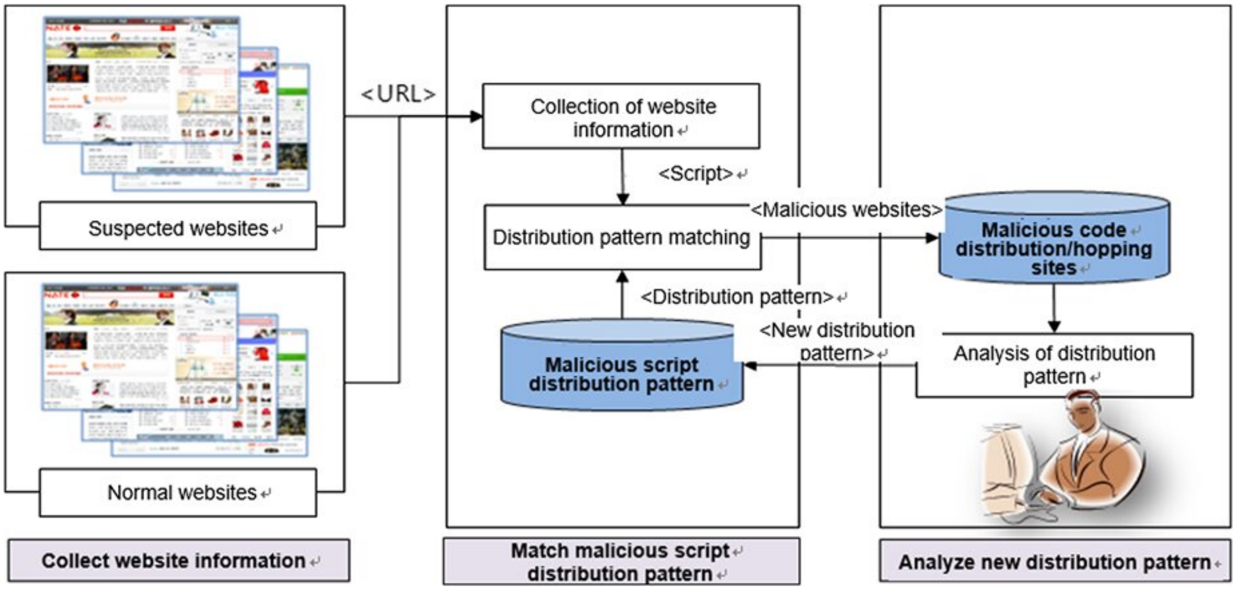
TechXplore

Safer web surfing with a new method for detecting malicious modes

July 13 2022


<URL>
Collection of website information
<Script>
Distribution pattern matching
<Malicious websites>
Malicious code distribution/hopping sites
<Distribution pattern>
<New distribution pattern>
Malicious script distribution pattern
Analysis of distribution pattern
Suspected websites
Normal websites
Collect website information
Match malicious script distribution pattern
Analyze new distribution pattern

Proposed detection system based on analyzing the distribution patterns of malicious code in websites. Zero-day attacks can be reliably detected by continuously updating the list of features of distribution patterns. Credit: Yong-joon Lee et al, *Journal of Electronic Imaging* (2022). DOI: 10.1117/1.JEI.31.3.033046

With the ever-increasing importance of the Internet in our lives, there are growing attempts to exploit software vulnerabilities in our PCs for personal benefit. One way to do so is by infecting the victim's PC with a malicious code injected through a website. In fact, it is common to come across websites that have been hacked and repurposed to distribute viruses or redirect visiting users to other webpages containing malicious codes.

Fortunately, modern web browsers implement security measures to detect hidden malicious codes in websites before they are run. These methods can be categorized as "signature-based detection" and "behavior-based detection." Signature-based methods detect threats by referring to a previously built list of "indicators of compromise" and checking whether a webpage displays any of those indicators. Though this approach offers good speed, it cannot detect new, unknown attacks, also called "zero-day attacks." On the other hand, behavior-based methods compare the state of an unprotected virtual machine before and after visiting a website to detect any suspicious changes that may have occurred. While this approach is slower, it can detect zero-day attacks much more effectively.

In a recent study published in the *Journal of Electronic Imaging*, researchers Yong-joon Lee of Far East University and Won-shik Na of Namseoul University, both in the Republic of Korea, have reported a novel approach to detecting hidden malicious codes in websites. Unlike the existing techniques, their method revolves around identifying and analyzing common attack patterns used during the distribution of malicious code in websites.

In their work, the researchers first gathered data necessary to find attack patterns by "crawling" through 500 harmful websites. They analyzed the approaches that were most commonly used in these websites for distributing malicious codes. They then focused on the programming techniques and scripts used in these malicious codes, such as running shell scripts, executable files (.exe), or performing suspicious manipulation of strings, to exploit vulnerabilities.

The researchers counted the number of times each of these techniques was used in malicious websites and developed an equation to determine the "risk score" for a given website. To do this, they quantified the reliability of each of these techniques as an indicator of suspicion by focusing on their false-positive detection rates, i.e., how often a benign website using these techniques was flagged (incorrectly) as "malicious."

With this information, the developed equation could identify the so-called distribution patterns that hackers use to spread malicious code. "Whereas previous detection methods focus on the actual execution of malicious code, our proposed detection method can identify malicious distribution patterns by analyzing user-side scripts while considering the characteristics of websites," Na said.

Based on the 500 harmful websites previously identified by Google and Microsoft, the researchers could establish the relative importance (and weight) of each individual aspect of malicious distribution patterns. The performance of their approach was outstanding, both in terms of accuracy and speed. "The proposed method can effectively detect malicious websites based on script patterns. The algorithm complexity and its load on memory are, therefore, low," Na said. Furthermore, the new approach could also successfully detect zero-day attacks.

The researchers expect that the novel method would help reinforce web user safety while contributing to cybersecurity science and education by gathering information on malicious code distribution patterns. Let us hope their approach makes its way to the field.

More information: Yong-joon Lee et al, Malicious script distribution pattern detection technique for image search websites, *Journal of Electronic Imaging* (2022). DOI: 10.1117/1.JEI.31.3.033046

Provided by SPIE

Citation: Safer web surfing with a new method for detecting malicious modes (2022, July 13) retrieved 9 April 2024 from https://techxplore.com/news/2022-07-safer-web-surfing-method-malicious.html