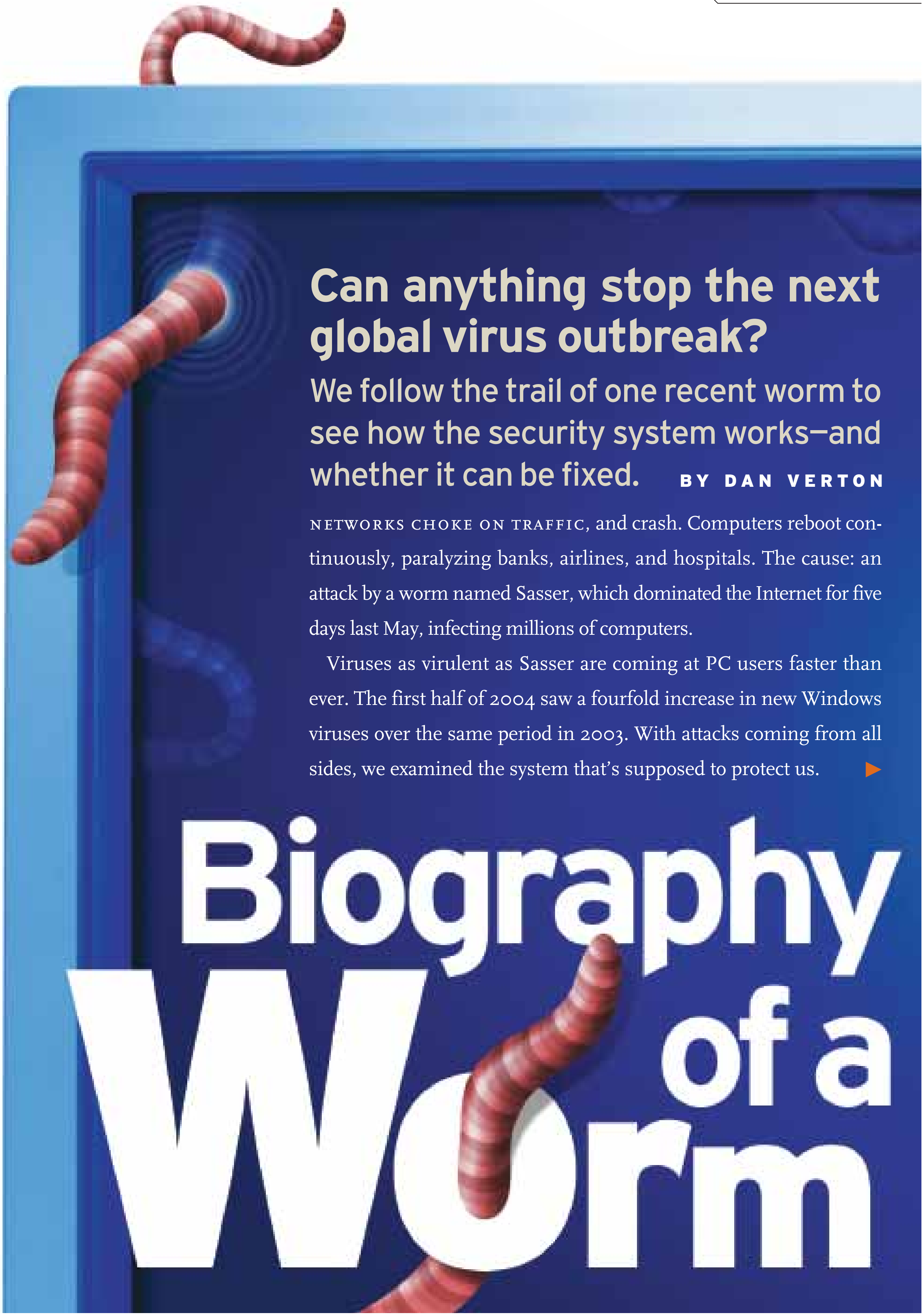


Biography of a Worm

Can anything stop the next global virus outbreak?

We follow the trail of one recent worm to see how the security system works—and whether it can be fixed.

BY DAN VERTON

NETWORKS CHOKE ON TRAFFIC, and crash. Computers reboot continuously, paralyzing banks, airlines, and hospitals. The cause: an attack by a worm named Sasser, which dominated the Internet for five days last May, infecting millions of computers.

Viruses as virulent as Sasser are coming at PC users faster than ever. The first half of 2004 saw a fourfold increase in new Windows viruses over the same period in 2003. With attacks coming from all sides, we examined the system that's supposed to protect us. ▶

PHOTO-ILLUSTRATION BY DIEGO AGUIRRE

BUG BUSTER Yuji Ukai of EEye Digital Security hunts for Windows vulnerabilities.

> **'It's just one line of code.... I don't know why Microsoft took so long to fix [it].'**
>
> –YUJI UKAI, SENIOR SOFTWARE ENGINEER, EEYE DIGITAL SECURITY

Who created Sasser? The short answer is a malicious hacker. But Sasser is also the by-product of the very system that's supposed to protect computer users. The hole Sasser wriggles through was discovered by an employee at a California security firm. And in releasing a patch for the hole, Microsoft supplied hackers worldwide with all the technical data they needed to exploit it. In short, you have to wonder whether this cure is worse than the disease.

To answer that question—and to examine what's right and what's wrong with the patch system—we followed Sasser's trail.

» Aliso Viejo, California, October 8, 2003.

Yuji Ukai is paid to find new ways to infiltrate your PC. Long after normal working hours at EEye Digital Security, where Ukai works on "vulnerability management" software (which large companies use to protect their computer networks from hack attacks), he's still in front of his office workstation.

He should be home, but instead he has opted to have a little fun. And in Ukai's world, "fun" means searching like a bloodhound for security flaws in the millions of lines of software code that power the most widely used operating system in the world.

EEye's products try to anticipate where hackers will strike next and to throw a blockade in their path. Its customers expect EEye to protect their computers even when there's no official fix for a problem. As a result, researchers at businesses like EEye constantly dig into Windows, looking for weaknesses that nobody else knows about.

The company's record speaks for itself: During the past 30 days, Ukai and his colleagues have discreetly notified Microsoft about six new Windows vulnerabilities they've discovered. Ukai found one of them, an unused command in a part of Windows called the Workstation Service.

Something tells him that other parts of the system have this same vulnerability. So tonight he's digging through DLL files, looking for the flaw. He starts out by checking other *services*—programs running various portions of the Windows operating system—that are turned on by default.

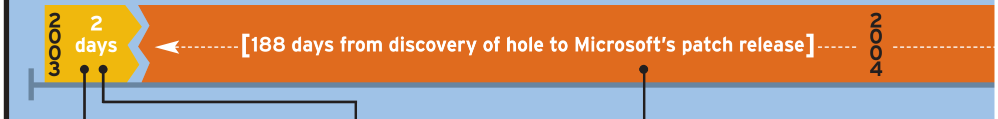
Almost immediately he finds another hole. And this one is inside the Big Kahuna: the Local Security Authority Subsystem Service. LSASS controls all aspects of security for the local Windows machine. He can get it to shut down, so Windows doesn't

PHOTOGRAPH: ANDREW BRANDT

TIMELINE

Tracking the Sasser Worm

» MORE THAN SIX MONTHS passed before Microsoft released a patch for the LSASS vulnerability. But it took only 18 days for the Sasser worm to appear, and less than a week for it to affect up to a million PCs. Meanwhile, the lead suspect has yet to go to trial.


2003
2 days
[188 days from discovery of hole to Microsoft's patch release]
2004

October 8
Yuji Ukai of EEye Digital Security discovers a Windows vulnerability in a file named LSASRV.DLL.

October 9
EEye reports the bug to Microsoft.

Winter-Spring
Microsoft develops and tests a patch for LSASS and 13 related vulnerabilities.

have any protection for a short period of time; he can also get LSASS to run a program of his choosing, thereby turning Windows' "security guard" into an insider that's working for him—one that can take control of Windows 2000 and Windows XP PCs. Hackers could do the same thing if they knew about the security flaw and were skilled enough to take advantage of it.

Ukai informs his boss that he's discovered a surprisingly easy method of controlling LSASS. Within hours, executives at EEye are on the phone to Microsoft. A significant portion of the world's computers have a major security hole. Fortunately, only EEye and Microsoft (as far as they're aware) know about it. Now, Microsoft must fix the problem before anyone else finds out.

The service EEye provides protects its customers, but it also creates two classes of Windows users: Those who are protected from newly discovered vulnerabilities (EEye's customers), and the rest of us, who must wait (sometimes months) for a patch and who remain ignorant of looming potential problems with our PCs.

» Redmond, Washington, October 8, 2003. At the Microsoft Security Response Center (MSRC), an ordinary-looking office space in the heart of the software giant's campus, the team's ten top members are scrambling around like emergency-room physicians to triage a wounded Windows.

The triage team first analyzes the report and reproduces the problem, says Kevin Kean, director of the MSRC. Next, they bring in the Secure Windows Initiative (SWI) group—the SWAT team for Windows security bugs—programmers and product managers, who create a fix. Once they have a good idea of how to patch the bug, the MSRC goes through a lengthy, in-depth test rollout "to make sure we have a quality fix," says Kean.

The LSASS case quickly grows into a mammoth undertaking. In less than a week, the ten analysts bring aboard hundreds of programmers, product managers, and bug testers.

PCs probed, per hour, by Sasser at its launch: about 200,000.

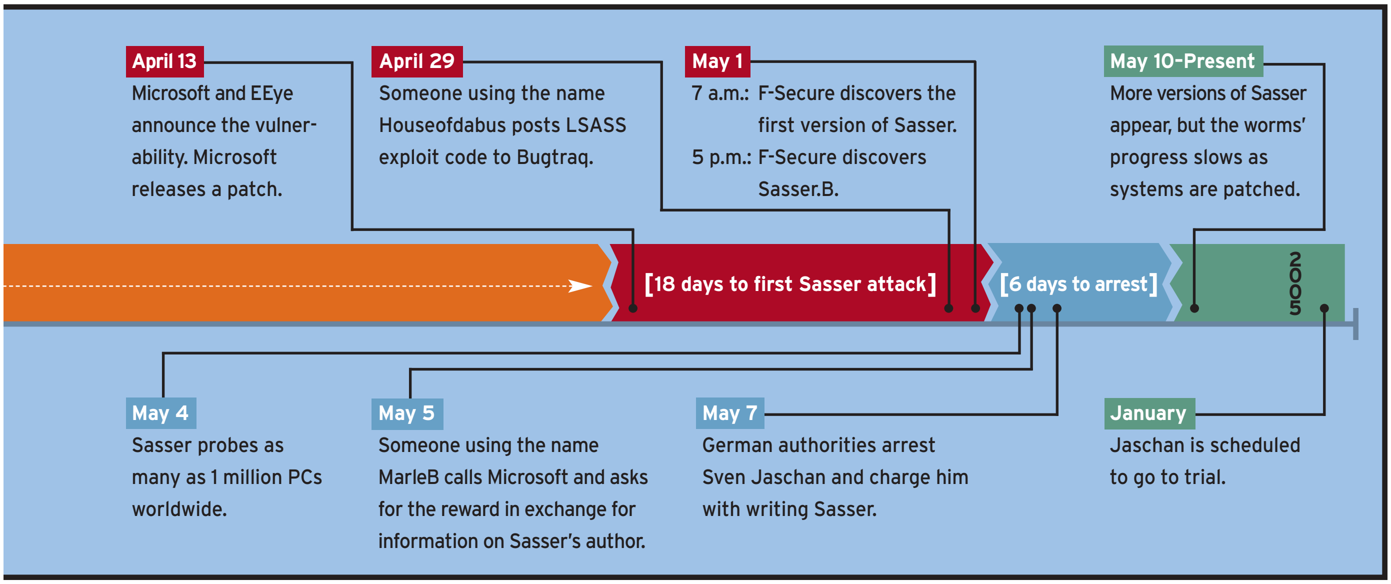
SOURCE: SYMANTEC

Despite the potential for catastrophe, Kean and Stephen Toulouse, the company's security program manager, breathe somewhat easier because EEye abides by the software industry's gentlemen's agreement known as *responsible disclosure*. Under these unofficial guidelines, the discoverer of a vulnerability gives the affected software company adequate time to work out a solution before the discoverer announces technical details to the world.

Responsible disclosure temporarily protects the public, at least in theory. Had EEye immediately posted these details online, Kean's team would have faced the nightmare of trying to fix a security hole at the same time as hackers were launching new viruses or worms. But keeping the details quiet can create a false sense of security, too. While Microsoft works on the patch, a criminal hacker might discover and covertly exploit the hole.

Kean says that most security researchers now refrain from posting details until after the patch comes out—a practice that used to be quite rare. As a result, Microsoft can focus on producing patches that don't cause additional problems. But that process requires testing—lots and lots of testing, in this case.

» Redmond, April 13, 2004. It's been more than six months since Ukai's discovery. Microsoft releases its patch, along with details of the LSASS problem, in an advisory labeled MS04-011. By waiting so long, Microsoft has violated a responsible disclosure guideline: Security companies generally agree that patches should appear within 30 days of when a ▶



April 13 Microsoft and EEye announce the vulnerability. Microsoft releases a patch.

April 29 Someone using the name Houseofdabus posts LSASS exploit code to Bugtraq.

May 1 7 a.m.: F-Secure discovers the first version of Sasser.
5 p.m.: F-Secure discovers Sasser.B.

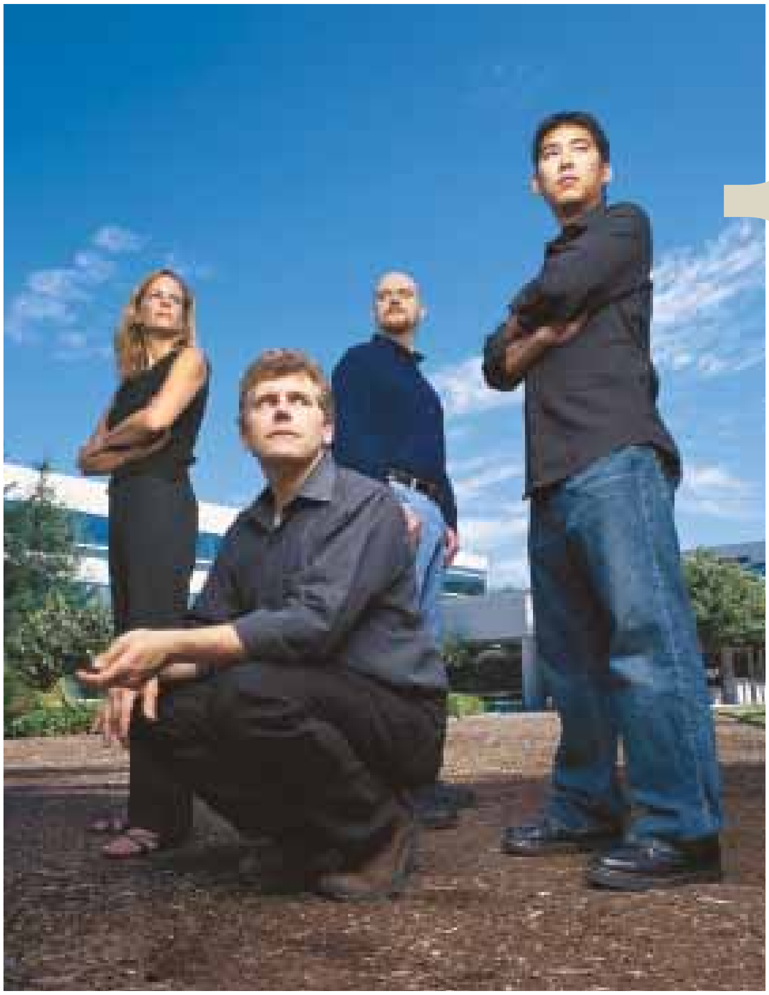
May 10-Present More versions of Sasser appear, but the worms' progress slows as systems are patched.

May 4 Sasser probes as many as 1 million PCs worldwide.

May 5 Someone using the name MarleB calls Microsoft and asks for the reward in exchange for information on Sasser's author.

May 7 German authorities arrest Sven Jaschan and charge him with writing Sasser.

January Jaschan is scheduled to go to trial.



WINDOWS BUG STOMPERS: The Microsoft Security Response Center's core members include (from left) Amy Carroll, Kevin Kean, Stephen Toulouse, and Richie Lai.

PHOTOGRAPH: RICK DAHMS

> **'[Microsoft aims to strike a] balance between timeliness and quality. We don't want to take risks that would ever cause people to distrust a patch.'**
>
> —KEVIN KEAN, MSRC DIRECTOR

bug is discovered. Kean explains that the patch fixes not just the bug Ukai found in LSASS, but 13 related vulnerabilities as well.

Windows users and IT professionals must install the patch quickly, lest they leave their networks open to ransacking.

The technical report, which system administrators use to evaluate the safety of applying the patch to their computers, also provides the technical data a highly skilled hacker needs to reverse-engineer the patch and write programs to attack unpatched PCs.

» **Russia, April 29, 2004.** Just 16 days later, at 3 p.m. local time, a Russian hacker known as Houseofdabus releases a proof-of-concept exploit—a program that shows how to take control of an unpatched PC—for the LSASS vulnerability.

The code that Houseofdabus writes is professional-quality work. The author claims to have tested the exploit against ten different Russian- and English-language versions of Windows XP and Windows 2000. A note embedded in it states, "This is provided as proof-of-concept code only for educational purposes and testing by authorized individuals with permission to do so." Nobody believes it will be used only by authorized individuals. For virus writers, who tend to be less skilled than exploit writers, this code is like candy.

The motivations of Houseofdabus are unclear, but virus expert Sarah Gordon, who has interviewed dozens of virus writers, says that most exploit coders see delays in applying patches as signs of laziness on the part of PC users and companies. They believe that the presence of their exploits online spurs a faster reaction to security holes.

Back in Redmond, Kean receives word about the Houseofdabus code, and puts the MSRC into "watchful normalcy" mode, a state of alert in which analysts monitor the Internet for signs that someone is trying to use the exploit code.

» **Helsinki, Finland, May 1, 2004.** At 7:02 a.m. local time, analysts at Helsinki-based antivirus firm F-Secure learn that a new worm exploiting the LSASS vulnerability is in the wild. F-Secure dispatches a bulletin about the worm to other antivirus researchers, and names the worm Sasser.

Sasser spreads fast, causing vulnerable computers to crash or reboot without warning. It doesn't inflict deliberate damage on infected systems, but infected PCs bog down as the worm floods the local network, attempting to replicate.

When news of Sasser reaches Microsoft, engineers begin studying the worm on a test-bed PC, to learn how it spreads. Meanwhile, Kean gathers the product teams that need to be involved, as well as people from Microsoft's communications wing, who will run the public and customer outreach efforts.

"It becomes a 24-by-7 operation," Kean says. "We set up a number of war rooms and establish rotating shifts."

About 10 hours later, a second variant of Sasser, Sasser.B, ▶

has already popped up on the radar screen of F-Secure. Sasser.B is sufficiently different that antivirus companies have to rerelease their antivirus software updates to detect and remove it.

Redmond, May 2, 2004. By Sunday, within 24 hours of Sasser's appearance, Microsoft decides to launch a broad outreach campaign that will last the entire week, including conducting a Webcast, posting information on the company's Web site, creating retail flyers and content for PC makers and key partners, and even paying Google to ensure that anyone who searches for information about the worm will see an ad that points to Microsoft.com for the patch and other downloads.

Despite all of these efforts, Microsoft is struggling to contain Sasser. Reports of the worm's impact fly in: Operations have been disrupted at companies like Goldman Sachs and British Airways. Computers in half of Taiwan's post offices have been infected. Sasser plagues PCs at government agencies in Hong Kong and on oil platforms off the coast of Mexico.

The magnitude of the worm's disruption is staggering: 5000 computer systems and associated X-ray equipment at a hospital in Lund, Sweden, stop responding; 1200 PCs at the European Commission headquarters in Brussels cannot get online; and Sun Trust bank and American Express in the United States lose Internet connectivity entirely for several hours.

PCs infected by Sasser through September 2004: 700,000 to 1 million.

SOURCES: AKAMAI AND MICROSOFT

By late Sunday evening, almost 1.5 million people have downloaded a free tool from Microsoft that kills Sasser. But Sasser is far from finished.

Waffensen, Germany, May 3, 2004. In this village of just 900 people, located about 21 miles from the city of Bremen in northwestern Germany, Sven Jaschan, an 18-year-old high school student, has allegedly spent the past three months writing and revising a series of Internet worms that he calls Skynet, but that antivirus software companies call Netsky. Variants of this earlier worm—one of the most prolific on the Internet—infect and reinfect tens of thousands of computer systems every month. But Netsky's goal isn't to wreak havoc on innocent bystanders: It's a weapon in a war against two other worms—Bagle and Mydoom—that turn infected machines into a spam distribution network. Netsky takes over those infected machines and deletes the spam-sending worms. ▶

PATCH DELAYS

How Long Is Too Long?

SOME SECURITY EXPERTS say software companies are taking too long to create security patches, leaving computers unprotected for months.

In the case of the LSASS vulnerability, EEye senior software engineer Yuji Ukai is baffled by the amount of time that it took Microsoft to fix one line of code. "LSASS was not a complex fix, so it was incomprehensible to me that they took 188 days to supply a patch," he says. "It's an unwritten rule that you give vendors 30 days to fix such a problem and 60 days if the problem is complex."

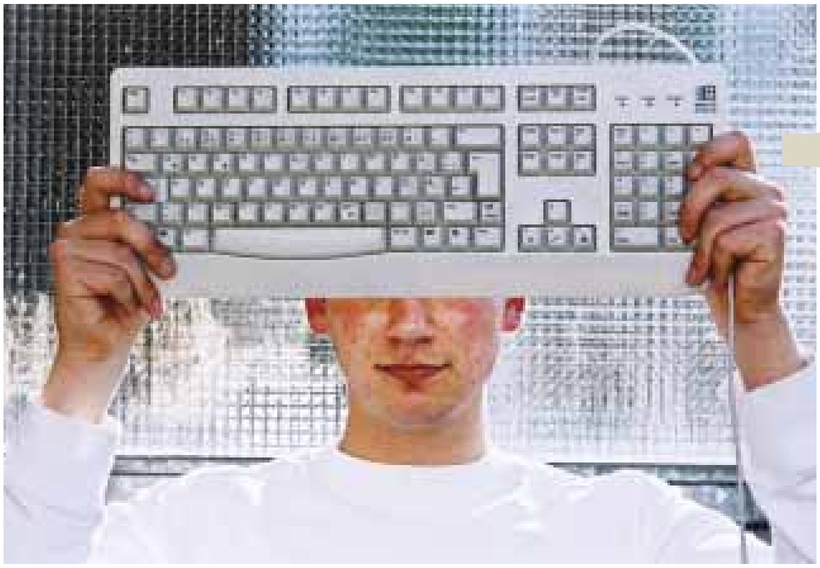
Rob Shively, CEO of PivX Solutions, a company that develops vulnerability and patch management software, agrees. If PivX has provided a company with enough proof of a vulnerability, PivX expects the vendor to patch that hole within a month, he says. If a patch is not available immediately, the vendor at fault should post a workaround (usually involving disabling the vulnerable feature in the program), "so users are not left in the lurch," he says.

In Microsoft's defense, Kevin Kean, director of the Microsoft Security Response Center, and Stephen Toulouse, Microsoft's security program manager, say that every hole or patch presents unique challenges. In the case of LSASS, 13 other vulnerabilities had to be fixed, explains Toulouse. Microsoft must balance timeliness and quality, says Kean. "We don't want to take risks that would cause people to distrust the patch."

But a security patch that takes more than six months to produce—even if it is well-tested and trustworthy when it arrives—is unacceptable, say some business users. Tom Kellerman, senior data risk management specialist at the World Bank, says, "We need patches before the underground finds exploits."

On the flip side, PC users have a lot of responsibility in this process, too, Kellerman adds. Users must install a patch within 24 hours of its release, he believes. When someone discovers a vulnerability, "hackers smell blood in the water, backdooring thousands of networks as [users] ponder when to patch."

MacDonnell Ulsch, managing director of Janus Risk Management, says that if customers are ever to get software that's secure straight out of the box, they must demand change. But for now, he adds, no one seems to be demanding it in an organized way.



LORD OF THE WORMS: Student Sven Jaschan, 18, allegedly wrote Netsky and Sasser.

'[Sven Jaschan] is a freak and very intelligent.'

–HELMUT TRENTMANN, PUBLIC PROSECUTOR IN GERMANY.

Today—a little over two months since the release of the first Netsky worm—Jaschan allegedly releases the 29th version of the worm, Netsky.AC, on his school network. Like previous versions, this variant contains a hidden message, but in this particular message, the author claims responsibility for writing Sasser.

"Hey, av firms, do you know that we have programmed the sasser virus?!?. Yeah thats true! Why do you have named it sasser? A Tip: Compare the FTP-Server code with the one from Skynet.V!!! LooL! We are the Skynet..."

>> Helsinki, May 4, 2004.

On Tuesday morning, antivirus companies are trying to verify the claims made in the hidden Netsky.AC message. Virus analysts at F-Secure dissect Sasser and Netsky, and produce a detailed flow chart of the worms' routines and subroutines.

This graphical depiction enables them to compare the code and the style of its author. "The same guy who wrote Netsky wrote Sasser," says Mikko Hypponen, antivirus research director at F-Secure, pointing to the graphic.

Antivirus companies and Microsoft estimate that each of the four versions of Sasser has infected anywhere from half a million computers to many millions of them. Each infection causes Windows XP and 2000 PCs, without warning, to begin a 60-second, unstoppable countdown to reboot. When office workers returned to work Monday morning, their unpatched PCs set off a tsunami of worm attacks that has yet to subside, and that infects PCs faster than any previously known worm.

>> Waffensen, May 5, 2004.

As the world's news media catches up with the Sasser story, the FBI joins in the hunt for Sasser's author. According to his own account, published in the German magazine *Stern*, Jaschan writes to one of his friends, known only as MarleB, declaring that he is getting out of worm writing; Jaschan plans to destroy his hard drive.

Six months earlier, Microsoft had caused quite a stir throughout the virus- and worm-writing world by establishing a $5 million fund that the company would use to reward informants for tips that led to the arrest and conviction of anyone responsible for an outbreak of malicious code.

Later that day, MarleB and another of the young man's friends from school call Microsoft's German headquarters to find out whether Microsoft will pay them the $250,000 bounty if they identify the author of the Sasser worm.

The call is passed along to Hemanshu Nigam, Microsoft's corporate attorney, who manages the antivirus Reward Program. "We informed the persons who were coming forward that, yes, we would gladly pay the reward," Nigam says.

But before the informants can get their money, Nigam explains, they must provide data that Microsoft can "technically analyze" to determine the truthfulness of their claims. MarleB sends along the source code to a version of Sasser. No one has revealed how MarleB got it.

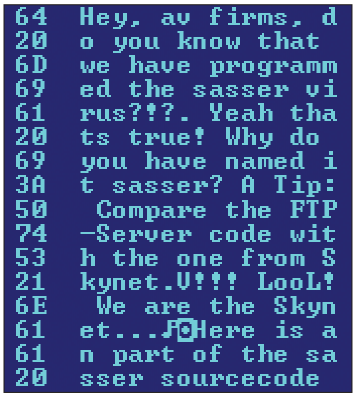
"Our security engineers took the information, analyzed it, and concluded that there was evidence that suggested the [informants] did know what they were talking about," Nigam says.

Microsoft now strongly suspects that it has its man, Sven Jaschan. This will be the first time in the history of the Reward Program that a tip from an informant actually leads to an arrest.

>> Seattle, May 7, 2004.

As soon as he receives confirmation about Sasser from his engineers, Nigam calls in federal investigators. An FBI task force based in Seattle immediately contacts police in the German state of Lower Saxony. Later that day, German law enforcement agents raid the cottage where 18-year-old Sven Jaschan lives with his parents, and confiscate Jaschan's computer. In his interrogation, Jaschan allegedly confesses everything about his role in creating Sasser, Net- ▶

PHOTOGRAPH: PETER THOMAN/STERN/PICTURE PRESS



```
64  Hey, av firms, d
20  o you know that
6D  we have programm
69  ed the sasser vi
61  rus?!?. Yeah tha
20  ts true! Why do
69  you have named i
3A  t sasser? A Tip:
50   Compare the FTP
74  -Server code wit
53  h the one from S
21  kynet.V!!! LooL!
6E   We are the Skyn
61  et...♪◙Here is a
61  n part of the sa
20  sser sourcecode
```

NETSKY'S AUTHOR claimed he wrote Sasser, in a note buried in Netsky.AC.

sky, and their variants.

Only 2 hours after his arrest, while Jaschan is still in police custody, a fifth version of Sasser appears online. Some security experts suspect that other hackers may be spreading Sasser, or that Jaschan may have offered a false confession. German authorities, for the moment, remain confident they have the culprit. Jaschan probably unleashed Sasser.E only minutes before authorities arrived at his house, German officials say.

>> Hannover, Germany, June 2004.

Despite Jaschan's confession, a trial is required under German law. Helmut Trentmann, the public prosecutor in Lower Saxony, gets the Jaschan case, which should go to trial in the state's capital, Hannover, sometime in January 2005.

Trentmann describes Jaschan as a young man who spends his free time working on his computer. The defendant is "a freak and very intelligent," he says. Based on evidence from computer experts and Microsoft, Trentmann is convinced that Jaschan authored and spread the Sasser worm, and that he acted with malicious intent. "In several steps, he put [Sasser] on the Internet and these steps he made alone," Trentmann says. "And he informed his friends about what he was doing. He was proud."

But Jaschan's malice has yet to be proved, Trentmann acknowledges. "I think his ambition was to get better [at programming] ," says Trentmann. "It was a kind of competition. But in the days before he was discovered, he became gripped by fear. He had heard about the FBI investigation. And it became too big for him."

As for Jaschen himself, though his legal status remains unclear, he may get the chance to put his skills to better use: A German firewall firm wants to recruit him as a programmer.

>> Hannover, September 2004.

As *PC World* goes to press, Trentmann is questioning five informants, four of whom are Jaschan's schoolmates. Trentmann and other investigators consider it likely that some of the informants may have assisted Jaschan in spreading the Sasser worm across the Internet.

Meanwhile, at least two new Sasser variants have appeared, indicating that accomplices of Jaschan may still be hard at work. And on August 23, Sasser.G, which at press time was the most recent variant discovered, was circulating on the Internet. Earlier versions of Sasser continue to infect unpatched machines every day. And Jaschan's mysterious spam-friendly rivals who produce the Bagle and MyDoom worms are still at it as well, releasing a new virus every few days.

All of the parties involved in this case say that their actions help others. EEye and Ukai's discovery of the LSASS hole helped the company's customers, who would have been at risk if a malicious hacker had found the vulnerability first. Microsoft's release of the patch enabled customers to avoid the problem.

Houseofdabus stated that the exploit was created only for educational purposes. Jaschan, too, claims that he was providing a service to the Internet at large. Although Sasser's primary effect was to spread as fast as possible, Netsky, on the other hand, attacked computers infected with the Bagle and MyDoom viruses (collectively known as spam zombies), preventing those PCs from sending spam to the rest of us.

So if everyone is looking out for our interests, why do we keep getting hit by ever-worsening viruses and worms that corrupt our data, gum up our networks, and crash our computers?

In practice, the patch system doesn't protect all of us—it protects those who patch quickly. According to Gerhard Eschelbeck, CEO of the security firm Qualys, only half of all PC users apply patches within three weeks of when they appear. That leaves the other half open to worms that might never have been created if the patch hadn't been released at all.

Cost of damage due to the Sasser worm: $979 million.

SOURCE: TRUSECURE

Clearly we can't simply scrap the current patch system. Malicious hackers will always be on the lookout for vulnerabilities in software, even without unwitting aid from Microsoft. Such hackers, working undetected, might do far more serious damage—all computer users would be vulnerable to data and identity theft, and businesses would be open to espionage.

The ultimate solution is to produce software that's secure from the get-go. Until then, improving the patch system must be the top priority for everyone involved. Users, however, have only one real option right now: Patch early and often. ■

Dan Verton is a senior writer for Computerworld. PC World *Senior Associate Editor Andrew Brandt contributed to this article.*

MORE ONLINE

Sasser News Updates

>> FOR NEWS DEVELOPMENTS about Sasser, Sven Jaschan's trial, and other topics in this story that broke after this issue went to press, head to our Web site at find.pcworld.com/44432.