A DNS Investigation into Mamba, the Latest AitM Phishing Player

Table of Contents

Executive Report

Phishing has been around for years, yet it still proves to be a major online threat. To continue profiting, cybercriminals must continuously adapt their techniques.

Phishing malware Mamba 2FA, for instance, has been armed with adversary-in-the-middle (AitM) capabilities. This new feature allowed the malware to bypass multifactor authentication (MFA) measures like one-time passwords (OTPs) and app notifications.

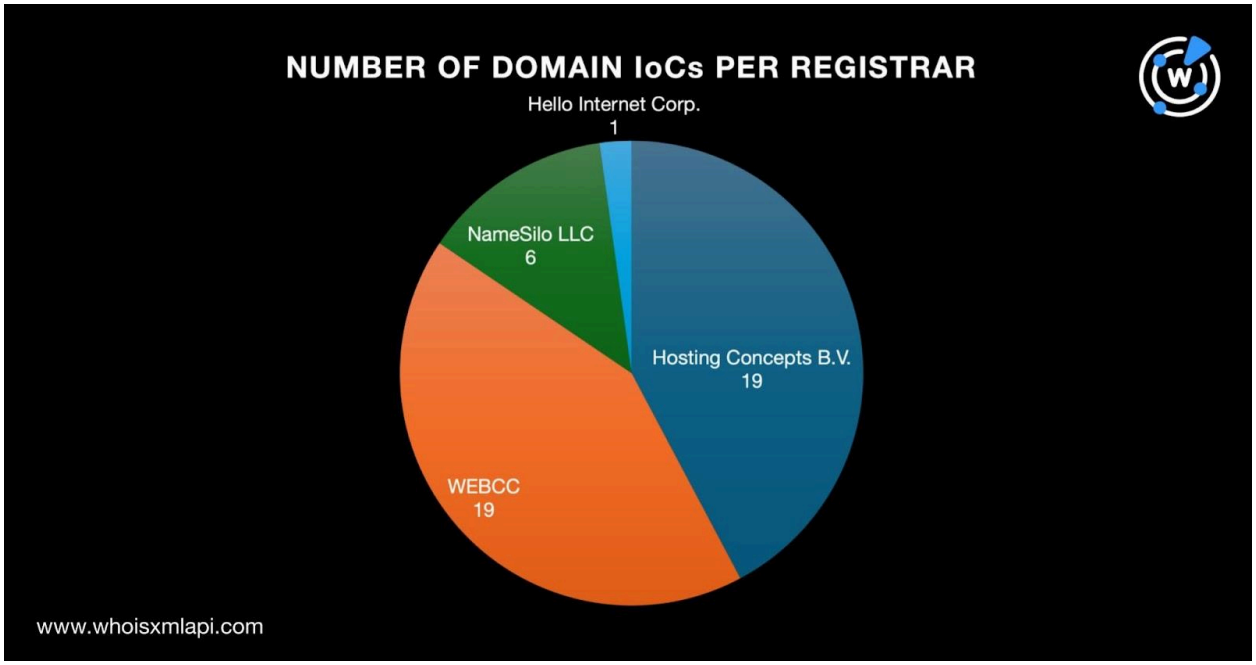
The Sekoia Threat Detection and Research (TDR) Team analyzed Mamba 2FA and identified 58 indicators of compromise (IoCs) comprising 45 domain names and 13 IP addresses. Our research team expanded the IoC list and uncovered additional threat artifacts, including:

- 346 registrant-connected domains, two of which turned out to be malicious
- 65 additional IP addresses, 51 of which turned out to be associated with various threats
- One IP-connected domain
- Six string-connected domains

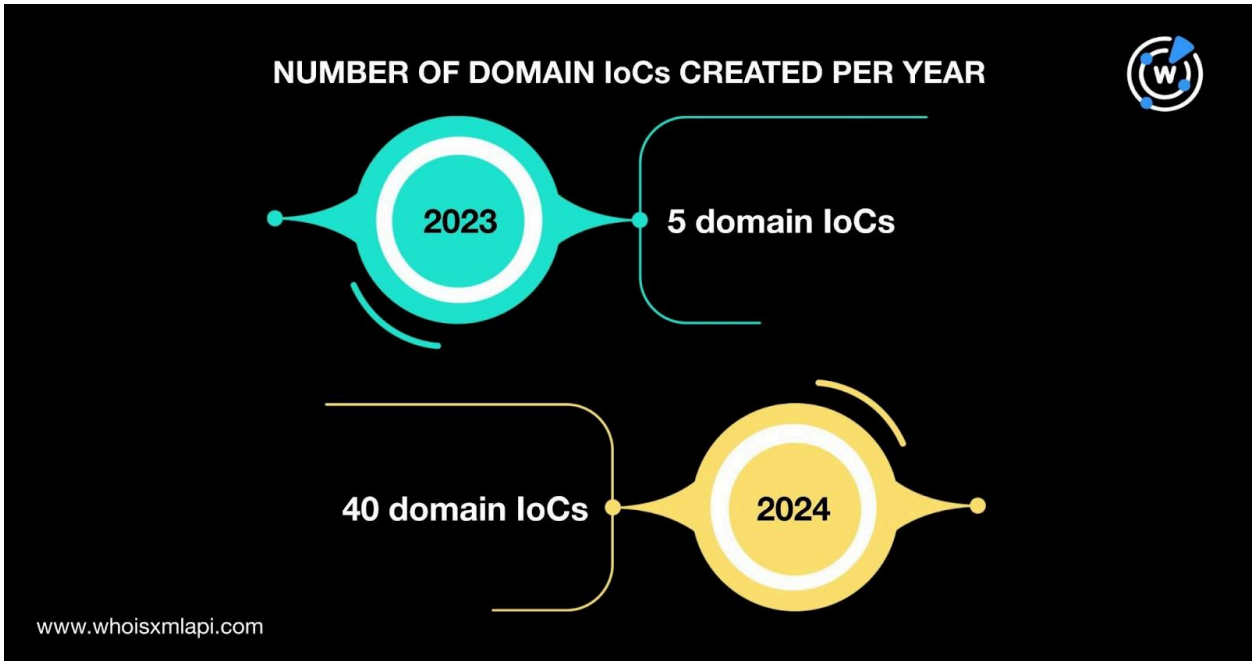
Under the Mamba 2FA Hood

As is our usual first step, we looked into the IoCs first beginning with a bulk WHOIS lookup for the 45 domain names. That revealed the following:

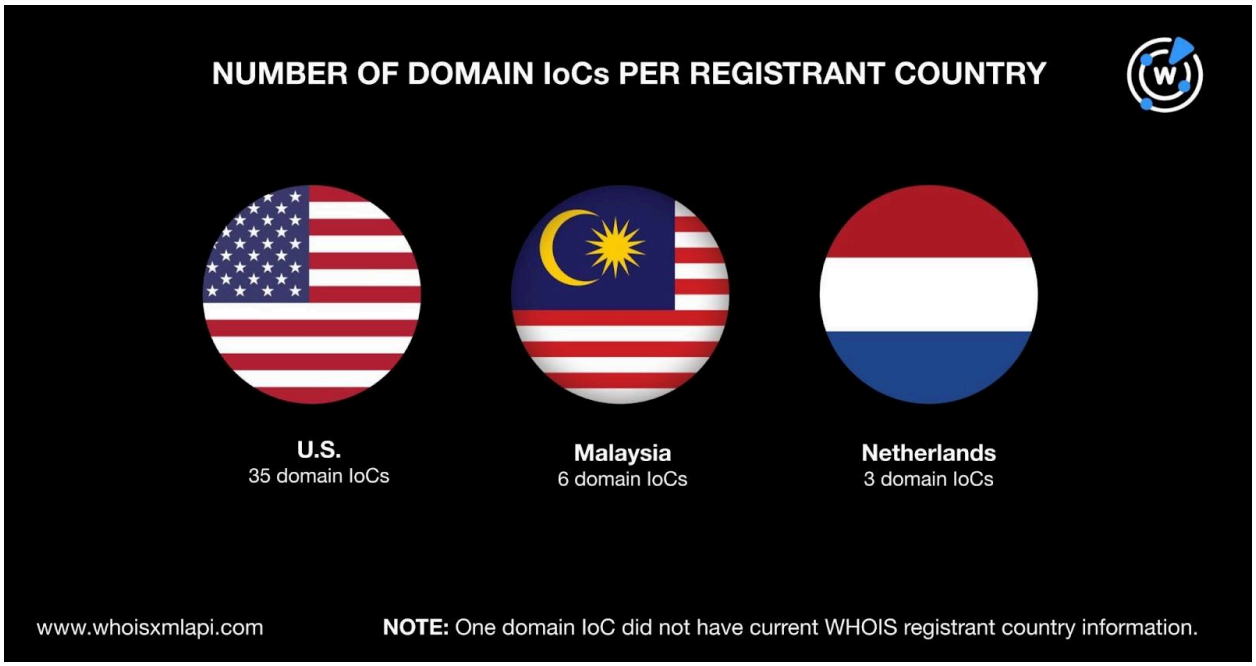
- The domains were distributed among four registrars led by Hosting Concepts B.V. and WEBCC, which tied in first place with 19 domain IoCs each. NameSilo LLC came in second, accounting for six domain IoCs. Hello Internet Corp. with one domain IoC rounded out the list.



- A majority of the domain IoCs, 40 to be exact, were created in 2024 while the remaining five were created in 2023.



- They were spread across three different countries led by the U.S. with 35 domain IoCs. Six domain IoCs were registered in Malaysia while three in the Netherlands. One domain IoC didn't have a registrant country in its current WHOIS record.



- Twenty-seven domain IoCs had public registrant information in their current WHOIS records. Specifically, 13 each had registrant email addresses and names, and all 27 had registrant organizations.

A bulk IP geolocation lookup for the 13 IP address IoCs, meanwhile, showed that all were geolocated in the U.S. but didn't have ISP information in their A records.

Mamba 2FA IoC List Expansion Results

We jump-started our search for additional Mamba 2FA artifacts with Reverse WHOIS Search queries for the registrant email address, name, and organization we obtained from our bulk WHOIS lookup earlier. Using the parameters **Advanced**, **Historic**, and **Exact match**, we uncovered 346 registrant-connected domains after filtering out duplicates and the IoCs.

Threat Intelligence API queries for the 346 registrant-connected domains revealed that two of them were associated with threats. The domain egensession[.]com, for instance, was tagged as an IoC for phishing and generic threats.

After that, we ran the 45 domain IoCs on WHOIS History API and obtained 23 email addresses from their historical WHOIS records. Only two, however, were public.

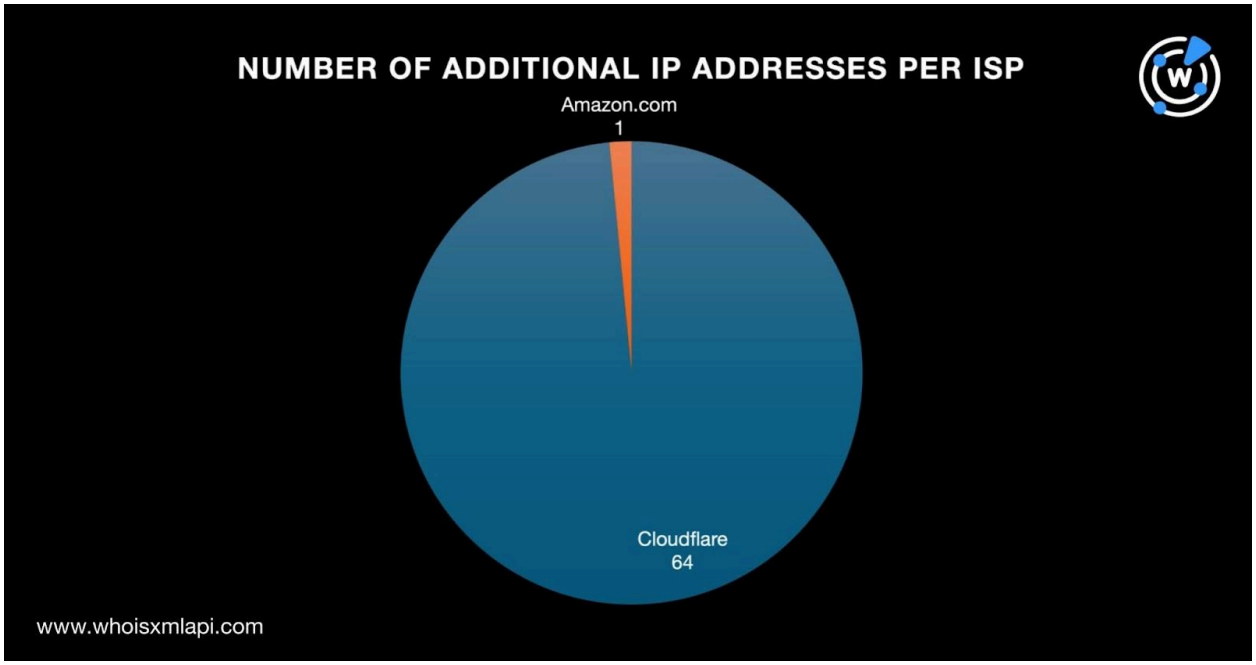
Of the public email addresses, only one had connected domains based on the results of our Reverse WHOIS API queries—the same email address that showed up in some of the domain IoCs' WHOIS records earlier. As such, none of the email-connected domains remained when we removed duplicates, the IoCs, and the registrant-connected domains from our list.

Next, we performed DNS lookups for the 45 domain IoCs and found 65 IP addresses after filtering out duplicates and the IoCs. Based on Threat Intelligence API queries for these additional IP addresses, 51 have already figured in various malicious campaigns. Take a look at five examples below.

ADDITIONAL IP ADDRESS	ASSOCIATED THREAT TYPES
104[.]21[.]17[.]140	Phishing
104[.]21[.]19[.]3	Attack Malware Phishing
104[.]21[.]26[.]155	Attack Generic Malware Phishing
104[.]21[.]32[.]230	Generic Phishing
15[.]197[.]130[.]221	Attack Command and control (C&C) Generic Malware Phishing Suspicious

In our hunt for more information about the 65 additional IP addresses, we performed a bulk IP geolocation lookup and found that:

- They were all geolocated in the U.S.
- All but one were administered by Cloudflare. The sole remaining email address was under Amazon.com.



We then subjected the 78 IP addresses (i.e., 13 tagged as IoCs and 65 additional) to reverse IP lookups. Only one could be a dedicated host and had one IP-connected domain—wm666888[.]com.

As the final step, we performed Domains & Subdomains Discovery searches to look for domains that resembled the 45 domain IoCs using the **Domains only** and **Starts with** parameters for the following 44 strings (**tenetur.** appeared in two domain IoCs):

- 10decadesmen.
- 10trioneyue8ss.
- 11beamgools.
- 11cyclesforest.
- 1messisnfarm.
- 2moniunesson.
- 3alphabetjay.
- 4sessionmoon.
- 5poleanalhy.
- 6treesmangle.
- 7motionmansa.
- 88mansession.
- 8boomandool.
- 9cantronnfit.
- ccokies1cakes.
- ccokies2mangoes.
- ccokies3tomatoes.
- copefood.
- copelustration.
- drensyoons1sedt.
- fivemanchool.
- fiveradio-newbam.
- fourmanchurch.
- fourthmanservice.
- grastoonm3vides.
- hypexfinancial.
- m1tis-apicookies.
- m2fes-apicookies.

- m3mas-apicookies.
- nine9manforest.
- onemanforest.
- planchereserver.
- sandoom2notnt.
- seven-oranges.
- sevenmanjungle.
- sithchibb.
- sixmanteams.
- tenetur.
- thirdmandomavis.
- threemanshop.
- twomancake.
- voltampereactive.
- winss0conect.
- winstnet80nss.

We also limited our queries to domains registered from 1 January 2023 onward. We found that only four of the strings (i.e., **copefood.**, **tenetur.**, **winss0conect.**, and **winstnet80nss.**) appeared in other domains. That said, we uncovered six string-connected domains.

IoC-to-Artifact Comparison

Of the 353 connected domains (346 registrant-connected, one IP-connected, and six string-connected domains) we uncovered, 163 had current WHOIS record details. Twenty-four of the 163 connected domains had commonalities with the 45 domain IoCs. Specifically, 11 connected domains shared the registrant email address, 11 shared the registrant name, and 22 shared the registrant organization of the IoCs. These findings further cemented the ties between Mamba 2FA and the 24 connected domains.

—

Our DNS deep dive into the 58 Mamba 2FA IoCs allowed us to identify 418 potentially connected artifacts comprising 346 registrant-connected domains, 65 additional IP addresses, one IP-connected domain, and six string-connected domains. A total of 53 of these artifacts turned out to be malicious.

Further investigation also revealed that 24 of the 353 connected domains we discovered could indeed be part of the Mamba 2FA infrastructure.

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 Registrant-Connected Domains

- 46336bd69jss529ang649snd730md bf693ns[.]com
- 6sessions[.]com
- acsport[.]agency
- acsport[.]cz
- acsport[.]sk
- alokirala[.]com
- altaneacorre[.]com
- altaneacorre[.]it
- altaneacorre[.]run
- antalyamaratonemlak[.]com
- apartamentoserika[.]com
- assetledgertrust[.]com
- atitlanmarathon[.]com
- atlakazan[.]com
- aventurasnomundo[.]com
- bulls-bicykle[.]sk
- celenkarna[.]cz
- centroamericacorre[.]com
- coffeereuniongmc[.]com
- corridadamulher[.]com
- corrinrosa[.]com
- corrinrosa[.]run
- cursomaratonamilitar[.]com
- decolardocorredor[.]com
- dehaar[.]com
- diecimiladelmontello[.]com
- diecimiladelmontello[.]it
- diecimiladelmontello[.]run
- dinalevacic[.]com
- ebikekralovahola[.]com
- ebikekralovahola[.]sk
- eeroolinko438364836383[.]com
- egensession[.]com
- energetika-dumanic[.]com
- erawpajnew[.]net
- eshel[.]at
- eshelmest[.]com
- esportesnomundo[.]com
- euaprendoemcasa[.]live
- eylisbon[.]com
- feelgoodcoffeeco[.]com
- fixingmindsets[.]com
- foodseseanalplentus[.]com
- fredericolourenco[.]com
- fundacionmapoma[.]com
- gengensharedpdf[.]com
- gle-support[.]com
- gtsport[.]it
- gunwimarathon[.]com
- has-nak[.]com

Sample Additional IP Addresses

- 104[.]21[.]0[.]209
- 104[.]21[.]12[.]42
- 104[.]21[.]17[.]140
- 104[.]21[.]19[.]3
- 104[.]21[.]2[.]93
- 104[.]21[.]26[.]155
- 104[.]21[.]30[.]47
- 104[.]21[.]31[.]46
- 104[.]21[.]32[.]230
- 104[.]21[.]33[.]162
- 104[.]21[.]37[.]208
- 104[.]21[.]4[.]164
- 104[.]21[.]40[.]87
- 104[.]21[.]44[.]178

- 104[.]21[.]47[.]240
- 104[.]21[.]49[.]94
- 104[.]21[.]53[.]225
- 104[.]21[.]54[.]127
- 104[.]21[.]56[.]195
- 104[.]21[.]56[.]201
- 104[.]21[.]56[.]47
- 104[.]21[.]57[.]169
- 104[.]21[.]64[.]195
- 104[.]21[.]71[.]111
- 104[.]21[.]81[.]146
- 104[.]21[.]82[.]195
- 104[.]21[.]82[.]30
- 104[.]21[.]82[.]59
- 104[.]21[.]82[.]98
- 104[.]21[.]84[.]200

Sample String-Connected Domains

- copefood[.]com
- copefood[.]it
- tenetur[.]buzz