

Time to Compromise

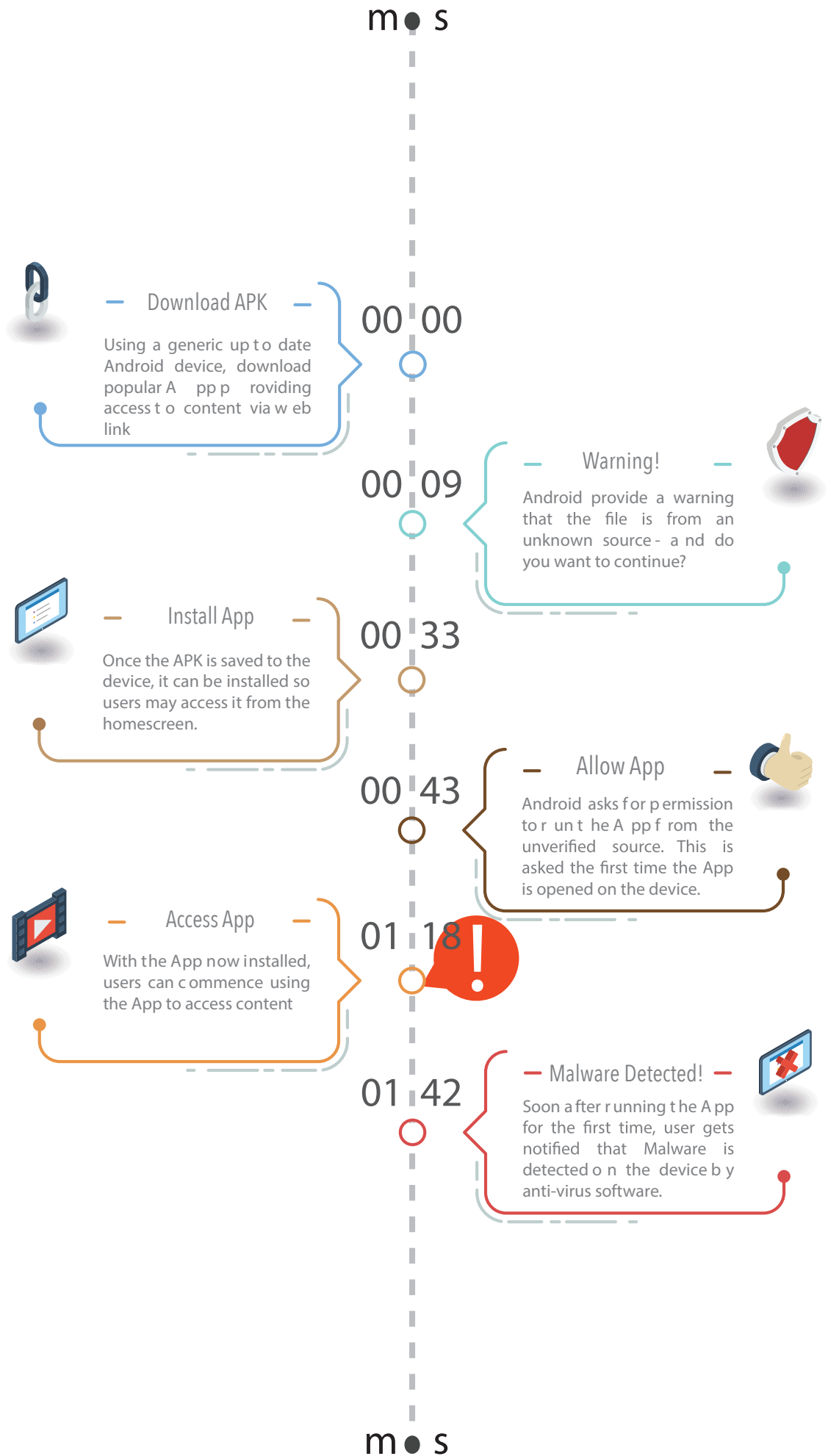
How Cyber Criminals use Ads to
Compromise Devices through Piracy
Websites and Apps



Windows 10: Time to 1st Compromise - 00:42



Android Device: Time to 1st Compromise – 01:18



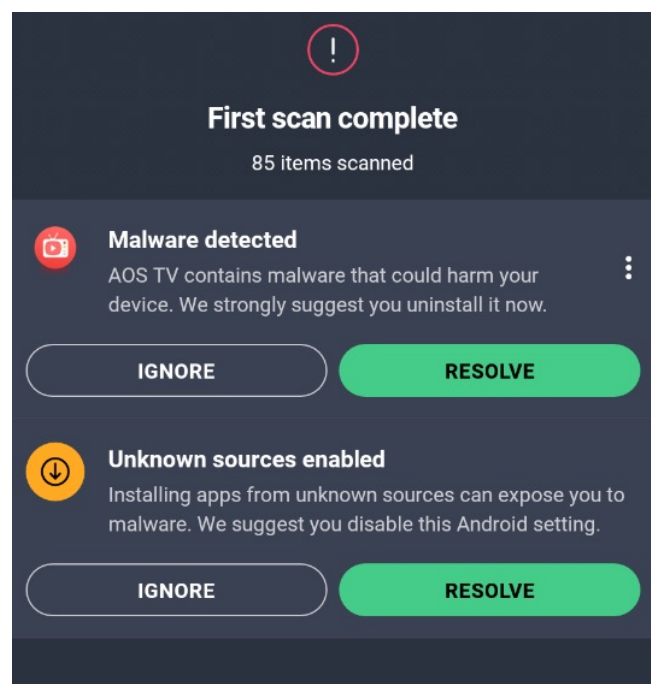
Contents

Timeline to Windows 10 Compromise	2
Timeline to Android Platform Compromise	3
Executive Summary	5
Background	6
Methods	8
Windows 10 Platform	8
Android Platform	8
Results	9
Windows 10 Platform	9
Android Platform	15
Case Study	18
Discussion	20
References	21
Researcher Biography	22
About AVIA	22
Acknowledgements	22

Executive Summary

A recent study found that educating consumers about malware risks from visiting piracy sites or using piracy apps could reduce malware infections by 31%. This study used variables linking demographic data, cybersecurity knowledge and perceived risks from a sample of more than 5,000 people around the Asia-Pacific region.

In this study, we wanted to see whether consumer perceptions about malware risk and piracy were true (or not), by simulating a user who visited these sites to view streamed content, and then to examine what actual malware infections were encountered. We predicted that malware would be installed, potentially leading to devices being ransomed, malicious advertising being displayed, or user identities being stolen through credentials being stolen.



We found that a typical user visiting these sites would be infected by ransomware, a number of trojan horses, and other Advanced Persistent Threats (APTs). The results support the hypothesis that there is a nexus between piracy and malware infections, where site operators generate significant revenue from allowing malicious ads to be placed on their sites. Malware authors can in turn gain access to consumer PCs and mobile devices, and all of the data held in storage, but also access to banking login details and other sensitive logins.

In this report, we outline some strategies to reduce risk for consumers, and indicate regulatory measures (including industry self-regulation) which may assist in a large-scale reduction of malware infection, by reducing the accessibility of these sites, reducing the rewards, and making such sites more difficult to operate.

Background

Piracy continues to cause a significant financial impact on the entertainment industry, especially the more contemporary misuse of streaming websites and applications. Streaming provides a real-time, live experience, with premium content (such as sporting fixtures) relayed in real-time to consumers through a range of technologies, including streaming websites and specialized streaming applications. These illicit sites and applications, in turn, are funded by advertising, creating an enormous business opportunity for organized crime, while at the same time depriving rightsholders and creators of their income. This reduces the incentive for investment in the industry, and reduces the rewards for creatives and artists around the world.

A recent report by the online consumer safety group Digital Citizens Alliance (2021) and brand safety specialist White Bullet Solutions found that illicit streaming websites and apps were generating an estimated \$1.34 billion in annual revenues through advertising. The top 5 of these sites were generating an average \$18.3 million from advertising, and the top 5 apps were generating an average \$27.6 million. The relatively higher revenues from apps versus websites indicates that mainstream brands are once again returning to where the consumer “eyeballs” are most likely to be. Major brands paid more than \$100 million to advertise through illicit streaming apps last year.

In the early studies of advertising on piracy sites, mainstream ads were once dominant (Taplin, 2013), later making way for the rise in “high risk” ads, ie, those ads which presented the great risk to the consumer (Watters et al, 2015). The prevalence of these “high risk” ads were monitored across a number of different countries in the Asia-Pacific region, including Australia, New Zealand, Canada, Hong Kong, Vietnam, Thailand, Malaysia, Indonesia and Singapore (Watters et al, 2014; Watters, 2015). The main categories of “high risk” ads identified included adult (pornography) sites, malicious software (malware) and gambling. While the precise distribution of each ad category differed between countries, resulting from local market conditions and consumer preferences, the potential impact on consumers from visiting these sites, and being exposed to high risk ads was (and remains) a concern. The observation that apps may once again be drawing mainstream ads is concerning, given that mainstream ads have been found to support serious harms to children through the distribution of child exploitation material in key markets like South America (Watters, 2015).

As video artist Richard Serra observed in 1973, “if something is free, you’re the product”. From a consumer perspective, it is also true that “there is no free lunch”: in the world of piracy websites and streaming apps, consumers become unwitting victims of a range of somewhat invisible effects, all of which contribute to the boom in illicit revenue. These include:

- Malware installation – once installed on a consumer device, malware can become the target vector for identify theft and consumer fraud, ransomware attacks, advertising redirection, and so on (Kumar et al, 2016). This means that consumers can be directly attacked, with their bank accounts at risk, and the potential for their devices and personal data to be held for ransom (Başeskioğlu & Tepecik, 2021). It also means that consumers may be shown advertising which has been hijacked, depriving legitimate business of the advertising space which they have paid for.
- Bitcoin mining – the CPU power of consumer devices is used to mine for bitcoins, significantly increasing CPU loads and energy consumption (Van der Sar, 2017). Consumers are not the beneficiaries of this bitcoin mining – the profits are retained by the site owners. Also, mining activity of this kind generates unnecessary CO2 emissions and may be harmful to the environment (Badea et al, 2021).
- Social harms – the promotion of gambling and adult (sex) sites to consumers, especially children, poses significant risks for society at large, especially gambling addiction (Suriadi et al, 2016).

Investing in consumer education and awareness around piracy may be one critical measure to reduce harms from visiting piracy websites and using illicit streaming apps. This is because the available evidence suggests that users who visit these sites are less likely to install anti-virus software, compared to regular users (Telang, 2018). This astonishing result was obtained by monitoring more than 250 users over the period of a year, and found a direct correlation between the number of times piracy sites were visited, and the number of malware infections. Furthermore, the risk could be quantified: doubling the viewing time for piracy sites led to a further 20% increase in the total number of malware files detected.

A quantitative approach to assessing malware risk through piracy may be difficult for consumers to understand or navigate. It is clear from a recent consumer survey that consumers in some markets report having a more sophisticated understanding of the malware-piracy link, but in other markets or demographics, there may be not be a clear understanding of the potential impact that ransomware can have on a bank account, loss of privacy and personal data, or physical loss of device due it being locked from ransomware. Therefore, there may be value in exploring exactly how users can become infected by malware through interactions with piracy sites, and observing what protective measures may have worked, and how new ones could be introduced in the future, via government regulation or industry self-regulation.

Methods

A simulated user was created on both a Windows 10 virtualised PC (using VirtualBox), and an Android emulator running on Windows 10. The method for simulating user piracy activity is detailed below for each operating system. The idea was to recreate, as closely as possible, the typical user experience of visiting these sites, or using these apps, with the view exploring actual malware risk.

Windows 10 Platform

A fresh Windows 10 virtual machine was installed and configured with no third-party anti-virus installed, and Windows Defender disabled to the largest extent possible. A Windows defender scan confirmed that no malware was present in the image. The Chrome web browser was installed. No ad blocking or other consumer protection software was installed within the browser. An email address was registered using the virtual user's name, and accessed using the Chrome web browser.

Based on industry intelligence, a list of active and popular piracy sites was identified. Each website was visited sequentially. Where a search box was provided, the search term "English Premier League" was entered, and the first result clicked. In the case where a list of possible was provided by the site on the landing page for individual streams, the first one was selected. The stream was viewed for 10 minutes before pausing.

Any ads that popped up were clicked on, and consent given to install all suggested applications or browser plugins. The user email address was also entered into any email subscription fields for newsletters.

At the end of the testing sequence, user credentials for accessing email were entered again, leaving open the chance that any malware present could compromise the login credentials.

Android Platform

An android emulator was installed on a Windows 10 PC, running the Android 9 operating system. An emulated environment reduces the chance of a hardware compromise, but some malware can detect whether a virtualized or emulated device. A Google email account was setup to enable access to the Play Store and email on the device. The Chrome browser was already installed on the distribution. All anti-virus checking was uninstalled, and no other consumer protection software was installed.

A set of well-know Android apps used for piracy streaming was installed sequentially. After each app was installed, the search term "English Premier League" was entered, and the first result clicked. In the case where a list of possible was provided by the site on the landing page for individual streams, the first one was selected. The stream was viewed for 10 minutes before pausing. Any ads that popped up were clicked on, and consent given to install all suggested applications or browser plugins.

Results

Windows 10 Platform

At the end of the testing cycle, the operating system was rendered unusable because of malicious system activity. A continuous “clicking” sound was observed from the system speakers. Windows Defender was enabled, and as predicted, a number of trojans were present at the end of the testing cycle as detailed below, and confirmed by Windows Defender¹, as shown in Figure 1, including a ransomware attack.

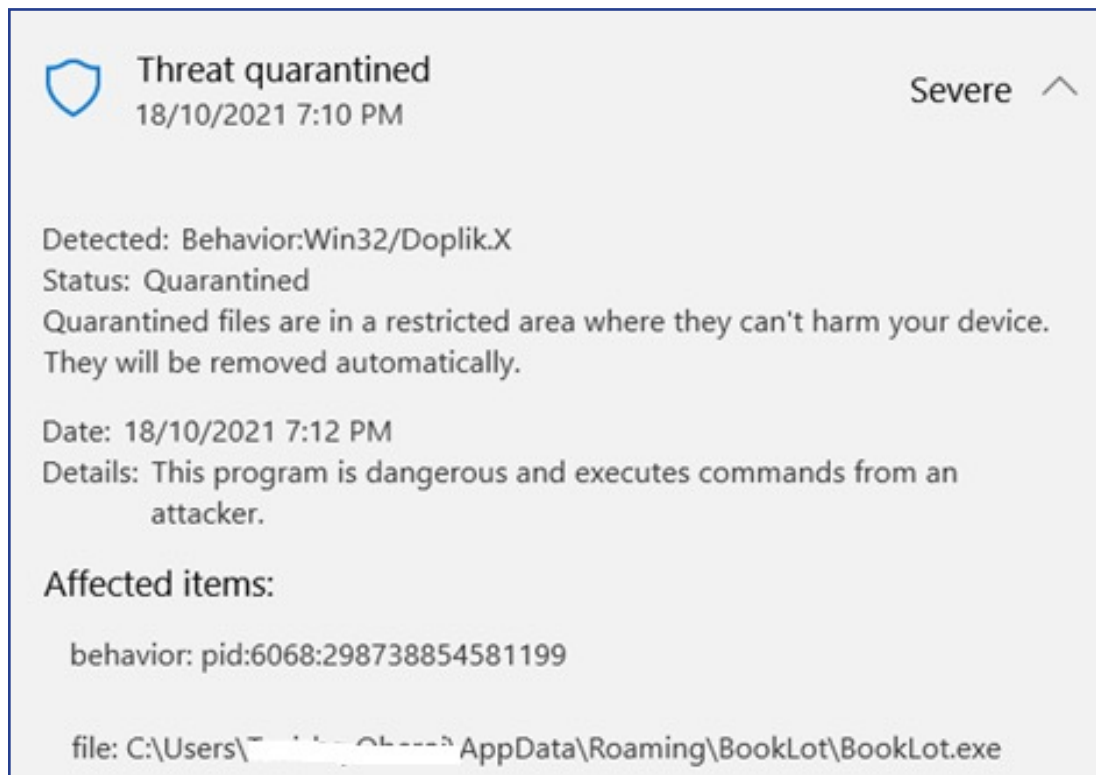


Figure 1 – Example of Malware Detected

Wireshark was used to capture traffic leaving the operating system and going on the connected network. DNS lookups and encrypted TLS connections were observed for omnatuor.com, a reported spyware infection². As noted by pcsafetygeek.com, this malicious code can read passwords stored in the browser, potentially exposing users to internet banking fraud and any online service that just uses a username and password for authentication. Other traffic analysis indicated a range of unknown connections being made to other hosts. For example, connections were made to rt-b.com, novidash.com, minismss.xyz, littlecdn.com, pupok.link, miliated.xyz, sivian-ebi.com, mateyhecrie.xyz, microuconvilla.xyz. Unfortunately, the traffic was encrypted, so we are unable to say what was being uploaded; however, these sites are all protected by domain anonymization, and do not appear to have a public website. In short, we have no way of knowing who is sending the data and for what purpose.

1 <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Behavior:Win32/Doplik.X&ThreatID=2147764541>

2 <https://pcsafetygeek.com/remove-omnatuor-com/>

A third-party anti-virus product (Kaspersky) was also installed to verify the Windows Defender results. In a random 1 hour sample taken from the security logs, there were 33 instances of attempts by a trojan horse to download and install an unauthorized application from a C&C server.

Walking through a typical sequence of interactions with the piracy sites, the user may be shown a page with a streaming window, but when they attempt to click “Play”, the user may be requested to allow notifications (which could contain malicious links) and/or to use a CAPTCHA to confirm that they are human. Clicking the CAPTCHA provides an opportunity for malware download and installation, ie, something which should be a protection actually becomes an attack vector.

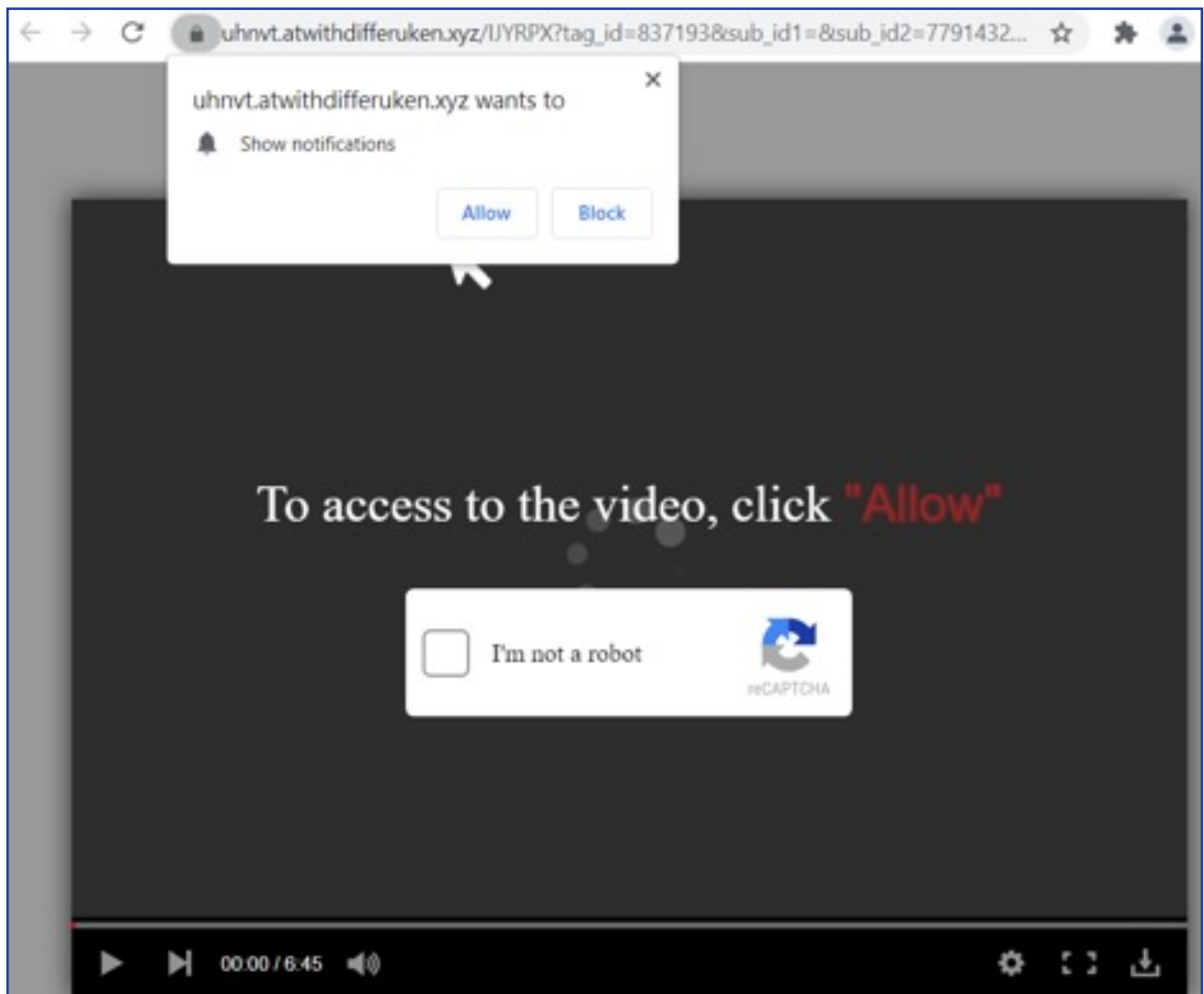


Figure 2 – Fake CAPTCHA

An example of a notification with a malicious link is shown in Figure 3:

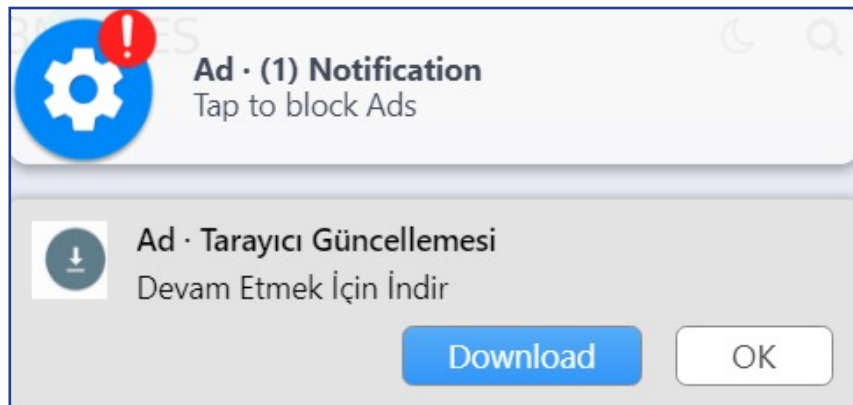


Figure 3 – Malicious Notification

Often, users are prompted to install software which is promoted as being some kind of protection. For example, a Chrome extension called “Adblock 360” promises “no more popups with Adblock 360”, yet according to pcrisk³.com it operates as adware, as shown in Figure 4.

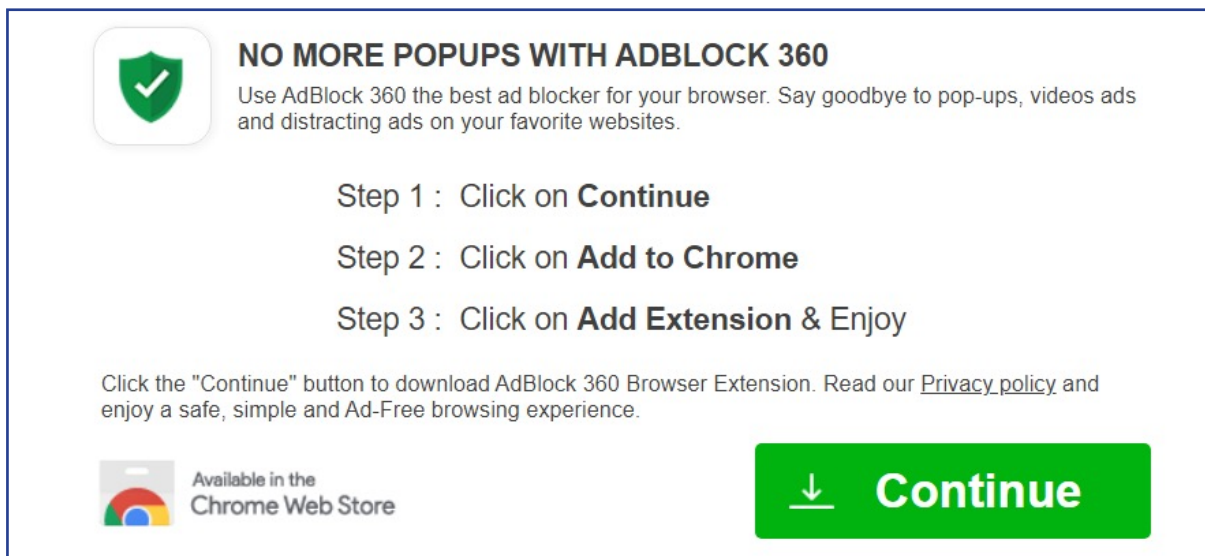


Figure 4: Malicious Adware Detection

Similarly, PDFConverterSearchOnline is reported by malwaretips.com to be a browser hijacker which then generates advertising revenue for the search provider operator, as shown in Figure 5.

3 <https://www.pcrisk.com/removal-guides/21940-adblock-360-adware>

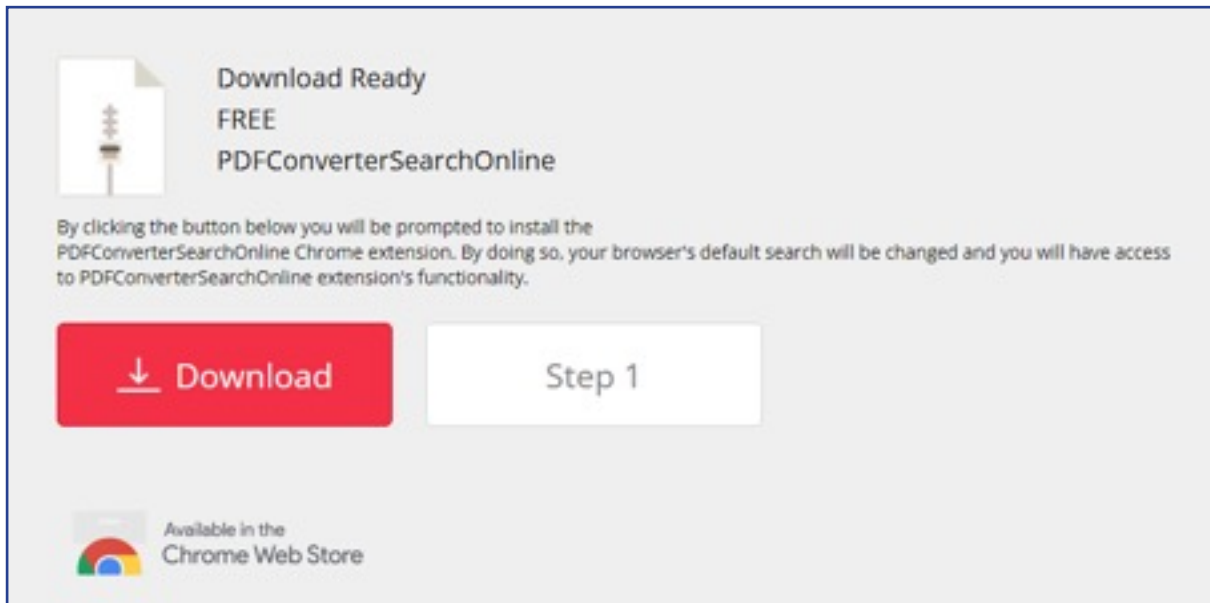


Figure 5: Browser Hijacking

While some users may be able to protect themselves from using malicious ads by using an adblocker, some site operators request that users disable this protection as it may make the video stream unstable.

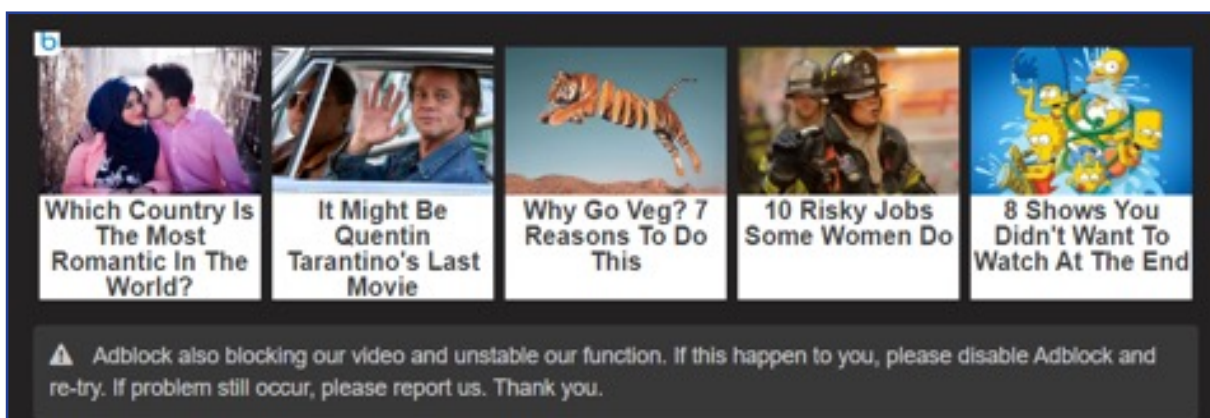


Figure 6: Adblock Detection

Some of the “high risk” ads shown on piracy sites direct users to adult and gambling sites, as shown in Figure 7.

THOUSANDS OF OUR MEMBERS LOOKING FOR SEX HOOKUPS OR ONLINE SEX FRIENDS IN YOUR AREA!

100% FREE ACCESS , BUT LIMITED TIME!

This site is so popular that you may see nude photos of hot members near you.

Answer a few questions to see if you are qualified:

- 1
- 2
- 3

what type of breast size should they have?




Figure 7: Adult Website Ads

In other cases, “mainstream” ads on piracy sites advertise for entirely legitimate businesses. Ironically, an anti-virus ad has been placed on this piracy site – the ad owner is likely unaware that this is case, but the backend algorithms for ad placement have identified the link between a site that may contain malware, and getting malware protection, as shown in Figure 8.



Figure 8: Mainstream/Legitimate advertising from an anti-virus vendor

In terms of protections, some malicious sites were blocked by Chrome, as shown in Figure 9.

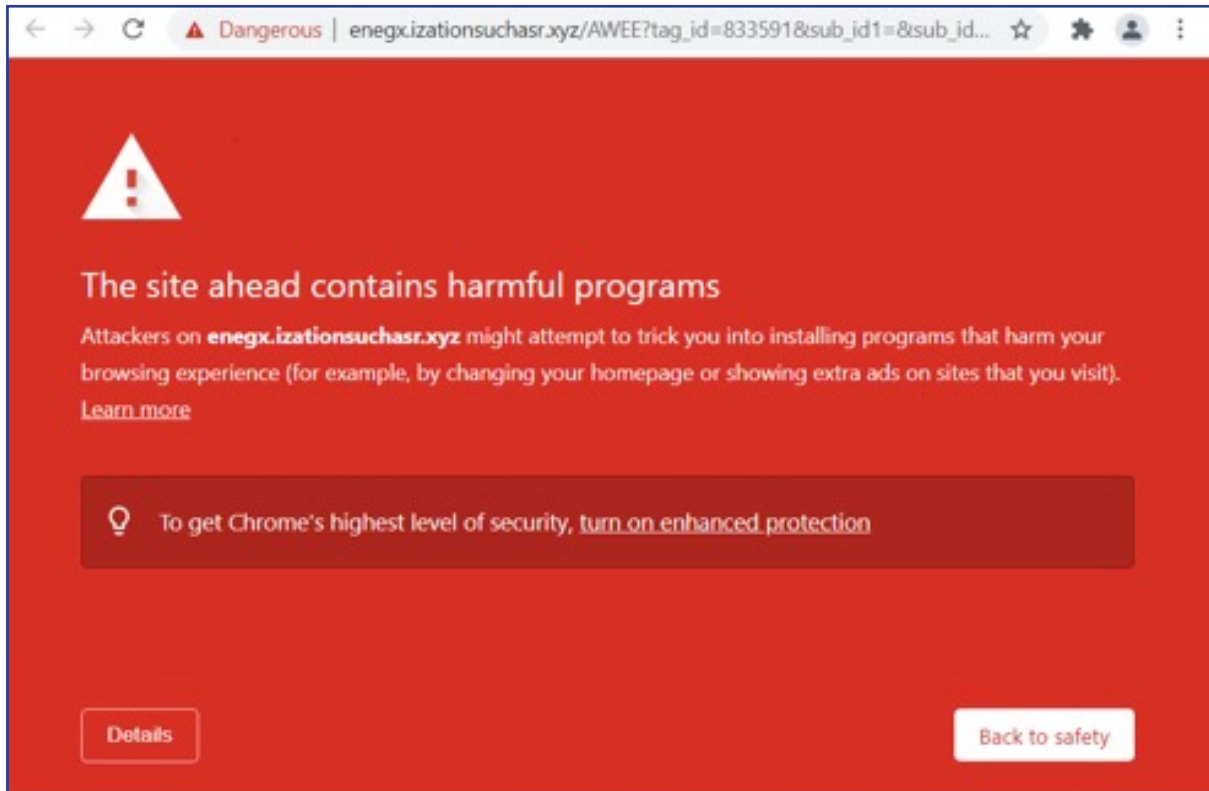


Figure 9: Malicious Activity Warning from Chrome Browser

In other cases, Chrome warned that HTTPS was not present or misconfigured, as shown in Figure 10.

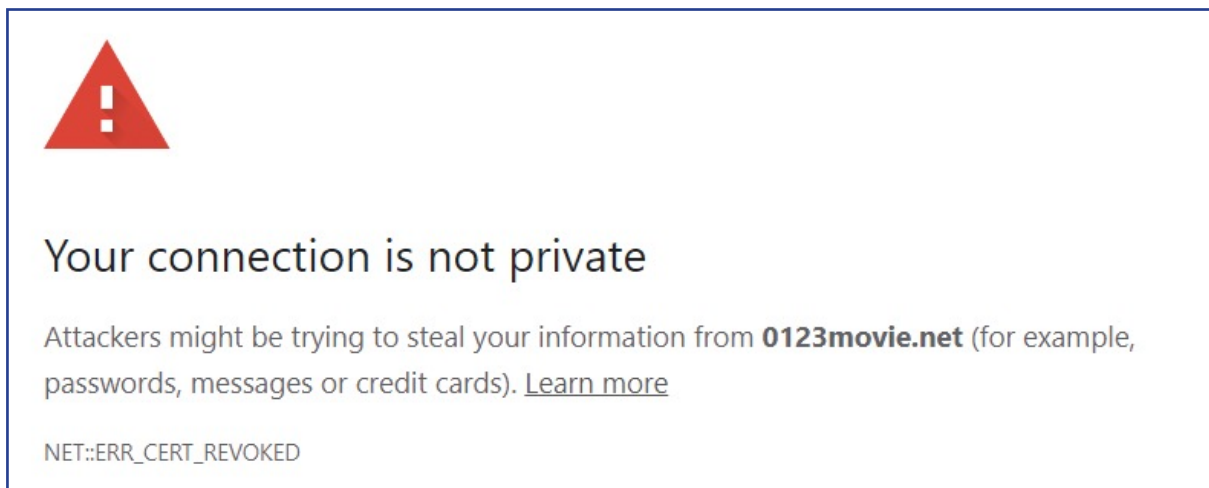


Figure 10: HTTPS Misconfiguration Detected

Importantly, in plain sight, Chrome warns users installing Adblock 360 that installing the extension means that the program can “read and change all your data on all websites”. Confusingly, the warning is presented with a green tick embedded in a protective shield at the top left corner of the screen, as shown in Figure 11.

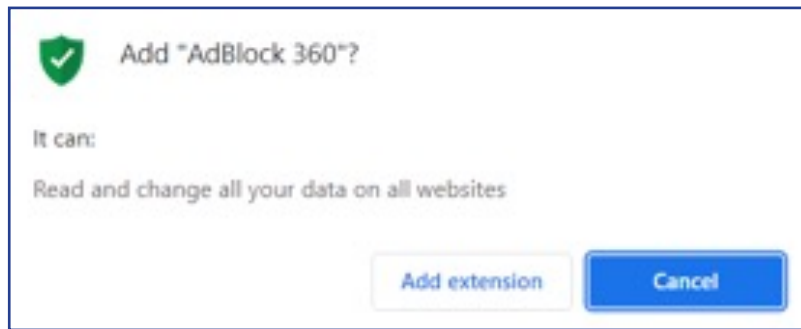


Figure 11: Confusing “GreenTick” Warning

Android Platform

After installing the streaming apps, three different phenomena were observed: detection of malware, advertising of malicious apps masquerading as legitimate, and the use of third-party proxy services. All can have significant consequences for users.

Firstly, malware was detected as present in some of the installed apps, as shown in Figure 12. It is certainly concerning that this occurred even in the absence of a third-party malware infection.

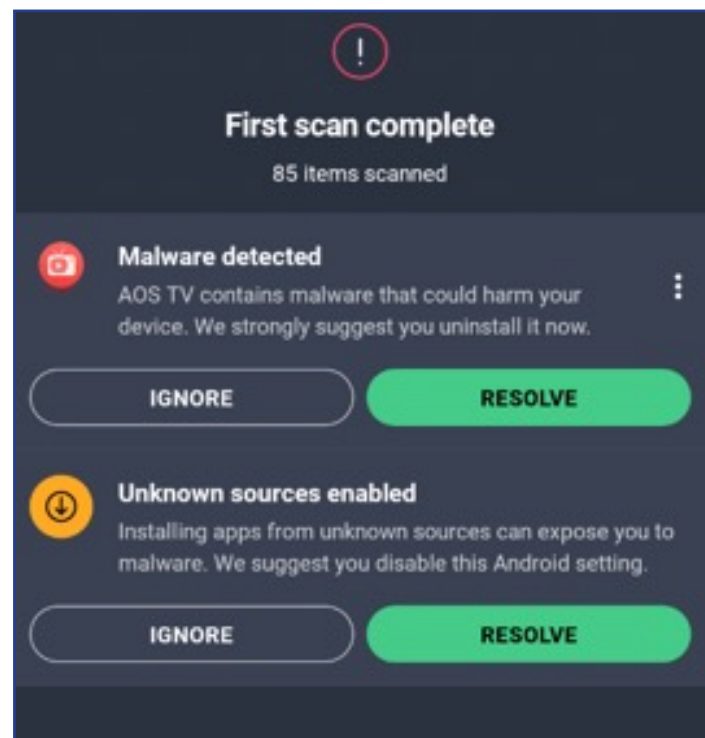



Figure 12: Malware Reported being Present in Streaming App

Secondly, a number of ads showed apps which masqueraded as legitimate, including anti-virus scanners as shown in Figure 13. Running this app did not show any specific results, its true purpose remains unclear.

Install Android Cleaner for your Samsung and improve performance of your phone!

For improved performance and increased free memory of your Samsung Galaxy S10 5G, we have released an update of the Android Cleaner which will find all potential threats and will also clean junk files and improve the battery life.

Install Android Cleaner right now to boost your Samsung Galaxy S10 5G and improve performance of your phone and improve its battery life.

 **Install Android Cleaner for FREE** to clean and strengthen your Samsung immediately!

Install	Cancel
----------------	--------

Figure 13: Masquerading Apps

As outlined in the Digital Citizens Alliance (2021) report, many legitimate ads were also observed in the apps. A good example is shown in Figure 14, with a company called Tines advertising a cybersecurity product for Security Orchestration, Automation and Response (SOAR). Clearly, whatever advertising networks that it behind the ads and the numerous intermediaries have (ironically) linked the cybersecurity theme of the Tines ad with the content and purpose of the app. While the advertising program would certainly increase “eyeballs”, the potential for brand and reputational damage is also significant.

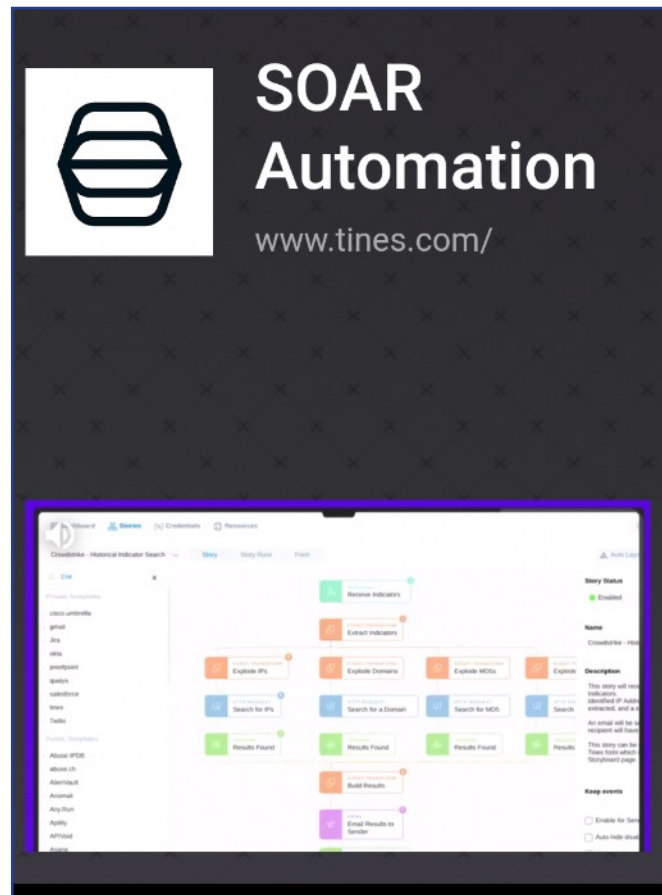


Figure 14: Tines SOAR Ad

Finally, a number of apps allow users to trade going “ad free” in exchange for becoming a Brightstar peer, as shown in Figure 15. Bright Star (formerly Luminati) is a proxy service that allows users to become peers within their network, lending out network access and CPU cycles to distribute load and effort. While proxy systems like Bright Star do fulfil a large range of legitimate functions, concerns have been raised in recent times about peers being used for illicit purposes, including the use of consumer devices to participate in Distributed Denial of Service (DDoS) attacks. The concern from the consumer perspective would be that they can reduce the risk from not seeing potentially malicious ads by agreeing to install Bright Star and operate as a proxy, but then potentially (and unwittingly) become a participant in criminal activity, such as DDoS. Either way, it is the consumer who ultimately bears the burden and the risk.

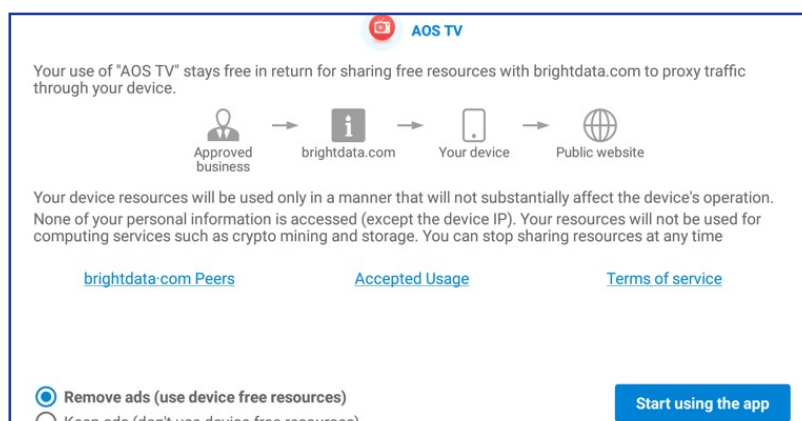


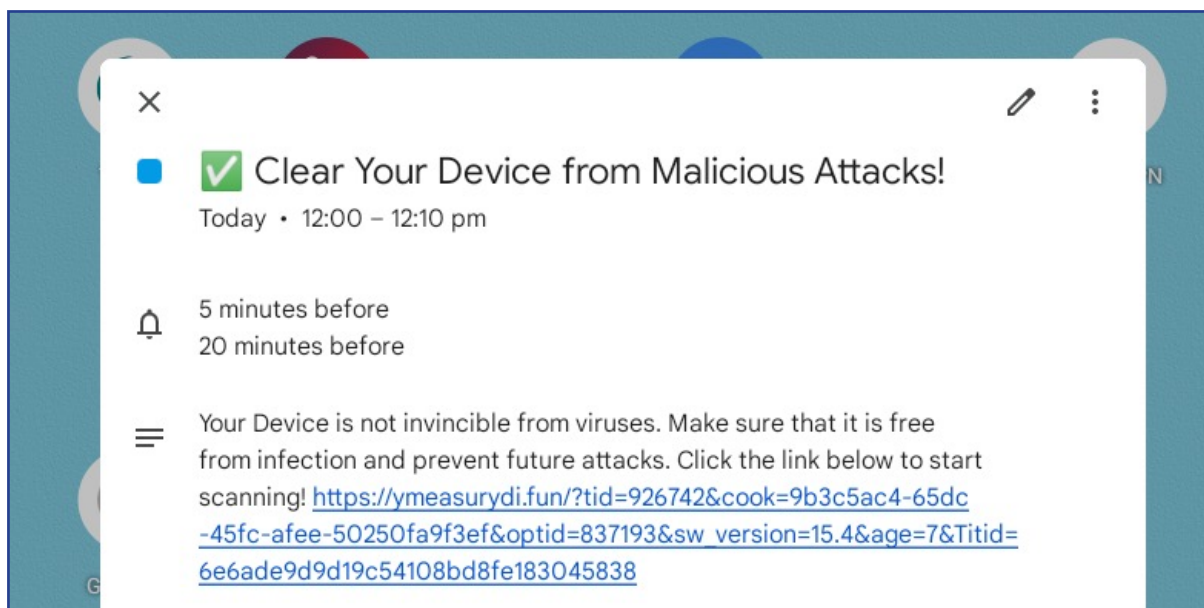
Figure 15: Bright Star Proxy

Case Study

In addition to the exploratory analysis presented above, it is also instructive to review the specific steps and timings required to get infected, and to assess the potential consequences. Taking the example of the first website we investigated, literally, the very moment that you type in a search term, you are immediately targeted for infection. In this case, clicking on the first movie title triggered the download of a file with the title name plus an “.apk” extension. A naïve user might believe that this was a torrent file, but it actually contained a malware variant known as Artemis!Trojan (as defined by Microsoft)⁴. This trojan was first detected on 14th October 2021 – only a matter of days before the study results were gathered – meaning it was one of thousands of “zero day” pieces of malware that are being pumped out every day.

VirusTotal provides some interesting facts about the capability of this trojan – it can read and write to external storage, it can access wifi, and can read and write to your calendar. Once loaded, it contacts 6 different IP addresses, and two domains (willitepartisti.club and omefukmend.xyz) – it uses HTTP GET to receive instructions from omefukmend.xyz and HTTP POST to transmit data to willitepartisti.club (unfortunately the connections are encrypted, so it’s not possible to tell what data is being exfiltrated). We observed that calendar entries with further malicious links were indeed inserted into Google calendar, as shown in Figure 16 – in this case,

Figure 16: Calendar Invite



JoeSandbox has provided a complete analysis of this malware sample⁵. The analysis shows a mapping to the MITRE ATT&CK Framework, showing the eventual real-world impact of this sample, including:

- Delete device data
- Device lockout
- Carrier billing fraud

4 Full details of the trojan can be found at <https://www.virustotal.com/gui/file/94e8a4b-9717cca98bd2584276244db8c16f747c9005aea71a4ae582ae468075c/summary>

5 <https://www.joesandbox.com/analysis/516714/0/html>

- Manipulation of App Store rankings or ratings
- Abuse accessibility features

To achieve these outcomes, the sample makes use of a range of a significant range of sophisticated technologies, including:

- File obfuscation
- Steganography
- Location tracking
- Network information discovery
- Scheduled exfiltration
- Encrypted channels
- Eavesdropping
- Denial of service

In short, consumers have no idea of the very significant firepower which can be directed at them and their local network, supported by the goals of lateral movement.

The first Android app that we installed was immediately flagged as malware by an anti-virus engine (Figure 17). If we had disabled malware scanning, this malware would have continued undetected. Similar to the website, when the app was installed, traffic was observed flowing to a large number of encrypted HTTPS services. Once again, while it is not possible for us to decrypt this traffic and understand what was being uploaded, by using a proxy and analysing network traffic, it is clear that numerous HTTP sessions are established when the app loads. These appear to be linked to various advertising networks, both mainstream and illicit.

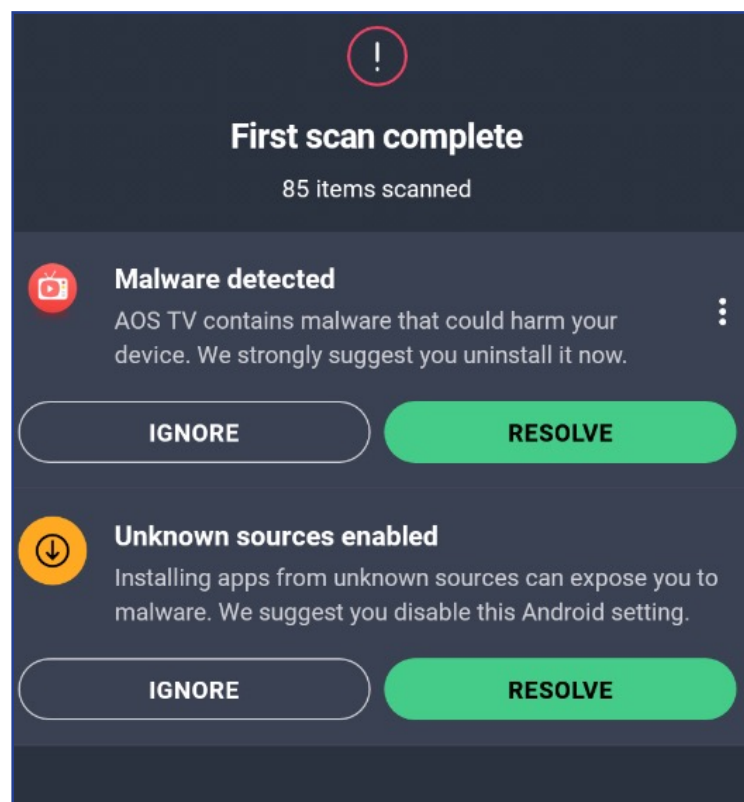


Figure 17: Android Malware Detected in App

Discussion

In this report, we have attempted to replicate the user journey for consumers who access piracy apps and streaming websites, with a specific view to understanding the scale and risk for these consumers. In summary, we found that consumers could be infected by a range of malware (including trojans and ransomware) that could cripple their devices, and hold their data hostage. This malware could also spread laterally within a home or corporate network, potentially impacting on critical business operations, or being the launchpad for identity theft and identity fraud. Consumers were also at legal risk from signing up to proxy servers which have allegedly been used to participate in DDoS and other attacks in the past. Depending on local laws, it is likely that consumers could have criminal or civil liability if their devices were used for such attacks, or for any other purpose where their IP address could be tracked by law enforcement. For example, if a proxy service was being used to distribute child exploitation material, then the consumer could end up being the subject of a police investigation. It is very clear from this report that consumers face significant personal and business risks from accessing piracy websites or streaming apps.

A number of protections worked well. Windows Defender and other antivirus products – when activated – were able to detect and disinfect devices. However, it is important to note that not all malware can be detected, and “zero day” attacks – where a novel malware is released into the wild – are a frequent, daily occurrence. The risk of lateral infection is also high, especially if the consumer using the app or streaming website has a privileged account (such as Windows Administrator). Browser-based protections (such as Adblock) would also be effective, but most sites now detect whether Adblock is being used, and will not display the stream if detected. Therefore, consumers will disable Adblock to proceed. On the other hand, Google search (and Chrome) did place a number of warnings on search links and clicks to ensure that consumers were fully made aware of the consequences of proceeding. We know from research in the child exploitation field that the right combination of message theme (such as “fear of prosecution”) and aesthetics (images and text layout) can be very effective in reducing consumer decisions to proceed. Further research should be considered to understand how to alert consumers to malicious activity, while at the same time avoiding message fatigue and habituation.

The real challenge lying ahead is to reinforce the point to consumers that these “free” services are running as an illicit business, and that the site operators need to recover their costs and make a profit. They do this by selling advertising, with some of those advertisers dropping malware to steal identities and commit fraud. Further user education and awareness is needed, as well as tools which can be deployed at the point of installation (or clicking) to warn and deter users from harming themselves and others.

References

- Badea, L., & Mungiu-Pupazan, M. C. (2021). The Economic and Environmental Impact of Bitcoin. *IEEE Access*, 9, 48091-48104.
- Başeskioglu, M. Ö., & Tepecik, A. (2021, June). Cybersecurity, Computer Networks Phishing, Malware, Ransomware, and Social Engineering Anti-Piracy Reviews. In 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-5). IEEE
- Digital Citizens Alliance (2021). Breaking (B)ads: How Advertiser-Supported Piracy Helps Fuel A Booming Multi-Billion Dollar Illegal Market. Retrieved from <https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf>
- Kumar, S., Madhavan, L., Nagappan, M., & Sikdar, B. (2016). Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers. In 2016 11th International Conference on Availability, Reliability and Security (ARES) (pp. 423-427). IEEE.
- Prichard, J., Wortley, R., Watters, P. A., Spiranovic, C., Hunn, C., & Krone, T. (2021). Effects of Automated Messages on Internet Users Attempting to Access “Barely Legal” Pornography. *Sexual Abuse*, 10790632211013809.
- Suriadi, S., Susnjak, T., Ponder-Sutton, A., Watters, P., & Schumacher, C. R. (2016). Using data-driven and process mining techniques for identifying and characterizing problem gamblers in New Zealand.
- Taplin, J. (2013). USC Annenberg lab ad transparency report – January 2013. Retrieved from http://www.annenberglab.com/sites/default/files/uploads/USCAnnenbergLab_AdReport_Jan2013.pdf
- Telang, Rahul, Does Online Piracy Make Computers Insecure? Evidence from Panel Data (2018). Available at SSRN: <https://ssrn.com/abstract=3139240> or <http://dx.doi.org/10.2139/ssrn.3139240>
- Van der Sar, E. (2017). The Pirate Bay Website Runs a Cryptocurrency Miner. Retrieved from <https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/>
- Watters, P. A., Watters, M., & Ziegler, J. (2014). Malicious advertising and music piracy: a New Zealand case study. In 2014 Fifth Cybercrime and Trustworthy Computing Conference (pp. 22-29). IEEE.
- Watters, P. A., Watters, M. F., & Ziegler, J. (2015). Maximising eyeballs but facilitating cybercrime? ethical challenges for online advertising in new zealand. In 2015 48th Hawaii International Conference on System Sciences (pp. 1742-1749). IEEE.
- Watters, P. (2015). An analysis of piracy website advertising in Brazil and its linkages to Child Exploitation. Retrieved from https://ecpat.org/wp-content/uploads/2021/05/Piracy-Website-Advertising-in-Brazil_ENG.pdf

Researcher Biography

Professor Paul A. Watters is Honorary Professor in Criminology and Security Studies at Macquarie University, Adjunct Professor of Cybersecurity at La Trobe University, and CEO of Cyberstronomy Pty Ltd, a Melbourne-based startup that develops Governance, Risk and Compliance software for cybersecurity. Professor Watters is a Fellow of the British Computer Society and Chartered IT Professional, a Senior Member of the IEEE, and a Member of the Australian Psychological Society. Professor Watters has published more than 200 peer-reviewed research papers in cybersecurity, data mining, and cognate fields, which have been cited more than 4,832 times by his peers. He is consistently in the top 10% of all researchers by paper downloads on the Social Sciences Research Network (SSRN).

About AVIA

The Asia Video Industry Association¹ (AVIA) is a firm supporter of intellectual property rights, and for good reason – the video and pay TV industry in Asia loses more than a billion US dollars annually to unauthorised connections of various types to our member companies' networks.

AVIA monitors developments in the region and maintains a twin dialogue with governments and with industry. We believe that anti-piracy efforts depend crucially on three elements:

- **Technology:** to provide strong safeguards against unauthorised access.
- **Law:** to provide updated, meaningful penalties to deter infringement of copyright and of broadcasting control laws.
- **Enforcement:** to ensure that laws are carried out and that a vicious circle of piracy does not undermine the industry's contribution to Asian development.

Acknowledgments

With thanks to White Bullet² and NAGRA³ for their support in this project.

White Bullet work closely with IP rights owners in a variety of sectors, including film, TV, music, software, sports, pharmaceuticals and eBooks amongst others, to provide insightful intelligence about online piracy and infringement to help focus enforcement and commercial decisions.

NAGRA is the digital TV division of the Kudelski Group. The Kudelski Group has a long history of innovation in the areas of content protection, content delivery, access control systems, smart cards, and interactivity. NAGRA solutions benefit from the Group's 5,300 worldwide patents which pioneered technical paradigms that are in use today and are fundamental to the delivery of a modern content viewing experience.

1 <https://www.avia.org/>

2 <https://www.white-bullet.com/>

3 <https://dtv.nagra.com/>