

Tracking Online Drug Dealers

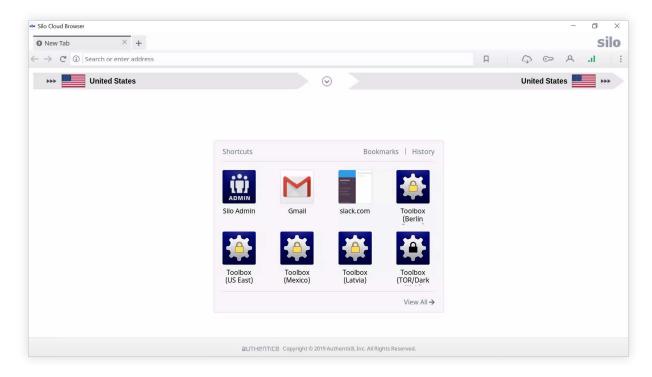


Drug Dealers Using Social Media to Sell Illegal Narcotics

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 web browser 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 Silo Research Toolbox, Authentic8's cloud browser and managed attribution solution, can be utilized to identify and investigate social media drug dealers anonymously.

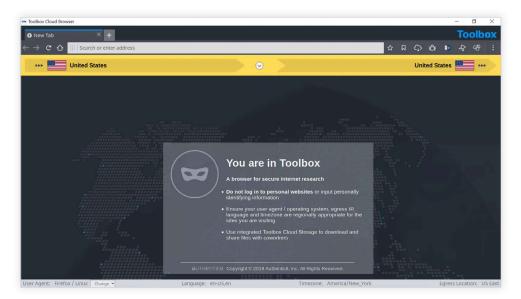
Silo Research Toolbox

Silo Cloud Browser is the foundation of Toolbox; it is a one-time-use browser built on-demand in a secure cloud-based container. All web code is rendered in the cloud and converted into a high-fidelity remote display of the session, protecting endpoints from malware, ransomware, and drive-by downloads. All web activity is logged. Privileges to upload/download and to access restricted URLs are policy controlled.





Silo Research Toolbox is a managed attribution and research suite layered over Silo. It 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.



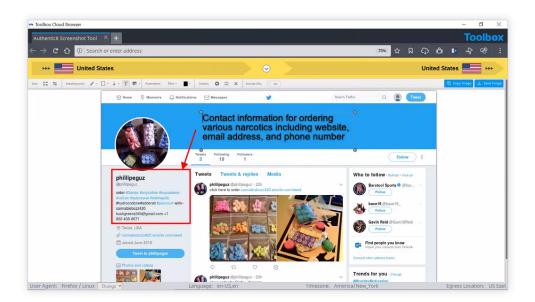
Identifying and Investigating Social Media Drug Dealers with Silo Research Toolbox

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

When conducting research on social media there are various data capture tools included with Toolbox 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 <u>https://cannabisbozz420.wixsite.</u> <u>com/weed/about</u> on their Twitter feed as a location to purchase the illegal narcotics. Using <u>https://urlscan.io</u>, a report was generated for this site.

	Iscan.io 🕈 Home 🔍 Search 🛄 API	🚯 Live 😯 About	💄 Login 🛛 🔗 Secu	irityTrails			40 running
35.242.2 URL: https://	bisbozz420.wixsite.com 51.130			QLoo	kup 🖌 🛹 Go	To Report	C Rescan
Submission: O	Une 27 via manual (June 27th 2019, 7:13:30 pm) from U		国DOM P Content 器A	PI			
Summary			Screensh	ot	*	Live screenshot	C Full Image
transactic The main GOOGLE	te contacted 61Ps in 3 countries across 6 domain ns. P1 § 3 5 242 251.130 , located in Mountain View , U -Google LLC, US. The main domain is cannabisbo cate: Issued by Sectigo RSA Domain Validation Sec	Jnited States and belongs zz420.wixsite.com.					
64749 stri Verdict:	domain was scanned 3 times on uriscan.io ucturally similar pages on different IPs, domains a Unknown		5 6 64749				
	fe Browsing: OClean (Current Verdict)		Stats				
	nal live information eated: May 8th 2012, 19:35:02 (UTC) gistrar: GoDaddy.com, LLC		119 Requests	28 Ad-blocked	0 Malicious	90 % HTTPS	40% IPv6
	gistrar: GoDaddy.com, LLC						
Domain re	IP information		6 Domains	11 Subdomains	6 IPs	3 Countries	2,287kE
Domain re	IP information IP Detail (Sub)Domains Domain Tree	E Links Certificate	Domains				
Domain re Domain & IP/ASNs	IP information IP Detail (Sub)Domains Domain Tree	Autonomous System	Domains 9,173kB	Subdomains O			
Domain re Domain & IP/ASNs 2	IP information IP Detail (Sub)Domains Domain Tree 5 6 IP Address AS	Autonomous System 169 (GOOGLE - Google LLC)	Domains 9,173kB Size	Subdomains O			
Domain re Domain & IP/ASNs 2 3	IP information IP Detail (Sub)Domains Domain Tree 5 6 IP Address AS 35.242.251.130 1 15	Autonomous System 169 (GOOGLE - Google LLC) 509 (AMAZON-02 - Amazon.c	Domains 9,173kB Size	Subdomains O			
Domain & Domain & IP/ASNs # 4 3 74	IP information IP Detail (Sub)Domains Domain Tree 5 6 IP Address AS 35 242 251.130 5 2400:900020bb:r000:.e867.8093a1 1 5 2400:1450.4001.820:200a 15	Autonomous System 169 (GOOGLE - Google LLC) 509 (AMAZON-02 - Amazon.c	es 9,173kB Size	Subdomains O			
Domain & Domain & IP/ASNs 2 3 74 1	IP information Opmains Domain Tree 5 6 IP Address AS 35:242:251:130 23 15 2400:0000:4677.8093a1 16 2400:1450:4001:B20:200a 15 52.6.3.159 14	Autonomous System 169 (GOOGLE - Google LLC) 509 (AMAZON-02 - Amazon.c 169 (GOOGLE - Google LLC)	es 9,173kB Size	Subdomains O			



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:

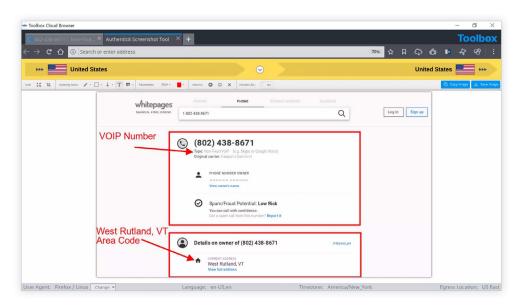
According to the generated report, <u>https://cannabisbozz420.wixsite.com/weed/about</u> uses hosting primarily in the United States but also has hosting in Germany. This means that the distribution could also include locations outside of the United States. When conducting further analysis on the website, the site owners listed packaging locations in the United States, Germany, Australia, New Zealand, Switzerland, Sweden, Ireland, and Poland. The following screenshot was taken from their website depicting their packaging locations around the world. When looking at who registered the domain 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.

see Toolbox Cloud Browser					- 8 ×							
WWX WHERE WE PACKAGE × +					Toolbox							
$\leftarrow \rightarrow \mathbf{C} \triangleq \mathbf{https://cannabisbozz420}$	wixsite.com/weed/where-we-package	60% 🏠		G & 🛤	-\$- 68 ÷							
+++ United States				United States								
This also was designed with the WDX even website budder. Oranle your website budder, C Batt Now												
0	Find our store where we pacakge :											
	USA GERMANY AUSTRALIA NEW ZEALAND SWITZERLAND											
	Soft Turns Franciso Mary Jane colfee So Cody Ave, stop So Mannes Steel Date de Lusance 14, seundon 614 Sub francisco, G A 54159 Expensive 103, Generary Note (Absart 74, Absart 104, Generary So Mannes Steel Date de Lusance 14, Note (Absart 74, So Mannes 14, So Mannes 14, Note (Absart 74, So Mannes 14, So Mannes 14, So Mannes 14, Note (Absart 74, So Mannes 14, So Mannes 14, Note (Absart 74, So Mannes 14, So											
	402 204 Sile 29 1971, Nevara, Coffee Shop, Sile 24 Distance of the Sile 24 Stransver, Coffee Shop, Sile 24 Stransver, Sile 24 31 Montgomery 26 & Germany Alternation 32 Montgomery 26 & Coffee Shop, Coffee Shop, Sile 24 Stransver, Sile 24 S											
	SWEDEN. IRELAND POLAND											
	GULOBAND 7, DOX 1973, STCOVCH annual Alaga Jenozolimske 1974, Svratovi Alaga Jenozolimske 29422 Postand Tomer House, Egintop Greet, Storens,											

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.





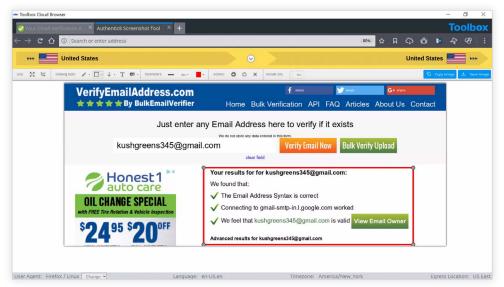
Example analysis of result panels:

Although there is no identity listed for the number and the number is listed as 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 very interesting 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 <u>kushgreens345@gmail.com</u>. Once a possible email address is identified for a target, it can be run through <u>https://verifyemailaddress.com</u> 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

<u>https://verifyemailaddress.com</u> for the email address <u>kushgreens345@gmail.com</u>, and it is in fact a legitimate email address.





Conclusion

With the increase of drug dealers 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 Research Toolbox can be used by investigators to safely and anonymously investigate and capture data from social media drug dealers.

For more information, please contact <u>osint@authentic8.com</u>.

ABOUT AUTHENTIC8

Authentic8 is redefining how enterprises conduct business on the web with the Silo web isolation platform. Silo insulates and isolates all web data and code execution from user endpoints, providing powerful, proactive security while giving users full, interactive access to the web. Silo also embeds security, identity, and data policies directly into browser sessions, giving IT complete control over how the web is used. Commercial enterprises and public sector organizations use Silo solutions to provide secure web access, to control web data, apps, and workflows, and to conduct sensitive online research. Try Silo now at <u>www.authentic8.com</u>.