



DARK WEB COMPROMISE REPORT

OF EXPOSED CREDENTIALS
FOR YOUR COMPANY

14



EXTERNAL THREAT INTELLIGENCE

Are you monitoring for compromised data that can be used to exploit your business?

Yes No

DATA BREACH & PRIVACY LAW COMPLIANCE

Do you have a compliant data breach response plan in place?



Yes No

WE IDENTIFY

COMPROMISES
Throughout your organization.

**EMPLOYEE
CREDENTIALS ARE
A BEST SELLER
ON THE DARK WEB**

WE MONITOR

- 24/7/365
- Hidden chat rooms
 - Private websites
 - Peer-to-peer networks
 - IRC (Internet relay chat) channels
 - Social media platforms
 - Black market sites
 - 640,000+ botnets

WE REPORT

80,000+
Compromised emails daily.

YOUR INFORMATION IS ALREADY EXPOSED

This information is used to compromise your corporate services such as: Office 365, payroll services, VPNs, remote desktops, banking, VOIP, ERP, CRM, social media access, ID Theft.

Most Recent 5 Compromises

| Date Found | Email | Password Hit | Source | Type | Origin | PII Hit |
|------------|----------------------------|--------------|----------------|---------------|---------------|---------|
| 03/22/18 | gary@marshallinfotech.com | gm19**** | id theft forum | Not Disclosed | Not Disclosed | None |
| 03/22/18 | daren@marshallinfotech.com | bung**** | id theft forum | Not Disclosed | Not Disclosed | None |
| 10/02/16 | gary@marshallinfotech.com | \$2a\$**** | Dark Web Site | Not Disclosed | Not Disclosed | None |
| 06/08/16 | daren@marshallinfotech.com | 7b03**** | social media | Data Breach | linkedin.com | None |
| 06/08/16 | gary@marshallinfotech.com | b087**** | social media | Data Breach | linkedin.com | None |

WHY MONITORING FOR EXPOSED CREDENTIALS IS IMPORTANT

HOW ARE CREDENTIALS COMPROMISED?



PHISHING

- Send e-mails disguised as legitimate messages
- Trick users into disclosing credentials
- Deliver malware that captures credentials



WATERING HOLES

- Target a popular site: social media, corporate intranet
- Inject malware into the code of the legitimate website
- Deliver malware to visitors that captures credentials



MALVERTISING

- Inject malware into legitimate online advertising networks
- Deliver malware to visitors that captures credentials



WEB ATTACKS

- Scan Internet-facing company assets for vulnerabilities
- Exploit discovered vulnerabilities to establish a foothold
- Move laterally through the network to discover credentials



Passwords are a twentieth-century solution to a modern-day problem. Unfortunately, user names and passwords are still the most common method for logging onto services including corporate networks, social media sites, e-commerce sites and others.

39%
Percentage of adults in the U.S. using the same or very similar passwords for multiple online services

28,500
Average number of breached data records, including credentials, per U.S.-based company

User names and passwords represent the keys to the kingdom for malicious attackers. Criminals who know how to penetrate a company's defenses can easily steal hundreds or even thousands of credentials at a time.

A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing credentials. And by selling those credentials to multiple buyers, organizations that experience a breach of credentials can easily be under digital assault from dozens or even hundreds of attackers.

\$1 - \$8
Typical price range for individual compromised credentials

WHAT CAN AN ATTACKER DO WITH COMPROMISED CREDENTIALS?



Send Spam from Compromised Email Accounts

Deface Web Properties and Host Malicious Content

Install Malware on Compromised Systems

Compromise Other Accounts Using the Same Credentials

Exfiltrate Sensitive Data (Data Breach)

Identity Theft

PROTECTING AGAINST CREDENTIAL COMPROMISE

While there is always a risk that attackers will compromise a company's systems through advanced attacks, most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only by implementing a suite of tools including monitoring, data leak prevention, multifactor authentication, employee security awareness training and others - can organizations protect their business from the perils of the dark web.

