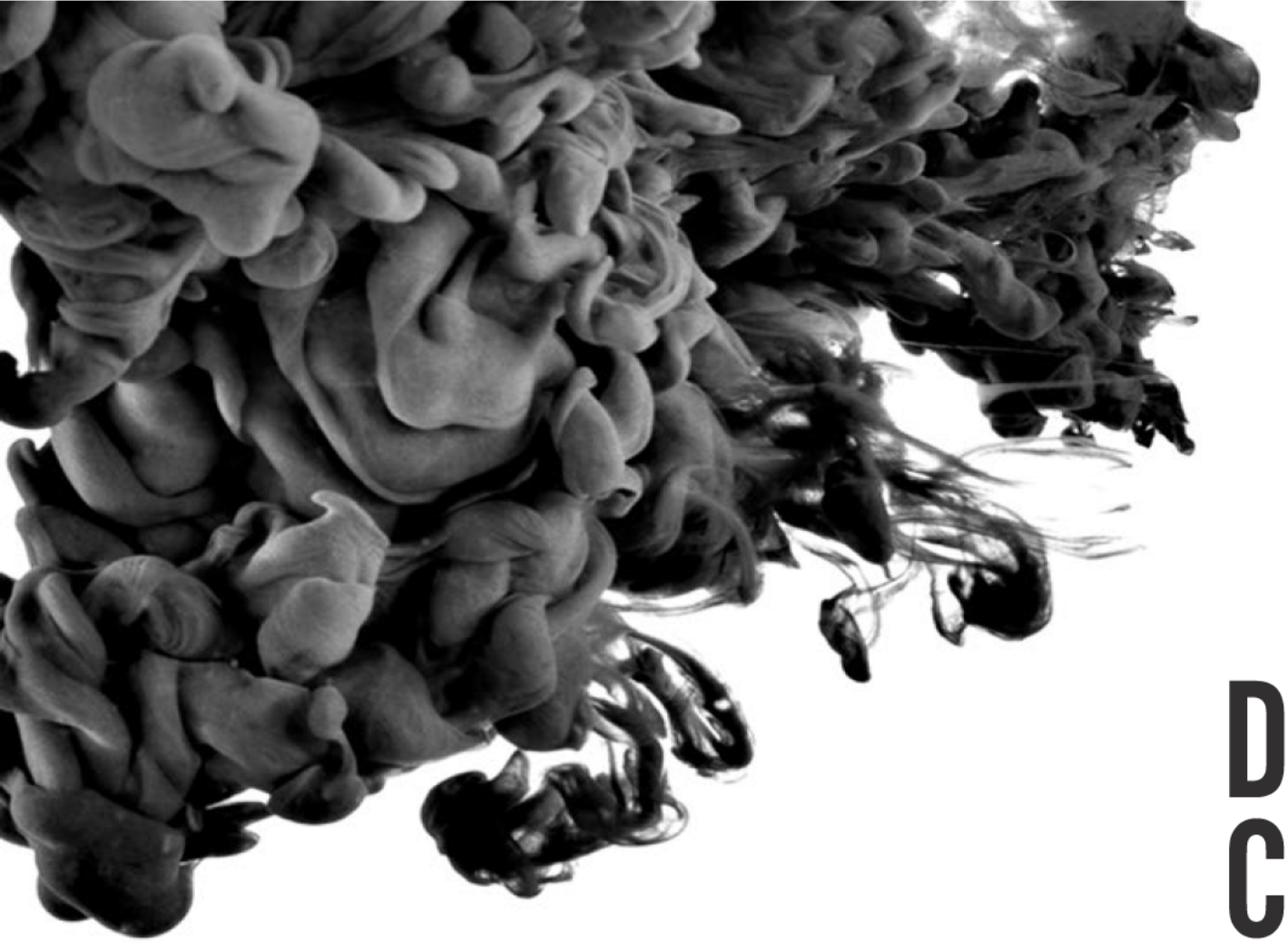

INTERNETEK

DARK WEB COMPROMISE REPORT

Prepared for ci[redacted]om

Jun 28, 2024

INTERNETEK

OF EXPOSED CREDENTIALS FOR YOUR COMPANY

5

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

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.

Certified in Dark Web Monitoring

Most Recent 5 Compromises

Date Found	Email	Password Hit	Source	Type	Origin	PII Hit
04/27/24	cid[redacted]com	Gree*****	Not Disclosed	combolist	Not Disclosed	None
04/12/24	cid[redacted]com	Gree*****	id theft forum	Phishing or Keylogging	Not Disclosed	1
04/12/24	cid[redacted]com	Gree*****	id theft forum	Phishing or Keylogging	Not Disclosed	1
02/07/24	cid[redacted]com	Gree*****	id theft forum	Phishing or Keylogging	Not Disclosed	1
01/18/24	cid[redacted]com	Gree*****	Not Disclosed	combolist	Not Disclosed	None

WHY MONITORING FOR EXPOSED CREDENTIALS IS IMPORTANT

INTERNETEK

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.