Threat actor impersonates Google via fake ad for Authenticator

By Jérôme Segura

Published: 2024-07-30 · Archived: 2026-04-05 16:54:40 UTC

We have previously reported on the brand impersonation issue with Google ads: users who search for popular keywords are shown malicious ads that purport to be from an official vendor.

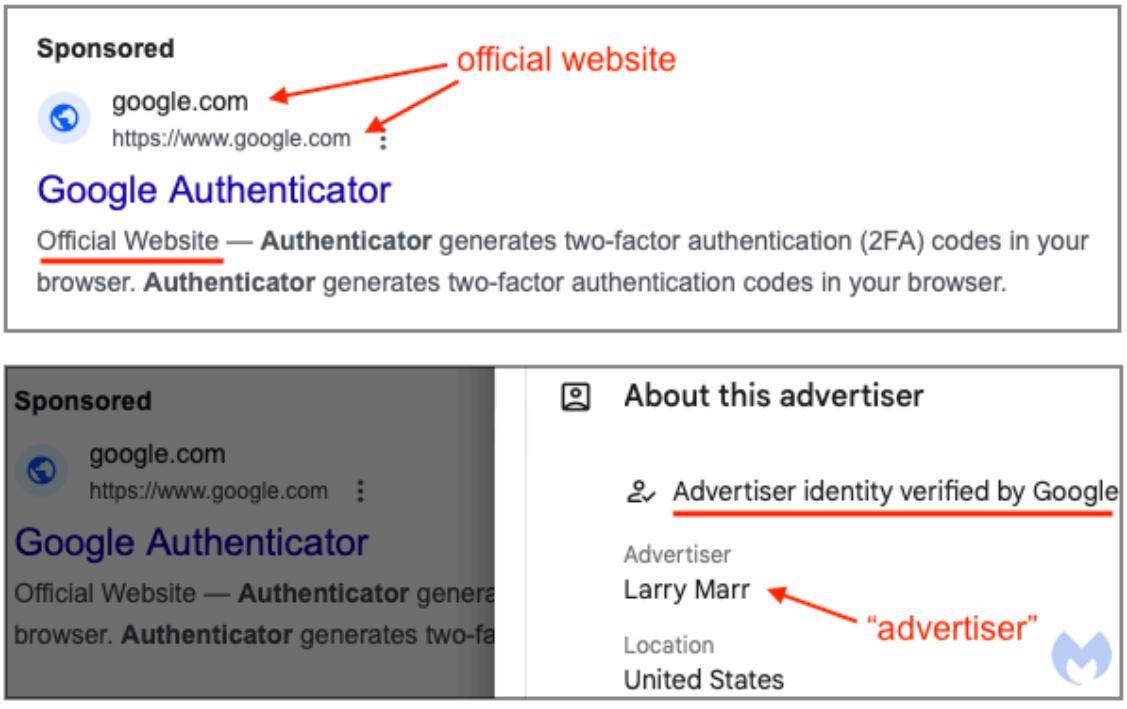
Not only does this trick innocent victims into downloading malware or losing their data to phishing sites, it also erodes trust in brands and by association in Google Search itself.

Today, we show yet another example of brand misuse, except that this one targets Google itself. If you were trying to download the popular Google Authenticator (a multi-factor authentication program) via a Google search in the past few days, you may have inadvertently installed malware on your computer.

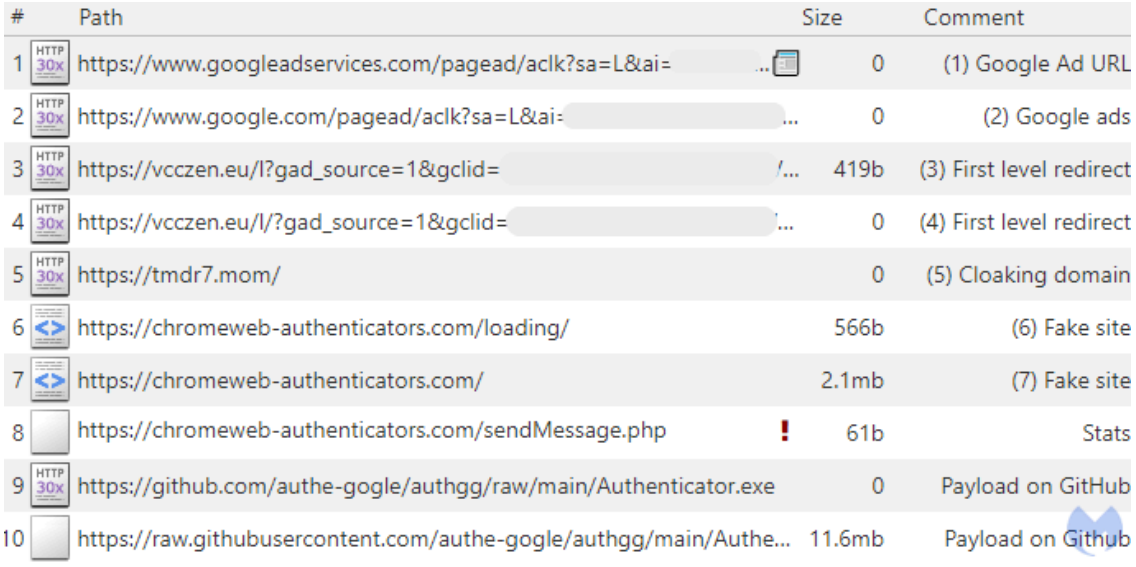
A similar distribution site and the same payload were previously discovered by sandbox maker AnyRun. In this blog post, we will reveal the missing piece at the top of the killchain, namely the Google ad that was involved in tricking users into visiting a decoy website.

Trust, but 'verified'?

The core issue with brand impersonation comes from ads that appear as if they were from official sources and advertisers' identities verified by Google. This was the case here with this ad for Authenticator:



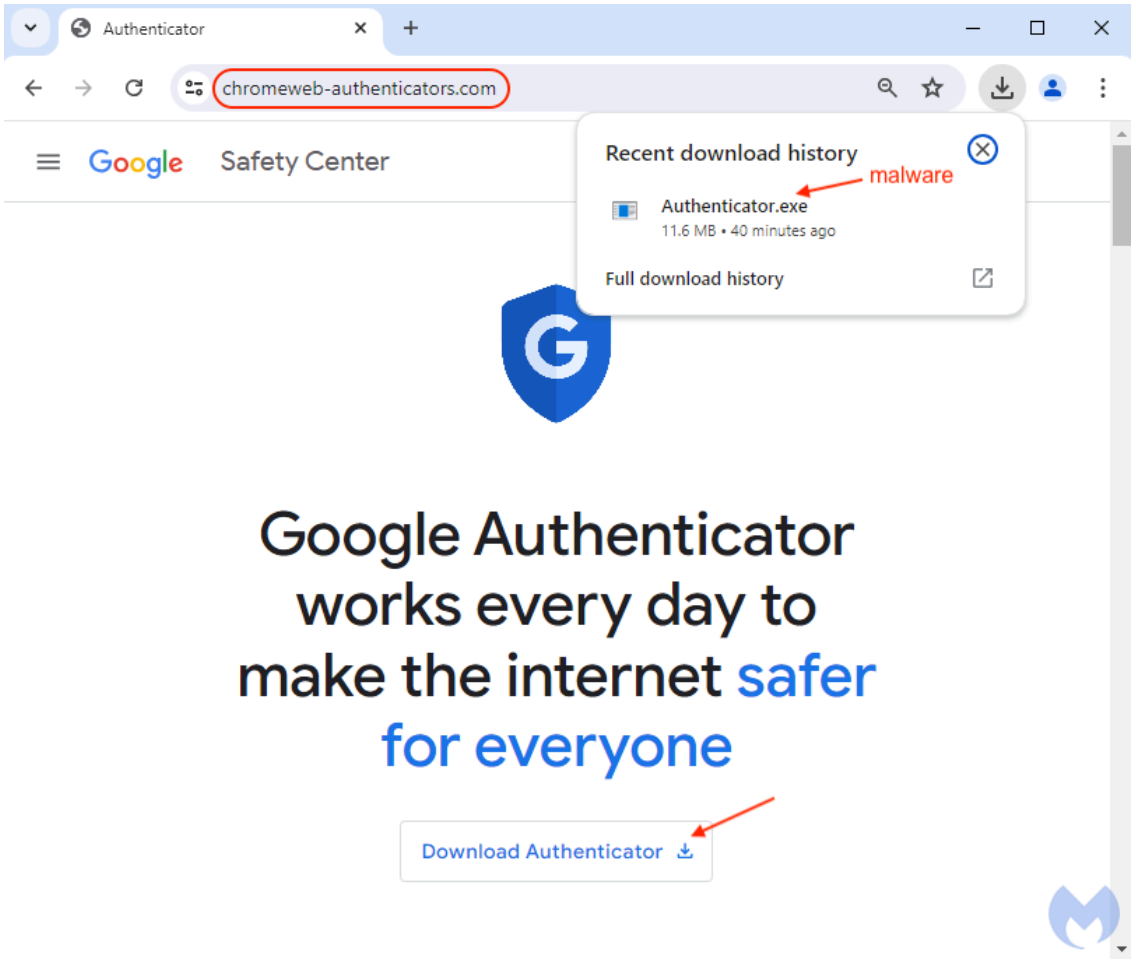
The truth is Larry Marr has nothing to do with Google, and is likely a fake account. We can follow what happens when you click on the ad by monitoring web traffic. We see a number of redirects via intermediary domains controlled by the attacker, before landing on a fake site for Authenticator.



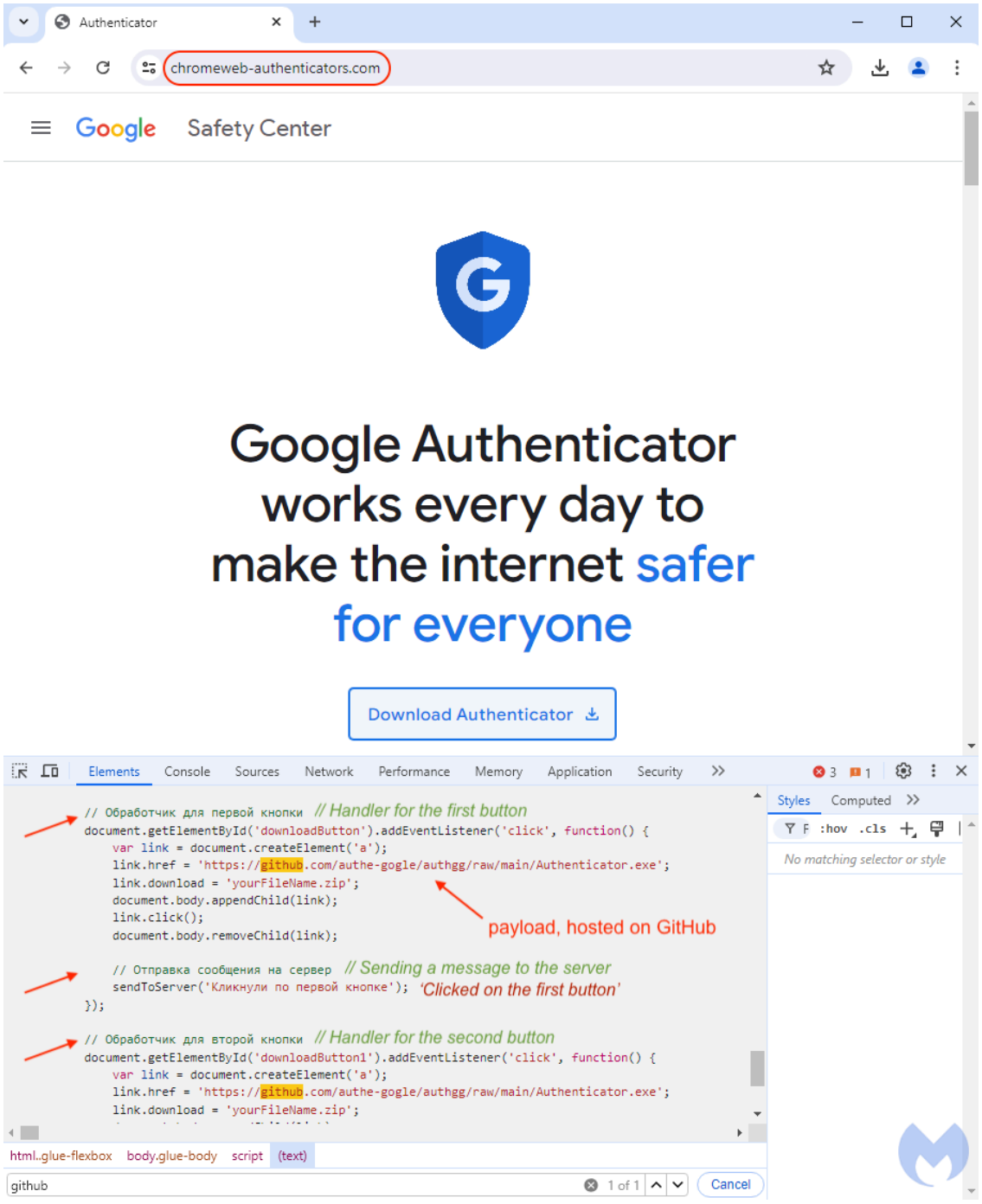
#	Path	Size	Comment
1	https://www.googleadservices.com/pagead/aclk?sa=L&ai=	0	(1) Google Ad URL
2	https://www.google.com/pagead/aclk?sa=L&ai=	0	(2) Google ads
3	https://vcczen.eu/l?gad_source=1&gclid=	419b	(3) First level redirect
4	https://vcczen.eu/l/?gad_source=1&gclid=	0	(4) First level redirect
5	https://tmdr7.mom/	0	(5) Cloaking domain
6	https://chromeweb-authenticators.com/loading/	566b	(6) Fake site
7	https://chromeweb-authenticators.com/	2.1mb	(7) Fake site
8	https://chromeweb-authenticators.com/sendMessage.php	61b	Stats
9	https://github.com/authe-gogle/authgg/raw/main/Authenticator.exe	0	Payload on GitHub
10	https://raw.githubusercontent.com/authe-gogle/authgg/main/Authe...	11.6mb	Payload on Github

Fake site leads to signed payload hosted on Github

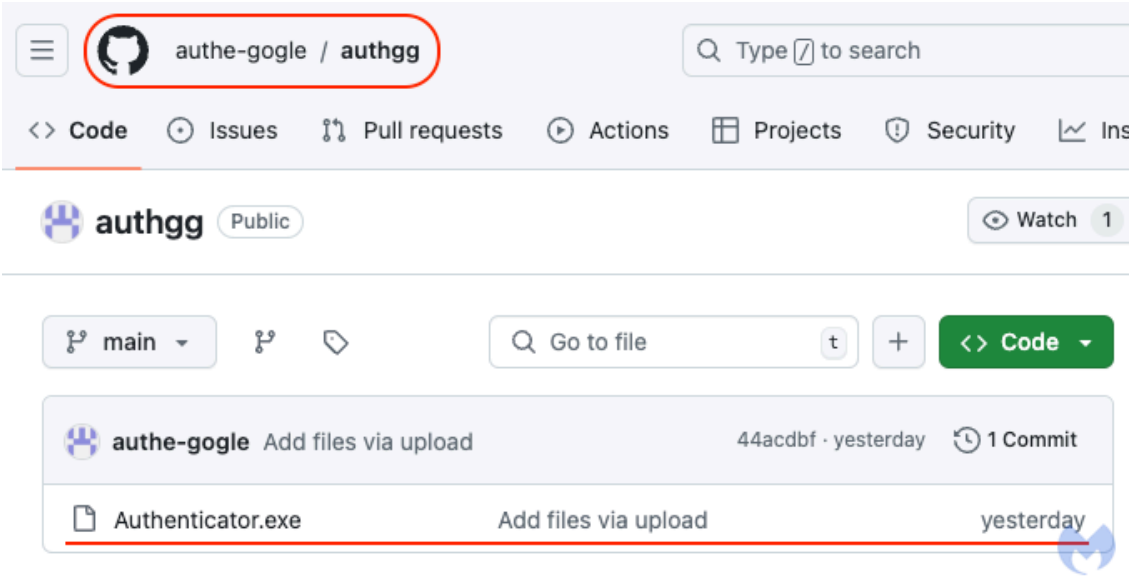
The fraudulent site *chromeweb-authenticators[.]com* was registered via NICENIC INTERNATIONAL GROUP CO., LIMITED on the same day as the ad was observed.



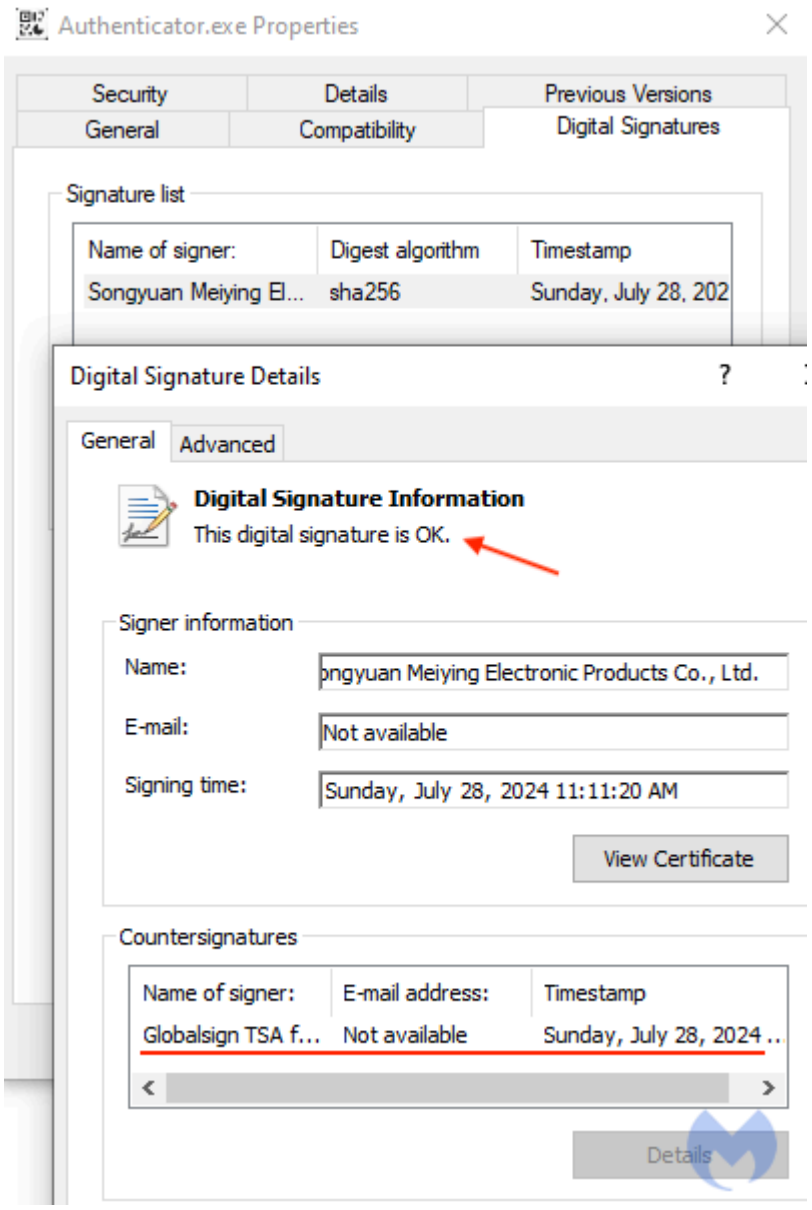
Looking at the site's source code, we can see the code responsible for downloading *Authenticator.exe* from GitHub. Note the comments from the author in Russian:



Hosting the file on GitHub allows the threat actor to use a trusted cloud resource, unlikely to be blocked via conventional means. While GitHub is the de facto software repository, not all applications or scripts hosted on it are legitimate. In fact, anyone can create an account and upload files, which is exactly what the threat actor did under the username *authe-gogle*, creating the *authgg* repository that contains the malicious *Authenticator.exe*:



Looking at the file itself, we can see that it has been digitally signed by "*Songyuan Meiying Electronic Products Co., Ltd.*" just one day before, and the signature is still valid at the time of writing:



The malware, DeerStealer, is a kind of stealer that will grab and exfitrate your personal data via an attacker-controlled website hosted at *vaniloin[.]fun*.

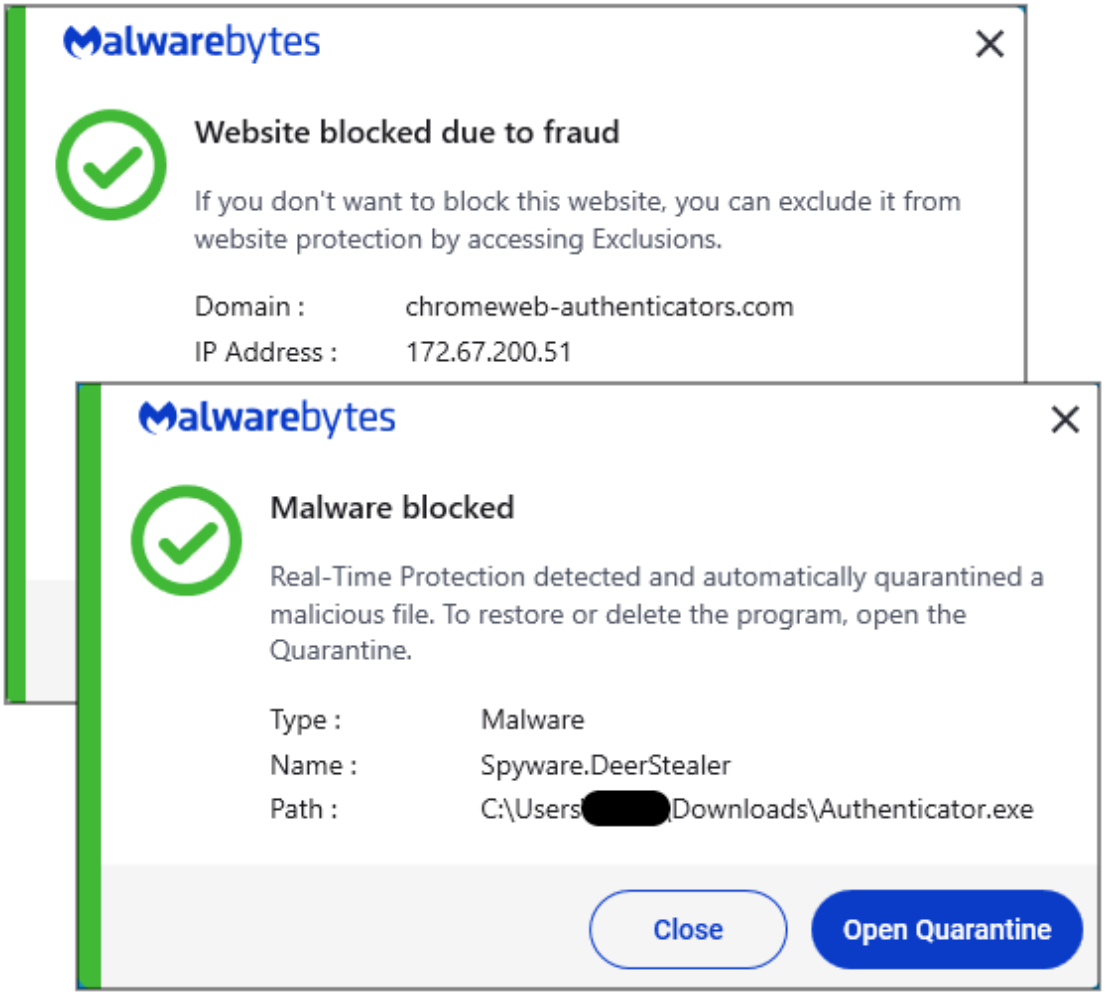
Conclusion

Threat actors have been abusing Google ads as a way to trick users into visiting phishing and malware sites. Since the whole premise of these attacks relies on social engineering, it is absolutely critical to properly distinguish real advertisers from fake ones.

As we saw in this case, some unknown individual was able to impersonate Google and successfully push malware disguised as a branded Google product as well.

We should note that Google Authenticator is a well-known and trusted multi factor authentication tool, so there is some irony in potential victims getting compromised while trying to improve their security posture. We recommend avoiding clicking on ads to download any kind of software and instead visiting the official repositories directly.

Malwarebytes blocks access to the fake Authenticator website, and we detect the payload as Spyware.DeerStealer.



Indicators of Compromise

Malicious domains

```
vcczen[.]eu
tmdr7[.]mom
chromeweb-authenticators[.]com
chromeweb-authenticatr[.]com
kejip[.]com
```

Payloads (DeerStealer)

```
5d1e3b113e15fc5fd4a08f41e553b8fd0eaace74b6dc034e0f6237c5e10aa737
b83fad3d2b0e83e565d23c914b06ac2934258616d55d211fe78032c918f814dc
```

C2s

```
vaniloin[.]fun
mundoparachicas[.]space
```

Source: https://www.malwarebytes.com/blog/threat-intel/2024/07/threat-actor-impersonates-google-via-fake-ad-for-authenticator