Uncovering DNS Details on Operation Celestial Force

Table of Contents

Executive Report

Advanced persistent threat (APT) groups will employ any means necessary to compromise the networks of their intended targets. And for Cosmic Leopard, that means using GravityRAT, an Android-based malware, and HeavyLift, a Windows-based malware loader, in their most recent operation Cisco Talos has dubbed "Operation Celestial Force."

Cisco Talos's in-depth investigation of Operation Celestial Force published 19 domains identified as indicators of compromise (IoCs). The WhoisXML API research team sought to find out if other threat artifacts could be found in the DNS via an IoC expansion analysis.

Our DNS deep dive led to the discovery of:

- Three email-connected domains
- 15 IP addresses, all of which turned out to be malicious
- 35 string-connected domains
- 3,927 brand-containing domains, nine of which turned out to be associated with various threats

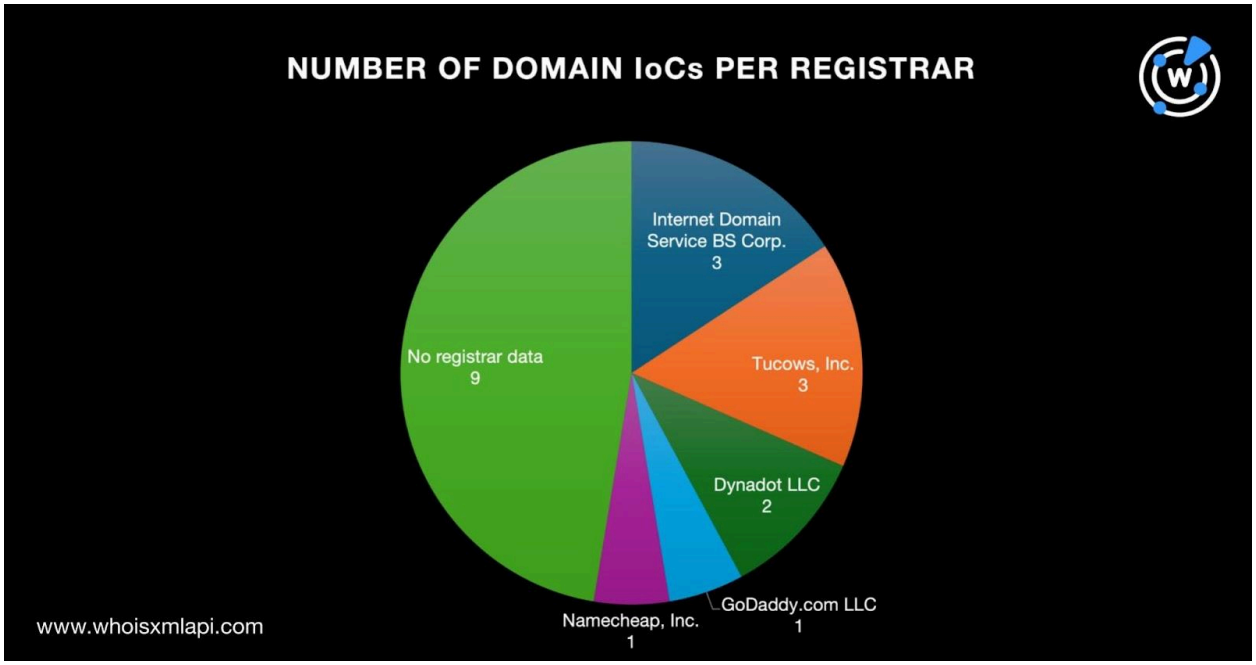
A sample of the additional artifacts obtained from our analysis is available for download from our website.

Operation Celestial Force IoC Facts

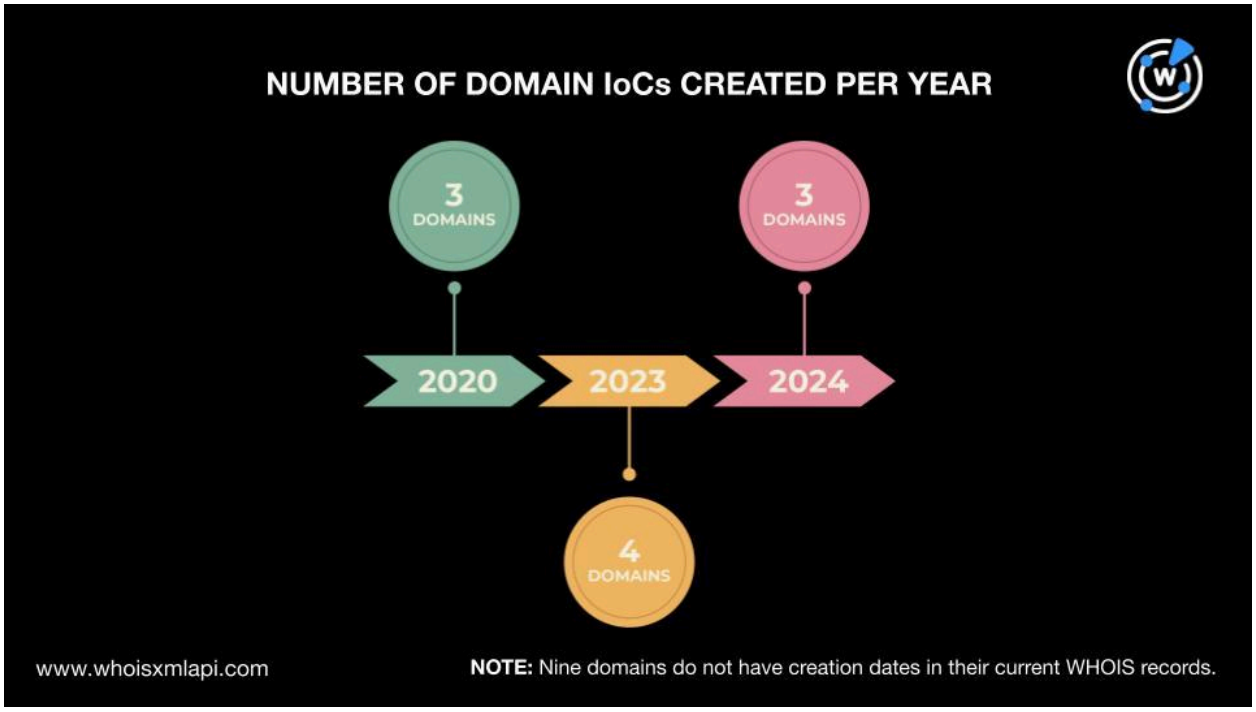
We began our analysis by subjecting the 19 domains identified as IoCs to a bulk WHOIS lookup, which revealed that:

- Internet Domain Service BS Corp. and Tucows, Inc. topped the list of registrars, accounting for three domain IoCs each. Dynadot LLC took the second spot with two

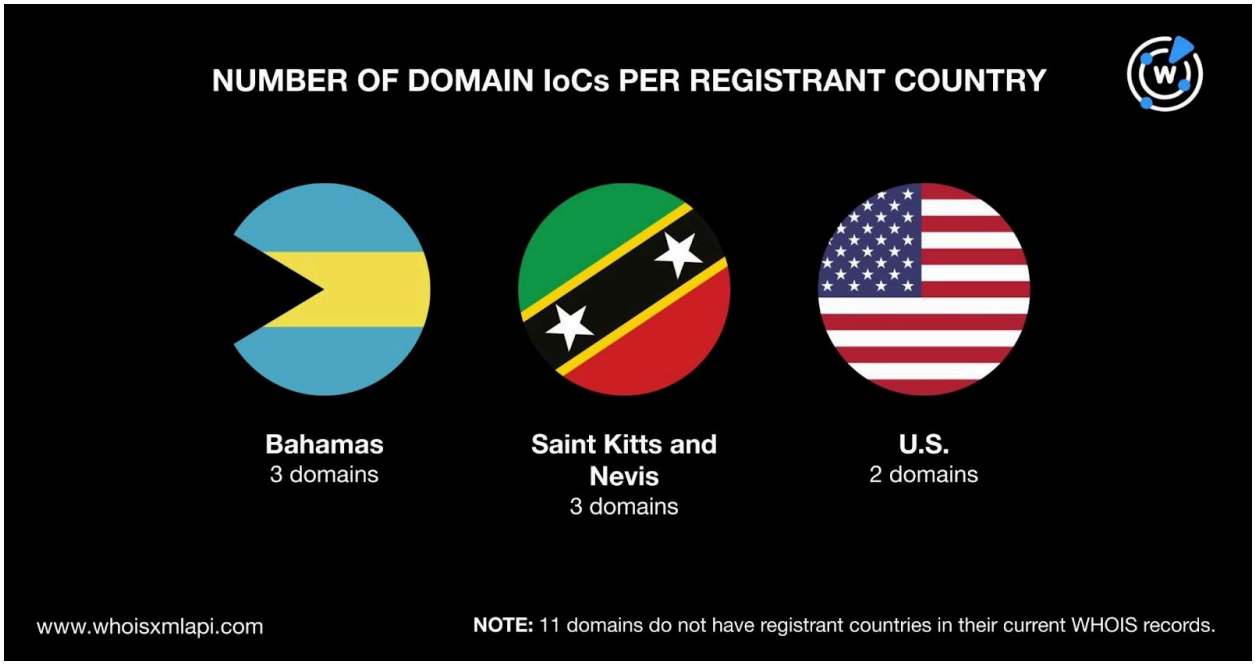
domain IoCs. One IoC each fell under the purview of GoDaddy.com LLC and Namecheap, Inc. Finally, nine domain IoCs did not have registrars in their current WHOIS records.



- The Cosmic Leopard APT group seems to prefer using somewhat recent or newly registered domains (NRDs) for their Operation Celestial Force campaign. Three domain IoCs were created in 2020, four in 2023, and three in 2024.



- The Bahamas and Saint Kitts and Nevis tied as the top registrant countries, accounting for three domain IoCs each. The U.S. accounted for two domain IoCs. Finally, 11 domain IoCs do not have registrant countries in their current WHOIS records.



Operation Celestial Force IoC List Expansion Findings

Our search for Operation Celestial Force artifacts started with running WHOIS History API queries for the 19 domains identified as IoCs. We collated 33 email addresses after filtering out duplicates from their historical WHOIS records. Only one of them, however, was a public email address.

A Reverse WHOIS API query for the sole public email address led to the discovery of three email-connected domains after filtering out duplicates and the IoCs.

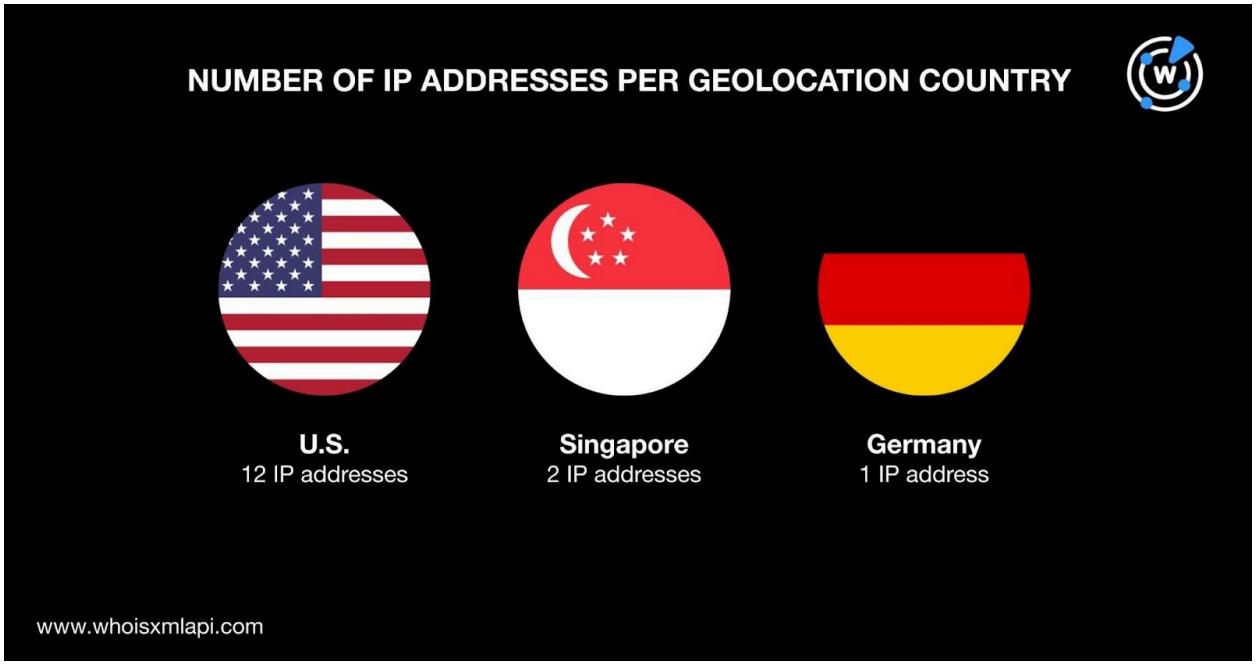
To uncover more threat artifacts, we performed DNS lookups for the 19 domains identified as IoCs. We found out that they resolved to 15 IP addresses in total after filtering out duplicates. Threat intelligence lookups for them showed that they were all associated with various threats. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREATS
18[.]141[.]10[.]107	Command and control (C&C) Generic Malware Spam
173[.]255[.]194[.]134	Attack C&C Generic Malware Phishing
198[.]58[.]118[.]167	Attack C&C Generic Malware Phishing Spam Suspicious
45[.]33[.]18[.]44	Attack C&C Generic Malware Phishing Spam Suspicious

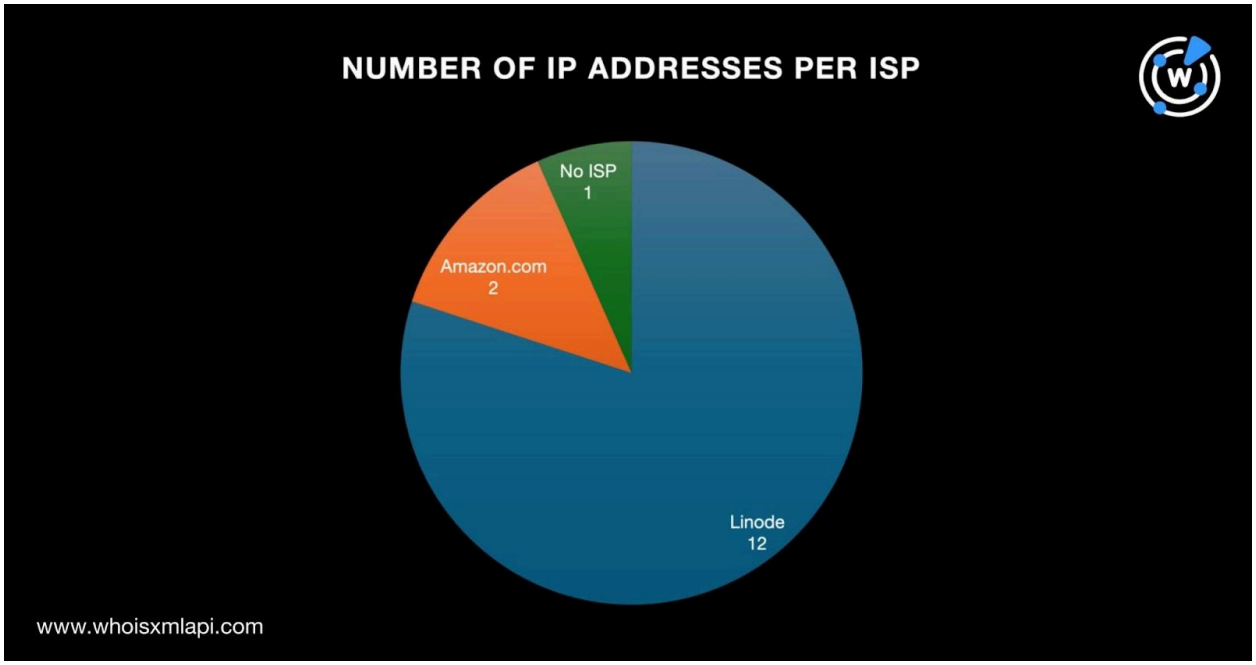
45[.]33[.]2[.]79	Attack C&C Generic Malware Phishing Spam Suspicious

To know more about the 15 IP addresses, we performed a bulk IP geolocation lookup that revealed that:

- A majority of them, 12 to be exact, are geolocated in the U.S. Singapore accounted for two IP addresses. The last IP address originated from Germany.



- Fourteen of the IP addresses were split between two ISPs. Linode accounted for 12 IP addresses while Amazon.com handled two. One IP address did not have an ISP mentioned in its IP geolocation record.



Next, we conducted reverse IP lookups for the 15 IP addresses and found out that the Cosmic Leopard threat actors seemingly preferred to use shared hosts. Unfortunately, that halted our search for IP-connected domains as the presence of false positives was far too likely.

We then moved on toward finding domains that started with the exact strings as those identified as IoCs and were created on 1 January 2020 onward. Our Domains & Subdomains Discovery searches revealed that only seven of the domain IoC text strings appeared in other domains. They are:

- **cloudieapp.**
- **craftwithme.**
- **cvscout.**
- **rockamore.**
- **sexyber.**
- **teraspace.**
- **webbucket.**

We uncovered 35 string-connected domains after filtering out duplicates, the IoCs, and email-connected domains.

Our first look at the 19 domains identified as IoCs showed that six contained popular brands—**android**, **java**, **mozilla**, and **playstore**—that other threat actors could abuse. We used them as search strings to look for brand-containing domains. Note, however, that we limited our searches to domains that started with the four strings created on 1 January 2024 onward. Domains & Subdomains Discovery allowed us to obtain 3,927 brand-containing domains after filtering out duplicates, the IoCs, and email- and string-connected domains.

Threat Intelligence API queries for the 3,927 brand-containing domains showed that nine of them were associated with various threats, specifically malware distribution, generic threats, and phishing. Take a look at five examples below.

MALICIOUS BRAND-CONTAINING DOMAIN	ASSOCIATED THREATS
androidstaticserve[.]com	Malware
javajive[.]xyz	Generic Phishing
javajourney[.]xyz	Generic Phishing
javajoy[.]xyz	Generic Phishing
playstore-update[.]online	Malware

WHOIS record comparisons between the legitimate Android, Java, Mozilla, and Play Store domain names and the 3,927 brand-containing domains using their registrant organizations as reference revealed that:

- Only nine of the **android**-containing domains shared android[.]com's registrant organization and so can be publicly attributed to Android owner Google.
- None of the **java**-containing domain names shared java[.]com's registrant organization, meaning Java did not own any of them.
- Only one of the **mozilla**-containing domains shared mozilla[.]org's registrant organization, which means the rest could potentially belong to typosquatters.
- None of the **playstore**-containing domain names shared play[.]google[.]com's registrant organization so they could all be typosquatting domains.

—

Our analysis of the Operation Celestial Force IoCs led to the discovery of 3,980 potentially connected artifacts comprising three email-connected domains, 15 IP addresses, 35 string-connected domains, and 3,927 brand-containing domains. Twenty-four of these newly uncovered threat artifacts have been weaponized for various attacks, most notably phishing and malware distribution.

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

- mipaginaprofesional[.]com
- mpmutchapizza[.]com

Sample IP Addresses

- 173[.]255[.]194[.]134
- 18[.]141[.]10[.]107
- 18[.]143[.]155[.]63
- 198[.]58[.]118[.]167
- 45[.]33[.]18[.]44
- 45[.]33[.]2[.]79
- 45[.]33[.]20[.]235
- 45[.]33[.]23[.]183

Sample Malicious IP Addresses

- 173[.]255[.]194[.]134
- 18[.]141[.]10[.]107
- 18[.]143[.]155[.]63
- 198[.]58[.]118[.]167
- 45[.]33[.]18[.]44
- 45[.]33[.]2[.]79
- 45[.]33[.]20[.]235
- 45[.]33[.]23[.]183

Sample String-Connected Domains

- cloudieapp[.]com
- craftwithme[.]co[.]uk
- craftwithme[.]com
- craftwithme[.]com[.]au
- craftwithme[.]live
- craftwithme[.]net
- craftwithme[.]org
- cvscout[.]com
- cvscout[.]pro
- cvscout[.]ru
- cvscout[.]ws
- rockamore[.]com
- rockamore[.]nu
- sexyber[.]com
- teraspace[.]au
- teraspace[.]click
- teraspace[.]cloud
- teraspace[.]com

Sample Brand-Containing Domains

- android--underground[.]org
- android-07[.]ngo[.]ph
- android-07[.]org[.]ph
- android-08[.]arab
- android-12847155c6246107-wifi[.]com[.]ph
- android-13[.]vg
- android-145b546afcfb535e-wifi[.]ph
- android-15[.]int[.]la
- android-1753e072e0e6fb6d-wifi[.]aquila[.]it
- android-178ee449b3e40ef3-wifi[.]arab
- android-178ee449b3e40ef3-wifi[.]org[.]ws
- android-18[.]net[.]ph
- android-1843317ab737e06e[.]ws
- android-1950f32e1aa27b92-wifi[.]int[.]la
- android-1decae99099ed67f-wifi[.]lib[.]ms[.]us
- android-1e4706d972029f19-wifi[.]org[.]ph
- android-21a79e663b5fa376-wifi[.]edu[.]ws
- android-21da3b3d3a82f012-wifi[.]df[.]gov[.]br
- android-222201d39792eba3-wifi[.]mil[.]ph
- android-22a899e34e22af3b-wifi[.]ws
- android-2772846a718256a8-wifi[.]vg
- android-2a201fcb429a5940-wifi[.]edu[.]ws
- android-2ada5e5b00c1b1c0-wifi[.]net[.]ph
- android-2ada5e5b00c1b1c0-wifi[.]vg
- android-2bac18cc5ce0c676-wifi[.]ngo[.]ph
- android-2d9a33df0f18a239-wifi[.]edu[.]ws
- android-2d9aa80d195f373-wifi[.]org[.]ws
- android-2ff46dcdcfe45706-wifi[.]arab
- android-2ff46dcdcfe45706-wifi[.]int[.]la
- android-2ff46dcdcfe45706-wifi[.]ws
- android-304fd17e742b9d0b-wifi[.]com[.]ph
- android-304fd17e742b9d0b-wifi[.]net[.]ws
- android-30606e8f651d4b61-wifi[.]int[.]la
- android-323931fda0b4523c-wifi[.]ws
- android-34d33e52b85b441e-wifi[.]org[.]ws
- android-34f5636c396e945d-wifi[.]edu[.]ws
- android-3585a85109938256-wifi[.]edu[.]ws
- android-3a4828ff0536410e-wifi[.]edu[.]ws
- android-3a98bea176335d6e-wifi[.]edu[.]ws
- android-3e6d93e7b5104f71-wifi[.]edu[.]ws
- android-3f295a33363ccf62-wifi[.]aquila[.]it
- android-3f318e269cc1961d-wifi[.]com[.]ws

- android-3f318e269cc1961d-wifi[.]ngo[.]ph
- android-3lm8h8[.]com
- android-4-pc[.]ru
- android-41b28ad4fafed493[.]arab
- android-46c2795191927526-wifi[.]org[.]ws
- android-46e1bbadc5debb90-wifi[.]aquila[.]it
- android-46e1bbadc5debb90-wifi[.]edu[.]ws
- android-46e7fbd2275fd262-wifi[.]ph
- android-49d8dae93a6b6928-wifi[.]vg
- android-4a184b1452dfe0a9-wifi[.]arab
- android-4af6f0287fc4a061-wifi[.]aquila[.]it
- android-4af6f0287fc4a061-wifi[.]org[.]ws
- android-4c9feab09bd0b927-wifi[.]arab
- android-4d[.]icu
- android-4d[.]us
- android-4d4ce4ebce3c6dcd-wifi[.]vg
- android-4db44a7dee096031-wifi[.]int[.]la
- android-4f8420aeb2473302-wifi[.]com[.]ph
- android-4rabet[.]click
- android-504ccb417864d7e1-wifi[.]arab
- android-545e5fc25f39e7ca-wifi[.]int[.]la
- android-55d846489eced893-wifi[.]com[.]ph
- android-5607548b9a4bc026-wifi[.]ph
- android-5869a33473519153-wifi[.]df[.]gov[.]br
- android-59af16a921fdbe0-wifi[.]arab
- android-5ba4c83b35942917-wifi[.]net[.]ws
- android-6219290997c396ec-wifi[.]int[.]la
- android-623c5efd0421f375-wifi[.]mil[.]ph
- android-625d9c1b44dc01d9-wifi[.]com[.]ws
- android-64ba048401505f47-wifi[.]int[.]la
- android-669fff558ae5ef45-wifi[.]com[.]ws
- android-669fff558ae5ef45-wifi[.]edu[.]ws
- android-669fff558ae5ef45-wifi[.]ngo[.]ph
- android-6924ff73740cf28-wifi[.]aquila[.]it
- android-6924ff73740cf28-wifi[.]com[.]ph
- android-6924ff73740cf28-wifi[.]ngo[.]ph
- android-6924ff73740cf28-wifi[.]ph
- android-69ef707ce486793b-wifi[.]df[.]gov[.]br
- android-6cca247736419248-wifi[.]mil[.]ph
- android-6f203e55ce1c8e43-wifi[.]org[.]ws
- android-6f203e55ce1c8e43-wifi[.]ws
- android-71630e28d48bc902-wifi[.]net[.]ph
- android-71faaeadad00f258-wifi[.]com[.]ws
- android-7266a55fff9980c4-wifi[.]ws
- android-75a655fbb30fc479-wifi[.]org[.]ph

- android-7c5e29eb5084bde4-wifi[.]org[.]ph
- android-7c5e29eb5084bde4-wifi[.]ws
- android-7cfcc59ec2168cbf-wifi[.]int[.]la
- android-7e28f43cf0ed78eb-wifi[.]net[.]ws
- android-80ae075b50f332ea-wifi[.]df[.]gov[.]br
- android-80ae075b50f332ea-wifi[.]edu[.]ws
- android-81abf7b632613fb1-wifi[.]int[.]la
- android-81d68526d3fb18a1-wifi[.]arab
- android-81d68526d3fb18a1-wifi[.]int[.]la
- android-81d68526d3fb18a1-wifi[.]ws
- android-841d1c1252c567b7-wifi[.]org[.]ws
- android-845554cc76a006dd-wifi[.]aquila[.]it
- android-84742cdd64587769-wifi[.]df[.]gov[.]br

Sample Malicious Brand-Containing Domains

- androidstaticserve[.]com
- javajive[.]xyz
- javajourney[.]xyz
- javajoy[.]xyz
- javajubilee[.]xyz