DNS調査：閉鎖されたxDedicは本当に終息したのか？

目次

1. 要旨
2. 付録：アーティファクトとIoCの例

要旨

サイバー犯罪者にウェブサーバーを提供するCaaS（cybercrime-as-a-service）マーケットプレイスの「xDedic」は、欧米の法執行機関によって2019年に閉鎖されました。しかし、WhoisXML API の脅威リサーチャー・Dancho Danchevは、xDedic のバックエンドインフラの一部が今も追跡可能なまま残っている可能性があると指摘しています。

WhoisXML APIの研究チームはこのほど、Danchevが特定した3個のドメイン名と16個のIPアドレスからなるxDedicの侵害インジケーター（IoC）19個をもとに、アクティブな状態にあるxDedic関連の他のアーティファクトを洗い出すため、DNSの徹底調査を行いました。この調査の結果、以下が新たに特定されました：

- IoCと同じメールアドレスを使用していたドメイン名15個、うち1個は悪意のドメイン名
- IoCとされるIPアドレスがホストしていたドメイン名126個、うち1個は悪意のドメイン名
- **xdedic**という文字列で始まるドメイン名9個

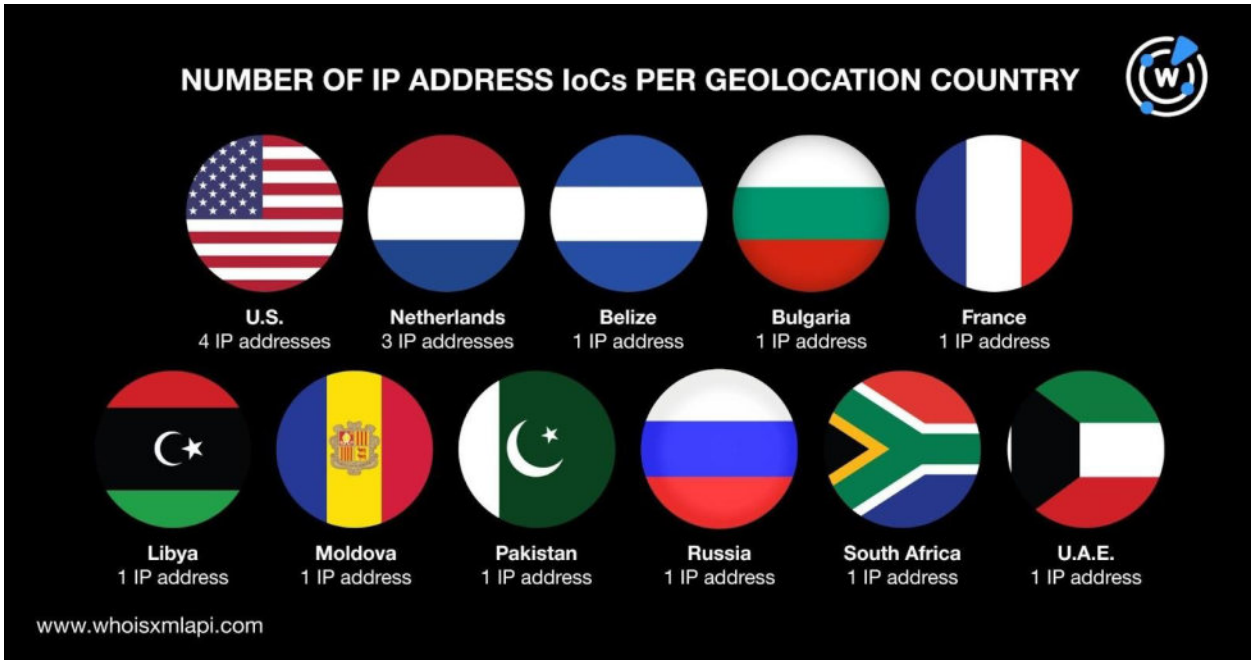
xDedicのIoCの実像

まず、IoCと特定された3個のドメイン名（以下「ドメインIoC」）をBulk WHOIS Lookupの一括検索にかけたところ、現在のWHOISデータが存在するドメインIoCは1個（xdedic[.]biz）しかありませんでした。xdedic[.]bizの現在のWHOISデータは以下の通りです：

- **レジストラ：**PSI-USA, Inc.
- **登録年月日：**2014年9月12日
- **登録者の国：**カナダ

他方、IoCと特定された16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：

- 16個は11のジオロケーションに分散していました。最も多かったのは米国（4個）で、これにオランダ（3個）が続きました。また、ベリーズ、ブルガリア、フランス、リビア、モルドバ、パキスタン、ロシア、南アフリカおよびUAEにそれぞれ1個ずつ位置していました。地理的位置のこうした多様性は、脅威のグローバルな性質に起因しているのかもしれません。



- また、13社が16個のIPアドレスIoCの管理ISPとして特定されました。最も管理アドレス数が多かったのは、Cloudflare, Inc.（4個）でした。この他、365 Online Technology Joint Stock Company、Alexhost SRL、Aljeel Aljadeed Technology、DIGIT1-IPOE、IQWeb FZ LLC、Liquid Telecommunications Operations Limited、Lirex.net、Multinet 125-101/24、OVH SAS、Pars Shabakeh Azarakhsh LLC、Serverius Holding B.V.およびTOV Highload Systemsが各1個のIPアドレスIoCを管理していました。

DNSにxDedicの痕跡は残っているか

次に、サイトが閉鎖された後もxDedicの痕跡が残っているかどうかを調べるため、DanchevのIoCリストの拡張を試みました。

まず、3個のドメインIoCをWHOIS History APIで調べたところ、過去のWHOISレコードから5個のメールアドレスを抽出することができました。そこで、抽出されたメールアドレスのうち未編集のまま公開されていたものに対象を絞り、その公開メールアドレスを使って登録された他のドメイン名がないか探しました。

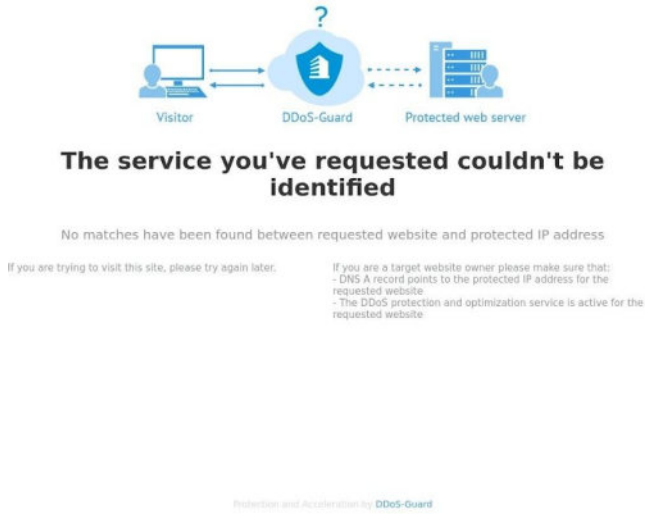
Reverse WHOIS Searchを実行した結果、過去のWHOISレコードにその公開メールアドレスが含まれているドメイン名が15個見つかりました。そのうち1個（omerta[.]cc）は、Threat Intelligence APIの結果によれば、1件のマルウェア攻撃に関与していた悪意あるドメイン名でした。

公開メールアドレスを使っていた15個のドメイン名をScreenshot Lookupにかけたところ、3個は現在もアクセス可能な状態にありました。1個はパークドメインで、1つはエラーページに繋がり、残りの1個は有効なコンテンツを持つページに繋がりました。なお、omerta[.]ccは、本稿執筆時点ではアクセスできませんでした。

アクセス可能だった3個のドメイン名に対してDNS Lookupを実行しましたが、いずれもIPアドレスに名前解決しませんでした。しかし、Danchevが特定した16個のIPアドレスIoCを調べることで、それらがホストしていたドメイン名を特定することができました。16個のIPアドレスIoCをReverse IP Lookupにかけたところ、3個（186[.]2[.]163[.]126、87[.]236[.]215[.]18、91[.]220[.]101[.]43）は専用アドレスらしいことがわかりました。そして、その3個のIPアドレスIoCが、合計126個（重複を除く）のドメイン名をホストしていました。

その126個のドメイン名についてThreat Intelligence APIを実行した結果、1個（vsoloviev[.]ru）はgeneric threatと関連していたことが確認されました。

また、Screenshot Lookupの結果から、vsoloviev[.]ruはアクセスできる状態にありました。ただし、本稿執筆時点では、繋がったのはエラーページでした。



soloviev[.]ruのスクリーンショット

さらに、3個のIPアドレスIoCを共用していた126個のドメイン名についてScreenshot APIで検索したところ、117個が現在もアクセス可能であることがわかりました。

最後に、Domains & Subdomains Discoveryを使い、**xdedic**という文字列で始まる他のドメイン名を探しました。その結果、該当するドメイン名が9個検出されました。
その9個のドメイン名をBulk WHOIS Lookupで調べたところ、以下が判明しました：

- ACTIVE-RU、Dynadot, Inc.、Eranet International Limited、GoDaddy.com LLCおよびTurnCommerce, Inc.が各1個の管理レジストラでした。残りの4個のドメイン名については、現在のレジストラに関するデータがありませんでした。
- 大半のドメイン名は、xDedicの閉鎖後に新規登録されたものでした。2個の登録年は2022年で、各1個が2021年と2023年に登録されていました。2019年以前に登録されたドメイン名は、xdedic[.]io（登録年月日：2016年6月16日）のみです。なお、4個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が記載されていませんでした。
- 3個のドメイン名が米国で、1個がセントクリストファー・ネイビスで登録されていました。5個は現在のWHOISレコードに登録者の国が記載されていませんでした。

xdedicという文字列で始まる9個のドメイン名の中には、ドメインIoCと何らかの共通点を持つものはありませんでした。しかし、xdedic[.]ioというドメイン名については、その登録日がxDedicの全盛期に当たることから、地下市場のインフラの一部であるか、xDedicのオペレーターによって登録された可能性があります。また、Wayback Machineにアーカイブされているxdedic[.]ioのスクリーンショットを見たところ、このドメイン名は3個のドメインIoCと同様に当局によって閉鎖されていました。

2019年1月28日時点でxdedic[.]ac、xdedic[.]biz、xdedic[.]tkがホストしていたページのスクリーンショット

2019年2月1日時点でxdedic[.]ioがホストしていたページのスクリーンショット

—

今回当社で行ったxDedicのIoCリスト拡張により、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15個、IPアドレスIoCを使っていたドメイン名126個、**xdedic**という文字列で始まるドメイン名9個からなる合計150個の関連アーティファクトが発見されました。また、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1個（omerta[.]cc）とIPアドレスIoCを使っていたドメイン名1個（vsoloviev[.]ru）は悪意のドメイン名であることが判明しました。さらに、**xdedic**という文字列で始まり、かつ現在もDNSに登録されているxdedic[.]ioは、CaaS市場のインフラの一部である可能性があります。

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：アーティファクトとIoCの例

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

- amtrustpills[.]com
- buycytotecnow[.]com
- buyingamoxicillin[.]com
- buyingclomid[.]com
- ed-generics-online[.]com
- goodfinance-blog[.]com
- gossipgel[.]com
- hotnpapers[.]com

IPアドレスIoCを使用していたドメイン名の例

- abargrit[.]com
- ablb[.]ir
- ablbaspar[.]ir
- absanatco[.]com
- absanattehran[.]com
- alirantrading[.]net
- amnafza-co[.]ir
- apadanaart[.]com
- atbinfam[.]com
- atlasfilm[.]net
- atousaco[.]com
- balansanat[.]com
- bently[.]co
- betawin[.]ir
- binaloodpaint[.]com
- binaloodpaint[.]ir
- boghratlab[.]com
- cafechimney[.]ir
- candonama[.]com
- cheftco[.]com
- dkc-uae[.]com
- drkahnamuee[.]com
- drkahnamuee[.]ir
- ecoffice[.]co
- ecoffice[.]ir
- ecoffice[.]org

- elmisaz-autopart[.]com
- englandtour[.]ir
- fixopen[.]com
- goalelectric[.]co
- goalelectric[.]ir
- goalelectric[.]net
- gritpash[.]com
- haniantenna[.]com
- hseoic[.]com
- innopraktika[.]ru
- iran-oilshow[.]ir
- iran-watex[.]com
- iranaac[.]ir
- iranianhairclinic[.]com
- iriclub[.]com
- isfahan-elecomp[.]com
- kdd-group[.]com
- keshtsanatj[.]com
- kimia-pharma[.]co
- kish-tours[.]com
- kmcco[.]ir
- mandtgroup[.]co
- mashhademoghadas[.]com
- mashhademoghadas[.]ir

xdedicという文字列で始まるドメイン名の例

- xdedic[.]cc
- xdedic[.]club
- xdedic[.]com
- xdedic[.]in
- xdedic[.]io