



TECHNICAL

BULLETIN

CONFIDENTIAL

SUBJECT:**TECHNICAL BULLETIN: 16-13****TRITON CONNECT 6.0 SERVICE PACK 5 INSTALLER MALWARE****DATE: OCTOBER 25, 2016**

Triton has determined that the installer in Triton Connect 6.0 SP5.zip was infected by malware sometime on or after July 1, 2016. If you downloaded and installed Service Pack 5 for Triton Connect 6.0 on or after July 1, it is possible that this could have affected you. Users should immediately delete all copies of this installer downloaded between July 1 and October 19, 2016.

If a user has already installed a version of Service Pack 5 after July 1, immediate countermeasures should be executed against malware infections. A user can determine if Service Pack 5 is installed by going to Help>About in Triton Connect and looking for Version: 6.0.33.

If you downloaded the Triton Connect SP5 installer from the Triton Partner site, you can check the file's MD5 hash by using the Windows utility certutil.

Ex: certutil -hashfile c:\Triton_Connect_6.0_SP5.zip MD5

MD5 hash of corrupted "Triton_Connect_6.0_SP5.zip": a2 72 af 04 25 79 e7 bc 52 1b a8 d9 c7 d6 d1 a3

MD5 hash of corrupted "Triton Connect 6.0.msi": b7 13 1f 10 fa 46 0f 30 66 ca 82 b4 fd 91 c3 9b

If you have Triton Connect SP5 installed and are unsure if your system is infected your IT support staff can run a packet capture for traffic destined for the IP address 5.39.218.204 coming from your Triton Connect server. If the results of the packet capture include communication to this remote IP then it has most likely been compromised.

We have removed the affected files from our site and we are working to provide our customers a more secure environment to download these and all other files. Please contact Triton Technical Support if you need a new copy of the installer.

Triton will provide further updates and information as it becomes available.

If you have questions regarding this Technical Bulletin, please contact Technical Support at 1-228-575-3100 option 4 or toll free in the U.S. / Canada 1-800-259-6672.