

Gootloader Returns: Malware Hidden in Google Ads for Legal Documents

By gootloadersites

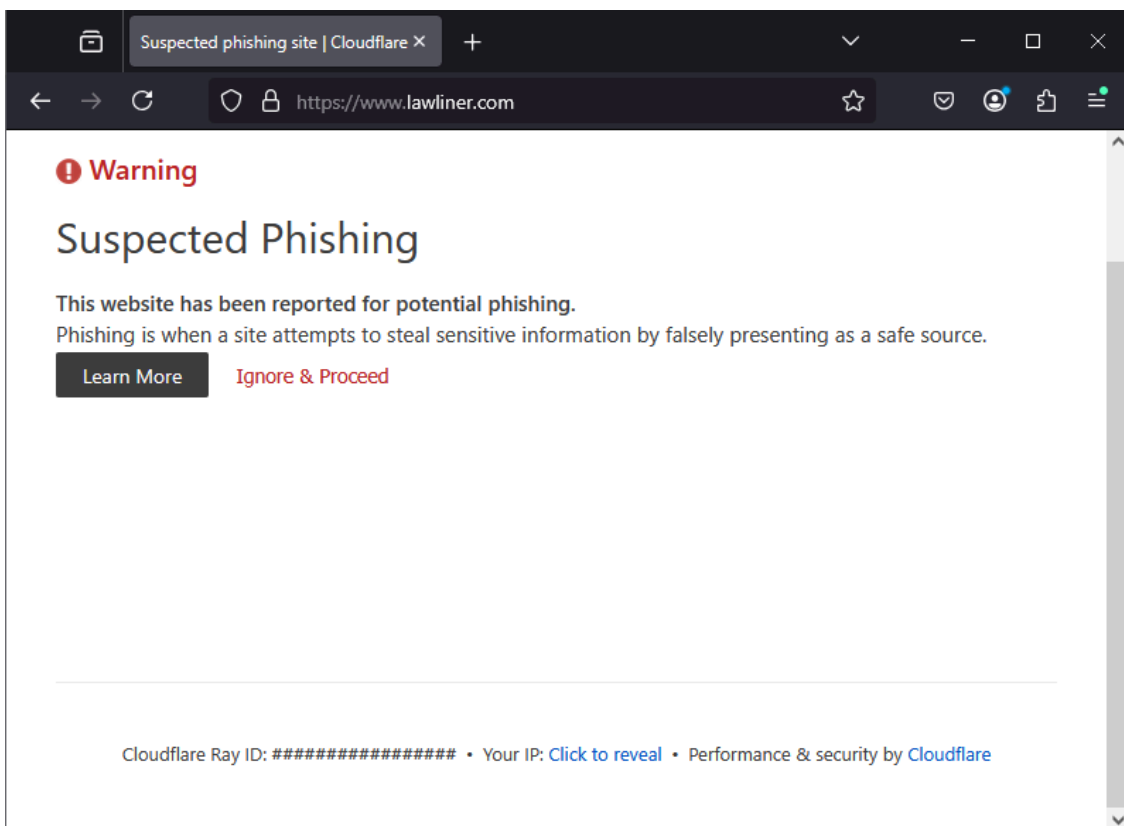
Published: 2025-03-31 · Archived: 2026-04-06 01:34:22 UTC

Update (31 Mar 2025 @ 822 PDT)

Thanks to Vultr for taking down skhm[.]jorg!

Update (31 Mar 2025 @1016 PDT)

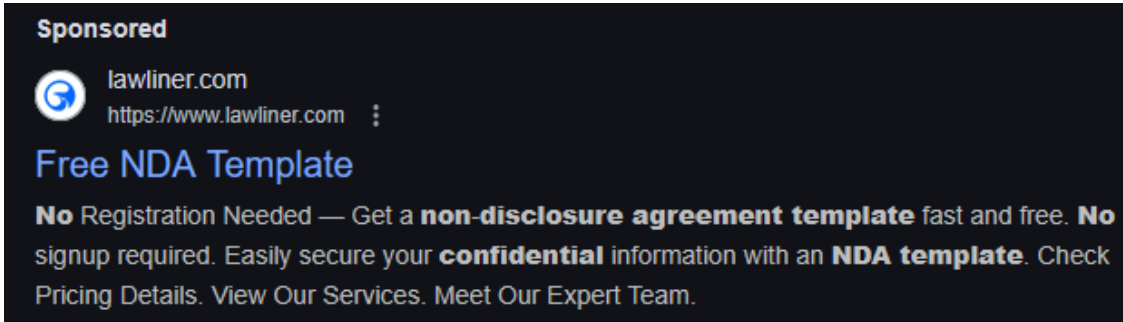
Thanks to CloudFlare for flagging lawliner[.]com!



The threat actor behind the Gootloader malware has once again changed their tactics, but also reverted to some of their old ways. Just like with the previous infection method, we are seeing Google Ads being used to target victims. But this time it is using a familiar lure.

The threat actor is advertising legal templates, mainly around agreements. If this sounds familiar, for a very long period, Gootloader had over 5 million legal terms poisoned on compromised WordPress blogs. Now it looks like they have stood up their own infrastructure to deliver the malware. Let me walk you through the infection process.

First it starts with a Google search for a legal template. For example “non disclosure agreement template”. Then the user will see an advertisement from lawliner[.]com.



These are being delivered by the advertiser “MED MEDIA GROUP LIMITED”, which I assume has been compromised. Here is a link to their other advertisements:

<https://adstransparency.google.com/advertiser/AR15344130772197965825>.

Once the user clicks on the malicious advertisement from lawliner[.]com and lands on said page, they are presented with a button to “Get document” and are prompted to enter their email address.

Non Disclosure Agreement Nda

Access a professional non disclosure agreement (NDA) template to safeguard confidential information. Easy to customize and ready for immediate use!

Get Document

Non-Disclosure Agreement

This Non-Disclosure Agreement, herein referred to as the “Agreement,” represents an essential and legally binding understanding formalized between the involved parties with the primary purpose of ensuring the confidentiality and protection of vital information exchanged or disclosed during the course of their business relationship. The agreement acts as a definitive contract that requires the strict non-disclosure of proprietary details and confidential information to safeguard the interests, intellectual property, and business processes of the concerned parties. By executing this document, the involved parties consent to uphold stringent confidentiality obligations, thereby preserving the secrecy of commercially sensitive information and mitigating unauthorized access or potential misuse by third parties. The Agreement serves as a crucial instrument in establishing a secure framework within which the parties can freely share valuable insights, ideas, and information necessary for their collaborative efforts without fear of disclosure or competitive disadvantage. Furthermore, by entering into this Agreement, the parties collectively affirm their mutual understanding of the terms and conditions delineated herein, ensuring compliance with the clauses set forth in order to promote a fruitful and long-lasting exchange of information.

This Non-Disclosure Agreement (the “Agreement”) is entered into as of [Disclose Date] by and between [Disclosing Party Name], having its principal place of business at [Disclosing Party Address] (hereinafter referred to as “Disclosing Party”), and [Receiving Party Name], with its principal place of business located at [Receiving Party Address] (hereinafter referred to as “Receiving Party”). This Agreement seeks to formalize a mutually binding understanding and commitment between the concerned parties, outlining the legal obligations of confidentiality and ensuring the safeguarding of sensitive information conveyed during their business interaction. The parties hereby acknowledge the importance of maintaining the confidentiality of the exchanged details, documents, or disclosures that hold

Send Document to Your Email

We will only use your email to send you the document. No spam, we promise!

Send Document

Shortly after they enter their email, they will receive an email from lawyer@skhm[.]org, with a link to their requested Word document (.docx). Example link: [https://skhm\[.\]org/XYZ/non_disclosure_agreement_nda.docx](https://skhm[.]org/XYZ/non_disclosure_agreement_nda.docx)

If the user passed all of their gates, they will download a zipped .JS file. Following the example above, it would be non_disclosure_agreement_nda.js, and the zipped would be non_disclosure_agreement_nda.zip.

SKHM Secure Document Delivery

Hello,

You recently requested the following document from **SKHM (Store, Keep, Host & Mail)**:

non_disclosure_agreement_nda.docx

To securely download your document, please click the button or link below:

[Download Document](#)

If you did not request this file or believe this email was sent in error, you can safely ignore it.

Best regards,

SKHM (Store, Keep, Host & Mail)

Email: lawyer@skhm.org | Tel: +44 7961 265818

ENDOLE LTD, 153 LODGE ROAD, WEST BROMWICH, WEST MIDLANDS, B70 8PJ, GB

© 2025 ENDOLE LTD. All rights reserved.

Note: You cannot tell from the URL if you are going to be passed the malicious zipped .JS or a benign .docx file.

When the user unzips and executes the .JS file, the same Gootloader behavior occurs. It creates a scheduled task, pointing to a separate .JS file in the user's appdata\roaming folder. It will then run PowerShell, and call out to 10 WordPress blogs (1-2 are actually compromised, the others are false positives).

Here are two samples:

<https://www.virustotal.com/gui/file/5663e22c46d72e04b88c7b223c113aafb5657993dba70428b1badd1fe13c3b34>

<https://www.virustotal.com/gui/file/95baedeb3be98760929c05055e516054db8c396cf5fce92784885f8a802ccc8f>

My recommendation is to block/alert lawliner[.]com and skhm[.]org for web traffic. Additionally, block/alert skhm[.]org from email traffic. Last, I would search through historical events for contacts with the above domains. Stay safe out there and happy hunting!

IOCs:

lawliner[.]com

skhm[.]org