

18 June 2009

By: Lucian Constantin, Web News Editor

## [Fake Outlook Re-Configuration Emails Spread New Zbot Variant](#)

*TheBat! users also targeted in similar campaign*



New Zbot distribution campaign targets Outlook and TheBat! users  
RITLABS and Microsoft (for TheBat! and Outlook logos)

Security researchers warn that a new version of Zbot is being propagated through Microsoft Outlook configuration-themed spam campaigns. Moreover, the malware distributors have extended their pool of potential victims by also targeting TheBat! users.

Cybercrooks are always on the lookout for new ways to trick users into installing their malicious programs or handing up their sensitive personal and financial information. Their creativity in this department seems to be never ending.

At the beginning of this month, the creators of the notorious Zbot computer Trojan came up with a [new theme](#) for their campaigns, which falsely instructed users that their Microsoft Outlook or Outlook Express email clients needed re-configuring.

One of these campaigns directed users to a phishing page and asked them to input their configuration details, including email username and password. Another one was distributing a .zip file attached to the messages and encouraged users to open it in order to configure their client. This archive actually contained a Zbot installer.

Despite the media attention that these campaigns got at the time, security researchers note that they were successful enough for the cybercrooks to keep making use of them. This doesn't normally happen with other attacks, as it is more profitable for malware distributors to switch themes once public awareness gets high.

Alex Eckelberry, CEO of Sunbelt Software, [announced](#) a few days ago that these attacks had mutated to target users of TheBat! email client too. "They've targeted TheBat! [⋮], but the bot seems to be a bit confused, mixing in TheBat! with Outlook and Outlook Express," he wrote on the company's blog.

The confusion referred to the fact that some e-mails that had subjects like "TheBat Setup Configuration," were asking users to re-configure Microsoft Outlook in the messages, and vice-versa. Regardless, an attachment called client\_update.zip was consistent with all e-mails.

Vanja Svajcer, principal virus researcher at Sophos, [warns](#) that a new such campaign was launched yesterday, this time spreading links to a malicious file. "Several URLs are used but the file name seems to consistently be Outlook\_update.exe," he notes. "Looking at the filename and the changes to the system when the file run in our automated analysis environment I would say this is a new Zbot variant," he concludes.