L

LokiBot Malware: Credential Theft, Detection, and Recovery

LokiBot is a credential-stealing malware name used across multiple campaigns and platforms. Cleanup must include revoking data already stolen from the device.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

LokiBot, also written **Lokibot** or **Loki PWS**, is a name associated with credential- and information-stealing malware. It has appeared in campaigns targeting Windows and Android, but detections on those platforms do not necessarily represent one identical codebase or capability set.

Use the operating system, file path, package name, process behavior, and security-vendor description to interpret an alert. Do not follow removal instructions for Android when the detection is a Windows executable, or vice versa.

What LokiBot can target

- browser, email, FTP, remote-access, and application credentials;
- cookies, session data, autofill information, and system details;

- cryptocurrency wallet data and selected files in some variants;
- SMS, notifications, overlays, or mobile banking data in Android-focused campaigns;
- additional payload delivery or further unauthorized access.

CISA's LokiBot advisory describes it as simple but effective credential- and information-stealing malware often delivered through malicious attachments.

Common delivery paths

- phishing documents, archives, disk images, or executable attachments;
- fake invoices, shipping notices, updates, cracks, and repacked installers;
- malicious links and loaders that install the stealer as a second stage;
- on Android, sideloaded APKs or deceptive apps requesting dangerous permissions.

Detection and warning signs

An antivirus or EDR alert, suspicious executable from a user-writable folder, unexpected process chain, or outbound credential-theft behavior is stronger evidence than general symptoms. Unauthorized logins, new MFA prompts, wallet transfers, or account-recovery changes may indicate that stolen data is already being used.

Battery drain, slow performance, or a sudden sign-out alone does not prove LokiBot. Infostealers frequently execute quickly with little visible impact.

Removal and device recovery

1. **Disconnect the affected device.** Do not use it for sensitive sign-ins.
2. **Preserve detection details.** Record path, hash, parent process or Android package, source, user, and timestamps.
3. **Windows:** run an updated full scan and remove the delivery file, persistence, and secondary payloads. Reinstall from trusted media if privileged or unknown components ran.

4. **Android:** remove the suspicious app, revoke accessibility, device-admin, notification, overlay, and SMS permissions, update the OS, and scan. Factory-reset when administrative control or the payload scope cannot be trusted.

Account and wallet recovery

From a clean device, revoke active sessions and tokens before changing passwords. Prioritize primary email, password managers, financial and work accounts, remote access, and every credential stored or used during the exposure window. Re-enroll MFA and replace recovery codes if needed.

If a seed phrase or private key may have been accessible, create a new wallet with a new seed on a trusted device and move assets. Changing only the wallet application's password is insufficient.

Additional organizational response

Review identity, VPN, email, proxy, DNS, and endpoint logs for use of stolen sessions or credentials. Hunt for the same attachment, hash, parent process, sender, and confirmed infrastructure across users. Investigate the initial delivery rather than treating the endpoint alert as the complete incident.

LokiBot FAQ

Does removing LokiBot secure my accounts?

No. Removal stops the local malware; already-stolen passwords, cookies, and keys remain usable until revoked or replaced.

Is every LokiBot alert the same malware?

No. Naming varies by platform, campaign, and security vendor. Base decisions on the exact detection context.

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