Imperva Issues 2013 Cyber Security Predictions

The Associated Press

Media Contact: Clinton Karr (415) 432-2441Clinton.Karr@lewispulse.com

Business security company highlights evolution of attack techniques and targets; underscores need for security community collaboration

Redwood Shores, Calif., December 20, 2012 - Imperva, Inc. (NYSE: IMPV), a pioneer and leader of a new category of business security solutions for critical applications and high-value data in the data center, today released its December Hacker Intelligence report "Trends 2013," which delineates Imperva's expections regarding major trends security practitioners should watch in 2013. These trends include hackers adopting malware techniques from "state sponsored" attacks, hackers leveraging cloud infrastructure to conduct attacks and hackers targeting less-protected SMBs; underscoring the need for greater security community collaboration.

"The unfortunate reality of most technology is that it is a double-edge sword - a truth made more real in the information security industry since some techniques for protection can be easily perverted to malicious ends," said Amichai Shulman, co-founder and CTO, Imperva. "In 2013, Imperva expects to see the sophistication of attacks increase as hackers leverage emerging technologies to execute new tactics."

Imperva's "Trends 2013" notes that security should improve for larger, well-funded organizations as strategies emerge to share information in the security community, reducing the randomness of attacks. However, Imperva contends that hackers are also becoming more sophisticated, underscored by these emerging trends for 2013:

Government Malware Goes Commercial - Citing its current research into various botnets, which indicates traditional attacks are becoming more amorphous and redundant, Imperva highlights how techniques previously reserved for allegedly "state sponsored" attacks are making their way into modern malware, blurring the line between cyber crime and cyber war.

Black Clouds on the Horizon - Cloud computing has become a ubiquitous technology term in the past few years, but more thought needs to be given to the impact of cloud computing in cyber attacks. The elastic and resilient benefits of cloud computing, coupled with its low cost, make it an attractive platform for hackers to launch attacks. Some clever hackers have already begun to leverage cloud computing to launch attacks, but Imperva expects this trend to grow even greater in 2013.

APT Targets the Little Guy - In 2012, Imperva saw the continuing trend of smaller businesses being hit by cyber criminals. Imperva believes this is an outcome of the

industrialization of hacking that successfully automated web application attacks. Attackers have learned to exploit and profit from compromised web applications- especially since automation can help uncover poorly protected, smaller companies. Imperva believes automation and poor protection will assist APT hackers target valuable information from smaller organizations.

Security in Numbers - As the security industry becomes more aware of the importance of information sharing, Imperva predicts that in 2013 business and governments will create collaborative defenses by sharing individual protection data.

Hacktivism Gets Process Driven - Hacktivism will breach first, announce second. This is a reversal from the typicall order seen in 2011 and 2012.

To download the full report, please visit the Imperva blog:
http://blog.imperva.com/2012/12/security-trends-2013-trend-1.html

Get up to date security news at the Imperva Data Security blog: www.blog.imperva.com

About Imperva Imperva is a pioneer and leader of a new category of business security solutions for critical applications and high-value data in the data center. Imperva's award-winning solutions protect against data theft, insider abuse, and fraud while streamlining regulatory compliance by monitoring and controlling data usage and business transactions across the data center, from storage in a database or on a file server to consumption through applications. With over 2,000 end-user customers in more than 60 countries and thousands of organizations protected through cloud-based deployments, securing your business with Imperva puts you in the company of the world's leading organizations. For more information, visit www.imperva.com, follow us on Twitter or visit our blog.
Forward Looking Statements
This news release contains forward-looking statements, including without limitation those regarding Imperva's predictions regarding top cyber security trends for 2013. These forward-looking statements are subject to material risks and uncertainties that may cause actual results to differ substantially from expectations. You should consider important risk factors, which include: the risk that our products are not adopted at levels that we anticipate; the risk that our products are not perceived as providing a solution against cyber security attacks; and other risks detailed under the caption "Risk Factors" in the company's Form 10Q filed with the Securities and Exchange Commission, or the SEC, on November 13, 2012 and the company's other SEC filings. We undertake no obligation to update any of the forward-looking statements contained herein after the date of this release, whether as a result of new information, future events or otherwise

© 2012 Imperva, Inc. All rights reserved. Imperva and the Imperva logo are trademarks of Imperva, Inc.

This announcement is distributed by Thomson Reuters on behalf of Thomson Reuters clients. The owner of this announcement warrants that: (i) the releases contained herein are protected by copyright and other applicable laws; and (ii) they are solely responsible for the content, accuracy and originality of the information contained therein. Source: Imperva Inc. via Thomson Reuters ONE

HUG#1666872

Source URL (retrieved on *09/16/2014 - 9:35am*):
http://www.chem.info/news/2012/12/imperva-issues-2013-cyber-security-predictions?cmpid=related_content