Roku 2024 Data Breach:

Analysis of the Credential Stuffing Attack and Roku's Corporate Response

Elliott Richter

SEC-110-002B

November 2, 2024

[Data breach information]

Overview:

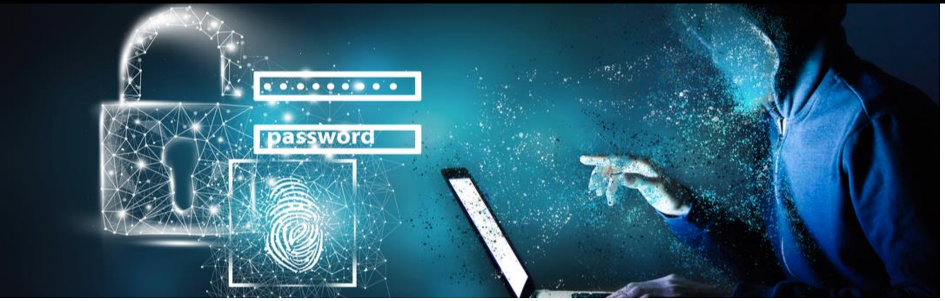
- In April of 2024, Roku announced they were breached by a cyberattack. This breach affected around 576,000 user accounts by a method know as credential stuffing.

- Credential stuffing is when hackers use various user login credentials that were stolen from other unrelated services and platforms and used to gain access to the target accounts.

- Once the attack was discovered, Roku publicly announced the breach to notify everyone. This announcement was also in hopes to encourage users to improve their account security practices.

- Luckily, the hackers were only able to make purchases on the platform and not actually see any sensitive user information like names, addresses, and credit cards.

[Data breach information]



Timeline:

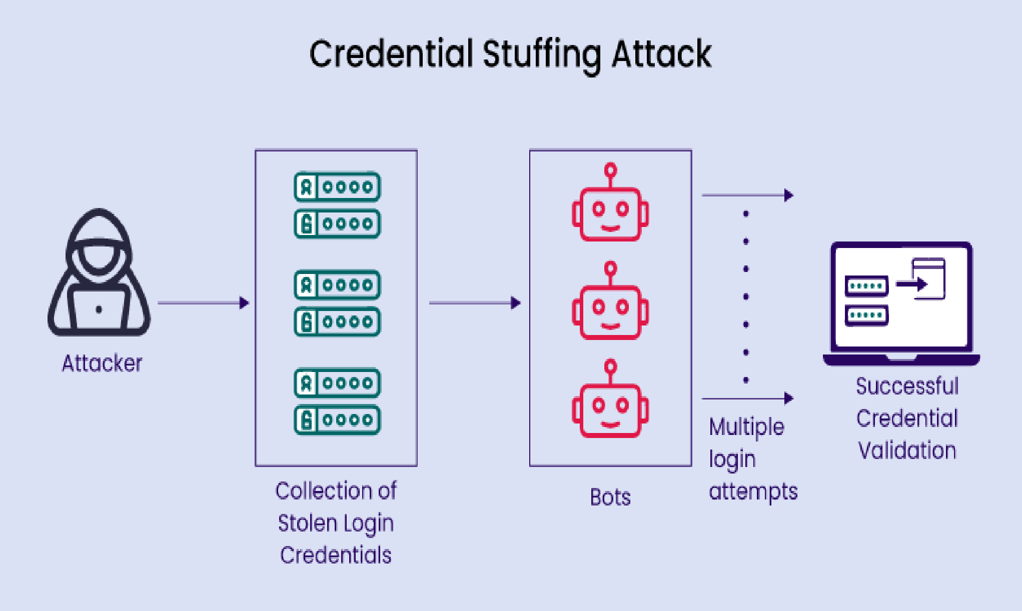
- On April 10, 2024 – Roku discovered the breach in their system. *
- On April 12, 2024 – Roku made their public announcement of the breach. They strongly encouraged users to change their passwords to a stronger one.

*This breach was discovered while monitoring account activity after another cyberattack earlier in the year affected 15,00 users. Roku was already on alert from the previous attack. This allowed Roku to discover the attack faster than usual.

[How did it happen]

- By using Credential Stuffing, the hackers focused on finding the users that use the same password across many login sites and platforms.
- This allowed the hackers to simply and easily automate the login attempts over various services like Roku.
- Roku insists the login information (usernames and passwords) had been obtained from other sources and not from Roku.
- The hackers most likely used automation to easily try thousands of passwords and account combinations in a relatively short amount of time.
- These types of tools are common and now with AI, are getting more sophisticated and efficient.

[How did it happen]


Credential Stuffing Attack
Attacker
Collection of Stolen Login Credentials
Bots
Multiple login attempts
Successful Credential Validation

Think about the cyberattack this way:

- Imagine having a master key (a list of valid stolen passwords) to a storage unit facility (user accounts).
- This key was obtained from another facility (previously successful cyberattack).
- The locks (passwords) are in process of being replaced slowly one at a time.
- All the new and old locks look the same (encryption), but the key only works on the locks that have not yet been changed (the compromised passwords).
- The hackers tried the key repeatedly on all the units (user accounts) until they found the doors the key opens.
- Then you go back and take as much stuff that was in the units (make purchases) as you can.
- However, you do not know who owns the unit nor their payment info as that is secure in the main office (sensitive information secured properly according to Industry standards and regulations) and you do not have the key for that.

[Evidence of compromise]

Forensic Analysis of the Breach:

- Roku’s security teams were already monitoring their systems due to a previous attack earlier in the year.
- The team noticed a massive increase in unsuccessful user login attempts and the various locations they came from.
- These patterns were atypical for normal user login attempts.
- Normally a user tries a couple of times from 1 or 2 locations in close proximity before logging in successfully, not thousands from across the globe for each account.

[Evidence of compromise]

- In addition, system logs were used to identify numerous unauthorized access to the user accounts.
- Logs also showed atypical and unusual new purchases / subscriptions on the accounts that were hacked.
- By using these logs, they were able to identify the full scope of the breach and how to contain it.

[Evidence of compromise]

The main factors that triggered the flags were:

- The numerous volume of unsuccessful login attempts from new and unfamiliar IP addresses across the globe.
- Increasing number of reports that came in from users claiming unusual activity, new icons of subscriptions, and unauthorized purchases on their dashboards.

[Impact to the organization/customers]

WAY
Streamed 27.7 billion hours since 2008
Roku®
Happy Streaming™
Streamed 27.7 billion hours since 2008
ROKU
Happy Streaming
THOMSON REUTERS

Customer Impact:

- Company’s image was injured, and customers have lost a lot of trust as they feel their information is not safe with Roku.
- 567,000 Users were affected. All were required to reset their passwords.
- Hackers only were able to make purchases on about 400 of the accounts.
- No confidential user information was accessed like names, addresses, or credit cards.
- This spurred heightened security and privacy concerns about how Roku handles sensitive information.

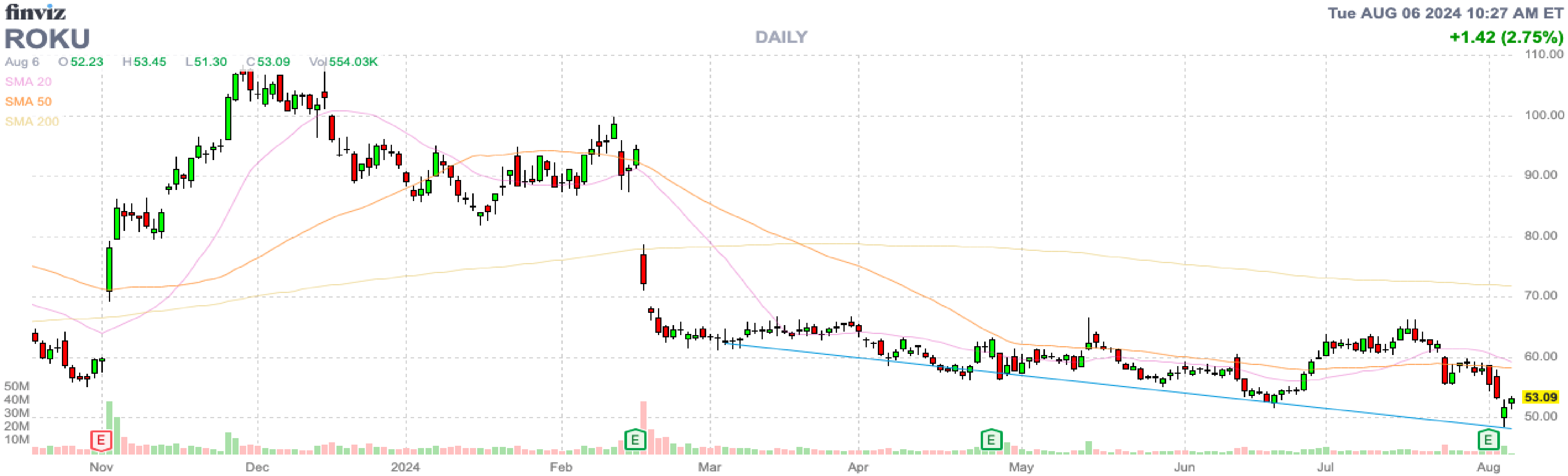
[Impact to the organization/customers]

WAY
Streamed 27.7 billion hours since 2008
Roku®
Happy Streaming™
Streamed 27.7 billion hours since 2008
ROKU
THOMSON REUTERS

Company Impact:

- Roku suffered significant reputation damage and loss of trust.
- The breach made main-stream news and was unavoidable.
- Significant financial costs were incurred to Roku due to customer reimbursement and support costs.
- In addition, Roku also spent significant amounts of money investing in additional and upgraded security measures and equipment.

Roku Stock Affected Due To Cyberattack



- Stock price tanked to almost half price from the Feb 2024 earnings report but was unable to recover from yearly lows through August 2024 due to the Cyberattack In April!!!
- The stock dropped 3% from the cyberattack alone!

[What was done to remediate]

First steps Roku had taken to fixing the problem:

- Company’s image was injured, and customers have lost a lot of trust, but the company is making efforts to right the situation.
- 567,000 Users were affected. All were required to reset their passwords.
- Users are encouraged to use stronger security practices with all their accounts across various platforms.
- Company implemented Multifactor Authorization (2FA) methods to help prevent future attacks by making access more difficult.
- Roku also refunded and cancelled all unauthorized purchases and subscriptions to the affected users.

[What was done to remediate]

Long-term steps Roku implemented to preventing another breach:

- Roku strengthened its monitoring systems to be better equipped at identifying unusual login activity.
- These systems are now more focused on targeting different patterns in credential stuffing and other techniques.
- Roku emphasized the importance on customers adopting stronger security practices for all their accounts.
- This involved creating stronger passwords and using Multifactor Authorization on all their sensitive information.

[Summary]

- The April 2024 Roku breach of 576,000 users accounts demonstrated the importance of why users should not be using the same password across all your accounts.
- The breach was performed by a method known as Credential Stuffing.
- This incident also highlighted the need for users and companies alike to use strong security measures.
- Looking forward, a more enhanced credential stuffing detection coupled with a better user security education could greatly lessen the impact of this type of breach in the future.

Roku Breach References

1. Gatlan, Sergiu. "Roku Breach Hits 567,000 Users." *Wired*, 12 Apr. 2024, https://www.wired.com/story/roku-breach-hits-567000-users/.

2. Lang, Brent. "Roku Breach: Over Half a Million User Accounts Compromised." *The Hollywood Reporter*, 12 Apr. 2024, https://www.hollywoodreporter.com/business/digital/roku-breach-accounts-compromised-half-million-1235872934/

3. Kastrenakes, Jacob. "Roku Discloses Data Breach Incident Affecting 576,000 Users." *CNET*, 13 Apr. 2024, https://www.cnet.com/tech/services-and-software/roku-discloses-data-breach-incident-affecting-576000-users/.

4. "Roku Security Breach: Over Half a Million Accounts Compromised." *National CIO Review*, 12 Apr. 2024, https://nationalcioreview.com/articles-insights/information-security/roku-security-breach-over-half-a-million-accounts-compromised/.

5. "Roku Data Breach." *Twingate*, 13 Apr. 2024, https://www.twingate.com/blog/tips/Roku-data-breach.

6. Horowitz, Julia. "Roku Security Breach: User Accounts Compromised." *CNN Business*, 12 Apr. 2024, https://www.cnn.com/2024/04/12/business/roku-security-breach-user-accounts/.

Images Used - Owner Website Links

*Images are not my creation. I found them through Google search, and the images are the property of their respective owners below. The images can be found on these sites below.

- Slide 1 – https://www.cnn.com/2024/04/12/business/roku-security-breach-user-accounts/index.html
- Slides 2 & 3 – https://ermprotect.com/blog/how-hackers-crack-passwords/
- Slide 4 – https://www.enzoic.com/blog/hack-encrypted-passwords/
- Slide 5 - https://www.indusface.com/blog/credential-stuffing-prevention-how-to-stop-and-mitigate-credential-stuffing-attacks/
- Slides 6 to 8 – https://www.euronews.com/next/2024/05/11/how-long-does-it-take-a-hacker-to-crack-a-password-in-2024
- Slide 9 & 10 – https://www.reuters.com/technology/cybersecurity/roku-says-more-than-500000-accounts-impacted-by-cyber-attack-2024-04-12/
- Slide 11 – https://seekingalpha.com/article/4711413-roku-still-priced-for-disaster
- Slide 12 & 13 – https://www.cleardata.com/costly-healthcare-cyber-threats/
- Slide 14 – https://www.questce.com/8-reasons-why-cybersecurity-should-be-your-1-priority/