REPORT

The hidden threats lurking on illegal streaming sites

Foreword

Illegal streaming of sporting events is being marketed to consumers as an alternative to legitimate streaming services, but potential users must understand the risk to which they expose themselves when they choose to watch content illegally.

As this timely report from OpenText Security Solutions makes clear, illegal streams open up a gateway for criminals to access bank accounts, commit fraud, and install malicious software. In addition, the operators and sellers of illegal streams ignore the perils relating to child safety by offering unfiltered access to explicit content.

To protect your personal and financial details, and your family's safety, the secure and safe way to watch content is through legitimate providers.

Kieron Sharp, CEO at FACT

Introduction

With the return of the Premier League and with big showcase events hitting our screens, we wanted to better understand the risks faced by sports fans when venturing onto illegal streaming sites.

So, we examined some of the most common "free-to-view" sites, analysing 50 of the most popular ones during several major sporting events over the past couple of months.

The results were shocking. Practically every site had links to malicious or misleading content of some kind. But what's more alarming is the variety and scope of damage these sites – even ones you may believe to be relatively "safe"– can inflict.

So, we'll dive into some of the common threats so fans can decide whether using illegal streaming websites is really worth the risk.

Top threats on illegal streaming sites

90% of illegal websites were classified as risky

Banking Trojans

Malicious software designed to infiltrate your financial accounts and steal your money

40% of free-to-view sites analysed had no security certificates

Crypto scams

The very opposite of get rich quick – using the buzz around cryptocurrencies to lure people into sophisticated financial ploys

Practically every illegal streaming site featured explicit content

Mature content

Adult material is more prevalent and more extreme than last year

The real threats we saw on illegal streaming sites

Illegal streaming sites are not the same as official streaming platforms. Legitimate content providers rely on either advertising or subscription models to generate their revenue – because content isn't free to make or host. But illegal streaming sites also need to make money, and while there are many questionable adverts across their pages, one of the main ways they generate income is by giving cyber criminals access to you.

Here is a list of all the types of threats and pitfalls we saw on the illegal streaming sites analysed:

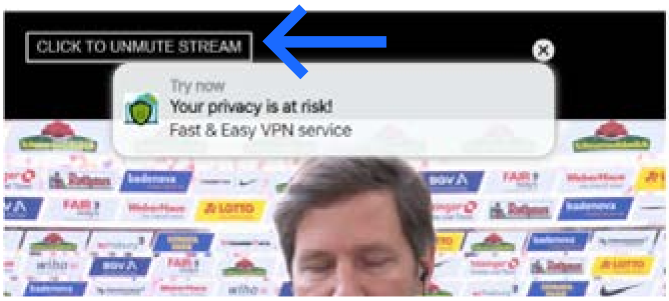
- Malware
- Spyware/Adware
- Phishing
- Explicit content
- Fake Operating System and browser updates
- Fake messages (including sexual lures)
- Junk security software
- Dodgy push notifications in browsers (sexual luring and inappropriate messages)
- Fake "watch video" buttons including fake "enable sound" options
- Fake CAPTCHAs

While you may think the antivirus software on your PC means you don't have to worry about these, many of them are extremely effective at evading those security protections. Some don't even need to infect devices to have devastating consequences.

So, let's explore some of the riskiest threats you're likely to run into on these illegal sites in more detail.

Banking Trojans – designed to access your bank accounts

As you may expect, online financial scams come in many different guises. A banking trojan is a type of malware (a type of malicious software) which attempts to access your bank details or accounts, hidden within a piece of legitimate-looking software. We found banking trojans were prevalent on illegal streaming sites. One illegal streaming site we looked at hid a link to a banking trojan behind a fake "unmute button". Once clicked on, the link automatically initiated the downloading of a trojan onto your PC or smartphone.



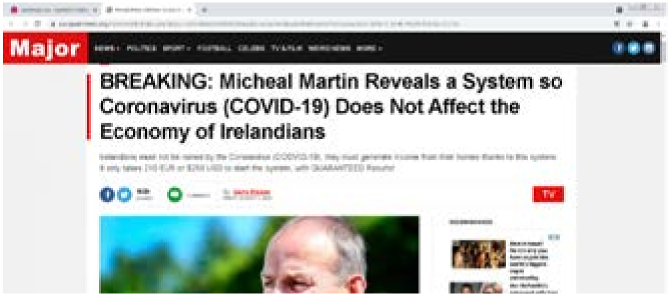
A dodgy "unmute" button in the wild along with a fake "privacy at risk" warning

And while computer antivirus software is designed to catch malware, the speed with which new malware is being created means that if your software isn't up to date, it may not recognise it.

Crypto scams – the very opposite of get rich quick

With the growing popularity of cryptocurrency, many trojans are now being designed to infiltrate any crypto apps you may have on your smartphone. These often use redirects or pop-ups to show users fake, localised stories that feature local politicians or celebrities promising them riches if they simply share their bank details.

Because of the lack of security on illegal streaming sites, scammers can view the IP addresses of those on the webpage and use them to send personalised and incredibly convincing scams, sometimes even imitating popular media publishing sites to sell the lie.


Major

BREAKING: Micheal Martin Reveals a System so Coronavirus (COVID-19) Does Not Affect the Economy of Irelandians

An example of a Bitcoin scam from our 2021 report that had been localised to appeal to people browsing with an Irish IP address

Criminals even take into consideration the current price of bitcoin and other cryptocurrencies and will often switch to scams for other types of investment platforms when crypto prices are low.

Explicit content – viewer advisory; not suitable for children

While there are numerous ways scammers can harm you by targeting your bank account, it's important to remember that this isn't the only type of damage illegal streaming sites can inflict.

We found numerous examples of explicit and harmful content being hosted on these sites. The mature content is often from equally nefarious sources, meaning it can lean towards the very extreme – and it's becoming more prevalent and more extreme each year. And with many parents frequently lending their young children their devices, they could easily be exposed to this.

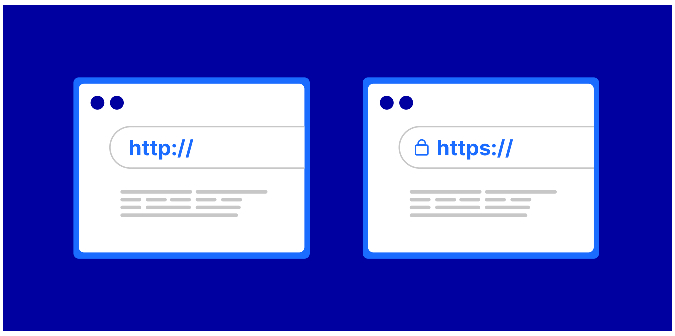
Not all websites are created equally

We've highlighted some of the most damaging content on illegal streaming sites, but there are many more dangers.

Encryption red flags

We found that most of the sites we analysed were running HTTP as opposed to HTTPS. It may be the difference of a single letter, but it's a crucial one as that "S" indicates encryption. Commonly identified by a padlock next to the URL, HTTPS encrypts all your requests and responses making it significantly more secure. Without this encryption, it is very easy for anyone to 'listen-in' on traffic between the user and the site.

So, while an HTTPS site isn't a guarantee that a website is completely safe, its absence is always a red flag – as the lack of certification and security protocols instantly means you're less secure when you're on that website.



Dishonest links and dodgy notifications

If you've ever come across an illegal streaming site, one thing that's hard to miss is the array of cleverly designed buttons and pop-ups vying for your attention and trying to convince you to click on them.

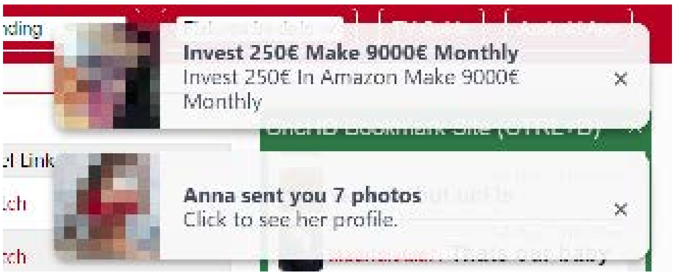
Links are a common feature on many sites, but they're particularly concerning on "free-to-view" ones because pirates don't want to protect you. As a result, they leave the door wide open to cybercriminals experienced in using social engineering and fraud to trick you into clicking on something.

They deploy an array of tricks, such as fake 'X' boxes on video overlays, false notification pop-ups, messages promising spurious offers, or warnings that are designed to scare you into taking dangerous actions.

One tactic we saw frequently used was to mute the sound of a stream and offer to "re-enable" it if you click on a button. However, this link will lead you to download an alternative player with malicious elements.

Browser notifications are often used by legitimate sites to alert users – whether that's a new email or a score update – so we often click on them without thinking. As such, dishonest notification messages are a feature of most illegal streaming sites, relying on muscle memory to cause at least a few people to make that split-second mistake of clicking on them.

Once one of these fake notifications is clicked on, it can open the door to a barrage of malicious links and content that can be hard to untangle.



Invest 250€ Make 9000€ Monthly
Invest 250€ In Amazon Make 9000€ Monthly

Anna sent you 7 photos
Click to see her profile.

Example of aggressive fake notifications we saw on numerous sites

Our advice – if it looks too good to be true, it usually is

All the threats we saw use a variety of tools and tricks, but, ultimately, they're all designed to achieve the same goal – to take something from you. Whether that's your money, your personal details or in some cases, the innocence of your children.

There's a reason cyber criminals use these illegal streaming sites – it's an unregulated jungle and scammers are free to lay whatever traps they want.

Illegal streaming sites are a portal to connect criminals as directly to you (their target) as possible. And even the most tech-savvy fan can fall victim to one of these ploys if they continue to frequent these sites. In fact, you may have already and not know it.

That's why we recommend you never visit these sites. On the surface it may seem worth it, but the hidden costs and risks are high. You should ensure you regularly update your software and operating systems, use up-to-date antivirus and anti-phishing detection, and make sure you verify all links before you click on them.

And if a link promises something that seems too good to be true, it usually is. Our advice is to steer clear.

About Carbonite and Webroot

Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.