WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

# Kimsuky: DNS Intel Gathering

## Table of Contents

## Executive Report

The Kimsuky Group, believed to be a North Korea-based advanced persistent threat (APT) group active since 2013, struck again several times this year. They gained notoriety for launching spear-phishing attacks on targets to gain initial access. While that tactic has not changed, the actors have changed their payload delivery means—from infected Hangul Word Processor (HWP) or Microsoft Word documents to compressed files or embedded links that contained or led to the download of a malicious LNK or shortcut file.

ASEC published an in-depth investigation of the latest Kimsuky attack specifically using RftRAT and Amadey and identified six domains and seven IP addresses as indicators of compromise (IoCs), namely:

| KIMSUKY ATTACK IoCs | |
|---|---|
| **DOMAINS** | **IP ADDRESSES** |
| brhosting[.]net | 152[.]89[.]247[.]57 |
| prohomepage[.]net | 172[.]93[.]201[.]248 |
| splitbusiness[.]com | 192[.]236[.]154[.]125 |
| techgolfs[.]com | 209[.]127[.]37[.]40 |
| theservicellc[.]com | 23[.]236[.]181[.]108 |
| topspace[.]org | 45[.]76[.]93[.]204 |
| | 91[.]202[.]5[.]80 |

The WhoisXML API research team sought to find other potential entry points the Kimsuky Group could exploit in future attacks by expanding the list of IoCs the AhnLab researchers published. Our DNS deep dive led to the discovery of:

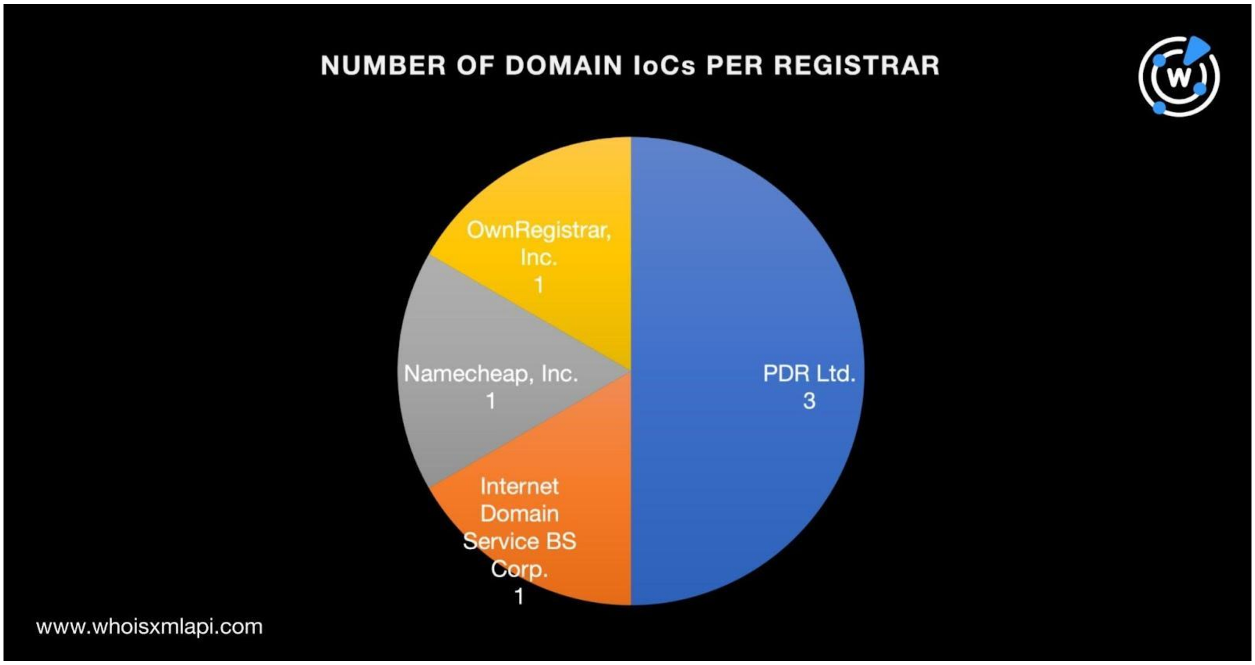
- 336 email-connected domains
- Five IP addresses to which the six domains identified as IoCs resolved, two of which were associated with various threats
- Five IP-connected domains
- 356 string-connected domains

## Behind the Kimsuky Attack IoCs

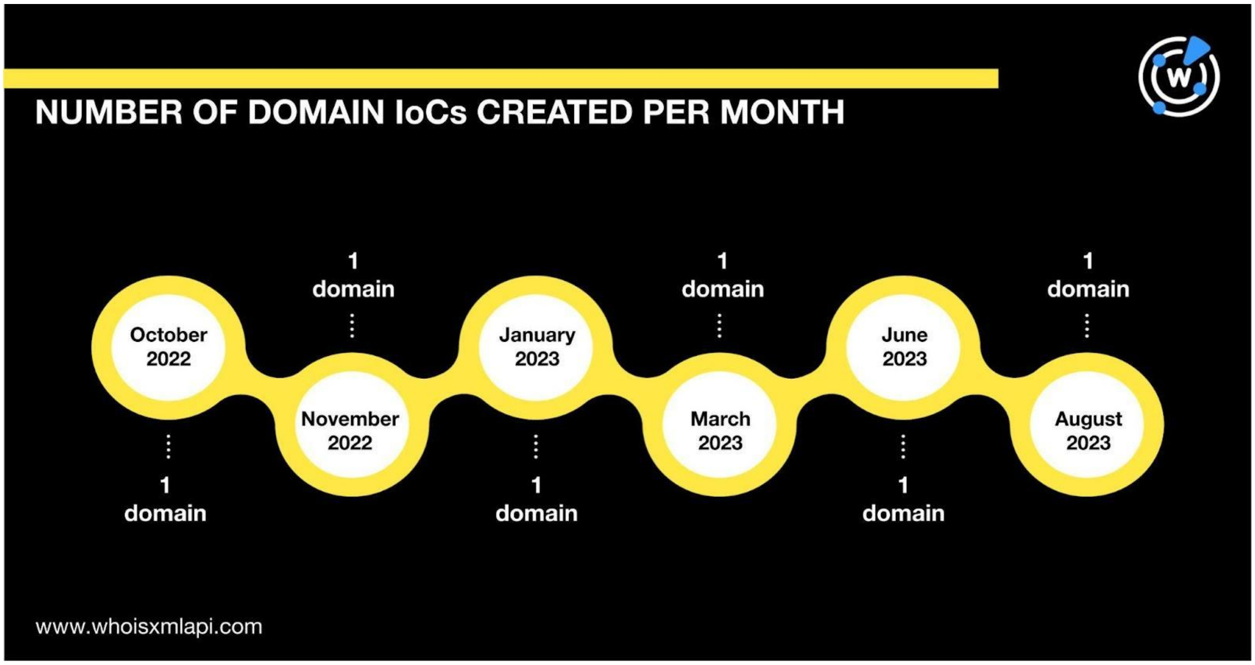
As usual, we started our analysis by taking a closer look at the 13 web properties—six domains and seven IP addresses identified as IoCs.

A bulk WHOIS lookup for the six domains revealed that:

- They were spread across four registrars topped by PDR Ltd., which accounted for three domains. One domain each was administered by three other registrars—Internet Domain Service BS Corp.; Namecheap, Inc.; and OwnRegistrar, Inc.



- They were created recently—two in 2022 and four in 2023.



NUMBER OF DOMAIN IoCs CREATED PER MONTH

October 2022
1 domain

November 2022
1 domain

January 2023
1 domain

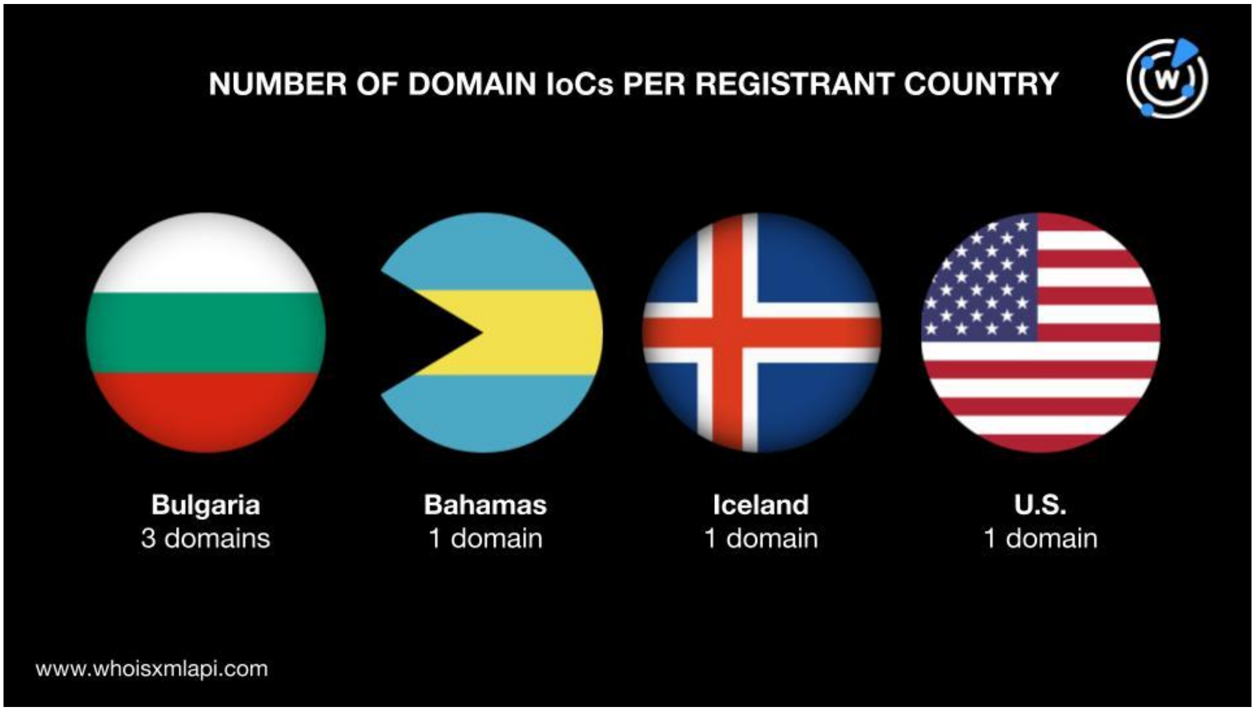
March 2023
1 domain

June 2023
1 domain

August 2023
1 domain

www.whoisxmlapi.com

- They were spread across four registrant countries led by Bulgaria, which accounted for three domains. One domain each identified Bahamas, Iceland, and the U.S. as their registrant countries.



NUMBER OF DOMAIN IoCs PER REGISTRANT COUNTRY

Bulgaria
3 domains

Bahamas
1 domain

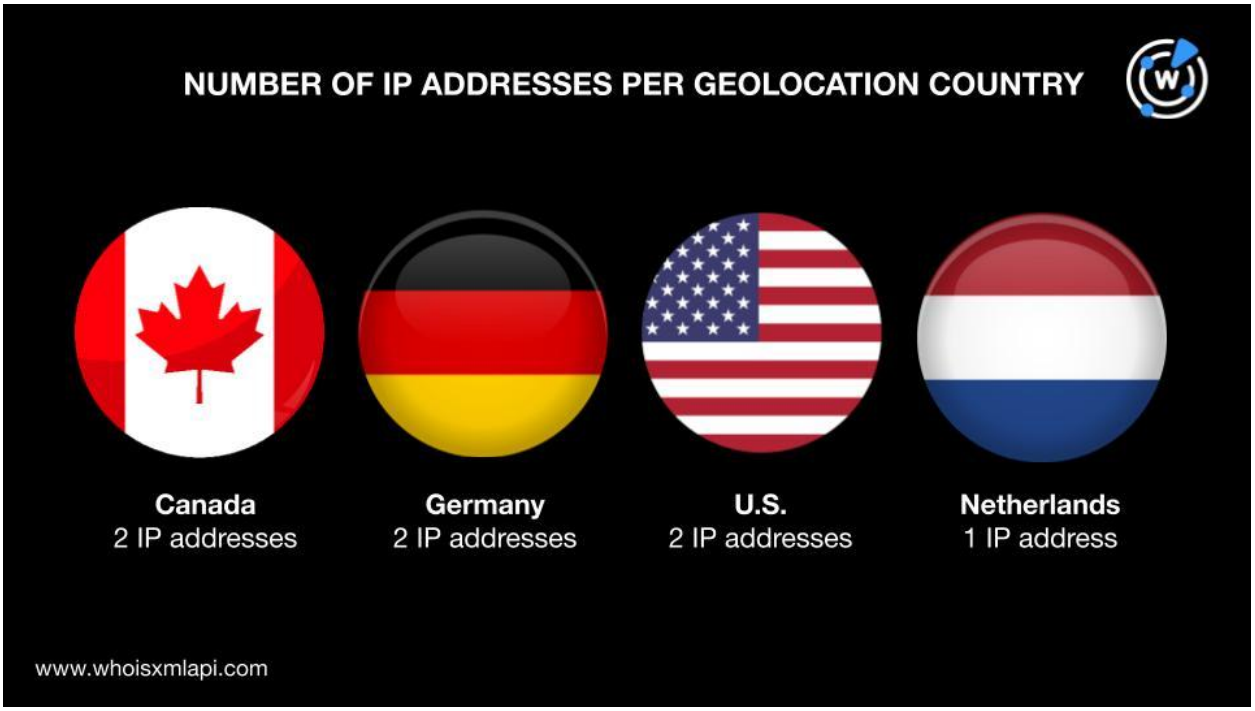
Iceland
1 domain

U.S.
1 domain

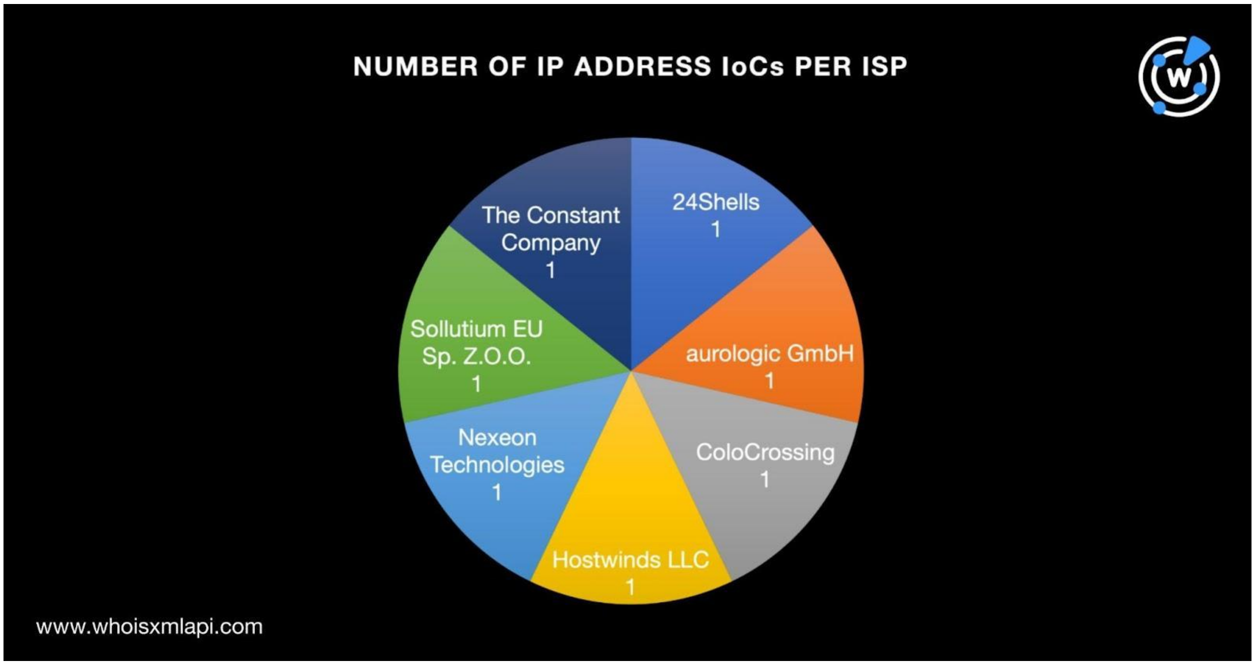
www.whoisxmlapi.com

Next, we ran the seven IP addresses through a bulk IP geolocation lookup and found that:

- Two IP addresses each were geolocated in Canada, Germany, and the U.S. The last originated from the Netherlands.



- They were spread across seven Internet service providers (ISPs) that accounted for one IP address each—24Shells, aurologic GmbH, ColoCrossing, Hostwinds LLC, Nexeon Technologies, Sollutium EU Sp. Z.O.O., and The Constant Company.



## Behind the Kimsuky Attack Infrastructure

In a bid to obtain as much information about the current Kimsuky Group attack infrastructure, we performed an expansion analysis beginning with WHOIS History API searches for the six domains identified as IoCs. Our queries led to the discovery of 30 email addresses found anywhere in their historical WHOIS records.

Seven of them were public email addresses. We subjected them to reverse WHOIS searches, which revealed that three of them also appeared in the current WHOIS records of 336 domains. None of them had duplicates nor have already been identified as IoCs.

It is interesting to note that 29 of them could figure in cryptocurrency-, blockchain-, or nonfungible token (NFT)-related threats should they get weaponized. The following table shows some examples.

| TEXT STRING | SAMPLE EMAIL-CONNECTED DOMAIN |
|---|---|
| **blockchain** | ablockchaincompany[.]com |
| **bitcoin** | bitcoinmover[.]com |
| **btc** | btclightningnetwork[.]com |
| **coin** | coinmarket[.]ca |

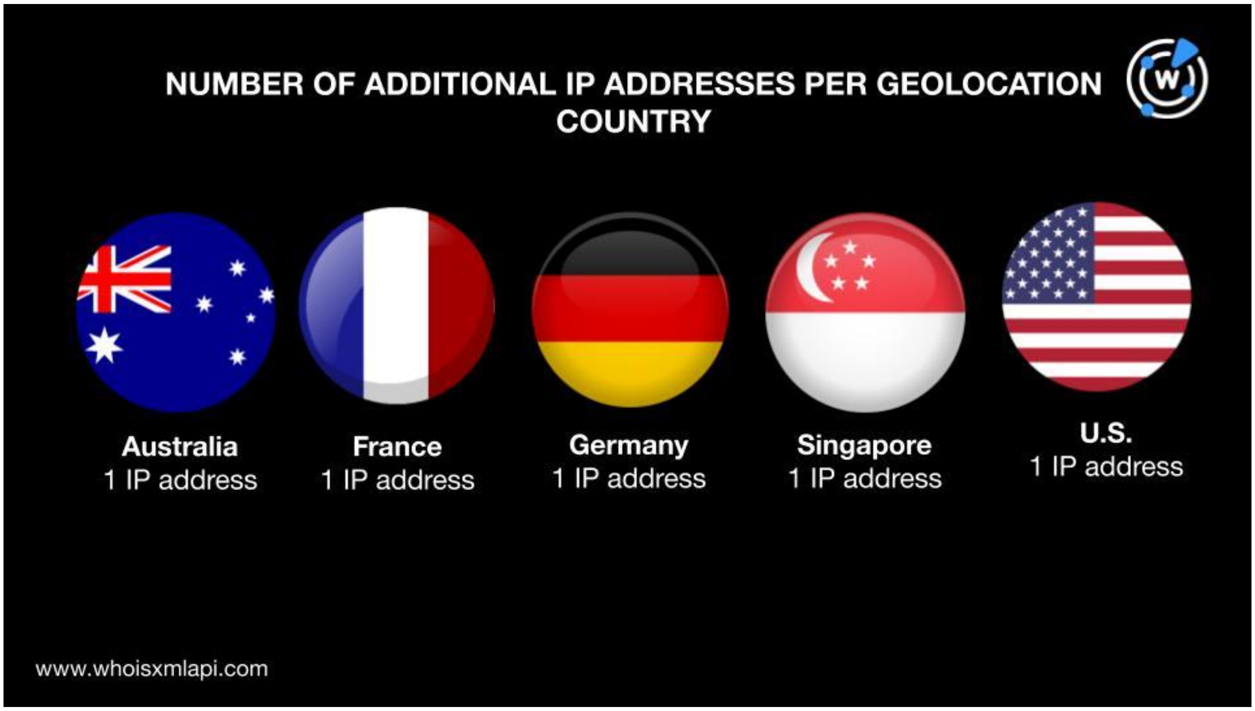
| | |
|---|---|
| **crypto** | cryptoadept[.]com |
| **matrix** | matrixcoin[.]net |
| **meta** | metapayment[.]ca |
| **nft** | nfttrader[.]ca |
| **token** | tokenpromoter[.]com |

Screenshot lookups also showed that the websites 37 of the email-connected domains pointed to remained accessible as of this writing. Only eight of them, however, led to functional websites.

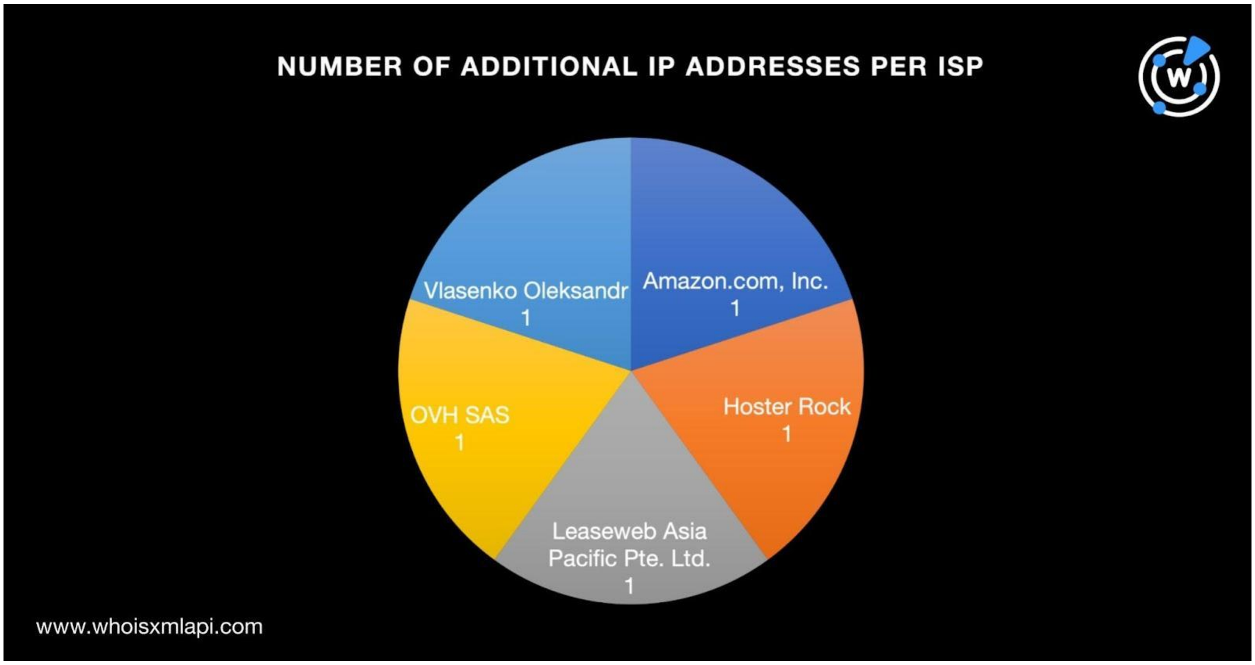
Next, we performed DNS lookups on the six domains identified as IoCs and found that they resolved to five unique IP addresses that have not yet been identified as IoCs.

IP geolocation lookups for the five IP addresses showed that:

- Each one was geolocated in five different countries—Australia, Germany, France, Singapore, and the U.S. Two of them shared Germany and the U.S. as geolocation countries like two of the IP addresses identified as IoCs.



- They were administered by five different ISPs—Amazon.com, Inc.; Hoster Rock; Leaseweb Asia Pacific Pte. Ltd.; OVH SAS; and Vlasenko Oleksandr. None of them shared the ISPs of the IP addresses identified as IoCs.



- Two of them—199[.]59[.]243[.]225 and 23[.]106[.]122[.]213—were associated with 106 threats in total based on integrated Threat Intelligence Lookup results. 199[.]59[.]243[.]225 was connected to 19 threats while 23[.]106[.]122[.]213 was related to 87 threats.

To further our search for possibly connected artifacts, we ran reverse IP lookups for the 12 IP addresses—seven identified as IoCs and five additional from our DNS lookups. We discovered that five of them could be dedicated and played host to five domains that were not part of the lists of domain IoCs and email-connected domains.

Based on screenshot lookups, only one IP-connected domain continued to host live content—thesisterize[.]gb[.]net.

As a final step, we ran Domains & Subdomains Discovery searches for text strings found among the domains identified as IoCs, namely:

- **brhosting**
- **prohomepage**
- **splitbusiness**
- **techgolfs**
- **topspace**

That led to the discovery of 356 string-connected domains after duplicates, the IoCs, and email- and IP-connected domains were filtered out. Note that we used the **Contains** parameter and included all the domains in our repository (collated over the past decade or so). Screenshot lookups revealed that 34 of them continued to point to live websites.

—

Our more in-depth investigation into the latest set of Kimsuky Group attack IoCs, specifically those that used the RftRAT and Amadey malware, allowed us to uncover 702 possibly connected artifacts—336 email-connected domains, five IP addresses, five IP-connected domains, and 356 string-connected domains.

***If you wish to perform a similar investigation or 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 and IoCs

### Sample Email-Connected Domains

- 6666[.]ca
- ablockchaincompany[.]com
- ahoteis[.]com[.]br
- aliancademoedaantiga[.]com[.]br
- anodynebusiness[.]com
- appentrepreneuradvice[.]com
- auctioning[.]ca
- barquebusiness[.]com
- bitcoinmover[.]com
- bitcoinpipe[.]com
- blendentrepreneur[.]com
- blockchainpolicies[.]com
- bloggingentrepreneuradvice[.]com
- boardentrepreneuradvice[.]com
- boldbusinessadvice[.]com
- btclightningnetwork[.]com
- btcorders[.]com
- btctesting[.]com
- btctransactions[.]com
- businesstrendadvice[.]com
- cabincruiserbusiness[.]com
- cashentrepreneuradvice[.]com
- casinosvr[.]net
- catwalkvr[.]com
- cementbusinessadvice[.]com
- cleaningentrepreneuradvice[.]com
- clik[.]ca
- clothesentrepreneuradvice[.]com

- coinmarket[.]ca
- conceptbusinessadvice[.]com
- conceptentrepreneuradvice[.]com
- contentbusinessadvice[.]com
- convincebusiness[.]com
- coursebusinessadvice[.]com
- crabberbusiness[.]com
- cryptoadept[.]com
- cryptoinvestments[.]ca
- cryptoportfolio[.]ca
- customerbusinessadvice[.]com
- dairyproducts[.]net
- decentralizedcryptos[.]com
- dicey[.]net
- dispatchbusiness[.]com
- dividebusiness[.]com
- dnbuyer[.]xyz
- dndeals[.]xyz
- dndepot[.]xyz
- dndrone[.]xyz
- dnfind[.]xyz
- dnfinder[.]xyz

## Sample IP Addresses

- 139[.]99[.]155[.]54
- 199[.]59[.]243[.]225
- 23[.]106[.]122[.]213

## Sample IP-Connected Domains

- hecug[.]com
- kv635616[.]info
- ot319954[.]info

## Sample String-Connected Domains

- 1stopspace[.]com
- 1topspace[.]com
- 52topspace[.]com
- 5topspace[.]top
- abrhosting[.]com
- abrhosting[.]ir
- abrhosting[.]xyz
- aerotechgolfshafts[.]com
- aerotechgolfshafts[.]net
- aerotechgolfshaftsjapan[.]com
- areotechgolfshafts[.]com
- atopspace[.]com
- aviatopspace[.]com
- bbrhosting[.]nl
- bitopspace[.]com
- bj-topspace[.]com
- bjtopspace[.]com
- bjtopspace[.]tw
- brhosting[.]cloud
- brhosting[.]co[.]uk
- brhosting[.]com
- brhosting[.]com[.]br
- brhosting[.]com[.]mx
- brhosting[.]ga
- brhosting[.]info
- brhosting[.]ml
- brhosting[.]nl
- brhosting[.]online
- brhosting[.]org
- brhosting[.]srv[.]br
- brhosting[.]store
- brhosting[.]tk
- brhosting[.]xyz
- brhostinger[.]com

- brhostings-ofc[.]tk
- brhostings[.]com
- brhostings[.]tk
- brhostingserver[.]com[.]br
- brhostingweb[.]com
- cbrhosting[.]co[.]uk
- cbrhosting[.]com
- cbrhosting[.]uk
- clickstopspace[.]online
- clickstopspace[.]site
- clubtechgolfshop[.]com
- coppertopspaces[.]com
- countertopspace[.]com
- csbrhosting[.]com
- csbrhosting[.]xyz
- ctopspace[.]com