



Bitdefender[®]

H2 2011 E-Threat Landscape Report Executive Summary

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

- Hactivism was a major concern through 2011 as a variety of companies and government agencies suffered significant breaches. The fall of the PlayStation Network in April was only the prelude to a series of attacks on targets including defense contractor Mitsubishi Heavy Industries, Adidas, RIM, Tiroler Gebietskrankenkasse, Nexon and even the United Nations.
- The second half of 2011 also witnessed unprecedented abuse of digital certificates in the largest scandal involving DigiNotar, Comodo's Dutch partner. A successfully exploited vulnerability in the DigiNotar website allowed cyber-criminals to issue 531 fake certificates for high-profile institutions such as Google, Tor, CIA and Israel's Secret Service, the Mossad.
- The spam landscape has undergone major modifications after termination of the most prominent spam affiliation services in late 2010 and termination of the Rustock Botnet. In the second half of 2011, the spam index reached 75.1 percent of the total number of e-mail messages sent worldwide. The spam breakdown on categories is as follows:
 - Medicine Spam – 47.5% (H1 2011 value: 48.12%)
 - Replica Products – 15% (H1 2011 value: 6.93%)
 - Casino and Gambling – 12.5% (H1 2011 value: 18.91%)
 - Dating & soft pornography - 6%
 - Employment & job offerings– 4%
 - Software – 3% (H1 2011 value: 4.95%)

- Bundled malware – 2.5% (H1 2011 value: 3.5%)
 - Diploma and Education – 2.5% (H1 2011 value: 4.46%)
 - Loans and Finance – 2% (H1 2011 value: 7.13%)
 - Phishing and Scam: 1.5%
 - Other advertisements – 3.5%
-
- Government-controlled malware shows up in Germany. This backdoor application is known as der Bundestrojaner and appears to particularly target VoIP applications. It tracks and sends to the C&C server information regarding instant messenger discussions and conferences, answered or missed calls, written messages between two or more users, and oral conversations via Skype.
 - The malware landscape has been mostly dominated by Trojan.Autorun.Inf and Win32.Worm.Downadup, two pieces of malware that have taken the top spots since 2009. Although they have been rendered ineffective by the release of Windows Vista, they still inflict damage on users who have not updated their operating system. The most active categories of malware in the second half of 2011 are Autorun-based threats, with 16.04%, file infectors (viruses), with 13.41% and worms, with 13.31%

Future Outlook

Year 2011 was extremely rich in terms of malware activity. A year that started under the auspices of data-breaches and corporate leaks continued with the emergence of highly sophisticated bots such as ZeroAccess and TDL4 and ended with a bang as Duqu, “the son of Stuxnet” was revealed.

Malware will continue its rampant evolution throughout 2012 to a whopping 90,000,000 samples, almost 17 million more than at the end of 2011. The malware pool will contain both variants of old malware repackaged to avoid detection and new malware built around 0-day vulnerabilities in the operating system and additional software.

Malware authors will focus on social networks in 2012. With Facebook surpassing 800 million active users, it has become the largest community on the web. Although the company has made significant progress in securing interactions between users and minimized the response time to threats, more than 400 million users are active and vulnerable to short-lived threats at all times of the day. Throughout 2012, we expect intensification of scams on Facebook and Twitter. We expect one major family of malware to spread via infected links posted on users’ walls.

The Android operating system became a major player in 2011, as a variety of smartphone and tablet vendors integrated their own distributions to power their hardware. Since its introduction in 2008, the Android market share has increased exponentially, taking up between 25% and 50% in the US and UK respectively, two countries with the highest penetration of smartphones. At the same time, the number of threats targeting the Android OS considerably increased, as did the risk of private data leaks.

For 2012, Bitdefender estimates the number of threats specifically designed for Android will grow exponentially as the OS gains ground in the low- and mid-range gadget market.

New technologies will also play a key role in malware incidents. Among these technologies, a crucial role will be played by the following:

The introduction of HTML5

At the moment, HTML5 is universally supported across major browsers and brings new layers of interactions between the user and the site. While enhanced interaction is the main purpose of releasing a major version of the popular mark-up language, the new features will allow cyber-crooks to craft more convincing scams against regular web users via the newly introduced Web Notifications, to track victims with geo-location data (especially if they use HTML5 on their smartphone), or even to initiate attacks against other sites straight from the victim's browser.

IPV6 and the end of the Internet

It is estimated that all the IP addresses in the IPv4 system will be exhausted in the last quarter of 2012. This serious shortcoming that will prevent any new subscriber from getting access to the web has been anticipated for some time now when the implementation of the IPv6 protocol has started. The protocol is supported in most operating systems such as Windows Vista, Windows 7, Mac OS/X, all Linux devices and BSD. By default, IPv6-capable devices support stateless auto-configuration which allows them to communicate with other IPv6 network devices and services on the same network segment by advertising its presence via the IPv6 Neighbor Discovery Protocol (NDP). However, this automated process may expose the network devices to attackers or, in extreme situations, to allow an attacker to take complete control over the network device.

IPv6 traffic also supports IPSec, a mechanism that allows traffic to flow encrypted between source and destination. Although this feature protects against traffic sniffing, it will likely be abused by cyber-criminals to mask botnet traffic to and from the command center to boost their botnets' stealth.

Windows 8 and zero-day exploits

The next year will bring Microsoft's brand-new operating system, Windows 8, to the table. Some releases leaked on torrent and p2p sharing web services ahead of time are usually repacked versions of the OS laden with malware that subvert the OS before it is even fully loaded, making

detection and disinfection much harder. Vulnerabilities in third-party software will also be an important vector of infection as they are constantly capitalized on in the so-called exploit packs.

Targeted phishing attacks based on social-network shared data

The 800 million users active on Facebook post large amounts of private and business-related information on the social network, and many times, these details are made available to non-friends through poor privacy settings. These pieces of information will increase the chances of targeted phishing attacks in 2012.