

Trojan Piggybacks on Windows Updater

Researchers discover a Trojan that uses an integral part of Windows to download files onto infected systems.

At least one Trojan virus writer is now using an integral part of the Windows operating system - BITS (Background Intelligent Transfer Service) - to download files to already infected systems.

Windows Update uses BITS as an asynchronous download service to fetch patches, updates and other files - and, in this instance, malware.

Security researcher Frank Boldewin, along with Symantec's Elia Florio, discovered the technique the week of May 7 after analyzing a recent Trojan distributed via spam e-mail in Germany toward the end of March. According to Florio's May 10 [posting](#) on Symantec's site, Boldewin determined that the Trojan - which he detected as "Downloader" - was using BITS to bypass the firewall and download files without firewall inspection. As part of the operating system, BITS is trusted and gets passed through without having to go through the firewall.

According to Florio, more common methods used by malware to bypass firewalls include running a continuous thread that sends "Yes, accept" messages to the firewall window, which warns users about strange network connections; shutting down the firewall or killing its processes; injecting malicious code into Internet Explorer or other processes in the firewall's trusted applications list; and patching network drivers to disable firewall filtering.

This new technique doesn't constitute a significant new threat, as the Trojan doesn't evade anti-virus products and is only using BITS as a means of connection. Still, it's an interesting new development in that attackers are using a component of Windows itself, rather than having to write downloaders or updaters themselves, Oliver Friedrichs, director of Symantec Security Response, said in an interview.

"The main impact of this particular threat is the ability to evade outbound firewall filtering," Friedrichs said. "That's not a new concept, ... - but - it's another novel way malicious code can use outbound connections."

Symantec, based in Cupertino, Calif., observed this technique being discussed as a means of downloading files on Russian hacker boards at the end of 2006. This is one of the first times it's been seen in the wild, Friedrichs said, and it's something the company expects to see more of in the future.

A Microsoft spokesperson said the company is aware of public reports that BITS is being used by the Trojan, whose official name is TrojanDownloader:Win32/Jowspry, to bypass policy-based firewalls in order to install additional malware.

However, Microsoft, based in Redmond, Wash., says the bypass relies on TrojanDownloader:Win32/Jowspry already being present on the system - in other words, BITS isn't an attack vector for the initial infection.

"The bypass most commonly occurs after a successful social engineering attempt lures the user into inadvertently running TrojanDownloader:Win32/Jowspry, which then utilizes BITS to download additional malware," the spokesperson said in an e-mail exchange.

Microsoft recommends that any users who believe their systems have been affected by TrojanDownloader:Win32/Jowspry visit [Windows Live OneCare](#) to scan their systems, determine if they are infected and clean up all currently known variants of the Trojan.

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.