Shylock/Caphaw malware Trojan: the overview

By Kaspersky

Published: 2014-07-14 · Archived: 2026-04-06 15:37:46 UTC

Recently Kaspersky Lab has contributed to an alliance of law enforcement and industry organizations, to undertake measures against the internet domains and servers that form the core of an advanced cybercriminal infrastructure that uses the Shylock Trojan to attack online banking systems around the globe.

Shylock is a banking Trojan that was first discovered in 2011. It utilizes man-in-the-browser attacks designed to pilfer banking login credentials from the PCs of clients of a predetermined list of target organizations. Most of these organizations are banks, located in different countries.

Kaspersky Lab products detect the Shylock malware as Backdoor.Win32.Caphaw and Trojan-Spy.Win32.Shylock.

We detected this malware generically from the end of August 2011, as Backdoor.Win32.Bifrose.fly. Specific detection of this separate family was added in February 2012. Since then we have observed a very few detections – approximately 24,000 attempts to infect PCs protected by Kaspersky Lab products worldwide.

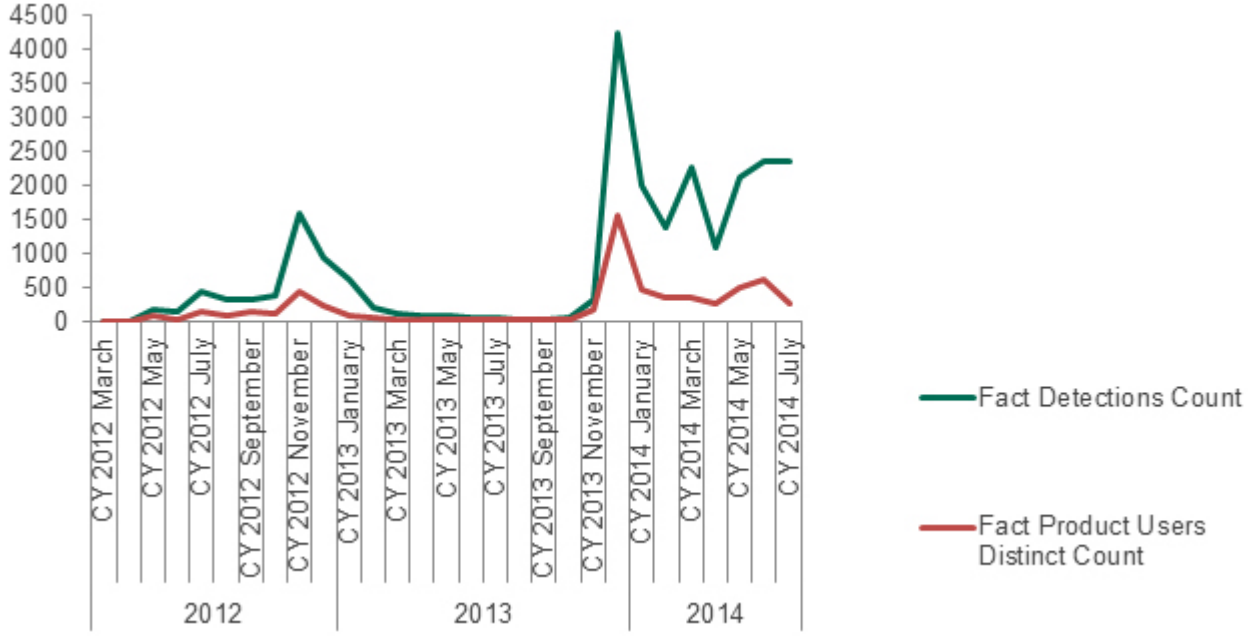
These are very modest numbers, especially in comparison with other infamous banking malware such as ZeuS, SpyEye, Carberp which have generated (and, in the case of some of them, such as ZeuS , still generate) tens or hundreds of thousands of detections. Of course, these numbers don’t tell us everything about how widespread or effective Shylock is, because Kaspersky Lab “sees” only a part of the total number of PC users – only those who use our products.

Low popularity doesn’t make Shylock less dangerous though. The set of malicious techniques it utilizes is no less dangerous than that used by other similar malware. It is able to inject its body in multiple running processes, has tools to avoid detection by anti-malware software, uses several plugins which add additional malicious functions aimed at bypassing anti-malware software, collects passwords for ftp-servers, spreads itself via messengers and servers, provides remote access to the infected machine, video grabbing and of course web injection.

This last function is used to steal online banking credentials by injecting fake data entry fields into the web page loaded in the victim’s browser.

During the entire period we’ve seen two relatively big peaks in detection rate for this malware.

The first one was in November 2012 and the second one was in December 2013.



The geography of the November 2012 peak was as follows:

United Kingdom
Italy
Poland
Russian Federation
Mexico
Thailand
Iran
Turkey
India
Spain

The table above shows the top 10 countries wheremost attacks using the Shylock malware were registered. A little more than a year later, in December 2013, the picture had changed dramatically.

Brazil
Russian federation
Vietnam
Italy

Ukraine
India
United Kingdom
Belarus
Turkey
Taiwan

As these tables show, the criminals behind this malware definitely stopped paying so much attention to the developed e-money markets of the UK, Italy and Poland in favor of the actively developing markets of Brazil, Russia and Vietnam. It's slso interesting that both peaks happened in the late autumn to early winter period, a traditional high retail season in many countries around the world.

According to Europol data, this malware has infected more than 30,000 PCs worldwide. This is a big enough scale to cause huge financial damage, so the disruption of the Shylock backbone infrastructure is very good news.

And even better news is that the recent operation, coordinated by the UK's National Crime Agency (NCA), brought together partners from the law enforcement and the private sector, including – besides Kaspersky Lab – Europol, the FBI, BAE Systems Applied Intelligence, Dell SecureWorks and the UK's GCHQ (Government Communications Headquarters), to jointly combat the threat. We at Kaspersky Lab were glad to add our modest contribution to this operation. Global action brings positive results – an example being the operation targeting the Shylock malware.

Source: https://securelist.com/shylockcaphaw-malware-trojan-the-overview/64599/