WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

A DNS Investigation of the GootLoader Campaign

Table of Contents

Executive Report

Back in 2015, a survey found that cats drove 15% of the overall Internet traffic. That said, it is not surprising for threat actors to use cat-related content to lure victims to visit their malware-laden sites. Such was the case for GootLoader, which allowed cybercriminals to steal data and deploy post-exploitation tools and ransomware.

Sophos recently analyzed GootLoader, which has been known to use search engine optimization (SEO) poisoning to gain initial access. Users who fall for the ruse get directed to a compromised site that hosts a malicious payload. If the malware remains undetected on a victim's computer, it makes way for a second-stage payload dubbed "GootKit," a highly evasive data stealer and remote access Trojan (RAT). Threat actors can use GootKit to deploy ransomware or other tools for follow-on exploitation.

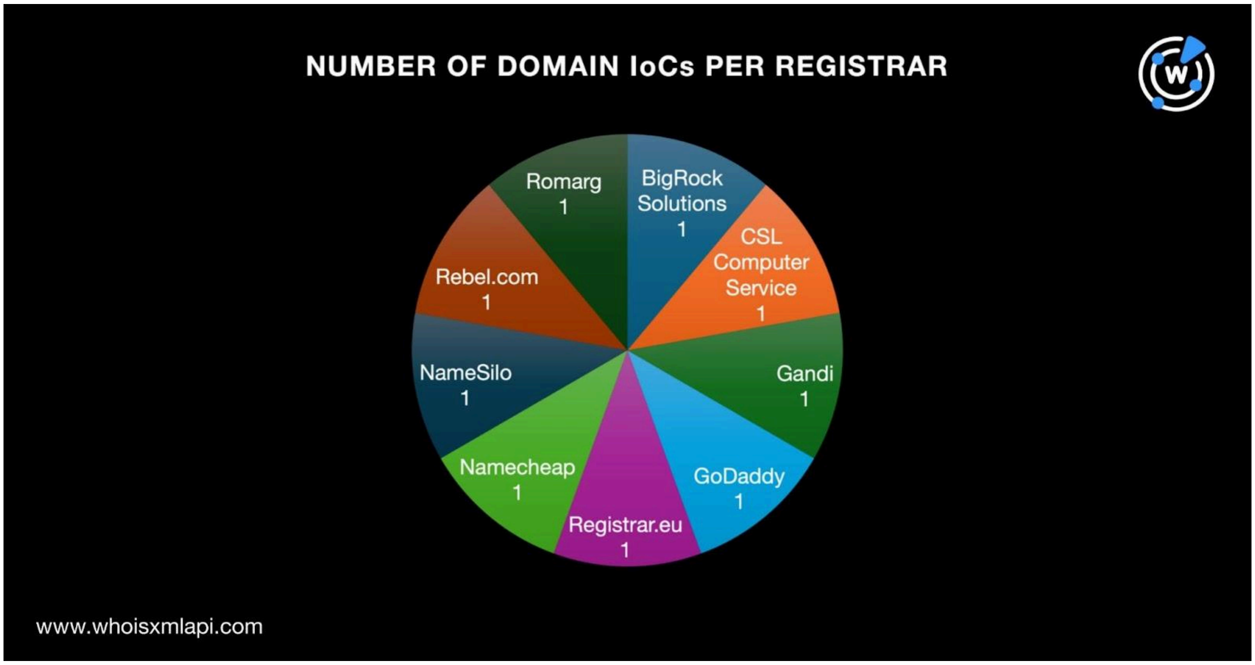
The Sophos researchers identified 12 domains as indicators of compromise (IoCs) in their report. The WhoisXML API research team expanded the IoC list aided by exhaustive DNS intelligence and found:

- 33 email-connected domains
- 15 IP addresses, six of which turned out to be malicious
- 692 IP-connected domains
- 302 string-connected domains

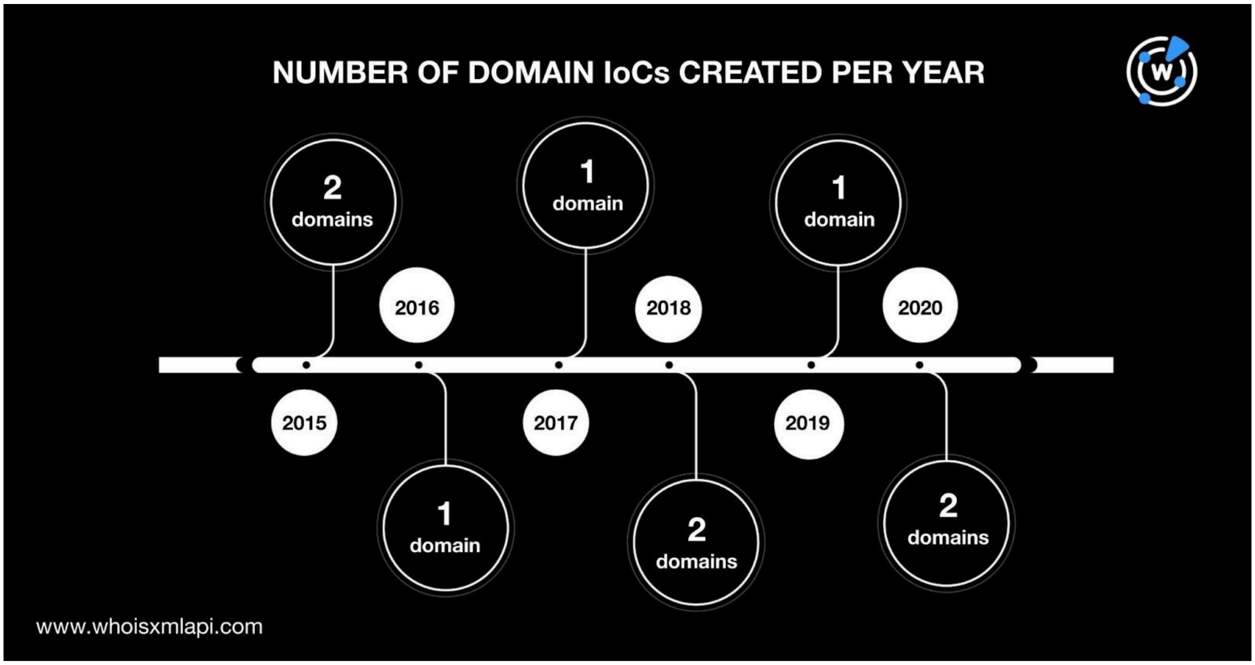
About the GootLoader IoCs

First off, we sought to find more information on the 12 domains tagged as IoCs. A bulk WHOIS lookup for them revealed that:

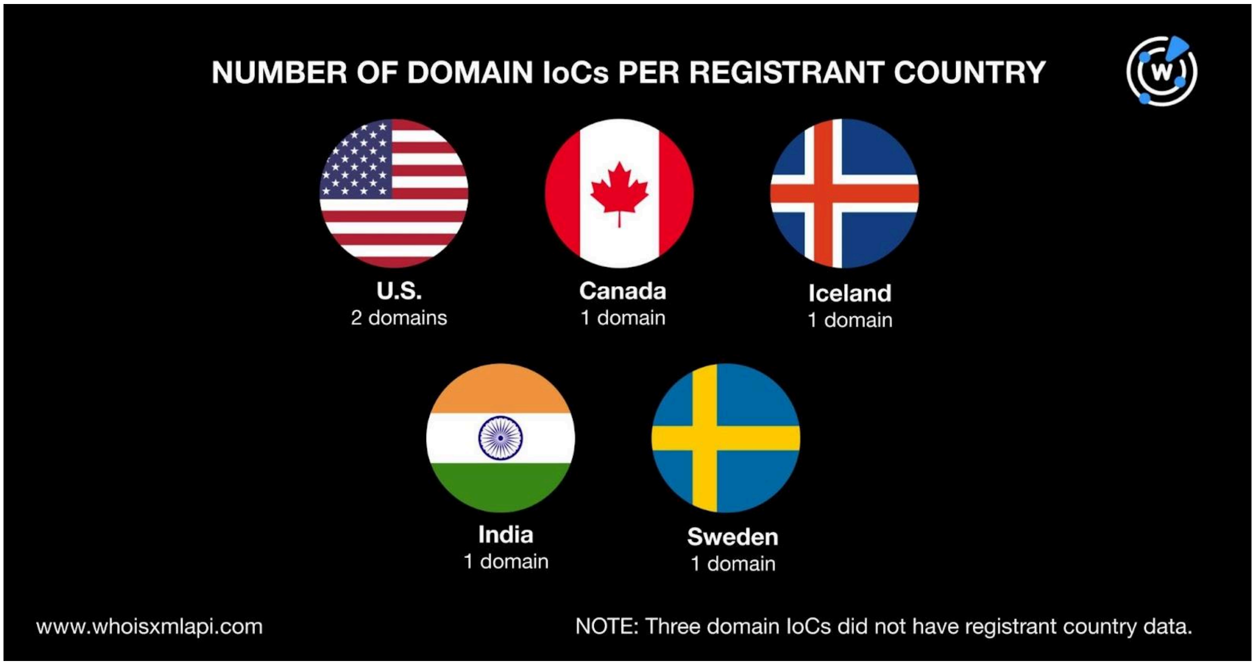
- Only nine of the domains had current WHOIS records.
- The nine domains with current WHOIS records were administered by a different registrar each, namely, BigRock Solutions, CSL Computer Service, Gandi, GoDaddy, Registrar.eu, Namecheap, NameSilo, Rebel.com, and Romarg.



- The nine domains were created between 2015 and 2020, indicating that the threat actors may have preferred using old domains.



- While three of the nine domains did not have registrant country details in their records, we found that two were registered in the U.S., while one each was registered in four different countries, namely, Canada, Iceland, India, and Sweden.



We also looked at the passive DNS records of the 12 domains tagged as IoCs and found that 83% or 10 of them have resolved to 50 or more IP addresses each since 2019. Take a look at five examples below.

DOMAIN IoC	DATE STARTED RESOLVING TO AN IP ADDRESS	TOTAL NUMBER OF IP ADDRESSES
beezzly[.]com	4 October 2019	50
chanderbhushan[.]com	2 May 2021	50
climatehero[.]me	4 October 2019	100+
fannisho[.]com	4 October 2019	51
playyourbeat[.]com	1 October 2019	92

The domain IoC playyourbeat[.]com, for instance, has seen 92 DNS changes since it first resolved to IP address 85[.]187[.]128[.]9 on 4 October 2019 according to DNS Chronicle Lookup. The first shift occurred 462 days after it was first recorded in our passive DNS database on 8 January 2021. After that, the number of days in-between each change ranged between one and 293 from 8 January 2021 to 1 September 2024.

GootLoader IoC List Expansion Findings

We began our search for connected artifacts by querying the 12 domains tagged as IoCs on WHOIS History API. That led to the discovery of 22 email addresses in their historical WHOIS records although only nine were public.

Next, we queried the nine public email addresses on Reverse WHOIS API. Three of them appeared in the current WHOIS records of other domains, leading us to uncover 33 email-connected domains after filtering out duplicates and the IoCs.

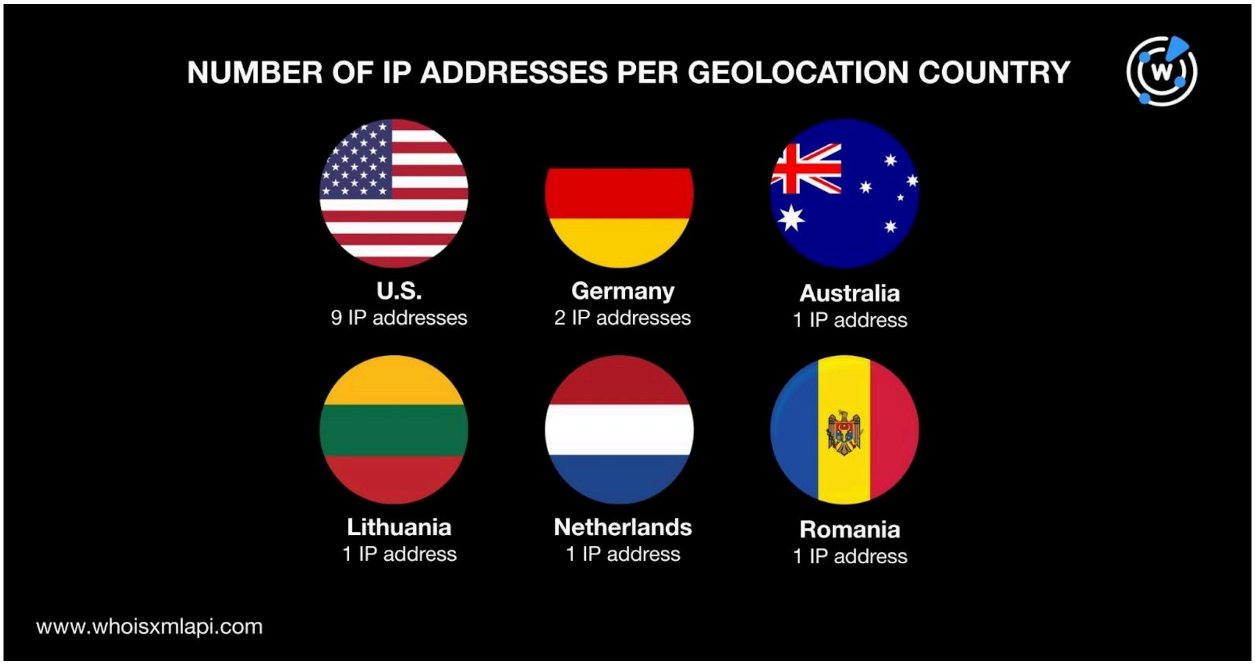
DNS lookups for the 12 domains tagged as IoCs showed that 11 actively resolved to 15 unique IP addresses.

Threat Intelligence API queries for the 15 IP addresses revealed that six have already figured in malicious campaigns. Take a look at three examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPES
103[.]169[.]142[.]0	Attack Command and control (C&C) Generic Malware Phishing Suspicious
141[.]193[.]213[.]10	Attack C&C Generic Malware Phishing Spam Suspicious
75[.]2[.]60[.]5	Attack C&C Generic Malware Phishing Spam

A bulk IP geolocation lookup for the 15 IP addresses showed that:

- They were geolocated in six different countries led by the U.S., which accounted for 9 or 60% of the IP addresses. Germany accounted for two IP addresses, while Australia, Lithuania, the Netherlands, and Romania accounted for one each.



NUMBER OF IP ADDRESSES PER GEOLOCATION COUNTRY

U.S.
9 IP addresses

Germany
2 IP addresses

Australia
1 IP address

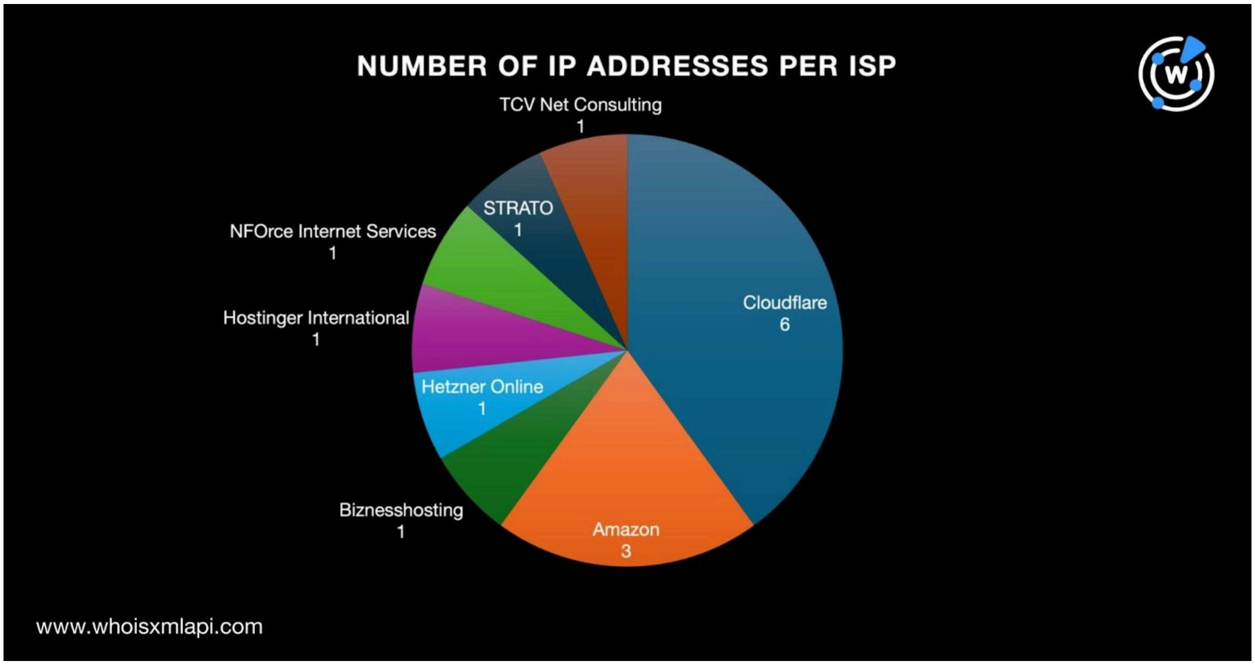
Lithuania
1 IP address

Netherlands
1 IP address

Romania
1 IP address

www.whoisxmlapi.com

- They were administered by eight different ISPs led by Cloudflare, which accounted for 40% of the IP addresses. Amazon accounted for three IP addresses, while Biznesshosting, Hetzner Online, Hostinger International, NFOrce Internet Services, STRATO, and TCV Net Consulting accounted for one each.



NUMBER OF IP ADDRESSES PER ISP

www.whoisxmlapi.com

We then queried the 15 IP addresses on Reverse IP API and found that nine of them could be dedicated hosts. The nine possibly dedicated IP addresses hosted 692 IP-connected domains after filtering out duplicates, the IoCs, and the email-connected domains.

As the final step, we used Domains & Subdomains Discovery to determine how many domains contained the same text strings as those tagged as IoCs. Out of the 12 strings the domains tagged as IoCs started with, these eight appeared at the beginning of other domains:

- beezzly.
- climatehero.
- fannisho.
- gobranded.
- ledabel.
- metropole.
- wowart.
- wyantgroup.

Our search led to the discovery of 302 string-connected domains after filtering out duplicates, the IoCs, and the email- and IP-connected domains.

—

Our in-depth DNS investigation of the GootLoader IoCs uncovered 1,042 potentially connected artifacts comprising 33 email-connected domains, 15 IP addresses, 692 IP-connected domains, and 302 string-connected domains. To date, six of the connected web properties have already been tagged as malicious.

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

- agitsolution[.]com
- ajaygour[.]com
- ayurvedkeraaz[.]com
- chanderbhushan[.]com
- climatehero[.]at
- climatehero[.]jp
- eurofoodsalexandriava[.]us
- garhwalsabhachd[.]com

- ghs47[.]com
- gmhs25[.]com
- gmhs26pl[.]com
- gmhsdhanasrc1[.]com
- gmhskarsan[.]com
- gmhsmaulicolonychd[.]com
- gmms23[.]com

Sample IP Addresses

- 103[.]169[.]142[.]0
- 104[.]26[.]6[.]29
- 104[.]26[.]7[.]29
- 136[.]243[.]223[.]149
- 141[.]193[.]213[.]10

Sample IP-Connected Domains

- a15p[.]uvronline[.]app
- a19p[.]uvronline[.]app
- a29p[.]uvronline[.]app
- a77p[.]uvronline[.]app
- abc-optic[.]ro
- abc-optics[.]ro
- abcoptic[.]ro
- abcpower[.]ro
- absensi[.]bengkaliskab[.]go[.]id
- academyadli[.]com
- acko[.]health
- adamlatoszynski[.]com
- adinabeauty[.]ir
- admin[.]gomexicorentacar[.]com
- admin[.]zaviaerp[.]com
- advanceddatarecovery[.]co[.]uk
- agingresearch[.]org
- agribiz[.]org
- akhbarworld[.]org
- akiel[.]de
- alghamdi[.]fun
- alirezabaghi[.]ir
- americanenergyinnovation[.]org
- americanfuturistpublishing[.]com
- amp[.]dascene[.]net
- apadanamatinshop[.]ir
- api-stage[.]kab[.]tools
- api-v2[.]laffahrestaurants[.]com
- api[.]birds[.]dog
- api[.]prismafinance[.]com
- api[.]stage[.]kab[.]tools
- api[.]zaviaerp[.]com
- app-ham[.]rvhotels[.]es
- app-hbb[.]rvhotels[.]es
- app-hcp[.]rvhotels[.]es
- app-hgc[.]rvhotels[.]es
- app-hnm[.]rvhotels[.]es
- app-hnp[.]rvhotels[.]es
- app-hsc[.]rvhotels[.]es
- app-stage[.]kab[.]tools
- app[.]ga179[.]com
- app[.]hotels[.]zaviaerp[.]com
- app[.]prismafinance[.]com
- app[.]stage[.]kab[.]tools
- applegift[.]ir
- arcamu[.]com
- arewealiens[.]com
- ariyanlift[.]com
- arrs[.]host
- asre4[.]com
- asset[.]birds[.]dog
- atlassteeledi[.]com
- atlus-capital[.]com
- atrinapetrogas[.]com
- autodiscover[.]reabilityonline[.]com
- avazhe[.]com

- awarehometest[.]com
- awatsurgical[.]com
- azarfilm-f[.]ir
- azincar[.]ir
- azyskowska[.]com
- bakercoin[.]com
- balancedvitality[.]cloud
- balanceessentials[.]cloud
- baldakas[.]lt
- balitbang[.]bengkaliskab[.]go[.]id
- baoba[.]ir
- bapenda[.]bengkaliskab[.]go[.]id
- bapokting[.]bengkaliskab[.]go[.]id
- bardonav[.]com
- bayiet[.]com[.]sa
- bazareqazvin[.]com
- be24x7[.]com
- beau-ty[.]pl
- beautymilly[.]com
- bellicon[.]com
- beloved[.]pk
- benefitsalliance[.]ca
- bengkaliskab[.]go[.]id
- benjaminque[.]net
- betkawa[.]com
- biologische-pflanzenpflege[.]shop
- birds[.]dog
- birdx[.]birds[.]dog
- bit-trust[.]pro
- bkpp[.]bengkaliskab[.]go[.]id
- blockswap[.]online
- blog[.]sfapp[.]magefan[.]top
- bodrumkebabandpizza[.]com
- booking[.]guruhotel[.]mx
- booking[.]sandbox[.]zaviaerp[.]com
- booking[.]zaviaerp[.]com
- booking2[.]zaviaerp[.]com
- boroughlottery[.]co[.]uk
- bortvita[.]lt
- bpkad[.]bengkaliskab[.]go[.]id
- brotcast-stage[.]kab[.]tools
- brotcast[.]stage[.]kab[.]tools
- broxbournelottery[.]co[.]uk
- bs588[.]co

Sample String-Connected Domains

- beezzly[.]eu
- beezzly[.]net
- beezzly[.]org
- climatehero[.]ai
- climatehero[.]app
- climatehero[.]ar
- climatehero[.]be
- climatehero[.]biz
- climatehero[.]ca
- climatehero[.]ch
- climatehero[.]co
- climatehero[.]co[.]nz
- climatehero[.]co[.]uk
- fannisho[.]ir
- fannisho[.]ws
- gobranded[.]co
- gobranded[.]co[.]in
- gobranded[.]co[.]uk
- gobranded[.]co[.]za
- gobranded[.]de
- gobranded[.]dk
- gobranded[.]email
- gobranded[.]gay
- gobranded[.]ink
- gobranded[.]me
- ledabel[.]com
- ledabel[.]com[.]tr
- ledabel[.]es
- ledabel[.]net
- ledabel[.]online

- metropole[.]adult
- metropole[.]ae
- metropole[.]agency
- metropole[.]app
- metropole[.]arq[.]br
- metropole[.]asia
- metropole[.]at
- metropole[.]au
- metropole[.]bayern
- metropole[.]be
- wowart[.]au
- wowart[.]be
- wowart[.]biz
- wowart[.]ca
- wowart[.]cat
- wowart[.]ch
- wowart[.]click
- wowart[.]club
- wowart[.]cn
- wowart[.]co
- wyantgroup[.]ca