

February 13, 2006

THE JOURNAL REPORT: TECHNOLOGY

Anatomy of a Threat

Two days after Christmas, hackers launched a potentially crippling attack. Here's how one security firm kept its clients safe.

By **RIVA RICHMOND**

February 13, 2006

The first volley was modest, but it set alarm bells ringing for **VeriSign** Inc.'s security mavens.

During the quiet post-holiday evening of Dec. 27, an anonymous message appeared on an email list where techies share information about vulnerabilities in computer security. The note claimed that hackers had discovered -- and were exploiting -- a previously unknown hole in **Microsoft** Corp.'s Windows operating system.

This type of situation, known as a "Zero Day" attack, is rare and perilous: Usually, by the time security holes are revealed publicly, Microsoft is aware of them and has a solution ready. In a Zero Day attack, millions of computer users are left exposed while the software giant rushes to fix the problem.

THE JOURNAL REPORT


1

See the complete [Technology report](#)².

Even worse, in this case the hole was in a commonly used portion of Windows' graphics program -- making it much tougher for users to avoid attacks.

For security firms like VeriSign, the message sparked more than a week of scrambling. Experts in high-tech war rooms around the country rushed to gather information about the threat and come up with effective protection for their corporate and government clients, keeping them safe until Microsoft could fix the Windows flaw.


A Close Watch

The incident shows the increasingly important role that security firms like VeriSign and **Symantec** Corp. play in corporate defense. From central command rooms, they monitor their clients' networks and trawl cyberspace for new threats, leaping into action whenever danger presents itself.

These hired guns are taking on a bigger role because hackers' methods and motives are changing. No longer interested in spreading viruses to get lots of attention, many hackers are becoming more sophisticated, stealthy and bent on material gain. They're finding low-key ways to invade computer networks to steal information or take over the machines and use them to send out spam, or advance other scams.

"The nature of attacks has changed dramatically," says Ken Dunham, director of the rapid-response team at iDefense, the VeriSign unit that monitors the hacker underground and analyzes security threats. "In the last few years, we've gone from code for fun to code for cash."

DOW JONES REPRINTS

 This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: www.djreprints.com.

- [See a sample reprint in PDF format.](#)
- [Order a reprint of this article now.](#)

The shift is stretching network operators' resources and expertise -- and increasingly they're calling on outsiders to help them out.

VeriSign, of Mountain View, Calif., runs six security-operations centers on four continents. In these war rooms, experts monitor firewalls, intrusion-detection software and other security systems for about 800 organizations, including U.S. government agencies and 18 of the world's top 20 financial-services firms.

The job is "a lot like panning for gold," says Ken Silva, VeriSign's chief security officer. Data "keeps going through cascades of filters....Our software mines it down to the things we should look at."

When team members find something, they alert clients to the problem and, if authorized, reprogram clients' firewalls to foil attacks. Its experts are tasked to respond to trouble 24 hours a day, 365 days a year.

That included two days after Christmas, when the anonymous message popped up on BugTraq, an email list run by a unit of Symantec. The message pointed to an apparently blank Web site laced with malicious software, and any computer that visited it -- even one fully protected with up-to-date security patches and antivirus software -- would be vulnerable.

VeriSign's team first tried to substantiate the anonymous poster's claim. And, in fact, when they visited the Web site it launched a malicious program that crashed their test computers.



Triage began. Researchers purposely infected lab computers to capture the malicious code, then started dissecting it to figure out how it used the flaw in Windows, and how it affected different versions of the operating system. This information would be vital for assessing the severity and scope of the problem.

"It's kind of like 'M.A.S.H.," Mr. Dunham says. "You bring it in and try to identify what's going on."

The attackers were using an error involving Windows Meta File, or WMF, images, such as pictures with the common ".jpg" tag. When Windows opened one of these bad images, attackers could slip malicious software onto a victim's PC undetected. Their goal: to steal data or take full control of the unsuspecting user's PC and use it to carry out all kinds of mischief, such as sending out spam.

As VeriSign's iDefense team started trawling the Internet, it found hackers exploiting the flaw using a number of other Web sites. Whenever users visited the sites, their computers would process the images on the page, causing the attack program to run, exploiting the flaw and taking control of the machine.

In some cases, the Web sites placed software on users' machines that generated pop-up sales pitches, including an ad for a dodgy antispymware program. Another attack caused infected machines to spew spam that promoted shares in a thinly traded Chinese pharmaceutical company.

High Alert

It would be easy enough to have clients steer away from these infectious Web sites. But it quickly became apparent the threat was even broader. Hackers could also insert malicious WMF files in email, instant messages and other forms of electronic traffic. Open a note containing an infected picture, for instance, and your computer could be invaded.

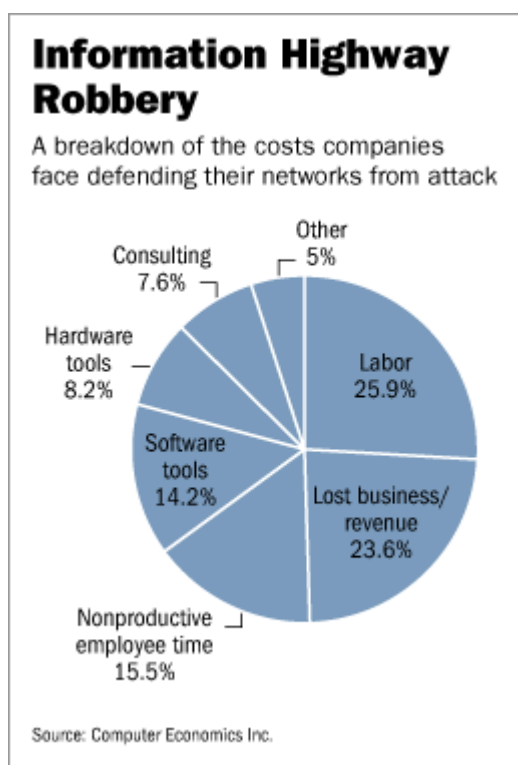
Things quickly got even more complicated, thanks to the Metasploit Project. This online forum, created

by prominent security expert H D Moore, is designed to help researchers and testers improve computer security by giving them tools to generate malicious programs. But hackers also have free entry and could use the tools to create new attacks.

On the night of the 27th, the site made a WMF exploit available. IDefense raised its risk rating to high from medium, and sent an alert to customers as well as VeriSign's lead security-operations center in Providence, R.I. The crew there would coordinate the effort to protect VeriSign's clients.

VeriSign's peers were also gearing up to tackle the threat. For instance, before the night was over, Symantec alerted subscribers to the company's DeepSight intelligence service about the emerging threat. By the next morning, a Wednesday, Symantec's security-services unit had detected a handful of contaminated PCs on the networks of its 500 clients.

Because the flaw existed in many software applications and there was no available patch from Microsoft, "most computers were naked to this exploit," says Grant Geyer, Symantec's vice president for managed security services. Worse, most client "companies were working on skeleton crews at the time" because of the holidays.



Mr. Moore of Metasploit says his work did much more good than harm. Attack programs provided by Metasploit helped defenders of corporate networks understand the risks they faced and security-software makers create more effective blocking tools, he says. He adds he hasn't seen an example of a malicious attack that cribbed from his programs. "All we're doing is shedding light on the vulnerability and [possible] permutations of the attack," he says.

State of Emergency

On Wednesday morning, things were buzzing at VeriSign's Providence center, where entry requires a badge and handprint scan. Rows of terminals face a large screen lit up with a world map specked with VeriSign facilities, as well as tables and charts tracking attack activity. A phone with a direct line to the Department of Homeland Security stands ready should a major incident threaten to disrupt the Internet; VeriSign operates two of the 13 mammoth servers world-wide that keep the Net running.

Joe Pepin, an engineer at the center, was alerted to iDefense's warnings at 6:30 a.m. He quickly began digging into the details of the software flaw and the attacks. Then he set to work with colleagues to create code that would let certain security-software programs recognize, and defend against, WMF attacks.

The first batch of code was ready that afternoon. But clients who didn't use the requisite software would have to try stopgap measures while they waited for help from their software providers.

Adding to the Black List

Symantec, which has security-operations centers in England, Germany, Australia and Alexandria, Va., was taking similar steps. Its response team began rolling out new code for the company's antivirus, intrusion-detection and intrusion-prevention products, and tools for ridding PCs of infections. The services group made sure that the new software -- as well as protections from other software makers --

were active in clients' security systems. It also created a "black list" of computer systems that were launching attacks.

Back at VeriSign, over the next week engineers, using information on new attacks from iDefense, would create 15 or 20 more batches of defensive code as the WMF attacks multiplied. Across the Web, hundreds of malicious Web sites appeared that used the attacks, followed quickly by email viruses and "bot" programs, which invade computers and link them up, often using their combined power to launch even bigger attacks.

But while the threats were multiplying, few of the attacks actually targeted VeriSign's customers -- until later in the week. "We didn't really see [any attacks on clients] until Friday evening," Mr. Pepin says. Attackers, it seemed, "were waiting for people to go home for the weekend." There was a rush of attacks that night and again on Sunday -- New Year's Day -- and Monday, a holiday for many companies. But VeriSign says none of its customers reported WMF-related infections.

VeriSign "engineers had to log in or come in from home," Mr. Pepin says. "I rang in the New Year by writing a report for a client" about ways to block email-based attacks, Mr. Dunham says.

At Symantec, the attacks peaked on Jan. 4, when the company's security-services group found and helped clean up about 100 infections.

The flurry of hacking ceased almost as quickly as it started. On Thursday, more than a week after the initial outbreak, Microsoft issued its fervently awaited patch, and network operators moved quickly to apply it. A large window of opportunity closed to a crack -- and VeriSign's engineers got their holiday.

Write to Riva Richmond at riva.richmond@dowjones.com³

URL for this article:

<http://online.wsj.com/article/SB113926056151566412.html>

Hyperlinks in this Article:

(1) http://online.wsj.com/page/2_1210.html

(2) http://online.wsj.com/page/2_1210.html

(3) <mailto:riva.richmond@dowjones.com>

Copyright 2006 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.