



**OBJECTIVE™**

Stress Free IT

# Dark Web Scanning

---

**Understanding the Why and How.**



01425 205200

[connect@objectiveuk.com](mailto:connect@objectiveuk.com)



# The Need for Dark Web Scanning

Dark web monitoring is emerging as a crucial element of a solid, advanced cybersecurity strategy.

Unfortunately, many organisations 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 organisation. **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 prioritising security as an essential element to their business success.

Take, for example, employee training. Many businesses don't realise 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 organisation 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?

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 prioritising security as an essential element to their business success.

Take, for example, employee training. Many businesses don't realise 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



## There's no better time to find out.

Many organisations 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 organisation'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**

### Executive Risk Summary

- 1 out of 10 endpoints with compromised and open configurations
- 3 user accounts required to look up for more than 30 days
- 88 out of 88 endpoints missing DMARC protection
- 1 out of 88 endpoints with missing security configurations
- 30 out of 88 endpoints missing advanced protection
- 4 out of 88 endpoints have no updates
- 4 out of 73 endpoints with patch status updated over 90% within 10 other endpoints with patch status updated over 70%
- 15 out of 88 endpoints have not logged in within the last 30 days
- 38 out of 88 endpoints with hardware backup policy configurations
- 1 out of 78 endpoints missing one of the Operating System
- 30 out of 78 endpoints with hard drive space utilized between 20-50%
- 4 out of 88 endpoints have not logged in within the last 30 days
- 23 out of 74 endpoints with hard drive space utilized between 20-50%
- 88 out of 88 endpoints with basic AV protection
- 88 out of 88 endpoints with BitLocker/BitLocker

## Risk Summary

**B**

### Assessments

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

**Risk Dashboard**

- Critical Security Vulnerability: 10
- High Severity Vulnerability: 23
- Medium Severity Vulnerability: 50
- Low Severity Vulnerability: 65

**Vulnerability Assessment**

**Risk Detected: High Risk Score**

**Patch Assessment**

**Apply Patch to Stay Protected**

Critical	High	Medium	Low
Apply patch within 30- 90 days	Apply patch within 30- 90 days	Apply patch within 60- 90 days	Apply patch within 90- 180 days

**Top 3 Missing Patches**

Patch Name	Number Found	Assess Count	Risk Score
Microsoft Windows Security Update KB4525213	10	45	1000
Microsoft Windows Security Update KB4525212	10	45	1000
Microsoft Windows Security Update KB4525211	10	45	1000

## Assessments

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

## Partner Report

**C**

### Contents

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

Open Vulnerability Details	Endpoint Health Details																																													
<table border="1"> <thead> <tr> <th>ID</th> <th>Vulnerability Name/Description</th> <th>CVE Score (Max Level)</th> <th>Required Action</th> <th>Implemented?</th> <th>Impact/Status</th> </tr> </thead> <tbody> <tr> <td>CVE-2019-1146</td> <td>OpenSSL before 1.1.1 allows remote denial of service (DoS) via a heap overflow in the SSL_CTX_set_cipher_list function.</td> <td>8.8 (CRITICAL)</td> <td>Update OpenSSL to 1.1.1g or later.</td> <td>Yes</td> <td>Resolved</td> </tr> <tr> <td>CVE-2019-1147</td> <td>OpenSSL before 1.1.1 allows remote denial of service (DoS) via a heap overflow in the SSL_CTX_set_cipher_list function.</td> <td>8.8 (CRITICAL)</td> <td>Update OpenSSL to 1.1.1g or later.</td> <td>Yes</td> <td>Resolved</td> </tr> </tbody> </table>	ID	Vulnerability Name/Description	CVE Score (Max Level)	Required Action	Implemented?	Impact/Status	CVE-2019-1146	OpenSSL before 1.1.1 allows remote denial of service (DoS) via a heap overflow in the SSL_CTX_set_cipher_list function.	8.8 (CRITICAL)	Update OpenSSL to 1.1.1g or later.	Yes	Resolved	CVE-2019-1147	OpenSSL before 1.1.1 allows remote denial of service (DoS) via a heap overflow in the SSL_CTX_set_cipher_list function.	8.8 (CRITICAL)	Update OpenSSL to 1.1.1g or later.	Yes	Resolved	<table border="1"> <thead> <tr> <th>Machine Name</th> <th>IP Address</th> <th>Operating System</th> <th>Annual Assessment</th> <th>Advanced Assessment</th> <th>OS Updates</th> <th>Security Software</th> <th>BitLocker</th> <th>BitLocker</th> </tr> </thead> <tbody> <tr> <td>10.10.10.1</td> <td>10.10.10.1</td> <td>Windows 10 Pro</td> <td>Pass</td> <td>Pass</td> <td>Pass</td> <td>Pass</td> <td>Pass</td> <td>Pass</td> </tr> <tr> <td>10.10.10.2</td> <td>10.10.10.2</td> <td>Windows 10 Pro</td> <td>Pass</td> <td>Pass</td> <td>Pass</td> <td>Pass</td> <td>Pass</td> <td>Pass</td> </tr> </tbody> </table>	Machine Name	IP Address	Operating System	Annual Assessment	Advanced Assessment	OS Updates	Security Software	BitLocker	BitLocker	10.10.10.1	10.10.10.1	Windows 10 Pro	Pass	Pass	Pass	Pass	Pass	Pass	10.10.10.2	10.10.10.2	Windows 10 Pro	Pass	Pass	Pass	Pass	Pass	Pass
ID	Vulnerability Name/Description	CVE Score (Max Level)	Required Action	Implemented?	Impact/Status																																									
CVE-2019-1146	OpenSSL before 1.1.1 allows remote denial of service (DoS) via a heap overflow in the SSL_CTX_set_cipher_list function.	8.8 (CRITICAL)	Update OpenSSL to 1.1.1g or later.	Yes	Resolved																																									
CVE-2019-1147	OpenSSL before 1.1.1 allows remote denial of service (DoS) via a heap overflow in the SSL_CTX_set_cipher_list function.	8.8 (CRITICAL)	Update OpenSSL to 1.1.1g or later.	Yes	Resolved																																									
Machine Name	IP Address	Operating System	Annual Assessment	Advanced Assessment	OS Updates	Security Software	BitLocker	BitLocker																																						
10.10.10.1	10.10.10.1	Windows 10 Pro	Pass	Pass	Pass	Pass	Pass	Pass																																						
10.10.10.2	10.10.10.2	Windows 10 Pro	Pass	Pass	Pass	Pass	Pass	Pass																																						

# 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.

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 organisation. If you identify any of your users' credentials for sale on the dark web, take the necessary steps to remediate the situation and prioritise strengthening your security posture for the future. That includes training your users on their role in defence of the organisation. 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 defence.

Additional tests, like a vulnerability scan, can further identify specific areas of weakness and recommend appropriate remediation.

