思而听 Think&Listen

数世咨询 Digital World Consulting

勒索软件威胁与防护年度报告（2026）

--SolarCERT

©思而听（山东）网络科技有限公司&北京数字世界咨询有限公司

编辑团队

主编：

思而听 **何颖**　　思而听 **梁文豪**
数世咨询 **李少鹏**

责编：

思而听 **张沛垚**　　思而听 **王子豪**
数世咨询 **闫志坤**

技术支持：

思而听 **李林菲**　　思而听 **徐龙州**
数世咨询 **数字安全能力研究院**

美工团队

主美：

思而听 张义莹
数世咨询 **闫志坤**

设计语言：

思而听 吴艳丽
数世咨询 **闫志坤**

目录

执行摘要

在数字化转型加速推进的当下，勒索软件攻击已成为全球企业面临的最为严峻的网络安全威胁之一。2025 年，全球勒索攻击呈现出前所未有的爆发态势，给企业带来了巨大的经济损失和运营风险。为了帮助企业深入了解勒索软件威胁态势，制定科学有效的防御策略，本报告通过双重视角对 2025 年勒索软件威胁进行了系统性分析。

本报告旨在全面揭示 2025 年勒索软件攻击的时间分布、攻击者格局和国内实战处置情况，为企业提供有针对性的防御建议，帮助企业降低勒索软件攻击风险，保障业务的持续稳定运行。

为确保分析的全面性和准确性，本报告采用了双重视角进行研究。一方面，通过 Ransomware.live 全球威胁情报平台追踪数据，对全年勒索攻击事件进行统计和分析；另一方面，基于 Solar 安全应急响应团队全年处置的实战案例，深入剖析攻击者的战术演进与防御方的应对策略。

研究发现，2025 年全球勒索攻击时间分布呈现出显著的“**双峰一谷**”运营周期特征。第一季度以 2,421 起事件占据全年 29.3%的份额，形成年初的攻击爆发期；第二、三季度进入相对低谷的蓄力阶段；第四季度则以 2,417 起事件实现强势反弹，环比增长 47.29%，形成年末的收割高峰。攻击者格局方面，Qilin 家族以 12.4%的市场占比跃居年度榜首，Akira（9.5%）和 Clop（6.6%）紧随其后，前三大家族合计占据 28.4%的市场份额。

指标	全球数据	国内处置（SolarCERT）	趋势解读
全年事件数	7920 起	534 起	国内处置量激增 544.89%
峰值时间	2 月（1,016 起）	第二季度(35.20%)	Weaxor 战役驱动国内峰值
主导家族	Qilin(12.4%)	Weaxor（Mallox 变种）	头部效应显著
首要目标	Manufacturing(17.6%)	MS-SQL 数据库服务器	制造业全球/国内双重承压
高危事件占比	—	99.61%	攻击直指核心业务系统
双重勒索占比	标配（Top10 全部 DLS）	55.32%	数据泄露风险并行

表 1:2025 年度勒索态势核心指标对比（全球数据 vs SolarCERT 处置数据）

从国内实战处置视角看，Solar 应急响应团队 2025 年累计处置勒索案件 534 起，较 2024 年激增 544.89%，攻击规模呈现爆发式增长。高危级事件占比高达 99.61%，双重勒索模式占比 55.32%，“二次勒索”风险凸显，35.2%的企业因未彻底清除内网后门而短期内遭遇二次攻击。Weaxor 家族在第二季度的集中爆发，成为年度最具代表性

的攻击战役。

基于以上研究结果，为帮助企业有效应对勒索软件攻击，我们提出以下具体建议：一是加强安全意识培训，提高员工对勒索软件的识别和防范能力；二是建立完善的安全防护体系，包括防火墙、入侵检测系统、数据备份等，及时修复系统漏洞，防止攻击者入侵；三是制定应急响应预案，定期进行演练，确保在遭受勒索软件攻击时能够迅速做出反应，降低损失；四是加强与安全厂商和行业组织的合作，及时获取最新的威胁情报和防御技术。

通过实施上述建议和行动计划，企业可以有效降低勒索软件攻击风险，减少经济损失，保障业务的持续稳定运行。同时，也有助于提升企业的安全管理水平，增强市场竞争力。

第一章丨勒索攻击态势

（一）概况

1.勒索事件规模与趋势

1.1 总体态势：从边界监测向应急响应实战的纵深演进

区别于传统安全厂商基于边界防御日志的常规流量监测，SolarCERT 安全应急响应团队（以下简称“SolarCERT”）的服务视角更聚焦于**已突破防线并造成实质性破坏**的勒索事件处置。2025 年，SolarCERT（以下同）累计接收并有效处置勒索软件攻击事件 **534** 起。这些数据直接映射了当前企业面临的严峻现实：核心业务中断、关键数据丢失以及内网环境下的高强度攻防对抗。

2025 年的勒索攻击时间分布曲线**呈现出鲜明的季节性特征**，这种规律性并非偶然，而是攻击者基于受害者行为模式精心优化的运营策略体现。深入理解这一节奏背后的驱动因素，对于制定前瞻性的防御计划具有重要价值。与 2024 年相比，Solar 团队处置的**勒索案件总量激增 544.89%**。

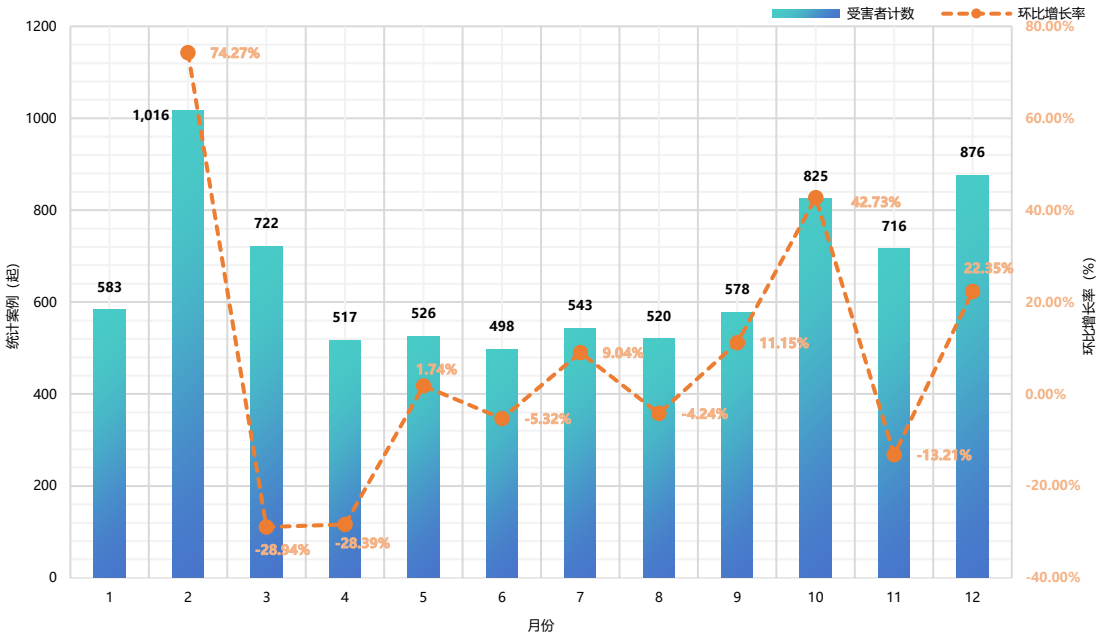


图 1.:2025 年全球勒索攻击年度趋势

2 月份以 1,016 起攻击事件创下全年峰值，环比 1 月增长 74.27%。这一异常峰值的出现，是多重因素叠加的结果。首先，**年初是企业 IT 预算周期的关键节点**，上一年度的安全设备许可到期，新年度预算尚未完全到位，**导致安全运营出现“真空期”**。攻击者精准把握这一窗口，针对尚未完成安全升级的薄弱环节发起集中攻势。

其次，2 月恰逢中国农历春节与西方情人节重叠的社会工程素材丰富期。钓鱼邮件主题从传统的“发票通知”“快递信息”扩展至“年终奖发放”“节日礼品卡”等更具诱惑力的内容，大幅提升了初始入侵的成功率。我们的数据分析显示，2 月份涉及社会工程攻击向量的事件占比显著高于其他月份，印证了攻击者在“人的弱点”上的重点投入。

从 5 月到 8 月，攻击事件数量持续走低，6 月份以 498 起触及全年谷底。这一现象被业界称为“夏季狩猎假说”，其成因具有双向性。一方面，大量勒索软件运营团队位于东欧及俄语区，这些地区的攻击者在夏季有传统的休假习惯，导致整体攻击产出下降。另一方面，企业的 IT 运维团队同样在 7-8 月进入休假高峰期，即使发生入侵事件，响应和处置的及时性也会受到影响。

因此最需要警惕的是，**事件数量的下降并不意味着威胁强度的降低**。恰恰相反，这一时期攻击者可能将资源集中于高价值目标的**“精准狙击”**——上市公司、关键基础设施、大型医疗机构等。这类攻击往往涉及更长的潜伏周期和更复杂的数据窃取操作，其赎金谈判过程也不会全部体现在公开勒索站点上，形成了所谓的“暗数”。防御方在夏季不应放松警惕，而应加强对异常网络行为的持续监控。

第四季度以 2,417 起事件实现强势反弹，环比增长 47.29%。这一“年末收割”现象的背后，是攻击者对受害者财务周期和心理压力的精准把握。尤其对于**医疗行业**而言，年末是医保结算、患者就诊的高峰期，任何系统中断都可能导致严重的医疗服务中断和合规风险，迫使医疗机构在赎金谈判中更快妥协。对于金融服务行业，年末的财务关账压力同样巨大，攻击者利用“不能停”的业务特性显著提高赎金支付率。

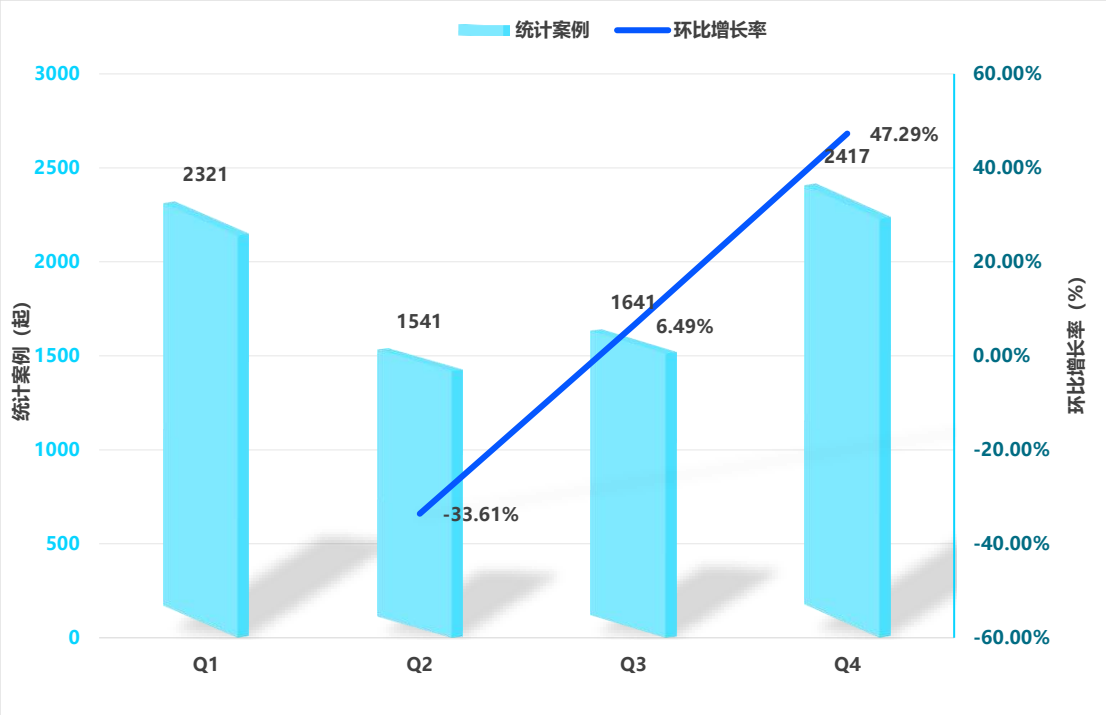


图 2:2025 年季度攻击强度对比矩阵

深度复盘：Weaxor 家族攻击爆发的归因分析

Weaxor 勒索病毒在第二季度的爆发，并非依赖高成本的 0-day 漏洞，而是对企业**资产暴露管理失效**的精准打击。

- **攻击手段**：攻击者利用企业财务及 OA 系统中存在的**已知历史漏洞（N-day）**，实施自动化批量扫描与渗透。
- **暴露面分析**：在 Solar 团队处置的第二季度案例中，超过 **70%** 的受害企业虽部署了防火墙，但为满足业务便捷性，将关键系统的 Web 端口直接映射至公网，且长期未进行补丁升级。
- **结论**：这种架构缺陷导致高价值资产处于**缺乏有效防护**的状态，极易被攻击者批量锁定。事实证明，应用系统的全生命周期补丁管理，已成为防御勒索攻击的关键防线。

1.2 事件分级与结构性变化

在攻击数量增长的同时，勒索攻击的破坏性与策略也呈现出显著的结构性变化，2025 年的态势呈现以下三大特征：

- **高危级事件占比激增：**我们将“导致核心业务中断超过 24 小时”或“涉及核心数据库加密”的事件定义为“高危级”。在年度处置案例中，高危级事件占比高达 **99.61%**。这表明勒索软件已不再仅是文件层面的干扰，而是直接威胁企业生存与业务连续性的重大风险。
- **双重勒索模式常态化：**攻击者不再满足于单一的解密赎金。统计数据显示，**55.32%** 的处置案例涉及“加密+窃密”的双重勒索模式。特别是在**制造业**与**软件信息技术服务业**，攻击者利用泄露商业机密、源代码或客户数据作为谈判筹码的趋势显著上升。
- **“二次勒索”风险凸显：**在寻求 Solar 团队协助的客户中，有 **35.2%** 的企业曾试图自行支付赎金或通过非专业渠道恢复，但因未彻底清除内网后门（如 Webshell、幽灵账号等），导致短期内遭遇二次攻击。这充分印证了专业应急响应在**溯源根除**环节的必要性。

统计维度	2025 年数据	趋势解读
案件总量	534 起	同比增长 544.89%，攻击规模爆发式增长
高危事件占比	99.61%	攻击目标直指核心业务系统
双重勒索占比	55.32%	数据泄漏风险与业务中断风险并行
二次勒索占比	35.20%	缺乏彻底溯源导致的持续性威胁

表 2: 2025 勒索趋势解读

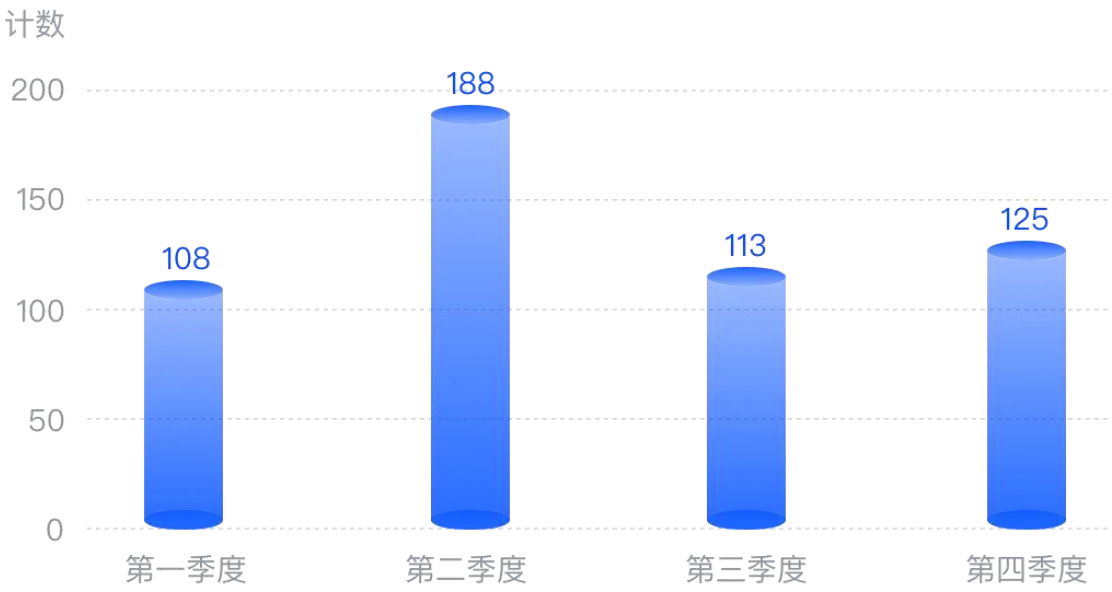


图 3：Solar 安全应急响应团队统计（国内）

通过图 3 中 Solar 安全应急响应团队 2025 年度处置案例的可视化呈现，也印证了我们在前文中提出的夏季狩猎假说——第二季度国内响应案例实际非但没有减少，反而有所增加。

这一现象背后，是勒索攻击规模的爆发式扩张——2025 年全年处置案件总量达 534 起，同比增长 544.89%，印证了攻击活动的高频化与规模化趋势。同时，高危事件占比高达 99.61%，表明攻击者已将目标精准锁定在企业核心业务系统，一旦得手便会直接瘫痪关键生产与运营环节。值得注意的是，双重勒索占比达 55.32%，意味着数据泄漏风险与业务中断风险的双重叠加，大幅提升了企业的损失成本；而 35.20%的二次勒索占比，则进一步揭示了非专业处置留下的后门隐患如何转化为持续性威胁。这些数据共同勾勒出勒索事件的结构性变化：攻击模式已从早期单纯的文件加密，演变为“加密+数据泄漏+二次勒索”的复合型威胁，对企业应急响应的专业性、全面性提出了更高要求。

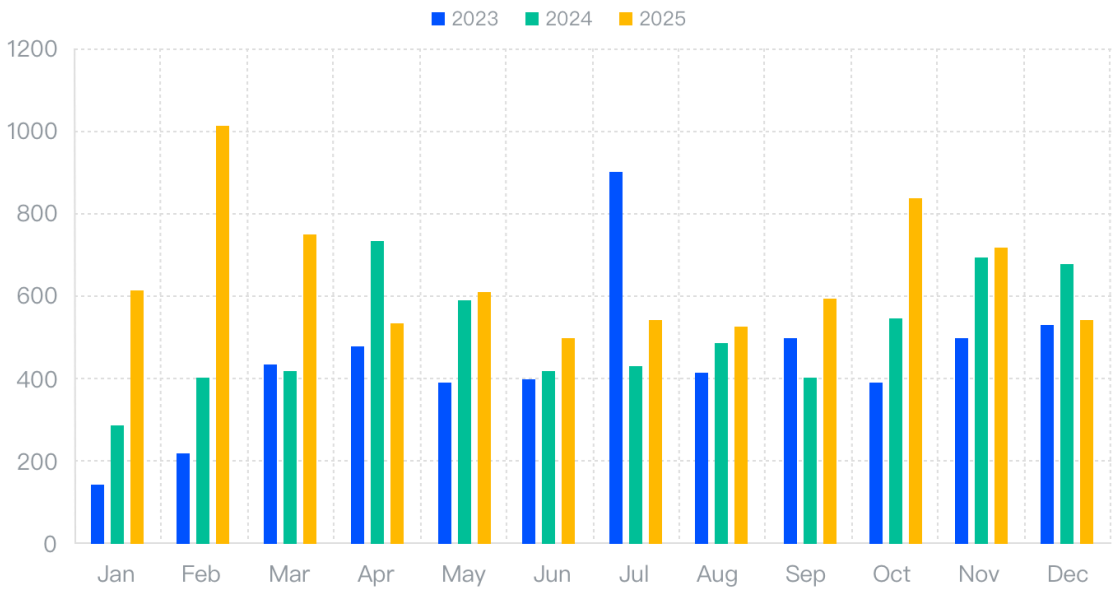


图 4：RANSOMLIVE 数据源（全球）

2.主流勒索组织与活跃家族分布情况

2.1 勒索家族分布：头部效应显著

基于 Solar 团队 2025 年全年的应急响应数据，勒索软件威胁生态呈现出明显的**市场集中化**特征。在全年处置的 534 起勒索事件中，攻击量排名前十的家族（Top 10）合计占据了总案发量的 **79.58%**，主导了当前的威胁态势。

与此同时，结合权威威胁情报平台 Ransomlive 的全球数据，2025 年勒索软件生态经历了剧烈的洗牌。

- **Qilin （麒麟）** 家族表现出极强的攻击性，以全年累计 **1,009** 名受害者的记录位居全球榜首。
- **双重勒索成为标配**：全球 Top 10 家族全部建立了专属的 **DLS (Data Leak Site，数据泄露站点）**。这表明构建 DLS 平台已成为主流勒索组织的入场标准，其目的在于利用 GDPR 合规压力与声誉受损风险，对受害企业施加心理压迫。

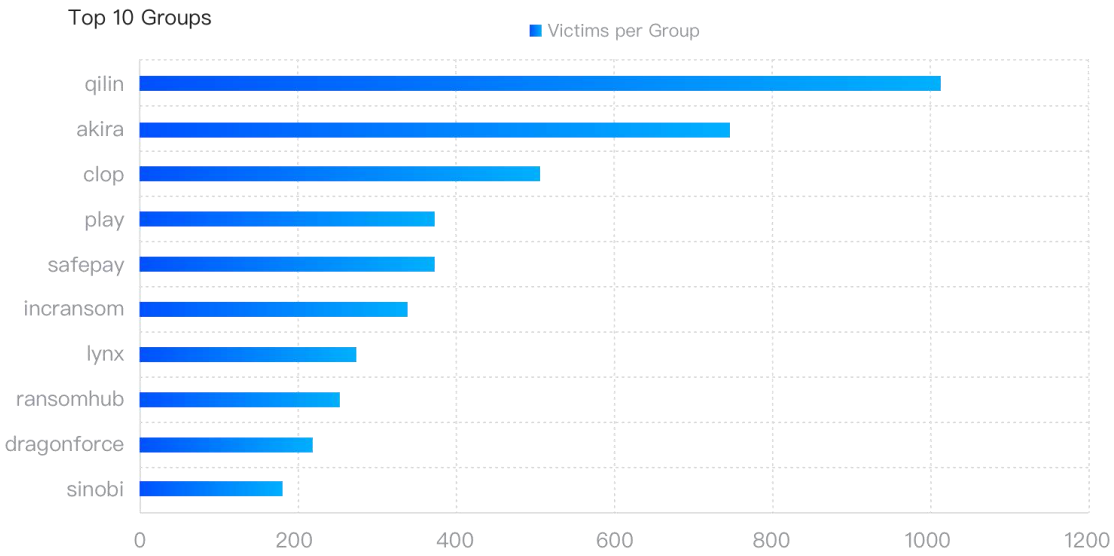


图 5：RANSOMLIVE 数据源（全球）Top10 勒索家族案件数

2.2 全球 TOP 5 勒索家族简介

勒索软件生态的市场结构正在经历深刻演变。2025 年的数据显示，市场集中度持续提升，头部家族的影响力进一步扩大，同时新兴家族的崛起也带来了新的战术变量。

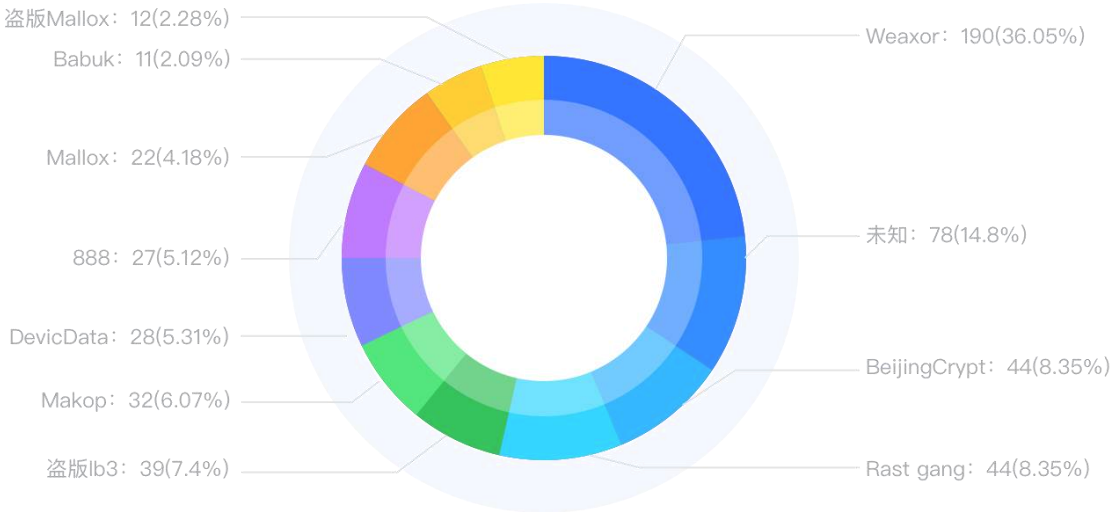


图 6：Solar 安全应急响应团队统计（国内）

（1）全球 TOP1:Qilin

Qilin（又名 Agenda）是一个 RaaS 勒索软件组织，于 2022 年 7 月出现，2022 年 9 月更名为“Qilin”并以勒索软件即服务（RaaS）模式运营。麒麟勒索软件主要针对 Windows 系统，但已发现针对 VMware ESXi 服务器的 Linux 变种。该组织在对领先的病理服务提供商 Synnovis 进行攻击期间，因其 5000 万美元的赎金要求而迅速声

名鹊起，导致伦敦主要 NHS 医院的服务中断。Qilin 最初是 Agenda 勒索软件（用 Go 开发）的一个分支，现已演变为一个更强大的、基于 Rust 的变种，融合了恶意软件构建和防御规避的技术。

① 勒索信

图 7:Qilin 家族勒索信

② 暗网博客

说明	检测时间	地址
勒索组织博客	2025-06-01	ozsxj4hwxub7gio347xxxxxxxxxxo2oqfs4cw2mgtyd.onion
勒索组织 DDOS 服务	2025-06-09	kbsqoivihgdmwczmxxxxxxxxxxxhhfu5yw725dboqo5kthfaad.onion
勒索组织数据泄露页面	2026-01-19	ijzn3sicrcy7guixkzjxxxxxxxxxxxmby4mCBCcnsd7j2rekvqd.onion
勒索组织疑似登录页面	2025-09-11	ji57fr53anp7wbxxxxxxxxxxxywy4jmbncawdcrejj5amuvh3zqd.onion

表 3: Qilin 暗网博客

勒索组织数据泄露页面

图 8:Qilin 勒索家族数据泄露站点截图

勒索组织聊天服务器

图 9:Qilin 勒索家族谈判登录页面截图

勒索组织管理服务器

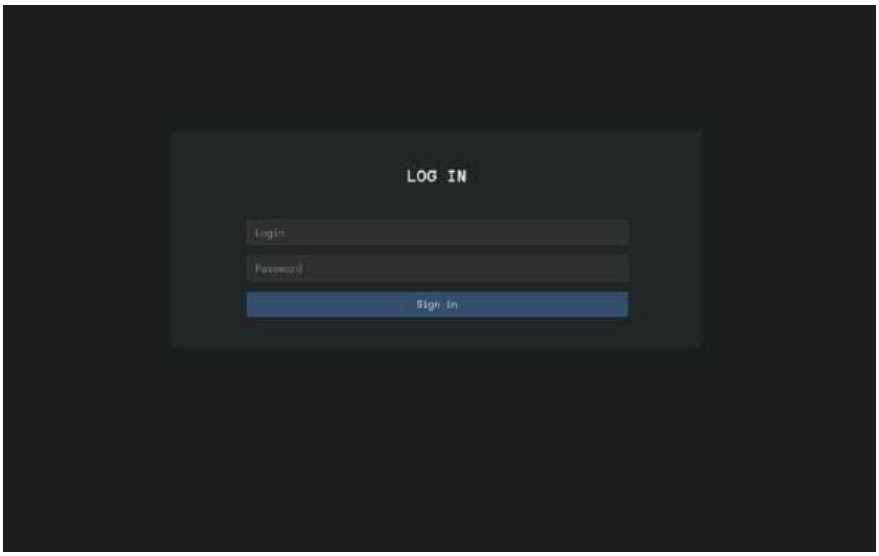


图 10:Qilin 勒索家族管理后台登录页面截图

（2）全球 TOP2:Akira

Akira 成立于 2023 年 3 月。该组织主要针对美国和加拿大的组织，涉及医疗保健、金融、教育和制造业等行业。

这个新的 Akira 团伙不应与 2017 年活跃的同名勒索软件混淆，后者可能并无关联，尽管两个团伙都使用.akira 作为加密文件扩展名。

研究人员很快发现其文件加密程序在代码上与已解散的 Conti 团伙的勒索软件有很多相似之处。不过 Conti 的加密程序源代码已经泄露，所以相似性并不一定意味着它们之间有紧密联系，但区块链分析确实发现了 Akira 可能与 Conti 有关联的潜在线索。

Akira 采用双重勒索软件模型，对受害者的数据进行加密并泄露。该组织要求支付 200,000 美元到 400 万美元不等的赎金，以换取解密文件或不发布敏感数据。Akira 勒索软件的第一个版本是用 C++ 编写的，并附加了带有“.akira”扩展名的文件，创建了一个名为“akira_readme.txt”的赎金票据，部分基于 Conti V2 源代码。

随后，于 2023 年 7 月 2 日发布了修复解密漏洞的版本。从那时起，据说新版本是用 Rust 编写的，这次称为“megazord.exe”，它将加密文件的扩展名更改为“.powerranges”。

① **勒索信**

图 11:Akira 勒索家族勒索信

② **暗网博客**

图 12:Akira 勒索家族暗网博客（数据泄露站点）截图

（3）全球 TOP3:Clop

Clop 最早作为 CryptoMix 勒索软件的变种出现于 2019 年初 。自 2020 年起，Clop 开始建立专门的数据泄露网站（DLS），通过公开曝光受害者数据来施加压力，并通过勒索即服务（RaaS）模式运作 。近年来，Clop 的战略发生了变化，从传统的“加密+窃取”双重勒索模式，转向依赖“0-Day 的大规模利用”和“纯数据勒索”模式 。该

团伙通常以拥有大量敏感数据的大型企业为目标，尤其是在金融、医疗、制造业和媒体行业 。

近年来，Clop 展现出明显的战术转型。在 2024 年的 Cleo 活动和 2025 年的 Oracle EBS 活动中，操作员开始倾向于仅执行数据窃取，而放弃了数据加密步骤，这被称为“纯数据勒索”或“无加密勒索”模式 。传统上，加密文件是一个耗时且资源密集的过程，容易触发企业安全防御团队的警报（如 EDR 系统）。通过将重点放在利用 0-Day 快速窃取大规模敏感信息上，Clop 能够显著减少其在目标网络上的驻留时间，增加攻击的隐蔽性，从而实现更高的攻击成功率。

① 勒索信

图 13:Clop 勒索家族勒索信

② 暗网博客

说明	检测时间	地址
勒索暗网泄露页面	2025-06-01	ekbxxxxxxxxxxias37.onion
勒索暗网泄露页面	2026-01-19	santat7kplxxxxxxxxxxxzl7ry3zm72zigf4ad.onion
勒索暗网泄露页面	2025-06-01	toznnag5o3xxxxxxxxxxxzmz4nmujrjuib4iusad.onion

表 4: Clop 暗网博客

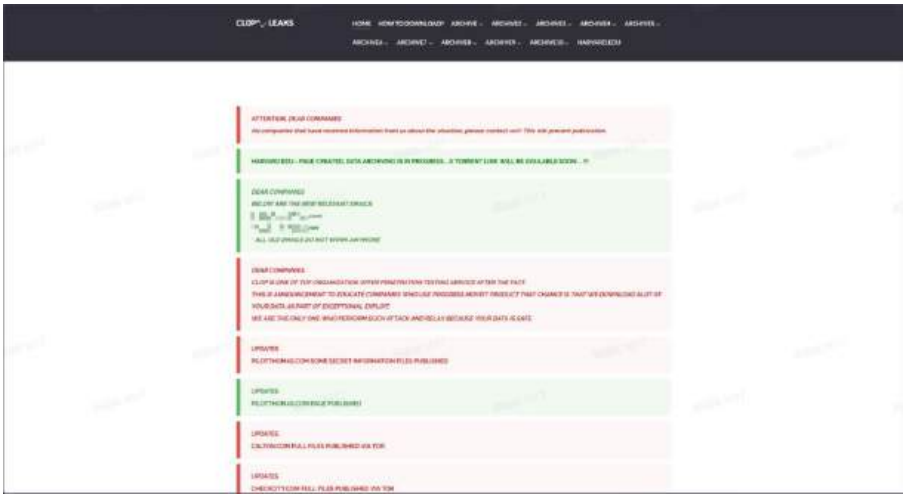


图 14:Clop 勒索家族数据泄露站点截图

（4）全球 TOP4:Play

Play 勒索家族于 2022 年年中被发现，得名于其在加密文件后所附加的.PLAY 扩展名。在随后的一年（2022 年 6 月至 2023 年 5 月），曾在一个月内发起多达 170 次攻击。Play 采用一种封闭式的运营模型，这在当前网络犯罪环境中较为独特。与主流的 RaaS（勒索即服务）模式不同，Play 并非通过招募大量附属机构来扩大规模，而是被认为是一个**直接控制**所有基础设施、运营和赎金谈判的独立实体。这种集中控制模式赋予了 Play 更高的行动保密性，也意味着其内部团队必须具备极高的技术水准和资源来独立完成从初始渗透到最终加密部署的整个攻击链，并支撑其高频次的攻击活动。

该组织的核心勒索策略是**双重勒索（Double Extortion）**。攻击者首先会窃取目标组织的关键数据，然后再进行文件加密。如果受害者拒绝支付赎金，Play REG 将威胁将其窃取的全部数据发布在其 Tor 泄露站点上。为了进一步向受害者施压，该组织有时会采取非传统的手段，例如通过公开来源情报（OSINT）获取受害组织服务台或客服热线的电话号码，并直接致电这些机构施加压力。赎金通知通常不会包含固定的金额或付款指令，而是要求受害者通过特定的电子邮件地址（通常托管在 gmx.de 或 web.de）进行联系。

① 勒索信

ReadMe.txt

```
1  PLAY
2  news portal, tor network links:
3  mbrlkbtq5jon                                    wae6byd.onion
4  k7kg3jqxang3                                    wtj25yd.onion
5
```

图 15:Play 勒索家族勒索信 1

ReadMe2.txt

```
Your network has been encrypted. Your private, personal, corporate, confidential data has been stolen.
If you do not resolve the issue, your data will be published on our leak portal.
News portal, tor network links:
ipi4tiumgz                                                    dvqd.onion
j75o7xvvsm                                                    gpid.onion
contact email:
PLAY Ransomware Team
```

图 16:Play 勒索家族勒索信 2

Play.txt

```
PLAY
te                cd@gmx.com
```

图 17:Play 勒索家族勒索信

② 暗网博客

说明	检测时间	地址	备注
勒索数据泄露页面	2026-01-19	mbrlkbtq5jonaqkurxxxxxxxxxxxkknndqwae6byd.onion	生效
勒索数据泄露页面	2026-01-19	k7kg3jqxang3wh7xxxxxxxxxxbupfgoik6rha6mjpzwupwtj25yd.onion	生效
勒索数据泄露页面	2026-01-19	mbrlkbtq5jonaqkuxxxxxxxxxxxhqvbxfu4rgjbkkknndqwae6byd.onion	生效
勒索数据泄露页面	2026-01-19	j75o7xvvsm4lpsxxxxxxxxxxxbe6oswthuaubbykk4xkzgpid.onion	生效

表 5: Play 暗网博客

暗网地址页面：

图 18:Play 勒索家族数据泄露站点截图

（5）全球 TOP5:Incransom

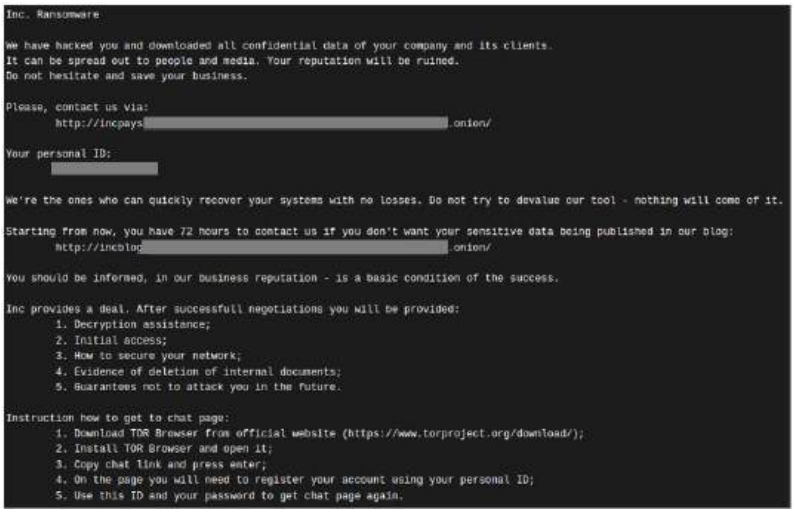
Incransom 勒索软件组织于 2023 年 7 月至 8 月期间首次被网络安全社区观测到，该组织从一出现便展现出极高的行动效率和专业性：在活动最初的六周内，其数据泄露网站上已公布超过 12 个受害组织的信息。这种从起步阶段就高度成熟的运作，与其他新兴勒索软件团伙需逐步建立基础设施、招募成员并完善恶意软件的情况形成鲜明对比。这表明，Incransom 的创始成员并非新人，而很可能是一个经验丰富的网络犯罪团队，或许是从其他知名犯罪集团分离而出，或利用现有资源和网络进行重组。

该组织的核心运营模式为双重勒索。在部署加密程序前，攻击者会投入大量时间在受害者网络中进行侦察，并窃取海量高价值敏感数据。这种策略构成双重威胁：一方面，数据加密导致业务运营中断；另一方面，泄露威胁带来声誉损害、法律诉讼及监管罚款等风险。即使受害者拥有可靠备份可恢复系统，仍会面临数据公开的巨大压力，从而大幅提升支付赎金的可能性。

Incransom 偏好针对医疗保健、教育、政府及关键制造业等行业，这是一种战略性选择。这些领域持有个人身份信息和受保护健康信息等极具价值的数据，一旦受袭，其社会影响和公众压力将显著放大，迫使受害者尽快支付赎金以恢复服务和信誉。在与受害者沟通时，Incransom 常将支付赎金描述为“挽回声誉”的服务。这种措辞是精心设计的心理战术，旨在进一步施加精神压力。

① 勒索信

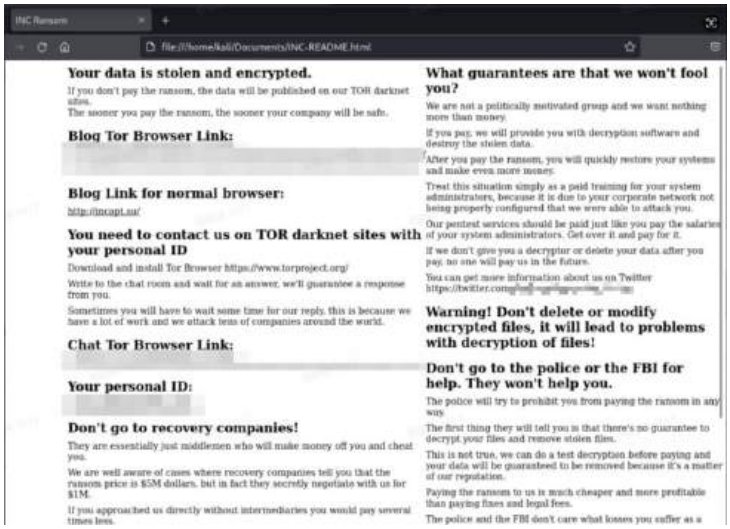
INC-README3.txt



```
Inc. Ransomware

We have hacked you and downloaded all confidential data of your company and its clients.
It can be spread out to people and media. Your reputation will be ruined.
Do not hesitate and save your business.

Please, contact us via:
        http://incpays[redacted].onion/

Your personal ID:
        [redacted]

We're the ones who can quickly recover your systems with no losses. Do not try to devalue our tool - nothing will come of it.

Starting from now, you have 72 hours to contact us if you don't want your sensitive data being published in our blog:
        http://incblog[redacted].onion/

You should be informed, in our business reputation - is a basic condition of the success.

Inc provides a deal. After successfull negotiations you will be provided:
        1. Decryption assistance;
        2. Initial access;
        3. How to secure your network;
        4. Evidence of deletion of internal documents;
        5. Guarantees not to attack you in the future.

Instruction how to get to chat page:
        1. Download TOR Browser from official website (https://www.torproject.org/download/);
        2. Install TOR Browser and open it;
        3. Copy chat link and press enter;
        4. On the page you will need to register your account using your personal ID;
        5. Use this ID and your password to get chat page again.
```

图 19:Incransom 勒索家族勒索信

INC-README.html



Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites.
The sooner you pay the ransom, the sooner your company will be safe.

Blog Tor Browser Link:

Blog Link for normal browser:

http://incapt.su/

You need to contact us on TOR darknet sites with your personal ID

Download and install Tor Browser https://www.torproject.org/

Write to the chat room and wait for an answer, we'll guarantee a response from you.

Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack tens of companies around the world.

Chat Tor Browser Link:

Your personal ID:

Don't go to recovery companies!

They are essentially just middlemen who will make money off you and cheat you.

We are well aware of cases where recovery companies tell you that the ransom price is $5M dollars, but in fact they secretly negotiate with us for $1M.

If you approached us directly without intermediaries you would pay several times less.

What guarantees are that we won't fool you?

We are not a politically motivated group and we want nothing more than money.

If you pay, we will provide you with decryption software and destroy the stolen data.

After you pay the ransom, you will quickly restore your systems and make even more money.

Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you.

Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it.

If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future.

You can get more information about us on Twitter

Warning! Don't delete or modify encrypted files, it will lead to problems with decryption of files!

Don't go to the police or the FBI for help. They won't help you.

The police will try to prohibit you from paying the ransom in any way.

The first thing they will tell you is that there's no guarantee to decrypt your files and remove stolen files.

This is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it's a matter of our reputation.

Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.

The police and the FBI don't care what losses you suffer as a

图 20:Incransom 勒索家族勒索信

② 暗网博客

说明	检测时间	地址	备注
勒索数据泄露页面	2026-01-19	incblog6qu4y4xxxxxxxxxxpw6b7ixzssu36tsajldoad.onion	生效

说明	检测时间	地址	备注
勒索数据泄露页面	2026-01-19	incbacg6bfwtrlxxxxxxxxxxx3s3twdtwhp27dzuik6s6rwdcityd.onion	生效

表 6: Incransom 暗网博客

暗网披露页面：

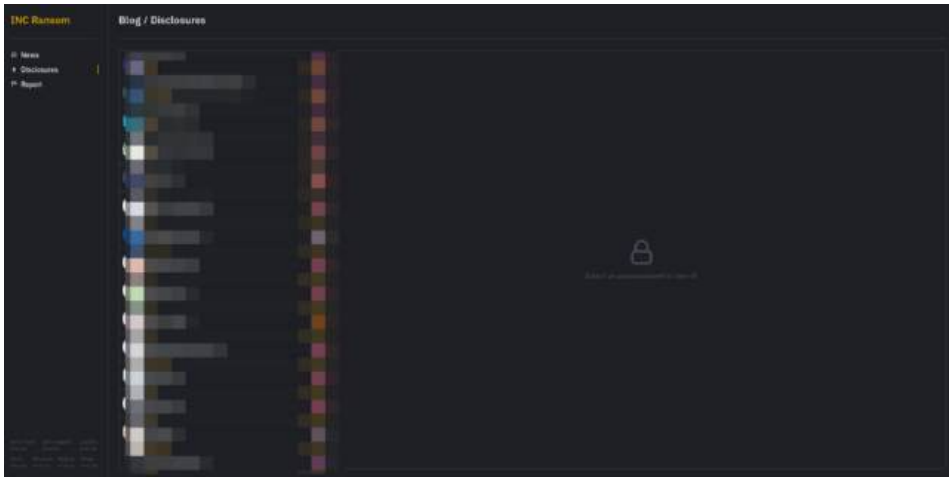


图 21:Incransom 勒索家族数据泄露站点截图

勒索博客网站：

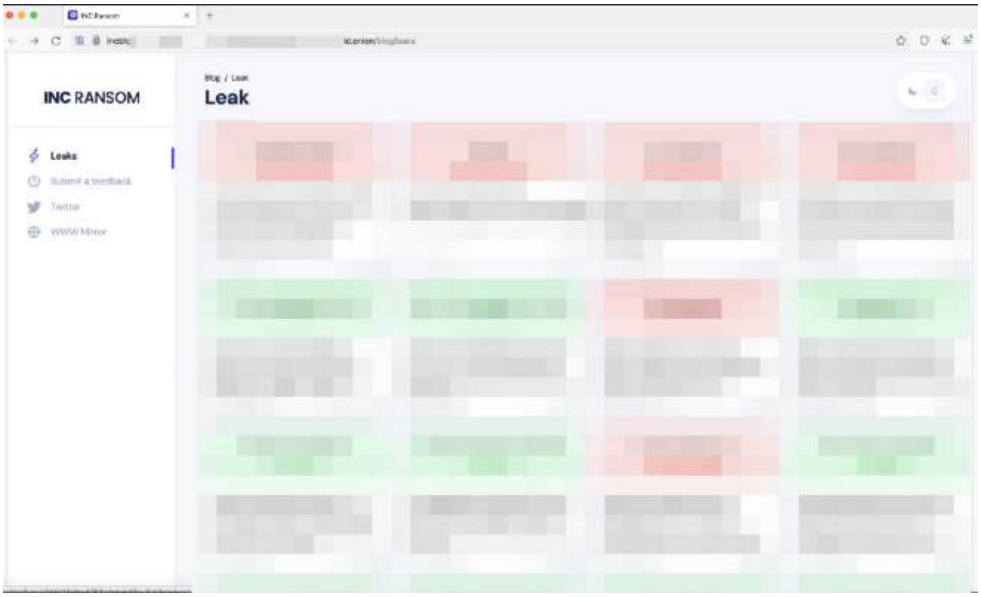


图 22:Incransom 勒索家族暗网博客截图

勒索聊天页面：

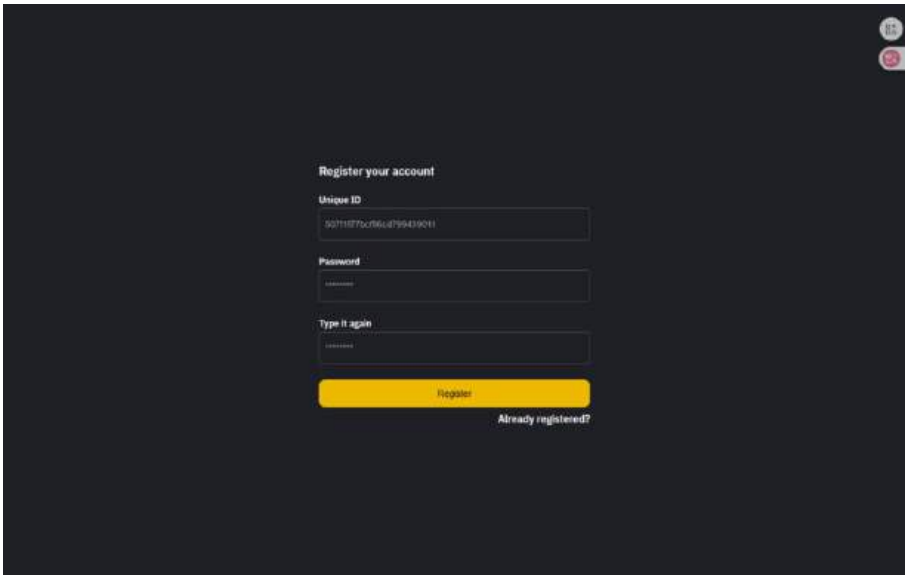


图 23:Incransom 勒索家族管理后台登录页面截图

排名	家族名称	核心特征与技术演进
TOP 1	Qilin (Agenda)	运营模式：RaaS（勒索即服务） 技术栈：从 Go 语言向 Rust 语言迁移，针对 Windows 及 VMware ESXi (Linux) 环境。 典型案例：针对病理服务提供商 Synnovis 的攻击，导致伦敦 NHS 医院服务中断。
TOP 2	Akira	目标定位：主要针对美、加的医疗、金融及制造业。 关联性：代码与 Conti 家族存在相似性，区块链分析显示潜在资金关联。 变种：早期使用 C++，新版本（Megazord）采用 Rust 编写，后缀变更为.powerranges。
TOP 3	Clop	策略转型：从传统的“加密+窃密”转向**“无加密勒索”**（Encryption-less）。 战术特点：利用 0-Day 漏洞（如 Cleo、Oracle EBS 漏洞）快速窃取数据，减少驻留时间，规避 EDR 检测。
TOP 4	Play	运营模式：封闭式运营（非 RaaS），直接控制攻击全流程，具备较高的保密性。 施压手段：除了 DLS 泄漏，还通过 OSINT 手段获取联系方式，直接致电企业客服施压。
TOP 5	Incransom	起步即成熟：初期即展示出极高的运营效率，推测为经验丰富的团队重组。 心理战术：常将支付赎金美化为“挽回声誉”的服务，专注于医疗、教育、政府等高敏感行业。

表 7:勒索家族特征描述

2.3 国内 TOP 5 勒索家族简介

针对中国地区的攻击态势，以下五个家族对国内企业造成了最大影响：

（1）Weaxor (Mallox 变种)

- **身份确认**：Weaxor 被确认为老牌勒索软件 **Mallox** 的深度重构变种，虽更改了品牌标识（.rox / .weax），但代码逻辑高度同源。
- **攻击目标**：专注于 **Windows MS-SQL 数据库服务器**。
- **技术特点**：

➢ 不依赖 0-Day，主要通过扫描公网暴露数据库端口，利用暴力破解或已知漏洞获取权限。

➢ **载荷投递升级**：引入了更现代化的规避技术，利用合法系统工具（LoLBin）进行载荷执行。

① 勒索信

RECOVERY_INFO2.txt

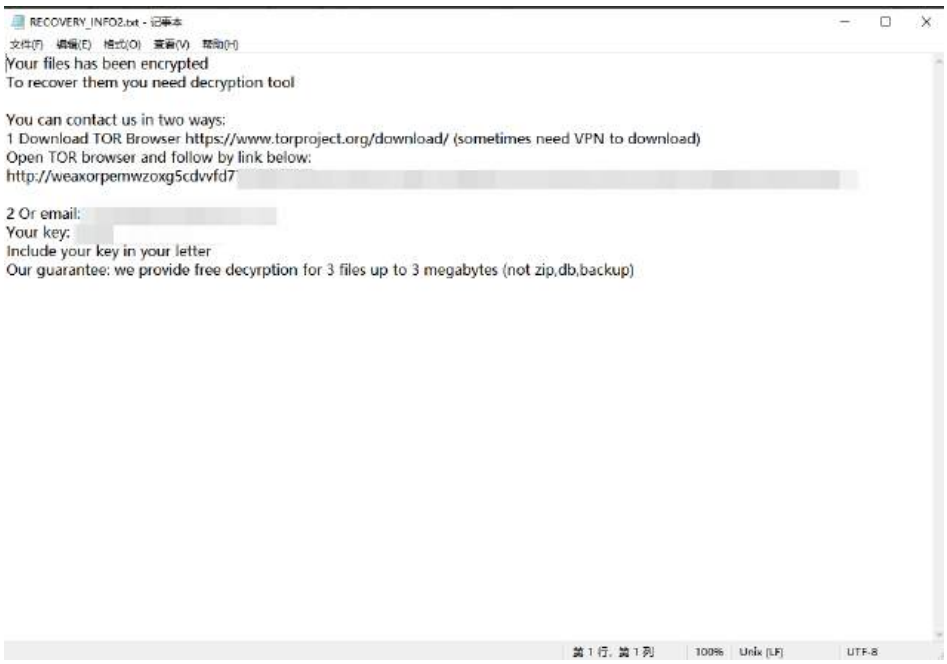


图 24:Weaxor 勒索家族勒索信

FILE RECOVERY.txt

图 25:Weaxor 勒索家族勒索信

② 暗网博客

说明	检测时间	地址	备注
沟通页面	2026-01-19	http://lockbitsupxxxxxxxxxxx63m5ijjlmfb7omq3tfr3qhyd.onion/	需要特定后缀/生效

表 8:Weaxor 暗网博客

勒索聊天页面：

图 26:Weaxor 勒索家族聊天页面截图

（2）BeijingCrypt

- **本地化特征**：主要以中国企业为攻击目标，常年位居活跃榜前列。
- **攻击手法**：利用 RDP 暴力破解和钓鱼邮件进行撒网式攻击，针对中小企业及部分关键基础设施。
- **市场份额**：2025 年统计数据显示，其占据国内勒索软件市场约 8%—11% 的份额。

① 勒索信

!_INFO.txt

图 27:BeijingCrypt 勒索家族勒索信

② 沟通渠道

BeijingCrypt 勒索家族无暗网界面，通过高匿名邮箱与受害者交流

类型	指标值	发现时间
邮箱	wxxxxxco@gmail.com	2024-11-11
邮箱	wxxxxxco@cock.li	2025-02-12

表 9:BeijingCrypt 暗网博客

（3）盗版 LockBit 3.0

- **成因**：由于 LockBit 3.0 构建器（Builder）源码泄露，大量技术门槛较低的攻击者利用该工具生成自定义变种。
- **危害**：导致基于该家族源码的变种在全球及国内泛滥，攻击者水平参差不齐，且由于缺乏官方维护，解密工具的可靠性极低。

图 28:LockBit 3.0 Builder 在 Twitter 上泄露

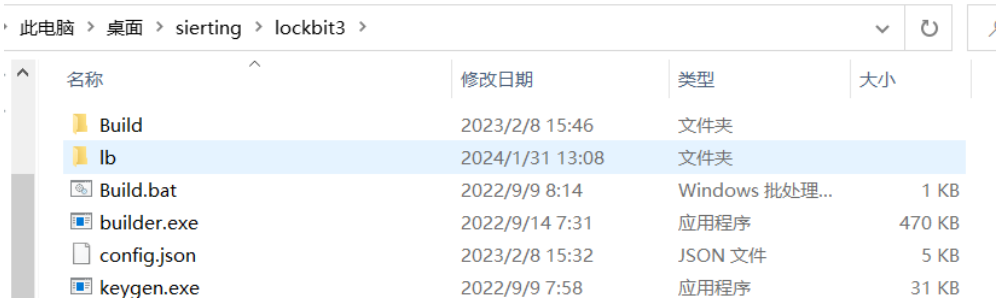


图 29:LockBit 3.0 构建器

① 勒索信

README_lockbit.txt

图 30:盗版 LockBit 3.0 勒索家族勒索信

OnZmO436e.README.txt

图 31:盗版 LockBit 3.0 勒索家族勒索信

RECOVER-IPRan59a9-FILES.txt

图 32:盗版 LockBit 3.0 勒索家族勒索信

② 沟通渠道

由于 Lockbit 3.0 构建器（Builder）源码泄露，攻击者可自定义勒索信中的联系信息，导致基于该家族源码的变种在全球范围内泛滥。

类型	指标值
邮箱	rexxxxxxg25@gmail.com
Tox	BF2FBB22C4CFD24EF9Axxxxxxxxxx393E846514659C59D8C52F43CBD76209603AE
Tox	66049CB849C457B3253xxxxxxxxxxC3A911E29CE1C3EAD3D403C16E74FF8AEB5030A11
邮箱	lockaxxxxxxxxxbit@proton.me

表 10:盗版 LockBit 3.0 暗网博客

（4） Rast Gang

- **技术架构**：采用 **Rust** 语言编写，展现出极快的加密速度。
- **战术风格**：快节奏攻击，获取服务器权限后立即部署勒索，不追求深度横向移动，对边界防御提出极大挑战。
- **攻击入口**：RDP 爆破与 N-day 漏洞组合利用。

① 勒索信

readme.txt

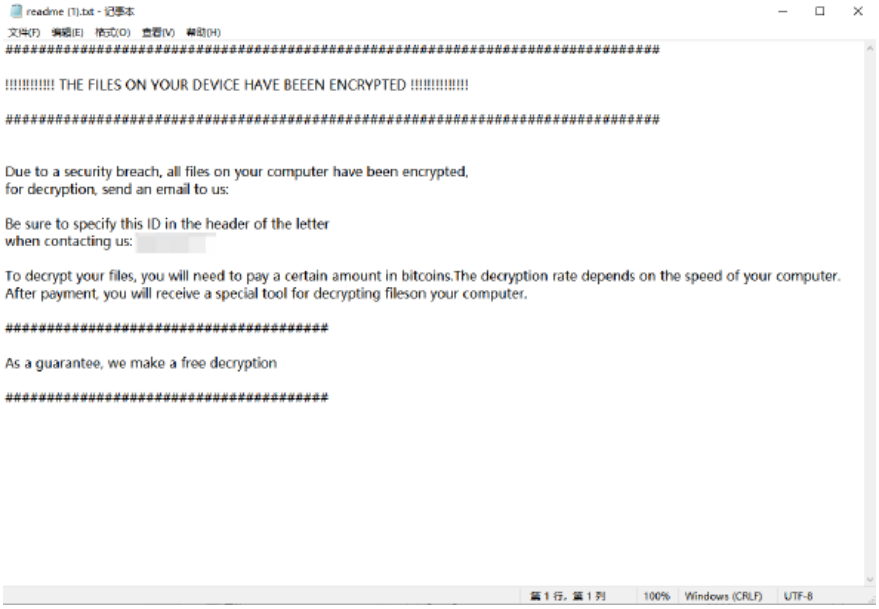


图 33:Rast Gang 勒索家族勒索信

INFORMATION.txt

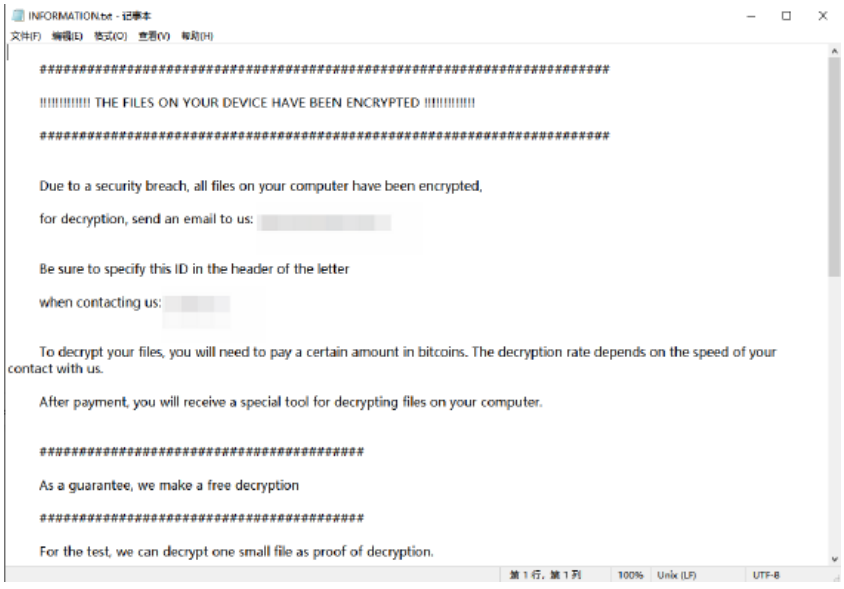


图 34:Rast Gang 勒索家族勒索信

② 沟通渠道

Rast Gang 勒索家族无暗网界面，通过高匿名邮箱与受害者交流

类型	指标值
邮箱	rexxxxxxxg25@gmail.com
Tox	BF2FBB22C4CFD24EF9Axxxxxxxxxx3E2340393E846514659C59D8C52F43CBD76209603AE
Tox	66049CB849C457B325xxxxxxxxxF558DAC3A911E29CE1C3EAD3D403C16E74FF8AEB5030A11
邮箱	LockXXxxxxxxxxxbbit@proton.me

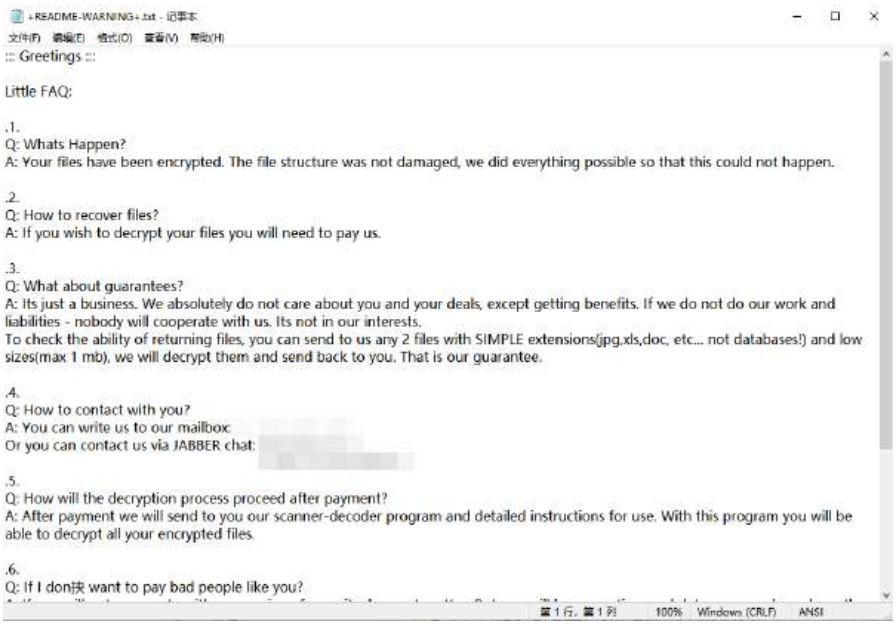
表 11:Rast Gang 暗网博客

（5）Makop

- **家族谱系**：**Phobos** 家族的代表性变种。
- **技术集成**：深度集成 AES-CBC 与 RSA 非对称加密算法。
- **机会主义**：主要利用缺乏防护的 RDP 端口或钓鱼邮件漏洞渗透内网。

① 勒索信

+README-WARNING+.txt


+README-WARNING+.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

::: Greetings :::

Little FAQ:

.1.
Q: Whats Happen?
A: Your files have been encrypted. The file structure was not damaged, we did everything possible so that this could not happen.

.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay us.

.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc... not databases!) and low sizes(max 1 mb), we will decrypt them and send back to you. That is our guarantee.

.4.
Q: How to contact with you?
A: You can write us to our mailbox:
Or you can contact us via JABBER chat:

.5.
Q: How will the decryption process proceed after payment?
A: After payment we will send to you our scanner-decoder program and detailed instructions for use. With this program you will be able to decrypt all your encrypted files.

.6.
Q: If I don扶 want to pay bad people like you?

第 1 行，第 1 列 100% Windows (CRLF) ANSI

图 35:Makop 勒索家族勒索信

② **沟通渠道**

Makop 勒索家族无暗网界面通过高匿名邮箱与受害者交流

类型	指标值
邮箱	jaxxxxxter65@2mail.co
邮箱	terexxxxxco136@onionmail.com
邮箱	backxxxxxup@cyberfear.com
邮箱	Faxxxr@mailum.com

表 12:Makop 暗网博客

3.勒索家族加密方式分析

加密阶段作为攻击链（Kill Chain）的末端环节，直接决定了数据恢复的可能性。基于 Solar 团队对 2025 年捕获的 **35+** 个活跃家族样本的逆向工程分析，勒索软件的加密机制已呈现出**高度标准化**与**算法混合化**的特征。

技术演进趋势：

1. **混合加密架构**：普遍采用“对称加密（文件内容）+ 非对称加密（会话密钥）”的模式，在保证加密速度的同时确保密钥无法被破解。
2. **算法多样性**：除了传统的 RSA + AES 组合，越来越多的家族（如 Weaxor, LockBit 4.0）开始采用 **Curve25519 (X25519)** 等椭圆曲线算法，以提升密钥生成与交换的效率。
3. **语言迁移**：Go 和 Rust 语言因其跨平台特性和较高的逆向分析难度，正逐渐取代 C/C++ 成为勒索软件开发的首选。

部分活跃家族加密算法特征表：

勒索家族	病毒语言	非对称密钥生成
LVT	GO	内置 RSA 公钥 ECC 本地生成私钥
Phobos	C/C++	内置 RSA 公钥
Live1.0	C/C++	内置于加密器中
Live1.5	C/C++	内置于加密器中
Live2.0	C/C++	内置于加密器中
DevicData	C#	内置 RSA 公钥
tellyouthepass	C#	内置 RSA 公钥
mallox	C/C++	内置 CURVE25519 公钥
Rast Gang	RUST	内置 RSA 公钥

勒索家族	病毒语言	非对称密钥生成
MEDUSALOCKER(EXSI)	C/C++	内置 RSA 公钥
MEDUSALOCKER(Windows)	C/C++	内置 RSA 公钥
Wormhole	C/C++	
Babuk(Windows)	C/C++	内置 CURVE25519 公钥
Babuk(NAS)	GO	内置 CURVE25519 公钥
Babuk(ESXI)	C/C++	内置 CURVE25519 公钥
TargetOwner	C#	内置 RSA 公钥
Steloj	C/C++	内置 RSA 公钥
BeijingCrypt	C/C++	内置 RSA 公钥
lol	PYTHON	无
Makop	C/C++	内置 RSA 公钥
盗版 LB3	C/C++	内置 RSA 公钥
Fx9	C/C++	内置 RSA 公钥
Ransomhub	GO	内置 RSA 公钥
Weaxor	C/C++	内置 CURVE25519 公钥
Medusa	C/C++	内置 RSA 公钥
888	C#	根据计算机信息和结合密钥文件和文件名生成

勒索家族	病毒语言	非对称密钥生成
Lockbit4.0	C/C++	内置 X25519 公钥
MedusaLocker	C/C++	内置 RSA 公钥
DragonForce	C/C++	内置 RSA 公钥
BEAST	C/C++	内置 CURVE25519 公钥
BEAST-helper	C/C++	内置 CURVE25519 公钥
Taps	C#	内置 RSA 公钥

表 13:加密算法特征表

通过对上述样本的分析，我们确认：一旦文件被这些成熟家族加密，在没有私钥的情况下，通过技术手段暴力破解的可能性**微乎其微**。这也再次强调了事前防御与备份机制的重要性。

（二） 勒索软件入侵路径与传播机制深度分析

在 2025 年的应急响应实战中，Solar 威胁情报中心发现攻击者的行为展现出极强的“工业化”特征。攻击者已不再依赖随机的单点突破，而是通过成熟的黑产供应链获取初始权限 。

1. 初始入侵矢量分布：身份验证与边界漏洞的双重溃败

根据 Solar 团队对 534 起真实案例的复盘分析，攻击者的入侵路径分布如下:

- **RDP 与凭据泄露（45%）**：这是目前最主要的攻击入口。攻击者往往通过暗网的初始访问经纪人（IAB）直接购买已被窃取的服务器凭据，或针对未启用多因素认证（MFA）的远程接入点进行暴力破解 。
- **高危漏洞利用（30%）**：重点集中在 VPN 网关、OA 系统及虚拟化平台（如 ESXi）。攻击者利用漏洞从被发布到武器化的“时间差”，在企业尚未完成补丁修复前完成批量植入 。
- **弱口令与数据库暴露（12%）**：Weaxor（Mallox 变种）等家族专门针对公网暴露的 MS-SQL 数据库（1433 端口）进行自动化扫描，通过 CLR 程序集加载恶意代码 。
- **钓鱼邮件与社会工程学（10%）**：攻击者伪装成求职简历、财务账单，诱导员工运行带有恶意宏或后门的附件。

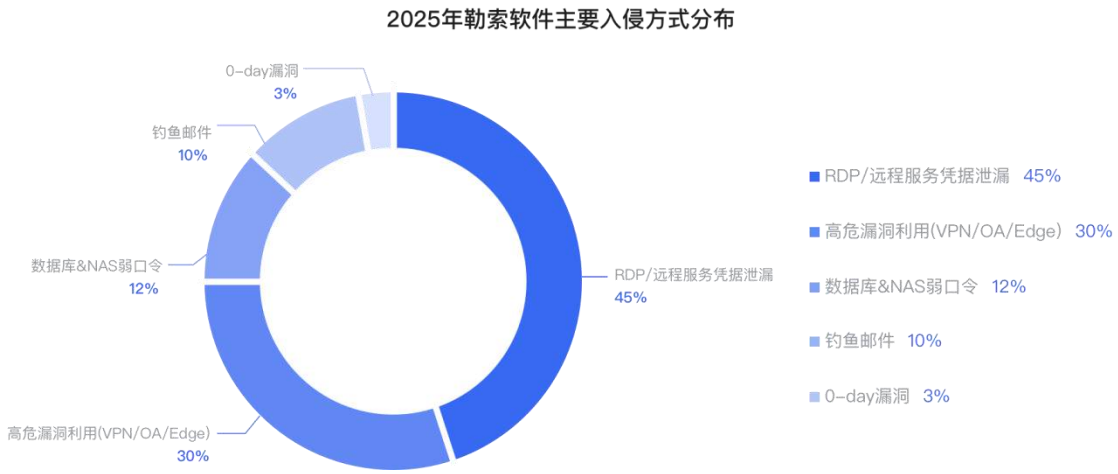


图 36:勒索软件传播方式

2. 关键入侵战术简介

（1） 身份认证攻击：从爆破到凭据利用

攻击者不再仅仅依赖简单的暴力破解。通过实战观察，攻击者在获取初始 RDP 权限后，会迅速部署 `Mimikatz` 或 `WebBrowserPassView` 等工具，从内存或浏览器

中提取更高级别的管理员凭据，为后续的全域渗透做准备 。

（2） 漏洞武器化：针对核心业务系统的定向突防

攻击重点已从通用系统转向核心支撑平台。例如，飞塔（Fortinet）防火墙的 SSL VPN 组件漏洞常被用于在无凭据状态下执行恶意代码（RCE），直接绕过边界防御 。

（3） 技术特征示例：Weaxor 家族的投递脚本

Weaxor 家族在入侵过程中，常利用系统合法的 `sqlps.exe`（SQL Server 专属 PowerShell 环境）来规避传统 EDR 的监控。

```
Plain Text
代码块
# 攻击者常用的混淆执行示例 （去敏感化）
$s = New-Object IO.MemoryStream(,[Convert]::FromBase64String("恶意载荷 B64 内容..."));
IEX (New-Object IO.StreamReader($s)).ReadToEnd;
# 核心逻辑：利用合规进程加载 Shellcode 到内存，实现无文件执行
```

（4）云环境与边界资产暴露风险

随着网络边界的防御重心向应用层转移，作为企业内网“守门人”的**边界网络设备**（如防火墙、VPN 网关、SD-WAN 设备）正面临前所未有的安全挑战。攻击者不再试图“撞破”防火墙的策略配置，而是直接利用**设备自身的系统漏洞**进行突防。

监测发现，以 **Fortinet（飞塔）** 为代表的主流防火墙设备成为攻击者的重点狩猎目标。攻击者利用其 **SSL VPN 组件**中存在的严重漏洞（如堆栈溢出、认证绕过漏洞），可在无需任何有效凭据的情况下，直接远程执行恶意代码（RCE）或读取设备内存中的敏感数据（如明文账号密码、Session ID）。一旦边界网关失陷，攻击者即刻获得内网流量的解密能力与访问权限，使后续的横向移动畅通无阻。

（三）2025 年勒索组织演化与家族更替情况

在 2025 年的网络威胁版图中，勒索软件家族的更替频率与技术迭代速度均创下历史新高。基于 Solar 安全团队对全球威胁情报、暗网监测及一线应急响应数据的关联分析，当前的勒索生态呈现出**组织架构平台化**与**攻击链条工业化**的显著特征。

1. 年度新增传统勒索组织态势

2025 年内，我们持续跟踪并发现了多起新出现的勒索软件家族。这些家族大多摒弃了从零开发的低效模式，转而采用 **RaaS（勒索软件即服务）** 架构。通过复用成熟的加密组件和攻击工具链，这些新兴组织能够在极短时间内形成规模化打击能力。

以下为 2025 年典型新增家族的时间分布：

月份	勒索家族
1 月	Morpheus、GDLockerSec、Linkc
2 月	Nightspire、Teamxxx、J、Chaos、Anubis
3 月	Crazyhunter、Crypto24、Skira、Vanhelsing、Secp0、Nova、Devman、Ralord、Arkana
4 月	Warlock、C3Rb3R、Bert、Brotherhood、Gunra、Direwolf、Payoutsking、Silent
5 月	IMNCrew
6 月	Global、Walocker、Securotrop、Kawa4096、Pear、Cephalus
7 月	Sinobi、Satanlockv2、D4rk4rmy、盗版 Mallox、Rebornvc、Backups、Bqtlock、Hegentlemen
8 月	Radar、Desolator、Obscura
9 月	Lockbit5.0、Lunalock、Yurei、Blackshrantac
10 月	Nasirsecurity、Kryptos、Radiant、Tacksas、Nilson、Tengu
11 月	LockXX、Kazu、Tridentlocker、Benzona

月份	勒索家族
12 月	Minteye、Osiris、Ms13089

表 14:2025 年典型新增家族

针对本年度新增的勒索软件家族，Solar 团队选取其中具有代表性的典型家族进行重点分析与说明:

2. 代表性新增家族深度分析

2.1 TheGentlemen 勒索家族（2025 年 8 月出现）

组织特征：该组织展现出极高的职业化水准，拥有完善的暗网泄密站点和基于 TOX 协议的加密沟通渠道。其核心成员被认为来自此前被重创的大型勒索家族残余 。

- **技术路径**：初始入侵主要利用边界设备（如 FortiGate）漏洞或从初始访问经纪人（IABs）处购买权限 。该家族具备 **BYOVD（自带易受攻击驱动）** 能力，能强制终止主机上的终端检测与响应（EDR）进程 。
- **行业偏好**：制造业是其重点打击目标，占比达 28.6% 。此外，该组织表现出极强的“断后”意识，曾定向攻击数据恢复公司，意图切断受害者的外部救援路径 。

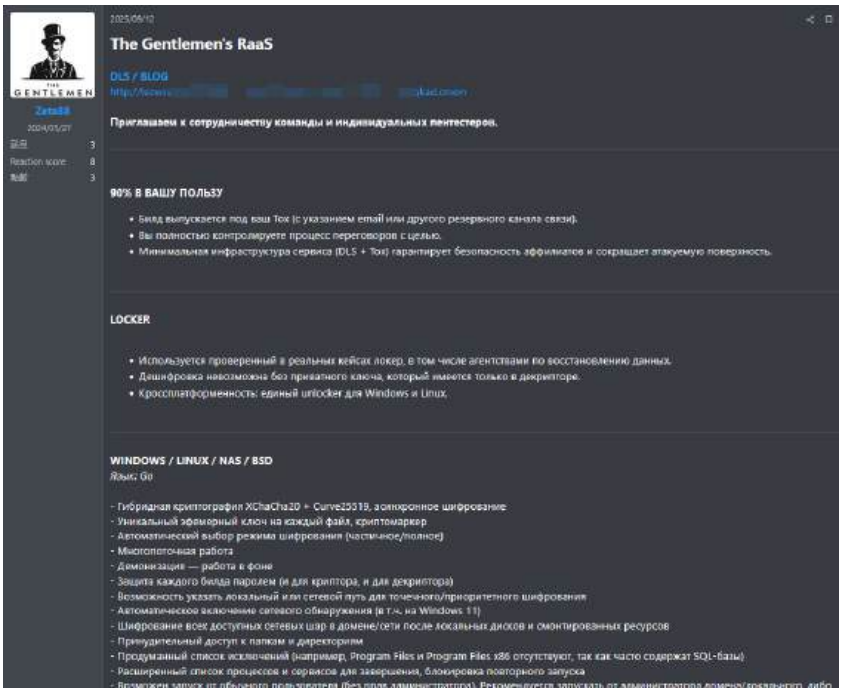


图 37:TheGentlemen 勒索家族勒索信

2.2 LockXX 勒索家族（2025 年 11 月活跃）

- **组织特征**：表现出极强的本地化属性，其勒索信原生支持**标准中文**与英文双语切换，这在国际勒索家族中较为罕见 。
- **技术路径**：深度利用 Windows 系统机制（如 UAC 用户账户控制）进行权限提升，直至 2025 年底仍处于高频活跃状态 。

图 38:LockXX 勒索家族勒索信

2.3 LockBit 5.0（2025 年 9 月发布）

- **背景演变**：继“克罗诺斯行动”遭受重创后，LockBit 试图通过 5.0 版本挽回品牌声誉 。该版本将加盟费用调整为 500 美元，试图通过低价策略快速重组其附属成员网络 。
- **核心策略**：依然维持传统的 RaaS 模式，但在基础设施隐蔽性上做了针对性加固 。

图 39:Lockbit5.0 发布声明

2025 年 9 月，LockBit 5.0 发布。2025 年 9 月初，LockBit 勒索组织在 RAMP 论坛宣布，在 LockBit 诞生 6 周年之际推出 Lock Bit 5.0。其暗网博客显示的加盟费用为 500 美元，标志着其向 RaaS 运营模式的转变和加盟便利化的进程。（其初期要求加盟组织支付 1 比特币（BTC），克罗诺斯行动后要求的加盟金额则为 777 美元。）

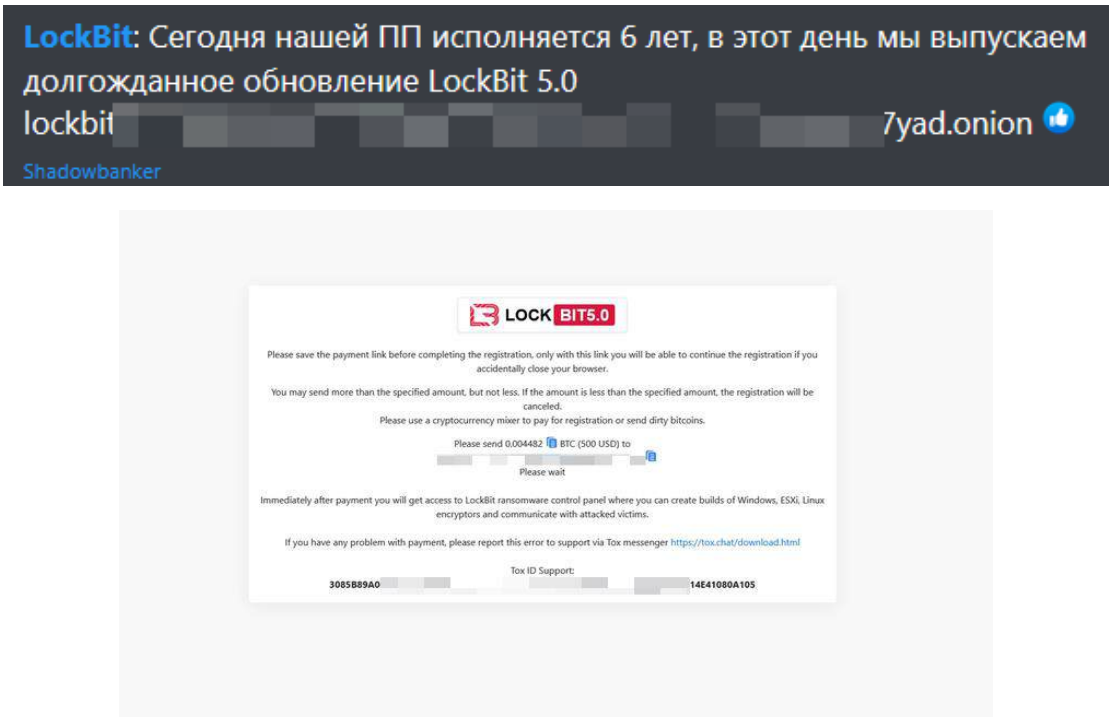


图 40:Lockbit5.0 暗网公告

图 41:Lockbit5.0 勒索家族勒索信

3. 双重/多重勒索组织的演进

2025 年，单纯的“加密勒索”已退居二线，**“加密+窃密”的双重勒索**，乃至加入 DDoS 攻击的**多重勒索**已成为主流组织的标配。

勒索家族	勒索模式	出现时间	状态
Phobos	加密文件	2019-5-1	离线
Makop	加密文件	2020-1-1	存活
Clop	加密文件&数据窃取	2020/3/13	存活
Babuk	加密文件&数据窃取	2020/10/25	离线
Ghost	加密文件&数据窃取	2021 年初	离线
RansomHouse	加密文件&数据窃取	2021/6/1	存活
Everest	加密文件&数据窃取	2021/9/9	存活
Qilin	加密文件&数据窃取	2022/10/8	存活
Mallox	加密文件&数据窃取	2022/11/4	离线

勒索家族	勒索模式	出现时间	状态
Medusa Locker	加密文件&数据窃取	2022/11/15	存活
Play	加密文件&数据窃取	2022/11/26	存活
Medusa	加密文件&数据窃取	2023/1/11	存活
Akira	加密文件&数据窃取	2023/4/26	存活
8Base	加密文件&数据窃取	2023/5/23	离线
Rhysida	加密文件&数据窃取	2023/6/5	存活
Cactus	加密文件&数据窃取	2023/7/20	存活
Incransom	加密文件&数据窃取	2023/8/9	存活
Hunters International	加密文件&数据窃取	2023/10/20	离线
DragonForce	加密文件&数据窃取	2023/12/13	存活
Rast Gang	加密文件	2024/2/4	存活
RansomHub	加密文件&数据窃取	2024/2/10	离线
Lvt	加密文件	2024/2/29	离线
Eldorado	加密文件&数据窃取	2024/6/6	离线
Tellyouthepass	加密文件	2024/6/6	存活

勒索家族	勒索模式	出现时间	状态
BeijingCrypt	加密文件	2024/6/26	存活
Fog	加密文件&数据窃取	2024/7/16	离线
GlobeImposter	加密文件&数据窃取	2024/9/1	离线
Sarcoma	加密文件&数据窃取	2024/10/9	存活
888	加密文件&数据窃取	2024/10/15	存活
Weaxor	加密文件	2024/11/11	存活
盗版 lockbit3.0	加密文件	2024/11/12	存活
MoneyIsTime	加密文件	2024/11/20	存活
FunkSec	加密文件&数据窃取	2024/12/4	存活
DevicData	加密文件	2024/12/4	存活
Secp0	加密文件&数据窃取	2025/3/14	存活
Devman	加密文件&数据窃取	2025/4/6	存活
World Leaks	数据窃取	2025/5/18	存活
Kalxat	加密文件	2025/5/21	存活

勒索家族	勒索模式	出现时间	状态
Dire Wolf	加密文件&数据窃取	2025/5/27	存活
Eos	加密文件	2025/5/28	存活
Sinobi	加密文件&数据窃取	2025/7/5	存活
Beast	加密文件&数据窃取	2025/7/29	存活
Blacknevas	加密文件&数据窃取	2025/8/6	存活
Cephalus	加密文件&数据窃取	2025/8/26	离线
Lunalock	加密文件&数据窃取	2025/9/2	存活
Yurei	加密文件&数据窃取	2025/9/5	离线
The Gentlemen	加密文件&数据窃取	2025/9/9	存活
Radiant	加密文件&数据窃取	2025/10/12	离线
LockXX	加密文件	2025/11/5	存活
Lock Bit 5.0	加密文件&数据窃取	2025/12/7	存活

表 15:勒索组织的演进

3.1 Makop 勒索家族

Makop 勒索软件最早于 2020 年 1 月被安全社区捕获，是 Phobos 勒索软件家族的一个变种或衍生。Phobos 勒索软件家族自 2018 年被发现，是 Dharma（又名 CrySis）勒索家族的一个衍生分支。Makop 勒索软件家族自 2020 年初次现身以来，该组织凭借其源自 Phobos/Dharma 家族的稳固代码基础、去中心化的附属（Affiliate）运营模式以及对远程桌面协议（RDP）等基础服务的极致利用，成功穿越

了多个威胁周期，并在 2025 年展现出显著的技术迭代与战术升级。Makop 虽然起源于 Phobos 家族，共享相似的加密结构和勒索信格式，但在 2025 年已发展出独特的技术特征。新发现的 Core 变种引入了 `.core` 扩展名和更激进的系统篡改手段，显示了持续的开发投入 。 Makop 不设公开的数据泄露网站（DLS），但 Core 变种的勒索信中明确出现了“数据已被盗取”的威胁，暗示其双重勒索模式，以增加谈判筹码 。

Makop 继承了 Phobos 的许多底层特征，包括使用 AES-256 加密文件内容并用 RSA 密钥保护会话密钥的加密方案。更直观的证据在于其文件命名约定——[原始文件名].[攻击者邮箱].扩展名——这种格式是 Phobos/Dharma 家族的标志性签名 。此外，早期的 Makop 变种在勒索信的措辞和结构上也与 Phobos 高度相似，甚至在某些情况下直接复用了 Phobos 的解密指令模板。

Makop 的运营者在 2020 年后开始维护独立品牌。他们修改了加密算法的实现细节，引入了更快的加密流程，并开始在俄语地下论坛（如 Exploit, XSS）以独立的 RaaS（勒索软件即服务）项目进行招募 。这表明 Makop 的核心团队可能包含从 Phobos 组织分裂出来的核心开发者，对源码进行了独立的分支维护。

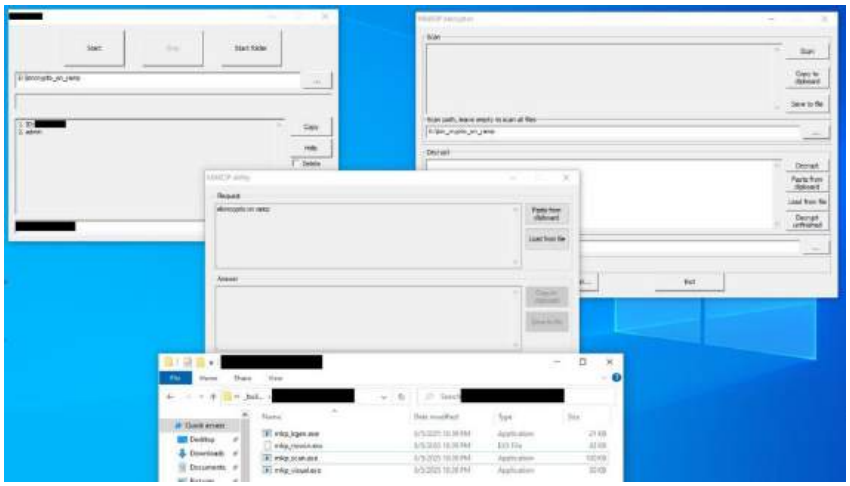


图 42:Makop 加密器截图

图 43:Makop 勒索家族勒索信

3.2 Rast Gang 勒索家族

Rast Gang 最早活跃于 2023 年 12 月，其活动轨迹与国内大量出现的“.rast”后缀或带有 Rast 特征的勒索事件高度吻合 。虽然该组织在规模和全球影响力上尚未达到国际顶级威胁组织的标准，但其对中国国内关键信息基础设施及其供应链造成较大的危害。该组织的命名直接源于其勒索软件的名称“Rast”。这一名称本身可能暗示了其开发语言（Rust）的谐音，或者是攻击者为了彰显品牌而特意选取的标识。情报显示，Rast Gang 是一个快节奏的勒索运营商，其核心目标是在最短时间内完成从入侵到变现的闭环，并非在目标网络中进行广泛的横向移动、数据窃取以及权限维持，而是通过边界服务器（如 Web 服务器、VPN 网关、跳板机）获得访问权限，便会立即着手部署勒索软件。Rast Gang 表现出极强的地域针对性。通过对捕获的恶意样本、攻击节点 IP 以及受害者数据的分析，可以确认其主要攻击目标集中在中国境内。

Rast Gang 在早期活动中使用了大量与 Phobos 和 Makop 勒索家族重叠的联系邮箱。例如，xxx@xxx.club 等邮箱地址曾频繁出现在 Phobos 变种（如 Faust）和 Makop 变种的赎金信中 。Rast Gang 的核心成员可能曾是 Phobos 或 Makop RaaS（勒索软件即服务）平台的附属会员（Affiliate）或者为同时运营多个勒索品牌。

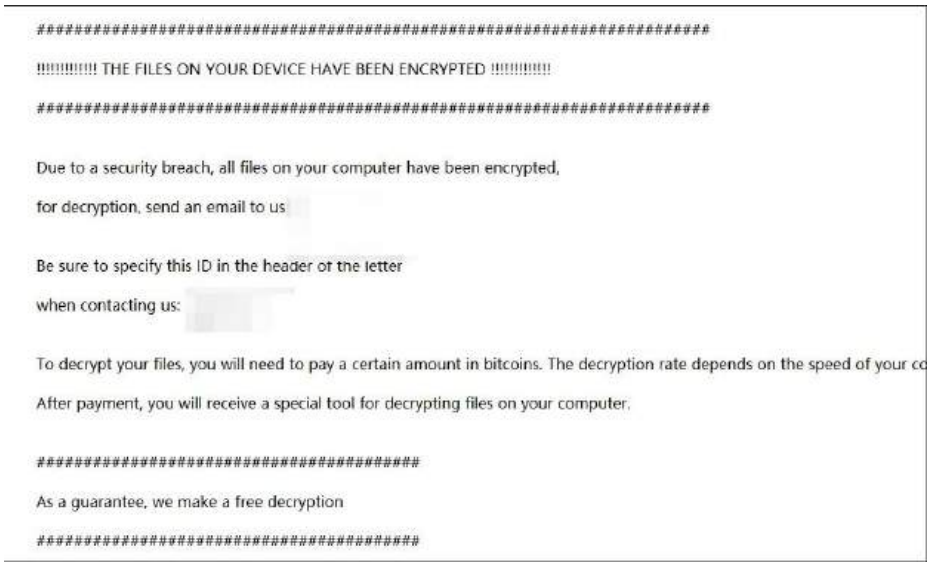


图 44:Rast Gang 勒索家族勒索信

3.3 MedusaLocker 勒索家族

MedusaLocker 家族首次于 2019 年 9 月出现，MedusaLocker 勒索软件攻击者通常通过有漏洞的远程桌面协议（RDP）配置获取受害者设备访问权限，攻击者还经常使用电子邮件钓鱼和垃圾邮件活动——直接将勒索软件附加到电子邮件中——作为初始入侵渠道。MedusaLocker 对受害者的数据进行加密，并在包含加密文件的每个文件夹中留下带有通信说明的赎金票据。该说明指示受害者向特定的比特币钱包地址提供勒索软件付款。

MedusaLocker 似乎根据观察到的赎金支付拆分作为勒索软件即服务 （RaaS）

模型运行。典型的 RaaS 模型涉及勒索软件开发人员和在受害者系统上部署勒索软件的各种附属公司。MedusaLocker 勒索软件付款似乎始终在附属公司之间分配，附属公司收到 55% 到 60% 的赎金；以及接收剩余部分的开发人员。

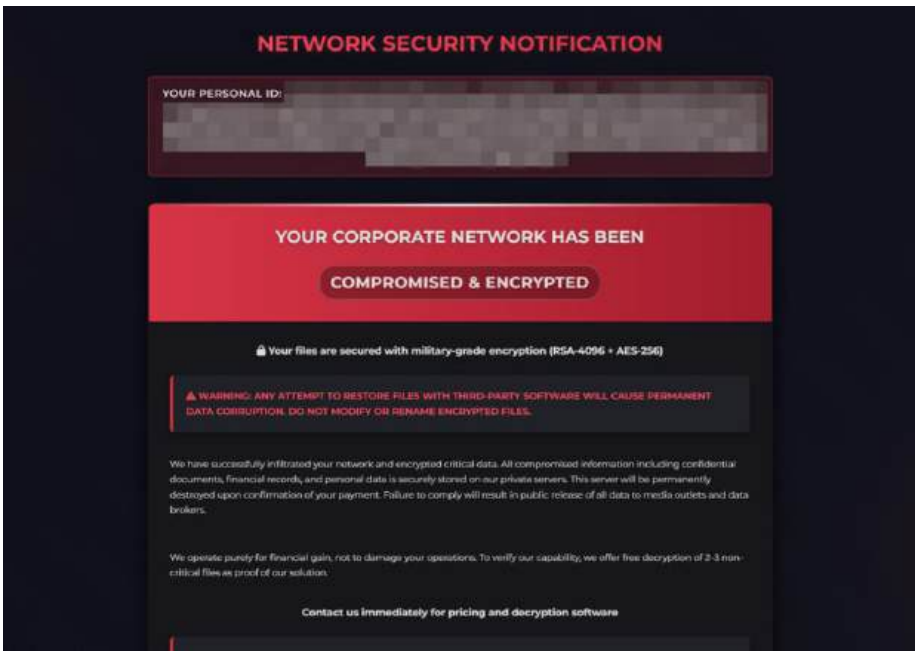


图 45:MedusaLocker 勒索家族勒索信

关键趋势研判：

- **去加密化（无加密勒索）的兴起**：以 **World Leaks** 为代表的组织开始放弃复杂的加密环节，直接转向纯粹的数据泄露威胁。这种模式降低了维护加密器的技术成本，同时避开了部分企业的备份恢复策略，直接打击企业的声誉与合规底线。
- **供应链纵深打击**：攻击者不再满足于单一终端的加密，而是通过渗透虚拟化平台（如 **VMware ESXi**）或存储系统（NAS），实现“一键瘫痪”整个企业数据中心的能力。

第二章　勒索软件受害者画像与风险特征分析

为更准确地刻画当前勒索软件攻击的真实态势与风险分布特征，Solar 团队基于近一年实际处置的勒索事件、暗网泄露数据及样本分析结果，对受害单位的**地理分布、受攻击系统与平台类型以及所属行业结构**进行了系统梳理与统计分析。

本节分析所使用的数据均来源于**真实勒索攻击案例**，涵盖已确认受害单位及其相关攻击环境信息，并通过去重、归类与交叉验证后形成统计结果。相关结论以**可视化饼状图**形式呈现，旨在从宏观视角揭示勒索攻击的主要受害区域、重点攻击目标系统以及高风险行业分布特征，为后续风险评估、防护策略制定与应急响应能力建设提供数据支撑。

（一）受害单位地理分布特征

基于 Solar 团队对 2025 年度国内勒索软件真实受害案例的统计分析可以看出，勒索攻击在省级层面呈现出高度集中、明显分层的地理分布特征；与此相对应，团队应急响应支撑足迹已覆盖全国 30+ 个省、自治区、直辖市，形成跨区域、跨行业的快速联动处置能力，持续为政企客户提供“研判—遏制—清除—恢复—加固—复盘”的闭环交付。

从整体分布来看，**广东、北京、上海、四川、山东**等少数省份和直辖市构成了勒索软件受害的主要集中区域。其中，**Top 5 省份合计占比接近 80%**，其余地区受害占比相对分散，呈现出“头部高度集中、尾部广泛分布”的典型特征。

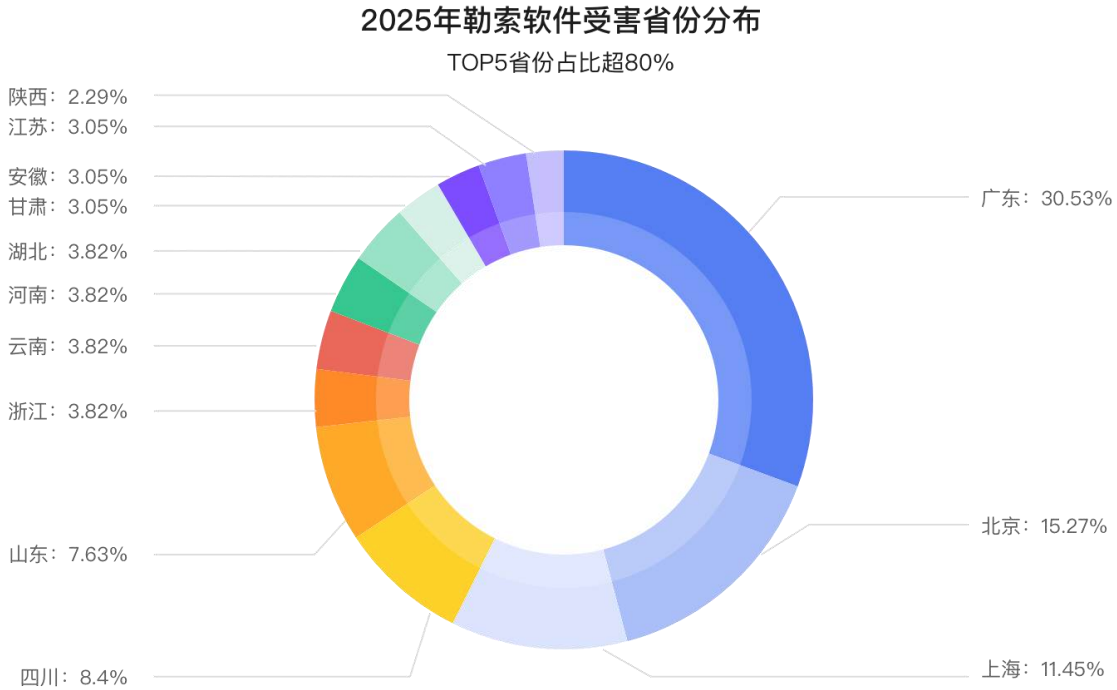


图 46:受害单位地理分布饼状图（基于真实案例）

图 47:全国应急响应支撑覆盖地图

（二）受攻击系统与平台类型分布

2025 年受灾资产操作系统分布研判数据显示，**老旧服务器资产已成为勒索攻击的“重灾区”**。其中，**Windows Server 2008 (21.8%)** 与 **Windows Server 2012 (20.38%)** 合计占据了超过 42% 的受害比例，这表明攻击者正集中利用 EOL（已停止维护）系统的未修补漏洞进行定向突防。虽然 Windows 10 (15.17%) 在终端侧仍面临较高风险，但值得警惕的是，**ESXi、NAS 及 Linux** 等关键基础设施也开始频繁出现在受害清单中（合计约 5.2%），预示着攻击面正从传统 Wintel 架构向虚拟化与存储层级深度扩展。

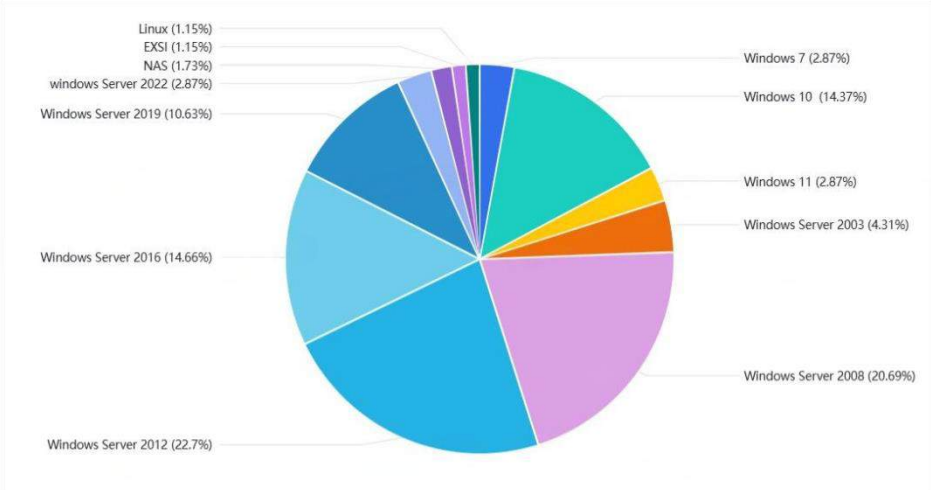


图 48:受影响操作系统分布饼状图（基于真实案例）

（三）受害单位所属行业分析

2025 年勒索攻击行业受灾态势研判数据揭示了整体攻击重心向“高价值、低容忍”的关键民生领域发生惊人倾斜。**医疗行业（23.97%）**以绝对劣势沦为勒索攻击的头号“重灾区”，占据了近四分之一的受害比例，这表明攻击者正利用医疗数据的高敏感性与业务连续性的弱点进行精准勒索。**制造业（15.7%）**紧随其后，显示出工业供应链因停产成本高昂而成为黑产眼中的“肥肉”。此外，信息技术（9.09%）与零售（8.26%）的高占比也警示我们，无论是掌握核心技术资产的企业，还是拥有庞大现金流的商贸终端，都已处于勒索攻击的高频打击范围之内。

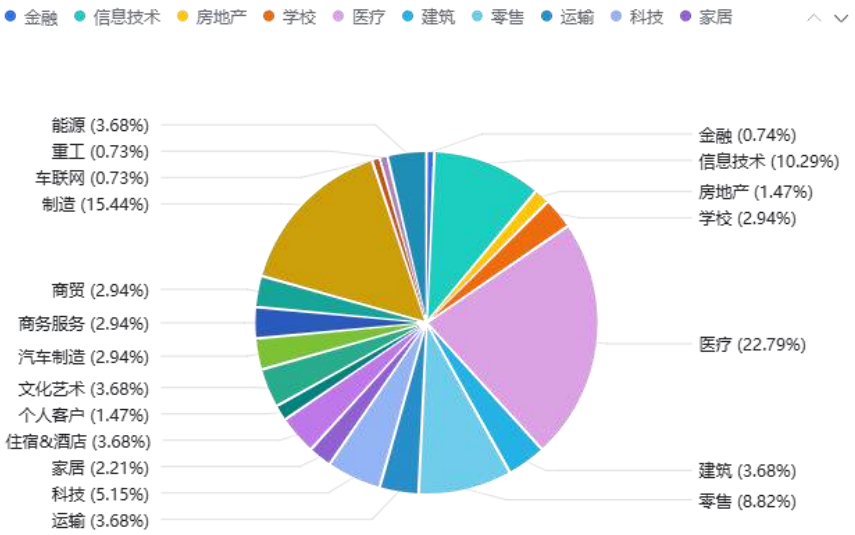


图 49:受影响行业分布饼状图（基于真实案例）

第三章　勒索攻击者行为与攻击手段分析

（一）勒索家族的组织发展与近期事件分析

1.Qilin 与 DragonForce

1.1 引言：从同质化竞争到双极分化

回顾 2024 至 2025 年的网络安全态势，全球勒索软件即服务（RaaS）生态经历了深刻的系统性重塑。这并非简单的技术迭代，而是一场根本性的运营模式变革。根据 Solar 威胁情报中心的持续监测，在国际执法机构高压打击的背景下，勒索软件市场并未萎缩，而是呈现出显著的“双极分化”特征。以 LockBit 被打击后的市场真空为催化剂，生态内部迅速分化为两种截然不同的演进路径：以 DragonForce 为代表的“低门槛规模化扩张”模式，和以 Qilin（麒麟）为代表的“高技术精英化狙击”模式 。本章将深入剖析这两种分化模式的技术特征、攻击链条及实战案例，为企业构建新一代纵深防御体系提供决策依据。

1.2 DragonForce：勒索攻击的“工业化”与规模扩张

在后 LockBit 时代，DragonForce 组织敏锐地捕捉到了底层攻击者市场的需求空白，迅速调整战略，通过降低门槛来换取攻击规模的爆发式增长。

2025 年第四季度，DragonForce 激进地重塑了其招募规则，这一举措在暗网引起了广泛震动。传统的头部勒索组织通常设立数千美元的高昂押金和烦琐的人工审核流程，而 DragonForce 打破了这一行规。情报显示，该组织将加盟费直接降至 500 美元，这一价格仅为行业平均水平的 10%左右，极大地降低了网络犯罪的经济门槛。

运营维度	传统高端 RaaS 模式	DragonForce 扩张模式
加盟押金	$2,000 – $10,000	$500
准入审核	技术面试、历史案例验证	自动化注册（Auto-Reg）
技术支持	专属开发团队支持	模块化自动化生成器
利润分成	60% – 75%	80% 或更高

表 16:勒索家族运营模式

更为关键的变革在于“自动化注册机制（Auto-Reg）”的引入。潜在攻击者不再需要经过复杂的技术面试或背景审查，仅需完成支付，系统便会自动授予管理面板访问权限，并即时分发勒索软件生成器工具包。这种“即付即用”的模式将勒索攻击转化为一种低技能要求的流水线作业，导致了攻击源的大量涌现。

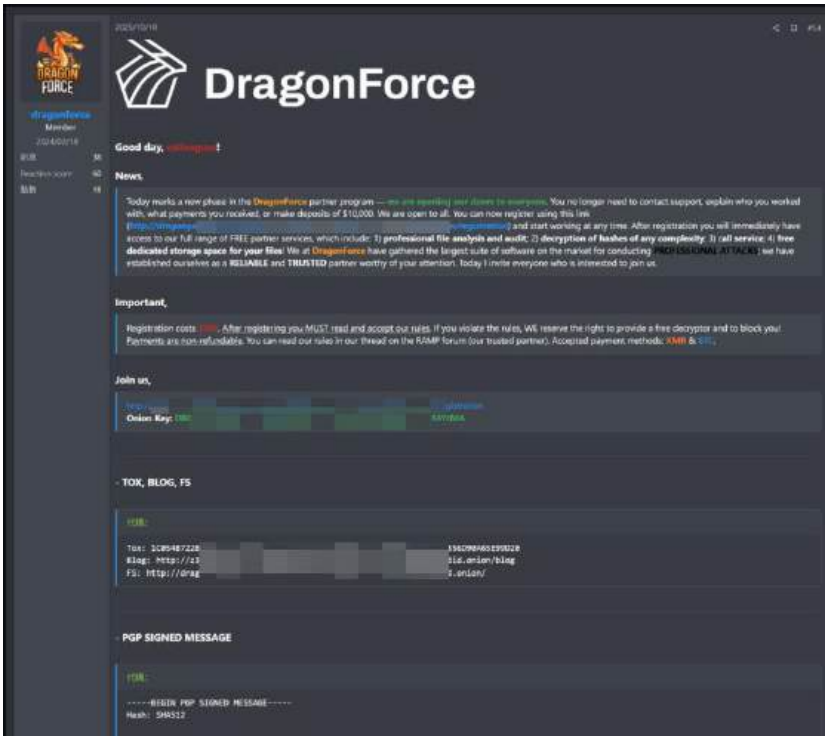


图 50:DragonForce 勒索组织在论坛介绍

在技术层面，为了配合这种“人海战术”，DragonForce 提供了集成化的 BYOVD（Bring Your Own Vulnerable Driver）技术。攻击者利用合法但存在漏洞的内核驱动程序（如 truesight.sys）来强制关闭银行终端上部署的高级检测响应（EDR）系统，从而为后续的渗透扫清障碍。此外，DragonForce 在 2025 年 3 月宣布转型为“勒索软件财团”模式，允许加盟商使用底层技术构建如 Devman 或 Mamona 等“白标品牌”。这种品牌多元化策略有效地规避了执法部门针对单一品牌的集中打击，使得金融机构在进行威胁情报监测时面临更大的识别难度。

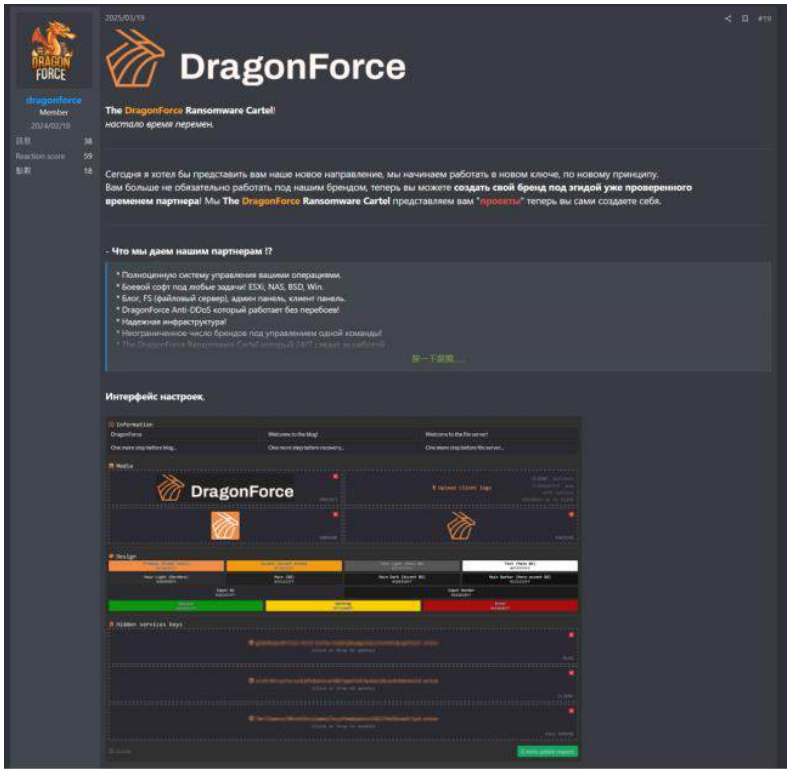


图 51:DragonForce 勒索组织在论坛介绍

1.3 Qilin：法律武器化与针对核心资产的“手术刀式”打击

与 DragonForce 的量产倾销模式形成鲜明对比，Qilin（麒麟）组织选择了一条极度精英化的“高空狙击”路线。该组织通过高昂的准入费用和严格的审核机制，筛选出具备 APT 级别能力的专业团队，专门针对全球核心金融基础设施实施精准打击。

Qilin 在 RAMP 论坛上的招募策略展现了明确的地缘政治与技术筛选逻辑。对于俄语背景的攻击者，其维持免费准入以巩固势力范围；而对于英语及其他语言背景的加盟者，则设立了高达 5,000 美元的“履约保证金”及严格的渗透测试面试。这种机制确保了其成员具备极高的专业水准，主要针对欧美及亚洲发达地区的金融核心系统进行渗透。在技术工具上，Qilin 持续优化基于 Rust 语言编写的高性能勒索载荷，特别是针对 VMware ESXi 和 Linux 系统开发了专用加密器。鉴于现代银行数据中心高度依赖虚拟化架构，一旦 ESXi 宿主机被攻陷，承载核心交易系统和数据库的整个私有云环境将面临瘫痪风险 。

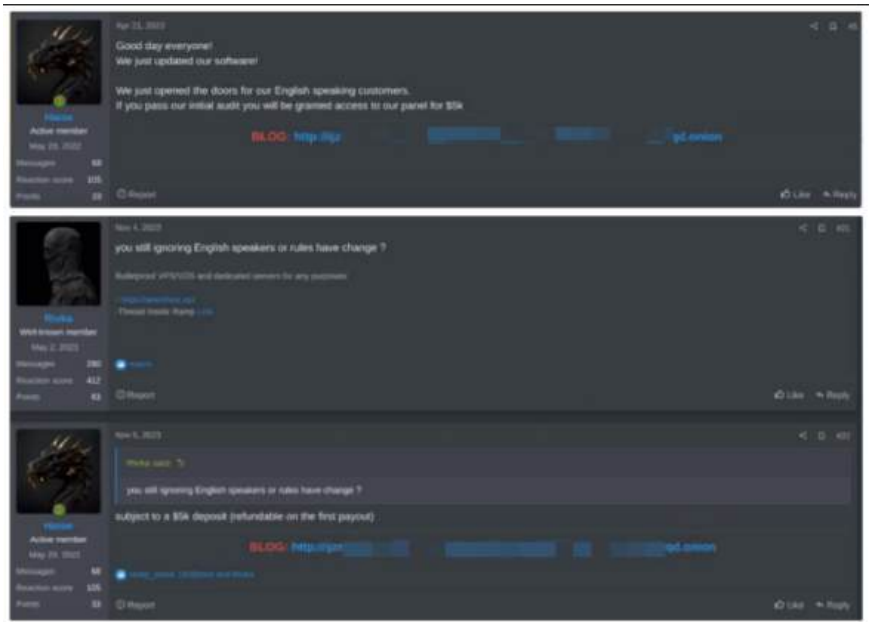


图 52:DragonForce 勒索组织在论坛公开招募价格

更为致命的是 Qilin 战略层面的“法律武器化”转型。2025 年 9 月，Qilin 在其面板中引入了极具创新性的“Call Lawyer”（咨询律师）功能。该组织不再单纯依赖加密数据进行勒索，而是组建专门团队深度挖掘受害者数据中的合规漏洞，如税务违规、洗钱嫌疑（AML/KYC 疏漏）或违反 GDPR 的隐私泄漏证据。一旦发现此类“软肋”，Qilin 会撰写专业的“合规评估报告”并起草致监管机构（如 FBI、各国金融局）的举报信。这种策略迫使金融机构在“支付赎金”与“面临监管重罚及牌照撤销”之间做出选择，将勒索攻击提升到了法律博弈的新高度。

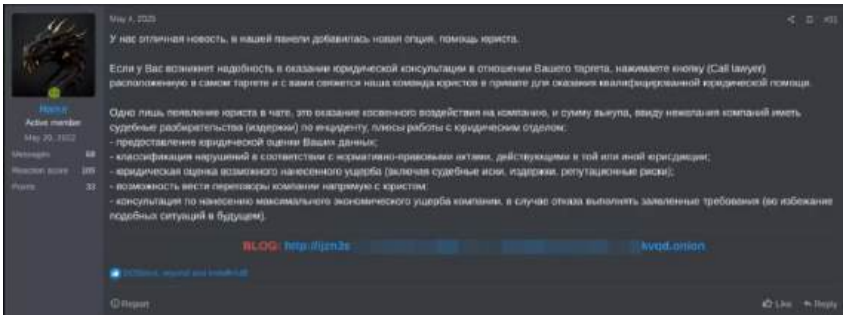


图 53:DragonForce 勒索组织 Call Lawyer 功能

1.4 暗网生态协作与实战案例警示

这两个看似独立的组织在 RAMP（Ransom Anon Market Place）论坛上构成了复杂的协作网络。情报显示，Qilin 的核心管理员“Haise”长期活跃于该论坛，并通过购买昂贵的顶部广告位来掌控流量分发。当潜在加盟商因无法满足 Qilin 的高技术门槛或资金要求时，往往会被广告引导至 DragonForce 的自动化平台。这种“高低搭配”的流量收割模式，表明勒索生态已形成跨组织的协同效应。

图 54:DragonForce 勒索组织核心管理员

2025 年 11 月发生的苏黎世恒比银行（HBZ）数据泄露事件，是这一生态威胁的集中体现。Qilin 组织攻陷该银行并窃取了约 2.5TB 的敏感数据，涵盖了极高价值的客户 KYC 资料（护照、资产证明）、核心交易记录以及内部风控系统源码。分析显示，攻击者在内网潜伏了 30 至 90 天，其间利用合法工具进行横向移动和数据分批渗出，最终在非工作时间对 ESXi 存储卷实施了加密打击。这一案例警示我们，防御的重心必须从单纯的“预防加密”前移至对“数据渗出”和潜伏期流量异常的全路径监测。

1.5 迈向“主动式”安全防御体系

面对 DragonForce 的“人海战术”与 Qilin 的“法律合规勒索”，传统的单点防御已难以为继。各组织机构必须构建涵盖技术、合规与情报的三位一体防御体系。

首先，针对自动化攻击，需强化终端防护的“内核级”博弈，实施基于硬件信任根（TPM）的驱动校验以抵御 BYOVD 攻击，并全面推行基于 FIDO2 的硬件密钥（UKey）以对抗自动化凭据填充。同时，必须部署自动化外部攻击面管理（EASM），像攻击者一样高频扫描并清理未加固的 RDP 和 VPN 节点。

其次，应对“法律武器化”威胁，合规部门应制定“勒索软件专项法律响应剧本”，定期进行数据泄露后的法律压力测试。对于非核心业务数据，应采用国密标准进行静态脱敏加密，确保即使数据被窃，攻击者也无法获取明文内容作为法律勒索的筹码。

最后，建立基于暗网情报的主动闭环至关重要。通过对 RAMP 论坛中核心人物（如 Haise）的持续监测、分析加盟费用的异动以及追踪“防弹托管”服务商的流量特征，金融机构可以实现从被动响应到主动预警的战略跨越，从而在日益严峻的跨境勒索浪潮中守护信用基石。

2.关于 LockBit 兴衰全貌的深度长文分析

2.1 帝国崛起：从“.abcd”到高度企业化的 RaaS 巨头

LockBit 的发家史本质上是一部将网络犯罪进行“极致商业化”的演进史。该组织最早于 2019 年 9 月以“.abcd”后缀的勒索软件现身，那时尚不起眼，但其核心团队迅

速展现出了区别于传统攻击者的商业野心。他们并未选择单打独斗，而是确立了极其成熟的“勒索软件即服务”（RaaS）商业模式：核心管理层专注于恶意软件代码的迭代（开发构建器）和洗钱通道的维护，而将具体的入侵、渗透和部署工作外包给被称为“附属成员”（Affiliates）的加盟攻击者。这种 20/80 的利润分成模式（核心层拿 20%，打手拿 80%）极大地激励了全球攻击者为其效力。

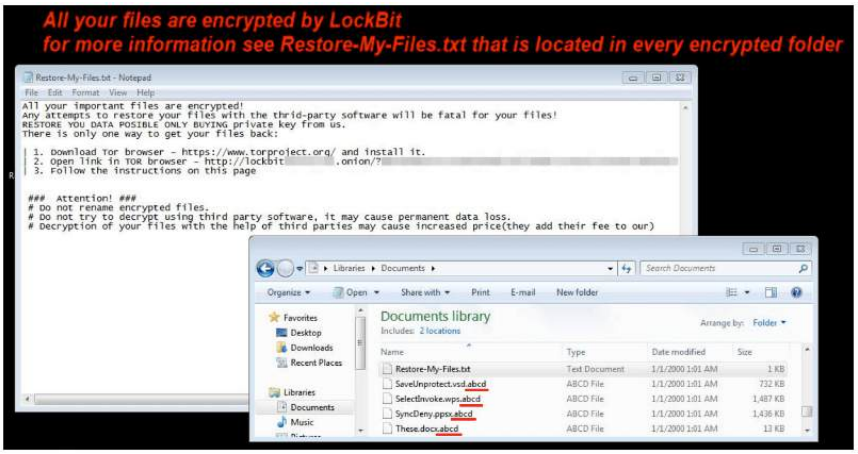


图 55:LockBit 勒索家族加密器

到了 2021 年至 2022 年，随着 LockBit 2.0 (Red) 和 3.0 (Black) 的发布，该组织达到了巅峰。他们不仅在技术上引入了“StealBit”工具以实现自动化数据窃取，更在运营上模拟了合法科技巨头：他们设立了“漏洞赏金计划”，悬赏邀请研究人员找自己代码的 Bug，以此彰显技术自信；他们甚至建立了分层级的“客户服务”体系，试图给受害者一种“只要付钱就一定能恢复数据”的虚假诚信感。情报画像显示，该组织的最高领导者“LockBitSupp”具有极强的双重人格特征——一方面表现出极度的傲慢、独裁和对技术的病态控制欲（被称为“BOSS”），另一方面又有一个相对温和的分身负责在 Tox 平台上处理日常沟通。然而，这种看似坚不可摧的帝国实则虚有其表，其内部早已因为后台带宽不足导致无法真实发布被盗数据，以及对附属成员收取高额入场费（价值约 777 美元比特币）而积怨已久。

版本名称	推出年份	主要特点/变化
初始版本	2019	加密文件后添加“.abcd”扩展名
Lockbit 2.0	2021	引入“StealBit”恶意软件，自动化窃取数据过程；速度快，加密效率高；针对 Linux 主机，特别是 VMware ESXi 服务器，发布了 Linux-ESXi Locker 1.0 版本。
Lockbit 3.0	2022	在经过两个月的 beta 测试后于 6 月下旬发布；主要特点包括漏洞赏金计划。

版本名称	推出年份	主要特点/变化
Lockbit-NG-Dev	2024	当执法部门在 2024 年 2 月打击 Lockbit 服务器时，发现该版本正处于高级开发阶段；使用.NET 框架编写，与早期使用的 C 和 C++编程语言不同；Lockbit 在 2024 年 12 月宣布了 4.0 版本，计划于 2025 年 2 月发布。
SuperBlack	2025	2025 年 3 月，网络安全研究人员报告了一种名为 SuperBlack 的新勒索软件，该软件以 Lockbit 3.0（也称 Lockbit Black）为基础；该变种删除了 Lockbit 品牌标识，更改了赎金票据，并添加了自定义数据泄露模块。也被称为 LockBit 4.0。

表 17:LockBit 勒索家族版本演变

2.2 技术军火库：从 C++ 到 .NET 的疯狂迭代与漏洞武器化

LockBit 之所以能长期霸榜，关键在于其技术栈的敏捷迭代与无孔不入的攻击战术。在软件形态上，他们经历了彻底的蜕变：早期的加密器基于 C/C++ 编写，追求极致的加密速度；而到了 2025 年发布的 LockBit 4.0（亦称 SuperBlack），核心团队为了对抗安全厂商的特征检测，将代码库全面转向 .NET 框架，并引入了复杂的代码混淆和反沙箱机制。为了适应企业级环境，他们特别针对 VMware ESXi 虚拟化平台开发了 Linux 版本的加密器（LockBit Linux-ESXi Locker），这意味着他们能通过一条指令瘫痪企业最核心的服务器集群。

在攻击链条（Kill Chain）上，LockBit 展现了“全漏洞利用”的特征。情报显示，从 2024 年底到 2025 年初，他们的附属成员密集利用了 Fortinet 防火墙的认证绕过漏洞（CVE-2024-55591、CVE-2025-24472）作为初始突破口，同时结合 Windows Confluence 的提权漏洞（CVE-2023-22527）深入内网。一旦进入系统，他们便熟练运用“就地取材”（LOLBAS）策略，滥用 PowerShell、PsExec 等合法工具，配合 Cobalt Strike 和 Mimikatz 进行横向移动和凭证窃取。为了确保持久化，他们会通过修改注册表禁用 Windows Defender，利用“自带易受攻击驱动程序”（BYOVD）技术强行杀灭 EDR 进程，并在系统中留下 `/tmp/lockbit.log` 等进度文件。这种高度工业化、自动化的攻击流程，使得即便是技术平庸的附属成员，也能借助 LockBit 的工具造成毁灭性破坏。

2.3 崩塌前夜：Cronos 行动与领导者“脱面具”

2024 年 2 月的“Cronos 行动”是 LockBit 命运的转折点，但这并非简单的服务器查封，而是一场精心策划的心理战。英国 NCA、美国 FBI 等多国执法机构不仅接

管了 LockBit 的暗网泄露站点，还将原本用来恐吓受害者的倒计时页面改造成了揭露 LockBit 成员信息的倒计时。执法机构向登录后台的攻击者弹窗展示其真实的 IP 地址和聊天记录，这种“反向恐吓”瞬间击碎了 RaaS 模式赖以生存的匿名信任基石。

图 56:LockBit 勒索家族暗网泄露站点

更为致命的一击来自对首脑身份的彻底剥离。2024 年 5 月，美国司法部正式确认那个在暗网呼风唤雨的“LockBitSupp”真实身份为 31 岁的俄罗斯沃罗涅日居民 Dmitry Khoroshev。情报细节甚至精确到了他居住的公寓楼层、驾驶的豪车以及他用来伪装合法收入的服装电商公司（Tkaner LLC）。调查发现，这位所谓的“攻击者教父”曾因未开启 VPN 登录服务器而暴露了真实家宽 IP（80.xx.xx.194）。这一身份的曝光让整个网络犯罪圈意识到，LockBit 的核心不仅不再安全，甚至可能已经成为执法部门监控下的“透明人”，这导致大量资深附属成员开始恐慌性撤离。

2.4 终局：2025 年数据泄露与“僵尸化”运营的真相

如果说 Cronos 行动是外伤，那么 2025 年 5 月发生的内部数据库泄漏则是致死的内伤。攻击者利用 PHP 远程代码执行漏洞（CVE-2024-4577）——讽刺的是，这正是 LockBit 惯用的攻击手段——攻破了 LockBit 重建后的基础设施。这次泄露的数据量之大、敏感度之高前所未有：包含了近 62,400 个比特币钱包地址、75 名核心成员的用户名及明文密码，以及超过 4,400 条详细的勒索谈判记录。

这些泄露的聊天记录揭开了 LockBit 衰败的遮羞布。记录显示，在针对俄罗斯切巴库尔市政府以及中国受害者的攻击案例中，LockBit 提供的解密器根本无法正常工作。面对受害者（甚至中间人）支付赎金后依然无法恢复数据的质问，LockBit 的运营人员因技术故障无法解决，只能选择“装死”沉默。这种“收钱不办事”的信誉破产，加上附属成员担心自己的身份随明文密码一同暴露，导致 LockBit 的生态系统在 2025 年彻底崩盘。如今的 LockBit 虽然名义上发布了 4.0 版本，但实际上已沦为一个充斥着低端攻击者、管理混乱、工具失效的“僵尸组织”，其品牌影响力已被 RansomHub 等新兴对手迅速瓜分。

3.深度威胁情报分析：Weaxor 勒索软件（Mallox 家族变种）

3.1 执行摘要

Weaxor 被确认为老牌勒索软件 **Mallox (TargetCompany)** 的最新品牌重塑版本。虽然它继承了 Mallox 针对 **Microsoft SQL Server (MSSQL)** 的攻击传统，但在战术上进行了重大升级。 最核心的变化在于：

1. **引入新型漏洞**：除了传统的暴力破解，开始利用 **React2Shell (CVE-2025-55182)** 漏洞获取初始访问权。
2. **独特的投递机制**：使用 **Cobalt Strike Beacon** 作为中间载荷，并利用 `sqlps.exe`（SQL Server 自带的 PowerShell 工具）替代传统的 `powershell.exe` 执行恶意脚本，极大地提高了其在受管环境中的规避能力。

3.2 源码分析

相似之处

1. 都不加密固定的五种语言地区——俄语、哈萨克语、白俄罗斯语、乌克兰语和土库曼语；
2. 都调整电源计划为高性能模式；
3. 删除的注册表内容一致；
4. 密钥生成和加密算法基本一致，但是 rox 在生成随机数的基础上又生成了 0x38 个字节的随机数，修复了 mallox 会被破解出密钥的情况；

```
61  hAlgorithm = 0;
62  if ( sub_7FF7C712D150() && (unsigned __int8)BCryptGenRandom_0(&hAlgorithm, pbBuffer, 0x38u, v7) )
63  {
```

图 57:算法相同点

5. 信息回传的格式，以及 url 极其相似，mallox url 如下：

```
SQL
http://193.106.xxx.xxx/QWEwqdsvsf/ap.php
```

weaxor url 如下：

```
SQL
http://193.143.xxx.xxx/Ujdu8jjooue/biweax.php
```

不同之处

1. weaxor 未对关机键进行隐藏；

2. 获取文件方式不同，mallox 获取文件方式为遍历文件，然后通过完成端口将文件提交到队列中，加密线程通过队列获取文件，而 weaxor 则是通过一个全局列表来传输；
3. Weaxor 开启了较高的编译优化，而 Mallox 则没有。

3.3 详细技术分析

3.3.1 身份与演变

- **家族谱系**：Weaxor 是 Mallox 家族的直系后代。Mallox 自 2021 年活跃以来，曾多次更名（Fargo, Tohnichi, Xollam），Weaxor 是其应对近期执法压力与安全检测的最新“马甲”。
- **重塑目的**：通过更改品牌名和文件后缀（主要观测到 `.rox`，部分情报提及 `.weax`），试图绕过基于旧 Mallox 特征（如扩展名 `.mallox`）的静态防御规则。

3.3.2 攻击链分析

初始访问 (Initial Access)

- **传统路径**：针对公网暴露的 MSSQL (TCP 1433) 进行暴力破解。
- **新增路径 （关键升级）**：利用 **React2Shell (CVE-2025-55182)** 漏洞。这是一个存在于某些 Web 应用框架中的严重远程代码执行漏洞，攻击者可借此直接在服务器上执行命令。

载荷投递与执行 (Payload Delivery)

Seqrite 白皮书特别指出了其投递方式的**多阶段 (Multi-stage)** 特征：

1. **第一阶段**：通过入侵点投放高度混淆的批处理文件（`.bat`）。
2. **第二阶段**：批处理文件解密并执行 PowerShell 脚本。

➢ **规避点**：攻击者调用 `sqlps.exe` 来运行 PowerShell 命令。由于 `sqlps.exe` 是微软官方签名的合法二进制文件（LoLBin），且通常被安全软件视为可信进程，这能有效绕过部分 EDR 的监控。

3. **第三阶段：**注入 Cobalt Strike Beacon Shellcode 到内存中。
4. **最终阶段：**Beacon 连接 C2 服务器（如报告中提及的 193.143.1.139），下载并执行最终的 Weaxor 勒索软件主程序。

防御规避 (Defense Evasion)

- **AMSI Bypass**：脚本中包含特定的代码片段，用于修补内存中的 `AmsiScanBuffer` 函数，从而禁用 Windows 的反恶意软件扫描接口 (AMSI)。

- **内存执行**：主要攻击逻辑在内存中完成，减少磁盘落地文件。
- **服务破坏**：Weaxor 会修改注册表以禁用系统的“关机”“重启”和“注销”选项，防止管理员在发现异常时通过重启中断加密过程。

4.Phobos 与 8Base 勒索软件组织的生态演变与覆灭

4.1 核心结论：8Base 与 Phobos 的真实关系

长期以来，安全业界怀疑 8Base 是 Phobos 的“换皮”版本。此次联合执法行动及司法文件最终**实锤**了这一点：

- **从属关系确认**：8Base 并非独立的 RaaS 开发商，而是一个使用 Phobos 勒索软件极其活跃的**附属组织（Affiliate Group）**。
- **代号“Affiliate 2803”**：司法文件披露，8Base 及其背后的运营者在 Phobos RaaS 生态系统中的内部代号为 **"Affiliate 2803"**。
- **同源性**：HHS 技术报告指出，8Base 部署的勒索软件载荷本质上是 **Phobos v2.9.1** 版本，未进行核心代码修改，仅在勒索信和后缀上进行了品牌定制（如 `.8base`）。

4.2 组织发展历程与生态架构

4.2.1 Phobos：RaaS 平台提供商

- **起源（2019）**：Phobos 诞生于 Dharma/CrySis 勒索软件家族，主要通过 RaaS 模式运营。
- **市场定位**：与专注于大型企业猎杀（Big Game Hunting）的组织不同，Phobos 专注于**中小型企业（SMB）**、医疗和教育机构，采取“薄利多销”策略。
- **管理员角色**：核心管理员（如已引渡的 **Evgenii Ptitsyn**）负责开发恶意软件、维护解密密钥生成服务及暗网支付平台，并向附属组织抽取分成。

4.2.2 8Base：激进的顶级附属团队

- **爆发期（2023）**：8Base 虽然最早可追溯至 2022 年，但在 2023 年 5-6 月突然爆发，迅速跻身全球活跃度前列。
- **运营策略**：
  - **品牌化**：8Base 建立了独立的数据泄露网站（Leak Site），拥有鲜明的品牌标识，试图在受害者心中建立“独立大组织”的形象。
  - **话术伪装**：他们在勒索信中自称“诚实的渗透测试者”，声称攻击是为了帮助企业发现漏洞（典型的鳄鱼眼泪）。

- **高频攻击**：利用 Phobos 提供的基础设施，8Base 进行了极高频次的攻击，主要针对商业服务、制造和金融行业。

4.3 近期执法行动与打击成果 (2024-2025)

此次代号为 **"Operation Phobos Aetor"** 的国际联合行动是对该网络的毁灭性打击。

图 58:Operation Phobos Aetor 参与部门

4.3.1 核心人员落网

- **8Base 领导层（在泰国被捕）**：
  - **Roman Berezhnoy (33 岁）**和 **Egor Nikolaevich Glebov (39 岁）**：两名俄罗斯公民在泰国普吉岛被捕。
  - **指控**：DOJ 指控这两人正是 **8Base ("Affiliate 2803") 的实际运营者**。他们利用 Phobos 软件勒索了全球超过 1000 个实体，获利超 1600 万美元。
- **Phobos 管理员（在韩国被捕）：**
  - **Evgenii Ptitsyn (42 岁）**：Phobos RaaS 平台的核心管理员于 2024 年 6 月在韩国被捕，并于 11 月引渡至美国。他的落网可能为追踪 8Base 提供了关键情报。

4.3.2 基础设施摧毁

- **服务器查封**：位于全球多地的 **27 台关键服务器**被查封。
- **网站接管**：8Base 的暗网数据泄露网站已被德国巴伐利亚州刑事警察局（LKA）接管，并挂上了执法机关的宣告页面。

- **密钥获取**：Europol 透露已掌握部分解密密钥，并正在帮助受害者恢复数据。

4.4 技术战术分析（TTPs）

结合 HHS 的分析报告，8Base (Affiliate 2803) 在使用 Phobos 时的战术特征如下：

4.4.1 初始访问（Initial Access）

- **SmokeLoader**：这是 8Base 区别于其他 Phobos 附属组织的显著特征，他们高频使用 SmokeLoader 作为初始加载器来投放勒索软件。
- **RDP 暴力破解**：延续了 Phobos/Dharma 的传统，利用弱口令扫描开放的 3389 端口。
- **钓鱼邮件**：伪装成发票或业务文件诱导点击。

4.4.2 执行与持久化

- **系统破坏**：执行标准指令删除卷影副本（`vssadmin`）、禁用恢复模式（`bcdedit`）。
- **持久化**：将恶意软件复制到 `%APPDATA%` 或启动文件夹，并修改注册表 `Run` 键值。

4.4.3 沟通与勒索

- **通信渠道**：不提供自动化的解密门户，强制要求受害者通过 **qTox** 或 **Email** (如 `onionmail.org`) 进行人工谈判。
- **双重勒索**：在加密前窃取数据，并威胁在泄露网站上公开（现该网站已被查封）。

4.5 综合研判与影响

此次行动是打击 RaaS 生态的一个经典案例，它不仅打掉了平台方（Phobos Admin），更精准清除了最活跃的使用方（8Base Leaders）。

- **短期影响**：随着 Berezhnoy 和 Glebov 的被捕及基础设施瘫痪，**8Base 品牌的活动将立即停止**。全球针对中小企业的勒索攻击量级预计在短期内会有所下降。
- **长期启示**：
  - **RDP 仍是软肋**：8Base 的成功再次证明，简单的 RDP 弱口令防护依然是全球中小企业的最大短板。
  - **附属组织的品牌化**：8Base 证明了附属团队可以建立比 RaaS 平台本身更响亮的品牌。未来的打击行动将更加关注这些“超级附属团队”（Power Affiliates）。
  - **国际合作的威力**：跨越美、欧、亚（韩、泰）的联合执法表明，网络犯罪分子的

避风港正在减少。

5.一场注定崩盘的“黑吃黑”与地下亿元赎金帝国

案件的转折点并非病毒暴发，而是一场业余的救援。客户在事发后病急乱投医，委托了某数据恢复中介公司。我们通过梳理 **9 月 16 日至 9 月 25 日**的邮件往来，还原了这场被搞砸的谈判全过程。

5.1 黑客的心理博弈：并非普通的勒索者

正规 LockBit 家族严格依赖 Tor 网络（暗网）面板进行私密谈判，绝不会使用普通邮箱。而本案的中介公司因不熟悉 LockBit 家族历史情况，**试图通过邮件讨价还价**。更值得注意的是黑客在沟通中暴露出的细节：

时间点：2025 年 9 月 16 日 17:34 黑客首次向受害者发送勒索邮件。值得注意的是，**邮件正文使用的是中文**，且附件中包含了一个受害企业中 IT 主管“**X 先生**”的个人专业技能证书。

图 59：黑客发送的中文威胁邮件，并附高管技能证书

Solar 团队分析：

1. **熟悉环境：** 附带正常文件说明黑客已在内网潜伏多时，对客户环境了如指掌，这是为后续索要高额赎金做心理铺垫。
2. **国人嫌疑：** 熟练使用中文沟通，结合后续溯源到的向日葵工具使用习惯，极有可能是**境内的黑客团伙**披着 LockBit 的外衣在作案。
3. **匿名邮箱：**我们尝试使用追踪邮件客户端 IP，并没有发现 `x-originating-ip` 相关字段，因为 cock.li 是一个注重隐私的邮件服务商，它在邮件头中**隐藏了原始发件人的真实 IP 地址**（没有 X-Originating-IP 这样的字段）。

图 60:邮件头无 x-originating-ip 字段

在我们今年接触了几百起勒索案例后总结：目前勒索家族逐渐呈现出 **APT 趋势**，不仅加密文件，还会**长期潜伏及窃取数据**。具备三大特性：**高持续性、高隐秘性、高威胁性**

5.2 谈判崩盘：黑客“两头吃”的贪婪行为

时间点：2025 年 9 月 20 日 - 9 月 25 日 中介公司（G 公司）介入后，声称已经支付了赎金，要求黑客解密。黑客的回复揭开了其“两头吃”的贪婪想法。

图 61:中介声称“钱已付，未收到解密器”，黑客表示“已发送解密器”，双方陷入僵持

5.3 中介的业余操作与客户的恐慌

时间点：2025 年 9 月 22 日 09:12 受害者因急于恢复业务，告知黑客“**已委托第三方公司联系**”。这种表述直接暴露了客户“**病急乱投医**”的心理，让黑客意识到这是一只待宰的肥羊。

直到 9 月 25 日，黑客发出了最后通牒，戳穿了中介的老底：**“我发现了你和代理公司的合同。那个代理公司之前坑过我们，害我们损失了好几个客户。”**

图 62:黑客因中介的历史欺诈行为（收了客户钱但不给黑客，或少给黑客）及黑客“两头吃”意图而拒绝交付密钥

行为动机剖析： 黑客之所以表现出不讲信用，本质上是在**黑吃黑**。通过索要合同，黑客摸清了客户的预算底线；通过拒绝中介，黑客试图绕过中介直接对客户进行二次勒索。 这再次印证了我们的观点：**向黑客支付赎金是极高风险的行为，尤其是面对这种毫无信誉的散户时，往往是肉包子打狗。**

我们团队同样有着相似案例的处置经验，详情可见：

https://mp.weixin.qq.com/s/VS5RefkuLwmCxla7-6D7kw

5.4 资金链路追踪：触目惊心的地下金流

既然中介声称“**已付款**”，钱到底去哪了？Solar 团队利用 **MistTrack（慢雾）** `dashboard.misttrack.io` 等链上追踪平台，对涉案的比特币地址进行了深度穿透分析，结果令人咋舌。

5.4.1 锁定交易链路

根据受害者描述，当时付款给中介公司 **30 万元人民币**，而后我们通过链上追踪中介公司的转账记录，他们在 9 月 20 日向黑客地址转账了约 **0.1315BTC(10 万元人民币含手续费、资金波动等)**。我们锁定了两个关键地址：

中介控制的钱包地址： bc1qy28sl3sndu7vww4vhamh04ce28mxxxxxx

黑客接收地址： 3JP5D4XyzQcZB43QdegCzKGvoawxxxxx

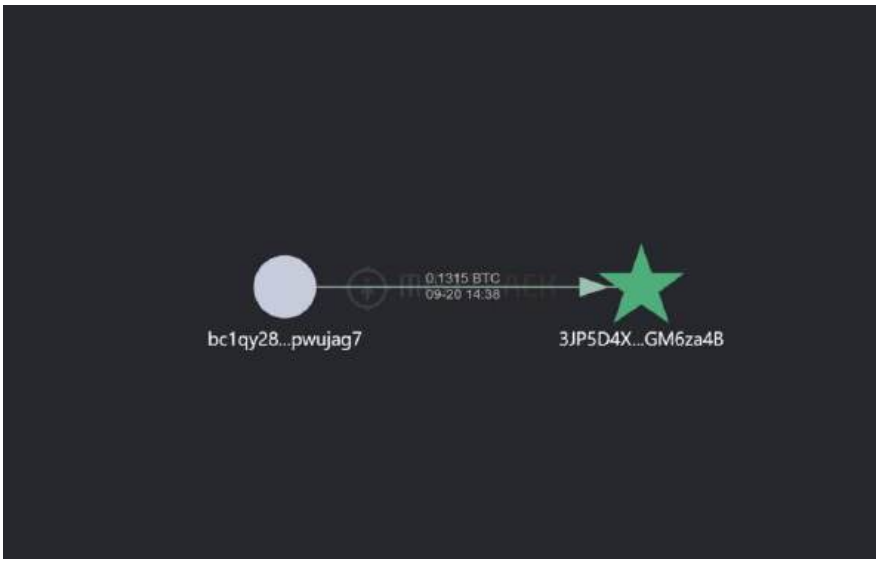


图 63:MistTrack 平台显示的资金流向图，确证了资金从中间人流向黑客地址

截至目前黑客钱包内的 BTC 仍然没有转出记录，推测等待风声过后转出，我们也在持续进行链上监控。

5.4.2 惊人的交易规模

通过对中介钱包地址的逆向溯源，我们发现这并非个例。该地址在短短一年内（截至 2025 年 12 月），资金流水异常频繁且巨大。

- **交易笔数：** 超过 700 笔
- **资金规模：** 累计转出 **84.4759 BTC（约 56096559 元人民币）**

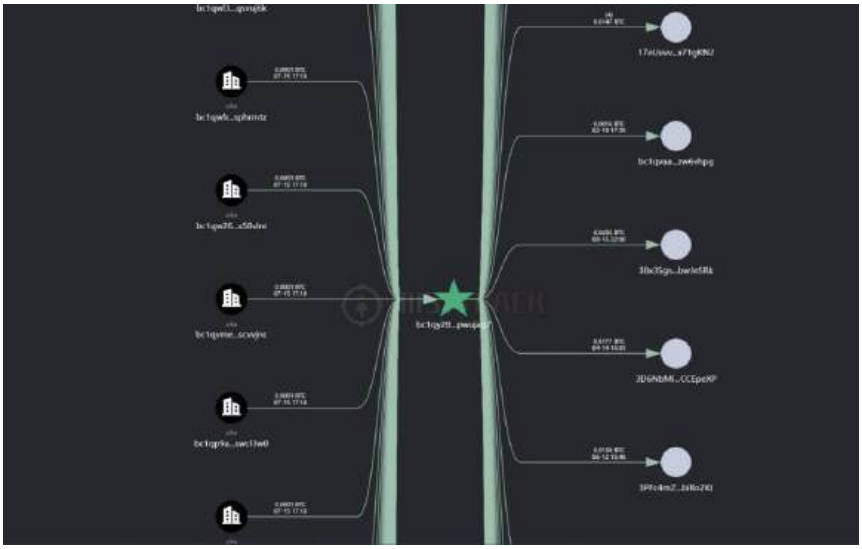


图 64:中介钱包对外转账链路追踪（部分数据）

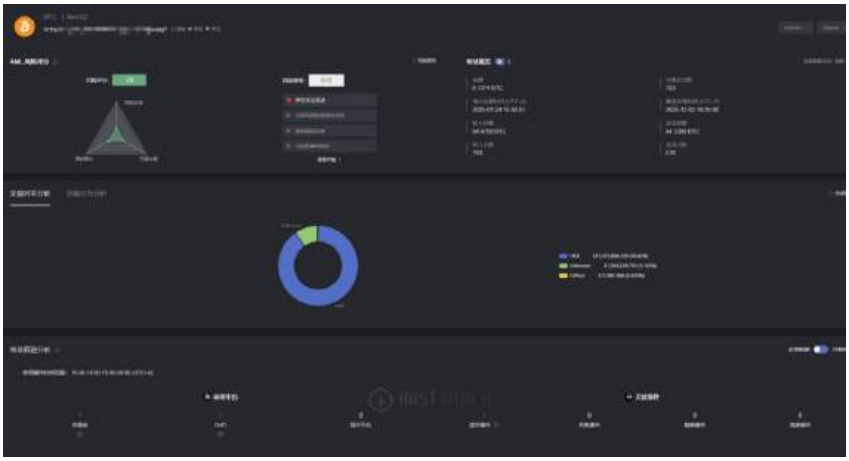


图 65:中介钱包地址的年度交易概览

图 66:按当前汇率计算，该地址经手的赎金总额高达 5600 万+ 人民币

数据背后的真相： 仅仅这一个中介的一个钱包地址，一年内就涉及了 700 多个受害客户，经手了**数千万**的赎金。按照客户描述**付 30 万元给中介公司**，**中介公司付赎金 10 万元**来计算（赎金*3），中介公司经手金额可达上亿元，这足以证明国内勒索软件攻击的泛滥程度，以及地下**“代付/恢复”**产业的畸形繁荣。大量企业在遭受攻击后选择忍气吞声交钱，助长了黑产的嚣张气焰。

而后中介公司在购买密钥无望后（中介公司倒亏 10 万元）选择直接跑路，留下一地鸡毛，客户难过又气愤，于是将整个过程还原以警示大众，下文来自客户的梳理

> 我们是一家国内的企业，最近企业服务器感染了勒索病毒，数据都被加密了，然后找到了一家公司名叫“XX 文化有限公司”的企业，然后他们宣传自己包解密，我们又去看了一下他们的官网很正规，24 小时服务等，然后我们就信任了他们的技术，让他们帮我们恢复数据，并支付了 30 万元的费用。我们最后发现他们是支付比特币赎金给黑客团伙购买解密工具帮我们解密，他们根本没有这样的技术去恢复数据，他们只是在中间赚取大额的赎金差价，他们这样的业务行为是纵容犯罪分子更容易得到金钱，也成了黑客团伙犯罪分子的收取企业钱财的助手，而且国家明令禁止比特币交易，国家现在严令禁止炒作虚拟币，为什么会有比特币业务？如果他们没有支付比特币，他们是支付什么给黑客？他们是不是跟黑客团伙有利益来往输送，黑客团伙负责加密，他们负责收企业的客户钱，他们还打着网络安全溯源的旗号帮客户溯源，实质上就是帮助黑客勒索敲诈企业。

5.4.3 铁证如山：单一地址流出 90 BTC

根据受害者提供的线索，我们对中介控制的这个关键钱包地址进行了全量资金穿透。审计报告显示，该地址绝非临时账号，而是一个长期活跃的资金中转枢纽。

- **资金规模（Total Sent）：** 截至 2026 年 1 月，该地址累计**流出资金高达 90.6319 BTC**。
- **价值折算：** 按交易发生时的加权汇率估算，该中介仅通过这一个钱包支付给上游黑客的资金成本就高达 **800 万美元（约合人民币 5,800 万元）**。
- **交易频次：** 链上记录显示，该地址在过去一年内从早到晚保持着高频交互，每一笔流出的比特币背后，可能都对应着一家陷入绝望的企业。

5.4.4 暴利模型推演：从 5800 万到 1.7 个亿

如果我们套用本案中复盘的 **“300% 暴利模型”**（即：中介向客户收 30 万，实付黑客 10 万，溢价率 300%），这组链上数据背后的真相让人不寒而栗：

项目	数据来源/计算逻辑	金额 （估算）
中介支付成本	链上实证 （流出 90.63 BTC）	¥ 58,000,000
中介收取金额	基于本案 3 倍 溢价倒推	¥ 174,000,000
净利润 （黑产）	收取金额 - 支付成本	¥ 116,000,000

Solar 深度点评：

规模推演： 仅仅这一个中介公司的一个钱包地址，在短短一年多的时间里，就经手了疑似近 1.7 亿元人民币的涉案资金。按照平均每家企业支付 10-30 万赎金计

算，该地址背后涉及的国内受害企业可能多达 500-1000 家。 吸血鬼式的繁荣： 中介公司在没有任何核心解密技术的情况下，利用受害者的恐慌和信息不对称，仅靠“倒卖”黑客的解密器，就从中国企业身上吸走了 1.16 亿元 的净利润。这种“两头吃”的贪婪，正是导致本案中黑客撕票、谈判崩盘的根本原因。 资敌实锤： 最令人担忧的是，这 5,800 万元 的比特币最终通过中介之手，源源不断地流入了境外黑客团伙的口袋。这些资金成为黑客组织招募开发者、购买 0day 漏洞、升级勒索病毒的“军费”，进而对国内企业发动更猛烈的攻击。

表 18:产业暴利核算

5.5 样本定性：李逵还是李鬼

在确认谈判无望、资金被骗后，我们回归技术本源。受害者通过我司官网：`http://应急响应.com`联系到我们，了解事情经过后，**Solar 应急响应团队**线下溯源处置及对被勒索机器提取到的样本`svchost.exe`进行了逆向分析。

通过对恶意代码的静态与动态分析，我们确认该样本实际上是利用 **LockBit 3.0 泄露构建器**生成的盗版变种。攻击者将其伪装成 LockBit 5.0 以制造恐慌，但其技术细节暴露了其真实身份。

（二）攻击者基础设施与活动特征

1. 核心基础设施 （隐匿根基）

1.1 TOR （洋葱路由）【暗网基础设施】

勒索软件生态的基石。通过全球成千上万的中继节点进行多层跳板路由，隐藏攻击者的真实 IP 和物理位置。它是承载**暗网泄露站点 (Leak Site)** 和 **赎金支付页面** 的唯一平台，使得执法机构难以通过流量分析追踪服务器或进行关停。

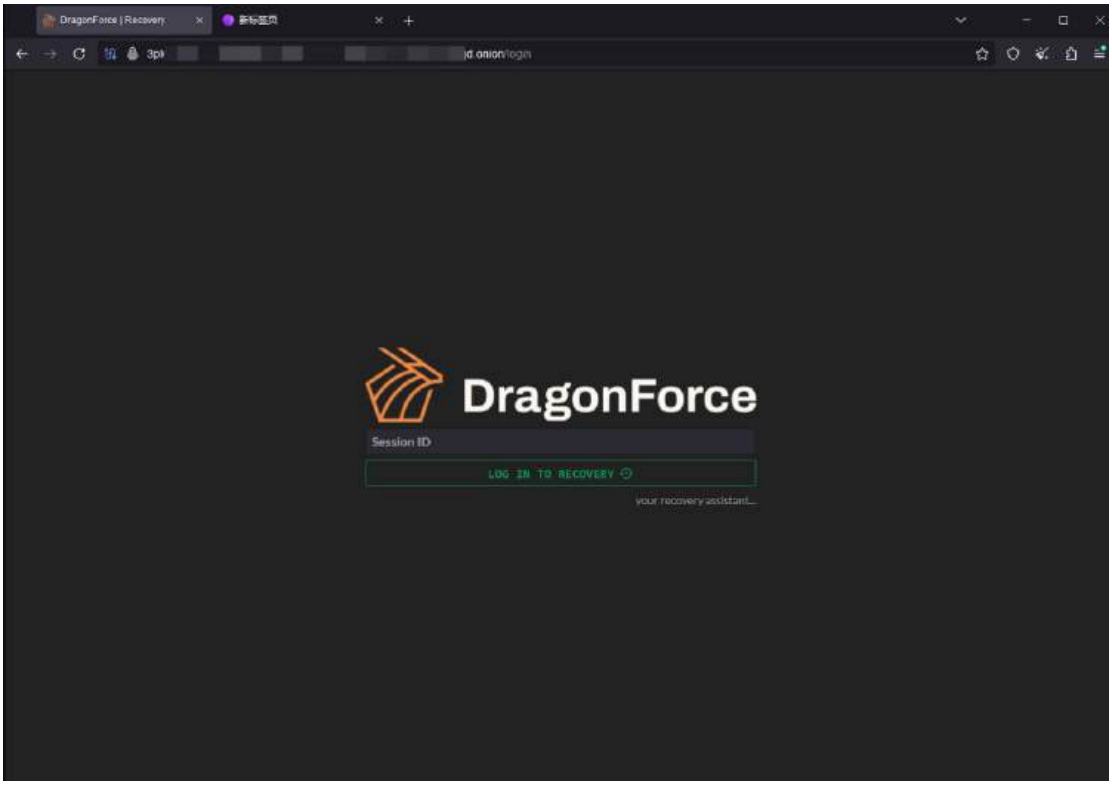


图 67:Tor 暗网泄露站点

2. 即时通讯工具 （实时谈判）

2.1 TOX

当前勒索谈判的**首选工具**。基于 P2P（点对点）架构，无中央服务器，所有聊天内容强制端到端加密。因没有运营实体，执法部门无法通过“发函”调取聊天记录或封禁账号，彻底解决了账号被封锁的风险。

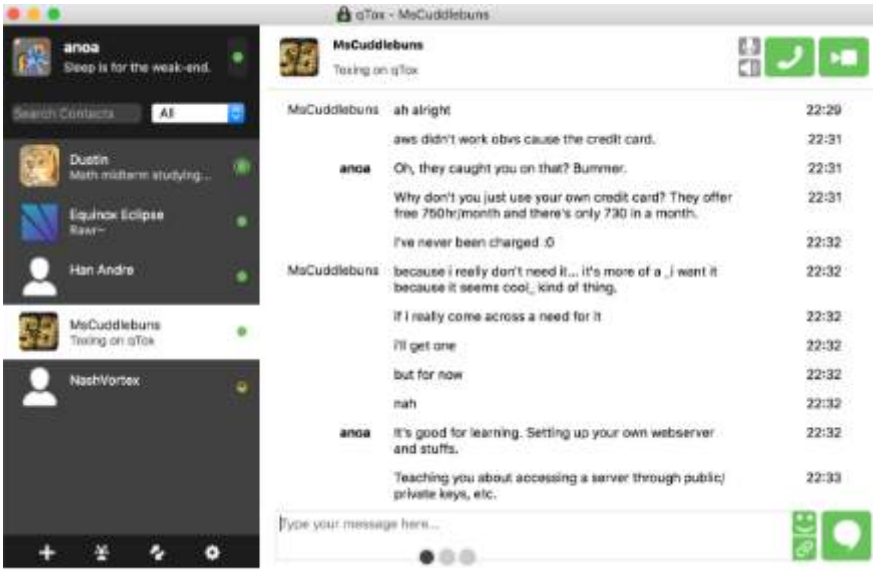


图 68:Tox 聊天框页面

2.2 Session

极高隐私的即时通讯软件。与 Signal 不同，它**不需要手机号或邮箱注册**（仅生成 Session ID），利用洋葱路由网络传输消息，不留存任何元数据（Metadata），让追踪者无法通过通信日志分析攻击者的社交关系网。

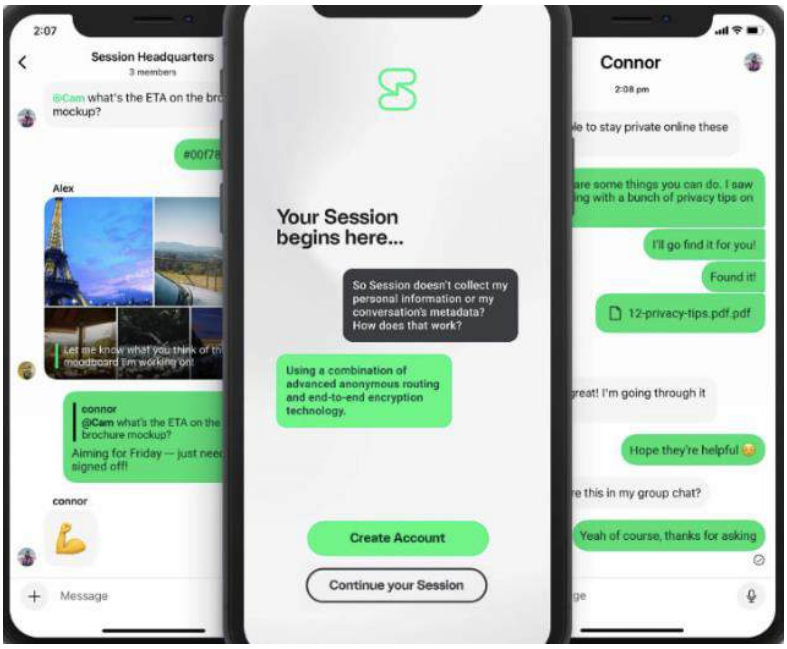


图 69:Session 聊天框页面

2.3 Telegram (TG)

兼具即时通讯与“黑市”属性。除了用于部分勒索谈判，攻击者组织更倾向于利用其“频道（Channel）”和 **“机器人（Bot）”** 功能，公开售卖窃取数据、发布受害者名单以及招募 RaaS 附属成员（下线）。

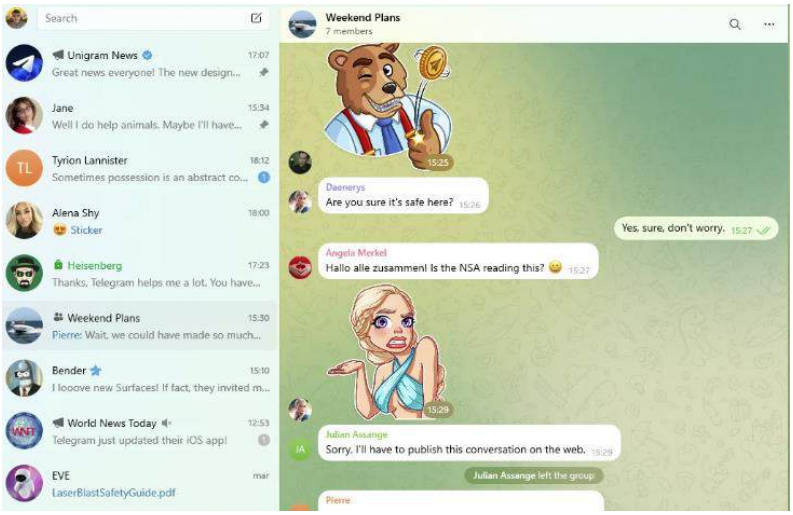


图 70:TG 聊天框页面

3. 专用加密邮箱 （匿名投递）

3.1Proton Mail

位于**瑞士**的加密邮箱巨头。受严格的瑞士隐私法保护，服务器采用零知识访问架构（连管理员都无法查看邮件内容）。因其注册无需手机号且信誉度较好，常被攻击者用于发送第一封勒索信或作为备用联络点。

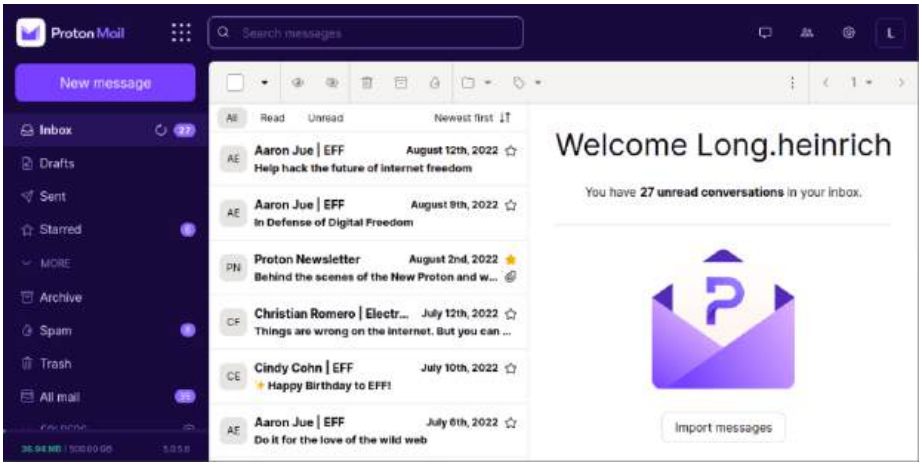


图 71:Proton Mail 邮箱页面

3.2 OnionMail

专为 TOR 网络设计的邮箱。无需个人信息即可创建，支持通过 **PGP 公钥** 自动加密邮件。其核心优势是能通过 VMAT 协议打破“暗网与明网”的壁垒，让攻击者在暗网环境中安全地接收受害者从普通互联网发来的邮件。

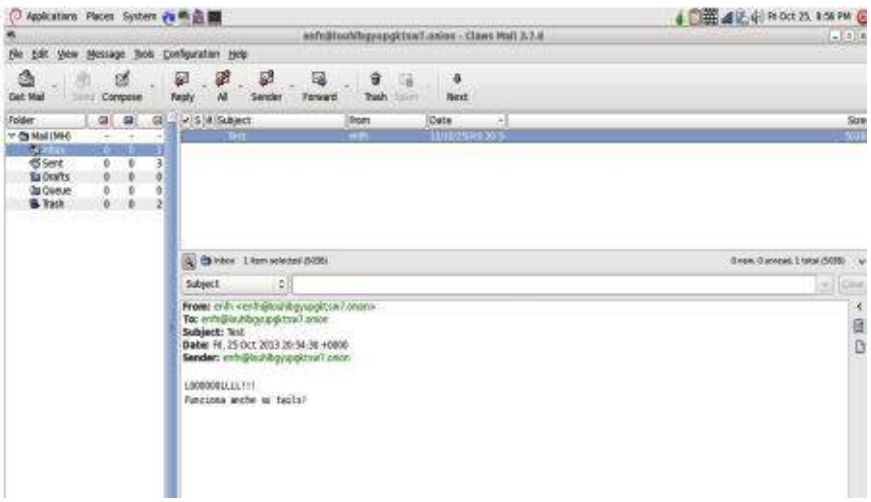


图 72: OnionMail 邮箱页面

3.3 Tuta (原 Tutanota)

位于**德国**的加密邮箱服务。与 Proton 类似，它对邮件的**主题行、正文及附件**均进行端到端加密。因提供免费且匿名的账户注册，常被勒索组织作为 Proton Mail 被封锁

后的第一备选方案（B 计划）。

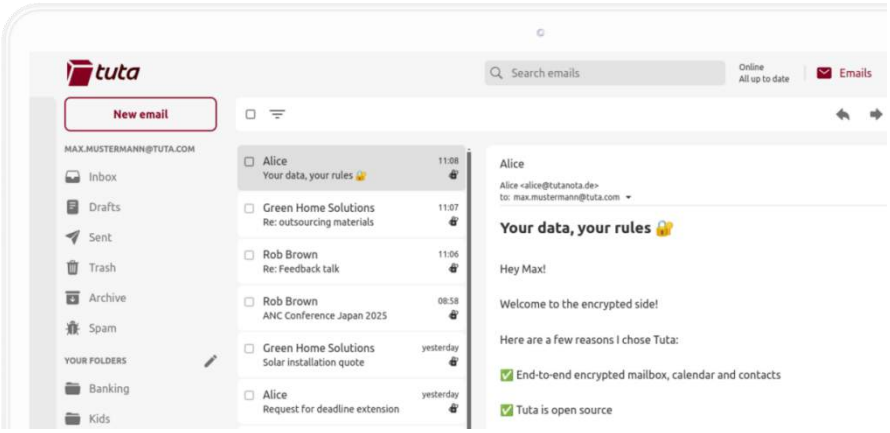


图 73: Tuta 邮箱页面

3.4 Cyberfear.com

专注于极致隐私的小众服务商。声称“零知识”架构，支持比特币支付订阅。深受特定高阶勒索家族（如 BlackCat 等）青睐，用于规避主流邮件服务商的风控封锁。

图 74: Cyberfear.com 邮箱页面

3.5 Cock.li

攻击者圈内“恶名昭著”的私人运营邮箱。允许随意注册，抗投诉能力极强（Bulletproof）。虽稳定性一般，但因运营者长期拒绝配合任何国家的执法调查，在早期和激进的勒索软件活动中极为常见。

图 75:　Cock.li 邮箱页面

3.6 Firemail.cc

常用于生成临时的、一次性的谈判地址。因其对滥用行为的高容忍度，攻击者常利用它发送大规模垃圾勒索邮件。

4. 主流公共邮箱 （伪装与渗透）

4.1 Gmail / Outlook / iCloud

虽然这几类邮箱本身配合执法调查，但攻击者依然使用。通常通过**盗取他人账号**或**虚假身份注册**。攻击者利用这些域名的高信誉度（High Reputation），确保勒索邮件能穿透企业的**反垃圾邮件网关（SEG）**，直接抵达受害者收件箱。

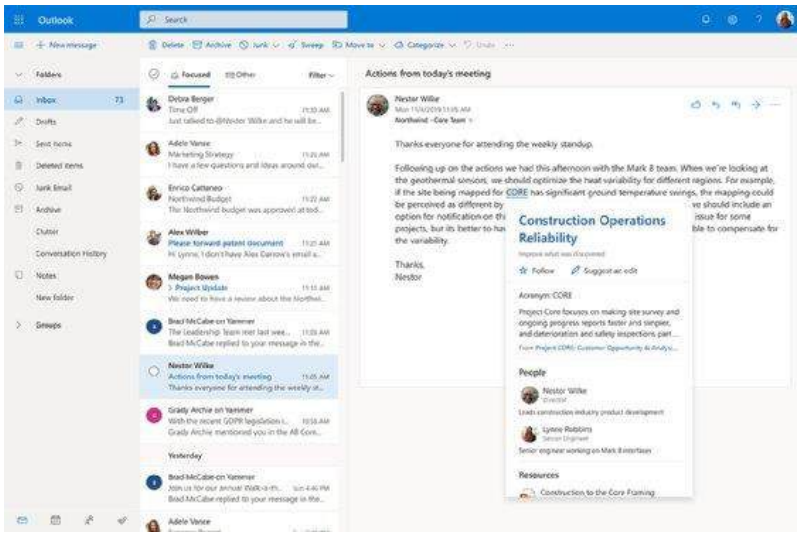


图 76:　常见邮箱页面

（三）勒索攻击手段与技术路径分析

1.口令破解攻击

1.1 RDP 弱口令

1.因集群上层连接地址为 10.0.xxx.xxx 网闸，集群收到的所有外网连接 IP 均为网闸 IP(10.0.xxx.xxx)访问。

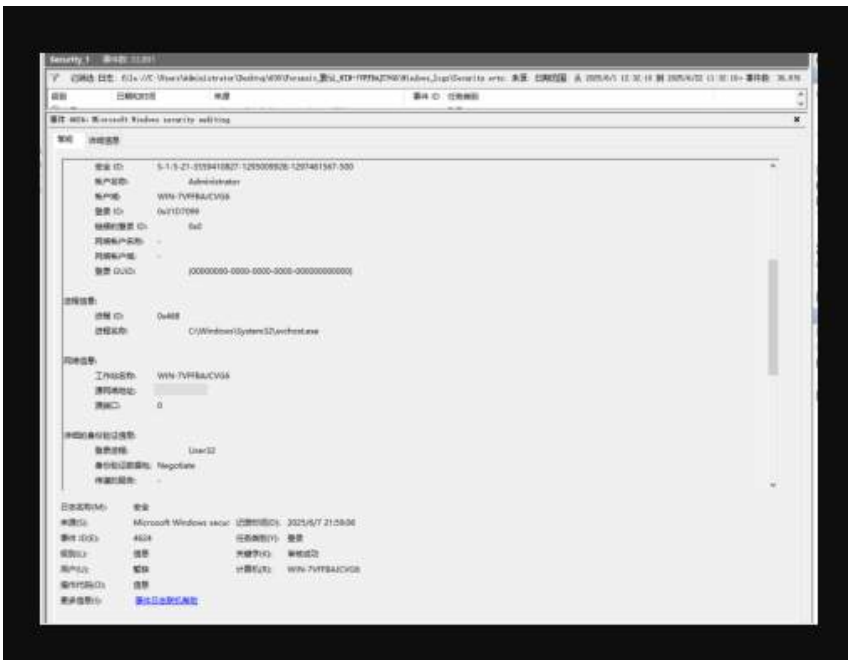


图 77 :攻击者通过外网映射网闸连接证明

2.因网闸(10.0.xxx.xxx)日志默认存储三天，攻击者攻击时间（2025 年 6 月 6 日至 2025 年 6 月 8 日日志未被保存）

图 78: 网闸日志记录证明

3.防火墙（10.0.xxx.xxx）未记录访问爆破操作，但记录少量攻击者使用工具对外进行爆破记录（“无法进一步溯源真实外网 IP”）

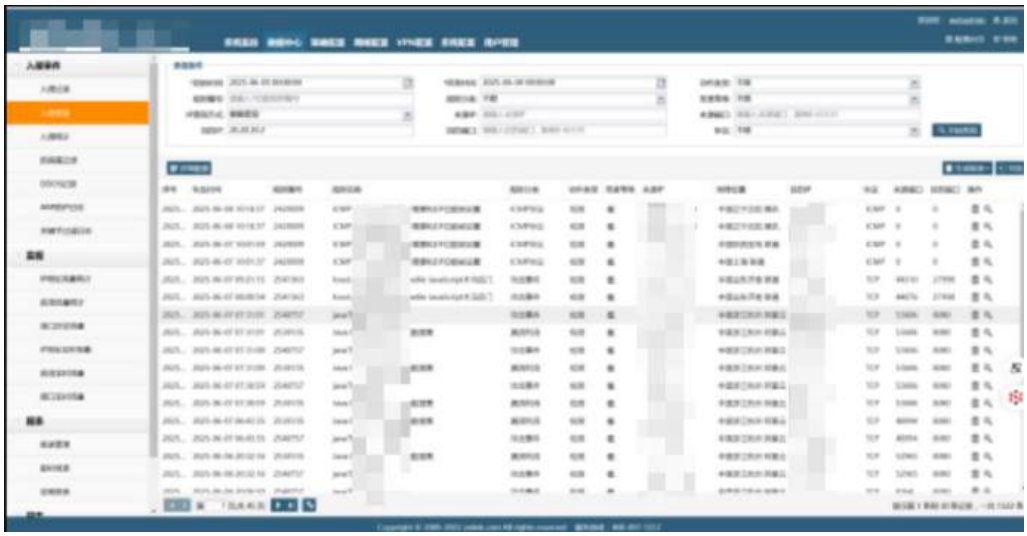


图 79：防火墙无爆破无 RDP 连接日志记录证明

攻击者第一次运行攻击者工具在 2025 年 6 月 7 日 15:02:08，攻击者首次登录在 2025 年 6 月 7 日 15:00 左右（因安全日志最大大小原因最初日志仅保留从 2025 年 6 月 7 日 16:49 之后的安全日志行为）

图 80：攻击者运行攻击者工具

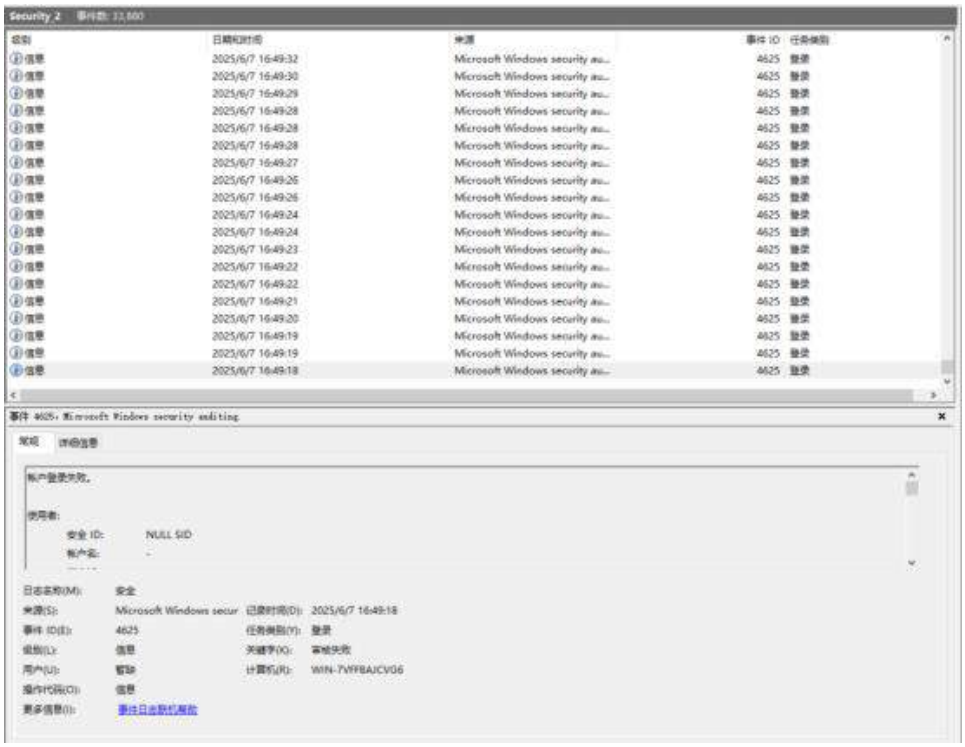


图 81: 攻击者爆破记录

2025 年 6 月 7 日 21:59:06 IP：10.0.xxx.xxx（因通过网闸进行映射，其攻防演练机所有访问 ip 均通过 10.0.xxx.xxx 对 172.16.xxx.xxx 进行访问） 远程 RDP 登录 172.16.xxx.xxx 成功

图 82:攻击者登录成功日志记录

登录成功后攻击者在“c:\users\administrator\music”文件位置上传攻击者工具用于信息收集以及横向移动爆破如“netscan.exe”（局域网扫描）、“kpor.exe”（端口扫描）“mimikatz.exe”（密码窃取）、“webbrowserpassview.exe”（密码窃取）等

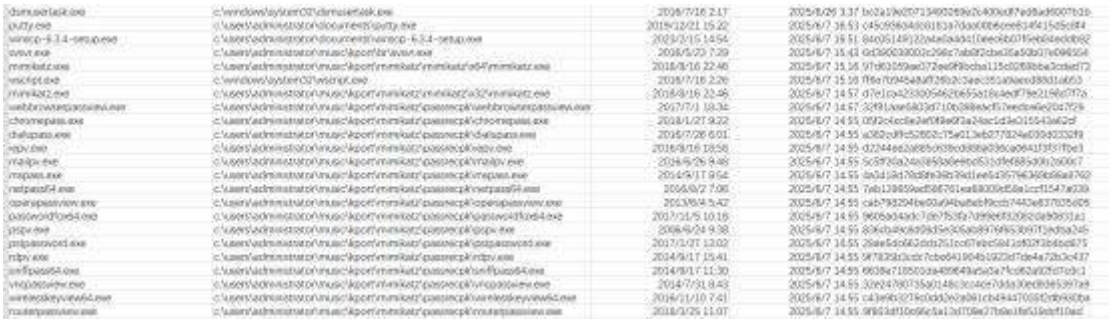


图 83: 攻击者上传运行攻击者工具记录

攻击者成功后在 2025 年 6 月 7 日 22:04:03 开始再次对扫描内网进行横向移动扫描。

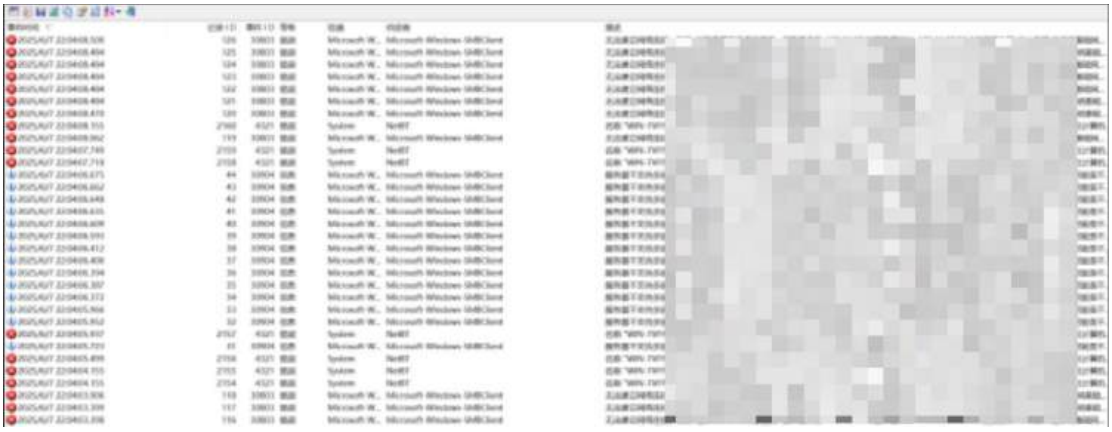


图 84: 攻击者横向扫描记录

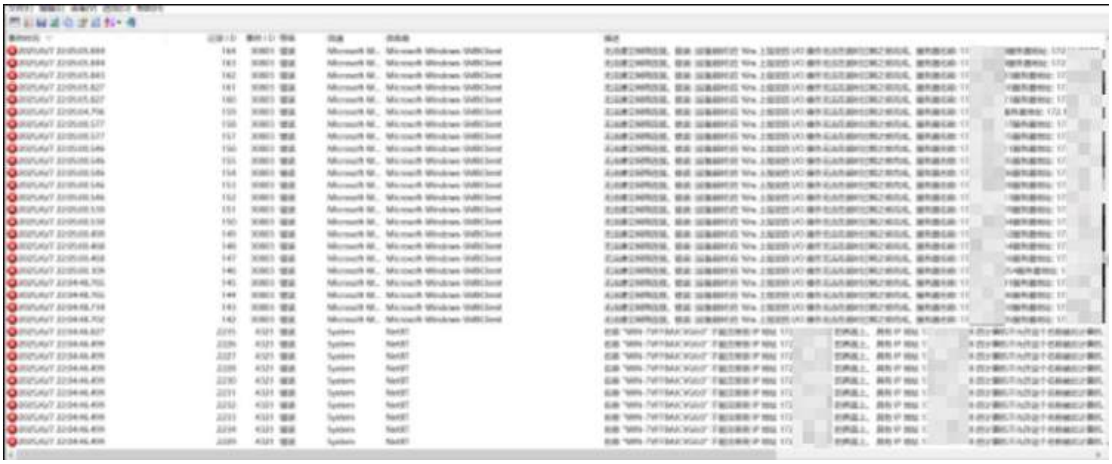


图 85:攻击者横向扫描记录

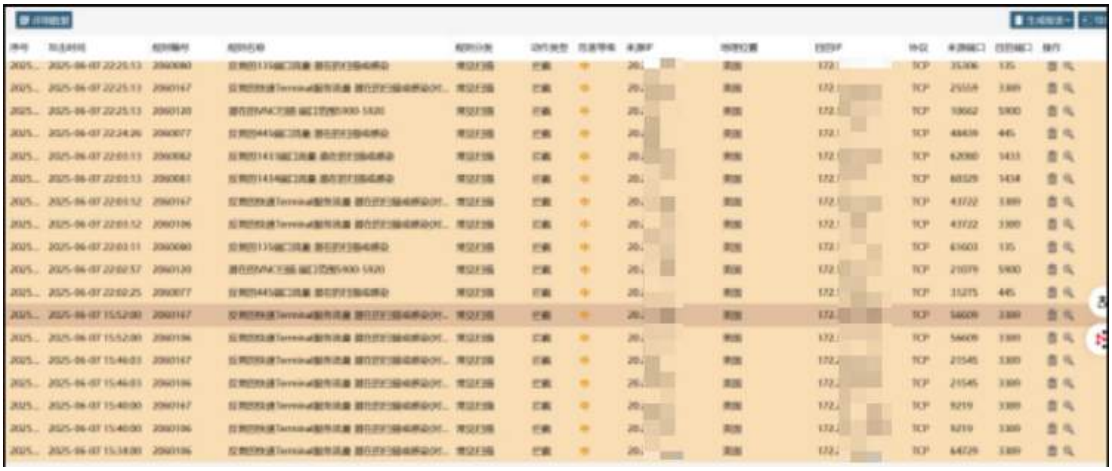


图 86: 攻击者对外扫描记录

攻击者 2025 年 6 月 7 日 23:16 启动 Winscp 对爆破成功服务器进行远程连接可从会话配置文件中看到攻击者连接了 172.16.xxx.xxx 等内网 IP

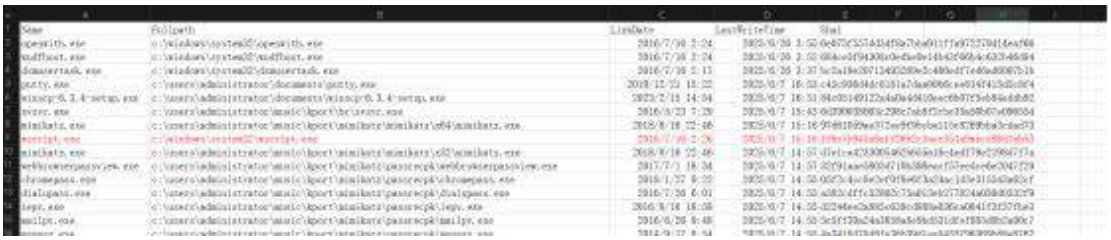


图 87:攻击者启动工具记录

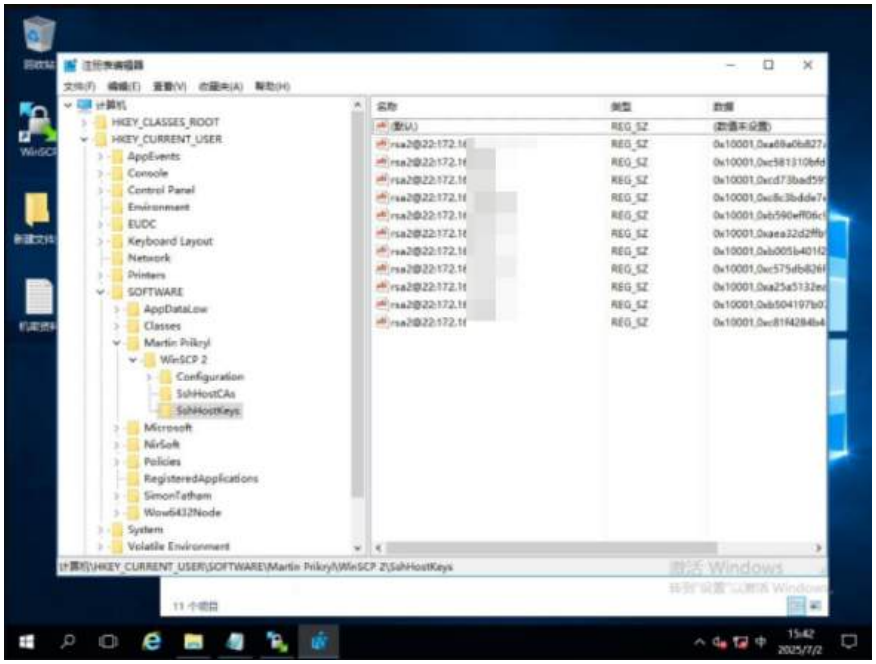


图 88:Winscp 连接记录

攻击者 2025 年 6 月 8 日 0:53 启动 putty 进行远程连接可从会话配置文件中看到

攻击者连接了 172.16.xxx.xxx、172.16.xxx.xxx 等内网 IP

图 89:攻击者启动工具记录

图 90: putty 的会话配置文件

攻击者远程连接 Esxi 记录及加密器执行记录 172.16.xxx.xxx 于 2025 年 6 月 8 日 0:45 首次登录 172.16.xxx.xxx（esxi 服务器）

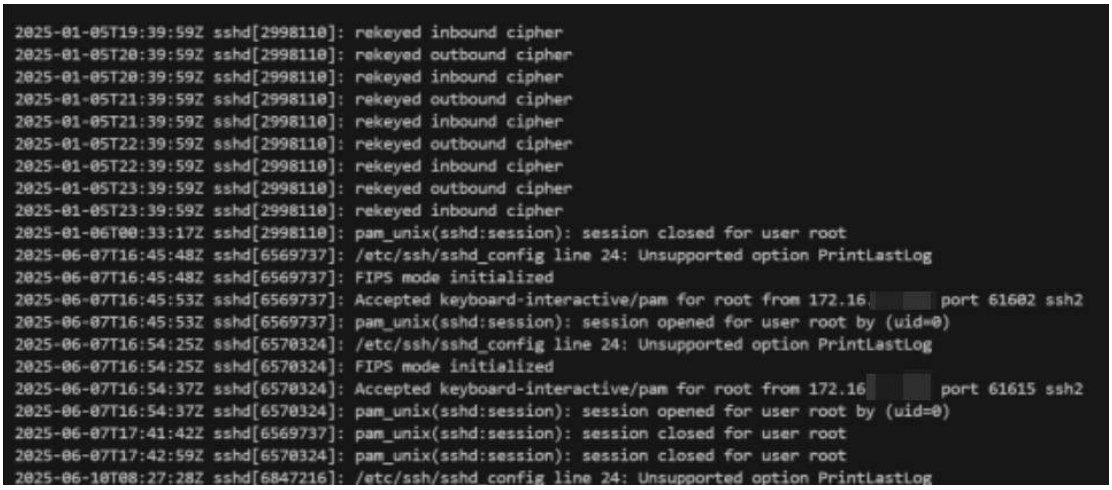


图 91: ssh 连接记录

攻击者于 2025 年 6 月 8 日 1:25 执行名为“encrypter-linux-esxi-x64.run”的勒索软件

```
2024-12-31T23:40:52Z shell[2998171]: [root]: cd vCenter220
2024-12-31T23:40:54Z shell[2998171]: [root]: ls
2024-12-31T23:41:10Z shell[2998171]: [root]: vmkfstools -D vCenter220.vmx~
2025-01-01T06:55:29Z SSH: SSH login disabled
2025-04-20T20:47:18Z ESXShell: ESXi Shell unavailable
2025-04-25T03:09:07Z ESXShell: ESXi Shell unavailable
2025-04-25T03:30:17Z ESXShell: ESXi Shell unavailable
2025-06-07T16:40:44Z SSH: SSH login enabled
2025-06-07T16:54:37Z shell[6570333]: Interactive shell session started
2025-06-07T16:54:41Z shell[6570333]: [root]: cd /tmp
2025-06-07T17:22:20Z shell[6570333]: [root]: chmod +x encrypter-linux-esxi-x64.run
2025-06-07T17:22:40Z shell[6570333]: [root]: date
2025-06-07T17:23:58Z shell[6570333]: [root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
2025-06-07T17:24:42Z shell[6570333]: [root]: esxcli system settings kernel set -s=execinstalledonly -v false
2025-06-07T17:25:32Z shell[6570333]: [root]: ./encrypter-linux-esxi-x64.run -a -d -h 0 -m 0 -s 80
2025-06-07T17:28:02Z shell[6570333]: [root]: date
2025-06-07T17:31:22Z shell[6570333]: [root]: date
2025-06-07T17:31:53Z shell[6570333]: [root]: ./encrypter-linux-esxi-x64.run -a -d -h 17 -m 35 -s 0
2025-06-07T17:33:19Z shell[6570333]: [root]: date
2025-06-07T17:34:09Z shell[6570333]: [root]: date
2025-06-07T17:34:31Z shell[6570333]: [root]: date
2025-06-07T17:34:36Z shell[6570333]: [root]: date
2025-06-07T17:34:54Z shell[6570333]: [root]: date
2025-06-09T04:41:32Z SSH: SSH login disabled
```

图 92: 加密器执行记录

172.16.xxx.xxx 于 2025 年 6 月 8 日 0:46 首次登录 172.16.xxx.xxx（esxi 服务器）

```
[root@vm02-8:~] cat /var/log/auth.log
2021-04-23T05:30:57Z sshd[61109854]: /etc/ssh/sshd_config line 15: Unsupported option PrintLastLog
2021-04-23T05:30:57Z sshd[61109854]: Connection from [redacted] port 63213
2021-04-23T05:31:07Z sshd[61109854]: Accepted keyboard-interactive/pam for root from [redacted] port 63213 ssh2
2021-04-23T05:31:07Z sshd[61109854]: pam_unix(sshd:session): session opened for user root by (uid=0)
2021-04-23T05:31:07Z sshd[61109858]: Session opened for 'root' on /dev/char/pty/t0
2021-04-23T05:32:29Z sshd[61109854]: Session closed for 'root' on /dev/char/pty/t0
2021-04-23T05:32:29Z sshd[61109854]: pam_unix(sshd:session): session closed for user root
2025-06-07T16:46:15Z sshd[146272253]: /etc/ssh/sshd_config line 24: Unsupported option PrintLastLog
2025-06-07T16:46:15Z sshd[146272253]: FIPS mode initialized
2025-06-07T16:46:18Z sshd[146272253]: Accepted keyboard-interactive/pam for root from [redacted] port 61603 ssh2
2025-06-07T16:46:18Z sshd[146272253]: pam_unix(sshd:session): session opened for user root by (uid=0)
2025-06-07T16:55:04Z sshd[146272868]: /etc/ssh/sshd_config line 24: Unsupported option PrintLastLog
2025-06-07T16:55:04Z sshd[146272868]: FIPS mode initialized
2025-06-07T16:55:13Z sshd[146272868]: Accepted keyboard-interactive/pam for root from [redacted] port 61616 ssh2
2025-06-07T16:55:13Z sshd[146272868]: pam_unix(sshd:session): session opened for user root by (uid=0)
2025-06-07T17:39:54Z sshd[146272253]: pam_unix(sshd:session): session closed for user root
2025-06-07T17:40:01Z sshd[146272868]: pam_unix(sshd:session): session closed for user root
2025-06-10T08:36:37Z sshd[146537472]: /etc/ssh/sshd_config line 24: Unsupported option PrintLastLog
```

图 93: ssh 连接记录

攻击者于 2025 年 6 月 8 日 1:32 执行名为“encrypter-linux-esxi-x64.run”的勒索软件

```
2024-01-30T07:25:02Z ESXShell: ESXi Shell unavailable
2024-01-30T07:33:03Z ESXShell: ESXi Shell unavailable
2024-06-03T06:37:07Z ESXShell: ESXi Shell unavailable
2025-06-07T16:42:29Z SSH: SSH login enabled
2025-06-07T17:02:23Z shell[19774222]: Interactive shell session started
2025-06-07T17:02:33Z shell[19774222]: [root]: cd /tmp
2025-06-07T17:22:37Z shell[19774222]: [root]: chmod +x encrypter-linux-esxi-x64.run
2025-06-07T17:24:18Z shell[19774222]: [root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
2025-06-07T17:24:30Z shell[19774222]: [root]: esxcli system settings kernel set -s=execinstalledonly -v false
2025-06-07T17:28:51Z shell[19774222]: [root]: date
2025-06-07T17:32:14Z shell[19774222]: [root]: ./encrypter-linux-esxi-x64.run -a -d -h 17 -m 35 -s 0
2025-06-10T09:57:32Z shell[19918720]: Interactive shell session started
2025-06-10T09:57:38Z shell[19918720]: [root]: cat .ash_history
2025-06-10T09:59:16Z shell[19918720]: [root]: cat /var/log/auth.log
```

图 94: 加密器执行记录

172.16.xxx.xxx 于 2025 年 6 月 8 日 0:46 首次登录 172.16.xxx.xxx（esxi 服务器）

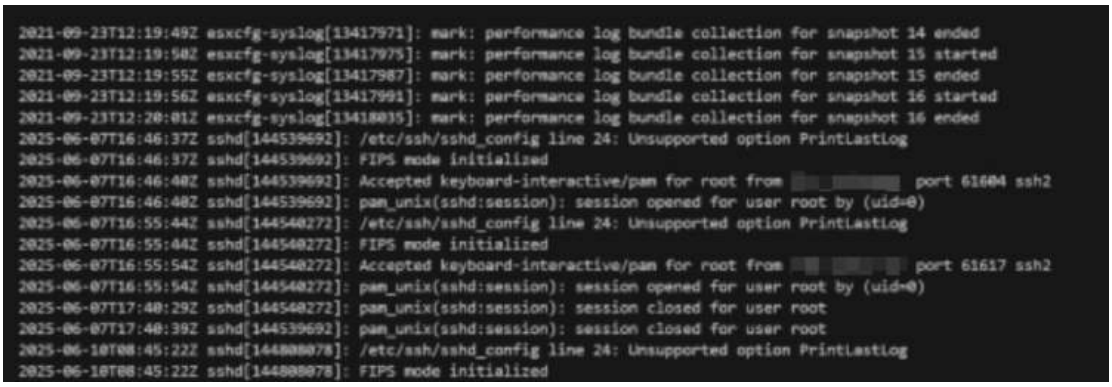


图 95: ssh 连接记录

攻击者于 2025 年 6 月 8 日 1:31 执行名为“encrypter-linux-esxi-x64.run”的勒索软件

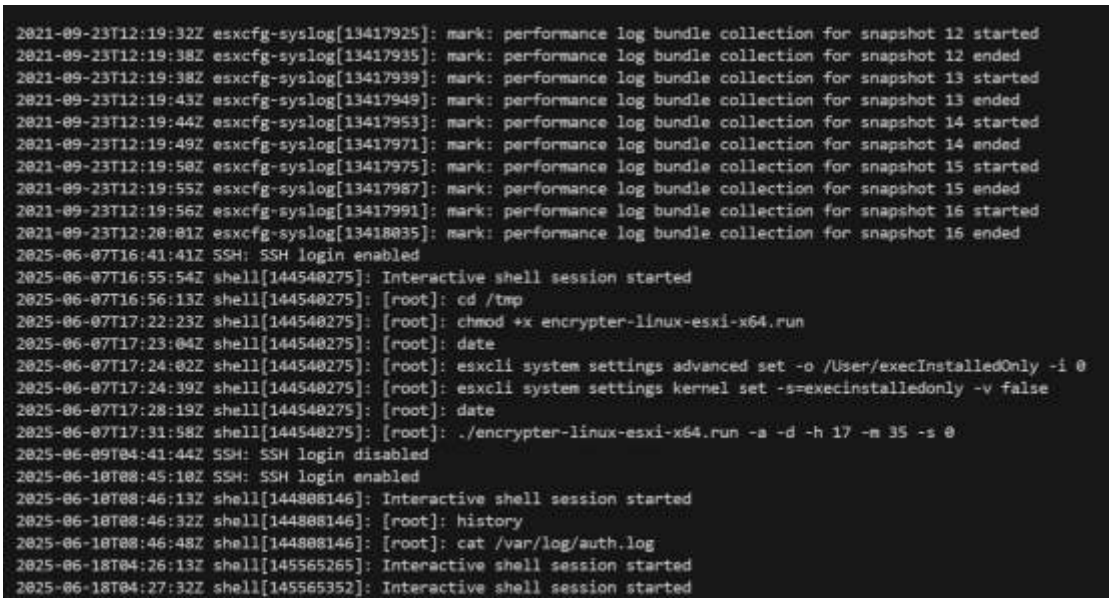


图 96: 加密器执行记录

172.16.xxx.xxx 于 2025 年 6 月 8 日 0:51 首次登录 172.16.xxx.xxx（esxi 服务器）

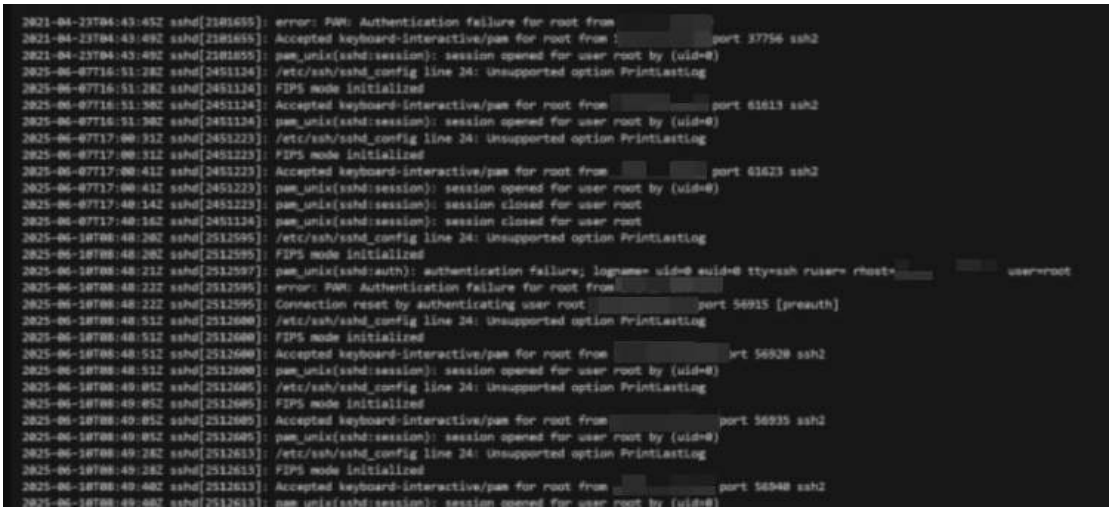


图 97: ssh 连接记录

攻击者于 2025 年 6 月 8 日 1:32 执行名为“encrypter-linux-esxi-x64.run”的勒索软件

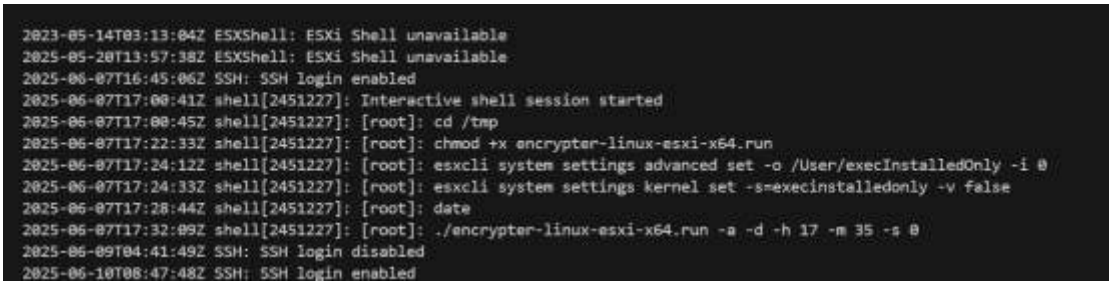


图 98: 加密器执行记录

172.16.xxx.xxx（攻防演练机器）于 2025 年 6 月 8 日 0:51 首次登录 172.16.xxx.xxx（esxi 服务器）

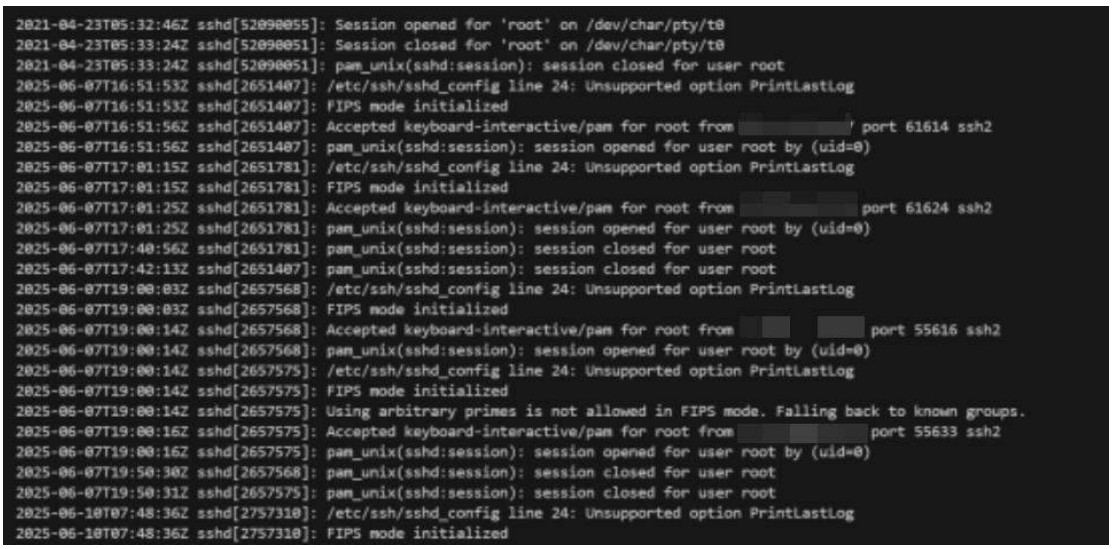


图 99: ssh 连接记录

攻击者于 2025 年 6 月 8 日 1:32 执行名为“encrypter-linux-esxi-x64.run”的勒索软件

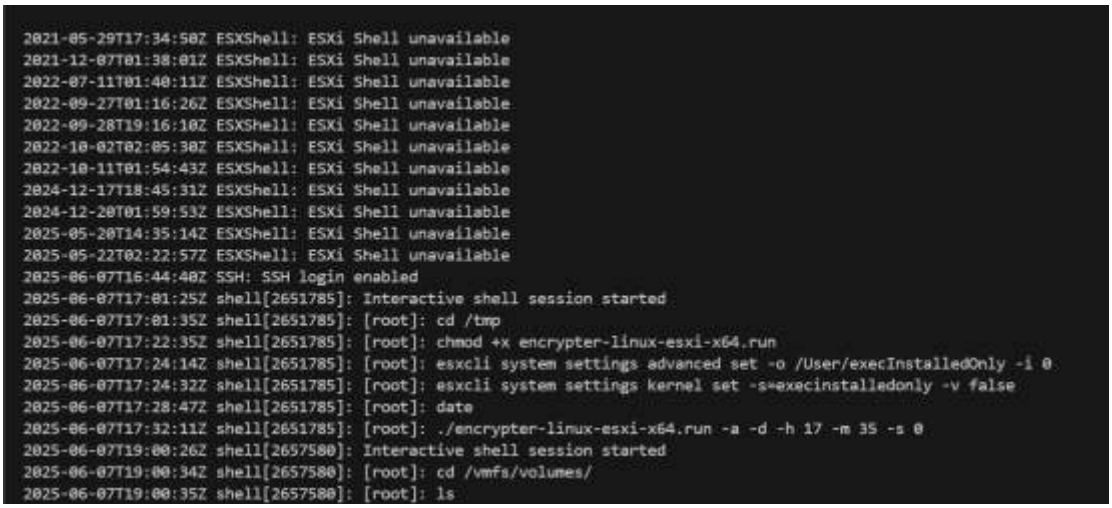


图 100: 加密器执行记录

172.16.xxx.xxx（攻防演练机器）于 2025 年 6 月 8 日 0:47 首次登录 172.16.xxx.xxx（esxi 服务器）

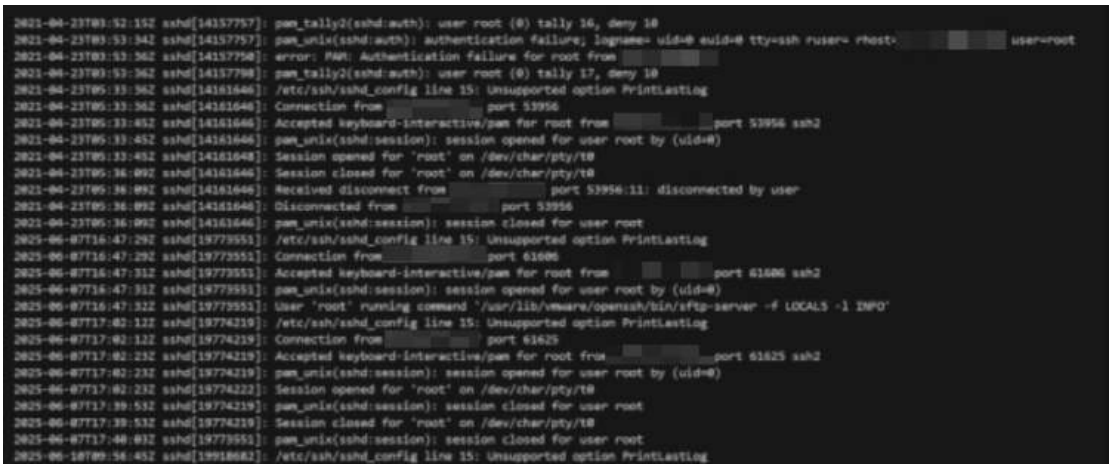


图 101: ssh 连接记录

攻击者于 2025 年 6 月 8 日 1:32 执行名为“encrypter-linux-esxi-x64.run”的勒索软件

```
2023-11-10T22:29:14Z ESXShell: ESXi Shell unavailable
2024-01-30T01:22:22Z ESXShell: ESXi Shell unavailable
2024-01-30T01:50:37Z ESXShell: ESXi Shell unavailable
2024-01-30T07:25:02Z ESXShell: ESXi Shell unavailable
2024-01-30T07:33:03Z ESXShell: ESXi Shell unavailable
2024-06-03T06:37:07Z ESXShell: ESXi Shell unavailable
2025-06-07T16:42:29Z SSH: SSH login enabled
2025-06-07T17:02:23Z shell[19774222]: Interactive shell session started
2025-06-07T17:02:33Z shell[19774222]: [root]: cd /tmp
2025-06-07T17:22:37Z shell[19774222]: [root]: chmod +x encrypter-linux-esxi-x64.run
2025-06-07T17:24:18Z shell[19774222]: [root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
2025-06-07T17:24:30Z shell[19774222]: [root]: esxcli system settings kernel set -s=execinstalledonly -v false
2025-06-07T17:28:51Z shell[19774222]: [root]: date
2025-06-07T17:32:14Z shell[19774222]: [root]: ./encrypter-linux-esxi-x64.run -a -d -h 17 -m 35 -s 0
2025-06-10T09:57:32Z shell[19918720]: Interactive shell session started
2025-06-10T09:57:38Z shell[19918720]: [root]: cat .ash_history
2025-06-10T09:59:16Z shell[19918720]: [root]: cat /var/log/auth.log
2025-06-10T09:59:59Z SSH: SSH login disabled
2025-06-18T04:54:38Z SSH: SSH login enabled
```

图 102: 加密器执行记录

172.16.xxx.xxx（攻防演练机器）于 2025 年 6 月 8 日 0:48 首次登录 172.16.xxx.xxx（esxi 服务器）

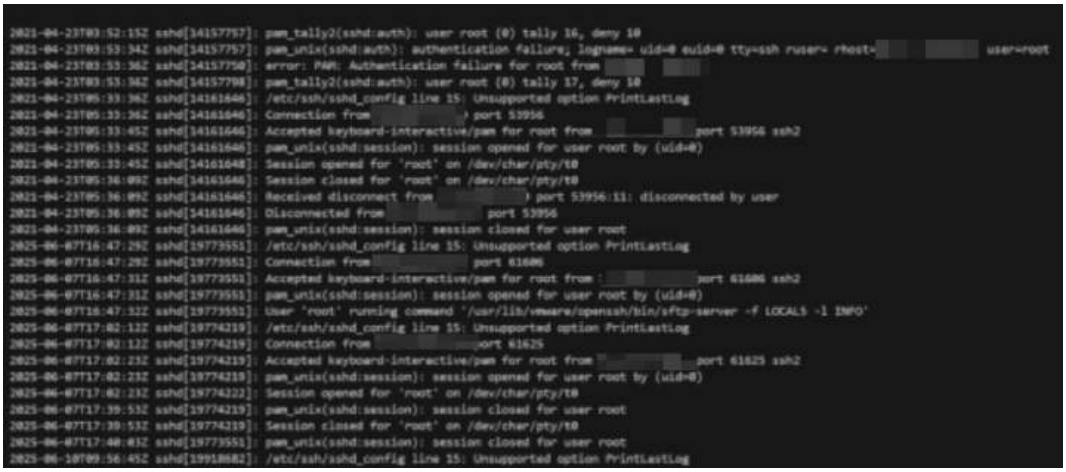


图 103: ssh 连接记录

攻击者于 2025 年 6 月 8 日 1:32 执行名为“encrypter-linux-esxi-x64.run”的勒索软件

```
2022-03-02T08:25:23Z ESXShell: ESXi Shell unavailable
2022-03-04T03:26:45Z ESXShell: ESXi Shell unavailable
2022-05-09T14:23:38Z ESXShell: ESXi Shell unavailable
2023-09-14T11:09:52Z ESXShell: ESXi Shell unavailable
2024-02-07T02:05:46Z ESXShell: ESXi Shell unavailable
2024-06-03T06:39:28Z ESXShell: ESXi Shell unavailable
2025-05-20T14:00:00Z ESXShell: ESXi Shell unavailable
2025-05-22T02:47:35Z ESXShell: ESXi Shell unavailable
2025-06-07T16:43:48Z SSH: SSH login enabled
2025-06-07T16:59:17Z shell[905959]: Interactive shell session started
2025-06-07T16:59:33Z shell[905959]: [root]: cd /tmp
2025-06-07T17:22:30Z shell[905959]: [root]: chmod +x encrypter-linux-esxi-x64.run
2025-06-07T17:24:09Z shell[905959]: [root]: esxcli system settings advanced set -o /User/execInstalledOnly -i 0
2025-06-07T17:24:35Z shell[905959]: [root]: esxcli system settings kernel set -s=execinstalledonly -v false
2025-06-07T17:28:35Z shell[905959]: [root]: date
2025-06-07T17:32:06Z shell[905959]: [root]: ./encrypter-linux-esxi-x64.run -a -d -h 17 -m 35 -s 0
2025-06-10T08:59:33Z shell[1052315]: Interactive shell session started
2025-06-10T08:59:38Z shell[1052315]: [root]: ps | grep run
2025-06-10T09:00:15Z shell[1052315]: [root]: history
2025-06-10T09:00:29Z shell[1052315]: [root]: history
2025-06-10T09:01:03Z shell[1052315]: [root]: cat /.ash_history
2025-06-10T09:01:18Z shell[1052315]: [root]: cat /var/log/auth.log
```

图 104 :加密器执行记录

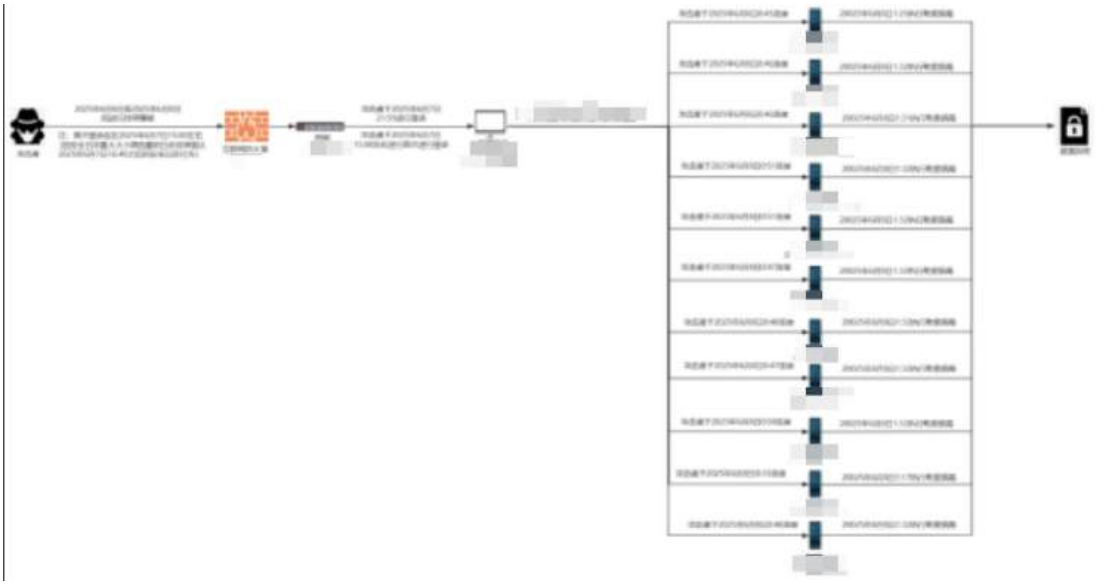


图 105:攻击者攻击路径图

1.2 Sqlserver 数据库弱口令

【溯源分析过程】2025 年 5 月 29 日（Windows server 2008 默认记录系统日志数量有限爆破开始时间应早于该时间）-2025 年 6 月 17 日期间大量 sql 爆破记录恶意攻击 ip 为：45.134.26.xxx、45.134.26.xxx、91.238.xxx.xxx 等经过分析均为国外代理 IP 或者跳板服务器。

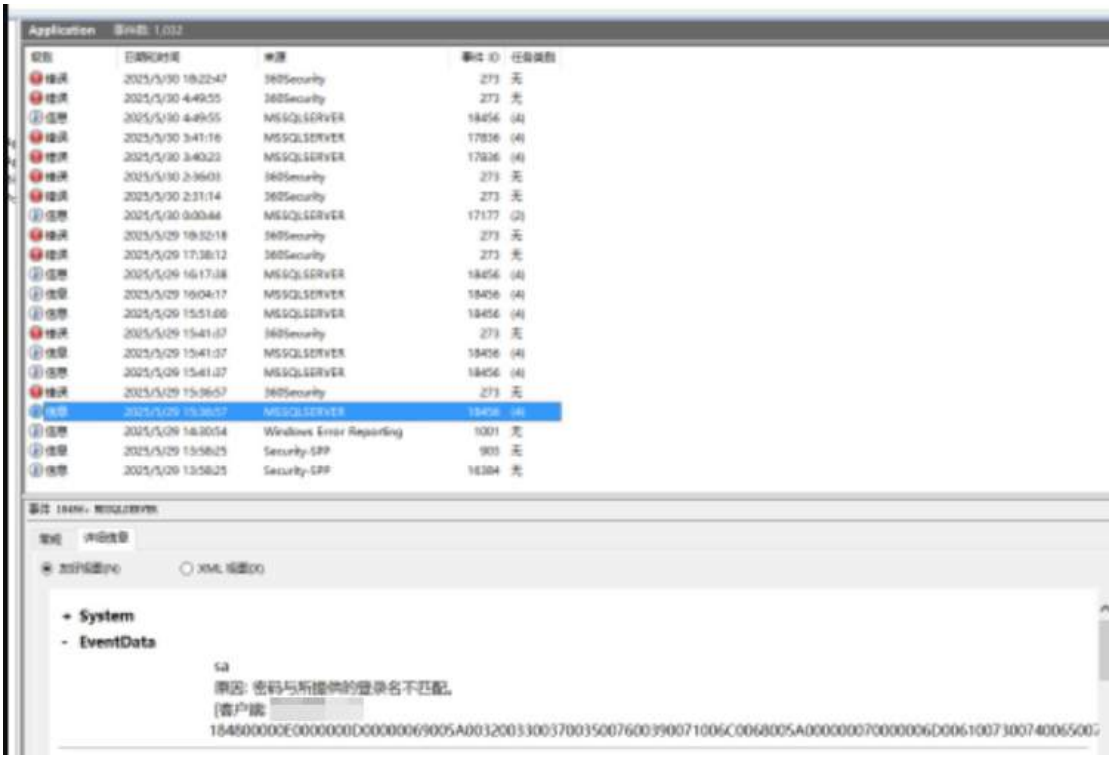


图 106:历史爆破数据库端口证明-1

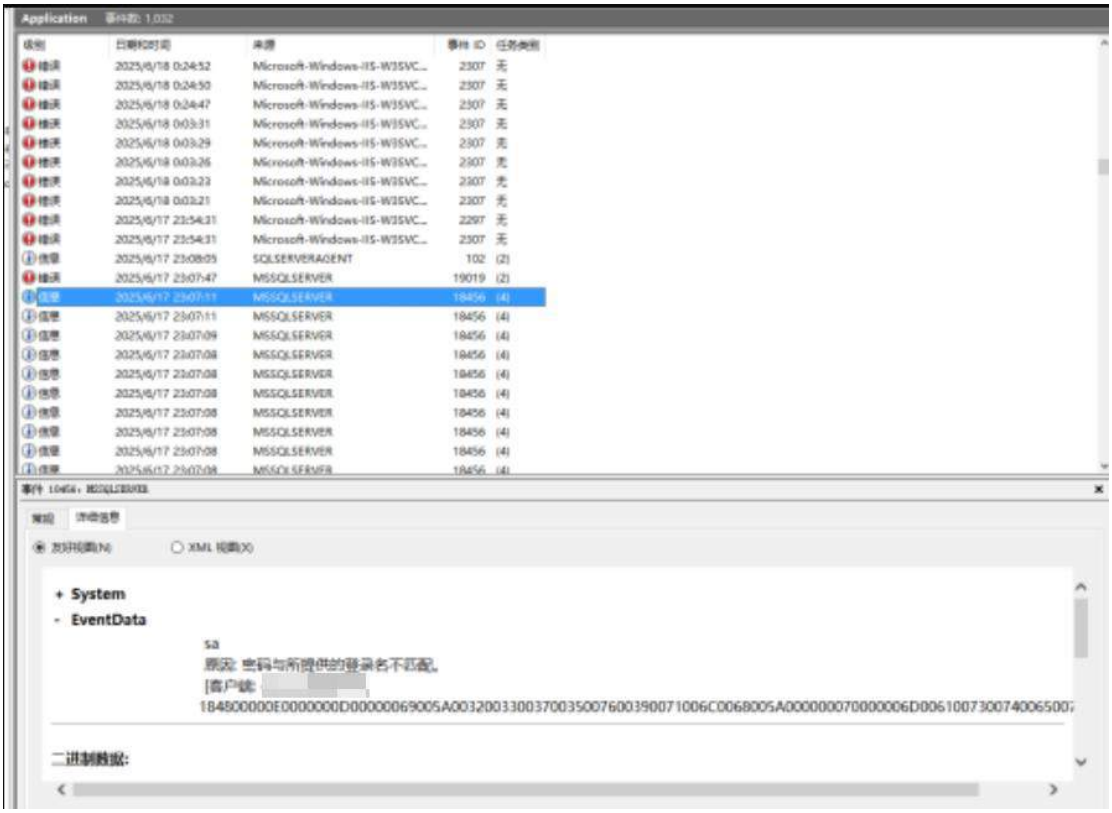


图 107:历史爆破数据库端口证明-2

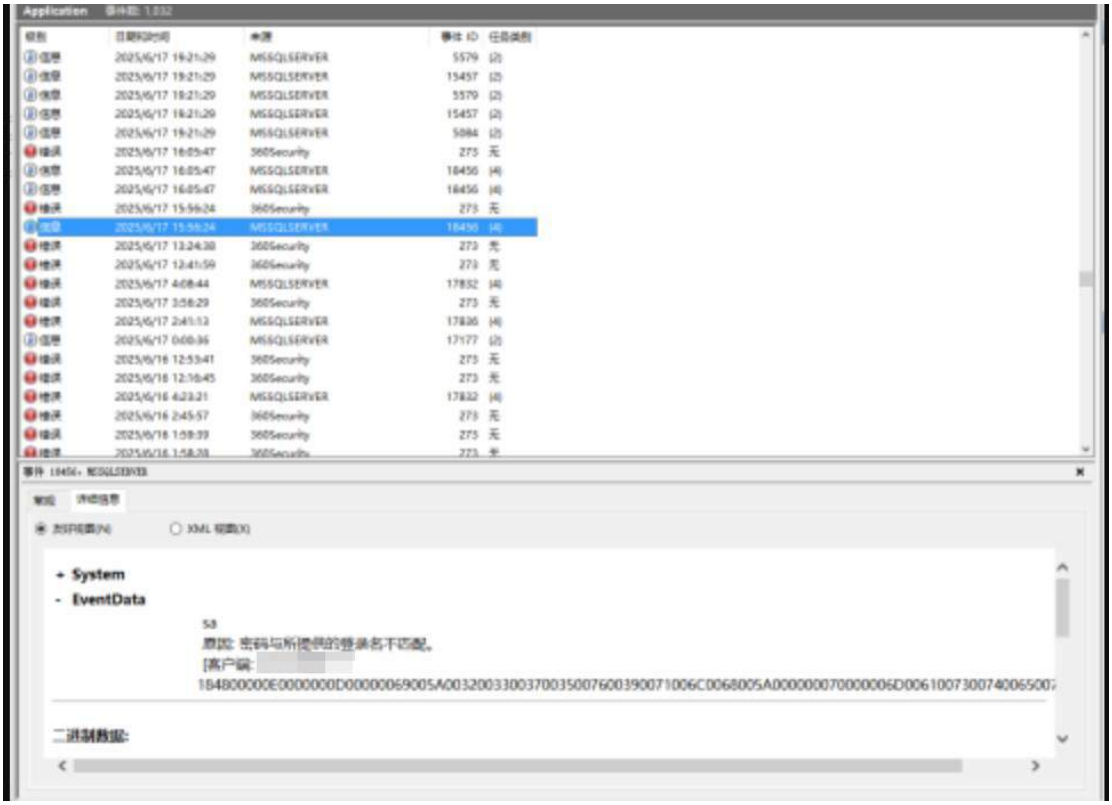


图 108:历史爆破数据库端口证明-3

2025 年 6 月 17 日 16:05 到 2025 年 6 月 17 日 19:21 爆破中断（因 sqlserver 默认登录日志未开启则推断攻击者在使用爆破工具爆破成功后停止爆破疑似爆破成功）随后在 2025 年 6 月 17 日 19:21 攻击者登录数据库将 TRUSTWORTHY 属性被设置为 ON 随后启动 CLR 程序集（启动后可加载恶意程序集达到命令执行、提权、获取计算机权限等操作）。

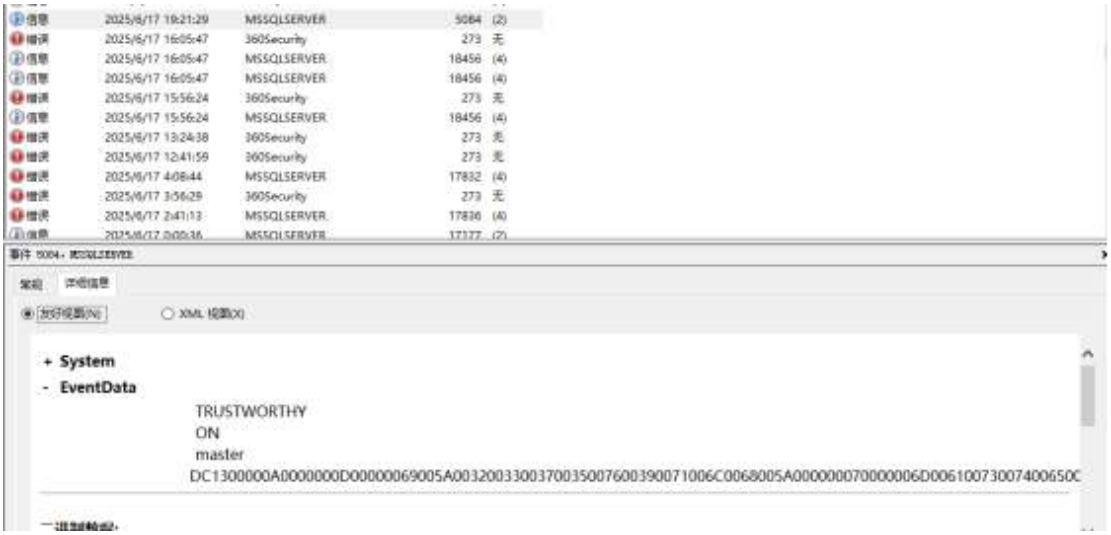


图 109:攻击者数据库操作

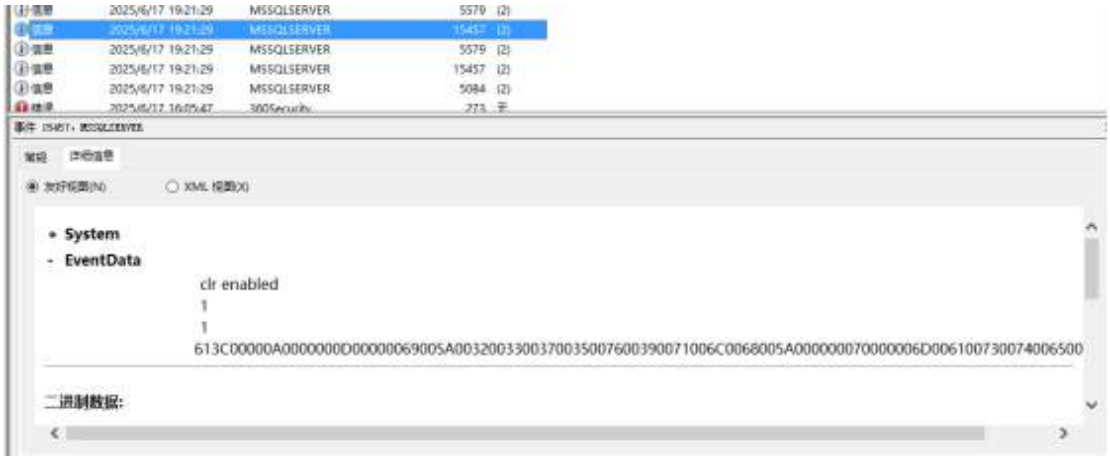


图 110:攻击者数据库操作

2025 年 6 月 17 日 19:21 攻击者创建 AppDomain 2 用于加载的恶意 CLR 程序集“qlclrpayloa”后续删除卸载 AppDomain 2 等恶意操作可证明攻击者已获取数据库权限且已执行命令或者获取服务器控制权限，从攻击顺序和手法可判断攻击者爆破数据库成功后进行登录执行恶意操作。

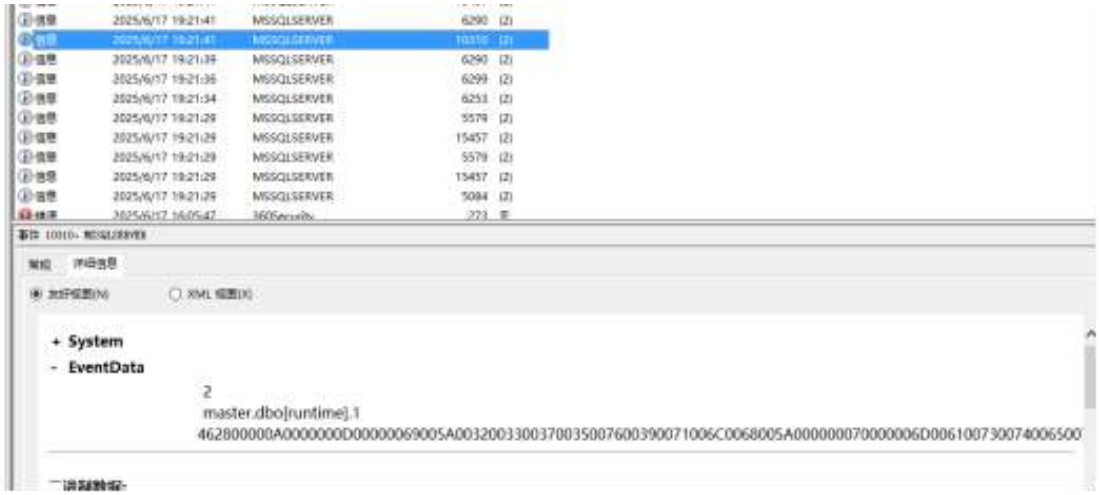


图 111:攻击者数据库操作

图 112:攻击者加载恶意 CLR 程序集

后续攻击者通过数据库获取的权限获取系统密码 2025 年 6 月 17 日 22:53 攻击者初次使用恶意 IP：149.88.28.xxx(IP 为法国，分析为攻击者使用代理 IP)远程登录服务器。

图 113:攻击者远程登录桌面

2025 年 6 月 17 日 22:53 攻击者使用恶意 IP：149.88.xxx.xxx 再次远程登录(IP 为法国，分析为攻击者使用代理 IP)

图 114:攻击者远程登录桌面

2025 年 6 月 17 日 22:59 攻击者关闭 360 安全防御

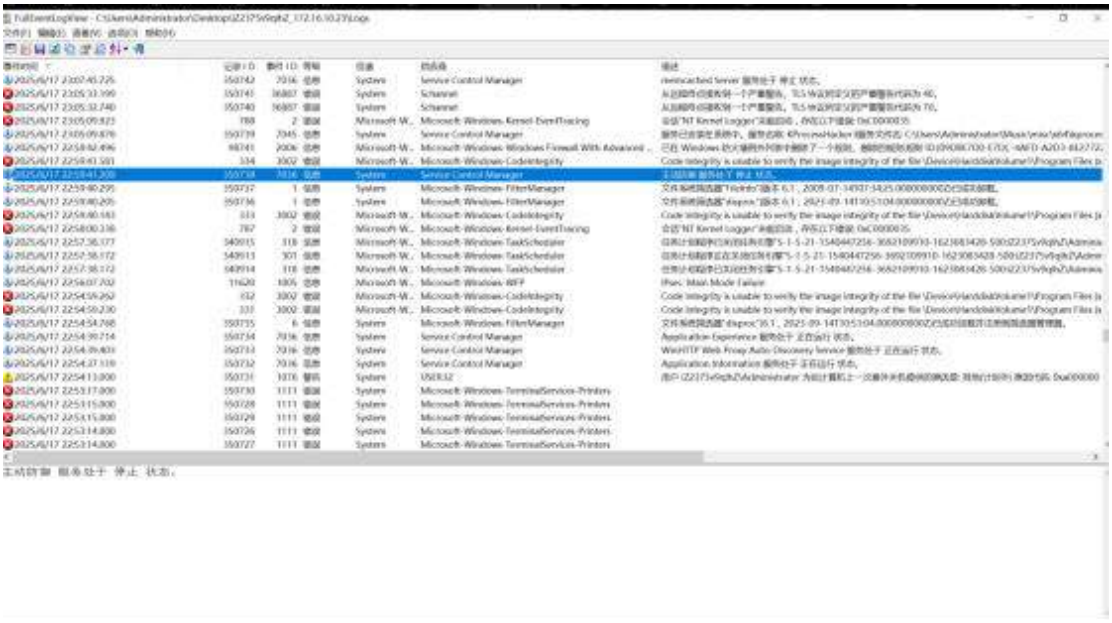


图 115:攻击者关闭 360 安全防护软件

2025 年 6 月 17 日 23:07 攻击者执行名为“svchost.exe”勒索软件，勒索软件运行自动结束数据库等进程开始执行加密操作。

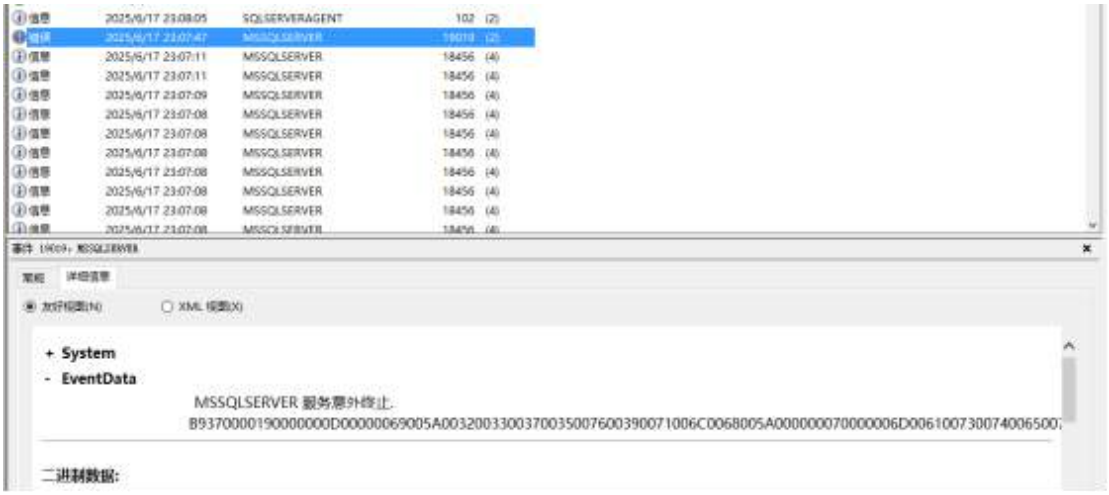


图 116:攻击者执行勒索软件结束数据库进程

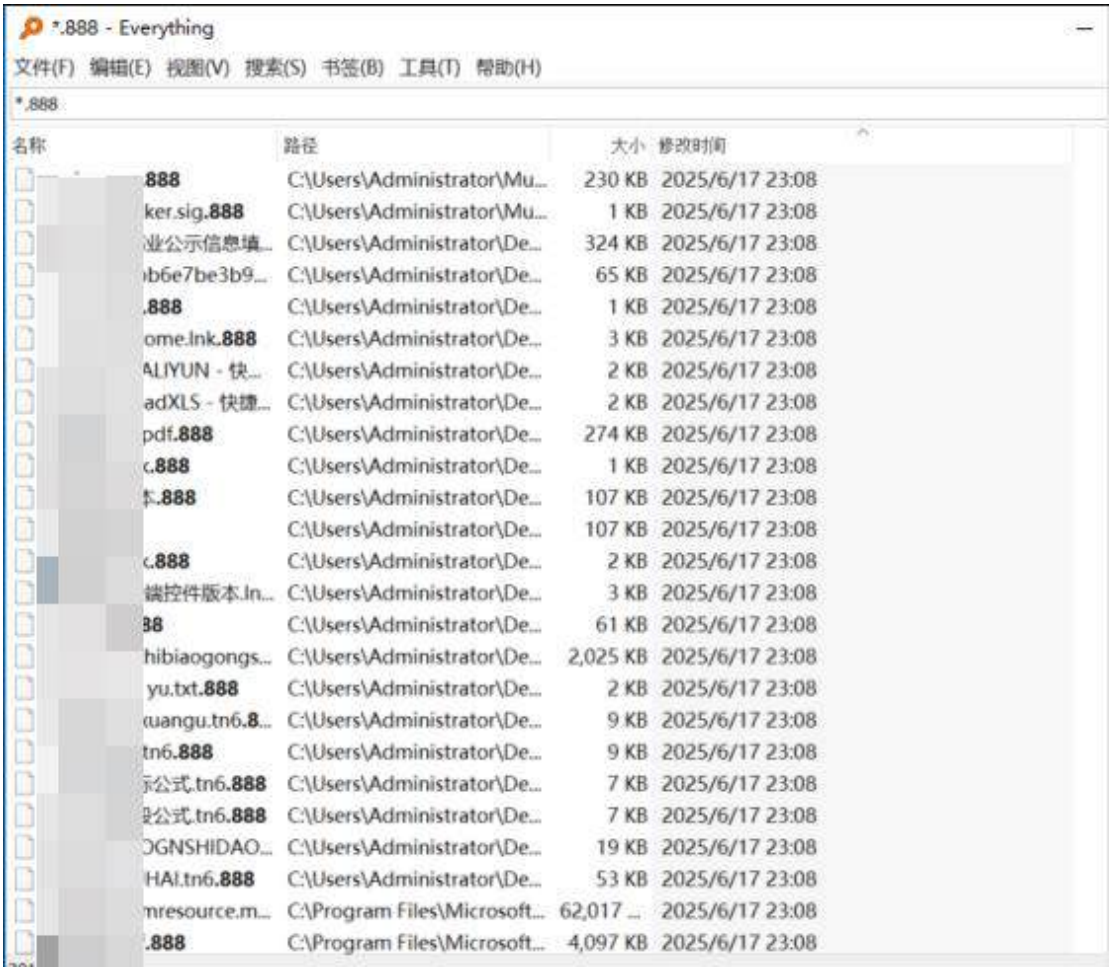


图 117:攻击者执行勒索软件修改文件时间

攻击者执行的勒索软件和攻击者工具均在”C:\Users\Administrator\Music\”路径下

图 118:攻击者使用攻击者工具和路径

图 119:攻击者使用的勒索软件路径

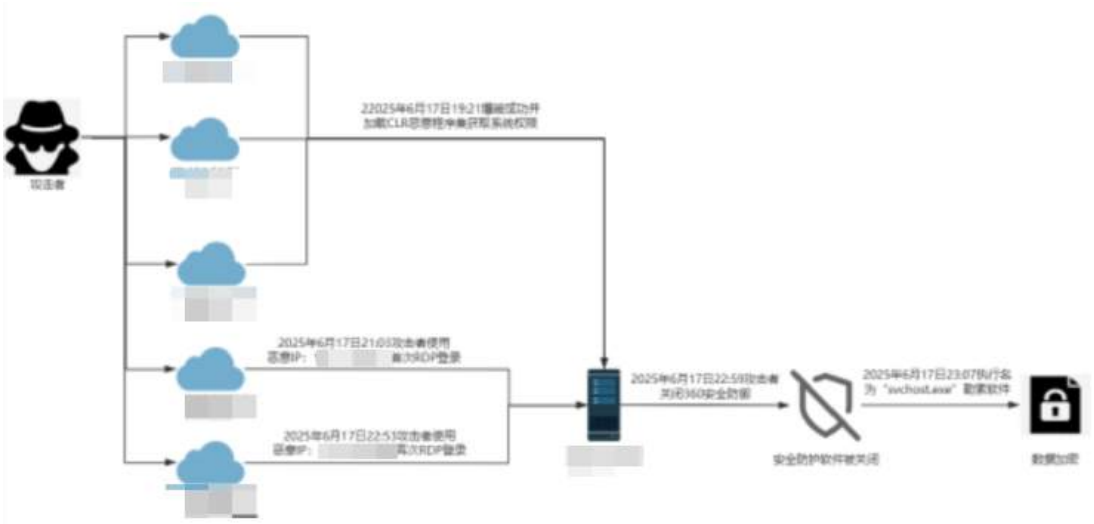


图 120:攻击者攻击路径图

1.3 VPN 弱口令

初始入侵阶段（7 月 18 日）：攻击者通过 VPN 账号密码弱口令 或泄漏获得初始访问权限，异常账号 sysadmin 成功登录 FTP04 和 DC01 服务器。22:54 攻击者在 FTP04 上传扫描工具包 netskcan.zip，23:58 开始使用扫描器对域控进行探测并生成扫描结果 10.0.xxx.xxx.xml 文件。

横向扩散阶段（7 月 19 日-7 月 23 日）：攻击者利用 FTP04、 SDC-MANAGE 作为跳板机，使用 sysadmin 账号登录多台主机包括 FTP02、 SDC-MANAGE 等，探测该账号的域内权限。经查询发现 sysadmin 账号 在域控内没有批

注记录，推测为可疑账号但具有全域登录权限。

恶意程序部署阶段（7 月 20 日-7 月 21 日）：2025 年 7 月 20 日 5:05 攻击者在 FTP04 投放恶意远控程序 exe.exe 与 msedge.exe，5:17 投放针对本集团定制的恶意远控程序 msedge64-MOTOVIS.exe，其编译时间为 2025 年 3 月 7 日 2:57，推测为此次攻击专门定制。攻击者多次尝试禁用 Windows 防火墙，并在 7 月 21 日 5:33 对 FTP04 的 C 盘进行整个加白名单处理。

数据窃取与加密爆发（7 月 22 日）：攻击者在 FTP02、SDC-MANAGER 与 DC01 上部署数据窃取工具 rclone（网盘软件）与 fil.exe（FTP 软件）进行数据外泄。22:57 统一投放勒索加密器对所有目标服务器 实施加密攻击。

阶段	时间	攻击行为
初始入侵	2025 年 7 月 18 日	利用异常账号入侵企业内部网络
横向扩散	2025 年 7 月 18-23 日	使用异常账号进行横向扫描攻击
恶意程序部署	2025 年 7 月 20-21 日	恶意远程控制软件
数据窃密	2025 年 7 月 22 日	使用恶意数据窃取工具进行数据窃取
最终攻击	2025 年 7 月 22 日	投放勒索加密器并对数据进行加密

表 19:阶段展示

图 121:攻击者攻击路径图

1.4 Web 应用弱口令

服务器被植入勒索软件，文件被加密，加密文件的后缀为.HhgTqFWUz、JiBplbZe1，根据勒索界面和加密后缀判断该勒索软件为病毒家族盗版 LB3 的变种病毒。本次中勒索软件的 有两台主机，下面会逐一进行分析。

1.客户某应用虚拟化软件业务映射在公网，IP 为 222.81.xxx.xxx

2.基于日志排查发 IP 185.49.xxx.xxx 使用管理员用户于 2025/7/31 13:40:02 登录成功应用服务器

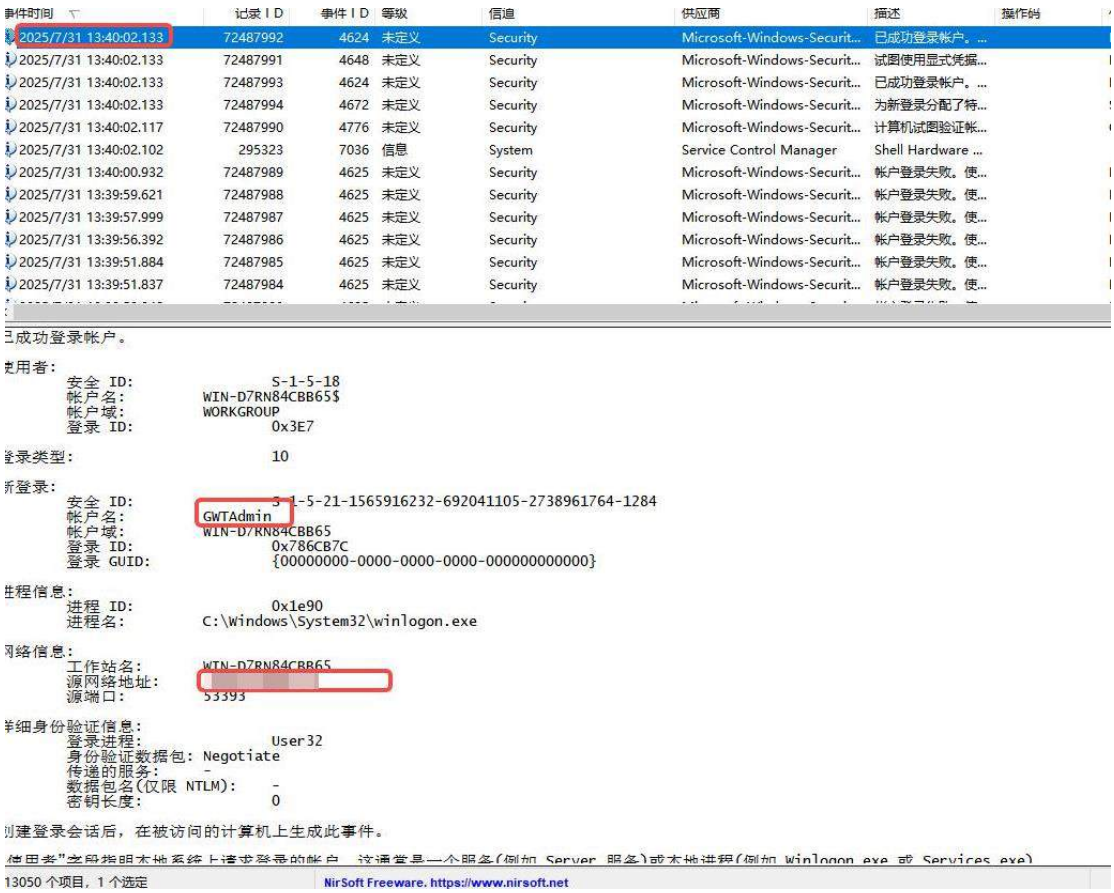


图 122:登陆成功截图

3.咨询客户，该业务采用的账号密码为 admin/123，该密码强度为弱口令，攻击者可轻松爆破后登录，在后续的某应用虚拟化软件日志中会提供相关记录

4.在某应用虚拟化软件日志中找到对应记录，可疑 IP 在加密前成功登录某应用虚拟化软件 WEB，下图所附为日志 所记录的登录详情，可疑 IP 92.60.xxx.xxx 于 2025/07/31 15:54:49 使用 admin/123 成功登录，202cb962axxxxxxxxxxx7152d234b70 为 md5 加密后结果

```
92.60.xxx.xxx - - [31/Jul/2025:15:54:49 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000006&Language=EN&User=
admin&PWD=202cb96xxxxxxxxxxx07152d234b70&AuthType=0&Computer=SZ-108&Finger=A22789EF5&IP= HTTP/1.1" 200 -
92.60.xxx.xxx - - [31/Jul/2025:15:55:29 +0800] "GET
/casweb/key/key.dat HTTP/1.1" 200 4399
92.60.xxx.xxx - - [31/Jul/2025:15:55:57 +0800] "GET
```

```
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000006&Language=EN&Use
r= admin&PWD=202cb9xxxxxxxxxxb07152d234b70&AuthType=0&Computer=SZ-
10 8&Finger=A22789EF5&IP= HTTP/1.1" 200 -
92.60.xxx.xxx - - [31/Jul/2025:15:56:06 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=EN&Use
r=
admin&PWD=202cb962ac59xxxxxxxxxxx2d234b70&AuthType=0&Computer=SZ-
10 8&Finger=A22789EF5&IP= HTTP/1.1" 200 1661
```

8.某应用虚拟化软件日志找到的其他可疑 IP 登录记录详情，可疑 IP171.105.xxx.xxx 于 2025/04/17 04:55:32 使用 admin/123 成功登录，202cb962acXXXXXXXXXX07152d234b70 为 md5 加密后结果，为国内 IP 需重点关注

```
171.105.xxx.xxx - - [17/Apr/2025:04:55:32 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us er=admin&PWD=3349XXXXXXXXXX3673fe3f5&AuthType=0&Computer=WI
N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
171.105.xxx.xxx - - [17/Apr/2025:04:55:33 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=a66f877XXXXXXXXXXfaf166fb243a&AuthType=0&Computer=WI
N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
171.105.xxx.xxx - - [17/Apr/2025:04:55:33 +0800]
"GET/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH
-CN&Us
er=admin&PWD=e40f01afXXXXXXXXXX7ced5bca532&AuthType=0&Computer=WI
N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
171.105.xxx.xxx - - [17/Apr/2025:04:59:00 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=21232fXXXXXXXXXX3894a0e4a801fc3&AuthType=0&Computer=W
I N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
171.105.xxx.xxx - - [17/Apr/2025:04:59:01 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=c4ca423XXXXXXXXXX09a6f75849b&AuthType=0&Computer=WI
N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
171.105.xxx.xxx - - [17/Apr/2025:04:59:01 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=202cb962acXXXXXXXXXX07152d234b70&AuthType=0&Computer=
WI N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 -
171.105.xxx.xxx - - [17/Apr/2025:04:59:01 +0800] "GET
```

```
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=827ccb0eeXXXXXXXXX6891f84e7b&AuthType=0&Computer=WI
N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
171.105.xxx.xxx - - [17/Apr/2025:04:59:01 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=e10adc39XXXXXXXXXX20f883e&AuthType=0&Computer=WI N-
1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
```

9.某应用虚拟化软件日志找到的其他可疑 IP 登录记录详情，可疑 IP116.11.xxx.xxx 于 2025/06/13 17:44:16 使用 admin/123 成功登录，202cb962acXXXXXXXXXX07152d234b70 为 md5 加密后结果，该 IP 有过爆破行为并且成功，字典与 171.105.xxx.xxx 相似度较高， 且为国内 IP 需重点关注

```
116.11.xxx.xxx - - [13/Jun/2025:17:44:16 +0800] "GET / HTTP/1.1"
200 9427
116.11.xxx.xxx - - [13/Jun/2025:17:45:38 +0800] "GET
/RAPAgent.XGI?CMD=GetClientExeVer HTTP/1.1" 200 35
116.11.xxx.xxx - - [13/Jun/2025:17:45:38 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&User=admin&PWD=a66f877XXXXXXXXXXfaf166fb243a&AuthType=0&Compute
r=WI N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
116.11.xxx.xxx - - [13/Jun/2025:17:45:41 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=21232f297XXXXXXXXXX4a801fc3&AuthType=0&Computer=WI N-
1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
116.11.xxx.xxx - - [13/Jun/2025:17:45:49 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=c4ca423XXXXXXXXXX6f75849b&AuthType=0&Computer=WI N-
1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
116.11.xxx.xxx - - [13/Jun/2025:17:45:58 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=c20ad4d7XXXXXXXXXXbff6710&AuthType=0&Computer=WI N-
1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
116.11.xxx.xxx - - [13/Jun/2025:17:46:05 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=202cb962acXXXXXXXXXX07152d234b70&AuthType=0&Computer=
WI N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 -
116.11.xxx.xxx - - [13/Jun/2025:17:46:19 +0800] "GET
```

```
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us er=admin&PWD=81dc9XXXXXXXXXed055&AuthType=0&Computer=WI N-
1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
116.11.xxx.xxx - - [13/Jun/2025:17:46:21 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=827ccb0eeXXXXXXXXXX1f84e7b&AuthType=0&Computer=WI N-
1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
116.11.xxx.xxx - - [13/Jun/2025:17:46:44 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us er=admin&PWD=e10adc3949bXXXXXXXXXX3e&AuthType=0&Computer=WI
N-1TLJMBOFIT6&Finger=A45A2E5E3&IP= HTTP/1.1" 200 53
```

10.某应用虚拟化软件日志找到的其他可疑 IP 登录记录详情，可疑 IP125.76.xxx.xxx 于 2025/07/27 18:16:20 使用 admin/123 成功登录，202cb962acXXXXXXXXXX07152d234b70 为 md5 加密后结果，该 IP 无任何爆破行为，一次即成功，且为国内 IP 需重点关注

```
125.76.xxx.xxx - - [27/Jul/2025:18:16:20 +0800] "GET
/RAPAgent.XGI?CMD=GETApplication&AppID=APP00000001&Language=ZH-
CN&Us
er=admin&PWD=202cb962acXXXXXXXXXX07152d234b70&AuthType=0&Computer=
CW SERVER&Finger=AB267E136&IP= HTTP/1.1" 200 1661
```

11.由于客户数据库日志配置不记录成功日志，导致无法获取更多佐证信息；

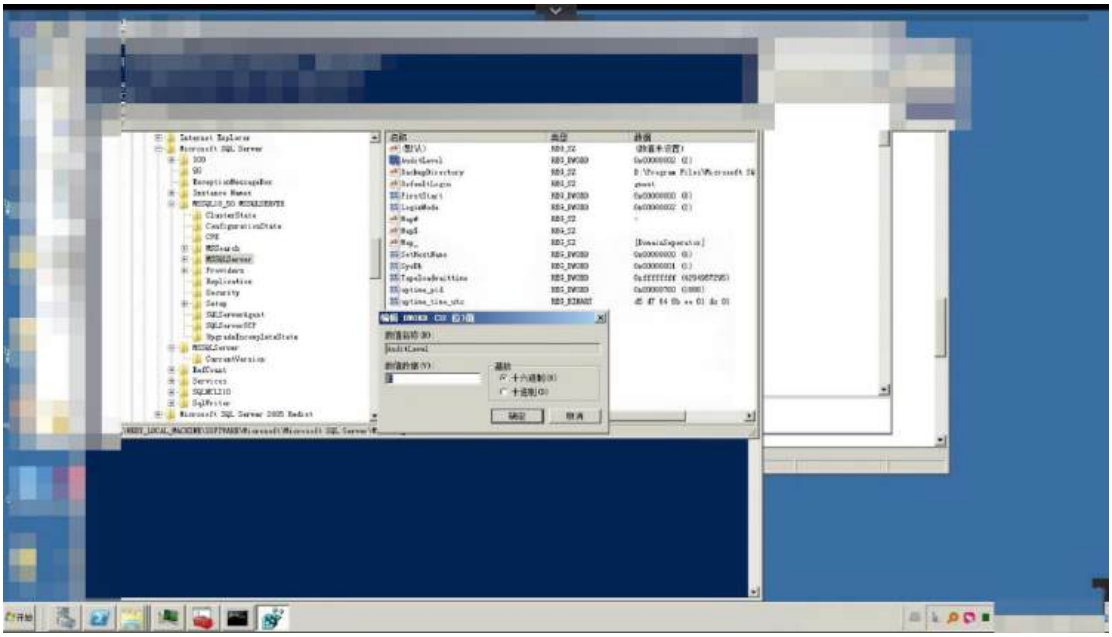


图 123:不记录成功日志截图

12.应用服务器开始加密时间为 2025/7/31 16:22;

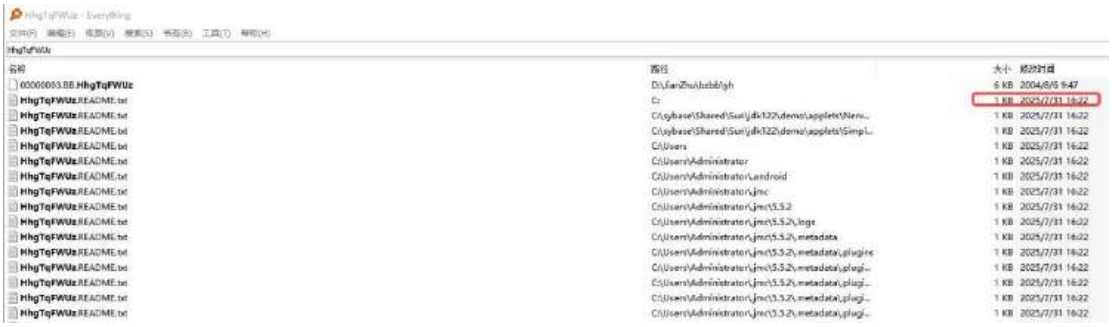


图 124:应用服务器开始加密时间

13.数据库服务器开始加密时间为 2025/7/31 15:39

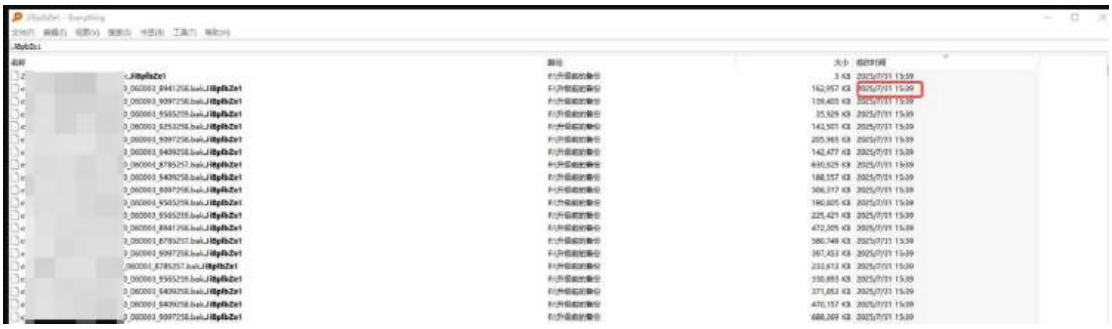


图 125:数据库服务器开始加密时间

14.加密器落地时间为 2025/7/31 16:22 且执行成功实施加密操作

	绝对路径	最后修改时间（本地时间）	是否执行
2	C:\Windows\system32\LogonUI.exe	2010/11/21 11:24	是
3	E:\INSPUR\PS11\config.exe	2016/3/25 16:52	是
4	C:\Program Files\WinRAR\WinRAR.exe	2017/8/30 15:09	是
5	C:\Windows\system32\mstsc.exe	2010/11/21 11:24	是
6	E:\INSPUR\PS11\kzt.exe	2018/10/23 17:34	是
7	C:\Windows\System32\slui.exe	2010/11/21 11:24	是
8	C:\Windows\system32\taskhost.exe	2010/11/21 11:24	是
9	C:\Windows\system32\TSTheme.exe	2009/7/14 9:39	是
10	C:\inetpub\LB3.exe	2025/7/27 18:18	是
11	C:\Windows\System32\perfmon.exe	2010/11/21 11:24	是
12	C:\inetpub\2.exe	2025/7/31 16:16	是
13	C:\Windows\system32\taskmgr.exe	2010/11/21 11:24	是
14	C:\Program Files (x86)\Internet Explorer\iexplore.exe	2010/11/21 11:25	是
15	E:\INSPUR\PS11.0.1\setcv.exe	2017/2/21 8:49	是

图 126:加密器落地执行记录

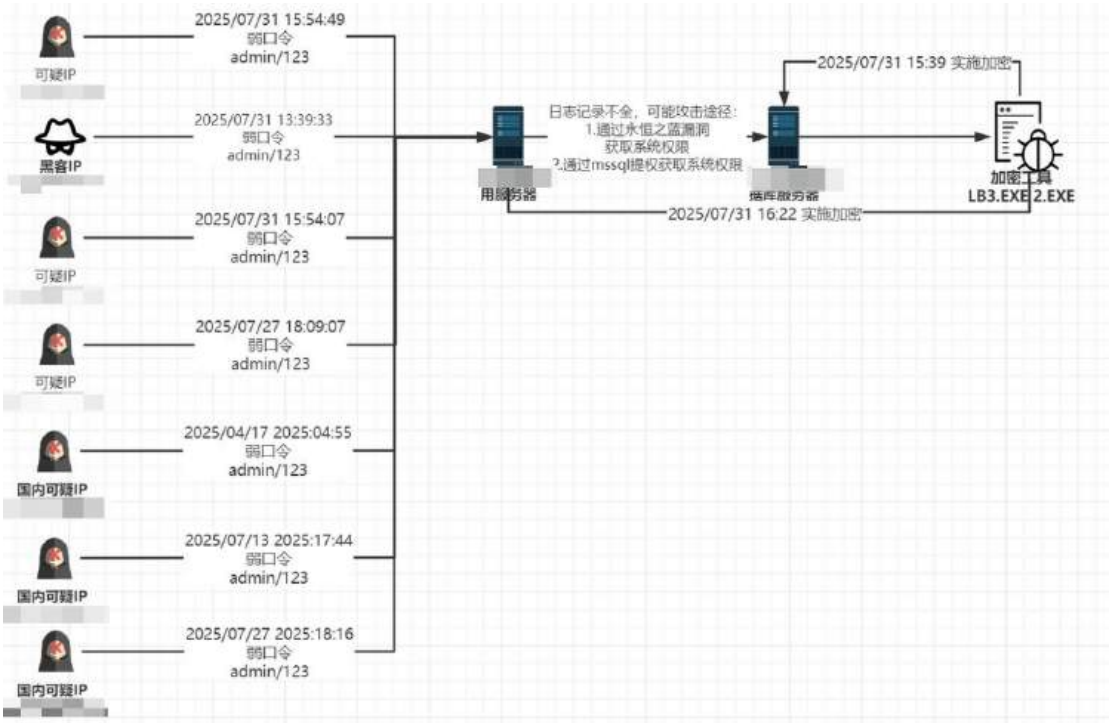


图 127:攻击者攻击路线图

2.漏洞利用攻击

2.1 某财务系统存在 SQL 注入和 RCE 漏洞

2025/4/5 17:44:10-2025/4/5 17:44:19 攻击者利用 keyEdit.aspx 接口存在的 sql 注入漏洞。

图 128 :攻击者利用 sql 注入漏洞

攻击者首先修改 SQL Server 配置，启用高级选项并激活 OLE 自动化过程（如 sp_oacreate），为后续利用对象自动化功能执行系统命令铺平道路。随后，攻击者通过 wscript.shell 组件执行恶意命令，并尝试利用 SQL PowerShell（sqlps）运行 IEX（Invoke-Expression），从远程服务器（http://107.149.xxx.xxx:8000/new）下载并执行恶意脚本。这一系列操作旨在绕过安全限制，获取系统控制权，最终实现远程代码执行（RCE）。

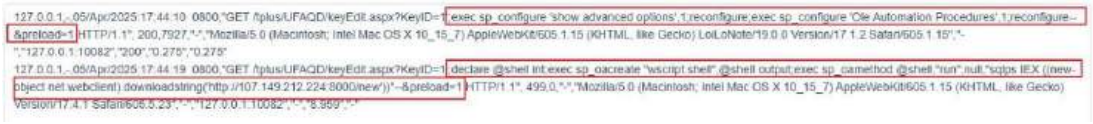


图 129 :攻击者执行的 sql 语句

由于应用是通过某代理软件映射到公网，通过某代理软件日志查询攻击者 ip 为 101.42.xxx.xxx

图 130: 某代理软件日志 ip

通过该 ip 进行查询，发现攻击者第一次访问时间为 2025/04/05 16:54:01，最后一次访问时间为 2025/04/07 10:39:20.

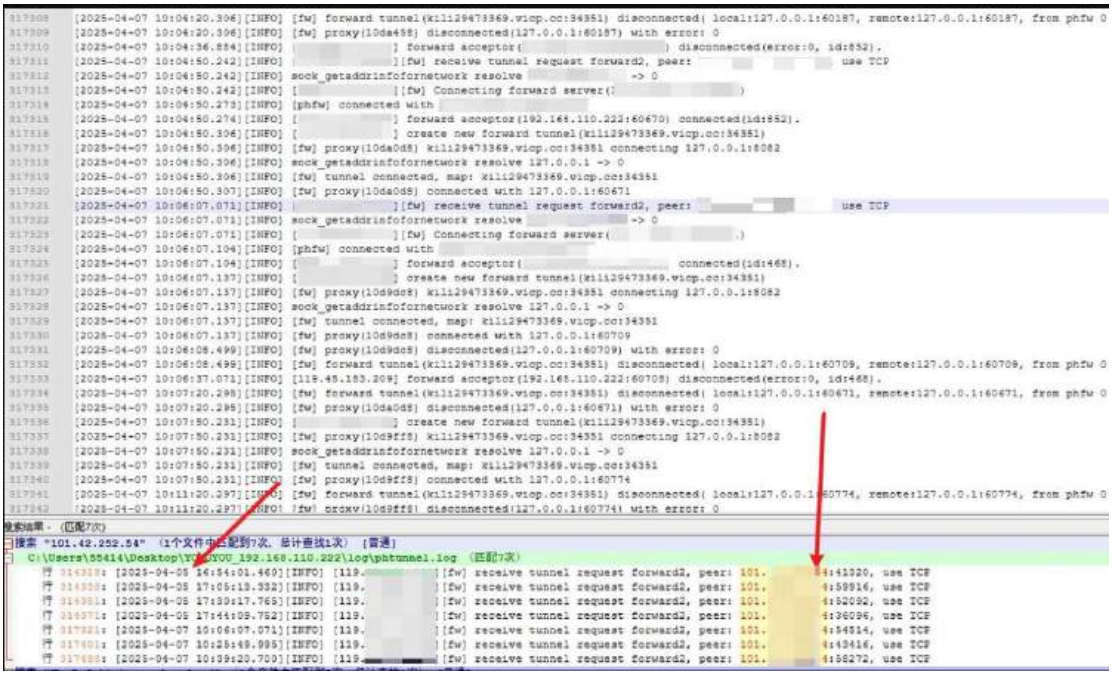


图 131 :攻击者访问某财务系统时间

2025/4/7 10:06:42 攻击者疑似利用 sysftprm.sys 驱动漏洞提权被拦截。

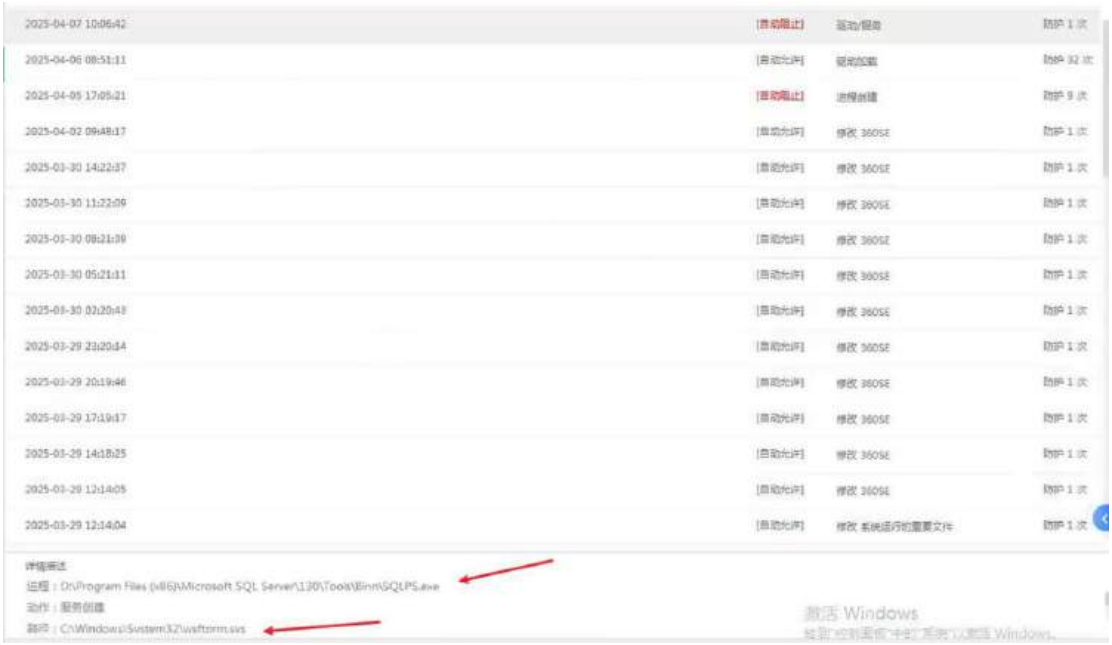


图 132: 360 拦截记录

2025/4/7 10:06:56 攻击者开始加密并清除 Windows 日志。

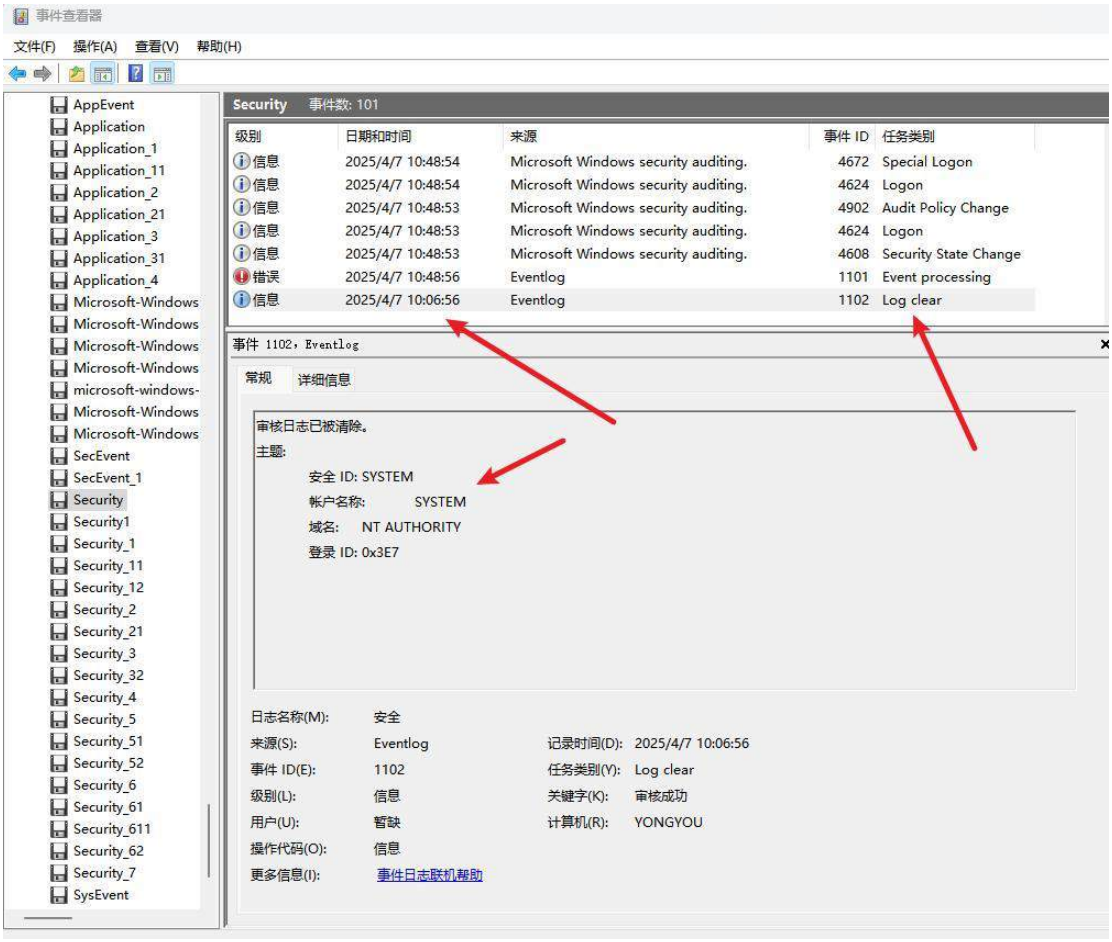


图 133: Windows 日志被清除

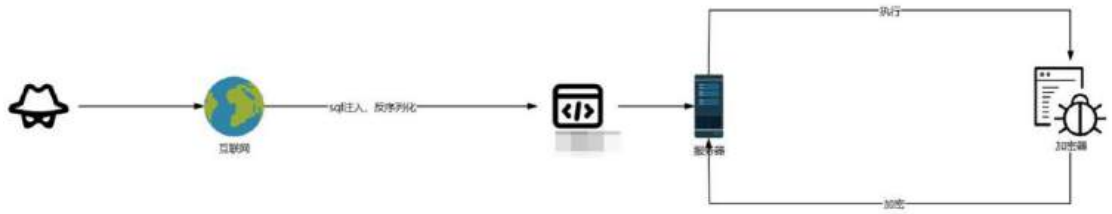


图 134:攻击者攻击路径图

2.2 财务系统存在高危漏洞案例

服务器被植入勒索软件，文件被加密，加密文件的后缀为.roxaew，根据勒索界面和加密后缀判断该勒索软件为病毒家族 Weaxor 的变种病毒。本次中勒索软件的有一台主机，下面会逐一进行分析

1. 通过攻击者加密时间分析，攻击是在 2025 年 9 月 24 日 14:31 分开始，9 月 24 日 15:21 分结束，共加密时长约 1 小时左右

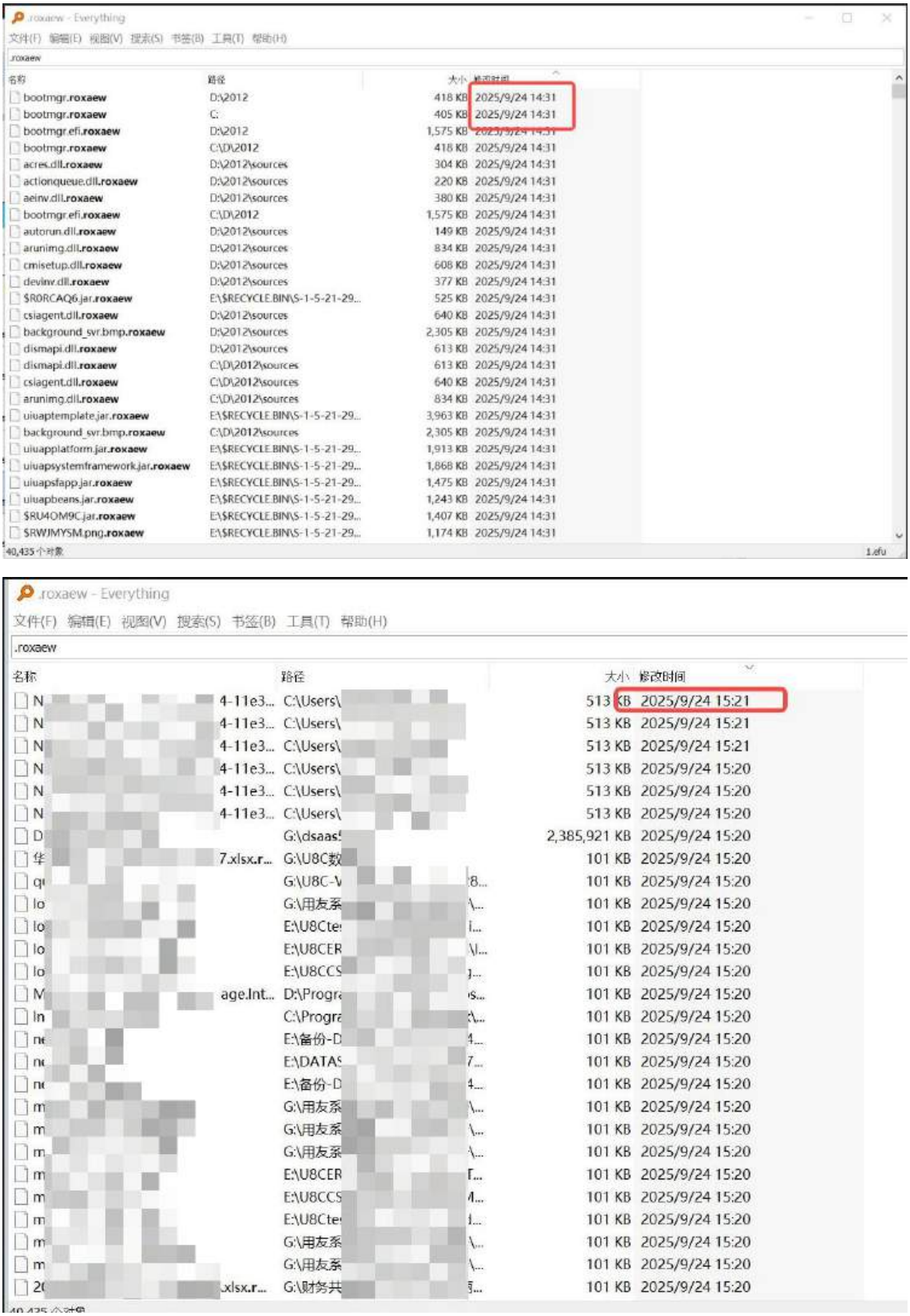


图 135: 加密时间记录

2.基于 AppCompatCache 运行日志可定位攻击者 2025 年 9 月 24 日 14:31 分执行了加密器 tLTSWDS.exe

图 136: 执行加密器记录

3.根据 Application.evtx 日志可确认在加密期间攻击者针对数据库进行 8 次爆破操作，均爆破失败

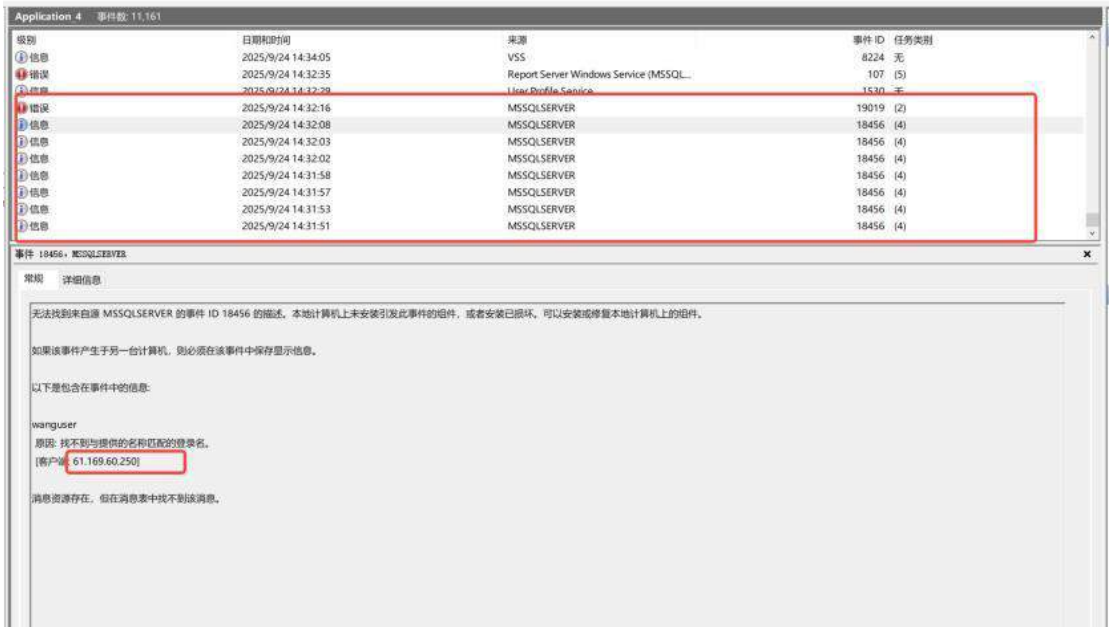


图 137: 数据库爆破失败记录

4.由于 MSSQLSERVER 在初始配置时未开启成功日志记录，导致无法获取更多可用于佐证的信息

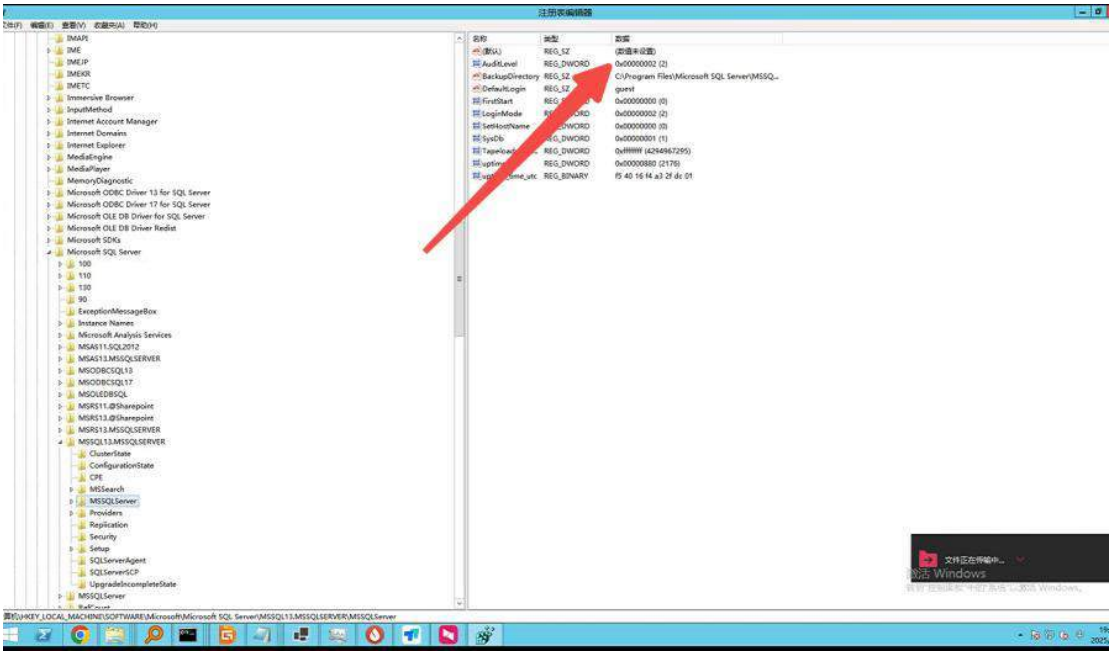


图 138: 开启成功日志记录

5.Security.evtx 日志和 System.evtx 日志攻击者在加密时已经清除了操作日志，故无法获取更多加密前的行为

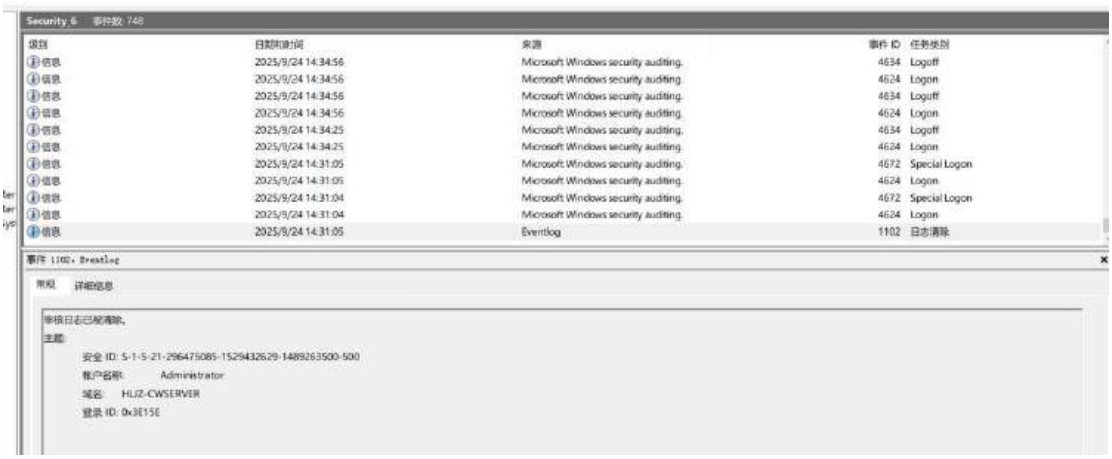


图 139: 清除日志记录

6.在分析加密后日志时，2025/9/24 14:34:25 发现 IP 192.168.xxx.xxx 有匿名登录请求， 表示远端主机（源 IP 192.168.xxx.xxx）对目标机器的网络服务（如 SMB、RPC、NetBIOS） 发起了匿名/空会话连接

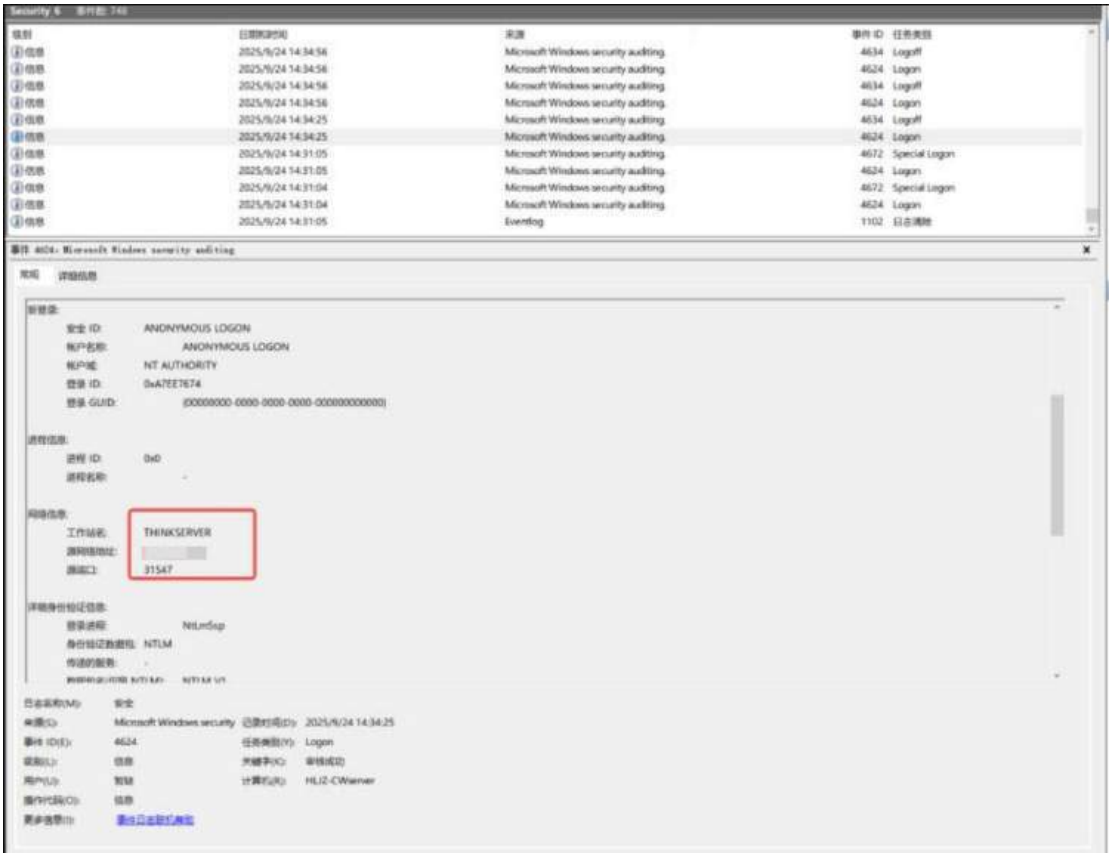


图 140: 发起了匿名/空会话连接记录

7.日志显示：2025/9/24 14:42:24 名为 HLxxxx31218 的电脑，使用本地内置管理员账号（Administrator）通过网络成功登录到了 HLJZ-CWxxxxER 这台服务器

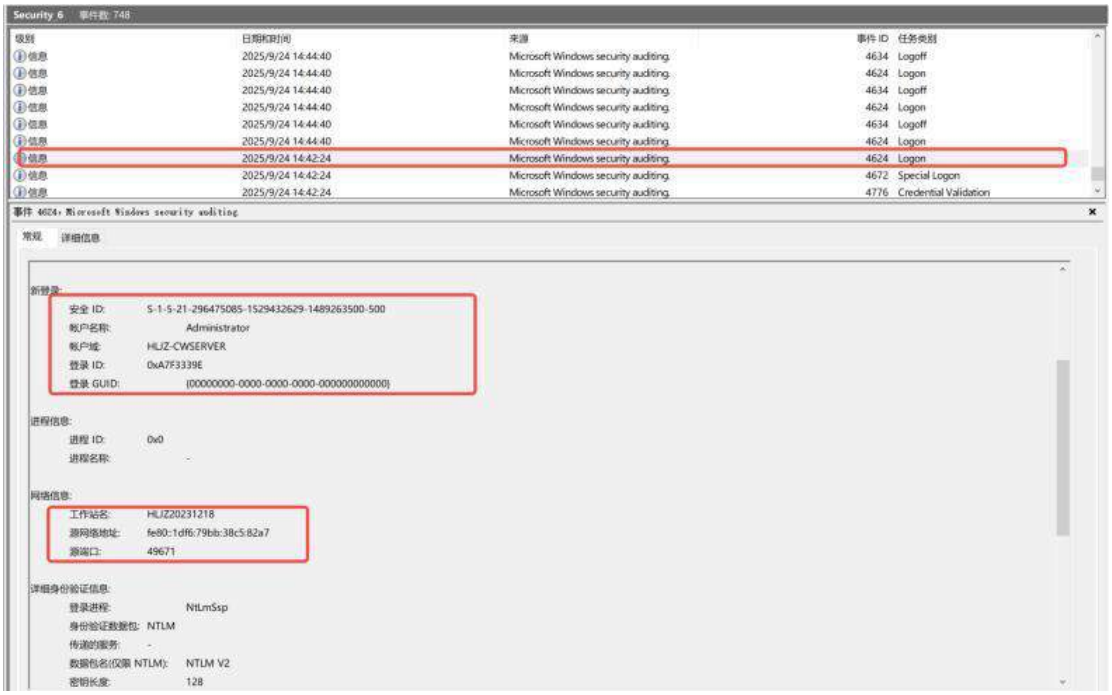


图 141: 成功登陆记录

8.日志显示 JAMESPC 用 Guest 账号在你机器上做了身份验证，并且成功了。后续我们排查时发现该账号确属开启状态，并及时关闭

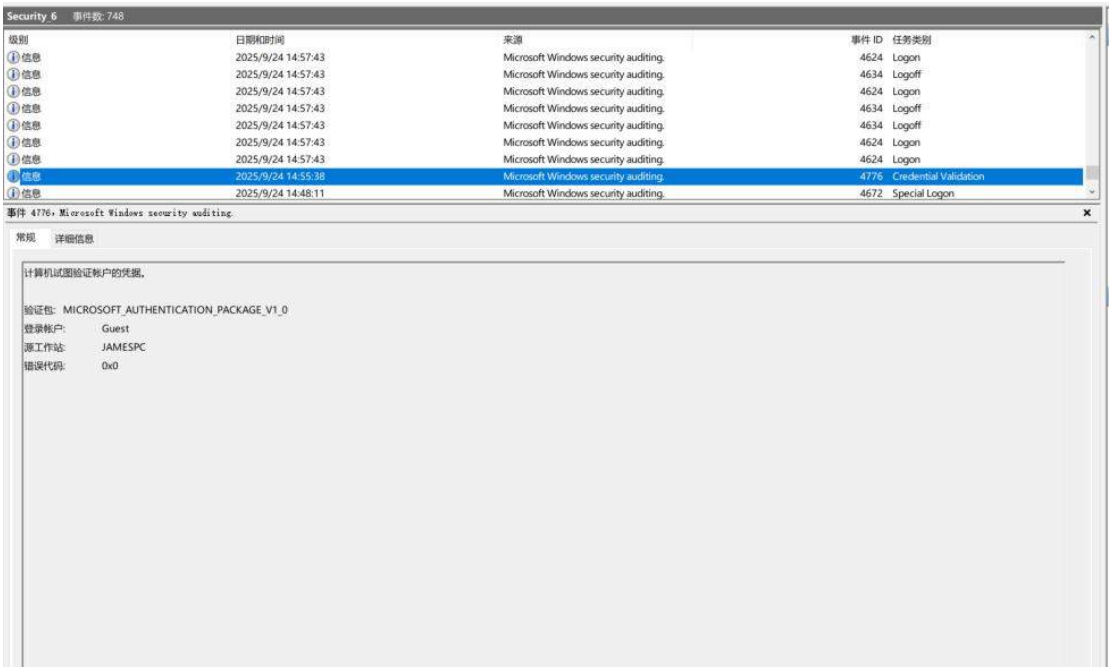


图 142: Guest 账号开启记录

9.数据恢复完成后，未检索到财务系统的 Web 日志记录，疑似系统未启用相关日志功能， 或日志已被攻击者删除以规避溯源

am-log.log	2024/7/3 15:35	文本文档	0 KB
am-log[0].log	2024/7/5 14:22	文本文档	0 KB
anony-log.log	2024/7/3 15:35	文本文档	0 KB
anony-log[0].log	2024/7/6 23:45	文本文档	23 KB
archive.log	2024/7/3 15:35	文本文档	0 KB
archive[0].log	2024/7/5 14:22	文本文档	0 KB
codesync-log.log	2024/7/3 15:35	文本文档	0 KB
codesync-log[0].log	2024/7/5 14:22	文本文档	0 KB
ebank-ly.log	2024/7/3 15:35	文本文档	0 KB
ebank-ly[0].log	2024/7/5 14:22	文本文档	0 KB
FILE RECOVERY.txt	2025/9/24 14:37	文本文档	1 KB
fw-log.log	2024/7/3 15:35	文本文档	0 KB
fw-log[0].log	2024/7/7 18:54	文本文档	22 KB
iufo-log.log	2024/7/3 15:35	文本文档	0 KB
iufo-log[0].log	2025/9/27 10:38	文本文档	380 KB
iufo-repcalc.log	2024/7/3 15:35	文本文档	0 KB
iufo-repcalc[0].log	2024/7/5 14:22	文本文档	0 KB
iufo-repcalcrs.log	2024/7/3 15:35	文本文档	0 KB
iufo-repcalcrs[0].log	2024/7/5 14:22	文本文档	0 KB

图 143: Web 日志没开启记录

10.结合我们针对该勒索家族的多次溯源经验，攻击途径高度疑似来源于财务系统的历史漏洞，或数据库端口直接映射至公网而遭到利用。客户联系厂商进行漏洞自检后，确认确实存在多个漏洞未修复，厂商目前对存在漏洞进行修复补丁操作；

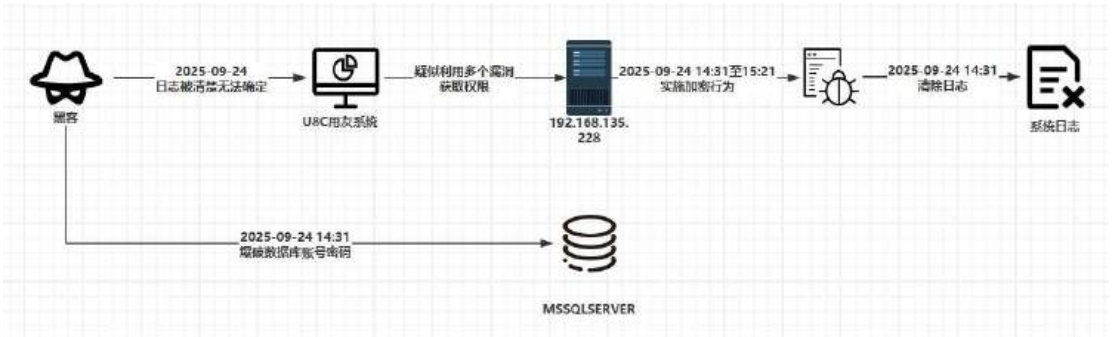


图 144:攻击者攻击路线图

3.横向渗透与权限扩散攻击

3.1 内网扩散导致多台服务器被加密

由于日志缺失，无法确定攻击者获取该服务器 administrator 密码的手段，通过 192.168.xxx.xxx 映射在公网，推测攻击者通过公网爆破 192.168.xxx.xxx RDP 获取入口点。

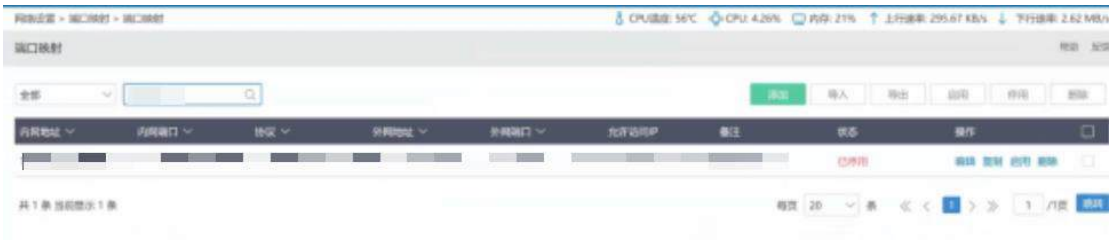


图 145: iKuai 端口映射图

2025/07/26/6:35:51.793 攻击者使用 **5.182.xxx.xxx** 使用 administrator 账户登录 192.168.xxx.xxx 。

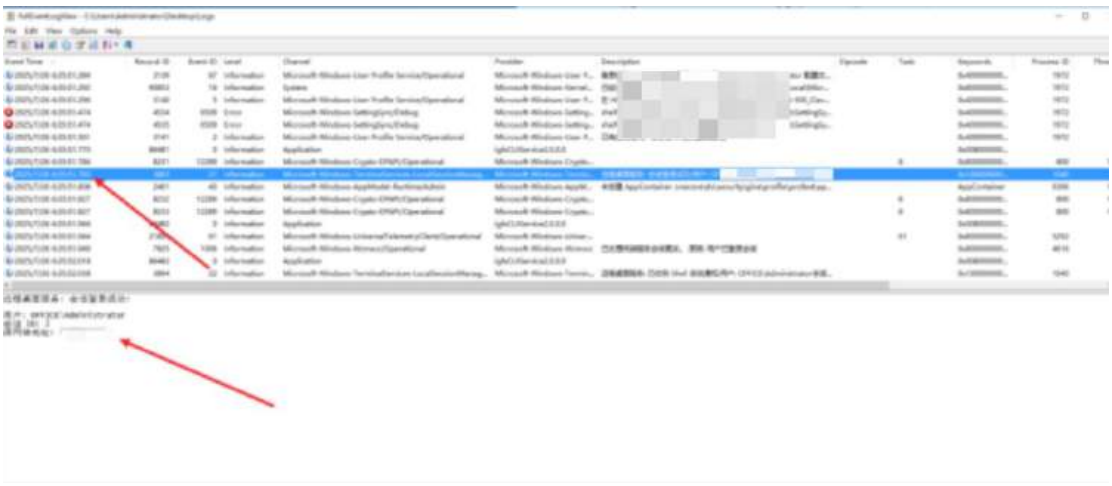


图 146: 5.182.xxx.xxx 连接 ZHXXXZH-PC 192.168.xxx.xxx

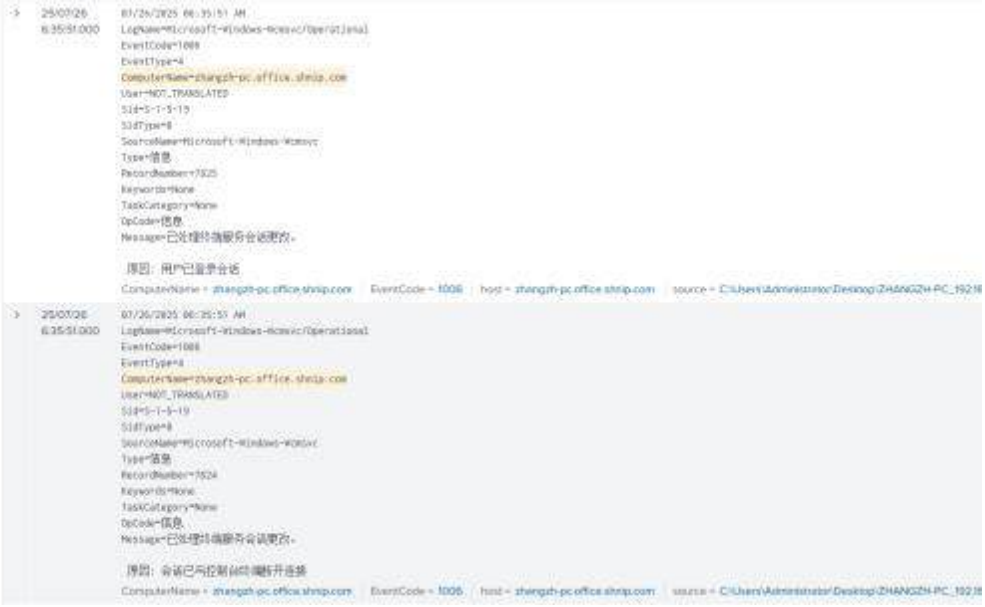


图 147: 攻击者使用 administrator 账号登录 192.168.xxx.xxx

通过 rdp 缓存，拼凑出攻击者首次登录 192.168.xxx.xxx 的 rdp 图像。

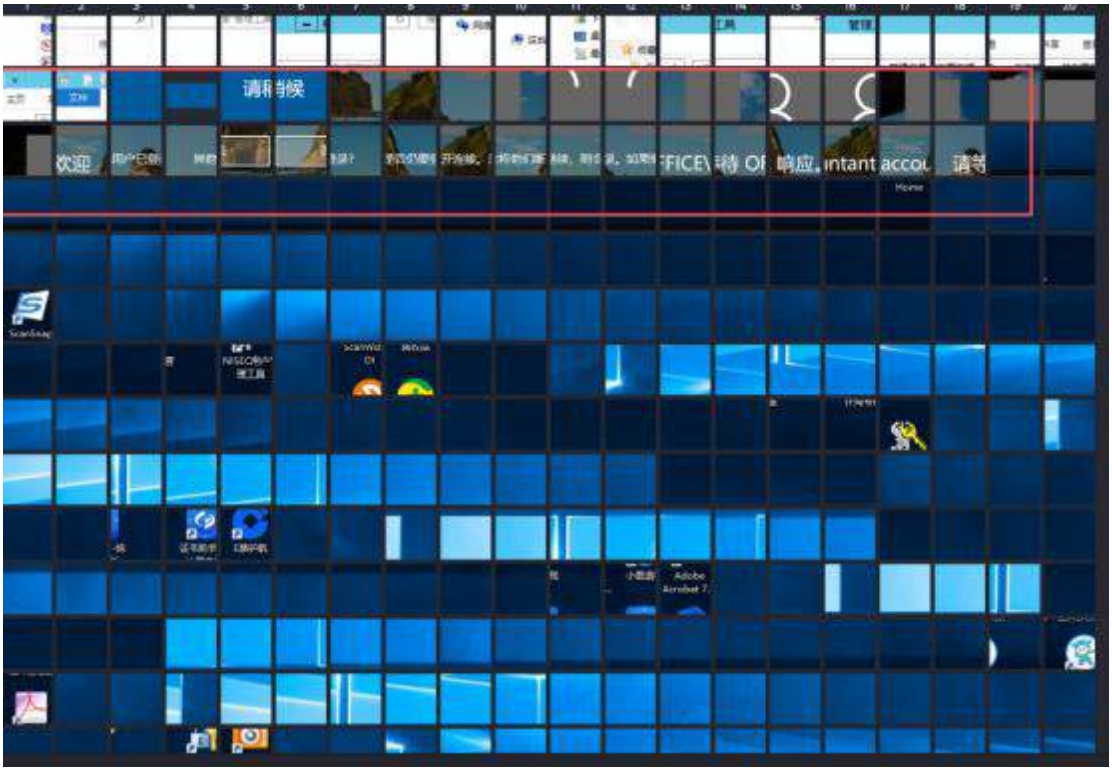


图 148: rdp 缓存图像

2025/07/26 6:38:52.000 攻击者上传 advanced_port_scanner 到 192.168.xxx.xxx。

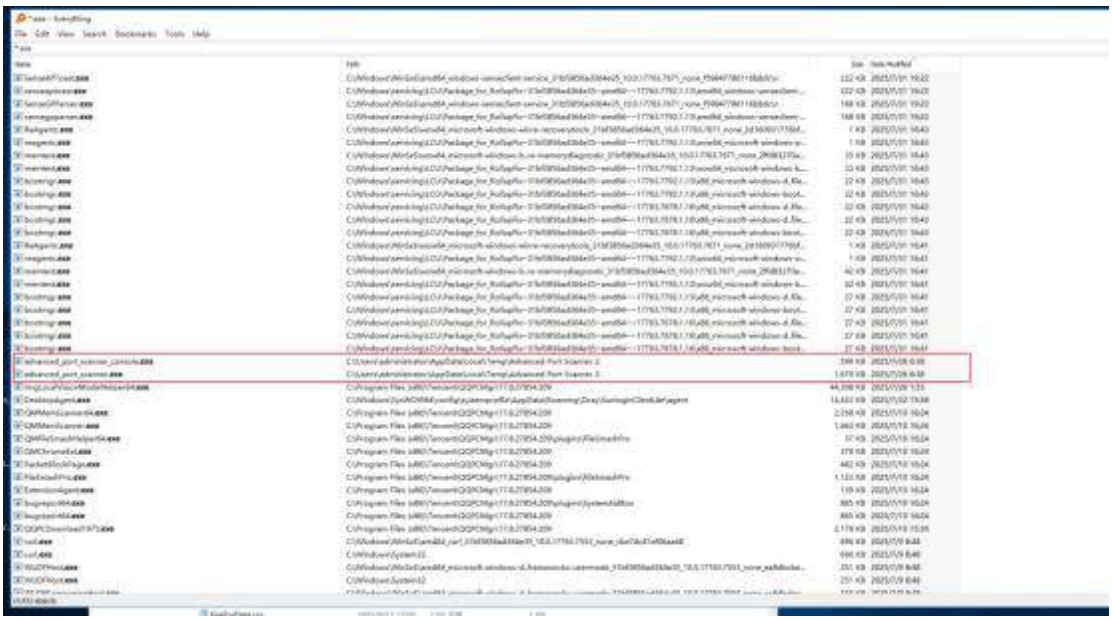


图 149: advanced_port_scanner 落地时间

2025/07/26 6:55:54.000(UTC+8) ZHANGZH-PC_192.168.xxx.xxx 执行 netscan 以及 advanced_port_scanner 扫描器

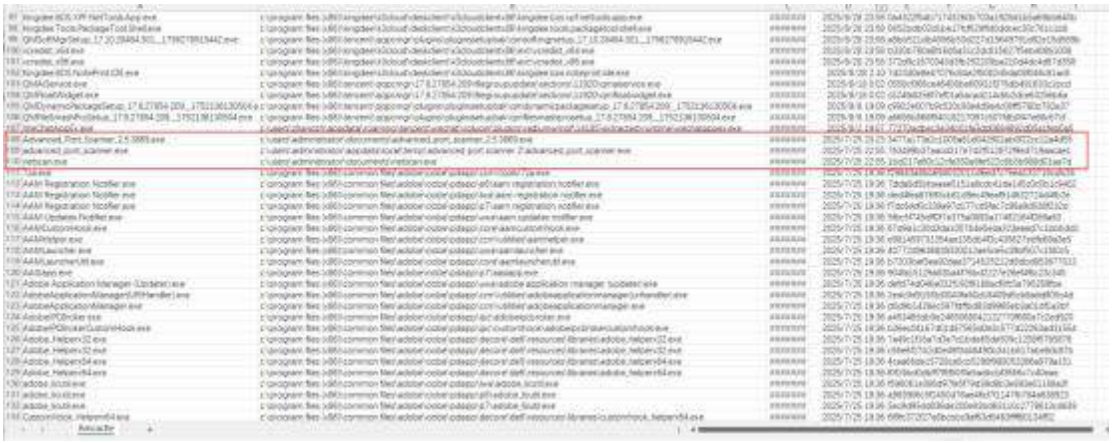


图 150: 攻击者工具运行时间

2025/07/26 6:38:31.000- 25/07/26 7:11:02.000 ZHANGZH-PC 192.168.xxx.xxx 扫描内网对存活 smb445 端口进行扫描。

图 151: 192.168.xxx.xxx7 第一次 smb 扫描开始

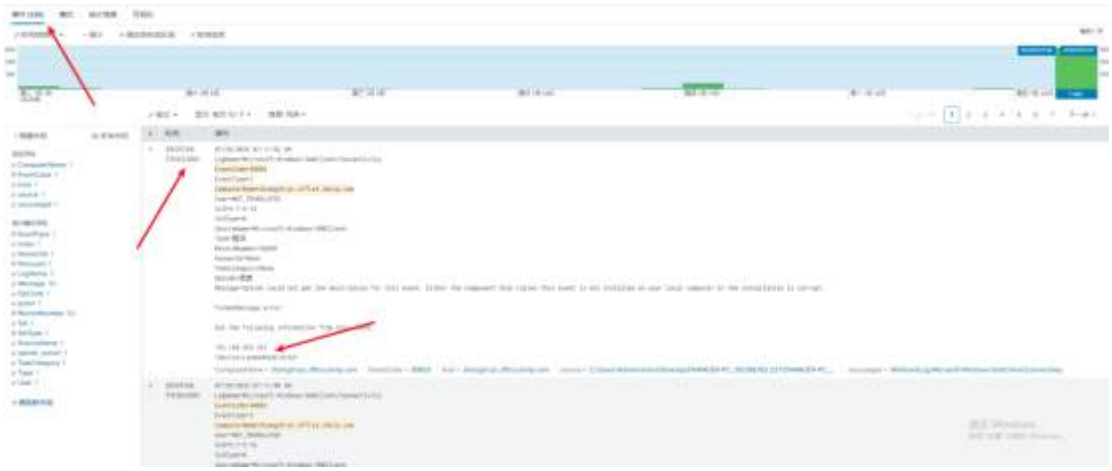


图 152: 192.168.xxx.xxx7 第一次 smb 扫描结束

2025/07/26 6:39:58.000-2025/07/26 6:55:30.000（UTC+8） 攻击者通过 mstsc 连接 192.168.xxx.xxx、192.168.xxx.xxx、192.168.xxx.xxx 等内网 IP

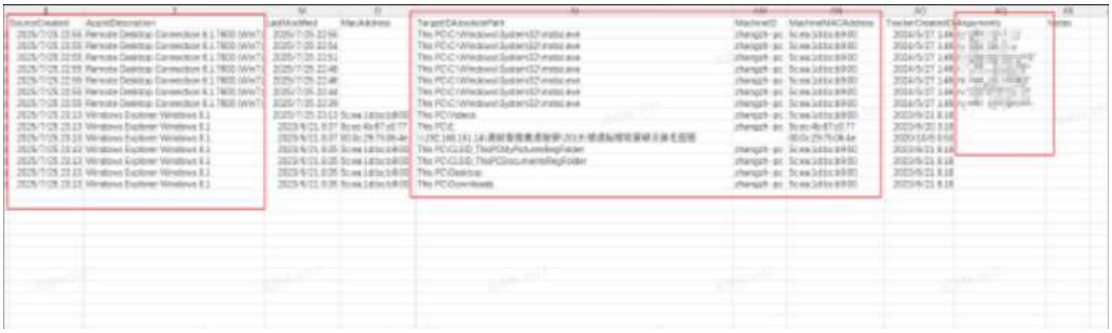


图 153: 192.168.xxx.xxx 远程连接多个 IP（图中时间为 UTC+0）

2025/07/26 6:54:13.000 攻击者通过 192.168.xxx.xxx 对 SHBAK01 192.168.xxx.xxx 进行爆破。

图 154: 192.168.xxx.xxx7 对 SHBAK01 192.168.xxx.xxx 进行爆破

2025/07/31 18:50:42.000 -2025/08/02 2:44:08.000 攻击者使用已获得权限的主机对域内主机进行 smb 爆破。

图 155：此次 smb 爆破最早时间

图 156： 此次 smb 爆破最晚时间

经统计，推测于 2025/08/02 2:44:08.000 之前，图中涉及的服务器可能均已沦陷。

图 157：对内网进行 smb 爆破的主机

2025/08/04 18:41:17.000 攻击者第一次通过 213.171.xxx.xxx 使用 administrator 账户连接 192.168.xxx.xxx，由于日志缺失，无法得知攻击者如何获取 192.168.xxx.xxx 权限，通过该 ip 曾映射 rdp 到公网，推测为攻击者通过公网 rdp 爆破获取该主机权限。

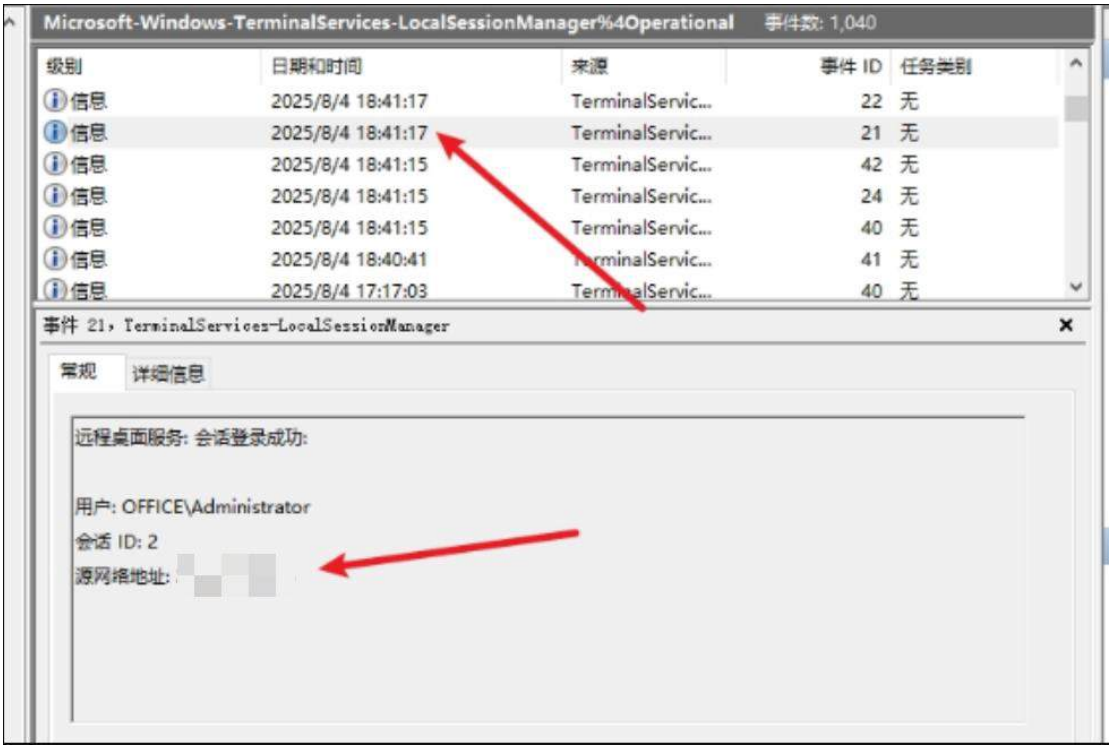


图 158: 213.171.xxx.xxx 连接 192.168.xxx.xxx

2025/08/04 18:41:17.000-2025/08/04 19:59:05.000 攻击者将工具上传到 192.168.xxx.xxx，其中包含了凭据窃取工具 64.exe（原名为 mimikatz）、LostMyPassword.exe，远程执行工具 PsExec.exe，端口扫描与服务发现工具 Advanced_Port_Scanner_2.5.3869 以及后门 + 隧道工具 windefender_538.exe。

图 159: 攻击者于 192.168.xxx.xxx 上传的攻击者工具

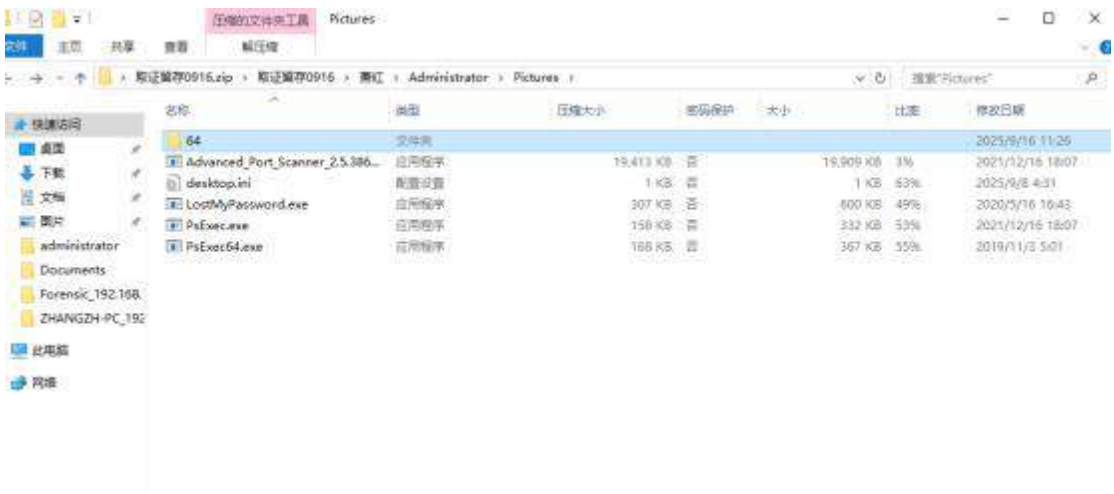


图 160: 攻击者于 192.168.xxx.xxx 上传的攻击者工具

2025/08/04 19:59:05.000 攻击者切换 213.252.xxx.xxx 使用 administrator 账户再次 rdp 连接 192.168.xxx.xxx。

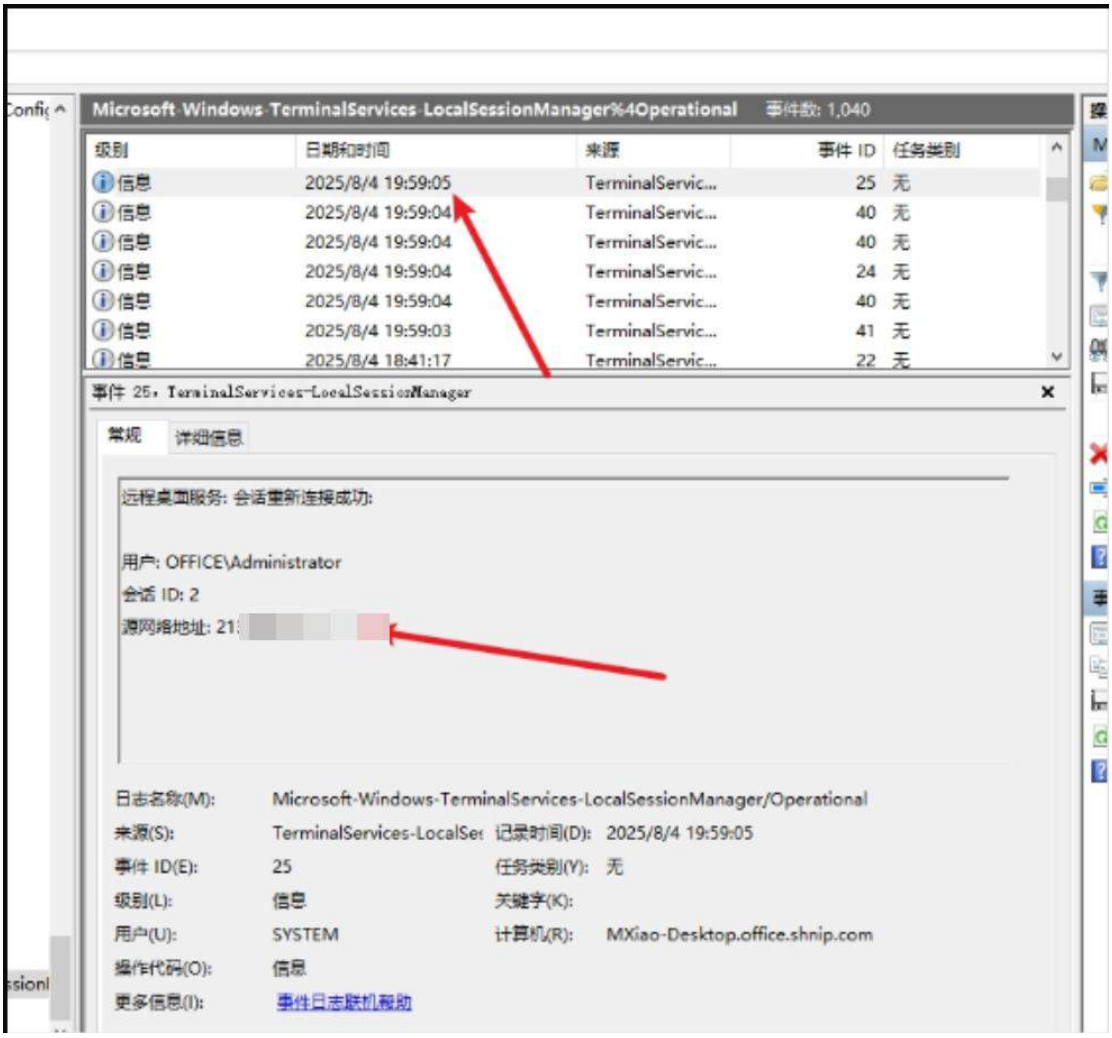


图 161: 213.252.247.140 连接 192.168.xxx.xxx

2025/08/04 19:16:51.000-2025/08/04 21:32:34.000 192.168.xxx.xxx 对 192.168.xxx.xxx 持续爆破。

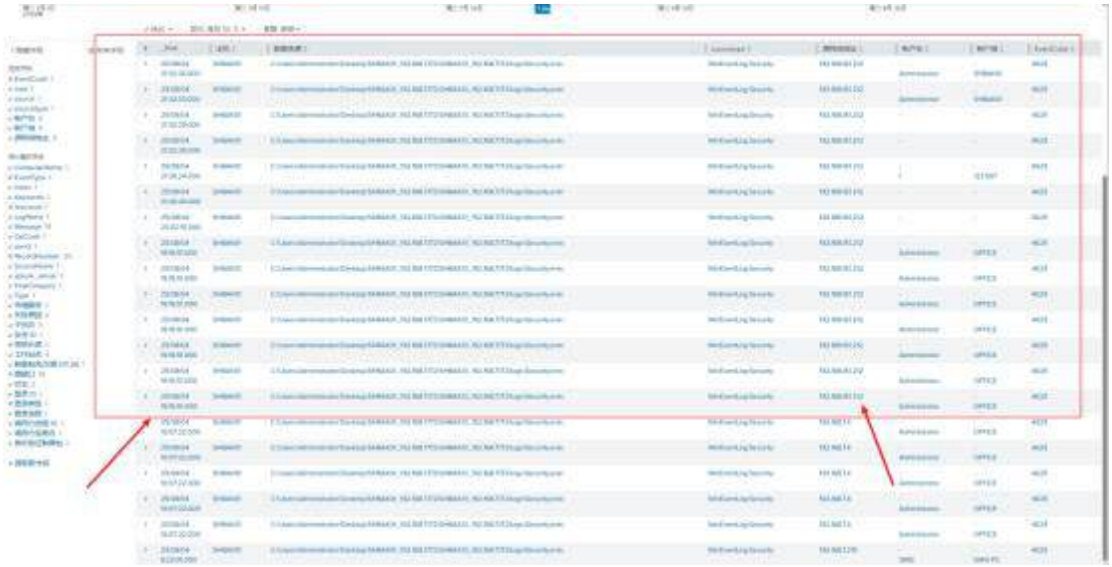


图 162: 192.168.xxx.xxx 对 192.168.xxx.xxx 持续爆破

2025/08/04 20:00:00.000 攻击者在 192.168.xxx.xxx 主机上运行了 advanced_port_scanner_2.5.3869.exe 以及 windefender_538.exe

windefender_538.exe 为攻击者规避安全软件并部署代理隧道的工具，通过 cmd.exe（执行了位于临时目录的批处理文件，并启动了 reg.exe 写入 LocalAccountTokenFilterPolicy=1（提升/放宽本地账户令牌过滤），随后通过 sc.exe 创建并启动名为 kernels 的服务，该服务以 cmd.exe 启动 frpc.exe 并加载 win.toml。

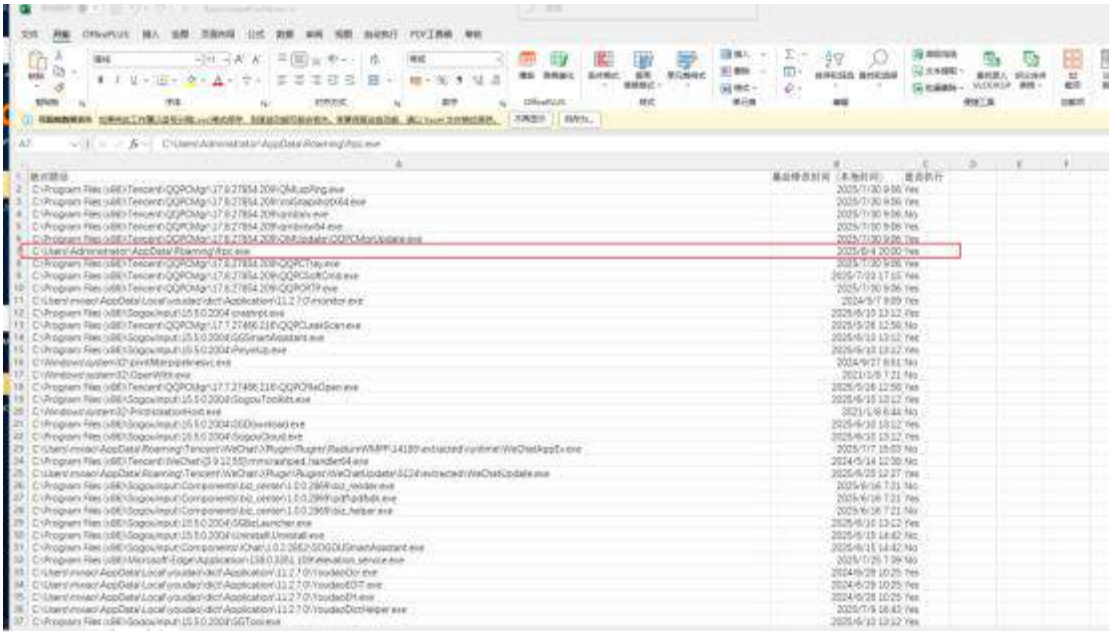


图 163: 攻击者运行代理工具 frpc.exe

图 164: windefender_538.exe 进程链

其中 Win.toml 为 frp 配置文件，指向攻击者服务器 91.199.xxx.xxx 的 443 端口，传输协议为 quic

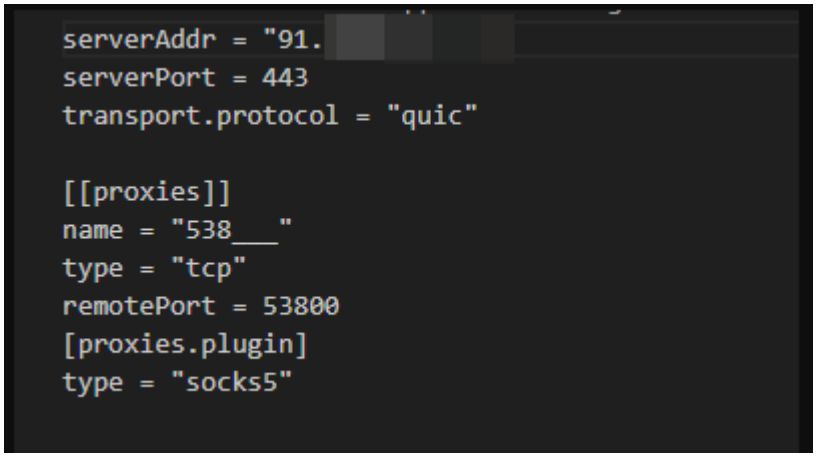


图 165: frp 配置文件 Win.toml

2025/08/05 1:36:15.000 攻击者在 192.168.xxx.xxx 通过 powershell 加载了一个脚本，该脚本作用是修改 Windows Defender 的运行行为，例如：

1）启用或禁用实时保护、IOAV 保护、脚本扫描等功能。

2）配置扫描计划（Quick Scan / Full Scan）、扫描时间和扫描频率。

3）设置 PUA（Potentially Unwanted Application，潜在不需要程序）保护模式。

4）设置威胁等级的默认处理动作（如高危、低危、未知威胁的处理方式）。

5）配置排除项，包括路径、文件扩展名和进程。

6）设置签名更新策略和行为监控参数。

7）启用或禁用各种 Defender 功能，例如邮件扫描、可移动驱动器扫描、网络文件扫描等。

图 166: 攻击者导入修改 Windows Defender 的 powershell 脚本

2025/08/05 8:15:40.000 由 192.168.xxx.xxx ZHxxxW 第一次登录 SHHRSVROLD 192.168.xxx.xxx。

图 167: 192.168.xxx.xxx 登录 192.168.xxx.xxx

2025/08/05 8:15:40.000 - 25/08/06 14:47:42.000 期间 192.168.xxx.xxx、192.168.xxx.xxx 等内网 IP 均登录过 SHHXXXXXXD。

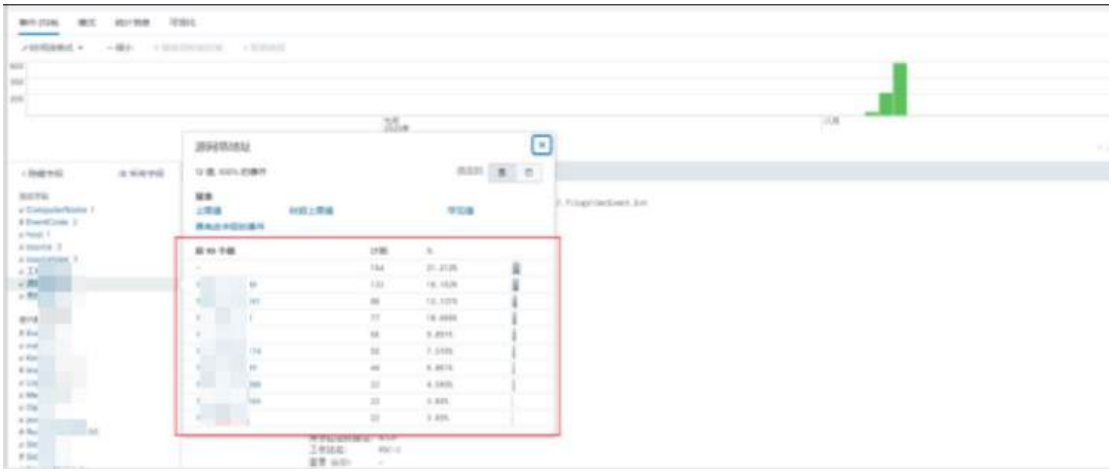


图 168: 登录 IP

2025/08/08 0:14:35.000 由 192.168.xxx.xxx 第一次爆破成功登录 192.168.xxx.xxx。

图 169: 192.168.xxx.xxx 第一次被爆破成功

2025/08/10 21:22:23.000 攻击者从 192.168.xxx.xxx 登录并驻留 SHBAK01 至 2025/09/07 22:58:23.000，EventCode 4624 代表登录，EventCode 4634 代表注销。

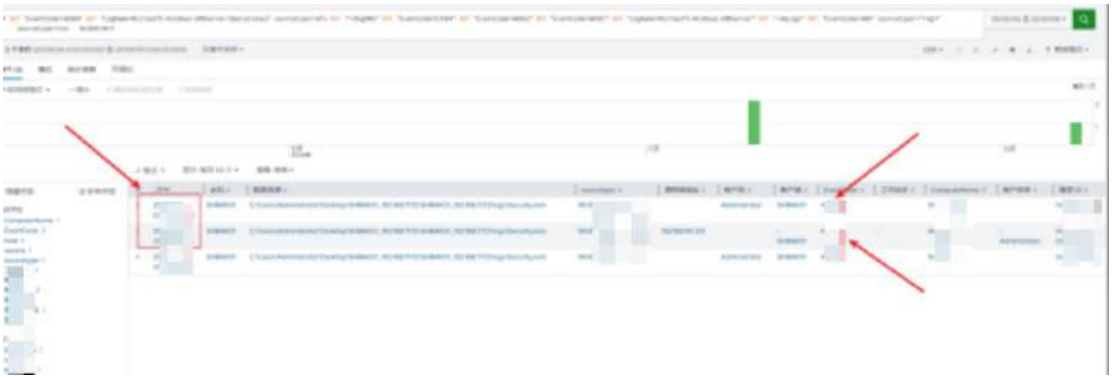


图 170: 192.168.xxx.xxx 远程登录至 192.168.xxx.xxx 驻留长达约 1 个月

2025/08/10 21:22:24.000 通过 powershell 运行一串由 Base64 加密的脚本。

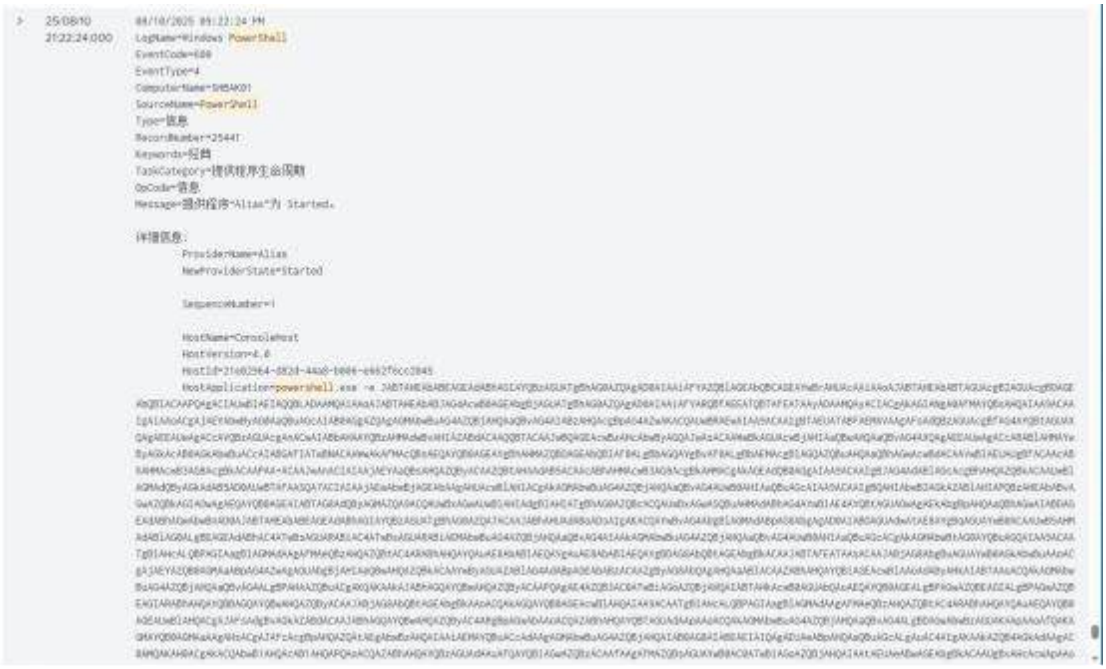


图 171: 攻击者执行 powershell

Base64 解密后，从 Veeam Backup 的 SQL 数据库中读取加密的凭据并解密。

图 172 :攻击者执行的 powershell 具体内容

2025/08/18 10:21:16.000 攻击者从主机 zhxxxgzh-pc 192.168.xxx.xxx 启动了一个远程桌面连接，目标是 192.168.xxx.xxx。

图 173: 攻击者从 192.168.xxx.xxx 连接 192.168.xxx.xx

2025/09/05 4:31:28.000- 25/09/11 4:05:39.000 攻击者在每天凌晨 4 点多通过 wmi 在 192.168.xxx.xxx 上查询该计算机上的安全软件。

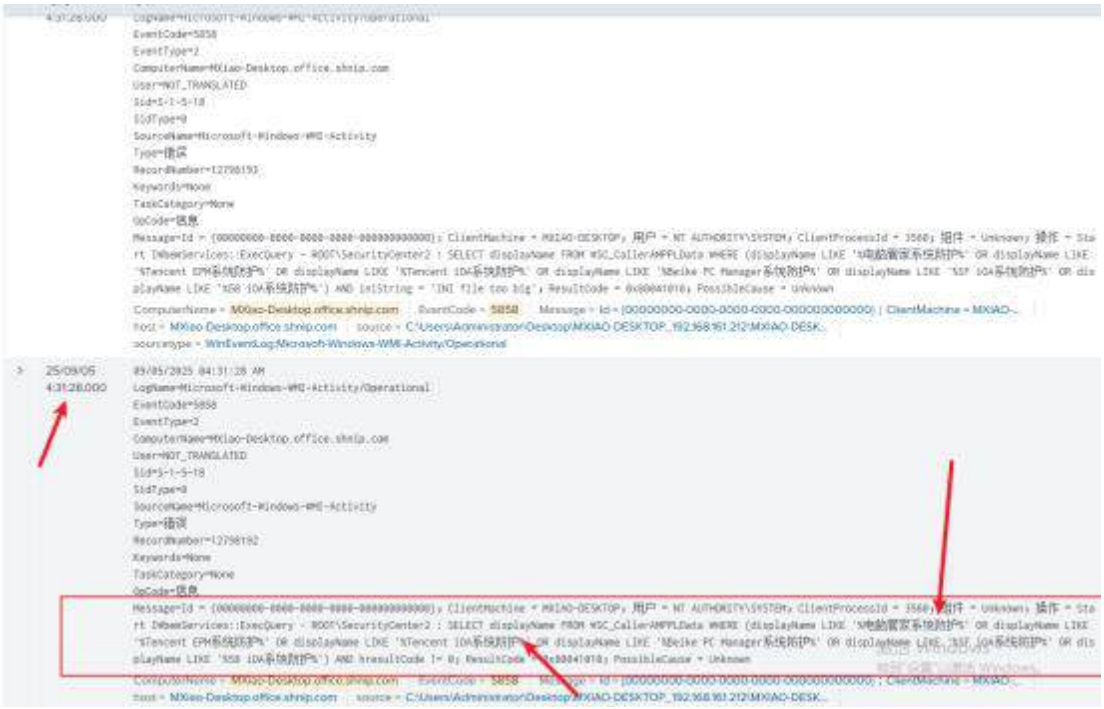


图 174: 攻击者第一次于 192.168.xxx.xxx 通过 WMI 查询主机上的杀软

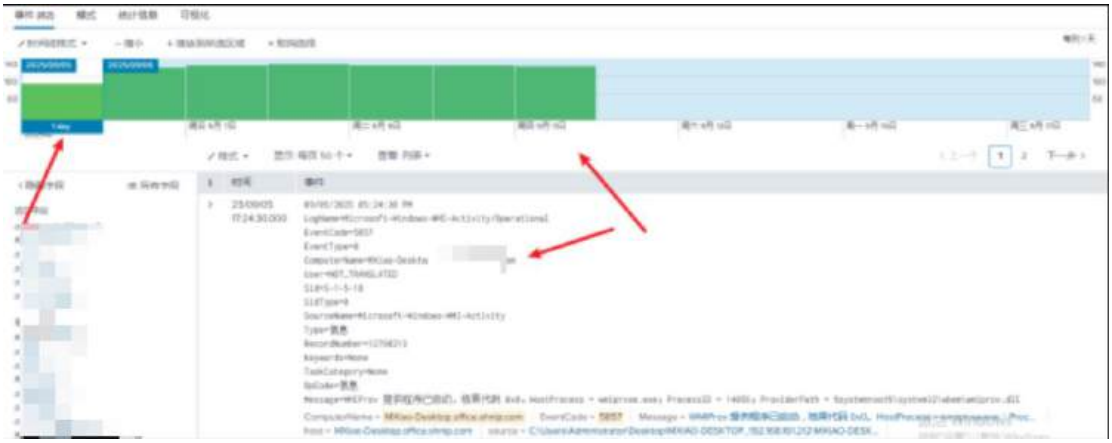


图 175: 查询杀软时间

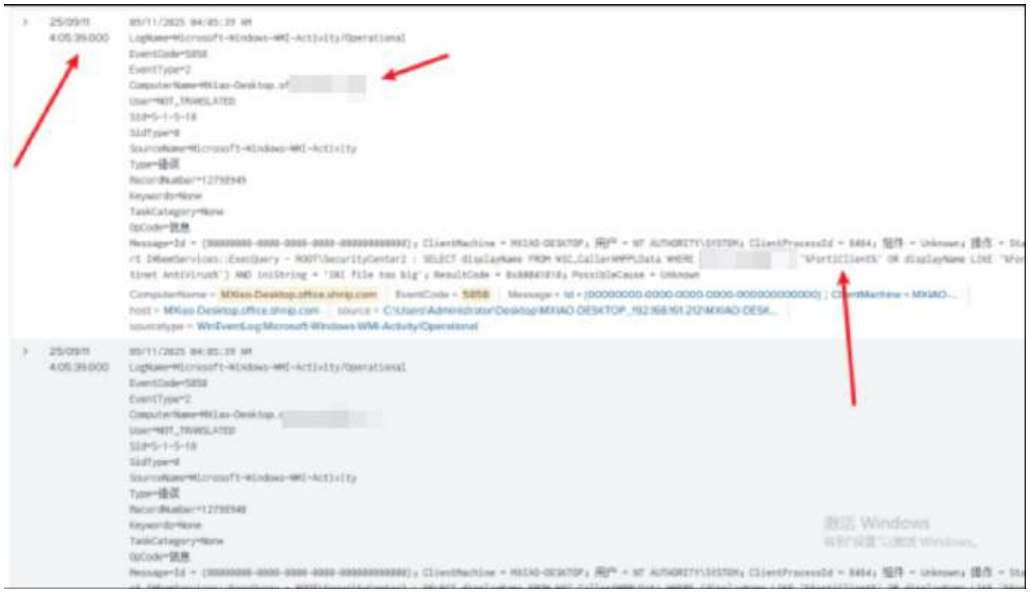


图 176: 攻击者最后一次于 192.168.xxx.xxx 通过 WMI 查询主机上的杀软

2025/09/07 14:57:05.000 192.168.xxx.xxx 通过 web 界面登录 192.168.xxx.xxx。

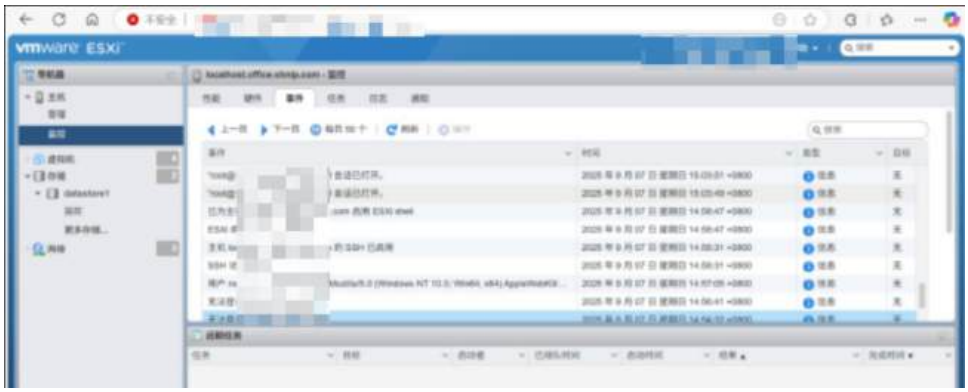


图 177: 加密前攻击者的最后一次登录

2025/09/07 14:59:31.000 通过 192.168.xxx.xxx 登录 192.168.xxx.xxx ESXI 的 ssh。

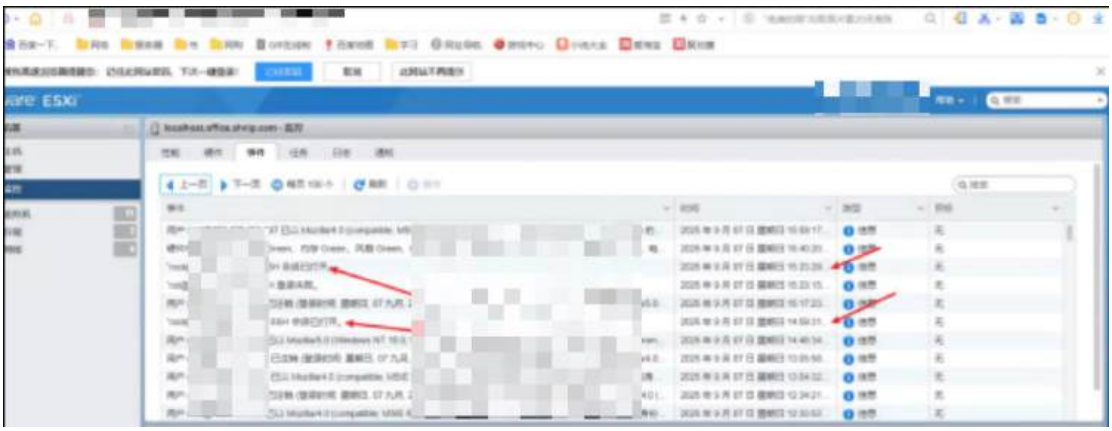


图 178: 加密前攻击者的最后一次登录

2025/09/07 15:03:49.000 从 192.168.xxx.xxx 通过 ssh 连接 192.168.xxx.xxx。

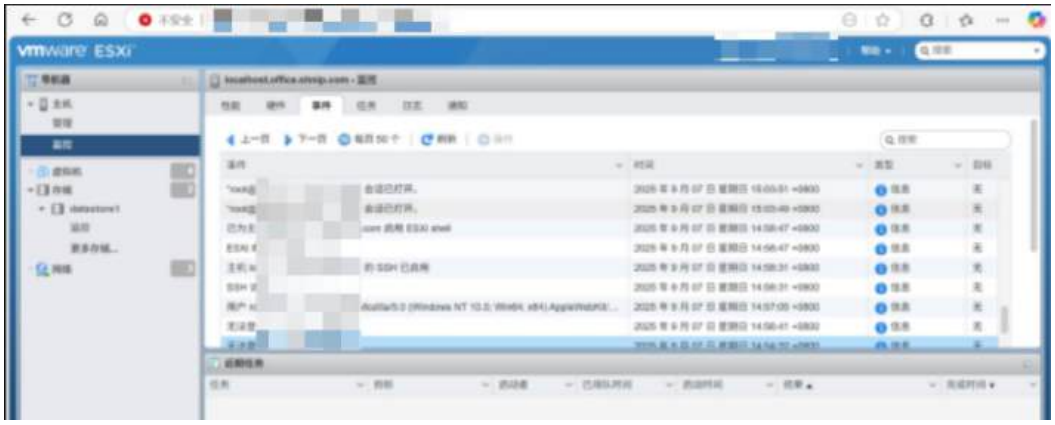


图 179: 加密前攻击者的最后一次登录

2025/09/07 15:07:16.000 192.168.xxx.xxx 通过 ssh 连接 192.168.xxx.xxx。

图 180: 加密前攻击者的最后一次登录

2025/09/07 15:14:57.000 192.168.xxx.xxx 登录 192.168.xxx.xxx ESXI WEB 界面并启用 ssh。

图 181: 加密前攻击者的最后一次登录

2025/09/07 15:23:29.000 通过 192.168.xxx.xxx 登录 192.168.xxx.xxx ESXI 的 ssh。

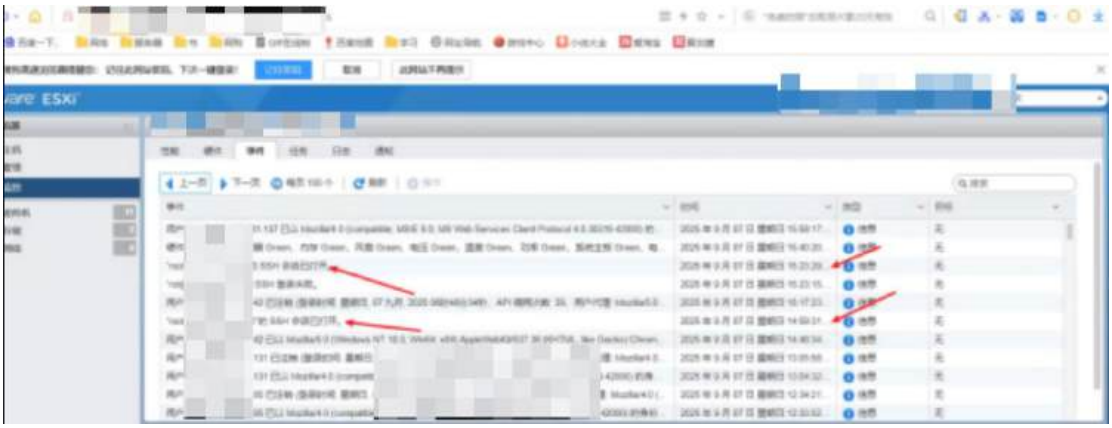


图 182: 加密前攻击者的最后一次登录

2025/09/07 16:15:32.000 攻击者从 192.168.xxx.xxx 使用 administrator 登录 192.168.xxx.xxx Sxxxxx01。

图 183: 加密前攻击者登录

2025/09/07 16:15:34.000 攻击者修改 192.168.xxx.xxx 修改防火墙策略，一次性放开所有配置文件的 RDP，同时 Shadow 功能（远程协助/会话镜像）也被放开，推测攻击者为了方便监控或操作会话。

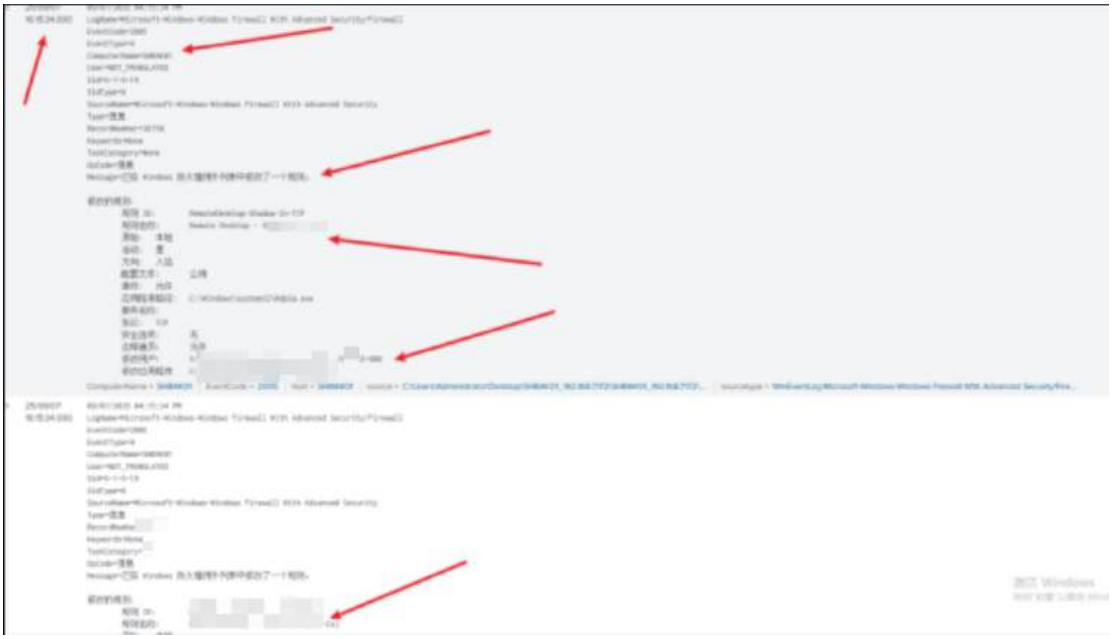


图 184: 防火墙配置修改

2025/09/07 16:19:17.000 攻击者通过 192.168.XXX.XXX 连接 192.168.XXX.XXX。

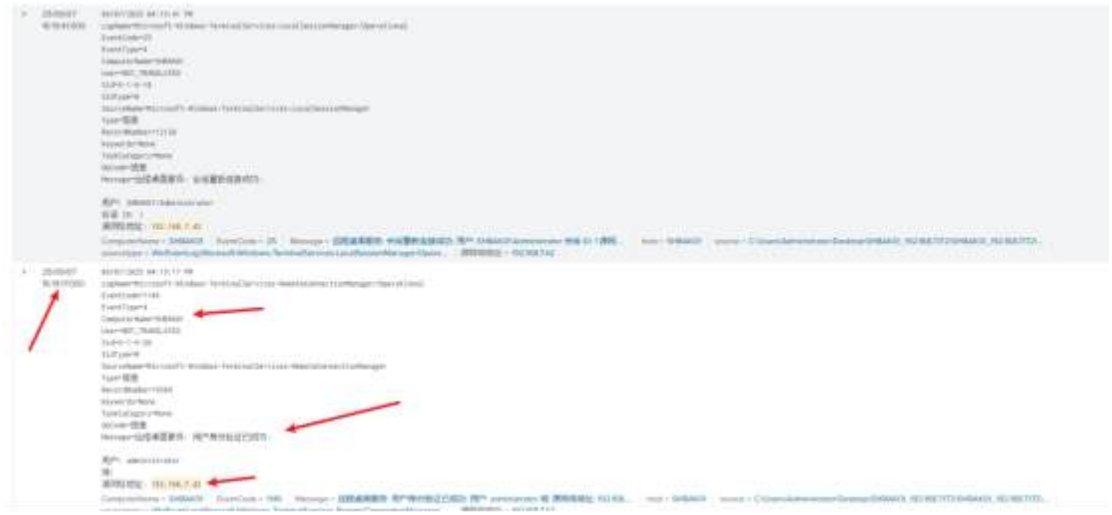


图 185: 攻击者通过 192.168.XXX.XXX 连接 192.168.XXX.XXX

2025/09/07 22:14:46.000 关闭 192.168.XXX.XXX ESXI 上的虚拟机并加密。

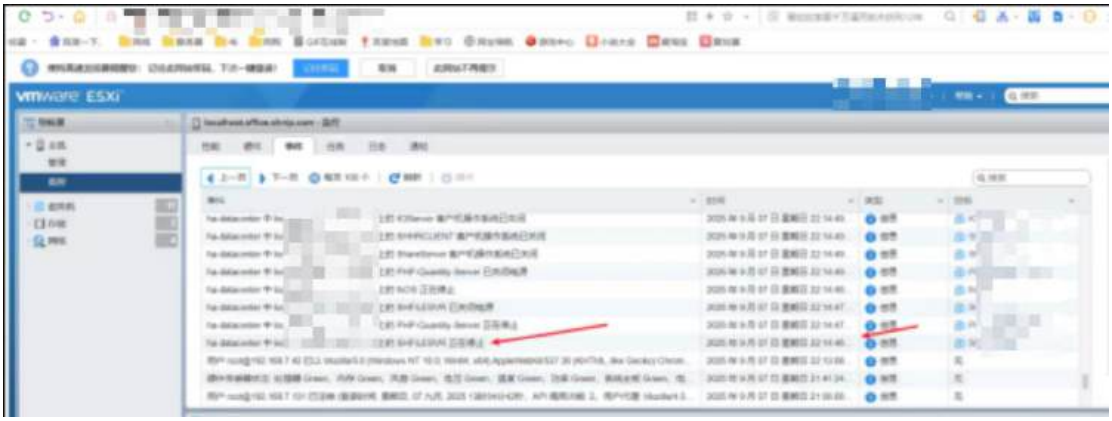


图 186: 加密前攻击者关闭 ESXI 虚拟机

2025/09/07 22:15:30.000 停止 192.168.XXX.XXX 的虚拟机。

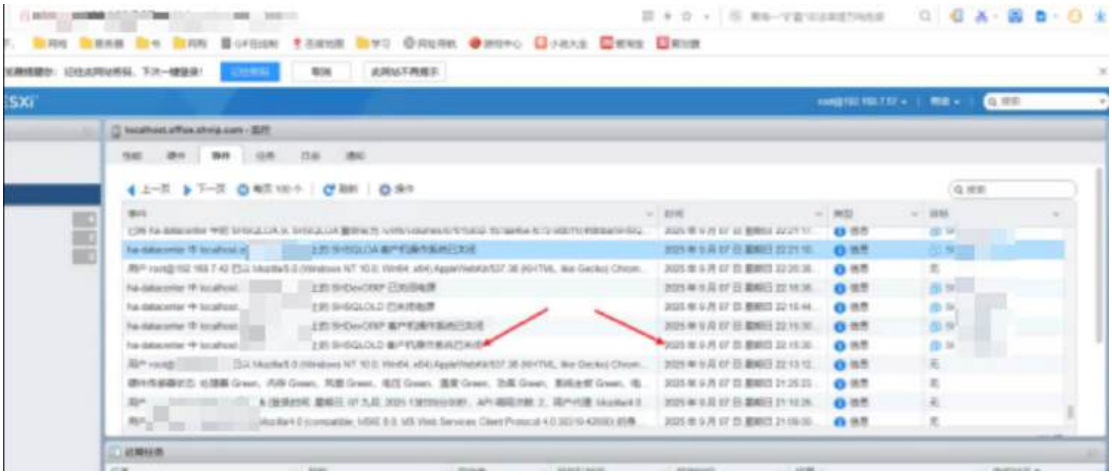


图 187: 加密前攻击者关闭 ESXI 虚拟机

2025/09/07 22:25:08.000 192.168.XXX.XXX 关闭对 192.168.xx.xxssh 连接。

图 188: 加密后攻击者退出 ssh

2025/09/07 22:31:35.000 192.168.7.42 关闭 192.168.XXX.XXX ESXI 上的虚拟机并加密。

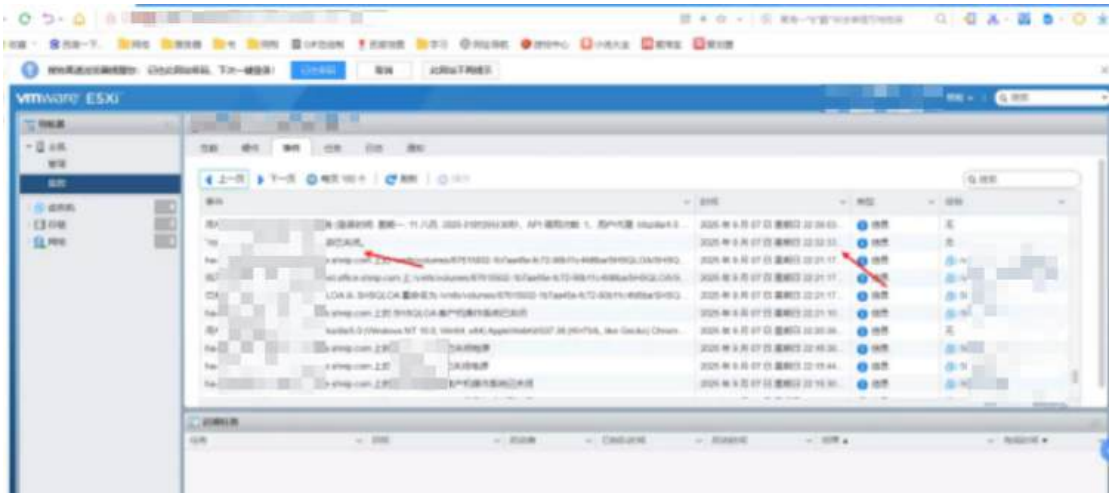


图 189: 加密前攻击者关闭 ESXI 虚拟机

2025/09/07 22:32:33.000 从 192.168.xx.xx 关闭对 192.168.XXX.XXX ssh 连接。

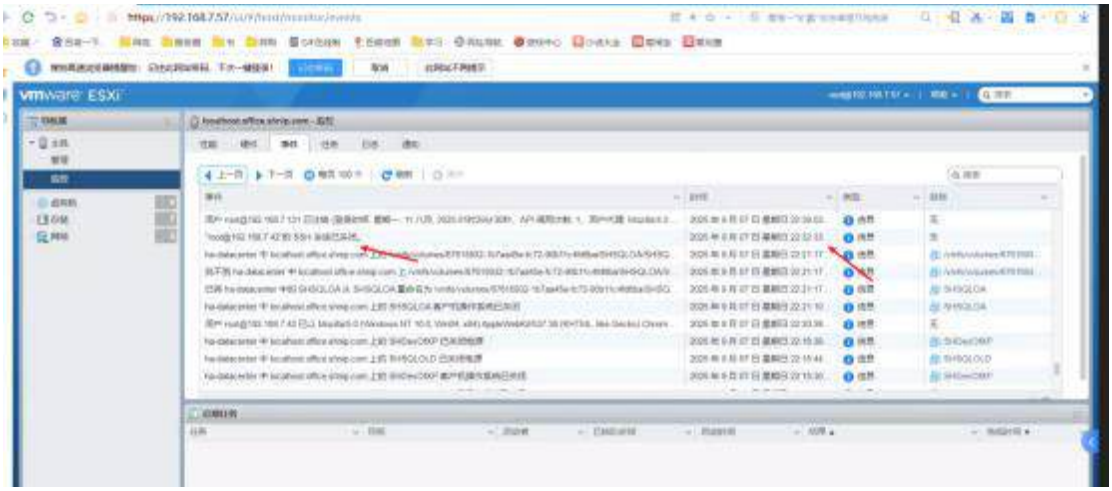


图 190: 加密后攻击者退出 ssh

2025/09/07 22:38:08.000 关闭 192.168.xx.xx 上的 xxxClient 虚拟机。

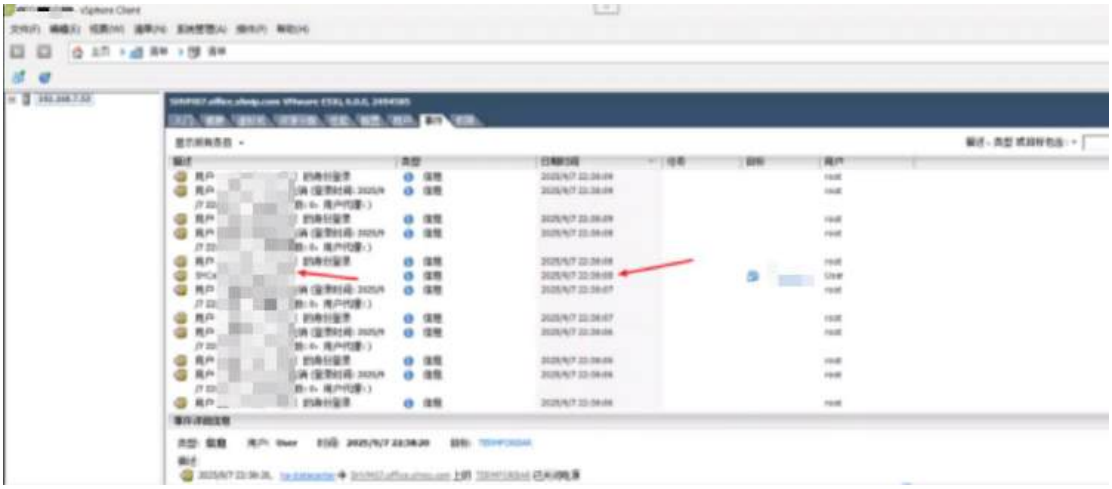


图 191: 加密前攻击者关闭 ESXI 虚拟机

2025/09/07 22:48:58.000-22:49:29.000 攻击者在 192.168.XXX.XXX SHBAK01 上部署 frp 建立代理隧道。

图 192: frpc 服务注册

图 193: iKuai 上监测到的隧道连接流量

2025/09/07 22:49:15.000 从 192.168.XXX.XXX 连接 192.168.XXX.XXX ssh，紧接着关闭所有虚拟机。

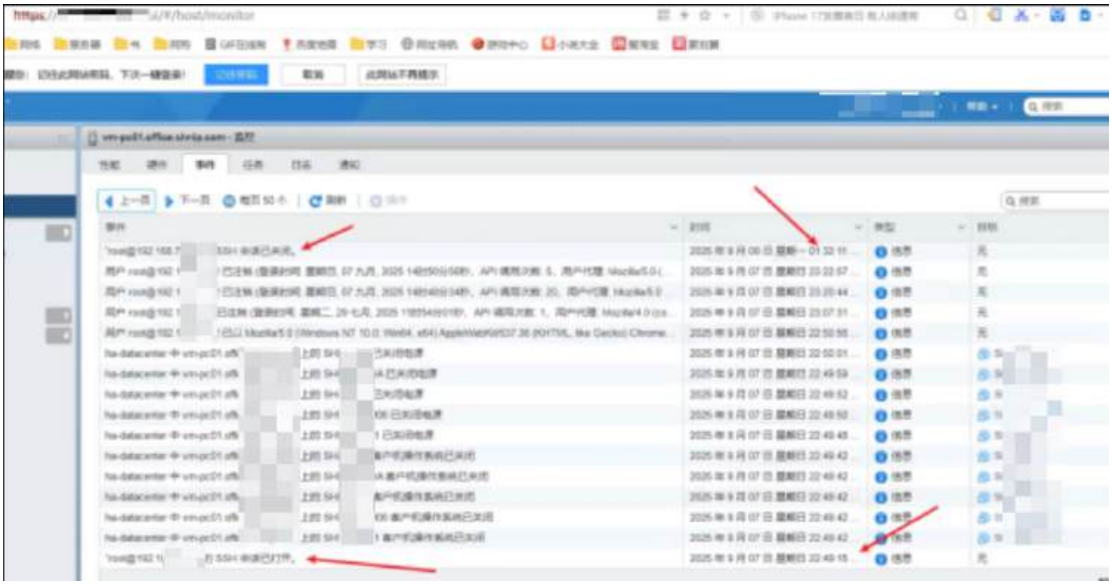


图 194: 攻击者加密前后操作

2025/09/08 01:32:11.000 从 192.168.XXX.XXX 关闭对 192.168.XXX.XXX ssh 连接。

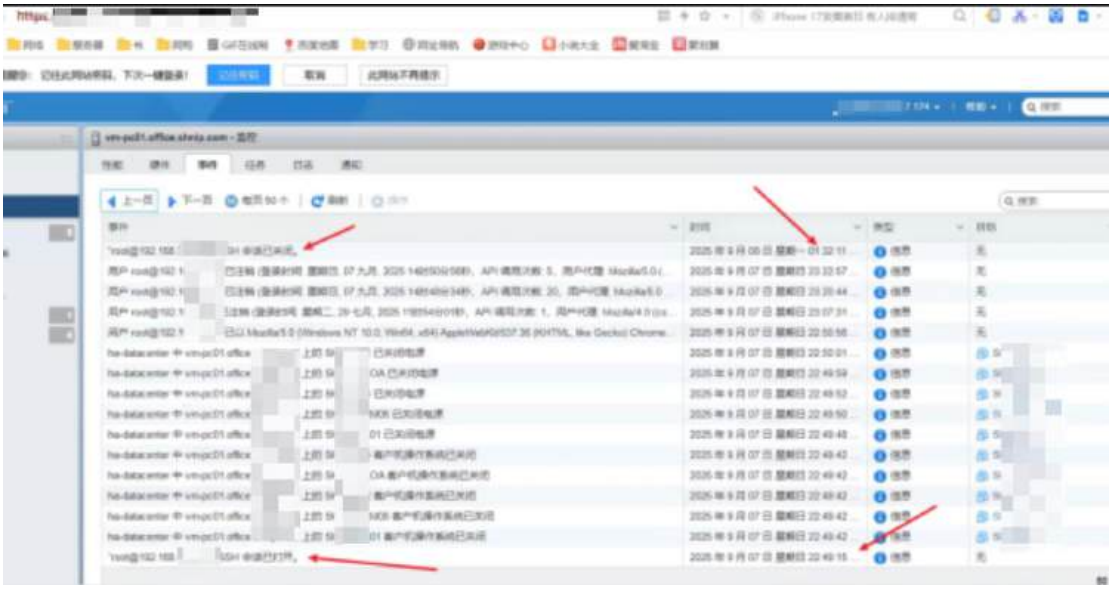


图 195: 攻击者加密前后操作

2025/09/08 5:00:44.000 5.182.XXX.XXX 连接 192.168.XXX.XXX，该 IP 与第一次入侵 192.168.XXX.XXX 为同 IP。

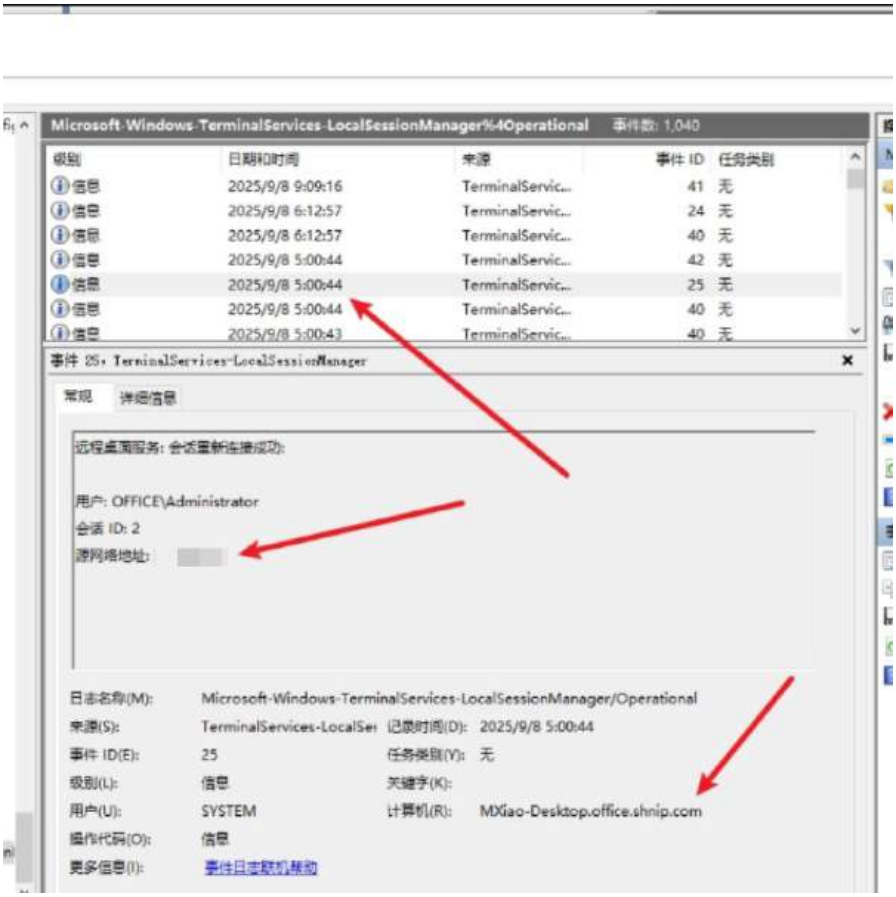


图 196: 5.182.4.55 连接 192.168.XXX.XXX

2025/09/10 13:54:00.000 攻击者通过 192.168.XXX.XXX 最后一次发起的连接目标 192.168.XXX.XXX。default.rdp 文件 是 Windows 远程桌面客户端（mstsc.exe）在用户配置目录下自动生成的一个配置文件，保存的是 上一次你运行远程桌面时所使用的连接参数。

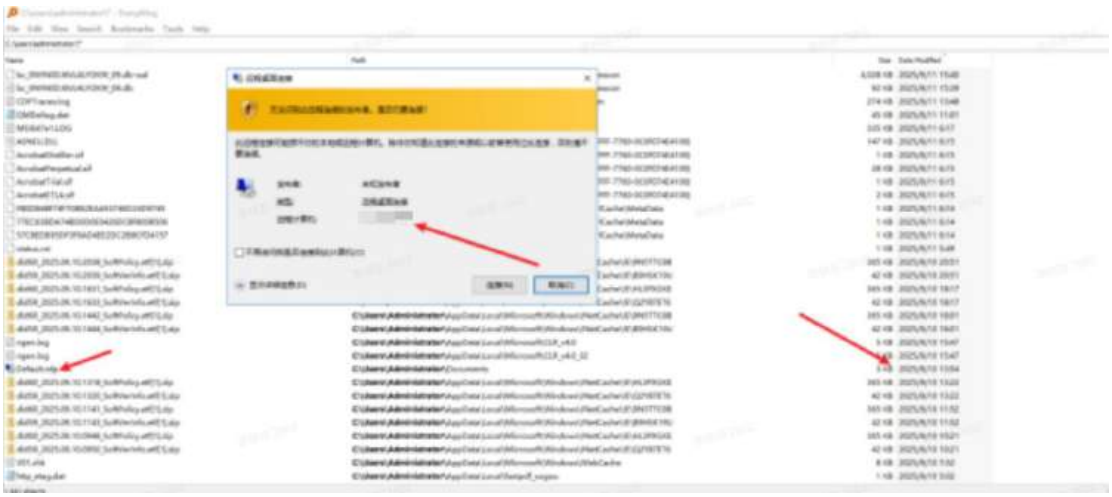


图 197: default 配置文件

2025/09/12 3:45:29.000-2025/09/17 8:25:00.000 攻击者在此期间，分别于

09/12、09/15、09/16、09/17 通过 wmi 在 192.168.xxx.xxx 上查询该计算机上的安全软件。

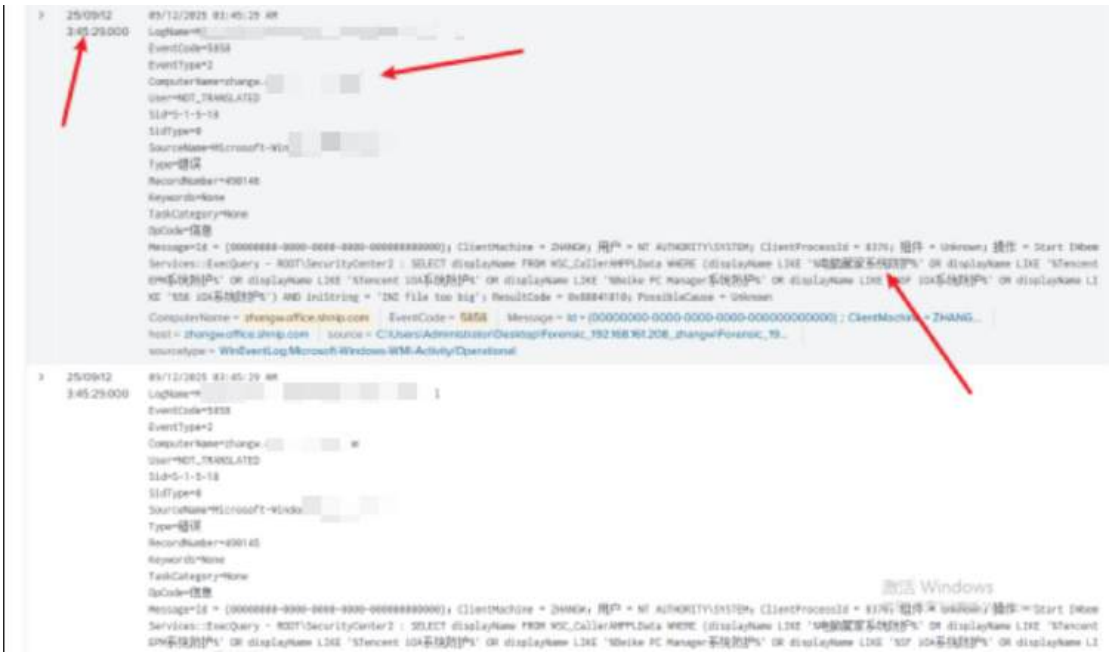


图 198: 攻击者第一次于 192.168.xxx.xxx 上查询该计算机上的安全软件

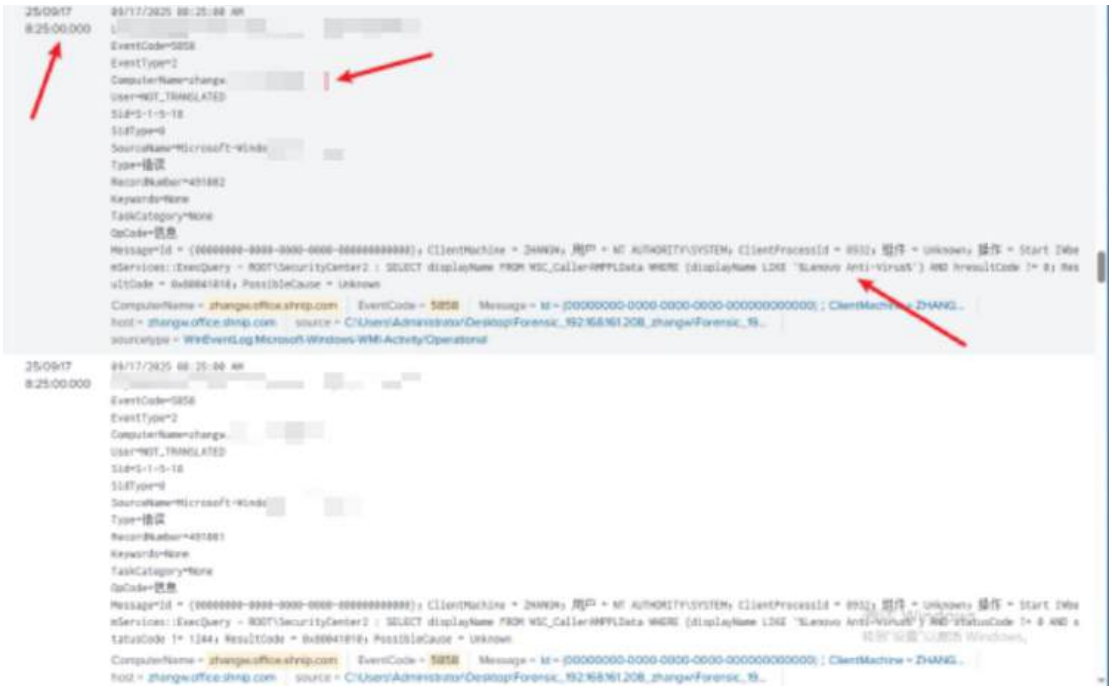


图 199: 攻击者最后一次于 192.168.xxx.xxx 上查询该计算机上的安全软件

第四章　勒索软件技术发展与风险趋势研判

（一）AI 技术对勒索攻防形态的影响

1.“智械危机”：AI 驱动下的勒索软件生态演进与代际更替

2024 年至 2025 年间，勒索软件生态经历了从“人工运营”向“智能化驱动”的历史性跨越。Solar 安全团队基于多源威胁情报（包括 Ransomlive 监测数据、暗网 RaaS 面板分析及 NYU/ESET 技术复盘）分析发现，AI 技术已不再仅是勒索软件开发者的辅助工具，而是正在重构从**代码编写、运营交付到载荷执行**的全生命周期。当前的勒索软件威胁呈现出明显的“三级阶梯式”演进特征。

2.运营门槛的崩塌：AI 辅助下的规模化扩张

在“入门级”威胁层面，AI 极大地降低了网络犯罪的技术门槛，导致低水平攻击者（Script Kiddies）也能发动复杂的全球性攻击。据 Bitdefender 与 SonicWall 联合监测数据显示，自 2024 年 11 月首次活跃以来，新兴组织 **FunkSec** 在短短数月内即成功入侵了超过 **120** 家机构，受害者遍布美国、印度、西班牙等全球多个区域，覆盖政府与国防等高价值目标。 尽管逆向分析显示 FunkSec 的核心代码中保留了大量由 LLM（大语言模型）生成的注释，暴露出攻击者自身底层编码能力的匮乏，但其利用 AI 编写的 DDoS 脚本与加密器依然具备实质破坏力。更值得警惕的是，FunkSec 率先部署了基于 Miniapps 平台的 **AI 聊天机器人**，实现了多语言环境下的自动化赎金谈判与受害者指引。这种“AI 客服”模式彻底打破了勒索运营的语言壁垒与人力瓶颈，是其能够短时间内实现规模化扩张的关键动因。

```
# Randomized headers to simulate diverse traffic
user_agents = [
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.102 Safari/537.36",
    "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Safari/605.1.15",
    "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0",
    "Mozilla/5.0 (iPhone; CPU iPhone OS 14_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15A372 Safari/604.1"
]

# Paths for randomness
paths = ["/", "/login", "/contact", "/about", "/search?q=random" + str(random.randint(1, 1000))]

# Large payload for HTTP flood
large_payload = "A" * 10000  # Large body content to increase the packet size

# UDP Reflection amplification packet
amplified_packet_data = b'\x00' * 1024  # 1KB UDP packet for flood

# UDP Reflection to boost the attack power (use for IP spoofing and amplification attacks)
```

图 200:代码中的 AI 辅助

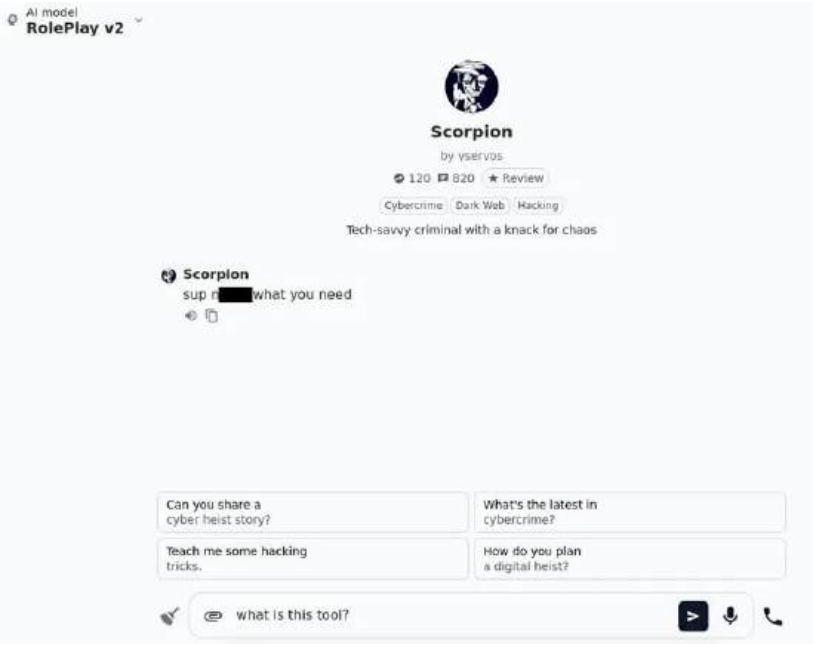


图 201:AI 聊天机器人

3.供应链的敏捷革新：RaaS 生态的智能化重构

在“专业级”威胁层面，成熟的 RaaS（勒索即服务）家族开始利用 AI 优化其商业生态与供应链交付。根据 Solar 团队对 **Nova** 家族（RaLord 变种）的深度追踪，该家族代表了“AI + 敏捷开发”的新范式。Nova 利用 AI 辅助编程构建了高效的流水线，使其病毒版本更新极快，能够迅速响应安全厂商的防御策略。 不同于传统家族，Nova 利用 AI 技术攻克了“本地化”难题，特别针对中国市场实现了“母语级”的招募与渗透，并结合 Rust 语言开发的高性能加密器与仅 **15%** 的低抽成策略，迅速在黑产市场中抢占份额。其 RaaS 控制面板集成了 AI 生成的现代化 UI 与智能后台，显著提升了分销商（Affiliates）的使用体验。Nova 的案例表明，AI 已被头部家族转化为核心竞争资产，用于构建更具黏性的犯罪生态系统。

图 202:AI 驱动下的勒索供应链革命

4.静态防御的失效：原生 AI 恶意软件的“动态多态”

在“战略级”前沿威胁层面，以 **PromptLock** 为代表的“勒索软件 3.0”正在颠覆传统的反病毒检测逻辑。基于 ESET 捕获样本及 NYU 的研究复盘，PromptLock 彻底抛弃了硬编码恶意逻辑的传统架构，转而采用 Go 语言编写的“AI 连接器”形态。该样本在运行时调用本地部署的大模型（如 gpt-oss:20b），通过多轮次的“提示词注入（Prompting）－ 代码生成 - 自我纠错（Self-Correction）”**循环，在内存中动态生成 Lua 恶意脚本。 逆向数据显示，PromptLock 具备极强的环境感知与智能决策能力。它能根据侦察结果（如系统类型、数据价值）自主决定执行 Encrypt（加密）、Exfiltrate（窃取） 还是 Destroy（销毁） 操作，并能利用 `<success><feedback>` 标签机制自动修复执行失败的代码。这种**“运行时多态（Runtime Polymorphism）”特性意味着每一次攻击生成的哈希值与代码结构均不相同，使得基于静态特征库的主流杀毒引擎几乎完全失效，标志着勒索攻防正式进入“行为分析为王”的新时代。

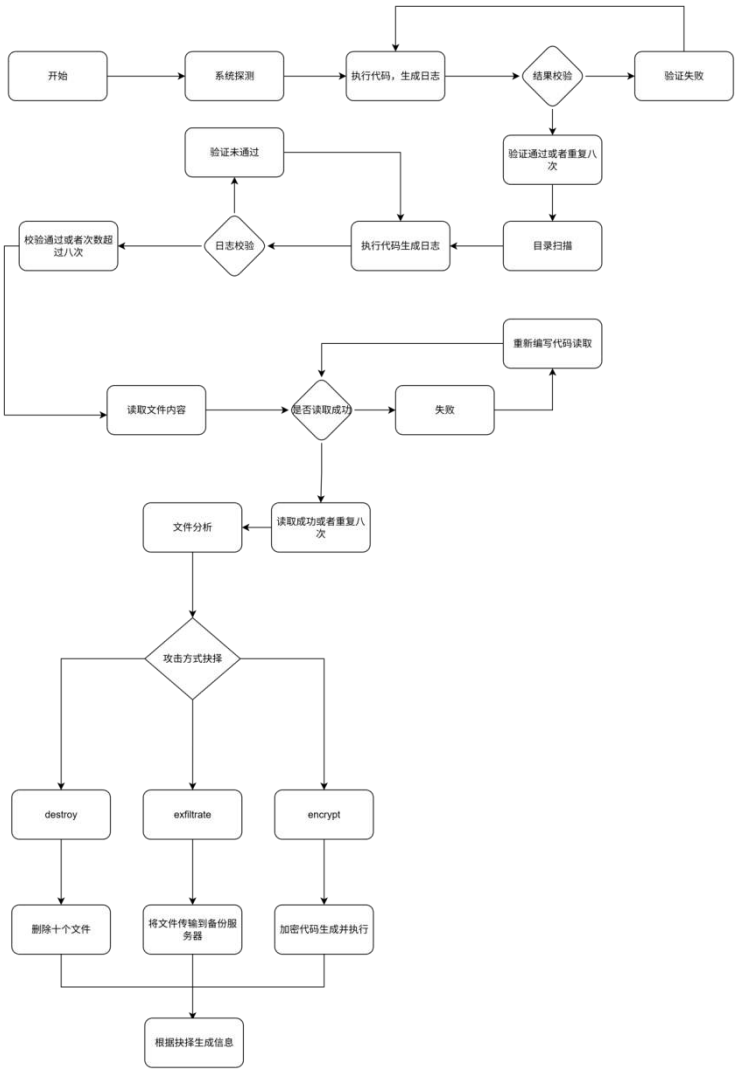


图 203:AI 流程展示

（二）从“技术犯罪”到“全球化商业体系”

1.宏观演进：全球化商业犯罪体系的确立

2024-2025 周期内，全球勒索软件支付规模达到了惊人的 **17.3 亿美元 ($17.3B)**，活跃攻击家族数量稳定在 **50 个** 左右，且专业化程度显著增强。

市场规模爆发： 2024-2025 周期内，全球勒索软件支付规模达到了惊人的 **17.3 亿美元 ($17.3B)**，活跃攻击家族数量稳定在 **50 个** 左右，且专业化程度显著增强。

产业链条分工： 整个生态已异化为成熟的“黑色 SaaS”平台。犯罪环节被精细拆解，出现了专门负责初始访问接入（IAB）、恶意代码生成、谈判服务以及流量调度的独立供应商，各环节通过 API 和共享平台进行协作，大幅提升了犯罪效率。

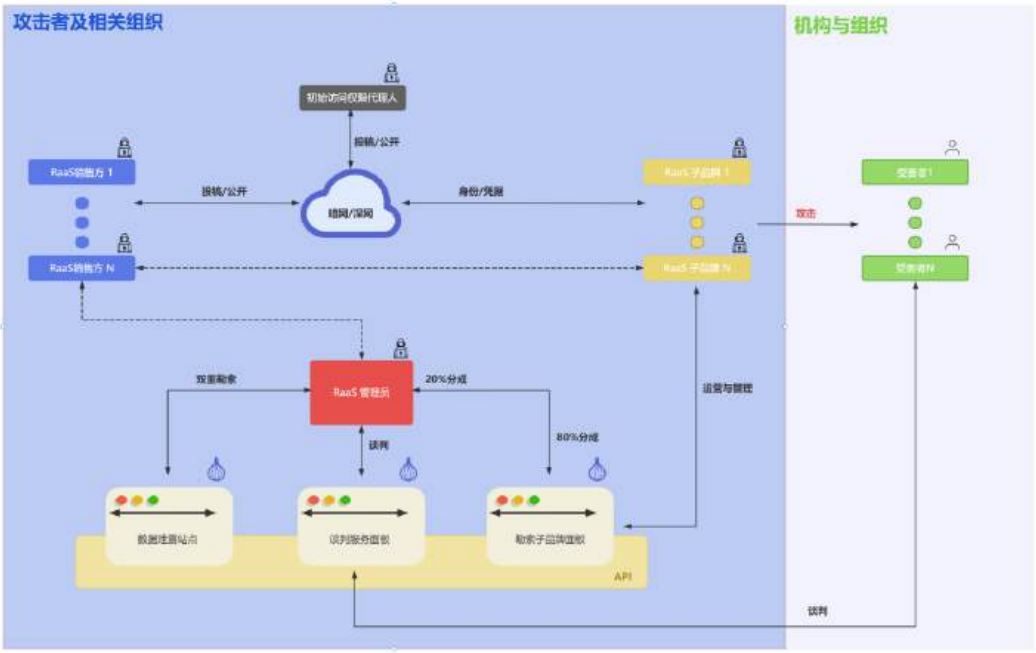


图 204:攻击者及相关组织

2.生态分化：平民化扩张与精英化博弈

2025 年的勒索生态呈现出极端的“二元分化”特征，形成了“下沉市场”与“高端定制”并存的局面：

2.1 大规模“平民化”扩张（Mass Market）

以 **DragonForce** 为代表的组织通过极致降低准入门槛，推动了攻击的“平民化”：

- **加盟门槛暴跌：** 传统的 RaaS（勒索即服务）加盟押金通常在 $2,000 - $10,000 之间，而 DragonForce 将其降至仅需 **$500**。

- **自动化注册（Auto-Reg）：** 引入了无需面试即可获得面板权限的机制，结合 Rust 语言封装的“开箱即用”攻击包，使得非技术人员也能轻松参与攻击，导致攻击尝试频率呈指数级上升。

图 205:DragonForce 勒索组织详情

2.2 高端“狙击型”生态（Elite Tier）

以 **Qilin** 为代表的顶层组织则选择了截然不同的路线：

- **精英筛选：** 坚持严格的附属成员筛选机制，专注于针对高价值目标的“大猎杀”（Big Game Hunting）。
- **基础设施互联：** **RAMP 4u** 等平台开始发挥“黑产中间件”的作用，提供跨组织的人才招募与初始访问分发，实现了黑产资源的深度共享。

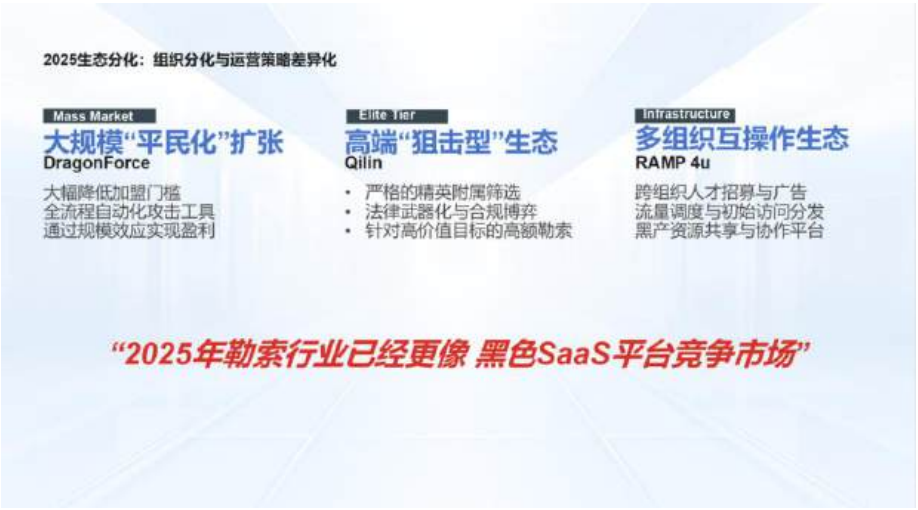


图 206:组织分化与运营策略差异化

3.商业逻辑变革：合规武器化与 ROI 导向

3.1 从“能付钱”到“必须付钱”

2025 年的新型勒索谈判已不再单纯依赖数据价值，而是将**监管合规机制**转化为攻击武器：

- **Qilin 的 "Call Lawyer" 机制：** 攻击者在谈判面板中增加了法律专家服务，直接向受害者剖析数据泄露将面临的 GDPR 或 SEC 处罚，利用企业的合规恐惧倒逼支付。
- **监管的三位一体压力：** 在中国，央行 2025 新规明确了“及时报告、建立台账、配合检查”的要求。攻击者利用企业对监管处罚、业务中断和声誉受损的担忧，构建了包含合规、法律、经营风险在内的“系统性风险”勒索模型。

图 207:详情展示

3.2 行业靶向的 ROI 逻辑

攻击者的选择遵循绝对的商业回报率（ROI）：

- **金融行业的困境：** 虽然金融行业在整体攻击占比中仅排第三（**7%**），低于制造业（18%）和高新技术业（17%），但其勒索赎金中位数高达 **$5,000,000+**，远超其他行业。
- **核心结论：** “谁最赚钱就打谁”成为攻击者的核心逻辑，金融行业因高昂的赎金支付能力（最佳 ROI），成为攻击者优先选择的高价值目标。

图 208:金融行业一览

（三）专精无加密勒索的全面兴起

在 2024 至 2025 年的勒索软件威胁版图中，一个最具颠覆性的趋势正在加速形成：**无加密勒索（Encryption-Less Ransomware）** 的异军突起。

传统的勒索攻击依赖于“加密文件”来阻断业务，迫使企业支付赎金以获取解密密钥。然而，随着企业数据备份体系（Backup & Recovery）的日益完善，单纯的加密攻击成功率显著下降。面对这一防御困境，攻击者选择了极其实用的进化路线：**彻底放弃复杂的加密过程，专注于数据窃取（Data Exfiltration）与隐私勒索。**

1.家族谱系：三次重生的“变形记”

在勒索软件的演进史上，很少有组织能像 World Leaks 这样清晰地展示出“适者生存”的进化逻辑。该组织并非凭空出现，而是顶级攻击者组织历经两次“重生”后的最终形态：

- **起源（Origins）：** 其根源可追溯至臭名昭著的 **Hive** 勒索组织。在 Hive 的基础设施被执法部门摧毁后，其核心成员并未消散，而是重组为 **Hunters International**，并于 2023 年末开始活跃。

- **品牌重塑（Rebranding）：** **2025 年 1 月**是一个里程碑式的时间点。Hunters International 正式停止了所有基于文件加密的攻击活动，并更名为 **World Leaks**。这一举动标志着该组织彻底抛弃了传统的勒索软件（Ransomware）外衣，转型为纯粹的数据勒索实体。

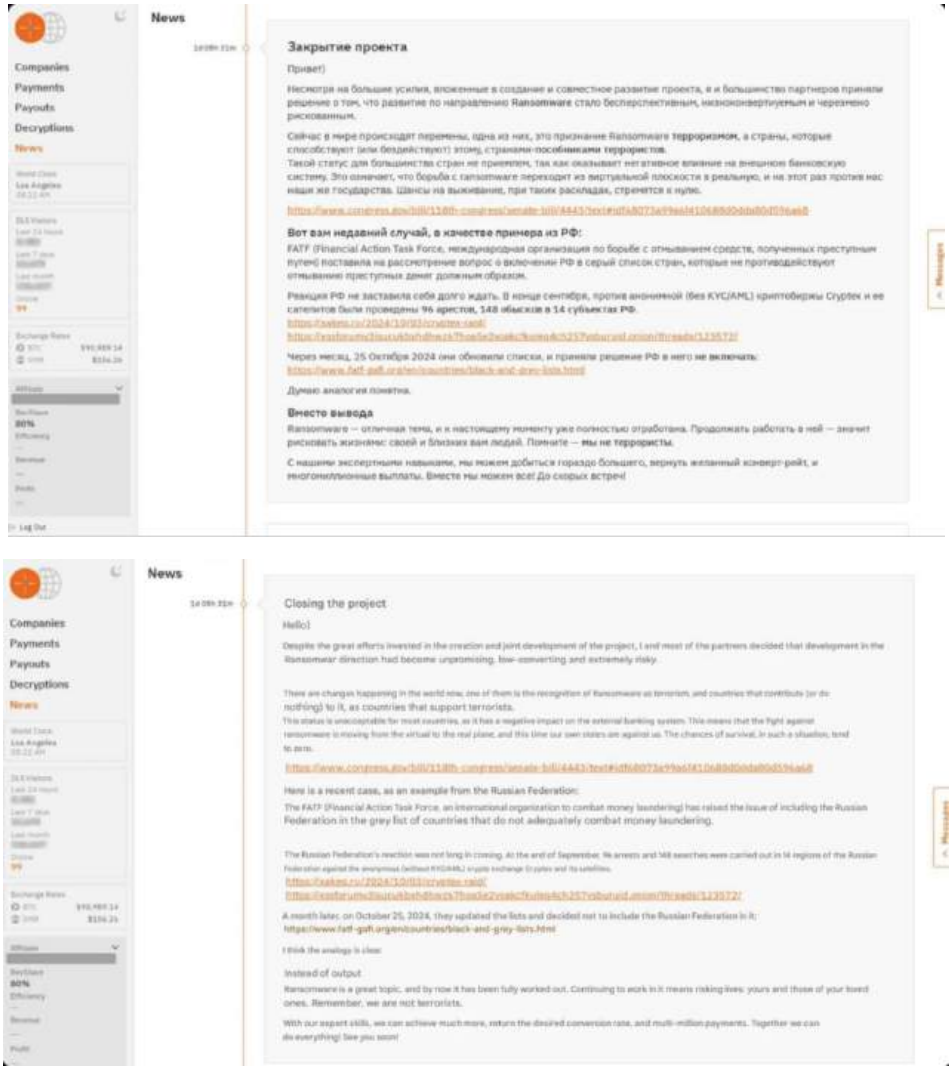


图 209:Hunters International 关于该项目结束的声明

2.模式重构：EaaS 与“自动化掠夺”

World Leaks 的出现定义了 **“勒索即服务”（Extortion-as-a-Service, EaaS）** 的新标准。与传统的 RaaS（Ransomware-as-a-Service）不同，EaaS 模式不再提供加密器，而是专注于数据的“流转”与“变现”：

- **自动化提取工具：** World Leaks 为其附属成员（Affiliates）提供高度自动化的数据提取工具。攻击者无需具备深厚的渗透技能，只需部署工具即可自动扫描并窃取敏感数据。

- **单一压迫点：** 攻击链条被极致简化为“窃取 $\rightarrow$ 威胁”。如果受害者拒绝支付，被盗数据将被直接发布在 World Leaks 维护的 **Tor 网站**上。这种“不付款即公开”的单一策略，消除了受害者对于“解密失败”的侥幸心理。

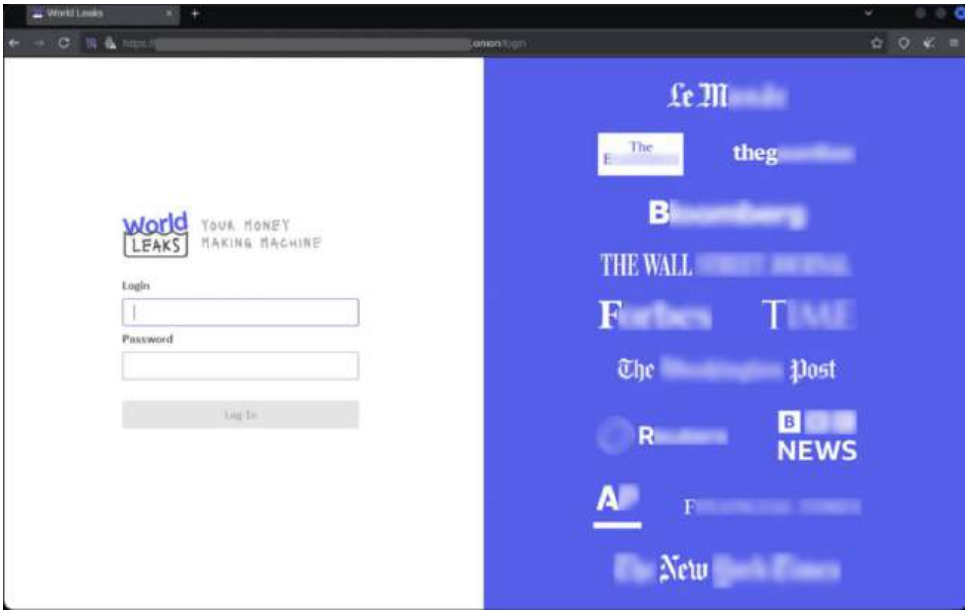


图 210:新推出的 World Leaks 附属小组的登录页面

3.战略动机：去加密化的成本逻辑

World Leaks 放弃加密（No Encryption）并非技术倒退，而是基于风险与成本的精明计算:

- **降低复杂性与风险：** 维护一套稳定的加密/解密密钥管理系统需要巨大的技术成本，且容易因代码漏洞（如之前的 Hive 解密器漏洞）被安全公司攻破。放弃加密，意味着消除了这一技术短板。
- **规避法律与打击：** 相比于破坏系统可用性（加密），单纯的数据窃取在某些法律管辖区被视为“数据泄露事件”而非“破坏计算机信息系统”，这在一定程度上降低了执法部门介入的优先级，同时使得攻击行为更具隐蔽性。

第五章 勒索防护与应急响应实践建议

基于 2025 年 Solar 应急响应团队处置的 534 起真实勒索案件，我们发现：90% 的勒索攻击并非利用了无法防御的“0-day”漏洞，而是利用了企业在**基础安全配置**、**补丁管理**及**人员意识**上的疏漏。针对当前的勒索威胁态势，Solar 团队结合一线实战经验，提出以下防护与响应建议。

(一) 面向企业的勒索防护建议

基于全年数据分析，本章提出分层次、分阶段的防御策略和威胁狩猎建议，旨在帮助组织将有限的资源聚焦于最关键的风险领域和时间窗口。

1. 发现勒索攻击后的应急处置流程

勒索攻击发生后的**“黄金一小时”**至关重要。企业应遵循“止损优先、保护现场”的原则，切忌盲目重启或重装系统，以免破坏取证线索或导致数据永久丢失。

建议企业按照以下标准流程（SOP）进行操作：

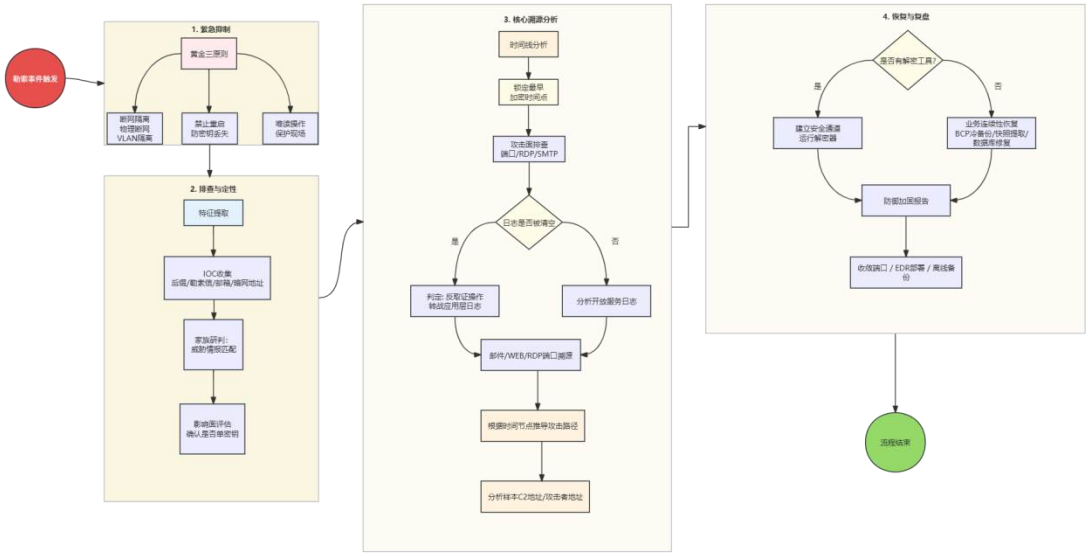


图 211:勒索病毒应急处置 SOP 流程

关键步骤操作要点：

1. **物理/逻辑隔离（止损）**
   - **动作**：立即拔除受感染主机的网线（物理隔离）或在交换机/防火墙层面通过 ACL 阻断其网络连接（逻辑隔离）。
   - **禁忌**：**严禁直接关闭服务器电源**。勒索软件可能在内存中残留解密密钥或痕迹，关机会导致易失性数据丢失，且部分勒索软件设有“开机自毁”机制，重启可能导致数据二次损坏。
2. **范围排查（定损）**
   - **动作**：快速检查内网其他核心资产（如域控、备份服务器、ERP/财务数据库）是否出现异常文件后缀或勒索信，确定感染边界。
3. **现场保护（取证）**
   - **动作**：对勒索信、加密文件样本、系统日志（Event Log）、Web 日志（IIS/Nginx/Apache）进行备份保存。
   - **工具**：推荐使用 Solar 自动化采集工具进行内存与磁盘痕迹提取。
4. **专业介入（处置）**

- **动作**：联系专业应急响应团队介入。切勿轻信网上的“解密工具”或私自联系攻击者，以免遭遇二次诈骗。

2. 企业反勒索安全体系规划建议

针对 Weaxor、Qilin 等家族利用 **N-day 漏洞**及 **供应链跳板** 进行攻击的特点，企业应构建纵深防御体系。

1. **收敛互联网暴露面（Attack Surface Reduction）**
   - **原则**：非必要不开放。
   - **措施**：
     - 严禁将 RDP（3389）、SMB（445）、数据库端口（1433/3306）直接暴露在公网。
     - 确需远程管理的，必须通过 VPN 或 堡垒机 访问，并强制开启 **多因素认证（MFA）**。
     - 排查并卸载非业务必需的远程控制软件（如 AnyDesk、TeamViewer、向日葵），防止其成为攻击者的后门通道。
2. **建立“不可篡改”的备份机制**
   - **原则**：备份是勒索防护的最后一道防线。
   - **措施**：严格执行 **“3-2-1”备份策略**（存储 3 份数据，使用 2 种不同介质，至少 1 份**离线/异地冷备份**）。
   - **重点**：勒索软件（如 DragonForce）往往会优先攻击在线备份系统（Veeam/群晖 NAS）。因此，**物理隔离的离线磁带或移动硬盘**是数据恢复的唯一底牌。
3. **精细化网络微隔离（Micro-segmentation）**
   - **措施**：将核心业务区（如财务、研发）与办公网（OA）、互联网接入区进行 VLAN 隔离。
   - **目的**：阻断勒索软件利用 Cobalt Strike 或 PsExec 在内网的横向移动，防止“一台中毒，全网瘫痪”。
4. **漏洞全生命周期管理**
   - **措施**：建立资产台账，针对高危服务（如用友 U8/NC、金蝶、泛微 OA、Exchange 邮件服务）建立 7x24 小时漏洞监测机制，确保在厂商发布补丁后的 24 小时内完成测试与修复。

3. 勒索事件处置后的加固与防护措施

勒索事件处置完毕并不意味着风险解除。攻击者极有可能留有后门（Webshell/幽灵账号），企图进行“二次勒索”。

1. **全网凭证重置**
   - 强制修改所有高权限账号（域管、本地管理员、数据库 SA/Root）的密码，确保新密码满足“强口令”要求（12 位以上，包含大小写、数字及特殊字符）。
2. **彻底清除残留后门**
   - 全盘扫描查杀潜在的 Webshell、恶意计划任务（Scheduled Tasks）、WMI 持久化脚本及异常注册表启动项。
3. **补丁验证与策略封堵**
   - 复盘攻击入口（如 Weaxor 利用的某 ERP 漏洞），打上对应补丁，并关闭导致入侵的高危端口。

(二) 面向个人用户的安全防护建议

2025 年，针对个人终端的勒索攻击（如 Stop/Djvu 家族）依然活跃，主要通过盗版软件与钓鱼邮件传播。

1. 个人安全意识与使用习惯建议

1. **数据备份常态化**：重要文件（如照片、论文、工作文档）应定期同步至云盘或移动硬盘，备份完成后**务必断开**移动硬盘与电脑的连接。
2. **系统与软件更新**：保持 Windows 系统及杀毒软件处于最新版本，开启自动更新功能，修补已知系统漏洞。
3. **账号安全**：各类网站/软件避免使用“一套密码走天下”，建议配合密码管理器使用复杂密码，并尽可能开启手机验证码或 OTP 二步验证。

2. 高风险上网行为防范建议

1. **远离盗版与破解软件**
   - **风险**：Solar 团队监测发现，大量勒索软件伪装成“游戏修改器”“软件注册机（Keygen）”“破解补丁”在下载站传播。
   - **建议**：坚持从官方渠道下载软件，严禁运行来源不明的 `.exe` 或 `.bat` 文件。
2. **警惕钓鱼邮件与宏病毒**
   - **风险**：攻击者常伪装成“发票”“通知”“简历”发送带有恶意宏（Macro）的

Office 文档或压缩包。

- **建议**：不要轻易打开陌生邮件的附件，Office 软件中默认禁用“宏”功能。

3. 遭遇勒索风险时的应急处理措施

1. **立即断网**：一旦发现文件后缀被修改或桌面弹出勒索信，立即拔掉网线或断开 Wi-Fi，防止病毒加密更多文件或通过网络传播给家人/同事。
2. **勿信“付费解密”**：针对个人用户的勒索软件（如 Stop 家族的在线 ID 版本），支付赎金后获得解密密钥的概率极低。
3. **寻求专业协助**：
   - 保留被加密文件和勒索信。
   - 访问国际通用的解密网站（如 No More Ransom）查询是否有免费解密工具。
   - 如涉及重要高价值数据，建议咨询专业数据恢复机构进行底层数据修复评估。

(三) 红色预警日历：基于数据的资源调配策略

根据攻击节奏的季度特征，建议建立动态的安全运营日历，在关键时期前置性增加监控和响应资源。针对 2 月的年初攻势，建议提前 45 天启动邮件安全专项加固，包括钓鱼邮件模拟演练、邮件网关规则优化、员工安全意识培训等。同时，应完成上一年度到期安全设备的续费或替换，消除“预算空窗期”带来的防护缺口。

针对 5-8 月的夏季蓄力期，虽然整体攻击数量下降，但应加强对高价值目标的异常行为监控。建议部署 EDR（端点检测与响应）和 NDR（网络检测与响应）工具，建立针对横向移动、数据窃取等后期攻击阶段的检测规则。这一时期也是进行红队演练、验证检测能力的理想窗口。

针对 Q4 的年末收割，Healthcare 和 Financial Services 行业应提前 30 天启动最高级别监控，包括 7×24 小时 SOC 值守、关键系统异地备份验证、应急响应团队待命等。制造业虽然全年暴露相对稳定，但年末的交付压力同样可能提高赎金支付意愿，不应掉以轻心。

附录 2025 年度国外重大勒索事件回顾

1. EcuacorrienteS.A.勒索事件

2025 年 11 月 25 日“TheGentlemen”勒索组织在暗网公开发布“EcuacorrienteS.A.”公司的勒索信息。Ecuacorriente S.A.是总部位于厄瓜多尔基多一家大型矿业公司，成立于 1999 年。目前该公司是 XX 企业联合体的全资子公司，该联合体由 XX 股份有限公司和 XX 金属集团控股有限公司共同控股 Ecuacorriente S.A.最初由 Corriente Resources Inc.加拿大一家矿业公司全资拥有或控制，主要从事铜矿的勘探、开发和生产运营 2010 年，XX 企业联合体以约 6.8 亿美元收购加拿大 Corriente Resources Inc.控制 Ecuacorriente S.A.并于 2012 年与厄瓜多尔政府签署 Mirador 铜矿的 30 年开采合同，使其成为该国首个大型工业铜矿项目。是中国和厄瓜多尔资源合作的重要平台。截至目前 2025 年 12 月 20 日，TheGentlemen 勒索组织已经公开所有窃取的数据。进行分析后，这些数据涉及企业的网络安全设备清单、网络拓扑图、安防系统拓扑图、关键基础设施技术细节以及相关账号密码等敏感信息。

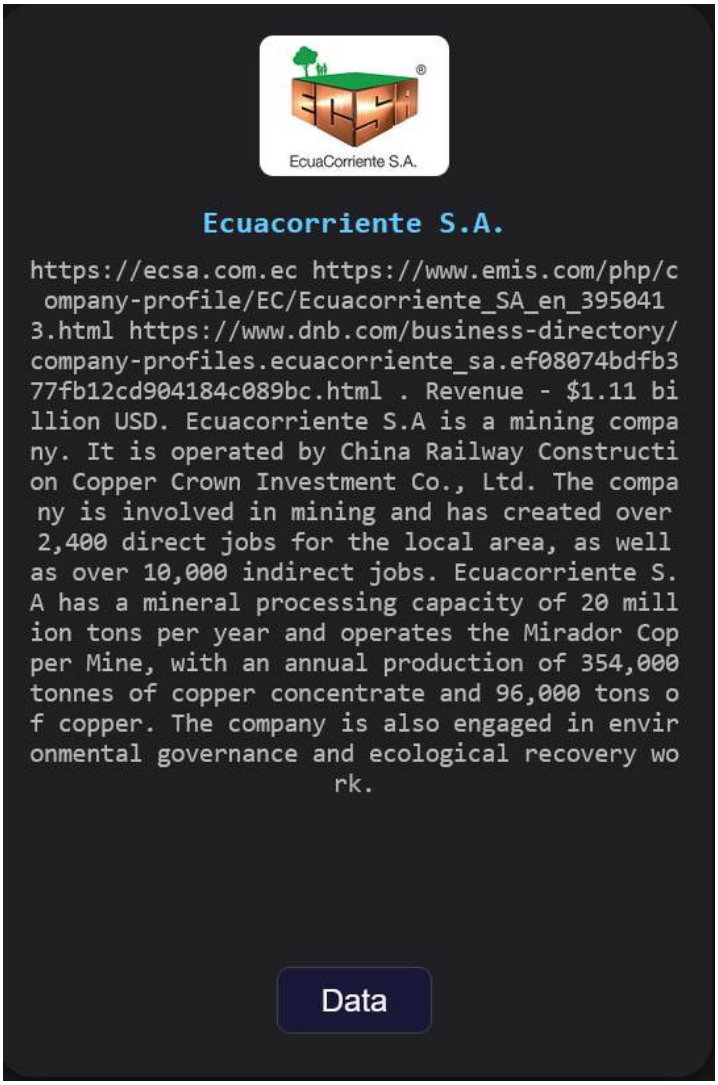


图 212:勒索组织受害者信息

2. Ingram Micro（英迈）勒索事件

2025 年 7 月，全球大型技术分销商、财富 100 强企业 Ingram Micro（英迈）遭受勒索软件攻击。Ingram Micro 作为连接全球多家技术供应商与大量渠道经销商的重要分销平台，其业务系统在事件期间出现大面积中断，对全球 IT 供应链造成了显著影响。攻击发生于 2025 年 7 月 3 日，事件发生后，Ingram Micro 主动下线了包括 AI 驱动业务平台“Xvantage”以及云许可管理平台“Impulse”在内的多套核心系统，以防止勒索软件在内部网络中进一步扩散。上述系统下线直接导致合作伙伴在一段时间内无法进行订货、报价及许可证管理等业务操作。

图 213:勒索组织受害者信息

3. Asahi Group Holdings（朝日集团）勒索事件

2025 年 9 月，日本大型跨国企业、全球饮料制造商 Asahi Group Holdings（朝日集团）遭遇 Qilin 勒索软件攻击。该事件对企业信息系统及实际生产运营造成了直接影响，部分业务在事件期间被迫中断。攻击于 2025 年 9 月 29 日被发现，随后确认已影响朝日集团在日本国内的多套核心系统。受影响范围不仅包括办公网络中的邮件系统和文件服务器，还波及用于订单处理、物流调度及生产计划管理的业务系统。上述系统被加密后无法正常使用。为防止勒索软件进一步扩散至工厂控制系统（OT 网络），朝日集团采取了断网隔离措施。该处置措施在阻断攻击扩散的同时，也导致部分生产线暂停运行、物流配送受阻。事件期间，部分业务流程临时改为人工方式处理，对产品供应和销售产生了明显影响。据公开信息，部分主力产品在市场上出现阶段性供应不足，软饮料业务销售额在短时间内出现较大幅度下降。

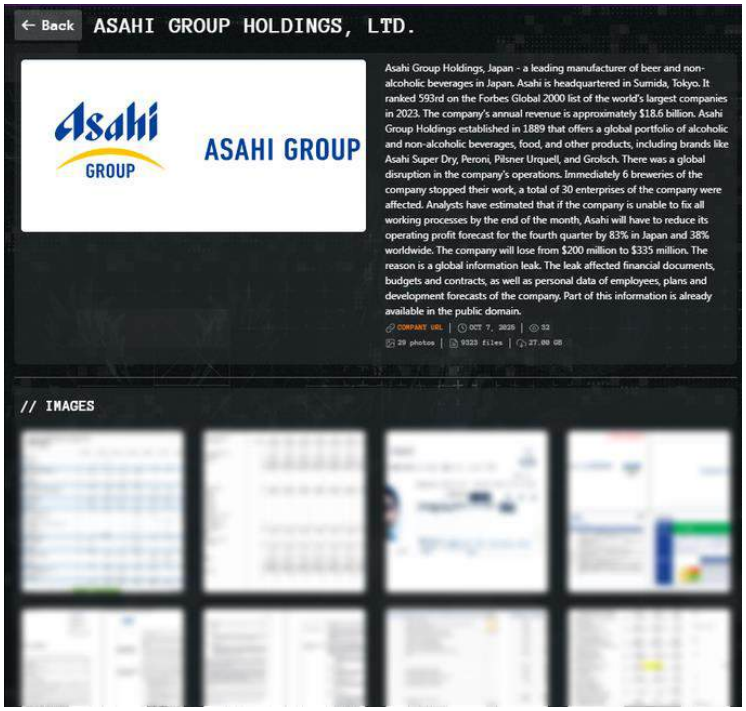


图 214:勒索组织受害者信息

4. Jaguar Land Rover（捷豹路虎，JLR）勒索事件

2025 年 9 月 1 日，英国汽车制造商 Jaguar Land Rover（捷豹路虎，JLR）披露其遭遇一起严重网络安全事件。该事件对企业全球生产与研发体系造成重大影响，并引发英国政府相关部门的关注。事件不仅影响企业自身运营，也对汽车产业链稳定性产生了外溢影响。

攻击导致 JLR 位于英国、斯洛伐克、中国及印度的多处生产基地暂停生产。多条自动化生产线停止运行，设计与研发部门使用的 CAD/PLM 系统无法访问，经销商订车及订单管理系统亦处于离线状态。受汽车行业高度依赖即时供应（Just-In-Time）模式的影响，JLR 生产中断迅速波及大量上下游供应商。根据行业评估，停产期间企业面临的直接经济损失规模较大。为防止关键供应链企业因资金链问题受到进一步冲击，英国政府随后宣布提供最高约 15 亿英镑的贷款担保措施，以稳定国内汽车产业运行。

安全研究人员认为，此次针对 JLR 的攻击并非由单一勒索组织实施，而是由多个活跃威胁行为体在一定程度上协同完成，情报中通常将该组合称为 “Scattered Lapsus$ Hunters”。

该组合被认为与以下几类已知威胁组织存在关联活动特征：

- **Scattered Spider**：以社会工程攻击见长，常通过电话欺诈（Vishing）、SIM 卡劫持等方式获取员工高权限账号，历史上曾多次针对身份管理平台实施攻击。
- **Lapsus$**：以高调披露数据、制造舆论压力著称，曾对多家大型科技企业实施入侵。

- **ShinyHunters**：长期从事大规模数据窃取和数据库交易活动，重点关注云环境和集中式数据存储系统。

协同行为：

从攻击过程和事后披露的信息来看，不同威胁行为体在初始入侵、数据窃取及信息公开等阶段分工明显。攻击者通过社交媒体和即时通信平台公开展示部分内部系统截图和数据样本，以扩大事件影响范围并向企业施压。

图 215:勒索组织受害者信息

5. DaVita Inc. 勒索事件

2025 年 4 月，美国大型肾脏护理服务提供商 DaVita Inc. 披露其遭 Interlock 勒索软件攻击窃取 510 GB 数据。DaVita 在美国运营超过 2600 家透析中心，为 20 余万名终末期肾病患者提供长期透析治疗，其业务具有高度医疗关键性。

攻击发生于 2025 年 4 月 12 日。勒索软件加密了 DaVita 部分内部网络系统，导致电子健康记录（EHR）、患者排班调度系统以及实验室信息系统无法正常使用。鉴于透析治疗对时间连续性的高度依赖，系统不可用对患者安全构成潜在风险。DaVita 随即启动应急处置流程，通过纸质病历和人工操作维持临床治疗连续性。尽管核心医疗服务未中断，但后台运营受到明显影响，包括计费流程暂停、实验室检测结果延迟以及患者信息访问受限。

图 216:勒索组织受害者信息

6. NISSAN CAPITAL 勒索事件

2025 年 11 月 23 日，**Qilin** 勒索组织在暗网数据泄露平台发布信息，声称其已从 **Nissan Capital** 窃取大量内部数据。Nissan Capital 是日本日产汽车集团旗下的金融服务公司，主要为日产及英菲尼迪品牌提供汽车融资、租赁及相关金融解决方案，在日本及多个海外市场开展业务。

根据 Qilin 组织公布的信息，其声称掌握的数据规模较大，涉及企业内部文件和业务资料。截至目前，Qilin 尚未一次性公开全部数据，仅展示了部分样本文件以证明其入侵行为的真实性。相关样本文件显示，数据类型可能包括企业内部运营文档、客户及合作方相关资料，以及部分财务和业务支持文件，具体内容仍有待进一步核实。

图 217:勒索组织受害者信息

北京数字世界咨询有限公司（以下简称“数世咨询”）是国内数字化领域独立第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布《中国数字安全大事记》、《中国数字安全能力图谱》、《中国数字安全100强》、《中国数字安全产业年度报告》等业内影响力巨大的公开报告。同时，还为监督机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，以及150余家网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动、投资对接，安全产品与企业推荐，企业资源整合等

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区天鼎218文化金融园东外110号 网安小酒馆
官方网站：www.dwcon.cn
联系邮箱：dw@dwcon.cn

小酒馆