For: Company

Dark Web Monitoring Sample Report

1. Background Information

What is the Dark Web?

The Dark Web is like the black market for cybercrime. When cybercriminals successfully breach or steal information, here is where they put it up for sale for other criminals to purchase as they wish. Often times, we are unaware if our information is being harvested and resold. As they continue to be profitable, breaches and phishing scams will continue to occur, and employee data could be up for grabs leaving whole organizations vulnerable.

Purpose of this Report

All data, new and old, found on the Dark Web can be used maliciously by cybercriminals. Exposed passwords can provide keys to various sites and services if still in use. Email addresses found can be used for direct phishing campaigns and personal data can be used to build advanced social engineering attacks. We cannot change the past, but we can learn from it, and help change the future.

2. Global Monthly Dark Web Summary

Dark Web Overview

February/2022

The Dark Web never sleeps. To highlight the severity of the Dark Web's popularity, we've provided a summary of all the breached information posted to the Dark Web in the month of February. Compare your organization-wide results found on topic 4 - Your Current Dark Web Status.

Exposed Passwords

8244	8139011
February/2022	Total-to-date

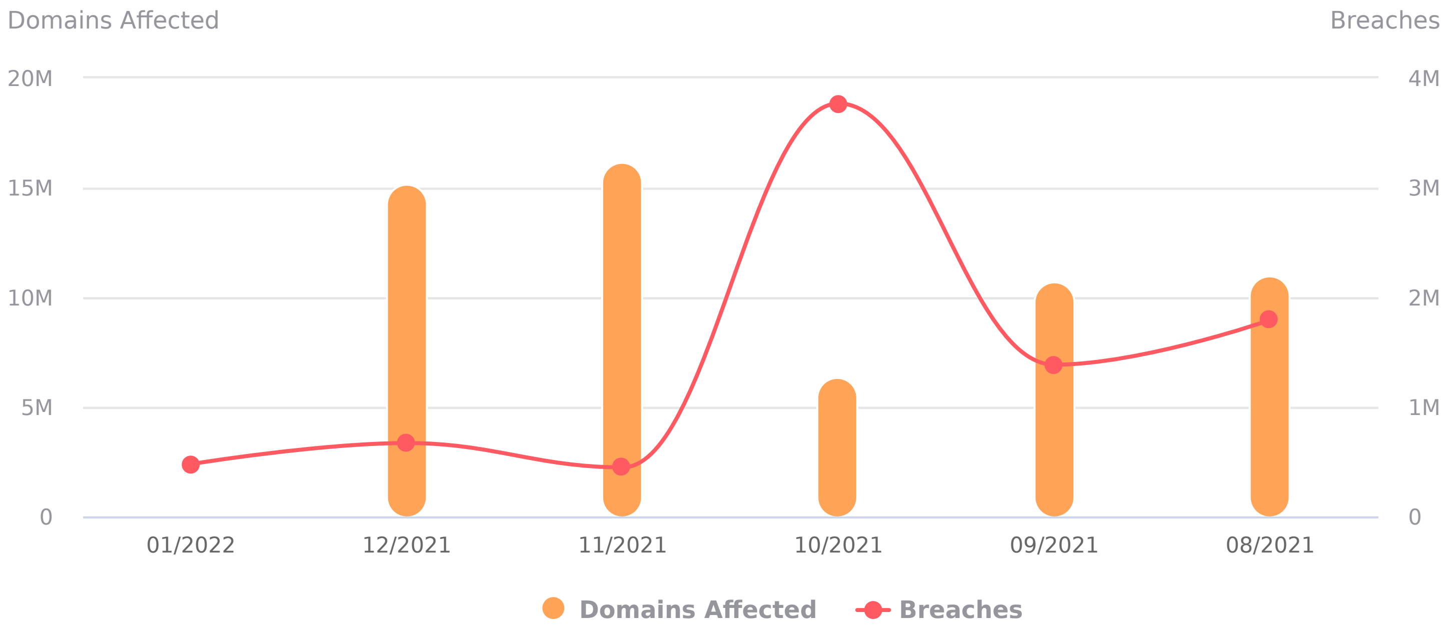
Total Data Breaches

18889	48834071
February/2022	Total-to-date

Dark Web Trends

Previous 6-Months

Our human operatives are constantly scouring the Dark Web for newly exposed data. Here's a look at what they've uncovered over the past six months. Understanding the previous Dark Web posting trends can help forecast risks.



3. Top Industries Attacked in the Last 12 Months

Some industries have more of a target on their back than others. Here's a closer look at the top attacked industries in the last 12 months.

Business and Economy

349

Breaches

Search Engines and Portals

0

Breaches

Sex

0

Breaches

N/A

0

Breaches

Social Networking

0

Breaches

Shopping

0

Breaches

Society and Lifestyles

139

Breaches

Games

781

Breaches

Educational Institutions

2794

Breaches

Forum

0

Breaches

Streaming Media

0

Breaches

Forums

0

Breaches

4. Your Current Dark Web Status

February/2022

Domains Monitored

abcco.com

Exposed Passwords

41

Total-to-date

Total Data Breaches

41

Total-to-date

Overall Risk

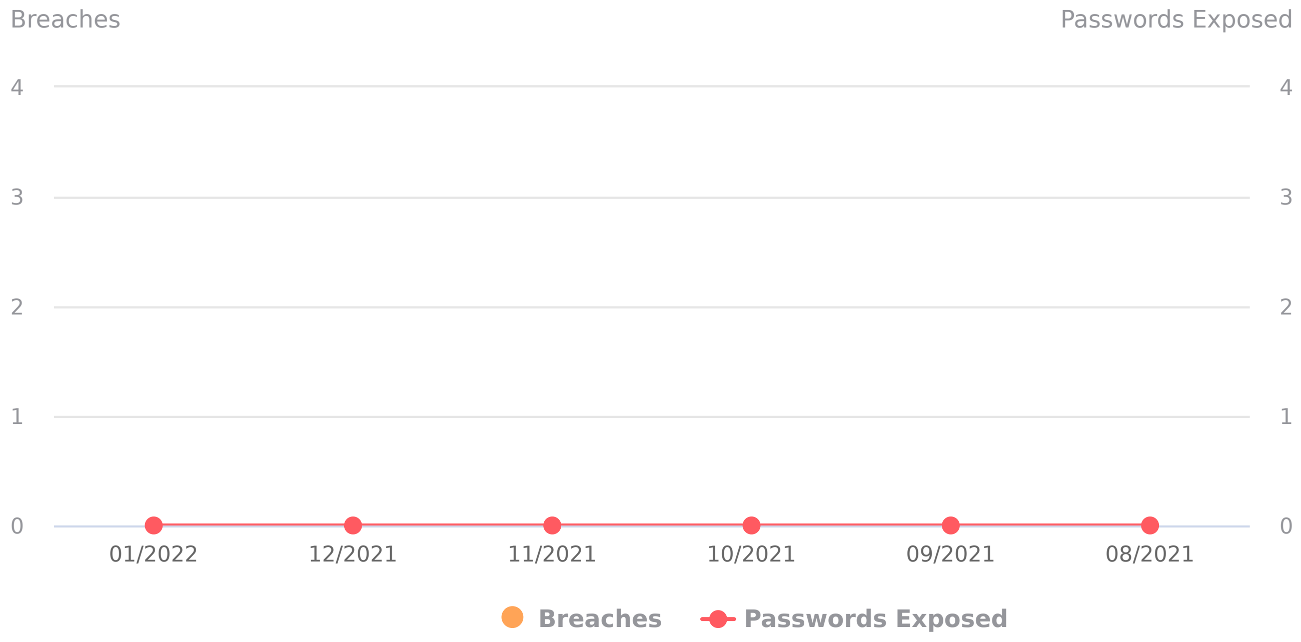
High

Dark Web exposure equals risk, plain and simple. An employee's exposed personal information can be used to craft highly convincing social engineering attacks, like phishing scams, phone scams, and more. By including just enough accurate information, the scammer can often convince their victim that they are the trust-worthy source they claim to be.

Exposed passwords and account information could lead to compromised business accounts, unauthorized access to data and major breaches if these credentials are reused.

With this detailed analysis of recent employee exposures, the time is now to inform the affected employees, change the appropriate passwords and provide proper education to avoid future issues.

Dark Web Exposure Details



5. Latest 22 Dark Web Breach Details

February/2022

We've compiled a list of the most recent compromised accounts affecting your domains. All exposed data is important, but the most recent breaches should be addressed immediately.

For a full list of breaches and more details, visit **https://portal.pii-protect.com** for more information.

1 gail@abcco.com

Date	Account Breached	Data Exposed
2021-06-14	2021_RockYou	

2 tawny@abcco.com

Date	Account Breached	Data Exposed
2021-04-26	clearvoicesurveys.com	address,date of birth,email,ip address,login,name,password
2020-12-07	cit0day_3 - sites.citycheers.com	address,email,password
2018-05-22	solenya2 collection sites.citycheers.com {40.479} [HASH]	email,password
2016-05-19	LinkedIn credentials dumped	address,email,password

3 clay@abcco.com

Date	Account Breached	Data Exposed
2020-11-18	cit0day_premium - ssgainstitutional.com	address,email,password
2016-05-19	LinkedIn credentials dumped	address,email,password
2013-11-11	Adobe Hack	address,email,login,password

Continue on the next page

6. Latest 22 Dark Web Breach Details

February/2022

4 dijo@abcco.com

Date	Account Breached	Data Exposed
2020-10-21	Mixed Credential and PII Dump - July 2020 - internal.labase.org	
2019-12-19	The 2844 Collection - internal.labase.org	
2018-03-15	internal.labase.org.txt solenya collection leak	

5 jsmith@abcco.com

Date	Account Breached	Data Exposed
2020-06-19	LeadHunter_Part-32	address,email,ip address,name,phone
2019-12-28	The 2844 Collection - evony.com	
2017-11-01	Onliner Spambot email list	email,password
2017-10-16	Evony game creds breach	password

6 123@abcco.com

Date	Account Breached	Data Exposed
2020-06-19	ExploitIN 800M - Part 38	email,password
2020-01-29	Big Asia Leak	address,email,password
2016-08-01	very large credential dump	
2015-08-18	Alleged AshleyMadison.com data breach release	address,email,login

Continue on the next page

7. Latest 22 Dark Web Breach Details

February/2022

7 abc@abcco.com

Date	Account Breached	Data Exposed
2020-06-17	ExploitIN 800M - Part 14	email,password
2016-08-01	very large credential dump	
2013-11-11	Adobe Hack	address,email,login,password

8 corinaperez@abcco.com

Date	Account Breached	Data Exposed
2020-06-17	ExploitIN 800M - Part 13	email,password
2016-08-01	very large credential dump	

9 jdoe@abcco.com

Date	Account Breached	Data Exposed
2020-06-17	ExploitIN 800M - Part 13	email,password
2019-06-24	Collections No. 1 Credentials Leak Deduped	
2016-08-01	very large credential dump	

10 jo@abcco.com

Date	Account Breached	Data Exposed
2020-05-13	PetFlow	address,email,password

Continue on the next page

8. Latest 22 Dark Web Breach Details

February/2022

11 trstaccount@abcco.com

Date	Account Breached	Data Exposed
2020-02-11	Zynga	address,email,password

12 a@abcco.com

Date	Account Breached	Data Exposed
2017-11-01	Onliner Spambot email list	email,password

13 jeff.smith@abcco.com

Date	Account Breached	Data Exposed
2017-11-01	Onliner Spambot email list	email,password

14 kim.williams@abcco.com

Date	Account Breached	Data Exposed
2017-11-01	Onliner Spambot email list	email,password

15 tim.jones@abcco.com

Date	Account Breached	Data Exposed
2017-11-01	Onliner Spambot email list	email,password

16 bm@abcco.com

Date	Account Breached	Data Exposed
2016-06-01	MySpace credentials dump	

Continue on the next page

9. Latest 22 Dark Web Breach Details

February/2022

17 amy.smith@abcco.com

Date	Account Breached	Data Exposed
2016-05-19	LinkedIn credentials dumped	address,email,password

18 REBECCA.SMITH@ABCCO.COM

Date	Account Breached	Data Exposed
2016-05-19	LinkedIn credentials dumped	address,email,password

19 sdawson@abcco.com

Date	Account Breached	Data Exposed
2016-05-19	LinkedIn credentials dumped	address,email,password

20 shane@abcco.com

Date	Account Breached	Data Exposed
2016-05-19	LinkedIn credentials dumped	address,email,password

21 fred@abcco.com

Date	Account Breached	Data Exposed
2016-03-11	Large credentials cache	email,password

22 user23@abcco.com

Date	Account Breached	Data Exposed
2015-08-18	Alleged AshleyMadison.com data breach release	address,email,login

10. What's the Impact?

Breached Passwords

When breached account credentials like email address and passwords become available on the dark web, they can be used to access that account, steal information, or access additional accounts that may use the same credentials.

Spear Phishing

Even if passwords weren’t compromised on the dark web, the email address, physical address, or other personally identifiable information can be used to craft specific and convincing phishing emails that could put your business at future risk.

Network Access

If the credentials compromised are the same credentials used to access your business network or sensitive customer information, criminals could use this information for unauthorized access to your network where they can wreak havoc.

11. What Happens Now?

Someone at your organization had data exposed on the dark web… what happens now? Unfortunately, the impact of a third-party data breach involving your or one of your employee's business accounts could be a vulnerability to your business. Learn what you can do to proactively address these hidden threats

How can I **protect** my employees and my business.

We know this information can be alarming and quite frankly, scary, but it doesn't have to be! We share this information with you to keep you informed so you can proactively prevent this compromised information from coming back to harm your organization in the future. We strongly recommend that all impacted employees take the following steps towards remediation.

1. Update your password on the compromised account
2. Be wary of an increase in phishing emails being sent to you.
3. Avoid using your business email address for non-business activities and account management.
4. Change the password for all accounts where this password may have been reused and remember to use strong, unique passwords for all your accounts

Have **questions** or want more tips on best practices?

If you have questions on any of these results or how to proactively protect your employees and your business, please feel free to contact us!