Worm:Win32/Autorun.ZZ

Article URL
malware.php?mal_id=6292631744ccae3b2d31fe3.84066274

Author
SecurityHome.eu

Published: 29 October 2010

Aliases :

Worm:Win32/Autorun.ZZ

is also known as *TR/Agent.eige (Avira), Win32.HLLW.Autoruner.26463 (Dr.Web), Win32/AutoRun.Agent.XK (ESET), W32/Autorun.worm.bbj (McAfee), Troj/Agent-OVO (Sophos)*

.

Explanation :

Worm:Win32/Autorun.ZZ is a worm that spreads by copying itself to mapped network drives as a file named "klickmich1000.exe". The worm attempts to communicate with the remote server "lysclassic.dyndns.org".
Top

Worm:Win32/Autorun.ZZ is a worm that spreads by copying itself to mapped network drives as a file named "klickmich1000.exe". The worm attempts to communicate with the remote server "lysclassic.dyndns.org". InstallationWhen run, the worm copies of itself as the following files: c:w1ndowswkeeper.exe c:sysdriversdriver.exe The worm also drops a batch script as "%TEMP%execfile.bat" that is used to run the dropped worm copy. The registry is modified to run the worm at each Windows start. In subkey: HKCUSOFTWAREMicrosoftWindowsCurrentVersionRunSets value: "drv"With data: "c:sysdriversdriver.exe" The batch script is executed by the worm and it runs the following instructions within a command shell: cmd /C start C:sysdriversdriver.exe -restart cmd /C start C:sysdriverswkeeper.exe -restart Spreads via€Â¦ Mapped network drivesThe worm copies itself to mapped network drives as the following file: <drive:>klickmich1000.exe The worm then writes an Autorun configuration file named "autorun.inf" pointing to the worm copy. When the drive is accessed from a computer supporting the Autorun feature, the worm is launched automatically. Payload Attempts a connection with remote serverThe worm attempts a connection with a remote server named "lysclassic.dyndns.org" using TCP port 9292. At the time of this writing, the server was not available.

Analysis by Jaime Wong

Last update 29 October 2010