SIM FILE

Subj: http://www.packet.com/
Date: 97-03-19 10:48:17 EST
From: simsong@vineyard.net (Simson L. Garfinkel)
Sender: owner-simsoft@vineyard.net
Reply-to: simsong@acm.org
To: simsoft@vineyard.net

Hard Pressed

Tech journalists are more interested in crises like the Explorer bug than the fundamental problems behind them

Ever wonder how the news really works behind the scenes? I got a powerful firsthand lesson on 3 March, when <http://www.wpi.edu/>Worcester Polytechnic student Paul Greene discovered that "serious flaw" in Microsoft's Internet Explorer. That's when I became the unwitting source of a sound bite that overshadowed the real news.

My first indication that something was up was an email from Gene Spafford, who has been my co-author and editor on three computer-security books. Gene subscribes to bugtraq@netspace.org, a "full-disclosure" mailing list about hot computer security holes. The subject line was "FYI - browser bug." The message pointed to Greene's <http://www.cybersnot.com/iebug.html>Cybersnot Web page.

As I read the message, my jaw dropped. "Cool," I thought. "I can run any program I want on anybody's computer who looks at my Web page with Internet Explorer." Sort of like ActiveX without the code-signing.

Five minutes later, my phone rang. It was Thomas Reardon, who works at Microsoft on IE. "I want you to know that this isn't an ActiveX problem," were the first words out of his mouth.

I told Reardon that I had read the Cybersnot message and didn't think that this IE problem was any more significant than the numerous security problems that have plagued Netscape's Java engine. After all, the <http://www.cs.princeton.edu/sip>Secure Internet Programming group at Princeton University had discovered a dozen or so ways of making Java Virtual Machines run arbitrary machine code. The only difference between their attacks and this one was that you needed to be fluent in Java bytecodes, x86 assembler language, and obscure type systems in order to exploit the Princeton attacks. For the Greene bug, all you needed to know was HTML.

But Reardon was worried. He said that his co-workers at Microsoft were certain that the press was going to burn them alive. And the bug was so simple - just two flipped bits in IE's registry entries. Internet Explorer has a list indicating whether files are safe or dangerous to open, Reardon explained to me. URL files and LNK files had been listed as safe, meaning it's OK for IE to open them without first asking the user's permission. They should have been listed as dangerous.

Next, my pager went off. My friend Beth Weise, cyberspace correspondent for the Associated Press, wanted me to call another reporter and fill him in. I tried to stress to the reporter that the real problem wasn't Internet Explorer - it's the fact that people use the Windows operating system, which has no built-in security. "What we really need is secure operating systems, but corporate America doesn't buy them," I said. But that didn't make for a good story.

The AP story must have gone out over the wire about 10 minutes after I hung up the phone, because I had just sat down to dinner when my phone rang again. This time it was CBS Radio News. They wanted to do an interview-to-tape right then! So I told the guy from CBS the same thing I had told George from the AP. The impact of this bug, I said, was that it acted as if somebody were messing with your computer while you "went out to lunch."

That "lunch" quote had wings of its own. Within the next 24 hours I was quoted on CNN, CNBC, National Public Radio, and in dozens of publications. The Seattle Times ran my quote. It was really weird, because the woman who wrote the story knows me, knows my home phone number, but she found it easier just to grab the quote from the AP than to call me up and get the story behind the sound bite.

This sort of quote reuse is actually typical for the nation's news services. I shouldn't be surprised. But I was upset that everybody focused on the immediate problem - a bug (oh no!) in Internet Explorer.

Nobody asked why today's computers are so brittle that a single bug could leave a Web surfer wide open to attack.

Nobody made the connection between this bug in Internet Explorer and ActiveX. Microsoft goes to great pains to make sure that security-critical bugs like this don't slip into its applications, and yet this one did. What about signed ActiveX components? They're sure to have security-critical bugs as well - especially since many of them will be written in C++. This is a problem that Java applets simply don't have, because they run within the restricted sandbox environment.

Nobody seems to be looking to the future. We're building a wired world, but all those wires are crossed. We've had a lot of warnings. Pretty soon, we're going to start having disasters. It's time we started looking harder at the threats.

==

This message (C) Simson L. Garfinkel. .

=

This message was sent to you by the simsoft mailing list.
Simsoft is a mailing list for exclusive use by Simson L. Garfinkel.
If you would like to be taken off the simsoft mailing list,
send the message "unsubscribe simsoft" to the address
"majordomo@vineyard.net".

————————— Headers —————————

From owner-simsoft@vineyard.net Wed Mar 19 10:47:59 1997
Return-Path: owner-simsoft@vineyard.net
Received: from vineyard.net (vineyard.net [204.17.195.100]) by emin37.mail.aol.com (8.6.12/8.6.12) with ESMTP id KAA28752; Wed, 19 Mar 1997 10:47:50 -0500
Received: (from root@localhost) by vineyard.net (8.8.5/8.7.3) id KAA04441 for simsoft-send; Wed, 19 Mar 1997 10:42:27 -0500 (EST)

```
Received: (from mail@localhost) by vineyard.net (8.8.5/8.7.3) id KAA04419 for <simsoft@vineyard.net>; Wed, 19 Mar 1997
10:42:26 -0500 (EST)
Received: from mac-slg.vineyard.net(204.17.195.43) by vineyard.net via smap/slg (V1.3)
    id sma004378; Wed Mar 19 10:42:02 1997
Message-Id: <v03101907af55b9a2c3e4@[204.17.195.43]>
Mime-Version: 1.0
Content-Type: text/plain; charset="us-ascii"
Date: Wed, 19 Mar 1997 10:41:43 -0500
To: simsoft@vineyard.net
From: "Simson L. Garfinkel" <simsong@vineyard.net>
Subject: http://www.packet.com/
Sender: owner-simsoft@vineyard.net
Precedence: bulk
Reply-To: simsong@acm.org
```