Qbot (QakBot) - what it is, how it steals credentials, and how to prevent it

Gridinsoft Help Center

Qbot (QakBot)

What it is

Qbot - also known as QakBot - is a modular banking trojan targeting Windows. It steals credentials, cookies, and session tokens from browsers and mail clients, monitors web logins with injects, and can log keystrokes. Campaigns often start with reply-chain phishing and exploit existing email threads to look trustworthy. Qbot also acts as a loader to bring in additional payloads. Background and removal tips: https://gridinsoft.com/threats/qbot

Why it matters

Stolen sessions and passwords enable account takeovers and fraudulent transfers. As a loader, Qbot can hand off access to other malware, raising the risk of business email compromise and wider breaches.

How it works

- Entry: phishing emails with malicious attachments or links, often in real conversation threads.

- Establish: drops in AppData/LocalAppData, sets autoruns via Run keys or Scheduled Tasks.

- Steal: harvests browser data, cookies, tokens, and mail client creds; may log keys and take screenshots.

- Persist and spread: updates itself, talks to C2, and can deliver follow-on payloads.

Red flags

- Unusual replies in existing email threads that include attachments or macro-enabled docs.

- New tasks or Run keys pointing to random-named files in AppData.

- Sudden logins from new locations despite MFA, or accounts staying logged in after password resets.

- EDR hits for credential access, LSASS scraping attempts, or browser data grabs.

Prevent it

- Block macro-enabled docs and ZIPs from unknown senders; use attachment sandboxing.

- Enforce phishing-resistant MFA and rotate tokens by signing out all sessions after resets.

- Disable Office macros from the internet and monitor for suspicious Scheduled Tasks.

- Keep endpoints patched and run reputable anti-malware with web filtering; isolate and

reimage if integrity is uncertain.