WhoisXMLAPI

A Study of APT Groups Known for Targeting North American Countries

Leveraging Current and Historical WHOIS Data

Table of Contents

Executive Summary

North America (NA) has long been one of the regions most targeted by advanced persistent threat (APT) groups.

In September 2023, the region was named the top APT target. The government, technology, healthcare, telecommunications, and education sectors were also found as the most affected industries.

In this report, the WhoisXML API research team expanded lists of indicators of compromise (IoCs) related to seven APT groups that have been targeting NA.

1. **The APT Groups at a Glance**
   - Take a look at details about the seven APT groups featured in this study.
2. **APT Group Email Footprints**
   - 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 footprints to find connected domains.
4. **A Closer Look at Each APT Group**
   - Know more about our analyses for the seven APT groups, including some website screenshots of still-accessible domain artifacts.

Methodology Overview

We began our study by compiling a list of 41 APT groups that we then filtered based on these criteria:

- Groups that launched attacks on NA targets in 2023 onward
- Groups that were active in 2023 onward in other regions yet targeted NA in the past

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

We then separated the public from privacy-protected email addresses and ran the public ones through WhoisXML API capabilities 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 seven APT groups that had email-connected artifacts.

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

Security Research References

Performing the expansion analyses for the seven 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 research:

- **Mandiant for APT33:** https://www.mandiant.com/resources/blog/apt33-insights-into-iranian-cyber-espionage
- **Lookout for APT41:** https://www.lookout.com/threat-intelligence/article/wyrmspy-dragonegg-surveillanceware-apt41
- **Cyware for FIN7:** https://cyware.com/resources/research-and-analysis/the-evolution-and-exploits-of-fin7-from-pos-malware-to-ransomware-dominance-0623
- **ASEC for Kimsuky:** https://asec.ahnlab.com/en/59590/
- **Proofpoint for Molerats:** https://www.proofpoint.com/uk/blog/threat-insight/ta402-uses-complex-ironwind-infection-chains-target-middle-east-based-government
- **Trend Micro for Turla:** https://www.trendmicro.com/en_us/research/23/i/examining-the-activities-of-the-turla-group.html
- **Kaspersky for ZIRCONIUM:** https://www.kaspersky.com/about/press-releases/2023_kaspersky-reports-attacks-on-industrial-sector-utilizing-cloud-infrastructure

IoC List Expansion Findings

Domain Threat Intelligence in Action

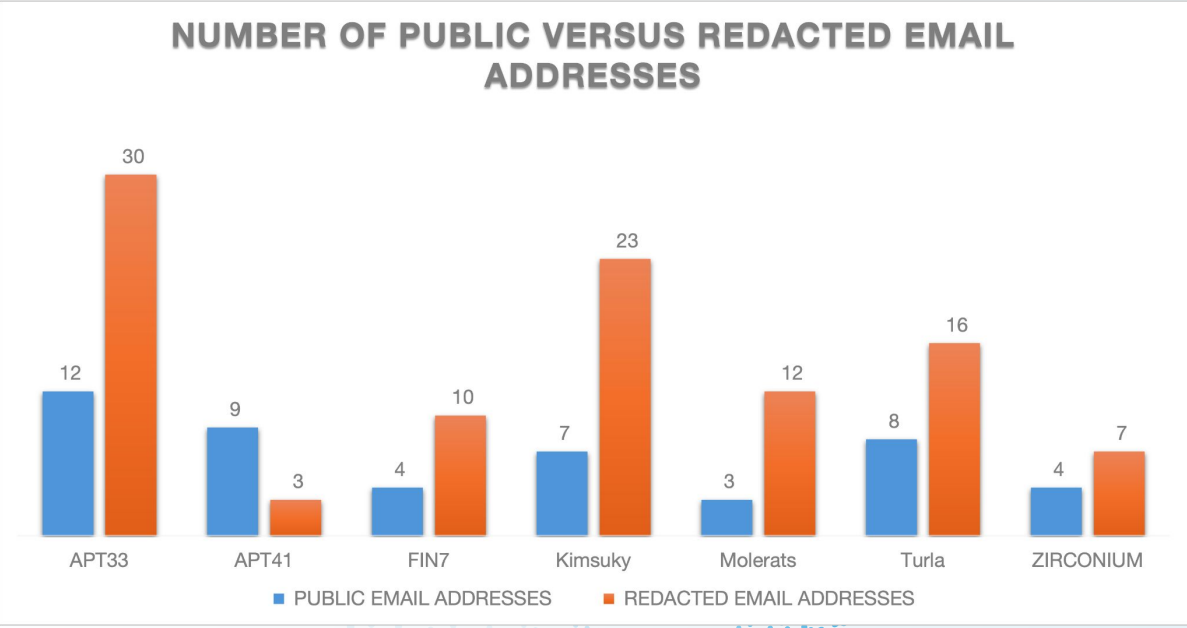
The APT Groups at a Glance

APT Group	Aliases	Based In	Target Countries	Active Since	Number of Domain IoCs Involved in the Most Recent Campaign
APT33	HOLMIUM, Elfin	Iran	U.S., Saudi Arabia, South Korea	2013	9
APT41	ARIUM, Winnti, LEAD, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly, Winnti Umbrella, Double Dragon	China	U.S.	2012	6
FIN7	GOLD NIAGARA, ITG14, Carbon Spider	Russia	North American countries	2013	18
Kimsuky	STOLEN PENCIL, Thallium, Black Banshee, Velvet Chollima	North Korea	U.S. in 2020	2012	6
Molerats	Operation Molerats, Gaza Cybergang	Saudi Arabia	Middle Eastern and European countries, U.S. in 2014	2012	3
Turla	IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear	Russia	50 countries, including the U.S. and Canada, in the past 20 years or so	2004	12
ZIRCONIUM	APT31	China	U.S. in 2020	2017	5
					59 IoCs in total

APT Group Email Footprints

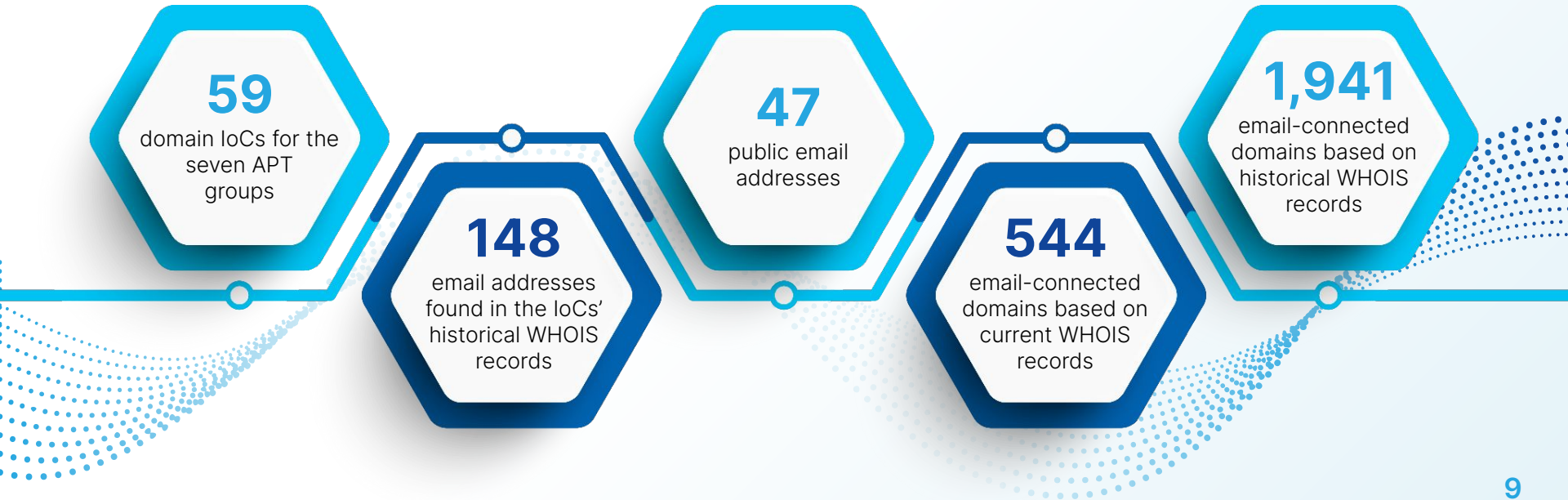
Despite the common practice of redacting domain ownership data, we were still able to look into the digital footprints of the seven APT groups aided by their associated domains' historical WHOIS record details.

In the featured APT groups' case, 32% of the email addresses obtained from related historical WHOIS records turned out to be public. Several were provided by free email service providers like Google, Yahoo!, QQ, and others.

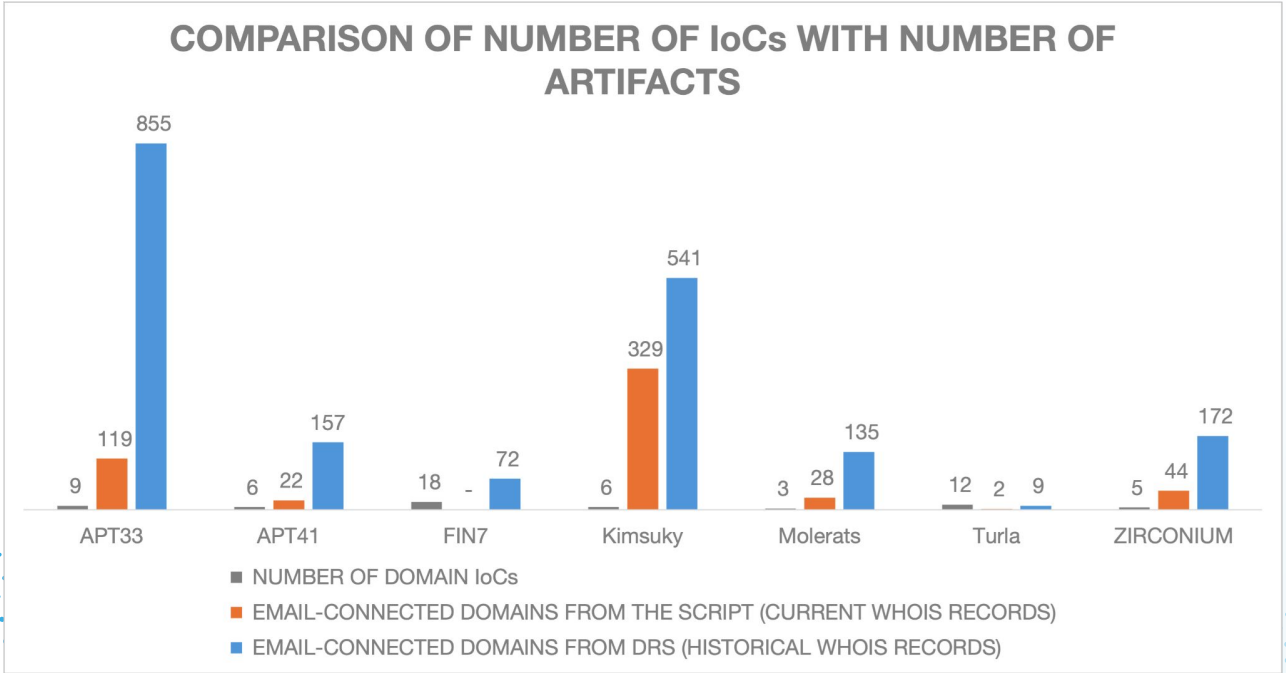


IoC List Expansion: From 59 IoCs to 1,900+ Artifacts

The WhoisXML API researchers pivoted off the email footprints of the seven APT groups and uncovered more than 1,900 email-connected domains that can be considered potential threat artifacts.



IoC List Expansion: ~3000% Increase from IoCs to Artifacts



From 59 domains identified as IoCs, our investigation led to 544 connected domains using current WHOIS record data, translating to nine times the number of IoCs.

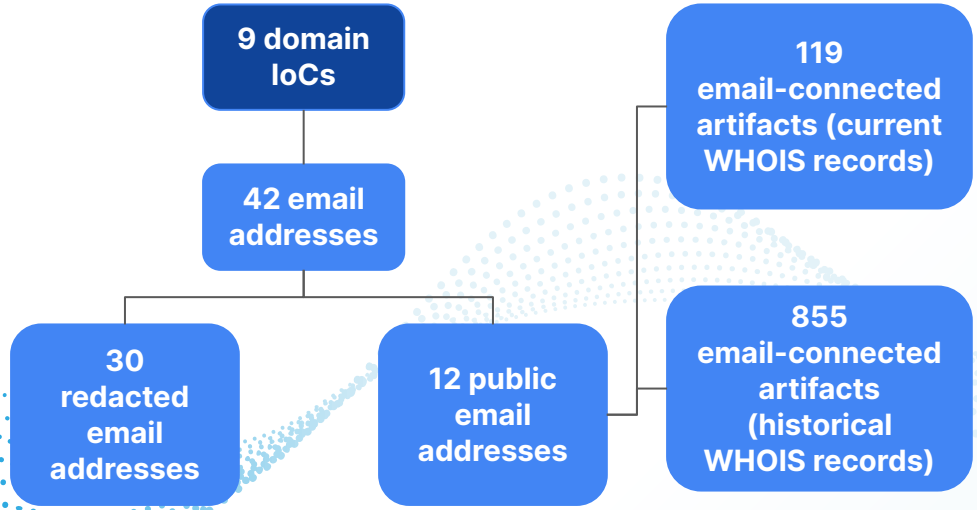
The ratio ballooned to 33 times the number of IoCs when we looked at the domain IoCs' historical WHOIS records. From 59 domain IoCs, we found 1,941 connected artifacts.

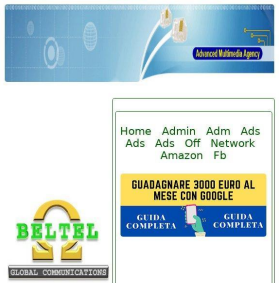
All in all, we recorded a more than 3000% increase from the number of IoCs to the number of artifacts.

A Closer Look at Each APT Group

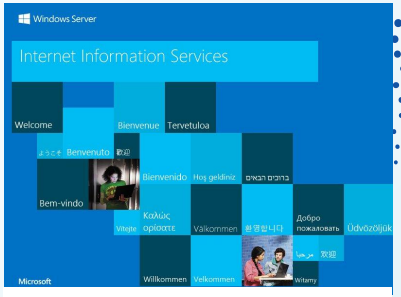
APT33

APT33, an APT group believed to be based in Iran, has been active since at least 2013. It most recently targeted the aerospace and energy sectors in the U.S., Saudi Arabia, and South Korea using two destructive malware—SHAMOON and Disttrack.





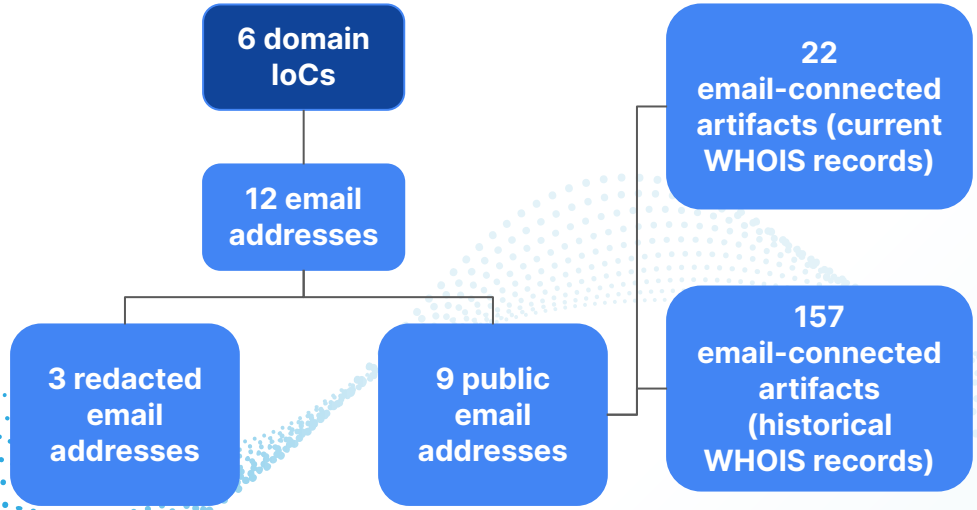
beltel[.]us



apggbcj[.]com

APT41

APT41, presumably based in China, has been active since at least 2012. It most recently targeted organizations in the U.S. using two mobile malware—WyrmSpy and DragonEgg.

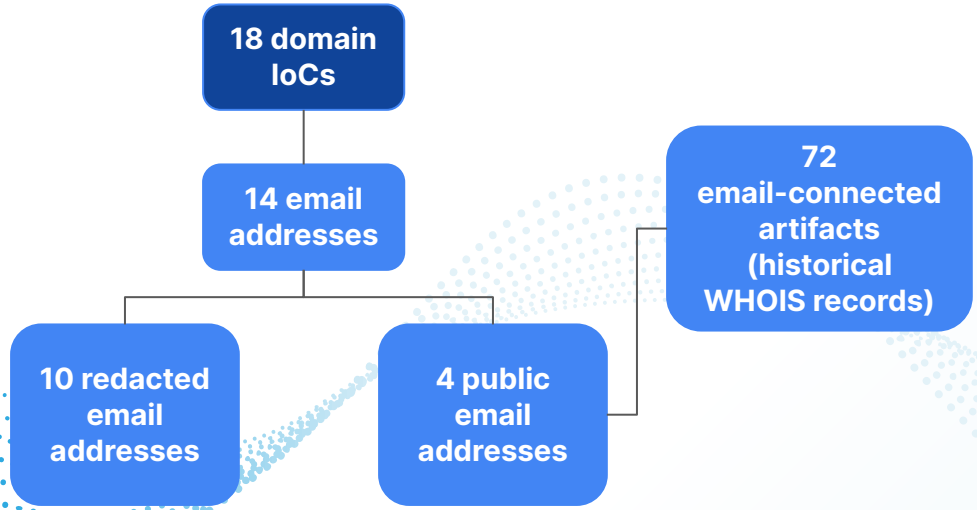


oray[.]hk

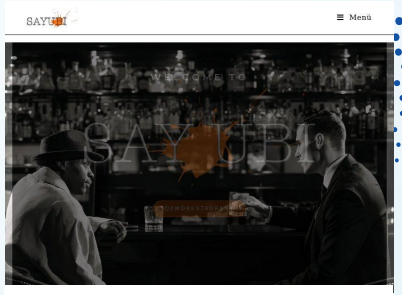
dmlao[.]net

FIN7

FIN7, a financially motivated threat group reportedly based in Russia, has been active since at least 2013. It most recently targeted the finance, retail, restaurant, and hospitality industries in North America using the ransomware Cl0p and several other malware.



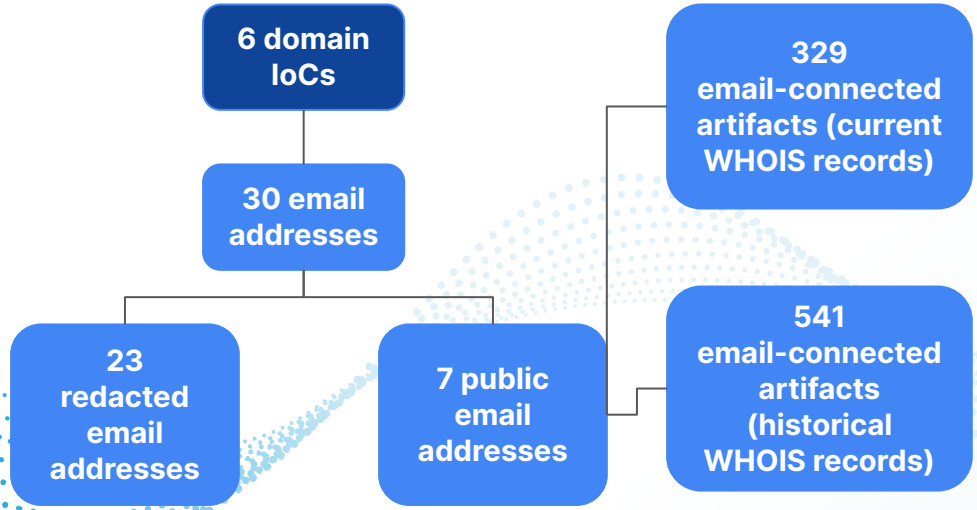
blairsdeathsauce[.]com



sayubi[.]com

Kimsuky

Kimsuky, an APT group believed to be based in North Korea, has been active since at least 2012. While it most recently targeted research institutes in South Korea, it has set its sights on field experts and think-tanks based in the U.S. in 2020 as well.

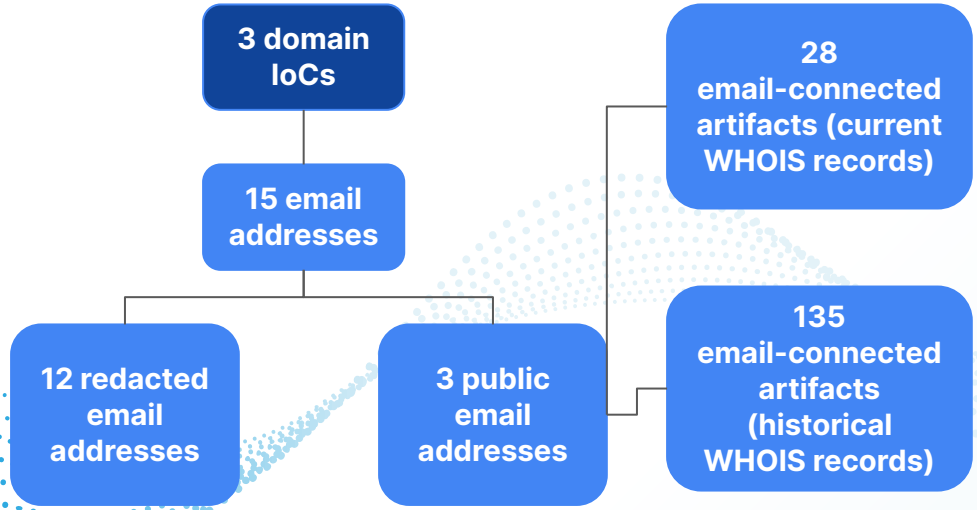


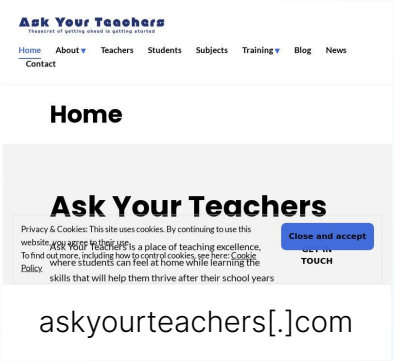
vitorpneus[.]com[.]br

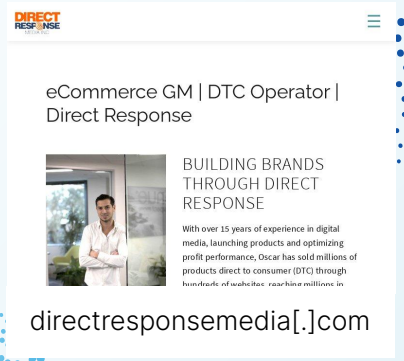
authenticbitcoin[.]com

Molerats

Molerats, presumably based in Saudi Arabia, has been active since at least 2012. While it most recently targeted government entities in the Middle East, it has trailed its sights on organizations in Europe and the U.S. in 2014 as well.

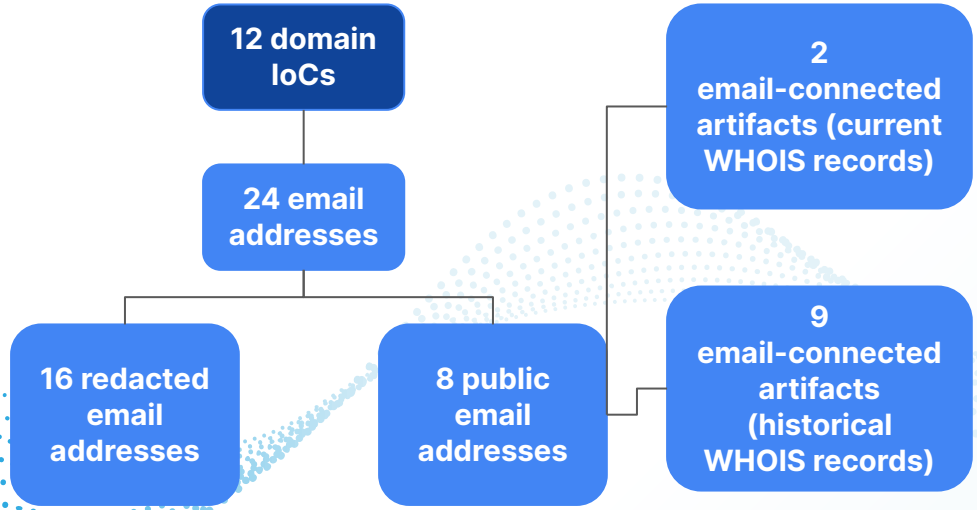


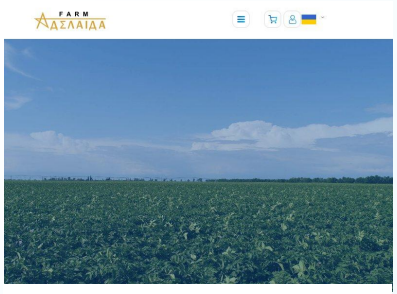




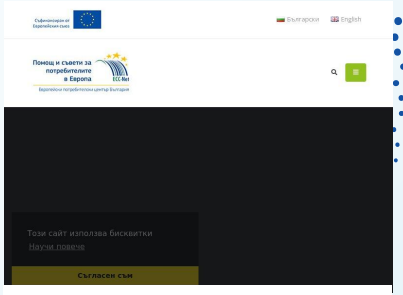
Turla

Turla, reportedly based in Russia, has been active since at least 2004. While it most recently targeted organizations in Ukraine, it has attacked entities in more than 50 countries, including the U.S. and Canada, in the past 20 or so years as well.





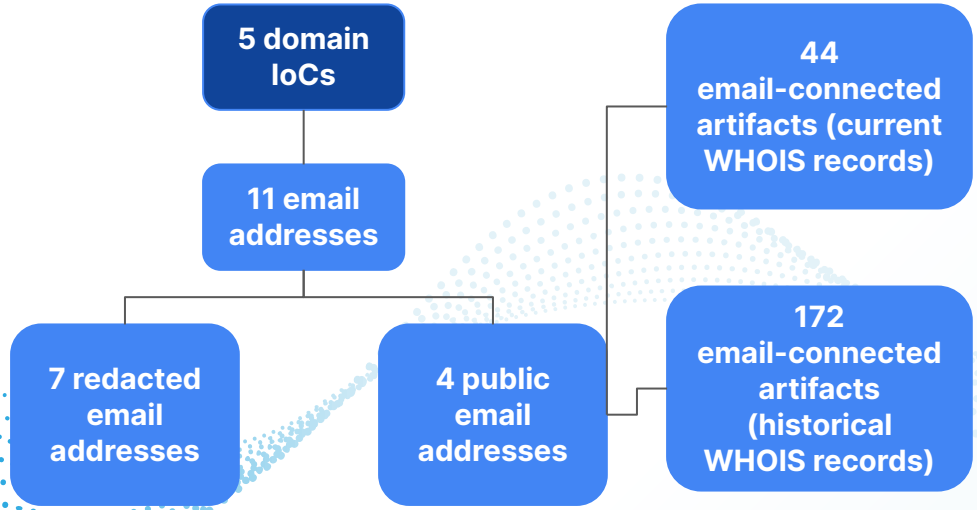
adelaidaua[.]com



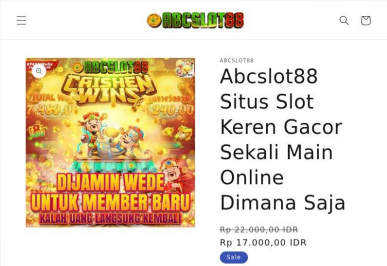
ecc[.]bg

ZIRCONIUM

ZIRCONIUM, believed to be based in China, has been active since at least 2017. While it most recently targeted Eastern Europe's industrial sector, it has launched attacks related to the 2020 U.S. elections as well.



aiadanang[.]com



kenh9[.]com

Wrap-Up

Wrap-Up

Domain ownership records contain clues that provide more information on 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 seven APT groups we investigated.

To recall, our analysis began with 59 domain IoCs whose current and historical WHOIS details led us to:

- Artifacts comprising nine times the number of IoCs based on current WHOIS record data
- Historically connected artifacts making up 33 times the number of IoCs
- Multiple email-connected artifacts that remain active as of this writing

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