Internet Initiative Japan

Internet Initiative Japan Inc.

Phone 03-5205-6310 E-mail press@iij.ad.jp URL http://www.iij.ad.jp/
Address Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan

For Immediate Release

IIJ to offer "IIJ Prevent Money Transfer Scam Solution"

--launch of solution for unauthorized online transaction due to banking malware infections--

TOKYO-December 25, 2014-Internet Initiative Japan Inc. (IIJ, NASDAQ: IIJI, TSE1: 3774), one of Japan's leading Internet access and comprehensive network solutions providers, today announced the start of a service, IIJ Prevent Money Transfer Scam Solution, that prevents damage from unauthorized Internet banking transactions in the event that a user's computer becomes infected by malware.

In recent years, incidents of unauthorized online transactions of a user's savings to a separate account have rapidly increased due to phishing and malware attacks. The National Police Agency announced that the total monetary damage from such incidents in the first half of 2014 (January-June) was 1.852 billion yen, which is approximately a nine-fold increase compared to the same period the previous year. The methods used to obtain these unauthorized transactions are becoming increasingly sophisticated. There is a growing number of so-called "Man in the Browser" (MITB) attacks[*1], where hackers hijack users' browsers after they have logged into Internet banking systems, and the hackers then tamper with the users' information. The IIJ Prevent Money Transfer Scam Solution is an effective defense solution for preventing, at the root of the problem, any unauthorized transactions as the result of an MITB attack due to Internet banking malware[*2] infection. These malware infections are difficult to detect using conventional antivirus software.

This solution provides a virtual application environment when accessing Internet banking services via web browsers. This environment will allow only the data displayed in the browser window on the user's PC to be displayed and transmitted, and it enables protection of the data transferred via the user's PC against theft or tampering. Even if the user's PC has been compromised by a banking malware infection, the malware script is unable to interfere with data transmission routes, thus allowing the user to safely carry out their transaction process.

Features of the IIJ Prevent Money Transfer Scam Solution

- For customers of financial institution
    - The implementation of the solution does not require any modifications to the existing banking system, and it creates an even more robust security system by working in conjunction with existing security measures (one-time passwords, risk-based authentication, etc.). Additionally, it is possible to limit access to the banking system using this solution, which can also reduce development time to support a variety of browsers and browser versions.
- For users
    - The solution does not require the installation of any dedicated applications or browser plug-ins, so users can access Internet banking services in the same environment as before.

This solution has already been adopted by Japanese major bank and used by its individual clients. It is scheduled to be adapted for use with smart devices and to be offered as a service for corporate customers.

This solution is not only offered for financial institutions. It can be used by a variety of companies that use the Internet to conduct business. It is an ideal solution to enable users to utilize secured online services. IIJ will continue to expand the variety of its solutions to enable both service providers and their customers to securely use Internet services.

(*1) Attacks carried out using the user's PC after it has become infected by banking malware. If the user attempts to access an Internet baking service via a PC infected with banking malware, the malware script will attempt to run after the legitimate user has passed the normal authentication gateway. These operations include displaying pop-up windows and rerouting transaction requests to different destination accounts. It is difficult for users to notice unauthorized remittances. It is also difficult for banks to detect because the processing of legitimate and unauthorized remittances is identical.

(*2) A type of malware that executes when a user attempts to access an Internet banking service.

About IIJ

Founded in 1992, Internet Initiative Japan Inc. (IIJ, NASDAQ: IIJI, Tokyo Stock Exchange TSE1: 3774) is one of Japan's leading Internet-access and comprehensive network solutions providers. IIJ and its group companies provide total network solutions that mainly cater to high-end corporate customers. IIJ's services include high-quality systems integration, cloud computing/data center services, security services, and Internet access. Moreover, IIJ has built one of the largest Internet backbone networks in Japan that is connected the United States, the United Kingdom and Asia. IIJ was listed on NASDAQ in 1999 and on the First Section of the Tokyo Stock Exchange in 2006. For more information about IIJ, visit the IIJ Web site at http://www.iij.ad.jp/en/.

The statements within this release contain forward-looking statements about our future plans that involve risk and uncertainty. These statements may differ materially from actual future events or results. Readers are referred to the documents furnished by Internet Initiative Japan Inc. with the SEC, specifically the most recent reports on Forms 20-F and 6-K, which identify important risk factors that could cause actual results to differ from those contained in the forward-looking statements.

For inquiries, contact:
IIJ Corporate Communications
Tel: +81-3-5205-6310 E-mail: press@iij.ad.jp
URL: http://www.iij.ad.jp/en/