Ivantiゼロデイ攻撃のIoCをDNSで追跡

目次

要旨

Ivantiは米国の連邦政府機関を含む様々な組織にエンドポイント管理およびリモートアクセスのソリューションを提供しているソフトウェア会社です。最近、Ivanti Connect Secure VPNおよびIvanti Policy Secureに影響を及ぼす重大なゼロデイ脆弱性が報告されました。この脆弱性に目をつけた脅威アクターは、高レベルのアクセス権限を使って勝手にコードを実行する可能性があります。

Mandiantが先般、中国を拠点とする脅威グループ「UNC5221」によるこうしたゼロデイ攻撃に関する詳細な報告を発表し、その中で10個のドメイン名、2個のサブドメイン、8個のIPアドレスからなるセキュリティ侵害インジケーター（IoC）を明らかにしました。

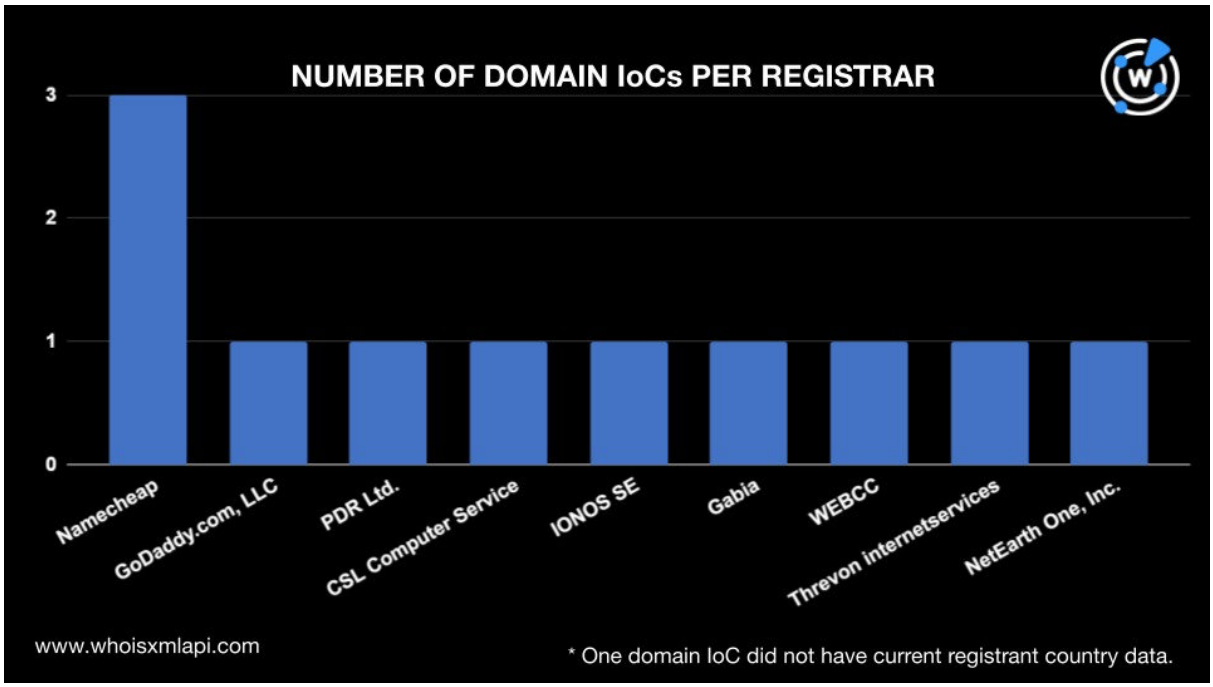
そこで、WhoisXML APIがこのほど、この攻撃に関連する未公開のアーティファクトを見つけるべく、MandiantのIoCリストをもとにDNSを調査しました。その結果、以下を新たに特定しました：

- ドメインIoCに使われていた公開のメールアドレス3個
- そのメールアドレスを使用していた別のドメイン名33個
- ドメインIoCをホストしていたIPアドレス13個
- ドメインIoCをホストしていたIPアドレス、またはIPアドレスIoCを使っていたドメイン名211個
- ドメインIoCと同じ文字列を含むドメイン名153個

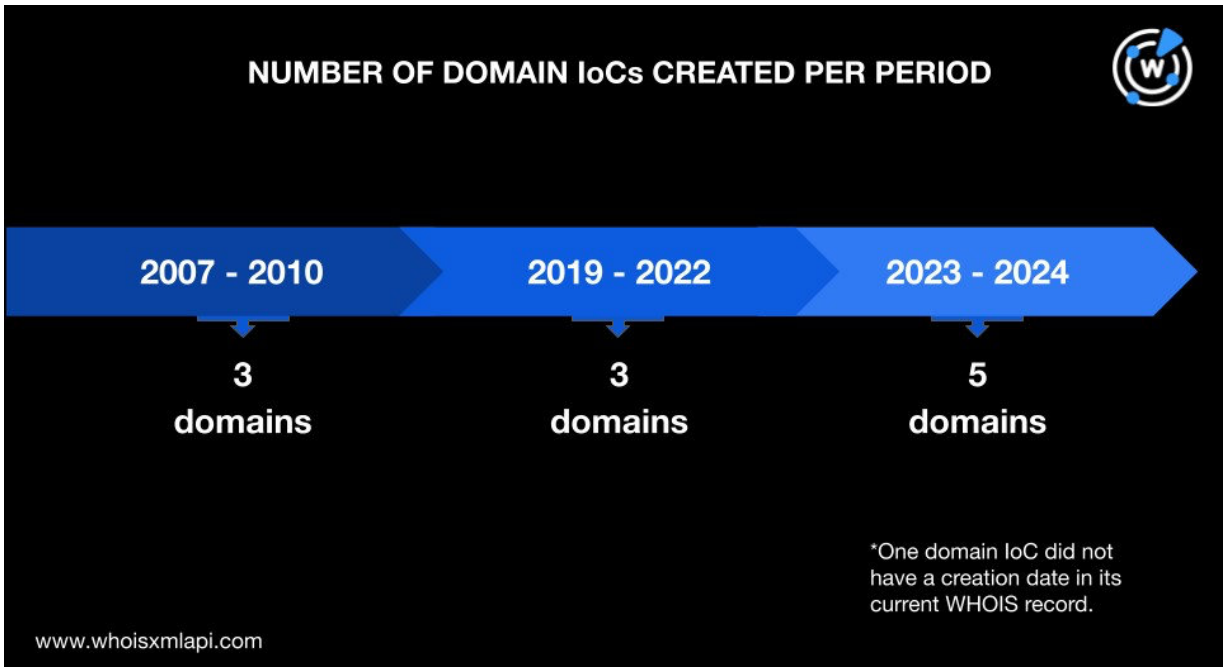
IvantiのIoCでゼロデイ攻撃インフラを分析

まず、12個のドメイン名（Mandiantが特定した10個のドメインIoCに加え、サブドメインIoCから抽出した2個のドメイン名）についてBulk WHOIS Lookupを実行しました。その結果、以下のことがわかりました：

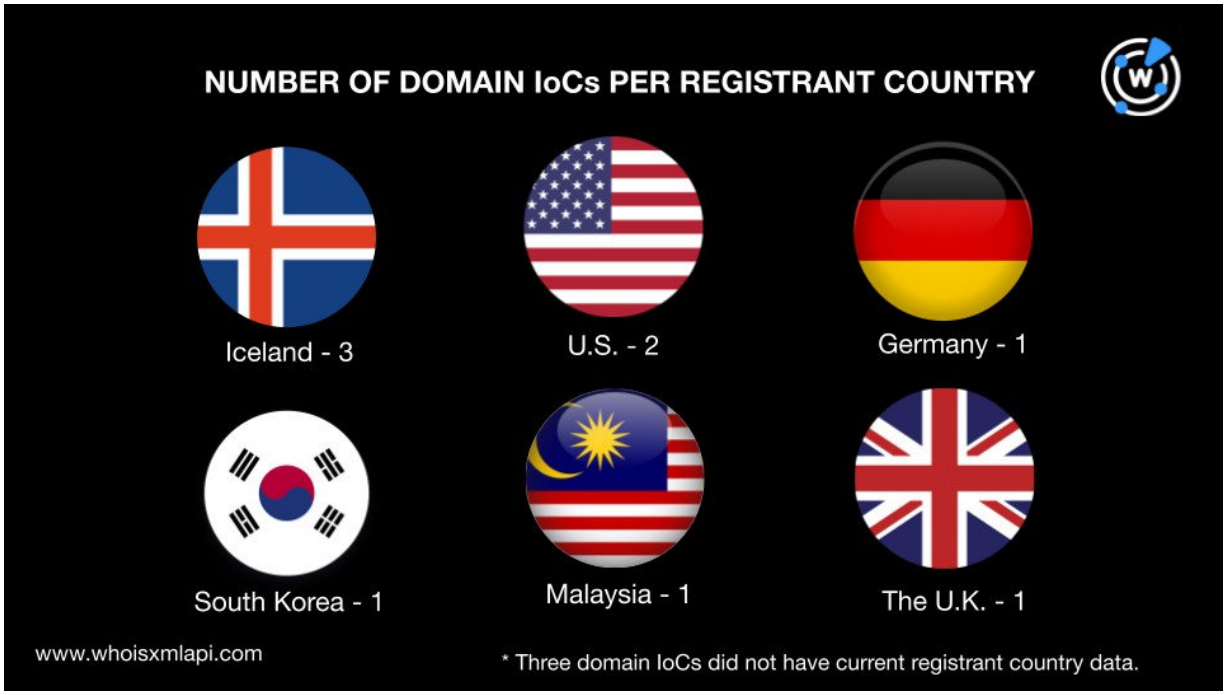
- 9社の管理レジストラが特定されました。Namecheapが3個のドメイン名を、GoDaddy.com LLC、PDR Ltd.、CSL Computer Service Langenbach GmbH、IONOS SE、Gabia、WEBCC、Threvon Internet Services、NetEarth One, Inc.がそれぞれ1個を管理していました。残り1個のドメイン名については、レジストラのデータがありませんでした。



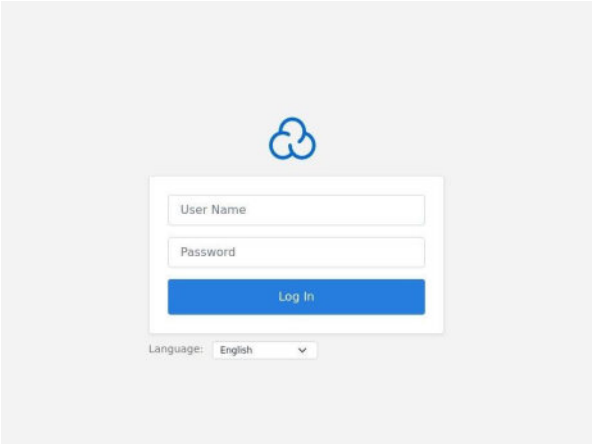
- 2024年に新規登録されたドメイン名が3個ありました。また、2個は2023年に登録されたものでした。2022年、2021年、2019年にそれぞれ1個が登録されていました。2010年に登録されたドメイン名が2個あり、1個は2007年に登録されていました（これが最も古いドメイン名）。残りのドメイン名については、現在のWHOISレコードに登録年月日の情報がありませんでした。



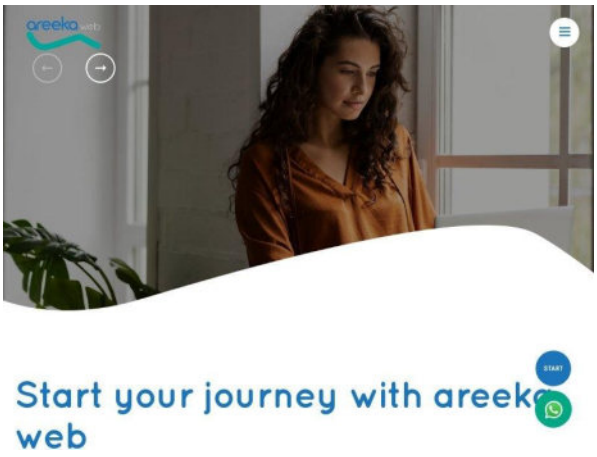
- 3個はアイスランド、2個は米国で登録されたドメイン名でした。ドイツ、韓国、マレーシア、英国でそれぞれ1個登録されていました。3個のドメイン名については、現在のWHOISレコードに登録者の国の情報がありませんでした。



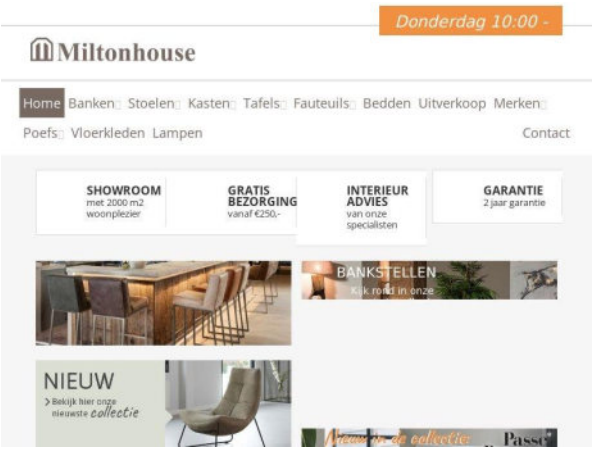
次に、ドメインIoCをScreenshot Lookupで分析し、一部のドメインが以下のサイトを含む有効なコンテンツをホストし続けていることを確認しました。



ドメインIoC「cpanel[.]netbar[.]org」のスクリーンショット



ドメインIoC「areekaweb[.]com」のスクリーンショット

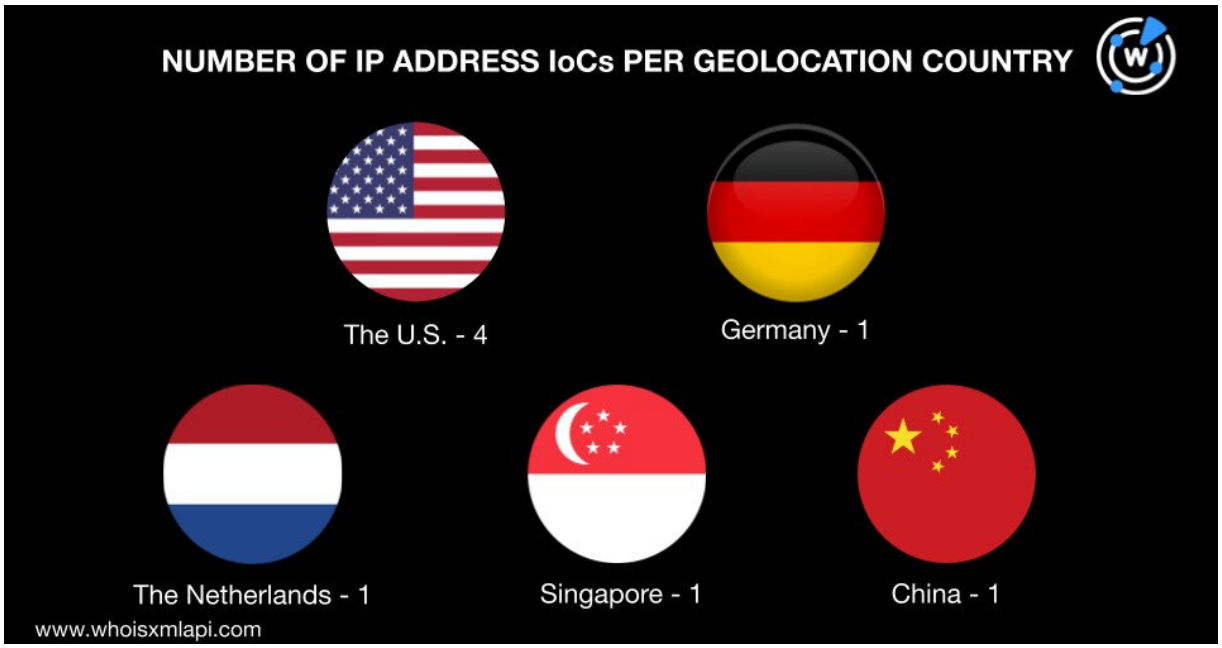


ドメインIoC「miltonhous[.]enl」のスクリーンショット

ドメインIoC「ehangmun[.]com」のスクリーンショット

さらに、8個のIPアドレスIoCに対してBulk IP Geolocation Lookupを実行した結果、以下が判明しました：

- 8個は6カ国に分散していました。4個が米国を指したほか、ドイツ、オランダ、シンガポールおよび中国に1個ずつ位置していることがわかりました。



- Host Europe GmbH、DigitalOcean LLC、Hangzhou Alibaba Advertising Co. Ltd.、Limenet、Corporación Dana S.A.、Comcast Cable Communications LLC、BL Networks、Cablevision Systems Corp.がそれぞれ1個のアドレスを管理していました。

Ivantiゼロデイ攻撃のIoCをもとにDNSをトラッキング

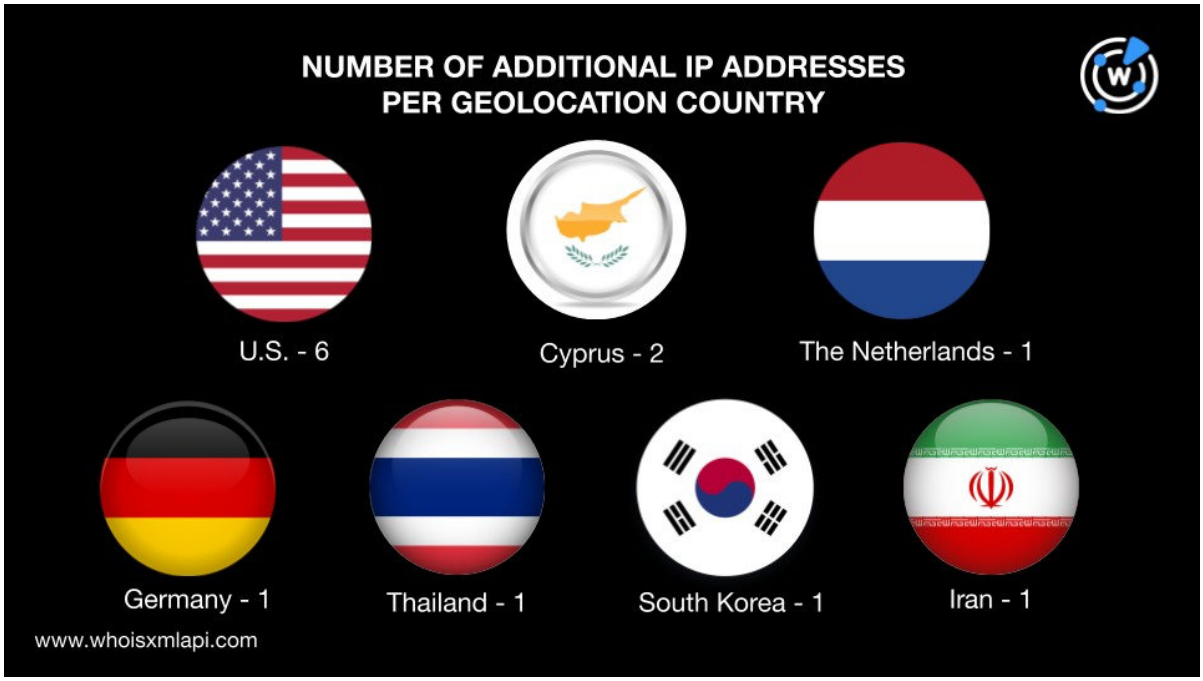
次のステップとして、攻撃に使われた悪意あるリソースの痕跡をDNSで探索しました。

ドメインIoCをWHOIS History APIで調べた結果、過去のWHOISデータから合計14個のメールアドレスを抽出することができました。そして、そのうち3個のメールアドレスは公開されていました。Reverse WHOIS APIで調べたところ、その3つの公開メールアドレスのいずれかが、ドメイン名33個（重複と既存IoCを除く）の現在のWHOISレコードに含まれていることがわかりました。

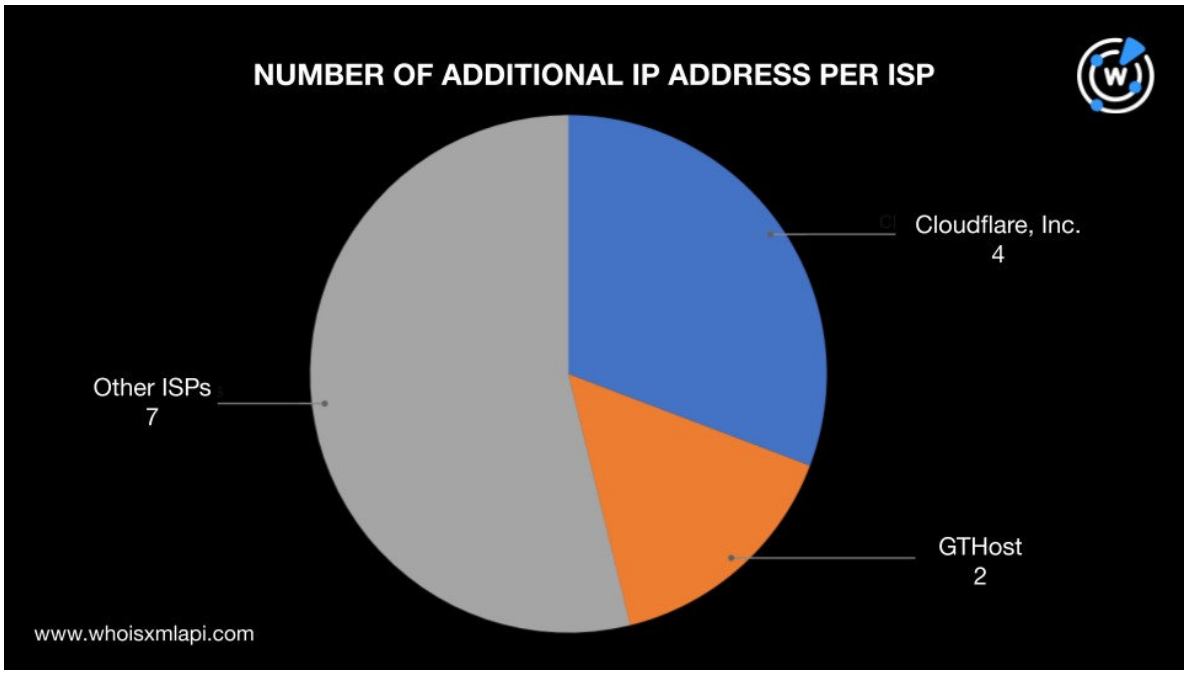
次に、12個のドメインIoC（サブドメインIoCから抽出した2個のドメイン名を含む）をDNS Lookupで検索しました。その結果、それらは合計13個のユニークなIPアドレスに名前解決しました（重複と既存IoCを除く）。

さらにその13個のIPアドレスの地理的位置をIP Geolocation Lookupで分析し、以下のことを確認しました：

- ジオロケーションとして7カ国が特定されました。6個のIPアドレスは米国、2個はキプロスに位置し、オランダ、ドイツ、タイ、韓国、イランにそれぞれ1個ずつありました。



- 4個のIPアドレスはCloudflare、2個はGTHostというISPが管理していました。この他、Signet BV、IONOS SE、Siamdata Communication Co. Ltd.、Korea Telecom、QuadraNet Enterprises LLC、SoftLayer、Pars Parva System LLCがそれぞれ1個の管理ISPになっていました。



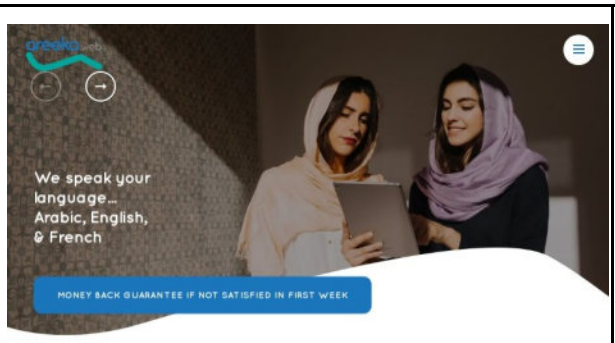
- Threat Intelligence APIを実行した結果、13個のIPアドレス全てが何らかの脅威に関連していたことが判明しました。例として一部のIPアドレスの情報を以下に示します：

IPアドレス	関連している脅威の種類
104[.]21[.]61[.]132	フィッシング マルウェア Generic
217[.]160[.]0[.]177	フィッシング マルウェア
5[.]8[.]18[.]6	マルウェア Generic
172[.]67[.]209[.]167	フィッシング マルウェア Generic
104[.]21[.]69[.]158	フィッシング マルウェア Generic

さらに多くの関連ドメイン名を特定するため、ドメインIoC が名前解決した13個のIPアドレスと8個のIPアドレスIoCをReverse IP Lookupで逆引きしました。その結果、9個は専用アドレスらしいこと、それらが211個のドメイン名をホストしていたことを突き止めました（重複、既存IoCおよびドメイン

IoCと同じメールアドレスを使っていたドメイン名を除く）。

211個のドメイン名のスクリーンショットを分析したところ、ドメインIoCのareekaweb[.]comと似たコンテンツをホストしているドメイン名を1個（tedtankal[.]xyz）特定しました。この2つのドメイン名のWHOISレコードは非公開でしたが、両方ともGoDaddy経由で登録されたことはわかりました。



ドメイン名「tedtankal[.]xyz」のスクリーンショット

ドメインIoC「areekaweb[.]com」のスクリーンショット

最後に、Domains & Subdomains Discoveryで「**Starts with**」パラメータを使い、ドメインIoCと同じ文字列を含むドメイン名を探しました。その結果、ドメインIoCに見られた以下のいずれかの文字列で始まるドメイン名が145個特定されました：

- **symantke**
- **miltonhouse.**
- **entraide-internationale**
- **clickcom.**
- **clicko.**
- **duorhytm**
- **line-api**
- **areekaweb**
- **ehangmun**
- **secure-cama**

また、Threat Intelligence APIで「**clicko**」という文字列を使ったワイルドカード検索（**clicko***）を行ったところ、フィッシングやマルウェアなどの脅威に関連する8個の悪意あるドメイン名が見つかりました。そのうちの1個は、有効なコンテンツをホストし続けていました。

ドメインIoCと同じ文字列を含む悪意あるドメイン名「clickcomputerservices[.]com」のスクリーンショット

—

Ivantiのゼロデイ攻撃に関与した10個のドメインIoC、2個のサブドメインIoC、8個のIPアドレスIoCをもとに当社で行った調査の結果、ドメインIoCに使われていた公開のメールアドレス3個、そのメールアドレスを使っていた別のドメイン名33個、ドメインIoCをホストしていたIPアドレス13個、ドメインIoCをホストしていたIPアドレスまたはIPアドレスIoCを使っていたドメイン名211個、ドメインIoCと同じ文字列を含むドメイン名153個が検出されました。また、ドメインIoCをホストしていたIPアドレス13個の全て、およびドメインIoCと同じ文字列を含むドメイン名のうち8個については、すでに様々な脅威で使用されていたことを確認しました。

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

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

- ohs[.]com[.]cn
- hw-tech[.]net
- hitcn[.]net
- istarwild[.]com
- xn--fiqa70wb2hn4c03sb4smo9d[.]xn--55qx5d
- xn--fhq199gu2f40o[.]xn--55qx5d
- xn--fiqa70wb2h5jo5h0y4cuib[.]xn--55qx5d
- xn----kq6ab834ak7i4rdzq2c[.]xn--55qx5d
- vf-transformerasia[.]com
- glodon[.]us
- chenxiango2o[.]com
- xn--p5tq45e76a[.]com
- viewrankshare[.]com
- videohover[.]com
- videohilarity[.]com
- affluencenetwork[.]marketing
- videostore[.]click
- afflinkit[.]com
- creativebranding[.]club
- viralvideoclass[.]com

ドメインIoCを使用していたIPアドレスの例

ドメインIoCを使用していた13個のIPアドレスは、その全てがすでに悪意のアドレスとしてタグ付けされていました。

- 104[.]21[.]61[.]132
- 188[.]240[.]53[.]22
- 217[.]160[.]0[.]177
- 5[.]8[.]18[.]6
- 5[.]8[.]18[.]4
- 172[.]67[.]209[.]167

共通のIPアドレスを使用していたドメイン名の例

- 2sky[.]co[.]kr
- 33in[.]or[.]kr
- affmewin888[.]com
- anyink[.]ink
- anyink[.]kr
- anyink[.]net
- app[.]ezyinn-panel[.]com
- arche1[.]co[.]kr
- arh[.]co[.]kr
- arika[.]live
- atlantic21c[.]com
- babycap[.]co[.]kr
- bangkokdesignandprint[.]com
- barweb[.]ir
- beerlaokorea[.]co[.]kr
- belfarm[.]net
- biz-apps[.]com
- btenc[.]com
- bydforkliftth[.]com
- cenit[.]kr
- cenwha[.]com
- changdaegagu[.]com

- charish[.]co[.]th
- chongsolcoop[.]com
- cimaro[.]co[.]kr
- cnkmachine[.]com
- coolclinic[.]co[.]kr
- depia[.]co[.]kr
- dhammanava[.]net
- dhmtech[.]com
- digitaxs[.]com
- diode[.]kr
- dkpile[.]co[.]kr
- domyeong[.]co[.]kr
- dooripension[.]co[.]kr
- dumbwaiter[.]co[.]kr
- e-goldenbridge[.]co[.]kr
- e-goldenbridge[.]com
- egundrill[.]co[.]kr
- epostbanner[.]co[.]kr
- eraguardian[.]com
- eunsungpoly[.]co[.]kr
- eventhappy[.]co[.]kr
- eyang-wa[.]com
- ezyinn-panel[.]com
- faceoff1[.]com
- faceoffbaby[.]com
- faceprove[.]com
- fariwealth[.]com
- favolosovillasapanca[.]com

ドメインIoCと同じ文字列を含むドメイン名の例

- symantkec[.]ga
- symantkec[.]tk
- miltonhouse[.]eu
- miltonhouse[.]pl
- miltonhouse[.]irish
- miltonhouse[.]co[.]uk
- miltonhouse[.]de
- miltonhouse[.]com[.]ua
- miltonhouse[.]gallery
- miltonhouse[.]cc
- miltonhouse[.]net
- miltonhouse[.]be
- miltonhouse[.]biz
- miltonhouse[.]com[.]pl
- miltonhouse[.]ca
- miltonhouse[.]co[.]za
- miltonhouse[.]uk
- miltonhouse[.]org
- miltonhouse[.]com
- clickcom[.]nl
- clickcom[.]info
- clickcom[.]app
- clickcom[.]co[.]uk
- clickcom[.]us
- clickcom[.]kr
- clickcom[.]pro
- clickcom[.]work
- clickcom[.]md
- clickcom[.]online
- clickcom[.]ru
- clickcom[.]store
- clickcom[.]org
- clickcom[.]net[.]br
- clickcom[.]tk
- clickcom[.]com
- clickcom[.]com[.]br
- clickcom[.]shop
- clickcom[.]at
- clickcom[.]biz
- clickcom[.]co[.]th
- clickcom[.]cl
- clickcom[.]it
- clickcom[.]es
- clickcom[.]vn
- clickcom[.]eu
- clickcom[.]xyz

- clickcom[.]co
- clickcom[.]net
- clickcom[.]io
- clickcom[.]guru

ドメインIoCと同じ文字列を含む悪意あるドメイン名の例

- clickcomputerstz[.]com
- clickcomfort[.]co
- clickco[.]net
- clickcounter1[.]com