Malware, data theft, and scams: Researchers expose risks of free livestreaming websites

15 June 2016

Credit: KU Leuven

Millions of people use free livestreaming websites to watch sports and other live events online, but this comes with a considerable security risk. Researchers from KU Leuven-iMinds and Stony Brook University have found that viewers are often exposed to malware infections, personal data theft, and scams. As much as 50% of the video overlay ads on free livestreaming websites are malicious.

Many users of free livestreaming websites may be aware that the video content on these websites is typically streamed without the content owner's consent. What they often underestimate, however, is the security risk that comes with watching these videos. Users may get their personal devices infected with malware, or they may be the victim of personal data theft and financial scams.

"Until now, free livestreaming services (FLIS) have mostly been analysed from a legal perspective. Our study is the first to quantify the security risk of using these services," explains M. Zubair Rafique (KU Leuven Department of Computer Science / iMinds). "We have assessed the impact of free livestreaming services on users. We also exposed the infrastructure of the FLIS ecosystem."

The researchers built a semi-automated tool that helped them identify more than 23,000 free livestreaming websites, corresponding with over 5,600 domain names (more than 20% of which are in Alexa's top 100,000 websites). They then performed more than 850,000 visits to the identified FLIS domains and analysed more than 1 Terabyte of resulting traffic.

"It's a public secret that the FLIS ecosystem is not averse to using deceptive techniques to make money from the millions of users who use their services to watch live (sport) events," says Nick Nikiforakis (Stony Brook University). "One example is the use of malicious overlay ads, which cover the video player with fake 'close' buttons. When users click these buttons, they risk being exposed to malware."

"The outcome of our research is quite confronting," adds M. Zubair Rafique. "In addition to exposing numerous copyright and trademark infringements, we found that clicking on video overlay ads leads users to malware-hosting webpages in 50% of the cases. Most of these pages are made to look like the actual free livestreaming websites. That's how they try to get users to install malware: users are tricked into believing they need special software to watch the livestream. Google Chrome and Safari are more vulnerable to this approach than other browsers, because attackers tend to target the more popular web browsers. Finally, FLIS services often use scripts that try to detect and defeat popular ad-blocker extensions."

To alert FLIS users to potentially dangerous pages,

the researchers have engineered an accurate and effective classifier. The tool can also help security analysts find and report unknown FLIS pages to curb copyright and trademark infringements. In a later stage, the classifier will be made publicly available for research purposes.

Provided by KU Leuven