H

Hupigon RAT: Remote Access and Removal

What it is Hupigon is a family of Windows backdoors and remote-access Trojans. Variants can let an unauthorized operator run commands, manage files and processes, capture information, and use the computer as part of other malicious...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
2 min

What it is

Hupigon is a family of Windows backdoors and remote-access Trojans. Variants can let an unauthorized operator run commands, manage files and processes, capture information, and use the computer as part of other malicious activity. A detection indicates that the confidentiality and integrity of the device may be compromised.

How it works

Hupigon variants have been distributed through malicious files, deceptive software, and other loaders. After execution, the malware creates persistence and contacts a remote server or listens for control traffic. Exact filenames and capabilities differ, so investigation should focus on behavior and related artifacts rather than one historical indicator.

Key points

- An attacker may install additional tools or create new accounts before the original Trojan is detected.
- Remote control can expose files, typed credentials, microphones, cameras, or network resources depending on the variant.
- Performance problems are possible, but many backdoors are designed to remain quiet.

What to do

- Disconnect the endpoint and collect recent process, startup, account, and network activity.
- Use a trusted full scan and remove related persistence; reimage if scope remains uncertain.
- Reset credentials from a clean device and revoke sessions used on the affected system.
- Review neighboring systems for reused credentials or lateral movement.

Assume remote actions were possible

After isolating the host, preserve the detected file, service or startup entry, listening port, process tree, and outbound destinations. Search for additional tools and accounts because a remote-access Trojan may be only one part of the intrusion. Remove persistence and rebuild the system if integrity cannot be trusted. From a clean device, rotate credentials used on the host and revoke active sessions. Review firewall and router exposure if inbound access was involved. Hunt for the same command-and-control indicators on other endpoints rather than treating Hupigon as one isolated file.