Backdoor:W32/Hupigon.EMV | F-Secure

Archived: 2026-04-05 12:37:19 UTC

Classification

Aliases:

Backdoor.Win32.Hupigon.emv

Summary

A backdoor is a Remote Administration Tools (RAT) that expose infected machines to external control via the Internet by remote attackers.

Removal

Based on the settings of your F-Secure security product, it will either move the file to the **quarantine** where it cannot spread or cause harm, or **remove** it.

A False Positive is when a file is incorrectly detected as harmful, usually because its code or behavior resembles known harmful programs. A False Positive will usually be fixed in a subsequent database update without any action needed on your part. If you wish, you may also:

- **Check for the latest database updates**

  First, check if your F-Secure security program is using the latest updates, then try scanning the file again.

- **Submit a sample**

  After checking, if you still believe the file is incorrectly detected, you can submit a sample of it for re-analysis.

  Note: If the file was moved to **quarantine**, you need to collect the file from quarantine before you can submit it.

- **Exclude a file from further scanning**

  If you are certain that the file is safe and want to continue using it, you can exclude it from further scanning by the F-Secure security product.

  Note: You need administrative rights to change the settings.

Technical Details

This backdoor is detected as a member of the Hupigon family. the Backdoor:W32/Hupigon description provides additional details.Copies itself to:

- %Windows%\dllhost.exe
- %Windows%\setuprs1.PIF

Replicates these original Windows applications with an additional "EXE" extension:

- %Windows%\system32\cmd.exe to %Windows%\system32\cmd.exe.exe
- %Windows%\regedit.exe to %Windows%\regedit.exe.exe

Hupigon.EMV attempts to disable/redirect Windows applications using the following registry entries:

- HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options\cmd.exe Debugger = setuprs1.PIF
- HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options\regedit.exe Debugger = setuprs1.PIF
- HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options\regedt32.exe Debugger = setuprs1.PIF
- HKLM\Software\Microsoft\Windows NT\ CurrentVersion\Image File Execution Options\msconfig.exe Debugger = 7303.PIF

Registers itself as Windows COM+ System Application service using these registry entries:

- HKLM\System\CurrentControlSet\Services\COMSystemApp Type = 00000110
- HKLM\System\CurrentControlSet\Services\COMSystemApp ErrorControl = 00000000
- HKLM\System\CurrentControlSet\Services\COMSystemApp ImagePath = C:\WINDOWS\dllhost.exe -netsvcs
- HKLM\System\CurrentControlSet\Services\COMSystemApp DisplayName = COM+ System Applications

Attempts to locate and terminate the following process:

- 360tray.exe
- autoruns.exe
- avp.exe
- avpcc.exe
- cpf.exe
- ewido.exe
- FireTray.exe
- FireWall.exe
- FYFireWall.exe
- jpf.exe
- kav.exe
- KAVPF.exe
- KavPFW.EXE
- kpf4gui.exe

- KPFW32.EXE
- KVCenter.kxp
- KvMonXP.kxp
- KVXP.kxp
- McAfeeFire.exe
- mmc.exe
- outpost.exe
- PFW.exe
- procexp.exe
- Ras.exe
- RfwMain.EXE
- RRfwMain.EXE
- runiep.exe
- ssgui.exe
- SysSafe.exe
- TrojDie.kxp
- WoptiProcess.exe

Attempts to close windows containing these strings:

- ZoneAlarm
- ZoneAlarm Pro

Attempts to connect to 218.16.138.64 on TCP port 81.

Propagation

It attempts to propagate by creating "\runauto..\autorun.pif" and "\autorun.inf" on all available drives, including removable drives.The autorun.inf file is detected as Worm.Win32.AutoRun.dms.The autorun.inf appears as:

- [AutoRun] open=RUNAUT~1\autorun.pif shell\1=´ò¿ª(&O) shell\1\Command=RUNAUT~1\autorun.pif shell\2\=ä¯ÀÀ(&B) shell\2\Command=RUNAUT~1\autorun.pif shellexecute=RUNAUT~1\autorun.pif

To make sure it will only run once, the mutex "Red_Server_2007" is created.

File System Changes

Create these directories:

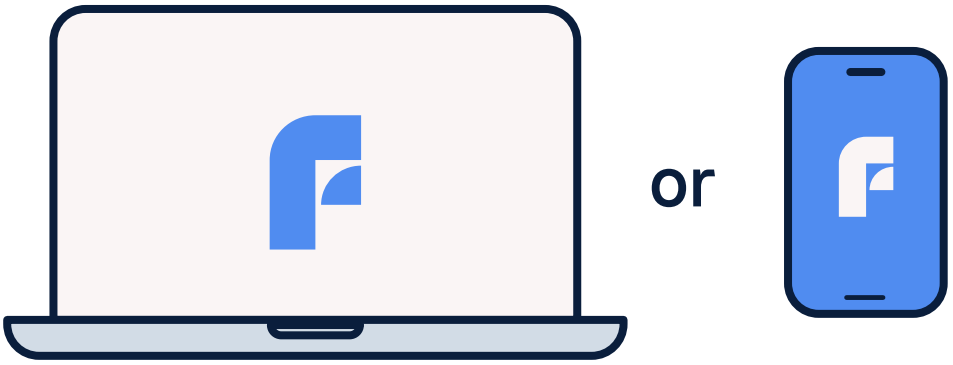
- %drive%\runauto..\

Protect your devices from malware with F-Secure Total

Protecting your devices from malicious software is essential for maintaining online security. F-Secure Total makes this easy, helping you to secure your devices in a brilliantly simple way.

- Award-winning antivirus and malware protection
- Online browsing, banking, and shopping protection
- 24/7 online identity and data breach monitoring
- Unlimited VPN service to safeguard your privacy
- Password manager with private data protection

Choose how many devices you want to protect to get started.



- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €69.99.

- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €89.99.

- Free customer support
- Cancel anytime
- The trial does not obligate you to buy the product

Try Total 30 days for freeAfter 30 days your subscription will renew automatically for one year at €99.99.

More Support

Contact Support

Chat with with or call an agent.