BCAP NewsClips

June 16, 2016

Meadville Tribune
Armstrong expands broadband services in area of Richmond, Randolph townships

Christian Science Monitor
Cheaper and more flexible data plans: are MVNOs right for you?

Chicago Tribune
CBS extends its deal to air the Grammy Awards through 2026

Reuters
Internet Ruling Could Hit Verizon and AT&T's Yahoo Pursuit

USA Today
Networks' binge-envy has spotty track record

Online streaming has become an increasingly popular way of enjoying live content from the confines of behind a computer screen, but a new report suggests millions of users risk being infected with malware and viruses by visiting websites ridden with security issues.

In a study touted by its authors as the first of its kind, researchers said Wednesday that roughly half of the advertisements appearing on free live streaming (FLIS) websites are malicious in nature — designed to deliver computer viruses to unsuspecting viewers and scam others for their money and private information.

It's no secret that sports competitions and other high-demand events routinely end up being illegally broadcast live on the web, and previous reports have attempted to make sense of the vast underground enterprise that operates in spite of efforts from internet police the world over. While those reports have largely involved the copyright aspect of those operations and the subsequent financial toll, however, the researchers behind the study — "It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services" — say their analysis is the first to examine in detail the security risks involved with visiting websites where live content is streamed for free.

The researchers used a custom-built tool to identify more than 23,000 free livestreaming websites across 5,600 domain names, including half which ranked within the one million most popular websites in the world. Those sites were then subjected to hundreds of thousands of automated mouse clicks so the researchers could review the resulting web traffic, in turn producing roughly 1 terabytes' worth of data and presenting a unique look at how illegitimate livestreaming services handle requests from individuals looking to avoid costly cable bills and pricey pay-per-view events.

"The outcome of our research is quite confronting," said the study's co-author, M. Zubair Rafique of the Computer Science program at the University of Leuven-KU in Belgium.

"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 percent of the cases," he said in a statement.

By littering free videos with ads, livestreaming websites can make it seem impossible to avoid clicking on a link and landing somewhere else. Indeed, out of the thousands of websites investigated by the report's authors, they determined that the average video player is obfuscated by between five and six ads obscuring more than 80 percent of the player itself.

"We observe that the majority of these ads consist of fake-button images displayed exactly in the center of a player to trick users into clicking. As such, this trickery directly benefits the FLIS services which earn ad commissions from unintended clicks on the ads," the researchers noted.

In addition to allowing livestreaming sites to earn revenue, however, those ads are often malicious, and may attempt to install malware on the machines of whomever had the misfortune of inadvertently pointing-and-clicking at the wrong place. Those ads directed to malicious websites roughly half of the time, and as a result the researchers allowed themselves to download 12,683 malicious payloads composed of 1,353 different district viruses targeting various web browsers and operating systems, both desktop and mobile, the researchers said.

“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,” Mr. Rafique said.

Among the malware discovered in one instance was a malicious payload that had not previous been identified by a respected anti-virus firm, the report noted. On other occasions, ads directed to malicious websites where hackers published demands for payment and personal information by posing as law enforcement responding to crimes such as copyright infringement.

Around 1 million minutes of digital video transverses the internet every second, the researchers noted. Amid this immense traffic load, however, the report suggests that an equally impressive number of livestream viewers are “exposed to deceptive, unavoidable and malicious ads” as a result.

“Given the ever-increasing incidents of copyright violations and discovered abuse, both against users as well as legitimate content providers, it is clear that current FLIS services are a rather parasitic part of the web. As such, automatic detection techniques are necessary to identify the aggregator webpages serving viewers with an index of free streams, most of which at are commonly reported as illegal,” the report noted.

Nick Nikiforakis, a computer scientist at Stony Brook University in New York, co-wrote the report with Mr. Rafique and three of his colleagues from KU Leuven. Together, the team unveiled a tool in tandem with the release of their report this week intended to help flag potentially dangerous webpages - ***Washington Times***

BCAP
Broadband
Cable Association
of Pennsylvania

127 State Street, Harrisburg, PA 17101
717.214.2000 • bcapa.com

First in Broadband.
The Future of Broadband.®