

# AI Tool Popularity: An Opportunity for Launching Malicious Campaigns?

## Table of Contents

1. [Executive Report](#)
2. [Part #1: WhoisXML API Analysis](#)
3. [Part #2: Bayse's Bard Technical Analysis](#)
4. [Appendix: Sample Artifacts](#)

## Executive Report

The latest fraud data Sift published in “[Q2 2023 Digital Trust & Safety Index](#)” revealed that 78% of users are concerned that fraudsters could exploit AI tools to victimize them. And given recent cyber attacks targeting [ChatGPT](#) and [Grammarly](#), their worries may not be unfounded.

From a brand and phishing protection perspective, WhoisXML API and [Bayse Intelligence](#) joined forces to uncover instances of cybersquatting or phishing properties that could be riding on the increasing popularity of some of what have been dubbed “[the best AI productivity tools in 2023](#).”

Our collaboration led to the following findings:

- A total of 2,003 domains containing the names of popular AI productivity tools.
- The identification of one threat actor actively targeting several popular AI productivity tools while hiding within trusted cloud provider infrastructure.

## Part #1: WhoisXML API Analysis

### Cybersquatting Property Discovery in the DNS

The first step was identifying the AI productivity tools to perform public domain ownership attribution on. We subjected the 37 AI tool developers’ official site domains to a [bulk WHOIS lookup](#) and chose eight tools whose domain registrants indicated any of the data points below.

TOOL	OFFICIAL SITE DOMAIN	REGISTRANT DATA TYPE	WHOIS RECORD DETAIL
------	----------------------	----------------------	---------------------



AgentGPT	agentgpt[.]reworkd[.]ai	Email address Name	contact.me.reworkd@gmail[.]com Reworkd AI
Bard	bard[.]google[.]com	Organization	Google LLC
EmailTree	emailtree[.]ai	Organization	TS Holding
Motion	motion[.]ai	Email address Organization	domain-groups@hubspot[.]com HubSpot, Inc.
ProWritingAid	prowritingaid[.]com	Organization	123-Reg Limited
Runway	runway[.]ml[.]com	Email address Organization	domain.administrator@bankofamerica[.]com Bank of America Corporation
SaneBox	sanebox[.]com	Name Organization	S**** R**** SaneBox
Slidesgo	slidesgo[.]com	Organization	Freepik Company S.L.

**Note:** We partially masked the registrant name found in sanebox[.]com's WHOIS record for privacy purposes.

To determine if threat actors could be trailing their sights on any of the eight tools for their upcoming campaigns, we performed [Domains & Subdomains Discovery](#) lookups using the following search terms:

- agentgpt
- bard + ai
- emailtree
- motion + ai
- prowritingaid
- runway + ml
- sanebox
- slidesgo

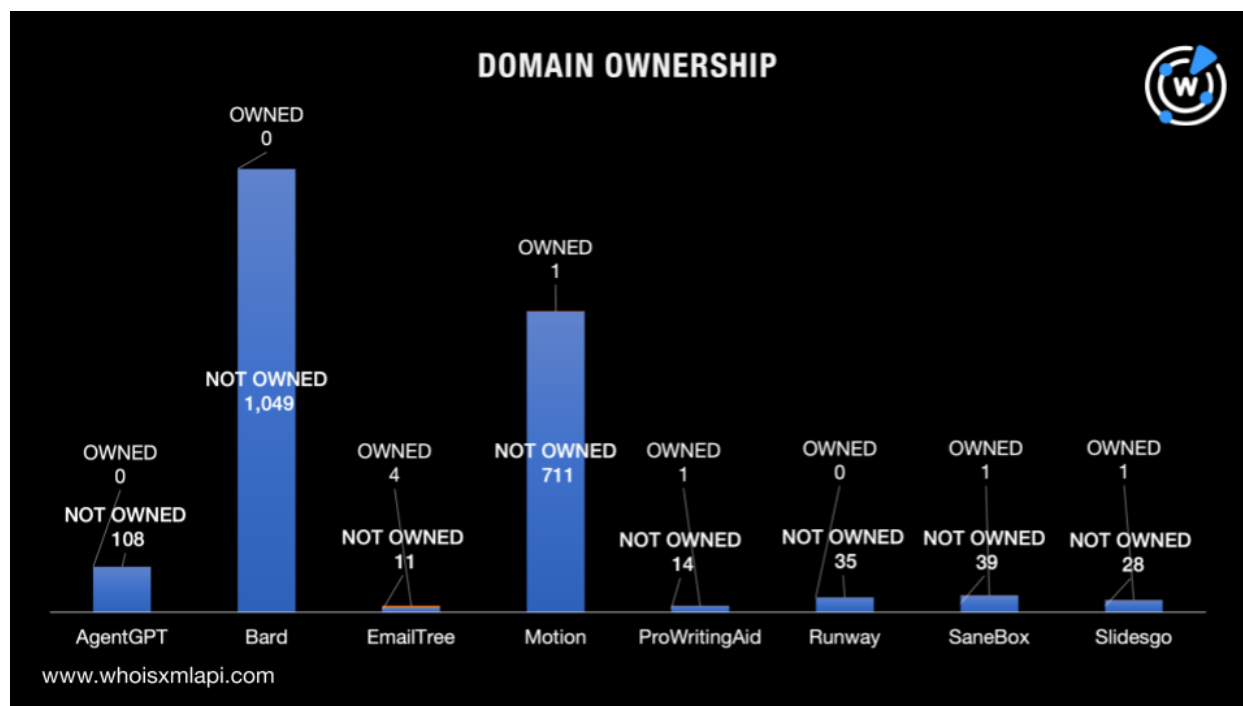
Our searches provided us with 2,003 domains in sum.

AI TOOL	DOMAIN VOLUME
Agent GPT	108
Bard	1,049
EmailTree	15
Motion	712
ProWritingAid	15
Runway	35



SaneBox	40
Slidesgo	29

Our WHOIS record detail comparisons revealed that less than 1% of the brand name-containing domains could confidently be publicly attributable to the AI productivity tool developers on our list.



## Part #2: Bayse's Campaign Analysis

One of the main ways attackers impersonate highly valuable websites is to reproduce or clone their content. This raises the likelihood that a user will visually associate the spoofed site with the legitimate one and enable the attacker to achieve their objectives (collect credentials or PII, download malware, and so on).

This tactic has been seen for several of these AI tools, but Bard was by far the most targeted.

After [submitting](#) Bard's legitimate site to Bayse Intelligence, we [can find out](#) how frequently, since when, and where else we've seen Bard's assets being referenced:



bayse.io/destination/bard.google.com

# Destination Insights for bard.google.com

Statistics for bard.google.com

**First Searched:**  
Sun Mar 26 2023 17:09:57 GMT-0400 (Eastern Daylight Time)

**Times Searched:**  
117

Seen on Sites (showing first 5 across the last week)

TIME SEEN	DESTINATION OF SITE	FINAL URL OF SITE INTERPRETED	VIEW RESULT
Wed Aug 09 2023 10:50:38 GMT-0400 (Eastern Daylight Time)	<b>bard.lmlm.workers.dev</b>	https://bard.lmlm.workers.dev/	
Wed Aug 09 2023 01:49:10 GMT-0400 (Eastern Daylight Time)	start-5nv.pages.dev	https://start-5nv.pages.dev/	
Tue Aug 08 2023 16:03:01 GMT-0400 (Eastern Daylight Time)	soundrss.knc.workers.dev	https://soundrss.knc.workers.dev/	
Mon Aug 07 2023 11:35:04 GMT-0400 (Eastern Daylight Time)	homepage.divemasterjm.duckdns.org	https://homepage.divemasterjm.duckdns.org/	

One of the sites that recently linked to Bard (highlighted above) is clearly [impersonating Bard](#):

### Interpretation Result for bard.lmlm.workers.dev

Bayse's Analysis

**Message:**  
The title for this page is 体验 Bard - Google 的 AI 实验项目.

### Interpretation Result for bard.google.com

Bayse's Analysis

**Message:**  
The title for this page is Try Bard, an AI experiment by Google.

Moreover, it has been seen multiple times over the last two months, and we've seen other sites associated with its parent domain (lmlm[.]workers[.]dev) as well:



bayse.io/destination/bard.lmlm.workers.dev

B Resources Search Upload API Docs

### Destination Insights for bard.lmlm.workers.dev

Statistics for bard.lmlm.workers.dev

**First Searched:**  
Sat Jun 03 2023 22:14:40 GMT-0400 (Eastern Daylight Time)

**Times Searched:**  
7

**Children Seen:**  
Showing first 0

DESTINATION	GET DETAILS
<b>Parent Seen?</b> lmlm.workers.dev ( <a href="#">See Details</a> )	

Pivoting to the [parent domain's details](#) shows us that not only is Bard targeted, but there's actually several other popular AI and cloud-related technologies being targeted since March 2023:



bayse.io/destination/lmlm.workers.dev

Resources Search Upload API Docs

### Destination Insights for lmlm.workers.dev

Statistics for lmlm.workers.dev

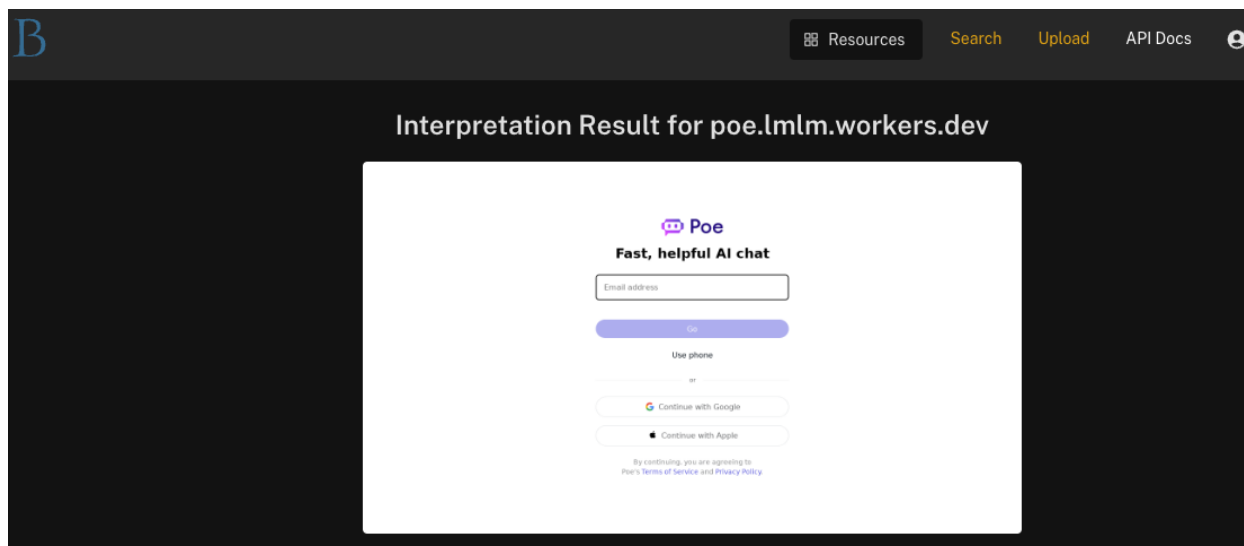
**First Searched:**  
Wed Mar 01 2023 16:25:37 GMT-0500 (Eastern Standard Time)

**Times Searched:**  
46

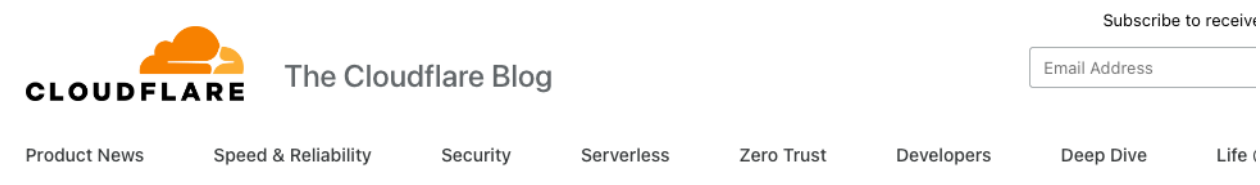
**Children Seen:**  
Showing first 10

DESTINATION	GET DETAILS
api-of-claude.lmlm.workers.dev	<a href="#">↗</a>
api-of-retool.lmlm.workers.dev	<a href="#">↗</a>
bard.lmlm.workers.dev	<a href="#">↗</a>
bing.lmlm.workers.dev	<a href="#">↗</a>
chartgpt.lmlm.workers.dev	<a href="#">↗</a>
chatgpt.lmlm.workers.dev	<a href="#">↗</a>
doprax.lmlm.workers.dev	<a href="#">↗</a>
openai.lmlm.workers.dev	<a href="#">↗</a>
openai-of-azure.lmlm.workers.dev	<a href="#">↗</a>
poe.lmlm.workers.dev	<a href="#">↗</a>

While several of those sites are down, pivoting to [some of them](#) gives us a view into still-live impersonations:



In conclusion, because the parent domain (*lmlm[.]workers[.]dev*) is hosted on Cloudflare’s web app hosting platform and these sites all share the same *lmlm* subdomain, it means that all of the sites highlighted earlier were actually created by the same threat actor! Evidence of this can be traced back to the official Cloudflare [announcement](#) in 2019:



## Announcing workers.dev

02/19/2019

We are working really hard to allow you to deploy Workers without having a Cloudflare domain. You will soon be able to deploy your Cloudflare Workers to a subdomain-of-your-choice.workers.dev, which you can claim now on [workers.dev](#)!

What this means is that there is a threat actor currently hosting content on Cloudflare’s infrastructure who—over the course of 5+ months—is likely targeting users of many highly popular AI- and cloud-based tools. Activity to this and anything under this particular subdomain (*lmlm[.]workers[.]dev*) should be treated as extremely suspect and should likely be blocked outright.



**If you wish to perform a similar investigation or learn more about the products used in this research, don't hesitate to visit [whoisxmlapi.com](https://www.whoisxmlapi.com) or [bayse.io](https://bayse.io).**

**Disclaimer:** We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as “threats” or “malicious” may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.

## Appendix: Sample Artifacts and IoCs

### Sample Brand-Containing Domains

- agentgpt[.]digital
- agentgptstudio[.]com
- agentgpt[.]pt
- agentgpt[.]team
- agentgptexpert[.]com
- agentgpt[.]red
- agentgpt-website[.]com
- agentgptcn[.]online
- agentgpt[.]com[.]br
- agentgpt[.]info
- agentgpt[.]finance
- agentgpt-p7pnrkh44-rogerthiede[.]vercel[.]app
- agentgpt[.]asia
- bardai[.]ai
- bardrail[.]ai
- bard-maintain[.]fr
- bard[.]ai
- bardaiklaipeda[.]lt
- bardaitraining[.]com
- bardaisanism[.]faith
- bardsaimailing[.]com
- barde[.]ai
- bardo[.]ai
- bards[.]ai
- bardavilaitaim[.]com[.]br
- bardai[.]uk
- emailtree[.]co
- emailtree[.]net
- emailtreefrog[.]ca
- emailtree[.]in
- emailtreeai[.]com
- emailtree[.]club
- emailtree[.]pw
- emailtree[.]ai
- emailtrees[.]com
- emailtree[.]icu
- emailtree[.]uk
- emailtree[.]com
- emailtree[.]co[.]uk
- motionaid[.]training
- motion[.]ai
- motions[.]ai
- motiong[.]ai
- motionit[.]ai
- motionos[.]ai
- motioniq[.]ai
- motionai[.]eu
- motionstakeairports[.]email
- motionai[.]ai
- motionai[.]cn
- motionai[.]io
- motionce[.]ai
- prowritingaid[.]tk





- prowritingaid[.]com
- prowritingaid[.]app
- prowritingaid[.]cn
- prowritingaide[.]com
- prowritingaid[.]ca
- prowritingaid[.]net
- prowritingaids[.]com
- prowritingaid[.]org
- prowritingaid[.]co
- prowritingaid[.]info
- prowritingaid[.]nl
- prowritingaid[.]co[.]uk
- runwayml[.]ml
- runwayml[.]ai
- runwayml[.]cn
- runwayml[.]fr
- runwayml[.]eu
- runwayml[.]it
- runwayml[.]de
- runwayml[.]co
- runwayml[.]net
- runwayml[.]xyz
- runwayml[.]com
- runwayml[.]vip
- runwayml[.]top
- sanebox[.]me
- sanebox[.]cloud
- sanebox[.]co
- saneboxoffst[.]gq
- sanebox-support[.]com
- sanebox[.]fr
- sanebox[.]net
- sanebox[.]rocks
- sanebox[.]com[.]au
- saneboxpartners[.]com
- sanebox[.]in
- sanebox[.]se
- sanebox[.]nl
- slidesgo[.]xyz
- slidesgoogle[.]com
- slidesgo[.]net
- slidesgoogle[.]gq
- slidesgoai[.]com
- slidesgo[.]com[.]de
- slidesgo[.]net[.]cn
- slidesgo[.]com
- slidesgo[.]cm
- slidesgoo[.]com
- slidesgo[.]ru
- slidesgod[.]com
- slidesgo[.]cn