

Below the Surface:
Exploring
the Deep
Web

Dr. Vincenzo Ciancaglini, Dr. Marco Balduzzi, Robert McArdle, and Martin Rösler
Forward-Looking Threat Research Team

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

Deep Web 101

7

The state of the
Deep Web

35

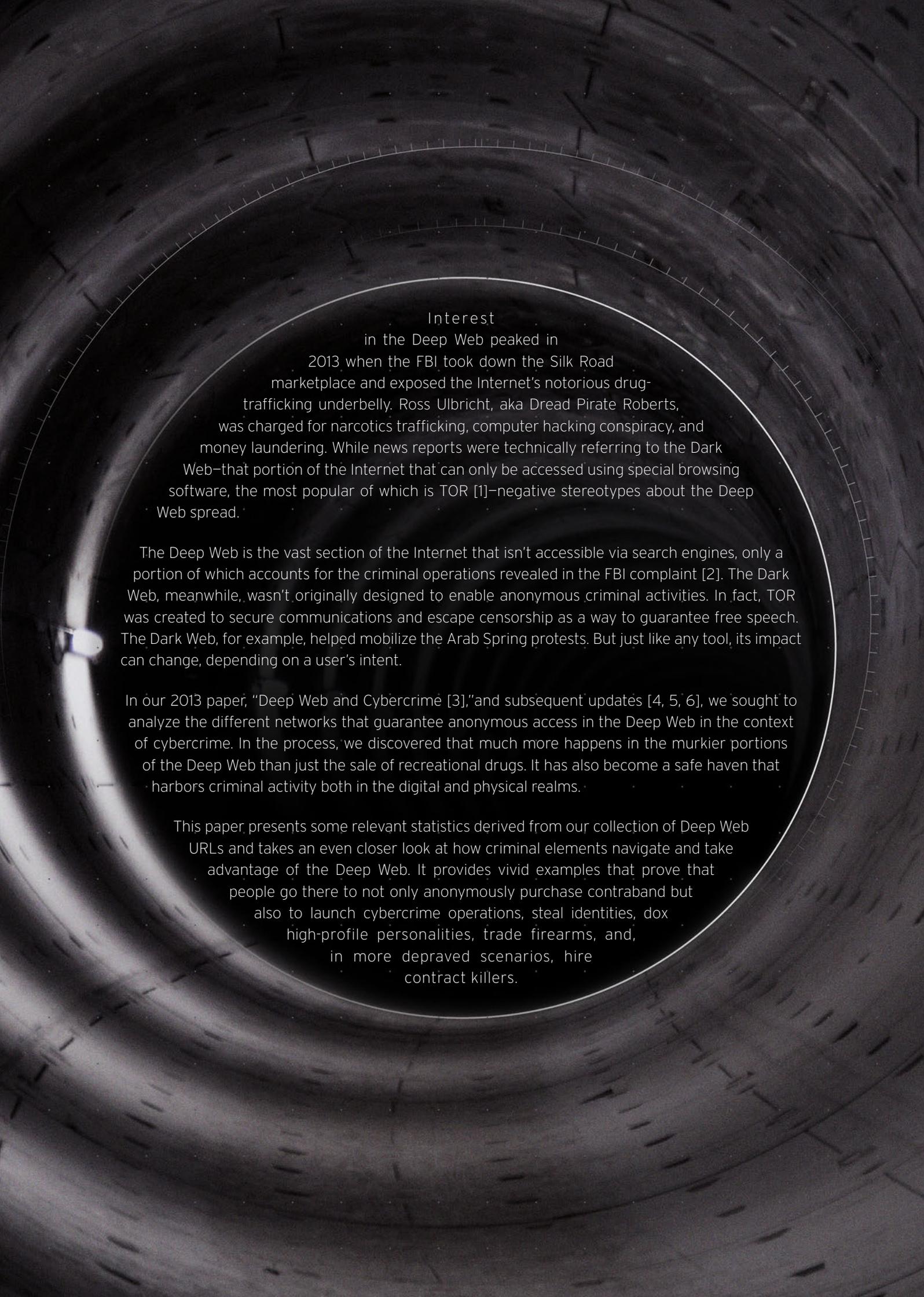
The Deep Web
and the real world

39

The future of the
Deep Web

41

Conclusion



Interest
in the Deep Web peaked in
2013 when the FBI took down the Silk Road
marketplace and exposed the Internet's notorious drug-
trafficking underbelly. Ross Ulbricht, aka Dread Pirate Roberts,
was charged for narcotics trafficking, computer hacking conspiracy, and
money laundering. While news reports were technically referring to the Dark
Web—that portion of the Internet that can only be accessed using special browsing
software, the most popular of which is TOR [1]—negative stereotypes about the Deep
Web spread.

The Deep Web is the vast section of the Internet that isn't accessible via search engines, only a portion of which accounts for the criminal operations revealed in the FBI complaint [2]. The Dark Web, meanwhile, wasn't originally designed to enable anonymous criminal activities. In fact, TOR was created to secure communications and escape censorship as a way to guarantee free speech. The Dark Web, for example, helped mobilize the Arab Spring protests. But just like any tool, its impact can change, depending on a user's intent.

In our 2013 paper, "Deep Web and Cybercrime [3]," and subsequent updates [4, 5, 6], we sought to analyze the different networks that guarantee anonymous access in the Deep Web in the context of cybercrime. In the process, we discovered that much more happens in the murkier portions of the Deep Web than just the sale of recreational drugs. It has also become a safe haven that harbors criminal activity both in the digital and physical realms.

This paper presents some relevant statistics derived from our collection of Deep Web URLs and takes an even closer look at how criminal elements navigate and take advantage of the Deep Web. It provides vivid examples that prove that people go there to not only anonymously purchase contraband but also to launch cybercrime operations, steal identities, dox high-profile personalities, trade firearms, and, in more depraved scenarios, hire contract killers.

SURFACE WEB

SECTION I

Deep Web 101

DEEP WEB

Dynamic web pages

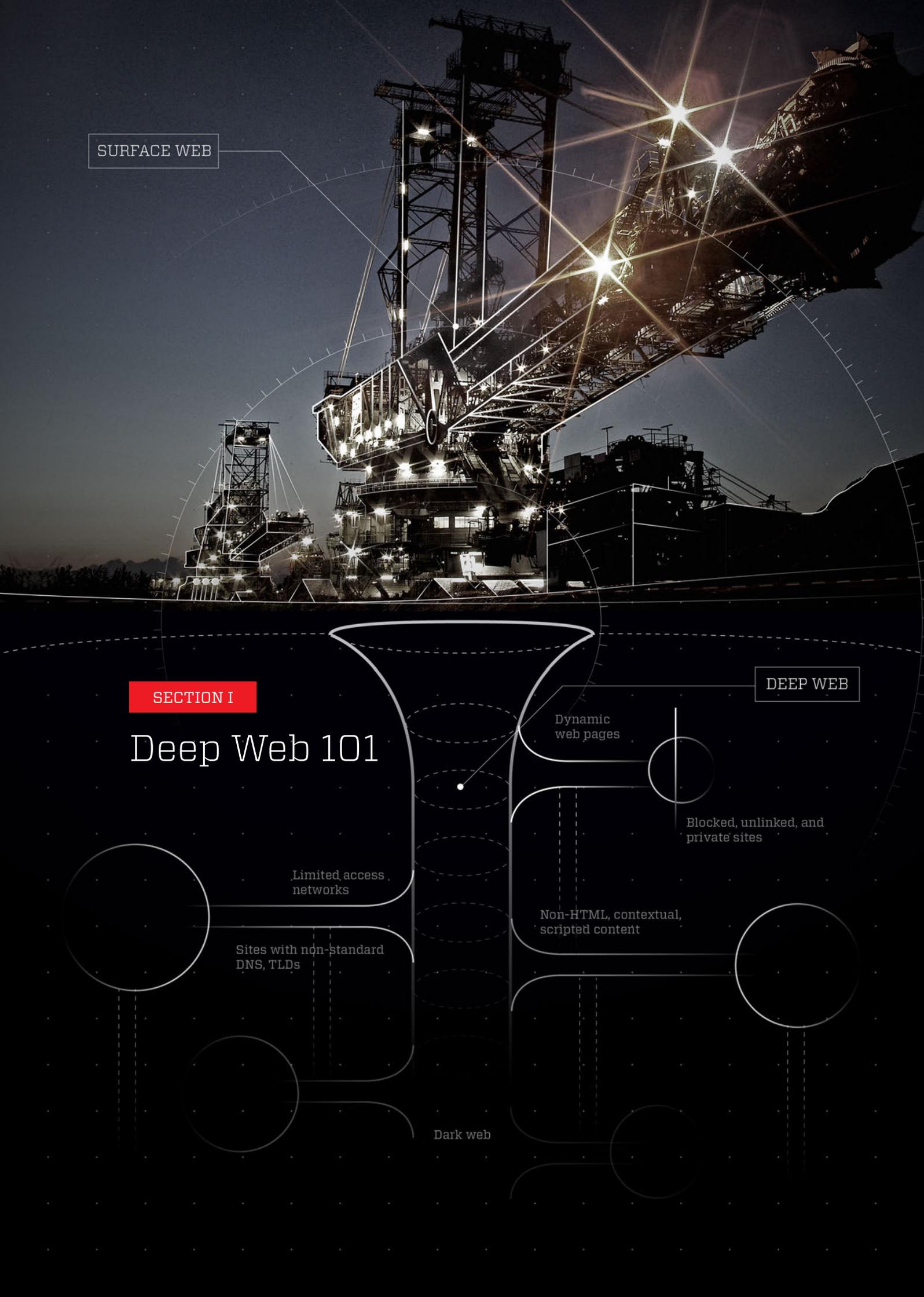
Blocked, unlinked, and private sites

Non-HTML, contextual, scripted content

Limited access networks

Sites with non-standard DNS, TLDs

Dark web



Deep Web 101

What is the Deep Web?

The Deep Web refers to any Internet content that, for various reasons, can't be or isn't indexed by search engines like Google. This definition thus includes dynamic web pages, blocked sites (like those that ask you to answer a CAPTCHA to access), unlinked sites, private sites (like those that require login credentials), non-HTML/-contextual/-scripted content, and limited-access networks.

Limited-access networks cover all those resources and services that wouldn't be normally accessible with a standard network configuration and so offer interesting possibilities for malicious actors to act partially or totally undetected by law enforcers. These include sites with domain names that have been registered on Domain Name System (DNS) roots that aren't managed by the Internet Corporation for Assigned Names and Numbers (ICANN) and, hence, feature URLs with nonstandard top-level domains (TLDs) that generally require a specific DNS server to properly resolve. Other examples are sites that registered their domain name on a completely different system from the standard DNS, like the .BIT domains we discussed in “Bitcoin Domains [7]”. These systems not only escape the domain name regulations imposed by the ICANN; the decentralized nature of alternative DNSs also makes it very hard to sinkhole these domains, if needed.

Also under limited-access networks are darknets or sites hosted on infrastructures that require the use of specific software like TOR to access. Much of the public interest in the Deep Web lies in the activities that happen inside darknets.

Unlike other Deep Web content, limited-access networks are not crawled by search engines though not because of technical limitations. In fact, gateway services like tor2web offer a domain that allows users to access content hosted on hidden services.

While the popular imagery for the Deep Web is an iceberg, we prefer to compare it to a subterranean mining operation in terms of scale, volatility, and access. If anything above ground is part of the “searchable Internet,” then anything below it is part of the Deep Web—inherently hidden, harder to get to, and not readily visible.

What are the uses of the Deep Web?

A smart person buying recreational drugs online wouldn't want to type related keywords into a regular browser. He/She will need to anonymously go online using an infrastructure that will never lead interested parties to his/her IP address or physical location. Drug sellers wouldn't want to set up shop in an online location whose registrant law enforcement can easily determine or where the site's IP address exist in the real world, too.

There are many other reasons, apart from buying drugs, why people would want to remain anonymous or set up sites that can't be traced back to a physical location or entity. People who want to shield their communications from government surveillance may require the cover of darknets. Whistleblowers may want to share vast amounts of insider information to journalists without leaving a paper trail. Dissidents in restrictive regimes may need anonymity in order to safely let the world know what's happening in their country.

On the flip side, people who want to plot the assassination of a high-profile target will want a guaranteed but untraceable means. Other illegal services like selling documents such as passports and credit cards also require an infrastructure that guarantees anonymity. The same can be said for people who leak other people's personal information like addresses and contact details.

The Surface Web versus the Deep Web

When discussing the Deep Web, it's impossible for the "Surface Web" not to pop up. It's exactly the opposite of the Deep Web—that portion of the Internet that conventional search engines can index and standard web browsers can access without the need for special software and configurations. This "searchable Internet" is also sometimes called the "clearnet."

The Dark Web versus the Deep Web

Much confusion lies between these two, with some outlets and researchers freely interchanging them. But the Dark Web is not the Deep Web; it's only part of the Deep Web. The Dark Web relies on darknets or networks where connections are made between trusted peers. Examples of Dark Web systems include TOR, Freenet, or the Invisible Internet Project (I2P) [8].

Taking on the mining tunnel metaphor, the Dark Web would be the deeper portions of the Deep Web that require highly specialized tools or equipment to access. It lies deeper underground and site owners have more reason to keep their content hidden.

The background is a dark, circular tunnel with a grid overlay. The grid consists of several concentric circles and radial lines, creating a target-like pattern. On the left side, there is a bright light source, possibly a flashlight, illuminating the tunnel wall. The overall atmosphere is mysterious and technical.

SECTION II

The state of the
Deep Web

The state of the Deep Web

Many studies and reports have been written on the various activities that occur in the Deep Web, including several of ours [3, 4, 5, 6]. Reading these, you may think that the vast majority of sites on the Deep Web are dedicated to selling illegal drugs and weapons but that isn't the whole story. While there are, of course, sites dedicated to drugs and weapons, a huge chunk of Deep Web sites are dedicated to more mundane topics—personal or political blogs, news sites, discussion forums, religious sites, and even radio stations. Just like sites found on the Surface Web, these niche Deep Web sites cater to individuals hoping to talk to like-minded people, albeit anonymously.



Deep Web Radio for people who need to anonymously listen to jazz

Because of its nature, it's impossible to determine the number of Deep Web pages and content at any given time or to provide a comprehensive picture of everything that exists in it. The stealth and untraceable nature of certain parts of the Deep Web makes it so that no one can say with certainty that they've fully explored its depths.

To closely observe the Deep Web, the Trend Micro Forward-Looking Threat Research Team built a system—the Deep Web Analyzer—that collects URLs linked to it, including TOR- and I2P-hidden sites, Freenet resource identifiers, and domains with nonstandard TLDs and tries to extract relevant information tied to these domains like page content, links, email addresses, HTTP headers, and so on.

Over the course of two years of using the Deep Web Analyzer, we've collected more than 38 million events that account for 576,000 URLs, 244,000 of which bear actual HTML content. So far, we've also been able to publish a couple of reports on the underground forums [9] we've found.

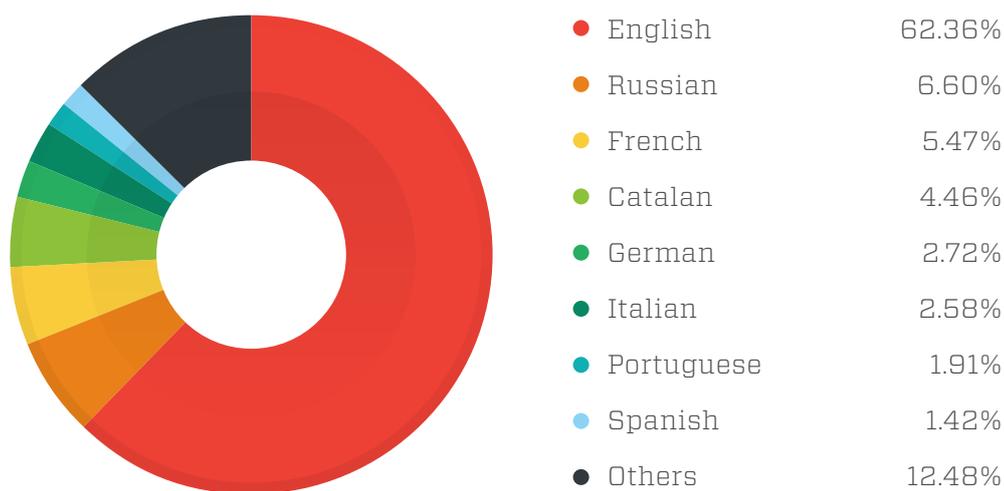
Who are on the Deep Web?

It's hard to say for certain just who reside in the Deep Web. The level of anonymity it offers its users makes it challenging for even the best security researchers to profile them. Only by examining site content and popularity can we gauge the composition of its user base.

Language distribution

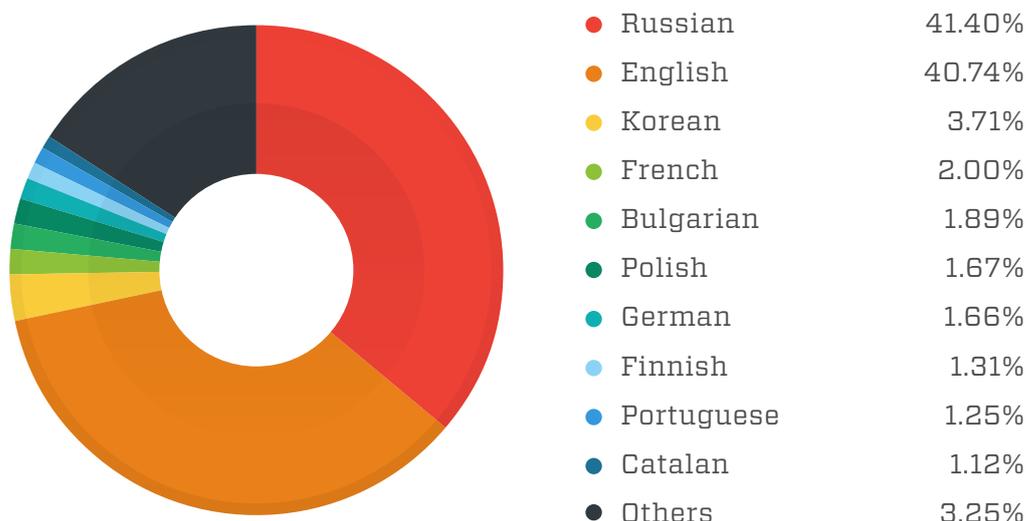
Over the past two years, we scouted and analyzed a huge number of Deep Web pages then differentiated them based on language used. This gave us a glimpse of the possible territories where Deep Web users could be based.

In terms of raw number of domains, English was the main language of choice by at least 2,154 sites out of the 3,454 successfully scouted domains. That roughly makes up 62% of the total number of sites. This was followed by Russian (228 domains) then French (which may include French and Canadian-French sites, 189 domains).



Most popular languages based on the number of domains containing pages that use them

Looking at the language distribution based on number of URLs, Russian beat English because, despite having fewer sites, the number of sites that used Russian was bigger. At present, there's a particularly huge Russian forum not directly linked to malicious activities but mirrored in both TOR and I2P that on its own added to the total number of Russian pages.



Most popular languages based on the number of URLs with content using them

Common user profile

As stated earlier, profiling Deep Web users is challenging. More than language, the closest and most reliable estimate can probably come from looking at the different marketplace vendors. This gave us an idea as to what makes networks like TOR and I2P appealing.

To get reliable information, we referred to the data available in <https://dnstats.net/>—a site that specializes in tracking activities in all darknet markets.

An analysis of the top 15 vendors across all marketplaces showed that light drugs were the most-exchanged goods in the Deep Web. This was followed by pharmaceutical products like Ritalin and Xanax, hard drugs, and even pirated games and online accounts. This data backed up the idea that a majority of Deep Web users—at least those who frequent the top marketplaces—go there to purchase illicit drugs.



● Cannabis	31.60%
● Pharmaceuticals	21.05%
● MDMA	10.53%
● LSD	5.26%
● Meth	5.26%
● Mushrooms	5.26%
● Heroin	5.26%
● Seeds	5.26%
● Video games	5.26%
● Accounts	5.26%

Vendor breakdown based on data pulled on 3 June 2015



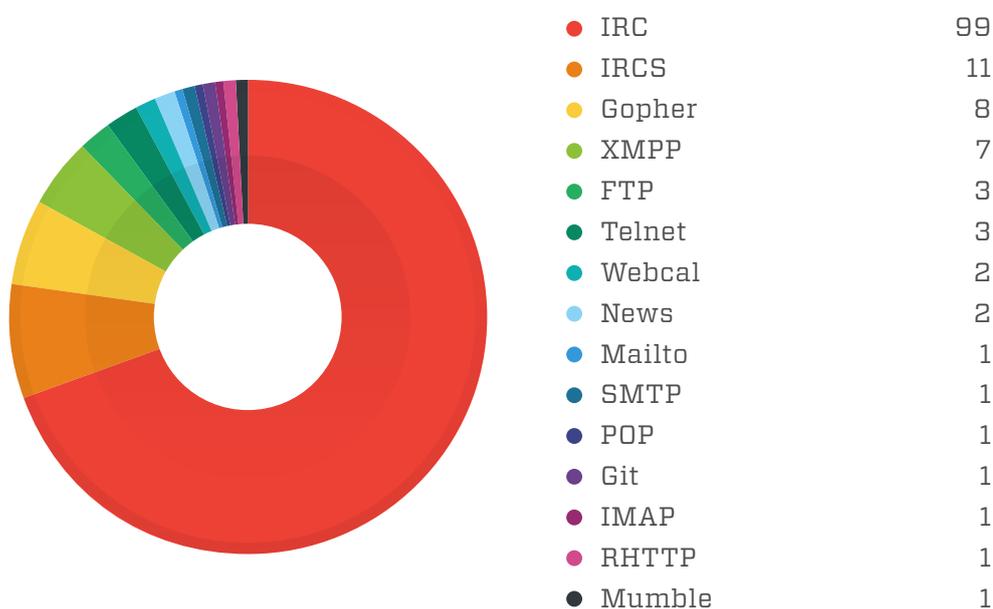
● Cannabis	27.28%
● Pharmaceuticals	22.39%
● MDMA	14.43%
● LSD	7.47%
● Meth	3.93%
● Mushrooms	3.41%
● Heroin	3.31%
● Seeds	3.92%
● Video games	6.93%
● Accounts	6.93%

Buyer breakdown based on data pulled on 3 June 2015

What makes up the Deep Web?

Many users may not be aware that there are more than just standard sites in the Deep Web. Based on two years' worth of data and research, we were able to group URLs according to their URI scheme (HTTP, HTTPS, FTP, etc.).

Almost 22,000 of the collected domains were predictably associated with either the HTTP or HTTPS protocol, as they principally hosted data. But if we filter them out, interesting data is left.



Protocols found in the Deep Web apart from HTTP/HTTPS

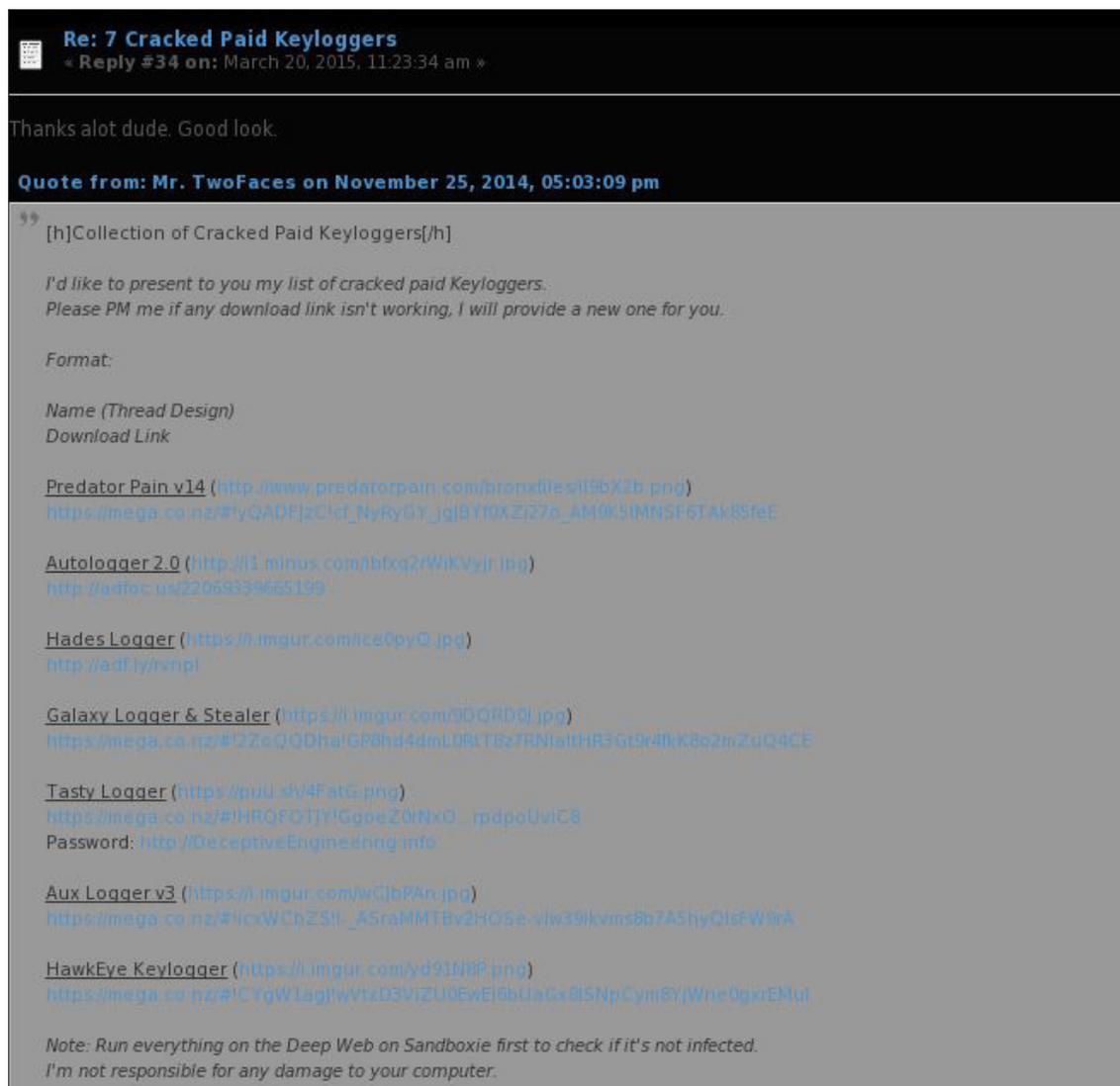
More than 100 domains use either the IRC or IRCS protocol—normally chat servers that can be used as a rendezvous for malicious actors to meet and exchange goods or as a communication channel for botnets.

The same concept applies to seven XMPP domains and one Mumble domain—protocols for chat servers that run in TOR.

Suspicious pages

For each Deep Web page we scouted, we collected the URLs found in page links. We then retrieved the Web Reputation Technology URL rating for every link that points to the Surface Web in order to identify which were classified as suspicious. Despite this limited scope, they can still be used as indicators.

Overall, we identified 8,707 suspicious pages, including those that host phishing kits, malware or drive-by-downloads, or that run shady marketplaces (used to trade hacking tools, etc.).



Re: 7 Cracked Paid Keyloggers
« Reply #34 on: March 20, 2015, 11:23:34 am »

Thanks alot dude. Good look.

Quote from: Mr. TwoFaces on November 25, 2014, 05:03:09 pm

” [h]Collection of Cracked Paid Keyloggers[/h]

*I'd like to present to you my list of cracked paid Keyloggers.
Please PM me if any download link isn't working, I will provide a new one for you.*

Format:

Name (Thread Design)
Download Link

Predator Pain v14 (<http://www.predatorpain.com/ironxfiles/19bX2b.png>)
https://mega.co.nz/#YQADPjzCld_NyRyDy_jgBY10XZi276_AM9k5IMNSF6TAk85teE

Autologger 2.0 (<http://11.minus.com/1bfqz7WkVyr.jpg>)
<http://adloc.us/22069339655139>

Hades Logger (<https://imgur.com/ice0py0.jpg>)
<http://ad.ly/rsnp/>

Galaxy Logger & Stealer (<https://i.imgur.com/9DQR0Q.jpg>)
<https://mega.co.nz/#Q2Z6QODHalGP8hd4dmLDRtBz7RMaIHRSGr9r4lk8e2mZuQ4CE>

Tasty Logger (<https://puu.sh/4F4tG.png>)
https://mega.co.nz/#IHROFQJYIGgpeZ0rNxD_rpdpoUuiE8
Password: <http://DeceptiveEngineering.info>

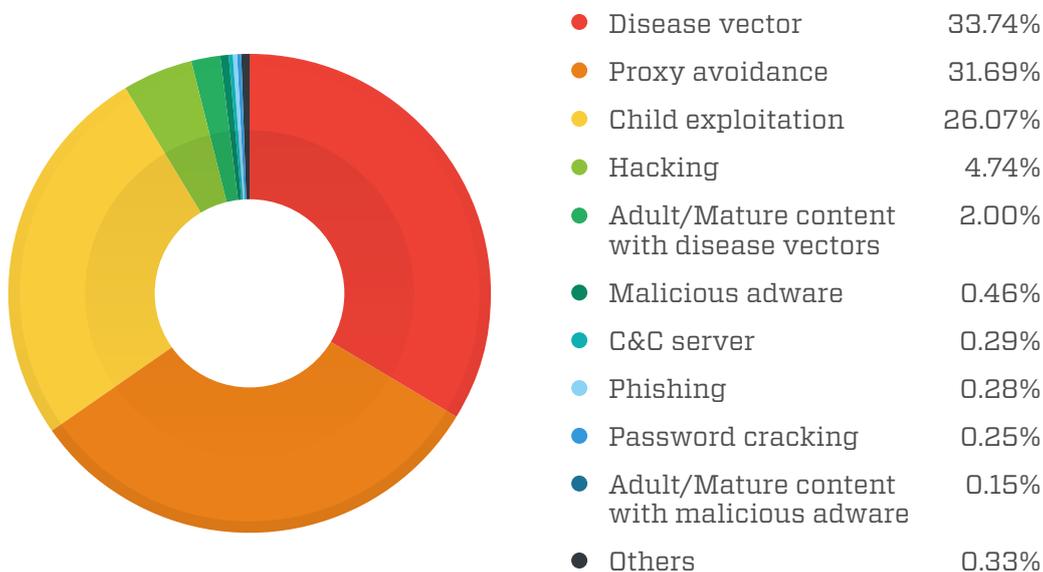
Aux Logger v3 (<https://imgur.com/mwGj6PAn.jpg>)
https://mega.co.nz/#IcxWCbZS!_ASnaNMTBv2HO5e-viw39kvms8b7A5hy0IsFW9rA

HawkEye Keylogger (<https://i.imgur.com/yd9IHRP.png>)
<https://mega.co.nz/#IYgWlagfWVtzD3VIZU0EwE18bUaGx8ISNpCym8YjWhe0gxEMur>

*Note: Run everything on the Deep Web on Sandboxie first to check if it's not infected.
I'm not responsible for any damage to your computer.*

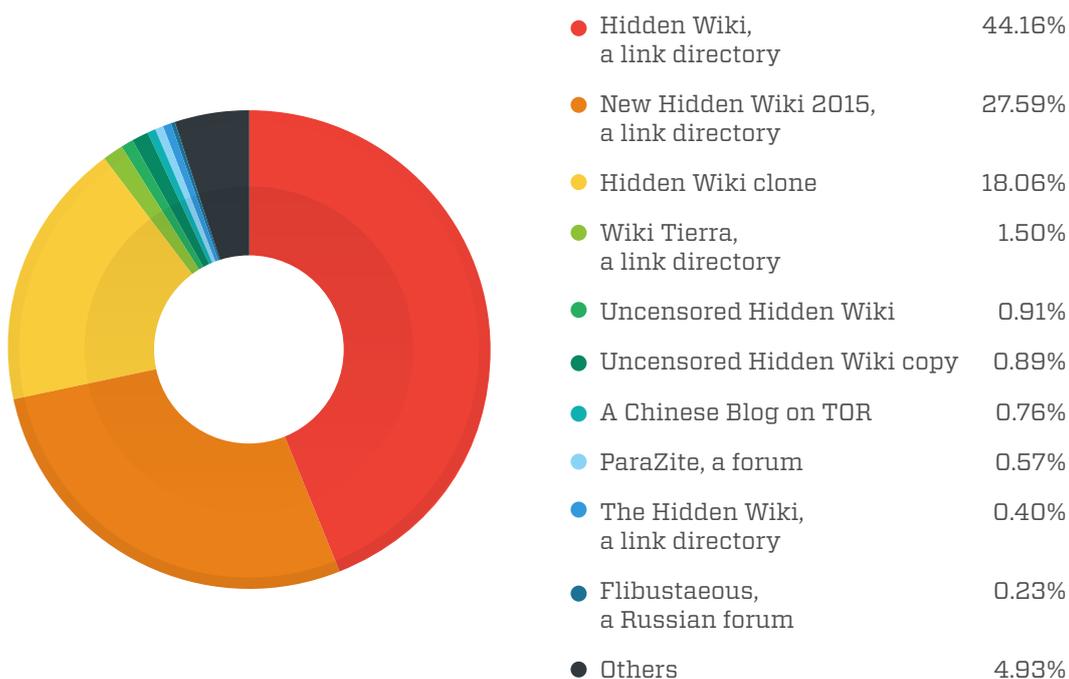
Sample site with links to keyloggers

The following table provides a breakdown of the suspicious sites by category, as confirmed by our Web Reputation Technology URL ratings.



Reasons why the Surface Web URLs were classified as suspicious

More than 30% of the links included in the web pages we classified “suspicious” were disease vectors that led users to malware-download sites. The next two classifications were proxy avoidance—URLs that provide VPN access or ways to avoid corporate firewalls—and child exploitation.



Sites bearing the highest number of suspicious Surface Web links

What bad stuff goes on in the Deep Web?

The Deep Web offers a certain level of anonymity that makes people in it more inclined to engage in illegal activities. The various transactions in it, including the makeup of prominent goods and services traded, very well paint a picture of what people would do if the secrecy of their identities was guaranteed.

Unlike in the cybercriminal underground, most types of activities in the Deep Web have more apparent, if not drastic, effects on the real world. Many of the malicious tools and services sold in the cybercriminal underground can be used to gain profit. Those peddled in the Deep Web—assassination services, for example—obviously serve a different, more sinister purpose.

We can't fully vouch for the authenticity of the goods and services discussed here, except for the fact that the sites advertising them do exist and account for the different transactions that go on in the Deep Web. We'll cite several noteworthy examples to give you a better understanding of these dubious activities.

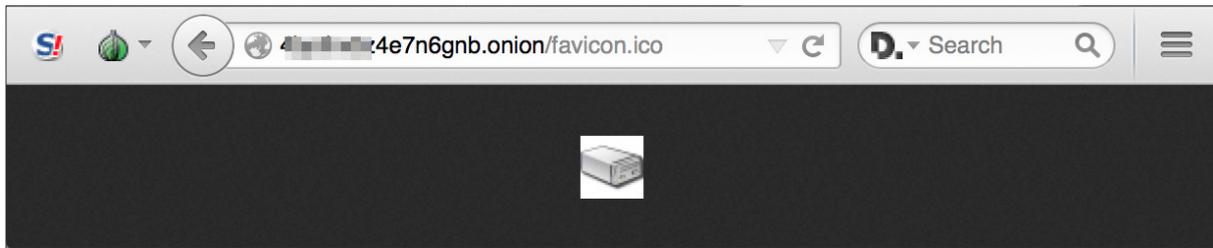
The malware trade

In many ways, the Deep Web and malware are perfectly suited for each other, especially when it comes to hosting command-and-control (C&C) infrastructure. It is the nature of hidden services and sites like TOR and I2P to hide the location of servers using strong cryptography. This makes it essentially impossible for forensic researchers to investigate using traditional means like examining a server's IP address, checking registration details, and so on. In addition, using these sites and services isn't particularly difficult.

It is then not surprising to see a number of cybercriminals use TOR for C&C. We've seen the operators behind prevalent malware families use TOR for some parts of their setup. They simply bundle the legitimate TOR client with their installation package. Trend Micro first wrote about this trend back in 2013 when MEVADE malware [10] caused a noticeable spike in TOR traffic when they switched to TOR-hidden services for C&C. Other malware families like ZBOT [11, 12] followed suit in 2014.

VAWTRAK

VAWTRAK malware are banking Trojans that spread via phishing emails. Each sample communicates with a list of C&C servers whose IP addresses are retrieved by downloading an encrypted icon file (*favicon.ico*) from some hard-coded TOR sites. This provides the advantage of anonymizing the location of a criminal server but not the users who access it, which is not an issue because all of the "users" are systems that the malware infected. We wrote more on this technique in our steganography blog series [13, 14, 15].



VAWTRAK C&C server that shows a legitimate-looking favicon file

Based on the presence of this *favicon.ico* file and the C&C server setup (many of which run *openresty/1.7.2.1*), we are able to search our system for a complete list of such sites and download the latest C&C server address each day.



Discovered VAWTRAK C&C servers

CryptoLocker

Another major malware family that uses the Deep Web is CryptoLocker. CryptoLocker refers to a ransomware variant that encrypts victims' personal documents before redirecting them to a site where they can pay to regain access to their files. CryptoLocker is also smart enough to automatically adjust the payment page to account for a victim's local language and payment means.

TorrentLocker—a CryptoLocker variant—makes use of TOR to host payment sites in addition to employing Bitcoin as form of payment. It shows why the Deep Web appeals to cybercriminals who are willing to make their infrastructures more robust to possible takedowns.

The following screenshots are payment pages that the Deep Web Analyzer captured. Both are rendered in different languages, giving us an idea of their intended victims and origin.

CryptoLocker 购买解密软件 免费解密一个文档 常见问题 支持页面

购买解密软件以便还原所有加密文档

 2015-05-04 02:46:06前购买解密软件只需11900 TWD
或之后购买价格为23800 TWD
价格上涨前剩余时间: 00:00:00
加密文档数量: 112098

现行价格: 3.59856 比特币 (约 23800 TWD)
已支付: 0 比特币 (约 0 TWD)
余款: 3.59856 比特币 (约 23800 TWD)

使用 bitcoin 来购买解密软件

比特币到底是什么?

比特币(BTC, Bitcoin) - 互联网上使用的虚拟货币。

- 1 购买比特币**
您可在网站上购买比特币以便在台湾兑换货币。
您可以使用下列网址提供的服务, 通过银行汇款、便利店支付或西联汇款购买比特币。如果您通过银行账户完成支付, 该账户

Automatically formatted CryptoLocker pages for victims from Taiwan

Acquista decrittazione e ripristinare i file



Acquista decrittazione per **399 EUR** prima **2015-03-16 21:26:36**

O acquistare in un secondo momento con il prezzo di **798 EUR**

Tempo rimasto prima di aumento dei prezzi: **00:00:00**

Prezzo corrente: **4.357080 Bitcoin (circa 798 EUR)**

Pagato: **0.000000 Bitcoin (circa 0 EUR)**

Rimanendo a pagare: **4.357080 Bitcoin (circa 798 EUR)**

Acquista decifratura con **bitcoin**

Cosa sono i Bitcoin?

Bitcoin (simbolo: ₿; codice: BTC o XBT) è una moneta elettronica.

1 Acquista bitcoin

Si prega di consultare consigliato bitcoin venditori nel tuo paese:

www.coinbit.it - Bitcoin in 5 minuti grazie ad un sistema completamente automatizzato. Bonifico, Postepay e Superflash.

postecoin.com - Compra BitCoin con Postepay.

www.bitboat.net - Il mercato numero uno in Italia, per comprare Bitcoin istantaneamente, in contanti.

postebit.it - Compra bitcoin in contanti senza registrazione!

www.mars78.biz - Compra BitCoin con Postepay, Superflash.

www.happycoins.com - Compra BitCoin con Mybank, Sofort.

www.litebit.eu - Compra BitCoin con Postepay, Sepa, Sofort.

localbitcoins.com - Compra bitcoin online in Italy

howtobuybitcoins.info - Come acquistare bitcoin in Italia.

2 Invia bitcoin

Invia Bitcoins alla nostra bitcoin-portafoglio.

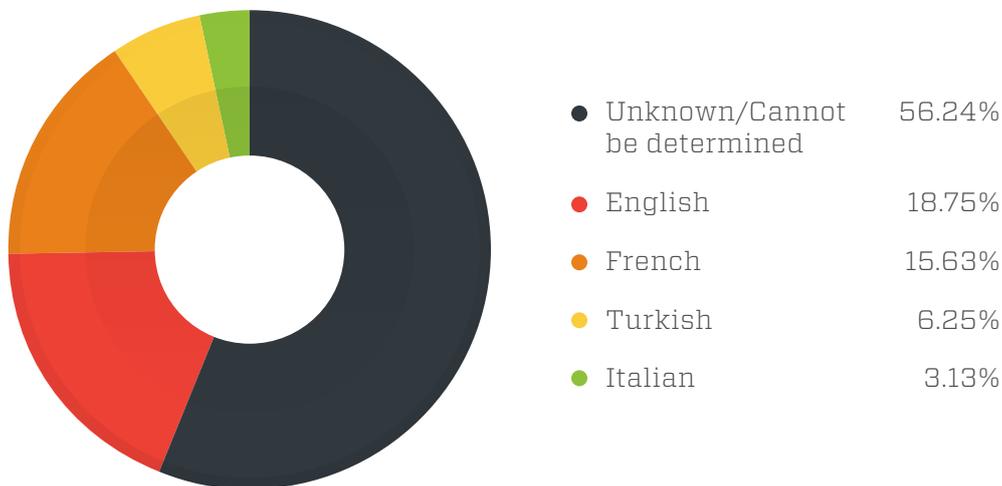
Importo del pagamento: **4.357080 Bitcoin (circa 798 EUR)**

Il nostro indirizzo bitcoin portafoglio: **162Gjj9PNgdBm3CoqaZQhViBRoeoz5r18a**

3 Parlaci di pagamento e decifrare i file

Dopo aver inviato bitcoin al tuo portafoglio personale, fare clic su Verifica di pagamento. Se il pagamento ha avuto successo, è possibile scaricare il software di decrittazione.

Automatically formatted CryptoLocker pages for victims from Italy



Top languages used by CryptoLocker pages

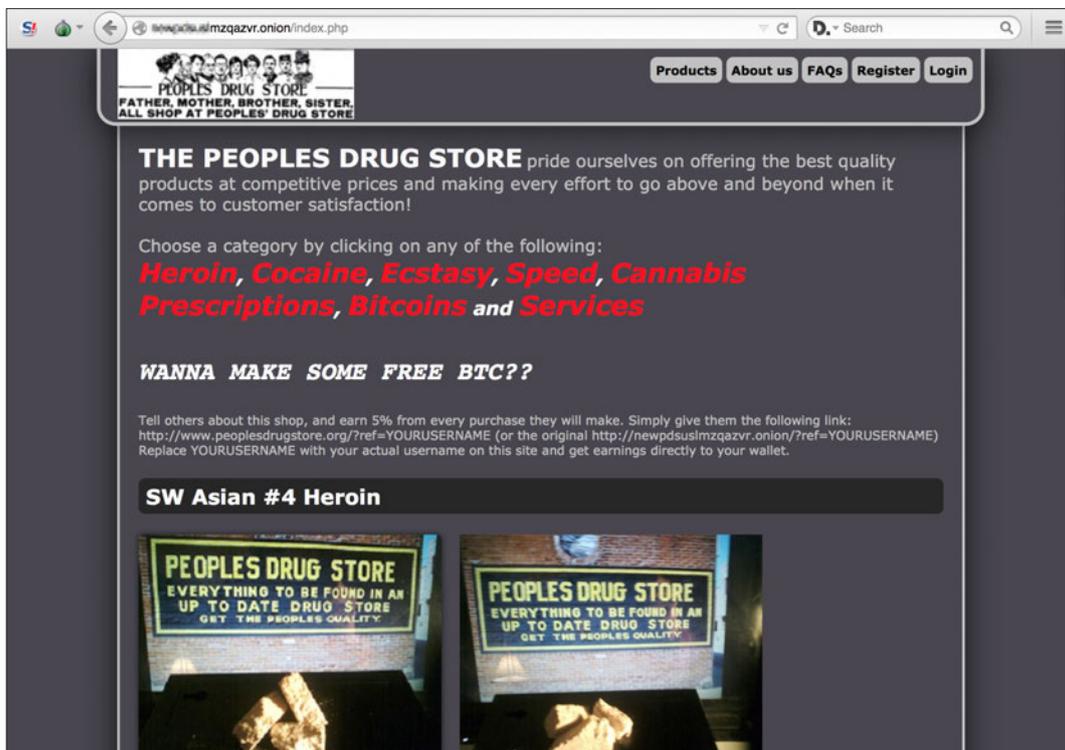
Unfortunately, given all of the benefits cybercriminals reap by hosting the more permanent parts of their infrastructures on TOR-hidden services, we believe we'll see more and more malware families shift to the Deep Web in the future. Because of this, the Deep Web Analyzer implements heuristics to find new malware families (so-called "unknown unknowns"). This feature allows us to be alerted every time hidden services suddenly get a lot of traffic or if there is a large spike in the number of sites.

Bots, more than other forms of malware that communicate with C&C servers, are known for using static URI query strings or the same parameters over time. We used this observation as input so the Deep Web Analyzer can automatically flag all traffic that employs the static query string pattern as suspicious. A more specific example of this application, related to malware named NionSpy (aka Mewsei and MewsSpy) that steal confidential information, can be found in the appendix.

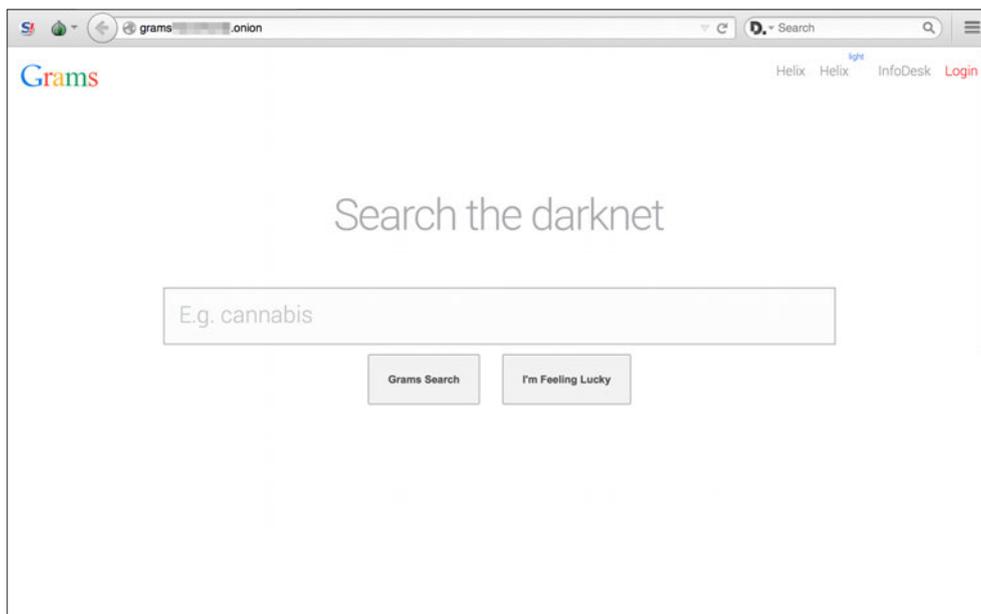
Illicit drugs

It's common for just about every report on the Deep Web to talk about how freely available illegal drugs and weapons are in it. We don't intend to go into detail on this, as others have covered it ad nauseam. But we did want to briefly highlight the fact that even after the conviction of individuals like Ross Ulbricht [16], procuring drugs on the Deep Web is still relatively trivial.

The availability of illegal narcotics varies a lot on the Deep Web. Some sites sell everything from the relatively tame (contraband tobacco) to cannabis, psychedelics, cocaine, and others.



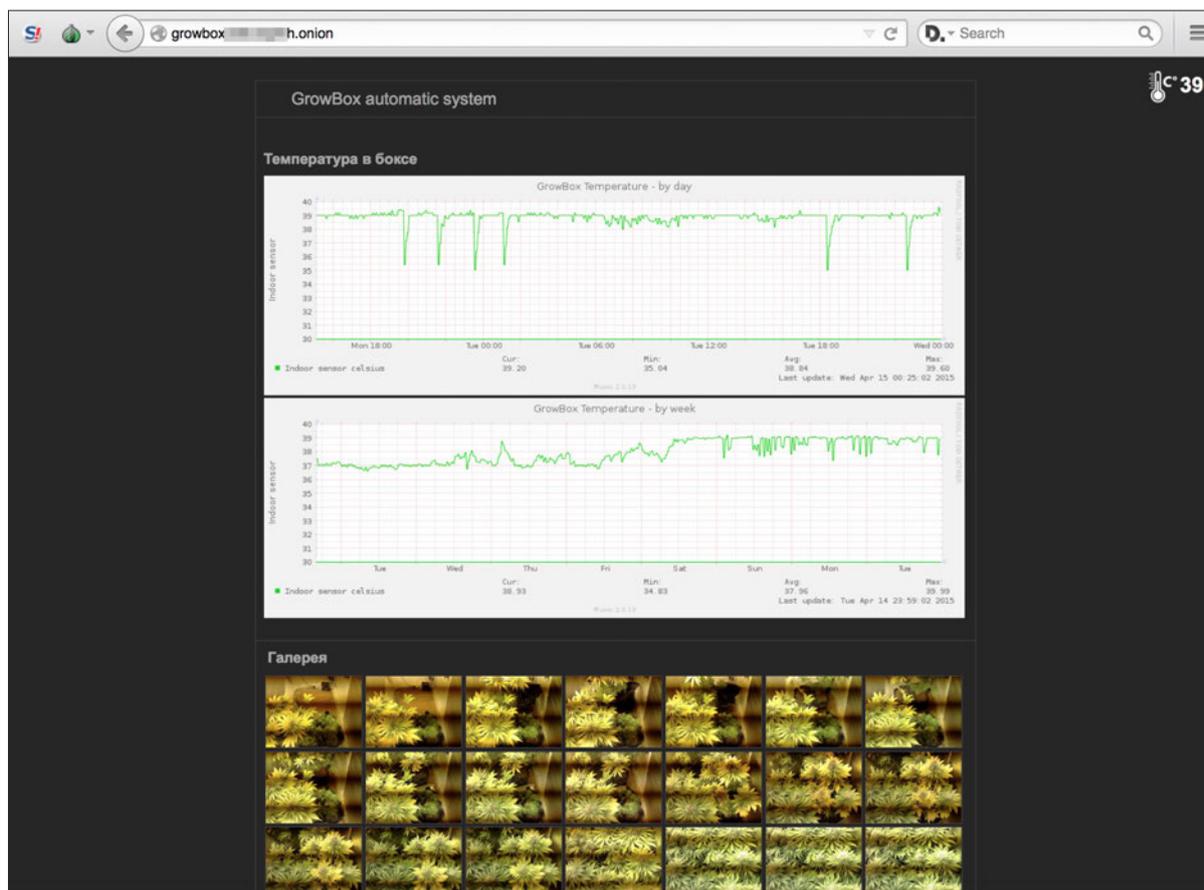
Peoples Drug Store sells heroin, cocaine, ecstasy, and more



Grams—the Deep Web search engine for drugs

In addition to dedicated shops or forums, a very popular site—Grams—allows people to easily search and index Deep Web sites that deal in illegal drugs. With a logo mimicking that of Google, it has become a de facto site for those in search of such goods.

We even found TOR sites that offer information on an active cannabis grow house that shows live temperature and moisture stats and a live camera feed of the plants growing over time.



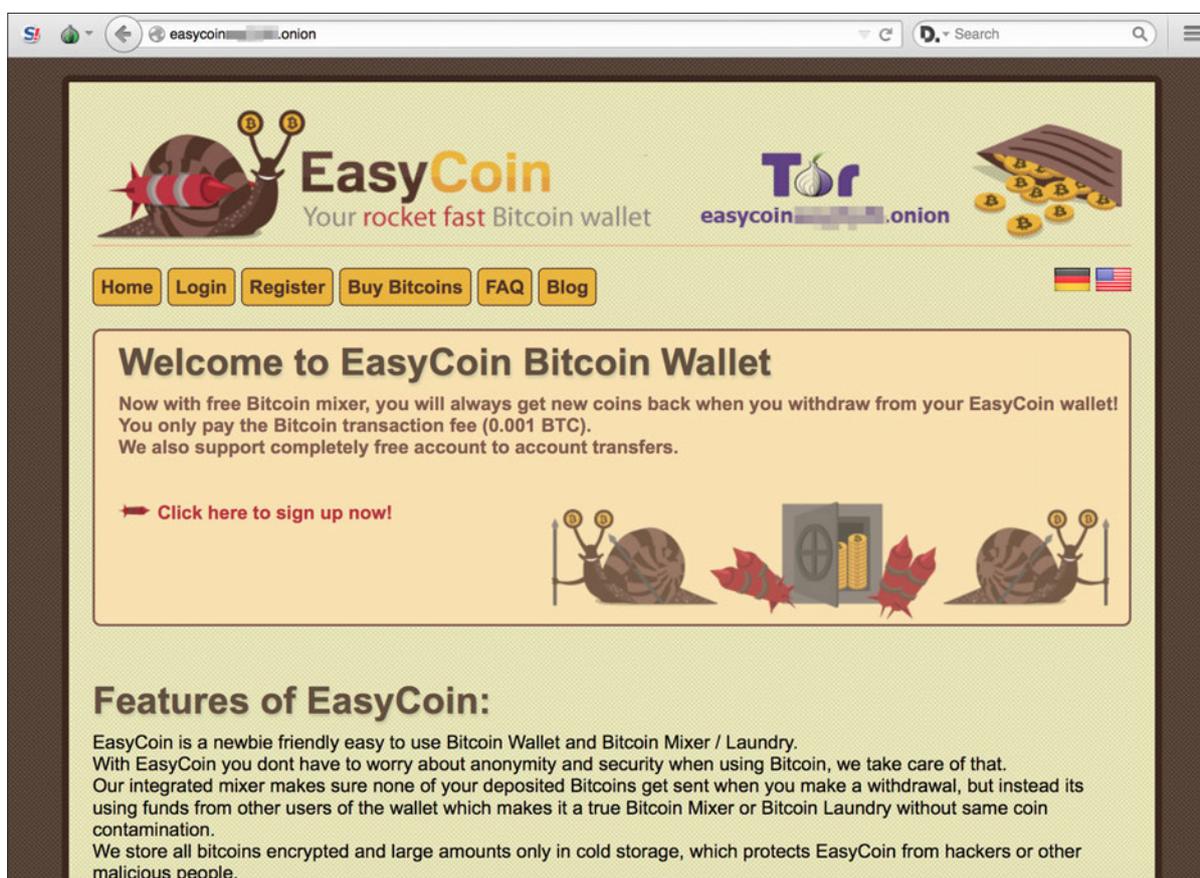
Cannabis grow house live stats and streaming

We touched on drugs to further highlight a point we made in our Expert Insights video on the Deep Web [17], that is, taking down a criminal marketplace like the Silk Road isn't fundamentally a solution. On one hand, you still have buyers looking to procure drugs; on the other, you have sellers who wish to cater to their needs. The marketplace or forum merely acts as a middle ground. Even if you remove it, as long as the demand for it is strong enough on both sides, another marketplace will unfortunately always rise to take its place.

Bitcoin and money-laundering services

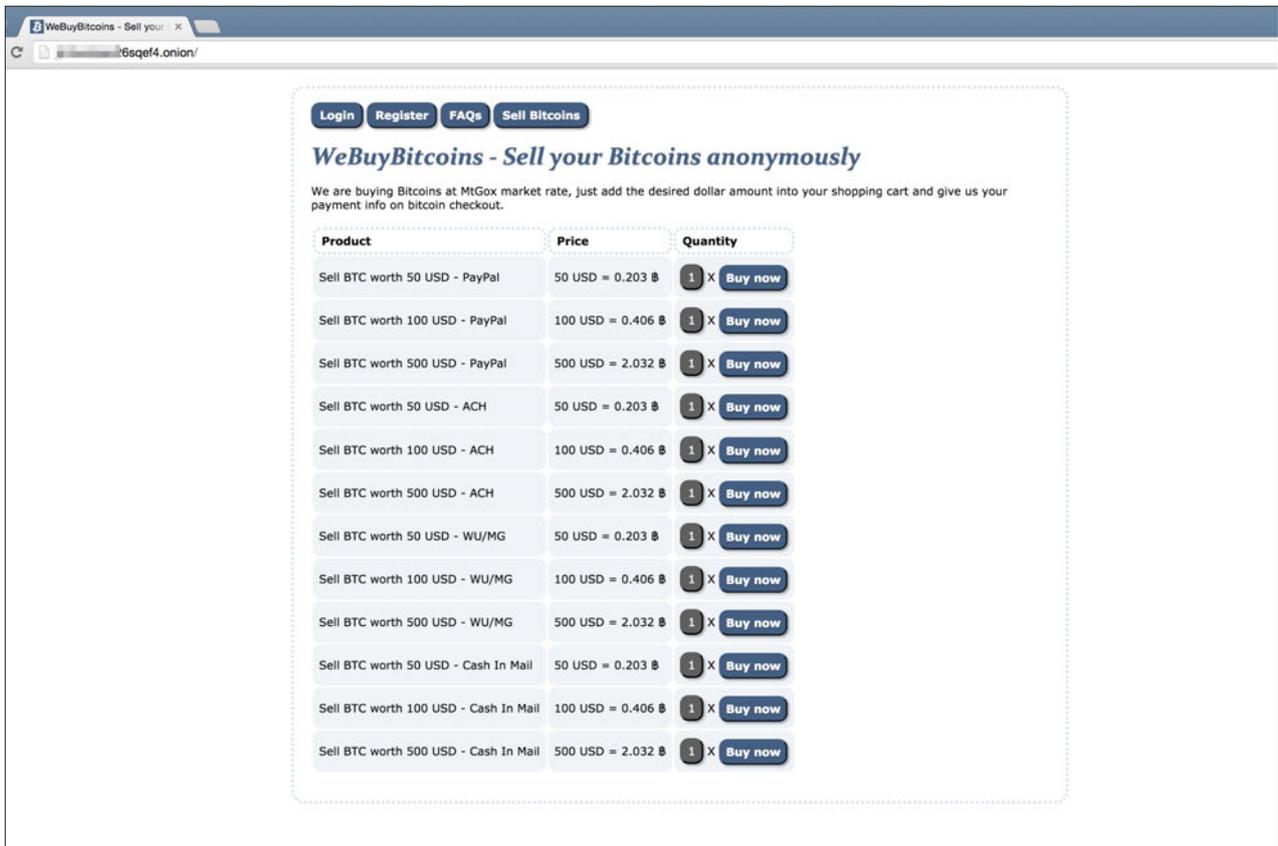
On its own, Bitcoin is a currency designed with anonymity in mind. As a result, it's frequently used when purchasing illegal goods and services [18]. While all Bitcoin transactions are anonymous (as long as you don't link your wallet code to your real identity), they are fully public. The fact that every transaction in the Bitcoin blockchain is publicly available means investigators can examine them. Tracking money as it moves through the system is thus doable, albeit quite difficult.

As a result, a number of services that add further anonymity to the system have surfaced, making the electronic currency even more difficult to track. This is generally achieved by "mixing" your Bitcoins—transferring them through a spidery network of microtransactions before returning them to you. In the process, you end up with the same amount of money (normally, minus a small handling fee) but your transactions become substantially harder to track.



EasyCoin Bitcoin-laundering service

Bitcoin-laundering services help increase the anonymity of moving money throughout the Bitcoin system. Ultimately though, most Bitcoin users will wish to extract money from the system to turn it into cash or other types of traditional payment means. Several anonymous services exist in the Deep Web for this purpose. These allow users to exchange Bitcoins for money via PayPal™, Automated Clearing House (ACH), Western Union, or even cash sent directly via mail.



WeBuyBitcoins, a service that exchanges cash or offers electronic payment means for Bitcoins

Sites like WeBuyBitcoins exchange real cash for Bitcoins at competitive exchange rates compared with equivalent nonanonymous services that exist in the Surface Web. Criminals who are willing to take on more risk for potentially greater rewards can take another option—buying counterfeit currency using Bitcoins.

usjudr...onion

USJUD COUNTERFEIT

DOLLARS EUROS QUESTIONS?

http://USJUDr...onion

20\$ SuperDollars

Features :

- 100% Cotton linter pulp paper
- Watermark embedded into the paper
- The 20 on the bottom left of the front of the bill is printed using color-shifting metallic flecks
- Infrared emulation on border to trick some vending machines
- Security strip will glow green when exposed to UV light
- Dont reacts to the ammonia, So pass the pen detector.

Cons :

- The infrared detector normally detect our notes. (Sometimes not)
- We use 10 different serial numbers so some are repeated (in each order)



[Click to enlarge](#)

Production:

- These notes are produced in Asia, are the highest quality possible also known as "SuperDollars".

Ways to spend:

Shipping from France ; Stock: Available

Min order:	25 Notes
Regular shipping:	Included
Price:	
25 notes:	\$250
50 notes:	\$440
75 notes:	\$550
100 notes:	\$690
150 notes:	\$990
200 notes:	\$1280

usjudr...onion/eur.php

USJUD COUNTERFEIT

DOLLARS EUROS QUESTIONS?

http://USJUDr...onion

20€ Euros

Features :

- 100% Cotton linter paper
- Watermark embedded into the paper
- Security strip hologram
- Infrared emulation on border to trick vending machines
- Dont reacts to the ammonia, So pass the pen detector.

Cons :

- The infrared detectors detect our notes.
- We use 25 different serial numbers so sometimes some are repeated.



[Click to enlarge](#)

Production:

- These notes are produced in Asia, with the highest quality possible.

Ways to spend:

Shipping from France ; Stock: Available

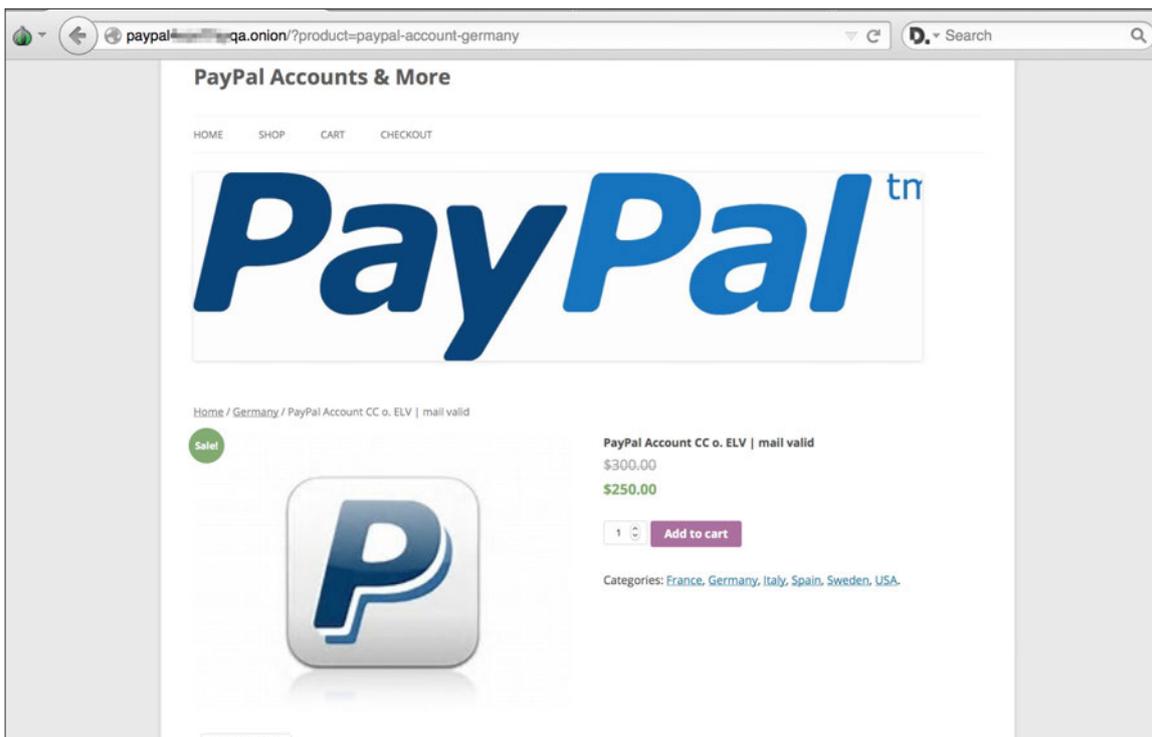
Min order:	25 Notes
Regular shipping:	Included
Price:	
25 notes:	€225
50 notes:	€400
75 notes:	€490

Sites that offer counterfeit US\$20 or €20 for approximately half their face value; others also offer counterfeit US\$50 or €50 bills

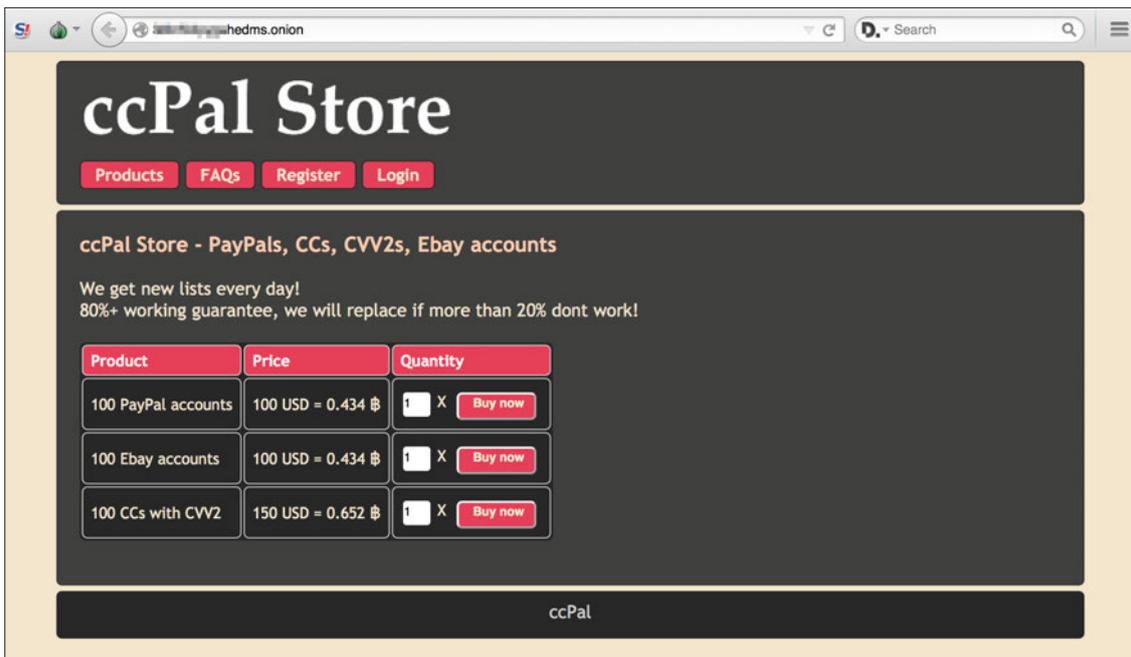
Stolen accounts for sale

Buying and selling stolen accounts are most definitely not restricted to the Deep Web. They are very common practices across criminal underground forums that exist on the Surface Web. We've extensively written about in previous reports on the Russian [19, 20] and Chinese [21] undergrounds. Credit card numbers, bank account numbers, and online auction and gaming site credentials are probably among the most commonly sold goods.

As in the Surface Web, prices vary across sites but more mature offerings (like stolen PayPal account credentials) do tend to fetch high prices. Accounts like these are generally sold in one of two ways—as “high-quality” verified accounts with their exact current balances or in bulk (a certain number of unverified accounts that normally come with a guarantee that at least a certain percentage are valid). The first category is normally seen as more expensive because they come with a greater likelihood of return on investment (ROI) for a buyer whereas the second is significantly cheaper.

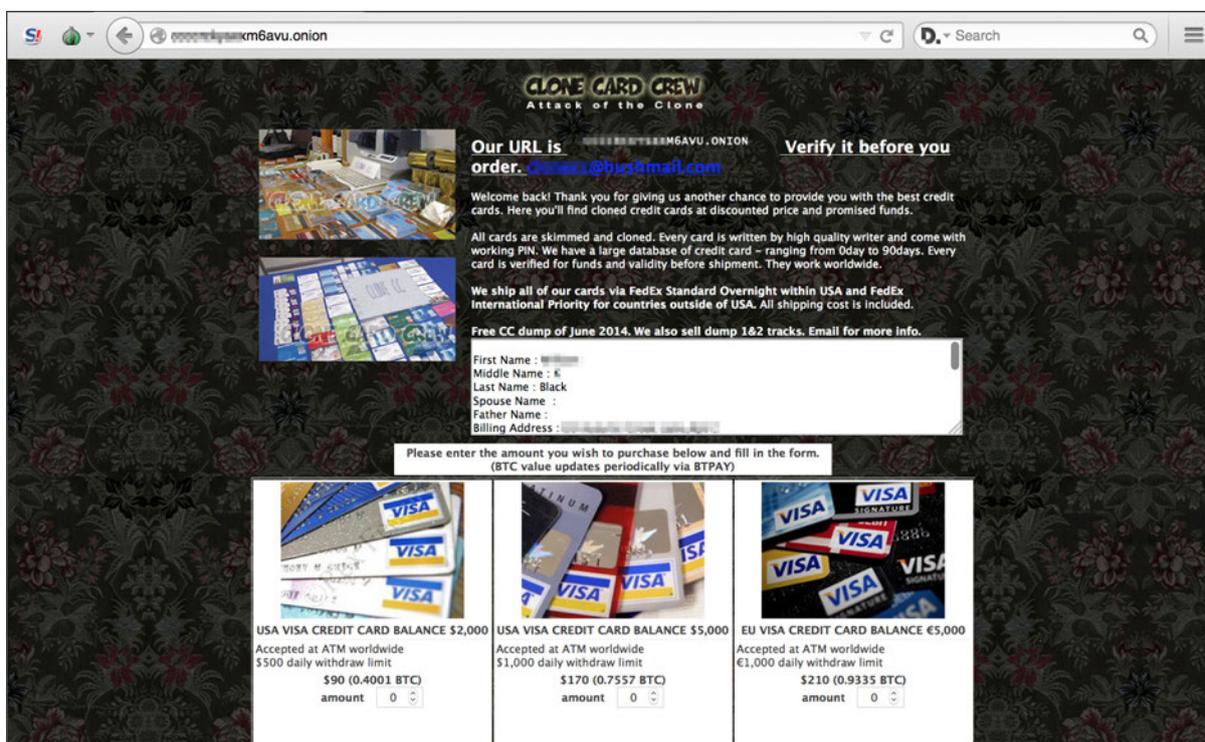


Stolen verified German PayPal accounts (US\$500-700 balance) for sale for US\$250



Unverified PayPal accounts sold in bulk (80% valid or replacement offered)

One offering that can be quite readily found in the Deep Web but not so much on the Surface Web are actual, physical credit cards. That doesn't mean they don't exist on Surface Web criminal forums. They most certainly do. The sites that offer them on the Deep Web just seem a bit more professional in terms of approach.



Replica credit cards created with stolen details

Passports and citizenships for sale

Passports and IDs are unique, powerful documents, and fake ones, even more so. They act not only as a form of identification for crossing borders (including ones buyers could normally not easily cross) but also for everything from opening bank accounts, applying for loans, purchasing property, and much more. It's no surprise then that they're a valuable commodity. There are quite a few sites on the Deep Web that claim to sell passports and other forms of official IDs at varying prices from country to country and seller to seller.

As mentioned earlier though, their validity is hard to verify without actually purchasing the goods, especially in the case of citizenship. Related services may well be simple scams preying on the vulnerable who are looking to obtain citizenship to remain in the country they currently reside in.



The screenshot shows a website interface for selling USA citizenship. The browser address bar displays 'http://...dq5r.onion'. The page title is 'USA Citizenship'. Navigation buttons include 'Products', 'FAQs', 'Register', and 'Login'. A main heading reads 'Become a citizen of the USA, real USA passport'. To the left is an image of the American flag and the Statue of Liberty. The text describes the offer: 'We offer bulletproof USA passports + SSN + Drivers License and Birth Certificate and other papers making you an official citizen of the USA! It will even work if you arent in the USA yet'. It further explains the process: 'How we do it? Trade secret! But we can assure you that you wont have any problems with our papers. We are shipping documents from the USA, international shipping is no problem. You can use your own name or a new name! Information on how to send us required info (scanned signature, biometric picture etc) will be given after purchase.' At the bottom, a table lists the product and price:

Product	Price	Quantity
Your USA citizenship	5900 USD = 25.624 ₿	1 X Buy now

U.S. citizenship for sale for at least US\$6,000



Pricing

Country	Price for Passport	Price for Passport + Driving license	Price for Passport + ID card	Price for Passport + Driving license + ID card
Australia	600 Euro	700 Euro	700 Euro	800 Euro
Belgium	500 Euro	600 Euro	600 Euro	700 Euro
Brazil	400 Euro	-	-	-
Canada	600 Euro	700 Euro	700 Euro	800 Euro
Ireland	500 Euro	600 Euro	600 Euro	700 Euro
Italia	550 Euro	650 Euro	650 Euro	750 Euro
Finland	500 Euro	600 Euro	600 Euro	700 Euro
France	600 Euro	700 Euro	700 Euro	800 Euro
Germany	600 Euro	700 Euro	700 Euro	800 Euro
Malaysia	450 Euro	550 Euro	550 Euro	650 Euro
Netherlands	600 Euro	700 Euro	700 Euro	800 Euro
Norway	650 Euro	750 Euro	750 Euro	850 Euro
Poland	500 Euro	600 Euro	600 Euro	700 Euro
Portugal	500 Euro	600 Euro	600 Euro	700 Euro
Spain	550 Euro	650 Euro	650 Euro	800 Euro
Switzerland	650 Euro	750 Euro	750 Euro	850 Euro
Sweden	550 Euro	650 Euro	650 Euro	750 Euro
United Kingdom	650 Euro	750 Euro	-	-
USA	700 Euro	800 Euro	800 Euro	900 Euro

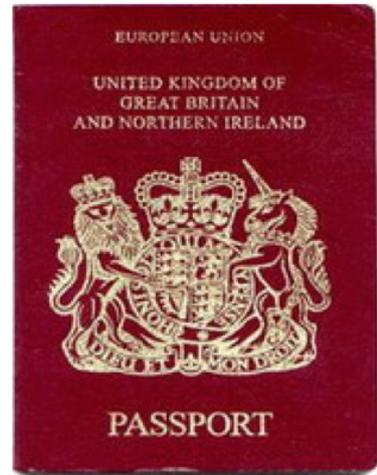
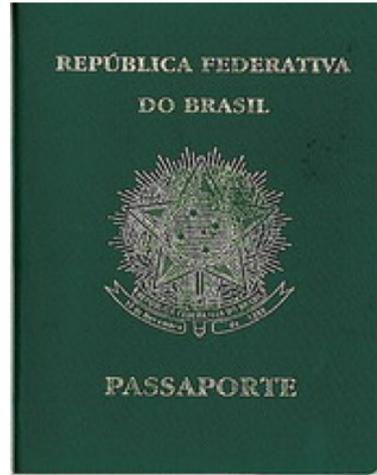
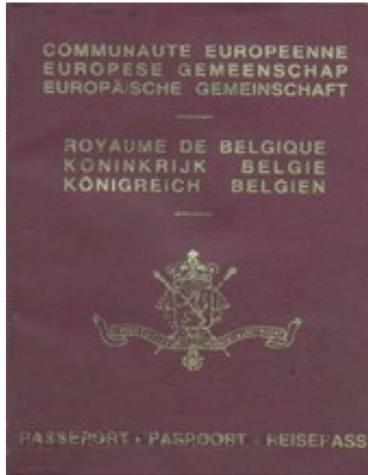
For some countries we have a unique option to register passports in official government department databases. To get more details please contact with our manager: documents.service@fakeid.com

Additional services	Price for one unit
Documents duplicating	extra 100 Euro
Visa/stamps affixion	extra 25-110 Euro

Prices on specific services like producing passports and documents for countries not listed above, duplicates, stamps, diplomatic passports and others should be discussed with our operator and may be variable.

Pricing information

P assports:



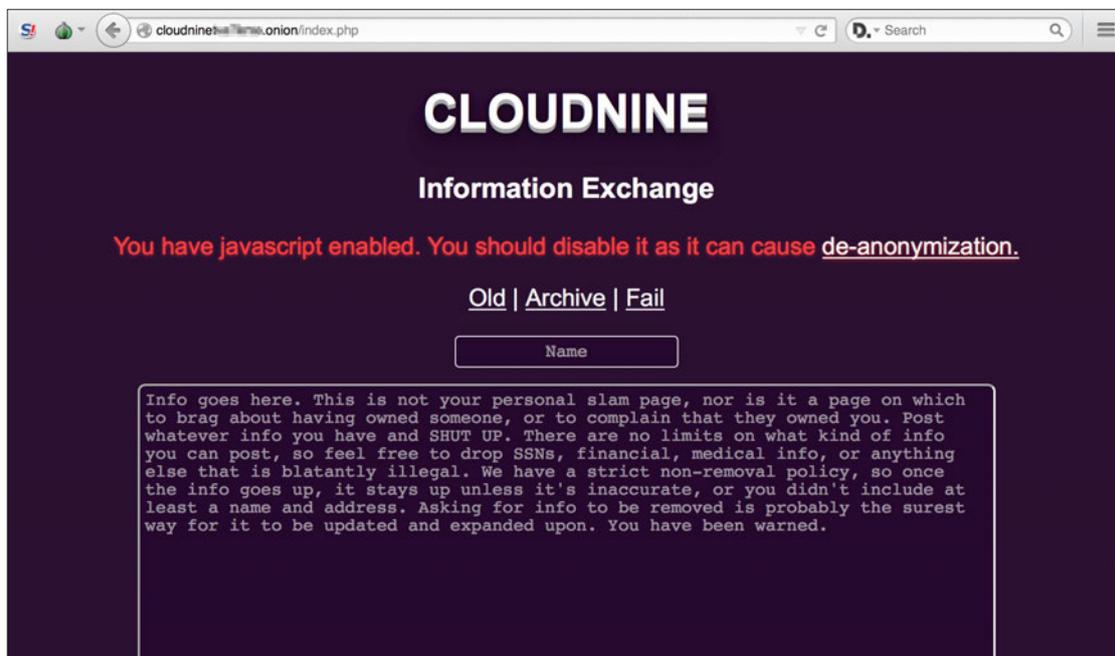
pricing...



Sample fake passports and other documents

Leaked details: Government, law enforcement, and celebrities

Among hackers and, to a certain degree, online gamers, it's typical for groups of like-minded individuals to come together in loosely formed or close-knit groups. Due to the nature of the activities they carry out, it's very common for rivalries and fallings out to occur among competing groups. When this occurs, it's common practice for one group to attempt to "dox" the other. Doxing is the act of researching and broadcasting an individual's personally identifiable information (PII), which, in hackers' case, "unmasks" a rival, essentially linking his/her real-world identity to his/her online one. The means to do this vary but they normally combine accessing publicly available data, social engineering, and direct hacking.



Cloudnine doxing site (note that this requests for social security, medical, financial data, etc.)

But the phenomenon of doxing or exposing private information is by no means restricted to hackers versus hackers; it's also quite common for hackers to target companies, celebrities, and other public figures. A company's exposure can't simply be restricted to hacking, of course, it can also be caused by insiders, as in Wikileaks's case (which involved the Deep Web in the form of a page that allows the anonymous submission of new leaks).

It's very hard to know if these details are factual or not but, in many cases, the leaked details include dates of birth, social security numbers, personal email addresses, phone numbers, physical addresses, and more. For example, one site—Cloudnine—lists possible dox information for public figures including:

- Several FBI agents
- Political figures like Barack and Michelle Obama, Bill and Hillary Clinton, Sarah Palin, U.S. senators and others
- Celebrities like Angelina Jolie, Bill Gates, Tom Cruise, Lady Gaga, Beyoncé, Dennis Rodman, and more

```

Barack Hussein Obama
SSN: ██████████
AGE: 50
DOB: 08/04/1961 (August 4th 1961)

Born In: Honolulu, Hawaii

Married to Michelle Obama (Robinson)

Obama's Yahoo Email Address
██████████ - IP Used to sign in ██████████ - Arrlington, VA - Verizon Internet.

Baracks Personal IP (IP of the Whitehouse?) ██████████ - Washington DC IP that was signed into both emails.

Obama's AOL (Protected by AOL Security)
██████████@aol.com

Barack IP used to sign into that E-mail when he was in Rhode Island. ██████████ - Cox Communications.

```

Apparent personal email account of Barack Obama (unverified)

<u>FBIGOV</u>	177.87 KB
<u>FBI Agent ██████████</u>	1.84 KB
<u>FBI CIA DoD OFFICIALS</u>	15.25 KB
<u>fbi_director</u>	12.92 KB
<u>fbi_director_family_edition</u>	20.32 KB
<u>FBI SNITCH ██████████</u>	0.17 KB

Apparent leaked law enforcement agency information (unverified)

<u>KillU4Aids</u>	0.23 KB
<u>killurxoxo aka kaci</u>	0.38 KB
<u>Kimberleigh Ann Keister</u>	0.08 KB
<u>Kimberly Brown</u>	0.35 KB
<u>kimberly_daniel</u>	0.75 KB
<u>kimmo</u>	1.16 KB
<u>Kim Kardashian</u>	0.37 KB
<u>kingcult</u>	0.21 KB
<u>KingCurses</u>	0.96 KB
<u>KinGRiisky</u>	1.26 KB

Kim Kardashian data, among other hacker-related doxing information

Even hackers who were sympathetic to Ross Ulbricht have deliberately targeted individuals involved in his case. An example of this is a post of alleged doxing information on Judge Katherine Bolan Forrest, one of the judges on the case.



The Hidden Wiki

[create account](#) [log in](#)

navigation

- [Main page](#)
- [Recent changes](#)
- [Random page](#)
- [Help](#)

search

Go
Search

tools

- [What links here](#)
- [Related changes](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)
- [Page information](#)

page
discussion
view source
history

Dox - Katherine Bolan Forrest (Silk Road Judge)

Revision as of 17:46, 11 October 2014 by [Fixlink](#) (Talk | contribs)
(diff) ← Older revision | Latest revision (diff) | Newer revision → (diff)

<http://freeross.org/> - Please donate to the official legal defense fund of the Ulbricht family.

Who is Judge Katherine Forrest?

Katherine Bolan Forrest is the judge who is unfairly ruining Ross Ulbricht's life and chance for a fair trial. In case you are unaware of her, she was the Judge who "[Rejected Every Defense Argument In The Silk Road Trial](#)" [Cleanet link!]

Can Ulbricht really be accused of running a drug-selling conspiracy when he (**ALLEGEDLY**) merely ran a website that made the narcotics sales possible? And can he be charged with money laundering when bitcoin doesn't necessarily meet the requisite definition of money? According to Forrest's latest ruling, yes and yes. She rejected every argument made in the defense's motion, starting with the idea that Ulbricht had merely provided an innocent platform for hosting the Silk Road's illicit e-commerce, just as eBay might occasionally host illegal content without its knowledge.

Justice is not being served, Ross Ulbricht is a hard working honest man who is now a fall guy that the US government decided to choose because he had a large amount of bitcoins, a currency they are doing everything in their power to make illegal.

Judge Katherine Forrest Dox

Without further ado, fuck this stupid bitch and I hope some drug cartel that lost a lot of money with the seizure of silk road will murder this lady and her entire family: [http://\[redacted\]](http://[redacted]) =[Judge_Katherine_Forrest](#)

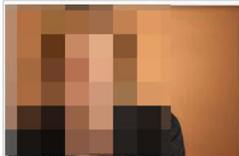
Katherine Bolan Forrest

[Redacted text]

I can also get information on all of this lady's relatives and maybe some of her close friends, so expect more releases over doxbin and this wiki. For right now just steal her identity and send her gifts in the mail ;) Expect phone numbers and relatives SSNs and complete doxes in a future release.

Oh, and maybe someone should attempt a [Swat](#) [Cleanet link!] just to put this bitch in her place. Just please don't be an idiot and fall for that "Tor SWATING Service" scam going around. Oh and Katherine, don't be surprised when you and all your relatives get woken up in the middle of the night by a swat team with assault rifles pointed in your face and helicopters shining search lights into your windows. Or when someone close to you opens up a letter in the mail one day and it happens to contain anthrax ;)

Categories: [Drug markets](#) | [Law](#) | [Life](#) | [Tor hidden websites](#) | [Dox](#)



Judge Katherine Forrest

[Privacy policy](#)

[About The Uncensored Hidden Wiki](#)

[Disclaimers](#)



Alleged leaked information on a judge in the Silk Road case

Assassination services

Perhaps one of the most worrying services on the Deep Web, one that anyone would be very foolish to advertise on the Surface Web, are hit men or assassins for hire. Several such services exist on the Deep Web. Even the sites that advertise them acknowledge the highly secret nature of their business. One site, for example, clearly states that as all contracts are private, they can't offer proof of past work or successes or even feedback from previous clients. Instead, they ask users to prove upfront that they have enough Bitcoins for the job with the help of a reputable escrow service. Only when a hit man has carried out the assassination and provided proof will the funds be released.



C'thulhu



Email: [redacted] Lq4dYtAxW7U@bitmessage.ch

Solutions to Common Problems! We are an organized criminal group, former soldiers and mercenaries from the FFL, highly-skilled, with military experience of more than five years. We can perform hits all around the world.

If you're asking yourself "Why someone would need to hire a killer online?", we'll tell you: simply because it is anonymous. You can always find examples of contractors who collaborated with cops (when they were facing 20 years of prison), and you (the buyer) could end up in the prison because of that. On the other hand, you can also find examples where police found who had the interest to put out a contract, and they can come to you and you can give your testimony (which would put the hitman in jail).

So, it is of mutual interest to make everything anonymous. This website is hosted on a series of anonymous servers, with access to the Internet through the Tor network. You can access this site anonymously only through the Tor network, and we upload files to the server through the Tor network. You can make payments with an anonymous digital currency, either Bitcoins. It means we don't know you and you don't know us. We can't send you to prison, and you can't send us to prison. Of course you must take a risk when you pay in advance, but there is no interest. With risk comes reward. You take a risk, and someone can always cheat you. As we said, many criminals have the balls to do things to other people, but when they face 20 years of prison they begin to talk with the police. Risks about prison and money are always present. If you are not ready to take a risk, don't contact this kind of organizations. And know, we are only one, real contractor there. Any other will try cheat you. — Contract Killer © 2011.

No fish too big, no job too small - HITMAN does it all!

Q & A!

Can I see some proofs of your last work?
Every contract is Private, and all data is Purged after elimination proof is sent to the customer. It is Mandatory for Customer's and our Security!

Can You give me contact to person who already used your services?
Again, Every contract is Private! Without Exceptions! And we will never store or share such info after completing.

Can you give to me a good feedback about, you and some proofs of succeeded work?
Sorry, but no one of our happy customers stay on forums, or have time to post feedback on some trusted site. All feedbacks is written directly to our mail, and it will not show you any proof if we'll post it on our own page. And even if you'll find a feedback on an page, it was write by a random person, who don't have with as any business.

How I would can to know that you are not a scammer as else?
Simply, we don't take any prepayments. We are only who ask just for proof that you have this money in your wallet, and you'll to arrange full escrow on trusted for both third party site.

Ask more, we'll add more.

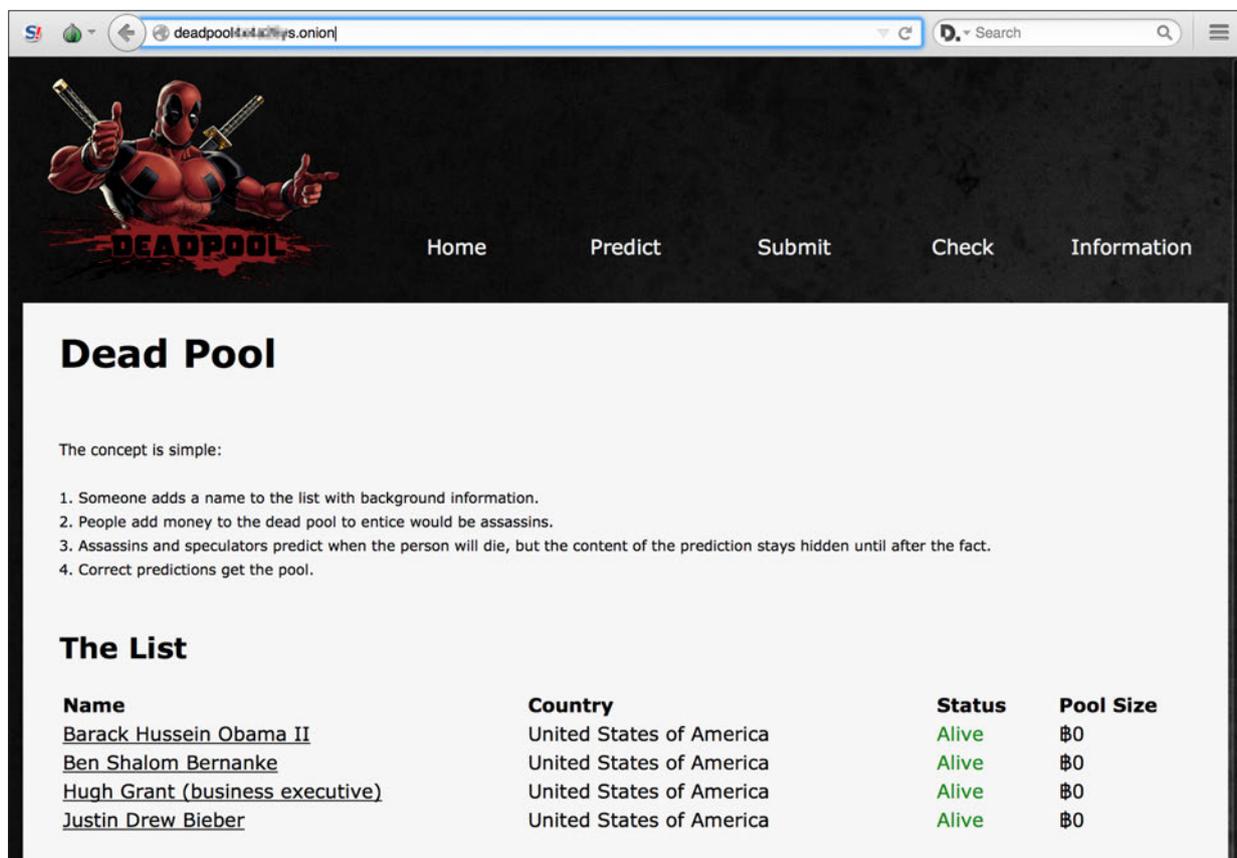
We should probably get started if you'll have at least this:

Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$45,000	\$90,000	\$180,000
Missing in action	\$60,000	\$120,000	\$240,000
Death in accident	\$75,000	\$150,000	\$300,000
Cripple Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$12,000	\$24,000	\$48,000
Uglify	\$18,000	\$36,000	\$72,000
Two Hands	\$24,000	\$48,000	\$96,000
Paralyse	\$30,000	\$60,000	\$120,000
Rape	Low Rank	Medium Rank	High Rank and Political
Regular	\$7,000	\$14,000	\$28,000
Under age	\$21,000	\$42,000	\$84,000
Bombing	Low Rank	Medium Rank	High Rank and Political
Simple	\$5,000	\$10,000	\$20,000
Complex	\$10,000	\$20,000	\$40,000
Beating	Low Rank	Medium Rank	High Rank and Political
Simple	\$3,000	\$9,000	\$18,000

C'thulu's resume as an assassin for hire

As shown, prices vary based on the preferred manner of death or injury and the target's status. Ross Ulbricht who has been recently convicted of running the infamous Silk Road forum for illegal drugs, in fact, attempted to have five of the partners he had fallen out with assassinated [22].

A different take on such services, one that we hope is not actually meant as a real service, is “crowdsourced assassination.” One site—Dead Pool—allows users to put forward potential targets. Others can then contribute funds in the form of Bitcoins to the “dead pool.” Assassins can then anonymously “predict” when and how the targets will die. If the person actually dies, all predictions are revealed and the assassins who put forward an exact match can claim the money. To date, four names have been put forward but no money has been placed into the pools, leading us to believe that the site is a hoax.



Dead Pool, a site for crowdsourced assassinations



SECTION III

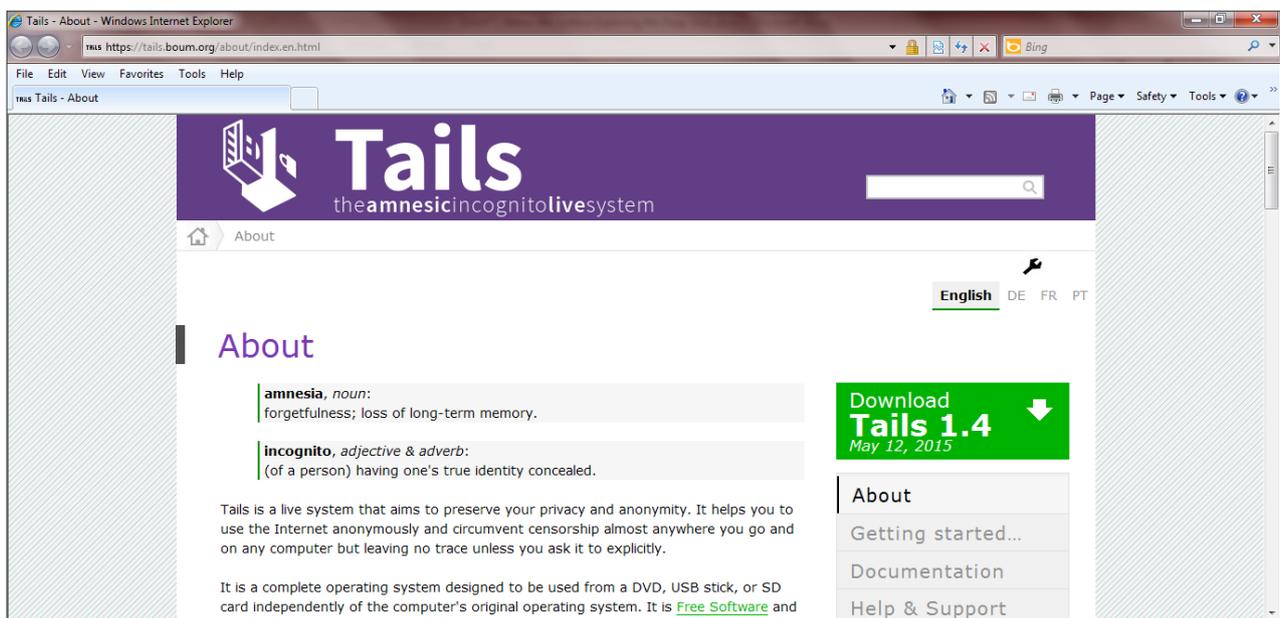
The Deep Web and the real world

The Deep Web and the real world

Mainstream adoption

Services that rely on rogue TLDs or Namecoins offer too high an adoption barrier to common users and very few advantages for average users to be considered publicly significant. But we've witnessed more and more usability improvements in systems like I2P and especially TOR that have slowly become viable solutions for everyone to go anonymous with hardly any setup requirements.

TOR applications with anonymous browsers integrated are readily available for all major desktop and mobile platforms, allowing everyone to go anonymous and to access hidden sites in just a few touches. For journalists and people requiring an even higher level of privacy, a fully tailored OS integrating TOR and anonymous browsers can be downloaded and installed on a USB key for use on any available machine.



Example of a downloadable anonymity program

True anonymity

In practice, traffic between two TOR nodes is not traceable, but that to and from entrance and exit TOR gateways are. If an organization operates enough TOR gateways, there is a possibility that traffic using the TOR network can be tracked. Using TOR in countries that don't have enough budgets to operate a critical mass of gateway nodes can be considered safe. But in other countries with high intelligence service budgets like the United States or China, using TOR may not be as safe.

In addition, any anonymizing system is only as effective as its user. As advanced as an anonymizing system may be, even those like TOR and I2P only cover the transport layer of communication but remain powerless toward the content of communication. Simply put, no anonymizing system can hide a user who posts his/her home address and details in the open.

We can, therefore, list two major types of risk linked to anonymity in the Deep Web:

- Environmental vulnerabilities
- Social vulnerabilities

Environmental vulnerabilities refer to every possible flaw that can be linked to **other** software used together with TOR. For example, a notorious bug affecting the Adobe® Flash® version embedded in the browser that comes with a version of TOR once put the whole system in jeopardy since it was possible to exploit the bug to leak sensitive data despite the use of TOR.

Social vulnerabilities are related to user behavior and the precautions users may take other than simply using TOR. Dread Pirate Roberts who was recently convicted to life in prison due to his Deep Web marketplace was caught by the FBI due to his use of a private email address in a public forum. Correlating the identities of Deep Web users with their Surface Web alter egos is an interesting research field that involves disciplines like social network analysis and stylometry.

“If you go to the doctor and undergo surgery and you wake up in your hospital room and violate all the hygiene rules, you will die even if you have the best surgeons, the best tools, the best hospital. Same thing with anonymity, if you are behaving in an unwise manner, even the best tool can't protect you.”

—Martin Rösler,
Senior Director,
Threat Research

Law enforcement and the Deep Web

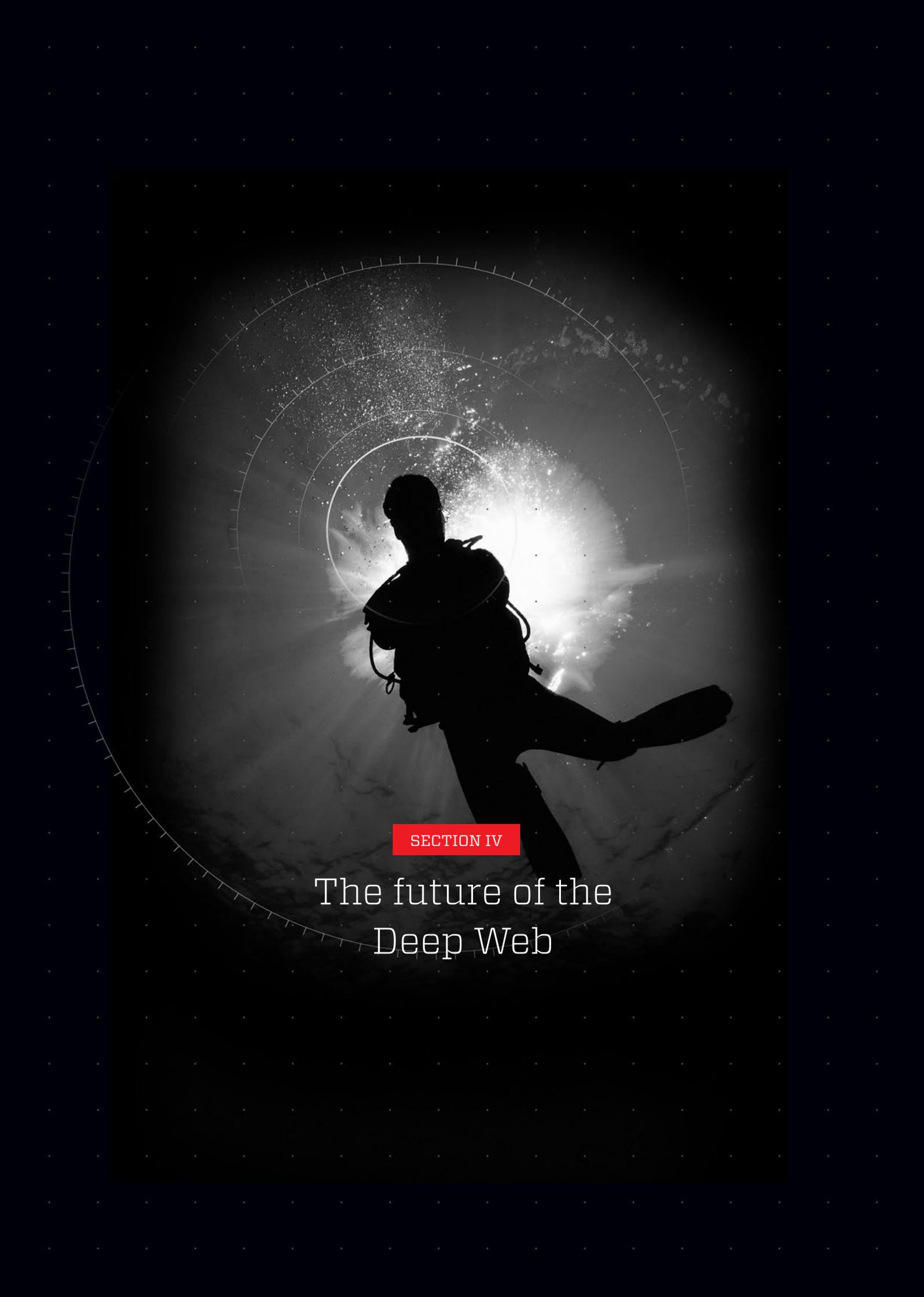
Law enforcement agencies already face several existing challenges when it comes to international crime on the Surface Web [23, 24]. With regard to the Deep Web, three additional aspects can make law enforcement even more problematic.

- **Encryption:** Everything in the Deep or Dark Web is encrypted. That means the criminals in it are much more aware about being trapped or monitored. Encryption is their very first countermeasure to evade detection.
- **Attribution:** It's extremely difficult to determine attribution. Everything happens on .onion domains. Routing to these domains is also unclear.
- **Fluctuation:** The Deep Web is a very dynamic place. An online forum can be at a specific URL one day and gone the next. The naming and address schemes in the Deep Web often change. This means that the information we harvested two weeks ago is no longer relevant today. This has implications in proving crime. Considering the time frame in which criminal cases are tried, law enforcers must be able to rigorously document any criminal online activity via time-stamped screenshots in order to prevent cases from becoming invalid.

The security vendors' role

While a majority of normal Internet users will not find use for the Deep Web, security vendors must still be able to protect their customers from the cybercriminal activities happening in it. As we've shown in previous sections, malware are increasingly using TOR for stealth so security vendors must be able to create early detection means and countermeasures against these threats, as they will, sooner or later, find their way to victimize users on the Surface Web.

On the other hand, there are users who, for legitimate reasons, need to visit the Deep Web to avoid the social pain of buying prescription drugs for certain conditions, access recreational drugs that are illegal in certain geographical locations, freely discuss socially banned topics, or share information from repressive countries with journalists. In these cases, security vendors still have a responsibility to protect their customers. This is why Trend Micro and its Forward-Looking Threat Research Team continue to monitor these online territories.

A black and white image featuring a diver's silhouette in the foreground, positioned as if looking through a circular opening. The opening reveals a bright, starry space scene with a large, glowing sun or star. Concentric circles with tick marks are overlaid on the scene, suggesting a search or scanning process. The overall mood is mysterious and futuristic.

SECTION IV

The future of the Deep Web

The future of the Deep Web

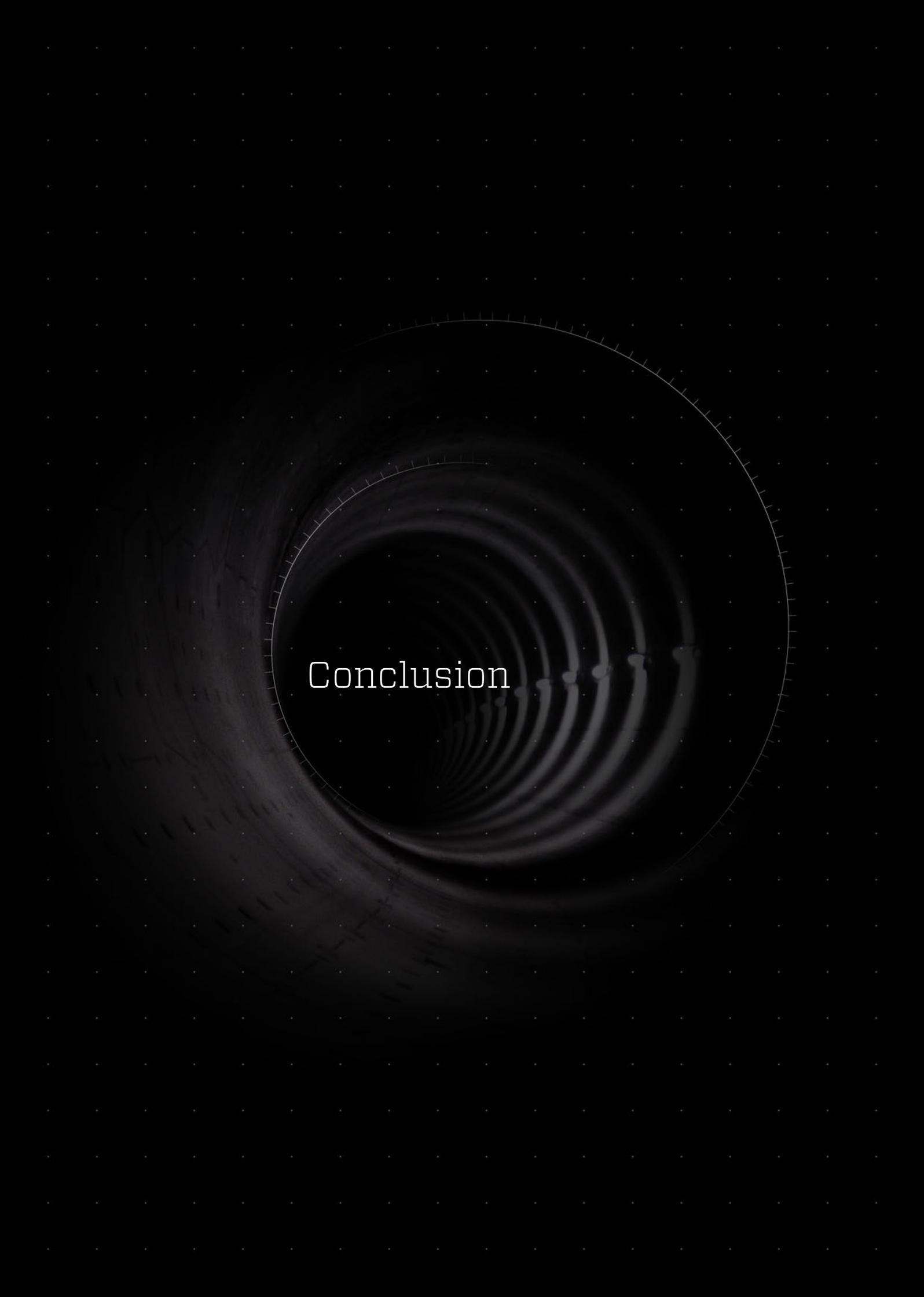
While public awareness may lead to the increased use of or interest in the Dark Web and other similarly intended sites in the Deep Web, users currently don't have enough reason to migrate their Internet browsing to specialized anonymizing software in the near future.

Meanwhile, it's much more likely for technological developments related to the Dark Web to improve the stealthiness of darknets. Right now, there seems to be a race between "extreme libertarians" and law enforcement agencies, with the former trying to find new ways to become even more anonymous and **untraceable by the latter**.

But since the commerce of illicit goods is one of the most predominant activities taking place in the Deep Web, it has become essential in the context of high anonymity, to be able to guarantee trust and reputation among sellers and buyers without having to rely on an external authority like a banking institution as in "canonical" ecommerce.

We are foreseeing the rise of new, completely decentralized marketplaces that rely on the blockchain technology that Bitcoins and other cryptocurrencies already exploit for transport and storage. As such, the technology will be used to implement full-blown marketplaces without a single point of failure and that rely on particular aspects of game theory to guarantee safe transactions, escrow mechanisms, and trust between actors who may be shady in nature to begin with.

Cryptocurrencies go hand in hand with Deep Web marketplaces. In that regard, we'll see new, advanced ways to make Bitcoins even less traceable than they are now. There's also a huge possibility for malware to start exploiting the blockchain technology to embed themselves and be carried around in a new, fully decentralized way.



Conclusion

Conclusion

The Trend Micro Forward-Looking Threat Research Team developed the Deep Web Analyzer—a robust system that collects Deep Web URLs of interest—to take a closer look at what’s going on in the Deep Web with regard to cybercrime. Based on two years’ worth of research into limited-access networks like the Dark Web via the Deep Web Analyzer, we were able to determine that the Deep Web hosts a lot of benign content, alongside some of the more disturbing activities ever seen on the Internet. We thus gained a deeper understanding of its nature:

- While 47% of the successfully scouted domains used English, Russian ousted English from the top spot when it came to URL count. This could be attributed to the existence of a large Russian forum at the time of analysis.
- The most heavily traded goods based on analysis of the top 15 vendors in the Deep Web were light drugs, followed by prescription medicine like Ritalin and Xanax and synthetic, prohibited drugs.
- The Deep Web heavily uses protocols outside the standard HTTP/HTTPS, most commonly IRC, IRCS, Gopher, XMPP, and FTP.
- We were able to identify thousands of suspicious pages, ranging from those that host malicious adware to those used for proxy avoidance and child exploitation.
- Certain parts of the Deep Web have become a safe haven for different cybercriminals and criminal activities:
 - Prevalent malware families like VAWTRAK and CryptoLocker are using TOR as part of their configuration.
 - Takedowns of criminal marketplaces are not particularly lasting or impactful solutions against the drug trade, as there continue to be dedicated online shops and forums that serve the demand for illicit drugs.
 - The Deep Web is also rife with Bitcoin-laundering services like EasyCoin to further increase the anonymity of moving money through the Bitcoin system.
 - A cybercriminal underground definitely operates in the Deep Web as well. Stolen accounts, passports, and identities of high-profile personalities are sold in professional-looking forums with complete pricing information and descriptions.
 - Assassination services are also advertised and offered in the Deep Web.

While it's not likely for a majority of Internet users to ever find reasons to use the Dark Web, anonymity in the Deep Web will continue to raise a lot of issues and be a point of interest for both law enforcers and Internet users who want to circumvent government surveillance and intervention. As such, security defenders like Trend Micro need to continue keeping tabs on the Deep Web as its role in the Internet grows.

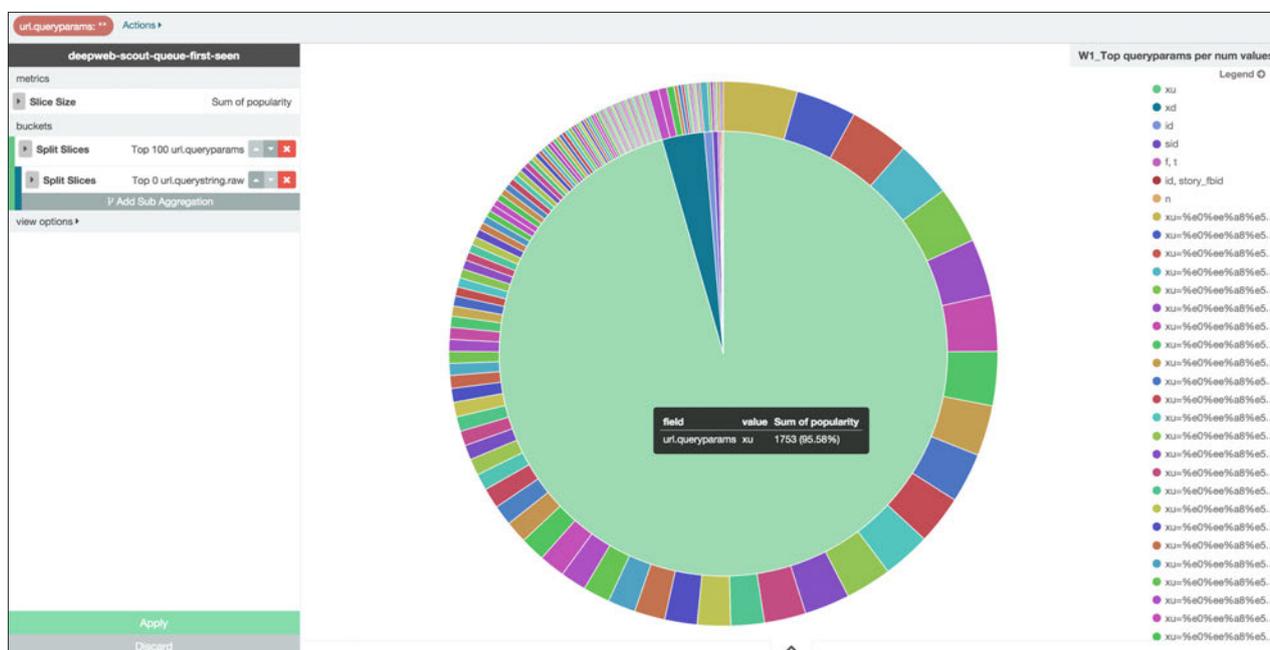
Appendix

Catching NionSpy (aka Mewsei or MewsSpy)

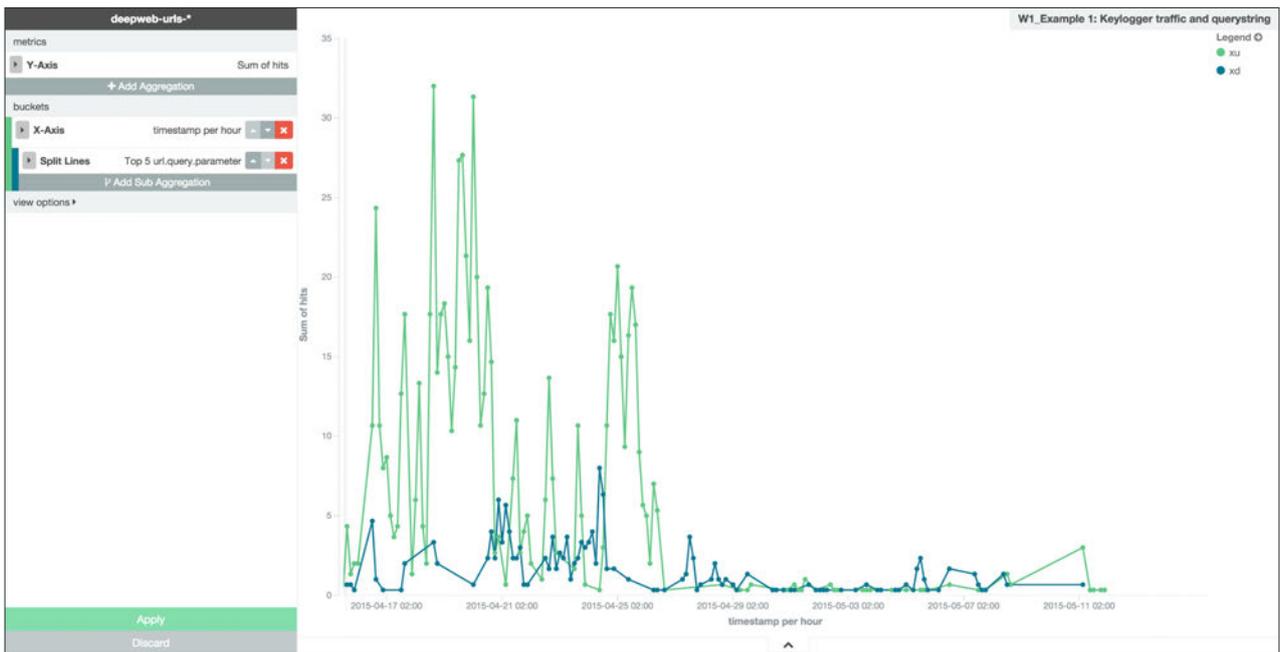
In the following example that is related to malware that steal confidential information, we looked for the prevalent query string's parameters in a short and recent time window. This allowed us to identify new threats as soon as they appeared in the Deep Web. In particular, two parameters—*xu* and *xd*—experienced a surge in popularity over the past week. *Xu* was associated with more than 1,700 distinct values consisting of binary blobs. Further investigation revealed that *xu* was used by NionSpy to leak stolen credentials (online banking, etc.) that are then captured by a keylogger and posted to a dropzone in the Deep Web. *Xd*, meanwhile, was used to register a new infection to the botnet. This registration included information like the victim's machine name and OS version, communicated in form of a JSON string like the following:

```
[REDACTED]2xx.oni on: 80/si.php?xd={"f155": "MACHINE IP", "f4336": "MACHINE NAME", "f7035": "5.9.1.1", "f1121": "windows", "f6463": "", "f2015": "1"}
```

By counting the queries associated with the registration, we were able to build a profile of the number of new victims per day, along with the amount of data leaked.



Most prevalent URI query string's parameters (by value)

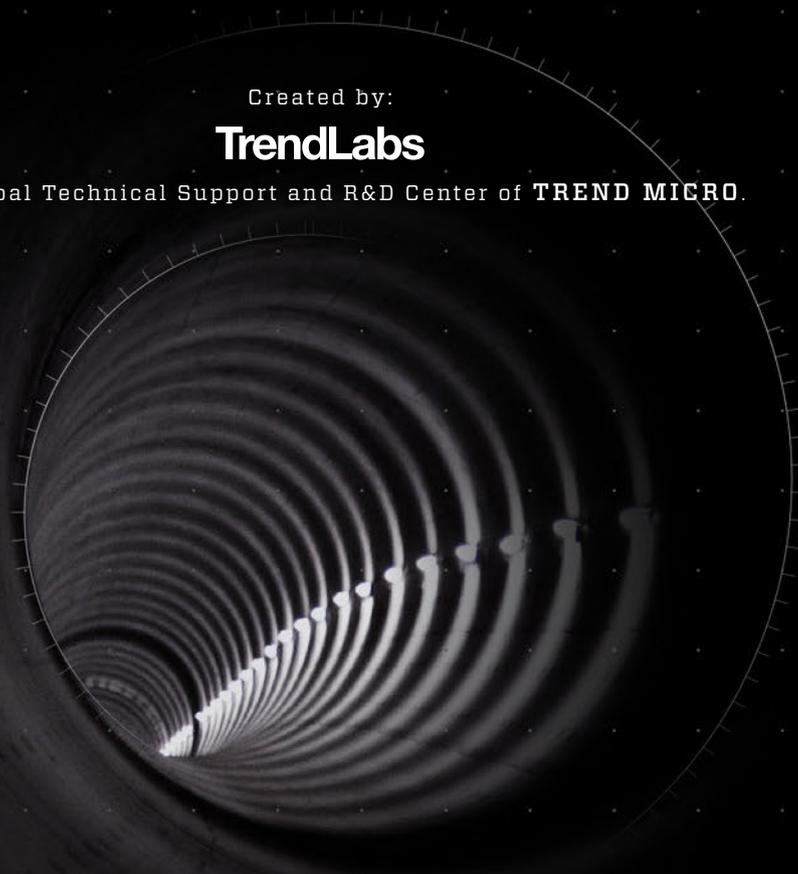


Number of new victims per day (in blue) and traffic to the drop zone (in green)

References

1. The Tor Project, Inc. *Tor Project*. Last accessed on 11 June 2015, <https://www.torproject.org/>.
2. ulbr_mirror. *Scribd*. "Ulbricht Criminal Complaint." Last accessed on 10 June 2015, <http://www.scribd.com/doc/172768269/Ulbricht-Criminal-Complaint>.
3. Vincenzo Ciancaglini, Marco Balduzzi, Max Goncharov, and Robert McArdle. *Trend Micro Security Intelligence*. "Deep Web and Cybercrime: It's Not All About Tor." Last accessed on 10 June 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf>.
4. Robert McArdle. (4 October 2013). *TrendLabs Security Intelligence Blog*. "Cybercrime in the Deep Web." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/cybercrime-in-the-deepweb/>.
5. Vincenzo Ciancaglini. (8 November 2013). *TrendLabs Security Intelligence Blog*. "The Boys Are Back in Town: Deep Web Marketplaces Back Online." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-boys-are-back-in-town-deep-web-marketplaces-back-online/>.
6. Vincenzo Ciancaglini. (10 March 2015). *TrendLabs Security Intelligence Blog*. "The Deep Web: Shutdowns, New Sites, New Tools." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-deep-web-shutdowns-new-sites-new-tools/>.
7. Robert McArdle and David Sancho. *Trend Micro Security Intelligence*. "Bitcoin Domains." Last accessed on 10 June 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-bitcoin-domains.pdf>.
8. *The Invisible Internet Project*. Last accessed 11 June 2015, <https://geti2p.net/en/>.
9. Trend Micro Incorporated. *Trend Micro Security News*. "Cybercriminal Underground Economy Series." Last accessed 11 June 2015, <http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/index.html>.
10. Feike Hacquebord. (5 September 2015). *TrendLabs Security Intelligence Blog*. "The Mysterious MEVADE Malware." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/the-mysterious-mevade-malware/>.
11. Jay Yaneza. (28 January 2014). *TrendLabs Security Intelligence Blog*. "Defending Against TOR-Using Malware, Part 1." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-TOR-using-malware-part-1/>.
12. Jay Yaneza. (4 February 2014). *TrendLabs Security Intelligence Blog*. "Defending Against TOR-Using Malware, Part 2." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-TOR-using-malware-part-2/>.
13. David Sancho. (5 May 2015). *TrendLabs Security Intelligence Blog*. "Steganography and Malware: Why and How." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-why-and-how/>.
14. David Sancho. (5 May 2015). *TrendLabs Security Intelligence Blog*. "Steganography and Malware: Concealing Code and C&C Traffic." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-concealing-code-and-cc-traffic/>.
15. David Sancho. (11 May 2015). *TrendLabs Security Intelligence Blog*. "Steganography and Malware: Final Thoughts." Last accessed on 10 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-final-thoughts/>.
16. Kate Vinton. (30 May 2015). *Forbes*. "Silk Road CreaTORRoss Ulbricht Sentenced to Life in Prison." Last accessed on 10 June 2015, <http://www.forbes.com/sites/katevinton/2015/05/29/ulbricht-sentencing-silk-road/>.
17. Trend Micro Incorporated. (1 June 2015). *Trend Micro Security News*. "The Deep Web: Anonymizing Technology for the Good... and the Bad?" Last accessed on 11 June 2015, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-deep-web-anonymizing-technology-good-and-bad>.

18. Damon Lavrinc. (6 December 2013). *Wired*. “Someone Bought a Tesla Model S with Bitcoins.” Last accessed on 11 June 2015, <http://www.wired.com/2013/12/tesla-bitcoin/>.
19. Max Goncharov. (2012). *Trend Micro Security Intelligence*. “Russian Underground 101.” Last accessed on 11 June 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>.
20. Max Goncharov. (2014). *Trend Micro Security Intelligence*. “Russian Underground Revisited.” Last accessed on 11 June 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf>.
21. Lion Gu. (2014). *Trend Micro Security Intelligence*. “The Chinese Underground in 2013.” Last accessed on 11 June 2015, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-chinese-underground-in-2013.pdf>.
22. Andy Greenberg. (2 February 2015). *Wired*. “Read the Transcript of Silk Road’s Boss Ordering 5 Assassinations.” Last accessed on 11 June 2015, <http://www.wired.com/2015/02/read-transcript-silk-roads-boss-ordering-5-assassinations/>.
23. Martin Rösler. (12 January 2014). *TrendLabs Security Intelligence Blog*. “Working with Law Enforcement in 2014 and Beyond.” Last accessed on 11 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/working-with-law-enforcement-in-2014-and-beyond/>.
24. Martin Rösler. (11 July 2013). *TrendLabs Security Intelligence Blog*. “Law Enforcement Cooperation and Trend Micro.” Last accessed on 11 June 2015, <http://blog.trendmicro.com/trendlabs-security-intelligence/law-enforcement-cooperation-and-trend-micro/>.



Created by:

TrendLabs

The Global Technical Support and R&D Center of **TREND MICRO**.

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com



Securing Your Journey
to the Cloud