CMSGu2021-02

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on protecting over-the-top (OTT) users from cyberattacks

CERT-MU

National Computer Board
Mauritius

Version 1.0

September 2021

Issue No. 2

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to guide consumers of over-the-top (OTT) streaming services on how they can protect themselves and their families against cyberattacks.

1.2 Audience

The target audience for this guideline is everyone who makes use of over-the-top (OTT) streaming services.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on OTT platforms.

Section 3 explains what makes OTT platforms vulnerable for cyberattacks.

Section 4 describes what users can so to secure their OTT experience.

Section 5 concludes the document.

2.0 Background

Over-the-top (OTT) platforms in today's age have become increasingly popular with the masses and a paradise for content creators. The popularity of these platforms has skyrocketed due to the COVID-19 pandemic. As consumers retreated indoors to stay safe from the novel coronavirus, they turned to Netflix, Disney+, Hulu, and other streaming services.

The downside to this phenomenon is that streaming media services have now caught the attention of cybercriminals. For example, in March 2021, ZEE5 – one of India's leading OTT platforms – was embroiled in a data breach. The breach exposed the personal information of 9 million users, including their names, email addresses, and phone numbers.

Leading OTT service providers, including Netflix, Amazon Prime Video, and Disney+, have also been involved in similar data breaches.

3.0 What makes OTT platforms vulnerable to cyberattacks?

Any cyberattack that results in a data breach could expose sensitive information, including customers' credit card numbers and bank details. Cybercriminals could also access and manipulate the app's source code to collect user data and sell it on the dark web. Apart from jeopardizing user safety through identity theft, such attacks also undermine OTT platform's reputation and credibility. This, in turn, will affect customer trust, increase customer churn, and take a toll on the company's revenue.

3.1 Lack of security for OTT login credentials

Users do not treat their OTT login credentials with the same significance as their online banking details and other sensitive information. They often log into multiple devices and even use the same password to sign-up for different video streaming services.

3.2 Concurrent login

Many users share their login credentials with friends, co-workers, and family members. That makes it easier for cybercriminals to hack into their accounts using various bots and brute force attacks.

3.3 Man-in-the-middle attacks

One of the most dangerous forms of hacking is the "man-in-the-middle" attack. This type of hack intercepts data in transit, and either copies it or modifies it. In some cases, these attacks can be used to impersonate a website or service and steal personal data or content. In the OTT video industry, MITM can result in piracy, stolen trade secrets, leaked medical info, and worse.

3.3. Phishing attacks

OTT platform users are prone to fall prey to phishing attacks. Users can be lured to click on malicious links or access malicious websites.

3.4 Other cyberattacks

Application (App) forgery, reverse engineering, and malware attacks are also known to affect OTT platforms. These attacks can result in loss of revenue.

4.0 How can you make your OTT streaming experience more secure?

4.1 Use strong passwords

Weak, easy to guess passwords, can be exploited by hackers to misuse privileges and impact the OTT service provider's sustainability.

4.2 Do not share login credentials

Various live streaming cloud OTT providers face challenges where concurrent login issues hamper user experience and eventually become a threat. Cybercriminals are exploiting consumer identities of OTT subscribers and are accessing critical consumer information and trying to exploit business data for diverse purposes.

4.3 Always use a secured connection

Using an SSL connection to access OTT services provides end-to-end encryption for enhanced security that protects your personal information.

4.4 Education and awareness

Educate yourself and your surroundings on emerging cyberattacks and best practices for setting strong passwords, for instance.

5.0 Conclusion

The COVID-19 pandemic and consequently the lockdowns in many countries has introduced us to the stark reality of our over dependence and reliance on OTT platforms. The deliberations clearly bring to the dawn that the dependence of people on OTT services is highly treacherous as there is a high probability of its misuse at this point in time. That is why, it is now more than ever essential that consumers of OTT services be aware of common cyberattacks and hence take appropriate measures to secure their own OTT experience.

6.0 References

- www.mondaq.com
- www.mazsystems.com
- www.dacast.com
- https://securityboulevard.com