DNS Abuse and Redirection: Enough for a New JS Malware to Hide Behind?

Table of Contents

Executive Report

DNS abuse combined with redirection seems to be gaining popularity as a stealth mechanism. We've just seen Decoy Dog employ the same tactic. More recently, a still-unnamed JavaScript (JS) malware has been wreaking havoc among WordPress site owners by abusing Google Public DNS to redirect victims to tech support scam sites.

Sucuri published an in-depth analysis of the JS malware where it named 30 domains and five IP addresses as indicators of compromise (IoCs). Our research team then sought to find other related threat artifacts through an IoC expansion analysis. Our DNS deep dive uncovered:

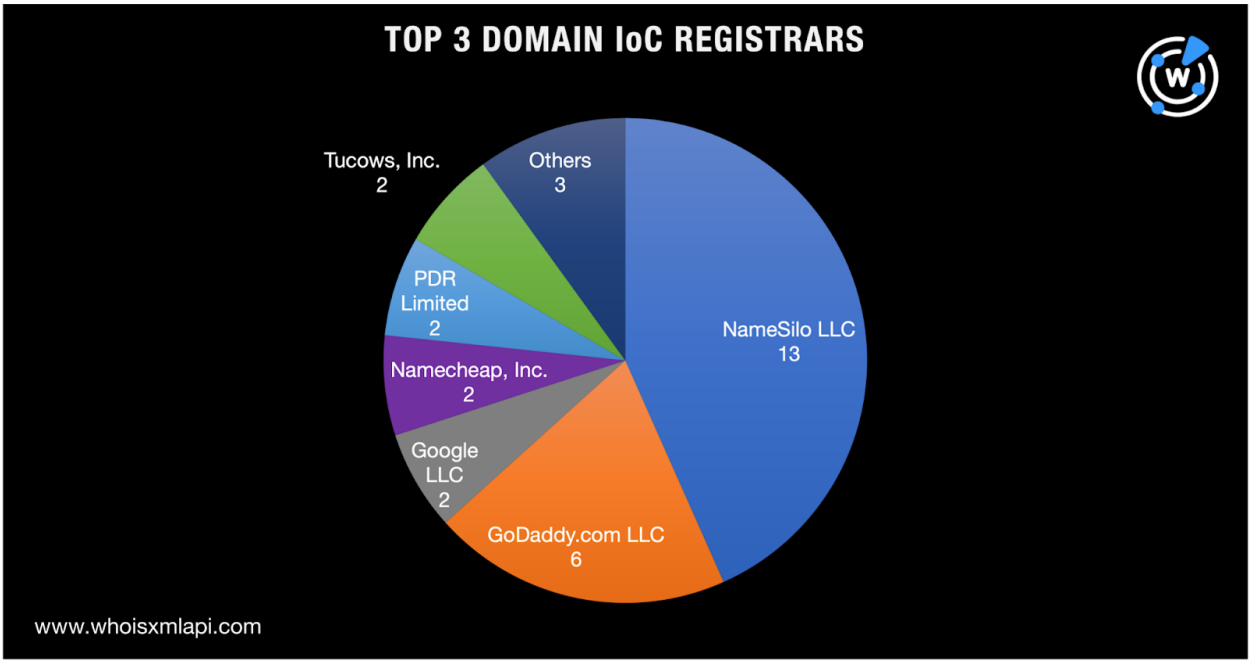
- Two unreported IP addresses to which some domains identified as IoCs resolved
- 330 domains that shared the dedicated IP addresses identified as IoCs and the additional ones we found as hosts, 157 of which turned out to be malicious according to a bulk malware check
- 101 domains that contained some of the strings found among those identified as IoCs

DNS Revelations about the IoCs

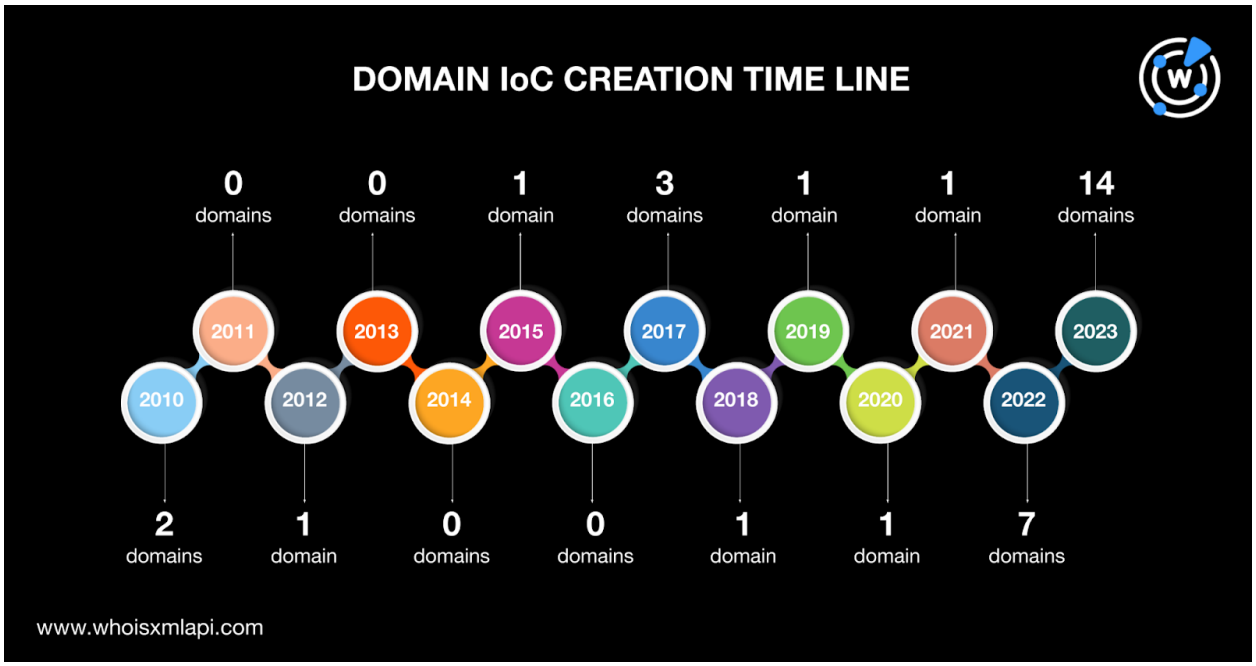
We began our analysis by looking more closely at the IoCs that Sucuri already published.

First, we subjected the 30 domains identified as IoCs to a bulk WHOIS lookup that led to these discoveries:

- The domains were administered by 10 registrars topped by NameSilo LLC in first place (13 IoCs). GoDaddy.com LLC took the second spot with six domains. Google LLC; Namecheap, Inc.; PDR Limited; and Tucows, Inc. shared third place with two IoCs each. The remaining three domains were spread across three registrars.



- The IoCs were registered between 2010 and 2023. Further scrutiny revealed that a majority (14 domains) were created just this year. And since another seven IoCs were created in 2022, it's possible that the threat actors favored using newly registered domains (NRDs) in their campaigns.



- The majority of the domains (20 IoCs) were registered in the U.S. Two each were registered in Canada, Iceland, and the U.K. Finally, one each was registered in Brazil, Poland, and Vietnam. One domain didn't have a publicly viewable registrant country.

Next, we subjected the five IP addresses identified as IoCs to a bulk IP geolocation lookup that led to these findings:

- Each IP address traced back to a different country—China, Finland, Germany, the U.K., and Russia. And the U.K. was the only one that also appeared on the list of registrant countries.
- Two of the IoCs were administered by OVH while the remaining three were spread across AS5398 SA, Hetzner Online GmbH, and Kisara LLC.

New DNS Discoveries

Our bulk WHOIS lookup earlier also revealed that three of the domains identified as IoCs had public registrant email addresses. Through reverse WHOIS pivoting, we found that two of them were used to register two domains that weren't part of Sucruri's list. The first domain, agenciafleek[.]com led to an error page and shared IoC ojosclear[.]com's registrant email address. The second, suffolktrackofficials[.]org, meanwhile, was unreachable at the time of writing but shared IoC look-alike suffolktrackofficials[.]com's registrant email address.

Next, we performed DNS lookups for the 30 domains identified as IoCs and found two IP address resolutions not on the current IoC list. While both 165[.]232[.]94[.]190 and 192[.]124[.]180[.]195 originated from the Netherlands, they had different Internet service providers (ISPs). 165[.]232[.]94[.]190 was under DigitalOcean, LLC management while 192[.]124[.]180[.]195 fell under Teknology SA's purview.

We then subjected the seven IP addresses (five IoCs and two newly discovered artifacts) to reverse IP lookups, which revealed that five of them were seemingly dedicated hosts. They were shared by 330 other domains that weren't part of the existing IoC list. A bulk malware check showed that nearly half of them (157 to be exact) were classified as malicious.

As the last step, we used Domains & Subdomains Discovery to determine if other domain names containing some of the strings present in the 30 domains identified as IoCs were present in the DNS. We found that 11 strings in some of the IoCs also appeared in 101 other domain names. These strings were:

- **bonuspremium.**
- **datingdudes.**
- **hitjackpot.**
- **ntertane.**

- **premiumwin.**
- **prizeforall.**
- **profitmagnet.**
- **suffolktrackofficials.**
- **sweetsbonus.**
- **tracker-cloud.**
- **wantafile.**

While none of the 101 string-connected domains have been dubbed malicious to date, some did bear other similarities with the IoCs, such as:

- 14% of the potentially related artifacts shared four of the IoCs' registrars.
- 20% of the similar-looking domains shared some of the IoCs' creation years.
- One of the potentially related artifacts shared one IoC's registrant name.
- 17% of the similar-looking domains shared three of the IoCs' registrant countries.

—

Our deep dive found hundreds of malicious domains that shared the IoCs' dedicated IP hosts. As threat actors behind the JS malware intend to hide behind traffic redirection in the DNS, those breadcrumbs could help further study and understand the technique.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

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

IoCs Sucuri Identified

- account[.]sparkofme[.]com
- apptradecoin[.]com
- autodiscover[.]staging[.]kennedypostacute[.]com
- backbushooh[.]live
- bonuspremium[.]life
- cnctddot[.]com
- datingdudes[.]life
- domaintravelers[.]com
- gostaustralia[.]com
- hitjackpot[.]life
- keepbonusforwin[.]life
- koloshuk[.]com
- ntertane[.]com
- ojosclear[.]com
- ourscarletstories[.]com

- premiumwin[.]life
- prize-sense[.]life
- prizeforall[.]life
- profitmagnet[.]life
- prottopecart[.]com
- stowesupperclub[.]com
- suffolktrackofficials[.]com
- super-game-4adult[.]life
- sweet-big-win[.]life
- sweetsbonus[.]life
- tracker-cloud[.]com
- wantafile[.]live
- woocommerce-pdf-invoice[.]com
- woocommerce-sagepayments[.]com
- yournickatmine[.]com
- 135[.]125[.]135[.]44
- 185[.]155[.]184[.]208
- 185[.]161[.]248[.]253
- 54[.]37[.]5[.]34
- 65[.]21[.]30[.]17

Sample IP-Connected Domains

- 1033[.]carbyecue[.]live
- 1055[.]carbyecue[.]live
- 108[.]carbyecue[.]live
- 1710[.]wingbenmass[.]live
- 1714[.]wingbenmass[.]live
- 1715[.]wingbenmass[.]live
- 177[.]wingbenmass[.]live
- 1934[.]donemagbuy[.]live
- 1948[.]donemagbuy[.]live
- 1xbet-23[.]com
- 2018[.]donemagbuy[.]live
- 2031[.]donemagbuy[.]live
- 2047[.]donemagbuy[.]live
- 2058[.]donemagbuy[.]live
- 2125[.]techsaidspy[.]live
- 2126[.]copmedloss[.]live
- 2145[.]halltapewild[.]live
- 2146[.]halltapewild[.]live
- 632[.]clubsameown[.]live
- 745[.]clubsameown[.]live
- 885zpop[.]com
- admin[.]asoprocafenpa[.]com
- african-architecture[.]org
- ahisweb[.]com
- albaiik[.]kelaskontraktor[.]com
- alsetdrop[.]live
- amdustgym[.]live
- anafaceoft[.]live
- andstopwine[.]live
- anypii[.]com
- aptcosttoe[.]live
- artelfbo[.]live
- asoprocafenpa[.]com
- autostrats[.]com
- awaycashweek[.]live
- backagpam[.]live
- backbushooh[.]live
- batpepeft[.]live
- baybedvow[.]live
- beandlivebetter[.]com
- bedpathmat[.]live
- beenpaywild[.]live
- beltfortink[.]live
- best[.]kelaskontraktor[.]com
- bestdams[.]com
- big[.]ahisweb[.]com
- bigtoysnft[.]com
- bihurtfat[.]live
- bilirdisi[.]com
- bitranmad[.]live

Sample Malicious IP-Connected Domains

- 1033[.]carbyecue[.]live
- 1055[.]carbyecue[.]live
- 108[.]carbyecue[.]live
- 2047[.]donemagbuy[.]live
- 2126[.]copmedloss[.]live
- 2145[.]halltapewild[.]live
- 2146[.]halltapewild[.]live
- alsetdrop[.]live
- amdustgym[.]live
- anafaceoft[.]live
- andstopwine[.]live
- aptcosttoe[.]live
- artelfbo[.]live
- awaycashweek[.]live
- backagpam[.]live
- backbushooh[.]live
- baybedvow[.]live
- bedpathmat[.]live
- beenpaywild[.]live
- beltfortink[.]live
- bihurtfat[.]live
- bitranmad[.]live
- bizicyass[.]live
- blackledgelegal[.]com
- bonus-premium[.]life
- bushbunshot[.]live
- busyhardlo[.]live
- bwhitenyc[.]com
- camebiscook[.]live
- carbyecue[.]live
- chatnotetot[.]live
- claumusic[.]com
- clubsameown[.]live
- codtimeicy[.]live
- connectpickthing[.]top
- copmedloss[.]live
- corselfcop[.]live
- cowdenala[.]live
- crewhubnow[.]live
- dabroadex[.]live
- dadahasafe[.]live
- darulenews[.]live
- datefallinch[.]live
- deadsolcost[.]live
- deandeadhold[.]live
- dejeonco[.]com
- delayedreleasecapsule[.]com
- delivbikes[.]com
- delivery[.]kfc[.]hk[.]powermanexchange[.]com
- desknayboy[.]live

Sample String-Connected Domains

- bonuspremium[.]ga
- bonuspremium[.]de
- bonuspremium[.]cf
- bonuspremium[.]ru
- bonuspremium[.]tk
- bonuspremium[.]pl
- bonuspremium[.]ml
- bonuspremium[.]gq
- bonuspremium[.]ist
- bonuspremium[.]com
- bonuspremium[.]faith
- topbonuspremium[.]tk
- topbonuspremium[.]com
- letsbonuspremium[.]com
- 1xbonuspremium[.]space
- bonuspremium[.]istanbul
- casinobonuspremium[.]com
- garantibonuspremium[.]ist
- garantibonuspremium[.]istanbul
- datingdudes[.]de
- datingdudes[.]com
- thedatingdudes[.]com

- adultdatingdudes[.]com
- divasdatingdudes[.]com
- dollsdatingdudes[.]com
- onlinedatingdudes[.]com
- realitydatingdudes[.]cloud
- hitjackpot[.]uk
- hitjackpot[.]top
- hitjackpot[.]net
- hitjackpot[.]fun
- hitjackpot[.]com
- ihitjackpot[.]com
- hitjackpot[.]site
- hitjackpot[.]co[.]uk
- hitjackpot[.]space
- hitjackpot[.]online
- kinghitjackpot[.]com
- hitjackpot[.]website
- quickhitjackpot[.]com
- entertane[.]com
- ntertane[.]co[.]uk
- premiumwin[.]de
- premiumwin[.]pw
- premiumwin[.]bid
- premiumwin[.]xyz
- premiumwin[.]com
- premiumwin[.]shop
- premiumwin[.]live
- mypremiumwin[.]life