DNS分析でIcedIDの実態をあぶり出す

目次

要旨

進化は人間をはじめとする生物の専売特許ではなく、マルウェアにもできることのようです。IcedIDはその好例です。

2017年にバンキング型トロイの木馬として初めて検出されたIcedIDは、更新を重ねてその危険性を高めています。最近の数カ月間には、IcedIDの亜種がランサムウェアのペイロードを配信することが確認されています。これはIcedIDの従来の機能（金融データの窃取）と異なるものであり、進化が認められます。

また、被害者のホストが8080番ではなく443番ポートを使用してIceIDのC&Cサーバーに接続するようになり、活動が検知されにくくなったことも、注目すべき変化です。こうした動きを踏まえ、Cymruの研究者[1]は、IcedID BackConnectプロトコルを継続的に追跡しています。 Cymruの最近のレポートでは、マルウェアのC&Cサーバーを指す34個のIPアドレス（以下）を挙げています。

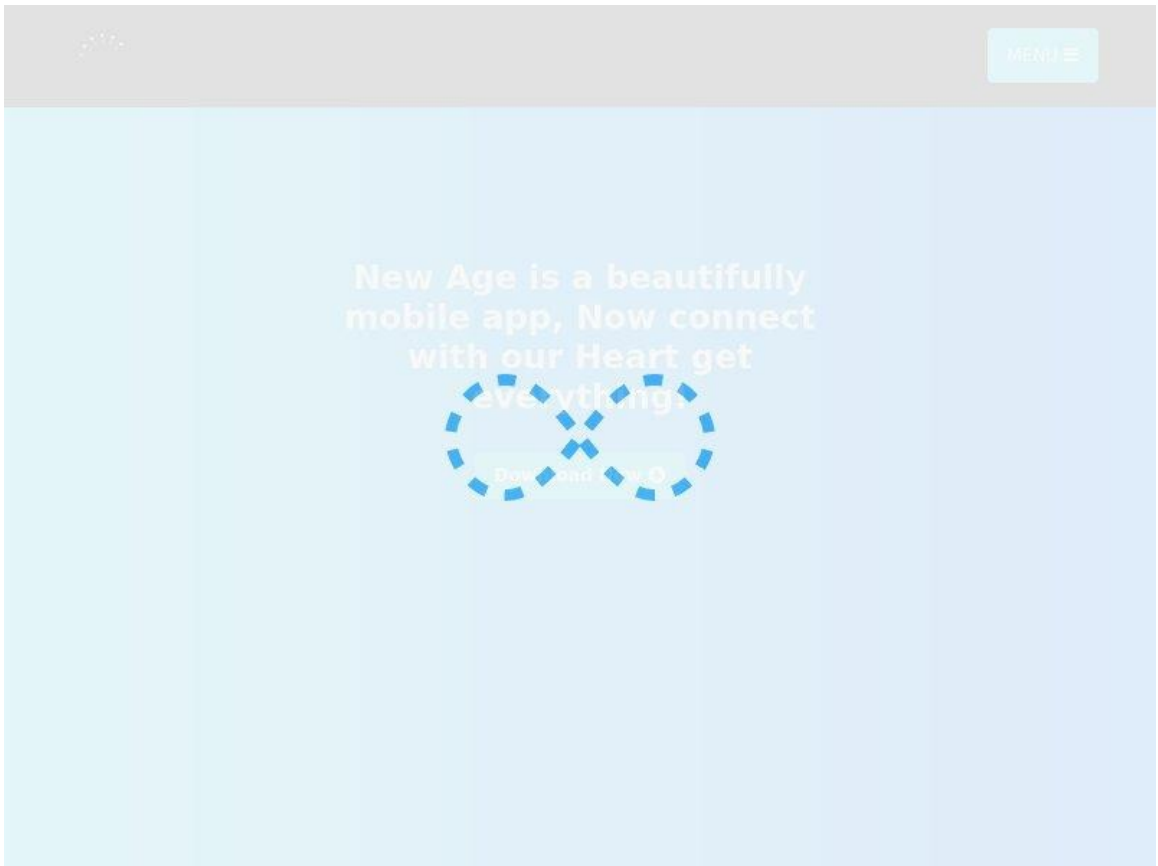
- 5[.]196[.]196[.]252
- 135[.]148[.]217[.]85
- 80[.]66[.]88[.]71
- 45[.]61[.]137[.]220
- 193[.]239[.]85[.]16
- 185[.]99[.]132[.]16
- 167[.]99[.]235[.]95
- 162[.]33[.]179[.]145
- 46[.]21[.]153[.]153
- 193[.]149[.]176[.]100
- 45[.]61[.]139[.]144
- 45[.]61[.]137[.]159
- 45[.]61[.]139[.]235
- 193[.]149[.]176[.]198
- 192[.]153[.]57[.]134
- 193[.]149[.]187[.]7
- 162[.]33[.]179[.]218
- 139[.]59[.]33[.]128
- 138[.]197[.]146[.]18
- 167[.]99[.]248[.]131
- 134[.]122[.]62[.]178
- 104[.]248[.]223[.]35
- 64[.]227[.]48[.]93
- 209[.]38[.]220[.]183
- 161[.]35[.]166[.]97
- 138[.]68[.]244[.]54
- 68[.]183[.]198[.]18
- 207[.]154[.]203[.]203
- 64[.]227[.]146[.]71
- 116[.]203[.]30[.]206
- 139[.]59[.]186[.]140
- 139[.]59[.]72[.]105
- 104[.]248[.]21[.]165
- 159[.]89[.]116[.]11

他方、WhoisXML APIは、3つのAlienVault OTX Pulse[2,3,4]でセキュリティ侵害インジケーター（IoC）をさらに見つけました。これは、上記のリストに9個のIPアドレスと15個のドメイン名を追加するものでした。当社では、これらのIcedIDのIoCをもとにこのたび調査を行い、以下を発見しました。

- IoCとして特定されたドメイン名を登録する際に使われた未編集のメールアドレス5個
- そのメールアドレスを使用して現在登録されている 44個のドメイン名
- IoCとして特定されたIPアドレスに名前解決する22個のドメイン名
- IoCとして特定されたドメイン名と同じIPアドレスを共用している33個のドメイン名
- マルウェアの一括チェックで、これらのアーティファクトの14%に悪意があることを確認

IcedIDのIoC：これまでに分かっていること

まず、IoCとして特定されている43個のIPアドレスをBulk IP Geolocation Lookupにかけたところ、45[.]61[.]137[.]159を除く全てのアドレスがドメイン名に名前解決しました。また、主なISPは、Digital Ocean（40%）とBL Networks（21%）でした。いくつかのIPアドレスは有効なウェブページを指しました。以下はその一部です。



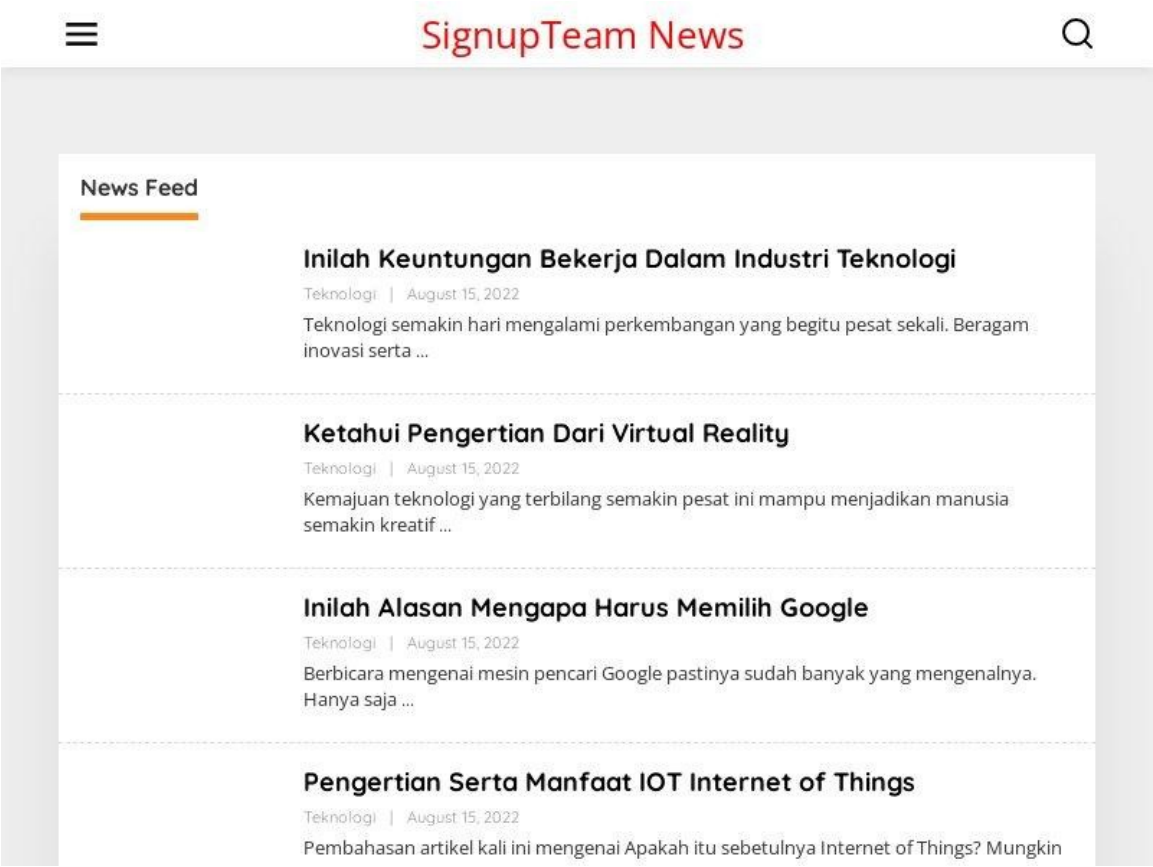
116[.]203[.]30[.]206のスクリーンショット。on-mail[.]ruに名前解決。

139[.]59[.]33[.]128のスクリーンショット

その一方で、AlienVaultがIoCとして特定したドメイン名については、異なる状況が見られました。15個のドメイン名のうち、調査時点でWHOISレコードが存在したのは1個（2fgithub[.]com）だけでした。このドメイン名は、WHOISプライバシー保護プロバイダーとしてPerfect Privacy LLCを使用しています。

さらに調査を進めたところ、いくつかのドメイン名が有効なウェブページをホストしていたり、そうしたページにリダイレクトしていることがわかりました。

click[.]orgのスクリーンショット



signup[.]teamのスクリーンショット

公開IoCから関連アーティファクトを検出

次に、まだ特定されていない関連プロパティを見つけるべく、IcedIDのインフラを詳細に調べました。脅威アクターは、追跡可能な状態のアーティファクトをうっかり放置しているかもしれません。あるいは将来その一部を使用するつもりかもしれませんし、すでに使っている可能性もあります。

IoCとされたIPアドレスから

IoCとして特定されたIPアドレスを全てReverse IP Lookupで検索したところ、ドメイン名に名前解決したのは12個だけでした。各アドレスに関連付けられていたドメイン名は4つ以下であったことから、この12個は専用アドレスと思われます。これらの悪意あるIPアドレスに解決されるユニークなドメイン名は、合計で22個見つかりました。

IoCとされたドメイン名から

悪意あるドメイン名をWHOIS Historyで検索し、関連するデジタルプロパティが他にないか確認しました。その結果、未編集のメールアドレスが5つ見つかりました。そのうち2つは50個を超えるドメイン名の登録に使用されていたことから、ドメイナーのメールアドレスである可能性があります。そこで、この調査では、残りの3つのメールアドレスを使用して登録された44個のドメイン名に焦点を当てることにしました。

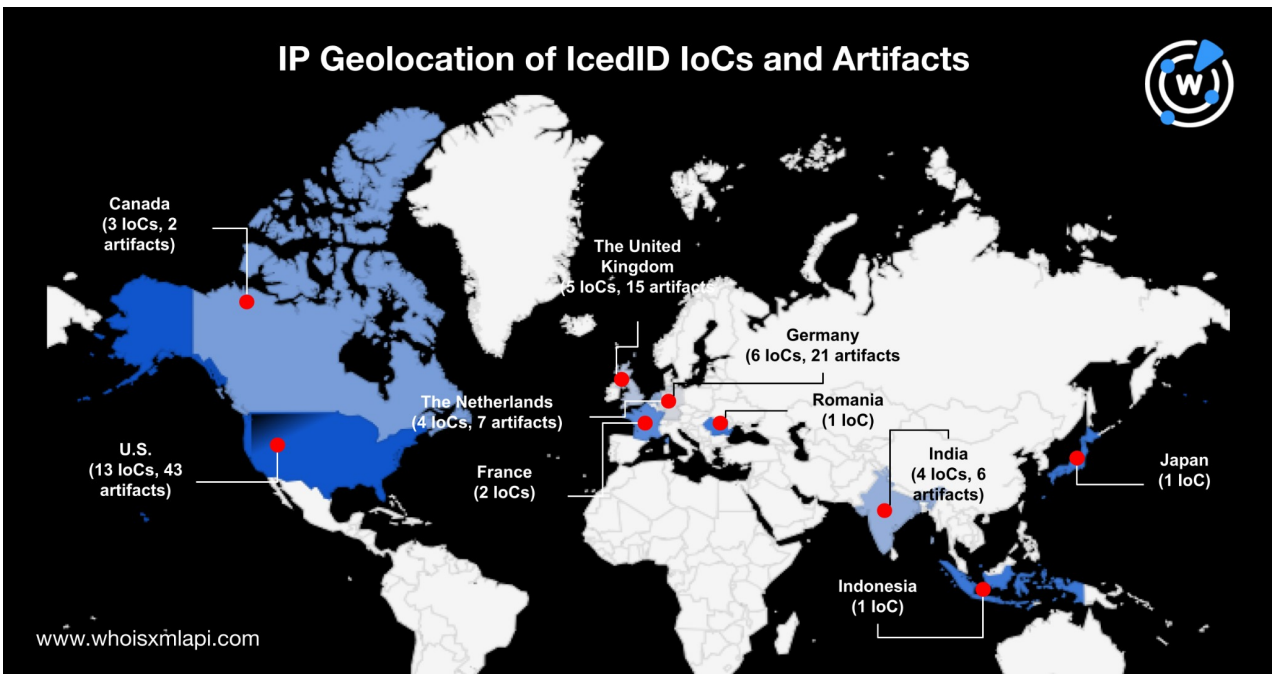
また、IoCのIPアドレスの名前解決を調べたところ、有効なコンテンツを指すアドレスは15個中6個のみであることがわかりました。うち3個は、250個あまりの別のドメインに共用されていました。これにより、悪意あるドメインネットワークに属している、または関連している可能性がより高いドメイン名が33個残りました。

今回判明したアーティファクトの詳細

全体として、IPアドレスを共用しているらしいアーティファクトとドメイン名を共用しているらしいアーティファクトが合計で99個特定されました。そのうちの約14%は、悪意あるものと分類されました。

また、関連付けられたドメイン名をBulk WHOIS Lookupで検索したところ、WHOISレコードがあるのは53個にとどまりました。それらはDomain Cost Clubをレジストラとして使っていました。

それらのジオロケーションをIP Geolocation Lookupで調べた結果、下図の通り、Cymruの研究者が名前を挙げたIPアドレスの位置またはそれに近い場所を含む7カ国に広がっていました。



—

最初に参照した59個のIoCから、脅威のインフラに属している、または関連している可能性のある99個のドメイン名が今回新たに見つかりました。それらとIoCの繋がりについてさらに精査する必要がありそうです。

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：出典、アーティファクトおよびIoCの例

出典

[1] https://www.team-cymru.com/post/inside-the-icedid-backconnect-protocol-part-2
[2] https://otx.alienvault.com/pulse/64cb26ac4990112e3f9e662f
[3] https://otx.alienvault.com/pulse/64c5cf320a92c0bdc8ab9068
[4] https://otx.alienvault.com/pulse/6401246d57e5b0d2ff1c6c58

IoCが名前解決したIPアドレスの例

- 1[.]23[.]82[.]72
- 104[.]248[.]21[.]165
- 104[.]248[.]223[.]35
- 106[.]177[.]224[.]34
- 116[.]203[.]30[.]206
- 134[.]122[.]62[.]178
- 135[.]148[.]217[.]85
- 138[.]112[.]25[.]25
- 138[.]197[.]146[.]18
- 138[.]68[.]244[.]54
- 139[.]59[.]186[.]140
- 139[.]59[.]33[.]128
- 139[.]59[.]72[.]105
- 159[.]89[.]116[.]11
- 161[.]35[.]166[.]97
- 162[.]33[.]179[.]145
- 162[.]33[.]179[.]218
- 167[.]99[.]235[.]95
- 167[.]99[.]248[.]131
- 185[.]99[.]132[.]16
- 192[.]153[.]57[.]134
- 193[.]149[.]176[.]100
- 193[.]149[.]176[.]198
- 193[.]149[.]187[.]7
- 193[.]239[.]85[.]16
- 2[.]12[.]51[.]56
- 207[.]154[.]203[.]203
- 209[.]38[.]220[.]183
- 21[.]15[.]46[.]55
- 35[.]3[.]46[.]245
- 36[.]75[.]75[.]75
- 45[.]61[.]137[.]159

- 45[.]61[.]137[.]159
- 45[.]61[.]137[.]220
- 45[.]61[.]139[.]144
- skigimeetroc[.]com
- skansnekssky[.]com
- askamoshopsi[.]com
- submit[.]org
- signup[.]team
- repository[.]click
- continue[.]email
- click[.]zero
- click[.]talk
- click[.]org
- click[.]open
- click[.]discover
- click[.]contact
- click[.]compare
- 2fgithub[.]com

共通のIPアドレスを使っていたドメイン名の例

- bortolatolino[.]it
- bxbotel[.]expert
- delivery-pt[.]com
- lfctoken[.]live
- liverpoolfctoken[.]club
- liverpoolfctoken[.]com
- liverpoolfctoken[.]online
- luisianafox[.]com
- mail[.]on-mail[.]ru
- nexus-api[.]scoutabroad[.]com
- gabrikxuira[.]com
- gyxplonto[.]com
- iskazorety[.]com
- keyzishaptu[.]com
- minesotkarpid[.]com
- nemchaprues[.]com
- pichervoip[.]com
- pinchersoftqum[.]com
- satifayban[.]com
- skansnekssky[.]com

共通のメールアドレスを使っていたドメイン名の例

- xn--qei8618m[.]ws
- xn--hl8haa[.]ws
- dcchosting1[.]ws
- xn--xj8haa[.]ws
- xn--k78h[.]ws
- emojis[.]ws
- xn--fz7h[.]ws
- xn--5h8h[.]ws
- whassup[.]ws
- xn--qei2808m[.]ws
- wassup[.]ws
- xn--57h9759n[.]ws
- xn--5l8haa[.]ws
- usa-merchant[.]com
- wesmile[.]ws
- worksuccess[.]ws
- xn--57hz0a[.]ws
- emojidomain[.]ws
- get-a-name[.]com
- geekwear[.]co

悪意あるアーティファクトの例

- dcchosting1[.]ws
- delivery-pt[.]com
- troptionstrading[.]com
- minesotkarpid[.]com
- nemchaprues[.]com
- pichervoip[.]com

- pinchersoftqum[.]com
- satifayban[.]com
- skansnekssky[.]com
- softwinmeod[.]com
- startinghpot[.]com
- troffyfrutlot[.]com
- yhorneedminf[.]com
- abigelofraj[.]com