GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

A

AZORult Malware: Data Theft, Detection, Removal, and Recovery

AZORult is a Windows information stealer and downloader. Removing its files does not invalidate stolen passwords, browser sessions, or cryptocurrency keys.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	3 min

AZORult is a Windows information-stealing malware family first observed in 2016. Variants have collected browser passwords and cookies, cryptocurrency-related data, application credentials, system information, and files. Some builds can download additional malware.

The family has changed over time and is often repacked, so a specific filename, folder, or network indicator is not universal. A current detection can identify an active payload, a blocked downloader, or an old artifact; read the path, execution status, and process history.

What AZORult can steal

- saved browser credentials, autofill records, browsing data, and cookies;
- active session tokens that may bypass a password until revoked;

- FTP, email, messaging, remote-access, or other locally stored application credentials;
- cryptocurrency wallet files and clipboard or system information in some variants;
- selected documents or a system profile used for later attacks.

Trend Micro's current AZORult guide likewise describes the family as an information stealer targeting browsing, credential, and cryptocurrency data.

How infections start

AZORult has been delivered through phishing attachments and archives, cracked software, fake installers, malicious advertisements, exploit chains, and other malware loaders. The initial downloader and any additional payloads are as important as the detected AZORult file.

Possible signs

- an antivirus or EDR detection for AZORult, an infostealer, or suspicious credential access;
- a newly run executable from Downloads, Temp, AppData, or an extracted archive;
- unexpected account sessions, password resets, exchange withdrawals, or MFA prompts;
- a short burst of outbound traffic followed by little visible activity.

Sudden sign-outs or network spikes are not proof. Infostealers often finish quickly and may leave few user-visible symptoms.

Remove AZORult and scope the infection

1. **Isolate the PC.** Do not use it for email, banking, work access, or cryptocurrency.
2. **Preserve evidence.** Record the alert, file hash and path, parent process, user, timestamps, and source download.
3. **Run an updated full scan.** Quarantine the stealer, its downloader, persistence, and additional payloads. Rescan after restart.

4. **Reinstall when integrity is uncertain.** Use trusted Windows media if privileged access, multiple payloads, altered security controls, or an unknown infection chain prevents reliable cleanup.

Recover accounts and wallets

From a clean device, revoke all active sessions and tokens, then change passwords stored or used on the PC during the possible exposure. Begin with email, password managers, business identities, remote access, financial services, and exchanges. Replace app passwords, API keys, and recovery codes where relevant.

If a seed phrase or private key may have been accessible, create a new wallet with a new seed on a trusted device and transfer assets. A password change does not replace a cryptocurrency private key.

Additional business response

Search identity, VPN, email, proxy, DNS, and EDR logs for use of stolen credentials and sessions. Hunt across endpoints for the same delivery source, hash, parent process, and confirmed infrastructure. Resetting one user's password without revoking tokens or finding the initial access path leaves the organization exposed.

AZORult FAQ

Can antivirus restore stolen data?

No. It can stop or remove known components, but already-exfiltrated secrets must be revoked or replaced.

Should I trust old indicator lists?

Use them only for historical context. Infrastructure, filenames, and packing change; behavior and local evidence are more durable.

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