

E-Threats Landscape Report

Executive Summary

JULY – DECEMBER 2009



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.

Copyright © 2009 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

Year 2009 witnessed a wide range of security threats aiming at both end-users and at corporate networks. The Downadup worm (also known as Conficker or Kido) took a dramatic surge and managed to stay one of the top three global e-threats during 2009. Although not entirely dangerous (as variants A, B and C had no malicious payload), its spreading mechanisms and its resistance to detection may be regarded as the cornerstone of the upcoming breeds of highly-destructive malware.

During the past six months since the release of our previous report, malware authors have preserved their focus to web-based attacks, but at the same time, they have been actively looking for new methods of disseminating their products. Large social networks and ephemeral web pages boosted by intense BlackSEO strategies have also become the favorite hotspots for drive-by downloads and worm distributions.

- **Trojan.Clicker.CM** holds as number one e-threat for the second half of the year. It is used to force advertisements inside the users' browsers when visiting grey area websites (such as porn websites or services offering "warez" software). The alarming infection rate reveals the fact that malware authors are driven by profit and pay-per-click fraud is enough of a motivation to cyber-criminals.
- Distributed Denial-Of-Service attacks are becoming a trend among botnet masters, who now target both financial institutions and popular web services such as **Blogger**, **Youtube**, **Facebook** and **Twitter**. More importantly, the battle between cyber-criminals and legitimate service providers seems to have replaced its financial interests with political ones.
- Spam has increased at an accelerated pace. The spam breakdown by type for the second half of 2009 is:
 - Medicine Spam – 51%
 - Phishing attempts – 7.5%
 - Replica products – 7%
 - Bundled malware – 6.5%
 - OEM Software – 6.5%
- Rogue antivirus software is on the rise, propelled by intense Black Hat SEO and taking advantage of users' lack of technical knowledge. During the second half of the year, rogue AV creators have pushed the legal boundaries even further by rigging their creations with a minimum amount of utility in order to avoid any consequences in the event of a lawsuit.
- One of the most critical vulnerabilities discovered this year is the SMB 2.0 bug that affects all operating systems newer than Vista, except for Windows 7 RTM and Windows Server 2008 R2. However, the RC version of Windows 7 is.

Future Outlook

The vast majority of malicious applications are oriented towards illicit financial gains. BitDefender estimates that the next year will bring an increased amount of malware, especially of adware applications and rogue antivirus software. More complex malware, such as rootkit-based file infectors and worms relying on multiple vectors of infection (e-mail, instant messaging and peer-to-peer protocols), are also expected.

Building on their experience with Facebook and Twitter, malware authors are expected to extend their reach with the new Google Wave, as the search engine's instant messaging service gains popularity. Facebook and Twitter will also stay in attackers' crosshair, given the fact that Facebook has surpassed 350 million users. Spam and phishing attempts targeting social networking users are also expected to rise.

Apart from the fact that social networking websites are expected to become one of the most important vectors of infection, they are also likely to trigger other security incidents such as involuntary public disclosure of sensitive information.

Microsoft's Windows Server 2008 R2 Hyper-V and the VMWare vSphere virtualization technologies have opened new opportunities for small and medium businesses. Accommodating multiple servers to a single machine with virtualization will dramatically contribute to cutting down on costs. During 2010, remote attackers are expected to look for vulnerabilities in software that would allow them to seize control over the hypervisor and, implicitly, on all the virtual machines deployed on the system.

Cloud computing services are also living their heyday. No matter whether they are used for e-mailing (such as Google's Gmail service) or for data storage and backup, the cloud technologies hold and process significant amounts of sensitive data. It is just a matter of time until attackers shift their focus on these infrastructures to seize control over or limit access to these cloud resources.

Netbooks and PDAs will slowly become security risks in corporate environments as their adoption ramps off. These intelligent devices are extremely small; in fact, they are so small that can be easily lost or snatched by a thief. If their physical value is sometimes negligible, the data stored on the local solid-state drive is priceless. Since netbooks do not come with Trusted Platform Modules or other types of hardware / software encryption and cannot be managed remotely (in order to wipe the storage medium clean in case of loss/theft), sensitive information may land into the wrong hands.

BitDefender® is the creator of one of the industry's fastest and most effective lines of internationally [certified security software](#). Since our inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe – giving them the peace of mind of knowing that their digital experiences are secure. BitDefender solutions are distributed by a global network of value added distribution and reseller partners in more than 100 countries worldwide. For more details about BitDefender's security solutions, please check www.bitdefender.com.