I

IcedID (BokBot): Banking Trojan and Malware Loader

IcedID, also called BokBot, evolved from banking malware into a modular access and payload-delivery platform. Learn what it can do, how infections unfold, and how defenders should respond.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What IcedID does
02 A typical infection chain
03 Why an IcedID alert is serious
04 Possible warning signs
05 Incident response
06 Prevention priorities
07 Frequently asked questions

IcedID, also known as **BokBot**, is modular Windows malware first associated with online-banking theft. It has also been used to establish access, steal browser information, and deliver additional tools. An IcedID infection should be treated as a possible entry point for

a larger intrusion, not only as a banking-password problem.

01 What IcedID does

Capabilities vary by version and campaign, but documented IcedID activity has included collecting system details, stealing credentials or browser data, manipulating web sessions, communicating with command-and-control infrastructure, and deploying secondary payloads. Its modular design allows operators to change the next stage without changing the initial infection method.

Historically, IcedID used techniques aimed at financial sessions, including web injection or traffic redirection. Later operations emphasized loader and access functions. That evolution explains why current descriptions may call it a banking Trojan, a loader, or a backdoor-like access platform.

02 A typical infection chain

1. **Delivery:** a user receives a convincing phishing message, follows a malicious link, or opens an archive or document lure.
2. **Initial execution:** a script, shortcut, installer, or another loader starts the IcedID component. Delivery methods change, so a single attachment type is not a permanent indicator.
3. **Establishment:** the malware gathers host information, creates or uses a persistence method, and contacts attacker-controlled infrastructure.
4. **Credential and session access:** browser information, cookies, credentials, and financial sessions may be targeted.
5. **Follow-on activity:** operators can deliver reconnaissance tools or other malware and use the foothold for lateral movement or extortion.

03 Why an IcedID alert is serious

- The first file found may be only one component of a multi-stage chain.
- Stolen browser sessions can remain useful even after a password is changed; sessions and tokens must also be revoked.
- A convincing reply inside a previously stolen email conversation can bypass a recipient’s normal suspicion.
- Follow-on tools may appear under different detection names, on other endpoints, or days after initial access.

04 Possible warning signs

- An endpoint alert naming IcedID, BokBot, or a related loader component.
- Office applications, archive utilities, scripts, or shortcuts launching unusual child processes.
- Unexpected scheduled tasks, registry run entries, DLL loading, or process injection alerts.
- Connections to newly observed domains or unusual encrypted traffic from user workstations.
- Unrecognized account sessions, mailbox rules, financial activity, or authentication attempts.

No single symptom proves IcedID. Confirm the process tree, file hashes, network destinations, persistence artifacts, and user activity for the affected time window.

05 Incident response

1. **Isolate the endpoint immediately.** Keep it away from internal resources and the internet while preserving evidence required by your response process.
2. **Identify the initial message or download.** Search other mailboxes and endpoints for the same sender, URL, attachment, hash, or execution pattern.
3. **Scope the intrusion.** Review endpoint, DNS, proxy, identity, email, and remote-access logs. Hunt for additional payloads and movement to servers or privileged accounts.

4. **Revoke access.** From a clean device, reset exposed credentials and revoke browser, email, VPN, cloud, and financial sessions. Rotate secrets stored or used on the host.
5. **Eradicate and recover.** Reimage systems when the chain or follow-on activity cannot be ruled out. Restore only verified data, patch the entry point, and monitor for recurrence.

06 Prevention priorities

Filter dangerous attachments and links, block unnecessary script and macro execution, patch browsers and document tools, and use multifactor authentication that resists phishing where possible. Endpoint detection should monitor suspicious child processes, injection, persistence, and credential access. Segment user workstations from critical servers and restrict administrative privileges so one infected account cannot easily become a network-wide incident.

07 Frequently asked questions

Is IcedID the same as BokBot?

Yes. BokBot is an alternate name commonly used for the IcedID malware family.

Does antivirus removal finish the response?

Not necessarily. If IcedID ran, responders must also check for stolen sessions, other payloads, persistence, and activity on neighboring systems.

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