Fuzzy logic helps detect redirection spam

June 16 2016

Web browsers might soon use fuzzy logic to spot redirection spam and save users from being scammed, phished or opening malicious sites unwittingly, according to researchers in India writing in the *International Journal of Electronic Security and Digital Forensics*.

Redirection spam occurs when a user opens a link in an email that leads to an unexpected and often malicious page, or when they open a page that has been hacked or injected with malware, which then redirects to a malicious page. Often the redirection occurs instantaneously and transparently without the user being aware until it is too late and login details or credit card number have been divulged to the criminal third party. Frequently, there will be a malware payload that infects the user's computer at the same time.

According to Kanchan Hans of Amity University, in Noida, India, and colleagues, legitimate web page redirections are a ubiquitous part of the web used for server load balancing, link logging and URL rewriting and shortening. Detection of illicit redirections is a difficult task as blocking them would block legitimate redirections too. Nevertheless, while redirection spam was originally little more than a "switch and bait" black hat search engine optimization (SEO) technique, today it interferes with the performance of search engines, leads to wastage of network bandwidth and disrupts user trust, as well as leading to fraudulent activity, identity theft and the spread of malware.

Most modern web browsers have security tools in place that will alert the user to the presence of malware on a site they attempt to visit.

Unfortunately, this relies on the developers of the browser having access to a continuously updated database of flagged sites. If a site has not yet been flagged as malicious, the unwary user may stumble on to a page and be the victim of a wide range of scams and problems. Hans and colleagues have developed a system that could be used in conjunction with such conventional alert systems and provide an extra layer of security against redirection spam.

The team's detection system analyses the characteristics of a given web address based on known spammy links and applies fuzzy logic to add a layer of probability to whether or not the suspicious link is likely to be a problem. Various different criteria are applied in terms of whether the link to be followed might be spam including the number of redirection hops that would take place after the user clicks or enters an address, the presence of a refresh delay, whether or not there are JavaScript redirects on the page, whether there is a meta tag redirection in place. All such characteristics are exploited by spammers to mask the true destination of a link from anti-malware and other security tools used by browsers and the search engines and so avoid the true destination site being detected and flagged as malware.

The application of fuzzy logic allows a probability to be calculated with looser rules based on the different criteria, so that a confidence level can be assigned to a given link as to whether it is safe or spam. In an actual browser implementation this might give users a red, amber or green signal to let them know whether they should proceed to visit a site. In practice, only red and amber sites would generate an alert, sites given the green light could be set to open and so reduce the need for users to make a decision when a site is almost certainly safe to visit, but give them a chance to think twice before visit a putatively hazardous page. Tests on the system show a high level of accuracy in flagging safe and spam sites from a known database without significant false positives or negatives, the team reports.

More information: Hans, K., Ahuja, L. and Muttoo, S.K. (2016) 'A fuzzy logic approach for detecting redirection spam', *Int. J. Electronic Security and Digital Forensics*, Vol. 8, No. 3, pp.191-204.