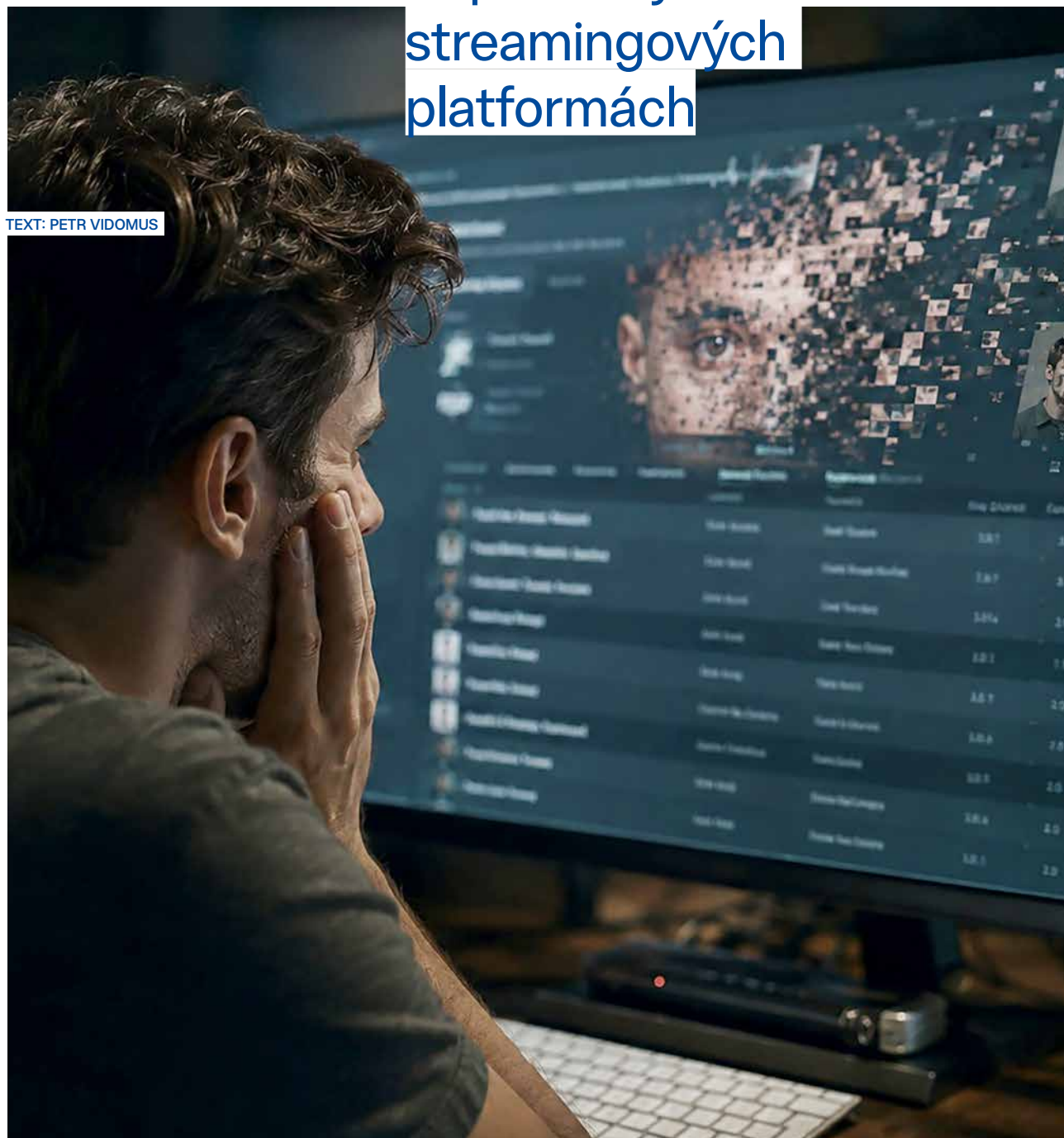


TOHLE JSEM OPRAVDU NEPSAL JÁ

AI podvody na
streamingových
platformách

TEXT: PETR VIDOMUS



**Ukrást identitu hudebníka
nebylo nikdy snazší.
Stačí k tomu průměrný
AI agent a znalost trhlin
v systémech Spotify.
Zatímco se platformy
chlubí miliardovými
zisky, tvůrci bojují
s digitálními piráty o svou
reputaci i přežití.**

Paul Bender je oceňovaný australský basista, třikrát nominovaný na Grammy. K jeho hlavním projektům patří jazz-funková kapela Hiatus Kaiyote, kterou na svých albech nasamplaovali Beyoncé nebo Kendrick Lamar. Ale v době pandemie Paul inicioval i svůj sólový projekt The Sweet Enoughs, který se prakticky bez proma stal na Spotify virálním hitem. Právě tento úspěch z něj však udělal ideální terč pro novodobý AI scam, který se dnes šíří jako lavina.

„Na profilu The Sweet Enoughs na streamovacích platformách (Spotify, Apple Music, Tidal atd.) se počátkem roku 2025 objevily čtyři skladby, které jsem nevytvořil, nemají se mnou nic společného a zněly jako naprostý odpad. Trápil jsem se celou věčnost, než se mi podařilo je z mého profilu odstranit. Trvalo přes osm týdnů, než platformy vůbec zareagovaly – k čemuž pravděpodobně přispěl až zájem médií o celou věc,“ popisuje Paul Bender.

Ačkoli se o záplavě AI hudby píše často, obvykle jde o tzv. „fiktivní umělce“, které platformy samy protežují pro vyšší zisk. Benderův případ je ale jiný: jde o čisté parazitování na jménu zavedeného tvůrce.

Z mylně přiřazené hudby daný umělec nemá žádný zisk, ale především kazí jeho reputaci. „The Sweet Enoughs má na streamovacích službách přes 30 milionů přehrání, takže spousta fanoušků dostala upozornění na ‚nové písničky‘, vzápětí však byli hrubě zklamáni těmito falešnými skladbami – a tohle se opakovalo ještě třikrát!“ zlobí se Bender. Australský

hudebník patří k jedněm z mála, kteří aktivně usilují o změnu. Jím iniciovanou petici za účinnější systém ověřování identity podepsalo přes 25 tisíc lidí, včetně Chaky Khan, Jill Scott nebo Jacoba Coliera. Bender nabízí jednoduché řešení: zavedení bezpečnostních prvků, běžných u e-shopů nebo bankovních služeb, jako je dvoufázové ověření.

JAK TO CELÉ FUNGUJE

Problém je, že řešení nemají v rukou jen streamovací společnosti, ale hlavně digitální distributoři. Služby jako DistroKid nebo TuneCore slouží radě nezávislých umělců jako rozhraní k tomu, aby svou hudbu dostali do několika streamovacích platforem najednou a inkasovali platby z odehrání. Principem řady podvodů v minulosti byla praxe, kdy sem hudbu mohl pod jakýmkoli jménem nahrát každý, což otevřelo dveře parazitování na jménech známých umělců.

Snad i v reakci na vlnu AI podvodů platformy i distributoři zavedli některé nové bezpečnostní prvky. Spotify od jara



testuje funkci Artist Profile Protection, která umožňuje umělcům schvalovat nové nahrávky ještě před jejich zveřejněním na profilu, aby se zabránilo chybám nebo záměnám. Nevýhodou je, že funkce vyžaduje aktivní správu a může zdržet i legitimní vydání. Je tedy vhodná hlavně pro umělce, kteří mají časté problémy se záměnami. A také Distrokid zavedl přísnější pravidla pro ověřování identity i výplatu peněz. Přesto tato opatření neznamenala konec podvodů a záměrně špatně přiřazená hudba se na profilech známých umělců vyskytuje dál.

Jak nedávno poukázal odborník na AI Nik Bear Brown z Northeastern University v Bostonu, parazitování na streamingových profilech známých umělců funguje nadále jednak proto, že podvodníci se zaměřují na relativně méně známé umělce se stabilní fanouškovskou základnou, kteří ale nedisponují silným digitálním managementem. Typicky jde o jazzové hudebníky. Dokládá to i bubeník Jorge Rossy, který se s fake skladbami pod vlastním jménem setkal také a následně zdokumentoval na dvě

stě podobných případů u ostatních jazzových umělců. Mnoho z nich nemá zapnutou funkci Artist Profile Protection, jež je poměrně nová a volitelná. Brown ale především vysvětluje, že i současné, bezpečnější standardy Spotify mají problém se zpožděním v detekci podvodného obsahu.

PODVOD S TISÍCINÁSOBNÝM ZISKEM

Nik Bear Brown nedávno na svém profilu na síti LinkedIn popsal, jak celý systém podvodů funguje: říká mu Okno zmateční (The Confusion Window) a staví na funkci Release Radar, která předplatitelům Spotify doporučuje skladby hudebníků, které mají v oblíbenosti.

„Posluchač, který roky sleduje svého oblíbeného jazzového pianistu, otevře v pátek ráno Spotify a uvidí novinku. Název je mu neznámý. Produkce zní divně. Tempo nesedí, instrumentace působí cizí a hlas tak docela neodpovídá tomu, co si pamatuje. A přesto čeká. Dopřeje skladbě třicet sekund. Předpokládá totiž,

že umělec experimentuje,“ popisuje Nik Brown princip, který zneužívá loajalitu skalních fanoušků. „V momentě, kdy posluchač u podvodné skladby, falešně připsané jím sledovanému umělci, překročí hranici třiceti sekund, dojde k aktivaci výplaty autorského honoráře. Peníze se dají do pohybu. Odcházejí od legitimního umělce, jehož jméno a pověst přilákaly ono kliknutí, k někomu, kdo pod jeho identitou nahrál digitální soubor,“ vysvětluje dále.

Podvodníci se zaměřují na (z globálního měřítka) „menší ryby“, které však mohou mít třeba deset až třicet tisíc sledujících na Spotify. Brown vysvětluje, že i když na Release Radaru dá nově nahrané skladbě onu třicetivteřinovou šanci jen necelá třetina příjemců, podvodným autorům se to i tak vyplácí. „Deset tisíc přehrání generuje částku čtyřiceti dolarů. Oproti vašim amortizovaným nákladům na distribuci ve výši padesáti centů tak návratnost vaší investice činí 7900 procent. Cyklus vyplácení autorských honorářů na Spotify funguje s osmitýdenním zpožděním. Průměrné

podvodné skladbě přitom trvá tři až osm týdnů, než je nahlášena a odstraněna. Toto načasování je – ať už záměrně, či omylem – téměř dokonalé.“

Jak nedávno upozornil americký jazzový pianista Jason Moran, který se s parazitováním na svém Spotify profilu také potýkal, ztížené možnosti obrany mají zejména ti umělci, kteří již nejsou naživu. „Jak mají kupříkladu John Coltrane nebo Billie Holiday ověřit, že nová nahrávka ‚právě nalezeného koncertu z Paříže 1952‘ není jen další podvrh?“ ptá se sugestivně. „Nemají se jak bránit.“ Ačkoli Spotify se dušuje, že pro dědice či držitele práv nabízí pro takové případy nové nástroje, je zřejmé, že u umělců se složitějšími katalogy nebo bez profesionální správy pozůstalosti je obrana proti zneužití profilu stále problematická.

Zmíněný odborník na AI dodává, že digitální distributoři i platformy typu Spotify rozhodně nejsou bez viny, protože v jejich zájmu je hlavně velký objem nahraných skladeb. Jakékoli pokročilejší bezpečnostní mechanismy tento proces zpomalují a také prodražují.

KDYŽ AI POSLOUCHÁ AI

Parazitování na profilech je jen špičkou ledovce širšího problému AI hudby na streamovacích platformách. Služba Deezer například udává, že do jejich systému je vloženo 60 tisíc AI generovaných skladeb denně, což je 39 procent všeho obsahu, který je na platformu každý den nahrán. Podle Deezeru je navíc AI hudba na jeho serverech z drtivé většiny (85 procent) poháněná boty farmami, které uměle navyšují počty poslechnů. Jinak řečeno, většinu nahrané AI hudby „poslouchá“ opět AI, nikoli reální lidé.

Podvodníci s uměle produkovanou hudbou obvykle zůstanou navždy skryti. Odhalené případy přesto pomáhají osvětlit skutečný rozsah problému. Na jaře letošního roku byl medializován případ „hudebníka“ Michaela Smithe ze Severní Karolíny, který se u federálního soudu v New Yorku přiznal k umělému navyšování počtu přehrání, díky kterému mezi lety 2017 až 2024 získal nelegálně více než 10 milionů dolarů. Smith

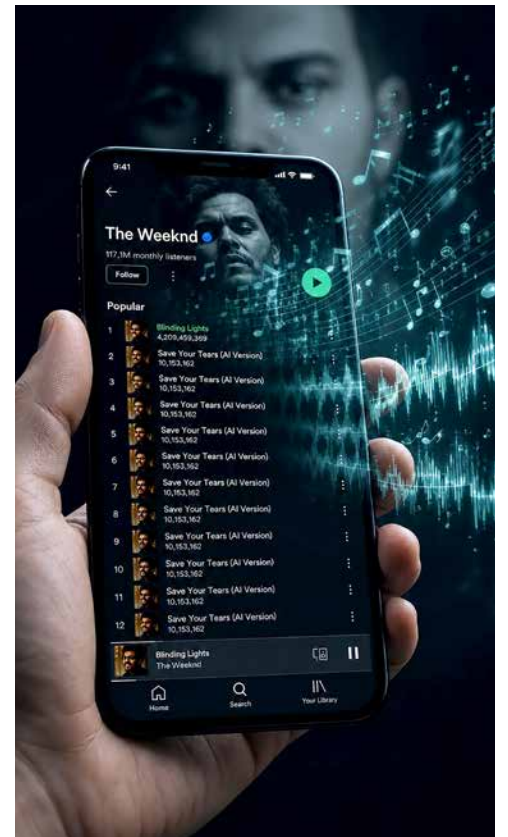
vytvořil stovky tisíc skladeb pomocí AI a následně využil „botí farmy“ (automatizované účty), aby tyto skladby miliardkrát přehrál. Tímto způsobem generoval falešnou poslechovost, za kterou mu streamovací platformy vyplácely autorské honoráře. Tento typ podvodu přímo poškozuje reálné hudebníky. Peníze na honoráře se totiž vyplácejí z jednoho velkého balíku podle podílu na celkovém počtu streamů. Smith tak peníze fakticky ukradl legitimním umělcům, jejichž podíl na trhu uměle rozředil.

JSTE PODEZŘELE ÚSPĚŠNÝ

Umělci menšinových žánrů nejsou poškozováni jen výše popsaným parazitováním na svém jméně, ale paradoxně i detekčními systémy, které by je měly před podvody chránit. Tyto důsledky boje platforem proti AI botům popsal loni web Guardian.

Tyto systémy jsou využívány k odhalování uměle zvyšovaného počtu přehrání, za nimiž často stojí AI boty a podvodné farmy. Problém je, že tyto bezpečnostní kontroly vedou mnohdy k falešně pozitivním nálezům a fungují na principu kolektivní viny. „Podezřelé“ jsou zejména ty skladby, které najednou získají větší počet přehrání, což samozřejmě může být způsobeno manipulací s AI boty, ale také nečekaným úspěchem např. na TikTok. Jak uvádí Guardian, distributoři dnes k větším výkyvům v počtu přehrání přistupují s nedůvěrou a množí se případy, kdy jsou takové skladby bez milosti mazány. Následky jsou likvidační. Hudebník může přijít o roky budované statistiky, pozice v playlistech a followery. Tento fenomén vytváří atmosféru strachu, kdy se umělec bojí i nečekaného úspěchu, aby nebyl algoritmem vyhodnocen jako podezřelý.

Ukazuje se, že platformy zatím nedokážou efektivně chránit identitu skutečných umělců. Upřednostňování kvantity a automatizace nahrává podvodníkům, kteří zneužívají jména zavedených tvůrců pro rychlý zisk z prvních vteřin poslechu. Dokud distributoři a platformy nezavedou přísnější ověřování uživatelů a rychlejší odstraňování falešného obsahu, budou na tento systém doplácet



hudebníci svou reputaci a fanoušci svou důvěrou.

JAK CHRÁNIT SVŮJ PROFIL V DIGITÁLNÍCH SLUŽBÁCH?

- 1. Aktivujte Artist Profile Protection:** V rozhraní Spotify for Artists si zapněte funkci schvalování nahrávek. Je to první obrana proti cizí hudbě na vašem profilu.
- 2. Monitorujte své statistiky:** Nástroje jako Chartmetric nebo Artist tools vám umožní sledovat, do jakých playlistů byla vaše hudba přidána. Podezřelý nárůst streamů z pochybného playlistu je lépe prověřit.
- 3. Hlásit při podezření:** Pokud najdete na svém profilu chybu, nečekejte. Kontaktujte distributora i podporu platformy.
- 4. Distributora vybírejte dle kvality služeb, nejen ceny:** Drobná úspora se nevyplácí v krizové situaci. Hledejte distributory s dobrou reputací v řešení sporů. ●