

Why hasn't Symantec addressed nastier Messenger spoofs

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-10/3499.html>

From: Jim Kutz (jimkutz@earthlink.net)

Date: 10/24/02

From: jimkutz@earthlink.net (Jim Kutz)

Date: 23 Oct 2002 20:36:10 -0700

The following was prevented from reaching Symantec's support message board. So as a show of submission to their censors or whatever, I'm posting these vulnerabilities publicly to get some answers after two months of silence from Symantec:

My question relates to the following:

Associated Press reported a warning by security engineer Gary Flynn at James Madison University, that

"hackers might... use the [Messenger] technique to persuade users to change their passwords or otherwise compromise security..."

-- http://www.usatoday.com/tech/news/2002-10-21-pop-up-spam_x.htm

AP says the new method of spamming pops up messages directly through Windows Messenger (not MSN Instant Messaging), even when the browser is closed.

The pop-ups resemble messages from an antivirus or a system administrator -- messages which could say, for example "Virus found in file CRUCIAL.DLL -- can only be deleted manually." Such a message can come through an 'always on' Internet connection at any time, and not be mentally associated with Internet.

Flynn says this might "one day" happen, but AP reports that the capability to broadcast such messages exists today in DirectAdvertiser, sold by Zoltan Kovacs through an outlet in Florida, which has already sold 200 copies.

The text messages broadcast by DirectAdvertiser aren't constrained to look like ads, and can emulate important system messages to catch the user's eye.

The files within DirectAdvertiser that control the pop-up's appearance are apparently unsecured and could be swapped out by a hacker. The

broadcast messages reportedly lack any identifying codes that could identify the purchaser of the sending software (or add them to a blocking list).

Although reporters have been all over Kovacs, there are no reports of any commitment to make DirectAdvertiser's messages distinctive (which would make them identifiable as ads). Kovacs doesn't see that as his company's problem, and AP quotes him as saying "If some people use it for bad things... it's their own problem."

Kovacs does not provide a current demo of DirectAdvertiser for testing, so anyone who wants to test it for abuse potential has to pay him \$699.

The AP article also states that "Users can disable Messenger through their operating system's control panel, although doing so could interfere with some anti-virus and other applications that send such messages."

Norton / Symantec has been silent on whether Norton Internet Security (with antivirus) requires that Messenger be left on in order to 'break over' other apps.

A system engineer at SBC Ameritech says they don't know whether their DSL firewall will stop these kinds of pop-ups. Various ISPs are playing dumb about whether or not their pop-up blockers prevent the spoofs -- but there've been sightings of the new pop-ups on most major ISPs and broadband systems. The pop-ups have apparently come FROM most ISPs and broadband systems.

A few [but not many] Internet providers say they use this type of messaging to send messages such as "system going down in 5 minutes", so they're not encouraging users to disable it. [The vast majority of ISPs don't bother notifying customers when they're going down, but some corporate and university intranets do, and so do a few gaming servers.

Obviously ISPs COULD filter such messages coming from outside, but one sysadmin (who asked not to be identified) said it may take awhile to assess the ramifications -- e.g. do stock alert services and such transmit urgent messages by this means -- or gateway for other ISPs that do. "I think we probably will filter it, to prevent denial-of-service spoofs such as "If you receive this message, contact your ISP at once", or "contact your firewall provider at once."

Given that denial of service attacks ARE probably not too far off, and given that antivirus / firewall companies could get behind on virus-related questions from customers as a result, it seems ill-advised for these companies and ISPs to tell their customers "No this isn't prevented by our firewalls and / or popup-blockers, but

here's what the deal is in case you get spoofed."

The logical place to trap spoofs would be in a personal firewall, but none of the major PC firewall providers have announced plans for such a feature, two months after the threat appeared. If a company DOES offer coverage on that, it should be able to grab some market share — because although the majority of personal firewall users aren't clueless enough to be spoofed, a majority have at least one family member who is.

My third question is, if Symantec does introduce a filter to warn or disable concerning these popups, will it also be able to 'let through' pop-ups from approved local apps or remote sites?

There's currently no mention of Windows Messenger whatsoever in Norton Internet Security Help, and nothing about this problem in the Symantec Knowledge Base. A PC user group we talked to is reporting "unknown vulnerability impact" on Symantec security products and certain other brands, because "If disabling the messages in Control Panel DOES prevent security alerts from displaying, the user may not know why their PC has halted, or how to un-halt it without disabling the security software. If they boot directly to Clean Mode in some versions of Windows to find out what's wrong, they can still use Internet to consult the mfr., but may not notice that their firewall and antivirus are down while doing so. Most users won't pay to ask the question by voice.

At least one firewall mfr. is already reporting a large surge in customer service queries, but isn't saying if these are related to virus alerts or firewall alerts they can't see or clear. This could lead to VAST customer annoyance, particularly if the security company is swamped with queries by then, and takes a long time to respond. Some PC users become alarmed when they see pop-ups and know their browser isn't on, thinking an unauthorized program has already defeated their security apps. They get even more alarmed when no such app shows on the taskbar, thinking their operating system is infected with a viral ad engine not listed in the virus dictionary.

"What's interesting about this", said a radio talk show guest "is that security software companies haven't explained the problem to users. Some news outlets alerted computerists, but a lot didn't."

Once again Microsoft has 'scored' for its partner companies, by providing yet another enabled-by-default method to shove ads onto people's desktops, and security be damned. And of course if you try to turn off the ads, something may break in your apps. What I'd like to see is a "Microsoft-backdoor-free" sticker on their competitors software, guaranteed not to need Windows features needing an endless stream of "critical updates" — after which your older, software may no longer work

comp.security.misc: Why hasn't Symantec addressed nastier Messenger spoofs

Please Cc: any response to jimkutz@earthlink.spamless.net

The above letter is in the public domain, and may be used by anyone seeking answers from ISPs or security software companies.

Thank you.

Jim Kutz

"Einstein didn't just discover the critical mass or the nuclear chain reaction. He also discovered that a critical mass of facts, in the right configuration, could cause a chain reaction that would change the world."

- *Next message:* : ["Re: Why hasn't Symantec addressed nastier Messenger spoofs"](#)
- *Previous message:* [North: "Want to do something on privacy protection"](#)
- *Reply:* [Walter Dnes: "Re: Why hasn't Symantec addressed nastier Messenger spoofs"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)