

IT BackbonesTM Security News



The IT Shield - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- **Home**
- **About**
- **Contact**
- **Submit PR**
- **Search News**
- **What We Can Offer You**
- **IT Events**
- **Time & Money**

Backdoor Sneaks Into Computers Through Japanese Text Editor

Published 23rd August 2006

Text files are perceived to be rather safe and harmless to download from the Internet or to receive via emails and open in one's computer without much fear about Virus infection. But not for the users of Japanese text editor program Ichitaro, which saves files with '.JTD' extensions.

Security experts at MicroWorld Technologies inform infected JTD files are smartly employed in exploiting a recently found vulnerability in Ichitaro, in order to spread a covert backdoor named 'Win32.Papi.a', thus orchestrating targeted computer attacks in the land of rising sun. Justsystems, the makers of Ichitaro, has issued a patch for the flaw, downloadable at <http://www.justsystem.co.jp/info/pd6002.html>

The backdoor penetration is carried out using a malicious JTD file that backpacks a Trojan Dropper named 'Ichitaro.Tarodrop.a'. The Trojan Dropper exploits a Unicode Stack Overflow Vulnerability in the text editing software to execute its code on the system and to extract a backdoor named 'Win32.Papi.a'.

Once activated, Win32.Papi.a installs itself in the system registry, initiates a Service named CAPAPI, drops its main DLL file which is then injected into the running processes of the compromised computer. It establishes a connection with the remote Server on port 8080 and listens for commands from the remote attacker.

The backdoor can harvest system information, stop and start processes, take

screenshots of the desktop and send them to the attacker, download files from the net and execute them, capture network user information, log off current user, search disks for files, create and move directories and restart the victim's machine. Using Win32.Papi the attacker takes over the targeted machine completely to conduct a range of online criminal activities.

"It's not the first time text editors are used in smuggling malware into user computers. In May, we had reported about 'Win32.Gusi' that was spread via a specially created Word file that exploited a security flaw in Microsoft Word, which incidentally was reported the first time in Japan with the attacker possibly sitting in China," says Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies.

MicroWorld has developed the World's most advanced Security Solutions, eScan and MailScan, that consistently maintain the fastest malware detection and prevention rate. Combining the superior AntiVirus System with its unique MWL technology, MicroWorld protects users from a range of zero-day threats of this nature.

The CEO of MicroWorld Technologies, Govind Rammurthy, gives a broader view on the issue "Trojans and Backdoors that exploit vulnerabilities in system and application software can spread quiet fast and deliver their payload without much of user intervention. They are like camouflaged infiltrators who sneak into your homeland and expand their deadly mission under the cover of darkness. And this particular case goes well to underline what we have been advocating all along, that users need to update timely security patches not just for their Operating Systems, but for application software programs as well."

Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)