

MICROSOFT DEALING WITH FRAUDULENT CLICKS ON ADVERTISEMENTS



Microsoft has made the initiative to work alongside of malware researchers in attempts to stop click fraud of online advertisements. The Microsoft Malware Protection Center has recently joined a partnership with Microsoft's Online Forensics team due to the fact that a large portion of malware is involved with some sort of click-fraud. There are several different types of malicious software that are currently supporting themselves through click-fraud, according to Infosecurity-Magazine. Click-fraud basically takes advantage of online advertising and the way that it functions. There are some marketers who are paying publishers for the advertisements based on individual clicks for each advertisement. This means that the marketers only have to pay when the customers end up clicking on an advertisement. The purpose of this is to help brands make changes to their campaigns, ultimately tailoring them to fit the wants and needs of the consumers. Brands are constantly looking for ways to improve their results with consumers. The difference between online advertising and television advertising is the fact that brands have the opportunity to ensure that the people who see their advertisements are people who are actually interested. With click-fraud, people are intentionally clicking on the advertisements as a means of generating revenue, even though the click is not coming from someone who would potentially buy the product or have an interest in it at all. As an example, an individual may create and develop their own website, sell advertisement links, and then click on those links just to generate revenue. The advertisers pay the website owner with the belief that actual customer are clicking on the advertisement, when in reality, they are being scammed because the website owner is clicking on those advertisements as a way to increase their earnings. An MMPC Software Developer, Nikola Livic, has said, "This [team-up] is an important link to target in any comprehensive disruption plan." Livic also said, "We are intersecting large data sets between malware telemetry and ad-clicks to detect anomalous behavior correlated to malware. And we are taking two relatively disparate domains of expertise and tools, namely malware and online advertising, and creating prevention systems and processes for identifying the entire chain of benefactors of click-fraud malware." Livic also made a point, stating that it is difficult for this type of fraud to be prevented and detected, which is a major part of the problem and the primary reason that this partnership has been created in the first place. Livic has said, "The complexity and opaqueness of where traffic comes from, and who benefits from a single click, is a new digital Wild West, fertile for unscrupulous cyber-slingers."