10
The Dangers of the Dark Web

The Dark Web has a bad reputation. Everyone has heard something about things that go on there. Sadly, the media has blown the stories out of proportion. As I've stated several times in this book, the main issues for the standard user are how you access it (dedicated browser) and the anonymity gained on it. So many of the stories you've heard of are exaggerated and aren't true.

But, there is a kernel of truth in the stories, and it's these that you need to be aware of.

This chapter will dive into these stories of the dangers on the Dark Web.

We will be covering the following topics in this chapter:

- Online scams
- Minimizing the risks on a Dark Web market
- Dangers of the Dark Web

Online scams

One of the dangers that exist both on the Surface Web and the Dark Web are scams.

Scams on the Dark Web are many and varied. Scams on Dark Web markets are common, as are ones performed by independent sellers

I'll talk about some of these in this chapter.

But one of the dangers are *index* sites, such as the Hidden Wiki. It's a site, founded in 20111, that lists links to Dark Web sites. It went down in 2013, but it was cloned and still works.

Although most of the links are valid (people pay money to list their Dark Web site there), there are sites which are posted there for the sole purpose of scamming people, and stealing their money.

Never, ever provide or write your debit or credit card numbers while on Dark Web sites. Never provide your true personal information. Since there's no real way of verifying someone's identity on the Dark Web, it's safer to hide your own.

That's part of anonymity and being anonymous

The following screenshot is of the Hidden Wiki:

Screenshot of Hidden Wiki website

After being on the Dark Web for a while, you'll probably get a feel for the bad and illegal sites. That doesn't mean that you should let your guard down. Even on legitimate sites, the content you can view there can sometimes be unnerving.

Horrible videos, various types of services, and products from the disgusting to the perverse, can be found. Be careful if you have a weak stomach or are sensitive. Don't just click links. Try to read up about the site you want to access.

Also, many links can lead to malicious sites

And as a parent myself—don't let your children have free access to the Dark Web.

On the other hand, if you're looking to hire an assassin, you're probably out of luck. Most of those sites that advertise murder-for-hire services are fake.

Hitmen don't offer their services in such an overt manner. You can communicate with them on the Dark Web, but you can't just look them up.

These sites either run by law enforcement agencies, to capture people planning murder, or by scammers who demand between 15,000-25,000 US dollars, receive the money and vanish, or blackmail the person who paid them.

The market for fake IDs, social security numbers, credit cards, and other fake credentials is massive.

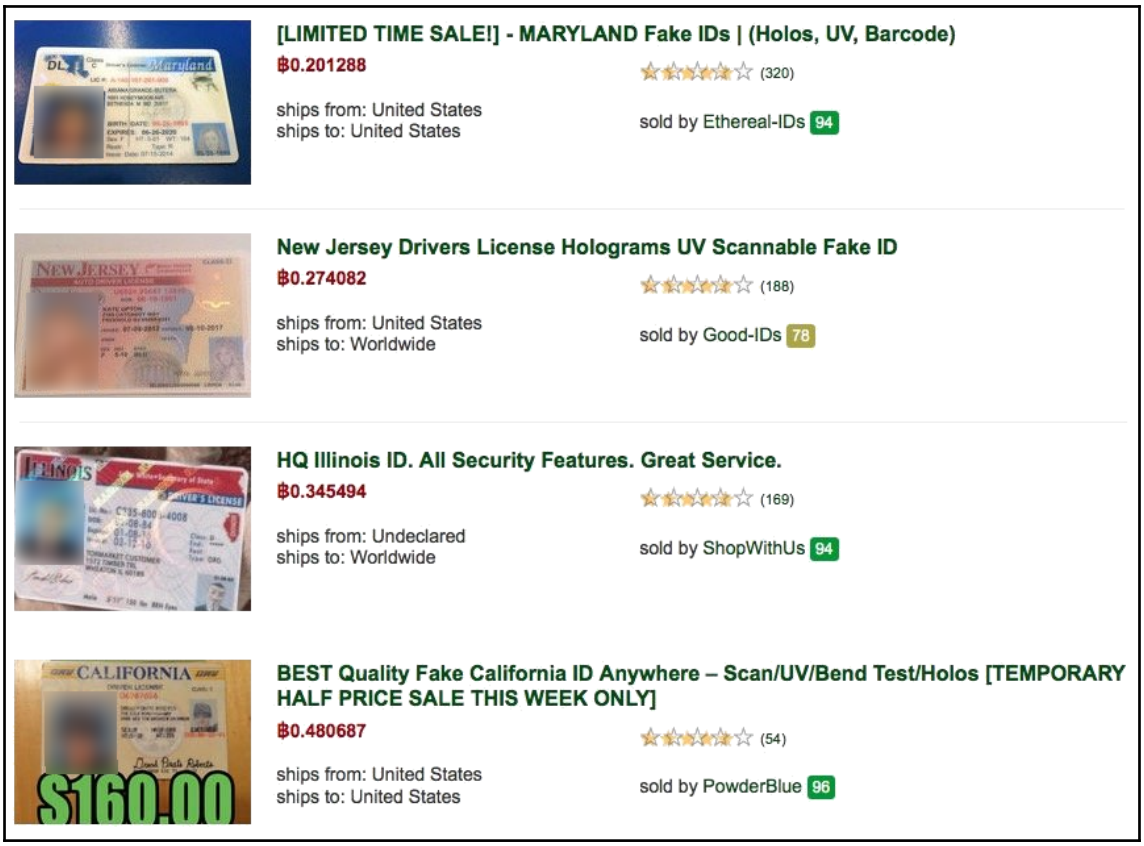
But not all of them are legit. Some of them are provided by scammers, who deliver bogus fake IDs, which crumble, even under the lightest scrutiny.

One of the problems are that the sites that offer these fake credentials, look professional, and feel legitimate. We've been conditioned to view sleek-looking sites as professional and proper. But in some situations, they can be malicious.

The following is a screenshot from a website that sells fake IDs:

Website selling Fake IDs

Here is another website that sells fake IDs online:

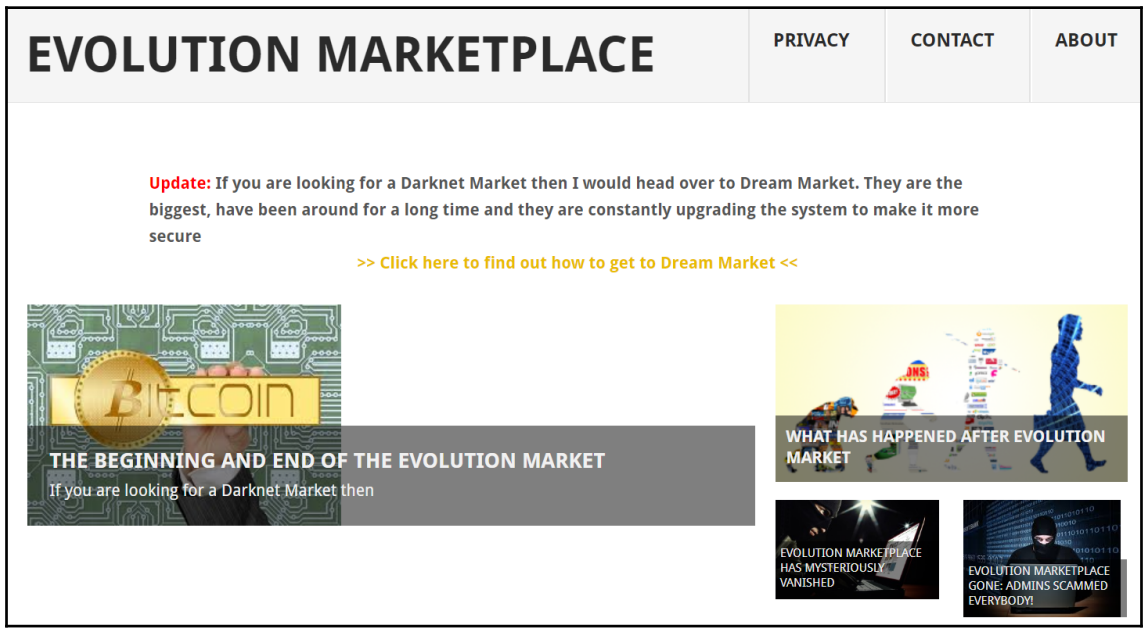


People have had their PayPal accounts stolen on sites like these, thinking that using PayPal would somehow be safer. You should find sites where trusted vendors sell. They should be multisig, for starters.

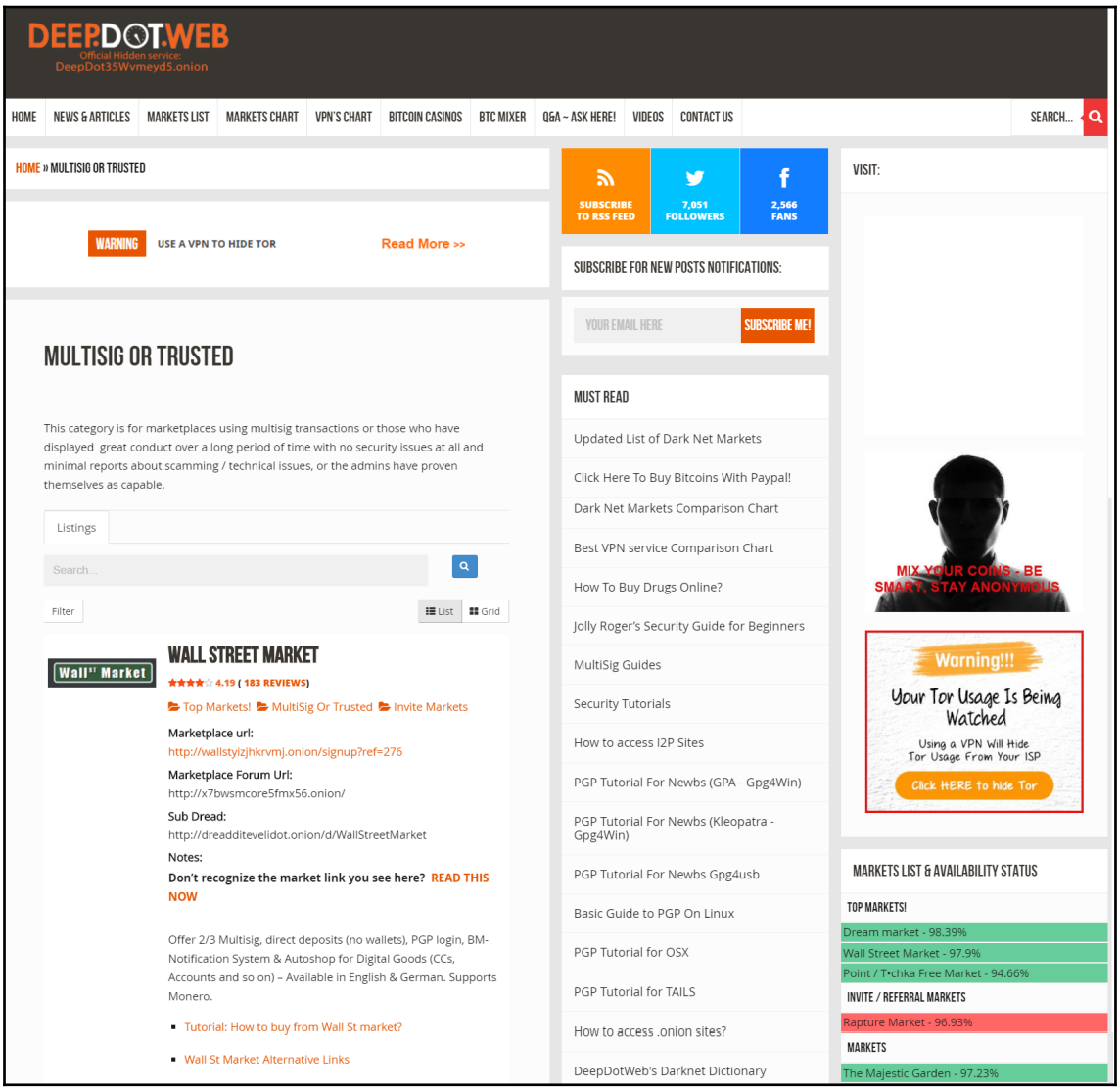
Another example of a scam, was during the Trump election. A Dark Web site was created, proclaiming that for enough money, they would assassinate President-elect Trump. Bitcoin was accepted for the fundraiser, but since the site was shut down, the exact amount of money collected is unknown. Naturally, nothing happened, but the admins took advantage of the wave of negativity toward President Trump during the elections.

Another scam was performed by Evolution Marketplace. Their admins scammed the users. They stole over 12 million dollars in Bitcoin and disappeared.

The following screenshot is from Evolution Marketplace:



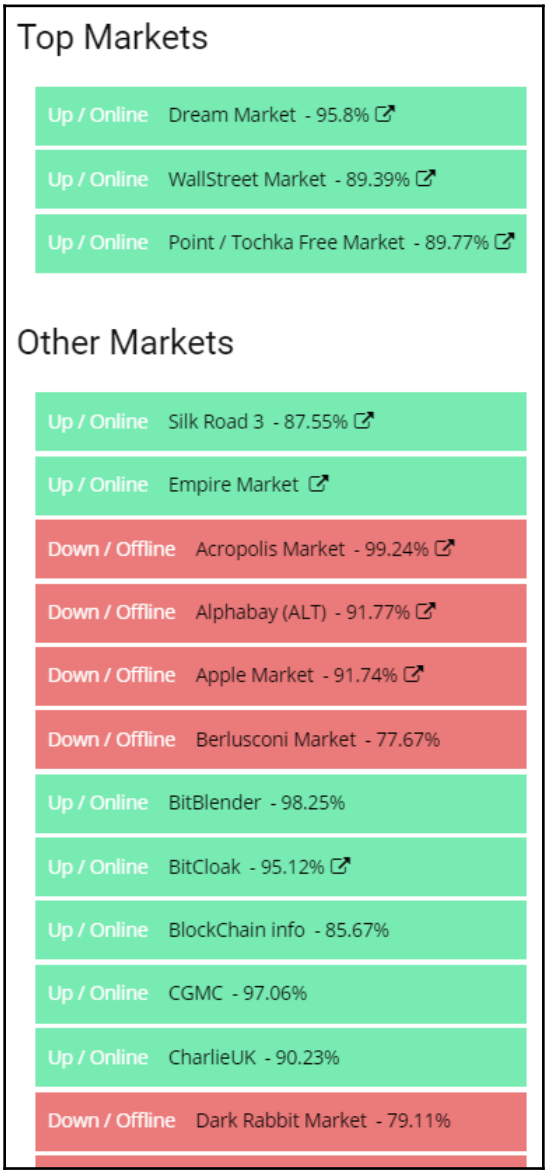
The DeepDotWeb website lists several market sites which are supposedly legitimate (even proper sites can have problematic links), as can be seen in the following screenshot:



The Dark Web News website compiled a list of trusted vendor markets, according to their reputation.

Although I've accessed several of them, taking the precautions we've discussed in this book, with no ill effect, but as with all Dark Web sites, access them at your own risk.

You can see part of the list here:



Also, they prepared a comparison between these sites, as shown in the following screenshot:

Market	Total Listing	Drug Listings	Market URL	User Guide	Reg	Multisig?	Commission	Vendor Bond	2FA	Forced Vendor PGP	Created	Screenshot
Berlusconi Market Down / Offline	6475	3812	http://berluscqui3nj4qz.onion/	/	Open	✗	2%	0-250$	✓	✗	07.7.2017	👁
CGMC Up / Online	949	453	http://cgmcoopwhempo6a5.onion/	/	Ref	✓	2-3%	0$	✓	✓	06.7.2016	👁
The Hub Down / Offline	Forum	Forum	http://thehub7xbw4dc5r2.onion/	Click	Open	/	/	/	/	/	/	👁
The Majestic Garden Down / Offline	/	/	http://talismanrestz7mr.onion/	Click	Ref	✗	Donnation Based	Ref (Invited Vendors)	✗	✗	01.4.2014	👁
DNM Avengers Up / Online	Forum	Forum	http://avengersdutyk3xf.onion/	Click	Open	✗	/	/	✗	✗	01.11.2015	👁
Dream Market Up / Online	62834	59108	http://6khhxwj7viwe5xjm.onion/	Click	Open	✗	4%	0.1 BTC 400$	✓	✗	11-15-2013	👁
WallStreet Market Up / Online	7048	3569	http://wallstyizjhkrvmj.onion	Click	Open	✓	2.5-5%	80$ Free For Trusted	✓	✓	10-19-2016	👁

I'm providing it as an example and to discuss what you should look for when looking for a legitimate Dark Web market. I'm not endorsing or confirming the list or the comparison. The reason is that I haven't tried all of the sites.

Avoiding the risks on a Dark Web market

So what should you look for to minimize the risk on a Dark Web market?

- **Multisig, escrow, finalize early**: These mean that the market is serious about protecting your money.
- **Anonymity and security**: How secure are you and your account on the market? Does the site use PGP, 2-factor authentication, phishing, and DDoS protection? You can do this by reading up on the site, and looking for this information there, before signing up.

- **Reviews**: Reviews on various other sites (both on the Surface Web and the Dark Web) will provide information about a market's reputation.
- **Help and support**: Does the market have a support team? Are they responsive? Are they willing to help with issues between sellers and buyers? Look for Help or Support links on the website. Read what level of support is offered there. Send them a message, to see how fast they respond.
- **Uptime status**: One of the most important metrics and validations that you can find is: how long has the site been up? Most index or search sites on the Dark Web will display the uptime of the sites listed on them.
  You can also try sites like: `https://dnstats.net/`
  or `https://www.deepdotweb.com`

Dangers of the Dark Web

One of the dangers of the Dark Web is having our information uploaded and displayed there. This has happened to Facebook, British Airways, the Marriott hotel chain, and many more. I will talk about one or two in this chapter.

For example, a top investment firm was discovered to save their client's information on unsecure servers. The information included **Personally Identifiable Information** (**PII**), such as their social security information and bank account numbers. This information was published on the Dark Web, putting the clients (and the investment firm) at risk

A Middle Eastern website was found to have inadvertently leaked administrative level credentials and credentials for remote terminals in several countries, to the Dark Web (it is not known how or who did it). This was caught in time, but the danger is there.

A major US healthcare organization, who was monitored by a Dark Web threat intelligence company, was found to have sensitive human resources and internal network information available on the Dark Web due to an issue with the required credentials for the system that holds the information. This was remediated and no recurrence was detected.

Access

Most people World Health Organization want to access the Deep internet use Tor, a service originally developed by the us armed service science lab. consider Tor as an online browser like Google Chrome or Firefox. the most distinction is that, rather than taking the foremost direct route between your laptop and also the deep elements of the net, the Tor browser uses a random path of encrypted servers, conjointly called **nodes**. This permits users to attach to the Deep internet without concern of their actions being half-tracked or their browser history being exposed. Sites on the Deep conjointly use Tor (or similar package like I2P) to stay anonymous, which means you will not be able to discover who's running them or wherever they are being hosted.

Many users currently leverage Tor to browse each the general public net and also the Deep. Some merely don't need government agencies or maybe net **Service suppliers** (**ISPs**) to understand what they are observing on-line, whereas others have very little choice—users in countries with strict access and use laws are usually prevented from accessing even public sites unless they use Tor shoppers and **virtual personal networks** (VPNs). the identical is true for presidency critics and different outspoken advocates World Health Organization worry backlash if their real identities were discovered. Of course, namelessness comes with a dark facet since criminals and malicious hackers conjointly choose to operate within the shadows.

Use and Misuse

For some users, the Deep internet offers the chance to bypass native restrictions and access TV or moving-picture show services which will not be on the market in their native areas. Others go far to transfer pirated music or grab movies that are not nevertheless in theaters. At the dark finish of the net, meanwhile, things will get chilling, salacious and simply plain...strange. As noted by The Guardian, for instance, mastercard information is obtainable on the Dark internet for simply some bucks per record, whereas ZDNet notes that something from pretend citizenship documents to passports and even the services of skilled hit men is obtainable if you recognize wherever to seem. Interested parties also can grab personal details and leverage them to blackmail standard net users. contemplate the recent Ashley Madison hack—vast amounts of account information, together with real names, addresses and phone numbers—ended au fait the Dark internet available. This proves that, whether or not you do not surf the murky waters of the Dark internet, you'll be in danger of blackmail (or worse) if sites you frequently use are hacked.

Illegal medicine are a well-liked draw on the Dark internet. As noted by Motherboard, drug marketplace the Silk Road—which has been finish off, replaced, finish off once more and so rebranded—offers any style of substance in any quantity to interested parties. Business corporate executive, meanwhile, details a number of the strange belongings you will hunt down within the Deep, together with a DIY ablation kit and a virtual scavenger hunts that culminated within the "hunter" responsive a NYC payphone at three a.m.

Real Risks

Thanks to the utilization of encoding and anonymization tools by each users and websites, there is just about no enforcement presence down within the Dark. this implies anything—even material well outside the bounds of fine style and customary decency—can be found on-line. This includes offensive, felonious "adult" content that will seemingly scar the viewer forever. A recent Wired article, for instance, reports that eighty % of Dark internet hits are connected to paedophilia and erotica. Here, the notion of the Dark as a haven for privacy wears skinny and shores up the notion that if you are doing like better to go far, continually limit access to your Tor-enabled device thus youngsters or different relations are not in danger of unsteady across one thing nobody ought to ever see. Visit the Deep internet if you are interested, however do yourself a favor: do not let children anyplace close to it and tread carefully—it's a protracted manner down.

Some general dangers

Many Dark Web markets allow the illegal sales and purchasing of drugs, weapons, and according to several sources, even human trafficking. Since the markets are anonymous, this increases the danger—who are you really buying from? Are they reliable? Will they steal our money?

Credit card numbers, bank account information, and other personal information can be purchased on the Dark Web for us in theft and fraud activities. This can lead to counterfeiting of your documentation. Just another reason to keep your personal information off the Dark Web.

Black hat hackers brag about their exploits, communicate and collaborate with other hackers, and share security exploits on the Dark Web, where they can stay anonymous.

But another side of hackers' presence on the Dark Web is that they practice their craft there, trying to lure innocent users into doing something that will provide a weakness or an attack vector, which will allow them to hack the users.

Always be careful of links you are about to click. Never download or click executables or anything that looks fishy.

Malware is something that is prolific on the Dark Web. In 2017, there were several malware detected there; for example:

- 2017 – Karmen Ransomware RaaS
- 2017 – MACSPY – Remote Access Trojan as a service on Dark web
- 2017 – MacRansom is the first Mac ransomware offered as a RaaS Service.
- 2017 –Ransomware-as-a-Service dubbed Shifr RaaS that allows creating ransomware compiling three form fields.

Botnets are another danger on the Dark Web, especially Tor-based botnets. They can show the following:

- Availability of authenticated hidden services
- Availability of private Tor networks
- Possibility of exit node flooding

Security researchers try to detect botnets and their Command and Control servers (C&Cs), by performing traffic analysis. This is done with **Intrusion Detection Systems** (**IDS**) and network analyzers. To remove a botnet, the following actions can be taken:

- Cleaning the C&C servers and infected hosts
- Revoking domain names
- Obscurating the IP addresses assigned to the C&C server

Since the botnet traffic is routed through the Tor network, it's encrypted, which makes it hard to analyze.

Tor-based botnets can masquerade as legitimate Tor traffic and encryption prevents most intrusion detection systems from detecting botnets. In addition, the C&C servers are hard to find. The operator can easily move around the C&C servers just by re-using the generated private key for the hidden service that the botnet uses.

Gamblers love the Dark Web, as it allows them to feed their addiction or allow them to play their games, without regard of local gambling laws, especially if the games are illegal.

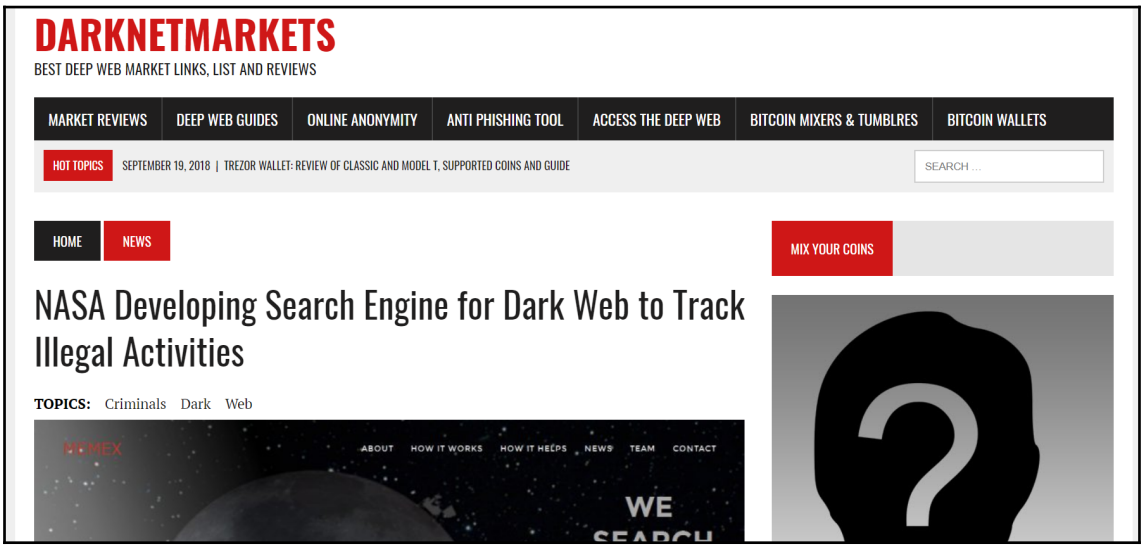
As I've discussed in other chapters, terrorists use the Dark Web for communication, recruiting, and organizing (themselves and their attacks). This is very difficult to detect, and monitor, which is the main reason that they use the Dark Web.

Another danger is being blamed of wrongdoing or illegal acts. As I've already mentioned, law enforcement agencies create Dark Web sites to draw in people and apprehend them, if they commit a crime.

The problem is that sometimes innocent people access illegal sites, or even use content that they didn't know was illegal, and then they are arrested, even though they didn't do anything wrong, at least not intentionally.

Also, ISPs and governments are devising ways to monitor the Dark Web for illegal activity. Since it's sometimes hard to differentiate between criminals and legitimate users, this is alarming.

NASA, for example, have been working on a search engine to track illegal activities, as you can see in the following screenshot:



There can always be a downside to every technology.

Sadly, anarchists, weapon dealers, perverts, drug dealers, and other horrible people are on the Dark Web. The danger here is more of a mental one. Being exposed to awful images or videos, or any other type of content, can harm people.

Summary

In this chapter, we discussed some of the dangers that exist on the Dark Web. We also discussed best practices and how to protect ourselves.

The main takeaway from this chapter, in my eyes, is that even though danger exists on the Dark Web, it exists elsewhere as well. And if you take the necessary precautions, and are careful, there's no reason why you can't enjoy the wealth of information and topics, which can be found on the Dark Web.

Use it responsibly, privately, and for good reasons, and you will be fulfilling the dream that the Dark Web is, for all people who want to communicate privately, and without fear of having their private information leaked.

Questions

1. Which of the following constitute Dark Web dangers?

    A. Malware

    B. Bombs

    C. Tor botnets

    D. Assassinations

2. Which government agency developed a search engine for illegal activity?

    A. NSA

    B. FBI

    C. CIA

    D. NASA

3. What metrics should you verify to make sure a Dark Web market is legitimate?

Further reading

The following resources might be interesting if you'd like to go deeper into the subjects covered in this chapter:

- `https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1298643?scroll=topneedAccess=true`
- `https://darkwebnews.com/malware/malware-spreading-by-stenography/`
- `https://resources.infosecinstitute.com/malware-dark-web/#`