E-Threats Landscape Report
Executive Summary
JANUARY– JUNE 2009

bitdefender

Disclaimer

The information and data asserted 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 assume no responsibility for errors and/or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. In addition, 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 information 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 damages arising here from.

The fact that an individual or organization, an individual or collective work, including printed materials, electronic documents, websites, etc., are referred 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 endorses 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.

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.

First Half's Spotlight E-Threats

During the first half of 2009, the most important security incident was triggered by the emergence and expansion of the Downadup / Conficker / Kido internet worm exploiting a vulnerability in Microsoft operating systems prior to Windows Vista.

The MS08-067 vulnerability allowed Downadup to infect about 11 million computers worldwide during the first half of 2009. The infection is still in the wild, with hundreds of systems compromised on a daily basis.

Other significant malware vectors were leaked, unofficial distributions of Microsoft's upcoming technologies: Windows 7, Microsoft Office 2010 and Microsoft Visual Studio 2010. Malware writers relied on kits infected with Trojans in order to infect unwary users leeching these novelties via Bit-Torrent.

- ATM malware spotted in the wild: Trojan.Skimer.A targets automated teller machines from US manufacturer Diebold. The malicious application creates a virtual 'skimmer' which is capable of recording card details and personal identification numbers without the user's knowledge.
- Fake disinfection tools for the Downadup Internet worm: building on the pandemics triggered by the Downadup worm (about 11 million infections to date), malware authors released fake disinfection tools for the worm that actually would drop miscellaneous malicious files, especially rogue security software.

- Spam has grown to new heights with Canadian Pharmacy ranking as number one spam source.
    - Medicine Spam – 519
    - Product Spam (replica products) – 6%
    - Hardcore pornography – 3%
    - Phishing attempts – 7%
    - Bundled malware – 6%
- Phishing and identity theft affect about 55,000 computer users per month. The most targeted financial institutions are Bank of America, Paypal and Abbey Bank.
- The first proof-of-concept rootkit targeting the upcoming Windows 7 operating system from Microsoft has been thoroughly documented and licensed under GPL license.
- MAC OS X scareware also witnessed a dramatic boost, indicating that it's time of Apple users to adopt a platform-specific security solution.
- Social networking and microblogging have also contributed to leveraging social engineering attacks. Apparently harmless games posted on Twitter exposed sensitive credentials allowing attackers to recover victims' passwords for miscellaneous web services.

Future Outlook

Malware development is a rapidly evolving business, both because this specific niche of software programmers are driven by illicit financial gains and because of technology's rapid evolution.

Most software companies run an extremely tight schedule from envisioning their products to actually delivering them to their users, in order to maximize sales. However, many times, such applications are not fully tested and proofed against various types of attacks or critical coding flaws. Malware authors rely on these flaws to envision novel approaches for penetrating users' systems in both home and corporate environments.

Malware distribution via Warez website and torrent downloads will keep an ascending pace as the number of Internet users increase. The so-called "nulled" PHP scripts used for creating virtual communities often contain backdoors allowing unauthorized third parties to seize control over web servers and host malware or use them as spam relays.

Other vulnerable factors in malware distribution schemes are the very end-users – their lack of awareness on the latest trends in the malware landscape can dramatically impact on both their budget and privacy.

Voluntary disclosure of trivial information via Web 2.0 websites or blogging platforms can also help malicious third parties build personal profiles or gather additional data to be used in phishing attempts.