DARKOWL

The Growth of the Darknet

The Darknet is Fundamentally Changing the Landscape on Who, Where and How Cyber Crimes are Perpetrated.

THE DARKNET ISN'T JUST ACCESSED BY A SMALL NUMBER OF PEOPLE

Darknet use in the United States has jumped **80% in the last 3 years.**

2 million active users connect to the darknet through the Tor browser every day.

32% of EU, 25% of North American, 5.6% of Latin American, and 10% across Russia and Ukraine users access the darknet daily.

THE ECONOMY ON THE DARKNET IS BOOMING

As of 2021, an estimated **4% of the US GDP** is laundered on the darknet annually.

In 2021, 67% of the offers on the darknet for access to corporate networks costs **$5,000 USD or less.**

Ransomware cost organizations around the world **$20 billion USD in 2021.**

DARKNET ACTIVITY SKYROCKETED DURING THE PANDEMIC

Fraudsters stole **$80 Billion** from the COVID Paycheck Protection Program; 10% of the total funds distributed.

Almost 44% of the US Pandemic Unemployment Assistance Funds were **stolen by darknet criminals.**

Nearly half a million COVID-related domains have been created since 2020. Most in use for phishing or scams by criminals.

In the last two years, COVID and Unemployment Exploitation Methods ("Sauce") sold on Telegram for **as little as $25 USD.**

YOUR DATA MAY ALREADY BE ON THE DARKNET, EVEN IF YOU HAVEN'T HAD A BREACH

In 2021, the cost to hire someone to **hack any Facebook account was $170 USD.**

The information for **700 Million Linkedin users or 92% of all accounts** have been scraped and leaked on the darknet in the last year.

In 2021, **37% of all businesses and organizations were hit with ransomware** and sensitive information leaked on the darknet.

In 2021, the average extortion ransom demand reached **$220,298 USD; an increase of 43% from 2020.**

From small businesses to nation states, this change in landscape is redefining cyber risk for everyone.

THOSE WHO ADAPT WILL SUCCEED.

THOSE WHO DO NOT WILL BE TARGETED.

Executives are targeted more than ever, but employees are not immune from threats.

>133,000

C-Level Fortune 1000 executives have had their credentials leaked on the darknet.

543M

Breached credentials associated with Fortune 1000 employees in circulation in the darknet in 2021.

>500,000

Zoom account credential data available for sale on the darknet.

Threats are evolving to become more effective and pervasive.

3X

The demand for malware on the darknet outpaces supply by up to three times.

>40

New unique ransomware Tor URLs leaking victim data identified by DarkOwl in 2021.

>50,000

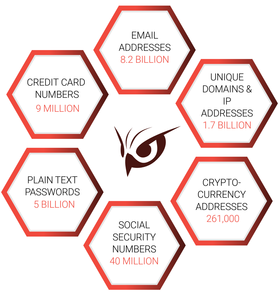
There are over 50,000 extremist groups that have a presence on the darknet.

In this new landscape, companies are also able to prevent known attacks, as opposed to doing forensics after they happen.

SUCCESS WILL BE ACHIEVED THROUGH THE IDENTIFICATION AND QUANTIFICATION OF RISK ON THE DARKNET.

Vision App > Search API > Entity API > Score API > Datafeeds >

NEW TOOLS HAVE EMERGED SPECIFICALLY DESIGNED TO FIND, MONITOR, AND MITIGATE RISKS EMERGING FROM THE DARKNET.



DARKOWL HAS THE LARGEST COMMERCIALLY-AVAILABLE DARKNET DATA SET IN THE WORLD

CONTACT US TO FIND OUT HOW DARKNET DATA APPLIES TO YOUR USE CASE

www.darkowl.com

DARKOWL

Sources: DarkOwl Vision, CSCDBS, Tor Project, ChainAnalysis, Cowware, NBC, Atlas VPN, TrustNet, Polymer, SpyCloud