

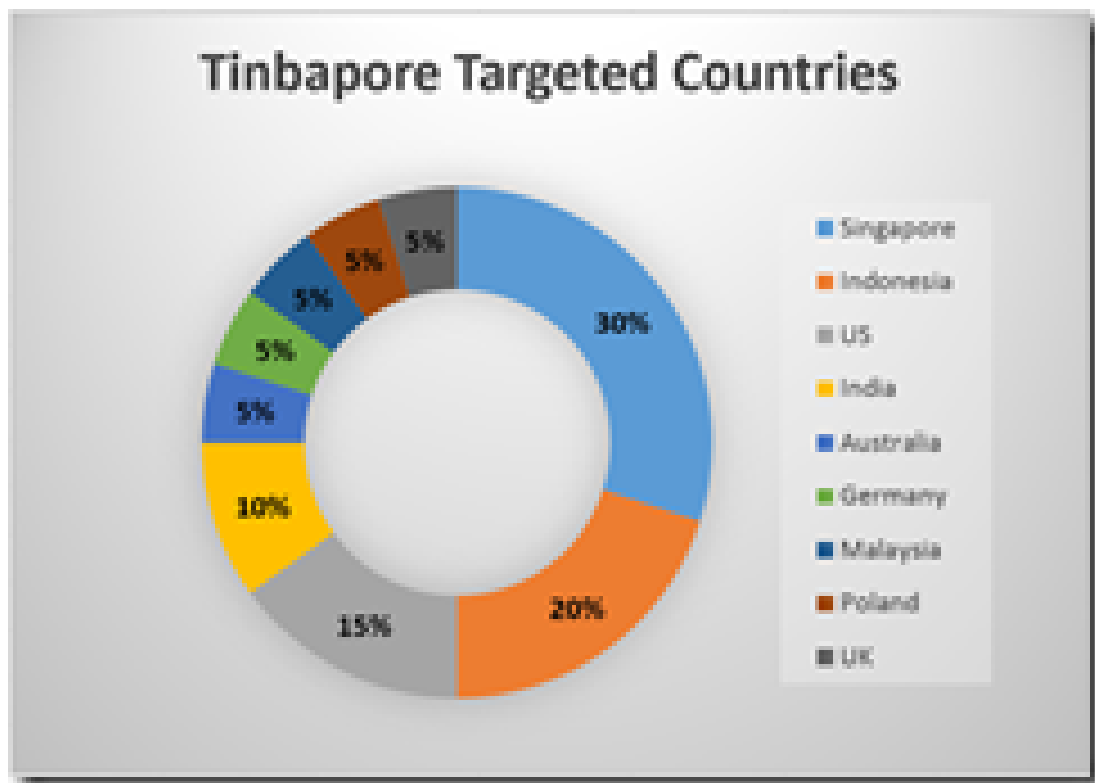
Slave – IBAN swap, persistency and Zeus-style webinject



Ilan Meller, 2015-18-06

Slave is a financial malware written in visual basic. It was first seen around March 2015 and has undergone a significant evolution. Slave conducts its attack by hooking the Internet browser functions and manipulating their code for various fraudulent activities. This manipulation can be used for fraudulent activities such as credentials theft, identity theft, IBAN swapping and fraudulent fund transfers.

Two weeks before the discovery of 'Slave', the F5 research team analyzed an unknown malware variant that was used for swapping IBAN numbers – a technique used by fraudsters to swap the destination account number before a funds transfer takes place. Static analysis has shown a strong relationship between the two malware samples, implying that 'Slave' started out with a simple IBAN swap capability and later advanced to more advanced capabilities such as persistency and Zeus-style webinjects.



If you want to deep-dive into the 'Slave' internals [click here](#) to read the full technical Malware Analysis Report by F5 SOC.

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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113