Google広告で拡散した不正ソフトの繋がりをたどる

目次

要旨

被害者のアカウントの支配は多くのサイバー犯罪者の最終目標であり、彼らは巧妙な方法を考え出すのに余念がありません。Bleeping Computerは最近、オープンソースソフトウェアのダウンロードサイトを指す建前のGoogle広告を通じてハッカーがマルウェアの被害を広げていることを発見しました。

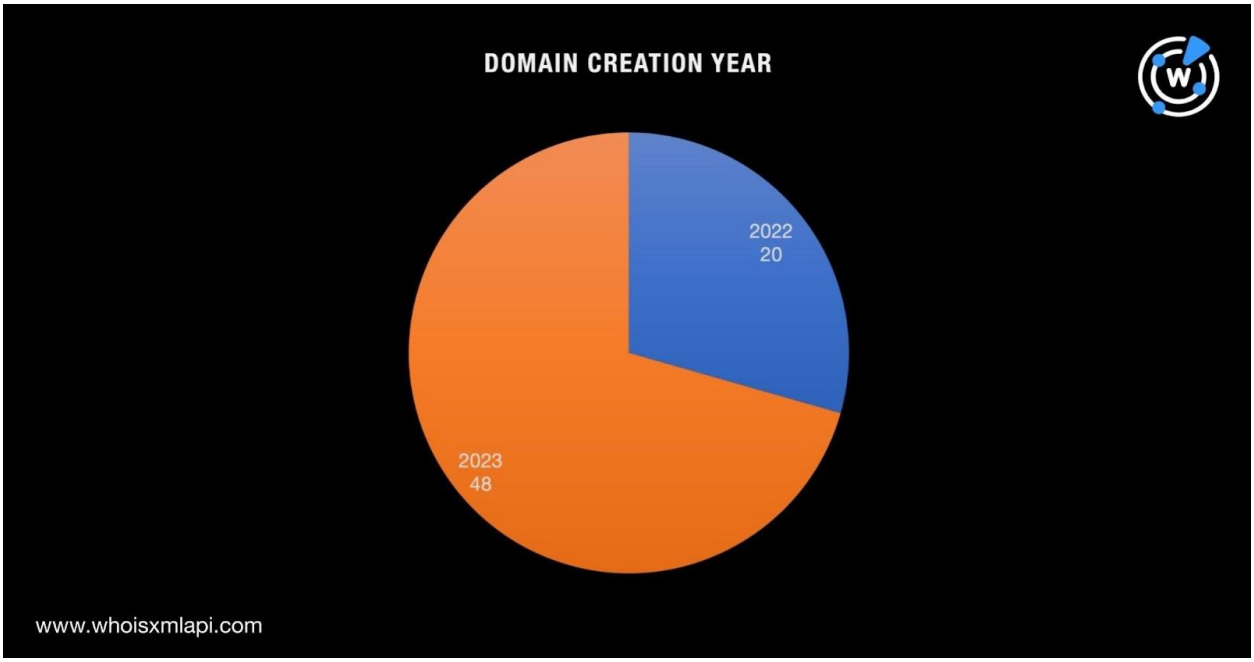
そこで、WhoisXML APIの研究者は、CronUpのGermán Fernández氏がまとめたIoC（セキュリティ侵害インジケーター）のリスト（68個のドメイン名）をもとに調査を展開しました。その結果、以下を発見しました。

- IoCの現在のWHOISレコードから、2つの無編集のメールアドレス。それらのメールアドレスを使っている18個の別のドメイン名も判明。
- IoCが名前解決した2つのIPアドレス。どちらも悪意があると確認。
- 同じIPアドレスに名前解決する329個のドメイン名。そのうち5つは悪意があると確認。
- 共通の文字列を使っているドメイン名84個。そのうち2つは悪意があると確認。
- 攻撃者が標的にした11のソフトウェアブランドを文字列として含む387個のドメイン名。そのうち27個はマルウェアのホストと確認。

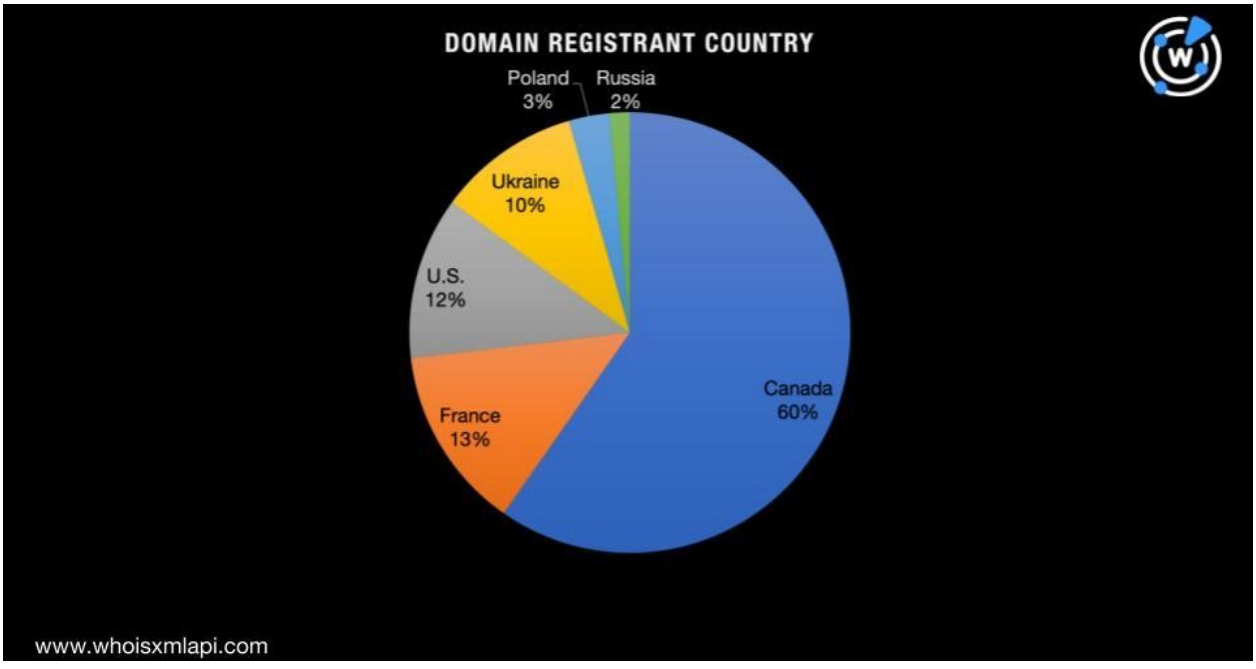
WHOISで関連性を解明

今回の調査では、まずIoCとして特定されたドメイン名をbulk WHOIS lookupで検索し、以下の共通点を見出しました。

- 全てのIoCはPDR Ltd.を通じて登録されている。
- 71%のIoCは2023年に登録されたばかり。残りの29%は2022年の登録。



- IoCの登録者は6カ国に散らばっている（カナダ60%、フランス13%、米国12%、ウクライナ10%、ポーランド3%、ロシア1%）。



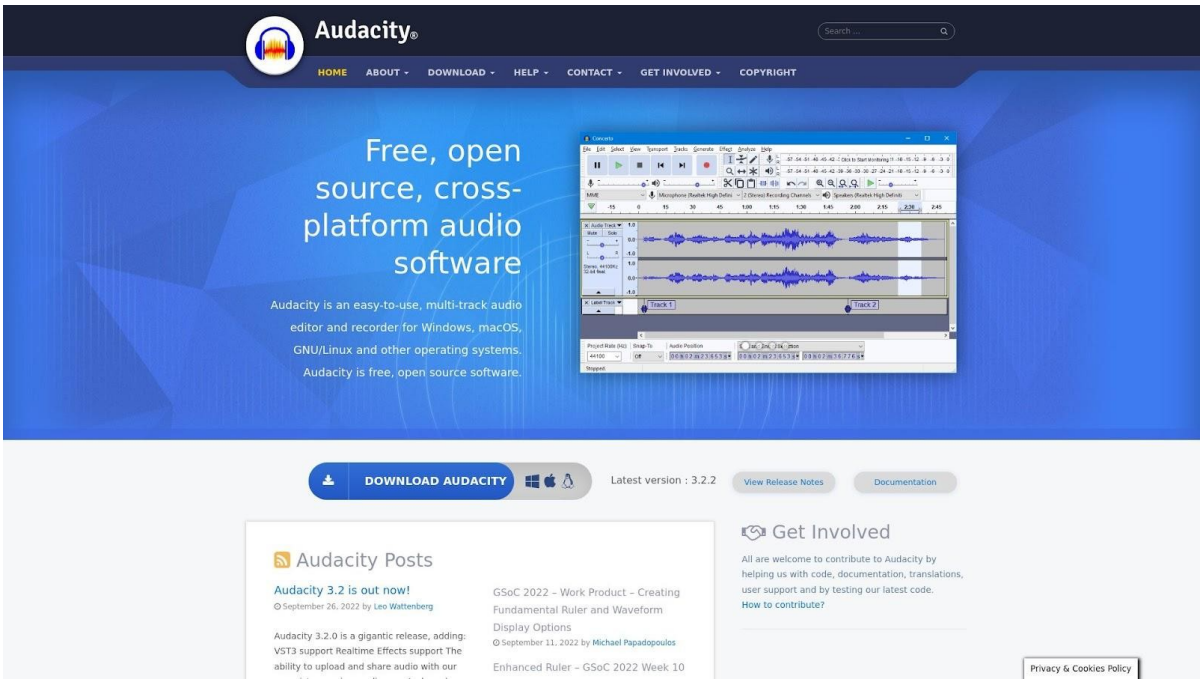
- 5つのIoCのレコードに無編集の登録者メールアドレスが表示された。

続いてそれらのメールアドレスをreverse WHOIS searchesで検索したところ、IoCリストに含まれていない19個のドメイン名を登録する際にもそれらが使われていたことがわかりました。IoCとの関連性を考えると、少なくとも不審な活動の兆候がないか監視する必要がありそうです。

DNSで関連性を解明

さらなる手がかりを見つけ出すため、次にDNSの繋がりに着目しました。まず、DNS lookupsで検索し、IoCが名前解決した2つのIPアドレス（74[.]119[.]239[.]234と185[.]149[.]120[.]133）に行き着きました。そして、どちらも悪意あるものと確認しました。オープンソースソフトウェアのダウンロードや使用を従業員に許可している組織は、これらの危険なIPアドレス（1つは米国、もう1つはロシアに位置）へのアクセスをブロックすることが望ましいでしょう。

また、Reverse IP/DNS lookupsでそれらを調べたところ、さらに329個のドメイン名が検出されました。そのうち5個は悪意あるドメイン名と確認されました。このうちの2つは、screenshot lookupによるとAudacityのダウンロードページと思われるものをホストしており、脅威と関連しているように思われました。



fantasyfootballfreaks[.]comとsilveralawjamaica[.]comのスクリーンショット

関連していそうなウェブプロパティをさらに見つけるため、次に文字列を分析しました。IoCリストで見受けられる以下のユニークな文字列をキーワードとして、Domains & Subdomains Discoveryで調べました。

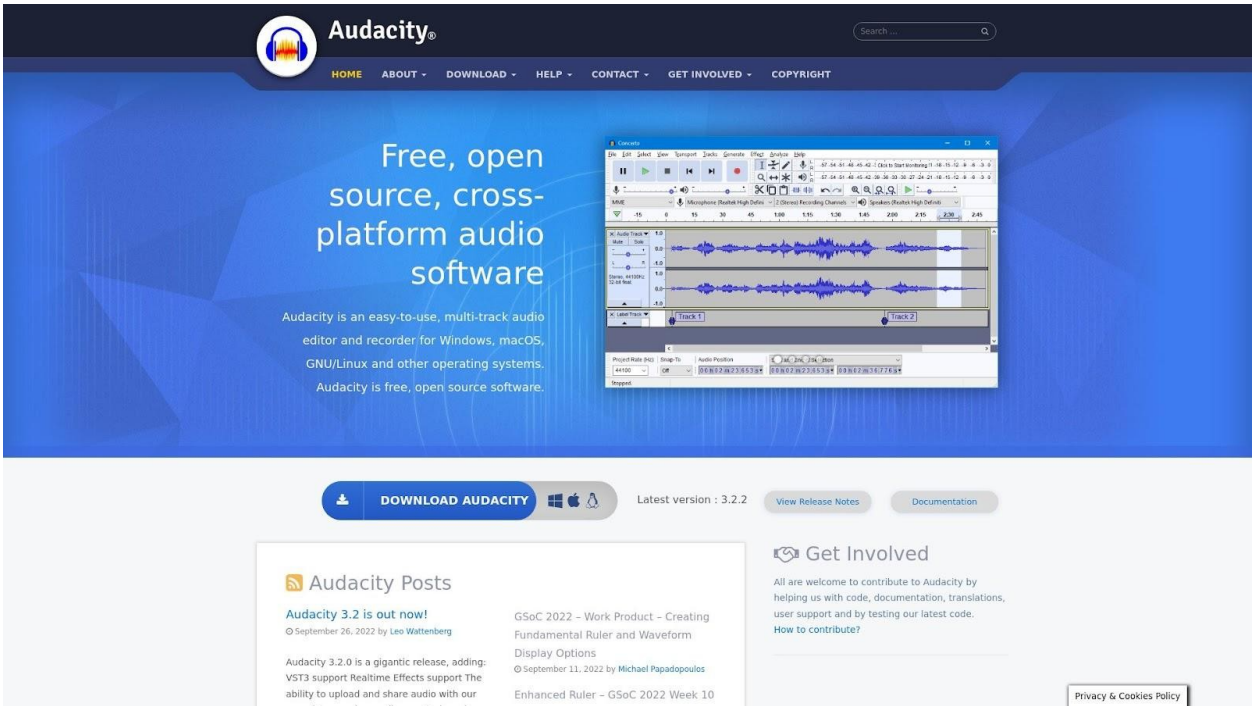
- ***vilc.***
- ***tecinovations.***

- *tecinnovations.*
- *tecinnovation.*
- *techinovation.*
- *qobstreamsviews.*
- *qobstreamsview.*
- *ostreeming.*
- *odstreamsviews.*
- *odstraeming.*
- *obstremswiev.*
- *obstremsview.*
- *obsspro.*
- *obsproect.*
- *obrproject.*
- *obpproject.*
- *obmprolect.*
- *oblproject.*
- *obcprolect.*
- *obcproect.*
- *godstreamsviews.*
- *godstreamsview.*
- *glmps.*
- *audasite.*
- *audacslty*

このアプローチにより、さらに84個のドメイン名が見つかりました。そのうち2つ、すなわちtecinovations[.]spaceとtecinovations[.]onlineは、悪意あるドメイン名と確認されました。

IoCであるtecinovations[.]pwと明らかに類似しており（違いはTLDのみ）、マルウェアのホストと確認されていることから、これらへのアクセスをブロックすることは良い予防策になると思われます。残りの82個のドメイン名は、現時点では悪意のないものとされています。しかし、他のIoCと類似しており、違いはTLDのみであることから、依然として監視の対象となり得ます。

なお、興味深いことに、今は悪意のないドメイン名とされているobsspro[.]pwは、同じIPアドレスを共用している悪意あるドメイン名やAudacity関連のIoCと同じコンテンツをホストしていました。



obsspro[.]pwのスクリーンショット

目立たない関連性？

Bleeping Computerの研究では、不正なGoogleの検索結果ページで見受けられた以下の11のオープンソースソフトウェアについて言及しています。

- 7-Zip
- Blender 3D
- Capcut
- CCleaner
- Notepad++
- OBS
- Rufus
- VirtualBox
- VLC Media Player
- WinRAR
- Putty

これらのソフトウェアの開発者が実際に所有しているドメイン名がいくつあるか、また、タイポの文字列を含む悪意あるドメイン名があるかどうかを確認するため、ソフトウェアの名前と「download」という文字列を含む（例：7-zip + download）ドメイン名を探しました。その結果、さらに387個のドメイン名が特定され、そのうちの27個は悪意あるドメイン名であることが確認されました。

また、WHOISレコードの詳細を比較した結果、これらのドメイン名のいずれもソフトウェア開発者自身の所有ではないことが分かりました。ただし、開発者の情報がWHOISレコードで参照できたのは7つのソフトウェアについてのみです。7-Zip、Notepad++、RufusおよびVirtualBoxについては、ドメイン名所有の正当性を確認できませんでした。

—

今回当社で行ったIoCリストの拡充を通じ、Google広告を侵入経路とする不正ソフトウェア攻撃に関連している可能性のあるデジタルプロパティ（メールアドレス、IPアドレス、ドメイン）を822個発見できました。さらに注目すべきは、元のIoCリストにはなかった36個の悪意あるIPアドレスとドメイン名を特定できたことで、その中にはIoCと酷似しているものもありました。

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、こちらまで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

Bleeping ComputerがIoCと特定したドメイン名

- vilc[.]site
- tecinovations[.]pw
- tecinnovations[.]online
- tecinnovation[.]website
- tecinnovation[.]space
- tecinnovation[.]site
- tecinnovation[.]online
- tecinnovation[.]fun
- techinovation[.]website
- techinovation[.]space
- techinovation[.]site
- techinovation[.]online
- techinovation[.]fun
- qobstreamsviews[.]website
- qobstreamsviews[.]space
- qobstreamsviews[.]site
- qobstreamsviews[.]online
- qobstreamsviews[.]fun
- qobstreamsview[.]website
- qobstreamsview[.]site
- qobstreamsview[.]online
- qobstreamsview[.]fun
- ostreeming[.]website
- ostreeming[.]space
- ostreeming[.]site
- ostreeming[.]online
- ostreeming[.]fun
- odstreamsviews[.]website
- odstreamsviews[.]space
- odstreamsviews[.]site
- odstreamsviews[.]online
- odstreamsviews[.]fun
- odstraeming[.]website
- odstraeming[.]space
- odstraeming[.]site
- odstraeming[.]online
- odstraeming[.]fun
- obstremswiev[.]space
- obstremswiev[.]site
- obstremswiev[.]online
- obstremswiev[.]fun
- obstremsview[.]online
- obsspro[.]website
- obsspro[.]site
- obsspro[.]online
- obsproect[.]site
- obrproject[.]com
- obpproject[.]com
- obmprolect[.]com
- oblproject[.]com
- obcprolect[.]com
- obcproect[.]site

- godstreamsviews[.]website
- godstreamsviews[.]space
- godstreamsviews[.]site
- godstreamsviews[.]online
- godstreamsviews[.]fun
- godstreamsview[.]website
- godstreamsview[.]space
- godstreamsview[.]site
- godstreamsview[.]online
- godstreamsview[.]fun
- glmps[.]site
- audasite[.]website
- audasite[.]space
- audasite[.]site
- audasite[.]online
- audacslty[.]site

同じ連絡先メールアドレスを使っていたドメイン名の例

- subliemetext[.]com
- obsiprojiect[.]com
- obspfoject[.]com
- obsporjeict[.]com
- obsprojtect[.]com
- obsprojitect[.]com
- obspjct[.]com
- glhister[.]com
- mlialterburner[.]com

同じIPアドレスに名前解決したドメイン名の例

- 0-100golf[.]online
- 0-scotiaonline[.]com
- 0000000fc[.]top
- 0000001fc[.]top
- 0000002fc[.]top
- 00187[.]online
- 007seacharter[.]com
- 01-kras[.]store
- 011sport[.]info
- 0121perspective[.]com
- 1-basket[.]com
- 1-domsumom[.]store
- 1-news-2[.]site
- 1-news-224[.]site
- 1-news-2blog[.]site
- 1-news-2centr[.]site
- 1-news-2club[.]site
- 1-news-2dom[.]site
- 1-news-2expert[.]site
- 1-news-2forum[.]site
- audecityy[.]site
- birdreston[.]com
- calmspin[.]com
- cannonbohn[.]com
- chrismieloch[.]com
- debopriyo[.]com
- fantasyfootballfreaks[.]com
- greyscalemarketing[.]com
- ilanportal[.]com
- larklaneliverpool[.]com
- naturalmanifestor[.]com
- obcproilect[.]site
- obesprojiect[.]site
- obsproj[.]fun
- obsproj[.]pw
- obsproj[.]site
- obsspro[.]pw
- obstremswiev[.]website
- odstreamsviews[.]website
- offbeatdoula[.]com
- ostreamview[.]fun
- ostreamview[.]online
- ostreamview[.]site
- ostreamview[.]space

同じIPアドレスに名前解決した悪意あるドメイン名の例

- 0nline-secure[.]com
- 1001-interactransfert-return[.]com
- 1001414202102278105999991[.]com

共通の文字列を含むドメイン名の例

- vilc[.]xyz
- vilc[.]tokyo
- vilc[.]net
- vilc[.]com
- vilc[.]org
- vilc[.]net[.]au
- tecinovations[.]space
- tecinovations[.]online
- tecinovations[.]fun
- tecinovations[.]website
- tecinnovations[.]site
- tecinnovations[.]website
- qobstreamsview[.]space
- obstremswiev[.]website
- obstremsview[.]fun
- obstremsview[.]space
- obstremsview[.]site
- obstremsview[.]website
- glmps[.]ca
- glmps[.]com
- glmps[.]pl
- glmps[.]org
- glmps[.]us

共通のブランド名を含むドメイン名の例

- 7-zip[.]download
- download7-zip[.]tk
- 7-zipdownload[.]us
- download-7-zip[.]ru
- 7-zipdownload[.]net
- 7-zip-download[.]ru
- 7-zip-download[.]de
- download7-zip[.]com
- 7-zipdownload[.]com
- 7-zipdownloads[.]com
- blender3d-download[.]org
- blender3d-download[.]net
- blender3d-download[.]com
- blender3ds-download[.]net
- blender3ds-download[.]org
- blender3ds-download[.]com
- capcutdownload[.]com
- capcutapp[.]download
- capcut-download[.]com
- capcutdownloader[.]com
- ccleaner[.]download
- ccleanerdownload[.]nl
- ccleanerdownload[.]ml
- ccleanerdownload[.]co
- ccleanerdownload[.]ru
- ccleanerdownload[.]me
- maccleaner[.]download
- ccleanerdownloads[.]ru
- ccleanerdownload[.]org
- download-ccleaner[.]de
- notepade[.]download
- notepadownload[.]cam

- notepad-download[.]ru
- notepad-download[.]de
- notepaddownload[.]com
- notepaddownload[.]net
- downloadnotepads[.]com
- notepad-download[.]com
- downloadnotepad73[.]tk
- notepaddownload[.]info
- obsdownload[.]com
- obs-download[.]com
- download-obs[.]com
- download-obs[.]live
- download-obs[.]xyz
- download-obs[.]life
- obs-download[.]website
- downloadobsfree[.]site
- downloadrufus[.]ml
- rufusdownload[.]ru

共通のブランド名を含む悪意あるドメイン名の例

- 7-zipdownload[.]us
- blender3ds-download[.]org
- blender3ds-download[.]com
- capcutdownload[.]com
- ccleaner-download[.]xyz
- download-ccleaner[.]tech
- ccleaner-downloads[.]com
- ccleaners-download[.]com
- rufus-download[.]ru
- rufusdownload[.]info
- virtualboxdownload[.]com
- downloadvirtualbox[.]com
- virtualbox-download[.]ru
- vlcmediaplayerfreedownload[.]com
- winrars-download[.]com
- download-winrarr[.]com
- winrar-downloads[.]com
- winrarr-download[.]com
- winrarr-downloads[.]com
- winrar-pro-download[.]com