



**FREE DOWNLOAD
CONTROL & SUPPORT
PCS OVER THE INTERNET
HELPING YOU HELP OTHERS**

**"Screamingly
Fast"**


[HOME](#)
[NEWSLETTERS](#)
[SIGN-IN](#)


FIND:

February 9, 2005

Updated Daily

NewsFactor ▼

[Home/NFN News](#)

[Enterprise](#)

[Databases](#)

[Hardware](#)

Network Security

[Data Storage](#)

[Wireless](#)

[Mac](#)

[Tech Jobs](#)

[Innovation](#)

Network Security

Make your Help Desk fly - [Click Here](#)

Son of MyDoom Stalks Microsoft



By Erika Morphy
Enterprise Security Today
February 10, 2004 1:42PM

Doomjuice appears to be targeting Microsoft, as did Mydoom.B. Security firm F-Secure reported that Microsoft's Web site experienced a disruption in service on Monday as a result. Such incidents are likely to continue in the foreseeable future, as the new worm has been programmed to start a DoS after February 8th.

[COMPLETE STORY](#) ▼

advertisement

[Free white paper](#) on ten best practices used by world-class companies providing email-based customer service. Email customer service, while popular, has historically ranked low in customer satisfaction. Learn how to do it the right way.

A major battle may have been won against MyDoom.A, which spread like wildfire earlier this month and last, but the war against this computer worm still rages on. A variant, dubbed "Doomjuice," has appeared on the scene.

▼ advertisement

Because of the similarity between the Doomjuice and MyDoom codes, it is clear that the same author has written both, Alan Wallace, spokesperson for [security](#) company Panda Software, told NewsFactor. "The attacks, in fact, leverage the computers infected by MyDoom.A," he said.

Unlike earlier versions, which counted on tricking unsuspecting users into downloading infected attachments, the new worm exploits an open port, or backdoor, created by MyDoom.A -- in much the same way that Slammer exploited a server vulnerability.

According to Wallace, Doomjuice creates an entry in the Windows Registry (HKEY_LOCAL_MACHINE SOFTWARE [Microsoft](#) Windows CurrentVersion Run "Gremlin" intrenat.exe), then generates a copy of itself to launch a denial of service (DoS) attack against Microsoft.

So far this morning, he said, none of Panda Software's clients have been affected. The company issued a patch for Doomjuice yesterday, he noted.

Setting Its Sights on Microsoft

Doomjuice appears to be targeting Microsoft, as did MyDoom.B. Security firm F-Secure reported that Microsoft's Web site experienced a disruption in service on Monday as a result. Such incidents are likely to continue in the foreseeable future, as the new worm has been

Top Tech News

CRM Alert

**Wireless Industry
Alert**

Top CIO News

**Enterprise
Security Report**

**Data Storage
Report**

BPM Industry Alert

**Contact Center
Industry Alert**

▼ advertisement

programmed to start a DoS after February 8th.

However, Doomjuice's main goal is not necessarily to shut down Microsoft, Tony Magallanez, a systems engineer with F-Secure, told NewsFactor.

"Doomjuice delivers the source code of the original worm to the infected computer, which is almost never done. Normally, computers that get infected rarely, if ever, have the source code on the hard drive, which makes it much easier to identify the culprits."


But since Doomjuice is implanting the original source code on infected hard drives, it will be much harder for the authorities to convict the virus writer or writers, Magallanez says.

ABCs of Patch Management

Not that companies needed yet another lesson in the efficiencies of automating patch management internally. However as such attacks become ever more commonplace, it is clear that patch management has moved beyond the status of "best practice" to "mandatory business requirement."

"It is what we do in-house and what we recommend to our clients," Anthony Deighton, general manager of [Siebel](#) ERM, told NewsFactor. He noted that there are two schools of thought behind patch management, though: Some companies do not like to automate patch updates because there is always a percentage of computers that break in the process. "Our view is that [the] risk of rolling out a patch that might break a single's person machine is less than the risk of having a virus slip into the network," Deighton said.

Siebel grades the threat as the update comes in, then catalogs all the machines affected by the threat, Deighton said. Not surprisingly, the company uses its own software to manage this process, including cataloging the [infrastructure](#) and rolling out data to employees as to the status of their machines and Siebel's response to the situation.

As for Doomjuice, in particular, Siebel probably can relax. This particular variant is attacking mainly home users who have [broadband](#) connections and who have not cleaned their computers after the first wave of MyDoom struck, Magallanez said. "It's a slower-moving virus than the earlier ones, but we guesstimate that there are tens of thousands infected machines still out there." 

Related Stories

- [MS Issues Explorer Fix, Girds for MyDoom](#)
(3-Feb-04)
- [MyDoom Forces SCO To Change Address](#)
(2-Feb-04)
- [MyDoom Crashes SCO Site](#)
(1-Feb-04)
- [MyDoom Mutates, Targets Microsoft](#)
(29-Jan-04)
- [SCO Posts Bounty for MyDoom Creator](#)
(28-Jan-04)

Latest News & Special Reports

- [PeopleSoft Board Rejects Oracle's Final Offer](#)
- [Juniper Buys NetScreen in \\$3.4B Stock Deal](#)
- [Linux Security on the Ropes](#)
- [The Secret World of ReiserFS](#)
- [ISPs Top Electronic-Billpay List](#)
- [Son of MyDoom Stalks Microsoft](#)
- [Mozilla Unveils Firefox Browser](#)


▼ advertisement

ATTENTION APACHE ADMINS:

TIRED OF THE MAD DASH TO PATCH BEFORE GETTING HACKED?

GET FREE INFORMATION ON THE PORTOLA™ AUTOMATED PATCH SERVICE FOR APACHE.

Portola™

CLICK FOR MORE DETAILS 

Sponsored Links

- [!\[\]\(746d018fdf6ab02bf5fb7681133e8b29_img.jpg\) Integration in Mid-Sized Firms: Necessary for Customer Care.](#)
- [!\[\]\(5daa6eee1904cb6b9d765700250de764_img.jpg\) Free Download - NetOp Remote Control makes your Help Desk Fly.](#)
- [!\[\]\(d72e437c7cc5947bc0b147aba6602563_img.jpg\) Remedy aids customers world-wide to align IT with their business-See how!](#)
- [!\[\]\(0d2a89e6d0cbcd8e0459b972b9332401_img.jpg\) Best Practices in Email Customer Service Used by Leading Companies.](#)
- [!\[\]\(cdcd8a42e5993b465235781ccc1c8555_img.jpg\) Covad S-DSL. Great service level guarantees. Up to \\$500 rebate](#)
- [!\[\]\(c0c9434f3698c901303014555ccb5687_img.jpg\) Siebel CRM OnDemand. \\$70 per person per month. View our CRM demo.](#)
- [!\[\]\(4f9bd4c242eb94a69f6647adc92289eb_img.jpg\) Join live MEGA Enterprise Architecture Web Conference - Feb 17.](#)
- [!\[\]\(2043c91b19713cb6115a4799f072cbca_img.jpg\) NewsFactor's CIO Today Magazine: FREE of charge - subscribe now.](#)

[RSS / XML](#)



NEWSFACTOR TOP TECH NEWS

FIND:

Navigation

NewsFactor Enterprise I.T. Top Tech News

[Home/NFN News](#) | [Enterprise](#) | [Databases](#) | [Hardware](#) | [Network Security](#) | [Data Storage](#) | [Wireless](#) | [Mac](#) | [Tech Jobs Innovation](#) |

NewsFactor Network Enterprise I.T. Sites

[NewsFactor Top Tech News](#) | [Data Storage Today](#) | [Wireless NewsFactor](#) | [CIO Today](#)
[Enterprise Linux I.T.](#) | [Enterprise Windows I.T.](#) | [Enterprise Security Today](#) | [TechExtreme](#)

NewsFactor Network Business Process Management Sites

[BPM Today](#) | [CRM Daily](#) | [Contact Center Today](#)

NewsFactor Services

[FreeNewsFeed](#) | [Free Newsletters](#)

[About NewsFactor Network](#) | [How To Contact Us](#) | [Article Reprints](#) | [Editorial Corrections](#) | [How To Advertise](#)

© Copyright 2000-2004 NewsFactor Network. All rights reserved.