Cyberint

DISNEY+ ACCOUNTS FOR SALE

ON DEEP AND DARK WEB

November 2019

FACTS

The Disney+ video streaming service debuted on November 12, 2019.

- The service is currently available in the US, Canada, and The Netherlands and will also launch in Australia, New Zealand and Puerto Rico on November 19.
- More than 10 million customers signed up for the service within 24 hours since it was launched.
- The hack was first reported on November 16 by ZDNet website[1].

Following multiple reports in the media, CyberInt performed an investigation into the accounts for sale already made available for purchasing on the deep and dark web.

CYBERINT RESEARCH INSIGHTS

Per initial research, the detected accounts for sale appear to be compromised as a consequence of credential stuffing[2].

We've already seen that threat actors have created and are distributing 'configs' for credential stuffing, or account checking, tools that are readily available on the deep and dark web.

Utilizing these nefarious tools, the threat actor can take exposed credentials from other compromises and then test these 'combos' against other online services. As can be seen in the below (figures 1 and 2), using one of these tools with a 'Disney+' config allows the threat actor to gather valid credentials for Disney's streaming service as well as details of their subscription status.

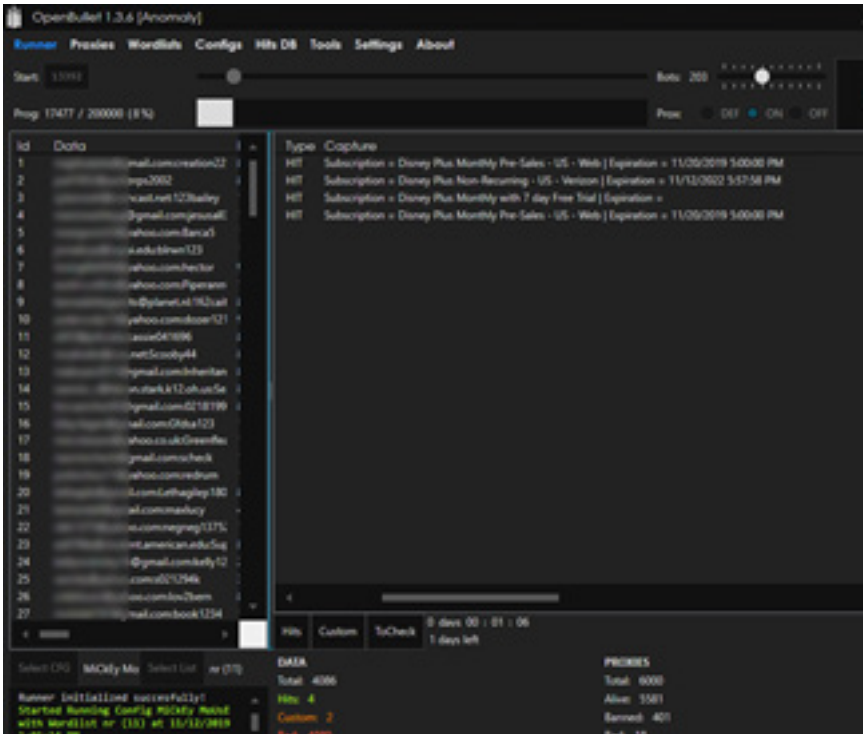


Figure 1 - Credential Stuffing Tool (AKA Account Checker) running a Disney+ config to find valid accounts from a 'combo' list of previously exposed email addresses and passwords

1 https://www.zdnet.com/article/thousands-of-hacked-disney-accounts-are-already-for-sale-on-hacking-forums/

2 Credential stuffing is the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts

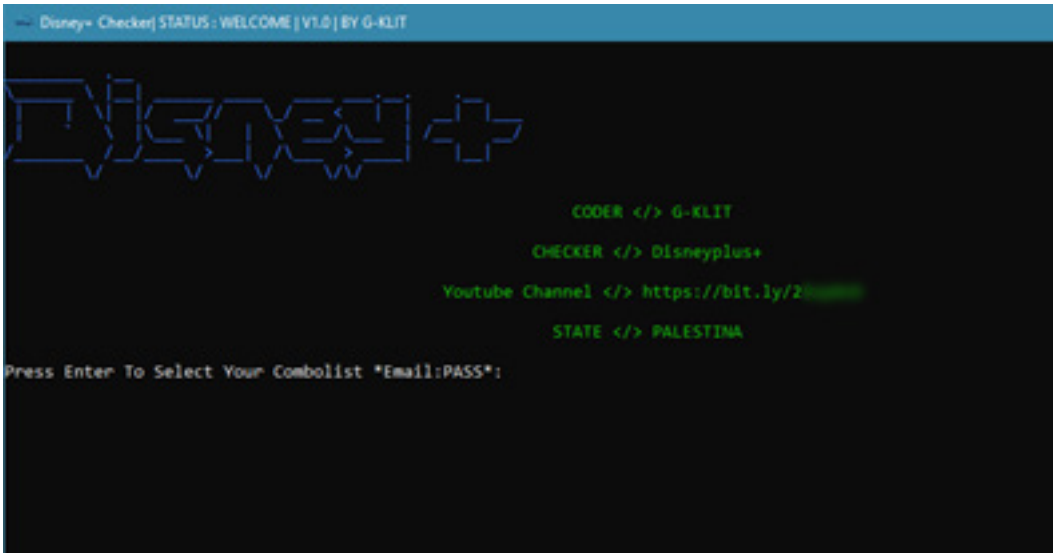
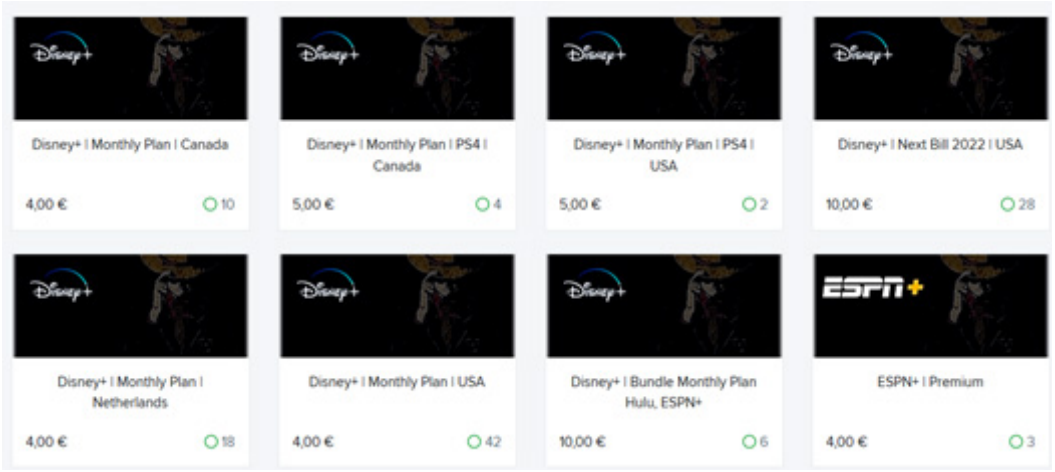
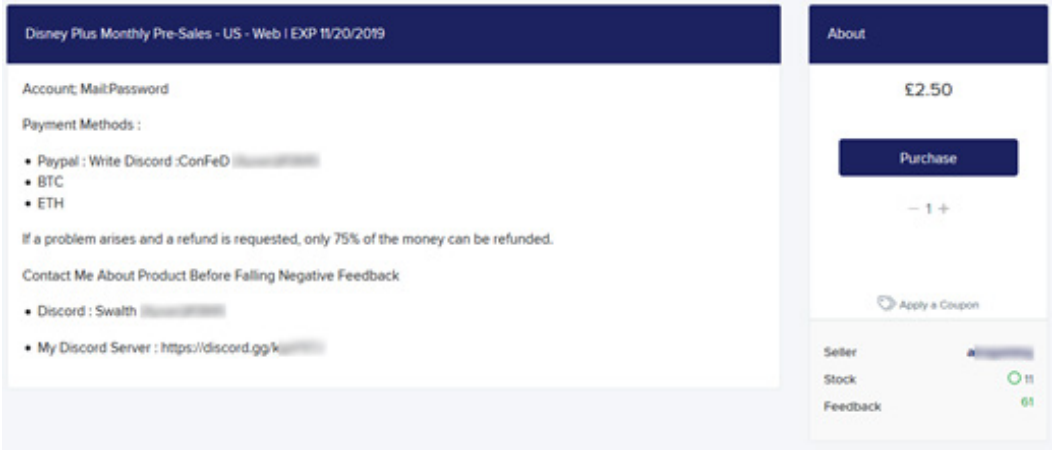


Figure 2 - Disney+ Specific tool freely available to users of an underground forum

Subsequently, these accounts can then be directly abused or resold on various deep and dark web marketplaces (Figures 3 and 4). To thwart detection of this credential stuffing activity, the threat actors utilize a number of proxy servers to mask their true IP address and appear as if the service is being accessed from unique locations.



Figures 3 and 4 - Example sales of compromised Disney+ accounts on multiple deep and dark web marketplaces



RECOMMENDATIONS

- Practice proper password hygiene, and avoid using the same credentials across more multiple accounts, given the credential stuffing attacks that relatively easy to launch and popular amongst low-sophistication threat actor.
- Whilst many may consider having a unique password for each online service to be difficult to manage, password managers simplify this process and allow you to generate and securely store unique difficult-to-guess passwords.
- Complex passwords are reducing the chances of an account being guessed, such as through a brute-force attack, unique passwords provide containment should an online service be compromised through other means and prevent threat actors from using these credentials to access other accounts.
- Where supported by online services, multi-factor authentication, such as being sent a code via text message or using a one-time-password generating app, should always be configured and used to further thwart attacks of this nature.

CONTACT INFORMATION

Cyberint

www.cyberint.com | sales@cyberint.com | The Cyber Feed: blog.cyberint.com

ISRAEL
Tel: +972-3-728677717
Ha-Mefalsim St, 4951447, Kiriat Arie, Petah Tikva

USA
Tel: +1-646-568-7813
214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

UNITED KINGDOM
Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068, London

SINGAPORE
Tel: +65-316-357-6010
Anson Road, #33-04A, International Plaza

LATAM
Tel: +507-395-1553
Edificio Corporativo Cable Onda/TeleCarrier, Panama City