You could be unknowingly loading malicious content from 'trusted' sites

May 27 2019, by Chris Chelvan

Credit: CC0 Public Domain

New research from CSIRO's Data61, the data and digital specialist arm of Australia's national science agency, questions the "trustability" of websites and in a world first quantifies the extent to which the trust

model of today's World Wide Web is fundamentally broken.

Researchers found that around half of the Internet's most popular websites are at risk of malicious activity because they depend on a chain of other third parties to import external resources—such as ad providers, tracking and analytics services and content distribution networks—which are often required to properly load content.

These third parties can further load resources from other domains creating a dependency chain of up to over 30 domains, underpinned by a form of implicit trust with the original website. The research found that the larger the dependency chain, the greater the threat to malicious activity.

Professor Dali Kaafar, Information Security and Privacy research leader at CSIRO's Data61 and Scientific Director of Optus Macquarie University Cyber Security Hub, said that although this is a well-known web design decision, often overlooked are its implications on security and privacy.

"Almost all websites today are heavily embedded with tracking components. For every website you visit, you could be unknowingly loading content from potentially malicious parties and leaving a trail of your internet activity," Professor Kaafar said.

The research also found that 1.2 percent of third parties linked to the top 200 thousand websites were suspicious. Popular web resource Javascript, generally used to improve the user experience of the web, represents the greatest risk of malicious activity as they are designed to be executed undetected.

"The potential threat should not be underestimated, as suspicious content loaded on browsers can open the way to further exploits including

Distributed Denial of Service attacks which disrupt traffic to websites, and ransomware campaigns which cost the world more than US$8 billion in 2018," Professor Kaafar said.

"Worryingly, the original or 'first party' websites have little to no visibility of where these resources originate. This points to a lack of 'trustability' of content on the web, and the need to better regulate the web by introducing standardised security measures and the notion of explicit trust."

Resolving the security issue created by dependency chains will require additional research, the support of the World Wide Web Consortium, the predominant organisation focused on developing web standards, as well as web 'hypergiants.'"

In the meantime, Professor Kaafar suggests installing simple web browser extensions such as ad- and JavaScript-blockers to limit exposure to malicious activity through the web.

More information: Muhammad Ikram et al. The Chain of Implicit Trust: An Analysis of the Web Third-party Resources Loading. arXiv:1901.07699v2 [cs.CR] 18 Feb 2019. arxiv.org/pdf/1901.07699.pdf

Provided by CSIRO