WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

APT37 Strikes Again, This Time with NarwhalRAT

Threat Report

Table of Contents

Executive Report

Genians Security Center researchers uncovered a new APT37 campaign leveraging NarwhalRAT, a malware designed to steal data via keylogging, screen capturing, USB data collection, and remote code execution.

The researchers believed initial access was achieved through spearphishing emails disguised as messages from the Microsoft account team and various cybersecurity advisories. Malicious LNK files then induced the installation of NarwhalRAT in the form of a compiled Python script. The threat actors also seemed to operate a dual C&C structure that used a Korean relay server and the pCloud API as a dead-drop resolver.

North Korean state-sponsored cyber espionage group APT37 has been active since at least 2012 and primarily targeted South Korea, Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other Middle East countries. It has also been linked to several campaigns seen between 2016 and 2018 like Operation Daybreak, Operation Erebus, Golden Time, Evil New Year, Are You Happy?, FreeMilk, North Korean Human Rights, and Evil New Year 2018.

Genians identified 11 network IoCs comprising five domains and six IP addresses related to the attack. After verifying that none of the domain IoCs were owned by legitimate entities via the WhoisXML API MCP Server, we analyzed all the IoCs, which led to these pertinent findings:

- One client IP address that communicated with a domain IoC
- 77 unique IP addresses potentially owned by victims that communicated with six of the IP IoCs
- 79 email-connected domains
- 792 IP-connected domains
- 17 string-connected domains

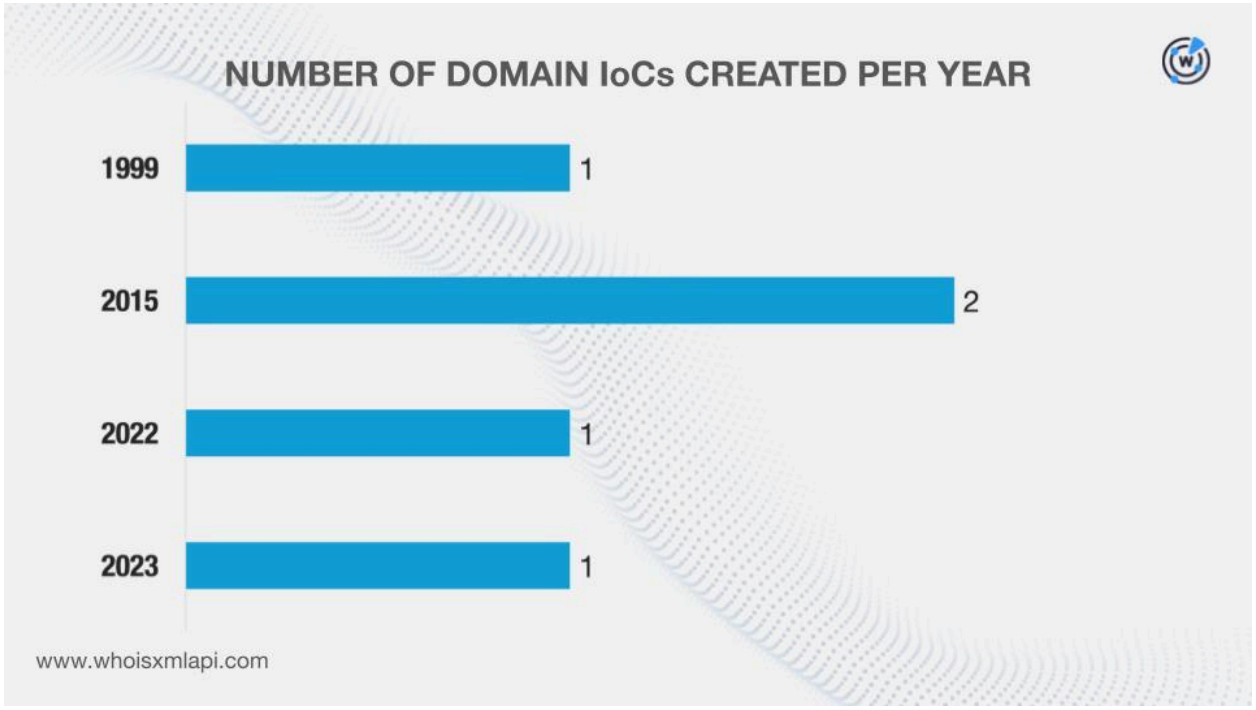
APT37 NarwhalRAT Attack Domain IoCs Dissected

We kicked off our in-depth investigation of the APT37 NarwhalRAT attack by looking more closely at the five domain IoCs.

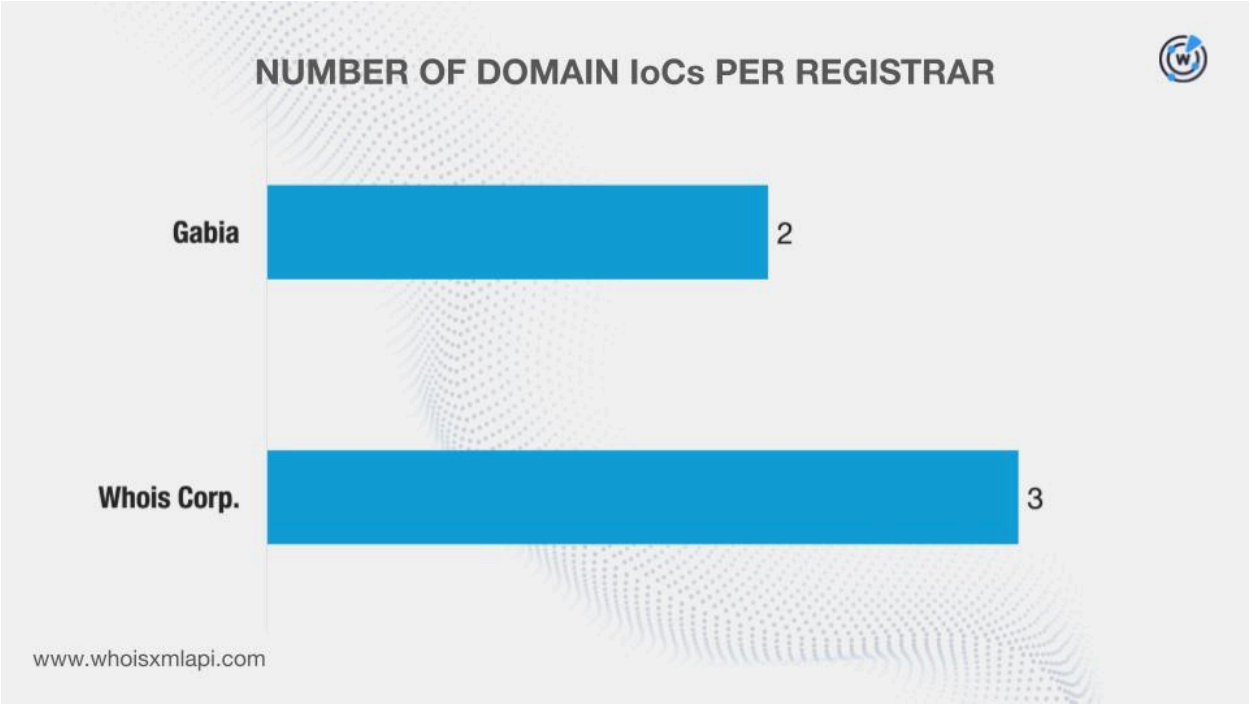
First, sample network traffic data from the IASC revealed that one client IP address communicated with the domain IoC novel21[.]co[.]kr via 24 DNS queries between 21 and 25 May 2026.

We then queried the domain IoCs on [WHOIS API] and discovered that:

- They were created between 12 April 1999 and 4 September 2023, hinting at APT37's preference for using aged domains for this particular campaign.



- They were administered by two registrars.



- While two did not have registrant countries on record, the remaining three were registered in South Korea.

Next, we queried the domain IoCs on DNS Chronicle API and learned that they all recorded 966 historical domain-to-IP resolutions over time. Take a look at more information for three examples below.

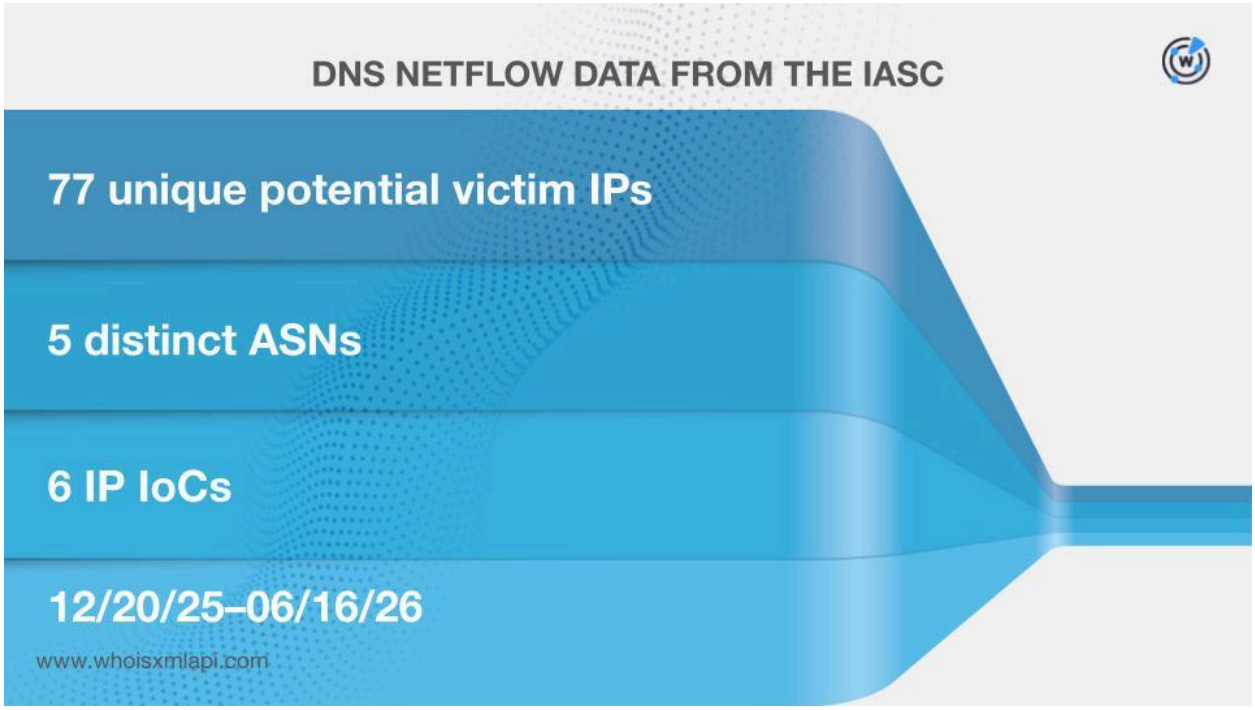
DOMAIN IoC	NUMBER OF DOMAIN-TO-IP RESOLUTIONS	DATES SEEN
webhostingkorea[.]com	329	02/05/17–05/26/26
novel21[.]co[.]kr	288	02/06/17–05/03/26
daehoat[.]com	286	04/28/17–06/08/26

Given their attack usage, it is not surprising that all five domains continued to post 2026 resolutions.

APT37 NarwhalRAT Attack IP IoCs Investigated

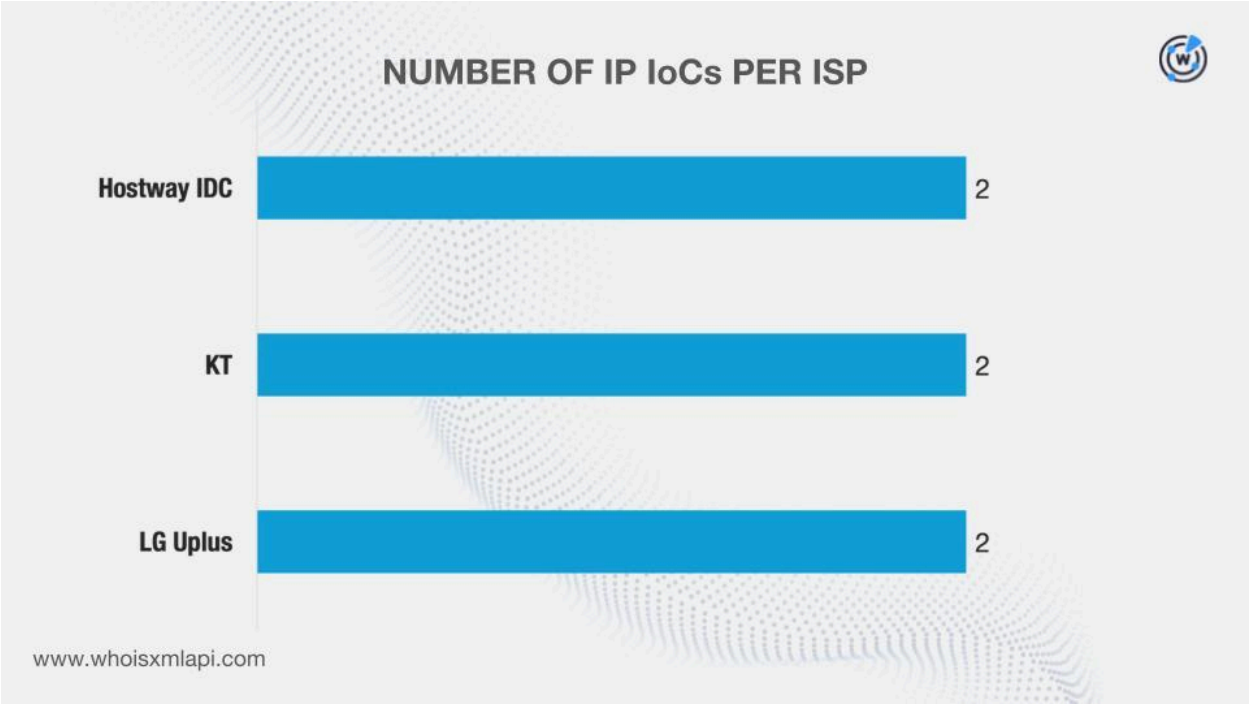
We looked further into the DNS footprint of the six IP IoCs next.

Sample network traffic data from the IASC showed that 77 distinct IP addresses that potentially belonged to victims under five unique ASNs communicated with all the IP IoCs between 20 December 2025 and 16 June 2026.



We then queried the IP IoCs on Bulk IP Geolocation Lookup and found out that:

- They were all geolocated in South Korea, which was expected since the Genians researchers did say APT37 used a Korean relay server for C&C.
- They were administered by three ISPs, all of which were also Korean-based.



Next, we queried the IP IoCs on DNS Chronicle API and discovered that they posted 2,999 historical IP-to-domain resolutions over time. Here are more details about three examples.

IP IoC	NUMBER OF IP-TO-DOMAIN RESOLUTIONS	DATES SEEN
218[.]150[.]78[.]198	1,000	02/04/17–06/17/17
218[.]150[.]78[.]231	1,000	02/05/17–07/03/20
61[.]100[.]9[.]206	467	02/07/17–06/14/26

Unlike the domain IoCs, which all continued to record domain-to-IP resolutions, only four of the six IP IoCs recorded 2026 IP-to-domain resolutions.

Finding New APT37 NarwhalRAT Attack Artifacts

We started our hunt for new artifacts by querying the five domain IoCs on WHOIS History API and learned that all of them had email addresses in their historical records. We obtained seven email addresses in all. Upon further scrutiny, five were public email addresses.

We then queried the public email addresses on Reverse WHOIS API, which led to the discovery of 79 distinct email-connected domains after those already dubbed as IoCs were filtered out.

Next, we queried the domain IoCs on DNS Lookup API and discovered that four of them actively resolved to four unique IP addresses that were already tagged as IoCs.

We queried the IP IoCs on Reverse IP API and learned that they could all be dedicated hosts. Together, they hosted 792 distinct IP-connected domains after those already identified as IoCs and the email-connected domains were filtered out.

We then scrutinized the domain IoCs and extracted five unique text strings. Using Domains & Subdomains Discovery, we found domains other than those already named as IoCs and the email- and IP-connected domains that started with these three strings:

- fe01.
- novel21.
- webhostingkorea.

We collated 17 distinct string-connected domains in all.

Note that the string-connected domains only serve to reflect the overall popularity of the strings extracted from the IoCs. As such, determining their legitimacy may require further investigation.

Final Thoughts

Our DNS deep dive into the APT37 NarwhalRAT attack revealed that one client IP address communicated with a domain IoC and 77 distinct IP addresses that could be victim-owned communicated with six of the IP IoCs according to sample network traffic data from the IASC.

We also found 888 new artifacts comprising 79 email-connected domains, 792 IP-connected domains, and 17 string-connected domains. None of them have been weaponized for attacks as of this writing.

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

- 5brothers[.]co[.]kr
- artistcenter[.]or[.]kr
- bequemhouse[.]com
- chec[.]or[.]kr
- daegulaon[.]or[.]kr
- e-dgpower[.]co[.]kr
- gbcosa[.]or[.]kr
- hanakk[.]co[.]kr
- icw[.]kr
- jokbal114[.]co[.]kr
- k-lako[.]com
- mibbum[.]com
- newsimco[.]com
- oneroombest[.]kr
- raker[.]co[.]kr
- sangone[.]com
- tbsolution[.]or[.]kr
- vineit[.]co[.]kr
- wmc-academy[.]com
- xn--2j1b77ohta391antt[.]com
- yjtown[.]co[.]kr

Sample IP-Connected Domains

- 003acdfc-546e-43c7-a327-7038 8d81f57c[.]random[.]cjcw[.]co[.]kr
- 012727da-19b3-4f39-8bdc-ac268 8d60abe[.]random[.]khhospital[.]co[.]kr
- 012727da-19b3-4f39-8bdc-ac268 8d60abe[.]random[.]kmot[.]co[.]kr
- a024b5eb-9855-4980-8f34-a4b1 9a4fdc1f[.]random[.]kairos-int[.]com
- a03b52ca-2cfa-440d-a695-8a28 7fb71472[.]random[.]buttonline[.]co[.]kr
- a12d794d-3a31-4aea-a678-ec44 0a7a6f8c[.]random[.]eyoungsan[.]com
- b1480b7d-92c2-40e4-a676-13ae d81da5b7[.]random[.]cwmodern[.]com
- b27aabff-4ecf-4d05-8fec-dac85a 276d5b[.]random[.]imdmart[.]com
- b27aabff-4ecf-4d05-8fec-dac85a 276d5b[.]random[.]sunwoogf[.]com
- c02e0923-76e8-4f42-86d4-9f115 2d2c841[.]random[.]dglovecoal[.]org
- c0349eb0-28fb-48be-b636-b866 060fb0a1[.]random[.]dilmahshop[.]co[.]kr
- c0349eb0-28fb-48be-b636-b866 060fb0a1[.]random[.]hostro[.]net
- d[.]imdmart[.]com
- d0efbde3-8c1a-4889-82cc-72eb7 b8bdfd7[.]random[.]gabangmode[.]com
- d112563f-c7c7-4108-afed-2ab780 79f3c7[.]random[.]dreamartschool[.]com
- e-samsam[.]co[.]kr
- e58318ec-a8b5-4a34-85e6-ba67 642d089f[.]random[.]dolgicap[.]com
- e5cd3619-8eae-4668-b0bf-8ce8 90ae068c[.]random[.]yoonhanki[.]net

- f0281756-b855-41c1-8ac1-013b1d8dcbb2[.]random[.]shinsengwon[.]com
- f2770c15-768b-4513-80d7-a99ce88ee7d2[.]random[.]khhospital[.]co[.]kr
- f2770c15-768b-4513-80d7-a99ce88ee7d2[.]random[.]yorun[.]co[.]kr
- gabangmode[.]com
- ghpeople[.]org
- go[.]dreamartschool[.]com
- hanarumfood[.]co[.]kr
- hansamfood[.]com
- hanwoolcenter[.]com
- icncsoft[.]com
- instanly[.]kwanghyespine[.]com
- inyouth[.]or[.]kr
- jjenglish[.]net
- jtasqjyriyz[.]xn--9d0b2b90vm1l9v4ara72a[.]org
- kairos-int[.]com
- kbcera[.]co[.]kr
- kbcera[.]com
- l[.]kwanghyespine[.]com
- link[.]icncsoft[.]com
- links[.]degec[.]or[.]kr
- m[.]canavena[.]co[.]kr
- m[.]cpckorea[.]com
- m[.]daehoat[.]com
- nomadtravel[.]kr
- ns2[.]yeonwedding[.]co[.]kr
- ns3[.]sgcera[.]kr
- o[.]dreamartschool[.]com
- office[.]kwanghyespine[.]com
- office79[.]co[.]kr
- pages[.]icncsoft[.]com
- pay[.]canavena[.]co[.]kr
- pay[.]cpckorea[.]com
- qpsutfuqhbs[.]daehoat[.]com
- rainbowcity[.]co[.]kr
- rainbowelec[.]co[.]kr
- random[.]canavena[.]co[.]kr
- s3[.]daeguedu[.]or[.]kr
- s3[.]gabangmode[.]com
- s3[.]imdmart[.]com
- taesungene[.]com
- tail[.]hanwoomart[.]com
- tarh[.]hanwoomart[.]com
- u[.]dsautotec[.]com
- u[.]ghpeople[.]org
- u[.]postmaster[.]plushospital[.]com
- visiondy[.]com
- viz[.]daehoat[.]com
- vpn[.]cjcw[.]co[.]kr
- w[.]sangone[.]com
- webcastlink[.]com
- webdisk[.]canavena[.]co[.]kr
- x-domainkey[.]dgwise[.]or[.]kr
- xmvoiouidhg[.]hostro[.]net
- xn--9d0b2b90vm1l9v4ara72a[.]org
- yeonwedding[.]co[.]kr
- yoonhanki[.]net
- yorun[.]co[.]kr
- zapps[.]imdmart[.]com
- zct[.]kwanghyepain[.]com
- zct[.]kwanghyespine[.]com

Sample String-Connected Domains

- fe01[.]aquila[.]it
- fe01[.]cc
- fe01[.]cn
- novel21[.]cc
- novel21[.]com
- novel21[.]net
- webhostingkorea[.]net