WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

# Peering into Midnight Blizzard's DNS Footprint

## Table of Contents

## Executive Report

Thousands of people working for organizations in the public, academia, and defense sectors are being targeted by spear-phishing attacks operated by a threat group called "Midnight Blizzard." The messages contained a Remote Desktop Protocol (RDP) configuration file connected to the malicious actor's server.

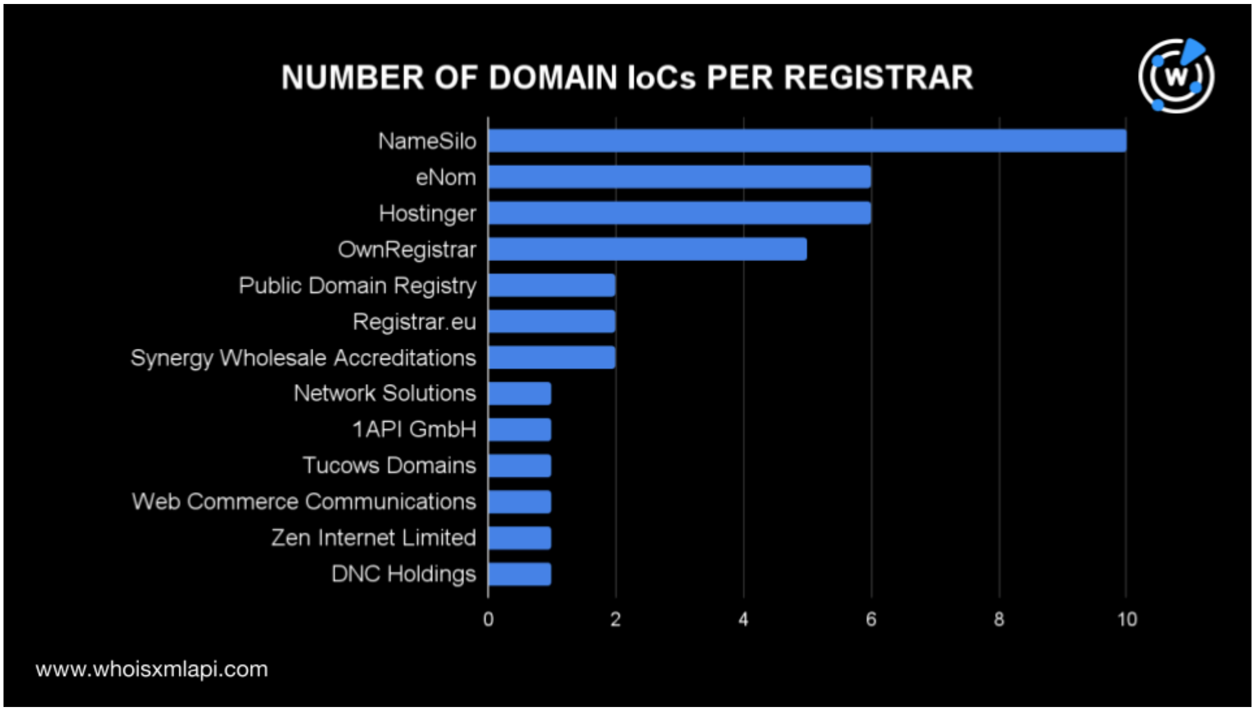
Midnight Blizzard has been active for decades now, but using a signed RDP config file to gain access to a victim's device is a new vector, according to Microsoft, which also published a list of indicators of compromise (IoCs) comprising 276 subdomains and five domains. From this list, the WhoisXML API research team analyzed and expanded a total of 39 domain IoCs (including 34 domains extracted from the subdomains tagged as IoCs), leading to the discovery of:

- 18 email-connected domains
- 16 IP addresses, 11 of which turned out to be malicious
- 20 IP-connected domains, one of which turned out to be malicious
- 106 string-connected domains, six of which turned out to be malicious

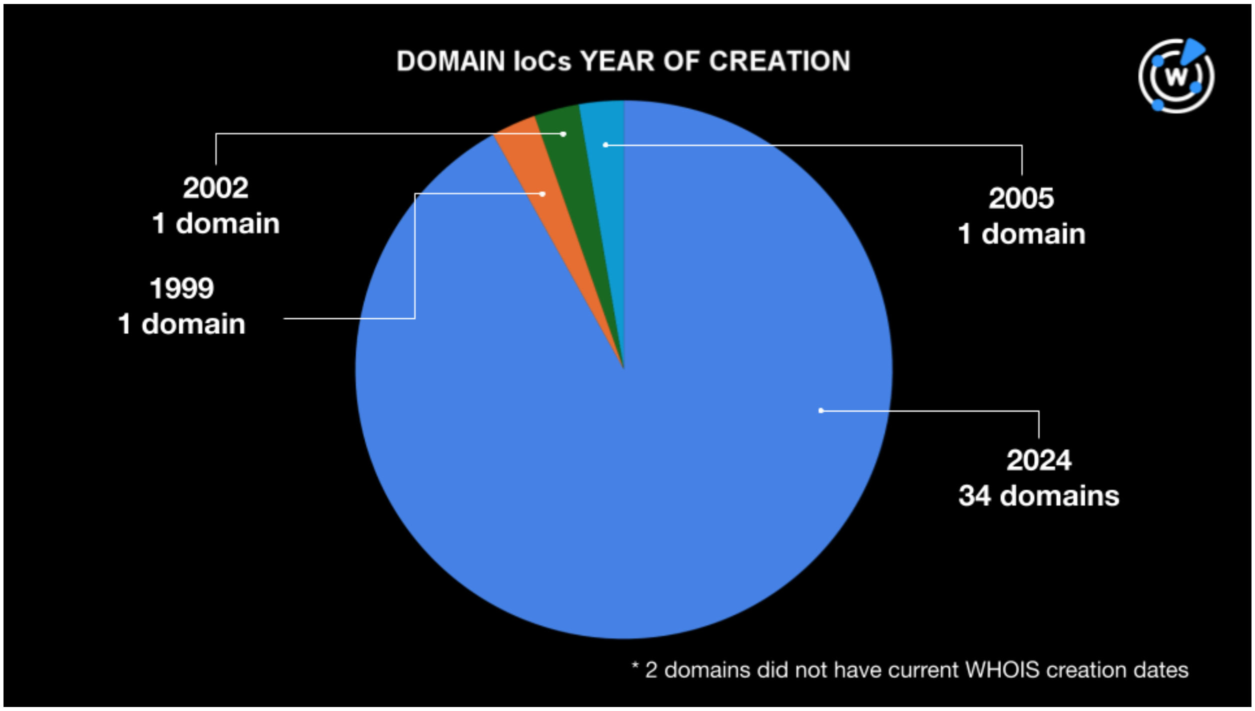
### What We Know about the Midnight Blizzard IoCs

To learn more about the attributes of the 39 domain IoCs, we ran them on Bulk WHOIS Lookup, which revealed that:

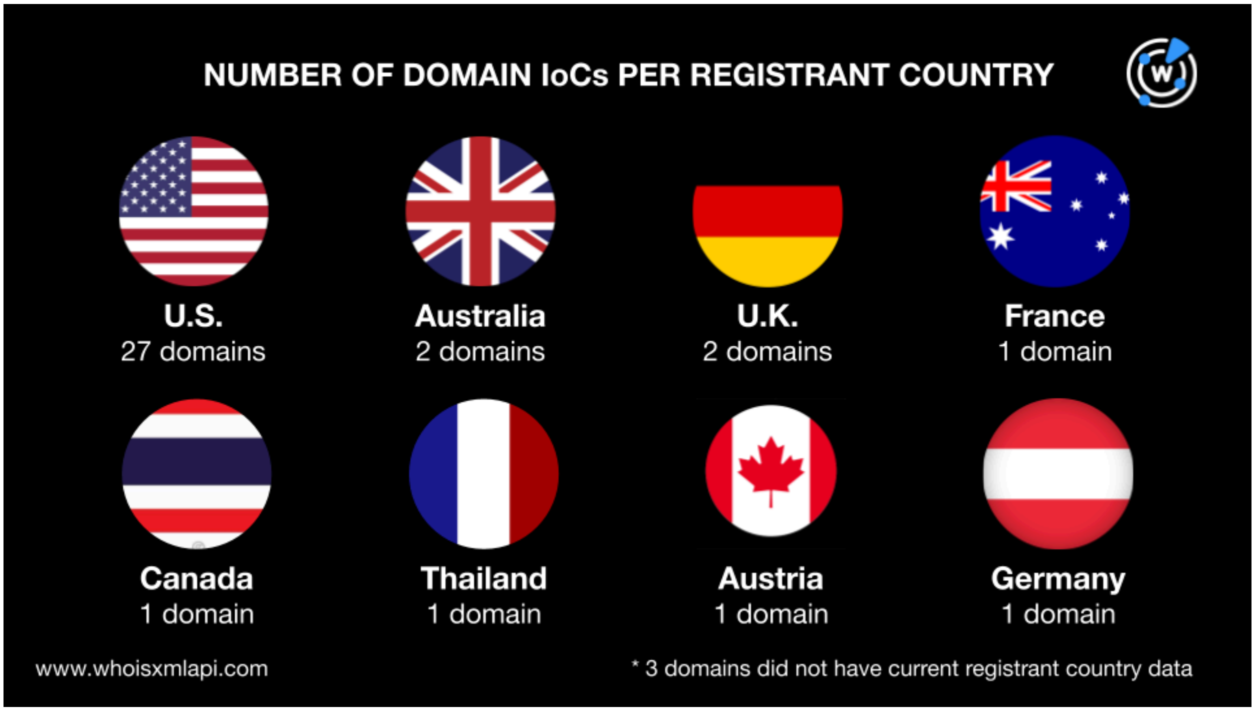
- 13 registrars administered the domains with NameSilo taking the lead (10 domains). It was followed by eNom and Hostinger with six domains each; OwnRegistrar with five domains; Public Domain Registry, Registrar.eu, and Synergy Wholesale Accreditations with two domains each; Network Solutions, 1API GmbH, Tucows Domains, Web Commerce Communications, Zen Internet Limited, and DNC Holdings with one domain each.



- A total of 34 out of the 39 domain IoCs were registered no earlier than August 2024, while one each was created in 1999, 2002, and 2005, respectively. Two domains did not have current WHOIS creation dates.



- A total of 69% of the domains were registered in the U.S., while the rest were registered in seven other countries, namely, Australia, the U.K., France, Canada, Thailand, Austria, and Germany. Three domains did not have current registrant country data.



Next, we queried the 39 domains tagged as IoCs on DNS Chronicle API to see their earliest IP resolution dates and mobilization timeline.

Excluding the two domains that did not have current creation dates, we found that about 57%, 21 to be exact, immediately resolved to different IP addresses within three days upon registration, 1 resolved 10–30 days from the day it was registered, and 9 domains resolved 30 days or beyond after their registration dates. Meanwhile, 6 domains did not have recorded historical IP resolutions. Below are some examples.

| DOMAIN IoC | DOMAIN REGISTRATION DATE | RESOLUTION START DATE | REGISTRATION-TO-RESOLUTION TIMELINE (DAYS) |
|---|---|---|---|
| difesa-it[.]cloud | 22 August 2024 | 22 August 2024 | 0 |
| mfa-gov[.]cloud | 15 August 2024 | 31 August 2024 | 16 |
| gov-ua[.]cloud | 15 August 2024 | 29 September 2024 | 45 |

In total, the 39 domains tagged as IoCs resolved to 47 unique IP addresses from the time they were registered until their most recent resolution dates.

We also queried the 39 domains tagged as IoCs on Screenshot API and found that five remained accessible, while eight returned a 403 Forbidden error.

## Midnight Blizzard IoC Expansion Analysis Findings

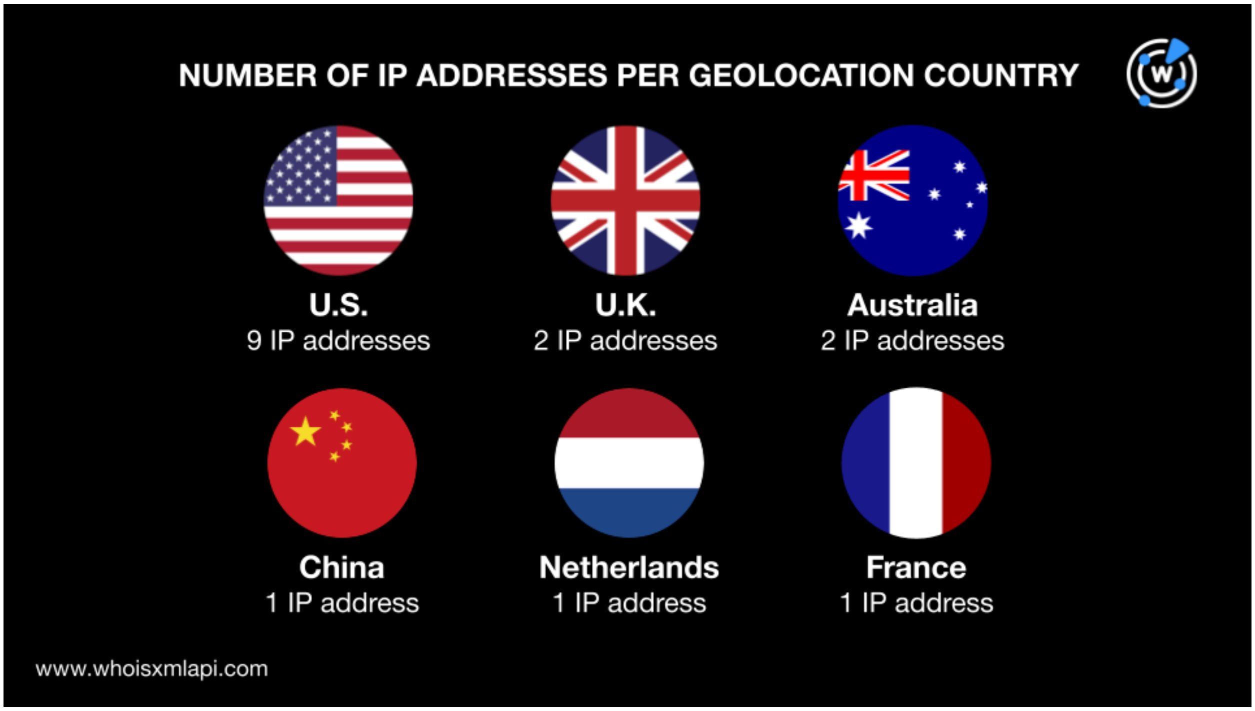
Among the goals of our threat reports is to discover additional threat artifacts. As our usual first step, we queried the 39 domains tagged as IoCs on WHOIS History API, which returned 11 email addresses from their historical WHOIS records. Only five of these email addresses were public.

Querying the five public email addresses on Reverse WHOIS API gave us 18 email-connected domains after duplicates and the IoCs were filtered out.

We then ran the 39 domain IoCs on DNS Lookup API and found that 16 of them resolved to 16 unique IP addresses, 11 of which were malicious according to Threat Intelligence API. All 11 malicious IP addresses were associated with malware distribution.

Next, a bulk IP geolocation lookup for the 16 IP addresses revealed that:

- They were spread across six geolocation countries led by the U.S. with nine IP addresses. The U.K. and Australia accounted for two IP addresses each, while China, the Netherlands, and France accounted for one IP address each.



NUMBER OF IP ADDRESSES PER GEOLOCATION COUNTRY

**U.S.**
9 IP addresses

**U.K.**
2 IP addresses

**Australia**
2 IP addresses

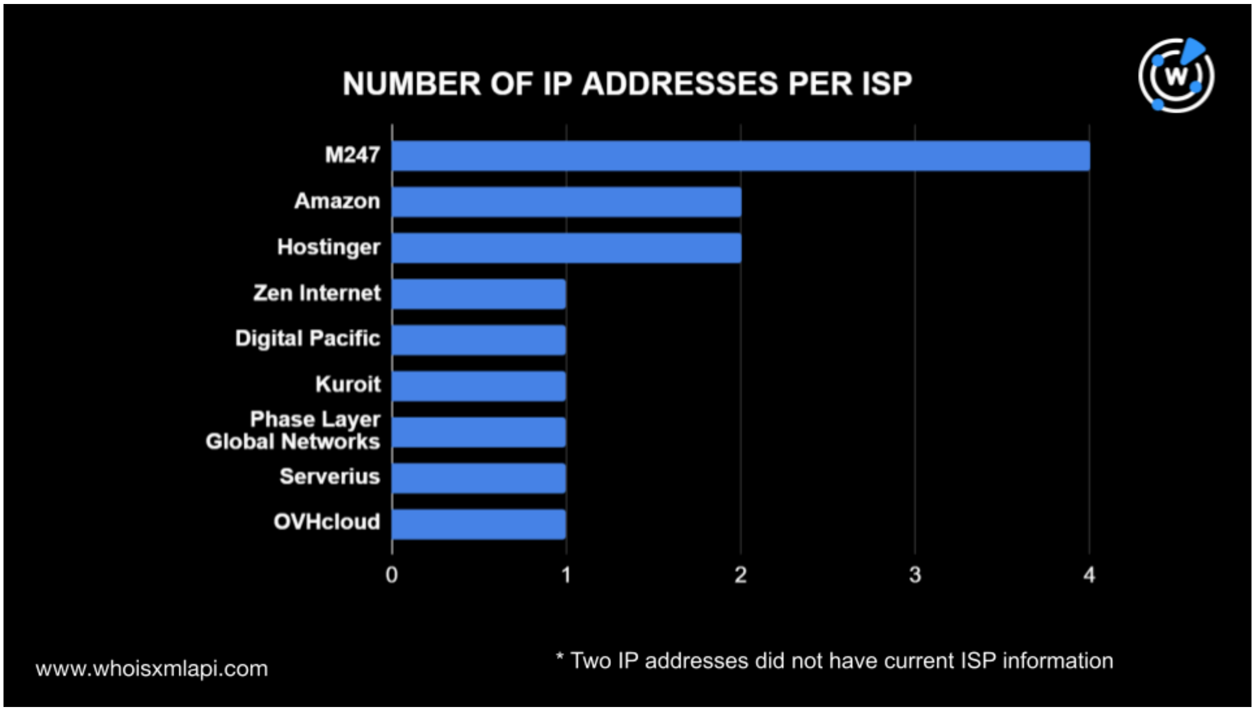
**China**
1 IP address

**Netherlands**
1 IP address

**France**
1 IP address

www.whoisxmlapi.com

- While two IP addresses did not have current ISP information, the rest were distributed across nine different ISPs led by M247 (four IP addresses). It was followed by Amazon and Hostinger (two IP addresses each) and Zen Internet, Digital Pacific, Kuroit, Phase Layer Global Networks, Serverius, and OVHcloud (one IP address each).



* Two IP addresses did not have current ISP information

We then sought to find IP-connected domains by querying the 16 IP addresses on Reverse IP API. We found that 11 of them could be dedicated, as they hosted only 3–39 domains each. Overall, we found an additional 20 unique IP-connected domains after removing duplicates, the IoCs, and the email-connected domains.

Threat Intelligence API also revealed that one IP-connected domain, eu-west-3-aws[.]minbuza[.]cloud, was malicious and associated with malware distribution.

Our next analysis leveraged Domains & Subdomains Discovery to uncover domains that contained the text strings that appeared in the domain IoCs. We found 106 string-connected domains that started with these strings added from 1 January to 9 December 2024:

- gov-ua.
- gov-pl.
- ncfta.
- amazonsolutions.
- ua-gov.
- mfa-gov.
- quirinale.
- sellar.
- ukrtelecom.
- gv-at.
- townoflakelure.
- ua-mil.
- ua-sec.
- minbuza.
- gov-sk.
- s3-be.
- regeringskansliet-se.
- msz-pl.
- difesa-it.
- mil-be
- ua-energy.
- mzv-cz.
- s3-ua.
- ukrainesec.
- aws-ukraine.
- dep-no.
- presidencia-pt.
- gov-trust.
- mil-pl.
- mindef-nl.
- mzv-sk.
- s3-esa.
- s3-nato.
- s3-de.
- admin-ch.
- mil-pt.

Six of the string-connected domains were malicious.

Finally, we ran the 144 domain artifacts (i.e., domains connected to the IoCs via email address, IP address, and text string) on Screenshot API. We found that 41 of them remained accessible to date.

—

Our DNS deep dive into the Midnight Blizzard IoCs led to the discovery of 160 additional artifacts comprising 18 email-connected domains, 16 IP addresses, 20 IP-connected domains, and 106 string-connected domains. Eighteen of these artifacts have already been weaponized, mainly for malware distribution.

***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

- whyhickorynutgorge[.]com
- whychimneyrockvillage[.]com
- nchighway9[.]com
- workinthegorge[.]com
- lakelurejobs[.]com
- whylakelure[.]com
- whylakelure[.]org
- whylakelure[.]net
- ernestpublications[.]com

## Sample IP Addresses

- 82[.]71[.]204[.]23
- 162[.]221[.]183[.]17
- 101[.]0[.]108[.]6
- 103[.]19[.]61[.]169
- 54[.]148[.]47[.]112
- 45[.]80[.]193[.]9
- 185[.]76[.]79[.]178
- 81[.]17[.]31[.]106

## Sample IP-Connected Domains

- brandstorm[.]pw
- camaramulsaodomingosdoaraguaia[.]pa[.]gov[.]br
- jimmie24[.]oceansaver[.]in
- cpanel[.]minbuza[.]cloud
- cmbaiao[.]pa[.]gov[.]br
- eu-west-3-aws[.]minbuza[.]cloud
- cmbrejograndedoaraguaia[.]pa[.]gov[.]br
- ftp[.]minbuza[.]cloud
- kitpublico[.]com[.]br
- localhost[.]minbuza[.]cloud

## Sample String-Connected Domains

- sellar[.]tech
- sellar[.]top
- sellar[.]so
- townoflakelure[.]ws
- townoflakelure[.]ph
- zsu-ua-gov[.]info
- ua-gov[.]ph
- ncua-gov[.]net
- ncua-gov[.]info
- ua-gov[.]org
- edopomoga-ua-gov[.]org
- ua-gov[.]space
- edopomoga6-gov-ua[.]com
- petition-gov-ua[.]org
- bkr-omv-gov-ua[.]xyz
- vb-bkr-omv-gov-ua[.]help
- petition-president-gov-ua[.]online
- hsc-gov-ua[.]online
- unicuef-gov-ua[.]buzz
- edopomoga8-gov-ua[.]com
- bkr-omv-gov-ua[.]buzz
- petition-president-gov-ua[.]com
- hsc-gov-ua[.]org[.]ua
- vb-bkr-omv-gov-ua[.]buzz
- police-gov-ua[.]ru
- dopomoga-gov-ua[.]com
- edopomoga7-gov-ua[.]net
- vb-bkr-omv-gov-ua[.]xyz
- rama-vb-bkr-omv-gov-ua[.]biz
- vb-bkr-omv-gov-ua[.]bond
- police-gov-ua[.]com
- edopomoga1-gov-ua[.]com
- edopomoga-gov-ua[.]org
- edopomoga7-gov-ua[.]com
- rama-vb-bkr-omv-gov-ua[.]bond
- mod-gov-ua[.]com
- pttgov-ua[.]top
- dpsu-gov-ua[.]com
- vb-bkr-omv-gov-ua[.]biz
- petition-gov-ua[.]com
- edopomoga-gov-ua[.]net
- rama-vb-bkr-omv-gov-ua[.]buzz
- login-gov-ua[.]com
- ukraongov-ua[.]com
- dopomoga-gov-ua[.]net
- edopomoga-gov-ua[.]com
- rama-vb-bkr-omv-gov-ua[.]shop
- opendata-hsc-gov-ua[.]site
- dopomogagov-ua[.]com
- bkr-omv-gov-ua[.]biz