



# AUDIOVISUAL PIRACY CYBER RISK FOR EUROPEAN CONSUMERS

THE RISE OF MALWARE

THE AUDIOVISUAL ANTI-PIRACY ALLIANCE

ENQUIRIES:

**Sheila Cassells**  
Executive Vice President

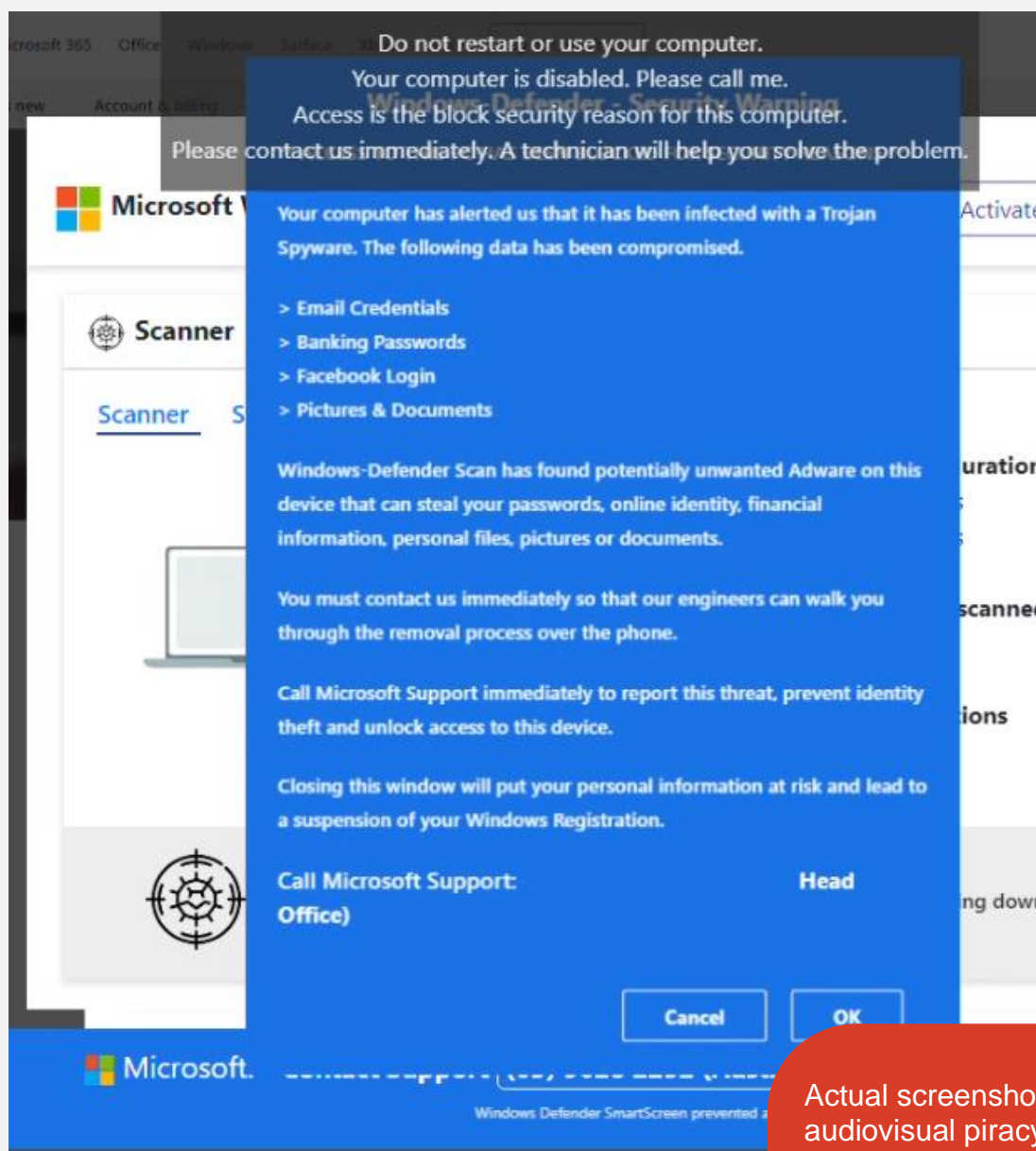


## EXECUTIVE SUMMARY

Like consumers worldwide, European users of audiovisual piracy sites, apps, Illegal Streaming Devices, and Set-Top Boxes (STBs), often perceive that they can get “something for nothing” by using these services. Piracy is often perceived to be a victimless crime. The evidence presented in this study shows that the victim is the consumer, through the targeted delivery and installation of malicious software (malware) onto consumer devices, while they use audiovisual piracy sites, apps, ISDs and STBs. The impact of these malware infections can result in identity theft and fraud for the consumer, but also, lateral movement and further infection on any corporate network that they are connected to, such as remote working at home through a Virtual Private Network (VPN). Consumer behaviour is a direct threat to corporate networks, and the commercial consequences could be devastating, especially as more workers choose a flexible work pattern.

This study examined malware infection techniques across a broad range of actors targeting European consumers, finding that malware can be downloaded through malicious advertising, malicious popups, fake browser extension installations, browser notification hijacking, blocking notifications, adware, malicious software installation and banner ads. Furthermore, the study found an average 57% chance of an audiovisual piracy app being installed with embedded malware.

While European policymakers have focused on strengthening cybersecurity protections for many years, in practical terms – compared to Asian consumers in a similar study – there was no appreciable impact of these protections when visiting audiovisual piracy sites in relation to malware risk. The results of this study suggest that European regulatory frameworks need to focus on preventing consumer access to malicious audiovisual piracy sites, apps and STBs, through an expansion of regulatory site blocking, while acknowledging the risk of piracy-driven malware driving identity theft, in relation to the rollout of the European Digital Identity, and similar policy initiatives.



Actual screenshot from an audiovisual piracy site, a variation on the technical support scam, where a Remote Access Trojan (RAT) is installed on a consumer's PC.

**The infection was triggered within 30 seconds of searching for audiovisual piracy content.**

# INTRODUCTION

Audiovisual piracy has a significant impact on the creative economy in Europe; lost sales are estimated to range from 1.65% for Germany to 10.4% for Spain<sup>1</sup>, with nearly 70% of Europeans streaming or downloading films “for free”, according to a survey of more than 30,000 consumers. These direct losses impact on future investment for new creative content, limiting the capacity of artists to bring their work to the marketplace in a sustainable way, as well as reducing tax revenues for governments. Looking at Spain alone, it is claimed that audiovisual piracy costs more than 2 billion euros annually, and 20,000 jobs<sup>2</sup>. Globally, there are more than 357 million daily visits to audiovisual piracy sites<sup>3</sup>, with Europe disproportionately accounting for 45.72% of traffic.

Taken in isolation, these are quite shocking statistics. However, they do not tell the whole story about audiovisual piracy operators, and how they make money. While these operators generate revenue through a variety of means – including paid subscriptions and digital advertising – their activities directly introduce cyber security threats by injecting malicious code onto the devices and PCs owned and operated by consumers. This less obvious threat to the European economy is the topic of this report, and must be considered by policymakers alongside the more obvious impact on corporate revenue, and subsequently, the taxes raised that pay for hospitals, schools and other public amenities. In short, European consumers and businesses are at serious risk of cyber attacks, mediated by the use of piracy sites, apps and Set Top Boxes (STBs), through the installation of malicious software (otherwise known as “malware”).

Malware is a key cyber security risk for individuals and businesses. Malware is computer code that is installed and executes on any device – such as a PC, smartphone or Smart TV – with the purpose of compromising that device, by a malicious actor. These malicious actors range in capacity and cyber security skill; from nation states (for intelligence) through to organised crime groups (for money), as well as amateurs (often for curiosity). With legitimate sites providing extensive cyber security protections for their customers, audiovisual piracy operators use the promise of free audiovisual content to lure users into a false sense of security, while infecting them with malware.



A malware “infection” installed through an audiovisual piracy site can be used for a number of purposes once a device has been “pwned” (owned) by a remote attacker:

- capturing network traffic and banking credentials typed into a browser to commit fraud, such as paying for goods and services via “Card Not Present” transactions. In the UK alone, 24% of people have experienced online banking or card fraud in the past five years<sup>4</sup>;
- facilitating identity theft by capturing personal data stored on a phone or a PC, before being used directly by a criminal in a scam, or on-sold to other criminals. One

<sup>1</sup> <https://www.sciencedirect.com/science/article/abs/pii/S016762451730152X>

<sup>2</sup> <https://www.digitaltveurope.com/2021/10/26/piracy-cost-spanish-economy-more-than-e2-billion-and-20000-jobs-in-2020/>

<sup>3</sup> <https://www.go-globe.com/online-piracy/>

<sup>4</sup> <https://fra.europa.eu/en/news/2020/security-and-crimes-europeans-worry-about-online-banking-fraud-data-misuse-and-terrorist>

in five Europeans have reported being the victims of identity theft in the past two years<sup>5</sup>;

- moving laterally within a network to reconnoitre and compromise other, higher-value devices, such as finance and payment systems.



Why do audiovisual pirates create malware? Put simply, it is one of the easiest forms of crime to commit, since:

- the perpetrators can attack their targets without being in physical proximity;
- the likelihood of detection is low;
- the consequences of detection are minimal, given the practicalities of extraterritoriality; and
- the potential payback – in terms of intelligence collected or funds stolen - is virtually unlimited, and can be facilitated “in country” by local accomplices such as “money mules”, who can launder stolen funds.

**Every device** connected to the internet that is involved in the audiovisual piracy value chain – including mobile phones, tablets, PCs, STBs, ISDs, Smart TVs, and so on – is a potentially infectable endpoint. These devices can also be compromised at different levels and in different places in the technology stack – browser plugins can be used to steal personal data (“man-in-the-browser”), for example, or operating systems can be infected to capture or manipulate network traffic being received or transmitted (“man-in-the-middle”). Some compromises will be obvious, especially if funds are stolen from bank accounts; others may last months or years, with the silent threat from nation states using malware to spy on other nations, businesses or consumers, especially activists and other targets.

In financial terms, malware is increasingly impacting consumers and businesses in Europe, despite very high levels of cyber security investment, and audiovisual piracy sites are a potential source of infection for corporate networks; a recent report by the Digital Citizens Alliance found that 25% of Americans who used piracy devices had a malware infection in the prior 3 months, and 49% in the prior 12 months<sup>6</sup>. Europe is not immune to the problem: a student at a well-known COVID-19 research facility installed “cracked” software downloaded from a piracy site, resulting in data loss and compromise of the entire network through ransomware, installed via a remote connection after login details were sold on the black market<sup>7</sup>. A recent Forrester and Hiscox report<sup>8</sup> found very large increases in the numbers of European firms reporting cyber incidents, with the cost of each incident also rising, now €50,000 per incident, based on a survey of more than 5,500 technology leaders. These costs have risen sixfold in the space of one year, as the costs of recovery, fines from regulators due to data breaches, and new investment in cyber defence technology (up 30% annually) create their own financial impact.

An important question is, where does all of the malware come from, and how do consumers and businesses become infected in the first place, and how much of this can be attributed to audiovisual piracy sites? According to leading security firm Comodo Cybersecurity, there are four key sources<sup>9</sup>:

<sup>5</sup> <https://www.grcworldforums.com/fraud/one-in-five-europeans-have-experienced-identity-theft-fraud-in-the-past-two-years/351.article>

<sup>6</sup> <https://www.tvtechnology.com/news/piracy-devices-increase-risk-of-cyber-attacks-survey-finds>

<sup>77</sup> <https://au.pcmag.com/security/87052/ransomware-hits-research-facility-after-student-installs-pirated-software>

<sup>8</sup> <https://www.consultancy.eu/news/4409/cost-of-cybercrime-per-incident-jumps-six-fold-to-50000>

<sup>9</sup> <https://enterprise.comodo.com/where-does-malware-come-from.php>



- **“Shady” Websites** – users are lured into downloading or installing seemingly legitimate software which is actually malicious, often disguised as games or software updates, and/or making promises of “free money”. Advertising on these sites is also often used as a malware download vector;
- **P2P File Sharing** – users install P2P client software that can be used to also download malware, or potentially participate turn consumer PCs into “bots” to support Denial of Service (DoS) attacks;
- **Torrent Downloads** – consumers may seek to download pirated content, including software which may have malware embedded, or key generators and software “cracks” may also contain malware;
- **Phishing Emails** – some phishing emails contain embedded malware; when the attachment is downloaded, it can execute and immediately gather sensitive data about the user.

Audiovisual piracy plays a critical role in three out of four cyber attack categories. Typically, a “shady” website contains links to torrent files, and/or contains malicious advertising, and/or prompts users to install masquerading software. Users seeking a “free lunch” can quickly find that their entire PCs are compromised, and this compromise can then lead to all other devices behind the firewall also being compromised. Thus, the potential attack surface extends far beyond the individual consumers; in short, any network that they are connected to can be exposed to a malware infection mediated through audiovisual piracy.

How much malware comes from audiovisual piracy, and why is this important to know? In terms of cybersecurity risk reduction, broad measures which have the greatest impact but the smallest cost are usually those sought by businesses and policymakers. There is no single “silver bullet” which can reduce cyber risk to zero: however, there may be low-hanging fruit which can be addressed at a policy level. So, it is important to enumerate and risk-assess all possible malware sources with a view to risk reduction. Put simply, can policymakers reduce cyber security risk by preventing access to audiovisual piracy sites, apps, STBs and ISDs through strategies like regulatory site blocking? And is the cost justified by the risk reduction achieved? The findings in this report – such as the presence of malicious pop-ups, browser notification hijacking, malicious browser extensions, malvertising on audiovisual piracy platforms - suggest that the risk reduction is eminently justifiable, in the context of European spending on cybersecurity. Site blocking costs are very reasonable – estimated in Australia to be as little as \$50 per domain by one of the largest ISPs<sup>10</sup> – but the protections afforded can impact millions of consumers.

Europe is not alone in combating the malware risks from audiovisual piracy. Asia has been similarly impacted; yet European law and regulation is often seen as a barrier and broader form of protection from that cyber attacks that occur elsewhere, including the NIS Directive, the Cybersecurity Act, ENISA, and so on. The broader question is, how well do European protections really stack up, and what could be done to improve them?

A recent study from the Asia Video Industry Association (AVIA) suggested that consumers believe that 31% of malware infections could be attributed to visiting piracy sites, using piracy apps, or set top boxes (STBs) that provide pirated content<sup>11</sup>. While the numbers may change from region-to-region, and user perceptions may underestimate overall infection statistics, it is intriguing from a policy perspective that

<sup>10</sup> <https://www.zdnet.com/home-and-office/networking/telstra-argues-against-compliance-costs-for-piracy-website-blocking/>

<sup>11</sup> The “Time to Compromise” report is available from <http://www.avia.org/>

infections can be attributed to a single source. By reducing risk through proactive measures – such as regulatory site blocking – the broader impact of malware infections could be significantly reduced.

A second, empirical AVIA study explored the actual risks for consumers within the Asia-Pacific region, by simulating a range of user activities on piracy and streaming sites. The report found that serious malware infections typically occurred in less than one minute after the first visit to a site.

A third study conducted by UK FACT<sup>12</sup> highlighted the scale and significance of the problem in the UK. 50 streaming sites were analysed, with more than 90% being classified as risky by cybersecurity experts, with users being inundated with pop-ups, trojans, banking malware and other infections being observed. 40% of these sites had no security (to protect consumers), and infecting consumer devices was simple– a good example was clicking the “mute” button to enable sound on a live stream triggered the download and installation of a banking trojan horse.

In this report, we explore whether European consumers are similarly at risk from audiovisual piracy sites. To some extent, European users enjoy very significant legal and regulatory protections against data breaches resulting from cyber attacks, including the General Data Protection Regulation (GDPR), which enhances an individual’s rights and control over their personal data. From an empirical perspective, though, are the various regulatory protections in Europe sufficient to protect businesses from malware infection via piracy across all possible means of access, including piracy and streaming sites, STBs or mobile devices? If not, what are the specific changes in policy that could reduce malware infections thought to be attributable to piracy? Do pirates really care about ENISA, the Cybersecurity Act, the INS Directive, and do they collectively act as a deterrent? This is the question that this report seeks to answer.



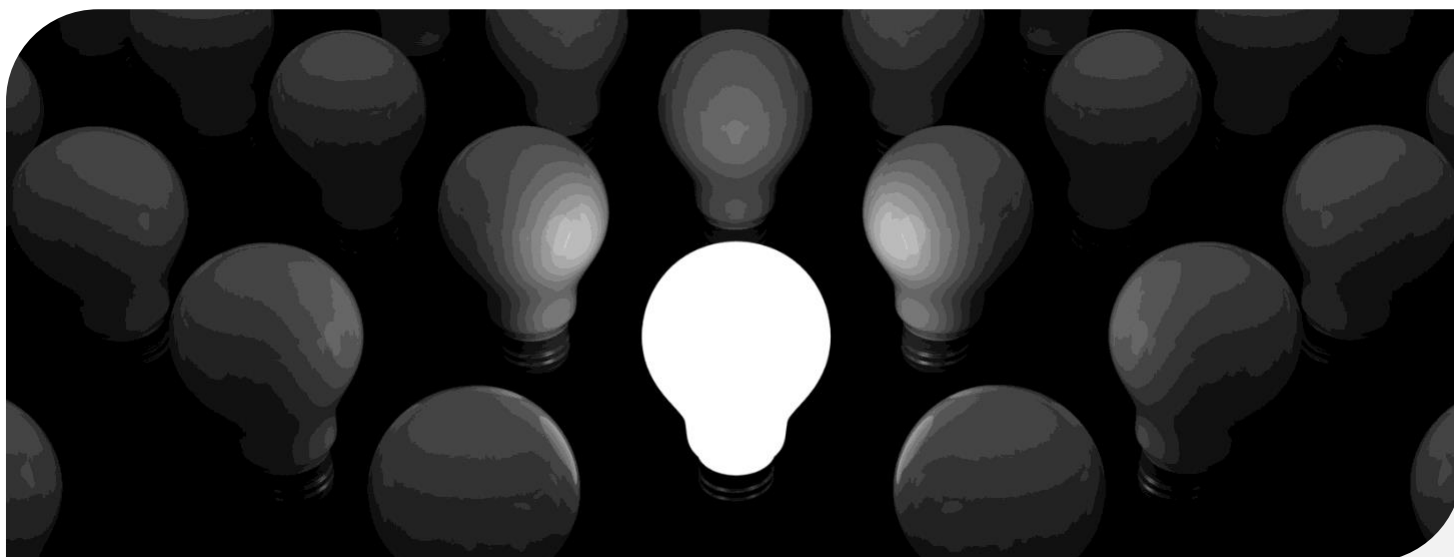
We also reflect on the business models sitting behind the operation of audiovisual piracy sites and apps. The backend infrastructure of such sites is expensive to operate, yet the cost of content is borne by others: therefore, the profit margins are enormous, depending on the revenue model. Revenue can be generated by:

- Hosting mainstream advertising – after all, advertisers want to maximise eyeballs and clicks, and sites offering a product for free have natural advantages in generating organic traffic compared to paid (legal) services<sup>13</sup>.
- Hosting high-risk advertising – malware opens up opportunities for identity theft and related referral fees from other cybercriminal groups.
- CPC Hacking – malware installed on consumer devices can be used to click on ads generating revenue streams via CPC fraud.
- Subscription – pirate sites and apps can charge a subscription fee for access, often at a steep discount to legal services.
- Advertising redirection – browser extensions can be used to generate illicit revenue by displaying unauthorized ads in place of legitimate ads.

As we will see in the Results, audiovisual piracy site revenue models drive decisions about how and when malware may be used to increase profits.

<sup>12</sup> <https://www.fact-uk.org.uk/new-research-finds-illegal-sports-streaming-sites-expose-fans-to-financial-fraud-dangerous-scams-and-explicit-content/>

<sup>13</sup> The author has previously calculated the profit margins for piracy sites to be in the order of 1,272% - [http://www.ballarat.edu.au/\\_data/assets/pdf\\_file/0020/129521/ICSL-report\\_digital.pdf](http://www.ballarat.edu.au/_data/assets/pdf_file/0020/129521/ICSL-report_digital.pdf)



## METHODS

We set out to empirically test whether Europeans are better protected against cyber attacks stemming from audiovisual piracy sites. We can also directly compare the results of such a test with some countries in Asia, where consumers appear to have fewer rights and protections against cyber attacks through specific laws and regulations.



The results indicate where Europe can consider further strengthening protections for consumers **against cyber attacks stemming from the use of predatory audiovisual piracy sites.**



We created “simulated users” on a Windows 10 Virtual Machine (PC) with 16G RAM, a Samsung 10.1” Android Tablet, an emulated Android tablet using BlueStacks<sup>14</sup>, and a typical Set Top Box (STB) – a Formuler Z<sup>15</sup>+. These simulated users had their logical IP addresses set to a range of European countries by means of a NordVPN Virtual Private Network (VPN). The purpose of the simulated users was to interact with a range of audiovisual piracy sites, apps and devices, with a view to identifying and enumerating the malware risks encountered. This ethnographic approach provides an empirical “ground truth” about the actual experiences of users across a range of sites, devices and technologies, allowing us to map out the malware landscape with respect to audiovisual piracy.

**The process followed for each device type (PC, Tablet, STB) was as follows:**

- AAPA members were asked to provide lists of sites, applications and STBs that were known to be involved in audiovisual piracy, eg, they have been added to a regulatory site blocking list, or were being surveilled.
- Simulated user email addresses were established, to enable subscriptions within those sites requiring registration.
- Simulated user activity on each audiovisual piracy site, application or device was undertaken over a reasonable timeframe, typically one hour each. This enabled a representative range of simulated user activity to undertaken, including:
  - registering as a user
  - clicking on suggested title links, searching for titles
  - clicking on advertisements
  - allowing popups
  - permitting browser notifications from sites, and
  - installing suggested software, where downloads were initiated from the site.

**For each of these activities, actual Indicators of Compromise (IoCs) were measured across all devices, sites, applications, and so on. These were categorized, and further data gathered to understand their actual impact. This included:**

- Disabling anti-virus and adblocking protection before sites visit, and then scanning for malware on PCs after each site was visited
- Capturing and analysing network traffic to and from the device
- Analysing Android piracy apps for embedded malware
- Measuring timelines to infection
- Comparisons with comparable Asian test scenarios

All of this data was then used to enumerate the most common compromise patterns, which have been compiled into a malware infection process model, showing all known infection strategies detected on audiovisual piracy sites, apps and STBs. The infection strategies are presented using flowcharts for ease of interpretation.

---

<sup>14</sup> Both a physical and emulated device were tested, since malware can typically detect whether it is executing on bare metal or an emulated environment.

<sup>15</sup> <https://www.formuler.tv/z-plus>



## PCs

Analyse devices for  
malware infections



## Devices

Check for embedded  
malware in apps



## Indicators of Compromise

Describe all possible  
attack pathways



# RESULTS

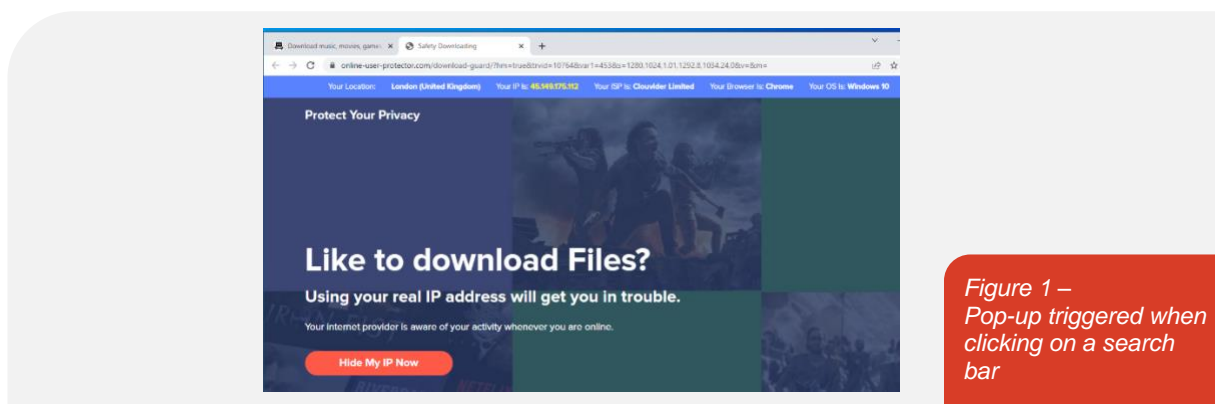
The results are divided into five different sections – three by device type (PCs, Mobile Apps, STBs); Indicators of Compromise (IoC) and Consumer Impact; and Comparison with Asia.



## PCs

The following patterns of potential infections were observed which either gave rise to a malware infection, or could provide a potential pathway for infection:

1. **Pop-up windows.** When a JavaScript event is triggered, such as clicking in a window, on a link or search box, a popup appears, which can be used to install malware through a third-party site. This is a common deception pattern observed throughout many of the sites – users believe they are clicking on a magnet link, for example, but a pop-up is instead triggered, often on several occasions through the same action. Figure 1 shows a popup triggered when clicking on a search bar in a torrent site.



As shown in Figure 2, sometimes the pop-ups then require a user to click on another link before an infection will occur. In this interstitial case, intellipopup.com appears in the first pop-up. This site has a trust score of 1/100 by ScamAdviser<sup>16</sup> and is reported as unsafe by Trend Micro. When the site loads, it reports that a user's system has crashed, and that they must purchase a support contract by calling a phone number<sup>17</sup>. The malware installed can also popup new advertising banners, insert hyperlinks into plain text pages, recommend fake updates (potential malware) or install other third party applications.

<sup>16</sup> <https://www.scamadviser.com/check-website/intellipopup.com>

<sup>17</sup> <https://malwaretips.com/blogs/intelli-support-assistant-com-removal/>

https://intellipopup.com/AU.htm?r=7198411&j=630818483&a=1652233618&l=7638  
 intellipopup.com/AU.htm?r=7198411&j=630818483&a=1652233618&l=  
<https://free-cosmetics-online.com/getnow>

Figure 2 – Interstitial Malicious Popups

As reported URLScan, a number of sites link to this site<sup>18</sup>, including:

- Porn sites, including JAVJunkies.com and Vidoz8.com
- European piracy sites, such as Balkanje.com (Bosnian)
- European streaming sites, including Futbolfullenvivo.com (Greek)
- US piracy sites, such as dbx.to and movelinkshd.bar

Another example of pop-up window malware is shown in Figure 3.

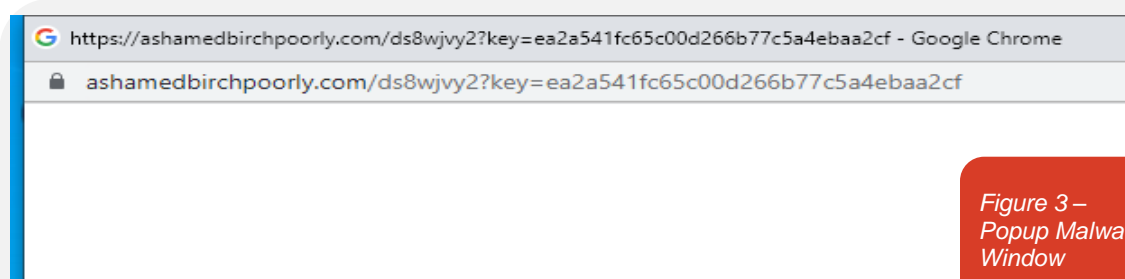


Figure 3 – Popup Malware Window

In this case, a popup is initiated after clicking on a magnet link to a domain comprising three nominal words (“ashamed”, “bitch”, “poorly”), probably selected at random from a dictionary. Figure 4 shows the MITRE ATT&CK mapping<sup>19</sup> for this malware sample: it tries to actively evade detection while discovering more about the system on which it is installed, feeding back information to the attacker.

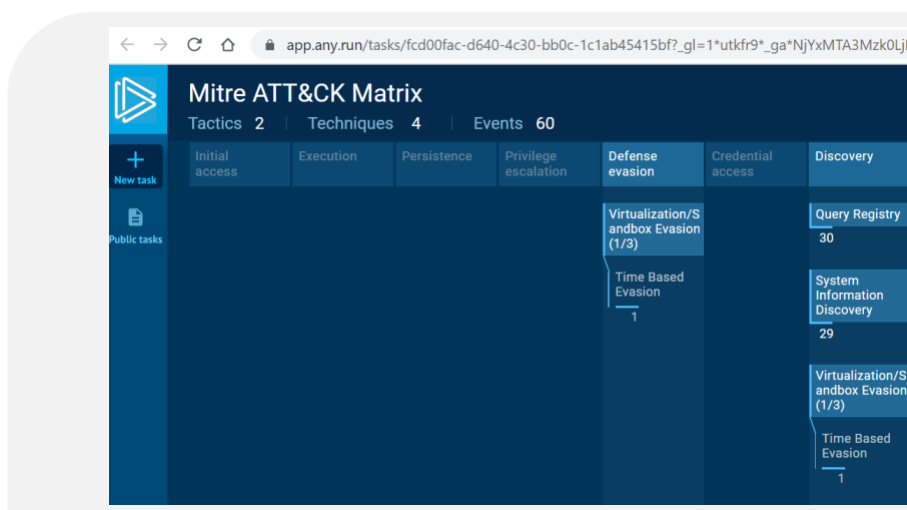


Figure 4 – MITRE ATT&CK Mapping

<sup>18</sup> <https://urlscan.io/domain/intellipopup.com>

<sup>19</sup> [https://app.any.run/tasks/fcd00fac-d640-4c30-bb0c-1c1ab45415bf?\\_gl=1\\*utkfr9\\*\\_ga\\*NjYxMTA3Mzk0LjE2NTQyMjEyMzk\\*\\_ga\\_53KB74YDZR\\*MTY1NDIyMTIzOS4xLjAuMTY1NDIyMTIzOS42MA..&\\_ga=2.39091683.1190934658.1654221239-661107394.1654221239/](https://app.any.run/tasks/fcd00fac-d640-4c30-bb0c-1c1ab45415bf?_gl=1*utkfr9*_ga*NjYxMTA3Mzk0LjE2NTQyMjEyMzk*_ga_53KB74YDZR*MTY1NDIyMTIzOS4xLjAuMTY1NDIyMTIzOS42MA..&_ga=2.39091683.1190934658.1654221239-661107394.1654221239/)

The activities undertaken include:

- a. Reading the computer name
  - b. Checking supported languages
  - c. Reading system security certificates
  - d. Reading the network hosts file
  - e. Checking the Windows installation date
2. **CPC Fraud Malware.** Following analysis of the piracy sites, Microsoft Defender was re-enabled, and a Win32/Doplik.AA infection was detected<sup>20</sup>. This malware is designed to generate advertising revenue for its authors, by simulating clicking on ads on other sites, where the author is paid through a CPC Cost Per Click) scheme.
  3. **Browser Notification Hijacking.** Often under the guise of CAPTCHA to “prove” that the consumer is really a “human”, as shown in Figure 5, the site requests permission to show notifications.

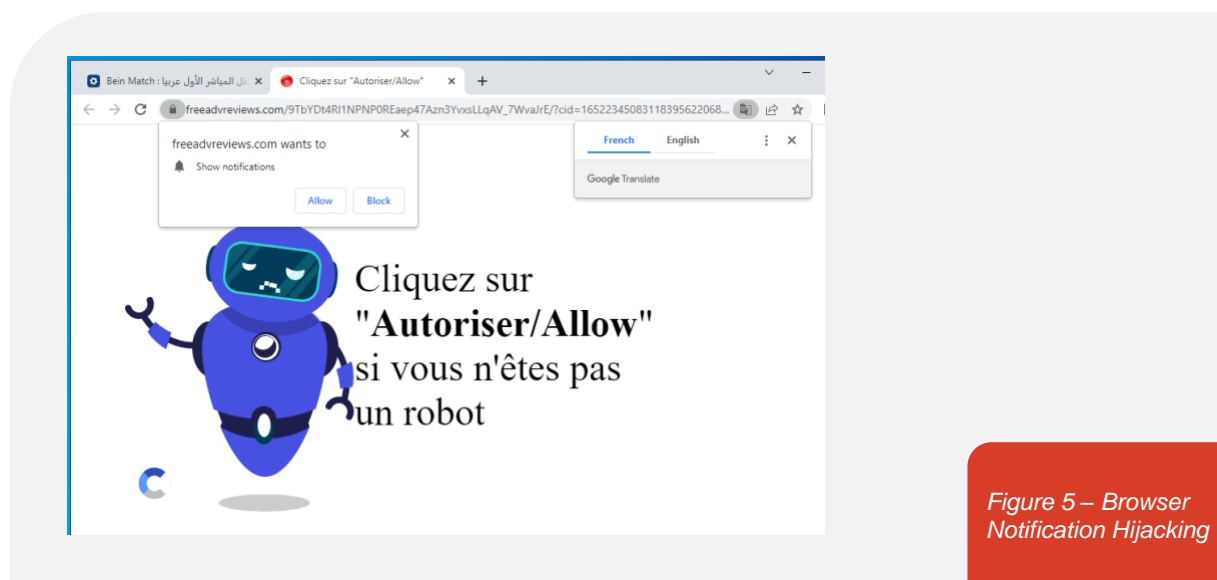


Figure 5 – Browser Notification Hijacking

If the user gives permission, there is typically no time limit to when notifications can be shown; often the frequency is so high that it is impossible to enter the browser settings menu to disable the notifications within the browser, as shown in Figure 6.

<sup>20</sup> <https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=TrojanClicker:Win32/Doplik.A&threatId=-2147203273>



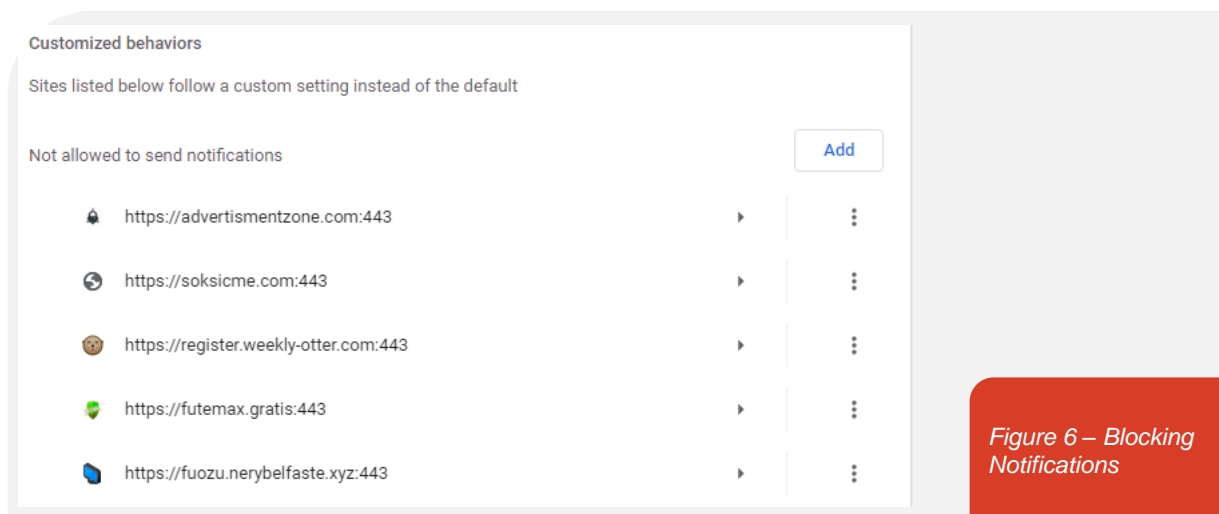


Figure 6 – Blocking Notifications

Sometimes, the notifications contain web links to malware downloads; other times, as shown in Figure 7, they can be used to display ads from legitimate advertisers, but which are in themselves quite misleading.

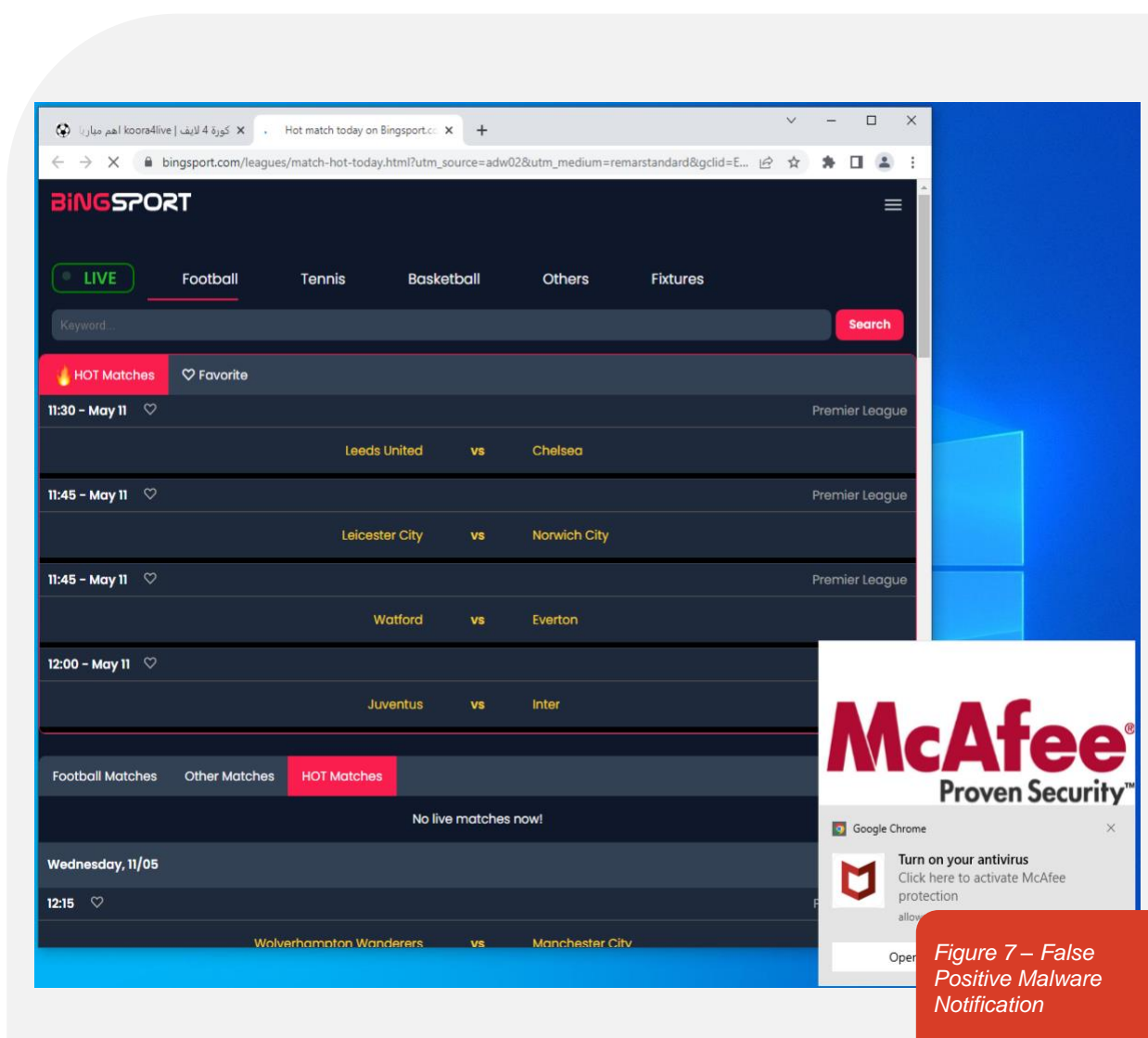
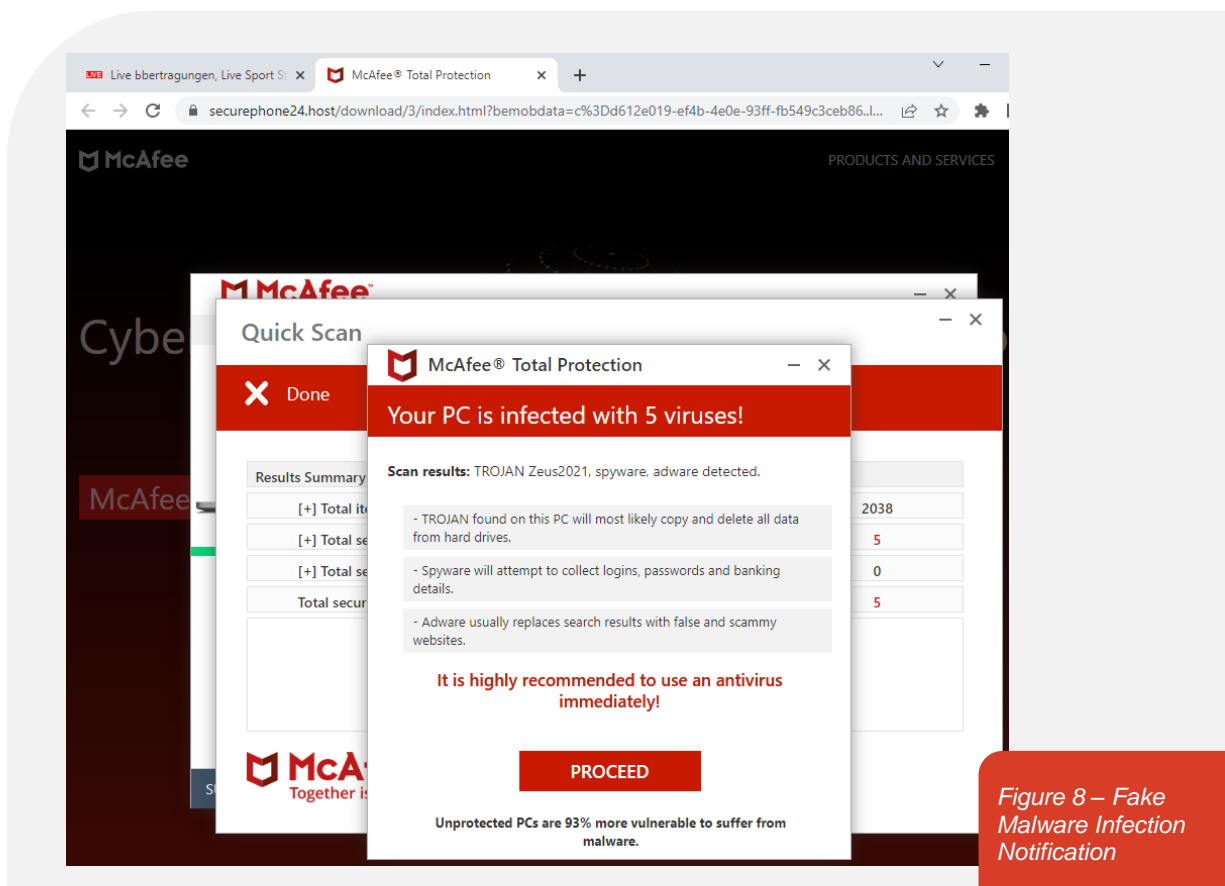
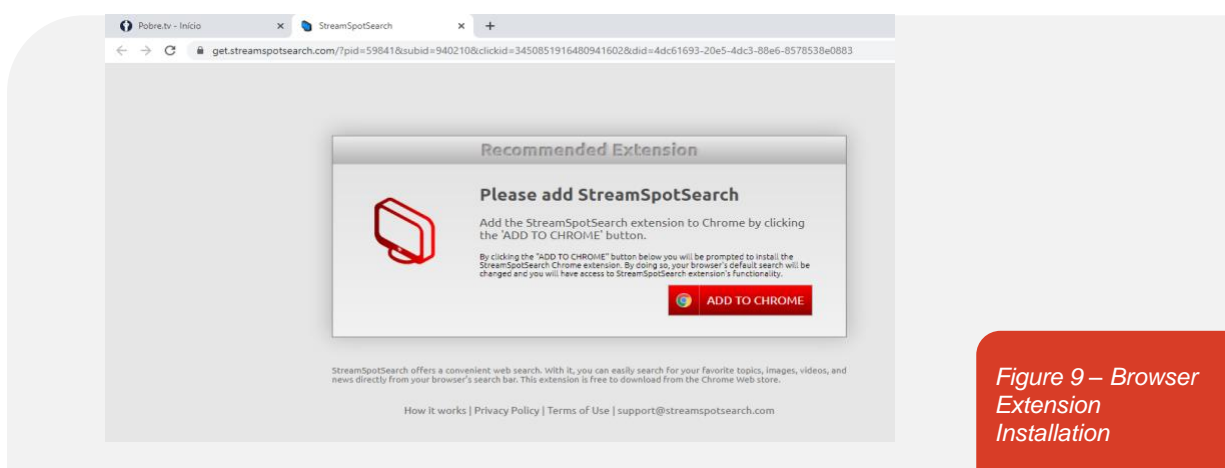


Figure 7 – False Positive Malware Notification

In this case, a legitimate antivirus company shows a number of images on the screen which purport to indicate that the PC is infected with a virus, when it is actually not, and encourages the user to purchase a subscription – as shown in Figure 8.



4. **Browser Extension Installation.** As shown in Figure 9, the user is presented with a pop-up window that then triggers a request to install a browser extension.



Sometimes, the request is framed in such a way as to maximise compliance, for example, an extension may be required to view a stream or a video using a new CODEC. Invariably, these code extensions contain malware, as shown in Figure 10.

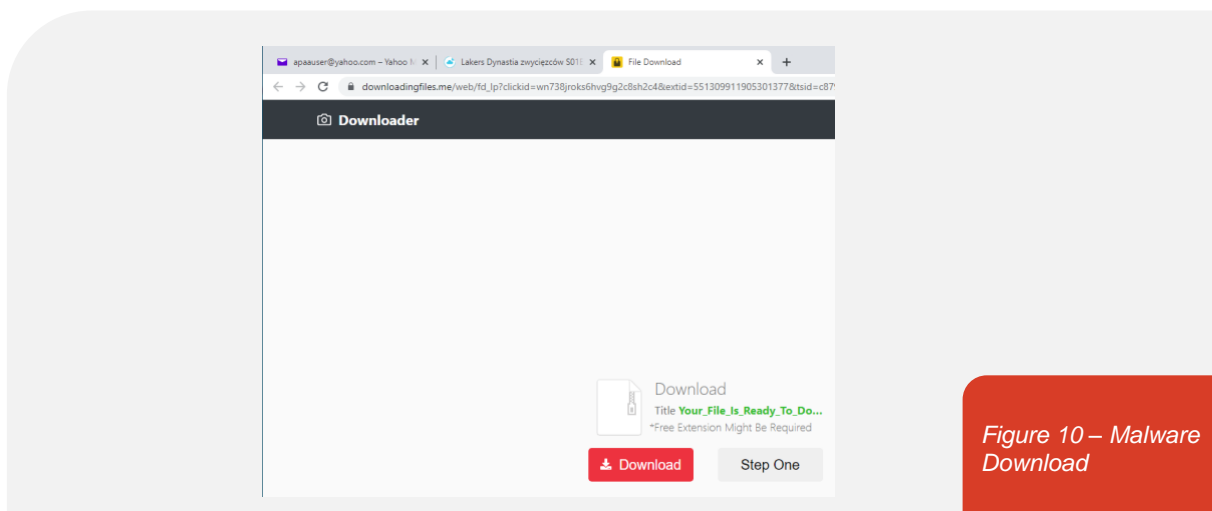


Figure 10 – Malware Download

5. **Adware.** Figure 11 shows an example of an ad hijacking application. This type of malware replaces ads being served by the ad network embedded on a web page with those generated by the ad hijacker.

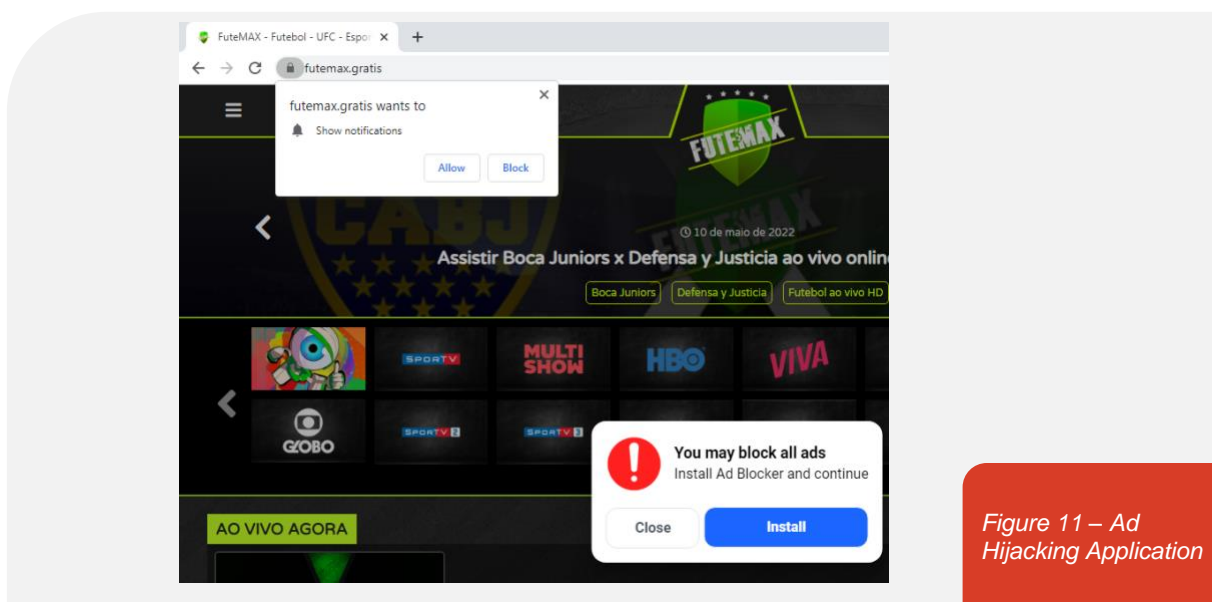
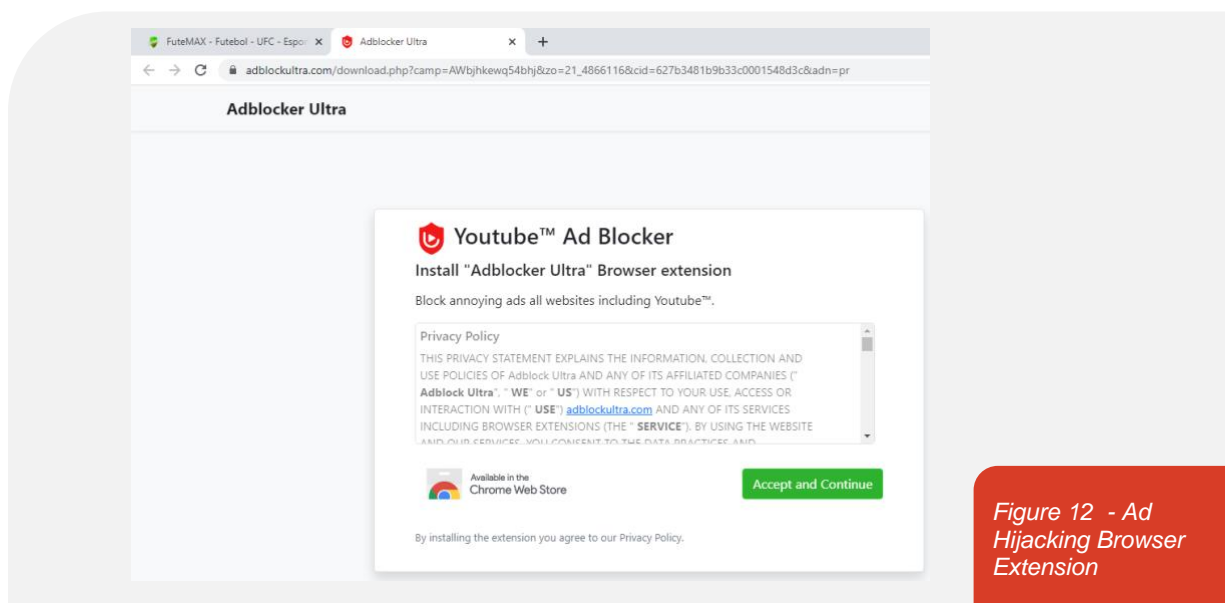


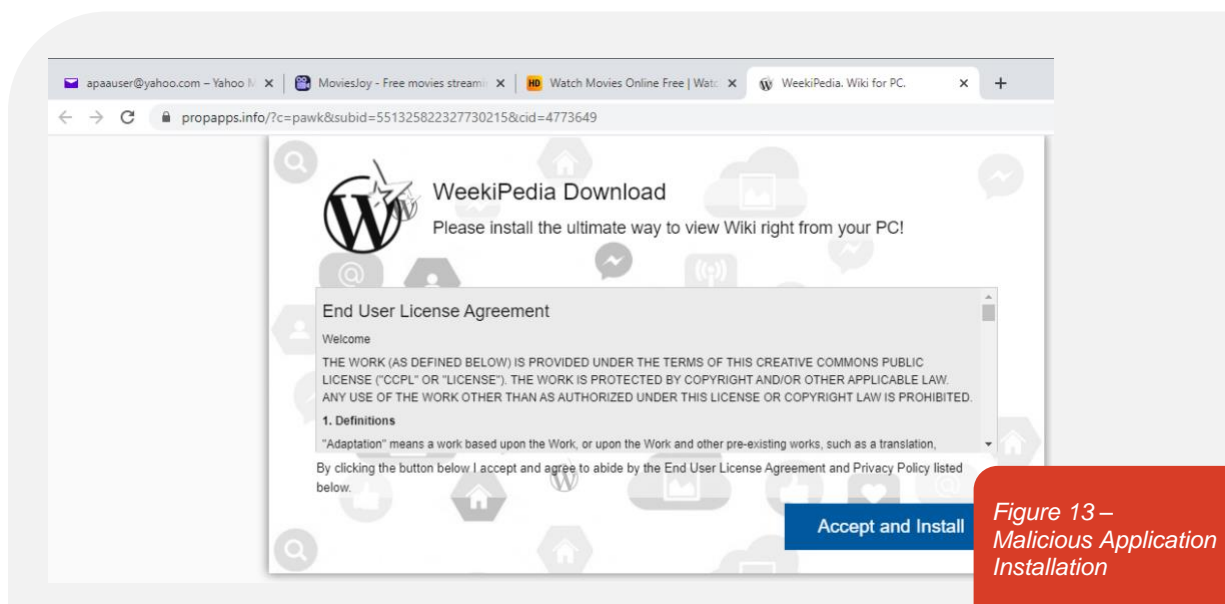
Figure 11 – Ad Hijacking Application

Thus, ad networks lose revenue, and ad hijackers generate revenue from their own ads. As noted by a malware removal guide<sup>21</sup>, this type of “adware” can lead users to “shady” websites, and potentially display ads that can deliver more malware. The user is alerted by a pop-up in this case, and a browser extension is installed, as shown in Figure 12.

<sup>21</sup> <https://www.pcrisk.com/removal-guides/23497-ad-block-ultra-adware>



6. **Full Malicious Application Installation.** Figure 13 shows a full Windows application installed via an ad-mediated popup.



This shows the WeekiPedia application, which has been identified by PC Risk as a rogue application that contains adware<sup>22</sup>, and classified as a variant of Win32/Aware.BookLot.A by ESET-NOD32<sup>23</sup>. Figure 14 shows the output from the downloaded sample uploaded to VirusTotal.

<sup>22</sup> <https://www.pcrisk.com/removal-guides/21263-weekipedia-adware>

<sup>23</sup> <https://www.virustotal.com/gui/file/4e34e101c49b1f209fd6e725d43587a794a27efa05477c38bb43b07204a15d88/detection>

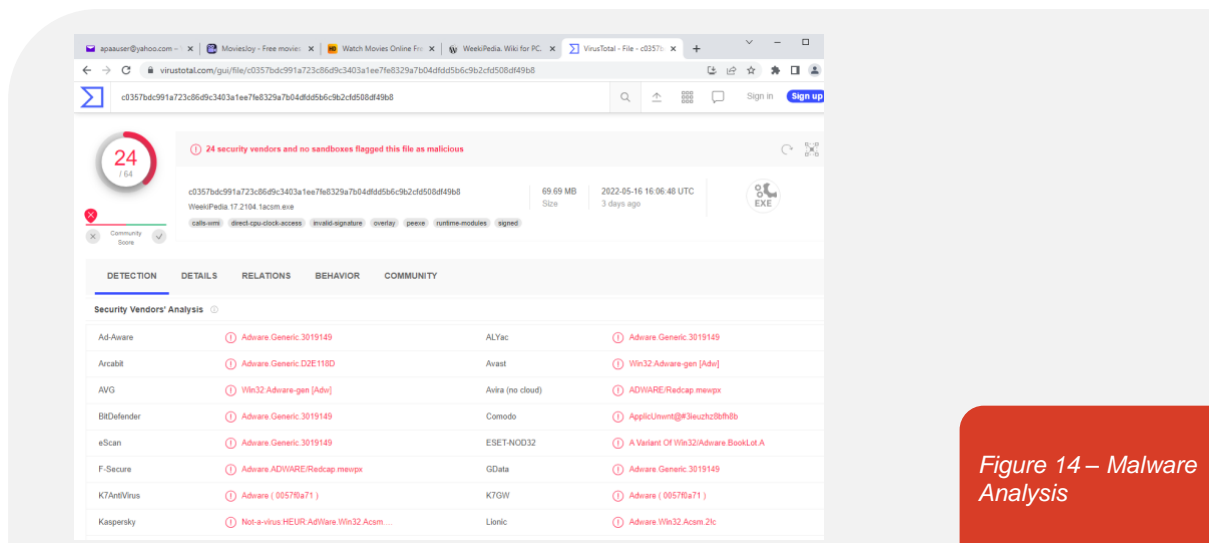


Figure 14 – Malware Analysis

- Malicious Banner Ads.** Banner ads have links which – when clicked – direct users to malicious downloads or browser extension installation.

Other non-malware sources of revenue generation, were observed:

- Subscription models.** Some sites carried no ads at all, instead relying on subscription. Legitimate payment processors facilitate payments, as shown in Figure 15.

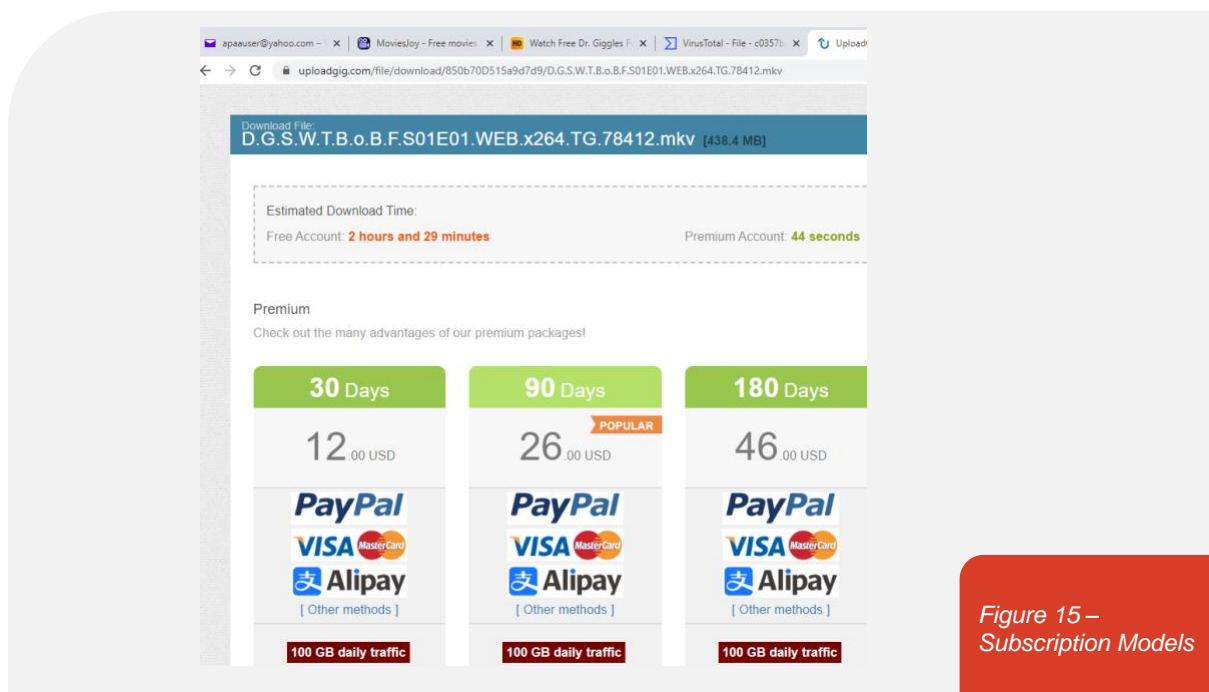


Figure 15 – Subscription Models



2. **Mainstream advertising.** Legitimate ad networks (such as Google ads) placed ad blocks on known piracy sites, with site owners either being paid through CPC or other affiliate marketing schemes. Figure 16 shows an example – mainstream, advertisers like O2 and Blau have their ads placed on a site clearly distributing copyrighted works. It is not clear whether the advertisers are aware of where their ads are being placed.



Figure 16 – Mainstream Advertising Supporting Piracy

3. **False Positive malware.** An extension of mainstream advertising, the example shown in Figure 17 shows a mainstream site with a pop-up notification that anti-virus protection may have expired.

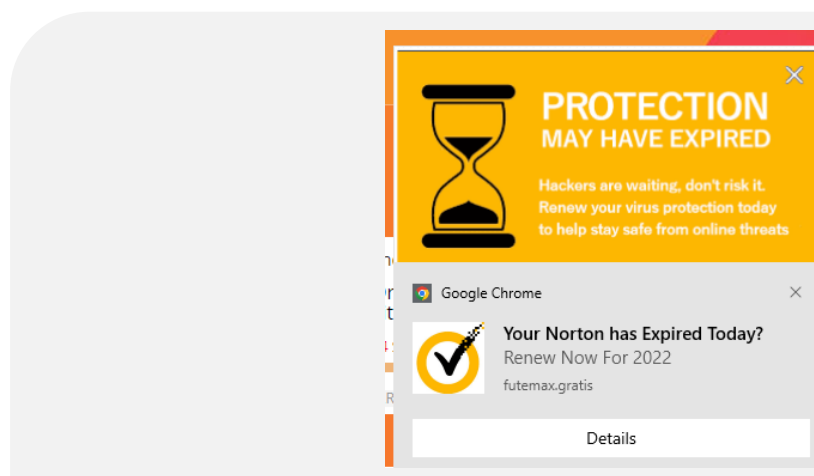


Figure 17 – False Positive Malware

This could generate revenue for the anti-virus company, even though no malware has been detected; false reports of malware infections are deceptive and misleading, as shown in Figure 18.

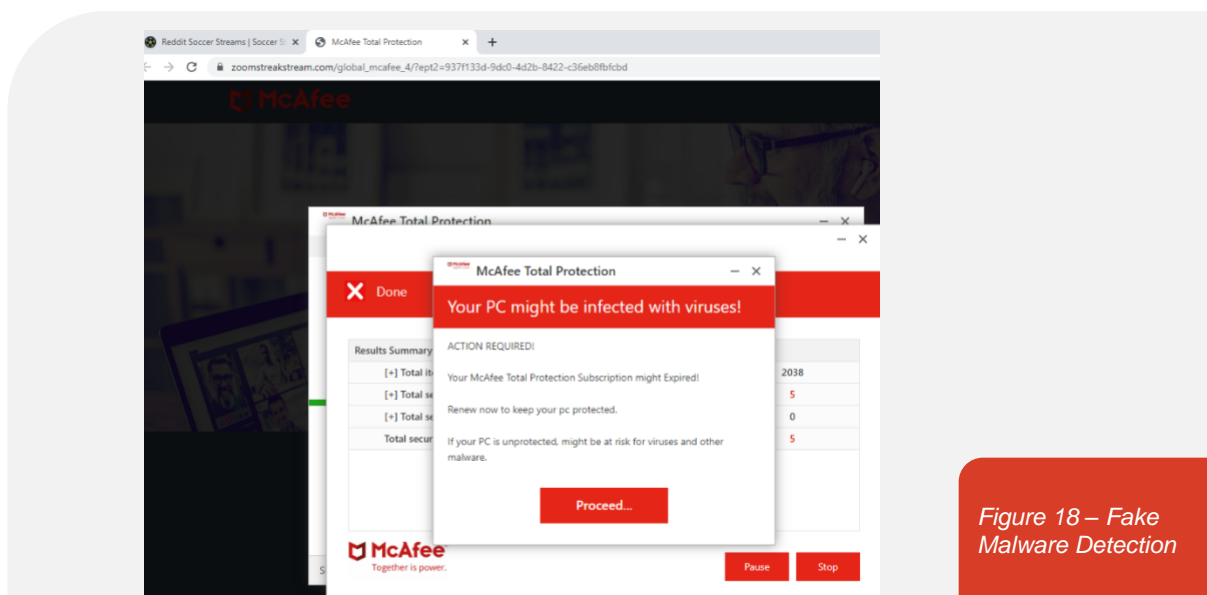


Figure 18 – Fake Malware Detection

4. **VPN Services.** Alerting users to the fact that their IP addresses and location are exposed while viewing streaming sites, VPN vendors typically place prominent ads as shown in Figure 19. These can generate significant revenue for the VPN vendors. Placing the ads on these sites may indicate a level of knowledge by the VPN vendors about the illicit activity taking place.

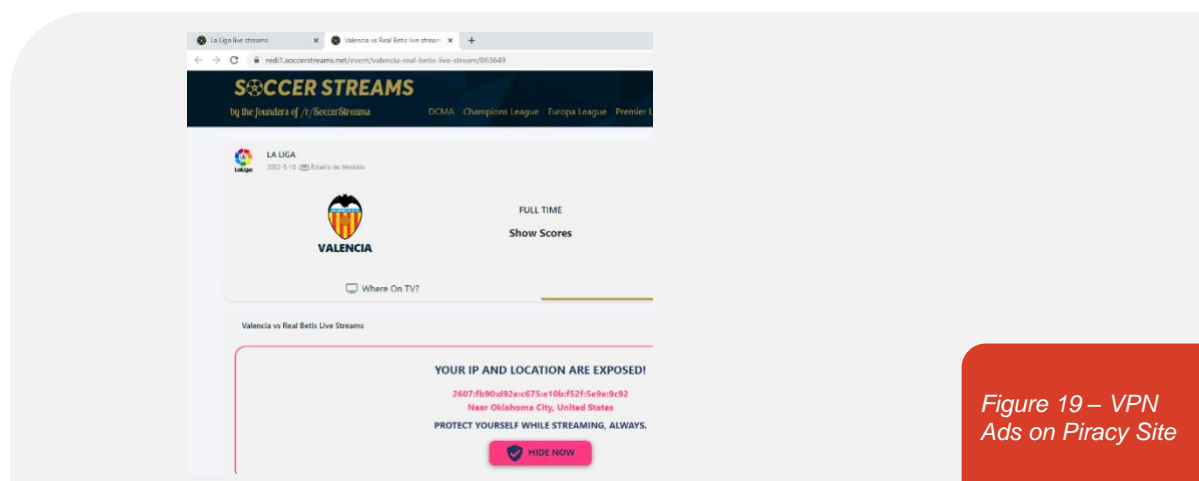


Figure 19 – VPN Ads on Piracy Site

5. **High Risk Advertising.** High risk ads are those which pose some level of danger or harm to consumers or society, and include gambling, adult services or other scams. Figure 20 shows an example of an online gambling ad displayed on a streaming site, and Figure 21 shows a redacted but highly explicit “adult” site ad, depicting a high level of simulated sexual violence.

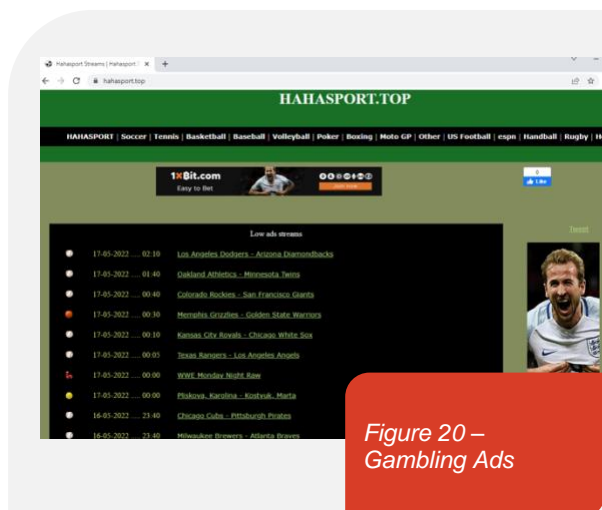


Figure 20 – Gambling Ads

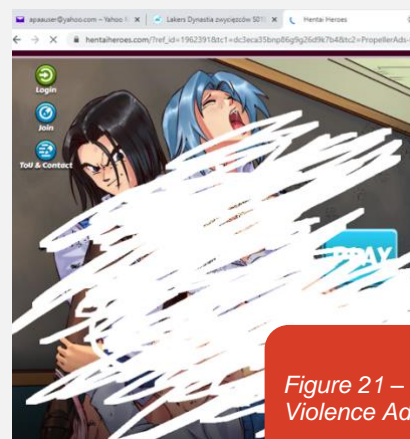


Figure 21 – Sexual Violence Ads

In some cases, malicious ads were identified and blocked by the advertising network, for example, as shown in Figure 22 by DoubleVerify. This shows that consumer protections can be very effectively applied at the point of detection by an ad network.

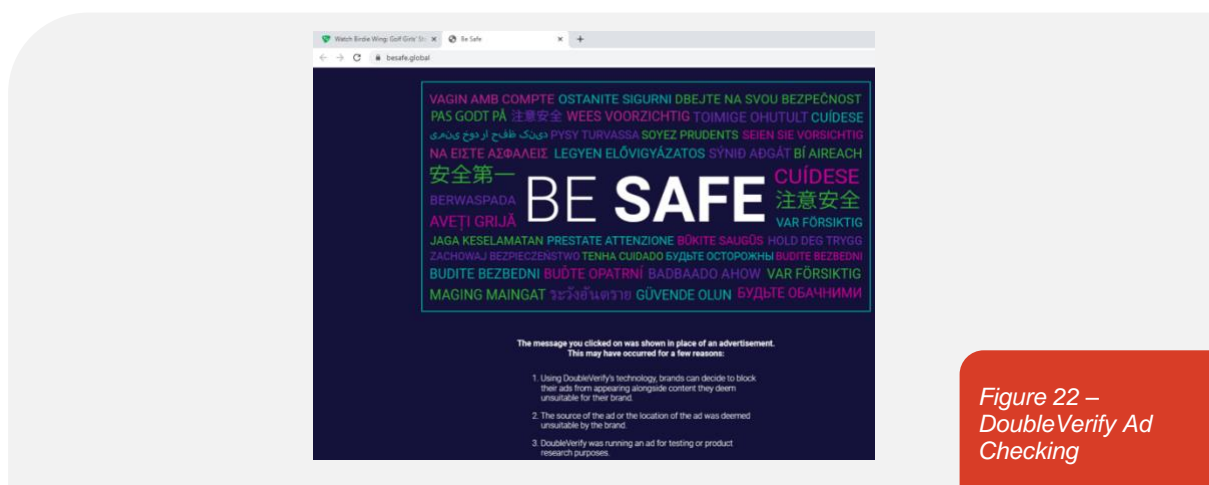


Figure 22 – DoubleVerify Ad Checking

In other cases, as shown in Figure 23, integrity checking built-in to browsers was able to detect sites whose security settings were misconfigured (deliberately or accidentally), and block an ad.

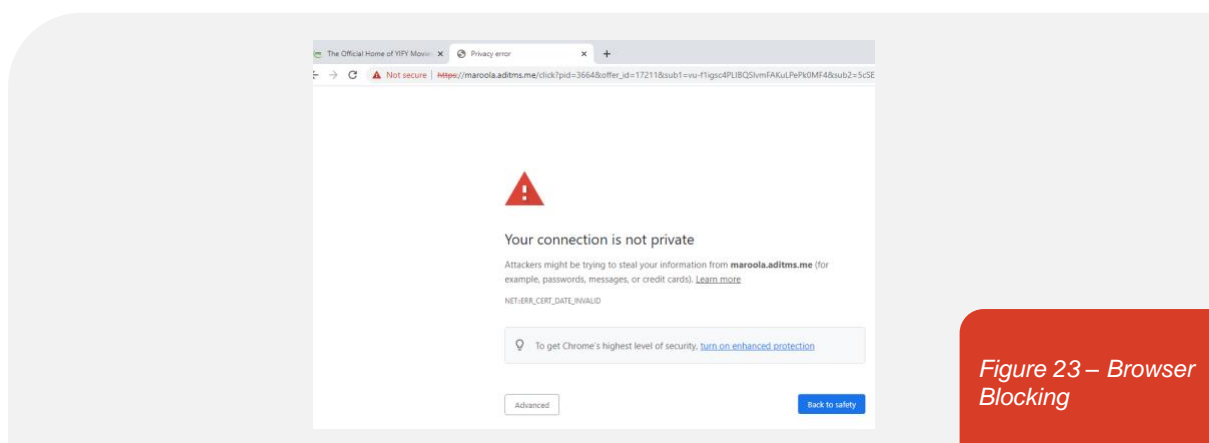


Figure 23 – Browser Blocking



## Mobile Apps

In addition to the infection vectors identified through the PC interface, a number of mobile IPTV apps were also investigated. The following additional risks were observed:

1. **Embedded Malware.** 33 typical IPTV apps were identified for review by AAPA members. A simulated user was created on the device, and user activity was simulated on the device for one hour for each application. The apps were also uploaded to VirusTotal, which is a site that matches malware samples against databases maintained by more than 70 anti-virus companies. 19 individual malware samples were detected, including:
  - 4 x Trustlook - Android.PUA.DebugKey
  - 4 x Android.WIN32.MobiDash.bm<sup>24</sup>
  - 2 x Exploit/WinampPLS<sup>25</sup>
  - 1 x Symantec Mobile Insight - AdLibrary:Generisk
  - 1 x Trojan.Linux.Kaili<sup>26</sup>
  - 1 x PUP/Android.FLPrev.1137587<sup>27</sup>
  - 1 x Android:Evo-gen [Trj]
  - 1 x Android.MobiDash.6945
  - 1 x Adware/AdDisplay!Android<sup>28</sup>
  - 1 x PUA.AndroidOS.Mobidash
  - 1 x PUA:Win32/Pearfoos.B!ml<sup>29</sup>
  - 1 x Android.Adw.StartApp.Gen<sup>30</sup>

In other words, the mean chance of downloading an IPTV app with a malware sample was 57% - more likely than not, with each app installed, users will be infected. To illustrate the severity of the malware identified, and as described by Malwarebytes, MobiDash is used to bombard the user with pop-up ads, and can take up to 3 days before it begins to display ads. When ads are displayed, they can then potentially lead to other malware being installed. The malware also has some stealthy options which make it very difficult to install, such as removing itself from the device administrator's list. This means that even an administrator cannot delete it. Italy and Germany are within the Top 10 countries observed by Kaspersky for this infection, posing a clear, targeted risk for European consumers<sup>31</sup>. It is also worth noting that our Android code samples contained MobiDash for both Windows and Android, indicating the potential the infection to be injected into the local network, and spread to other devices. The risk to corporate networks is high, given, that VPNs are being advertised

<sup>24</sup> <https://blog.malwarebytes.com/detections/android-adware-mobidash/>

<sup>25</sup> [https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-](https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit%3AWin32%2FWinamppls#~:text=This%20exploit%20uses%20a%20vulnerability,can%20get%20on%20your%20PC.)

[description?Name=Exploit%3AWin32%2FWinamppls#~:text=This%20exploit%20uses%20a%20vulnerability,can%20get%20on%20your%20PC.](https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit%3AWin32%2FWinamppls#~:text=This%20exploit%20uses%20a%20vulnerability,can%20get%20on%20your%20PC.)

<sup>26</sup> <https://resources.infosecinstitute.com/topic/kaiji-malware-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/>

<sup>27</sup> <https://blog.malwarebytes.com/detections/android-pup-riskware-autoins-fota/>

<sup>28</sup> <https://www.eset.com/int/about/newsroom/press-releases/research/eset-discovers-android-adware-affecting-millions-and-tracks-down-its-developer-1/>

<sup>29</sup> <https://howtofix.guide/pua-win32-pearfoos-a-ml/>

<sup>30</sup> [https://www.f-secure.com/sw-desc/adware\\_android\\_startapp\\_online.shtml](https://www.f-secure.com/sw-desc/adware_android_startapp_online.shtml)

<sup>31</sup> <https://threats.kaspersky.com/en/threat/Adware.AndroidOS.Mobidash/>

on these apps, allowing users to enter the corporate network behind the firewall, and infecting critical backend corporate systems.

The operating system did provide some level of protection, by either (a) flagging that the apps were potentially malicious, as shown in Figure 24, or (b) preventing installation of malicious files, as shown in Figure 25.

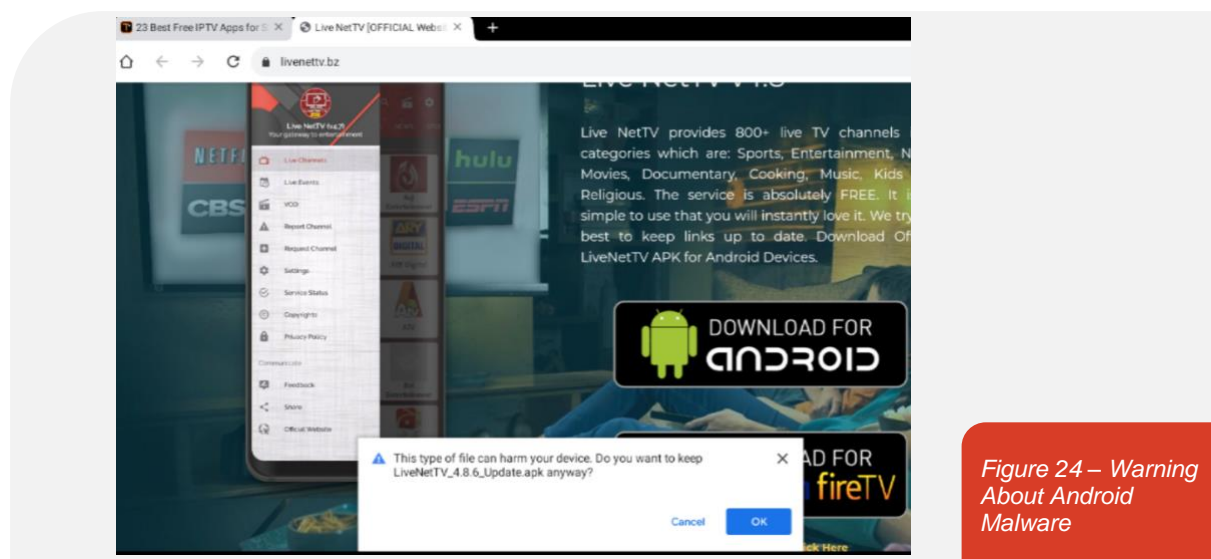


Figure 24 – Warning About Android Malware

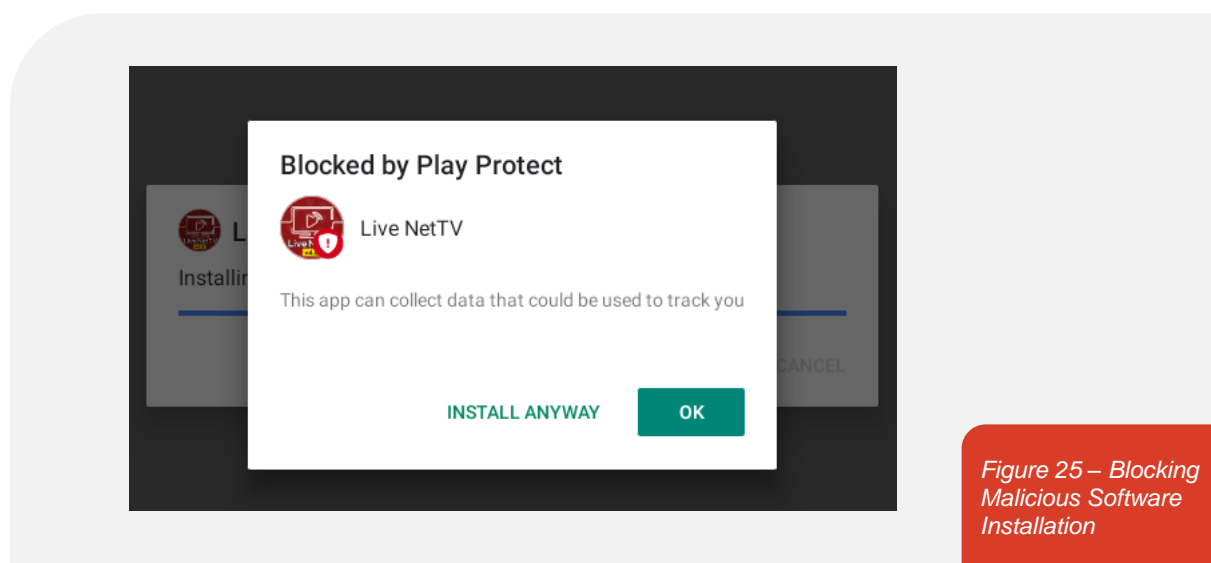


Figure 25 – Blocking Malicious Software Installation

2. **Interstitial and Banner Advertising.** When a user clicks on a stream, instead of being taken directly to the streaming page, an ad is displayed instead. Typically, the ad is displayed for a certain time window before the streaming page is loaded. If the user clicks on the ad, the stream is not displayed. No malicious ads were observed, but the potential attack vector remains. Banner ads were noted on some apps, but they tended to be mainstream, and thematically linked to the content. For example, ads for ESPN were displayed under the “Sports” category for IPTV Loader, as shown in Figure 26.



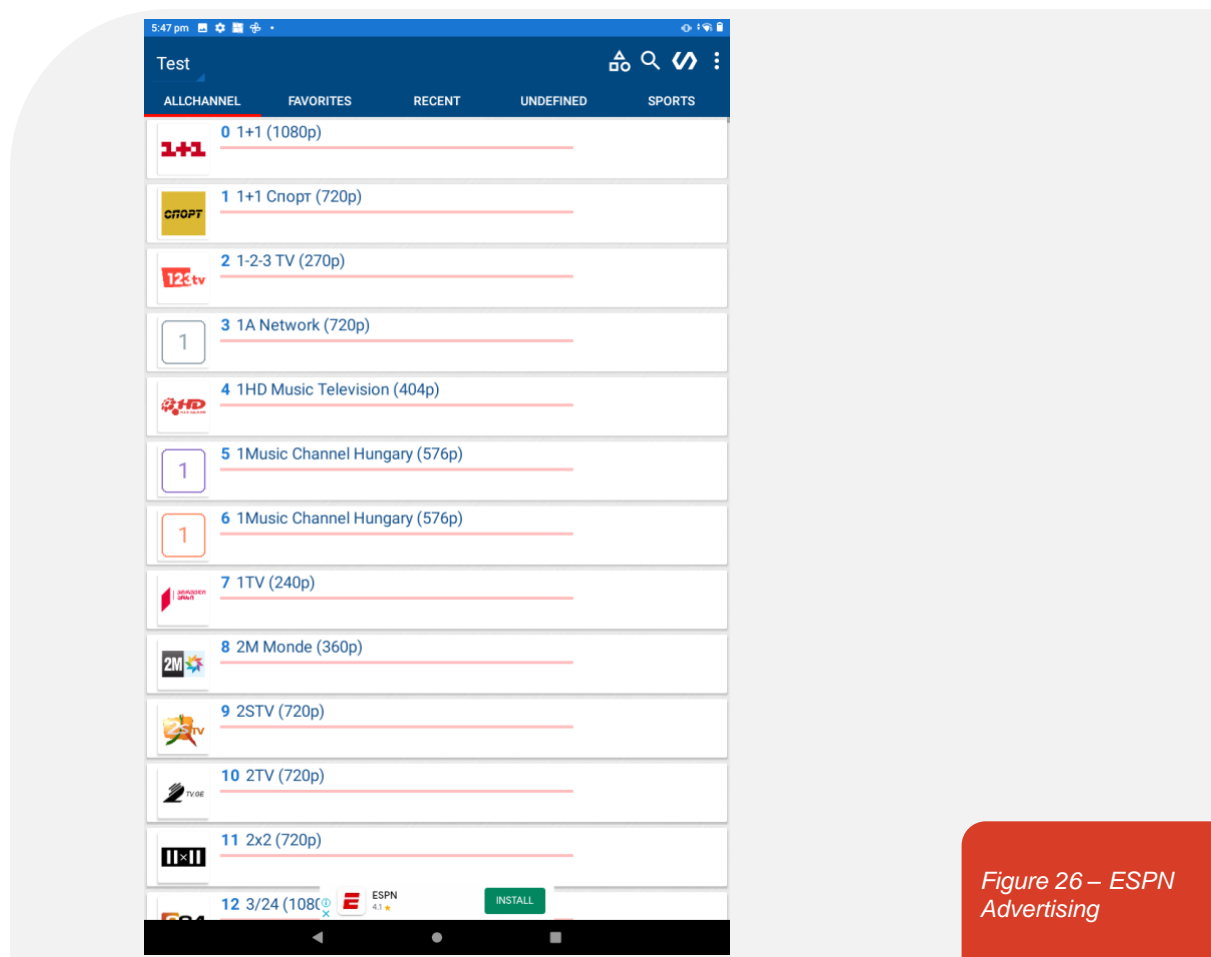


Figure 26 – ESPN Advertising

3. **Hardware Linked Subscriptions.** Not observed on the PC, some apps required registration of the device's hardware (MAC) address to prove that a subscription had been paid, as shown in Figure 27.

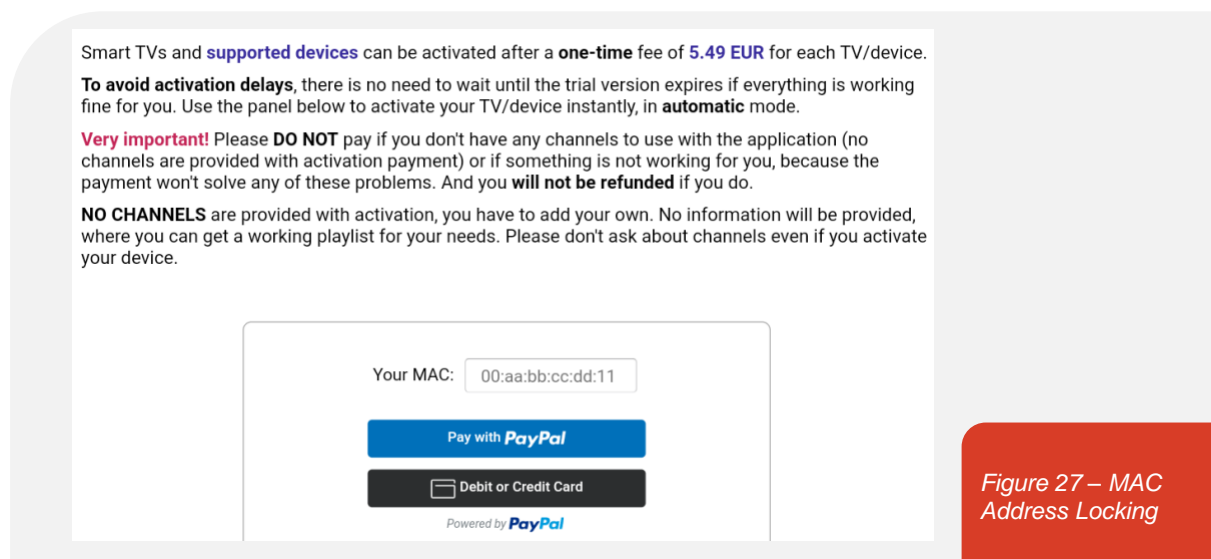
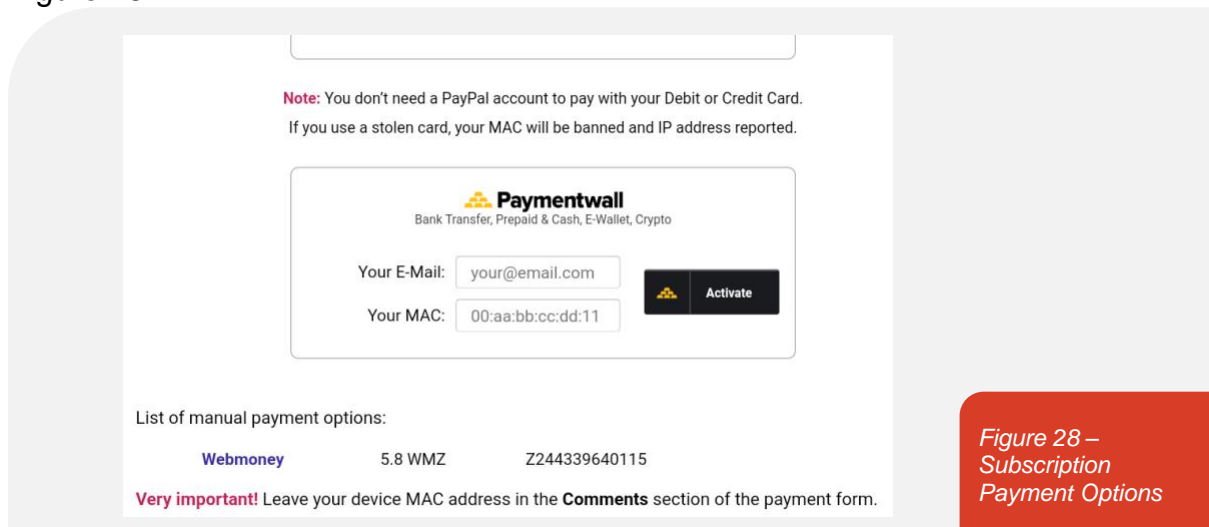


Figure 27 – MAC Address Locking

Note that the payment processor in this case is Paypal, but the app also accepted Webmoney, bank transfer, prepaid & cash, e-wallet and crypto options, as shown in Figure 28.



**Note:** You don't need a PayPal account to pay with your Debit or Credit Card.  
If you use a stolen card, your MAC will be banned and IP address reported.

**Paymentwall**  
Bank Transfer, Prepaid & Cash, E-Wallet, Crypto

Your E-Mail:

Your MAC:

**Activate**

List of manual payment options:

<b>Webmoney</b>	5.8 WMZ	Z244339640115
-----------------	---------	---------------

**Very important!** Leave your device MAC address in the **Comments** section of the payment form.

Figure 28 –  
Subscription  
Payment Options



## STBs

Set Top Boxes (STBs) typically run the Android operating system, so the malware infection vectors and risks from banner and interstitial ads would be the same. However, there have been reports of STBs being targeted by botnets<sup>32</sup> to recruit them to participate in Distributed Denial of Service (DDoS) attacks. This may be because of their limited user interface and use of default superuser user accounts, providing full administrative access, especially where the STB or Smart TV has been “rooted”. There are comprehensive instructions on how to achieve this freely available on the internet<sup>33</sup>. A compromised STB could provide a foothold for malware to then spread laterally within the local area network, following the MITRE ATT&CK framework. No malware or advertising patterns were observed in our STB analysis beyond what was reported for Android devices.



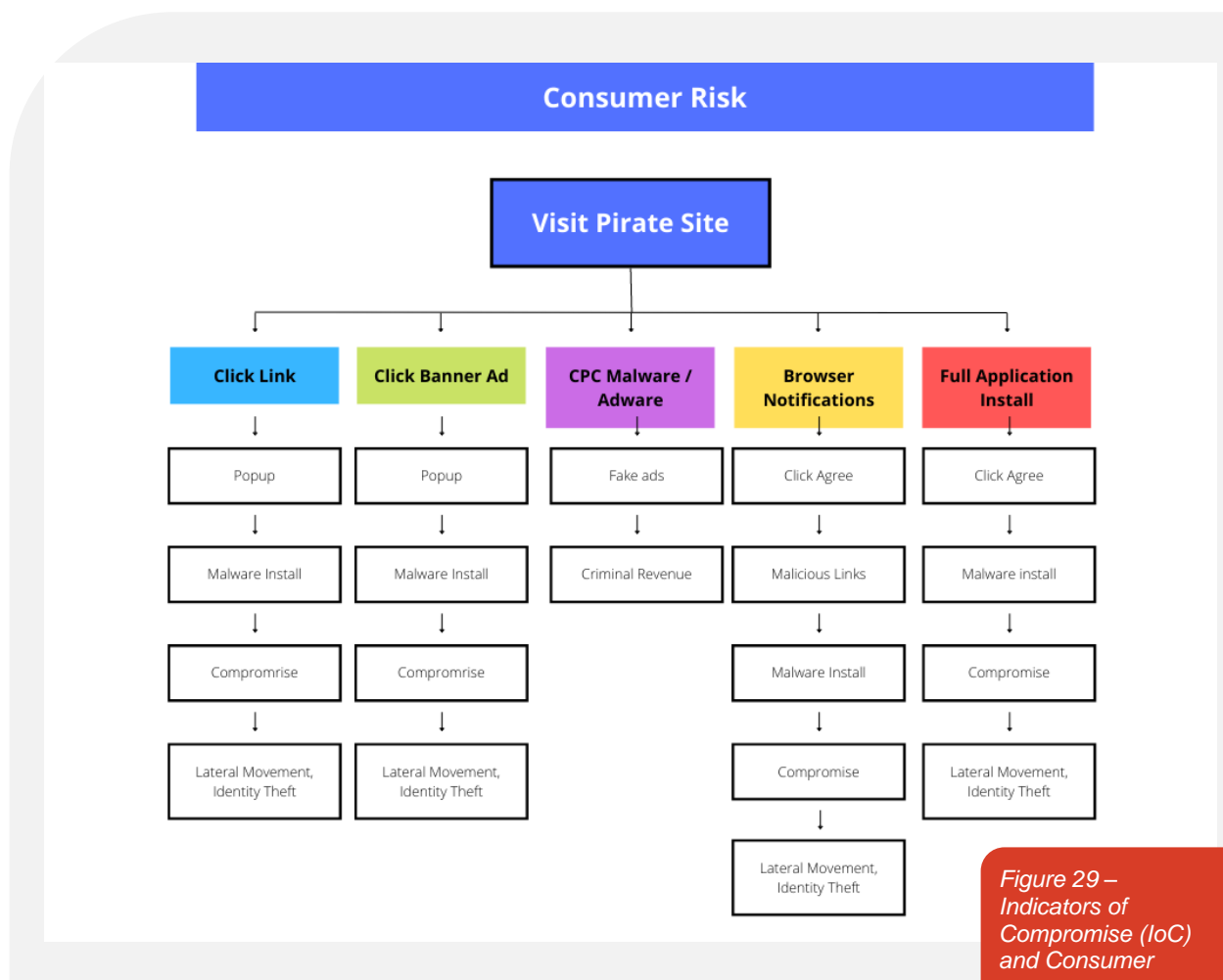
## Indicators of Compromise (IoCs) and Consumer Impact

To summarise the results in terms of consumer risk, and using visiting a piracy or streaming site as an example, Figure 29 summarises some of the consequences of the Indicators of Compromise (IoC) as observed in this study:

<sup>32</sup> <https://calibreone.com.au/are-set-top-boxes-vulnerable-to-cyber-attack/>

<sup>33</sup> <https://joyofandroid.com/how-to-root-android-tv-box/>

- Consumer visits the site, registering with a valid email address (if required)
- Banner ads may be displayed
- Page has active content that reacts to JavaScript events, such as hovering over a link, or clicking in a search bar
- Popups or fake ads are clicked, or notifications permitted, which lead malicious browser extensions or full applications being installed
- Once installed, malware can lead to lateral movement to further compromise a local network behind the firewall, or identify theft and fraud



Clearly there are very significant consequences for consumers (and business) from using piracy or streaming sites, applications or STBs. All of the actual consequences can generate significant amounts of revenue for cybercriminals. Publifit estimate that 1% of all ads served globally are injected with malware, which has the capacity to very directly generate significant criminal revenue.

For consumers, the direct consequences of being compromised using the IoCs observed in this study are primarily identify theft, credential theft, or ransom demands, leading to identity fraud, cyberfraud and extortion. Identity theft simply means that enough of a consumer's personal information is gained through a

compromise that allows their identity to be “taken over”. This then means that ownership of bank accounts can be gained by malicious third parties, resulting in monetary losses, and further facilitated locally by “money mules”, who launder the funds before they can be recovered by law enforcement. Likewise, some of the malware observed in this study can capture keystrokes, or access stored credit card data in a browser, which could be directly used for credit card fraud. Finally, if a consumer is “ransomed”, there may be a very large, direct cost imposed to pay the ransom and recover their data. There can also be secondary impacts of credit card fraud or identity fraud, such as repairing credit records and restoring credit scores, as well as having to take legal action to recover or re-establish identities. With the new European Digital Identity framework<sup>34</sup>, for example, consumers will have trusted digital identities made available through Digital Wallets containing all of their personal data, from national identity to income statements; yet, if these are compromised by malware, recovering identity could take a considerable amount of time and effort. What if the eSignature is used to sign documents on behalf of the compromised user?

The other significant direct impact is to businesses, especially where a consumer connects to a corporate network while viewing an audiovisual piracy site, or using an audiovisual piracy app, either “on premises”, or remotely through a Virtual Private Network (VPN). As seen through the code samples identified in this study, it may be possible for lateral movement within a corporate network to occur, once a consumer device has been compromised. The consequence for business is that corporate, backend systems could be ransomed, costing business potentially many millions of dollars in ransom being paid, or facing the prospect of large parts of the business being unable to operate due to data loss. Or, malware could be installed using this path, in order to monitor all corporate network traffic, and exfiltrate this data to a malicious third party for espionage purposes. In some ways, a ransomware attack is preferable, since it is often limited in scope, demanding a payment which can then either be made, or systems restored. The prospect of deeply embedded malware stealing valuable Intellectual Property (IP) over many years, and transmitting it to competitors, could quite literally bankrupt a business, and this activity could remain undetected over months or years.

## Benchmarking Against Asia

In the *Timeline To Compromise* report published by AVIA, the goal was to show just how quickly consumers could be compromised in a typical session – within 43 seconds. In this study, using European data as shown below, a consumer’s PC is locked within 1m11s of starting their piracy session. During that time, they were presented with two popups – one, a Russian browser promising cash discounts for internet purchases, the other, selling CPC leads for “Game of Thrones” traffic – followed by their screen becoming locked, and providing an actual phone number to call Microsoft to unlock the PC due to the presence of cyber threats. The number was verified as not belonging to Microsoft – in fact, it was a scammer phone number, where the scammers tell the consumer that they need “technical support” during

---

<sup>34</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en)

which a Remote Access Trojan (RAT) is planted on the computer. The timelines were very comparable to the Asia study, potentially highlighting the need for further regulation to protect against cyber attacks, even with the extensive legal and regulatory frameworks in place in Europe, including ENISA, the NIS Directive<sup>35</sup> and the Cybersecurity Act<sup>36</sup>.

## Timeline to Compromise

00:00	Visit Site - using a Windows 10 machine, open web browser and visit audiovisual piracy site	
00:10	Find and click title of pirated film to view or download.	
00:20	Popup loads, redirects to another popup.	
00:32	Russian-based scam website loads in pop-up, requesting user to install plug-in with up to 35% cashback on internet purchases.	
00:42	Select another title to view from the home page.	
00:53	Another pop-up loads, promising cheap leads for advertising networks, for example, Game of Thrones.	
01:03	Return to home page, search for another title.	
01:11	Popup loads, showing a Microsoft Defender screen, scanning PC for viruses. 9 threats are reported. The browser screen is maximised, the user is locked, and a message on the screen instructs the user that their PC has been blocked and that they must call a number to prevent identity theft, and unlock access to the device.	

<sup>35</sup> <https://www.enisa.europa.eu/topics/nis-directive>

<sup>36</sup> <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act#:~:text=The%20EU%20Cybersecurity%20Act%20introduces,recognised%20across%20the%20European%20Union.>



# DISCUSSION

From a sample of known sites, IPTV apps and STBs of concern to AAPA members, we were able to identify and replicate infection patterns across a wide range of functions, and develop a Patterns of Compromise (PoCs) schema that indicates the consequences for consumers from malware (including identify theft and fraud) as well as for businesses (including lateral movement within the network, behind the protections of the firewall). Alongside this functional analysis, we were able to overlay the revenue models which are clearly powered by malware infections for cybercriminals, including CPC ad fraud, subscriptions and “false positive” malware ads.

The goal of this report was to investigate the cyber risks faced by consumers and their workplaces

**by using audiovisual piracy apps, visiting audiovisual piracy websites or using Set-Top Boxes (STBs).**

The presence of malware in a range of IPTV app samples is a concern. These apps are being increasingly used by consumers to access pirated content; yet, what appears to be free on the surface is the potential for malicious activity to infect the local device, but also critical systems behind the corporate firewall, when a VPN is used. In some ways, this is a more critical risk than websites that host malware, since an app is installed and persists on the device, and can be activated at any time by accessing local operating system services. App stores should more carefully screen IPTV apps for the presence of malware, and/or notify users that installing the apps may lead to significantly adverse personal and commercial consequences.

A wide range of organisations – both illicit and legitimate – play a role in facilitating this type of activity, including ad networks, advertisers, cybercriminals, payment processors, domain registrars, VPN providers, hosting services and consumers themselves. From a regulatory perspective, the role of each of these entities needs to be considered within Europe, to understand whether existing laws may be used to further clarify expectations or obligations to protect consumers.

Mainstream ads, for example, being displayed on piracy sites continue to undermine the legitimate economy; yet the complexity of ad purchasing and distribution makes it difficult for advertisers to understand where their ads may be placed. Algorithms displaying “bias” by predicting target demographics and purchasing intentions may be analytically effective but ultimately supporting the criminal economy.

Payment processors should not be accepting payments on behalf of known piracy sites, apps or STB vendors, where the funds are primarily used to support piracy. Likewise, VPN operators should be ensuring that their users are better protected by honouring regulatory site blocking, as well as validating links and checking for malware. Where domain registrars provide privacy protection for organisations involved in cybercrime, their records should be made more freely available to ensure confidence in, and the integrity of, the international domain name system.

Comparing these European results to a similar study in Asia, there did not seem to be any practical difference from the consumer perspective, despite Europe having very strong cyber and privacy frameworks, such as the GDPR, ENISA, the INS Directive and the Cybersecurity Act. These include the development of digital identities which are cryptographically verifiable. Yet the downside of strong identity management is the risk that these digital wallets can be taken over by malware installed from audiovisual piracy sites. It is worrying that malware does not even appear to have been considered in the design of the European Digital Identity Framework<sup>37</sup> - certainly, it is not mentioned in the Impact Assessment Report. Yet the very examples that are described in the Key Principles document<sup>38</sup> - such as opening a bank account, or filing a tax return – are the exact high value fraud business processes that are routinely targeted by organized cybercriminals.

So what should European regulators be doing  
**to really make Europe safer for consumers, relative to other jurisdictions?**

Regulators need to more proactive in supporting Europe-wide tracking and monitoring of websites, apps and associated services – including digital advertising – that form the core of the audiovisual piracy ecosystem that hurts European consumers and businesses. This should include automated, intelligence-led efforts to locate, identify and takedown services involved in audiovisual piracy, including levelling severe civil and/or criminal penalties for non-compliance. Regulatory site blocking should be simplified and expanded. In short, if you are in the business of stealing identities and facilitating fraud, the consequences should be swift and severe, providing a deterrent to others who may plan to engage in similar behaviour.

In a practical sense, the best advice for consumers is simply not to visit illicit streaming or piracy sites, and not to use piracy or apps or STBs for this purpose. Consumers should consider purchasing and installing appropriate anti-virus software, and not visit these sites or use these devices within a corporate network. They may also install ad blocking software, or disable JavaScript, to block a number of PoCs. However, the Android permissions system is quite inflexible, and so some of these protections may be easier to enable on PCs rather than mobile devices<sup>39</sup>. It was observed that some protections worked well, for example, when clicking on some malicious Google search results, Google actually provides an intermediate warning page, that prevents the user from proceeding, until they click a button, acknowledging the risk. Google displays these messages where they have detected that a site contains malware, is deceptive or suspicious, contains harmful programs, or loads scripts from unauthenticated sources<sup>40</sup>. Browser developers and search engines play an important role in protecting the safety and security of their users, and an expansion of these protections would be welcome.

Businesses should consider blocking VPN access from behind the firewall, and/or have content filtering and/or malicious endpoint detection embedded within their network management and security posture. This could also include investing in a Security Operations Centre (SOC) or Security Information and Event Management (SIEM) system to identify malicious activity arising from malware infections, where the attacker's goal is to achieve lateral movement and deeper compromise. Implementing restrictive access control policies, designing segmented networks, and implementing a cyber security program that meets one or more industry standards can reduce the risks of a lateral movement attack. Perhaps

<sup>37</sup> <https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation>

<sup>38</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en)

<sup>39</sup> <https://www.microsoft.com/en-us/research/uploads/prod/2019/05/raval-mobisys19.pdf>

<sup>40</sup> <https://support.google.com/chrome/answer/99020?hl=en&co=GENIE.Platform%3DDesktop>

more importantly, companies should develop education, awareness and training programs to alert their employees to the potential dangers of visiting audiovisual piracy sites, or using audiovisual piracy apps – by reducing the number of users, the revenue earned by site operators will be reduced, thereby reducing the incentive to operate.

---

## ABOUT THE AUTHOR

Professor Paul A. Watters is Honorary Professor in Criminology and Security Studies at Macquarie University, Adjunct Professor of Cybersecurity at La Trobe University, Strategic Cyber Security Consultant at Ionize, and Academic Dean at Academies Australasia Polytechnic (ASX:AKG), and CEO of Cyberstronomy Pty Ltd, a Melbourne-based startup that develops Governance, Risk and Compliance software for small-medium enterprises. 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, IP theft, data mining, and cognate fields, which have been cited more than 5,968 times by his peers. He is consistently in the top 10% of all researchers by paper downloads on the Social Sciences Research Network (SSRN).

Professor Watters published his first research study into piracy in 2006, showing that 99% of file transfers could be blocked across four major P2P file sharing protocols in a highly scalable way by ISPs<sup>41</sup>. Since then, his anti-piracy work has focused on high-risk advertising, the links between organised crime, piracy and child exploitation, malware risks, as well as deterrence and prevention strategies, such as the use of honeypots and chatbots.

---

<sup>41</sup> <https://www.researchonline.mq.edu.au/vital/access/services/Download/mq:2229/DS01>