

Forum:[Hack Forums](#)

Thread: [Bypass Google Chrome Antivirus](#)

?Anna? - July 4, 2024, 6:09 am

What is the best way to avoid triggering google chrome detection when someone will download my file ?

I mean it's better to put everything in an RAR archive with a password or in a ZIP with a password ?

DramaKing - July 4, 2024, 6:59 am

(Jul 4, 2024 06:09 AM)AnnaEngineer Wrote: [\[CITE\]](#) What is the best way to avoid triggering google chrome detection when someone will download my file ?

I mean it's better to put everything in an RAR archive with a password or in a ZIP with a password ?
This thread explains Google Safe Browsing: <https://hackforums.net/showthread.php?tid=6244776>.

Tentco - July 4, 2024, 7:38 am

Google chrome Scanner is solely based on scantime, so you can do 2 things, either pump the file size to like 500mb around smh to exhaust the scanner, or obfuscate it properly/use a stager for your final payload.

DramaKing - July 4, 2024, 9:27 am

(Jul 4, 2024 07:38 AM)Tentco Wrote: [\[CITE\]](#) Google chrome Scanner is solely based on scantime, so you can do 2 things, either pump the file size to like 500mb around smh to exhaust the scanner, or obfuscate it properly/use a stager for your final payload.

It's not just AMSI signature detection. Reputation plays a part, too. See the thread that I posted.

Tentco - July 4, 2024, 9:31 am

(Jul 4, 2024 09:27 AM)DramaKing Wrote: [\[CITE\]](#) It's not just AMSI signature detection. Reputation plays a part, too. See the thread that I posted.

Reputation has nothing to do with "This File is malicious warning.", the topic is about bypassing anti-virus not other warnings like- "This File is not Commonly Downloaded.", Good thread though.

Also the rep part is for red screen which can be easily bypassed, but im sure any one would have their own host to upload files and stuff.

DramaKing - July 4, 2024, 9:45 am

(Jul 4, 2024 09:31 AM)Tentco Wrote: [\[CITE\]](#) Reputation has nothing to do with "This File is malicious warning.", the topic is about bypassing anti-virus not other warnings like- "This File is not Commonly Downloaded.", Good thread though.

Also the rep part is for red screen which can be easily bypassed, but im sure any one would have their own host to upload files and stuff.

I concede the point.

?Anna? - July 4, 2024, 12:45 pm

(Jul 4, 2024 12:24 PM)wilzonsss Wrote: [\[CITE\]](#) ty for this
???

DramaKing - July 4, 2024, 12:55 pm

(Jul 4, 2024 12:45 PM)AnnaEngineer Wrote: [\[CITE\]](#) ???

What [mention=5543725] did is to post any random bit of text in any random thread in order to download an attachment.

Brill - July 6, 2024, 1:13 pm

(Jul 4, 2024 07:38 AM)Tentco Wrote: [\[CITE\]](#) Google chrome Scanner is solely based on scantime, so you can do 2 things, either pump the file size to like 500mb around smh to exhaust the scanner, or obfuscate it properly/use a stager for your final payload.

this pretty much sums up viable options. proper obfuscation and staged payloads are your best bet.

I suppose, in some unlikely situation, if you have control over the dns you can sinkhole the safe browsing domains, but you'll still get caught by defender without adequate obfuscation.

sb-ssl.google.com

safebrowsing.googleapis.com

safebrowsing-cache.google.com

safebrowsing.google.com