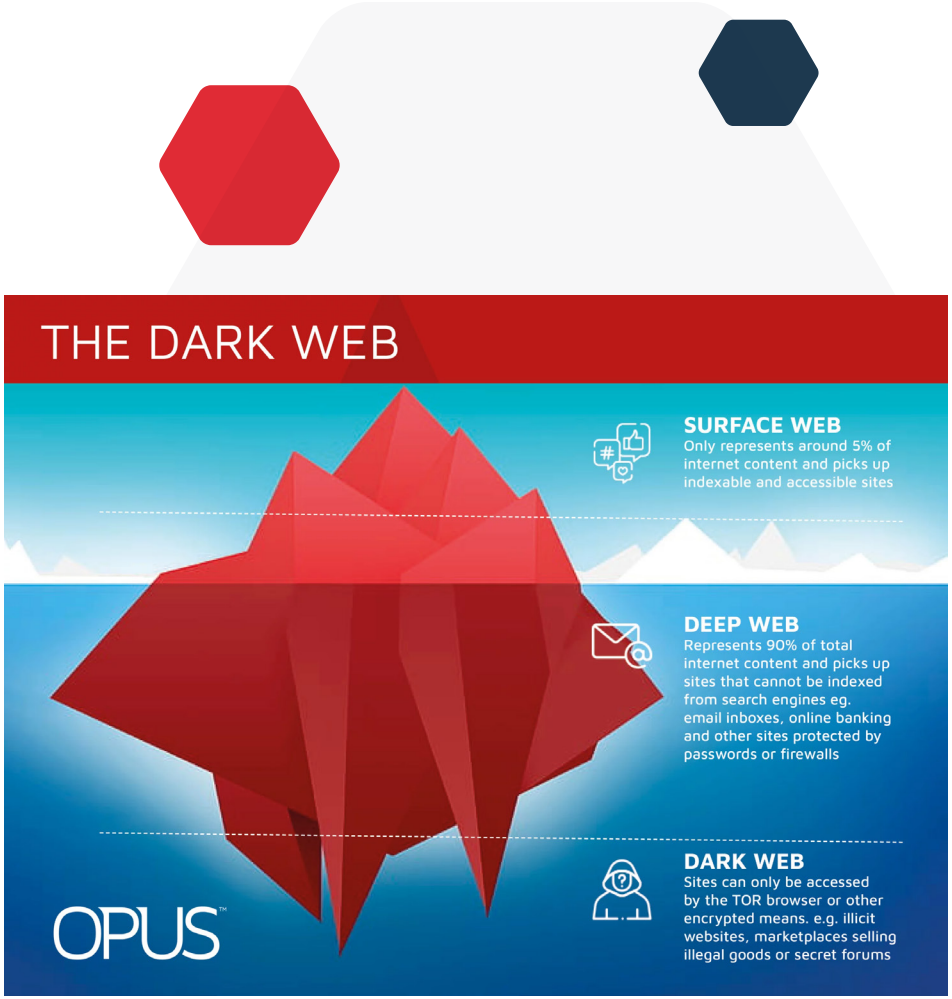
Dark Web Monitoring Guide

OPUS

What is the Dark Web?

The Dark Web, part of the deep web, refers to an unregulated portion of the internet that is not indexed by traditional search engines and is only accessible through the specialist Tor Onion browser or other encrypted means.

It is a hidden network that offers anonymity to its users through specialist web browsers and is often associated with illegal activities, such as online scams, the sale of illicit goods and services, medical records, legal documentation, sale of stolen data, and more. Not many people are aware of the Dark Web, but the data available to criminals on it poses a significant threat to businesses.



My credentials are on the Dark Web

At this point, you have likely received a report on your business domain and discovered that a number of credentials relating to your business and its employees are available on the Dark Web.

A Dark Web scan will indicate the number of exposed credentials and can help to determine the severity of the risk, however, is only relevant at the time of the scan. If a breach occurs the following day and more credentials are obtained, your report will not account for this.

As a result, this guide has been created to outline the damage limitation exercises you should follow to significantly reduce the risk of being affected by stolen credentials, now and in the future.

How did we end up on the Dark Web?

Credentials such as usernames and passwords most commonly end up on the Dark Web through data breaches. Often it is third party sites that employees are signed up to which are targeted by criminals and subsequently breached.

Unfortunately, as individuals, there is nothing we can do to prevent this from happening. When signing up to a new site or service, you are trusting the third party to correctly store and manage your personal data.

Your e-mail address could also appear on a data list owned by a data broker, perhaps through signing up to an untrustworthy site before the GDPR was introduced, which are notoriously shared with cybercriminals.

What are the risks?

Having credentials that are directly related to your business available on the Dark Web puts you in a vulnerable position, increasing the chances of your business suffering a breach.

Often employees use the same usernames and passwords to log in to multiple applications for personal and work purposes. This includes access to your network, VPN and critical business applications such as CRM's and your website. If the credentials found on the Dark Web are the same as what employees use at work, it can be very easy for a criminal to gain access to your business' systems.

The secondary risk is the increased chance of falling victim to a targeted spear-phishing attack. With only a single employee e-mail address available on the Dark Web, criminals are able to form incredibly targeted phishing e-mails appearing from the victim and attack your business. This information dramatically improves the success rate of phishing attacks and opens your business up to much wider threats.

Tips for protecting your business

It is not possible to remove yourself or your employees from the Dark Web.

As soon as you make it there, your records are likely to be sold and shared multiple times throughout criminal networks. This means that you can only limit the damage that can be caused by stolen credentials.

We have written this guide to provide steps you can take to reduce the risk of breached credentials affecting your business and steps you can take to prevent them from appearing on the Dark Web again.

Get your staff passwords updated
The very first action you should take is to ensure that all passwords are changed for all employees across all business applications. This is the most important and easiest way to reduce the risk of your business being affected by exposed credentials. A password manager is the best way to manage this as they centralise all of the applications being used, allow global actions to be taken and make it easier for employees by only requiring a single password to access each application. A PAM (Privileged Account Management) tool will ensure that administrator passwords are secured and monitored.

It is also best practice to introduce regular password changes. We recommend monthly changes to keep your business secure.

Does your business have a strong password policy? If not, now would be an ideal time to introduce one.

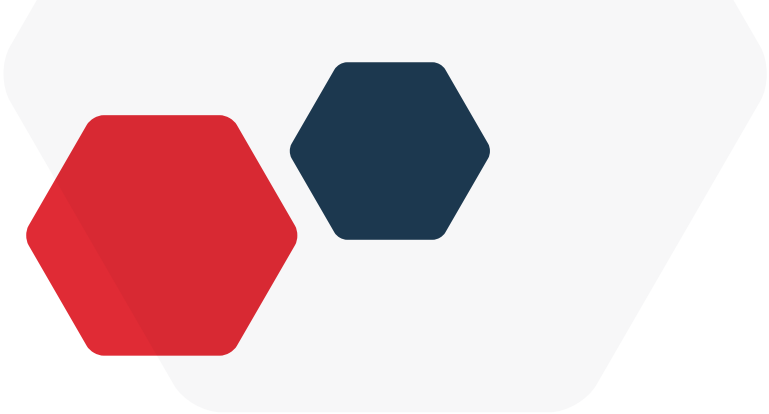
Strong passwords consist of:
- **12-15 characters**
- **Passphrases rather than single words**
- **A mixture of letters, numbers and symbols**
- **Upper and lowercase letters**

By introducing a strong password policy, you are much improving the security of business applications across your business. Additionally, we recommend that you state that business e-mail accounts are not to be used for non-business purposes.

Enable multi-factor authentication
With passwords now changed, the next step is to enable multi-factor authentication across business applications. Commonly found across third party sites, multi-factor authentication requires the user to provide another means of authentication (on top of their password) to log in. This is most commonly via a code sent in a text message or through an authenticator app.

Having this in place within your business prevents criminals, who only have login credentials, from logging into critical business applications and systems. Solutions such as SecurEnvoy or OneLogin are our recommendation.

Vulnerability scan
To ensure that the stolen credentials haven't already resulted in malware making its way onto your network, you should carry out a vulnerability scan. This is usually an automatic process in which your end points, network and infrastructure are scanned for potential threats. If you already have good anti-virus in place, you should expect a clean result.



Penetration testing
Your web presence is under constant threat from attackers. Stolen credentials provide criminals with access to embed code that will allow unceasing access even after detection. By introducing a continuous penetration testing service, your web services are protected with threat monitoring and risk analysis by both machine intelligence and trusted ethical hackers.

Monitor the Dark Web on an ongoing basis
With your business now much less likely to suffer a breach from stolen credentials, the final step is to enable Dark Web monitoring. This will alert you to new breaches associated with your corporate domain, giving you notice so that you can deal with the newly breached credentials in good time. Our Opus Credentials Breach Monitoring service does just this, along with monthly reports, supply chain monitoring and up to five personal e-mail address searches.

Social engineering and phishing training
There is also an increased chance of your business being targeted through phishing or social engineering. These types of attacks are responsible for over 90% of breaches according to a thorough study by IBM and the Ponemon Institute. The only way you can truly prevent phishing attacks from being successful is through training and regularly testing your employees. We recommend using a fully managed security awareness solution to reduce the time and resource efforts you would need to invest for an effective service.

Additional layers of security
The following recommendations are not essential to stopping stolen credentials from harming your business, however, do go a long way to protecting you from developing threats.

User endpoint behaviour analytics (ueba)
A User Endpoint Behaviour Analytics tool looks at human behavioural patterns and identifies anomalies within them. In doing so, UEBA is able to flag suspicious activity which can indicate potential threats.

In context, a User Endpoint Behaviour Analytics solution would be able to detect and assess a change in a user's behaviour or location when logging into business applications. This would make you instantly aware of stolen credentials being used to access your internal systems.

Data governance tool
Data Governance gives your business a comprehensive view of where your data is stored and how it is being used. By applying permissions that manage how and when data can be accessed, you have much greater control over your data. If a data breach occurs through stolen credentials, a Data Governance tool will give you alerts and visibility if a cybercriminal is attempting to access or move your data.

Frequently asked questions

Here are some frequently asked questions about Opus' Dark Web Monitoring Service and how it can help your business.

What does this data mean?
Opus data shows compromised e-mail accounts, passwords and sometimes PII that is readily available on the Dark Web. Typically this information is obtained through employees signing up to third party websites, apps or services with their corporate e-mail accounts. If these sites or services are breached, your business credentials can be obtained by cybercriminals. The bigger threat to your business however is through a phishing attack. Opus can identify trends where credentials could have been obtained through a phishing attack on your business.

That is not my current password, I don't use it anymore
This report provides historical as well as live real-time data. At one point in time, there was risk associated with these credentials and there could still be. 47% of people are using the same or very similar passwords for multiple online sources. These passwords (whether active or not) are being used in phishing exercises and can be very compelling.

Why is there no password listed?
We pull in very large data sets that include passwords. Sometimes in those data sets a variety of credentials do not include passwords, while in other cases, several categories of PII (Personally Identifiable Information) may have been exposed. (Ex. Name, DOB, Address). Why does the PII matter in lieu of the password? Often, the categories of PII are extremely sensitive and may include credit card information or home addresses. These can be catastrophic to the individual.

I don't see the value of continuous monitoring
It only takes one user to click on a phishing e-mail or to use work credentials on a third-party site that may get compromised for your credentials to become available on the Dark Web. The results can be devastating. Without sight of such data for sale on the Dark Web, such compromises can go undetected. Opus is a low cost early warning system that helps to mitigate the effects caused by a breach, with an easy to use portal available 24 x 7.

I'm worried about additional exposure (as a result of the search)
The data we are pulling in is considered publicly available information. Our analysts DO NOT know who our Partners are, or who their clients are. They are pulling in credible credential exposures from the Dark Web, not placing it out there or using the data for any other purpose.

I've never used that password
If a password appears in your report that an individual has never used, it will be for one of three reasons;

- They have either forgotten they've used it before
- A criminal is testing a password
- Someone is creating a fictitious account for fraudulent purposes.

Often, when criminals handle breach data, they work to put a value on the data. This may involve attempting to conirm the validity of a username/ password combination. If such testing is positive, the password is often left in the source data. If the test is negative, the handler may fill in some placeholder value such as noted above to indicate that the username/ password could not be confirmed as valid. Our guidance is to treat such compromises with the same weight you would one that has a clear text password.

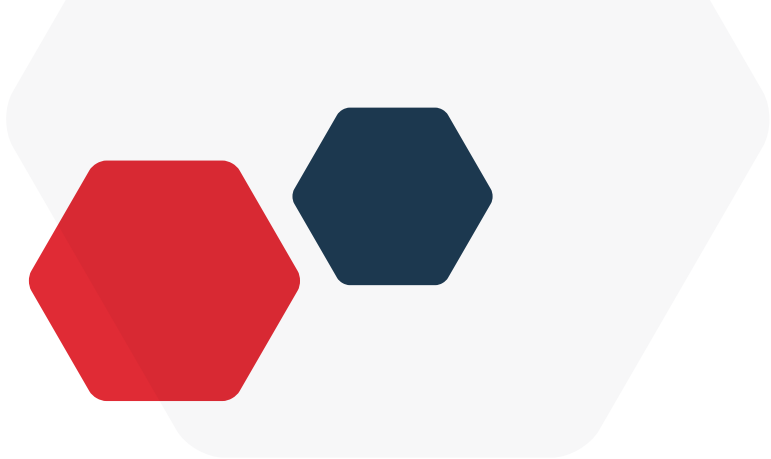
What is the difference between your service and Haveibeenpwned.com?
Opus Dark Web monitoring service will monitor the whole domain and provide any exposed PII on any account that contains your domain name(s). Standard HaveIBeenPwned.com service only monitors individual e-mail addresses. We use a wide range of data sources to identify exposed credentials, providing more extensive coverage than Haveibeenpwned.com, which does not include passwords making it impossible to verify the data for your employees/business.

Under website it's saying, "Not Disclosed,"... why should I care if it doesn't say where it came from?
While we do our best to provide as much attribution as possible, every category on the Dark Web is not always available and there are cases where we are waiting for public acknowledgment of a breach for legal purposes before assigning attribution to a specific website. With increased notification laws, we will see the speed of published attribution increase. We also retroactively provide attribution when we can.

The most important piece of information however is not where the password came from but instead that if it is an active network password, a variation of one or their banking password, you need to get it changed.

Why do some passwords appear as a key/code?
These passwords are encrypted, but can quite easily be cracked using various sites readily available on the internet. While initially a breach might include encrypted data, it's important to understand that the data is only safe if the encryption key has not been published.

Once the encryption key is published, much of that data is no longer safe. LinkedIn is a great example of this. 164M records were exposed in the LinkedIn breach. The passwords in the breach were stored as SHA1 hashes without salt, the majority of which were quickly cracked in the days following the release of the data.



How 'continuous' is your monitoring?
Our monitoring is, indeed, 24 x 7 with information pulled around the clock. We gather data directly from the Dark Web but also have people in there listening, watching, learning and then sharing that information for posting. The data we collect on your business is then encrypted and stored securely.

How many Dark Web 'Sites' are you monitoring to get the results and what percentage is this approximately?
The Dark Web is not something you measure in the way of number of sites and percentage. It's an ever-changing place where information comes and goes including data, chats, forums, other conversations. The websites that post data in the Dark Web are there one moment, gone the next (literally, they just shut down and may open again with new information in the future).

I can't validate the report because it shows employees that no longer work here.
While employees may have moved on from your business, their company issued credentials can still be active and valid within the third party systems they used while employed. In many cases, the third party systems or databases that have been compromised have been in existence for 10+ years holding millions of "zombie" accounts that can be used to exploit your business. Discovery of credentials from legacy employees should be a good reminder to confirm you've shut down any active internal and third party accounts that could be used for exploit. The real value of this data is the ongoing monitoring which enables you to know about the credential exposure happening today, next week and next month.

These passwords are old and not used, where is the risk?
This report provides historical as well as live real-time data. At one point in time, there was risk associated with these credentials and there could still be. 47% of people around the world are using the same or very similar passwords for multiple online sources. These passwords (whether active or not) are being used in phishing exercises and can be very compelling.

Why are no passwords shown?
We pull in very large data sets that include passwords. Sometimes in those data sets a variety of credentials do not include passwords, while in other cases, several categories of PII (Personally Identifiable Information) may have been exposed. (Ex. Name, DOB, Address, SSN) Why does the PII matter in lieu of the password? Often, the categories of PII are extremely sensitive and may include credit card information or home addresses. These can be catastrophic to the individual.

How do I access data and reports on an ongoing basis?
Signing up to the full Opus Dark Web monitoring service gives you access to a dedicated portal, where you can view the Dark Web presence of all of your corporate, supply chain and personal domains. You can run live searches and pull reports at any time. Login to your portal with the details our provisioning team have provided and go to the 'Compromises' section to view all of your data.

How do I create a compromise summary report?
Login to your portal and visit the 'Dashboard' page. Reports are generated within a specific date range that you can set. Set your desired date range using the 'date range' field in the top left hand corner. To the right of this is the 'print report' button. Click this to generate the report and choose whether you would like to include a glossary of terms with the report. This is useful if the report is being passed onto other individuals within your business.

How do I track the status of new and existing breaches?
In the 'compromises' section of the portal, select a single compromise and expand the drop-down box under 'record status'. This is where you can set the status of a breach in relation to how it is being remediated. If a new breach is identified, it will be tagged as 'new'. When you are working on resolving it, set the status to 'in progress'. When it has been seen to, set the status to 'resolved'. You can filter your searches across breaches via status.

How do I build filters for my searches?
In the 'compromises' section of the portal, scroll down to 'filters' and select 'add'. You can build certain filters based on different variables. Start with 'compromise type' and select the domain you wish to search for. Variables after this could be things like the source of the breach (filtered only to show breaches through file sharing) or date of the breach (filtered to show a specific month).

How do I contact Opus support?
In the top right hand corner of the portal, you'll find a navigation bar with 'support' furthest right. Expand the box and click support to get in contact with us.

Glossary of Terms

Compromise Type:

Accidental Exposure
The compromise of data is attributed to an unintentional disclosure by non-malicious actors on a web page, social media, or peer-to- peer site.

Bot
The compromise of data is attributed to botnet activity.

Breach
This data was compromised as part of a organisation's data breach.

Data Dump
A consolidated collection of new and/or previously compromised credentials were made available for bulk consumption.

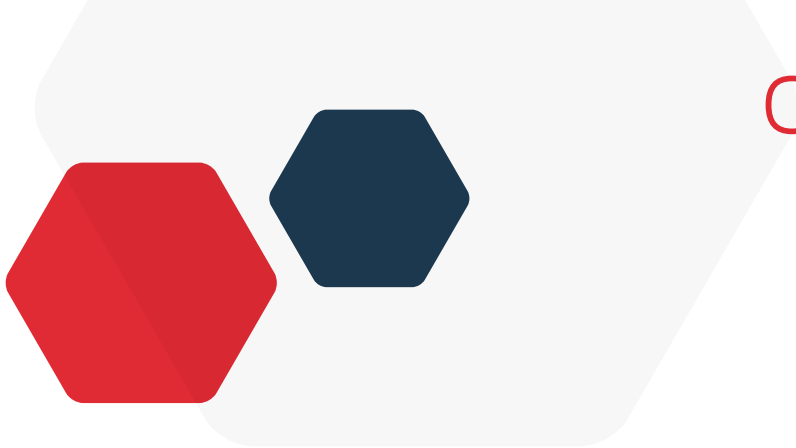
Dox
The data was disclosed as a part of a Doxing export. Doxing is the research, collection and broadcast of private or personally identifiable information (PII) about an individual or organisation. Doxing may be carried out for various reasons, including extortion, coercion, inflicting harm, harassment, and online shaming.

Keylogged / Phished
The compromise of data is attributed to entering into a phishing website or extracted through software designed to surreptitiously harvest personally identifiable information (PII)

Not Disclosed
The corresponding metadata associatedwith the collected information is currently insuficient to accurately attribute to a specific compromise type.

Sample
The data was disclosed is a subset of a larger dataset disclosed by an individual or organisation to prove its validity of an exploit / breach.

Tested
The data was legally tested to determine if it is live/active data.



Source Type:

Asprox
The IP address has been identied as associated with the Asprox botnet, also known by its aliases Badsrc and Aseljo, and is mostly involved in phishing scams and performing SQL injections into websites in order to spread malware.

C2 Server
The IP address has been identified as being associated with a Command-and-control (C2) Server. Command-and-control servers are used by attackers to maintain communications with compromised endpoints within a targeted network. These compromised endpoints collectively are referred to as a botnet. This is achieved through infecting endpoints with malware. Botnets are leveraged by attackers to conduct malicious activity (send spam, distribute malware, etc) without the knowledge of the system owner.

Chat Room
This data was discovered in a hidden Dark Web internet relay chatroom (IRC).

Cutwail
The IP address has been identified as associated with the Cutwail botnet and is mostly involved in sending spam e-mails. The bot is typically installed on infected machines by a Trojan component called Pushdo. It affects computers running Microsoft Windows.

File Sharing
The IP address has been identified as associated with malicious file sharing activities.

ID Theft Forum
This data was discovered being exchanged on a Dark Web forum or community associated with ID theft activities.

P2P File
This data was discovered as part of a file being exchanged through a peer-to-peer file sharing service or network.

Public Web Site
This data was discovered on a publicly-accessible web forum or data dump site.

Social Media
This data was discovered being shared as a post on a social media platform.

Webpage
This data was discovered on a hacker website or data dump site.

Zero Access
The IP address has been identified as associated with the Zero Access botnet. At the time of discovery, the ZeroAccess rootkit responsible for the botnet's spread is estimated to have been present on at least 9 million systems (2012).

OPUS

Combining unrivalled expertise, a customer-centric approach, and world-class technology to power our clients' ambitions.

opustech.co.uk
080 0047 3537