Identity Under Attack: How Generative AI is Fueling Cybercrime-as-a-Service



Ashish Jain

Chief Technology Officer

Twitter: @AshishJa1n

identiverse[,]





Identity Evolution



Web-based cross-domain Single Sign-On

2001: Liberty Alliance

Frameworks for Federation, Assurance and Governance

2008: OpenID 1.0/ Information Cards

User-centric Identity Dynamic Trust Model

> 2010 OAuth Standard for Access Delegation

2023: Passkeys

202X:

DID

Verifiable Credentials

Mobile Wallets

PKI based passwordless portable authentication

2018: FIDO: WebAuthn

PKI based Strong Authentication

2012: OpenIDConnect

Authentication protocol on top of OAuth 2.0



Good vs Bad Actor?





Friction for "good users"



Defense for "bad users"



The Threat Is Evolving — And Accelerating



Headless browsers used to automate HTTP requests

1997: cURL

And other tools to script HTTP requests

2010s: Proxy Services

Gain popularity as websites implement anti-bot measures

2017: Puppeteer

A popular tool that executes JS & automates complex tasks

2023: CaaS is Mainstream

Solutions like EvilProxy remove barriers to entry

2018: Stealth Plugins

Allow attackers to avoid detection at scale



Identity-as-a-Service (IDaaS)





Attacker Evasion Techniques



Cybercrime-as-a-Service (CaaS)

🗰 🖌 Home / Bots												
21 Bots						Extended Search Q						
Enabled	⊙ I	Resource name / URL O Without Resource	all Resources total		\$ Price							
boa			min	max	mix	max						
🕑 🖂 FormParser	☑ 🛛 SavedLogins	☑ ⊕ InjectScript			o 💼 o	nly Sale						
Bot Name			Bot OS		Fingerp	rints (browsers)						
Bot name			Win		min	Forderite						
	💆 Last I	Update	🝽 Bot Country		IP		Ë	Available Services & Prices	Account Balan	ce: 3600		C Root
from yyyy-mm-dd	from y	ryyy-mm-dd	Any country		• 95.123	A conferente						
to yyyy-mm-dd	to yyy	y-mm-dd					~					
							(Q Search for				
						② Dashboard	>					_
	≅ ~	RESOURCES KNOWN / OTHER			<u>.</u>	Campaign URLs	~	Bundle	Entry Scopes	Data Collected	Price	
Filter bot name	Any	Filter resource name/domain: paypal,e	bay.com,hotmail.com			Create Campaign				. Login	10 days 1508	
	^ଭ				🖂 0 🗔 170 💬 0 - 17	All Compained			cubucomo ora		10 days - 1505	statements in the local division in the loca
5BB0CD12867AD0290C53CF6DCC4593EE	BitcoinDE NiceHash	Facebook instagram		G Google		All Campaigns		rubygems	rubygenis.org	 passworu session cookies 	20 days - 2005	and the second se
₩ 2022-03-31 00:59:23 Ø 2022-04-04 19:26:29	KuColn Binance	Steam AppleStore		 Blockchain Wordpress 		🚯 Proxy Groups	>			V Session Cookies	10 days - 4003	
	V Twitter	Amazon		Adobe	known 7	E Drovy Sequert		••	drophox com	✓ login	10 days - 1505	and have been
	com.oneschat.germany		com.textmeinc.textme		other 10	E PIOXy Servers	-	dropbox	diopbox.com		20 days - 2005	and a second second
	* ~ ~ ~ ~				⊡0 □ 138 ⊕0 = 13	密 Sessions				< login	10 days - 4003	
06B574C2699A7E69777716DD4B7A5C0D	& SonyEntertainm WishStore	Pinterest		Spotify PayPal		Captured Data Log		0	vandex ni		20 days - 2505	the last last
₩ 2022-04-04 18:35:32 Ø 2022-04-04 19:26:29	T-mobile	Google		Ebay Raiffeisenbank		@ captaled bata Log		X yandex	yandex.ru	 password session cookies 	31 days - 400\$	the second se
	NvidiaStore com.netflix.mediaclient	MediaMarkt	192.168.8.1	Cffic	known 3.	🖏 Cookies Log					10 days - 150\$	
	M. 					∩ Notifications		and under	vahoo com		20 days - 250\$	and the second second
	Werrenger	E Live		Learne offerend-	⊡1 □ 103 ⊕0 = 10			y. yanoo	Junoo.com	 session cookies 	31 days - 400\$	
80070EF9004C2AAE0A88645220388F97	Spotify PavPal	Skype		Steam NvidiaStore		💈 Guides			xbox com		0. uuju - 4000	
2022-04-04 14:12:03 ⑦ 2022-04-04 19:26:29	N Netflix	C EANetwork		Google	known 2				skype com			
	com.discord tv.twitch.android.app		com.instagram.android		other 7				onenote.com			
	© « ₽₽₽₽				C2 C 100 CD - 40				office.com	✓ login	10 days - 150\$	Courses in succession in succession
FFF938453AD1FA9855F116D4DD06FF37	Kickstarter	USPS		Immobilienscout24	C2 M 109 TO = 19			microsoft	microsoftonline.com	✓ password	20 days - 250\$	
# 2022.04.04 12:11:25	& SonyEntertainm G Google	Ebay BBahn		Booking					microsoft.com	✓ session cookies	31 days - 400\$	
2022-04-04 19:26:29	DHL Expedia	& Sony		Facebook	known 4				Bive.com			
	berlinreport.com	2*	checkers.storynex		other 14				bing.com			
						contacts:	-			✓ login	10 days - 150\$	
						https://t	me	/ wilnrovy	google.com	✓ password	20 days - 250\$	1000 Inter 1000
						incepsi//t	·····e	/ comproxy		✓ session cookies	31 days - 400\$	
										✓ login	10 days - 150\$	
								6 facabaak	facebook com	< nassword	20 days - 250\$	1700 Jame 1 400



#identiverse



• Volumetric (e.g. Credential Stuffing)

Low and Slow (e.g. pig butchering)



Fraudster Tools

Goll Abort	Site: Switch Site: Progress:	0%	- [] >					
Settings General HTTP Header Proxy Settings	Site Settings Timeout (s): 30 Bot relaunch delay Combo Settings	y (s): 0 Resolve Hostname	Save automatically "To Check" combos Save automatically "To Check" combos Annoying sound on Hit ->	anycapto	cha© ■ info@anycaptcha.com		API Document Success avg: 99.03%	User Dashboard User Dashboard Orime avg: 35,524.37 ms
Fake Settings Keywords	Minimum Length: 6 Letters Digits Forbidden Chars: Lowercase and Uppercase Le <email> filter: Must Be Email</email>	Maximum Length: 8 Maximum Length: 8 Alphanumeric - Email Allowed Chars: Etter and Digit Special Character Pr	Popup Memo containing Hit debug information Minimize to Tray Float Statistics in Progression Detect "network lost" conditions while bruteforcing ogression updates: 0	Automatic captch Fastest & cheapes 99% uptime Pay as you go Cheapest price on the p	a solving service st Easy i Resolv market	ntegration ve 10,000+ captchas/minute m your captcha if the budge	FRI IMAGETOTEXT Auto Detect Pick an image to dem Pick an image to dem Results after solving v	EE TRIAL
<> Code	⊙ Issues 126 îî Pull re ⁹ master → î' 5 branches	equests (•) Actions [11] Pr	ojects 🖽 Wiki 🔃 Security 🗠 Insights Go to file Cc	Services & Pricing Our solution RECAPTCHA V2	Pricing	🐨 Speed	≁ Success avg	Pay per usage Package
<> Code ۴	Issues 126 12 Pull re master P master P 5 branches openbullet Re-enabled Keep-re	equests (•) Actions (*) Pr (•) 27 tags Alive header	ojects 🖽 Wiki 🔅 Security 🗠 Insights Go to file Co b43b166 5 days ago 🕥 1,718 corr	Services & Pricing Our solution RECAPTCHA V2 Google Inc RECAPTCHA V3 Google Inc	 Pricing \$ 0.55/1000 requests \$ 0.55/1000 requests 	☞ Speed 28.0 s 11.0 s	Success avg 98%	Pay per usage Packages
<> Code	 Issues 126 11 Pull re master - 12 5 branches openbullet Re-enabled Keep-re .github Announcements 	equests (c) Actions (II) Pr (c) 27 tags Alive header Update bug-report.yaml Update native.md	ojects III Wiki ③ Security ⊻ Insights Go to file Cc b43b166 5 days ago ③ 1,718 corr 2 months 2 months	Services & Pricing	 Pricing \$ 0.55/1000 requests \$ 0.55/1000 requests \$ 0.7/1000 requests 	 ✓ Speed 28.0 s 11.0 s 10.7 s 	 Success avg 98% 98% 99% 	Pay per usage Packages
<> Code	 Issues 126 11 Pull re master - 12 5 branches openbullet Re-enabled Keep-re .github Announcements Changelog 	equests	ojects III Wiki ③ Security ⊠ Insights Go to file Cc b43b166 5 days ago ③ 1,718 corr 2 months 2 months 19 days	Services & Pricing	 Pricing \$ 0.55/1000 requests \$ 0.55/1000 requests \$ 0.7/1000 requests \$ 0.5/1000 requests 	☞ Speed 28.0 s 11.0 s 10.7 s 1 s	 Success avg 98% 98% 99% 99% 	Pay per usage Packages
<> Code	 Issues 126 11 Pull re master - 12 5 branches openbullet Re-enabled Keep- .github Announcements Changelog OpenBullet2.Console OpenBullet2.Core 	equests Actions 27 tags Alive header Update bug-report.yaml Update native.md Update native.md Preparation for 0.1.26 Updated to latest Captchate Fixed a bug when obtaining	ojects III Wiki ① Security ⊻ Insights Go to file Cc b43b166 5 days ago ③ 1,718 corr 2 months 2 months 19 days Sharp last m	Services & Pricing	 Pricing \$ 0.55/1000 requests \$ 0.55/1000 requests \$ 0.7/1000 requests \$ 0.7/1000 requests \$ 0.5/1000 requests \$ 0.5/1000 requests 	 ✓ Speed 28.0 s 11.0 s 10.7 s 1 s 0.1 s 	✓ Success avg 98% 98% 98% 99% 99% 295% Commit >100K tokens/day (Support 24/7)	Pay per usage Package
<> Code	 Issues 126 11 Pull re master - 12 5 branches openbullet Re-enabled Keep- .github Announcements Changelog OpenBullet2.Console OpenBullet2.Core OpenBullet2.Native 	equests Actions Pr 27 tags Alive header Update bug-report.yaml Update native.md Update native.md Update to latest Captchas Fixed a bug when obtaining Added console helper	ojects II Wiki I Security ⊻ Insights Go to file CC b43b166 5 days ago I,718 corr 2 months 2 months 19 days Sharp last m g hits last m	Services & Pricing	 Pricing \$ 0.55/1000 requests \$ 0.55/1000 requests \$ 0.7/1000 requests \$ 0.5/1000 requests \$ 0.5/1000 requests \$ 5000-\$10,000/month Private APIs(contact us) \$ 3/1000 requests 	☞ Speed 28.0 s 11.0 s 10.7 s 1 s 0.1 s 0.1 s	 Success avg 98% 98% 99% 99% 99% 00K tokens/day (Support 24/7) 100% 	Pay per usage Package

Volumetric Attacks





4:22



f 🗾 in 🖂

 \leftarrow

By **Bill Toulas**



Outdoor apparel brand 'The North Face' was targeted in a large-scale credential stuffing attack that has resulted in the hacking of 194,905 accounts on the thenorthface.com

		Bloomb
1PUTER	≡	
		Technology

...

PayPal Gets Stung by 'Bad Actors,' Shuts 4.5 Million Accounts

Shares plummet as payments firm abandons goal for new accounts

bloomberg.com

Bot farms took advantage of sign-up rewards, company says



John Rainey Source: Bloomberg

By Jennifer Surane +Follow February 2, 2022 at 6:44 AM PST

Get unlimited access today.

 \sim



SPORTS

 \equiv

Teen charged with hacking DraftKings bragged 'fraud is fun,' feds say

PUBLISHED THU, MAY 18 2023 11:33 AM EDT UPDATED THU, MAY 18 2023 9:20 PM EDT

Dan ManganJessica Golden@_DANMANGAN@JGOLDEN5

WATCH LIVE

KEY POINTS

- Federal prosecutors in New York announced criminal charges against an 18-year-old Wisconsin man for a scheme to hack user accounts of the sports betting site DraftKings.
- Joseph Garrison is accused of working with others to steal about \$600,000 from approximately 1,600 victim accounts during the November 2022 attack.



10:39 • cybernews.com

affiliate commissions.

Home » Editorial

Bots ruin everything: how Taylor Swift concert made us compete against non-humans

Updated on: 21 February 2023 🛛 📿





\sim	website uses cookies. By	continuina to use this
Chat	GPT Best Practices	\triangleright >
tay Ah dge LL	ead of the Competition With Ch .M Technology.	atGPT and Other Cutting-
ataiku		Download

Social Engineering Attacks

3:57



SUBSCRIBE FOR \$1/WEEK

>

Retirees Are Losing Their Life Savings to Romance Scams. Here's What to Know.

Con artists are using dating sites to prey on lonely people, particularly older ones, in a pattern that accelerated during the isolation of the pandemic, federal data show.

Give this article



Unlimited access to all of The Times. \$6.25 \$1 a week for your first year.



cbsnews.com

Û

60 MINUTES OVERTIME >

What it sounds like to be targeted by the grandparent scam







Q

Sex, Dating & Relationships Relationships

Woman loses \$450,000 in 'pig butchering' romance scam

Last month, the Department of Justice seized over \$112 million linked to pig butchering.

By Anna lovine on May 11, 2023

f 🎔 🖬



4:13 forbes.com \equiv Forbes Subscribe Sign In

Toyota Parts Supplier Hit By \$37 Million Email Scam

Lee Mathews Senior Contributor ()

Observing, pondering, and writing about tech. Generally in that order.

Sep 6, 2019, 01:06pm EDT

C This article is more than 3 years old.

The Toyota Boshoku Corporation, a major supplier of Toyota auto parts, reported some distressing news this week. Fraudsters fleeced the company via an email scam to the tune of about ¥ 4 billion (JPY). That works out to just over \$37 million at today's exchange rate.



Toyota Boshoku Asia тоуота возноки

ADVERTISEMENT



Generative AI impact on Identity

4:33		.⊪ ≎ ∎,	4:35
	arstechnica.com	Û	
	ars TECHNICA		DJIA 1.00%
(Θ)	PRIUS	ALE VONO ZEF Voltagen, for more taking to but of the grant part to but of the grant part to but of the grant part	PERSONAL

Microsoft's new AI can simulate anyone's voice with 3 seconds of audio

6	<u>Benj Edwards</u>	•	01/9/2023 10:15 pm	•	Biz & IT
	View non-Al	ИР	version at arstechnica	.co	m



	∎wsj.	com	Û
DJIA 1.00% 🔺	S&P 500 1.30% ▲	Nasdaq 2.19% 🔺	U.S. 10 Yr 3
\equiv	WS	SJ	

.... 🗢 🔳

PERSONAL TECHNOLOGY: JOANNA STERN I Cloned Myself With

AI. She Fooled My Bank and My Family.

Our columnist replaced herself with Al voice and video to see how humanlike the tech can be. The results were eerie.





f 🄰 🖂

4:50

Scammers now using chatbots to fool people, steal personal info and money

■ wcpo.com

Chatbot comes across as a real human



Scammers are now using AI chat to fool people into thinking they are speaking with a real person, and get money and personal info out of them.

		ADVERTISEMENT		
\leftarrow	\rightarrow	+	:)	

4:46	'II S	•
● bloom	berg.com	
Bloomberg	Subscribe	≡

Newsletter

Watch Now

Al Deep Fake of the Pope's Puffy Coat Shows the Power of the Human Mind



A fake image of Pope Francis generated by AI (left); a real photo of Pope Francis (right). Source: r/midjourney via Reddit.com created using Midjourney v5; photographer: Grzegorz Galazka/Mondadori Portfolio via Getty Images

By Drake Bennett +Follow April 6, 2023 at 4:00 AM PDT

	🖙 Copy Link
You're Reading Tech Dally	-



How can generative AI be used for cybercrime



Generative AI can potentially be used for cybercrime in several ways:

0 6 7

- Phishing: Generative AI can be used to create highly convincing phishing emails or messages that mimic the style of legitimate organizations or individuals, tricking users into providing sensitive information.
- 2. Deepfakes: AI can generate very realistic audio and video content, creating a 'deepfake' of a real person. This could be used for fraud, impersonation, or disinformation campaigns.
- 3. Bypassing CAPTCHA: Generative models can be trained to solve CAPTCHA challenges, potentially allowing automated systems to bypass security meant to prevent bots.
- 4. Fake News: Al can generate plausible-sounding but false articles or posts, which can be used to spread misinformation or propaganda.
- 5. Malware: Advanced AI systems could potentially be used to create sophisticated malware or to identify vulnerabilities in software systems for exploitation.



How do you protect?

$\circ~$ Help with Evolution / Education

• Strong Active Authentication e.g. passkeys

• Passive Authentication / Risk Signals



Passive and Continuous Authentication

dentiverse



Passive and Continuous Authentication



Device Fingerprinting

Behavior Biometrics



II.s





Mouse Motions

Keypress

Touch Screen Interactions Fidentiverse



Risk Signals of Fraudulent Activity

Device Intelligence	Browser Spoofing	OS spoofing	Behavioral Biometrics	Email Intelligence
Assess the fingerprint received against known valid signature	Look for abnormal usage of outdated or obsolete browsers	Look for abnormal usage of outdated or obsolete Operating Systems	Assess how the user interacts with the challenge	Evaluate the syntax of the email address and the domain used
IP Intelligence & Reputation	Headless	Known Bots	User Behavior	САРТСНА
aneputation	Browsers	and Automation	Analysis	Farms

Good vs Bad Actor?





Friction for "good users"



Defense for "bad users"



THANK YOU!

Ashish Jain Twitter: @AshishJa1n



