1,800を超えるCloud Atlas関連アーティファクトを発見、企業の情報漏洩回避を支援

目次

要旨

サイバー犯罪組織のCloud Atlasは、2014年に発見されて以来、政治的紛争に苦しむ国の重要インフラ事業者に狙いを定めてサイバースパイ活動を行っています。「インセプション」との異名を持つCloud Atlasの戦術は功を奏しているようで、これまでさまざまな標的への侵入に成功しています。

Check Point Research（CPR）は先般、標的となり得る組織が情報漏洩の危険を回避できるよう、以下のIoC（セキュリティ侵害インジケーター）を公表しました。

- translate-news[.]net
- technology-requests[.]net
- remote-convert[.]com
- protocol-list[.]com
- gettemplate[.]org
- driversolution[.]net
- desktoppreview[.]com
- comparelicense[.]com
- 185[.]227[.]82[.]21
- 146[.]70[.]88[.]123

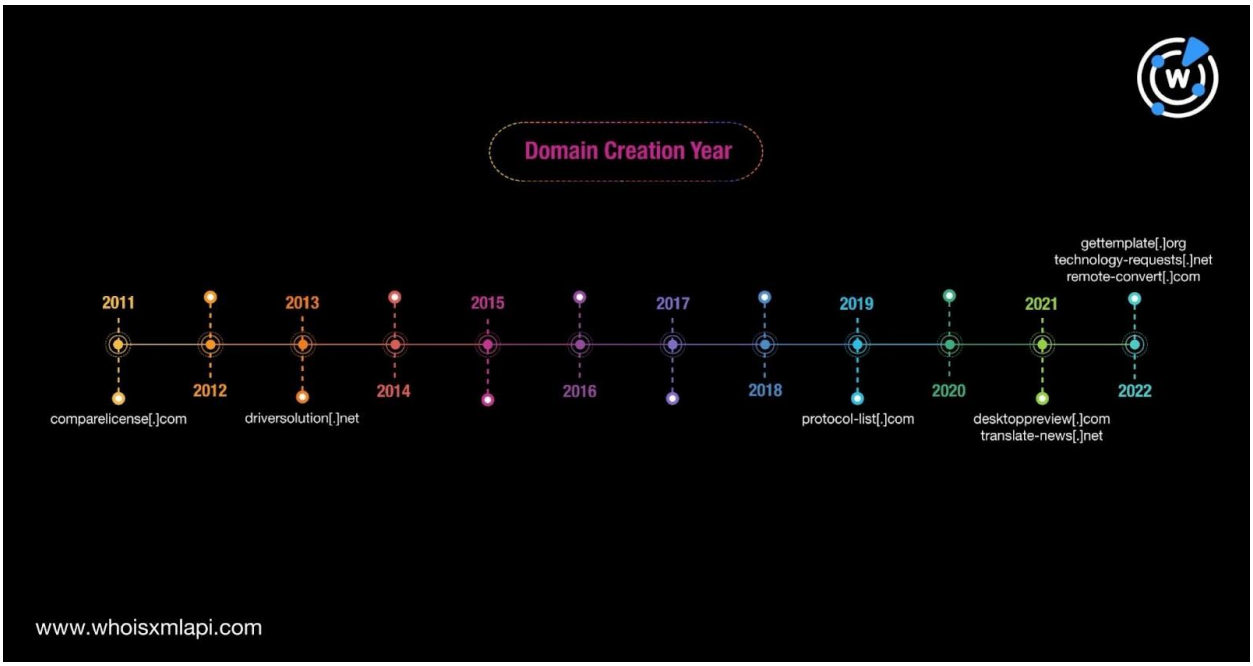
WhoisXML APIでは、上記もとに調査を展開し、さらに以下のアーティファクトを発見しました。

- IoCとされたドメイン名が名前解決したIPアドレスをさらに8つ。
- IoCと同じIPアドレスを使用しているドメイン名をさらに324件。そのうち2件は悪意あるドメイン名。
- IoCとされたドメイン名と同じ文字列を含んだドメイン名をさらに1,519件。そのうち1件は悪意あるドメイン名。

IoC分析の結果

当社はまず、IoCをbulk WHOIS lookupで検索しました。結果は以下の通りです。

- IoCとしてタグ付けされたドメイン名（以下「ドメインIoC」）のうち、2件（gettemplate[.]org とcomparelicense[.]com）は検索できるWHOISレコードがなかった。
- WHOSレコードが存在するドメインIoCのうちprotocol-list[.]comとtechnology-requests[.]netのレジストラはNetEarth One, Inc、driversolution[.]netとremote-convert[.]comのレジストラはPDR Ltd.（商号： PublicDomainRegistry.com）。残り2件のドメイン名のレジストラはそれぞれDanesco Trading Ltd.とInternet Domain Service BS Corp。
- 全てのドメインIoCのWHOISレコードは一部非表示になっていた。
- 下図の通り、ドメインIoCの多くは2022年に新規登録された。



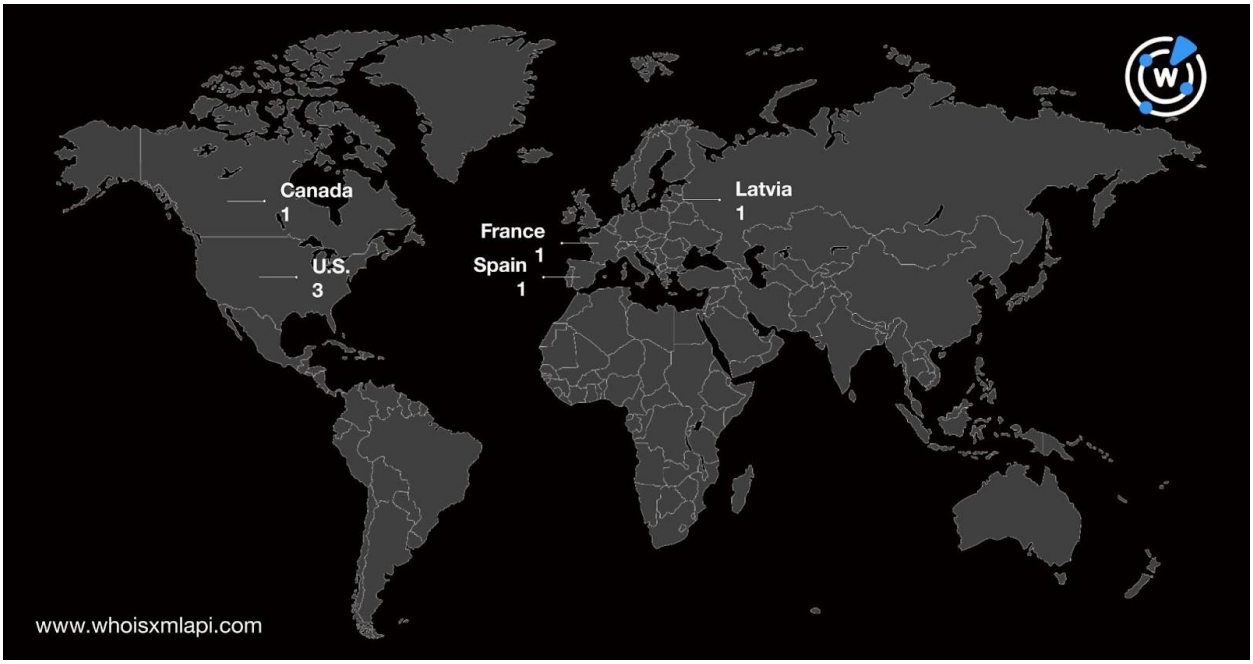
- ドメインIoCの登録者はオランダ、フィンランド、キプロス、イギリスおよびカナダに分散。
- 今のところいずれのドメインIoCも悪意あると判定されず。しかし、Cloud Atlasとの関連から、これらへのアクセスは全てブロックすることが得策と思われる。

他方、IoCと識別されたIPアドレス（以下「IPアドレスIoC」）をIP geolocation lookupsで調べたところ、共通点は見つかりませんでした。185[.]227[.]82[.]21のISPはAccess2.IT Group B.V.で、地理的にはオランダにありました。146[.]70[.]88[.]123のISPはM247 Europe SRLで、地理的にはフランスです。2つとも悪意があると見なされませんでしたが、Cloud Atlasとの関係を考慮し、少なくとも疑わしい動きがないか厳しく監視しておく必要がありそうです。

Cloud Atlasがこれまで標的のネットワークへの侵入に成功していること、そして重要なインフラ事業者に的を絞っていることを踏まえ、当社は公表されているIoCのリストを広げ、 将来標的となり得る企業が脅威を軽減できるようにすることを目指しました。

IoCの調査を水平展開

関連している可能性のあるアーティファクトをできるだけ多く見つけるため、まずドメインIoCをDNSルックアップで調べ、8つのIPアドレスを発見しました。次にそれらをbulk IP geolocation lookup で検索し、5[.]135[.]199[.]19がIoCである146[.]70[.]88[.]123と同様にフランスで登録されたことがわかりました。それ以外のIPアドレスは、以下の通り4カ国にありました。



悪意があると判定されたIPアドレスはなかったものの、詳細に調べた結果、全てについてSSL（Secure Socket Layer）の設定に誤りがあることが判明しました。

加えて、2つのIPアドレスIoCとさらに7つのアーティファクトをreverse IP lookupsで検索したし、324件のドメイン名を特定しました。そのうちの2件、すなわちlucid-banzai[.]104-219-233-120[.]plesk[.]pageとwww[.]lucid-banzai[.]104-219-233-120[.]plesk[.]pageは、悪意のあるドメイン名であることが明らかになりました。

また、ドメインIoCの中に特定の文字列があることに気づいたため、以下を条件としてDomains & Subdomains Discoveryでさらに潜在的な繋がりを探ってみました。

- “translate + news”
- “technology + request”

- “remote + convert”
- “protocol + list”
- “get + template”
- “driver + solution”
- “desktop + preview”
- “compare + license”

その結果、さらに1,519件のドメイン名がアーティファクトと判定されました。当社が使用したマルウェアエンジンで悪意あるドメイン名とされたのは、solutionefordriversandrestornow[.]onlineという1件のみです。IoCに最もよく似たアーティファクトの例は以下です。異なるトップレベルドメイン（TLD）の下に同じ文字列を登録したものなどが見られます。

- translate-news[.]com
- gettemplate[.]ir
- gettemplate[.]co
- gettemplate[.]us
- gettemplate[.]de
- gettemplate[.]io
- gettemplate[.]tk
- gettemplate[.]ru
- gettemplates[.]co
- gettemplate[.]net
- gettemplate[.]com
- driversolution[.]pl
- driversolution[.]com
- driversolution[.]info
- desktoppreview[.]ws

—

今回IoCの情報を水平展開して調査した結果、3件の悪意あるドメイン名を含む1,850のCloud Atlas関連のアーティファクトが追加で見つかりました。それらがホストしているウェブサイトにアクセスすると、潜在的な標的やその他の組織を危険にさらす可能性があります。IPアドレス、DNSおよびWHOISの情報がなければ、このような関連性の発見は不可能だったでしょう。

同様の調査をご希望のお客様、またはこの調査のデーター式をご希望のお客様は、こちらへお気軽にお問い合わせください。

付録：アーティファクトとIoCの例

CPRが特定したCloud AtlasのIoC

- translate-news[.]net
- technology-requests[.]net
- remote-convert[.]com
- protocol-list[.]com
- gettemplate[.]org
- driversolution[.]net
- desktoppreview[.]com
- comparelicense[.]com
- 185[.]227[.]82[.]21
- 146[.]70[.]88[.]123

IoCとされたドメイン名が名前解決したIPアドレスの例

- 192[.]144[.]39[.]67
- 149[.]56[.]175[.]181

- 172[.]105[.]103[.]207
- 5[.]135[.]199[.]19

IoCと同じIPアドレスを共用していたドメイン名の例

- 064625[.]parkingcrew[.]net
- 0x21[.]in
- 104-219-233-120[.]plesk[.]page
- 23012002[.]com
- 2mblk[.]com
- 43nutrientes[.]com
- 548260[.]parkingcrew[.]net
- 5pneuovxi22i4fagh9[.]today
- 7-eleven-handbags[.]com
- 825610[.]parkingcrew[.]net
- 8tril[.]com
- 944279[.]parkingcrew[.]net
- a-plague-tale[.]top
- a2c491023580[.]com
- a2e6b661ca0e4c4c4[.]awsglobalaccelerator[.]com
- a5c6a0cc95db01a9[.]com
- abrakadabras[.]net
- abvtqhwodwjmi[.]work
- accemfsqovkd[.]pw
- account[.]adfs[.]kyivstar[.]online
- acerthk3v9fvsby5n[.]today
- acjhwpdjhlhbncf[.]click
- adams679[.]drcopps[.]com
- adfs[.]kyivstar[.]online
- admiral-juegos[.]com
- adobe-update [.]net
- adobestats[.]com
- adsdsadsalifsa[.]digital
- agceram[.]com
- agusanplantation[.]com
- ahsqbeospcdrngfv[.]info
- aliensdrop[.]com
- allen1037[.]pelangiqq99[.]com
- allen139[.]drcopps[.]com
- allen618[.]drcopps[.]com
- allsofttech[.]com
- amakeperfeita[.]online
- ampjsppmftmfdblpt[.]info
- anderson360[.]pelangiqq99[.]com
- anderson576[.]pelangiqq99[.]com
- anderson856[.]drcopps[.]com
- anderson858[.]drcopps[.]com
- antichltabompadre[.]com
- asdakasma[.]digital
- asiaworldremit[.]com
- assumethepositionstudio[.]com
- autoconfig[.]celikklczet[.]com
- autoconfig[.]simsekaluminyurn[.]com
- autodiscover[.]celikklczet[.]com
- autodiscover[.]simsekaluminyurn[.]com

IoCに含まれるものと同じ特定の文字列を含んでいるドメイン名の例

- translate[.]news
- translates[.]news
- translated[.]news
- translatenews[.]ru
- translatenews[.]org
- newstranslate[.]com
- translatednews[.]de
- translatethe[.]news
- translatenews[.]com
- translatednews[.]com
- translatednews[.]net
- news-translate[.]com
- translate-news[.]com
- newstranslated[.]com

- translate-news[.]net
- newstranslater[.]com
- utranslatenews[.]com
- newstranslate[.]info
- ektranslatednews[.]fun
- translatethenews[.]net
- translatethenews[.]com
- translateall-news[.]com
- translatenewsspeed[.]gq
- thenewstranslated[.]com
- thetranslatednews[.]com
- technologyrequest[.]ga
- technologyrequest[.]bid
- requesttechnology[.]xyz
- requesttechnology[.]org
- requesttechnology[.]net
- technologyrequest[.]com
- requesttechnology[.]com
- technologyrequest[.]life
- technology-request[.]com
- technology-requests[.]net
- requesttechnology[.]nom[.]za
- requestfortechnology[.]com
- requesttechnology[.]com[.]au
- thoughtrequest[.]technology
- technologyofferrequest[.]com
- requestintegrity[.]technology
- gdprdatarequests[.]technology
- uor-technology-request-form[.]com
- subjectaccessrequest[.]technology
- personaldatarequests[.]technology
- subjectaccessrequests[.]technology
- technologyrequestinformation[.]info
- gdprpesonaldatarequests[.]technolo gy
- alternativeenergyrequestfortechnolo gy[.]com
- convertremote[.]com
- protocolist[.]ru
- protocolist[.]xyz
- protocolist[.]xn--kpry57d
- protocolist[.]xn--kprw13d
- protocolist[.]com
- protocolist[.]pro
- protocollist[.]com
- protocolist[.]tech
- protocolista[.]com
- protocolist[.]site
- protocolist[.]info
- listprotocol[.]com
- protocolistas[.]es
- protocolistas[.]net
- protocol-list[.]com
- protocolistas[.]com
- protocolslist[.]com
- protocolist[.]trade
- protocolist[.]com[.]ua
- protocolist[.]online
- theprotocolist[.]com
- calistoprotocol[.]com
- listingprotocol[.]com
- holisticprotocol[.]com
- protocollist[.]website
- gettemplate[.]ir
- getemplate[.]com
- gettemplate[.]co
- gettemplate[.]us
- gettemplate[.]de
- gettemplate[.]io
- gettemplate[.]tk
- gettemplate[.]ru
- pagetemplate[.]no
- templateget[.]net
- gettemplates[.]co
- gettemplate[.]org
- gettemplate[.]net
- gettemplate[.]com
- templateget[.]com
- getemplates[.]com
- getatemplate[.]co

- getatemplate[.]ca
- gettemplates[.]ru
- get-template[.]eu
- gettemplates[.]io
- pagetemplate[.]cn
- edgetemplate[.]com
- get2template[.]com
- pagetemplates[.]de