ThinkGard
Total Data Security

DARKWEB ID

# Digital Credentials:
## Your Most Critical Corporate Asset

**39%** **Percentage of adults in the U.S. using the same or very similar passwords for multiple online services, which increases to 47% for adults age 18-29**

Passwords are a twentieth-century solution to a twenty-first century problem. Unfortunately, user names and passwords - the most common digital credentials used today - are all that stands between your employees and vital online services including corporate networks, social media sites, e-commerce sites and others. A good security practice is to use a completely different password for every service, but the fact is that nearly 40% of Americans replicate the same or very similar passwords for each service they use.

Pew Research Center, "Americans and Cybersecurity", January 2017

## How Are Credentials Compromised?

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

**Malvertising**
- Inject malware into legitimate online advertising networks
- Deliver malware to visitors 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

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

Federal Financial Institutions Examination Council (FFIEC), "Joint Statement: Cyber Attacks Compromising Credentials", March 2015

## 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

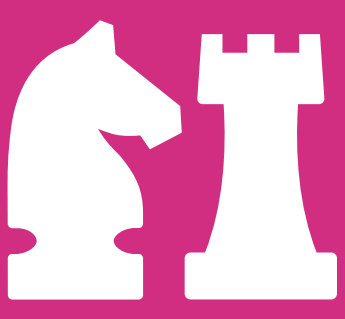
**28,500** **Average number of data records per company, including credentials, compromised during a data breach**

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, each one representing another potential entry point to compromise the organization's networks and data.

Ponemon Institute and IBM, "Cost of Data Breach Study", June 2017

## Protecting Against Credentials Compromise

While there is always a risk that attackers will compromise a company's systems through advanced attacks, the fact is that most data breaches exploit common vectors such as known vulnerabilities, unpatched systems and unaware employees. Only through defense in depth - implementing a suite of tools such as security monitoring, data leak prevention, multifactor authentication, improved security awareness and others - can organizations protect their credentials and other digital assets from seeping onto the Dark Web.



*"For [attackers targeting] big corporate networks, persistence and focus will get you in without a zero day; there are so many more vectors that are easier, less risky, and more productive."*

Rob Joyce, Chief, Tailored Access Operations (TAO), National Security Agency USENIX Enigma 2016 Conference, January 27, 2016

**Typical price range on Dark Web markets for compromised credentials, ranging from online services to corporate network usernames and passwords** **$1-$8**

For those who make credentials available on the Dark Web, the financial rewards can be significant. A criminal dealing in stolen credentials can make tens of thousands of dollars from buyers interested in purchasing them. 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.

Brian Krebs, "Krebs on Security" blog, June 13, 2013

## Dark Web ID: Find Out Before the Damage is Done

**Dark Web ID from ID Agent** provides continuous searching, monitoring and reporting on the presence of your organization's credentials on the Dark Web, and immediately notifies you so that you can take action before these critical digital assets are used to compromise your personnel, networks and data. Coupled with a layered approach to security, Dark Web ID can help your organization to reduce the likelihood and impact of compromised credentials, meet compliance, and ensure that you're not the next organization in the headlines for the wrong reason.


ThinkGard
Total Data Security

DARKWEB ID

ThinkGard, LLC | 160 Yeager Parkway, Suite 200 | Birmingham, AL 35124 (205) 564-2724 • sales@ThinkGard.com