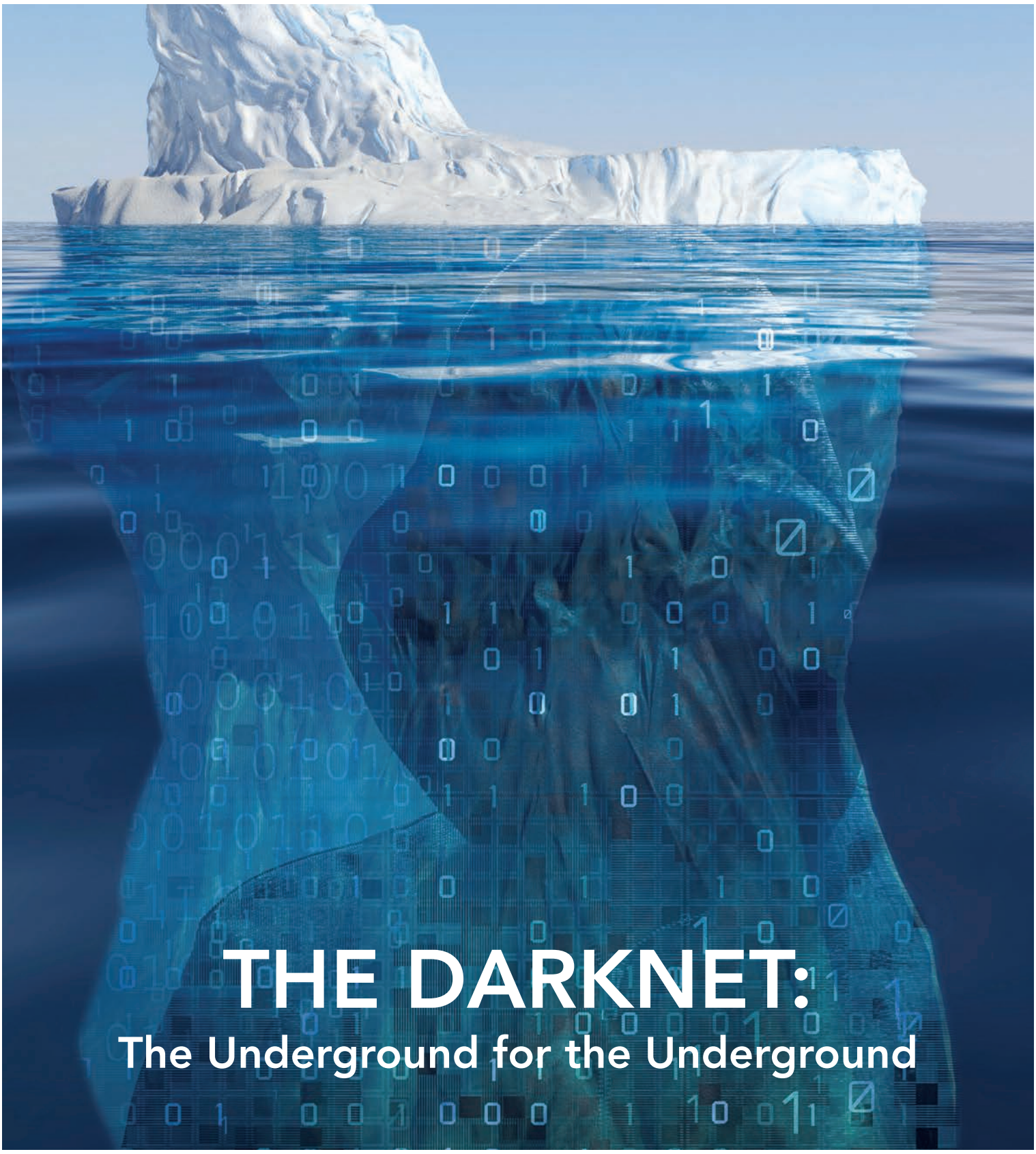

THE DARKNET:

The Underground for the Underground

BATBLUE

THE CLOUD SECURITY COMPANY

www.batblue.com

Contents

The Darknet: Introduction

The Internet as most users know it is only a fraction of what is out there.

The Darknet was invented by the U.S. naval intelligence research lab which wanted a Web browser that would allow intelligence officers to browse the Internet without revealing their identities. Unlike the "surface Internet" or "clear Internet," which is indexed by search engines like Google, Bing, and Yahoo, the Darknet is not indexed and requires special software to access.

The Darknet is a part of the Internet where people can interact anonymously online. It is often accessed using encryption mechanisms like ToR, but there are other ways to access the network, such as through password-protected forums. The Darknet is used to purchase and sell illegal drugs, pornography, and hacking exploits, as well as legitimate purposes like avoiding government censorship in repressive countries and contacting journalists anonymously.

The Darknet has an estimated 200,000 to 400,000 sites, with the exact number impossible to determine. Websites are hosted on servers with hidden locations thanks to encryption and virtual private networks (VPNs). As a result, Darknet sites are extremely difficult to shut down. Some researchers believe that websites related to child abuse and child pornography could account for as much as 80 percent of traffic to ToR hidden services.

DEFINITIONS: Darknet vs. Deep Web

The Darknet and Deep Web are often used as synonyms, but there is a distinction. The Deep Web refers to all online material, including the Darknet and mainstream sites, that is not indexed or not accessible through search engines. For example, a majority of the content on Facebook is part of the Deep Web because many users set their privacy settings to only allow friends to view their profile. The Deep Web includes many webpages that are encrypted with passwords or documents in formats that cannot be indexed. Therefore, the Darknet is part of the Deep Web, but the Deep Web is a much broader term than the Darknet.

What is ToR?

The Onion Router (ToR) is a technology that anonymizes users and allows them to browse the Internet without revealing their identities, developed by the U.S. Navy Research Laboratory in the mid-1990's to hide communication. The Laboratory released the code for ToR under a free license in 2004.

When a user peruses the web with a ToR-based browser, his or her communications are automatically bounced off of several other ToR servers before they reach their destination. The process makes it almost impossible for anyone to trace the traffic.

ToR also functions as a method for hosting hidden services, such as the websites and applications that make up the Darknet. Hidden sites use a string of seemingly random characters, followed by the domain name .onion. These hidden sites can only be accessed by other ToR users.

ACTORS: Those who lurk beyond the shadows of the Darknet

Public

- Politically Oppressed
- Socially Disenfranchised
- Whistle Blowers
- Illicit Product/ Service Buyers

Government

- Agencies
- Contractors
- Researchers

Criminals

- Drug Cartels
- Organized Crime
- Human Trafficking

xHATs

- Script Kiddies
- White Hats
  - Vulnerability Researchers
  - Ethical Hackers
- Gray Hats
  - Hacktivists
- Black Hats
  - Botmasters
  - Financial Hackers
  - Hackers
  - Trolls

Terrorists

- Political Terrorists
- Environmental Terrorists
- Religious Terrorists

DARKNET SECTORS

How to Access the Darknet

Accessing the Darknet is relatively easy; browsing it is difficult.

First, a user must download a ToR browser from **https://www.torproject.org/**. Downloading a ToR browser is quite simple and easy to use. ToR is based on Firefox, making its functions convenient for most users who are familiar with the popular browser. The ToR browser is available on Windows, iOS, and Linux.

Using ToR alone does not leave a user completely anonymous. Mac OSX and Windows both have security holes that must be fixed with other software. Some users employ a system called The Amnesiac Incognito Live System (TAILS) for added security. It is also advisable to use a virtual private network (VPN) for increased anonymity.

The Darknet is accessible through proxies such as Onion.City; however, browsing the Darknet this way does not ensure anonymity.

Secondly, users must find a directory site or similar list of .onion URLs. Since .onion websites are hidden, the Darknet is very difficult to browse. Darknet webpages are not indexed by search engines. However, several pages such as the Hidden Wiki (**http://zqktlwi4fecvo6ri.onion**) provide an index of links to the most popular marketplaces and chat forums. Websites such as DuckDuckGo (**http://3g2upl4pq6kufc4m.onion**) and Grams (**grams7enufi7jmdl.onion**) function as close to a "search engine" as possible, but links on these sites are often false or out of date.

Using ToR to browse the Darknet can be frustrating for a user. Since ToR utilizes a number of relays to anonymize browsing, it can take thirty seconds or longer to load a webpage.

It is important to remain cautious when using the Darknet and refrain from downloading any materials. Links may not lead to the website as claimed, and could instead lead to a website selling illegal or shocking materials.

Anonymous Mobility

The major attraction to the Darknet is the benefit of anonymity. However, the Darknet is not only anonymous, it is also highly mobile. The typical static Domain Name System (DNS) of the traditional Internet has given way to a dynamic process where Darknet sites update the ToR network to deliver an anonymous service known as a Hidden Service. Furthermore, the traditional process of acquiring domains from a registrar is replaced with a self-generated public / private key pair address.

The public key is used to generate a sixteen character hash (a one-way mathematical operation that creates a reference to the public key) that ends in a .onion. Here is an example of a .onion hash of a public key: batblue4y5flmoji.onion. The .onion hash serves as an address to access the Hidden Service much like a Fully Qualified Domain Name (FQDN) on the traditional Internet such as: **www.BatBlue.com**.

Once a site is accessed, it goes through a key exchange process with the accessing system to establish an encrypted channel for communications to take place. Since communications are encrypted end-to-end, traditional security tools do not have visibility into the communications rendering them minimally effective.

To create a .onion address special tools may be used like Shallot and Eschalot to generate a public / private key pair and a .onion hash. An imposter can theoretically use the same tools to reverse engineer a specific .onion site's address. However, given the compute resources available today this is highly improbable. Below is a list highlighting general compute time needed to replicate characters in a .onion address.

Characters	Time to Generate
1	Sub Second
2	Sub Second
3	Sub Second
4	2 Seconds
5	60 Seconds
6	30 Minutes
7	1 Day
8	25 Days
9	2.5 Years
10	40 Years
11	640 Years
12	10 Millenia
13	160 Millenia
14	2.6 Million Years

It is feasible that the developers of ToR could decide to filter or block specific .onion sites; however, this would take away from the integrity of the overall service. ToR developers have not yet attempted to filter or block .onion sites, nor is it conceivable that they would in the near future.

Once a site registers with the ToR network, all traffic will be appropriately routed to it regardless of its location, making the .onion site highly mobile and available on-demand. For example, a notebook computer can be outfitted with a ToR client and a web server. The notebook can then be taken to a location with public Internet access such as a coffee shop.

Many retail facilities have cameras so in order to maintain anonymity, the individual can stand or park within WIFI range outside of the coffee shop. The individual may also choose to keep the notebook computer inconspicuously in a backpack. As soon as WIFI connectivity is achieved, the system registers with the ToR network making it accessible for the user and ready for a transaction. Once the transaction is complete, the individual can simply walk or drive away.

The design of the Hidden Services platform offers enhanced mobility for those accessing content as well as those who serve content or services. ToR can be served up and accessed from anywhere, at anytime, for any service, making it a highly mobile and versatile anonymous platform.

The Markets of the Darknet

The Darknet has gained notoriety for its markets selling illegal goods and services, including drugs, child pornography, fake identification and passports, and stolen movies and music.

The most popular marketplaces include Agora, BlackBank, Alphabay, Cloud-Nine, Evolution, NiceGuy, Pandora, East India Company, and The Pirate Market—some of which have already been shut down by the FBI and other law enforcement authorities. Websites on the Darknet also contain how-to guides such as *The Terrorist Handbook*, which details how to create bombs and other weapons, access to hit men and links to forums for terrorist groups like the Islamic State of Iraq and Syria (ISIS).

The Darknet covers more than just illegal substances and immoral activities. Political dissidents, free speech and privacy advocates use the Darknet to communicate and share information banned by their governments. Wikileaks, founded by Australian Julian Assange in 2006, was launched as a Darknet site before going public, and still exists on the Darknet today as a place where dissidents and whistleblowers can anonymously upload information. Hacktivist groups like Anonymous and Lulzsec use ToR to communicate and plan operations. Journalists and media companies use ToR to communicate with sources who wish to remain anonymous. Darknet users often have a strong libertarian stance operating the Darknet to explore a world without laws and experiment with different forms of law and self-rule.

SILK ROAD: The Soul of the Darknet

Ross Ulbricht, creator of the Silk Road

Silk Road was a website on the Darknet that functioned as an illicit marketplace selling drugs, stolen credit card numbers, fake identification, pirated entertainment, and even hit men. All transactions were conducted in Bitcoin, a Cryptocurrency that cannot be traced. The site was run by Ross Ulbricht under the pseudonym Dread Pirate Roberts.

Silk Road operated from 2011 to 2013, leading to over 4,000 drug sales worth $200 million. Silk Road transactions were all paid for in Bitcoin. Ulbricht personally owned $18 million in Bitcoin at the time of his arrest.

Authorities arrested the creator, Ross Ulbricht, in 2013, and he was sentenced to life in prison in May 2015 by a New York district court.

Copycats like Silk Road 2 have popped up since Silk Road was taken down, but often do not survive.

BLACK DEATH: Human Trafficking Marketplace on the Darknet

Human trafficking is just one of the illicit activities commonly found on Darknet marketplaces. Black Death is a marketplace that deals in human trafficking along with drugs, fake IDs, and a variety of other illegal products and services.

The pictures on the right claim to show a young American woman presented on Black Death for a starting bid of $150,000. When one researcher posed as an interested buyer, Black Death administrators were immediately suspicious saying, "We don't want popularity. No Europol. No people just looking around. No journalists or bloggers." Black Death told the researcher that a deposit in Bitcoin was required as a guarantee to engage in the bidding process.

> ***"We don't want popularity. No Europol. No people just looking around. No journalists or bloggers."***

In this case, the Black Death human trafficking auction shown to the right was deemed a scam due to the dramatic, polished quality of the photographs and excessively detailed descriptions of the girls, as well as their abduction and holding locations.

The Darknet is a lawless place and outside the buyer and seller ratings on some sites, there are no authorities, controls, or governing agencies. This is especially true for countries with lax Internet laws and minimal Internet forensics resources and expertise. The Darknet black markets can have a material impact on many lives. As Ulbricht demonstrated, when things go wrong it could lead to murder.

Photo Credit: Screenshot of Black Death site, Joseph Cox

THE LAWLESSNESS OF THE DARKNET

Darknet marketplaces are volatile, frequently changing addresses, names and administrators. Site administrators are the only form of authority on the Darknet. They often seek to build trust among customers by adding integrity to their brand and transactions through escrow accounts and buyer and seller ratings.

However, when sites grow in popularity and the escrow accounts grow to large sums the site administrators may be tempted to abscond with the funds leaving customers' wallets empty. This phenomenon is referred to as an exit scam.

Evolution, a Darknet marketplace notorious for selling illegal drugs and other illicit products, is believed to have scammed its customers out of immeasurable sums. The Darknet site developed prominence following the fall of Ross Ulbricht's Silk Road marketplace by promoting a centralized escrow system and claiming less fraudulent postings.

Evolution's administrators suddenly shut down the site in March 2015 allegedly taking large sums in customer escrow vaults.

Cryptocurrency

All goods and services on the Darknet are traded using Cryptocurrency rather than traditional forms of currency.

Cryptocurrencies are anonymous and adaptable digital currency. They were introduced by computer experts looking to explore alternatives to traditional nation-based currency systems. Bitcoin was the first Cryptocurrency introduced to the market, and since then dozens of other Cryptocurrencies—sometimes called "Altcoins"—have entered the field. Cryptocurrencies are stored in digital wallets without identifying signatures and used for Darknet transactions, as well as some traditional transactions. Cryptocurrencies are celebrated by libertarians and privacy advocates as alternatives to traceable currency controlled by central governments.

Cryptocurrency's anonymity allows individuals to use Bitcoin and "Altcoins" to buy illegal substances and services, send money anonymously, or simply bypass taxes and regulation. Terrorist groups have begun using Bitcoin as part of terrorist financing; an ISIS member under the pseudonym Amreeki Witness published an article entitled *Bitcoin wa Sadaqat al-Jihad: Bitcoin and the Charity of Violent Physical Struggle.*

However, critics point to the extreme volatility of the currencies as proof that they are not reliable forms of payment. Unlike traditional currency, which is regulated by a central bank and a national government, Cryptocurrencies are traded peer-to-peer with no centralized control. As a result, the value of Cryptocurrencies has changed wildly, and many fail.

There are dozens of Cryptocurrencies in the world, many of which only survive for a few months. Three of the most popular include:

Bitcoin (฿) – Bitcoin is the first and best-known Cryptocurrency created in 2009 by a mysterious person going by the pseudonym Satoshi Nakamoto. Bitcoins are acquired by mining complex computations, and there is a 21 million limit to the number of Bitcoins that can ever be mined. Bitcoins aren't printed, like dollars or euros–they're produced by people, and increasingly businesses, running computers all around the world. Bitcoin has a market capitalization of $5 trillion and at its height was worth over $1,000 per Bitcoin. Bitcoin mining programs compute an encryption function called a "hash" on a set of random numbers. Coins are awarded every 10 minutes to whichever miner happens to compute a number below a certain threshold.

Litecoin (Ł) – Litecoin has a market capitalization of approximately $127 million and was introduced in 2011 by Charles Lee, former Google employee and MIT grad. Litecoin aims to process a block every 2.5 minutes, rather than every 10 minutes like Bitcoin. The Litecoin network will produce 84 million Litecoins, or four times as many currency units as the Bitcoin network will issue.

Dogecoin (Ð) – Dogecoin began as a joke in 2013 by Australian Jackson Palmer, capitalizing on the popular "Doge" meme of a Shiba Inu dog with poor spelling and funny phrases. Billy Markus, a Portland-based software engineer, helped Palmer create and introduce the currency to market. Dogecoin reached a peak capitalization of $60 million in January 2014, before beginning a decline to approximately $21 million at the time of writing. Dogecoin has a fast production cycle, with 100 billion Dogecoins in production by 2015 and over 5 billion every year afterwards. The currency has gained traction to tip Internet users for valuable content, rather than the traditional commercial uses of Bitcoin.

EXCHANGES

Cryptocurrencies are almost exclusively used in all transactions on the Darknet. Bitcoins, Litecoins and Dogecoins are just three Cryptocurrencies of many which grease the wheels of Darknet commerce.

Cryptocurrencies are not only an alternative monetary note, they also serve as a mechanism for the transfer of funds. These qualities differentiate Cryptocurrencies from other notes as Bitcoin and other "Altcoins," alternative Cryptocurrencies to Bitcoin, fulfill the role of funds as well as fund-transfer mechanism in a single platform. A buyer can convert a traditional currency into Cryptocurrency, then transfer the funds to the seller who may convert it to their currency of choice in a matter of minutes.

For example, a buyer may use US dollars to purchase a Denial-of-Service (DoS) attack from a commercial DoS provider in China (Yuan), he or she can use a Cryptocurrency, such as Bitcoin, as a mechanism to complete the transaction between the two different currencies with the added value of anonymity. The Cryptocurrency serves as both the denomination and the mechanism that facilitates the transaction.

Cryptocurrency exchanges are easily accessible online, located on both the "surface Internet" and Darknet. Popular exchanges include MT Gox, BTC-E, BitStamp and Coinbase. Bitcoin is the most popular Cryptocurrency on the Darknet and is used by a majority of marketplaces, gambling sites, and other platforms. Litecoin, often called the silver to Bitcoin's gold, is the second most popular Cryptocurrency that is increasingly used across a variety of platforms for its faster transaction time and low transaction fees. Although Dogecoin is less frequently used than the other two major Cryptocurrencies, the currency has remained relatively stable in value and market capitalization.

One of the primary factors that drives the use of alternative Cryptocurrencies to Bitcoins is the ease with which Cryptocurrencies such as Litecoin or Dogecoin can be mined comparatively. Cryptocurrency miners serve to validate transactions in a manner comparable to traditional banks for wire transfers and credit card companies for card based transactions. The Cryptocurrency algorithms provide the miners the means to earn coins.

Miners initially used off-the-shelf high-performance graphics cards to mine coins. However, as more coins are mined the process became increasingly mathematically intensive, forcing miners to transition to purpose-built hardware.

The mining process for coins became a balancing act between the cost of buying and operating the mining hardware, the increasing mathematical complexity of the Cryptocurrency mining calculations, and the ever-growing competition from other miners. Mining has become so competitive that miners banded together to form mining pools to deal with the mathematical complexities of mining and competition. It is not uncommon for one pool to conduct Denial-of-Service attacks on other pools to prevent access to Cryptocurrency transactions that require mining.

During Bitcoin's early days, a man who mined coins using spare capacity on his home computer once offered 100 Bitcoins for anyone who would deliver two pizzas to his home. A few years later, 100 Bitcoins were worth well over $100,000 and mining 100 Bitcoins was no longer possible without significant investment in purpose-built hardware.

Government Responses to the Darknet

Governments around the world have tried to find ways to suppress the Dark Web and the illicit activities that take place on its platform. Many law enforcement agencies, especially the FBI and Europol, have launched raids to shut down Darknet websites, marketplaces, and hosts.

In November 2014, U.S. and European authorities seized more than 400 secret website addresses and arrested sixteen people in a sweep across eighteen countries targeting black markets for drugs and other illegal services. This major operation is just one of many raids targeting Darknet websites and site administrators. Other raids have targeted distributers of child pornography, insider trading schemes and other illegal activities.

The United States government has a complex relationship with the Darknet. As previously mentioned, the U.S. Naval Research Laboratory originally created and released ToR browser. The U.S. government continues to research ways to anonymously browse the Internet and release new technology. The United States also releases new technology to foreign populations to promote dissidence against authoritarian regimes. At the same time, intelligence agencies monitor activity and attempt to trace ToR users for their own strategic purposes.

NSA documents released by Edward Snowden show the National Security Agency (NSA) and other government authorities have had difficulty tracing ToR users. The Darknet then serves as a dual purpose for governments as both the enablers and disablers of Darknet sites. Regardless of government views on Darknet activities, authorities do not have the means to completely shut down the underlying technologies that keep the Darknet thriving and alive.

The Darknet's Effect on Cybersecurity

Hackers use the Darknet to trade and sell exploits, zero-day vulnerabilities, and stolen information. In particular, many markets on the Darknet function as a meeting place for those desiring to target websites or organizations—including nation-states—to find a wide variety of hackers, each with their own expertise, who can work together to infiltrate even the most sophisticated networks.

For example, TheRealDeal Market functions as a site to buy and sell code as well as access to hackers. A message from the site says, "Welcome…We originally opened this market in order to be a 'code market'—where rare information and code can be obtained. Completely avoid the scam/scum and enjoy real code, real information and real products." Services and products for sale include a new method of hacking Apple iCloud accounts; a technique to hack WordPress' multisite configuration; and an Internet Explorer attack that claims to work on Windows XP, Windows Vista and Windows 7. Many marketplaces allow Bitcoin payments to be held temporarily until the exploit can be proven legitimate.

Hacking Team, a provider of surveillance and intrusion software based in Italy, serves as an example of a company covertly buying an exploit from a Russian hacker, Vitaliy Toropov. A major cyberattack against Hacking Team's servers in July 2015 resulted in an extensive data leak of sensitive company information, including internal emails. The emails reveal the interaction and transaction between Hacking Team and Toropov. Toropov successfully propositioned selling a zero-day Adobe Flash exploit to the company. Hacking Team bought the exploit from Toropov for $45,000. Further emails show Hacking Team employees' intentions to sell the zero-day exploit to government clients.

Government and intelligence agencies are often the highest bidders for valuable zero-day vulnerabilities and exploits. Most nation-state buyers are Western countries that are willing to pay hundreds of thousands or millions of dollars for significant exploits. The United States government is widely believed to have bought multiple zero-day vulnerabilities in order to launch Stuxnet, a virus that temporarily disabled Iran's nuclear program by inserting flaws into nuclear centrifuges.

Conclusion

The Darknet provides a marketplace for a wide variety of illegal substances, services, and communications. But it is more than just a black market—the Darknet also houses the most controversial political debates and sharing of information between dissidents, journalists, whistleblowers, extremists and trolls. Just like the black markets that have existed for centuries, the Darknet is dynamic and grows organically. It is near impossible for law enforcement or governments to contain or control it with the tools available today; in fact, nation-states even play a role in helping it thrive.

However, governments and a range of other actors will continue to engage in Darknet marketplaces, to pursue information, obtain data, and even act on exploits, malware and other cyber-related tools. The weaponization of cybersecurity is gaining substantial momentum as actors realize the profitability of vulnerabilities associated with a range of industries. In fact, the Darknet is the underground platform for a cyber arms race as well as mechanism for various actors to communicate and coordinate schemes.

The Darknet is also a platform for new and innovative ways to commit crime. Empowered by the Darknet's global reach and emboldened by the anonymity it offers, gamification and crowdfunding of crimes like murder and human trafficking represent an increasingly grim aspect of the Darknet.

With every site that is taken down, multiple sites appear in its place. When Silk Road was taken down, multiple similar marketplaces appeared in the blink of an eye, vying to take its place. And the rule of thumb on the Darknet is caveat emptor and venditor (let the buyer and seller beware)—every person for themselves.

The Darknet is a volatile ecosystem where sites appear, transform, expand and disappear at an unprecedented pace. It is also a dichotomous space serving as both a lawless platform for deviance, corruption, exploitation and crime for the unsavory; as well as an empowering equalizer that gives voice to the oppressed and disenfranchised. Regardless of the faction or motive, the underlying drivers and actors of the Darknet will continue to shape the world we live in for the foreseeable future. The Darknet is the first-ever virtual global underground for the underground.

About Bat Blue

Bat Blue is the innovator of Unified Cloud Security, the first ever to deliver consistent security across all organizational assets including: Cloud & SaaS, Mobile & IoT, as well as Brick & Mortar. Bat Blue is the only market solution that helps executives answer the questions:

"Where is my Data?"

"How do I find it?"

"How do I secure it?"

Bat Blue delivers a complete security infrastructure as a cloud utility, eliminating the need for all security products and software. Furthermore, Bat Blue's platform addresses the "Cloud Penalty" — cloud service performance penalties — to offer performance improvements over traditional on-site products and ISPs or cloud security services.

Traditional approaches to securing distributed assets are unsustainable, requiring the buildout of multiple security silos each with many products spanning a variety of technologies. These include on-site products, end-point software, and secure web gateways that have web-only limitations, along with mobile device management (MDM). This one-off approach is expensive, resource intensive, and ultimately cannot offer visibility, mitigate risks or meet industry compliance standards.

Bat Blue has developed Cloud/Sec, a technology that delivers the entire security stack as an in-the-cloud service. Where other Cloud Security technologies are proxy-based and are limited to the web, Cloud/Sec is a complete security infrastructure delivering controls, threat management, and content protection across every port, protocol and application. Furthermore, Cloud/Sec does not depend on on-site hardware and software, nor does it require implementation.

Cloud/Sec runs on Blue/Net, an advanced global network that utilizes Bat Blue's proprietary "Internet Wormholing" technology offering between 30%–400% performance advantage over traditional ISPs.

Bat Blue delivers a robust security-as-a-service that is simple, agile, comprehensive and faster, making it the most strategic way for an organization to implement security.

www.batblue.com

info@batblue.com

@BatBlue

Bat Blue

Bat Blue

Gillian Ibach, *Lead Cyber Intelligence Analyst*, Bat Blue Networks
Babak Pasdar, *an Ethical Hacker and CEO*, Bat Blue Networks

Bat Blue Networks is the innovator and provider of next generation unified security services in-the-cloud

For more information please contact Jim Engineer at jim.engineer@e-rainmaker.com