

What's Lurking on the Dark Web

Presented by:
Kevin Gulledge, CAMS
Senior Risk Management Consultant
Abrigo



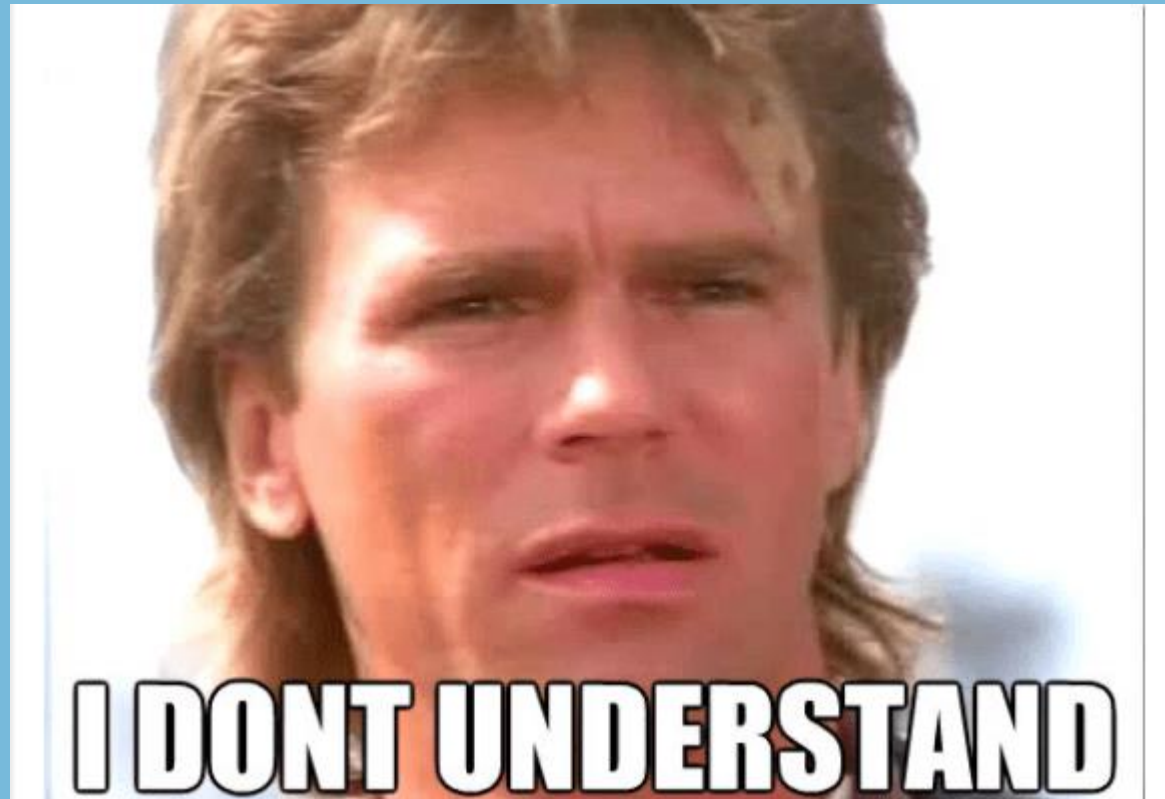
Agenda

- Introduction
- Key Terms
- Dark Web vs Deep Web
- Access
- Darknet Markets
- Cryptocurrencies
- Communication
- DEMO
- Q&A

Introduction

- So, what is it?
- According to Wikipedia: “The dark web is the World Wide Web content that exists on darknets, overlay networks that use the Internet but require specific software, configurations, or authorization to access. The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines.”

Introduction



Key Terms

SURFACE WEB

Any website that is indexed by a search engine (for example: ESPN.com or Amazon.com)

DEEP WEB

Websites that may be indexed, but also contain sensitive data that is protected from wider populations via login usernames and passwords (for example: online banking, Travelocity.com Search Results, your Gmail)

DARK WEB

Encrypted websites that are not indexed by search engines that require special browsers in order to view

Dark Web vs Deep Web

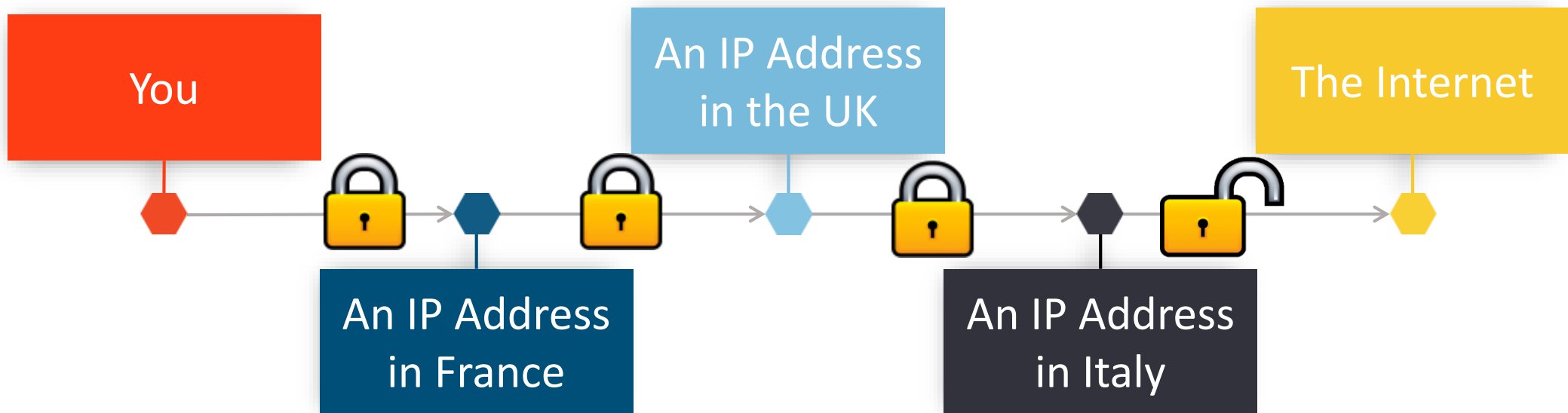


Access

- How do you access the dark web?
- You need a special internet browser
 - **Most popular is “Tor” (“The Onion Router”)**
 - **These browsers provide the user anonymity and the ability to decrypt the dark web**
 - **Bounces your IP Address all over the world**
 - **Dark web websites use the top-level domain of .onion**

Access

So how does the TOR Browser work?



Access

- Due to anonymity of the dark web, most of the websites are not common names, like <https://www.abrigo.com> or <https://www.ibanys.com>
- Usually a combination of numbers, letters and punctuation
 - For example: <http://tveoujogp67evxq7.onion>
- There are few “surface websites” that provide information and links to dark web websites, but are increasingly being shut down

Access

- Until recently, one of the primary “surface” websites that promoted darknet marketplaces and dark web news was <https://www.deepdotweb.com/>
- **The Justice Department shut this website down in May 2019 and arrested the website owners, charging them with money laundering**
- DeepDotWeb acted as a referral website for many darknet marketplaces, earning “referral fees” from markets like Alphabay, Hansa, Wall Street Market, Agora and more

Darknet Markets

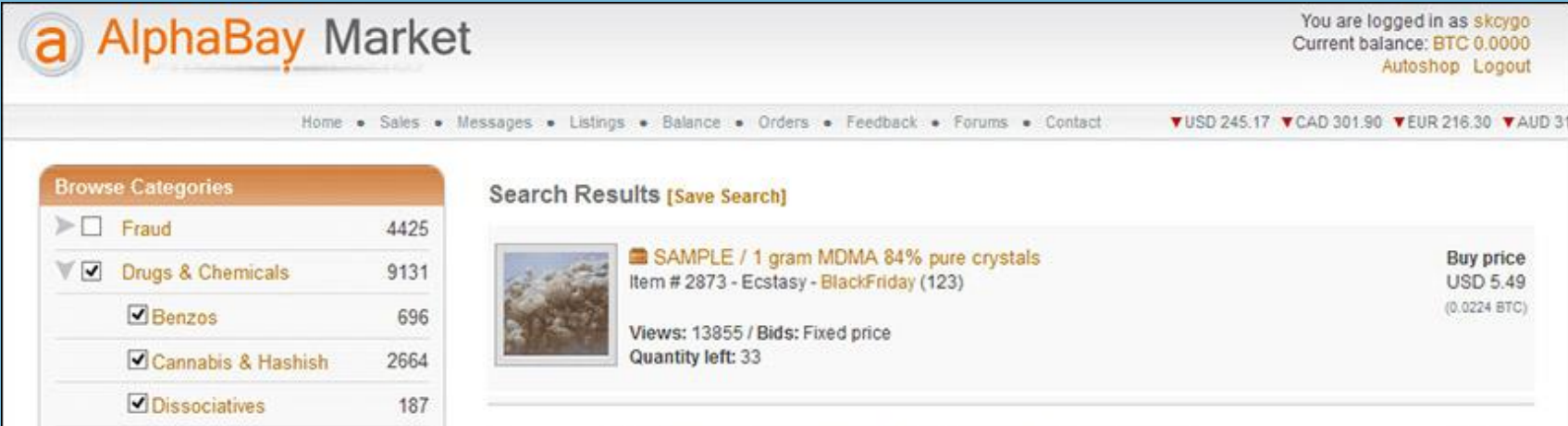
- The dark web hosts several “darknet markets”

The screenshot displays the Silk Road anonymous market interface. At the top, it shows the site name 'Silk Road anonymous market', user statistics (messages 0, orders 0, account B0,000), and a search bar. A navigation menu on the left lists various categories such as Drugs, Apparel, and Electronics. The main content area features a grid of product listings, each with a small image, a description, and a price in Bitcoin (B). The listings include items like '1g High Quality Cocaine', 'HYDROPONIC BUD', '5 liters OBL, 99.99% pure', '1g 3-FA / crystalline powder', '25x180Me (hot) 50mg', '10 Xanax 2mg bars -USA, stock-', '1.0 g Amphetamine Paste HQ German Lab', '25 LSD Blotter (United Kingdom)', '5G FLINSTONE MEFEDRONE, Yabba Dabba', '10 x 10mg Oxycodone - OC Formula Crush', 'MX 197 (Max Pro), 10ml, 197mg/ml', and 'Custom Listing 50g HQ Pure Cocaine'. A sidebar on the right contains a 'From the forum' section with several discussion topics.

Item	Price (B)
1g High Quality Cocaine	B0.6056
HYDROPONIC BUD 224g(1/2lb) BULK BUY	B17.1890
5 liters OBL, 99.99% pure	B9.9474
1g 3-FA / crystalline powder	B0.1663
25x180Me (hot) 50mg	B0.2794
10 Xanax 2mg bars -USA, stock-	B0.3425
1.0 g Amphetamine Paste HQ German Lab	B0.1067
25 LSD Blotter (United Kingdom)	B1.4835
5G FLINSTONE MEFEDRONE, Yabba Dabba	B0.7761
10 x 10mg Oxycodone - OC Formula Crush	B0.9522
MX 197 (Max Pro), 10ml, 197mg/ml	B0.8522
Custom Listing 50g HQ Pure Cocaine	B40.7000

Darknet Markets

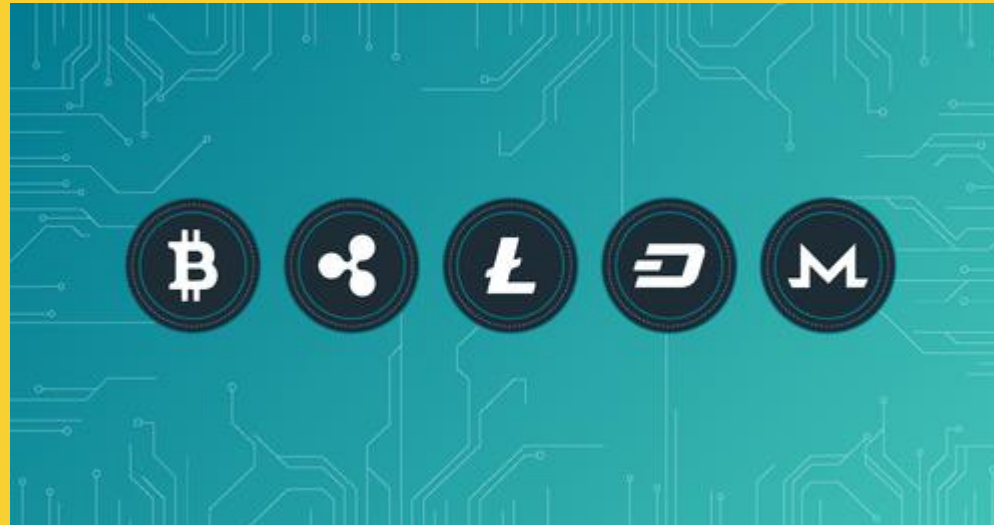
- Similar to Amazon or eBay, but usually involve illegal items for sale
 - Include, stolen or counterfeit identification cards, hacked data, drugs, “services”, credit/debit cards, pornography, weapons and more



The screenshot shows the AlphaBay Market website interface. At the top, the logo "AlphaBay Market" is visible on the left, and user information on the right: "You are logged in as skcygo", "Current balance: BTC 0.0000", and links for "Autoshop" and "Logout". A navigation bar below the logo contains links for Home, Sales, Messages, Listings, Balance, Orders, Feedback, Forums, and Contact. Currency exchange rates are shown on the right: USD 245.17, CAD 301.90, EUR 216.30, and AUD 31. On the left side, there is a "Browse Categories" section with a list of categories and their item counts: Fraud (4425), Drugs & Chemicals (9131), Benzos (696), Cannabis & Hashish (2664), and Dissociatives (187). The "Drugs & Chemicals" category is selected. The main content area displays "Search Results [Save Search]" for a specific item. The item is "SAMPLE / 1 gram MDMA 84% pure crystals", with item number 2873 and a "BlackFriday" tag (123). It includes a small image of the crystals, a "Buy price" of USD 5.49 (0.0224 BTC), and statistics: "Views: 13855 / Bids: Fixed price" and "Quantity left: 33".

Darknet Markets

- Purchases made with cryptocurrencies like Bitcoin help to make the entire enterprise completely anonymous



Cryptocurrencies

- FinCEN released guidance on May 9, 2019 on “**Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies**”
- **FIN-2019-G001**
- This guidance does not establish any new regulatory expectations or requirements. It consolidates current FinCEN regulations, and related administrative rulings and guidance issued since 2011, and then applies these rules and interpretations to other common business models involving Convertible Virtual Currency (CVC) engaging in the same underlying patterns of activity.

Cryptocurrencies

- FinCEN also released on May 9, 2019 an advisory: “**Advisory on Illicit Activity Involving Convertible Virtual Currency**”
- **FIN-2019-A003**
- “FinCEN is issuing this advisory to assist financial institutions in identifying and reporting suspicious activity concerning how criminals and other bad actors exploit convertible virtual currencies (CVCs) for money laundering, sanctions evasion, and other illicit financing purposes, particularly involving darknet marketplaces, peer-to-peer (P2P) exchangers, foreign-located Money Service Businesses (MSBs), and CVC kiosks.”

Communication

- The dark web also allows for encrypted communication
- This is helpful when “whistleblowing” on companies or governments
 - Edward Snowden
 - Wikileaks



Communication

- Also allows for journalists to communicate and keep their sources confidential
 - ProPublica, an online news website, has set up a dark web website
- <https://www.propublica.org/podcast/why-propublica-joined-the-dark-web>

Key Dates in Dark Web History

Mid-1990s

US Naval Researchers develop the core principles of "TOR" ("The Onion Router")

2002-2003

TOR is released to the public, along with I2P, another anonymous internet application

2006

The TOR Project becomes a Non-Profit Organization

2009

Bitcoin is created by Satoshi Nakamoto

2011

Ross Ulbricht creates the Darknet marketplace, Silk Road

2013

Ulbricht is arrested and Silk Road is shutdown (Ulbricht would be later convicted of money laundering, computer hacking and more and was sentenced to life in prison)

2017-2019

Many popular Darknet Marketplaces were shut down, including Hansa, AlphaBay, TradeRoute, Bloomsfield, Wall Street Market and more

Demo

- Before we begin the demonstration, 2 quick announcements:
- As previously mentioned, a lot of the material on the dark web is illegal and in demonstrating some of these websites, we may see adult or risqué images or text. I want everyone to be prepared as I cannot predict what will be visible on these websites.

Demo

- Abrigo periodically hosts free “Thought Leadership” webinars on our website (<https://www.abrigo.com>)
- A prior webinar was recorded:
- “The Dark Web – A Treasure Trove Of Actionable Threat Intelligence” by Eli Dominitz, CEO of Q6 Cyber.
- The recording is available at:
- <https://www.abrigo.com/webinars/webinar-the-darkweb-a-treasure-trove-of-actionable-threat-intelligence/>

DEMO

QUESTIONS?

Thank You!

