C

# CryptBot Infostealer: Detection and Account Recovery

CryptBot is Windows information-stealing malware associated with theft of browser credentials, account sessions, and cryptocurrency-related data.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

## In this guide

01 What is CryptBot?
02 What CryptBot may steal
03 How CryptBot is distributed
04 Signs and evidence
05 What to do after detection
06 Prevention
07 Source

**Quick answer:** CryptBot is Windows information-stealing malware designed to collect sensitive data such as authentication credentials, social-media logins, browser information, and cryptocurrency-wallet data. It has been distributed through maliciously

modified software packages. Isolate an affected computer and recover accounts from a known-clean device, including revoking sessions rather than only changing passwords.

## 01 What is CryptBot?

CryptBot is an infostealer: malware that searches an endpoint for information valuable to criminals, packages the results, and sends them to an operator. Google reported in 2023 that recent versions targeted Google Chrome data and estimated approximately 670,000 infections during the preceding year. Google pursued legal and technical disruption against distributors and related domains.

A takedown can slow a campaign but does not clean already infected devices or guarantee that every distributor and variant disappears. Treat a current detection according to the endpoint evidence and the detecting vendor’s latest information.

## 02 What CryptBot may steal

- Saved browser credentials, cookies, autofill data, and authentication sessions.
- Social-media and other account logins stored on the device.
- Cryptocurrency wallet files, extensions, or related access material.
- System information that helps an operator identify and value the victim.

Capabilities vary by version. A family name alone does not prove that every possible browser, wallet, or application was accessed. Investigators should identify the sample, execution time, user profile, and observed file or process access.

## 03 How CryptBot is distributed

Google documented distributors offering maliciously modified versions of popular software, including packages impersonating Google Chrome and Google Earth Pro. Similar infostealer campaigns commonly use search advertising, search-result manipulation, fake download sites, cracked software, and archives that ask the user to bypass warnings. The advertised application

may install or appear to work while the stealer runs in the background.

Verify software by navigating independently to the publisher, checking the registered domain and signature, and avoiding sponsored or third-party download buttons when the source is unclear.

## 04 Signs and evidence

An antivirus or EDR alert may be the only local symptom. Account-side signs include unfamiliar sessions, changed recovery information, new mailbox rules, fraudulent messages, cryptocurrency transfers, or logins that continue after a password change. Gather the detection name, hash, path, signer, process tree, browser profile, download URL, DNS and network events, and first-seen time. Determine whether the file was merely downloaded or actually executed.

## 05 What to do after detection

1. Disconnect the computer from Ethernet, Wi-Fi, and VPN. Do not sign into additional accounts on it.
2. Preserve the security alert and delivery evidence. Hunt for loaders, persistence, remote access, and other payloads.
3. From a clean device, change exposed passwords—starting with email and the password manager—and revoke all active sessions and application tokens.
4. Verify MFA methods, recovery addresses, forwarding rules, OAuth grants, API keys, and logged-in devices.
5. Follow wallet-provider procedures if cryptocurrency secrets may have been exposed. A password change may not invalidate a copied recovery phrase or private key.
6. Run updated full and offline scans. Reimage the endpoint when sensitive access was stored or system integrity is uncertain.

Restore known documents rather than an unverified browser profile or full system image. Reinstall software from official sources and monitor recovered accounts for follow-on abuse.

## 06 Prevention

Use a password manager with unique credentials and phishing-resistant MFA. Keep the operating system, browser, and extensions updated. Enable browser reputation warnings and endpoint protection. Avoid cracked software and installers from advertisements, file-sharing services, or imitation domains. Organizations should restrict untrusted executables, centralize identity and endpoint logs, protect browser credential stores, and monitor session-token abuse.

## 07 Source

CryptBot’s purpose, targeted data, distribution through modified software, and disruption context are documented by Google in Continuing our work to hold cybercriminal ecosystems accountable.

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**