JOINT ADVISORY BY THE SINGAPORE POLICE FORCE AND CYBER SECURITY AGENCY OF SINGAPORE

SAFEGUARDING AGAINST THE DANGERS OF STREAMING DEVICES

The Singapore Police Force (SPF) and Cyber Security Agency of Singapore (CSA) would like to inform members of the public to be vigilant against the dangers of streaming devices commonly known as Android TV boxes. These Android boxes can be plugged directly to the TV to watch streamed content on their TV screens. It is important for the public to be aware that there are various types of Android TV boxes. Certified Android TV boxes will support official, licensed applications like Netflix and Disney+, while non-certified devices often support illegal streaming sites or distribute malicious applications. If users visit illegal streaming sites or download unofficial applications through their TV boxes, they may be exposed to malware that can compromise their home networks and personal information.

2. Malware present in the affected TV boxes infect users' devices with malicious applications, turning it into part of a botnet - a network of compromised computers used to carry out cyberattacks such as Distributed Denial-of-Service (DDoS) attacks and spam campaigns. The malware also commonly steals users' personal data and users' Internet Protocol (IP) addresses to commit crimes. These include phishing campaigns, spam email distribution, ad fraud and online scams.

3. Users affected by such malware may notice slow device performance, unusual account behaviour, persistent pop-ups, suspicious programmes, and system instability on their devices.

4. It is important to adopt the following precautionary measures to safeguard your personal information and systems against botnets:

a) Use official streaming services e.g. Disney+, Netflix, Prime Video or purchase certified streaming devices from reputable brands like Apple TV 4K, Google Chromecast.

b) Buy products from reputable manufacturers. Well-known reputable manufacturers are more likely to produce devices that are secure, while considering industry standards and best practices for Internet of Things[1] (IoT). Additionally, you can assess a manufacturer's track record in how they manage and how quickly they address security vulnerabilities. You may refer to CSA's website on the Cybersecurity Labelling Scheme (CLS) for consumer smart devices to obtain more information on IoT security.

c) Download applications from official app stores and websites. Refrain from downloading applications from third-party websites, as these applications may contain malicious software that gives cybercriminals access to your personal data and device functions.

d) Certain streaming devices supports the use of anti-virus applications. Ensure that these applications are regularly updated so that they can detect the latest malware. You can refer to the CSA website for the recommended list: https://www.csa.gov.sg/resources/tips-and-resources/recommended-security-apps-list.

5. In the event you suspect that your streaming device is infected by malware, perform the following actions:

a) Disconnect the device from the internet immediately;
b) Run a security scan, uninstall any suspicious third-party apps and check your bank / SingPass / CPF accounts for any unauthorised transaction(s);
c) If malware is detected on your device or there are unauthorised transaction(s), report to the bank, relevant authorities and lodge a police report immediately.

[1] IoT - Smart devices, embedded with sensors, software, and Wi-Fi connectivity that collect and exchange data over the Internet. Some examples are internet cameras, wearable fitness trackers etc.

Do not perform a factory reset before reporting the incident to the police as this could hinder investigations.; and

d) If no malware is detected and there are no unauthorised transaction(s), you may resume usage or choose to perform a full factory reset on the device to be on the safe side.

6. If you believe that your account has been compromised, do the following:

a) Change your password immediately and enable MFA, if available, to secure your account. If you have used the same compromised password for other accounts, those passwords should be reset to prevent unauthorised access.

b) Perform a full system scan with an updated anti-virus software if you have clicked on a phishing link or opened a suspicious attachment in a phishing email.

c) If there are unauthorised transactions detected in your bank account(s) and/or suspicious activities in your Singpass account, report the incident to your bank and/or Singpass helpdesk immediately. Your bank should be able to freeze your bank account as a precautionary measure until investigations are complete.

d) Report the incident to the relevant authorities and lodge a police report at any Neighbourhood Police Post or online at https://eservices1.police.gov.sg. You may also wish to report the incident to SingCERT at https://go.gov.sg/singcert-incident-reporting-form.

7. If you have any information related to a crime or are in doubt, please call the Police Hotline at 1800-255-0000, or submit a report online at www.police.gov.sg/i-witness. If you are unsure if something is a scam, call and check with the 24/7 ScamShield Helpline at 1799.

8. For more information on securing your IoT devices, visit CSA's advisory at https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2024-012/.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
12 NOVEMBER 2025 @ 4.15 PM