# Compromised Credentials

## Learn From the Exposure of the World's 1,000 Biggest Companies

digital shadows_

# Table of Contents

# Executive summary

Barely a week goes by without reports of a leaked database. Amid all this noise, it's often still difficult to make sense of the leaked information and understand what it means for organizations.

By using the world's 1,000 largest companies as a sample from the Forbes Global 2000, it enables us to better understand the extent to which organizations are effected and how threat actors may be looking to exploit these credentials. Armed with this insight, organizations of all sizes can better prepare and mitigate for instances of credential compromise.

# The Proliferation of Compromised Accounts

Credential compromise is not new, but the frequency of appearance of compromised credentials online has increased. Dumps of stolen credentials are regularly sold, traded and shared online across paste sites, file-sharing sites and online marketplaces. For example, actors using the names "Peace of Mind" and "Tessa88" recently thrust themselves into the media limelight following the public release of the LinkedIn and MySpace databases. We have also seen "thedarkoverlord" offering multiple healthcare databases on the Real Deal marketplace and, more recently, the claimed Dropbox leak. As demonstrated by the LinkedIn and Dropbox breaches, which were made public four years after the initial breach, there are likely many more credentials circling in underground forums that are yet to be made public.

As a result, the number of compromised credentials that are available online is staggering, providing a goldmine for attackers. With this in mind, it is unsurprising that one report claimed that breached credentials were responsible for 63 percent of data breaches.[1]

For the companies that were the source of the breach, there are clear reputational, brand and financial implications.[2] However, the consequences of these breaches extend far beyond these companies. Organizations with employees who have reused corporate emails and passwords can be at risk of account takeovers, credential stuffing and extortion attempts.

What does this all mean for organizations? After all, a recent report claimed that 60 percent of companies are unable to detect compromised credentials.[3] This report seeks to help organizations readdress this by understanding where they are exposed, how threat actors are using this information, and what they can do to prepare for and mitigate such events.

# Methodology

Given the rate at which credentials are leaked online, this research seeks to better understand the impact these breaches have on organizations.

By taking a data-driven approach, it is possible to better understand this phenomenon and identify any trends that may exist between sectors and geographies. This analysis identifies how many credentials have been leaked online, using the biggest 1,000 companies in the Forbes Global 2000 list.

Using Digital Shadows SearchLight™, our proprietary blend of technology and expertise that continually monitors paste sites, social media, forums, dark web sources and criminal sites, we have identified and collected over 30,000 claimed breaches between April 2014 and June 2016. This includes credentials dumped on paste sites, but also larger data files shared online.

This analysis takes the world's biggest 1,000 companies – in terms of sales, profits, assets and market value – from the Global 2000.[4] The domains of these 1,000 companies, as well as identifiable subsidiaries, were subsequently crosschecked against these instances. Further quality assurance was conducted to ensure that the most appropriate domains were selected for each company, and consumer email domains were omitted where applicable. In total, 19,362 domains were crosschecked against our breach data.

In order to understand trends across different industries, the Forbes sectors were mapped to smaller groupings:

- Financial Services
- Food and Hospitality
- Healthcare and Pharmaceutical
- Manufacturing
- Oil, Gas and Utilities
- Retail
- Technology
- Travel and Leisure
- Real Estate
- Industrial Goods and Services
- Entertainment
- Other

# Credential Compromise Affecting the World's 1,000 Biggest Public Companies

## Overview

In total, 5,550,485 email and password combinations were detected across all companies. Although there are several companies with significantly higher than average footprints, 97 percent had breached credentials publically available online, with a median average of 706 credentials per organization.

Many claimed breaches are often simply copies and reposts of previously leaked databases. In total, over 500,000 claimed breach credentials were, in fact, duplicates. This leaves approximately 5 million unique credentials available online. This illustrates the challenge organizations face to verify the uniqueness of the claimed breach and prioritize accordingly.

## Regional Variations

Increasingly we see campaigns and operations targeted at specific geographies. Of course, OpOlympicHacking tended to target companies based in Rio, and OpIsrael tended to target Israeli companies. But it is not just hacktivist campaigns; many malware and extortion campaigns are heavily tied to certain geographies. It is understandable, however, that Figure 1 demonstrates a high percentage of companies from North America, Europe, and the United Kingdom.

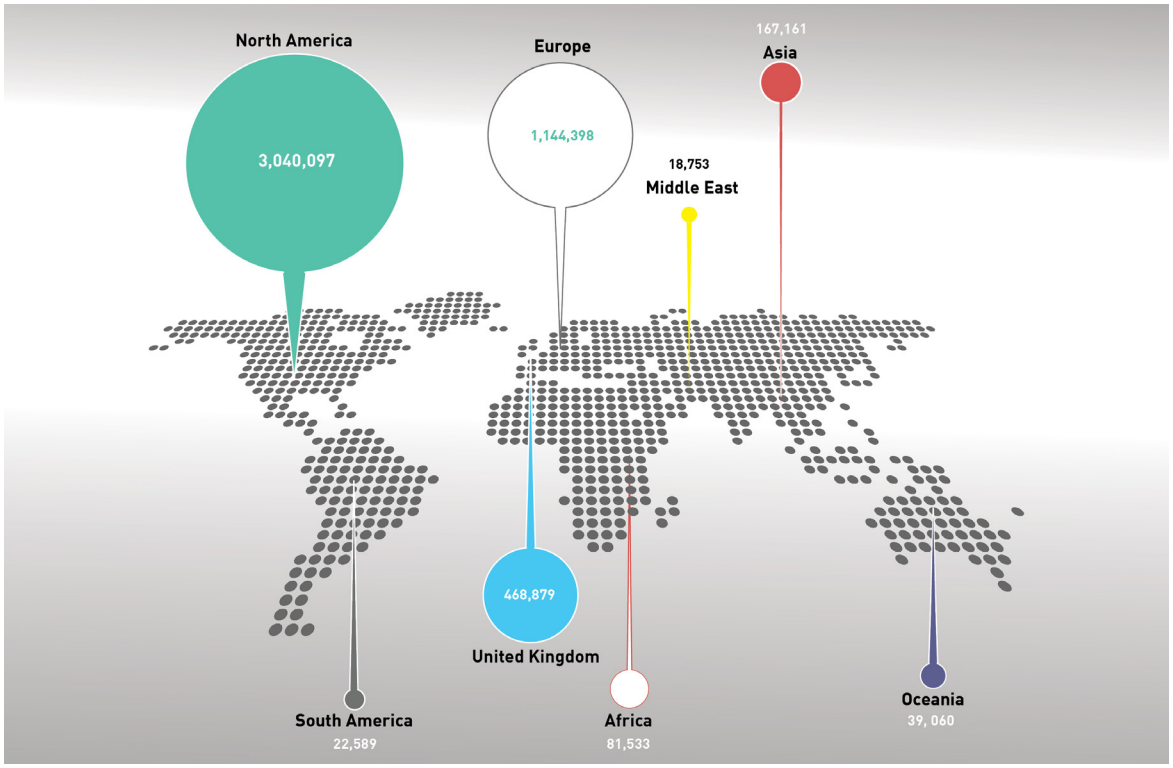


*Figure 1: Total unique leaked credentials mapped to region*

Of course, it is likely that North America features so heavily due to the high percentage of organizations that reside in the United States. If we look at Figure 2, it shows the average (mean) number of credentials per company, per continent, making the figures far more balanced.

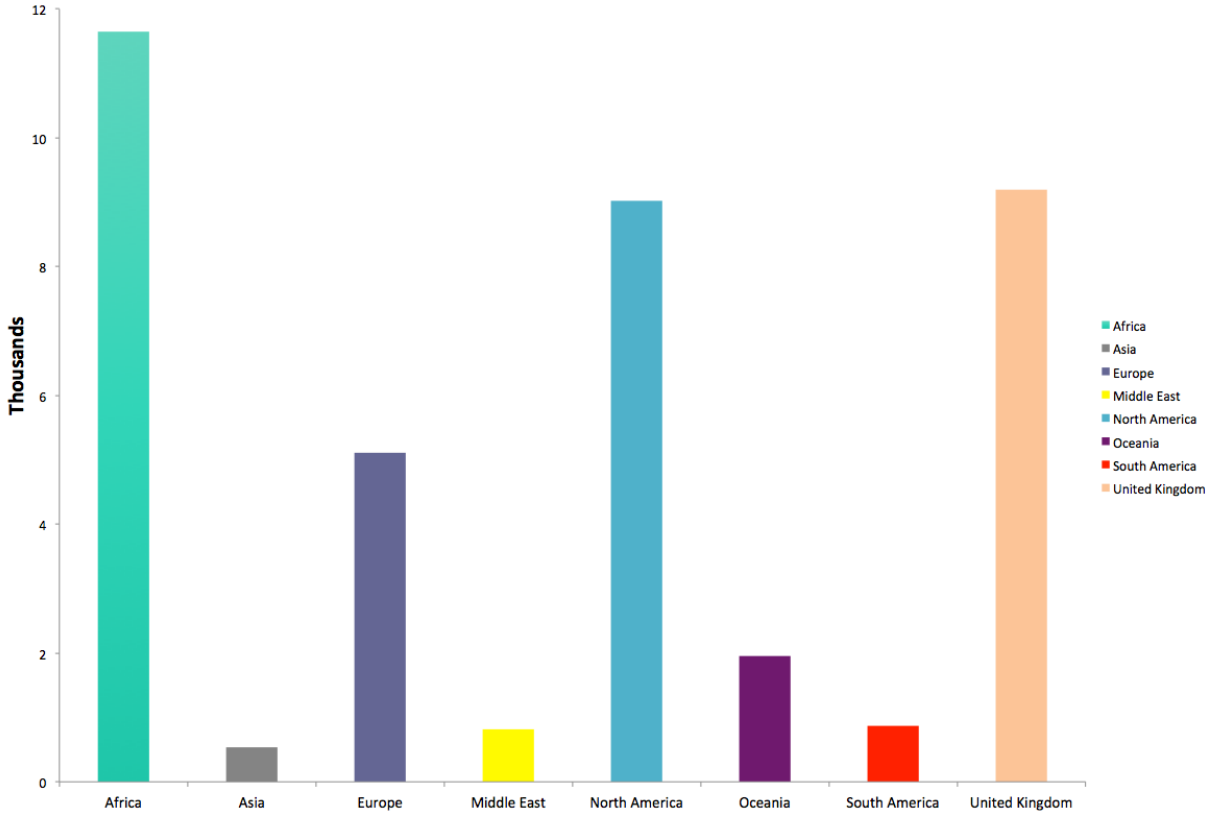


*Figure 2: Average leaked credentials per company distributed by region*

## Most Impacted Industries

It is important to note that not all industries are affected in the same way. As Figure 3 shows, the top three industries that were affected in these breaches were technology, entertainment and financial services. Of course, this is all relative and even proportionally lower sectors were significantly impacted:

1. Oil, Gas and Utility - 172,685 (3 percent)
2. Healthcare and Pharmaceutical – 165,764 (3 percent)
3. Industrial Goods and Services – 157,968 (3 percent)
4. Retail – 156,807 (3 percent)

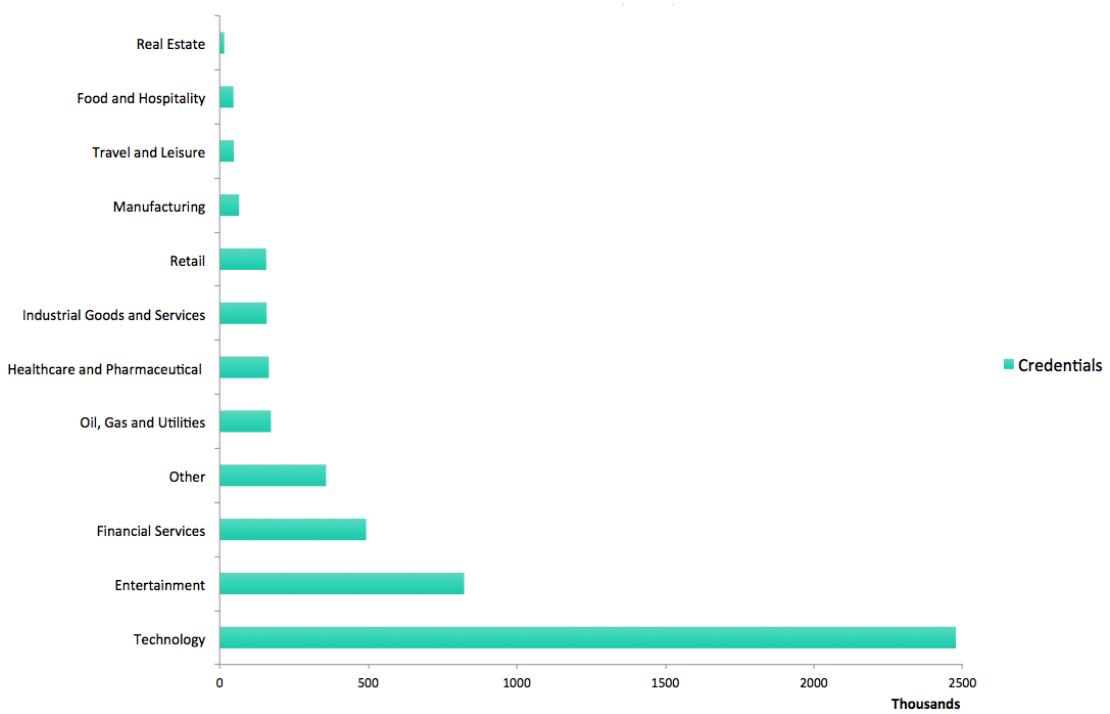


*Figure 3: Credentials broken down by industry*

So how does this look at an individual organization's level? Figure 4 provides an overview of the average (mean) number of leaked credentials across each industry, helping to better represent those industries with fewer organizations represented in the sample. This changes the picture slightly, with Healthcare and Pharmaceutical and Industrial Goods and Services having a respective average of 3,453 and 2,289 leaked credentials per company.

| Industry | Average Leaked Credentials |
|---|---|
| Entertainment | 37,399 |
| Technology | 25,806 |
| Healthcare and Pharmaceutical | 3,453 |
| Other | 2,470 |
| Industrial Goods and Services | 2,289 |
| Financial Services | 1,832 |
| Retail | 1,802 |
| Manufacturing | 1,191 |
| Food and Hospitality | 1,188 |
| Travel and Leisure | 975 |
| Oil, Gas and Utilities | 767 |
| Real Estate | 395 |

*Figure 4: Average (mean) leaked credentials per company broken down by industry*

## Usual and Unusual Suspects: Most Significant Breaches

Every time a breach is publicly announced, it attracts a significant amount of media attention. But which were the most significant for organizations? Many employees of these organizations reused their corporate emails for other services and, when these services were breached, it also revealed their credentials. The top breaches were, somewhat unsurprisingly, social media platforms. Indeed, LinkedIn, MySpace and Tumblr breaches were responsible for a respective 30 percent, 21 percent and 8 percent of the total credentials.

A similarly high amount of credentials came from the iMesh breach (5 percent), a file and media sharing client, and the Adobe (25 percent) leaks. Although proportionately low, there were gaming sites also responsible for leaked credentials; MPGH (6,641), XSplit (5,106) and Minecraft (232) all featured a notable amount of credentials.

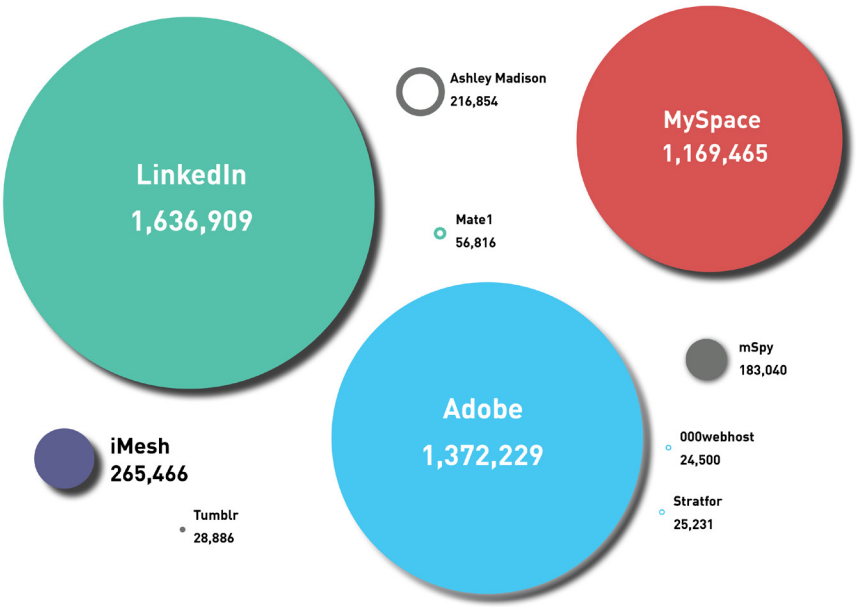


*Figure 5: Credentials broken down by breach source*

What is the significance? The leaked passwords from Adobe were encrypted (rather than hashed) using Triple DES (3DES) in Electronic Code Book (ECB) mode and are, therefore, susceptible to recovery in certain conditions. For LinkedIn and MySpace, however, the situation is worse; both were SHA1 hashed and unsalted, making it easier for cybercriminals to ascertain the clear text passwords.

These sources are all to be expected, but there were also many unexpected sources. Dating websites were surprisingly high, especially as many credentials used for these sites were corporate accounts. Ashley Madison (216,854), Adult Friend Finder (4,364) and Mate1 (56,816) were the top three examples of this. These dating sites are significant because they breach far more than merely

emails and passwords; personally identifiable information (PII), sexual preferences and partial credit card numbers were also leaked. The significance of this will be explored in following sections.

## Summary

The number of credentials leaked online for the world's 1,000 biggest organizations is staggering. However, it is important to remember that this is not the whole picture and does not provide an exhaustive list. In fact, organizations are likely further exposed by third parties and suppliers. Figure 6 illustrates a weak correlation between a company's size and the number of credentials. In reality, credential compromise affects organizations of all sizes.

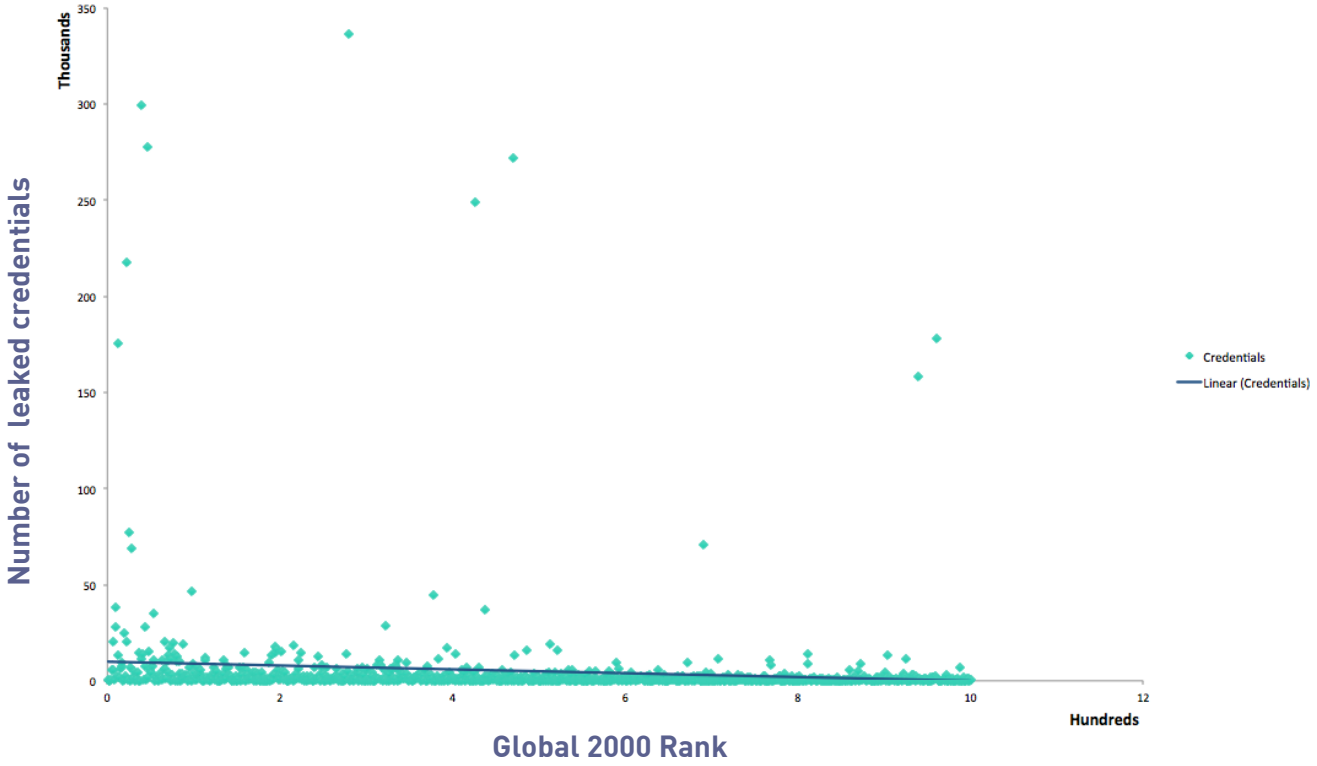


*Figure 6: Leaked credential mapped to organizations' size.*

But why does this matter? If organizations find out, can they not simply reset their passwords? What is more, some organizations may even have a policy that dictates passwords must be changed every four to six weeks. However, this does not mean organizations should care any less, as compromised credentials offer a host of options for attackers.

# Why Your Credentials Matter

As a result of these breaches it is clear that, irrespective of size, industry or geography, the vast majority of organizations have credentials exposed online. Before resetting passwords, an organization's first step should be to determine if their credentials have previously been exposed. This is wise, given that 10 percent of breaches were duplicates. After all, the process of resetting password causes friction for organizations. In order to achieve this, an organization may either collect and validate the data itself, or with the help of third party services.[5]

## Understanding the Value

Not all credentials were made equal and there are three main factors that affect the value an organization's credentials have to an attacker:

1. **Recoverability.** How were the passwords stored? Were they encrypted, hashed, salted and hashed or clear text?
2. **Freshness.** How recent is the data, and is it likely to have already been used extensively on the criminal underground?
3. **Transferability.** Was additional information leaked, such as PII or payment data?

Figure 7 illustrates the varied uses of leaked credentials and how an attacker can benefit.

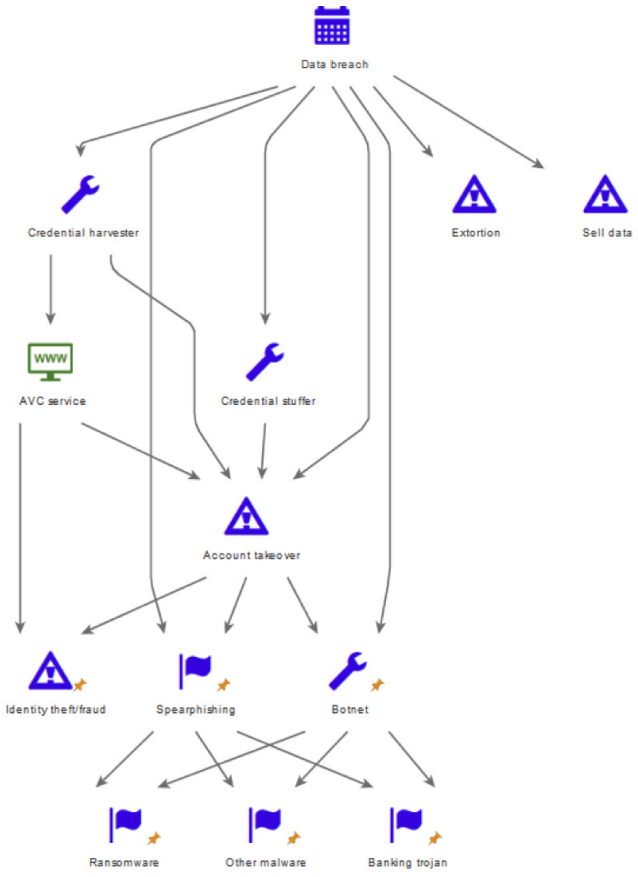


*Figure 7: Link analysis for industrialized use of breached data*

## Uses and Abuses

It is possible to identify five main ways in which threat actors can use organizations' leaked credentials.

### 1. Account takeover

On May 23, 2016, OurMine Team reportedly compromised a number of social media profiles for various business personnel and celebrities. The accounts that were affected included Twitter, Tumblr, and LinkedIn profiles. The group initially claimed the use of zero-day exploits to compromise accounts, but later confirmed access was secured through the use of information from the recently exposed dataset from LinkedIn.

More recently, it was reported that the alleged Dropbox leak also occurred from password reuse of the LinkedIn breach.[6] The likelihood is that people have neglected to change their passwords since 2012, and proceeded to recycle the same password for multiple services.

### 2. Spear-phishing

On June 11, 2016, Germany's Computer Emergency Response Team (CERT-Bund) reportedly detected spear phishing emails that had been sent to company executives, which CERT-Bund claimed were likely used information derived from the 2012 breach of LinkedIn.[7] It was reported that threat actors had been able to craft personalized emails using the target's first name, last name, job role and company name as part of their distribution of malicious, macro-enabled Microsoft Word documents to individuals in the Netherlands. When the documents were opened and macros were enabled, it reportedly led to the delivery of the Panda Banker banking trojan.[8]

### 3. Credential stuffing

Threat actors can automatically inject breached username and password pairs in order to fraudulently gain access to user accounts. This technique, known as credential stuffing, is a type of brute force attack whereby large sets of credentials are automatically inputted into websites until a match with an existing account is found. An attacker can then hijack that account for a variety of purposes, such as draining stolen accounts of funds, the theft of personally identifiable information, or to send spam. According to the Open Web Application Security Project (OWASP), credential stuffing is one of the most common techniques used to take-over user accounts.[9]

One popular piece of software in this regard is Sentry MBA, a freely and publicly available piece of

software that can be loaded with configuration files in order to automate the attempted access of user accounts by trying numerous credential combinations against online login portals. The tool has functions to mitigate traditional online login form security controls, such as IP rate limits and blacklists. Sentry MBA relies to some extent on weak passwords and password reuse as it uses previously leaked credential combinations as part of its attacks.

Sentry MBA has the capability to bypass CAPTCHA controls that are designed to impede automated interaction. It attempts to bypass these controls by using Optical Character Recognition (OCR) software and other mechanisms so that it can read and solve CAPTCHA challenges.

**4. Post-breach extortion**

Over 200,000 corporate email addresses of the sampled companies were leaked as part of the Ashley Madison breach. Following the breach of online dating site Ashley Madison in July 2015, extortion attempts were directed against specific individuals identified within the compromised dataset. Users received extortion emails threatening to share the exposed information with the victim's partner, unless one Bitcoin was paid into a specified Bitcoin wallet.

A number of automated post-breach extortion services also emerged which looked to exploit the sensitivity of the data exposed in the Ashley Madison breach, such as websites offering searchable databases for users who suspected they had been leaked in the breach. One site reportedly spammed users with unsolicited bulk emails that suggested their spouses or employers may find out their details were exposed. These alarmist emails contained additional marketing material for their services, and even encouraged users to pay for the services of a private investigator. Messages were allegedly sent both to users who checked their own emails, as well as those who had their addresses checked by partners or a third party.[10]

**5. Botnets**

Breached datasets containing email addresses can be used in the operation of botnets, which can subsequently be used to deliver spam or more malicious pieces of malware.

In September 2015, it was reported that criminals using the Dridex banking trojan had targeted 385 million email addresses, predominantly from UK companies.[11] Dridex is primarily a banking malware that is designed to infect systems and steal banking credentials from users. The data is

used to facilitate the access of online bank accounts and transfer funds to accounts under the control of the attackers. Once a victim machine is infected, it becomes part of a botnet, a group of infected machines under centralized control.[12]

When reported in September 2015, Fujitsu claimed they had detected 12 phishing attempts a day, with victims primarily being those in accounting roles in UK-based banks, government agencies and other corporations. Fujitsu also released a YouTube video warning that Dridex hackers were using socially-engineered phishing emails to spread the Trojan through infected spreadsheet attachments.[13] Once opened, the trojan executed and enabled macros, allowing Dridex to capture any online banking activity through keylogging or screenshots of the victim's computer screen.

# It Doesn't Matter Who You Are, What Matters is Your Plan

Large data breaches often come from very large organizations, which have become a target for threat actors. However, organizations of all sizes are impacted by data breaches. But how can organizations better prepare for and mitigate against such instances? These findings help to highlight ten tips for preparing for compromised credentials.

1. Establish a policy for which external services are allowed to be associated to corporate email accounts. Although social media accounts were the most common source of leaked credentials, dating and gaming services were also common.

2. Implement an enterprise password management solution. This is not only great for secure storage and sharing but also strong password creation and diversity.

3. Understand and monitor approved external services for password policies and formats to understand the risks and lowest common denominators.

4. Proactively monitor for credential dumps relevant to your organization's accounts. Consider additional monitoring for your high value targets' (e.g.: executives) non-enterprise accounts.

5. Internally (or with the help of an external service) evaluate credential dumps to determine if the dumps are new or have been previously leaked. In total, 10% of all claimed credential compromises were duplicates.

6. Implement multi-factor authentication for external facing corporate services. This might include services like Microsoft Outlook Web Access, and Secure Sockets Layer Virtual Private Networks, as well as for software-as-a-service offerings like Google Applications, Office365, and Salesforce.

7. Understand and document any internal services that aren't federated for faster and more complete incident response to any breach that impacts an organizational account.

8. Ensure that you have an emergency password reset process in place. Make sure that all of the users' accounts are included, not just Microsoft Active Directory accounts.

9. If you have any user behavior analytics capabilities, import compromised identity information and look for any suspicious activity (e.g.: accessing resources that have not been accessed in the past.)

10. Update security awareness training to include the risks associated with password reuse. Encourage staff to use consumer password management tools like 1Password or LastPass to also manage personal account credentials.

**Authors: Rick Holland, Michael Marriott, Bryan O'Neil, Aleksej Polukarov, Daniel Telehagen, Abhay Shete**

# Appendix 1: Sub Sector Breakdown

| Sector | Sub Sector | Percentage of Leaked Credentials | Average (mean) Leaked Credentials |
|---|---|---|---|
| Entertainment | Advertising | 2% | 37,399 |
| | Broadcasting & Cable | 95% | |
| | Printing & Publishing | 3% | |
| Technology | Telecommunications Services | 51% | 25,806 |
| | Software & Programming | 5% | |
| | Semiconductors | 1% | |
| | Electronics | 0.4% | |
| | Computer Storage Devices | 1% | |
| | Computer Services | 31% | |
| | Computer Hardware | 9% | |
| | Communications Equipment | 3% | |
| Healthcare and Pharmaceutical | Pharmaceuticals | 62% | 3,453 |
| | Medical Equipment & Supplies | 14% | |
| | Managed Healthcare | 12% | |
| | Healthcare Services | 6% | |
| | Biotechnologies | 6% | |
| Industrial Goods and Services | Security Systems | 2% | 2,289 |
| | Railroads | 4% | |
| | Heavy Equipment | 17% | |
| | Other Industrial Equipment | 11% | |
| | Business Products & Supplies | 12% | |
| | Business & Personal Services | 22% | |
| | Electrical Equipment | 10% | |
| | Other | 22% | |
| Financial Services | Banks | 75% | 1,832 |
| | Investment | 16% | |
| | Other financial services | 9% | |
| Retail | Personal & Household Goods | 36% | 1,802 |
| | Apparel | 12% | |
| | Department Stores | 4% | |
| | Discount Stores | 10% | |
| | Drug Retail | 2% | |
| | Food Retail | 21% | |
| | Internet & Catalog Retail | 9% | |
| | Other Retail | 6% | |
| Manufacturing | Auto & Truck Parts | 30% | 1,191 |
| | Auto & Truck Manufacturers | 70% | |
| Food and Hospitality | Beverages | 42% | 1,188 |
| | Food Processing | 44% | |
| | Other | 13% | |
| Travel and Leisure | Airlines | 53% | 975 |
| | Casinos | 1% | |
| | Hotels and Motels | 46% | |
| Oil, Gas and Utilities | Oil and Gas | 68% | 767 |
| | Utilities | 32% | |
| Real Estate | Real Estate | 88% | 395 |
| | Leasing | 12% | |
| Other | Other | - | 2,470 |

# End Notes

1. Verizon DBIR http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

2. A recent ENISA report provided a great overview of attempts to assign a cost to a company suffering a data breach http://www.securityweek.com/whats-real-value-cost-breach-studies

3. https://www.rapid7.com/resources/incident-detection-response-survey.jsp

4. http://www.forbes.com/global2000/list/3/#tab:overall

5. See Troy Hunt's haveibeenpwned.com

6. www.techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/

7. https://twitter.com/certbund/status/739825583962656776

8. https://blog.fox-it.com/2016/06/07/linkedin-information-used-to-spread-banking-malware-in-the-netherlands/

9. https://www.owasp.org/index.php/Credential_stuffing

10. https://www.troyhunt.com/ashley-madison-search-sites-like/

11. http://www.scmagazine.com/uk-firms-hit-as-dridex-criminals-target-385-million-emails/article/438572/

12. http://www.justice.gov/opa/pr/bugat-botnet-administrator-arrested-and-malware-disabled

13. https://www.youtube.com/watch?v=iRIRG6nJP1E&feature=youtu.be&list=FLDgRapfUbo_IoIgN-dsgP_w

# About Digital Shadows

Digital Shadows provides cyber situational awareness that helps organizations protect against cyber attacks, loss of intellectual property, and loss of brand and reputational integrity. Its flagship solution, Digital Shadows SearchLight™, is a scalable and easy-to-use data analysis platform that provides a view of an organization's digital footprint and the profile of its attackers. It is complemented with intelligence operations analyst expertise to ensure extensive coverage, relevant intelligence and frictionless deployment. SearchLight continually monitors the visible, deep and dark web and other online sources to create an up-to-the minute view of an organization and the risks requiring mitigation.

The company is jointly headquartered in London and San Francisco.

**digitalshadows.com**


**London**

Level 39, One Canada Square, London, E14 5AB

+44 (0) 203 393 7001 info@digitalshadows.com

**San Francisco**

332 Pine Street, Suite 600 San Francisco, CA 94104

+1 (888) 889 4143


digital shadows_