D

DanaBot Malware: Banking Theft, Remote Access, and Recovery After Detection

DanaBot is a modular banking Trojan, infostealer, loader, and remote-access platform. Learn how it steals browser and financial data and how to recover after a confirmed infection.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 What DanaBot can do
02 How DanaBot reaches devices
03 Possible signs
04 Immediate response
05 Removal and device recovery
06 Account and financial recovery
07 What the 2025 disruption changed
08 Prevention
09 Frequently asked questions
10 References

DanaBot is a modular Windows banking Trojan, information stealer, loader, and botnet platform first identified in 2018. Criminal affiliates have used it to hijack browser sessions, steal credentials and cryptocurrency data, remotely control computers, and install follow-on malware including ransomware.

Law enforcement disrupted major DanaBot infrastructure during Operation Endgame in May 2025. That action did not make an existing infection safe: compromised devices and stolen credentials still require remediation, and malware operations can rebuild or change infrastructure.

01 What DanaBot can do

Capability	Risk to the victim
Web injects and browser manipulation	Fake fields or messages appear inside legitimate banking and shopping sessions to capture credentials, card data, or transaction information.
Credential and cookie theft	Saved browser, email, FTP, VPN, remote-desktop, and other application data can enable account takeover.
Keylogging, screenshots, and video	Sensitive information can be captured even when it is not stored on disk.
Proxy and remote access	Operators can route activity through the victim and interact with accounts from a familiar device or IP address.
Cryptocurrency targeting	Wallet data, credentials, clipboard content, or transaction workflows may be stolen or manipulated.
Loader functionality	The initial DanaBot infection can install additional malware or provide access used before ransomware.

DanaBot has been sold or leased as malware-as-a-service. Affiliates can use different delivery methods, modules, configurations, and targets, so no single symptom or indicator covers every campaign.

02 How DanaBot reaches devices

Commonly reported delivery paths include phishing email attachments or links, malicious scripts, multi-stage downloaders, cracked or pirated software, and other malware distribution services. The first visible file may be only a loader that retrieves the main DanaBot component.

Campaign infrastructure changes. Old domain or IP lists are useful for historical investigation but should not replace current endpoint behavior, email telemetry, DNS and proxy logs, and up-to-date threat intelligence.

03 Possible signs

- A security product detects DanaBot, its loader, or a related malicious script or DLL.
- A banking or shopping page shows unfamiliar fields, prompts, or overlays that appear only on one computer.
- Unknown proxy settings or unexplained traffic appears from a user workstation.
- Browser, FTP, VPN, remote-access, or cryptocurrency files are accessed by an unexpected process.
- Unfamiliar startup files, tasks, services, or processes return after restart.
- Accounts show logins, transfers, or session activity that the user did not initiate.
- A follow-on malware or ransomware alert appears after an earlier phishing or script event.

Bank-site errors and slow performance alone do not prove DanaBot. Record the exact detection, process tree, command line, hashes, persistence, and network activity.

04 Immediate response

1. **Disconnect the affected computer.** Stop wired, wireless, and VPN access without using it for further logins.
2. **Notify financial and security teams.** If banking, payment, cryptocurrency, business email, or privileged access was used, speed matters.

3. **Preserve evidence.** Save the alert, malicious email, process tree, memory where appropriate, persistence, network connections, DNS, proxy, and authentication records.
4. **Do not trust the visible browser session.** Use a known-clean device and a separately verified phone number or official site to contact providers.
5. **Scope the intrusion.** Search for the delivery email, downloader, related payloads, remote access, unusual account activity, and other infected endpoints.

05 Removal and device recovery

Quarantining one DanaBot file is not enough to prove the device is clean. The initial loader, persistence, modules, remote-access activity, and follow-on malware must all be addressed.

1. Run updated endpoint and offline scans and collect their results.
2. For a confirmed active infection, especially one with remote access or credential theft, rebuild the computer from trusted installation media and an approved baseline.
3. Patch the operating system and applications before restoring access.
4. Restore only necessary data from backups created before the incident; reinstall applications from original sources.
5. Validate that proxy, browser, DNS, startup, and security settings match the approved configuration.

06 Account and financial recovery

1. From a clean device, change passwords used or stored on the infected computer.
2. Prioritize email, banking, card, cryptocurrency, password-manager, VPN, remote-desktop, cloud, and administrator accounts.
3. Revoke sessions, browser tokens, app passwords, remembered devices, and unauthorized OAuth or connected applications.
4. Enable phishing-resistant MFA where available. A stolen session can bypass a normal password change, so session revocation matters.

5. Ask financial institutions to review and monitor transactions. Follow their fraud-reporting procedures rather than responding to a popup or number shown on the infected PC.
6. Move cryptocurrency assets only after securing wallet seeds, exchange accounts, email, and devices. Do not type a seed phrase into an unsolicited recovery site.

07 What the 2025 disruption changed

In May 2025, U.S. authorities announced charges connected to DanaBot and seizures of command-and-control servers, while Europol described a broader Operation Endgame action against initial-access malware infrastructure. The action can interrupt active control and provide victim notification, but it does not:

- remove malware already present on a computer;
- restore stolen passwords or money;
- prove that every DanaBot server or affiliate is gone;
- make an old DanaBot sample safe to run.

If an ISP, law-enforcement agency, or Shadowserver sends a legitimate infection notice, verify the sender independently and follow the remediation guidance. Do not install a "cleanup tool" from an unexpected attachment.

08 Prevention

- Use email filtering, attachment sandboxing, and web controls for scripts and executable downloads.
- Block untrusted macros and scripts and apply attack-surface reduction rules appropriate to the organization.
- Do not install cracks or pirated software.
- Keep Windows, browsers, Office, and endpoint protection updated.
- Use password managers and phishing-resistant MFA, while monitoring for session theft.
- Separate user workstations from administrative and backup systems.

- Monitor new proxy settings, unusual browser injection, credential-store access, and loader behavior.

09 Frequently asked questions

Is DanaBot only a banking Trojan?

No. Banking fraud was an early focus, but documented versions also steal broader information, provide remote access, proxy traffic, and install additional malware.

Can DanaBot steal an MFA code?

Keylogging, screen capture, web injection, and remote access can expose codes or manipulate a live session. Phishing-resistant MFA reduces risk, but the infected endpoint still must be rebuilt and sessions revoked.

Did Operation Endgame eliminate DanaBot?

It significantly disrupted infrastructure in 2025, but defenders should not equate a takedown with permanent eradication. Validate current alerts and remediate compromised devices and accounts.

10 References

- U.S. Department of Justice: 2025 DanaBot charges and disruption
- Europol: Operation Endgame, May 2025
- Microsoft Security Intelligence: DanaBot
- Proofpoint: History of DanaBot

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