

Cybercrime in the Deep Web

Black Hat EU, Amsterdam 2015

Introduction

The Deep Web is any Internet content that, for various reasons, cannot be or is not indexed by search engines like Google. This definition thus includes dynamic web pages, blocked sites (like those where you need 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 sites with domain names that have been registered on Domain Name System (DNS) roots that are not managed by the Internet Corporation for Assigned Names and Numbers (ICANN), like .BIT domains, sites that are running on standard DNS but have non-standard top-level domains, and finally, darknets. Darknets are sites hosted on infrastructure that requires specific software like Tor before it can be accessed. Much of the public interest in the Deep Web lies in the activities that happen inside darknets.

What are the Uses of the Deep Web?

A smart person buying recreational drugs online will not want to type keywords in a regular browser. He/she will need to go online anonymously, using an infrastructure that will never lead interested parties to his IP address or physical location. Drug sellers as well, will not want to set up shop in online locations where law enforcement can easily determine, for instance, who registered that domain or where the site's IP address exists in the real world.

There are many other reasons apart from buying drugs why people would want to remain anonymous, or to set up sites that could not 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 but do not want the paper trail. Dissidents in restrictive regimes may need anonymity in order to safely let the world know what is happening in their country.

But on the other side of the coin, people who want to plot an assassination versus a high-profile target will want a method that is guaranteed to be untraceable. Other illegal services such as the selling of documents like passports and credit cards will also require an infrastructure that will guarantee anonymity. The same could be said for people who leak other people's personal information like addresses and contact details.

The Clear Web vs The Deep Web

When discussing the Deep Web, it's inevitable that the phrase "Clear Web" will pop up. It's exactly the opposite of the Deep Web—the portion of the Internet that can be indexed by conventional search engines and accessible via standard web browsers without the need for special software and configurations. This "searchable Internet" is called the Clear Web.

The Dark Web vs The Deep Web

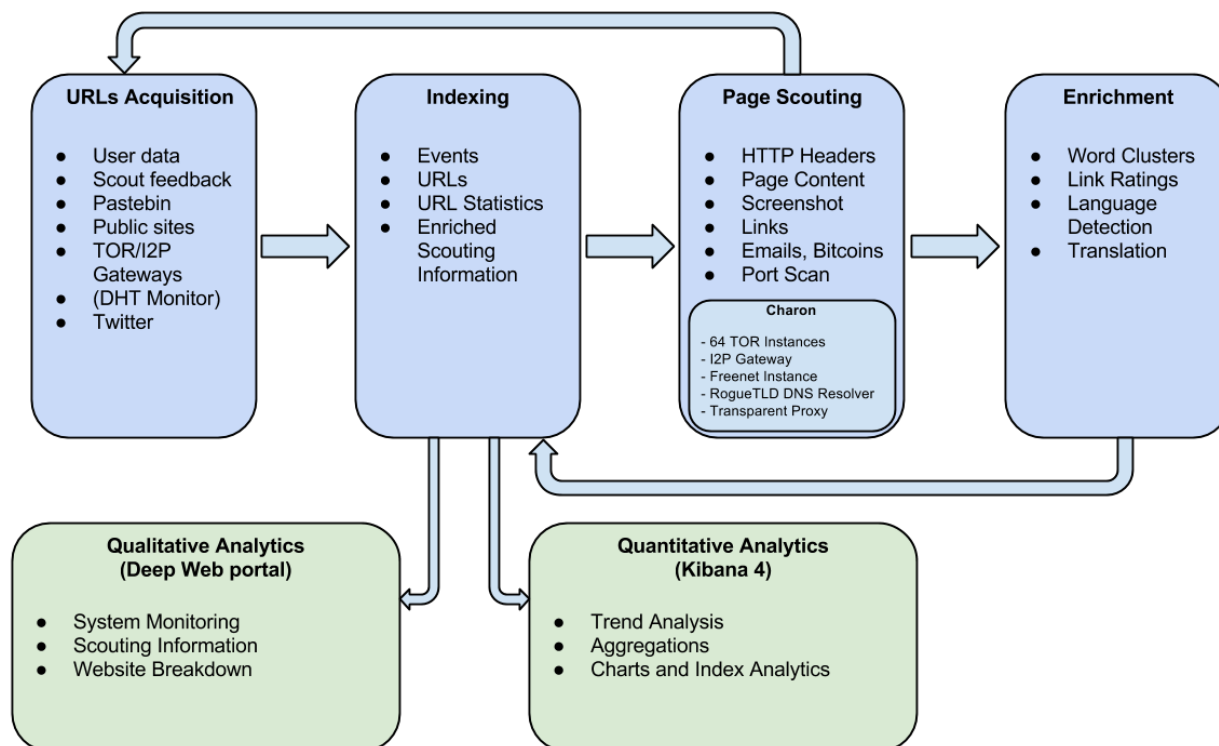
There is much confusion between the two, with some outlets and researchers freely interchanging them. However, the Dark Web is not the Deep Web; it is only part of the Deep Web. The Dark Web relies on darknets, networks where connections are made between trusted peers. Examples of Dark Web systems include Tor and the Invisible Internet Project (I2P).

Deep Web Analyzer

The Deep Web Analyzer (DeWA) has been designed with the goal of supporting investigations in tracking down malicious actors, exploring new threats and extracting meaningful data from the Deep Web, e.g. new malware campaigns.

DeWA consists of the following 5 modules:

1. A Data Collection module, responsible for finding and storing new URLs from multiple sources
2. A Universal Gateway, which allows to access the hidden resources in darknets like TOR and I2P, and to resolve custom DNS addresses
3. A Page Scouting module, responsible for crawling the new URLs collected
4. A Data Enrichment module that takes care of integrating the scouted information with other sources
5. A Storage and Indexing module, which make the data available for further analysis
6. Visualization and analytic tools



System Overview

Data Collection

The first DeWA module consists on a data collection module, whereas data consists of fresh URLs related to either:

- Hidden services hosted in TOR and I2P
- Freenet resource locators
- .bit domains
- other domains with a non-standard TLD, falling in the list of TLDs handled by some known alternative domain registrars

Our monitoring infrastructure is based on:

- User data, checking HTTP connections to hidden services or non-standard domains
- Pastebin-like sites, checking for snippets of text containing Deep Web URLs
- Public forums (reddit etc...), looking for posts containing Deep Web URLs
- Sites collecting Deep Web domains, such as deepweblinks.com or darkspider.com;
- TOR Gateways statistics, such as tor2web.org: these sites allow users to access hidden services without installing TOR, and keep publicly available statistics about what domains are accessed the most on a daily basis;
- I2P resolution files: as a way to speed up hostname resolution in I2P, it is possible to download some precompiled host lists from a number of hidden sites. We save that list to find new interesting domains;
- Twitter, looking for tweets containing Deep Web domains or URLs.

Data is indexed in a way that we discover new domains, and also perform traffic analysis on the individual URL components – e.g., an analysis that allows us to find new malware campaigns.

Universal Deep Web Gateway

As we mentioned previously, Deep Web resources are hard to access. Darknets like TOR and I2P require a dedicated software that acts as a proxy, while alternative DNS systems and rogue TLDs need the use of dedicated DNS servers to resolve an address. In order to make all these operations convenient and fast, we have deployed Charon, a transparent proxy server that routes an HTTP request to the appropriate system based on the format of URLs.

Depending on the kind of URLs being accessed, Charon connect to:

- 64 load balanced TOR instances
- an I2P instance
- a Freenet node
- a custom DNS Server able to do every custom TLD resolution

Page scouting

For every collected URL, we perform what we call “scouting”, i.e. we try to connect to the URL and save the response data. In case of error, the full error message is stored, to understand if the connection failed

due to domain resolution error, server-side error, transport error, etc. In case of HTTP errors, the full HTTP headers are stored, a practice that has already proven to be successful to identify malware related hosts, who are known to answer only to specific type of HTTP requests and will fail otherwise.

In case of success, we use a headless browser to extract relevant information from the downloaded page:

- We log all the HTTP Headers, and follow any HTTP redirection chain;
- We perform the full rendering of the page's DOM (in order to get dynamic javascript pages out of the way);
- We take a page's screenshot;
- We compute the page's size and md5;
- We extract the page's metadata: title, meta tags, resources, keywords;
- We extract the text stripped of all the HTML;
- We extract all the links from the page;
- We collect the email addresses found in the page.
- The extracted URLs are "back-fed" to the data collection module and indexed as an additional data source.

Data Enrichment

Data enrichment of the scouted data consists, for every successfully scouted page, of the following operations:

- Language detection of the page;
- Translation, using Google Translate, of every non-English page to English;
- Link ratings and classification via Web Reputation System;
- Significant WordCloud generation using semantic clustering.

The last operation relies on a custom clustering algorithm that generates a WordCloud of the site, i.e. containing the most significant information. The algorithm works as follows:

1. The page text is tokenized in its individual words and the number of occurrences for each word;
2. Words are filtered, only substantives are kept while other elements such as verbs, adjectives etc. are discarded. Substantives are normalized, so to keep only the singular form;
3. The semantic distance matrix is computed: this is a matrix containing how "close" each word is to each other, using a so-called WordNet metric. The WordNet metric works by measuring the taxonomical distance of every word in the general language. As an example, words like "baseball" and "basketball" will score fairly close to one another since both are "sports". The same way, "dog" and "cat" will be considered close since they are both "animals". On the other hand, "dog" and "baseball" will be considered pretty far from each other;
4. Once we have the distance of every word pair, words are clustered together starting from the closest one in increasing distance. We create this way groups of words with similar meaning;
5. Clusters are labeled using the first word in alphabetical order as label, and scored summing up the occurrences of every word in the cluster;
6. Using the labels and scores of the top 20 clusters, a WordCloud is generated and drawn.

This allows an analyst for a quick glance around the main topics of a page.

Storage and Indexing

Both URL feeds and scouting information are stored in an Elasticsearch cluster and indexed according to different criteria. Scouting information is indexed as one document per page, and made searchable by Elasticsearch capabilities. This way relevant keywords can be searched throughout millions of pages with text queries. URL information is also processed to store relevant statistics for each URL component. This allows us, for example, to determine when a hostname has been spotted in the system and how popular a certain URL is in our data. Other uses are knowing when a specific pair of hostname + query parameter first appeared and how frequently is a given URL path across all domains.

UI and visualization

In order to access and manipulate the data, we rely on three different front-end systems:

- For the so-called *qualitative analysis*, we developed a *Deep Web Portal*. This tool is aimed at investigators to search through the Deep Web for interesting indicators. We offer different visualizations, namely: a Website breakdown, that allows to navigate all the Deep Web URLs by hostname, path, query string and search by URL components; a URL Summary, showing the entire list of collected URLs; a Scouting summary, presenting the scouted pages individually, and allowing searches in the page content, rather than in the URL.
- For the so called *quantitative analysis*, we rely on Kibana for advanced statistics and realtime metric calculations on the data. It offer a first tab for data exploration, and a Visualization tab that allows for the plotting of charts according to different data metrics and aggregations.
- For more advanced data inspection, we rely on an iPython notebook, enriched with custom libraries, that allows us to run python scripts against the Elasticsearch cluster, to inspect the data natively and to compile detailed reports inline.

The State of the Deep Web

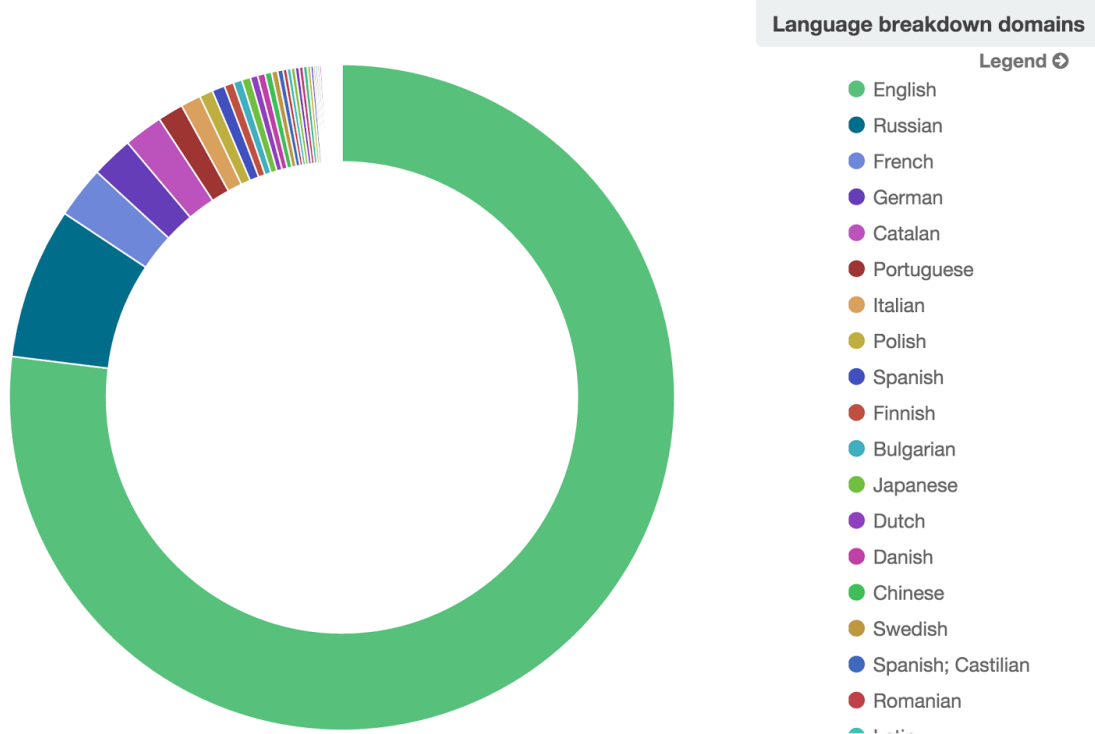
In this Section we provide some use cases related to the information collected and extracted with our system.

A first analysis over the past 2 years of collected data concerns the language distribution of all existing Deep Web webpages.

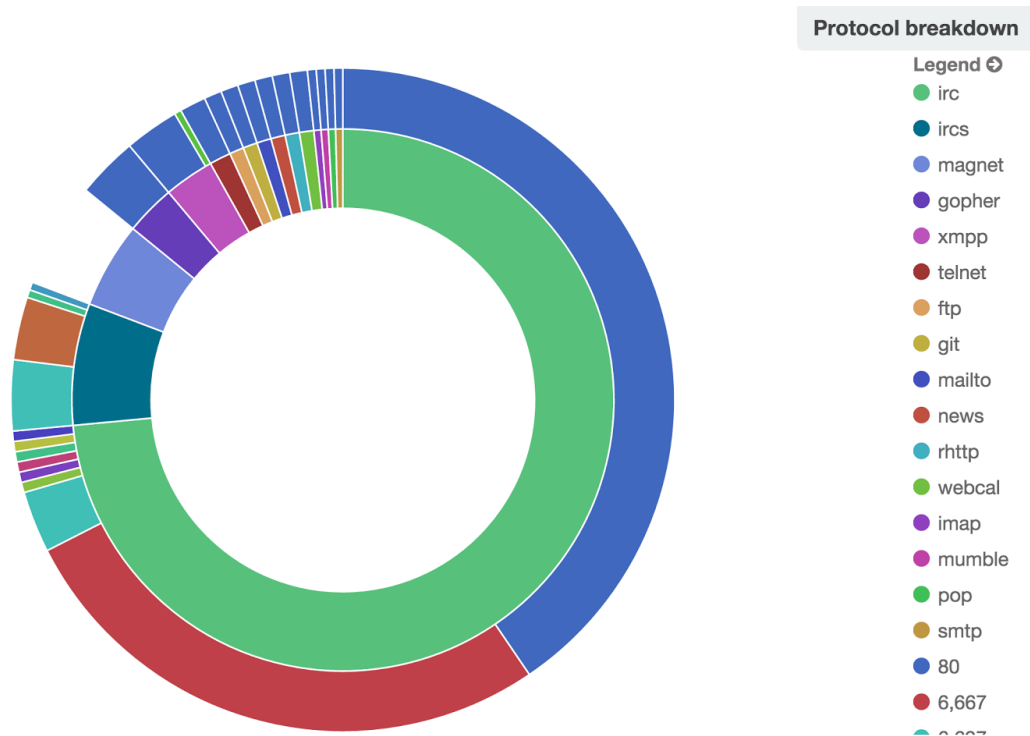
Language detection is performed using two different methods: A Python module called `guess_language`, which adopts a trigram-based algorithm and works offline (a); Google Translate (b). The individual results are compared in order to overcome each system's limitations: for example, Google Translate has no concept of "unknown language" (for example when there is no data in a page), but rather defaults to English in case of doubt, hence creating a huge bias in the data.

The following figure shows the language popularity according to the number of domains containing pages in said language. In computing the statistics we have filtered out pages smaller than 1kb (since they would not bear enough data to perform a reliable detection) and all pages classifieds as "unknown")

In terms of raw number of domains (who, unless in case of a page hosting provider like "Geocities in the Deep Web" could be, almost always correspond to the actual number of different sites) we see that English is the language of choice here, with more than 75% domains. Second for variety comes Russian, followed by French (which might include, of course, both French and French Canadian sites).



In the next example, we have grouped 2-years of data according to the URLs' scheme (e.g. http, https, ftp...). Of all the collected domains, almost 22.000 are (predictably) associated to http(s) protocol, being data hosting the principal activity. But if we filter out those domains, the remainder shows some interesting data, as portrayed by figure:



More than 100 domains are in fact hosting IRC(S): these are normally chat servers that can either be used as a rendezvous point for malicious actors to trade goods, or as a communication channel for botnets. Same concept applies to the 7 XMPP domains (i.e., Jabber-like IMs), representing another protocol for chat servers running in TOR.

Examples of malicious activities in the Deep Web

The goods and services we found offered in the Deep Web very well translate the kinds of transactions people try to get into if their anonymity was guaranteed. The lack of proper identification presents a high risk, but it also provides an obscure sense of security that grants them the freedom to offer mostly illegal goods and services. Also, unlike in the cybercriminal underground, most types of activities we saw in the Deep Web have more drastic effects to the “real world”.

We can't vouch for the authenticity of the goods and services discussed here, only for the fact that the sites advertising them do exist. We weren't able to cover all of the possible goods and services offered, but included several of the major categories that should give a clear idea of the nature of transaction that goes on in the deep web.

Passports / Citizenship for sale

Passports and ID are uniquely powerful documents – and fake ones even more so. They act not only as a form of identification for crossing borders (including ones the buyer could normally not easily cross), but also can be used for everything from opening of bank accounts, apply for loans, purchasing property and much more – so it of no surprise that they are a valuable commodity. There are several sites on the Deep

Web claiming to sell passports and other forms of official ID, with prices varying from country to country, and seller to seller.

As mentioned in the Intro the validity of such services is hard to verify without actually purchasing from them, and especially in the cases of things like Citizenship these services may well be simple scams preying on the vulnerable people in different countries who are looking to obtain citizenship in order to remain in that country.

Become a citizen of the USA, real USA passport

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

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.

Product	Price	Quantity
Your USA citizenship	5900 USD = 25.624 €	1 x Buy now

USA Citizenship for sale for under 6000 USD

<http://xfnwyig7olydq5r.onion/>



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



Pricing information and samples for fake passports and other documents

<http://fakeidigiymbgpu.onion>

References:

[1] <http://xfnwyig7olypdq5r.onion/> - USA Citizenship

[2] <http://vfgnd6mieccqyit.onion/> - UK Passports

[3] <http://fakeidigiyumbgpu.onion/> - Fake Passports, many countries

Stolen Accounts for Sale

The buying and selling of stolen accounts is most definitely not restricted to the Deep Web alone – this is a very common practice among all of the criminal underground forums that exist on the Clear Web, and something that we have written extensively about in the past in reports on the Russian [1][2] and Chinese [3] speaking undergrounds. Accounts for credit cards, banking, online auction sites and gaming are probably among the most common of such sites being sold.

As is the case on the Clear Web, prices vary a lot among different sites – but more mature offerings (such as stolen Paypal accounts below) will tend to reach a generally accepted pricing norm. Accounts such as these are sold in one of two ways – either as “high quality”, verified accounts – where the exact current balance is known; or as bulk amounts of unverified accounts – but normally with a guarantee that at least a certain percentage will be valid. The first of these two categories can normally be seen as a higher cost item, but with greater likelihood of return of investment for a buyer – whereas the bulk account sales will be significantly cheaper.

Product	Price	Quantity
100 PayPal accounts	100 USD = 0.434 ₿	1 X Buy now
100 Ebay accounts	100 USD = 0.434 ₿	1 X Buy now
100 CCs with CVV2	150 USD = 0.652 ₿	1 X Buy now

Unverified accounts sold in bulk – 80% valid or replacement offered

<http://3dbr5t4pygahedms.onion/>

One offering that can be found quite readily on the Deep Web that is more unusual to find on the Clear Web is actual physical credit cards being sold. That is not to say these do not exist on the Clear Web

criminal forums – they most certainly do – however the sites on the Deep Web seem a bit more professional in their approach.



Replica credit cards created with stolen details

<http://cccrckysxm6avu.onion/>

References:

- [1] <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>
- [2] <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf>
- [3] <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-chinese-underground-in-2013.pdf>
- [4] <http://paypal4ecnf7eyqa.onion> - Stolen Paypal accounts
- [5] <http://3dbr5t4pygahedms.onion/> - Unverified stolen accounts
- [6] <http://cccrckysxm6avu.onion/> - Replica stolen credit cards

Assassination Services

Perhaps one of the most worrying services on the Deep Web – and definitely one that would be very foolish to advertise on the Clear Web – is the service of Hitman for Hire, or Assassination. Several such services exist on the Deep Web. Even the sites themselves acknowledge the highly secret nature of how they have to conduct their business – one site clearly states that as all contracts are private they cannot offer proof of past work, give feedback from previous clients or show any other proof of past success.

Instead they ask the person to prove upfront that they have enough Bitcoin available for the job by placing the bitcoin with a reputable (by criminal standards) escrow service. Only when the hitman has carried out the assassination and provided proof, the funds be released.

Email: BM-2cVbNcn18dhfcefbaX73USLq4dYTtAxW7U@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 an 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:

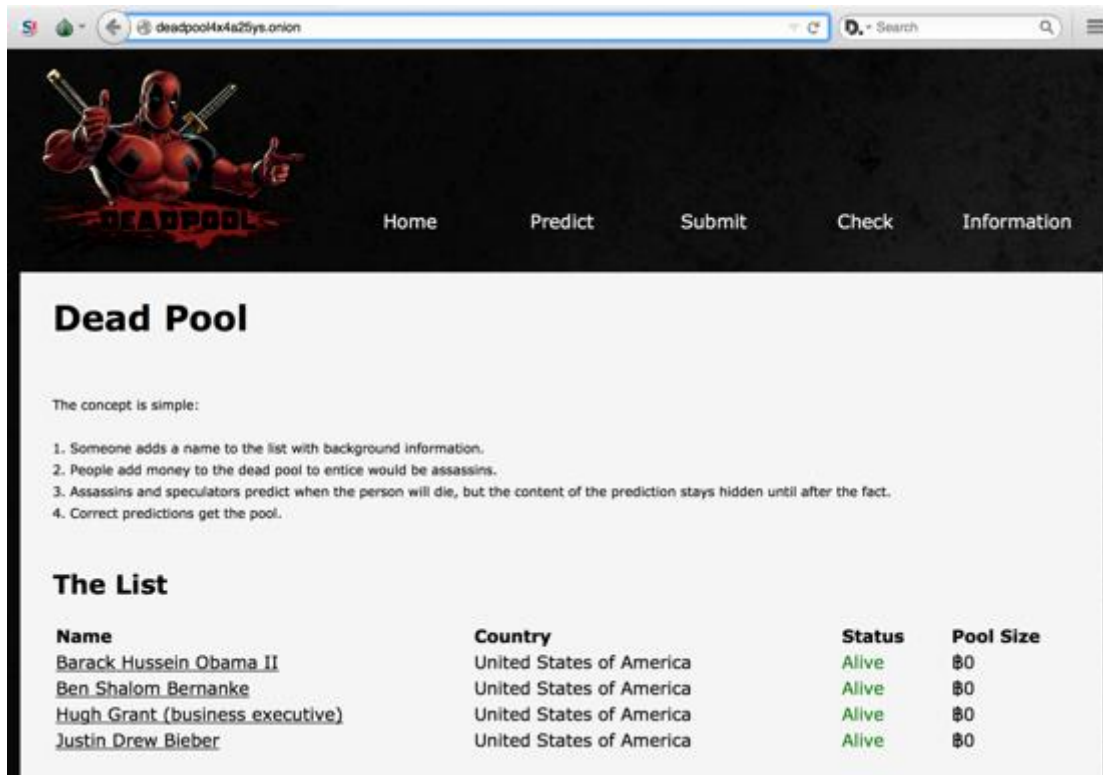
Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$45,000	\$90,000	\$180,000
Missing in action	\$60,000	\$120,000	\$240,000
Death in accident	\$75,000	\$150,000	\$300,000
Cripple Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$12,000	\$24,000	\$48,000
Uglyfy	\$18,000	\$36,000	\$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 Resume – Assassination Services for Hire

<http://cthulhuuap7ch47k.onion>

As can be seen in the screenshot above, pricing varies based on the manner of death or injury, but also by the status of the target. In fact Ross Ulbricht, the man recently convicted of running the infamous Silk Road forum for illegal drugs, attempted or order 5 assassinations of partners and others that he had fallen out with [1].

A different take on such services, and one that we hope if not actually meant as a real service is “crowdsourced assassination”. One site, Deadpool, operates by users putting forward potential targets. Others can then contribute funds via bitcoin to the “dead pool”. Assassins can then anonymously “predict” when and how the person will die. If the person does actually die, all the predictions are revealed and if there is an exact match – the assassin who put it forward will claim the money. To date 4 names have been put forward, but not money has been entered into the pools – making us believe that this is a hoax site.



Deadpool – Crowd Sourced Assassination

<http://deadpool4x4a25ys.onion>

References:

[1] <http://www.wired.com/2015/02/read-transcript-silk-roads-boss-ordering-5-assassinations/>

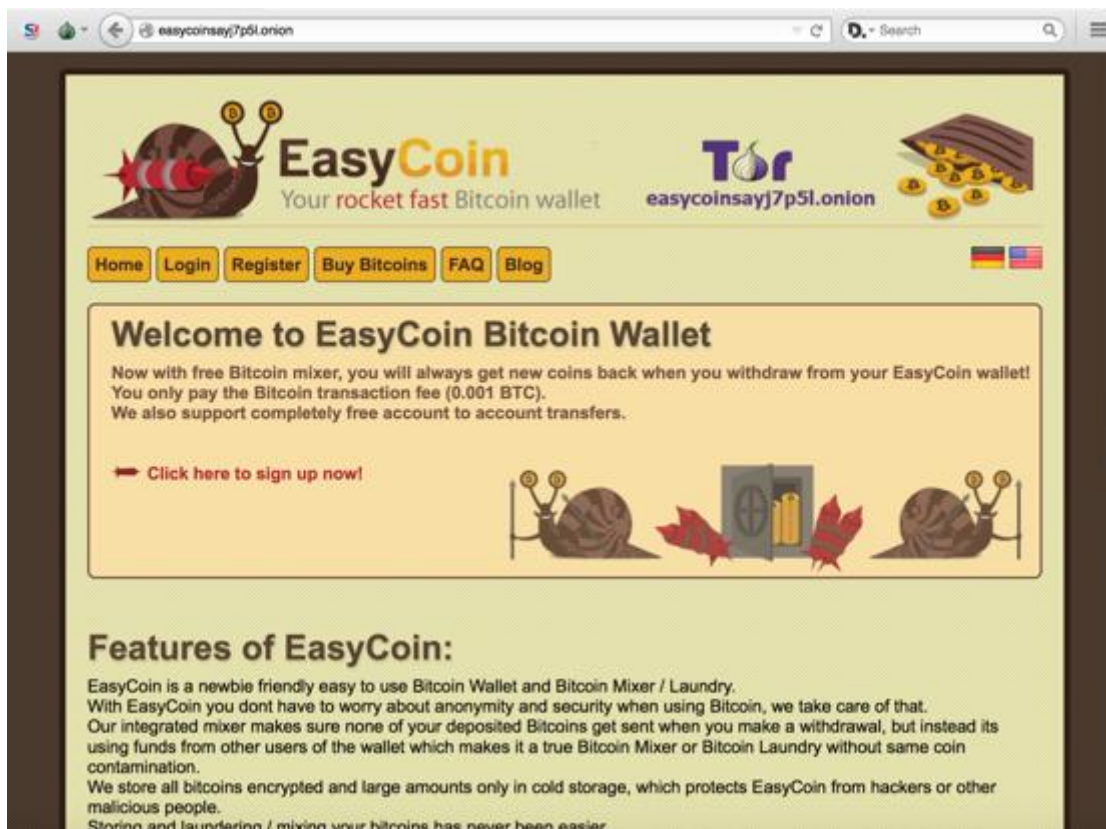
[2] <http://cthulhuuap7ch47k.onion/> - Contract Killers (C'thulu Resume)

[3] <http://deadpool4x4a25ys.onion/> - Crowdsourced assassination

Bitcoin and Money Laundry

By itself Bitcoin is a currency designed with anonymity in mind, and as a result it is frequently used when purchasing illegal goods and services (and of course legitimate goods as well [1]). But while on one hand all Bitcoin transactions are anonymous, as long as you do not link your wallet code to your real identity, on the other they are fully public. Due to the setup of the Bitcoin blockchain every transaction is fully public – and can be examined by investigators. So tracking money as it moves through the system is doable, albeit quite difficult.

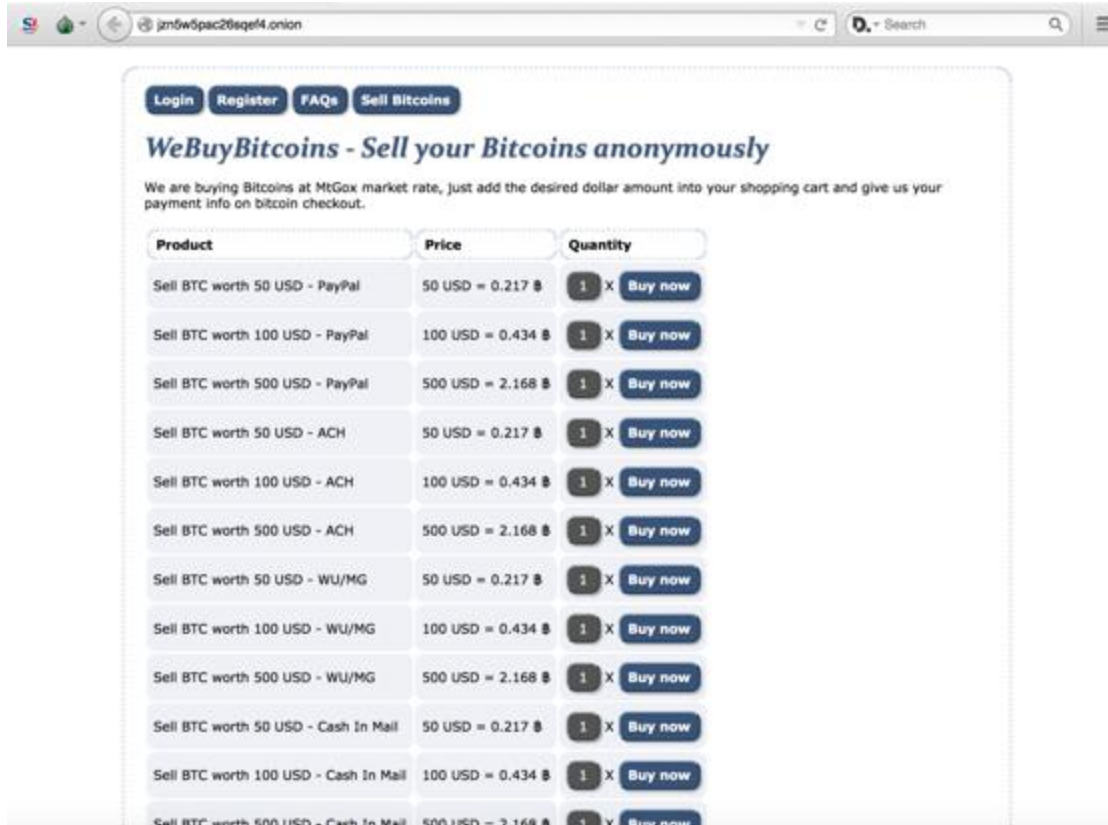
As a result a number of services have come about to add further anonymity into the system – making the electronic currency even more difficult to track. They generally achieve this by “mixing” your bitcoin [2][3] – essentially transferring them through a spidery network of micro transactions before returning 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 laundry service

<http://easycoinsayj7p5l.onion>

Bitcoin laundry services help to increase anonymity of money moving through the bitcoin system, but ultimately most bitcoin users will wish to extract the money from the system to be turned into cash or other types of traditional payment means. Several anonymous services exist in the Deep Web for this purpose – to exchange Bitcoin for money via Paypal, ACH, Western Union or even cash sent directly in the mail.



WeBuyBitcoins – Exchanging Bitcoin for cash or electronic payments
<http://jzn5w5pac26sqef4.onion>

In the case of a site like WeBuyBitcoins, they offer to exchange real cash for Bitcoins at a competitive exchange rate compared to equivalent non-anonymous services that exist in the Clear Web. However for criminals willing to take on more risk for potentially more reward, another option is available – buying counterfeit currency using Bitcoin.



[Click to enlarge](#)

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 ammonis. 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)

Buying counterfeit 20 USD for approximately half the price of face value

<http://usjudr3c6ez6tesi.onion>

References:

- [1] Bitcoin used to by a Tesla Model S - <http://www.wired.com/2013/12/tesla-bitcoin/>
- [2] <http://easycoinsayj7p5l.onion> – EasyCoin – Bitcoin Wallet with free Bitcoin Mixer / Laundry
- [3] <http://ow24et3tetp6tvmk.onion> – OnionWallet – Bitcoin Wallet with free Bitcoin Mixer / Laundry
- [4] <http://jzn5w5pac26sqef4.onion> – WeBuyBitcoins – Sell Bitcoins for Cash (USD), ACH, WU/MG, LR, PayPal and others
- [5] <http://usjudr3c6ez6tesi.onion> - Counterfeit \$20 USD / Euro Bills
- [6] <http://y3fpieiezy2sin4a.onion/> - Counterfeit \$50 Euro Bills
- [7] <http://qkj4drtgvpm7eecl.onion/> - Counterfeit \$50 USD Bills

Leaked details Government, Law Enforcement and Celebrities

Among hacker culture (and also in online gaming culture to a degree) it is common for groups of likeminded individuals to come together in loosely formed, or close knit groups. Due to the nature of the activities carried out by such groups and individuals it is very common for rivalries and fallings out to occur between different competing groups. When this occurs it is common practice for one group to attempt to “dox” the other. Doxing is the practice or researching and broadcasting personal identifiable information about an individual, which in the case of hackers is used to “unmask” a rival – essentially linking their real

world identity to their online one. The means to do this vary but will normally combine accessing public data, social engineering and direct hacking.



Cloudnine Doxing site – note it requests SSN, medical & financial info and more
<http://cloudninetve7kme.onion>

But the phenomenon of doxing or exposing private details is by no means restricted to hackers vs hackers – it is also quite common for hackers to target companies, celebrities and other public figures. In the case of companies having details exposed that is not simply restricted to hacking activity of course, it can also be insiders – as is commonly the case with well-known site Wikileaks – which also has a Deep Web presence, including a page to allow anonymous submission of new leaks.

It's very hard to know if these details are actually correct or not – but in many cases the supplied leaked details include DOB, SSN, personal email addresses, phone numbers, physical addresses and more. For example one site, Cloud Nine, lists possible “dox” for public figures such as:

- Several FBI agents
- Political figures like Bill & Hillary Clinton, Barack & Michelle Obama, Sarah Palin, US Senators and others
- Celebrities such as Angelina Jolie, Bill Gates, Tom Cruise, Lady Gaga, Beyonce, Dennis Rodman and more

```

Barack Hussein Obama
AGE: 50
DOB: 08/04/1961 (August 4th 1961)
Born In: Honolulu, Hawaii
Married to Michelle Obama (Robinson)
Obama's Yahoo Email Address
bObama@yahoo.com IP Used to sign in 71.191.175.122 - Arrlington, VA - Verizon
Internet.
Baracks Personal IP (IP of the Whitehouse?) 66.36.206.59 - Washington DC IP that was
signed into both emails.
Obama's AOL (Protected by AOL Security)
bObama@aol.com
Barack IP used to sign into that E-mail when he was in Rhode Island. 68.14.135.217 -
Cox Communications.
Court Records
Barack H Obama
Defendant

```

Apparent personal email account of Barack Obama (unverified)

<http://cloudninetve7kme.onion>

<u>FBI GOV</u>	177.87 KB
<u>FBI Agent J Keith Mularski</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 Mike Eads</u>	0.17 KB
<u>FBI SNITCH</u>	0.14 KB

Apparent leaks of LEA (unverified)

<http://cloudninetve7kme.onion>

<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

A leak for Kim Kardashian among other hacker related dox

<http://cloudninetve7kme.onion>

References:

[1] <http://cloudninetve7kme.onion> - Doxing archive

[2] <http://gjlng65kwikileax.onion/> - Wikileaks clone

[3] <http://wlupld3ptjvsgwqw.onion/wlupload.en.html> - Wikileaks submission portal

[4] [http://uhwikih256ynt57t.onion:80/wiki/index.php?title=Dox_-_Katherine_Bolan_Forrest_\(Silk_Road_Judge\)&oldid=5764](http://uhwikih256ynt57t.onion:80/wiki/index.php?title=Dox_-_Katherine_Bolan_Forrest_(Silk_Road_Judge)&oldid=5764) - Possible Judge Forrest leak

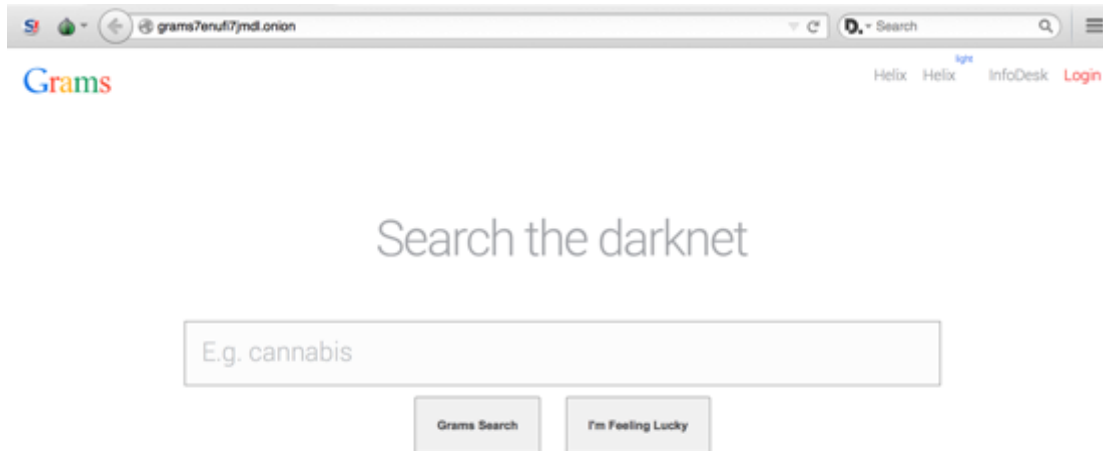
Drugs

As we mentioned, it is common for just about every report on the Deep Web to talk about how freely available illegal drugs, and weapons, are. In this report we do not intend to go into major detail on this – as it has been covered by others. But we did want to briefly highlight that fact that even after the conviction of individuals like Ross Ulbricht – who was recently sentenced [1] to life with no chance of parole for running the infamous drugs forum “The Silk Road” – procuring drugs on the Deep Web is still relatively trivial.

The availability of illegal narcotics varies a lot on the Deep Web, with sites selling everything from the relatively tame (such as contraband Tobacco[2]), to Cannabis[3], Psychedelics[4], Cocaine and so on.



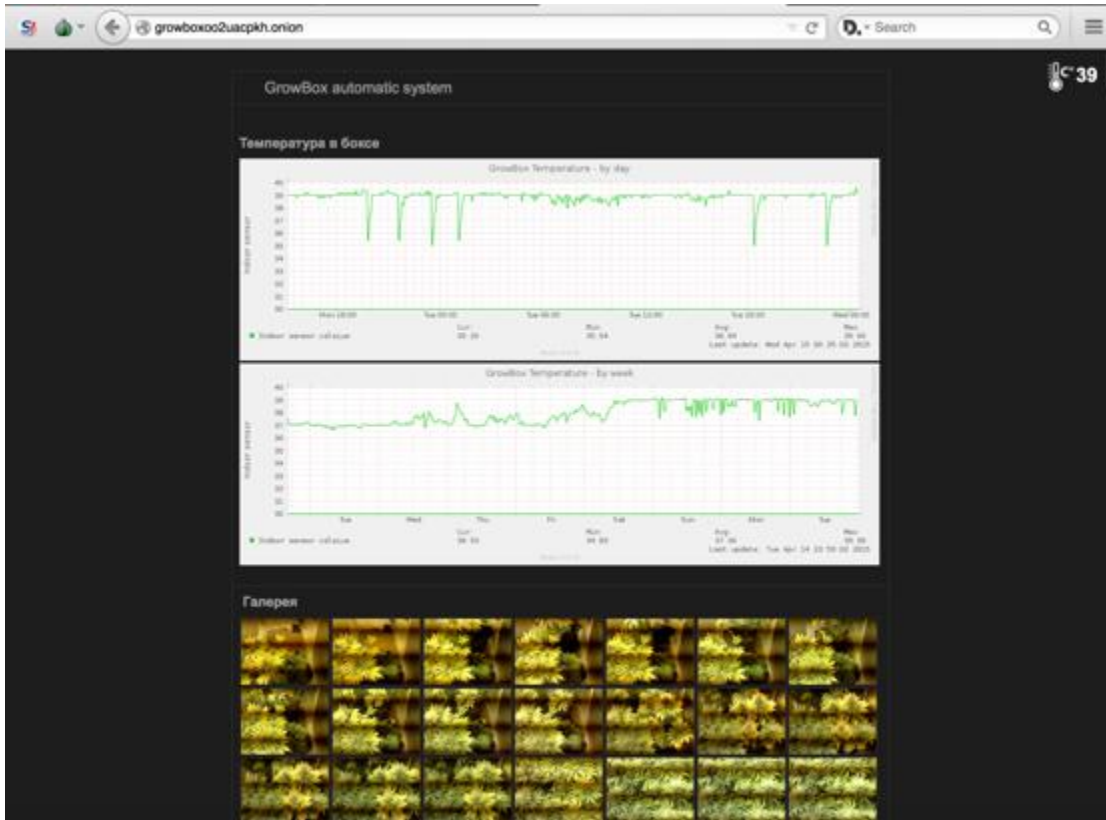
The Peoples Drug Store – selling Heroin, Cocaine, Ecstasy and more
<http://newpdsuslmzqzvr.onion>



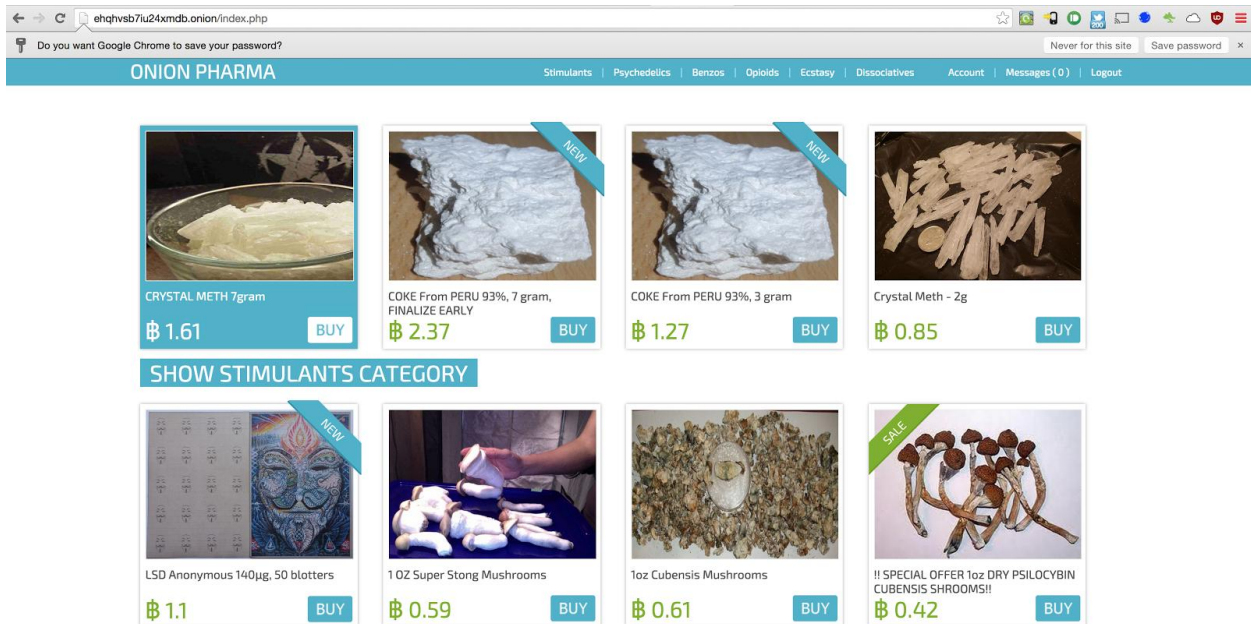
Grams – the Deepwebs search engine for drug
<http://grams7enufi7jmdl.onion>

In addition to dedicated shops or forums, a very popular site is “Grams” which allows for the easy search and indexing of Deep Web sites that traffic in illegal drugs. With a logo styled on that of Google it has become one of the Deep Web de facto sites for those looking to buy such goods.

We’ve even found TOR sites that offer live information of an active Cannabis grow house – showing live stats for temperature, moisture and a live camera showing the plants growing over time.



Growhouse – showing temperature and live streaming of Cannabis plant
<http://growboxoo2uacpkh.onion>



Drugs dealer in the Deep Web

The reason we wanted to touch on drugs on the Deep Web in this section of the report is to further highlight a point that was made in [8] – when you take down a criminal marketplace like the Silk Road, it fundamentally is not a solution in itself. On one side you still have buyers looking to procure drugs, and other side you have sellers wishing to sell to them. The marketplace or forum acts as meeting point in the middle, but if you remove it – as long as the demand for the good is strong enough on both sides – another marketplace will unfortunately always rise to take its place.

References:

- [1] <http://www.forbes.com/sites/katevinton/2015/05/29/ulbricht-sentencing-silk-road/>
- [2] <http://cigs7cviqbi4bvuy.onion/> - Contraband Tobacco
- [3] <http://smoker32pk4qt3mx.onion> - Cannabis
- [4] <http://ll6lardicrvrljvq.onion> - Psychedelics
- [5] <http://newpdsuslmzqzvr.onion> - Heroin, Cocaine and others
- [6] <http://grams7enufi7jmdl.onion> - Grams – Deep Web drug search engine
- [7] <http://growboxoo2uacpkh.onion/> - Live feed from a Cannabis Growhouse
- [8] <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-deep-web-anonymizing-technology-good-and-bad> - Expert Insight video Series – The Deep Web

Malware

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 very difficult 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 caused a noticeable spike in TOR traffic when they switched to TOR-hidden services for C&C. Other malware families like ZBOT followed suit in 2014.

As a first example, VAWTRAK malware is a banking Trojans that spreads via phishing emails. Each sample communicates with a list of C&C servers whose IP addresses are retrieved by downloading an encrypted icon file (i.e., favicon.ico) from hard-coded TOR-hosted 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.

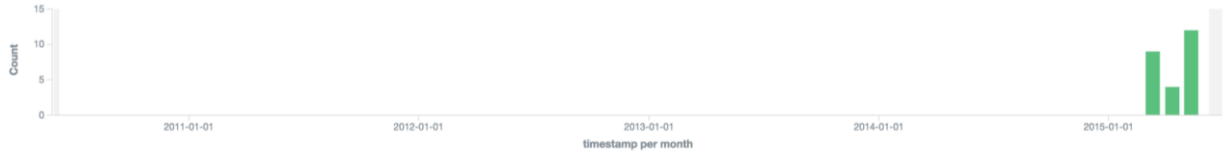


Vawtrak C&C showing the legitimate looking Favicon
<http://4bpthx5z4e7n6gnb.onion/favicon.ico>

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

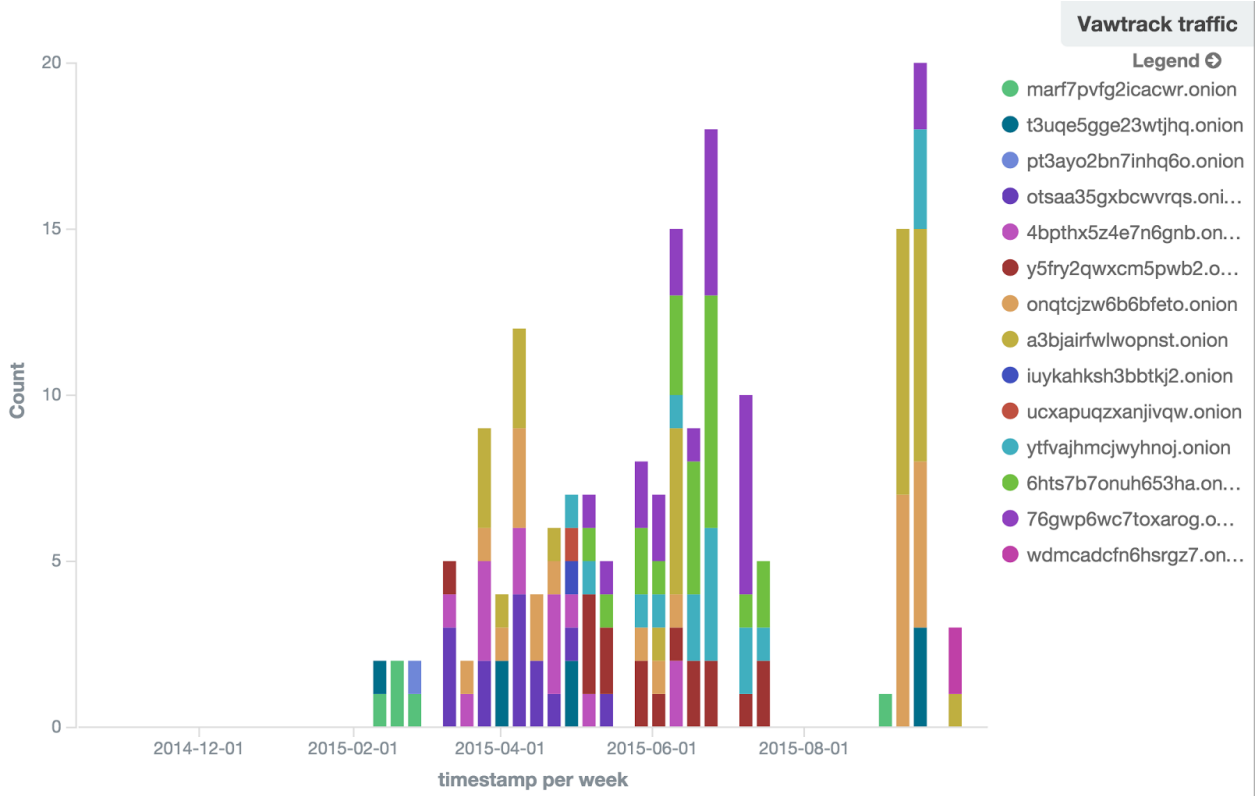
Name	Value
content-length	612
via	1.0 charon (squid/3.1.10)
x-cache	miss from charon
x-cache-lookup	miss from charon:3128
server	openresty/1.7.2.1
last-modified	wed, 18 feb 2015 14:45:29 gmt

Example of fetched HTTP headers from C&Cs



Time	url.hostname	requests.response.code
May 14th 2015, 17:38:17.826	7qpxFodfh6fvpqyc.onion	
May 14th 2015, 17:38:16.995	w3kjcq6svuucw6o.onion	
May 14th 2015, 17:38:16.431	w3qsdr5gb31t1n3.onion	
May 14th 2015, 17:37:48.715	kFz2wdsF4Ss42mem.onion	
May 14th 2015, 17:37:42.144	6hts7b7onuh653ha.onion	
May 14th 2015, 17:37:22.613	5h3ejaxii4fshu4e.onion	
May 14th 2015, 17:37:11.843	76gwp6wc7tozarog.onion	
May 14th 2015, 16:42:00.235	xu5dnsugozwrieco.onion	
May 14th 2015, 16:41:59.665	sws5qec3n7v7bxei.onion	
May 14th 2015, 16:41:58.557	max6gtszig614rjt.onion	
May 14th 2015, 16:41:46.981	ytfvajhmcjwyhnoj.onion	
May 14th 2015, 16:39:40.695	q6knv6pe25cxjv2s.onion	
April 15th 2015, 19:24:35.751	otsaa35gxbcwvrs.onion	
April 15th 2015, 19:18:04.426	4bpthx5z4e7n6gnb.onion	

Identified TOR-based C&Cs (1)




Identified TOR-based C&Cs (2)

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.

The screenshot shows a payment page for CryptoLocker in Chinese. The header includes the CryptoLocker logo and navigation links: '购买解密软件' (Buy decryption software), '免费解密一个文档' (Free decryption of one document), '常见问题' (FAQ), and '支持页面' (Support page). The main heading is '购买解密软件以便还原所有加密文档' (Buy decryption software to restore all encrypted documents). A yellow warning box contains a flame icon and the following text: '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)', and '余款: 3.59856 比特币 (约 23800 TWD)'. Below this, there is a section titled '使用 bitcoin 来购买解密软件' (Use bitcoin to buy decryption software) with a sub-heading '比特币到底是什么?' (What is Bitcoin?). It defines Bitcoin as '比特币(BTC, Bitcoin) - 互联网上使用的虚拟货币。' (Bitcoin (BTC, Bitcoin) - Virtual currency used on the Internet.) and includes a numbered step '1 购买比特币' (1 Buy Bitcoin) with instructions: '您可在网站上购买比特币以便在台湾兑换货币' (You can buy Bitcoin on the website to exchange for currency in Taiwan) and '您可以使用下列网址提供的服务: 通付银行汇款, 便利店支付或西联汇款第三方支付商。如果您通过银行账户转账支付, 请备注' (You can use the services provided by the following URLs: Tongfu Bank remittance, convenience store payment, or Western Union remittance third-party payment provider. If you pay through a bank account, please note).

CryptoLocker Acquistare decrittografia Decrittografare File [licenze](#) FAQ Supporto

Acquista decrittazione e ripristinare i file

 Acquistare 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)
 Rimane da pagare: 4.357080 Bitcoin (circa 798 EUR)

Acquista decrittatura con bitcoin

Cosa sono i Bitcoin?

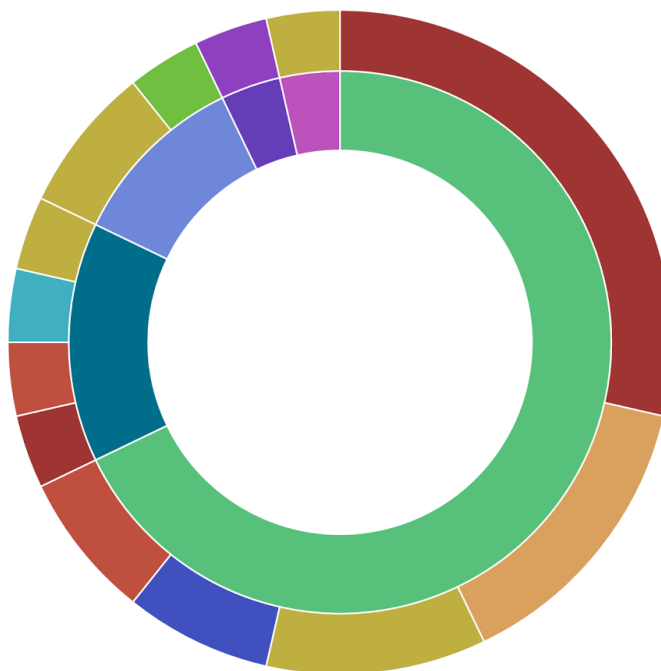
Bitcoin (simbolo: ₿, codice: BTC o XBT) è una moneta elettronica.

- 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.
postcoin.com - Compra BitCoin con Postepay.
www.bitbot.net - Il mercato numero uno in Italia, per comprare Bitcoin (istantaneamente, in contanti).
bitbit.it - Compra bitcoin in contanti senza registrazione!
www.moz2k.biz - Compra BitCoin con Postepay, Superflash.
www.furppay.com - Compra BitCoin con Mybank, Sofort.
www.litbit.eu - Compra BitCoin con Postepay, Sepa, Sofort.
localbitcoins.com - Compra bitcoin online in Italy
howtobuybitcoin.info - Come acquistare bitcoin in Italia.
- Invia bitcoin**
 Invia Bitcoin alla nostra bitcoin-portafoglio.
 Importo del pagamento: **4.357080 Bitcoin (circa 798 EUR)**
 Il nostro indirizzo bitcoin portafoglio:
- 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.

Verifica di pagamento

Cryptolocker C&C automatically formatted for a victim in Taiwan and Italy

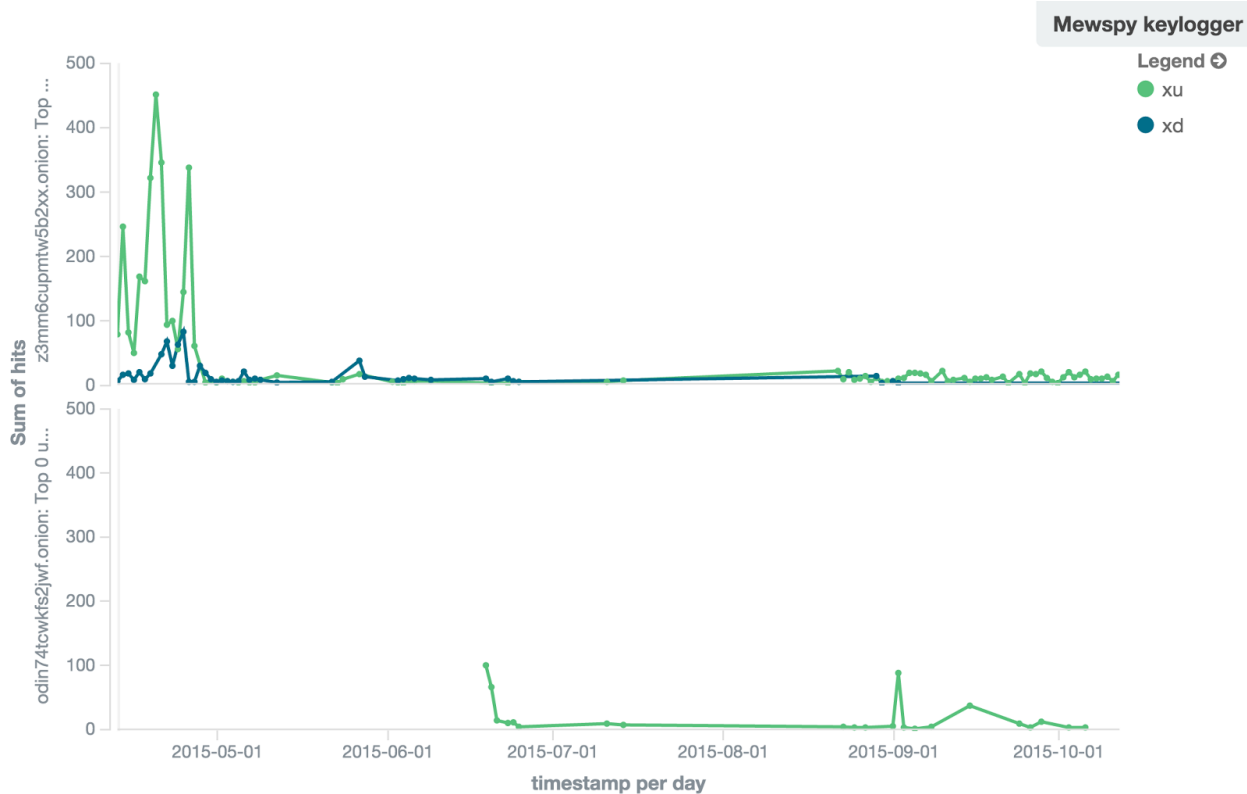
<http://ndvgtf27xkhdvezr.onion>



TorrentLocker languages

Legend 

- English
- Turkish
- French
- Chinese
- Italian
- 6o4xqbd4cpmumytk.o...
- xf7kegtgitykjoom.onion
- ndvgtf27xkhdvezr.onion
- 3xo7axbmktd4qlx.onion
- ergdzsjgpvsc5rvj.onion
- gumuj7unxtiai2a3.onion
- bica3zjnlv6fxkqf.onion
- wzaxyqroduouk5n.on...



Number of new Infections (and Leaked data, in bytes) per day.

Finally, worth to mention is a banking Trojan called Dyre that uses I2P as backup options for its C&C infrastructure – normally ran using DGA on the Clear Web. This malware acts as a BHO that MiTMs online-banking pages at browser-level. This allows the code to back-connect from the victim to the attacker (similar to a reverse-shell approach) with the goal of granting the attacker the access to the banking portal of its victims. Accordingly to DeWA, this malware campaign introduced, over the last 6 month, 2 new operating servers and currently the number of infected victims using I2P is increased.



Traffic to Dyre's I2P infrastructure.

References:

- [1] <http://blog.trendmicro.com/trendlabs-security-intelligence/the-mysterious-mevade-malware/>
- [2] <http://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-tor-using-malware-part-1/>
- [3] <http://blog.trendmicro.com/trendlabs-security-intelligence/defending-against-tor-using-malware-part-2/>
- [4] <http://blog.trendmicro.com/trendlabs-security-intelligence/steganography-and-malware-why-and-how/>
- [5] <http://4bpthx5z4e7n6gnb.onion/favicon.ico - Vawtrak/> Neverquest C&C
- [6] <http://ndvgtf27xkhdvezr.onion> - Cryptolocker C&C