USWGO Virus Report

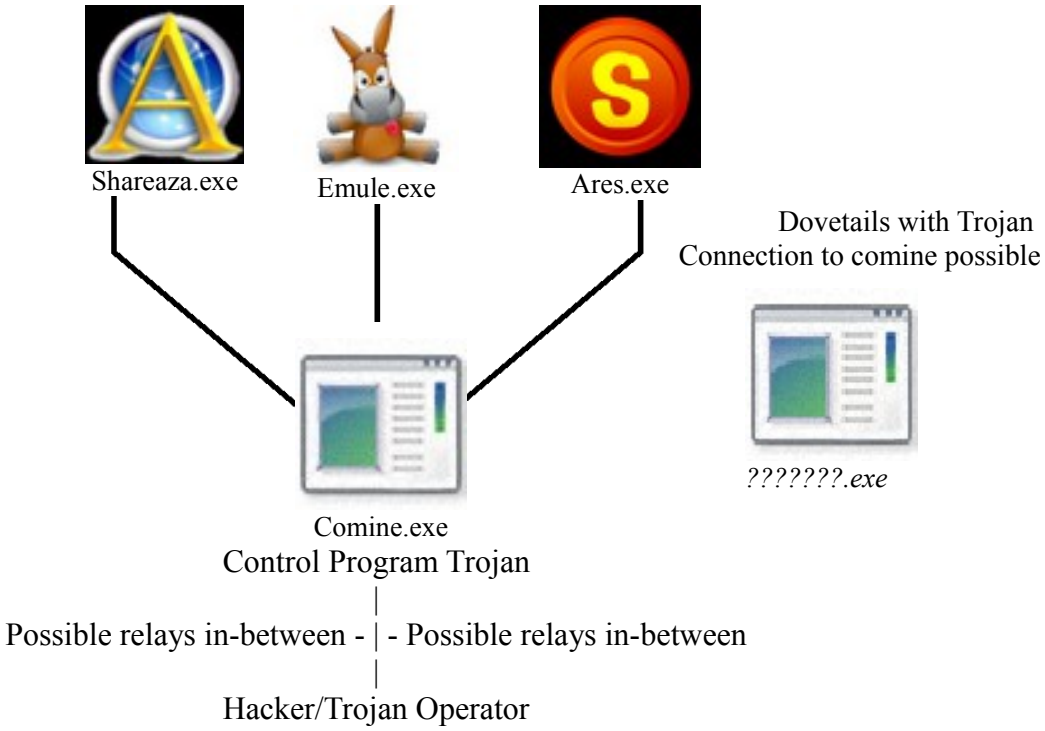
Dated: Mar 21st 2013 #0001 Personal Investigative Report

Notice: If anyone has encountered such a virus then please contact admin@uswgo.com Immediately.

Report contributed by Brian D. Hill:

I believe it was surrounded by comine.exe along with another exe file that had random characters so I don't remember that file name since it had a certain kind of random characters and I believe it may have been in the TEMP folder.

It came with three rogue P2P file sharing applications that were not stored in the usual file directories for programs or even portable programs. Those files are called ares.exe, emule.exe, and shareaza.exe. They share possibly illegal files and files with Trojans embedded without the computer owners permission despite invalid claims by law enforcement that no one can force a user to download and share files on P2P networks. When the user discovers them and attempts to shut down the program using process termination on Task Manager(taskmgr.exe) the rogue Trojan control program attempts to revive the operation of the rogue P2P programs and will fully operate within 3-5 seconds or even up to 10 seconds depending on processing speed from CPU. No matter how many times the user continues stopping the program it comes right back. When the user attempts to end the task then quickly remove the files even with certain software, the Trojan that controls the rogue programs seems to regenerate the rogue programs which continues to share and download illegal material which can get the user in trouble especially with any number of law enforcement task forces.



Not enough information to completely confirm information due to the original viruses being stolen.