THREAT INTELLIGENCE REPORT

威胁情报 · 调查报告

SafeW / SafeX 即时通讯软件安全调查报告

虚假宣传、SparkCat 加密货币窃取木马
与“屡犯”行为时间线分析

报告对象	**SafeW 即时通讯应用及其变体小号 SafeX**
威胁类型	**SparkCat — 基于 OCR 的加密货币钱包助记词窃取木马**
涉及平台	**iOS（App Store）、Android（Google Play）；桌面 / 网页端风险评估**
首次披露	**2025 年 2 月 5 日 · 卡巴斯基 Securelist**
再次披露	**2026 年 4 月 3 日 · The Hacker News（援引卡巴斯基）**
综合风险等级	**高危 / CRITICAL**
报告日期	**2026 年 6 月 20 日**

本报告基于公开来源情报（OSINT）整理，部分桌面端结论为基于证据的风险推断。

目录

SafeW 即时通讯软件调查报告：虚假宣传、SparkCat 恶意软件与“屡犯”时间线

核心结论（TL;DR）

执行摘要 · EXECUTIVE SUMMARY

- **SafeW 是一款自称“端到端加密”“企业级安全”的即时通讯软件，但卡巴斯基已两次（2025 年 2 月、2026 年 4 月）在其应用中查获 SparkCat 加密货币窃取木马**，其“安全”宣传与“暗中用 OCR 扫描相册、窃取钱包助记词”的实际行为构成严重的虚假宣传与隐瞒恶意行为。
- **SparkCat 目前仅被证实感染 iOS 与 Android 移动端，PC / 桌面端不存在已记录的 SparkCat 变体**；但其前身（ESET 2023 年披露的木马化 Telegram / WhatsApp）确曾感染 Windows 并投放 Gh0st RAT，因此从官方商店之外下载 SafeW 桌面版 / 网页版仍属高风险，且其桌面客户端从未经过权威安全厂商独立检测。
- **SafeW 是“屡犯”（repeat offender）**：同一开发者（Safe Company）的应用在两轮 SparkCat 行动中均被点名，其变体小号 SafeX（包名 `com.ekhizc.carterocourrier`）在 2026 年第二轮中携带同款木马，卡巴斯基明确判断“两版恶意软件出自同一开发者”，证明这是有组织、持续演进的恶意行为而非一次性事故。

关键发现

1. **两次被卡巴斯基点名。**SafeW 的安卓包名 `org.safew.messenger` 与 `org.safew.messenger.store`、iOS 包名 `com.safew.messenger` 均出现在卡巴斯基 2025 年 2 月 5 日 SparkCat 首份报告的感染清单中。2026 年 4 月，卡巴斯基再次发现 SparkCat 新变体，The Hacker News（2026-04-03，记者 Ravie Lakshmanan）援引卡巴斯基披露：App Store 两款、Google Play 一款受感染——iOS 端被点名的正是“SafeW - 云办公助理”（及“悟空外卖: 泰国华人生活管家”），安卓端则是其变体 SafeX（`com.ekhizc.carterocourrier`，版本 2.1.0）。

2. **虚假宣传成立。**SafeW 官网与商店描述宣称采用“最先进的端到端加密”“MTProto 2.0 加密+二次混淆加密”“连开发者也无法查看”，并自我标榜“绝不在隐私保护上妥协”。但实际应用内嵌入了通过 OCR 扫描用户相册、窃取加密货币钱包助记词并外传至攻击者服务器的恶意 SDK / 框架——其“安全”卖点与暗藏窃密行为构成根本性矛盾与隐瞒。

3 **SparkCat 技术原理。**SparkCat 利用 Google ML Kit 的 OCR 文字识别模型扫描手机相册中的截图，匹配“助记词 / Mnemonic / Phrase”等多语种关键词，将命中图片上传 C2 服务器；卡巴斯基指出其使用了移动应用中不常见的 Rust 语言实现 C2 通信，并自 2024 年 3 月起活跃。安卓端 Google Play 感染应用累计下载超过 24.2 万次（卡巴斯基原文：“The infected apps in Google Play had been downloaded more than 242,000 times.”），这是首次在苹果 App Store 发现窃密木马（卡巴斯基：“this marks the first time a stealer Trojan has been detected in the App Store”）。

4 **PC 端风险定性。**截至本报告日期（2026 年 6 月 20 日），没有任何安全厂商记录过运行于 Windows / macOS 桌面 / 网页 / 浏览器扩展的 SparkCat 变体——SparkCat 被一致描述为纯移动端（Android + iOS）威胁。但其 2023 年前身（ESET 披露的木马化 Telegram / WhatsApp）确曾感染 Windows。SafeW 桌面版从未经权威厂商独立检测，从官方应用商店外的渠道安装仍是公认的高风险向量。

5 **SafeX 是同源小号。**SafeX 与 SafeW 的宣传文案高度雷同（同样宣称 MTProto 2.0、私有化部署、远程销毁、截屏提醒、双密码系统），在 2026 年第二轮 SparkCat 行动中携带同款木马。卡巴斯基研究员 Sergey Puzan 判断：“Considering the similarities of the current sample and the previous one, we believe that the developers of the new version of malware are the same.”（鉴于当前样本与此前样本的相似性，我们认为新版恶意软件的开发者与此前相同。）SafeX 本质是 SafeW 换皮重新上架以规避封禁的马甲应用。

详细分析

一、虚假宣传与隐瞒恶意行为

SafeW 在多个官方域名（safew.org、safewapp.com、safewpc.org、safew-official.com、safew.surf）及第三方商店投放高度一致的营销话术，核心卖点包括：

- **加密宣传**：“使用最先进的端到端加密技术，确保用户聊天内容始终加密传输，即使是应用开发者也无法查看”；官网进一步称“SafeW 使用与 Telegram 相同的端到端加密”。安卓商店描述则称采用“MTProto 2.0 端到端加密方案，并在此基础上进行二次混淆加密，使其能够抵御黑客攻击”。
- **隐私与合规**：宣称支持私有化部署“确保消息记录、文件资料与用户数据始终处于企业控制之下，满足各类合规及安全管理要求”；自我标榜“在数字时代，SafeW 绝不在隐私保护上妥协”。
- **安全增强功能**：远程销毁消息、截屏提醒、双密码系统（副密码自动隐藏敏感数据）、多次输错密码自动拍照上传、匿名群聊、无限云存储。

这些宣传与实际行为的差距是本案的核心。卡巴斯基技术分析显示，SafeW / SafeX 等被感染应用嵌入了名为 Spark 的恶意 SDK（安卓）/ 框架（iOS），在用户授予相册权限后，后台用 OCR 扫描所有可触及的照片，搜索加密货币钱包助记词并外传。卡巴斯基特别指出：令这一木马尤其危险的是，应用内没有任何迹象表明存在恶意植入物；它请求的权限看起来像是其核心功能所需，或乍看之下无害。换言之，一款以“安全 / 隐私”为最大卖点的通讯软件，实际却在系统性地窃取用户最敏感的金融凭据，并刻意隐瞒——这构成典型的虚假宣传与欺诈。

关于宣传中的技术真实性还存在两点疑问：其一，官网同时声称“与 Telegram 相同的加密”和“MTProto 2.0”，而 MTProto 本身是 Telegram 自有协议，与业界公认的强端到端方案（如 Signal 协议）不同，且 Telegram 默认聊天并非端到端加密；其二，SafeW 大量第三方“官网”上的用户好评（如“端到端加密让我安心”“团队全部切换后效率立刻提升”）无法独立核实，且 AppBrain 数据显示其安卓应用评分为 0.0、无任何评分记录，与官网呈现的好评墙不符，存在刷评 / 伪造口碑的嫌疑。

下载量方面也存在夸大空间：第三方统计（AppBrain）显示 `org.safew.messenger.store` 实际安装约 1.7 万次、`org.safew.messenger` 约 3.4 万次，Google Play 标注为“10,000+”。SafeW 已于 2024 年 12 月 13 日前后从 Google Play 下架。

二、SparkCat 恶意软件：感染历史、传播方式与技术原理

发现者与命名

SparkCat 由卡巴斯基（研究员 Dmitry Kalinin 与 Sergey Puzan）于 2025 年 2 月 5 日在 Securelist 首次公开披露。名称来自其安卓端恶意模块“Spark”与 iOS 端恶意框架的 bundle ID“bigCat.GZIPApp”。根据恶意文件时间戳与 GitLab 配置文件创建日期，该行动至少自 2024 年 3 月起活跃。卡巴斯基博客补充，本轮共发现 Google Play 10 款、App Store 11 款恶意应用。

iOS 感染历史（里程碑式）

SparkCat 是已知首个进入苹果 App Store 的 OCR 窃密木马，打破了“iOS 对恶意应用免疫”的神话。iOS 恶意框架用 Objective-C 编写，经 HikariLLVM 混淆，在不同应用中以 GZIP、googleappsdk、stat 三种名称出现。框架保留了调试符号，卡巴斯基由此提取到开发者设备上的项目路径与用户名（`/Users/qiongwu/` 为项目作者主目录、`/Users/quiwengjing/` 为 Rust 库作者主目录），C2-Rust 通信模块名为 im_net_sys。关键恶意类包括 PhotoMgr（搜索并上传含关键词照片）、MMMaker、ApiMgr、MMCore、MMLocationMgr（收集位置）。

Android 感染历史

安卓端恶意模块解密并启动基于 Google ML Kit 的 OCR 插件，识别图库文字，将命中 C2 关键词的图片上传服务器。最早引起卡巴斯基注意的是 UAE / 印尼的外卖应用 ComeCome（卡巴斯基原文：“a food delivery app in the UAE and Indonesia, named ‘ComeCome’ (APK name: com.bintiger.mall.android)... with more than 10,000 downloads”），此外还有 ChatAi（下载超 5 万次）等。Google Play 上受感染应用累计下载超过 24.2 万次。

技术原理（OCR 窃取助记词）

依据系统语言，SparkCat 下载相应字符集（拉丁、韩、中、日）的 OCR 模型；识别文字后，与 C2 下发的规则比对——除关键词（如各语言的“助记词 / Mnemonic / Phrase”）外，还可按备份码特有的无意义字母组合、种子短语词序等模式触发。命中图片连同识别文字、设备信息一并上传至攻击者服务器（经 Amazon S3 云存储或自建“rust”服务器）。该木马还包含 KeywordsProcessor、DictProcessor、WordNumProcessor 三种过滤模式以降低误报。卡巴斯基判断开发者为中文母语者（代码注释、C2 错误描述均为中文）。

危害与处置

卡巴斯基强调，种子短语一旦泄露即足以完全控制并清空受害者钱包；且木马可被轻易改造以窃取相册中的其他敏感信息（密码、文件截图）。重要的是，Dmitry Kalinin 在 Securelist 评论区明确澄清该木马的处置边界（原文）：

> “The malware described in this post doesn't persist, nor does it spread across network. It only exists on the mobile phone as long as an infected app is installed... transfer your funds to a new crypto wallet.”
>
> — Dmitry Kalinin, Kaspersky / Securelist：本帖所述恶意软件不在设备上持久化，也不跨网络扩散，仅在受感染应用安装期间存在于手机上……请将资金转移至新钱包。

卸载应用即可清除木马本体，但仍须将资金转移至新钱包。

三、PC 端 / 桌面端风险评估（重点）

用户最关心的问题是：SafeW 的桌面版 / 网页版是否也有同样隐患？基于现有公开证据，结论需分层表述：

1. **SparkCat 本身无桌面变体。**卡巴斯基的三份相关报告（2025 年 2 月 SparkCat、2025 年 6 月 SparkKitty、2026 年 4 月 SparkCat 新变体）一致将其定性为移动端（Android + iOS）威胁。2026 年 4 月新变体披露时，卡巴斯基专家 Sergey Puzan 与 Dmitry Kalinin 均称其为“移动威胁（mobile threat）”，防护建议是“为智能手机使用安全解决方案”。截至本报告日期，没有任何厂商记录过运行于 Windows、macOS 桌面、网页或浏览器扩展的 SparkCat 变体。
2. **但同类威胁在 PC 端确有先例。**SparkCat 的直接前身——ESET 于 2023 年 3 月 16 日披露的“木马化 WhatsApp 与 Telegram”行动——明确包含 Windows 组件。ESET 研究员 Lukáš Štefanko 与 Peter Strýček 发现两类 Windows 恶意程序：(a) 替换剪贴板钱包地址的 clipper；(b) 捆绑在 Telegram / WhatsApp Windows 安装包中的远程访问木马（RAT）。ESET 指出（原文）：“With one exception, all the remote access trojans we analyzed were based on the notorious Gh0st RAT, malware that is frequently used by cybercriminals due to its public availability.”（除一例外，我们分析的所有 RAT 均基于臭名昭著、因公开可得而被网络犯罪分子频繁使用的 Gh0st RAT。）这些 RAT 具备窃取剪贴板、键盘记录、查询 Windows 注册表、屏幕截图、获取系统信息、文件操作等能力，多通过 DLL 侧加载执行。值得注意的是，2023 年行动中的 OCR 窃密能力仅存在于安卓端，Windows 端为 clipper + RAT，不含 OCR。卡巴斯基本身在 SparkCat 报告开篇即引用此前身，称该行动“针对 Android 与 Windows 用户，通过非官方渠道传播”。

3. **SafeW 桌面版 / 网页版未经独立检测，渠道风险高。**SafeW 在 safew-official.com、safewpc.org 等站点提供 Windows / macOS / Linux 桌面安装包，并在 safew.org/web-signin 提供网页版；部分桌面“官网”明确表示“此处不提供安卓 / iOS 客户端”，即桌面与移动端分布在不同域名、脱离官方应用商店。截至本报告日期，未发现任何权威安全厂商对 SafeW 桌面或网页客户端进行过具名恶意软件分析（仅见 ANY.RUN、Joe Sandbox 等自动沙箱的零散提交，未经核实，不能作为结论）。鉴于：同一开发者的移动端已两次被实锤携带窃密木马；其同类前身曾在 Windows 投放 RAT；桌面安装包脱离官方商店审核——从这些渠道安装 SafeW 桌面版 / 网页版应视为高风险。McAfee、ESET 等厂商一贯警告：不要安装官方商店之外分发的通讯软件桌面客户端，它们可能是恶意软件。

> **桌面端风险定性结论** 高危
>
> 不能因为“SparkCat 暂无桌面变体”就认为 SafeW 桌面版安全。考虑到开发者已被证实的恶意意图、同类家族的 Windows 前科，以及桌面包脱离商店审核且无第三方安全背书，理性假设应是 SafeW 桌面 / 网页版同样不可信，在未经独立审计前不应安装或用于任何涉及加密货币、敏感凭据的场景。

四、“屡犯”时间线（repeat offender 证据链）

2023 年 3 月 16 日

ESET 披露木马化 Telegram / WhatsApp 行动（SparkCat 前身），首次出现安卓 OCR 窃取助记词，并含 Windows clipper 与 Gh0st RAT。这是该攻击模式的源头。

2024 年 3 月

据卡巴斯基对文件时间戳与 GitLab 配置的分析，SparkCat 行动开始活跃。

2024 年 12 月

SafeW（`org.safew.messenger.store`）前后在 Google Play 上架 / 更新（版本 1.5.6，2024 年 12 月 7 日；`org.safew.messenger` 约于 2024 年 12 月 13 日前下架）。

2025 年 2 月 5 日

卡巴斯基在 Securelist 首次公开 SparkCat，SafeW 的安卓包名（`org.safew.messenger`、`org.safew.messenger.store`）与 iOS 包名（`com.safew.messenger`）在感染清单之列。2025 年 2 月 6 日苹果、2 月 7 日 Google 先后下架相关应用。

2025 年 6 月

卡巴斯基披露 SparkKitty（SparkCat 的演进版），同样针对 iOS / Android、用 OCR 窃取相册中的助记词截图。

2026 年 4 月 3 日

The Hacker News 报道（记者 Ravie Lakshmanan）卡巴斯基发现 SparkCat 新变体，iOS 端被点名为“SafeW - 云办公助理”，安卓端为变体小号 SafeX（`com.ekhizc.carterocourrier`，版本 2.1.0）。卡巴斯基判断“新版本恶意软件的开发者与此前相同”。安卓新变体新增罕见混淆手段，Dmitry Kalinin 评价（原文）：“methods used by the SparkCat developers, such as code virtualization and cross-platform programming language usage, are rare for mobile malware. This demonstrates the high skill of the threat actors.”（SparkCat 开发者使用的代码虚拟化、跨平台编程语言等手法在移动恶意软件中罕见，显示出威胁行为者的高超技术。）iOS 版改为扫描英文助记词，潜在受害面更广。

时间线清楚地表明：同一开发者（Safe Company）旗下的 SafeW 在 2025 年第一轮被实锤后，于 2026 年携换皮小号 SafeX 卷土重来并继续携带同款木马，且卡巴斯基明确归因为“同一开发者”。这正是“屡犯”的核心证据——不是被冒名或一次性供应链污染，而是持续、有组织、不断升级反检测手段的恶意行为。

五、SafeX 与 SafeW 的关系

- **宣传同源**：SafeX 的 Google Play / Uptodown 描述与 SafeW 几乎逐条对应——同样主打“MTProto 2.0 端到端加密+混淆”“私有化 / 本地服务器部署”“远程销毁消息”“截屏提醒”“双密码系统（副密码隐藏敏感数据）”“匿名群聊”“企业级无限云盘”。SafeX 描述中甚至直接出现“SafeX 等主流平台”字样。
- **恶意同款**：SafeX（`com.ekhizc.carterocourrier`）在 2026 年第二轮 SparkCat 行动中被卡巴斯基点名为安卓端感染应用，与 iOS 端的 SafeW 配对出现。
- **关系定性**：SafeX 应被视为 SafeW 的马甲 / 换皮重新上架应用，用于在 SafeW 因 2025 年曝光而失去信誉 / 被下架后延续同一窃密行动。卡巴斯基“开发者相同”的判断进一步支持这一结论。
- **命名混淆提示**：需注意市面上还有同名但不相关的实体（如 safex.org 的 Monero 仿盘加密项目、SafeX Pro / safexmax.com 被加拿大 BCSC 列入黑名单的未授权金融平台、safex.inc 加密交易所），这些与本报告所指的 SafeW 通讯软件变体 SafeX 并非同一对象，调查与避险时应以包名 `com.ekhizc.carterocourrier` 为准。

建议与行动项

对普通用户 / 已安装者（立即执行）

1. 立即从所有设备卸载 SafeW 与 SafeX（移动端与桌面 / 网页端一并停用）。SparkCat 不持久化，卸载即可清除木马本体。
2. 若曾在相册中存过任何加密货币钱包助记词 / 私钥截图：视同已泄露。立即创建全新钱包，将资金全部转出后彻底弃用旧钱包（助记词无法更改）。
3. 排查相册中其他敏感截图（密码、银行信息、证件），相应修改密码、挂失卡片。
4. 不要从 safew.org、safewpc.org、safew-official.com 等任何渠道下载 SafeW / SafeX 的桌面版或网页版；改用经独立审计、开源、有良好记录的通讯工具（如 Signal）。

对企业 / 合规团队

1. 将 `org.safew.messenger`、`org.safew.messenger.store`、`com.safew.messenger`、`com.ekhizc.carterocourrier` 及卡巴斯基公布的 C2 域名（如 api.aliyung.com / .org、api.firebaseo.com、api.googleapps.top、99ai.world 等）加入 MDM / EDR 黑名单与网络阻断规则。
2. 对持有加密资产或敏感数据的员工设备进行排查；禁止从官方商店外侧载通讯类桌面客户端。
3. 启用 Google Play Protect（Google 称可自动拦截已知版本）；iOS 侧依赖卡巴斯基等方案在连接 C2 时告警。

改变建议的判断阈值（BENCHMARKS）

- 若未来出现权威安全厂商（卡巴斯基 / ESET / Trend Micro 等）对 SafeW 桌面 / 网页客户端的具名、洁净的代码审计结论，可重新评估其桌面端可信度；在此之前默认不可信。
- 若卡巴斯基或同级厂商记录到 SparkCat / 同源家族的 Windows / macOS 桌面变体，应立即将桌面端风险等级由“高（基于渠道与开发者信誉）”上调为“已确认感染”。

参考来源

下列来源按类别整理，均为本报告引用的公开资料。访问日期：2026 年 6 月。链接为原始 URL，供核验之用。

一手安全研究（卡巴斯基 / ESET）

[1] **SparkCat crypto stealer in Google Play and App Store.** Securelist by Kaspersky（Dmitry Kalinin, Sergey Puzan），2025-02-05。
https://securelist.com/sparkcat-stealer-in-app-store-and-google-play/115385/

[2] **SparkCat — first OCR trojan stealer to infiltrate the App Store.** Kaspersky official blog，2025。
https://www.kaspersky.com/blog/ios-android-ocr-stealer-sparkcat/52980/

[3] **Kaspersky discovers new SparkCat variant bypassing App Store and Google Play security.** Kaspersky Press Release，2026。
https://www.kaspersky.com/about/press-releases/kaspersky-discovers-new-sparkcat-variant-bypassing-app-store-and-google-play-security

[4] **ESET Research discovers trojanized WhatsApp and Telegram applications stealing crypto funds.** ESET Newsroom（Lukáš Štefanko, Peter Strýček），2023。
https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-discovers-trojanized-whatsapp-and-telegram-applications-stealing-crypto-funds-and-with/

新闻报道与媒体分析

[5] **New SparkCat Variant in iOS, Android Apps Steals Crypto Wallet Recovery Phrase Images.** The Hacker News（Ravie Lakshmanan），2026-04-03。
https://thehackernews.com/2026/04/new-sparkcat-variant-in-ios-android.html

[6] **SparkCat Malware Uses OCR to Extract Crypto Wallet Recovery Phrases from Images.** The Hacker News，2025-02。
https://thehackernews.com/2025/02/sparkcat-malware-uses-ocr-to-extract.html

[7] **Lookalike Telegram and WhatsApp Websites Distributing Cryptocurrency Stealing Malware.** The Hacker News，2023-03。
https://thehackernews.com/2023/03/lookalike-telegram-and-whatsapp.html

[8] **Mobile security — Latest News, Reports & Analysis.** The Hacker News（专题页）。
https://thehackernews.com/search/label/mobile%20security

[9] **Crypto-stealing iOS, Android malware found on App Store, Google Play.** Help Net Security，2025-02-05。
https://www.helpnetsecurity.com/2025/02/05/crypto-stealing-ios-android-malware-found-on-app-store-google-play-sparkcat-malicious-sdk/

[10] **SparkCat campaign target crypto wallets using OCR to steal recovery phrases.** Security Affairs。
https://securityaffairs.com/173873/malware/sparkcat-campaign-target-crypto-wallets.html

[11] **Weaponized Telegram and WhatsApp Apps Attack Android & Windows Users.** Cyber Security News。
https://cybersecuritynews.com/weaponized-telegram-and-whatsapp-apps/

[12] **SparkKitty Malware Targets Crypto Users, Steals Seed Phrases.** Ainvest，2025-06。
https://www.ainvest.com/news/sparkkitty-malware-targets-crypto-users-steals-seed-phrases-2506/

[13] **Kaspersky discovers new SparkCat variant bypassing App Store and Google Play security.** Zawya（新闻稿转载）。
https://www.zawya.com/en/press-release/companies-news/kaspersky-discovers-new-sparkcat-variant-bypassing-app-store-and-google-play-security-lht2mx4r

[14] **SparkCat Malware (Android) — Malware removal instructions.** PCRisk。
https://www.pcrisk.com/removal-guides/32117-sparkcat-malware-android

应用商店、下载页与官网

[15] **SafeW（`org.safew.messenger`）.** APKCombo。
https://apkcombo.com/safew/org.safew.messenger/

[16] **SafeW（`org.safew.messenger.store`）.** APKCombo。
https://apkcombo.com/safew/org.safew.messenger.store/

[17] **SafeW for Android — Download.** Softonic。
https://safew.en.softonic.com/android

[18] **SafeW（`org.safew.messenger`）— Free APK Download.** AppBrain。
https://www.appbrain.com/app/safew/org.safew.messenger

[19] **SafeW（`org.safew.messenger.store`）— Free APK Download.** AppBrain。
https://www.appbrain.com/app/safew/org.safew.messenger.store

[20] **SafeW Official Download — PC for Windows, macOS & Linux.** safew-official.com。
https://safew-official.com/en/

[21] **SafeW Official Download Center.** safew-official.com。
https://safew-official.com/en/download/

[22] **SafeX：打造企业通信安全的新基石.** Google Play（`com.ekhizc.carterocourrier`）。
https://play.google.com/store/apps/details?id=com.ekhizc.carterocourrier

[23] **SafeX for Android — Download the APK.** Uptodown。
https://safex.en.uptodown.com/android

其他参考（同名实体辨识）

[24] **safex.org Reviews.** Trustpilot（注：与本报告 SafeX 通讯应用无关，用于辨识同名实体）。
https://www.trustpilot.com/review/safex.org

[25] **Is SafeX Pro a Safe or Scam?（Feb 2026）.** Traders Union（注：指 SafeX Pro 金融平台，非通讯应用）。
https://tradersunion.com/scam-or-safe/safex-pro-review/

报告编制说明：本文档由公开来源情报（OSINT）汇编而成，旨在用于安全研究、风险告知与防护决策参考。文中标注为“原文”的英文引用均来自上述安全厂商与媒体的公开报道，中文为对照译述。涉及加密货币资产处置、企业合规等具体决策，建议结合专业法律与安全意见执行。