C

Carberp Banking Trojan: Credential Theft and Recovery

Carberp is a Windows banking-Trojan family known for stealing credentials, injecting into processes, logging keystrokes, and downloading additional malware.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What is Carberp?

02 How Carberp affected a computer

03 Possible signs

04 What to do after a Carberp detection

05 How to prevent banking-Trojan infections

06 Sources

Quick answer: Carberp is a Windows banking-Trojan family documented for stealing online-banking and application credentials, capturing keystrokes and screenshots, exporting certificates, and downloading additional components. It is primarily a historic family, but a current detection still requires verification and response because old code can be reused and credentials may already be exposed.

01 What is Carberp?

Carberp became prominent in the early 2010s, particularly in attacks on online-banking users and businesses. Microsoft describes it as a family rather than one fixed file. Different components could collect logon data, receive commands, disable security functions, or fetch other malware. Public reporting also documented web injections that added fraudulent fields to genuine banking pages as they appeared in an infected browser.

Because source code and technical details circulated after the original campaigns, the name may appear in modern detections for a reused component, a signature match, or a related sample. Do not infer that the exact historic botnet is active from the family label alone. Confirm the detection with the file, process, time, and security-product telemetry.

02 How Carberp affected a computer

- **Delivery:** documented variants arrived through malicious downloads, compromised sites, exploit kits, or other malware.
- **Persistence and concealment:** variants used startup locations, code injection, and API hooking to run with Windows and hinder inspection.
- **Credential theft:** browser monitoring, web injections, keylogging, screenshots, stored-password collection, and certificate export could expose financial access.
- **Remote control:** modules contacted command servers, uploaded collected information, and downloaded or executed additional files.

03 Possible signs

Security alerts may be the only obvious sign. Investigators should also review unexpected executables in user or startup folders, unusual processes injecting into browser or shell processes, disabled security updates, unexplained outbound connections, and financial login pages requesting information the bank does not normally ask for. These behaviors are not unique to Carberp and require correlation.

Do not use decade-old domains, IP addresses, or filenames as the sole test. They can be inactive, reassigned, or changed by a new build. Current EDR evidence and the detecting vendor’s latest intelligence are more useful.

04 What to do after a Carberp detection

1. Disconnect the Windows device from networks and stop online banking or other sensitive activity on it.
2. Preserve the alert, file path, hash, process tree, persistence entries, network records, and relevant browser or email evidence.
3. From a clean device, contact the bank through a verified number, review transfers, and follow its fraud procedures.
4. Change exposed passwords, revoke active sessions, replace unknown MFA methods, and consider certificate revocation if private certificates were accessible.
5. Run an updated full and offline scan, then hunt other endpoints for the same delivery path and follow-on malware.
6. Reimage a business, finance, or administrator workstation when trustworthy eradication cannot be demonstrated. Restore clean data rather than unknown executables.

05 How to prevent banking-Trojan infections

Use a supported and patched operating system and browser, reputable real-time protection, least-privilege accounts, and application control. Obtain software only from verified sources and block risky script or document execution. Use phishing-resistant MFA for email and business

systems, enable bank transaction alerts, and separate payment approval from the workstation or person that creates a payment where possible.

A padlock in the browser does not defeat malware already running inside the endpoint. For high-risk business banking, use a dedicated managed device and out-of-band verification of new beneficiaries or unusual transfers.

06 Sources

Capabilities and response context are based on the Microsoft Security Intelligence description of Win32/Carberp and Kaspersky's analysis of banking web injections.

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