Stormous 勒索软件家族简介

Stormous 勒索软件基本信息

Stormous 勒索软件最早出现于 2021 年中期，是一款采用勒索软件即服务（RaaS）模式运营的双重勒索软件。该团伙对外发布的一些帖子是使用阿拉伯语撰写而成，因此推测团伙的成员可能位于中东国家和北非地区。Stormous 勒索软件利用了俄罗斯与乌克兰紧张局势的升级，公开表示支持俄罗斯，这种策略与 Conti 勒索软件的行为类似，被认为旨在吸引公众关注，加大该团伙的影响力。该团伙擅长利用鱼叉式钓鱼技术或已知漏洞来攻击受害组织/企业网络，截至 2024 年 10 月，Stormous 勒索团伙已成功攻击了 172 个组织和企业，影响了包括古巴、阿根廷、波兰、中国、黎巴嫩、以色列、乌兹别克斯坦、印度、南非、巴西、摩洛哥等 40 多个国家。受害行业广泛，其中信息技术、教育、制造业、政府、交通、能源、法律、房地产和电信行业受到的影响最为严重。

Stormous 勒索软件的攻击行动存在很大的争议，因为被该勒索软件组织公布的受害者中，有的确实被成功攻击，有的攻击却缺少足够的证据证明。因之前被发现利用已泄露数据伪装成新攻击事件，该勒索软件攻击行动还被调侃为“清道夫行动”(scavenger operations)，因此 Stormous 勒索软件组织的攻击可能存在欺诈，其中一些典型案例如下：

可口可乐(Coca-cola)的攻击事件

Stormous 勒索软件组织宣称从可口可乐公司网络中窃取了 161GB 数据，并索要 1.65 比特币（约折合 64,000 美元）作为赎金 。然而，赎金数额与声称窃取的数据量相比显得微不足道，引发了对该团伙所掌握数据真实价值的质疑 ；

美泰(Mattel Inc)公司攻击事件

美泰公司曾在 2020 年 11 月遭受勒索软件攻击，而 Stormous 勒索软件组织公布的针对该公司的数据，很可能仅仅是对之前被盗数据的重新包装，企图混淆视听，以期从中获利;

乌克兰外交部攻击事件

3 月 1 日宣布攻击了他们声称从该部的数据库中获取了大量敏感数据，例如电话号码、电子邮件、密码和卡号。但据了解，这些数据在暗网上长期流传，并且是免费共享的。

Epic Gams 攻击事件

Stormous 声称攻击了 Epic Games，并窃取了近 200GB 数据，其中包括 3300 万用户的信息。然而，这些数据的真实性还没有得到证实。

Stormou 勒索软件发展史

2023 年发展情况

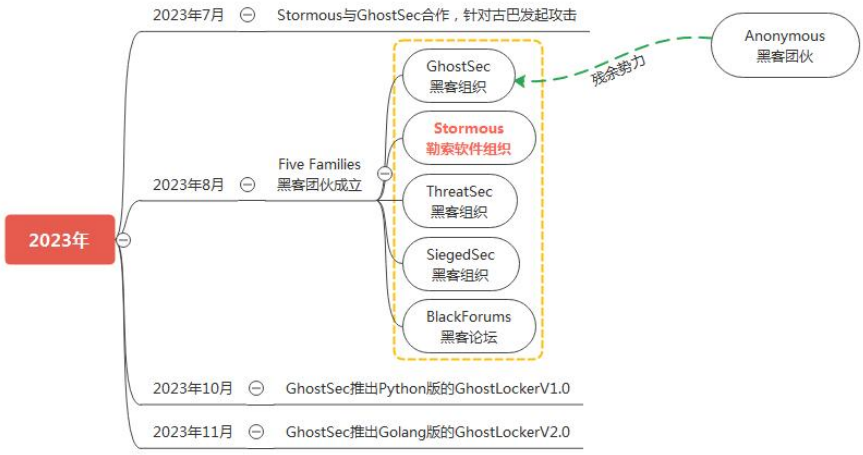

图 1. Stormous 勒索软件 2023 年发展情况

- 2023 年 7 月 13 日，Stormous 勒索软件组织通过 GhostSec 的 Telegram 频道宣布，正式与 GhostSec 建立合作伙伴关系，并成功合作针对古巴各部委实施行动。
- 2023 年 8 月 Five Families 黑客团伙正式成立。该团伙包括了三大黑客组织、一大勒索软件组织和一个黑客论坛，具体包括：ThreatSec、GhotsSec、SiegedSec、Stormous 和 BlackForums。

图 2. The Five Families 黑客团伙

- 2023 年 10 月，GhostSec 宣布推出了名为 GhostLocker 的新勒索软件即服务（RaaS）框架，该框架使用的是基于 Python 的 Nuitka 编译项目。Stormous 组织随后宣布，除了他们现有的 StormousX 程序外，还将 GhostLocker 勒索软件程序纳入其攻击工具库中。

2024 年发展情况

图 3. Stormous 勒索软件 2024 年发展情况

- 2024年2月24日,Stormous组织在“The Five Families”Telegram频道宣布,与GhostSec合作启动了新的勒索软件即服务（RaaS）计划“STMX_GhostLocker”。该计划包含三种服务：付费服务、免费服务，以及针对那些没有长期计划、只想在博客上出售或发布数据的个人的 PYV 服务。
- 2024 年 4 月 29 日，Stormous 的暗网专用数据泄露站点（DSL）出现了无法访问的情况，而该团伙并未在其任何官方频道发布相关声明，这导致了外界一度猜测 Stormous 可能已经停止运营；
- 2024 年 5 月 17 日，长期与 Stormous 合作的 GhostSec 黑客团伙在 Telegram 频道宣布，由于已筹集足够资金支持未来活动，将关闭 GhostSec 服务渠道和 GhostLocker RaaS 服务。他们计划将 V3 GhostLocker 勒索软件的源代码共享给 Stormous，以确保合作伙伴顺利过渡，并避免诈骗或服务中断。Stormous 将接管“Five Families”的 Telegram 频道。
- 2024 年 6 月，Stormous 宣布他们没有停止运营，而是对服务进行了重大更新，将他们的勒索软件 GhostLocker 升级到了第四版。
- 2024 年 10 月 23 日，DragonRansom 勒索软件组织开设了名为@Stormouss 的 Telegram 频道，并运营@stmcrychat 频道，企图冒充 Stormous 团伙，这一行为始于 2024 年 3 月。
- 2024 年 10 月 27 日,Stormous 勒索软件组织在其 Telegram 频道@StmXRansomware 宣布，为了修复服务中的一些问题，计划在下周一或周二恢复运营。

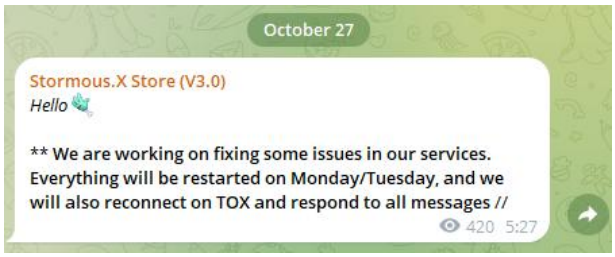

图 4. Stormous 在 Telegram 发布的消息

- 2024 年 11 月 1 日，Stormous 勒索软件组织通过其 Telegram 频道@StmXRaaS 公开发布了受害者数据，并宣布这些数据也被同步到了该组织的专用数据泄露站点，标志着其恢复运营。

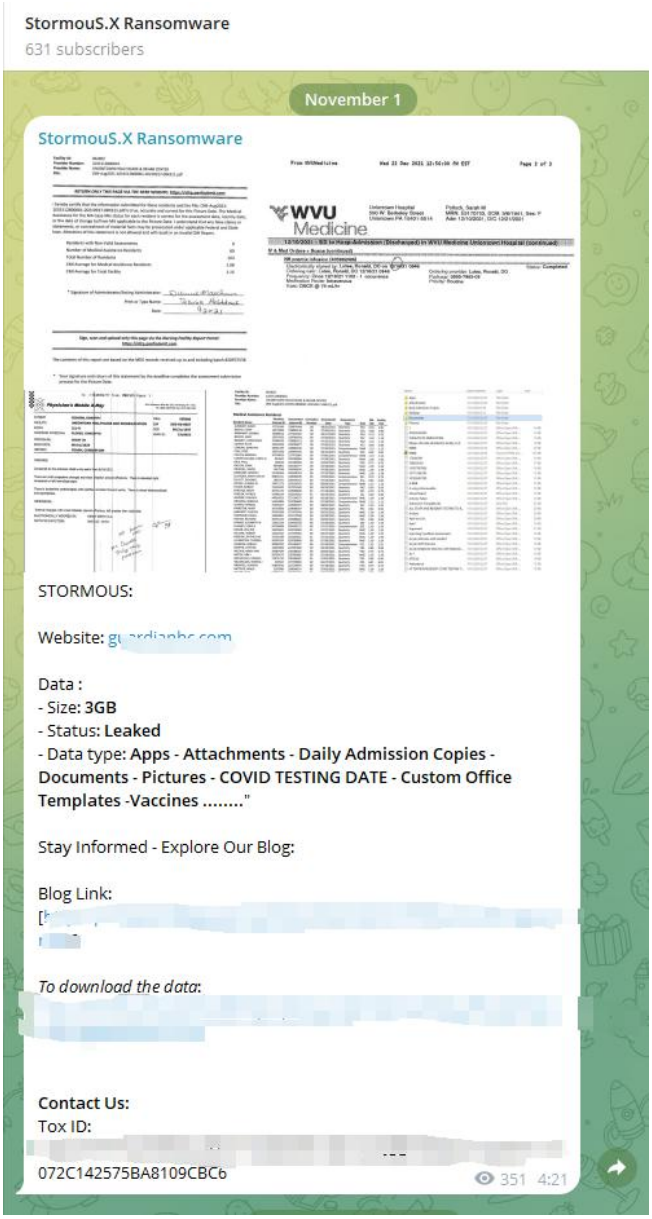

图 5. Stormous 在 Telegram 平台发布受害者信息

RaaS 计划

Stormous 勒索软件组织自 2021 年起活跃于网络犯罪领域，并在 2023 年与 GhostSec 合作攻击多个目标。2024 年 2 月，该组织正式推出了其勒索软件即服务（RaaS）平台，命名为 STMX_GhostLocker，并向有意加入的个人或团体提供了三种加入方案。

付费版附属公司

支付 1500 美元，即可成为附属公司，将有权限访问一个高效控制面板，加入专属论坛与行业伙伴交流，享受在“附属”板块的品牌展示，以及博客快速发布攻击目标的权利。对于成功获得勒索赎金的案例，Stormous 仅收取 15%的分成。

以下是 STMX_GhostLocker 为付费附属公司展示的功能图：

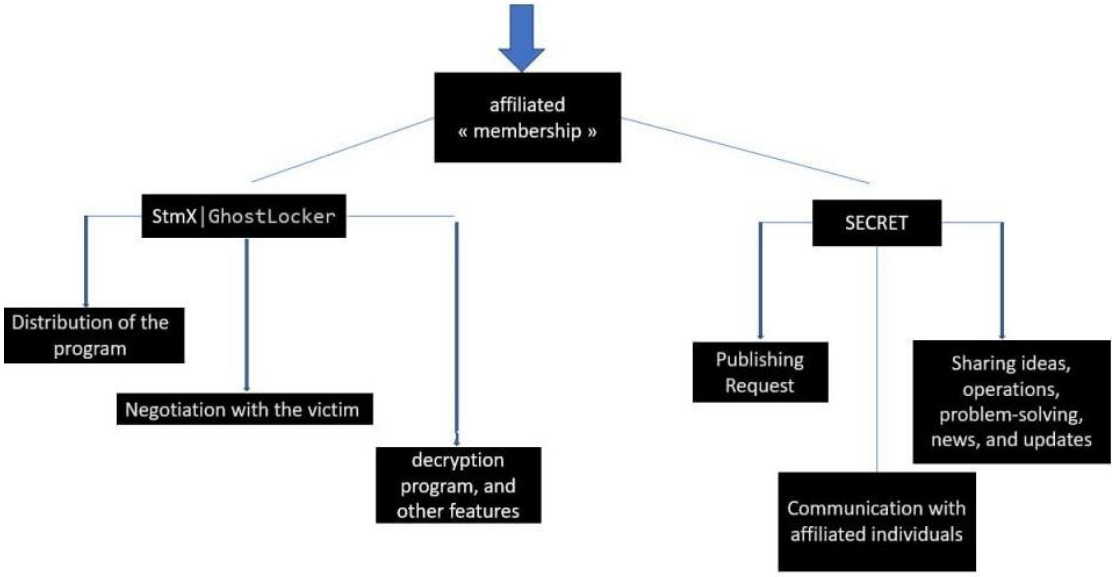

图 6. 付费版功能图

免费版附属公司

为所有使用 Stormous 程序的人提供免费版本。为享受此服务，使用者需要具备现成的访问权限。需注意的是，该服务使用者将无法访问控制面板；如果使用者选择信任 Stormous 的一个附属公司，或者他们有意与免费使用者建立联系，相关的谈判将由他们负责。使用者设定的目标将在 Stormous 的博客上发布，同时 Stormous 将从中抽取 20%的费用。

PYV 服务

针对那些没有长期计划、仅希望在 Stormous 的博客和相关频道上出售或发布数据的个人，其提供以下服务：用户可以免费在 Stormous 平台上发布待售公司的数据。一旦数据成功出售，Stormous 将收取 10%的佣金作为服务费。

2024 年 5 月 GhostSec 宣布退出 STMX_GhostLocker 勒索软件即服务(RaaS)计划后，Stormous 勒索软件组织在 2024 年 6 月推出了新的 RaaS（勒索软件即服务）方案，该方案相较于之前更为简化：

终身会员

潜在参与者只需支付 1500 美元即可获得终身会员权限，享受以下服务：访问控制面板、加密程序以及在数据泄露网站上发布攻击目标的权限。

季度会员

潜在参与者可以选择支付 400 美元以获得与终身会员相同的权限，但该权限仅限 3 个月的使用期限，如果附属公司在到期后未进行续费，Stormous 将保留其数据，直至他们再次付款。

2024 年 9 月 14 日，Stormous 勒索软件组织通过其 Telegram 频道宣布对其勒索软件即服务（RaaS）计划进行调整，取消了季度会员选项，并下调了终身会员的价格。现在，潜在的参与者仅需支付 950 美元，即可获得 Stormous RaaS 方案的全部访问权限。该组织对 RaaS 计划的频繁调整，包括减少服务项目和降低服务费用，引发了外界对其运营状况的猜测。特别是在与 GhostSec 组织分道扬镳之后，Stormous 似乎面临了一定的运营挑战

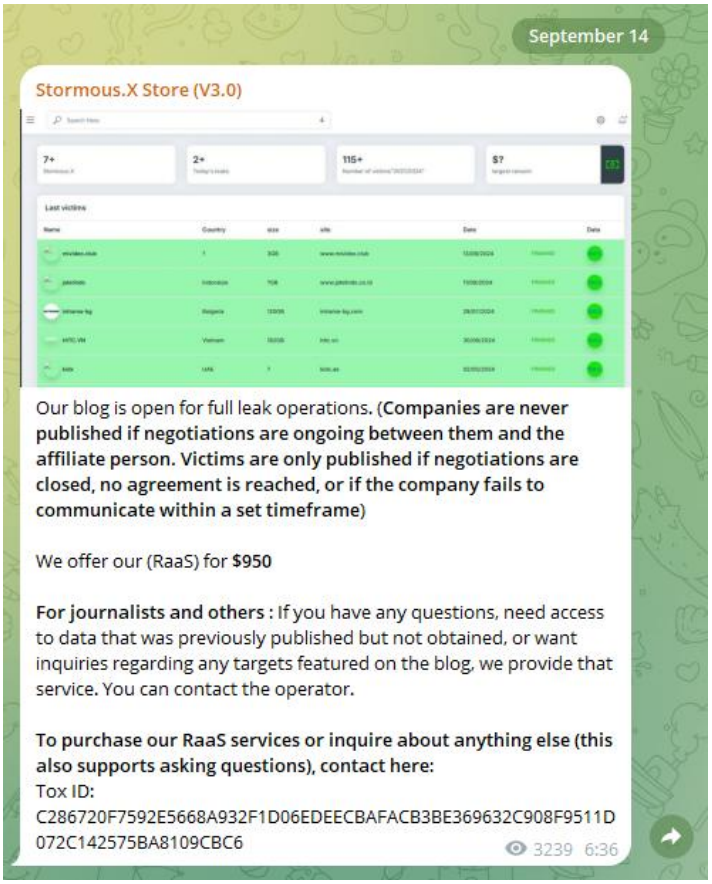

图 7. Stormous 最新调整后的收费策略

攻击案例

Duvel Moortgat

2024 年 3 月，勒索软件组织 Stormous 对比利时知名啤酒制造商 Duvel Moortgat 发起网络攻击，导致该公司的 IT 系统检测到入侵并迅速响应，宣布暂时关闭了包括 Duvel、La Chouffe、Liefmans、De Koninck 和 Maredsous 等品牌的生产线。尽管生产活动受到影响，

Duvel Moortgat 发言人表示，由于库存充足，预计不会对产品供应造成影响。

Stormous 随后在其数据泄露网站上公布了从 Duvel Moortgat 窃取的 88GB 数据，这些数据包括财务、人力资源、客户身份信息和网络信息等敏感数据。

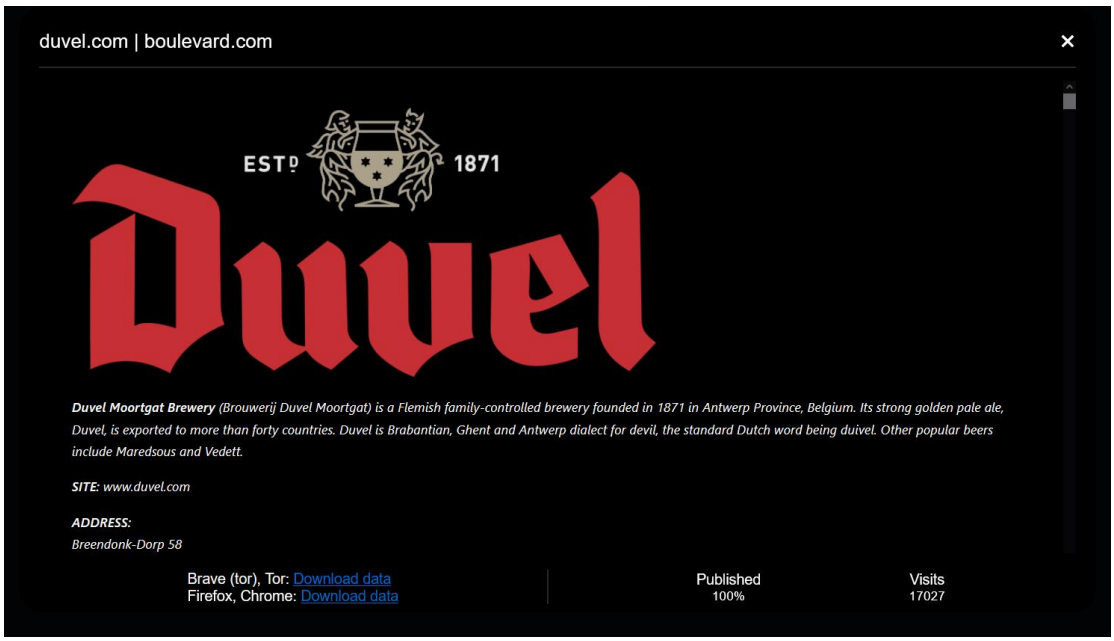

图 8. Stormous 发布的 Duvel Moortgat 被窃取信息

AOSense/NASA

2024 年 9 月，Stormous 勒索软件组织宣称对 AOSense 公司，发起网络攻击，并声称此次攻击同时波及了 NASA(美国联邦政府负责民用太空计划的独立机构，主要进行航空和航天研究)。AOSense 公司，总部位于加利福尼亚州森尼维尔，是一家专注于量子传感技术的开发商和制造商。据 Stormous 组织在其官方 Telegram 频道发布的消息，该团伙从 AOSense 窃取了高达 1TB 的数据。然而，与 NASA 相关的数据量并未在官方控制面板中明确展示

图 9. AOSense/NASA 相关数据公开页面

Stomous 在其官方 Telegram 频道发布的消息可知，NASA 的数据是通过 AOSense 获取到。并向 AOSense 索要赎金高达 500 万美元的赎金。

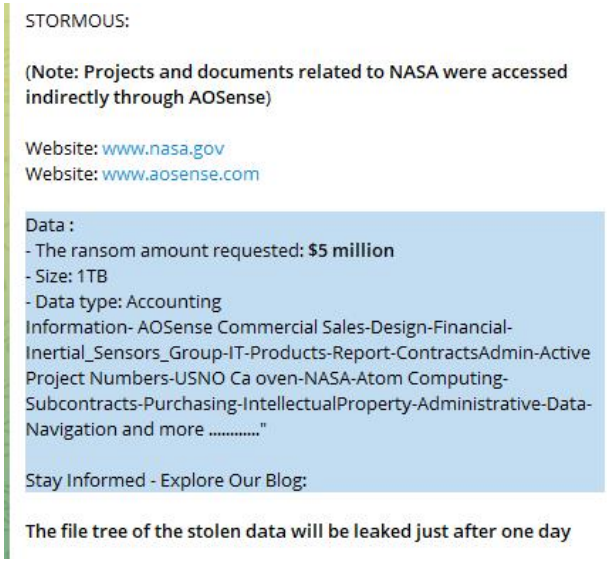

图 10. Stomous 发布的 NASA 图纸

TRANSAK

2024 年 10 月 21 日，Transak 公司就 Stormous 勒索软件攻击事件发表声明，确认攻击影响了其 1.14%的用户群体，总计 92,554 名用户。然而，Stormous 组织对此数据提出异议，声称通过审查窃取的数据后发现，实际受影响的用户数量远超 Transak 所公布的，高达 500 万，涉及 Trust Wallet、METAMASK、ZilSwap 等多个平台的用户数据，窃取的数据总量超过 300GB。Stormous 还指控 Transak 关于受影响用户数量的声明是不实的。

Stormous 勒索软件集团在其 Telegram 频道上发表声明，断然拒绝了 Transak 安全团队提出的 3 万美元以删除被盗数据的提议，强调所涉及的数据价值远超此报价，认为此要求是不合理的。Stormous 还对 Transak 提出的参与漏洞赏金计划的请求表示嘲讽，称之为荒谬。该团伙明确表示不会接受这一微不足道的报价，并威胁将泄露额外的 50GB 数据，同时计划将剩余数据出售给出价最高的买家。

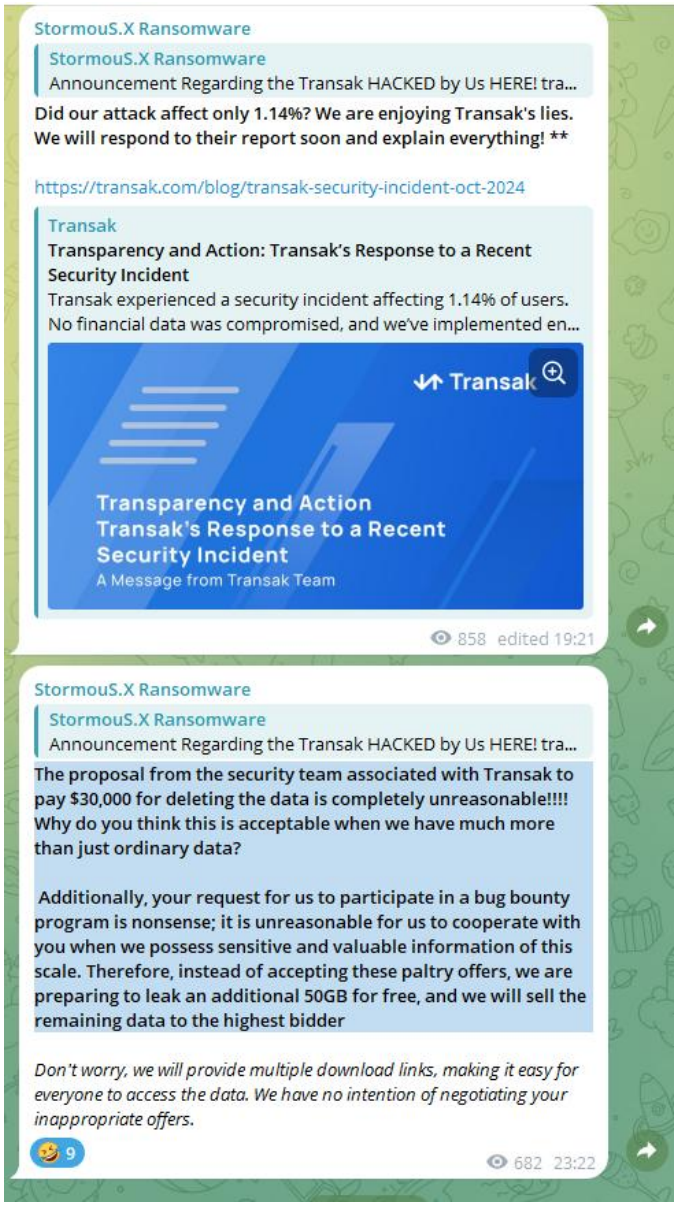

图 11. Stormous 拒绝 Transak 的 3 万美元赎金请求