

A New Worm Threatens to Sue You on Various Counts

Released by: Manish Katara

Web Site: <http://www.mwti.net>

Bagle worm aims to spread by threatening victims via imposter lawsuits!



Email: manish@mwti.net

Keywords: [New software release](#), [new product release](#), [antivirus](#), [content security](#), [antispam](#), [spyware detection](#)

Update Date: 3/9/2006 2:55:41 PM

Hits: 5

Description:

A new variant from the Bagle worm family named 'Bagle-DO' or 'Win32.Bagle.fr' aims to spread by threatening victims via imposter lawsuits!

Experts at MicroWorld Technologies have found various legal subjects lines in the message. Some of them read "We wait your response", "Pay your debts before we come to you", "Lawsuit against you" and alike. The content of the mail talks about legal action due to a varied set of financial and criminal offenses allegedly committed by the recipient or his company.

Users are threatened with choicest words to open an attachment named "lawsuit.exe", documents.exe or explanation.exe. Once you download and run the file it will install the worm into your computer. From that point, the worm gets down to business very fast by stealing mailing addresses to send mass mails and proliferating in networks via P2P methods.

The most interesting factor to notice here is the innovative psychological ploy employed to get the user to open the mail and download the attachment. A greeting card, sexual content or a fantastic utility were all tried and tested over the years. Now they are trying negative tactics like shock and scare. Here the recipient's reaction will be either of fear or of anger. In both cases the person's natural judgment and logical thinking takes a back seat, and the emotional impulse to see the what's in the lawsuit takes over. That's when virus writer wins hand down!

"Multiple ways of Social Engineering employed by virus writers are something we have been closely following at MicroWorld. As the theory of mass psychology goes, peripheral cues and mental shortcuts can be employed to trigger desired action from a targeted group. Same is happening here, in newer and smarter ways." analyzes Govind Rammurthy, CEO, MicroWorld Technologies. The recent FBI phishing mail employed a similar tactic to terrorize the victim to fall in line.

Another important aspect that emerges from this worm is the multi-tier strategy in relaying the worm. Once the Bagle Worm steals the email addresses from the victim's computer it resorts to the older methods like salacious content like Britney Spears sex photos.exe, Paris Hilton video.exe, Porno Screensaver.scr and more, in the next level of proliferation.

"This time the mail is coming from the mail id of your friend or a known person. Thus, there's a great chance of you opening the mail, as sending pornographic content is a hugely popular activity around the world, among friends and colleagues." explains Govind Rammurthy.

MicroWorld has been continuously updating their users about various modes of malware proliferation employed by virus writers, as they believe this war is as much about psychology one as it is about technology.

Contact information:

sales@mwti.net