Darkweb Demystified
Let’s travel to the scary place
• cybersecurity person trapped in public accounting
• a bit obsessive about technology
• prolific indoorsman
• absolute pro with PowerPoint
• bgogel@bswllc.com
• robots will take over my job one day
"Technology Stock Photos" Starterpack

This colour scheme. No exceptions

Weird Minority Report touch screens

Way more diversity than the actual tech industry

A guy with 10 different screens that all have nothing useful on them

So much blue

Locks = security

Did I mention the colour blue?
01

KEY CONCEPTS

What enables the dark web?

02

WINDOW SHOPPING

Danger zone! What’s for sale on the dark web?

03

SO WHAT?

Why do we care as auditors?
“I was reminded of what is perhaps the fundamental rule of technological progress: if something can be done, it probably will be done, and possibly already has been.”

—Edward Snowden
01 KEY CONCEPTS
What enables the darkweb?
SO MANY THINGS YOU COULD COVER

- How is it different from the Internet?
- What’s a bitcoin?
- How YOU can get on the dark web! (but don’t)
HISTORY OF THE DARKWEB

- **Sept 2002**: Tor browser released by US Naval Research Lab
- **Jan 2009**: Silk Road exposed
- **June 2011**: In decline but active
- **Today**:
**Internet**
Communicates over standard protocols using your normal internet browser.
*(aka surface web, clear web, clearnet)*

**Deepweb**
Sites on the internet that are not indexed by Google and other search engines. Estimated that it’s 500-5000x larger than the internet. Relies on obscurity to hide illegal activity.

**Darkweb**
Communicates over a private protocol (kind of like a VPN) with a special browser. Inaccessible from the internet without the right tools.
*(aka darknet)*

All three host and sell legal and illegal content.
WHAT DO YOU DO ON THE DARKWEB?

- **Marketplace**
  - Buy illegal things

- **Private Communities**
  - Talk about illegal things

The darkweb isn’t as big as you think it is.
I DON'T KNOW HOW BITCOIN WORKS

AND AT THIS POINT I'M TOO AFRAID TO ASK
CRYPTO ANONYMITY

• All transactions are on a public ledger, so anonymity is crucial for darkweb transactions

  - Buy crypto on an exchange without identify verification
  - “Tumble”, “mix”, or launder your crypto
  - Use a new digital address for each transaction (like having a single use credit card)
  - Use a prepaid debit card (cash → debit card → bitcoin)
  - Use a bitcoin ATM (cash → bitcoin)
  - Use a VPN for all purchasing on exchanges
Exchanges with verification requirements
Exchanges w/o verification requirements
Mixers/tumblers are services for mixing cryptocurrency funds from different sources with other funds, in order to obscure the trail back to the original source.

Darknet entities are entities that operate via the darknet and offer illegal services or goods in exchange for (mainly) cryptocurrency.

Other entity types are entities such as payment processors, gambling services, illegal services, miners, marketplaces, online wallets, ransom extortioners, scams, stolen coins, and/or others.
WHAT DO YOU BUY ON THE DARKWEB?

Drugs
No more small talk with your dealer

Weapons
Did you know it's hard to buy a gun outside of the USA?

Stolen Data
Credit cards, identify theft, hacked passwords

Adult Content
Big yikes here
DON’T GO ON THE DARKWEB

but here’s how if you really want to...
WHO GOES ON THE DARKWEB?

Researchers & Law Enforcement
Professionals that are monitoring for new hacks, stolen data, and cracking down on illegal merchandise

Criminals & Buyers
Organizations/individuals that are buying and selling goods and services on darkweb marketplaces

Activists
Secure and anonymous communications hide activity from governments

Plus: You might be surprised who’s got a darkweb marketplace!
TOOLS TO CONNECT TO DARKWEB

Tor Browser
Free web browser (like Google Chrome, Firefox) that enables a connection to “onion sites” (Works as a normal browser too)

Tails OS
Optional: An entire operating system (like Windows or Linux) that’s like a “burner” phone.
What does Tor have to do with the government and onions?

- Technology was developed by US Naval Research Lab for US intelligence officers to communicate securely.
- There are nested/layered levels of security within the Tor browser and secure communications, like an onion.
Skype update introduces call recording

by Martin Brinkmann on September 05, 2018 in Music and Video - 5 comments

Users of Microsoft’s Skype messaging application for desktop and mobile operating systems can now use a new call recording feature that Microsoft has built into the application recently. Call recording functionality has been a [...]
Darkweb sites end in .onion
02 WINDOW SHOPPING

Danger zone!
What’s for sale on the darkweb?
Dark.fail is one of many darkweb indexers

- Lists popular darkweb sites (forums and marketplaces mostly)
- Does not list any private site
- Lists 89 sites today

**What markets exist on the darknet?** Here’s a quick tour of today’s notable cryptomarkets, for fellow darknet researchers.

**NEW:** Verify signatures with darkfail.org’s new PGP Tool. Don’t get phished. Always PGP verify, onion and Bitcoin addresses before interacting with them.

Tor is the uncensored internet. Install Tor Browser to explore it. Set darkfail11lnk4vf.onion as your home page to save time. Links are PGP verified and unclickable for your safety. darkfail.org’s philosophy and finances

This resource is intended for researchers only. I do not vouch for any sites.

**Darknet Live**
- http://darkzzx4avcsuogfgez5zq75cgc4mprjvfgyw045dcoaxrwq6qrlf.id.onion

**Darknet Avengers Forum**
- http://avengersdutyk3xf.onion

**Dread**
- http://dreadit.evelidot.onion
- http://dreadytc.fatprotdj61o71kxptbeto2ouroyno2yv7jlcxbkxyazubrad.onion

**White House Market**
- http://auzb+dykqyhnxohw5zcywqwh2wqkjhh1hawp35fuh45wy3itslcnwid.onion
- http://usercontrol7z7hawpd35nm35tclog.nx1/10onion
- More...

**The Versus Project**
- http://pqpmr3bagmrhrdp23d20yjpyuo4dakn?amedbjik4uj7cwb2wftccad.onion

**Dark Market**
- Offline
Warning: In order to use this market, you need to add your PGP key. Users without a PGP key can only browse listings and may be deleted at some point.

Simple Search | Advanced Search

Search terms: Product or Vendor

Shipping from: any

Shipping to: any

Sort by: Random

Search

Featured Listings

- GG EGGSHELL XTAL - 100ug
  - spyfox
  - View Store
  - 100.00% / 0 - 10 sales

- "NATURAL" (Bufo Alvarius) Full sp
  - thetruthiswatin
  - View Store
  - 100.00% / 10 - 50 sales

- with Next Day Delivery - WORKS
  - stackz420
  - View Store
  - 97.40% / 90 - 100 sales

Top Vendors

- trippy
  - View Store
  - 99.40% / 580 - 580 sales

- southernandman
  - View Store
  - 97.60% / 60 - 70 sales

- cindicator
  - View Store
  - 94.00% / 40 - 50 sales

- euroshopper
  - View Store
  - 93.40% / 500 - 510 sales
<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Vendor</th>
<th>Verified</th>
<th>Trust</th>
<th>Member since</th>
<th># of Deals</th>
<th>Stealth</th>
<th>Quality</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truck EGR 5-KETAMINE 100-500G</td>
<td>60.00 EUR per GRAM</td>
<td>Spotify</td>
<td>Level 46</td>
<td>💫👩‍💼</td>
<td>2020-02-06</td>
<td>36</td>
<td>✅</td>
<td>🤗</td>
<td>🎉</td>
</tr>
<tr>
<td>Omnigen Anavar 10mg 100tablets CLONE</td>
<td>31.99 EUR per BOX</td>
<td>SocialPharma</td>
<td>Level 140</td>
<td>💫👩‍💼</td>
<td>2020-02-03</td>
<td>270</td>
<td>✅</td>
<td>🤗</td>
<td>🎉</td>
</tr>
<tr>
<td>100 gram mg/mq 84 % HQ</td>
<td>265.00 EUR per 100 gram</td>
<td>Coffeshop</td>
<td>Level 213</td>
<td>💫👨‍💼</td>
<td>2020-02-17</td>
<td>551</td>
<td>✅</td>
<td>🤗</td>
<td>🎉</td>
</tr>
<tr>
<td>2.5 Grams Amphetamine Pasté - Speed Pasté</td>
<td>16.00 EUR per unit</td>
<td>NightlifeKings</td>
<td>Level 69</td>
<td>💫👨‍💼</td>
<td>2020-01-29</td>
<td>83</td>
<td>✅</td>
<td>🤗</td>
<td>🎉</td>
</tr>
<tr>
<td>Encyclopedia of online Fraud</td>
<td>7.56 EUR per item</td>
<td>Goldenday</td>
<td>Level 34</td>
<td>💫👨‍💼</td>
<td>2020-03-07</td>
<td>56</td>
<td>✅</td>
<td>🤗</td>
<td>🎉</td>
</tr>
<tr>
<td>0.23 Million Portugal Emails Leads</td>
<td>8.41 EUR per File</td>
<td>GoldApple</td>
<td>Level 53</td>
<td>💫👨‍💼</td>
<td>2020-01-29</td>
<td>119</td>
<td>✅</td>
<td>🤗</td>
<td>🎉</td>
</tr>
</tbody>
</table>
I currently have approvals and passwords that allow me to manually enter CC at the registers of Guitar Center, Bypassing the usual 3 code verify( address, ph, ip).

I also have physical access to the server room and I am looking to exploit this with the help of some seriously skilled people. I have been with the company for years and know the ins and outs. I also know that these approvals have no way of coming back to me/

I am looking for a partnership where we can work together to get product and refunds, or Customer info and ccs.

If anyone is interested PM me or get me at [email]12stems@sigaint.org[/email] 

---

Anyone that has an insider in Vodafone or O2 and can provide Sim swaps please contact me ASAP. Ready to pay as well. Please message me!

can confirm william hill and ladbrokes cant verify have an insider in both so you should be okay not sure about the rest tho
Online Gift Card Shop Breached: 330k Payment Cards and $38m in Gift Cards Exposed

April 6, 2021
DisrupTor
ACTIVE ON DARK MARKETS? YOU HAVE OUR ATTENTION.

The Dutch police and judicial authorities collaborate with their foreign counterparts to combat IRL crime and cyber-enabled crime. Those who offer illicit goods or services have our attention. Are you one of them? How's your OpSec?

ARRESTED VENDORS
- DutchMasters
- BHShop (Domain Seized)
- BarryBusiness
- DShop
- DrugsTradeCentre
- DutchCartel
- DutchLucky
- Fatamorgana
- Foggyperson
- Guzman
- HectoraMom
- Imny2018
- JimmyWoo

ARRESTED VENDORS
- KeepDutch
- Krav
- MISSPINK
- Mirageexpress
- Mirageexpress
- Mr.Ted
- NEVERPRESSEDRX
- Nardhippies
- NoLove2323
- Nolove1818
- PillCosby
- RCQUEEN
- Pacho Herrera

ARRESTED VENDORS
- Stealthgod
- TheCommission
- TheCovenant
- TheFactoryTeam
- TheFlip
- TheGlassDoctor
- TheTrip
- TrippingBallz
- Xtcmen
- Yourfinest
- gemstoned.net
- largomoney

More info? General FAQ

Who are we? Verification

POLITIE OPENBAAR MINISTERIE
Koninklijke Marechaussee
The Northern California Illicit Digital Economy (NCIDE) Task Force

The Sacramento-based NCIDE task force (composed of Homeland Security Investigations, the United States Postal Inspection Service, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Internal Revenue Service Criminal Investigation) investigates violations of U.S. law involving cryptocurrencies and dark web marketplaces in the greater Northern California area and beyond.

ARRESTED VENDORS

- Farmacy41
- sicknessVersion2 a/k/a 23MightyMouse23
- HouseofDank a/k/a BestBuyMeds a/k/a TrapMart
- DankStox
- BudgetBudsExpress
- CokeWave
- SafeDealzDirect
- Cannabars a/k/a thefastplug
- PhantomLabs
- Diablo a/k/a raiseAppeals a/k/a RaisedByDiablo
- CellCereal a/k/a Playground a/k/a GammoCrimeFamily a/k/a DopeQueen
- DiFrosty
We are the Nation's first line of defense.

We accomplish what others cannot accomplish and go where others cannot go.

A career at CIA is unlike any other. We are looking for people from all backgrounds and walks of life to carry out the work of a Nation.

FIND YOUR CALLING
03

SO WHAT?

Why do we care as auditors?
LAW ENFORCEMENT
There are a lot of criminals and scammers on the darkweb, so law enforcement is very active here.

DIGITAL FORENSICS
If you were hacked (or one of your vendors was hacked) it might be published for sale on the darkweb.

FRAUD MONITORING
Fraud monitoring services are constantly looking for their customers’ information.
CRIMINALS MIGHT BE TARGETING YOU ON THE DARKWEB

**Does your company issue gift cards?**
Gift cards are a great way to launder money. Maybe criminals are buying yours?

**Do you accept e-commerce card payments?**
Criminals can sell a stolen credit if they know it still works. Are they using your checkout process to test them?

**Are your employees re-using compromised passwords?**
Criminals might get lucky and use those passwords to get into your email.
DO YOU KNOW IF YOUR COMPANY (OR VENDOR) HAS BEEN BREACHED?

Monitoring the darkweb for stolen credentials or data can be an indicated that you’ve been hacked.
DO YOU KNOW IF YOUR COMPANY (OR VENDOR) HAS BEEN BREACHED?

Monitoring the darkweb for stolen credentials or data can be an indicated that you've been hacked.
PROTECTING YOURSELF

- Use unique passwords and a password manager
- If you need to go on the darkweb, do your research and know how to protect yourself
- Assume everything on the darkweb is a scam
KEY TAKEAWAYS

- **Darkweb** facilitates illegal activity, but is not inherently illegal
- Confidentiality and anonymity is the driver for using the darkweb
- There are professionals that scrape the darkweb for stolen data