

manageableIT

 one agent, one platform,
one solution


Zotob, PnP Worms Slam 13 DaimlerChrysler Plants

August 18, 2005

By Paul F. Roberts

A round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. auto manufacturing plants offline for almost an hour this week, stranding some 50,000 auto workers as infected Microsoft Windows systems were patched, a company spokesperson told eWEEK.

Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware and Michigan were knocked offline at around 3:00 PM on Tuesday, stopping vehicle production at those plants for up to 50 minutes, according to spokesperson Dave Elshoff.

ADVERTISEMENT

is connected to
petabytes
of data

Confidence in a
connected world.

The company has patched the affected Windows 2000 systems, but is still mopping up after the attack and doesn't know whether deliveries from parts suppliers, who were also affected, might be delayed, he said.

RELATED LINKS

- [Microsoft Ships Zotob Worm Zapper](#)
- [Zotob Proves Patch Management Isn't Enough](#)
- [Zotob Madness and the Real Cost of Windows vs. Linux](#)
- [Zotob Worms Target Windows 2000 Hole](#)
- [Fast-Moving Worms Slam Media, Enterprise Networks](#)

"The effect was not insignificant," he said.

The news from DaimlerChrysler is just the latest in a string of announcements from major U.S. corporations who have been hit by worms with names such as Zotob, RBot and IRCBot.

Read more [here](#) about the Zotob worm and how it attacks.

The New York Times, SBC Communications Inc., ABC Inc. and CNN (of 2005 Cable News Network LP, LLLP) have also said they were hit by the worms, and the full list of those affected is believed to be much longer.

Customer support workers at SBC were forced to work without their computers while IT staff at the

company patched Windows systems that kept rebooting as a result of worm infections that spread across the whole company, said Wes Warnick, a spokesperson at the San Antonio, Texas, telecommunications company.

At DaimlerChrysler, the effects were more dramatic. Assembly lines at 13 plants stopped while staff attempted to patch Windows systems that are integral to the manufacturing process, Elshoff said.

More than 50,000 assembly line workers were forced to cease work during the outages, which ranged from 5 to 50 minutes, but no workers were sent home. The impact of the shutdown was also mitigated by a shift change that normally happens at 3:00 PM, Elshoff said.

The company, which has headquarters in Stuttgart, Germany, is still counting the total number of vehicles that it lost as a result of the disruption, but plans to make up the lost production over time, he said.

Elshoff said DaimlerChrysler believes its network was hit with more than one of the worms, and the company is still feeling the effects of the attacks.

"I wouldn't characterize our operations as out of the woods yet," Elshoff said. The company's financial services group was also hit by the recent worms, which caused PC outages there, he said.

The new malicious programs all rely on code that exploits a hole in the Windows PnP (Plug and Play) service, a common component that allows the operating system to detect new hardware on a Windows system.

Microsoft addressed the PnP hole on Tuesday, issuing [MS05-039](#) with its August patches, a fix rated "critical."

On Wednesday, code for exploiting the hole in Windows 2000 systems appeared on a well-known security Web site. By late Saturday, somebody had combined that exploit with code for spreading across the Internet and created Zotob.A.

[Click here](#) to read about the malware detector Microsoft is shipping for dealing with Zotob worms.

To date, at least 19 different kinds of malicious software have been identified that exploit the PnP hole, including at least five variants of Zotob and new versions of malicious programs like IRCbot and SDbot, according to F-Secure Corp., an anti-virus software firm in Helsinki, Finland.

The most recent worms caused the most damage to companies, which use Windows 2000 more than home users.

DaimlerChrysler is still dealing with suppliers that are also dealing with infections, but does not know whether there will be any disruption in supplies and parts from those third-party companies, Elshoff said.

Zotob isn't the first virus to hit the car maker, but Elshoff defended DaimlerChrysler's approach to security.

"You're only as good as your IT security. I think we play pretty good defense," he said.

However, the company is "Monday morning quarterbacking" and looking into the outbreak to see if changes need to be made in the way software patches are distributed, he said.

Some companies may have deprioritized patching because of a recent drought of high-profile worms and viruses, said John Pescatore, a vice president at analyst firm Gartner Inc.

"There hasn't been a major worm since Sasser [in April 2004]. We've been seeing signs of complacency about patching," he said.

A similar drop-off in worms in 2002 is also believed to have lulled IT staff into relaxing about patches, which led to a number of widespread outbreaks in 2003, such as SQL Slammer and Blaster, he said.

Flashy worms like Blaster and Sasser may have been scarce in the last year, but there has been no drought of automated attacks, said Alan Paller, director of research at The SANS Institute.

Noisy attacks are easy to stop, so attackers just adopted stealthy, low-profile, means of compromising networks.

"When all they want is 10,000 zombie machines, what difference does it make if it takes three years instead of three days?" Paller said.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at eWEEK.com Security Center Editor [Larry Seltzer's Weblog](#).

Copyright (c) 2007 Ziff Davis Media Inc. All Rights Reserved.