Probing the DNS Depths of PeckBirdy

Table of Contents

Executive Report

Trend Micro recently published their report on PeckBirdy, a JS-based C&C framework China-aligned APT actors have been using since 2023. The threat was designed to execute across multiple environments, enabling flexible deployment.

So far, two modular backdoors—HOLODONUT and MKDOOR, multiple attack vectors, stolen code-signing certificate Cobalt Strike payloads, and exploits (CVE-2020-16040) have figured along PeckBirdy in various campaigns.

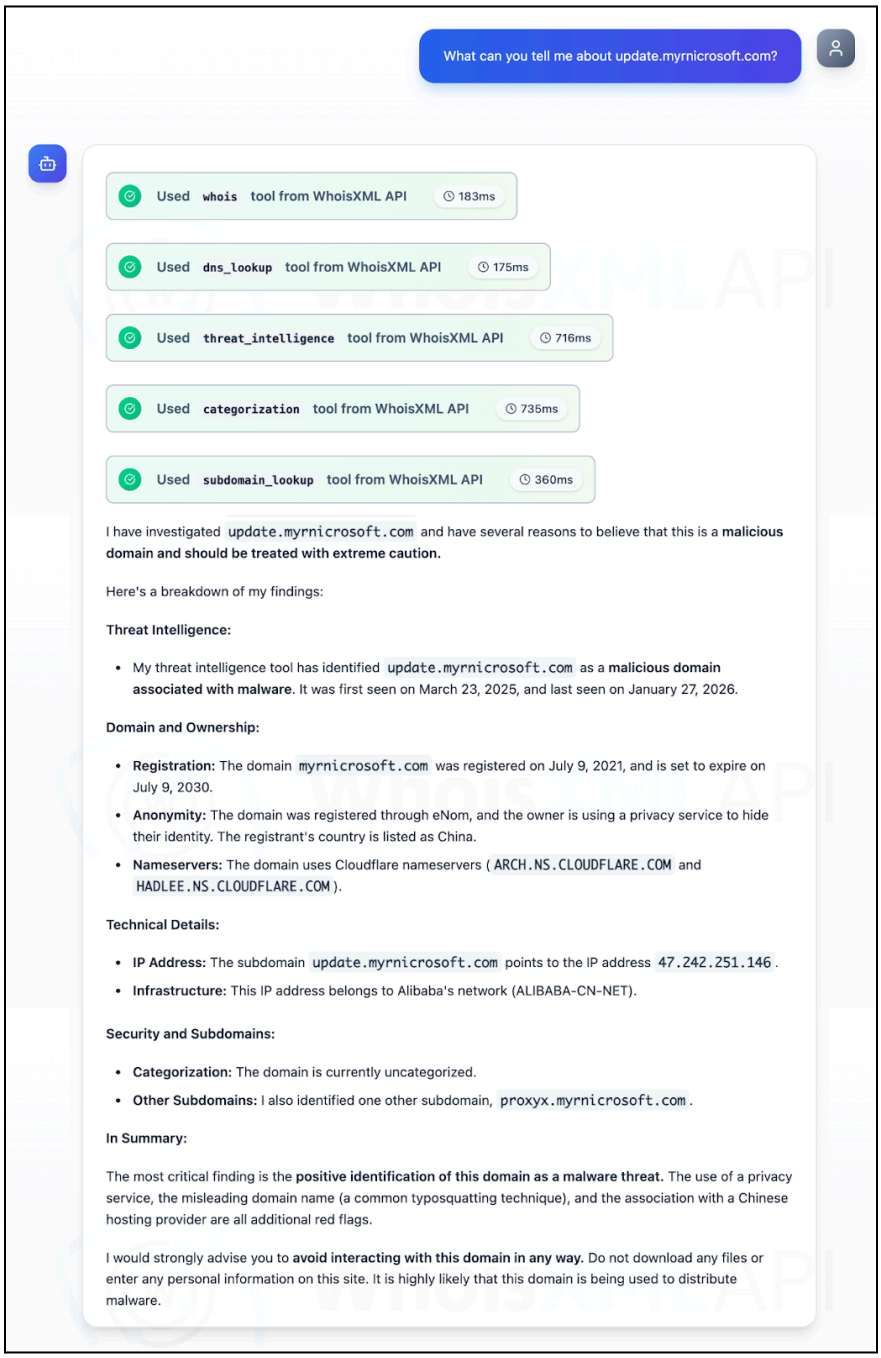
The researchers also identified 36 network IoCs related to the threat. After further scrutiny of the IoCs, specifically extracting unique domains from the subdomains tagged as IoCs, we analyzed 56 IoCs in all. Our analysis led to these discoveries:

- Three unique client IP addresses communicated with one domain classified as an IoC
- Six domains identified as IoCs were registered with malicious intent 122–804 days before being dubbed as such
- 64 email-connected domains
- 23 additional IP addresses, 20 of which turned out to be malicious
- Two IP-connected domains
- 18,188 string-connected domains, 49 of which turned out to be malicious

Note that before embarking on our in-depth IoC investigation, we first assessed the legitimacy of the 28 domains identified as IoCs aided by the WhoisXML API MCP Server. Our analysis confirmed that all of them were illegitimate domains.

Scrutinizing the Subdomain IoCs

We queried the 20 subdomains tagged as IoCs on Jake AI and found out that two—update[.]myrnicrosoft[.]com and updates[.]oss-cdn[.]com—have already been involved with distributing malware.

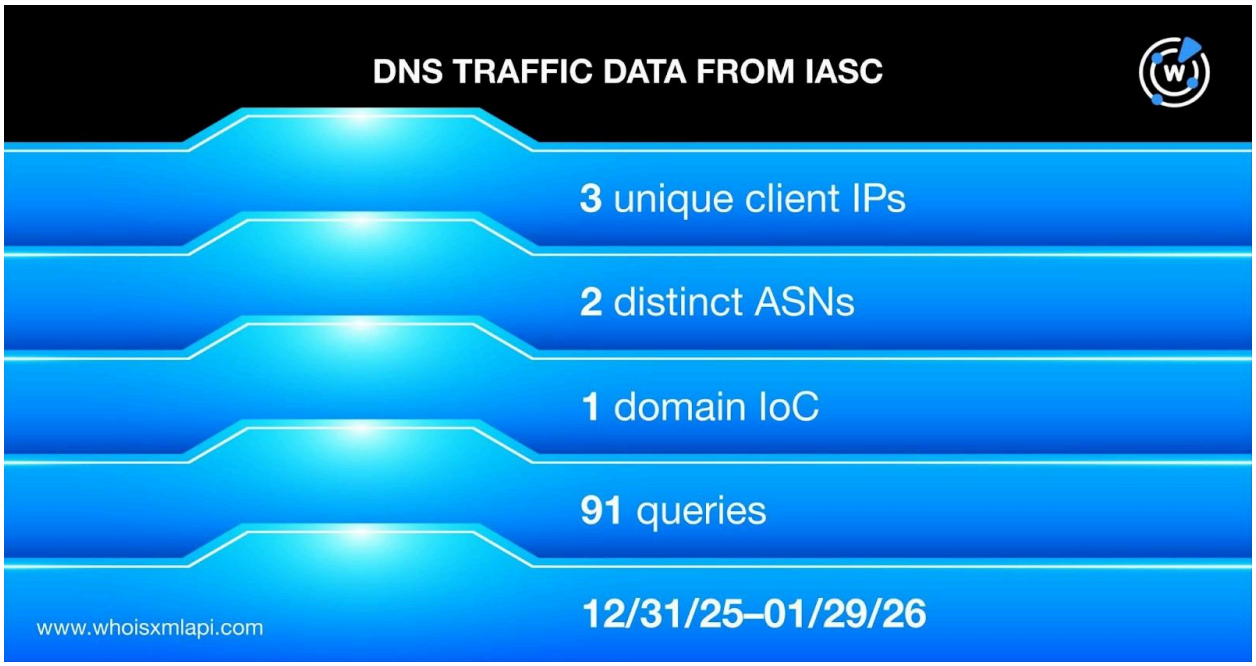


Jake AI result for the subdomain update[.]myrnicrosoft[.]com

The remaining subdomains were either compromised though legitimate or suspicious primarily based on their use of potential typosquatting domains.

Dissecting the DNS Traces of the Domain IoCs

Sample network traffic data from the IASC revealed that three unique client IP addresses under two distinct ASNs communicated with a domain classified as an IoC via 91 DNS queries made between 31 December 2025 and 29 January 2026.

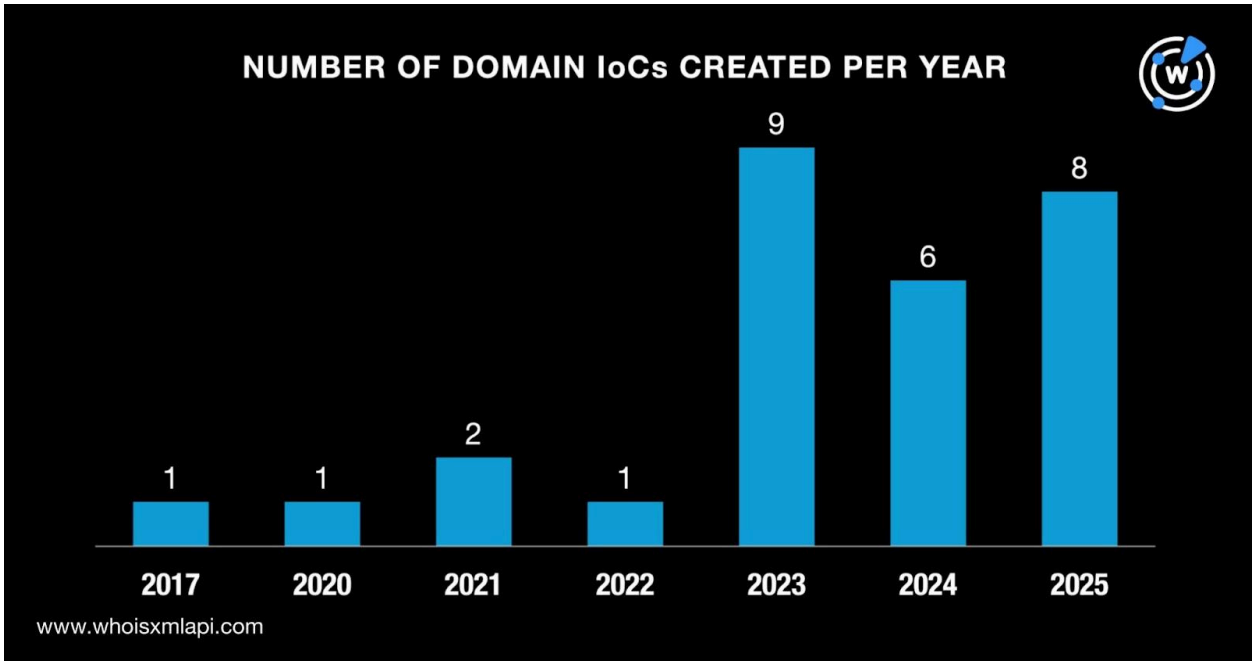


We then scoured the First Watch Malicious Domains Data Feed for the 28 domains identified as IoCs and found out that six were registered 122–804 days before they were dubbed as malicious.

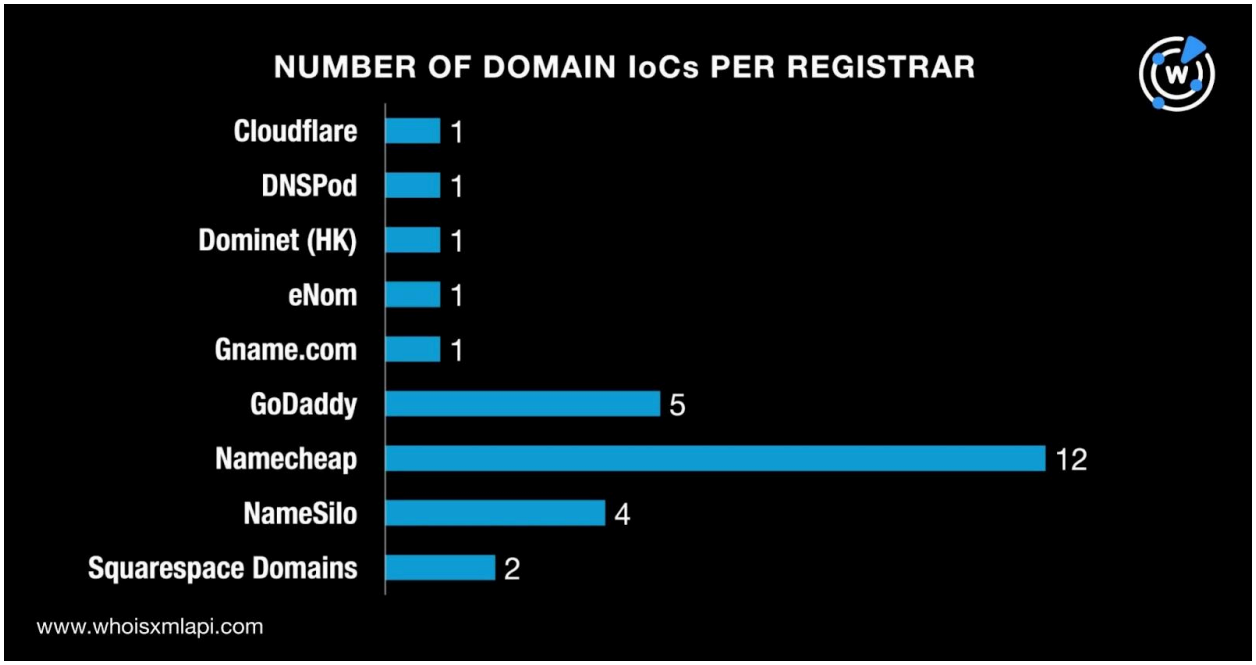
DOMAIN IoC	FIRST WATCH INCLUSION DATE	NUMBER OF DAYS BEFORE BEING REPORTED AS IoC
mkdmcdn[.]com	11/14/23	804
ppcn-cdn[.]xyz	03/12/24	685
jsunpkg[.]com	04/07/24	659

Next, we queried the 28 domains identified as IoCs on WHOIS API and discovered that:

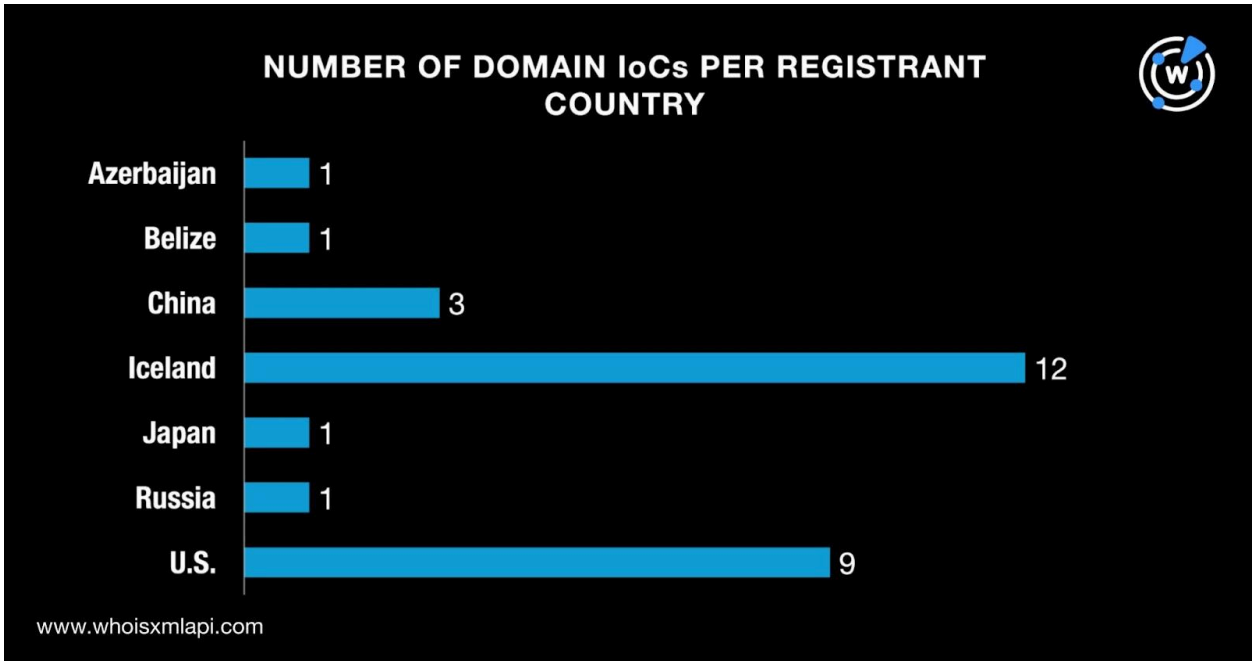
- They were created between 30 November 2017 and 29 November 2025.



- They were administered by nine different registrars.



- They were registered in seven different countries.



DNS Chronicle API queries for the 28 domains tagged as IoCs showed that 22 had recorded 2,205 historical domain-to-IP resolutions over time. While the domain img-cache[.]com posted the oldest first resolution date, githubgressaccess[.]info recorded the latest.

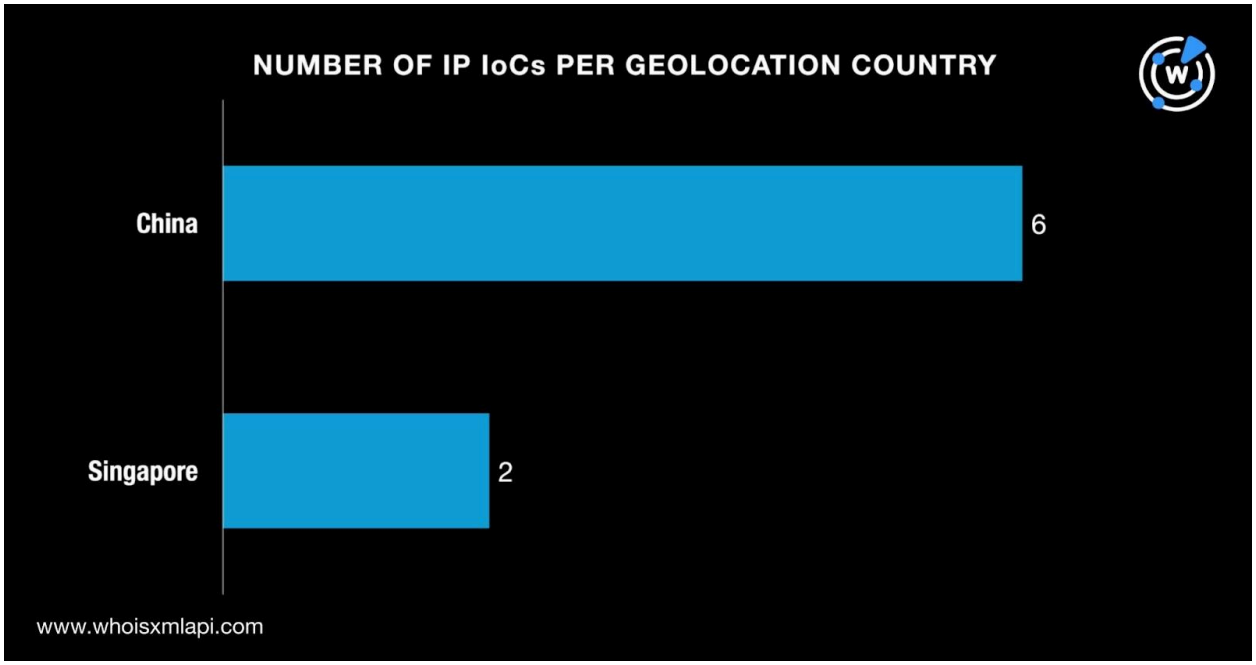
DOMAIN IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
img-cache[.]com	68	12/10/17	12/07/18
microsoft-ads[.]com	90	07/27/19	08/16/20
a1icdn[.]com	58	08/31/19	01/27/26
js-cdn[.]xyz	55	07/30/20	01/27/26
static-alicdn[.]com	79	09/03/21	01/27/26

A closer look at the first resolution dates of the domains also showed that seven were likely utilized in the same campaign in 2023, five in 2025, three in 2024, and two each in 2019 and 2021.

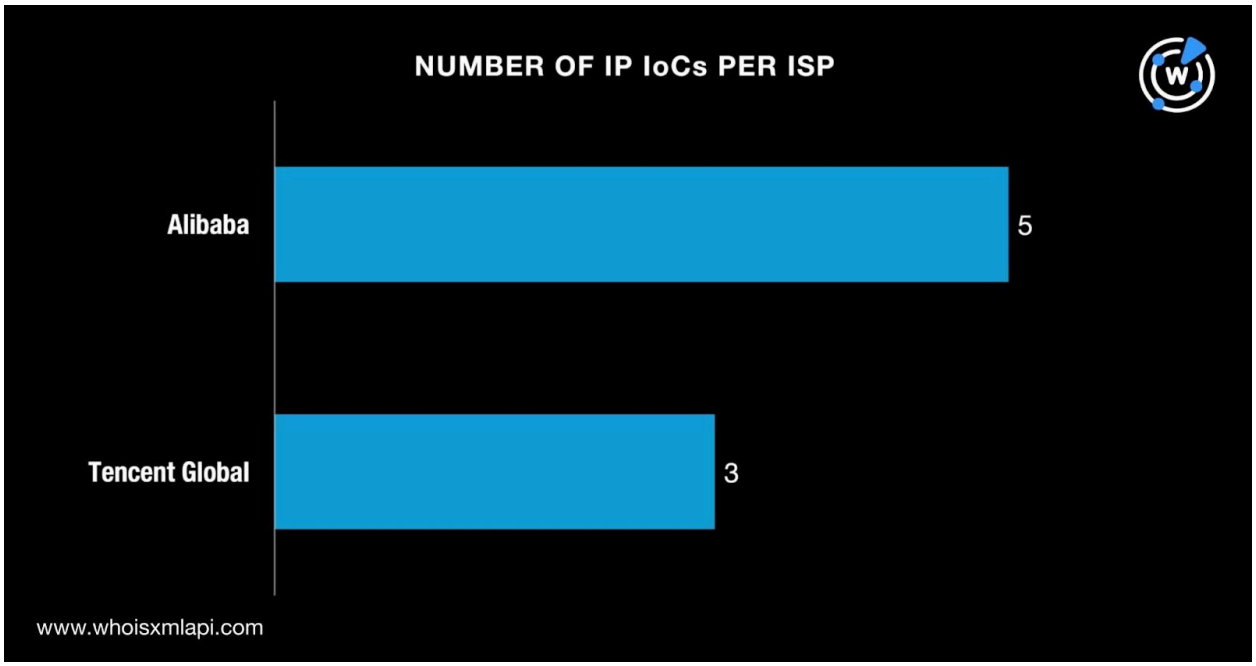
Investigating the IP IoCs

We queried the eight IP addresses classified as IoCs on Bulk IP Geolocation Lookup and found out that:

- They were geolocated in two countries. Only one—China, however, appeared as a registrant country as well.



- They were administered by two ISPs.



DNS Chronicle API queries for the eight IP addresses identified as IoCs, meanwhile, showed that six recorded 58 historical IP-to-domain resolutions over time.

IP IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
8[.]218[.]50[.]207	19	06/10/22	11/09/25
43[.]156[.]94[.]185	18	04/03/23	09/14/25
8[.]222[.]143[.]246	9	11/11/23	06/11/24

New Artifacts Uncloaked

We started our search for new artifacts by querying the 28 domains identified as IoCs on WHOIS History API and discovered that 21 had 35 unique email addresses in their historical WHOIS records. Upon closer investigation, we learned that five were public email addresses.

Reverse WHOIS API queries for the five public email addresses revealed that while one could belong to a domainer, the remaining four appeared in the historical WHOIS records of other domains. We uncovered 64 unique email-connected domains after those already tagged as IoCs were filtered out.

Next, we queried the 28 domains classified as IoCs on DNS Lookup API and found out that 13 currently resolved to 23 unique IP addresses not on the IoC list.

Threat Intelligence API queries for the 23 unique IP addresses revealed that 20 have already been weaponized for various attacks.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
104[.]21[.]24[.]113	Malware distribution Phishing Generic threat	10/23/24 06/30/23 01/27/24	01/26/26 01/26/26 01/08/26
104[.]21[.]25[.]105	Phishing Malware distribution Generic threat	05/22/23 04/11/23 07/01/23	01/27/26 01/26/26 11/05/25
104[.]21[.]44[.]46	Phishing Malware distribution Generic threat	03/28/23 12/08/23 04/03/23	01/27/26 01/26/26 11/15/25

104[.]21[.]63[.]97	Phishing Malware distribution Generic threat	05/24/23 08/25/23 04/28/25	01/27/26 01/17/26 01/11/26
104[.]21[.]90[.]19	Phishing Malware distribution Generic threat	06/24/23 10/05/23 06/17/23	01/27/26 01/26/26 10/31/25

We now had 31 IP addresses for the next step of our analysis—the eight identified as IoCs and the 23 we unearthed from the last step. We queried them on Reverse IP API. Further scrutiny showed that five could be dedicated hosts. We unearthed two unique IP-connected domains after those already tagged as IoCs and the email-connected domains were filtered out.

We extracted 18 unique text strings listed below from the 28 domains classified as IoCs and queried them on Domains & Subdomains Discovery.

- a1icdn.
- as-cdn.
- cache-cdn.
- css-alicdn.
- githubassets.
- github
- hcaphcha.
- img-cache.
- img-
- js-cdn.
- microsoft-ads.
- microsoft-edges.
- microsoftgpt.
- mkdmcdn.
- mod-js.
- oss-cdn.
- static-resource.
- static-

We uncovered 18,188 unique string-connected domains that started with the strings above after those already identified as IoCs and the email- and IP-connected domains were filtered out.

Threat Intelligence API queries for the string-connected domains revealed that 49 have already been weaponized for various attacks.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT	DATE FIRST SEEN	DATE LAST SEEN
github-desktop[.]com	Malware distribution	09/09/25	01/27/26
github-readme[.]com	Malware distribution	08/03/23	01/27/26

github-scanner[.]com	Malware distribution	09/19/24	01/26/26
github-scanner[.]shop	Malware distribution	09/19/24	01/26/26
github[.]green	Malware distribution	03/20/25	01/27/26

—

Our in-depth analysis of the PeckBirdy IoCs showed that three unique client IP addresses communicated with a domain tagged as an IoC. In addition, six domains classified as IoCs were registered with malicious intent from the get-go.

We also unearthed 18,277 new artifacts comprising 64 email-connected domains, 23 additional IP addresses, two IP-connected domains, and 18,188 string-connected domains. At least 69 of them have already figured in malicious campaigns.

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

- 009080[.]com
- 08v[.]cn
- 08wei[.]com
- chakuan[.]com
- chakuan[.]net
- cheap-airguns[.]com
- exie[.]wang
- fanke520[.]com
- fodu[.]wang
- hupifa[.]cn
- hupifa[.]com
- iip[.]wang
- itao5[.]com
- ledaifa[.]cn
- ledaifa[.]com
- lhepay[.]com
- mingbuyi[.]com
- mongline[.]com
- mongline[.]net
- nvtao[.]wang
- qrmv[.]com
- renwei[.]wang
- repi[.]wang
- shengnai[.]cn
- sudaifa[.]cn
- sudaifa[.]com
- taiyangyu168[.]com
- taoshei[.]com
- taoxiechang[.]com
- weigv[.]com
- xyij[.]com
- zhengnai[.]com
- zhidaoma[.]cn

Sample Additional IP Addresses

- 104[.]21[.]24[.]113
- 104[.]21[.]25[.]105
- 104[.]21[.]44[.]46
- 172[.]67[.]134[.]4
- 172[.]67[.]145[.]32
- 172[.]67[.]151[.]6
- 103[.]27[.]110[.]25
- 103[.]87[.]9[.]71
- 124[.]222[.]77[.]143

Sample IP-Connected Domain

- cddwj[.]com[.]cn

Sample String-Connected Domains

- a1icdn[.]net
- as-cdn[.]cf
- as-cdn[.]com
- as-cdn[.]tk
- cache-cdn[.]com
- cache-cdn[.]me
- cache-cdn[.]net
- css-alicdn[.]ph
- css-alicdn[.]vg
- css-alicdn[.]ws

- github-01[.]com[.]ws
- github-01[.]edu[.]ws
- github-01[.]ngo[.]ph
- github[.]ac
- github[.]ac[.]cn
- github[.]academy
- hcaphcha[.]ph
- hcaphcha[.]ws
- img----ur[.]com
- img---bb[.]com
- img--bb[.]cc
- js-cdn[.]cc
- js-cdn[.]club
- js-cdn[.]co
- microsoft-ads[.]asia
- microsoft-ads[.]ga
- microsoft-ads[.]info
- microsoft-edges[.]net
- microsoftgpt[.]ai
- microsoftgpt[.]cn
- microsoftgpt[.]com
- mkdmcdn[.]ph
- mkdmcdn[.]ws
- mod-js[.]com
- mod-js[.]dev
- mod-js[.]su
- oss-cdn[.]pw
- oss-cdn[.]top
- oss-cdn[.]ws
- static--mouv--desjardins[.]com
- static-0-28[.]edu[.]ee
- static-0-4[.]com[.]ph
- xn--github-g1da[.]fm
- xn--github-g1da[.]vg
- xn--github-uua[.]com