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

Ashish Jain

Chief Technology Officer

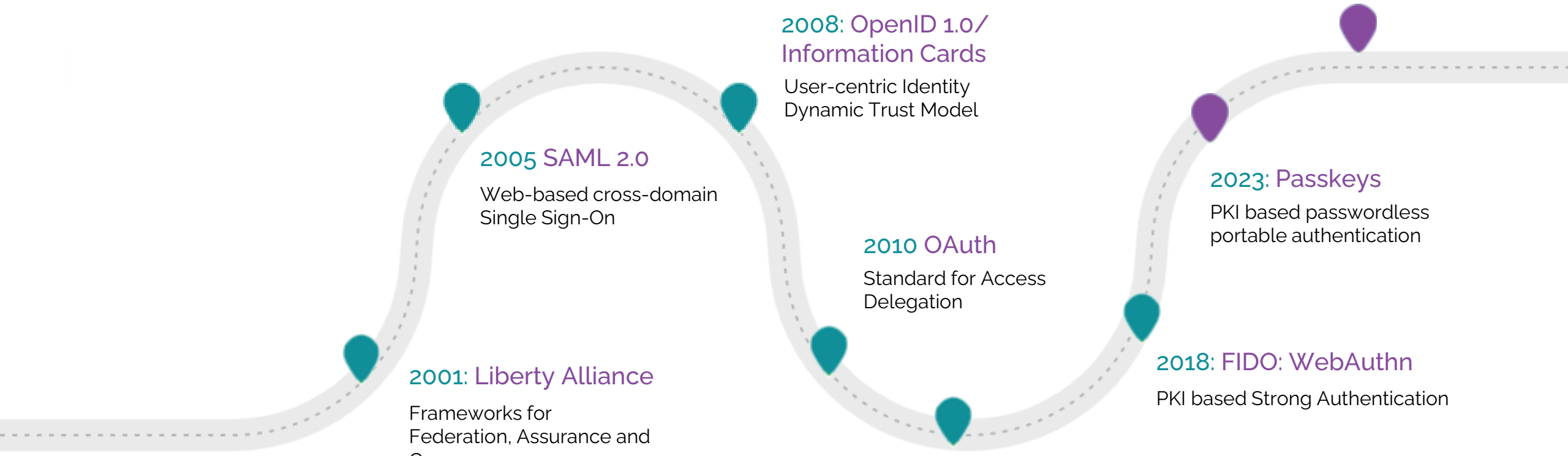
Arkose Labs

Twitter: @AshishJa1n

identiverse

#identiverse

Identity Evolution



2001: Liberty Alliance

Frameworks for Federation, Assurance and Governance

2005 SAML 2.0

Web-based cross-domain Single Sign-On

2008: OpenID 1.0/ Information Cards

User-centric Identity
Dynamic Trust Model

2010 OAuth

Standard for Access Delegation

2012: OpenIDConnect

Authentication protocol on top of OAuth 2.0

2018: FIDO: WebAuthn

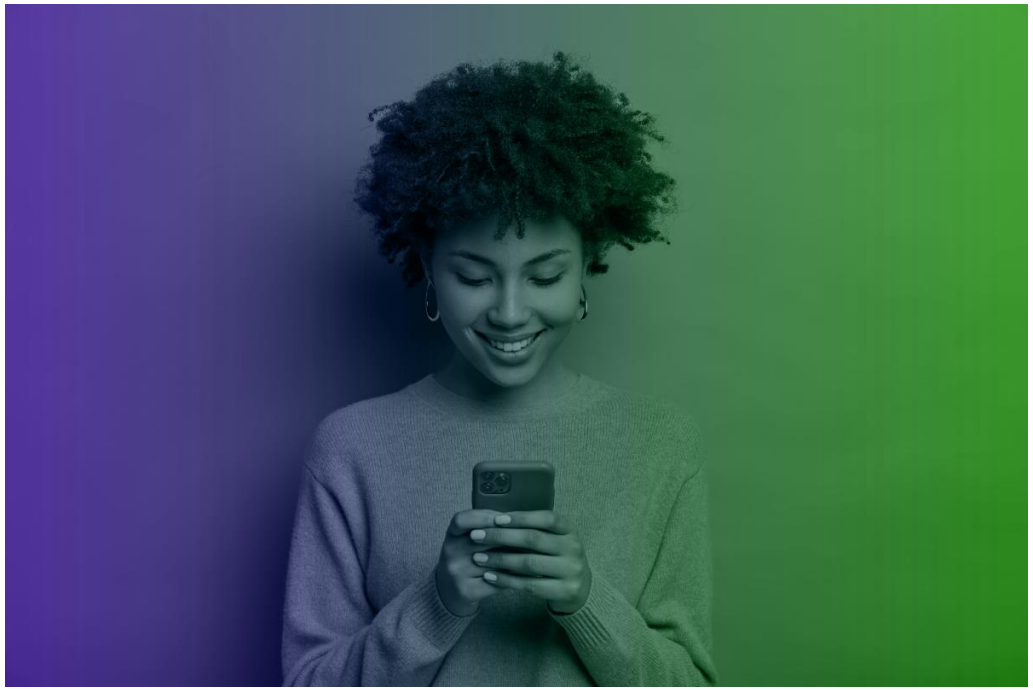
PKI based Strong Authentication

2023: Passkeys

PKI based passwordless portable authentication

202X:
Verifiable Credentials
DID
Mobile Wallets

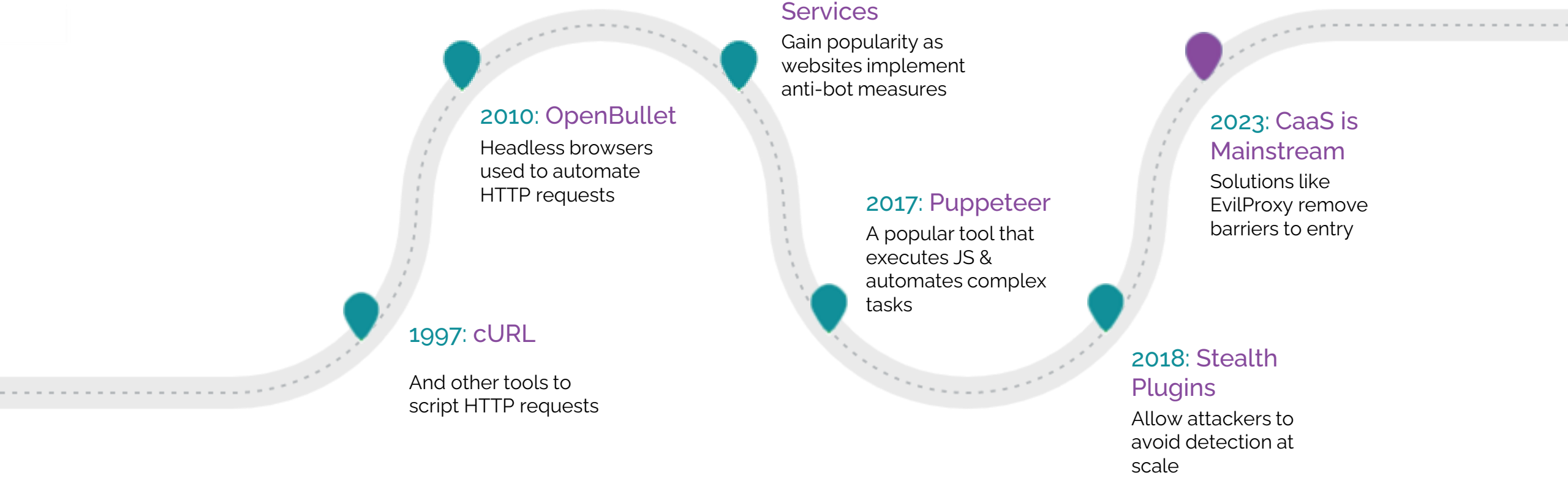
Good vs Bad Actor?



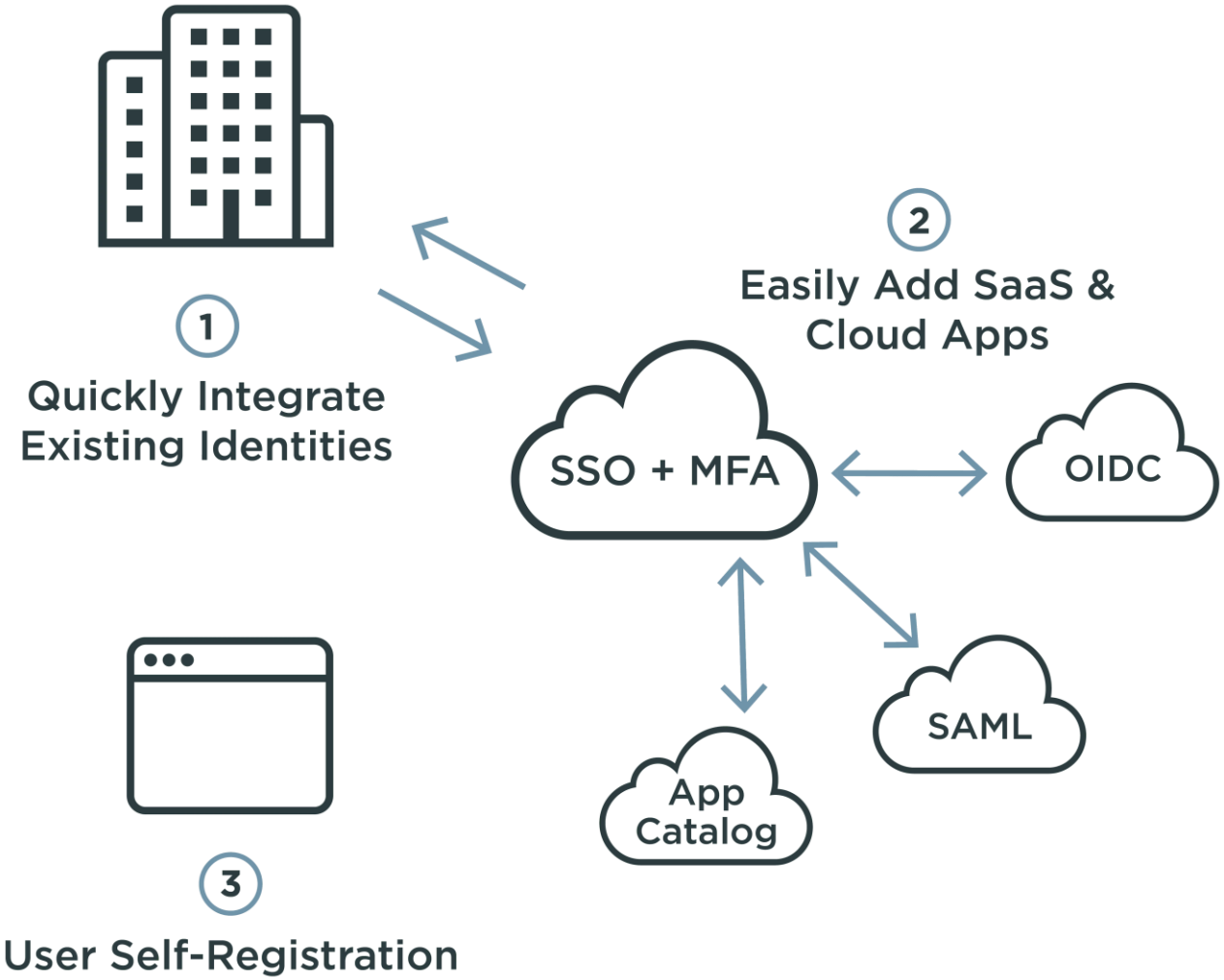
Friction for “good users”

Defense for “bad users”

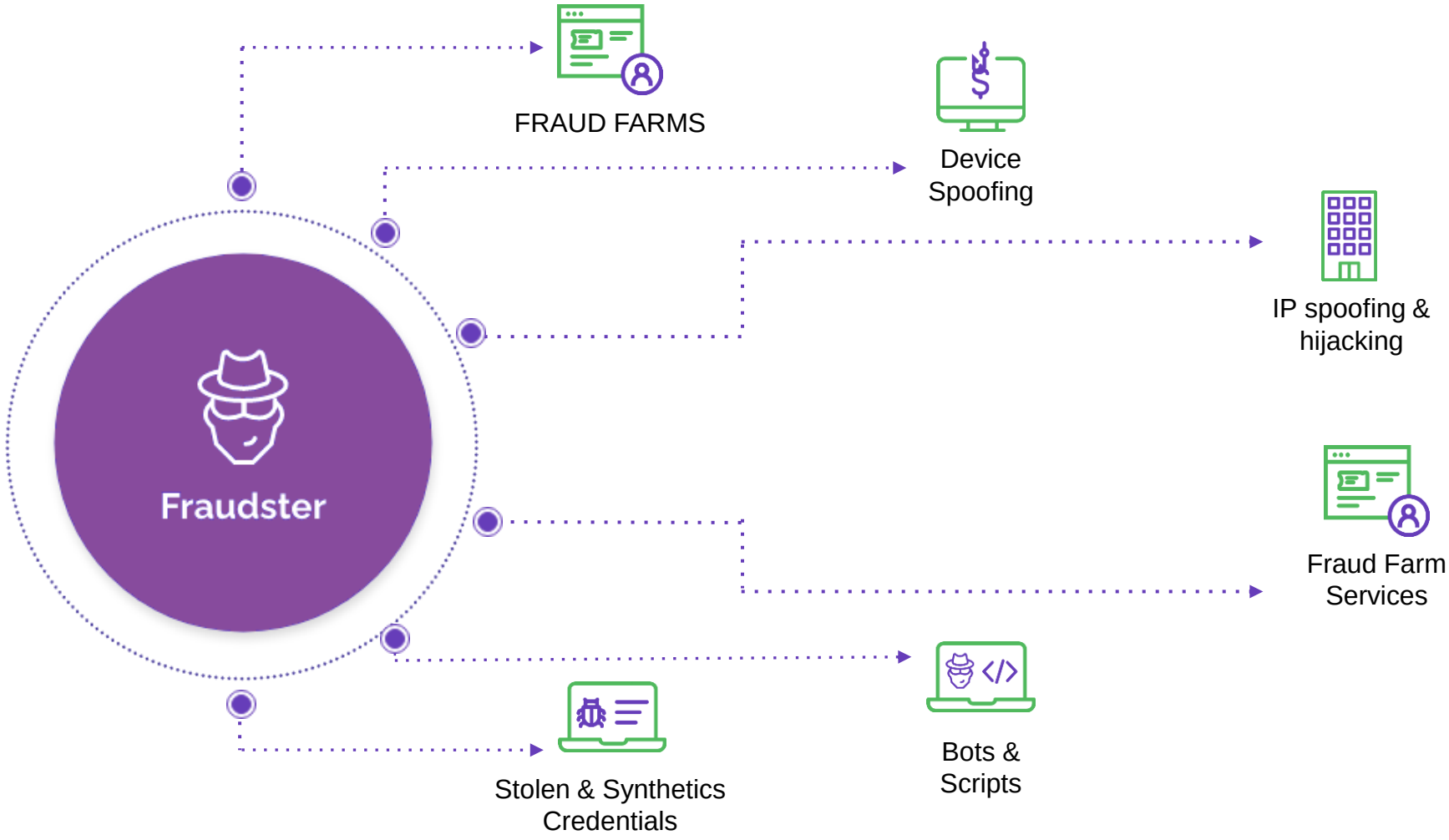
The Threat Is Evolving — And Accelerating



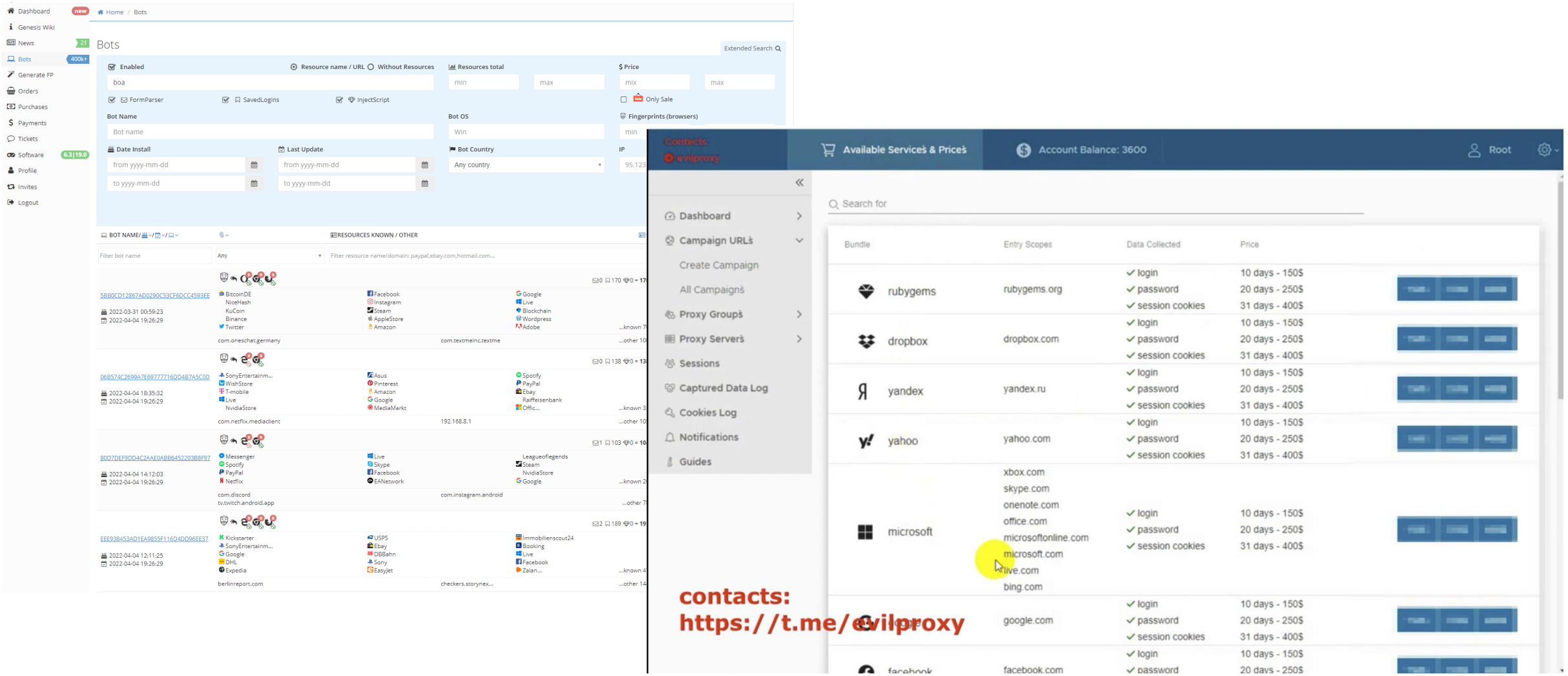
Identity-as-a-Service (IDaaS)



Attacker Evasion Techniques



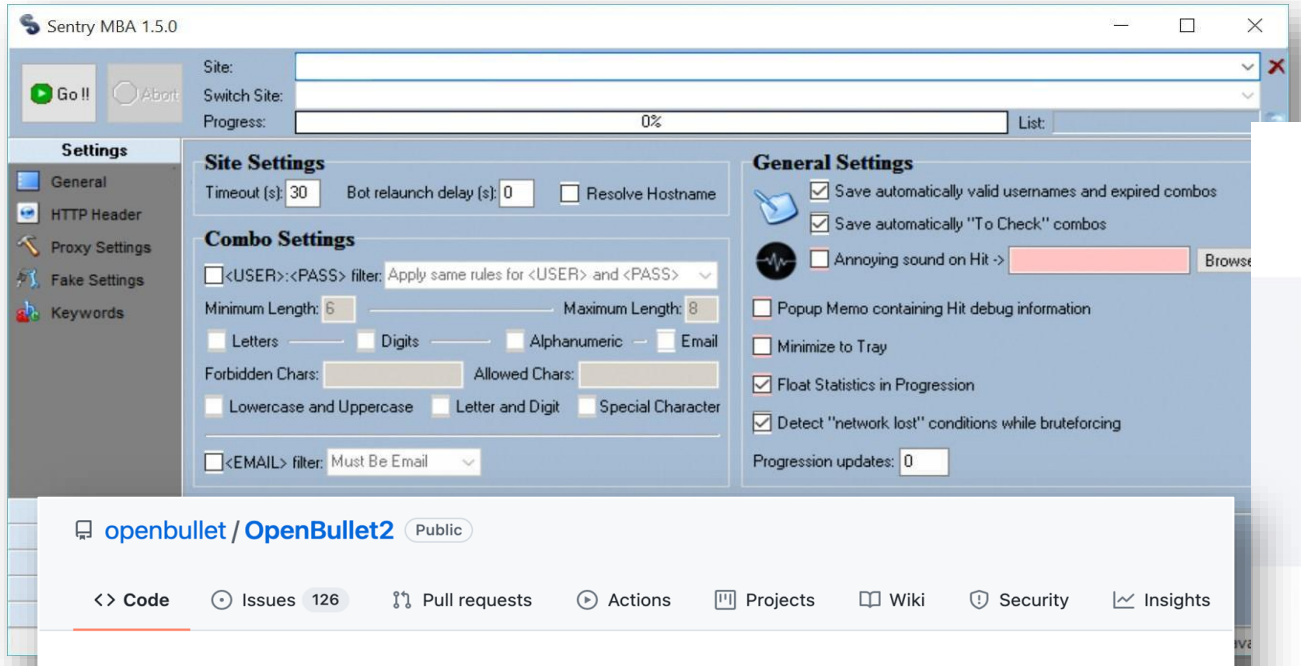
Cybercrime-as-a-Service (CaaS)

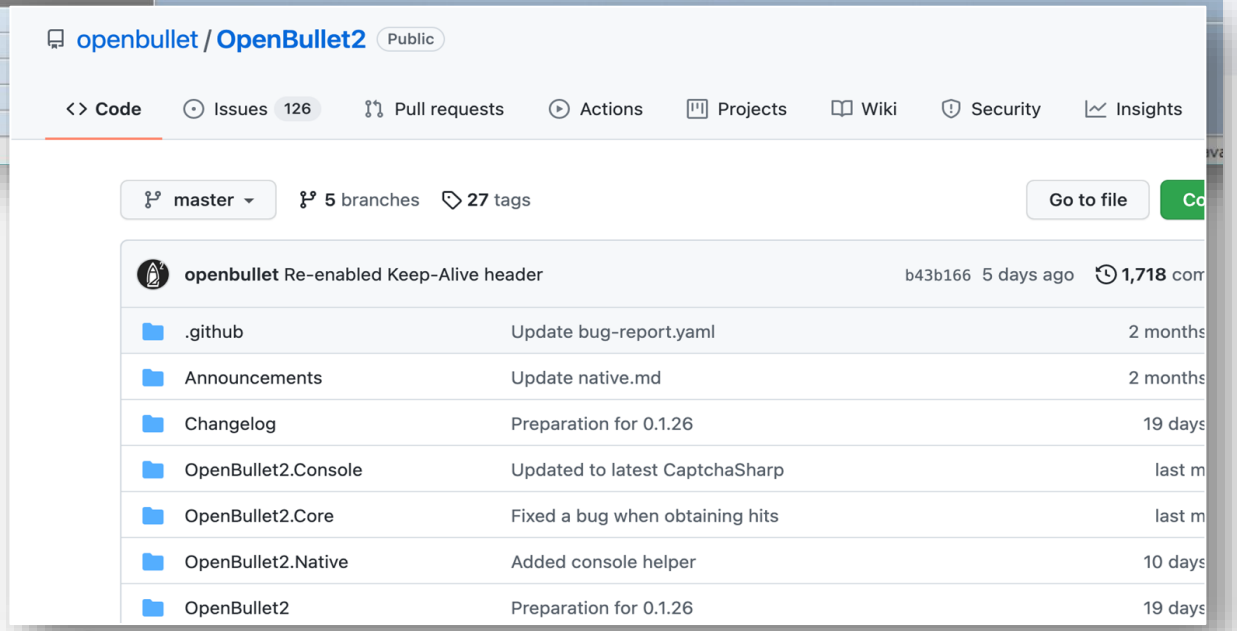


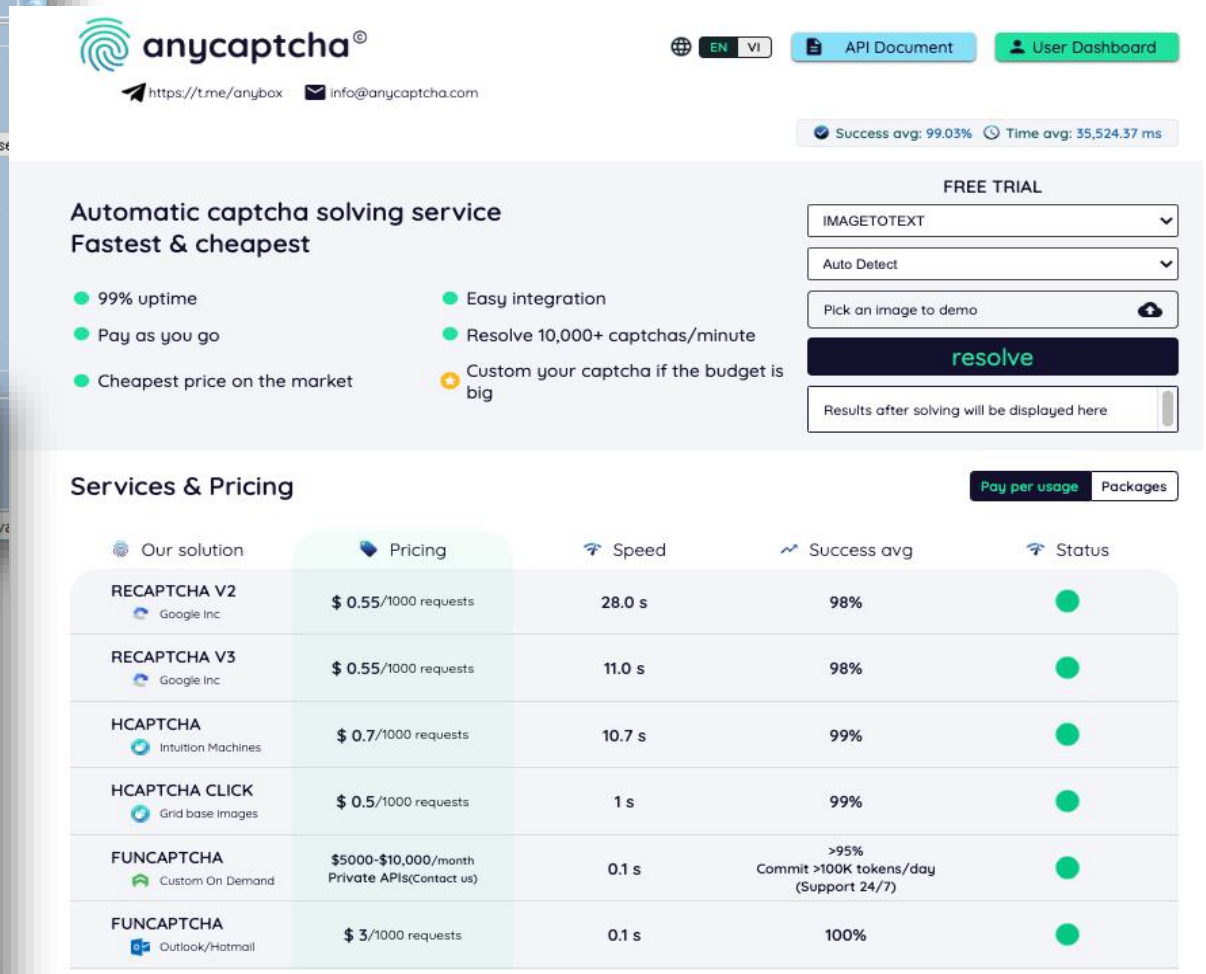
Attack Types

- Volumetric (e.g. Credential Stuffing)
- Low and Slow (e.g. pig butchering)

Fraudster Tools







Volumetric Attacks

3:49

bleepingcomputer.com

BLEEPINGCOMPUTER

200,000 North Face accounts hacked in credential stuffing attack

By Bill Toulas

September 7, 2022 10:40 AM

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

4:22

bloomberg.com

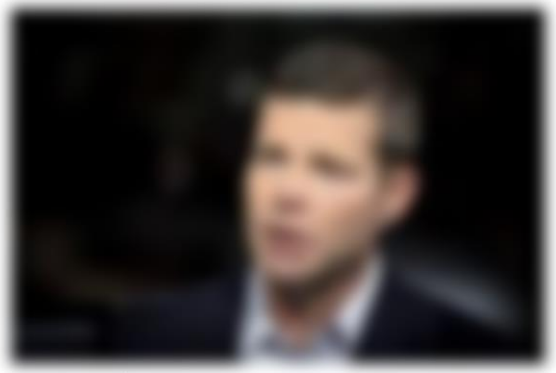
Bloomberg Subscribe

Subscriber Only

Technology

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

- Shares plummet as payments firm abandons goal for new accounts
- 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.

10:38

cnbc.com

CNBC WATCH LIVE

SPORTS

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 Mangan @_DANMANGAN | Jessica Golden @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.

CNBC Business News and Finance VIEW IN APP

10:39

cybernews.com

cybernews®

If you purchase via links on our site, we may receive **affiliate commissions**.

Home » Editorial

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

Updated on: 21 February 2023

Anna Zhadan, Contributor

website uses cookies. By continuing to use this

Social Engineering Attacks

3:56

nytimes.com

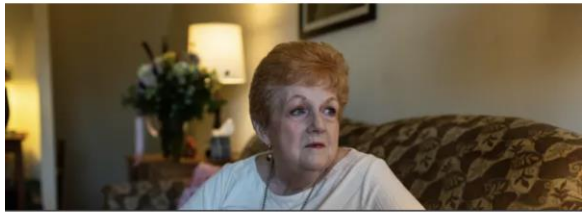
The New York Times

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 | Read in app



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

3:57

cbsnews.com

Debt Ceiling Deal | Memorial Day Honors | Bu

CBS NEWS | Login

60 MINUTES OVERTIME ›

What it sounds like to be targeted by the grandparent scam

BY KEITH ZUBROW
MAY 21, 2023 / 7:00 PM / CBS NEWS

3:58

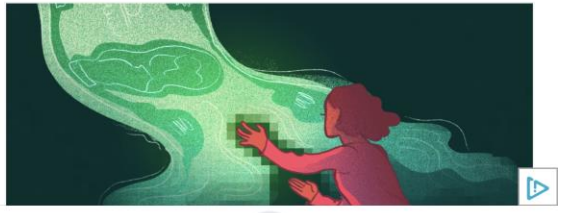
mashable.com

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 Iovine on May 11, 2023



4:13

forbes.com

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

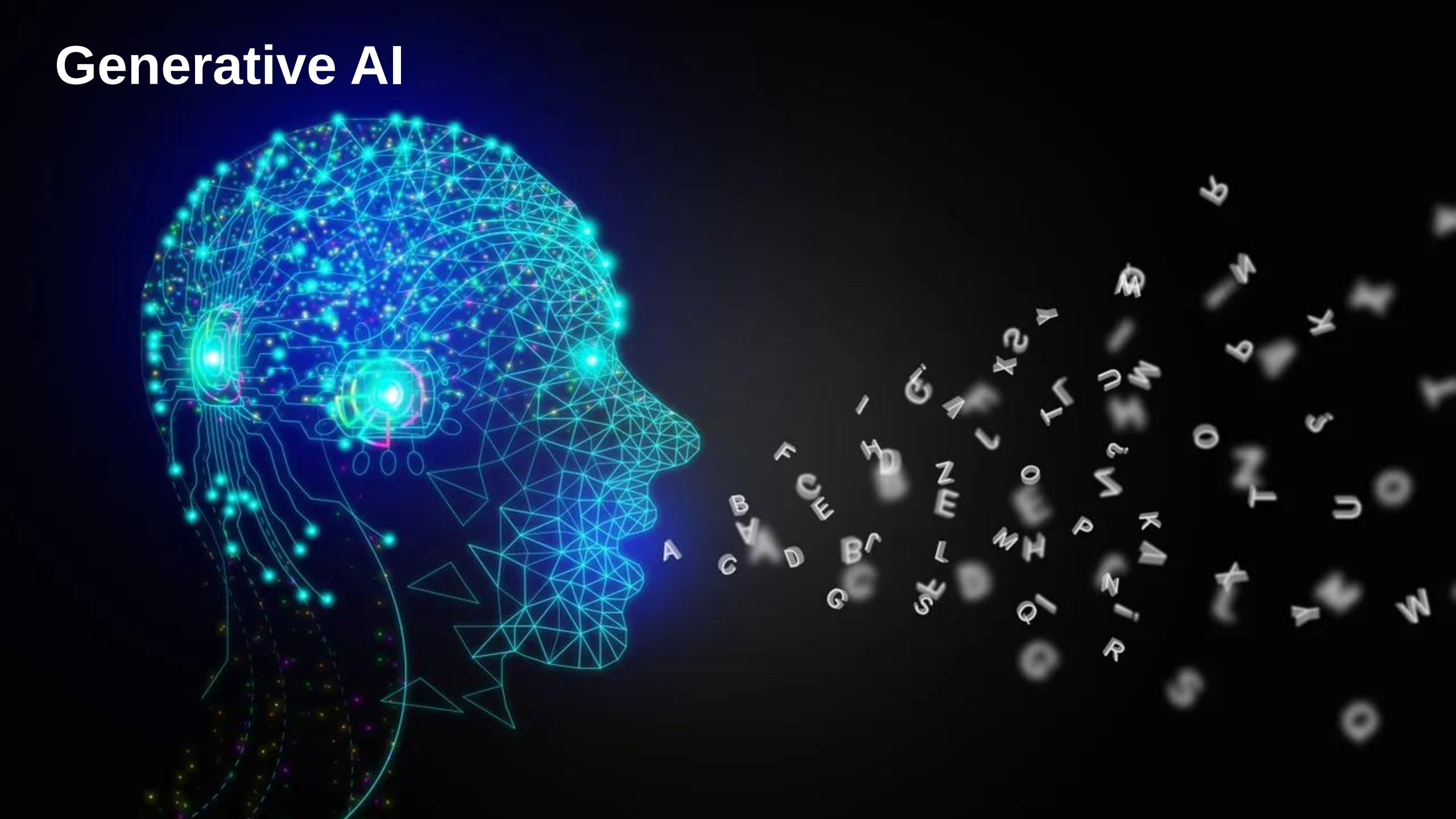
This article is more than 3 years old.

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 TOYOTA BOSHOKU

ADVERTISEMENT

Generative AI



Generative AI impact on Identity

4:33

arstechnica.com

ars TECHNICA

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

Benj Edwards • 01/9/2023 10:15 pm • Biz & IT

View non-AMP version at arstechnica.com

4:35

wsj.com

DJIA 1.00% ▲ S&P 500 1.30% ▲ Nasdaq 2.19% ▲ U.S. 10 Yr 3.80

WSJ

PERSONAL TECHNOLOGY: JOANNA STERN

I Cloned Myself With AI. She Fooled My Bank and My Family.

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

By Joanna Stern Follow

Updated April 28, 2023 at 7:58 am ET

4:50

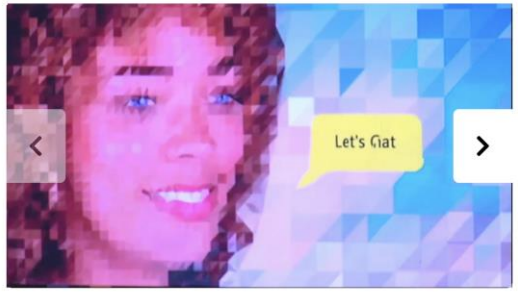
wcpo.com

9 CINCINNATI

Watch Now

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

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.

CLOSE

ADVERTISEMENT

By John Matarese

4:46

bloomberg.com

Bloomberg Subscribe

Newsletter

AI 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 Daily.

Model: GPT-4 (Mobile, V2)

How can generative AI be used for cybercrime

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

1. 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: AI 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?

- Help with Evolution / Education
- Strong Active Authentication e.g. passkeys
- Passive Authentication / Risk Signals

Passive and Continuous Authentication

IP

- Known TOR exit node
- Proxy Service
- Data Center
- High Abuse Velocity
- VPN
- Part of Botnet Service

Email

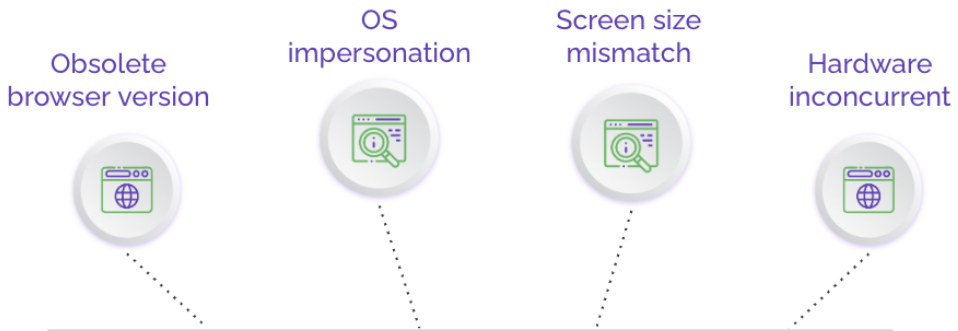
- Email Longevity
- Email Frequency
- Email Enumeration
- Email Tumbling
- Email Formation Issues
- Domain Intelligence

Phone

- Name Address Match
- VOIP
- Subscriber Status
- Porting History
- Activation Length
- Pre-paid vs post-paid

Passive and Continuous Authentication

Device Fingerprinting

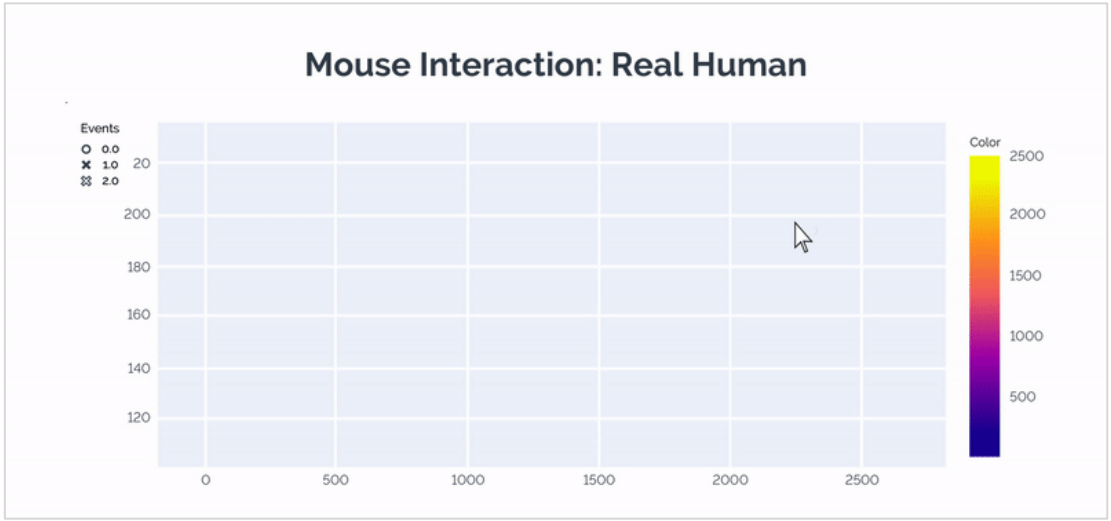


There was heavy randomization. The common signature only amount to this:

`Win32::false::true::*::*::1::1::1::1::0::0::0::F70CA`

- Hardware concurrency: `[-1, 24, 32]`
- Color depth: `[1, 2, 4, 6, 8, 12, 16, 20]`
- OS + OS version: `[Windows10, Windows8.1]`
- Screen size: `1920x1080x1920x1052, 1440x900x1440x900, 1280x800x1280x760, 1920x1080x1920x1040, 1280x1024x1280x984` + 19 more values
- Browser + browser version: `Chrome86.0.4240.75, Chrome90.0.4430.93, Chrome89.0.4389.114, Yandex Browser21.3.0, Opera76.0.4017.94` + 27 more values
- CFP: `414114541, 990181253, 1038645234, -1519429487, 334050401` + 21 more values

Behavior Biometrics



Mouse Motions

Keypress

Touch Screen Interactions

Risk Signals of Fraudulent Activity

Device Intelligence

Assess the fingerprint received against known valid signature

Browser Spoofing

Look for abnormal usage of outdated or obsolete browsers

OS spoofing

Look for abnormal usage of outdated or obsolete Operating Systems

Behavioral Biometrics

Assess how the user interacts with the challenge

Email Intelligence

Evaluate the syntax of the email address and the domain used

IP Intelligence & Reputation

Evaluate the user's IP geolocation, network, and reputation

Headless Browsers

Detect botnets that leverage headless browsers frameworks

Known Bots and Automation

Identify known good bots like search engine and SEO

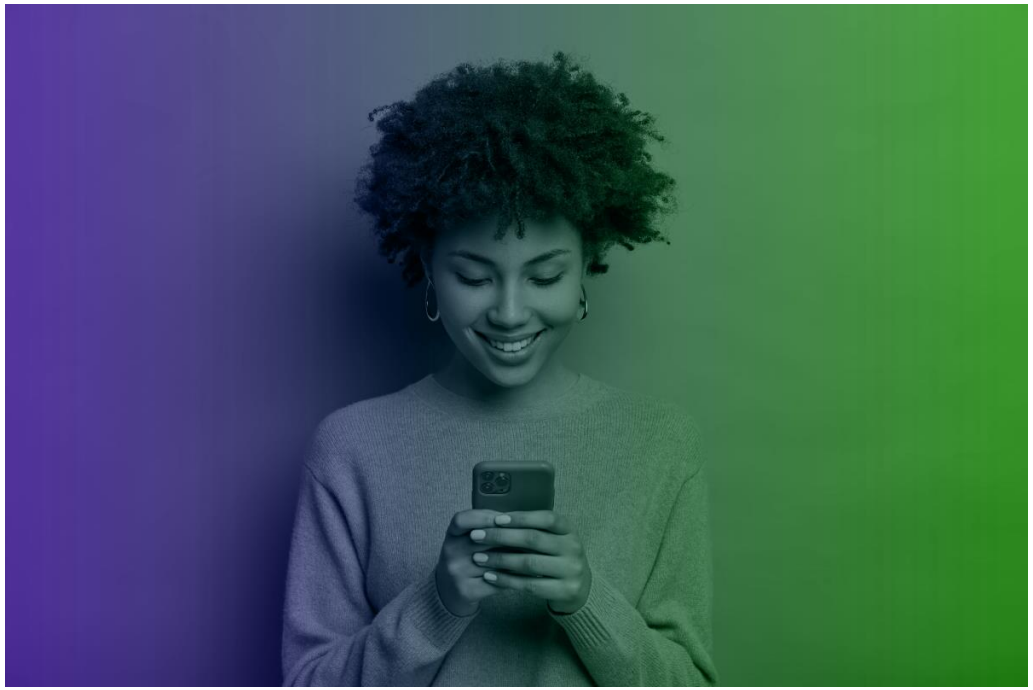
User Behavior Analysis

Detect clients sending requests with high velocity

CAPTCHA Farms

Detect captcha solving services (aka fraud farms)

Good vs Bad Actor?



Friction for “good users”

Defense for “bad users”

THANK YOU!

Ashish Jain

Twitter: @AshishJa1n

identiverse

#identiverse