Issued 8/25/17

Facebook Messenger user? Watch Out for Fake Messages Rigged with Malware

Cybercriminals are using Facebook Messenger to spread adware, duping victims by redirecting them to fake versions of popular websites that are tailored to their browser. The attacks were uncovered by a security researcher who received a suspicious Facebook message from a contact and analyzed its contents. "This malware was spreading via Facebook Messenger, serving multi-platform malware/adware, using tons of domains to prevent tracking, and earning clicks. The code is advanced and obfuscated," said David Jacoby, senior security researcher in the global research and analysis team at Kaspersky Lab. Researchers have suggested that malicious links are being sent from Messenger accounts that have been compromised as a result of stolen credentials, hijacked browsers, or clickjacking.

The initial attack is fairly simple. Given the user knows the person they're receiving the message from, it's likely they'll trust what is being sent, and so click on what appears to be links to videos, memes, and other content. The user is sent a message composed of their name followed by the word 'Video', and a shocked emoji face with a shortened URL: for example, in the documented case, the message said 'David Video'. The link leads to a Google Doc, which blurs a photo taken from the victim's Facebook page and makes it look like a playable movie. When the victim clicks on this video, the malware will send them to one of a number of different websites, depending on their browser, operating

system, location, and other factors. This site will then attempt to encourage the target to install adware. For example, a Google Chrome user is sent to a website designed to look like YouTube, complete with the official logo and branding. The website shows the visitor a fake error message designed to trick them into downloading a malicious Chrome extension. Firefox users get directed to a website displaying a fake Flash Update notice, which attempts to run a Windows executable to deliver the adware. Meanwhile, Safari users get a similar page customized for macOS, which offers the download of a .dmg file, which is also adware.

These adware programs track browser activity using cookies and display targeted adverts across the web, which in some cases socially engineer the victim into clicking on them. Each click on one of these adverts will generate revenue for those behind the scheme.