State of the DARK WEB

4 Key Takeaways + 2 Things to Do Right Now to Protect Your Data



ID AGENT
A Kaseya COMPANY

Fast Facts

COVID-19 has affected every corner of the world - including the Dark Web. As we've monitored and analyzed the Dark Web in 2020, we've discovered trends that point to today's biggest cybersecurity threats and gained insight into the risks of tomorrow.

There are more than **4.5 billion** web pages on the "standard" internet.

The "full" internet, including the Dark Web, is estimated to be **400 to 500 times larger.**

A 2019 analysis of 2,723 Dark Web sites found that **57%** of them included **illicit material.**

The Dark Web offers approximately **75,000 terabytes** of data.

Takeaway #1

The Dark Web isn't just accessed by a small number of people.

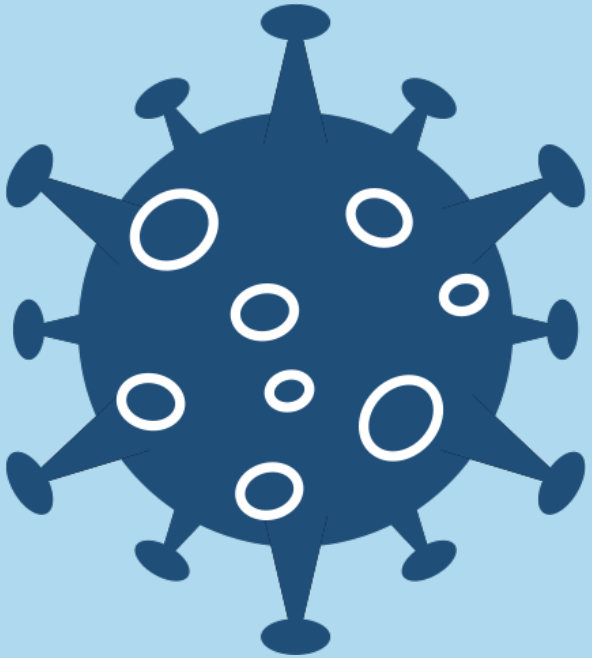
- 2 million active users connect to the Dark Web through the TOR browser every day.
- 26% of North American and 17% of EU users access the Dark Web daily.
- Approximately one third of North Americans used the Dark Web in 2019.
- About 60% of the information on the Dark Web could potentially harm organizations.



Takeaway #2

Dark Web activity is skyrocketing post-pandemic.

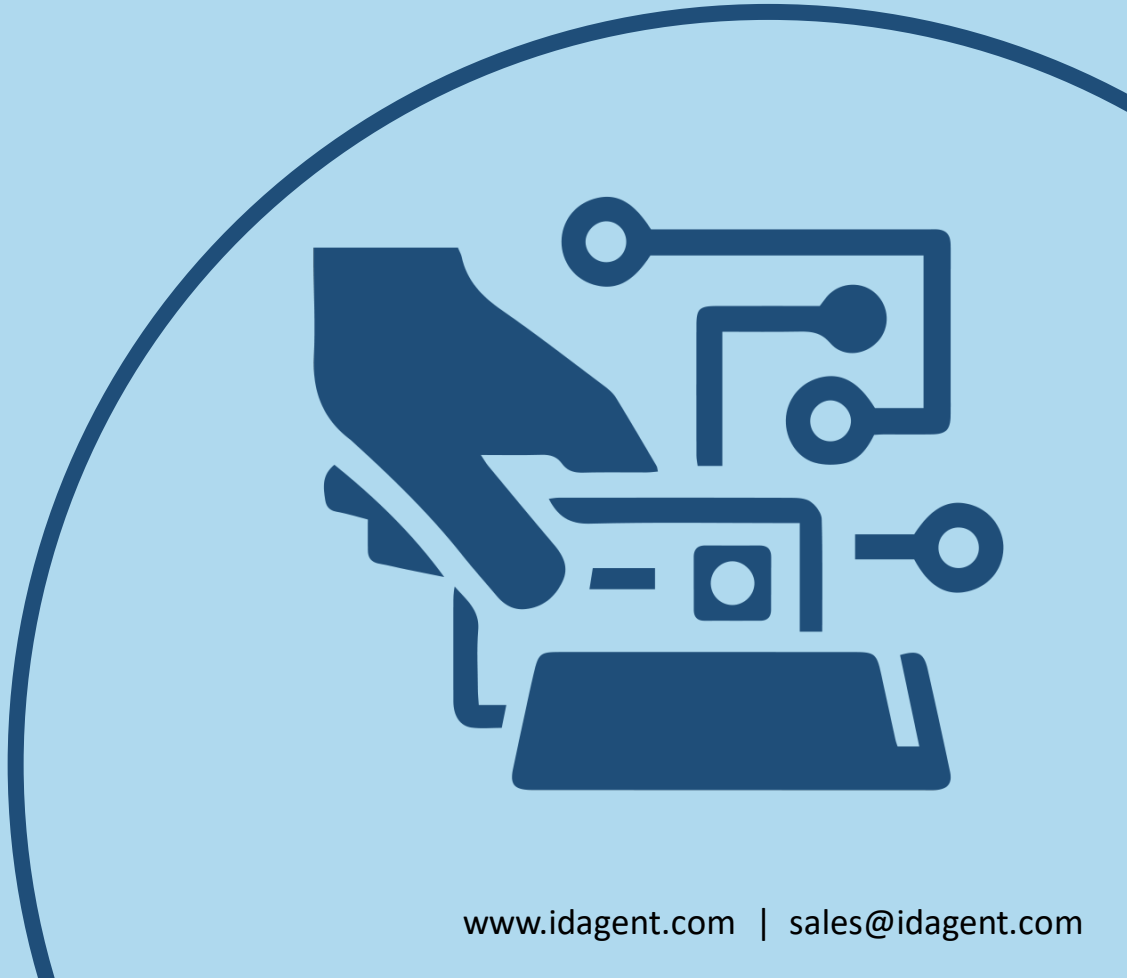
- Over 1,400 COVID-19 related domains were registered in Q1 2020.
- There was a 738% increase in COVID-19-related terms on the Dark Web in March 2020.
- Phishing attacks including COVID-19 scams have climbed 667% in 2020.
- Dark Web use has increased by more than 300% in the last 3 years.



Takeaway #3

The Dark Web economy is booming.

- An estimated 2 to 5% of the global GDP is laundered on the Dark Web in one year.
- More than 75% of Dark Web sites appear to be marketplaces.
- The price for access to corporate networks increased by 61% in Q1 2020.
- Cybercrime yields in excess of $1.5 trillion in revenue per year.



Takeaway #4

Your data may already be on the Dark Web, even if you haven't had a breach.

- Information on 267 million Facebook users sold in Q1 2020 for $540.
- In Q1 2020 alone over 73.2 million new user records hit the Dark Web.
- 164 million user records from a dozen major companies were exposed in a single Q1 2020 dump.
- 53% of organizations have had a data breach caused by third party information theft.



IDAGENT A Kaseya COMPANY

2 Actions That You Can Take Today to Protect Your Data

1. Get Someone to Watch Your Back.

Are your passwords for sale on the Dark Web? Is one of your staffers selling access to your systems? Were you exposed in a third-party Dark Web data dump? Find out with Dark Web ID. We'll dive deep into the corners of the Dark Web to look for potential risks to your organization. Dark Web ID also watches for new Dark Web threats to your systems and data 24/7/365 to alert you to potential trouble quickly, enabling you to stop cyberattacks before they start.

2. Get Ready to Defend Against Your Biggest Threat.

Over 90% of data breaches start with a phishing attack, and everything a cybercriminal needs to mount an effective phishing attack against you is available on the Dark Web. Prevent those attacks from landing with BullPhish ID. With 80 phishing kits and 50 video campaigns (including COVID-19 threats), plus 4-6 new training tools added per month in 8 languages, BullPhish ID ensures that your staff is ready to be your first line of defense against this Dark Web threat.