Malware piggybacks on Windows' Background Intelligent Transfer Service

By Matt Mondok

Published: 2007-05-11 · Archived: 2026-04-05 17:52:15 UTC

When Windows Update downloads patches to a PC, it relies on a service called the Background Intelligent Transfer Service, or BITS. In a nutshell, BITS asynchronously downloads updates from Microsoft's servers while attempting to use as little bandwidth as possible. Besides downloading updates, it is also used to transfer files within Microsoft's messaging products.

While the service is primarily used by Microsoft, it also exposes a COM application programming interface (API) for programmers, and according to Elia Florio of the Symantec Security Response Weblog, hackers have started to take advantage of the API.

> Why does malware use BITS for downloading files? For one simple reason: BITS service is part of the operating system, so it’s trusted and bypasses the local firewall while downloading files. Malwares need to bypass local firewalls, but usually the most common methods found in real samples are intrusive, require process injection or may raise suspicious alarms.

Florio states that the Trojan known as "Downloader" currently uses BITS to attack Windows PCs. The malware accesses BITS with the CoCreateInstance() method, and it downloads files to the local PC using the CreateJob() and AddFile() methods.

Though Symantec has known about the BITS exploit since it was first discussed on a Russian message board at the end of 2006, the company did not see the technique being used in the wild until March of this year. Right now, there's not much one can do to protect against the BITS attack except disable the service, but Symantec's Oliver Friedrichs claims that there is no need to worry about Windows Update being exploited. "There's no evidence to suspect that Windows Update can be compromised. If it has a weakness, someone would have found it by now."

Microsoft has yet to respond to the claims, but we should expect something to pop up on the Microsoft Security Response Center blog shortly.
