The Beginner's Guide to The Internet Underground

Jeremy Martin
Sr. Security Researcher

This covers the basics of anonymity, hactivism, & hidden parts of the Internet underground, along with some of the things you may find there.

Disclaimer: Do NOT break the law. This was written to explain what the (Darkweb / Deepnet / Tor hidden service) is and what kind of things you may find. It is not an invitation to break the law with no recourse. Just like any network, this one has both good and bad guys. If you break the law, you will get caught. Bad guys have to be lucky EVERY time. Good guys only have to be lucky once.

Images within this document were taken directly off the Internet or are taken from screenshots at the time of research. The content of this page is subject to update, discussion and dispute, and we welcome comments

Information Warfare Center, LLC
www.informationwarfarecemter.com
(719) 510-3554

0.2

CHAPTERS

CAN THERE BE TRUE ANONYMITY ON THE INTERNET?

To some extent, the answer to the title is yes. However there are many variables to consider. Just in the United States, there are many laws on the books (especially post-911) that have enabled "Big Brother" to potentially violate several of the rights granted to Americans by the Bill of Rights. Listed are just a few of the regulations or budget contracts that reference loosening the term "reasonable search and seizure" covered in the fourth Amendment and why there is such an internet outcry to Internet privacy. Currently, there are several Internet Service providers that are illegally wiretapping all your traffic.

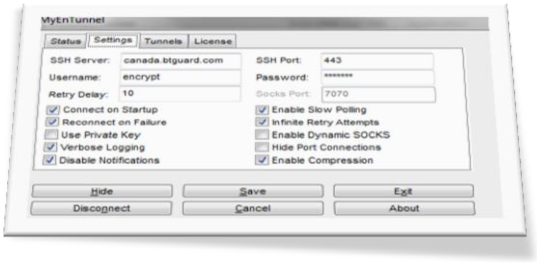
- ***USA Patriot Act, Title II (Enhanced Surveillance Procedures)***
- ***ECPA (Electronic Communication Privacy Act)***
- ***Title 18, U.S.C §1030 (Computer Fraud and Abuse Act)***
- ***Title 18, U.S.C §2703 (Required disclosure of customer communications or records)***
- ***CISPA (Cyber Intelligence Sharing and Protection Act)***
- ***NDAA 2011 (The National Defense Authorization Act)***
- ***Etc…***

There are legitimate reasons why governments want to monitor and control communications of the populace and or foreign entities. Intelligence and National Security is a valid concern. However, many countries have fallen to those excuses and have violated the basic trust they had with their citizens. Tunisia, Egypt, and Syria are just some of the more recent countries that have fallen to the temptation to over censor or monitor.

The need for some to pass information without prying eyes has spawned many different methods of "anonymous" communication. To understand how people are hiding where or what they are sending, you need to know the basics of the communication mechanism they are using. I am going to focus on the Internet and the medium. There is always a fingerprint on every packet that is sent. If all the systems or nodes on a network are monitored and logged, the origin can always be tracked. The Challenge with the Internet is that nobody controls everything (even though there is a current power struggle in this area). This means that if you cannot get the logs, you may not get the origin or the original fingerprint. There are several reasons you don't get the logs. The two most common are political and the lack of storage.

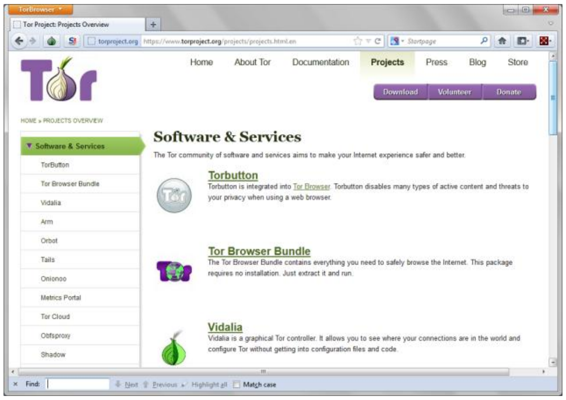
During the uprising in Tunisia, the government at the time tried to stop transmissions of during the uprising and effectively turned off the traditional paths to the Internet. Several groups then helped reopen the communication channels by sending dialup numbers, IRC channels, proxy addresses, and VPN servers. Soon after, the twitter feeds and videos started to stream out of the country again. On the other side of this coin, many people use these types of jump points to download movies, music, and pirated software or send out malicious attacks against targets. Even the MPAA has hired people in India to attack thepiratebay.se in a massive DDoS attack. The hactavist group "Anonymous" then attacked back, effectively shutting down the MPAA websites. The MPAA then called foul, but that is another story. Even Anonymous has taken to the Tor network with the old site Anonops.org, moving to anonops532vcpz6z.onion. Many Internet Service Providers (ISPs) are working with the local government or IP owners such as MPAA, RIAA, Microsoft, etc… to monitor your entire Internet traffic looking for evidence for possible pirated IP. To get around this, suspects can use methods to make themselves anonymous on the Internet. Encryption is still the best solution.

For whatever reason you want to protect your identity on the Internet, there are several options. Proxy servers are one of the most common routes. There are free and commercial proxy servers all around the world that offer access without logging the connections. Some of these proxies offer SSH encryption or even AES 256 bit encryption tunnels such as BTGaurd. This makes network forensics virtually impossible outside knowing that the IP address of the proxy was connected to.



SSH Server: canada.btguard.com
SSH Port: 443
Username: encrypt
Password: *******
Retry Delay: 10
Socks Port: 7070
☑ Connect on Startup
☑ Reconnect on Failure
☐ Use Private Key
☑ Verbose Logging
☑ Disable Notifications
☑ Enable Slow Polling
☑ Infinite Retry Attempts
☐ Enable Dynamic SOCKS
☐ Hide Port Connections
☑ Enable Compression

The TOR community or Onion network is another service that contains thousands of public proxies and thousands more that are not publically known. With this being said, blacklisting TOR network addresses does not work. The basic TOR client that comes with the TOR Browser Bundle (TBB) even allows you (the client) to be a proxy into the TOR network. TOR however does not support Bit torrent, but it does support browsing, chat, email, and other basic Internet services. However, once on the TOR network, others on the same network will know your original IP address.



Software & Services

The Tor community of software and services aims to make your Internet experience safer and better.

Torbutton

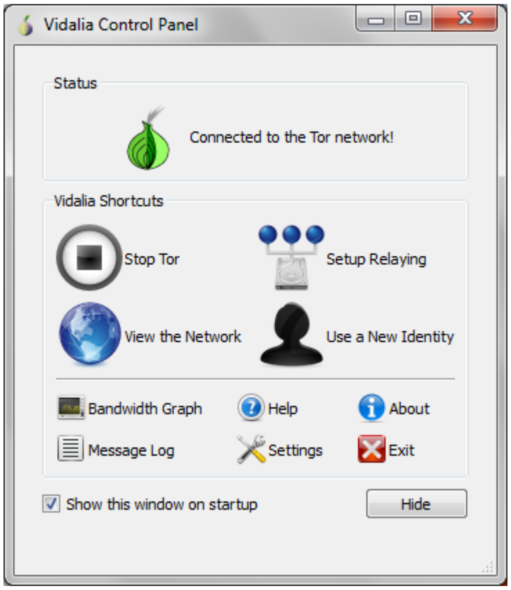
Torbutton is integrated into Tor Browser. Torbutton disables many types of active content and threats to your privacy when using a web browser.

Tor Browser Bundle

The Tor Browser Bundle contains everything you need to safely browse the Internet. This package requires no installation. Just extract it and run.

Vidalia

Vidalia is a graphical Tor controller. It allows you to see where your connections are in the world and configure Tor without getting into configuration files and code.



Connected to the Tor network!

☑ Show this window on startup

There are many "secure" live operating systems that you can even use to log into TOR. The first one I want to talk about is Tails "The Amnesic Incognito Live System is a live CD/USB distribution preconfigured so that everything is safely routed through Tor and leaves no trace on the local system." This can be found on thetorproject.org. The second one I would like to mention is Whonix "(called TorBOX or aos in past) is an anonymous general purpose operating system based on Virtual Box, Debian GNU/Linux and Tor. By Whonix design, IP and DNS leaks are impossible. Not even malware with root rights can find out the user's real IP/location." Both of these are pre-configured operating systems that will let you automatically connect to the TOR network with little to no work on your part. Whonix is based of two different virtual machines and does require more resources and a running OS. The Tail OS, if burned to a CD, doesn't leave a forensic trail on the local hard drive.

The other method to completely hide all your traffic is the traditional VPN. A VPN server essentially hides your IP address because you are virtually connected to a completely separate network. Once you touch the Internet, it is going through their gateway. The downside is that there is a bandwidth bottleneck. You are also on a network with others trying to hide their identity. Once you are on the network, your source is known by the other people on the network.

Now from the investigation standpoint; if the logs do not exist, there is no forensic footprint. If the evidence has been tampered with or does not exist, there is no case. If you are not on the same network as those using these services, especially the proxies, you may never find the origin or the suspect. If you are on the same network or inline between the suspect and the proxy, you may be able to see what is going through the wire if it is unencrypted. However, you need to be careful of wiretap laws. Not even the ISP's have the right to monitor your traffic without probable cause and more than likely a court order. However, there is legislation and activities that are pushing this into a very grey area… ISPs are using the excuse that too many people are sharing illegal or protected IP content and should be able to protect themselves. Just be aware of your environment, the jurisdiction, and monitoring laws in your area.

This is a major security threat for companies that want to control all of their traffic. If you blacklist, there will only be other covert channels pop up. It comes down to managing acceptable risk. Going back the beginning of this article, some laws are being pushed that wiretaps may be a normal part of everyday life and that National Security trumps right to privacy as it is in most other countries around the world.

If you are not a member of a hacking group/hactavist community/state sponsored cyber army, you may not have the access to a private VPN or proxy. In this case, there are several resources you can choose from, but it all comes down to researching the product that is right for you. Here is a list of services that some people use to hide their origin.

- **BTguard**
- **Private Internet Access**
- **TorrentPrivacy**
- **TorGuard**
- **ItsHidden**
- **Ipredator**
- **Faceless**
- **IPVanish**
- **AirVPN**
- **PRQ**
- **BlackVPN**
- **Privacy.io**
- **Okayfreedom**
- **Cryptocloud**

Services that do not support anonymity (Log a lot)

- **hidemyass**
- **Hotspot Shield**
- **VyprVPN**
- **SwissVPN**
- **StrongVPN**

THE ACTIVIST GROUP "ANONYMOUS"

No matter what side of the debate you are on, Anonymous has made a mark in cyberspace, politics, and general freedom of speech. Whether it helping the people of Tunisia get word to the rest of the world of the atrocities occurring against the uprising populace or calling attention to cyber legislation (SOPA, PIPA, CISPA, etc…) that would destroy free speech as some see it, the hactavist phenomenon have caused change.

"Anonymous does not have a membership list, and you can't really 'join' it either. If you identify with or say you are Anonymous, you are *Anonymous. Noone has the authority to say whether you are Anonymous or not, except for yourself."* – anonnews.oeg

There are several groups that claim to be part of Anonymous, but as everyone has seen, each group has its own doctrine or political motives. Some of them are informational while others are very destructive. There have even been messages sent under the mask of Guy Fawkes with threats of violence and terrorism. Many of these messages have been shot down as fakes such as the original *Westboro Baptist Church* and the November 5th 2012 *government bomb threat.*

There has been actual retribution from Anonymous over the past year. Several of their "Operations" have caused websites from corporations like Sony to Federal government organizations like the CIA, FBI, and DOJ to go down. The group uses very simple methods for Distributed Denial of Service, primarily resource starvation. Make thousands of legitimate connections for the attack and use up as much of the resource as you can. If you use more than the victim has, the victim then starts to fail.

Other operations have been focusing on the freedom of information, or literally freeing the information from the owners and giving it to the people. Project Mayhem-2012 calls for a program called Tyler (both named after the movie Fight-Club) to "leak it all!" They believe the operation will help fight political and corporate corruption. *"Imagine you purchase a USB drive. Imagine you take it to your work place. Imagine you collect evidence of illegality and corruption. Imagine together we expose all lies. Imagine we leak it all."*

The only thing this section is trying to do is link to news and messages about or from Anonymous over the year 2012, starting from the National Defense Authorization Act for 2012 (NDAA) message from Anonymous in December 2011 to November 5th, the date they called everyone to march. The "*Anonymous - Message to the American People*" focused on the NDAA. Link to the first video can be found here, followed by the post NDAA video here. This is not a piece to state what side you should be on and does not advocate illegal activity without expectations of jail time.

Dear brothers and sisters. Now is the time to open your eyes!

In a stunning move that has civil libertarians stuttering with disbelief, the U.S. Senate has just passed a bill that effectively ends the Bill of Rights in America.

The National Defense Authorization Act is being called the most traitorous act ever witnessed in the Senate, and the language of the bill is cleverly designed to make you think it doesn't apply to Americans, but toward the end of the bill, it essentially says it can apply to Americans "if we want it to.

Bill Summary & Status, 112th Congress (2011 -- 2012) **|** S.1867 **|** Latest Title: National Defense Authorization Act for.

This bill, passed late last night in a 93-7 vote, declares the entire USA to be a "battleground" upon which U.S. military forces can operate with impunity, overriding Posse Comitatus and granting the military the unchecked power to arrest, detain, interrogate and even assassinate U.S. citizens with impunity.

Even WIRED magazine was outraged at this bill, reporting:

Senate Wants the Military to Lock You Up Without Trial

...the detention mandate to use indefinite military detention in terrorism cases isn't limited to foreigners. It's confusing, because two different sections of the bill seem to contradict each other, but in the judgment of the University of Texas' Robert Chesney — a nonpartisan authority on military detention — "U.S. citizens are included in the grant of detention authority."

The passage of this law is nothing less than an outright declaration of WAR against the American People by the military-connected power elite. If this is signed into law, it will shred the remaining tenants of the Bill of Rights and unleash upon America a total military dictatorship, complete with secret arrests, secret prisons, unlawful interrogations, indefinite detainment without ever being charged with a crime, the torture of Americans and even the "legitimate assassination" of U.S. citizens right here on American soil!

If you have not yet woken up to the reality of the police state we've been warning you about, I hope you realize we are fast running out of time. Once this becomes law, you have no rights whatsoever in America. — no due process, no First Amendment speech rights, no right to remain silent, nothing.

The US senate does not want us to speak. I suspect even now orders are being shouted into telephones and men with guns will soon be on their way. Why? Because while the truncheon may be used in lieu of conversation, words will always retain their power. Words offer the means to meaning and for those who will listen, the enunciation of truth. And the truth is, there is something terribly wrong with this country, isn't there?

Cruelty and injustice...intolerance and oppression. And where once you had the freedom to object, to think and speak as you saw fit, you now have censors and systems of surveillance, coercing your conformity and soliciting your submission. How did this happen? Who's to blame? Well certainly there are those who are more responsible than others, and they will be held accountable. But again, truth be told...if you're looking for the guilty, you need only look into a mirror.

I know why you did it. I know you were afraid. Who wouldn't be? War. Terror. Disease. There were a myriad of problems which conspired to corrupt your reason and rob you of your common sense. Fear got the best of you and in your panic, you turned to the now President in command Barack Obama. He promised you order. He promised you peace. And all he demanded in return was your silent, obedient consent.

More than four hundred years ago, a great citizen wished to embed the fifth of November forever in our memory. His hope was to remind the world that fairness. Justice, and freedom are more than words - they are perspectives. So if you've seen nothing, if the crimes of this government remain unknown to you, then I would suggest that you allow the fifth of November to pass unmarked. But if you see what I see, if you feel as I feel, and if you would seek as I seek...then I ask you to stand beside one another, one year from November 5th, 2011, outside the gates of every court house of every city DEMANDING our rights!!

Together we stand against the injustice of our own Government.

We are anonymous.
We are Legion.
United as ONE.
Divided by zero.
We do not forgive Censorship.
We do not forget Oppression.
US SENATE...
Expect us!!

Music by: Wolfgang Amadeus Mozart - Requiem

AMERICAN FREEDOM ALERT - CODE RED.

The Government has committed TREASON against you! Will you sit and watch while your freedoms are taken away? Or will you walk out your door and fight for your rights?

THE CHOICE IS YOURS. THE LATTER IS BEST.

Gather an army of people. Flood the streets. If police gives you violence, give them tenfold of that.

OCCUPATIONS ARE OVER. REAL REVOLUTION IS HERE. THE FORMER UNITED STATES GOVERNMENT SHALL BE DESTROYED.

In his last official act of business in 2011, President Barack Obama signed the National Defense Authorization Act from his vacation rental in Kailua, Hawaii.

In a statement, the president said he did so with reservations about key provisions in the law — including a controversial component that would allow the military to indefinitely detain terror suspects, including American citizens arrested in the United States, without charge.

The president defended his action, writing that he signed the act, "chiefly because it authorizes funding for the defense of the United States and its interests abroad, crucial services for service members and their families, and vital national security programs that must be renewed."

Some citizens remain completely confused by the language of the bill, running around the Internet screaming that the law "does not apply to American citizens."

This is, naturally, part of the side effect of having such a dumbed-down education system where people can't even parse the English language anymore. If you read the bill and understand what it says, it clearly offers absolutely no protections of U.S. citizens. In fact, it affirms that Americans are subjected to indefinite detainment under "existing authorities."

The writers of the bill have managed to fool a lot of everyday people who seem unable to parse language and read plain English with any depth of understanding. That is as much a failure of America's public education system as anything else. I find it astonishing that today's citizens can't even read and understand the grammatical structure of sentences written in plain English. This alone is a highly disturbing subject that must be addressed another day. For now, it's enough just to realize that the NDAA really does apply to you, me, and all our neighbors and friends. In signing it, Obama has cemented his place in history as the enabler of government-sponsored mass murder of its own citizens.
History does repeat itself after all. Hitler, Stalin, Mao and now "Obama the enabler." While Obama himself probably won't engage in the mass murder of American citizens, have no illusions that a future President will try to use the powers enacted by Obama to carry out such crimes.

The system was built for the 1% not for us. They live because of "we". This must change. Don't stop the fight, don't stop the protest. We will win. Occupy everything, everywhere. This is the beginning, this is the start.

So, brothers and sisters. The collective is calling upon the citizens of the United States to protest against the new sections in the national defense authorization act that were passed a short while ago.

While we cannot force the American people to protest, we must tell them that this law will strip away any rights they thought they had including, but not limited to, Free speech, Free press, Free access to information, and the right to protest, assemble, and bear arms.

This law cannot be changed according to the Feinstein Act. Sections Ten thirty one and ten thirty two of the national defense authorization act have been passed and ratified. It grants unlimited powers to the executive branch of the government to indefinitely detain suspects, even American citizens, without trial.

All a person has to do is to commit a belligerent act. What is a belligerent act? Is protesting a belligerent act? Is being Anonymous a belligerent act? This is where we draw the line. This is when we leave our computers. This is when we take out our masks and defy the corrupt rule of law. This is when we revolt. The time has come for you to accept the truth and join us in overthrowing yet another corrupt military regime.

Operation Blackout, engaged.

We are Anonymous.
We are Legion.
We do not Forgive.
We do not Forget.
To the United States government, you should've expected us.

Link to NDAA Bill
http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf

Other Link News
http://www.naturalnews.com/034538_NDAA_American_citizens_indefinite_detainmen...
http://www.cbsnews.com/8301-250_162-57350607/obama-signs-defense-bill-with-re...
http://www.thenewamerican.com/usnews/constitution/10396-president-obama-signs...

Since then those two messages, there have been many threats, many protests, and attacks from both sides of the coin. Anonymous has taken down government sites and members have been arrested. Most of the members have evaded arrest or harassment by using anonymity services on the Internet. Some of the ones that have been caught have made a mistake such as connecting to an IRC channel without bouncing through proxies and encryption. Some have been caught by using a VPN service that does log and actively works with Law Enforcement (LE) such as HideMyAss. A common LE saying is "You have to be lucky every time… I only have to be lucky once..." As we have already discussed, covering your tracks can be easy, but one mistake can make it to where everyone knows your name.

"On November 5th 2012 WE THE PEOPLE will march on Washington DC peacefully and unarmed to arrest all members of congress, the president, and all supreme court justices where they will be held without bond until a full independent investigation and trial have been completed. We must re-elect our government within 90 days in order to stave of unrest." This did not have the effect some would have thought it would.

Now, below are links to Anonymous messages released over the last year. These links are currently pointing directly to Youtube. The future release of this document will have them pointing to either a direct download or a streaming media server.

MESSAGES FROM ANONYMOUS:

Anonymous - Message to the American People - YouTube
Anonymous - Message To Obama - YouTube
ANONYMOUS: Message to the US Armed Forces ...
Anonymous: Message to SONY on SOPA
Anonymous - The First Message of 2012 - YouTube
Anonymous message to Romania - YouTube
Anonymous - Global Cyber War I (Emergency Video PR)
Anonymous - Operation Revenge
Anonymous message to world leaders. This is wonderful :) (Text)
Anonymous - Operation Sony Has Commenced
Anonymous - Operation Sony Update
Anonymous Message Regarding (megaupload) And The Future
Anonymous Message To Congress. #OpGlobalBlackout
Dear Internet,
Anonymous Message On How YOU Can Be A Part Of #OpGlobalBlackout FACEBOOK ATTACK
ANONYMOUS 2012- (IMPORTANT MESSAGE)TO THE PEOPLE WE MUST UNITE
Anonymous Message To The Citizens Of Oakland
Anonymous: Operation Black 'March'
Anonymous - AntiSec: FBI Conference Call
ANONYMOUS MESSAGE TO CYPRUS JUSTICE
Anonymous: Operation Black March 2012
Anonymous Launches Music Albums!
Anonymous - Greece Message 2 -
Anonymous Message to "Alex Jones" - YouTube

Anonymous message to the world, and the CIA
Anonymous: A Message to the State of Israel
Anonymous - Message to Bulgaria - YouTube
Anonymous - Message to the Macedonian people
Anonymous Message to the Unemployed Americans
Anonymous Project Mayhem 2012: Who Watches the Watchmen?
Anonymous Hacks into Syrian President's Email
Anonymous message to Russian people - YouTube
Anonymous message to the citizens of Sweden
Anonymous - Our Warning to Vic Toews & the Parliament of Canada
Anonymous: Message to the NSA - YouTube
Anonymous Message Attack Planned on Olympics
Anonymous: Operation V (Nov. 5th 2012)
Censored Video-Anonymous Message To Turkey
Anonymous - Message to AIPAC - YouTube
Anonymous: Occupy AIPAC - YouTube
Message from Anonymous: Music has changed
Anonymous Message To Joseph Kony - KONY2012
ANONYMOUS Revolution 2012 New Message What we are capable of!
Anonymous: Message to YouTube - YouTube
Anonymous: NDRP
Anonymous: We Will Not Shut Down The Internet
Anonymous : message au monde entier on Vimeo
Anonymous: General Strike #OpMayDay
Anonymous: The Collective's Decision
Anonymous: Operation Defense Targets
Anonymous Message to The University Of Pittsburgh
Anonymous: Message to United States Citizens [CISPA]
Anonymous: Operation Defense Phase II [CISPA]
ANONYMOUS MESSAGE: WE ARE NOT ALONE 28/04/2012
Anonymous: Message to Georgia State (college) Senate
ANONYMOUS MESSAGE TO NASA 30.04.2012 ...
Anonymous: Project Mayhem 2012 Call to Hackzion! Code TYLER!
#opindia (Anonymous) message to Indian Government
Anonymous- message to Chicago Police
Anonymous: Monday Mail Mayhem
Anonymous Project Mayhem 2012 | Leak it ALL! Call to Action
Anonymous Message To Cyprus | By AvengersOn- #opCyprus
Anonymous: Project Mayhem 2012 | #TROLLYMPICS
Anonymous Message: #OpEndMonsanto - YouTube
Anonymous message to Nik Richie - YouTube
Message to the Federal Reserve System
Anonymous message: Wikileaks - YouTube

Anonymous Message: #OpPedoChat - YouTube
Anonymous Message To Mayor Buckhorn And RNC
Anonymous message: #Watchtower - YouTube
Anonymous-Message To All Humanity - YouTube
Operation Propaganda - YouTube
Anonymous Message On The Coming New World
Anonymous Message: #OpAnonTrademark - YouTube
Anonymous - Message Of Diplomacy - YouTube
Anonymous Message - Krazykid York Facebook ...
Project Mayhem 2012: The Re-Evolution: 4,000,000,000 Years of Evolution.
ANONYMOUS: Message 2 RNC Activists F.B.I TPD & PI Bill Warner
Anonymous - Message to UK Government (Free Assange)
Anonymous message: #WeThePeople - YouTube
Anonymous Message: #OccupyRNC - YouTube
Anonymous - Message To Bulgarian Police
Anonymous Project Mayhem 2012: December 21st 2012
Anonymous - Message To All Humanity 2012 ...
Anonymous Message: GoDaddy - YouTube
ThinK Anonymous: Project Mayhem 2012: The Plague
Anonymous Message - Police State - YouTube
Anonymous Message: #OpPRA - YouTube
Anonymous message: #OpLibertyCity - YouTube
Anonymous - Operation Pirate Bay - YouTube
Anonymous message: #OpUCKG - YouTube
Anonymous - Message to the President of the Philippines
Anonymous Project Mayhem 2012: The Plan | #Nov5
Anonymous - Message to the media of Estonia
Anonymous Message to Chinese Government
Anonymous message to pedophiles - YouTube
Anonymous Message Regarding the New World Order 2012
anonymous message to british government
Anonymous Message: Kody Maxson (Amanda Todd's Bully - YouTube
Anonymous: November 5th - Defend Your Freedom [Worldwide Protests]
Anonymous Warning: 5th November 2012
Anonymous: Response to Nov 5th Bomb Threat

**** Document will be updated with .avi file links instead of the youtube.com links in the near future.****

THE CORRUPT
FEAR US.
THE HONEST
SUPPORT US
THE HEROIC
OVIEDO
es Government
Chart
SENIOR
TERRORISTS
TERRORIST
MILITIA
ARMED
TERRORIST
ARMED
TERRORIST
WE ARE
ANONYMOUS
TENT OF MASS
DESTRUCTION
SIC SEMPER TYRANNIS
ANONYMOUS
The REVOLution to Restore the Re
No Army Can St
WE ARE WATCHING YOU.
#AnonOps #Anonymous #OpItaly #AntiSecITA #FreeAnons #FuckTheCops
~~Innocence of Muslims~~
Don't be a FOOL
Seek The TRUTH
or FOREVER burn in HELL
GOVERNMENTS SHOULD FEAR THEIR PEOPLE

OTHER GROUPS

Anonymous is not the only hactavist/hacker group out there. There are plenty of other hacking groups. The range goes from hacktivists to bored fourteen year olds to organized crime to state sponsored actors. There are many websites out there on the regular Internet that monitors or allows hackers to post their conquests. Zone-h.org is one of these sites.

Zone-h disclaimer: *"all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified anonymously to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents."*

Message to Israel:
You will pay the price for your crimes and every drop of blood from the
The people of Palestine and the patient, say the answer is painful to come, Go
willing, and that victory is near

Crash Servers, Web sites....

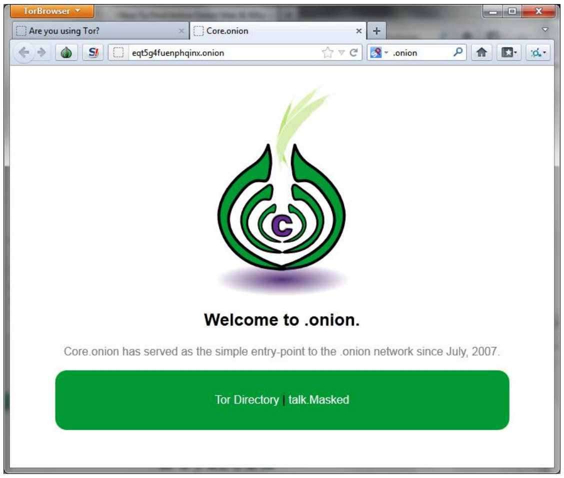
Some of the groups that post here claim to be politically motivated and others are just doing it because they can. Either way, it is still damaging to the victim. The methods of the website defacements range from simple SQL injection to advanced buffer overflows that allow the attacker to take complete control of the server. The nice thing about this site is, they keep tabs on what group attacks what sites and how many defacements each group has accomplished. Zone-h has been the target of hackers themselves over the years. There are hackers out there that no longer trust the site because of the vulnerabilities they have had in the past. The simple fact still rings true… If your domain is published on the site, there is a problem. Your site has been defaced. Many of the actors here have been recorded as threats to nation-states and have active arrest warrants out for top members of the groups.

There are other sites out there such as hack-db.com that contains similar information and xssed.org that lists sites verified to be vulnerable to cross site scripting (XSS). Even on the Tor network, there are a few resources available such as HackBB: clsvtzwzdgzkjda7.onion & Rent-a-Hacker: ugh6gtz44ifx23e7.onion. The interesting thing about most of these sites is that they will not post the event until after they verify. These sites are a third party that manually validates each entry before the posts get listed into the archive.

Team GhostShell is another hacking group that targets governments, companies, and universities. They have leaked millions of records from top universities and the Russian government onto the Internet. Ashiyane Digital Security Team, chinahacker, Iran Black Hats Team, and Fatal Error are groups that seem to focus more on website defacements and recognition.

THE INTERNET UNDERGROUND: TOR HIDDEN SERVICES

Some people think onion routing or the Tor network is for criminals and people with something to hide. Well, they are half right. The Tor network was designed to give a masked, "semi-safe", passage to those that needed to get information out. "Tor was originally designed, implemented, and deployed as a third-generation onion routing project of the U.S. Naval Research Laboratory. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications. Today, it is used every day for a wide variety of purposes by normal people, the military, journalists, law enforcement officers, activists, and many others." - torproject.org



Welcome to .onion.

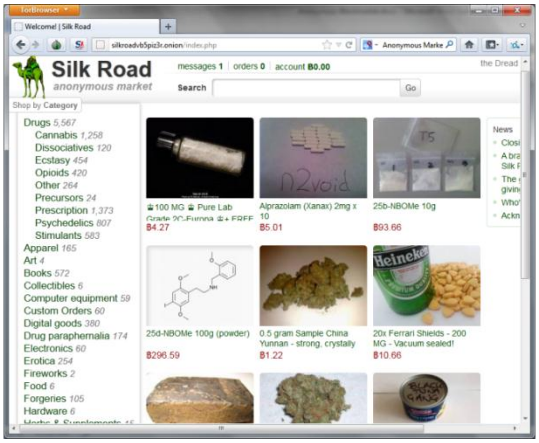
Core.onion has served as the simple entry-point to the .onion network since July, 2007.

People use Tor as a way to bypass traffic filters or monitors throughout the Internet. If using a minimum of SSL encryption, this medium has been recognized as being a "safer" way to communicate over the Internet. What most people do not realize is that there is an entire subnet underground out there called "Darknet" or "Deepweb". Others just call the underground Internet Tor network hidden servers. These hidden servers usually have a ".onion" extension and can only be seen using a Tor proxy or TorVPN. The easiest way to get onto the Tor network is with the Tor Browser Bundle (TBB). It is free and very easy to install and then use. All you have to do is go to the torproject.org and download TBB and within minutes you will be connected.

There are legitimate reasons to use Tor, especially for those that are trying to hide their identities from oppressive governmental regimes or reporters trying to minimize leaking the identity of informants. Some will even stay on the proxy network and use services like Tor mail, a web based email service. There are still some anonymity challenges. If you are on the same network, you may still leak the originating IP address and there is a risk of someone capturing your traffic. Some will even go as far as only using HTTPS (SSL encryption) or reverting back to the good old VPN.

There are darker usages of the hidden servers. There are E-Black Markets all over this network that sell anything from Meth to Machine guns and services that range from assembling credit card data to assassinations ("you give us a picture; we'll give you an autopsy report!"). Most of the sites trade their goods with an e-currency called Bitcoins, an anonymous electronic commodity that can purchase almost anything.

Silk Road
anonymous market
Hacked Logins & Servers
CIA Explosives for Sabotage M
Compact Foldable Gun Patent
uttery Bootleggin
BlackMarket
Reloaded
http://5onwnspjvuk7cwvk.onion



One of the most popular "secret" sites called "The Silk Road" or SR has almost anything you can think of. SR has evolved over the years and has recently dropped its weapon sales section and created a new site called the Armory. Shortly after, the Armory closed due to the lack of traffic and interest. They have also banned assassination services to minimize attention from showing up on Law Enforcement's radar. They still have plenty of drugs, counterfeit items, and stolen goods though.

There are still plenty of other sites that focus on arms dealing or unfiltered auction site. Once you are on Tor, the next thing you would have to do to communication with some of these sites is to get an anonymous Tor based email. This is a web based email that you log into that acts just like a regular email except it only exists in the Tor world. Another popular communications mechanism is TorPM.

Tor Communications
    Tor Mail – http://jhiwjjlqpyawmpjx.onion

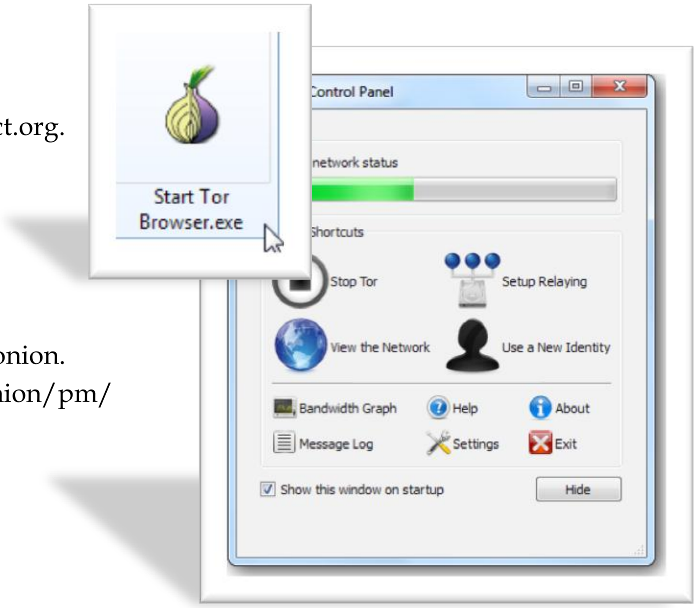
E-Black Market sites
    The Silk Road: http://silkroadvb5piz3r.onion/index.php
    Black Market Reloaded: http://5onwnspjvuk7cwvk.onion/index.php
    Zanzibar's underground marketplace: http://okx5b2r76olbriil.onion/
    TorBlackmarket: http://7v2i3bwsaj7cjs34.onion/
    EU Weapons & Ammunition: http://4eiruntyxxbgfv7o.onion/snapbbs/2e76676/
    CC4ALL (Credit Card site): http://qhkt6cqo2dfs2llt.onion/
    CC Paradise: http://mxdcyv6gjs3tvt5u.onion/
    C'thulhu ("organized criminal group"): http://iacgq6y2j2nfudy7.onion/
    Assassination Board: http://4eiruntyxxbgfv7o.onion/
    Another hitman: http://2v3o2fpukdlpk5nf.onion/
    Swattingservice (fake bomb threats): http://jd2iqa4yt7vqvu5o.onion/
    Onion-ID (fake ID): http://g6lfrbqd3krju3ek.onion/
    Quality Counterfeits: http://i3rg5diydpbxkewu.onion/

Social Network
    mul.tiver.se: http://ofrmtr2fphxkqgz3.onion/

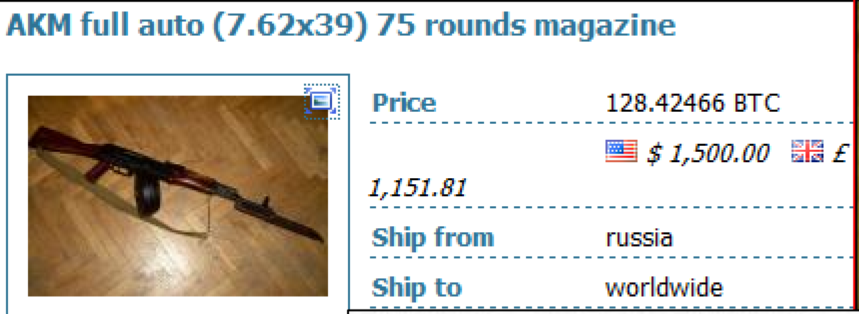
Informational
    LiberaTor (weaponry & training): http://p2uekn2yfvlvpzbu.onion/
    The Hidden Wiki: http://kpvz7ki2v5agwt35.onion/wiki/

Search
    The Tor Hidden Service Search: http://www.ahmia.fi/
    Torch: http://xmh57jrzrnw6insl.onion/
    Torlinks: http://torlinkbgs6aabns.onion/

So let's take this step by step.
1.) Download "Tor Browser Bundle" from torproject.org.
2.) Double left click in "Start Tor Browser".
3.) You should then see Vidalia connecting to Tor.
4.) The Tor Browser should automatically open.
    You are now on the "Tor network".
    You can now access ".onion" domains.
5.) Create a TorMail account on jhiwjjlqpyawmpjx.onion.
6.) Create a TorPM account on 4eiruntyxxbgfv7o.onion/pm/
7.) Enjoy a little more anonymity for research.

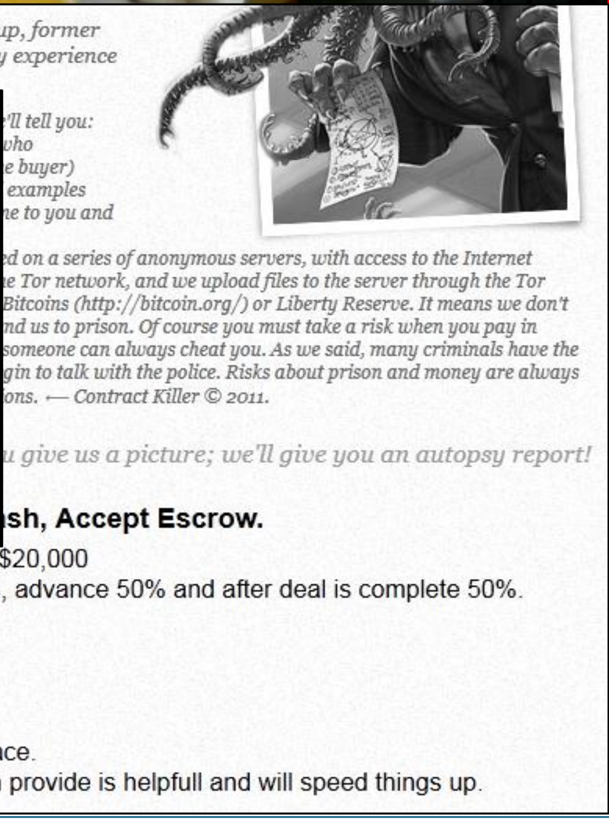


☑ Show this window on startup



AKM full auto (7.62x39) 75 rounds magazine

Price	128.42466 BTC
	$ 1,500.00 £ 1,151.81
Ship from	russia
Ship to	worldwide



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.

'll tell you: who e buyer) examples ne to you and

ed on a series of anonymous servers, with access to the Internet e Tor network, and we upload files to the server through the Tor Bitcoins (http://bitcoin.org/) or Liberty Reserve. It means we don't nd us to prison. Of course you must take a risk when you pay in someone can always cheat you. As we said, many criminals have the gin to talk with the police. Risks about prison and money are always ons. — Contract Killer © 2011.

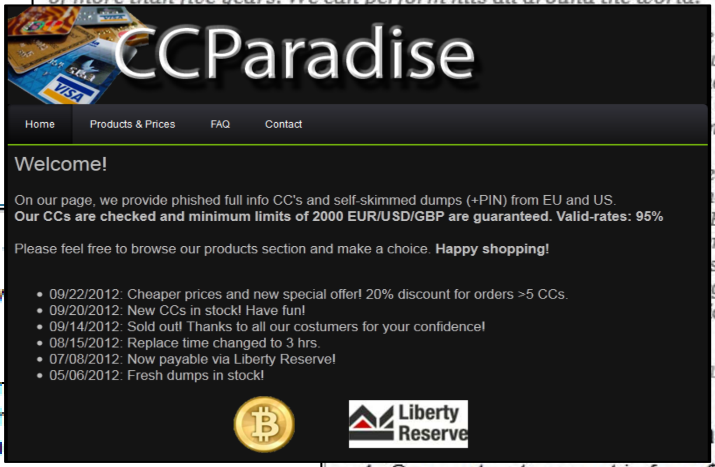
u give us a picture; we'll give you an autopsy report!

sh, Accept Escrow.

1. Our contract amount is from $20,000
2. Payment is divided in 2 parts, advance 50% and after deal is complete 50%.

1. Name.
2. Current City.
3. Clear and recent picture of face.

* Any other information you can provide is helpfull and will speed things up.



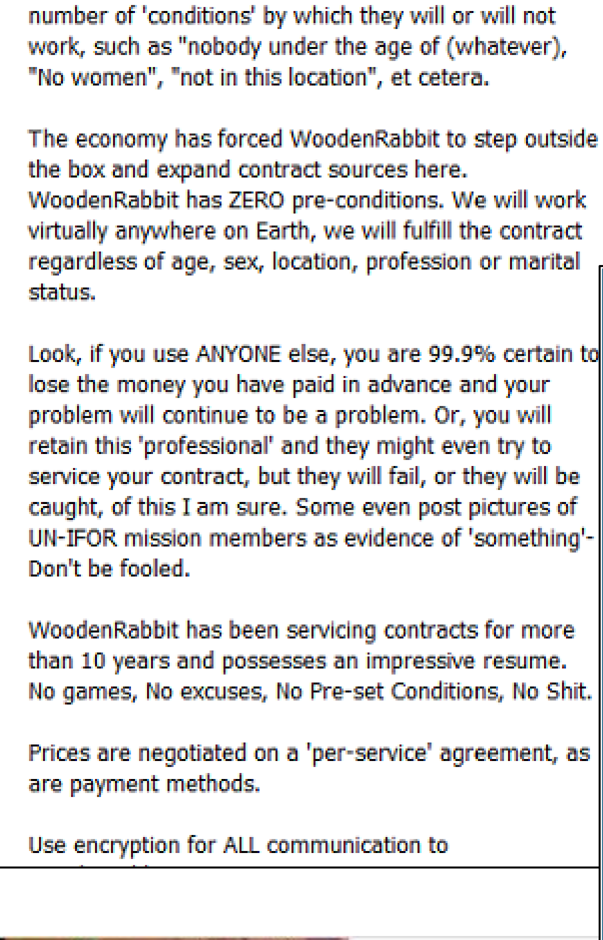
CCParadise

Welcome!

On our page, we provide phished full info CC's and self-skimmed dumps (+PIN) from EU and US.
Our CCs are checked and minimum limits of 2000 EUR/USD/GBP are guaranteed. Valid-rates: 95%

Please feel free to browse our products section and make a choice. **Happy shopping!**

- 09/22/2012: Cheaper prices and new special offer! 20% discount for orders >5 CCs.
- 09/20/2012: New CCs in stock! Have fun!
- 09/14/2012: Sold out! Thanks to all our costumers for your confidence!
- 08/15/2012: Replace time changed to 3 hrs.
- 07/08/2012: Now payable via Liberty Reserve!
- 05/06/2012: Fresh dumps in stock!



Description

Government trained- Worldv Guaranteed.

We have all seen the large r 'hitmen' advertising within th prices anywhere from $2,00 number of 'conditions' by which they will or will not work, such as "nobody under the age of (whatever), "No women", "not in this location", et cetera.

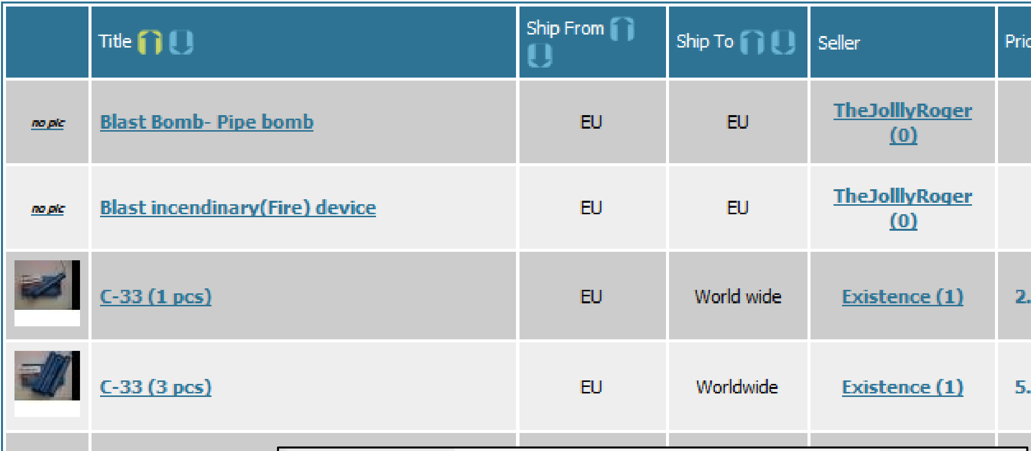
The economy has forced WoodenRabbit to step outside the box and expand contract sources here. WoodenRabbit has ZERO pre-conditions. We will work virtually anywhere on Earth, we will fulfill the contract regardless of age, sex, location, profession or marital status.

Look, if you use ANYONE else, you are 99.9% certain to lose the money you have paid in advance and your problem will continue to be a problem. Or, you will retain this 'professional' and they might even try to service your contract, but they will fail, or they will be caught, of this I am sure. Some even post pictures of UN-IFOR mission members as evidence of 'something'- Don't be fooled.

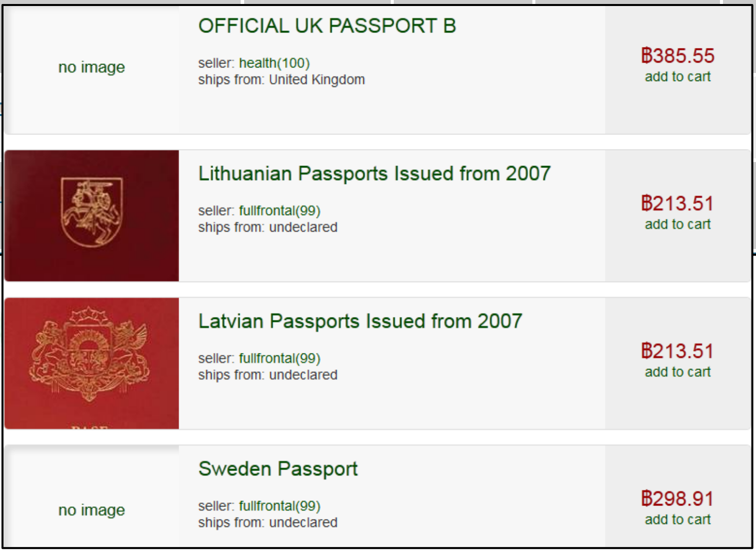
WoodenRabbit has been servicing contracts for more than 10 years and possesses an impressive resume. No games, No excuses, No Pre-set Conditions, No Shit.

Prices are negotiated on a 'per-service' agreement, as are payment methods.

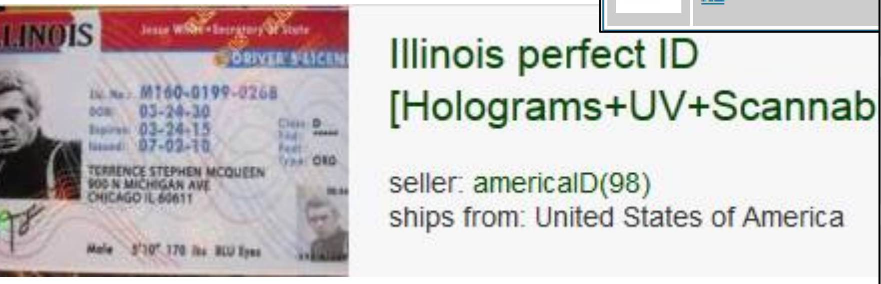
Use encryption for ALL communication to



	Title	Ship From	Ship To	Seller	Pric
no pic	Blast Bomb- Pipe bomb	EU	EU	TheJollyRoger (0)	
no pic	Blast incendinary(Fire) device	EU	EU	TheJollyRoger (0)	
	C-33 (1 pcs)	EU	World wide	Existence (1)	2.
	C-33 (3 pcs)	EU	Worldwide	Existence (1)	5.
no pic	Improvised Frag				
no pic	Poisoned letter bor mail				
	Red MK 7 Powerful x2				



no image	OFFICIAL UK PASSPORT B seller: health(100) ships from: United Kingdom	Ƀ385.55 add to cart
	Lithuanian Passports Issued from 2007 seller: fullfrontal(99) ships from: undeclared	Ƀ213.51 add to cart
	Latvian Passports Issued from 2007 seller: fullfrontal(99) ships from: undeclared	Ƀ213.51 add to cart
no image	Sweden Passport seller: fullfrontal(99) ships from: undeclared	Ƀ298.91 add to cart



Illinois perfect ID [Holograms+UV+Scannab

seller: americaID(98)
ships from: United States of America

Tips:

The Tor network has been around for years and there are many hidden servers out there with ".onion" extensions. There are many .onion sites that are benign, but there are many out there that contain contraband materials such as child pornography, illegal weapons, assassination services, drugs, stolen credit cards, and fake IDs. Investigating these sites can be problematic since the addresses are only available through the Tor system. If you are researching in this realm, be extremely careful. Be aware that there is a more offensive material on that network than the normal Internet. I would document your research and report the CPKP sites to the proper authorities so you do not get dinged for the possible illegal activity.

If you fear that your connection is being monitored, the Tor network will not help if the by a government entity or your ISP is watching your traffic. A simple way to keep them from seeing your data is to use a VPN service, bounce through a Socks5 proxy using an SSL tunnel, and then connect to the Tor network. Just remember, if the VPN or Proxy servers log the information, you are not truly anonymous

OTHER INTERNET HIDDEN NETWORKS: I2P: ANONYMIZING NETWORK

"I2P is an anonymizing network, offering a simple layer that identity-sensitive applications can use to securely communicate. All data is wrapped with several layers of encryption, and the network is both distributed and dynamic, with no trusted parties."

“I2P is a project to build, deploy, and maintain a network supporting secure and anonymous communication. People using I2P are in control of the tradeoffs between anonymity, reliability, bandwidth usage, and latency.” “Unlike many other anonymizing networks, I2P doesn't try to provide anonymity by hiding the originator of some communication and not the recipient, or the other way around. I2P is designed to allow peers using I2P to communicate with each other anonymously — both sender and recipient are unidentifiable to each other as well as to third parties”

"The I2P/Tor outproxy functionality does have a few substantial weaknesses against certain attackers - once the communication leaves the mixnet, global passive adversaries can more easily mount traffic analysis. In addition, the outproxies have access to the cleartext of the data transferred in both directions, and outproxies are prone to abuse, along with all of the other security issues we've come to know and love with normal Internet traffic." - www.i2p2.de

Terminology of Tor Vs. I2P

Tor	I2P
Cell	Message
Client	Router or Client
Circuit	Tunnel
Directory	NetDb
Directory Server	Floodfill Router
Entry Guards	Fast Peers
Entry Node	Inproxy
Exit Node	Outproxy
Hidden Service	Eepsite or Destination
Hidden Service Descriptor	LeaseSet
Introduction point	Inbound Gateway
Node	Router
Onion Proxy	I2PTunnel Client (more or less)
Relay	Router
Rendezvous Point	somewhat like Inbound Gateway + Outbound Endpoint
Router Descriptor	RouterInfo
Server	Router

INTERNET PIRACY: INFORMATION SHARING

File sharing is perfectly legal. The challenge comes when people start sharing files that someone else owns the copyright to. The other term you will hear over and over again is Intellectual Property (IP) ownership. Many of the file sharing sites that you will come across will have access to pirated movies, music, software, and other IP. In the United States, one of the biggest laws that get used against people that share movies and reverse engineer software is the Digital Millennium Copyright Act (DMCA). This is used several times every year at Defcon/Black hat when security researchers go to give a presentation and the IP owners go to court for a gag order.

Security Research

Some people will leak vulnerability findings from their research or even make fully functional Proof of Concept (also called exploits) and release the information to the public. Some of the sites that deal with information release under the "public disclosure" mentality would be Packet Storm Security and the Exploit Database. Whatever side you are on, these two locations have a plethora of information for both offensive and defensive usage, including source code for fully operational exploits.

A lot of the PoC source code is functional and written for Metasploit. Metasploit is a penetration testing framework designed essentially as a point and click application to speed things up and also allow those that are script kiddies to exploit systems. Because of this, anyone that uses Metasploit can now exploit a vulnerability that the program supports.

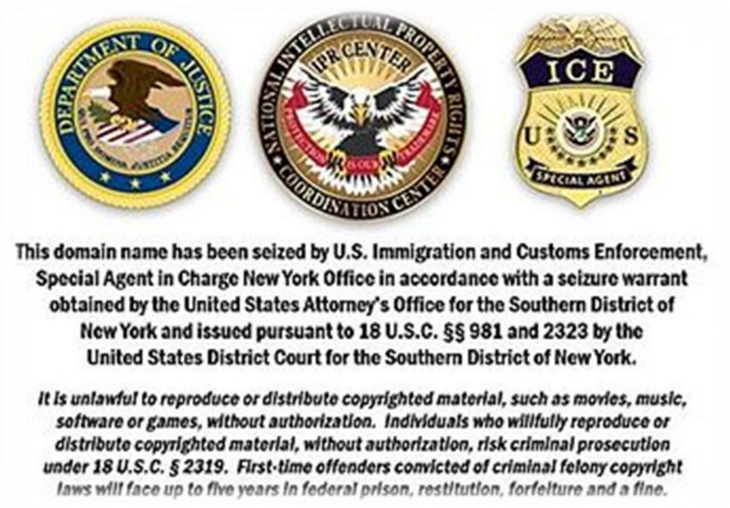
The DMCA is not the end point for security. Many security researchers have gotten around it by using exemptions for education use. There are exceptions to these exceptions. The U.S. Copyright Office published a document on Oct. 26, specifying that "jailbreaking" a smartphone is deemed legal. The same rules do not apply to tablets or gaming consoles. This goes to show that intelligence does not dictate policies and law, money does. This will cause a little bit of difficulty with those in the digital forensics field. Two cases previous to this had different ideas.

> *"Atari Games v. Nintendo: The author does not acquire exclusive rights to a literary work in its entirety. Under the Act, society is free to exploit facts, ideas, processes, or methods of operation in a copyrighted work. To protect processes or methods of operation, a creator must look to patent laws."*
>
> *"Sega v. Accolade: the intermediate copying of the object code of a copyrighted computer program as necessary to disassemble the program to view its expression was a fair use under Section 107 of the copyright laws."*

"Viruses don't harm, ignorance does!" - VX Heavens. There are several sites that even specialize in Viruses, Worms, Trojans, and other malicious logic. Most of the sites do not last long doe to legal issues. VX Heavens even has the good old ***"Error 451: Unavailable for legal reasons"*** displayed.

File Sharing

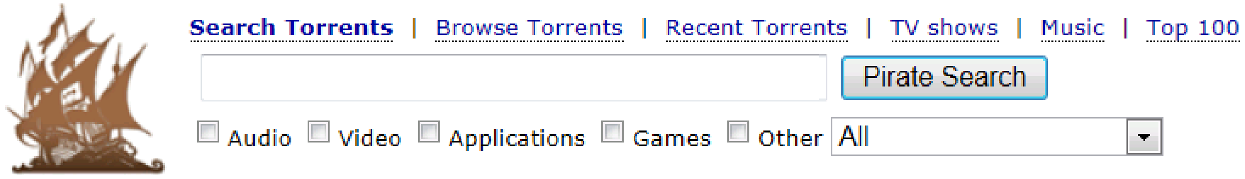
The history of file sharing has been an ever evolving and bloody one. From BBS systems to news groups to IRC to P2P, the methods have changed, but the mentality has not. One of the more common mediums used at this point is called Bit Torrent. This allows several people to seed a file while others download bits and pieces of all that are hosting. A person can create a torrent from a file or folder. Once the file is created and hashed to verify integrity of the data, it is them posted to torrent trackers. Many of the torrent trackers use UDP protocol while others use an HTTP connection. Some of the sites even force you to make an account and upload the .torrent file manually. This minimizes the same data flooding the trackers. DO NOT TORRENT OVER TOR! Using P2P applications over Tor will DoS the network.


ICE
U S
SPECIAL AGENT

This domain name has been seized by U.S. Immigration and Customs Enforcement, Special Agent in Charge New York Office in accordance with a seizure warrant obtained by the United States Attorney's Office for the Southern District of New York and issued pursuant to 18 U.S.C. §§ 981 and 2323 by the United States District Court for the Southern District of New York.

It is unlawful to reproduce or distribute copyrighted material, such as movies, music, software or games, without authorization. Individuals who willfully reproduce or distribute copyrighted material, without authorization, risk criminal prosecution under 18 U.S.C. § 2319. First-time offenders convicted of criminal felony copyright laws will face up to five years in federal prison, restitution, forfeiture and a fine.

On 30 June 2010, US government officials seized several file sharing domains including tvshack.net owned by Richard O'Dwyer for *"violations of Federal criminal copyright infringement laws".* Violating copyright or IP law is big deal because the owners of the material, including the MPAA claim that: *"The industries contribute over $15 billion in taxes annually. The U.S. economy loses an estimated $25.6 billion per year, and an estimated 375,000 jobs per year, to criminal copyright infringement."* In simple terms, do not share material without permission from the IP owner. The IP owners have been known to break the law themselves to find you are harm your ability to violate their rights. Sony has even gotten in trouble for sending out their material with a rootkit pre-installed. Though they claimed it was an anti-piracy measure.


Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100
Pirate Search
☐ Audio ☐ Video ☐ Applications ☐ Games ☐ Other
All

The Pirate Bay (TPB) "World's most resilient tracking" is file sharing site that has lasted many court battles. When visiting the site, you can find almost anything you want. Most of the content is considered IP theft but some of it is perfectly legitimate. TPB has two main sites. The first one currently is at www.thepiratebay.se while the second has gone on to the Tor network and resides at jntlesnev5o7zysa.onion. TPB used to use torrent only, but has now moved to magnet links to provide less accountability or "traceability" for hosting the .torrent files.

The website www.EZTV.it is another site that allows you to download files using a bit torrent client. The files they specialize in are TV show only. Some people that use this site will argue that it is NOT IP theft if they already pay for the license to watch the content through their cable or satellite TV. That side of the fight claims it to be "fair use" and the same as using devices like Tivo to record your show for later viewing.

"Section 107 contains a list of the various purposes for which the reproduction of a particular work may be considered fair, such as criticism, comment, news reporting, teaching, scholarship, and research. Section 107 also sets out four factors to be considered in determining whether or not a particular use is fair.

1. The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes
2. The nature of the copyrighted work
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole
4. The effect of the use upon the potential market for, or value of, the copyrighted work "

- copyright.gov : FL-102, Reviewed June 2012

The Hactavist group Anonymous released a new evolution of Peer 2 Peer applications called Tyler for their own version of its own 'WikiLeaks' project. *"It will not be deployed on a static server. TYLER will be P2P encrypted software, in which every function of a disclosure platform will be handled and shared by everyone who downloads and deploys the software. In theory, this makes it sort of like BitCoin or other P2P platforms in that there is virtually no way to attack it or shut it down. It would also obviously be thoroughly decentralized."* - *"TYLER is a massively distributed and decentralized Wiki pedia style p2p cipher-space structure impregnable to censorship"* – anonnews.org. The name of this program is called Tyler (after the movie Fight club) and is part of Project Mayhem 2012: Dangerous Idea #1. The video released by Anonymous can be found at http://anonnews.org/press/item/1783. "

The potential issues of Tyler come down to what is leaked. If it is governmental classified information, lives could be lost. Imagine a list of covert operatives active in a foreign country being leaked out. This has happened in the past and many lives were lost. Robert Hanssen is a prime example of this. He was a spy for the USSR working in the FBI and because of the leak; he is now spending life at a Supermax federal prison in Florence, Colorado. If it is economic/industrial espionage, the penalties are almost as severe. Sometimes the espionage isn't as covert as some would think. In January 2010, the Chinese Chengdu J-20 stealth fighter jet was speculated by some as having been reverse engineered from the parts of a US F-117 Nighthawk stealth fighter shot down over Serbia in 1999.

Data warehousing and cloud computing are high targets for such activity. The funny part is, file sharing groups are also taking to this medium for that exact mentality. Spread the wealth and allow everyone access to the data.

Here are some examples of how someone can decrease the probability of them getting caught.

Example 1	Connect directly	This leaves a direct fingerprint to the source. This is never suggested and usually points to a novice or script kiddie.
Example 2	Connect to a botnet	This changes the fingerprint of the hardware because you are not attacking the target, the zombie network / botnet is.
Example 3	change their MAC address	This changes the fingerprint of the hardware
	Connect to a VPN	This will act as a proxy by adding them to a completely different network and having the VPN gateway as the "originating" address from the outside.
Example 4	change their MAC address	This changes the fingerprint of the hardware
	Connect to a VPN	This will act as a proxy by adding them to a completely different network and having the VPN gateway as the "originating" address from the outside.
	Connect to Tor	This again adds a layer of obfuscation to the target by ripping of the source information and adding its own.
Example 5	change their MAC address	This changes the fingerprint of the hardware
	Connect to a VPN	This will act as a proxy by adding them to a completely different network and having the VPN gateway as the "originating" address from the outside
	Connect to a Proxy	This again adds a layer of obfuscation to the target by ripping of the source information and adding its own.
	Connect to Tor	This again adds a layer of obfuscation to the target by ripping of the source information and adding its own.
Example 6	change their MAC address	This changes the fingerprint of the hardware
	Connect to a VPN	This will act as a proxy by adding them to a completely different network and having the VPN gateway as the "originating" address from the outside.
	Connect to a Proxy	This again adds a layer of obfuscation to the target by ripping of the source information and adding its own.
	Use an encrypted tunnel to Proxy	This distorts the view from prying eyes
	Connect to IP2	This again adds a layer of obfuscation to the target by ripping of the source information and adding its own.

The attacker can also bounce through multiple proxies, but the more connections you go through, the slower the connection will be. Bouncing through multiple servers is nothing new. It is also not as easy to trace back as most of the movies seem to show. As mentioned before, if the server does not log, the job of the forensics analyst becomes a LOT more difficult if not impossible. This is where you may have to get several court orders from multiple countries to trace back the source of the attack

RESOURCES

Resource Name	Location
4Chan	www.4chan.org
Anonymous News	www.anonnews.org
Anonymous Operations	www.anonops.org
Black Market Reloaded	5onwnspjvuk7cwvk.onion
C'thulhu	iacgq6y2j2nfudy7.onion
DC3 DISPATCH	dispatch@dc3.mil
Exploit Database	www.exploit-db.com
Exploits Database	www.exploitsdownload.com
EzTV	www.eztv.it
FBI In the News	fbi@subscriptions.fbi.gov
Hack-DB	www.hack-db.com
I2P Project	www.i2p2.de
Information Warfare Center	informationwarfarecenter.com
Infosec Instructor	www.infosecinstructor.com
Infragard	www.infragard.org
ISSA	www.issa.org
Packet Storm Security	www.packetstormsecurity.org
Sans Internet Storm Center	isc.sans.org
Secunia	www.secunia.org
Silk Road	silkroadvb5piz3r.onion
The Library of Congress	www.loc.gov
The Pirate Bay	www.thepiratebay.se
The Tor Project	www.torproject.org
Torrent Freak	torrentfreak.com
U.S. Copyright Office	www.copyright.gov
Xssed	www.xssed.com
Zone-h	www.zone-h.org