Chainalysis报告：为何被盗资金和勒索软件不断增加

来源：Chainalysis；编译：陶朱，本站

## 摘要

今年迄今为止，链上非法活动总量下降了近 20%，表明合法活动的增长速度快于非法活动。

尽管与去年同期相比，非法交易有所减少，但两类非法活动——被盗资金和勒索软件——却在增加。具体来说，被盗资金流入量几乎翻了一番，从 8.57 亿美元增至 15.8 亿美元，而勒索软件流入量增长了约 2%，从 4.491 亿美元增至 4.598 亿美元。

## 被盗资金

每次抢劫案中被盗的加密货币平均数量增加了近 80%。

部分原因是比特币 (BTC) 价格上涨，比特币占这些抢劫案总交易量的 40%。加密货币窃贼似乎也回归本源，更频繁地瞄准中心化交易所，而不是优先考虑 DeFi 协议，后者是交易 BTC 的不太受欢迎的工具。

包括与朝鲜有关的 IT 工作者在内的高级网络犯罪分子越来越多地利用社会工程等链下方法，通过渗透加密相关服务来窃取资金。

## 勒索软件

2024 年将成为勒索软件支付收入最高的一年，这在很大程度上是由于这些勒索软件发起的高调攻击较少，但收取的赎金却很大（业内称为“大猎物狩猎”）。2024 年出现了有史以来最大的勒索软件支付，约 7500 万美元支付给 Dark Angels 勒索软件组织。

支付给勒索软件的平均赎金已从 2023 年初的不到 20 万美元飙升至 2024 年 6 月中旬的 150 万美元，这表明这些勒索软件优先针对的是大型企业和关键基础设施提供商，这些提供商可能更有可能支付高额赎金，因为它们资金雄厚且具有系统重要性。

由于最近执法部门对 ALPHV/BlackCat 和 LockBit 等最大参与者的干扰，勒索软件生态系统经历了一些分裂。在这些中断之后，一些分支机构已转向效果较差的病毒或推出自己的病毒。

2024 年，加密货币生态系统取得了许多积极的发展。在美国批准了现货比特币和以太坊交易所交易基金 (ETF) 以及美国财务会计准则委员会 (FASB) 修订了公平会计规则之后，加密货币在许多方面继续获得主流认可。但与任何新技术一样，无论是好人还是坏人，采用加密货币的人数都会增加。虽然今年迄今为止 (YTD) 的非法活动与前几年相比有所下降，但特定网络犯罪相关实体的加密货币流入显示出一些令人担忧的趋势。

如下图所示，今年到目前为止，合法服务的流入量是自 2021 年（上一次牛市高峰）以来的最高水平。这一令人鼓舞的迹象表明，加密货币在全球范围内将继续被采用。流入高风险服务的资金（主要由不收集 KYC 信息的混合器和交易所组成）的趋势比去年同期更高。与此同时，今年迄今非法活动总额下降了 19.6%，从 209 亿美元降至 167 亿美元，表明链上合法活动的增长速度快于非法活动。与往常一样，我们必须提醒大家，这些非法数字是基于我们今天发现的非法地址流入量得出的下限估计值。随着时间的推移，随着我们归类更多非法地址并将其历史活动纳入我们的数据，这些总数几乎肯定会更高。



今年另一个重要更新是，我们已开始根据 Chainalysis Signals 数据将可疑的非法活动纳入某些犯罪类型的总体估计中。此前，我们的估计仅包括与 Chainalysis 有支持文件证明其属于某个非法实体的地址相关的总数。Signals 利用链上数据和启发式方法来识别特定未知地址或地址集群的可疑类别，置信度范围从可能到几乎确定。Signals 的引入不仅随着时间的推移增加了我们对某些类别非法活动的估计，而且使我们能够改进前几年的估计，因为有更多的时间来收集输入并了解可疑活动的链上模式。随着不良行为者继续发展他们的策略，我们的检测和破坏方法也将随之发展。

尽管与去年同期相比，非法交易总体有所下降，但两种值得注意的非法活动——被盗资金和勒索软件——一直在增加。加密货币盗窃案中被盗资金同比增长，截至 7 月底，几乎从 8.57 亿美元翻了一番，达到 15.8 亿美元。在去年的年中更新中，截至 2023 年 6 月，勒索软件流入总额为 4.491 亿美元。今年，同期勒索软件流入量已超过 4.598 亿美元，这表明我们可能会看到勒索软件的又一个创纪录年份。

## 攻击者重回，瞄准中心化交易所，被盗资金激增

与 2022 年相比，2023 年被盗加密货币价值下降了 50%，而今年黑客活动又重新兴起。比较被盗金额和黑客事件的同比数量，这很能说明问题。如下图所示，截至 7 月底，今年被盗累计价值已达到 15.8 亿美元，比去年同期被盗价值高出约 84.4%。有趣的是，2024 年黑客事件的数量仅略高于 2023 年，同比仅增长 2.76%。根据被盗时的资产价值，每起事件的平均被盗价值增加了 79.46%，从 2023 年 1 月至 7 月的每起事件 590 万美元增加到 2024 年迄今为止的每起事件 1060 万美元。



被盗价值的变化很大程度上归因于资产价格上涨。例如，比特币的价格从 2023 年前七个月的平均价格 26,141 美元上涨到今年截至 7 月的平均价格 60,091 美元，涨幅达 130%。

比特币的价格在这里尤为重要。Chainalysis 跟踪的一项黑客指标是黑客攻击发生后与被盗资金流动相关的交易量。这可以作为被盗资产的替代指标，因为很多时候被黑客入侵的服务不会公开报告被盗资产的明细。去年，这笔交易量的 30% 与比特币有关。今年，与被盗资金活动相关的 BTC 交易量占这些流量的 40%。这种模式似乎是由被入侵实体类型的变化所驱动的，2024 年中心化服务被黑客入侵以获取高额资金。DMM 等中心化交易所尤其如此，其损失了 3.05 亿美元。据报道，在 DMM 黑客攻击中，约有 4500 个 BTC 被盗，约占 2024 年被黑客攻击价值的 19%。

加密货币窃贼似乎又回到了他们从前的操作，在四年前专注于去中心化交易所（通常不交易比特币）之后，再次瞄准了中心化交易所。



虽然针对 DeFi 服务（尤其是跨链桥）的攻击在 2022 年达到顶峰，但我们推测，在中心化交易所增加了安全投资后，攻击者已将注意力转向了更新、更易受攻击的组织。现在，包括与朝鲜有关的攻击者在内的攻击者正在利用越来越复杂的社会工程策略（包括申请 IT 工作）来窃取加密货币，方法是渗透到中心化交易所中他们历史上最主要的攻击目标之一。联合国最近报告称，西方科技行业公司已雇用了 4,000 多名朝鲜人。

## 2024 年有望成为迄今为止勒索软件收入最高的一年

2023 年，勒索软件创下了超过 10 亿美元的赎金记录。这些巨额赎金来自引人注目的破坏性攻击，例如对 MoveIT 零日漏洞的 Cl0p 攻击和 ALPHV/BlackCat 勒索软件组织对凯撒酒店物业的攻击，导致该公司支付了 1500 万美元的赎金。[1] 尽管执法部门针对勒索软件部署者恶意软件和组织基础设施采取了重大行动，但这些支付仍然发生了。去年此时，我们报告称，截至 2023 年 6 月底，累计勒索软件支付约为 4.491 亿美元。今年同期，我们记录的赎金总额为 4.598 亿美元，2024 年有望成为有记录以来最糟糕的一年。

Kiva Consulting 总法律顾问 Andrew Davis 表示，尽管 LockBit 和 ALPHV/BlackCat 造成了破坏，但勒索软件活动仍然保持相对稳定。 “无论是这些知名威胁行为者行动的前分支机构，还是新崛起的勒索软件组织，大量新的勒索软件组织都加入了竞争，展示了实施攻击的新方法和技术，例如扩大其初始访问手段和横向移动方法。”

如下图所示，勒索软件攻击也明显变得更加严重。一个显著的变化是，我们在一年内观察到的最高赎金支付额激增。到目前为止，2024 年出现了有史以来最大的单笔支付，约为 7500 万美元，支付对象是一个名为 Dark Angels 的勒索软件组织。最高支付额的这一跃升也代表了 2023 年最高支付额同比增长 96%，比 2022 年的最高支付额增长 335%。



如果最高支付金额的快速增长还不够糟糕的话，更令人沮丧的是，每年异常值的这种趋势实际上反映了中位数支付的增长趋势。这种趋势在最具破坏性的勒索软件事件中尤其常见。为了达到这一点，我们根据链上活动水平将所有病毒株分为以下几类：

极高严重程度的病毒：在给定年份收到的最高付款超过 100 万美元

高严重程度的病毒：在给定年份收到的最高付款在 10 万至 100 万美元之间

中等严重程度的病毒：在给定年份收到的最高付款在 1 万至 10 万美元之间

低至中等严重程度的病毒：在给定年份收到的最高付款在 1 千至 1 万美元之间

低严重程度的病毒：在给定年份收到的最高付款少于 1 千美元

利用这一分类系统，我们可以跟踪不同严重程度的中位支付金额随时间推移的异常增长。这种上升趋势在“极高严重程度”的病毒株中尤为明显，其中位支付金额已从 2023 年第一周的 198,939 美元增加到 2024 年 6 月中旬的 150 万美元。这意味着在此期间，最严重病毒株类型支付的赎金通常增加了 7.9 倍，自 2021 年初以来增加了近 1200 倍。这种模式可能表明，这些病毒株开始针对较大的企业和关键基础设施提供商，由于这些目标财力雄厚且具有系统重要性，它们可能更有可能支付巨额赎金。



然而，如下图所示，严重程度最高的勒索病毒株的表现仍低于 2023 年迄今总量 50.8%。这可能归因于最大的参与者 ALPHV/BlackCat 和 LockBit 的执法干扰，这导致勒索软件运营一度停止。在这些干扰之后，生态系统变得更加分散，关联方迁移到效率较低的勒索病毒株或推出自己的勒索病毒株。因此，严重程度较高的勒索病毒株的年初至今活动增加了 104.8%



勒索软件的另一个趋势是，攻击也变得越来越频繁，根据 eCrime.ch 的数据泄露网站统计数据，今年迄今为止的攻击次数至少增加了 10%。值得注意的是，尽管今年的赎金总额有望创下历史新高，赎金金额也创下了历史新高，攻击形势也日益恶化，但仍有一线好消息。在所有这些不利因素中，受害者支付赎金的频率仍然较低。勒索软件泄露网站的帖子数量作为勒索软件事件的衡量标准同比增长了 10%，如果有更多受害者受到威胁，我们预计会出现这种情况。然而，按链上衡量的勒索软件支付事件总数同比下降了 27.29%。将这两个趋势结合起来看，表明虽然今年迄今为止的攻击次数可能有所增加，但支付率却同比下降。这对生态系统来说是一个积极的信号，表明受害者可能准备得更充分，不需要支付赎金。

戴维斯表示：“在基伍组织协助受害组织处理的问题中，约有 65% 已经得到解决，无需支付赎金。受影响组织继续保持积极的恢复趋势，无需向攻击者支付赎金。”



虽然加密生态系统中的非法活动继续呈下降趋势，但两种加密犯罪似乎逆势而上：资金被盗和勒索软件。值得注意的是，这两种犯罪类型往往是由具有某些共同特征的行为者实施的。他们通常是利用复杂网络基础设施的有组织团体。在资金被盗案件中，与朝鲜有关的黑客组织是一些最大抢劫案的幕后黑手。众所周知，这些行为者采用精心策划的社会工程策略闯入加密企业，窃取加密资产，并利用专业的洗钱技术，试图在资金被扣押之前套现。

打击网络犯罪的关键是破坏其供应链，包括攻击者、关联公司、合作伙伴、基础设施服务提供商、洗钱者和套现点。由于加密抢劫和勒索软件的运作几乎完全在区块链上进行，因此拥有正确解决方案的执法部门可以追踪资金，以更好地了解和破坏这些行为者的运作。 eCrime.ch 研究员 Corsin Camichel 表示：“我认为‘克罗诺斯行动’、‘猎鸭行动’和‘终局行动’等打击和执法行动对于遏制这些活动以及表明犯罪行为必将产生后果至关重要。”