Q

# QakBot (Qbot): Detection, Containment, and Recovery

QakBot is a modular Windows malware family associated with credential theft and follow-on attacks. Detection requires an incident response, not just file removal.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

## In this guide

01 What is QakBot?
02 What QakBot can do
03 Signs that need investigation
04 What to do after a detection
05 How to reduce the risk
06 Sources

**Quick answer:** QakBot, also called Qbot or Pinkslipbot, is a modular Windows malware family that evolved from a banking Trojan into an initial-access and malware-delivery platform. A detection can mean that credentials, email data, or browser sessions were exposed and that another payload was installed. Isolate the device, preserve evidence, revoke exposed sessions, and investigate the wider environment before restoring it.

## 01 What is QakBot?

QakBot has been observed stealing credentials and data, enumerating networks, moving laterally, and delivering additional tools or ransomware. Historically, campaigns frequently used malicious email links or attachments, including replies inserted into stolen email conversations. The familiar context made the message more convincing, but delivery methods can change; a filename or email theme is not a reliable long-term indicator.

The FBI-led Operation Duck Hunt disrupted QakBot infrastructure in August 2023 and issued an uninstaller to identified bots. That action was significant, but it did not remove other malware already delivered to those computers. A May 2025 U.S. court filing also said people connected with the conspiracy continued seeking access through other techniques after the disruption. Therefore, neither an old QakBot alert nor the takedown itself proves a system is safe.

## 02 What QakBot can do

- **Steal access:** collect account credentials, browser or email information, cookies, and other authentication material.
- **Survey a network:** gather host, user, domain, and security information useful for further intrusion.
- **Provide remote access:** receive commands and load modules on an infected endpoint.
- **Deliver another payload:** QakBot infections have preceded ransomware and other hands-on-keyboard activity.

## 03 Signs that need investigation

An antivirus alert is the clearest signal, but an absence of visible symptoms is not proof of safety. Review email telemetry for unexpected archive, shortcut, disk-image, or document delivery; endpoint records for unusual child processes, scheduled tasks, script interpreters, or binaries in user-writable folders; and identity logs for new devices, impossible travel, session reuse, or mailbox-rule changes. Network defenders should correlate the time of the first alert with DNS, proxy, EDR, and authentication events.

Do not copy old domain or IP lists into permanent block rules and assume the hunt is complete. Infrastructure rotates, and an address may later be reassigned. Use current indicators from the security product or incident report, then search for behavior and affected identities.

## 04 What to do after a detection

1. Disconnect the affected computer from wired, wireless, and VPN networks without powering it off if evidence collection is required.
2. Record the alert name, time, user, file path, process tree, email, and network connections. Preserve relevant logs and the original message safely.
3. From a known-clean device, reset exposed credentials, revoke active sessions and tokens, review MFA methods, and inspect mailbox forwarding and application grants.
4. Hunt across other endpoints for the same delivery chain, credential access, remote administration, lateral movement, and follow-on payloads.
5. Reimage high-value systems or systems whose integrity cannot be established. Restore only clean data and patch the original entry path.

For organizations, a QakBot alert should be handled as a possible breach. Notify the incident-response team, preserve evidence needed for legal or regulatory duties, and contact financial institutions promptly if payment or banking access may have been exposed.

## 05 How to reduce the risk

Use phishing-resistant MFA where possible, block risky attachment types, disable Office macros from internet-originated files, keep browsers and operating systems patched, and restrict script interpreters and user-writable execution. EDR, centralized email logs, protected backups, and tested response playbooks reduce the time between initial access and containment.

## 06 Sources

Technical behavior and response guidance are based on the CISA and FBI QakBot advisory and the U.S. Department of Justice Operation Duck Hunt announcement.

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**