DNS Deep Diving into 2025's Up and Coming Ransomware Families

Table of Contents

1. Executive Report
2. Appendix: Sample Artifacts

Executive Report

Ransomware attacks have been plaguing individual users and organizations worldwide for years now. And that is not surprising because they work. In fact, ransomware victims were asked to pay an average of US$2.5 million in 2024.

A report published on TheHackerNews named 10 of the most active ransomware families in 2024, which WhoisXML API decided to further investigate. We obtained lists of indicators of compromise (IoCs) for each of these ransomware variants:

- RansomHub
- LockBit 3.0
- Play
- Akira
- Hunters
- Medusa
- BlackBasta
- Qilin
- BianLian
- INC. Ransom (aka Lynx)

We collated a total of 120 IoCs for all the ransomware families comprising 48 domains and 72 IP addresses. Take a look at their detailed breakdown below.

VARIANT	DOMAIN IoCs	IP ADDRESS IoCs
RansomHub	5	9
LockBit 3.0	16	3
Play	1	1
Akira	1	1
Hunters	8	0

Medusa	5	32
BlackBasta	9	15
Qilin	1	7
BianLian	1	0
INC. Ransom	1	4

We sought to uncover connected artifacts that have not yet been published in any other threat report using various DNS intelligence sources. Our IoC list expansion analysis led to the discovery of:

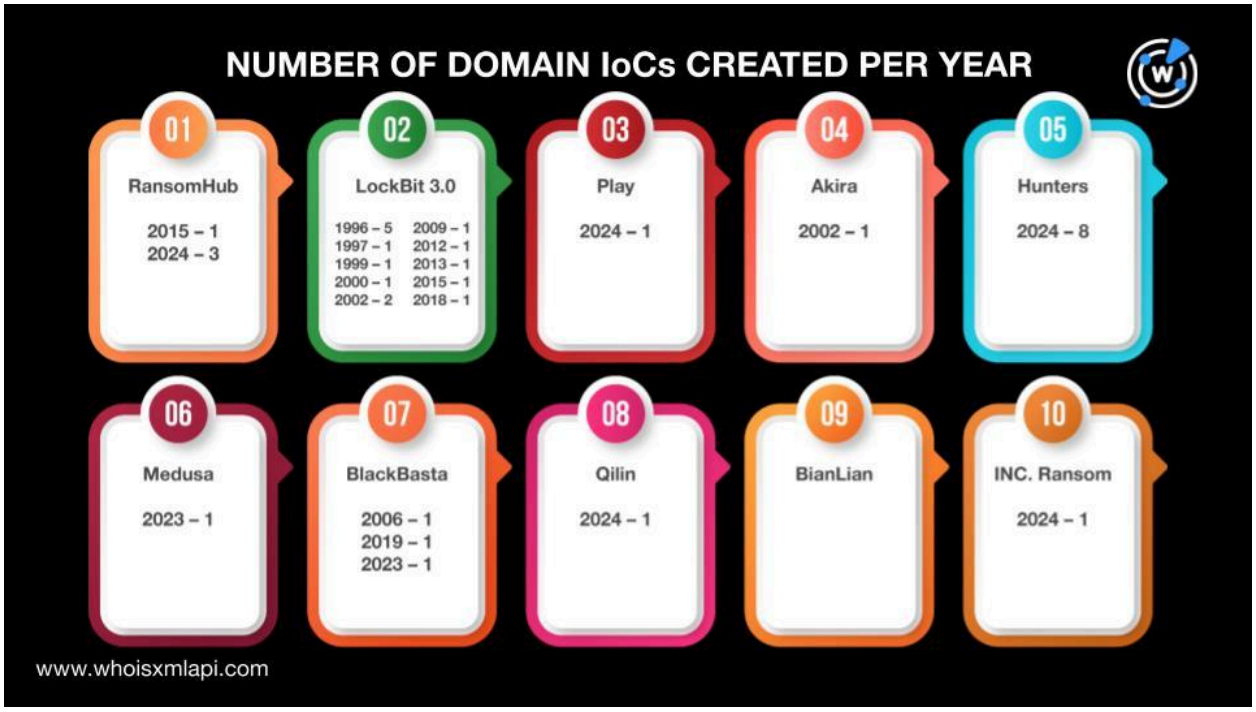
- 944 email-connected domains, 27 of which turned out to be malicious
- 48 additional IP addresses, 34 of which already figured in malicious campaigns
- 201 IP-connected domains, two of which were already associated with threats
- 1,192 string-connected domains, three of which have already been weaponized for attacks

A Closer Look at the IoCs

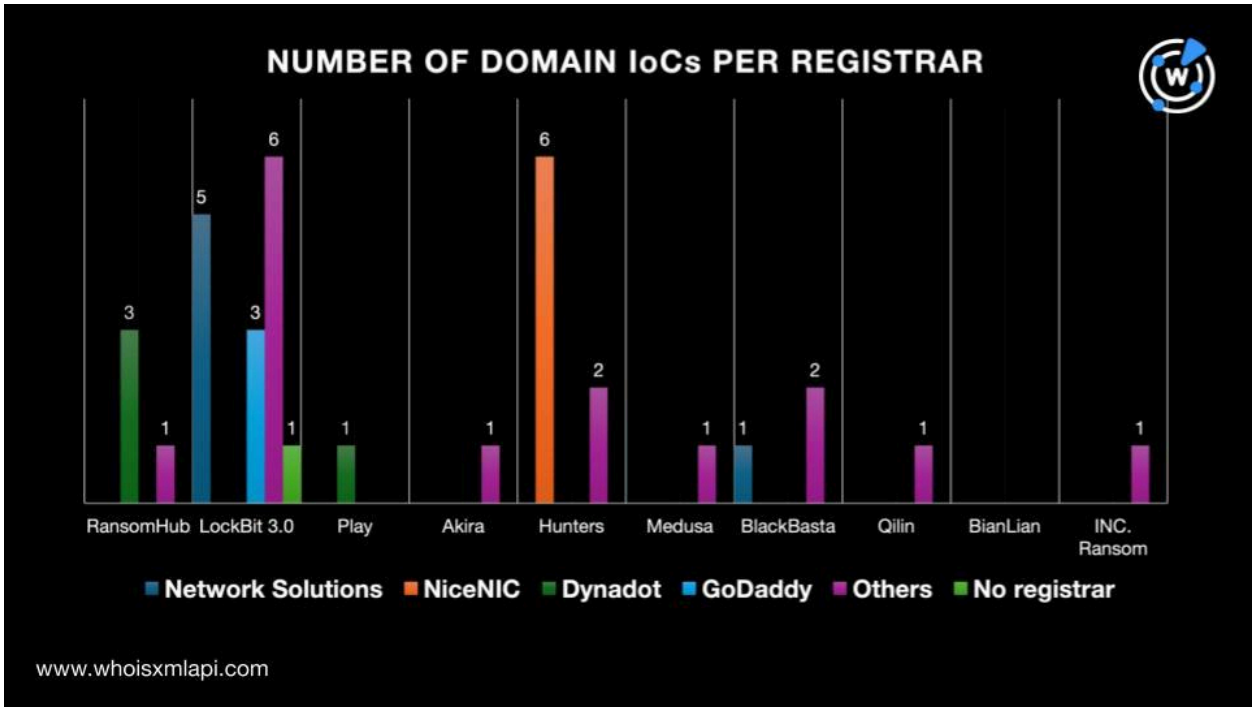
Before embarking on our expansion analysis, we sought to find more information on the IoCs first.

We started by querying the 48 domains identified as IoCs on Bulk WHOIS API. Only 35 of the domains had current WHOIS records. The results showed that:

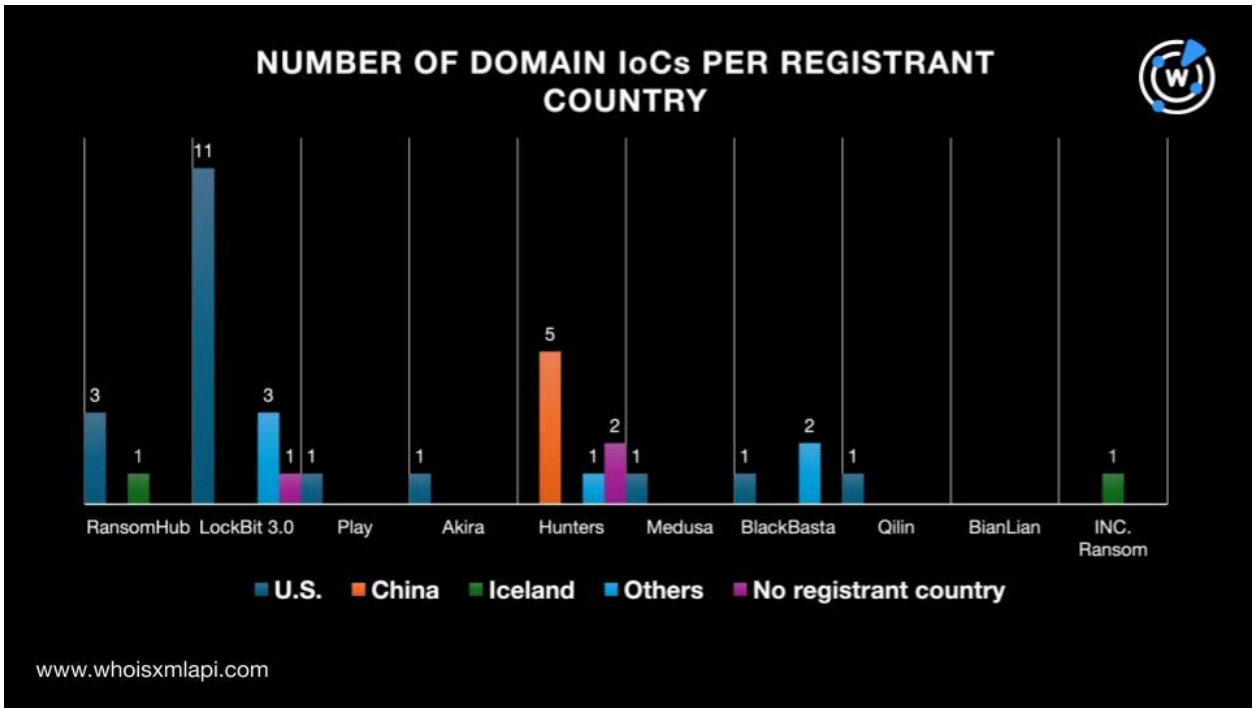
- They were created between 1996 and 2024.



- Out of the 35 domains with current WHOIS record data, only 34 had registrar information. They were split among 15 registrars topped by Network Solutions and NiceNIC, which accounted for six domains each. Dynadot took the second spot with four domains. GoDaddy placed third with three domains. Amazon, Namecheap, PDR, and RU-CENTER accounted for two domains each. Cloudflare, eNom, NameSilo, Nominalia Internet, Register, Register.com, and Wild West Domains accounted for one domain each. Finally, one domain did not have a registrar on record.



- Out of the 35 domains with current WHOIS record data, 32 had registrant country data. They were registered in nine different countries led by the U.S., which accounted for 19 domains. China placed second with five domains. Iceland took the third spot with two domains. Austria, India, Italy, Russia, Spain, and the U.K. accounted for one domain each. Finally, three domains did not have registrant countries on record.

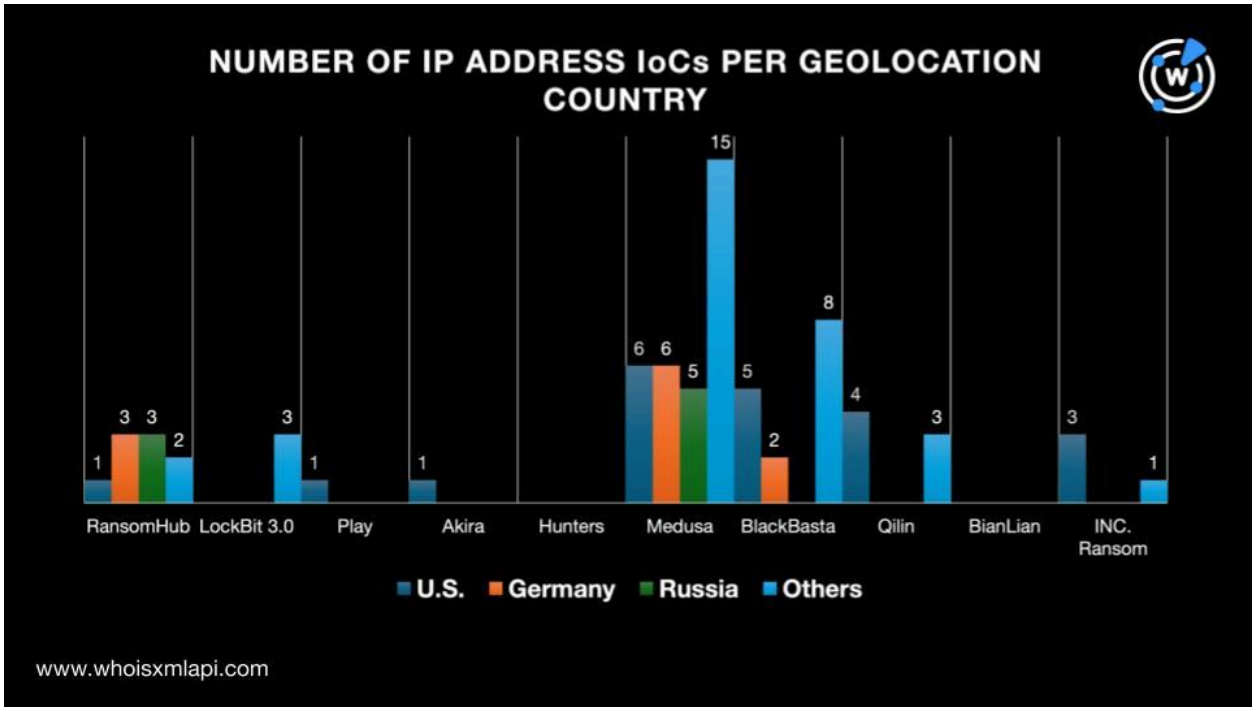


We also queried the 48 domains tagged as IoCs on DNS Chronicle API and found that 36 had historical domain-to-IP resolutions. The 36 domains had 3,905 resolutions over time. A total of 11 domains—capsonic[.]com, cornwelltools[.]com, grupcovesa[.]com, hacla[.]org, imacorp[.]com, piramal[.]com, sterlingcheck[.]com, and valleywomenshealth[.]com (LockBit 3.0); dict[.]gov[.]ph (Medusa); grabify[.]link (RansomHub); and malicious-domain[.]com (BlackBasta)—posted the oldest resolution date—4 October 2019. Take a look at DNS Chronicle API details for five domains below.

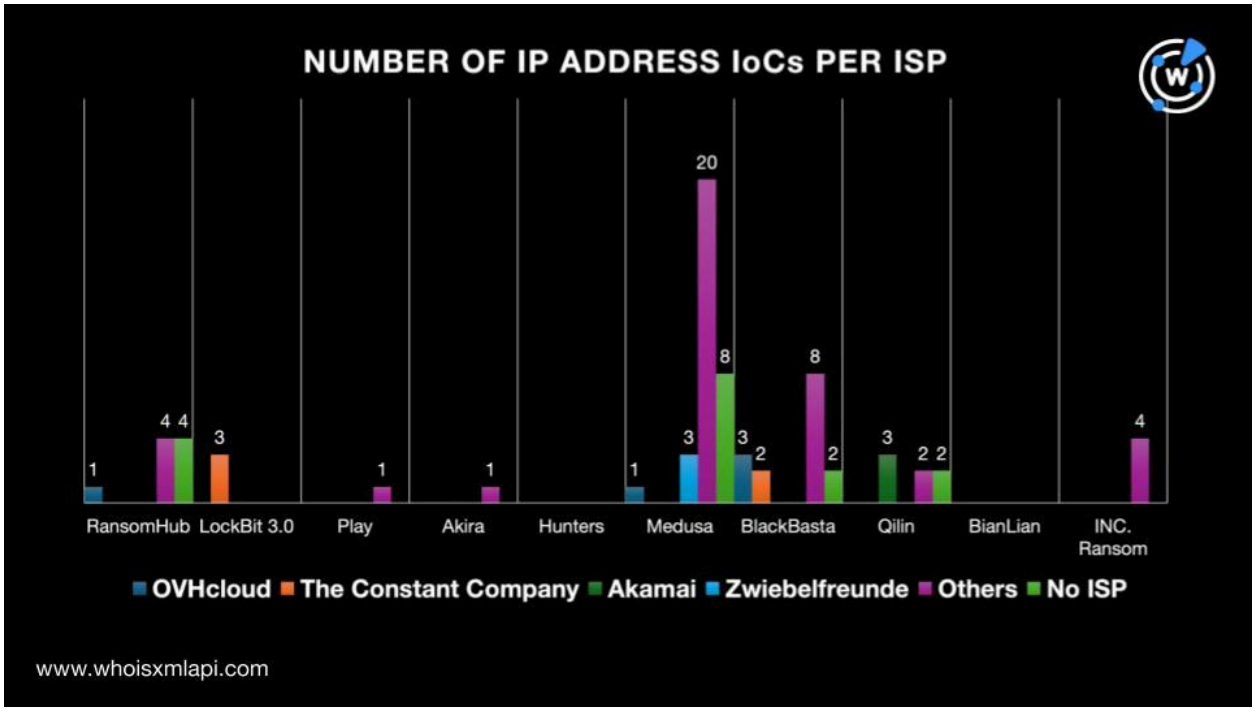
DOMAIN IoC	NUMBER OF IP RESOLUTIONS	FIRST IP RESOLUTION DATE
12301230[.]co (RansomHub)	44	16 July 2023
americajobmail[.]site (Play)	17	24 July 2023
attacker-server[.]com (BlackBasta)	55	17 December 2021
cobcreditunion[.]com (LockBit 3.0)	46	5 October 2019
cybersecsentinel[.]com (INC. Ransom)	14	14 February 2024

Next, we queried the 72 IP addresses identified as IoCs on Bulk IP Geolocation Lookup and discovered that:

- They originated from 22 different countries topped by the U.S., which accounted for 21 IP addresses. Germany took the second spot with 11 IP addresses. Russia came in third place with eight IP addresses. The Netherlands accounted for six IP addresses while Singapore accounted for four. Austria, Canada, France, Lithuania, and Switzerland accounted for two IP addresses each. Finally, one IP address each was geolocated in China, the Czech Republic, Hungary, Italy, Latvia, Moldova, Poland, Romania, South Africa, the U.A.E., Ukraine, and Vietnam.



- The 56 IP addresses with ISP information were administered by 41 different ISPs. OVHcloud and The Constant Company were the top ISPs, accounting for five IP addresses each. Akamai and Zwiebelfreunde tied in second place with three IP addresses each. Hivelocity, Selectel, and Stark Industries took the third spot with two IP addresses each. AlexHost, Alibaba, AT&T, BeGet, Charter Communications, Cherry Servers, Clouvider, Comcast, DHUB, DigitalOcean, EDIS, EvosHosting, F3 Netze, FBW Networks, Fiber Gride, FranTech Solutions, Green Floid, Hetzner Online, IWACOM, Latitude.sh, Linode, Magenta Telekom, Mediacom Communications, Microsoft, Namecheap, Nubes, OKB Progress, ServerAstra, Shock Hosting, Simoresta, VDSINA, Verizon, ViewQwest, and VNPT accounted for one IP address each. Finally, 16 IP addresses did not have ISPs on record.



We also queried the 72 IP addresses tagged as IoCs on DNS Chronicle API and found that 56 had historical IP-to-domain resolutions. Specifically, the 56 IP addresses recorded 7,171 domain resolutions over time. Three IP addresses—104[.]86[.]182[.]8 and 209[.]197[.]3[.]8 (Qilin) and 91[.]219[.]236[.]204 (Medusa)—recorded the oldest domain resolution date—4 October 2019. Take a look at DNS Chronicle API details for five IP addresses below.

IP ADDRESS IoC	NUMBER OF DOMAIN RESOLUTIONS	FIRST DOMAIN RESOLUTION DATE
104[.]187[.]107[.]81 (BlackBasta)	14	19 November 2021
108[.]11[.]30[.]103 (Medusa)	13	19 November 2021
139[.]180[.]184[.]147 (LockBit 3.0)	41	2 July 2021
154[.]12[.]242[.]58 (INC. Ransom)	49	4 December 2024
172[.]96[.]137[.]224 (Play)	14	24 July 2023

IoC List Expansion Findings

After unearthing more information on the IoCs, we further proceeded with our IoC list expansion.

First, we queried the 48 domains identified as IoCs on WHOIS History API and found that 26 had email addresses in their historical WHOIS records. In fact, the 26 domains had 252 email addresses after duplicates were filtered out. Upon closer examination, 44 email addresses were public.

We then queried the 44 public email addresses on Reverse WHOIS API and discovered that 30 appeared in the historical WHOIS records of 944 domains after duplicates and those already tagged as IoCs were filtered out.

A Threat Intelligence API query for the 944 email-connected domains showed that 27 were already considered malicious. Take a look at five examples below.

MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT
aaaeieiiiofffpn[.]su	Malware distribution
arculus[.]su	Malware distribution
eoufaoeuhoauengi[.]su	Generic threat
mertonera[.]su	Malware distribution
podisong[.]su	Malware distribution

Next, we queried the 48 domains identified as IoCs on DNS Lookup API and discovered that 30 currently resolve to 48 IP addresses after duplicates and those already tagged as IoCs were filtered out.

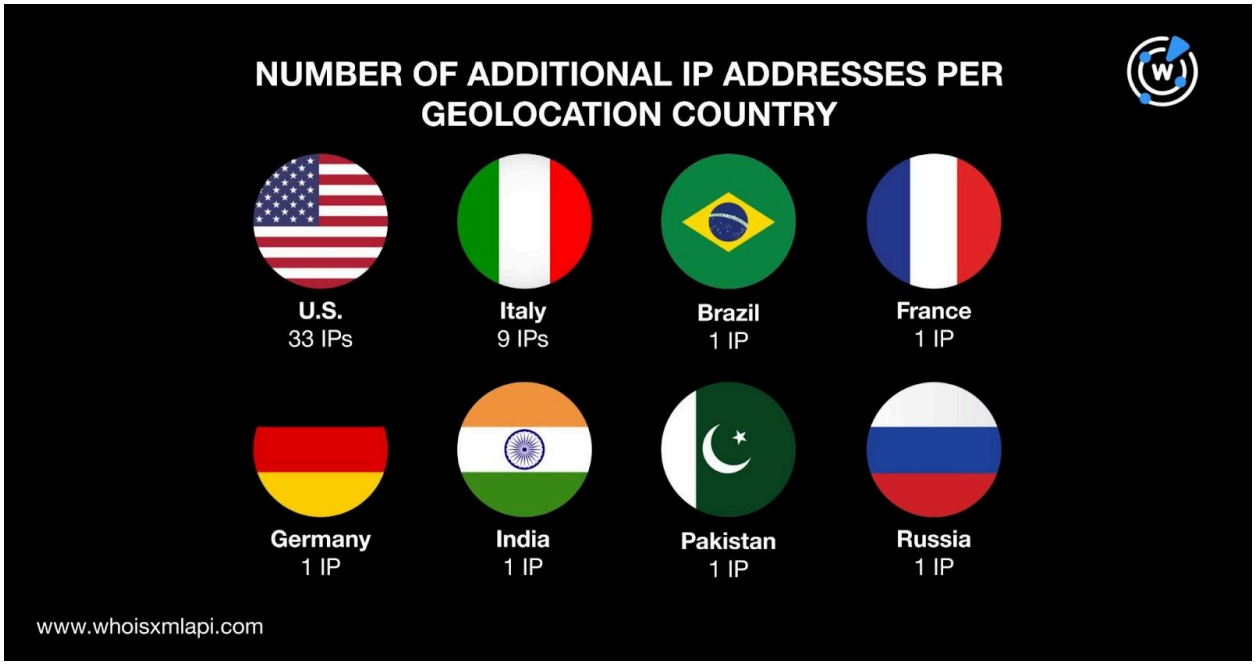
A Threat Intelligence API query for the 48 additional IP addresses revealed that 34 have already figured in malicious campaigns. Take a look at five examples below.

MALICIOUS ADDITIONAL IP ADDRESS	ASSOCIATED THREAT
104[.]21[.]79[.]68	Malware distribution Phishing
154[.]199[.]243[.]231	Malware distribution

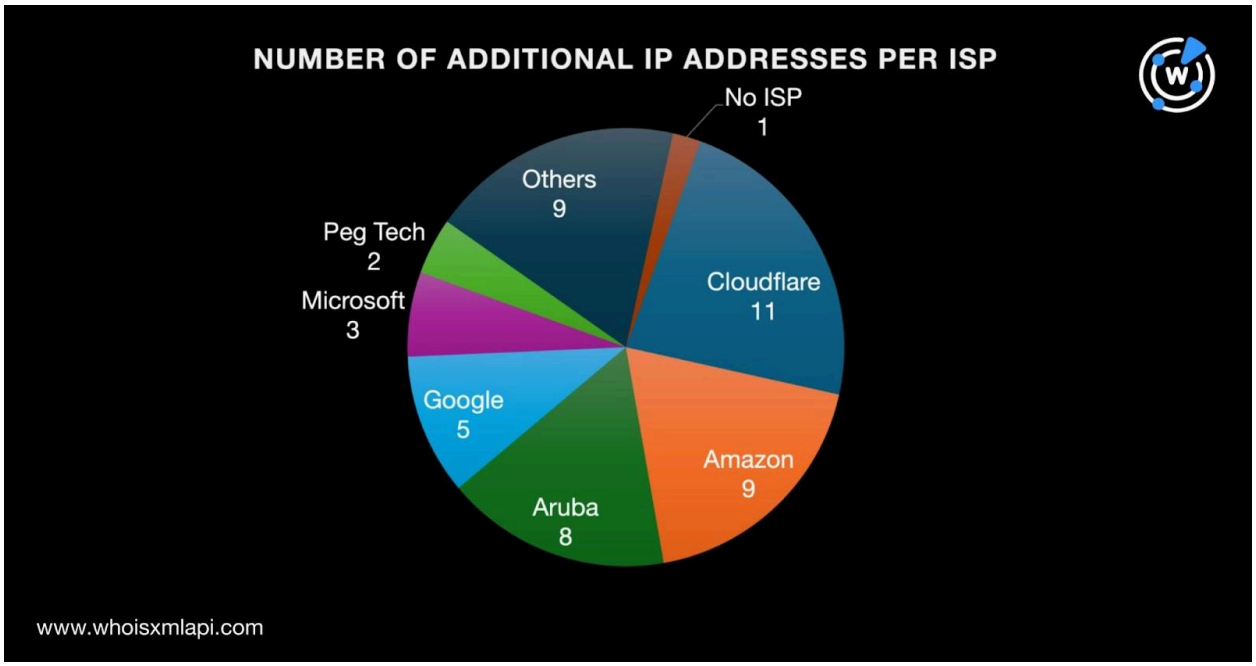
172[.]67[.]169[.]60	Malware distribution Phishing
34[.]132[.]102[.]6	Attack Command and control (C&C) Generic threat Malware distribution Phishing
52[.]217[.]227[.]85	Generic threat

A Bulk IP Geolocation Lookup query for the 48 additional IP addresses showed that:

- They were geolocated in eight different countries led by the U.S., which accounted for 33 IP addresses. Italy came in second place with nine IP addresses. One IP address each originated from Brazil, France, Germany, India, Pakistan, and Russia.



- A total of 47 of them had ISPs on record. Cloudflare took the top spot with 11 IP addresses. Amazon accounted for nine IP addresses while Aruba accounted for eight. In third place came Google with five IP addresses. Microsoft administered three IP addresses while Peg Tech administered two. One IP address each was administered by DDoS-Guard.net, InMotion Hosting, IRIDEOS, OVHcloud, PTCL, RAKsmart, Scala Data Centers, Suddenlink Communications, and The Constant Company. Finally, one IP address did not have an ISP on record.



Now, by combining the 72 IP addresses identified as IoCs and the 48 additional we uncovered, we had 120 IP addresses in all for the remainder of our analysis.

We queried the 120 IP addresses on Reverse IP API and found that 72 had current IP-to-domain resolutions. In fact, the 72 IP addresses hosted 12,054 domains in all. Closer scrutiny showed that 33 of the IP addresses could be dedicated hosts. The 33 dedicated IP addresses hosted 201 domains after duplicates, those already tagged as IoCs, and the email-connected domains were filtered out.

A Threat Intelligence API query for the 201 IP-connected domains revealed that two were have already been weaponized for attacks. An example would be ikea0[.]com, which was associated with malware distribution. Note the appearance of the IKEA brand name in the malicious domain. It could have been used in an attack targeting the company or its customers.

As the final step, we scrutinized the 48 domains tagged as IoCs and found that they started with 40 unique text strings. Domains & Subdomains Discovery searches revealed that 29 strings appeared in 1,192 domains after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out. Here are the 29 text strings.

- 12301230.
- 40031.
- americajobmail.
- attacker-server.
- capsonic.
- cobcreditunion.

- cornwelltools.
- dict.
- electronicsystem.
- grabify.
- grupcovesa.
- hacla.
- huntersinternational.
- imacorp.
- inara.
- malicious-domain.
- manfil.
- osintcorp.
- piramal.
- requests.
- rimex.
- samuelelena.
- socket.
- sterlingcheck.
- swiftatlanta.
- tecnosysitalia.
- valleywomenshealth.
- vulnerableapp.
- winscp.

A Threat Intelligence API query for the 1,192 string-connected domains revealed that three were already associated with various threats. An example would be electronicsystem[.]ml, which was considered a generic threat.

—

Our analysis of the 120 IoCs connected to 2025's top ransomware families comprising 48 domains and 72 IP addresses led to the discovery of 2,385 artifacts. We specifically unearthed 944 email-connected domains, 48 additional IP addresses, 201 IP-connected domains, and 1,192 string-connected domains. In addition, we found that 66 of the artifacts—32 domains and 34 IP addresses—have already been weaponized for various attacks.

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

- 01vikings[.]su
- 1mosaic[.]biz
- 1mosaic[.]co
- aaaeieiiiofffpn[.]su
- aauaaaeieiieepn[.]su
- abcstore[.]su
- baesystemsindia[.]com
- bancobpm-autenticazione[.]com
- banusdore[.]su
- caldas[.]mobi
- caldasnovas[.]mobi
- candclawncare[.]com
- danubiacrispim[.]com[.]br
- darkjabber[.]su
- darkode[.]su
- e3housing[.]com
- e3housing[.]org
- e3hsg[.]com
- facaumpedido[.]com
- facilitateco[.]com
- fafhoafouehfufh[.]su
- gallatincomputers[.]com
- gallatincomputersystems[.]com
- gallatinwomenscenter[.]com
- hacla[.]biz
- hagantodd[.]com
- hagantoddlaw[.]com
- ic-meats[.]com
- icmeats[.]com
- imaclaims[.]com
- jackwardplumbing[.]com
- jbryanlewislaw[.]com
- jcneumann[.]com
- kandiiworld[.]com
- karbocon[.]com
- karbocon[.]net
- lactocalaminereneu[.]com
- ladadensuarupddipl12343423233[.]info
- landtrusttn[.]org
- machadoealvarenga[.]com[.]br
- mackandkatecatering[.]com
- mackandkatescatering[.]com
- nahonfirm[.]com
- nandinipiramal[.]com
- napierdental[.]com
- ob1shinobi[.]com
- obgynvalley[.]com
- office365-en-update[.]com
- p0s3id0n[.]su
- paalai[.]su
- panulisib[.]com
- r2cia9ovmrqnwe5b[.]com
- rackz[.]su
- radiomusiclicense[.]com
- scotiatrinidad[.]com
- securedpccheck[.]com
- securitytestpin[.]com
- t-ignition[.]com
- talengenharia[.]com[.]br
- technicalpreviews[.]com
- uisdl[.]com
- ulefieskil[.]com
- un-tox[.]net
- vaikunthbypiramal[.]com
- vaikunthinthane[.]com
- vaikunthpiramal[.]com
- waldogrouplc[.]com
- wardp-m[.]com
- wayneadams[.]net
- xiheiufisd[.]su
- xternalia[.]com

- youweb-bancobpm[.]com
- yvex[.]su
- zeebira[.]su
- zimbabwe[.]su
- zimmerton[.]su

Sample Additional IP Addresses

- 104[.]18[.]41[.]237
- 104[.]21[.]79[.]68
- 104[.]26[.]8[.]202
- 20[.]40[.]40[.]148
- 216[.]194[.]167[.]111
- 221[.]120[.]239[.]84
- 34[.]132[.]102[.]6
- 34[.]136[.]111[.]81
- 34[.]174[.]132[.]235
- 45[.]196[.]180[.]161
- 45[.]32[.]205[.]26
- 51[.]116[.]98[.]156
- 52[.]216[.]205[.]26
- 52[.]216[.]39[.]45
- 62[.]149[.]128[.]154
- 62[.]149[.]128[.]157
- 62[.]149[.]128[.]160
- 94[.]23[.]82[.]202

Sample IP-Connected Domains

- 74-207-252-129[.]ip[.]linodeusercontent[.]com
- 75[.]117[.]168[.]109[.]host[.]static[.]ip[.]kpnqwest[.]it
- a111[.]dscw105[.]akamai[.]net
- a1531[.]g2[.]akamai[.]net
- a1531[.]g2[.]akamai[.]net[.]0[.]1[.]cn[.]akamaitech[.]net
- b-team[.]it
- bba-92-97-159-185[.]alshamil[.]net[.]ae
- brmeptr3[.]clientebrmedico[.]com[.]br
- c1102604[.]sgvps[.]net
- chipkin[.]ru
- cpanel[.]cutram[.]vn
- declercqjan[.]be
- decsx[.]freeddns[.]org
- demo[.]delivery4all[.]it
- fioredipuglai[.]com
- ftp[.]cutram[.]vn
- ftp[.]fioredipuglai[.]com
- galenmclean[.]giize[.]com
- gerli1870[.]it
- grantsac-heatng[.]com
- headachemeter[.]com
- hiyurukianpu[.]casacam[.]net
- icanhelp[.]in
- ikea0[.]com
- inara[.]io
- junglemagic[.]in
- lactocalamine[.]in
- lemarkcentr[.]ru
- lemarkel[.]ru
- mail-vi1eur05olkn2105[.]outbound[.]protection[.]outlook[.]com
- mail[.]ankeweber[.]at
- mail[.]blackout-detector[.]com
- naturolax[.]in
- neko[.]co[.]in
- nfnas01[.]direct[.]quickconnect[.]to
- pchf[.]in
- piramalfoundation[.]org
- piramalhousing[.]in
- quikkool[.]in

- relay-2a705639[.]net[.]anydesk[.]com
- sharpsoftstudio[.]it
- shop[.]belom[.]it
- sloans[.]co[.]in
- terofmail[.]com
- test[.]sonicle[.]com
- throatsil[.]in
- web[.]bernietravis[.]accesscam[.]org
- web[.]galenmclean[.]giize[.]com
- web[.]ricohneal[.]kozow[.]com
- yaoyeyuruki[.]ddnsfree[.]com
- zaqiikoush[.]kozow[.]com

Sample String-Connected Domains

- 12301230[.]cc
- 12301230[.]cn
- 12301230[.]com
- 40031[.]biz
- 40031[.]cc
- 40031[.]club
- attacker-server[.]de
- capsonic[.]app
- capsonic[.]co[.]kr
- capsonic[.]eu
- cobcreditunion[.]co
- cornwelltools[.]co
- cornwelltools[.]co[.]uk
- cornwelltools[.]eu
- dict[.]ac
- dict[.]ac[.]cn
- dict[.]ac[.]ke
- electronicsystem[.]biz
- electronicsystem[.]co
- electronicsystem[.]co[.]in
- grabify[.]ai
- grabify[.]app
- grabify[.]asia
- hacla[.]cc
- hacla[.]cl
- hacla[.]cn
- huntersinternational[.]cc
- huntersinternational[.]co[.]uk
- huntersinternational[.]com
- imacorp[.]be
- imacorp[.]biz
- imacorp[.]cl
- inara[.]academy
- inara[.]ae
- inara[.]agency
- malicious-domain[.]org
- manfil[.]club
- manfil[.]cn
- manfil[.]com
- osintcorp[.]ca
- osintcorp[.]com
- osintcorp[.]digital
- piramal[.]app
- piramal[.]chat
- piramal[.]cloud
- requests[.]agency
- requests[.]ai
- requests[.]app
- rimex[.]ac[.]cn
- rimex[.]agency
- rimex[.]arab
- samuelelena[.]com
- socket[.]agency
- socket[.]ai
- socket[.]app
- sterlingcheck[.]ai
- sterlingcheck[.]app
- sterlingcheck[.]au
- swiftatlanta[.]net
- tecnosysitalia[.]cloud

- tecnosysitalia[.]com
- tecnosysitalia[.]it
- valleywomenshealth[.]co
- valleywomenshealth[.]org
- vulnerableapp[.]ml
- winscp[.]app
- winscp[.]audnedaln[.]no
- winscp[.]best