Hupigon

By Contributors to Wikimedia projects

Published: 2015-09-30 · Archived: 2026-04-06 03:25:43 UTC

From Wikipedia, the free encyclopedia

Hupigon	
Malware details	
Type	Backdoor
Author	Red Apollo
Technical details	
Platforms	Windows, Linux, iOS, Android

Hupigon (also **Graftor**) detected as (**Backdoor.Win32.Hupigon**, **Trojan.Win32.Hupigon**, **Backdoor.Win32.Graftor**, and **Trojan.Win32.Graftor**) is a backdoor Trojan. Its first known detection goes back to November 2008, according to Securelist from Kaspersky Labs.[1]

This malicious software, which usually should be a portable executable (and may be packed with *UPX*), is mostly used in order to connect a (worldwide) group of victimized PCs and form a botnet (also known as a zombie network). The software is able to spread through networks in order to infect other computers as computer worms do (see Conficker). The difference is that such backdoors do not spread automatically (as worms do), but are started through a command and control-center who is supervising them.

In the Hupigon family, there are a large number of variants. They are written in Borland Delphi.

- *Trojan.Win32.Boht* (Kaspersky Labs and Fortinet)
- *Backdoor:Win32/Bezigate* (Microsoft)
- *Backdoor.Win32.Graftor* (Bitdefender)[2]

- Analysis of a file - VirusTotal
- Analysis of a file Archived 2016-03-04 at the Wayback Machine - Threat Expert

1. ^ *"Backdoor.Win32.Hupigon @ Securelist". Archived from the original on 2016-03-05. Retrieved 2015-09-30.*
2. ^ Refs of a Hupigon-File