**Dunkin Donuts Incident Response Analysis**

by Austin Brinning, Drew Hartwig, Tommy Melles, Ben Shabaz

**Introduction**

Dunkin Donuts has been the target of two major cyber-attacks, one in 2015 and another in 2018. The 2015 attack was a credential stuffing attack, where the threat actor used automated tools to test large numbers of username and password combinations stolen from other sources. As a result, thousands of customer accounts were compromised, allowing the attacker to gain unauthorized access to customer accounts on Dunkin Donuts' website and mobile application, and steal sensitive information such as names and email addresses. Dunkin Donuts quickly responded by launching an investigation, identifying the source of the breach, notifying affected customers, and providing free identity theft protection and credit monitoring services. Despite their efforts, the incident raised serious concerns about the company's ability to protect customer data, highlighting the need for stronger cybersecurity measures in the fast-food industry. The 2018 hack was also a credential stuffing attack and resulted in the compromise of more than 300,000 customer accounts.

**Analysis**

*Target –* Dunkin Donuts, as a multinational company with over 9,000 stores in 36 countries, was a high-value target for cybercriminals. The company's vast customer base and the volume of financial transactions processed daily made it an attractive target for cybercriminals seeking to steal sensitive data for profit. Dunkin Donuts was targeted in two major cyber-attacks in 2015 and 2018 that compromised thousands of customer accounts. In both cases, the primary target of the attacks was the company's customer data, including personally identifiable information such as names and email addresses, which was stored in the company's databases. The attackers accessed this data through the company's website and mobile application, using automated tools to test large numbers of username and password combinations stolen from other sources. The attacks also targeted the company's financial information, including bank account information and transaction data, with the aim of stealing money from Dunkin Donuts and its customers. The attackers likely intended to use this information to conduct fraudulent transactions or sell the data on the dark web to other cybercriminals. The Dunkin Donuts cyber-attacks highlight the importance of implementing robust cybersecurity measures to protect customer data and financial information, especially for businesses with a large customer base and a high volume of financial transactions.

*Attack –* The attack on Dunkin Donuts was carried out using a credential stuffing technique, which involved the use of automated tools to test large numbers of username and password combinations stolen from other sources. The threat actor used these tools to bypass Dunkin Donuts' security measures and gain unauthorized access to customer accounts on the company's website and mobile application. Once inside, the attacker was able to steal a variety of sensitive information, including names and email addresses. As a result of the attack, both Dunkin Donuts and its customers suffered significant financial losses. The company had to bear the costs of notifying affected customers, providing them with free identity theft protection and credit monitoring services, and implementing additional security measures to prevent future attacks. Customers who fell victim to fraudulent transactions also had to bear the financial burden of recovering their losses and repairing their credit scores. The Dunkin Donuts cyber-attack serves as a reminder of the severe financial consequences that can result from a successful cyber-attack and highlights the need for strong cybersecurity measures to protect against such attacks.

*Threat Actor –* There was no specific name or group given to the attackers in this case. The attackers that used a credential stuffing attack to hack their way into the Dunkin Donuts accounts were simply referred to as “hackers”. These hackers are an example of a cybercriminal as their main motivation was to gain access to valuable data and monetary value from different Dunkin Donuts accounts on their app. Dunkin Donuts has still failed to investigate into who committed these attacks on their accounts.

*Investigation -* The investigation revealed that threat actors gained unauthorized access to customer accounts by leveraging stolen login credentials obtained through third-party breaches, a technique commonly known as credential stuffing. This occurred both in 2015 and in 2018. So, these occurrences had two separate investigations that lasted two separate time periods. In 2015 the attack was much smaller with not as many customers affected. Dunkin’ notified customers to change passwords while filing up the incident with law enforcement. This is a very short investigation with minimal changes being made due to the threat actor being unknown. Dunkin’ was informed to make changes to their security but took very minimal changes that lead to another attack in later years. The 2018 attack was very similar to the 2015 attack since it was also a credential stuffing attack, but at a much larger scale with 300,000 accounts being breached. This took Dunkin’ more by surprise and took a more extensive investigation than the pervious years. The investigation team worked closely with cybersecurity experts and law enforcement to identify the attack vectors, contain the incident, and enhance the organization's security posture. The remediation measures included resetting passwords, implementing multi-factor authentication, and enhancing monitoring and detection capabilities to prevent future attacks. As a result of the attack, Dunkin' also faced several lawsuits from customers who claimed that the company failed to implement adequate security measures to protect their personal and financial information, a violation of data privacy regulations.

*Impact -* The Dunkin' Donuts cybersecurity attacks had a significant impact on the company, its customers, and its reputation. The attack resulted in the compromise of customer login credentials and stored value cards, which led to unauthorized transactions and financial losses. This constituted a breach of confidentiality, integrity, and availability of customer data, which are key principles of information security. The incident also had legal and regulatory implications for Dunkin', as the company was subject to data privacy laws that require organizations to protect their customers' personal and financial information. Failure to do so can result in penalties, fines, and legal action, which can damage a company's reputation and financial standing. After all investigations were complete Dunkin’ was required to pay $650,000 in fees and return all other monetary values back to their DD perk users. The attack also had a negative impact on customer trust and confidence in Dunkin'. Customers may have lost faith in the company's ability to protect their sensitive information, which can lead to a loss of business and revenue. Overall, the Dunkin' Donuts cybersecurity attack underscores the importance of implementing effective cybersecurity measures to protect against threats and ensure the confidentiality, integrity, and availability of sensitive data.

*Response –* The first attack that occurred in 2015 Dunkin’ Donuts had 10,000s of accounts acquired and the customers information and monetary values were stolen. The attackers used millions of automated attempts to access customers account login and password information. This ended up being a larger problem than originally should’ve been due to Dunkin’ Donuts not taking proper protocol to inform users of their breached information. Customers then noticed that their DD Perk reward points and other monetary values were being deducted from their accounts without them redeeming them. Due to this the customer support team was just informing their users to create a new password in hopes of resolving the issue in the short run. They then made a small investigation into this issue, and they failed to resolve them as we can see later. During the first attack in 2015 these attackers were able to gain customer information and Dunkin’ made minimal changes to provide security to their customers moving into future years!

The second attack occurred in 2018. At this time the hackers were able to access more than 300,000 customer accounts. When these accounts were accessed by the unauthorized hackers Dunkin’ did not tell the customers that their account information was stolen once again, they made the excuse that a third party tried to obtain their information but ended up failing to do so. After such a similar issue happened again just three years later there was an investigation launched by the state of New York against Dunkin’ Donuts. Through this investigation all the hidden facts that Dunkin’ was hiding from their customers came to light. They were then fined $650,000 and had to take more advanced security precautions to help protect their customers information. The way Dunkin’ has implemented security changes is to inform them to change their passwords often. They told users not to repeat any pervious usernames or passwords. Most importantly they learned not to lie to your users when their information has been acquired!

**Conclusion**

References

<https://informer.io/resources/dunkin-donuts-data-breach>

<https://cylanda.com/dunkin-donuts-hacked/>

<https://www.zdnet.com/article/dunkin-donuts-accounts-compromised-in-second-credential-stuffing-attack-in-three-months/>

https://ag.ny.gov/press-release/2020/attorney-general-james-gets-dunkin-fill-holes-security-reimburse-hacked-customers