The GenAI-Fueled Threat Landscape

A Dark Web Report by the Transmit Security Research Lab

Executive Summary

Months after OpenAI released ChatGPT in late 2022, blackhat AI platforms such as FraudGPT were discovered on the dark web. These services increase the volume, velocity and variety of attacks by providing subscription-based access to generative AI services without the content restrictions of their legitimate counterparts.

In this report, we present trends that the Transmit Security Research Lab observed on the dark web following the advent of generative AI (GenAI) and the impact of these trends on customer identity security. More importantly, we present what you can do to mitigate the new breed of threats — from malicious code to deepfakes — fueled by GenAI.

Impact of GenAI on the fraud landscape

Volume	Velocity	Variety
The number of threats and fraud in the wild has more than tripled	Threats and fraud occur at breakneck speeds	Many variants: customized, targeted & modified

Now you need ML and GenAI tools to fight back

Key Findings

1	Generative AI services accelerate the sale of enterprises' validated consumer accounts on the dark web by helping fraudsters locate vulnerabilities, create configuration (config) files, scale attacks and perform other tasks.
2	Tools built on top of GenAI automate pentesting, which expedites and simplifies corporate reconnaissance (recon) on enterprise vulnerabilities and provides step-by-step instructions for getting around security layers.
3	Configs used to validate accounts sell for anywhere from $6-400 USD, with high-end configs capable of validating up to 500 user credentials per minute and include as many as 1000 high-end proxies.
4	Blackhat AI services are bundled with Remote Desktop Protocols (RDPs), credit card checkers and other tools to streamline the creation of attacks, enhance their impact and evade detection. These tools can be purchased with custom features for $2200 or with the source code for $428.
5	Real or synthetic data can be quickly generated with GenAI to create phony accounts that are difficult to detect. Accounts may be aged with 8+ years of order history to make them appear legitimate.
6	The creation of fake IDs that allow fraudsters to pass step-up challenges is also aided by the use of GenAI tools, which make fake IDs harder to detect and enable fraudsters to circumvent liveness checks.
7	Video and voice deepfakes are being used to lure more victims to fall for scams. And in call centers, voice cloning is being used to dupe voice authentication systems.
8	24/7 escrow services and verified purchase reviews are commonly provided alongside dark web products. Seller ratings are as high as 4.99/5 stars — assuring purchasers the products work as advertised.

Recommendations

To protect against these the growing volume, velocity and variety of highly-deceptive threats, enterprise identity, security and fraud teams should do the following:

1	Deploy phishing-resistant credentials and risk-based authentication to dynamically administer step-ups based on anomalies in individual user behavior. Additionally, as GenAI tools facilitate vulnerability scanning, security gaps in strong authentication methods such as passkeys should be protected across their entire lifecycle.
2	Introduce fraud solutions that replace static rules and algorithms with context-aware AI-driven services capable of detecting new and emerging MOs (modus operandi), paired with orchestration tools that can improve risk and trust decisioning and accelerate the creation of new security rules.
3	Leverage offline analysis tools to help analysts quickly identify and take action on fraud rings and large-scale attacks. New GenAI analytics can immediately spot trends, anomalies and weak points, making sense of event logs and large datasets.
4	Expand and consolidate detection to include a broader range of detection methods in order to prevent fraud & scams. Customer identity and access management (CIAM) should be unified with anti-fraud and identity verification to remove data silos, security gaps and complexity that hinder protection from evasive threats and fraud.
5	Implement risk-aware identity verification that utilizes threat intelligence to improve the detection of today's sophisticated fake IDs and presentation attacks. Due to an expected increase in account reset fraud, identity verification should be an integral part of securing the full customer identity lifecycle.
6	Employ an AI-based identity-first approach to securing APIs used for registration, logins and transactions, allowing teams to see the connection between fraud and the API-based attacks that often enable them.
7	Deploy fraud detection that checks for strong indicators of automated tools like OpenBullet, by checking IP/proxy reputation, device reputation and behavioral anomalies.

Part I: GenAI Threat Innovation

Dark web intelligence and consumer fraud

In 2023, data breaches set a new yearly record. This comes as no surprise, but what is astonishing is that even for enterprises that haven't suffered a recent breach, mass quantities of their customers' accounts are for sale at this moment on the dark web.

The sale of compromised accounts is big business for fraudsters, and the dark web provides easy access through a supply chain of multiple threat actors who gather information and craft specialized attack tools custom-made to evade the protections of their targets, with accounts from large, global brands yielding the best return on investment.

Now, with the advent of blackhat AI tools, such as WormGTP and DarkBARD, GenAI helps fraudsters identify vulnerabilities, write attacks that exploit these vulnerabilities, use tools to automate attacks and other tasks.

A complex and evolving ecosystem

Fraudsters on the dark web are far from homogenous; instead, they can be thought of as a complex ecosystem of users, each with their own area of speciality. With regard to stolen accounts, these threat actors can be broadly divided into three key personas.

Supply chain: Specialized fraudsters use technical skills or social engineering to gain corporate recon on enterprise vulnerabilities, security layers, and the data that is collected on users to develop config files, malware and other tools.

Fraud tools: Other fraudsters purchase and operate tools sold on the dark web to compromise customer accounts or create fraudulent new accounts. This often includes using specific config files, alongside automation tools like OpenBullet to quickly validate user credentials or scrape credit card data.

Monetization: The third type of fraudsters buys stolen credentials or cookies to take over accounts and then transfers money to fraudulent accounts, often cashing out via fintech apps. Alternatively, they purchase retail goods using account credits or credit card data sold on the dark web.

Read the full report

and see screenshots of fraud activity on the dark web