WhoisXMLAPI

A Study of APT Groups Known for Targeting European Countries

Leveraging WHOIS and Passive DNS Data

Dear Reader,

I proudly present the latest APT Group Report, this time looking at targeted individuals and organizations in Europe in 2023 and 2024.

As the volume of APT threats continues to soar, gaining visibility into the groups responsible for attacks and their infrastructure has become more critical than ever.

Feel free to review this report carefully and share the insights with your team.

Let us make the Internet a safer place.

Jonathan Zhang

CEO of WHOIS API, Inc.,
doing business as WhoisXML API

Find me on LinkedIn

Executive Summary

Europe serves as home base for international organizations like the European Union Agency for Law Enforcement Cooperation (Europol), the INTERPOL, and the North Atlantic Treaty Organization (NATO), among others. That makes it one of the regions most targeted by advanced persistent threat (APT) groups.

In this report, the WhoisXML API research team expanded lists of indicators of compromise (IoCs) related to six APT groups that have been targeting countries in Europe either recently or in the past.

1. **The APT Groups at a Glance**
   - Take a look at details about the six APT groups featured in this study.
2. **APT Group Email and DNS Footprints**
   - Discover the ratio of public versus redacted email addresses found in the WHOIS records of the domains tagged as IoCs.
   - Uncover interesting facts about the groups' DNS footprints based on their known IP addresses.
3. **IoC List Expansion**
   - Learn how we expanded the IoC lists using the groups' email and IP address footprints to find connected web properties.
4. **A Closer Look at Each APT Group**
   - Know more about our analyses for the six APT groups leveraging our extensive WHOIS and passive DNS data sources.

Methodology Overview

We began our study by compiling a list of 40 APT groups that we then filtered based on these criteria:

- Groups that launched attacks targeting European countries from 2023 onward
- Groups active in 2023 onward in other regions (e.g., Asia-Pacific, etc.) yet targeted European countries in the past

Using WHOIS History API, we obtained email addresses found in the historical WHOIS records of the domains identified as IoCs. Note that we included the email addresses tagged as IoCs in our final lists of email addresses.

We then separated the public from privacy-protected email addresses. The public email addresses were queried on WhoisXML API services to obtain artifacts, particularly:

- Domains containing the email addresses in their current WHOIS records (via Reverse WHOIS API)
- Domains containing the email addresses in their historical WHOIS records (via DRS Reverse WHOIS Search)

We were left with six APT groups that had email-connected artifacts.

Screenshot API was then used to determine if the connected artifacts remained accessible.

We also looked deeper into the four groups for which IP addresses were named as IoCs using data from Premium DNS Database.

Security Research References

Performing the IoC expansion analyses for the six APT groups featured in this report would not have been possible without the in-depth malware analyses and lists of IoCs we gathered from the following published cybersecurity reports:

- **Palo Alto Networks Unit 42 for APT28:** https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/
- **Sophos for BackdoorDiplomacy:** https://news.sophos.com/en-us/2024/06/05/operation-crimson-palace-sophos-threat-hunting-unveils-multiple-clusters-of-chinese-state-sponsored-activity-targeting-southeast-asia/
- **Zscaler for Kimsuky:** https://www.zscaler.com/blogs/security-research/kimsuky-deploys-translatext-target-south-korean-academia
- **ESET for MoustachedBouncer:** https://www.welivesecurity.com/en/eset-research/moustachedbouncer-espionage-against-foreign-diplomats-in-belarus/
- **Check Point Research for Muddy Water:** https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/
- **Kaspersky for ToddyCat:** https://securelist.com/toddycat-traffic-tunneling-data-extraction-tools/112443/

IoC List Expansion Findings

Domain and DNS Threat Intelligence in Action

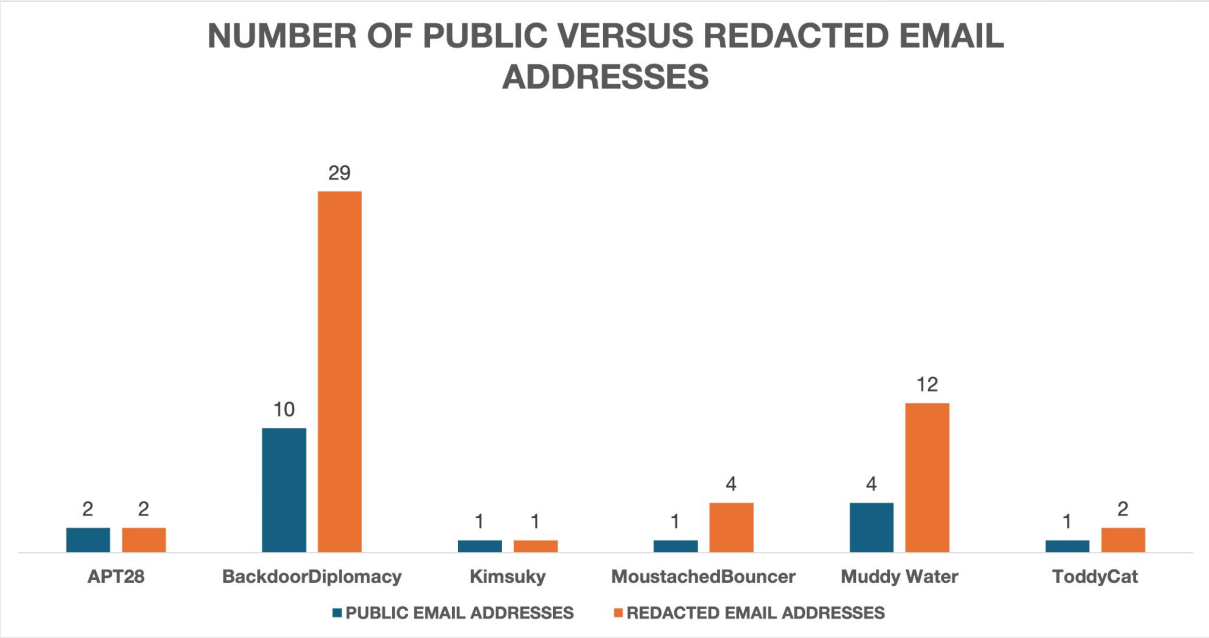
The APT Groups at a Glance

APT Group	Aliases	Based In	Target Countries	Active Since	Number of Domain IoCs in Studied Campaign	Number of Email IoCs in Studied Campaign	Number of IP IoCs in Studied Campaign
APT28	Tsar Team	Russia	Worldwide	2007	2	0	0
BackdoorDiplomacy	NA	China	Southeast Asia but targeted Europe in the past	2017	14	0	38
Kimsuky	Black Banshee, Velvet Chollima, Emerald Sleet, THALLIUM	North Korea	South Korea but targeted Europe in the past	2012	3	0	0
MoustachedBouncer	NA	Belarus	Belarus	2014	5	4	10
Muddy Water	Earth Vetala, MERCURY, Static Kitten, Seedworm, TEMP.Zagros, Mango Sandstorm, TA450	Iran	Saudi Arabia, Turkey, Azerbaijan, India, Portugal	2017	7	0	17
ToddyCat	NA	China	Asia-Pacific but targeted Europe in the past	2020	3	0	3
							106 IoCs in total

APT Group Email Footprints

Despite the now-widespread practice of redacting domain ownership data, especially in Europe, we were still able to look into the digital footprints of the six APT groups aided by their associated domains' historical WHOIS records.

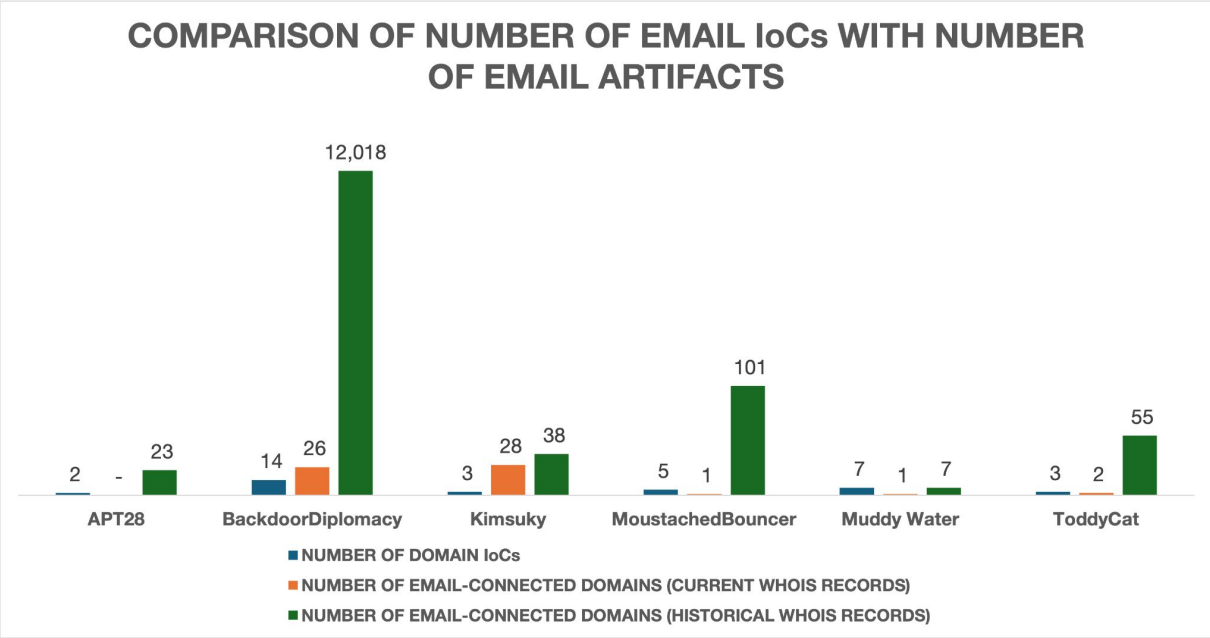
In the featured groups' case, 28% of the email addresses from historical WHOIS records and those named as IoCs were public. Several were provided by free email service providers like Google, Yahoo!, QQ, and others.



IoC List Expansion: From 38 Email IoCs to 12.2K+ Artifacts

The WhoisXML API researchers pivoted off the email footprints of the six APT groups and uncovered 12,242 email-connected domains that can be considered potential threat artifacts.

IoC List Expansion: ~321x Increase from IoCs to Artifacts



From 34 domains and four email addresses identified as IoCs, our investigation led to 58 connected domains using current WHOIS record data, translating to 1.53 times the number of IoCs.

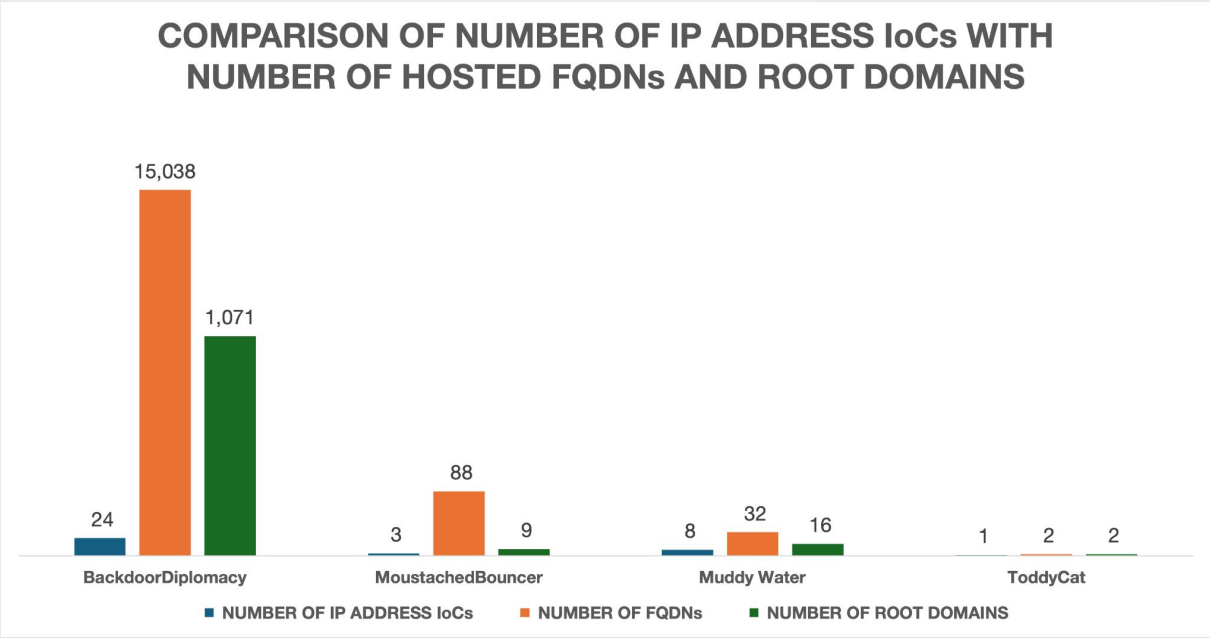
The ratio ballooned to 360.06 times the number of IoCs when we looked at the domain IoCs' historical WHOIS records. From 38 domain and email IoCs, we found 12,242 connected artifacts.

All in all, we recorded a 32115.8% expansion from the number of IoCs to the number of artifacts.

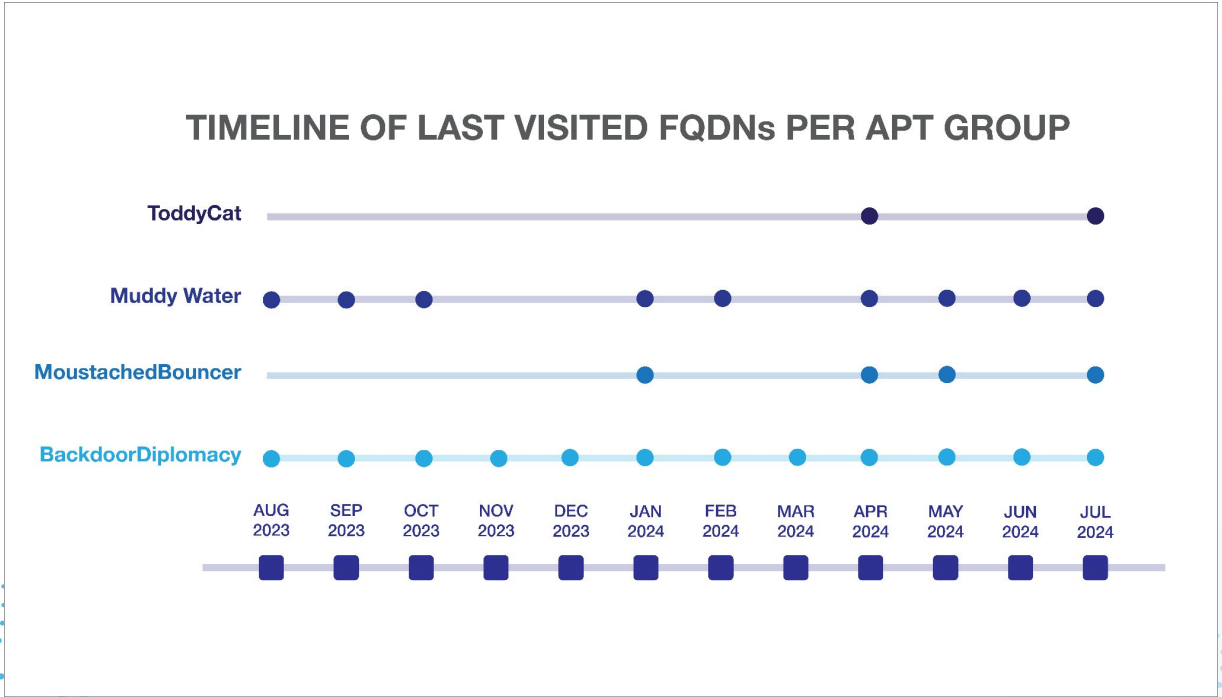
APT Group DNS Footprints

Exhaustive passive DNS databases can provide deeper insights into the inner workings of APT groups.

For this study, 36 IP addresses have been identified as IoCs for four of the six featured groups—BackdoorDiplomacy, MoustachedBouncer, Muddy Water, and ToddyCat. Altogether, they hosted 15,160 fully qualified domain names (FQDNs) under 1,098 root domains.



IoC List Expansion: Timeline of FQDN Last Visit Dates



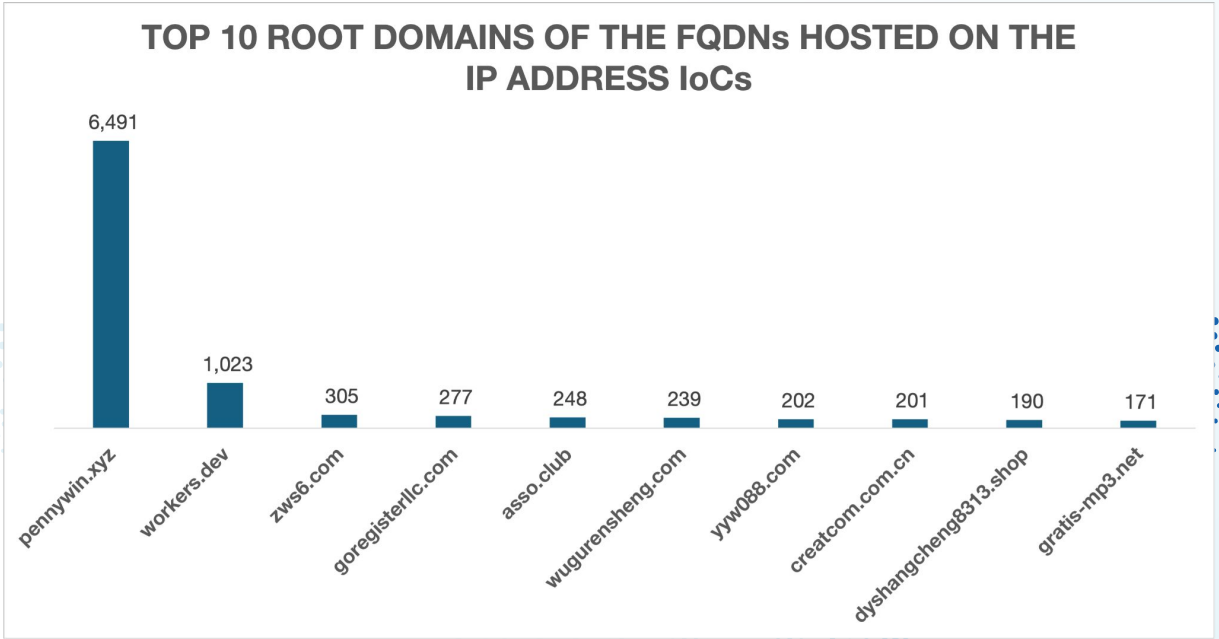
Our analysis of the Premium DNS Database results identifying the FQDNs hosted on the IP addresses identified as IoCs for the four APT groups revealed when they were last visited.

The BackdoorDiplomacy and Muddy Water IP IoCs, for instance, were last visited between August 2023 and July 2024. Those for MoustachedBouncer, meanwhile, were last visited from January to July 2024. Finally, the ToddyCat IoCs were last visited between April and July 2024.

IoC List Expansion: Top 10 Root Domains

After extracting the root domains of the FQDNs, we identified the top 10 root domains.

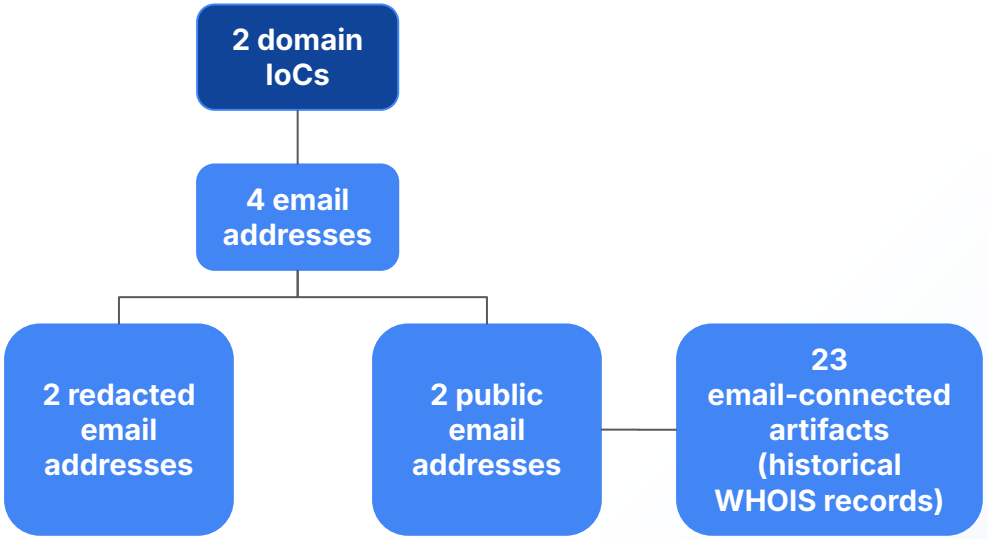
Pennywin[.]xyz, a sweepstakes website, led the pack. Workers[.]dev, a serverless code deployment service site, took the second spot. Zws6[.]com, goregisterllc[.]com, asso[.]club, wugurensheng[.]com, yyw088[.]com, creatcom[.]com[.]cn, dyshangcheng8313[.]shop, and gratis-mp3[.]net completed the top 10.

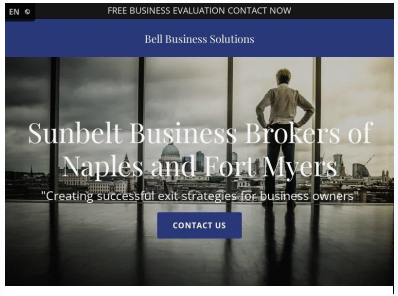


A Closer Look at Each APT Group

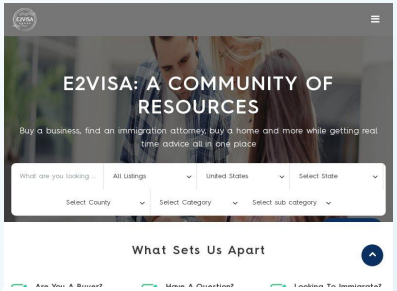
APT28

APT28, an APT group believed to be based in Russia, has been active since at least 2007. It most recently targeted diplomats the world over using the HeadLace backdoor likely since March 2024.





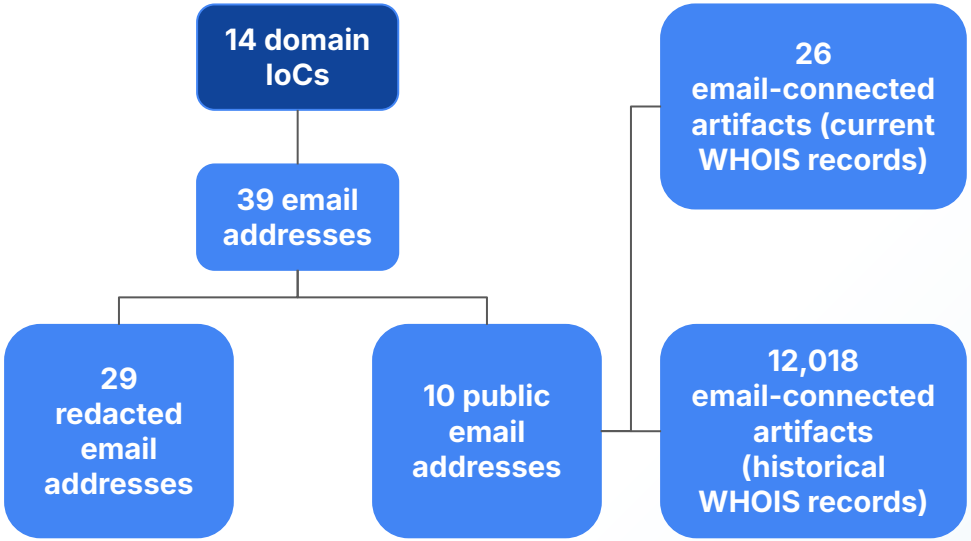
buyfloridabusinesses[.]com



e2visa[.]com

BackdoorDiplomacy

BackdoorDiplomacy, presumably based in China, has been active since at least 2017. It most recently targeted Southeast Asian governments using an upgraded version of the EAGERBEE malware. In the past, however, it also went after foreign affairs ministries and telecommunications companies in Europe, Africa, the Middle East, and Asia.



atomicwave[.]net

vietnamvisaonarrival[.]info

BackdoorDiplomacy

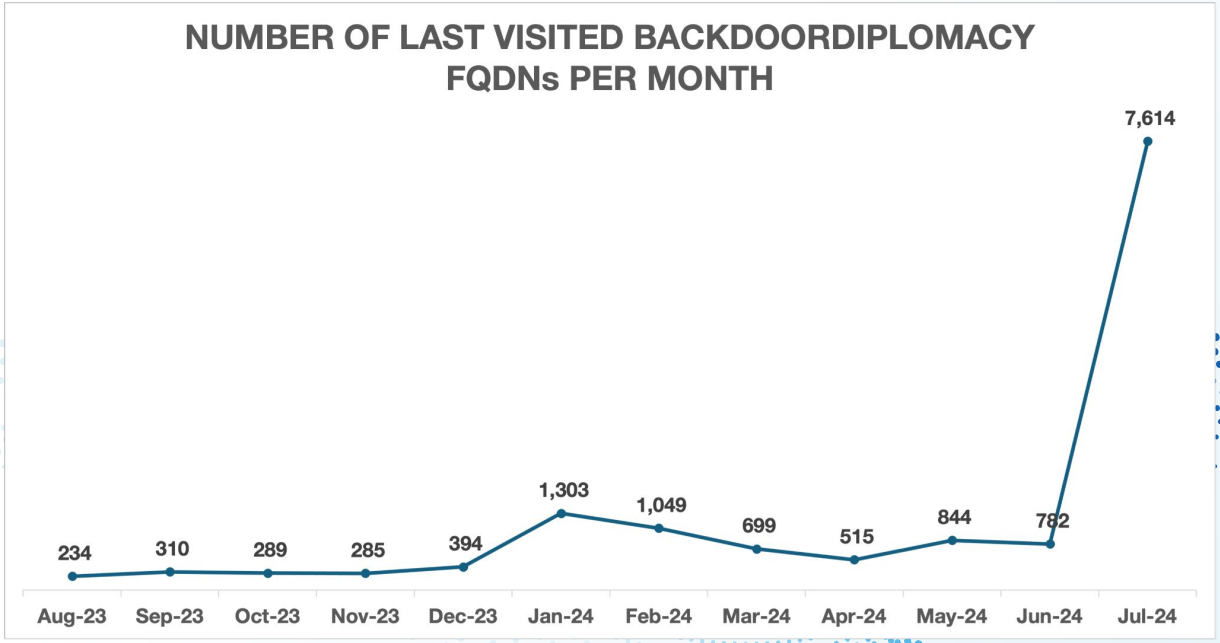
Researchers also identified 38 IP addresses as IoCs.

38 IP IoCs

1,071 root domains

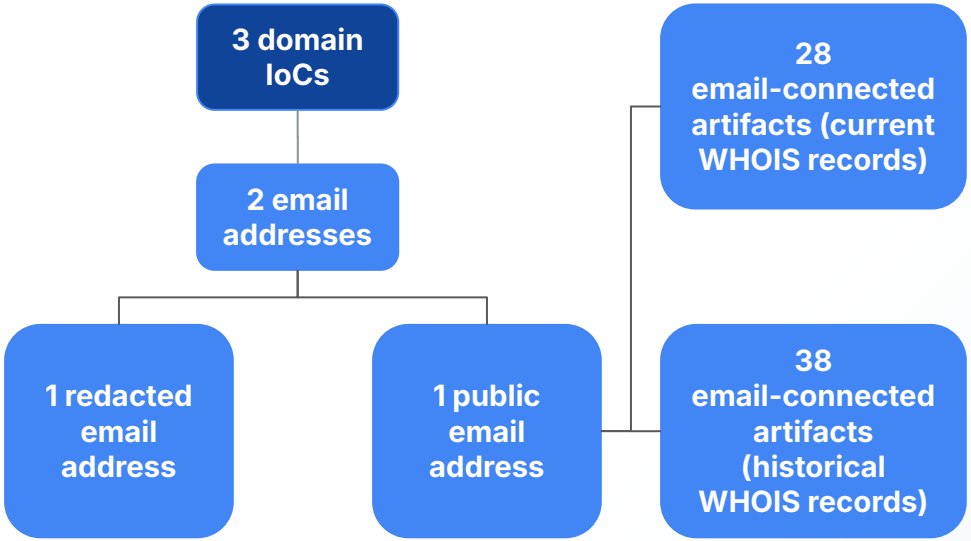
14,318 FQDNs

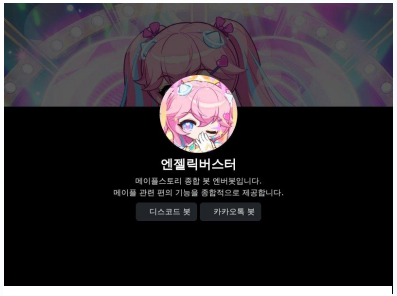
August 2023 to July 2024



Kimsuky

Kimsuky, believed to hail from North Korea, has been active since at least 2012. It most recently targeted members of the academe in South Korea using malicious Google Chrome extensions. In the past, though, it also trailed its sights on think tanks and individuals identified as experts in various fields in Europe, the U.S., Russia, and other UN member states.



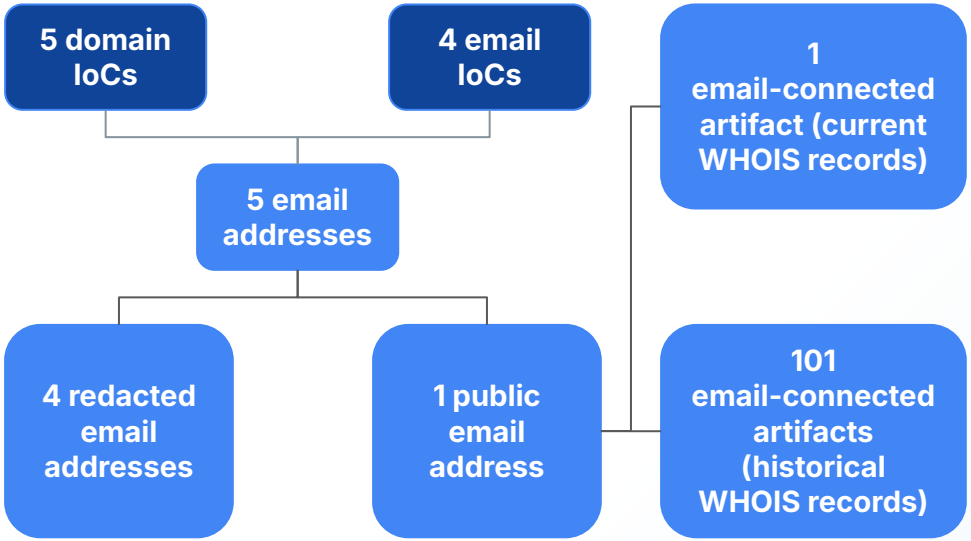


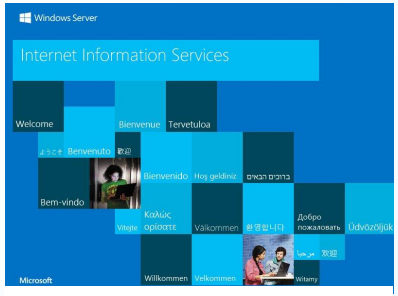
angelic[.]kr

maplehistory[.]kr

MoustachedBouncer

MoustachedBouncer, presumably originating from Belarus, has been active since at least 2014. It most recently targeted foreign diplomats based in Belarus using email-based command-and-control (C&C) protocols, C++ modular backdoors, and adversary-in-the-middle (AitM) attacks.





bizonyou[.]com

sleazebrigade[.]com

MoustachedBouncer

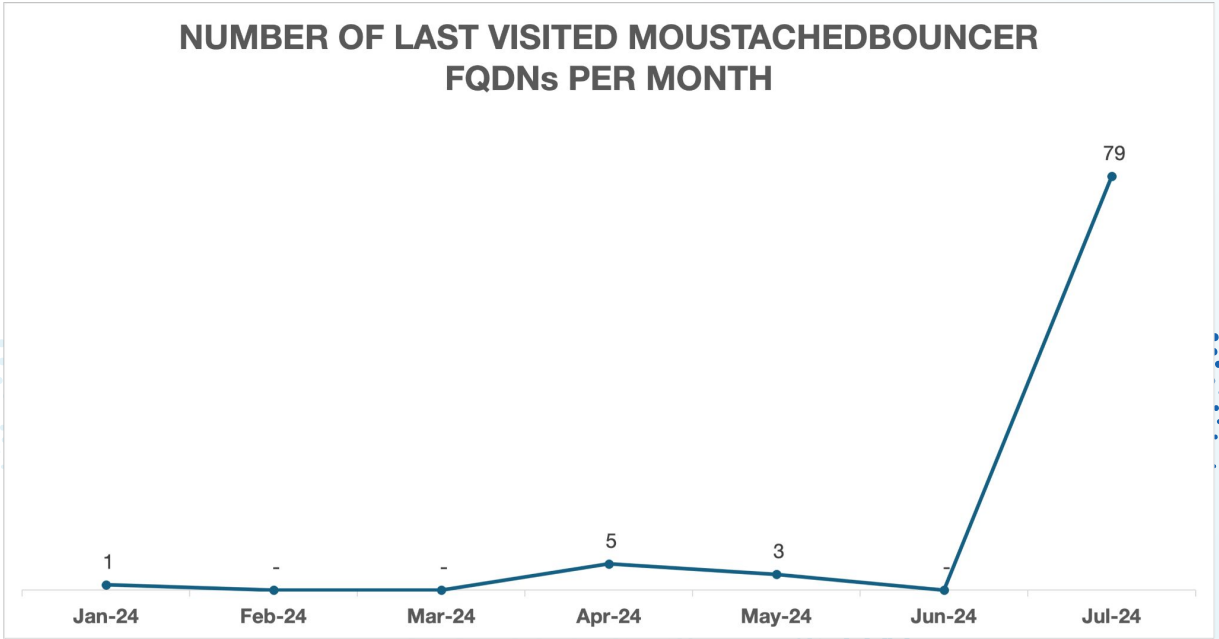
Researchers also identified 10 IP addresses as IoCs.

10
IP IoCs

9
root domains

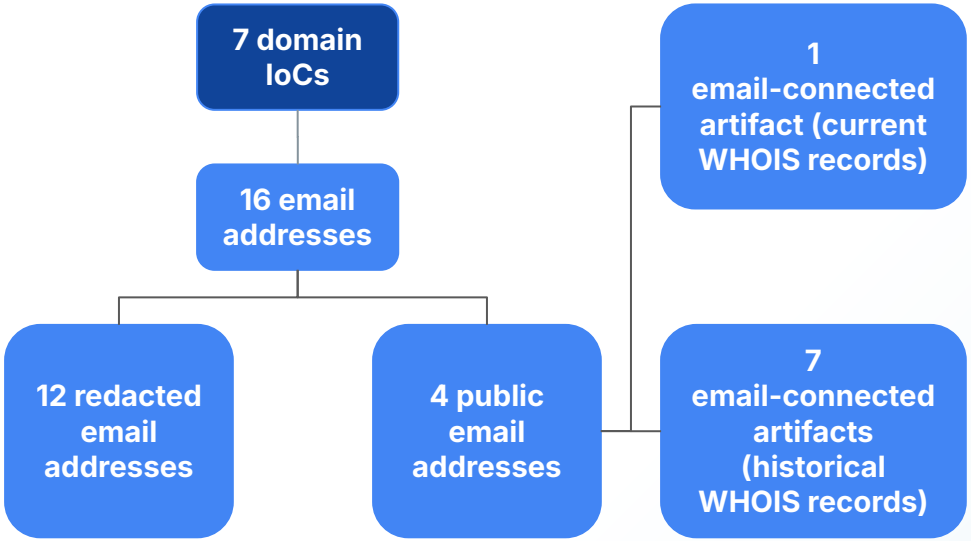
88
FQDNs

January to July 2024

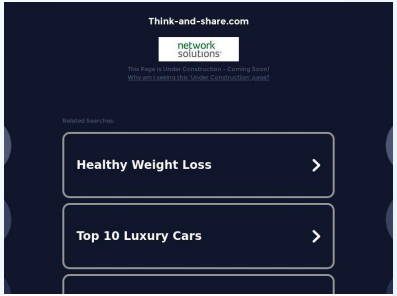


Muddy Water

Muddy Water, believed to be based in Iran, has been active since at least 2017. It most recently launched a widespread phishing campaign targeting organizations in Portugal, Saudi Arabia, Turkey, Azerbaijan, and India aided by the BugSleep backdoor.



predictivefss[.]com



think-and-share[.]com

Muddy Water

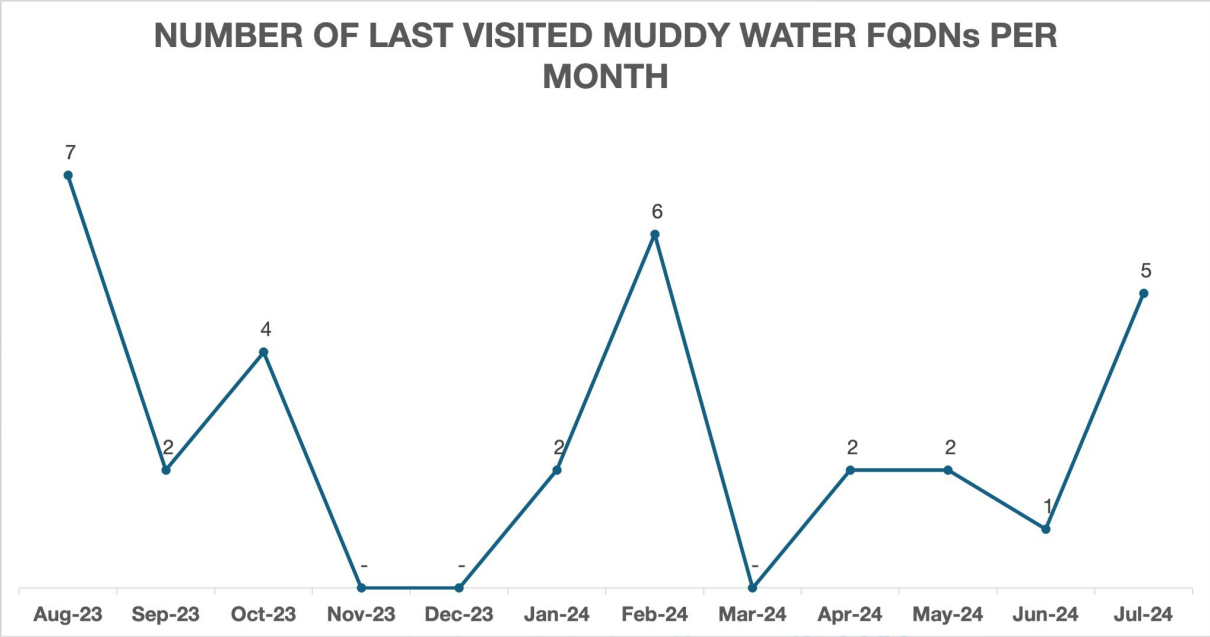
Researchers also identified 17 IP addresses as Muddy Water IoCs.

17 IP IoCs

16 root domains

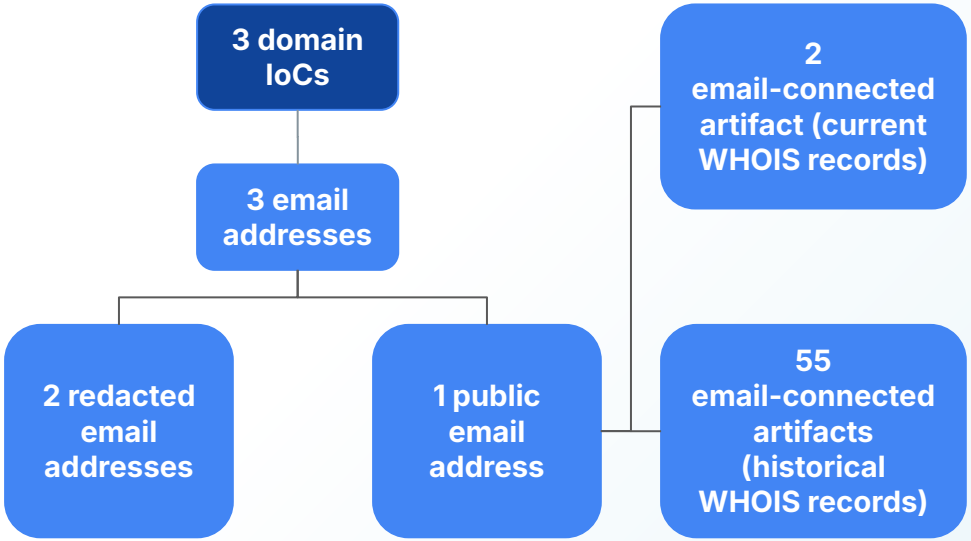
31 FQDNs

August 2023 to July 2024



ToddyCat

ToddyCat, presumably based in China, has been active since at least 2020. While it most recently targeted organizations in Asia-Pacific, it has also trailed its sights on government and military targets across Europe and Asia in the past.



ToddyCat

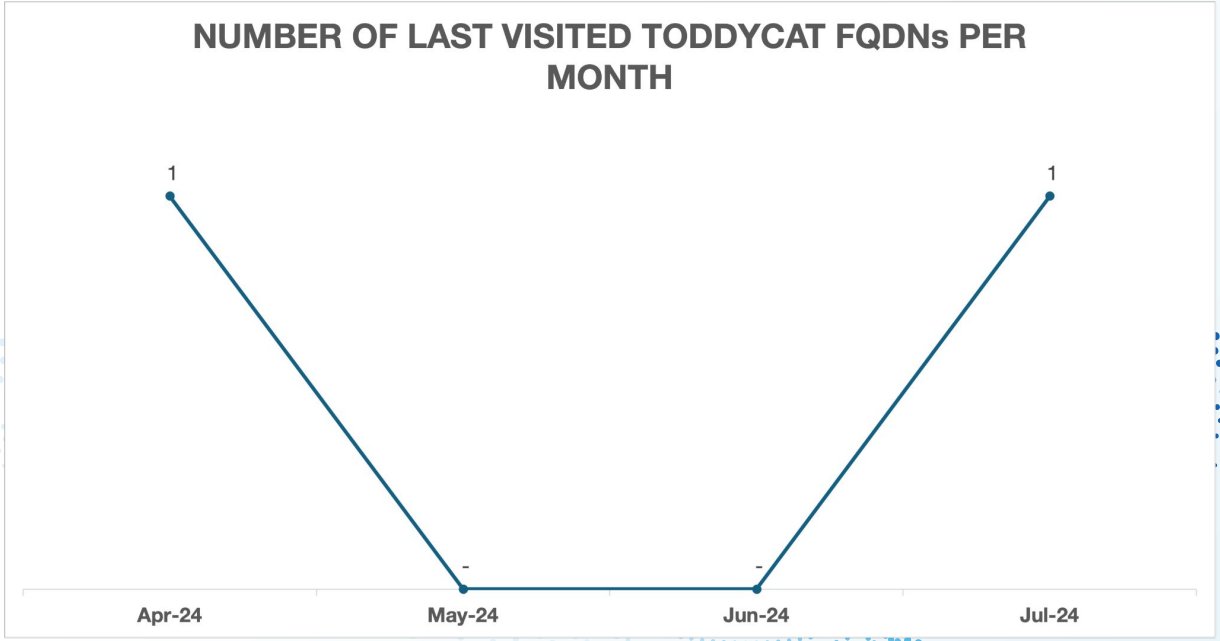
Researchers also identified 3 IP addresses as ToddyCat IoCs.

3
IP IoCs

2
root domains

2
FQDNs

April to July 2024



Wrap-Up

Wrap-Up

Domain ownership and passive DNS records contain clues that provide more information about APT groups or, at least, their connected domain portfolios. This analysis highlighted associations through the current and historical WHOIS records of the domains identified as IoCs for the six APT groups we investigated. It also revealed DNS connections for four of the groups with IP address IoCs.

To recall, our analysis began with 34 domain, four email address, and 68 IP address IoCs that allowed us to uncover:

- Artifacts comprising 1.53 times the number of IoCs based on current WHOIS record data
- Historically connected artifacts totaling 360.06 times the number of IoCs
- 2,541 email-connected artifacts that remain active as of this writing
- 15,160 FQDNs hosted on the 36 IP addresses identified as IoCs for BackdoorDiplomacy, MoustachedBouncer, Muddy Water, and ToddyCat under 1,098 root domains

About WhoisXML API

WhoisXML API empowers all types of cybersecurity enterprises, including MSSPs, SOCs, Fortune 1000 organizations, government agencies, and SMBs with digital footprints. We relentlessly collect, process, and deliver the most comprehensive and readily available domain, IP, and DNS intelligence there is on the market.

To explore how our data can fortify your digital presence, visit our website or contact our sales team.

50 billion+
domains and subdomains

21 billion+
historical WHOIS records

116 billion+
DNS records

14+
years of data crawling

Contact sales@whoisxmlapi.com
for more information.