WhoisXMLAPI

2023 IoC List Expansion for APAC-Based/Targeting APT Groups

Leveraging Current and Historical WHOIS Data

Table of Contents

Executive Summary

Advanced persistent threat (APT) groups are among the most methodical and well-resourced threat actors, making them dangerous. The increasing number of activities involving them warrant the utmost security strategies from organizations, especially since the APT protection market is forecast to reach a value of US$15.16 billion by 2026, indicating a massive 677% increase over a 10-year period.

The WhoisXML API research team expanded lists of indicators of compromise (IoCs) related to six APAC-based/targeting APT groups that have been active in 2023.

1. The APT Groups at a Glance

- Take a quick look at some of the details about the six APT groups featured in this study.

2. Email WHOIS Footprints of the APT Groups

- Discover the ratio of public versus redacted email addresses found in the WHOIS records of the domains tagged as IoCs.

3. IoC List Expansion

- Learn how we expanded the IoC lists using the APT groups' email WHOIS footprints to find connected domains.

4. A Closer Look at Each APT Group

- This section details the IoC list expansion analyses for the six APT groups, including some website screenshots we obtained from still-accessible domain artifacts.

Methodology Overview

We began our study by compiling a list of 34 APT groups that we then filtered based on these criteria:

- Groups that launched attacks in 2023
- Groups based in/targeting APAC countries

We were left with 12 APT groups for which we gathered IoC lists.

Using WHOIS History API, we obtained email addresses found in the historical WHOIS records of the domains identified as IoCs for six of the APT groups.

We then separated the public from privacy-protected email addresses and ran the public ones on Reverse WHOIS API and the Domain Research Suite (DRS) Reverse WHOIS Search 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)

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

IoC List Expansion Findings

Domain Threat Intelligence in Action

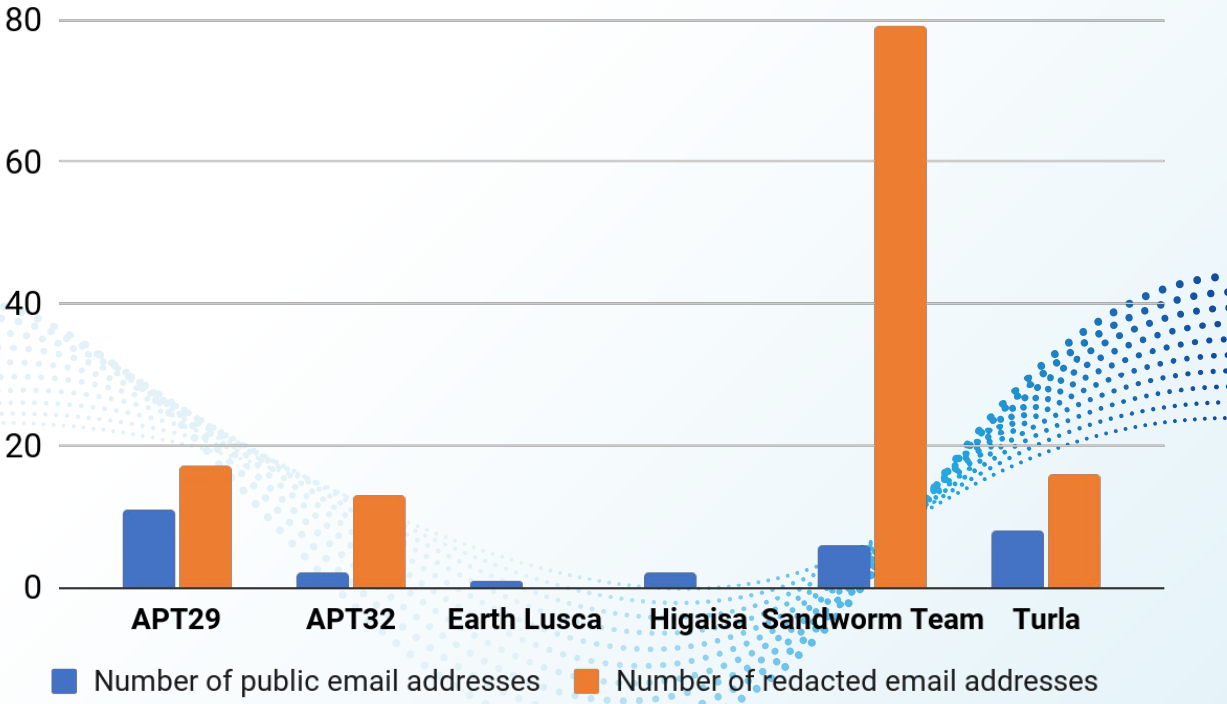
The APT Groups at a Glance

APT Group	Aliases	Based In	Target Countries	Active Since	Number of Domain IoCs Involved in the Most Recent Campaign
APT29	IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, SolarStorm, Blue Kitsune	Russia	U.S.	2008	11
APT32	SeaLotus, OceanLotus, APT-C-00	Vietnam	Southeast Asian countries	2014	5
Earth Lusca	TAG-22	China	Australia	2019	2
Higaisa	None	South Korea	North Korea	2009	1
Sandworm Team	Electrum, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM	Russia	Ukraine	2009	13
Turla	Iron Hunter, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear	Russia	45 countries	2004	12
					44 IoCs in total

Email WHOIS Footprints of the APT Groups

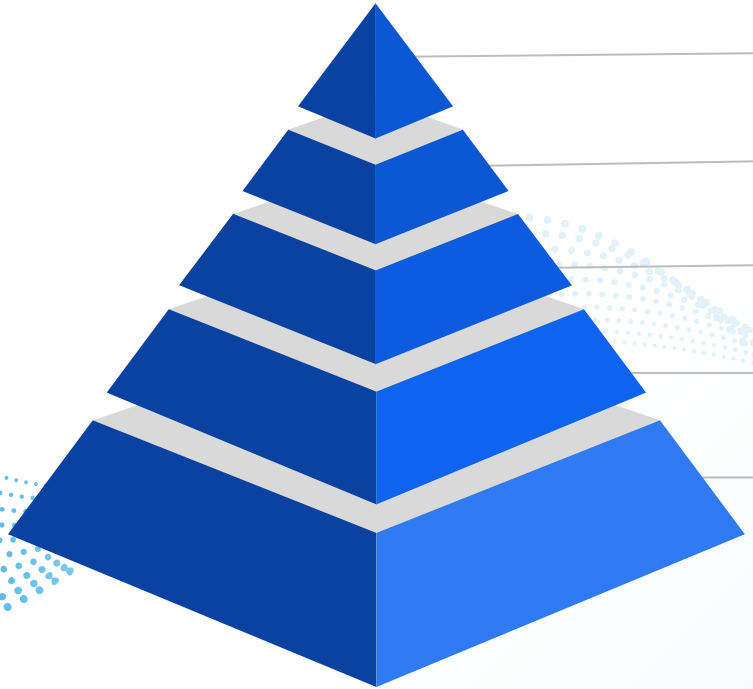
Amid WHOIS data redaction, threat actors continue to leave digital breadcrumbs in historical WHOIS records.

In the case of the six APT groups we studied, around 19% of the email addresses found in the historical WHOIS records of the domain IoCs were public email addresses provided by Gmail, Yahoo!, Hotmail, and other popular email service providers.



IoC List Expansion: From Dozens to Hundreds of Domains

The WhoisXML API researchers pivoted off the email WHOIS footprints the APT groups left behind, leading us to uncover more than 350 email-connected domains that can be considered potential threat artifacts.



44 **Domains tagged as IoCs for the recent activities of the six APT groups**

155 **Email addresses found in the domain IOCs' historical WHOIS records**

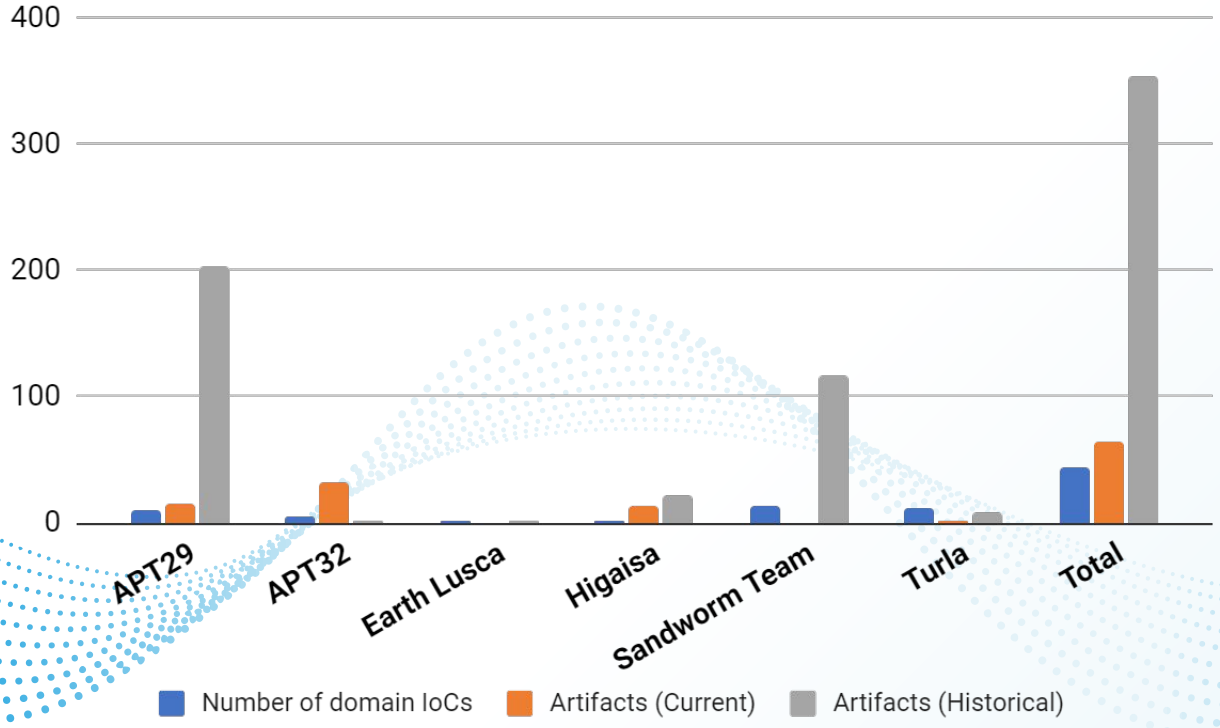
30 **Public email addresses**

64 **Domains containing the IoCs' email addresses in their current WHOIS records**

353 **Domains containing the IoCs' email addresses in their historical WHOIS records**

Excluding 9,998 domains possibly belonging to a domainer

IoC List Expansion: ~700% Increase from IoC to Artifact Volume



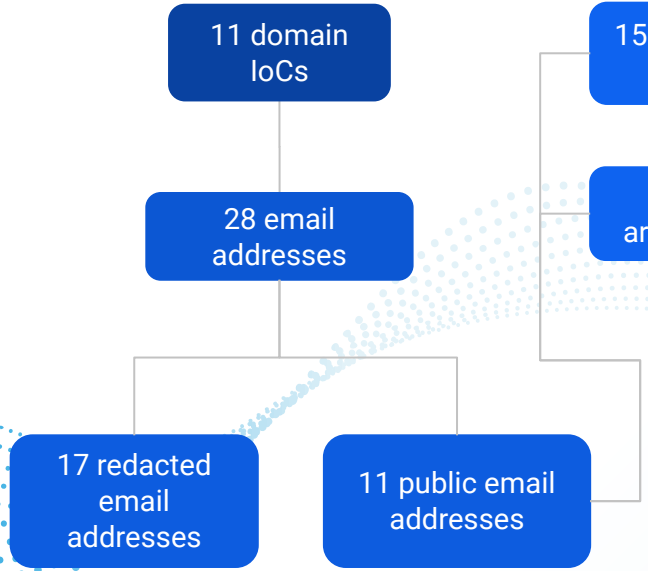
From a total of 44 domains tagged as IoCs, the investigation found 64 connected domains based on their current WHOIS records, which translated to 1.46 times the number of IoCs.

This ratio ballooned to 8 times the number of IoCs when we looked at the IoCs' historical WHOIS records. From 44 domain IoCs, we found 353 artifacts.

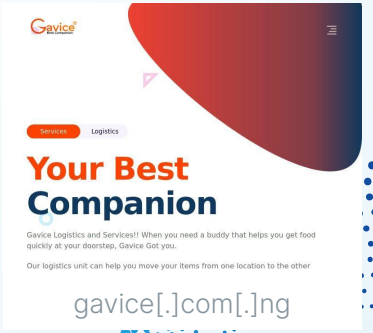
A Closer Look at Each APT Group

APT29

APT29, a cyber espionage group linked to Russia's Foreign Intelligence Service (SVR), has been active since at least 2008. The group has a history of targeting government networks in Europe and NATO member countries, as well as research institutes and think tanks. In a notable operation, APT29 is believed to have compromised the Democratic National Committee (DNC) starting in the summer of 2015. The group reportedly targeted organizations in Ukraine in the first half of 2023.



revistaevolution[.]com[.]br

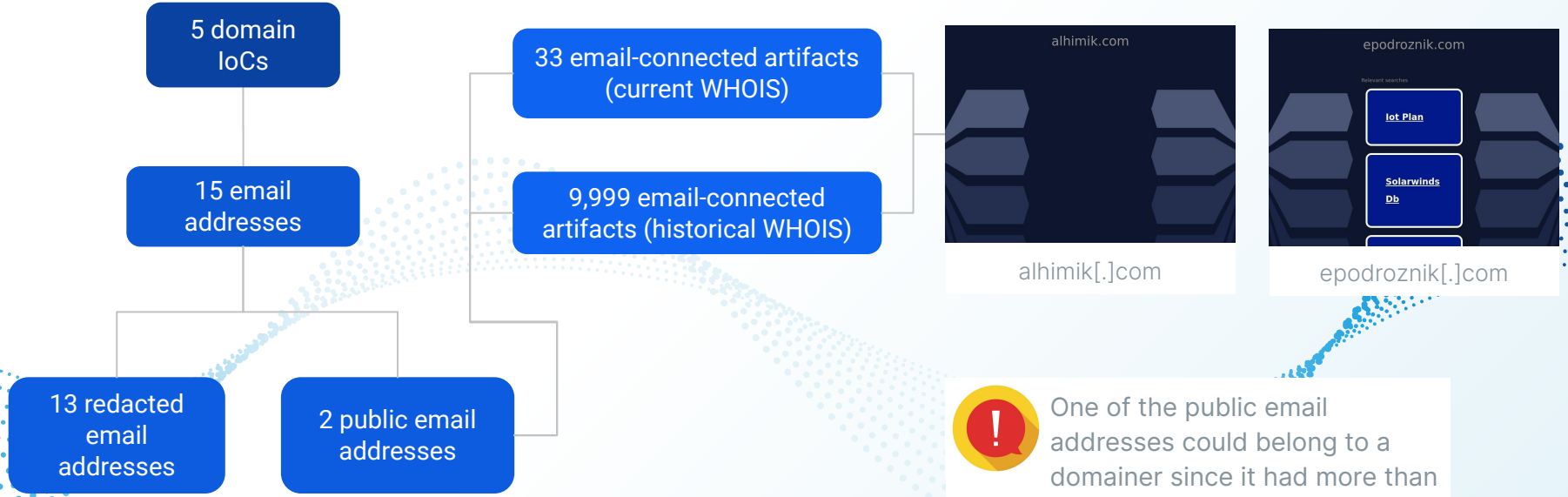


gavice[.]com[.]ng

fbh[.]com[.]br

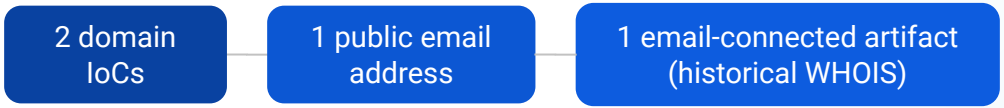
APT32

APT32 is presumed to be based in Vietnam and has been active since 2014. The group's targets have spanned multiple private sector companies, foreign governments, dissidents, and journalists primarily based in Southeast Asian nations like Vietnam, the Philippines, Lao PDR, and Cambodia. In June 2023, APT32 was suspected to have used SPECTRALVIPER to attack a Vietnamese agribusiness.



Earth Lusca

Earth Lusca is a suspected China-based cyber espionage group that has been active since April 2019. It has targeted government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, and cryptocurrency trading platforms in various countries. Security researchers believe that some Earth Lusca operations may be financially motivated. In the first half of 2023, the group was observed targeting government organizations in Southeast Asia, Central Asia, the Balkans, Latin America, and Africa through a Linux backdoor.

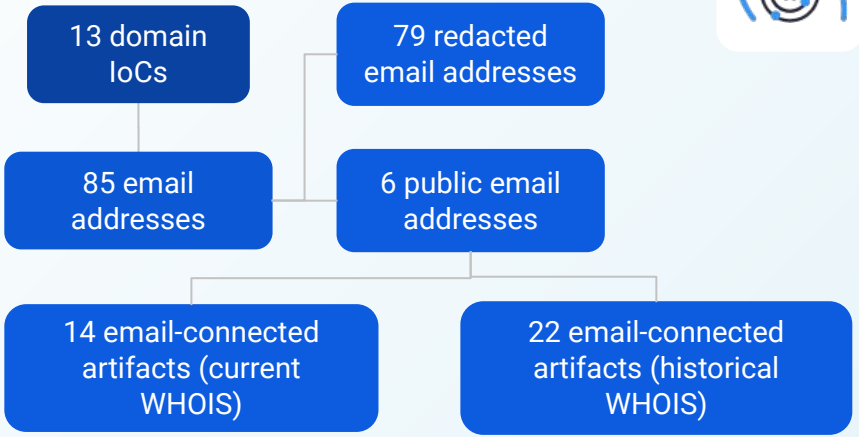


Higaisa

Higaisa is believed to have taken root in South Korea. The group has primarily targeted government, public, and trade organizations in North Korea, but their operations have also extended to China, Japan, Russia, Poland, and other countries. Higaisa first came to light in early 2019, but its activities are suspected to date back as early as 2009. A phishing campaign targeting Chinese Internet users in October 2023 was attributed to the group.

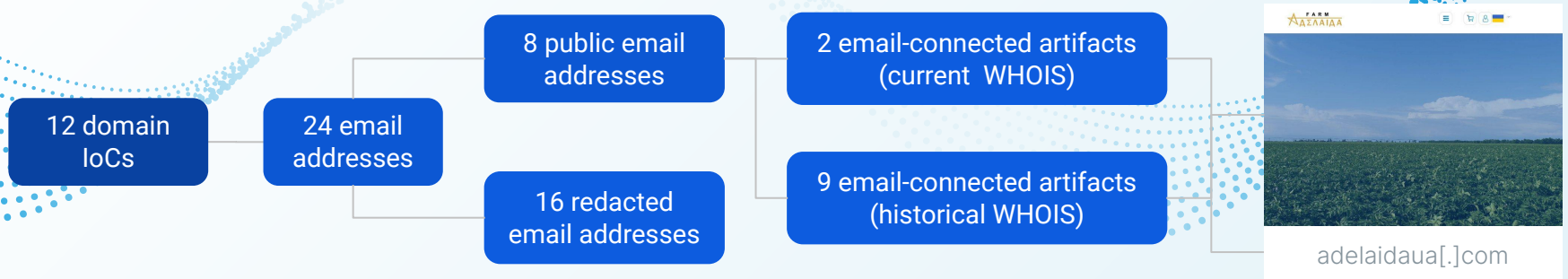
Sandworm Team

Sandworm Team is a cyber warfare group linked to the Main Center for Special Technologies (GTsST) of the Russian General Staff Main Intelligence Directorate (GRU). The group has been active since at least 2009. It is known for destructive cyber attacks, including the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide NotPetya attack, and the 2018 Olympic Destroyer attack related to the Winter Olympic Games. The group targeted Ukraine in April 2023.



Turla

Turla is a Russian-based threat group notorious for its sophisticated cyber espionage operations. Since its inception in 2004, Turla has stealthily infiltrated the networks of government entities, embassies, military organizations, educational institutions, research centers, and pharmaceutical companies spanning more than 45 countries. The group was seen targeting Ukraine in July 2023.



Wrap-Up

Tracking APT Groups

Domain ownership records contain clues that provide more information on APT groups or, at least, their possible domain portfolios. This study showed connections through the historical WHOIS records of the domains tagged as IoCs for the six APT groups we investigated.

To recall, our analysis began with 44 IoC domains whose historical WHOIS details led us to:

- Artifacts comprising 1.46 times the number of IoCs based on current WHOIS records
- Historically connected artifacts making up 8 times the number of IoCs
- Several email-connected artifacts that remain active

Conclusion

APT groups remain elusive, potentially because they are often backed by powerful and resourceful entities. However, this should not discourage the cybersecurity community from relentlessly tracking and preventing them from wreaking havoc on nations, critical infrastructures, and organizations across industries.

This research shows that several cyber intelligence sources can help provide more insights into APT-related activities. Current and historical WHOIS data has the potential to help organizations better understand the malicious domain networks operated by APT groups and other cyber attackers.

Get in touch with us to access the data featured in this report and discuss collaboration opportunities.

WhoisXMLAPI

The Who Behind Domain, IP & Cyber Threat Intelligence

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.

4.2 billion+
domains and subdomains

16.7 billion+
historical WHOIS records

Billions
DNS records

12+
years of data crawling


WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence