

# Dark Web Scanning



Understanding  
the *Why* and the *How*

# Contents



## **Introduction:**

The Need for Dark Web Scanning

# 1

## **Chapter 1:**

What You and Your Employees Don't Know Can Hurt You

# 2

## **Chapter 2:**

What to Do When Your Credentials Have Been Exposed

# 3

## **Chapter 3:**

Using a Dark Web Scan as an Early Warning Tool



## **Summary:**

Comprehensive Cybersecurity Resources

# The Need for Dark Web Scanning



## *Dark Web Monitoring*

is emerging as a crucial element to a solid, advanced cybersecurity strategy.

Unfortunately, many organizations are not aware of the dark web and its dangers. Others don't take it seriously, thinking it can't possibly be a threat to their organization. Don't let your business fall victim!

Dark web monitoring is another arrow that you should add to your cybersecurity quiver.

# What You and Your Employees Don't Know Can Hurt You

Today's hackers are working smarter, not harder, and they have become increasingly adept at lucrative opportunities tied to the hostage of business email. Yet many companies aren't prioritizing security as an essential element to their business success. Take, for example, employee training. Many businesses don't realize their employees are one of their most significant security risks. You've probably heard the stories of cyber criminals dumping thumb drives loaded with malicious hacker code in employee parking lots, waiting for someone to pick one up and plug it into a work laptop. Pretty clever, right? Unfortunately, research studies have found that more than 60% of people who find a thumb drive will do just that— potentially handing over network access to an enterprising hacker.


Research finds that most breaches are not initially detected and may not be discovered until several months after the

initial attack. According to IBM's Cost of a Data Breach Report 2020, the average time to identify and contain a data breach is 280 days (approximately nine months). Often, breaches are only detected after it is discovered that compromised, sensitive information has been released or is for sale on the dark web.

Does your organization have compromised information available for sale to hackers?



# Do You Have Employee Credentials on the **Dark Web**?

A graphic of an iceberg floating in water. The tip of the iceberg is above the water line, while the much larger base is submerged below. The water is a light blue color, and the sky above is a darker blue. The iceberg is white and light blue.

When conducting a risk assessment for identification of unknown security vulnerabilities and defensive gaps, a dark web scan can help further identify risk exposure and act as an early warning to potential dark web risks.

A dark web scan can also protect employee credentials. The scan can uncover any exposed employee credentials and allows you to set up ongoing monitoring so you will be notified of any future credential leaks.



## There's No Better Time to Find Out

Many organizations are shocked and surprised when they see their employees' access information available for sale on the dark web. Whether you have a large enterprise or a small to mid-sized business, be sure you aren't a target!

# What to Do When Your Credentials Have Been Exposed

Running a dark web scan against an email domain can provide illuminating results. For example, one organization's email domain scan uncovered 30 compromised emails, including the business owner's bank account login credentials. Keep in mind, this is just one example. There have been instances where several hundred or even a few thousand compromised emails have been found.

## Client Report

### A. Risk Summary

### B. Assessments

- Dark Web Assessment
- Anti-Spam Assessment
- Vulnerability Assessment
- Endpoint Assessment
- Patch Assessment
- User Risk Assessment
- IT Infrastructure Assessment

## Partner Report

### C. Details

**A.**

#### Executive Risk Summary

- 1 out of 1 domains with inappropriate endpoint configurations
- 5 user accounts exposed on dark web for more than 30 days
- 66 out of 68 endpoints missing DNS protection
- 1 out of 68 endpoints with remote access enabled
- 66 out of 68 endpoints missing advanced protection
- 2 out of 23 endpoints with possible assessment policy violations
- 4 out of 23 accounts never logged in
- 4 out of 14 accounts with last time space utilized over 90% within 10 other accounts with last time utilized over 70%

13 out of 23 accounts have not logged in within the last 90 days

66 out of 68 endpoints with vulnerable banking policy configurations
- 1 out of 14 accounts having expired the Operating System
- 27 out of 74 accounts with last time space utilized between 20-60%

4 out of 23 accounts have not logged in within the last 30 days

23 out of 74 accounts with last time space utilized between 20-60%

**B.**

05 Anti-Spam Assessment

06 Vulnerability Assessment

08 Endpoint Assessment

10 Patch Assessment

11 User Risk Assessment

12 IT Infrastructure Assessment

#### Security Assessment

This security assessment report provides specific weaknesses and deficiencies in an endpoint within or created by the system.

Such weaknesses and deficiencies are not vulnerabilities if required by a threat actor generator during the security control assessment information that facilitates a threat structure approach to mitigating risks in an organizational profile.

#### Risk Dashboard

The dashboard lists threat categories from multiple assessments performed on endpoints with their associated risk. A high level overview of the health and a summary.

This report details the areas likely to show issues. In addition to the overall Consider the report and provide separate requests areas of assessment.

#### Vulnerability Assessment

A vulnerability assessment is the process of defining, identifying and prioritizing vulnerabilities in computer network infrastructures to provide the organization with all the necessary knowledge, awareness and risk taking capabilities to the business in an environment and next steps.

**Risk Detected: High Risk Score**

**Critical Security Vulnerability**  
10

**High Security Vulnerability**  
23

**Medium Security Vulnerability**  
50

**Low Security Vulnerability**  
65

#### Patch Assessment

Patch assessments in the process that help acquire, test and install multiple patches on a computer, operating systems, or any related or existing hardware and software for IT environment from vulnerabilities and exploits.

**Apply Patch to Stay Protected**

**Critical** Apply patches within 30 days of release

**High** Apply patches within 30-60 days

**Medium** Apply patches within 60-90 days

**Low** Apply patches within 90-180 days

#### Top 3 Missing Patches

Patch Details	Existing Count	Server Count	Risk Score
Security Update for Windows Server 2016	10	45	CRITICAL
Security Update for Windows 10 Pro x64	34	34	HIGH
Security Update for Windows 7 Full Edition (x64)	56	2	HIGH

**C.**

## Contents

- Anti-Spam Configuration Details
- Dark Web Exposure Details
- Endpoint Health Details
- Users with Possible Policy Violations Details
- Users Login Details
- Endpoint Hygiene/Asset Details
- Open Vulnerability Details
- Missing Patch Details

#### Open Vulnerability Details

CVE ID	Vulnerability Name/Description	CVSS Score (Risk Level)	Impacted Endpoints	Deprecated?
CVE-2015-3762	observed on before 1.7.7 allows login by unauthorized accounts due to a bug in the REST api	8.8 (HIGH)	SERVER1, DESKTOP2	-
CVE-2015-7486	Cross-site scripting (XSS) vulnerability in the backend in Clear-Exchange [URL redacted] 7.2.4 before 7.2.4.2017 and 7.4 before 7.4.0 (x64) allows remote attackers to inject arbitrary web script or HTML via the body of an email. NOTE: the vulnerability was split from CVE-2015-0242 (Denial of Service) different sets of requests.	6.1 (MEDIUM)	SERVER1, DESKTOP1, DESKTOP7	-
CVE-2014-0104	in Group objects before 6.0 SP1 does not verify service SID, certificates in the binary, client, and so forth which can potentially allow for man-in-the-middle attacks to spoof SIDs, servers via arbitrary SIDs.	6.9 (MEDIUM)	DESKTOP2, DESKTOP3, DESKTOP7	-
CVE-2013-3843	The MS00 patch (MS00-01) before 6.0 SP1 for SharePoint allows remote attackers to execute arbitrary code via a stored log.	7.8 (HIGH)	DESKTOP7	Yes

#### Endpoint Health Details

Machine Name	IP Address	Machine Type	Operating System	Firewall Protection	Advanced Protection	DNS Protection	Remote Desktop Enabled	Open Vulnerability
SERVER1	192.168.16.2	Server	Microsoft Windows Server 2016 R2 Standard	✓	✓	✓	✓	0
DESKTOP1	192.168.2.8	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	10
DESKTOP2	192.168.11.166	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	23
DESKTOP3	192.168.16.8	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	50
DESKTOP4	192.168.16.246	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	65
DESKTOP5	192.168.2.106	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	0
DESKTOP6	192.168.254.10	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	0
DESKTOP7	192.168.2.8	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	0

#### Users with Possible Policy Violations Details

User Name	User Role	Last Login Timestamp	Password Required	Password Changed	Password Complexly Enabled	Password Expiring in Less Than 90 Days	Remote Desktop Access Enabled
SERVER1user1	Administrative	N/A	✓	✓	✓	✓	✓
SERVER1user2	Client	04/07/2020 11:45 PM	✓	✓	✓	✓	✓
DESKTOP7user2	User	04/06/2020 7:53:48 PM	✓	✓	✓	✓	✓
DESKTOP7user3	Administrative	N/A	✓	✓	✓	✓	✓
SERVER1user3	Administrative	04/06/2020 10:14 PM	✓	✓	✓	✓	✓
DESKTOP4user5	Administrative	03/17/2020 10:31 AM	✓	✓	✓	✓	✓
SERVER1user4	Administrative	106/20/2016 4:16:16 PM	✓	✓	✓	✓	✓

# Brush up on Password Best Practices

If your credentials have been exposed publicly, you can never use that password again. Once that password is part of a public list, especially one that is associated with your email address, you can be sure it will be used in a future attack. The risk is too great to even consider using it again, and any other account that uses the same password should be immediately changed as well. Similar passwords used with other accounts should be changed, too.

Cybercriminals will use your password in an attempt to gain access to other accounts like banking and social media. This is why

business email addresses should NOT be used for non-business-related activities, and separate passwords should be used for each site or application you use. The results of a dark web scan will show if any of your employees may have used their business email for non-business reasons and had their credentials compromised, bringing unnecessary risk to your organization.

If you identify any of your users' credentials for sale on the dark web, take the necessary steps to remediate the situation and prioritize strengthening your security posture for the future. That includes training your users on their role in defense of the organization. While a clear dark web scan may provide peace of mind today, be sure not to develop a false sense of security. Instead, use the assessment to identify other potential vulnerabilities that require resolution.



# Using a Dark Web Scan as an Early Warning Tool

Think of a dark web scan as a regular checkup with your doctor. You may feel fine, but medical tests could uncover underlying problems. A dark web scan is just like the routine tests your doctor orders. It's one more way to understand the strength of your current cyber defense. Additional tests, like a vulnerability scan, can further identify specific areas of weakness and recommend appropriate remediation.





# Comprehensive Cybersecurity Resources



All it takes is one end user clicking on the wrong link to undo all your hard work.

We have solutions to strengthen your security defense, including employee training, endpoint protection, vulnerability assessments and a fully staffed SOC. Contact us to learn more!



**(800) 669-8513**