SECURITY NOW!

Transcript of Episode #1

As the worm turns: The first Internet worms of 2005

Description: How a never-disclosed Windows vulnerability was quickly reverse-engineered from the patches to fix it and turned into more than 12 potent and damaging Internet worms in three days. What does this mean for the future of Internet security?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-001.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-001-lq.mp3

Leo Laporte: Hi, this is Leo Laporte, and I'd like to introduce a brand-new podcast to the TWiT lineup, Security Now! with Steve Gibson. This is Episode 1 for August 18, 2005. You all know Steve Gibson. He, of course, appears on TWiT regularly, This Week in Tech. We've known him for a long time. He's been a regular on the Screensavers and Call for Help. And, you know, he's well-known to computer users everywhere for his products. He's very well known to consumers for SpinRite, which was the inspiration for Norton Disk Doctor and still runs rings around it. It is the ultimate hard-drive diagnostic recovery and file-saving tool. It's really a remarkable tool that everybody should have a copy of from GRC.com. But he's also been a very active consumer advocate, working really hard to help folks with their security. He first came to my attention with the Click of Death, which was - that was the Zip drive Iomega...

Steve Gibson: Right.

Leo: ...hassle. And was it you that kind of talked Iomega into admitting that there was a problem?

Steve: Actually, I think it was our show. It was the Screensavers show that...

Leo: It came out of the Screensavers. Wow.

Steve: Yeah, because they - we had them on the phone, and it was David something, I can't remember his name now, who said there is...

Leo: Oh, that's right.

Steve: There is a problem. And it was great because we cornered him into saying that...

Leo: On the air, yes.

Steve: ...on the air, that if anyone had this problem, they would replace - Iomega would replace their drives.

Leo: I forgot about that.

Steve: And I made a WAV file of that and put it on my site. Say, hey, you heard it from the guy, from Iomega themselves. They're going to replace your drive if you've got the Click of Death. And people were like, woohoo, you know, and they were emailing this WAV file to Iomega, saying, hey, this is what you said, I want a new drive.

Leo: It worked.

Steve: It was great.

Leo: It worked. I'm also going to mention, of course, the fact that you were the first to discover spyware, coin the term spyware," wrote the very first anti-spyware program, and...

Steve: Yeah, found some on my own machine.

Leo: Yeah.

Steve: And then, of course, Dale Haag was the guy who publicized it. He actually sort of overpublicized it. He talked about the Aureate spyware, and he said it was doing all kinds of other things. And that's what OptOut - I wrote OptOut, you know, in a few days, in order to remove that.

Leo: The very first anti-spyware tool.

Steve: Yup.

Leo: And ShieldsUP! has up to now, what, 30 million...

Steve: 39.

Leo: Almost 40 million systems tested. I've just used it last night. And then finally, of course, Steve's continually coming out and really been very good at analyzing security threats, particularly in Windows, and publicizing these threats, things like the problems with Plug and Play. And he wrote the great program, UnPlug n' Pray - UnPlug and Play - and DCOMbobulator to fix the DCOM flaw. So he's been very good about calling Microsoft to task and, in fact, was probably the one sole voice in the wilderness against raw sockets...

Steve: Boy, was I.

Leo: ...and even took a lot of heat for that. And Microsoft pooh-poohed it, and others said, oh, Steve Gibson is, you know, just being hysterical. And then, lo and behold, some years later, Microsoft just a few months ago secretly, without much fanfare, turned off raw sockets in Windows, finally admitting there indeed is a huge problem with raw sockets.

Steve: And, you know, the one other thing, too, is LeakTest. That is still the number one most downloaded freeware we have.

Leo: What does LeakTest do?

Steve: LeakTest was the thing I did years ago because none of the personal firewalls were checking to see whether the program was actually the program you had permitted.

Leo: Ah.

Steve: So it prevented programs masquerading as Internet Explorer.

Leo: And that's still the number one download.

Steve: Yeah.

Leo: Interesting.

Steve: Even though it's dumb.

Leo: And ladies and gentlemen, despite all this, he still uses Windows. I don't know what's wrong with you, Steve.

Steve: Everybody else does, so that's where I - I am in the middle of where the problem is.

Leo: So, Steve Gibson, this is going to be fun. We'll do this every week and talk about what's going on in security. And what you really have a knack for, and I've observed this now working with you for years, is taking what is really obscure, difficult-to-understand security information, understanding it because, you know, you get it, you're brilliant, and then making it accessible for us. And I hope that's what you'll do each week on this show.

Steve: I look forward to it.

Leo: Yeah. So let's talk a little bit about Zotob, this virus that has been sweeping the world, particularly media companies.

Steve: Yeah, see, it's interesting that it hit them. Basically the problem is, one week ago, on the 9th, I think it was, Microsoft did their standard second-Tuesday-of-the-month announcement of vulnerabilities. Here are the things that we now have patches for. The thing that has really brought people up short is that, within three days of announcing it, the hackers, the malicious hackers of the world had analyzed the patch, figured out what it was patching - although Microsoft really gave no information about that - and had figured out, based on what the patch was, this is the vulnerability that Microsoft was fixing, and then engineered a worm, an Internet worm to go after Windows 2000 machines, based on this vulnerability that was never really disclosed. Only the fix for it was disclosed.

Leo: That's the fastest turnaround ever, yes?

Steve: Yes. Normally it's been, like, a month and a half. When, like, Sasser, the vulnerability from late April of 2004, that was a vulnerability called LSASS. It is a service running in Windows. And then the Sasser worm was created from that, but it took about six weeks.

Leo: Why? Is it that they're getting smarter, or this is just an easy one to exploit? How come so quick?

Steve: Actually, I think it's probably desperation. There hasn't been anything for about, what, 14 months, 15 months. And they were all still using this old LSASS vulnerability. So, you know, the idea is that all of the carrier technology, the bot technology, the worm technology, everything is, like, well developed now and poised to take advantage of anything that happens in Windows.

Leo: So they've got everything ready to go, they just need a hole.

Steve: Exactly. So as soon as they had some way to get control, remote control of a Windows machine, they just stuck that little bit of code into their existing infrastructure, and off they went.

Leo: What are these guys doing? Are they trying to put mail servers on my system? What is their goal?

Steve: Well, first of all, many of the news stories mischaracterized this as a virus because, you know, I guess just it's easy for them to say "virus" because that's just what they think of.

Leo: What is it?

Steve: But in fact what we're seeing are worms. And of course the difference between a worm and a virus is that a worm self-propagates, whereas a virus has traditionally been defined as the user has to do something to get themselves infected.

Leo: Usually opening an email attachment. So you don't have to open an attachment to get this one.

Steve: No. The ideal situation would be a Windows 2000 machine. And so we ought to mention that XP won't have this problem.

Leo: Is that because of the patch?

Steve: Actually, XP has the vulnerability, and the patch fixes this in XP, even the most recently patched Windows, you know, XP Service Pack 2 machine with all the security stuff. However, in XP, and further in Service Pack 1 and even further in Service Pack 2, other sort of related security enhancements, specifically anonymous log-on and admin log-on, are required. Whereas on Windows 2000, an anonymous connection to a Windows 2000 machine can infect it.

Leo: That's funny because I usually think of 2000 as being more secure than XP. In this case not.

Steve: Well, and of course that's certainly the case. And also in Service Pack 2 you would finally have XP's firewall running by default, and so that would block it.

Leo: So if you had a firewall of any kind, a router or a software firewall running, if you were running XP, you would not be vulnerable. So it's really only Windows 2000 machines that have not been patched, that are not behind a firewall, that are vulnerable.

Steve: True. And so as a consequence of that, most end-users were not affected. The other protection that an end-user might have, even if you had a Windows 2000 machine - which of course most end-users went from the last edition of 98, and they jumped over 2000 and went to XP.

Leo: Right, it's mostly business that has 2000.

Steve: Exactly.

Leo: Right.

Steve: But even if you were an end-user with 2000, no add-on firewall, no NAT router protecting you, with, like, a raw, broadband connection, where you'd, like, be "Okay, come get me," I mean, you know, like, first of all I'd be surprised if your machine was still on the 'Net anyway because, you know, it would just be attacked so quickly. But it turns out the exploit port is NetBIOS, the good old, I mean, it's what I created ShieldsUP! to warm people about five years ago.

Leo: File sharing.

Steve: Exactly. It's the NetBIOS ports 139 and 445. And, for example, my cable modem provider, Cox, they block those ports for me. So, for example, I have a 98 machine on my cable modem. And sometimes I'll bring my firewall down just to see what's going on. And if I scan it with my own shield web service, I see green spots. Everything is...

Leo: Protected, stealthed.

Steve: It's stealthed. Like those ports, 135 through 139 and 445 and a couple other, are being stealthed by Cox, my cable modem provider.

Leo: Interesting. In fact, more and more ISPs are doing that. They're providing, in effect, firewalls for their users.

Steve: Exactly, because they don't want their clients' machines to get infected by these things because typically it turns these machines into zombies that then obey remote-control instructions and, for example, are sending spam out.

Leo: So who got it?

Steve: Well, that's what's...

Leo: And how?

Steve: That's what's really interesting is that CNN did a big story on this on Sunday night. ABC, "The Financial Times," "The New York Times," General Electric, UPS, and even Caterpillar, you know, major corporations got it. And the way they got it is they're not the typical end-user. Apparently about 50 percent of corporate desktops are still using Windows 2000 because it works. I mean, I'm using Windows 2000. I'm really not yet even an XP user because XP doesn't really have anything that I want or need. So about half of the corporate desktops are using Windows 2000. Now, of course...

Leo: But they're still behind firewalls.

Steve: Exactly. They're absolutely behind a corporate firewall. But they're not running individual machine firewalls.

Leo: Oh, so a corporate firewall - okay. I'm going to let you follow the train of thought here. Plus, and I might add, they don't update these things as regularly as end-users might.

Steve: Exactly. Well, for example, the patch was available from Microsoft the prior Tuesday before infection Tuesday, which was...

Leo: Does Windows 2000 do automatic updates in the same way that Windows XP does?

Steve: It can, although it doesn't force it on you sort of in the same way.

Leo: Most corporate computers probably don't have it turned on.

Steve: They probably don't have - exactly. They don't have automatic update turned on. And it might not be able to function through the corporate firewall anyway because, I mean, certainly corporations have had problems like this in the past. I mean, they got zapped by Sasser, and they got zapped by Blaster. So, you know, the IT guys in corporate world, they're going to have a firewall super locked down. But what happened was some telecommuters got their laptops infected over the weekend, when this thing began propagating at the end of last week, and then they brought the laptops into work, plugged them into the network, and got infected from within.

Leo: Ah. So the road warriors, out for the weekend, who didn't have protection, brought it in and then infected the network because there's no internal firewalling. They brought it into the safe space.

Steve: Brought it inside, exactly. So Windows 2000 machines didn't have local personal firewalls. They were all depending upon the corporate barricade on, you know, at the Internet interface. But they got infected massively from within.

Leo: Do you think there's a lesson learned here? There's behavioral changes that need to be made?

Steve: Well, I think so. I mean, it's certainly the case that, if corporations wanted to stay with 2000, and they had firewalls per machine, then they wouldn't have got - I mean, you know, CNN and "The New York Times" were seriously hurt by this. You know, they got really zapped. So had those machines had local personal firewalls, this wouldn't have been a problem. There are companies who, for example, ZoneAlarm has the technology, and Sygate has the technology. In fact, Symantec just yesterday announced they're buying - Symantec is buying Sygate in order to acquire their corporate lockdown technology, whatever they call it, where they would run a Sygate personal firewall, soon to be renamed the, you know, Norton Internet Security for Corporations 2006...

Leo: Or something.

Steve: ...or something, who knows, and they'd be running that on every single one of these machines. And then the idea is that they would have central policy control over what the individual machines' firewalls would be able to do.

Leo: Right.

Steve: I mean, and no one wants to do it because it just mucks up your computer. But it's clearly necessary.

Leo: Either that or ban laptops.

Steve: Well, exactly. Now, for example, I have a friend who has a corporate laptop. He works for 3M. And the only way that laptop can get on the Internet is by using a VPN tunnel into 3M that then allows the 3M network to go out.

Leo: So you're never on the 'Net on your own connection. You're always on 3M's connection.

Steve: Exactly, I mean, and he hates it because, you know, it's a slower connection than anything he just could get his own - he could get that laptop on the 'Net. But 3M's IT guys have, like, you know, screwed this thing down so tight that nothing is able to run at all.

Leo: And now you know why they do that.

Steve: And now it's real clear that that was a good policy on their side.

Leo: Does this herald anything new, or is this just business as usual, just yet another network worm and some people who had one little hole that they weren't keeping an eye on?

Steve: I would say this was another network worm. It's probably significant that it was back on Windows 2000 and not on XP because, you know, most of the world is moving to XP. Microsoft's security provisions in XP, even though they didn't deal with this vulnerability, it would have prevented a worm from being written to an XP machine both because of internal policies and because Microsoft finally is running a firewall by default on Service Pack 2 of XP. So...

Leo: We talked about this the last time you were on Call for Help. Hackers are going to have - because finally XP is getting so buttoned down, hackers are going to start to have to look for new ways and new operating systems to attack.

Steve: It's funny, too, because I've thought about that several times. Since you and I did that Call for Help show, there have been several announcements of vulnerabilities in third-party software, backup software specifically, where exactly this is going on, is external, remote, take-your-computer-over-if-you're-using-this-backup-software kind of stuff.

Leo: So more and more, do you think attacks will take those avenues?

Steve: I think so because I think Microsoft, I mean, it's taken Microsoft, God knows, you know, 15 years to button this stuff up. But they're finally, as a policy, they're showing some real improvements.

Leo: Steve Gibson, as usual, you did it again.

Steve: Always a pleasure, Leo.

Leo: That's it for this edition of Security Now! with Steve Gibson. Security Now! with Steve Gibson can be heard every Thursday, starting at midnight. You can download it for Friday or your weekend. You can listen on AOL Radio at AOLmusic.com or, of course, through our feed at feeds.feedburner.com/securitynow. And we thank AOL Radio for the bandwidth for this podcast. I'm Leo Laporte. See you next time on Security Now! with Steve Gibson.