F

FormBook Malware (XLoader): Credential Theft and Response

FormBook, now commonly associated with XLoader, is an information stealer that can capture credentials, keystrokes, screenshots, and form data. Learn how to contain and respond.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 What can FormBook steal or do?
02 How FormBook infections start
03 Possible signs of FormBook or XLoader
04 What to do after a FormBook detection
05 Organization-wide investigation
06 How to reduce the risk
07 Frequently asked questions
08 Authoritative sources

FormBook is an information-stealing malware family used to capture credentials and other sensitive data from infected Windows systems. The closely related successor is commonly tracked as XLoader; MITRE ATT&CK notes that XLoader was previously known and is still sometimes referred to as FormBook. Naming varies across detections and reports, so defenders should search for both names.

Removing the detected executable is only part of the response. If FormBook or XLoader ran, assume that passwords, browser data, email or FTP credentials, clipboard contents, keystrokes, screenshots, and session information accessible on the device may have been exposed.

01 What can FormBook steal or do?

- Log keystrokes and monitor clipboard content.
- Capture screenshots and information entered into web forms.
- Collect credentials and data from supported browsers, email clients, and FTP applications.
- Record system and user information for victim profiling.
- Receive commands from command-and-control infrastructure.
- Download and execute additional files, expanding the incident beyond the initial stealer.

The exact capabilities depend on the version and campaign. A detection name does not reveal which data was successfully stolen; incident response must use execution evidence, network telemetry, identity logs, and the applications present on the host.

02 How FormBook infections start

Campaigns commonly use phishing messages that imitate invoices, purchase orders, shipment notices, quotations, or payment documents. Attachments or links may deliver archives, disk images, documents, scripts, or executables. Attackers change file types and loaders over time, so a fixed list of extensions is not a reliable defense.

Evidence	Likely stage	Response priority

Attachment blocked before opening	Delivery attempt	Remove the message, hunt for other recipients, and verify no execution
File downloaded but not run	Payload present	Quarantine it and confirm with endpoint telemetry
Process, persistence, or command-and-control activity	Execution or active compromise	Isolate the host and begin credential and incident response
Login anomalies after the alert	Possible account misuse	Revoke sessions, reset credentials, and investigate access
Additional malware detections	Follow-on payload	Expand the scope and consider rebuilding the system

03 Possible signs of FormBook or XLoader

- An endpoint alert naming FormBook, XLoader, an infostealer, keylogger, or suspicious loader.
- A recently opened invoice or archive followed by a process launched from Downloads, Temp, AppData, or another user-writable directory.
- Unexpected outbound traffic from a process that normally does not contact the internet.
- New startup entries, scheduled tasks, or other persistence near the time of the phishing message.
- Unfamiliar account logins, mailbox rules, token use, or password-reset activity.

There may be no visible symptoms. Infostealers are designed to operate quietly, and the absence of pop-ups or slowness is not evidence that data remained safe.

04 What to do after a FormBook detection

1. **Isolate the device.** Disconnect it from networks or use endpoint containment, especially if execution is confirmed or uncertain.

2. **Preserve evidence.** Record the alert, path, hash, process tree, user, timestamps, email, URL, and network connections before cleanup.
3. **Run updated scans.** Quarantine detected components and check for loaders, persistence, and additional payloads. An offline scan can help with stubborn threats.
4. **Protect accounts from a clean device.** Revoke active sessions and tokens first, then change passwords used or stored on the affected computer. Prioritize email, password managers, financial accounts, remote access, and administrator credentials.
5. **Review identity activity.** Check logins, mailbox forwarding rules, consent grants, recovery settings, and suspicious transactions.
6. **Rebuild when trust cannot be restored.** Reimage from known-good media if the stealer ran, additional payloads appeared, persistence remains, or complete investigation is unavailable.

Do not use the suspected computer to change passwords: malware could capture the new credentials. Password changes alone are also insufficient when an attacker has active sessions, refresh tokens, API keys, or application-specific passwords.

05 Organization-wide investigation

- Search mailboxes for the sender, subject, attachment hash, URL, and similar message patterns.
- Identify every recipient and determine who opened or executed the content.
- Hunt endpoint and network telemetry for both FormBook and XLoader indicators, parent-child process patterns, persistence, and secondary downloads.
- Review authentication logs for affected users and for credentials used on the host.
- Block confirmed malicious infrastructure and hashes, while remembering that campaigns rotate them.
- Preserve required evidence and follow breach-notification, legal, and regulatory procedures when data exposure is plausible.

06 How to reduce the risk

- Filter dangerous attachments and detonate suspicious content before delivery.
- Block executable content from common user-writable and archive extraction paths where business needs allow.
- Patch operating systems, browsers, document tools, and email clients.
- Use multifactor authentication resistant to phishing and restrict legacy authentication.
- Apply least privilege and separate administrator accounts from email and browsing.
- Monitor unusual process chains, credential access, and outbound connections rather than relying only on filenames.

07 Frequently asked questions

Are FormBook and XLoader the same?

XLoader is widely described as the successor to FormBook, and some sources or products still use the older name. Treat either detection as an information-stealer incident and use both names during threat hunting.

Is FormBook a banking Trojan?

It can steal credentials that enable financial fraud, but it is more accurately described as a general information stealer and form grabber rather than only a banking Trojan.

Is deleting the detected file enough?

No if it ran. The response must address stolen credentials and sessions, possible persistence, other payloads, and account misuse.

08 Authoritative sources

- MITRE ATT&CK: XLoader (S1207)
- Google Cloud / Mandiant: FormBook malware distribution campaigns

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