

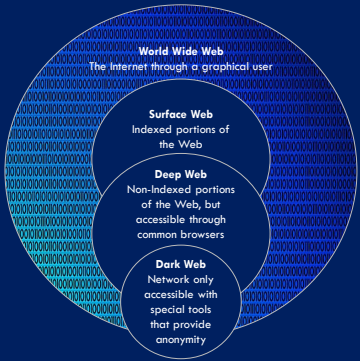


DARK WEB AND RANSOMWARE | Introduction

WHAT IS THE DARK WEB?

- Anything that is not accessible by standard browsers like Google Chrome or Firefox.
- Anyone who wants or needs to communicate anonymously, or who wants to mask their identity for any reason, can do so via the Tor Network.







World Wide Web
The Internet through a graphical user interface

Surface Web
Indexed portions of the Web

Deep Web
Non-Indexed portions of the Web, but accessible through common browsers

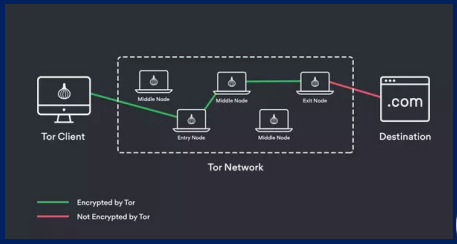
Dark Web
Network only accessible with special tools that provide anonymity



DIFFERENT LEVELS OF THE INTERNET



HOW THE DARK WEB WORKS



HOW THE DARK WEB WORKS



WHO MIGHT USE THE DARK WEB?

As of 2022, approximately 2 million people use the dark web daily.

Nefarious Users

- Dealers
- Hacktivists
- Bombers
- Identity Thieves
- Internet Stalkers
- Scammers

Authentic Users

- Law Enforcement
- Journalists
- Businesses
- Financial Institutions
- Retail Security



DARK WEB TOPICS

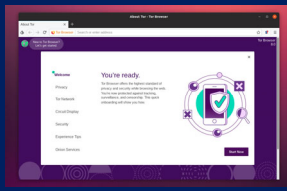
- Hacking Software
- Hacking Code
- Illegal Pornography
- Drugs
- Weapons
- Stolen user accounts and passwords
- Murder Contracts
- Terrorism



HOW THE DARK WEB IS ACCESSED?

TOR

- The Onion Router
- Most popular
- 3rd generation onion routing
 - 3 layers encryption
- [https://check.torproject\[.\]org](https://check.torproject[.]org)



WHAT IS RANSOMWARE?

• Type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access



WHAT IS RANSOMWARE?



WHAT IS RANSOMWARE?



ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
For more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquires access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password for RDP, VPN, corporate email, etc.
Open our letter of your email. Launch the provided virus on any computer in your company.
Companies pay us the thousands for the description of files and prevention of data leak.
You can communicate with us through the Tor messenger.
<http://bit.ly/2G8888888>
Using Tor messenger, we will never know your real name, it means your privacy is guaranteed.
3085888AAC1520F8124D645688F5030A0C89705EAD70590A24F90302A0E1D700C3C4AE987
If you contact us, we will never respond you, look for the relevant contact data on our website via Tor or Brave Browser
<http://lockbit2.com>



PAYING RANSOMWARE

- Ransomware operators commonly specify ransom payments in bitcoin
- Recent ransomware variants have also listed alternative payment options such as iTunes and Amazon gift cards
- ***Paying the ransom does not guarantee that users will get the decryption key or unlock tool required to regain access to the infected system or files that are being held hostage***



QUESTIONS?

Nicole McCombs
Ohio Homeland Security
(614) 387-6171
Email: saicyber@dps.ohio.gov
Website: HomelandSecurity.ohio.gov