DNS Spotlight: Rockstar2FA Shuts Down, FlowerStorm Starts Up

Table of Contents

Executive Report

It's not unusual for threat actors to pick up after fellow cyber attackers shut down their operations. Many of them still want to cause as much trouble without having to start from scratch—buidling their own malicious creations and infrastructure.

That is the story of phishing-as-a-service (PhaaS) offering FlowerStorm as well. Weeks after cybersecurity experts disrupted Rockstar2FA's operations, Sophos noticed an uptick in the use of similar PhaaS portals believed to be part of FlowerStorm. The researchers identified 190 FlowerStorm indicators of compromise (IoCs) comprising 183 domains and seven IP addresses.

The WhoisXML API research team scoured the DNS for more artifacts possibly connected to the FlowerStorm infrastructure and uncovered:

- 192 email-connected domains
- Three additional IP addresses
- 100 IP-connected domains
- 1,053 string-connected domains

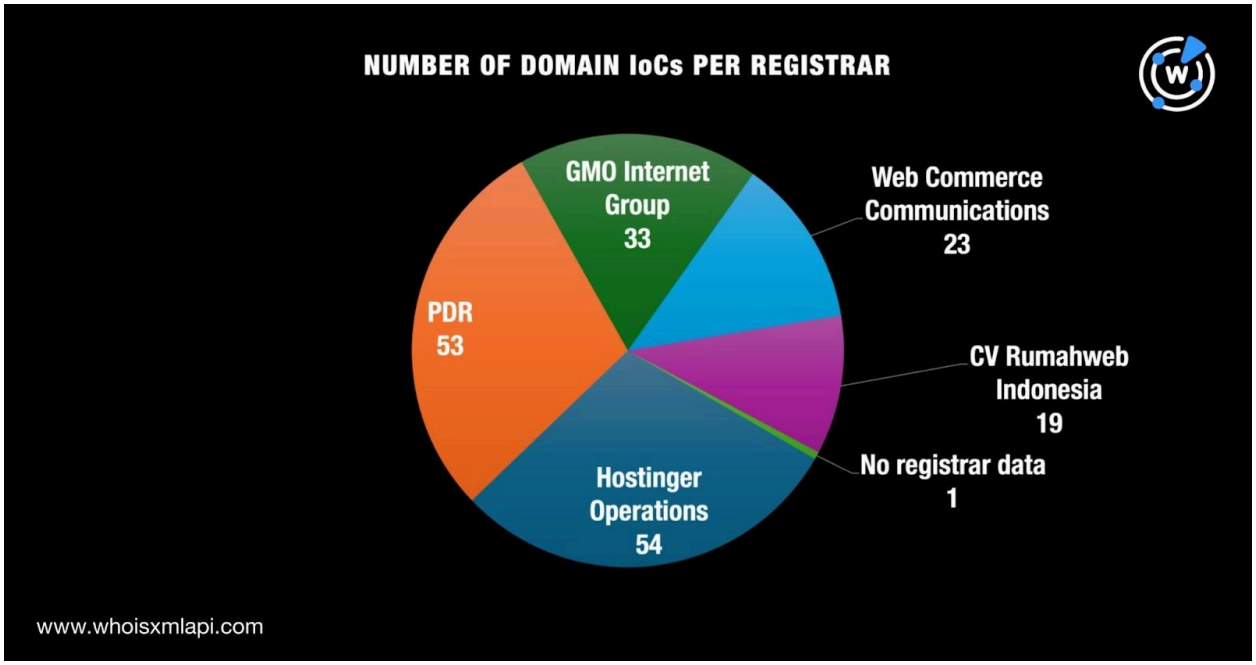
More on the FlowerStorm IoCs

As is our usual first step to expand existing IoC lists, we looked more closely at the 183 domains tagged as IoCs.

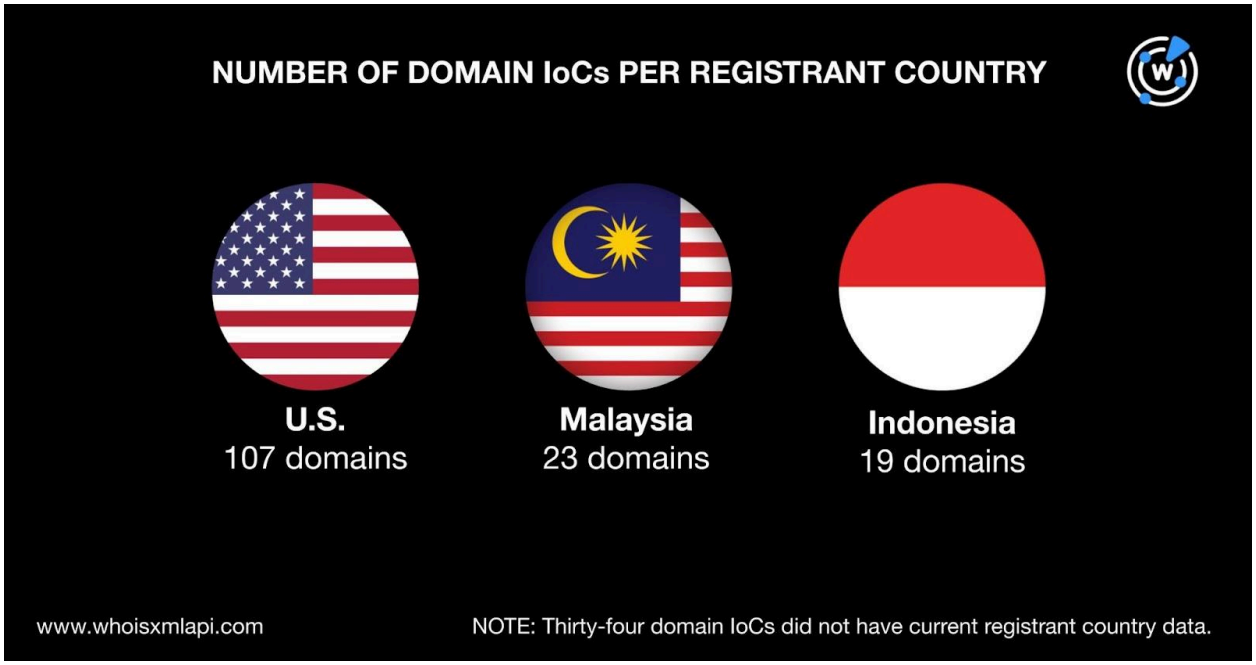
A Bulk WHOIS API query for the 183 domains tagged as IoCs revealed that:

- Only 182 had registrar data in their current WHOIS records. Hostinger Operations led the pack with 54 domain IoCs. PDR followed closely with 53 domains. GMO Internet

Group came in third place with 33 IoCs. Web Commerce Communications and CV Rumahweb Indonesia completed the list with 23 and 19 domain IoCs, respectively.



- While 182 domain IoCs were created in 2024, one was created way back in 2013.
- A majority of the domains, 107 to be exact, were registered in the U.S. A total of 23 IoCs were registered in Malaysia, while 19 were registered in Indonesia. Meanwhile, 34 domain IoCs did not have registrant country information in their current WHOIS records.

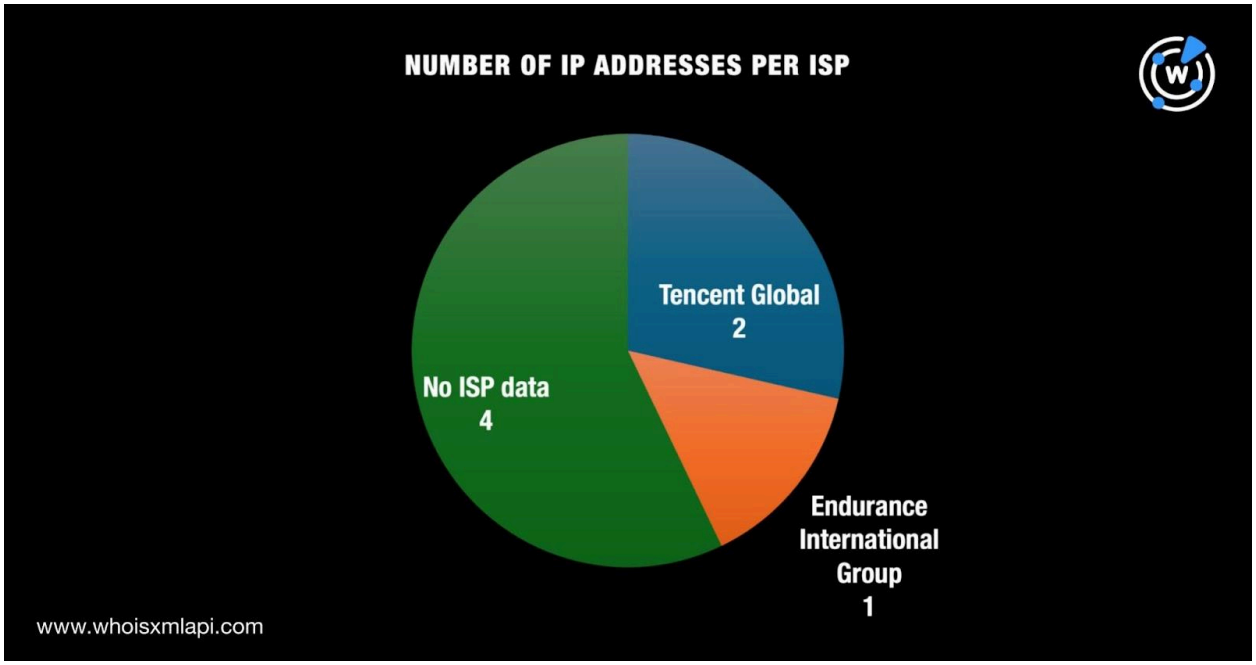


Next, we queried the 183 domains tagged as IoCs on DNS Chronicle API and found that 181 had 645 IP resolutions to date. Take a look at five other examples below.

DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
database-server[.]com	45	6 October 2019
1069083060[.]site	8	14 June 2024
5043056047[.]cloud	7	9 July 2024
1616117488[.]site	6	11 June 2024
1960373846[.]cloud	5	2 July 2024

We then took a closer look at the seven IP addresses tagged as IoCs through a Bulk IP Geolocation Lookup query, which showed that:

- Only four had geolocation countries in their records—two IP address IoCs each originated from Japan and the U.S.
- Only three had ISPs—two IP addresses were administered by Tencent Global and one by Endurance International Group.



A query on DNS Chronicle API for the seven IP addresses tagged as IoCs revealed that four had 2,019 domain resolutions over time. The IP address IoC 69[.]49[.]230[.]198 recorded the first domain resolution on 7 January 2022. Here are two other examples.

IP ADDRESS IoC	NUMBER OF DOMAIN RESOLUTIONS	FIRST DOMAIN RESOLUTION DATE
162[.]241[.]71[.]126	1,000	14 December 2022
43[.]153[.]176[.]84	19	7 September 2023

FlowerStorm DNS Investigation Findings

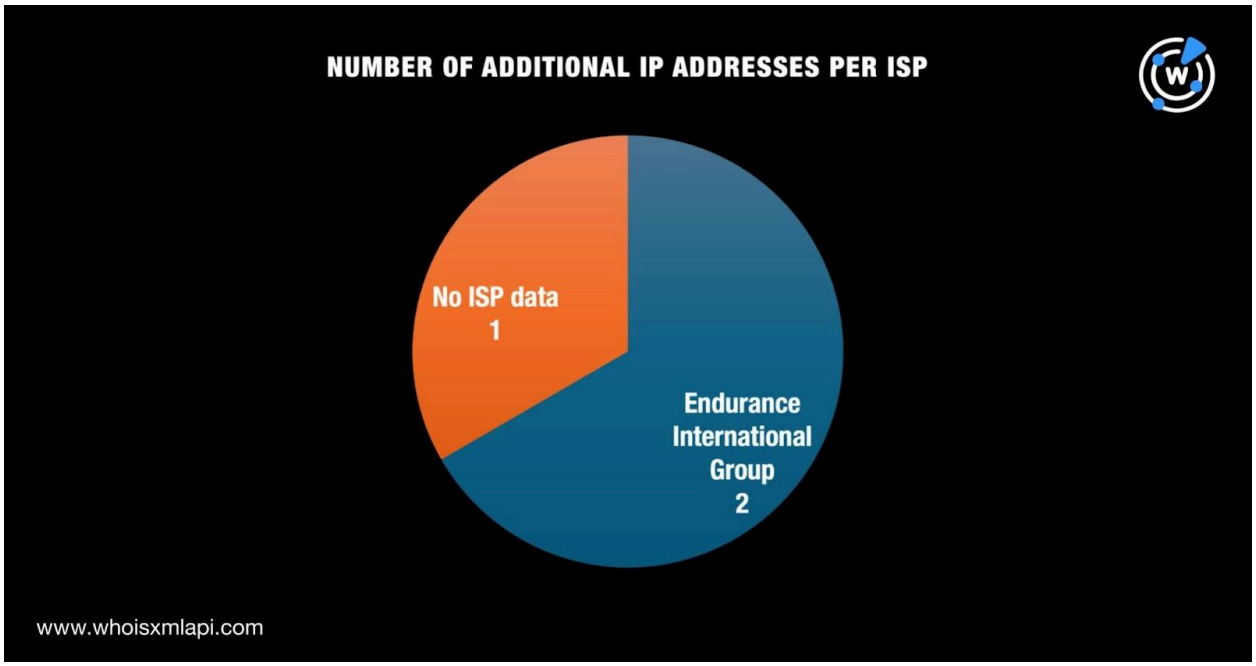
To kick off our search for connected artifacts, we queried the 183 domains tagged as IoCs on WHOIS History API and found that 34 had 15 email addresses in their historical WHOIS records after duplicates were filtered out. Upon closer examination, three of the addresses were public email addresses.

A Reverse WHOIS API query for the three public email addresses showed that two appeared in the current WHOIS records of 192 email-connected domains after duplicates and those already identified as IoCs were filtered out.

Next, we queried the 183 domains tagged as IoCs on DNS Lookup API, which revealed that 38 actively resolved to three IP addresses that have not yet been named as IoCs.

A Bulk IP Geolocation Lookup query for the three additional IP addresses showed that:

- They were all geolocated in the U.S.
- Only two had ISP information and they were administered by Endurance International Group.



Now, we had 10 IP addresses—seven identified as IoCs and three additional from the DNS Lookup API query—to work with for the next step.

A Reverse IP API query for the 10 IP addresses revealed that two could be dedicated hosts. Together, they hosted 100 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

To complete our DNS deep dive, we used Domains & Subdomains Discovery to uncover domains that started with the same text strings found among the 183 domains tagged as IoCs. We found that only these 70 strings were present in other domains:

- 1001635381.
- 1183502499.
- 1270872185.
- 1548899511.
- 1557129175.
- 1620798101.
- 1699745252.
- 1822912119.
- 2113850516.
- 379646778.

- 5005296674.
- 5013230888.
- 5036511802.
- 5043056047.
- 5145178238.
- 5200447943.
- 5261427917.
- 5332779822.
- 5348755448.
- 5460020305.
- 5511861877.
- 5552899895.
- 5569611731.
- 5676123293.
- 5686077371.
- 5696938214.
- 5711491921.
- 5712759205.
- 5748851318.
- 5788485503.
- 5803251012.
- 5864871966.
- 5900172885.
- 5923881203.
- 5933749687.
- 5980245431.
- 6034123867.
- 6063819294.
- 6089251830.
- 6110368953.
- 6113229448.
- 6146851516.
- 6173798458.
- 6268939629.
- 6394563624.
- 6452146665.
- 6471928182.
- 6578617773.
- 6691869997.
- 6721918489.
- 6723980055.
- 6767743674.
- 6785433762.
- 6798247249.
- 6871778911.
- 6975034634.
- 7039858554.
- 7073547716.
- 7100962795.
- 7111612845.
- 7121654589.
- 7184432502.
- 7411669836.
- 7445995473.
- 7524604902.
- 7546805667.
- 8019800353.
- appinvoices.
- database-server.
- my.

All in all, we discovered 1,053 string-connected domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

—

Our latest DNS foray to find otherwise-hidden connections to FlowerStorm via an IoC list expansion led to the discovery of 1,348 artifacts comprising 192 email-connected domains, three additional IP addresses, 100 IP-connected domains, and 1,053 string-connected domains.

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

- appbizconstruction[.]com
- appcloudfederal[.]com
- appconstructionhub[.]com
- bizappdocs[.]com
- bizidentityapp[.]com
- boudouresque[.]fr
- cloudappbuilders[.]com
- cloudbasedbusinessapp[.]com
- cloudconstructionhub[.]com
- doc-invoice[.]com
- doccloudhosting[.]com
- docfederal[.]com
- ekvoetbal[.]info
- fblawyeroutlook[.]com
- fbusinesslawyer[.]com
- feddocsolutions[.]com
- hostcloudbusiness[.]com
- hostconstructionapp[.]com
- hostedbusinessapp[.]com
- identitybusinessapp[.]com
- identitycraftsman[.]com
- identityinbuilding[.]com
- lawapplic[.]com
- lawbusinessapp[.]com
- lawbusinessdocs[.]com
- microsoft-tech-app[.]com
- microsoftappdocs[.]com
- microsoftapphub[.]com
- outlookbusinesslaw[.]com
- outlookbusinesslawyer[.]com
- outlookfederallaw[.]com
- probusinessapps[.]com
- profhost[.]us
- smartconstructionhost[.]com
- tecdocproject[.]com
- techappdocuments[.]com
- techdocsapp[.]com
- uscourtadvice[.]com
- uscourtconstructionlaw[.]com
- uscourtlawservices[.]com

Sample Additional IP Addresses

- 162[.]241[.]149[.]91
- 162[.]241[.]71[.]126

Sample IP-Connected Domains

- cpanel[.]bureaubusinesslawyer[.]com
- cpanel[.]businesslawoutlook[.]com
- cpanel[.]businesslawyeroutlook[.]com
- cpanel[.]constructionlawcourts[.]com
- cpanel[.]constructionlawus[.]com
- cpanel[.]courtdocumentsupport[.]com
- cpanel[.]federalattorneyoutlook[.]com
- cpanel[.]federalbusinessdoc[.]com
- cpanel[.]federalbusinesslawyer[.]com
- cpanel[.]federallegalexpert[.]com
- ftp[.]bureaubusinesslawyer[.]com
- ftp[.]businesslawoutlook[.]com
- ftp[.]businesslawyeroutlook[.]com
- ftp[.]constructionlawcourts[.]com
- ftp[.]constructionlawus[.]com
- ftp[.]courtdocumentsupport[.]com
- ftp[.]federalattorneyoutlook[.]com
- ftp[.]federalbusinessdoc[.]com
- ftp[.]federalbusinesslawyer[.]com
- ftp[.]federallegalexpert[.]com
- mail[.]bureaubusinesslawyer[.]com
- mail[.]businesslawoutlook[.]com
- mail[.]businesslawyeroutlook[.]com
- mail[.]constructionlawcourts[.]com
- mail[.]constructionlawus[.]com
- mail[.]courtdocumentsupport[.]com
- mail[.]federalattorneyoutlook[.]com
- mail[.]federalbusinessdoc[.]com
- mail[.]federalbusinesslawyer[.]com
- mail[.]federallegalexpert[.]com
- scgx02[.]org
- webdisk[.]bureaubusinesslawyer[.]com
- webdisk[.]businesslawoutlook[.]com
- webdisk[.]businesslawyeroutlook[.]com
- webdisk[.]constructionlawcourts[.]com
- webdisk[.]constructionlawus[.]com
- webdisk[.]courtdocumentsupport[.]com
- webdisk[.]federalattorneyoutlook[.]com
- webdisk[.]federalbusinessdoc[.]com
- webdisk[.]federalbusinesslawyer[.]com
- webdisk[.]federallegalexpert[.]com

Sample String-Connected Domains

- 1001635381[.]my[.]id
- 1183502499[.]my[.]id
- 1183502499[.]space
- 1270872185[.]my[.]id
- 1548899511[.]my[.]id
- 1557129175[.]my[.]id
- 1557129175[.]space
- 1620798101[.]my[.]id
- 1699745252[.]my[.]id
- 1822912119[.]my[.]id
- 2113850516[.]my[.]id
- 379646778[.]my[.]id

- 5005296674[.]my[.]id
- 5013230888[.]my[.]id
- 5036511802[.]my[.]id
- 5043056047[.]my[.]id
- 5145178238[.]my[.]id
- 5200447943[.]cloud
- 5200447943[.]fun
- 5200447943[.]my[.]id
- 5261427917[.]my[.]id
- 5332779822[.]my[.]id
- 6034123867[.]my[.]id
- 6063819294[.]my[.]id
- 6089251830[.]my[.]id
- 6110368953[.]my[.]id
- 6113229448[.]my[.]id
- 6113229448[.]online
- 6146851516[.]my[.]id
- 6173798458[.]my[.]id
- 6268939629[.]my[.]id
- 6394563624[.]my[.]id
- 7039858554[.]my[.]id
- 7073547716[.]my[.]id
- 7100962795[.]my[.]id
- 7111612845[.]my[.]id
- 7121654589[.]my[.]id
- 7184432502[.]my[.]id
- 7411669836[.]my[.]id
- 7445995473[.]my[.]id
- 7524604902[.]my[.]id
- 7524604902[.]space
- 8019800353[.]my[.]id
- appinvoices[.]click
- database-server[.]de
- database-server[.]eu
- database-server[.]ml
- database-server[.]red
- my[.]abbott
- my[.]abbvie
- my[.]abogado
- my[.]ac
- my[.]ac[.]cn
- my[.]ac[.]kr
- my[.]ac[.]th
- my[.]ac[.]uk
- my[.]academy
- my[.]accountant