How to Reduce the Cybersecurity Risks Posed by Leaked Data

By Avi Gesser, Will Schildknecht, Guy Nizan (IntSights) & Ariel Ainhoren (IntSights) on April 24, 2019

As we highlighted in our predictions for 2019, the proliferation of leaked personal information online provides an increasingly valuable resource for threat actors to use in cyber attacks. So far in 2019, billions of records have been leaked, creating significant additional cybersecurity risks for companies. To help understand this threat, and the steps companies can take to reduce risk, we've invited **IntSights**, a leading cyber intelligence platform focused on external threat monitoring across the open, deep and dark web, to collaborate on this post.

The Fallout from the Collections #1-5 and Verifications.io Leaks

In January, **security researcher Troy Hunt announced the discovery of Collection #1**, a tranche of 773 million unique usernames and passwords available online. Collections #2-5 followed, introducing billions of additional usernames and passwords. Separately, in March, an unsecured database maintained by Verifications.io, a company that facilitates email distribution lists, resulted in the exposure of 763 million records, including email addresses, names, gender, IP addresses, phone numbers, and other data points. Last year, credential leaks were one of the most common alerts identified by IntSights' dark and deep web monitoring, with the company flagging dozens of companies' databases offered for sale each day. In fact, an entire dark web economy has been fueled by leaked credentials. Hackers with sophisticated technical ability search for openings in corporate networks or exposed data to acquire database files. They then will typically sell the raw dataset to middlepersons, who invest the time to break any encryption on the files and package them for sale. These middlepersons then sell the packaged, decrypted files to end users on **dark web marketplaces** to facilitate fraud using automation tools.

How Cybercriminals Use Leaked Data

These leaks, and the economy that has grown up around them, reflect a growing trend that is unlikely to decline any time soon. Indeed, as it becomes easier for companies to aggregate massive repositories of consumer data, the volume of information that can be exposed in data leaks similarly increases. And the exposure of more personal data means greater risk to companies from credential stuffing and targeted phishing attacks.

In a credential stuffing attack, the threat actor uses an automated process to test stolen username and password combinations on various sites in the hopes of gaining access to an account. The tactic exploits the vulnerability created when employees reuse the same or a similar username and password across multiple websites.

As we have previously discussed on this blog, phishing is a social engineering attack where the threat actor pretends to be a trustworthy user, such as an employee, in order to access sensitive information without authorization. Attackers can leverage personal information obtained from data leaks and public sources to aid them in targeting and deceiving company employees, e.g., through fake computer support emails and correctly answering security questions.

IntSights found that in 2018, its threat monitoring technology most frequently identified leaked credentials for telecommunications, information services, retail, financial services and healthcare companies. The risks associated with leaked credentials are exacerbated by the SEC's scrutiny of **public companies** and regulated **financial services companies** for inadequate phishing and email compromise security measures.

How to Reduce the Risk of Data Leaks

Fortunately, there are a few common-sense measures that companies are adopting to manage risks from these voluminous data leaks.

1. Mandatory Password Rotation and Complexity. Even if a leak does not involve the compromise of any company emails or passwords, a company's data may be at risk because employees often use their work email address as their login for nonwork websites, and the same passwords for both. Because the effectiveness of password rotation programs may be diminished where users repeat variations on the same password, e.g., "Password1" followed by "Password2," some companies are requiring that new passwords be complex and not similar to previously used passwords. While it may seem obvious that non-unique passwords are particularly susceptible to compromise, the **United Kingdom National Cyber Security Centre reported this week** that 23.2 million breached accounts worldwide used "123456" as their password.
2. Requiring Unique Passwords for Work. To further reduce this risk, some companies have a policy prohibiting employees from (1) using their corporate email address as a login for non-company applications or websites, and (2) using the same password, or very similar passwords, for both work and nonwork purposes.
3. Cybersecurity Training. Employee training that highlights the implications and severity of data leakage, while showing them live examples of employee actions that compromised companies' data, can go a long way to reducing the risks of data leakage.
4. Multifactor Authentication (MFA). **As we have previously discussed**, it is good practice to set up MFA for remote access to company accounts. With proper MFA, even if a threat actor finds a leaked username and password combination that corresponds to a company account, the threat actor will also need the employee's authentication key to successfully penetrate the account. Companies with MFA should also be sure that related policies, e.g., a lost phone policy, do not undermine the value of having MFA requirements—**as we have noted here before**. Many companies are also employing more advanced MFA methods that use authenticator apps and code generator chips to avoid advanced attacks that can hijack text massages and circumvent MFA.
5. Deep and Dark Web Monitoring. Services like those offered by IntSights, find leaked data associated with the company and thereby can help in knowing where companies are vulnerable. Data in Collections #1-5 **may have been available among hacker collectives long before they became public**. If a company merely reacts to the public release of the information, sophisticated threat actors may have already leveraged the data to attack that company's systems. Web monitoring tools can provide valuable reconnaissance to address leaks of employee credentials well before they make the headlines.

Read more about these cybersecurity practices on the **Davis Polk Cyber Portal**, where you can also find dozens of other resources designed to help our clients prepare for, and respond to, cyber incidents.