macOSバックドアの台頭をDNSで追跡

目次

要旨

2023年後半以降、macOSは多くのバックドアオペレーターを引きつけています。Bitdefenderは2024年2月、Rustで書かれ、Windowsランサムウェアのオペレーターと関係している可能性のある「RustDoor」を発見し、その調査結果および7個のセキュリティ侵害インジケーター（IoC）（5個のドメインIoCと2個のIPアドレスIoC）を公表しました。他方、SentinelOneは2023年11月に、macOSユーザを標的とした「KandyKorn」による暗号窃取攻撃を分析しました。SentinelOneのレポートでは、4個のIPアドレスがKandyKornのIoCとして公開されました。

WhoisXML APIの研究チームはこのほど、RustDoorとKandyKornのIoCをもとに、それぞれと関連するウェブプロパティが他にどれだけ存在しているかをDNSで調査しました。その結果、以下を発見しました：

- RustDoor関連：
    - ドメインIoCと同じメールアドレスを使用していたドメイン名5個
    - 新たに検出されたIPアドレス4個。そのうち1個は悪意あるアドレス
    - ドメインIoCと同じ文字列を含むドメイン名72個
- KandyKorn関連：
    - IPアドレスIoCによってホストされていたドメイン名28個。その全てが悪意あるドメイン名

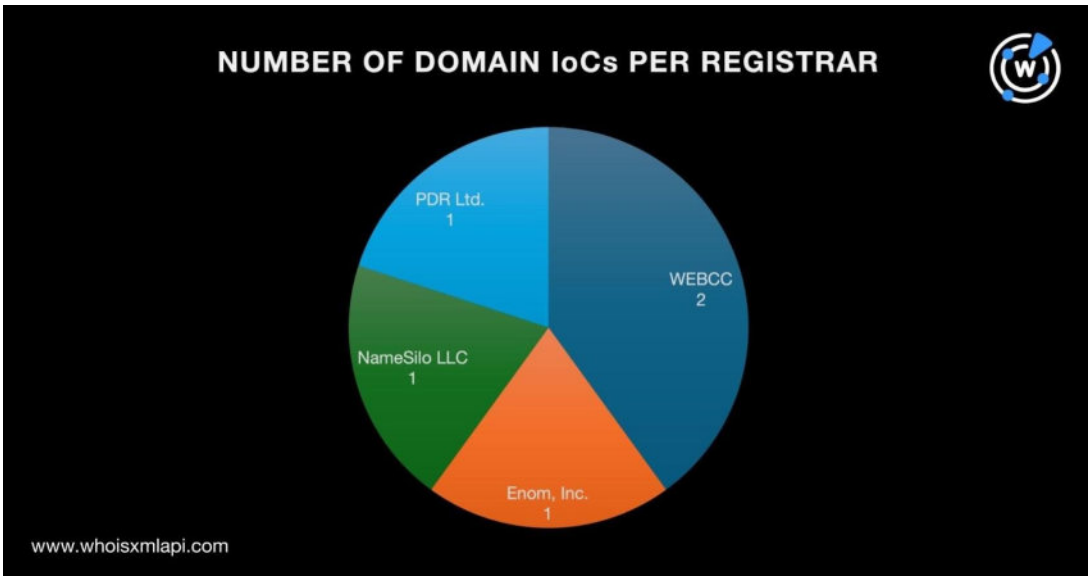
RustDoorの調査

RustDoorのIoCの実態

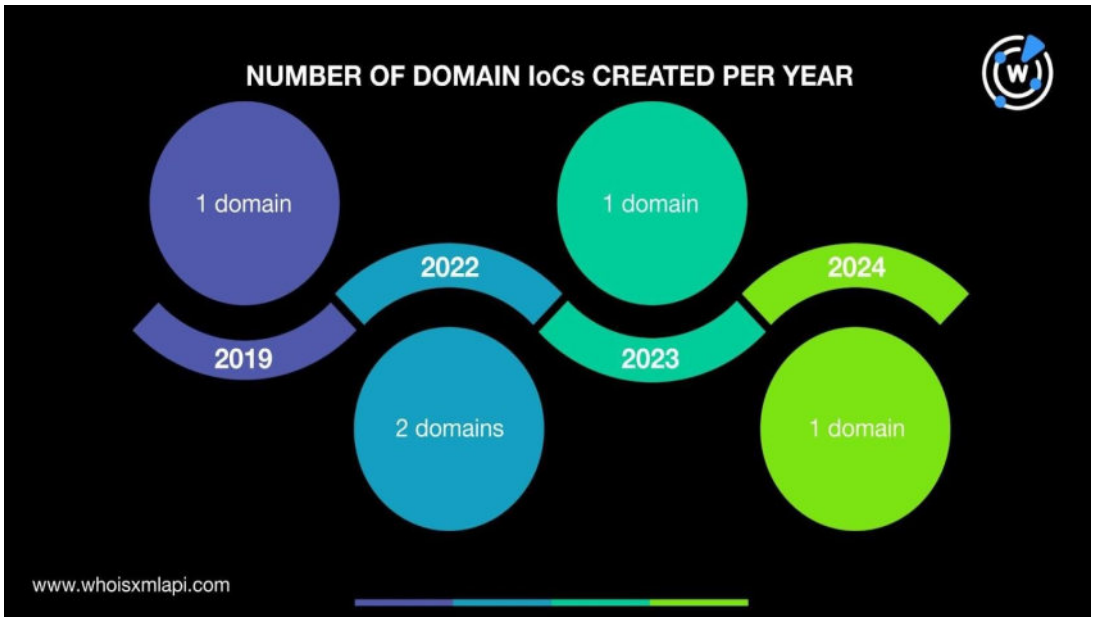
まず、RustDoorの7つのIoC（5個のドメインIoCと2個のIPアドレスIoC）を詳しく調べることから分析を始めました。

5個のドメインIoCをBulk WHOIS Lookupで調べたところ、以下のことがわかりました：

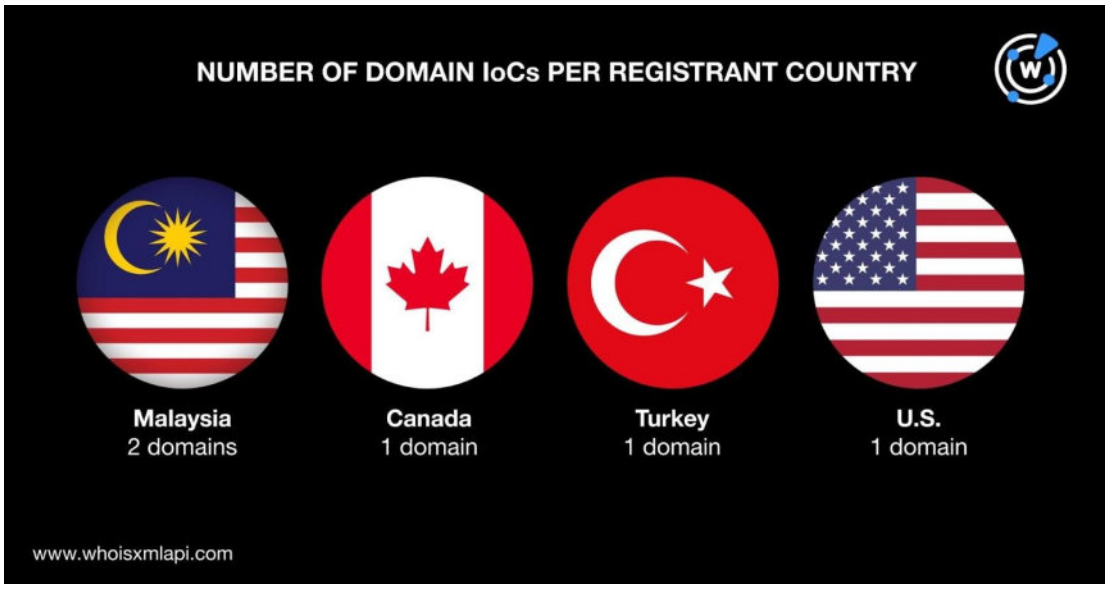
- 5個のうち2個はWEBCCというレジストラが管理していました。また、Enom, Inc.、NameSilo LLCおよびPDR Ltd.が1個ずつを管理していました。



- 2個のドメインIoCは2022年に新規登録されたものです。また、2019年、2023年および2024年に1個ずつが新規登録されていました。



- 2個はマレーシアで、1個ずつがカナダ、トルコおよび米国で登録されていました。



2個のIPアドレスIoCについてIP Geolocation Lookupを実行したところ、以下のことが判明しました：

- 1個はハンガリー、もう1個はセーシェルに位置するIPアドレスでした。
- 1個はBunea Telecom SRL 、もう1個はAlviva Holding Limited というISPによって管理されていました。

5個のドメインIoCのうち2個（maconlineoffice[.]com とserviceicloud[.]com）には、macOSおよびiCloudに関連したテキスト文字列が含まれていました。RustDoorのオペレーターはそれらのドメイン名で自分たちのキャンペーンを正当化しようとしたのかもしれません。ユーザーにMicrosoft 365 for Mac、Office for Mac、またはiCloudをインストールしていると思わせることで、バックドアをダウンロードさせようとした可能性があります。

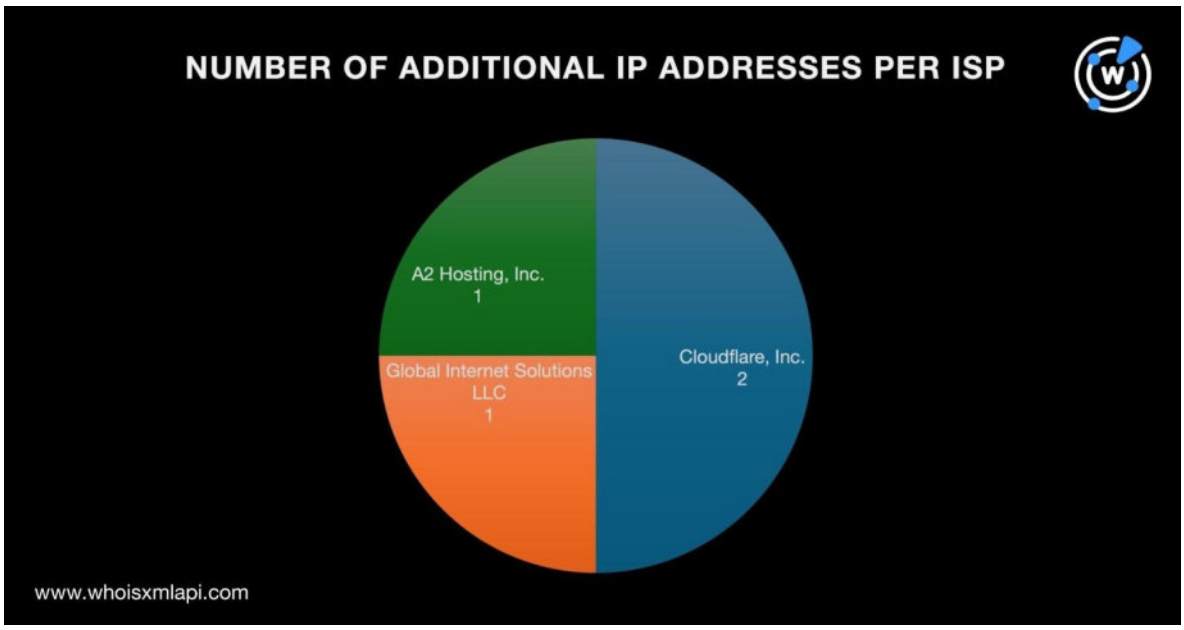
RustDoor IoCの関連アーティファクト

他のRustDoor関連のアーティファクトがDNSに存在するかどうかを調べるため、5個のドメインIoCをキーワードにWHOIS History APIで検索したところ、過去のWHOISレコードから10個のメールアドレスが検出されました。そして、そのうちの1個は公開されていました。

その公開メールアドレスをReverse WHOIS APIにかけ、アウトプットから重複と既存IoCを取り除いた結果、そのメールアドレスを共用していたドメイン名を5個発見できました。そのドメイン名の文字列から、5個のうち3個（findmy-inc[.]us、findmy-lcloud[.]us、findmyapp-location[.]us）はmacOSの「Find My」追跡サービスとの関連を示唆していると思われます。

次に、5個のドメインIoCに対してDNS Lookupを実行し、新たに4個のIPアドレスを特定できました。さらにその4個のIPアドレスについてIP Geolocation Lookupを実行した結果、以下が明らかになりました：

- 3個は米国、1個はオランダを指していました。
- 2個はCloudflare, Inc.が管理していました。また、Global Internet Solutions LLCとA2 Hosting, Inc.がそれぞれ1個を管理していました。



そして、Threat Intelligence Lookupにより、追加で見つかった4個のうちの1つ（85[.]187[.]128[.]40）がフィッシングに関連していることが判明しました。

次に、6個のIPアドレス（2個のIPアドレスIoCと今回新たに見つかった4個のIPアドレス）をReverse IP Lookupにかけました。その結果、2個については専用アドレスかもしれないとわかりましたが、それらはドメインIoCやドメインIoCとメールアドレスを共用しているドメイン名には繋がりませんでした。

さらに、5個のドメインIoCに含まれているテキスト文字列を検索語としてDomains & Subdomains Discoveryを実行しました。その結果、ドメインIoCと同じ文字列を含むドメイン名が72個検出されました。

iCloudなりすましの兆候

次に、iCloudのなりすましの可能性を探しました。Domains & Subdomains Discoveryで、**icloud**という文字列を含み、かつ2024年1月1日以降に新規登録されたドメイン名を検索したところ、785個が該当しました。

それらのWHOISレコードをapple[.]comのWHOISレコードと比較した結果、登録者情報からApple社に帰属していることを確認できたドメイン名は1個（icloud[.]global）しかありませんでした。

Threat Intelligence APIにより、**icloud**という文字列を含む785個のドメイン名のうち8個がフィッシングやジェネリックな脅威と関連していることも明らかになりました。具体的には、8個の全てがフィッシングに関連しており、うち1つはジェネリックな脅威にも関わっていました。

KandyKornの調査

KandyKornのIoCの実態

SentinelOneは、KandyKornのIoCとして4個のIPアドレスを特定しました。今回、それらをIP Geolocation Lookupで調べた結果、以下がわかりました：

- 全て米国に位置するIPアドレスでした。
- 全てがHostwinds LLCというISPの管理するIPアドレスでした。

KandyKornのIoCとの関わり

他の潜在的な関連アーティファクトを特定するため、4個のIPアドレスIoCをReverse IP Lookupにかけました。その結果、3個は専用アドレスらしいことがわかりました。また、その3個の専用らしいIPアドレスによってホストされているドメイン名が28個見つかりました（重複を除く）。

その28個のドメイン名を使ってThreat Intelligence Lookupで検索したところ、全てがマルウェア攻撃と関連していたことが判明しました。

—

今回、11個のIoCをもとに2つのmacOSバックドアについてDNSで徹底的に調査した結果、潜在的な関連アーティファクトが109個特定されました。具体的には、ドメインIoCと同じメールアドレスを共用しているドメイン名5個、IPアドレス4個、IPアドレスIoCによってホストされているドメイン名28個、ドメインIoCと同じ文字列を含むドメイン名72個を発見することができました。また、解析の結果、発見したウェブプロパティのうち29個が悪意あるもの（1個はフィッシングに関連しており、28個はマルウェアのホストの可能性がある）と判明しました。

RustDoorとKandyKornとの関連が疑われるアーティファクトが109個追加されたことから、これまでに特定も報告もされていない新たな脅威が存在していると推測できます。また、**icloud**という文字列を含むドメイン名785個（うち8個は悪意あるドメイン名）は、クラウドサービスを標的にした脅威の可能性を示唆しています。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトの例

RustDoor

ドメインIoCと同じメールアドレスを使用していたドメイン名の例

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

新たに検出されたIPアドレスの例

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

ドメインIoCと同じ文字列を含むドメイン名の例

- 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

icloudという文字列を含むドメイン名の例

- 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

IPアドレスIoCによってホストされていたドメイン名の例

- 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