IBM MSS

The Deep Dark Web

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: FEB 3, 2015

BY: JOHN KUHN, SENIOR THREAT RESEARCHER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW/KEY FINDINGS

In the security world and mainstream media, we always hear the term "Deep Web" come up as a place that contains more content than the "standard" web everyone uses. It is also known as a place where you can purchase nefarious goods, such as drugs, firearms, and pornography, anything an entrepreneuring criminal might need. These statements are correct. In fact, the Deep Web is hardly a place you want to visit for any legitimate reason.

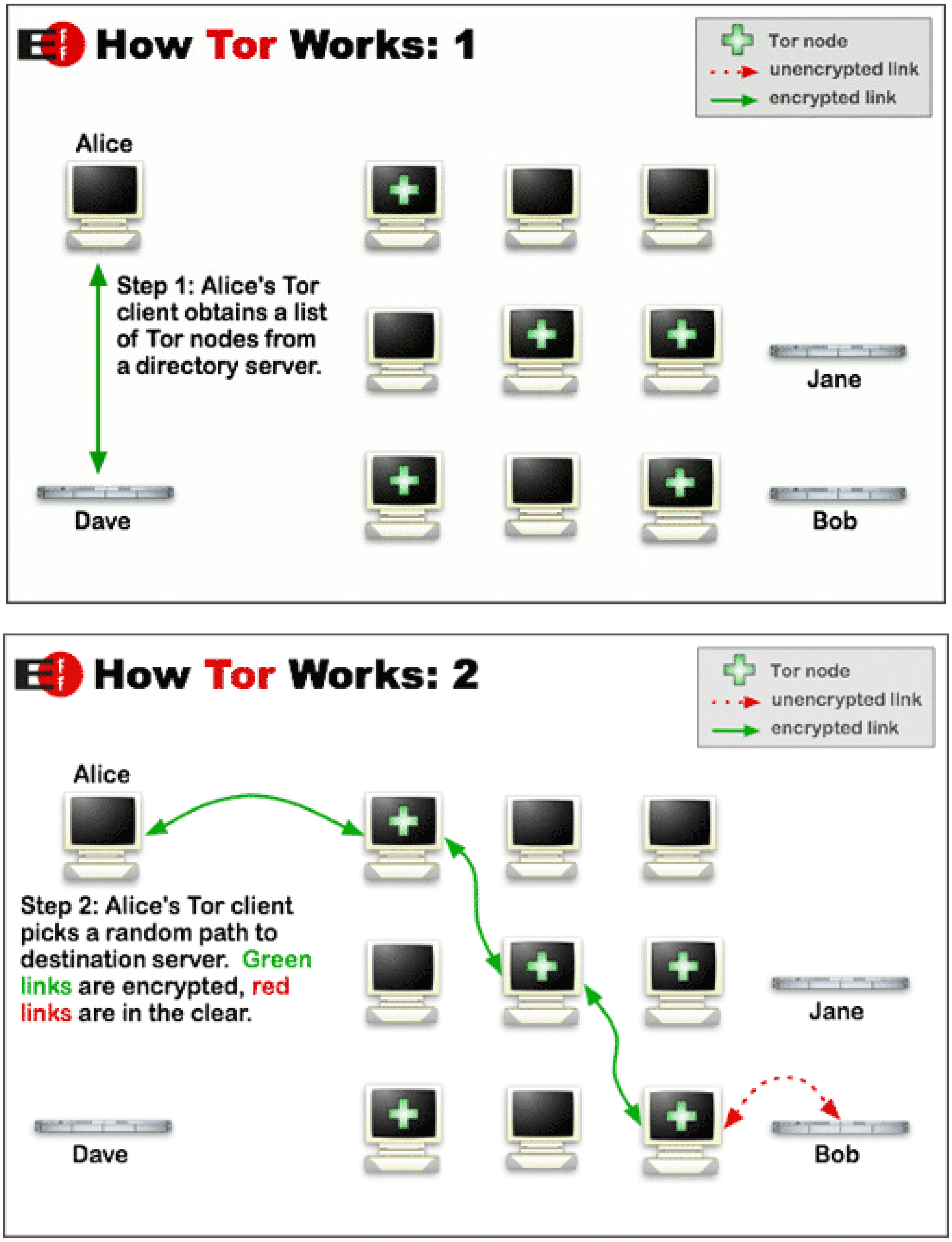
This paper takes a high level overview of two mainstream dark webs, including TOR or Onion sites as well as I2P, a lesser known, but still popular anonymous peer-to-peer (P2P) network. There are, of course, other similar anonymous networks, however these are the two most used. This underbelly of the Internet is filled with sites, images, and videos of illegal content making it a den for criminals worldwide.

The importance of understanding the Deep Web for any organization is twofold. You do not want to allow access to the Deep Web from users within your network because of the illegal content and services stored there. That being said, it is important for organizations to understand that there could be content pertaining to them being shared such as potential attacks, leaked data, or stolen accounts being sold to allow direct access into their network.

TOR AND ONION SITES - WHAT ARE THEY AND HOW DO THEY WORK?

Tor was originally designed, implemented, and deployed in 2004 as a third-generation onion routing project of the U.S. Naval Research Laboratory. It was 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 civilians, the military, journalists, law enforcement officers, activists, and many others.

Tor at its very basic level is a P2P network that allows anonymous, encrypted communication from host to host. It can also serve as a proxy with exit points known as "exit nodes" to allow users to anonymously browse web pages externally to the World Wide Web. This offers moderate anonymity to anyone looking to hide their identity as well as encrypt communication back to their host computer or device.



Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

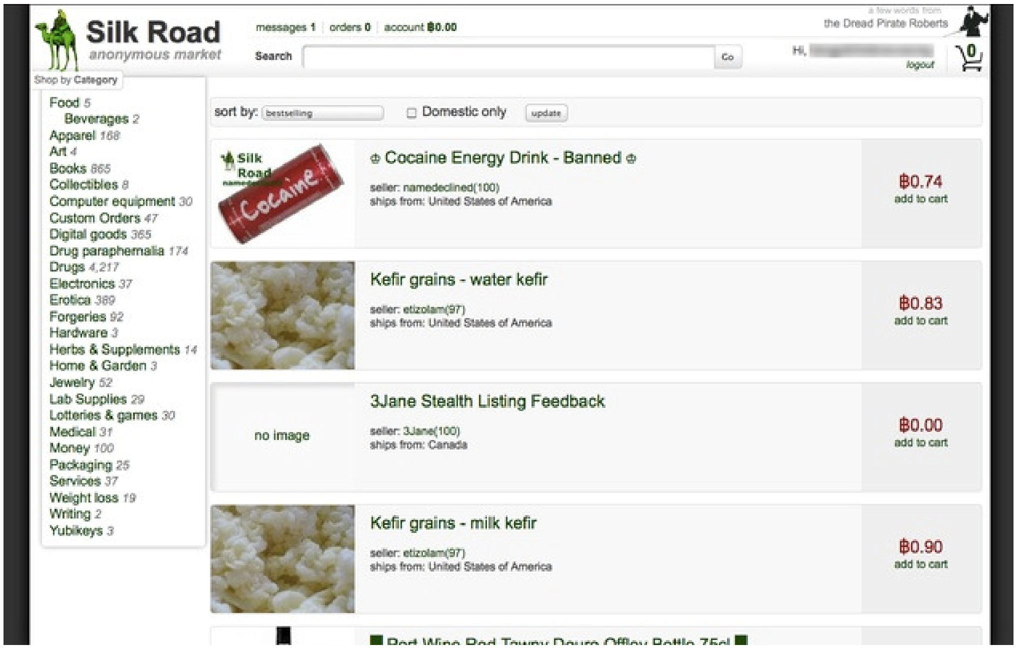
Source: Electronic Frontier Foundation (EFF)

Tor's hidden services let users publish websites and other services without needing to reveal the location of the site. These sites have the domain .onion and can only be accessed once you've entered the Tor network. Addresses in the .onion pseudo-TLD are generally opaque, non-mnemonic, 16-character alpha-semi-numeric hashes, which are automatically generated based on a public key when a hidden service is configured. These 16-character hashes can be made up of any letter of the alphabet and decimal digits beginning with 2 and ending with 7, thus representing an 80-bit number in base32. It is possible to set up a human-readable .onion URL (e.g. starting with an organization's name) by generating massive numbers of key pairs (a computational process that can be parallelized) until a sufficiently desirable URL is found. For example, "http://ext5g4fuxxxhqi11.onion/" is how these site names are commonly formatted. However, more popular sites can have a more descriptive name within the first 16 characters.

It is within these sites that the trouble lies with the Tor network. What was once a place to anonymously share information has been over ridden with criminal activity. Services, such as buying drugs, weapons, stolen credit cards, or even ordering an assassination, have become common place.

SILK ROAD

One of the most notorious sites that existed on the Deep Web was Silk Road, a site that specialized in buying, selling, and trading all sorts of illegal contraband. In March 2013, the site had 10,000 products for sale by vendors, 70 percent of which were drugs. In October 2014, there were 13,756 listings for drugs, grouped under the several categories such as, psychedelics, prescription, opioids, cannabis, and several others. There were also legal goods and services for sale such as apparel, art, books, cigarettes, erotica, jewelry, and computer equipment.



⊕ Cocaine Energy Drink - Banned ⊕
seller: namedeclined(100)
ships from: United States of America
฿0.74

Kefir grains - water kefir
seller: etizolam(97)
ships from: United States of America
฿0.83

3Jane Stealth Listing Feedback
seller: 3Jane(100)
ships from: Canada
฿0.00

Kefir grains - milk kefir
seller: etizolam(97)
ships from: United States of America
฿0.90

Port Wine Red Tawny Douro Offley Bottle 75cl

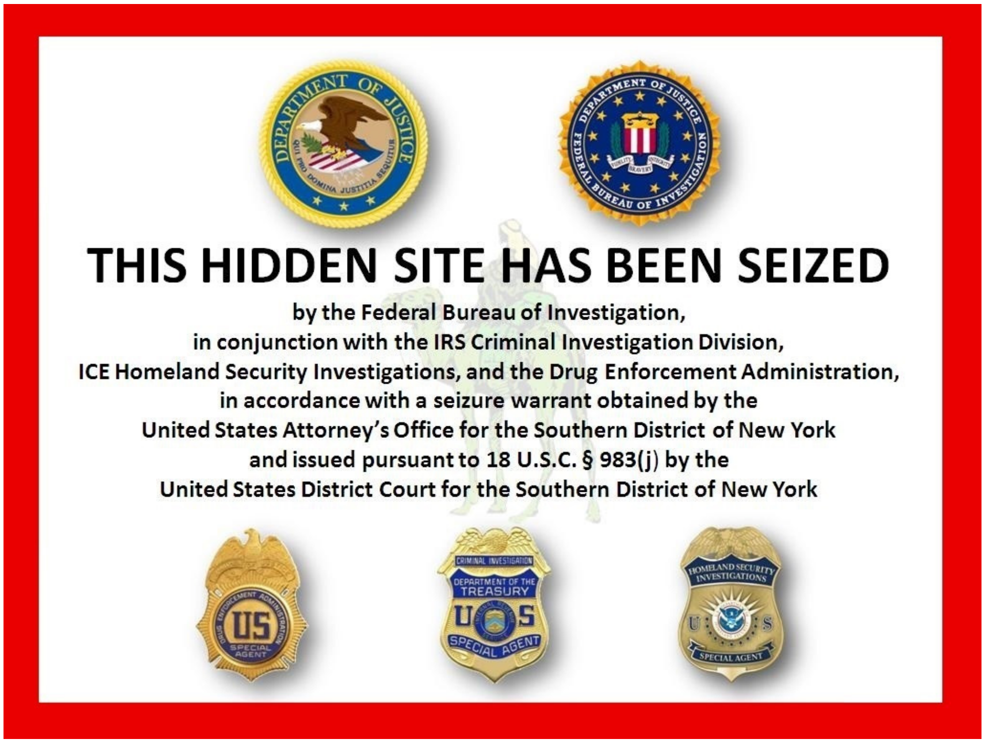
Source: Wikipedia

In order to purchase an item from Silk Road, a potential buyer would need to have bitcoins. This is the most common form of currency used on the Deep Web today. Buyers needed to put their bitcoins into an escrow account or wallet with Silk Road and they facilitated the transfer of funds for an 8 to 15 percent commission fee.

This escrow system was compromised in 2014 and bitcoins valued at 2.7 million dollars were reported stolen from the Silk Road patrons.

After a sale, the illegal drugs were shipped to the buyer at their own risk. P.O. Boxes and fake addresses were commonly used to receive the goods at much risk to the buyer. For example, Ulbricht, one of the founders of Silk Road, was caught because he had documents shipped to himself in the U.S. from Canada, which were intercepted by customs.

Silk Road has a troubled history with law enforcement and rightly so.



THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
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. § 983(j) by the
United States District Court for the Southern District of New York

Source: WIkipedia

Aside from multiple investigations and arrests made by federal law enforcement of vendors using the site, the site itself has been attacked and taken down several times. After the first seizure of all Silk Road assets, another replacement site was born dubbed "Silk road 2.0" and illegal buying and selling continued. Once again in June 2014, the FBI seized the reborn website and its assets. Since the Tor network is so dynamic, it shows how quickly marketplaces like Silk Road can be created, however the creators are certainly not hidden from law enforcement.

Silk Road has now moved to the I2P network and is accepting a wider range of crypto-currency including Darkcoin, Dogecoin, and Anoncoin, with more along the way. Now dubbed Silk Road Reloaded, they continue to offer a wide range of goods while maintaining their no credit card data or weapons policy. At the time of this writing, the new site remains largely unused, likely due to it being slightly more difficult to set up the I2P network. This may change, however, in time as more criminals become aware and savvier at using I2P.

I2P - WHAT IS IT AND HOW DOES IT WORK?

When speaking in terms of Deep Web, I2P would be considered the "very Deep Web". On the technology side, it is very different from Tor, however, the same basic principle remains. It's an encrypted P2P network that has services, as well as exit nodes, or out proxies. Whereas Tor has a much larger user base, I2P was designed and optimized for its hidden services.

Services include (from the I2P main site):

Email: Integrated web mail interface, plugin for serverless email.

Web browsing: Anonymous websites, gateways to and from the public Internet.

Blogging and forums: Blogging and Syndie plugins.

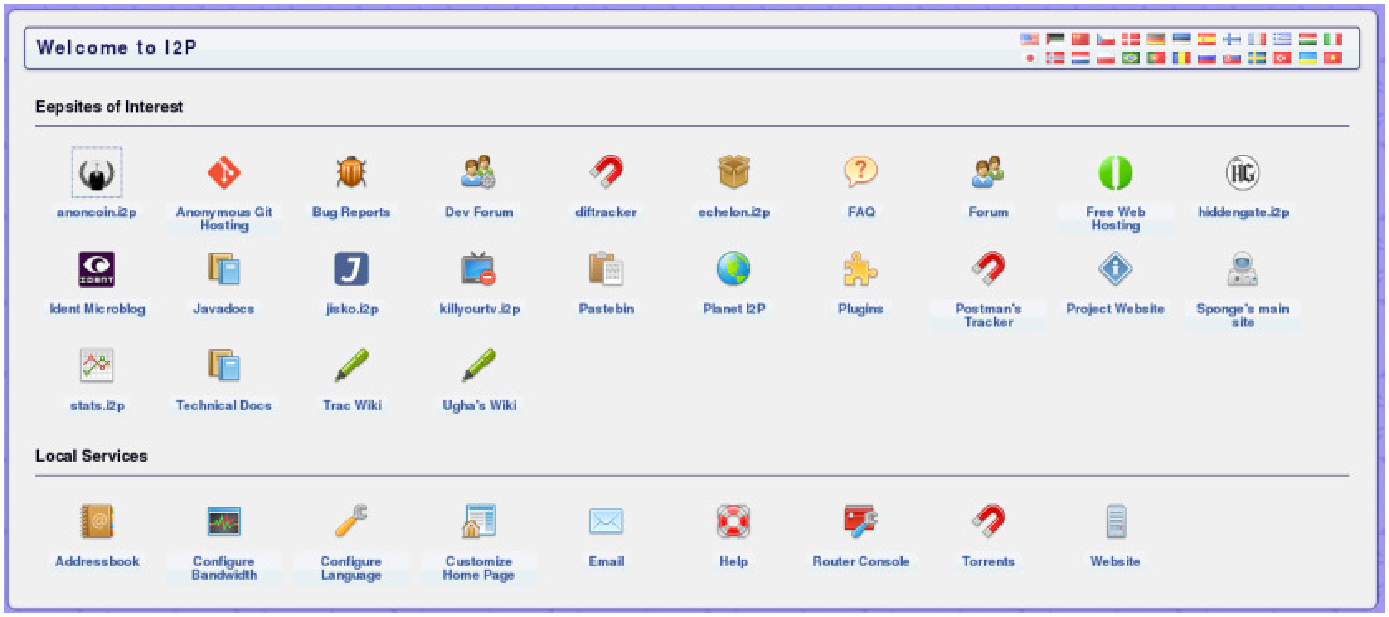
Website hosting: Integrated anonymous web server.

Real-time chat: Instant messaging and IRC clients.

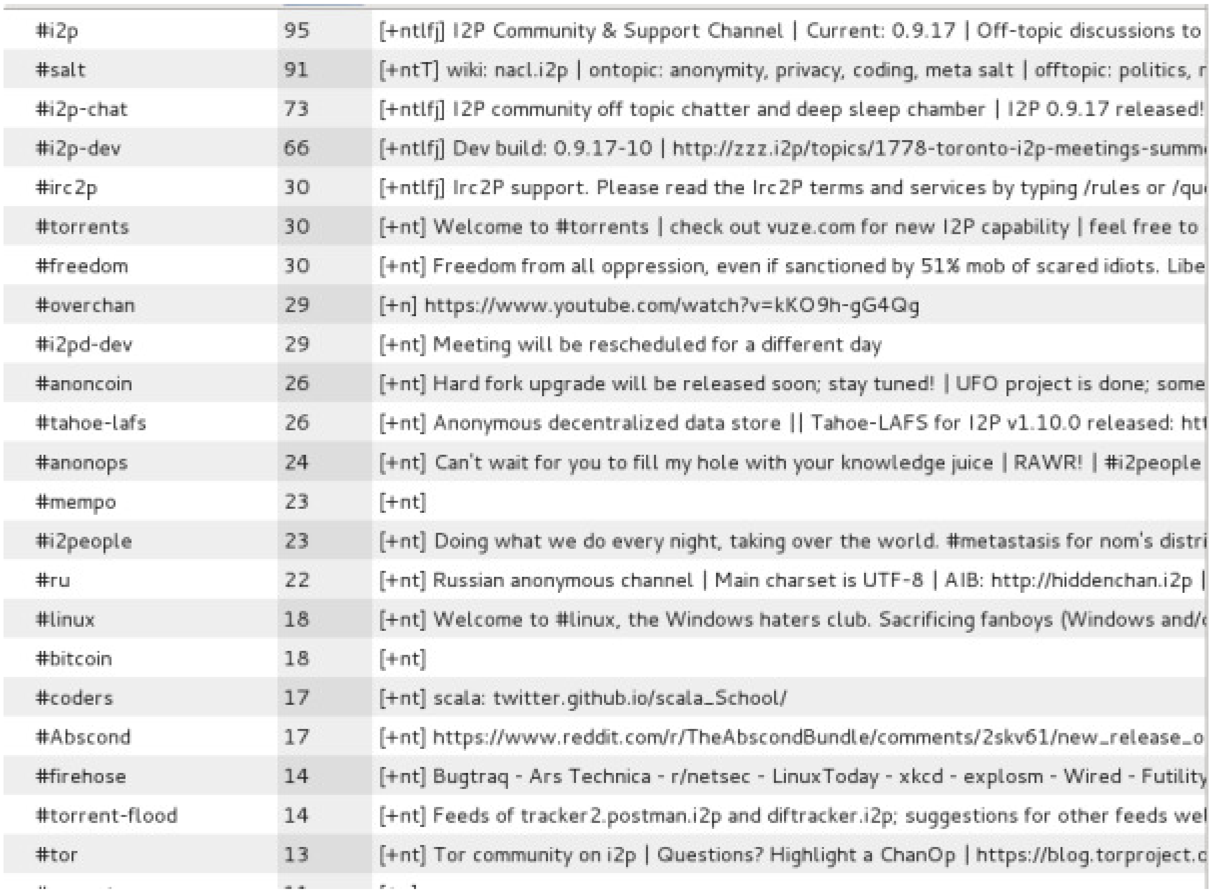
File sharing: ED2K and Gnutella clients, integrated BitTorrent client.

Decentralized file storage: Tahoe-LAFS distributed filesystem plugin.

I2P sites are known as "eepSites" with an extension of .i2p and also offer anonymous and encrypted web hosting not accessible by the standard Internet. Finding these eepSites can prove to be far more difficult then locating nefarious sites on Tor, simply because the underground markets and sites still remain in the onion network.



Where I2P really shines is within its built in services and most of the users converse over Internet Relay Chat (IRC).



#i2p	95	[+ntlfj] I2P Community & Support Channel | Current: 0.9.17 | Off-topic discussions to
#salt	91	[+ntT] wiki: nacl.i2p | ontopic: anonymity, privacy, coding, meta salt | offtopic: politics, r
#i2p-chat	73	[+ntlfj] I2P community off topic chatter and deep sleep chamber | I2P 0.9.17 released!
#i2p-dev	66	[+ntlfj] Dev build: 0.9.17-10 | http://zzz.i2p/topics/1778-toronto-i2p-meetings-summ
#irc2p	30	[+ntlfj] Irc2P support. Please read the Irc2P terms and services by typing /rules or /qu
#torrents	30	[+nt] Welcome to #torrents | check out vuze.com for new I2P capability | feel free to
#freedom	30	[+nt] Freedom from all oppression, even if sanctioned by 51% mob of scared idiots. Libe
#overchan	29	[+n] https://www.youtube.com/watch?v=kKO9h-gG4Qg
#i2pd-dev	29	[+nt] Meeting will be rescheduled for a different day
#anoncoin	26	[+nt] Hard fork upgrade will be released soon; stay tuned! | UFO project is done; some
#tahoe-lafs	26	[+nt] Anonymous decentralized data store || Tahoe-LAFS for I2P v1.10.0 released: htt
#anonops	24	[+nt] Can't wait for you to fill my hole with your knowledge juice | RAWR! | #i2people
#mempo	23	[+nt]
#i2people	23	[+nt] Doing what we do every night, taking over the world. #metastasis for nom's distri
#ru	22	[+nt] Russian anonymous channel | Main charset is UTF-8 | AIB: http://hiddenchan.i2p |
#linux	18	[+nt] Welcome to #linux, the Windows haters club. Sacrificing fanboys (Windows and/
#bitcoin	18	[+nt]
#coders	17	[+nt] scala: twitter.github.io/scala_School/
#Abscond	17	[+nt] https://www.reddit.com/r/TheAbscondBundle/comments/2skv61/new_release_o
#firehose	14	[+nt] Bugtraq - Ars Technica - r/netsec - LinuxToday - xkcd - explosm - Wired - Futility
#torrent-flood	14	[+nt] Feeds of tracker2.postman.i2p and diftracker.i2p; suggestions for other feeds wel
#tor	13	[+nt] Tor community on i2p | Questions? Highlight a ChanOp | https://blog.torproject.c

Most of the channels on the network are for open, encrypted communication for users of the network. However, as you can see from the list above, a small number of members from the hacktivist group Anonymous have opened a channel here.

The majority of "malicious" content still resides on the Tor network as I2P seems to be less used by criminals. This may change in the coming months and years as Tor has had its issues with arrests, snooping and even malware being injected at exit nodes. We may see a larger movement to other anonymous networks such as I2P to continue their black markets.

RECOMMENDATIONS/MITIGATION TECHNIQUES

Use web gateways, web proxies, and IDS to identify outgoing communication to anonymous networks. It's imperative that you block communication from your network to these networks. Illegal content, goods, and wares are extremely common place within them, allowing users of your network to access them can put them and the corporation at great risk. Additionally, an advanced adversary might utilize these networks as a place to exfiltrate stolen data and bypass security measures because of their default encryption capability.

Block Tor exit nodes from communicating with your network. Obtaining lists of commonly known exit nodes on a regular basis is key for this. Setting blocking rules into your firewall infrastructure for these exit nodes can go a long way in keeping attacks sourcing from the Tor network from your infrastructure. These lists can often be found freely on the Internet or through your security intelligence provider.

Understanding what the Dark Web might contain when it pertains to your company or brand is a delicate situation to tackle. It's critical that organizations understand that content on these networks can be illegal to view or open (even by accident). It's highly recommended you employ an intelligence service that specializes in traversing the many darknet sites for intelligence gathering purposes.

IDPS SIGNATURES

IBM PROVENTIA

Tor_Client_Request

This signature detects a host running TOR for the purposes of anonymous browsing, file transfer, or any other application supporting SOCKS or HTTP proxies. Each time the client attempts to retrieve a TOR server encryption key, this event will fire. Each client will attempt to get keys continuously resulting in a number of events. As part of the server request, the client sends their key / certificate which can result in the event SSL_Unsolicited_Certificate triggering if it's enabled. By manually setting a block response for TOR_Client_Request, the client will be unable to tunnel traffic with TOR.Because TOR encrypts the traffic, it is not possible to process the proxied data.

SNORT

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 80,443,9001,9030 (msg: “TOR client access detected”; pcre:”/.*(Tor).+(client <identity>).*/i”; classtype:policy-violation; sid:50009;
```

```
alert tcp any any -> $HOME_NET any (msg: "TOR 1.0 Proxy Connection Attempt"; content: "TOR"; content: "<identity>"; within:30; classtype:policy-violation; resp:rst_all; sid:5000030; rev:1;)
```

CISCO

Tor

Tor over HTTP

REFERENCES

Wikipedia
https://www.wikipedia.org/

I2P
https://geti2p.net/en/

Tor Project
https://www.torproject.org/

CONTRIBUTORS

Michelle Alvarez, Researcher/Editor, Threat Research Group

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. This information is provided “AS IS,” and without warranty of any kind.