WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

On the DNS Trail of the Rise of macOS Backdoors

Table of Contents

Executive Report

macOS has been gaining the unwanted attention of more and more backdoor operators since late 2023.

In February 2024, Bitdefender uncovered RustDoor, which was written in Rust and possibly has ties to the operators of a Windows ransomware. They published their findings, including seven indicators of compromise (IoCs) comprising five domain names and two IP addresses. Back in November 2023, meanwhile, SentinelOne analyzed crypto theft attacks targeting macOS users aided by KandyKorn. Their report unveiled four IP addresses as IoCs.

The WhoisXML API research team sought to find out how many potentially related web properties there are for the two threats in the DNS and uncovered:

- RustDoor-connected properties:
    - Five email-connected domains
    - Four additional IP addresses, one of which turned out to be malicious
    - 72 string-connected domains
- KandyKorn-connected properties:
    - 28 IP-connected domains, all of which turned out to be malicious

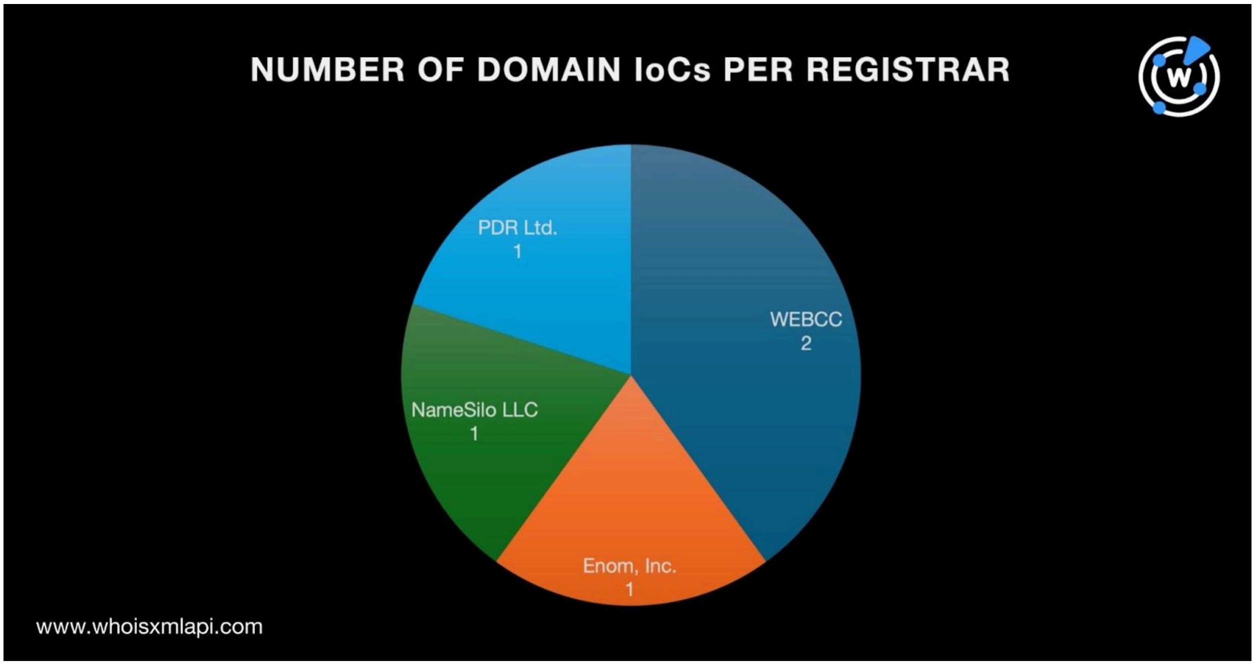
Dissecting RustDoor

RustDoor IoC Facts

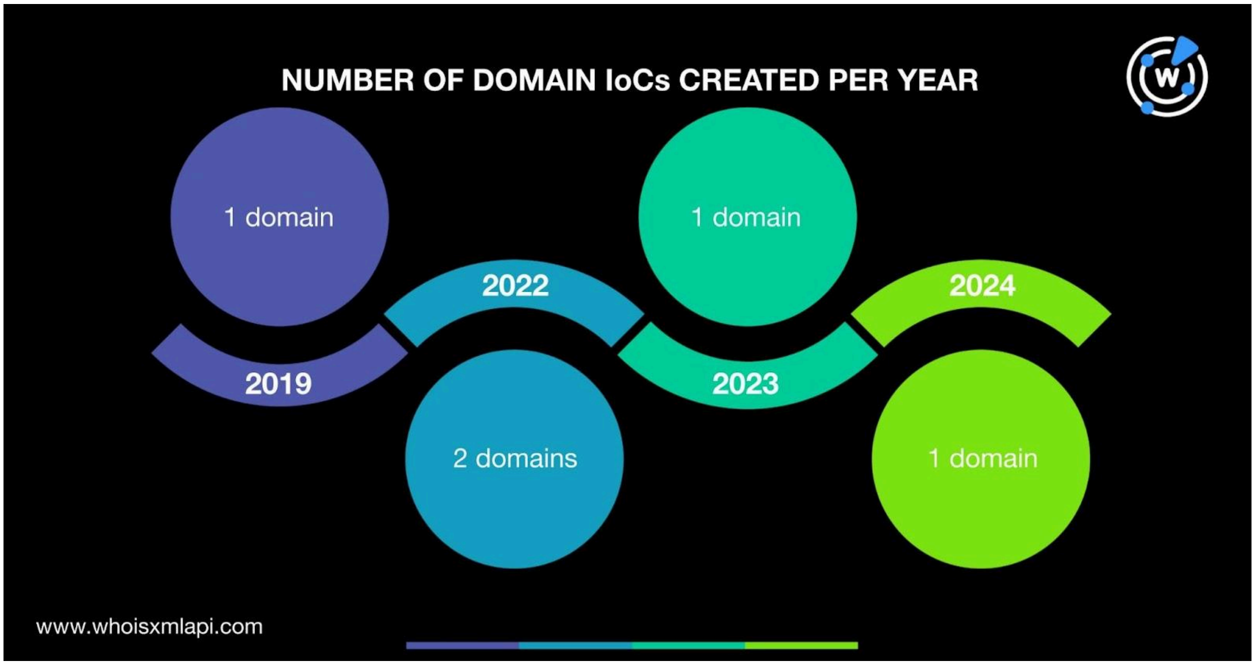
As per usual, we kicked off our analysis by looking more closely at the seven RustDoor IoCs—five domain names and two IP addresses.

A bulk WHOIS lookup for the five domain names identified as IoCs found that:

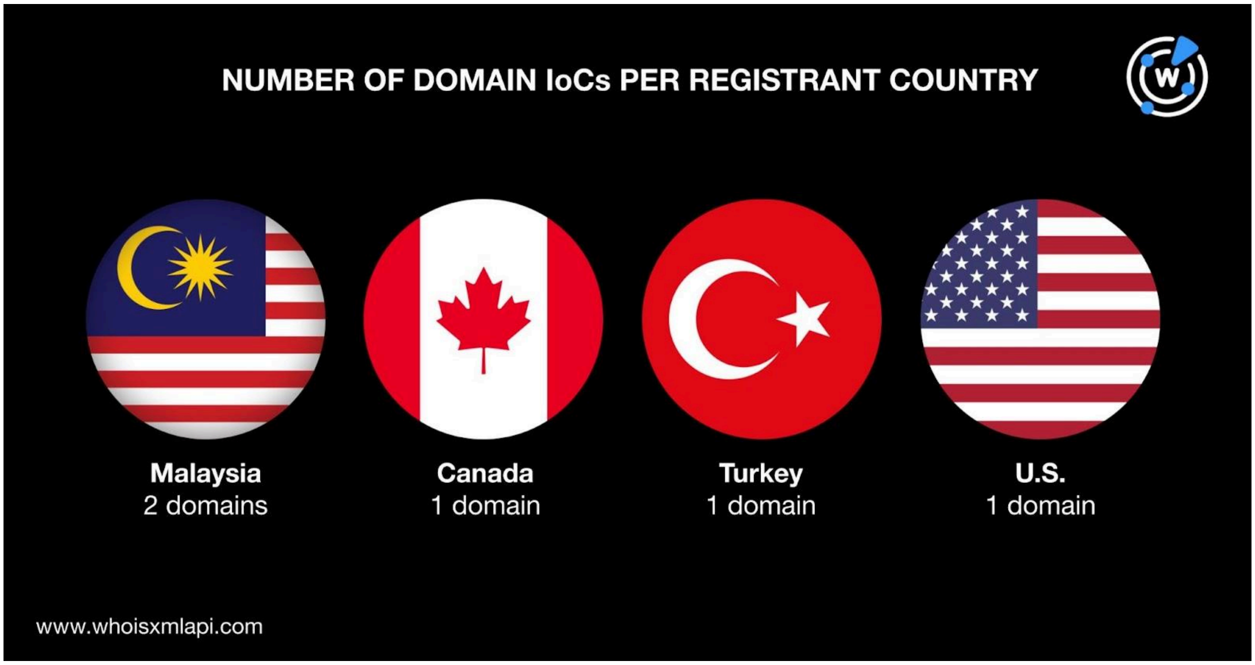
- They were distributed among four registrars led by WEBCC, which accounted for two domain IoCs. One domain IoC each was administered by Enom, Inc.; NameSilo LLC; and PDR Ltd.



- They were created between 2019 and 2024. Specifically, two domain IoCs were created in 2022 and one each was created in 2019, 2023, and 2024.



- They were registered in four different countries. Two domain IoCs were registered in Malaysia and one each was registered in Canada, Turkey, and the U.S.



IP geolocation lookups for the two IP addresses classified as IoCs revealed that:

- They were geolocated in two different countries—one IP address IoC in Hungary and the other in Seychelles.
- They were also administered by two different ISPs—one IP address IoC by Bunea Telecom SRL and the other by Alviva Holding Limited.

Two of the domain IoCs contained macOS- and iCloud-related text strings—maconlineoffice[.]com and serviceicloud[.]com—that could indicate attempts to legitimize their campaign. The threat actors possibly hoped to trick users into downloading the backdoor by making them think they were installing Microsoft 365 for Mac, Office for Mac, or iCloud.

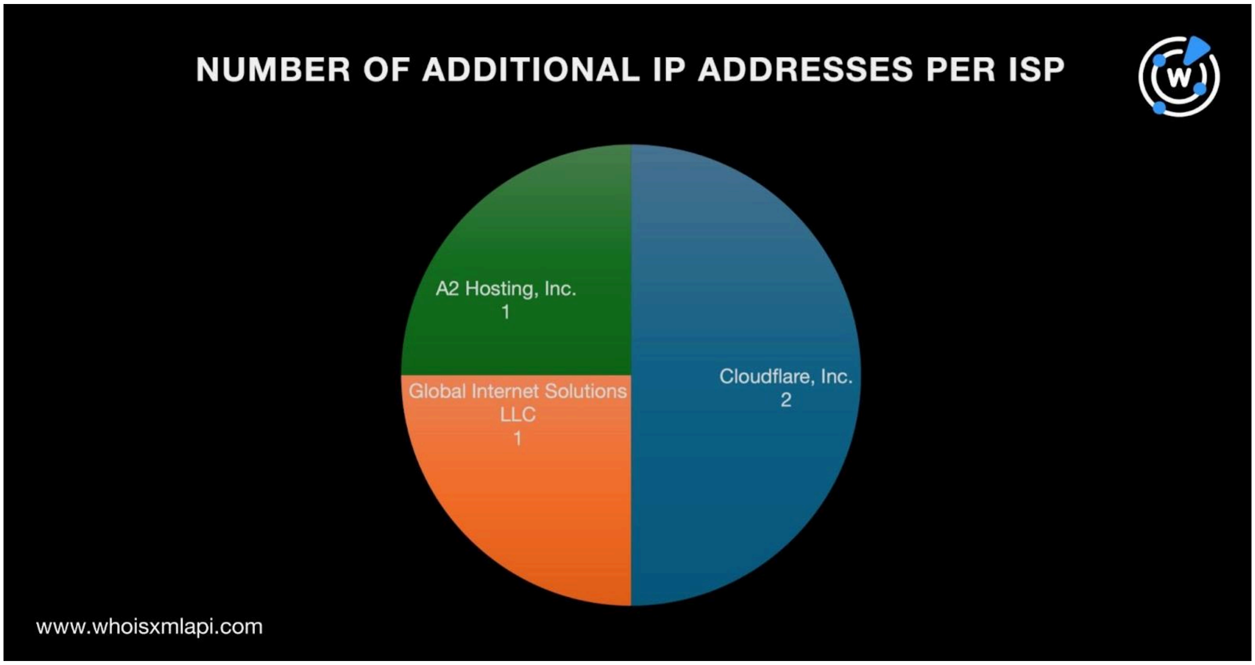
RustDoor IoC-Connected Analysis Findings

To find out if other RustDoor-connected artifacts were present in the DNS, we performed an expansion analysis beginning with WHOIS History API searches for the five domain names categorized as IoCs. That led to the discovery of 10 email addresses from their historical WHOIS records, one of which was public.

A current Reverse WHOIS API query for the public email address allowed us to collate five email-connected domains after duplicates and the IoCs were filtered out. Interestingly, judging by the domains (i.e., findmy-inc[.]us, findmy-lcloud[.]us, and findmyapp-location[.]us), a majority of them (three out of five domains) seemed to allude to connections to macOS's Find My asset tracking service.

Next, we performed DNS lookups for the five domain IoCs that enabled us to uncover four additional IP addresses. IP Geolocation Lookup showed that:

- They were spread across two geolocation countries—three in the U.S. and one in the Netherlands.
- They were administered by three ISPs led by Cloudflare, Inc., which accounted for two IP addresses. One IP address IoC each was handled by Global Internet Solutions LLC and A2 Hosting, Inc.



Threat Intelligence Lookup revealed that one of the additional IP addresses—85[.]187[.]128[.]40—was associated with phishing.

Next, we subjected the six IP addresses (i.e., the two originally identified as IoCs and four additional hosts) to reverse IP lookups. We found that two of them could be dedicated although they did not lead to any other connected domain that has not been dubbed an IoC or email-connected.

To cover all the bases, we used exact text strings found among the five domains named as IoCs as Domains & Subdomains Discovery search terms. That led to the discovery of 72 string-connected domains.

iCloud Impersonation Signs

To satisfy our curiosity, we searched for possible signs of iCloud impersonation. A Domains & Subdomains Discovery search for **icloud**-containing domain names created just this year (i.e., since 1 January 2024) uncovered 785 such web properties.

WHOIS record comparisons with apple[.]com showed that only one of them—icloud[.]global—could be publicly attributed to Apple based on its registrant organization.

Threat Intelligence API also revealed that eight of the **icloud**-containing domains were associated with phishing and generic threats. Specifically, all were phishing-related and one was also associated with a generic threat.

Investigating KandyKorn

KandyKorn IoC Facts

For our second case, SentinelOne identified four IP addresses as IoCs. IP geolocation lookups for them showed that:

- They were all geolocated in the U.S.
- They were also administered by a single ISP—Hostwinds LLC.

KandyKorn IoC-Connected Analysis Findings

To find other potentially connected artifacts, we began with reverse IP lookups for the four IP addresses tagged as IoCs. We found out that three of them could be dedicated and enabled us to collate 28 IP-connected domains after duplicates were removed.

Threat intelligence lookups for the 28 IP-connected domains revealed that all of them were associated with malware attacks.

—

Our in-depth DNS foray into two of the latest macOS backdoors using a total of 11 IoCs as expansion analysis jump-off points led to the discovery of 109 potentially connected artifacts. Specifically, they allowed us to uncover five email-connected domains, four additional IP addresses, 28 IP-connected domains, and 72 string-connected domains. The analysis also revealed that 29 of the web properties we dug up were malicious—one was associated with phishing and 28 could be malware hosts.

That said, the 109 additional artifacts possibly related to RustDoor and KandyKorn inferred the presence of additional threats that have not yet been identified or reported to date. And the 785 **icloud**-containing domains, eight of which were malicious, pointed to threats targeting the cloud service.

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

RustDoor

Sample Email-Connected Domains

- findmy-inc[.]us
- findmy-Icloud[.]us
- findmyapp-location[.]us

Sample Additional IP Addresses

- 104[.]21[.]24[.]221
- 172[.]67[.]220[.]221

Sample String-Connected Domains

- linksammosupply[.]ca
- serviceicloud-webapps[.]us
- serviceicloud[.]business
- serviceicloud[.]ir
- serviceicloud[.]ml
- serviceicloud[.]monster
- serviceicloud[.]us
- serviceicloud[.]ws
- serviceicloud10[.]com
- serviceicloudaccount[.]info
- serviceicloudaccountdisabled[.]ga
- serviceicloudapple[.]com
- serviceicloudcenter[.]com
- serviceicloudiddataaccountdvs[.]com
- serviceicloudmail[.]com
- serviceicloudmanager[.]com
- serviceiclouds[.]biz
- serviceiclouds[.]com
- serviceicloudwebapps[.]us
- turkishfurniture-b2b[.]com

Sample icloud-Containing Domains

- 13247-icloud[.]com
- 360multicloud[.]com
- 360multicloud[.]de
- 666bandit666icloud[.]com
- 81tbicloud[.]com
- accounts-icloud[.]us
- agamicloud[.]com
- agicloud[.]ai
- agicloudservices[.]com
- agicloudtech[.]com
- agicloudtraining[.]com
- agicloudtransformation[.]com
- agricloud[.]asia
- ahuicloud[.]top

- ai-multicloud[.]com
- ai-multicloud[.]de
- aicloud[.]au
- aicloud[.]com[.]au
- aicloud[.]expert
- aicloud[.]no
- aicloud[.]sg
- aicloud[.]xn--fiqs8s
- aicloud[.]xn--fiqz9s
- aicloud4all[.]com
- aicloud4all[.]pt
- aicloudassist[.]com
- aicloudcomputingai[.]com
- aicloudcraft[.]com
- aiclouderp[.]com
- aicloudexec[.]com
- aicloudgenius[.]online
- aicloudhostai[.]com
- aicloudinfy[.]com
- aicloudjiasu[.]xyz
- aicloudkit[.]com
- aicloudlabs[.]ai
- aicloudlinks[.]com
- aicloudllc[.]com
- aicloudltd[.]co[.]uk
- aicloudnative[.]io
- aicloudoc[.]com
- aicloudpartner[.]pl
- aicloudprivacy[.]com
- aicloudservice[.]org
- aicloudtech[.]dev
- aicloudtechsolutions[.]com
- aicloudtest[.]cn
- aiicloudtech[.]com
- aiq-multicloud[.]com
- aiqmulticloud[.]com
- akamaicloudday[.]com
- alerta-icloud[.]us
- alicloud[.]io
- alicloud[.]realtor
- alicloudentertainment[.]com
- alicloudinc[.]cn
- alicloudos[.]cn
- alicloudscdn[.]com
- alicloudtest[.]xyz
- alpha-icloud[.]aquila[.]it
- altariclouds[.]com
- alticloud[.]co
- andiamicloud[.]com
- andiamicloud[.]org
- andylawabwinicloud-zxcvbasdqwe[.]com
- angelastewart59icloud[.]com
- anth77521icloud[.]com
- anthony2985icloud[.]com
- anticloud[.]lol
- anticloud[.]monster
- anticloud[.]site
- anticloud[.]space
- anticloudspam[.]com
- aolanicloud[.]sg
- ap-icloud[.]store
- apicloud[.]ir
- app-fmicloud[.]info
- app-onlineicloud[.]info
- appcloudicloud[.]online
- apple-icloud-support[.]online
- apple-icloud[.]photos
- appleicloud-gps[.]com
- appleicloud[.]cam
- appleprooficloudtw[.]com
- apps-icloud-id[.]click
- arabicloud[.]ai
- areasicloud[.]com
- arianaicloud[.]com
- artistatlarge01icloud[.]uk
- aselicloud[.]net
- asimji321icloud[.]com
- assaicloud[.]nl
- aus-icloud[.]com

- authicloud[.]net
- autobicloudbot[.]com
- avicloud[.]cl
- aytounnoumeiricloud[.]com
- azamicloud[.]com
- azaricloud[.]ir
- banicloud[.]ir

KandyKorn

Sample IP-Connected Domains

- bitscrunch[.]linkpc[.]net
- bitscrunnch[.]linkpc[.]net
- coupang-network[.]pics
- datasend[.]fun
- dma[.]linkpc[.]net
- docs-send[.]online
- docsend-host[.]cloud
- docsendinfo[.]linkpc[.]net
- exodus[.]linkpc[.]net
- floriventurescapital[.]linkpc[.]net
- floriventuresfinance[.]linkpc[.]net
- floriventuresfund[.]linkpc[.]net
- gumi-cryptos[.]loan
- indaddy[.]xyz