

Cyber Threat Advisory

SilentBanker



Operational Data

The following data can be used for Investigation and Defense. Silent Banker accesses the following URLs for updates, and to transfer stolen data:

- ◆ iloveie.info
- ◆ webcounterstat.info
- ◆ microcbs.com
- ◆ reservaza.com
- ◆ screensaversfor-fun.com
- ◆ mystabcounter.info
- ◆ 85.255.119.218

Silent Banker also downloads a Trojan.Flush.J, that can change the users DNS settings to the following attacker settings. At this time these are the two know attacker settings.

- ◆ 85.255.116.133
- ◆ 85.255.112.87



Contact: Kevin G. Coleman
4017 Washington Road
Mail Stop 348
McMurray, PA 15317
P 888-650-0800
F 412-291-1193

www.Spy-Ops.com

Category:	Trojan Horse
Level of Sophistication:	4.2 High
Level of Threat:	3.5 Moderate
Scale of Threat:	1.2 Low (400+)
First Noticed:	Mid 2007
Suspected Source:	Organized Crime Extremist Groups



Overview: This cyber threat has already struck over 400 banks in the U.S. Canada, France, Spain, Ireland, the UK, Finland and Turkey. The malicious code has the ability to get around two-factor authentication and the capability to distribute other Trojan software as well as to update itself. The scale and sophistication of this banking Trojan is worrying, even for someone who sees banking Trojans on a daily basis.

Operation: This software is downloaded to an unsuspected computer. It contains a configuration file that includes domain names of over 400 banks. The banks include large U.S. banks and also banks in at least seven other countries and the list is growing.

This Trojan is a derivative of the older man-in-the-middle (MitM) attacks and becomes a man-in-the-browser (MitB) type exploit. The exploit intercepts valid transactions that use two-factor authentication and silently changes the user-entered destination bank account details to the attacker's account details. Silent-Banker intercepts authentication traffic before it is encrypted so that even if using SSL, the exploit can still take place. As with MitM, MitB style malicious code exploits the collection of user data stolen from valid transactions and the self updating capability are two characteristics that makes this attack very concerning to security experts, banking officials and international law enforcement.

Investigating Agencies Include: Interpol, Scotland Yard, the FBI, KRP (Finland's FBI) and possibly more than a dozen other agencies.

Reference Links:

- http://www.symantec.com/enterprise/security_response/weblog/2008/01/banking_in_silence.html
- <http://www.microsoft.com/security/portal/Entry.aspx?ThreatId=-2147367388>
- <http://www.networkworld.com/news/2008/011408-silentbanker-trojan.html?page=1>