CYBERSIXGILL REPORT

CONSCIOUSNESS OF STREAMING

How many Netflix and Disney+ accounts are on the Dark Web?

JUNE 8, 2021

Consciousness of Streaming

EXECUTIVE SUMMARY

- Credentials for popular streaming services, generally harvested through credential stuffing attacks, are shared widely on the forums of the deep and dark web. Threat actors distribute them for free or sell them for several cents apiece. With so many credentials available, we attempted to discover **how many Netflix and Disney+ accounts were shared from January 2020 through March 2021.**

- We calculated the number of accounts that posts advertised to be sharing/selling, as well as the number of unique usernames and passwords that we were able to verify. The former metric can be seen as a maximum and the latter, a minimum, in the count of compromised accounts.

- Our investigation found 805,085 Netflix and 596,502 Disney advertised accounts, corresponding to 0.39% of all Netflix and 0.63% of all Disney+ accounts.

- There were 114,491 Netflix and 106,424 Disney+ verified accounts. This means that **at least 1 out of every 1,650 Netflix (0.061%) accounts and 1 out of every 714 Disney+ accounts (0.139%) were leaked to the deep and dark web in 2020.**

- Both metrics were very volatile from month to month. We attribute this to several factors: Due to COVID lockdowns, the supply and demand for Netflix and Disney+ accounts peaked in March-May 2020, then reverted as the year progressed. Despite a slight uptick in the fall, overall numbers trended downwards as content providers presumably improved defensive measures. Later the numbers dropped precipitously when a popular site for posting credentials went down.

- Ultimately, this study illuminates the supply chain for compromised credentials—from procurement to distribution to consumption. If defenders succeed in disrupting any of these stages, they can frustrate attackers. However, history tells us that the adversary will adapt and develop new tactics, techniques, and procedures. Only continued monitoring and agility will allow security engineers to outwit adversaries when the next round arrives.

INTRODUCTION

In earlier generations, individuals seeking to access in-house entertainment without paying resorted to measures such as illegal cable hookups or downloading mp3s from Napster. Nowadays, as content is delivered on-demand through online streaming services, the only thing preventing an aspiring viewer from reaching massive libraries of content is a legitimate username and password.

How do actors obtain these credentials? While there are many methods of cracking passwords, the primary tactic is *credential stuffing*. In this attack, actors scour massive data breaches for username-password combinations, and then they compile them into *combolists*. Next, actors use automated tools (such as *OpenBullet*) to test these known credentials to login to other types of accounts. Because people tend to recycle passwords, pairings of usernames and passwords revealed in a breach of, for example, a gaming site may also be valid to login to a Minecraft account. Or also, a Paypal account.

Anyone even marginally familiar with the dark web knows that credentials for popular streaming services are tremendously widespread on its forums. Cybersixgill research from earlier this year revealed that OpenBullet configurations targeting Netflix, Hulu, and Disney+ ranked in first, forth, and fifth most-popular, respectively, on the underground in 2020.

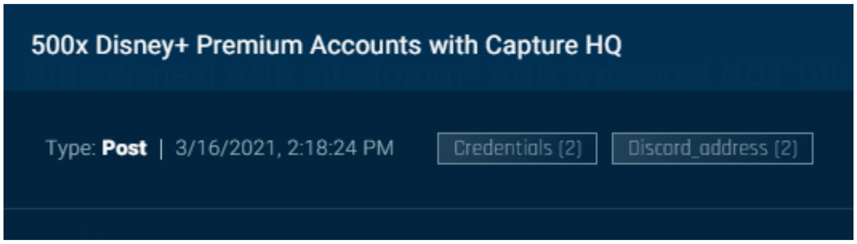
Meanwhile, many threat actors simply share streaming credentials for free, sometimes by the thousands, while others try to sell them for several cents apiece. We should note that the value of these credentials is low in comparison to financial accounts, since a compromised Netflix account cannot be monetized like that of a bank or credit card. Furthermore, the demand is higher: we would presume that many more actors would be comfortable consuming streaming content with stolen credentials than there are actors that would steal money from someone’s bank account.

In this report, we seek to understand just how many Netflix and Disney+ accounts were distributed on the deep and dark web from the beginning of 2020 through the end of 2021 Q1, and then analyze the trends in the numbers.

METHODOLOGY

Our investigation will include three metrics: Account posts, advertised accounts, and verified accounts.

Account posts: A post on an underground forum advertising a specific quantity of streaming accounts, whether for free or for sale. For example, the post below is counted as a single account post:

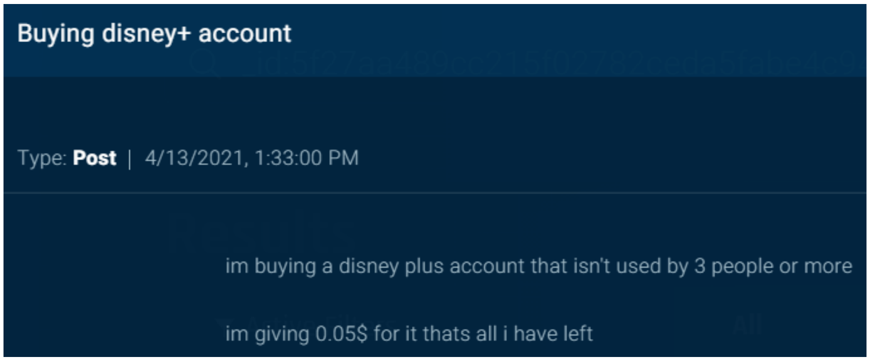


500x Disney+ Premium Accounts with Capture HQ

Type: **Post** | 3/16/2021, 2:18:24 PM

Figure 1: An actor posts 500 Disney+ accounts for free

However, the post below, in which an actor states merely a desire to acquire accounts, is excluded from our count.



Buying disney+ account

Type: **Post** | 4/13/2021, 1:33:00 PM

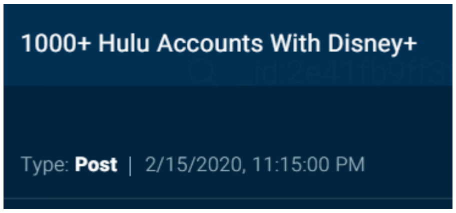
im buying a disney plus account that isn't used by 3 people or more

im giving 0.05$ for it thats all i have left

Figure 2: An actor posts that he is seeking to purchase Disney+ accounts

Similarly, we excluded posts offering gift cards, as well as posts offering tools needed to compromise accounts, such as combos, configs, and proxies.

As a final note, for this study we counted Hulu accounts when they included Disney+ access, such as the post below:

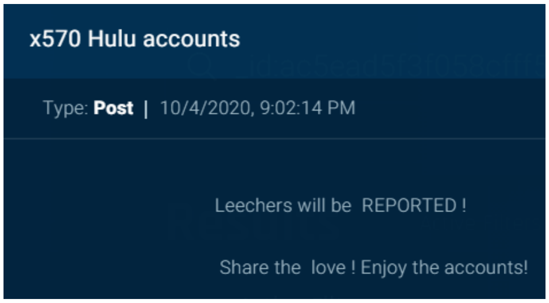


1000+ Hulu Accounts With Disney+

Type: **Post** | 2/15/2020, 11:15:00 PM

Figure 3: 1,000 Hulu accounts, including the Disney+ add-on

However, we disregarded posts in which Hulu accounts were shared but there was no mention of Disney+, such as this:



x570 Hulu accounts

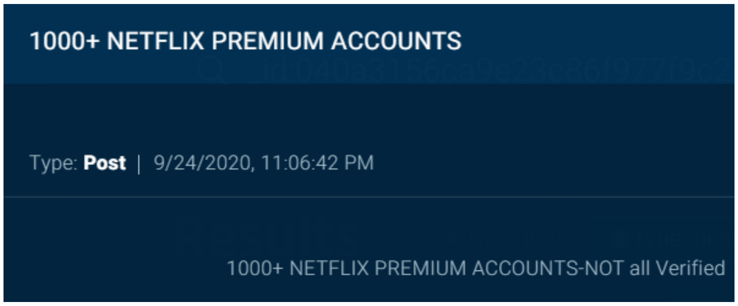
Type: **Post** | 10/4/2020, 9:02:14 PM

Leechers will be REPORTED !

Share the love ! Enjoy the accounts!

Figure 4: 570 Hulu accounts without specifying the Disney add-on

Advertised accounts: This refers to the number of accounts that the post is advertising, sometimes given out for free, while other times, for sale. For example, we would count the post below as 1,000 accounts (even though the actor indicates that they have more than 1,000):



1000+ NETFLIX PREMIUM ACCOUNTS

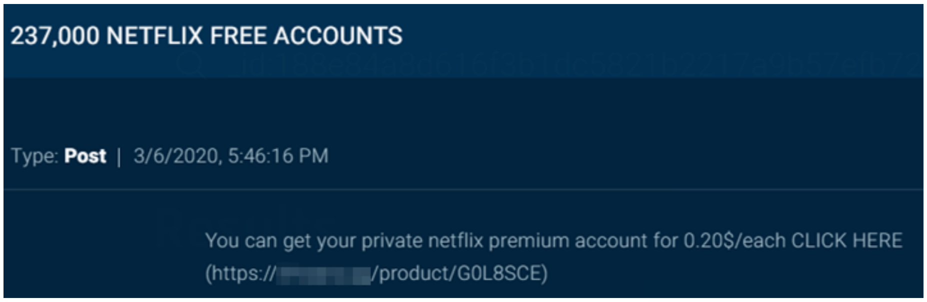
Type: **Post** | 9/24/2020, 11:06:42 PM

1000+ NETFLIX PREMIUM ACCOUNTS-NOT all Verified

Figure 5: A post offering 1000+ Netflix accounts

Actors tend to post several times advertising accounts, so we wanted to avoid counting items that were reposted. Therefore, we removed duplicate posts from within each month.

Finally, we filtered out some outliers—dumps that advertised 20,000 or more accounts. These accounted for a tiny fraction of the overall account posts—one for Disney (35,000 accounts) and twelve for Netflix (averaging at 53,452 accounts)—yet their numbers seriously skewed the data. For example, this post titled "237,000 NETFLIX FREE ACCOUNTS" from March 6, 2020 exceeded the *monthly* totals for advertised Netflix accounts for every other month.



237,000 NETFLIX FREE ACCOUNTS

Type: **Post** | 3/6/2020, 5:46:16 PM

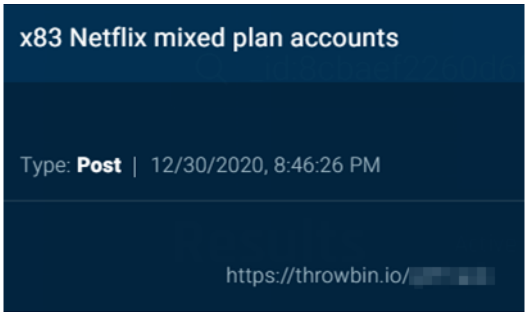
You can get your private netflix premium account for 0.20$/each CLICK HERE (https://[redacted]/product/G0L8SCE)

Figure 6: A mega-dump alleging 237,000 Netflix accounts

<u>Verified accounts</u>: These are accounts for which we succeeded in retrieving the actual account credentials—an email address and password.

The forum posts themselves rarely include compromised credentials, since posts generally have character limits. Rather, actors generally include in the post a link to a paste site, most often Throwbin, but also Pastebin and Ghostbin, where the credentials are actually stored.

For example, this post advertises 83 Netflix credentials. It includes a Throwbin link.



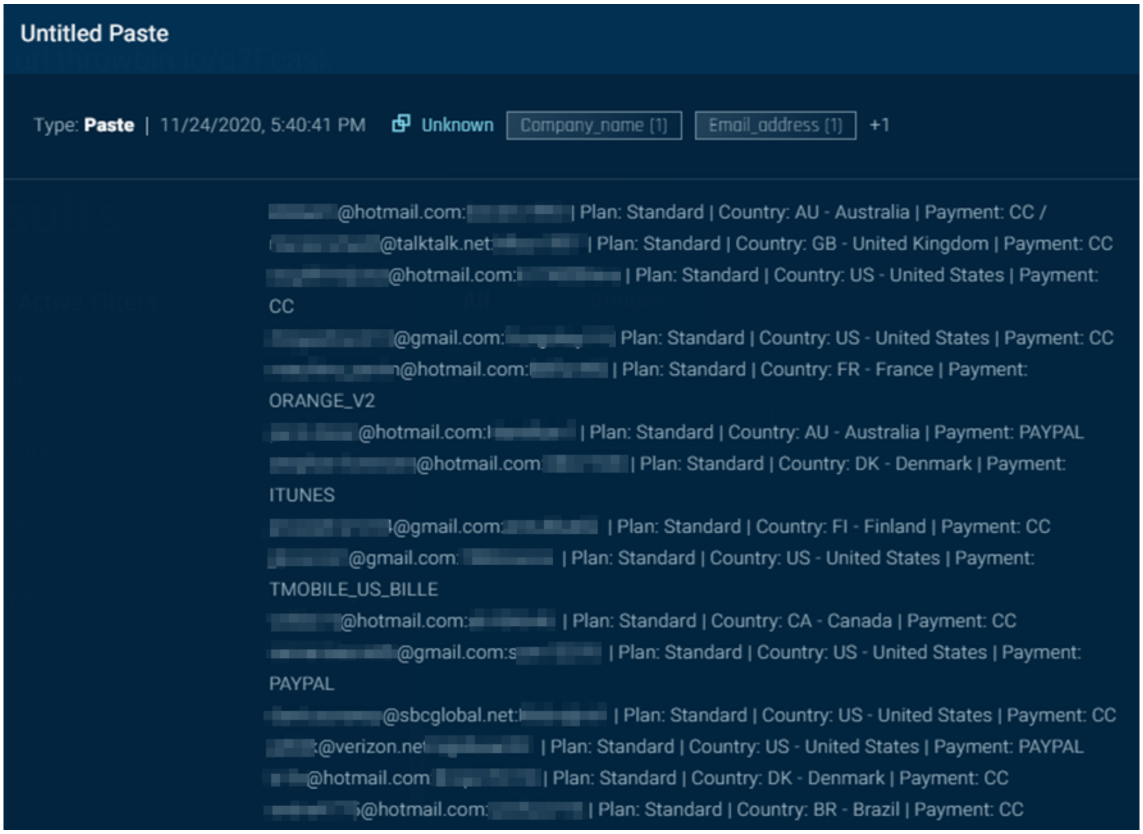
x83 Netflix mixed plan accounts

Type: **Post** | 12/30/2020, 8:46:26 PM

https://throwbin.io/[redacted]

Figure 7: A post advertising 83 Netflix accounts, which are accessible via the Throwbin link

Opening the Throwbin link in Cybersixgill's Investigative Portal (the only way to recover the post's content, since most of these links are taken down after several days), we can view the credentials themselves. For this post, they include the email address, password, account information, country, and payment method. It is important to note that the paste does not even explain what types of accounts these credentials open. Only someone that first saw the link in the forum can know that they are for Netflix.



Untitled Paste

Type: **Paste** | 11/24/2020, 5:40:41 PM

```
[redacted]@hotmail.com:[redacted] | Plan: Standard | Country: AU - Australia | Payment: CC /
[redacted]@talktalk.net:[redacted] | Plan: Standard | Country: GB - United Kingdom | Payment: CC
[redacted]@hotmail.com:[redacted] | Plan: Standard | Country: US - United States | Payment:
CC
[redacted]@gmail.com:[redacted] Plan: Standard | Country: US - United States | Payment: CC
[redacted]@hotmail.com:[redacted] | Plan: Standard | Country: FR - France | Payment:
ORANGE_V2
[redacted]@hotmail.com:[redacted] | Plan: Standard | Country: AU - Australia | Payment: PAYPAL
[redacted]@hotmail.com:[redacted] | Plan: Standard | Country: DK - Denmark | Payment:
ITUNES
[redacted]@gmail.com:[redacted] | Plan: Standard | Country: FI - Finland | Payment: CC
[redacted]@gmail.com:[redacted] | Plan: Standard | Country: US - United States | Payment:
TMOBILE_US_BILLE
[redacted]@hotmail.com:[redacted] | Plan: Standard | Country: CA - Canada | Payment: CC
[redacted]@gmail.com:[redacted] | Plan: Standard | Country: US - United States | Payment:
PAYPAL
[redacted]@sbcglobal.net:[redacted] | Plan: Standard | Country: US - United States | Payment: CC
[redacted]@verizon.ne[redacted] | Plan: Standard | Country: US - United States | Payment: PAYPAL
[redacted]@hotmail.com[redacted] | Plan: Standard | Country: DK - Denmark | Payment: CC
[redacted]@hotmail.com:[redacted] | Plan: Standard | Country: BR - Brazil | Payment: CC
```

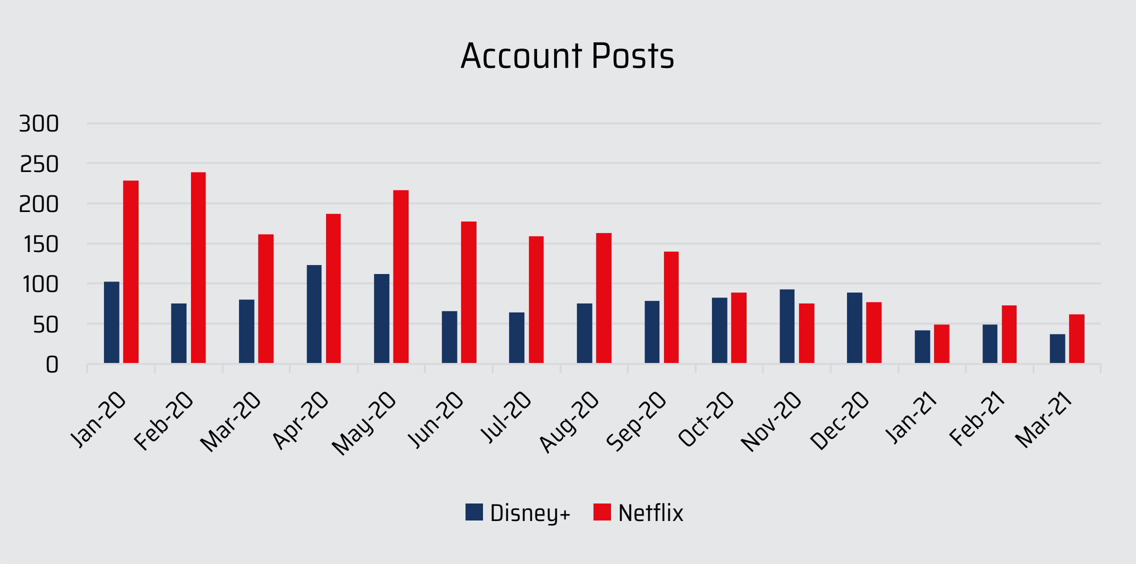
Figure 8: Netflix usernames and passwords on Throwbin

In our research, we extracted the email addresses from pastes linked in account posts. Then, we de-duplicated them to determine the number of unique, verified accounts.

FINDINGS

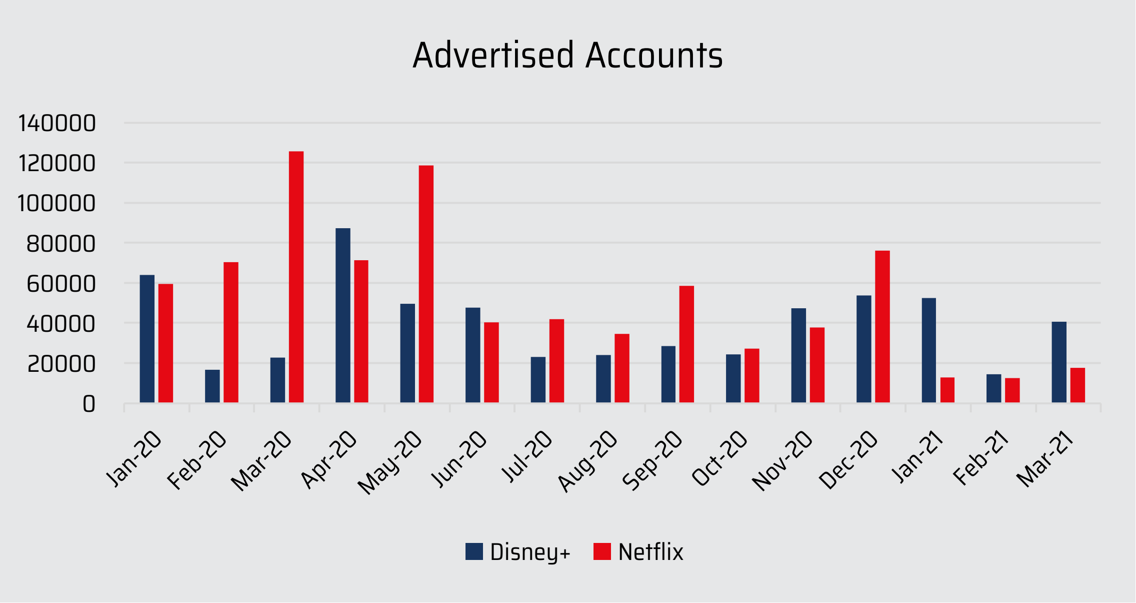
Account posts

During the fifteen months investigated (January 2020 through March 2021), there were 2,095 Netflix and 1,167 Disney+ account posts. Both experienced fluctuations, but Netflix had a much larger range. Furthermore, while Netflix began the year as the prohibitive leader, the number of its account posts declined to the point that it was surpassed by Disney+ in November and December, only to regain the lead in 2021.



Advertised accounts

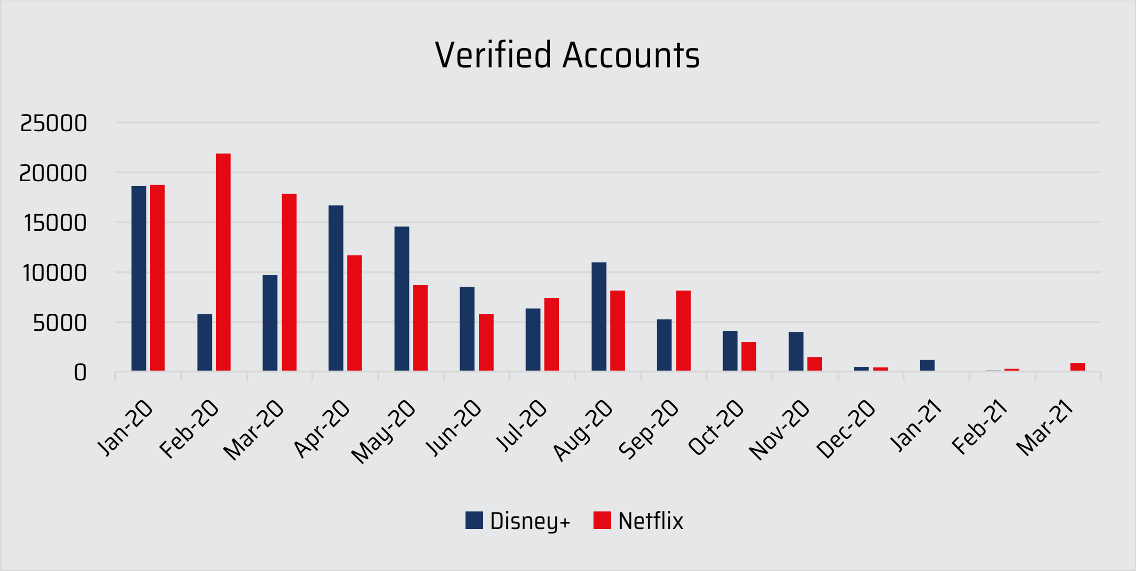
Here, too, Netflix led, with 805,085 advertised accounts, compared with Disney's 596,502. Both peaked in spring, 2020, declined over the summer, then picked up again in the fall (with Disney+ taking the lead in November).



Let's put these numbers in perspective: At the end of 2020, Netflix reported 204 million subscribers[1] and Disney+ had 94.9 million.[2] Therefore, there were advertised accounts corresponding to 0.39% of all Netflix accounts and 0.63% of all Disney+ accounts.

Verified Accounts

The following figures represent the number of verified accounts per month. There was a very sharp decline in the fall of 2020, and then nearly none towards the beginning of 2021.



In total, over these fifteen months there were 106,424 unique, verified Disney+ credentials and 114,491 unique, verified Netflix credentials.

Therefore, we can verify that **at least 1 out of every 1,650 Netflix** (0.061%) **and 1 out of every 714 Disney+ credentials** (0.139%) were leaked to the deep and dark web in 2020.

ANALYSIS

In this study, we examined three metrics—account posts, advertised accounts, and verified accounts. Despite the fact that all three metrics were looking at different data

[1] https://s22.q4cdn.com/959853165/files/doc_financials/2020/q4/FINAL-Q420-Shareholder-Letter.pdf

[2] https://thewaltdisneycompany.com/app/uploads/2021/02/q1-fy21-earnings.pdf

points, they all followed the same rough pattern: the number peaked in March-May, 2020, then declined until the fall, then dropped off precipitously. Head-to-head, Netflix began the year as the leader, but then Disney+ pulled ahead in the fall.

How do we explain the trends in this data? We can offer several reasons that could have influenced why these numbers appeared in this way, looking at arguments for supply and demand.

DEMAND

1. **COVID-19**: As noted in our 2020 annual report, the months of the lockdowns (March-May, 2020) generated an unprecedented spike in actors and posts in underground forums and platforms. Along with this, criminal activity rose in all areas, including hacked gaming store accounts, compromised RDP credentials, money laundering services, and narcotics. It would appear, therefore, that credential stuffing attacks against streaming services followed the same trend, explaining the peaks observed in these months.

2. **Content**: Similarly, the number of accounts may have been affected by the demand for content. Netflix accounts peaked in March and April, when its most-viewed shows, *Money Heist* and *Tiger King*, were released. Disney+ surpassed Netflix in November, just as its leader, the second season of *The Mandalorian*, was released. Could there be a correlation between Baby Yoda and credential stuffing?

3. **Subscription growth:** In 2020, Netflix added 37 million paid subscribers and Disney+ added 68.4 million. On one hand, more subscribers increase potential targets for credential stuffing. On the other hand, many of these new customers may have been individuals that were using leaked credentials, who then decided to pay for their entertainment.

4. **Oversaturation (I):** How many compromised accounts does one need? It is not as if having several Netflix logins unlocks extra content. This, if the market was so

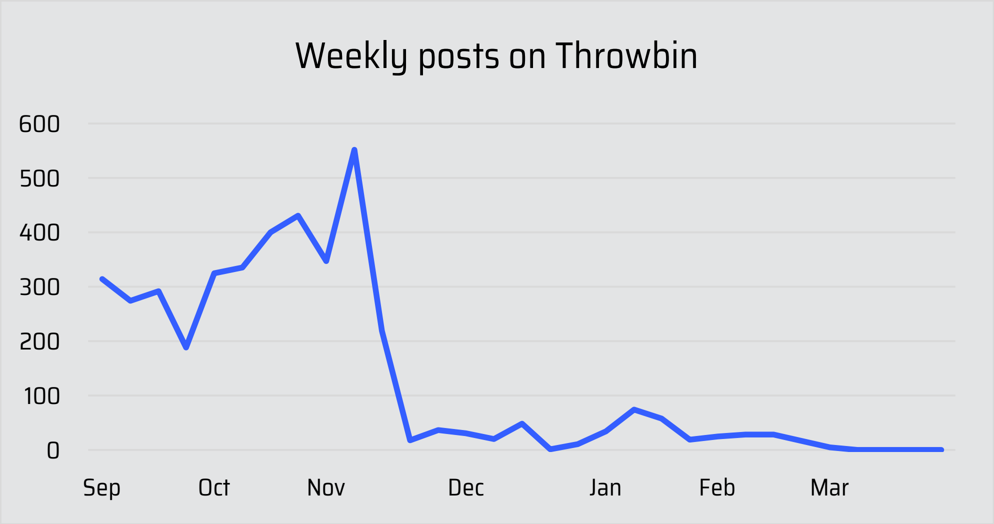
flooded with credentials that anyone who wanted to consume free content could do so, there would be no need to continue finding them.

SUPPLY

1. **Oversaturation (II)**: Since these streaming accounts are difficult to monetize, the main motivation for actors to crack them and distribute for free would be to improve their reputations on forums (i.e., hacker cred). However, if these accounts were too easy to crack, it is no great accomplishment, so actors simply may lose interest in posting them. (We find a parallel to this with Zoom accounts; in the early days of the pandemic, many actors posted cracked Zoom credentials. However, these subsided by the end of April 2020, even as Zoom use intensified.)

2. **Better defense**: On the contrary, perhaps we need to credit Netflix and Disney's security engineers for creating better defenses against credential stuffing tools and for preventing suspicious logins. If it became so difficult for actors to harvest accounts, and if compromised accounts, once used, were shut down quickly, it could have frustrated the market to the point of collapse. Indeed, recent headlines indicate that Netflix has been working on preventing password sharing.[3]

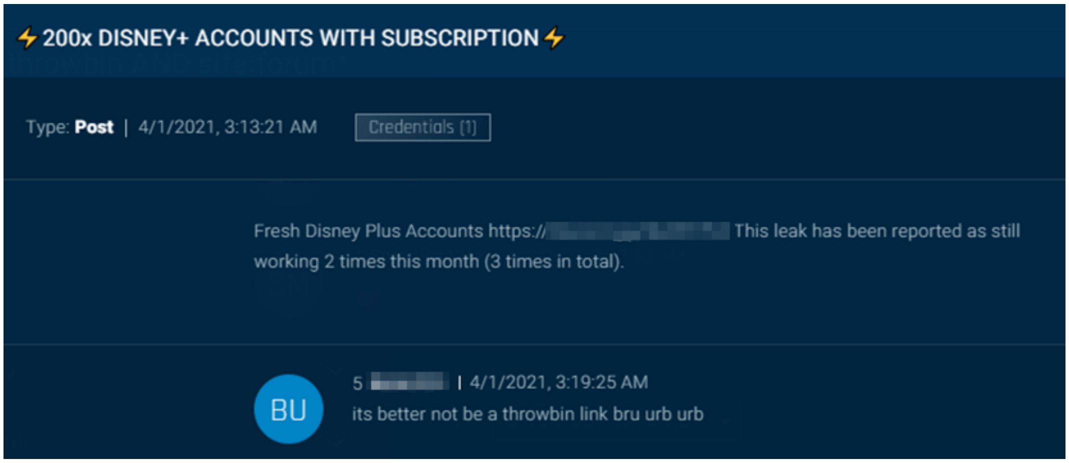
3. **Throwbin**: As mentioned earlier, a majority of the free accounts were posted to Throwbin, a paste site. However, Throwbin activity plummeted in the end of



[3] https://www.theverge.com/2021/3/11/22325831/netflix-password-sharing-test-feature-piracy-security-streaming-video

November. The site experienced many extended outages through February, then went completely down in March. The figure below represents the number of all collected posts from Throwbin from September through the end of March:

Actors complained about Throwbin's disappearance. For example, this actor responded to a post of Disney+ accounts, "its better not be a throwbin link."



⚡200x DISNEY+ ACCOUNTS WITH SUBSCRIPTION⚡

Type: **Post** | 4/1/2021, 3:13:21 AM

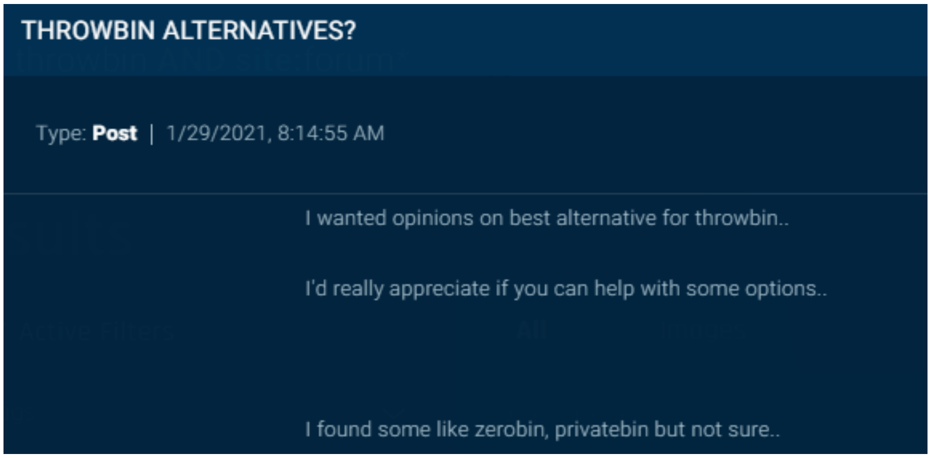
Fresh Disney Plus Accounts https://[redacted] This leak has been reported as still working 2 times this month (3 times in total).

5[redacted] | 4/1/2021, 3:19:25 AM

its better not be a throwbin link bru urb urb

Figure 9: An actor requests that Disney+ accounts are not shared over Throwbin, as the site is down

The absence of Throwbin has left a glaring hole in the supply chain of *all* compromised accounts. Several actors have asked about alternatives, but based on our research, none of them have yet stepped up and filled the void that Throwbin left.



THROWBIN ALTERNATIVES?

Type: **Post** | 1/29/2021, 8:14:55 AM

I wanted opinions on best alternative for throwbin..

I'd really appreciate if you can help with some options..

I found some like zerobin, privatebin but not sure..

Figure 10: An actor seeks Throwbin alternatives

Note that account posts and advertised accounts are down but not out since Throwbin disappeared. A closer look reveals that the majority of advertised accounts are now being sold (as opposed to given away for free) on dark web markets and messaging sites. Indeed, if it becomes harder to give away credentials for free, then perhaps actors can actually sell them for something.

CONCLUSION

We set out to discover how many Disney+ and Netflix accounts were leaked on the deep and dark web in 2020 through 2021 Q1. What is the answer?

Well, it's complicated. Using our verified accounts metric as the floor and advertised accounts as the ceiling, we can estimate that it is between 114,491 to 805,085 Netflix and 106,424 to 596,502 Disney+ accounts.

However, the number of compromised accounts was very volatile from month to month. This demands additional explanation, but with so many factors affecting the number of compromised accounts, interpreting the data trends is not straightforward. Our assessment is as follows:

Due to COVID lockdowns, the supply and demand for Netflix and Disney+ accounts skyrocketed. This reverted quickly due to market oversaturation. As the year progressed, despite a slight uptick in the fall, overall numbers trended downwards as content providers became more effective at preventing compromised credentials from being discovered and used. Meanwhile, the numbers dropped precipitously as Throwbin went down. Through 2021 Q1, the number of freely-shared accounts did not recover.

More broadly, this investigation revealed the steps necessary for account takeover to flourish: First, actors must procure tools—credential stuffers and combolists—and then perform automated login attempts to harvest credentials. Next, there must be some medium for the credentials to be distributed. Finally, consumers of compromised credentials must succeed in using them for personal gain.

From a defender's perspective, this offers several opportunities to frustrate the supply chain. Account providers—whether streaming services or banks—can take measures to disrupt procurement, distribution, and consumption of compromised accounts. This includes preventing password reuse, blocking suspicious login attempts, and requiring more stringent authentication (MFA). They can also monitor distribution channels on the deep and dark web to immediately lockdown any account whose credentials are shared.

In this study, it appears that a mix of factors drastically reduced the number of available Netflix and Disney+ accounts. However, we do not anticipate that this victory is decisive and permanent. History tells us that adversaries will adapt and develop new tactics, techniques, and procedures. In the near future, it is likely that a new site will replace Throwbin. Sooner or later, actors will find a new way to circumvent account protection measures, such as location and hardware spoofing. Only continued monitoring and agility will allow security engineers to detect and outwit adversaries when the next round arrives.