Name : Arham Asif Syed

Section: A2

Email id : arhamasif2702@gmail.com

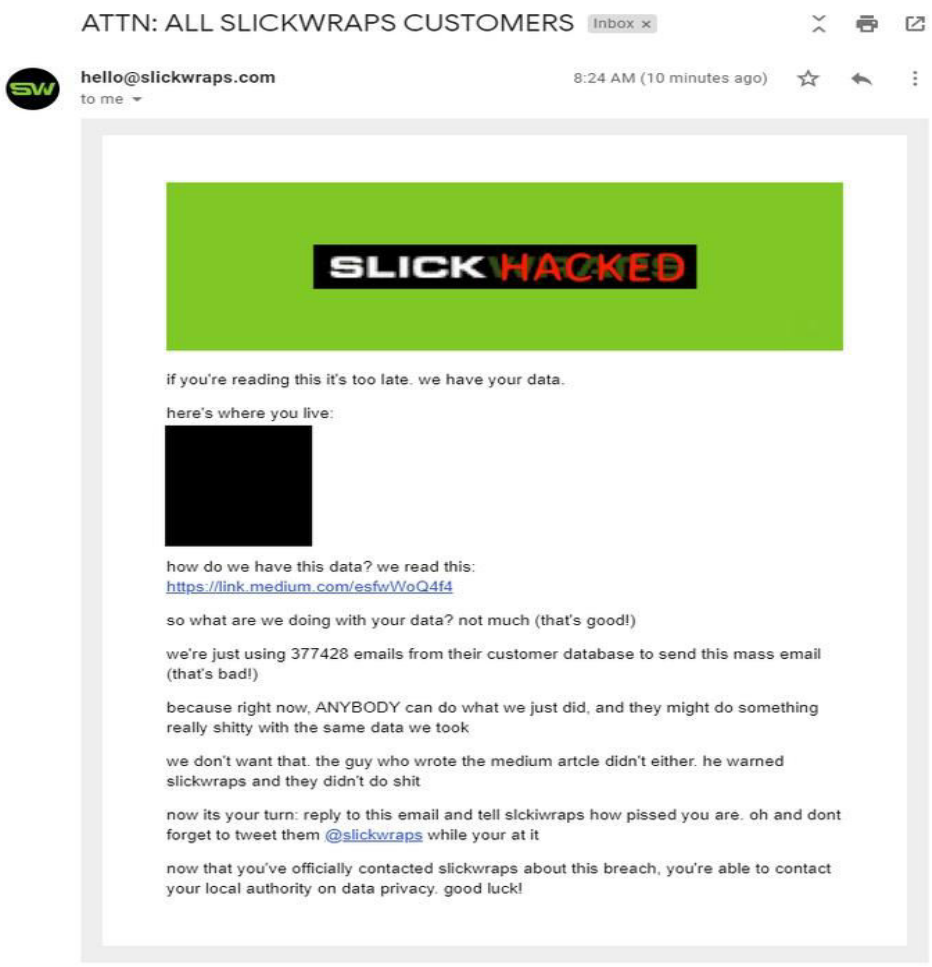
SLICKWRAP'S

Data breach

Introduction:-

Slickwraps, a company that lets users design custom skins for their electronics, was embroiled in a data breach story. The breach started when someone claimed to be a "white hat" hacker who tried to alert the company about its "abysmal cybersecurity."

Unfortunately, **Slickwraps** ignored them, so the hacker published a now-deleted Medium post about the experience. A second hacker read this post and exploited **Slickwraps'** vulnerability, hacking the company. In a particularly egregious touch, the



hacker then emailed all the customers to notify them that their data had been compromised.

How and when the Breach Happened:-

The breach happened on February in 2020.The company's phone customization tool was vulnerable to remote code execution. Users needed to be able to upload their custom photos, but **Slickwraps** let them upload any file to the highest directory on the

server. So, this hacker uploaded a file that allowed them to achieve remote code execution and execute shell commands.

What Data Was Exposed:-

Per the original hacker, the vulnerability gave them nearly free rein over **Slickwraps'** systems, including access to customer photos, billing and shipping addresses, admin account details, and the resumes of all employees.

Vulnerabilities:-

What's unusual about this case is how the hacker apparently breached **Slickwraps'** systems: not by discovering the vulnerability on their own, but by reading a post which is now deleted from an anonymous fellow hacker.

In its blog post, **Slickwraps** said customer data in some of the company's non-production databases was "mistakenly made public via an exploit" and that those databases were "accessed by an unauthorized party."

Data lost:-

- Resumes of current and past **SlickWraps** employees
- 9GB of customer photos uploaded to the case customization tool
- All **SlickWraps** admin account details, including password hashes
- All current and historical **SlickWraps** customer billing addresses

- All current and historical SlickWraps customer shipping addresses
- All current and historical SlickWraps customer email addresses
- All current and historical SlickWraps customer phone numbers
- All current and historical SlickWraps customer transaction history
- The company's content management system

Remedies taken by SLICKWRAP'S:-

Slickwraps said the exploit had been repaired, that "all data is secured," and that it's working with a "third-party cybersecurity team" for analysis of the situation. The FBI had also opened an investigation on this.

The company recommended users change their passwords for their Slickwraps account. It also said it will make security improvements moving forward.

Lessons learnt (as a customer):-

1. Always make sure you trust the website you share your data with
2. Always use strong passwords and do not keep guessable credentials
3. Read the privacy policies of the company carefully before registering
4. Check whether the company is secure or not

5. Always use double factor authentication which helps keep your data safer

6. You must understand the fact that once you share your data on the internet it is no longer safe, so you must be careful at each step

Lessons learnt (as company owner/employee):-

1. Learn to keep the customers data private and secure

2. Do not disobey your privacy guidelines

3. If there is a data breach, we should take necessary actions ASAP

4. We should make sure that there are no loop holes left unchecked after rectifying a data breach which might give the hacker a second chance.

5. Form a strong cyber security team which will defend your company from deadly hackers and their attacks

6. Hire proficient and sincere employees which will help in keeping your customers data safe