GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

G

Gootkit and GootLoader: Infection, Detection, and Response

Gootkit began as a banking Trojan, while GootLoader is a related JavaScript initial-access family spread through poisoned search results. Learn how to contain and investigate both.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	4 min

CONTENTS

In this guide

01 Gootkit vs GootLoader

02 How a GootLoader infection begins

03 How to interpret an alert

04 Possible warning signs

05 What to do after a Gootkit or GootLoader detection

06 Organization-wide hunting

07 How to reduce risk

08 Frequently asked questions

09 References

Gootkit is historically a Windows banking Trojan and credential-stealing malware family; GootLoader is a related JavaScript-based initial-access family that developed from the same lineage. Modern reports frequently focus on GootLoader because it uses poisoned search results and compromised websites to deliver scripts that can establish persistence and install additional tools or malware.

The names are related but not interchangeable. A GootLoader alert may represent the delivery chain rather than the original Gootkit banking payload. Defenders should search for both names, determine which stage executed, and investigate any secondary payload.

01 Gootkit vs GootLoader

Name	Primary role	Typical risk
Gootkit	Banking Trojan and information stealer	Credential and financial data theft, remote control, additional malware
GootLoader	JavaScript loader and initial-access malware	Persistence and delivery of Cobalt Strike, ransomware, stealers, or other payloads
Gootkit Loader	Older or overlapping reporting term	May refer to the loader stage associated with Gootkit

Detection vendors may use family or generic names differently. The file path, script content, process tree, registry changes, and network activity are more useful than relying on the label alone.

02 How a GootLoader infection begins

1. A victim searches for a business document such as a contract, agreement, template, or legal form.
2. Search poisoning leads to a compromised site containing a fake forum or download page tailored to the query.

3. The victim downloads an archive that appears to contain the requested document but includes an obfuscated JavaScript file.
4. Opening the script launches a Windows scripting process and establishes persistence.
5. Later stages retrieve or reconstruct payloads and give the operator a foothold for further intrusion.

Campaigns change their lures, obfuscation, filenames, and payloads. A high Google position, HTTPS padlock, familiar website, or realistic forum comments do not make a download trustworthy.

03 How to interpret an alert

Evidence	Likely stage	Response
ZIP or JavaScript blocked before opening	Delivery attempt	Quarantine, remove the download, and verify no execution
Script host launched from Downloads or extracted archive	Execution	Isolate the device and start incident response
Scheduled task, logon script, or unusual registry data	Persistence	Preserve evidence and hunt for later stages
Cobalt Strike, RAT, stealer, or ransomware alert	Follow-on compromise	Expand scope to identities, network, servers, and data
Suspicious logins or banking activity	Possible credential misuse	Revoke sessions and contact affected providers

04 Possible warning signs

- A downloaded document template arrives as ZIP, JavaScript, or another executable content type.

- `wscript.exe`, `cscript.exe`, PowerShell, or another interpreter launches from a browser or archive workflow.
- Obfuscated scripts or staged files appear in a user's AppData directory.
- New scheduled tasks, logon persistence, registry blobs, or outbound connections appear after the download.
- Endpoint protection reports GootLoader, Gootkit, a loader, Cobalt Strike, or a secondary payload.

There may be no visible symptoms. The operation is designed to turn an ordinary web search into quiet initial access.

05 What to do after a Gootkit or GootLoader detection

1. **Contain the endpoint.** Isolate it from networks when the script ran or execution cannot be ruled out.
2. **Preserve context.** Save the search query, URL, downloaded archive, hashes, process tree, user, timestamps, persistence, and network destinations.
3. **Run current security scans.** Quarantine identified components, but do not assume that deleting the initial script removes later stages.
4. **Hunt for payloads and attacker activity.** Review interpreters, scheduled tasks, registry changes, remote tools, credential access, lateral movement, and exfiltration.
5. **Protect identities from a clean device.** Revoke sessions and tokens, then rotate credentials used or stored on the affected computer.
6. **Rebuild when trust is lost.** Reimage from known-good media when execution and persistence occurred, a remote-access payload ran, or complete eradication cannot be shown.

06 Organization-wide hunting

- Search web and DNS telemetry for the source site and similar poisoned downloads.
- Find archive and script hashes, filenames, and browser-to-script-host process chains across endpoints.
- Hunt for the observed persistence mechanism and follow-on command-and-control traffic.
- Review affected identities, administrator activity, remote access, and systems reachable from the endpoint.
- Block confirmed indicators while recognizing that compromised sites and infrastructure rotate.

07 How to reduce risk

- Obtain legal and business templates from trusted primary sources, not anonymous forum downloads.
- Show file extensions and block JavaScript and other executable content from internet archives where possible.
- Use application control and restrict script interpreters for users who do not need them.
- Monitor browser and archive tools spawning script engines or command shells.
- Keep browsers, operating systems, and security tools updated and use least privilege.

08 Frequently asked questions

Is GootLoader the same as Gootkit?

No. They share a lineage, but GootLoader is primarily an initial-access JavaScript loader, while Gootkit is known as a banking Trojan and information stealer.

Can GootLoader lead to ransomware?

Yes. It can deliver tooling or malware used in later ransomware activity, although the exact follow-on payload varies by campaign.

Is deleting the downloaded ZIP enough?

Only if reliable telemetry shows the content never executed. If the script ran, investigate persistence, payloads, credentials, and attacker access.

09 References

- Microsoft Security Intelligence: GootLoader
- Red Canary Threat Detection Report: GootLoader
- Palo Alto Networks Unit 42: Dissecting GootLoader

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