More Signs of the more_eggs Backdoor Found in the DNS

Table of Contents

Executive Report

Using resumes to fake job applications is not a novel social engineering lure for run-of-the-mill phishing campaigns. But utilizing the same tactic to launch a targeted attack isn't that common.

The threat actor known as "TA4557," who has been active since 2018, recently made waves with the lure, however, aided by the backdoor that has been dubbed "more_eggs." How does it work? In short, the malware is delivered via resumes. The threat actor asks recipients to click a link to the applicant's personal website, jumpstarting the infection until the final payload—credential theft—is achieved.

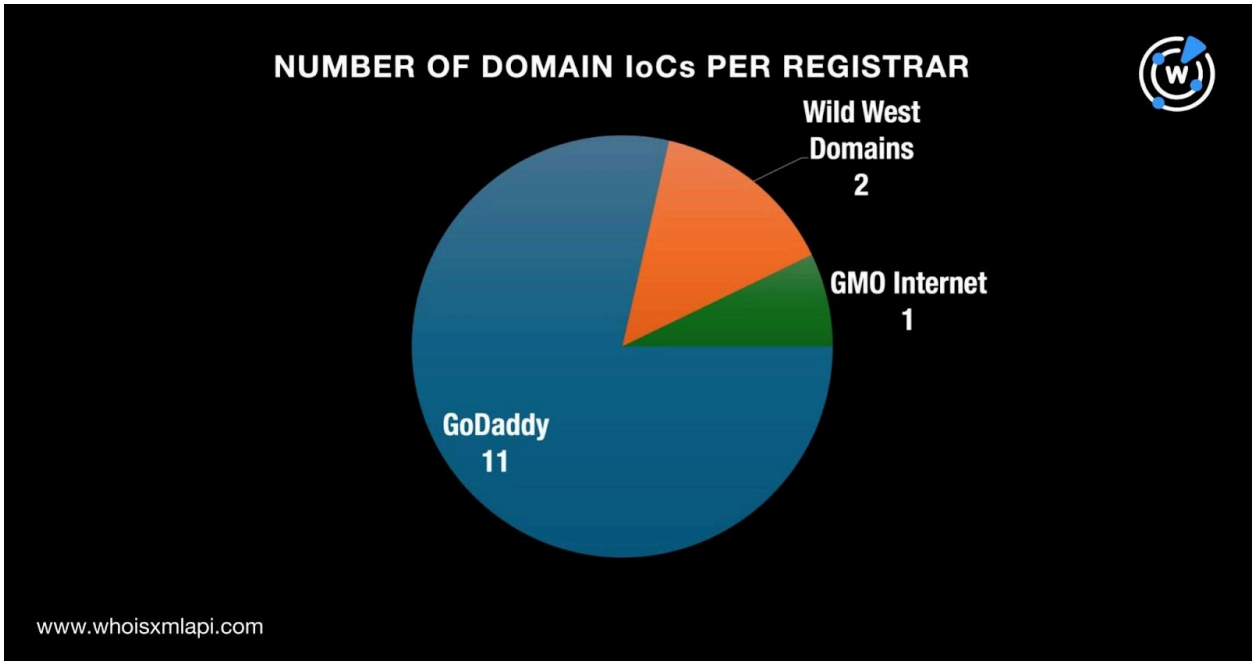
The DFIR Report identified 14 domain names and three IP addresses as more_eggs indicators of compromise (IoCs). The WhoisXML API research team expanded this list and uncovered connected artifacts, namely:

- 35 email-connected domains
- 11 additional IP addresses, three of which turned out to be malicious
- 700 IP-connected domains, 131 of which turned out to be malicious
- 22 string-connected domains

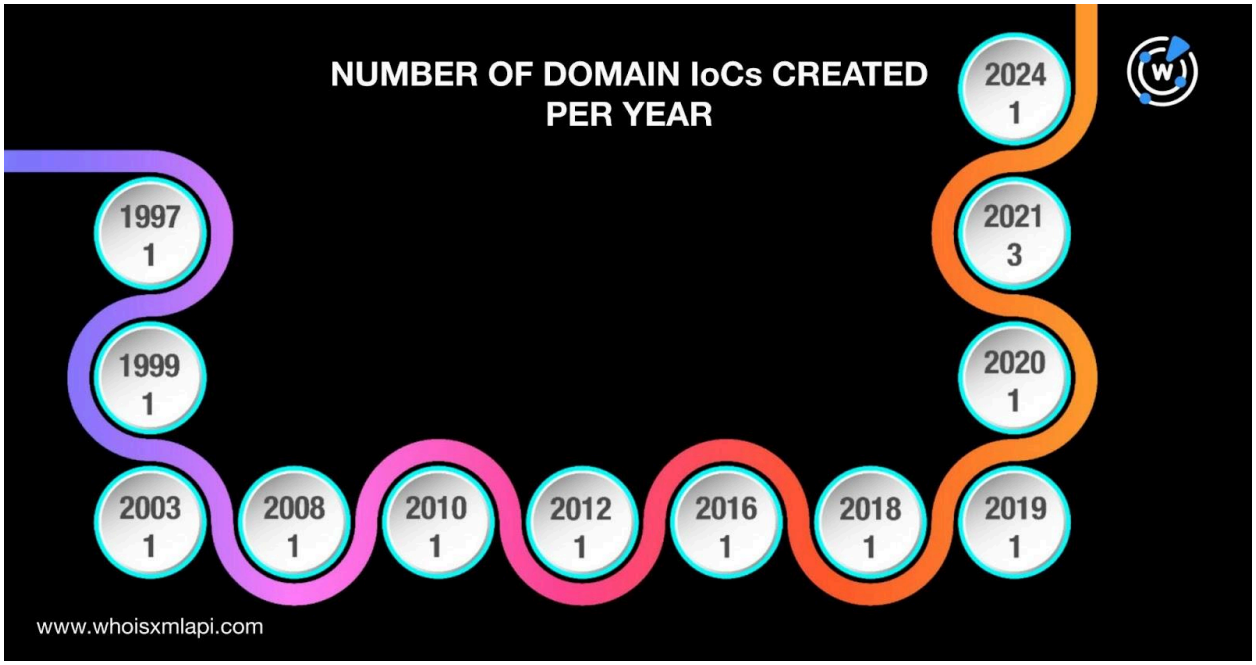
More Information on the more_eggs IoCs

First off, we sought to find more information on the 17 IoCs that have already been identified beginning with a bulk WHOIS lookup for the 14 domains tagged as IoCs. The results revealed that:

- They were administered by three registrars led by GoDaddy with 11 domains. Wild West Domains took the second spot with two domains, while GMO Internet administered the last remaining domain.



- They were created between 1997 and 2024, possibly inferring TA4557's penchant for older domains. Specifically, three domains were created in 2021, while one each was created in 1997, 1999, 2003, 2008, 2010, 2012, 2016, 2018, 2019, 2020, and 2024.



- While a huge chunk, 13 domains to be exact, were registered in the U.S., the remaining domain did not have current registrant country data.

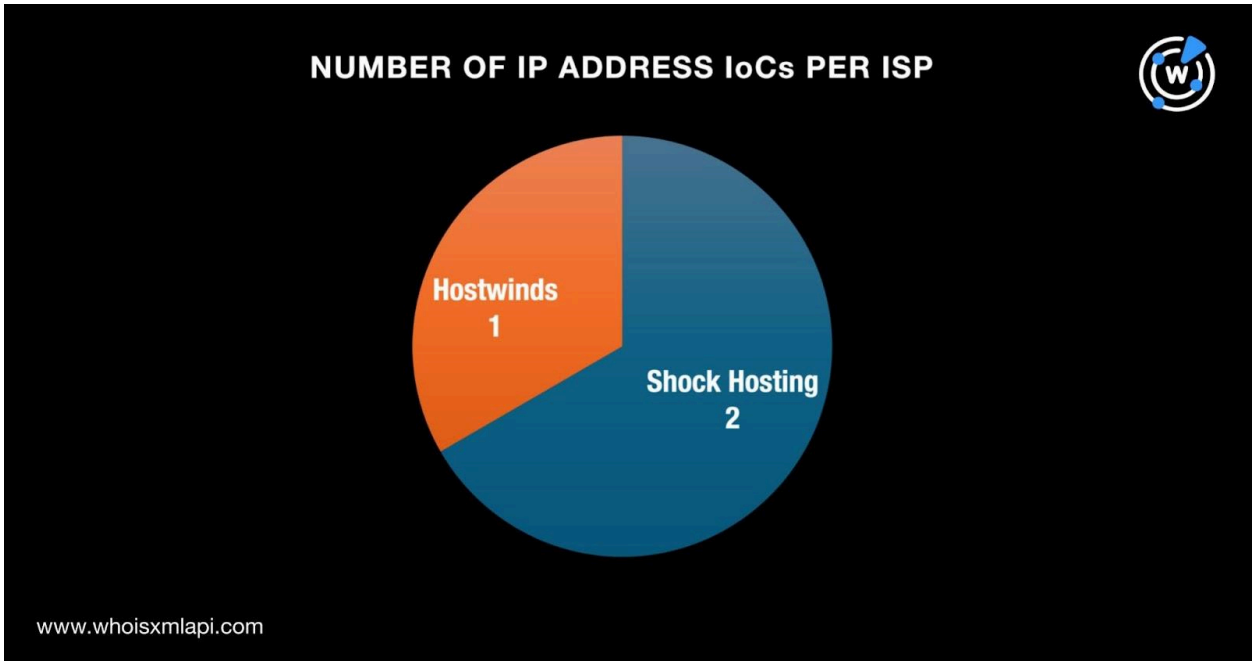
We also queried the 14 domains tagged as IoCs on DNS Chronicle API and found that they have had 871 IP resolutions over time. The first resolution dates ranged from 7 October 2019 and 19 March 2024. Take a look at five examples below.

DOMAIN IoC	FIRST RESOLUTION DATE	LAST RESOLUTION DATE	NUMBER OF IP RESOLUTIONS
annetterawlings[.]com	10/18/19	10/2/24	37
howasit[.]com	11/8/19	1/30/24	35
johnshimkus[.]com	10/10/19	12/30/22	66
markqualman[.]com	11/19/21	11/27/24	74
shehasgone[.]com	3/19/24	10/18/24	6

Next, we queried the three IP addresses tagged as IoCs on Bulk IP Geolocation Lookup and found that:

- All three were geolocated in the U.S.

- They were administered by two ISPs led by Shock Hosting with two IP addresses. Hostwinds managed the remaining IP address.



We also queried the three IP addresses tagged as IoCs on DNS Chronicle API and found that they have had 460 domain resolutions over time. The first resolution dates ranged from 4 October 2019 to 17 November 2020. The IP address IoC 172[.]96[.]139[.]82, for instance, first resolved tx[.]cyrex[.]io on 17 November 2020.

More DNS Connections for more_eggs

Our search for more_eggs-connected artifacts started with a WHOIS History API query for the 14 domains tagged as IoCs. The results showed that 13 of them had 40 email addresses in their historical WHOIS records after duplicates were filtered out. 19 of the 40 email addresses turned out to be public.

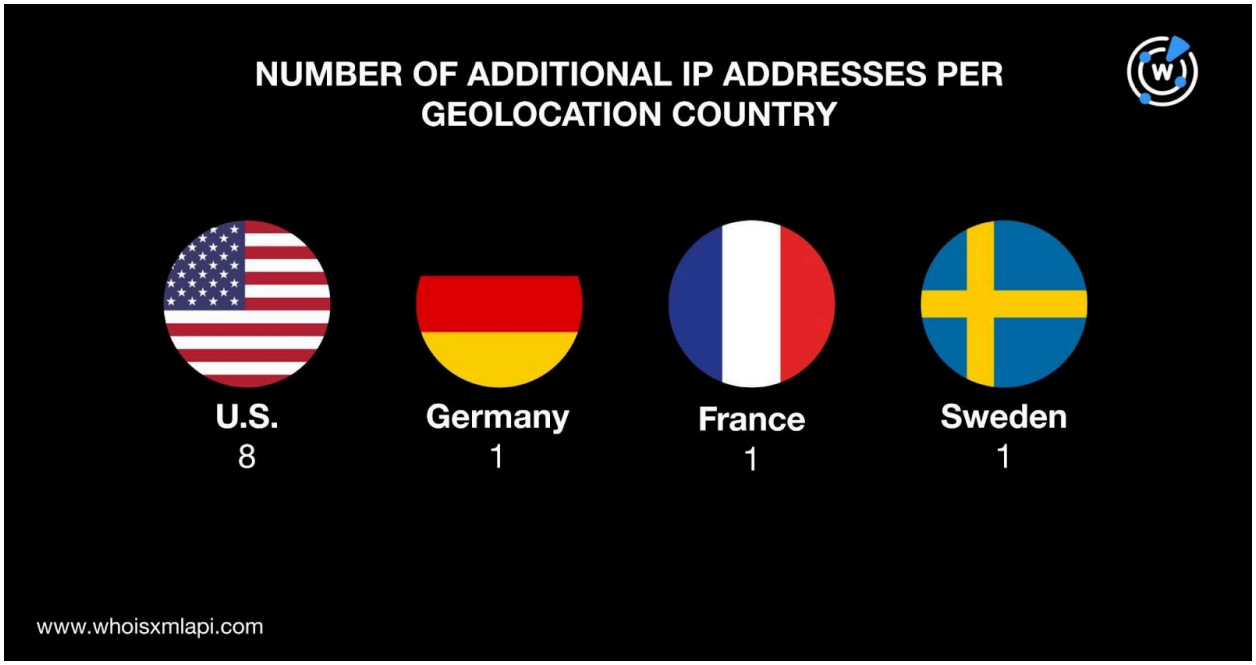
A Reverse WHOIS API query for the 19 public email addresses revealed that four appeared in the current WHOIS records of 35 email-connected domains after filtering out duplicates and the domain IoCs.

Next, we queried the 14 domains tagged as IoCs on DNS Lookup API and found that 13 of them resolved to 11 IP addresses after removing duplicates that are not found on the original IoC list.

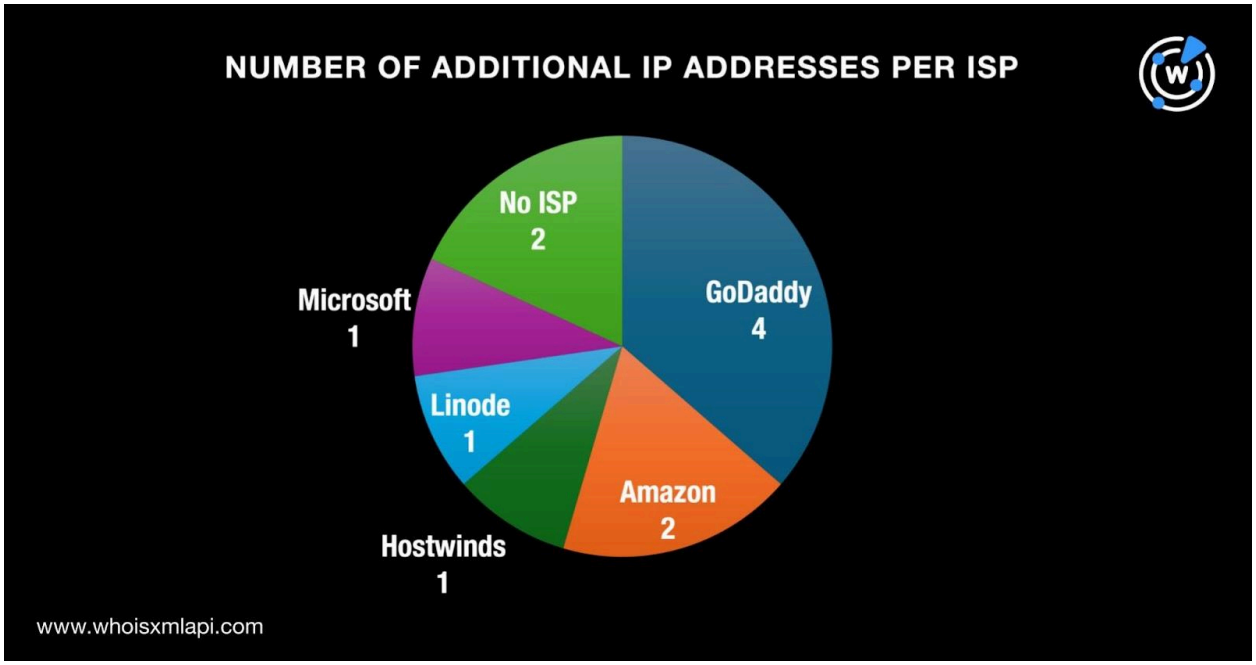
A Threat Intelligence API query for the 11 additional IP addresses revealed that three of them have already figured in malicious campaigns. The IP address 199[.]59[.]243[.]227, for instance, has seemingly been involved in phishing, command and control (C&C), generic threats, malware distribution, attacks, and suspicious activities.

We also subjected the 11 additional IP addresses to a bulk IP geolocation lookup and found that:

- They were geolocated in four countries topped by the U.S. with eight IP addresses. One IP address each was geolocated in Germany, France, and Sweden.



- Only nine of them had public ISP data and spread across five ISPs led by GoDaddy, which administered four IP addresses. Amazon took second place with two IP addresses, while Hostwinds, Linode, and Microsoft administered one IP address each.



We then queried the 14 IP addresses (i.e., three tagged as IoCs and 11 additional from the DNS lookups) on Reverse IP API and learned that 10 of them hosted 700 IP-connected domains after filtering out duplicates, the domain IoCs, and the email-connected domains.

A Threat Intelligence API query for the 700 IP-connected domains revealed that 131 of them have already been weaponized for various attacks. Take a look at five examples below.

MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREATS
0-finanzierung[.]com	Generic Phishing
acecnouwglass[.]xyz	Malware
bahrain-fine[.]org	Malware
carsfootyelo[.]com	Malware
damageagio[.]xyz	Malware

As the final step, we looked for string-connected domains via Domains & Subdomains Discovery. We found 22 string-connected domains after duplicates, the domain IoCs, and the email- and IP-connected domains were filtered out. They started with these seven strings that appeared in the 14 domains tagged as IoCs:

- howasit.
- johnshimkus.
- lisasierra.
- mitchellspearman.
- shehasgone.
- wlynch.

—

Our search for more artifacts connected to more_eggs via an IoC list expansion analysis led to the discovery of 768 web properties comprising 35 email-connected domains, 11 additional IP addresses, 700 IP-connected domains, and 22 string-connected domains. It's also worth noting that 134 of these artifacts have already figured in various malicious campaigns.

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

- 3sixtyislam[.]com
- astuterenaissance[.]com
- bornhuge[.]com
- chalenq[.]com
- crepeteriaandgrill[.]com
- esmcslimited[.]com
- eventcheckbox[.]com
- globalconvoytravels[.]com
- grids2homes[.]com
- hefrworld[.]com
- hotjist[.]com
- howmarket[.]com[.]ng
- imisihaus[.]com
- innovatinghealth[.]ng
- kolaoluyemi[.]com
- michigabbi[.]com

Sample Additional IP Addresses

- 142[.]11[.]194[.]191
- 173[.]255[.]204[.]62
- 199[.]59[.]243[.]227
- 20[.]3[.]249[.]101
- 208[.]109[.]230[.]172
- 208[.]109[.]247[.]38

Sample IP-Connected Domains

- 0--1----------23456789abcdefghijklmnqrsuvwxyz[.]top
- 0--e-lt2s6zlgvc540dowy08nqndafoi[.]narcisussa[.]eu[.]org
- 0-0-0-0[.]com
- 173-255-204-62[.]ip[.]linodeusercontent[.]com
- 17475872967[.]pw
- 18247343188[.]pw
- 24india[.]site
- 390698[.]ru
- 44xyq[.]nsb994[.]com
- 52922597867[.]pw
- 736526437472[.]com
- 8t8g8jquy[.]life
- abitamart[.]com
- acecnouwglass[.]xyz
- achiversacademy[.]shop
- bahrain-fine[.]org
- balancelag[.]xyz
- basdbjabsjdbas[.]pw
- canstealer[.]com
- capitalsbank[.]com
- carnivalsale[.]com
- daewooservicecentreauthorized[.]com
- damageagio[.]xyz
- dareka4te[.]shop
- eaglehardwares[.]com
- ehonlionetodo[.]com
- eniloramesta[.]com
- fastestfreecdn[.]com
- fastsecurityup[.]com
- fbdasfhdsfdshgiksd[.]shop
- gaspatchommm[.]fun
- gemcreedarticulateod[.]shop
- gertaret[.]com
- harmonyshoused[.]com
- hausdhuashdauhs[.]biz
- hbfyewtuvfbhsbdjhjwebfy[.]net
- idcwlaw[.]com
- iliveona[.]cloud
- illoskanawer[.]com
- jegyfuy0[.]xyz
- jmenoff-architect[.]com
- joagfhreetdsa[.]com
- kdaljjjkdalka[.]info
- kgabstract[.]com
- kglawteam[.]com
- lbm[.]nyc
- legendsworld[.]cloud
- lgfjerkud[.]space
- mail[.]christianvelour[.]com
- mail[.]davidopkins[.]com
- mail[.]jacksallay[.]com
- nawlaw[.]com
- nomadgroup[.]io
- nycdentalsmileteam[.]com
- paradisocreations[.]com
- petermwolf[.]com
- pop[.]christianvelour[.]com
- queerarchivestt[.]org
- rizvitraverse[.]com
- smtp[.]christianvelour[.]com
- smtp[.]jacksallay[.]com
- smtp[.]markqualman[.]com
- thinkoralhealth[.]com
- upstagedu[.]com
- uscgx[.]com
- virginlaw[.]com
- webdisk[.]christianvelour[.]com
- webdisk[.]jacksallay[.]com
- webdisk[.]markqualman[.]com

Sample String-Connected Domains

- annetterawlings[.]net
- howasit[.]net
- johnshimkus[.]co
- lisasierra[.]work
- mitchellspearman[.]golf
- shehasgone[.]cn
- wlynch[.]cx