WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Tracing Connections to Rogue Software Spread through Google Search Ads

Table of Contents

Executive Report

Taking control of victims’ accounts is typically the end goal of many cybercriminals, and they never cease to come up with wily ways to do so. Bleeping Computer researchers recently spotted hackers spreading malware mayhem through Google search ads supposedly pointing to open-source software download sites.

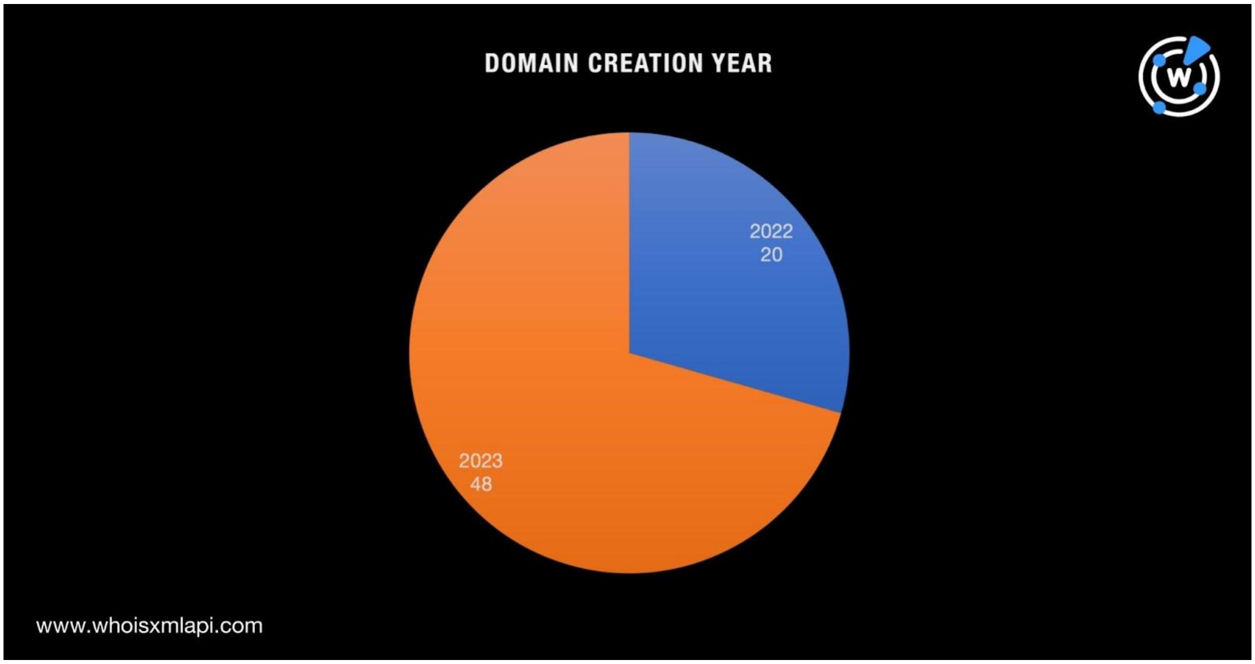
WhoisXML API researchers subjected the list of indicators of compromise (IoCs) compiled by CronUp’s Germán Fernández—68 domains to be exact—to an expansion analysis and found:

- Two unredacted registrant email addresses from the IoCs’ current WHOIS records that led to 18 email-connected domains
- Two IP addresses to which the IoCs’ resolved, both of which were found malicious
- 329 IP-connected domains, five of which turned out to be malicious
- 84 string-connected domains, two of which were malicious
- 387 domains that contained the 11 software brands the attackers targeted, 27 of which were confirmed malware hosts

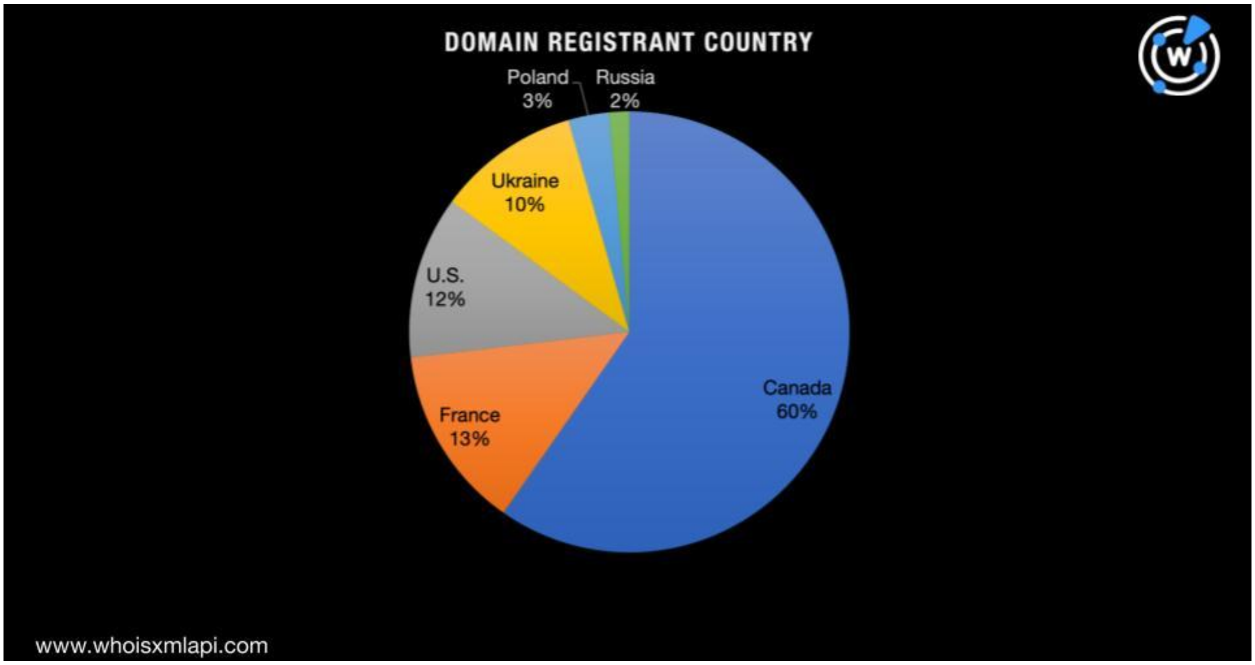
WHOIS Connections Uncovered

We began our in-depth look into the threat with a bulk WHOIS lookup for the domains identified as IoCs that allowed us to identify these similarities:

- All of the IoCs were registered with PDR Ltd.
- A majority of the IoCs, 71% to be exact, were recently created—just this year, while the remaining 29% were created last year.



- The IoCs' registrants were spread across six countries—Canada (60%), France (13%), the U.S. (12%), Ukraine (10%), Poland (3%), and Russia (1%).



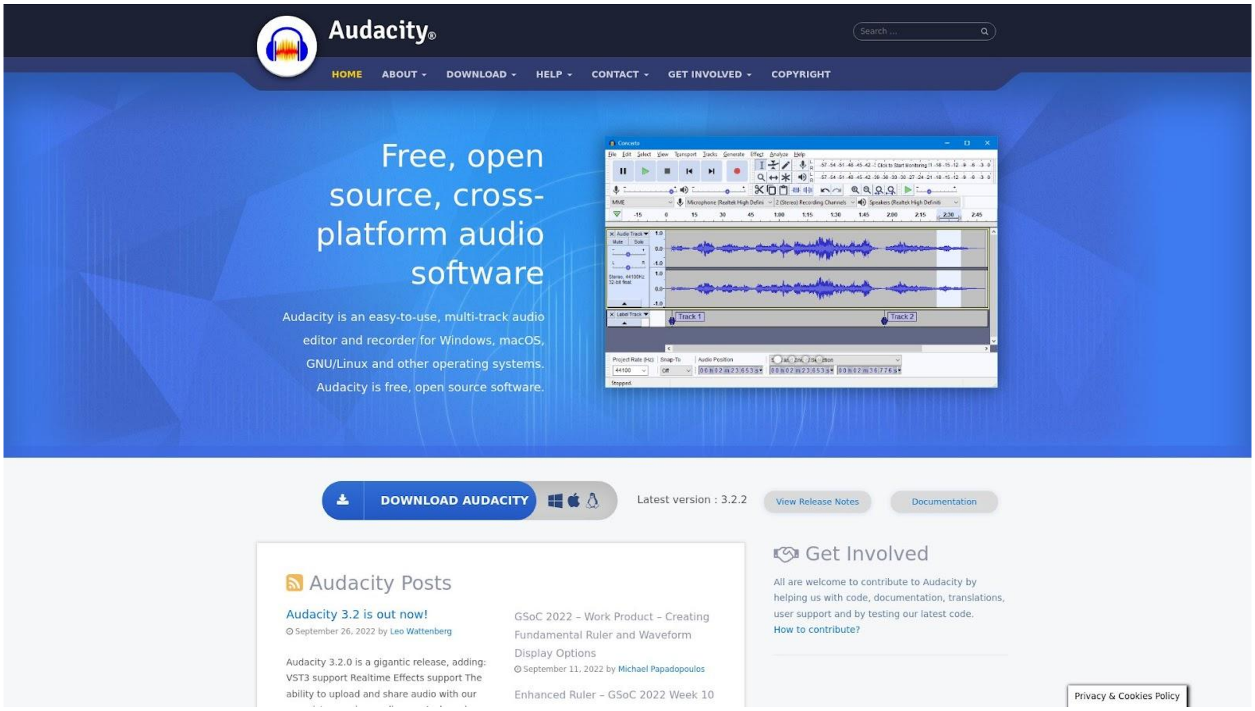
- Five of the IoCs indicated unredacted registrant email addresses in their records.

Advanced reverse WHOIS searches for the email addresses showed they were used to register 19 other domains not included in the IoC list. Given their connection to the IoCs, they may warrant monitoring for signs of suspicious activity at least.

DNS Connections Unraveled

In an effort to find more digital breadcrumbs, we looked at DNS connections next, starting with DNS lookups that uncovered two of the IoCs' IP hosts—74[.]119[.]239[.]234 and 185[.]149[.]120[.]133—both of which turned out to be malicious. Organizations that allow employees to download and use open-source software would do well to block access to these dangerous web properties—one geolocated in the U.S. and the other in Russia.

Reverse IP/DNS lookups then led to the discovery of 329 more domains, five of which were found to be malicious. And like the IoCs, two of these hosted what seemed to be Audacity download pages based on screenshot lookup results, making them appear to be related to the threat.



Free, open source, cross-platform audio software

Audacity is an easy-to-use, multi-track audio editor and recorder for Windows, macOS, GNU/Linux and other operating systems. Audacity is free, open source software.

Latest version : 3.2.2

Audacity Posts

Audacity 3.2 is out now!
September 26, 2022 by Leo Wattenberg

Audacity 3.2.0 is a gigantic release, adding: VST3 support Realtime Effects support The ability to upload and share audio with our

GSoC 2022 – Work Product – Creating Fundamental Ruler and Waveform Display Options
September 11, 2022 by Michael Papadopoulos

Enhanced Ruler – GSoC 2022 Week 10

Get Involved

All are welcome to contribute to Audacity by helping us with code, documentation, translations, user support and by testing our latest code.
How to contribute?

Screenshot of fantasyfootballfreaks[.]com and silveralawjamaica[.]com

To find more possibly connected web properties, we turned to a string analysis. We used the unique strings found among the IoCs listed below as Domains & Subdomains Discovery search terms.

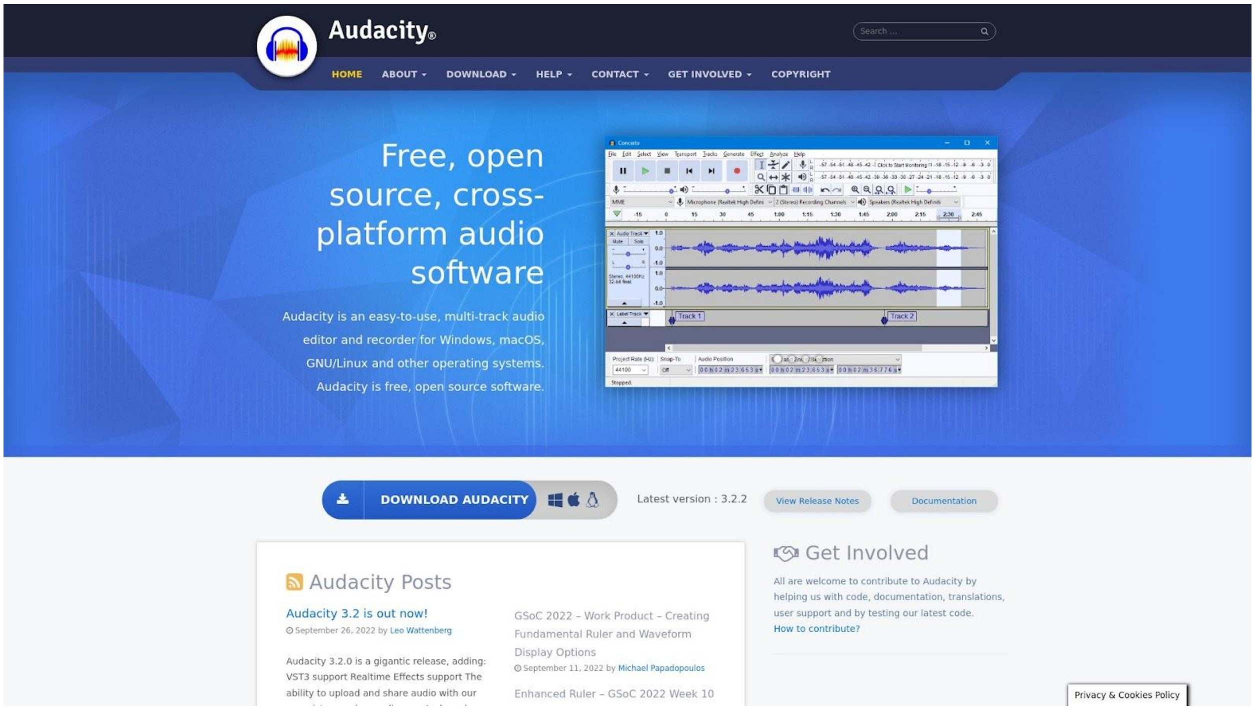
- ***vilc.***
- ***tecinovations.***

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

Through this approach, we compiled a list of 84 more domains, two of which—tecinovations[.]space and tecinovations[.]online—turned out to be malicious.

Given their obvious similarity with the IoC tecinovations[.]pw (they only differed in terms of TLD extension) and that they were confirmed malware hosts, it would be a good precaution to block access to and from these properties. And while the remaining 82 domains are currently considered nonmalicious, they may still warrant monitoring given that they look like the other IoCs and just sported different TLD extensions.

One nonmalicious domain—obsspro[.]pw—proved particularly interesting, though, since it hosted the same content as the malicious IP-connected domains and Audacity-related IoC.



Free, open source, cross-platform audio software

Audacity is an easy-to-use, multi-track audio editor and recorder for Windows, macOS, GNU/Linux and other operating systems. Audacity is free, open source software.

Latest version : 3.2.2

Audacity Posts

Audacity 3.2 is out now!
September 26, 2022 by Leo Wattenberg

Audacity 3.2.0 is a gigantic release, adding: VST3 support Realtime Effects support The ability to upload and share audio with our

GSoC 2022 – Work Product – Creating Fundamental Ruler and Waveform Display Options
September 11, 2022 by Michael Papadopoulos

Enhanced Ruler – GSoC 2022 Week 10

Get Involved

All are welcome to contribute to Audacity by helping us with code, documentation, translations, user support and by testing our latest code.
How to contribute?

Screenshot of obsspro[.]pw

Less Obvious Connections, Perhaps?

The Bleeping Computer study mentioned 11 open-source software they saw rogue Google search result pages for, namely:

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

We looked for domains containing their names plus the string ***download*** (e.g., ***7-zip + download***) to see how many were owned by their developers and if any of the typosquatters were malicious. Our search identified an additional 387 domains, 27 of which were confirmed malicious.

WHOIS record detail comparisons also showed that none of these web properties were owned by the developers of the imitated software. Note, however, that due to the fact that only seven of the 11 developers had unredacted WHOIS records, we weren't able to confirm the legitimacy of domain ownership for 7-Zip, Notepad++, Rufus, and VirtualBox.

Our IoC list expansion analysis led to the discovery of 822 digital properties—email addresses, IP addresses, and domains—that could be tied to the rogue software attack that used Google search ads as entry vectors. More notably, it allowed us to identify 36 malicious IP addresses and domains not in the original IoC list, some of which bore starkling resemblances to the IoCs.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Domains Identified as IoCs by Bleeping Computer

- 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

Sample Email-Connected Domains

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

Sample IP-Connected Domains

- 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

- ostreamview[.]website
- qobstreamsview[.]space
- searchlightinteractive[.]com
- silveralawjamaica[.]com
- sodartwater[.]com
- 01252022test2[.]com

Sample Malicious IP-Connected Domains

- 0nline-secure[.]com
- 1001-interactransfert-return[.]com
- 100141420210227810599991[.]com

Sample String-Connected Domains

- 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

Sample Brand-Connected Domains

- 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

Sample Malicious Brand-Connected Domains

- 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