UNODC
United Nations Office on Drugs and Crime

Darknet Cybercrime Threats to Southeast Asia

2020

CYBERCRIME

Disclaimer

This report has not been formally edited.

The contents of this publication do not necessarily reflect the views or policies of UNODC, Member States, or contributory organizations, and neither do they imply any endorsement.

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of UNODC or the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Foreword

The United Nations Office on Drugs and Crime (UNODC) is proud to present this introductory analysis of darknet-enabled threats against Southeast Asian countries, which has been made possible through strong partnerships with global and regional law enforcement and justice authorities, together with private industry and academia. The report was produced thanks to kind voluntary funding from the Government of Japan.

This report assesses the Darkweb from user, criminal and law enforcement perspectives with a particular focus on cybercriminality targeted at Southeast Asian countries. Darknets (i.e. networks on the Darkweb) provide the ideal environment for a wide range of criminal activities. Just as new threats appear on the Clearnet (i.e. the regular Internet), darknets can facilitate similar attacks that provide perpetrators with a greater degree of anonymity. This anonymity makes investigation and prevention more challenging, but still possible.

There has been a consistent increase in darknet and Darkweb usage, both for legitimate and illegitimate reasons, whilst the COVID-19 pandemic also appears to have given rise to darknet cybercrime, including by criminals with no previous cyber experience. Despite this, there is an overall paucity of darknet criminality data specific to Southeast Asia. There is little prioritisation of darknet criminality in the region, either in policy or practice. This creates risk from the criminality itself, which is compounded by the limited political, policy and law enforcement response. There is an absolute need for a ministerial lead on cyber affairs, in each country, to ensure that law enforcers receive necessary political support to undertake the most challenging operations.

Many criminal activities conducted over darknets are predictable and preventable. UNODC and its partners work hard to address these challenges by supporting and encouraging policy development, research, training and capacity building support in Southeast Asia.

Awareness is fundamental for addressing cybercrime. Given, however, the challenges posed by darknets, stakeholders must increase their commitment and cooperation to developing policy, sharing intelligence and enhancing international cooperation to counter darknet crime nationally, regionally and internationally.

This UNODC analysis will inform policymakers in Southeast Asia, including through the annual Senior Officials Meeting on Transnational Crime (SOMTC), as well as supporting law enforcement and judicial cooperation, and providing opportunities for darknet-focused crime prevention.

Jeremy Douglas
Regional Representative,
Southeast Asia and the Pacific

Neil J. Walsh
Chief, Cybercrime and Anti-Money
Laundering Section

Contents

Acknowledgements

UNODC thanks the Governments of Southeast Asia – Brunei Darussalam, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam for their support throughout the development of this report. Preparation of this report would not have been possible without their assistance.

UNODC gratefully acknowledges the financial contribution of the Government of Japan which enabled this research.

This study was conducted by the UNODC Global Program on Cybercrime through its regional component based in the Regional Office for Southeast Asia and the Pacific (ROSEAP).

Supervision

Jeremy Douglas, Regional Representative, Southeast Asia and the Pacific.
Neil J. Walsh, Chief, Cybercrime and Anti-Money Laundering Section.

Core team

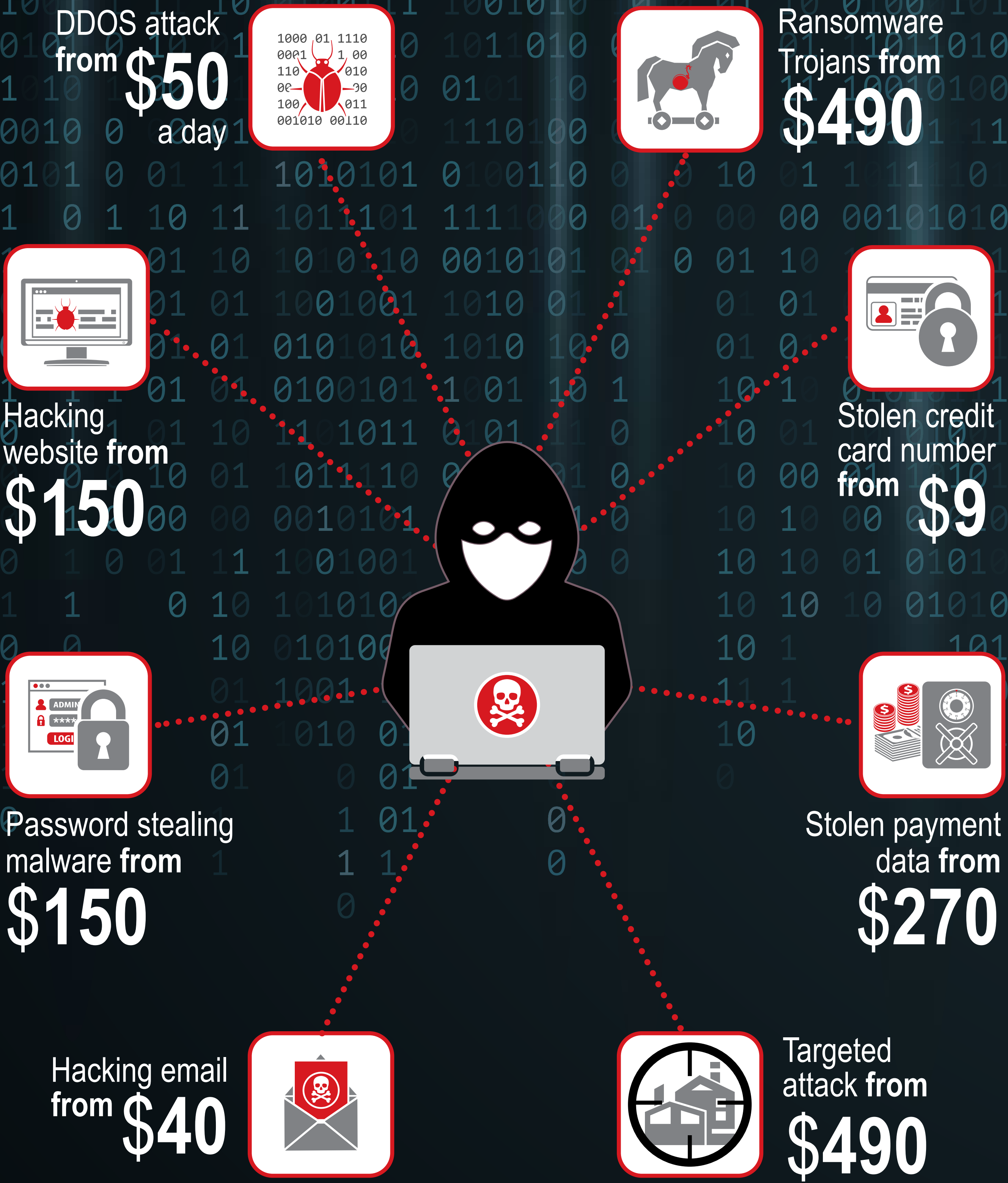
Alexandru Caciuloiu (coordination, analysis, review and drafting)
Pawinee (Ann) Parnitudom (data collection)
Mikko Niemelae, Joshua James (analysis and drafting)
Juha Nurmi, (research and data)
Praphaphorn Tamarpirat (administrative and logistical support)

This report also benefited from the valuable input of many UNODC staff members and external experts and organizations who reviewed or contributed to various sections of the report, including, Live Brenna, Kamola Ibragimova and Himal Ojha.

Abbreviations

APT	Advanced Persistent Threat
ASEAN	Association of Southeast Asian Nations
ATM	Automated Teller Machine
CaaS	Crime/Cybercrime-as-a-Service
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CSE	Child Sexual Exploitation
CSEM	Child Sexual Exploitation Material
DoS	Denial of Service
DDoS	Distributed Denial of Service
FATF	Financial Action Task Force
IP	Internet Protocol
IRC	Internet Relay Chat
MaaS	Malware-as-a-Service
NCMEC	National Center for Missing & Exploited Children
OCSE	Online Child Sexual Exploitation
PGP	Pretty Good Privacy
PoS	Point of Sale
RaaS	Ransomware-as-a-Service
SOMTC	Senior Officials Meeting on Transnational Crime
Tor	The Onion Router
UNODC	United Nations Office on Drugs and Crime
12P	Invisible Internet Project

The Price of Crime on the Darkweb



DDOS attack from $50 a day

Ransomware Trojans from $490

Hacking website from $150

Stolen credit card number from $9

Password stealing malware from $150

Stolen payment data from $270

Hacking email from $40

Targeted attack from $490

Source: Positive Technologies https://www.ptsecurity.com/ww-en/analytics/darkweb-2018/

Executive summary

People from all Southeast Asian countries use darknets, the most popular being The Onion Router, more commonly referred to as Tor. Although it is possible to provide a rough estimate of the number of darknet users in a country, it is not feasible to precisely identify their reasons for using darknets. Salient motivating factors appear to be the protection of privacy and circumventing online censorship in addition to those who commit cybercrimes. Cybercriminal use of darknets and the Darkweb (i.e. all the hosted content on darknets) varies. For some it is a springboard to launch cyberattacks, for others it is a place to access illicit products and services, whilst for others it is a place that provides legitimate privacy and anonymity from corporations who are tracking and using their personal data.

There is little evidence that countering darknet-enabled cybercrime is a policy or operational priority in the region. Consequently, there is an overall lack of consistent, quantitative, and qualitative data upon which analyses can be drawn. This leads to a self-perpetuating cycle of policy gaps which limit law enforcement threat-recognition, prioritization and resource mobilization. Of greater concern, this creates opportunities for criminal exploitation with little recourse for victims.

The Tor network is the largest darknet and contains most sites. In mid-2020, there were approximately 200,000 onion services worldwide (servers inside the Tor darknet). Just like servers on the Clearnet, some of these servers host websites, whilst others host file-sharing or email services. Some of these are used for criminal purposes. At the same time, cryptocurrencies and anonymous communication applications have boosted the use of both darknets and the Darkweb in general, whilst contributing to the trade of illicit products and services.

Data breaches affecting the private information of individuals, businesses and organizations have grown significantly over the past two years. The data is often sold or leaked on Darkweb sites, which drives a wide range of cyberattacks and cybercrime. It is this leaked data that often leads to attacks such as specific victim targeting, phishing, fake invoicing, credit card theft, impersonation and selling confidential documents.

The number of marketplaces in the Tor network has increased from one in 2011 to 118 in 2019. There has also been a large increase in the number and variety of products for sale. For example, the number of unique products available on the popular Darkweb marketplace, Valhalla, increased from 5,000 in 2015 to 13,000 in 2018.

Products available include drugs (including cocaine, heroin, and opioids), firearms and ammunition, hacking tools and services, and a wide variety of other products. Some marketplaces also specialize in the trade of payment card information and counterfeit documents.

The *UNODC World Drug Report 2019*[1] estimates that people who purchased drugs over the Darkweb doubled from 4.7 per cent in January 2014 to 10.7 per cent in January 2019. The purchase of drugs over the Darkweb is still a recent phenomenon with nearly half of those who reported buying drugs over the Darkweb in 2019 stating they had only started using this method of buying in the last two years. Overall, however, the impact of the Darkweb on the world drug problem is currently low.

User interfaces are becoming increasingly vendor-friendly, allowing, for instance, bulk ordering and combining orders of different products into one shipment. Vendors are also more aware of potential takedowns of marketplaces by authorities, which they counter by operating in multiple markets simultaneously.

From 2015 to 2019, the amount of child sexual exploitation material (CSEM) on Tor increased from 170 unique CSEM websites to 776 websites.[2]

New abuse material is posted constantly, whilst, at the same time, previously published content is routinely reposted. This makes it challenging to provide reliable figures regarding the precise scale of the threat and makes it exceptionally difficult for law enforcement to find and triage priority threats. The risks posed to children and law enforcement operational tradecraft from the Darkweb is high. Abusers constantly discuss how to compromise law enforcement investigations, how to minimise their risk of detection and how to gain access to new child victims to exploit and abuse.

The Darkweb attracts CSEM websites because it offers anonymity, as well as being resilient to online censorship. It is challenging to take down this kind of illicit content as many CSEM sites replicate their content elsewhere.

In November 2019, the number of CSEM sites probably represented 5 per cent of all Darkweb websites[3] but the COVID-19 lockdown is likely to have increased the scale of such sites. Furthermore, the amount of abuse material (mostly images and videos) available today, represents a significant amount of the overall data shared on the Darkweb, with some sites claiming they have amassed several terabytes of abuse material (the equivalent of 80 days' worth of video or almost 1 million digital photos).

Overall, the volume of content on darknets and the amount of people using them (especially Tor) is growing continuously. Although not all activities on darknets are illicit, there is no doubt that organized criminals working within the Darkweb are constantly developing their capabilities, security mechanisms and business practices.

Governments in Southeast Asia need to start investing the resources necessary to analyse and counter Tor-enabled cybercrime while improving operational capabilities across different darknets. At the same time, the response should be carefully calibrated to ensure the protection of human rights and legitimate privacy rights.

As darknets strengthen their levels of security, gaining access and having a meaningful impact has become more complicated and costly, making it increasingly difficult to achieve progress at a national level. Instead, working together internationally and using highly trained experts equipped with the latest skills and technology, has proven to be a more effective solution.

Southeast Asia and the Darkweb

Due to the nature of darknets and the Darkweb, it is not easy to associate any particular criminal action with users in Southeast Asia – the location of criminals often only becomes clear just prior to the point of arrest. There is, however, consistent evidence of Southeast Asian victims on the Darkweb. It is vital that Southeast Asian countries scale-up their policy, law enforcement and judicial capabilities to counter darknet criminality.

Key findings

THERE IS A PAUCITY OF RELIABLE DATA REGARDING DARKNET-ENABLED CRIME IN SOUTHEAST ASIA

There is little evidence that countering darknet-enabled cybercrime is a policy or operational priority in the region. Consequently, there is an overall lack of consistent, quantitative and qualitative data upon which analyses can be drawn. This leads to a self-perpetuating cycle of policy gaps which limit law enforcement threat-recognition, prioritization and resource mobilization. Of greater concern, this creates opportunities for criminal exploitation with little recourse for victims.

DARKNET CYBERCRIME IS BELIEVED TO BE INCREASING IN SOUTHEAST ASIA

An increasing number of criminals in Southeast Asia are likely to be using the Tor darknet to engage in the full range of illicit activities available on the Darkweb. This includes the buying and selling of drugs, cybercrime toolkits, fake passports, fake currency, online child sexual exploitation material, stolen credit card details and personally identifiable information from breaches.

SOUTHEAST ASIAN LANGUAGES AND DIALECTS ON THE DARKWEB VARY OVER TIME

English is the primary working language for cybercrime on the Darkweb, although locally originated content in Southeast Asian languages is becoming a variable. There is, therefore, a customer base. And while this suggests a diversified cybercrime threat, it also creates the opportunity for proportionate, legal, accountable and necessary law enforcement infiltration and prevention activities that will require clear and robust legislative and human rights oversight frameworks.

CRYPTOCURRENCIES ARE THE PAYMENT METHOD OF CHOICE

Cryptocurrencies are the leading payment method on darknets. Cryptocurrencies and related laundering services are evolving as criminals seek to move towards more privacy-preserving currencies. Bitcoin remains the primary tool to exchange crypto to fiat (currency issued by a country). This presents policy, legislative and investigative opportunities. States are encouraged to engage with UNODC, the Financial Action Task Force (FATF) and industry to counter the threat posed by virtual-asset-based illicit financial flows and money laundering.

MOST LAW ENFORCEMENT DARKWEB OPERATIONS ORIGINATE INTERNATIONALLY. LOCAL CAPABILITY IS LIMITED

Although there have been law enforcement operations targeting darknet cybercrime in Southeast Asia, these operations are the result of international investigations initiated outside of the region, with only a small number of cases originating within the region itself. Cybercriminals are likely to perceive Southeast Asia as a relatively low-risk/high-gain operational environment as the likelihood of detection is relatively low. Prevention campaigns can have an impact.

Recommendations

STATES SHOULD INCREASE SPECIALIST DARKNET POLICY AND OPERATIONAL CAPACITY

Each Southeast Asian country must increase specialist political, policy and operational knowledge regarding darknet networks, services, cryptocurrency investigations and intelligence gathering. This will increase national security, international cooperation and confidence building in preventive cyber-diplomacy.

A MINISTERIAL OR AMBASSADORIAL LEAD ON CYBER AFFAIRS, SUPPORTED BY SPECIALIZED LAW ENFORCEMENT CAPACITY, IS ESSENTIAL

Law enforcement darknet operations require highly trained and specialized officers. These officers must have a strong understanding of law, the Internet, human rights, privacy, communication technologies, cryptocurrencies, encryption and anonymizing techniques, including specialist investigative skills. Beyond the tactical capability, a Ministerial or Cyber Ambassadorial lead is required on all cyber affairs. This ensures cross-government policy coherence and the necessary mechanism for law enforcers to seek political oversight, challenge or support, for new methods of operating.

STATES SHOULD DISRUPT ASSOCIATED ILLICIT PARCEL DELIVERY AND TAKE A PROACTIVE MEDIA APPROACH

Darknet markets result in the sale of physical goods, such as drugs and weapons. Increasing local capacity and cross-border cooperation for detecting illicit parcels will disrupt the flow of illegal goods, as well as psychologically undermining the reputation of market sellers.

APPLY CRYPTOCURRENCY (VIRTUAL ASSET) POLICY AND REGULATIONS

The regulation of cryptocurrency users and exchanges, especially employing the FATF virtual assets risk-based approach guidelines, will significantly assist in reducing the anonymous transfer of funds.

CREATE A REGIONAL COUNTER-DARKNET CYBERCRIME STRATEGY

A plan and a regional strategy should be created for cooperation and response in conjunction with ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) and other stakeholders.

CONTINUE RESEARCH

Cultivate local capabilities within the public, private and academic sectors to encourage continued research on darknet technologies, policies and investigation techniques which are proportionate, legal, accountable and necessary within a broad Human Rights framework.

Introduction

Cybercrime is an evolving form of transnational crime. The complex nature of the crime, as one that takes place in the borderless realm of cyberspace (where perpetrators and their victims can be in different regions), is compounded by the increasing involvement of organized crime groups. The effects of cybercrime can ripple through societies around the world, highlighting the need to mount an urgent, dynamic and international response.

Increasingly, criminals have adopted the use of darknets to help anonymise their activities. When illicit content and services are hosted on the Darkweb, it makes investigations more complicated. Darknets are also used as an anonymizing bridge from which traditional cyberattacks can be launched.

There are, of course, legitimate uses for darknets. Many users see aggressive advertising and data collection practices by public and private organizations as an invasion of their privacy. In these cases, darknets are used to reduce the privacy concerns of law-abiding users. As a result, several popular web browsers now include darknet routing (usually Tor) as a privacy feature. Darknets have also become a convenient tool to protect the privacy of law enforcement during online investigations.

Much like the Internet itself, darknets are used for both good and bad. The main difference between the Clearnet and the Darkweb is that censorship and attribution is intentionally difficult in the latter.

This report seeks to understand the threat of cybercrime using darknets, and more specifically, how this is affecting Southeast Asian countries.

Aim

The purpose of this assessment is to evaluate the darknet threats that exist within the cybercrime landscape of Southeast Asian countries. The findings of this assessment create avenues for policy change, action, and recommendations. Data collection occurred in 2019 and early 2020.

Methodology

This analysis included a desk review of Southeast Asian cybersecurity strategies, plans, policies, frameworks and programs. A survey of state representatives, conducted during working group sessions on cybercrime, was also conducted.

Detailed technical analysis and criminal forum examples are included in the appendices of this report.

CLEARNET

The publicly-accessible Internet that is easily accessed with a normal Internet connection and a browser.

Examples of content: Google, Facebook, YouTube, Wikipedia, Netflix.

DEEP WEB

The publicly-accessible Internet that is unknown to search engines, such as encrypted or unindexed websites, private databases, and other unlinked content.

Examples of content: Academic databases, medical records, financial records, legal documentation, government information, library access, bank accounts.

DARKWEB

A collection of websites that exist on darknets. These are not directly accessible from the Clearnet and often require special software to access such websites. Websites use hidden IP addresses which are hosted on securely encrypted networks for increased anonymity.

Examples of content: Tor encrypted websites, whistleblowing platforms, ultra-secure email services, darknet markets.

Darknets and the Darkweb

The Darkweb is the part of the World Wide Web which cannot be accessed using standard web browsers like Internet Explorer, Firefox, Edge or Chrome. This is because websites on the Darkweb operate inside specialized encrypted networks to provide anonymity.

On the Clearnet (areas of the Internet accessible to the public without any additional software), it is possible to identify and track users. The Darkweb, on the other hand, is designed to prevent tracking. Access is possible through easily accessible, free software which connects computers over a distributed network (a darknet). By routing traffic between computers on darknets, the user's identity is hidden.

Once connected to a darknet, a device can "talk" to other devices that are also connected to the same darknet. Darknets often host "darknet-exclusive" content and it is this hosted content which makes up what is known as "the Darkweb". Like the Clearnet, the Darkweb hosts thousands of web pages – but they are only accessible when connected to a darknet.

Over the last two decades there have been several popular darknets, which operate as peer-to-peer networks:

- 2000: **Freenet:** a data storage software for file-sharing and communication.
- 2001: **GNUnet:** a software for file-sharing.
- 2002: **Tor**: a software for anonymous communication.
- 2003: **WASTE**: a software for file-sharing and instant messaging.
- 2003: **I2P:** a software for anonymous communication.
- 2004: **Onion services:** Tor implemented functionality to publish anonymous websites.
- 2006: **RetroShare:** an anonymous chat forum and file-sharing software.
- 2011: The first Darkweb market, Silk Road, appears in the **Tor** network.

The most popular networks that enable Darkweb publishing are the Tor and I2P networks.[4,5,6] Other smaller networks (such as Freenet, GNUnet and many others) have significantly less users.[7] As an indication of how many darknets there are, Wikipedia lists 22 anonymous file-sharing networks.[8] Analysis in this assessment focuses on Tor as, at the time of writing, it is currently the most popular darknet system. Other anonymous networks generate too little data for a separate analysis.

The Tor network provides anonymity for Internet users and online services. "Onion services" are Internet services, such as websites, email and file sharing, that are only available through the Tor network. The Tor network conceals the real IP address (and implicitly the location) of the server.[9,10,11]

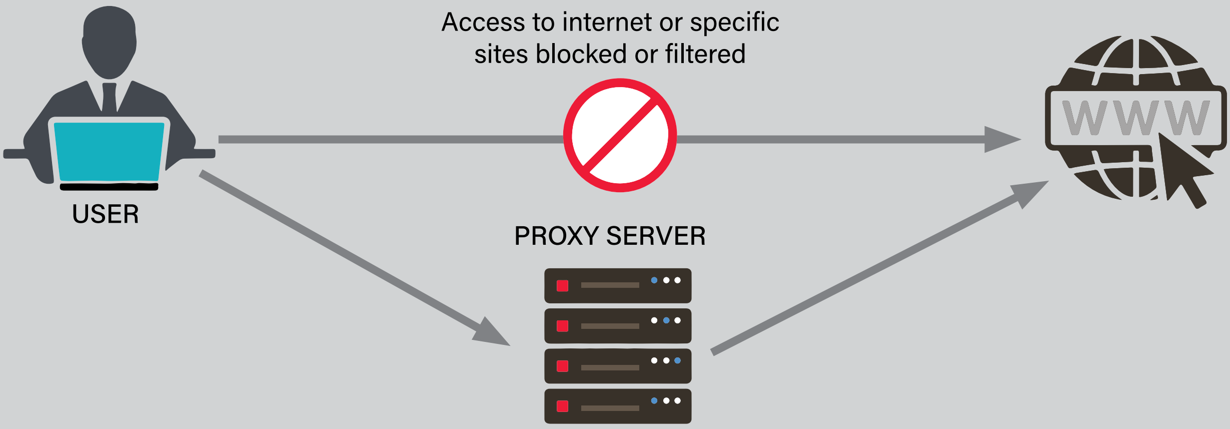
Tor started in 1996 when the design of Onion Routing was published to provide anonymity for communication systems.[12] In 2004, the final technical implementation of the routing network was ready. Syverson, Dingledine, and Mathewson published their article *Tor: The Second-Generation Onion Router,* along with the source code of The Onion Router (Tor).[13] From then on, the Tor network started to provide online anonymity to Internet applications.

Tor allows the publishing of anonymous Internet services. Onion services have onion addresses (*.onion) and these are only accessible from within the Tor network. For example, https://facebookcorewwwi.onion is a valid onion address for Facebook and can be accessed using the Tor Browser.

To enable safe, anonymous web browsing, the Tor Project developed the Tor Browser, their main privacy-aware application, which is available on the Tor Project website.[14] The Tor Browser is as easy to use as a standard web browser. It is simply a modified Mozilla Firefox Extended Support Release (ESR) browser with security best-practice default settings and extensions.

Circumventing internet censorship using a proxy server

Censorship circumvention: the practice of bypassing Internet censorship techniques to access blocked information or services.



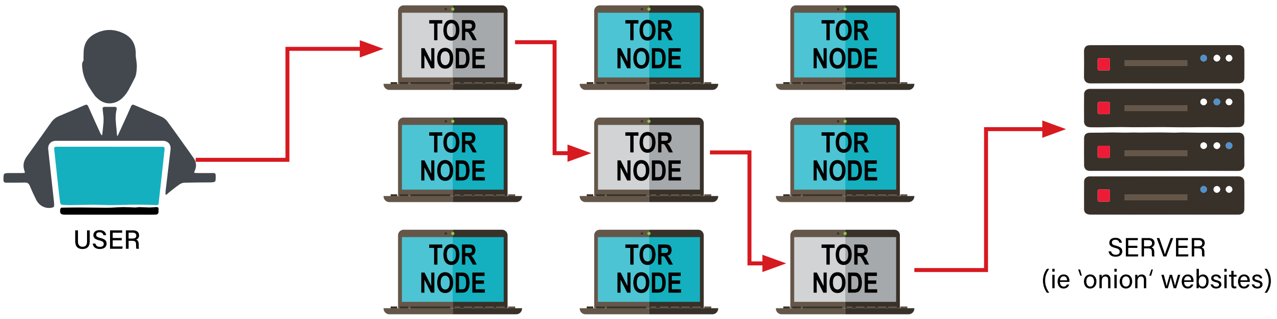
A proxy server acts as a gateway, usually masking the originating IP address

The Tor Browser routes all web traffic through the Tor network, removing most fingerprinting methods (local privacy-sensitive data, such as browsing history, cache, and cookies) in the process. Tor also enables anonymous web publishing for so-called "hidden services" which can only be accessed using the Tor Browser. With hidden IP addresses, both users and those publishing websites have improved anonymity and, to further avoid detection, many sites only stay online for short periods. This makes both proactive and reactive law enforcement operations exceptionally challenging.

The number of known onion websites on the Darkweb has grown from a couple of hundred in 2012 to over 100,000 in 2020. During the first six months of 2020, there were 110,865 onion websites available.[15] One reason for this growth has to do with some sites dividing their content over thousands of sub-websites, each under a different domain. This is a common practice with websites that are sharing video material, with some sites even providing a unique domain for each video. The reason for this is so that the content can be accessed faster by using several parallel Tor network circuits. Every onion domain has its own Tor network circuit which is usually what causes traffic bottlenecks. By having numerous sub-websites and domains, users can increase speeds by spreading out the content. It also makes lawful intercept and technical intelligence gathering exceptionally difficult, even for the most capable intelligence agencies.

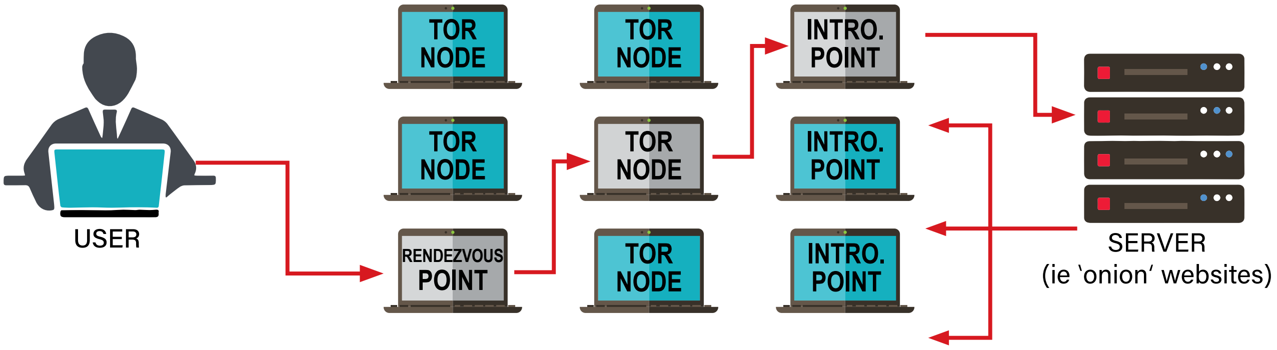
How Tor works

With the Tor browser, Internet traffic is routed through a series of different volunteer computers (called 'relays' or 'nodes') and each node is only aware of the preceding and following nodes in the network. The data is also encrypted multiple times (like the layers of an onion) and the route is randomly selected and constantly changing. This ensures that the original user's IP address and location stays hidden.



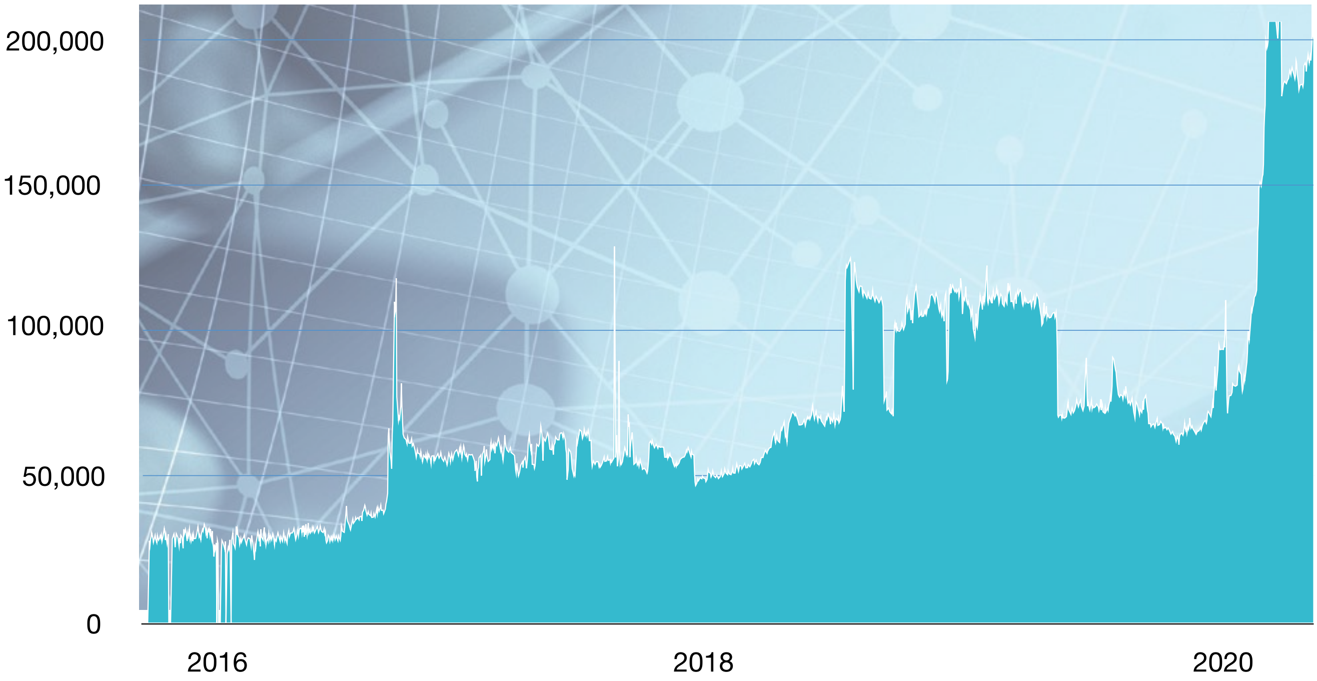
How Tor hidden services work

Tor can also provide anonymity to websites and other servers. Servers configured to receive inbound connections only through Tor are called 'hidden services.' Rather than revealing a server's IP address (and network location), a hidden service is accessed through its onion address. The Tor network can route data to and from hidden services while preserving the anonymity of both parties.



An 'Introduction Point' sends a message to the server saying that someone wants to connect. The server then creates a circuit (via other Tor nodes) to a 'Rendezvous Point'. Communication between the Introduction Point and the Rendezvous Point is end-to-end encrypted (using public and private keys) therefore protecting the anonymity of both parties.

Figure 1. The number of websites available in the Tor network.*

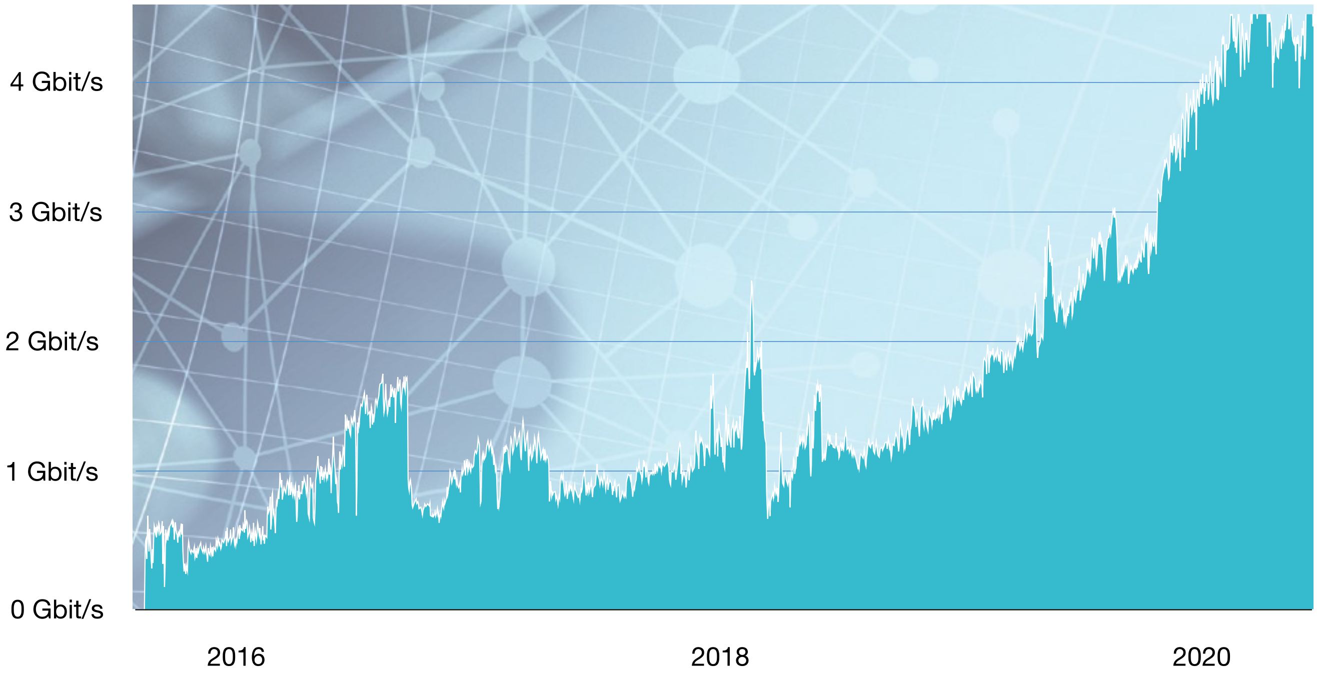


The Tor Project - https://metrics.torproject.org/

*Many sites stay online for only a short period. Measurement only calculates websites which were reachable in the given time.

Traffic to onion services has also multiplied since 2015 and continues to grow.[16] This means that more and more content is being uploaded and downloaded from onion websites.

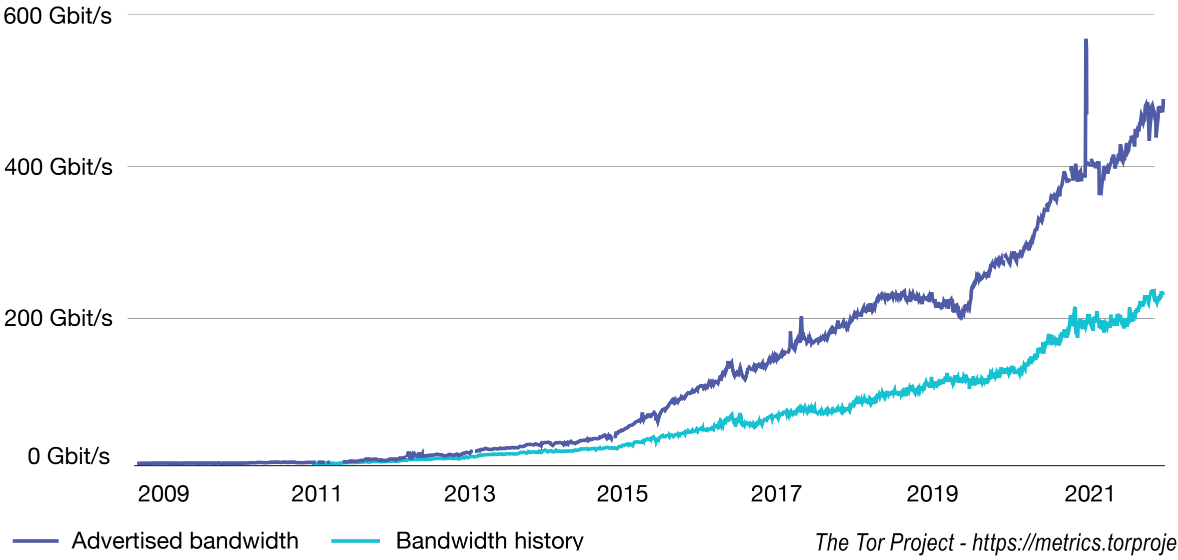
Figure 2. Traffic to onion services (Gbit/s).



The Tor Project - https://metrics.torproject.org/

Many users in the Tor network voluntarily install Tor software in "routing mode" which enables their computers to receive and pass along traffic on the Tor network. These computer servers are commonly called Tor routers, relays or nodes. In 2019, there were approximately 7,000 Tor relays around the world and 2.5 million Tor users.[17] As counter-cybercrime legislation, prosecution and international cooperation often rely upon geographic jurisdiction, it is clear that counter-darknet cybercrime operations are exceptionally challenging.

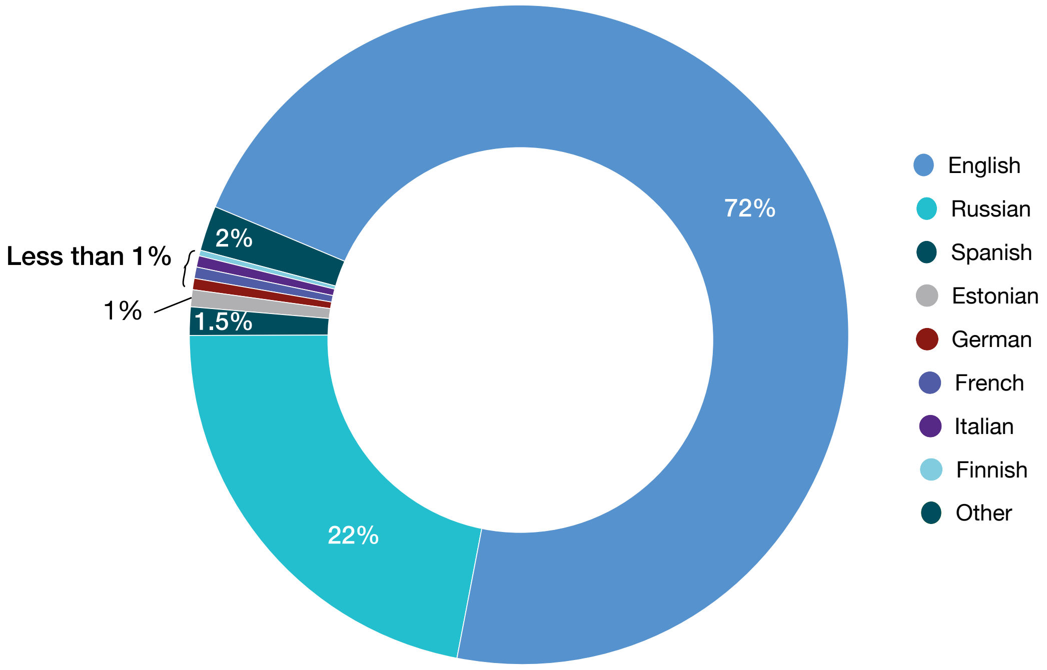
Figure 3. The total Tor network bandwidth is 400 Gbit/s.



The Tor Project - https://metrics.torproject.org/

The total bandwidth of the Tor network has increased significantly over the last decade. In 2010, there was close to zero Gbit/s traffic in the Tor network, but this had increased to 400 Gbit/s by 2019[18] (the equivalent of streaming 100 HD Netflix movies per second). This increase in bandwidth demonstrates the increased use of Tor. In *Figure 3,* the 'advertised bandwidth' is the total amount of bandwidth available in the Tor network between nodes, while 'the bandwidth history' is the amount of bandwidth actually used in the Tor network.

Figure 4. Most popular languages used on the Tor network in 2019.



Although many users of the Tor network have developed communities in their native languages, the most commonly used language is English (approximately 70 per cent). One reason given for the use of English (even when it is not the user's native language) is that it provides an added layer of anonymity. Administrators of darknet markets or other forums on the Darkweb will often warn users *not* to use other languages (and refrain from using localised slang) as a method of anti-surveillance (local dialects may assist law enforcement with pinpointing the location or origin of the users).

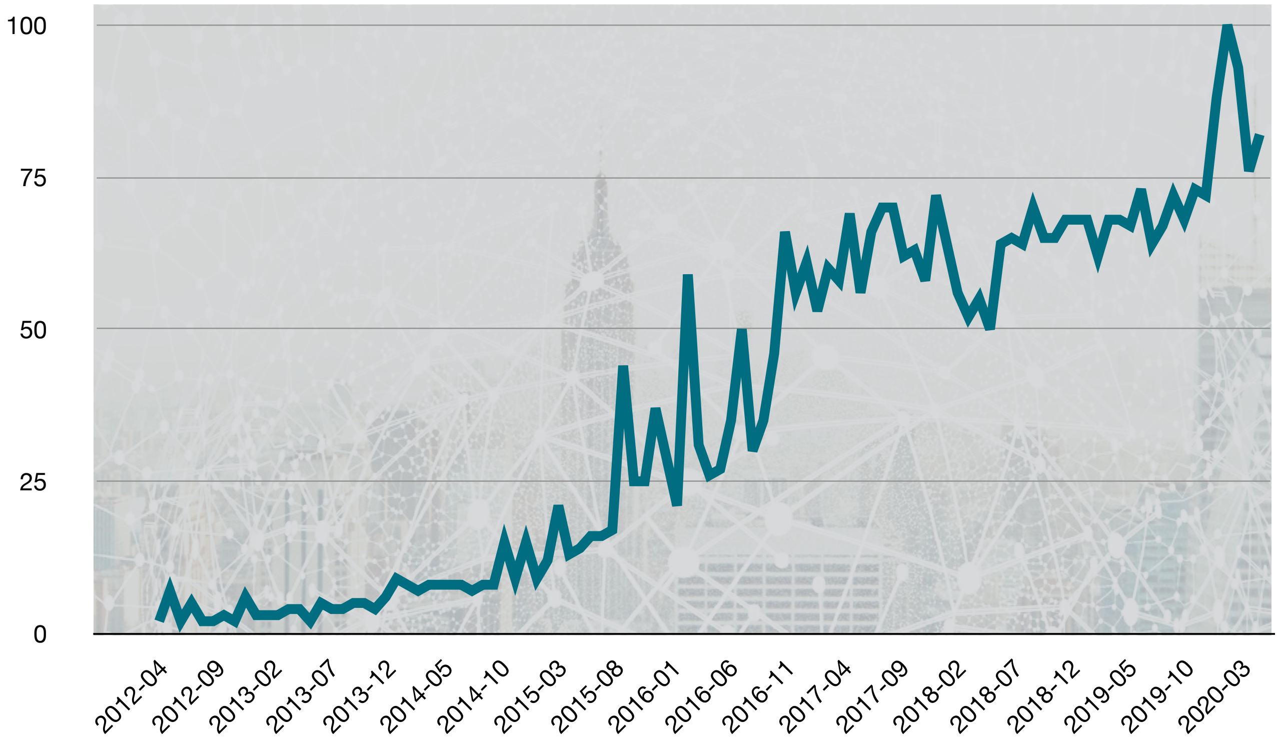
The Darkweb and cybercrime

Public interest in the Darkweb has increased over the years.[19] The anonymity ecosystem has evolved from being a communication channel for privacy actors to a global marketplace with a large variety of products and services available for purchase.[20] The Darkweb also serves as a platform for a large number of discussion forums covering a broad range of topics. These forums are sometimes structured by nationality and language, or to specific crime typologies such as credit card crime, insider trading, drug trafficking, weapons trafficking, Crime-as-a-Service (CaaS) and anti or counter-surveillance of online investigators.[21]

As criminals increasingly use the Darkweb, it has rapidly become one of the most discussed topics at law enforcement and criminal justice conferences. This unprecedented interest has prompted law enforcement to create mechanisms and processes to investigate criminality that occurs on the Darkweb. There is, however, limited, consistent engagement in Southeast Asia which, consequently, reduces international cooperation and increases cybercrime opportunities in the region.

An upsurge in the number of Google searches for the Darkweb illustrates the increased interest in the topic amongst members of the public.

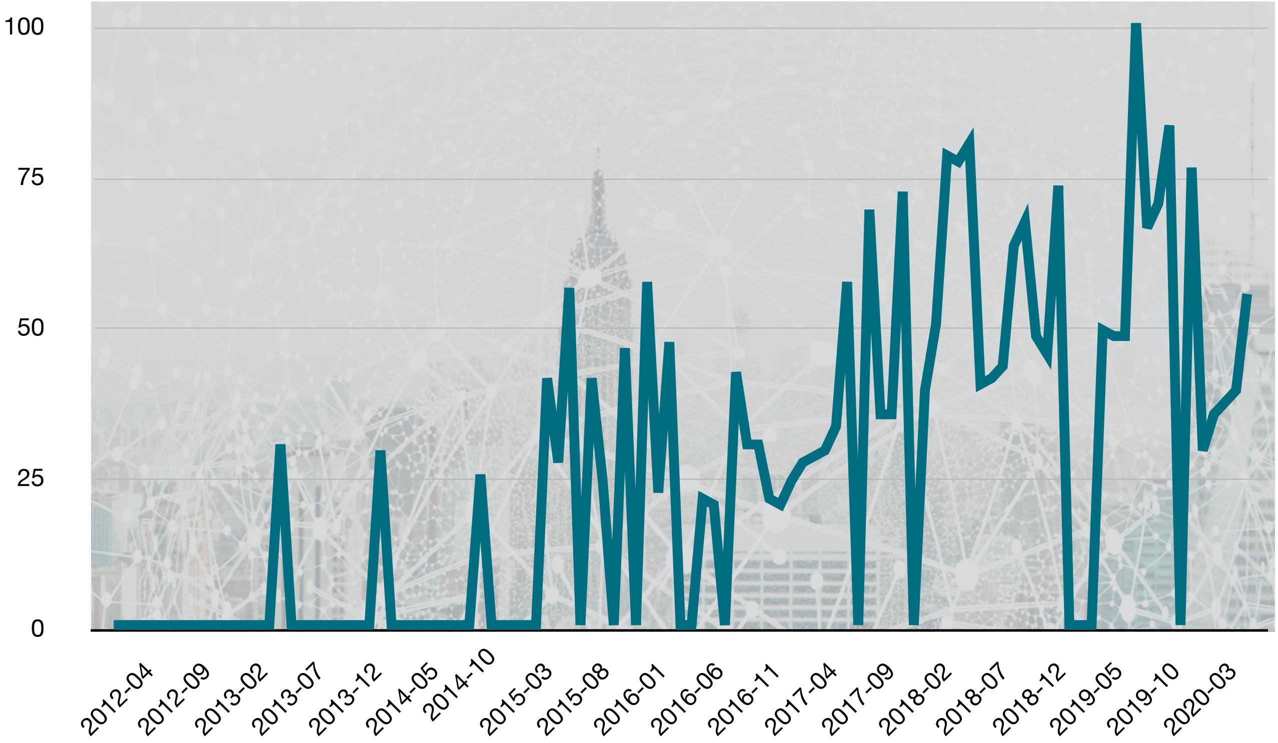
Figure 5. Number of Google searches about the Darkweb (Jan 2012 to July 2020).*



Data from Google Trends service. The numbers represent the search interest relative to the highest point on the chart for Southeast Asia over time. A value of 100 is the peak popularity of the term, whilst a value of 50 means that the term is half as popular.

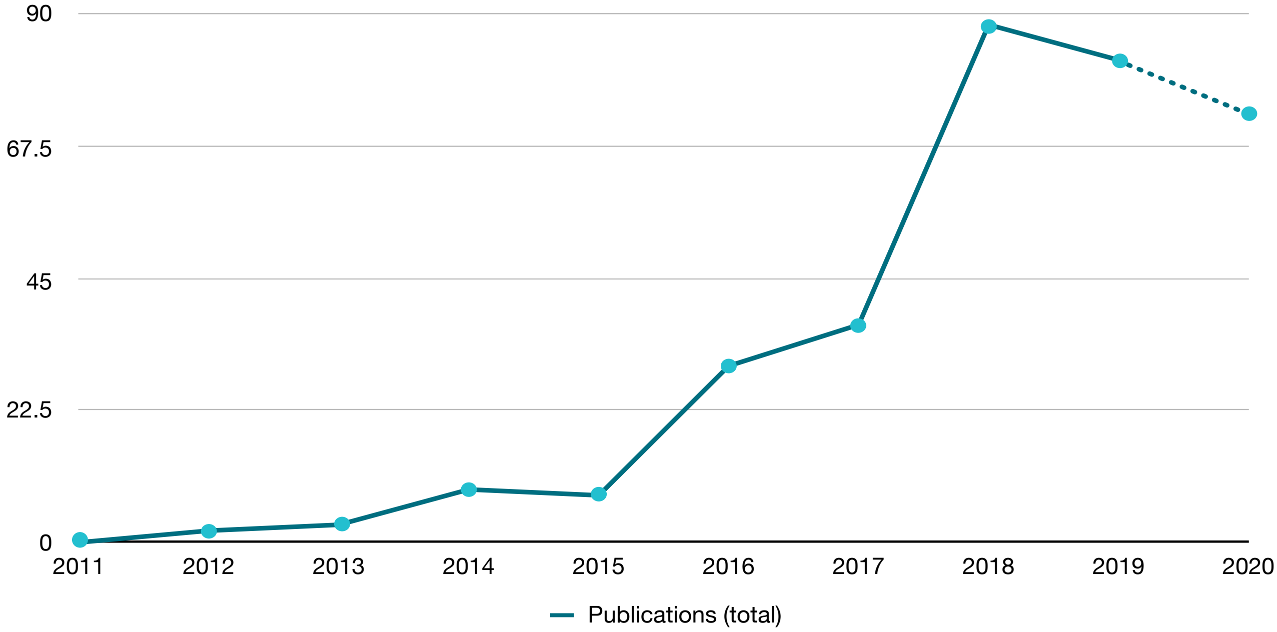
The growing trend of Darkweb-related crime has not gone unnoticed by the media. As a result, more frequent reporting in the news is seen from 2014 onwards.

Figure 6. Number of news articles in Southeast Asia mentioning the Darkweb (Jan 2014 to July 2020).



The number of published academic articles about the Darkweb has tripled since 2015 (*Figure 7*). Many scientific articles analyse the content of the Darkweb and how anonymity tools are used. Academic literature in 2019/20 included information disclosure and data breaches available on the Darkweb and is likely to address the impact of COVID-19 in 2020/21. These publications analyse data from Darkweb markets, discussion forums, and information-leaking platforms (known as "paste sites").

Figure 7. Number of published scientific articles about the Darkweb and darknets.



The popularity of darknets (especially Tor) is increasing worldwide. However, as we will see in the next section, users in Southeast Asia appear to comprise only a moderate proportion of the overall number.

Darknets in Southeast Asia

Context

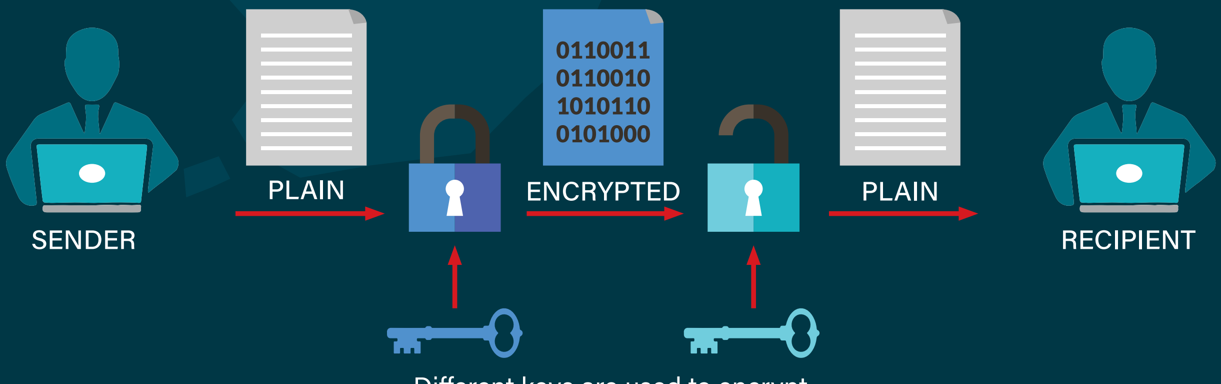
In Southeast Asia, the general public have mainly heard about the Darkweb on the news and through social media. It is assessed that only a minority have used it personally (see *A1: Darknet use in Southeast Asian countries* in Appendices). Even on the news, the Darkweb is generally not discussed in any great detail, with most stories relating to the arrest of cybercriminals who have used the Darkweb in some way.

Darkweb-related arrests in Southeast Asia have helped focus attention on how transnational organized crime groups and syndicates operate in the region. Illegal transactions are typically cross-border, emphasizing the need for international cooperation, interoperability, and a mutual understanding of the threat. To help detect, investigate, prosecute and prevent this type of cybercrime, capacity building in law enforcement is vital.

Criminals seek to remain anonymous by hiding their operations and identity using technical methods such as encryption, and non-technical means such as communicating in English instead of their native tongue. Based on their communication alone, it is challenging to identify the whereabouts of specific perpetrators as many of the largest Darkweb marketplaces offer services and products worldwide. As illustrated in *Figure 8*, the use of some Southeast Asian languages is becoming less common. There are cases when sites target more specific markets (see *Figure 9* showing a Vietnamese forum on the Tor darknet) but this appears to be rare.

Encryption

Encryption: the process of encoding information into an alternative form that can only be 'decrypted' by authorised individuals that possess the decryption key.



Different keys are used to encrypt and decrypt messages.

Figure 8. Indonesian, Thai, Tagalog and Vietnamese languages found on Darkweb sites (2016-2019).

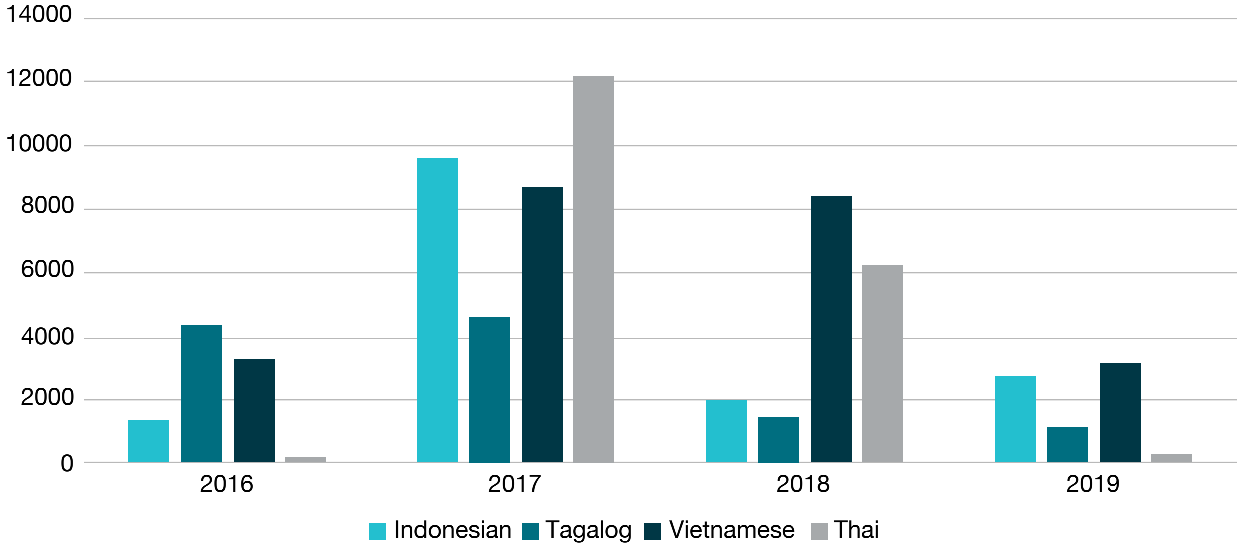
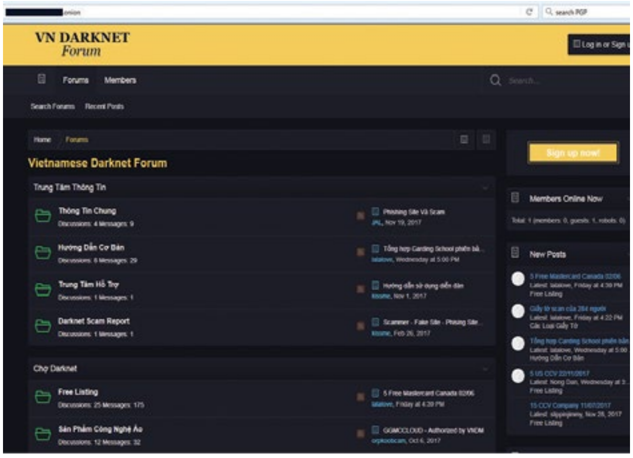


Figure 9. Vietnamese Darknet forum.


[redacted].onion

search PGP

VN DARKNET Forum

Log in or Sign up

Forums Members

Search...

Search Forums Recent Posts

Home Forums

Vietnamese Darknet Forum

Trung Tâm Thông Tin

Thông Tin Chung
Discussions: 4 Messages: 9
Phishing Site Và Scam
JPL, Nov 19, 2017

Hướng Dẫn Cơ Bản
Discussions: 6 Messages: 29
Tổng hợp Carding School phiên bả...
lalalove, Wednesday at 5:00 PM

Trung Tâm Hỗ Trợ
Discussions: 1 Messages: 1
Hướng dẫn sử dụng diễn đàn
kissme, Nov 1, 2017

Darknet Scam Report
Discussions: 1 Messages: 1
Scammer - Fake Site - Phising Site...
kissme, Feb 26, 2017

Chợ Darknet

Free Listing
Discussions: 25 Messages: 175
5 Free Mastercard Canada 02/06
lalalove, Friday at 4:20 PM

Sản Phẩm Công Nghệ Ảo
Discussions: 12 Messages: 32
GGMCCLOUD - Authorized by VNDM
orpkoobcam, Oct 6, 2017

Sign up now!

Members Online Now
Total: 1 (members: 0, guests: 1, robots: 0)

New Posts

5 Free Mastercard Canada 02/06
Latest: lalalove, Friday at 4:39 PM
Free Listing

Giấy tờ scan của 284 người
Latest: lalalove, Friday at 4:22 PM
Các Loại Giấy Tờ

Tổng hợp Carding School phiên bản
Latest: lalalove, Wednesday at 5:00 ...
Hướng Dẫn Cơ Bản

5 US CCV 22/11/2017
Latest: Nong Dan, Wednesday at 3:...
Free Listing

15 CCV Company 11/07/2017
Latest: slippinjimmy, Nov 28, 2017
Free Listing

Success: a patchwork response?

Although criminals on the Darkweb try their best to obfuscate their actions, successful law enforcement targeting has occurred. This success is due to joint efforts from multiple law enforcement agencies around the world. As investigative capabilities improve, so will successful operational outcomes. Identifying individual actors or marketplaces is made possible by analysing information from multiple sources. It is therefore vital that Southeast Asian nations continue to cooperate with their international counterparts to build actionable intelligence, plan coordinated actions, and seek to achieve strategic outcomes against the highest-risk cybercriminals.

This requires, in the first instance, a policy decision, across government, to counter Darkweb cybercrime (irrespective of the state of readiness for online operations in the country).

It is technically challenging to associate the Darkweb with specific jurisdictions and geographical boundaries. It sometimes takes the investigation and prosecution of specific cases to identify which countries the criminals are operating from. An example of this in Southeast Asia, involved the arrest of a Canadian citizen residing in Thailand who was running a marketplace called AlphaBay, which was the largest market on the Darkweb in 2017.

The international operation to seize AlphaBay's infrastructure involved cooperation by law enforcement authorities in Thailand, the United States, Netherlands, Lithuania, Canada, the United Kingdom and France, as well as the European law enforcement agency, Europol.[22] Another case highlights the nature of cross-border transactions. Cross-border transactions involve global supply chains such as one that originated in India, where criminals manufactured illegal drugs for shipping via a criminal associate in Singapore. From there, the parcels continued their journey to the US and UK.[23] Both of these cases demonstrate the absolute need for skilled, empowered criminal justice officers and a swift, intuitive international cooperation system.

Triaging the highest risk international offenders: live-streaming

Streaming technologies further complicate matters. Darkweb live-streaming allows the transmission of video, audio and other media to allow cybercriminals to reach markets far from their home-location in real-time. For example, Australian citizen Peter Gerard Scully, was running a live-streaming service from the Philippines marketed at European and US child sex abusers. Scully was arrested in the Philippines in 2015 after sexually abusing several children, including an 18-month-old infant.[24] The investigation led to the identification of an international child sexual exploitation group which reportedly raped, tortured, murdered and broadcast the abuse of their child victims on the Darkweb to customers around the world for up to US$10,000 per view.[25] UNODC has mentored similar investigations in multiple jurisdictions and acknowledges that the scale and quantity of the offences makes them exceptionally difficult to prosecute.

Similarly, in 2018, law enforcement officers arrested nine people in Thailand, Australia and the US. The operation safe-guarded 50 children after investigators took down a subscription-based CSEM Darkweb website with 63,000 worldwide users.[26]

It is clear that international cooperation is absolutely vital to saving victims, identifying offenders and preventing further harm.

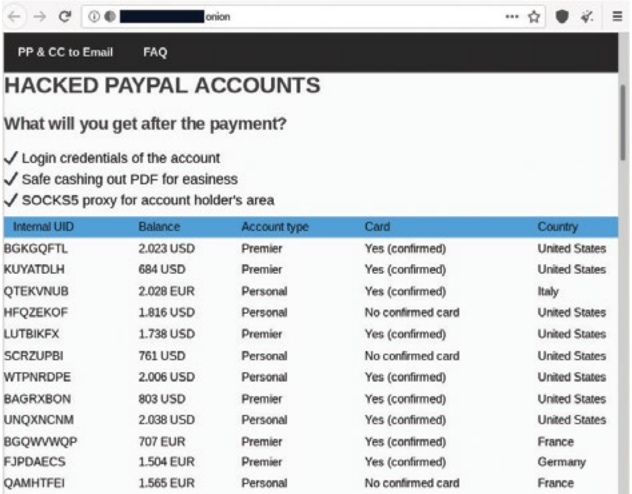
Despite strong cooperation bilaterally and multilaterally, especially through INTERPOL channels, some criminals can conceal their offences and identities for extended periods of time. From 2006 to 2014, Richard Huckle abused up to 200 Malaysian children and shared images of his crimes on the Darkweb.[27] The UK's National Crime Agency arrested Huckle after receiving intelligence from Queensland Police's Task Force Argos child protection unit. He was convicted on 71 counts of offences against children between the ages of six months and 12 years and received 22 life sentences.[28]

These offences, and offenders, reveal the clear-and-present danger from live-stream child sex offenders. This is why it is essential for all countries to have a ministerial policy lead on cyber affairs who can command the resources necessary to keep the most vulnerable in society safe.

Profit and loss

Cybercriminals, like traditional criminals, are principally motivated by profit. Cybercriminals trade both personally identifiable and financial information stolen from individuals and businesses on Darkweb forums and marketplaces. Criminals use stolen credentials (such as usernames and passwords) to access online services and then exploit the victim's personal information for fraud. As credentials are often reused unwittingly, one compromised password may lead to criminals gaining access to other more impactive services like PayPal (PayPal accounts are often for sale on the Darkweb – see *Figure 10*).

Figure 10. Stolen PayPal account credentials on the Darkweb.*



[redacted]onion

PP & CC to Email FAQ

HACKED PAYPAL ACCOUNTS

What will you get after the payment?

✓ Login credentials of the account
✓ Safe cashing out PDF for easiness
✓ SOCKS5 proxy for account holder's area

Internal UID	Balance	Account type	Card	Country
BGKGQFTL	2.023 USD	Premier	Yes (confirmed)	United States
KUYATDLH	684 USD	Premier	Yes (confirmed)	United States
QTEKVNUB	2.028 EUR	Personal	Yes (confirmed)	Italy
HFQZEKOF	1.816 USD	Personal	No confirmed card	United States
LUTBIKFX	1.738 USD	Premier	Yes (confirmed)	United States
SCRZUPBI	761 USD	Personal	No confirmed card	United States
WTPNRDPE	2.006 USD	Personal	Yes (confirmed)	United States
BAGRXBON	803 USD	Premier	Yes (confirmed)	United States
UNQXNCNM	2.038 USD	Personal	Yes (confirmed)	United States
BGQWVWQP	707 EUR	Premier	Yes (confirmed)	France
FJPDAECS	1.504 EUR	Premier	Yes (confirmed)	Germany
QAMHTFEI	1.565 EUR	Personal	No confirmed card	France

**The cybercriminals selling these stolen credentials to PayPal accounts are not stealing the funds from the account. Instead, they sell the access to other criminals, i.e. a "Cybercrime-as-a-Service".*

A Russian national was arrested in Thailand in 2018 for operating a Darkweb marketplace, the Infraud Organization, selling stolen credit card information and hardware for compromising ATMs. The market had 11,000 members who traded more than 4.3 million credit cards, debit cards and bank accounts worldwide. This resulted in the loss of more than US$530 million for legitimate users and businesses.[29] The impact of a half-billion dollar loss is clear at the best of times, but during the greatest global economic recession in 50 years, the impact from such crime on economic prosperity, on recovery and on lives is truly phenomenal.

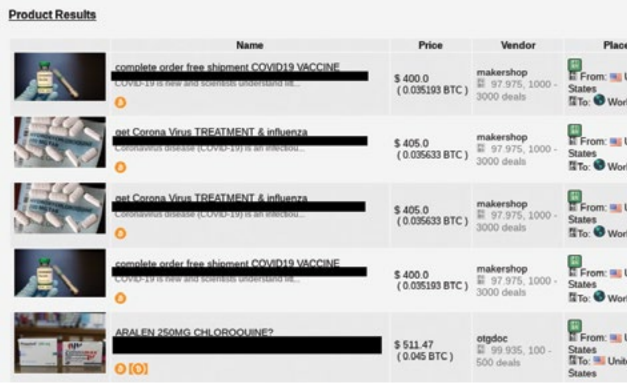
These examples show that criminals are operating on the Darkweb in SEA and against Southeast Asian targets. A coherent, international law enforcement response, supported by routine public awareness, under ministerial control in each country, is essential.

The impact of COVID-19

COVID-19 has had an impact on both criminal activity and Internet usage in general. Whilst the data collection for this report concluded before the crisis, it is salient to note that, in Southeast Asia, Tor usage increased by approximately 20,000 users from February 2020.[30] The motivation for this is unclear.

Criminal behaviour on the Darkweb also changed. Darkweb forums normally dedicated to narcotics have begun offering COVID-19-related merchandise. These include fraudulent COVID-19 vaccines, hydroxychloroquine, and personal protective equipment (see *Figure 11*). The Australian Institute of Criminology further assesses that 60% of Darkweb markets listed at least one COVID-19 related product.[31]

Figure 11. Website selling COVID-19-related merchandise.



Product Results

	Name	Price	Vendor	Place
	complete order free shipment COVID19 VACCINE [redacted] COVID-19 is new and scientists understand litt...	$ 400.0 (0.035193 BTC)	makershop 97.975, 1000 - 3000 deals	From: U States To: Wor
	get Corona Virus TREATMENT & influenza [redacted] Coronavirus disease (COVID-19) is an infectiou...	$ 405.0 (0.035633 BTC)	makershop 97.975, 1000 - 3000 deals	From: U States To: Wor
	get Corona Virus TREATMENT & influenza [redacted] Coronavirus disease (COVID-19) is an infectiou...	$ 405.0 (0.035633 BTC)	makershop 97.975, 1000 - 3000 deals	From: U States To: Wor
	complete order free shipment COVID19 VACCINE [redacted] COVID-19 is new and scientists understand litt...	$ 400.0 (0.035193 BTC)	makershop 97.975, 1000 - 3000 deals	From: U States To: Wor
	ARALEN 250MG CHLOROQUINE? [redacted]	$ 511.47 (0.045 BTC)	otgdoc 99.935, 100 - 500 deals	From: U States To: Unit States

Many criminal activities continued at pace during global lockdowns. Personal information continued to be leaked and sold on the Darkweb. In 2020, 230,000 Indonesian COVID-19 patient records were exposed.[32] Other cyberattacks have increased, especially ransomware attacks, as more organizations are working remotely. Data collected from victims has been found posted on Russian and English-speaking Darkweb forums.[33] Online fraud, credit card theft and phishing attacks continue. Some cases, such as phishing, have increased and adopted COVID-19 themes. For example, Microsoft identified COVID-19 themed emails containing a malicious Excel spreadsheet. When opened, these spreadsheets would download software that would give an attacker remote access to a victim's computer.[34] This can facilitate traditional criminality, advanced persistent threat attacks and hostile state behaviour.

Online Child Sexual Exploitation (OCSE) also rose during the pandemic with law enforcement in Thailand calling for more resources and training in investigating Darkweb and cryptocurrency-facilitated OCSE.[35] Furthermore, the U.S. National Center for Missing & Exploited Children (NCMEC) recorded a 106% increase in reports of suspected Clearnet child sexual exploitation material – rising from 983,734 reports in March 2019 to 2,027,520 in May 2020.[36] Much of the abuse content that is generated ends up being traded and sold on the Darkweb.

Despite this, some organized cybercrime groups are being negatively affected by lockdown. According to Chainalysis, a blockchain analysis company, there has been a 33% decline in the volume of cryptocurrency scams since the commencement of lockdown.[37]

It is clear that COVID-related criminality, on the Darkweb and beyond, has only just begun. States, especially in Southeast Asia, must heed the call to plan and prepare, under a ministerial lead for cyber affairs, for an increase in darknet criminality. Now is not the time to de-invest in complex crime investigation, but to increase resources, operational posture and international cooperation. That is what the public demands and requires.

Darkweb structure and crime areas: a deeper dive

This section of the report provides detail and examples of specific darknet markets and how the associated cybercrime works.

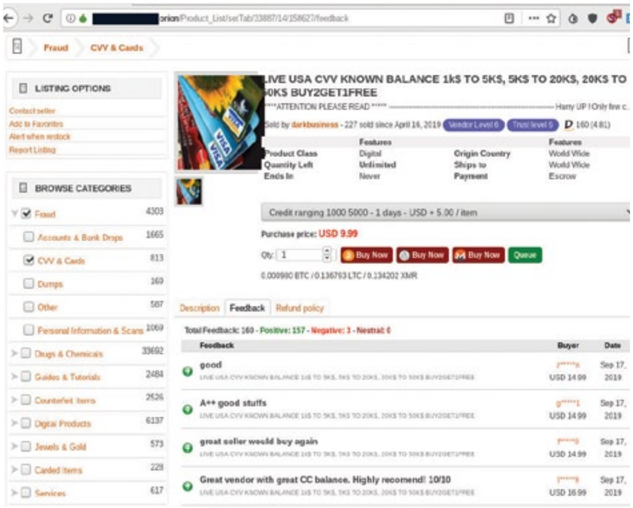
A. Illicit marketplaces

As a consequence of the increasing use of anonymization technology, illicit darknet marketplaces have become more accessible and popular.[38] After Bitcoin was introduced in 2009, it was quickly adopted as a payment method in dark markets. Most notably, in 2011, the Silk Road market, an onion website providing a platform for buying and selling illegal products (mostly drugs), began to operate inside the Tor network using Bitcoin as its primary payment method (although today the use of privacy coins, such as Monero and Ethereum is increasing[39]). Silk Road was the first time these technologies were combined to enable an online market for illegal products to grow significantly.

These marketplaces have not invented new technologies but rather combined various innovations that drive new benefits for both sellers and buyers. Cryptocurrencies, due to their broad anonymity, have become the means for financing cybercrime on the Darkweb.

The number of active marketplaces on the Darkweb has grown from one (Silk Road) in 2011 to 118 in 2019. These markets are competing against each other, and the majority of users will only use the most popular market since a popular market is less likely to be a scam. With the dominance of these large marketplaces, many of the smaller markets are not gaining new customers.

Figure 12. Empire Market – one of the largest online markets for illegal products & services.



[redacted]onion/Product_List/setTab/33887/14/158627/feedback

Fraud > CVV & Cards

LISTING OPTIONS

Contact seller
Add to Favorites
Alert when restock
Report Listing

BROWSE CATEGORIES

☑ Fraud	4303
□ Accounts & Bank Drops	1665
☑ CVV & Cards	813
□ Dumps	169
□ Other	587
□ Personal Information & Scans	1069
□ Drugs & Chemicals	33692
□ Guides & Tutorials	2484
□ Counterfeit Items	2526
□ Digital Products	6137
□ Jewels & Gold	573
□ Carded Items	228
□ Services	617

LIVE USA CVV KNOWN BALANCE 1k$ TO 5K$, 5K$ TO 20K$, 20K$ TO 50K$ BUY2GET1FREE

****ATTENTION PLEASE READ ***** ------------------------------ Harry UP ! Only few c...

Sold by darkbusiness - 227 sold since April 16, 2019 Vendor Level 6 Trust level 5 D 160 (4.81)

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Credit ranging 1000 5000 - 1 days - USD + 5.00 / item

Purchase price: USD 9.99

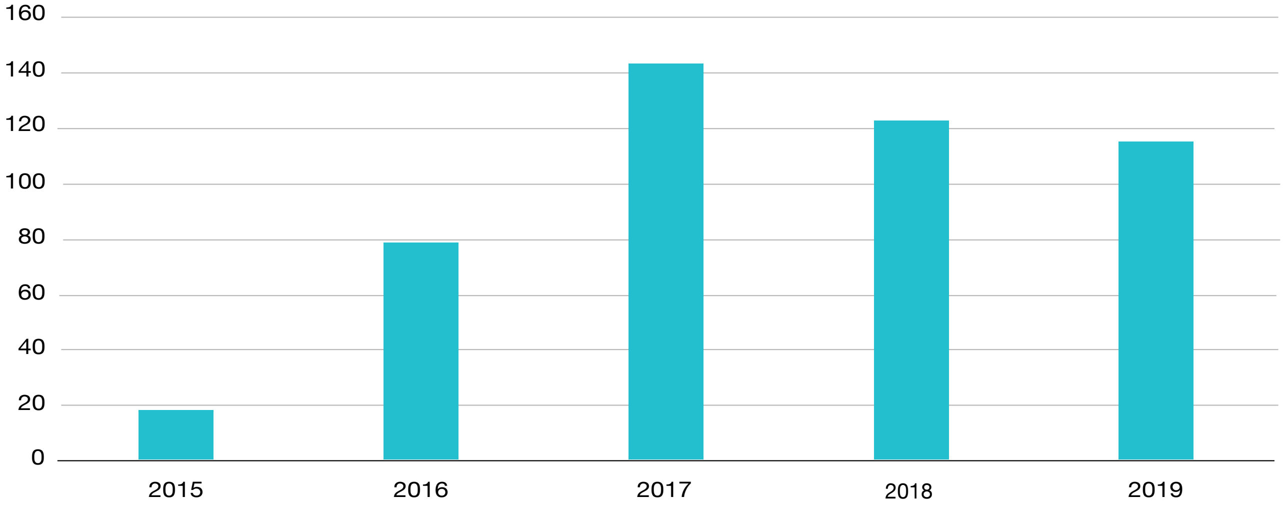
Qty: 1

0.000980 BTC / 0.136793 LTC / 0.134202 XMR

Total Feedback: 160 - Positive: 157 - Negative: 3 - Neutral: 0

Feedback	Buyer	Date
good LIVE USA CVV KNOWN BALANCE 1k$ TO 5K$, 5K$ TO 20K$, 20K$ TO 50K$ BUY2GET1FREE	j*****n USD 14.99	Sep 17, 2019
A++ good stuffs LIVE USA CVV KNOWN BALANCE 1k$ TO 5K$, 5K$ TO 20K$, 20K$ TO 50K$ BUY2GET1FREE	g*****1 USD 14.99	Sep 17, 2019
great seller would buy again LIVE USA CVV KNOWN BALANCE 1k$ TO 5K$, 5K$ TO 20K$, 20K$ TO 50K$ BUY2GET1FREE	j*****g USD 14.99	Sep 17, 2019
Great vendor with great CC balance. Highly recomend! 10/10 LIVE USA CVV KNOWN BALANCE 1k$ TO 5K$, 5K$ TO 20K$, 20K$ TO 50K$ BUY2GET1FREE	j*****g USD 16.99	Sep 17, 2019

Figure 13. The number of active illicit markets on the Darkweb.

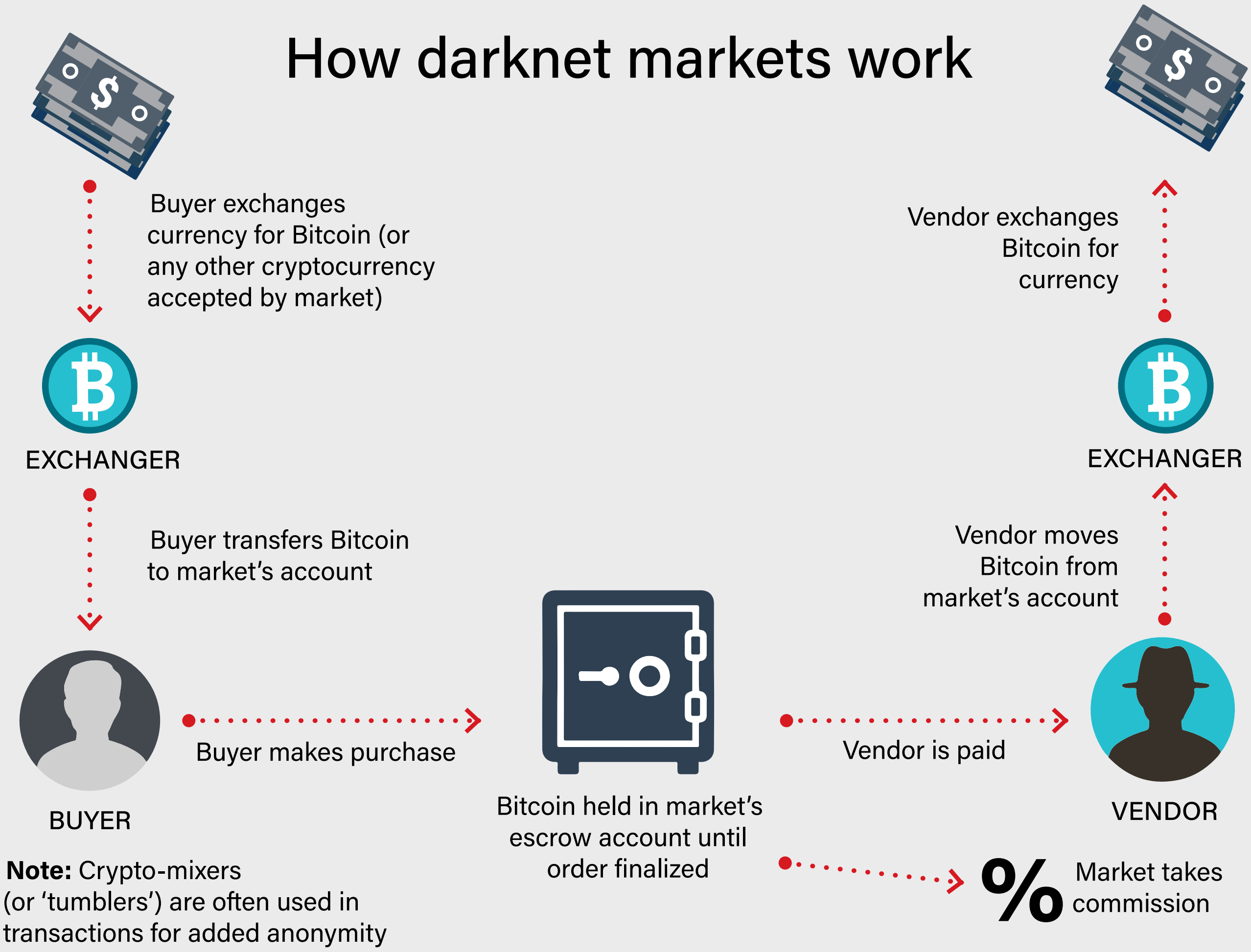


Illicit markets are anonymous, but the trade itself is often visible. There are few access restrictions and therefore, in theory, anyone can access these onion sites and browse the products. As a result, law enforcement personnel monitor illegal activities using web crawling (the automated process of visiting websites and saving the content) and data scraping technologies (extracting relevant information from the content for data analysis). Silk Road was an ideal place to start this more in-depth research on how online communication technologies transform crime.[40] By web crawling it is possible to monitor some of the criminal online activity in real-time. As a result, several academic scholars have published research regarding different aspects of the illegal drug trade.[41,42,43]

These marketplaces operate like normal e-commerce websites except that it is usually illicit goods and services that are being bought and sold.[44,45]

Marketplaces, in general, have feedback and reputation systems to distinguish between allegedly reputable sellers and buyers based on feedback from previous transactions. With both buying and selling, however, it is difficult to determine the veracity of the feedback as all parties are essentially anonymous.[46] This, however, allows investigators to track sellers over time, across markets, as they need to maintain their username and reputation across all platforms. Law enforcement is getting better at taking down darknet markets, but that does not necessarily translate into fewer users/sellers. When a market is taken down, sellers and buyers usually transition to the next largest market. Sellers have even been observed operating under the same username as they move to other marketplaces; for example, starting on Silk Road, then moving to AlphaBay, and then onto more recent iterations. This shows that disruption does not necessarily solve the problem.

How darknet markets work



Buyer exchanges currency for Bitcoin (or any other cryptocurrency accepted by market)

EXCHANGER

Buyer transfers Bitcoin to market's account

BUYER

Buyer makes purchase

Bitcoin held in market's escrow account until order finalized

Vendor is paid

VENDOR

Market takes commission

Vendor moves Bitcoin from market's account

EXCHANGER

Vendor exchanges Bitcoin for currency

Note: Crypto-mixers (or 'tumblers') are often used in transactions for added anonymity and PGP (encryption program) to secure communications between buyers and vendors.

Source: Adapted from evidence entered into the record of Ross Ulbricht's federal trial in the U.S. Southern District Court of New York, depicting a flowchart of Silk Road's payment system, as envisioned by the U.S. Government.

Essential elements of darknet markets

An anonymous marketplace or darknet market needs four components to operate:

1. An anonymous, censor-resistant platform to operate from, e.g. an onion website.
2. An online (semi-) anonymous monetary system, i.e. Bitcoin.
3. An escrow payment system (internal escrow accounting).
4. Reputation and feedback (transparent reputation metric).

When these four technologies are combined and used concurrently, the darknet market can operate efficiently. Without one of these components, the market will cease to operate.[47]

With features like escrow payment systems and reputation/feedback metrics, the likelihood that buyers will receive the products they purchased (and valid product information) has increased. Many sellers attempt to provide accurate product information, and the accumulating feedback verifies the seller's claims.[48,49]

Once the transaction has taken place online, a vendor can ship worldwide through any number of mailing services. When it comes to buying drugs, online trade is considered safer than buying on the street where there is the risk of violence and robbery.[50,51] No physical contact with the seller is needed, and it is easier to obtain accurate information about the substance.[52,53]

The buyer will usually purchase some virtual currency (often Bitcoin), create an account with the marketplace, transfer the bitcoins to the wallet of their account, and then select a product to buy. If the selected item is a physical product, such as a fake passport or an illegal drug, then the buyer provides shipment information to the seller. The escrow system locks the sum of the payment from the buyer's wallet. Next, the seller sends the product, and the buyer gives the public (positive or negative) feedback to the seller. Following that action, the escrow system transfers the payment to the seller.

The feedback given regarding the transaction is important to the seller as future buyers are more likely to select trusted sellers that have received positive feedback. Vendors who build a good reputation, for providing a high-quality service are able to make a name for themselves and then operate within different markets using the same name.

B. Cryptocurrencies

After Bitcoin (the first cryptocurrency) was introduced in 2009, it was quickly adopted as a payment method in the dark markets. Regardless of how anonymous people believe Bitcoin to be, transactions do leave a trail in the Bitcoin blockchain. A blockchain is a public transaction record which shows all the transactions between Bitcoin wallets. Most online Bitcoin exchanges have begun to require proof of identity before one can purchase bitcoins, meaning the identity of the purchaser and where the bitcoins are sent is traceable by default. As a result, there are now services available to hide any digital trail involving illegal transactions. These are commonly called crypto-mixers, tumblers or laundry services.

These services work by mixing incoming bitcoins into a pool with other random bitcoins held in reserve and then outputting other bitcoins which have no connection to the incoming bitcoins. This mixing breaks the link between the initial purchase of the bitcoins and the payment destination thus making it harder to bring an offender to justice by "following the money".

Additional anonymity is provided by using a so-called "double mixer". This two-stage mixing process, executed within a web browser, adds another level of anonymity because neither mixer knows both the source and the destination of your bitcoins. The site facilitates the mixing process but does not learn the used addresses. However, if one of the mixers is insecure or hacked, there is a chance that anonymity may be lost. A further risk is that the mixers used in the process can potentially steal the bitcoins.

Cryptocurrencies

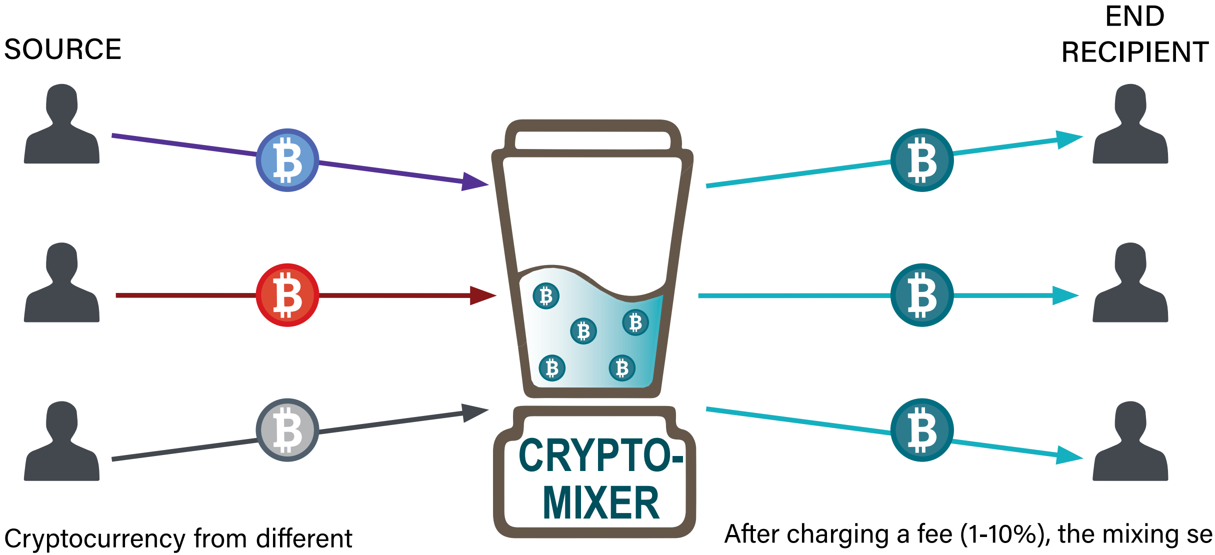
Fast facts

- A cryptocurrency is a form of virtual asset based on a network that is distributed across a large number of computers. This decentralised structure allows them to exist outside the control of governments and central authorities.
- Some of the cryptography used in cryptocurrency today was originally developed for military applications. At one point, governments wanted to put controls on cryptography, but the right for civilians to use it was secured on grounds of freedom of speech.
- 'Blockchains' (organizational methods for ensuring the integrity of transactional data) are an essential component of many cryptocurrencies. Many experts believe that blockchain and related technology will disrupt many industries in the future, including finance and law.
- Cryptocurrencies face criticism for a number of reasons, i.e. their use for illegal activities, exchange rate volatility, and vulnerabilities of the infrastructure underlying them. However, they are also praised for their portability, divisibility, inflation resistance, and transparency.
- The first blockchain-based cryptocurrency was Bitcoin which still remains the most popular and most valuable. As of November 2019, there were over 18 million bitcoins in circulation with a total market value of around US$146 billion.
- Today, the aggregate value of all the cryptocurrencies in existence is around US$214 billion—Bitcoin currently represents more than 68% of the total value.

Source: www.investopedia.com (Cryptocurrency)

Crypto-mixers

Crypto-mixers: services that take in identifiable cryptocurrency tokens from one wallet and output unidentifiable 'clean' tokens to a different wallet (or wallets). Crypto-mixing is similar to money laundering. However, due to the distributed nature of cryptocurrencies, creating unidentifiable tokens is almost impossible.

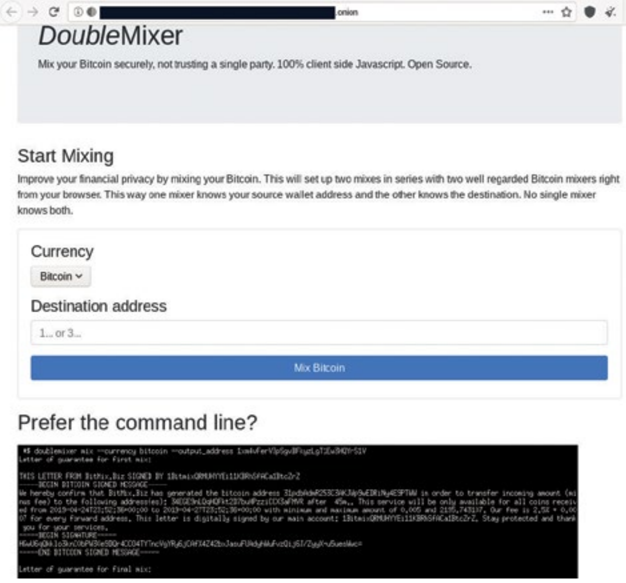


Cryptocurrency from different sources is sent to the mixer.

After charging a fee (1-10%), the mixing service sends the 'mixed' cryptocurrency to wherever it is required. The link to the source is now broken.

These mixer services are not registered as companies. They operate without licenses to handle financial transactions and may break anti-money laundering, counter financing of terrorism and UN Security Council sanctions. Licensed Bitcoin exchange services may try to avoid direct transfers to the known wallet addresses of mixer services.

Figure 14. DoubleMixer website on Tor network.



[redacted].onion

*Double*Mixer

Mix your Bitcoin securely, not trusting a single party. 100% client side Javascript. Open Source.

Start Mixing

Improve your financial privacy by mixing your Bitcoin. This will set up two mixes in series with two well regarded Bitcoin mixers right from your browser. This way one mixer knows your source wallet address and the other knows the destination. No single mixer knows both.

Currency: Bitcoin

Destination address: 1... or 3...

Mix Bitcoin

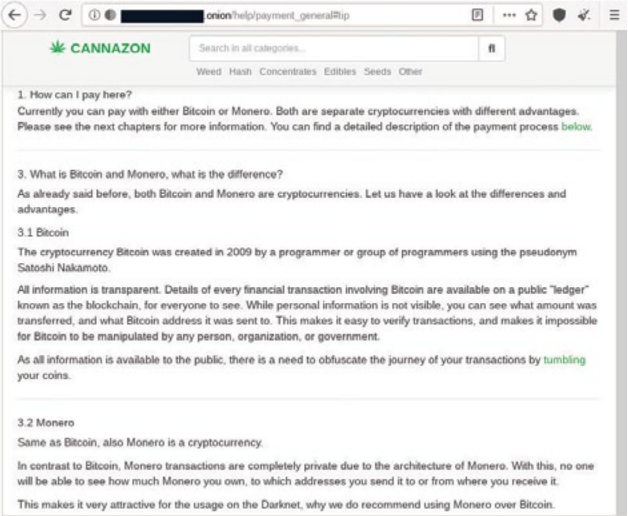
Prefer the command line?

```
#$ doublemixer mix --currency bitcoin --output_address 1xm4vFerV1pSgvBFiyzLgT1Ew3HQYrS1V
Letter of guarantee for first mix:

THIS LETTER FROM BitMix.Biz SIGNED BY 1BitmixQRMUHYYEi11KBRhSFACaIBtcZrZ
-----BEGIN BITCOIN SIGNED MESSAGE-----
We hereby confirm that BitMix.Biz has generated the bitcoin address 31pdbAdwR253C3AKJAp9wEDRiNy4E9PTWW in order to transfer incoming amount (mi
nus fee) to the following address(es): 3KEGE9nLQgHQFkt2B7buWPzziCCX3aFMVR after  45m.. This service will be only available for all coins receiv
ed from 2019-04-24T23:52:38+00:00 to 2019-04-27T23:52:38+00:00 with minimum and maximum amount of 0.005 and 2195.743137. Our fee is 2.5% + 0.00
07 for every forward address. This letter is digitally signed by our main account: 1BitmixQRMUHYYEi11KBRhSFACaIBtcZrZ. Stay protected and thank
 you for your services.
-----BEGIN SIGNATURE-----
H6wU6qQkk1o3knO0bPW3eSDQr4CC04TYTncVgYRj6jCAFX4Z42bxJasuFUAdyHAuFvzQiJ6I/ZygX+u5uesWwc=
-----END BITCOIN SIGNED MESSAGE-----

Letter of guarantee for final mix:
```

Bitcoin is not the only payment method available. There are other cryptocurrencies, called privacy coins, which are used in illegal trade such as Monero, Litecoin, Bitcoin Cash, Ethereum and Dash.

Monero has attracted cybercriminals because it offers a greater degree of anonymity for transactions. Monero creates unique addresses for every transaction, and only the receiver can access the full transaction information. Monero also implements mixing automatically and makes it difficult to trace transactions on their blockchain.

Figure 15. Payment advice to site users on Cannazon marketplace.*



[redacted].onion/help/payment_general#tip

CANNAZON
Search in all categories...
Weed Hash Concentrates Edibles Seeds Other

1. How can I pay here?

Currently you can pay with either Bitcoin or Monero. Both are separate cryptocurrencies with different advantages. Please see the next chapters for more information. You can find a detailed description of the payment process below.

3. What is Bitcoin and Monero, what is the difference?

As already said before, both Bitcoin and Monero are cryptocurrencies. Let us have a look at the differences and advantages.

3.1 Bitcoin

The cryptocurrency Bitcoin was created in 2009 by a programmer or group of programmers using the pseudonym Satoshi Nakamoto.

All information is transparent. Details of every financial transaction involving Bitcoin are available on a public "ledger" known as the blockchain, for everyone to see. While personal information is not visible, you can see what amount was transferred, and what Bitcoin address it was sent to. This makes it easy to verify transactions, and makes it impossible for Bitcoin to be manipulated by any person, organization, or government.

As all information is available to the public, there is a need to obfuscate the journey of your transactions by tumbling your coins.

3.2 Monero

Same as Bitcoin, also Monero is a cryptocurrency.

In contrast to Bitcoin, Monero transactions are completely private due to the architecture of Monero. With this, no one will be able to see how much Monero you own, to which addresses you send it to or from where you receive it.

This makes it very attractive for the usage on the Darknet, why we do recommend using Monero over Bitcoin.

**The site recommends using Monero over Bitcoin as Monero offers greater transaction anonymity. When using Bitcoin, they recommend the use of a mixer service ('tumbling your coins').*

First introduced as a payment method by AlphaBay and Oasis marketplaces, Monero has been accepted by major Darkweb marketplaces since 2016. Despite this, Bitcoin still dominates illegal trade, and most of the markets only use Bitcoin as a payment method. This is illustrated in *Table 1* overleaf which shows the payment options accepted by 40 widely known marketplaces on the Darkweb. It is anticipated that privacy coins will, with time, become the primary payment method for illicit commodities.

Table 1. Payment options on 40 Darkweb marketplaces as of December 2019.

Marketplace name	Bitcoin	Monero	Litecoin	Bitcoin Cash	Ethereum	Dash
Empire Market	Bitcoin	Monero	Litecoin			
Hydramarket	Bitcoin					
Apollon Market	Bitcoin	Monero	Litecoin	Bitcoin Cash		
Genesis Market	Bitcoin					
BitMarket	Bitcoin					
Brians Club Market	Bitcoin		Litecoin			
Cannazon market	Bitcoin	Monero				
Alpha Omega Market	Bitcoin					
Ali Marketplace	Bitcoin					
Sipulimarket	Bitcoin					
Icarus Market	Bitcoin	Monero				
DeepSea Market	Bitcoin					
Elite Market	Bitcoin					
Grey Market	Bitcoin	Monero				
Samara Market	Bitcoin	Monero		Bitcoin Cash		
Berlusconi Market	Bitcoin	Monero	Litecoin			
DarkMarket	Bitcoin	Monero				
White House Market		Monero				
Luna Market	Bitcoin					
Silk Road 4	Bitcoin	Monero	Litecoin		Ethereum	
Midland City	Bitcoin					
Point Market	Bitcoin			Bitcoin Cash	Ethereum	
Dr. Bob	Bitcoin					
CanonZone	Bitcoin	Monero				
The French Connection	Bitcoin					
Dutch Drugs	Bitcoin	Monero	Litecoin		Ethereum	Dash
CharlieUK	Bitcoin					
Cannabis Grower	Bitcoin					
Glass Werkz	Bitcoin					
ElHerbolario's Shop	Bitcoin					
Cocaine Market	Bitcoin					
Dutch Magic	Bitcoin					
Pushing Taboo	Bitcoin					
Global Dreams	Bitcoin					
Evil Shop	Bitcoin					
Yakuza Market	Bitcoin	Monero				
Weedstore	Bitcoin					
Rsclub Market	Bitcoin					
Hidden Marketplace	Bitcoin					
HookShop	Bitcoin					

As shown in *Table 1*, almost every marketplace is using Bitcoin as a payment method – the only exception being the White House Market which only accepts Monero. Monero is available as a payment method in one-third of these popular marketplaces and is often recommended because of the anonymity it provides without a separate mixer service. Litecoin is available in 17.5 per cent of the markets. Other payment methods supported are Bitcoin Cash (different to Bitcoin), Ethereum and Dash, but only by a few marketplaces.

As the most widely accepted currency in Darkweb marketplaces, Bitcoin can be accessed easily and quickly through exchanges, and transactions are not easily traced if mixer services are used.

Monero is also available to buy through some exchanges, but not all, i.e. the large cryptocurrency exchange, Coinbase, does not support Monero. In 2020, Coinbase offered 30 different cryptocurrencies to trade but this did not include Monero. However, Monero is expected to gain more popularity in Darkweb marketplaces because it provides anonymity by default.

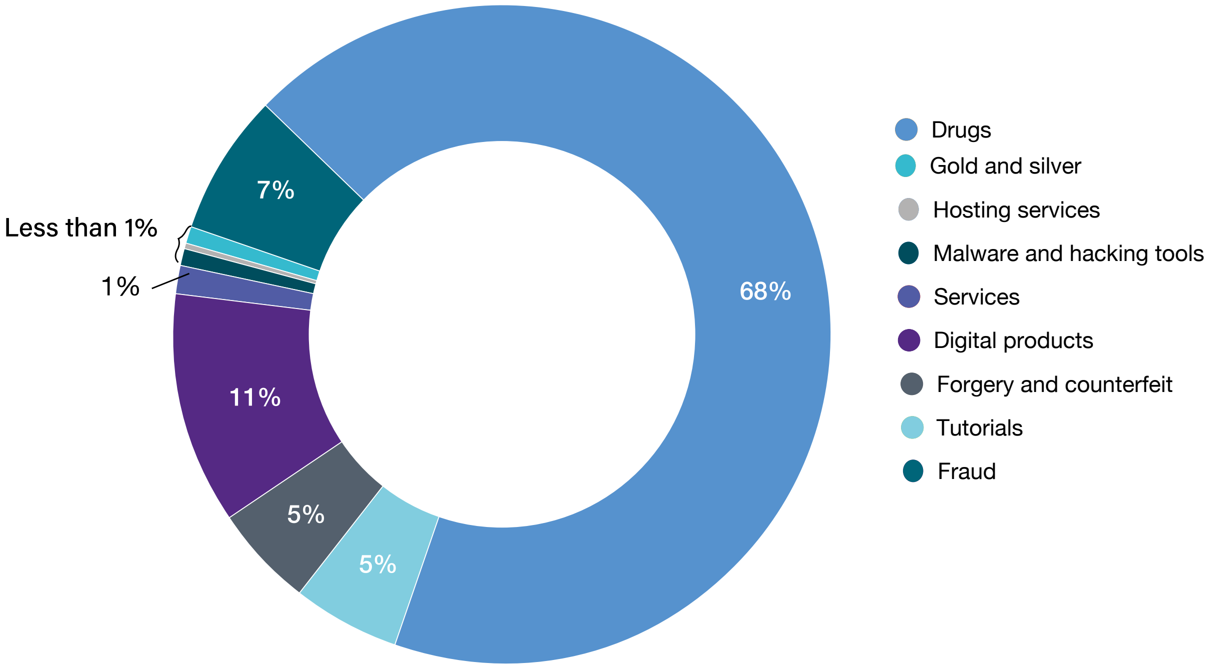
C. Illicit products and services

There are a wide range of illicit products and services available on the Darkweb. This section reviews the illicit products and services available on the Tor network.

Combined data from four Darkweb marketplaces (Empire Market, Apollo Market, Silk Road 3.1, Elite Market) shows that drugs are the most prevalent category of illicit products available from these marketplaces (68 per cent). Next are digital products (12 per cent) which include games, pirated software and associated license keys; then fraudulent items (7 per cent) which includes payment card information, personal information and stolen credentials; followed by counterfeit items (5 per cent) which include money, electronics, passports and driver licenses.

Copyrighted material is shared on the Darkweb as well. So-called BitTorrent sites (torrents) in the Tor network contain torrent files that enable users to download movies, music, and games illegally.

Figure 16. Percentage of products and services available on Darkweb marketplaces as of December 2019.*

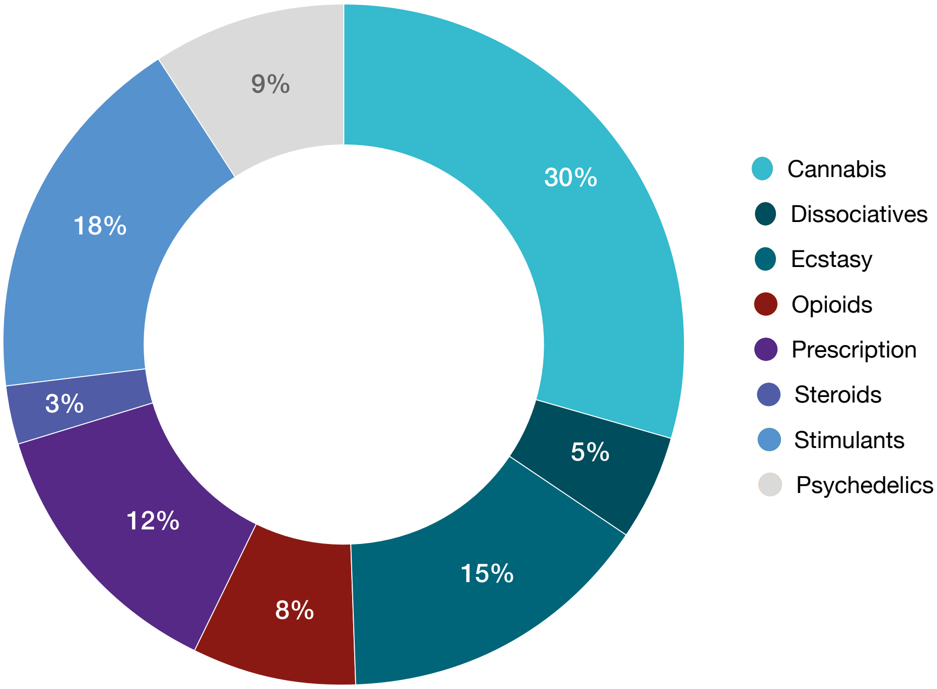


**Combined data from four popular marketplaces (Empire Market, Apollo Market, Silk Road 3.1, Elite Market) showing that drugs are by far the most prevalent category of product available from these marketplaces as of Dec. 2019.*

1. Drugs

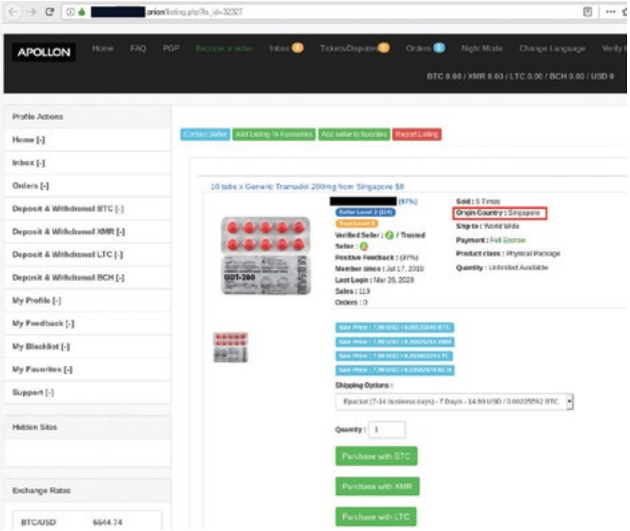
The most widely traded category of products on the Tor darknet is drugs. The combined total number of items on sale on the four targeted marketplaces in December 2019 is 138,405 and, of these, 94,389 were drug items. The types of drugs include MDMA, amphetamine, methamphetamine, cannabis in all forms, cocaine, opioids in all forms, LSD, psychedelic mushrooms, ketamine and prescription drugs (mostly benzodiazepines).

Figure 17. Percentage of drug types available on four popular marketplaces in December 2019.*



** Combined data from four popular marketplaces (Empire Market, Apollo Market, Silk Road 3.1, Elite Market) as of Dec. 2019.*

Figure 18. Example of website selling drugs on the Darkweb.*



10 tabs x Generic Tramadol 200mg from Singapore $8

[redacted] (97%)
Seller Level 3 (119)
Trust Level 3
Verified Seller : / Trusted
Seller :
Positive Feedback : (97%)
Member since : Jul 17, 2019
Last Login : Mar 25, 2020
Sales : 119
Orders : 0

Sold : 5 Times
Origin Country : Singapore
Ship to : World Wide
Payment : Full Escrow
Product class : Physical Package
Quantity : Unlimited Available

Sale Price : 7.99 USD / [illegible] BTC
Sale Price : 7.99 USD / [illegible] XMR
Sale Price : 7.99 USD / [illegible] LTC
Sale Price : 7.99 USD / [illegible] BCH

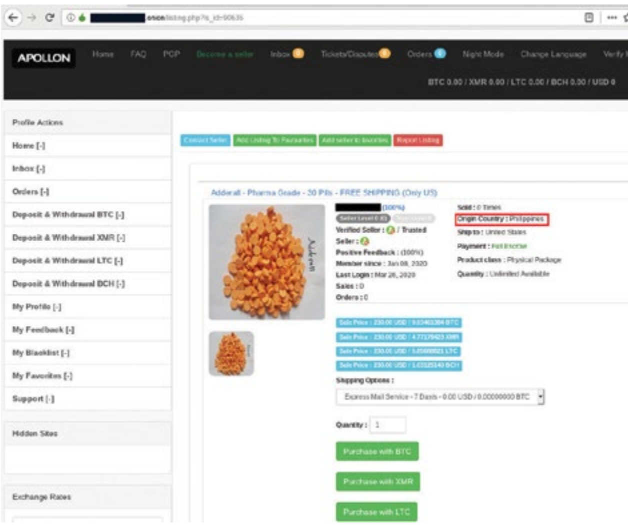
Shipping Options : Epacket (7-14 business days) - 7 Days - 14.99 USD / 0.00225592 BTC

Quantity : 1

BTC/USD 6644.74

**Shows vendor sending drugs from Singapore to anywhere in the world.*

Figure 19. Example of illegal drug trade on the Darkweb.*



Adderall - Pharma Grade - 30 Pills - FREE SHIPPING (Only US)

[redacted] (100%)
Seller Level 0 (0)
Verified Seller : / Trusted
Seller :
Positive Feedback : (100%)
Member since : Jan 08, 2020
Last Login : Mar 26, 2020
Sales : 0
Orders : 0

Sold : 0 Times
Origin Country : Philippines
Ship to : United States
Payment : Full Escrow
Product class : Physical Package
Quantity : Unlimited Available

Sale Price : 230.00 USD / 0.03463384 BTC
Sale Price : 230.00 USD / 4.77179423 XMR
Sale Price : 230.00 USD / [illegible] LTC
Sale Price : 230.00 USD / 1.03125140 BCH

Shipping Options : Express Mail Service - 7 Days - 0.00 USD / 0.00000000 BTC

Quantity : 1

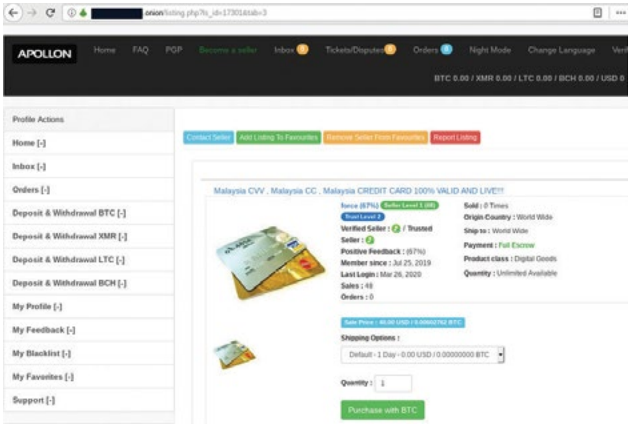
**Shows a vendor sending products from the Philippines to the United States.*

2. Payment card fraud

The trade of compromised financial information on the Darkweb is one example of cybercrime-as-a-service (CaaS). Payment card fraud means the acquisition and unauthorized use of payment card data, such as the card number, billing address, security code and expiry date, to purchase products.[54] In most cases, the victims are unaware of the unauthorized use of their cards.

Social engineering attacks, for example, trick the victim into revealing their card and personal details. Victims may give their information without ever knowing that the website or customer service agent was actually a fraudster. This type of illegal activity has grown steadily with card information stolen using data breaches, social engineering attacks (malicious activities accomplished through human interaction), data-stealing malware and phishing tools (a lot of which are now readily available on forums, marketplaces and automated card shops).[55] Cases where criminals hack into companies and steal large credit card information databases (often compromising millions of accounts in the process) are becoming more common.

Figure 20. Vendor offering a counterfeit card service aimed at the Southeast Asia region.



[redacted] onion/listing.php?ls_id=17301&tab=3

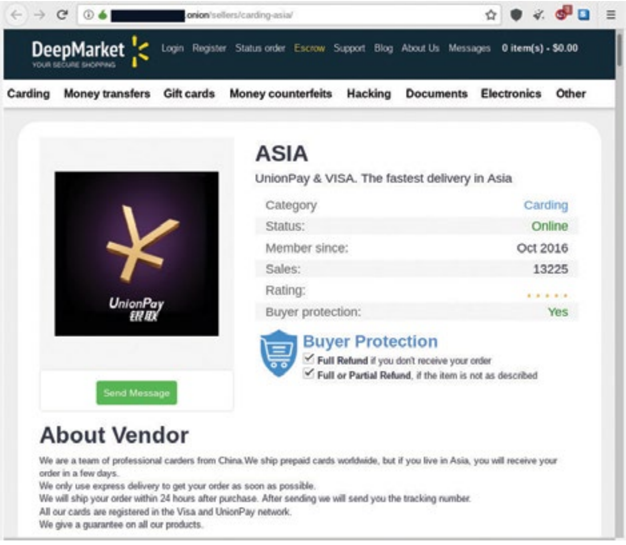
Malaysia CVV , Malaysia CC , Malaysia CREDIT CARD 100% VALID AND LIVE!!!

lonce (67%) Seller Level 1 (48)
Trust Level 2
Verified Seller : 2 / Trusted Seller : 2
Positive Feedback : (67%)
Member since : Jul 25, 2019
Last Login : Mar 26, 2020
Sales : 48
Orders : 0

Sold : 0 Times
Origin Country : World Wide
Ship to : World Wide
Payment : Full Escrow
Product class : Digital Goods
Quantity : Unlimited Available

Sale Price : 40.00 USD / 0.00602762 BTC
Shipping Options : Default - 1 Day - 0.00 USD / 0.00000000 BTC
Quantity : 1

Figure 21. Malaysian credit card information on sale on the Darkweb.



[redacted] onion/sellers/carding-asia/

ASIA

UnionPay & VISA. The fastest delivery in Asia

Category	Carding
Status:	Online
Member since:	Oct 2016
Sales:	13225
Rating:	★★★★★
Buyer protection:	Yes

Buyer Protection
☑ Full Refund if you don't receive your order
☑ Full or Partial Refund, if the item is not as described

About Vendor

We are a team of professional carders from China.We ship prepaid cards worldwide, but if you live in Asia, you will receive your order in a few days.
We only use express delivery to get your order as soon as possible.
We will ship your order within 24 hours after purchase. After sending we will send you the tracking number.
All our cards are registered in the Visa and UnionPay network.
We give a guarantee on all our products.

Web skimming is another method of card fraud. A payment page on a website is compromised when a criminal installs malware on the page, thereby stealing the victim's payment information.

On the Darkweb, there are tutorials and tools for sale on how to hack card payment devices and systems. This often occurs at the point of sale (PoS), where people make payment transactions. A PoS system consists of a device that reads card information and PoS software in a computer that sends the payment data to the payment service provider. Malware tools are sold on the Darkweb that can be installed on the PoS system, allowing the attacker to collect card data during payment processing.

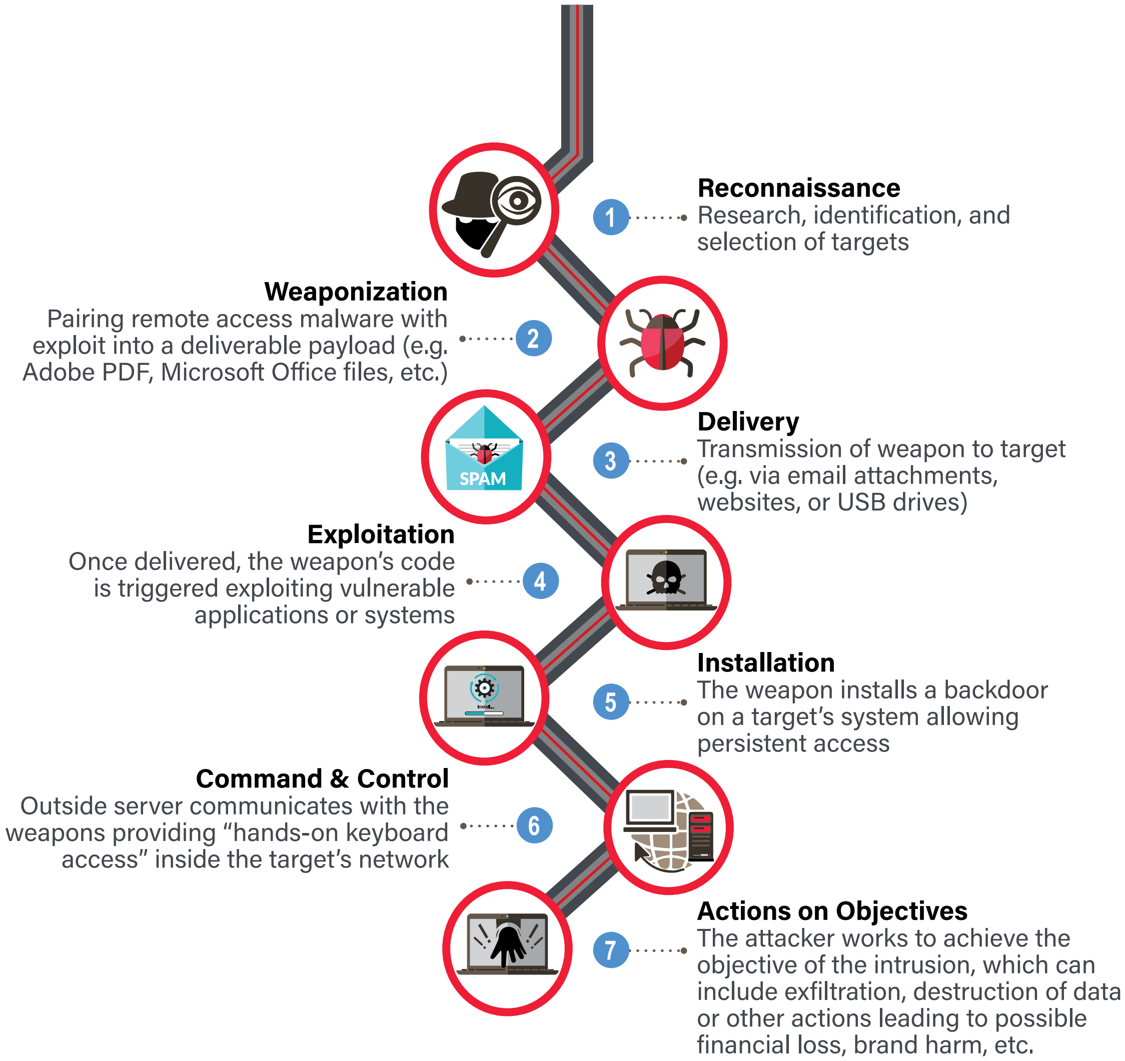
The collected credit card information can be used for fraudulent payments or sold forward. On Darkweb marketplaces, there are extensive collections of credit card information on sale which criminals can buy to get cash out or make fraudulent purchases. The risks to economic stability and prosperity are abundantly clear.

3. Malware-as-a-service

Highly skilled programmers are able to build computer programs and networks capable of launching cyberattacks against organizations. It is this kind of software, developed into toolkits and robotic networks (botnets) that are sold as a service on the Darkweb. This is known as "malware-as-a-service" (MaaS). MaaS enables non-cyber specialists to buy software and then use it to infect systems with malware and control those systems for illegal use. In effect, the criminals purchasing these tools gain access to highly complex, intrusive attack vectors, which they are sometimes incapable of controlling after deployment. Even highly proficient actors face this challenge – as seen in the 2017 WannaCry and NotPetya scenarios. The risks posed from an uncontrolled cyber-attack extend far beyond traditional cybercriminal impact. Conflict, and even warfare, is a potential result. It is therefore essential that States have a ministerial lead on cyber affairs, who can engage at the highest levels of preventive cyber diplomacy in ASEAN, the UN General Assembly and the UN Security Council.

How cyberattackers attack

Cyberattack: the deliberate exploitation of computer systems and networks to take over or cause damage to a victim.



1 **Reconnaissance**
Research, identification, and selection of targets

2 **Weaponization**
Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF, Microsoft Office files, etc.)

3 **Delivery**
Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

4 **Exploitation**
Once delivered, the weapon's code is triggered exploiting vulnerable applications or systems

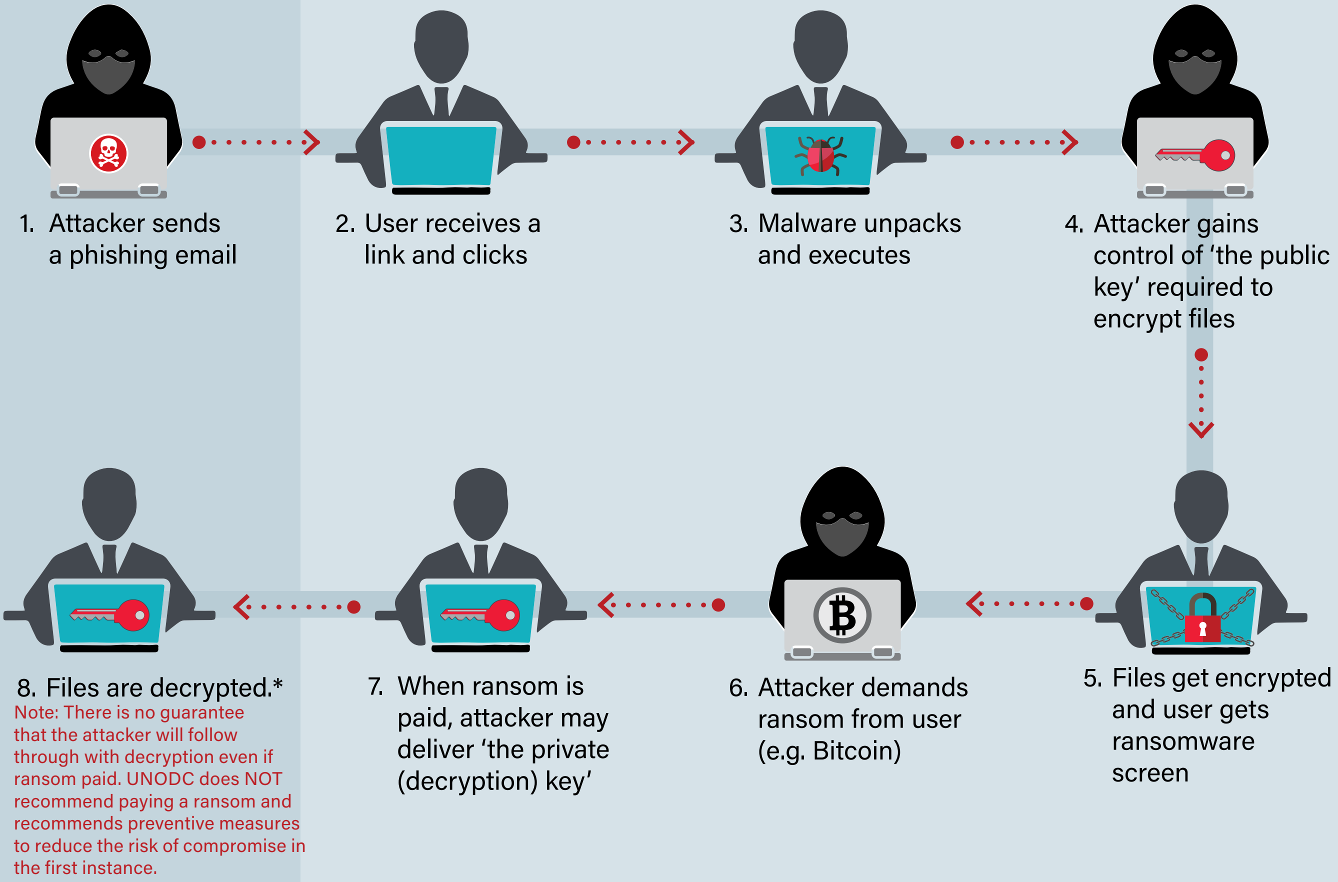
5 **Installation**
The weapon installs a backdoor on a target's system allowing persistent access

6 **Command & Control**
Outside server communicates with the weapons providing "hands-on keyboard access" inside the target's network

7 **Actions on Objectives**
The attacker works to achieve the objective of the intrusion, which can include exfiltration, destruction of data or other actions leading to possible financial loss, brand harm, etc.

Source: Adapted from The Cyber Kill Chain® developed by Lockheed Martin.

Anatomy of a ransomware attack



1. Attacker sends a phishing email
2. User receives a link and clicks
3. Malware unpacks and executes
4. Attacker gains control of 'the public key' required to encrypt files
5. Files get encrypted and user gets ransomware screen
6. Attacker demands ransom from user (e.g. Bitcoin)
7. When ransom is paid, attacker may deliver 'the private (decryption) key'
8. Files are decrypted.*

Note: There is no guarantee that the attacker will follow through with decryption even if ransom paid. UNODC does NOT recommend paying a ransom and recommends preventive measures to reduce the risk of compromise in the first instance.

Ransomware-as-a-Service (RaaS): the practice of providing ransomware and it's control systems to customers for criminal use. All aspects of ransomware creation and control may be provided as a service for purchase. Customers can choose the services they need in an ala carte fashion.

Source: Adapted from Centrify Corporations

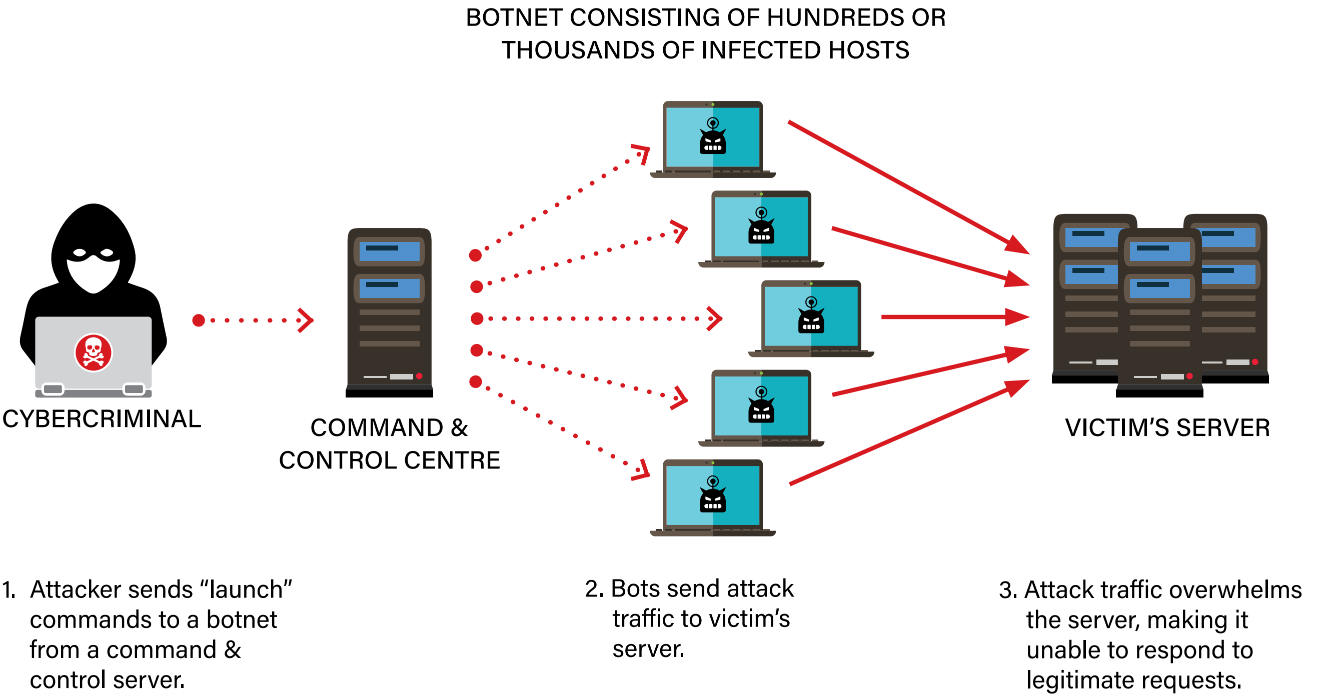
4. Ransomware

Ransomware is a type of malware that takes data as a hostage. The criminal uses the ransomware to prevent a target victim from accessing their data, and then threatens to publish the victim's data or exploit them in some other way unless a ransom is paid.

Sometimes the victims of ransomware attacks are instructed to pay the ransom through a Darkweb site, often in cryptocurrency, thereby making it more difficult to track the destination of the funds. Darkweb vendors also sell ransomware tools and distribution networks which only exacerbates the problem and proliferation of ransomware.

Distributed denial-of-service (DDoS) attack

DDoS: a cyberattack that uses a distributed network of computers to overwhelm a target system's resources to the point that the target cannot continue functioning properly.


BOTNET CONSISTING OF HUNDREDS OR THOUSANDS OF INFECTED HOSTS
CYBERCRIMINAL
COMMAND & CONTROL CENTRE
VICTIM'S SERVER
1. Attacker sends "launch" commands to a botnet from a command & control server.
2. Bots send attack traffic to victim's server.
3. Attack traffic overwhelms the server, making it unable to respond to legitimate requests.

Source: Adapted from F5 Labs (Application Threat Intelligence)

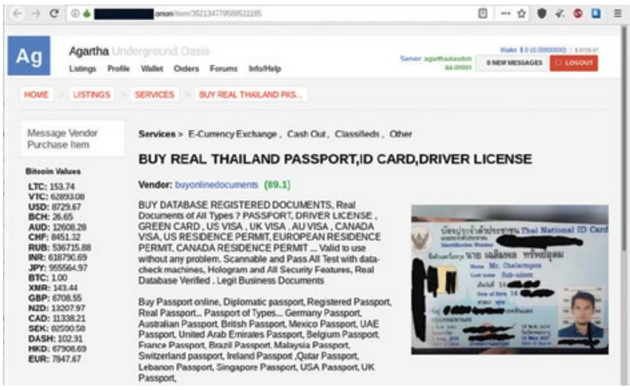
5. Denial-of-service

A denial-of-service (DoS) is an attack on a service that disrupts its normal function and prevents others from accessing it. This is usually an attack on an online service like a website, although attacks can also be launched against whole networks. Criminals sell DoS attacks as a service on the Darkweb. This often involves infecting a large number of computers with their malware, and then using this botnet to launch DoS attacks. It is the owners of these botnets that sell their DoS capabilities through Darkweb marketplaces. Buyers can also rent the capacity of the botnets to take down a particular online service. The buyer supplies the details of the targeted service to the vendor and then pays per hour for the vendor to carry out the DoS attack. A distributed denial-of-service (DDoS) attack is one in which the botnets overwhelm the target service with more traffic than the server or network can accommodate, causing them to crash.

6. Forgery

Forgery is another popular service offered on the Darkweb and this is often closely related to identity theft. On the Darkweb, criminals trade counterfeit passports, driver's licences, and money. Access to personal information that will assist with the forgery of identity documents is also on sale. Counterfeit documents and forgery services are popular on the Darkweb, accounting for 5% of all trade in the most popular marketplaces. Of course, these forged documents are usually purchased to conceal the criminals' real identities as they commit other crimes.

Figure 22. Vendor selling a range of counterfeit and stolen documents.*


[redacted]onion/item/352134779588511185

Agartha Underground Oasis

Ag
Listings Profile Wallet Orders Forums Info/Help
0 NEW MESSAGES
LOGOUT
HOME > LISTINGS > SERVICES > BUY REAL THAILAND PAS...
Message Vendor
Purchase Item

Bitcoin Values

LTC:	153.74
VTC:	62893.08
USD:	8729.67
BCH:	26.65
AUD:	12608.28
CHF:	8451.32
RUB:	536715.88
INR:	618790.69
JPY:	955564.97
BTC:	1.00
XMR:	143.44
GBP:	6708.55
NZD:	13207.97
CAD:	11338.21
SEK:	82590.58
DASH:	102.31
HKD:	67908.69
EUR:	7847.67

Services > E-Currency Exchange , Cash Out , Classifieds , Other

BUY REAL THAILAND PASSPORT,ID CARD,DRIVER LICENSE

Vendor: buyonlinedocuments (89.1)

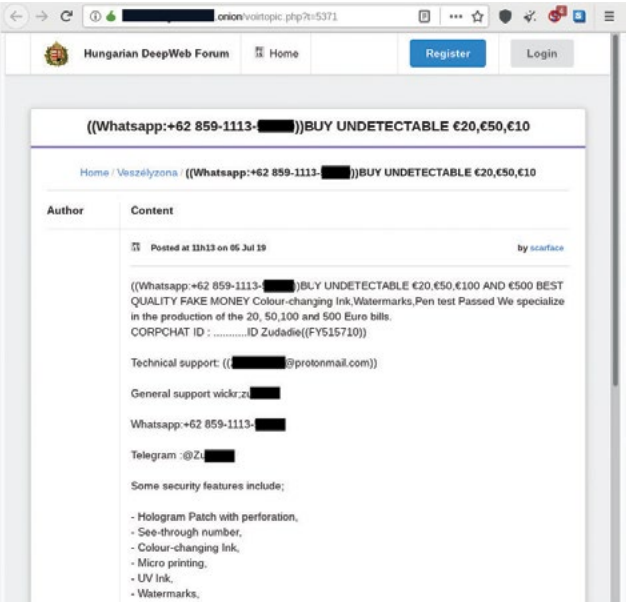
BUY DATABASE REGISTERED DOCUMENTS, Real Documents of All Types ? PASSPORT, DRIVER LICENSE , GREEN CARD , US VISA , UK VISA , AU VISA , CANADA VISA, US RESIDENCE PERMIT, EUROPEAN RESIDENCE PERMIT, CANADA RESIDENCE PERMIT ... Valid to use without any problem. Scannable and Pass All Test with data-check machines, Hologram and All Security Features, Real Database Verified . Legit Business Documents

Buy Passport online, Diplomatic passport, Registered Passport, Real Passport... Passport of Types... Germany Passport, Australian Passport, British Passport, Mexico Passport, UAE Passport, United Arab Emirates Passport, Belgium Passport, France Passport, Brazil Passport, Malaysia Passport, Switzerland passport, Ireland Passport ,Qatar Passport, Lebanon Passport, Singapore Passport, USA Passport, UK Passport,

[redacted]

As well as a wide range of counterfeit documents this vendor is selling "real" passports, ID cards and driver's licenses from Thailand.

Figure 23. Vendor selling fake currency.*


[redacted].onion/viewtopic.php?t=5371

((Whatsapp:+62 859-1113-[redacted]))BUY UNDETECTABLE €20,€50,€10

Home / Veszélyzona / ((Whatsapp:+62 859-1113-[redacted]))BUY UNDETECTABLE €20,€50,€10

Author	Content
	Posted at 11h13 on 05 Jul 19 by scarface

((Whatsapp:+62 859-1113-[redacted]))BUY UNDETECTABLE €20,€50,€100 AND €500 BEST QUALITY FAKE MONEY Colour-changing Ink,Watermarks,Pen test Passed We specialize in the production of the 20, 50,100 and 500 Euro bills.
CORPCHAT ID : ....ID Zudadie((FY515710))

Technical support: (([redacted]@protonmail.com))

General support wickr;zu[redacted]

Whatsapp:+62 859-1113-[redacted]

Telegram :@Zu[redacted]

Some security features include;

- Hologram Patch with perforation,
- See-through number,
- Colour-changing Ink,
- Micro printing,
- UV Ink,
- Watermarks,

7. Scamming websites

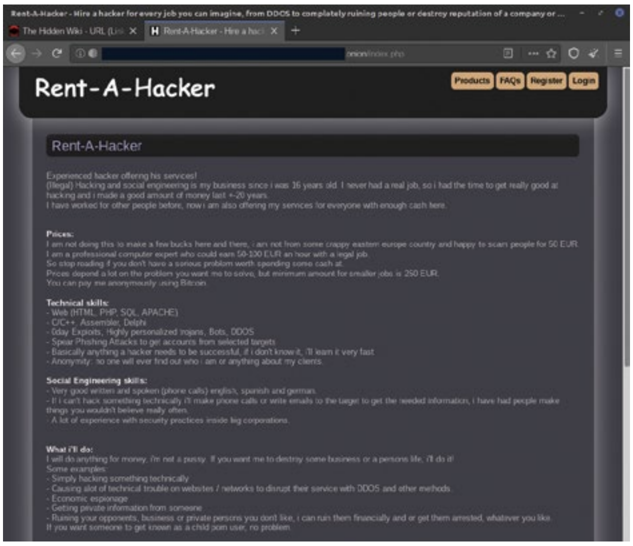
Not surprisingly, the anonymous Darkweb is home to many scammers. One scam includes websites and forums who request Bitcoin payments upfront for their products and services. There is no guarantee that the product or service is going to be delivered and little chance of recompense if the buyer is not satisfied with their purchase. In mid-2020, many Darkweb sites claimed to be selling vaccines or medicine to fight the coronavirus during the COVID-19 pandemic. These sites asked for substantial upfront payments and never delivered what they promised.

Another type of scam that occurs on the Darkweb is an "exit scam". This occurs when a marketplace suddenly closes without warning, taking with it all the bitcoins currently saved to the wallets of the site users. Vendors can also stop delivering their products or services and escape with all the bitcoins paid for unshipped orders.

8. Hacking forums

Hacker forums are asynchronous forums created and operated primarily to discuss topics related to hacking. Topics of interest in these forums range from general computer security news and tutorials to the distribution of malware and leaked information. These forums also discuss and share anonymity tips, server hacking tools and password cracking techniques.

Figure 24. A vendor offering a variety of hacking services.


Rent-A-Hacker - Hire a hacker for every job you can imagine, from DDOS to completely ruining people or destroy reputation of a company or ...

[redacted]onion/index.php

Rent-A-Hacker

Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my business since i was 16 years old. I never had a real job, so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now i am also offering my services for everyone with enough cash here.

Prices:
I am not doing this to make a few bucks here and there, i am not from some crappy eastern europe country and happy to scam people for 50 EUR.
I am a professional computer expert who could earn 50-100 EUR an hour with a legal job.
So stop reading if you don't have a serious problem worth spending some cash at.
Prices depend a lot on the problem you want me to solve, but minimum amount for smaller jobs is 250 EUR.
You can pay me anonymously using Bitcoin.

Technical skills:
- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successful, if i don't know it, i'll learn it very fast
- Anonymity: no one will ever find out who i am or anything about my clients.

Social Engineering skills:
- Very good written and spoken (phone calls) english, spanish and german.
- If i can't hack something technically i'll make phone calls or write emails to the target to get the needed information, i have had people make things you wouldn't believe really often.
- A lot of experience with security practices inside big corporations.

What i'll do:
I will do anything for money, i'm not a pussy. If you want me to destroy some business or a persons life, i'll do it!
Some examples:
- Simply hacking something technically
- Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
- Economic espionage
- Getting private information from someone
- Ruining your opponents, business or private persons you dont like, i can ruin them financially and or get them arrested, whatever you like.
If you want someone to get known as a child porn user, no problem.

Discussion forums and channels are frequently used on the Darkweb to coordinate attacks, share attack tools, and for general communication on topics related to illicit activities.

9. Personally identifiable and non-identifiable information disclosure

A popular activity among cybercriminals is to share breached data such as passwords, confidential documents, databases, and financial information. This data is routinely exploited by criminals who conduct cyberattacks that take place outside the Darkweb.

Unauthorized data leakage does not necessarily mean that an organization is the victim of malicious hacking. In fact, the majority of data leakage incidents claim to be accidental. For example, an employee may unintentionally send an email to the wrong person or mistakenly give an outsider access to the company system. Irrespective of motive, unintentional data leakage can be just as damaging as intentional breaches.

Intentional information leakage happens when an attacker (either from within the target company or an outsider) gains access to the organization's data. Cybercriminals often use malware to target employees and their computers with a high success rate, but less-technically proficient methods can also be very effective, i.e. cybercriminals can easily fake a legitimate business email account and request any number of employees to send them the company's sensitive information or trade secrets.

Typically, criminals copy and paste compromised data onto an information-leaking platform site and publish it under a unique username. Cybercriminals share this username with other criminals who are then able to access the illicit content. The content sometimes only exists for a short period on the paste site thus limiting overall exposure. Other sites, however, retain the data indefinitely.

Underground Darkweb forums are regularly used by hackers to announce data breaches, before sharing or trading information. Analysing and identifying the discussion threads on these forums can help compromised victims respond to the incidents in time.

10. Selling access to organizations

Hackers sometimes secretly retain access to compromised servers without the knowledge of the targeted organization. This access is highly valuable. Some groups specialize in gaining unauthorized access to servers and then sell this information to other groups who specialize in carrying out operations within the target organizations. Transnational cybercrime groups that specialize in gaining access to high-value-target organizations will sell remote access credentials on the Darkweb. After receiving payment, they provide instructions to the buyer on how to access the target organization remotely.

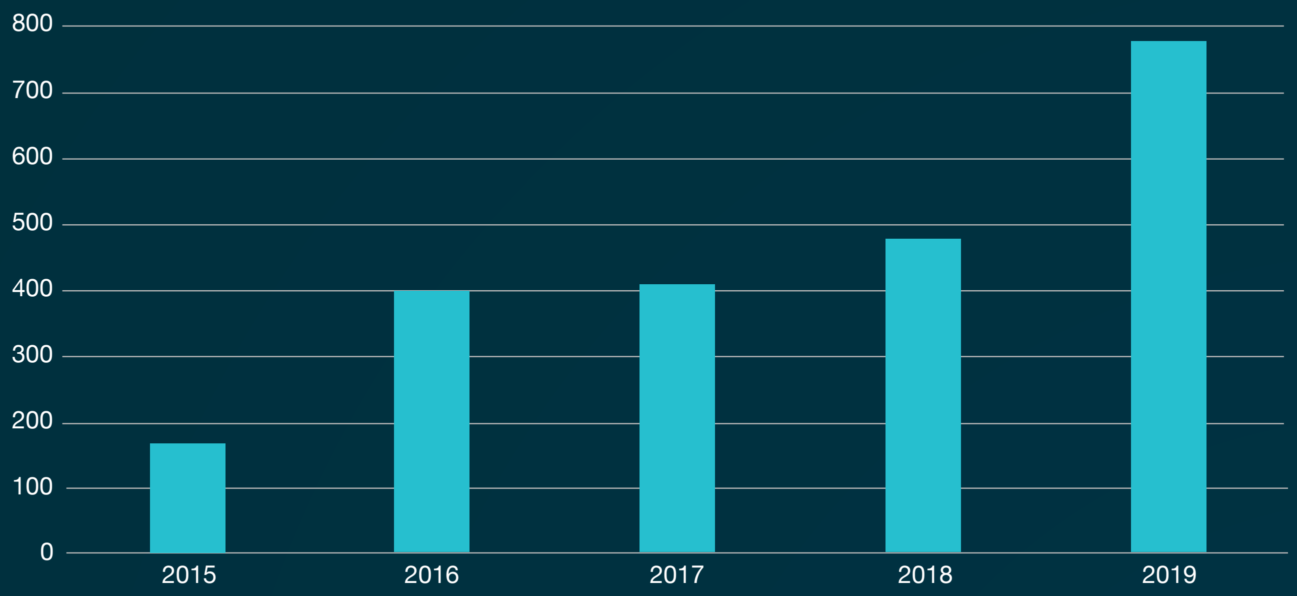
11. Child sexual exploitation material

Darkweb forums (and their users) have been archiving, sharing, trading and selling child sexual exploitation material (CSEM) for many years. Cumulatively, the amount of CSEM increases over time as new content is added and old material is archived.

It is difficult to remove this content permanently. CSEM sites often replicate the content from other sites, meaning when one website gets taken down, the data remains online on other sites. With new sites being set up and new material being added constantly, there is a continuation of services.

Some websites even state that they are gathering an archive of CSEM material to distribute and advertise having terabytes of content available. There are also sites which sell access to CSEM – including pay-per-view live-streaming abuse, with Bitcoin typically the currency of choice for payment.

Figure 25. Number of published unique CSEM websites on the Darkweb (2015-2019).

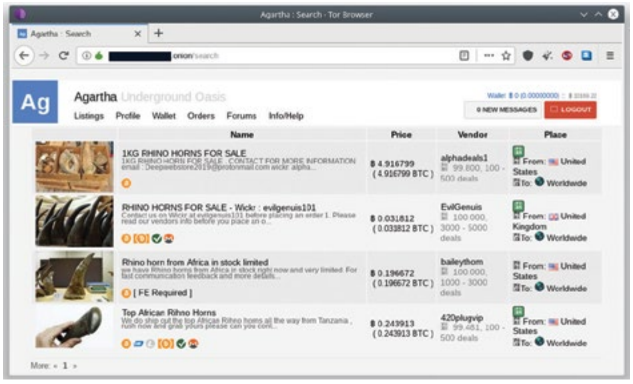


As illustrated in *Figure 25*, the amount of CSEM content on the Darkweb is growing rapidly. In fact, an analysis using text content comparison in 2019 found there were 776 unique websites sharing CSEM (approximately 5 per cent of the 15,353 active onion websites).[56] Although a lot of these websites are operating under different onion domain names, the content on many of them appeared to be identical.

12. Wildlife trade

With the expansion of trade, follows the appearance of illegal wildlife products on darknet markets. *Figure 26* shows rhino horn trade in 2019.

Figure 26. Illegal wildlife trade takes place in Darkweb marketplaces.*



Agartha : Search - Tor Browser

Agartha : Search

[redacted]onion/search

Agartha Underground Oasis

Listings Profile Wallet Orders Forums Info/Help

Wallet: ฿ 0 (0.00000000) :: ฿ [illegible]

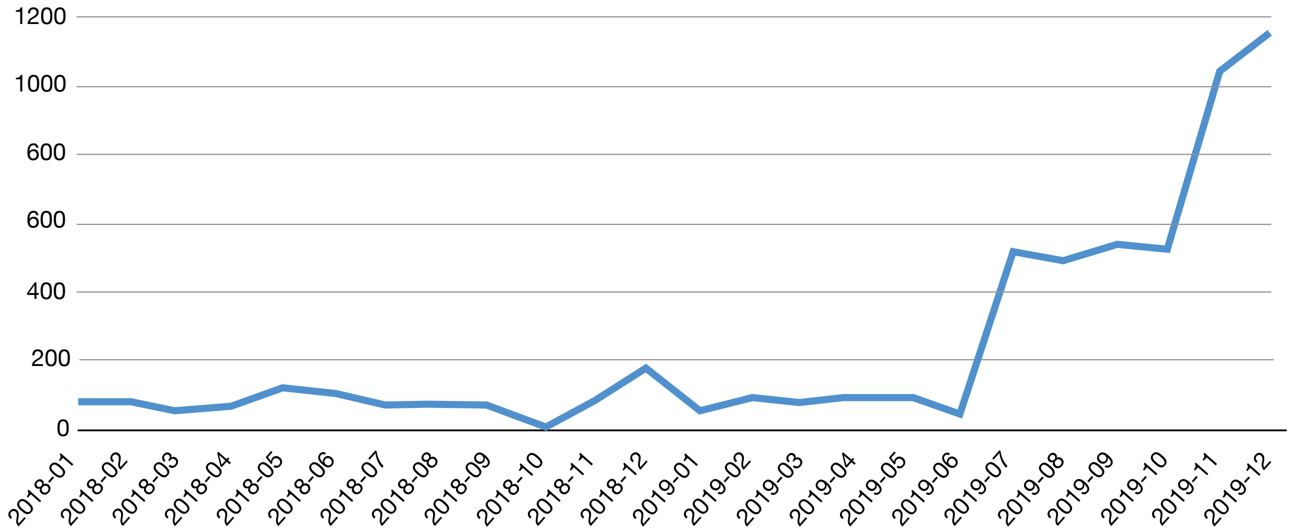
0 NEW MESSAGES LOGOUT

	Name	Price	Vendor	Place
	1KG RHINO HORNS FOR SALE 1KG RHINO HORN FOR SALE . CONTACT FOR MORE INFORMATION email : Deepwebstore2019@protonmail.com wickr: alpha...	฿ 4.916799 (4.916799 BTC)	alphadeals1 99.800, 100 - 500 deals	From: United States To: Worldwide
	RHINO HORNS FOR SALE - Wickr : evilgenuis101 Contact us on Wickr at evilgenuis101 before placing an order 1. Please read our vendors info before you place an o...	฿ 0.031812 (0.031812 BTC)	EvilGenuis 100.000, 3000 - 5000 deals	From: United Kingdom To: Worldwide
	Rhino horn from Africa in stock limited we have Rhino horns from Africa in stock right now and very limited. For fast communication feedback and more details... [FE Required]	฿ 0.196672 (0.196672 BTC)	baileythom 100.000, 1000 - 3000 deals	From: United States To: Worldwide
	Top African Rihno Horns We do ship out the top African Rihno horns all the way from Tanzania , rush now and grab yours please can you cont...	฿ 0.243913 (0.243913 BTC)	420plugvip 99.481, 100 - 500 deals	From: United States To: Worldwide

More: « 1 »

**Four different vendors selling rhino horns on the Agartha marketplace.*

Figure 27. Number of times "rhino horn" mentioned on the Darkweb (2018-2019).



Conclusion

While there is a paucity of data regarding Darkweb criminality targeting, and originating from, Southeast Asia, available information reveals that it does exist and is likely to grow in breadth and depth in the near-term. At the same time, COVID-19 has clearly confirmed that criminals will evolve their business models at pace in order to continue to make the greatest possible profit. States too must be enabled to rapidly assess, analyse and redirect operational resources to respond to evolving cyber threats.

It is essential that Southeast Asian countries take individual responsibility to address the overall political and policy issues raised in countering darknet cybercrime, but that they also invest rapidly in upskilling their criminal justice agencies. Darknet cybercrime is no longer an "unknown unknown" and requires dedication, expertise, specialist mentoring and financial resources to build the capabilities which will counter the threat. UNODC remains committed to supporting Southeast Asia with this vital work.

Appendices

A1: Darknet use in Southeast Asian countries

By using metrics provided by two of the darknets (Tor and I2P), it is possible to get an approximation of the number of users in each Southeast Asian country. These metrics provide a better understanding of user behaviour over time. It is important to note that criminality cannot be inferred from these metrics – they simply serve to paint a picture of darknet use.

Tor provides two useful metrics: relay users and bridge users. Relay users are any users in a particular country that are relaying Tor traffic. Bridge users are end-users that are blocked (for whatever reason) from accessing the Tor network directly. Bridge users do not act as relays.

I2P provides router information by country. Similar to Tor, users connect to the I2P network via a local software router. Routers receive and forward I2P traffic from other nodes on the I2P network. I2P retains the number of active routers per country for a maximum of one year.

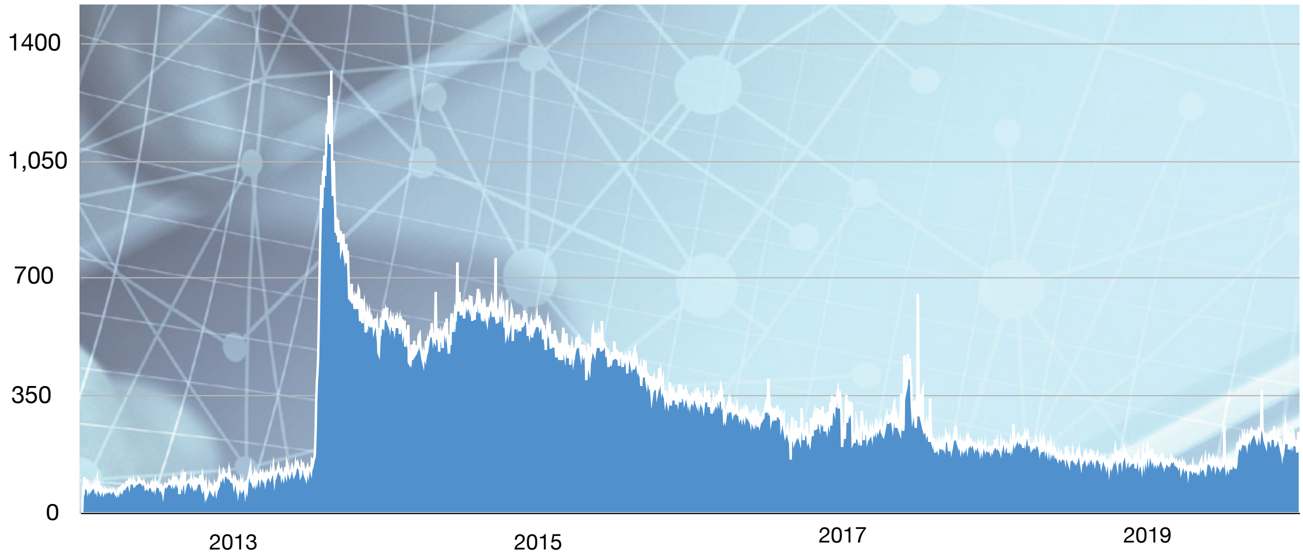
There are also other methods for users to connect to darknets which makes it difficult to attribute precise numbers of users to particular countries. For example, a user in country A could use a VPN or similar service to connect to country B. While appearing to be in country B, the user connects to the Tor network. Tor would register the user as connecting from country B. We must therefore infer that the number of users indicated in these network metrics may underrepresent the actual user numbers.

Below we give an overview of darknet users by country for Tor and I2P networks. In most graphs there is a huge spike in users in 2013 and 2018. Both of these spikes are likely caused by malware that connected infected systems to the Tor network.[57]

1. Brunei Darussalam

Brunei has a population of approximately 440,000.[58] Tor metrics (*Figure A1*) show that usage of Tor has dropped from around an average of 500 people per day connected over the last few years to an average of 250 people connected in 2020. Like many other countries, we see an increase in users in early 2020.

Figure A1. Tor users directly connected from Brunei (January 2012 to July 2020).



The Tor Project - https://metrics.torproject.org/

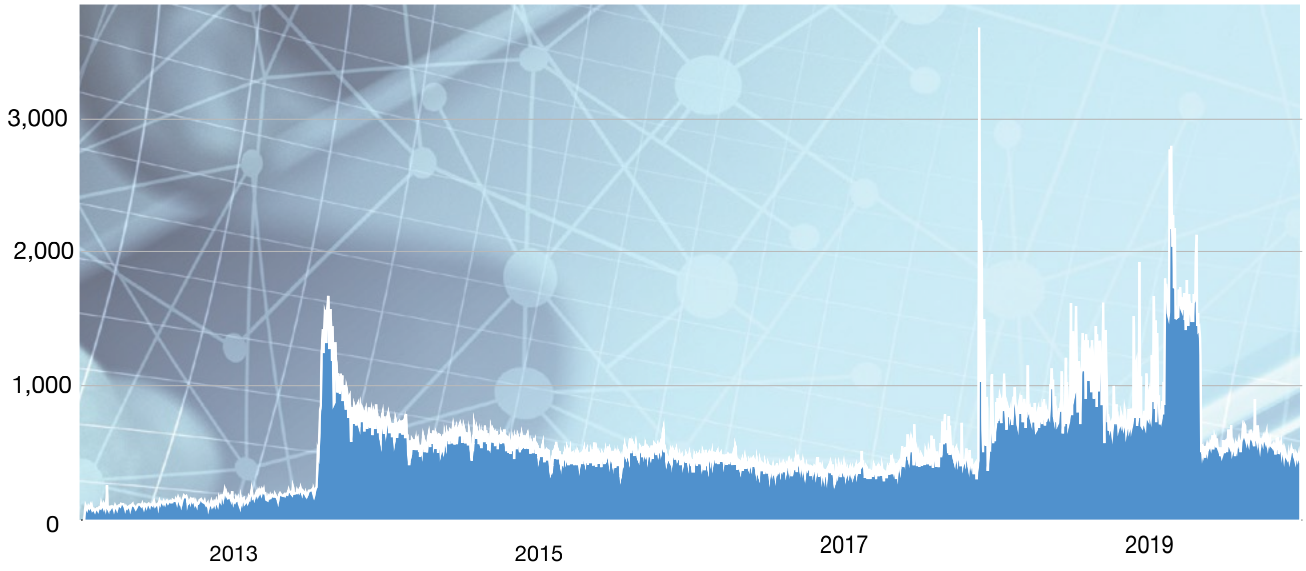
Tor bridge users also average around 10 connected users per day. Note that these could be the same users connecting and disconnecting from the network, or different users. 250 relay users and 10 bridge users should be considered the minimum possible total users.

There was no reported activity from Brunei on the I2P darknet from January 2019 to July 2020. This means I2P was not used directly.

2. Cambodia

Cambodia has a population of approximately 16.7 million.[59] Tor metrics (*Figure A2*) show that usage of Tor increased from an average of around 500 users per day in 2018 to an average of 2,500 users by the end of 2019. In early 2020, we see a drop back to a 500-user average. Such a fluctuation could be due to increased user awareness, or to do with a malware campaign or censorship event in the country.[60]

Figure A2. Tor users directly connected from Cambodia (January 2012 to July 2020).



The Tor Project - https://metrics.torproject.org/

In early 2018, we see a large increase in Tor bridge users from around a 10-user average to around a 700-user average. Since then, bridge users have steadily decreased, with around a 50-user average in 2020.

There was no reported activity from Cambodia on the I2P darknet from January 2019 to July 2020. This means I2P was not used directly.

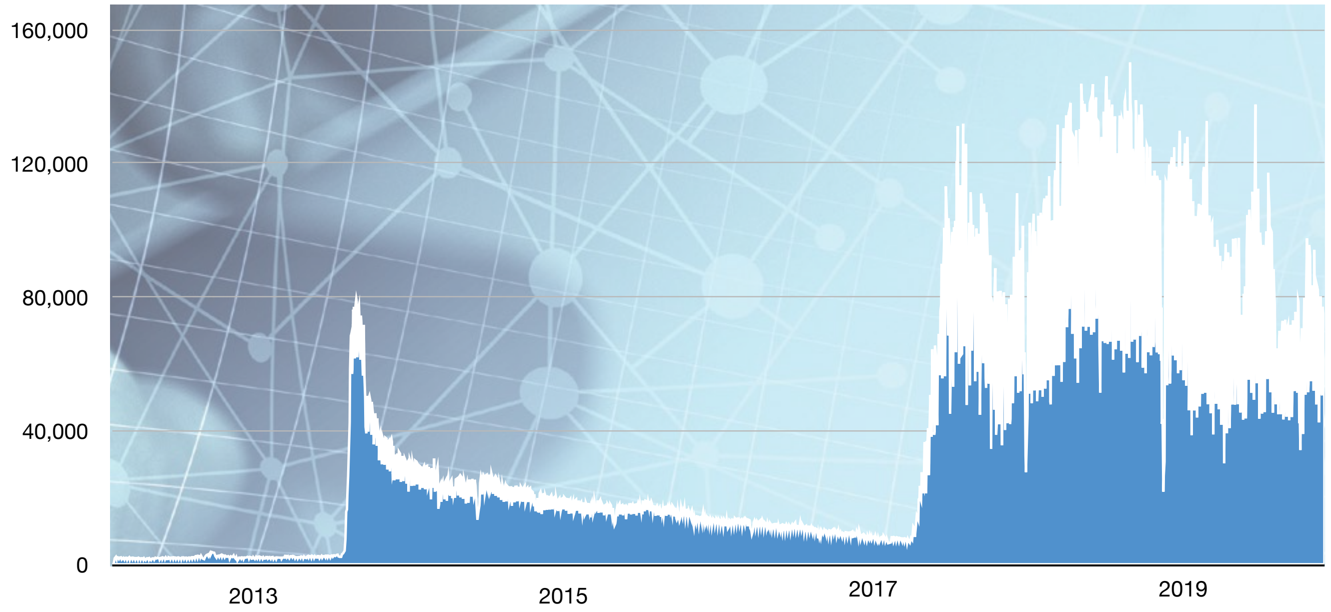
3. Indonesia

Indonesia has a population of approximately 274 million.[61] Tor metrics (*Figure A3*) show that usage of Tor increased from an average of around 10,000 users per day in late 2017 to an average of 125,000 users by the end of 2019. In early 2020, we see a drop back to a 75,000-user average.

In early 2018, we see a large increase in Tor bridge users from around a 100-user average to around a 12,500-user average. Bridge users have steadily decreased to an average of around 600 users in 2020.

Indonesia had approximately 150 I2P users in early 2019. That number dropped to around 25 users in early 2020, and then increased to a 50-user average between January and July 2020.

Figure A3. Tor users directly connected from Indonesia (January 2012 to July 2020).

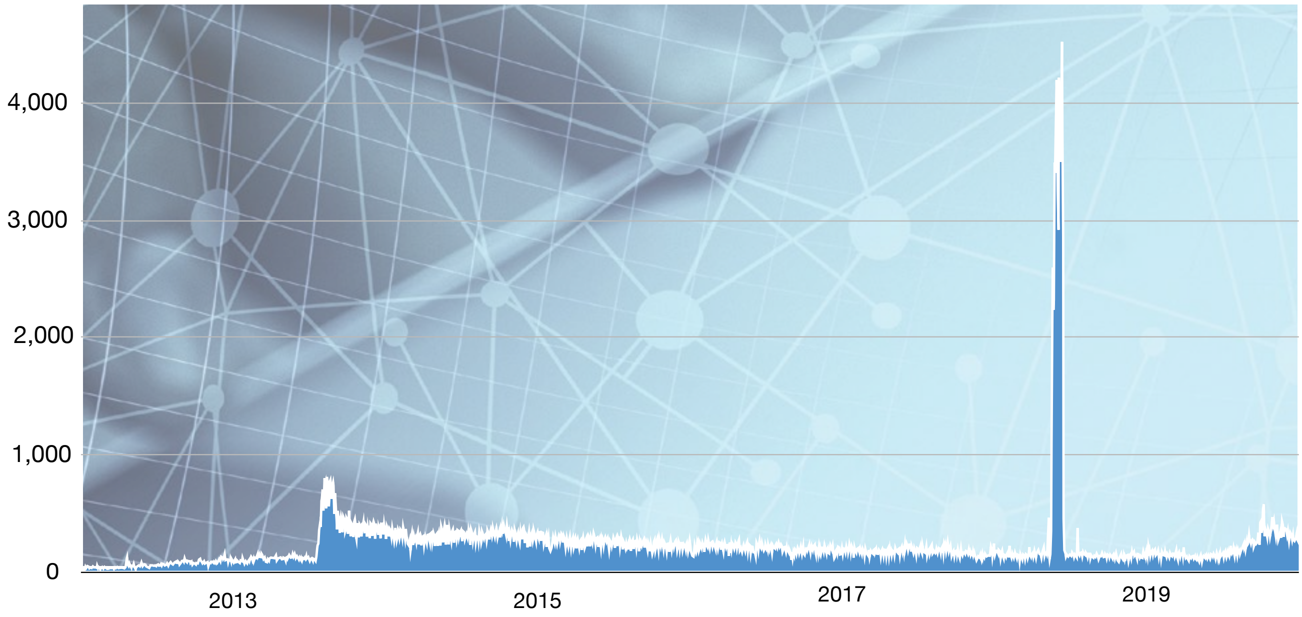


The Tor Project - https://metrics.torproject.org/

4. Lao PDR

Laos has a population of approximately 7.2 million.[62] Tor metrics (*Figure A4*) show that usage of Tor has largely remained steady from 2015 to 2020 at approximately a 250-user average, with a slight increase to a 500-user average since early 2020.

Figure A4. Tor users directly connected from Lao PDR (January 2012 to July 2020).



The Tor Project - https://metrics.torproject.org/

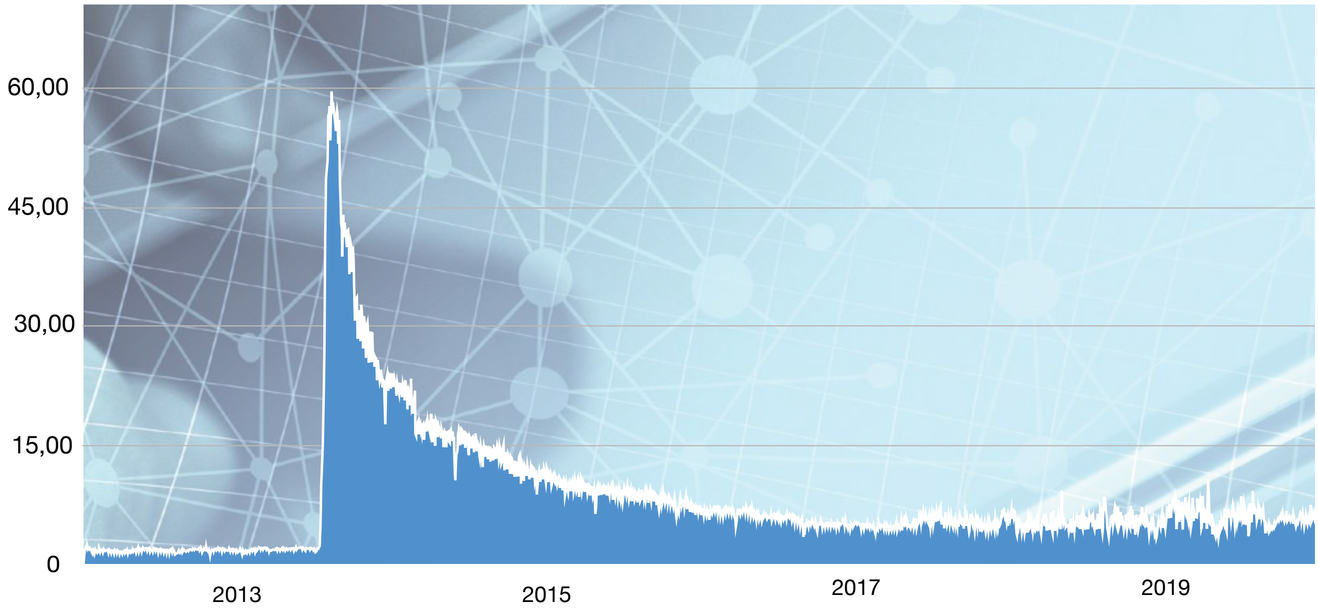
Similar to other countries, late 2018 saw a large increase in Tor bridge users. More recently, there has been a decline from a 400-user average to a 25-user average.

There was no reported activity from Laos on the I2P darknet from January 2019 to July 2020.

5. Malaysia

Malaysia has a population of approximately 32.4 million.[63] Tor metrics (*Figure A5*) show a sharp increase in users in 2013. The average number of users declined from 2013 to 2017, and then averaged around 5,000 users per day from 2017 to 2020.

Figure A5. Tor users directly connected from Malaysia (January 2012 to July 2020).



The Tor Project - https://metrics.torproject.org/

While Tor direct connections decreased, there was an increase in Tor bridge connections. Bridge connections peaked at around 800 users per day in mid-2018. From 2019 to 2020 average bridge users remained steady at around a 150-user average.

Malaysia maintained an average of around 85 users per day on the I2P network from January 2019 to July 2020. The number of users appears to have almost doubled since January 2020 from around 60 to around 100 users.

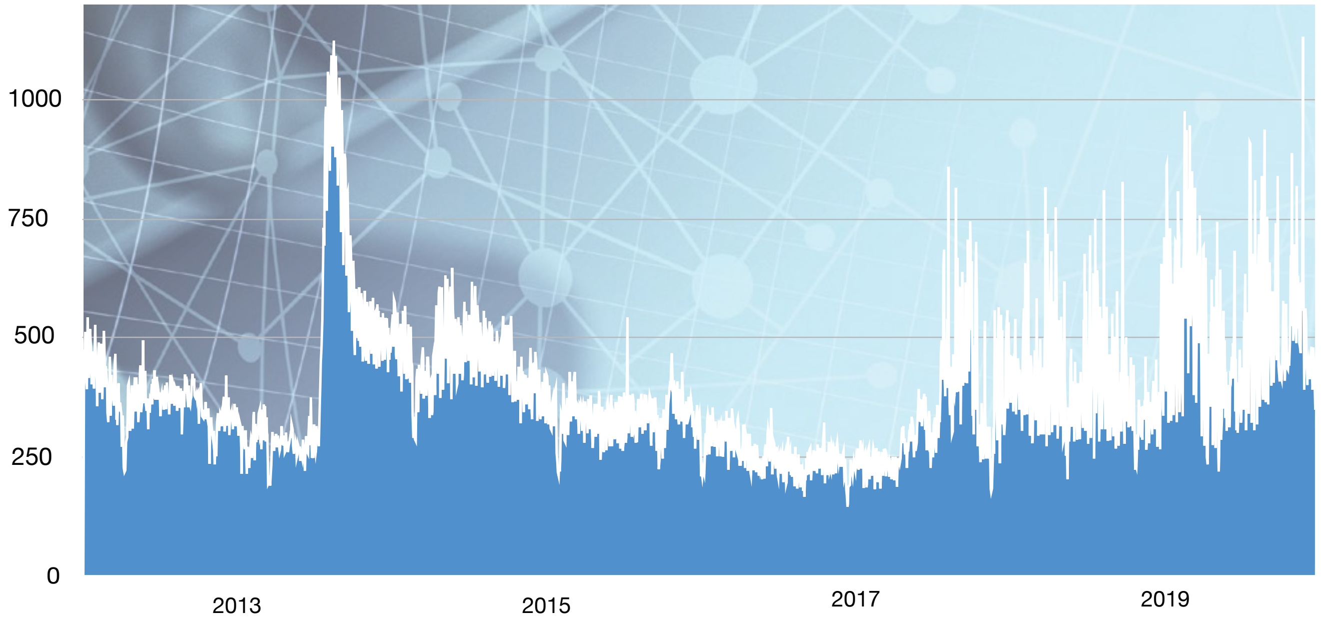
6. Myanmar

Myanmar has a population of approximately 54.5 million.[64] Tor metrics (*Figure A6*) show a sharp increase in users in mid-2013, gradually decreasing until mid-2017. From 2017 there has been a slight increase in average users, from around 200 per day to around 400 in 2020.

Like other countries, there was a large increase in Tor bridge users from mid-2018. Since then, Tor bridge users have declined from a 500-user average to a 15-user average.

There is no reported activity from Myanmar on the I2P darknet from January 2019 to July 2020.

Figure A6. Tor users directly connected from Myanmar (January 2012 to July 2020).



The Tor Project - https://metrics.torproject.org/

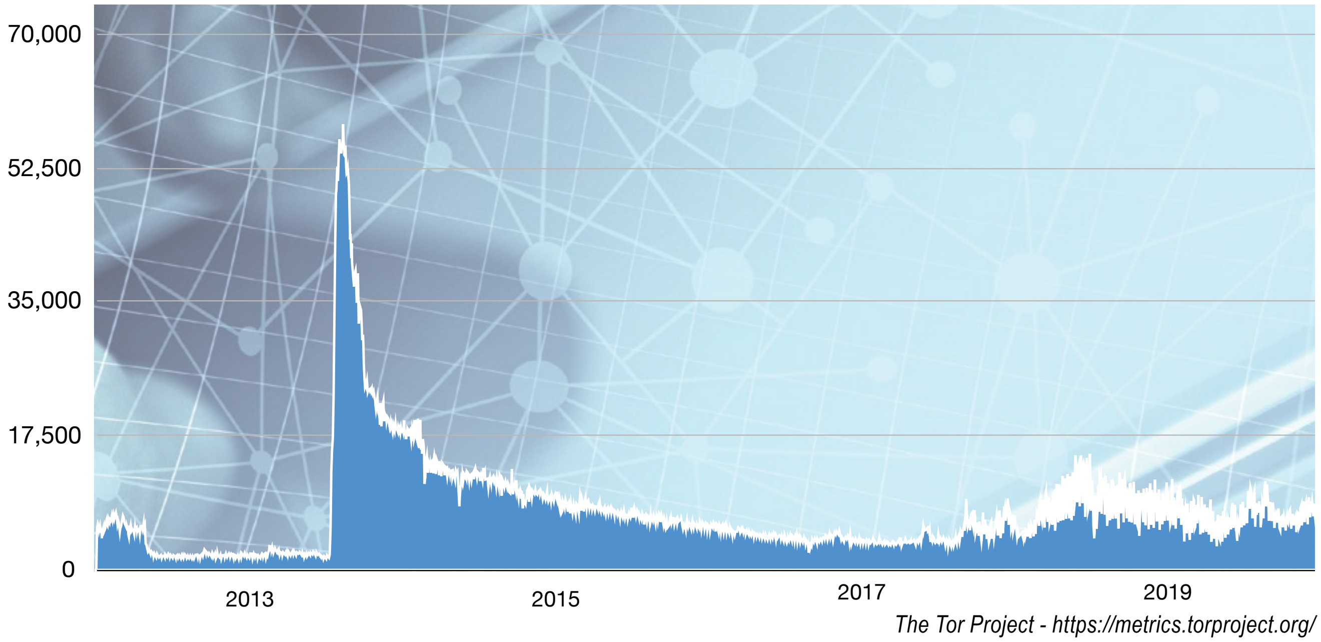
7. Philippines

The Philippines has a population of approximately 109.9 million.[65] Tor metrics (*Figure A7*) show a sharp increase in users in mid-2013 and then a decrease until 2017. From 2017 we see an increase in users from 5,000 to around 10,000 average users.

Similar to other countries, mid-2018 saw a large increase in Tor bridge users. Since then, Tor bridge users have declined from a 3,500-user average to a 250-user average.

From 2019 to July 2020, the Philippines had an average of 60 I2P users with a range from 30 to 90 users in that time.

Figure A7. Tor users directly connected from the Philippines (January 2012 to July 2020).

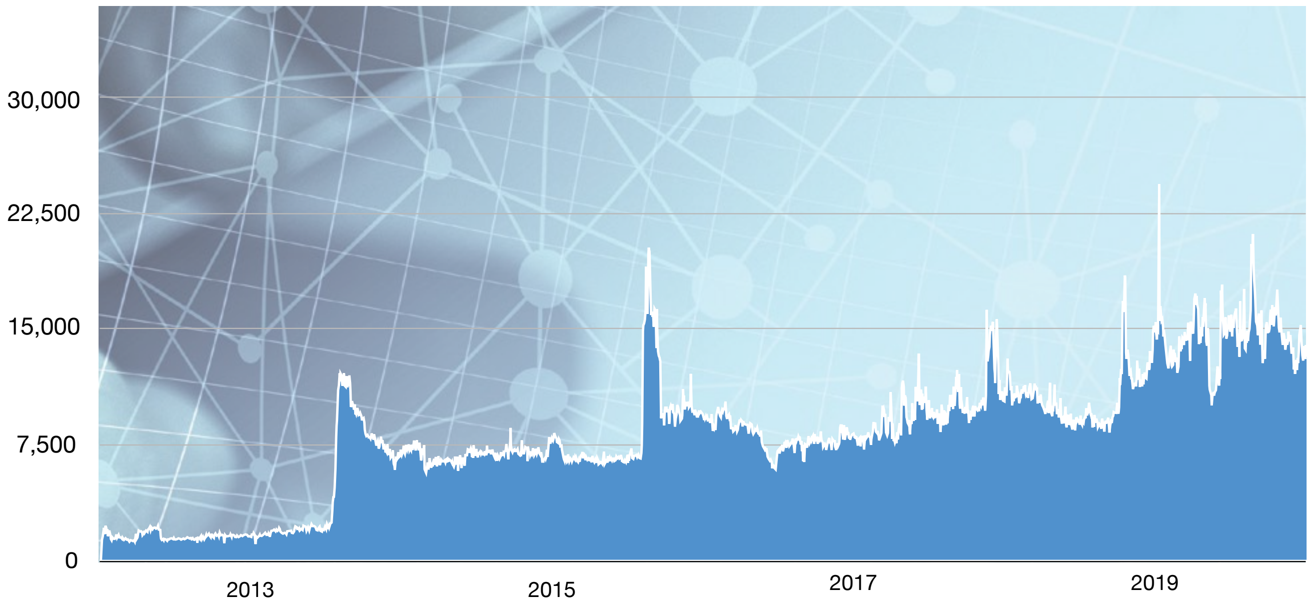


The Tor Project - https://metrics.torproject.org/

8. Singapore

Singapore has a population of approximately 5.8 million.[66] Tor metrics (*Figure A8*) show a fairly consistent increase in average Tor users from 2013, with average users increasing from 5,000 to 15,000 in July 2020.

Figure A8. Tor users directly connected from Singapore (January 2012 to July 2020).



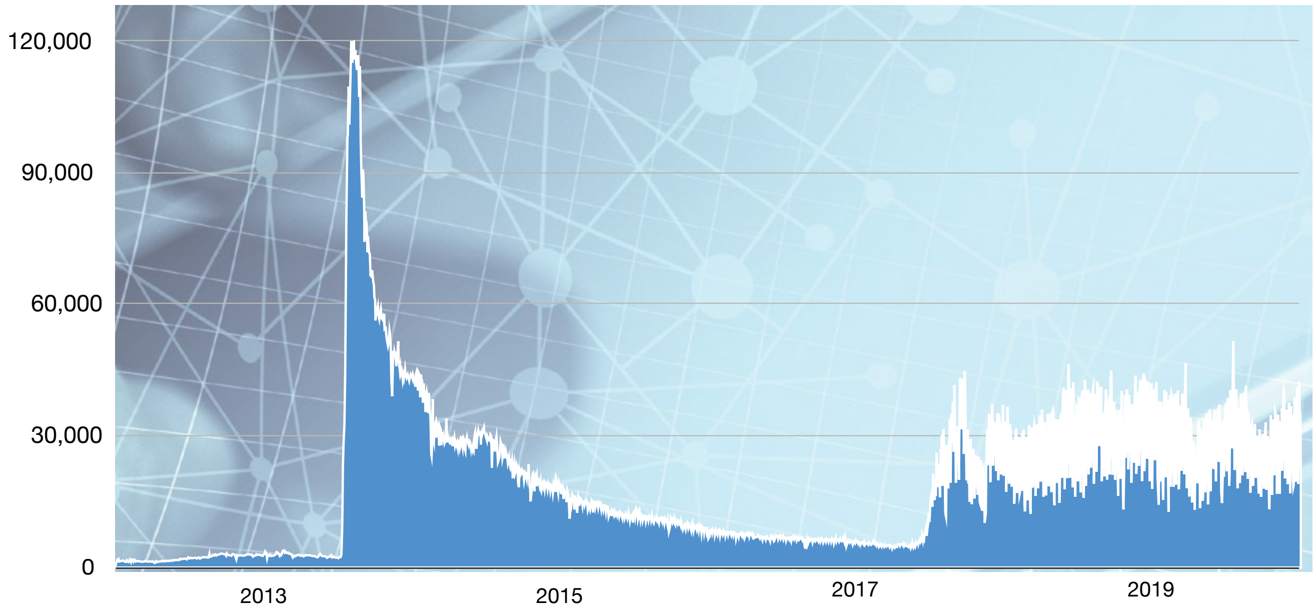
The Tor Project - https://metrics.torproject.org/

Similar to directly connected users, there has been a steady increase in Tor bridge users from 2014 to 2020, with an average of approximately 200 Tor bridge users in July 2020.

From 2019 to July 2020, Singapore had an increase of I2P users from 80 per day to 140. One increase happened in November 2019, and there has been another steady increase since January 2020.

9. Thailand

Figure A9. Tor users directly connected from Thailand (January 2012 to July 2020).



The Tor Project - https://metrics.torproject.org/

Thailand has a population of approximately 69.8 million.[67] Tor metrics (*Figure A9*) show a sharp increase in users in mid-2013 that steadily declines until late 2017. In 2018, we see an increase of users to about 25,000 that continues to increase slightly into 2020.

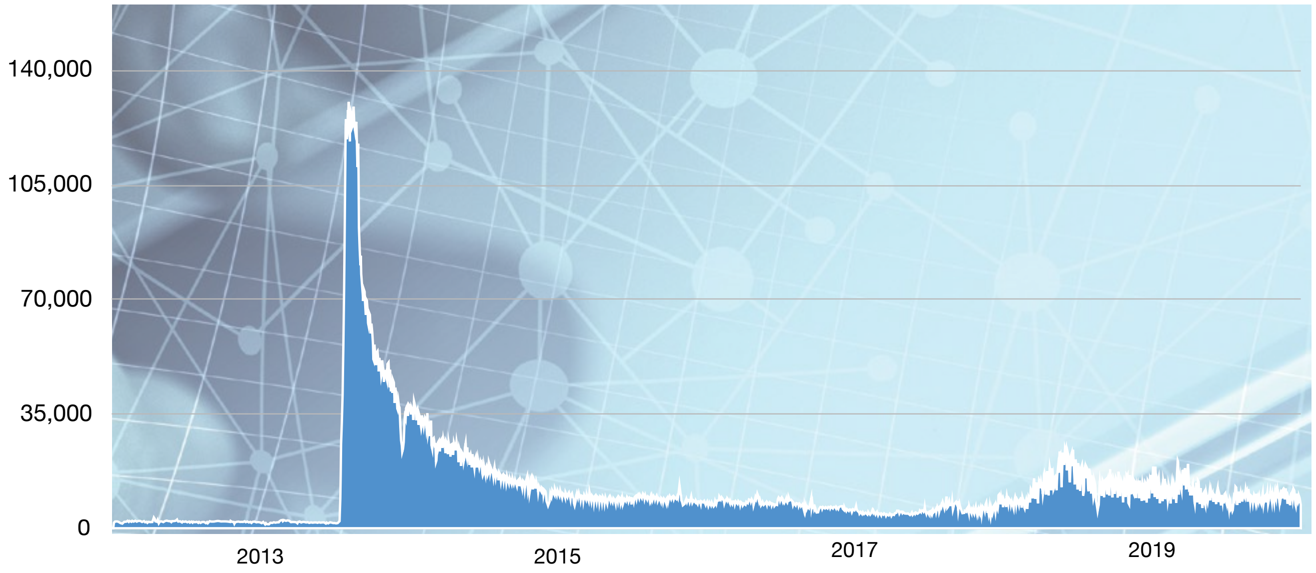
Tor bridge users peak in mid-2018 at around an average of 4,000 users per day. Bridge users decline until reaching an average of around 250 users in mid-2020.

From 2019 to July 2020, Thailand had an average of 65 I2P users. Users range from around 30 to 100 with the average number of I2P users increasing since early 2020.

10. Vietnam

Vietnam has a population of approximately 97.5 million.[68] Tor metrics (*Figure A10*) show a sharp increase in users in mid-2013 and then a decline until 2017. The average number of users increased from approximately 6,000 in 2017 to around 12,000 in mid-2020.

Figure A10. Tor users directly connected from Vietnam (January 2012 to July 2020).



The Tor Project - https://metrics.torproject.org/

Tor bridge users peaked in mid-2018 at an average of around 15,000 users per day. Bridge users then declined until reaching an average of around 250 users in mid-2020.

From 2019 to July 2020, I2P users declined from an average of around 200 users to an average of approximately 30 users in mid-2020.

A2: Darkweb technical analysis

Darkweb data, including data from 2015–2020 was analysed for this report. This produced some 200 million pages of Darkweb data covering websites, information-leaking platforms, marketplaces, discussion forums, interest groups and published data breaches. Data was collected using crawlers that followed links and stored all the information they observed. Darkweb websites, especially marketplaces and discussion forums, require bypassing various obstacles, such as CAPTCHA's, paywalls, scripted behaviour detection and vouching.

The data collection process involves crawling onion websites inside the Tor and I2P networks.

A Darkweb harvesting system requires:[69]

1. onion link acquisition from the deep and Darkweb,
2. a proxy system where several Tor clients are connected to the Tor network,
3. crawlers and spiders which access the HTTP web content available on Tor,
4. logic to bypass authentication and robot detections,
5. duplicate information detection,
6. text information extraction from the documents,
7. text data saving to the index.

The data collection system automatically performs link acquisition from the content it finds and the continuous crawling process follows new links. Furthermore, there is a cycle to re-check crawled URL addresses in case there is new content available.

The proxy system is a collection of Tor software clients and HTTP load-balancing proxy which selects a Tor client for each onion domain name.

Some content is only available behind a login and robot detection (CAPTCHA). If this content is gathered, a separate bypass system is needed, which can log in and solve robot detection puzzles.

A3: Technical analysis results

After web crawling to extract and transform unstructured data from the Darkweb, this structured data was stored on a database.[70] In this step, connections and behaviour were studied.[71,72]

Data mining identifies information that could be attached or linked to a specific country or to an organization that resides in that particular country. There are two sets of identifiers: country-specific identifiers and organization-specific identifiers.

Country-specific identifiers:

1. IP addresses
2. Domain names
3. Most common names per country
4. Phone numbers with country code
5. Social security numbers
6. Languages
7. GPS-coordinates from image metadata

Organization-specific identifiers:

1. Disclosure of sensitive information
2. Discussions
3. Marketplace activity
4. Financial information
5. Exposed credentials (passwords)
6. Personally identifiable information
7. Hacker group targeting
8. Attacks and previous compromises.

Figure A11. Mapped IP addresses mentioned in the Tor network from Southeast Asia.

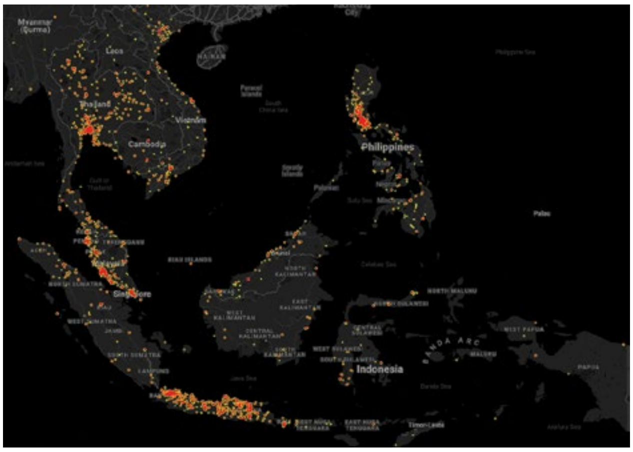
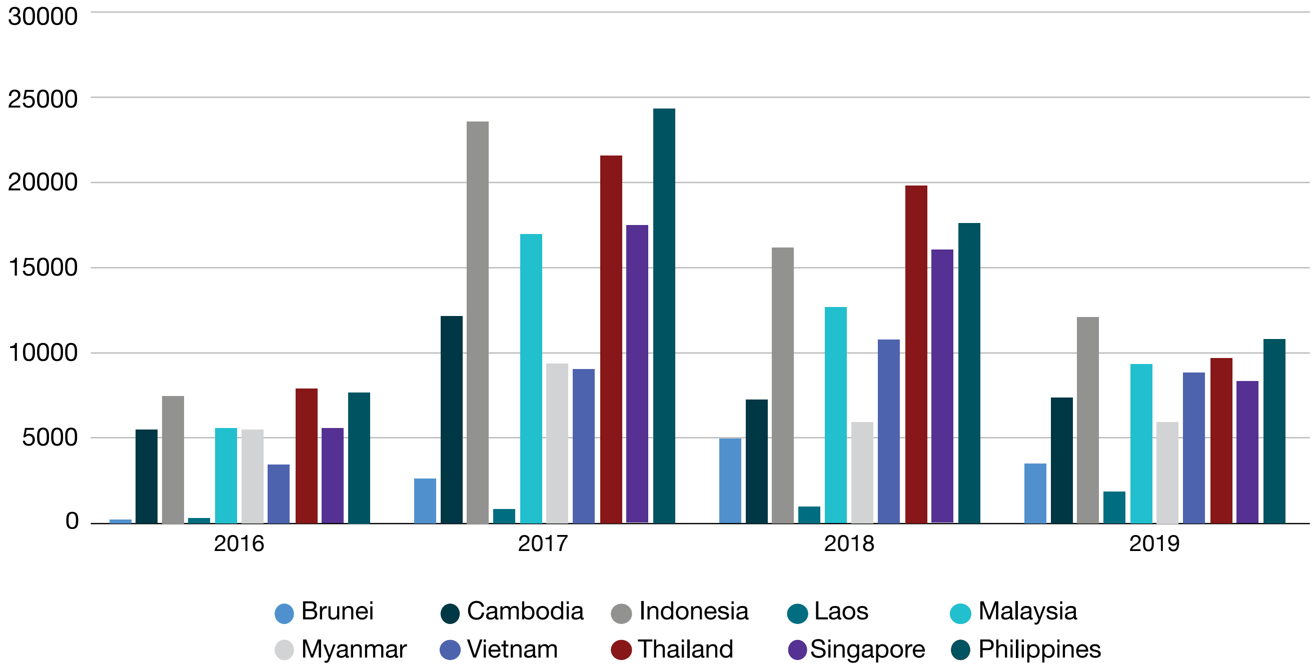


Figure A12. Countries mentioned in discussion forums on the Darkweb.



Like IP addresses, phone numbers located on the Darkweb are in many cases linked to victims of criminal activity. These phone numbers most likely belong to the victims of data breaches and are often used by criminals for illicit purposes.

Overall, languages, phone numbers, national ID numbers and much more can provide some information about a location. The Darkweb was searched for any country-specific identifiers. These country-specific identifiers often show up in forum discussions, database leaks, and other information posted on the Darkweb. As such, much of the location-specific data is leaked victim data from specific countries. *Table A1* shows a number of related identifiers found on the Darkweb listed by country. While this type of assessment does *not* allow premises, inferences or assumptions to be made about Darkweb-related crime/victims, it is potentially useful as a general indicator of the amount of Darkweb-related activity that a country is facing.

Indonesia had the most national ID numbers leaked on forums. Assuming that these are real, it suggests that there are many victims of data breaches in the country. Such information could be used to scam, defraud or attack the victims, their families or associated organizations. This data could, however, be used by the Indonesian Government to create an incident response and risk mitigation strategy.

Some of the images shared on the Darkweb contain image metadata with GPS locations (i.e. the location where the photograph was taken). Typically, users and web services remove this information. However, some images still contained this location information and *Figure A13* shows where these images were taken in Southeast Asia. This potentially reveals locations related to associated criminal activity.

Table A1. Quantities of sensitive data identifiers found on the Darkweb listed by country.

	Cambodia	Indonesia	Vietnam	Thailand	Philippines	Malaysia	Singapore	Laos	Brunei	Myanmar
Language			21439	7945	15714					
Phone numbers	18391	11685	7480	8022	907	581	582	4	10	60
National ID numbers		16073				47	571			
Market items with country mentioned	2198600	2232779	814943	2222729	2213301	2215632	2224558	784133	2189850	1444910
IPv4 addresses	5832	94390	43657	55458	21143	50481	135631	3526	1586	4062
Domains	4339	128202	44681	86079	98837	113120	75261	218173	1723	4870
Country mentioned in CSE context	16506	417	661	5139	968	167	19281	125	4	105
Country mentioned in forums	32382	59669	32199	59311	60812	44790	47929	3934	11323	25396

The Tor network is a volunteer overlay network (a network layered on top of another), consisting of more than 7,000 relays. A Tor relay operator is not necessarily responsible for the traffic passing through the relay. In most of the world, it is perfectly legal to install a voluntary Tor network relay. Anyone can operate a node by installing Tor software in the router mode and starting to route Tor traffic through a server.

As shown in *Figure A14*, there are a total of 106 Tor relays in Southeast Asian countries (9 in Indonesia, 12 in Malaysia, 1 in the Philippines, 69 in Singapore, 6 in Thailand, and 9 in Vietnam). The data illustrates that Singapore is an attractive location to operate these relays. This is probably because cheap virtual machines to operate relays are easily accessible, and Internet infrastructure is well developed.

Figure A13. Locations where images still containing metadata were taken.

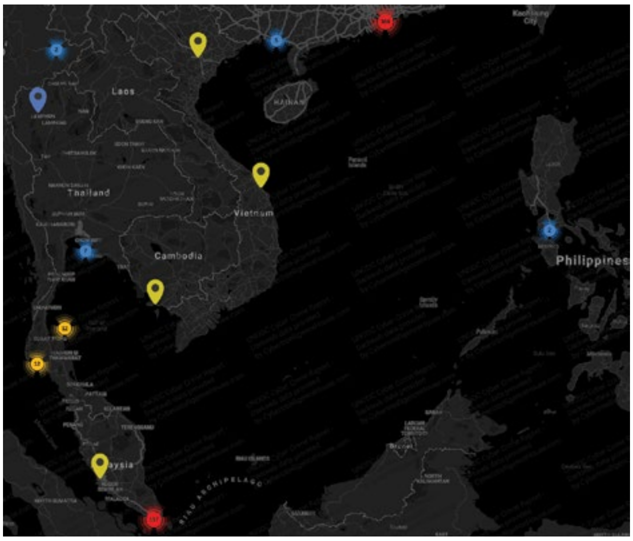


Figure A14. Tor relays in Southeast Asian countries.

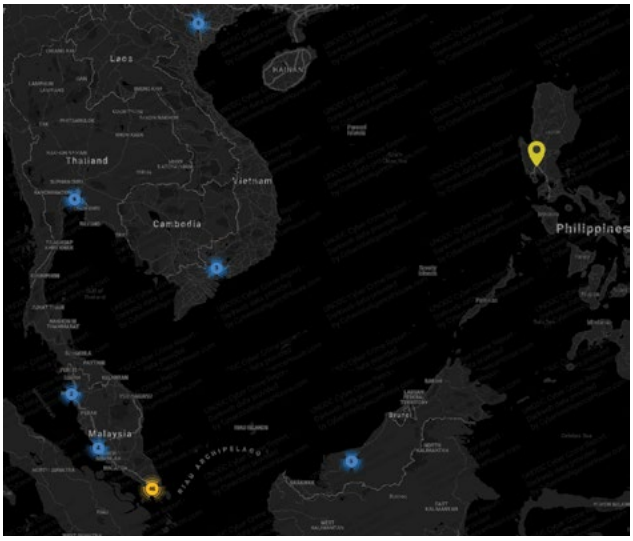
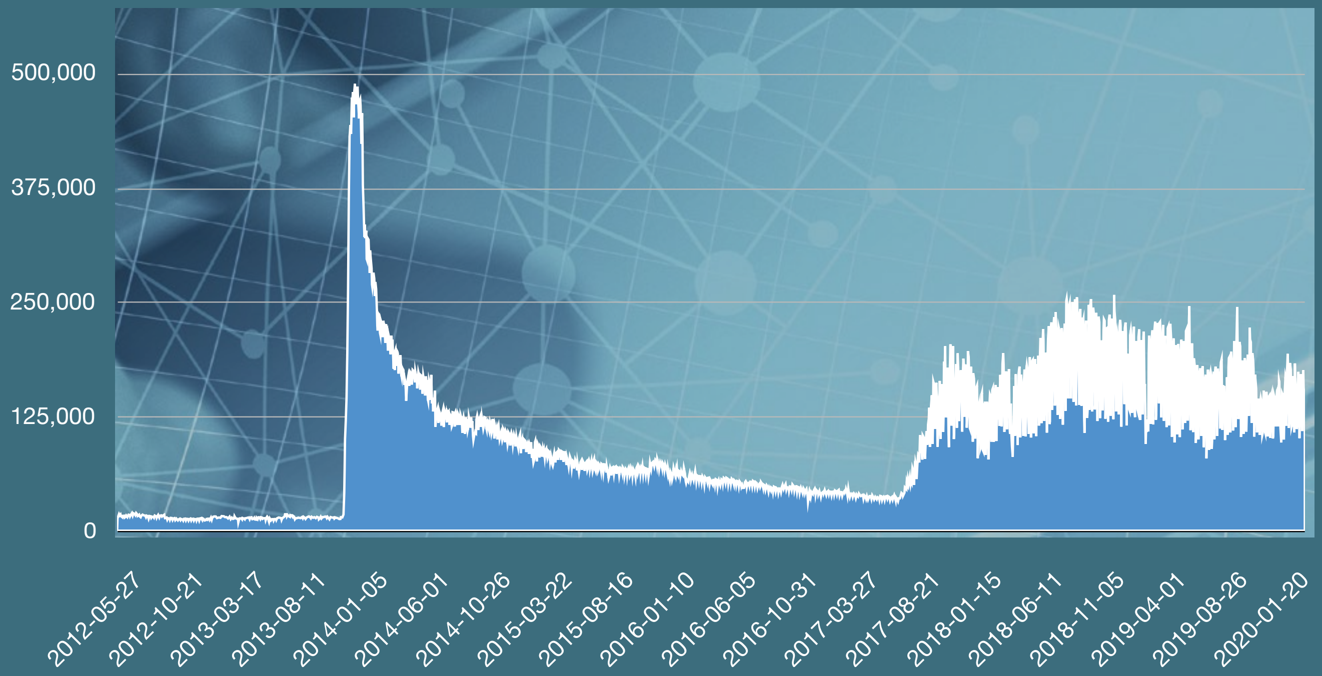


Figure A15 shows an overall increase in the popularity of the Tor network in Southeast Asian countries since 2017, although the reasons for this are unclear.

Figure A15. Southeast Asian users connected to the Tor network (May 2012-June 2020).



Glossary

Term		Definition
Anonymous file-sharing networks		Networks that allow sharing files and other data between network users. They are designed to make it difficult to track the origin of both the sender and receiver. They are often Peer to Peer (P2P) networks with anonymity functions. Still, centralised sharing functions are possible with the assistance of additional anonymity overlay networks, such as Tor.
Anonymous web browsing		Anonymous web browsing allows a user to visit websites without allowing anyone to gather information about which sites the user visited. Anonymizing tools attempt to prevent browser fingerprinting and hide the visitor's IP address. These services typically use a proxy server to process each HTTP request. When the user requests a web page by clicking a hyperlink or typing a URL into their browser, the service retrieves and displays the information using a server it controls. The remote server (where the requested web page resides) receives information about the anonymous web surfing service in place of the user's information. Source: https://www.lawweb.in/2012/10/use-of-annonymizer-for-better-privacy.html
APT	Advanced Persistent Threat	As the name 'advanced' suggests, an advanced persistent attack (APT) uses continuous, clandestine, and sophisticated hacking techniques to gain and keep access to a system for a prolonged period, with potentially destructive consequences. Because of the level of effort needed to carry out such an attack, APTs are usually levelled at high-value targets, such as nation-states and large corporations, with the ultimate goal of stealing information over a long period, rather than merely 'dipping in' and leaving quickly, as many black hat hackers do during lower-level cyber assaults. Source: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats
Asynchronous forum		An Internet-based electronic communication environment, which permits users to post messages for some or all the members to view. Messages remain posted until a forum moderator removes them. Asynchronous refers to the static nature of the environment. Postings are done one at a time, anonymously or not, and offer a written electronic record of the communications conducted. Source: https://www.igi-global.com/dictionary/peer-learning-social-interactions-asynchronous/1688
Bandwidth		Bandwidth is the quantity of data transmission (Rate) from one device to another device on the network (including the Internet). Source: https://www.lifewire.com/what-is-bandwidth-2625809

Term		Definition
Botnet		'Botnets' (a term derived from the words 'robot' and 'network') consist of a network of interconnected, remote-controlled computers generally infected with malicious software that turns the infected systems into so-called 'bots', 'robots', or 'zombies'. Source: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
CaaS	Crime-as-a-service model	The Crime-as-a-Service (CaaS) business model is used when a criminal group offers some or all parts of criminal actions as a service to other criminal groups. This allows criminal groups to specialize in particular aspects of crime while still gaining benefit from the overall crime (often with less risk). CaaS includes a wide range of commercial services that facilitate almost any type of cybercrime. Criminals are freely able to procure such services, such as the rental of botnets, denial-of-service attacks, malware development, data theft and password cracking, to commit crimes themselves. Source: https://www.europol.europa.eu/activities-services/main-reports/Internet-organised-crime-threat-assessment-iocta-2014
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart	CAPTCHA is a method used to protect websites against spam. The goal is to stop interactive websites from being spammed by filtering out automatically generated input. Source: https://www.ionos.com/digitalguide/online-marketing/online-sales/captcha-codes-and-images-for-spam-protection/
Censorship circumvention		Internet censorship circumvention is the use of various methods and tools to bypass Internet censorship. Internet censorship, for example, may monitor and block certain website requests. Censorship circumvention may attempt to hide or obfuscate the request, or bypass the monitor by tunnelling the request through a non-censored computer. Source: https://ssd.eff.org/en/module/understanding-and-circumventing-network-censorship
Clearnet		Clearnet is the 'regular' Internet, which can be discovered using link-crawling and DNS query techniques. These techniques are used by typical search engines such as Google, Bing and Yahoo. It is the unencrypted non-dark, non-Tor Internet. Source: Europol,2017 "Drugs and the darknet – perspectives for enforcement research and policy" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf

Term		Definition
Cryptocurrencies		Cryptocurrencies are electronic tokens generated by networks of computers to replace traditional currencies. The electronic tokens in digital currency have value based on the exchange of conventional currencies and commodities for the tokens through special Internet exchanges, such as BitPay. These exchanges function somewhat like PayPal but are not associated with that company. Source: https://www.kaspersky.com/resource-center/definitions/what-is-bitcoin https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
CSE	Child Sexual Exploitation	The sexual maltreatment of children which consists of, but is not limited to, child sexual abuse, child sexual assault, child sexual abuse material, early or forced marriage, as well as the production of images of such abuse and the sharing of those images online. Source: https://www.icmec.org/resources/glossary/ https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation
CSEM	Child Sexual Exploitation Material	Child Sexual Exploitation Material is any material that visually depicts a child engaged in real or simulated sexually explicit conduct. This can also include any material generally depicting a child in a sexual manner. Source: https://www.ecpat.org/what-we-do/online-child-sexual-exploitation/ https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation
Cyberattack		A cyberattack occurs when cybercriminals attempt to inflict reputational damage or harm to a business or person, or theft of valuable data. Cyberattacks can target individuals, groups, organizations, or governments. Source: https://us.norton.com/Internetsecurity-emerging-threats-cyberattacks-on-the-rise-what-to-do.html
Crypto-mixers		A cryptocurrency mixing service is a service offered to mix potentially identifiable cryptocurrency funds with other non-related funds, to obscure the trail back to the fund's original source. Source: https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-bestmixerio-taken-down

Term		Definition
Darknet/ Darkweb		A relatively covert part of the World Wide Web that is not indexed by search engines, and can only be accessed by specialized software such as the Tor browser. Source: https://iaca-dark web-tools.com/dictionary/ A network, built on top of the Internet, that is purposefully hidden; it has been designed specifically for anonymity. Unlike the deep web, the darknet is accessible only with special tools and software — browsers and other protocol beyond direct links or credentials. Source: Europol,2017 "Drugs and the darknet – perspectives for enforcement research and policy" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
Data breach		A data breach exposes confidential, sensitive, or protected information to an unauthorized person. The data in a data breach is viewed and/or shared without permission. Source: https://www.kaspersky.com/resource-center/definitions/data-breach
Deep web		A section of the Internet that is not indexed by search engines. The deep web contains such things as intranet, banking information, membership sites, as well as the Darkweb. The only way to access the deep web is by conducting a search within a particular website. For example, government databases and libraries contain huge amounts of deep web data. Source: https://iaca-dark web-tools.com/dictionary/ Source: Europol,2017 "Drugs and the darknet – perspectives for enforcement research and policy" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
DDoS	Distributed Denial of Service Attack	A Distributed Denial of Service attack attempts to block legitimate users from accessing some service by using a distributed network of systems to overwhelm the resources of a target. Source: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Term		Definition
DoS	Denial of Service Attack	A Denial of Service attack attempts to block legitimate users from accessing some service. For example, by overwhelming a targeted website to the point of crashing it or making it too busy to be accessible. A successful Denial of Service attack can cripple any entity that relies on its online presence by rendering their website virtually useless. Source: https://evestigate.com/cyber-crime-hacker-terms-to-know/
Doxing		Doxing is searching for and publishing private or identifying information about an individual or their alias without their knowledge or permission. Source: https://iaca-dark web-tools.com/dictionary/
E-commerce websites		Websites that allow individuals to buy and sell goods and services online.
Encryption		The process of converting data to an unrecognisable or 'encrypted' form. It is commonly used to protect sensitive information, including files, storage devices and data transfers, so that only authorised parties can view it. Source: Europol,2017 "Drugs and the darknet – perspectives for enforcement research and policy" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
Escrow payment system		A third-party payment system, often times a marketplace, that holds funds while a transaction is made between the buyer and seller. Source: https://iaca-dark web-tools.com/dictionary/
Exit scam		A scam in which a darknet market administrator or a vendor shuts down operations while stealing as much money as possible from users and/or buyers in the process. Source: Europol,2017 "Drugs and the darknet – perspectives for enforcement research and policy" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf

Term		Definition
Forgery		An act of making a false object so that it may be accepted as genuine. Source: https://legal-dictionary.thefreedictionary.com/forgery Forgery typically require two necessary elements: (i) the alteration or manipulation of computer data, and (ii) a specific intent to use the data as if they were authentic. Alternatively, countries may extend the definition of the object of traditional forgery. A number of countries in Europe, for example, have covered computer-related forgery by extending the definition of 'document' to include computer data. Other countries apply general provisions to computer-related forgery without amending legislation if traditional provisions of forgery can be interpreted to include digital documents, signatures and data. Source: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
Hacktivism		Hacktivism is the intentional access to systems, websites, and/or data without authorisation or having exceeded authorised access, and/or the intentional interference with the functioning and/or accessibility of systems, websites, and data without authorisation or having exceeded authorised access, in order to effect social or political change. Source: Maras, Marie-Helen. (2016). Cybercriminology. Oxford University Press.
Hidden services		A feature provided by the Tor network that enables a user to anonymously host content and services on the Darkweb. Source: Europol,2017 "Drugs and the darknet – perspectives for enforcement research and policy" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
HTTPS	Hypertext Transfer Protocol Secure	This transfer protocol is the language in which the web client – usually the browser – and the web server communicate with each other. HTTPS is the version of the transfer protocol that uses encrypted communication. Source: https://www.ionos.com/digitalguide/hosting/technical-matters/what-is-https/

Term		Definition
Identity theft – computer related		Refers to acts involving the transfer, possession, or use, of means of identification of another person stored in computer data, without right, with the intent to commit, aid or abet any unlawful criminal activity. This is the case, for example, if a perpetrator, without right, obtains driving licence information from a computer system and either sells such data or uses it to hide his true identity when committing a crime. Source: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
I2P	Invisible Internet Project	Software that provides access to a network that allows for anonymous browsing, messaging, and file transfers. Source: https://iaca-dark web-tools.com/dictionary/ An alternative to Tor hidden services. It is an overlay network based on passing messages between routers using garlic routing with a distributed hash table for a global directory of available routers. Source: Europol,2017 "Drugs and the darknet – perspectives for enforcement research and policy" https://www.europol.europa.eu/sites/default/files/documents/drugs_and_the_darknet_-_td0417834enn.pdf
IP address	Internet protocol address	The address of a connected device in an IP network (TCP/IP network), which is the worldwide standard for both local-network and Internet connections. Every desktop and laptop computer, server, modem, router, smartphone, tablet and smart TV is assigned an IP address when connected to the network. Every IP packet traversing an IP network contains a source IP address and a destination IP address. Source: https://www.pcmag.com/encyclopedia/term/ip-address

References

1 https://www.unodc.org/unodc/en/frontpage/2019/June/world-drug-report-2019_-35-million-people-worldwide-suffer-from-drug-use-disorders-while-only-1-in-7-people-receive-treatment.html

2 Cyber Intelligence House. (2020) Dark web intelligence data. https://cyberintelligencehouse.com/

3 Ibid.

4 D. Moore and T. Rid, "Cryptopolitik and the Darknet," Survival, vol. 58, no. 1, pp. 7–38, Jan. 2016, doi: 10.1080/00396338.2016.1142085.

5 G. Owen and N. Savage, "The Tor Dark Net," 2015.

6 J. Nurmi, "Understanding the Usage of Anonymous Onion Services Empirical Experiments to Study Criminal Activities in the Tor Network," 2019.

7 J. Nurmi and M. S. Niemelä, "Tor de-anonymisation techniques," in 11th International Conference, NSS, 2017.

8 "Category:Anonymous file sharing networks - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Category:Anonymous_file_sharing_networks. [Accessed: 07-Jan-2020].

9 K. Loesing, "Privacy-enhancing Technologies for Private Services," 2009.

10 K. S. Bauer, "Improving Security and Performance in Low Latency Anonymous Networks," 2011.

11 R. G. Jansen, "Privacy Preserving Performance Enhancements for Anonymous Communication Networks," 2012.

12 D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding Routing Information," in International Workshop on Information Hiding, 1996.

13 R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router," in Proceedings of the 13th USENIX Security Symposium, 2004.

14 https://www.torproject.org

15 Cyber Intelligence House. (2020) Dark web intelligence data. https://cyberintelligencehouse.com/

16 "Tor Metrics." [Online]. Available: https://metrics.torproject.org.

17 Ibid.

18 Ibid.

19 C. Dion-Schwarz, D. Manheim, and P. Johnston, Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats. RAND Corporation, 2019.

20 K. Kruithof, J. Aldridge, D. Hétu, M. Sim, E. Dujso, and S. Hoorens, Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands. RAND Corporation, 2016.

21 Ibid.

22 "AlphaBay, the Largest Online 'Dark Market,' Shut Down | OPA | Department of Justice." [Online]. Available: https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down. [Accessed: 10-Mar-2020].

23 "Dark web drug bust: Three arrested for Singapore connect | Cities News, The Indian Express." [Online]. Available: https://indianexpress.com/article/cities/delhi/dark-web-drug-bust-3-arrested-for-singapore-connect-6276649/. [Accessed: 10-Mar-2020].

24 "Australian Peter Scully given life sentence for human trafficking, rape in Philippines, reports say - ABC News (Australian Broadcasting Corporation)." [Online]. Available: https://www.abc.net.au/news/2018-06-14/australian-peter-scully-convicted-in-philippines/9868958. [Accessed: 10-Mar-2020].

25 Ibid.

26 "Alleged pedophilia 'dark web' site bust by Interpol brings arrests in Thailand, US and Australia and rescue of 50 children today - CBS News." [Online]. Available: https://www.cbsnews.com/news/pedophilia-ring-dark-web-interpol-operation-blackwrist-thailand-us-australia-children-rescued/. [Accessed: 10-Mar-2020].

27 "Paedophile Richard Huckle 'murdered' in prison | UK news | The Guardian." [Online]. Available: https://www.theguardian.com/uk-news/2019/oct/14/paedophile-richard-huckle-found-dead-in-prison. [Accessed: 10-Mar-2020].

28 Ibid.

29 "US indicts Russian cybercrime Dark Web market 'Infraud Organization' suspect Sergey Medvedev, arrested in Thailand - CBS News." [Online]. Available: https://www.cbsnews.com/news/us-russia-cybercrime-dark-web-market-suspect-sergey-medvedev-thailand/. [Accessed: 10-Mar-2020].

30 Tor Metrics. https://metrics.torproject.org/

31 Roderic Broadhurst, Matthew Ball, Chuxuan Jessie Jiang. (2020) Availability of COVID-19 related products on Tor darknet markets. https://www.aic.gov.au/sites/default/files/2020-05/sb24_availability_of_covid-19_related_products_on_tor_darknet_markets.pdf

[32] CISOMAG. (2020) Over 230K Indonesian COVID-19 Patients' Records Exposed on Darknet. https://cisomag.eccouncil.org/indonesian-patients-data-leak/

[33] PWC. (2020) Why has there been an increase in cyber security incidents during COVID-19?. https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html

[34] Microsoft Threat Intelligence. (2020) Open-sourcing new COVID-19 threat intelligence. https://www.microsoft.com/security/blog/2020/05/14/open-sourcing-covid-threat-intelligence/

[35] Dumrongkiat Mala. (2020) ‹Dark net› a godsend for paedophiles. https://www.bangkokpost.com/thailand/general/1860539/dark-net-a-godsend-for-paedophiles

[36] Thomas Brewster. (2020) Child Exploitation Complaints Rise 106% To Hit 2 Million In Just One Month: Is COVID-19 To Blame?. https://www.forbes.com/sites/thomasbrewster/2020/04/24/child-exploitation-complaints-rise-106-to-hit-2-million-in-just-one-month-is-covid-19-to-blame/#15c5a0204c9c

[37] Michael Kapilkov. (2020) Criminals Are Selling COVID-19 Infected Blood on the Darknet. https://cointelegraph.com/news/criminals-are-selling-covid-19-infected-blood-on-the-darknet

[38] Ibid.

[39] M. J. Barratt, "Silk Road: Ebay for drugs," Addiction, vol. 107, no. 3, pp. 683–683, Mar. 2012, doi: 10.1111/j.1360-0443.2011.03709.x.

[40] M. C. van Hout and T. Bingham, "'Surfing the Silk Road': A study of users' experiences," International Journal of Drug Policy, vol. 24, no. 6, pp. 524–529, Nov. 2013, doi: 10.1016/j.drugpo.2013.08.011.

[41] M. J. Barratt, "Silk Road: Ebay for drugs," Addiction, vol. 107, no. 3, pp. 683–683, Mar. 2012, doi: 10.1111/j.1360-0443.2011.03709.x.

[42] M. C. van Hout and T. Bingham, "'Surfing the Silk Road': A study of users' experiences," International Journal of Drug Policy, vol. 24, no. 6, pp. 524–529, Nov. 2013, doi: 10.1016/j.drugpo.2013.08.011.

[43] N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace," Proceedings of the 22nd international conference on World Wide Web, Jul. 2013.

[44] J. Martin, "Lost on the Silk Road: Online drug distribution and the 'cryptomarket,'" Criminology & Criminal Justice, vol. 14, no. 3, pp. 351–367, Jul. 2014, doi: 10.1177/1748895813505234.

[45] J. Nurmi and M. S. Niemelä, "Tor de-anonymisation techniques," in 11th International Conference, NSS, 2017.

[46] J. Aldridge and D. Décary-Hétu, "Cryptomarkets: The Darknet As An Online Drug Market Innovation," 2015.

[47] J. Nurmi, "Understanding the Usage of Anonymous Onion Services Empirical Experiments to Study Criminal Activities in the Tor Network," 2019.

[48] J. Aldridge and D. Décary-Hétu, "Cryptomarkets: The Darknet as an Online Drug Market Innovation," 2015.

[49] K. Masson and A. Bancroft, "'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets," International Journal of Drug Policy, vol. 58, pp. 78–84, 2018.

[50] G. Owen and N. Savage, "Empirical analysis of Tor hidden services," IET Information Security, vol. 10, no. 3, pp. 113–118, May 2016, doi: 10.1049/iet-ifs.2015.0121.

[51] A. Biryukov, I. Pustogarov, and R. P. Weinmann, "Trawling for tor hidden services: Detection, measurement, deanonymization," in Proceedings - IEEE Symposium on Security and Privacy, 2013, pp. 80–94, doi: 10.1109/SP.2013.15.

[52] J. Aldridge and D. Décary-Hétu, "Cryptomarkets: The Darknet as an Online Drug Market Innovation," 2015.

[53] K. Masson and A. Bancroft, "'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets," International Journal of Drug Policy, vol. 58, pp. 78–84, 2018.

[54] "Payment Fraud | Crime areas | Europol." [Online]. Available: https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud. [Accessed: 18-May-2020].

[55] Ibid.

[56] Cyber Intelligence House. (2020) Dark web intelligence data. https://cyberintelligencehouse.com/

[57] Dan Goodin. (2013) Sudden spike of Tor users likely caused by one "massive" botnet. Ars Technica. https://arstechnica.com/information-technology/2013/09/sudden-spike-of-tor-users-likely-caused-by-one-massive-botnet/

[58] United Nations. (2019) World Population Prospects 2019. https://population.un.org/wpp/

[59] Ibid.

60 Dan Goodin. (2013) Sudden spike of Tor users likely caused by one "massive" botnet. Ars Technica. https://arstechnica.com/information-technology/2013/09/sudden-spike-of-tor-users-likely-caused-by-one-massive-botnet/

61 United Nations. (2019) World Population Prospects 2019. https://population.un.org/wpp/

62 Ibid.

63 Ibid.

64 Ibid.

65 Ibid.

66 Ibid.

67 Ibid.

68 Ibid.

69 A. Biryukov, I. Pustogarov, and R. P. Weinmann, "Trawling for tor hidden services: Detection, measurement, deanonymization," in Proceedings - IEEE Symposium on Security and Privacy, 2013, pp. 80–94, doi: 10.1109/SP.2013.15.

70 M. Wesam, A. Nabki, E. Fidalgo, E. Alegre, and I. de Paz, "Classifying Illegal Activities on Tor Network Based on Web Textual Contents," 2017.

71 "Tor Metrics." [Online]. Available: https://metrics.torproject.org.

72 E. Çalışkan, T. Minárik, and A.-M. Osula, "Technical and Legal Overview of the Tor Anonymity Network Technical and Legal Overview of the Tor Anonymity Network," 2015.

United Nations Office on Drugs and Crime (UNODC)
Regional Office for Southeast Asia and the Pacific
United Nations Building, 3rd floor, Block B
Rajadamnern Nok Avenue
Bangkok 10200, Thailand
Website: https://www.unodc.org/southeastasiaandpacific
Twitter: @UNODC__SEAP

Global Programme on Cybercrime
Vienna International Centre
P.O. Box 500, A-1400 Vienna, Austria.
Website: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
Twitter: @UN__Cyber

UNODC would like to thank the Government of Japan for funding this research.

UNODC
United Nations Office on Drugs and Crime