Search GO
Advanced Search

Home
Pay & Benefits
Management
Homeland Security
Defense
E-Government
Per Diems & Travel
Jobs & Careers
Procurement
A-76 & Outsourcing
Bill Tracker
Calendar
Mailbag

Print Subscriptions
E-Newsletters
Events & Awards
Editorial Calendar
Media Kit
Reprints
FAQ
Privacy Policy
About Us
Contact Us

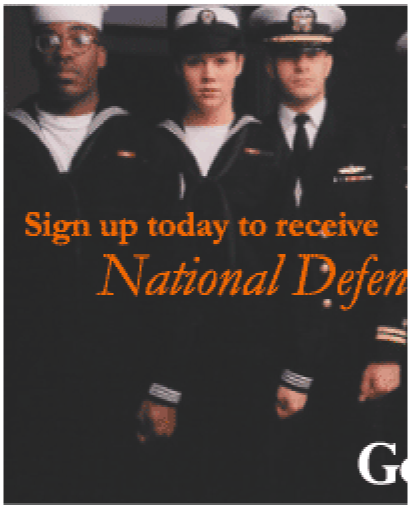
GOVEXEC.COM

FROM THE MAGAZINE
May 1, 2004

FEATURES

# Blindsided

Printer Friendly Version
E-mail this Story to A Friend



By Shane Harris
sharris@govexec.com

*Zero Day attacks come without warning, exploiting computer weaknesses known only to the attacker. They're poised to proliferate and there's no defense against them.*

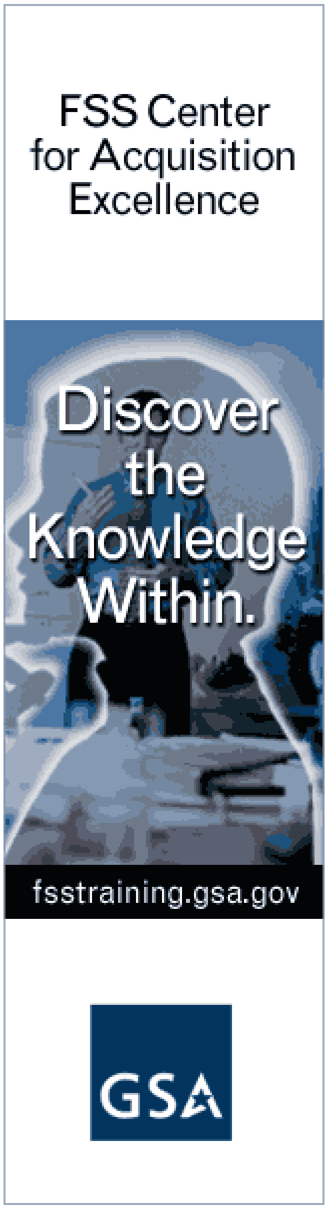
RELATED LINKS
Factoids

Return to
Table of Contents

The Defense Department's electronic networks, the nervous system that controls America's military muscles, bristle with more than 3 million desktop compute battlefield so big that even the soldiers who defend it say it's beyond their con streams of data and commands, from the mundane to the most secret and restr through more than 1,500 internal networks and 100,000 data servers. And at r locations, this behemoth connects to the Internet. These connections help Am its military might across the globe. But they also open the military computer r attack. And it is attacked ferociously. Once every 12 minutes.

Most attacks fail. Digital assailants bombard the networks with worms, viruse digital artillery, known as "exploits," 47,000 times a year. Most don't penetrat defenses. Rings of sensors and firewalls detect and destroy electronic invader military network, though an enticing target for hackers, spies and enemy state mostly impenetrable, its defenders say. But now and then, something slips pas

When an exploit breaches the outer realm through a structural weakness in the



sets the defenders' hair on end. A well-tuned worm or virus can corrupt files a network arteries. Some exploits can put whole portions of the network under t control. Every network, military or civilian, government or nongovernment, h weaknesses. But defenders usually know where they are vulnerable and, with they can thwart assailants.

Recently, however, a new form of attack is turning the tables. Defenders neve coming and discover it only after its damage is done. Defenders have tagged i ominous moniker: Zero Day.

Zero Day attacks mark a turning point in the cyber war. For some time, netwo have held the high ground because software manufacturers publicize vulnerab products as soon as they're discovered, usually by the companies themselves o freelance security researchers. The firms distribute patches so users can fortify perimeters. Most attackers wait for these announcements and then build explo the vulnerable spots, hoping to catch companies and computer owners nappin defenders patch their systems quickly. But most tarry, leaving themselves def fast and sophisticated foes.

But there is no warning of Zero Day attacks. They target vulnerabilities only a have discovered - holes unknown even to software architects. The Zero Day a secretly penetrate a system. They can dominate it undetected. Zero Day explo stealth bombers of the Internet, and they turn traditional network defense on i

## IT COMES QUIETLY

Security experts can't say how many Zero Day exploits are circulating, but so rare. A successful attack offers a precious glimpse into the digital undergroun defenders got just such a peek behind enemy lines a little more than a year ag

In early 2003, an Air Force computer technician monitoring a Web server, at a Air Force won't name, noticed strange activity on the machine. Someone had server with a new user account and several aberrant files. The technician was notice the irregularities, and he was so startled that he alerted the Computer E Response Team, an electronic SWAT team stationed at Lackland Air Force B CERT computer forensics experts scrambled. Checking the machine's log, the been connecting to a restricted nonmilitary network. Typically, those include casinos and pornographic Web sites.

But investigators found no corresponding inbound connection a digital attacke used to gain entry. How could that be? If someone had hacked the system, the get in? The absence of an inbound connection could indicate an inside job: an employee manipulating the system. But that theory fell apart when, a few day investigators discovered other Air Force machines around the world connectin same restricted site. This was no insider. It was a never-before-seen vulnerabi Day had arrived.

From the perspective of Maj. Gen. David Bryan, who is in charge of defendin Department computer networks, this was a first strike. The phantom intruder w files from across the Air Force network. At the time, the U.S. military was ge the invasion of Iraq. An air attack on Baghdad would comprise the first wave. running loose in the Air Force network was especially unwelcome.

Bryan weighed two choices. He could block the intruder by restricting his onl his Internet protocol address. But the intruder could switch identities. And blc wouldn't reveal the vulnerability the hacker was exploiting. He'd simply use a address and the same vulnerability to re-enter.

The second option: Bryan could wait. The Air Force Office of Special Investi been called in and had begun monitoring the hack as a criminal matter. Don F unit's chief computer investigator, hoped he could observe activity on the infe machines to find the hole. Bryan gave Forrester a week, and a cat-and-mouse ensued. Bryan wondered how much leeway to give the investigators. Was it b contain the intruder or give him some room, maybe by putting out tantalizing what he was after? The days dragged on, but Forrester was no closer to plugg The vulnerability remained invisible.

Forrester made a final plea. Let us hook up a decoy, he proposed, a machine l victims, but one that hadn't yet been compromised. The decoy was rigged witl equipment. This time, when the intruder went after the vulnerability, Forreste it. Bryan acquiesced and gave the investigators 24 hours. But after that, he wc Internet address.

## OUT OF TIME

Keeping a network exposed to attack is like withholding treatment from a sicl order to study a virus. Network defenses mirror human immune systems. A Z exploit "is a microbe or a pathogen the body has never been exposed to," says Hofmeyr, the founder and chief scientist of Sana Security, an Internet security San Mateo, Calif.

Healthy networks, like healthy people, can fight off viruses. But coping requi and networks have none to Zero Day exploits. Early warning systems, sensors firewalls are impotent. The system has to be infected before the exploit can be makes a Zero Day exploit "any vendor's worst nightmare," says Mary Ann Da chief security officer at Oracle Corp., one of the biggest software providers to government. And such exploits are on the rise, she warns.

The time between a vulnerability announcement and the first attempt to explo to shrink. Six months passed, from June 2002 to January 2003, between Micro announcement of a weakness in its server software and the attack by the Slam that exploited it, knocking phones and automated banking machines off-line. year, it took just 26 days for a hacker to release the Blaster worm after word c about weaknesses in numerous products, including Microsoft's most popular operating systems. At the time, Blaster was the fastest spreading worm in hist hundreds of thousands of computers in a few days. Later last year, an exploit a week after the announcement of a vulnerability in a component common to two dozen software programs.

It's hard enough to get thousands, perhaps millions of users to patch a well-pu

But when the window of opportunity closes in a few days, every attack is like

## THE BATTLE BEGINS

More than a week after the 2003 Zero Day attack, the Air Force had containe in its own networks, protecting the other military services. The intruder did n hitting only unclassified systems. But his rifling through files looked like rec and Bryan feared the intruder could launch attacks from inside the network. F decoy sat untouched. If the hacker took the bait, revealing his secret, the Air permanently block him, instead of playing a dangerous waiting game.

The clock ticked down. Forrester's 24 hours nearly were up when his quarry f enabling the Air Force to gather priceless intelligence. The hacker had exploit site program called Internet Information Services 5.0, made by Microsoft. Mi products are everywhere on Defense Department networks. And, Bryan notes products contain hundreds of vulnerabilities.

An Air Force security technician called a counterpart at Microsoft headquarte the company into full alert. Technicians worked around-the-clock for three da the vulnerability and develop a patch. "Microsoft took it very well," Forrester that military officials "were very impressed" with the prompt response. Micro mounted a defense. A broad base of private sector customers uses the IIS soft too, could be under attack and not know it. And they were.

On March 17, 2003, Microsoft warned its customers that the previously undis vulnerability had let hackers take control of corporate Web servers. Microsoft Zero Day vulnerability with its highest "critical" rating and warned that the h hackers "run code of [the] attacker's choice" on an infected machine. An Inter company in Atlanta reported that the exploit already was circulating on the In Hackers now could arm themselves. Security experts braced for a global onsl

Further research showed the vulnerability was more severe than first thought. were affected. But the root weakness resided in file systems in the core of the 2000 operating system for personal computers. Headlines announced that Mi flagship product was under attack. Zero Day had come quietly, but now, it ha attention.

Yet there was no digital Pearl Harbor. In June, e-mail spammers used the vul send large amounts of junk mail through Microsoft's Hotmail service, but this nuisance. High-profile and ferocious worms such as Blaster and SoBig - whic Blaster as the fastest spreading worm in history - also were grabbing headline experts refer to that one "horrible week" in August as the worst for worm atta one appeared to have fully exploited the Zero Day hole the Air Force discove

Ironically, a military service suffered the worst damage. On August 20, the N that a worm called Welchia had infected 100,000 computers on the Navy Mar Intranet by targeting the Zero Day hole. About three-quarters of the Navy's gl was disabled, officials reported. Bryan's staff had issued a departmentwide al warning to patch systems. But Welchia found the Zero Day hole before the N

## NEW DAY DAWNS

Navy systems were knocked off-line. But for all the hubbub, the damage fron Day attack worldwide was minimal. It was focused. It was mitigated. Agencie corporations weren't brought to their knees. But to think that means the attack have been worse - or that it's not a sign of things to come - would be folly, wa watchers, who are accustomed to being labeled histrionic doomsayers.

Howard Schmidt served as second-in-command of federal cybersecurity at th House from 2001 until April 2003. He and his boss, Richard Clarke - who als government's counterterrorism coordinator - were called "Cassandras of the o for proclaiming Zero Day was near, Schmidt says. But today, their concern ap justified. The time between vulnerability and exploit dwindles. Worm attacks time high. And attackers are aiming their creations at several publicized vulne once. If hackers combined their techniques, built a fast-spreading worm arme more Zero Day exploits, the world might witness the big attack Schmidt and c predicted.

Before he left government, Schmidt warned, "Cybersecurity cannot now be re second-tier issue." The Homeland Security Department is responsible for safe nation's networks, but it has been criticized for not according the effort suffici and for making it the responsibility of low-level officials. The department did to repeated requests for comment for this story.

The government increasingly is seen to be complacent about cyber war. The I Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census gave federal agencies a D in cor security in 2003, up from an F in 2002. Agencies cannot undertake new proje paying better attention to security. The Office of Management and Budget no detailed business cases, including security plans, before it will seek money fo project.

Across government, security policies are inconsistent. Some agencies apply p quickly. Some don't. Bryan's Defense Department team responded to its Zero militaristic precision. But most agencies - and corporations, for that matter - ta hearted approach to defending their networks, ceding the high ground to hack meantime, as attackers sharpen their skills, Zero Day draws near.