WEBROOT®
an opentext™ company

Scams, malware and extreme content found on more than 90 per cent of illegal streaming sites during big weekend of football

- Sophisticated Bitcoin scams, mobile app scams and malware target football fans
- Explicit and extreme pop-ups bombard users
- More than 90% of sites analysed by Webroot exhibited red flags – some very serious

Research from Webroot, a market leader in cyber resilience, has exposed the extent of scams and malware found on illegal streaming sites that were shared on social media channels during a big weekend of football across Europe.

Football fans across Europe trying to watch the Carabao Cup Final or major clashes across the Premier League, La Liga, Serie A and Bundesliga for free are likely to have been exposed to a sophisticated Bitcoin scam targeted at gaining financial details, various different types of malware and mobile app scams.

In fact, 92% per cent of illegal streaming sites analysed by Webroot were found to contain some form of malicious content.

Some of the more unusual activities discovered also included hi-jacking users' web browsers and notifications through the sites. Once users' browsers were hi-jacked cybercriminals were able to influence users' search results and use notifications to bombard them with junk, scams and explicit or extreme content.

Fans using the sites on mobile devices were also at risk from a range of cyber threats, including fake and malicious mobile apps.

Kelvin Murray, Senior Threat Researcher at Webroot: "These illegal streaming sites are a maze of scams, malware and dangerous content. Simply put there's no "safe" way to use them without putting yourself at risk. The level of sophistication and detail behind the Bitcoin scam we found is a hallmark of a well thought-through and well-resourced criminal operation. These sites are purposely built to trap users into clicking on something nasty – whether that's a scam or fake app, or serving up explicit and dangerous content.

"It's a common misconception that you're safe using your mobile, tablet or smart TV on these sites, but that's simply not true. The behaviour we've seen on these sites is a big red flag."

Webroot's recent report "2021 Webroot BrightCloud® Threat Report" found that consumer devices saw twice as many malware infections when compared to business devices.

Five threats to watch

Bitcoin scams

- Targeted and localised bitcoin scams promising riches and asking users for banking details.
- Convincing ads and websites that link directly to fake new sites with local celebrities and politicians.

Mobile apps scams

- Links to fake mobile apps with privacy issues and useless in-app purchases ranging from £2.09 - £114.99
- Apps that push notifications for junk and that scam their users
- Mobile apps can also be installed on PCs and laptop devices and difficult to remove.

Hi-jacked search results

- Hi-jacking browsers allows cybercriminals to switch users' default browser and take over their browser notifications. This means different search results are served up or users can be spammed with junk notifications and explicit content.
- Even if users shut down their laptops the changes will remain.

Fleeceware

- A type of malware mobile application that come with hidden, excessive subscription fees.
- On streaming sites these are often in the form of fake virus "scans" that push users to download antivirus software. The software looks legitimate but provides no protection.

Notification hi-jacking

- Users looking to watch a stream are tricked into allowing notifications which bombards users with explicit and extreme content as well as scams and links to other malicious sites

ends

Methodology

- Machine learning assisted searches identified active domains with dictionary terms relating to illegal streaming and piracy behaviour
- Domains determined to be malicious were flagged and provided in human readable format
- Human statistical analysis was completed on the results with the explicit aim to identify patterns and emerging trends.
- Per standard practice, malicious domain names have been obfuscated.
- Monitoring took place from the 19th April – 25th April.

Data used:

- Domains displaying an extremely high certainty of malicious activity or content.
- Domains containing dictionary terms relating to typical streaming phrases and terminology common in US & UK English language.

Data excluded:

- Domains detected by Webroot BrightCloud Threat Intelligence as benign.

Webroot is an OpenText Company.

###

About OpenText
OpenText, The Information Company™, enables organizations to gain insight through market leading information management solutions, powered by OpenText Cloud Editions. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com

Connect with us:
Twitter | LinkedIn

Contacts:
Amy McRitchie
Harvard PR

WEBROOT®
an opentext™ company
Amy.McRitchie@Harvard.co.uk