A DNS Deep Dive into the NetSupport RAT Campaign

Table of Contents

Executive Report

Remote access trojans (RATs) can be considered the malware of choice by the world's most notorious advanced persistent threat (APT) groups. And there's a good reason for that. They are hard to detect, making them ideal for lateral movement, and also difficult to get rid of.

Talos recently published a detailed analysis of one such tool dubbed "NetSupport RAT." This particular RAT is a weaponized version of NetSupport Manager, a legitimate remote device administration tool that has been commercially available since 1989. Its malicious counterpart, on the other hand, has been around since 2023. To date, NetSupport RAT has been used in at least two massive campaigns.

Since then, security researchers have been tracking the RAT's development and latest activities. An in-depth analysis of the tool involved in the latest campaign identified nine domain names as indicators of compromise (IoCs).

The WhoisXML API research team expanded the list of IoCs to identify other potentially connected artifacts, namely:

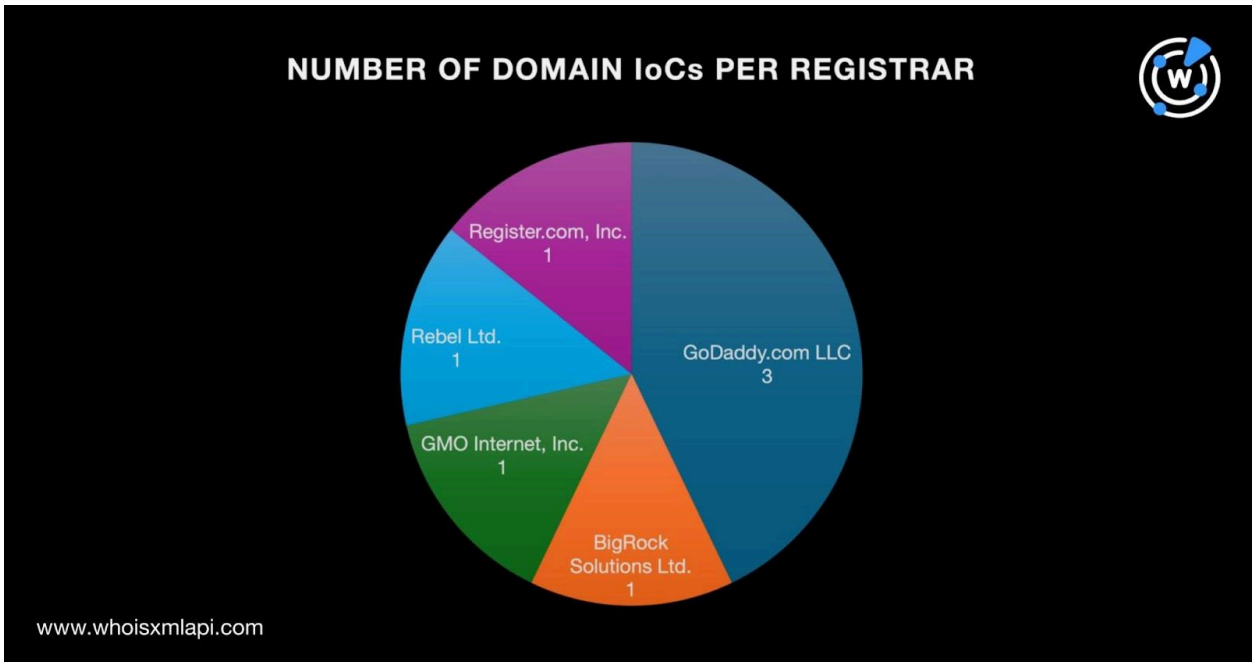
- 239 email-connected domains based on the current and historical WHOIS records
- 1,010 registrant-connected domains
- Three IP addresses, all of which turned out to be malicious
- Two string-connected domains

A Closer Look at the NetSupport RAT IoCs

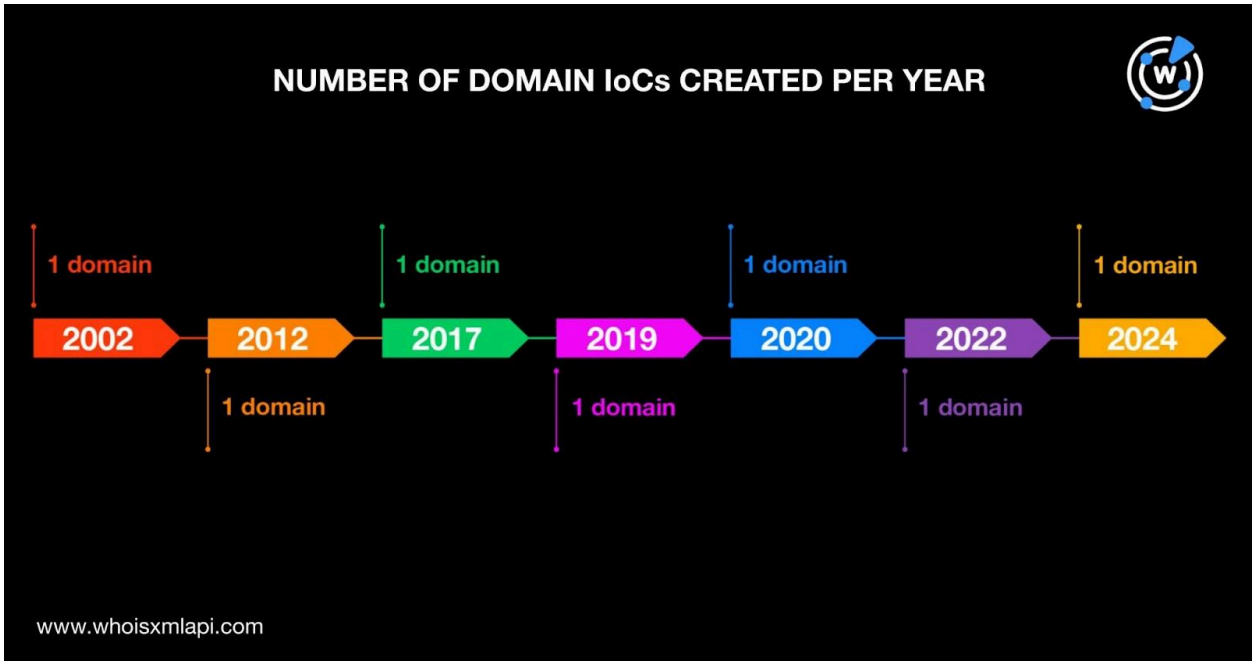
As is our usual first step, we sought to find more information about the IoCs security researchers have already identified, specifically nine domain names.

A bulk WHOIS lookup for the nine domain IoCs revealed that:

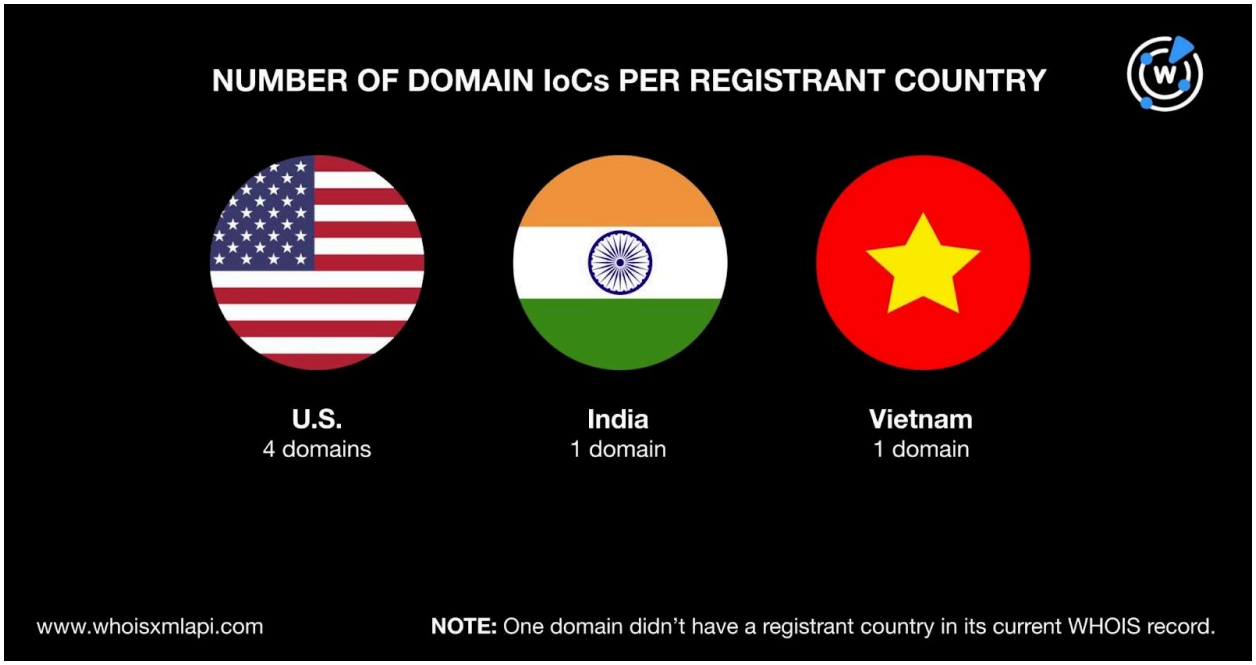
- Only seven of them had current WHOIS record details, reducing the number of IoCs for further analysis from nine to seven.
- The seven domain IoCs were distributed among five registrars led by GoDaddy.com LLC, which administered three. One domain IoC each was administered by BigRock Solutions Ltd.; GMO Internet, Inc.; Rebel Ltd.; and Register.com, Inc.



- The seven domain IoCs were created between 2002 and 2024. They were evenly distributed (i.e., one IoC per year), which could be an effective evasion tactic in that security teams would find it hard to zoom in on specific time frames while threat hunting.



- The U.S. was the top registrant country, accounting for four domain IoCs. One domain IoC each was registered in India and Vietnam. Finally, one domain IoC did not have a registrant country in its current WHOIS record.



- Two domain IoCs had public registrant names.

NetSupport RAT DNS Deep Dive Findings

We began our hunt for connected artifacts by querying the seven domain IoCs on WHOIS History API. That led to the discovery of 12 email addresses in their historical WHOIS records after filtering out duplicates. Four were public email addresses.

Querying the four public email addresses on Reverse WHOIS API came next. The step revealed that only three of them appeared in the current WHOIS records of other domains. Specifically, we uncovered 17 email-connected domains after we filtered out duplicates and the IoCs.

To see if there were other email-connected domains, we queried the four public email addresses this time using Reverse WHOIS Search on the Domain Research Suite (DRS). That enabled us to find 222 domains whose historical WHOIS records contained the email addresses. Note that the number excluded duplicates, the IoCs, and the domains with the email addresses in their current WHOIS records.

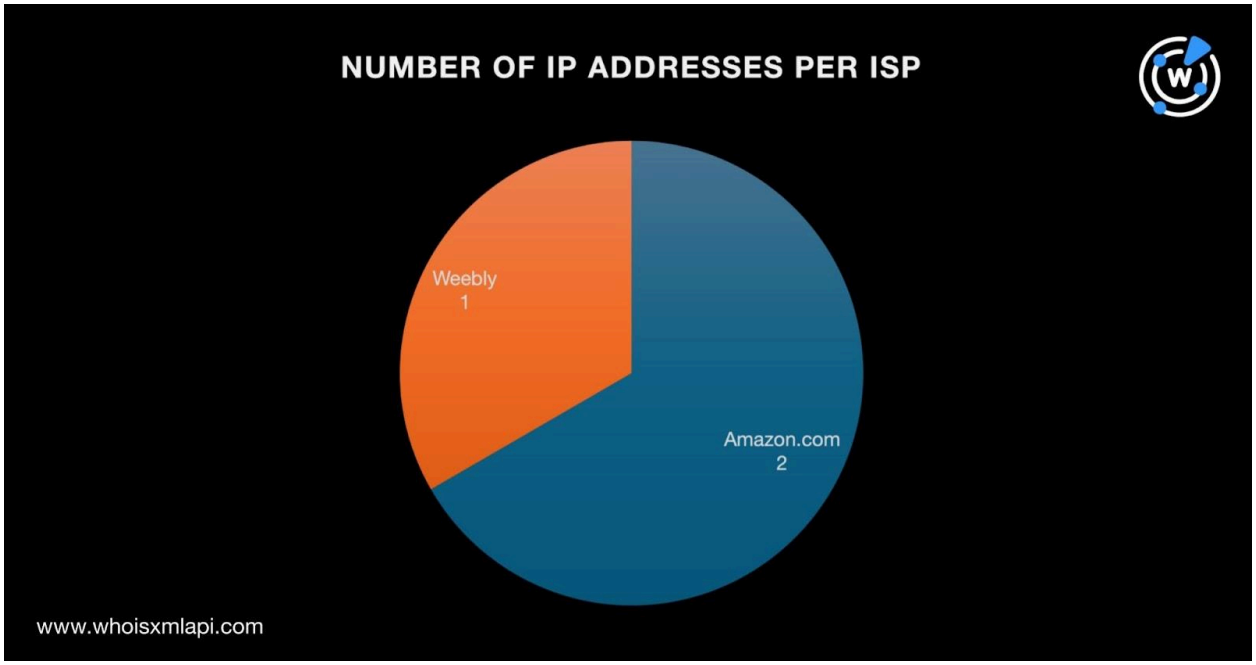
Earlier, we mentioned that two of the domain IoCs had public registrant names. Our historical reverse WHOIS search queries for them turned up 1,010 registrant-connected domains. They had the same registrant names in their historical WHOIS records.

We then hunted for the IP resolutions of the seven domain IoCs. Our DNS lookups revealed that only two had active IP resolutions. Specifically, they resolved to three IP addresses after we filtered out duplicates.

Threat intelligence lookups for the three IP addresses revealed that all of them were associated with various threats. The IP address 13[.]248[.]169[.]48, for instance, was associated with malware infections, generic threats, phishing, attacks, suspicious activities, command and control (C&C), and spam campaigns.

A bulk IP geolocation lookup for the three IP addresses, meanwhile, revealed that:

- They were all geolocated in the U.S.
- They were spread between two ISPs. Two IP address IoCs were administered by Amazon.com and one by Weebly.



Reverse IP lookups for the three IP addresses revealed that they were all shared hosts, halting our search for IP-connected domains. Nonetheless, we still looked into the shared IP address connections out of curiosity since many if not all of them may not even be directly connected to NetSupport RAT but may have ties to other threats. We found 601 shared IP-connected domains.

As a final step, we looked for string-connected domains, ones that only differed from the IoCs in terms of top-level domain (TLD) extension. Our Domains & Subdomains Discovery searches for text strings found in the seven domain IoCs led to the discovery of two string-connected domains after filtering out duplicates, the IoCs, and the email-connected domains. They were choosetotruck[.]ca and kineticwing[.]tech. Note that we used the **Domains only** and **Starts with** parameters.

—

Our in-depth DNS investigation into the latest NetSupport RAT campaign led to the discovery of 1,254 potentially connected threat artifacts, comprising 239 email-connected domains (based on their current and historical WHOIS records), 1,010 registrant-connected domains, three IP addresses, and two string-connected domains. To date, only three of the artifacts, specifically all of the connected IP addresses, have been weaponized for attacks.

And while we don't think the 601 domains that shared the IoCs' hosts were directly connected to NetSupport RAT, knowing they resolved to malicious IP addresses could prove useful for

security teams. Monitoring them for suspicious activity could be worth the effort for hunting down other threats.

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 Based on Current WHOIS Records

- criterioninteractive[.]us
- doinkzee[.]info
- freepster[.]info
- liviaistrate[.]info
- malemay[.]info
- merrymerlot[.]us
- pcunifi[.]net
- rapidzap[.]info
- refersimply[.]info

Sample Email-Connected Domains Based on Historical WHOIS Records

- 1stratedesign[.]com
- 1strateweb[.]com
- 365angels[.]org
- adlookout[.]info
- agilemedical[.]com
- alamopianostars[.]com
- alamopianostars[.]info
- auracast[.]info
- automaticdonation[.]com
- bestdomainsmarket[.]com
- biofrog[.]com
- blogrz[.]com
- blogrz[.]info
- boulz[.]com
- brainycare[.]com
- buenu[.]com
- buyaffiliatelinks[.]com
- buyaffiliatetraffic[.]com
- cafe2[.]me
- cafe2[.]us
- cafe2me[.]com
- canvaswithakick[.]com
- carefreepainter[.]com
- carestripe[.]com
- cc2check[.]com
- cctocash[.]com
- cctocheck[.]com
- chixa[.]com
- cloudpure[.]com
- cloudscrub[.]com

- cloudtrim[.]com
- coffee2[.]us
- cokye[.]com
- cokye[.]info
- craak[.]info
- creditcard2check[.]com
- criterioncreative[.]com
- criterioncreative[.]us
- criterioninteractive[.]com
- dannytaggart[.]com
- denifi[.]com
- denify[.]care
- denify[.]com
- denify[.]info
- denify[.]mobi
- denify[.]net
- denify[.]org
- denify[.]us
- denifycare[.]com
- docextend[.]com

Sample Registrant-Connected Domains

- 11wallpapers[.]com
- 2016februarycalendar[.]com
- 247pillsonline[.]com
- 365angels[.]com
- 3doshas[.]com[.]au
- 3monthpaydayloansukonline[.]co[.]uk
- 4farmer[.]com
- 4sherfreightsystem[.]com
- 7bows[.]com
- a2zgaming[.]com
- aac[.]vet
- aalishanfashions[.]com
- aanganwadiindia[.]net
- abnready[.]com[.]au
- abytechh[.]com
- accsociety[.]com
- accurotech[.]com
- acmeconsultants[.]org
- acrossayurveda[.]com
- actautomation[.]in
- adarshjantaintercollege[.]com
- adavancecashservices[.]biz
- aditifs[.]com
- aditikirasoi[.]com
- aditissilverbells[.]com
- adminjob[.]in
- adminwala[.]com
- adukkamvaliyaveed[.]com
- advancedanimalcarellc[.]com
- advocateyash[.]com
- aecpatiala[.]com
- aectl[.]au
- aectl[.]com[.]au
- aeiryknitwears[.]com
- agatsyaacharya[.]com
- agricultrure[.]com
- agrivikalp[.]com
- ahaw[.]org
- aioamante[.]com
- airconcomfortvehicles[.]com
- airfarebookers[.]us
- aishwariarealty[.]com
- akshitfoods[.]com
- alaseeljewelleryfze[.]com
- alignmysystems[.]com
- allercoheatingandplumbing[.]co[.]uk
- allmineranch[.]com
- alphaitclasses[.]com
- alpineassociation[.]com
- americanmaidhousekeeping[.]com
- andrewandjenwedding[.]com
- angrypanda[.]us
- aniltingre[.]com

- animaxhealthcare[.]com
- animaxhealthcare[.]in
- annapurna-groups[.]com
- anonrepair[.]com
- anuraganathsevasamiti[.]org
- apparels4foot[.]com
- appleexpresslane[.]online
- applesupporttech[.]com
- arogyakavach[.]com
- artesiawater[.]com
- ashriyainfotech[.]co[.]in
- asianinstruments[.]net
- askprophoto[.]com
- assurets[.]com
- asthaengineers[.]com
- atcelectricals[.]com
- atharvwines[.]com
- atomshealth[.]com
- australishome[.]com[.]au
- awaremesothelioma[.]us
- azadurbanwear[.]com
- badlywritten[.]com
- bahasabali[.]asia
- bakesncreams[.]com
- balvinderhayer[.]com
- bansumfashion[.]com
- bansurivala[.]com
- bargainmuse[.]com
- behance[.]in
- beinginspirational[.]com
- bestaccountant[.]com[.]au
- bestcafegroup[.]com
- bestcitideals[.]com
- bestpricecars[.]com[.]au
- besttrucks[.]com[.]au
- bhaaratbazaar[.]com[.]au
- bharatfuture[.]com
- bhopalpost[.]com
- bicentenary[.]in
- bigtickets[.]com[.]au
- bikebeltsville[.]org
- bikeonrentnainital[.]com
- bingleconsulting[.]com
- biryanipalace[.]com[.]au
- bitcoinrunway[.]com
- bizyera[.]com
- bkims[.]org

Sample IP Addresses

- 13[.]248[.]169[.]48
- 199[.]34[.]228[.]191