Credential Compromise Affecting the Entertainment Industry

Credential compromise is not new, but the frequency of appearance of compromised credentials online has increased. Perhaps the most famous cybersecurity incident in the entertainment industry occurred in 2014 with the Sony hack, which revealed the personal information of tens of thousands of people.[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.

This report seeks to help organizations understand where they are exposed, how threat actors are using this information, and what they can do to prepare for and mitigate instances of credential compromise.

Methodology

By taking a data-driven approach, it is possible to better understand credential compromise 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 service that combines scalable data analytics with human analysts to monitor for cyber threats, data leakage, and reputation risks, 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.[3] 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, of which Entertainment was one.

Findings

In total, 935,870 email and password combinations were detected for this industry, with over 80,000 being duplicates. This leaves more than 850,000 unique credentials available online for entertainment organizations.

The impact of credential compromise on the entertainment industry varies from subsector to subsector. Broadcasting and cable organizations experienced the majority of leaked credentials, with 79 percent. To put this in context, advertising, which constituted seven percent, encountered over 28,000 breach credentials.

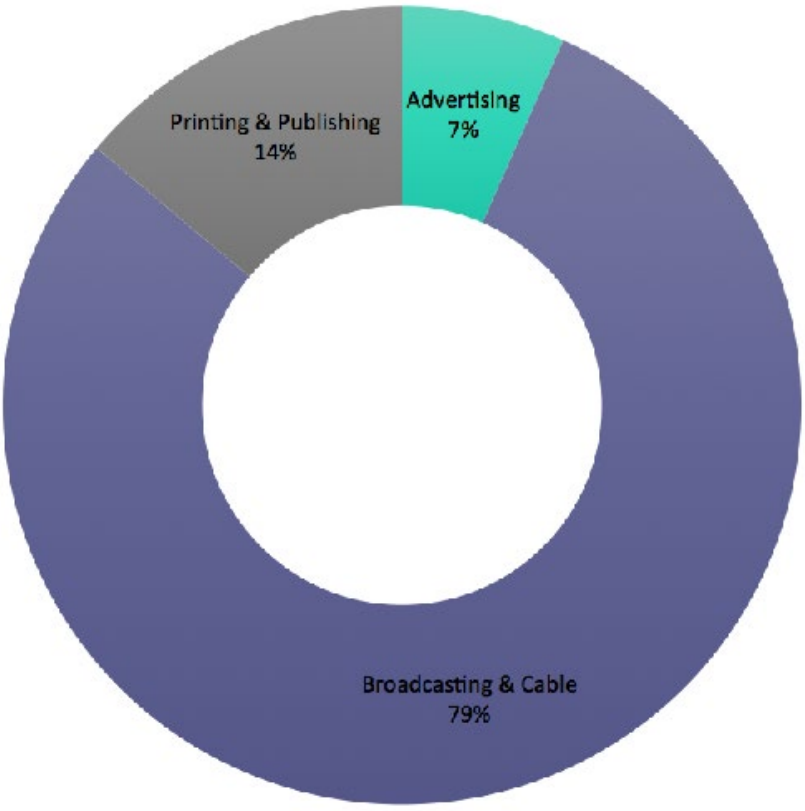

Figure 1: Unique leaked credentials distributed by subsector

Most Significant Breaches

Each 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, MySpace, LinkedIn, and Tumblr breaches were responsible for a respective 41, 14 and 3 percent of the total leaked credentials. A similarly high amount of credentials came from the iMesh (11 percent), a file and media sharing client, and the Adobe breach (22 percent) leaks.

The significance weighs heavily on how the passwords were stored. For example, 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.

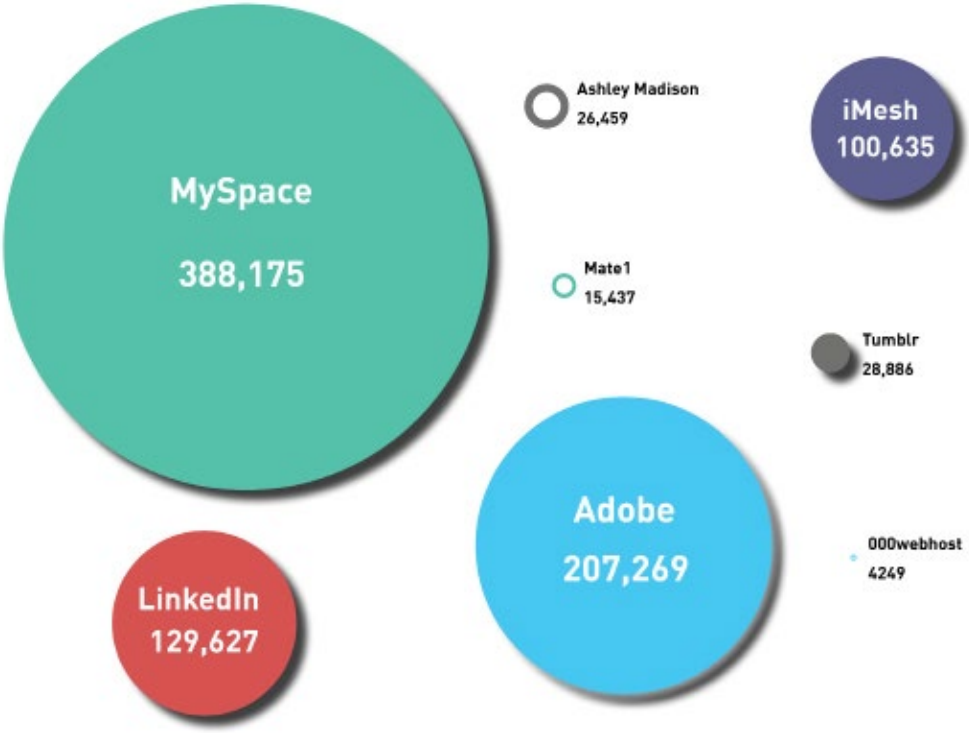

Figure 2: Most significant breaches

These sources are all to be expected, but there were also many unexpected sources. Dating websites were surprisingly high, especially as these credentials were corporate accounts. Ashley Madison (26,459), Adult Friend Finder (917) and Mate1 (15,437) 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), in addition to the preferences, encrypted passwords, and partial credit card numbers, were also leaked. The significance of this will be explored in following sections.

Why Your Credentials Matter

In order to understand the significance of these compromised credentials, it is important to understand why they are sought after by cybercriminals. It is possible to identify five main ways in which organizations' leaked credentials can be exploited.

1. Account takeover

It was recently reported that the alleged Dropbox leak also occurred from password reuse of the LinkedIn breach.[4] 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.[5] 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.

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.[6]

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.

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.

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.

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

End Notes

1. http://www.cnbc.com/2015/11/24/the-sony-hack-one-year-later.html
2. In fact 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. http://www.forbes.com/global2000/list/3/#tab:overall
4. www.techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/
5. https://twitter.com/certbund/status/739825583962656776
6. https://www.owasp.org/index.php/Credential_stuffing

About Digital Shadows

Digital Shadows provides insight into an organization's external digital risks and the threat actors targeting them. Digital Shadows SearchLight™ service combines scalable data analytics with human analysts to monitor for cyber threats, data leakage, and reputation risks. Digital Shadows continually monitors the Internet across the visible, deep and dark web, as well as other online sources to create an up-to-the minute view of an organization and provide it with tailored threat intelligence. The company is jointly headquartered in London and San Francisco. For more information, visit www.digitalshadows.com.

London +44 (0) 203 393 7001
Level 39, One Canada Square, London, E14 5AB

San Francisco +1 (888) 889 4143
332 Pine Street, Suite 600 San Francisco, CA 94104

info@digitalshadows.com

digital shadows_