D

Dridex Malware: Banking Trojan, Delivery, and Response

Dridex is modular Windows banking malware used for credential theft, fraudulent transactions, and delivery of additional payloads. Learn how infections begin, which evidence matters, and how to protect accounts after detection.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 19, 2026

READ TIME
4 min

CONTENTS

In this guide

Dridex is modular Windows malware best known as a **banking Trojan**. It has been used to steal passwords, personal information, and online-banking details for fraudulent transactions. Dridex has also served as an access and payload-delivery platform, so an

infection can lead to more than bank-account theft.

The UK National Cyber Security Centre reports that Dridex has affected victims since at least 2014 and commonly arrives through malicious phishing attachments or is dropped by existing malware such as Emotet. Delivery methods and modules change, so responders should analyze the observed campaign rather than depend on one historical filename or document format.

01 What Dridex does

Capabilities vary by version and operator configuration. Documented activity includes:

- Collecting system and user information.
- Stealing browser, form, password, and financial data.
- Capturing input through keylogging or browser interception.
- Connecting to distributed command infrastructure.
- Downloading modules and additional malware.
- Providing a foothold used in broader criminal intrusion and ransomware chains.

TLS between the browser and bank does not protect a session from malware already running on the endpoint. A banking Trojan can read data before it is encrypted or after the browser decrypts it.

02 A typical Dridex infection chain

1. **Delivery:** a user receives a convincing invoice, payroll document, archive, link, or other phishing lure.
2. **Execution:** a document macro, script, shortcut, loader, or exploit launches the next stage.
3. **Installation:** Dridex establishes execution and communicates with attacker infrastructure.
4. **Collection:** modules monitor browsers, credentials, forms, or financial sessions.
5. **Follow-on activity:** stolen access is used for fraud, or other malware is deployed into the environment.

A detection for the loader may occur after the attachment has already launched another component. Conversely, a blocked attachment that never executed does not automatically mean the endpoint was infected. Process and network telemetry determine the outcome.

03 Possible warning signs

- A security alert naming Dridex, Bugat, or a related campaign component.
- Office software or an archive utility starting scripts, command shells, or unexpected system tools.
- New persistence, packed DLLs, or unfamiliar processes in user-writable folders.
- Connections to unusual or newly observed destinations from a workstation.
- Unrecognized financial transactions, payees, logins, mailbox rules, or account-recovery changes.
- Additional detections for loaders, credential theft, remote access, or ransomware.

04 What to do after a detection

1. **Isolate the endpoint** and stop using it for email, banking, administration, or password changes.
2. **Preserve evidence:** message, attachment, URLs, hashes, process tree, persistence, DNS and proxy records, and detection times.
3. **Contact affected financial institutions** through verified channels if banking data or payments may be exposed. Review transactions and newly added payees.
4. **Protect accounts from a clean system.** Revoke sessions, reset passwords and recovery information, and enable strong MFA.
5. **Search other mailboxes and endpoints** for the same campaign indicators and execution pattern.
6. **Scan or rebuild.** Remove every stage and reimage high-value systems when follow-on access cannot be ruled out.

7. **Monitor after recovery** for renewed authentication, payment, email, and command-and-control activity.

05 Prevention

Block risky attachment types and unnecessary macros or script interpreters, patch browsers and document software, and give users only the privileges they require. Use email authentication and filtering, endpoint behavior monitoring, network segmentation, and controls for unusual child processes. Financial workflows should require independent approval for new payees and high-risk transactions so one compromised workstation cannot authorize payment alone. Regularly test payment-fraud escalation contacts so employees know how to stop a suspicious transfer quickly.

06 Frequently asked questions

Is Dridex ransomware?

Dridex is primarily classified as banking and access malware. It has been associated with chains that deliver ransomware, but the Dridex component itself should not be equated with the later encryptor.

Does removing Dridex make stolen credentials safe again?

No. Reset exposed credentials and revoke sessions from a clean device after containment, then review accounts for abuse.

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