

## Backdoor Sneaks into Computers through Japanese Text

### Editor

2006-08-23

Text files are perceived to be rather safe and harmless to download from the Internet or 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."

MicroWorld

MicroWorld ([www.mwti.net](http://www.mwti.net)) is the developer of the world's first Real-Time Anti-Virus and Content Security software eScan for desktops and servers. Its communication security software, MailScan is the first comprehensive e-mail scanner for your SMTP/POP3 Mail Server. MicroWorld Winsock Layer (MWL) is the revolutionary technology underlying these products, powering them to several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready, and Novell Ready. Combining their powerful scanner with MWL technology, MicroWorld solutions provide a Real-Time Proactive security for your systems. For network security of enterprises, eConceal Firewall is the latest powerful offering from MicroWorld.

Information:

Company Name: MicroWorld Technologies, Inc.

Company Contact: Manish Katara

Company Phone: 248 848 9081

Company Site: <http://www.mwti.net>

Category: [Computer](#)

Source: [Press Base](#)

2004-06-01: [New Yorkers Dined, Danced And Dished At The Ninth Annual Taste of Summ...](#)

New York's top restaurants such as Spice Market and Jean George sampled their cuisines for charity to benefit Central Park. CENTRAL PARK, NEW YORK CITY, NY -Summer has officially begun and New Yorker got a taste of what the hottest chefs

Category: [Food](#) Company: [CENTRAL PARK CONSERVANCY](#)

2004-06-11: [Leptin Problems Cause Heart Disease and Obesity...](#)

New science linking the hormone leptin to heart disease and obesity. Announcing the second edition of Mastering Leptin. - Obesity-related diseases claimed approximately 400,000 lives in the last year, closing the gap on smoking as the lea

Category: [Food](#) Company: [Wellness Resources](#)

2004-06-28: [Restaurantica expands directory to include greater Hamilton area...](#)

Interactive dining guide site Restaurantica.com has officially launched a new wing dedicated to restaurants in the greater Hamilton area. Guelph, ON - Restaurantica, Southern Ontario's newest online dining guide, has launched areas dedica

Category: [Food](#) Company: [RESTAURANTICA](#)

2004-06-06: [It's Time to Put Your Hats On for BSE Research...](#)

It's Time to Put Your Hats On for BSE Research Partnership in Support for Beef Research - Smithbilt Hats, the World Professional Chuckwagon Association (WPCA) and UFA have partnered to help raise money for BSE research. Calgary, Alberta

Category: [Food](#) Company: [World Professional Chuckwagon Association](#)

2004-06-06: [The One and Only Germs-Free Skin and Surface Antiseptic Disinfectant T...](#)

The One and Only Germs-Free Skin and Surface Antiseptic Disinfectant Towelette - Germs-Free Disinfecting Towelettes are a Brand New Product for Hand and Surface Disinfecting Our new on the market medical application, Germs-free anti-microbial ethyl

Category: [Food](#) Company: [GERMS-FREE TOWELETTES INC. AKRON, OHIO](#)

2004-06-22: [Diabetic Cures Own Sweet Tooth with Every-Diet Solution...](#)

The owner of an ice cream shop learns he is diabetic and wants to find an ice cream substitute -- he ends up creating a low-fat, low-carb, low-lactate, sugar-free drink that fits the needs of every diet. Aberdeen, NC - Doc Helli, of Aberd

Category: [Food](#) Company: [Carolina 7 Smoothies](#)

2004-06-19: [All-PVC Diaphragm Seals for Corrosive Environments...](#)

All-PVC Diaphragm Seals for Corrosive Environments The "Revolution" Diaphragm Seal also features two revolutionary designs that make it the ideal solution for corrosive environments. First, the "Revolution" features threaded housings that screw toge

Category: [Food](#) Company: [BLACOH FLUID CONTROL](#)

2004-06-11: [Michaelo Espresso Teams with BEST on Espresso Machine Training Program...](#)

Michaelo Espresso Teams with BEST on Espresso Machine Training Program Michaelo Espresso, a Seattle-based espresso machine importer makes committment to espresso technician training program. Michaelo supplied the superautomatic espresso machine trai

Category: [Food](#) Company: [MICHAELO ESPRESSO, INC.](#)

2004-06-26: [Improved Inlet Flow Conditions For Your Pumping System...](#)

The patented "J" Model Inlet Stabilizer was designed specifically for the inlet side of all pumps and drastically improves inlet flow conditions, insuring adequate flow into the pump and extending the service life of all inlet system components.

Category: [Food](#) Company: [BLACOH FLUID CONTROL](#)

2004-06-15: [Uniform Application In The Spray & Metering of Agrichemicals...](#)

Positive Displacement pumps create a pulsating flow and hydraulic shock due to the reciprocating nature of their stroking action. This pulsation makes the uniform application of product in spray and metering applications extremely difficult and can

Category: [Food](#) Company: [BLACOH FLUID CONTROL](#)

**America - Post 9/11**

**Architecture**

**Art & Entertainment**

**Automotive**

**Business**

**Chemical**

**Computer**

**Databases**

**Games & Entertainment**

**Instruction**

**Linux & GNU -Open Source**

**Operating Systems**

**Programming**

**Security**

**Software**

**Utilities**

**Consumer**

**Economy**

**Education**

**Employment / Careers**

**Environment**

**Events / Trade Shows**

**Gaming / Casinos**

**Government**

**Home and Family**

**Industry**

**Insurance**

**Legal / Law**

**Lifestyle**

**Machinery**

**Maritime**

**Medical**

**Miscellaneous**

**Nanotechnology**

**Non-profit**

**Opinion / Editorial**

**Politics**

**Public Utilities**

**Religion**

**Science and Research**

**Society**

**Sports**

**Technology**

**Telecom**

**Trade**

**Transportation**

**Volunteer**

[Web Hosting](#)

[Bulgaria Property](#)

[Secured Loans](#)[Loan](#)[Bielizna](#)[Experience Day](#)[Hotels In Calais](#)

© 2003-2005 www.press-base.com  
Free **press release** distribution service.