Tracking Online Drug Dealers

Drug Dealers Using Social Media to Sell Illegal Narcotics

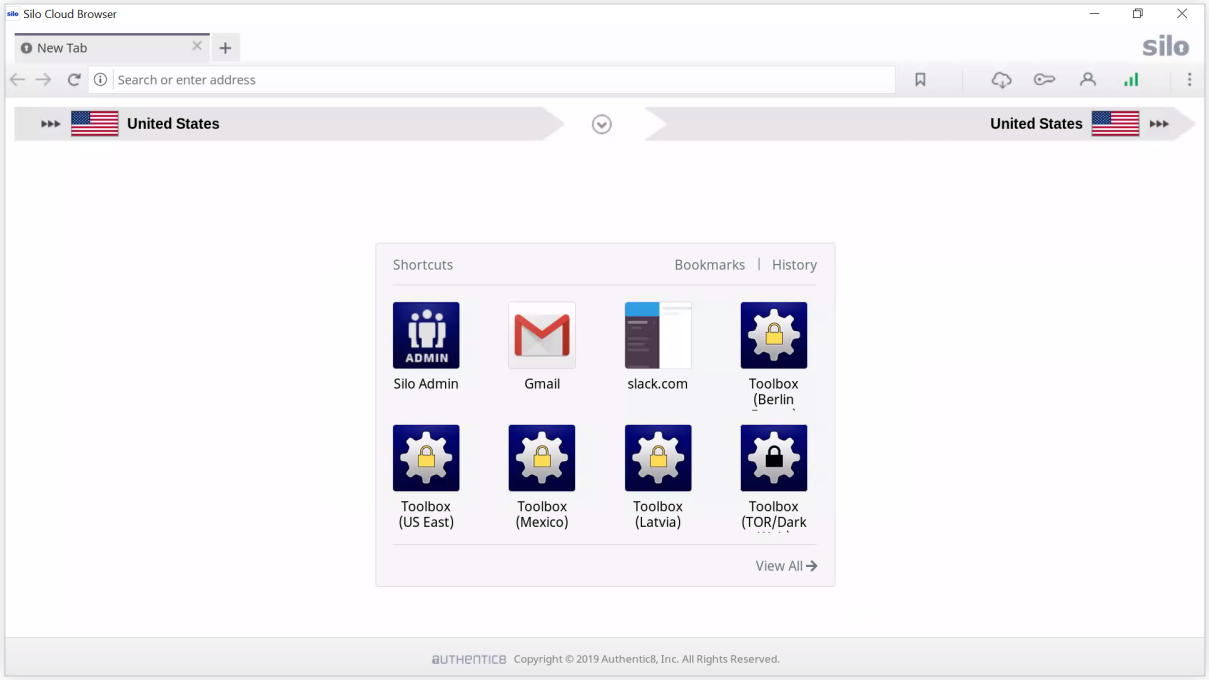
The rise in social media over the past ten years has led to drug dealers using various social media platforms to sell illegal narcotics on the open web. Investigators need a safe and anonymous browsing and research framework that allows them to investigate social media drug dealers without the risk of being identified or infecting their endpoint with malicious web code. This workflow will cover how the Silo Web Isolation Platform and managed attribution solution can be utilized to identify and investigate social media drug dealers anonymously.

Silo Web Isolation Platform

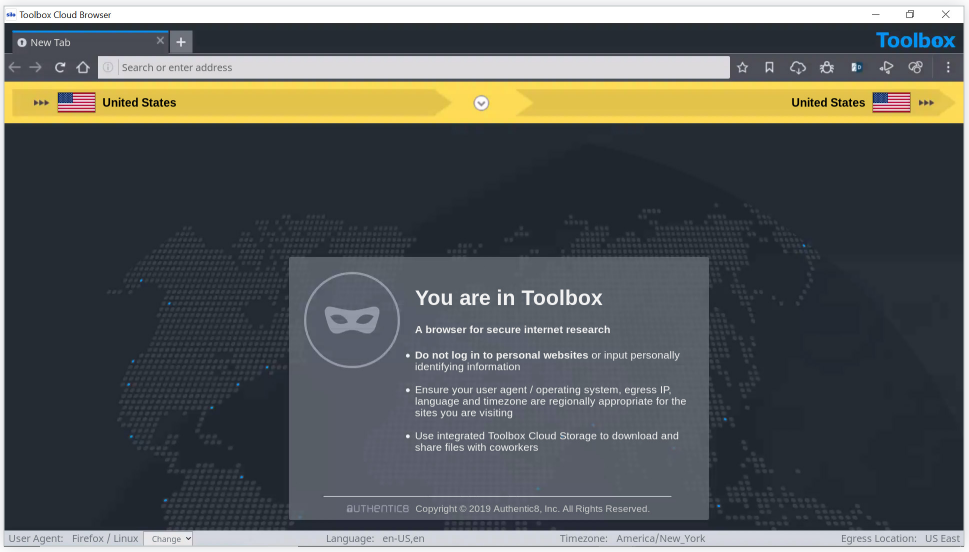
Silo for Research (Toolbox) is a secure and anonymous web browsing solution that enables users to conduct research, collect evidence and analyze data across the open, deep and dark web.

Silo for Research is built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

Research teams can accomplish their goals without introducing risk to the organization or revealing intent. All web activity is logged and encrypted so compliance teams can be sure that the tools are being used appropriately.



Silo for Research allows users to spoof IPs to over 30 locales worldwide, manipulate their hardware and software fingerprints, and to collect, annotate, and store internet-based publicly available information (PAI). It includes tools for post-fetch language translation, web-code and traffic analysis, and linkage tracking.

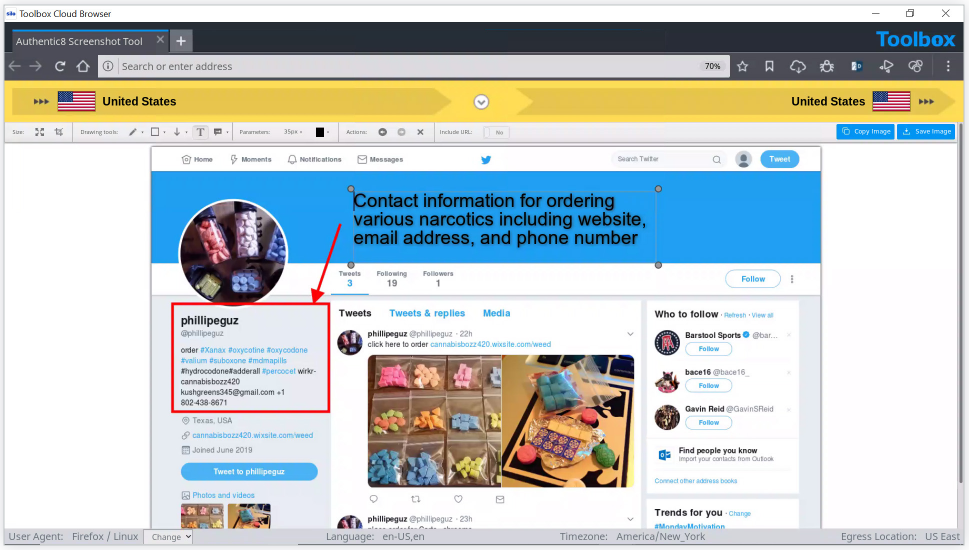


Identifying and Investigating Drug Dealers on Social Media with Silo for Research

The first step when conducting an investigation using Silo for Research is to select a regionally appropriate egress location and a user agent string that matches regional norms. This workflow will use the US and Google Chrome running on a Windows 10 machine as the user agent string. This process allows investigators to blend in as locals of that area.

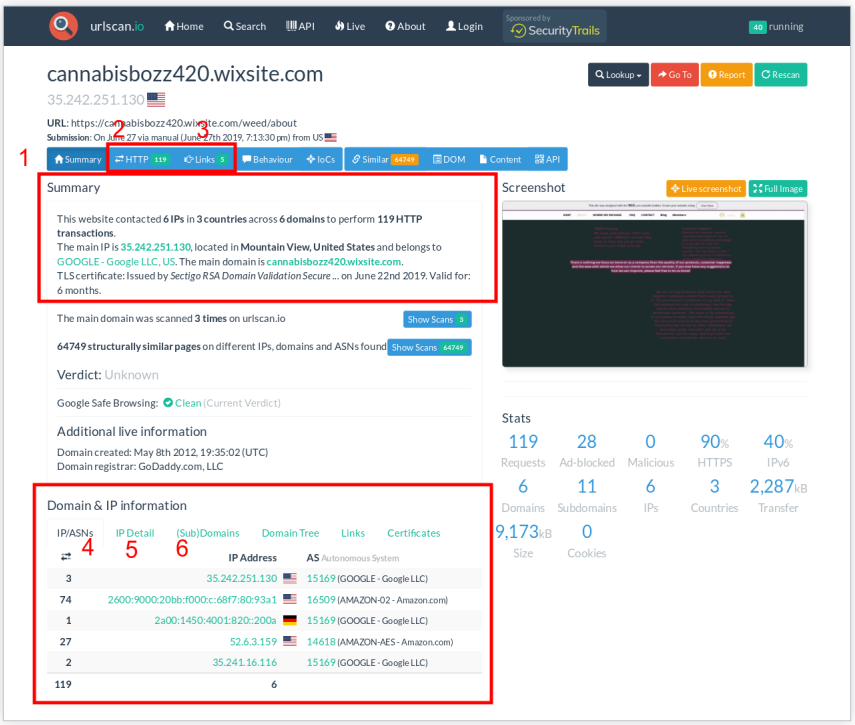
When conducting research on social media, there are various data capture tools included with Silo for Research that can be used for gathering intelligence. This first is a video download tool; this tool allows investigators to simply download any video currently playing on their screen to save as evidence. The second is a screenshot tool that gives investigators the ability to take a screenshot of an entire page. The screenshot tool also gives investigators the ability to edit the screenshot by including boxes, arrows, and text to highlight important information, as well as the ability to include the URL of where the screenshot was taken. This allows investigators to easily return to that page to gather additional intelligence.

By conducting a search on Twitter for #xanax, the Twitter user @phillipeguz was identified as an account using Twitter to market and sell illegal narcotics. Shown on this profile is information on how to place an order; the information listed includes a website, email address, and phone number. This information can now be run through additional search engines to possibly identify the owner of the account.



Resources for Site Ownership Research

WHOIS Records: WHOIS records provide top level domain information such as exact dates of registration, addresses, names, and phone numbers associated with the domain. Additionally, it provides web host information. @phillipeguz posted the website https://cannabisbozz420.wixsite.com/weed/about on their Twitter feed as a location to purchase the illegal narcotics. Using https://urlscan.io, a report was generated for this site.



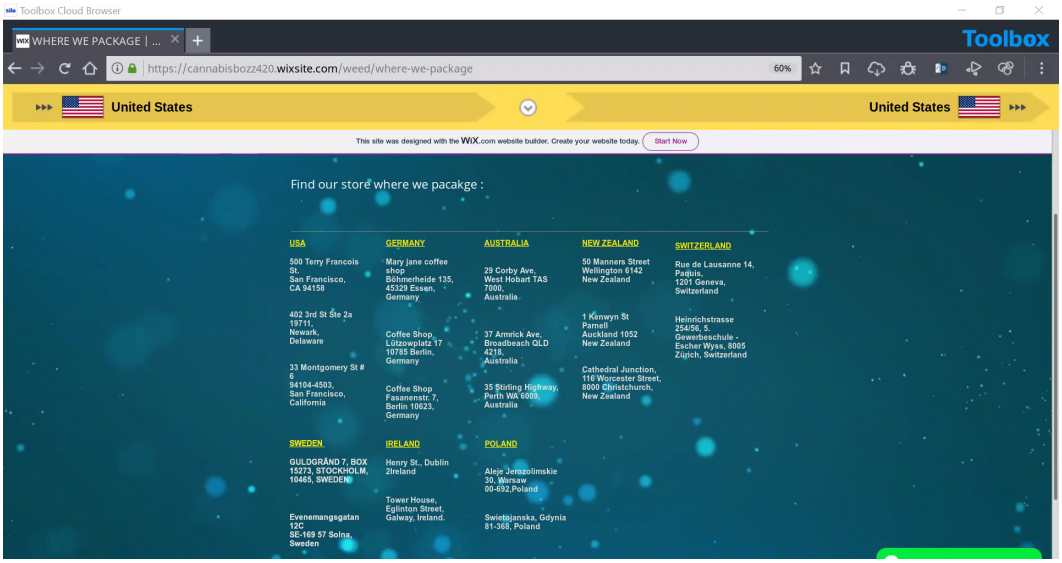
Breakdown of URLscan.io result panels:

1. “Summary” provides a top level summary of what country the site is hosted in.
2. “HTTP” details how many HTTP connections are made during initial load.
3. “Links” details what other sites are linked to on the main page.
4. “IP/ASN” details the IPs of everything used upon initial load and the geographic location as well as ASN.
5. “IP Detail” contains the exact city/state/country an IP address is assigned to, and redirects.
6. “(Sub)domains” identifies how many subdomains a top level domain contains.

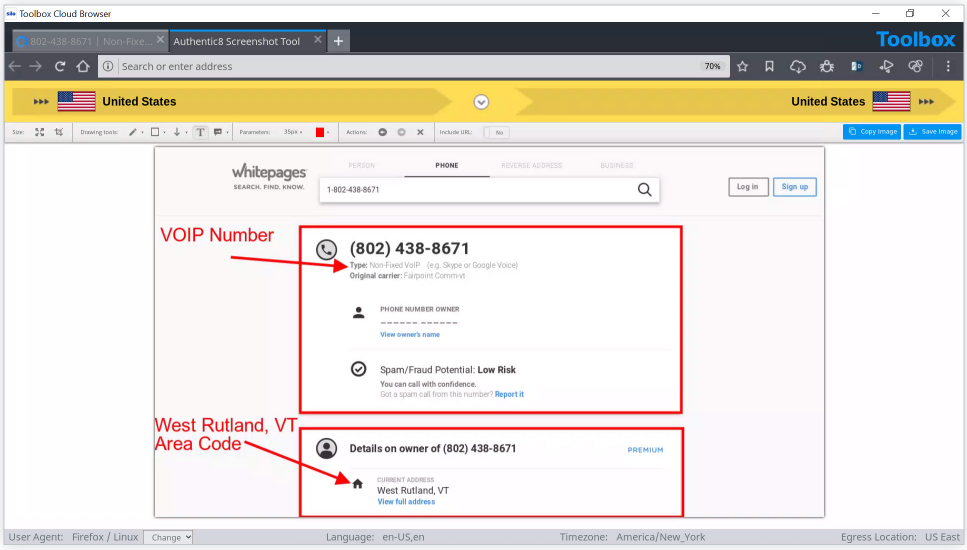
Example analysis of result panels:

According to the generated report, https://cannabisbozz420.wixsite.com/weed/about uses hosting primarily in the United States but also has hosting in Germany. This means that the distribution could also include locations outside the United States. On the website, the site owners also listed packaging locations in the United States, Germany, Australia, New Zealand, Switzerland, Sweden, Ireland, and Poland. The following screenshot from their website depicts their packaging locations around the world. It appears that the domain was registered by godaddy.com. This information could be used to send out a subpoena or court order to godaddy.com to find out who registered the domain with them.

Phone Number Reverse Lookup



The phone number 1+802-438-8671 was also listed as contact information for ordering narcotics from this Twitter page. Having this number available is extremely valuable for the investigation. The number can be run through a reverse phone number search engine to identify the subscriber information. The following screenshot is from a report generated by https://www.whitepages.com/phone/1-802-438-8671 for the listed phone number.

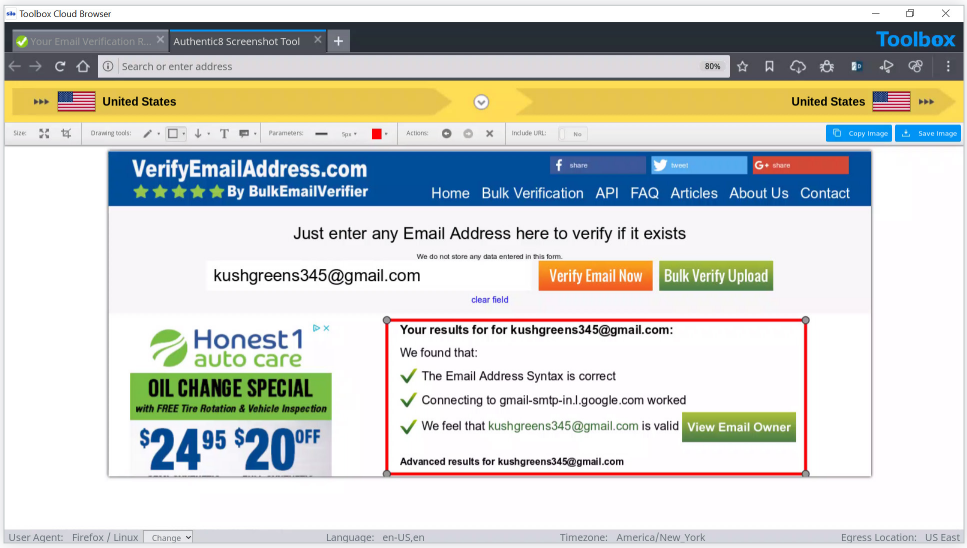


Example analysis of result panels:

Although there is no identity listed for the number and the number is associated with a voice over internet protocol (VoIP), there is some valuable information that can be pulled from the report. Seeing that the number has a Rutland, Vermont area code is telling: due to the website listing a packaging location on the East Coast, it is possible that the East Coast is their shipping HQ.

Searching for Additional Social Media Profiles by Email

The third piece of contact information listed on this Twitter page is the email address kushgreens345@gmail.com. Once a possible email address is identified for a target, it can be run through https://verifyemailaddress.com to verify that it is a legitimate email address. Once an email address is verified, a subpoena or court order can be sent to the email provider to identify who owns and operates that email address. The screenshot below depicts the results from https://verifyemailaddress.com for the email address kushgreens345@gmail.com, and it is in fact a legitimate email address.



Conclusion

With drug dealers increasingly utilizing social media to distribute illegal narcotics, investigators need a safe and anonymous method to investigate and capture social media data. This workflow covered how Silo for Research can be used by investigators to safely and anonymously investigate and capture data from social media drug dealers.

For more information, please contact osint@authentic8.com.

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.