



only with

GFI MailSecurity

Download your FREE trial today!

- ABOUT US
- CONTACT
- ADVERTISE

Welcome to a new version of Help Net Security. Much has improved and more is on the way. [Subscribe to our RSS feeds and stay updated!](#)

NEWS

- [Off The Wire](#)
- [Security World](#)
- [Virus Center](#)

ARTICLES

- [Latest Articles](#)
- [Reviews](#)
- [Interviews](#)
- [Book Chapters](#)

SOFTWARE

- [Windows Linux](#)
- [Mac OS X](#)
- [Pocket PC](#)

VULNERABILITIES

- [Vendor Advisories](#)
- [Vulnerability Database](#)

EVENTS

- [Webcasts](#)
- [Conferences](#)

NEWSLETTER

- [Subscribe](#)
- [Current](#)
- [Issue Archive](#)

HOME

E-MAIL ALERTS

SEARCH

RSS

OFF THE WIRE SECURITY WORLD

- [IBM to buy Internet Security](#) • [Microsoft delays re-issue of IE patch](#) • [Protect your applications with AppArmor](#) • [Airport security vs the business traveler](#) • [SELinux Policy Editor: Removing micromanagement from administrative control](#) • [Microsoft campaign goes after 'cybersquatters'](#) • [SSH tunnels: bypass \(almost\) any firewall](#)
- [Microsoft Internet Explorer crash is exploitable](#) • [Sophos offers free rootkit detection and removal tool](#) • [Application Security seeks Common Criteria Certification](#) • [Multi-purpose Windows security and care tool released](#) • [Couple charged in a pump-and-dump stock spam](#)

LATEST ARTICLES VIRUS CENTER

- [Intelligent Data Protection in Today's Enterprise](#) • [Assessing Java Clients with the BeanShell](#) • [What Should Businesses Require of Data Protection Solutions?](#)
- [How to Start Up a Mobile Security Project](#) • [10 Tips for Reducing Storage TCO](#)
- [Backdoor sneaks into computers through Japanese text editor](#) • [Weekly Report on Viruses and Intruders - Oscarbot.KD worm and the Naload.JC and Banker.EEA Trojans](#) • [Fake BBC report spreads Berlusconi death claim and malicious trojan](#) • [Worms exploit critical Microsoft security vulnerability](#) • [New worm](#)

[claims to show you pictures of Paris](#)

## SECURITY SOFTWARE



• [++ GFI LANguard Network Security Scanner 7](#) • [++ Acunetix Web Vulnerability Scanner 3.0](#) • [Kaspersky Security for MS Exchange Server 2003 5.5](#) • [Eraser 5.8](#) • [SSL-Explorer 0.2.7-02](#) • [Kaspersky Anti-Virus for Windows Workstations 5.0](#) • [ScatterChat 1.0.1](#) • [Kaspersky Internet Security 6.0](#) • [Kaspersky Anti-Virus 6.0](#) • [Tor 0.1.1.23](#) • [Password Safe 3.02](#) • [CommView 5.3](#)  
• [Sussen 0.28](#) • [Kaspersky Anti-Spam Enterprise Edition FreeBSD \(25 mailboxes\) 2.0](#) • [Kaspersky Anti-Spam Enterprise Edition Linux \(25 mailboxes\) 2.0](#) • [strongSwan 2.7.3](#) • [yaSSL 1.4.0](#) • [grsecurity 2.1.9](#) • [NuFw 2.0.8](#) • [P0f 2.0.7](#) • [Dazuko 2.2.2](#) • [KisKis 0.19.2](#) • [Samhain 2.2.3](#) • [Firewall Builder 2.0.12](#)  
• [Crypt 3](#) • [Web Confidential 3.7.6](#) • [Pastor 1.7.3](#) • [Little Snitch 1.2.3](#) • [KisMAC 0.21a](#) • [iStumbler 96](#) • [Fugu 1.2.0](#) • [Victor 2.0](#) • [Net Tool Box 3.1](#) • [PDFKey Pro 1.0](#) • [HenWen 2.1.2](#) • [Mac GPG 1.4.1](#)  
• [WiFiFoFum 2.1.1](#) • [Crippin 2.8](#) • [AirFix 1.0b](#) • [Aircanner Mobile Encrypter 2.5](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3](#)  
[RC3](#) • [SignWise Pro 2.52](#) • [Sentry 2020 2.8](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#) • [Touch Password Protection 2.3](#)

## ADVISORIES VULNERABILITIES

• [Cisco Security Advisory - Cisco VPN 3000 Concentrator FTP Management Vulnerabilities \(cisco-sa-20060823-vpn3k\)](#) • [Cisco Security Advisory - Unintentional Password Modification in Cisco Firewall Products \(cisco-sa-20060823-firewall\)](#) • [Mandriva Linux Security Update Advisory - squirrelmail \(MDKSA-2006:147\)](#) • [Mandriva Linux Security Update Advisory - mozilla-thunderbird \( MDKSA-2006:146\)](#) • [Mandriva Linux Security Update Advisory - mozilla-firefox \(MDKSA-2006:145\)](#) • [Mandriva Linux Security Update Advisory - php \(MDKSA-2006:144\)](#)  
• [AOL Directory Permission Weakness Local Privilege Escalation](#) • [Douran FollowWeb register.aspx XSS](#) • [XMB IMG Element SRC Attribute XSS](#) • [PowerPortal index.php search Variable XSS](#) • [PowerPortal search.php search Variable XSS](#) • [SaralBlog view.php website XSS](#)

**GFI:** [Control entry & exit of data on your network with GFI EndPointSecurity. FREE eval!](#)

### Backdoor sneaks into computers through Japanese text editor

Posted on 23.08.2006

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.

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.

[ [Virus Center main page](#) ]



**GFI EndPoint Security**

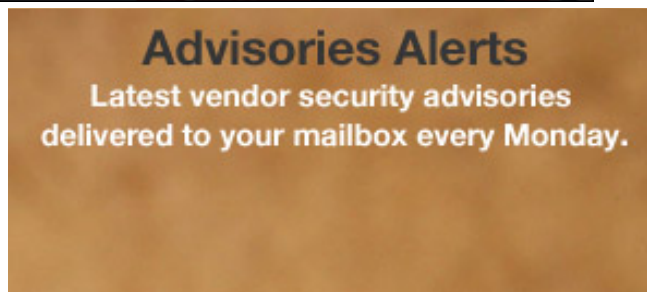
**DOWNLOAD YOUR  
FREE EVAL TODAY!**



**Gartner**  
**IT Security Summit 2006**

18-19 September 2006  
Royal Lancaster Hotel, London

[europe.gartner.com/security](http://europe.gartner.com/security)



**Advisories Alerts**

Latest vendor security advisories  
delivered to your mailbox every Monday.