

E-Threats Landscape Report

Executive Summary

IT&C SECURITY COURSE JULY– DECEMBER 2010



Disclaimer

The information and data included in this document represent the current opinion of BitDefender® on the topics addressed as of the date of publication. This document and the information contained herein should not be interpreted in any way as a BitDefender's commitment or agreement of any kind.

Although every precaution has been taken in the preparation of this document, the publisher, authors and contributors take no responsibility for errors and/or omissions. Nor is any liability undertaken for damage resulting from the use of the information contained herein. In addition to that, the information in this document is subject to change without prior notice. BitDefender, the publisher, authors and contributors cannot guarantee further related document issuance or any possible post -release information.

This document and the data contained herein are for informative purposes only. BitDefender, the publisher, authors and contributors make no warranties, express, implied, or statutory, as to the information stated in this document.

The document content may not be suitable for every situation. If professional assistance is required, the services of a competent professional person should be sought. Neither BitDefender, the document publishers, authors nor the contributors shall be liable for damage arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred to in this document as a citation and/or source of current or further information does not imply that BitDefender, the document publisher, authors or contributors endorse the information or recommendations the individual, organization, independent or collective work, including printed materials, electronic documents, websites, etc. may provide.

Readers should also be aware that BitDefender, the document publisher, authors or contributors cannot guarantee the accuracy of any information presented herein after the date of publication, including, but not limited to World Wide Web addresses and Internet links listed in this document which may have changed or disappeared between the time this work was written and released and the moment it is read.

The readers are entirely responsible to comply with all applicable international copyright laws arising from this document. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of BitDefender.

BitDefender may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from BitDefender, this document does not provide any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2011 BitDefender. All rights reserved.

All other product and company names mentioned herein are for identification purposes only and are the property of, and may be trademarks of, their respective owners.

Second Half's Spotlight E-Threats

The information security landscape has been shifting for quite some time, as the natural fight between cyber-criminals and antivirus vendors unfolds: new technologies make place to new attack vectors, which are fixed by new technologies again. It took more than 40 years for malware to morph from programming flaws and innocent pranks into a money-making industry cashing on the unwary, but it took it less than 5 years to reach its next evolutionary step and become one of the most feared weapons of cyber-warfare.

- Social networks have constantly been in the cyber-criminals focus. With a user base of more than 500 million active users, Facebook ranks as the largest social network in the world. Cyber-criminals have been increasingly interested in disseminating their malicious creations to the social network's user base, while also trying to harvest whatever information they find on users' profiles to carry on subsequent attacks.
- Do-It-Yourself malware has made it easier for script kiddies and people with limited IT knowledge to launch attacks against other computer users. The Facebook Hacker, Gmail Hacker and the iStealer keylogger have been some of the tools of choice for junior cyber-criminals.
- Although dramatically crippled by the termination of the spamit.com affiliate program, the spam index has reached 85.1 percent of the total number of e-mail messages sent worldwide. The spam breakdown on categories is as follows:
 - Medicine Spam – 48.12%
 - Casino and Gambling – 18.91%
 - Replica Products – 6.93%
 - Bundled malware – 3.5%
 - Loans and Finance – 7.13%
 - Software – 4.95%
 - Diploma and Education – 4.46%
- Phishers have paid much more attention to social networks than to financial institutions. During the past six months, Facebook has become the prime target of cyber-criminals, with PayPal and Visa ranking second and third, respectively. Online gaming websites conclude the list of the most targeted institutions and services.
- The malware landscape has been mostly dominated by Trojan.Autorun.Inf and Win32.Worm.Downadup, two malicious contenders that have their roots in the Windows XP era, but managed to keep their places despite the fact that operating system upgrades or applying patches would have solved the security issues exploited by these pieces of malware.

Future Outlook

Year 2010 has been full of unexpected surprises in terms of security. The e-threat landscape has witnessed new and unusual activity, such as the advent of the Stuxnet worm. Also, the recent events related to the Wikileaks scandal has triggered a massive wave of protest from select groups of internet users, who turned their Low-Orbit Ion Canons against the institutions that withdrew support for Wikileaks or publicly condemned their actions.

The massive wave of distributed denial-of-service attacks has paralyzed network activity for Internet service providers, payment processors and government websites. Unlike regular DDoS attacks which rely on infected computers to launch the bulk of packets against their victim, this was a voluntary, coordinated effort of millions of users who willingly surrendered their computers to unknown persons to provide the necessary attack power.

Conventional botnets have witnessed a slight decrease in the number of spam messages sent through the multitude of infected drones. However, early signs revealed that the slowdown has been temporary and botnets are rapidly ramping up spam in order to catch up with their financial loss.

Along with conventional botnets comprised of infected computers, new threats will emerge from botnets created with users' consent. These networks of computers will likely focus on performing DDoS attacks as forms of social protest against institutions that regulate the use of the Internet.

During 2011, malware authors will pay special attention to making their creations as stealthy as possible. The highly successful debut of malware signed with genuine stolen digital certificates or with counterfeit ones (as seen in Stuxnet and various variants of ZBot) will likely continue in high-profile malware created throughout 2011.

Other significant security threats we will likely see in 2011 will be related to the widespread access to new technologies such as HTML5, which will offer users new ways to interact with the online media, as well as the development of cross-platform malware that uses Java to infect both Mac OS X and Windows users.

In 2011, the mobile security landscape will see the rapid rise of Google's Android operating system and the availability of an intuitive software development kit which will simplify malware writers' efforts to create rogue applications for both Android-based phones and the upcoming Android-based tablet PCs.