Shlayer macOS malware unleashes ads, involves fake Flash traps

January 28 2020, by Nancy Cohen

Credit: CC0 Public Domain

The macOS traditionally has been considered to be a relatively secure bet and Apple users are the first to say that in the presence of their Windows-owning companions.

Well, Shlayer is out to prove that even owners of Apple machines can be duped into clicking into malware.

Apple can join the Windows club, however reluctantly it wants to do so, when it comes to the nasty topic of computer mischief-makers injecting malware. "Many people think that malware only targets Windows and that Macs are safe," said *BleepingComputer*. Well, you know where that discussion may be going. South.

A new report from cybersecurity company Kaspersky said that the Shlayer Trojan attacked Apple computers, and Tara Seals said in *Threatpost* that the malware used thousands of partner websites to spread code.

Ad circus anyone?

Seals said, "Shlayer is a trojan downloader, which spreads via fake applications that hide its malicious code...Its main purpose is to fetch and install various adware variants. "These second-stage samples bombard users with ads, and also intercept browser searches in order to modify the search results to promote yet more ads."

Wired said, "the attacker can both intercept your search queries and seed the results with their own ads. It's an annoyance, more than anything."

In 2019, one in ten of their Mac security solutions encountered the malware at least once, and it accounted for almost 30 percent of all detections for this OS, according to Kaspersky.

"Having studied the Shlayer family, we can conclude that the macOS platform is a good source of revenue for cybercriminals. The Trojan links even reside on legitimate resources—attackers are adept in the art of social engineering, and it is hard to predict how sophisticated the next

deception technique will be."

Lawrence Abrams in *BleepingComputer* described how Shlayer does its business—a turn from the usual phishing attacks you hear about, by focusing on trending events or popular shows and then building fake web sites surrounding them. The scene is you, the computer user, visiting a fake site via search, YouTube video link, or Wikipedia article link. You are shown a reminder that you need to update your Flash player.

"These Flash Player updates, though, are the Shlayer Trojan," said Abrams, "and when executed will install a malware cocktail onto the computer." (The malware tricks users into thinking it's an update for the Flash software necessary to play videos.)

As Kaspersky's blog post on the matter pointed out, "Distribution is a vital part of any malware's life cycle, and Shlayer and the creators of Shlayer have taken this issue to heart. Looking for the latest episode of your favorite TV show? Want to watch a live broadcast of a soccer match?" A run-in with Shlayer was a possibility.

The team's comment that the attackers were "adept in the art of social engineering" is interesting.

TechRadar said, "Since Shlayer was first detected, its infection algorithm has hardly changed despite the fact that its activity has barely decreased."

Kaspersky said the majority of Shlayer attacks were against users in the U.S. (31 percent), followed by Germany, France and the UK, in that order. They said it was difficult to predict how sophisticated the next deception technique will be

Abrams offered two common-sense bits of advice for Apple users :(1)

Install reliable antivirus software and (2) When browsing the web, say goodbye to any site telling you to first install an update to watch your video or start an activity.

Kaspersky turned the advice-giving up a notch by saying not only install programs and updates only from trusted sources but find out "more information about the entertainment website you are planning to visit: scan its reputation on the internet and try to find feedback on it."

Anton Ivanov, Mikhail Kuzin and Ilya Mogilin, who wrote "Shlayer Trojan attacks one in ten macOS users," regarded the Shlayer Trojan as a common threat on the macOS platform and it's not like they discovered this just recently.

"The first specimens of this family fell into our hands back in February 2018, and we have since collected almost 32,000 different malicious samples of the Trojan and identified 143 C&C server domains."

They saw that the user was prompted to run an installation file which was a Python script, "already atypical of macOS installation software."

Kaspersky said its specialty is in the "installation of adware."

In a Kaspersky post, dated Jan. 23, the 'economics' of the perpetrators was clearly presented.

"Shlayer is offered as a way to monetize websites in a number of file partner programs, with relatively high payment for each malware installation made by American users, prompting over 1,000 'partner sites' to distribute Shlayer. This scheme works as follows: a user looks for a TV series episode or a football match, and advertising landing pages redirect them to fake Flash Player update pages. From here the victim would download the malware. For each such installation, the partner who

distributed links to the malware receives a pay-per-install payment."

Anton Ivanov, Kaspersky security analyst, said the macOS platform was a good source of revenue for cybercriminals, eyeballing new ways to deceive users and using social engineering techniques to spread the malware, but at least the most widespread threats going after macOS "revolve around feeding illicit advertising rather than something more dangerous, such as stealing financial data."

But wait. Could it be that soon events could make this less of a worry and more of a dead issue? Isn't Flash to go off in the sunset this year?

Why would any fake Flash update have a chance? As Lucian Armasu reminded readers in Tom's Hardware, "The next version of Safari will end support for the real Flash player for good, as will all the other major browsers, including Chrome and Firefox. This sort of social engineering shouldn't work once people are aware that Flash can no longer work with their browser."

However, and Armasu struck a strong however, users could still be tricked by the malware for years, "as not everyone stays abreast of the latest news in the Flash world."