

Dark Web Scanning: Understanding the Why and the How



Contents



Introduction:
The Need for Dark
Web Scanning



Chapter 1:
What You and
Your Employees
Don't Know Can
Hurt You



Chapter 2:
What to Do When
Your Credentials
Have Been
Exposed



Chapter 3:
Using a Dark Web
Scan as an Early
Warning Tool



Summary:
Comprehensive
Cybersecurity
Resources



Gavin Hitchmough

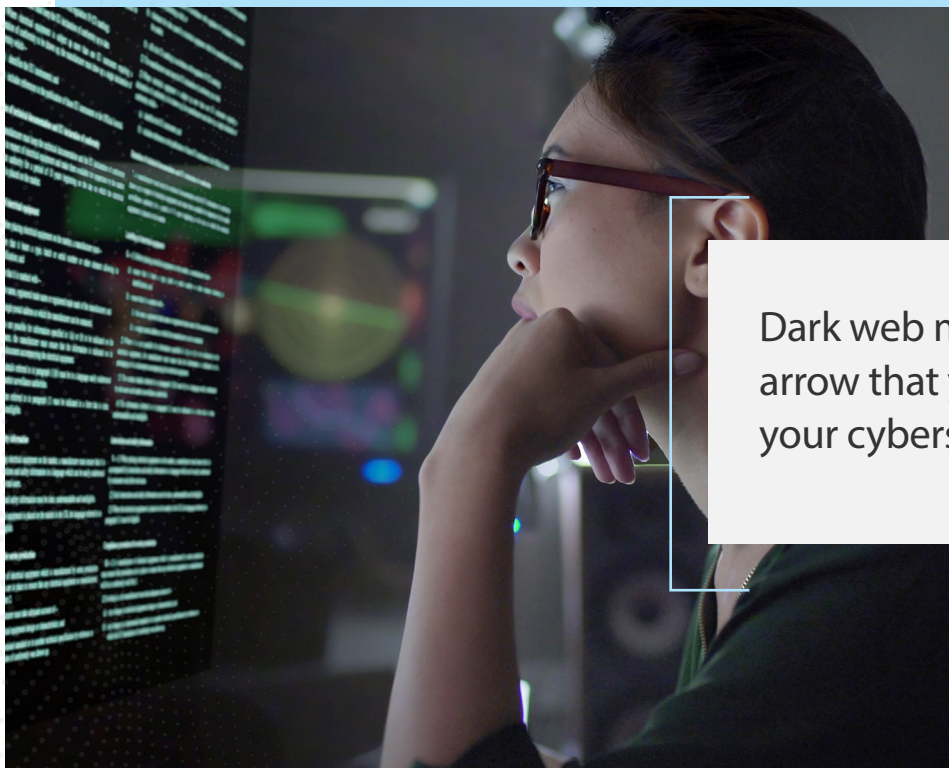
Red Circles ITS Limited, Denby House Business
Center, Taylor Lane,
Loscoe, Derbyshire DE75 7AB
0330 135 9478

<https://www.redcircles-its.com>



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

Partner Report

C. Details

A

Executive Risk Summary

- 1 out of 18 endpoints with misconfigurations with agent configurations
- 7 user accounts exposed on dark web for more than 90 days
- 88 out of 88 endpoints missing DNS protection
- 1 out of 88 endpoints with remote access enabled
- 88 out of 88 endpoints missing advanced protection
- 39 out of 88 endpoints with password protection policy violations
- 4 out of 88 endpoints never updated
- 4 out of 74 assets with hard drive space utilized over 90% while 10 other assets with hard drive space utilized below 70%

B

Security Assessment

The security assessment report provides specific weaknesses and deficiencies in IT environment either or checked by the above. Such weaknesses and deficiencies are put into categories as required by threat and generalised during the security control assessment. Information that facilitates a risk structured approach to mitigating risks in IT environment.

Risk Dashboard

RISK

10 Critical Severity Vulnerability

23 High Severity Vulnerability

50 Medium Severity Vulnerability

65 Low Severity Vulnerability

Patch Assessment

Patch assessment is the process that helps acquire, test and install multiple patches on a computer, operating system or the network or existing patches and safeguards the 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 180 days

Top 3 Missing Patches

Patch Details	Missing Count	Server Count	Risk Score
Security Update for Windows Server 2016	10	45	100%
Security Update for Windows 10 Fall Creators Update (KB1801342)	34	34	100%
Security Update for Windows 7 Fall Address Rollup (KB2875635)	88	2	100%

C

Contents

- Open Vulnerability Details
- 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

CVE ID	Vulnerability Name/Description	CVSS Score (Risk Level)	Impacted Endpoints	Exposed?	URL
CVE-2019-1302	0day server before 1.7.7 allows remote login by unauthenticated accounts due to bug in the REST API implementation.	8.8 (HIGH)	SERVER1, DESKTOP2	-	http://192.168.1.100:8080/
CVE-2019-7468	Chrome side-rolling (SSS) vulnerability in Open-Exchange (OX) Application 7.2.4 before 7.4.0-dev02 allows remote attackers to inject arbitrary code or HTML via the body of an email. NOTE: this vulnerability was first reported by CVE-2019-0424 because it affects different sets of versions.	6.1 (MEDIUM)	SERVER1, DESKTOP1, DESKTOP7	-	http://192.168.1.100:8080/
CVE-2014-0168	in fence-agent before 4.0.17 does not verify remote SSL certificates in the fence_pass_curl job by server which can potentially allow for injection of remote attackers to inject SSL certificates.	5.9 (MEDIUM)	DESKTOP3, DESKTOP7	-	http://192.168.1.100:8080/
CVE-2013-3662	The SUDO program (sudo) allows before 1.8.17 for sudo/note allow remote attackers to execute arbitrary code via a remote log.	7.8 (HIGH)	DESKTOP7	Yes	http://192.168.1.100:8080/

Machine Name	IP Address	Machine Type	Operating System	Firewall	Advanced Protection	DNS Protection	Remote Desktop Disabled	Open Vulnerabilities
SERVER1	192.168.1.2	Server	Microsoft Windows Server 2016 R2 Standard	✓	✓	✓	✓	0
DESKTOP1	192.168.1.8	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	10
DESKTOP2	192.168.1.188	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	17
DESKTOP3	192.168.1.8	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	0
DESKTOP4	192.168.1.348	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	0
DESKTOP5	192.168.1.28	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	11
DESKTOP6	192.168.204.102	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	0
DESKTOP7	192.168.2.6	Desktop	Microsoft Windows 10 Pro	✓	✓	✓	✓	0

User Name	User Role	Last Login Timestamp	Password Received	Password Changeable	Password Complexity Enforced	Password Expires in Less Than 90 Days	Remote Desktop Access Enabled
SERVER1\server1	Administrator	N/A	✓	✓	✓	✓	✓
SERVER1\user1	Guest	04/07/2020 11:45 PM	✓	✓	✓	✓	✓
DESKTOP7\user2	User	04/06/2020 12:58 PM	✓	✓	✓	✓	✓
DESKTOP7\user3	Administrator	N/A	✓	✓	✓	✓	✓
SERVER1\user4	Administrator	04/08/2020 11:17 AM	✓	✓	✓	✓	✓
DESKTOP4\user5	Administrator	03/17/2020 2:35:51 AM	✓	✓	✓	✓	✓
SERVER1\user6	Administrator	06/12/2019 4:18:15 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!



Gavin Hitchmough

Red Circles ITS Limited, Denby House Business
Center, Taylor Lane,

Loscoe, Derbyshire DE75 7AB

0330 135 9478

<https://www.redcircles-its.com>

