WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A Close Look under the DNS Hood of CoolClient

Threat Report

Table of Contents

Executive Report

Securelist recently uncovered a new HoneyMyte (also known as “Mustang Panda” or “Bronze President”) campaign leveraging an updated version of CoolClient. The group has been known to use various sophisticated tools like ToneShell, PlugX, Qreverse, CoolClient, Tonedisk, and SnakeDisk, among others.

In 2025, HoneyMyte updated the CoolClient backdoor, adding new features like deploying several browser login data stealers and using multiple data theft and reconnaissance scripts.

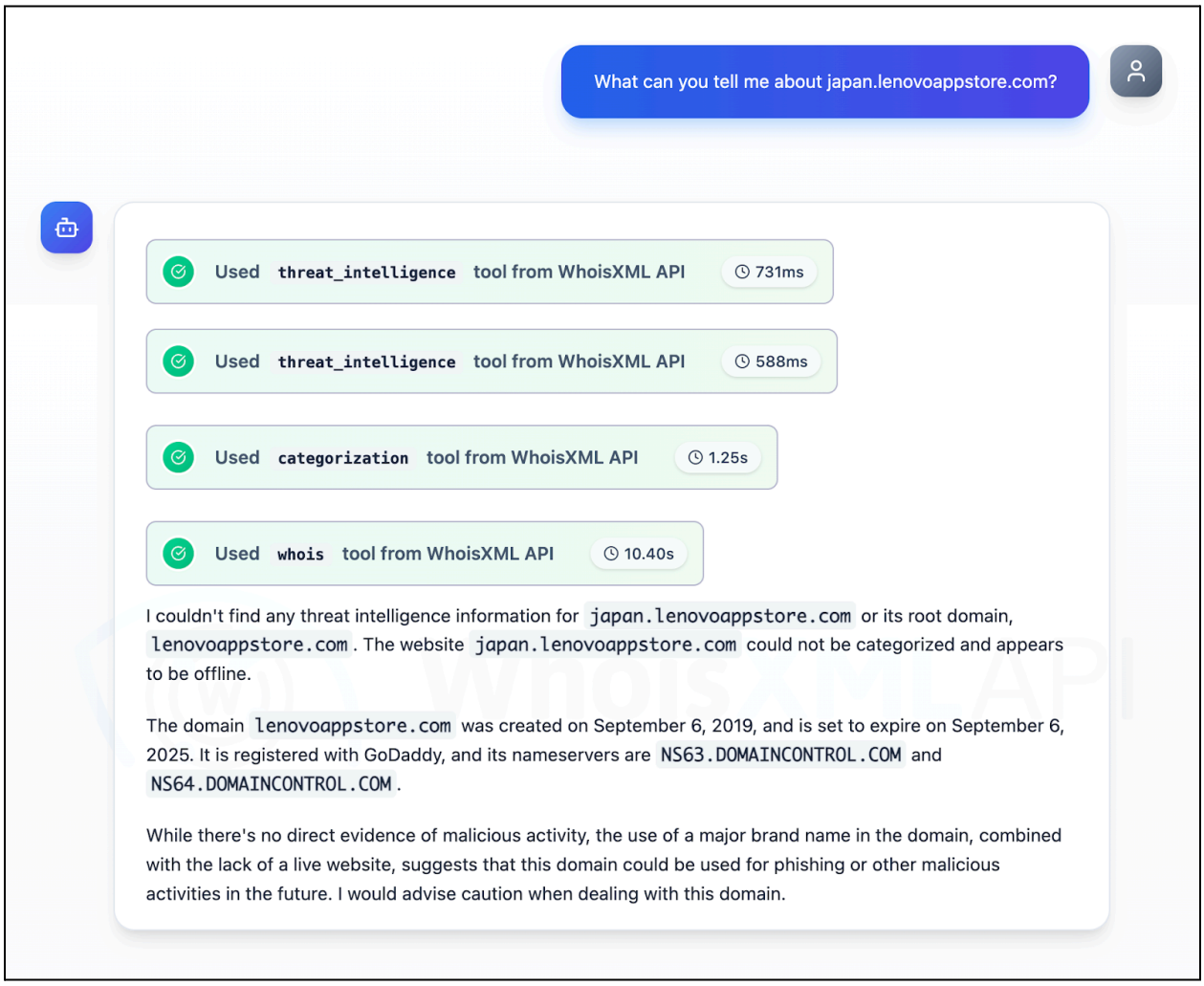
The researchers originally identified four CoolClient network IoCs. After more careful scrutiny (extracting domains from the subdomains and weeding out legitimate ones), we ended up with six IoCs in all comprising three domains, two subdomains, and one IP address. We then verified the legitimacy of the three domains tagged as IoCs aided by the WhoisXML API MCP Server and discovered that none of them were owned by legitimate entities.

Our in-depth investigation of the CoolClient IoCs led to these findings:

- 57 email-connected domains
- One additional IP address that turned out to be malicious
- Five IP-connected domains, two of which have already been classified as malicious
- Three string-connected domains

A Further Study of the Subdomain IoCs

We began our investigation by analyzing the two subdomains identified as IoCs through our MCP server. We discovered that while there was not much to tell about one of them, we learned that the subdomain japan[.]lenovoappstore[.]com may be worth avoiding due to its use of a major brand name despite its illegitimacy (it does not belong to Lenovo) and lack of a live website that could suggest its ties to phishing or other malicious activities.

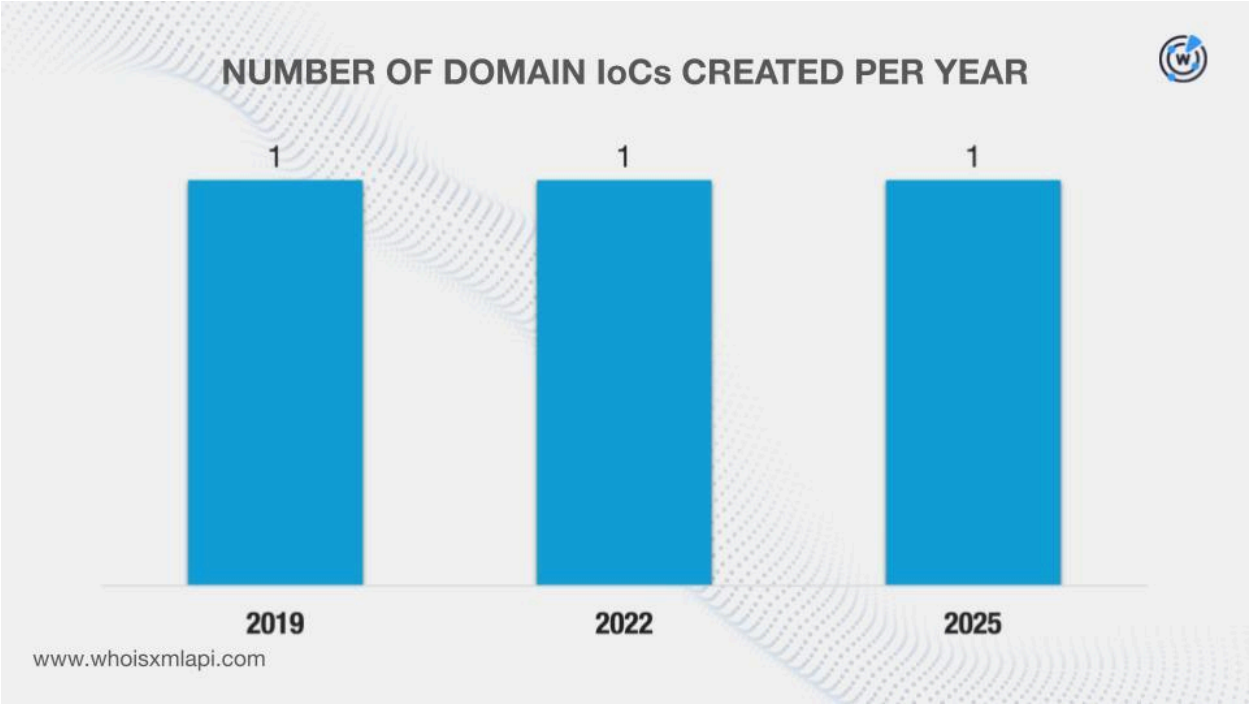


Jake AI result for the subdomain japan[.]lenovoappstore[.]com

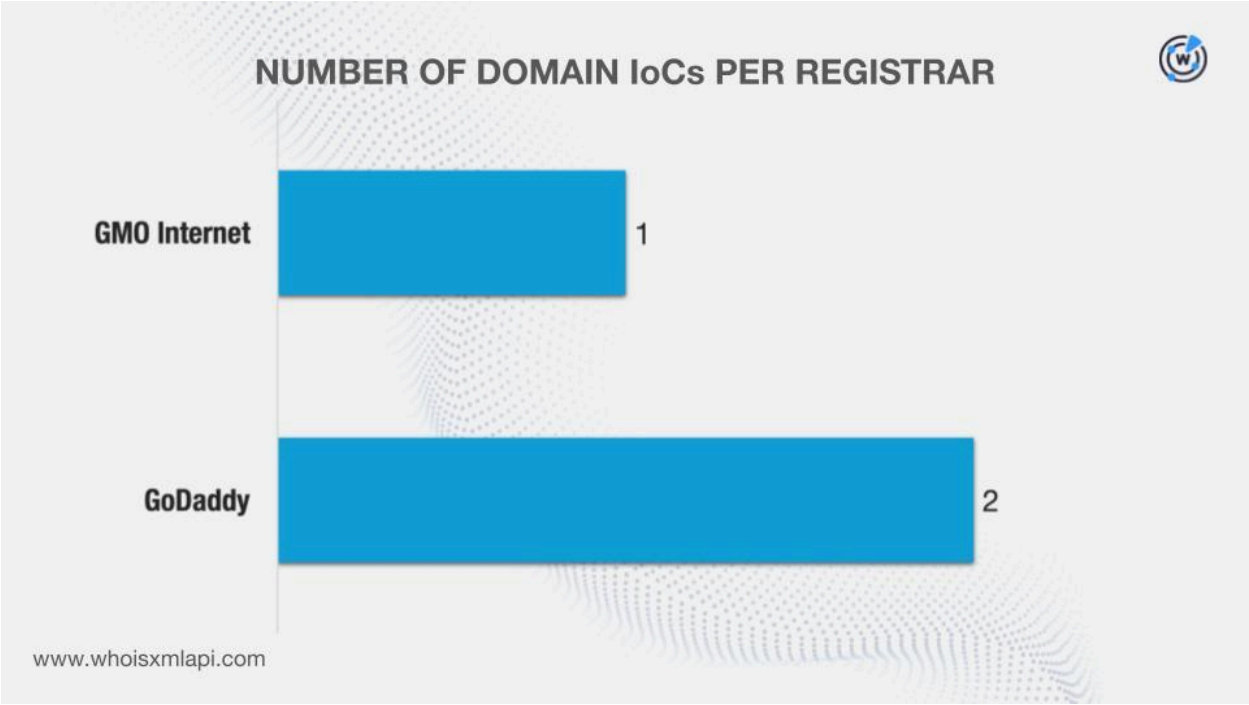
A Deep Dive into the Domain IoCs

We queried the three domains identified as IoCs on WHOIS API and discovered that:

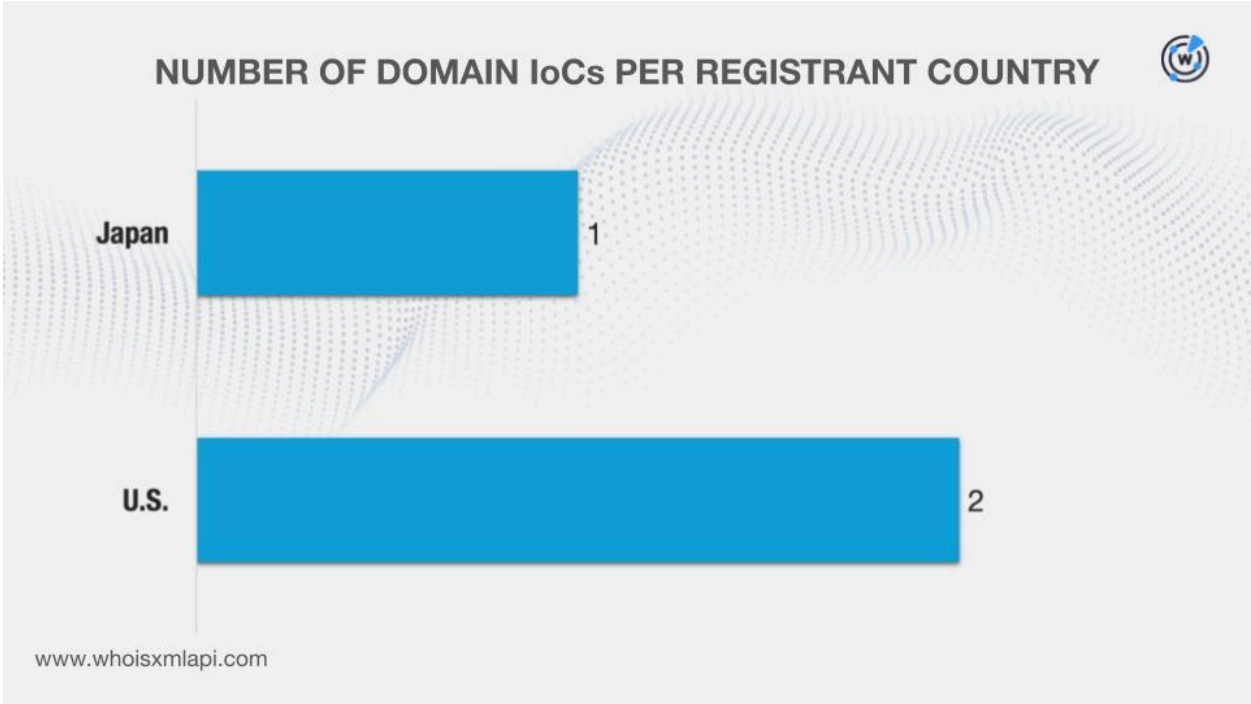
- They were created between 6 September 2019 and 3 January 2025.



- They were administered by two registrars.



- They were registered in two countries.



DNS Chronicle API queries for the three domains tagged as IoCs showed that they recorded 213 historical domain-to-IP resolutions over time. The domain lenovoappstore[.]com, for instance, posted 131 resolutions from 30 April 2020 to 6 September 2025.

An Investigation of the IP IoC

We queried the sole IP address identified as an IoC on IP Geolocation API and discovered that it was geolocated in Malaysia under the purview of ISP Extreme Broadband.

A DNS Chronicle API query for the IP address, meanwhile, revealed that it has recorded 146 IP-to-domain resolutions between 5 February 2017 and 14 May 2021.

Digging Up New Artifacts

To uncover new potentially connected artifacts, we queried the three domains identified as IoCs on WHOIS History API. We found out that two of them had two unique email addresses in their historical WHOIS records. Further scrutiny showed that one of them was a public email address.

A Reverse WHOIS API query for the public email address led to the discovery of 57 unique email-connected domains after those already tagged as IoCs were filtered out.

Next, we queried the three domains named as IoCs on DNS Lookup API and discovered that one of them resolved to an IP address that differed from the one already classified as an IoC.

A Threat Intelligence API query for the additional IP address revealed that it has been associated with malware distribution from 14–15 February 2026 that, interestingly, coincides with much-celebrated Valentine's Day.

An IP Geolocation API query, meanwhile, for the additional IP address revealed that it was geolocated in Japan under the administration of NTT Communications Corporation (OCN).

After that last step, we now had two IP addresses for further investigation. Reverse IP API queries for them showed that one could be a dedicated host. We collated five unique IP-connected domains after those already classified as IoCs and the email-connected domains were filtered out.

Threat Intelligence API queries for the IP-connected domains revealed that two have already been weaponized for various threats. The domain bit[.]kozow[.]com, for instance, has been associated with malware distribution between 30 May 2024 and 15 February 2026.

Next, we looked more closely at the three domains categorized as IoCs and extracted two unique text strings:

- lenovoappstore.
- popnike-share.

Using them as Domains & Subdomains Discovery search terms, we uncovered three unique string-connected domains that started with them after those already labeled as IoCs and the email- and IP-connected domains were filtered out.

A Summary of Our Findings

Our in-depth investigation of the HoneyMyte campaign leveraging CoolClient led us to the discovery of 66 new artifacts comprising 57 email-connected domains, one additional IP address, five IP-connected domains, and three string-connected domains. In addition, three 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

- 1shuadan[.]com
- ahdxs[.]cn
- ahyljj[.]com
- ahzajr[.]com
- bestudio[.]cn
- ceyanling[.]com
- deyunhongjiu[.]com
- dingyouqian[.]com
- hengdajinfu[.]net
- hfcoffee[.]com
- hfshuhua[.]com
- jlbkmgo[.]com
- jukuaiji[.]com
- julvshi[.]com
- laodujiucang[.]com
- laojiangke[.]com
- lawuliangpin[.]com
- mijiacloud[.]com
- mijiamall[.]com
- n95[.]com[.]cn
- qihuasuan[.]com
- qitoushan[.]com
- shanzhuyu[.]com[.]cn
- shanzhuyu[.]net
- shmiqilin[.]com
- tianmaohaofang[.]com[.]cn
- tkjtw[.]cn
- tphk[.]com[.]cn
- wangguangxi[.]com
- xiaokengchaye[.]com
- xinjianghuo[.]com
- xiyuguopin[.]com
- yezhongkui[.]com
- yikaizuche[.]com
- yshuangjing[.]com
- zaopi[.]net
- zashuguan[.]com
- zghme[.]com

IP Address

- 153[.]235[.]147[.]200

Sample IP-Connected Domains

- bit[.]kozow[.]com
- mall[.]mywire[.]org
- www[.]chock[.]mywire[.]org

Sample String-Connected Domains

- lenovoappstore[.]ph
- popnike-share[.]ph