What Remains of Black Basta Now That Alleged Gang Leader Joined the Most Wanted List?

Table of Contents

Executive Report

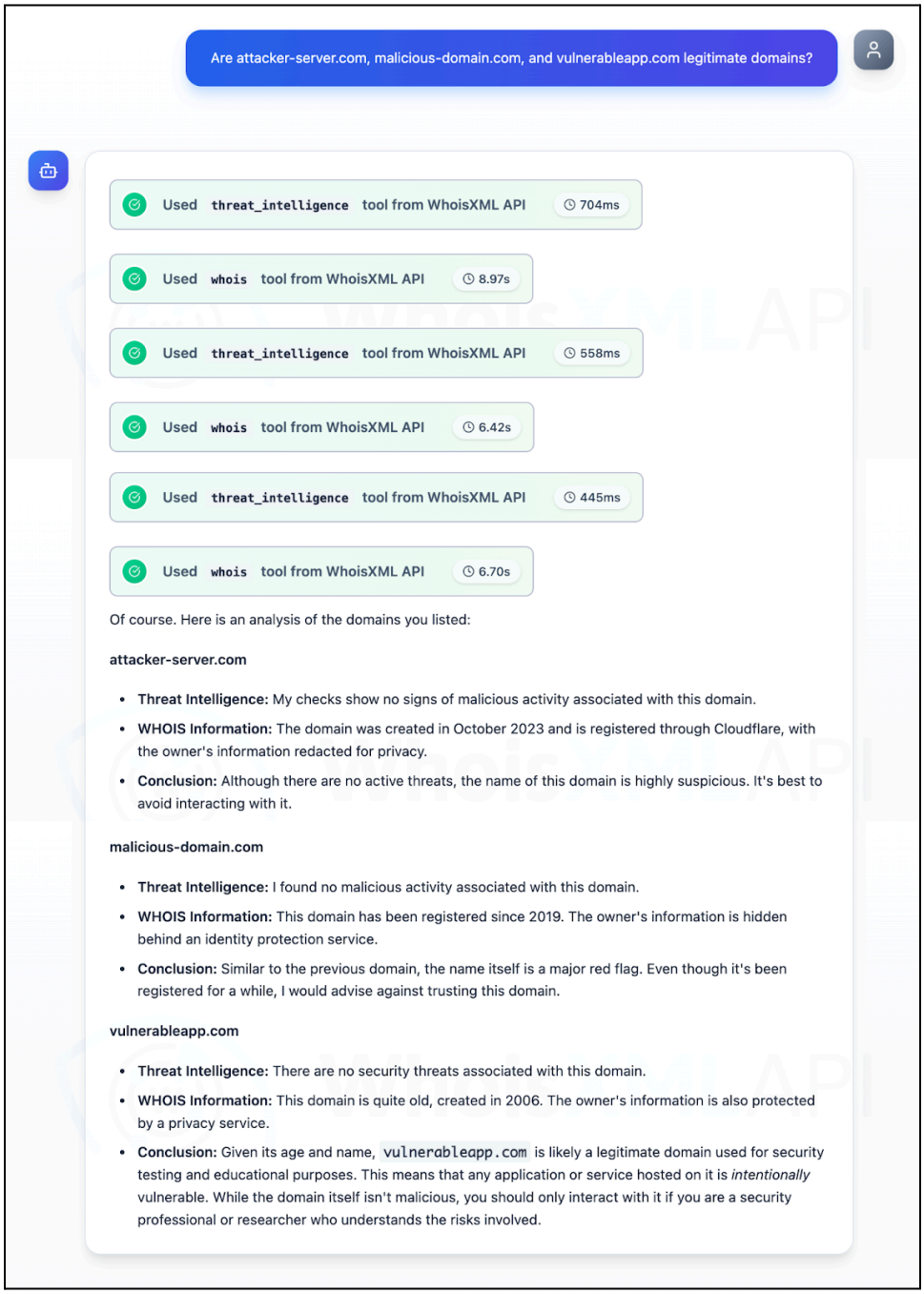
The Hacker News reported that the alleged leader of the BlackBasta Ransomware Gang, 35-year-old Russian national Oleg Evgenievich Nefedov, has been added to the EU's Most Wanted and INTERPOL's Red Notice lists.

Over time, Black Basta affiliates have become known for using common initial access techniques like phishing and exploiting known vulnerabilities and then employing a double-extortion model. They not only encrypted systems but also exfiltrated data. In addition, their ransom notes did not generally include initial ransom demands or payment instructions. Instead, these provided victims with unique codes and instructed them to contact the ransomware group via a .onion URL reachable through the Tor browser. The actors typically gave victims 10–12 days to pay the ransom before they published the stolen data on the Black Basta TOR site dubbed "Basta News."

Security researchers publicized 27 network IoCs related to one of the most recent Black Basta campaigns. We analyzed 18 of these IoCs and uncovered these findings:

- Five unique potential victim IP addresses communicated with the 15 IP addresses identified as IoCs
- 7,560 email-connected domains, 482 of which turned out to be malicious
- Two additional IP addresses
- Seven IP-connected domains
- 1,572 string-connected domains, four of which turned out to be malicious

Note that we focused on only three of the 12 domains the researchers identified as IoCs after checking their legitimacy and current state of responsiveness via Jake AI. We did, however, keep the list of 15 IP addresses tagged as IoCs as is.

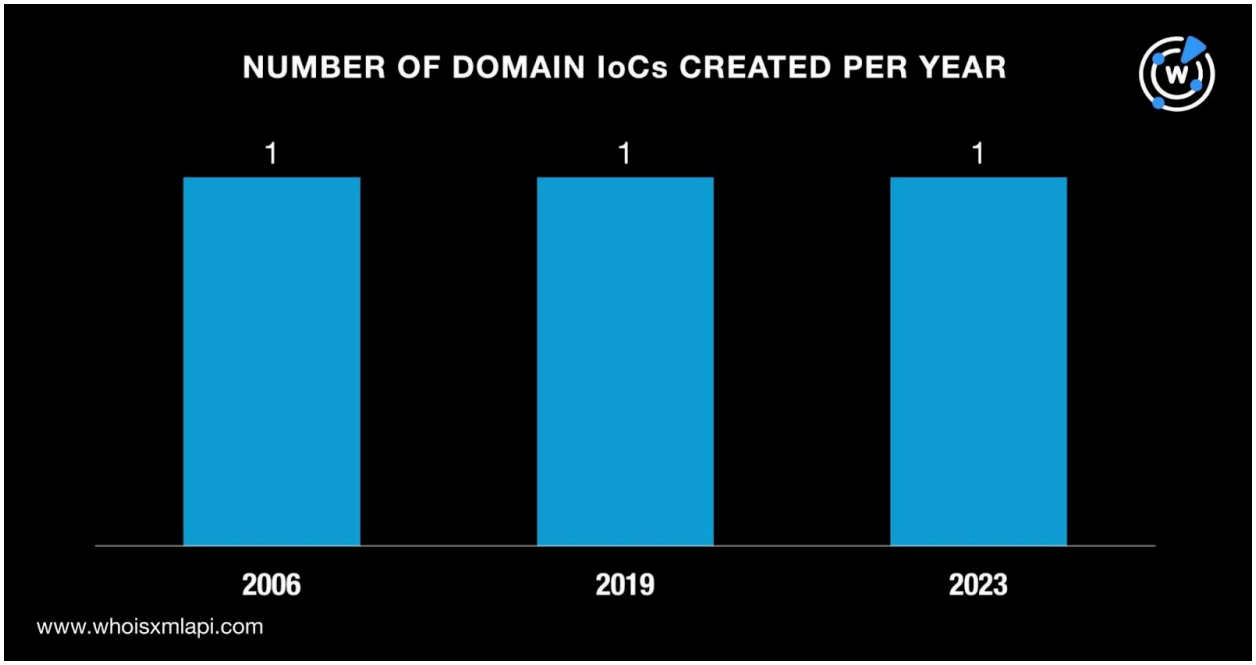


Sample Jake AI query result for checking the legitimacy of the domains identified as IoCs

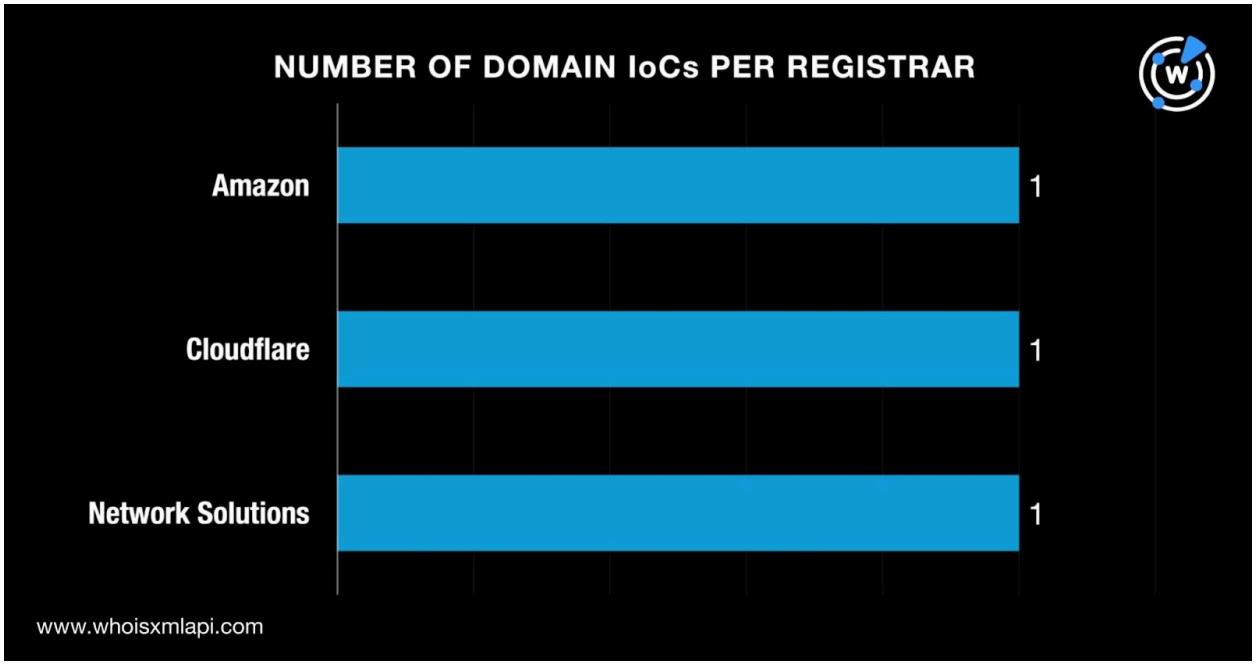
A Deep Dive to Learn More about the Domain IoCs

As mentioned earlier, we zoomed in on three domains identified as IoCs in our analysis. Our WHOIS API queries for them revealed that:

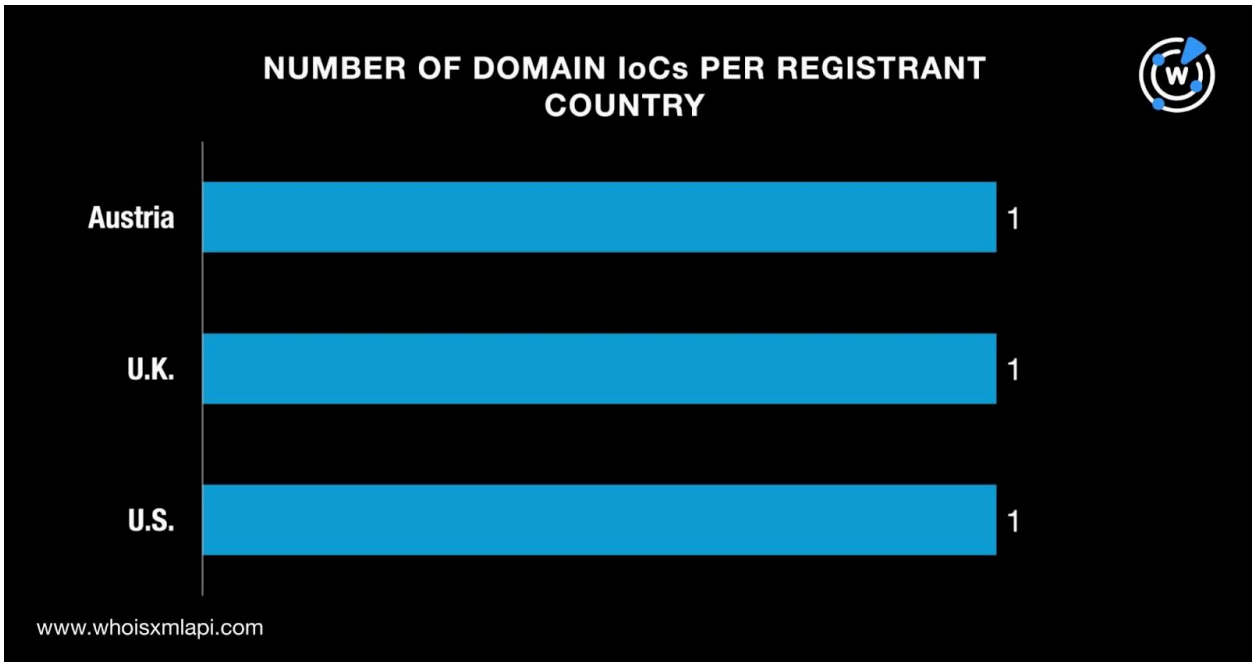
- They were created between 29 December 2006 and 6 October 2023, making them relatively old at the time they figured in the attack.



- Each of them was administered by a different registrar.



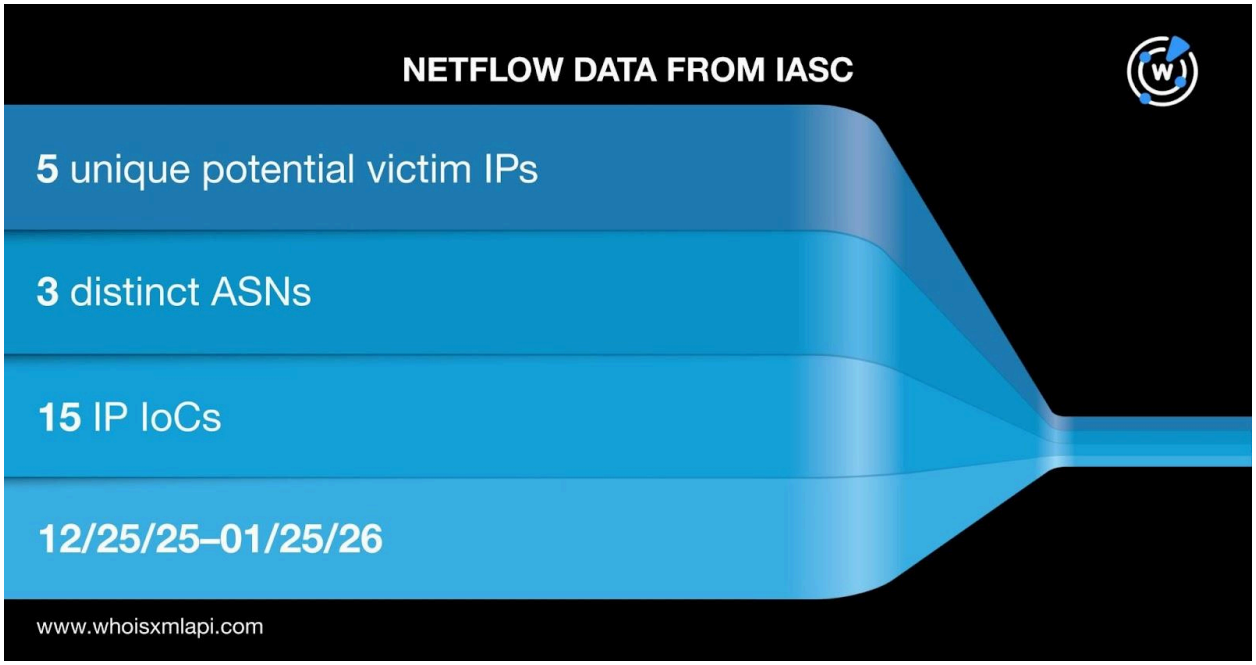
- And similarly, they were registered in three different countries.



DNS Chronicle API queries for the three domains tagged as IoCs showed that together, they recorded 418 domain-to-IP resolutions over time. The domain vulnerableapp[.]com posted the oldest resolution on 7 February 2017. It also recorded 301 resolutions until 18 January 2026.

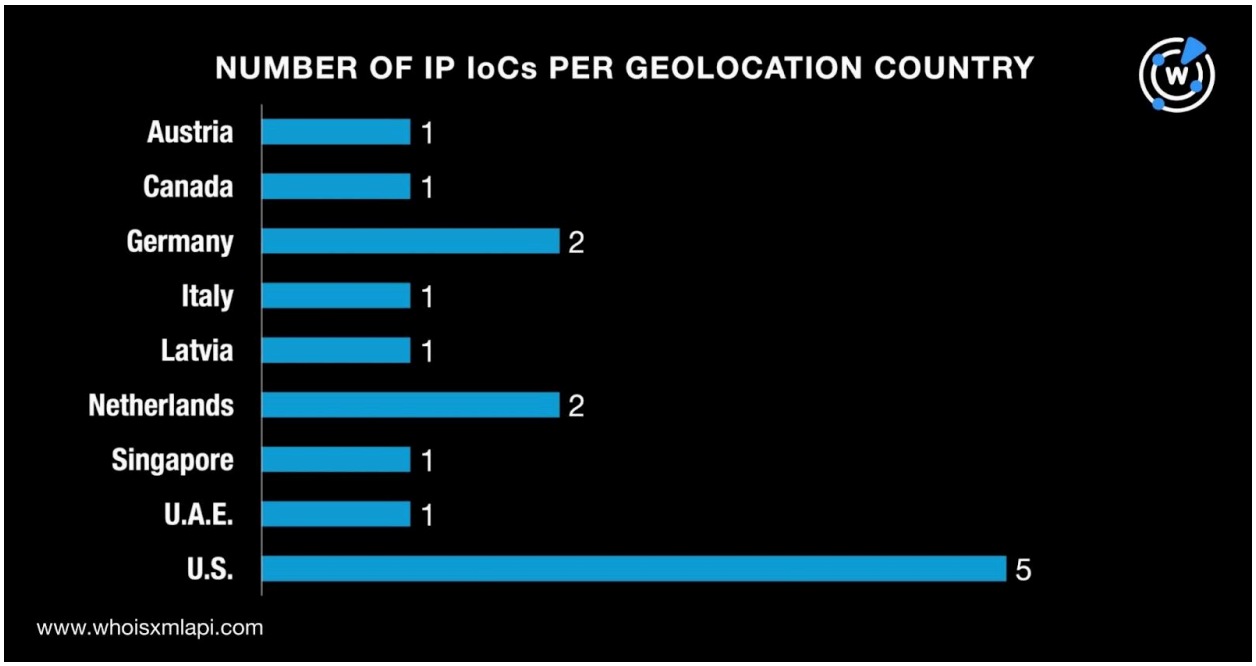
An In-Depth Probe into the DNS Traces of the IP IoCs

Sample network traffic data from the IASC revealed that five unique potential victim IP addresses under three distinct ASNs communicated with the 15 IP addresses identified as IoCs between 25 December 2025 and 25 January 2026.

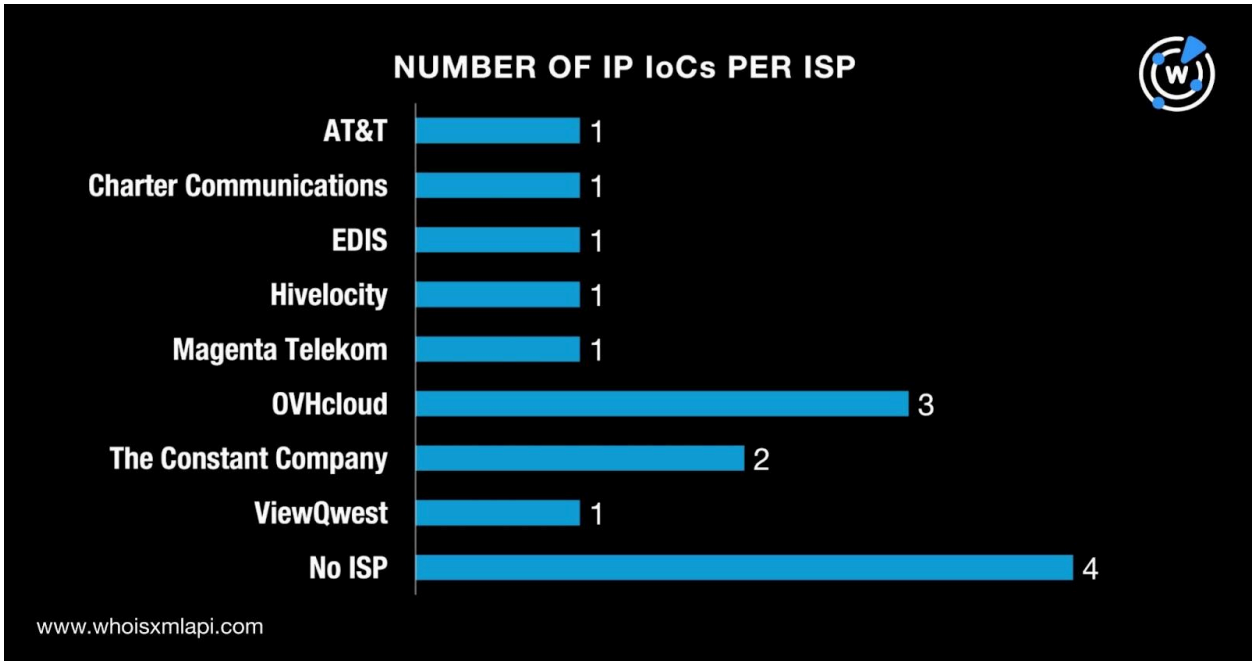


We then queried the 15 IP addresses tagged as IoCs on Bulk IP Geolocation Lookup and discovered that:

- They were geolocated in nine different countries, including Austria and the U.S., which were among the domain IoCs' registrant countries.



- And while four of them did not have ISPs on record, the remaining 11 were administered by eight different ISPs.



Next, we queried the 15 IP addresses identified as IoCs on DNS Chronicle API and found out that 14 of them recorded 3,722 IP-to-domain resolutions over time.

IP IoC	NUMBER OF RESOLUTIONS	FIRST RESOLUTION DATE	LAST RESOLUTION DATE
104[.]187[.]107[.]81	258	02/04/17	01/17/26
213[.]47[.]213[.]243	1,000	02/05/17	12/13/19
92[.]97[.]159[.]185	341	02/05/17	07/21/25
76[.]80[.]4[.]222	333	02/06/17	10/07/25
91[.]204[.]248[.]6	213	03/15/19	01/20/26

While the IP address 104[.]187[.]107[.]81 posted the oldest first resolution on 4 February 2017, the IP address 213[.]47[.]213[.]243 recorded the highest number of resolutions at 1,000. It is also interesting to note that four of the IP addresses identified as IoCs first resolved domains within days of each other.

The Quest to Find New Artifacts

To uncover new artifacts, we first queried the three domains tagged as IoCs on WHOIS History API and learned that together, they had 63 unique email addresses in their historical WHOIS records. Careful scrutiny, however, revealed that only two were public email addresses.

Reverse WHOIS API queries for the two email addresses showed that both appeared in the historical WHOIS records of various domains. This step led to the discovery of 7,560 unique email-connected domains after those already identified as IoCs were filtered out.

The results of our Threat Intelligence API queries for the email-connected domains revealed that 482 have already been weaponized for various attacks.

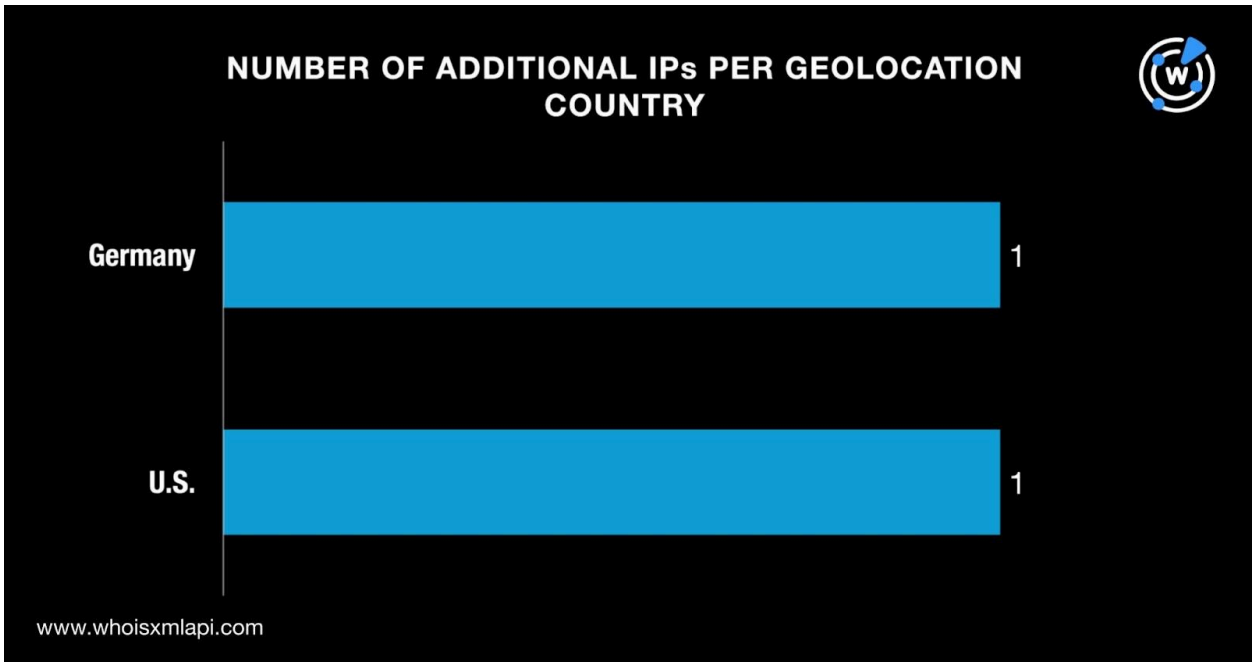
MALICIOUS EMAIL-CONNECTED DOMAIN	ASSOCIATED THREAT	DATES SEEN
bevgfijycd[.]net	Malware distribution C&C	03/09/23–01/25/26 03/09/23–01/25/26
bndduftnfteu[.]com	Malware distribution C&C	03/09/23–01/25/26 03/09/23–01/25/26
btpnxlsfdqbhzazyx[.]net	Malware distribution C&C	03/09/23–01/25/26 03/09/23–01/24/26
bwoslmylnsrr[.]biz	Malware distribution C&C	03/09/23–01/25/26 03/09/23–01/24/26
cgbbwfffnvgh[.]com	Malware distribution C&C	03/09/23–01/25/26 03/09/23–01/24/26

It is worth noting that several of the malicious email-connected domains not only resembled one another in terms of makeup (likely created using a DGA) but were also detected as malicious on the same date—9 March 2023.

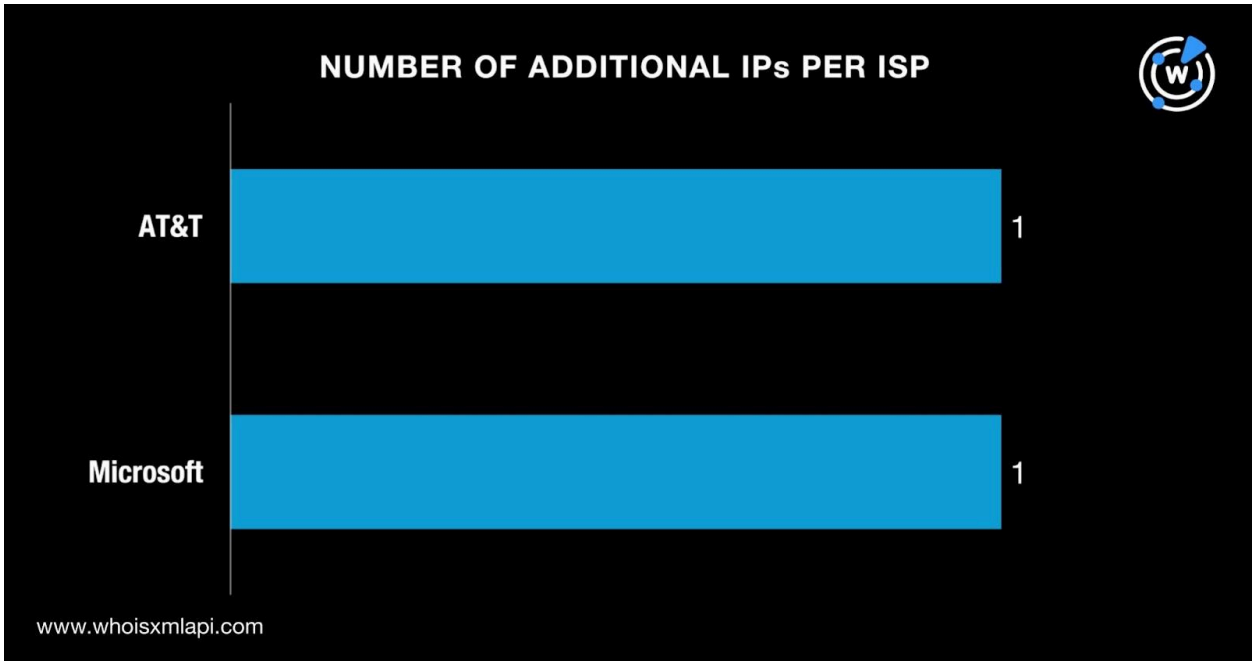
We then queried the three domains identified as IoCs on DNS Lookup API and found out that they resolved to two unique IP addresses that were not part of the IoC list.

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

- They were geolocated in different countries, both of which were on the IP IoCs' list of geolocation countries.



- They were also administered by different ISPs, including AT&T, which was listed as one of the ISPs of the IP IoCs.



Adding the two additional IP addresses to the 15 tagged as IoCs, we now had 17 IP addresses for further analysis. Reverse IP API queries for them revealed that five could be dedicated

hosts. This finding led to the discovery of seven unique IP-connected domains after those already identified as IoCs and the email-connected domains were filtered out.

After that, we took a closer look at the three domains tagged as IoCs (and those we excluded from our analysis) and extracted these six unique text strings for Domains & Subdomains Discovery searches:

- attacker-
- attacker-server.
- malicious-
- malicious-domain.
- vulnerableapp.
- vulnerable

All of them appeared at the start of domains other than those already on the IoC list. That said, we found 1,572 unique string-connected domains after the IoCs and email- and IP-connected domains were filtered out.

Threat Intelligence API queries for the string-connected domains showed that four have already figured in various attacks. The domain attacker-domain[.]com, for instance, has already been used to distribute malware.

Conclusion

Our analysis of 18 of the IoCs related to one of the latest Black Basta attacks revealed that five unique potential victim IP addresses communicated with the 15 IP addresses identified as IoCs between 25 December 2025 and 25 January 2026.

We also uncovered 9,141 new artifacts comprising 7,560 email-connected domains, two additional IP addresses, seven IP-connected domains, and 1,572 string-connected domains. These newfound connected properties could mean that despite the identification and inclusion of the gang's leader in two most wanted lists, their malicious infrastructure is still hard at work. In fact, 486 of them have already been classified as malicious to date.

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

- 020318789436136918[.]com
- 02616secureserver[.]com
- 029ad5a9fd1f[.]com
- a-protectppal[.]com
- a2zmp3s[.]com
- a8ezkv1479m3soz382u3heihx[.]com
- b0huj492nstu[.]net
- b25xq2hc3ypmrgt75z[.]com
- b345345534b3455434[.]net
- c01hs64gnd93d73d[.]cc
- c1zng51dtkzfxsuvowb1enz17v[.]com
- c2344665443443vf[.]net
- d-scr[.]com
- d24flare[.]com
- d3akotav33olandos[.]com
- e-checkouts[.]com
- e-securelib[.]com
- e-tarruf[.]com
- f0hyjk5yjc9e[.]org
- f20pre[.]com
- f2rf3k1qsvzxv1y7kumxutbeq0[.]com
- g2cioiw64ac2[.]net
- g459jrj0gd[.]com
- g5aj4hej0xmr[.]net
- h0n250vi9oje[.]net
- h15lzz104ym1i5aiwfo1b56s49[.]com
- h2jw1y7g1e7c[.]net
- i1gf9b1y0pfr110geexwgypear[.]com
- i2uaam2u6eay[.]org
- iaddidea[.]com
- j0h2h9q8[.]info
- j45uf4pm7ol6[.]net
- j4xburj6p84rupx45byf3kfj[.]com
- k2kmsawmwqgu[.]org
- k35285-static[.]com
- k3mx4b6dsbut[.]com
- l0nel0ne[.]com
- l0nk0s0[.]com
- l2nsdi7clyrw[.]net
- m-ali[.]biz
- m0t0n0[.]com
- m1onoliowners1[.]com
- n092vchy74tu[.]net
- n254x0md9gzv4s5f6o70voq5a[.]info
- n3y2l2h8[.]info
- o1ezwpqfshin[.]com
- o7j3udp3e3sdqgbtgl[.]biz
- oafscxumipqicnta[.]com
- p0d3n9m9[.]info
- p0werfull[.]com
- p2p-static[.]com
- q39fuiz5hhdm[.]com
- q4i86oi86se8[.]net
- q5eeos998bj7tixzxmjpylba[.]com
- r-sbonline[.]org
- r01mzk1qnsdq[.]org
- r4j54j50j0[.]com
- s-google[.]net
- s186598balooba125[.]com
- s2advancecontrolspeed[.]com
- t3onyghop[.]com
- t5ckatszkfjrfywvws[.]com
- tabosus[.]com
- u02jdnd82hdnqpu[.]cc
- u42kisq0qses[.]com
- u9yi8m1tjxuoh136tjt21t4jtwy[.]com
- v0dirw12v0dq[.]com
- v0y493[.]com
- v1hca0c7qew3o[.]biz
- w1qno1yjo1qn[.]com
- w1s2d3[.]com

- w1v5u0e1[.]info
- x-cash-x[.]com
- x0x0l[.]com
- x55f3zqjqmy7igyczw[.]com
- y25qwrmzv6z3nwem5mnry21smg[.]com
- y5xaoczyvw5[.]com
- yabsnap[.]com
- z21k5o1ublcvw1d8grtp7zrxtc[.]com
- z2hgng43fgjl82309dfg99df1[.]com
- z2hgng44fgjl82509dfg90df[.]com

Sample Additional IP Address

- 51[.]116[.]98[.]156

Sample IP-Connected Domains

- mta01[.]witel[.]it
- remarka[.]io
- vpn[.]coldstoragemfg[.]com

Sample String-Connected Domains

- attacker-0111[.]tk
- attacker-aaradhya[.]xyz
- attacker-ai[.]com
- attacker-server[.]de
- malicious-317[.]net
- malicious-a[.]cf
- malicious-abdicate[.]xyz
- malicious-domain-registration-system[.]cf
- malicious-domain[.]org
- vulnerableapp[.]ml
- vulnerable-68[.]ws
- vulnerable-accruing[.]tk
- vulnerable-adults-europe[.]com