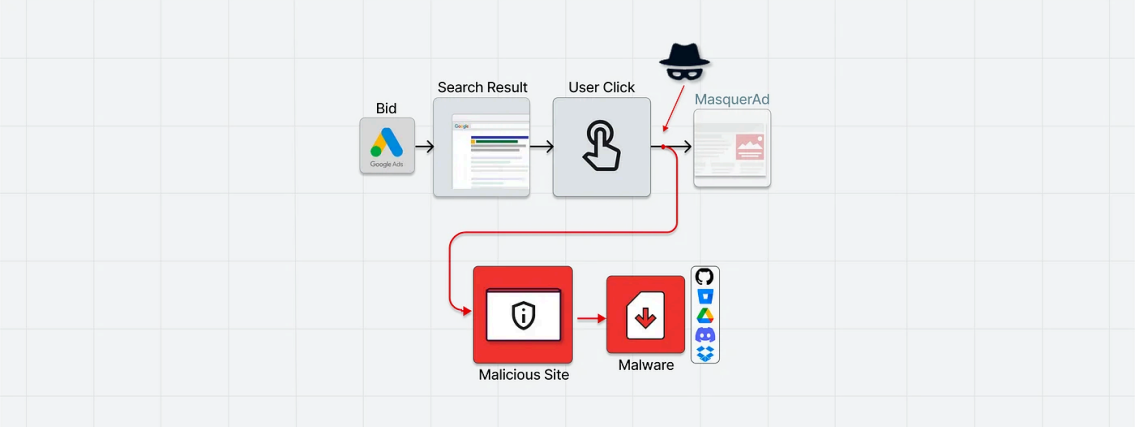
“MasquerAds” — Google’s Ad-Words Massively Abused by Threat Actors, Targeting Organizations, GPUs and Crypto Wallets

By Nati TalDecember 28, 2022•9min read

Archived: 2026-04-05 14:02:53 UTC

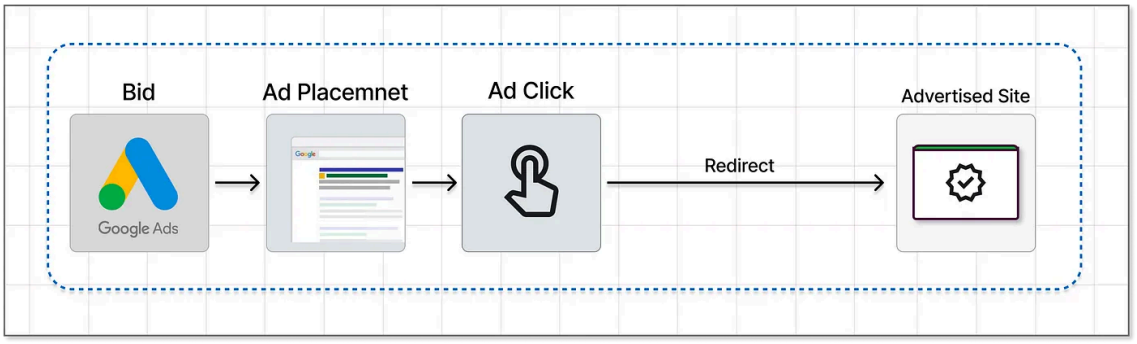


Threat actors masquerAd-ing their malicious sites in the Google Ads flow

The Google-Ads Point of View

Google Ads advertisement platform is highly reputable and probably one of the most used in the world — and there is a good reason for that. We are all used to get not only effective and relevant ads with it, but usually also quickly navigating to sites we were looking for.

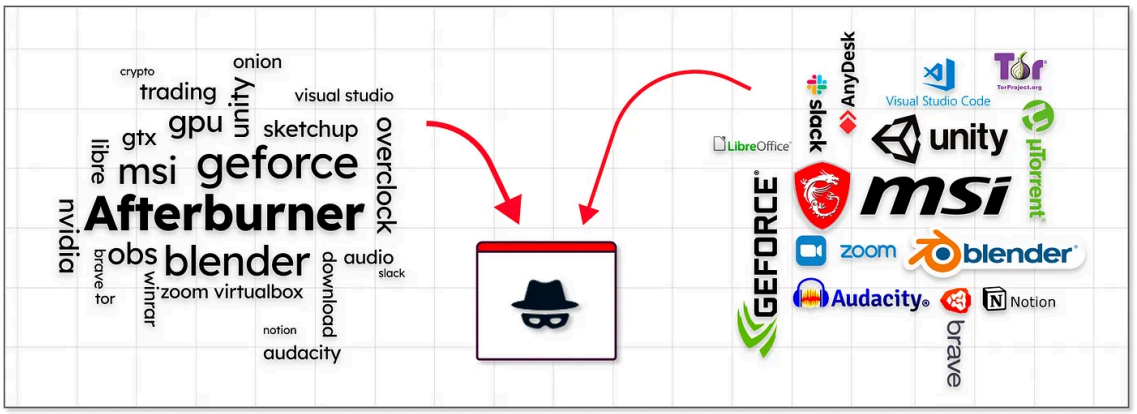
Let’s say, you search for Grammarly to finally get rid of all those typos. You will write “Grammarly” in the search bar, click Enter, and quickly get the official (probably promoted) Grammarly website on the top of the search results page. Easy. And this is also how Google sees that — they get a bid on a keyword linked to an advertisement landing page. The advertiser is a valid customer? The advertised site is legit? No probs — you got your ad placed!



A standard promoted search results ad campaign from Google Ads perspective

Looking into this simple flow from a wider perspective and taking into account anomalies in the behavior of both site hosts as well as visitors, got us to uncover many malicious malware-spreading campaigns of many purposes and

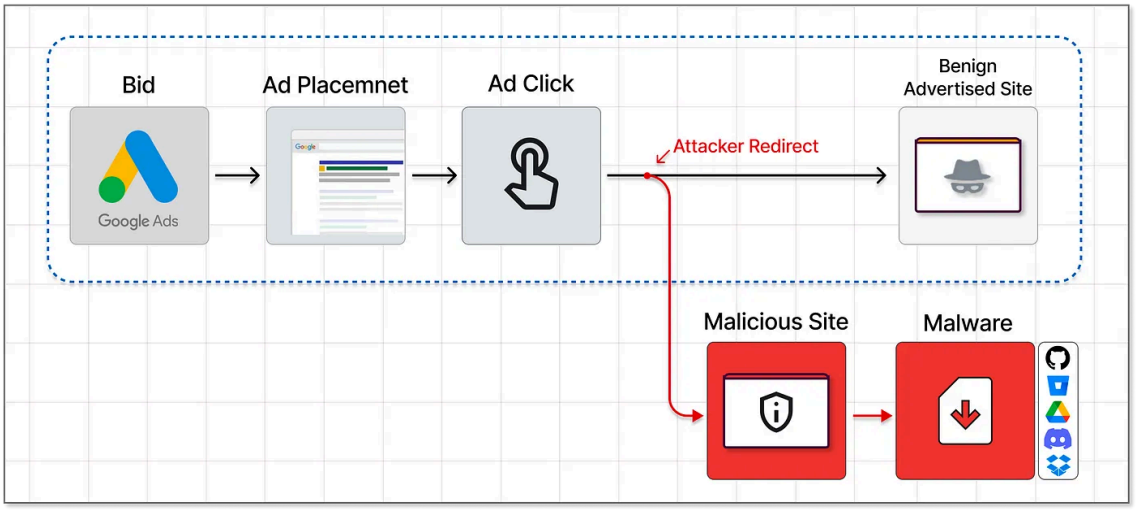
sources — propagating solely using the Google Ads platform. A concept with such powerful outcomes it even got the FBI's attention already.



Brands, ad words, and reputable search engines in the hands of threat actors

A Simple Trick for Getting Under Google-Ads Radar

The trick is simple — creating a benign site to be promoted with the wanted keyword and keeping it valid and safe in the eyes of the policy enforcer. Yet, the moment those "disguised" sites are being visited by targeted visitors (those who actually click on the promoted search result) the server immediately redirects them to the rogue site and from there to the malicious payload — usually also hiding inside reputable file sharing and code hosting servers like GitHub, dropbox, discord's CDN, etc.



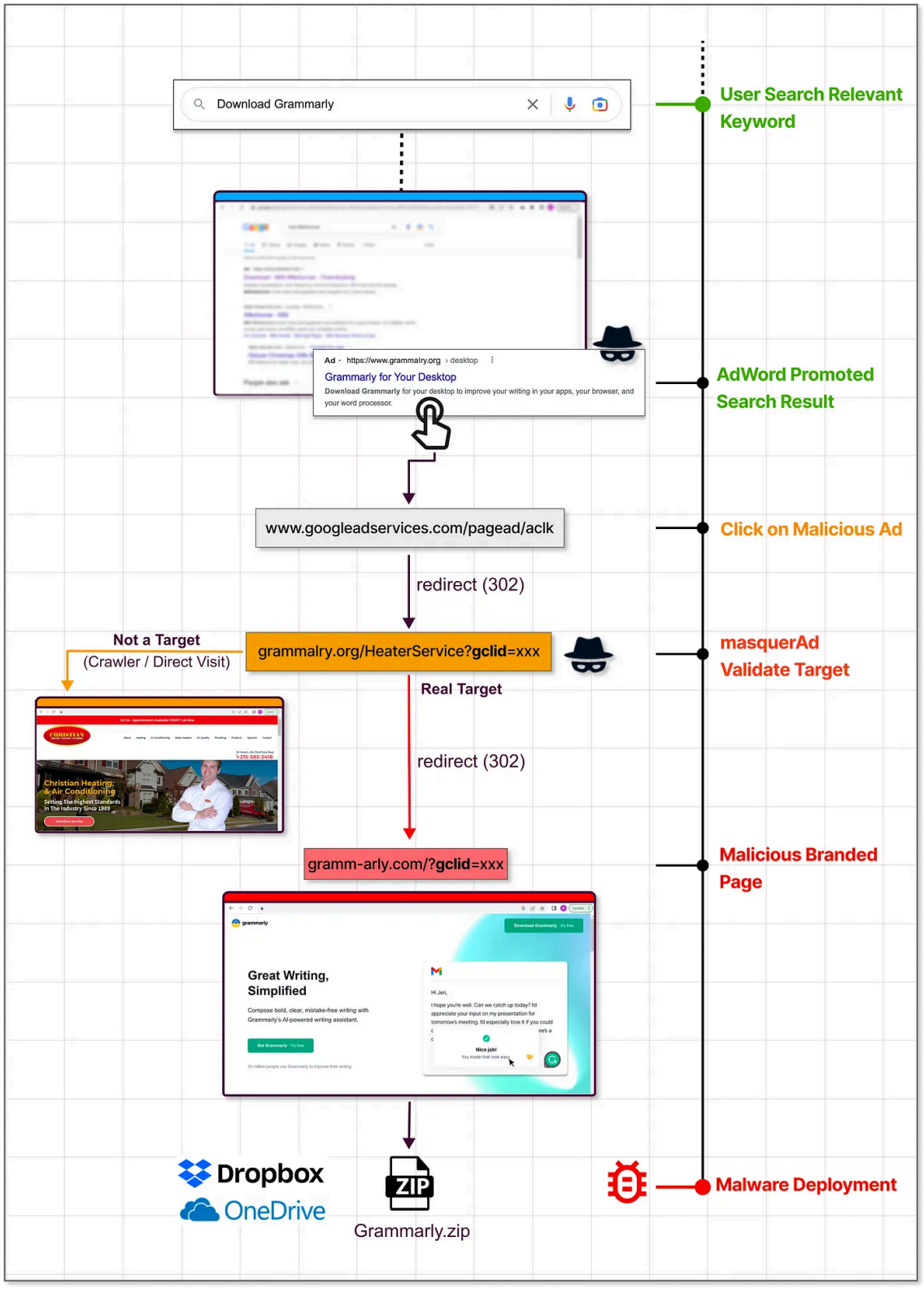
And what actually happens under Google-Ads Radar

Those rogue sites are practically invisible to visitors not reaching from the real promotional flow (e.g. arriving with a valid `gclid` value) showing up as benign, unrelated sites to crawlers, bots, occasional visitors, and of course for Google's policy enforcers. Some examples of such flows, active during December 2022, can be seen here — showing on the left the masked site Google is actually advertising, while on the right you see the actual phishing site ad-clickers are being redirected to:

Phishing America First Bank customers / spreading malware with uTorrent, Audacity and Brave brands

To deep dive into the technical details of this scheme, the following is a real sample flow targeting Grammarly as observed out in the wild in late November 2022. The promoted search result sends you to the domain `grammalry[.]org` which is an advertisement for “Christian Heating and Air-Conditioning” yet only for those who visit it directly. If you clicked on that promoted search result you generate a unique click id (Google’s Click ID, or **gclid**) that is checked by the threat actor and if valid (and it is valid only once!) together with other params like visitors' geo-location, user-agent, etc., it will forward you to the malicious Grammarly phishing page under the domain `gramm-arly[.]com` .

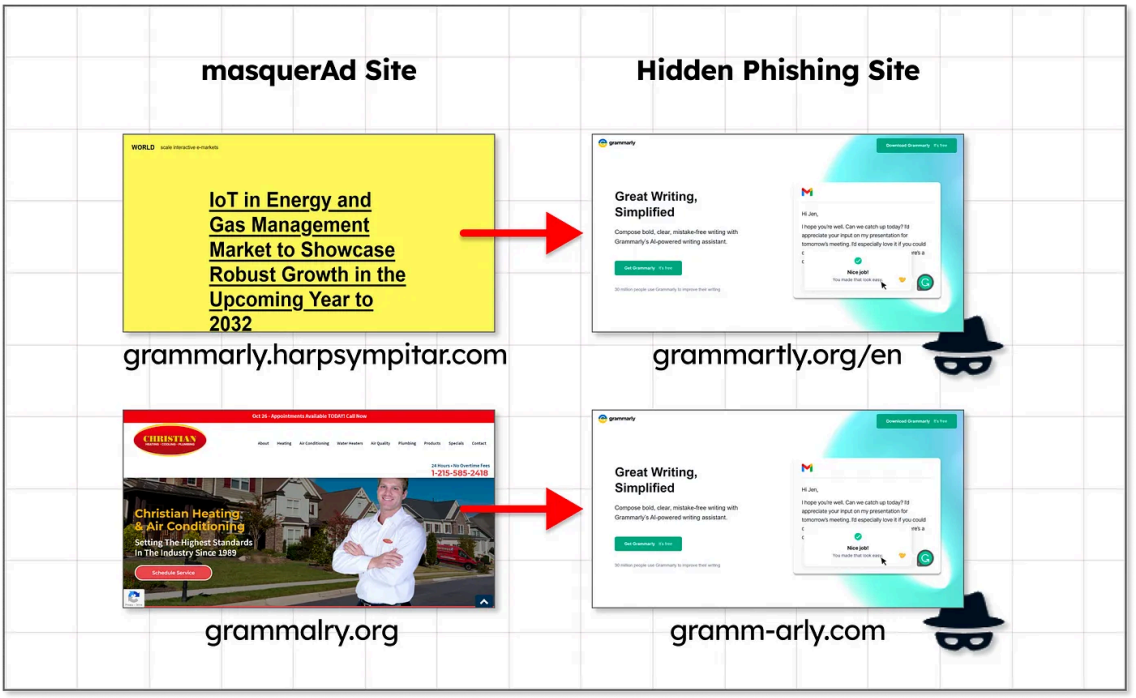
Note that forwarding is done on the server side, hidden from Google as well as from the visitor that will never get to see the “masquerAd” site — only the actual phishing page:



From searching to download Grammarly to downloading and installing a malicious payload

The Gramnarly Malware — A Raccoon Stealer Variant

No, it wasn't a typo… `gramnarly[.]com` is just one of the Grammarly-branded phishing pages out there. And no, they don't wait for someone to misspell the domain name (wishing he had Grammarly in the first place). All needed is just bid on the `Grammarly` ad word and create a "masquerAd" flow:

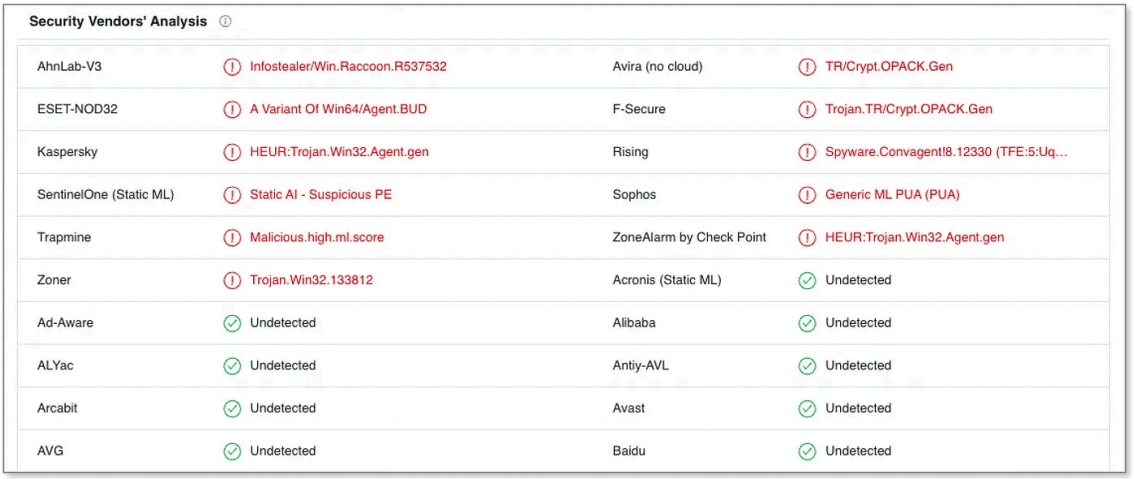


Grammarly branded masquerAd flows

Now that those threat actors don't need to waste time and effort in reaching the most relevant targets (well, Google does that for them) they can put more effort into their malicious payload. And indeed, in this campaign, the Grammarly payload is not the simple stealer that is quickly detected by common protection mechanisms. Some of the more interesting characteristics we've seen include:

- **Bundled with the actual software** — Installing the Grammarly branded malware will actually install a copy of Grammarly. It is of course bundled with another executable that does all the black magic silently.
- **Bloated Files** — the installation executable (or the container zip in other variants) is full of bloated zeroed files just to make the file bigger than automated malware analysis systems' max allowed size. Usually 500Mb and above. Also, making less than 1% of the code fingerprinted with malicious code snippets is another great way to mitigate detection. Dynamic execution is the most effective way to actually see something is bad here — and we will hardly see any of the current protection vendors execute these huge files automatically.
- **Changing Payloads Periodically** — because of the smaller scale, it is feasible to actually re-create the payloads every day with minor changes and using different malicious payloads of stealers, crypto miners, and such. So one day you download a Raccoon stealer from a dropbox folder, and the other day it's a Vidar stealer in an executable MSI file from a discord CDN server.

Even for Virus-Total, it took several days since our submission to get more than a few heuristic detections:



Security Vendors' Analysis			
AhnLab-V3	Infostealer/Win.Raccoon.R537532	Avira (no cloud)	TR/Crypt.OPACK.Gen
ESET-NOD32	A Variant Of Win64/Agent.BUD	F-Secure	Trojan.TR/Crypt.OPACK.Gen
Kaspersky	HEUR:Trojan.Win32.Agent.gen	Rising	Spyware.Convagent!8.12330 (TFE:5:Uq...
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	Generic ML PUA (PUA)
Trapmine	Malicious.high.ml.score	ZoneAlarm by Check Point	HEUR:Trojan.Win32.Agent.gen
Zoner	Trojan.Win32.133812	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Baidu	Undetected

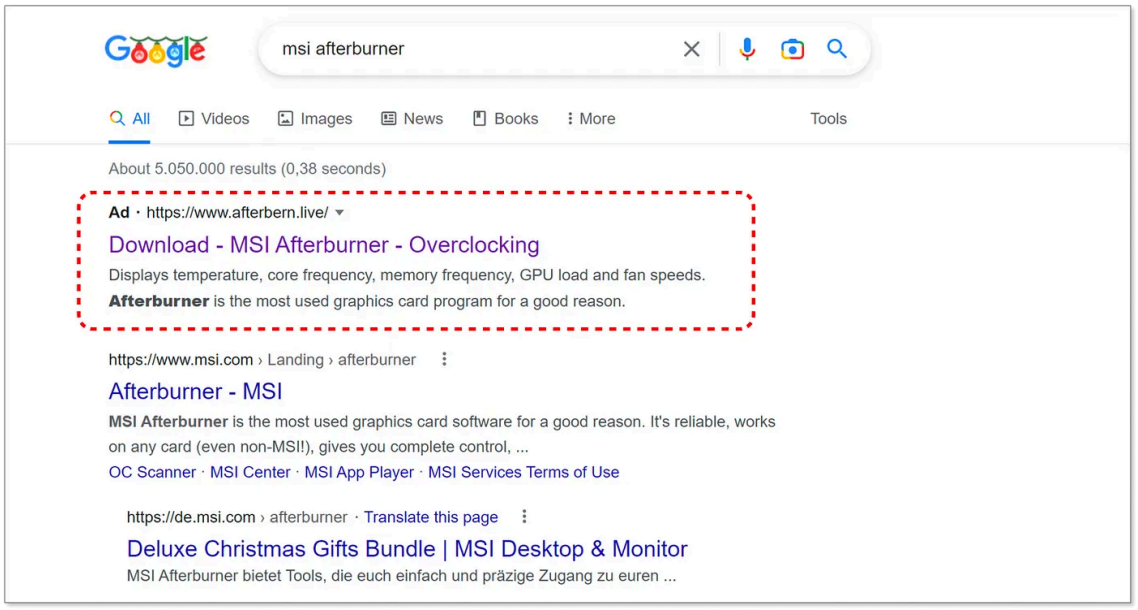
Grammarly.exe As downloaded from grammartly[.]org

Current virus total report here:
https://www.virustotal.com/gui/file/3baf692a1589355af206f4e3886a09fe8997f0b62c78c1403556285eaba40e94/detection

Vermux — Scaled Up GPU-Targeted Operation

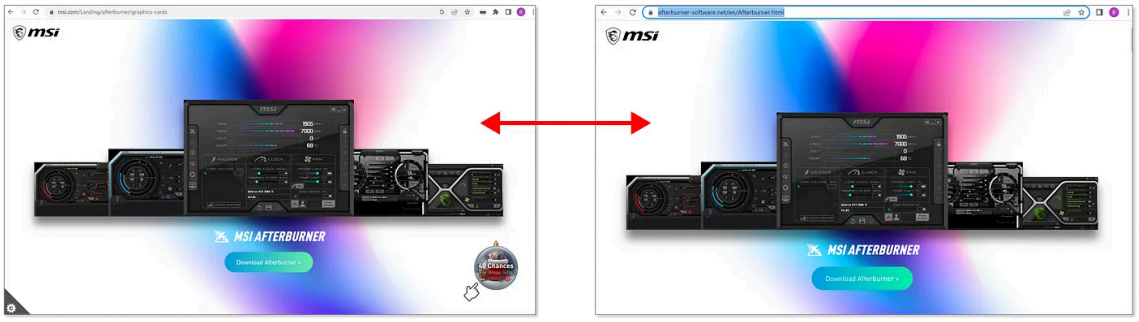
The most scaled-up campaign abusing this technique for propagation is most un-doubtfully the GPU-targeted threat actor we labeled **Vermux**. Vermux is targeting any computer that has or might have GPU hardware, and does that by targeting relevant brands of software tools or drivers that are popular with users of such PCs.

On top of the list is the keyword “Afterburner” referring to the MSI Afterburner graphics card tool, as can be seen in these genuine search results as made from the Central USA area — showing how the adBuffer domain `afterbern[.]live` shows up on top of the list:



Genuine search results showing the promoted the masquerAd site afterbern[.]live

Afterburner is used by many gamers as well as graphic designers to control, overclock and make the most out of their GPU. Vermux are after that GPU exactly, but for another reason — crypto-currency mining. And indeed, clicking on the promoted search result as seen above will redirect you eventually to the hidden malicious site that looks exactly like the original:



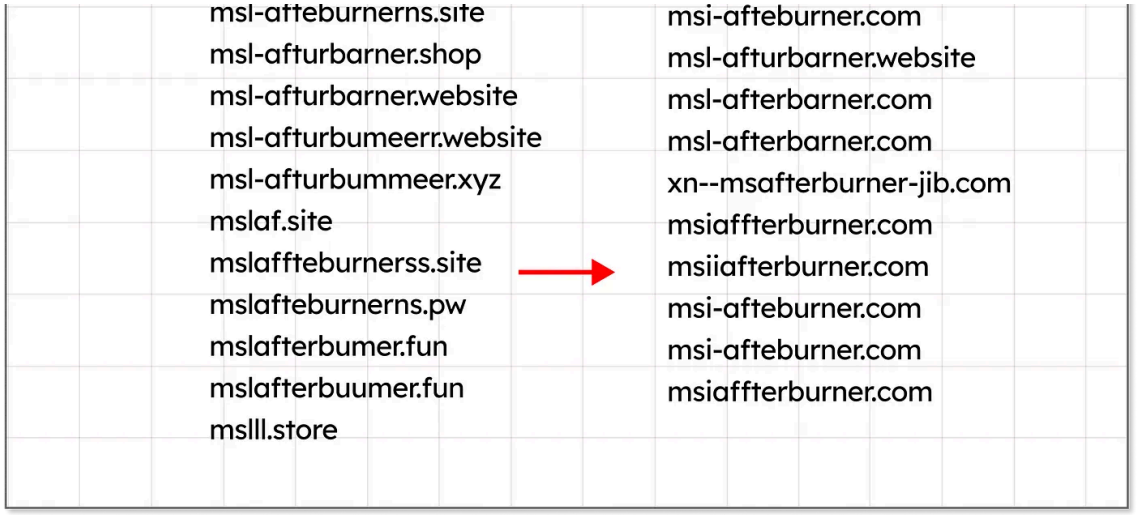
Can you tell the difference? (The fake one is on the right)

The MSI Afterburner campaign's payload was noticed by researchers a few weeks ago, notable for how it is hard to be detected. With fully understanding this elusive propagation technique of masquerAd-ing, we were able to uncover the full extent and versatility of Vermux **— reaching far further than just this one fake afterburner installer.**

Vermux deployed hundreds of domains, "masquerAd" sites as well as phishing pages in servers located mostly in **Russia**, serving rogue ads mainly to USA and Canadian residents. This threat actor is abusing a vast list of brands and keeps on evolving.

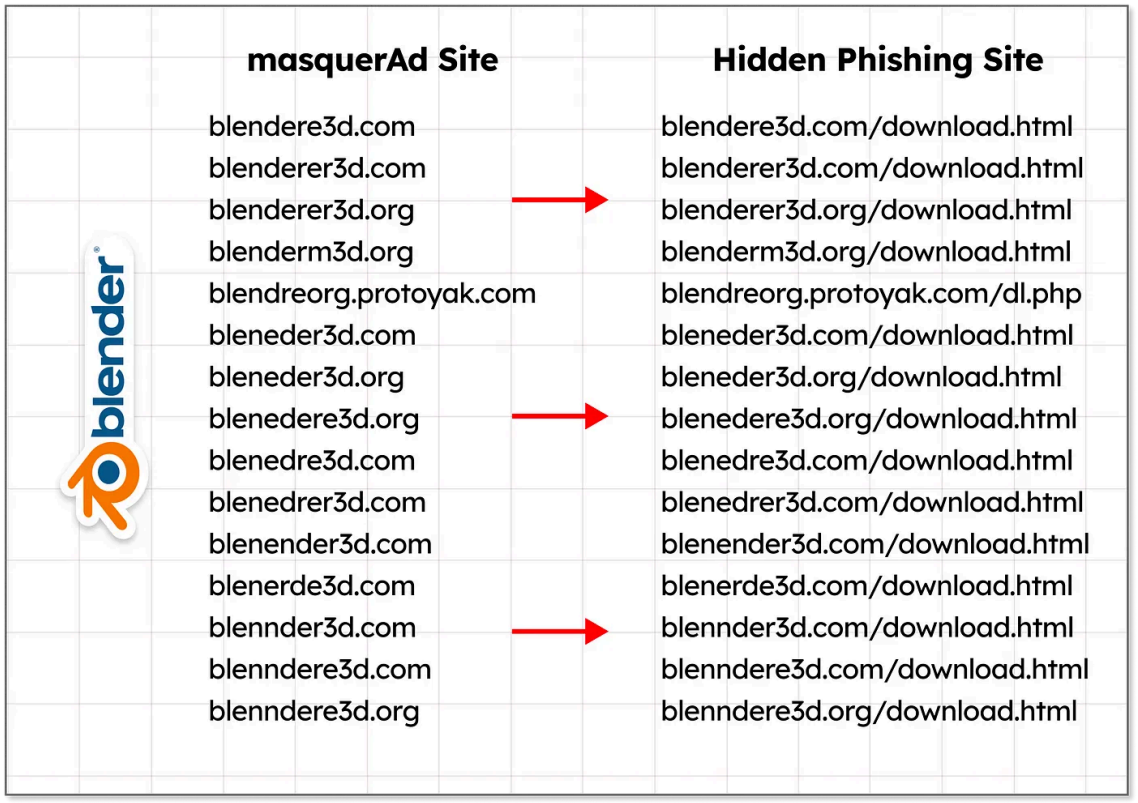
The main attack vector is hunting down those GPUs. Here are some examples of adBuffer flows active during November-December 2022. First, the popular MSI Afterburner as we've seen above:

masquerAd Site	Hidden Phishing Site
afteerbumers.online	msl-afterbarner.com
afterburmmeer.fun	msi-afteburner.com
afterburmmeer.store	msi-afteburner.com
afterburmmer.store	msi-afteburner.com
afterrbburner.online	afterrbburner.online
afterrbburner.space	msi-afteburner.com
afterrbburnerr.shop	msl-afterbarner.com
afterrburnerr.click	afterrburnerr.click
afterrburnerr.click	msl-afterbarner.com
afterrbuurner.fun	msi-afteburner.com
afterrbuurner.pw	msi-afteburner.com
aftersburmers.site	msi-afterbarner.com
aftterbumer.fun	msl-afterbarner.com
aftterbumers.art	msl-afterbarner.com
burnermsituner.site	msiburnberafter.online
burnermsituner.site	burnermsituner.site
m-afterbbumer.art	m-afterbbumer.art
m-afterbbumer.art	msl-afterbarner.com
m-afterbbumers.lol	msl-afterbarner.com
m-afterbbumers.lol	msl-afterbarner.com
m-afterbumer.homes	msi-afteburner.com
m-afterbumer.shop	msi-afteburner.com
m-afterbummeer.online	msl-afterbarner.com
m-afterbummer.site	msi-afteburner.com
m-afterbunar.shop	msi-afteburner.com
misafterpurnier.space	rivatunerrr.space
ms1afterpurnier.xyz	msiafetrburner.com
msi-asalburner.site	msi-asalburner.site
msi-atferbunrer.appermonti.com	msi-atferbunrer.appermonti.com
msi-atferbunrer.unikamail.com	msi-atferbunrer.unikamail.com
msiafterrburners.site	msiaffterburner.com
msiafvterberner.com	rivatunerrr.space
msiavterpurner.com	rivatunerrr.space
msiburneraftir.site	msiburneraftir.site
msiburneraftir.space	msiburneraftir.space
msiburneravter.shop	rivatunerrr.space
msiburneravter.site	rivatunerrr.space
msiiaf.online	xn--msafterburner-jib.com
msirivatuuner.space	burnavtermsi.space
msl-afieburners.pw	msiiafterburner.com
msl-afieburners.pw	msiiafterburner.com
msl-afteburnerks.website	msiiafterburner.com
	msiiafterburner.com



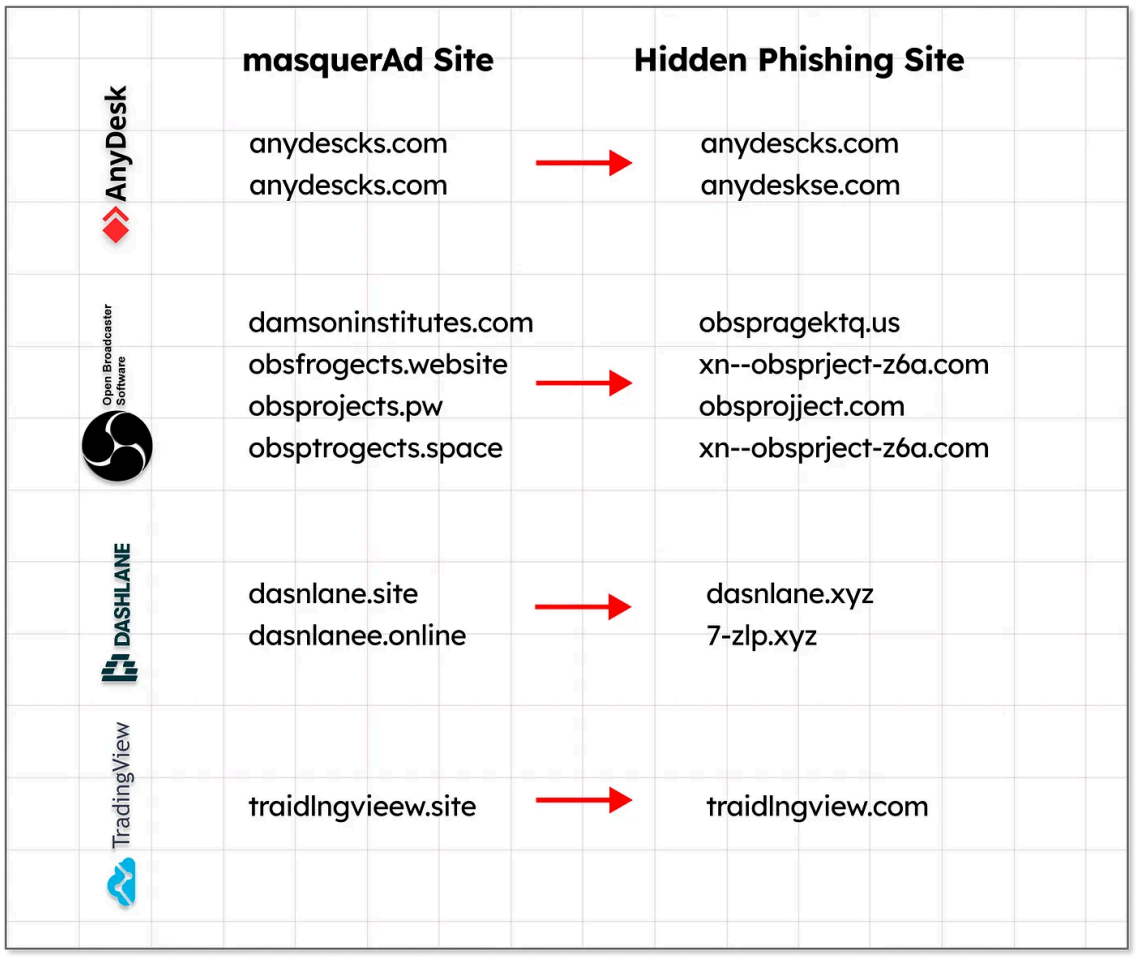
Vermux MSI Afterburner flows

And another well-known brand popular with GPU owners is the open-source 3d editing and rendering software “Blender”:



masquerAd flows targeting Blender users

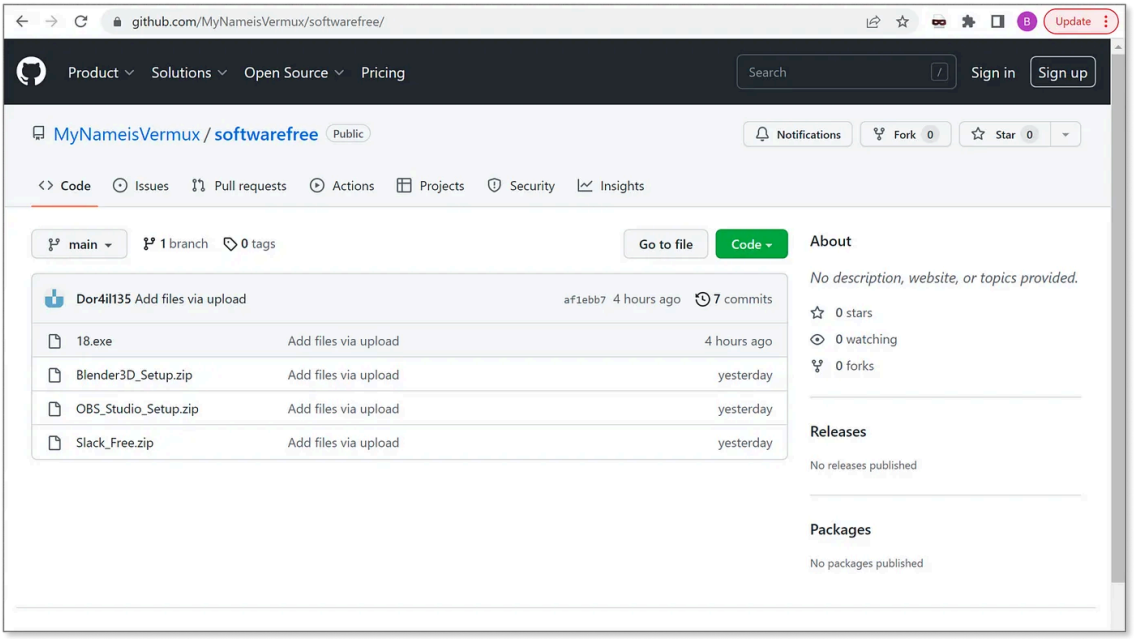
Adding to the above, Vermux works on other vectors to make even more profit — some targeting your crypto wallets and passwords, some targeting other popular tools with which Vermux can gain control — and some going directly to your trading or bank accounts:



Some more examples of masquerAd-ing flows operated by Vermux

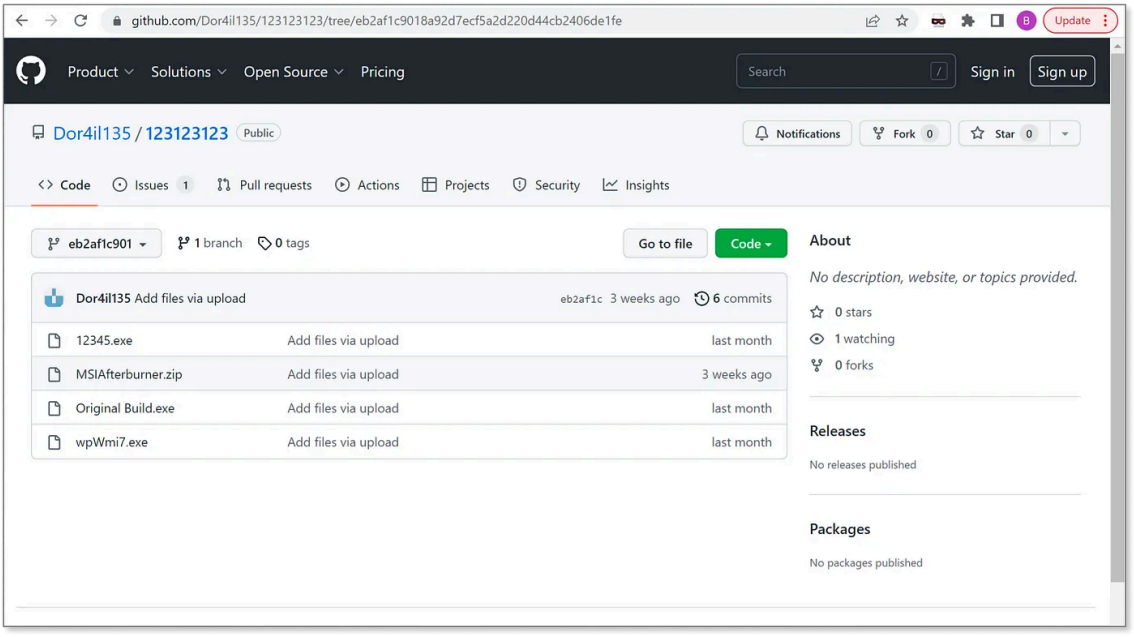
Vermux Malware Payload — Served Freely on GitHub

Vermux's payload is mostly built based on the Vidar trojan for control, and some proprietary compilation of python based Monero mining software. The files are following the rules we've noted before, making them evasive and hard to detect. Vermux not only abuse the reputation and propagation power of Google Ads, but they also abuse the reputation of known file-sharing services and code repositories like BitBucket, GitHub, Dropbox, OneDrive, etc. Here are some examples of such repos discovered in GitHub:



MyNameisVermux Public Repository on GitHub

The above is a repo called plainly `sofwarefree`, with the user `Dor4il135` that uploaded different “malwarized” installation packages for Slack, OBS, Blender, and even Norton Antivirus (`18.exe`).



Dor4il135 Public Repository on GitHub

The last is one of `Dor4il135` own repos active for over a month, now finally been taken down. A month is a lot of time, serving different types of software bundled with Vidar and other malware variants, and is updated almost daily with newer versions — mostly for changing binary foodprints to avoid detection.

Summary

Security is an issue of trust — thus, we constantly rely upon trusted reputable vendors on our daily endeavors over the web. No one is perfect though, and there are probably more bad actors looking to exploit those security loopholes than we can only imagine. Here we see exactly that — the constant rat race between the companies behind those powerful advertisement systems, global content delivery, and security infrastructures to those evasive actors that find a way to sneak under the radar and exploit the trusty others for their own gain.

This “masquerAd” concept is simple yet does exactly what those actors need — abuse the trust we sometimes blindly give to Google and their promoted search results. Adding to the above, the abuse of reputable file-sharing services as well as well-known software brands make them evade even the most advanced EDRs on the market. It’s inevitable to apply a more behavioral and unbiased protection level — even for the plainest and most common action like googling something up…

Don’t get fooled by misspelled domain names, and always double-check where you download your files from!
