A Peek at the PikaBot Infrastructure

Table of Contents

Executive Report

It is not uncommon these days for threat actors to use malicious search ads to distribute malware. To do that, though, they would need to know how to bypass Google's security measures by setting up decoy infrastructures.

PikaBot is one such malware that started gaining renown in early 2023. Malwarebytes Labs researchers conducted an in-depth analysis of the threat and published 11 indicators of compromise (IoCs)—two domains and nine IP addresses—in the process.

In a bid to make the Internet safer and more transparent, the WhoisXML API research team expanded the list of IoCs and found hundreds of potentially connected artifacts, namely:

- 112 email-connected domains
- Three additional IP addresses to which some domain IoCs resolved, two of which turned out to be malicious
- 210 IP-connected domains, three of which have been tagged as malicious
- 14 string-connected domains

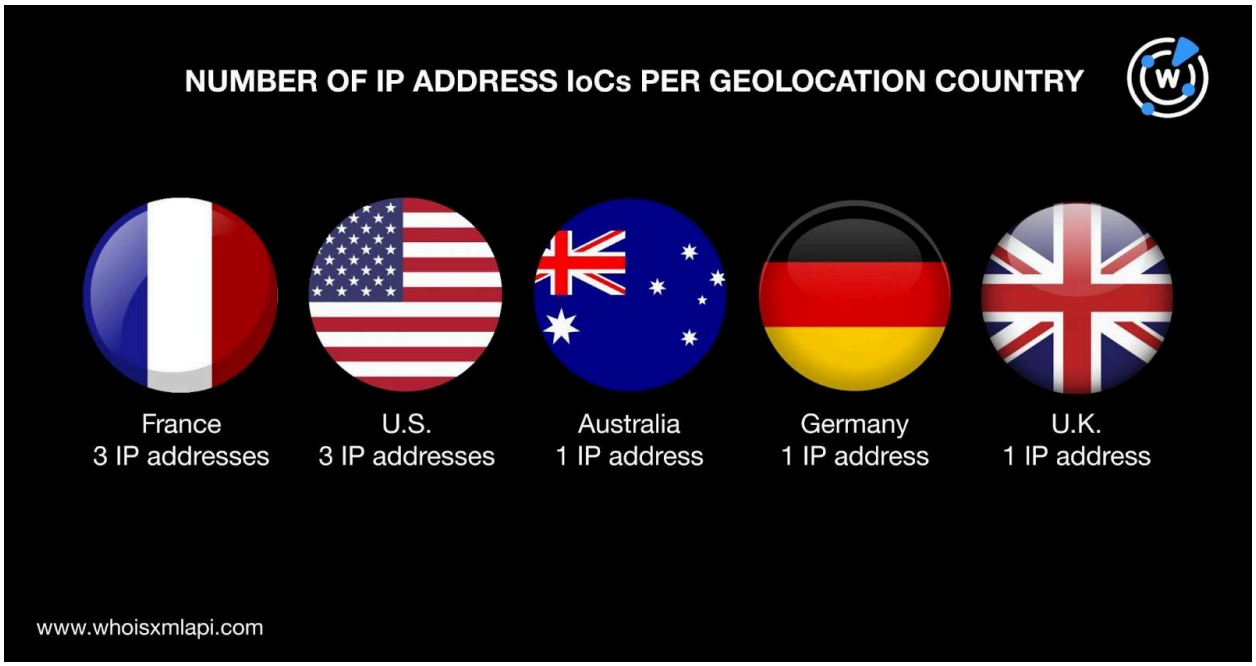
A Quick Look at the PikaBot IoCs

As a first step, we looked at the two domains identified as IoCs via WHOIS lookups, which revealed that:

- They were administered by different registrars—cxtensones[.]top by NiceNIC International Group Co. Ltd. and ovmv[.]net by Hosting Concepts B.V.
- Both domains were created in December 2023, making them newly registered when they were used for attacks.
- The IoC cxtensones[.]top indicated the U.S. as its registrant country while ovmv[.]net was supposedly registered in the Netherlands.

A bulk IP geolocation lookup, meanwhile, for the nine IP addresses tagged as IoCs showed that:

- Three IP addresses each appeared to be geolocated in France and the U.S. One IoC each pointed to Australia, Germany, and the U.K. as their origins.



- They were split between two Internet service providers (ISPs)—six for OVH and three for Akamai Technologies, Inc.

Threat Intelligence API searches for the IoCs also revealed interesting tidbits as detailed in the table below.

IoC	NUMBER OF ASSOCIATED THREATS	ASSOCIATED THREAT TYPE	DATE FIRST SEEN
139[.]99[.]222[.]29	1	Malware	15 December 2023
172[.]232[.]162[.]198	4	Attack Botnet C2 Malware	14 December 2023
172[.]232[.]164[.]77	4	Attack	13 December 2023

		Botnet C2 Malware	
172[.]232[.]186[.]251	4	Attack Botnet C2 Malware	14 December 2023
54[.]37[.]79[.]82	4	Attack Botnet C2 Malware	15 December 2023
57[.]128[.]108[.]132	4	Attack Botnet C2 Malware	14 December 2023
57[.]128[.]109[.]221	4	Attack Botnet C2 Malware	15 December 2023
57[.]128[.]164[.]11	4	Attack Botnet C2 Malware	14 December 2023
57[.]128[.]83[.]129	4	Attack Botnet C2 Malware	14 December 2023

On the Flip Side of the PikaBot Campaign

To uncover other possibly related PikaBot artifacts, we began by subjecting the two domains identified as IoCs to WHOIS history lookups, which revealed that one of them—ovmv[.]net—had four email addresses in their historical WHOIS records. Three of them were public email addresses.

Reverse WHOIS API queries using two of the three public email addresses as search terms led to the discovery of 112 domains after duplicates and the IoCs were removed, almost all of which were either Chinese-sounding or composed of random number combinations. Examples include:

- 1869666[.]net
- 240690[.]com
- 242302[.]com
- 354374[.]com
- 375324[.]com
- dalianchu[.]com
- didichihuo[.]com
- duolianchu[.]com
- fulianchu[.]com
- hangtianyun[.]com

Next, we performed DNS lookups on the two domains identified as IoCs and found three IP addresses that are not part of the original IoC list.

IP geolocation lookups for the three additional IP addresses revealed that:

- Each one was geolocated in a different country—Brazil, Switzerland, and the U.S.
- Two—104[.]21[.]72[.]66 and 172[.]67[.]176[.]15—were associated with various threats based on the built-in Threat Intelligence API engine. In addition, both IP addresses were flagged for phishing and generic threats from 23 May 2023 to the current date.

We now had 12 IP addresses in total to work with—nine identified as IoCs and the three additional resolutions. Reverse IP lookups showed that three of them could be dedicated hosts. The potentially dedicated IP addresses hosted 210 other domains that were not yet part of the original IoC list nor email-connected.

Threat Intelligence API revealed that three of them—fakty-info[.]com, twinsources[.]shop, and txid-coinbase[.]net—were associated with various threats. Take a look at the details in the table below.

IP-CONNECTED DOMAIN	NUMBER OF ASSOCIATED THREATS	ASSOCIATED THREAT TYPE
fakty-info[.]com	2	Phishing Generic
twinsources[.]shop	1	Malware
txid-coinbase[.]net	1	Phishing

To fill in possible gaps, we then sought to uncover other potentially connected domains via text string usage. We used Domains & Subdomains Discovery to find domains containing the string **ovmv.** using the **Starts with** parameter. We discovered 14 string-connected domains, all of which looked exactly as the IoC ovmv[.]net albeit using different top-level domain (TLD) extensions.

WHOIS comparisons with the domain ovmv[.]net, however, showed that none of them seemingly bore similarities with the IoC.

—

Our DNS deep dive into the PikaBot infrastructure allowed us to identify 339 possibly connected artifacts comprising 112 email-connected domains, three additional IP addresses, 210 IP-connected domains, and 14 string-connected domains. Additionally, our analysis enabled us to uncover five malicious web properties—two IP addresses (104[.]21[.]72[.]66 and 172[.]67[.]176[.]15) and three domains (fakty-info[.]com, twinsources[.]shop, and txid-coinbase[.]net).

If you wish to perform a similar investigation or 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 and IoCs

PikaBot IoCs

DOMAINS	IP ADDRESSES
• cxtensones[.]top • ovmv[.]net	• 139[.]99[.]222[.]29 • 172[.]232[.]162[.]198 • 172[.]232[.]164[.]77 • 172[.]232[.]186[.]251 • 54[.]37[.]79[.]82 • 57[.]128[.]108[.]132 • 57[.]128[.]109[.]221 • 57[.]128[.]164[.]11 • 57[.]128[.]83[.]129

Sample Email-Connected Domains

- 1869666[.]net
- 240690[.]com

- 242302[.]com
- 354374[.]com
- 375324[.]com
- 375714[.]com
- 375974[.]com
- 376294[.]com
- 531773[.]wang
- 531775[.]wang
- 531776[.]wang
- 547276[.]com
- 547296[.]com
- 547376[.]com
- 547926[.]com
- 643185[.]com
- 643191[.]com
- 643193[.]com
- 643252[.]com
- 643257[.]com
- 645276[.]com
- 647916[.]com
- 714903[.]com
- 721504[.]com
- 725179[.]net
- 725181[.]net
- 725183[.]net
- 725186[.]net
- 725187[.]net
- 725381[.]net
- 725382[.]net
- 725385[.]net
- 725781[.]net
- 725783[.]net
- 725785[.]net
- 725787[.]net
- 725813[.]net
- 725815[.]net
- 725816[.]net
- 725817[.]net
- 725819[.]net
- 725821[.]net
- 725904[.]com
- 725935[.]net
- 725937[.]net
- 725939[.]net
- 725951[.]net
- 729054[.]com
- 729074[.]com
- 729104[.]com

Sample Additional IP Addresses

- 104[.]21[.]72[.]66
- 172[.]67[.]176[.]15

Sample IP-Connected Domains

- 0212top[.]xyz
- 0ccctt[.]com
- 0zzccc[.]com
- 0zzmmm[.]com
- 0zzzjj[.]com
- 1009451[.]com
- 1cccss[.]com
- 1inchapp[.]com
- 2zzppp[.]com
- 2zzyyy[.]com
- 3aaann[.]com
- 3cccjj[.]com
- 3cccww[.]com
- 3ddduu[.]com
- 3zzzgg[.]com
- 3zzzll[.]com
- 4bbbqq[.]com
- 4dddoo[.]com
- 4dddrr[.]com
- 4zzkkk[.]com

- 4zzzee[.]com
- 6aaahh[.]com
- 6aaazz[.]com
- 7bbbvv[.]com
- 7dddxx[.]com
- 8aaaww[.]com
- 8h01[.]com
- 8qqqaa[.]com
- 8zzlll[.]com
- 9aaaxx[.]com
- 9bbbxx[.]com
- 9cccjj[.]com
- aaaww3[.]com
- abcash[.]co[.]uk
- argentina-changelife[.]com
- argentina-com[.]com
- argentina-job[.]com
- argentina-new[.]com
- arkhamprotocol[.]com
- avanzar-dream[.]com
- badkushmmo[.]com
- bankingston[.]com
- bbusjy[.]com
- binanselendas[.]com
- blessedtent[.]com
- boldcryptos[.]online
- bonusblackemdobro[.]com
- canadasignin[.]com
- cashbackcongrat[.]com
- chile-changelife[.]com

Sample String-Connected Domains

- ovmv[.]be
- ovmv[.]cn
- ovmv[.]com
- ovmv[.]cz
- ovmv[.]dk
- ovmv[.]eu
- ovmv[.]link