起底史上最大胆的加密货币盗窃团伙 黑客组织Lazarus Group洗钱分析

来源：Beosin

此前，路透社获得的一份联合国机密报告显示，朝鲜黑客团伙Lazarus Group去年从一家加密货币交易所窃取资金后，今年 3 月份通过虚拟货币平台 Tornado Cash 洗钱 1.475 亿美元。

监察员在之前提交的一份文件中告诉联合国安理会制裁委员会，他们一直在调查 2017 年至 2024 年间发生的 97 起疑似朝鲜黑客针对加密货币公司的网络攻击，价值约 36 亿美元。其中包括去年年底的一次攻击，HTX 加密货币交易所的 1.475 亿美元被盗，然后在今年3月完成洗钱。

美国于 2022 年对 Tornado Cash 实施制裁， 2023 年，其两名联合创始人被指控协助洗钱超过 10亿美元，其中包括与朝鲜有关的网络犯罪组织Lazarus Group。

根据加密货币侦探 ZachXBT 的调查，Lazarus Group在 2020年 8 月至 2023 年 10月期间将价值 2 亿美元的加密货币洗钱为法定货币。

在网络安全领域，Lazarus Group长期以来一直被指控进行大规模的网络攻击和金融犯罪。他们的目标不仅仅限于特定行业或地区，而是遍布全球，从银行系统到加密货币交易所，从政府机构到私人企业。接下来，我们将重点分析几个典型的攻击案例，揭示Lazarus Group如何通过其复杂的策略和技术手段，成功实施了这些惊人的攻击。

## LazarusGroup操纵社会工程和网络钓鱼攻击

这个案例来自于欧洲相关媒体报道，Lazarus 此前将欧洲和中东的军事和航空航天公司作为目标，在 LinkedIn 等平台上发布招聘广告来欺骗员工，要求求职者下载部署了可执行文件的 PDF ，然后实施钓鱼攻击。

社会工程和网络钓鱼攻击都试图利用心理操纵来诱骗受害者放松警惕，并执行诸如点击链接或下载文件之类的行为，从而危及他们的安全。

他们的恶意软件使特工能够瞄准受害者系统中的漏洞并窃取敏感信息。

Lazarus 在针对加密货币支付提供商 CoinsPaid 的为期六个月的行动中使用了类似的方法，导致CoinsPaid被盗 3700万美元。

在整个活动过程中，它向工程师发送了虚假的工作机会，发起了分布式拒绝服务等技术攻击，以及提交许多可能的密码进行暴力破解。

## 制造CoinBerry、Unibright等攻击事件

2020年 8 月 24 日，加拿大加密货币交易所 CoinBerry 钱包被盗。

黑客地址：

0xA06957c9C8871ff248326A1DA552213AB26A11AE

2020年 9 月 11 日，Unbright 由于私钥泄露，团队控制的多个钱包中发生了 40万美元的未经授权的转账。

黑客地址：

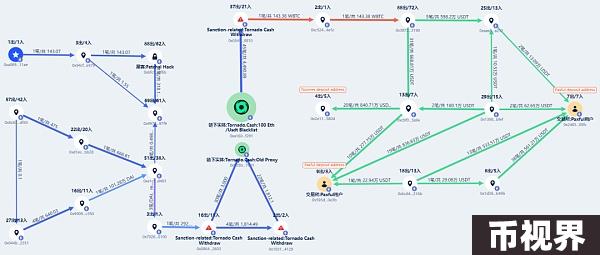
0x6C6357F30FCc3517c2E7876BC609e6d7d5b0Df43

2020年 10月 6 日，由于安全漏洞，CoinMetro热钱包中未经授权转移了价值 75 万美元的加密资产。

黑客地址：

0x044bf69ae74fcd8d1fc11da28adbad82bbb42351

Beosin KYT:被盗资金流向图



2021年初，各个攻击事件的资金汇集到了以下地址：

0x0864b5ef4d8086cd0062306f39adea5da5bd2603。

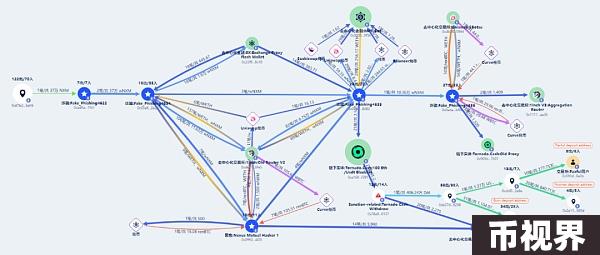
2021年1月11日，0x0864b5地址在Tornado Cash存入了3000ETH，随后再次通过0x1031ffaf5d00c6bc1ee0978eb7ec196b1d164129地址向Tornado Cash存入了1800多枚ETH。

随后在1月11日至1月15日，陆续从Tornado Cash中提取了近4500枚ETH到0x05492cbc8fb228103744ecca0df62473b2858810地址。

到2023年，攻击者经过多次转移兑换，最终汇集到了其他安全事件资金归集提现的地址，根据资金追踪图可以看到，攻击者陆续将盗取的资金发送至Noones deposit address以及Paxful deposit address。

## NexusMutual创始人(HughKarp)遭黑客攻击

2020年 12 月 14 日，Nexus Mutual 创始人 Hugh Karp 被盗37万NXM（830万美元）。



Beosin KYT:被盗资金流向图

被盗资金在下面几个地址之间转移，并且兑换为其他资金。

0xad6a4ace6dcc21c93ca9dbc8a21c7d3a726c1fb1

0x03e89f2e1ebcea5d94c1b530f638cea3950c2e2b

0x09923e35f19687a524bbca7d42b92b6748534f25

0x0784051d5136a5ccb47ddb3a15243890f5268482

0x0adab45946372c2be1b94eead4b385210a8ebf0b

Lazarus Group通过这几个地址进行了资金混淆、分散、归集等操作。例如，部分资金通过跨链到比特币链上，再通过一系列转移跨回以太坊链上，之后通过混币平台进行混币，再将资金发送至提现平台。

2020年12月16日-12月20日，其中一个黑客地址0x078405将超2500ETH发送至Tornado Cash，几个小时之后，根据特征关联，可以发现0x78a9903af04c8e887df5290c91917f71ae028137地址便开始了提款操作。

黑客通过转移以及兑换，将部分资金转移至上一个事件涉及的资金归集提现的地址。

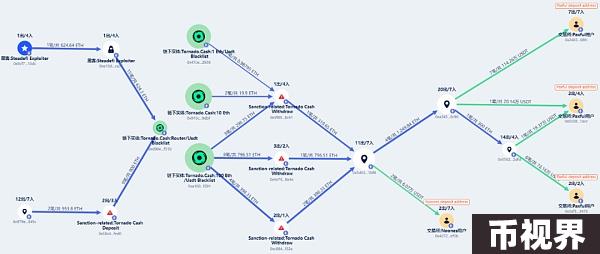
之后，2021年5月-7月，攻击者将1100万USDT转入Bixin deposit address。

2023年2月-3月，攻击者通过0xcbf04b011eebc684d380db5f8e661685150e3a9e地址，将277万USDT发送到Paxful deposit address。

2023年4月-6月，攻击者通过0xcbf04b011eebc684d380db5f8e661685150e3a9e地址，将840万USDT发送到Noones deposit address。

## Steadefi和CoinShift黑客攻击

Beosin KYT:被盗资金流向图



Steadefi事件攻击地址

0x9cf71f2ff126b9743319b60d2d873f0e508810dc

Coinshift事件攻击地址

0x979ec2af1aa190143d294b0bfc7ec35d169d845c

2023年8月，Steadefi事件的624枚被盗ETH被转移到Tornado Cash，同一个月，Coinshift事件的900枚被盗ETH被转移到Tornado Cash。

在转移ETH到Tornado Cash之后，立即陆续将资金提取到下面地址：

0x9f8941cd7229aa3047f05a7ee25c7ce13cbb8c41

0x4e75c46c299ddc74bac808a34a778c863bb59a4e

0xc884cf2fb3420420ed1f3578eaecbde53468f32e

2023年10月12日，上述三个地址将从Tornado Cash提取的资金都发送到了0x5d65aeb2bd903bee822b7069c1c52de838f11bf8地址上。

2023年11月，0x5d65ae地址开始转移资金，最终通过中转和兑换，将资金发送到了Paxful deposit address以及Noones deposit address。

## 事件总结

以上介绍了朝鲜黑客Lazarus Group过往几年的动态，并对其洗钱的方式进行了分析与总结：Lazarus Group在盗取加密资产后，基本是通过来回跨链再转入Tornado Cash等混币器的方式进行资金混淆。在混淆之后，Lazarus Group将被盗资产提取到目标地址并发送到固定的一些地址群进行提现操作。此前被盗的加密资产基本上都是存入Paxful deposit address以及Noones deposit address，然后通过OTC服务将加密资产换为法币。

在Lazarus Group连续、大规模的攻击下，Web3行业面临着较大的安全挑战。