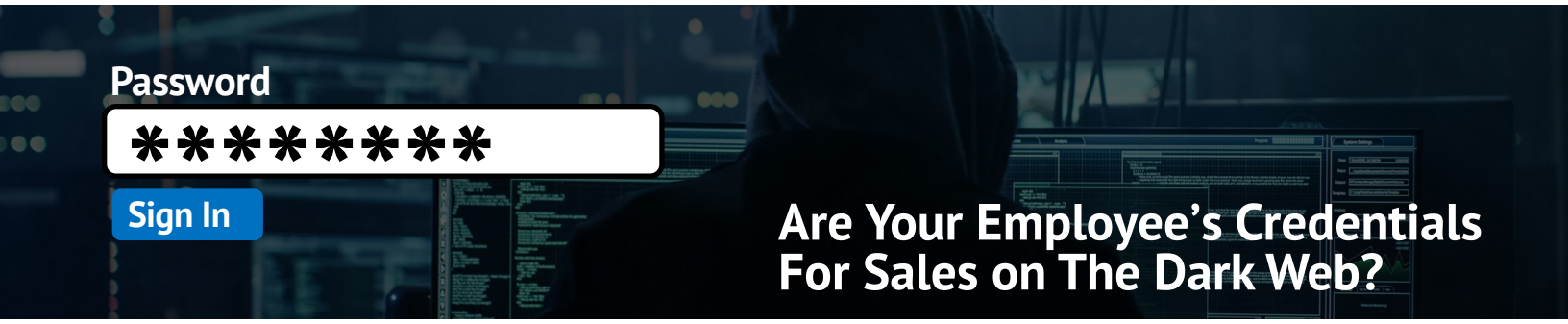
SECNAP NETWORK SECURITY

Dark Web Monitoring

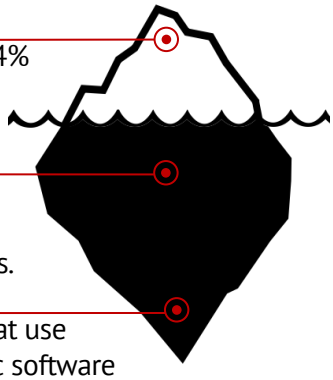


Are Your Employee's Credentials For Sales on The Dark Web?

We live in a digital age where highly sensitive data is stored in systems that most likely have vulnerabilities. In just 2018 alone, major companies such as Marriott Hotels, Facebook and Bitly have had breaches that have exposed millions of digital credentials and personally identifiable information (PII).

What is the Dark Web?

The Dark Web is made up of digital communities that are only accessible via special software, allowing users and website operators to remain anonymous or untraceable. While there are legitimate purposes to the Dark Web, it is estimated that over 50% of all sites on the Dark Web are used for criminal activities, including the disclosure and sale of digital credentials. Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed by law enforcement.



Surface Web makes up less than 4% of content on the internet and is indexed by search engines.

Deep Web makes up 90% of the information on the internet. Sites are not accessible by web crawlers.

Dark Web consist of websites that use public internet but require specific software to access to ensure anonymity.

Why are Stolen Credentials such a Risk?

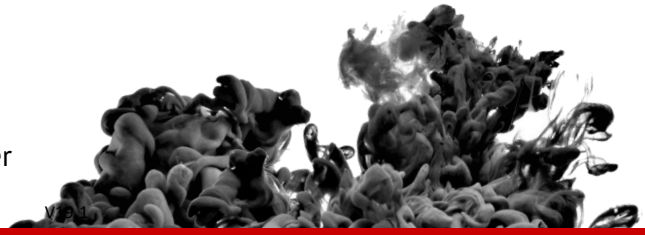
When your employees use their work email on third party websites, like the types listed below, it makes your business more vulnerable to a breach. According to a LastPass Study, 47% say there is no difference in passwords created for work and personal accounts. With our Dark Web Monitoring, we can alert you if your company's credentials or PII have been detected on the Dark Web. What if a cybercriminal was able to access one of these services leveraging stolen credentials?

- Human Resource
- Email Services
- Travel Sites
- Payroll Services
- Banking Account
- Company's Social Media
- Marketing Tools
- Customer Relationship Management
- Document Repository

What is PII?

Personal Identifiable Information (PII) is data about an individual that can be used to identify and therefore steal a person's identity. PII typically combines a person's first and last name with various pieces of personal information. Here are some of the most common examples:

- Social Security Number
- Driver's License number
- Passport Number
- Credit Card Numbers
- Medical Records
- Bank Account Number



SECNAP NETWORK SECURITY

Dark Web Monitoring

What You Can Do To Protect Your Business?

Our Dark Web Monitoring service leverages Dark Web intelligence with search capabilities to be able to identify, analyze and proactively monitor for your organization's compromised PII and employee credentials. Being aware of exposed stolen data can allow you to take steps such as resetting passwords to avoid further compromise.

WE GO INTO THE DARK WEB TO KEEP YOU OUT OF IT.

Cybercriminals exchange data in...

- Social media platforms
- Black market sites
- 640,000+ botnets
- Hidden chat rooms
- Peer-to-peer networks
- Internet Relay Chat channels

Technology

Our proactive technology connects to multiple high-risk Dark Web services including Tor, I2P and Freenet, to search for compromised credentials. From these technologies, we are able to provide intelligent insight of compromised credentials and PII.

Monitoring

Our 24/7 Security Operations Center will alert you based on information scoured from the Dark Web. They will alert you daily if there are findings. Monthly summary reports can be reviewed to confirm that users have taken the appropriate steps.

Top 3 Reasons Why Monitoring for Stolen Credentials is Important

- **Reused Passwords Increase Risk.** Employees often use the same password for multiple services which exponentially increase the potential damage from a single compromised credential.
- **Compromised Credentials are a Warning.** The sooner you know about exposed data on the Dark Web, the less damage you will endure. Once the information is out there, you want to take the appropriate steps to remediate and close any gaps that could be open for cybercriminals to exploit.
- **Risky Business on Your Accounts.** Your credentials can lead a hacker to your financial assets, contacts, sensitive data and permissions which can be leveraged to conduct further criminal activity.

Over 80% of data breaches leverage stolen passwords as the principal attack vector.*

*2017 Verizon Data Breach Report

Get Started With a Complimentary Dark Web Scan of Your Domain.

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM/DARKWEB