G

Glupteba Malware: Persistence, Detection, and Recovery

Glupteba is modular Windows malware associated with credential theft, proxying, cryptomining, and resilient command-and-control discovery.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What is Glupteba?
02 Why the blockchain feature matters
03 What Glupteba can do
04 Possible signs and investigation
05 What to do if Glupteba is detected
06 Prevention
07 Source

Quick answer: Glupteba is modular Windows malware associated with credential and cookie theft, cryptocurrency mining, proxy services, and delivery of additional components. Some versions use data published through Bitcoin transactions as a backup

way to discover command servers. A detection should trigger isolation, account recovery, and investigation for other payloads—not only deletion of one file.

01 What is Glupteba?

Glupteba is both a malware family and part of a botnet ecosystem. Google's Threat Analysis Group documented infections worldwide and described components used to steal credentials and cookies, mine cryptocurrency, and operate proxies involving Windows and internet-connected devices. Its capabilities can vary by campaign because modules are delivered according to the operator's goal.

Google disrupted key Glupteba infrastructure and filed a civil action in December 2021. Google also warned at the time that the operators could attempt to restore control. A disruption reduces an operation's capacity at a particular point; it is not proof that every infected device is clean or that a family can never return.

02 Why the blockchain feature matters

Normal command-and-control servers can be blocked or seized. Google reported that Glupteba used HTTPS for its primary command traffic and a backup discovery method tied to the public Bitcoin blockchain. If primary servers were unavailable, infected systems could read encoded information in selected transactions to find replacement domains.

The blockchain did not execute malware on the PC, secretly spend the victim's Bitcoin, or make the malware impossible to remove. It provided a resilient public noticeboard for locating infrastructure. Endpoint removal, credential recovery, and blocking the active delivery chain remain effective defensive actions.

03 What Glupteba can do

- Steal browser credentials, cookies, account names, and other device information.
- Download and run modules or additional malware under remote direction.

- Use computing resources for hidden cryptocurrency mining.
- Turn affected connectivity into a proxy that can relay third-party traffic.
- Maintain persistence and update its configuration or command-server location.

04 Possible signs and investigation

An antivirus or EDR detection is more reliable than visible symptoms. Other clues can include unexpected CPU use, unfamiliar startup items or scheduled tasks, browser credential access, unexplained downloads, and outbound traffic from processes that do not normally use the network. Proxy activity may create abuse complaints or logins apparently originating from the victim’s public IP.

Investigators should capture the detecting product, verdict, hash, path, signer, process ancestry, persistence, network destinations, user, and first-seen time. Search the wider fleet for the delivery file and behavior. Avoid depending solely on old wallet addresses, domains, or hashes because modules and infrastructure change.

05 What to do if Glupteba is detected

1. Disconnect the device from all networks, including VPN, while preserving evidence needed by the response team.
2. Run updated endpoint scans and inspect scheduled tasks, services, startup entries, browser data access, downloads, and network logs for related modules.
3. From a clean device, reset exposed passwords, revoke sessions and cookies, verify MFA methods, and review high-value account activity.
4. Check routers and other managed devices if telemetry indicates proxying or configuration changes; update firmware and replace unknown settings.
5. Reimage the Windows endpoint when persistence, secondary payloads, or system integrity cannot be resolved confidently. Restore only known-clean data.

06 Prevention

Keep Windows, browsers, and network-device firmware supported and patched. Use reputable endpoint protection, application control, least privilege, DNS or web filtering, and unique passwords stored in a password manager. Avoid cracked software, deceptive downloads, fake updates, and installers promoted through suspicious advertising. Organizations should monitor new persistence, credential-store access, mining behavior, and unusual proxy traffic.

07 Source

The capabilities, disruption context, and backup command-discovery description come from Google Threat Analysis Group's Glupteba technical report.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com