Cybersecurity Risks from Illicit Streaming Devices in Taiwan

Paul A. Watters <ceo@cyberstronomy.com>
Cyberstronomy Pty Ltd

Executive Summary

Illicit Streaming Devices (ISDs) are popular in Taiwan and represent a growing threat to revenue for rightsholders due to their key role in enabling piracy. However, they also represent a risk to consumers, due to their potential role in being recruited for malware, and potentially to national infrastructure. A recent study[1] found that ISDs manufactured in the People's Republic of China (PRC) were being used to infect consumers, and to generate revenue through an advertising fraud scheme – around US$24m per year[2]. Recruiting unwitting consumers to participate in these schemes represents a novel money-making opportunity for organised crime.

In this study, we analysed the possible and actual routes by which consumer ISDs could be recruited and utilised for malware attacks in Taiwan. We begin with a theoretical analysis of attack vectors for ISDs, followed by an empirical vulnerability analysis of the most popular ISDs available in Taiwan, and then an attempt to trigger and detect malware infections on these devices through normal consumer operation. In one case study we undertook, 49% of the 67 apps that consumers were directed to download to utilise their device contained malware – for one app, 20 malware detections were triggered when analysed by the industry-leading VirusTotal threat detection system. Our findings suggest that consumers in Taiwan using ISDs remain vulnerable to their devices being remotely hijacked and used to attack other devices and networks globally, and collectively presenting a potential national security infrastructure risk for Taiwan. We conclude by providing three recommendations to address this threat: regulator on the sale and distribution of ISDs; greater enforcement on the ISDs and their associated support services, and; blocking access to the ISDs.

[1] https://www.databreachtoday.com/chinese-criminals-backdoor-android-devices-for-ad-fraud-a-23261

[2] The study was unable to determine whether the malware was inserted during the manufacturing process, or also introduced later in the consumer lifecycle, for example, by downloading an app linked to a fake supply-side as platform. However, it should also be acknowledged that all devices were manufactured in the People's Republic of China.

Table of Contents

Table of Contents

Researcher Biography

Professor Watters is a trusted cybersecurity researcher and thought leader at Cyberstronomy Pty Ltd. He is the author of *Counterintelligence in a Cyber World* (Springer - ISBN 978-3031352867) and *Cybercrime and Cybersecurity* (CRC Press - ISBN 978-1032524511). Professor Watters is Honorary Professor of Security Studies and Criminology at Macquarie University, and a former Adjunct Professor of Cybersecurity at La Trobe University. Professor Watters is a Chartered IT Professional, a Fellow of the British Computer Society, a Senior Member of the IEEE, Member of the ACM, and a Member of the Australian Psychological Society. His work has been cited 9,031 times, with a *h*-index of 43, and an *i*-10 index of 136. He is in the Top 10% of SSRN-cited authors globally and ranked within the top 0.84% of researchers worldwide (all fields) by ScholarGPS.

Acknowledgements

Funding for this research was provided by the Asia Video Industry Association. The work was produced independently by Dr Paul Watters.

Introduction

In this section, we briefly outline the Taiwan cyber threat landscape, and then indicate the potential cyber risks posed by ISDs in Taiwan.

The Taiwan Cyber Landscape

Taiwan, like any other country, faces a range of cyber threats that can impact its government, businesses, and individuals. Some of the main cyber threats to Taiwan include:

- *State-Sponsored Attacks*: Taiwan, due to its political situation, is a frequent target of state-sponsored cyber-attacks, up 80% year-on-year[3]. These attacks can include espionage, data theft, and disruption of critical infrastructure.

- *Espionage and Intelligence Gathering*: Taiwan is a hub for technology and innovation. Other nations or entities may conduct cyber espionage to gain access to sensitive research, development, and industrial information[4].

- *Advanced Persistent Threats (APTs)*: APTs are long-term cyber campaigns conducted by sophisticated threat actors, often state-sponsored[5]. These attacks are highly targeted and focus on stealing sensitive data over an extended period.

- *Ransomware Attacks*: Ransomware attacks involve encrypting a victim's data and demanding payment (usually in cryptocurrency) for its release. Critical infrastructure, government agencies, and businesses (including their supply chains) are at risk of such attacks[6].

- *Distributed Denial of Service (DDoS) Attacks*: DDoS attacks involve overwhelming a target's online services with a flood of traffic, making websites and online services unavailable. These attacks can disrupt government websites, businesses, and even core internet infrastructure[7].

- *Financial Cybercrime*: Taiwan faces threats from cybercriminals attempting to steal financial information, conduct online fraud, scams[8] or compromise banking systems.

[3] https://www.raconteur.net/supply-chain/cyber-attacks-taiwan-semiconductors
[4] https://therecord.media/chinese-hackers-target-taiwanese-organizations-cyber-espionage
[5] https://www.securityweek.com/chinese-backed-apt-flax-typhoon-hacks-taiwan-with-minimal-malware-footprint/
[6] https://edition.cnn.com/2023/06/30/tech/tsmc-supplier-ransomware/index.html
[7] https://focustaiwan.tw/sci-tech/202308160017
[8] https://www.taiwannews.com.tw/en/news/5015605

- *Critical Infrastructure Attacks*: Attacks on critical infrastructure such as energy grids, transportation systems, and communication networks can disrupt essential services and impact national security[9].

- *Phishing and Social Engineering*: Phishing attacks involve tricking individuals into revealing sensitive information or clicking on malicious links. Social engineering tactics are commonly used to target government employees or individuals with access to valuable data[10].

- *Internet of Things (IoT) Vulnerabilities*: With the increasing number of connected devices, Taiwan is vulnerable to attacks that exploit insecure IoT devices to gain unauthorised access to networks or launch attacks[11].

- *Insider Threats*: Insider threats involve individuals within an organisation, such as employees or contractors, misusing their access privileges to steal data, disrupt operations, or facilitate cyber attacks.

To mitigate these threats, Taiwan, like other countries, invests in cybersecurity measures, public awareness campaigns, and collaborations with international cybersecurity organisations, formalised through the National Cyber Security Program of Taiwan[12]. Additionally, individuals and businesses are encouraged to practice good cybersecurity hygiene, regularly update software, use strong and unique passwords, and employ security solutions such as firewalls and antivirus software.

Illicit Streaming Devices (ISDs)

Illicit Streaming Devices (ISDs), also known as "Kodi boxes," "Android TV boxes," or "jailbroken Fire TV sticks," are media streaming devices that have been modified or configured to allow users to access copyrighted content illegally. These devices are typically sold online and more rarely in physical stores, often marketed to cut the cord and access a vast array of movies, TV shows, and live sports without a subscription or the need for authorised streaming services that is to say, illegally. These devices are typically manufactured and/or serviced in the People's Republic of China.

Briefly, these devices typically work using the following components:

- *Hardware*: ISDs are usually small devices that resemble streaming media players such as Roku or Apple TV. They often run on Android operating systems and are equipped

[9] https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html
[10] https://cybernews.com/security/rock-tsai-taiwan-mobile-the-most-significant-cyberthreat-that-organizations-face-today-is-social-engineering-attacks/
[11] https://www.scmagazine.com/news/forescout-says-operational-tech-has-become-constant-target-details-attack-on-taiwanese-ot-devices
[12] https://www.twncert.org.tw/Download/National%20Cyber%20Security%20Program%20of%20Taiwan%20(2021-2024).pdf

with internet connectivity, allowing users to connect them to their TVs via HDMI ports. KKTV is an example of a legitimate streaming service in Taiwan that can be access through a digital set-top box, through Android TV or via Chungwha Telecom.

- *Modified Software*: The key feature of ISDs manufactured in the People's Republic of China is the modified software or apps that come pre-installed or are installed by the user. These apps often include open-source media players, along with various add-ons and plugins that enable access to illegal streaming sources, typically supplied via the People's Republic of China.

- *Illegal Streaming Apps and Add-ons*: ISDs are loaded with unauthorised streaming apps and add-ons that provide access to copyrighted movies, TV shows, live sports events, and other premium content without the necessary licenses or legal subscriptions. These apps scrape content from illegal sources on the internet and make it available to users, sometimes at a cost, essentially enabling piracy.

- *Subscription-Based IPTV Services*: Some ISDs also offer subscription-based IPTV (Internet Protocol Television) services that provide live TV channels, including premium channels, at a fraction of the cost of legitimate cable or satellite subscriptions. These services often include copyrighted content without proper authorisation.

- *User Interface*: ISDs typically have user-friendly interfaces that resemble those of legal streaming devices. Users can navigate through menus, search for content, and play videos, making them accessible to individuals who may not be tech-savvy.

- *Updates and Support*: The sellers of ISDs often provide software updates and customer support (often on WeChat – a social media service operated from the People's Republic of China), making it easier for users to maintain their devices and continue accessing pirated content.

The sale and/or use of ISDs to access copyrighted content without authorisation is illegal in many countries. Purchasing or using these devices to stream copyrighted material without a proper license or subscription constitutes copyright infringement. Additionally, users of ISDs are at risk of encountering malware, viruses, and other security threats, as these devices often lack the security features found in legitimate streaming devices. Law enforcement agencies and copyright holders actively work to identify and shut down operations that distribute ISDs to curb piracy and protect the interests of content creators and the entertainment industry.

Malware and ISDs

Using Illicit Streaming Devices (ISDs) to access copyrighted content illegally exposes users to significant malware risks. Some of the potential malware-related dangers associated with these devices includes:

- *Malicious Apps and Add-ons*: ISDs often come with pre-installed or downloadable apps and add-ons that provide access to pirated content. These apps and add-ons are sourced from unknown and unverified developers, making them susceptible to containing malware. When users install these applications, they might unknowingly download malicious software onto their devices.

- *Phishing Attacks*: Some ISD apps and websites associated with illegal streaming may attempt to steal users' sensitive information through phishing attacks. These fake websites or apps imitate legitimate streaming services or other popular platforms, tricking users into providing their usernames, passwords, or credit card details.

- *Man-in-the-Middle Attacks*: Cybercriminals can exploit vulnerabilities in ISDs to intercept and modify the communication between the device and the server. This allows them to inject malware, advertisements, or malicious code into the streaming content, compromising the security and privacy of users.

- *Ransomware*: Some ISD apps or files may contain ransomware, a type of malware that encrypts files on the user's device and demands payment for their release. Ransomware attacks can result in the loss of important files and documents unless the victim pays the ransom, which is not guaranteed to restore access to the files.

- *Botnets and DDoS Attacks*: Compromised ISDs can be used to create botnets, networks of infected devices controlled by cybercriminals. These botnets can be used to launch Distributed Denial of Service (DDoS) attacks, overwhelming websites or online services with traffic, causing them to become unavailable.

- *Data Theft*: Malware on ISDs can be designed to collect sensitive personal information, such as login credentials, credit card details, or social security numbers. This stolen data can be used for identity theft, financial fraud, or other malicious purposes.

- *Unwanted Adware*: Some ISD apps may contain adware, which bombards users with unwanted advertisements. Adware not only disrupts the user experience but can also lead to further malware infections if users accidentally click on malicious ads.

- *Unpatched Security Vulnerabilities*: ISDs often use outdated or unpatched versions of operating systems and software. These vulnerabilities can be exploited by malware to gain unauthorised access to the device, compromising user privacy and security.

To protect themselves from these risks, consumers are typically strongly advised to avoid using ISDs and opt for legitimate streaming services that offer a safe and secure environment for accessing content. Legal streaming platforms invest in security measures to protect their users and provide a better overall experience while supporting the creators and the

entertainment industry. However, the growth in illicit streaming and related services indicate that many consumers ignore these risks.

Taiwan and ISDs

Taiwan has recently been flagged as a "hot spot" for the use of ISDs[13] by according to the 2024 Special 301 Report on Intellectual Property Protection and Enforcement released by the Office of the U.S. Trade Representative (USTR). This trend is longstanding – a 2024 study by AVIA CAP found that 50% of consumers have used piracy services in Taiwan, and that 12% has used an ISD. Contrary to expectation, the study also found that utilisation of piracy streaming services increased with income. So, if well-heeled, cashed-up consumers in Taiwan are exposing themselves to malware and identity theft, the financial consequences would be higher than if only lower-income groups were accessing content using these services. This makes understanding the pathways that ISDs can be exploited in Taiwan an important research question – not only detecting actual instances of malware on ISDs, but understanding all of the potential attack vectors.

Methods

In this study, we propose two approaches to understanding the cybersecurity risks from ISDs:

1. *Vulnerability Analysis* – "out of the box", do ISDs have vulnerabilities which can be remotely exploited, allowing for Remote Access Trojans (RATs) or other malware to potentially infect the device? The industry standard vulnerability scanner – Tenable Nessus – can be used to identify potential entry points to compromise network and system infrastructure.
2. *Malware Analysis* - "out of the box", do the devices actually contain malware pre-installed, or will malware be downloaded and installed during the setup and configuration process?

Following the data collection and analysis, the overall risks to consumers will be analysed and discussed in relation to regulation and policy in Taiwan.

To answer these research questions, four common ISDs – manufactured in the People's Republic of China - were purchased from Taiwan. All four were confirmed to support the illicit streaming of content.

Results

The results from the two different sets of analyses are reported below.

[13] https://focustaiwan.tw/business/202304270007

Vulnerability Analysis

Tenable Nessus Vulnerability Scanner was used to scan for - and identify - vulnerabilities across the four ISDs[14]. Tenable Nessus is a widely used vulnerability scanner designed to help organizations identify and address security issues in their IT environments. It scans networks, systems, and applications for vulnerabilities such as misconfigurations, outdated software, and potential weaknesses that could be exploited by attackers. Nessus offers comprehensive reports and remediation guidance, helping security teams prioritize risks based on severity. It supports various environments, including cloud, on-premises, and hybrid, and is known for its accuracy, scalability, and ease of use, making it a preferred tool for vulnerability management across industries.

The results indicate that the ISDs examined contained an average 7.75 vulnerabilities. On a positive note, none of the ISDs allowed remote access "out of the box", for example, by enabling access through port 22 for Secure Shell (SSH). However, the ISDs all operated by not having piracy apps installed by default; instructions were included to download these apps after the ISD hardware had been configured. As demonstrated in the next section, this is where the main vulnerability lies.

Nessus operates using a "black box" testing approach, where only externally observable vulnerabilities can be observed. However, internal vulnerabilities may exist which are not externally observable, yet are nonetheless present. This includes the ability to install and execute arbitrary code, which could include malware, as outlined in the next section.

Table 1 - ISD 1 Vulnerabilities

Vulnerability	Interpretation
ICMP Timestamp Request Remote Date Disclosure	The box answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Common Platform Enumeration (CPE)	CPE identified the box runs the Linux Kernel 2.6.
Device Type	Device type was identified as "general-purpose", confidence level 65%.
Ethernet MAC Addresses	MAC address identified A4:7C:48:83:FC:7F
Nessus SYN scanner	It is possible to determine which TCP ports are open. Port 8123/tcp (web) and port 8443/tcp (web) were found to be open. This should be protected with an IP filter.
OS Identification	Linux Kernel 2.6 identified.

[14] https://www.tenable.com/products/nessus

Service Detection	Web server running on tcp/8123/www.
TCP/IP Timestamps Supported	The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Traceroute Information	It was possible to obtain traceroute information.
mDNS Detection (Local Network)	The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. Detected on udp/5353/mdns. Service advertised on port 7896 (adb).

Table 2 - ISD 2 Vulnerabilities

Vulnerability	Interpretation
ICMP Timestamp Request Remote Date Disclosure	The box answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Ethernet MAC Addresses	MAC address identified C4:1C:A6:2F:95:1F.
Traceroute Information	It was possible to obtain traceroute information.
mDNS Detection (Local Network)	The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. Detected on udp/5537/mdns. Should be protected with an IP filter on port 5353.

Table 3 - ISD 3 Vulnerabilities

Vulnerability	Interpretation
ICMP Timestamp Request Remote Date Disclosure	The box answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Common Platform Enumeration (CPE)	CPE identified the box runs the Linux Kernel 2.6.
Device Type	Device type was identified as “general-purpose”, confidence level 65%.
Ethernet MAC Addresses	MAC address identified FC:61:44:D0:F4:51.
Nessus SYN scanner	It is possible to determine which TCP ports are open. Port 5555/tcp WAS found to be open. Should be protected with an IP filter.
OS Identification	Linux Kernel 2.6 identified.
TCP/IP Timestamps Supported	The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.
Traceroute Information	It was possible to obtain traceroute information.
mDNS Detection (Local Network)	The remote service understands the Bonjour (also known as ZeroConf or mDNS) protocol, which allows anyone to uncover information from the remote host such as its operating system type and exact version, its hostname, and the list of services it is running. Detected on udp/5353/mdns. Service advertised on port 5555 (adb). Should be protected with an IP filter on port 5353.

Table 4 - ISD 4 Vulnerabilities

Vulnerability	Interpretation
ICMP Timestamp Request Remote Date Disclosure	The box answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted

	machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols.
Ethernet MAC Addresses	MAC address identified A8:43:A4:9984:47.
Ethernet Card Manufacturer Card Detection	China Dragon Technology Limited
Traceroute Information	It was possible to obtain traceroute information.

Malware Analysis

Using ISD 4 as a case study, instructions were followed to install apps so that pirated content could be viewed. The user is prompted in the instructions to open a web browser using the ISD, and to download the desired apps from https://6868c.cc/. This site has 67 apps available for download; each app is installed using an .apk file, which is then downloaded from yet another site https://appres.1357c.cc/. Note that both the domains have private registration, with DNS supported by the Cloudflare CDN.

Each .apk file was downloaded, and then uploaded to VirusTotal cyber threat detection system. VirusTotal (owned by Google Inc) analyses suspicious files to detect malware, by combining the results of more than 75 independent antivirus scanners. It is the industry "gold standard" to detect malicious software, and provides a range of outputs, including malware family types, mapping to MITRE ATT&CK, and sandboxing to observe real-time infection outcomes.

From the 67 .apk files, 157 total malware detections were reported, with an average 2.34 detections per .apk file. The range of detections was between 0-20 per .apk file, with 49% of all .apk files containing malware. In other words, there was a roughly even chance of each .apk file containing at least one malware sample.

A typical example output is shown in Figure 1 for the app "饭团TV(会员版)". While some independent malware detections have identified the same family (eg, Styricka), there are numerous unrelated detections, including SecAPK.401187, Evo-gen[Tri], Riskware.Agent.BOK, SMForw.AA.gen!Eldorado, SmsReg.CH, Generic/Z.77708D!tr, Trojan (00532d071), smforw.ff, Artemis!7E480DFDB98C, and so on. A mapping to the MITRE ATT&CK framework was then performed. The MITRE ATT&CK framework is a globally recognized knowledge base that catalogs adversary tactics, techniques, and procedures (TTPs) used in cyberattacks. It provides a detailed matrix that maps how attackers progress through various stages of an attack, from initial access to data exfiltration, highlighting the specific techniques they use. The framework is designed to help organizations understand and defend against real-world cyber threats by providing a common language for security teams, threat hunters, and incident responders to assess vulnerabilities, identify attack patterns, and develop stronger defenses. It is widely used in cybersecurity for threat intelligence, adversary emulation, and enhancing defensive strategies through red and blue team exercises.

The following tactics and techniques were identified:

- Discovery (TA0007)

- Command and Control (TA0011)
- Defence Evasion (TA0030)
- Discovery (TA0032)
- Impact (TA0034)
- Collection (TA0035)

The Command and Control (TA0011) capability is especially worrying, since it allows the ISD to be remotely controlled from a Command and Control (C2) server. These C2 servers lie at the heart of the Mirai botnet and other advanced persistent threats.

The relevance of the Mirai botnet to Taiwan stems from its role in significant cyberattacks, including Distributed Denial of Service (DDoS) attacks that have targeted critical infrastructure and organizations worldwide, including those in Taiwan. Mirai, which compromises IoT devices to form large botnets, has been used in politically motivated cyber operations, particularly in regions facing geopolitical tensions like Taiwan. Given Taiwan's strategic importance and its strained relations with certain nation-states, Mirai's capabilities raise concerns about cyber warfare and national security, as its attacks can disrupt communication, financial systems, and other essential services. Taiwan's focus on strengthening its cybersecurity defenses is in part a response to threats from botnets like Mirai that are capable of launching large-scale, coordinated attacks.

In terms of Android permissions, the app is able to read and write external storage, mount and unmount filesystems, install new packages, access the internet, access and change the Wi-Fi state and change system settings. Nine of the domains contacted by the app are from the PRC, alongside 3 of the IP addresses. The “su” shell command is also used by the app to obtain “superuser” permissions, i.e., full-control of the device. A full analysis of the app can be reviewed at the VirusTotal website[15].

The malware detections for each app are shown in Appendix A; the reader can independently verify the presence of malware using the URLs provided.

15 https://www.virustotal.com/gui/file/c3010cc7c057fcae595bf254822e025c466c1ce6d8a514303f17609893d3dbd4/summary

AhnLab-V3	PUP/Android.SecAPK.401187
Avast-Mobile	Android:Evo-gen [Trj]
Avira (no cloud)	SPR/ANDR.Styricka.SRDO.Gen
BitDefenderFalx	Android.Riskware.Agent.BOK
Cynet	Malicious (score: 99)
Cyren	AndroidOS/SMForw.AA.gen!Eldorado
ESET-NOD32	A Variant Of Android/Styricka.C Potentially Unsafe
F-Secure	Riskware:Android/SmsReg.CH
Fortinet	Android/Generic.Z.77708D!tr
Google	Detected
Ikarus	PUA.AndroidOS.Styricka
K7GW	Trojan (00532d071)
Lionic	Riskware.AndroidOS.Styricka.z!c
MaxSecure	Android.smforw.ff
McAfee	Artemis!7E480DFDB98C
McAfee-GW-Edition	Artemis
Microsoft	TrojanSpy:AndroidOS/SMforw.E
QuickHeal	Android.Styricka.GEN39443
Symantec Mobile Insight	AppRisk:Generisk
Trustlook	Android.PUA.General

Figure 1 – Malware Analysis of “饭团TV(会员版)” app

Summary

In summary, this study provides clear and independently verifiable evidence that ISDs in Taiwan have both the capacity to be infected by malware, operating with the highest operating system privileges, and that malware is routinely present in apps installed on these devices. The study also showed that ISDs have a number of external vulnerabilities which could be used to construct an attack; however, given the visible and frequent presence of malware operating with the highest operating system privileges – and being flagged as exploitable using MITRE ATT&CK criteria for Command and Control (c2) server penetration, there is really no need for an attacker to devise any exotic approaches. The infrastructure is clearly compromised in a very serious way.

What do these results mean for the security of cyber infrastructure in Taiwan? Put simply, every ISD in Taiwan represents an opportunity for an attacker to control a very large number of households. These nodes can be coordinated through one or more malicious c2 servers, by bad actors who have the mechanism to control the delivery and installation of software on the devices. In the ISD 4 case study, this means the registrants of the domains 6868c.cc and 1357c.cc. Unfortunately, the .cc domain is ranked by the Internet Watch

Foundation (IWF) as one of the top 10 most-abused top-level domains[16], and previous attempts to reduce the levels of abuse have been somewhat unsuccessful. Confusingly, the .cc TLD was created for Cocos (Keeling) Islands, which are an external Australian territory, but it appears that Australia has no control over the domain. The prospects of uncovering the bad actors behind the insertion of malware into ISD apps remains slim. What, therefore, can Taiwan do to protect the ISD infrastructure, and reduce the risk of ISDs being misused? There are three main strategies recommended in this report.

Firstly, Taiwan could consider further regulations on the sale and distribution of ISDs. Most modern, legitimate streaming services do not require the purchase of an ISD, therefore, there is little to be gained from allowing the market to continue. Secondly, the government should expand intelligence-led law enforcement to track and monitor the domains and internet hosts involved in the distribution of ISD malware. This would allow the uncovering of malicious domains like those listed in this report. The risk is that in identifying one, the operators would simply move to another, creating a "whack a mole" scenario. However, measures to control access implemented in other jurisdictions – such as regulatory site blocking – have been provably effective in risk reduction. Thirdly, after identifying these domains, even if prosecution proves difficult, Taiwan could consider blocking access to these domains through site blocking, and/or displaying a warning message to users who try to access the web pages. This approach has been provably successful in deterring other types of cybercrime online.

Of course, consumer awareness, training and education remain critically important to highlighting the risks. The challenge is to persuade users who may believe that illicit subscription services are not just bad for the creative industries (as outlined in the Introduction), but also represent a security risk for themselves and their families. Furthermore, consumers need to understand the collective effect of tens of millions of malicious devices being coordinated en-masse – an almost perfect cyber weapon that could be deployed for DDoS attacks. This is not just a theory – the recent infection of ISDs with the Mirai botnet[17] show that there is a clear and present danger to Taiwan's national security from these devices.

[16] https://www.theguardian.com/australia-news/2021/jun/08/australia-urged-to-take-control-of-cocos-cc-internet-domain-to-foil-scammers-and-child-abuse-sites

[17] https://www.bleepingcomputer.com/news/security/mirai-variant-infects-low-cost-android-tv-boxes-for-ddos-attacks/

Appendix A – VirusTotal App Analysis

APK File	App Name	Malware Detections
1528282807946.apk	Chrome	0
1538058612531.apk	完美视频	9
1538310022746.apk	千寻VIP破解版	1
1544685172790.apk	锋彩直播	3
1544687093440.apk	电视家	6
1564111363848.apk	IQQI	0
1572833067150.apk	RSS Player	1
1577959342411.apk	Watch Me	0
1582118507064.apk	MX Player	0
1582684450103.apk	INDOSIAR TV	1
1584081805772.apk	Aptoide TV	0
1591612025671.apk	超级直播	6
1591612127033.apk	大视界TV	10
1592195305188.apk	Baidu TV Input	0
1614337139875.apk	X Cinema	0
1614337221584.apk	X Channel	0
1619584274267.apk	TED	0
1622018553984.apk	饭团TV(会员版)	20
1622018872838.apk	极光影院TV	2
1622019058251.apk	片库TV	9
1629686618545.apk	Shafa Market	1
1644577566784.apk	Trust DNS	0
1644844135726.apk	SmartTubeNext	0
1649757818822.apk	谷歌注音輸入法	0
1649763787690.apk	Emotn Store	0
1654077297726.apk	Malaysia Live	5
1654078529952.apk	HK Live	4
1654078599282.apk	Indonesia Live	4
1654135158908.apk	Luca Kids	4
1655175608562.apk	WeTV	0
1656925235978.apk	搜狗输入法TV版	0
1663750628753.apk	小鸡模拟器TV版	0
1663828635470.apk	Luca VOD	3

1663932597885.apk	Luca TV	4
1666266110640.apk	Indonesia VOD	4
1666266148211.apk	Malaysia VOD	5
1669695669173.apk	Vidio	0
1673522949023.apk	Smart YouTube TV	0
1675233788445.apk	Youtube Kids	0
1676884472478.apk	Spotify	0
1677466161464.apk	Internet Speed Test -	3
1677470899210.apk	今日影视	10
1678435014188.apk	moretv	0
1679051090931.apk	云视听小电视	0
1681957647098.apk	STN Beta	0
1682480284385.apk	泥视频TV	0
1682503485387.apk	当贝市场	1
1685365426402.apk	Air Screen	0
1685950637157.apk	Cinema HD	0
1686641133043.apk	Keep	0
1692673819942.apk	金星点播	0
1692673893590.apk	金星直播	0
1692678042150.apk	UPLive	12
1692678082921.apk	UP影視	8
1692678800574.apk	UPTV	10
1693197721489010.apk	Transocks	2
1694763859837.apk	Yogurt TV	1
1695382015811.apk	Yogurt Kids	1
1695386977234.apk	阖家欢	3
1695391005086.apk	Cherry TV	1
1695391162542.apk	Yogurt Malaysia	2
1695391434130.apk	Yogurt Indonesia	1
1695643487944.apk	Youtube	0
1698207262159.apk	芒果TV	0
1698207573020.apk	QQ音乐	0
1698915380708.apk	Disney+	0
1698915721125.apk	Netflix	0