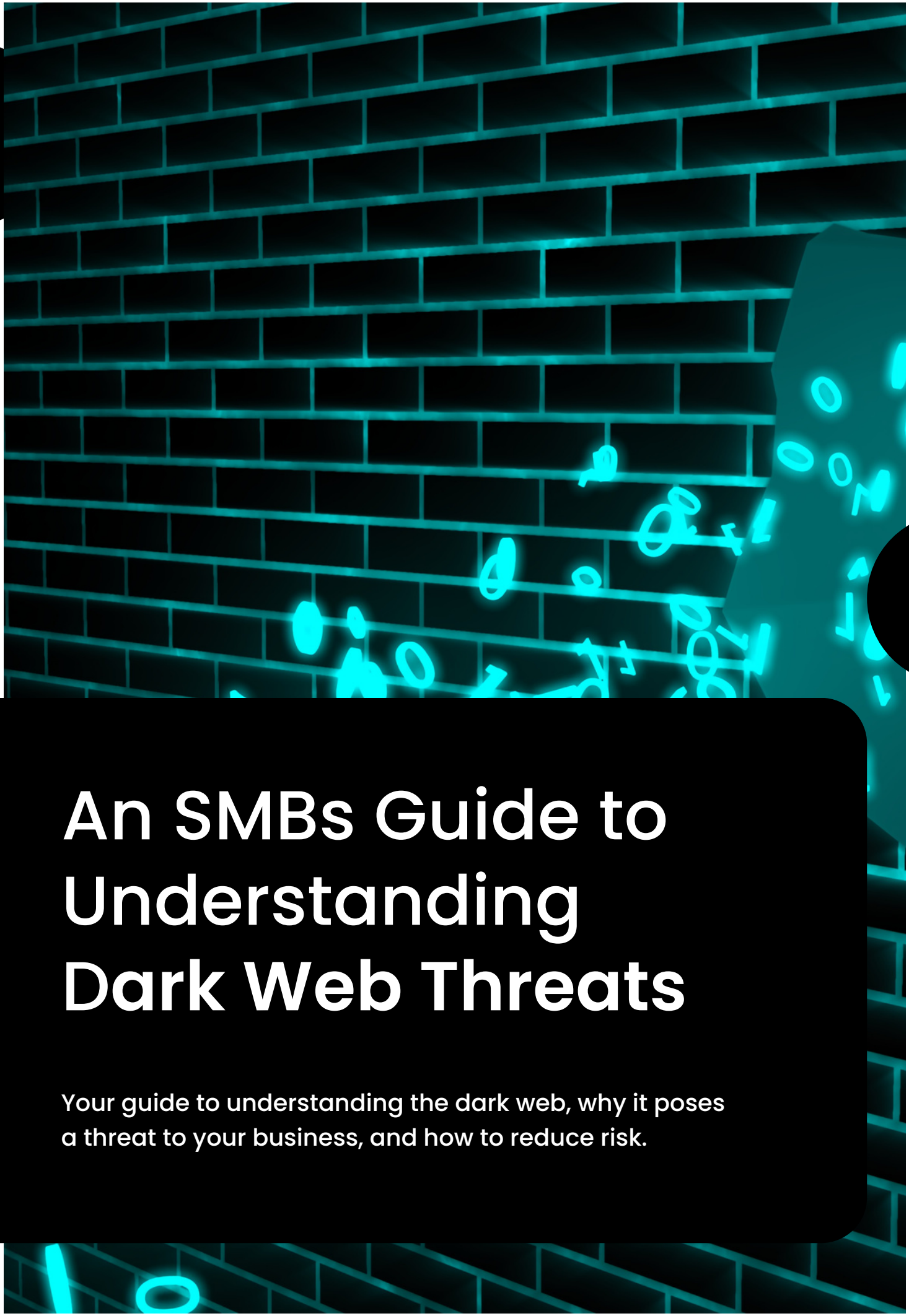


An SMBs Guide to Understanding Dark Web Threats

Your guide to understanding the dark web, why it poses a threat to your business, and how to reduce risk.

Contents

Introduction: Navigating the dark web 03

What is the dark web? 04

How cybercriminals leverage the dark web for crime 05

Types of business data that can be exposed 06

Why is exposed data a threat for businesses? 07

Examples of real-world data breaches 08

How to safeguard your business against the dark web 09

Dark Web Monitoring: An essential layer of security 10

Get in touch with us for a free breach report 11





Introduction

Navigating the dark web

In today's digitally driven world, businesses, especially small and medium-sized enterprises (SMBs), are more reliant on technology than ever before. While this connectivity brings many advantages, it also exposes companies to an ever-growing range of cyber threats.

One such peril is the dark web, where stolen user credentials can become potent weapons in the hands of cybercriminals. This comprehensive guide is crafted for IT leaders and senior management at SMBs. It delves into the critical topic of why stolen user credentials on the dark web pose a significant threat to your business.

About this guide

We will explore what the dark web is, how it operates, and how cybercriminals exploit it for malicious purposes. Furthermore, we will investigate the types of business data that can be exposed and why this exposure represents a substantial threat.

Real-world examples of data breaches caused by exposed credentials will be examined, along with strategies for mitigating the risk and the effectiveness of dark web monitoring as a solution.

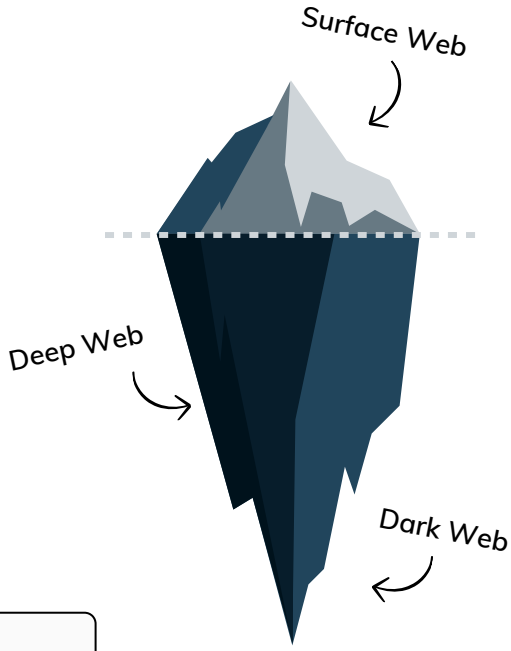
Understanding the Dark Web

What is the dark web?

The dark web is a concealed part of the internet that is not indexed by conventional search engines. It operates within the deep web, intentionally designed to remain hidden from public view. To access the dark web, individuals use specific software, such as Tor (The Onion Router), which allows them to browse anonymously. This inherent anonymity makes it an attractive hub for various illegal activities.

The dark web is a breeding ground for fraudulent activities

The dark web operates within the deep web, intentionally designed to remain hidden from public view. To access the dark web, individuals use specific software, such as Tor (The Onion Router), which allows them to browse anonymously. This inherent anonymity makes it an attractive hub for various illegal activities.

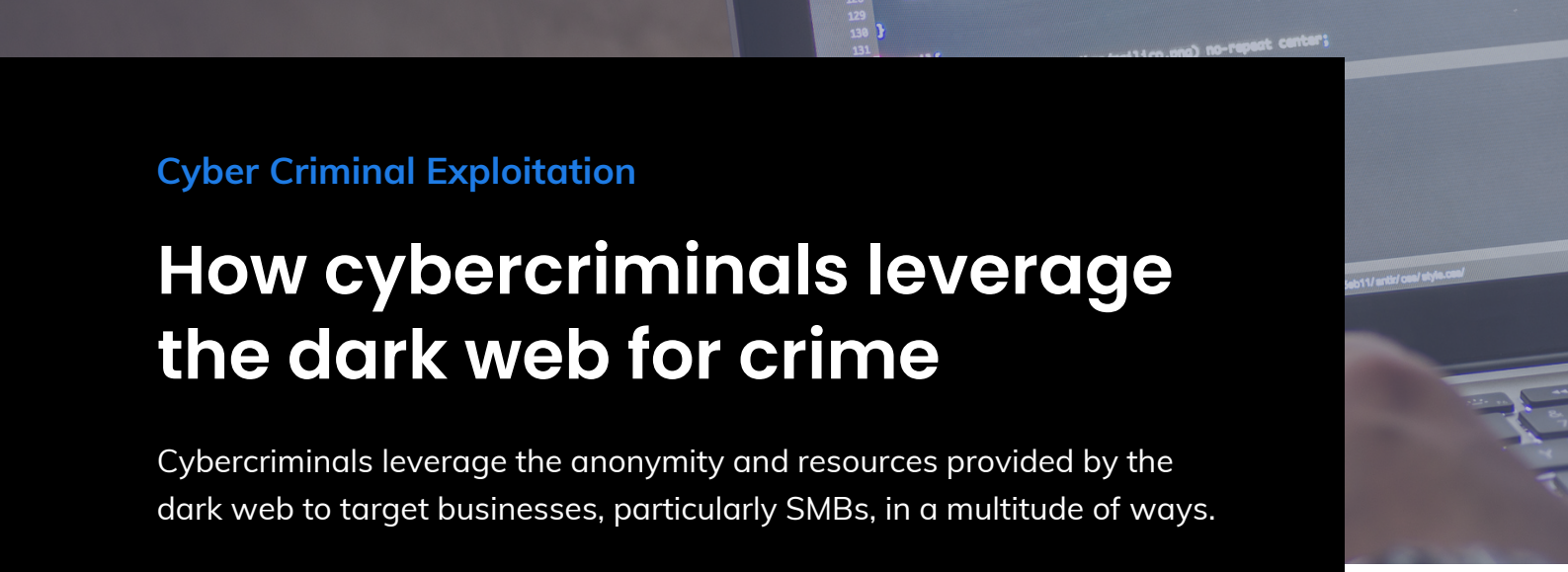




Google Cloud's 2023 Threat Horizons Report found that 86% of breaches involve stolen credentials.



A Digital Shadow report found that 24 billion usernames and passwords are available on the dark web, an increase of 65% in just two years.



Cyber Criminal Exploitation

How cybercriminals leverage the dark web for crime

Cybercriminals leverage the anonymity and resources provided by the dark web to target businesses, particularly SMBs, in a multitude of ways.

Stolen Credentials

Cybercriminals often acquire login credentials for business accounts through data breaches, phishing campaigns, or malware attacks. Credentials are then sold on the dark web, providing unauthorized access to business systems and sensitive data.

Credential Stuffing Attacks

Attackers use stolen username and password combinations to gain unauthorized access to multiple accounts across various online services. SMBs may use shared passwords or weak security measures, making them vulnerable to such attacks.

Ransomware

Cybercriminals on the dark web sell ransomware-as-a-service, enabling less technically proficient criminals to launch ransomware attacks on businesses. SMBs, with limited cybersecurity resources, can be attractive targets.

Phishing Campaigns

Criminals on the dark web offer phishing kits and services that allow them to create convincing phishing emails and websites. SMB employees may inadvertently fall victim to these scams, leading to data breaches or financial losses.

Fraudulent Activities

The dark web provides a platform for cybercriminals to engage in various fraudulent activities, such as identity theft, credit card fraud, and tax refund scams, all of which can target SMBs and their employees.\

Data Sale and Trade

Stolen business data, including customer information, employee records, and proprietary data, is often traded or sold on the dark web. This data can be exploited for financial gain or used in further attacks.

What business data can be exposed?

Businesses store a wealth of sensitive information that can be targeted by cybercriminals through stolen credentials. This data may include:

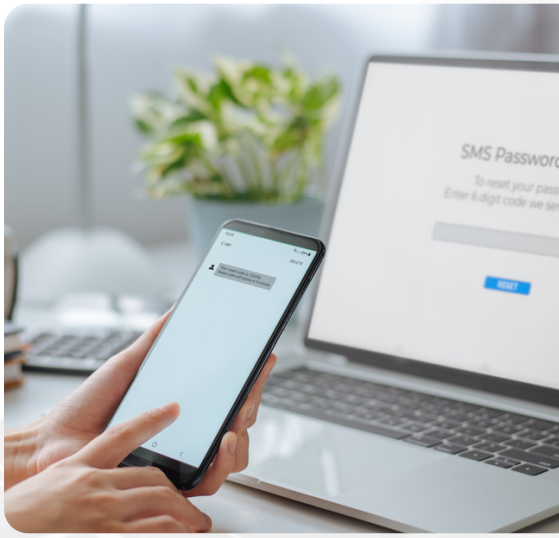
- **User Credentials:** Stolen login credentials, such as usernames and passwords
- **Customer Information:** Personal and financial data of customers
- **Financial Records:** Business financial data, including bank account details
- **Intellectual Property:** Trade secrets, patents and proprietary information
- **Employee Data:** HR records and employee PII (Personally Identifiable Information)
- **Email Correspondence:** Business email accounts are a valuable target
- **Operational Data:** Information related to business operations and supply chains
- **Authentication Tokens:** API keys, access tokens and authentication credentials
- **Financial Data:** Business financial data, including budgets and financial forecasts
- **Legal Documents:** Contracts, legal agreements and compliance reports
- **Vendor and Partner Information:** Information related to vendors and partners

65%

Username and password combinations offered for sale on the dark web has increased 65% since 2020.

24.6 Billion

Some 24.6 billion complete sets of usernames and passwords are in circulation in cybercriminal marketplaces.



Source: Digital Shadows Photon Research

Why is exposed data a threat for businesses?

Exposed user data on the dark web poses a significant problem for businesses as it can lead to severe security breaches and identity theft. This exposure not only risks the personal and financial information of customers and employees but also damages the company's reputation and trust. It can also result in legal consequences and financial losses due to fraud and compliance violations.

Here are just some of the risks businesses face by not addressing dark web threats.

Financial losses
Caused by fines, legal expenses and unauthorized transactions.

Reputation damage
A data breach can erode trust among customers and stakeholders.

Legal repercussions
Caused by lawsuits, regulatory fines, and compliance violations.

Operational disruption
Restoring normal operations after a breach is time-consuming.

> The average impact of a data breach on organizations with **fewer than 500 employees** is $3.31 million; the average cost per breached record is $164.

IBM

IBM 2023 Cost of a Data Breach Report



Examples of real-world data breaches

Large data breaches pose a significant threat to businesses, largely due to the common practice of password reuse across personal and professional accounts. When one account is compromised, it can lead to unauthorized access to others, endangering sensitive business information and trust. Here, we explore some of the largest data breaches of recent times and the scale of data that was compromised.

yahoo!

Date
August 2013
Impact
3 billion accounts

Yahoo

Yahoo's massive data breach, first reported in 2016 but occurring in 2013. Initially estimated at over a billion affected user accounts, Yahoo later revised this to 3 billion. The breach compromised account information like security questions, but did not include plaintext passwords or financial data.

LinkedIn

Date
June 2021
Impact
700 million users

LinkedIn

A hacker posted data from 700 million LinkedIn users on the dark web after exploiting the site's API. LinkedIn classified this as a terms of service violation, not a data breach, as it didn't include sensitive personal data. However, the exposed data contained email addresses, phone numbers, and other details, raising concerns about potential social engineering attacks.

facebook

Date
April 2019
Impact
533 million users

Facebook

In April 2019, it was discovered that data from Facebook apps, including phone numbers, account names, and Facebook IDs of over 530 million users, was publicly exposed. By April 2021, this data appeared for free on the dark web, suggesting criminal intent.



Tackling Dark Web Threats

How to safeguard your business against the dark web

Reducing the risks associated with exposed user data on the dark web is a critical aspect of modern cybersecurity. Here are some essential ways businesses can enhance their defenses and protect sensitive user information.

Regular Data Monitoring and Audits

Conduct regular monitoring and audits of your data. Utilize tools that scan the dark web for stolen data to alert the business if their information is compromised.

Comprehensive User Training

Implement ongoing user training programs for employees to educate them on cybersecurity best practices, phishing scams, and the importance of secure password management, with regularly updated training materials.

Strong Cybersecurity Measures

Adopt robust cybersecurity protocols such as firewalls, intrusion detection systems, and ensuring regular updates to security software. This creates a formidable first line of defense against cyber threats.

Data Encryption

Encrypt sensitive data, both in transit and at rest. Encryption acts as a critical barrier, making it difficult for unauthorized individuals to make use of the data, even if they manage to access it.

Access Control and Authentication Protocols

Implement strict access control measures with strong authentication methods like two-factor or multi-factor authentication. This ensures that only authorized personnel have access to sensitive data.



Dark Web Monitoring

Dark Web Monitoring: An essential layer of security

Dark web monitoring is a proactive approach to detecting and mitigating the risks associated with exposed user credentials. It involves using specialized tools and services to continuously scan the dark web for signs of compromised data, including login credentials.

Here are some reasons why dark web monitoring is an effective solution:

Early detection

Dark web monitoring can identify compromised credentials early in the cybercriminal supply chain, giving businesses a head start in mitigating the risk.

Rapid response

With timely information, businesses can take swift action, such as password resets or notifying affected parties, to minimize the damage.

Benefits of Dark Web Monitoring

Proactive protection

By actively searching for exposed data, businesses can protect themselves before cybercriminals have a chance to exploit it.

Comprehensive coverage

Dark web monitoring tools can scan multiple layers of the dark web, providing comprehensive coverage and reducing blind spots.

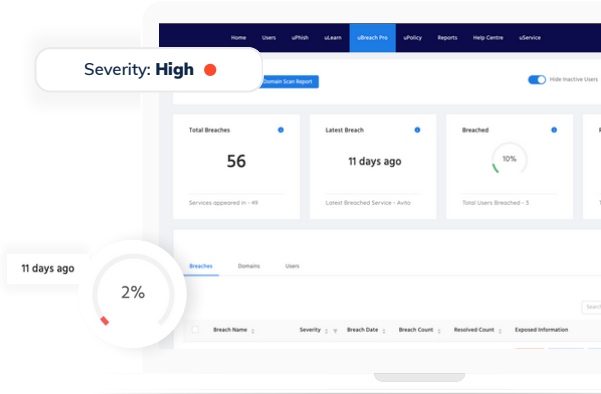


Get in Touch

Does your business have sensitive data exposed on the dark web? Let's find out...

Get a free dark web breach report for your business

Take a crucial step towards safeguarding your business against cyber threats by reaching out for your complimentary dark web breach domain scan.



How it works

Your free domain scan will assess if any of your end-users' business information, including email account passwords, is exposed on the dark web.

What does my business need to provide?

Just provide us with your company's domain name and, if available, a list of specific email addresses you want us to analyze (optional).

Upon completion, you'll receive a PDF report detailing your businesses exposure on the dark web, and what mitigation steps you need to take.



Contact us now and gain peace of mind with our expert breach analysis.