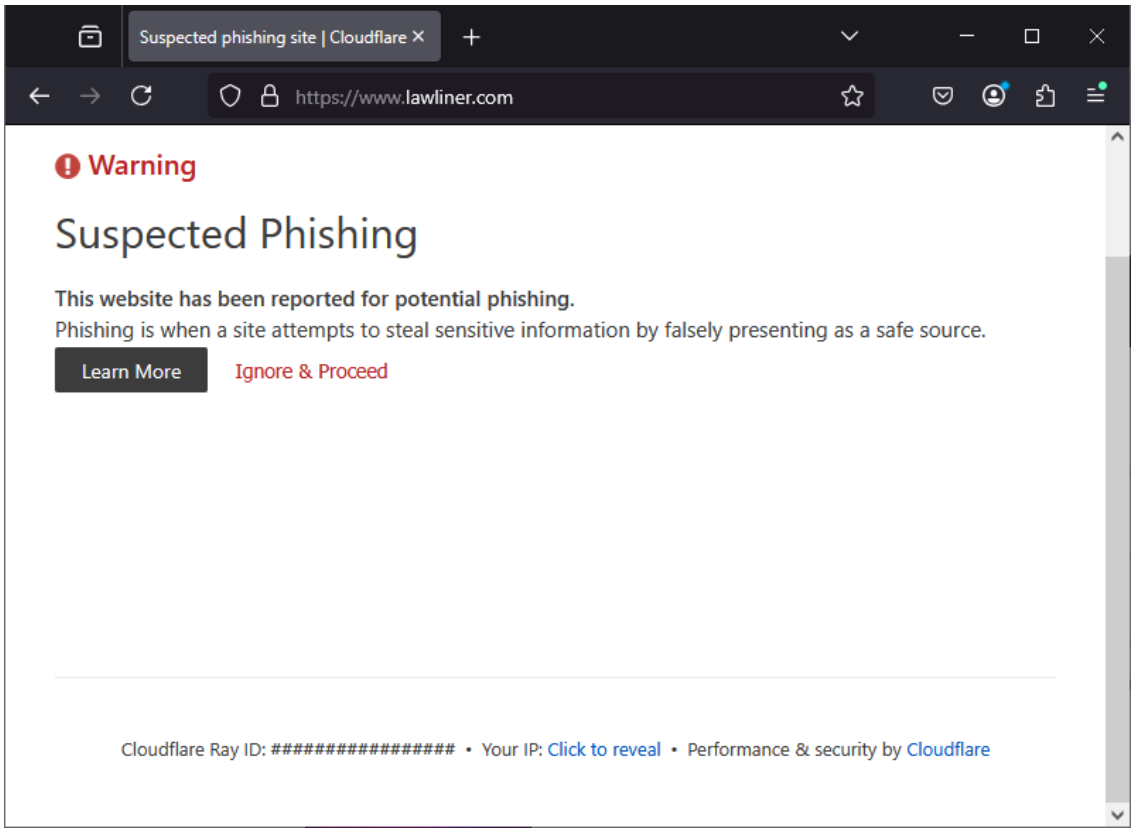
🚨Gootloader Returns: Malware Hidden in Google Ads for Legal Documents

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[.]org!

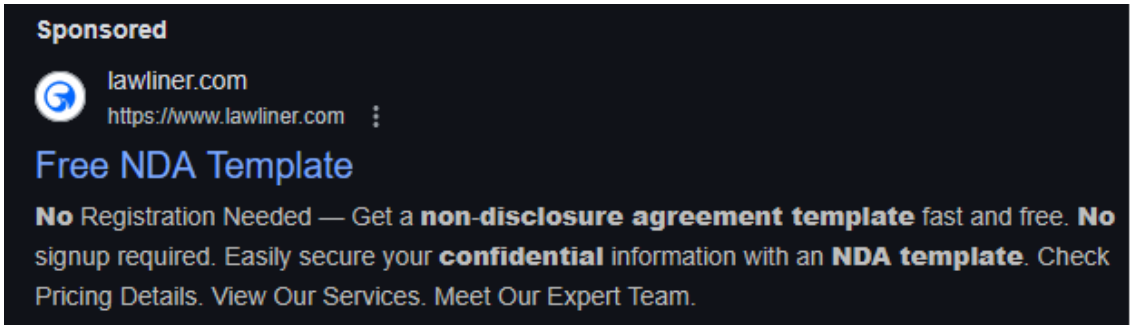
Update (31 Mar 2025 @1016 PDT)
Thanks to CloudFlare for flagging lawliner[.]com!



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.

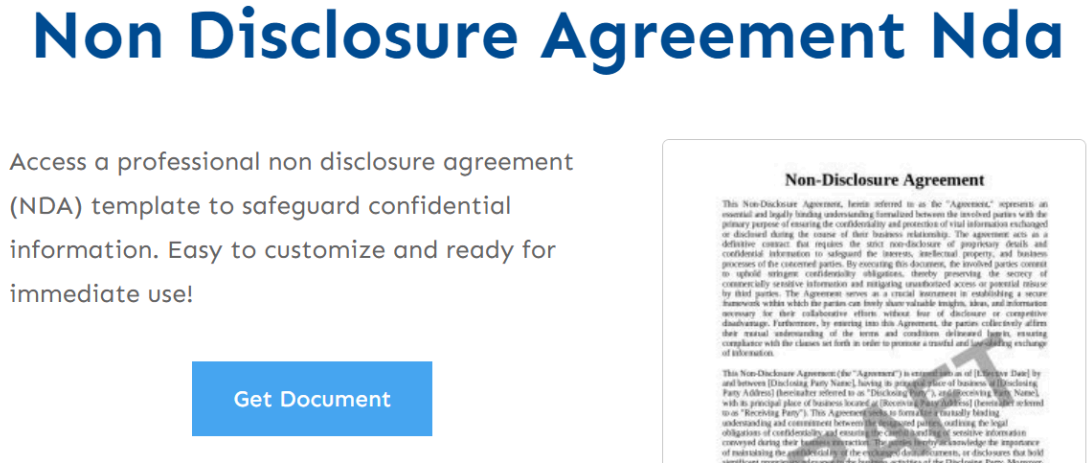
The threat actor is advertising legal templates, mainly around agreements. If this sounds familiar, for a very long period, Gootloader had over 5 million legal terms poisoned on compromised WordPress blogs. Now it looks like they have stood up their own infrastructure to deliver the malware. Let me walk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

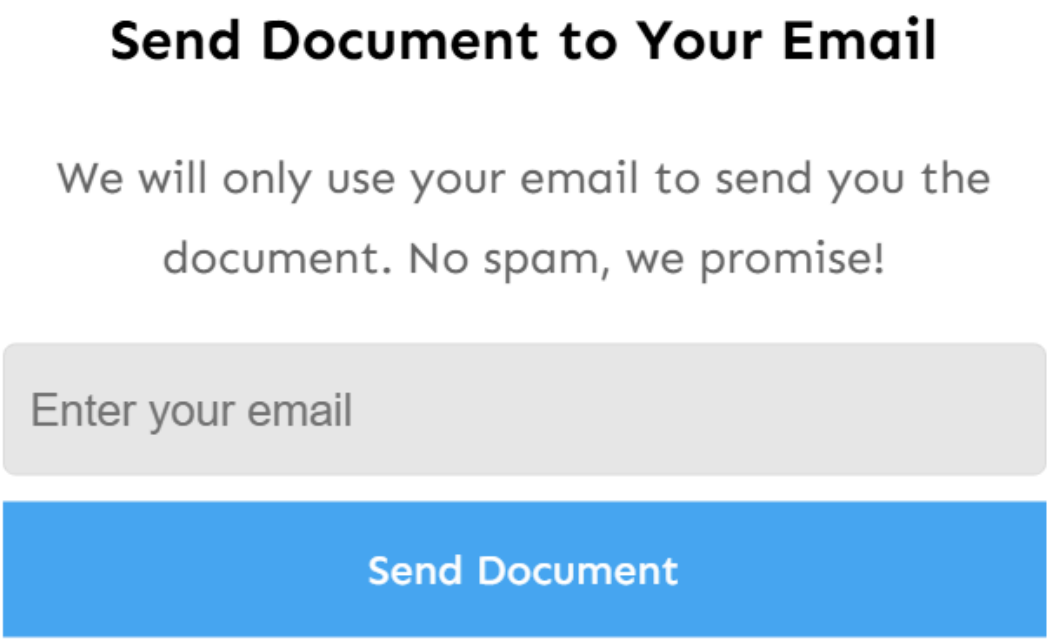
First it starts with a Google search for a legal template. For example “non disclosure agreement template”. Then the user will see an advertisement from lawliner[.]com.



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.

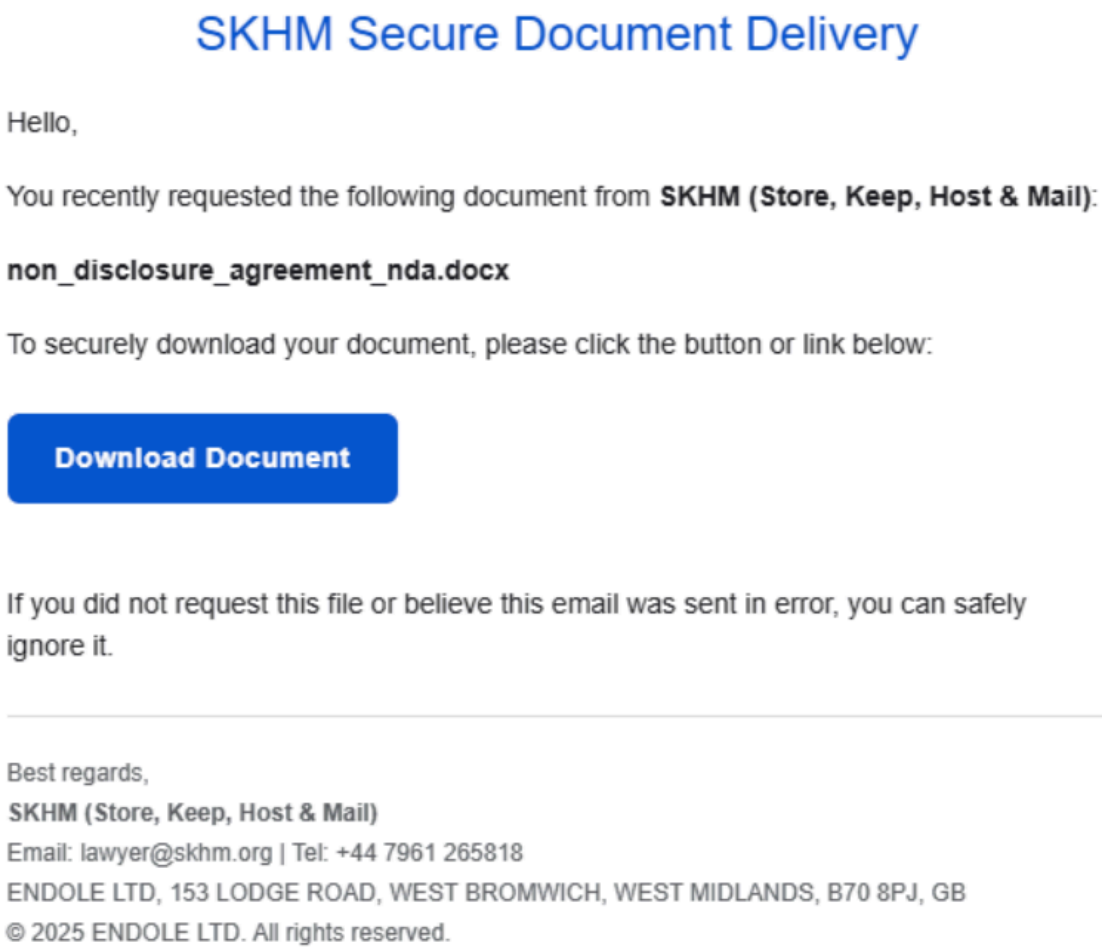
Once the user clicks on the malicious advertisement from lawliner[.]com and lands on said page, they are presented with a button to “Get document” and are prompted to enter their email address.





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

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.



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

Source: https://gootloader.wordpress.com/2025/03/31/gootloader-returns-malware-hidden-in-google-ads-for-legal-documents/