Backdoor:W32/Hupigon | F-Secure

Archived: 2026-04-05 22:50:54 UTC

Classification

Aliases:

Backdoor:W32/Hupigon

Summary

A remote administration tool (RAT) that bypasses the security features of a program, computer or network to give unauthorized access or control to its user.

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

Hupigon variants are backdoor programs, which provide an attacker with access to, and control of, an infected machine. There are a large number of variants in the Hupigon family.

The backdoor's file is a PE executable. The file may be packed with UPX. Unpacked, the code size is 710kB. It is very rare for a Hupigon variant to be smaller than 299kB.

Hupigons are written with Borland Delphi.

The following text strings can typically be found in a Hupigon variant:

- 6600.org
- BEI_ZHU
- GrayPigeon
- Hacker.com.cn.exe
- huaihuaitudou
- Rejoice2007
- woainisisi

Installation

When the backdoor's file is started, it copies itself as a file named something similar to "Hacker.com.cn.exe" in the Windows System folder and then uses the following processes to make itself to look like a valid Windows program:

- calc.exe
- cmd.exe
- mmc.exe
- mspaint.exe
- mstsc.exe
- notepad.exe
- osk.exe
- sndrec.exe
- sndvol32.exe
- svchost.exe
- winchat.exe

It also makes a number of additions to the registry.

Activity

Hupigon variants have several different types of features. The following list is an example of some:

- It allows others to access the computer
- Allows for recording with the user's webcam
- Can make the user's computer to attack various servers
- Send victim's computer messages

- Has rootkit functionality so it has a stealth component that hides files
- Create logs from keystrokes, steals passwords, and sends this information to remote servers

Propagation

Hupigon doesn't have any automatic mechanisms to spread itself. It must be sent by its author via email, through a website, or even via Instant Messengers (IM) such as Yahoo, MSN, ICQ, and Skype.

Creating Hupigon Variants

Hupigon variants are created using kit software. The kit is maintained in a very professional fashion with a highly developed User Interface (UI).

The main UI of the kit can be seen below:

Many options can be set. The "Fast Configuration" shown below enable the following options:

- Service name is rejoice44.exe
- Installation path is Msinfo…
- Password is 1234
- Icon is taken from MS Media Player
- Uses Internet Explorer to bypass firewall
- Create mutex and remove installer from installer folder
- Pack code by using UPX
- Self/auto-clone protected installation path is "system32"
- Executable is calc.exe

There is also a "rootkit" option available. Other options including adding a URL to target for a Distributed Denial of Service (DDoS) attack:

The kit as default settings to create mutexes. Many Hupigon variants therefore create mutexes in the following format:

- xxx.com.cn_MUTEX

The "xxx" being a variable, for example: Hacker.com.cn_MUTEX

Registry Modifications

Creates these keys:

- HKLM\System\CurrentControlSet\Services\system32 ImagePath = C:\WINDOWS\Hacker.com.cn.exe

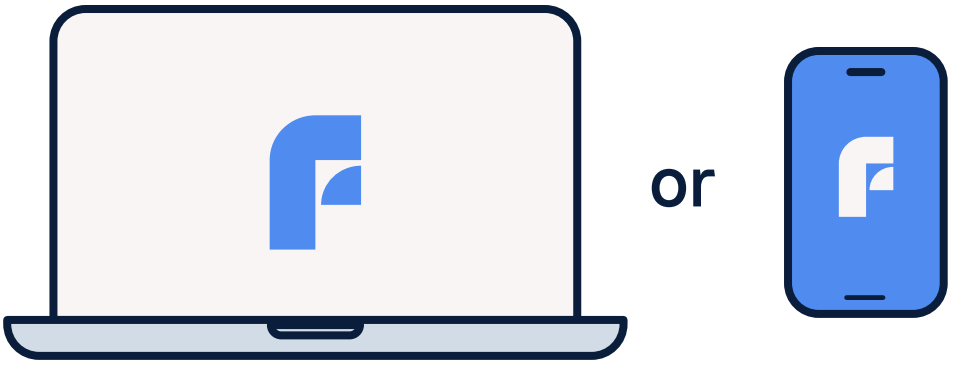
- HKLM\System\CurrentControlSet\Services\system32
- HKLM\System\CurrentControlSet\Services\system32\Security

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.