COLDRIVER's MAYBEROBOT in the DNS Spotlight

Table of Contents

Executive Report

The Google Threat Intelligence Group (GTIG) recently discovered that Russia-affiliated threat group COLDRIVER seems to have just retooled yet again. Their homegrown backdoor NOROBOT, redesigned into YESROBOT and now, MAYBEROBOT.

The redesigned tool MAYBEROBOT figured in the group's latest attack going after the same targets—high-profile individuals in nongovernment organizations (NGOs), policy advisors, and dissidents. Based on the GTIG analysis, while the group typically took the phishing route to distribute NOROBOT and YESROBOT, MAYBEROBOT may be meant for more specific targets.

GTIG publicized 14 indicators of compromise (IoCs) comprising 13 domains and one IP address in their report. WhoisXML API dove deeper into the IoCs and uncovered these findings:

- Four of the domain IoCs were deemed likely to turn malicious 127–182 days before they were reported as such
- One email-connected domain
- Four additional IP addresses, all were malicious
- Five IP-connected domains, two were malicious

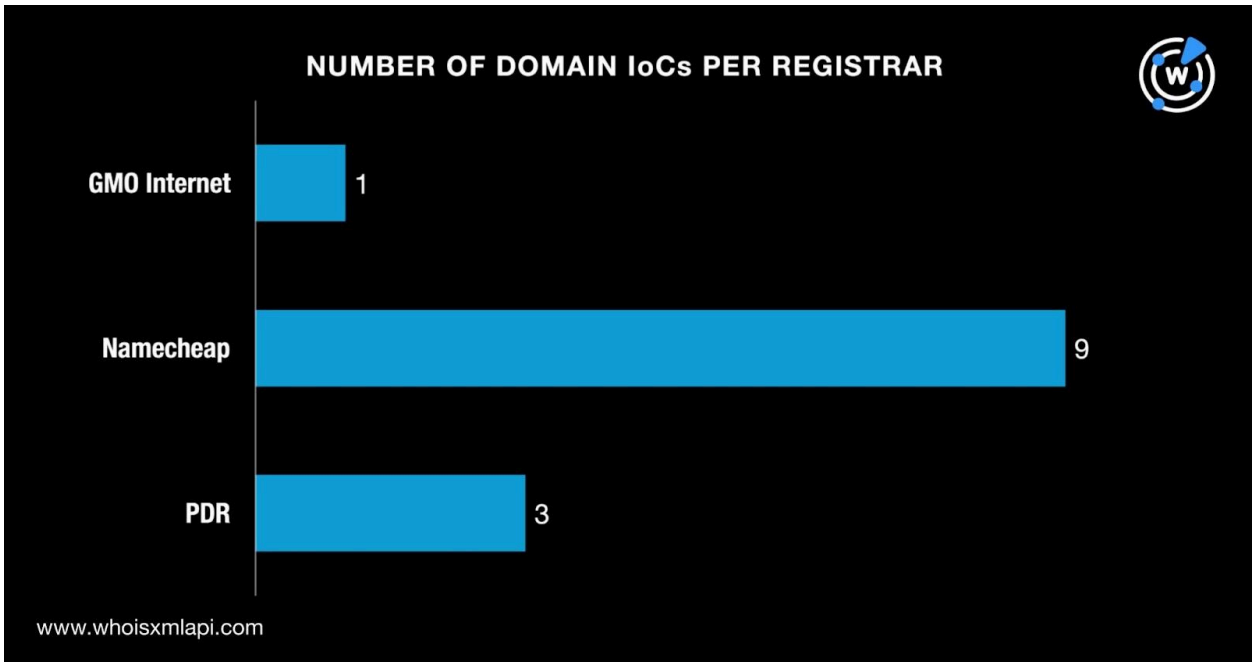
More Information about the IoCs

We queried the 13 domains identified as IoCs on First Watch Malicious Domains Data Feed and discovered that four of them were deemed likely to turn malicious 127–182 days before they were reported as such on 21 October 2025. Here are more details for two of them.

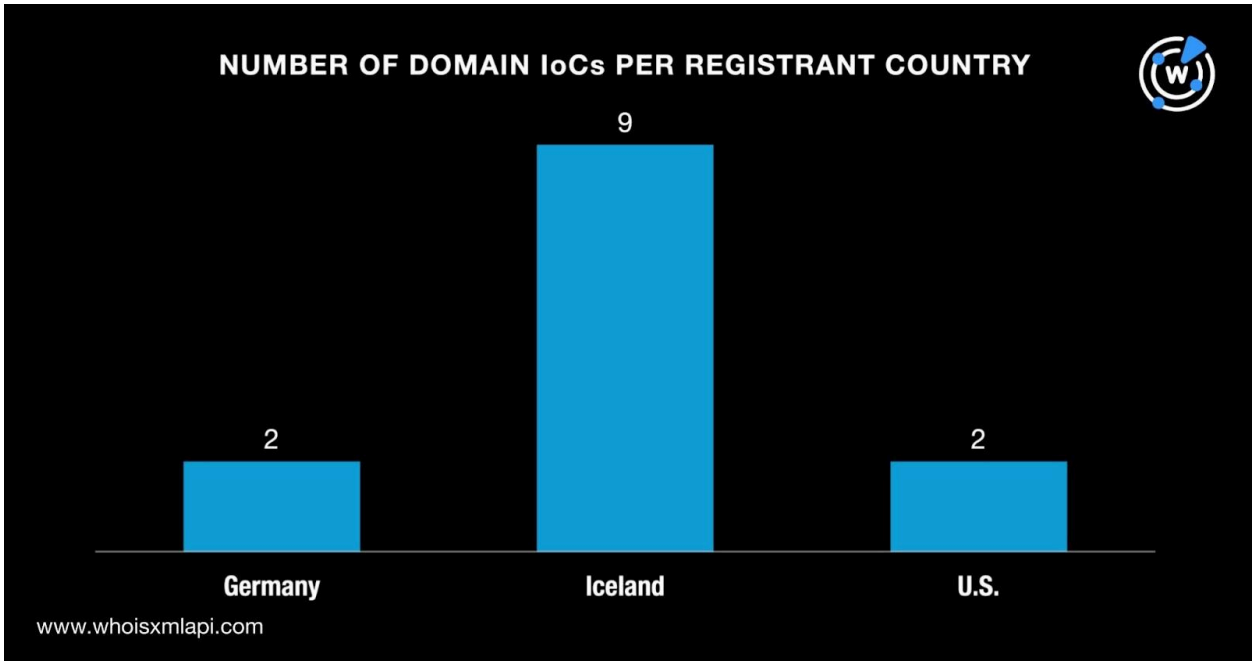
DOMAIN IoC	FIRST WATCH DATE	NUMBER OF DAYS SPOTTED BEFORE THE REPORTING DATE
documentsec[.]online	22 April 2025	182
system-healthadv[.]com	9 May 2025	165

Then, we queried the 13 domains identified as IoCs on WHOIS API and found out that:

- They were all relatively new, created between 2 April and 2 July 2025.
- They were split across three registrars led by Namecheap, which accounted for nine domains. PDR took the second spot with three domains. GMO Internet completed the roster with one domain.



- They were registered in three countries topped by Iceland, which accounted for nine domains. Two domains each, meanwhile, were registered in Germany and the U.S.



Next, we queried the 13 domains identified as IoCs on DNS Chronicle API, which revealed that they had 57 historical domain-to-IP resolutions in all. The domain inspectguarantee[.]org posted the oldest resolution on 4 April 2025. It had six resolutions until 29 September 2025. Take a look at more details for five other domains below.

DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
southprovesolutions[.]com	7	5 April 2025	2 October 2025
documentsec[.]online	4	23 April 2025	2 May 2025
oxwoocat[.]org	1	24 April 2025	24 April 2025
documentsec[.]com	5	29 April 2025	29 August 2025
system-healthadv[.]com	6	10 May 2025	25 September 2025

After that, we queried the sole IP address identified as an IoC on IP Geolocation API and found out that it was geolocated in the U.S. and administered by TimeWeb.

A DNS Chronicle API query for the sole IP address as an IoC showed that it had 79 IP-to-domain resolutions from 6 February 2020 to 5 September 2025.

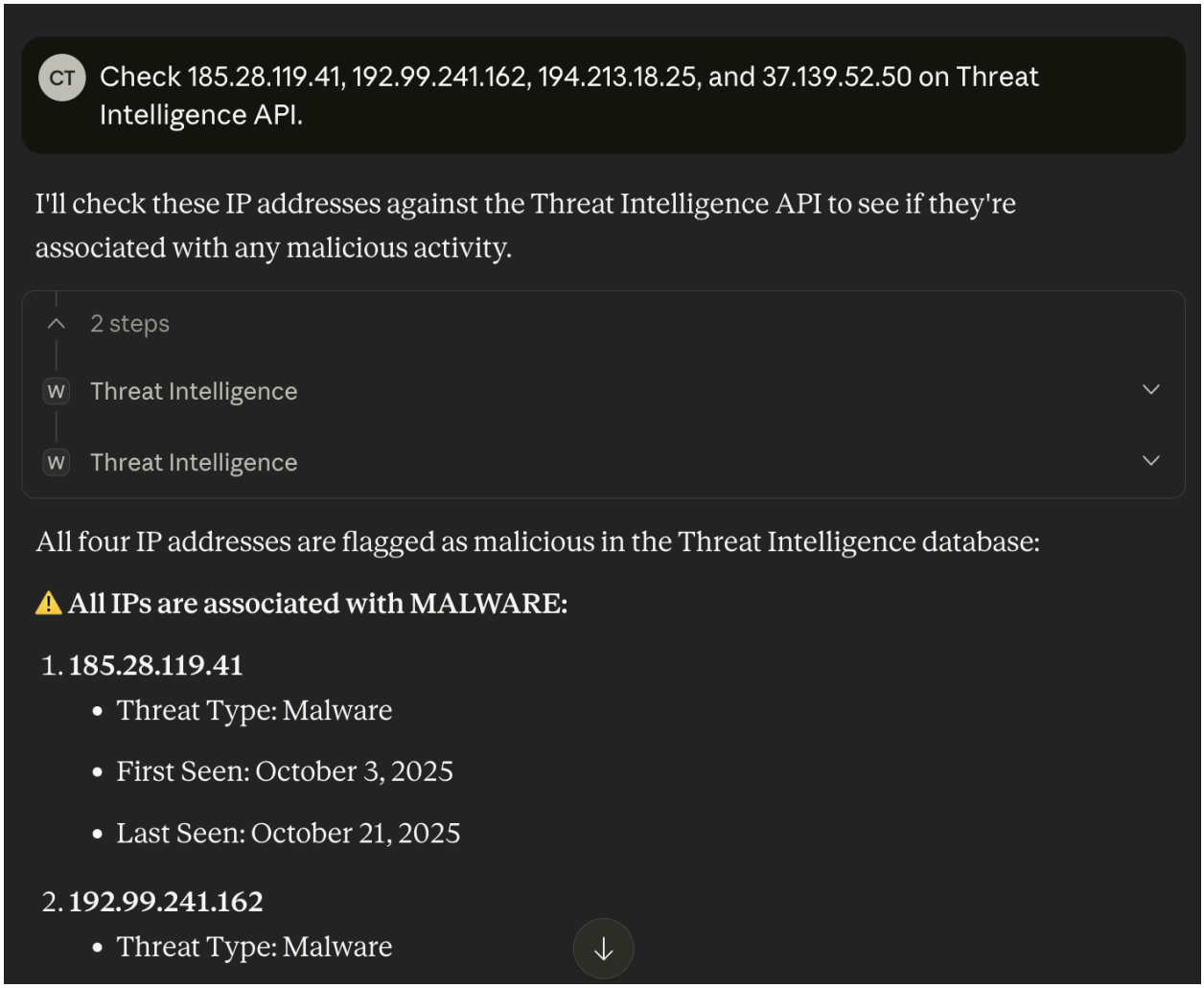
The Hunt for New Artifacts

After knowing more about the IoCs, we then hunted for more connected artifacts starting with a WHOIS History API query for the 13 domains identified as IoCs. We found out that 10 of them had email addresses in their historical WHOIS records. We uncovered nine unique email addresses and one of them was a public address.

A Reverse WHOIS API query for the sole public email address led to the discovery of a single email-connected domain after duplicates and those already identified as IoCs were filtered out.

Then, we queried the 13 domains identified as IoCs on DNS Lookup API, which showed that six of them had active IP resolutions. They resolved to four unique additional IP addresses.

A Threat Intelligence API query via the WhoisXML API MCP Server for the four additional IP addresses revealed that all of them have been weaponized for malware distribution. We used the prompt “Check 185.28.119.41, 192.99.241.162, 194.213.18.25, and 37.139.52.50 on Threat Intelligence API.”

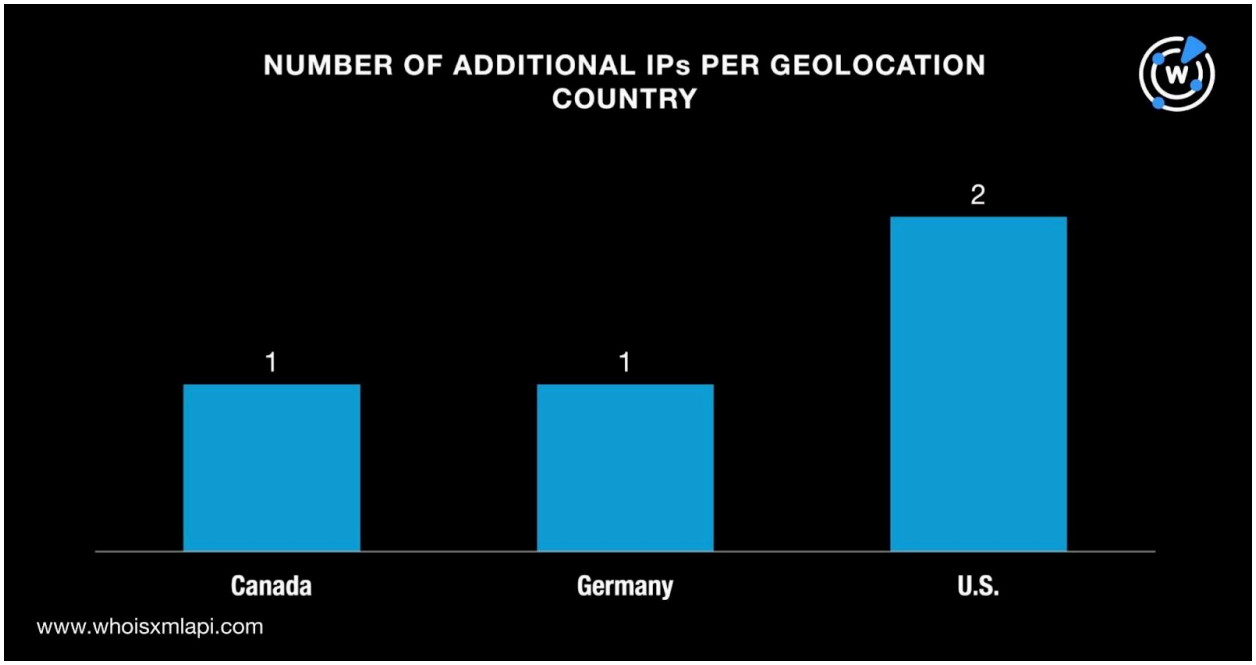


Here are more details for two of them.

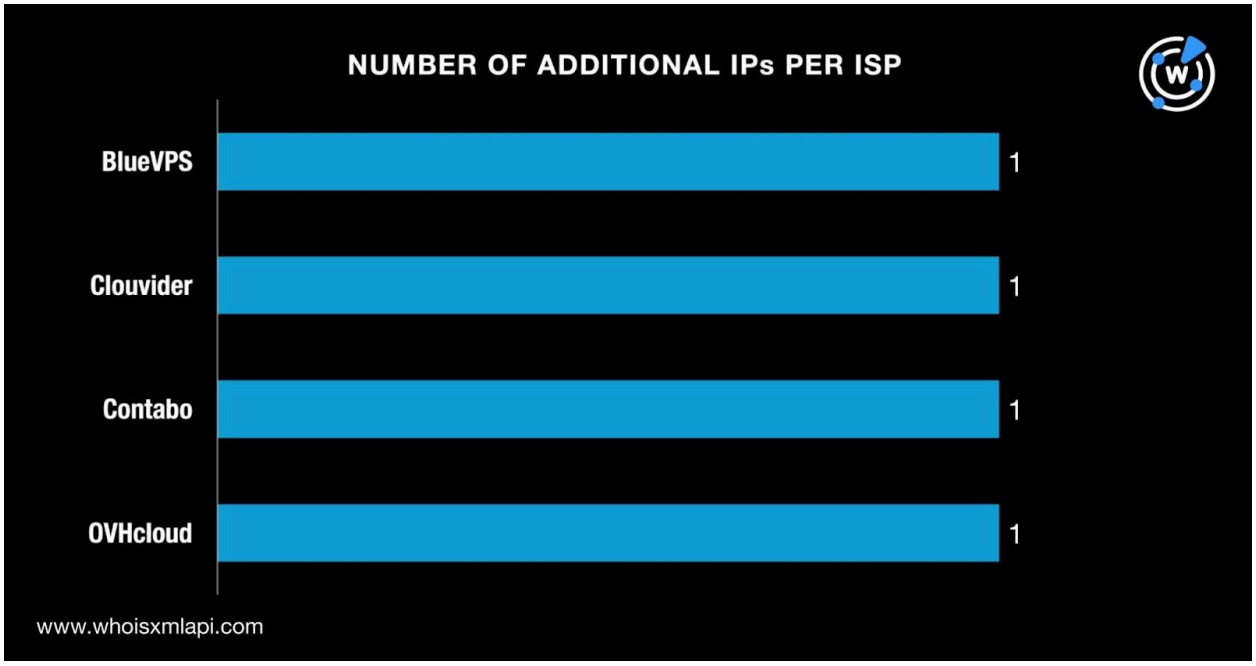
ADDITIONAL IP ADDRESS	ASSOCIATED THREAT	DATE SEEN
185[.]28[.]119[.]41	Malware distribution	3–21 October 2025
37[.]139[.]52[.]50	Malware distribution	26 September–21 October 2025

A Bulk IP Geolocation Lookup for the four additional IP addresses, meanwhile, unveiled that:

- They were split across three geolocation countries led by the U.S., which accounted for two IP addresses. One IP address each originated from Canada and Germany. Note that the sole IP address identified as an IoC also hailed from the U.S.



- One IP address each was administered by BlueVPS, Clouvider, Contabo, and OVHcloud.



At this point, we now had five IP addresses for further analysis. We queried them on Reverse IP API and discovered that all of them could be dedicated hosts. They hosted five IP-connected

domains after filtering out duplicates, those already identified as IoCs, and the email-connected domain.

A Threat Intelligence API query for the five IP-connected domains showed that two have already figured in cyber attacks. The domain hazerscotomacarted[.]org, for instance, was associated with malware distribution.

—

Our in-depth investigation of MAYBEROBOT revealed that four of the domains identified as IoCs were dubbed likely to turn malicious 127–182 days before being dubbed as such. We also uncovered 10 new artifacts comprising six domains (i.e., one email-connected and five IP-connected) and four IP addresses. Notably, six of the artifacts we just uncovered are already considered malicious.

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

Email-Connected Domain

- numencapt[.]space

Additional IP Addresses

- 185[.]28[.]119[.]41
- 192[.]99[.]241[.]162

IP-Connected Domains

- hazerscotomacarted[.]org
- mediasrangylavi[.]org
- ned-application-proposal[.]org