I

IcedID (BokBot): Banking malware, infection chain, and response

What it is IcedID, also called BokBot, is modular Windows malware that began as a banking Trojan and later became a common access and delivery platform for broader cybercrime. It can steal browser and financial information, collect...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

IcedID, also called BokBot, is modular Windows malware that began as a banking Trojan and later became a common access and delivery platform for broader cybercrime. It can steal browser and financial information, collect system data, and provide a foothold for additional tools or ransomware.

How it works

Campaigns have used malicious email threads, password-protected archives, document lures, fake updates, and loaders. Once active, IcedID establishes persistence and communicates with command infrastructure. Operators can deploy modules, steal cookies or credentials, and hand access to another criminal group for lateral movement and extortion.

Key points

- A reply inside a genuine stolen email conversation can make the malicious attachment unusually convincing.
- The first detected loader may be only one stage of an infection that already includes other tools.
- Browser cookies and sessions may remain valuable to attackers after a password change.

What to do

- Isolate the endpoint and review email, process, PowerShell, scheduled-task, and network evidence.
- Revoke sessions and reset credentials from a clean device after the endpoint is contained.
- Hunt across the environment for the same message, hash, domain, and persistence pattern.
- Restore from trusted media or reimage when follow-on activity cannot be ruled out.

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