New Version of Shylock Malware Spreading Through Skype

By Dennis Fisher

Published: 2013-01-17 · Archived: 2026-04-05 20:39:59 UTC

There is a new version of the Shylock malware that is now capable of spreading through Skype. The new version is spreading mainly in the U.K., Europe and the U.S. and is playing off the fact that Microsoft is about to kill its Messenger application in favor of Skype.

There is a new version of the Shylock malware that is now capable of spreading through Skype. The new version is spreading mainly in the U.K., Europe and the U.S. and is playing off the fact that Microsoft is about to kill its Messenger application in favor of Skype.

The new version of Shylock has a number of new capabilities, but its goal is the same: stealing sensitive financial data from infected machines. Shylock has been known publicly for more than a year and researchers have watched it morph and adapt its tactics in the last few months. The malware, like other Trojan bankers of its ilk, is designed specifically to steal credentials for online banking sites, and also has the ability to perform code-injection attacks.

One recent change in the Shylock malware's capabilities was the addition of a feature that can detect whether the malware is being installed on a remote machine via the RDP protocol. That method is one that malware analysts and researchers use to analyze the behavior of malware.

The newest addition to Shylock's arsenal is its ability to spread via Skype instant messages. An analysis by researchers at CSIS in Denmark shows that the newest version of the malware includes a plugin named "msg.gsm" that uses the chat function in Skype in order to spread to new machines. The malware relies on a network of infected Web sites to perform drive-by download attacks as the initial infection vector, and once it is resident on a new machine and finds the Skype application, it then sends malicious links to the victim's contacts through the chat function.

"The Skype replication is implemented with a plugin called "*msg.gsm*". This plugin allows the code to spread through Skype and adds the following functionality:
– *Sending messages and transferring files*
– *Clean messages and transfers from Skype history (using sql-lite access to Skype%smain.db)*
– *Bypass Skype warning/restriction for connecting to Skype (using "findwindow" and "postmessage")*
– *Sends request to server: https://a[removed]s.su/tool/skype.php?action=…,"* according to the CSIS analysis.

The newest Shylock malware also includes some other extra features, such as the ability to spread via network shares and USB drives. The attacker behind the malware has the ability to perform a number of functions once he's on the infected machine, including stealing cookies, injecting malicious code into Web sites and downloading and executing files.

This is by no means the first piece of Skype malware that has emerged in recent years. Other samples have had the ability to spread via USB drives, as well.

Source: https://threatpost.com/new-version-shylock-malware-spreading-through-skype-011713/77416/