Nachi worm infected Diebold ATMs

Kevin Poulsen, SecurityFocus 2003-11-24

The Nachi worm compromised Windows-based automated teller machines at two financial institutions last August, according to ATM-maker Diebold, in the first confirmed case of malicious code penetrating cash machines.

The machines were in an advanced line of Diebold ATMs built atop Windows XP Embedded, which, like most versions of Windows, was vulnerable to the RPC DCOM security bug exploited by Nachi, and its more famous forebear, Blaster.

At both affected institutions the ATMs began aggressively scanning for other vulnerable machines, generating anomalous waves of network traffic that tripped the banks' intrusion detection systems, resulting in the infected machines being automatically cut off, Diebold executives said.

"The outbound traffic from the ATM was stopped -- limited, from a network standpoint -- and effectively isolated," said Nick Billett, Diebold's director of software engineering. "In many cases, the machines were cleaned up that day."

A patch for the critical RPC DCOM hole had been available from Microsoft for over a month at the time of the attack, but Diebold had neglected to install it in the infected machines. Billett defended the company's patching process, which he said involves testing each new bug fix, and deploying at a wide variety of institutions with a mix of network architectures. "A lot of those machines actually have to be visited by a service technician" to be patched, said Billett. "Our experience in the past is we are able to turn those around in one or two days."

In this case, the two affected financial institutions, which Diebold declined to name, somehow slipped thought the cracks, said Billett. The company would not say how many machines were knocked out by the worm.

Windows Bugs

The incident highlights new dangers for financial institutions, as legacy ATMs running OS/2 and propriety communications protocols give way to more versatile and cost effective terminals built on Microsoft Windows and TCP/IP -- with all the attendant security problems.

Though ATMs typically sit on private networks or VPNs, the most serious worms in the last year have demonstrated that supposedly-isolated networks often have undocumented connections to the Internet, or can fall to a piece of malicious code inadvertently carried beyond the firewall on a laptop computer.

January's Slammer worm indirectly shut down some 13,000 Bank of America ATMs by infecting database servers on the same network, and spewing so much traffic that the cash machines couldn't processes customer transactions.

"I think of ATMs as a relative of SCADA systems, as those things not really being on the Internet, but being on *some* network," says Peter Lindstrom, an analyst with Spire Security. "In some ways, it's kind of ironic, that I think standardization across the board has created some of the issues."

In response to the problem, and to meet their customer's IT requirements, Diebold next month plans to begin shipping all new Windows-based ATMs preinstalled with a software-based firewall, made by Sygate Technologies. The company will also offer to put the Sygate product on existing machines already in the field. "We have many customers that are placing ATMs on their network, and as a result of that we have to meet certain criteria ... we haven't had to meet before," said Chuck Somers, vice president of global software development at Diebold.

Somers said he wasn't aware of Diebold ATMs being infected by earlier Windows worms, like Blaster or Slammer. "I'm not aware specifically of machines that were [comprised] as a result of previous ones," he said. "I was made aware specifically of the ones with Nachi, and that was cleaned up"

Microsoft had no immediate comment Monday.

Despite the allure of hard cash, don't expect to see a rash of made-for-Hollywood ATM hacks -- machines around the country suddenly spitting out wads of 20s at random, said Marc Maiffret, Windows expert and "chief hacking officer" at California-based eEye Digital Security.

"The actual point of service terminal itself getting infected-- that's pretty crazy," said Maiffret. "But worms are always going to be able to infect a lot more interesting machines than individual intruders are." Moreover, before reaching an ATM network, a human attacker would likely encounter more alluring high-finance targets along the way. "They're going to have to go through a lot of juicer networks first."

Comments

Mode: Threaded Go

Expand all | **Post comment**

- Nachi worm infected Diebold ATMs 2003-11-25
  Anonymous (2 replies)
  - Nachi worm infected Diebold ATMs 2003-11-25
    Anonymous
  - Nachi worm infected Diebold ATMs 2003-11-26
    Larry Seltzer (2 replies)
    - Nachi worm infected Diebold ATMs 2003-11-26
      Anonymous
    - Nachi worm infected Diebold ATMs 2003-11-29
      Anonymous
- Nachi worm infected Diebold ATMs 2003-11-25
  Anonymous (1 replies)
  - Nachi worm infected Diebold ATMs 2003-11-26
    Frank Sfalanga (1 replies)
    - Nachi worm infected Diebold ATMs 2003-11-28
      Anonymous (2 replies)
      - Nachi worm infected Diebold ATMs 2003-11-29
        Anonymous
      - Nachi worm infected Diebold ATMs 2003-12-08
        Tom Rowe
- Nachi worm infected Diebold ATMs 2003-11-26
  Anonymous
- I wish Mr Poulsen could find out if the voting machines are also at risk. 2003-11-26
  AnonVoter (1 replies)
  - Okay, so I'm not Kevin... 2003-12-05
    Crystal Webb
- No Firewall?? 2003-11-27
  Anonymous (1 replies)
  - No Firewall?? 2003-11-29
    Anonymous (1 replies)
    - No Firewall?? 2003-12-01
      Anonymous
- Nachi worm infected Diebold ATMs 2003-11-27
  HG (1 replies)
  - Nachi worm infected Diebold ATMs 2003-12-04
    Anonymous
- Nachi worm infected Diebold ATMs 2003-11-27
  Biff (2 replies)
  - Nachi worm infected Diebold ATMs 2003-11-28
    Anonymous
  - Nachi worm infected Diebold ATMs 2003-12-02
    Jimbo
- Nachi worm infected Diebold ATMs 2003-11-29
  Anonymous
- Nachi worm infected Diebold ATMs 2003-12-01
  hamster1
- Nachi worm infected Diebold ATMs 2003-12-01
  hamster1 (2 replies)
  - Nachi worm infected Diebold ATMs 2003-12-04
    Babylon
  - Nachi worm infected Diebold ATMs 2003-12-05
    Babylon (1 replies)
    - Windows on ATM's 2003-12-08
      Tom Rowe
- Nachi worm infected Diebold ATMs 2003-12-04
  Anonymous
- Nachi worm infected Diebold (Windows based) ATMs 2003-12-08
  Anonymous