

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

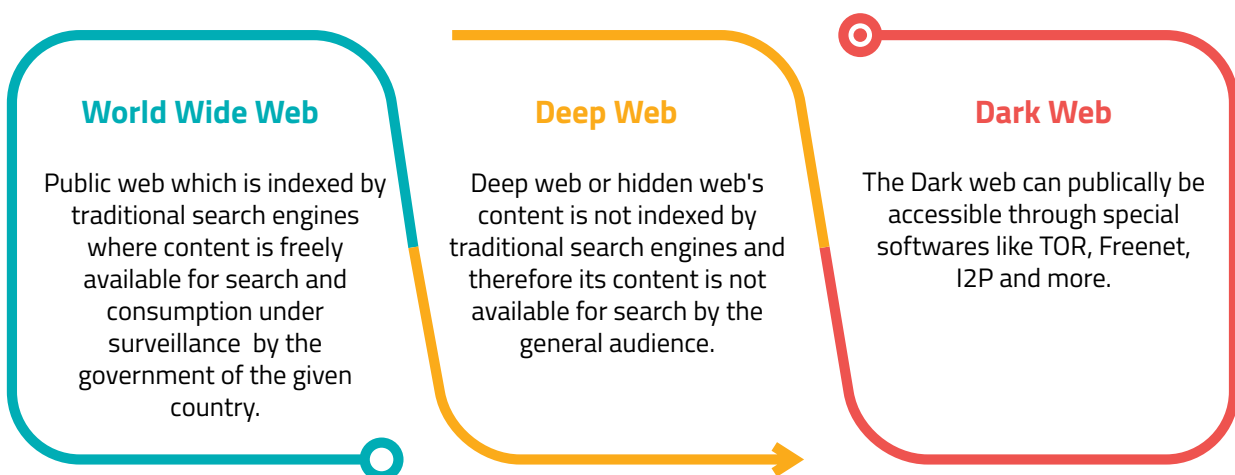
In the modern internet age, personal information shared or stored online is not secure. Many organizations are facing data breach issues and hacks. The hackers are breaking into the security system and loot information such as email accounts, credentials, credit card, customer data, sales report, project 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:



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.

Data Breach Records in 2019	Data Breach Records in 2020
7.6 Million – BlankMediaGames, January 3, 2019	250 Million – Microsoft, January 22, 2020
108 Million – Various Online Betting Sites, January 23, 2019	At least 10,000 – LabCorp, January 28, 2020
6 Million – Coffee Meets Bagel, February 14, 2019	Unknown – Defence Information Systems Agency, February 11, 2020
600 Million – Facebook, March 21, 2019	330,000 – Slickwraps, February 21, 2020
Unknown – Microsoft Email Services, April 15, 2019	900,000 – Virgin Media, March 5, 2020
885 million – First American, May 25, 2019	201,162,598 Million – Unknown, March 5, 2020
11.9 Million – Quest Diagnostics, June 3, 2019	6.9 Million – The Dutch Government, March 11, 2020
100 Million – Capital One, July 29, 2019	At Least 81.6 Million – Antheus Tecnologia, March 11, 2020
3 Million – UniCredit, October 28, 2019	29,969 – Norwegian Cruise Line, March 20, 2020
267 Million – Facebook, December 19, 2019	5.2 Million – Marriott, March 31, 2020

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.

Personal Identifiable Information & Personal Health Information is at high risk



Credit Card



Identity Theft



Chat



Phone Numbers



Social Security Services



Email Adresses



Social Network



Health Records



Driving License

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

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.

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

Infests those sites with malware.

Deliver malware to capture visitor's credentials or sensitive information including passwords, ID etc.

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

DuckDuckGo

DuckDuckGo, is one of the most commonly used search engines on the Tor network, which is a privacy-focused search engine.

Not Evil

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

Torch

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

Pipl

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

Grams

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

AHMA

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

Candle

Candle is like Google of the dark web except that it does not display ads, and it does not have as many indexed sites.

Abiko

Abiko is another simple dark net search engine that displays search results for only onion websites.

Haystak

Haystak another search engine with over 1.5 billion pages indexed with about 260,000 onion websites, including historical onions.

Onionland Search

Onionland is a popular search engine on the dark web which indexes only onion sites, and it has other numerous features.

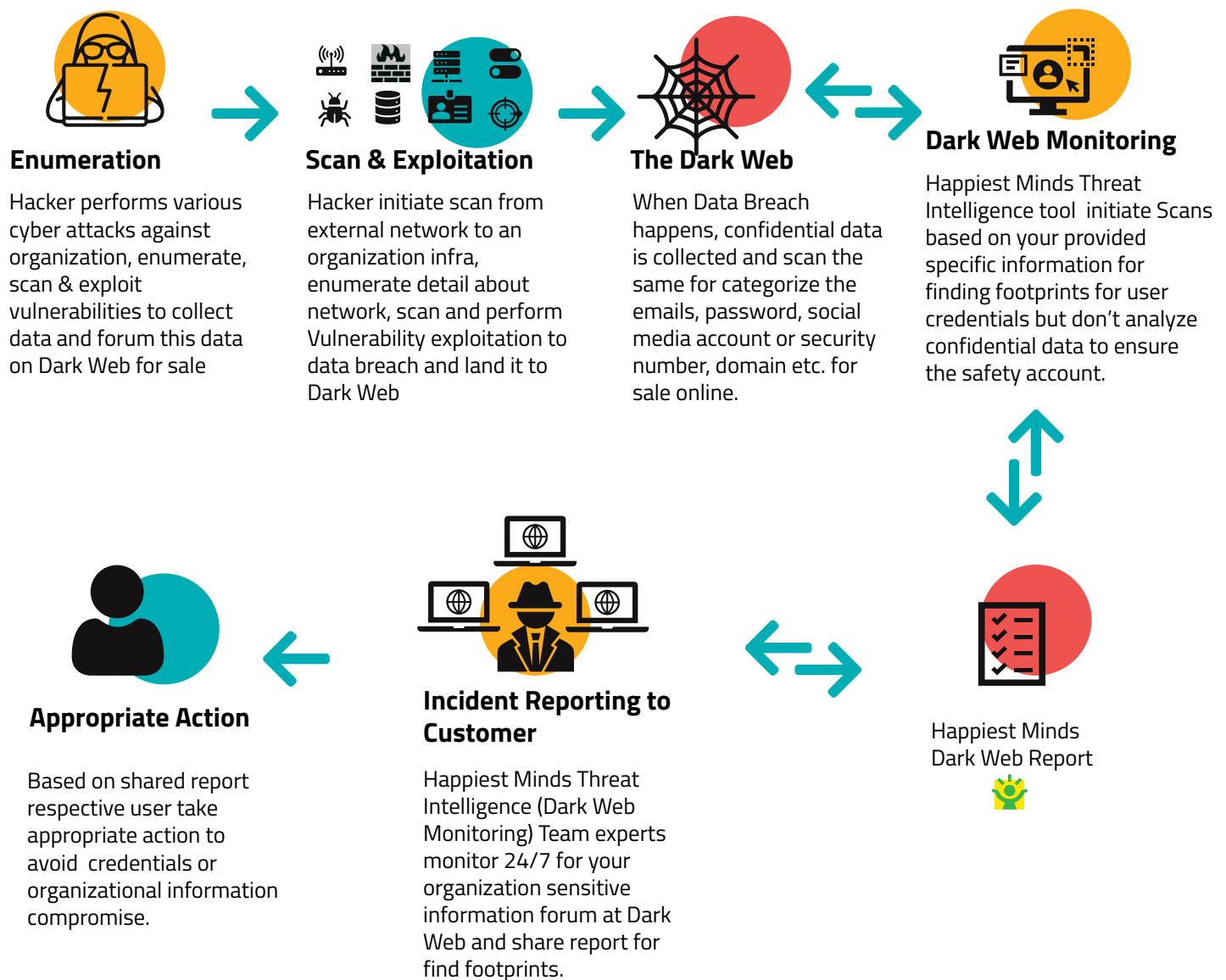
Types of information traced online on Dark Web forums

Personal Infromation	Organization Records	Social Confidential Records
Credit/Debit Cards	Company data	Court Records
Email Address	Bulletin Boards	Dark Web Internet Surveillance
Health Records	Vulnerability Detail	Financial Account
Passport Number	Malware Samples	Identity Validation
Phone Numbers	Peer-To-Peer Sharing Networks	National Change of Address
Membership Cards	Web Pages, Web Services, Servers, And File Transmissions	Non-Credit Loans
Social Security Number	Exploits & Payload	Sex Offender Registry
Social Media Feeds	Similar look- alike domains	Social Network & Security Number Trace

Happiest Minds Threat Intelligence tool against the Dark Web

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**.

Threat Intelligence tool Dark Web Monitoring Workflow



Why Happiest Minds Threat Intelligence tool?

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 organiza-tions 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.

CREDENTIALS

happiest minds
The Mindful IT Company
Born Digital . Born Agile

https://twitter.com/

Mark as incident Mark as favorite Mark as read Mark as unread Labels Delete threat Follow Up Comments · 0

RATING: ☆☆☆☆☆

DOMAIN: [REDACTED].org

LABELS: [REDACTED] Clear Password Hacktivism Credentials

UPLOADED AT: 2/3/2017, 3:55 AM

LEAK ORIGIN: https://twitter.com/

LEAK FOUND AT: https://mega.nz/#pkJI2QQRI_nWYeIZCF4LGOh2k2_0Y9X9ti3YPz4_[REDACTED]dpKws

LEAK DATE: 12/20/2016, 5:30 AM

CREATED AT: 4/29/2020, 3:31 PM

CHECKED AT: 4/29/2020, 3:31 PM

CHANGED AT: 4/29/2020, 3:31 PM

USERNAME	EMAIL	PASSWORD/HASH	DOMAIN/URL
jl[REDACTED].org	jl[REDACTED].org	[REDACTED]	https://twitter.com/

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.

DOMAIN PROTECTION

as[REDACTED]co.com

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Back to list

Mark as incident Mark as favorite Mark as read Mark as unread Labels Delete threat Follow Up Comments · 0

RATING: ☆☆☆☆☆

TITLE: a[REDACTED]co.com

URL: http://a[REDACTED]co.com

LANGUAGE: English

TRANSFORM NAME: Cybersquatting

LABELS: CyberSquatting Domain

STATUS: NEGATIVE

SEARCH WORDS: [REDACTED].mg

CONTENT TYPE: text/html

CREATED AT: 4/13/2020, 10:09 PM

CHECKED AT: 4/13/2020, 10:09 PM

UPDATED AT: 4/13/2020, 10:09 PM

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.

DATA LEAKAGE

happiest minds
The Mindful IT Company
Born Digital . Born Agile

Back to list

Mark as incident Mark as favorite Mark as read Mark as unread Labels Delete threat Follow Up Comments · 0

RATING: ☆☆☆☆☆

TITLE: [REDACTED]

URL: https://www.[REDACTED]

COUNTRY: US

LANGUAGE: English

LABELS: NoSourceCode Public TopScribdDocsSearch

STATUS: POSITIVE

TRANSFORM NAME: Top [REDACTED] Search

SEARCH WORDS: "hometown"

CONTENT TYPE: text/html; charset=utf-8

DOMAIN TYPE: Social Network

CREATED AT: 4/19/2020, 6:20 PM

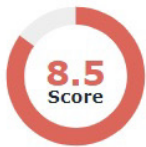
CHECKED AT: 4/19/2020, 6:20 PM

UPDATED AT: 4/19/2020, 6:20 PM

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.

CVE-2020-0796

[Back to list](#)

NAME	Born Digital . Born Agile	CVE-2020-0796
PUBLICATION DATE	12/03/2020	
MENTIONS	1170	>

Common Vulnerability Scoring System

CVSS V2 (Score: 7.5/10) >

[# Description](#)
[Malware \(10\)](#)
[Threat Actors \(0\)](#)
[Campaigns \(0\)](#)
[Tools \(0\)](#)
[Attack Patterns \(53\)](#)
[Signatures \(1\)](#)
[Mentions \(1170\)](#)

Description

A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'.

Affected Platforms

TITLE	CPE
Windows 10 Version 1903 for 32-bit Systems	cpe:2.3:o:microsoft:windows_10:1903:*:*:*:*x86.*
Windows 10 Version 1903 for ARM64-based Systems	cpe:2.3:o:microsoft:windows_10:1903:*:*:*:*arm64.*
Windows 10 Version 1903 for x64-based Systems	cpe:2.3:o:microsoft:windows_10:1903:*:*:*:*x64.*
Windows 10 Version 1909 for 32-bit Systems	cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*x86.*

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.

DATA LEAKAGE

[Back to list](#)
[Mark as incident](#)
[Mark as favorite](#)
[Mark as read](#)
[Mark as unread](#)
[Labels](#)
[Delete threat](#)
[Follow Up](#)
[Comments - 0](#)

★ **RATING:** ☆☆☆☆☆

📄 **TITLE:** [REDACTED]

🔗 **URL:** [https://www.s\[REDACTED\].com](https://www.s[REDACTED].com)

🌐 **COUNTRY:** US

🗺️ **LANGUAGE:** English

🏷️ **LABELS:** NoSourceCode Public TopScribdDocsSearch

📌 **STATUS:** POSITIVE

🔧 **TRANSFORM NAME:** Top [REDACTED] Search

🔍 **SEARCH WORDS:** "hometown"

📄 **CONTENT TYPE:** text/html;charset=utf-8

🌐 **DOMAIN TYPE:** Social Network


🕒 **CREATED AT:** 4/19/2020, 6:20 PM

🕒 **CHECKED AT:** 4/19/2020, 6:20 PM

🕒 **UPDATED AT:** 4/19/2020, 6:20 PM

MALWARE HUNTING

Threat Context

 **happiest minds**
The Mindful IT Company
Born Digital . Born Agile

Q Syntax

Malware Hunting showing: 95 results

FIRSTSEEN	SHA256	SCORE	SOURCES	TYPE	STATUS	#PROP	NET	C&C	URLS	FILE TYPE
10/05/2020	7656d6519...	45	virustotalAPI	MAZE	✓	0	✗	✗	✗	PE
04/05/2020	877f8c8591...	42	virustotalAPI	MAZE	✓	0	✗	✗	✗	PE.DLL
04/05/2020	bde2e35fa0...	68	virustotalAPI	MAZE	✓	0	✗	✗	✗	PE.DLL
04/05/2020	b6e2c213d0...	42	Adminusavir...	MAZE	✓	0	✓	✗	✗	PE.DLL
04/05/2020	71085facb3...	41	virustotalAPI	MAZE	✓	0	✓	✗	✗	PE.DLL
03/05/2020	b8a8895dfa...	63	virustotalAPI	MAZE	✓	0	✗	✗	✗	PE.DLL
28/04/2020	81145757f3...	84	CTA_TELE...	MAZE	✓	0	✓	✗	✗	PE
27/04/2020	543f72aaf9...	75	virustotalAPI	MAZE	✓	0	✓	✗	✗	PE.DLL
24/04/2020	0d8b74e1e...	44	virustotalAP...	MAZE	✓	0	✗	✗	✗	PE.DLL
24/04/2020	557f62d5df...	77	virustotalAPI	MAZE	✓	0	✗	✗	✗	PE.DLL
23/04/2020	b3473d205...	55	virustotalAPI	MAZE	✓	0	✓	✗	✗	PE

Quick fixes to fight leaked data on the Dark Web

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:

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

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

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

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

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

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

IT Support team should encourage good password management policy

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

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

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

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

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

Avoid generic account uses

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.

Business Contact business@happiestminds.com

About Happiest Minds Technologies

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, Blockchain, Automation including RPA, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

A Great Place to Work-Certified™ company, Happiest Minds is headquartered in Bangalore, India with operations in the U.S., UK, The Netherlands, Australia and Middle East.



www.happiestminds.com