Checking Out the DNS for More Signs of ResumeLooters

Table of Contents

Executive Report

Group-IB uncovered ResumeLooters, a threat actor group specializing in victimizing job hunters to steal their personally identifiable information (PII). Along with their in-depth threat analysis, they identified 15 indicators of compromise (IoCs), specifically seven domain names, three subdomains, and five IP addresses.

The WhoisXML API research team used the 15 IoCs as jump-off points for an expansion analysis in a bid to find more potential ResumeLooters attack vectors that led to the discovery of:

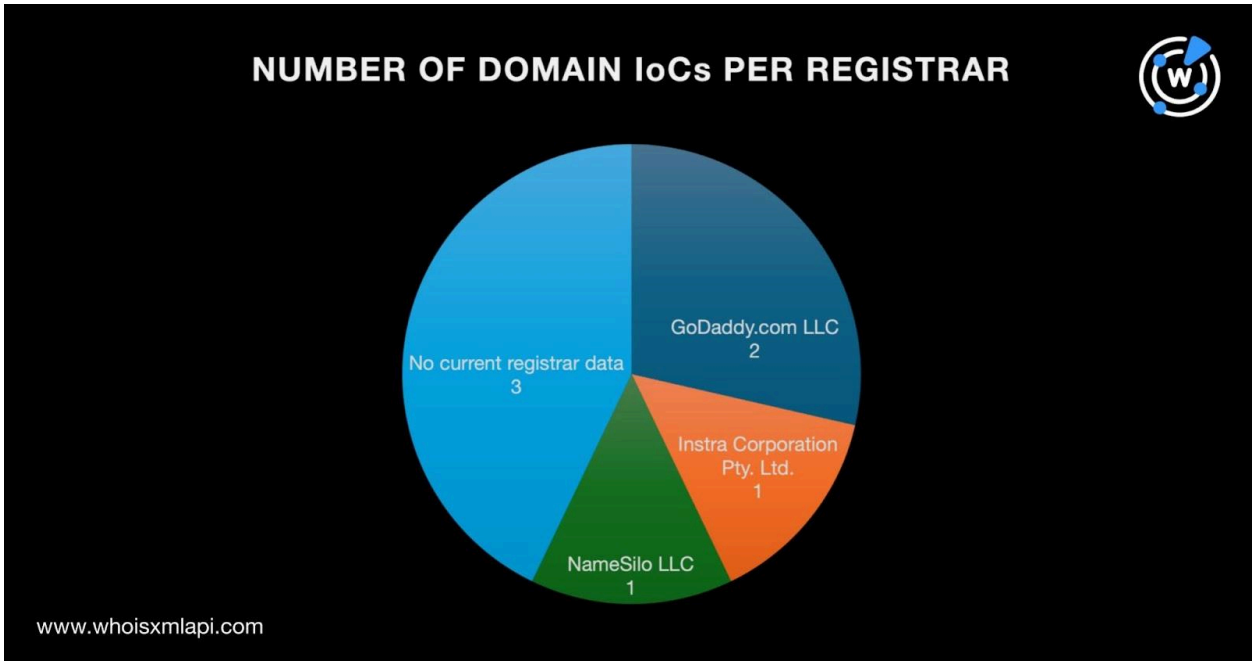
- 302 registrant-connected domains
- 69 email-connected domains
- Six additional IP addresses, all of which turned out to be malicious
- Three IP-connected domains
- 573 string-connected domains, two of which turned out to be malicious

ResumeLooters IoC Facts

We began our investigation by taking a closer look at the 15 IoCs starting with the seven domain names.

A bulk WHOIS lookup for the seven domains identified as IoCs led to these findings:

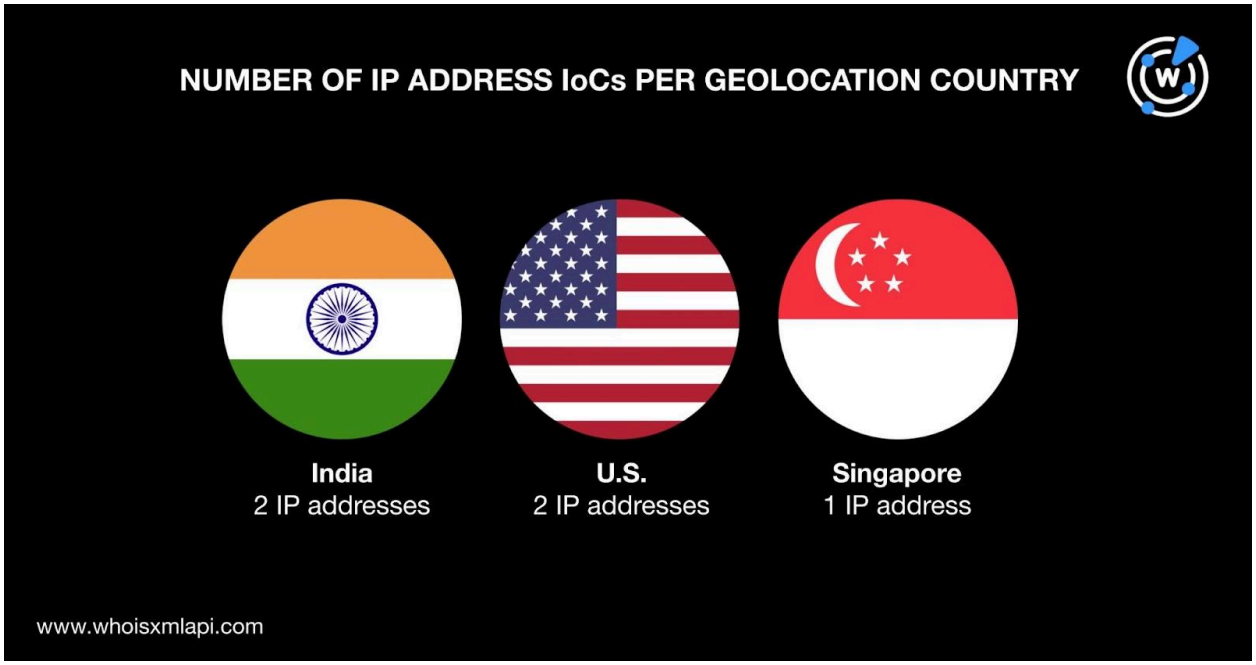
- They were split among three registrars. GoDaddy.com LLC accounted for two domains and Instra Corporation Pty. Ltd. and NameSilo LLC for one domain each. Three domains did not have registrar data in their current WHOIS records.



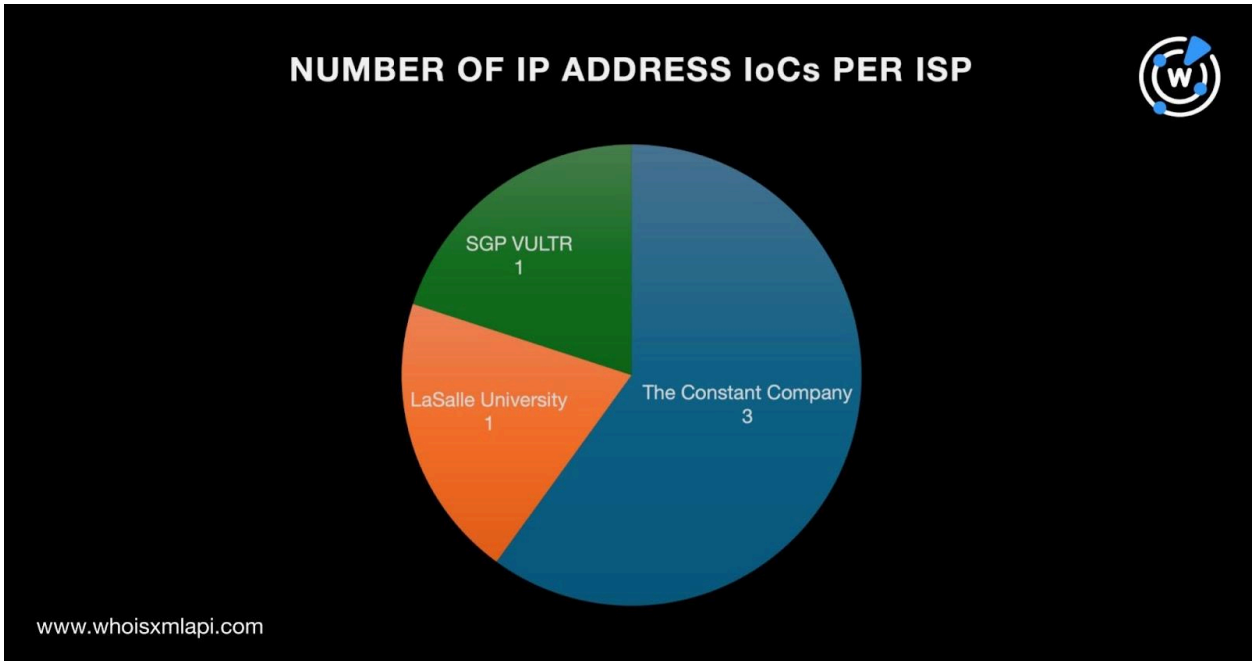
- Three domains classified as IoCs with creation dates in their current WHOIS records were created in 2023. The other four domains had no current creation date information.
- The only domain IoC with registrant country data in its current WHOIS record was registered in the U.S.
- The domain IoC 8t[.]ae had publicly available registrant name and organization information.

The bulk IP geolocation lookup for the five IP addresses named as IoCs gave these results:

- They were geolocated in three countries. India and the U.S. accounted for two IP addresses each and Singapore accounted for one.



- They were spread out across three ISPs led by The Constant Company, which accounted for three IP addresses. One IP address each was administered by LaSalle University and SGP VULTR.



ResumeLooters IoC Expansion Analysis Findings

This section describes how we went about finding artifacts potentially connected to ResumeLooters.

Our bulk WHOIS lookup earlier revealed the registrant name and organization of domain IoC 8t[.]ae. A reverse WHOIS search using the registrant name as input provided us with 302 connected domains after duplicates and the IoCs were filtered out, 77 of which remained accessible at the time of writing according to Screenshot API results.

WHOIS History API also allowed us to obtain four email addresses from the historical WHOIS records of the seven domain IoCs after duplicates were removed. Two of them were public, which we then used as Reverse WHOIS API search inputs. They gave us 69 email-connected domains after filtering out duplicates, the IoCs, and the registrant-connected domains. Twenty-seven continued to host live pages to date.

Next, we performed DNS lookups for the seven domain IoCs and found that they resolved to six additional IP addresses after removing duplicates and the IoCs. Like two of the IP address IoCs, all of them were geolocated in the U.S. and administered by Cloudflare, Inc. All six additional IP addresses were also associated with various threats. Specifically:

- All six IP addresses were associated with phishing.
- Four IP addresses were associated with generic threats.
- Two IP addresses were associated with malware attacks.
- Two IP addresses were associated with suspicious activities.

We then subjected the 11 IP addresses in total (i.e., five IoCs and six additional hosts) to reverse IP lookups and found that three of them could be dedicated. They enabled us to uncover three IP-connected domains after duplicates, the IoCs, and the registrant- and email-connected domains were filtered out.

To complete our investigation, we used Domains & Subdomains Discovery to look for domains that started with text strings found among the seven domain IoCs. Our searches enabled us to gather 573 string-connected domains, two of which—8t[.]pm and 8t[.]wf—were associated with malware attacks according to Threat Intelligence API.

Are There Other Signs of Legitimate Job-Hunting Site Impersonation in the DNS?

Group-IB, in their report, also identified three ResumeLooters subdomain IoCs. Two of them—recruit[.]iimjobs[.]asia and recruiter[.]foundit[.]asia—seemed to be impersonating legitimate job-hunting websites.

Google searches for the two sites revealed that the legitimate job-hunting websites' domain names were iimjobs[.]com and foundit[.]in. They both had public registrant organization data in their current WHOIS records according to WHOIS lookups. The same searches for iimjobs[.]asia and foundit[.]asia, meanwhile, did not turn up registrant organization information for both likely typosquatting domains. Screenshot lookups for iimjobs[.]asia and foundit[.]asia also showed both were unreachable as of this writing.

If ResumeLooters specially crafted the domains iimjobs[.]asia and foundit[.]asia for their campaign, could they or other cybercriminals have done the same thing? We trooped to Domains & Subdomains Discovery to find out.

Our closer looks uncovered eight **iimjobs.**- and 166 **foundit.**-containing domains.

While none of the **iimjobs.**-containing domains were associated with any threat, only three of them could be publicly attributed to iimjobs[.]com's registrant organization.

Like the **iimjobs.**-containing domains, none of the **foundit.**-containing domains were classified as malicious. But WHOIS record comparisons showed that only one of them could be publicly attributed to foundit[.]in's registrant organization.

—

Our analysis of ResumeLooters led to the discovery of 953 potentially connected web properties, specifically 302 registrant-connected domains, 69 email-connected domains, six additional IP addresses, three IP-connected domains, and 573 string-connected domains. Eight of the related digital properties were associated with various threats, including phishing, malware attacks, generic threats, and suspicious activities.

Our analysis of two of the subdomains ResumeLooters used in their campaign also showed signs of possible job-hunting site impersonation targeting iimjobs[.]com and foundit[.]in.

If you wish to perform a similar investigation or 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 Registrant-Connected Domains

- 36084[.]wang
- 3sumz[.]com
- 51bisai[.]com
- 51xifu[.]net
- aacgroup[.]com[.]au
- aboveevent[.]com
- abovevent[.]com
- acmoney[.]com[.]au
- adjusted-book-value[.]com
- adjusted-earnings[.]com
- adorningembellishments[.]com
- afmg[.]com[.]au
- aipa20[.]com
- airhotsale[.]com
- airtelchampionsleague[.]com
- algrealestate[.]com[.]au
- allofhalf[.]com
- alorabeautystudio[.]com[.]au
- americas-goods[.]com
- amsterdambyfood[.]com
- amsterdamchinatown[.]com
- annuo-leather[.]com
- antaiengineering[.]com
- aoborealty[.]com[.]au
- asianaac[.]com
- asianaac[.]org
- asiancuisinenorman[.]com
- asset-approach[.]com
- asset-sale[.]com
- aussie-home[.]com[.]au
- australianunityparty[.]com[.]au
- bambusplatten[.]com
- base-year[.]com
- beautybridaldress[.]com
- bjdmty[.]com
- bodyorbust[.]com
- boyalife[.]com
- bsfgtj[.]net
- burstratecreative[.]com
- buying-american-real-estate[.]com
- c60changshou[.]com
- caiche-printing[.]com
- camedia[.]com[.]au
- canadian2for1pizza[.]com
- cannatonicstrain[.]com
- cannyowldesigns[.]com
- charterlicensing[.]com
- chaunisthebomb[.]com
- cheapbestbags[.]com
- cheapbestbags[.]net

Sample Email-Connected Domains

- 1533[.]one
- 1663[.]online

- 18girl[.]sex
- 3155[.]one
- 3338[.]com[.]cn
- 3522[.]online
- 6122[.]online
- 68008[.]net
- 7258[.]online
- 7268[.]online
- 9077[.]com[.]cn
- agelocgamma[.]org
- cunhua[.]cn
- cunshe[.]cn
- dblw[.]com[.]cn
- diaogui[.]cn
- dqd[.]one
- fjf[.]one
- fkf[.]one
- fwf[.]one

Sample Additional IP Addresses

- 104[.]21[.]71[.]172
- 104[.]21[.]75[.]250
- 104[.]21[.]9[.]29

Sample IP-Connected Domains

- cloudnetsofe[.]com
- futurexah[.]life

Sample String-Connected Domains

- 3x1[.]ai
- 3x1[.]app
- 3x1[.]aquila[.]it
- 3x1[.]at
- 3x1[.]biz
- 3x1[.]ca
- 3x1[.]cc
- 3x1[.]ch
- 3x1[.]cl
- 3x1[.]club
- 3x1[.]cn
- 3x1[.]co
- 3x1[.]co[.]uk
- 3x1[.]com
- 3x1[.]com[.]br
- 3x1[.]com[.]cn
- 3x1[.]de
- 3x1[.]es
- 3x1[.]eu
- 3x1[.]gratis
- 3x1[.]hu
- 3x1[.]immobilien
- 3x1[.]in
- 3x1[.]info
- 3x1[.]io
- 3x1[.]ir
- 3x1[.]it
- 3x1[.]lat
- 3x1[.]link
- 3x1[.]mil[.]ph
- 3x1[.]net
- 3x1[.]net[.]ph
- 3x1[.]ngo[.]ph
- 3x1[.]nl
- 3x1[.]nyc
- 3x1[.]one
- 3x1[.]online
- 3x1[.]org
- 3x1[.]org[.]ph
- 3x1[.]pizza

- 3x1[.]pl
- 3x1[.]ro
- 3x1[.]ru
- 3x1[.]site
- 3x1[.]tk
- 3x1[.]top
- 3x1[.]uk
- 3x1[.]us
- 3x1[.]uz
- 3x1[.]wang
- 3x1[.]xin
- 3x1[.]xn--kprw13d
- 3x1[.]xn--node
- 3x1[.]xyz
- 3x1[.]zone
- 7o[.]africa
- 7o[.]ai
- 7o[.]am
- 7o[.]at
- 7o[.]au
- 7o[.]audio
- 7o[.]be
- 7o[.]beauty
- 7o[.]beer
- 7o[.]blackfriday
- 7o[.]boats
- 7o[.]ca
- 7o[.]casa
- 7o[.]casino
- 7o[.]cc
- 7o[.]charity
- 7o[.]christmas
- 7o[.]ci
- 7o[.]click
- 7o[.]club
- 7o[.]cm
- 7o[.]cn
- 7o[.]co
- 7o[.]co[.]uk
- 7o[.]co[.]za
- 7o[.]com
- 7o[.]com[.]au
- 7o[.]com[.]br
- 7o[.]com[.]cn
- 7o[.]com[.]tw
- 7o[.]com[.]ws
- 7o[.]country
- 7o[.]cx
- 7o[.]cz
- 7o[.]de
- 7o[.]diet
- 7o[.]dk
- 7o[.]edu[.]ws
- 7o[.]ee
- 7o[.]eu
- 7o[.]feedback
- 7o[.]fi
- 7o[.]fit
- 7o[.]flowers
- 7o[.]football

Sample iimjobs.-Containing Domains

- iimjobs[.]jobs
- iimjobs[.]org
- iimjobs[.]xyz
- iimjobs[.]net

Sample foundit.-Containing Domains

- foundit[.]fun
- foundit[.]homes
- foundit[.]loans
- foundit[.]top
- foundit[.]com[.]hk
- foundit[.]tech

- foundit[.]digital
- foundit[.]ai
- foundit[.]ga
- foundit[.]market
- foundit[.]ir
- foundit[.]dk
- foundit[.]marketing
- foundit[.]com[.]ph
- foundit[.]pro
- foundit[.]info
- foundit[.]fit
- foundit[.]company
- foundit[.]page
- foundit[.]co[.]zm
- foundit[.]co[.]za
- foundit[.]com[.]my
- foundit[.]education
- foundit[.]com[.]tw
- foundit[.]jobs
- foundit[.]io
- foundit[.]space
- foundit[.]london
- foundit[.]technology
- foundit[.]name
- foundit[.]insure
- foundit[.]cool
- foundit[.]repair
- foundit[.]click
- foundit[.]uk
- foundit[.]online
- foundit[.]construction
- foundit[.]vlaanderen
- foundit[.]com[.]au
- foundit[.]nu
- foundit[.]ventures
- foundit[.]kiwi
- foundit[.]net
- foundit[.]app
- foundit[.]systems
- foundit[.]forsale
- foundit[.]nyc
- foundit[.]eco
- foundit[.]me