



*Issued 4/1//17*

## **Skype Users Hit By Ransomware Through In-App Malicious Ads**

Several users have complained that ads served through Microsoft's Skype app are serving malicious downloads, which if opened, can trigger ransomware.

News of the issue came from a Reddit thread on Wednesday, in which the original poster said that Skype's home screen -- the first screen that shows up on consumer versions of the software -- was pushing a fake, malicious ad, purporting to be a critical update for the Flash web plug-in.

According to the thread, the ad triggered a download of an HTML application, designed to look like a legitimate app. The app, when opened, would download a malicious payload, which locks the user's computer and encrypts its files for ransom. Many other users in the past few days have also complained of similar issues with Skype's in-app ads, with at least two other people having the same "fake Flash" ad into Thursday.

The "fake Flash" ad, designed to target Windows machines, pushed a download, which when opened would trigger obfuscated JavaScript. The code starts a new command line, then deletes the application that the user just opened, and runs a PowerShell command, which then downloads a JavaScript Encoded Script (JSE) from a domain that no longer exists, likely one of many disposable domains used to hide an attacker's operations.

All of these steps, one after another, help the malware evade detection by antivirus tools.

In a brief statement sent more than a day after we asked for comment, Microsoft said the rogue malware-pushing ad found within Skype was a "social engineering" effort, and deflected any responsibility for the issue. "We're aware of a social engineering technique that could be used to direct some customers to a malicious website," said the spokesperson. "We continue to encourage customers to exercise caution when opening unsolicited attachments and links from both known and unknown sources and install and regularly update antivirus software."