Dark Web Monitoring
Stay vigilant to know if your footprints are available at Dark Web
# Table of Contents

Abstract 03

What is Dark Web? 03

Top 10 data breach in 2019 & 2020 04

Overview of Dark Web Monitoring 04

Personal Identifiable Information & Personal Health Information is at high risk 05

How is your organization sensitive information compromised and land on the Dark Web? 05

Top 10 Best Dark Web Search Engines in 2020 06

Types of information can be traced online on Dark Web forums 07

How our service helps your footprints to avoid being at Dark Web? 03

Happiest Minds Dark Web Monitoring Workflow 03

How Happiest Minds Dark Web Monitoring can benefit your organization? 09

Happiest Minds Dark Web Monitoring Use Cases 09

Quick fixes to do when you detected your personal or organization information is on the Dark Web? 13

Conclusion 15

Author Bio 15
Abstract

In the modern internet age, personal information shared or stored online is not secure. Many organizations are facing data breach issues and hacks. The hackers are breaking into the security system and loot information such as email accounts, credentials, credit card, customer data, sales report, project information, social security numbers and more. This information is exposed online over dark web sites to make business deals with these data. Data breach are causing financial as well as reputation loss for an organization.

Unfortunately, many organization or people do not realize the urgency of the situation until it personally affects them through data leak, identity theft, or other malicious activity. Hence, dark web monitoring is the need of the hour for every organization to know if they have ever been hacked.

What is Dark Web?

The Dark Web is a secret world of Hackers. Cyber Criminals and terrorists exist on the internet, and one cannot have access to them through traditional search engines or regular browsers. They can only be accessed through specially designed tools like TOR (The Onion Router), Freenet, I2P (Invisible Internet Project) where hackers and buyers meet anonymously and plot deals for various illegal services or information.

Web Surface is divided into three sections of the internet, shown below in the image:

- **World Wide Web**: Public web which is indexed by traditional search engines where content is freely available for search and consumption under surveillance by the government of the given country.
- **Deep Web**: Deep web or hidden web's content is not indexed by traditional search engines and therefore its content is not available for search by the general audience.
- **Dark Web**: The Dark web can publically be accessible through special softwares like TOR, Freenet, I2P and more.

Top 10 data breach in 2019 & 2020

According to risk-based security research newly published report from Selfkey, the Top ten data breach records for the year 2019 and 2020 are listed below. These major data breaches that happened because of various severe security risk/threat that was identified by hackers and compromised which has caused massive data breach around the world and has put all the information of users at high risk.
## Overview of Dark Web Monitoring

The Dark Web, also known as the Dark net is a platform rich in illegal content and services. Provided you have the money to source these scammers and hackers and buy or sell personal or organizational sensitive information such as passwords, credit card numbers, email IDs, names, addresses, business reports and more anonymously.

Dark Web Monitoring based threat intelligence tools can help your organization by notifying you if it finds any information over the Dark Web. This process helps organizations seal all the loopholes in the system that is exposing sensitive data and secures it from any kind of data leakage.

### Data Breach Records in 2019

<table>
<thead>
<tr>
<th>Data Breach Records in 2019</th>
<th>Data Breach Records in 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.6 Million – BlankMediaGames, January 3, 2019</td>
<td>250 Million – Microsoft, January 22, 2020</td>
</tr>
<tr>
<td>108 Million – Various Online Betting Sites, January 23, 2019</td>
<td>At least 10,000 – LabCorp, January 28, 2020</td>
</tr>
<tr>
<td>600 Million – Facebook, March 21, 2019</td>
<td>330,000 – Slickwraps, February 21, 2020</td>
</tr>
<tr>
<td>Unknown – Microsoft Email Services, April 15, 2019</td>
<td>900,000 – Virgin Media, March 5, 2020</td>
</tr>
<tr>
<td>885 million – First American, May 25, 2019</td>
<td>201,162,598 Million – Unknown, March 5, 2020</td>
</tr>
<tr>
<td>11.9 Million – Quest Diagnostics, June 3, 2019</td>
<td>6.9 Million – The Dutch Government, March 11, 2020</td>
</tr>
<tr>
<td>100 Million – Capital One, July 29, 2019</td>
<td>At Least 81.6 Million – Antheus Tecnologia, March 11, 2020</td>
</tr>
<tr>
<td>3 Million – UniCredit, October 28, 2019</td>
<td>29,969 – Norwegian Cruise Line, March 20, 2020</td>
</tr>
<tr>
<td>267 Million – Facebook, December 19, 2019</td>
<td>5.2 Million – Marriott, March 31, 2020</td>
</tr>
</tbody>
</table>
Hacker or cybercriminals use various techniques to compromise sensitive information of an organization. They spend more time gathering information and undertake several scanning processes to collect enough data from strategizing the attacks further and exploiting the vulnerability to collect the needed information and then sell them on the Dark Web.

How sensitive information is compromised and land on the Dark Web?

**Personal Identifiable Information & Personal Health Information is at high risk**

- Credit Card
- Identity Theft
- Chat
- Phone Numbers
- Social Security Services
- Email Addresses
- Social Network
- Health Records
- Driving License

**Phishing Attack**

- The recipient considers this An attacker sends fraudulent email masquerading as a trusted entity to victim to click on malicious link.
- Email coming from trusted source and click on a malicious link.
- Deliver malware that capture sensitive information including passwords, ID and details of credit cards etc.

**Watering Holes Attack**

- Attacker observes the popular sites like social media, corporate internet often visited by a victim and infects those sites with malware.
- Deliver malware to capture visitor’s credentials or sensitive information including passwords, ID etc.
DuckDuckGo, is one of the most commonly used search engines on the Tor network, which is a privacy-focused search engine.

Not Evil is another dark net search engine that allows users to access content hosted inside the Tor network.

Torch is another good dark net search engine, which claims to have indexed more than a million dark web page results.

Pipl search engine has an index of people identity. This search engine provides access to over six billion non-surface web results.

Grams is a dark web search engine built especially for dark net markets.

AHIMA is a free, open source dark net search engine.

Web Attacks
- Cyber Criminals/Hackers scan internet facing organization infra or assets for finding vulnerabilities.
- Exploitation of found security vulnerabilities in order to gain access to the compromised machine.
- Hackers perform lateral movement in the network to capture sensitive information such as credentials.

Malvertising
- Attacker sprinkling malicious code to legitimate-looking ads.
- Deliver malware to capture visitor’s credentials or sensitive information including passwords, ID etc.

Vulnerability Exploitation
- Attacker uses various tools and scripts and run them against an organization infra or a system of a victim
- Perform scan and enumeration and collects vulnerability detail.
- Compromise organization servers and drop backdoor to capture sensitive information etc.

Top 10 Best Dark Web Search Engines in 2020
The Dark Web is the marketplace where breached and compromised data can be sold and bought. The scammers and hackers can anonymously buy or sell personal/organizational sensitive information such as passwords, credit card numbers, names, addresses and more. This activity can only be monitored and reported by Dark Web Monitoring. Happiest Minds Technologies Threat Intelligence Tool can detect your exposure or footprints online and help you protect and prevent your data from being exposed or from credential stuffing risk.
Given a scenario where your organization was a victim to Cyber Crime 93 days ago, where your data was compromised. It took around 28 days for your organization to detect and address this concern. However, the damage was already done, or another damage is still waiting to happen because there was a huge time gap between the breach, detection and response. Happiest Minds Technologies Threat Detection tool will help you monitor the Dark Web and will constantly check for footprints of your organizational information and notify you as and when it appears. This will be a preventive measure to keep your organization from being prey to Cybercrime and will drastically reduce the detection and response time.
Happiest Minds Dark Web Monitoring can help your organization with the following:

01. Reduce the gap between incident, detection and response.
02. 24/7 Dark Web Monitoring for your organization.

03. Information on Dark Web Threat Scoring & Alerts on priority.
04. Identifying exposed credentials.

05. Detailed reports of data breaches.
06. Malware exploit and payload detail.

07. Resource Connect Threat Monitoring.
08. Insights on current threat posture and benchmark.

09. Customer Threat Management.

Happiest Minds Threat Intelligence Tool’s Success Story

Dark Web Monitoring (Threat Intelligence) can provide solutions to the customer in multiple ways. However, it is paramount for the customer to identify the potential Cyber Risk in their environment in order to opt the right threat intelligence solution for their infrastructure. Listing below some used cases describing different risks that organizations face. Happiest Minds Threat Intelligence solution has helped customers counter these threats with optimal accuracy and agility.
**Leaked Credential** – Malicious threat actors are performing phishing, malware attacks, weak or bad password management system are reasons that can cause online credential leakage. These credentials can be used to authenticate the applications/systems in an organization and eventually leads to compromised data.

Our Web Monitoring Service has helped the customer in identifying their leaked credentials on the Dark Web Forum. The Threat Intelligence team can extract these sensitive data from Dark Web through various online sources like Pastebin, hidden blogs and other dark sites. Therefore, providing a detailed report to the customer in order to take necessary actions against such leaked credentials.

**Domain Protection** – Cybercriminals register look-alike domains matching the original domain of a reputed company and create fraudulent websites, email spam, phishing and email scams therefore affecting the company’s brand value and reputation.

Our Dark Web Monitoring service has helped such organization to protect their domain reputation. In the image below, we can see how the Threat Intelligence team has captured registered look-alike domains that mimics the original reputed domain.
**Data Leakage** – One of the major challenges for every organization is to keep their data safe and secure. Data Leakage has been the most significant threat to the organization as it enables cybercriminals to access sensitive data on the internal system. Continuous cyber-attacks from cybercriminals for phishing, exploiting vulnerabilities, theft of company’s employee credentials, weak/default passwords, accidentally emailing confidential information or publishing the same online, malware attack and more result in data leakage.

Our Threat Intelligence team keeps an eye on the sensitive information of our customer’s Project Reports, Sales Reports, Customer, Data Business Reports and Business partner details or any other sensitive records if found on the Dark Web.

**Mitigating cyber risk with better prioritizing CVE Patching** – Security patches helps in addressing vulnerabilities in the software that might be used by cyber criminals to exploit and gain access to the system, device, and existing data on them. Now an organization must decide on which patch should be prioritized and applied to their infrastructure. The Threat Intelligence tool that not only helps in monitoring the dark web for respective exploits available, can also support your organization in prioritizing CVE patches based on your infrastructure needs and environment. As part of the activity, we provide a complete end to end information about respective CVE IDs related to a vulnerability.

Happiest Minds Threat Intelligence tools have helped in defending against the probable damage from such unknown threat or exploit it to their customer. One of the latest released security bug/vulnerability was identified running in the customer environment over a respective server, and our CVE Report has helped customer in address and fixing the vulnerability on time before it could have been exploited.
Contextualize IOC Feeds – Organization security also depends upon how good threat feeds are available at the defensive control measures in order to identify network breach, threats or malware infection. In simple term, it can be said that unless an organization has a good relevant threat feeds, it’s difficult to create a defensive shield around an infra from an unknown threat.

Our Threat Intelligence tool (Dark Web Monitoring) with the above features is rich in contextualizing IOC feeds and helps in scanning the footprints in the customer environment to check if any malicious actors exist and quickly identifies and create alerts for actions. A snippet is provided below where Threat Intelligence tool has helped in collecting IOCs from various sources for a ransomware case- “MAZE RANSOMWARE”. It is used for scanning logs collected from customer infra for checking if footprints exist for the same threat in the customer environment.
If you discover that your personal or organization information is on the Dark Web by using a threat intelligence monitoring tool, then you can take following preventive measures:

Quick fixes to fight leaked data on the Dark Web

Best Practice when found your personal information on the Dark Web Forum

01 Change your password immediately for a personal account
02 Keep a watch over your accounts

03 Inform your banks, credit card companies, and other financial services providers
04 Get a copy and monitor your credit/debit card reports

05 Order your credit statements
06 Freeze your credit/debit cards
Best Practice when found your organization information on the Dark Web Forum

Change your password immediately for the official account

Please ensure your official laptop or machine has file encryption technique in place to use

Contact your organization IT Support Team and notify them about this alert or notification

Request initiate to perform full system scan in your system for ensuring the machine is malware free

Please ensure that regular back up is being taken every week to avoid data loss & recover the issue

Company provided online cloud services should have file encryption and authorized repository access so that only authorized user can access

Cloud Security Assessment should be done by the organization periodically to ensure the safety of the employees or organization data

The organization should keep a watch over data exfiltration to avoid any data leakage

Origination should disable USB/HDD plug-n-play function for their employees, which can infect the official machine with unknown threat or malware.

Across the organization, all employees should be educated well that not to click on any an unknown or unsolicited email from unknown sender

Password enforcement policy with a combination of [A-Z], [a-z], [0-9] & […@#$%].

Avoid generic account uses

IT Support team should encourage good password management policy
Conclusion

Data sources on the dark web are panoptic and ever changing incessantly which poses a cyber-security risk to an organization over internet. Our research demonstrates that cybercriminals trade organization information online and make money out of it. To counter this, we require an innovative technology-based tool to monitor the Dark Web landscape and detect the data breach right in time so that appropriate actions can be taken. This tool reduces the amount of time taken in detection and breach. Dark web monitoring is a best practice to safeguard customer, company, key executives, employees’ information/data securely from being exploited on the Dark Web.

Author Bio

Vikas Kumar is a techno-savvy profession with 8.5 years of experience in Security Operation Center (SOC), Cyber Forensics, Web Application and Network vulnerability management also certified with CEH, ECSA, CHFI, ACISE, ITILv3 certifications. He is currently part of Infrastructure Management and Security Services business unit of Happiest Minds Technology Pvt. Ltd. He is primarily responsible for uncovering threats, vulnerabilities and security risks as Information Security Specialist focusing on threat intelligence and investigation of advanced cyber-attacks. He is also involved and contributing in designing new security solutions. Vikas is an active member of EC-Council organization.