DARK WEB MONITORING USE CASES

APRIL 28, 2021

Forint Limited
Authored by: David Martin-Woodgate

Introduction

The need for Dark Web Monitoring

A large-scale data breach has the power to cripple any organisation, including the potential to gain access to your third parties concurrently. Unfortunately, most of the reported data breaches start with the use of compromised credentials, of which are sold to the highest bidder on the dark web.

Dark web monitoring is essential for any company that wants to keep their data secure and avoids the far-reaching ramifications of a data breach, like noncompliance fines, loss of business, virtual theft, damaged reputations, and more. In a world where everything is digital, companies need to be vigilant in their data protection.

> ***"Right now, all that stands in the way of your data and a costly breach is a single compromised password"***

Secondly, in an age of increasingly common data breaches and the high costs that come with them, the dark web monitoring service can be a competitive advantage for your company. Incorporating this service into your organisation can provide you with the forward intelligence of an impending attack, or the potential that leaked credentials can be used for nefarious purposes.

As such, the dark web monitoring service can be incredibly beneficial to an organisation, as an additional defence-in-depth layer, if they know where and what to look for. The following use cases for dark web monitoring will explain how this service can be used within various risk-based opportunities within your organisational (and home) environments.

Use Cases – Dark Web Monitoring

Use Case 1 – Tracking Threats

Cybersecurity threats monitoring for risk management is one of the dark web monitoring use cases. This will allow an organisation to understand the threat actors that focus upon their organisation, VIPs and brands. Efficient investigation of these sources can carry insight to attackers' tools, strategies, methods, operations, and motive which then we can apply to our security strategy.

Specifically, we need to understand the personas of the threat actors and how organised and well-known these threat actors and attack surface are which we need an understanding of their dark web forum handles, their reputations, what they do, where they do the work and their whole modus operandi. Constantly gathering and tracking this data will help to apply context to these actors and better foresee and recognize threats also empowering organizations to plan defence strategies.

Similarly, insiders with valuable data or privileged access can use online forums and marketplaces to sell your valuable data. These insider threats are difficult to remediate quickly and pose a major challenge to any security team. Applying this context of threat actors and knowledge of the dark web landscape to tracking can allow you to proactively uncover threat actors targeting your company, VIP, and brand and further, allow an organisation to put into place the necessary protection to support the defence against a pre-determined attack.

Use Case 2 – Identification of Exposed Credentials

The second dark web monitoring use case is security from discovered data and credential stuffing. Since password reuse is so normal, credential stuffing has formed into a well-known strategy to access sensitive data. In the end, the defence system is just as good as how weak the credential is.

Credentials from data breaches are sold in bulk on the dark web to other threat actors. These threat actors take the usernames and passwords and automate an overhaul login to gain access to valuable assets. Recently, it has been seen that more than just exposed credentials are being compiled and sold.

THIS IS THE DARK WEB

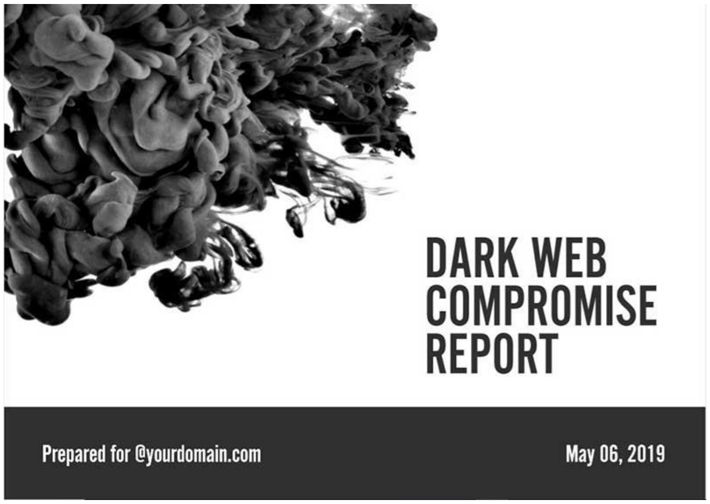
And we help to keep you out of it.

Our Dark Web monitoring platform provides the most validated credential exposure data available. ID Agent's sophisticated intelligence allows companies to focus on their business with peace of mind.

One gated market, Genesis Store, sells bots that bypass fingerprinting controls – providing customers with fingerprints, cookies, logs, saved passwords, and other personal information to emulate users and bypass security systems. This is an interesting development, enabling cybercriminals to bypass traditional anti-fraud controls.

Use Case 3 – Fraud Identification

One application of these stolen credentials is to commit fraud – whether that is trading payment card details, selling counterfeit goods, or phishing. One of the benefits of Genesis market taking this approach to collect credentials is they can have a more novel and effective way to impersonate users online for fraudulent purposes.



DARK WEB COMPROMISE REPORT

Prepared for @yourdomain.com

May 06, 2019

Phishing and other fraudulent techniques are used by actors to entice victims into sharing their sensitive data. Phishing kits look akin to the original websites and possess the ability to block certain IP addresses of known security companies to prevent timely remediation. Identifying fraudulent sites, products, or activities promotes better security practices.

Gift card fraud is another common activity conducted by online fraudsters. Over the past six months, there have been thousands of gift cards traded across criminal forums, dark web markets, dark web pages, IRC, and Telegram. Approaches to fraud are adapting, for example, a trending Telegram Market called “OL1MP” utilizes a bot to automate the browsing for items – holidays, hotels, taxis, driver’s licenses, and documents.

OL1MP utilises the privacy and encryption of the telegram chat but is an automated marketplace so buyers can chat with a reputable dealer without running the risk of getting scammed.

Use Case 4 – Protecting High Net-Worth Individuals

Another use case is the act of utilising stolen credentials of individuals and accessing the resources of High Net-Worth Individuals to compromise an individual, extort an individual or exfiltrate information from 'secure' environments. Cyber threats are quickly becoming the most prevalent security threats to high net-worth individuals, especially as more information is posted and stored online.

As with each of the use cases 1-3 above, the high net-worth individual is a valuable target for a threat actor to gain information from. Therefore, the need to maintain a constant watch for stolen credentials of personal and corporate accounts is a 'must' within the threat landscape of which these individuals are presented within.

OF EXPOSED CREDENTIALS
FOR YOUR COMPANY
0

EXTERNAL THREAT INTELLIGENCE
Are you monitoring for compromised data that can be used to exploit your business?
□ Yes □ No

DATA BREACH & PRIVACY LAW COMPLIANCE
Do you have a compliant data breach response plan in place?
□ Yes □ No

YOUR INFORMATION IS ALREADY EXPOSED
This information is used to compromise your corporate services such as: Office 365, payroll services, VPNs, remote desktops, banking, VOIP, ERP, CRM, social media access, ID Theft.

WE IDENTIFY
COMPROMISES
Throughout your organization.

WE MONITOR
24/7/365
- Hidden chat rooms
- Private websites
- Peer-to-peer networks
- IRC (Internet relay chat) channels
- Social media platforms
- Black market sites
- 640,000+ botnets

WE REPORT
80,000+
Compromised emails daily.

Certified in Dark Web Monitoring

Conclusion

Dark web monitoring supports the defence-in-depth approach for an organisation and should not be used solely as a standalone product, albeit the value that the service does provide is invaluable, once known.

Other services, such as integrated monitoring solutions, having a robust and tested incident response plan in place and understanding where the risks against your business and/or individuals are likely to originate from are also required to build up the defences to prepare, identify and recover from a Cyber Attack.

Each of the cases studies provided within this document allow the reader to see that the use of the toolkit allows for the service to be adaptable to a range of risk-based opportunities, allowing for the forward intelligence that credentials have been leaked, but also identified. As such, the threat can be addressed, remediated, and monitored.