

# DARK WEB COMPROMISE REPORT

Prepared for @sample.com

Jul 03, 2020

# OF EXPOSED CREDENTIALS  
FOR YOUR COMPANY

**1,000+**



### 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.

 **Certified in  
Dark Web Monitoring**

# Most Recent 100 Compromises

Date Found	Email	Password Hit	Source	Type	Origin	PII Hit
06/23/20	sample@sample.com	4568****	id theft forum	Not Disclosed	Not Disclosed	None
06/22/20	john.doe@sample.com	derp****	id theft forum	Data Breach	vendor.com	None
06/22/20	sample@sample.com	rara****	id theft forum	Data Breach	vendor.com	None
06/22/20	sample@sample.com	poop****	id theft forum	Data Breach	vendor.com	None
06/22/20	samp134e@sample.com	samp****	id theft forum	Data Breach	vendor.com	None
06/22/20	sample@sample.com	samp****	id theft forum	Data Breach	vendor.com	None
06/22/20	jane.smith@sample.com	bobe****	id theft forum	Data Breach	vendor.com	None
06/22/20	name@sample.com	pick****	id theft forum	Data Breach	vendor.com	None
06/22/20	nam23@sample.com	1004****	id theft forum	Data Breach	vendor.com	None
06/22/20	sample1@sample.com	samp****	id theft forum	Data Breach	vendor.com	None
06/22/20	samplez@sample.com	hock****	id theft forum	Data Breach	vendor.com	None
06/22/20	sample@sample.com	12du****	id theft forum	Not Disclosed	Not Disclosed	None
06/22/20	name@sample.com	vege****	id theft forum	Not Disclosed	Not Disclosed	None
06/22/20	sample123@sample.com	samp****	id theft forum	Data Breach	vendor.com	None
06/18/20	example2323@sample.com	denn****	id theft forum	Not Disclosed	Not Disclosed	None
06/17/20	ndia@sample.com	[]>[]****	id theft forum	Not Disclosed	Not Disclosed	None
06/16/20	j.doe@sample.com	tany****	id theft forum	Not Disclosed	Not Disclosed	None
06/16/20	samplejones@sample.com	TheR****	id theft forum	Not Disclosed	Not Disclosed	None
06/16/20	sample@sample.com	samp****	id theft forum	Not Disclosed	Not Disclosed	None
06/16/20	email_sample@sample.com	spar****	id theft forum	Not Disclosed	Not Disclosed	None
06/16/20	j.smith@sample.com	eesp****	id theft forum	Not Disclosed	Not Disclosed	None
06/16/20	test@sample.com	jaso****	id theft forum	Not Disclosed	Not Disclosed	None
06/16/20	email@sample.com	hatc****	id theft forum	Not Disclosed	Not Disclosed	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.

**\$1 - \$8**

Typical price range for individual compromised credentials

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.

## 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.

