The Dark Web
and
Cybercriminals

Bill Olmo
March 2019
Updated May 2021

1

Sources

- AARP Bulletin September 2018
- Wikipedia
- Dark Web News (darkwebnews.com)

2

Uniform Resource Locator

Every device on the web has an address, URL. It consists of Protocol (http://) and Domain Name (www.reif.us). These URLs are translated into an Internet Protocol (IP) Address. There are two formats IPv4 (old) and IPv6 (new).

IPv4 had/has a format of nnn.nnn.nnn.nnn and was actually a 32 bit number inside the computer

IPv6 has a format of xxxx:xxxx etc.

3

IPv4

- Format of nnn.nnn.nnn.nnn
- Example 192.169.0.14
- Actually a 32 bit binary number inside the Internet
- 32 bits is **4,294,967,295**
- Limitation only 4.3 billion devices can be connected to the Internet
- Not thought of as a limitation in 1980

4

IPv6

- Format
  hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh
- Example
  2001:0db8:0000:0042:0000:8a2e:0370:7334
- A 64 bit number on the internet
- 64 bits is **18,446,744,073,709,551,616** (18 zetabits)
- Not thought of as a limitation in 2017

5

The Web

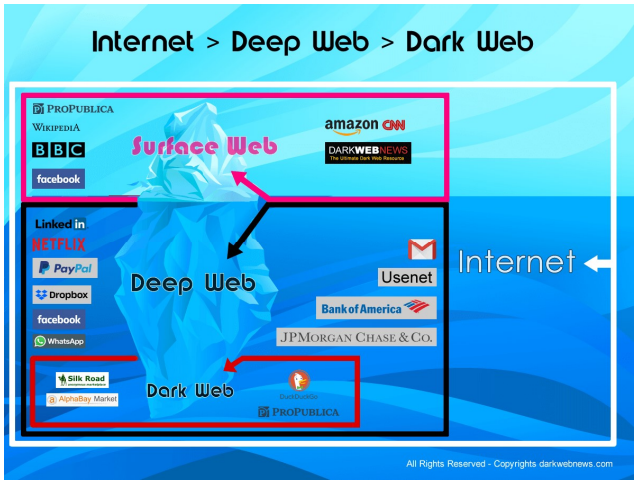
The web has three parts:

1. Surface Web 5-10%
   a) Google
   b) Facebook
   c) Amazon
2. Deep Web 90-95%
   a) PayPal
   b) Your Bank
3. Dark Web .01%
   a) Silk Road
   b) AlphaBay Market

AARP

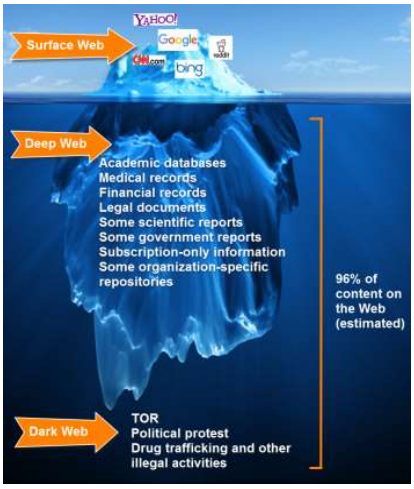
6

The Web



7

Another Look



8

Surface Web

- Public websites, thousands of them
- Google and Bing can find them all
- All are
  - Public
  - Searchable
  - Friendly
- Where you spend most of your time

9

Deep Web

- Google and Bing can get you to the front door
- Google and Bing can not see inside
- Pages are not indexed therefore not searchable therefore unreachable
- You need an ID and Password to enter

10

Dark Web

- Google and Bing can not find them
- Addresses are encrypted
- Sites are unregulated
- Everything is anonymous
- Requires a special browser (TOR)
- Many are legal
- Home of the Cybercriminals
- Transactions are carried out in Bitcoin

11

Examples

- Silk Road
  - Launched in February 2011
  - Best know for selling drugs
  - Shutdown by FBI in October 2013
- AlphaBay Market
  - Launched in September 2014
  - Over 200,000 users
  - Revenue $600,000 to $800,000 per day
  - Shut down by FBI in July 2017

12

Safe Sites

The Hidden Wiki **G**et to know the Dark Web.
Dream Market Market and browse the goods.
The Hidden Wallet A digital wallet and allows you to transact in Bitcoins.
Facebook **C**aters to those who want a social network that's anonymous
Impreza Hosting Secured and anonymous web hosting
Buy Bitcoins at Blockchain
Report Oppressive Policing Stay anonymous and submit sensitive info.
Torch Search engine
Tor Shops Tor Shops is the website builder for dark web.
ExpressVPN Premium VPN service
Rent-A-Hacker Prices start from around 250 Euros for small time hacking.
Apples 4 Bitcoin All phones come factory unlocked and can work anywhere
The Campfire Virtual gather-round-the-campfire-and-chat place.

Web Hosting Secrets Revealed 3/9/21

13

Dangerous Sites

The Cannibal Café The Cannibal Cafe is devoted to people who want to eat other people — as well as people who want to be eaten.

The Cruel Onion Wiki The Cruel Onion Wiki is a Wikipedia-like site that allows users to post them abusing animals online.

Besa Mafia Besa Mafia, allegedly allowed people to hire hitmen to take out any rival they wished — as long as they paid the price to do so*. (hoax?)*

Peter Scully's Red Room Red rooms are websites that allow you to witness someone being raped, tortured, or killed for a price.

The Human Experiment The Human Experiment is a website that allegedly involves real human experimentation — specifically, of the torture variety.

Cybersecurity 2018

14

The Onion Router (TOR)

- Developed by US Navy Research Lab in mid 1990's
- Objective was to protect US Intelligence online communications
- Everything is anonymous so all users look the same
- Released to the public in 2004
- The TOR Project, Inc
  - 501(c)(3) non profit
  - 80% funded by US Government

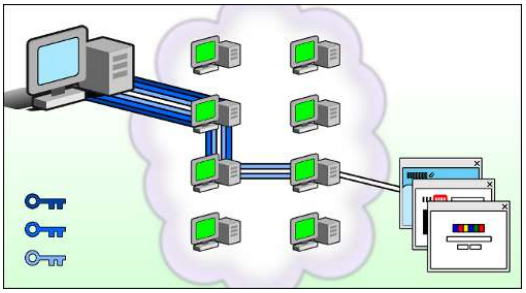
15

TOR Browser

- It prevents somebody watching your Internet connection from learning what sites you visit
- It prevents the sites you visit from learning your physical location
- It lets you access sites which are blocked
- Available as a free download
- Portable, can be run from a USB flash drive
- Windows, MacOS and Unix
- Available in 25 languages

16

TOR Network



17

Data Breach

- The intentional or unintentional release of secure or private/confidential information to an untrusted environment.
- Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill.
- Incidents range from concerted attacks by black hats associated with organized crime, political activist or national governments to careless disposal of used computer equipment or data storage media.
- Definition: "A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so."
- Data breaches may involve financial information such as credit card or bank details, personal health information, personally identifiable information, trade secrets of corporations or intellectual property.

18

Top 10 Data Breaches

Company/Organization	Number of Records Stolen	Date of Breach
Yahoo	3 billion	August 2013
Equifax	145.5 million	July 2017
eBay	145 million	May 2014
Heartland Payment Systems	134 million	March 2008
Target	110 million	December 2013
TJX Companies	94 million	December 2006
JP Morgan & Chase	83 million (76 million households and 7 million small businesses)	July 2014
Uber	57 million	November 2017
U.S. Office of Personnel Management (OPM)	22 million	Between 2012 and 2014
Timehop	21 million	July 2018

As of 3/2018

19

2020 Top Data Breaches

- Microsoft – 250 million records
- Wattpad – 268 million records
- Broadvoice – 350 million records
- Estée Lauder – 440 million records
- Sina Weibo – 538 million records
- Whisper – 900 million records
- BlueKai – billions of records
- Keepnet Labs – 5 billion records
- Advanced Info Service (AIS) – 8.3 billion records
- CAM4 – 10.88 billion records

Security 12/3/20

20

2021 First Four Months

January
Parler
Facebook, Instagram and LinkedIn
Mimecast
Pixlr
MeetMindful
Bonobos
VIPGames
U.S. Cellular

February
"Compilation of Many Breaches" (COMB)
Nebraska Medicine
California DMV
Kroger
T-Mobile

March
Microsoft Exchange
SITA
MultiCare
California State Controller's Office (SCO)
Hobby Lobby
Cancer Treatment Centers of America

April
Facebook
LinkedIn
ClubHouse
ParkMobile
GEICO
Reverb

Identity Force

21

Experian Data Breach Industry Forecast 2021

- We predict that intruders will plot to disrupt vaccine supply chains, sow confusion and spur increased national competition, creating a new kind of pandemic warfare.
- Mass transition to remote work provided hackers with a wealth of network targets through connected household devices. Attacks are getting smarter and more dangerous, and many families are unprepared for this onslaught in the coming year.
- Many contact tracing apps don't employ sufficient security protection, making these new tools a boon for hackers looking to steal shared data in 2021.
- Cybercriminals will certainly find ways to gain access to 5G networks to cause chaos with our cell phones, autonomous vehicles, health records and more.
- More breaches involving personal medical information may be on the horizon.

22

Recent Headline

First ten days of May 2021

- Contact Tracing Data Breach Exposes 72,000 Pennsylvanians' Personal Information
- Greek Teenagers Go On Spending Spree with Dark Web Counterfeit Money
- Illinois Attorney General computer system breached early Saturday morning
- Why cybercriminals looking to steal personal info are using text messages as bait
- A cyberattack has prompted major energy pipeline in the U.S. to shut down operations
- CyberNews researchers found more than 29,000 unprotected databases worldwide that are still publicly accessible, leaving close to 19,000 terabytes of data exposed
- Ransomware Hits Research Facility After Student Installs Pirated Software
- Thousands of Tor exit nodes attacked cryptocurrency users over the past year

23

May 12, 2021

- Nearly all Microsoft 365 customers have suffered email data breaches
- Up to $1K offered on dark web for patient medical records
- Ransomware group follows through on threat to release personnel files of DC police officers
- AWS configuration issues lead to exposure of 5 million records
- 200K Veterans' Medical Records May Have Been Stolen
- University of California data breach: Sensitive information of staff, students leaked
- Hackers Leverage Adobe Zero-Day Bug Impacting Acrobat Reader

24

pwned

A corruption of the word "Owned." This originated in an online game called Warcraft, where a map designer misspelled "owned." When the computer beat a player, it was supposed to say, so-and-so "has been owned."

Instead, it said, so-and-so "has been pwned."

It basically means "to own" or to be dominated by an opponent or situation, especially by some god-like or computer-like force.

25

How About You?

To find out if your identity has been stolen go to: https://haveibeenpwned.com/ and enter your email address.

The last time I looked I was hit eight times!

Firefox offers the same service at : https://monitor.firefox.com/

26

They Found Me

- **Your Privacy Is Vulnerable!**
- IP Address -- 73.93.100.90
- Location -- San Ramon, United States
- Browser -- Firefox on Windows
- Screen Resolution -- 1536x864

27

What Are You Worth?

- Online banking logins cost an average of $40
- Full credit card details including associated data costs: $14-$30
- Stolen online banking logins, min. $100 on account: $40
- U.S. driving license, high quality: $400
- Hacked Facebook account: $45
- Europe national ID card, high-quality: $500

PrivacyAffairs Mar 08, 2021

28

Dark Web Price Index 2021

PRIVACY Affairs

Category	Product	Avg. dark web Price (USD)
Credit Card Data	Cloned Mastercard with PIN	$25
	Cloned American Express with PIN	$35
	Cloned VISA with PIN	$25
	Credit card details, account balance up to $1,000	$150
	Credit card details, account balance up to $5,000	$240
	Stolen online banking logins, minimum $100 on account	$40
	Stolen online banking logins, minimum $2,000 on account	$120
	Walmart account with credit card attached	$14

29

Credential Stuffing

The technique works because people reuse the same password across multiple accounts. You're at risk if you use the same password for your TurboTax account and some other service that got hacked. It's the same approach hackers appeared to use to take over a Nest security camera owner's device in January 2019 and play a hoax message.

Dark Reading 2/25/19

30

Stop Cybercriminals

AARP Recommends

- Freeze your credit
- Monitor your accounts
- Use a password manager
- Use Two Factor Authentication (2FA)

31

Freeze Credit

- www.transunion.com/credit-freeze
- www.experian.com/freeze/center.html
- www.freeze.equifax.com
- www.innovis.com/personal/securityFreeze
- www.nctue.com/consumers

32

Best Free Password Managers

1. LastPass — #1 overall free password manager. Offers unlimited password storage on multiple devices (but you have to choose either desktop devices or mobile devices). LastPass is the only free password manager that offers password auditing, 2FA compatibility, password sharing, and a built-in authenticator.

2. Avira Password Manager — Unlimited storage on unlimited devices, plus an intuitive interface. Includes biometric logins, a built-in 2FA authenticator, and a well-functioning auto-saving and auto-filling capability.

3. RememBear — Very user-friendly program which provides unlimited password storage on one device. Provides cute bear cartoons, a helpful achievement system for accessing additional features, and biometric logins for free users.

4. Bitwarden — Unlimited password storage + multi-device sync, but challenging interface. One of the best free password management plans, but the issues with auto-filling and auto-saving passwords make Bitwarden best for technically experienced users.

5. Sticky Password — Saves unlimited passwords and works with lots of browsers. Provides USB portability and biometric login, but you have to upgrade for multi-device sync.

Safety Detectives 4/12/21

33

Two Factor Authentication

- 2FA requires an additional login credential – beyond just the username and password – to gain account access, and getting that second credential requires access to something that belongs to you.
- Typically this is a six digit number sent to your smartphone.

34

Good Advise from CITI

If Citi's Fraud team contacts you we will not ask you to provide any of the following information:

- Your account number
- Existing security word (i.e. mother's maiden name)
- PIN number
- Online User ID or online password
- One-time passcode --If you receive a one-time passcode you did not initiate, please do not provide the code to anyone who contacts you requesting it.

If you receive a suspicious communication, do not respond and do not use any contact information provided.

35

Closing Thought

Never click on a link sent to you in an email

Stay Safe

Thanks for listening

36