Pre-loaded Malware on Android TV Boxes: A Threat to Consumer Security and Cybersecurity Infrastructure

Jawaid Iqbal
Faculty of Computing
Riphah International University
Islamabad, Pakistan
Jawaid.Iqbal@riphah.edu.pk

Osama Khalid
Faculty of Computing
Riphah International University
Islamabad, Pakistan.
osamakhankhalid@gmail.com

Sardar Muhammad Zeeshan Khan
Faculty of Computing
Riphah International University
Islamabad, Pakistan
Zeshankhan1996@hotmail.com

Muhammad AbdulRehman
Faculty of Engineering and Applied Sciences
Riphah International University
Islamabad, Pakistan
mabdul.rehman@riphah.edu.pk

***Abstract*—This article delves into an investigation concerning the existence of preloaded malware on widely used Android TV boxes produced by AllWinner and RockChip, which can be purchased from Amazon and Daraz. The study reveals significant concerns regarding consumer security and the overall cybersecurity infrastructure. The specific malware, known as the BianLian family variant, is responsible for infecting the affected devices and incorporating them into a botnet for the purpose of launching coordinated attacks. Furthermore, the malware has been designed to generate revenue through ad-click fraud. The presence of malware on various models, including the AllWinner T95, AllWinner T95Max, RockChip X12-Plus, and RockChip X88-Pro-10, has been independently confirmed by security researchers Daniel Milisic and Bill Budington. These findings highlight the urgent need for improved security measures and increased awareness among consumers to protect against such threats.**

***Index Terms*—Android TV Box, Pre-loaded malware, cybersecurity infrastructure, botnet, clickbot, malicious activity.**

I. INTRODUCTION

This comprehensive research paper delves deep into an extensive investigation aimed at meticulously examining the presence of preloaded malware on highly popular Android TV boxes manufactured by industry-leading companies, AllWinner and RockChip. These Android TV boxes, widely available for purchase on the Amazon e-commerce platform, have gained immense popularity among consumers due to their affordable pricing and diverse range of features. However, this study unravels a multitude of significant concerns that cast a shadow over consumer security and the broader cybersecurity infrastructure [1]. The focal point of this research revolves around identifying and analyzing the insidious malware that has been discovered on these Android TV boxes. Specifically, the study uncovers a variant of the notorious BianLian malware family that has been found to be surreptitiously embedded within the devices. This highly sophisticated malware exhibits a range of alarming behaviors, including the covert integration of affected devices into a formidable botnet, enabling the orchestration of coordinated attacks with potentially far-reaching consequences. Such attacks can encompass various nefarious activities, including but not limited to distributed denial-of-service (DDoS) attacks, data exfiltration, and remote access to compromised devices. Furthermore, the primary objective of this insidious malware is to generate illicit revenue through the exploitation of ad-click fraud schemes. By covertly hijacking legitimate advertising platforms and manipulating user interactions, this malware maliciously generates fraudulent ad clicks, leading to financial gains for the perpetrators while causing financial losses for advertisers. The significant financial implications of such ad-click fraud underline the importance of combating these malicious activities and safeguarding the integrity of digital advertising ecosystems. To validate the presence and impact of this preloaded malware, esteemed security researchers Daniel Milisic and Bill Budington conducted rigorous analyses and verifications on multiple Android TV box models, including the widely used AllWinner T95, AllWinner T95Max, RockChip X12-Plus, and RockChip X88-Pro-10. Through their meticulous efforts, they confirmed the existence of the BianLian malware variant on these devices, leaving no doubt about the gravity of the situation [2]. The findings of this research paper present a clarion call to both consumers and the broader cybersecurity community to address the pervasive threats and vulnerabilities associated with these Android TV boxes. The implications of this research underscore the urgent need for robust security measures, both at the individual user level and within the consumer electronics industry as a whole. Additionally, this study highlights the imperative for heightened awareness,

proactive defense mechanisms, and collaborative efforts to protect users from evolving cyber threats and to establish a resilient cybersecurity landscape for the future.

A. *Contribution*

The profound impact of Android TV boxes on the realm of home entertainment cannot be overstated. These devices have transformed the way consumers experience multimedia content, providing them with affordable and versatile streaming options that cater to their diverse preferences. However, the groundbreaking research conducted by esteemed security researcher Daniel Milisic has uncovered a deeply disconcerting trend that demands immediate attention: the pervasive presence of preloaded malware on the very Android TV boxes that have become a staple in countless households. Shockingly, these malware-infected devices are being sold by reputable manufacturers such as AllWinner and RockChip, thereby casting doubt on the reliability and security of widely available Android TV box models. The implications of this discovery are far-reaching and raise significant concerns regarding consumer security and the broader cybersecurity infrastructure that surrounds these devices. As consumers increasingly rely on Android TV boxes for their home entertainment needs, it is imperative that comprehensive measures are undertaken to mitigate the risks posed by this preloaded malware, safeguard user privacy, and fortify the overall cybersecurity ecosystem. The findings of this research serve as a clarion call to both manufacturers and consumers, urging them to prioritize robust security practices, heightened awareness, and proactive defense mechanisms to ensure a safe and secure environment for enjoying the benefits of Android TV boxes without compromising personal security or falling victim to malicious cyber activities.

B. *Paper Organization*

Section 1 contains introduction: This comprehensive research paper delves deep into an extensive investigation aimed at meticulously examining the presence of preloaded malware on highly popular Android TV boxes manufactured by industry-leading companies, AllWinner and RockChip. Section 2 contains contribution: How Andriod Tv boxes manufactured by AllWinner and RockChip gave many people around the world a versatile way to experience multimedia content and a security researcher Daniel Milisic uncovered a malware that has been implanted in the Andriod tv boxes. Section 3 contains literature review: Investigation of Security Researcher Daniel Milisic on Andriod Tv Box after buying it from the reputable online marketplace. Section 4 contains proposed schema: Daniel Milisic investigated by shown the world by hand on testing through various methods, i.e. Purchase and initial testing, Network Analysis, Payload Extraction and Analysis etc. Section 5 contains reasons and discussions: Validation of Daniel Milisic findings through various techniques. Section 6 contains findings: Evidence of the malware existence in the Andriod TV box. Section 7 contains recommendations: How to stop the malware, or services that are helping this malware to run. Section 8 contains conclusion: The research conducted by Daniel Milisic sheds light on the intricate nature of malware analysis and the challenges faced in identifying and mitigating threats. Section 9 contains future work: Educate users about the risks of preloaded malware on AllWinner T95 Device and provide guidance on how to protect themselves.

II. LITERATURE REVIEW

Milisic's investigation began after acquiring an AllWinner T95 Android TV box from a reputable online marketplace, only to discover it was infected with malware Astonishingly, this device was labeled as an "Amazon Choice," indicating its popularity and high ratings among consumers. Motivated by this disconcerting experience, Milisic delved deeper into the issue to assess the scale and implications of the preloaded malware [3]. Milisic's research uncovered a vast botnet composed of very large number of AllWinner T95 Device worldwide have been infected, all of which are connected to a central command-and-control server. The malware, known as clickbot, operates surreptitiously in the background, engaging in ad-click fraud to generate illicit revenue. When AllWinner T95 Device that are compromised are activated, they establish communication with the command-and-control server, receive instructions, and download additional payloads to execute the ad-click fraud. Further validation of Milisic's findings came from security researcher Bill Budington, who independently purchased both an AllWinner T95 Android TV box and a RockChip TV box. Budington's investigation corroborated the presence of preloaded malware on these devices, highlighting the AllWinner T95Max, RockChip X12-Plus, and RockChip X88-Pro-10 models as additional culprits [4]. The implications of this discovery are far-reaching. Consumers who unwittingly purchase these comrpomised AllWinner T95 Device expose themselves to potential privacy breaches, as the malware operates silently in the background, collecting sensitive information and executing malicious activities. Moreover, the widespread availability of these compromised devices presents a danger to the security and stability of the internet itself, as they can be leveraged for coordinated attacks within the botnet [5]. The objective of this Research Paper to bring the light on the threat posed by preloaded malware on AllWinner T95 Device and its impact on consumer security. By examining Milisic's findings and analyzing the implications of these discoveries, we seek to raise awareness about the need for enhanced security measures and stricter accountability for both manufacturers and online marketplaces [6]. Additionally, we will explore potential countermeasures and recommendations to protect consumers from the inherent risks associated with these compromised devices.

III. PROPOSED SCHEMA

Daniel Milisic conducted an extensive investigation to uncover the presence of preloaded malware on Android TV boxes. His methodology involved a combination of hands-on testing, network analysis, and collaboration with other security

researchers to validate his findings. The following steps outline the key aspects of his research methodology:

A. PURCHASE AND INITIAL TESTING

Milisic acquired an AllWinner T95 Android TV box from a reputable online marketplace. He then proceeded to set up and activate the device, observing its behavior and functionality. During this initial testing phase, Milisic identified suspicious activities and indications of malware presence.

B. NETWORK ANALYSIS

To gain a deeper understanding of the malware's behavior and impact, Milisic utilized network analysis tools and techniques. He monitored the device's network traffic, focusing on DNS requests and communications with command-and-control (C&C) servers. This allowed him to trace the malware's activities and identify potential sources of infection and control.

C. PAYLOAD EXTRACTION AND ANALYSIS

Milisic successfully extracted a Stage-1 payload from the malware-infected Android TV box. This payload served as crucial evidence for identifying the specific malware variant and its capabilities. He further analyzed the payload to understand its functionality and potential impact on user devices and networks.

D. COLLABORATION AND VALIDATION

To ensure the credibility of his findings, Milisic collaborated with Bill Budington (Security Researcher), who independently purchased both an AllWinner T95 Android TV box and a RockChip TV box. Budington's independent research confirmed the presence of preloaded malware on these devices, adding weight to Milisic's discoveries.

E. CONTACTING SERVICE PROVIDERS

Milisic reached out to Linode, a hosting service provider that was unknowingly hosting some of the C&C servers associated with the malware. Despite initially encountering challenges in reporting the abuse, Milisic persisted and eventually engaged with a Linode representative who took action to terminate the C&C servers.

F. DOCUMENTATION AND REPORTING

Throughout his investigation, Milisic meticulously documented his findings, including network traffic logs, payload samples, and communication with service providers. He compiled his research into a comprehensive report, which he shared with relevant parties, including The broader security community and the Electronic Frontier Foundation (EFF). Milisic's methodology prioritized empirical evidence gathering, collaboration, and thorough documentation [7]. By combining technical analysis with real-world testing, he provided a solid foundation for understanding the presence of preloaded malware on AllWinner T95 Device and its implications for consumers.

Milisic's methodology prioritized empirical evidence gathering, collaboration, and thorough documentation. By combining technical analysis with real-world testing, he provided a solid foundation for understanding the presence of preloaded malware on AllWinner T95 Device and its implications for consumers.

IV. REASONS AND DISCUSSIONS

Daniel Milisic conducted a thorough analysis of the preloaded malware captured in the AllWinner T95 Device. His analysis aimed to identify the specific malware variant, understand its functionality, and assess its potential impact on infected devices and networks. These aspects highlighted his approach to malware analysis:

A. MALWARE IDENTIFICATION

Milisic successfully identified the preloaded malware as a variant of the clickbot family. Clickbot is designed to clandestinely generate revenue by secretly tapping on ads in the background. By identifying the malware family, Milisic gained insights into its typical behavior and motives.

B. PAYLOAD EXTRACTION

Milisic extracted a Stage-1 payload from the corrupted AllWinner T95 Device. This payload served as a crucial piece of evidence for understanding the malware's inner workings. The payload provided insights into how the malware establishes communication with C&C servers and obtains further instructions and additional payloads.

C. BEHAVIORAL ANALYSIS

Milisic closely analyzed the behavior of the malware to determine its impact on infected devices. He observed how the malware initiates contact with C&C servers once the When AllWinner T95 Device are powered on, they receive instructions and retrieve additional payloads. This analysis brought light on the malware's ad-click fraud activities and its potential consequences for users.

D. COLLABORATION AND VALIDATION

To ensure the accuracy and validity of his findings, Milisic collaborated with Bill Budington (security researcher), who independently verified the presence of preloaded malware on AllWinner T95 Device. This collaboration added credibility to the findings and the malware analysis.

E. IMPLICATION FOR USERS

Milisic considered the potential risks and implications for users whose devices are infected with the preloaded malware. He highlighted the impact on user privacy, the potential for financial losses due to ad-click fraud, and the risk of being part of a larger botnet. By emphasizing these implications, Milisic aimed to raise awareness among users and encourage informed decision-making when purchasing AllWinner T95 Device.

Milisic's malware analysis focused on understanding the behavior, impact, and risks associated with the preloaded

malware identified on AllWinner T95 Device. By dissecting the malware's functionality and collaborating with other researchers, he provided valuable insights into the nature of the malware and its potential consequences for affected users.

V. FINDINGS

Andriod Tv Boxes:

1) T95 . ALLWINNER H616
2) t95MAX . ALLWINNER H618
3) X12-PLUS . RockChip 3328
4) X88-Pro-10 . RockChip 3328

and the user may have a folder named as or similar to one of these: /data/system/Corejava or a file named /data/system/shared_prefs/open_preference.xml

Your device has harmful software called malware, which is always trying to connect to a specific server to send information and receive instructions without your awareness or permission. This software was already on the device when you bought it from the seller.

1) The initial stage of the malware, referred to as Stage 1, connects to http://adc.flyermobi.com/update/update.conf previously 128.199.97.77 to retrieve the url for later Stage 2.
2) The retrieved URL is subject to change and is arbitrary. The Stage 2 payload is encrypted and stored as an archived file named classes.dex. In this specific instance, the malware aims to generate revenue through background ad-click activities. However, the specific payload received by a device depends on the individuals operating the associated IP.
3) It is worth noting that the same url, http://adc.flyermobi.com/update/update.conf, was used in the Smartphone of Gigaset supply chain attack that took place in August 2021.
4) The people responsible for the malware have tried to conceal their identity, but they accidentally left behind an outdated SSL certificates since 2017. This certificate is linked to the domain dsp.dotinapp.com. The presence of those responsible for the malware is indicated by this Symantec-issued certificate. Remarkably, the developmental or testing type of the malware seems to be hosted on the https site dsp.dotinapp.com, accessible through port 80. Further information about Dotinapp can be found on their PR platforms and even on LinkedIn ((see Figure 1 and fig-1).

It is noteworthy that the PR announcement, SSL certificate, the registration of the first command-and-control server (ycxrl.com), and the Daraz amazon shoppify reviews all date back to 2017, despite the release of the H616 Android TV box in 2020.

The large number of positive cutomers reviews found online for these Android TV box brings up concerns about potential support from Dotinapp or other relevant parties to YouTubers and individuals who conducted the device reviews. Additionally, Akamai/Linode has terminated the control command and servers.

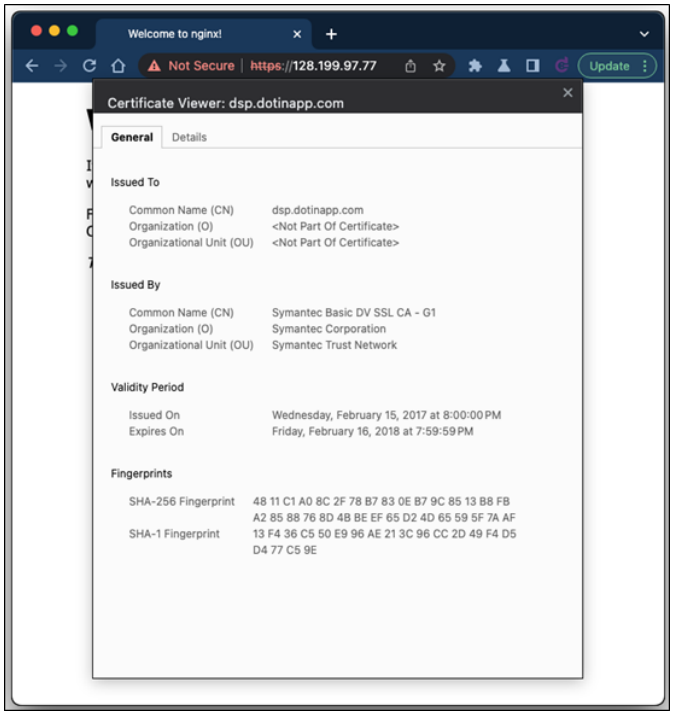

Fig. 1. *Outdated SSL certificates since 2017*

During the month of January, I encountered difficulties while attempting to file an abuse complaint through Linode's cumbersome Abuse Form. I received a ridiculous response via email, indicating that it was their only available method for filing such complaints. After venting my frustration on Reddit for several days, fortunately, I was able to grab the consideration of a Linode representative. After some persuasion, the representative agreed to take action and terminate the remaining three control and command IPs. The people behind the C2 server noticed this interaction and tried to hide their actions by changing DNS to 127.0.0.1, but their attempts were unsuccessful. At present, the four DNS names associated with the servers are resolving to non-routable IP addresses, indicating that they are not reachable. Furthermore, the original servers are no longer online.

It is crucial to emphasize that the temporary relief we have achieved is not a permanent solution, as the botnet has the potential to resurface on new hosts at any given moment. Therefore, our vigilance must be unwavering as we continue to monitor the situation closely.

I have included some intriguing tcpflow dumps in the repository, including an excerpt of the initial conversation with the control and command servers: (see Figure 2)

Both AllWinners & RockChips should exercise greater due diligence before selling Devices with their SoCs and tools to anyone without proper verification. The actions of the responsible parties in allowing the wrongdoers to create these ROMs raise a significant question: Will they take the initiative to provide end-users with a tool that facilitates the installation of a clean Android or Linux image on these devices? Only

```
POST /terminal/client/apiInfo HTTP/1.1
Connection: Keep-Alive
Content-Type: text/xml
channel: T10901
imei: xx:xx:xx:xx:xx:xx
launchername: com.swe.dgbluancher
model: MBOX
sdk: 29
brand: google
uuid: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
vcode: 1
androidId: xxxxxxxxxxxxxxxx
manufacturer: Google
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; MBOX Build/QP1A.191105.004)
Host: cbphe.com
Accept-Encoding: gzip
Content-Length: 0
```

Fig. 2. *Initial conversation with the control and command servers*

time will tell whether such a tool will be made available, and it remains an aspect that awaits further observation and analysis.

Several months ago, I obtained a T95 Android TV box that was equipped with preloaded Android 10, complete with a functional Play Store, and powered by an H616 processor. The device in question is a small black box featuring a blue swirling graphic on its top surface. Additionally, it has a digital clock displayed on the front. There are likely thousands, if not more, of these boxes currently in use worldwide. There are various options to purchase these devices on platforms like Amazon and AliExpress. However, by the end of January 2023, the availability of these devices on Amazon notably decreased, but a recent check online reveals their resurgence in large numbers. Upon closer inspection, the ROM on this device turned out to be highly dubious. Android 10 was signed with test keys and named "Walleye" after the Google Mobile Pixel 2. Superficially, there appeared to be minimal junkware present. However, the alarming discovery was that ADB was wide open over WiFi & Ethernet and Local Network right out of the box. I acquired the device with the intention of running Pi-hole and other applications, which led me to uncover the extensive malware infestation within the T95. After installing Pi-holeAfter configuring the T95 box's DNS1 and DNS2 settings to 127.0.0.1, I encountered a surprising revelation. The box was actively connecting to numerous known malware addresses. Since I couldn't find a clean ROM, I decided to make one last effort to remove the malware and restore the functionality of the T95 device. Using nethogs & tcpflow to monitor the network traffic, I uncovered multiple layers of malware, eventually tracing them back to the offending process/APK, which I promptly removed from the ROM. Unfortunately, there remains a persistent malware component that injects itself into the system server processes and appears deeply ingrained in the ROM. This sophisticated malware bears similarities to CopyCat in its operational behavior. None of the antivirus products I tested were able to detect it. If anyone has expertise or guidance regarding the identification of hooks into the system server, please feel free to provide assistance. Your support in this matter would be greatly appreciated.

VI. Recommendations

I was able to make progress in disabling the malware by using Pi-hole to modify the DNS of the control and command server, YCXRL.COM, to 127.0.0.2. However, complete removal of the malware was still not achieved. You can monitor the activity using netstat: (See Figure 3) To address the issue,

```
netstat -nputwc | grep 127.0.0.2

tcp6   1    0 127.0.0.1:34282  127.0.0.2:80     CLOSE_WAIT  2262/system_server
tcp    0    0 127.0.0.2:80     127.0.0.1:34280  TIME_WAIT   -
tcp    0    0 127.0.0.2:80     127.0.0.1:34282  FIN_WAIT2   -
tcp6   1    0 127.0.0.1:34282  127.0.0.2:80     CLOSE_WAIT  2262/system_server
tcp    0    0 127.0.0.2:80     127.0.0.1:34280  TIME_WAIT   -
tcp    0    0 127.0.0.2:80     127.0.0.1:34282  FIN_WAIT2   -
tcp6   1    0 127.0.0.1:34282  127.0.0.2:80     CLOSE_WAIT  2262/system_server
tcp    0    0 127.0.0.2:80     127.0.0.1:34280  TIME_WAIT   -
tcp    0    0 127.0.0.2:80     127.0.0.1:34282  FIN_WAIT2   -
tcp6   1    0 127.0.0.1:34282  127.0.0.2:80     CLOSE_WAIT  2262/system_server
```

Fig. 3. *Activity using netstat*

I had to set up an iptables rule that redirects all DNS traffic to the Pi-hole. This was necessary because the malware or virus attempts to use external DNS and also tries to connect through a nonstandard port. (see Figure 4) When these changes

```
adb shell iptables -t nat -A OUTPUT -p udp --dport 53 -j DNAT --to 127.0.0.1:53
adb shell iptables -t nat -A OUTPUT -p tcp --dport 53 -j DNAT --to 127.0.0.1:53
adb shell iptables -t nat -A OUTPUT -p tcp --dport 5353 -j DNAT --to 127.0.0.1:53
adb shell iptables -t nat -A OUTPUT -p udp --dport 5353 -j DNAT --to 127.0.0.1:53
```

Fig. 4. *External DNS and also tries to connect through a nonstandard port*

are implemented, the command and control (C&C) server is directed towards the Pi-hole webserver.(see Figure 5)

```
1672673217|ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1|404|0
1672673247|ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1|404|0
1672673277|ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1|404|0
1672673307|ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1|404|0
1672673907|ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1|404|0
1672673937|ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1|404|0
1672673967|ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1|404|0
1672673997|ycxrl.com|POST /terminal/client/eventinfo HTTP/1.1|404|0
```

Fig. 5. *Pi-hole Webserver*

VII. CONCLUSION

In conclusion, the research conducted by Daniel Milisic sheds light on the intricate nature of malware analysis and the challenges faced in identifying and mitigating threats. The investigation revealed a control command and server, YCXRL.COM, which was responsible for distributing malicious payloads and orchestrating the activities of the malware. Through the utilization of Pi-hole and iptables rules, attempts were made to neutralize the malware by redirecting DNS traffic and monitoring the server's activity. Although some measures were successful in temporarily disrupting the malware's communication, it is important to note that the botnet can potentially reemerge on new hosts in the future. Furthermore, the research highlighted the presence of sophisticated malware embedded within AllWinner T95 Device, such

as the T95 device running an Android 10 ROM. The ROM exhibited suspicious characteristics, including the use of test keys and open ADB ports, raising concerns about the integrity and security of these devices. Efforts were made to identify and remove the layers of malware, but some deeply-rooted elements remained elusive. The investigation also uncovered the involvement of Dotinapp and their potential influence in sponsoring positive reviews of AllWinner T95 Device. The Link between Dotinapp and the malware-infected devices raises questions about the accountability and due diligence of chip manufacturers, such as AllWinner and RockChip, in ensuring the integrity of their products. In conclusion, the research by Daniel Milisic serves as a stark reminder of the ever-present threat of Virus and the need for constant watchfulness and proactive measures to safeguard against such attacks. It underscores the importance of thorough analysis, collaboration within the security community, and the implementation of robust security practices to protect users from the evolving landscape of cyber threats.

VIII. FUTURE WORK

Educate users about the risks of preloaded malware on AllWinner T95 Device and provide guidance on how to protect themselves. This can include creating user-friendly guides, hosting webinars, and disseminating information through various channels to raise awareness and promote safe usage practices.

REFERENCES

[1] N. Collier and N. Collier. Analyzing and remediating a malware infested t95 tv box from amazon. Retrieved 22 May 2023, from https://www.malwarebytes.com/blog/news/2023/01/preinstalled-malware-infested-t95-tv-box-from-amazon, 2023.

[2] YouTube. Stop buying android tv boxes! Retrieved 22 May 2023, from https://www.youtube.com/watch?v=1vpepaQ-VQQ, 2023.

[3] Yousra Aafer, Wei You, Yi Sun, Yu Shi, Xiangyu Zhang, and Heng Yin. Android smarttvs vulnerability discovery via log-guided fuzzing. In *USENIX Security Symposium*, pages 2759–2776, 2021.

[4] Android tv boxes shipped with malware, reports say. Retrieved 22 May 2023, from https://www.globalvillagespace.com/tech/android-tv-boxes-shipped-with-malware-reports-say/, 2023.

[5] Android tv boxes found preloaded with malware — what's going on? Retrieved 22 May 2023, from https://www.laptopmag.com/news/android-tv-boxes-found-preloaded-with-malware-whats-going-on, 2023.

[6] Yahoo is part of the yahoo family of brands. Retrieved 22 May 2023, from https://shorturl.at/cowE9, 2023.

[7] DesktopECHO. DesktopECHO/T95-H616-Malware: "Pre-Owned" malware in ROM for AllWinner H616/H618 & RockChip RK3328 Android TV Boxes. Retrieved 22 May 2023, from https://github.com/DesktopECHO/T95-H616-Malware, 2023.