Igniting a DNS Spark to Investigate the Inner Workings of SparkCat

Table of Contents

Executive Report

SecureList recently published a study of Android and iOS apps that have been laced with a malicious software development kit (SDK) dubbed “SparkCat” that steals crypto wallet recovery phrases. The infected apps on Google Play have been downloaded 242,000+ times. The malicious apps were also probably the first stealers made available on Apple’s App Store. Based on the malware time stamps and configuration file creation dates found in GitLab repositories, SparkCat has been active since March 2024.

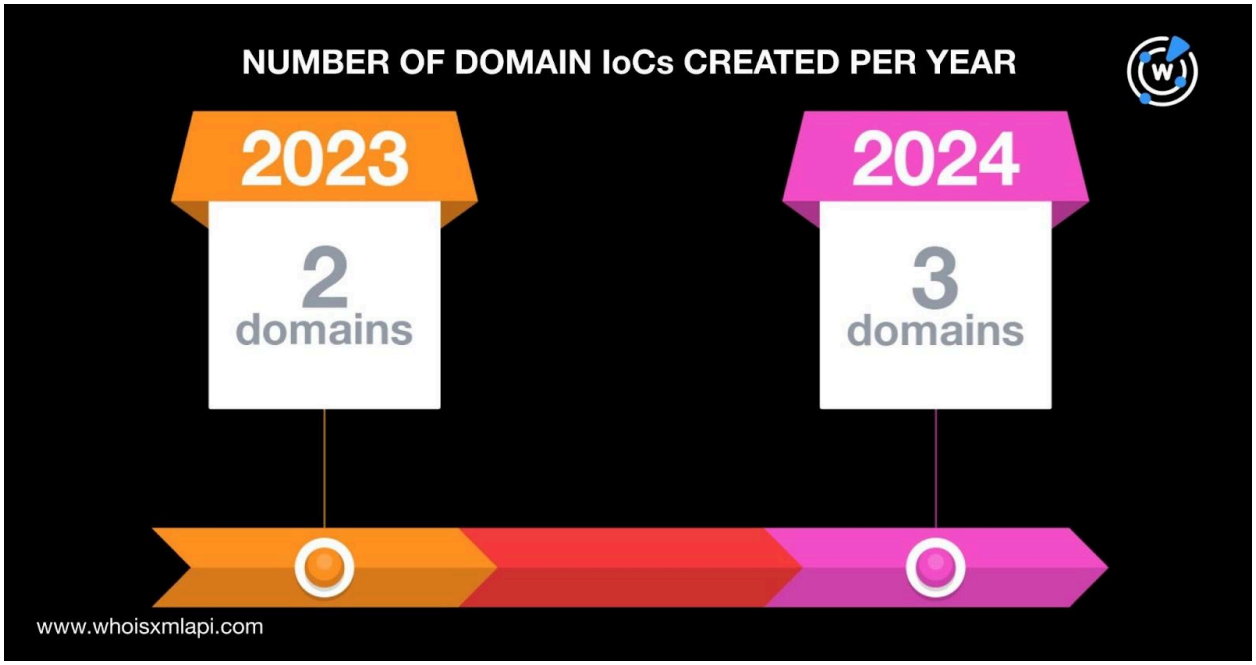
The report “Take My Money: OCR Crypto Stealers in Google Play and App Store” identified five domains as indicators of compromise (IoCs), which the WhoisXML API research team expanded through a DNS intelligence analysis. We uncovered various connected web properties comprising:

- 611 email-connected domains, one of which turned out to be malicious
- 179 string-connected domains, one of which has already been weaponized for attacks

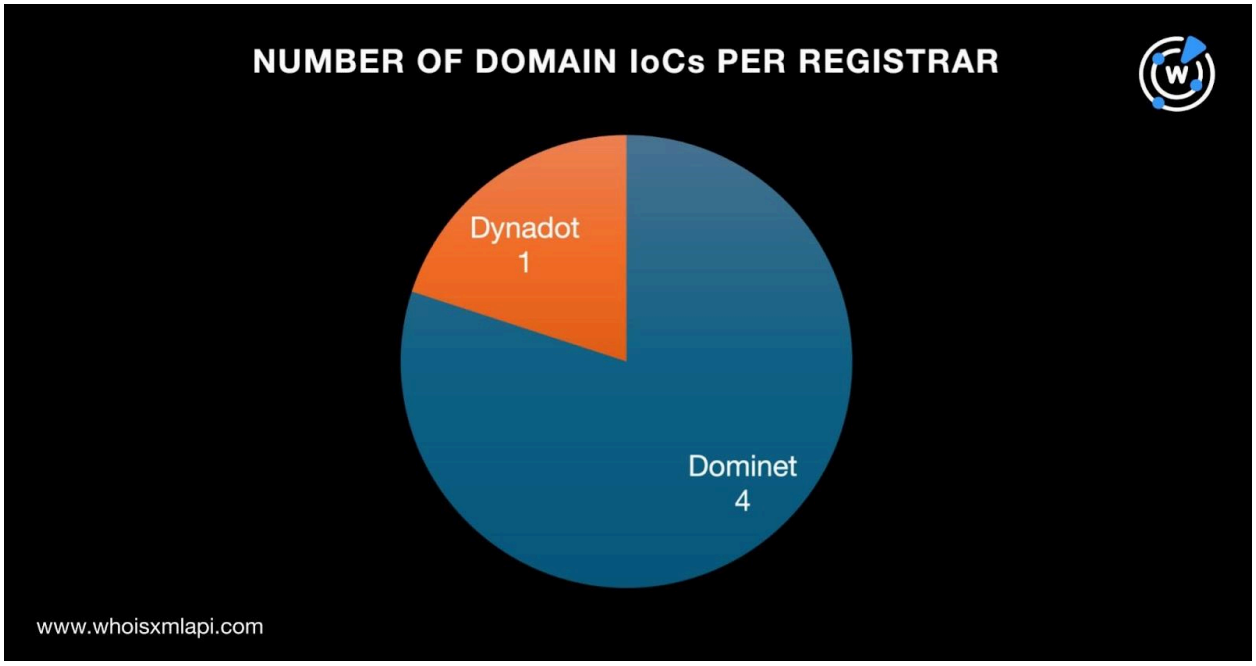
More about the SparkCat IoCs

As is our usual first step in expanding IoC lists, we sought to obtain more information about the IoCs. We queried the five domains identified as IoCs on Bulk WHOIS API and found that:

- They were fairly new domains. Specifically, two were created in 2023 and three in 2024.



- They were split between two registrars led by Dominet, which accounted for four domains. One domain was administered by Dynadot.



- Only two of the domains had registrant countries in their current WHOIS records, that is, Lao People's Democratic Republic (PDR).

A query for the five domains on DNS Chronicle API showed that only two had historical IP resolutions. Specifically, they had two IP resolutions. The domain with the older first IP resolution date—19 October 2023—was aliyung[.]com. The domain googleapps[.]top, meanwhile, recorded its first IP resolution on 24 December 2023.

SparkCat IoC List Expansion Analysis Findings

We started our search for connected artifacts by querying the five domains identified as IoCs on WHOIS History API. Two of them had 11 email addresses in their historical WHOIS records after duplicates were filtered out. A closer examination of the 11 email addresses revealed that six of them were public addresses.

We then queried the six public email addresses on Reverse WHOIS API and found that none of them appeared in the current WHOIS records of other domains. So, we dug deeper. Another query, this time accessing historical WHOIS records, revealed that three of the email addresses were likely not owned by domainers and had existing connections. In particular, they appeared in the historical WHOIS records of 611 email-connected domains after duplicates and those already identified as IoCs were filtered out.

A Threat Intelligence API query for the 611 email-connected domains showed that one of them—atozb[.]com—was associated with a generic threat.

Next, we queried the five domains identified as IoCs on DNS Lookup API and found that none of them actively resolved to IP addresses. That halted our search for IP-connected domains.

After that, we looked for domains that started with the same text strings as the five already identified as IoCs. Our searches on Domains & Subdomains Discovery revealed that out of the four strings (i.e., one was used in two IoCs) on our list, only these three appeared in other domains:

- 99ai.
- aliyung.
- googleapps.

Specifically, the three text strings above appeared at the beginning of 179 string-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

A Threat Intelligence API query for the 179 string-connected domains showed that one—googleapps[.]xyz—has already been weaponized for malware distribution.

As a final step, we queried the two malicious connected domains on Screenshot API and found that both were already unreachable, potentially taken down by their owners.

Are We Seeing Traces of Future Typosquatting Attacks?

Upon further scrutiny of all of the connected artifacts we have obtained so far, we noticed that many had these text strings, which also appeared in the domains identified as IoCs:

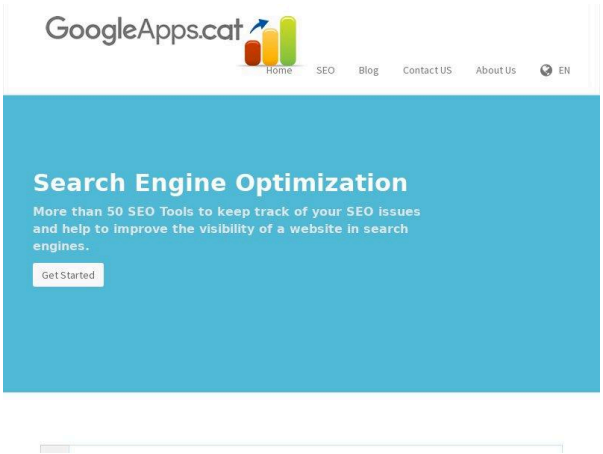
- **aliyung.**, which could be a typosquatting variant of Aliyun, another name Alibaba Cloud is known as
- **googleapps.**, which contains the Google brand name

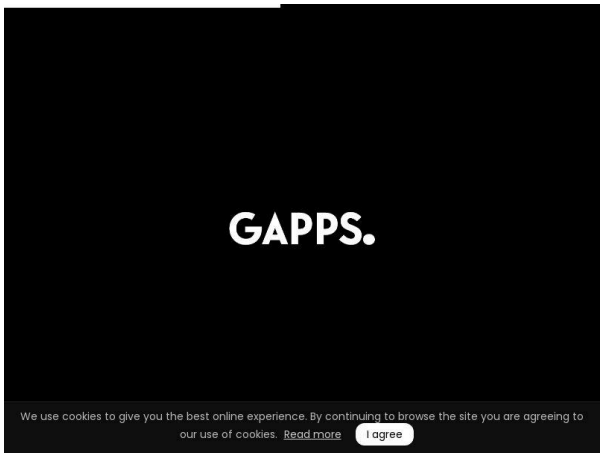
While the SparkCat threat actors may have also preyed upon Firebase users, as evidenced by the IoC firebaseo[.]com, our list of all connected domains did not contain domains with the brand.

We uncovered four connected domains with the string **aliyung.**, none of which were publicly attributable to Alibaba Cloud based on the results of our Bulk WHOIS API query that showed their registrant details.

Meanwhile, we collated 123 connected domains with the text string **googleapps.**, only 15 of which could be publicly attributed to Google based on the registrant information in their current WHOIS records.

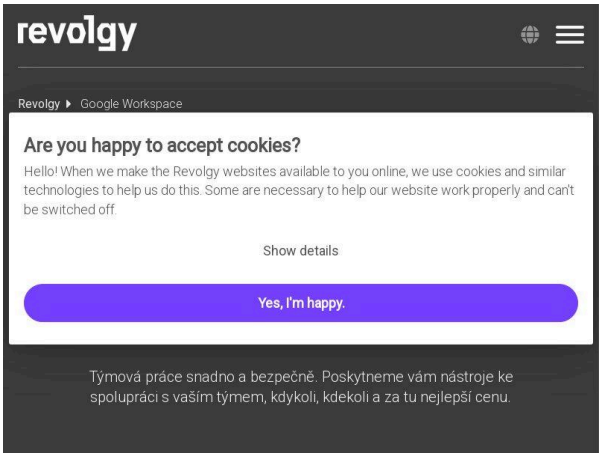
A Screenshot API query for the 112 unattributable brand-containing domains (108 for Google and four for Alibaba Cloud) showed that 13 remained accessible to date. While most led to blank or parked pages, three led to content.





googleapps[.]cat

googleapps[.]co[.]nz



googleapps[.]cz

—

Our DNS deep dive into the SparkCat IoCs led to the discovery of 790 connected artifacts comprising 611 email-connected domains and 179 string-connected domains. To date, two of them have already played a part in malicious campaigns.

We also discovered that 112 of the connected domains we unearthed contained text strings related to the two tech giants named earlier even if they could not be publicly attributed to the companies based on the registrant details in their current WHOIS records.

If you wish to 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

Sample Email-Connected Domains

- 0905590099[.]com
- 100person[.]com
- 100persons[.]com
- a1988[.]com
- actualitefrancais[.]com
- ad0577[.]com
- baihoctructuyen[.]com
- baixingtang[.]com[.]cn
- banmua24h[.]net
- cachenet[.]cn
- canadaglobe[.]net
- carspost[.]net
- danzige[.]com
- darge[.]cn
- dattroi[.]com
- eastflour[.]com
- elect8[.]com
- energyresources[.]cn
- f2cn[.]net
- face-news[.]net
- fajm[.]gov[.]cn
- galaxygiare[.]com
- gamespost[.]net
- gatbi[.]com
- hcdx[.]org
- hch111[.]com
- hchzq[.]gov[.]cn
- ihv[.]cn
- iih[.]cn
- inyulu[.]com
- j-skw[.]com
- jbc0000[.]com
- jbc0888[.]com
- kaiwofishing[.]com
- katemoss[.]cn
- keylead[.]cn
- lastendencias[.]net
- latestvisitors[.]com
- lestendances[.]net
- maichengxu[.]com
- maitianguaiquan[.]com
- makebtg[.]com
- nalisha[.]com
- nbgct[.]net
- nblyxh[.]com
- onlinejobsworking[.]com
- ooath[.]net
- orthophosphoric-acid[.]com
- past[.]hk
- pcate[.]net
- poath[.]net
- qaposts[.]com
- qingcaofireworks[.]com
- qoath[.]net
- r-news[.]net
- rcjxyz[.]com
- recommendednews[.]net
- sanlimedical[.]com
- scjrly[.]com
- sclyt[.]com
- tailieubk[.]com
- tailieubk[.]net
- tegou[.]com[.]cn
- uoath[.]net
- urlinquiry[.]com
- urlsinfo[.]com
- vgbbs[.]com
- vn45[.]com
- vn75[.]com
- w3-info[.]com
- wadecn[.]com
- webs-info[.]com

- xfw[.]gov[.]cn
- xhxgtzyj[.]gov[.]cn
- xiangai365[.]com
- yananda[.]com
- yanshaoutlets[.]com
- ybedu[.]cn
- zbajj[.]gov[.]cn
- zetney[.]com
- zetney[.]net

Sample String-Connected Domains

- 99ai[.]ai
- 99ai[.]app
- 99ai[.]art
- aliyung[.]cc
- aliyung[.]cn
- aliyung[.]top
- googleapps[.]academy
- googleapps[.]ae
- googleapps[.]ai