

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

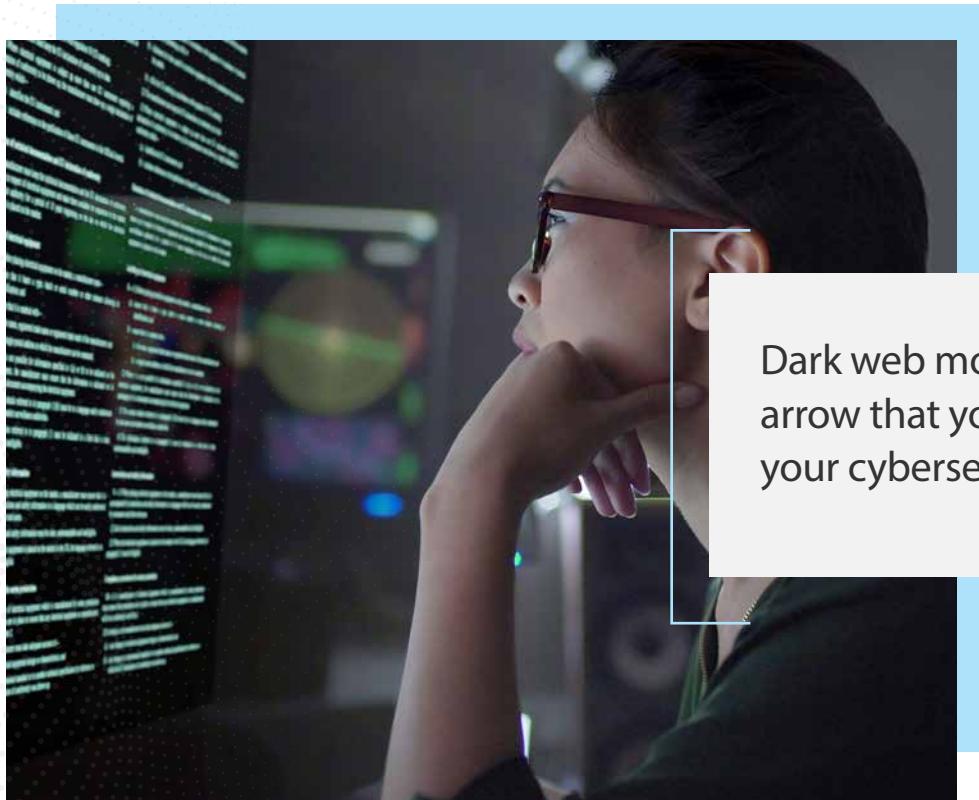


Summary:
Comprehensive
Cybersecurity
Resources



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?

280 days

The average time it takes to identify and contain a data breach is 280 days (approximately nine months).

Do You Have Employee Credentials on the Dark Web?

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



A

Executive Risk Summary

13 out of 23 domain(s) have not logged in within the last 90 days
68 out of 88 endpoint(s) with inadquate backup policy configurations
1 out of 64 endpoint(s) running end-of-life Operating System
4 out of 23 user(s) never logoff in
4 out of 10 endpoint(s) with remote access enabled
68 out of 88 endpoint(s) with basic AV protection
37 out of 74 endpoint(s) with hard drive space utilization between 25-50%



B

Assessments

05 Anti-Spam Assessment
06 Vulnerability Assessment
08 Endpoint Assessment
10 Patch Assessment
11 User Risk Assessment
12 IT Infrastructure Assessment



C

Risk Dashboard

Risk Detected: High Risk Score

10 Critical Severity Vulnerability
23 High Severity Vulnerability
50 Medium Severity Vulnerability
65 Low Severity Vulnerability

The ClientReport Risk Dashboard provides a summary assessment performed on your system. Such weaknesses and deficiencies are potential security risks if exploited by a threat agent. This report highlights the most critical vulnerabilities and important information that facilitates a more structured approach to mitigating risks in your organizational processes.

Security Assessment

This security assessment report provides specific weaknesses and deficiencies in the security of your organization's IT environment. Such weaknesses and deficiencies are potential security risks if exploited by a threat agent. This report highlights the most critical vulnerabilities and important information that facilitates a more structured approach to mitigating risks in your organizational processes.

Vulnerability Assessment

A vulnerability assessment is the process of detecting, classifying and prioritizing vulnerabilities in computing systems and networks to protect the organization doing business online. It helps to identify and mitigate the threats to the environment and need to patch them.

Patch Assessment

Patch assessment is the process that helps organizations test and evaluate the effectiveness of their existing patching system to be updated on existing patches and safeguards the IT environment from vulnerabilities and exploits.

Apply Patch to Stay Protected

Critical	High
Apply patches within 30-days of release	Apply patches within 30 - 60 days
Medium	Low
Apply patches within 60 - 90 days	Apply patches within 180 days

Risk Detected!

- 7 ANOMALY REPORTED
- 12 VULNERABILITIES IN EXPOSURE
- 12 SECURITY BREACHES IN A VULNERABILITY
- 12 SECURITY BREACHES IN A VULNERABILITY
- 12 SECURITY BREACHES IN A VULNERABILITY

Top 3 Missing Patches

Patch Details	Desktop Count	Server Count	Risk Score
Security Update for Windows Server 2008 R2 and later editions (MS12-014)	10	40	HIGH
Security Update for Windows 7 and later editions (MS12-014)	34	34	HIGH
Security Update for Windows 7 and later editions (MS12-014)	36	2	HIGH

Please refer to the detailed report for more details.

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	CVE Score (Base Score)	Impacted Endpoints	Deprecated?
CVE-2010-3782	cit-server before 1.7.7 allows remote code execution via a bug in the REST api	8.8 (HIGH)	SERV01, DESKTOP2	-
CVE-2013-7466	Cross-site scripting (XSS) vulnerability in Open-Xchange (OX) Appliance 7.2.x and 7.4.0-0.0 allows remote attackers to inject arbitrary HTML and script via a crafted URL, via the body of an email message. This issue is different from the one listed from CVE-2013-6424 because it concerns a different component.	5.1 (MEDIUM)	SERV01, DESKTOP1, DESKTOP2	-
CVE-2014-0154	In-tel-agency before 4.0.17 does not verify service SSL certificates in certain situations. This issue can potentially allow for man-in-the-middle attacks on services that accept SSL/TLS, services via arbitrary SSL/TLS, and services via self-signed SSL/TLS.	5.8 (MEDIUM)	DESKTOP1, DESKTOP2, DESKTOP3	-
CVE-2013-3945	The MS13_012 update (MS13-012) before 4.37 for Internet Explorer removes remote code via a Microsoft bug.	2.8 (HIGH)	DESKTOP7	Yes

Could not be determined/analyzed/patched

Endpoint Health Details

Machine Name	IP Address	Management Type	Operating System	Firewall Protection	Advanced Protection	DNS Protection	Remote Desktop Enabled	Open Vulnerabilities
SERVERT1	192.168.2.1	Server	Microsoft Windows Server 2008 R2 Standard Edition	✓	✗	✗	✗	75
DESKTOP1	192.168.2.8	Desktop	Microsoft Windows 10 Pro	✓	✗	✗	✓	87
DESKTOP2	192.168.11.180	Desktop	Microsoft Windows 10 Pro	✓	✗	✗	✓	71
DESKTOP3	192.168.11.181	Desktop	Microsoft Windows 10 Pro	✓	✗	✗	✓	71
DESKTOP4	192.168.16.248	Desktop	Microsoft Windows 10 Pro	✓	✗	✗	✓	0
DESKTOP5	192.168.20.200	Desktop	Microsoft Windows 10 Pro	✓	✗	✗	✓	45
DESKTOP6	192.168.20.201	Desktop	Microsoft Windows 10 Pro	✓	✗	✗	✓	45
DESKTOP7	192.168.2.6	Desktop	Microsoft Windows 10 Pro	✓	✗	✗	✓	0

Could not be determined/analyzed/patched

Users with Possible Policy Violations Details

User Name	User Role	Last Login Timestamp	Password Required	Password Changeable	Password Complexity Enabled	Password Expiring In Less Than 90 Days	Remote Desktop Access Enabled
SEVERTUser1	Administrator	04/07/2023 9:16:45 PM	✓	✓	✗	✗	✓
DESKTOPUser2	User	04/06/2023 7:53:48 PM	✓	✓	✗	✗	✓
DESKTOPUser3	Administrator	N/A	✓	✓	✗	✗	✓
DESKTOPUser4	Administrator	04/08/2023 8:57:14 AM	✓	✓	✗	✗	✓
DESKTOPUser5	Administrator	03/17/2023 2:35:51 AM	✓	✓	✗	✗	✓
SERVERTUser6	Administrator	06/12/2018 4:18:15 PM	✓	✓	✗	✗	✓

6

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!





milner.com

800.875.5042

Follow us



Blog



LinkedIn



Facebook



Twitter