G

Glupteba: How this modular backdoor persists and what it can do

What it is Glupteba is a modular Windows malware family that can act as a backdoor, information stealer, downloader, and cryptomining component. It is also associated with a botnet and mechanisms intended to keep command infrastructure...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

Glupteba is a modular Windows malware family that can act as a backdoor, information stealer, downloader, and cryptomining component. It is also associated with a botnet and mechanisms intended to keep command infrastructure resilient. Capabilities vary because operators can deliver different modules to different infected systems.

How it works

Infections have been linked to deceptive downloads, malicious advertising, software cracks, and traffic-distribution systems. Glupteba establishes persistence, collects system data, and contacts command infrastructure for tasks or additional modules. Some versions used public blockchain

data as a fallback method for locating command servers when normal domains were disrupted.

Key points

- High CPU usage may indicate a mining module, but a quiet backdoor can remain with few visible symptoms.
- Credential theft and remote control mean cleanup must include account and network investigation.
- Deleting one module does not prove the loader, persistence, or other payloads are gone.

What to do

- Isolate the endpoint and collect process, persistence, DNS, and proxy evidence.
- Perform a full scan or rebuild the system when the infection chain cannot be fully established.
- Rotate credentials and revoke sessions used on the affected device.
- Remove unofficial software sources and block known malicious download and advertising paths.