

# What makes the Dark Web "Dark"?



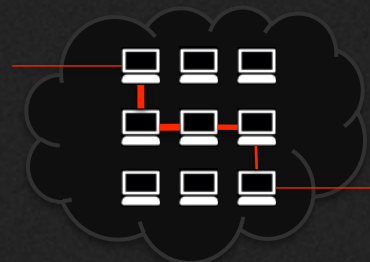
Part of the Internet has been indexed so that content is accessible by members of the general public using web search engines. The Surface Web (or ClearNet) contains at least 4.5 Billion pages.

Part of the Internet contains content that is not indexed so search engines cannot see or retrieve it, such as web mail or databases. The Deep Web could be >500 times bigger than the Surface Web.

Parts of the Deep Web are only accessible using specific software or configuration such as F2F, P2P, I2P, Freenet and the Tor Network. The Dark Web (consisting of DarkNets) is used for anonymity.

The most popular of the darknets is the Tor Network. Tor software encrypts content in multiple layers, like the layers of an onion, which is where the name comes from - "The Onion Router network".

Traffic is directed through a network of more than 7,000 relays managed by volunteers and a layer is decrypted at each relay revealing only the IP address of the next relay so at no point in the virtual circuit is the source and destination information available. This makes both the sender and the receiver anonymous. This anonymity provides a safe way for victims, civil rights activists, government and military professionals to communicate in an uncensored way. Unfortunately, this same anonymity provides a safe haven for criminals, malicious activists and deviants to communicate and collaborate - Dark content, Dark Users and for some, Dark intentions!

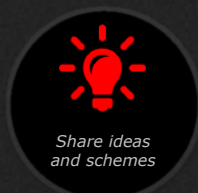


# What's on the Dark Web that relates to you and/or your business?

A wide range of illegal activity is conducted on the Dark Web including activities that could directly impact you and/or your organisation, such as:-

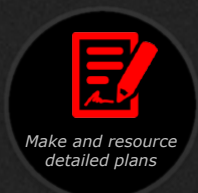
- Personal Information – credit card numbers, medical records and damaging revelations
- Corporate Information – copyright infringement, unauthorized news leaks, patents & IP
- Theft – money transactions, confidential data, customer & client data, digital products
- Activists – protestors, human or animal rights, malicious or disgruntled staff, competitors
- Terrorism – threats to senior management or staff, action against company operations

The Dark Web provides a perfect platform for collaboration by individuals or groups from anywhere in the world to plan, resource, execute and profit from malicious activity against you and/or your business.



Share ideas and schemes

Egging On  
Radicalization  
Collaborators



Make and resource detailed plans

Chat Rooms  
Anonymous Groups  
Suppliers



Launch anonymous attacks

Direct Hacks  
Ransomware  
Slur Campaign



Market stolen data or goods

Market Places  
Direct Sales  
Stolen to Order

# How can you protect yourself against something you can't see?

# What feels most at home crawling around on a Web – a Spider!

A "Spider" is a software programme that crawls from one website to another reading their pages and other information.

Major Search Engines all have Spiders, with names like Crawlers, Bots and Scooters and they follow the rules of politeness laid down in the Standard for Robot Exclusion (SRE) asking which files should be excluded and waiting between requests to allow user traffic to take priority.

Their primary role is to index web pages



The Pervade **OpIndex™** Spider is a very different beast!

It is custom-built for the Dark Web where the normal rules of engagement do not apply and it is engineered to circumvent anonymisation measures and circumnavigate routing relays.

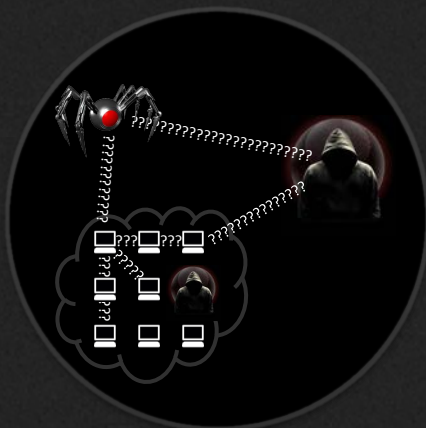
The unique architecture enables parallel tasking including Index and/or Search with Reporting and/or Alerting as well as offensive capabilities to Disrupt and/or Destroy threat actors who operate in the Dark Web.

**OpIndex™** from Pervade Software has been specifically designed to hunt down and identify sites and information that would otherwise be anonymised in the Dark Web. Dark Nets are continuously growing and the most commonly used – the Tor Network – has already reached a formidable size:-

- ✓ More than 1.8 million directly connecting users
- ✓ Over 50,000 unique ".onion" addresses
- ✓ Around 30,000 hidden services (*services are not sites, they includes chat servers and other services*)

The size of a network will not protect those who skulk in its dark corners however because hundreds of Pervade Spiders can be released into an environment through multiple bridges to very quickly 'pervade' every node and service...

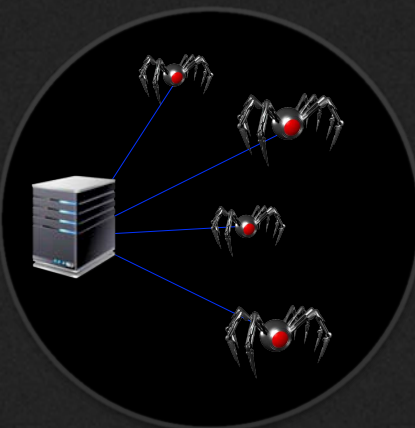
Index Search



Full Spectrum Scanning

- ✓ Index FULL Content
- ✓ Search for Key Words
- ✓ Seek Vulnerabilities

Report Alert



Gathering Evidence

- ✓ Forensic Logging of Activity
- ✓ Proof of Location/Identity
- ✓ Sit-Reps & Auto-Reporting

Deter Disrupt



Auto-Reporting

- ✓ Full details of Activities
- ✓ Specification of Infrastructure
- ✓ Report in Appropriate Format

## Would like to know if any threats are lurking in the Dark Web:-

Plots against your organisation

Threats against your people

Attacks against your sites

Hacks against your IT infrastructure

Confidential information being released

Data or IP being sold

Reputation being attacked

Contact Pervade Software and ask for a demonstration of the **OpIndex™** Spider in action.