WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A DNS Exploration of Operation Olalampo

Threat Report

Table of Contents

Executive Report

MuddyWater has been in the APT business for some time now. And this time, it set its sights on organizations and individuals primarily across the MENA region, leveraging ongoing geopolitical tensions. Dubbed “Operation Olalampo,” the threat actors deployed new malware variants and used Telegram bots for C&C.

Group-IB published their analysis of the threat, including seven network IoCs comprising four domains and three IP addresses, which we further dove into. Note that we checked if any of the domains were owned by legitimate entities aided by the WhoisXML API MCP Server. None of them were so we did not exclude any of them in our investigation.

Our DNS exploration into the IoCs led to these findings:

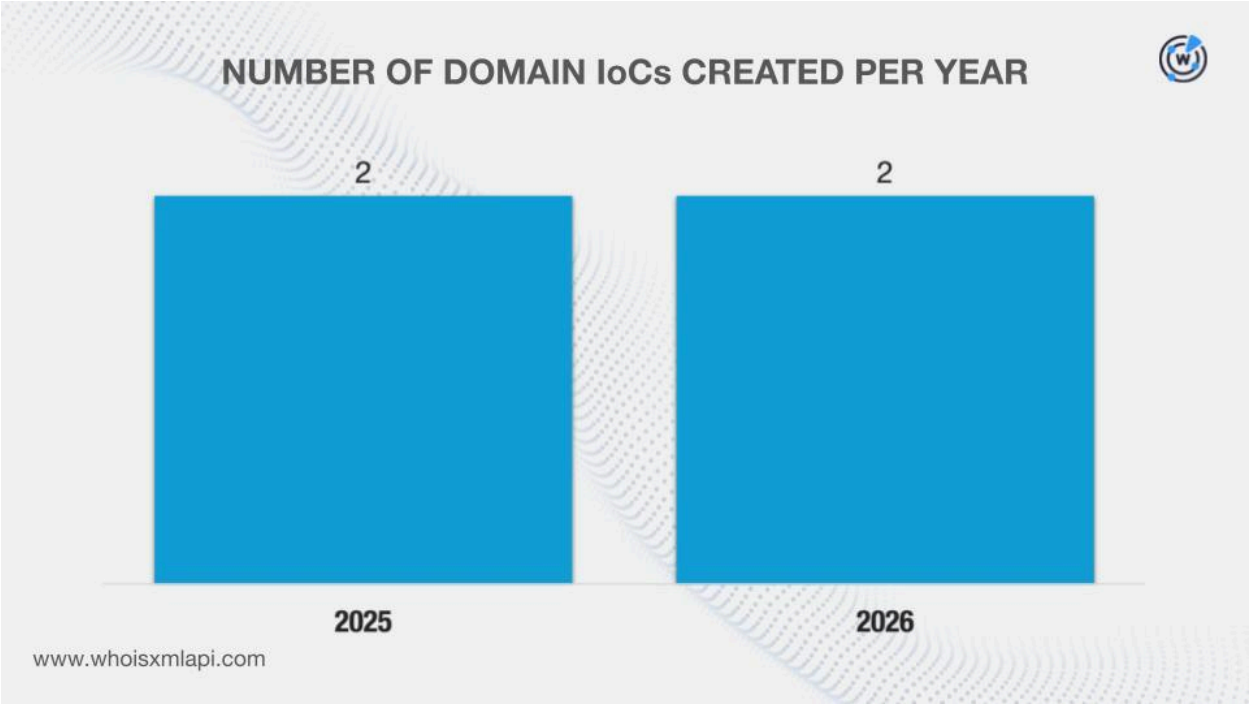
- 10 unique potential victim IP addresses communicated with one of the IP addresses identified as IoCs
- 2,530 email-connected domains
- Six additional IP addresses, all of which turned out to be malicious
- 55 string-connected domains

A Deep Dive into the Operation Olalampo Domain IoCs

We began our investigation by looking more closely at the four domains identified as IoCs.

We queried them on WHOIS API and found out that:

- They were created between 28 October 2025 and 2 February 2026, making them all relatively new when they were used for the campaign.



- They were all administered by Namecheap.
- They were all registered in Iceland.

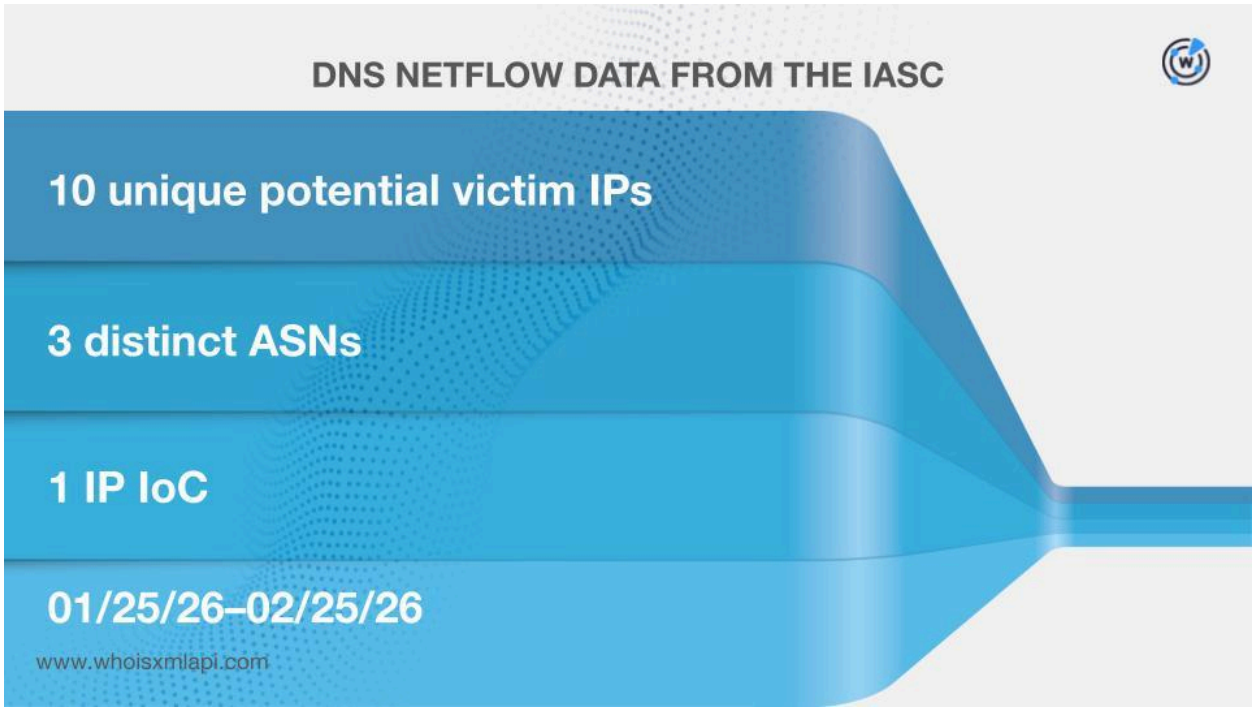
DNS Chronicle API queries for the domains revealed that three recorded 27 historical domain-to-IP resolutions over time, consistent with their ages. Take a look at more information below.

DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
jerusalemsolutions[.]com	16	10/29/25–02/23/26
miniquest[.]org	9	01/29/26–02/11/26
codefusiontech[.]org	2	02/03/26–02/07/26

An Investigation of the Operation Olalampo IP IoCs

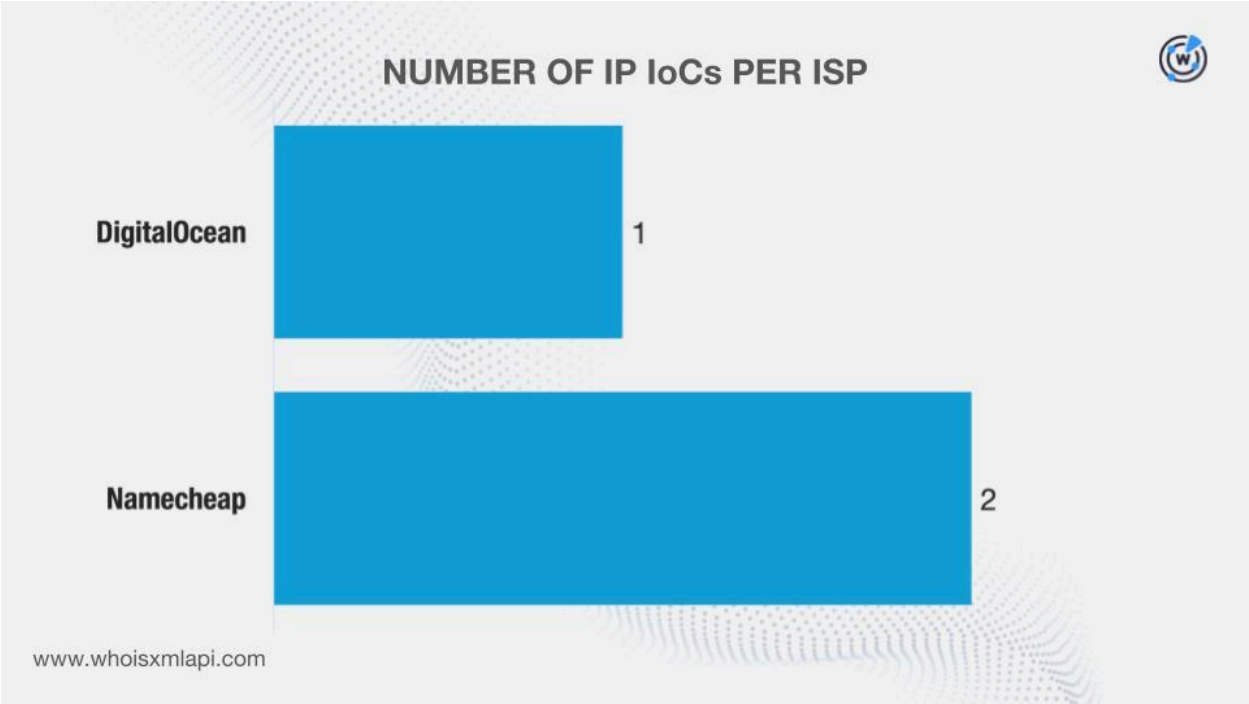
We then sought for more information about the three IP addresses identified as IoCs.

First, sample network data from the IASC showed that 10 unique IP addresses possibly owned by victims under three distinct ASNs communicated with one of the IP addresses tagged as IoCs between 25 January and 25 February 2026.



We queried them on Bulk IP Geolocation Lookup and discovered that:

- They were all geolocated in the U.S., a far cry from the registrant country.
- They were administered by two ISPs.



DNS Chronicle API queries for the IP addresses revealed that two recorded 1,017 historical IP-to-domain resolutions over time. Here are more details.

IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	DATES SEEN
162[.]0[.]230[.]185	1,000	09/05/20–07/24/21
209[.]74[.]87[.]100	17	03/10/25–05/10/25

A DNS Sweep for New Operation Olalampo Artifacts

We then used a variety of solutions to gather as many new potentially connected artifacts as possible.

First, we queried the four domains identified as IoCs on WHOIS History API. We found out that all of them had seven unique email addresses in their historical WHOIS records. Further scrutiny revealed that one was a public email address.

A Reverse WHOIS API query for the sole public email address allowed us to collate 2,530 unique email-connected domains after those already tagged as IoCs were filtered out.

Next, we queried the domains named as IoCs on DNS Lookup API and discovered that three resolved to six unique additional IP addresses (i.e., not on the IoC list).

Threat Intelligence API queries for the additional IP addresses showed that all of them have already been weaponized for various attacks. Take a look at more details below.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATES SEEN
104[.]21[.]63[.]16	Phishing Malware distribution Generic threat	01/02/24–03/02/26 10/25/23–03/02/26 04/09/23–03/01/26
172[.]67[.]142[.]102	Malware distribution Phishing Generic threat	10/25/23–03/02/26 01/02/24–03/02/26 04/09/23–03/01/26
104[.]21[.]14[.]92	Malware distribution Phishing	06/02/23–02/27/26 07/22/23–02/24/26

We also queried the additional IP addresses on Bulk IP Geolocation Lookup and found out that:

- They were all geolocated in the U.S. akin to those dubbed as IoCs.
- They were all administered by Cloudflare, which was not on the list of ISPs of the IoCs.

We now had nine IP addresses for further analysis. Reverse IP API queries for them revealed that none could be dedicated hosts, thus halting our search for IP-connected domains.

Next, we extracted unique text strings from the domains classified as IoCs. We then scoured the DNS for other domains that started with them using Domains & Subdomains Discovery. We uncovered 55 unique string-connected domains after those already categorized as IoCs and the email-connected domains were filtered out. They started with these strings:

- codefusiontech.
- jerusalemsolutions.
- miniquest.
- promoverse.

Note that these string-connected domains only serve to reflect the overall popularity of the strings extracted from the IoCs. As such, determining their legitimacy may require further investigation.

A Summary of Our Operation Olalampo Analysis

Our DNS deep dive into the Operation Olalampo network IoCs revealed that 10 unique IP addresses that could belong to potential victims communicated with one IP address identified as an IoC.

We also unearthed 2,591 new artifacts comprising 2,530 email-connected domains, six additional IP addresses, and 55 string-connected domains. It is worth noting that six of these artifacts have already been weaponized for various attacks.

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

- 2016paralympics[.]website
- 2020paralympics[.]co
- 2020paralympics[.]info
- abuja[.]website
- abusesurvivors[.]club
- abuyers[.]guide
- babeorgy[.]com
- babysitters[.]website
- badlands[.]place
- cagliari[.]place
- cagliari[.]website
- cajun[.]place
- dados[.]juegos
- dallasflight[.]net
- dalycity[.]place
- earbionics[.]com
- eastasia[.]place
- easternafrica[.]place
- faden[.]rocks
- faden[.]website
- fadenquartz[.]rocks
- gaborone[.]website
- galapagos[.]website
- galapagosecotours[.]com
- hades[.]website
- hagadobleclicenla[.]link
- hagiasophia[.]place
- iahflight[.]com
- iahflights[.]com
- iamahippie[.]clothing
- jadeite[.]rocks
- jamesbrown[.]link
- jamesmcneillwhistler[.]link
- kandinsky[.]link
- kansascity[.]place
- kant[.]rocks
- labusquedadela[.]link
- laincorporaciondela[.]link
- lakebaikal[.]place
- machuphotographchu[.]guide
- machuphotographchu[.]ninja
- machupicchu[.]academy
- nante[.]link
- napa[.]place
- nassau[.]place
- oceaniaecotours[.]com
- oceanus[.]website
- odessa[.]place
- pachelbel[.]link
- pacificocean[.]link
- padparaschasapphire[.]website
- qiuck[.]auction
- quangnin[.]rocks
- quartz[.]website
- rachmaninov[.]link
- rainforest[.]website
- rainforests[.]website
- sacramento[.]place
- safaris[.]place
- safesexyes[.]com
- taaffeite[.]rocks
- taaffeite[.]website
- taekwondo[.]place
- uccello[.]rocks
- ucello[.]rocks
- uhuru[.]place
- vaduz[.]website
- valletta[.]website
- vanadanite[.]auction
- wakeboarders[.]club
- wanderingto[.]link
- warhol[.]link
- yamoussoukro[.]website
- yangon[.]place

- yaounde[.]website
- zagreb[.]place
- zazdomains[.]com
- zazzy[.]xyz

Sample Additional IP Addresses

- 104[.]21[.]63[.]16
- 172[.]67[.]142[.]102
- 104[.]21[.]14[.]92

Sample String-Connected Domains

- codefusiontech[.]com
- codefusiontech[.]my
- codefusiontech[.]net
- jerusalemsolutions[.]guru
- jerusalemsolutions[.]org
- jerusalemsolutions[.]photography
- miniquest[.]app
- miniquest[.]click
- miniquest[.]cn
- promoverse[.]app
- promoverse[.]at
- promoverse[.]biz