"Wire transfer canceled" Watch out for spammed-out malware attack

On April 30, 2012, Graham Cluley, a computer security industry veteran who writes for Sophos's award-winning *Naked Security* site has reported warned of the new malware attack reprinted below:

"If you've received an email in your inbox telling you that your wire transfer has been cancelled, take care - as it's the latest attempt by online criminals to infect the general public's Windows computers.

> Brits (as opposed to Americans) probably won't be as likely to be duped by the spammed-out messages which use the US spelling of "canceled" in the subject line, and claim to come from the Federal Reserve.

> The Wire transfer, recently sent from your bank account, was not processed by the FedWire.
> Transfer details attached to the letter.
> This service is provided to you by the Federal Reserve Board. Visit us on the web at website
> To report this message as spam, offensive, or if you feel you have received this in error, please send e-mail to email address including the entire contents and subject of the message. It will be reviewed by staff and acted upon appropriately

Attached to the emails is a file called PAYMENT RECEIPT 30-04-2013-GBK-75.zip which Sophos products detect as containing the Troj/Zbot-EVX Trojan horse, designed to hijack your computer and - potentially - plunder your finances and steal private information.

Of course, the danger is that unsuspecting computer users will open the malicious email attachment even if they haven't recently tried to wire some cash.

The social engineering trap used in this attack takes advantage of people's natural curiosity, which - in many cases - will drive them to investigate the file even if alarm bells should be ringing.

Up-to-date anti-virus software and software patches can help protect your computer, but the real lesson that internet users need to learn is to not be so trusting of unsolicited emails that arrive out of the blue in their inbox.“

(See http://nakedsecurity.sophos.com/2013/04/30/wire-transfer-canceled-malware-attack/)