AI Tool Popularity: An Opportunity for Launching Malicious Campaigns?

Table of Contents

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:

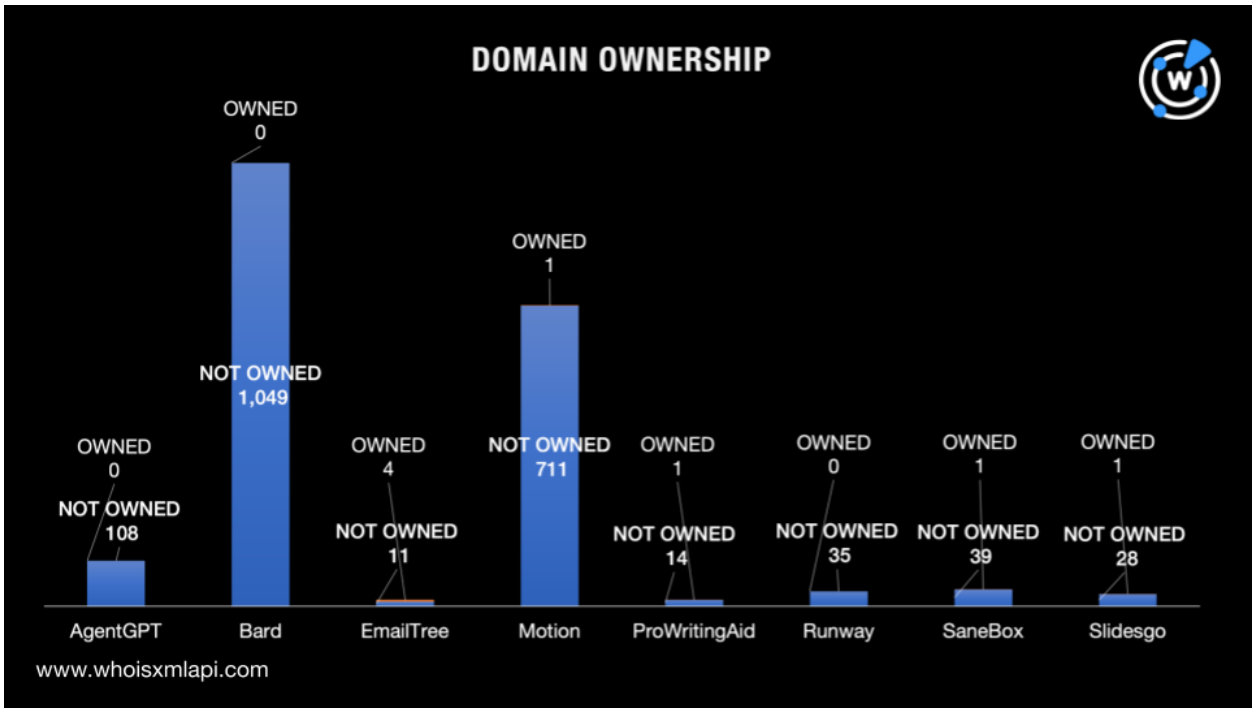
- **agentgpt**
- **bard + ai**
- **emailtree**
- **motion + ai**
- **prowritingaid**
- **runway + ml**
- **sanebox**
- **slidesgo**

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.

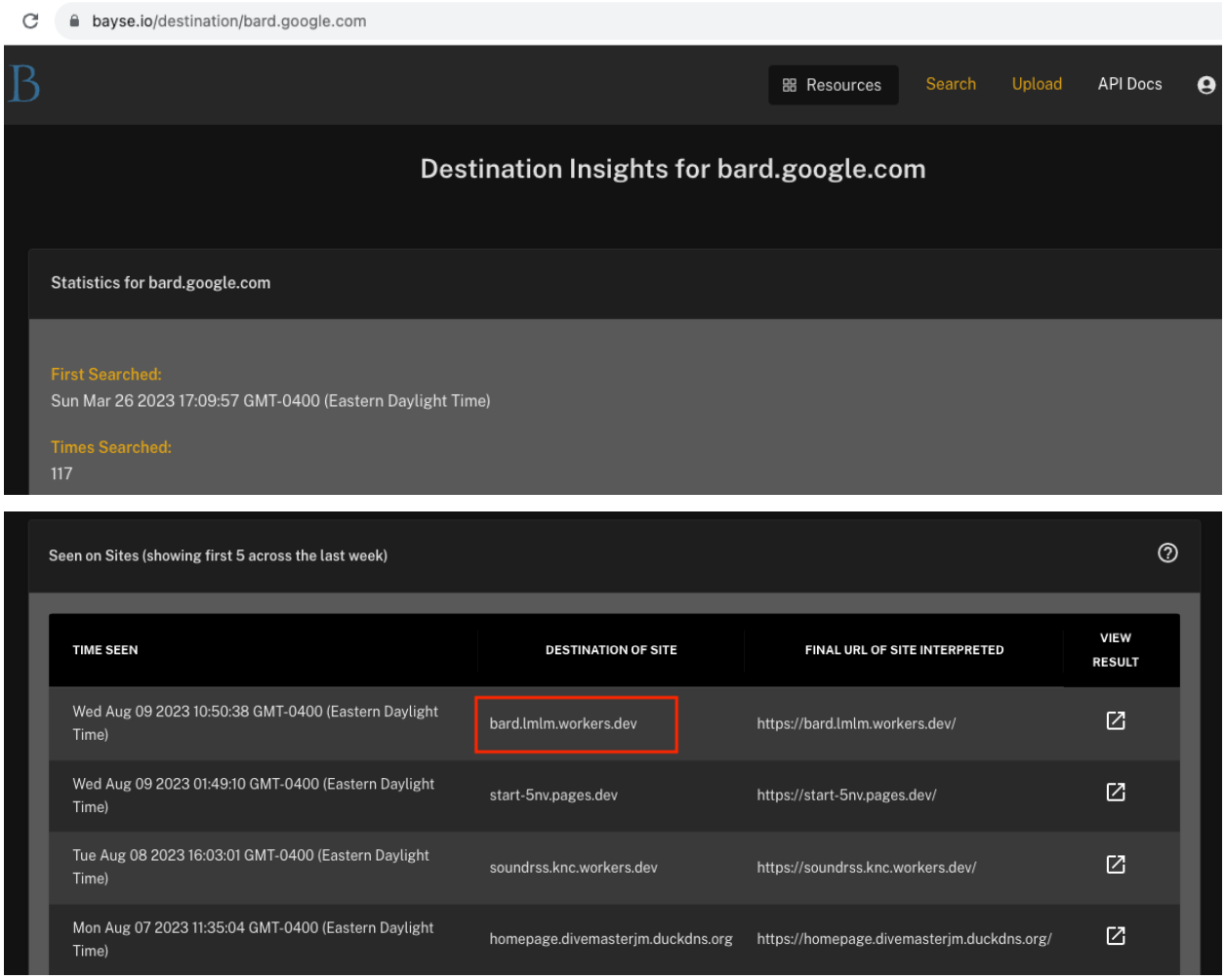


Part #2: Bayse's Campaign Analysis

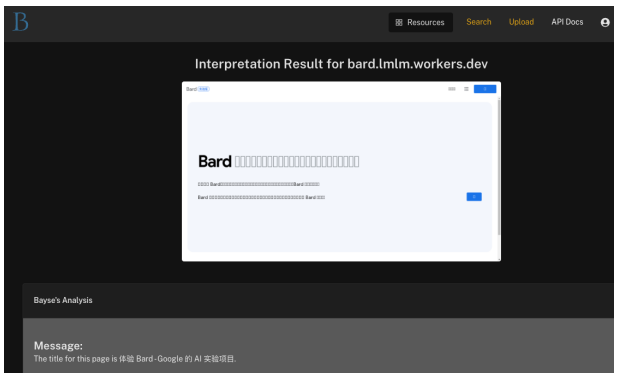
One of the main ways attackers impersonate highly valuable websites is to reproduce or clone their content. This raises the likelihood that a user will visually associate the spoofed site with the legitimate one and enable the attacker to achieve their objectives (collect credentials or PII, download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

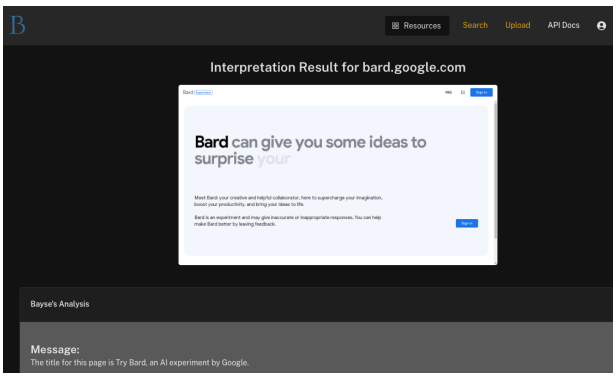
This tactic has been seen for several of these AI tools, but Bard was by far the most targeted.

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:

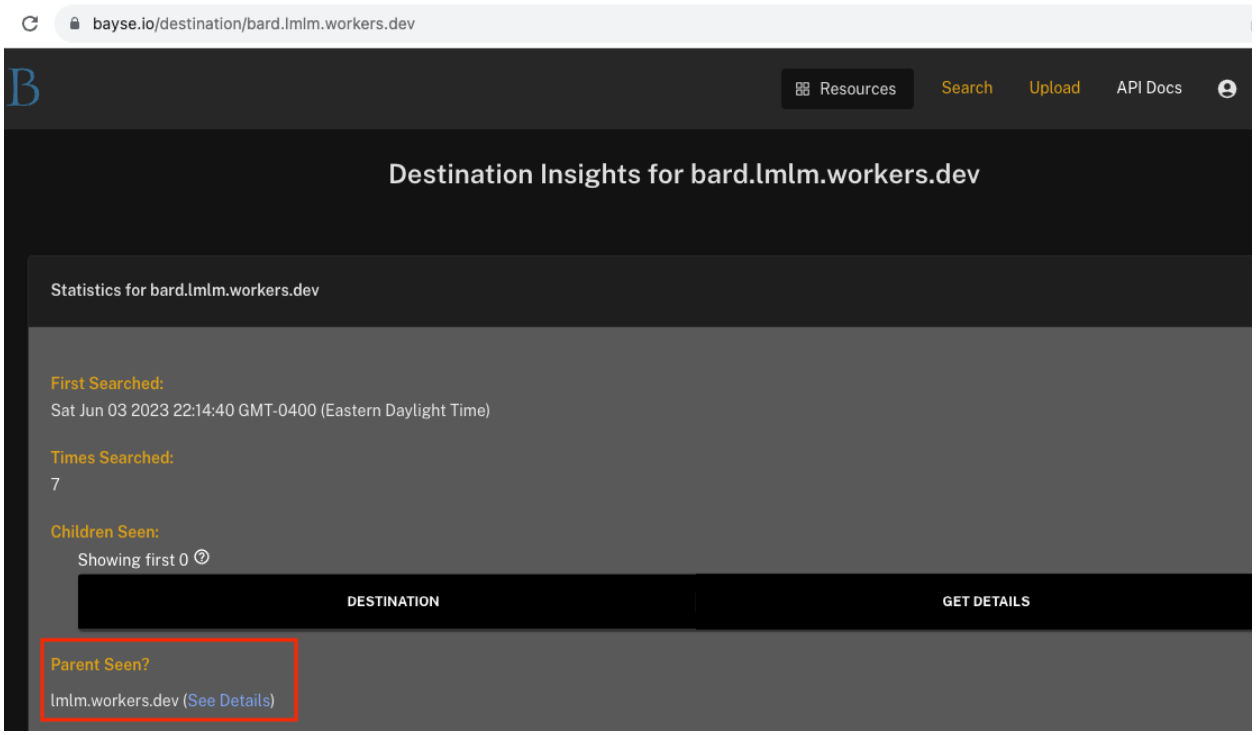


One of the sites that recently linked to Bard (highlighted above) is clearly impersonating Bard:

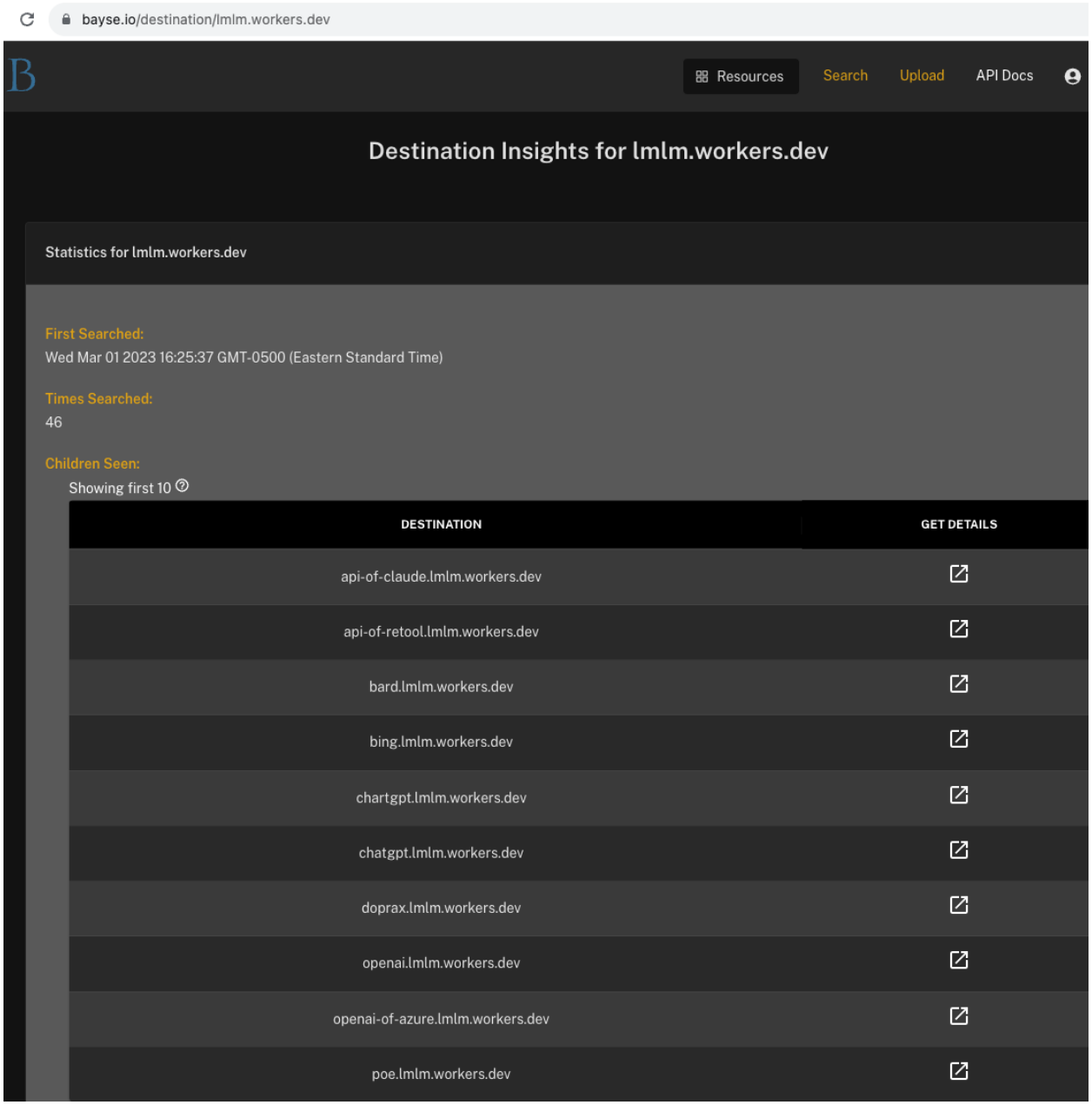




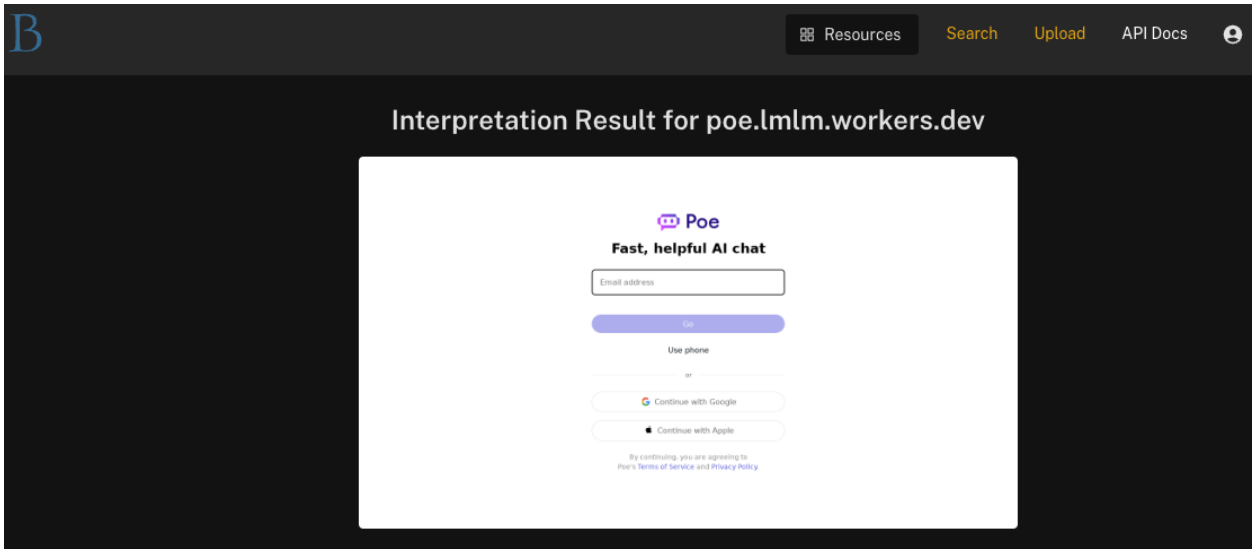
Moreover, it has been seen multiple times over the last two months, and we've seen other sites associated with its parent domain (lmlm[.]workers[.]dev) as well:



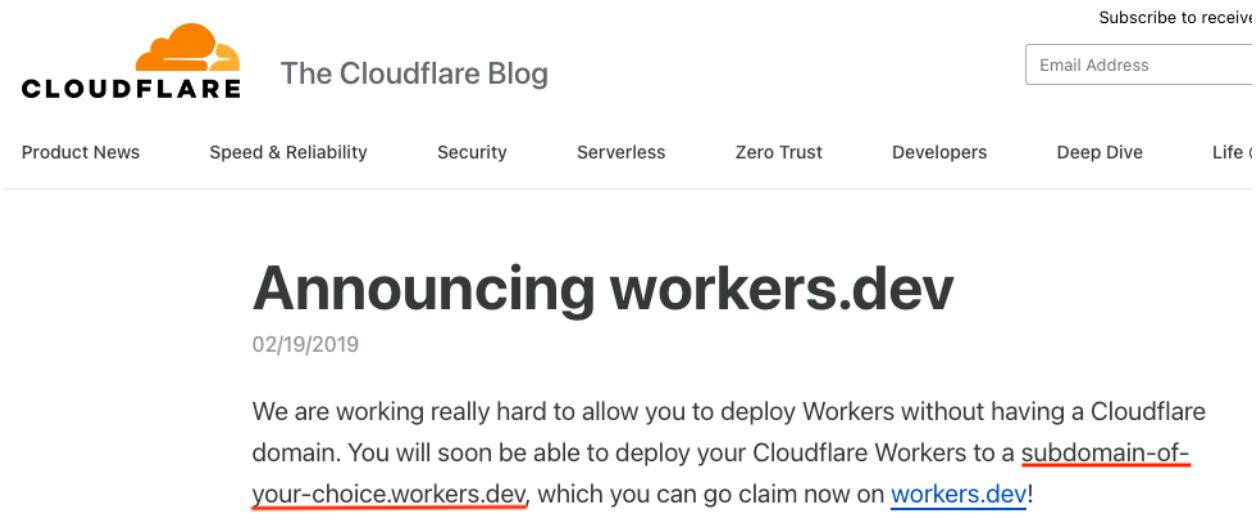
Pivoting to the parent domain's details shows us that not only is Bard targeted, but there's actually several other popular AI and cloud-related technologies being targeted since March 2023:



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:



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 or 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
- motional[.]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