H

HawkEye Keylogger and Stealer: What It Collects and How to Recover

HawkEye is a Windows credential stealer and keylogger distributed through phishing campaigns. Learn what it can collect, how exfiltration works, and which accounts must be secured.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What HawkEye can collect
02 How HawkEye infections begin
03 Possible warning signs
04 How to remove HawkEye
05 Account recovery from a clean device
06 Frequently asked questions

HawkEye is a Windows credential-stealing malware family commonly described as a keylogger or stealer. Public campaign analyses show that it can record keystrokes, collect credentials from browsers and email applications, gather system information, and send stolen data to an attacker. It has often been delivered through targeted phishing

attachments.

Why removal is not enough: cleaning the executable does not invalidate passwords, cookies, email credentials, or other information already captured. Recover the device and the affected accounts as two separate tasks.

01 What HawkEye can collect

Data or capability	Potential impact
Keystrokes	Passwords, messages, payment details, and searches typed while active
Browser credentials	Access to websites and reused passwords
Email and FTP credentials	Mailbox takeover, further phishing, and access to hosted files
Clipboard and system information	Copied secrets and details useful for targeting the victim
Screenshots or form data in some variants	Information visible even when it is not stored as a password
Additional payload execution	A wider infection than the HawkEye alert alone reveals

Capabilities vary by version and configuration. Microsoft noted that HawkEye “Reborn” was more than a simple keylogger, while Mandiant documented variants sending collected credentials through email or FTP. The exact exfiltration route should be confirmed from network and endpoint evidence.

02 How HawkEye infections begin

Campaigns frequently use business-themed phishing: invoices, purchase orders, shipping documents, job material, or other attachments designed to look routine. The attachment or embedded object starts a script or executable, which then launches the HawkEye payload. Repacked software and malicious downloads are also possible.

1. The user opens a malicious attachment or file.
2. A loader or exploit starts an obfuscated .NET payload.
3. HawkEye establishes execution or persistence and collects selected data.
4. Credentials and system details are sent using a configured channel such as SMTP, FTP, or web traffic.
5. The stolen mailbox or password may be used for additional phishing and account access.

03 Possible warning signs

- a security detection for HawkEye, HawkEyeKeylogger, a generic keylogger, or a credential stealer;
- an office or archive process launching an unexpected executable from a temporary folder;
- outbound SMTP or FTP traffic from a workstation that should not send it directly;
- small text or log-like files created and deleted around suspicious activity;
- unrecognized email forwarding, sent messages, sign-ins, or MFA prompts;
- new startup entries, tasks, or processes with misleading names.

HawkEye is intended to remain quiet. The absence of obvious pop-ups or performance problems does not show that credentials are safe.

04 How to remove HawkEye

1. **Isolate the computer.** Disconnect it from networks to interrupt ongoing exfiltration and payload delivery.
2. **Preserve the attack evidence.** Save the original message, attachment, full headers, process tree, detected file path and hash, persistence, and network destinations.
3. **Quarantine and scan.** Update the security tool, run a full scan, restart, and use an offline scan when persistence or privileged activity is suspected.

4. **Search for companion malware.** Review files and processes created at the same time, scheduled tasks, startup entries, and additional security alerts.
5. **Remove the initial path.** Delete the malicious message from other mailboxes, block its sender and indicators, and patch the exploited application.
6. **Rebuild when trust cannot be established.** This is especially important after administrator use, additional backdoor detections, or incomplete forensic visibility.

05 Account recovery from a clean device

1. Reset the primary email and password-manager credentials first.
2. Revoke active sessions, remembered devices, app passwords, refresh tokens, and API keys.
3. Change browser, VPN, cloud, financial, and work credentials used or stored on the endpoint.
4. Enable MFA after changing the primary password, preferably using a phishing-resistant method.
5. Review mailbox forwarding, inbox rules, recovery addresses, delegated access, and sent mail.
6. Warn contacts if the compromised mailbox sent messages and search the organization for the same lure.

Changing passwords on the infected computer can expose the new values to the keylogger. Always use a separate trusted device.

06 Frequently asked questions

Is HawkEye only a keylogger?

No. Documented versions also extract stored credentials and system data and can use several methods to send it out.

Can MFA prevent all damage?

MFA reduces password-only takeover but cannot undo stolen session tokens, mailbox data, or credentials for services without MFA. Revoke sessions and review account changes.

Should I monitor only the infected user?

No. Search for the same phishing message, attachment hash, sender, process pattern, and exfiltration destination across other users and endpoints.

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