DARK WEB MONITORING:
What you need to know

What is the Dark Web

The cybercrime landscape is evolving fast . The “Nigerian” email scams are now old. Cybercriminals are smarter and more organized now--almost functioning like professionals. In fact, there’s a sort of a parallel universe where they all operate in a very corporate-like manner. And that parallel universe is called the Dark Web.

The surface web, the Deep Web, and the Dark Web

Essentially, the internet can be categorized into 3 parts.

- The surface web, which includes your ‘regular’ websites--the kinds that just show up on web searches. For example, you type, Dog Videos and links to a bunch of dog videos on YouTube shows up. YouTube, in this case, is an example of the surface web.
- The deep web, which shows up in web searches, but requires you to log in to view specific content. For example, your internet banking page or your Netflix subscription.
- Then comes the dark web.

The dark web is part of the internet that isn't visible to search engines and requires the use of an anonymizing browser called Tor to be accessed[1]. The dark web offers anonymity and hence is the hub for all sorts of illicit activities in today’s internet age. Strictly speaking, the dark web typically hosts illicit content. The kind of content that you find in the dark web include

- Credit card details, stolen login credentials for something as serious as internet banking accounts to something as trivial as Uber or Netflix,
- Contact details/communication platform for striking deals with hitmen, drug dealers, weapon dealers, hackers, etc.,

[1] ***CSO Online:*** *https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html*

- Marketplace to buy malicious codes to help corrupt or jam IT systems and even RaaS (Ransomeware as a service!)

All of the above and more, for a fee of course. In short, the dark web is like the underworld of the internet.

So, how does it concern you? Well, your data could be on the dark web as well. The dark web is essentially a marketplace for cyber criminals. If your data has been compromised, the dark web is the place where it is traded. It could be sold by miscreants, to miscreants, who can later hack into your system or extort money from you to prevent a data leak and so on.

What can be the implications for your organization if you are on the dark web?

If your data is on the dark web, it puts your business and your customers at risk. For example, as a business, you possess a lot of the Personally Identifiable Information (PII) of your customers, which, if leaked can even shut down your business by

- Attracting lawsuits that require you to shell out large sums of money in the form of fines or settlements
- Causing serious damage to your brand
- Resulting in the loss of customers and new business

What are dark web monitoring services?

One way to mitigate the risks of the dark web is by signing up for dark web monitoring services.

As a part of the dark web monitoring service, a company may keep an eye out for any information you specify or that is related to you that may be present or traded on the dark web. There are various avenues where such information may be made available on the dark web. Examples include

1. Chat forums
2. Blogs
3. Social media platforms
4. Online marketplaces (Dark web's equivalent of eBay or Craigslist)

Another service offered as a part of dark web monitoring includes vulnerability alerts. On the dark web, there will be entities who will be willing to give away information about vulnerabilities in certain systems/software for a price. A company that offers dark web monitoring will keep an eye out for such information and alert its customers of such threats.

Companies offering dark web monitoring services may also be able to offer you industry insights, trends and benchmarks that can help you proactively tighten your cybersecurity.

What you can do: Safeguarding your data against the dark web

With dark web monitoring services, you will know if there has been a data breach. Let's say you come to know your e-commerce website's user IDs and passwords have been stolen, or your customer's credit card data has been leaked via your database, you can take the necessary steps to mitigate a possible ransomware attack or data leak before it happens. But, that's reactive. That's damage control after the damage has been done. While dark web monitoring services can warn you if your data has been compromised, here are a few things that you can do to keep your data safe in the first place.

Password Hygiene

Follow good password hygiene and industry best practices. Establish clear password policies and rules and regulations regarding password sharing. For example, discourage the use of the same passwords for multiple accounts or use of passwords that are too simple or obvious such as user's name, date of birth/date of joining organization or numbers in sequence, etc, establish policies regarding password update at regular intervals.

Train your Staff

Train your staff to identify spam, phishing, and other malware traps. Conduct tests and mock drills and re-train those who don't pass them. Provide updates when there's a new threat in cyberspace that may affect you.

BYOD Policies

If you allow your employees to bring their own devices to work, establish a clear BYOD framework that will help you manage the risks associated with this setup.

Access Permissions and Roles

Establish different user roles for your staff and give them role-based data editing, copying or sharing permissions, so that each employee only has as much access to information as they really need.

Being exposed in the dark web can be exhausting, scary and life-threatening to a small or medium-sized business. Teaming up with an MSP who specializes in cybersecurity or offers dark web monitoring services can help keep you safe.

HALOCK®

For more information please contact,
Cindy Kaplan
HALOCK Security Labs
P: 847.221.0200
ckaplan@halock.com
https://www.halock.com
1834 Walden Office Square, Suite 200, Schaumburg, IL, 60173