# Shlayer, No. 1 Threat for Mac, Targets YouTube, Wikipedia

By Tara Seals

Published: 2020-01-23 · Archived: 2026-04-05 22:28:29 UTC

The malware uses thousands of partner websites to spread malvertising code.

The malvertising-focused trojan known as Shlayer has burbled to the top of the malware heap when it comes to targeting Mac users. It made up 29 percent of all attacks on macOS devices in Kaspersky's telemetry for 2019, making it the No. 1 Mac malware threat for the year. To spread, it has been swindling visitors to websites with millions of visitors, especially YouTube and Wikipedia, into clicking on malicious links.

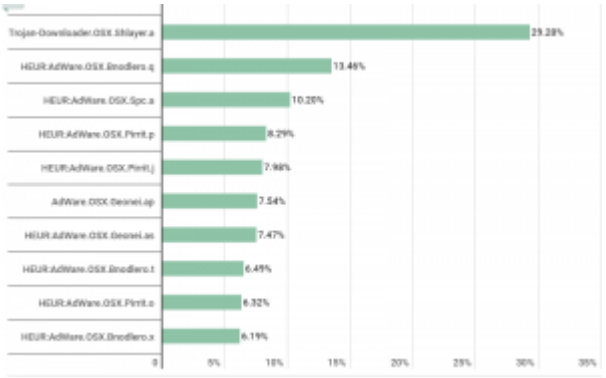
Shlayer is a trojan downloader, which spreads via fake applications that hide its malicious code, according to Kaspersky. Its main purpose is to fetch and install various adware variants. These second-stage samples bombard users with ads, and also intercept browser searches in order to modify the search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



Thus it's perhaps not surprising that, out of the remaining Top 10 macOS threats detailed by Kaspersky for the year, most of them were adware that Shlayer installs – namely, AdWare.OSX.Bnodlero, AdWare.OSX.Geonei, AdWare.OSX.Pirrit and AdWare.OSX.Cimpli.

## Infection Process

Shlayer generally arrives on users' desktops via a malicious download. Kaspersky noted that the cybercriminals behind the code have set up an elaborate distribution system with a number of channels leading users to download the malware.




Top 10 Mac Malwares of 2019 (click to enlarge)

"Shlayer spreads via a partner network of thousands of websites, often targeting visitors of legitimate sites, including YouTube and Wikipedia," Kaspersky explained in an analysis of the code, released Thursday. "YouTube,

where links to the malicious website were included in video descriptions, and Wikipedia, where such links were hidden in the articles' references."

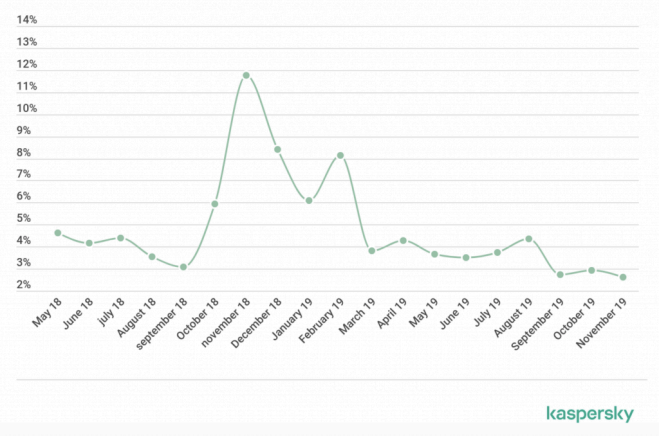
To put this affiliate network together, Shlayer's operators court website owners (and those willing to, say, upload a YouTube video or edit a Wikipedia page) with a promise to monetize their sites in exchange for pushing malicious links pointing to Shlayer downloads. The crooks offer websites "relatively high payment for each malware installation made by American users, prompting over 1,000 partner sites to distribute Shlayer," according to the research.

Most of the campaigns hinge on entertainment themes. Unwitting web users searching for, say, a popular TV series episode or a sports broadcast will be redirected to a fraudulent site claiming to offer content streams; in reality, the links on the site are pushing the malware.

Kaspersky has also seen advertising landing pages redirecting victims to fake Flash Player update pages.

## Under the Hood

Overall, Shlayer is being hosted for download on 700 different domains, to which the links redirect visitors. The most recent Shlayer variant is Trojan-Downloader.OSX.Shlayer.e, Kaspersky analysis revealed, which stands apart because it's written in Python rather than Bash, as its prior versions were.




Shlayer Detections Over Time (click to enlarge).

Upon initial download, the user is prompted to run an "installation" file.

"However, the seemingly standard installer turns out to be a Python script, which is already atypical of macOS installation software," the research explained. "The directory with executable files inside the application package contains two Python scripts: gjpWvvuUD847DzQPyBI (main) and goQWAJdbnuv6 (auxiliary)."

The auxiliary script implements data encryption on the malware's functions. Next, the main script generates a unique user and system ID, and also collects information about the version of macOS in use. Based on this data, the GET query parameters are generated to download the ZIP file containing Shlayer.

"The ZIP archive downloaded to the /tmp/%(sessionID) directory is unpacked to the /tmp/tmp directory using the unzip function," Kaspersky explained. "The ZIP archive was found to contain an application package with the

executable file 84cd5bba3870. After unpacking the archive, the main Python script uses the chmod tool to assign the file 84cd5bba3870 permission to run in the system."

After that, the trojan runs the downloaded and unpacked application package using the built-in open tool, and deletes the downloaded archive and its unpacked contents.

## Second Stage Adware

Shlayer simply penetrates the victim system, loads the main payload, and runs it. After that, the second-stage adware takes over; in recent campaigns, Kaspersky observed Shlayer actively downloading the AdWare.OSX.Cimpli family.

Cimpli masquerades as a useful Mac utility (i.e., "Any Search") – but in actuality installs a malicious extension in Safari, hiding the OS security notification behind a malware fake window.

"By clicking on the buttons in the notification, the user in effect agrees to install the extension," according to the research.

The extension is called ManagementMark, which monitors the victim's online searches and redirects them by injecting a script into the browser pages. The sample also loads the mitmdump tool, which is given permission to view HTTPS traffic via special trusted certificate that the malware adds to the system (also achieved by superimposing a fake window over the installation confirmation box). All traffic passing through mitmdump is then processed by a script that redirects all user search queries to a SOCKS5 proxy.

"Cimpli adware thus becomes firmly anchored in the system; in the event that traffic does not pass through the proxy server, the JS code of the extension injected in the page handles the redirection of queries," according to the research. "The attacker gains access to the user's search queries and can modify the search engine results to display advertising. As a result, the user is inundated with unsolicited ads."

Luckily for macOS users, these campaigns are all aimed at feeding illicit advertising to victims, rather than something more dangerous, such as stealing financial data. However, the cybercriminals behind Shlayer could evolve their focus at any time, according to Kaspersky.

"Despite macOS' reputation as a much safer and more secure system, there are still cybercriminals trying their luck to profit from macOS users, and Shlayer is a perfect example," the firm noted. "Furthermore, ever since Shlayer was first detected, its infection algorithm has hardly changed, even though its activity barely decreased, making it an especially relevant threat."

---