Tinba Malware – New, Improved, Persistent

Ilan Meller, 2014-07-11

As investigated by Pavel Asinovsky, F5 SOC Malware Researcher, Tinba, also known as “Tinybanker”, “Zusy” and “HµNT€R$”, is a banking Trojan that was first seen in the wild around May 2012. Its source code was leaked in July 2014. Cybercriminals customized the leaked code and created an even more sophisticated piece of malware that is being used to attack a large number of popular banking websites around the world.

The original Tinba malware was written in the assembly programming language and was noted for its very small size (around 20 KB including all Webinjects and configuration). The malware mostly uses four system libraries during runtime: ntdll.dll, advapi32.dll, ws2_32.dll, and user32.dll. Its main functionality is hooking all the browsers on the infected machine, so it can intercept HTTP requests and perform web injections.

The new and improved version contains a domain generation algorithm (DGA), which makes the malware much more persistent and gives it the ability to come back to life even after a command and control (C&C) server is taken down.

Tinba configuration file reveals browser injections of several targeted banks, mainly from Australia, but also from Germany, Spain, Finland, and Switzerland.

There are multiple injection types, most likely bought in the underground from different Webinject writers. There is a generic VBV grabber, ATSEngine CC+VBV grabber, some specially crafted injections that are adjusted to each bank, and some other miscellaneous injections such as a Bitcoin stealer. Some of the man-in-the-browser (MITB) panels and files are hosted on different servers.

The ATSEngine CC+VBV grabber is also widely used by the known Zeus Trojan, and is sold as a toolkit in the underground. This is a dynamic injection that can be updated easily on the server side without sending a new configuration to each bot, and it can be configured to steal credit card and other sensitive information from Google, Yahoo!, Windows Live, and Twitter websites.

When an infected user logs in to his banking account, a specially crafted injection may produce a popup requesting additional details, credit card information, PIN/OTP authentication, or other info that may be used for fraudulent activities such as performing transactions, stealing sensitive data, and more. It all depends on the configuration of the malware and the script it injects. Some scripts may present false information in regards to the banking account, such as balance information, history of transactions, out-of-service messages, and more.

Download Tinba full technical analysis report from here.

Get your Tinba executive summary here.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com