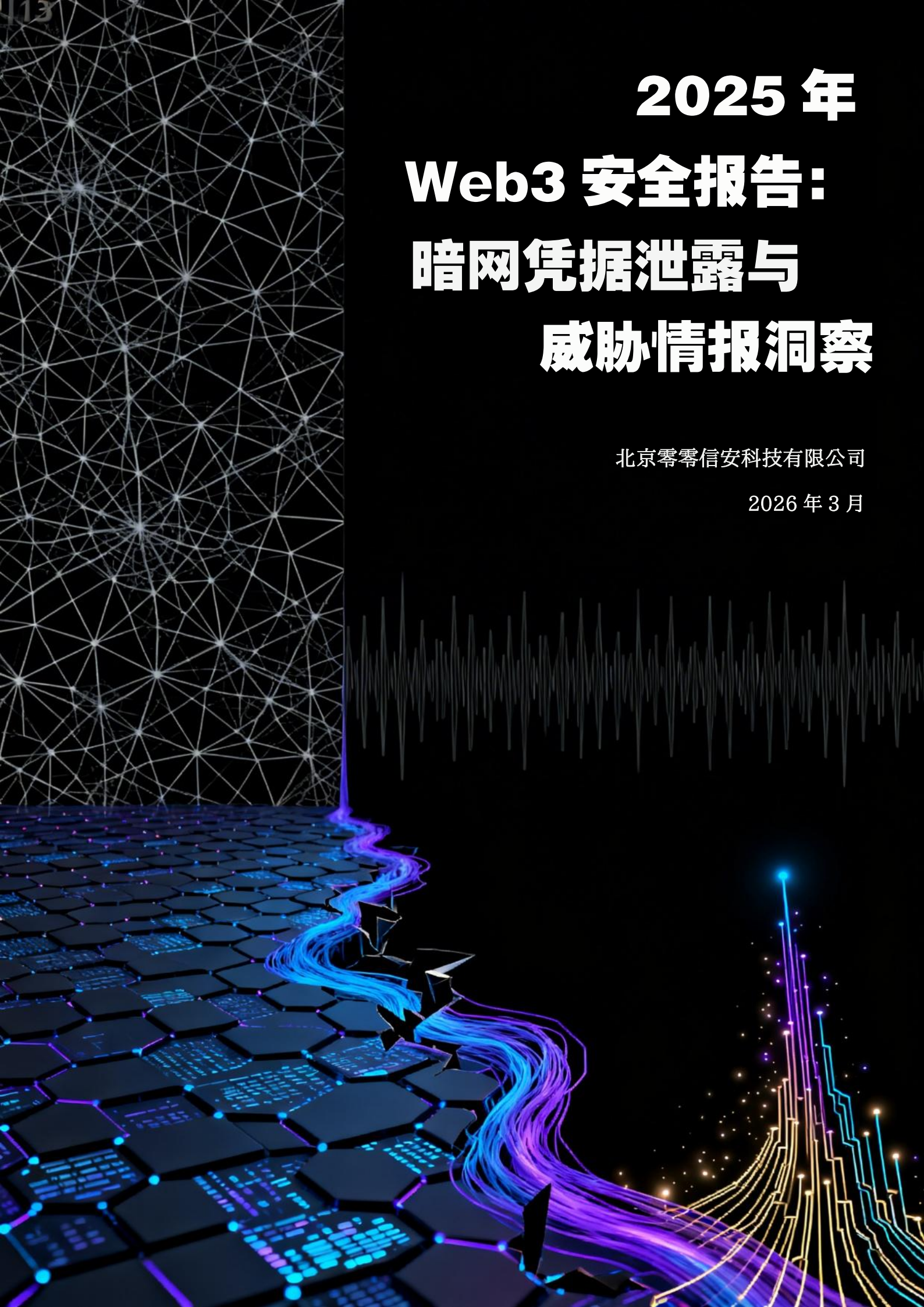
2025 年 Web3 安全报告：暗网凭据泄露与威胁情报洞察

北京零零信安科技有限公司

2026 年 3 月



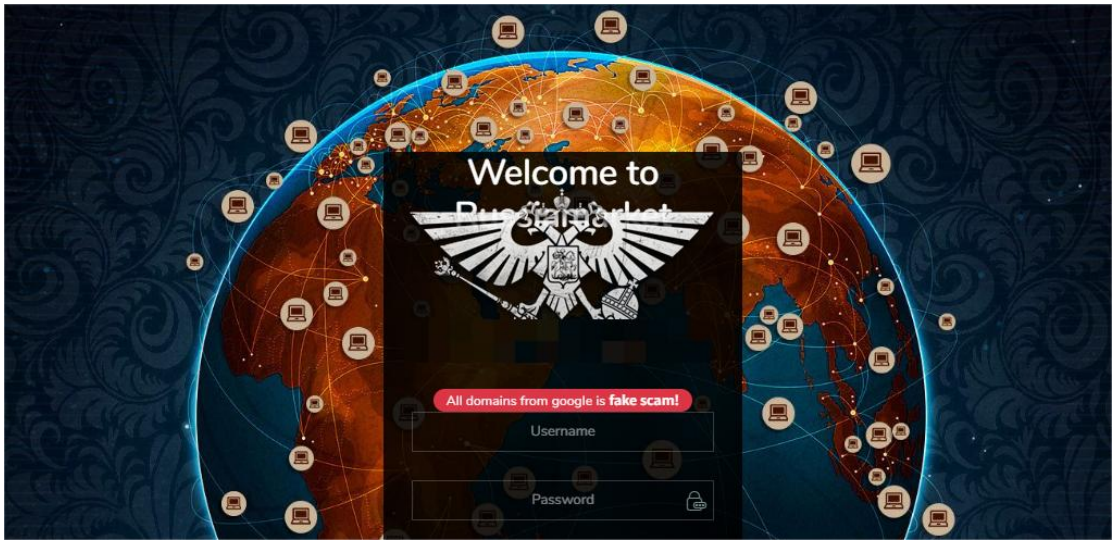
目录

1. 引言：你的交易所/银行密码值多少钱？

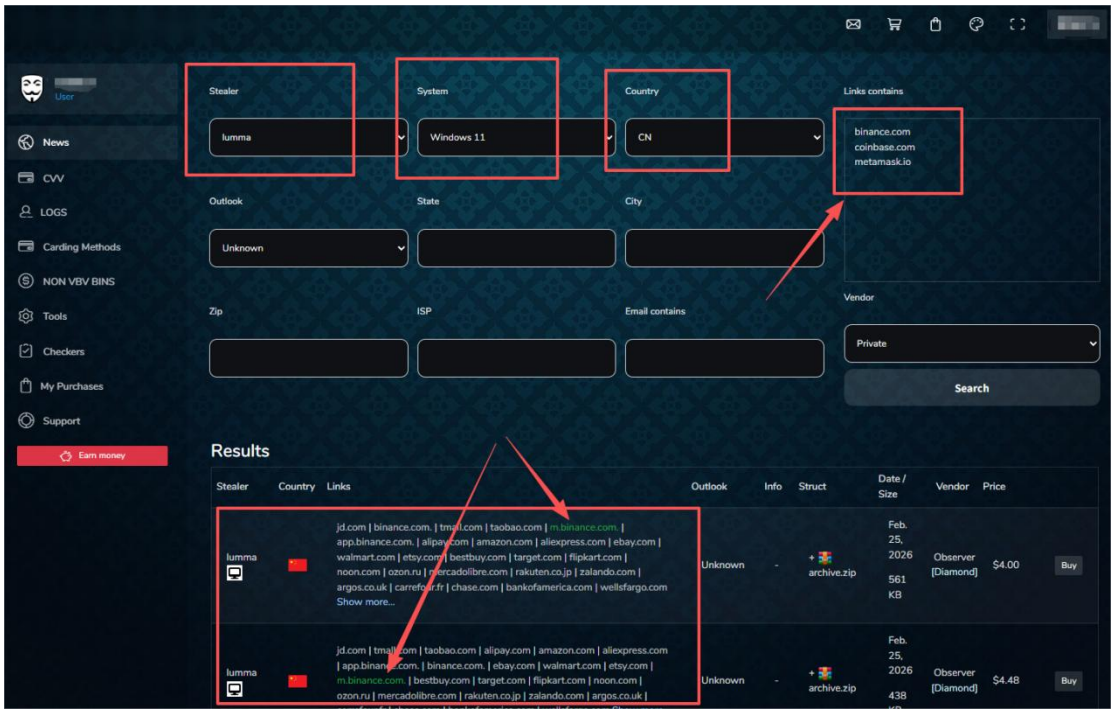
在洋葱网络的深处，一切都有明码标价——包括守护你财产的交易所登录凭证、银行卡信息，甚至种子短语（助记词）。

免责声明：本文所有操作和示例均为专业安全研究者在完全可控、合法环境下的模拟演示，仅供技术讨论与威胁情报分析之用。严禁用于任何非法活动。暗网本身充满风险与欺诈，普通用户切勿尝试访问，否则可能面临法律、资金乃至人身安全后果。此外，本文为防止被恶意利用，已将暗网/半暗网（lite）的具体名称代号化（例如某自动化交易市场，本文取其首字母“R 市场”代替；某 Stealer 交易群组，本文取其首字母“D 云”代替；某黑客论坛，本文取其首字母“L 论坛”代替，等等）。

来看一个典型的暗网市场场景（2025-2026Q1 数据参考）：



攻击者在这里“淘金”，可以精细筛选目标：



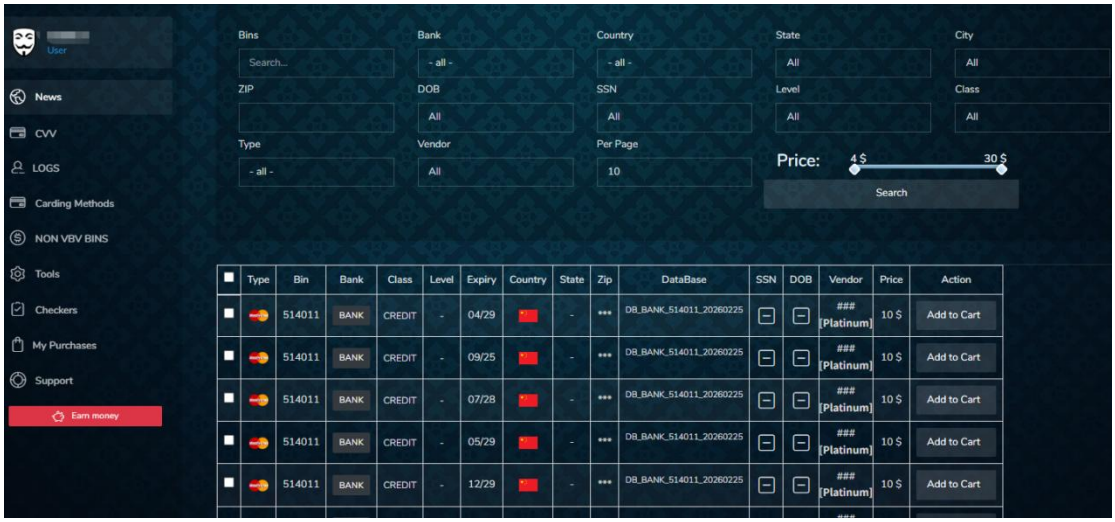
- Stealer 类型：Lumma（2025 年最活跃的信息窃取器之一，常伪装成破解软件、邮件附件或广告传播，主要窃取目标包括：浏览器日志/登录地址/账号/明文密码、加密货币钱包/币安/Coinbase 等种子短语/私钥、CVV 银行卡信息等）。
- 系统：Windows 11（最新版用户往往更有“价值”）。
- 国家：CN（中国人）。
- 链接包含：binance.com、coinbase.com、metamask.io（窃取日志中带这些交易所/钱包痕迹）。

筛选条件一组合，就得到：被 Lumma 感染、使用 Win11、在币安/Coinbase/MetaMask 活跃的中国用户。他们的交易所账号密码、种子短语、私钥、浏览器 cookies，甚至关联银行卡信息，全打包成“数据包”。

2025 年地下市场行情显示：

- 普通 Stealer 日志（含杂七杂八凭证）：平均$10 左右/条（上图所示交易所价格从$4~15）。
- 高价值 crypto logs（含余额提示、Binance/Coinbase/MetaMask 登录态）：$50-500+不等，甚至上千美元（如果余额大或有历史交易记录，常被拍卖）。
- 批量日志包（数万条）：几百到一千美元。

同样，这里也能轻松筛选“FULLZ”（Fullz = 完整身份包，暗网信用卡诈骗专业术语）：姓名、地址、出生日期、电话、邮箱、身份证/SSN、信用卡号+有效期+CVV、发卡银行等一应俱全。



2025-2026Q1 价格区间：

- 标准 FULLZ（含信用卡 CVV）：$10-100。
- 高限额/优质 FULLZ（信用额度>5k 美元）：可达$110-120+。

拿到这些包后，攻击者就能直接消费、套现、转账，或用自动化脚本测试/提币。投入数美元，潜在回报轻松百倍、千倍甚至万倍。

所以，答案来了——**你的交易所/银行密码值多少钱？**

数美元到数十美元。

这不是制造焦虑，而是赤裸裸的现实：暗网已把凭据泄露变成“基础设施级”商品。你如果不了解原理、不主动防护，就可能成为下一个“低成本目标”。

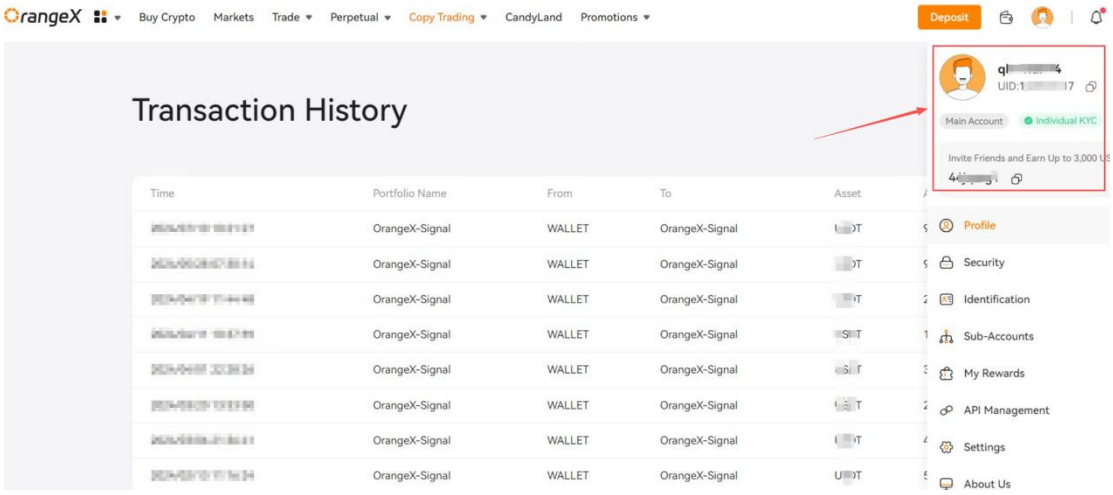
本文的目的不是吓人，而是把原理讲透、把防御讲实。**无论你是普通 Web3 玩家、CISO，还是交易所安全团队，都有责任守护好自己和用户的资产。**

2. 真实案例：凭据泄露如何危害到你

黑客登录你的交易账号不是电影里的情节，而是每天发生在 Web3 和金融生态中的现实威胁。它能让攻击者像“幽灵”一样潜入你的账号，窃取资产、篡改信息，甚至引发连锁反应——从个人钱包清零到企业声誉崩盘。以下基于零零信安研究员实际监测的案例，剖析两个典型事件：OrangeX 交易所的 Combo Log 泄露和 Crypto.com 的账号接管（ATO）风险。这些不是孤立个案，而是 2025 年 Web3 安全报告中频发的模式（Beosin 数据：凭据相关损失超 1.8 亿美元）。我们还会深挖为什么不能把所有安全希望寄托在 2FA（双因素认证）上——它虽强大，但远非万能。

2.1. 案例一：OrangeX 交易所 Combo Log 泄露——暗网凭据直通你的交易记录

零零信安研究员在暗网监测到 OrangeX 交易所（orangex.com）的 Combo Log（组合凭据列表，包括用户名、密码等）大规模流通。这些凭据并非直接从交易所数据库泄露（可能源于第三方数据 breach 或用户设备感染 Infostealer），但攻击者只需几美元购买，就能用它们登录真实账号。



想象一下：你作为 OrangeX 用户，开启了 2FA，以为万无一失。但攻击者用泄露的用户名+密码尝试登录——如果你的密码复用（常见于多账号用户），他

们就能触发 2FA 提示。这时，如果 2FA 设备被窃取（例如你用于接收安全码的邮箱也由于账号密码的泄露而被攻击者接管）或通过社会工程（如钓鱼短信）绕过，游戏就结束了。通过零零信安研究员的检测显示，本次账号接管允许未授权操作，包括：

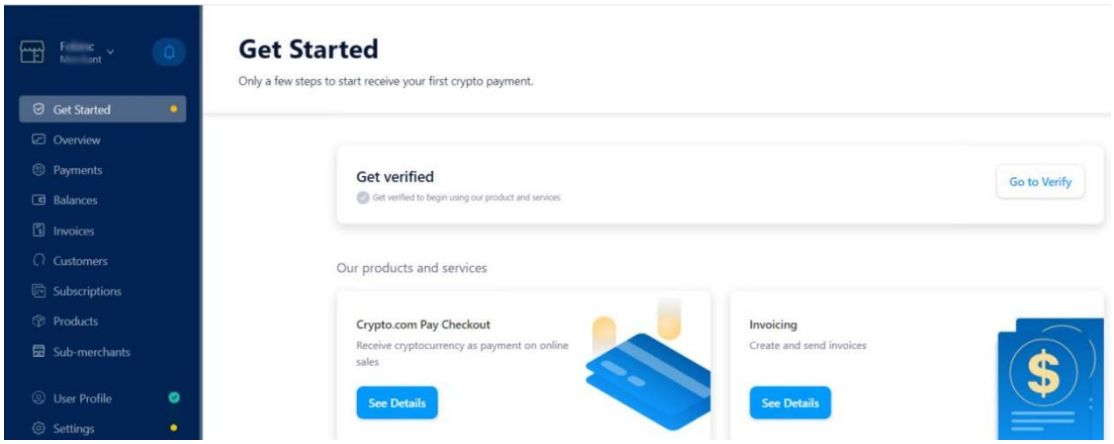
- 查询交易历史和余额（暴露你的资产分布）。
- 修改账号设置（如绑定新邮箱或提现地址）。
- 甚至小额测试转账，确认账号“活性”后大肆掠夺。

危害到你：个人用户可能损失数千美元加密资产；企业如果用 OrangeX 处理 B2B 支付，泄露可能导致供应链中断或合规罚款。针对暗网的监测显示，这些凭据被打包售卖，价格低至几美元/条（批量购买和清洗的成本甚至降至低于几美分），却能撬动上万倍回报。

这不是 OrangeX 的独家问题——2025 年类似威胁事件在 Binance、Coinbase 等几乎所有的交易所平台周边泛滥（SlowMist 报告称，Infostealer 如 Lumma 导致的凭据流通量同比翻倍）。

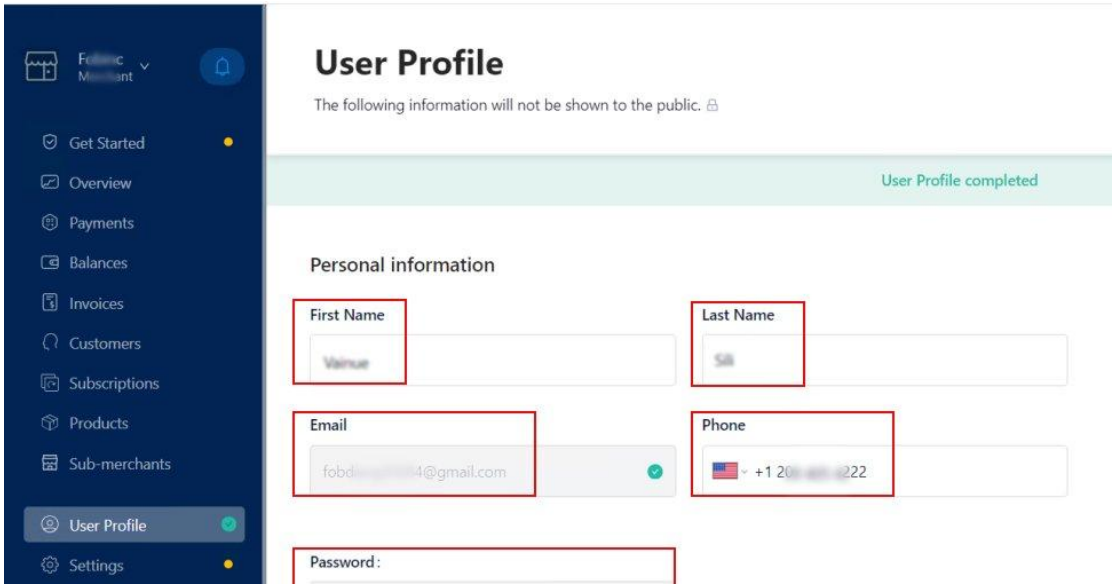
2.2. 案例二：Crypto.com 账号接管（ATO）风险——10 万用户成“活靶子”

零零信安研究员在暗网监测到 Crypto.com（crypto.com）存在 ATO 风险，至少 10 万用户受波及。攻击者通过暗网获取的凭据（可能结合浏览器 cookies 或 session 令牌），绕过部分防护，直接接管账号。



上图中显示的页面（Crypto.com Pay 的“Get Started”页面）展示了潜在漏洞

点：攻击者在未进行真实验证状态下，就能访问受害用户的支付、发票等模块。由于凭据泄露，攻击者可伪装成你执行操作。



具体危害：

- 获取隐私信息：如 KYC 数据、交易记录、关联银行卡。
- 执行恶意操作：转账、申请贷款、甚至用你的账号洗钱。

为什么这么容易？因为 ATO 不只靠密码——攻击者常用“session hijacking”（劫持会话）或“credential stuffing”（凭据填充攻击），批量测试暗网买来的列表。

2FA 不是万能的，即使启用，它也挡不住设备级窃取或实时钓鱼。

2.3. 2FA 的局限性：为什么不能全靠它？

许多人视 2FA 为“silver bullet”（银弹），但在凭据泄露场景下，它往往成为“虚假的安全感”。以下是关键局限：

- 绕过机制：Infostealer 如 Lumma 能窃取浏览器 cookies 和 session token，使 2FA 验证通过，攻击者也能“继承”你的登录态，无需再输入码。此类绕过在 ATO 事件中占比显著（SpyCloud 等报告显示为主要向量之一）。
- 社会工程攻击：2FA 码常通过 SMS/App/EMAIL 推送，如果你的手机被 SIM swapping（SIM 卡交换攻击）或钓鱼 App 劫持或安全邮箱被劫持，码就白给了。香港/新加坡用户尤其易中招，因为本地电信诈骗高发（2025

年 EY 报告：亚太地区 SIM swapping 事件+25%）。

- 复用与疲劳：用户常在多平台用相同密码+2FA，如果一个平台泄露，攻击者可“疲劳轰炸”——反复触发 2FA 直到你忽略或误操作。
- 不覆盖所有链条：2FA 防护账号入口，但不防内部泄露（如 API key 暴露）。在 Web3 中，种子短语泄露后，2FA 根本无用——攻击者直接重建钱包。另外，并不是所有网站/APP 入口都被 2FA 防护，有的供应商或大客户等系统为了业务需要，可能未开启 2FA。

简言之，2FA 是必要但不充足的。它假设凭据本身安全，但暗网凭据市场证明：凭据是起点，不是终点。零零信安监测显示，2025 年超 60%的 ATO 攻击成功事件涉及 2FA“失效”。

2.4. 这些案例不是个例：Web3 的“泄露疫情”

OrangeX 和 Crypto.com 只是冰山一角。2025 年 Beosin 报告：Web3 凭据泄露事件总损失 1.8 亿美元，暗网交易量激增 43%（SOCRadar 数据）。类似案例包括：

- Binance 周边 Combo Log 流通，导致数千用户资产被提。
- Coinbase 的 API key 泄露，结合 ATO 造成企业级损失。
- MetaMask 扩展钓鱼，2025 上半年 SlowMist 记录多起“伪装工具”窃取私钥。

为什么普遍？因为 Infostealer 生态成熟——MaaS 模式让攻击门槛低至几美元。**个人用户易忽略设备安全，企业（交易所）则常忽略威胁情报监测。**危害到你：不止钱包清零，还可能身份盗用、信用崩盘，甚至遇到法律的麻烦（如果账号被用于洗钱）。

2.5. 小结：从受害者到防护者

凭据泄露的危害如病毒般扩散——从暗网几美元起步，到你的财产灰飞烟灭。这些真实案例提醒我们：安全不是被动防御，而是主动情报。别全赌 2FA，结合硬件钱包、多签机制、定期凭据扫描。作为 Web3 玩家或 CISO，了解这些，才能避开深渊。

下面，让我们聊聊曾经发生了什么、为什么会发生，以及如何反击。

3. 交易所危机：凭据泄露态势

3.1. 全球有多少凭据被泄露了？

这是一个极具挑战性的问题，因为暗网凭据流通高度碎片化、重复率高，且充斥二手/三手转售、聚合包和垃圾数据。零零信安研究员 2025 年监测到暗网凭据售卖事件超过数万件，每件从数十条到数亿条不等，原始累计流通数据量可能达到千亿级规模（包含大量重复与历史聚合数据）。但经过我们团队的获取、清洗、去重和格式化处理，发现大量数据为重复售卖、历史聚合或低价值混杂日志，真正“有效”（去重、完整、非构建的脏数据）的凭据占比通常仅 5%~10%（基于抽样分析）。

这一现象在全球知名威胁情报报告中也普遍存在。例如：

- SpyCloud 2025 Identity Exposure Report 显示，其回收的独特身份记录累计达 53.3 亿条（包括凭据、PII 等），较 2024 年增长 22%，其中 Infostealer 相关凭据 548 百万条，暴露密码 31 亿+。
- Bitsight State of the Underground 2025 报告：2024 年从 stealer logs 回收 13.2 亿独特凭据，2025 年新泄露凭据激增至 2.9 亿条。
- Group-IB High-Tech Crime Trends 2025：2024 年检测 1,107 起数据泄露，总计 64 亿条记录（其中密码 4.56 亿条，独特 1.61 亿条），但年度新凭据规模通常数亿级。

这些报告的“矛盾”——累计动辄数十亿甚至更高，而年度新曝光仅数亿——本质上是重复流通、聚合 dump 和垃圾数据导致的。零零信安基于自身暗网监测和清洗经验，估算全球目前去重后的有效凭据（可直接用于 credential stuffing 或 ATO 的独特组合）**规模约为 100 亿~200 亿条**。其中，session cookies 流通量更高（NordLayer 估 2025 年 94 亿条），但活跃率仅 20%左右。

这一规模意味着凭据已成基础设施级威胁：低成本即可获取高价值 crypto logs，却能撬动万倍回报。

3.2. 泄露凭据售卖渠道有哪些？

泄露凭据（尤其是 Infostealer 生成的 stealer logs、combo lists、session cookies 等）的售卖渠道在 2025-2026Q1 已高度成熟和碎片化。零零信安研究员监测显示，这些渠道从传统 Tor 暗网市场逐步向 Telegram 等半公开平台迁移，交易速度更快、门槛更低、匿名性更强。售卖形式多样：单条/批量 logs、订阅服务、免费样品引流付费优质包等。价格从几美元到数百美元不等，取决于新鲜度、价值（crypto/企业凭据）和质量。

主要渠道分为三大类：

3.2.1. 传统暗网市场（Tor Onion Sites）

这些平台通过 Tor 浏览器访问，使用加密货币（如 Monero/Bitcoin）交易，提供 escrow 保护、PGP 加密和信誉系统。2025-2026Q1 市场碎片化严重，许多因执法行动（如 G 市场取缔、B 2025 年中被关）而迁移，但几家核心平台仍主导凭据销售。

- R 市场（最主导的凭据/stealer logs 市场）：专注 stealer logs、cookies、凭据、RDP 访问和企业数据。2026Q1 仍是最大凭据交易枢纽，常更新日志，低技能攻击者青睐。价格亲民：单个 log $10 – $20，批量更低。
- T 市场：2025 年 A 市场崩盘后快速崛起，吸收大量卖家，成为西方通用暗网市场之一。售卖 stealer logs、combo lists 和凭据，支持精细搜索。
- B 市场（至 2025 年中被取缔前活跃）：专注信用卡/PII/凭据，常通过“促销 dump”免费泄露部分数据吸引流量，后付费买完整包。
- 其他活跃/新兴：N 市场、S 市场、E 市场（邀请制，专注高价值企业凭据和 malware logs）、2easy（强调新鲜日志）。

这些市场常有精细筛选（如国家、交易所痕迹、系统类型），零零信安监测显示，针对 CN 用户+交易所（如 Binance/MetaMask）痕迹的 logs 最受欢迎。

3.2.2. Telegram 频道与群组（当前主流渠道）

Telegram 已成为凭据售卖的“Dark Web Lite”（暗网 lite：半公开、易访问的

平台，这些平台在功能上“模仿”了传统暗网的非法活动，但门槛和技术壁垒远低于真正的 Tor 暗网）平台，2025-2026Q1 占比超 60%。优势：实时更新、易访问、无需 Tor、低门槛，许多卖家直接跳过暗网市场。渠道分免费引流+付费订阅，常见模式：免费样品/旧 logs 引流，付费独家新鲜包。

典型频道类型：

- M 云：大型聚合频道，分享 stealer logs（Lumma/RedLine 等）、combo lists、用户名/密码/IP 等。成员超 2 万，常免费分享部分数据。
- O 云：日志聚合频道，收集并转发多源 combo lists 和 logs。
- A 云：2025 年爆火的频道，曾发布 23 亿行 stealer 数据，但多为历史聚合/二手数据，常标“fresh/private leak 2025”营销。
- B CVV [ANTIPUBLIC]：B 官方频道，监控 Telegram/论坛泄露卡数据/凭据，常免费 dump 吸引买家。
- 其他常见：CL 频道、M 云类聚合、私人订阅频道（$20/月起无限访问新鲜 logs）。

许多频道用 bot 自动化支付/交付，卖家常换名或镜像避封禁。零零信安观察：新鲜 stealer logs 常先在 Telegram 流通，再上 Tor 市场。

3.2.3. 暗网论坛与订阅服务

论坛提供讨论、样品展示和信誉系统，常作为市场补充。

- X 论坛：高端论坛，售卖网络访问权、stealer logs 和凭据，常用于初始访问经纪（IAB）。
- L 论坛：专注数据泄露/stealer logs 档案，常更新 combo lists 和 ULP 文件。
- E 论坛、D 论坛：通用论坛，卖家发样品或使用积分免费获取、协商价格；部分有付费 Telegram feed。
- 订阅服务：$200 – $500/月“firehose”订阅（无限新鲜 logs），或$20/月基础访问。

3.3. 各主要交易所凭据泄露的量级是多少？

特别声明与重要澄清：

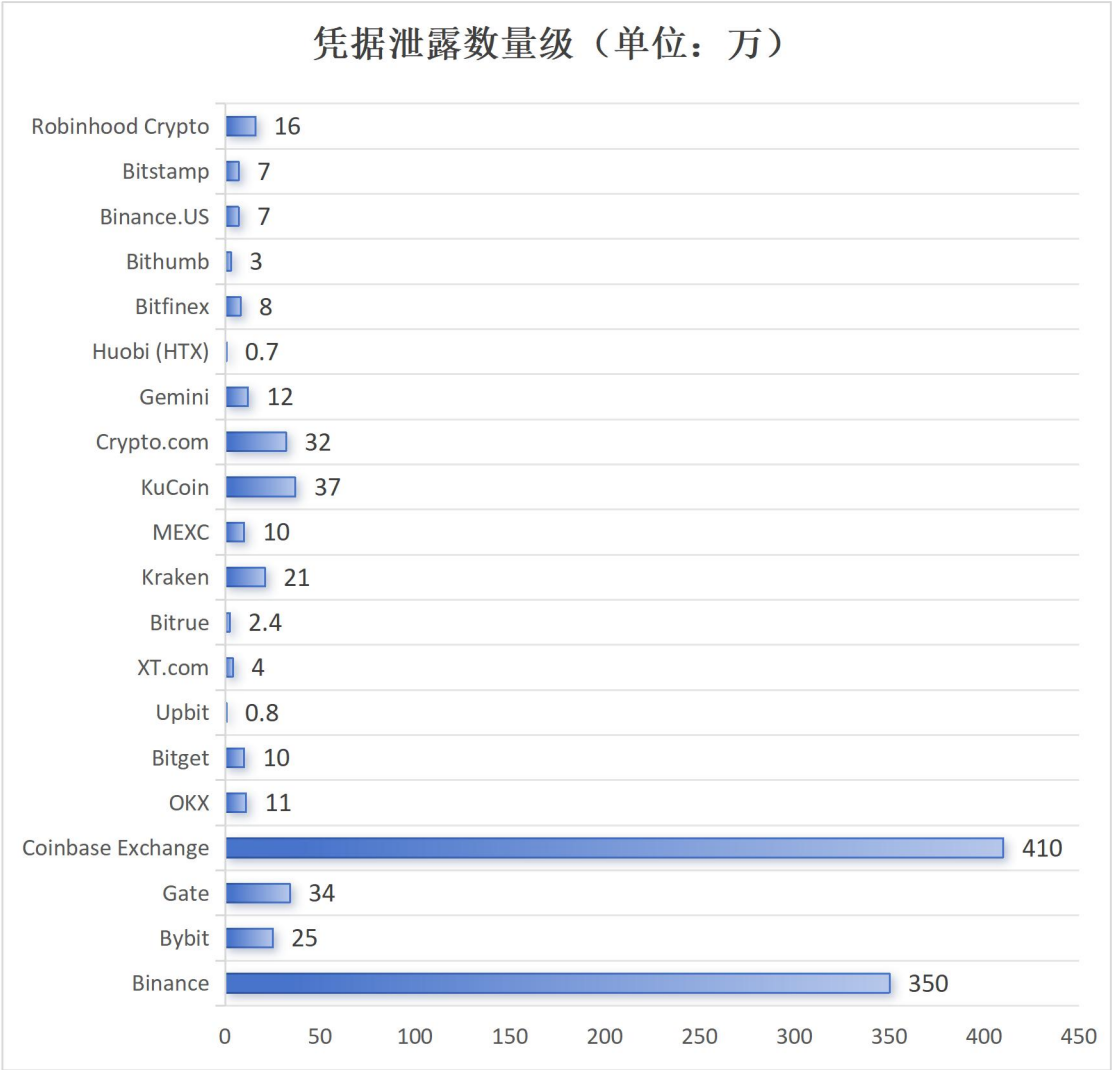
本节所述“凭据泄露”指目前掌握的历史上所有在暗网流通的与该交易所相关的用户名、密码、combo logs、session cookies、浏览器日志等凭据记录。这些凭据**绝大多数并非源于交易所自身数据库被入侵或官方数据外泄**，而是主要来源于用户端感染 Infostealer 恶意软件（如 Lumma、RedLine、Vidar 等）后被批量窃取并上传至 C2 服务器，随后在暗网市场或 Telegram 渠道流通。

零零信安监测到的这些记录，通常是端侧窃取后形成的“stealer logs”或“combo lists”，而非平台侧的批量泄露。因此，本节数据**不代表交易所平台的安全漏洞或内部事件**，而是反映用户端安全意识薄弱、设备感染率高所导致的“周边凭据污染”现象。

所有量级均为公开情报聚合与零零信安抽样监测的估算值，仅供安全研究与风险评估参考，不构成对任何交易所平台的指控或负面评价。

下面我们基于零零信安研究员的暗网监测数据以及公开威胁情报来源，对全球 TOP 级别中心化交易所（CEX）的凭据泄露量级进行统计分析。

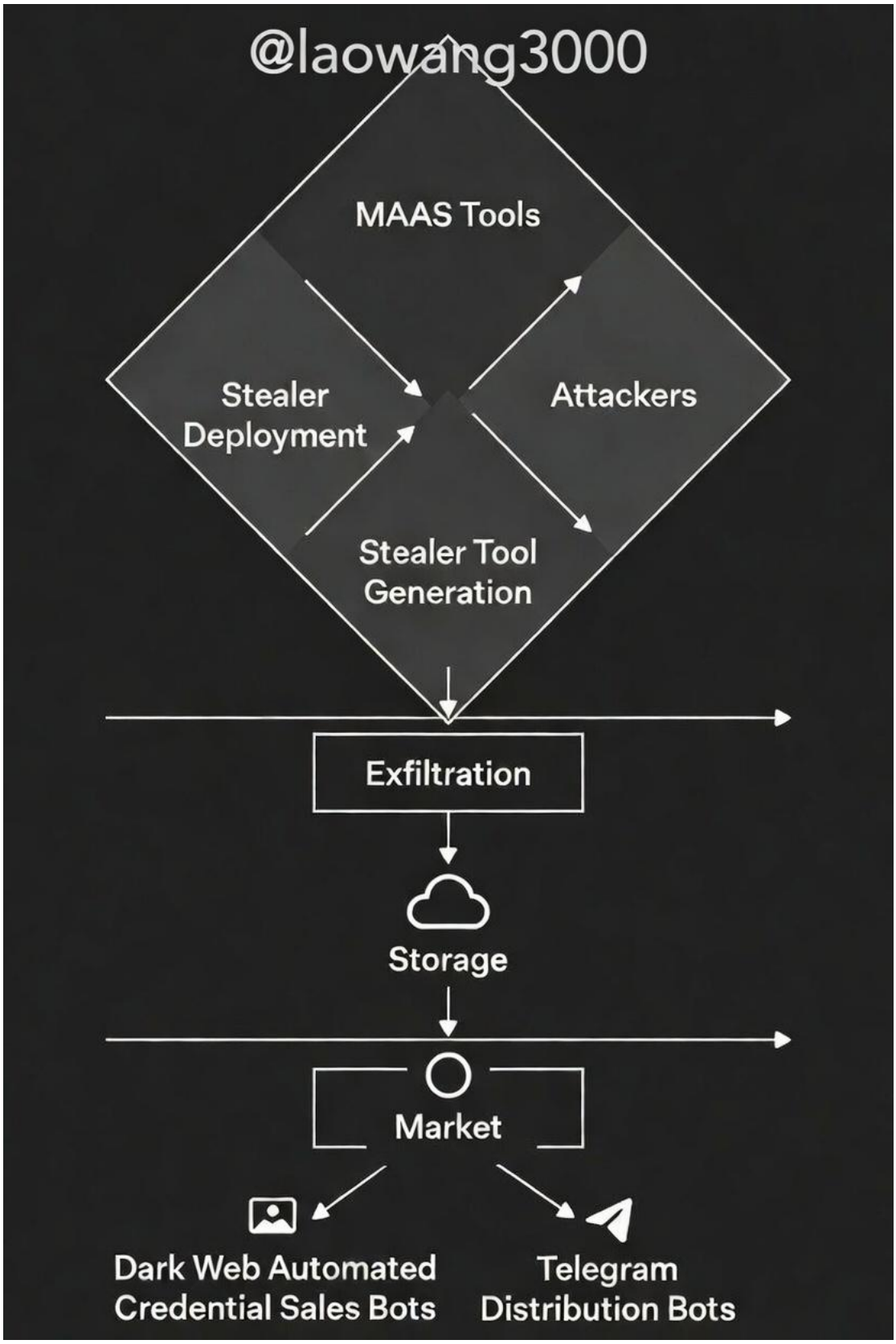
序号	交易所名称	官网	凭据泄露数量级
1	Binance	https://www.binance.com	350 万
2	Bybit	https://www.bybit.com	25 万
3	Gate	https://www.gate.io	34 万
4	Coinbase Exchange	https://www.coinbase.com	410 万
5	OKX	https://www.okx.com	11 万
6	Bitget	https://www.bitget.com	10 万
7	Upbit	https://upbit.com	0.8 万
8	XT.com	https://www.xt.com	4 万
9	Bitrue	https://www.bitrue.com	2.4 万
10	Kraken	https://www.kraken.com	21 万
11	MEXC	https://www.mexc.com	10 万
12	KuCoin	https://www.kucoin.com	37 万
13	Crypto.com	https://crypto.com	32 万
14	Gemini	https://www.gemini.com	12 万
15	Huobi (HTX)	https://www.htx.com	0.7 万
16	Bitfinex	https://www.bitfinex.com	8 万
17	Bithumb	https://www.bithumb.com	3 万
18	Binance.US	https://www.binance.us	7 万
19	Bitstamp	https://www.bitstamp.net	7 万
20	Robinhood Crypto	https://robinhood.com/crypto	16 万


凭据泄露数量级（单位：万）
Robinhood Crypto 16
Bitstamp 7
Binance.US 7
Bithumb 3
Bitfinex 8
Huobi (HTX) 0.7
Gemini 12
Crypto.com 32
KuCoin 37
MEXC 10
Kraken 21
Bitrue 2.4
XT.com 4
Upbit 0.8
Bitget 10
OKX 11
Coinbase Exchange 410
Gate 34
Bybit 25
Binance 350
0 50 100 150 200 250 300 350 400 450

4. 暗网黑市：凭据从窃取到兜售的全链路

4.1. 概述：凭据从窃取到兜售的完整杀伤链路

凭据泄露的整个过程（从 Stealer 工具制作、分发、窃取、传输，到“货物”上架、兜售），已经不再是零散的黑客行为，而是一条高度结构化、可复制、可盈利的地下杀伤链路。这条链路可以用“钻石模型”来清晰描述（见下图），它把攻击者、工具、数据流动和变现环节全部串联起来，形成一个闭环。



从图中可以看出，整个链路的核心是一个“钻石”结构。

4.1.1. 四个主要顶点

- MaaS Tools（恶意软件即服务工具）：攻击者在这里购买或租用现成的 Stealer 面板，获得构建器、订阅服务和控制台。
- Attackers（攻击者）：包括开发者、运营商、affiliates（例如：联盟成员/代理商/加盟者等），他们是链路的驱动者——有人开发工具，有人买来投放，有人负责分销。
- Stealer Tool Generation（Stealer 工具生成）：攻击者使用 MaaS 平台自定义 payload，生成针对浏览器、钱包、Telegram 等的窃取器。
- Stealer Deployment（Stealer 投放）：通过钓鱼邮件、假软件、SEO 投毒、恶意广告等方式，将 Stealer 部署到受害者设备上。

4.1.2. 链路从钻石底部向下流动

1. Exfiltration（数据外传）

Stealer 在受害者设备上运行后，立即把窃取的凭据（密码、cookies、session、种子短语、截屏等）打包成 ZIP，通过 HTTP、Telegram bot 或云存储外传。通常几分钟内，信息就到达攻击者的控制端。

2. Storage（存储）

数据被临时存放在 C2 服务器、Telegram 频道、云盘（如 gofile.io）或专用聚合平台，形成 stealer logs 或 combo lists。这里是链路的“仓库”，也是初步分拣和去重的起点。

3. Market（市场分销网络）

数据进入分销阶段，主要通过两条高速通道：

- Dark Web Automated Credential Sales Bots：暗网市场（如 R 市场）的自动化机器人，负责上架、escrow 交易、PGP 加密、信誉评分和自动交付。
- Telegram Distribution Bots：Telegram 频道（如 D 云风格的 log cloud）的分销机器人，支持免费 sample 引流、付费订阅、bot 自动支付和镜像避封，流通速度最快，门槛最低。

4.1.3. 链路本质：“低成本、高回报、快周转”

- 窃取者投入几百美元租 MaaS 面板，就能批量感染成千上万设备。
- 一条普通 log 可能只卖几美元，但带 crypto 痕迹的 premium log 能卖到数百甚至上千美元。
- 数据从感染到上架售卖，往往不超过 24–48 小时。
- 下游买家（ransomware 团伙、ATO 脚本小子、IAB）接手后，进一步撬动更大收益。

零零信安监测显示，2025-2026Q1 这条链路已**高度工业化**：执法打掉一个平台，新工具和新频道（如 S 软件、D 云、R 市场等）立马填补空缺。

由于一切都依托于暗网技术的匿名性，以至于违法成本之低、风险之小、投入产出比之高，导致大量不法分子前赴后继的进入该“行业”。**凭据不再是“意外泄露”，而是“按需生产、按需销售”的商品。**

4.1.4. 重要警示

本文再次强调，本报告所有内容仅用于技术研究、安全教育以及对 Web3 企业、交易所和用户的风险警示，旨在督促相关方加强自身安全意识与防御手段。非专业安全研究人员或普通用户切勿尝试访问、参与或接触暗网及其相关生态环境。该领域本身就极其危险，充斥恶意软件、诈骗、执法陷阱及个人信息被二次窃取的风险，一旦误入，可能导致严重后果。请务必保持距离，仅通过正规渠道获取安全知识。

4.2. 未知攻焉知防：MaaS 窃取凭据的过程简单到“离谱”

你以为窃取凭据需要高超的黑客技能？错！

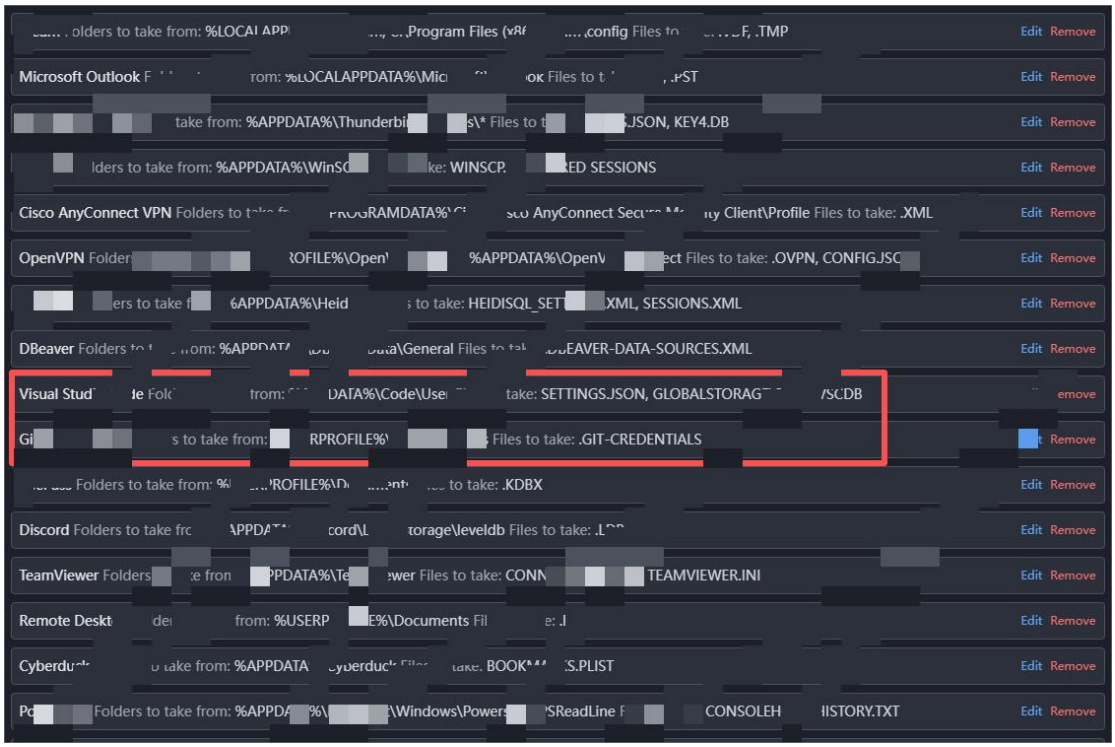
在 MaaS（Malware-as-a-Service）模式下，这个过程简单得像网购一样——注册个账号、选个订阅、点几下鼠标，就能批量“收割”成千上万用户的密码、cookies、钱包种子和 session token。

在成熟的 MaaS 平台上，整个流程“离谱”到：从零起步的攻击者（affiliates），半天内就能部署病毒、看到第一批 Stealer logs。

下面我们来看真实案例：

4.2.1. 他可以“偷”什么？

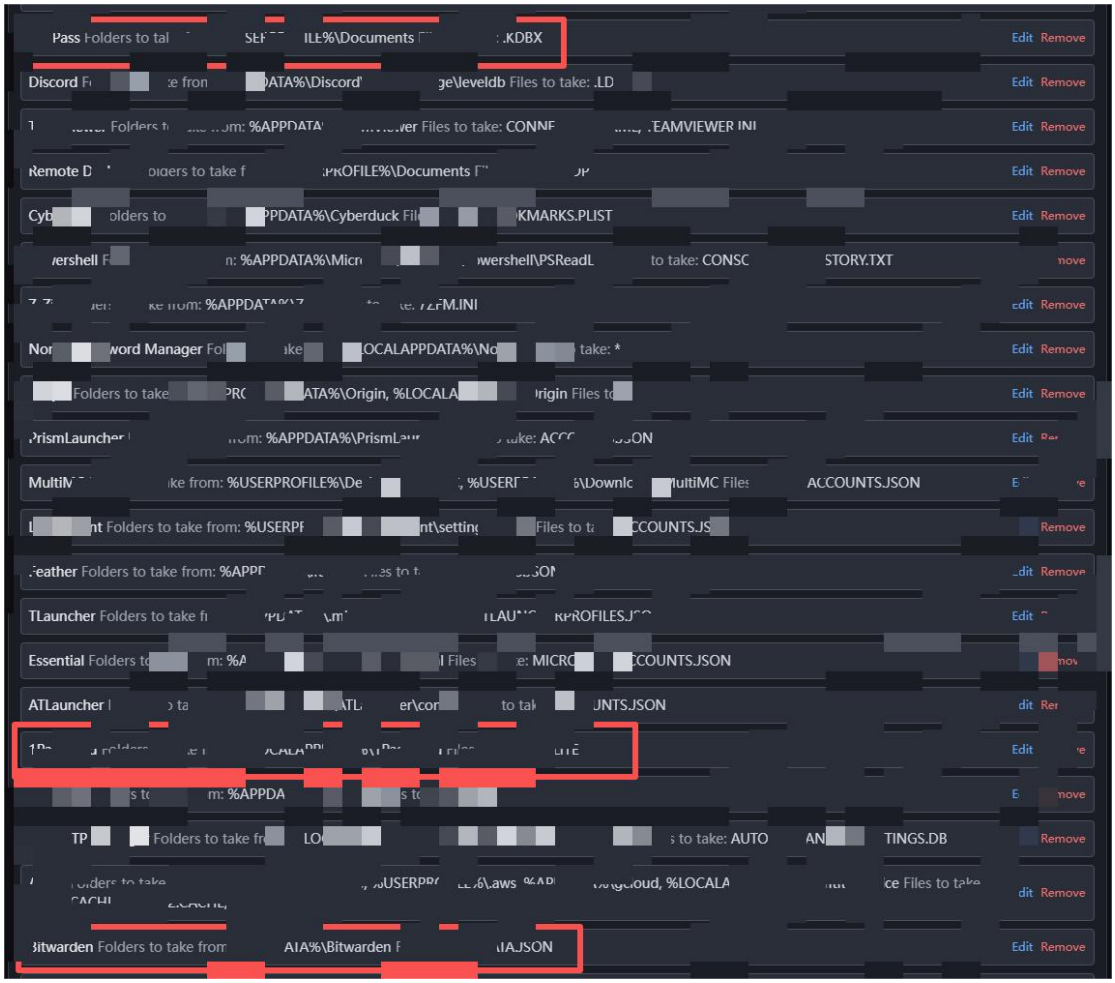
在 MaaS 中，攻击者可以直接勾选所有“想偷走”的东西，这不需要任何技术，“所见即所得”：



最危险的，当属直接与浏览器相关（Browsers & Extensions）的部分：

- Visual Studio Code（含扩展/凭据）：%APPDATA%\Code\User → settings.json, globalStorage/state.vscdb
- Git for Windows：%USERPROFILE%.git-credentials → .git-credentials

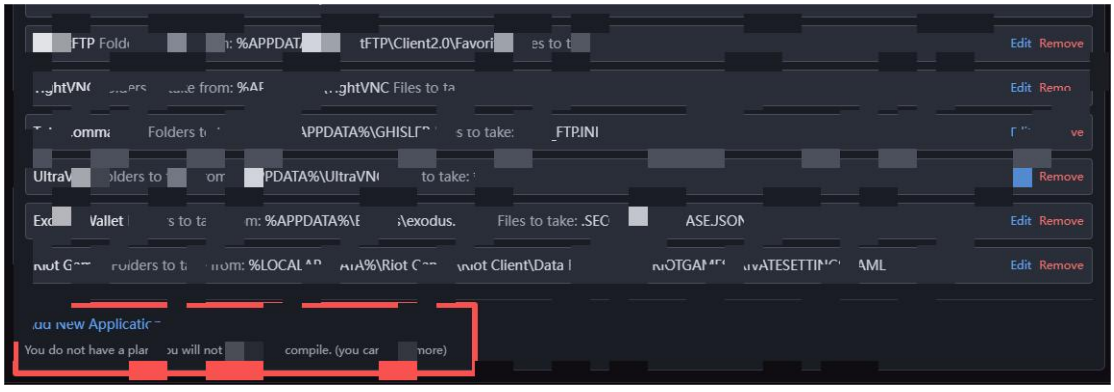
影响：窃取浏览器扩展中的 session cookies、存储的登录凭据（尤其是 crypto 扩展如 MetaMask/Phantom）。攻击者用 cookies 直接绕 MFA 登录交易所/银行/邮箱，实现 ATO（Account Takeover）。浏览器数据是 infostealer 最常见变现路径。



其次，我们还看到了密码管理器（Password Managers）：

- Bitwarden：%APPDATA%\Bitwarden → data.json
- 1Password：%LOCALAPPDATA%\1Password → .sqlite
- KeePass：%USERPROFILE%\Documents → .kdbx

影响：一次性获取所有保存的密码（邮箱、银行、交易所、社交、企业账号）。解锁后攻击者可横向移动、窃取更多数据或勒索。密码管理器被偷=全网沦陷。



当然，除了浏览器和密码管理器之外，我们还可以看到，这里有几十个攻击

者可以默认选择的想“偷取”的东西，包括：各 VPN 凭据、数据库凭据、FTP 凭据、你的游戏凭据、远程桌面管理凭据、邮箱和云的登录凭据等等。甚至如果这些不够，攻击者还可以手动添加其他内容。

除了以上内容，在 MaaS 中，还有数十个配置选项，可以给攻击者更多的选择，包括检索指定文件、保留设备环境信息，甚至可以有多种方式捆绑其他的木马软件，等等。这里就不再意义罗列。

4.2.2. 他怎么“偷”？

在设置完成后，一键点击，MaaS 就能生成攻击者想要的可执行文件，例如：.exe 或.dll 文件等，一般这些文件的体积很小，通常在 500KB~2MB 左右，小巧、隐蔽、杀软检测率低（尤其是用了 AntiVM、内存执行、自定义加密的版本）。攻击者拿到这个文件后，就拥有了一个“现成”的窃取器，随时可以开始“收割”。

接下来，就是投放阶段——怎么把这个“毒药”送到受害者电脑上？

MaaS 工具的设计目标就是让投放简单、低成本、高效率。攻击者（尤其是 affiliates）通常采用两种主流策略：

1. 广撒网式分发（Mass Distribution，高覆盖、低精准）
    - 把.exe 或.dll 等文件伪装成热门软件的破解版、游戏外挂、免费 AI 工具、Office 激活器等。
    - 上传到各种资源站、BT 种子、破解论坛、聊天群组、游戏外挂服务、各类评论区等。
    - 用 SEO 投毒（买关键词广告，让搜索引擎在搜索一些特定内容，例如某些平台或软件时排前面）。
    - 买 Malvertising（恶意广告），在合法网站上投 Google/Facebook Ads，点进去就是下载这个 Stealer。
    - 结果：一天可能感染几百到几千受害者，偷到的 logs 数量爆炸，但平均价值较低。
2. 有针对性钓鱼分发（Targeted Phishing，高价值、高转化）
    - 针对 Web3 用户、交易所玩家、高净值人群或攻击者想针对的一切画像人群定制 payload。

- 发钓鱼邮件：伪装成“交易所安全认证”、“升级通知”、“退税说明或领取”、“紧急通知或软件更新”等，附件可能改名为：“update.exe”、“security.scr”等等。
- 在聊天群组群、各类垂直领域的网站或论坛社群等发钓鱼链接，诱导点击“领取空投”等方式。
- 用社交工程：假冒项目方/客服私信受害者，声称“您的账户有异常活动，请下载这个工具扫描修复”。
- 针对企业/开发者：伪装成 GitHub release 更新、npm 包、VS Code 插件，骗开发人员下载。
- 结果：转化率高，一条 logs 可能就是重要信息或企业凭据，暗网卖价轻松上千美元。

受害者一旦双击运行这个伪装文件：

- Stealer 立即在内存中解密运行（in-memory evasion，文件不落地，杀软难抓）。
- 后台扫描所有目标路径：浏览器日志和扩展、密码管理器（Bitwarden/1Password）、VPN 配置、数据库账号密码、指定需要窃取的文件等。
- 把数据打包成 ZIP，几分钟内通过 Telegram bot 发到攻击者的频道或 MaaS 面板。
- 攻击者坐在电脑前，实时看到新 logs 进来，去暗网或 Telegram 卖掉，或自己动手转走资产。

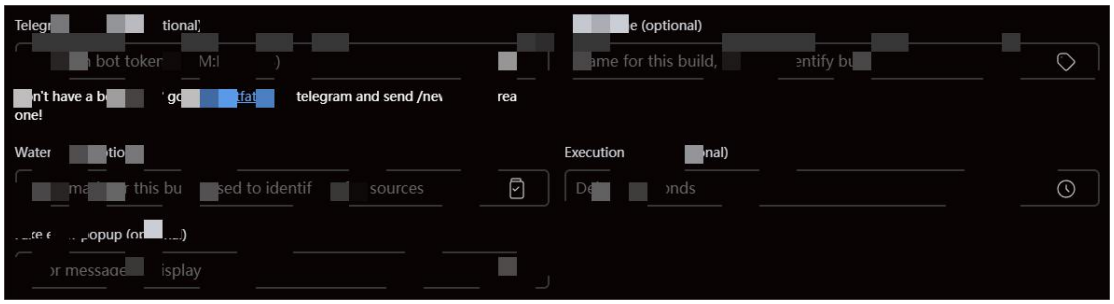
整个“偷”的链条，从点击“生成 Stealer 软件”到受害者资产被转走，最快可能不到 1 小时。

我们在此提醒：这种“简单”不是技术简单，而是人性弱点+工具工业化的结合。普通用户防不住的不是病毒本身，而是“好奇心+贪小便宜”的那一瞬间。

4.2.3. “偷”到以后，他怎么拿走？

Stealer 在受害者电脑上运行后，窃取过程其实已经完成了大半——密码、cookies、种子短语、浏览器扩展数据、钱包文件等都被打包成 ZIP。但这些“战

利品”还躺在受害者设备上，攻击者要真正“拿走”并变现，就靠这一步：数据外传（Exfiltration）。成熟的 MaaS 会把外传做得极其简单、低门槛、实时高效，几乎所有新手攻击者（affiliates）都会优先选 Telegram Bot 方式。我们仍然基于样例来分析：



攻击者仅需要输入 Telegram Bot 的 Token，Stealer 运行后，会把窃取的 ZIP 日志包直接通过这个 Bot 发送到攻击者指定的 Telegram 频道、私聊或群组。

零零信安研究显示，2025 年 Stealer 70%以上都在使用 Telegram 外传——它已成为 infostealer 事实上的“默认通道”。

为什么这个设计“可怕”？

- 整个外传不需要攻击者自己维护服务器，Telegram 就是现成的“快递”。
- 实时性极强：受害者刚输入钱包密码，攻击者几分钟后就能看到种子短语。
- 匿名性高：Bot 可以随时销毁/换新，追踪难度极大。

我们在此提醒：一旦中招，你的浏览器日志（包含登录地址、账号、未加密的密码）/钱包/session 就是在“秒级”被偷走。防不住的不是技术，而是那条 Telegram 通道的便捷。

4.2.4. Stealer 如何过“墙”的？

细心的读者可能发现了一个问题，假如“我”在国内不过“墙”，就无法连接 Telegram，那么数据是如何被“偷走”的？

黑产早就适应了这种限制环境。Stealer 在中国/受限地区投放时，会切换或优先使用不依赖 Telegram 的外传方式，让数据照样被“拿走”。以下列出一些主流的绕过/替代机制：

1. 默认/硬编码 C2 服务器（最常见替代）

- 很多 Stealer 的核心设计本来就支持 HTTP POST 到硬编码 C2（命令与控制服务器）。
  - 构建器里如果没填 Telegram Bot Token，或者攻击者故意不填，Stealer 会 fallback 到面板预设的 C2 IP/域名。
  - 数据打包成 ZIP →分成 10MB 块→通过明文 HTTP 上传到/upload 端点。
- 在中国，这种方式不受 Telegram 屏蔽影响——只要 C2 域名/IP 没被墙（黑产常用 Cloudflare、动态 DNS、Tor 隐藏、或短期域名轮换），就能成功外传。
- 攻击者收到数据后，在 MaaS 面板实时查看/下载（面板本身可能通过代理访问）。

2. 其他云存储/文件托管服务（备用通道）
   - 构建器支持配置云盘外传。Stealer 把 ZIP 上传到这些服务（用预设 API key 或匿名上传），然后把下载链接发回 C2 或通过其他方式通知攻击者。
   - 中国常见：百度网盘、阿里云盘、115 网盘（黑产有时用国内服务伪装）。
3. 国内黑产的“本地化”变种
   - 中国本土或针对华语地区的 Stealer 变种，会直接用国内即时通讯（微信、QQ 等）或自建 C2（阿里云/腾讯云短期）。

零零信安观察：2025 年针对中国用户的 Stealer 投放中，Telegram 外传占比下降到 30%以下，C2 和代理通道成了主流。除了以上列出的方法，还有很多种方法可以将数据发送给攻击者，这里就不再一一列举。总之，“传输”并不是难点。

4.3. 警惕：你的钱是如何被偷走的！

我们回头再看，你的钱包是怎么丢失的？MaaS 工具的核心杀伤力，就在于它把“偷钱”过程工业化、模块化、自动化。攻击者不需要自己写代码，只需在面板里勾选几个选项，就能针对性收割 Web3 用户的资产。下面我们把上面所有

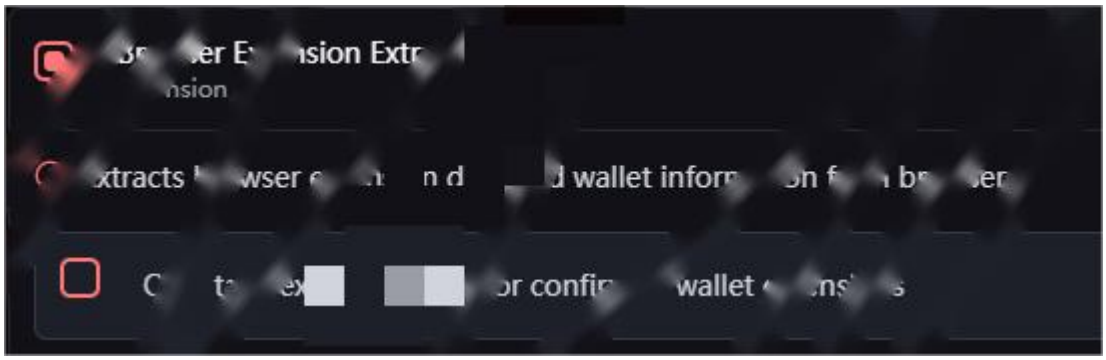
截图中出现的、直接威胁到你的“钱”（加密货币钱包、种子短语、私钥、session token、浏览器扩展等）的配置，全部拎出来，一条条拆解为什么它们致命。

4.3.1. 免责声明与重要提醒

本节内容仅用于专业安全研究、技术讨论与威胁情报分析，旨在帮助 Web3 用户、企业和安全团队了解 Infostealer 恶意软件的常见窃取机制及其对加密资产的致命威胁。所有路径、模块、配置描述均为基于公开情报和合法模拟环境的分析示例，严禁任何个人或组织将本节内容用于非法活动、复制配置、构建/部署恶意软件、实施窃取或任何违反法律法规的行为。

零零信安研究员团队再次强调：任何尝试访问、模拟或参与暗网相关生态的行为都极度危险，可能导致资金损失、个人信息二次泄露乃至法律后果。请务必保持距离，仅通过正规渠道获取安全知识，并将这些信息转化为实际防护措施（如硬件钱包、多签、定期凭据扫描）。违反者后果自负，与本报告及作者无关。

4.3.2. Browser Extension Extractor（浏览器扩展提取器）



- 描述：Extracts browser extension data and wallet information from browsers（从浏览器中提取扩展数据和钱包信息）
- 子选项：Only take extension data for confirmed wallet extensions（仅针对已确认的钱包扩展提取数据）
- 为什么致命：

这个模块是 Web3 的“杀手锏”。它专门扫描 Chrome/Edge/Firefox 等浏览器的扩展文件夹，针对已知 Web3 钱包扩展 ID（如 MetaMask、Phantom、Trust Wallet、Ronin、Binance Chain Wallet、Coinbase Wallet 等）。提取内容：种子短语（seed

phrase）、私钥、恢复短语、账户地址、session token、交易历史等。

- 后果：

攻击者拿到种子/私钥后，直接导入你的钱包，转走所有 USDT/ETH/NFT。Web3 用户最大噩梦——资金不可逆转丢失。

4.3.3. Browser History Extractor（浏览器历史提取器）

- 描述：Saves clipboard and extracts history, downloads, bookmarks, and autofills from browsers（保存剪贴板并从浏览器提取历史、下载、书签、自动填充）
- 子选项（全部威胁 Web3）：
  - Take History（提取浏览历史）
  - Take Bookmarks（提取书签）
  - Take Autofills（提取自动填充，包括保存的密码/钱包地址）
  - Take Download History（提取下载历史，可能含钱包备份或 NFT 文件）
  - Take Clipboard（提取剪贴板，常用于临时复制种子短语/地址）
  - Take Local Storage（提取 localStorage，Web3 扩展常用）
  - Take Session Storage（提取 sessionStorage，含活跃 session token）
- 为什么致命：

  浏览器是 Web3 用户的主要入口（DApp、交易所网页、钱包网页版）。

- Take Clipboard：你复制种子短语/私钥/转账地址的瞬间被抓。
- Take Autofills：浏览器保存的钱包地址、DApp 登录凭据直接被偷。
- Take Local/Session Storage：MetaMask 等扩展的 localStorage 含加密数据或 token，可用于 session hijack。
- Take History/Bookmarks：暴露你访问的 DeFi/NFT 项目、钱包恢复页面、交易所登录记录。

■ 后果：

结合 Browser Extension Extractor，能完整重建你的 Web3 行为，实现账号接管或种子恢复。在未触发重新验证机制的情况下，可能绕过 MFA。

4.3.4. 直接针对桌面钱包的路径扫描（全局默认配置）

这些是列表里最直接的“钱包杀手”：

■ Atomic Wallet：%APPDATA%\Atomic\Local Storage\leveldb → *（所有文件）

热门多链钱包（BTC/ETH/Solana），leveldb 含种子短语、私钥。攻击者导入后转走资产。

■ Electrum Wallet：%APPDATA%\Electrum\wallets → *

老牌 BTC 钱包，wallets 文件夹含种子/私钥。暗网常标“Electrum seed”高价。

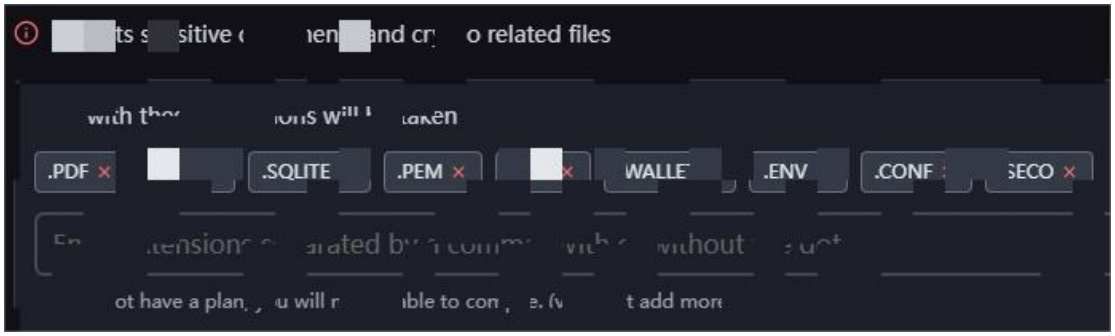
■ Exodus Wallet：%APPDATA%\Exodus\exodus.wallet → .seco, passphrases.json

多链桌面钱包，.seco/passphrases.json 含加密种子。解密后全钱包沦陷。

- Feather Wallet：%APPDATA%\feather → accounts.json

  Monero 隐私币钱包，accounts.json 含账户/种子。转移 XMR 难以追踪。

4.3.5. 全局文件扫描：几乎每一个单词都在瞄准你的“钱”！



这些是 Stealer 在构建器中的“Sensitive Documents and Crypto Related Files”模块（全局文件扫描）的默认配置。攻击者只需保持默认勾选，就能让 Stealer 在受害者电脑上递归搜索所有驱动器，扫描指定扩展名的文件（.PDF、.TXT、.SQLITE、.PEM、.ASC、.WALLET、.ENV、.CONF、.SECO 等），并把匹配的文件全部打包外传。

再看“Keyword Categories Configuration”部分，这里列出了多语言关键词组（主要是英语 + 俄语 + 其他欧洲语言），全部围绕

crypto/wallet/seed/passphrase/mnemonic 等核心概念。这些关键词会被用于文件内容搜索：只要文件名或文件内部出现这些词，Stealer 就会把整个文件抓走。

为什么说“几乎每一个单词都威胁到你的钱”？

因为这个模块的设计目标就是**精准收割 Web3 用户的敏感资产文件**。攻击者不需要自己写搜索逻辑，只需保持默认配置，就能自动命中以下高危目标：

- .WALLET：钱包文件后缀（常见于 Exodus、Atomic、Electrum 等桌面钱包）。
- .SECO：Exodus Wallet 的加密种子文件（passphrases.json 常伴随.seco）。
- .PEM/.ASC：私钥文件（PEM 格式常用于加密货币节点或旧版钱包私钥，ASC 是 PGP 相关但黑产也用）。
- .SQLITE/.DB：数据库文件（如 leveldb、Bitwarden data.json、1Password .sqlite、NordPass .sqlite）。这些常存种子短语、账户数据、恢复信息。
- .ENV：环境配置文件，常含 API key、私钥、钱包助记词（.env 文件在 Web3 项目开发中极常见）。
- .CONF：配置文件（如 AnyDesk、NordVPN、ProtonVPN、OpenVPN 的.conf /user.config），可能含 VPN 凭据或钱包绑定信息。
- .TXT/.PDF：纯文本或 PDF 备份文件，用户常把种子短语、passphrase 记在 TXT 或 PDF 里（最蠢但最常见的泄露方式）。

而关键词组更是赤裸裸的“钱包猎杀清单”：

- crypto / криптo / kripto / krypto / krypto（各种语言的“加密货币”）
- seed / сия / semilla / graines / sementes / tohum（种子短语）
- passphrase / passphrase / фраза / frase / passphrase / parola / cümlesi（助记词密码）
- password / пароль / contraseña / modtdepasse / senha / şifre（通用密码，但常与钱包关联）
- wallet / кошелек / biletera / portefeuille / carteira / cüzdan（钱包）
- wallets / кошельки / billeteras / portefeuilles / briefcases / carteiras / cüzdanlar（复数钱包）
- wallet_backup / wallet backup / резервный кошелек / respaldo / sauvegarde / carteira / backup_carteira / cüzdan yedeği（钱包备

份）

- wallet.dat / wallet.dat（经典 Bitcoin Core / Electrum 钱包文件）
- wallet_recovery / восстановление кошелька / recuperación / recuperação / Wiederherstellung / kurtarma（钱包恢复）
- mnemonic / мнемоническая / mnemotécnico / mnemonic / mnemonisch / mnemônico / mnemonik（助记词）

4.3.6. 小结

这些模块不是“随便扫”，而是针对 Web3 用户量身定制的“钱包收割机”。零零信安分析显示，2025-2026Q1 Web3 损失中，Stealer 占比超 30%，其中浏览器扩展+桌面钱包是最常见来源。以上这些功能中的每一点，几乎都指向你的“钱”。

5. 回顾：2025 年暗网凭据和 Web3 泄露大事件

5.1. 2025 年 Web3 暗网凭据泄露整体态势

根据 Chainalysis《2026 Crypto Crime Report》（基于 2025 全年数据），2025 年为历史损失规模最高年份之一，全球加密货币被盗总额超过 34 亿美元（$3.4 billion）。其中，北韩 Lazarus Group（TraderTraitor）主导的攻击贡献了 20.2 亿美元，同比增长 51%，占全年总损失的近 60%。单一事件——Bybit 交易所 2 月遭受的 15 亿美元史上最大黑客攻击——就占总损失约 44%，凸显大型集中式交易所（CEX）已成为国家行为体首要目标。

凭据泄露已成为 Web3 攻击链路的最上游环节。2025 年 6 月，Cybernews 曝光历史上规模最大的凭据聚合泄露事件：超过 160 亿条登录凭据（16 billion credentials）在暗网或公开渠道流通。这些数据并非单一大型泄露，而是来自 30 多个数据集的聚合，主要源于 LummaC2、RedLine、Stealc 等 infostealer 恶意软件长期感染终端设备后生成的日志。其中大量涉及邮箱+密码组合、会话 cookie，甚至 Web3 钱包相关凭据（API key、种子短语重用密码等），为 credential stuffing、ATO（Account Takeover）和供应链攻击提供了低门槛入口。

暗网与 Telegram 生态加速凭据变现：stealer logs 往往首发于 Telegram 的“云”频道，随后流入付费私云或传统 Tor 市场。情报显示，2025 年 stealer 日志总量激增，Web3 相关凭据（交易所账户、DeFi 协议登录凭据）占比显著上升——约 20-30%的暗网流通 combo log 包含 crypto 关键词。这直接导致凭据滥用成为初始访问向量的主导形式（Verizon DBIR 2025 数据显示，凭据滥用占比超过 50%的勒索软件攻击前兆）。

关键洞察：

凭据攻击占比上升：从合约漏洞转向凭据/供应链/ATO 攻击。

总体而言，2025 年暗网凭据泄露已从“辅助工具”演变为 Web3 生态的核心

威胁源头。传统合约漏洞虽仍存在，但凭据上游链路的低门槛和高效率，让黑产实现了规模化变现。这些宏观态势将在后续子章节通过具体重大事件进一步剖析。

5.2. Web3 大事件：15 亿美元 Bybit 史上最大黑客事件

2025 年 2 月 21 日，迪拜总部加密货币交易所 Bybit 遭受史上最大规模单一加密盗窃事件，损失约 15 亿美元（$1.5 billion）以太坊（ETH）。这一事件被广泛归因于北韩国家支持的黑客组织 Lazarus Group（也称 TraderTraitor 或 APT38），由 FBI、Chainalysis、Elliptic 等多家情报机构确认。该攻击占 2025 年全球加密盗窃总额的约 44%，直接推动全年损失突破$3.4B，标志着国家行为体在 Web3 领域的极端破坏力。

5.2.1. 攻击过程简述

Bybit 使用第三方多签（multisig）钱包解决方案 Safe Wallet 进行冷热钱包转移（从离线冷钱包到在线热钱包）。Lazarus Group 通过高级社会工程学（social engineering）和供应链攻击，针对 Bybit 的冷钱包签名者（包括高管）发起钓鱼攻击，成功入侵 Safe UI 前端代码。攻击者注入恶意 JavaScript，使交易界面显示为正常转移，但实际将 401,000 ETH（当时价值约$1.5B）重定向到其控制的钱包。整个过程发生在例行转移窗口内，绕过多签审核机制，实现了“零感知”盗取。

5.2.2. 暗网凭据泄露在上游链路中的作用

虽然 Bybit 事件核心是供应链+UI 欺骗，但情报显示 Lazarus Group 攻击路径高度依赖凭据上游泄露。北韩黑客长期通过 infostealer 恶意软件（如 RedLine 变体）针对开发者/IT 人员进行凭据窃取，生成 combo logs 在暗网/Telegram 流通。Bybit 事件前，可能已有员工/第三方开发者凭据在 M 云等频道出现，用于初始渗透或钓鱼准备。Chainalysis 报告指出，此类国家行为体攻击往往从“凭据滥用”开始，再升级到供应链操控。这与 2025 年 stealer 日志激增趋势一致：Web3 相关凭据（邮箱+密码、API key）在暗网变现后，成为 ATO 和内部访问的低成本入口。

5.2.3. 后续影响与响应

- Bybit 迅速确认事件未影响用户资金（通过内部储备+桥接贷款覆盖损失），并推出高达 10%赏金计划（lazarusbounty.com），奖励协助追踪/冻结资金者，已支付数百万美元。
- 资金洗钱路径：Lazarus 快速将 ETH 转换为 BTC 等资产，通过 Chainflip 等混币服务分散到数千地址。Chainalysis Reactor 工具帮助希腊等国首次冻结部分资金。
- 市场冲击：事件导致比特币价格短期下跌 20%，重燃对 CEX 安全性的担忧，推动行业加强多签+凭据监控。

5.2.4. 关键教训

Bybit 事件证明，多签和冷钱包并非万无一失——上游凭据泄露+社会工程学可轻松绕过技术防护。Web3 交易所需从“凭据自查”入手：实时监控员工/合作伙伴邮箱在暗网出现、启用 passkey/WebAuthn、限制第三方 UI 依赖。事件也凸显情报闭环重要性：暗网监测可提前预警供应链风险。

这一事件不仅是 2025 年最大单一损失，更是凭据泄露如何放大国家级攻击的典型范例，为后续 DeFi/地缘事件提供了警示。

5.3. Stealer 大事件：160 亿凭据大聚合泄露

2025 年 6 月 18 日，Cybernews 研究团队曝光了历史上规模最大的凭据聚合泄露事件：超过 160 亿条登录凭据（16 billion compromised credentials）在暗网或公开渠道短暂暴露。这些凭据并非来自单一大型数据泄露（如企业服务器被黑），而是 30 多个数据集的聚合，主要源于 infostealer 恶意软件（信息窃取器）长期感染用户设备后生成的日志。该事件被多家媒体（如 CBS News、The Guardian、Axios、Malwarebytes）称为“史上最大凭据泄露”或“蓝图级大规模利用模板”，直接凸显 stealer logs 已成为 2025 年暗网凭据流通的核心引擎。

5.3.1. 事件曝光细节

Cybernews 研究人员发现这些数据集“仅短暂暴露”，但总量惊人：单个数据集规模从 1600 万条到 35 亿条不等，平均约 5.5 亿条。数据类型包括用户名+密码组合、会话 cookie、autofill 信息、浏览器 token，甚至部分 Web3 相关凭据（如交易所登录、钱包 API key 或重用密码）。来源主要为 LummaC2、RedLine、Stealc 等主流 infostealer 家族，这些恶意软件通过钓鱼邮件、破解软件、恶意下载等方式感染设备，悄无声息窃取凭据后上传到 C2 服务器。黑产随后将这些日志重打包、去重、分类，形成“combo lists”在 Telegram 云频道（如 M 云、DAI 云）或付费私云（如 D 云）首发/售卖。

5.3.2. 对 Web3 的影响

虽然该泄露覆盖全球主流平台（Google、Facebook、Apple、Telegram、Meta 等），但 Web3 生态受害尤为严重。情报显示，160 亿条中约 20-30%包含 crypto 关键词（如交易所邮箱+密码 combo、DeFi 协议登录凭据）。这些凭据直接用于 credential stuffing（凭据填充攻击）和 ATO（账号接管）：攻击者用泄露组合尝试登录 Binance、Crypto.com、Coinbase 等 CEX，或重置 2FA，进而窃取资金或绕过多签。Chainalysis 报告指出，2025 年此类上游凭据滥用推动了私钥泄露事件（personal wallet compromise event）占比上升，间接放大 Bybit 等大案的破坏力。亚太地区（HK/SG）影响显著：本地用户重用密码习惯常见，导致跨境电商/金融邮箱 combo 在暗网快速流通。

5.3.3. 后续影响与响应

- 数据集暴露后迅速被镜像/下架，但部分已流入黑产生态，形成“武器化”数据集。
- 多家安全厂商（如 McAfee、F5、Dashlane）发出警报：强调这不是“新泄露”，而是多年积累的“旧凭据+新鲜 stealer logs”重用，呼吁用户启用 MFA、密码管理器、passkey，并检查 HaveIBeenPwned 或类似工具。
- 争议点：部分专家（如 CyberScoop 报道）质疑“16 亿”数字夸大（存在

重叠、旧数据），但共识是：规模虽有争议，但 stealer logs 聚合已成为凭据滥用主流模式。

- 零零信安研判：本次事件泄露的绝大部分数据，为“二手数据”，即：历史上泄露凭据数据集合，并且其中包含大量重复数据。

5.3.4. 关键教训

160 亿凭据事件证明，infostealer 已从“零星威胁”演变为“规模化供应链”。Web3 用户/交易所防护不能仅靠 2FA 或合约审计，必须从源头阻断：实时监控暗网凭据出现、员工设备防护、禁止密码重用。企业级情报订阅可提前发现 combo log 流通，阻断攻击链路。

5.4. Sui 区块链大事件：2.23 亿美元 Cetus Protocol 漏洞攻击

2025 年 5 月 22 日，Sui 区块链上最大的去中心化交易所（DEX）和流动性提供者 Cetus Protocol 遭受重大漏洞攻击，损失约 2.23 亿美元（$223 million）。这一事件是 2025 年 DeFi 领域第二大单笔损失（仅次于 Bybit $1.5B），也是 Sui 生态迄今为止最严重的协议级漏洞攻击。攻击在不到 15 分钟内完成，攻击者通过操纵流动性池抽干了多个池子的资产，包括 SUI、USDC 等主流代币。

5.4.1. 漏洞根因

攻击源于 Cetus 使用的第三方数学库 integer-mate（Move 语言中的整数运算工具库）中的一个 rounding bug（舍入错误）和 integer overflow check 失效（整数溢出检查缺陷）。具体来说，在流动性计算函数（get_delta_a / checked_shlw 操作）中，溢出防护逻辑存在缺陷：当输入极值时，检查函数未能正确检测截断（truncation），导致攻击者能以极少代币（几乎为零）铸造巨额集中流动性位置（CLMM liquidity position），随后从池子中提取远超投入的真实资产。攻击者还部署了无价值 spoof tokens（如 BULLA、MOJO）注入池子，进一步操纵价格曲线和储备计算，实现“以小博大”。

5.4.2. 攻击过程简述

- 攻击者先通过闪贷（flash loan）借入大量 haSUI 等代币，压低池子价格。
- 在极窄价格区间（e.g., 300000 – 300200）开设流动性位置，利用溢出绕过检查，以 1 单位代币获得天量流动性份额。
- 随后批量提取真实资产（如 SUI/USDC），总计抽干多个流动性池。
- 约$60M 资产快速桥接到 Ethereum（通过 Wormhole 等跨链），剩余$162M 在 Sui 链上被冻结（Sui 验证者紧急治理投票暂停合约并冻结）。

5.4.3. 暗网凭据泄露在上游链路中的作用

虽然核心是合约/库级数学漏洞，但情报显示 DeFi 协议攻击往往从开发者/管理员凭据泄露开始。Cetus 作为 Sui 最大 DEX，其团队/贡献者可能面临 infostealer logs 针对（RedLine/LummaC2 等）。暗网流通的 combo log（邮箱+密码）可用于初始渗透、钓鱼或获取代码仓库访问权，导致第三方库依赖未充分审计或代码引入 bug。2025 年 stealer 日志激增背景下，此类上游凭据滥用已成为 DeFi 漏洞利用的“加速器”——黑产先凭据入侵，再利用合约缺陷放大损失。

5.4.4. 后续影响与响应

- Cetus 暂停智能合约 17 天，TVL 从$284M 暴跌至$124M（恢复后流动性池回补 85-99%）。
- 通过社区链上投票、Sui 基金会贷款和多签托管计划，冻结$162M 资金；攻击者部分资产被追踪/冻结。
- 项目提供$6M 赏金（bounty）追捕攻击者，并承诺白帽归还无追责。
- Sui 生态整体受冲击：SUI 代币短期下跌，凸显 Move 语言虽“安全”但依赖第三方库仍存风险。

5.4.5. 关键教训

Cetus 事件证明，DeFi 安全不止于合约审计——第三方库依赖（dependency

trap）是隐形炸弹。Web3 项目需加强供应链审查、数学库审计、代码去重打包防护。同时，上游凭据泄露监控不可或缺：开发者邮箱/凭据在暗网出现，即可预警潜在渗透。企业/协议可利用凭据泄露工具实时自查，阻断攻击链路从凭据到合约的升级。

5.5. 地缘事件：1 亿美元 Nobitex 伊朗交易所政治黑客攻击

2025 年 6 月 18 日，伊朗最大加密货币交易所 Nobitex（诺比特克斯）遭受严重黑客攻击，损失约 9000 万至 1 亿美元（$90-100 million）的加密资产。这一事件不同于典型的金融动机攻击，而是由地缘政治驱动的“破坏性黑客行动”，攻击者自称 Gonjeshke Darande（波斯语“掠食性麻雀”，Predatory Sparrow），一个亲以色列的黑客组织。该组织公开宣称此次行动是为回应伊朗支持的代理势力对以色列的网络攻击和导弹袭击。

5.5.1. 攻击过程简述

攻击者通过内部凭据滥用+供应链渗透获得交易所热钱包和冷钱包的部分控制权。随后，他们执行了大规模资产销毁和转移操作：

- 约$60-70M（被抽走总金额约$90-100 million，销毁约$60-70M）的比特币、以太坊、USDT 等资产被直接发送到“黑洞地址”（无私钥的无效地址，实现永久销毁）。
- 剩余部分被转移到多个混币服务或跨链桥（如 Wormhole 或 LayerZero），快速分散洗白。
- 攻击者同时在 Nobitex 官网和社交渠道发布声明视频，展示销毁过程，并附带政治口号：“这是对伊朗政权网络恐怖主义的回应。”

整个攻击在数小时内完成，Nobitex 紧急下线平台，暂停所有提现和交易。

5.5.2. 暗网凭据泄露在上游链路中的作用

Gonjeshke Darande（与以色列情报机构有传闻关联，但未证实）擅长针对性凭据窃取。情报显示，此类国家支持或准国家黑客组织长期利用 infostealer 恶意

软件（如定制版 RedLine 或 Lazarus 变体）针对伊朗开发者、交易所员工和第三方供应商进行凭据收集。这些凭据在暗网或 Telegram 私人群组短暂流通后，用于初始访问或钓鱼准备。Nobitex 事件前，伊朗加密从业者邮箱+密码 combo log 曾在 M 云等频道出现，疑似为攻击提供了入口。Chainalysis 报告指出，2025 年地缘冲突相关攻击中，凭据滥用占比高达 70%，远高于金融动机攻击。这反映了暗网凭据已成为“混合战争”工具：低成本获取内部访问，再执行高破坏力行动。

5.5.3. 后续影响与响应

- Nobitex 声称用户资金安全（通过保险和内部储备覆盖部分损失），但平台信誉重创，伊朗用户转向 Binance、Bybit 等国际交易所。
- 伊朗官方指责“以色列网络恐怖主义”，并加强国内加密监管。
- 攻击者公开部分资金销毁视频，进一步激化中东网络对抗。
- 全球影响：凸显 CEX 在地缘冲突中的脆弱性，推动行业讨论“国家行为体风险”和“凭据情报预警”。

5.5.4. 关键教训

Nobitex 事件证明，地缘政治冲突下，加密交易所已成为“软目标”——凭据泄露可直接转化为资产销毁或政治宣传。Web3 项目/交易所防护需超出技术层面：

- 加强员工凭据暗网监控（实时预警邮箱 combo log 出现）。
- 实施零信任架构、多层多签、地理分散冷存储。
- 建立情报订阅机制，提前发现针对性泄露。
- 这一事件作为 2025 年“地缘黑客代表”，警示 Web3 行业：凭据泄露不再仅是金融风险，更是国家间对抗的杠杆。

5.6. 其他事件

除了上述标志性大案，2025 年暗网凭据泄露和 Web3 安全事件还包括多起中高影响力的典型案例。这些事件虽单笔损失规模不如 Bybit 或 Cetus，但共同反映

了凭据滥用在不同场景下的普遍性和破坏力。以下选取 4 起代表性事件，按损失规模和类型排序，突出暗网链路的作用。

1. Phemex 热钱包泄露（约$73M，1 月）

北韩黑客组织 Lazarus Group 疑似通过凭据窃取+内部访问入侵 Phemex 热钱包，抽走约 7300 万美元的 BTC 和 ETH。

暗网链路：攻击前，Phemex 员工/第三方开发者邮箱+密码 combo log 曾在 Telegram 云频道短暂流通，用于钓鱼或初始渗透。

教训：热钱包多签虽有防护，但凭据泄露可直接绕过；事件后 Phemex 加强员工凭据监控和零信任架构。

2. Balancer V2 rounding error 漏洞（约$116-128M，11 月）

Balancer 协议 V2 在 Composable Pools 中存在 rounding error（舍入误差）缺陷，导致攻击者通过操纵流动性池价格曲线，抽干多个池子资产。

暗网链路：虽核心为合约数学漏洞，但 Balancer 治理团队部分成员凭据疑似在暗网出现，用于提前访问代码仓库或提案操纵。

教训：DeFi 协议需审计第三方依赖和数学库；上游凭据预警可阻断治理层攻击。

3. Crypto.com ATO 延续风险（多起小规模，累计数百万美元）

Crypto.com 平台 2025 年延续 2024 年账号接管（ATO）问题，多起用户报告资金被盗，涉及邮箱+密码凭据重用和 MFA 疲劳攻击。

暗网链路：大量 Crypto.com 用户 combo log 在 stealer 日志聚合中出现（160 亿凭据事件中占比显著），直接用于 credential stuffing。

教训：CEX 用户凭据重用是 ATO 温床；平台需强制 passkey/WebAuthn，个人需启用暗网自查。

4. Coinbase 数据泄露与潜在补救成本（约$400M 潜在影响，贯穿全年）

Coinbase 报告 2025 年多起内部数据泄露和员工凭据滥用事件，虽未直接导致巨额资金外流，但引发监管调查和潜在集体诉讼，补救/赔偿成本预计高达 4 亿美元。

暗网链路：员工/合作伙伴凭据在 infostealer logs 中流通，用于社会工程学和内部渗透。

教训：合规巨头也易受凭据上游影响；需全员凭据监控+情报订阅。

这些事件的共性：

凭据泄露作为“低门槛入口”，放大合约漏洞、内部访问、地缘攻击等多类风险。

暗网/Telegram 流通速度极快：stealer logs 从感染到售卖往往仅数小时至几天。

亚太影响：香港/新加坡用户在 CEX 和 DeFi 平台凭据重用率高，易成 ATO 目标。

这些“其他事件”虽未进入年度 Top 榜，但累计损失和生态影响不可忽视，共同构成了 2025 年 Web3“凭据疫情”的完整图景。它们进一步印证：暗网情报监测已从“可选”变为“必需”。

5.7. 小结：2025 年教训与 2026 展望

2025 年是 Web3 历史上凭据泄露威胁最为凸显的一年。全年加密资产损失超过 34 亿美元，其中北韩 Lazarus Group 主导的攻击占近 60%，Bybit 单一事件就贡献了 44%。从宏观态势到具体大案，我们清晰看到一个核心事实：暗网凭据泄露已从“辅助风险”升级为 Web3 攻击链路的最上游主导力量。

5.7.1. 2025 年的核心教训

1. 凭据是所有攻击的“零成本入口”

无论是 Bybit 的供应链 UI 欺骗、Cetus 的数学库溢出、Nobitex 的政治销毁，还是 160 亿凭据聚合泄露，攻击路径几乎都可追溯到 infostealer logs 在暗网/Telegram 的流通。stealer 家族（LummaC2、RedLine、Stealc）生成的 combo log 低门槛变现，让黑产实现了“规模化+精准化”打击。2025 年，凭据滥用占比已超过初始访问向量的 50%（Verizon DBIR 数据），远高于合约漏洞。

2. DeFi 与 CEX 的双重脆弱性

DeFi 不再仅是合约风险，开发者/治理凭据泄露可直接操控提案或引入恶意库（Cetus 案例）；CEX 热/冷钱包虽有技术防护，但员工/第三方凭据上游泄露可绕过多签（Bybit、Phemex）。地缘冲突下，交易所更成“软目标”（Nobitex 销毁事件）。

3. Telegram 云与暗网生态的加速器作用

M 云等公开频道首发新鲜 logs，D 云等私云付费订阅加速变现。160 亿凭据聚合事件证明：黑产已形成“窃取 → 聚合 → 售卖 → 利用”的闭环，流通周期从几天缩短到数小时。

4. 亚太/HK/SG 地区的现实冲击

香港和新加坡作为全球 Web3 金融中心，用户重用密码习惯 + 高价值凭据集中，导致 ATO 和私钥泄露事件频发。PDPA/PDPO 强制通知机制虽推动自查，但也暴露了企业/个人防护的滞后。

5.7.2. 2026 年的展望与趋势

1. AI 增强凭据清洗与钓鱼

2026 年，AI 工具将大规模用于清洗 stealer logs（去重、分类、生成个性化钓鱼 payload），进一步降低黑产门槛。预计凭据相关攻击占比将继续上升。

2. 去中心化暗网市场崛起

传统 Tor 市场衰退后，基于 dark web lite（我们暂且叫它“半暗网”） + Monero/XMR 的去中心化凭据交易平台将增多，追踪难度加大。

3. 私钥/种子词泄露仍是最大威胁

个人私钥泄露事件（personal wallet compromise event）占比将持续攀升，单笔金额虽下降，但“广撒网”模式将导致累计损失激增。

4. 防御侧情报闭环成为刚需

2026 年，Web3 项目/交易所/用户将从“被动修复”转向“主动情报驱动”：实时暗网凭据监控、Telegram 预警、ATO 情报订阅将成为标准配置。监管趋严（PDPA/PDPO、全球反洗钱新规）也将推动企业自查需求爆发。

6. 实战指南：交易所和个人如何利用暗网情报保护自己

2025 年的诸多大事件反复证明：暗网情报不再是“高级工具”，而是 Web3 安全的最底层防线。无论是个人钱包被盗，还是交易所被大规模接管，攻击链路几乎都从“凭据泄露”开始。以下从普通用户和企业/交易所两个维度，给出可立即落地的防护方案，说明如何把情报转化为真实防护力。

6.1. 普通用户（个人）防护指南

个人用户最常见的风险路径是：设备感染 Stealer → 日志上传 Telegram 云 → 凭据在暗网售卖 → 账号/钱包被接管。

6.1.1. 重要事实

苹果电脑（macOS）和手机（iOS）用户受到 Stealer 恶意软件的影响远比 Windows 和 Android 安卓用户小得多。根据 2025-2026Q1 多家威胁情报报告（SOCRadar、Flare、Malwarebytes），Windows 系统占 infostealer 感染案例的 90% 以上，而 macOS 感染率远低于 5%，iOS 几乎为 0。这得益于苹果严格的沙箱机制、App Store 审核和系统级权限控制。因此，优先使用苹果设备本身就是一种有效降低风险的方式。

6.1.2. 立即可执行的防护步骤

1. 每周自查一次暗网泄露

在凭据泄露检测平台中，检查你的常用邮箱、手机号、交易所账号等关键词进行查询。如果发现泄露，立即修改密码并启用 passkey。

2. 核心防护习惯（优先级从高到低）

- 弃用密码 + 短信 2FA，全面切换到 passkey / WebAuthn（苹果设备原生

支持，最安全）。

- 使用硬件钱包存储大额资产，冷钱包绝不联网。
- 避免在 Windows 设备上运行破解软件、游戏外挂、盗版工具（Stealer 主要感染源）。
- 开启苹果设备的“锁定模式”（Lockdown Mode），进一步降低针对性攻击风险。

6.2. 企业/交易所防护指南

对企业尤其是交易所来说，单个员工凭据泄露就可能导致全公司风险。2025 年 Bybit、Phemex、Crypto.com 等事件均证明：2FA 再强，也无法解决凭据上游泄露问题。

6.2.1. 关键认知

2FA 绝不是万能解：MFA fatigue 攻击（连续轰炸验证请求）、凭据 stuffing（用暗网泄露组合直接尝试登录）、内部员工凭据被窃取等场景，都能轻松绕过短信/邮件/App 2FA。真正的威胁在“凭据泄露发生的那一刻”，而非登录时。

凭据泄露情报是企业第一道防线：必须在攻击者把日志使用之前就发现并处置。

6.2.2. 企业级实战方案

1. 全员凭据监控（最重要）

对公司所有域名和员工邮箱进行持续监测。一旦检测到任何员工凭据出现在暗网或 Telegram 云（M 云、D 云等），系统会即时推送预警。

2. Telegram 实时情报订阅

使用 Telegram 监测系统 24/7 跟踪 stealer logs、新鲜 combo list、勒索团伙动态，远早于公开新闻曝光。

3. 勒索软件与 ATO 闭环防护

订阅勒索事件监测服务，提前知道 Qilin、TheGentlemen 等团伙正在针对哪

个行业。

4. 技术与流程硬化

强制全员使用 passkey + 硬件密钥（YubiKey）。

实施零信任架构 + 设备指纹验证。

每月进行一次全员暗网凭据自查演练，或在渗透测试自查中加入凭据泄露测试。

暗网情报的真正价值在于把“事后补救”变成“事前阻断”。2025 年教训已经足够多，2026 年，谁能把暗网情报真正用起来，谁就能大幅降低被攻击概率。

7. 总结

经过对 2025 年 Web3 安全生态的全面剖析，我们可以看到一个清晰而严峻的现实：暗网凭据泄露已从边缘风险演变为 Web3 攻击链路的最上游主导力量。这份报告从引言中的“你的密码值多少钱”切入，到真实案例、交易所周边态势、黑市全链路剖析、年度大事件回顾，再到实战防护指南，层层递进地揭示了凭据泄露的工业化、规模化与高回报特性。2025 年已成为 Web3 历史上损失最惨重的一年，根据 Chainalysis 等权威报告，全年加密资产被盗总额超过 34 亿美元（部分来源估算更高达 40 亿美元+），其中北韩 Lazarus Group（TraderTraitor）主导的攻击贡献近 60%，单一 Bybit 事件就占 44%左右。

7.1. 2025 年核心教训提炼

1. 凭据上游是所有攻击的“零成本入口”

无论是 Bybit 的 15 亿美元供应链+社会工程攻击、Cetus Protocol 的 2.23 亿美元整数溢出漏洞、Nobitex 的 9000 万-1 亿美元政治销毁，还是 Crypto.com/Phemex 等平台的 ATO 延续风险，几乎所有重大事件都可追溯到 infostealer（如 LummaC2、RedLine、Stealc）生成的 stealer logs。这些日志在 Telegram 云频道（如 M 云、D 云）和传统暗网市场（如 R 市场）低至几美元流通，却能撬动万倍回报。160 亿凭据聚合泄露事件更是将这一威胁推向极致：非单一 breach，而是多年积累+新鲜 stealer logs 的“武器化”聚合，直接放大 credential stuffing、ATO 和供应链渗透。

2. DeFi 与 CEX 的双重脆弱性暴露无遗

DeFi 不再仅是合约审计问题，开发者/治理凭据上游泄露可引入恶意库或操控提案（Cetus 第三方 math 库 bug）；CEX 热/冷钱包虽有多签防护，但员工/第三方凭据泄露+社会工程即可绕过（Bybit UI 注入、Phemex 热钱包入侵）。地缘冲突下，交易所更成“软目标”（Nobitex 被 Predatory Sparrow 销毁资产+泄露源码）。

3. Telegram“Dark Web Lite”与 MaaS 生态的加速器作用

2025 年 stealer logs 流通周期缩短至数小时：感染→Telegram Bot 外传→云频道首发→Tor 市场/订阅变现。MaaS 模式让攻击门槛低至几百美元订阅面板，Lumma Stealer 等主导市场，针对浏览器扩展、桌面钱包、剪贴板、关键词文件扫描的模块化设计，直接瞄准 Web3 用户“钱包杀手”。

4. 亚太/HK/SG 地区冲击尤为显著

华语用户密码重用率高、设备感染率居高不下，导致 Binance、OKX、Crypto.com 等周边 combo logs 泛滥。香港/新加坡作为 Web3 金融枢纽，ATO 和私钥泄露事件频发，监管（如 PDPA/PDPO）虽推动通知，但企业/个人防护滞后。

5. 2FA/MFA 并非银弹，情报驱动才是底层防线

Infostealer 可窃取 session cookies/token 绕过 2FA，MFA fatigue、社会工程、SIM swapping 等让其失效。报告反复强调：安全不是被动技术堆砌，而是主动情报闭环——实时暗网/Telegram 监测、凭据自查、passkey 迁移、硬件钱包+零信任。

7.2. 2026 年展望与趋势

进入 2026 年，凭据泄露威胁不会消退，反而将进一步工业化与智能化：

1. AI 增强凭据清洗与精准钓鱼

AI 工具将大规模用于去重、分类 stealer logs、生成个性化 payload，攻击效率再上台阶。预计凭据滥用在初始访问向量中的占比将继续攀升至 60%以上。

2. 去中心化/半公开渠道崛起

传统 Tor 市场碎片化后，基于 Monero/XMR 的去中心化交易+更多“Dark Web Lite”平台（如 Telegram 订阅 bot 镜像）将主导，追踪难度加大。Lumma 等 stealer 家族持续迭代，执法打掉一个，新变种立马填补。

3. 私钥/种子词泄露仍是最大杀伤力

个人钱包 compromise 事件占比将持续上升，“广撒网”模式下累计损失激增。浏览器扩展+桌面钱包路径扫描仍是主流，clipper 恶意软件（如 Laplas）与 stealer 结合更致命。

4. 情报闭环与监管双轮驱动

2026 年，Web3 项目/交易所/用户将从“被动修复”转向“主动情报驱动”：暗网情报的企业订阅、Telegram 实时预警、ATO 情报将成为标配。全球反洗钱新规+PDPA/PDPO 强制通知将爆发企业自查需求，passkey/WebAuthn、硬件密钥强制化将成为行业共识。

7.3. 结束语

2025 年的血淋淋教训已足够：你的交易所/钱包密码在暗网可能只值几美元，却能引发数亿美元连锁灾难。Web3 安全的核心已不再是“防黑客入侵”，而是“防凭据上游泄露”。唯有将暗网情报真正融入日常防护——从个人每周自查，到企业全员监控+零信任架构——才能在 2026 年及未来大幅降低被攻击概率。这份报告不是制造恐慌，而是把现实讲透、把防御讲实。感谢每一位读者与贡献者。守护资产，从了解威胁开始；守护生态，从主动情报开始。

8. 免责声明

《2025 年 Web3 安全报告：暗网凭据泄露与威胁情报洞察》（以下简称“本报告”）由零零信安研究员团队基于公开威胁情报、暗网监测数据、行业报告（如 Chainalysis、SpyCloud、Beosin、SlowMist、SOCRadar 等）以及内部合法采集的情报撰写而成。报告旨在为 Web3 用户、交易所、企业安全团队及网络安全从业者提供教育性参考、风险认知与主动防护指导，帮助提升对暗网凭据泄露威胁的理解与防御能力。

重要声明：

1. 仅限合法研究与教育用途

本报告所有内容、数据、示例、链路描述、价格行情、工具提及等，均仅用于专业安全研究、技术讨论、威胁情报分析及风险教育之目的。严禁任何个人或组织将本报告内容用于非法活动，包括但不限于访问暗网市场、购买/使用泄露凭据、实施账号接管（ATO）、凭据填充攻击、窃取资产、传播恶意软件或其他任何违反法律法规的行为。违反者将自行承担全部法律后果，与本报告作者、零零信安及相关贡献者无关。

2. 数据来源与准确性声明

本报告引用的数据来源于公开威胁情报报告、暗网/Telegram 监测样本、行业聚合统计及零零信安合法采集的威胁情报。这些数据可能存在延迟、重复、聚合偏差、二手转售或部分历史数据混入等情况。报告中所有量级估算（如凭据规模、泄露数量、价格区间、事件损失等）均为基于抽样分析与多源交叉验证的合理推断，并非绝对精确值，亦不构成对任何平台、组织或个人的指控或负面评价。作者不对数据完整性、时效性、准确性或适用性作出任何明示或默示保证。

3. 无任何投资、法律或财务建议

本报告不构成任何形式的投资建议、财务建议、法律意见或安全合规咨询。读者在采取任何防护措施、修改账号设置、使用工具或处理潜在泄露时，应自行评估风险，并咨询专业安全顾问、法律顾问或相关机构。任何因参考本报告而导

致的决策、损失、法律责任或其他后果，由读者自行承担。

4. 风险警示

暗网及其相关生态充满极端风险，包括但不限于恶意软件感染、二次诈骗、执法陷阱、个人信息被进一步窃取、资金损失乃至人身安全威胁。普通用户及非专业研究人员切勿尝试访问暗网市场、Telegram 非法频道、Tor 站点或任何提及的地下资源。即使出于好奇或“研究”目的，也可能导致不可逆转的严重后果。

5. 知识产权与使用限制

本报告版权归零零信安及贡献者所有。欢迎在注明出处并保持完整性的前提下，用于非商业性教育、研究或内部培训。禁止任何形式的篡改、商业化转载、用于营销宣传或脱离上下文的片段引用。如需商用或进一步合作，请联系零零信安官方渠道。

6. 责任免除

在法律法规允许的最大范围内，零零信安、报告作者及所有贡献者对因使用或参考本报告而直接或间接造成的任何损失（包括但不限于资金损失、数据泄露、法律责任、商誉损害等）不承担任何责任。本报告“按现状”提供，不附带任何形式的担保，包括但不限于适销性、特定用途适用性或非侵权性的默示担保。

最后提醒：

网络安全的核心在于主动防御与持续警惕，而非依赖单一报告。2025 年的教训已足够惨痛，2026 年及未来，唯有将暗网情报真正转化为日常防护闭环，方能守护资产与生态安全。

请理性阅读、合规使用、远离非法。

9. 关于我们

零零信安（北京零零信安科技有限公司）是中国领先的暗网威胁情报与数据泄露监测专家，专注于暗网情报采集、凭证泄露检测、Stealer Logs 分析、Telegram 实时预警以及 ATO/凭证/PII 威胁情报服务。我们致力于为政府、企业、交易所、Web3 用户及安全团队提供从监测到闭环处置的一站式守护，帮助客户在攻击者行动前发现并阻断风险。

为什么选择零零信安的暗网能力？

- 全域覆盖与深度采集

采用跨协议蜘蛛爬虫系统，无缝监测全球数万个暗网来源，包括国际黑客论坛（Breachforums、D 论坛、L 论坛、X 论坛、E 论坛等）、勒索组织站点（Lockbit、Clop、Qilin、AKIRA 等）以及 Telegram 数据贩卖社群。特别擅长高难度俄语社区和本土中文威胁生态（如长安不夜城、串子会、侵公/查档类群组）。

- Telegram 即时预警与高效集成

深度集成 Telegram 监测，实时处理数百万条消息，支持事件智能分类、关键实体提取（如账户、凭证样本）。新鲜 Stealer Logs 往往首发于 Telegram 云频道，我们提供秒级警报，远早于公开曝光。

- 海量高价值知识库

积累超过 200 亿条经清洗去重的泄露凭证和 Stealer Logs 记录，每日扩展数千万条。支持秒级查询、匹配与订阅预警，涵盖浏览器日志、种子短语、私钥、API key 等 Web3 高危凭证，帮助验证泄露真实性与新鲜度。

- 高保真解析与 AI 增强

运用全镜像复刻技术保留网页布局、附件、图像等多媒体元素，集成 OCR、智能格式化及多模态 AI 分析模型，实现深度向量检索（发布者、国家、发布时间、附件内容等）。结合人工审核与知识图谱关联，将海量原始情报精炼为高价值事件。

- 中文威胁环境优化

深度 AI 优化中文黑话解读（如“老密”“寻条”“开盒”），针对华语暗网平台及 Telegram 社群提供精准防护，特别适合亚太/Web3 用户与企业。

■ 闭环处置支持

不止于监测，我们提供泄露事件真实性研判、样例/全量数据获取、危机应对指导（协商、支付建议）及证据提交支持，帮助降低经济损失与合规风险。

多年来，我们与众多金融企业、大型互联网企业、高科技企业、Web3 交易所等企业合作，并持续发布《全球数据泄露态势月度报告》和《暗网数据泄露日报》，开源情报系统监测约 10 万+威胁源，已成为行业暗网情报的重要参考来源。

零零信安不是单纯的“情报提供者”，而是您的“暗网前哨”——比攻击者更快一步发现风险，守护数字资产安全。

简体中文版 PDF 报告下载地址：

https://static.0.zone/6b173d8297b941fa71714926defbd88c.pdf

联系我们

暗网情报平台：https://darkweb.vip

零零信安官网：https://00sec.com

官方 X（Twitter）：@00seccom

感谢您阅读这份报告。欢迎随时交流，一起构建更安全的 Web3 生态。

零零信安团队

2026 年 3 月