



Unraveling the DNS Connections of ToxicPanda

Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Artifacts](#)

Executive Report

Banking Trojans have [been around for decades](#) and still persist to this day because they effectively siphon off victims' financial data and savings. And one of the latest additions to the ever-growing malware type—ToxicPanda—has been plaguing bank customers throughout Asia and Latin America since October 2024.

ToxicPanda primarily affects Android devices. Its main goal is to initiate money transfers from compromised devices via account takeovers (ATOs) using a technique called “on-device fraud (ODF).” It bypasses bank countermeasures to enforce user identity verification and authentication as well as behavioral detection techniques to identify suspicious money transfers.

Cleafy analyzed the malware in great depth and identified 26 indicators of compromise (IoCs), including 21 domain names in their [report](#). The WhoisXML API research team expanded the list of 21 domain IoCs through a DNS deep dive and uncovered more connected artifacts, including:

- Six email-connected domains
- Seven IP addresses, four of which turned out to be malicious
- One IP-connected domain, which turned out to be malicious
- 817 string-connected domains

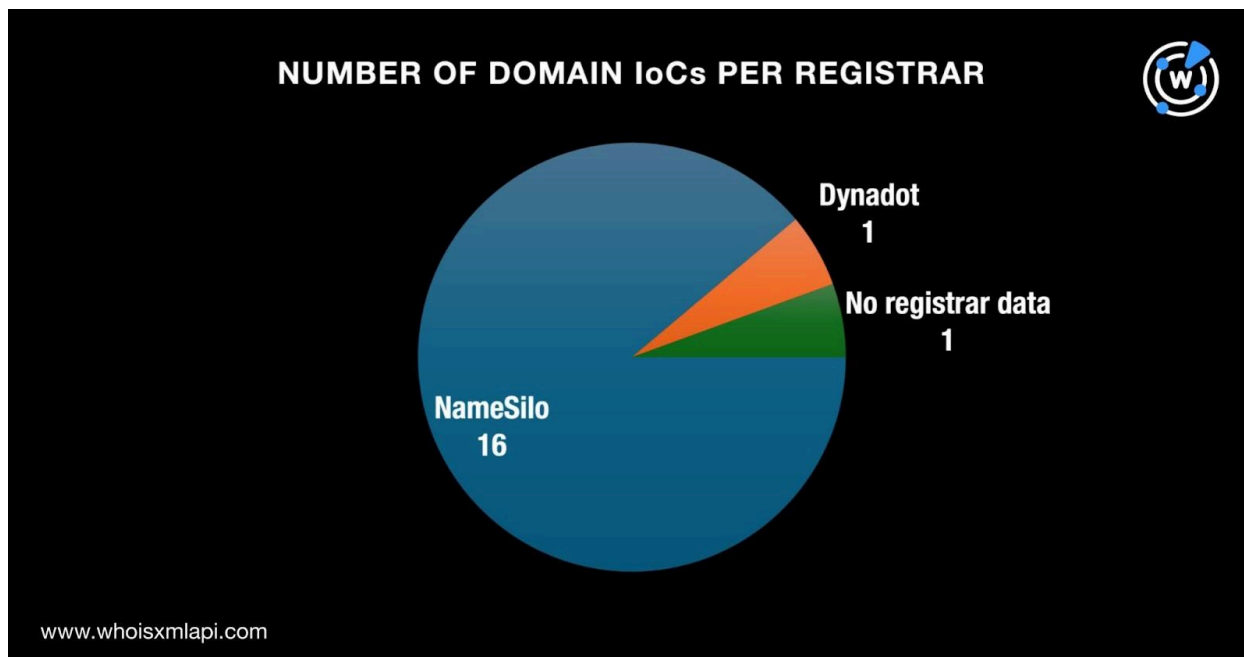
ToxicPanda IoC Facts

As per usual, we began our study by looking for more information about the IoCs.

We queried the 21 domains tagged as IoCs on [Bulk WHOIS Lookup](#), which revealed that only 18 of them had current WHOIS records. The lookup results showed that:



- They were administered by only two registrars. A majority, 16 to be exact, fell under the purview of NameSilo. One was administered by Dynadot, while another did not have registrar data.



- A total of 17 domain IoCs were created in 2024, while one was created way back in 2015.
- While 44% of them were registered in the U.S., the majority, 56% to be exact, did not have registrant country data.

We also queried the 21 domains tagged as IoCs on [DNS Chronicle API](#) and found that they resolved to 122 IP addresses between 8 July 2020 and 27 November 2024. Take a look at five examples below.

DOMAIN IoC	START DATE	END DATE	NUMBER OF IP RESOLUTIONS
cpt[.]lol	7 July 2023	7 August 2024	4
dksu[.]top	16 August 2024	12 September 2024	14
freebasic[.]cn	16 August 2020	27 November 2024	71
mixcom[.]one	21 September 2024	10 November 2024	8
unk[.]lol	14 April 2023	27 April 2024	3



ToxicPanda IoC Expansion Analysis Findings

We kicked off our expansion analysis by querying the 21 domains tagged as IoCs on [WHOIS History API](#), which gave us seven email addresses from their historical WHOIS records. Further scrutiny of the email addresses showed that five of them were public.

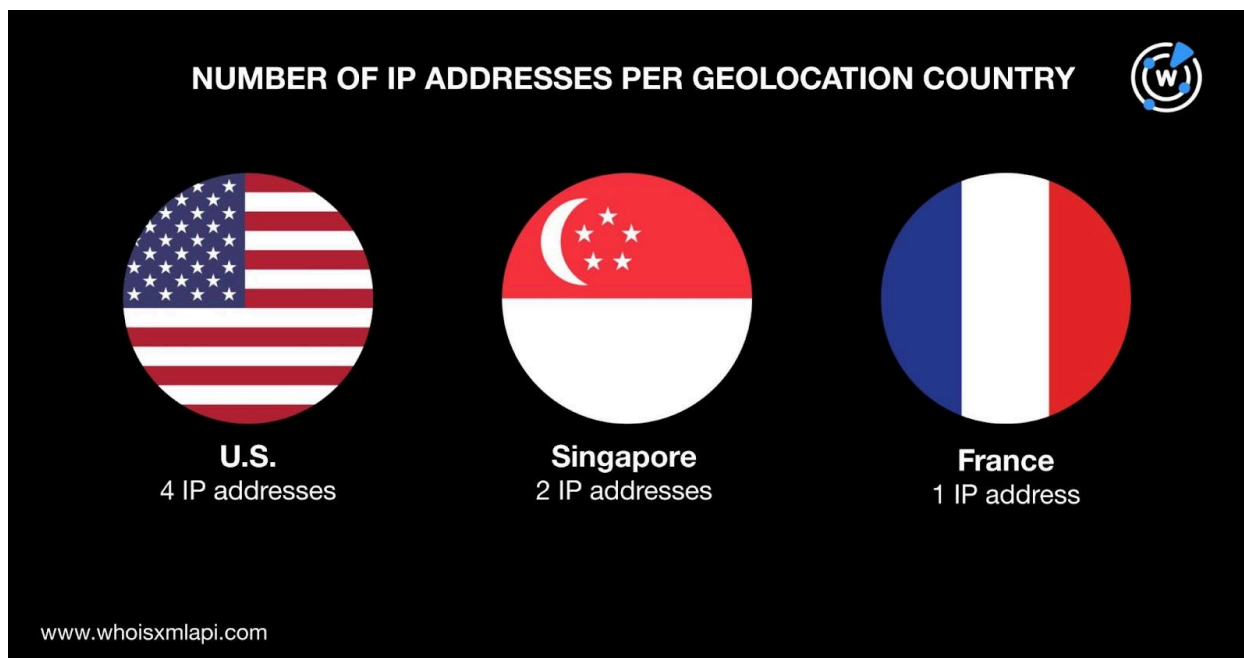
Querying the five public email addresses on [Reverse WHOIS API](#) provided us with six email-connected domains after duplicates and the IoCs were filtered out.

Next up, we queried the 21 domains tagged as IoCs on [DNS Lookup API](#) and found that they resolved to seven unique IP addresses.

[Threat Intelligence API](#) revealed that four of the seven IP addresses were malicious. The IP address 172.[.]67[.]176[.]238, for instance, was associated with phishing, malware distribution, attacks, and generic threats. The IP address 104.[.]21[.]6[.]160, meanwhile, has figured in malware distribution, phishing, and generic threats.

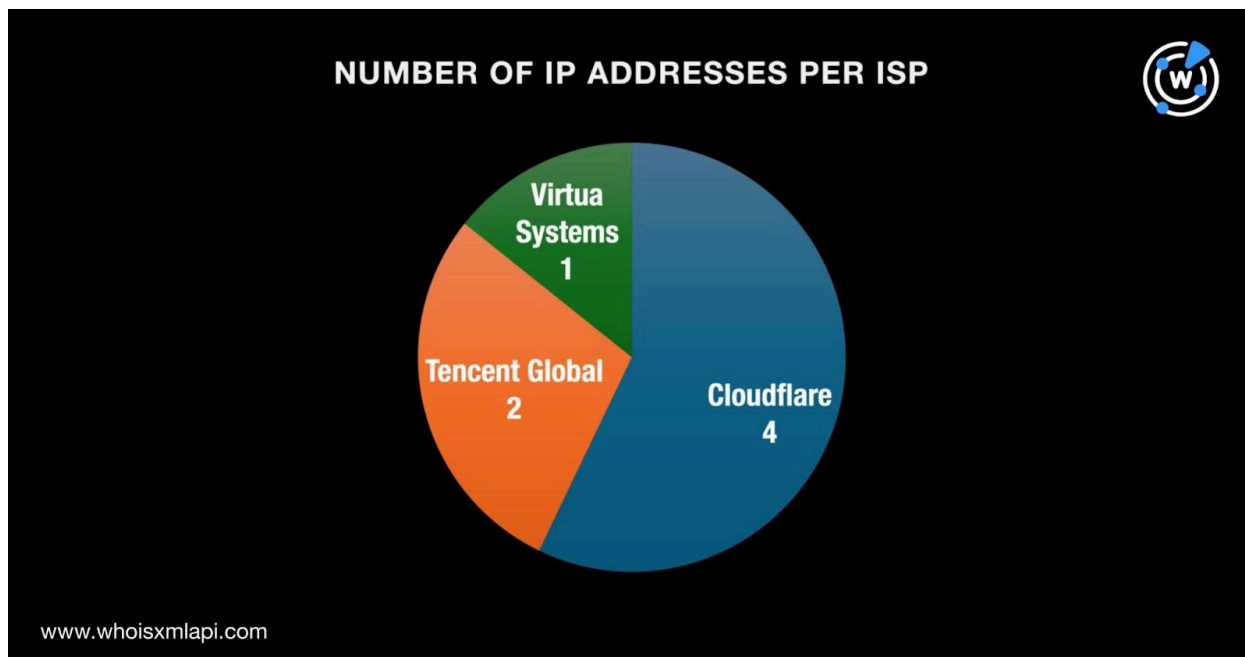
Next, a [bulk IP geolocation lookup](#) for the seven IP addresses showed that:

- They were spread across three geolocation countries led by the U.S., which accounted for four IP addresses. Two IP addresses were geolocated in Singapore, while one originated from France.





- They were also split among three ISPs led by Cloudflare, which accounted for four IP addresses. Tencent Global administered two IP addresses, while Virtua Systems handled one.



After that, we queried the seven IP addresses on [Reverse IP API](#) and found that one of them could be dedicated. It hosted one IP-connected domain after duplicates, the loCs, and the email-connected domains were filtered out.

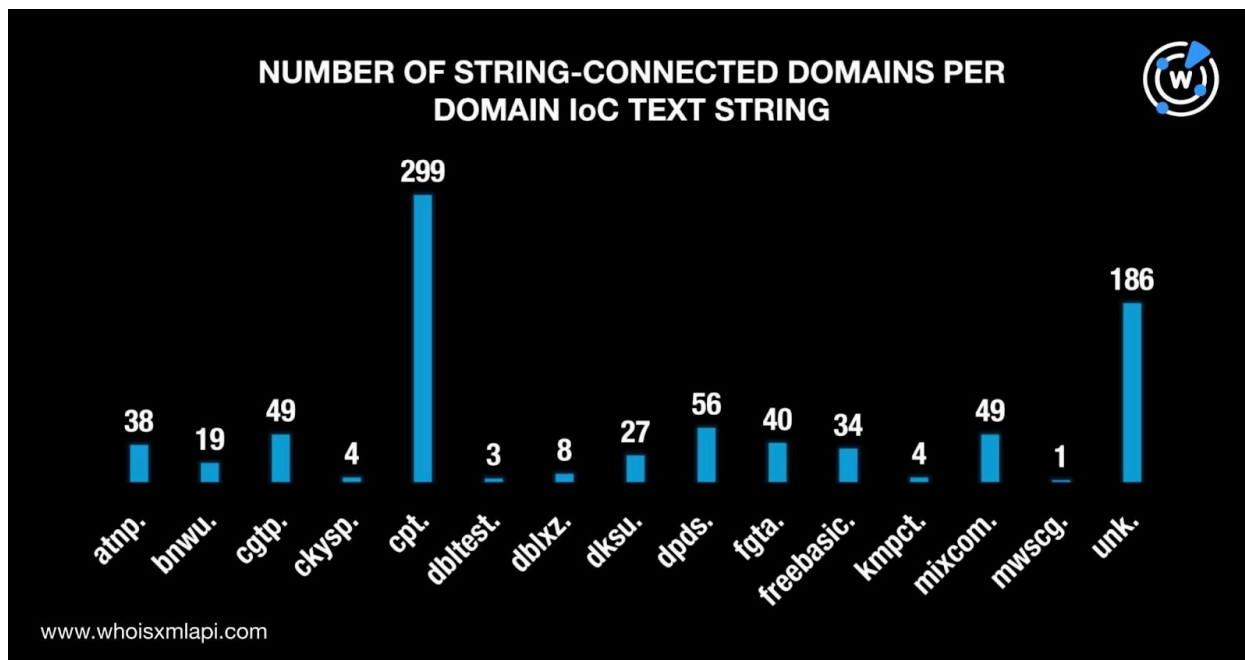
Threat Intelligence API also revealed that the malicious IP-connected domain brwd[.]lol was associated with malware distribution.

Next, we used [Domains & Subdomains Discovery](#) to look for domains that contained text strings found in the domain loCs. We found 817 connected domains that started with these 15 strings:

- atnp.
- bnwu.
- cgtp.
- ckysp.
- cpt.
- dbltest.
- dblxz.
- dksu.
- dpds.
- fgta.
- freebasic.
- kmpct.
- mixcom.
- mwscg.
- unk.



Here is a breakdown of the 817 string-connected domains by text string that appeared in the domains tagged as IoCs.



As our final step, we queried the 824 connected domains (i.e., via email addresses, IP addresses, and text strings) on [Screenshot API](#) and found that 315 of them remained accessible to date.

—

Our in-depth analysis of ToxicPanda’s DNS footprints led to the discovery of 831 new artifacts comprising six email-connected domains, seven IP addresses, one IP-connected domain, and 817 string-connected domains. To date, five of these artifacts—four IP addresses and one connected domain—have already been weaponized for various 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

- 17tv8[.]top
- 17tvmall[.]top
- 17tvos[.]top

Sample IP Addresses

- 104[.]21[.]51[.]68
- 104[.]21[.]6[.]160
- 172[.]67[.]135[.]3
- 172[.]67[.]176[.]238

Sample String-Connected Domains

- atnp[.]aquila[.]it
- atnp[.]be
- atnp[.]belau[.]pw
- atnp[.]best
- atnp[.]bm
- bnwu[.]audnedaln[.]no
- bnwu[.]buzz
- bnwu[.]cc
- bnwu[.]cn
- bnwu[.]co[.]uk
- cgtp[.]bid
- cgtp[.]biz
- cgtp[.]ca
- cgtp[.]cc
- cgtp[.]cl
- ckysp[.]cn
- ckysp[.]com
- ckysp[.]gdn
- ckysp[.]jicu
- cpt[.]ac[.]cn
- cpt[.]ac[.]in
- cpt[.]ac[.]th
- cpt[.]academy
- cpt[.]adv[.]br
- dbltest[.]com
- dbltest[.]store
- dbltest[.]juk
- dblxz[.]cn
- dblxz[.]com
- dblxz[.]icu
- dblxz[.]loan
- dblxz[.]ml
- dksu[.]ca
- dksu[.]cc
- dksu[.]cn
- dksu[.]com
- dksu[.]com[.]cn
- dpds[.]arab
- dpds[.]bid
- dpds[.]biz
- dpds[.]buzz
- dpds[.]club
- fgta[.]ai
- fgta[.]aquila[.]it
- fgta[.]biz
- fgta[.]ca
- fgta[.]cc
- freebasic[.]asia
- freebasic[.]at
- freebasic[.]biz
- freebasic[.]cf
- freebasic[.]ch



- kmpct[.]com
- kmpct[.]org
- kmpct[.]wang
- kmpct[.]webcam
- mixcom[.]academy
- mixcom[.]biz
- mixcom[.]ca
- mixcom[.]cc
- mixcom[.]cf
- mwscg[.]com
- unk[.]academy
- unk[.]adv[.]br
- unk[.]aero
- unk[.]agency
- unk[.]ai