Kimsuky：DNSでインテリジェンスを収集

目次

要旨

北朝鮮を拠点として2013年から活動している高度標的型攻撃（APT）グループ「Kimsuky Group」は、今年もすでに数回にわたり攻撃を仕掛けています。このグループは、標的にスピアフィッシング攻撃を仕掛けて最初のアクセスを獲得する手口で有名になりました。現在も基本的な手口は変わっていませんが、ペイロードの配信手段が、感染したHangul Word Processor（HWP）やMicrosoft Wordの文書という当初の形から、悪意あるLNKファイルやショートカットファイルを含んでいる、またはそれらのダウンロードに誘導する圧縮ファイルあるいは埋め込みリンクへと変遷しています。

AhnLab Security Emergency Response Center（ASEC）は先般、RftRATとAmadeyを使用した最新のKimsuky攻撃に関する詳細な調査結果を公表し、その中でセキュリティ侵害インジケーター（IoC）として6個のドメイン名と7個のIPアドレスを特定しました：

Kimsuky攻撃のIoC	
ドメイン名	**IPアドレス**
brhosting[.]net	152[.]89[.]247[.]57
prohomepage[.]net	172[.]93[.]201[.]248
splitbusiness[.]com	192[.]236[.]154[.]125
techgolfs[.]com	209[.]127[.]37[.]40
theservicellc[.]com	23[.]236[.]181[.]108
topspace[.]org	45[.]76[.]93[.]204
	91[.]202[.]5[.]80

WhoisXML APIの研究チームはこれを受け、ASECによるIoCリストをもとに、Kimsukyが将来攻撃で悪用する可能性のある他のエントリーポイントをDNSで徹底的に探しました。その結果、以下を発見することができました：

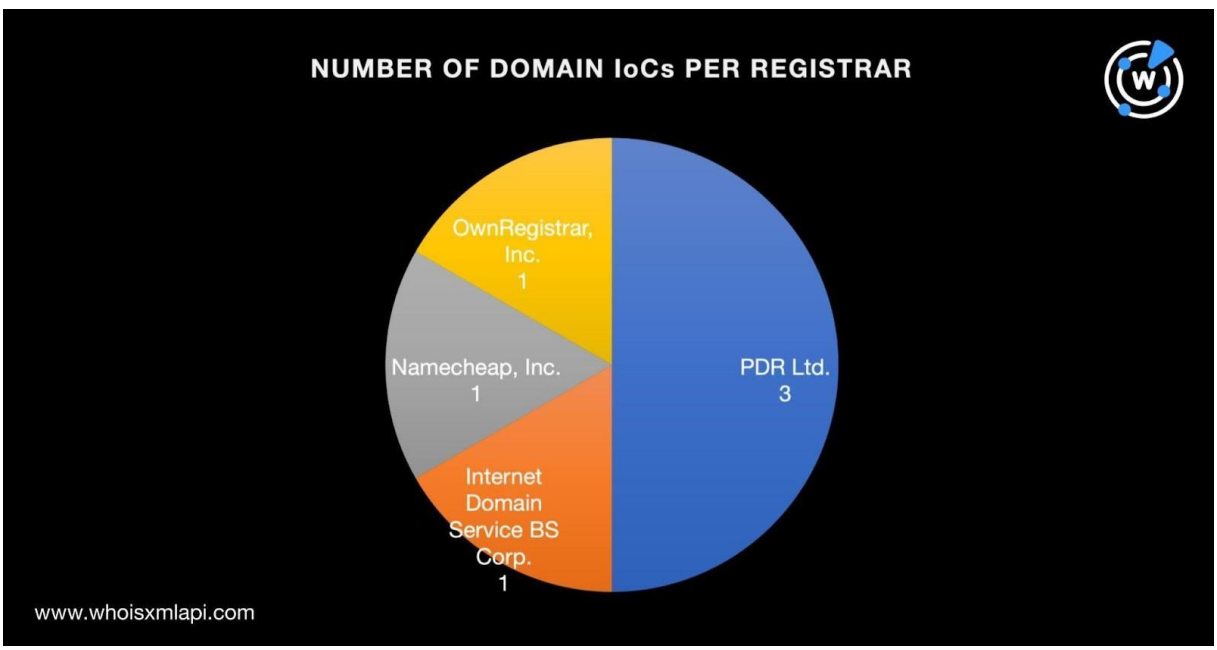
- 共通のメールアドレスを使用していた336個のドメイン名
- IoCとして特定されたドメイン名6個が名前解決した5個のIPアドレス。そのうち2個は様々な脅威と関連
- 共通のIPアドレスを使用していた5個のドメイン名
- IoCとして特定されたドメイン名と同じ文字列を含む356個のドメイン名

Kimsuky攻撃のIoC

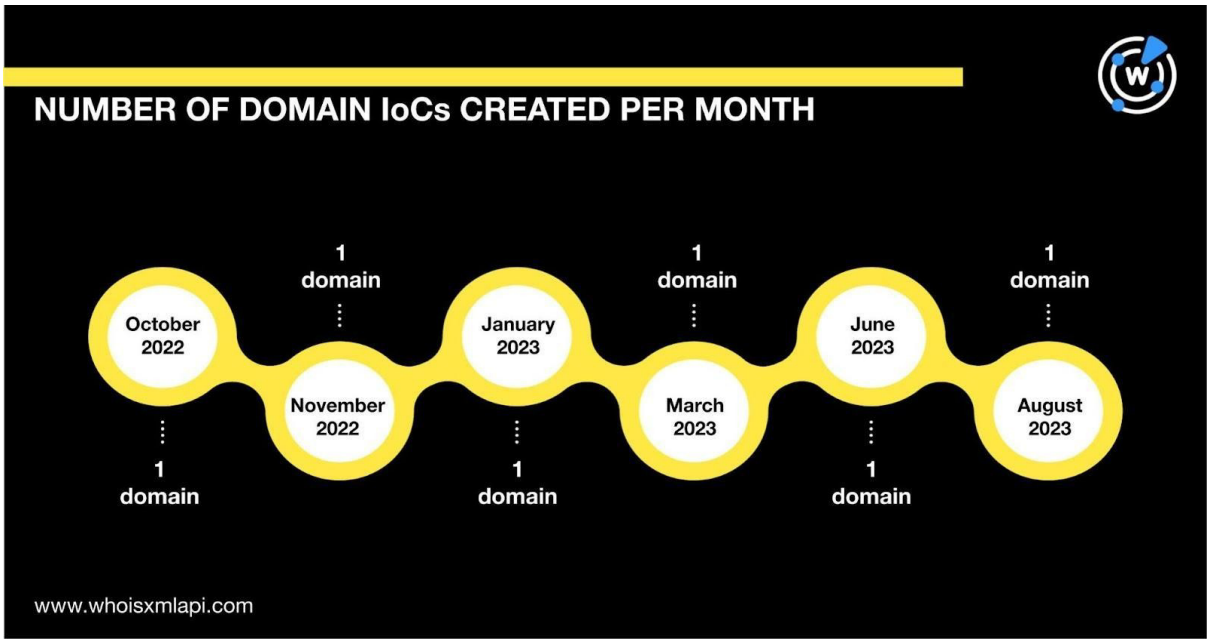
当社のチームはまず、IoCと特定された13個のウェブプロパティ（6個のドメイン名と7個のIPアドレス）を詳しく調べることから始めました。

6個のドメイン名（以下「ドメインIoC」）をBulk WHOIS Lookupにかけたところ、以下が判明しました：

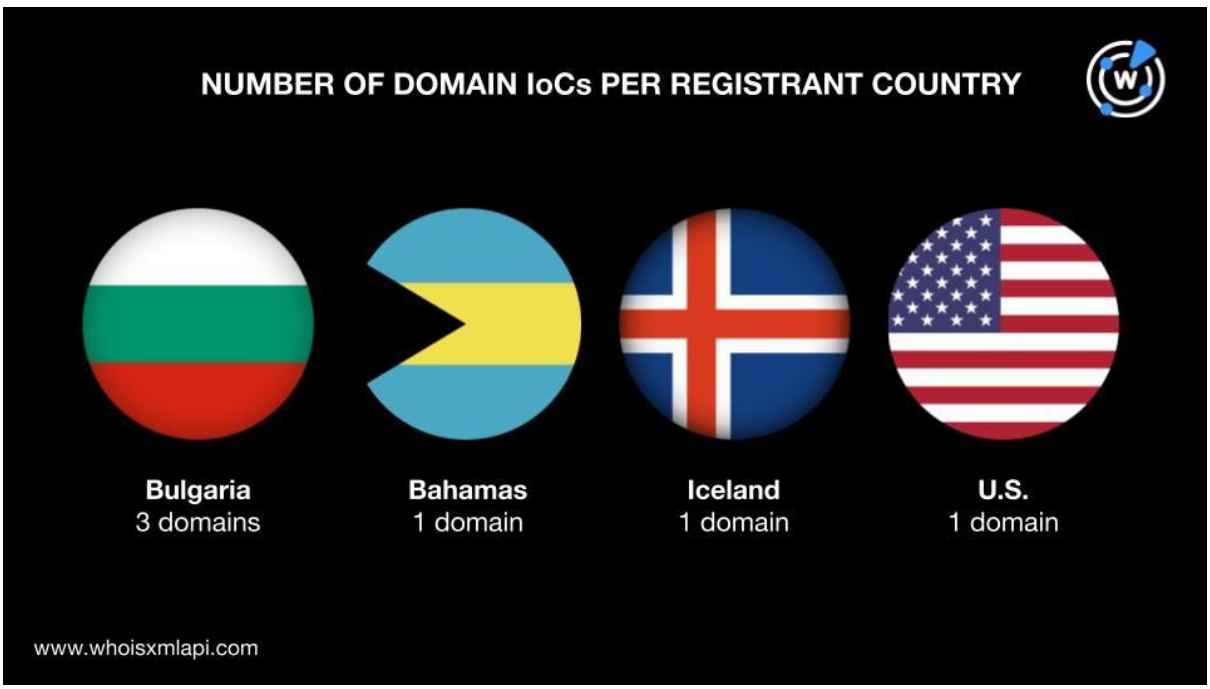
- 6個は4社のレジストラに分散しており、そのうち最も多くの管理レジストラになっていたのはPDR Ltd.（3個）でした。この他、Internet Domain Service BS Corp.、Namecheap, Inc.およびOwnRegistrar, Inc.が1個ずつのドメインIoCを管理していました。



- 6個はいずれも最近新規登録されたドメイン名です（2個は2022年、4個は2023年）。

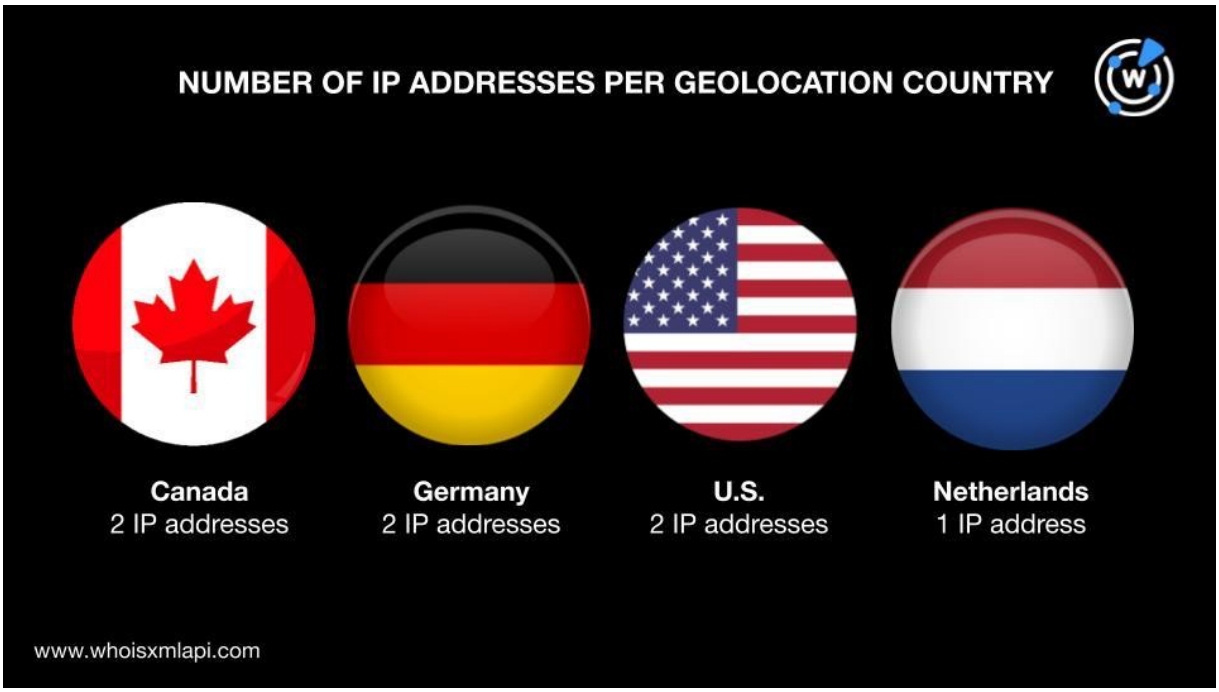


- ブルガリアで登録されたドメインIoCが最も多く、3個ありました。また、バハマ、アイスランドおよび米国で1個ずつが登録されていました。

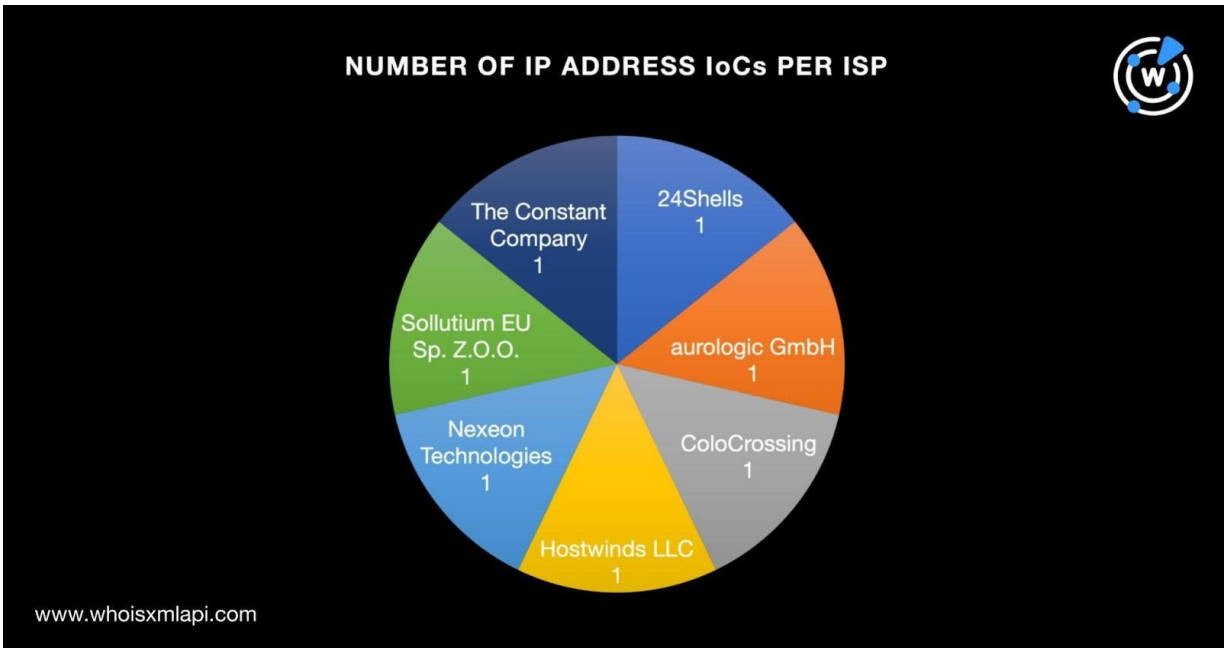


次に、IoCとして特定された7個のIPアドレス（以下「IPアドレスIoC」）についてBulk IP Geolocation Lookupを実行した結果、以下のことがわかりました：

- カナダ、ドイツおよび米国にそれぞれ2個が地理的に位置していました。残りの1個はオランダのIPアドレスでした。



- 24Shells、aurologic GmbH、ColoCrossing、Hostwinds LLC、Nexeon Technologies、Sollutium EU Sp. Z.O.O.およびThe Constant Companyがそれぞれ1個の管理ISPとなっていました。



Kimsukyの攻撃インフラの背後に迫る

Kimsukyの現在の攻撃インフラに関する情報を可能な限り入手するため、6個のドメインIoCをWHOIS History APIで検索してみました。その結果、過去のWHOISのいずれかのレコードに記録されている30個のメールアドレスが見つかりました。

そのうち、公開のメールアドレスは7個ありました。その7個をReverse WHOIS Searchで調べたところ、 3個がドメイン名336個の現在のWHOISレコードに表示されました。それらのドメイン名に重複はなく、また、いずれもIoCとして特定されたことがないものでした。

興味深いのは、そのうち29個のドメイン名は、暗号通貨、ブロックチェーン、非代替性トークン（NFT）関連の脅威に悪用される可能性があるということです。いくつかの例を以下の表に示します。

テキスト文字列	共通のメールアドレスを使用していたドメイン名の例
blockchain	ablockchaincompany[.]com
bitcoin	bitcoinmover[.]com
btc	btclightningnetwork[.]com
coin	coinmarket[.]ca

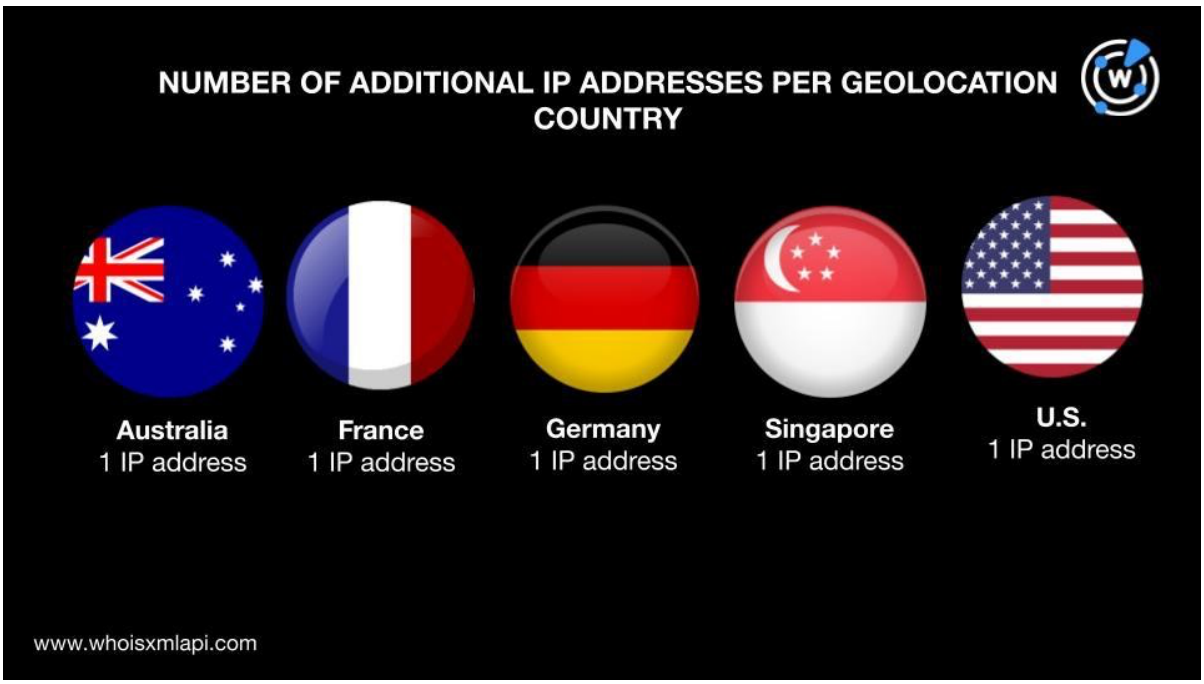
crypto	cryptoadept[.]com
matrix	matrixcoin[.]net
meta	metapayment[.]ca
nft	nfttrader[.]ca
token	tokenpromoter[.]com

同じメールアドレスで紐づけられているドメイン名に対してScreenshot Lookupを実行したところ、37個が指していたウェブサイトは本稿執筆時点でアクセス可能なままでした。ただし、その中で機能しているサイトに繋がったドメイン名はわずか8個でした。

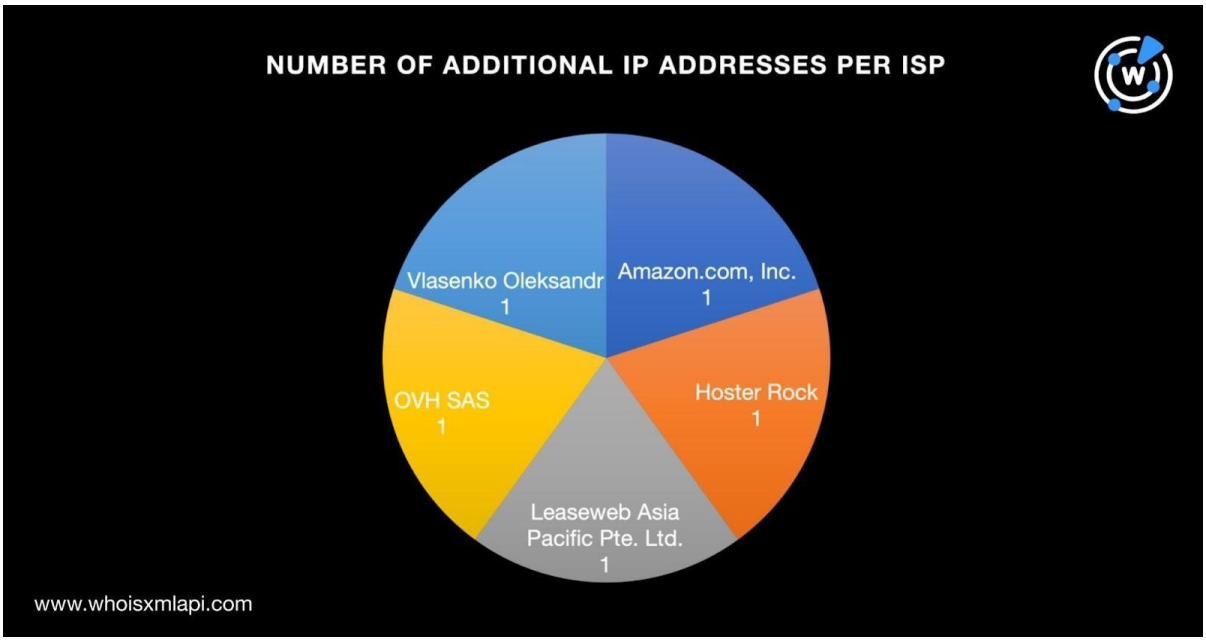
次に、6個のドメインIoCをDNS lookupで調べた結果、これまでにIoCとして特定されたことのない5個のユニークなIPアドレスに名前解決しました。

その5個のIPアドレスをIP Geolocation Lookupで分析した結果、以下のことが判明しました：

- 5個はそれぞれ別の国に位置していました（オーストラリア、ドイツ、フランス、シンガポール、米国）。そのうち2個は、IPアドレスIoCのうち2つと同様に、ジオロケーションがドイツと米国でした。



- 5個のIPアドレスは、管理ISPについても全て別々でした（Amazon.com, Inc.、Hoster Rock、Leaseweb Asia Pacific Pte. Ltd.、OVH SAS、Vlasenko Oleksandr）。IPアドレスIoCと同じISPを使っているアドレスはありませんでした。



- Threat Intelligence Lookupの結果から、2つのIPアドレスが106件の脅威と関連していることが明らかになりました。具体的には、199[.]59[.]243[.]22は19件、23[.]106[.]122[.]213は87件の脅威に関わりを持っていました。

関連している可能性のあるアーティファクトをさらに洗い出すため、12個のIPアドレス（ASECが特定したIPアドレスIoC 7個と、当社のDNS検索で見つかったIPアドレス5個）をReverse IP Lookupにかけました。そして、5個のIPアドレスが5個のドメイン名をホストしているか、またはそれらの専用アドレスになっていることがわかりました。なお、その5個のドメイン名は、既存のドメインIoCまたは前述のメールアドレスで紐づけられたドメイン名のいずれにも該当しませんでした。

Screenshot Lookupで調べたところ、その5個のうち1個（thesisterize[.]gb[.]net）は有効なコンテンツをホストし続けていました。

最後に、Domains & Subdomains Discovery検索を使い、ASECのドメインIoCに見られた以下のいずれかのテキスト文字列を含むドメイン名を探しました。

- **brhosting**
- **prohomepage**
- **splitbusiness**
- **techgolfs**
- **topspace**

その結果から重複、既存のIoC、共通のメールアドレスまたはIPアドレスを使っているドメイン名をフィルタリングした後、356個がASECのIoCと同じ文字列を含むドメイン名として残りました。なお、この作業では**Contains**パラメータを使用しており、当社のレポジトリにある全てのドメイン名（過去10年分）を対象にしています。また、Screenshot Lookupの結果、34個のドメイン名が有効なウェブサイトを指し続けていることがわかりました。

—

今回、Kimsukyの最新のIoC、具体的にはRftRATとAmadeyマルウェアを使用した攻撃のIoCを詳細に調査した結果、合計702個の潜在的な関連アーティファクト（共通のメールアドレスを使用していたドメイン名336個、名前解決したIPアドレス5個、共通のIPアドレスを使用していたドメイン名5個、IoCと同じ文字列を含んだドメイン名356個）を新たに見つけることができました。

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：アーティファクトとIoCの例

共通のメールアドレスを使用していたドメイン名の例

- 6666[.]ca
- ablockchaincompany[.]com
- ahoteis[.]com[.]br
- aliancademoedaantiga[.]com[.]br
- anodynebusiness[.]com
- appentrepreneuradvice[.]com
- auctioning[.]ca
- barquebusiness[.]com
- bitcoinmover[.]com
- bitcoinpipe[.]com
- blendentrepreneur[.]com
- blockchainpolicies[.]com
- bloggingentrepreneuradvice[.]com
- boardentrepreneuradvice[.]com
- boldbusinessadvice[.]com
- btclightningnetwork[.]com
- btcorders[.]com
- btctesting[.]com
- btctransactions[.]com
- businesstrendadvice[.]com
- cabincruiserbusiness[.]com
- cashentrepreneuradvice[.]com
- casinosvr[.]net
- catwalkvr[.]com
- cementbusinessadvice[.]com
- cleaningentrepreneuradvice[.]com
- clik[.]ca
- clothesentrepreneuradvice[.]com

- coinmarket[.]ca
- conceptbusinessadvice[.]com
- conceptentrepreneuradvice[.]com
- contentbusinessadvice[.]com
- convincebusiness[.]com
- coursebusinessadvice[.]com
- crabberbusiness[.]com
- cryptoadept[.]com
- cryptoinvestments[.]ca
- cryptoportfolio[.]ca
- customerbusinessadvice[.]com
- dairyproducts[.]net
- decentralizedcryptos[.]com
- dicey[.]net
- dispatchbusiness[.]com
- dividebusiness[.]com
- dnbuyer[.]xyz
- dndeals[.]xyz
- dndepot[.]xyz
- dndrone[.]xyz
- dnfind[.]xyz
- dnfinder[.]xyz

IPアドレスの例

- 139[.]99[.]155[.]54
- 199[.]59[.]243[.]225
- 23[.]106[.]122[.]213

共通のIPアドレスを使用していたドメイン名の例

- hecug[.]com
- kv635616[.]info
- ot319954[.]info

IoCと同じ文字列を含むドメイン名の例

- 1stopspace[.]com
- 1topspace[.]com
- 52topspace[.]com
- 5topspace[.]top
- abrhosting[.]com
- abrhosting[.]ir
- abrhosting[.]xyz
- aerotechgolfshafts[.]com
- aerotechgolfshafts[.]net
- aerotechgolfshaftsjapan[.]com
- areotechgolfshafts[.]com
- atopspace[.]com
- aviatopspace[.]com
- bbrhosting[.]nl
- bitopspace[.]com
- bj-topspace[.]com
- bjtopspace[.]com
- bjtopspace[.]tw
- brhosting[.]cloud
- brhosting[.]co[.]uk
- brhosting[.]com
- brhosting[.]com[.]br
- brhosting[.]com[.]mx
- brhosting[.]ga
- brhosting[.]info
- brhosting[.]ml
- brhosting[.]nl
- brhosting[.]online
- brhosting[.]org
- brhosting[.]srv[.]br
- brhosting[.]store
- brhosting[.]tk
- brhosting[.]xyz
- brhostinger[.]com

- brhostings-ofc[.]tk
- brhostings[.]com
- brhostings[.]tk
- brhostingserver[.]com[.]br
- brhostingweb[.]com
- cbrhosting[.]co[.]uk
- cbrhosting[.]com
- cbrhosting[.]uk
- clickstopspace[.]online
- clickstopspace[.]site
- clubtechgolfshop[.]com
- coppertopspaces[.]com
- countertopspace[.]com
- csbrhosting[.]com
- csbrhosting[.]xyz
- ctopspace[.]com