

22 June 2009

By: Lucian Constantin, Web News Editor



Computer trojans
advertised as
Microsoft security
updates
Microsoft

[Microsoft Updates Spam Emails Spread Malware](#)

Fake Conficker removal tool and Outlook security update in circulation

Security researches from CA and Sophos warn of two malware distribution campaigns that try to push trojans as Microsoft security updates. One claims to offer a Conficker removal tool, while the other masquerades as an update for Microsoft Outlook and Outlook Express.

"Researchers at Microsoft have been working closely with Symantec, the creators of Norton antivirus, and have come up with a removal tool for the conflicker [sic.] virus," the malicious e-mails intercepted by CA read. "You are hereby immediately advised to download and run the removal tool from the link provided below to make sure you are not infected […]," they go on to advise.

The download link starts with windowsupdate.microsoft.com, but actually points to a .ru domain name. "The email comes from a certain Microsoft[dot]ssl[dot]com whose IP address is 38.100.66.185. This IP address originates from a server which is located in Texas and is not a Microsoft server," Rossano Ferraris, research engineer at CA Internet Security Business Unit, [notes](#).

Visiting the link prompts the download of a file called remtool_conf.exe, that, when run, displays a Symantec EULA and offers to start scanning the computer. However, instead of performing any malware scan, the application contacts another host from where it downloads winupdate.exe, identified by CA as DelfInject CX. The fake removal tool is being detected as FakeScan A.

"Although there has been a decrease in the number of fake Microsoft update emails, the current fake emails are more sophisticated and use a very high profile social engineering technique to lure and trap people," Mr. Ferraris warns.

Meanwhile, Julie Yeates, malware analyst at antivirus vendor Sophos, describes a similarly themed campaign that targets users of the Microsoft Outlook and Outlook Express email clients. "Microsoft has released an update for Microsoft Outlook / Outlook Express. This update is critical and provides you with the latest version of the Microsoft Outlook / Outlook Express and offers the highest levels of stability and security," the messages read.

The attached officexp-KB910721-FullFile-ENU.exe file is actually an installer for Troj/Spy-CU. "It does look plausible, the spelling and grammar are surprisingly correct, for malware authors, but, as ever, one should always be cautious concerning e-mail attachments," Ms. Yeates [warns](#). Windows users are advised to download security fixes through Automatic Updates or from Microsoft's download website directly.