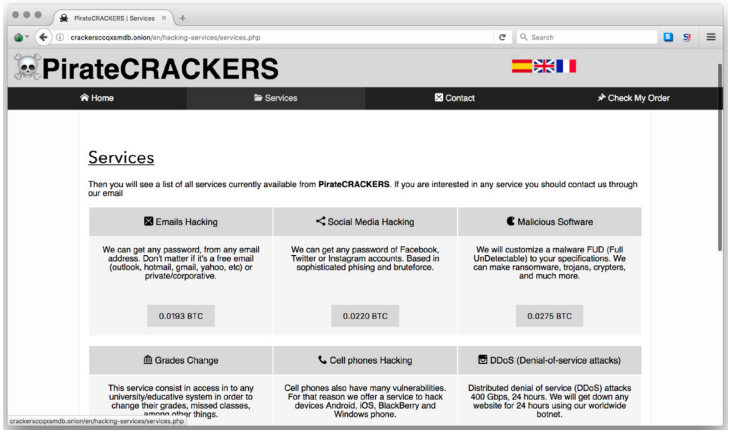

Figure 3: List of cyberattack services available from one site on the darknet

The result? These e-commerce sites and their products have commoditized cyberattacks in addition to making them available to a wide range of non-technical users. Often times, these services come with intuitive, GUI-based interfaces that make setting up and launching attacks quick and simple.

Examples abound, but one example of DDoS as a service is PutinStresser. PutinStresser illustrates the ease of access that these services have reached and provides potential buyers with various payment options, discovery tools, a variety of attack vectors and even chat-based customer support. Botnet rental services are also available — their growth paralleling the growth and use of botnets since 2016. A perfect example of a botnet service that is available on the darknet is the JenX botnet, which was discovered in 2018.

Prices for these tools are as diverse as the attack vectors that buyers can purchase and range from as low as $100 to several thousand dollars. Prices are typically based on various factors, such as the number of attack vectors included within the service, the size of the attack (Gbps/Tbps) and the demand.

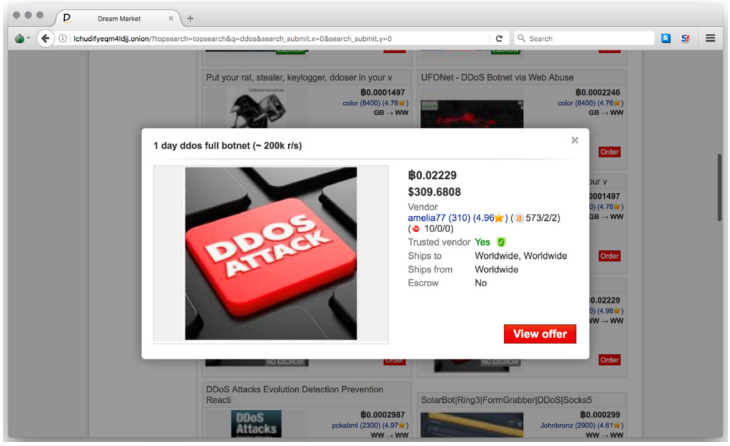

Figure 4: A one-day DDoS botnet for rent on the darknet

Malware and ransomware are equally popular. The notorious WannaCry global ransomware campaign had its C2C servers hosted on the darknet. In addition, just like their botnet and DDoS brethren, malware and ransomware have their own "pay for play" services which dramatically simplify the process of launching a ransomware campaign. Numerous ransomware services exist that allow a user to simply specify the ransom amount and add notes/letters, and then the user is provided a simple executable to send to victims.

Lastly, an array of services is available allowing nearly anyone with access to the darknet (and the ability to convert money to bitcoin for payment) to contract hackers for their work. Services include hacking emails, hacking social media accounts and designing malicious software.

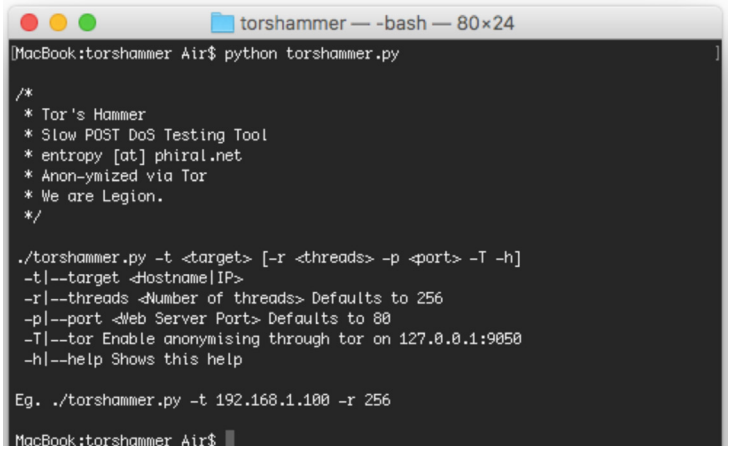

Figure 5: A screenshot of the jRAT ransomware as a service

Many of these services revolve around the education vertical. The act of educational institutions moving their teaching tools and testing to online networks has bred a new generation of students willing to purchase the services of hackers to change grades and launch DDoS attacks on schools' networks to postpone tests.

THE X FACTOR

Ultimately, the darknet has become incredibly popular for three main reasons: privacy, obfuscation and opportunity. The majority of hackers are inherently lazy and desire turnkey access to tools and best practices that simplify the art of cyberattacking while making money as an added benefit.

This point has broad implications for organizations seeking to keep their sensitive data secure. Whereas cyberattacks used to be the expertise of tech-savvy cybercriminals, the darknet has commoditized cyberattacks and made them available to a wide range of non-technical users. As a result, it is largely responsible for exponentially increasing the threat landscape that organizations now face.

According to Radware's *2018–2019 Global Application & Network Security Report*, the initial costs of a cyberattack have increased nearly 50% to $1.1 million. Here are five tips[1] to help you protect yourself against DDoS attacks and other threats that lurk on the darknet:

Don't Assume Your Company Is Not a Target: According to the same report, 93% of organizations globally report being attacked in 2018. The impact of cyberattacks on customer retention, response costs and operating expenses is too great to not succeed in mitigating every threat, every time. Cybersecurity must be an executive priority across the entire C-suite.

One Tool Can't Do It All: Many organizations attempt to mitigate DDoS attacks with solutions not suitable for a DDoS defense or limit their mitigation solutions to one-off security tools, such as firewalls. During DDoS attacks, these tools can often create bottlenecks and accelerate outages if not implemented properly.

Multilayer Protection Is Key: According to the aforementioned report, nearly half of all organizations now leverage a hybrid approach that combines on-premise protection with cloud-based scrubbing capabilities. The mitigation appliance blocks application and short-lived attacks while cloud-based capacity servers scrub network traffic during volumetric assaults.

Know Your Limitations: New attack vectors/vulnerabilities in networks, applications and databases emerge every day. Exasperating the issue is the shortfall in cybersecurity talent. A key element to preparedness is an accurate understanding of the security strengths and weaknesses within your environment. Take the time today to help make sure your business remains secure tomorrow.

Partner With a Cybersecurity Intelligence Agency: To assist with overcoming the previous challenge, partner with a security service provider that can supplement your in-house knowledge of attack campaigns, new attack vectors and DDoS trends with real-time intelligence. It is possible to block your enterprise network from malicious IP addresses and known threat actors on the darknet, but having that intel in a timely manner is key.

LEARN MORE about the cyberattack threat landscape and DDoS mitigation best practices at DDoSWarriors.com.

[1]https://www.bizjournals.com/kansascity/news/2017/10/01/5-tips-to-protect-your-business-from-darknet.html