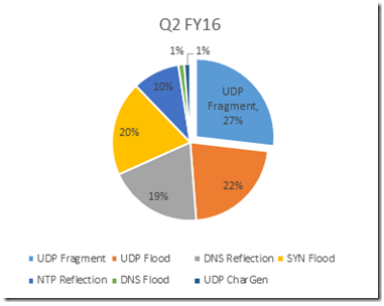
# Tinbapore: Millions of Dollars at Risk

Ilan Meller, 2016-13-01

Detected by F5 WebSafe security solutions during November 2015, Tinbapore attack has put millions of US dollars at risk. F5 Security experts investigation revealed that Tinbapore is actually a new variant of the good old Tinba Malware that so far was targeting financial institutions in the Europe, Middle East, and Africa (EMEA) region and the Americas. 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.

Newer and improved versions of the malware employ 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. This new variant of Tinba, Tinbapore, now creates its own instance of explorer.exe that runs in the background. It differs from most previous versions in that it actively targets financial entities in the Asian Pacific (APAC), which was previously uncharted territory for Tinba.




To download your copy of the Tinbapore variant analysis report, click here.

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

| | | | |
|---|---|---|---|
| F5 Networks, Inc.<br>Corporate Headquarters<br>info@f5.com | F5 Networks<br>Asia-Pacific<br>apacinfo@f5.com | F5 Networks Ltd.<br>Europe/Middle-East/Africa<br>emeainfo@f5.com | F5 Networks<br>Japan K.K.<br>f5j-info@f5.com |