E-Threats Landscape Report

Executive Summary

IT&C SECURITY COURSE JANUARY – JUNE 2010

bitdefender

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.

First Half's Spotlight E-Threats

If year 2009 was everything about the Conficker worm and its rapid mutations, the first half of 2010 saw the rise of worms exploiting various Web 2.0 platforms. Various breeds of the Palevo worm or the more advanced rootkit-based Tofsee family have taken instant messenger users by surprise, triggering miniature pandemics among infected contacts.

Social networks and Web 2.0 services have become one of the most valuable channels of malware dissemination during the last six months. Malware authors usually rely on worldwide events and popular showbiz names to entice unwary users into downloading and running malware. The FIFA World Cup and the massive floods in Guatemala are only two of the many events used for Black-Hat SEO optimization to improve the ranking of various malware-serving websites..

- **Trojan.AutorunINF.Gen** ranks first in the BitDefender half-yearly malware top with more than 11 percent of the total number of infections. Initially designed to simplify the installation of applications located on removable media, the Windows Autorun feature has been used on large scale as a means of automatically executing malware as soon as an infected USB drive or an external storage device has been plugged in.

- MBR worms have made a comeback with upgraded viral mechanisms. Late January saw the emergence of Win32.Worm.Zimuse.A, a deadly combination of virus, rootkit and worm. Upon infection, the worm would start counting down the days. 40 days from the infection, it would overwrite the hard disk drive's Master Boot Record, thus rendering the OS unable to boot.

- Pharmacy spam has reached new heights, jumping from 51 to 66 percent during the six-month period. The spam breakdown by type for the first half of 2010 is:
    - Medicine Spam – 66%
    - Replica products – 7%
    - Loans and insurance – 5%
    - Bundled malware – 3.5%
    - Casino and gambling – 3.5%
- Critical 0-day exploits on popular software such as the Internet Explorer browser from Microsoft® or Adobe® Reader®, Adobe® Flash Player® and even Adobe® Photoshop® CS 4 have also played a key role in the malware landscape for the first half of 2010. Some of the Internet Explorer exploits have even been used to attack major companies such as Google, Adobe® and Rackspace®.
- For the first half of 2010, phishers have mostly focused on impersonating Paypal and eBay. The HSBC Bank ranks third, while Poste Italiene and EGG conclude the list of the most abused online identites

Future Outlook

While the first six months of 2010 have been dominated by conventional e-threats such as Trojans and worms, various exploits pointing at third-party applications have rapidly gained ground, both in count and in terms of impact. As seen in the case of Exploit.Comele.A, zero-day vulnerabilities may be used for purposes that are beyond identity theft or compromising banking accounts: we are looking at fully-fledged weapons used in cyber-warfare and top-level industrial espionage.

With Facebook® surpassing 400 million users, most of the malware authors will focus on the social networking platform to deliver their newest payloads. Some of these attacks will focus on social engineering tricks (such as launching various malware offensives from compromised computers), while others will try to exploit different vulnerabilities or features already implemented across the platform.

Personal information leaks will also dramatically contribute to the success of various attacks, especially when data harvested from social networks is corroborated with personal blogs, career history and other relevant data. Third-party applications are also expected to play an important role in social networking abuses.

The introduction of HTML5, the upcoming major revision of the HTML standard, will add extra levels of interaction between the user and the webpage and will probably change the face of the Web as we know it. The new technology is highly likely to be exploited by malware authors to compromise the browser security.

Cracked and non-genuine software will also constitute a key element in the propagation of various malware. On the one hand, most of the mechanisms of circumventing commercial software protection available for download on “warez” portals are already rigged with various types of malware from keyloggers to backdoors. On the other hand, non-genuine copies of the Windows® operating system can’t receive the latest security updates, which will leave the machines running it unprotected against the upcoming 0-day exploits and vulnerabilities which are expected to be discovered in the next 6 months.