

CyberSoft White Papers

On Being the Target of an Email Worm

Dateline: late November, 2001.

A sad tale of woe.

About 8 years ago, UT (my place of employment...the University of Texas at Austin) set up an email service that allowed users to select their own mailbox name. This was the height of luxury back then. Up to that point, we'd been stuck with really clunky email addresses (things like peea890@utxvms.cc.utexas.edu, things having no relation to the "real" world). So, I jumped at the chance to grab "joanna" for myself. And, I've been using that address (joanna@mail.utexas.edu) as my primary email address since then. That's a long time. I liked it. It was simple. It was easy for others to remember. It served me well. Until the 24th of November.

That morning, the Saturday after Thanksgiving, I started getting messages from people (all of them strangers to me) asking why I'd sent them a blank email message (some complained of "odd" attachments). I had no idea what they were talking about. I hadn't sent any blank messages. My first thought was that someone had their email client configured incorrectly with my return email address. And, that (as if that wasn't enough of a problem!) their computer was infected with some sort of virus. I made sure my virus definitions were up-to-date and verified that there were no viruses (virii?) on my system.

Side note. A few times, in the past several years, new freshmen have shown up on campus and just started using my email address. The handouts for the mail service say something like "you can pick your own mailbox name" and some people seemed to think that meant all they had to do was configure their email client with an address and they were set. So, they'd set the return address to match mine and send out a few messages. Then, of course, the replies would come to me. It usually took a day or two to find the yay-hoo and explain that the name was already taken and that they had to actually sign up for the service. It would be a slight inconvenience. No big deal, though. When I got the first few reports of blank email messages with "suspect" attachments, I thought it was happening again.

I replied to the messages I received saying I hadn't sent them anything and asking if they'd send back the full headers of the first message so I could investigate the matter further. In the meantime, I sent a message to my email postmaster saying I thought my email address had been "hijacked" and asked for suggestions on what I should do. And, then I went off to enjoy my Saturday without really worrying too much about what was going on.

I got home about 9 o'clock that night to find another 60 messages in response to "my" messages. Many of the messages were from auto responders thanking me for my feedback (or interest or question or ...). This confirmed my suspicions that some sort of email virus was to blame since (to my mind, at any rate) that would indicate that something was "harvesting" cached web pages for email addresses. There were a couple of messages generated by antivirus software warning me that I had a virus. About half of the messages were from real people asking what I wanted or why I'd sent a blank message...things along that line. There were a couple of rather rude responses including one from some guy in San Antonio threatening to report me to campus police and the Attorney General for abusing campus facilities. There were also several replies in German and Italian. Huh? Thankfully, there were also a couple of replies to my request for full headers from the earlier messages. The first set of headers I got back indicated that the messages from "me" were actually originating from an AOL user in the UK. What? That didn't fit with my guess about someone here on campus mistakenly using my return address. And, as I thought about it I realized that since it was the middle of the academic semester, it was rather unlikely that the problem was originating from a new freshman who didn't understand how to set up an email account. Hmmm. One last message was from the postmaster at UT telling me I probably had a virus and offering nothing helpful. I replied, including the headers I'd received, and explained what I'd managed to find out to that point.

I started looking through the antivirus sites in hopes of finding specific information about a new email virus. I found a site that talked about an email worm called W32.Badtrans.B@mm. It mentioned (quite casually...and you only noticed it if you read the report very carefully) that the worm would modify the "From" header with a random return address. This struck me as a truly evil twist on the part of the person who'd authored the virus. That meant there wasn't any way to warn the person whose computer really was infected! I came up with a standard reply I could send to the folks sending me reports and replies. In the message I explained that I hadn't sent out any messages and that there was a new worm that modified the "From" header. I pointed them to the web page I'd found for information. I asked people to send back full headers of the first message they'd received from "me" if they knew how to do such a thing. Without even looking at the full headers, there was a glaring difference between messages I sent out and messages sent

out by the worm. My real messages always include my full name (Joanna L. Castillo) while the worm-induced messages only included my first name. Most people didn't reply to my message. Several helpfully returned headers, though. And, it was clear that messages from "me" were going out from several sites around the world. The first ones started in Europe but then there were messages going out from Mexico and then the US.

One of the other things this worm did was assign pseudo-random names to the attachments. One of those names included the phrase "You are Fat!" Using such an inflammatory name for the attachment was a surefire way to get some people to look at the file. Regardless of whether they looked at the file or not, lots of people who received it took offense at the name and, in turn, took that offense out on me...thinking I was attacking them without even knowing them. There were a couple of people who vehemently argued with me about whether or not my computer was infected. The guy from San Antonio insisted I somehow prove the message hadn't come from me. I told him there was no way I could prove it conclusively but that if he'd compare the headers from the first message to the headers from my real messages, he should see some significant differences. He never wrote back. I guessed that meant he was satisfied with my explanation. Then there was the guy in Japan who insisted that even though I didn't know I was sending out a virus, I was doing so. Twice I asked him to compare the headers and he (despite his claimed expertise) never would believe the infected message wasn't from me; not even after I pointed out that the worm was taking advantage of Windows vulnerabilities and that I was running non-Microsoft software on a Macintosh which was incapable of perpetuating this sort of worm! Another guy also insisted (in an extremely condescending and arrogant manner) that I didn't know what the hell I was talking about and that my machine was, in fact, infected. I pointed him to the web site again and offered to send him dozens of email headers that would prove otherwise. I ended my message to him asking if he was always this arrogant and condescending when he didn't know what he was talking about. He didn't reply. I took that to be a resounding "yes." Heh.

Anyway, I was still quite puzzled. By Sunday I'd received another 200 or so messages. I was terrified at the enormity of this virus. If this thing was just randomly picking email addresses and I was receiving hundreds of replies, I couldn't begin to imagine how horrible this would be come Monday morning when people started reporting to work. But, I was puzzled at the fact that the antivirus sites were still reporting this as a worm of "medium" threat or risk. I couldn't imagine how the sites could be so blasé. And, I was somewhat surprised that this didn't seem to be getting any media coverage...like earlier widespread threats. I spent several hours late Saturday night and early Sunday morning replying to people's messages. One of the things that really worried me about this was the number of replies I was getting from people saying things like:

What did you need? I tried opening the attachment in your email but couldn't. Please send the message again in another format.

These people clearly didn't understand anything about the latest email worm attacks that had taken place. They were all trying to open attachments arriving from complete strangers! I really couldn't believe it. I added a note to my standard reply imploring them to never open unsolicited attachments and to run to the nearest store, buy some antivirus software, and install it on their machines. (Of course, it turns out that this virus takes advantage of a bug in some Microsoft products that allows certain types of files found on a web page to be executed automatically. The email messages sent out by the worm were formatted in such a way that they took advantage of this bug and executed the attachments automatically on some users' machines.)

About noon on Sunday, I went to some friends' house for an afternoon of fun. I told them my story and they were appropriately horrified and sympathetic. I speculated on the number of responses I seemed to be getting and wondered if I wasn't being singled out in some way. It seemed so very unlikely, though. I mean...why me? And, who would do such a thing?

I got home around 8 or 9 Sunday evening to find about 250 new responses. By this time quite a few of the responses were automated responses from virus detection software packages informing me that my machine was infected. On the one hand, it was somewhat comforting to see that the antivirus community was responding so quickly and that users were updating their virus detection software as they should be. On the other hand, this twist of changing the "From" header was really screwing things up. Usually, this sort of automated reply might prove quite helpful. But, in this case, the folks whose systems were infected weren't getting the notices. I was. And, I didn't have the virus!

Sigh...

So, I just kept plugging away. I was up until the wee hours of Monday morning sorting through and replying to messages. I'd get 50 messages, reply to the ones I felt needed a reply (you know...warning people about the virus, telling them to check their systems, etc.), send the messages, check mail, and there'd be another 50 new messages. By this time, I'd sent 4 or 5 more messages to my email postmaster with more headers asking for help and insight. I didn't get any responses. I took this to mean that the system was overloaded with this problem and that they were working on some sort of solution. I worried about how

things would be when I got to work the next morning. I couldn't sleep. I'd doze for 30 minutes or so and then get up and do more sorting and replying. I don't imagine I got more than about 2 hours of sleep all night. About 4:00 AM on Monday morning, I went in search of more info on the antivirus sites. I found a page on the antivirus.com site that listed my email address (among 14 others) as being hard-coded into the worm. While seeing that was rather upsetting, it actually brought me some small amount of comfort. At last...real, hard proof. I sent messages to all the "strangers" who'd shown concern and asked to be kept informed on my investigation (as well as the guy from San Antonio, the one from Japan, and the condescending jerk) pointing out that my address had, indeed, been specifically singled out. That explained to some extent why I was getting so many messages and why the antivirus companies didn't seem to be all that concerned; they didn't know how many replies were being sent to the 15 addresses on the list.

I'd already begun wondering if I'd have to abandon my "perfect" email address. Once I saw that it was hard-coded into the worm, I knew I had virtually no choice in the matter. I knew that it would never truly die down. So, I headed into the office later that morning with a bit of a heavy heart.

By the time I was able to check email at the office (about 45 minutes after shutting down my computer at home), 381 (yes...381!) more responses had arrived. It was too much. I couldn't possibly warn all the people who didn't know better than to open an attachment from a stranger. Even if I dedicated myself full-time to the project of warning well-meaning (some not so well-meaning) strangers and never did another thing, there would be no way I could reply to all those people. It was overwhelming. I cried in frustration. How many hours had I lost over my holiday weekend to this mess? I called the postmaster and left a message...begging him to call me back. And, I tried to go about my job. I warned people I worked with most closely to use an alternate email address if they really needed to get in touch with me. Because there was little hope of finding "real" mail in that mess. The postmaster finally sent me a message saying my only choices were to try and ride out the storm or change my mailbox name...abandoning joanna@mail.utexas.edu for good. He warned that there would be no smooth transition...that legitimate mail would be lost along with the bad. I had no choice. I set up a new mailbox and asked him to kill the old one. He did that sometime around 1:00 that afternoon.

When I left for work on Monday morning (about 48 hours after the first message arrived), I'd received more than 2,500 messages in response to the worm. At the time the joanna address was killed, I was receiving 5 or 6 messages a minute. All told, I received almost 4,000 message in just over 2 days. By contrast, I usually get 20 or 30 messages a day. On "bad" days, I average 60 or 70.

Then...poof!...it was over. What a relief. Of course, it wasn't really over. And there was little sense of relief. I still had to notify people of my new email address. And, I still had to go through all the many web pages I maintain at work that contain my email address and change them to reflect the new email address. I know there's no hope of me notifying everyone who needs to be notified of the new address and that there will be people in the coming months who will send messages to me at the old address that'll never find their way to me. That makes me sad. The postmaster did set up an auto responder informing people that the address was the target of an email worm and that it no longer exists. Motivated people will be able to find my new email address if they go to the University's online directory. So, I really shouldn't lose much. Still.

On Tuesday evening (the 27th), I noticed that the folks at Symantec had upgraded the threat from mild to high. And, they'd written up a very comprehensive and thorough description of the worm. I wrote to the author of that document, told him who I was, and asked if he had any insights on what I should do...if there was any point in filing some sort of complaint with any legal authorities on the off-chance that the author would eventually be caught. He sent his sympathies, said it seemed likely the virus was written by someone in Russia, and said there was really very little I could do.

So...there you have it. A tale of woe in this age of wonder. Working in academia meant I was one of the first people to use the Internet. I've had at least a dozen different email addresses since the early 80s. I was a USENET junky before anyone in the "real" world had a clue about the Internet. I learned HTML and put up my very first web page about a project we had going on here at work in early 1995 (wow...almost seven years ago). I've been involved in the odd flame war now and again. But, I'm having a hard time remembering being this frustrated and hurt by anything to do with the 'Net. It'll never be the same place for me. I mean...why my address? Why those other 14 people? It just seems so cruel and pointless.

Every time I see my new email address I feel a bit of a jolt. It's just not me. Sigh...

A brief postscript...

I have to admit to being somewhat frustrated by the fact that the antivirus experts didn't try to contact me when they found my address hard-coded into the worm. If they'd done so immediately, it would've eased my mind so much earlier. I hope they modify their policies to do just that sort of thing, when possible, in the future. It took a lot of time and effort on my part to get that information. It would've been so easy to drop me a line and let me know what was going on.

Contact info: Joanna L. Castillo - jlc@mail.utexas.edu
URL: <http://www.pe.utexas.edu/~castillo/attack.html>
Last updated: Nov. 29, 2001

[Back](#)

[Home](#) | [Products](#) | [Support](#) | [Purchase Info](#) | [About Us](#) | [News](#) | [Contact](#)

Questions or comments about this website? Please contact the webmaster. 

© Copyright 2009 CyberSoft, Inc. All rights reserved.



This site certified 508 Compliant