Browser tool aims to help researchers ID malicious websites, code

22 October 2019, by Matt Shipman

Credit: NC State

Researchers from North Carolina State University have developed an open-source tool that allows users to track and record the behavior of JavaScript programs without alerting the websites that run those programs. The tool, called VisibleV8, runs in the Chrome browser and is designed to detect malicious programs that are capable of evading existing malware detection systems.

"When you go to most websites, your browser starts running the site's JavaScript programs pretty much immediately—and you have little or no idea of what that JavaScript is doing," says Alexandros Kapravelos, co-author of a paper on VisibleV8 and an assistant professor of computer science at NC State. "Previous state-of-the-art malware detection systems rely on making changes to JavaScript code in order to see how the code is being executed. But this approach is easily detected, allowing malware programs to alter their behavior in order to avoid being identified as malicious.

"VisibleV8 runs in the browser itself, recording how JavaScript is executed; it doesn't interact with the code and, as a result, is far more difficult to detect."

VisibleV8 saves all of the data on how a site is using JavaScript, creating a "behavior profile" for the site. That profile, and all of the supporting data, can then be used by researchers to identify both malicious websites and the various ways that JavaScript is used to compromise web browsers and user information.

Because VisibleV8 consists of only 600 lines of code, out of the millions of lines of code in Chrome, the software tool is relatively easy to keep up-to-date. This is an important consideration given that Chrome's code is updated approximately every six weeks. VisibleV8 can also be used to target the most likely malicious behaviors without hurting browser performance.

"We've created a stealthy tool for monitoring JavaScript in the wild," Kapravelos says. "We're now making it open source, in hopes that it will be useful to anyone doing research on web privacy and security."

The paper, "VisibleV8: In-browser Monitoring of JavaScript in the Wild," is being presented at the ACM Internet Measurement Conference 2019, being held Oct. 21-23 in Amsterdam, Netherlands. First author of the paper is Jordan Jueckstock, a Ph.D. student at NC State.

More information: VisibleV8 can be downloaded from Kapravelos' site at http://kapravelos.com/projects/vv8.

Provided by North Carolina State University