NYU, Google researchers hack business model of adware, scareware, other unwanted software

August 4 2016

A team of researchers from Google and the New York University Tandon School of Engineering next week will offer the first public view into shady practices that deliver unwanted advertising and software bundled with legitimate downloads - a problem that occurs far more often than malware attempts. Their research suggests that some of the affiliates that distribute such software may be complicit in the scheme, which provides layers of deniability that they are installing unwanted software.

Few computer users have been spared the nuisance of unwanted software: Following what appears to be a legitimate software update or download, a barrage of advertisements overruns the screen, or a flashing pop-up warns of the presence of malware, demanding the purchase of what is often fraudulent antivirus software. On other occasions, the system's default browser is hijacked, redirecting to ad-laden pages.

Despite the prevalence of such unwanted software—Google tracks more than 60 million attempted installs per week, three times the number of malware attempts—the source of these installs and the business model underlying the practice were not well understood. The researchers from Google and New York University Tandon School of Engineering conducted the first analysis of the link between commercial pay-per-install (PPI) practices and the distribution of unwanted software.

Kurt Thomas, a research scientist at Google, and Damon McCoy, an assistant professor of computer science and engineering at NYU Tandon, led a team of researchers from Safe Browsing and Chrome Security to investigate commercial PPI schemes as a main vehicle for moving unwanted software from developers to unwitting installers. Their paper, Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software, will be presented at the USENIX Security Symposium, a top computer security conference, in Austin, Texas, next week.

Commercial PPI is a monetization scheme wherein third-party applications—often consisting of unwanted software such as adware, scareware, and browser hijacking programs—are bundled with legitimate applications in exchange for payment to the legitimate software company. When users install the package, they get the desired piece of software as well as a stream of unwanted programs riding stowaway. Thomas, McCoy, and their colleagues cite reports indicating that commercial PPI is a highly lucrative global business, with one outfit reporting $460 million in revenue in 2014 alone. It should be noted that this revenue reflects a mix of both legitimate as well as unwanted software downloads.

"If you've ever downloaded a screen saver or other similar feature for your laptop, you've seen a 'terms and conditions' page pop up where you consent to the installation," McCoy explained. "Buried in the text that nobody reads is information about the bundle of unwanted software programs in the package you're about to download." The presence of a consent form allows businesses to operate legally, but McCoy classifies the extra applications as "treading a fine line between malware and unwanted software."

The report explains that PPI businesses operate through a network of affiliates— brokers who forge the deals that bundle advertisements

(often unwanted software) with popular software applications, then place download offers on well-trafficked sites where they're likely to be clicked on. Parties are paid separately—meaning some legitimate developers do not know their products are being bundled with unwanted software—and they are paid as much as two dollars per install.

To better understand the install process, the researchers gained access to four PPI affiliates by routinely downloading the software packages and analyzing the components. Among their more important discoveries was the degree to which such downloaders are personalized to maximize the chances that their payload will be delivered.

When an installer runs, the user's computer is "fingerprinted" to determine which adware is available to run on that particular machine. Additionally, the downloader searches for antivirus protection, factoring in the presence or absence of such protections in its approach. "They do their best to bypass antivirus, so the program will intentionally inject those elements—whether it's adware or scareware—that are likeliest to evade whichever antivirus program is running," McCoy said.

Google has long tracked web pages known to harbor unwanted software offers and continuously updates the Safe Browsing protection in its Chrome browser to warn users when they visit such pages. Yet research shows that PPI affiliates are also adjusting their tactics in an attempt to dodge Safe Browsing detection.

The researchers emphasize that these actions imply that PPI affiliates are directly catering to the unwanted software market, avoiding user protections while intentionally delivering unwanted software under a "thin veil of consent," as McCoy deems it. "We're hoping to expose these business practices so people are less likely to get duped into flooding their computers with programs they never wanted," he said.

Provided by New York University