# RANSOMWARE THREAT REARCH REPORT 2024

# 2024年勒索软件流行态势报告

360数字安全 360安全大模型

360安全能力中心反病毒部

2025年1月

# 前　言

本报告以三六零数字安全集团能力中心反病毒部（CCTGA勒索软件防范应对工作组成员）在2024年全年监测、分析与处置的勒索软件事件为基础，结合国内外与勒索软件研究相关的一线数据与安全数据进行全面研判、梳理与汇总而成。报告聚焦国内勒索软件的发展动态，同时融入国际热点事件与形势的分析判断，旨在评估2024年勒索软件传播与演化趋势，并深入探讨未来可能的发展方向，以协助个人、企业和政府机构更有效地制定安全规划，降低遭受勒索攻击的风险。

360反病毒部是三六零数字安全集团的核心能力支持部门，由一批常年奋战在网络安全一线的攻防对抗专家组成。该部门负责监测、防御、处置流行病毒木马以及研究新安全威胁。维护有360高级威胁主动防御系统、360反勒索服务等基础安全服务，并提供横向渗透防护、网络入侵防护、Web服务保护、挖矿木马防护等多项保护功能，保护政企单位与广大网民的网络安全。

# 摘　要


- 2024年，360反勒索服务平台共处理约2151起勒索软件攻击求助案例，国内勒索软件攻击的整体态势依然严峻。勒索软件攻击的目标继续集中于企事业单位，其中中小企业受到的攻击尤为严重，显示出这一群体在安全防护能力上的薄弱环节亟待加强。

- 国内流行勒索软件家族以TargetCompany(Mallox)、Makop和phobos为主，这三大勒索软件家族的反馈占比近六成。

- 2024年，勒索软件的传播手段整体变化不大，但Web应用漏洞利用正逐渐形成更大范围的采用。无论是头部家族TargetCompany(Mallox)，还是新兴家族RNTC，都表现出对Web应用漏洞传播手段的高度依赖。这一趋势表明，利用Web漏洞作为入侵点已成为勒索软件家族扩散攻击的主要选择之一。

- 各勒索家族的核心加密功能开始向效率方面进行优化。Curve25519、ChaCha20等高效算法被越来越多的采用。

- 根据对受害者的问卷调查分析，发现办公文档和数据库文件是在遭到勒索攻击后最被“在乎”的文件类型。反应出针对个人用户的勒索攻击更多是发生于办公场景之中。

- 2024年，双重勒索和多重勒索模式的赎金要求进一步攀升，多家勒索软件家族在成功攻击后开出了超过千万美元的赎金。其中，DarkAngels家族向美国知名药品公司Cencora提出了7500万美元赎金诉求，并最终勒索成功。这可能是目前全球最大的一笔勒索软件成交案例。这表明勒索软件团伙的攻击目标更具针对性，赎金金额也愈发惊人。

- 双重/多重勒索的重点攻击目标锁定在制造业、租赁和商务服务业以及批发零售业。公开的被勒索企业方面，美国企业以接近半数的占比位居榜首，国内亦有多家金融、能源企业上榜。

- 2024年，广东、山东和江苏三省成为国内勒索软件攻击最为严重的地区。受攻击的系统类型中，桌面操作系统仍然位居首位。这一现象与大量中小型企业将Web应用部署于如Windows 10这样的桌面操作系统平台密切相关。

- 互联网及软件、制造业、批发零售是2024年国内勒索软件攻击的主要目标，而金融行业所面临的威胁也有显著提升，已紧随其后位于榜单的第四名。

- 在攻击IP来源方面，俄罗斯依然是勒索攻击IP的第一大来源地，位列其后的也与去年相同——分别是德国和美国。而勒索软件作者所采用的沟通邮箱则依然以匿名邮箱为主。

- 在与勒索软件对抗的安全技术发展方面，我们认为未来将朝着AI技术应用、专业化与系统化攻防对抗等方向进一步演进。同时，360也推出了多款创新工具，持续走在与勒索软件对抗的安全技术前沿，推动行业在防护能力和应对策略上的不断升级。

# 目录 | CONTENTS


P001 | 第一章 勒索软件攻击形势

002 勒索软件概况
011 勒索软件传播方式
013 多重勒索与数据泄露
026 勒索软件家族更替

P053 | 第二章 勒索软件受害者分析

054 受害者所在地域分布
055 受攻击系统分布
057 受害者所属行业
058 受害者支付赎金情况
059 对受害者影响最大的文件类型
060 受害者遭受攻击后的应对方式
061 受害者提交反勒索服务申请诉求

P062 | 第三章 勒索软件攻击者分析

063 黑客使用IP
064 勒索联系邮箱的供应商分布
065 攻击手段

P082 | 第四章 勒索软件发展与趋势分析

083 Ai成为勒索对抗热点
086 专业化、系统化攻击频发
087 创新驱动反勒索技术发展——安全技术新突破

P088 第五章 安全建议
089 针对企业用户的安全建议
093 针对个人用户的安全建议
094 不建议支付赎金
095 勒索事件应急处置清单
P096 附录1 2024年勒索软件大事件
097 多家中国公司遭SANGGIERO勒索
099 江森自控称勒索攻击导致的数据被盗造成其2700万美元损失
100 特朗普案件的机密信息遭勒索软件窃取
101 瑞士表示PLAY勒索软件泄露了65000份政府文件
103 芯片制造商安世在遭勒索软件公布数据后确认泄露事件
104 波音公司证实有勒索软件试图向其勒索2亿美元
105 多名勒索软件相关黑客在美国被起诉
109 UNITEDHEALTH称有一亿条数据在勒索事件中被盗
110 施耐德电器确认黑客窃取数据后开发平台遭到破坏
112 俄罗斯逮捕多名勒索组织成员并判刑
P115 附录2 360终端安全产品 反勒索防护能力介绍
116 远控与勒索急救功能
119 勒索预警服务
120 弱口令防护能力
122 数据库保护能力
123 WEB服务漏洞攻击防护
124 横向渗透防护能力
125 提权攻击防护
126 挂马网站防护能力
127 钓鱼邮件附件防护
P128 附录3 360解密大师
P130 附录4 360勒索软件搜索引擎

第一章

# 勒索软件攻击形势

P001

P052

# 勒索软件攻击形势

2024年，勒索软件的整体传播趋势延续了2023年的平稳态势。无论是新兴勒索软件家族，还是传统勒索软件团伙的攻击活动，依然构成严峻威胁，但未出现单一勒索家族在短时间内的大规模爆发性攻击事件。此稳定态势一方面得益于全球主流安全厂商在反勒索防护方面的持续努力，另一方面也源于个人用户和政企单位对勒索软件这一特定恶意软件类别的高度重视与防范意识的增强。

然而，值得注意的是，“平稳”并不等于“安全”。尽管未见大规模的单个勒索事件爆发，但勒索软件仍是当前企业面临的头号安全风险。传统勒索软件家族不断改进其技术与传播手段，而新兴家族也积极寻求机会，带来新的威胁。例如，Makop和Phobos等老牌家族依然稳步扩散，保持其技术与渠道优势，TargetCompany(Mallox)家族在2024年通过引入新的传播手段，成功跃升为传播量最广泛的勒索软件家族之一。此外，新的勒索家族如RNTC和Anony等，凭借创新的攻击手段迅速崭露头角，首次出现即进入年度Top10榜单，显示出新的威胁正在崛起。

国内勒索软件形势依然严峻，随着Web漏洞作为主要传播手段逐渐被新老勒索软件家族广泛应用，许多依赖Web服务的企业OA系统、财务软件和管理软件已成为政企单位遭受勒索攻击的主要入口。2024年，国内多个金融和能源领域企业遭遇勒索攻击。与此同时，港台地区及部分跨国贸易企业仍频繁遭遇勒索事件。知名企业如Halara和PandaBuy因数据泄露而遭受勒索，而宏碁和酷冷至尊等IT企业也因数据外泄面临勒索威胁。此外，闻泰科技收购的荷兰芯片制造商Nexperia在2024年遭遇疑似由Dark Angels勒索软件发动的攻击，并收到了赎金威胁。

通过对2024年勒索软件样本的深入分析及攻击案例的溯源研究，我们发现，尽管勒索软件的整体技术架构未发生根本性变化，但在具体实现层面，各家族持续进行优化与改进。为了提高入侵效率和成功率，越来越多的勒索软件家族开始采用软件漏洞、web漏洞作为主要入侵手段。同时，为了进一步提升勒索成功率，许多新兴及传统勒索家族已开始广泛采用

双重勒索或多重勒索策略。值得注意的是，一些极端勒索团伙已明确表示将放弃传统的文件加密方式，转而专注于数据窃取，将数据泄露作为勒索的主要筹码。

值得关注的是，随着AI技术的快速发展和广泛应用，勒索软件在AI的助力下不断更新迭代，更新速度更快，入门门槛更低。未来，AI驱动的勒索攻击将成为我们必须面对的一大安全威胁。与此同时，AI在安全领域的应用也取得了显著进展，各大安全公司纷纷推出结合AI技术的产品和服务。展望未来，能够有效利用AI技术的组织，将在与勒索软件及其他网络威胁的对抗中占据主动。因此，AI无疑已成为当前勒索软件攻防演化中的核心热点。

2024年,360反勒索服务共处理了超过2151例勒索攻击求助，发现77个新勒索家族，其中多重勒索家族38个约占一半，拦截43.1亿次网络暴破攻击，保护近270万台设备免遭入侵，协助约3996设备完成勒索解密。

2024年，通过我们的勒索预警订阅服务，基于360全网安全大数据视野，监测勒索攻击的多个环节，在勒索攻击的准备阶段，以及病毒初始投递阶段，对监管、企业用户提供勒索预警订阅服务。希望在勒索的前期阶段，进行阻断，避免造成受害单位的进一步损失。2024年共计捕获勒索攻击事件线索5863起，涉及受害单位2148家，确认勒索病毒家族59个，攻击IP来源地涉及境外54个国家或地区，配合监管输出勒索攻击事件线索658起，覆盖全国多个地区。

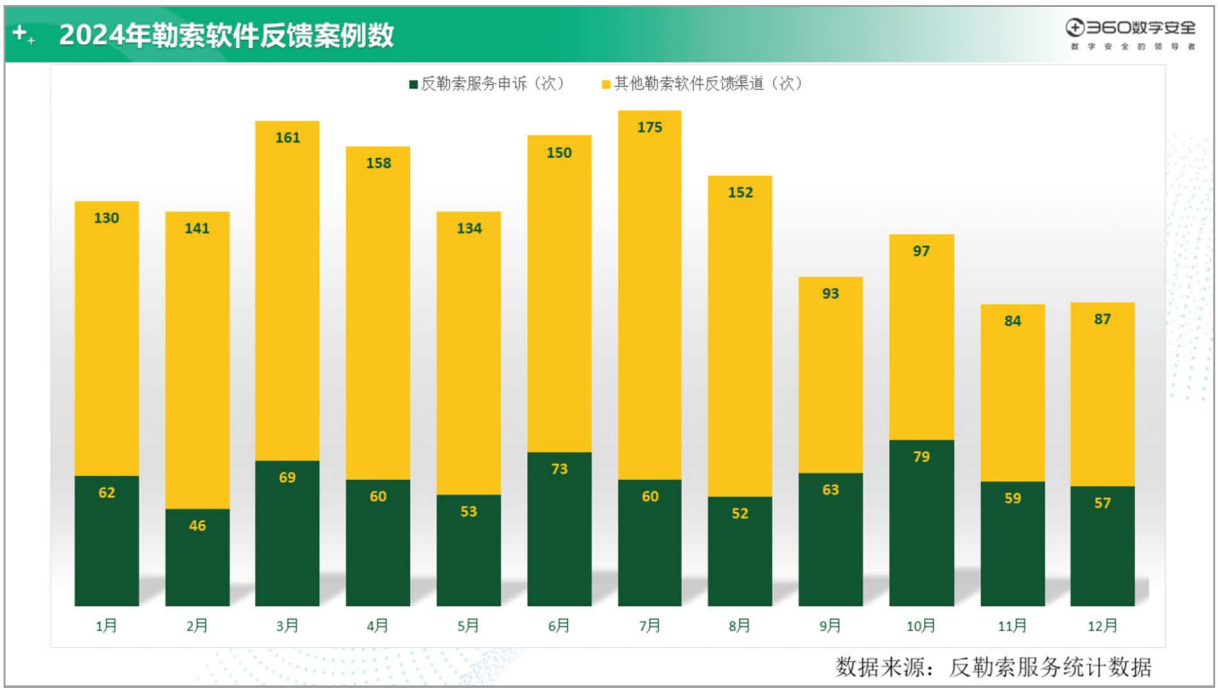
本章将对2024年全年，360政企安全检测到的勒索软件相关事件与数据进行分析，并进行解读。

# 一

# 勒索软件概况

2024年全年，360反勒索服务平台、360解密大师两个渠道，一共接收并处理了超过2151位遭遇勒索软件攻击的受害者求助。这其中来自企业用户的求助占比有较为明显的上涨，与个人受害者相比，组织单位受攻击后所影响的设备数量、造成的损失程度以及勒索金额通常更为严重。勒索软件针对企业的影响正在进一步加深，社会整体面临的勒索软件威胁依旧严峻。

下图给出了在2024年全年，每月通过360安全卫士反勒索服务和360解密大师渠道提交申请并最终确认感染勒索软件的有效求助量情况。

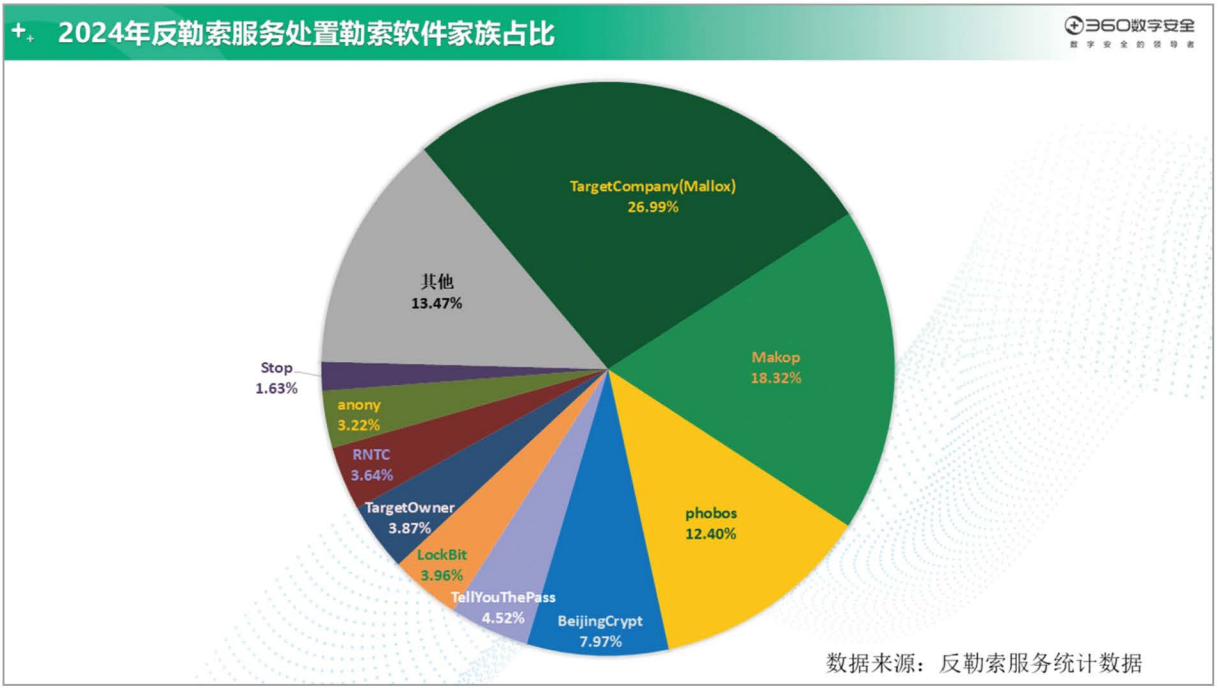



与近几年情况类似，2024年整体勒索反馈量同样呈现相对平稳的趋势。与以往略有不同的是，2024年春节假期在2月，往年2月春节会导致各类办公设备的开机总时长有较大幅度降低，进而导致在这段时间内即便遭到勒索攻击也会出现由于相关人员休假而未能及时发现等情况。但2024年2月的反馈量却并无明显降低。根据相关数据分析，这可能与Black

Basta、LockBit、Play、BlackCat等一些较为成熟且具有一定规模的勒索家族在年初时较为活跃的攻击表现有关，但所幸由于近年来大家在防范勒索方面的安全意识提高，国内并未出现较为严重的勒索事件。而在后续的数月中，各月的月度反馈量总体相对平稳，并未出现大规模波动情况。

## （一）
## 勒索家族分布

下图给出的是根据360反勒索服务和360解密大师数据所计算出的2024年勒索软件家族流行占比分布图。




其中，PC端系统中TargetCompany(Mallox)、Makop和phobos这三大勒索软件家族的受害者占比最多，都属于老牌勒索家族。TOP10家族中值得注意的有下面几点：

1、TargetCompany(Mallox)一直以来都是传播量较大的传统勒索软件家族之一，且其反馈量持续处于较高水平。到2024年，该家族已开始吸纳其他勒索软件家族的传

播渠道，并在自身传播方式中新增了Web漏洞利用途径。结合其原有的广泛传播网络和庞大的感染设备基础，使得这一勒索软件家族在2024年成为了最具威胁的勒索软件之一。

2、Makop作为另一老牌勒索软件家族，在2024年的反馈量排名跃升至第二位。尽管今年该家族未发生大规模的爆发性攻击事件，也未采用过于复杂的传播手段，但其扎实的技术积累使得其在入侵受害者系统后能够与安全防护软件进行有效对抗。特别是在内核攻击与防御技术方面的深入研究，使得Makop具备了较高的生存能力和入侵成功率，成为其他家族难以企及的对手。

3、Phobos作为排名靠前的勒索软件家族之一，拥有较长时间的传播历史。然而，2024年该家族首次跌出了反馈量排名的首位，预计这一变化与其传播方式的相对单一性密切相关。尽管如此，Phobos仍以第三位的反馈量占比保持强劲的攻击势头，且在传播和加密技术方面依然表现成熟稳定，因此仍需对其持续保持高度警惕。

4、TellYouThePass勒索软件家族延续了2023年的攻击势头，依然是勒索软件攻击中的活跃参与者。该家族主要通过利用OA系统、财务软件以及基于Web技术开发的企业管理软件中的漏洞进行传播，并通常选择在周末或其他非工作时间发起攻击。通过在管理人员休息期间实施集中的突袭，极大地提高了入侵成功率。尽管随着Web漏洞的修复，TellYouThePass在2024年的反馈量占比仅为4.5%，其依然稳居第五名，表明该家族的威胁依然不可忽视。

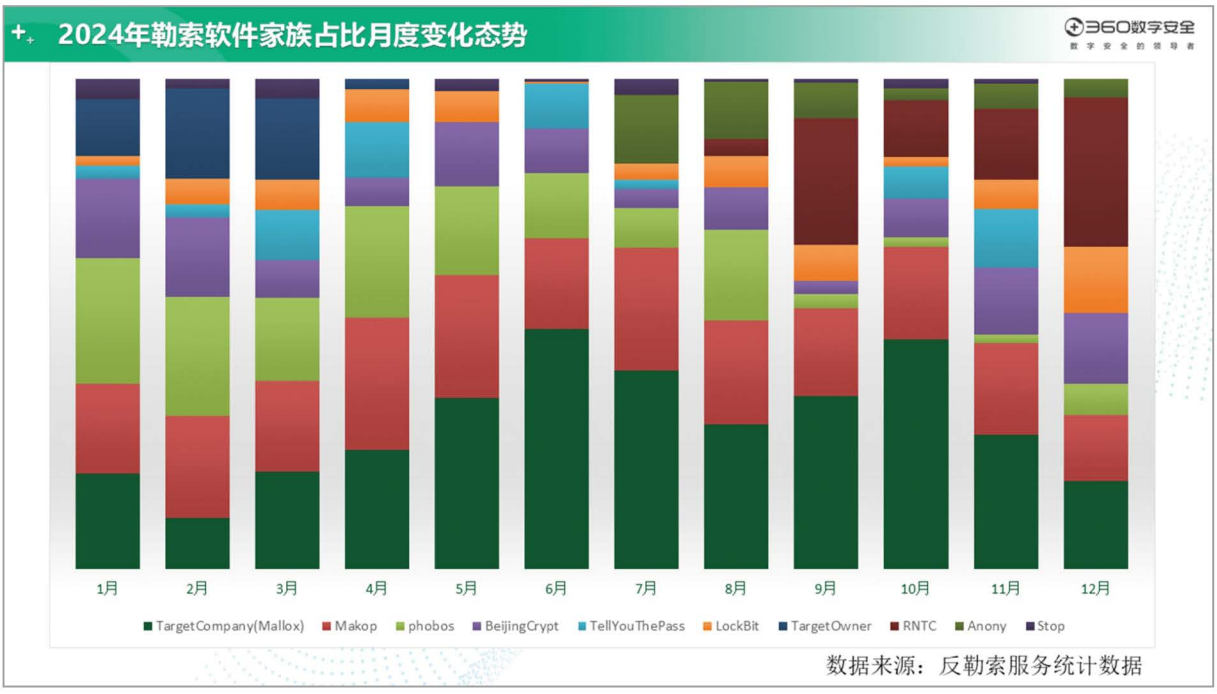
5、RNTC和Anony作为新兴勒索软件家族，分别位列2024年反馈量的第八和第九位。尽管这两个家族在传播途径和加密技术上并未展现出特别的创新，但它们依靠弱口令入侵等简单、粗暴但有效的手段迅速进入了安全领域的视野。此类攻击方式反映出勒索软件攻击手段的逐步标准化，犯罪分子只需利用现有的成熟技术方案，就能轻松复制以往的成功模式，从而为不法分子带来利益，同时给社会安全带来严重的风险。

## （二）
## 主流勒索软件趋势

我们汇总了2024年各月勒索软件家族的月度感染量TOP10数据，发现通过传统弱口令等相对基础的传播手段进行扩散的Makop和Phobos勒索软件家族，尽管其感染量持续较高，但整体波动较为平稳。这些家族展现了典型的稳定性，未出现剧烈的波动。而与之形成鲜明对比的是，2024年新出现的勒索软件家族，或是采用了创新传播手段的家族，它们的感染量呈现出更为动态的增长趋势，尤其在某些月份表现出明显的爆发式增长。

其中，TargetCompany(Mallox)勒索软件家族虽然同样属于“老牌”勒索家族，但由于该家族自2024年4月起加入了利用Web漏洞入侵受害者网络的新手段进行传播，所以在下半年出现了一波较为明显的爆发。

传统家族再度发力，新兴家族中自然也有后起之秀。2024年下半年异军突起的anony和RNTC两个勒索软件家族作为今年的“新秀”，更是一经问世便展示出了强大的破坏能力，在年末对各大企业目标展开了一波颇为强劲的攻势。



# （三）
# 加密方式分布

我们对2024年仍在活跃传播且具有代表性的勒索软件家族进行了深入分析，并统计了各家族所采用的编程语言、加密算法及非对称密钥生成方式。部分勒索软件家族曾对其代码进行重构，或针对不同操作系统平台使用了不同的编程语言，因此在编程语言这一项中，某些家族可能出现多种编程语言的使用。为了加密文件，这些家族采用了多种技术手段，包括但不限于RSA、Curve25519、AES、ChaCha20、Salsa20等算法。以下是各家族采用的具体情况：

| 家族名称 | 编译语言 | 加密算法 | 非对称密钥生成 |
|---|---|---|---|
| LockBit | C++ | RSA1024+ChaCha20 | 内置RSA-1024公钥 |
| Mallox | C# | Curve25519+AES128/ChaCha20 | 内置Curve25519公钥 |
| BlackMatter | C++ | RSA1024+Salsa20 | 内置RSA-1024公钥 |
| Cuba | C++ | RSA1024+ChaCha20 | 内置RSA-1024公钥 |
| RansomEXX | Rust | RSA4096+AES256 | 内置RSA-4096公钥 |
| Makop | C++ | RSA1024+AES256 | 内置RSA-1024公钥 |
| Buran | Delphi | RSA2048/512+AES256 | 内置RSA公钥 |
| phobos | C++、Delphi | RSA1024+AES256 | 内置RSA-1024公钥 |
| Stop | C++ | RSA1024+Salsa20 | 下载RSA-1024公钥 |
| TellYouThePass | C# | RSA2048+AES256 | 内置RSA-2048公钥 |
| Loki | C# | RSA2048+AES256 | 内置RSA-2048公钥 |
| BeijingCrypt | C++ | RSA1024+AES256 | 内置RSA-1024公钥 |
| MedusaLocker | C++ | RSA2048+AES256 | 内置RSA-2048公钥 |
| Thanos | C# | RSA2048+AES256 | 内置RSA-2048公钥 |
| Black Basta | C++ | RSA4096+ChaCha20 | 内置RSA-4096公钥 |

| | | | |
|---|---|---|---|
| Mount Locker | C++ | RSA2048+ChaCha20 | 内置RSA-2048公钥 |
| Play | C、C++ | RSA+AES | 内置RSA公钥 |
| Qilin | Golang、Rust | RAS2048+AES256 | 内置RSA-2048公钥 |
| Qilin.B | Rust | RSA4096+AES256 | 内置RSA-4096公钥 |
| Medusa | C、C++ | RAS2048+AES256 | 内置RSA-2048公钥 |
| Trigona | Delphi | RSA4096+AES256 | 内置RSA-4096公钥 |
| Money Message | C++ | ECDH+ChaCha20 | ECDH生成密钥对 |
| ESXiArgs | C++ | RSA1024+Sosemanuk | 内置RSA-1024公钥 |
| Cactus | C、C++ | RSA4096+AES256 | 内置RSA-4096公钥 |
| 8BASE | C、C++ | RSA1024+AES256 | 内置RSA-1024公钥 |
| INC Ransom | - | Curve25519+AES | 内置Curve25519公钥 |
| Rhysida | Golang、C++ | RSA4096+ChaCha20 | 内置RSA-4096公钥 |
| Hunters International | Rust | RSA4096+ChaCha20 | 内置RSA-4096公钥 |
| FunRansomware | C# | RSA2048+AES256 | 内置RSA-1024公钥 |
| Mimic | | RAS4096+ChaCha20 | 内置RSA-4096公钥 |
| Ransomhub | Golang、C++ | ChaCha20+AES256 | 内置RSA-1024公钥 |
| DoNex | C、C++ | RAS4096+ChaCha20 | 内置RSA-4096公钥 |
| MeowCorp | | RAS4096+ChaCha20 | 内置RSA-4096公钥 |
| Beast | Golang、Delph、C | Curve25519+ChaCha20 | 内置Curve25519公钥 |
| EMBARGO | Rust | Curve25519+ChaCha20 | 内置Curve25519公钥 |
| Cicada3301 | Rust | RSA+ChaCha20 | 内置RSA公钥 |
| Eldorado | Golang | RSA+ChaCha20 | 内置RSA公钥 |
| Elpaco | - | RSA4096+ChaCha20 | 内置RSA-4096公钥 |
| InterLock | - | RSA+AES | 内置RSA公钥 |

| | | | |
|---|---|---|---|
| GoZone | Golang | RSA+ChaCha20 | 内置RSA公钥 |
| LVTLocker | - | RSA+ECC+ChaCha20 | 内置RSA公钥<br>ECC本地生成私钥 |

2024年代表性勒索软件家族编写语言及算法实现方案

通过对2024年勒索软件样本的技术分析，我们发现，尽管当前主流勒索软件家族在核心加密功能方面依然呈现出“技术趋同”的趋势，大多数家族采用了“对称与非对称”的多级加密逻辑，但在具体的“算法实现”层面，2024年却出现了一些新的发展动态：

在非对称加密阶段，Curve25519算法逐渐崭露头角。主流勒索软件家族采用多级加密逻辑的主要原因是平衡加密强度与加密效率。而Curve25519的高效性显著提升了最为耗时的非对称加密过程，相比传统的RSA算法，Curve25519的性能优势更为明显，且加密强度不逊色。

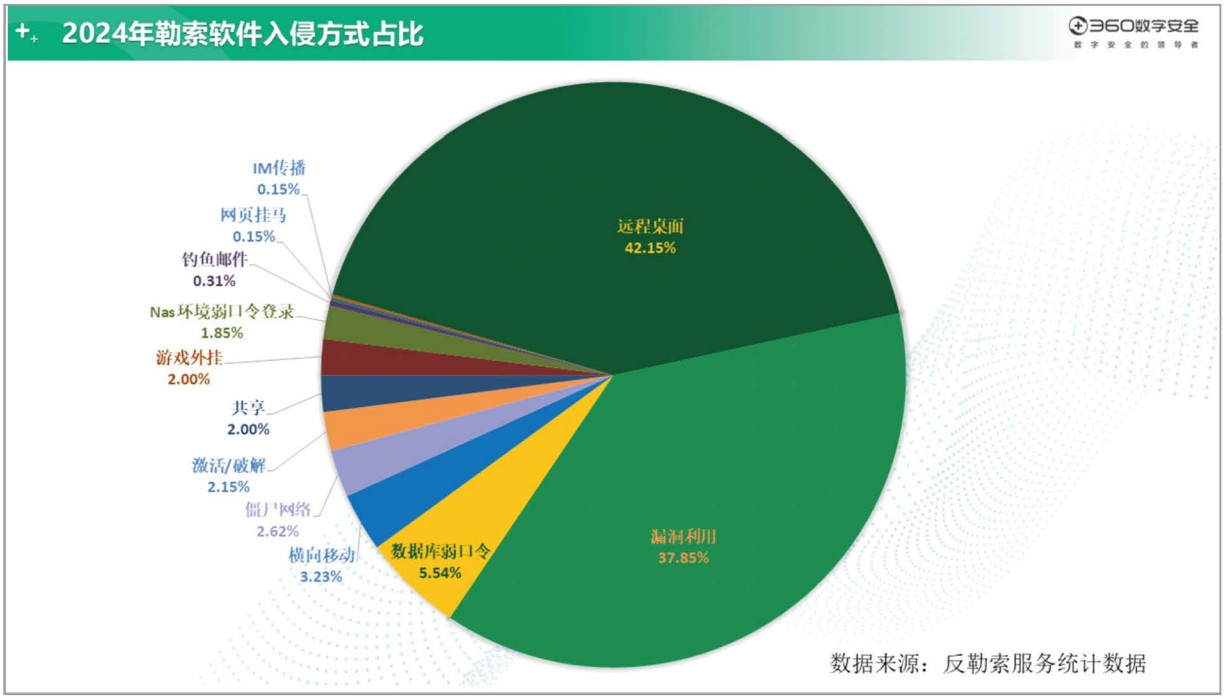
与此同时，ChaCha20、Salsa20、Sosemanuk等对称加密算法也越来越受到青睐。尽管这些算法早已在部分勒索软件家族中被采用，但2024年它们的普及率显著提升，展现出替代传统AES算法的趋势。其高效的加密能力使得这些算法在勒索软件中得到了广泛应用，尤其在对性能要求较高的攻击场景下，优势更加突出。

总体而言，多级加密作为一种成熟的加密方案，已在效率和安全性之间达到了较为理想的平衡，各家族在这一标准框架内的技术实现已得到充分验证。然而，值得注意的是，勒索软件家族的开发者并未停止对核心加密技术的优化，算法实现层面的效率提升已成为各家族优化代码的共同方向。

# 二

# 勒索软件传播方式

下图展示了2024年攻击者在投放勒索软件时所采用的各种入侵方式的占比情况。根据统计可以观察到：远程桌面入侵仍然是导致用户计算机感染勒索软件的主要途径；而与往年不同的是，今年利用漏洞对目标网络实现入侵的占比有了非常明显的增加，虽然总体占比仍位居第二，但与传统通过远程桌面入侵量的占比已相差无几，说是并列第一也并不为过。




通过对勒索软件在2024年的具体传播案例进行分析，发现位列前三的传播与入侵方式呈现出当前占比分布情况的主要原因如下：

### 1、远程桌面入侵

通过远程桌面入侵依然是国内最频发的勒索攻击手段。此类攻击手段由来已久，有着一套非常成熟的入侵方案和现成工具软件。同时，数量众多的中小型企业也始终未对这类安全隐患采取有效的防范措施，也是让远程桌面入侵常年稳居最受攻击者青睐的入侵手段榜首的重要原因。

### 2、漏洞利用

2024年通过漏洞利用发起的勒索攻击量有着非常大幅的增加。而在各类应用的漏洞利用中，针对Web应用或嵌入Web组件的各类管理系统的漏洞攻击是所有漏洞利用类攻击中的重灾区。使用这类攻击手段的典型代表是TellYouThePass家族，而该家族自2023年出现以来就一直是勒索软件界的活跃分子，其在2024年的攻击势头自然也是未见放缓。

此外，亦如前文所述，以TargetCompany(Mallox)为代表的一些勒索软件家族也在2024年新增了利用Web漏洞来入侵目标网络的手段。这类勒索软件家族本就有着较为完善的分发体系和感染基数，今年又利用Web漏洞对各类服务器应用和嵌入了Web代码的企业管理软件发起攻击。也进一步扩大了这些传统家族的传播数量，同时自然也拉高了漏洞攻击的占比。

### 3、数据库弱口令

与远程桌面入侵清醒类似，数据库弱口令问题也是中小型企业——甚至一些大型企业中较为官方存在的安全隐患。不过相对而言此类入侵方式的效率较低并且对入侵者的“字典规模”有着一定的要求，所以此类攻击的总体占比并不像远程桌面入侵一样夸张。

令人欣慰的是，随着现在各企业对内的安全培训制度完善，此类隐患也相对容易防范，故此数据库弱口令入侵在2024年的总体占比情况有着较为明显的下降。

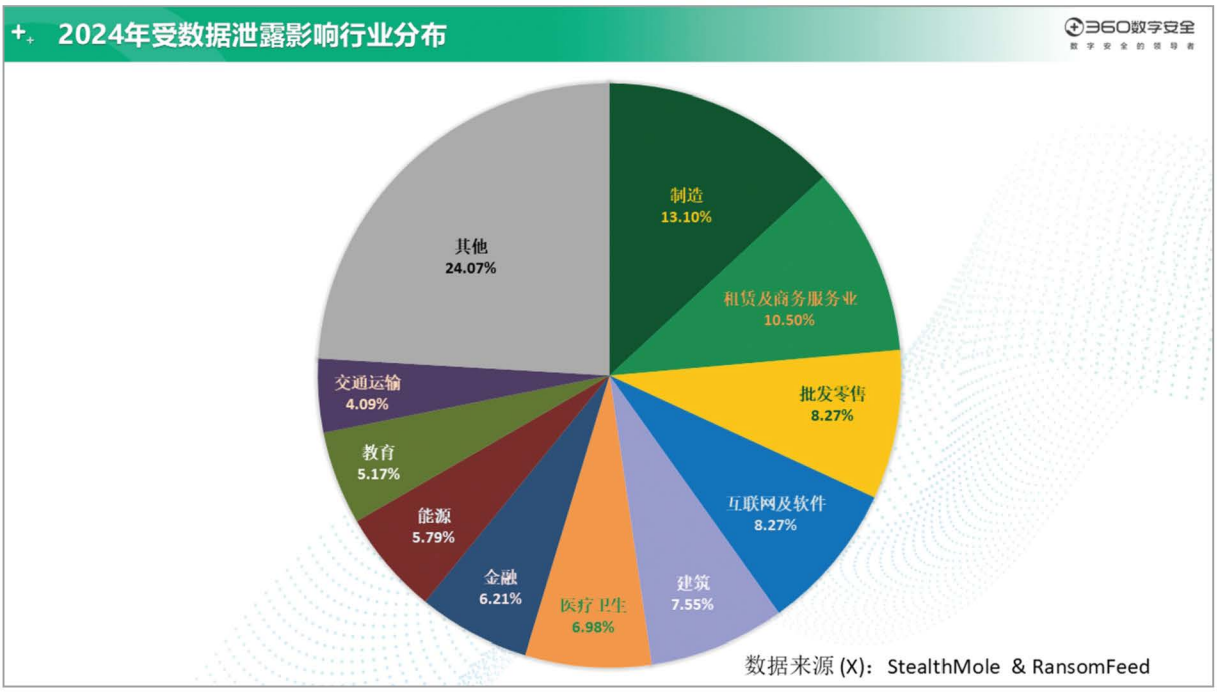
# 三
# 多重勒索与数据泄露

近年来，通过双重勒索或多重勒索模式获利的勒索软件攻击团伙越来越多。在2024年甚至有勒索软件家族宣称要放弃传统的加密手段，而仅进行数据窃取来实现对政企受害者的勒索攻击。

本章将对StealthMole和RansomFeed提供的数据进行多种维度的分析，展现多重勒索与数据泄露问题在勒索攻击中的发展态势。

## （一）
## 行业统计

从受数据泄露影响的行业分布来看，今年受影响的各行业分布占比显得更为平均。其中，制造业、租赁和商务服务业、批发零售业、互联网及软件位列前四。虽然前四的行业较

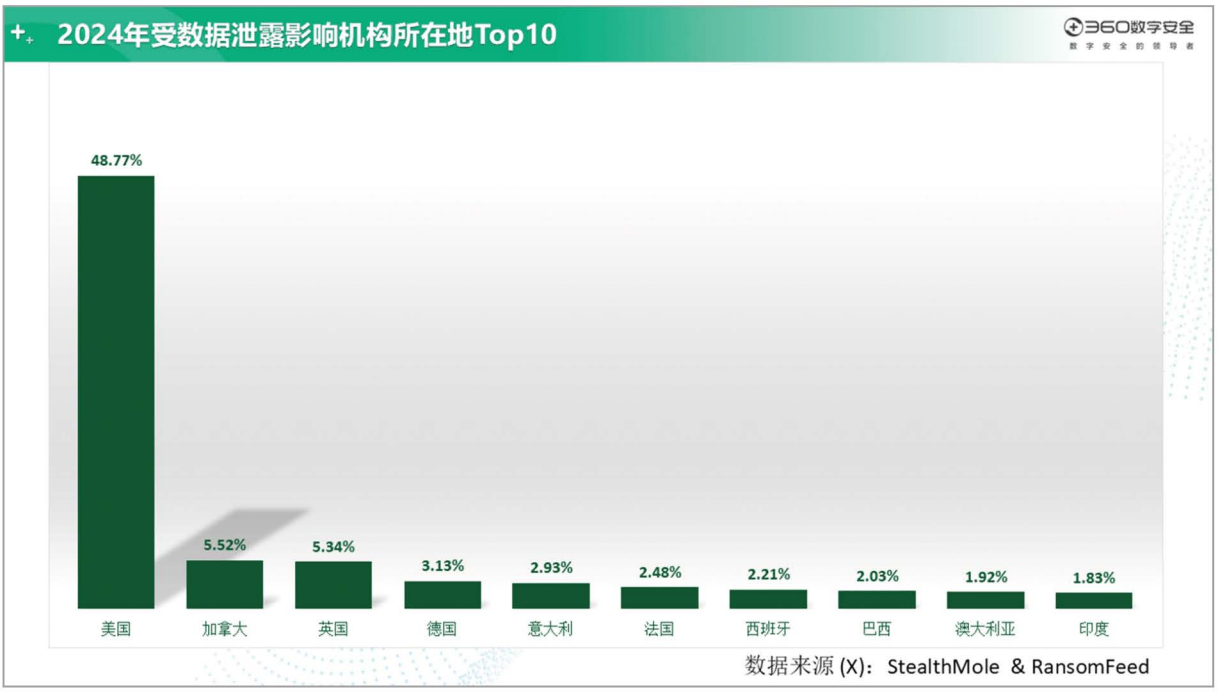


之往年变化不大，但其占比与往年数据对比，则均有不同程度的下降。当然，这并不意味着这些行业在2024年受到的安全威胁就有所降低，而是由于Web漏洞广泛存在于各类企业管理类软件中，所以针对Web漏洞的入侵量上升也给各个行业带来了一份“众生平等”的安全威胁。

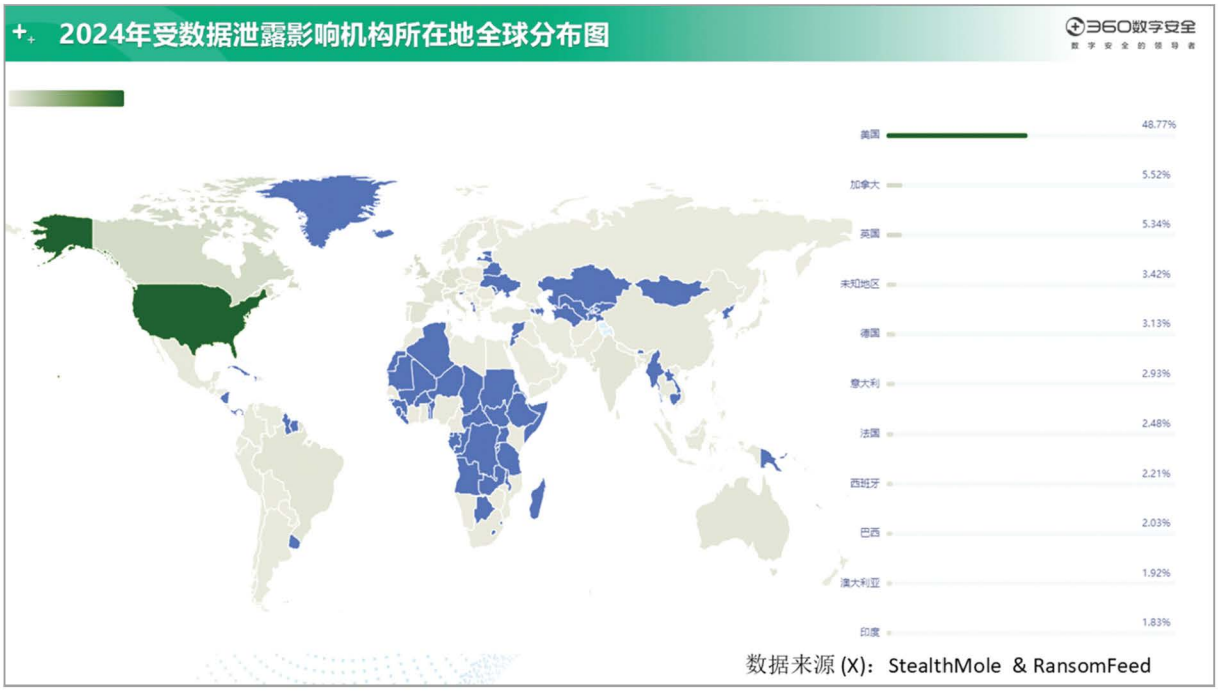
不过，针对能源行业的数据泄露案例有着较为明显的提升，推测这一情况与Web漏洞的入侵方式上升同样有着千丝万缕的关联。能源行业通常规模较大，所以其企业管理系统的应用往往也更为广泛。

## （二）
## 国家与地区分布

从遭到数据泄露机构所在地分布情况来看，美国机构的占比相较于2023年有所升高，但总体波动很小。这可以看作是美国机构在2022年占比下降后的一种常态回归。美国机构常年位居榜首一方面是由于美国网络发达且企业众多，同时也与其发达的云服务产业与设备托管业务有关。



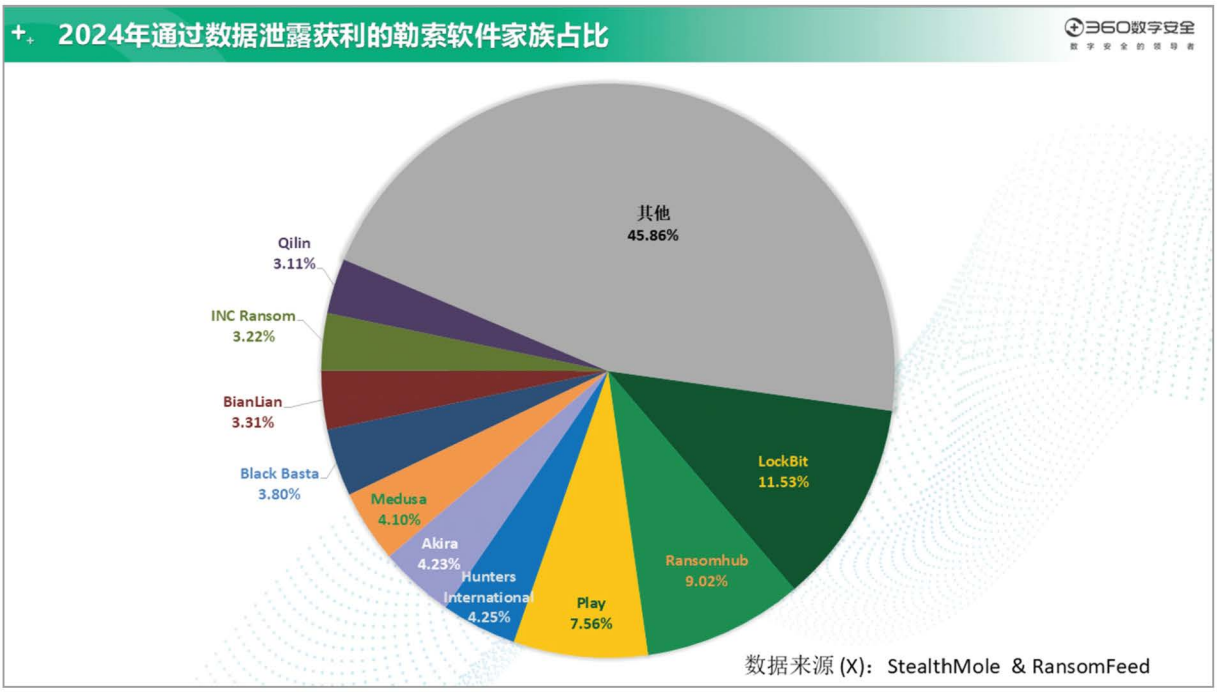
下图为根据全球地区分布数据所绘制的更加直观的地区分布图：




需要说明的是，以上数据来自于各勒索软件的公开数据，各勒索软件家族手中究竟还有多少尚未公开的数据，或是由于已支付赎金等原因导致不会再被公开的数据，外界无从知晓也无法进行统计分析。

## （三）
## 家族统计

2024年参与双重/多重勒索活动的主要活跃勒索软件家族共计94个。家族总量与2023年相比有显著增加，增幅近五成。这一方面是由于有越来越多的勒索软件家族加入到了多重勒索的队伍中，另一方面也是由于新增勒索软件往往更倾向于采取这种更为有效的勒索模式所致。具体的占比分布情况如下图所示。




通过对2024年双重/多重勒索软件的占比分布数据进行分析，不难发现Top10中的各家族占比均有不同程度的下降。而未被列出的“其他”家族占比则有着极大的提升。显然各家族的占比分布更加的平均。这一方面自然是与采取此类勒索手段的家族大幅度增加有关，同时也意味着勒索软件的入侵手段也在日趋成熟和模板化。这让各类新型勒索家族在出现伊始便具有了非常高的入侵成功率。

## （四）
## 逐月统计

从数据泄露的相关统计来看，总体有一定的波动，但并未出现较大规模的爆发现象。


2024年各月的数据泄露机构数量延续了2023年平稳的态势，但在5月和11月出现了两个较为明显的峰值。结合目前已公开的勒索事件判断，5月的高峰数据应与TargetCompany(Mallox)采用了新的入侵手段有关。而年底的一波峰值数据，则主要是受到了今年的新型勒索软件家族RNTC和Anony大范围传播有关。这其中，RNTC在年底的传播量尤为可观。

## （五）
## 赎金

对2024年勒索软件赎金进行跟踪发现，勒索软件攻击的规模和赎金要求达到了前所未有的水平。以下是一些勒索软件家族针对不同组织和企业发起的攻击案例，赎金要求从数百万到数千万不等，凸显了勒索软件攻击的严重性和对受害者的财务影响。

| 勒索家族 | 受害组织/企业 | 赎金 |
|---|---|---|
| BlackCat | LoanDepot | 600万美元 |
| Hunters International | Hoya Optics | 1000万美元 |
| Trigona | Claro | 1000万美元 |
| LockBit | Majorca city Calvi à | 1100万美元 |

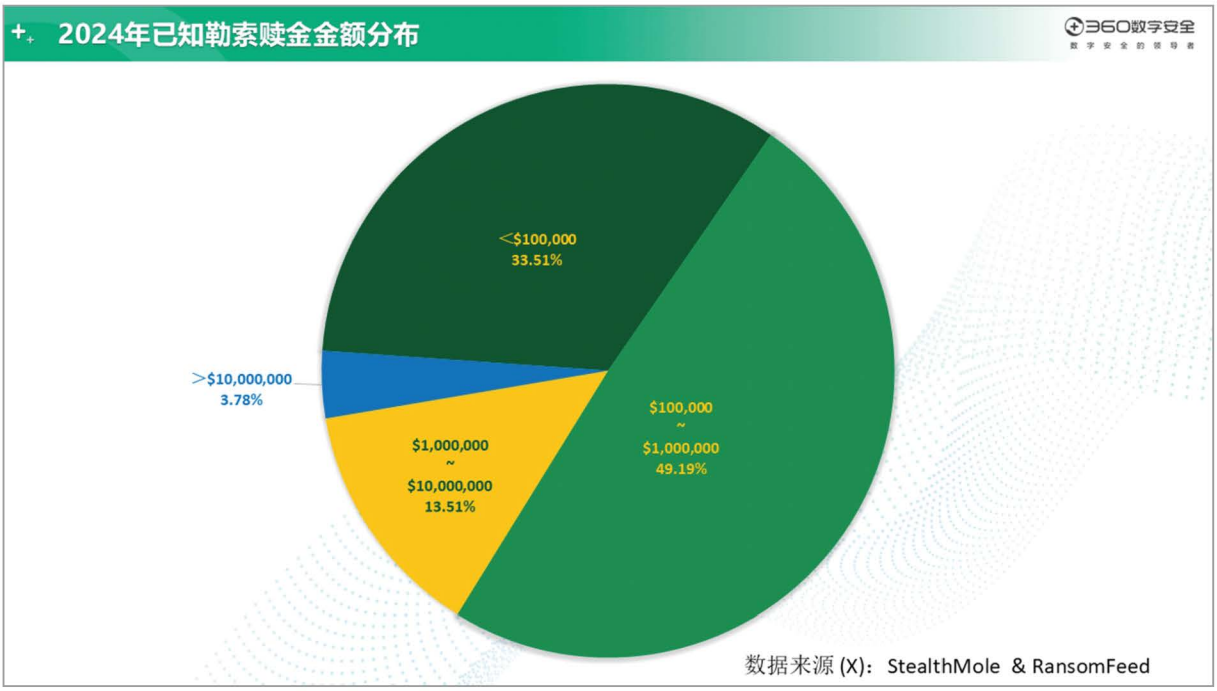
| | | |
|---|---|---|
| BlackCat | Change Healthcare | 2200万美元(已支付) |
| LockBit | London Drugs | 2500万美元 |
| Qilin | Synnovis | 5000万美元 |
| Dark Angels | Cencora | 7500万美元(已支付) |
| STORMOUS | uffs.edu.br | 1200美元 |
| Medusa | Digitel Venezuela | 500万美元 |
| Medusa | Bimbo Bakeries | 650万美元 |
| Trigona | Dinamic Oil | 500万美元 |
| Cactus | ammega.com | 900万美元 |
| LockBit | crinetics.com | 4000万美元 |
| Ransomhub | Frontier | 2200万美元 |
| BlackSuit | CDK Global | 2500万美元(已支付) |
| Cactus | isometrix.com | 4580万美元 |
| DAIXIN | Acadian Ambulance (US) | 700万美元 |

典型勒索攻击事件赎金金额

今年，双重勒索软件攻击首次出现了即使支付赎金数据依然被泄露的案例。UnitedHealth Group的子公司Change Healthcare遭受了BlackCat勒索软件的攻击，导致超过1亿人的敏感个人信息和医疗数据被盗取。据执行此次攻击的BlackCat勒索软件的附属组织透露，赎金高达2200万美元。原本这笔赎金应在附属组织和勒索软件运营商之间分配，但BlackCat却突然关闭，私自侵吞了全部赎金，并实施了退出骗局。

在BlackCat消失之后，该附属组织转而与名为RansomHub的新勒索软件团伙合作，开始泄露部分被盗数据，并要求额外支付费用以防止数据进一步泄露。这一事件最终导致Change Healthcare的数据被公开，成为近年来规模最大的医疗数据泄露事件之一。

通过对赎金金额的总体数据进行统计，发现勒索金额在各个区段内的分布逐步趋于平均：无论是低于10万还是高于1000万的金额，相较于2023年的占比都有比较显著的增加，而居于中段的10万~100万赎金区间占比则有了大幅度的减少。不过，需要说明的是勒索金额超过1千万美元的情况往往仅是一种漫天要价的“起手操作”，通常并不会真的以这个金额成交。大金额勒索事件的最终结果通常是私下和解或被受害者直接无视。




## （六）
## 泄露取数据波及范围

受害组织/企业拒绝支付赎金后，勒索软件运营团伙会选择在其数据泄露站点(DLS)上传窃取到的全部数据，通过对这部分数据分析发现，2024年的勒索软件攻击事件波及了数百万计的个人和组织，泄露的数据量之大、影响范围之广。这些数字不仅代表了数据泄露的规模，更揭示了勒索软件攻击对个人隐私和企业安全的广泛影响。数据泄露的危害不容小觑，它可能导致身份盗窃、金融欺诈、商业机密泄露，甚至影响到国家安全。以下是2024年部分被攻击案例数据泄露波及人数的统计。

| 勒索家族 | 受害组织/企业 | 波及人数 |
|---|---|---|
| BlackCat | Change Healthcare | 100,000,000 |
| LockBit | Evolve Bank & Trust | 7,600,000 |
| Cl0p | U.S. govt agency CMS | 3,100,000 |
| BlackCat | Prudential Financial | 2,500,000 |
| RansomHub | Rite Aid | 2,200,000 |
| BlackCat | LoanDepot | 1,600,000 |
| BlackCat | Fidelity National Financial | 1,300,000 |
| RansomHub | Patelco | 1,000,000 |
| BlackSuit | Young Consulting | 950,000 |
| Rhysida | Singing River Health System | 900,000 |
| RansomHub | Frontier Communications | 750,000 |
| RansomHub | City of Columbus | 500,000 |
| RansomHub | Christie's | 500,000 |
| 3AM | Kootenai Health | 460,000 |
| Money Message | Anna Jaques | 300,000 |
| BlackCat | Henry Schein | 160,000 |
| Rhysida | MarineMax | 125,000 |
| LockBit | Community Clinic of Maui | 120,000 |
| BlackCat | Jewish Home Lifecare | 100,000 |
| INC Ransom | Access Sports | 88,000 |
| RansomHub | Christie's | 45,000 |

典型勒索攻击事件波及人数

# （七）
# 数据泄露的多重影响：商业、法律与声誉风险

随着数字化和信息化时代的到来，数据已经成为企业最重要的资产之一。然而，随着信息技术的飞速发展，数据泄露事件的发生频率也在不断上升，给企业带来了深远的影响。这些影响不仅限于直接的经济损失，更多的是涉及到企业的声誉、合规性、运营连续性等多个层面。在勒索软件攻击等网络安全威胁日益增多的背景下，数据泄露已成为全球范围内各行各业面临的严重问题。

近年来，传统的勒索攻击模式——通过加密关键数据要求赎金，已经不再是唯一的攻击手段。随着勒索软件的演变，数据勒索成为了一种更加复杂和具有破坏性的攻击方式。企业在遭遇数据泄露后，不仅要应对数据的泄漏和加密问题，还要面对可能来自攻击者的多重威胁和敲诈。为了帮助企业全面了解数据泄露带来的潜在风险，本章将从多个维度剖析数据泄露的负面影响及应对策略。

## 声誉风险：品牌形象受损与客户信任危机

声誉风险是数据泄露带来的最直接后果之一。当企业的数据遭到泄露或篡改时，客户和公众对企业的信任度会大幅下降。攻击者通过多种方式加剧这种信任危机，通常采取以下手段：

- **直接威胁客户**

  在数据被泄露的情况下，攻击者会利用盗取的数据直接联系客户，警告其个人信息可能已被泄露。例如，攻击者可能通过电子邮件、电话等方式通知客户，要求其尽快采取措施保护个人信息，或要求客户支付一定费用以防止进一步的信息泄漏。通过这种方式，攻击者不仅增加了受害者的心理压力，还有效削弱了客户对企业的信任度。

- **操控媒体舆论**

  攻击者通过与媒体的合作，扩大数据泄露事件的曝光度。在一些情况下，勒索团伙甚至建立了自己的媒体关系，主动向记者透露攻击细节，确保事件得到广泛报道，放大舆论效应。通过这些手段，攻击者不仅在经济上获得勒索收益，还在社会层面加大了

对企业的压力。攻击者可能将这些新闻报道链接嵌入赎金页面，迫使企业在公众的强大压力下妥协。

这些攻击方式能够迅速放大企业的危机，并引发公众的不信任，进而影响客户忠诚度和市场份额。对于企业来说，一旦品牌声誉受损，恢复的过程通常需要数年甚至更长时间。企业应在数据保护和网络安全方面投入足够资源，避免数据泄露事件的发生，同时建立危机公关机制，在发生泄露事件时能够及时、有效地管理舆情，减少声誉损失。

## 数据竞拍：非法数据交易的经济驱动

随着数据泄露事件的不断升级，非法数据交易市场逐渐成熟，勒索团伙不仅通过勒索获得赎金，还通过数据竞拍获得额外的经济收益。数据竞拍已经成为许多勒索团伙的常见手段，通常包括以下几种情况：

### ●数据拍卖

勒索团伙会通过建立专门的黑市网站或平台，公开拍卖窃取的数据。这些数据通常包括企业的敏感信息、客户资料、内部文件等。一些团伙甚至会设置竞拍机制，将窃取的数据以高价售卖给其他犯罪分子、竞争对手或第三方公司。通过这种方式，勒索团伙不仅增加了经济收益，还加剧了受害企业的压力，使其不得不尽早支付赎金，避免数据进一步流出。

### ●案例分析

以Rhysida团伙为例，该团伙通过非法竞拍获得了巨额收益。例如，Rhysida团伙以340万美元的价格售卖了从芝加哥卢里儿童医院泄露的数据，并以30比特币（约合190万美元）的价格拍卖了从俄亥俄州哥伦布窃取的6.5TB数据。这些团伙通过拍卖的方式获得了极高的利益，同时也让受害企业面临了前所未有的威胁。

这些现象显示出非法数据交易市场的繁荣，企业不仅面临赎金的威胁，还可能因数据被公开交易而遭受更大的商业损失。因此，企业在网络安全建设中，必须加强对敏感数据的保护，减少数据泄露的可能性，并对数据的流向进行有效监控。

## 合规压力：法律法规的严格要求

随着全球范围内网络安全法规的不断完善，企业在遭遇数据泄露事件时，必须面对更加严格的法律和合规压力。许多国家和地区对数据泄露事件的报告要求已经变得愈加严格，企业如果未能及时报告，可能会面临严厉的罚款和法律后果。

### ●隐瞒事件的后果

许多企业在遭遇勒索软件攻击或数据泄露时，可能会选择隐瞒事件，试图通过支付赎金解决问题，而不向公众或监管机构报告。这种做法虽然可能暂时缓解企业的压力，但一旦被揭露，企业将面临更为严峻的法律制裁。例如，南达科他州的一家整形外科诊所（PSASD）因未及时报告数据泄露事件，最终被美国卫生与公众服务部（HHS）处罚50万美元。

### ●案例警示

2023年，生物技术公司Enzo Biochem因数据泄露事件被迫支付450万美元的罚款，涉及超过240万人数据泄露的事件。这一罚款是由纽约、新泽西和康涅狄格州的检察长联合要求的，显示出各州对数据保护和网络安全的高度重视。类似的案例还有英国IT服务公司Advanced，该公司因在2022年遭遇LockBit勒索软件攻击，可能面临高达774万美元的罚款。

企业在面临数据泄露时，必须严格遵守相关法律法规，确保及时向监管机构报告事件，并配合相关调查。通过加强合规性，企业可以避免不必要的罚款，同时提升公众和监管机构对企业的信任度。

## 业务中断：运营能力的系统性受损

数据泄露事件不仅会导致企业声誉受损，还会对企业的正常运营产生严重影响。在数据被加密或备份失效的情况下，企业的关键业务系统可能无法及时恢复，进而影响日常运营和服务交付。特别是在一些关键行业，数据泄露可能导致灾难性的后果。

**●医疗行业**

美国血液中心OneBlood因遭遇勒索软件攻击，导致血液库存供应受阻，数百家医院不得不启动“血液短缺”应急程序。这一事件突显了数据泄露对公共健康服务的严重影响。在医疗行业，数据泄露可能不仅导致经济损失，还可能对患者的生命健康产生直接威胁。

**●工业和制造行业**

伏特加制造商Stoli集团的美国子公司在遭遇勒索软件攻击后，运营暂停，最终申请破产保护。该事件反映了勒索软件对企业运营连续性的影响，尤其是在供应链管理和生产能力方面的风险。

因此，企业必须采取有效的业务连续性管理措施，确保关键数据和系统能够在数据泄露或攻击事件发生后尽快恢复，以减少对运营的影响。

## 经济损失：直接与间接成本的双重压力

勒索攻击的直接后果是企业需支付赎金，但其经济损失远不止于此。企业还需要承担由于数据泄露导致的业务中断、数据恢复、法律诉讼等一系列间接费用。企业的财务状况可能因此受到严重影响。

**●公开案例**

例如，Johnson Controls和Clorox因勒索攻击所造成的直接和间接经济损失达到数千万美元。此外，勒索软件攻击可能导致企业网站瘫痪，进一步影响客户访问，导致潜在的销售损失。例如，台湾半导体公司Foxsemicon因遭受LockBit攻击，导致公司股价下跌约3%。

| 受害组织/企业 | 赎金 |
| --- | --- |
| LoanDepot | 600万美元 |
| Hoya Optics | 1000万美元 |
| Claro | 1000万美元 |
| Majorca city Calvià | 1100万美元 |
| Change Healthcare | 2200万美元(已支付) |

公开案例中的勒索赎金

## 法律责任：隐私泄露引发的巨额赔偿

数据泄露事件不仅涉及到企业的合规问题，还可能引发客户和员工的集体诉讼，导致企业面临巨额赔偿。在一些情况下，客户对企业未能有效保护个人数据提出诉讼，要求赔偿因数据泄露而产生的经济损失。

**●典型案例**

利哈伊谷健康网络（LVHN）因未支付BlackCat团伙的赎金，导致约13.4万名患者的敏感数据被泄露。泄露的数据中包括未经患者同意拍摄的隐私照片，最终，LVHN与原告达成6500万美元的和解协议，解决集体诉讼。

# 四
# 勒索软件家族更替

## （一）
## 每月新增传统勒索情况

360安全大脑监控到，每月都不断有新的勒索软件出现。以下是2024年每月新出现的传统勒索软件(仅通过加密文件对受害者进行勒索)的部分记录信息，共计31款：

| 月份 | 新增传统勒索软件 |
| --- | --- |
| 2024年1月 | USDLocker,TOLKONEPERDITE |
| 2024年2月 | Mirror,LVTLocker |
| 2024年3月 | - |
| 2024年4月 | Rincrypt,FakePenny,Wormhole,Balloon |
| 2024年5月 | Moneyistime，ShrinkLocker,Phalcon |
| 2024年6月 | RebornRansomware,Anony,PSAUX,DeathGrip,RSAGen |
| 2024年7月 | ShadowRoot,Ymir,Black4Over |
| 2024年8月 | RNTC,Kasper,BaiduLock |
| 2024年9月 | Elpaco |
| 2024年10月 | Hacker Sadism,Weaxor |
| 2024年11月 | XmrData、Frag、Nyxe、MrBeast |
| 2024年12月 | RdpLocker |

2024年各月新增传统勒索软件家族

**针对以上新增勒索软件家族，我们对其中几个典型家族进行具体的说明：**

## USDLocker/TOLKONEPERDITE/Elpaco

USDLocker和TOLKONEPERDITE是Mimic勒索软件家族的两个变种，它们在2024年1月出现，主要针对俄语和英语用户。这两个变种之所以被重新命名，是因为勒索提示信息中有所体现。Mimic勒索软件特别之处在于，它利用了名为Everything的合法工具的API，这是一个由Voidtools开发的Windows文件名搜索引擎，以其高效的搜索能力和资源使用率低而著称。

```
TOLKONEPERDITE Ransomware!!!
ATTENTION!
YOUR PERSONAL DECRYPTION ID -
7vDqxWAlMkYNzcfcRYUV1jbNfTrY5REw28Z6N7r4xxk*TOLKONEPERDITE
At the moment, your system is not protected.
We can fix it and restore your files.
To get started, send 1-2 small files to decrypt them as proof
You can trust us after opening them
2.Do not use free programs to unlock.
OUR CONTACTS:
1) TOX messenger (fast and anonymous)
https://tox.chat/download.html
Install qtox
Press sign up
Create your own name
Press plus
Put there our tox ID:
E9164A982410EFAEBC451C1D5629A2CBB75DBB6BCDBD6D2BA94F4D0A7B0B616F91149
6E469FB
And add me/write message
2)ICQ - @TOLKONEPERDITE
3)SKYPE - TOLKONEPERDITE Decryption
Also we have a temporary mail,pls use it only if neccesary
tolkoneperdite@onionmail.org
```

TOLKONEPERDITE勒索信息

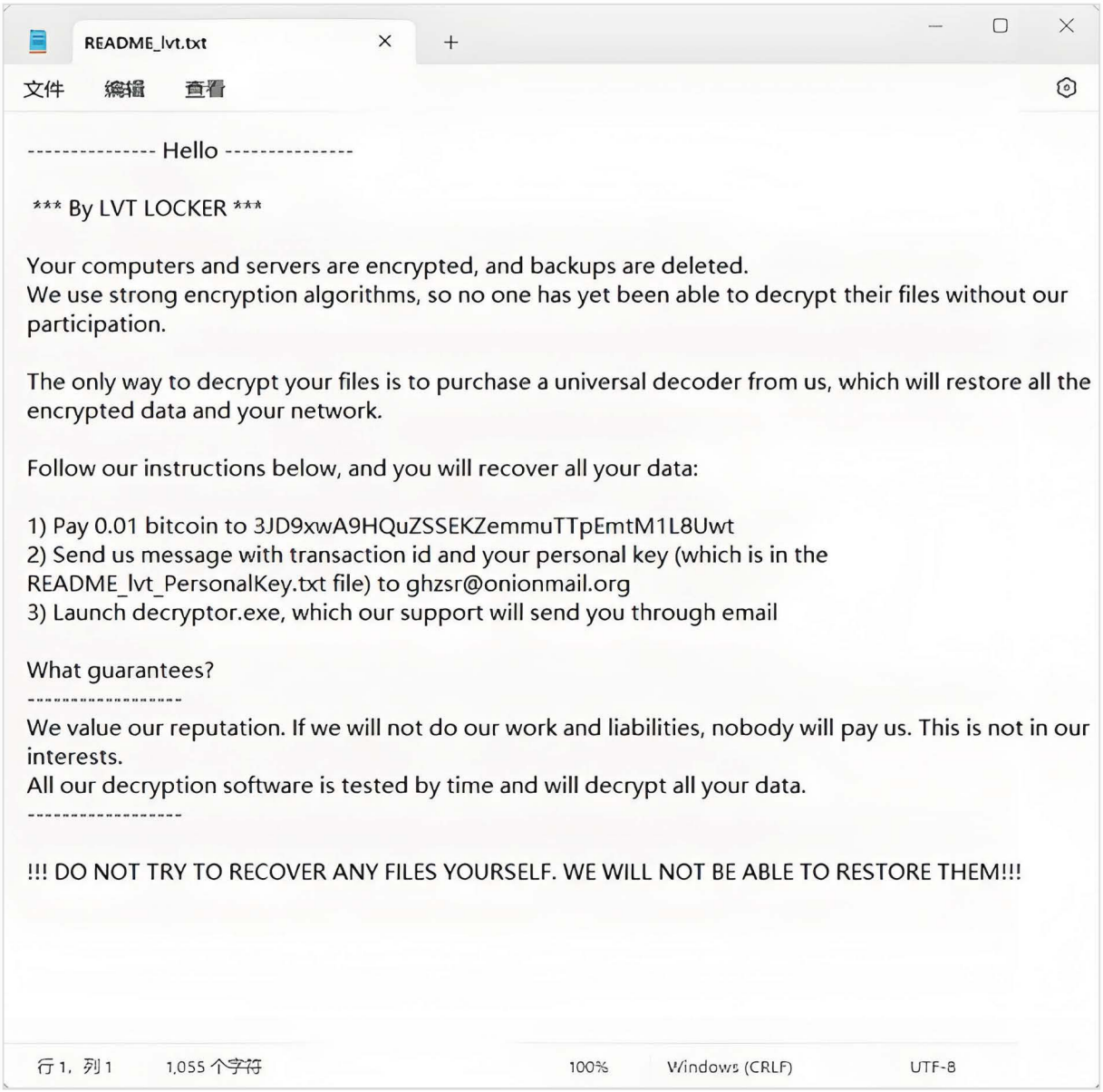
在对Mimic勒索软件进行深入分析时，研究人员发现其部分代码与Conti勒索软件存在关联。Conti勒索软件团伙在俄乌战争期间公开支持俄罗斯，导致内部出现问题，其源代码随后被泄露。这种代码上的相似性表明，Mimic勒索软件可能在某种程度上共享或借鉴了Conti勒索软件的代码。例如，Mimic勒索软件使用了泄露的Conti勒索软件代码来实现访问共享和端口扫描等。

Elpaco虽然也是Mimic勒索软件家族的变种，但该变种出现于2024年8月，但其攻击范围更广，主要集中在美国、俄罗斯、荷兰、德国和法国，然而，其影响并不局限于这些地区，因为在全球范围内，包括加拿大、罗马尼亚、韩国、英国等地也有Elpaco勒索软件的案例报告。在攻击手段上，Elpaco勒索软件延续了通过暴力破解RDP（远程桌面协议）来连接受害者服务器的策略。但与以往不同的是，Elpaco在攻击过程中加入了对CVE-2020-1472（Zerologon）提权漏洞的利用。

## LvtLocker

LvtLocker勒索软件最早出现于2024年2月，是一款基于泄露的Babuk勒索软件源码改编而成的勒索软件。与主流勒索软件相似，LvtLocker在代码中内置了RSA公钥用于加密数据，而对应的私钥则掌握在攻击者手中。在软件激活后，它会在受害者的机器上利用ECC算法生成一对密钥，然后用内置的RSA公钥对ECC私钥进行加密。接着，LvtLocker采用ChaCha20对称加密算法对文件进行加密，这种加密方式因其效率而被主流勒索软件广泛采用。

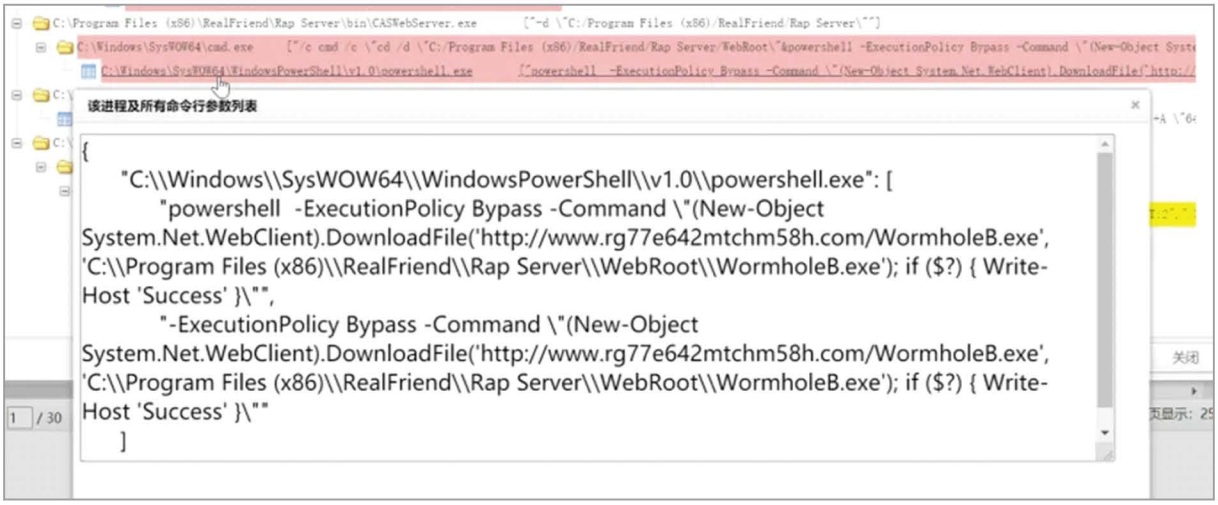
LvtLocker勒索软件在春节期间被发现，它利用国内知名品牌NAS系统的漏洞进行攻击，例如：CVE-2020-28188、CVE-2022-24989和CVE-2022-24990在加密文件后，LvtLocker会留下勒索提示信息，当前版本的赎金要求为0.01个比特币，按照2024年2月的价格约为3700元人民币




LvtLocker勒索信息

## Wormhole

Wormhole勒索软件自2024年4月16日起开始被360安全大脑监控到，它利用了瑞**翼软件中的SQL注入漏洞作为其主要传播手段。这种漏洞允许攻击者在没有适当身份验证的情况下，向数据库注入恶意SQL代码，从而获取对系统的非法访问权限。




Wormhole攻击进程链

目前，360安全大脑已经监测到Wormhole勒索软件有两个主要版本，它们在加密文件后的勒索策略上存在细微差异。

第一个版本在成功加密受害者的文件之后，会在文件名后添加“.locked”的后缀。尽管勒索提示信息中明确指出了0.04比特币（BTC）的赎金要求，受害者仍然有机会通过电子邮件与攻击者进行谈判，以期达成更低的赎金支付或者获取解密密钥。

第二个版本在加密文件后，会在文件名后添加“.Wormhole”的后缀。与第一个版本不同，这个版本的勒索提示信息并没有明确指定赎金的具体金额。受害者只能通过攻击者提供的TOX Id（一个用于点对点通信的标识符）与攻击者进行联系和谈判。这种不透明的做法可能会使受害者在谈判过程中处于不利地位，因为他们缺乏关于赎金金额的明确信息。

## Moneyistime

Moneyistime勒索软件自2024年5月初首次出现以来，已成为中小型企业面临的一个重大威胁。这种恶意软件通过暴力破解技术，专门针对远程桌面协议（RDP）的登录凭据进行破解。一旦破解成功，攻击者便能够获得目标系统的访问权限，并手动部署勒索软件，随后向受害者索取赎金以换取解密密钥。

2024年5月检测到Moneyistime勒索软件的一个新变种。这一新变种的特点是高度定制化，针对每个受害者的不同特点进行个性化定制。具体来说，被加密的文件会被赋予一个带有受害组织或企业名称特征的新后缀，如“.CloverGroup”或“.ZKUNGFU”等。此外，勒索提示信息也进行了定制化处理，不仅包含受害者公司的名称，还包含了根据受害者公司专门创建的电子邮箱地址，这进一步增加了勒索信息的针对性和紧迫感。

Moneyistime勒索软件的操作者采用了一种策略性的方法来增强其勒索效果。他们利用Lightshot这一截图工具，来捕捉被加密设备上的磁盘使用情况，记录了受害组织或企业的网络加密状态。攻击者将这些截图作为证据，上传并保留记录。在与受害组织的代表通过指定的电子邮件地址进行赎金谈判时，这些截图被用作索要高额赎金的有力依据。

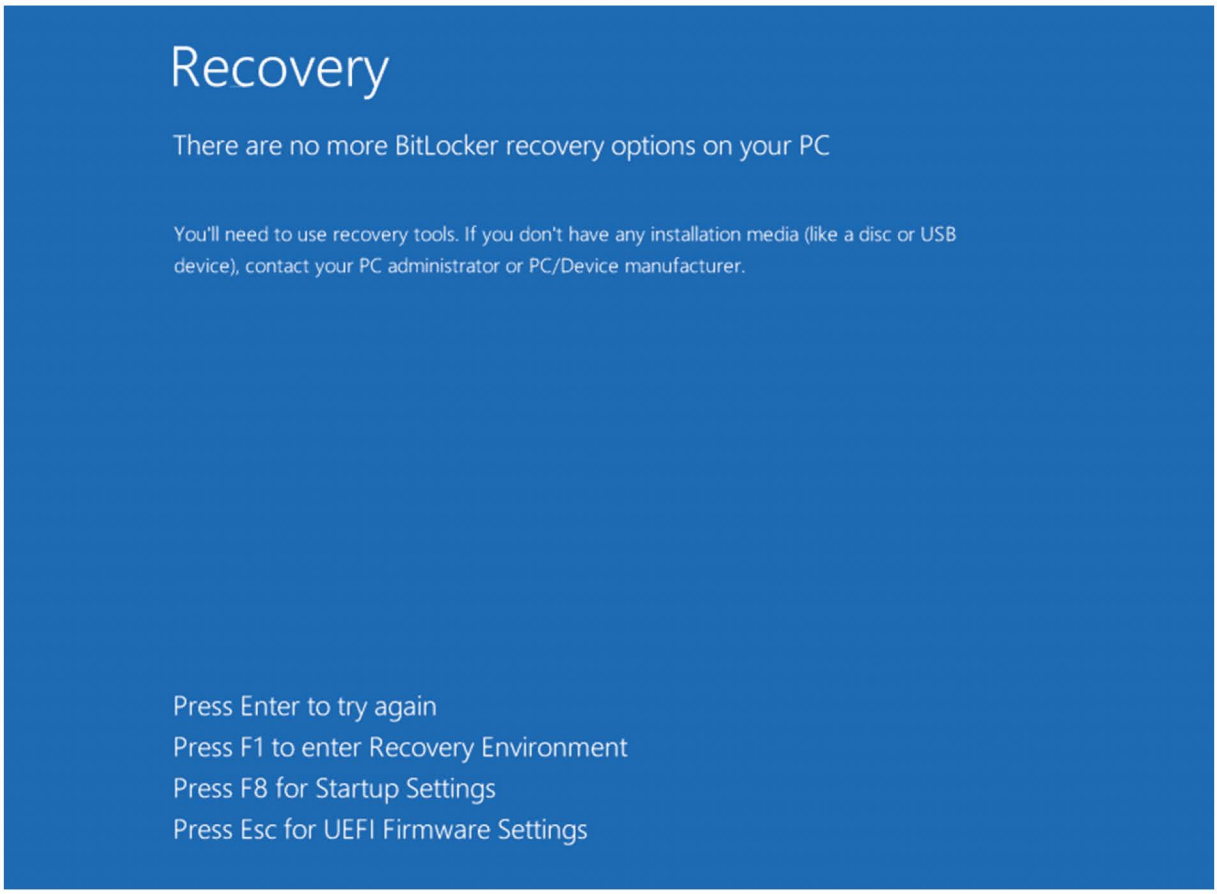

Moneyistime勒索软件或者的截图

## ShrinkLocker

ShrinkLocker勒索软件最早出现于2024年5月，该勒索软件会创建一个新的启动分区，并使用Windows BitLocker加密公司系统。之所以命名为ShrinkLocker，是因为它通过缩小可用的非启动分区来创建启动卷。该恶意程序曾被用来攻击政府实体以及疫苗和制造业的公司。

ShrinkLocker勒索软件仅在满足特定条件时才会继续攻击，例如当前域与目标匹配，

操作系统版本比Vista新。否则，ShrinkLocker会自动结束并删除自身。如果符合攻击条件，它会利用BitLocker加密文件，并通过TryCloudflare攻击将密钥传回。加密完成后，锁定驱动器，没有有效的BitLocker恢复选项。2024年11月，Bitdefender创建并发布了该勒索软件的解密器。




ShrinkLocker调用BitLocker加密系统

## PSAUX

PSAUX勒索软件自2024年6月开始活跃，主要针对Unix/Linux系统发起攻击。通过已知漏洞和配置缺陷瞄准暴露的Web服务器。PSAUX勒索软件通过这些漏洞入侵服务器，并使用名为“ak47.py”的脚本利用这些漏洞，以及“actually.sh”脚本来加密文件。值得庆幸的是，由于PSAUX勒索软件加密算法中存在错误，使得被加密的文件可以免费解密。


PSAUX勒索信息

2024年10月，检测到攻击者利用CyberPanel网站管理平台的漏洞进行攻击，特别是2.3.6和2.3.7版本，这些版本存在多个严重漏洞，包括:

- **CVE-2024-51378 身份验证缺陷漏洞**
- **CVE-2024-51568 命令注入漏洞**
- **CVE-2024-51567 远程命令执行漏洞**

研究人员在2024年10月23日向CyberPanel开发人员通报了该漏洞，CyberPanel的创建者Usman Nasir在收到报告后半小时内宣布发布2.3.8版本，修复了该漏洞，并积极帮助用户更新和解决与消除攻击后果相关的问题。然而，在报告漏洞时，互联网上有超过22,000个未打补丁的服务器。攻击发生后，大多数服务器变得不可用，可能已被破坏并感染了PSAUX勒索软件。

## RSAGen

RSAGen勒索软件最早出现于2024年6月，它是由P2Pinfect僵尸网络发起的，专门针对Linux操作系统。P2Pinfect是一种利用Rust编程语言编写的蠕虫，它通过点对点(P2P)网络进行命令和控制，主要的入侵途径为Redis数据库，入侵成功后会利用Redis执

行功能命令来下发恶意软件;如果Redis这条路“走不通”，蠕虫也会利用内置的弱口令库进行对更多常见程序进行弱口令暴力破解攻击，不断使用常见口令尝试登录各类常用网络服务，而一旦任何一个尝试成功，便可以进入对应设备中进行进一步操作。这种僵尸网络不仅能够部署勒索软件，还能植入加密货币挖矿程序。

RSAGen勒索软件部署成功后，会在临时目录(/temp)生成一个“Your data has been locked.txt”勒索通知文件，文件详细列出了与攻击者联系的两个电子邮件地址，用于受害者与攻击者之间的沟通。此外，文件中会向受害者索要1个门罗币用于换取文件解密。根据本文撰写时的汇率，1门罗币约等于1107人民币。

```
1. Your data has been locked, but not leaked. If you have a backup, you can recover data by yourself.

2. Do not delete these files, the decryption program: /tmp/rsagen, files database: OBa3qL.lockedfiles (in t

3. Your encrypted id(include decryption key):
    ZP/DAKcKbeaL6IrBqz8nHKonYnZwAR1NBLrRMkbVYXzQnKbfqi2Hsam6iGPSFnZSbJQ/dnzSTMGGtLqCIfByf0tnONU51Bbzy/mtr7Z

4. You need to transfer 1.00 monero coin to monero wallet address 463xknx5QEX6akYMpCNnkNdXzv9j16yrF6a6wiDvn

5. You need to send your id and the "monero transaction screenshot" to our mailbox. Once we confirm the tra

6. You can get the monero client from https://www.getmonero.org/, buy or "change" from other cryptocurrency

7. Our email: besttrcovery@firemail.cc,randbnothing@tutanota.com. Any questions are welcome!
```

RSAGen勒索信息

# （二）

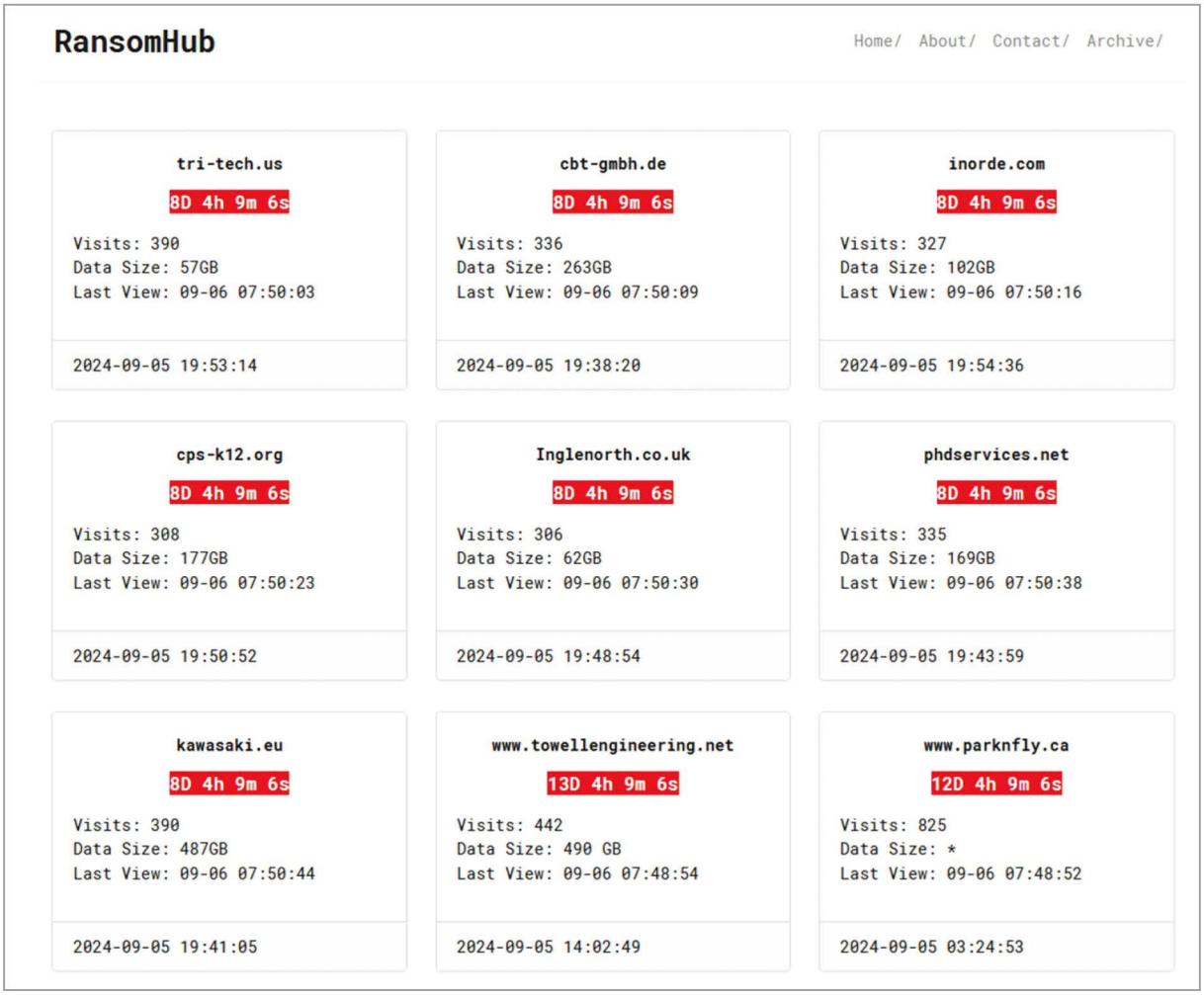
## 每月新增双重、多重勒索情况

另经统计发现，2024年各月也时常出现新的勒索软件加入到双重/多重勒索模式的行列中。仅360安全大脑监控到的此类双重/多重勒索软件家族在本年度就共计新增38个。近年来还出现了具体家族名及出现时间分布如下：

| 月份 | 新增双重/多重勒索软件家族 | 勒索模式 |
|---|---|---|
| 2024年1月 | MorLock | 勒索加密 |
| 2024年2月 | Red Ransomware | 加密文件/数据泄露 |
| | Ransomhub | 加密文件/数据泄露 |
| 2024年3月 | Kill Security | 加密文件/数据泄露 |
| | DoNex | 加密文件/数据泄露 |
| | APT73 | 加密文件/数据泄露 |
| | Eldorado | 加密文件/数据泄露 |
| 2024年4月 | EMBARGO | 加密文件/数据泄露 |
| | Space Bears | 加密文件/数据泄露 |
| | Qiulong | 加密文件/数据泄露 |
| | FSOCIETY | 加密文件/数据泄露 |
| | Pryx | 加密文件/数据泄露 |
| | dAn0n | 加密文件/数据泄露 |
| 2024年5月 | Arcus Media | 加密文件/数据泄露/声誉恐吓 |
| | Zero Tolerance | 加密文件/数据泄露 |
| | Trinity | 加密文件/数据泄露 |

| | | |
|---|---|---|
| 2024年6月 | Cicada3301 | 加密文件/数据泄露 |
| | Brain Cipher | 加密文件/数据泄露 |
| 2024年7月 | Vanir Group | 加密文件/数据泄露 |
| | Lynx | 加密文件/数据泄露 |
| | MAD LIBERATOR | 加密文件/数据泄露 |
| 2024年8月 | Helldown | 加密文件/数据泄露 |
| 2024年9月 | Nitrogen | 加密文件/数据泄露 |
| | InterLock | 加密文件/数据泄露 |
| | Orca | 加密文件/数据泄露 |
| | ValenciaLeaks | 加密文件/数据泄露 |
| | Argonauts | 加密文件/数据泄露 |
| | Chort | 加密文件/数据泄露 |
| | Funksec | 加密文件/数据泄露 |
| 2024年10月 | Sarcoma Group | 加密文件/数据泄露/DDOS攻击 |
| | Dragon Ransomware | 加密文件/数据泄露 |
| | PlayBoy | 加密文件/数据泄露 |
| | HellCat | 加密文件/数据泄露 |
| 2024年11月 | NotLockBit | 加密文件/数据泄露 |
| | Kairos | 加密文件/数据泄露 |
| | Safepay | 加密文件/数据泄露 |
| | Termite | 加密文件/数据泄露 |
| 2024年12月 | Blueox | 加密文件/数据泄露 |

2024年各月新增双重/多重勒索软件家族

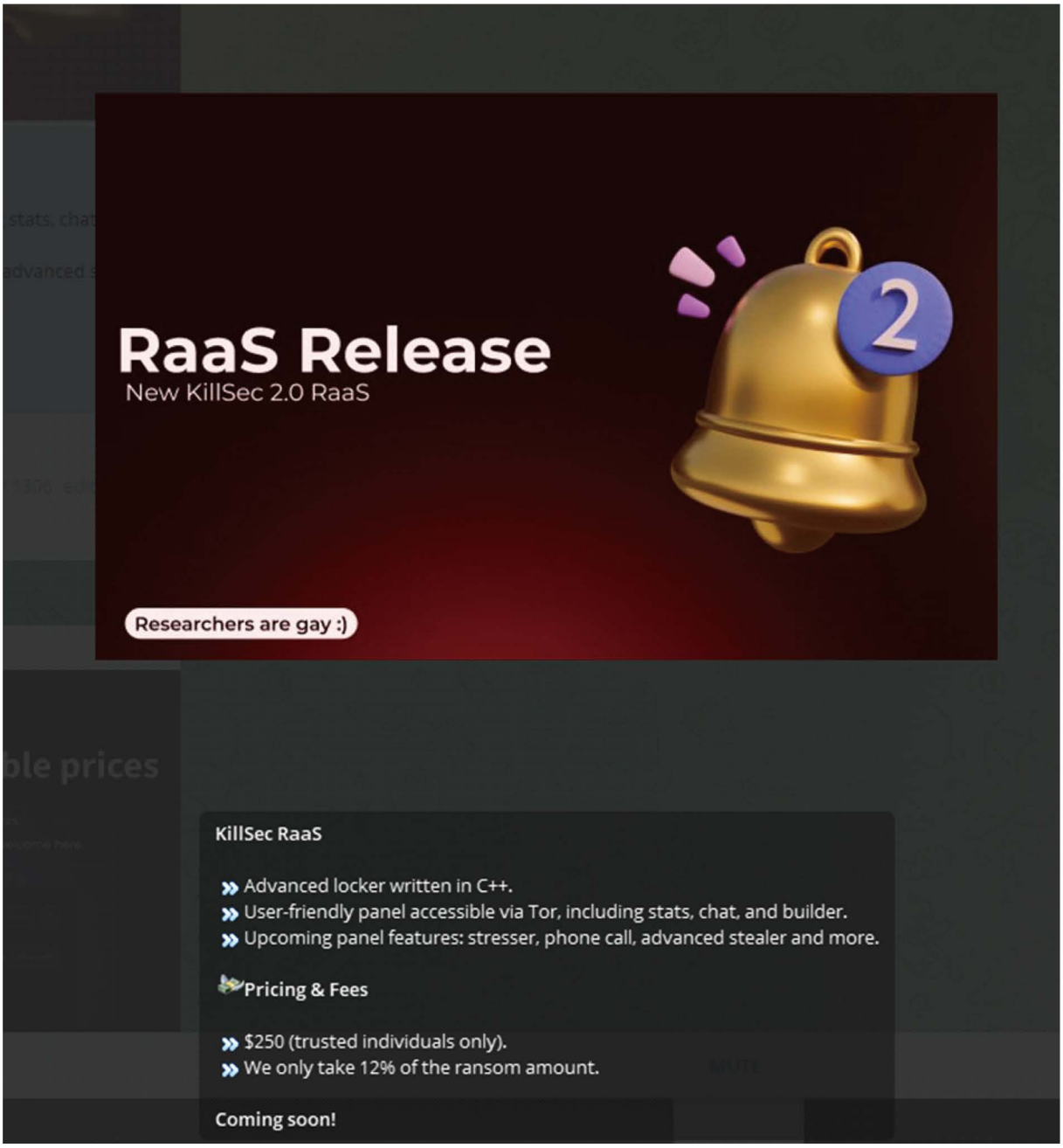



RansomHub勒索信息公开站点

## Kill Security

Kill Security勒索软件又被称作Killsec勒索软件。该组织最初在2023年10月通过其Telegram频道公开招募渗透测试人员和开发人员，但在此阶段并未有勒索活动的记录。直到2024年3月，KillSec勒索软件组织开始活跃，首次在其设立的专用数据泄露站（DLS）公布了受害组织和企业的数据。其受害者涵盖了政府机构、金融行业、互联网企业以及服务行业等多个领域。特别值得注意的是，该组织攻击的目标中包括了多个国家的警察局，例如印度的喀拉拉邦警察局、孟加拉国的拉比赫德以及罗马尼亚的警察局等，但由于该团伙索要的赎金并不高，通常是在1500欧元至10000欧元之间，其攻击的真实性有待考察。

2024年6月25日，Killsec在其Telegram频道推出其最新产品：KillSec RaaS（勒索软件即服务），该服务包括一个可通过Tor网络访问的面板，该面板提供各种功能，包括：统计功能、聊天功能、构建器工具；以及即将推出的：DDoS攻击工具、拨打电话功能、高级窃密工具等。其定价仅为250美元，并承诺后续发布的功能不会再向附属成员索要任何费用，在赎金分成上，Killsec勒索软件组织核心负责人仅收取赎金的12%，剩下的88%由附属机构持有。




KillSec官网页面

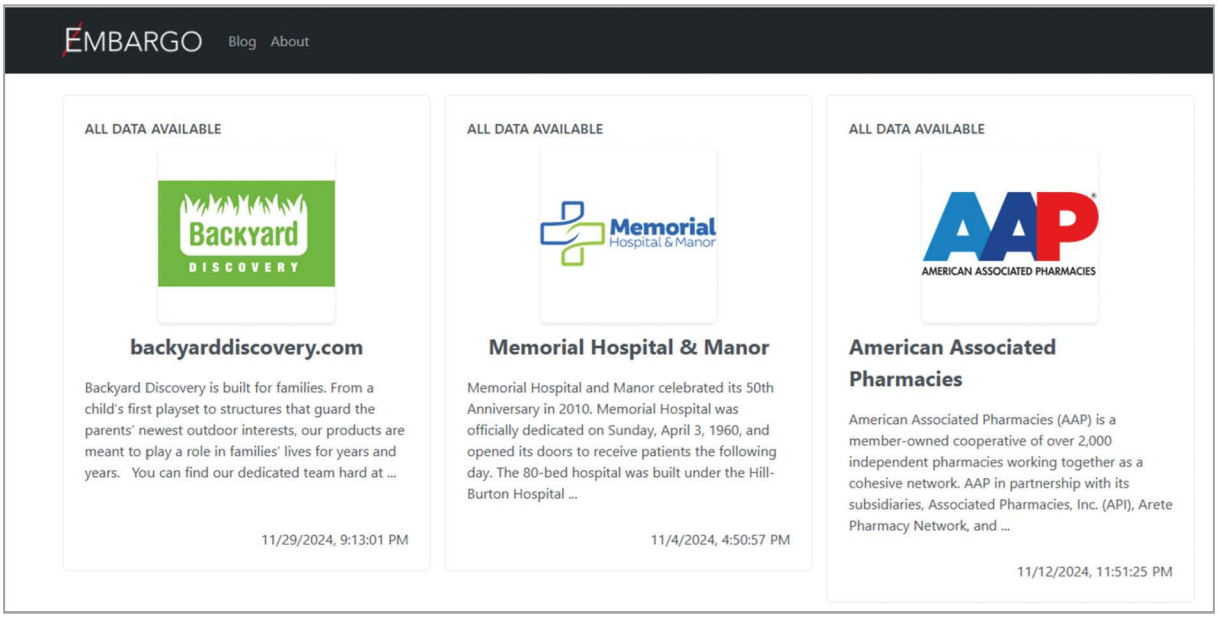
2024年6月25日，Killsec在其Telegram频道推出其最新产品：KillSec RaaS（勒索软件即服务），该服务包括一个可通过Tor网络访问的面板，该面板提供各种个能，包括：统计功能、聊天功能、构建器工具；以及即将推出的：DDoS攻击工具、拨打电话功能、高级窃密工具等。其定价仅为250美元，并承诺后续发布的功能不会再向附属成员索要任何费用，在赎金分成上，Killsec勒索软件组织核心负责人仅收取赎金的12%，剩下的88%由附属机构持有。

## Embargo

Embargo勒索软件最早出现于2024年5月，是一款使用Rust语言编写的勒索软件，采用勒索软件即服务（RaaS）模式运营，但该勒索软件的赎金分配比例和其他家族不同，Embargo勒索软件家族会根据附属公司的同能力给与不同的赎金分配比例：

- 附属公司自己获取网络权限并自己部署勒索，那么附属公司可获得赎金的80%
- 附属公司仅拥有网络权限，但没有部署勒索能力，那么附属公司将只能保留赎金的20%

Embargo勒索软件的一个附属组织，被追踪为Storm-0501，不仅部署Embargo勒索软件，还是BlackCat(ALPHV)、Hive、LockBit等勒索软件的附属公司，显示出其强大的攻击能力。该组织通过云攻击获取权限，关键方法之一是窃取Microsoft Entra ID（前称Azure Active Directory）凭据，从而操纵云环境中的数据和账户。



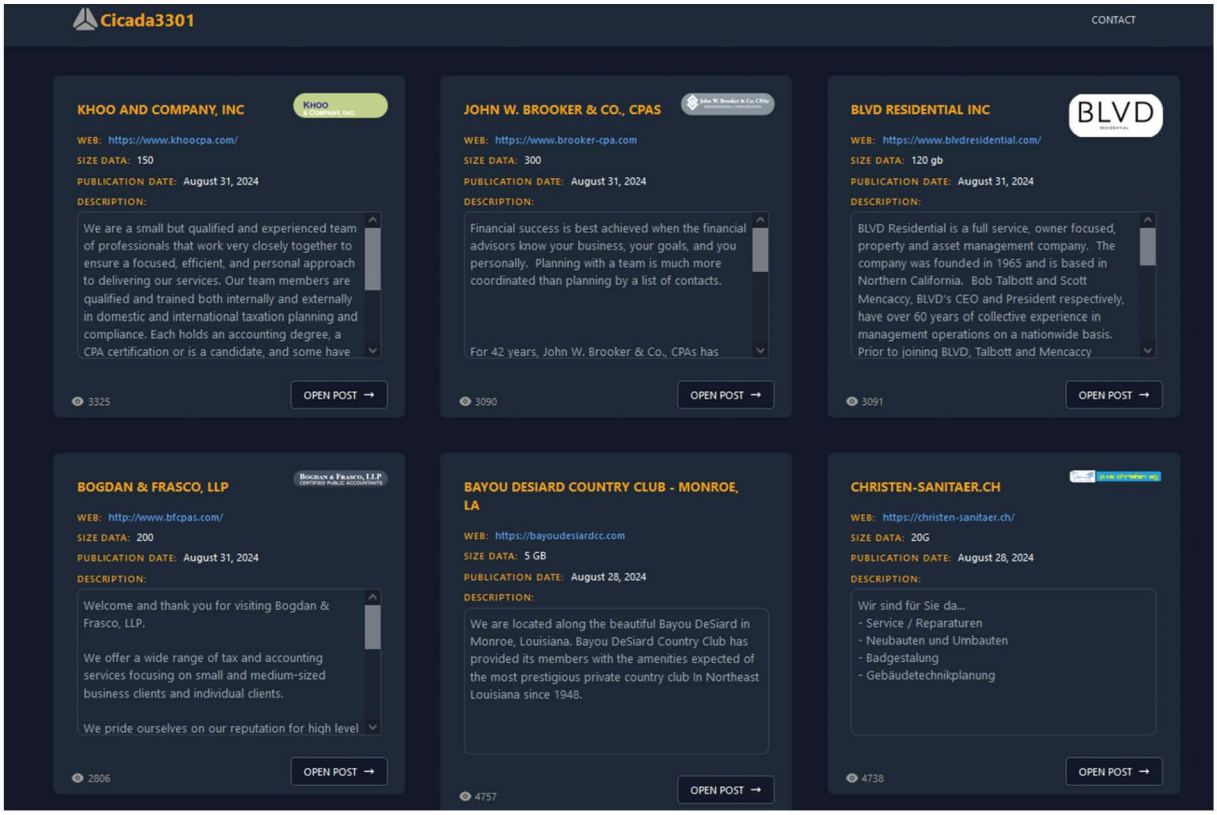

Embargo官网页面

尽管有安全研究员将Embargo勒索软件与BlackCat联系在一起，但Embargo的运营成员在采访中否认了这一关联，声明两者没有任何联系。

## Cicada3301

Cicada3301勒索软件，也称为Cicada，自2024年6月起活跃。尽管名称与2012至2014年间的Cicada 3301网络谜题系列相同，后者旨在吸引聪明人参与解谜，但两者并无关联。Cicada 3301谜题系列的组织者已明确否认与勒索软件有任何联系，并谴责了勒索行为。

Cicada3301勒索软件团伙采用勒索软件即服务（RaaS）模式运作。虽然2024年6月6日就已发现其攻击行为，但直到6月29日，该团伙才开始在网络犯罪论坛RAMP上推广并招募渗透测试人员和访问经纪人，提供20%的佣金，并为联盟提供具有广泛功能的基于网络的面板。Cicada3301勒索软件团伙还运营一个DLS(数据泄露站点)，如果受害组织或企业未能在规定时间内支付赎金，他们会在该站点公开窃取的数据。



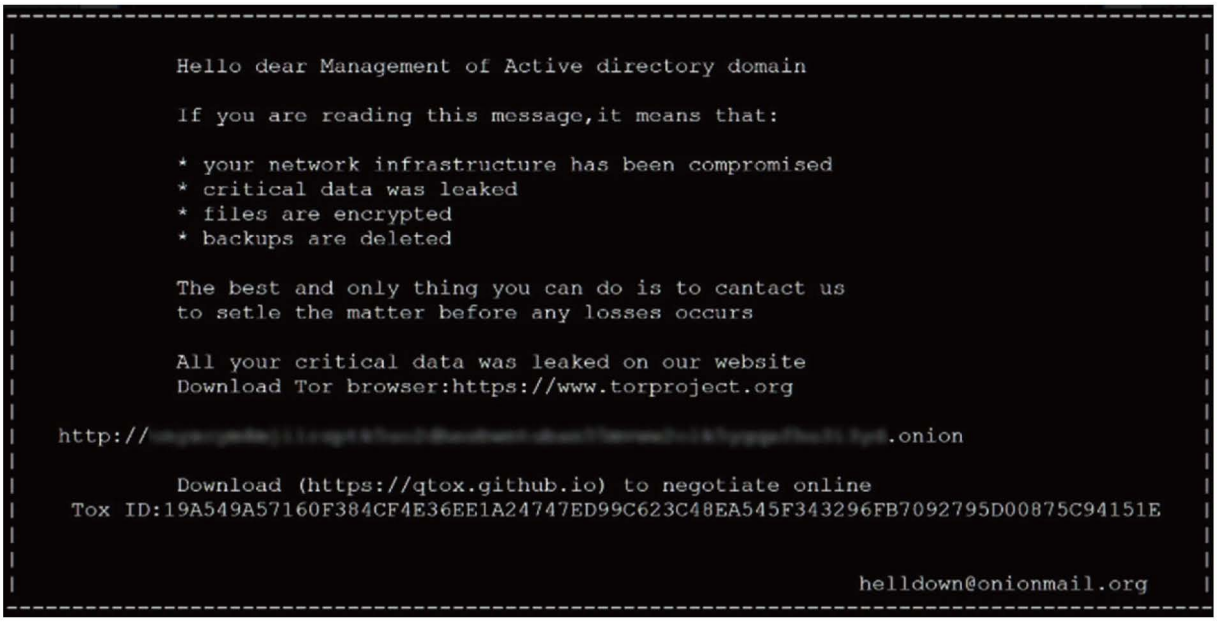

Cicada3301官网页面

对Cicada3301的加密程序分析显示，它与已解散的BlackCat/ALPHV勒索软件(BlackCat/ALPHV因内部对Change Healthcare公司2200万美元赎金分配不均而停止运营。)有诸多相似之处，例如两者都使用Rust语言编写，采用ChaCha20加密算法，用户界面命令参数相同，文件命名规则一致，以及赎金票据的解密方法也相同。

## HellDown

HellDown勒索软件自2024年8月首次露面，与名为Greppy的黑客组织有所关联。HellDown采用双重勒索策略，不仅窃取数据，还威胁受害者若不支付赎金则公开数据。该组织倾向于大量窃取数据，这表明该勒索软件组织可能对被盗数据的类型没有选择性。尽管其复杂性属于中等水平，但HellDown主要针对非营利组织以及多个行业，包括制造业、医疗保健、能源、房地产、商业服务、电信、软件、运输和教育。其受害者主要是美国和欧洲的中小企业。

HellDown存在两个版本，其中针对Windows的加密程序是基于泄露的LockBit3.0构建器构建的.而针对VMware ESXi的Linux变种首次出现于2024年10月，利用Zyxel防火墙中的漏洞，以破坏企业网络，从而窃取数据和加密设备。

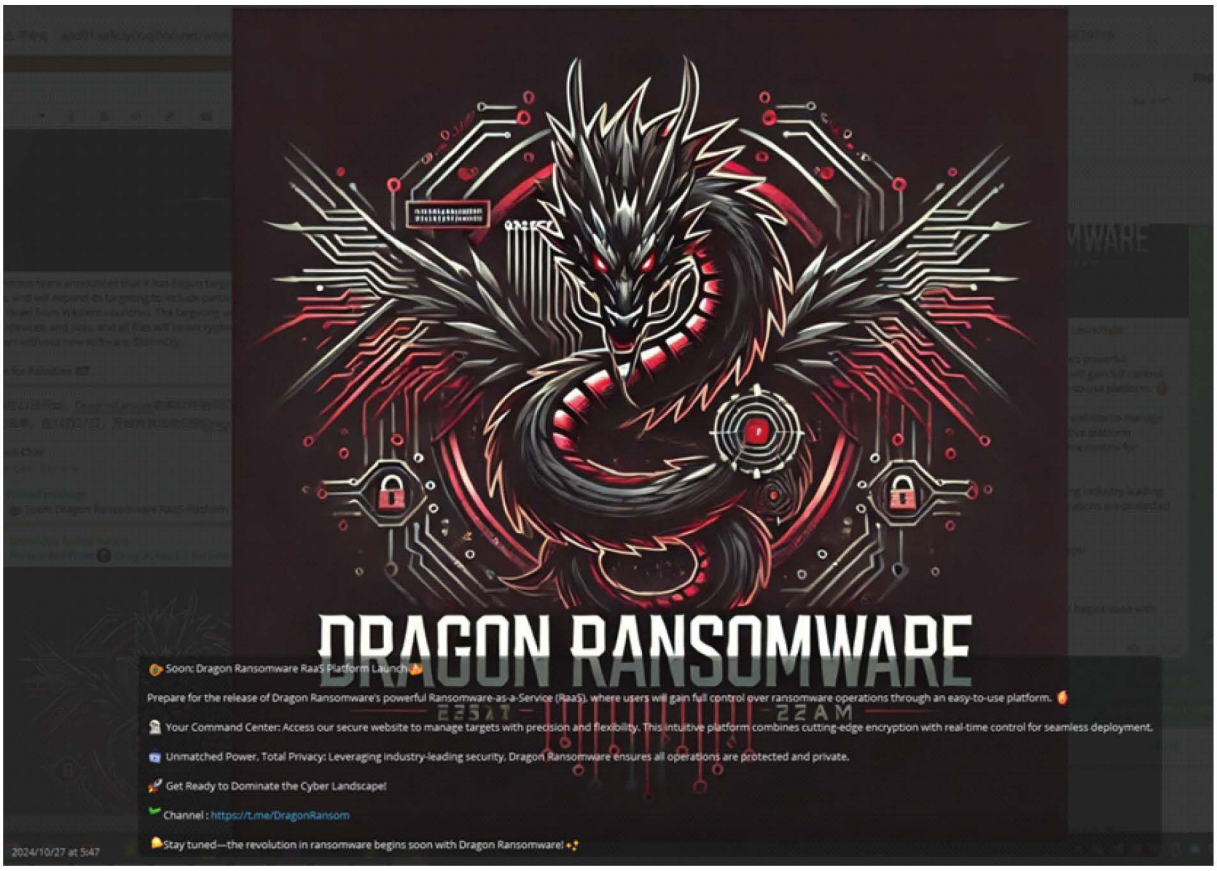



HellDown勒索信息

## Dragon Ransomware

DragonRansom勒索软件是2024年10月推出的新型勒索软件组织。该组织此前以“Stormous”模仿者的身份行动，虽然该团伙在2021年创建了Telegram频道，但并未活跃。2024年3月，该团伙推出了名为“StormCry”的勒索软件工具，并声称Stormous团伙针对以色列以及西方支持以色列的政党进行攻击时使用的加密程序是StormCry。但Stormous勒索软件组织在声明其官方Telegram频道时并未提及@stormouss频道，并称除去已申明频道外，并未开启其他频道。

2024年10月23日开始，DragonRansom勒索软件组织仍在以Stormous勒索软件组织的名义在其Telegram频道发布受害组织/企业名单，在10月27日，开始将其活动归到DragonRansom，并正式推出了Dragon RaaS平台，创建其官方Telegram频道@DragonRansom(命名为：Dragon RaaS|Version 1.0)。该勒索软件组织承诺提供快速且可定制的勒索软件操作，专门针对Windows系统。其主要特点包括一个紧凑的50KB文件大小、超快的加密速度，以及一个允许用户个性化配置勒索软件的构建器工具。这种高度的

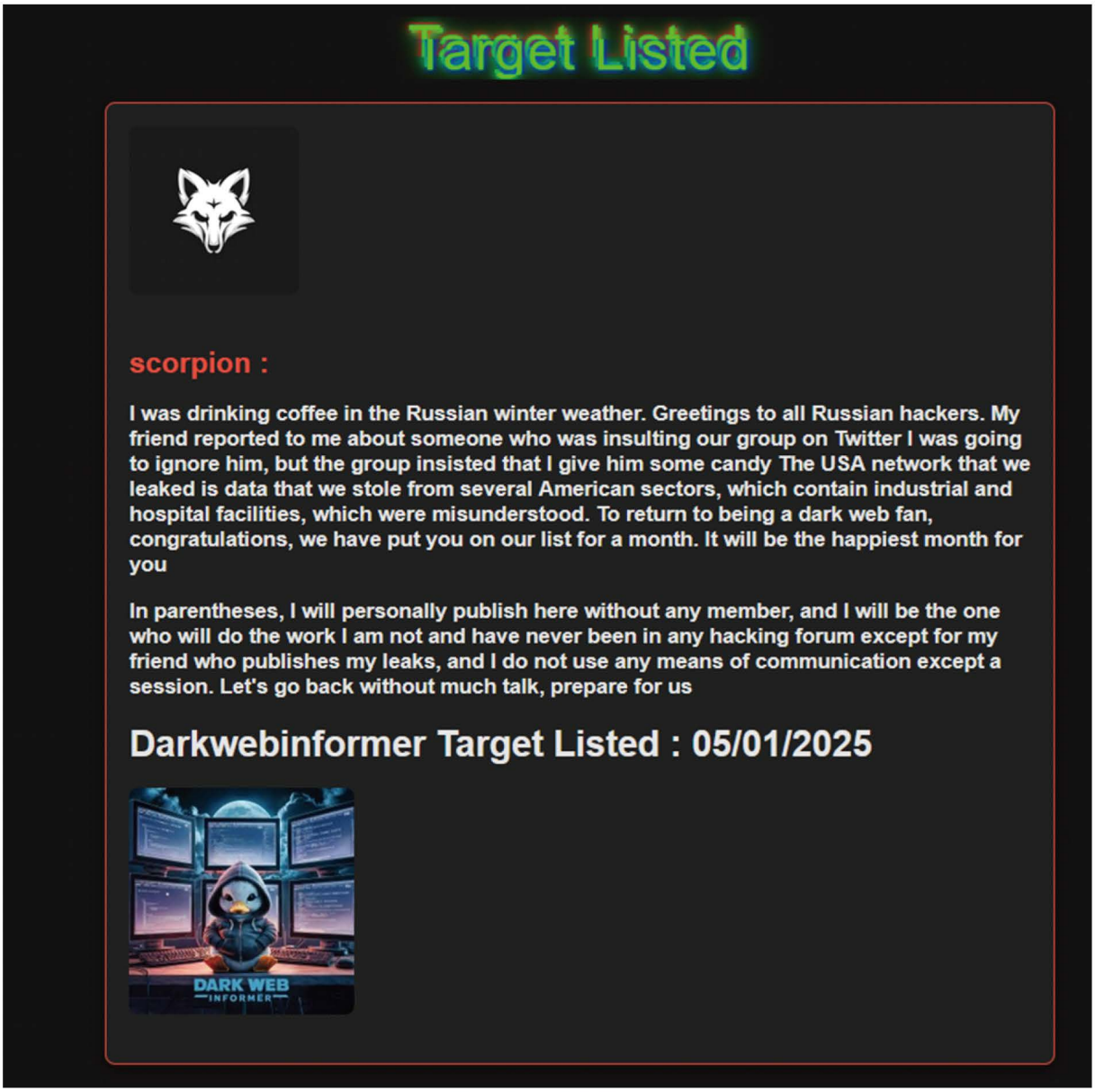



Dragon Ransomware官网页面

定制化和用户友好的配置工具，使得勒索软件的操作更加灵活和隐蔽。值得注意的是，DragonRansom勒索软件的公开策略与其Telegram频道订阅者数量挂钩。一旦频道订阅者达到1,000名，该工具将向公众开放，这可能预示着勒索软件的威胁行为者可用性的增加，从而扩大其潜在的影响范围和危害。这种基于订阅者数量的公开策略在勒索软件领域较为罕见，显示了该组织行为模式的特立独行。

## FunkSec

Funksec勒索软件最早出现于2024年9月，它是一款采用RaaS（勒索软件即服务）模式运营的双重勒索软件。该组织在暗网论坛上非常活跃，多名用户在2024年9月发布了与




FunkSec官网页面

Funksec组织相关的数据泄露事件，并且这些用户拥有很高的声誉评分，这表明其攻击的可行性较高。从受害组织/企业的地区分布来看，Funksec勒索软件组织影响了美国、突尼斯、印度、法国、泰国、秘鲁、约旦和阿拉伯联合酋长国，从行业来看：媒体、IT、零售、教育、汽车、专业服务和非政府组织部门等均受到影响。

Funksec勒索软件组织在其数据泄露网站（DLS）上免费提供了一款DDoS工具，该工具宣称能够通过HTTP和UDP协议持续进行DDoS攻击，并且强调这是该团伙独立开发的，说明该组织是具备DDoS功能能力的。同时该组织发布的公告中声称“在俄罗斯的冬天喝着咖啡，向俄罗斯的黑客问好，因此其背后的运营者很可能来自俄罗斯。

## （三）
## 其他性质勒索家族

网络上涌现的勒索软件越来越多，其勒索的行为也出现多样化，有的打着勒索软件的名义，其本质上却是数据擦除器；有的为了降低被发现的概率选择了仅通过窃取数据来勒索赎金，以下是2024年新增的其他勒索性家族。

| 月份 | 新增双重/多重勒索软件家族 | 勒索模式 |
|---|---|---|
| 2024年2月 | GitLocker | 数据擦除 |
| | Dispossessor | 数据泄露/声誉恐吓 |
| | RADAR | 数据泄露/声誉恐吓 |
| 2024年4月 | Wuibei | 数据擦除 |
| | HelloGookie | 数据泄露 |
| 2024年6月 | LukaLocker | 加密文件/声誉恐吓 |
| 2024年10月 | GoZone | 加密文件/声誉恐吓 |
| 2024年11月 | Termite | 数据泄露 |

2024年各月新增其他勒索性质家族

**针对以上其它类型勒索家族，我们对其中几个典型家族进行具体的说明：**

## Dispossessor / RADAR

Dispossessor数据勒索团伙最早出现于2024年2月，其运作模式类似于数据代理。该组织采用了勒索软件即服务（RaaS）的商业模式，要求其附属成员预先支付1比特币作为保证金，这笔款项将作为未来赎金的一部分。此举旨在筛选出不够谨慎的新手、执法人员、记者和竞争对手，确保团队的专业性和安全性。

Dispossessor拥有自己的专属数据泄露平台（DLS），其设计与LockBit的官方网站极为相似，无论是在配色方案、页面布局还是字体选择上都几乎如出一辙。该平台在上线首日就完全复制了LockBit的受害者名单，并且保留了详细的发布日期和相关信息。

Dispossessor勒索团伙与RADAR勒索团伙有着紧密的联系，尽管一度被误认为属于同一组织，但根据DataBreach的采访，两者实际上是独立的实体。但他们参与了共同的攻击行动，共享私人工具、方法和访问权限，并共同分配利润。尽管Dispossessor在2024年2月才正式露面，但其负责人声称已经在勒索行业活跃了三年。

起初，Dispossessor并未直接部署勒索软件，而是通过其专用数据泄露站点(DLS)发布受害者信息。其发布的受害者名单中，大多数受害组织或企业已由LockBit、Cl0p、Hunters International、8base以及Snatch等勒索软件家族披露。Dispossessor还试图在违规市场和黑客论坛（如BreachForums和XSS）上出售这些数据。因此，研究人员普遍认为，Dispossessor并非一个新兴的勒索软件团伙，而是一群犯罪分子，他们试图利用其他团伙的攻击来谋取私利，更准确地说，他们应该被称为数据代理。

2024年6月，Dispossessor开始使用泄露的LockBit3.0构建器来加密攻击目标系统中的文件。到了2024年8月12日，FBI和巴伐利亚州刑事警察(BLKA)宣布成功关闭了与该组织相关的24台服务器，包括18台位于德国、3台位于美国和3台位于英国的服务器。执法机构还拆除了该组织使用的9个域名，其中8个在美国，1个在德国。这标志着Dispossessor勒索软件活动的终结。


Dispossessor官网被查封

## WuiBei

Wuibei勒索软件最早出现于2024年4月，这款软件通过发送带有公民隐私信息查询的功能描述进行钓鱼邮件传播。钓鱼邮件中暗示用户可以通过打开附件中的软件查询开房记录、微信记录以及居住地址等公民的私人数据。

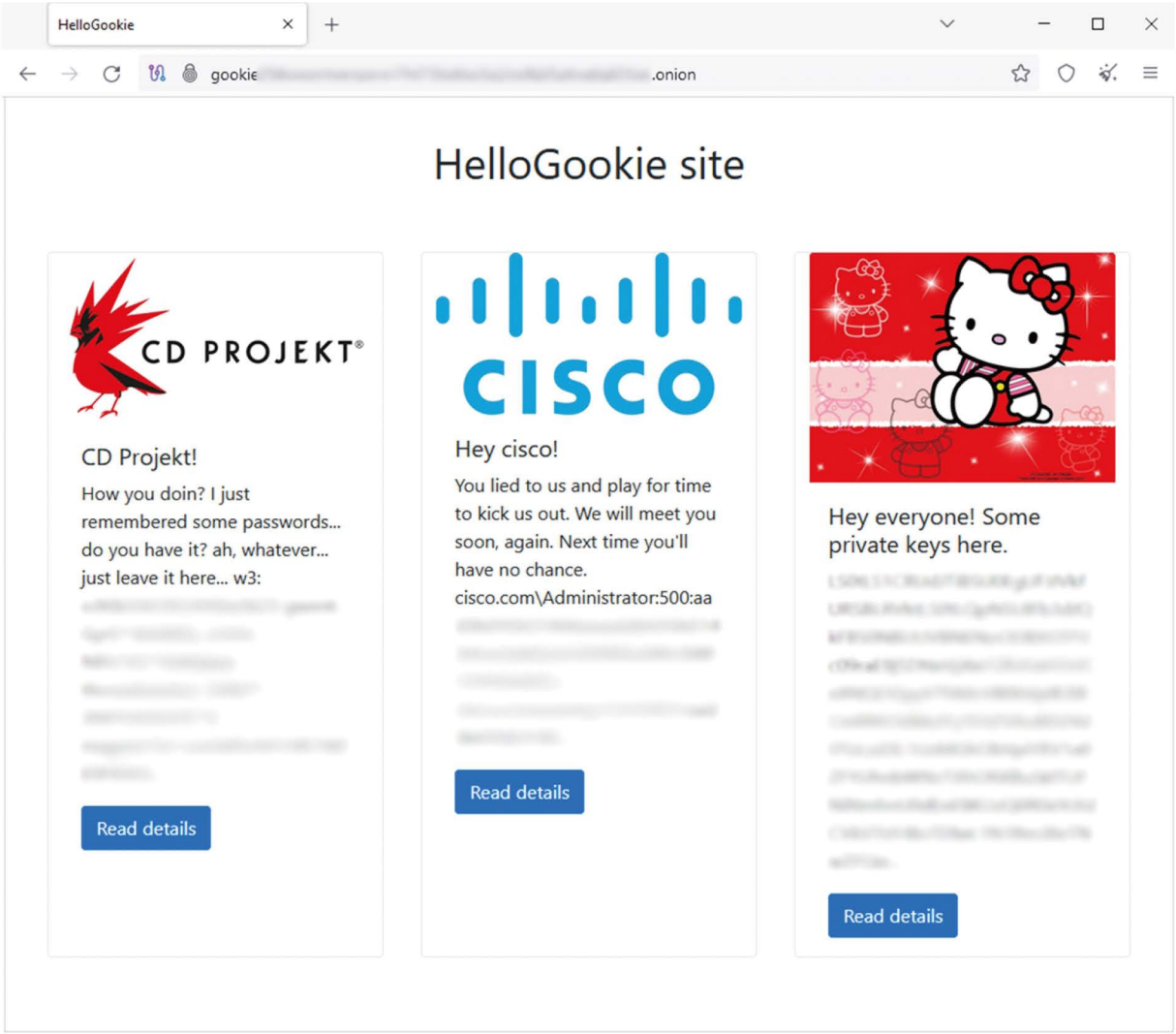
若收件人处于好奇下载运行该程序，系统中的文件将会被加密，被加密文件后缀会被修改为.enc，但由于该勒索软件在“加密”文件时，使用的随机数对原始内容进行覆盖，并且不存在备份数据的操作，因此该勒索软件也被认为是数据擦除器。会在每个磁盘中生成一个trash.dat文件，向里面疯狂写入大量垃圾数据，直到最终将整个磁盘的空间占满(C盘除外，C盘会将数据写到系统临时目录下(temp))。


Wuibei勒索软件钓鱼邮件

## HelloGookie

HelloGookie勒索软件，作为HelloKitty勒索软件品牌重塑后的新形态，首次出现在2024年4月。其前身HelloKitty勒索软件在2023年10月因源码泄露而终结。当时，Gookee/kapuchino在黑客论坛上公开了HelloKitty构建器和源代码，这直接导致了勒索活动的终止。

HelloGookie勒索软件的发现并非源自新的文件被加密受害者，而是由于在数据泄露站点上发布了之前攻击CD Projekt和思科时窃取的数据。这些泄露的信息不仅包括了这些旧攻击的数据，还包含了旧版HelloKitty勒索软件加密器的四个私人解密密钥。




HelloGookie官网页面

## LukaLocker

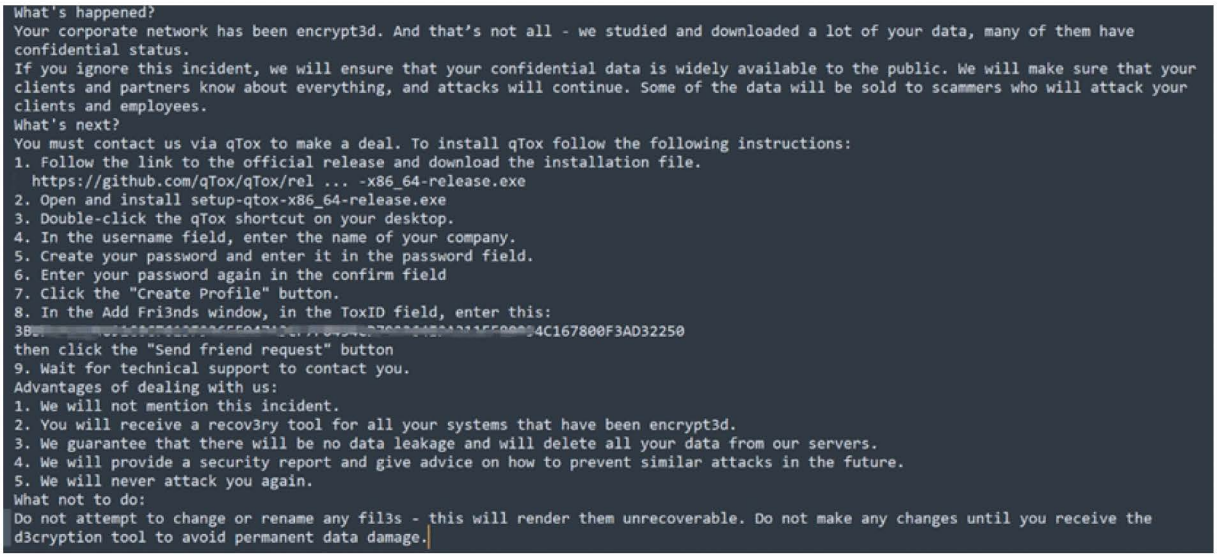
LukaLocker勒索软件最早出现于2024年6月。这款恶意软件由C++语言精心编写，被臭名昭著的Volcano Demon勒索软件组织所采用，专门用于加密目标企业和组织的内部文件。在发动攻击前，该组织会通过网络搜集常见的管理凭据，以期实现对受害组织设备的最大控制。此外，Volcano Demon还涉嫌从受害组织内部窃取数据，尽管目前尚未发现其在暗网上泄露数据的行为。

LukaLocker在执行攻击时，会利用Truesight.sys驱动程序进行操作。一旦该驱动程

序被安装，任何运行的安全应用程序（如Trend Micro产品）将立即失效，为勒索软件的部署铺平道路。

攻击者通过使用无法追踪的电话，以威胁性的语气联系受害企业的IT高管和决策者，要求支付赎金。这种通讯方式使得追踪变得极为困难。Volcano Demon组织承诺，一旦收到赎金，他们将不会共享任何数据，并会向受害者提供事件恢复工具和安全报告，同时保证不再对受害者发起进一步的攻击。

在加密数据方面，LukaLocker采用了Chacha8算法，通过Curve25519椭圆曲线Diffie-Hellman（ECDH）密钥协商算法随机生成Chacha8密钥和随机数，以实现数据的批量加密。该软件能够根据攻击者的需求，选择性地加密文件，加密比例可以是100%，也可以是50%、20%或10%。




LukaLocker勒索信息

## GoZone

GoZone勒索软件最早出现于2024年10月，这是一款使用GoLang语言编写的恶意软件，它结合了ChaCha20和RSA算法对受害者的文件进行加密，受害者想要解密文件仅需支付1000美元，根据当前的勒索软件趋势，GoZone似乎更倾向于针对个人用户而非企业组织。当GoZone运行完毕后，会将桌面背景修改为下图，提示受害者到指定的比特币地址去支付赎金。


GoZone勒索信息

该勒索软件在受害者的设备上显示了一条极具威胁性的警告信息，声称检测到了涉及儿童性虐待的内容。勒索者威胁称，如果受害者不在指定的时间内按照勒索要求支付赎金，他们将向执法机构报告这些所谓的非法材料。这种手段不仅对受害者施加了巨大的心理压力，还可能引发法律问题，进一步迫使受害者支付赎金以避免潜在的法律后果。

# （四）

# 家族衍生关系

随着勒索软件不断的更新迭代，一些勒索软件家族之前便存在了千丝万缕的联系，有的可能是有相同的源码改写而成；有的可能是有相同构建器创建而成；还有的可能是由相同的运营者运营等。针对这一现状，进行了以下概括：

- **品牌重塑**：勒索软件团伙为了逃避法律制裁、重获信誉或因内部矛盾，经常进行品牌重塑。例如，HelloKitty勒索软件品牌重塑为HelloGookie。这种品牌重塑不仅有助于团伙逃避追踪，还能吸引新的附属机构加入。

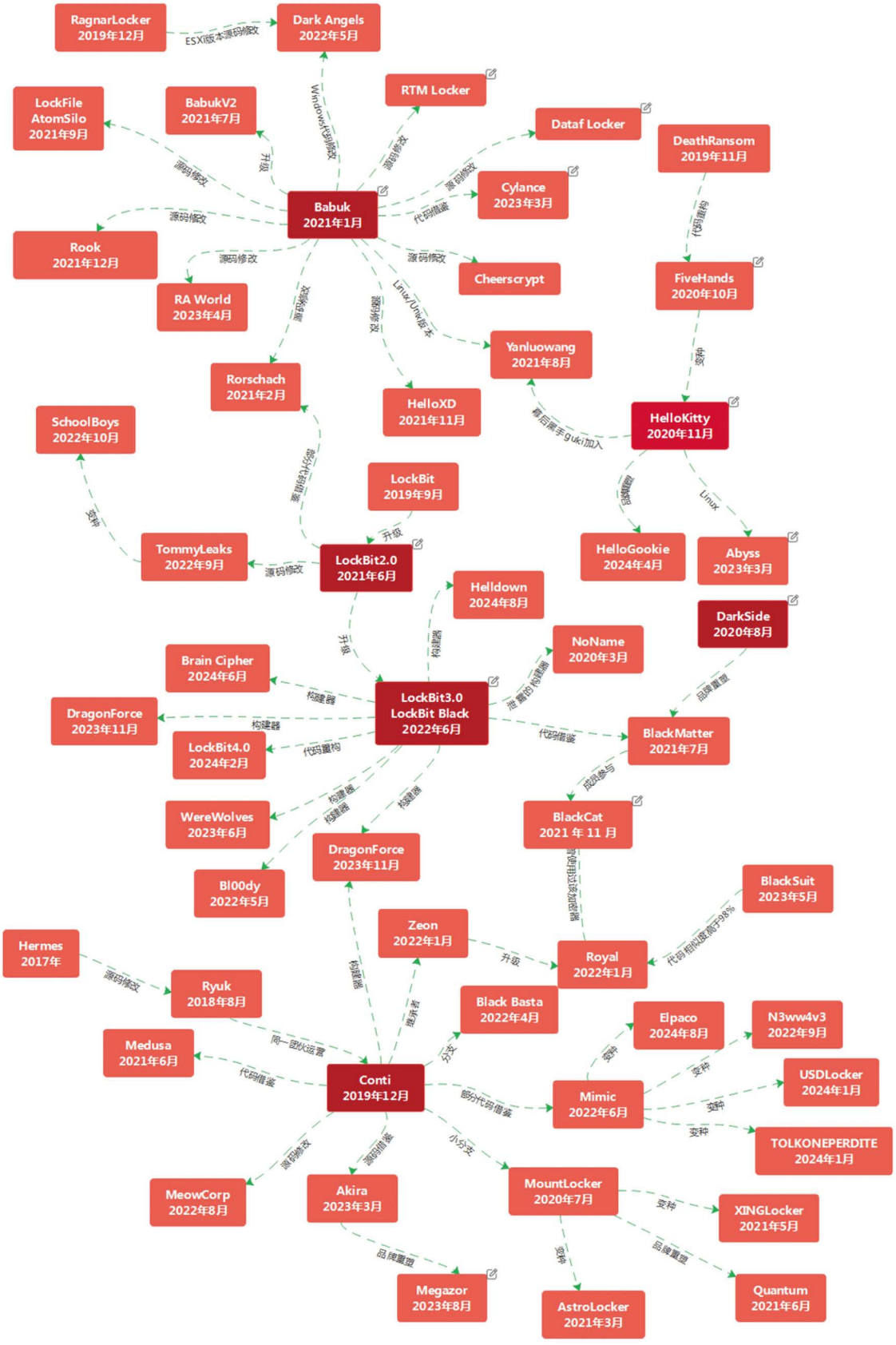
- 源码出售：勒索软件宣布停止运营或对品牌进行升级，将代码进行出售。例如：INC勒索软件升级成Lynx后，其源代码在黑客论坛上以30万美元的价格出售。

- 源码泄露：内部矛盾或政治立场的差异也导致了勒索软件源码的泄露。例如Babuk内部因对华盛顿警察数据处理发生内部矛盾，其创始者将其源代码公开发布；Conti勒索软件因在俄乌战争中明确支持俄罗斯，导致内部矛盾，其源代码被泄露。

- 构建器泄露：同样也是因为内部矛盾等因素而被公开，例如LockBit3.0的构建器，因其雇佣的开发人员对其领导不满，导致其加密程序构建器被公开发布。

- 开发者发布：一些勒索软件的开发者出于共享源码，以方便研究人员研究目的公开源代码，如Jigsaw勒索软件，但这些代码往往被恶意利用。

**下面是几大关联家族的脉络图：**


RagnarLocker 2019年12月
ESXi版本源码修改
Dark Angels 2022年5月
LockFile AtomSilo 2021年9月
BabukV2 2021年7月
RTM Locker
Dataf Locker
DeathRansom 2019年11月
Cylance 2023年3月
Babuk 2021年1月
Rook 2021年12月
RA World 2023年4月
Cheerscrypt
FiveHands 2020年10月
Yanluowang 2021年8月
Rorschach 2021年2月
HelloXD 2021年11月
HelloKitty 2020年11月
SchoolBoys 2022年10月
LockBit 2019年9月
HelloGookie 2024年4月
Abyss 2023年3月
TommyLeaks 2022年9月
LockBit2.0 2021年6月
Helldown 2024年8月
DarkSide 2020年8月
NoName 2020年3月
Brain Cipher 2024年6月
LockBit3.0 LockBit Black 2022年6月
DragonForce 2023年11月
LockBit4.0 2024年2月
BlackMatter 2021年7月
WereWolves 2023年6月
DragonForce 2023年11月
BlackCat 2021 年 11 月
Bl00dy 2022年5月
BlackSuit 2023年5月
Hermes 2017年
Zeon 2022年1月
Royal 2022年1月
Ryuk 2018年8月
Black Basta 2022年4月
Elpaco 2024年8月
N3ww4v3 2022年9月
Medusa 2021年6月
Conti 2019年12月
Mimic 2022年6月
USDLocker 2024年1月
TOLKONEPERDITE 2024年1月
MeowCorp 2022年8月
Akira 2023年3月
MountLocker 2020年7月
XINGLocker 2021年5月
Megazor 2023年8月
AstroLocker 2021年3月
Quantum 2021年6月

**勒索家族关系图**

第二章

# 勒索软件受害者分析

P053

P061

# 勒索软件受害者分析

基于360反勒索服务中求助用户所提供的信息，我们对2024年全年遭受勒索软件攻击的受害人群做了分析。在地域分布方面并没有显著变化，依旧以数字经济发达地区和人口密集地区为主。而受感染的操作系统、所属行业则受今年流行的勒索软件家族影响，与以往有较为明显的变化。

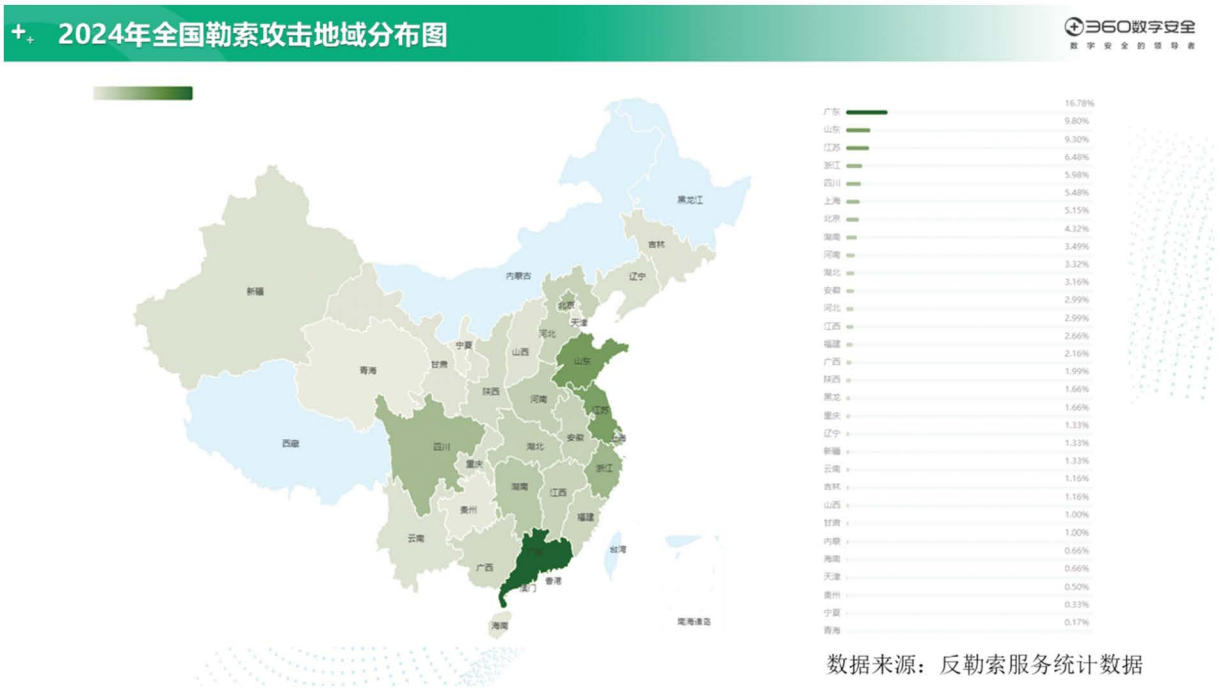
## 一

## 受害者所在地域分布

以下是对2024年攻击系统所属地域采样制作的分布图，总体而言地区排名和占比变化波动始终均不大。数字经济发达地区仍是攻击的主要对象。


数据来源：反勒索服务统计数据

下图为根据全国地区分布数据所绘制的更加直观的地区分布图：

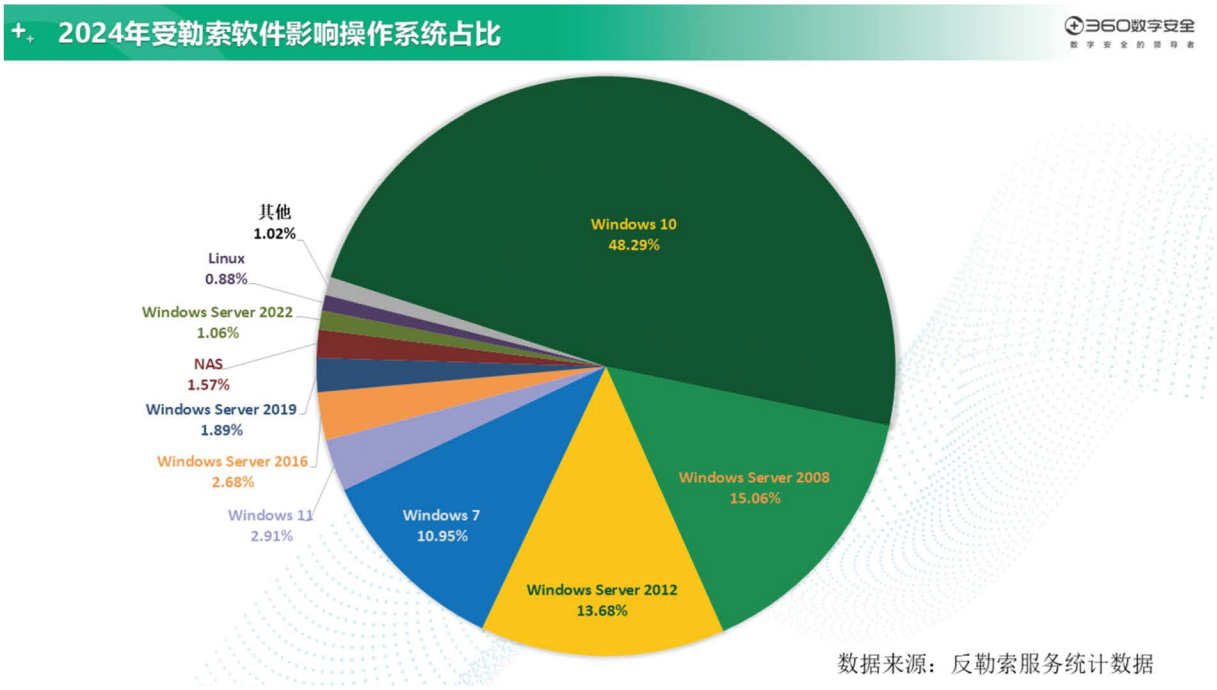



数据来源：反勒索服务统计数据

# 二

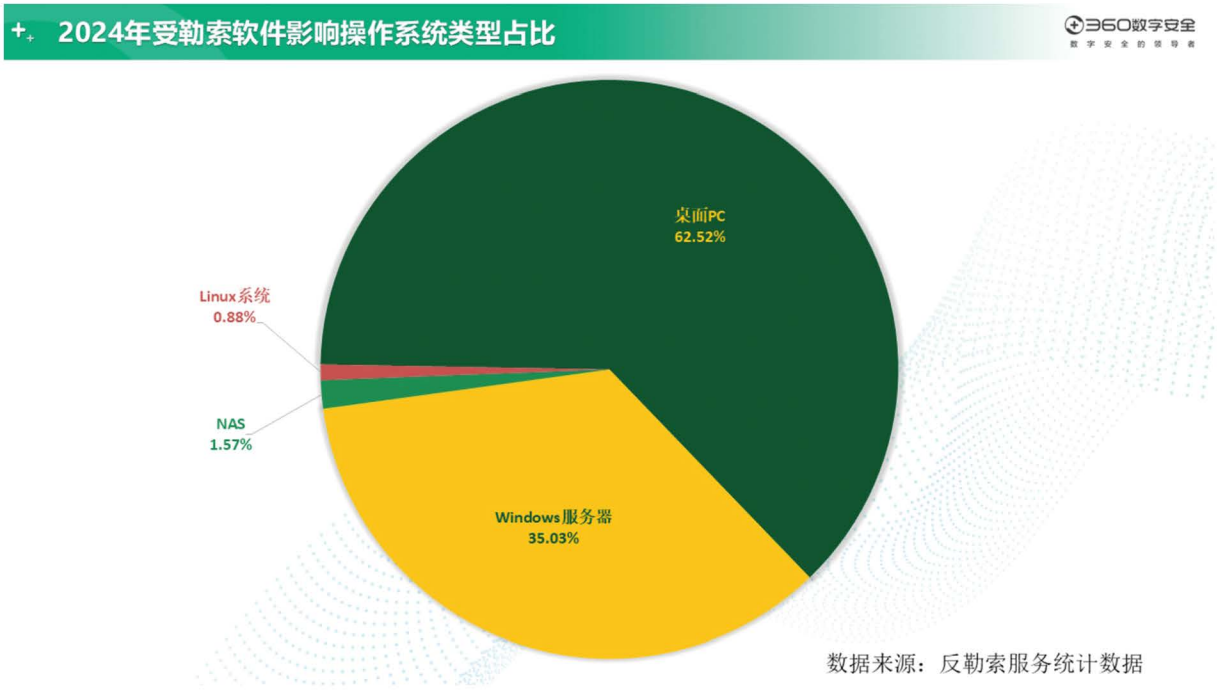
# 受攻击系统分布

对2024年受攻击的操作系统数据进行统计，位居前三的系统为Windows 10、Windows Server 2008和Windows Server 2012。而其中Windows 10系统的占比相较2023年有着明显提升——增加了近14个百分点。一方面，这与Windows 10系统本身巨大的装机量不无关联。另一方面，不少中小型企业将各类内部管理系统部署在Windows 10这类家用系统中也是其受勒索量增加的原因之一。




从操作系统类型的角度看，受到Windows 10的占比激增影响，桌面PC的占比同样出现了接近12个百分点的大幅度提高。不过，针对Linux和NAS系统的供给量则依然保持着存在但占比不高的稳定态势。

虽然桌面PC占比再度甩开服务器系统，但与勒索软件早年针对个人用户的攻击态势不

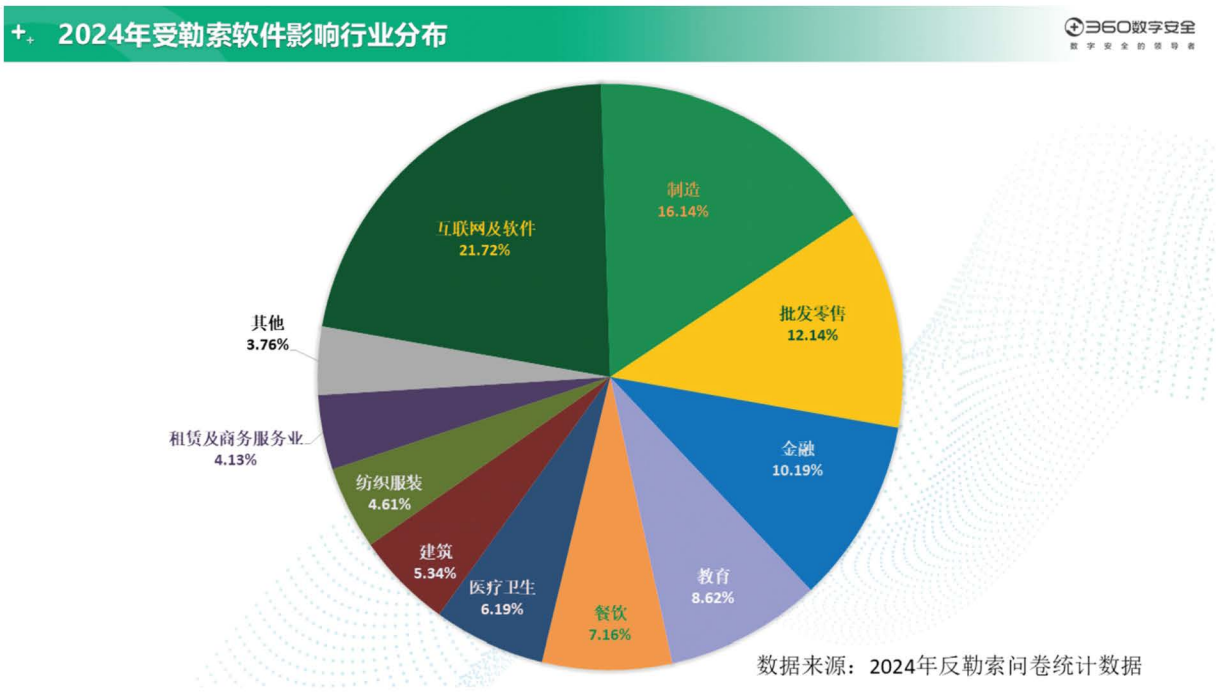


同，本轮桌面系统的占比回归更多是受到了Web漏洞入侵手段增加和中小型企业采用Windows 10系统部署管理系统的双重因素影响。因此，针对企业目标的攻击依旧是勒索软件演变的发展趋势。

# 三
# 受害者所属行业

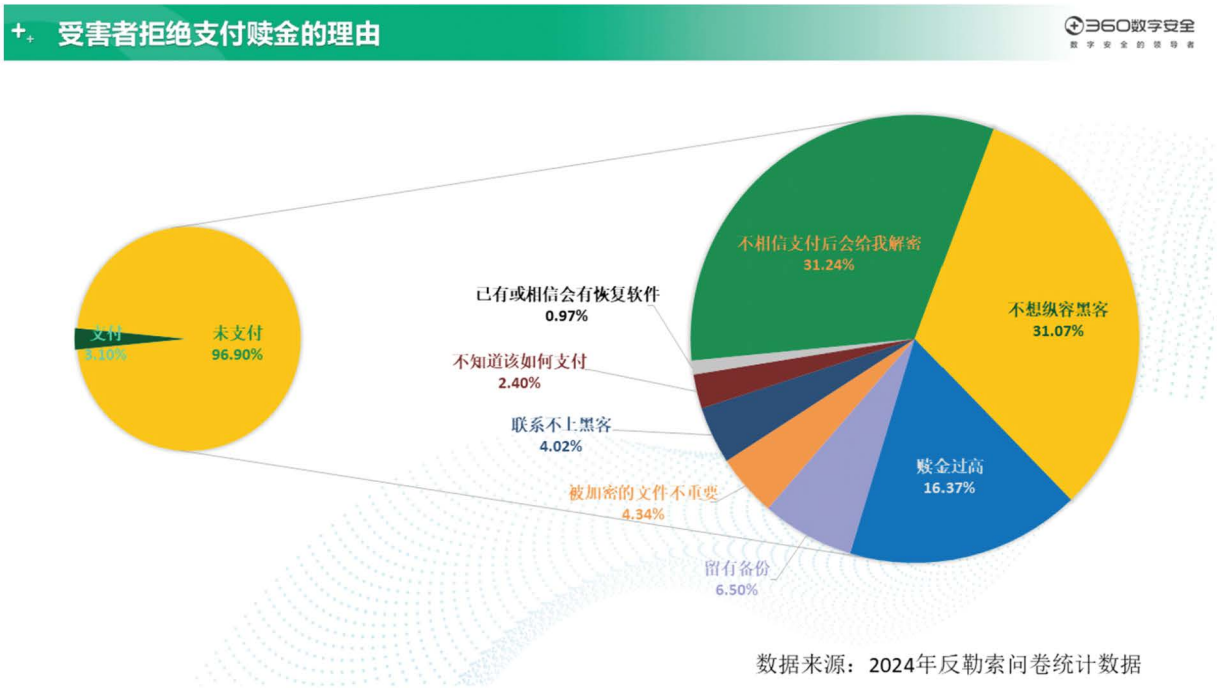
对来自反勒索服务申诉的受害者所属行业进行统计，发现互联网及软件、制造业、批发零售分列受影响最为严重的前三类行业。而金融行业则紧随其后位居，占比位居第四。推测这与越来越多的勒索家族针对政企单位采取有的放矢的定向攻击有关。近年来，越来越多的勒索软件家族会在入侵前就指定较为具体的入侵方案，入侵目标也更为明确。那么“财大气粗”的金融行业自然也就成为了入侵者严重的香饽饽。毕竟更为雄厚的资金实力通常也就意味着更高的勒索成功率。

此外，受到越来越多的勒索家族采用双重/多重勒索攻击影响，金融行业所掌握的数据相较于其他行业有着更高的勒索价值。攻击者在窃取到大量内部金融数据后，无论是凭借数据对受害机构狮子大开口，还是直接转卖这些高价值数据直接获利，甚至是两者兼而有之，都将会是一笔非常可观的巨额收益。



# 四
# 受害者支付赎金情况

通过分析受害者对于赎金支付情况的反馈，发现受害者在遭遇勒索病毒后的赎金支付操作并无显著变化，大多数受害者依然并选择不支付勒索赎金，而不支付的理由也依旧是不相信黑客或不想纵容黑客。当然，也有不少受害者不愿支付赎金的理由则是对黑客开出的天价赎金望而却步。

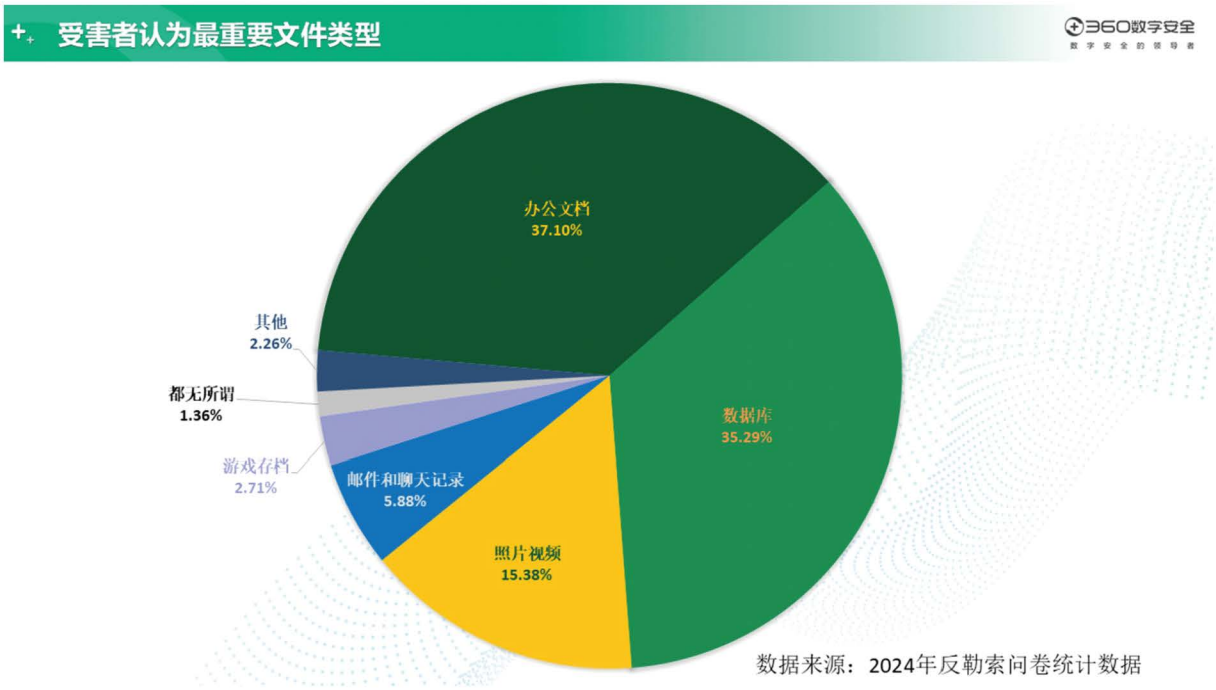



数据来源：2024年反勒索问卷统计数据

不过，支付赎金的占比也延续了2023年的上涨势头，有了进一步的显著提升。经分析，这与勒索软件进一步的侧重于针对政企相关单位的攻击有着密切关系。此类受害者通常更愿意为了减小损失而支付赎金，同时也更有经济实力来承担高额的赎金。

# 五
# 对受害者影响最大的文件类型

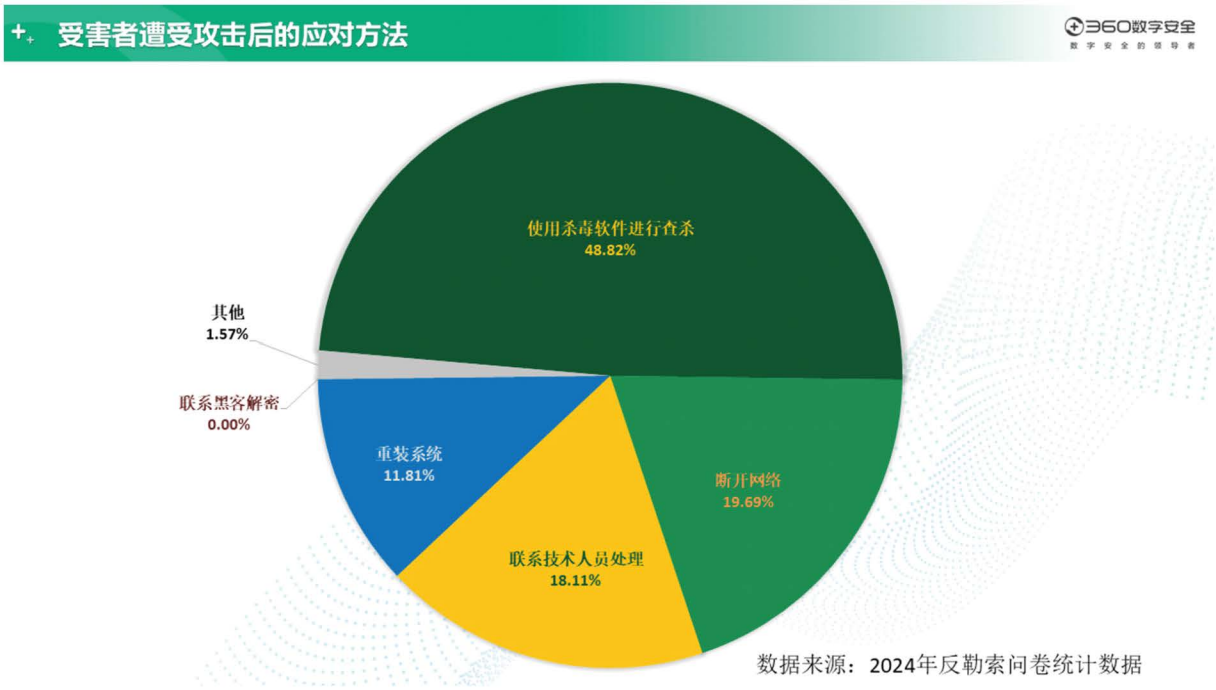
通过分析受害者对于赎金支付情况的反馈，发现受害者在遭遇勒索病毒后的赎金支付操作并无显著变化，大多数受害者依然并选择不支付勒索赎金，而不支付的理由也依旧是不相信黑客或不想纵容黑客。当然，也有不少受害者不愿支付赎金的理由则是对黑客开出的天价赎金望而却步。



# 六
# 受害者遭受攻击后的应对方式

同样的，我们对2024年勒索受害者在受到攻击后的应对方式进行的问卷调查统计结果与2023年的占比分布也几乎完全一样：利用安全软件查杀、断开网络、求助于技术人员以及重装系统都是被官方采用的主流应对手段。

这也意味着，随着勒索软件的流行，对勒索攻击的应对手段也显现出了明显的模式化和预案化。显然，勒索软件对于公众而言已不再是一个陌生的恶意软件，而是被大众更为广泛的熟知。



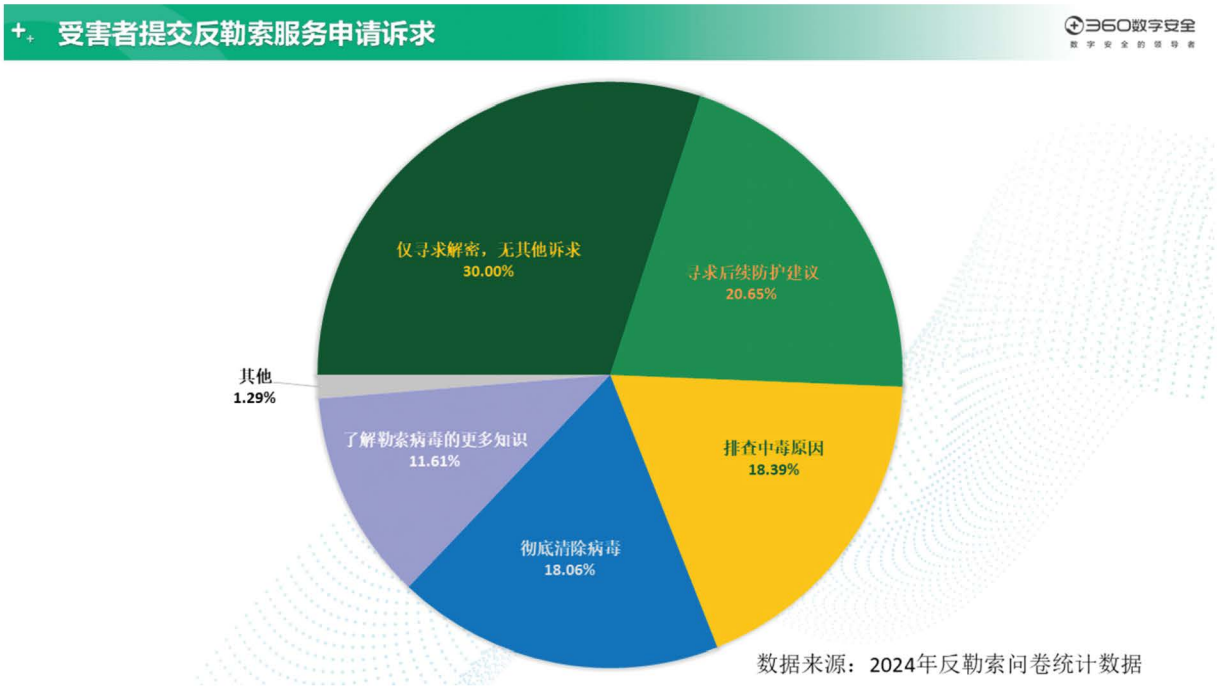

数据来源：2024年反勒索问卷统计数据

# 七

# 受害者提交反勒索服务申请诉求

根据问卷反馈的统计数据来看，在申请反勒索服务的用户中，大多数用户主要诉求依然是为了能够恢复被加密的数据。这也是我们提供该服务的初衷之一。而令人欣慰的是，“了解勒索软件更多知识”这一选项的占比同样有着进一步的提升。

这说明了广大用户对安全态势的关注和安全意识的不断提高，这也为我们与勒索软件持续对抗并完善相关知识库提供了源源不断的动力。



# 第三章

# 勒索软件攻击者分析

P062

P081

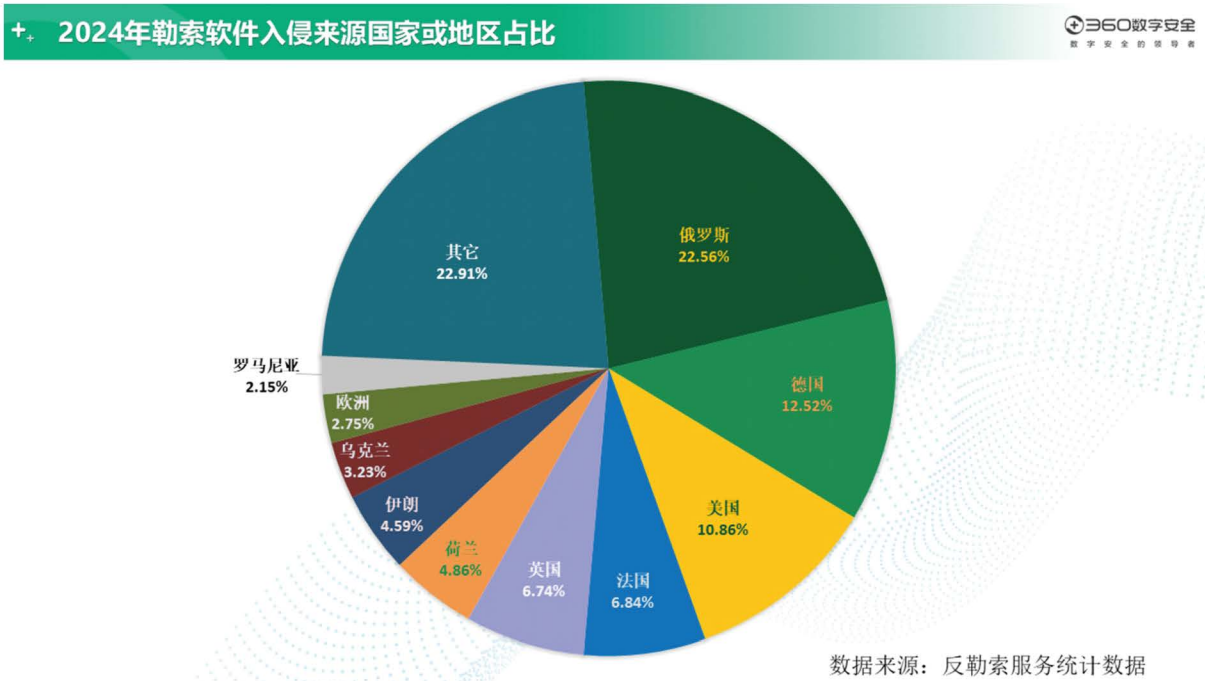
# 勒索软件攻击形势

2024年的勒索软件攻击数据分析揭示，弱口令攻击仍然是最普遍的网络攻击形式，但通过漏洞利用发起攻击的占比有显著上升，尤其是对1day的应用更加普遍，通过漏洞发起攻击成为最主要的攻击方式之一。

## 一

## 黑客使用IP

远程桌面弱口令攻击和漏洞攻击依旧是勒索软件入侵的最流行方式，但2024年的数据库弱口令攻击数量有着显著提升。对于各类入侵方式的攻击来源IP进行分析发现，其归属最多的是俄罗斯地区，其次则是德国和美国（此数据仅反映攻击者发起攻击的IP地址，并不代表攻击者所属国家，攻击者往往会使用代理服务器来隐藏其真实IP地址）。




数据来源：反勒索服务统计数据

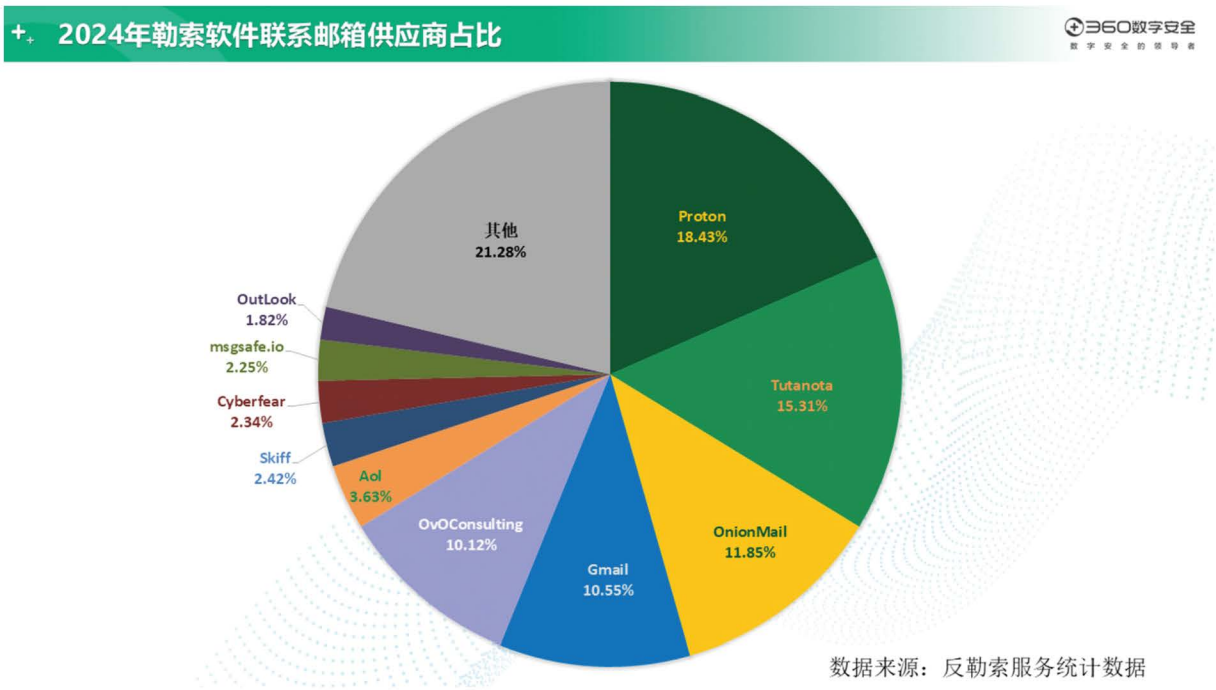
# 二

# 勒索联系邮箱的供应商分布

2024年，勒索软件主流的联系方式依然自建聊天室、第三方通信工具和邮箱三种。其中：自建聊天室的通常需要需受害者注册或使用黑客勒索提示信息中提到的账户和密码或唯一的ID进行登录才能进行对话，保证其对话的唯一性与私密性。

第三方通信工具则主要以Jabber、Telegram、Tox等匿名聊天工具为主。攻击者与受害者会通过这些软件进行赎金谈判，但现在它们的用途已经扩展。例如：Telegram被一些勒索软件团伙用于创建数据泄露频道，公开受害者敏感信息以此作为施压手段；Tox也不再局限于赎金谈判，而是被用作数据买卖的沟通平台。这些工具的多功能性使得它们成为双重甚至多重勒索软件组织的青睐之选。

电子邮件作为赎金谈判的渠道，已经成为传统勒索软件攻击者的首选方式。为了确保受害者能够顺利联系到他们，攻击者通常会提供至少两个电子邮件地址，并定期更换以避免被追踪。在某些情况下，同一勒索软件家族的不同传播者也会使用不同的电子邮件地址进行通信。这种做法导致我们能够监测到的活跃邮件地址数量相较于其他通信方式要多得多。




数据来源：反勒索服务统计数据

通过对2024年收集到的黑客邮箱进行数据分析,我们发现最受勒索软件作者欢迎的是ProtonMail。针对TOP10邮件服务商提供的邮箱属性进行研究发现，其中匿名邮箱占到了总量的76.02%，相较于去年上涨了3.65%。

# 三
# 攻击手段

本节将介绍一些常见的攻击手段，帮助读者更好地理解勒索软件攻击，并提供相应的防治措施。

## （一）
## 口令破解攻击

口令破解类攻击是网络攻击中最为基础和历史悠久的攻击手段之一，同时也是国内勒索病毒传播的重要原因。尽管当前已有多种技术手段用于解决口令脆弱性问题，但“弱口令”问题依然是困扰企业和个人用户的重大安全隐患。此问题的根源多方面存在，且在多个层级的企业中普遍存在。

需要首先澄清的是，“弱口令”并非仅指那些简单、易记的密码。实际上，即便是看似复杂的密码，也可能是“弱口令”。常见的“弱口令”情况包括：过于简单的密码、常见的密码字典词汇（如：888888、qwerty等）、包含个人身份信息的密码等。此外，还有一些常被忽视的弱口令类型：

- 产品内置的默认账户和默认密码：这些密码通常未经过修改，攻击者可以通过简单的扫描工具获取。
- 统一运维账户的默认口令：许多企业使用默认的统一运维密码，这为攻击者提供了方便的突破口。

- 失窃的口令：在发生网络攻击后，未及时更换的旧账户密码可能已经泄露，成为攻击者的突破点。
- 信息泄露：管理员在维护日志中记录了后台账户信息，在代码仓库中上传了私钥等也可能导致密码泄露。

**在勒索软件攻击事件中，常见的弱口令问题通常出现在以下几类环境中：**

- 远程桌面服务（RDP）
- 数据库服务
- NAS设备

这些环境的共同特点是，它们通常会将认证接口暴露到公网。攻击者只要掌握相关账户和密码信息，就可以直接登录到这些设备，从而成为进一步攻击内网的入口。如果攻击者能够控制一个高权限账户，那么就能够在内网中自由行动，进一步窃取数据和控制其他设备。

对于密码管理，用户和企业在实践中常常遇到诸多困难。虽然大家都已熟知一些密码安全的基本措施，比如定期更新密码、不使用简单密码、避免密码重用等，但在实际操作中，这些措施的落实常常存在挑战。以下是一些建议，旨在加强对密码的管理：

- 避免在单一设备上存储大量密码或登录凭据

  不要低估攻击者对设备信息的挖掘能力，黑客在攻击过程中通常首先会寻找设备中存储的账户凭据信息。

- 加强账户验证策略

  可以通过设置IP白名单、限制密码验证尝试次数等简单有效的手段，缓解暴力破解攻击的风险。另外，对于一些老旧系统，缺乏足够的安全防护，容易遭受口令暴力破解攻击的系统应当避免使用。

- 启用多因素认证（MFA）

  如果条件允许，务必启用多因素认证（MFA）。MFA可以显著增加口令破解的难度，是一种简单而有效的防护措施，能够有效减少由于口令泄露带来的风险。

- 使用密码管理工具和单点登录（SSO）

尽管一些人可能认为单点登录（SSO）会增加系统风险，但实际上，当企业使用多个系统时，维护多个认证系统和口令信息会带来很大的管理负担。尤其是让员工记住多个复杂的密码并定期更新，这在实际操作中非常困难。使用SSO能够将认证过程集中化，提高可操作性，同时可以结合MFA进一步增强认证的安全性。

此外，密码管理工具能够帮助员工生成强密码，减少设置“弱口令”的可能性，并且可以避免将明文密码存储在不安全的位置。

## （二）

## 漏洞利用攻击

漏洞问题在全球范围内的勒索攻击中，都占有重要地位，通常作为攻击的初始入口，或在横向移动过程中被利用。随着信息系统的日益复杂，漏洞的出现几乎是不可避免的，且其类型多样，包括硬件漏洞、操作系统漏洞、应用软件漏洞、以及第三方组件漏洞等。在勒索软件攻击案例中，应用软件漏洞尤为常见，涉及的系统包括Web服务程序（如OA、ERP系统）、域控服务器、以及网络边界服务（如VPN服务器）。根据漏洞是否已被修补，漏洞可分为“0day漏洞”（厂商尚未修复）和“nday漏洞”（厂商已修复）。根据过去一年的分析，勒索攻击活动中，最常被利用的仍然是nday漏洞。

漏洞的复杂性和多样性往往让管理者不知从何入手，因此我们从不同的视角帮助读者更好地理解漏洞攻击问题。

### 黑客视角

黑客发起攻击从来不是“徒手”进行的，他们通常使用各种“武器”来实现攻击目的。攻击的第一步通常是使用扫描工具对潜在目标进行侦查，目的是发现开放的服务和潜在漏

洞。黑客可能会针对整个网段或特定机房进行集中扫描，或者基于前期收集到的服务器信息，针对目标服务器进行扫描。这一过程一般通过租用的服务器、通过“肉鸡”或第三方开放平台来进行。由于这种扫描过程是持续性的，互联网公开服务几乎都能被快速探测到。因此，管理员不要心存侥幸，认为自己部署的服务不受黑客关注。

在准备攻击武器时，并非所有黑客都有能力自主发现漏洞或编写完整的攻击代码。大多数黑客依赖知名的漏洞利用工具集（Exploit Kits，简称EK），这些工具集通常包含多个漏洞利用模块，尤其是那些已被厂商修复但尚未普及的1Day漏洞。对于这些漏洞，黑客不必自己编写攻击代码，只需替换攻击载荷（payload）即可完成攻击。对于厂商修复但尚未广泛打补丁的设备，黑客会迅速展开攻击，特别是当漏洞权限较高且相关平台流行时，攻击便进入了高效阶段。

勒索攻击的实施往往选择在非工作时间，尤其是周五晚上，这样攻击者可以利用较长的时间窗口来解决潜在问题而不被管理员发现。攻击通常是自动化的，部分过程中可能需要半自动化操作来辅助，因此一个黑客团伙能够在一晚上攻击数千甚至上万台服务器。

因此，管理员需要认识到，在大规模的网络攻击面前，只要开放了外部服务，就必须做好充分的防御准备，不能心存侥幸。

## 软件供应商视角

当前主流操作系统供应商对安全问题普遍重视，且在产品安全性上进行了充分的测试，出现问题后能及时发布补丁。用户只要及时更新补丁，通常可以避免大部分操作系统漏洞导致的勒索风险。

然而，第三方软件供应商在漏洞问题上的态度和能力差异较大。一些厂商积极响应并及时修复漏洞，而另一些厂商则回避漏洞问题，认为其产品漏洞是负面信息，不愿过多公开。此外，也有厂商认为漏洞与网络攻击是安全厂商和黑客的问题，而与其产品无关，对漏洞问题不够重视，不积极发布补丁。也有部分厂商对盗版用户或未续费的用户不提供补丁服务，导致问题的加剧。

第三方组件的安全性问题也是厂商的痛点。如今的系统通常引入大量第三方组件，当某个组件出现漏洞时，如果厂商未及时更新或适配，可能导致严重后果。例如，php的一个漏洞，可能会影响所有使用该基础组件的服务。

## 安全公司视角

安全公司在维护系统安全过程中面临着众多挑战。操作系统漏洞通常可以通过安装补丁来修复，但对于第三方应用而言，受限于版权和技术多样性，安全公司难以为每一个应用安装专门的补丁。因此，安全公司往往通过热修复（hotfix）和通用漏洞缓解措施（如输入验证、内存监控、行为分析等）来提供一定的保护。然而，这些措施并非万能，更多的是应对一些常见、通用的漏洞，为无法打补丁或没有补丁的环境提供保障。

## 用户视角

从用户的角度来看，我们希望通过本节内容让读者意识到，不能心存侥幸——任何对外开放的服务都可能成为黑客的攻击目标。用户不应相信“补丁无用论”或质疑补丁有效性的错误观点，诸如认为安装补丁会导致系统性能下降、产生兼容性或稳定性问题等。即使部分用户因未支付相关服务费用而无法获得补丁，也应寻求其他方式保护系统安全。

另外，有些用户可能由于担心补丁带来的潜在不稳定性或对业务的影响而选择不更新系统。然而，必须明确的是，安全补丁是防止和修复漏洞的最有效手段之一，应该将补丁管理作为常规安全实践，定期执行。

## 漏洞治理建议

1. **定期更新与补丁管理**：及时更新系统和软件补丁，是解决漏洞问题最可靠的手段。管理员应建立健全的补丁管理机制，确保所有设备和系统都在第一时间获得修复。

2. **安装安全防护软件**：如前文所述，安全软件能够提供多层次的漏洞防御和缓解机制，减少通用漏洞造成的危害。定期更新安全软件，提升防护能力。

3.**减少对外暴露的服务**：尽量减少非必要的对外服务暴露，采用反向代理等技术手段降低服务被探测的可能性，减少潜在攻击面。

## 漏洞与工具

我们总结了在2024年的勒索攻击活动中经常被使用到的漏洞。其中主要的漏洞基于CVE/CNVD编号的归类汇总如下：

**勒索传播中经常使用到的漏洞（基于CVE/CNVD编号）**

| 漏洞编号 | 涉及产品/应用/服务/设备 | 相关关键词 |
|---|---|---|
| CVE-2022-2294 | Chrome | 缓冲区溢出漏洞 |
| CVE-2022-21999 | Windows Print Spooler服务 | 权限提升漏洞 |
| CVE-2022-2295 | Chrome | 堆损坏 |
| CVE-2023-27532 | Veeam Backup & Replication | 关键功能漏洞身份验证缺失 |
| CVE-2023-22515 | Atlassian Confluence | 身份验证漏洞 |
| CVE-2022-22954 | Vmware Workspace ONE Access<br>VMware Identity Manager | 远程代码执行漏洞 |
| CVE-2022-41080 | Microsoft Exchange Server服务 | 权限提升漏洞 |
| CVE-2023-24880 | Windows SmartScreen | 安全功能绕过漏洞 |
| CVE-2021-27876 | Veritas Backup Exec | 代理文件访问漏洞 |
| CVE-2021-27877 | Veritas Backup Exec | 代理不正确身份验证漏洞 |
| CVE-2021-27878 | Veritas Backup Exec | 命令执行漏洞 |
| CVE-2023-47246 | SysAid | 路径遍历漏洞 |
| CVE-2019-1068 | Microsoft SQL Server | 远程代码执行漏洞 |
| CVE-2019-068 | Microsoft SQL Server Reporting Services | 远程代码执行漏洞 |
| CVE-2020-3259 | Cisco AnyConnect | 信息泄露漏洞 |
| CVE-2024-1708 | ConnectWise ScreenConnect | 路径遍历漏洞 |

| | | |
|---|---|---|
| CVE-2024-1709 | ConnectWise ScreenConnect | 身份绕过漏洞 |
| CVE-2017-10271 | WebLogic | 远程代码执行漏洞 |
| CVE-2022-41802 | OpenHarmony | 内核堆栈溢出漏洞 |
| CVE-2022-41082 | Microsoft Exchange Server服务 | 远程代码执行漏洞 |
| CVE-2023-3467 | Citrix | 权限提升漏洞 |
| CVE-2022-24682 | Zimbra Webmail | 跨站脚本漏洞 |
| CVE-2018-13374 | FortiADC, Fortinet FortiOS | 不当访问控制漏洞 |
| 瑞友天翼SQL注入漏洞 | 瑞友天翼 | SQL注入漏洞 |
| CVE-2022-27924 | Zimbra | Zimbra memcache命令注入 |
| CVE-2022-27925 | Zimbra | 管理目录遍历 |
| CVE-2022-30333 | UnRAR | 目录遍历漏洞 |
| CVE-2022-37042 | Zimbra | 身份验证漏洞, 远程代码执行漏洞 |
| CVE-2022-24521 | Windows 通用日志文件系统驱动程序 | 特权提升漏洞 |
| CVE-2022-30190 | Microsoft Windows支持诊断工具 | 远程代码执行漏洞 |
| CVE-2021-42278 | Active Directory 域 | 特权提升漏洞 |
| CVE-2021-42287 | Active Directory 域 | 特权提升漏洞 |
| CVE-2017-5638 | Apache Struts | 远程代码执行漏洞 |
| CVE-2017-0199 | Microsoft Office, WordPad | 远程代码执行漏洞 |
| CVE-2021-22205 | GitLab | 远程命令执行漏洞 |
| CVE-2023-3519 | Citrix ADC, Citrix Gateway | 远程代码执行漏洞 |
| CVE-2024-26169 | Windows 错误报告服务特权漏洞提升 | 特权提升漏洞 |
| CVE-2024-4577 | PHP-CGI | 参数注入 |
| CVE-2022-29499 | Mitel VoIP | 远程代码执行漏洞 |

| | | |
|---|---|---|
| CVE-2023-48788 | Fortinet FortiClientEMS | SQL注入漏洞 |
| CVE-2021-22986 | F5 BIG-IP | 远程代码执行漏洞 |
| CVE-2024-37085 | VMware ESXI | 身份验证漏洞 |
| CVE-2021-1732 | Windows Win32k | 权限提升漏洞 |
| CVE-2024-23897 | Jenkins | 身份验证漏洞 |
| CVE-2023-38831 | WinRAR | 代码执行漏洞 |
| CVE-2023-46747 | F5 BIG-IP | 身份验证漏洞 |
| CVE-2023-27997 | Fortinet FortiOS | 堆缓冲区溢出漏洞 |
| CVE-2023-36884 | Windows Search | 远程代码执行漏洞 |
| CVE-2020-0787 | Windows Background Intelligent Transfer Service (BITS) | 权限提升漏洞 |
| CVE-2022-41352 | Zimbra | 文件上传漏洞 |
| CVE-2023-24489 | Citrix ShareFile | 身份验证漏洞 |
| CVE-2024-21338 | Windows Kernel | 权限提升漏洞 |
| CVE-2024-40711 | Veeam Backup & Replication | 反序列化漏洞 |
| CVE-2023-41266 | Qlik Sense | 身份验证漏洞 |
| CVE-2023-41265 | Qlik Sense | 权限提升漏洞 |
| CVE-2020-28188 | TerraMaster TOS | 远程代码执行漏洞 |
| CVE-2022-24989 | TerraMaster NAS | 代码执行漏洞 |
| CVE-2022-24990 | TerraMaster NAS | 信息泄漏漏洞 |
| CVE-2019-7192 | QNAP | 任意文件读取漏洞 |
| CVE-2019-7194 | QNAP | 路径遍历漏洞 |
| CVE-2019-7195 | QNAP | - |
| CVE-2018-4878 | Adobe Flash Player | 代码执行漏洞 |

| | | |
|---|---|---|
| CVE-2023-38035 | Ivanti MobileIron Sentry | 身份验证绕过漏洞 |
| CVE-2023-48365 | Qlik Sense | 远程代码执行漏洞 |
| CVE-2024-51567 | CyberPanel | 远程命令执行漏洞 |
| CVE-2024-51568 | CyberPanel | 身份验证绕过漏洞 |
| CVE-2024-51378 | CyberPanel | 身份验证绕过漏洞 |
| CVE-2024-40766 | SonicWall SonicOS | 不当访问控制漏洞 |
| CVE-2022-47966 | Apache Santuario xmlsec | 远程代码执行漏洞 |
| CVE-2023-29300 | Adobe ColdFusion | 代码执行漏洞 |
| CVE-2023-38203 | Adobe ColdFusion | 代码执行漏洞 |
| CVE-2022-42475 | FortiOS SSL VPN | 代码执行漏洞远程命令执行漏洞 |
| CVE-2017-0290 | Microsoft Malware Protection Engine | 远程代码执行漏洞 |
| CVE-2024-42057 | Zyxel ATP | 命令注入漏洞 |
| CVE-2022-37969 | Windows 通用日志文件系统驱动程序 | 特权提升漏洞 |
| CVE-2023-20263 | Cisco HyperFlex HX | 身份验证绕过漏洞 |

勒索软件传播中所利用的漏洞编号

# （三）

# 横向渗透攻击

横向渗透攻击是中大型企业内网面临的一项重大安全挑战，尤其在勒索攻击场景中，常常成为攻击者的关键策略之一。在典型的攻击模式下，攻击者首先通过一个受感染的终端或节点入侵，随后利用各种手段在内部网络中扩展，最终可能导致大规模的设备感染，甚至使整个网络瘫痪。

## 攻击目标：核心资产

企业的域控制服务器（DC）和管理服务器通常是黑客的首要攻击目标。一旦这些核心资产被攻陷，攻击者便能够在网络中自由行动，进一步渗透到其他系统和设备。此外，企业内网中往往存在统一或相似的软件配置和口令设置，这为攻击者提供了便利，使得他们可以通过攻破一个设备来威胁整个网络。

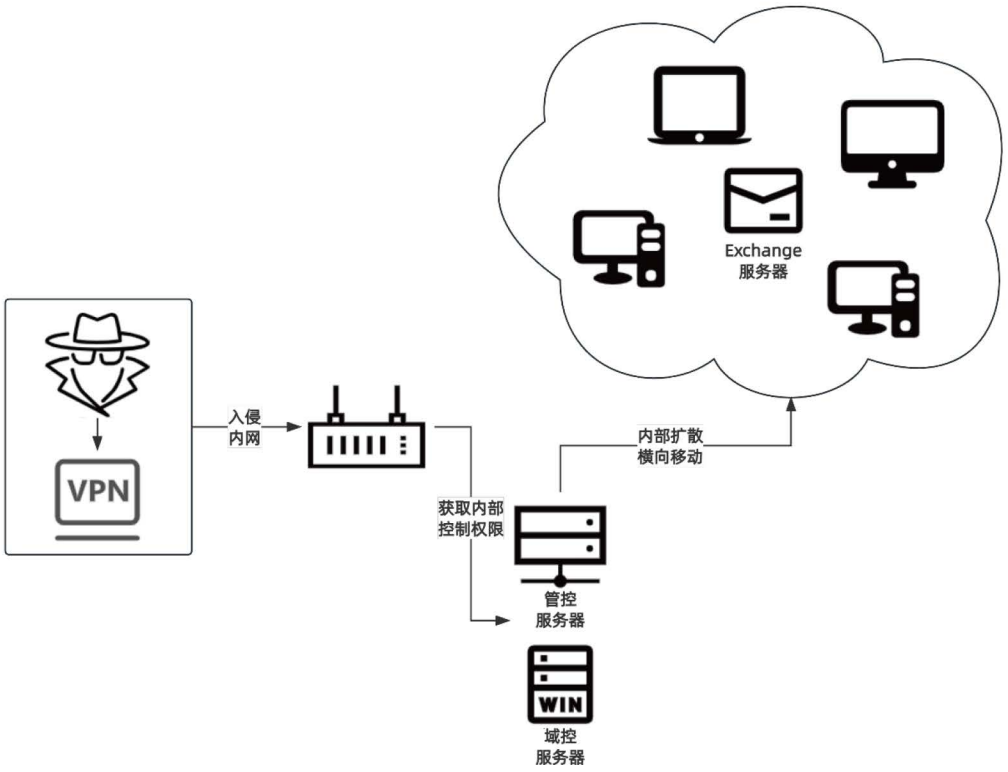
## 安全漏洞与攻击工具

内网设备的安全性与是否及时应用系统补丁密切相关。许多设备由于缺乏及时更新，变得异常脆弱，成为黑客攻击的首选目标。现代攻击者通常使用集成了多种漏洞利用工具的攻击工具包（如Exploit Kits），针对未打补丁的设备进行攻击，从而快速获得控制权并扩大影响范围。

## 横向渗透与勒索预警

在我们的勒索预警服务中，横向渗透攻击的检测占据了重要部分。通过监测网络中横向渗透到勒索软件投毒的短暂时间差，我们能够及时发出警报，帮助企业在攻击初期采取应急响应措施，防止攻击蔓延并降低损失。

下图展示了，横向渗透攻击，如何在内网中渗透活动。




**典型横向渗透攻击流程**

下面整理了一些勒索家族在横向渗透中常用的攻击工具，包括进程查看器，端口扫描工具，口令提取工具，各种内网渗透工具。黑客通过这些工具大大简化了攻击过程，降低了黑客的攻击门槛。其中有部分工具是通用工具，被几乎所有黑客团伙使用，最为常见的通用工具有如下这些：

- **Rootkit工具**：PChunter、Process Hacker、Process Explorer
- **密钥窃取工具**：Mimikatz
- **资源收集与数据窃取工具**：Everything、NetworkShare

  （值得一提的是：Everything除了被用来搜集文件外，还被黑客用来批量窃取文件。Everything可被部署为文件服务器，攻击者利用这一特性，在被攻击设备中暗中植入everything作为后门使用。）
- **远程控制工具**：AnyDesk

**下面对当前最流行的部分勒索家族，及其使用的工具进行了一些整理：**

## 勒索软件横向传播中利用的工具

| 勒索家族 | 利用工具 |
| --- | --- |
| LockBit | MEGAsync, CrackMapExec, Mimikatz, PsExec, AnyDesk, GMER, Process Explorer, FileZilla, ScreenConnect, LaZagne, NetworkShare, Cobalt Strike, Exfitrator-22, KPortScan, NetScan, PChunter, PowerTool, Process Hacker, Network Password Recovery, HRSWord, denfendercontrl, Exmatter, Poortry, SplashTop |
| Mallox | fscan, AnyDesk, powercat, lcx, DefinderControl, Mimikatz, NetScan, Process Hacker, PChunter, Cobalt Strike, Nasp, NetworkShare |
| BlackByte | Cobalt Strike, AnyDesk, anonymfiles.com, file.io, LoLBins, WinRAR, Exbyte |
| CL0P | DEWMODE, FlawedGrace, SDBot, Truebot, Cobalt Strike |
| Everest | ProcDump, NetScan, SoftPerfect Network Scanner, WinRAR, AnyDesk, Cobalt Strike, SplashTop, Atera Agent, TeamViewer |
| RansomEXX | Cobalt Strike, Mimikatz, Metasploit, Vatet Loader, LaZagne |
| GlobeImposter | Process Hacker, NetScan, PChunter, NetworkShare, Mimikatz |
| Makop | PChunter, Process Hacker, Process Explorer, NetScan, dfcontrol, netpass, NetworkShare, Everything, Mimikatz, mouselock, Exploit, Advanced Port Scanner, ARestore, PuTTY, PsExec, YDArk, PuffedUp, KPortScan, NLBrute, denfendercontrl, ydayk, GotoHTTP, Nasp, Bdcontrol |
| Buran | AZORult, Vidar, Rig EK, PChunter, Mimikatz, NetworkShare, Process Hacker, dfcontrol, YDArk |
| Magniber | Magnitude Exploit Kit, YDArk, Pchunter |
| phobos | DataBase, DefinderControl, accountrestore, denfendercontrl, netpass, pyark, NetworkShare, Everything, FRP, frpc, KPortScan, Mimikatz, luciroot, NetScan, Nasp, PChunter, YDArk, PuTTY, dfcontrol, GMER, HRSWord, NLBrute, ydayk, WebBrowserPassView, Process Hacker, SmokeLoader, Cobalt Strike, BloodHound, Sharphound, NirSoft, MEGAsync, WinSCP, FTP |
| Stop | NetworkShare, Advanced Port Scanner, LaZagne |
| TellYouThePass | certutil, bitsadmin, PowerShell |
| BeijingCrypt | AnyDesk, PChunter, Everything, Process Hacker, netpass, PEview, KPortScan, Nasp, NetworkShare, HRSWord, GMER, NetScan |
| MedusaLocker | PChunter, denfendercontrl, Mimikatz, Process Hacker, NetScan, Advanced Port Scanner, HRSWord, PsExec, Bdcontrol |
| Medusa | NetScan, PsExec, put.io, Poortry, ConnectWise |

| | |
|---|---|
| Trigona | HRSWord, Atera Agent, SplashTop, ScreenConnect, AnyDesk, LogMeIn, TeamViewer |
| Cactus | PAExec, SuperOps, SplashTop, AnyDesk, Chisel, Rclone, PowerShell, SoftPerfect Network Scanner, Plink, ManageEngine UEMS, 7zip, PSnmap, Cobalt Strike |
| 8BASE | AnyDesk, SystemBC RAT, Gofile, Pixeldrain, files.dp.ua, AnonFiles, anonymfiles.com, MEGAsync |
| BlackSuit | Sliver, Chisel, Cloudflare, AnyDesk, Atera Agent, MobaXterm, PsExec, Rubeus, ScreenConnect, Cobalt Strike, Mimikatz, WinRAR, WinSCP, Sharphound, SystemBC RAT, AdFind, SysInternals |
| INC Ransom | PsExec, MEGAsync, WinRAR, LoLBins, AnyDesk, NetScan, 7zip, PuTTY, Advanced IP Scanner, AdFind, restic, Restic |
| Rhysida | Pstools, PuTTY, AnyDesk, NetSupport Manager, PsExec, WinSCP, MEGAsync, SystemBC RAT, SysInternals, Azure Storage Explorer |

勒索软件传播中所使用的黑客工具

# （四）

# 共享文件

## 加密共享文件夹：勒索攻击中的潜在风险

虽然加密共享文件夹本身并不直接属于勒索软件的传播手段，但根据实际用户反馈和安全事件处理经验，这一问题在企业和个人网络中频繁出现，值得特别关注。了解并采取适当的防护措施可以显著降低勒索软件加密共享文件夹带来的风险。

在加密共享文件夹的事件中，通常不是存储这些文件的服务器或存储设备本身遭到了入侵，而是其他具有访问权限的设备被感染，导致共享文件夹内的文件遭到加密。

## 勒索软件如何加密共享文件

当前流行的勒索软件通常具备扫描和枚举网络资源的能力，包括共享文件夹。这些勒索软件在传播过程中，会自动扫描网络中的共享资源，并尝试加密其中的文件。加密共享文件

夹通常是这些勒索软件的默认行为，且加密操作在没有用户干预的情况下自动进行。

此外，许多用户在配置共享文件夹时为了便捷访问，可能设置了过于宽松的权限管理，甚至允许具有写权限的访客用户进行访问。这种设置无意中为勒索软件提供了通过低权限账户访问并加密文件的路径。

### 有效防护措施

**要有效防范共享文件夹被勒索软件加密的风险，可以从以下几个方面着手：**

1. **实行严格的权限管理**：限制普通用户对关键共享文件的写入权限，确保只有授权的管理员或特定用户组能够对敏感文件进行修改。避免将过高的访问权限授予不必要的用户。
2. **创建网络分隔（VLAN）**：通过将关键业务系统和数据存储区域分隔到不同的虚拟局域网（VLAN）中，可以减少跨区域的网络访问。这样，勒索软件在感染某一设备后，无法轻易横向渗透至其他关键区域。
3. **定期审计用户访问权限**：对共享文件夹和其他重要资源的访问权限进行定期审计，及时撤销不再需要的权限，防止权限过度扩展而增加安全风险。
4. **定期备份共享文件夹数据**：对共享文件夹中的重要数据进行定期备份，并确保备份数据的安全性。备份可以保证在勒索攻击发生后，数据能够迅速恢复，减少企业运营中断的时间和经济损失。

## （五）

## 僵尸网络投毒

僵尸网络，是网络攻击者执行各种恶意行为最喜爱的工具之一。攻击者通常会利用木马病毒、蠕虫、以及利用安全漏洞的工具来攻击劫持设备，将其转化为“肉鸡”以加入其庞大的僵尸网络中。一旦网络建立，攻击者可随时通过远程控制命令，操控这些“肉鸡”计算机或设备发起各种攻击活动。今年通过僵尸网络投递勒索的攻击有较为明显的减弱，但对僵尸网络的防范仍不可掉以轻心。

# （六）

# 社会工程学

社会工程学攻击是勒索软件攻击中常见且危险的手段之一，攻击者通过操控受害者的心理和行为来达到其目的。Black Basta勒索软件团伙就是一个典型的案例，它利用微软的快速助手（Quick Assist）功能，通过社会工程学手段发动勒索攻击。

Black Bast勒索软件团伙在选定攻击目标后，向目标用户的电子邮件发送大量合法订阅的邮件，然后通过电话联系目标用户，伪装成公司的IT技术支持团队，声称要帮助解决垃圾邮件问题，然后诱使受害者使用Quick Assis共享他们的设备。一旦获得访问权限，攻击者使用迅速在用户计算机中投递驻留后门，如QakBot、Cobalt Strike等，这些工具用于进一步控制受害者的系统。


勒索软件利用社会工程学手段攻击

# （七）

# “自带易受攻击的驱动程序”（BYOVD）

“自带易受攻击的驱动程序”（BYOVD，Bring Your Own Vulnerable Driver）是近年来新兴的一种勒索软件攻击技战术，攻击者通过利用易受攻击的或专门编写的恶意驱动程序绕过安全防护，直接在内核层面关闭或干扰安全软件，从而为勒索软件的部署提供便利。

## 攻击案例分析

LukaLocker勒索软件：在LukaLocker的攻击过程中，攻击者利用Truesight.sys驱动程序进行操作。安装该驱动程序后，任何正在运行的安全应用程序（如Trend Micro的产品）都会立即失效，这使得勒索软件得以顺利部署并执行。

Makop勒索软件：在Makop勒索软件的攻击中，攻击者利用了loldrivers技术在内核层关闭安全软件进程。攻击过程中，发现的恶意驱动程序包括ksapi64.sys、viragt64.sys和SysMon.sys，这些驱动程序通过绕过安全软件的保护，使得勒索软件能够在目标系统中顺利运行。

RansomHub勒索软件：RansomHub攻击者通过自定义的工具EDRKillShifter，专门设计了绕过EDR（端点检测与响应）防护软件的驱动程序。这些驱动程序可以根据攻击者的需求，绕过不同种类的防护系统，使得勒索软件能够在受害者的系统中执行并加密数据。

# （八）

# 其它攻击因素

以上我们详细介绍了国内勒索软件最常见的传播手法。除此之外，勒索软件的传播途径还包括：网页挂马、激活破解类软件、游戏外挂、钓鱼邮件、即时通讯（IM）传播、供应链攻击等。这些攻击手法在往年的报告中已有充分讨论，因此在此不再赘述。值得注意的是，勒索软件的传播策略和渠道已变得非常多样化，几乎涵盖了过去传统病毒和木马攻击所采用的所有手段。

然而，勒索软件攻击的核心区别在于其攻击目标：勒索软件专注于对数据的劫持，而与传统恶意软件的主要目标——破坏功能或窃取信息——有所不同。勒索软件通过加密数据并要求赎金，直接影响企业的核心资产和运营，给受害者带来更为严重的经济损失和业务中断。

第四章

# 勒索软件发展与趋势分析

P082

P087

# 勒索软件发展与趋势分析

在2024年，勒索软件威胁毫无意外的再次成为年度最热门网络安全话题。个人、企业和政府都无法忽视勒索软件带来的影响。不管是在国际纷争、商贸活动还是个人社会生活中，勒索软件威胁都无处不在。短短几年的时间里，勒索软件已经从一个新兴威胁发展成为信息网络中最受关注的威胁之一。我们通过回顾今年发生的重大勒索事件，来探索勒索软件的发展趋势，并从我们为应对勒索软件威胁所做的努力中，探讨未来的勒索应对之道。

## 一

## AI成为勒索对抗热点

2024年被认为是人工智能（AI）井喷之年，AI技术，尤其是以GPT为代表的生成式AI，展现出了前所未有的优势，推动了各行各业的数字化转型。在安全领域，AI的应用也开始取得显著进展，各大安全公司纷纷推出了结合AI技术的产品和服务。AI不仅渗透到企业的安全产品中，也出现在当前的红蓝对抗（攻防对抗）中，成为安全防护的重要工具。未来，谁能有效利用AI技术，谁就能在与勒索软件等网络威胁的对抗中占据主动。因此，AI无疑成为当前勒索软件攻防发展的热点。

### （一）

### 利用AI发起更加智能化的网络攻击与勒索攻击

随着生成式AI和深度学习技术的飞速发展，黑客和攻击者已经在借助AI发起更加高效、复杂、隐蔽的网络攻击。AI技术已经被广泛应用于攻击工具的生产，病毒软件的制造，攻击数据的清洗筛选等场景。未来，AI将进一步增强勒索软件的智能化特点，使其具备自我学习与适应能力。AI不仅可以通过模拟用户行为绕过传统的安全防护，还能根据受害者的系统架构和漏洞进行精准定制化攻击，未来的攻击都将是“定制化”攻击。

## （二）

## 勒索病毒的自动化攻击能力增强

勒索病毒的自动化能力大幅提升是AI应用在网络攻击中的一个重要体现。当前，勒索病毒的传播通常仍依赖于人为操作，尽管已有一定程度的自动化工具，但攻击者仍需手动选择扫描目标、挑选漏洞利用方式、部署恶意软件等关键步骤。而AI的引入，使得勒索病毒的攻击更加智能化和自动化，攻击者无需手动干预即可实现自动扫描、漏洞利用、传播及数据加密等一系列过程。AI驱动的勒索病毒将能够自我学习和适应目标环境，不断优化攻击路径和手段。通过分析目标系统的弱点，AI可以自动选择最优的攻击方法，显著提高勒索攻击的成功率。此外，AI还能自动生成变种病毒，以躲避检测和防御系统的识别，从而实现持续的攻击。这种自动化和持续性将大大增加企业防御的难度。

## （三）

## AI赋能的“新安全”产品

AI在安全产品中的应用，特别是增强离线安全能力，正成为解决当前网络安全难题的新思路。在“云查杀”模式逐渐成为主流的今天，如何有效防御离线环境中的攻击并及时发现潜在威胁，依然是网络安全领域的一大挑战。传统的离线安全防护依赖于持续更新的情报资源，通常通过标准化后将情报打包并同步到离线环境中。这种方式存在多个问题：一是运行效率低，情报资源更新不够及时，导致防御反应延迟；二是转化过程中的损耗较大，尤其是在威胁数据量巨大的情况下，筛选后的信息可能无法充分覆盖所有潜在的攻击场景；三是更新周期较长，无法实现实时响应和动态防护。借助AI技术，可以通过训练模型来模拟当前网络攻击的战术和技术，进而识别潜在威胁。这些训练好的AI模型能够在离线环境中执行高效的安全分析和攻击识别，不依赖于实时更新的情报资源。通过这种方式，AI能够较为完整地传递“大网安全”的能力到离线环境中，实现对未知威胁的快速响应。目前这一方案已经开始在360的安全产品中验证并使用。

不仅限于上述几点，AI在提升安全产品的预测能力、降低运营强度等方面也已经显现出显著优势。利用AI改造当前的安全产品，将是一个充满潜力且需要持续探索的领域。接下来一年，将有更多创新的安全思路和解决方案逐渐得到验证和落地。

## （四）

## AI在企业中的应用，降低企业使用安全产品的门槛

AI技术在安全领域的应用也在大幅降低企业使用高端安全产品的门槛。许多传统的安全产品需要高度专业的技能才能有效使用，尤其是在安全分析、应急响应等方面，对企业的安全团队要求较高。然而，AI技术的加入使得这些复杂的任务能够被自动化处理，降低了安全运维的难度。

AI驱动的安全产品能够提供更加智能化的威胁检测、自动化的事件响应和实时的漏洞修复建议，这些功能使得即便是没有深厚安全背景的IT人员，也能够使用AI来提升企业的整体安全防护水平。尤其是对于中小企业，AI提供的低成本、高效能的安全服务，使其能够在资源有限的情况下，也能享有与大企业相同的安全防护能力。

AI正在成为网络安全领域的转折点。其广泛应用不仅提升了安全产品的效能，也引发了一场深刻的变革。从防御角度来看，AI的自我学习、数据处理和异常检测等优势，使得安全防护更加智能和动态，弥补了传统防护手段无法快速应对演化攻击的不足。然而，AI的双刃剑效应逐渐显现，它既是防御方的利器，也被攻击者用来增强攻击能力。这种技术的双向演进，令网络安全的未来充满不确定性。因此，AI的应用不仅代表技术创新的突破，也标志着网络安全发展的一次重要转折，未来的安全防护将更加依赖AI技术。掌握这项技术的产品将在竞争中占据主导地位。

# 二

# 专业化、系统化攻击频发

近年来，随着勒索软件攻击的规模化和系统化发展，中小企业面临的网络安全威胁日益加剧。以TargetCompany(Mallox)和TellYouThePass为代表的勒索黑客组织，在过去一年内发起了数十次大规模攻击，主要针对中小企业的各类业务系统，攻击规模从数百台到数千台不等。攻击过程中，利用n-day漏洞的情况愈加普遍，尤其是大量公开漏洞被黑客迅速应用于攻击活动中。虽然这些攻击团伙没有大规模发现0day漏洞或编写漏洞利用代码的能力，但他们具备较强的安全敏感度，能够迅速获取并利用公开的漏洞信息，改写PoC代码，应用于最新的攻击之中。

解决这一问题的关键在于加强安全管理。对于资源有限的中小企业而言，服务器的安全运维是一个亟待解决的现实问题。许多中小企业选择将此类任务外包给IT部门或第三方服务商。然而，由于安全管理经验和技术能力的差异，企业的安全防护能力存在较大差距。许多小型供应商由于缺乏专业的安全管理经验，通常只能完成基础的产品部署，忽视了对系统的持续监控与安全运维，造成了安全防护的漏洞。

在实际案例中，我们发现许多中小企业在遭遇勒索攻击后，无法有效查明攻击源和漏洞根本原因。在缺乏专业安全团队的介入下，企业通常只能通过简单的恢复系统来应对攻击，导致漏洞未能及时修复，进而使企业反复遭遇勒索攻击。缺乏专业防御机制和漏洞修复流程，使得企业长期暴露在安全风险之中。

为应对这一挑战，中小企业可以考虑采用第三方托管服务（SaaS解决方案），提升其安全运维能力。通过与经验丰富的安全团队合作，企业可以更高效地识别、响应并防御安全威胁，从而以较低成本增强安全防护水平。结合外部专业力量与企业内部IT运维人员的协作，不仅能够优化企业的安全防护能力，还能减少因技术和资源不足带来的安全隐患，确保企业能够有效应对复杂的网络安全挑战。

# 三

# 创新驱动反勒索技术发展——安全技术新突破

在于勒索软件攻击的对抗过程中，创新始终是打破平衡，实现突破的关键方法。2024年360也在这方面做了大量努力。

2024年，我们在企业安全产品中，强化了弱口令暴破防护的能力，提供了包括登录时间段控制、风险地区IP拦截，ip黑白名单以及爆破日志查询等功能，以适应企业不同的使用环境。增加支持了更丰富的协议，保护更多的企业应用。

2024年，我们改进了一系列反勒索方案，新增了一套一种轻量化，不依赖白名单机制的勒索攻击行为识别防护技术，基于360多年来采集的大量勒索攻击行为特点，通过实时记录程序对文件的操作历史，判别可能存在的勒索攻击行为。

新增了对Linux、信创等终端的勒索防护方案，扩展了防护范围，为政企单位提供了更多选择。

提升了反勒索溯源工具能力，在“渗透痕迹记录”中目前已收集了超过600项攻击痕迹检测点，覆盖了国内外百余家安全厂商的安全产品的防护致盲检测。能够协助管理员快速定位攻击原因，帮助管理员排查设备安全状况。

在安全内功方面，扩展了JavaRasp通用java漏洞防御，已支持6大类漏洞的动态防御，可用于各类基于java的web应用的防护。经过验证，已确认支持的超过30款产品，超过300类各类漏洞的防御。

新增DNRSP漏洞防御，DNRSP专门用于保护基于.Net技术构建的应用程序。借助360的云体系大数据，DNRSP能够有效防范与.Net相关的各种安全漏洞，包括但不限于远程代码执行、文件上传攻击和反序列化漏洞，实现NDay漏洞的防护和0Day漏洞的告警，从而保障应用程序的安全运行和系统数据的安全。同时，针对IIS，增强了对IIS Backdoor模块的告警和拦截，实现了对IIS全面的检测能力和防护能力。

还有“远程桌面截杀对抗”，“远程工具阻断”，“浏览器密钥保护”等多项安全功能更新。

# 第五章

# 安全建议

P088

P095

# 安全建议

面对严峻的勒索软件威胁态势，我们分别为个人用户和企业用户提供了以下安全建议。希望能够为尽可能多的用户提供全方位的计算机安全保障，最大限度的降低勒索软件感染用户系统的成功率。

## 一

## 针对企业用户的安全建议

### （一）

### 发现遭受勒索软件攻击后的处理流程

1.发现有设备感染勒索软件后不要惊慌，及时进行安全处置，在第一时间将潜在损失降至最低，并可有效减少被勒索软件二次攻击可能性。

2.对被攻击设备及时进行隔离，切断其与整个内部系统和其他设备的连接。如果同一子网下多台设备中招，可尝试对整个子网进行整体的外部隔离操作

3.企业所面对较为常见的外部攻击入口包括：远程桌面弱口令、Web服务漏洞以及数据库弱口令。而企业的内部设备则通常会在勒索软件利用上述外部入口成功入侵后遭遇横向渗透攻击。因此，在建议企业的IT管理人员在发现遭到勒索攻击的第一时间，可通过防火墙等安全软件切断外部对远程桌面的访问。并关闭服务器的Web服务端及数据库的外部访问端口，作为应急防护手段。

4.在发现勒索攻击后，尽快联系安全厂商或专业安全团队对内部网络进行全面的排查处理。如果企业拥有自己的安全团队也可自行排查，但仍需查清具体的入侵来源、攻击路径以及受影响资产情况，避免留下安全隐患。

5.根据排查结论对风险点位做对应的加固修复。同时，应假定黑客已窃取了所有相关设备中存储的凭据。对于公司内部在攻击中涉及到的所有设备中的各类口令及凭据全部进行统一更新。

6.目前主流勒索软件均无法通过技术手段直接破解，因此，预防永远是面对勒索攻击最有效的应对手段。而对攻击原因进行相近的排查则可以最大限度的避免企业再次成为勒索攻击的目标。无视原因，一味盲目的重置系统，则只会埋下更为严重的安全隐患！

## （二）

## 企业安全规划建议

对企业信息系统的保护，是一项系统化工程，应在企业信息系统建设初期就加以考虑，但对现有环境的改善提升，也能提升企业应对网络攻击风险的能力。以下从最关键的网络建设，资产管理，人员管理方面进行介绍。

### 1.网络建设

●网络架构

业务、数据、服务分离。不同职能部门与区域之间通过VLAN或子网等手段进行分离，减少因为单点沦陷造成更大范围的网络受到攻击。

●内外网隔离

合理设置对外开放区域，对外提供服务的设备要做严格管控。减少企业被外部攻击的暴露面。

●安全设备部署

在企业终端和网络关键节点部署安全设备，并对安全设备告警情况进行日常监控和及时处置。

●权限控制

包括业务流程权限与人员账户权限都应该做好控制，如控制共享网络权限等。原则上应以最小权限提供服务，降低因为单个账户沦陷而造成更大范围的影响。

●数据备份保护

对关键数据和业务系统做备份，如离线备份、异地备份、云备份等，避免因为数据丢失、损坏、无法访问等情况造成的业务停摆，甚至被迫向攻击者妥协。

●敏感数据隔离

对敏感业务及其相关数据做好网络隔离，如有必要甚至建议做好设备之间的物理隔离。避免双重勒索软件在入侵后轻易窃取到敏感数据，对公司业务和机密信息造成重大威胁。

**2.安全管理**

●账户口令管理严格执行账户口令安全管理，重点排查弱口令问题。杜绝各类口令及凭据长期不更新、账户口令共用、直接使用应用的内置或默认账户等安全问题。

●漏洞修补

了解企业数字资产情况，将补丁管理作为日常安全维护项目。关注补丁发布情况，及时更新和修补系统、应用、服务及硬件产品的相关固件。定期执行漏洞扫描，及时发现设备中存在的安全问题。

●权限管控

定期检查账户情况，审核账户权限的适当性，及时停用非必要的账户权限，对新增账户应有足够警惕并做好各类账户的登记管理。

●内网加固

进行内网主机加固，定期排查未正确进行安全设置、未正确安装安全软件的设备，关闭设备中的非必要服务，提升内网设备安全性。

3.人员管理

●安全教育

对员工进行安全教育，培养员工安全意识，如识别钓鱼邮件、钓鱼页面等。

●行为规范

制定工作行为规范，指导员工如何正常处理数据，发布信息，做好个人安全保障。如避免员工将公司网络部署，服务器设置发布到互联网之中。

●设备及网络使用规范

要求员工不共享企业内网，办公设备不安装来路不明的软件等。

## （三）

## 遭受勒索软件攻击后的防护措施

1.比照“企业安全规划建议”中的事项，对未尽事项进行及时更正或加强。

2.检测系统和软件中的安全漏洞，及时进行修补。

3.检查口令及凭据是否具有足够的长度和复杂性，并更新安全度不足或疑似已遭泄露的口令及凭据。

4.对于在勒索攻击中尚未遭到加密的重要文件进行及时备份，避免被仍处于活跃状态的勒索软件进行新一轮加密。

5.加强对敏感数据的隔离。如有条件，建议尽可能完全断开敏感数据与外界的一切连接。避免具有多重勒索功能的病毒进一步获取更多的重要信息作为勒索筹码。

# 二

# 针对个人用户的安全建议

对于普通用户，我们给出以下建议以帮助用户免遭勒索软件攻击。

## （一）

## 养成良好的安全习惯

1.电脑应当安装具有高级威胁防护能力和主动防御功能的安全软件，不随意退出安全软件或关闭防护功能，对安全软件提示的各类风险行为不要轻易采取放行操作。

2.可使用安全软件的漏洞修复功能，第一时间为操作系统和浏览器，常用软件打好补丁，以免病毒利用漏洞入侵电脑。

3.尽量使用安全浏览器，减少被挂马攻击、钓鱼网站攻击的风险。

4.重要文档、数据应经常做备份，一旦文件损坏或丢失，也可以及时找回。

5.电脑设置的口令要足够复杂，包括数字、大小写字母、符号且长度至少应该有8位，不使用弱口令，以防攻击者破解。

## （二）

## 减少危险的上网操作

1.不要浏览来路不明的色情、赌博等不良信息网站，此类网站经常被用于发起挂马、钓鱼攻击。

2.不要轻易打开陌生人发来的邮件附件或邮件正文中的网址链接，也不要轻易打开扩展

名为js、vbs、wsf、bat、cmd、ps1等脚本文件和exe、scr、com等可执行程序。对于陌生人发来的压缩文件包，更应提高警惕，先使用安全软件进行检查后再打开。对各类通讯群发来的文件，更不要盲目打开。

3.电脑连接移动存储设备（如U盘、移动硬盘等），应首先使用安全软件检测其安全性。

4.对于安全性不确定的文件，可以选择在安全软件的沙箱功能中打开运行，从而避免木马对实际系统的破坏。

### （三）

### 采取及时的补救措施

1.安装360安全卫士并开启反勒索服务，一旦电脑被勒索软件感染，可以通过360反勒索服务寻求帮助，以尽可能的减小自身损失。

## 三

# 不建议支付赎金

最后——无论是个人用户还是企业用户，都不建议支付赎金！支付赎金不仅变相鼓励了勒索攻击行为，而且解密的过程还可能会带来新的安全风险。

用户可以首先尝试通过还原备份、数据恢复、数据修复等手段挽回部分损失。例如部分勒索软件为了提高加密效率，只会对文件的头部数据进行部分加密，对于某些特定类型的文件（通常是数据库文件）可以尝试通过数据修复手段来找回被加密的文件内容。

即便在损失不可挽回又无法承受的前提下不得不支付赎金，也可尝试与黑客协商来降低赎金价格，同时在协商过程中应尽可能避免暴露自己真实身份信息和急迫程度，以免黑客漫天要价。

# 四

# 勒索事件应急处置清单

在此，我们准备了一份勒索软件事件的应急排查处置清单，遇到此类问题的管理员，可对照下面清单，完成事件的初步处理，之后再由专业团队详细排查事故原因。

## 勒索软件应急处置清单

**✧检查中招情况**

检查有哪些设备被攻击，常见被攻击特征有：文件后缀为被改，文件夹留下勒索信息，桌面背景被修改，弹出勒索提示信息。

□公网服务器
□域控设备与管控设备
□内网共享服务器
□办公机（检查是否仅是共享文件夹被加密）

**✧控制勒索蔓延**

根据现场情况，对已经发现的被攻击设备或者存在风险的设备与网段进行临时管控，常见管控方法包括：

●访问控制
- □网络隔离/主机隔离
- □端口访问控制（常见端口包括：445、135、137、139、3389、22、6379、3306、7001）
- □设置IP访问黑白名单：禁止国外IP访问/仅允许特定IP访问 或 仅允许本地IP访问
- □控制重要设备的访问权限，或对重要设备做临时下线处理。

●物理隔离
- □关闭设备/设备断电
- □拔出网线/禁用网卡/禁用无线网卡/移除移动网卡

●密码策略
- □修改全部管理员账号密码
- □禁用归属不明账号
- □临时停用非必要账号，修改所有普通用户账号密码

**✧排查关键节点**

在完成上述应急处置后，尽快确认以下事项，并联系安全团队进行进一步排查。（注意：被加密的文件本身不是病毒。）

□确定机器感染勒索软件时间
□收集可疑样本、被加密文件（少量）、勒索提示信息（一份）
□收集中招设备系统安全日志与防火墙日志
□检查存储有敏感信息设备是否被异常访问
□检查设备中账户情况，包括第三方软件账户，最近新增账户
□检查数据库账户，VPN账户，NAS账户，VNC类软件配置
□排查Web日志
□排查最近运行记录
□临时禁用发现的攻击账号
□使用安全软件进行扫描
□完成后续安全加固工作，安装补丁，修补存在的其它问题。

附录1

# 2024年勒索软件大事件

P096

P114

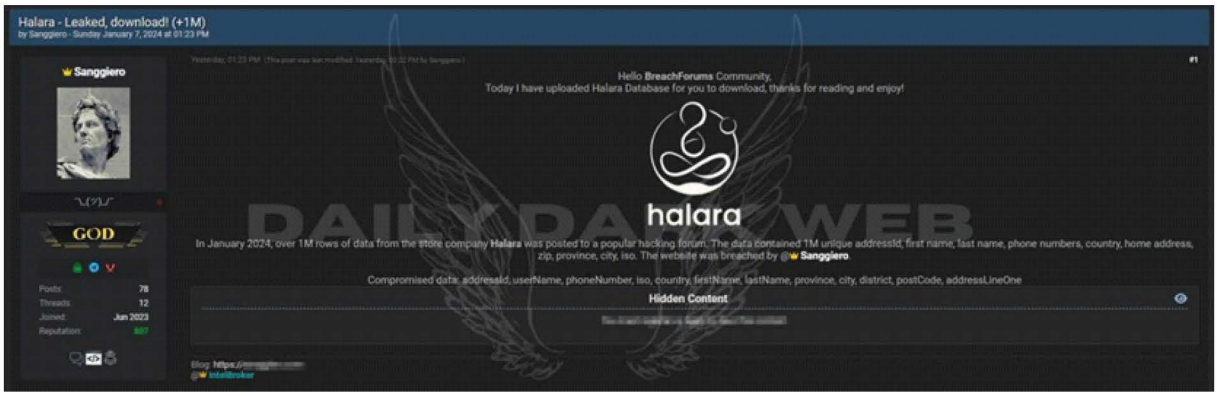
# 2024年勒索软件大事件

## 一

## 多家中国公司遭Sanggiero勒索

香港热门运动休闲服装品牌Halara正在调查一起数据泄露事件，此前据称有近95万名顾客的数据在黑客论坛上遭泄露。Halara称已经获知其客户数据已被窃取并在网上泄露，目前正在调查导致此次数据泄露的原因。

此次泄露来自于一个自称名叫“Sanggiero”的人。其声称1月初入侵了Halara并在黑客论坛和Telegram频道上分享了包含超过100万行被盗客户数据的文本文件。



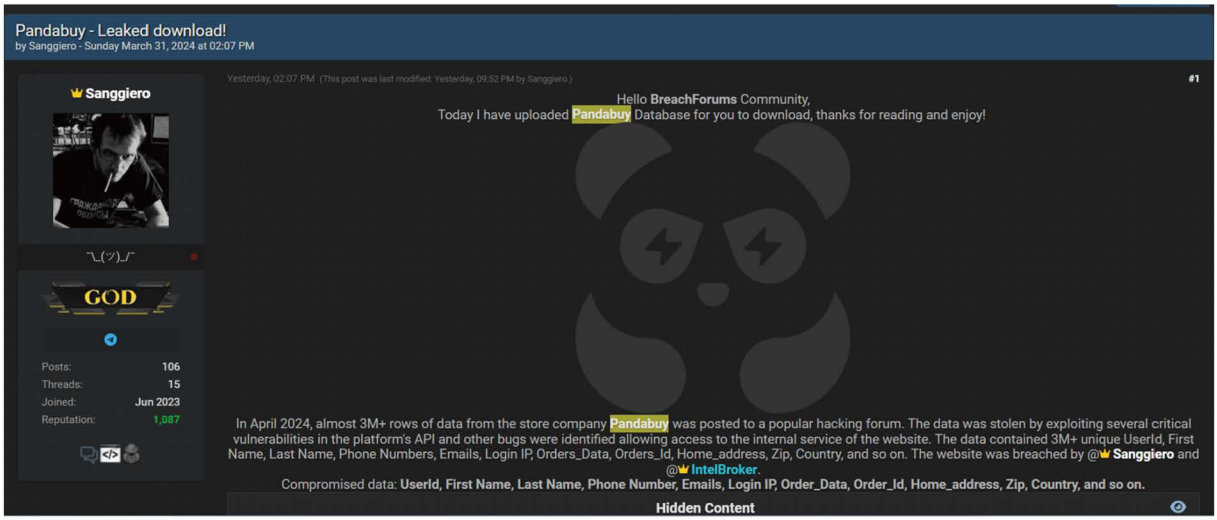

Sanggiero声称入侵了Halara

据称是遭窃取的数据中包含了：唯一地址ID、客户姓名、电话号码、国家/地区、家庭地址、邮政编码、省份、城市、ISO。

虽然Sanggiero称其包含超过100万行数据，但其发布的文本文件中仅包含941910条记录。目前尚无法确认所有数据准确的准确性，但其中一部分被泄露信息的人员确认了他们的确是Halara的客户，并称他们被列出的电话号码、姓名和地址等信息都是准确的。

Sanggiero方面表示并没有就被盗数据与Halara联系并决定免费发布这些数据，因为他认为这些数据并没有太大价值。

与之相似的是另一家中国公司——海外转运代购平台“Pandabuy”，也在2024年遭到了Sanggiero的勒索。该公司此前已向勒索者支付了赎金以防止被盗数据外泄，但在6月初，同一黑客组织再次对该公司进行了勒索。




Sanggiero对Pandabuy的勒索告示

2024年3月31日，Sanggiero在BreachForums上发布了据称是从Pandabuy窃取到的300万条数据，其中包含客户姓名、电话号码、电子邮件地址、登录IP地址、家庭地址以及订单详细信息。攻击者声称他们利用Pandabuy平台API中的几个关键漏洞窃取了这些数据。该数据被共享给了数据泄露通知服务“我是否已被窃取”(HIBP)，该服务将此次事件中多达135万个电子邮件地址添加到了其系统中。当时，Pandabuy选择了不发表任何公开声明，甚至有报道称该公司试图在Discord和Reddit上屏蔽相关用户的投诉。

而2024年6月3日，同一攻击者再次提出了4万美元的价格出售他声称之前从Pandabuy窃取的整个数据库。据称该数据库包含1700万行数据，这意味着数据集的规模比前一次要大得多。这一次，Sanggiero没有提供任何形式的客户数据样本，但他上传了包含敏感员工信息的截图——如电子邮件和密码等数据。

Pandabuy的一位发言人则表示他们此前已向黑客支付了一笔未披露的赎金以阻止数据泄露。但他们也在之后的调查中发现攻击者可能在受到赎金后又另将数据出售给了其他人，

因此公司决定不再与其进行沟通及支付赎金。

目前只能建议Pandabuy的用户立即重置与Pandabuy相关的各类密码，以尽可能避免真如攻击者所称的有更多数据被盗。

# 二

# 江森自控称勒索攻击导致的数据被盗造成其2700万美元损失

江森自控国际公司确认其在2023年9月的一次勒索软件攻击中出现了数据泄露问题，并造成了约2700万美元的经济损失。

根据此前报道，江森自控的亚洲办事处于去年9月遭到勒索软件攻击，导致该公司关闭了大部分IT设施，并影响了其面向客户的系统。而此次攻击的发起者为Dark Angels勒索软件，其声称从江森自控窃取了超过27TB的机密数据。随后，攻击者索要5100万美元的赎金以换取删除数据并提供文件解密器。


Dark Angels发布对江森自控的攻击信息

该公司承认服务中断并将原因归结为“网络安全事件”，但没有提供有关攻击类型或导致数据泄露的更多信息。

但在1月30日，江森自控向美国证券交易委员会提交的季度报告中证实，他们在2023年9月23日遭受的网络攻击实际上是勒索软件攻击，并导致了数据被盗。此外，该公司还表示处置此次网络攻击所耗费的相关费用达2700万美元。江森自控预计，随着他们后续的排查及各类取证、补救工作的进行，这一成本在未来几个月内将还会继续上升。

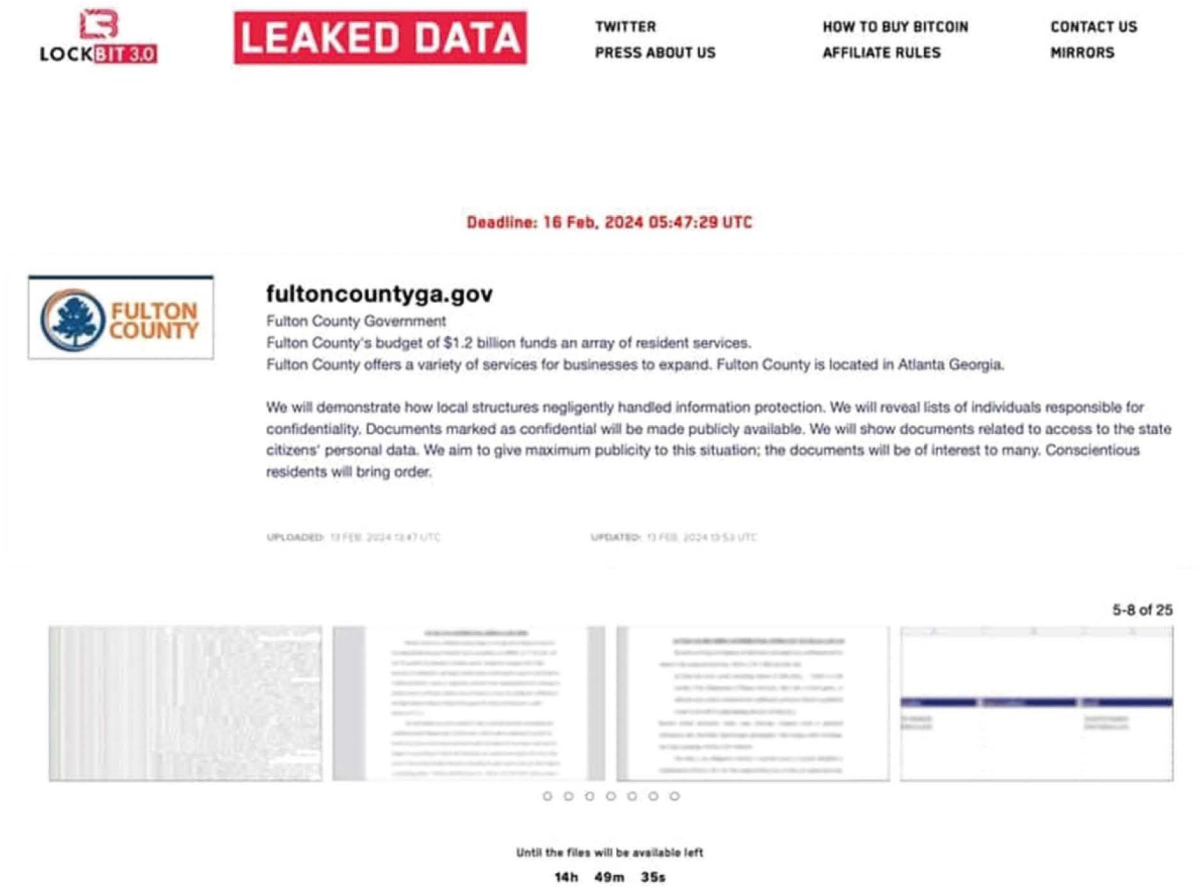
# 三

# 特朗普案件的机密信息遭勒索软件窃取

2月底，臭名昭著的勒索软件团伙LockBit宣称要进行一次大动作——即使是对于一个已经造成医院瘫痪并导致天然气管道关闭的犯罪组织来说也是绝无仅有的一次大动作：泄露美国前总统同时也是当前总统大选候选人特朗普的刑事起诉文件。

在2月的最后一周，LockBit在其暗网站上宣称：除非佐治亚州富尔顿县支付其要求的赎金，否则便将公布从该县政府系统中窃取的数据。而该县高等法院正是美国共和党总统候选人特朗普被控干预2020年大选一案的审判地。然而，当黑客组织指定的截止日期到来时，却没有公开任何文件。LockBit甚至神秘地从其网站上删除了任何提及此事的内容。富尔顿县官员否认已支付了赎金，也没有回答为什么泄密事件会就此作罢以及LockBit是否真的持有并仍然持有法院的相关文件。

而就在此次勒索威胁消失之前，执法部门针对LockBit展开了一次联合行动。该行动由英国国家犯罪局牵头，控制了LockBit大部分的网络设备，夺取了其数百个加密货币钱包，摧毁了其勒索活动中使用的暗网网站，执法机构甚至声称已经抓获了其一些成员及合作者。但就在几天后，LockBit便利用一个新的暗网网站死灰复燃，并发布了一份新的受害者名单。在该名单中，泄露富尔顿县文件的截止日期定在2月29日13点49分。




LockBit勒索软件发布对富尔顿县的勒索信息

# 四

# 瑞士表示Play勒索软件泄露了65000份政府文件

瑞士国家网络安全中心(NCSC)发布了一份报告，分析了Xplain遭受勒索软件攻击后的数据泄露情况，披露该事件影响了数千份敏感的联邦政府文件。Xplain是一家瑞士技术和软件解决方案提供商，为各种政府部门、行政单位，甚至该国的军事力量提供服务。

当时，攻击者声称盗取了包含机密信息的文件，而其也确实在之后的2023年6月初兑现了该威胁，并在其暗网门户上发布了被盗数据。这之后，瑞士政府开始调查泄露的文件，并立即承认泄露的数据可能包含属于瑞士联邦管理局的文件。


**瑞士遭Play勒索软件攻击**

2024年3月7日，瑞士政府发布了一份关于此事的声明，称有65000份政府文件遭到泄露：

- 这些文件中的大部分(95%)影响了联邦司法和警察部(FDJP)的行政单位：联邦司法办公室、联邦警察办公室、国家移民秘书处和内部IT服务中心ISC-FDJP。
- 联邦国防部、民防和体育部(DDPS)受到的影响较小，占该数据的3%多一点。
- 大约5000份文件包含敏感信息，包括个人数据(姓名、电子邮件地址、电话号码和地址)、技术细节、机密信息和账户密码。
- 一个由几百个文件组成的小集合，包含IT系统文档、软件或架构数据和密码。

公告称调查将于本月底完成，并将与联邦委员会分享全部结果和网络安全建议。

# 五

# 芯片制造商安世在遭勒索软件公布数据后确认泄露事件

荷兰芯片制造商Nexperia是中国公司闻泰科技的子公司。在4月12日的新闻声明中，该公司披露了其在3月份因遭到勒索攻击而迫使其关闭了IT系统并启动调查以确定影响范围。目前勒索软件团伙已泄露了涉嫌被盗数据的样本。Nexperia方面表示已向荷兰警方和数据保护机构报告了这一事件，并与FoxIT签约以寻求调查方面的协助。

4月10日，勒索网站Dunghill Leak宣布入侵了Nexperia，并声称窃取了1TB的机密数据，同时也发布了据称是被盗文件的样本作为证据。攻击者发布了电子元件、员工护照、保密协议和各种其他样本的扫描图像，但这些样本的真实性尚未得到Nexperia方面的证实。


Dunghill窃取安世数据并在网站发布

Dunghill声称，若不支付赎金，他们计划泄露以下数据：

- 371GB的设计和产品数据，包括：QC、NDAs、商业秘密、技术规格、机密原理图和生产说明。
- 246GB的工程数据，包括：内部研究和制造技术。
- 96GB的商业和营销数据，包括：定价和营销分析。
- 41.5GB的公司数据，包括：HR、员工个人详细信息、护照、保密协议等。
- 109GB的客户和用户数据，包括：SpaceX、IBM、Apple和华为等品牌。
- 121.1GB的各种文件和杂项数据，包括：电子邮件存储文件。

# 六

# 芯波音公司证实有勒索软件试图向其勒索2亿美元

波音公司5月8日表示，该公司于2023年10月已向LockBit勒索软件平台的网络犯罪分子缴纳了其向该公司索要的2亿美元勒索赎金。波音公司证实，该公司就是美国司法部于5月7日公布的一份起诉书中所提到的一家未具名的跨国航空和国防公司。这份起诉书指控俄罗斯公民德米特里·尤里耶维奇·霍罗舍夫是LockBit勒索软件的主要管理员和开发者。

但除此以外，波音公司拒绝进一步置评，并表示已将问题转交给FBI。而FBI方面则并未立即回应此次事件。

去年11月初，LockBit网站上曾公布了约4.3GB的波音公司数据，波音公司在当时曾表示并未向LockBit支付任何赎金。而在起诉书中提到的未具名公司是科罗谢夫及其同伙“索要巨额赎金”的一个例子，自2019年底或2020年初以来，他们已从受害者手中勒索了逾5亿美元赎金。

航空航天巨头波音公司正在调查一场影响其零部件和分销业务的网络攻击，此前LockBit勒索软件团伙声称他们攻入了该公司的网络系统并窃取到了数据。

波音公司表示此次事件并未影响其飞行安全，并称已经与执法和监管机构合作展开调查。目前，波音的服务网站已关闭，并在页面上展示消息称页面关停是由“技术问题”引起的。

虽然波音公司方面尚未证实LockBit的说法，但该团伙在暗网搭建的数据泄露页面已删除了波音的相关数据。而LockBit团伙则在删除数据前表示：“如果波音公司不在最后期限内与团伙联系，便会泄露和发布大量敏感数据。”……“目前为了保护该公司数据，我们不会公布详细列表或样例，但在截止日期之后，我们便不会再有所保留。”

# 七

# 多名勒索软件相关黑客在美国被起诉

2024年的一则公开消息显示，白俄罗斯-乌克兰国民Maksim Silnikau在西班牙被捕，现已被引渡到美国并面临在2021年创建Ransom Cartel勒索软件以及2013年至2022年间运行恶意广告等指控。

攻击者在俄语论坛上以“JP Morgan”、“xxx”和“lansky”的别名进行活动，其他在这些论坛上进行了大范围的网络犯罪活动的推广。当局还公布了两份独立的起诉书：一份是针对新泽西州地区关于恶意广告投放的起诉书，另一份是针对弗吉尼亚州东区关于Ransom Cartel勒索攻击的起诉书。此外，其同谋：38岁的白俄罗斯-乌克兰公民Volodymyr Kadariya和33岁的俄罗斯公民Andrei Tarasov也因在恶意广告投放中的作用而被指控。

2013R01333/AMT/AAH/LKB/CG

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

| | | |
|---|---|---|
| UNITED STATES OF AMERICA | : | Hon. |
| | : | |
| v. | : | Crim. No. 23- |
| | : | |
| MAKSIM SILNIKAU, | : | Count 1 |
| a/k/a "Maksym Silnikov," | : | (Conspiracy to Commit Wire Fraud) |
| a/k/a "Maksim Silnikov," | : | 18 U.S.C. §§ 1349, 3559(g)(1) |
| a/k/a "Maxsim Andreyevich Silnikov," | : | |
| a/k/a "Maksym Mykolaiets," | : | Count 2 |
| ANDREI TARASOV, and | : | (Conspiracy to Commit Computer |
| VOLODYMYR KADARIYA, | : | Fraud and Abuse) |
| a/k/a "Volodymyr Kadaria," | : | 18 U.S.C. §§ 371, 3559(g)(1) |
| a/k/a "Vladimir Kadaria" | : | |
| | : | Counts 3-4 |
| | : | (Wire Fraud) |
| | : | 18 U.S.C. § 1343 |
| | : | 18 U.S.C. § 2 |
| | : | |
| | : | **FILED UNDER SEAL** |

**INDICTMENT**

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

**Count 1**
**(Conspiracy to Commit Wire Fraud)**

**Introduction**

1. From at least in or about October 2013 through in or about March 2022,

法院对Maksim Silnikau的起诉文件

"据称，这些共谋者实施了一项多年计划，将恶意软件分发到全球数百万毫无防备的互联网用户的计算机上，"新泽西州联邦检察官Philip R. Sellinger说"为了实施该计划，他们使用恶意广告来诱骗受害者点击看似合法的互联网广告。"

英国国家犯罪局在2024年8月13日宣布，Silnikau于2023年7月18日在一场由NCA协调组织的联合执法形同中于西班牙被捕。根据起诉书中的内容，Silnikau创建和管理了Ransom Cartel勒索软件，并从俄语论坛招募其他网络犯罪分子参与攻击。他还与“初始访问经纪人”（IAB）进行合作，这些经纪人提供对受感染企业网络的访问权限，管理与受害者的通信并处理赎金支付。此外，Silnikau还通过加密货币转移赎金以掩盖资金流向并使执法工作复杂化，显然在行动中发挥着核心作用。

NCA还指出，Silnikau也是臭名昭著的Reveton木马的幕后黑手，这是一种Windows恶意软件，可将用户锁定在操作系统之外——直到其被迫支付赎金。该恶意软件于2011年推出，伪装成执法部门，并称是由于检测到儿童色情和受版权保护的材料才将受害用户的计算机锁定。而要访问计算机，受害者需要通过MoneyPak、PaySafeCard或其他在线支付支付赎金。在2012年至2014年期间，Reveton还被出售给其他网络犯罪分子，这些网络犯罪分子通过受到漏洞利用工具包入侵的网站进行了大量传播。NCA报告称，Reveton的感染在2011年至2013年期间产生了400000美元的违法犯罪所得。该木马的成功还刺激了其他网络犯罪分子推出类似的恶意软件，例如Urausy和Harasom Ransomware系列，在许多情况下其行为功能与Reveton并无区别。可悲的是，该恶意软件非常成功——以至于有人因为担心会入狱而结束了自己和其儿子的生命。

同时，Silnikau还被起诉涉嫌于2013年10月至2022年3月期间策划及执行一项大型恶意广告投放计划。他的主要职责包括开发和分发恶意广告，这些广告看似合法，但将用户重定向到包含Internet Explorer漏洞利用工具包、恶意软件、恐吓软件和在线诈骗的网站。

根据这两项起诉书中的指控，Maksim Silnikau面临着非常严重的法律后果，包括因电汇欺诈、计算机欺诈、计算机欺诈和滥用、严重身份盗窃和访问设备欺诈而被判处监禁。如果所有指控均被定罪，Silnikau可能面临超过100年的监禁。不过由于刑期的叠加，最终宣判的刑期通常要短得多。

除了Maksim Silnikau外，另一名勒索软件相关黑客也在美国遭到起诉。

2024年12月，美国当局逮捕了一名与该Scattered Spider网络犯罪团伙有关的19岁少年，他现在被指控入侵一家美国金融机构和两家未具名的电信公司。这位名叫Remington

Goy Ogletree（其在网络中曾化名为“remi”）的少年使用针对其员工的短信和语音网络钓鱼消息中窃取的凭据入侵了这三家公司的网络。他还冒充受害者的IT支持部门打电话，旨在迫使员工访问网络钓鱼网站，要求他们输入用户名和密码。

据传，被Ogletree入侵的金融机构对FBI表示，其大约有149名员工成为了网络钓鱼攻击的目标，该钓鱼攻击将他们的网络访问重定向到了冒充公司网页的钓鱼登录页面。这些钓鱼网站旨在要求目标员工输入他们用于访问金融机构系统的凭据。

此外，在2023年10月至2024年5月期间，Ogletree还利用他对电信系统的访问权限向美国各地的电话号码发送了超过860万条网络钓鱼短信，旨在帮助窃取收件人的加密货币。

今年2月，FBI在搜查他在德克萨斯州沃思市的住所时还曾在他被缴获的iPhone中发现了Ogletree犯罪活动的大量证据：包括冒充科技公司的网络钓鱼文本截图、凭据收集网络钓鱼页面的截图以及拥有数万美元加密货币的加密钱包的截图。在随后收到FBI审问时，Ogletree还表示他认识“犯下各种罪行的人”和“Scattered Spider的主要成员”，并补充说该黑客组织以业务流程外包（BPO）公司为目标，因为“他们的安全性不如”他们工作的公司。

2024年11月，美国司法部逮捕并指控了另外五名与网络犯罪团伙有关的嫌疑人，他们据称使用针对数十个目标的短信网络钓鱼攻击窃取了数百万美元的加密货币。这五名嫌疑人面临电汇诈骗、策划电汇诈骗和严重身份盗窃的指控，每人至少面临20年监禁：英国警方还在2024年7月逮捕了一名17岁的嫌疑人，据信他是参与2023年米高梅度假村勒索软件攻击的Scattered Spider黑客集体的一员。与该黑客组织相关的其他备受瞩目的攻击包括Caesars、MailChimp、Twilio、DoorDash、Riot Games和Reddit上的攻击。

自2023年初以来，Scattered Spider还与多个俄罗斯勒索软件团伙合作，包括Qilin、BlackCat/AlphV和RansomHub。

# 八
# UnitedHealth称有一亿条数据在勒索事件中被盗

美国联合健康保险集团（UnitedHealth Group）已确认向勒索软件组织支付了赎金以保护其在2月底Optum遭到勒索软件攻击期间被盗的敏感数据。此次攻击导致了其服务中断，并影响了Change Healthcare的支付系统，最终导致美国各地医疗保健组织和药房所使用的一系列重要服务停摆，这其中主要包括支付、处方书写和保险索赔等系统。根据该集团的报告称，网络攻击已造成其约8.72亿美元的经济损失。

BlackCat/ALPHV勒索软件团伙声称对此次攻击负责，并称窃取到了6TB的敏感患者数据。在3月初，BlackCat表示已从联合健康保险手中获得了2200万美元的赎金。当时，该团伙的一个名为“Notchy”的下属机构声称，是他们具体实施了本次攻击并获取了联合健康保险的数据，但BlackCat却骗取了他们的赎金。而根据比特币区块链上的信息，研究人员确认赎金确实已进入了BlackCat相关人员钱包。

而到了4月中旬，勒索组织RansomHub则开始泄露他们声称在攻击期间窃取到的公司和患者数据，从而给联合健康保险带来了更大的压力。在Notchy对联合健康保险进行了新一轮的勒索后，被盗数据再次到达了RansomHub手中。

根据确认，RansomHub已将相关数据从其网站中删除，并同时将联合健康保险从其受害者名单中删除。而联合健康保险也在23日发表声明确认，已向新的勒索软件团伙付款，而此次付款并不是3月份据称向BlackCat支付的2200万美元。

近期针对UnitedHealth集团子公司Optum的网络攻击时间导致了Change Healthcare支付平台持续中断。而据消息人士透露称此次攻击可能与BlackCat勒索软件组织有关。

Change Healthcare在2月21日公开宣布因遭遇网络安全事件而导致其部分服务不可用，这也导致了美国医疗保健系统的大范围的计费中断。自系统受到攻击以来，Change Healthcare一直在进行相关调查。据参与调查的相关人员透露，此次攻击可能与BlackCat(ALPHV)勒索软件团伙有关，攻击者可能是通过ScreenConnect的身份验证绕过漏洞(CVE-2024-1709)成功入侵的服务器系统，并在服务器上部署了勒索软件。

目前为止，BlackCat组织尚未对Change Healthcare遭受的攻击表示负责。UnitedHealth集团也没有确认BlackCat是否对此次攻击负责。

# 九
# 施耐德电器确认黑客窃取数据后开发平台遭到破坏

据知情人士透露，法国能源业巨头施耐德电气遭到了Cactus勒索软件攻击，导致公司数据被盗。据悉勒索软件攻击开始于1月17日，而遭到攻击的是该公司的可持续发展业务部门。本次攻击扰乱了施耐德电气的部分资源顾问云平台，这些平台至今仍处于中断状态。

据报道，勒索软件团伙在网络攻击期间窃取了以TB计的公司数据，并以此威胁该公司。虽然尚不清楚被盗数据的类型，但可持续发展业务部门为企业组织提供咨询服务就可再生能源解决方案提供建议并帮助他们满足全球公司复杂的气候监管要求，所以被盗数据可能包含有关客户用电、工业控制和自动化系统以及环境和能源法规合规性的敏感信息。

目前尚不清楚施耐德电气是否会支付赎金，但该公司在声明中证实其可持续发展业务部门确实遭受了网络攻击，并且确认攻击者获取到了内部数据。不过该公司同时以呃表示此次攻击仅限于该部门，并未影响公司其他部门。

施耐德电气已确认，在攻击者声称从该公司的JIRA服务器窃取了40GB的数据后，开发人员平台遭到破坏。

10月底，一位名叫“Grep”的攻击者在X上嘲讽该公司，表示他们已经入侵了其系统。在与媒体的对话中，Grep表示他们使用暴露的凭据入侵了Schneider Electric的Jira服务器。获得访问权限后，他们声称使用MiniOrange REST API抓取了400k行用户数据。Grep表示，其中包括75000个唯一的电子邮件地址以及Schneider Electric员工和客户的全名。

在暗网网站的帖子中，攻击者开玩笑地要求125000美元的“Baguettes”来换取不泄露数据，并分享了有关被盗内容的更多详细信息。

Grep进一步告诉媒体他们最近成立了一个新的黑客组织International Contract Agency（ICA），以《杀手：代号47》游戏命名。攻击者表示，该组织以前没有勒索他们入侵的公司。然而，在得知“ICA”名称与“伊斯兰恐怖分子团体”有关后，攻击者表示他们再次更名为Hellcat勒索软件团伙，目前正在测试用于勒索攻击的加密器。


法国公司施耐德遭勒索攻击

十

# 俄罗斯逮捕多名勒索组织成员并判刑

俄罗斯与2024年10月表示已判处REvil勒索软件行动的四名成员超过4年监禁，罪名是分发恶意软件和非法流通支付方式。REvil勒索软件（又名Sodin和Sodinokibi）于2019年4月作为GandCrab勒索软件的直接继任者被推出。在不到一年的时间里，该团伙成为全球最高产的勒索软件团伙，曾提出当时最高的赎金金额，并在一年内赚取超过1亿美元的非法收入。

然而，在2021年7月，当Revil在Kaseya供应链攻击中袭击了全球1500多家企业时，该勒索软件团伙的处境也变得更糟——作为对这次攻击的回应，美国总统拜登要求俄罗斯总统普京对居住在俄罗斯的网络犯罪分子采取行动，否则美国将自行采取行动。或许是感受到来自国际的压力，REvil暂停行动了一段时间，然后在两个月后恢复运营。但是，随后美国执法部门便联通国际合作机构在泄露之前已经破坏了他们的服务器。

此后，应美国政府的要求，俄罗斯联邦安全局（FSB）于2022年1月在一项国际执法行动中逮捕了该勒索软件的成员（包括Kaseya攻击背后的分支机构）后，捣毁了REvil勒索软件团伙。FSB在此次行动中逮捕了14名勒索软件团伙成员、突袭了25个地址，同时没收了660万美元的非法收入。俄罗斯联邦安全局当时在一份新闻声明中表示：“搜查活动的基础是美国主管当局的呼吁，他们报告了犯罪社区的头目，以及他通过引入恶意软件、加密信息和勒索解密信息来参与侵占外国高科技公司的信息资源。”

据媒体报道，8名成员最终受到审判，其中Artem Zayets、Alexey Malozemov、Daniil Puzyrevsky和Ruslan Khansvyarov在2024年10月25日被判刑，另外四人被单独审理。据俄罗斯媒体《生意人报》报道，Zayets今天被判处4年6个月的有期徒刑，Malozemov则被判处5年有期徒刑，Khansvyarov被判处5年6个月有期徒刑，Puzyrevsky被判处6年有期徒刑。

其他四名成员现在将在单独的程序中接受非法访问计算机信息的审判。

除此之外，俄罗斯执法部门还在2024年11月底逮捕并起诉了臭名昭著的勒索攻击参与者Mikhail Pavlovich Matveev（又称Wazawaka、Uhodiransomwar、m1x或Boriselcin等），罪名是其开发恶意软件并参与多个黑客组织。


FBI对Wazawaka的悬赏信息

据俄罗斯国有新闻机构RIA Novosti所接到的匿名来源消息称：虽然检察官办公室尚未公布有关此人身份（在法庭文件中被描述为“程序员”）的任何细节，但此人正是Matveev。俄罗斯内务部在一份声明中说：“目前，调查人员已经收集到足够的证据，检察官签署起诉书的刑事案件已送交加里宁格勒市中央地区法院进行审议。”

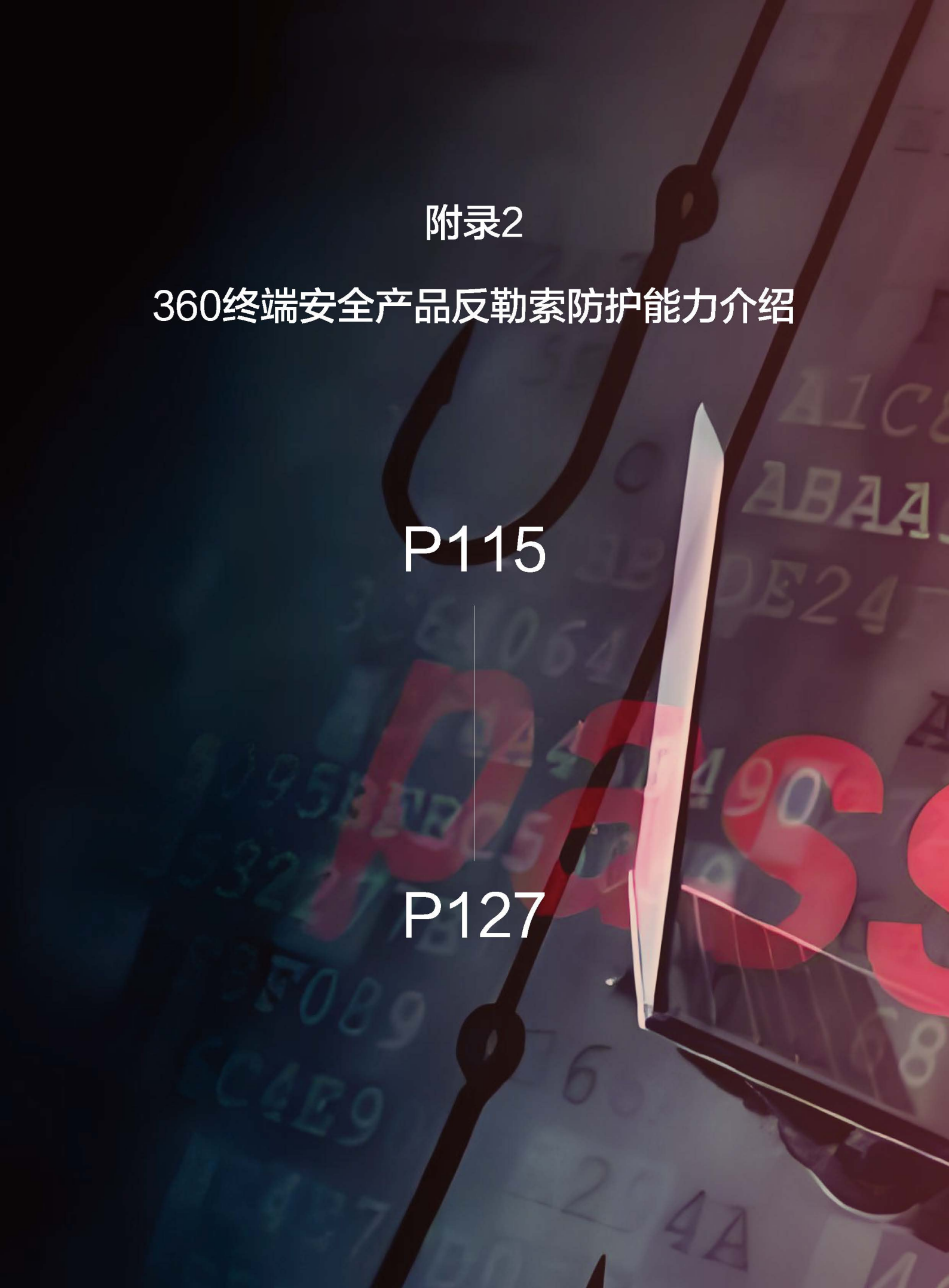
正如网络政策专家Oleg Shakirov首次发现的那样，Matveev被指控开发勒索软件（检察官办公室将其描述为可以加密文件和数据的“专用恶意软件”），并称其计划使用勒索软件来加密“商业组织的数据，以便然后从他们那里获得赎金进行解密”。

去年，即2023年5月，美国司法部还对Matveev提出指控，称其参与开发了针对美国受害者的Hive和LockBit勒索软件。此外，他还被认为是“Orange”黑客论坛的创建者和管理员，以及Babuk勒索软件的最初运营者。而后者在组织成员无法抉择是否发布从华盛顿特区首都警察部队窃取的数据后分道扬镳。

根据美国司法部的新闻稿和新泽西州及哥伦比亚特区的公开起诉书，可以整理出他在与三个勒索软件团伙合作时活动的大致时间表：

- 2020年6月，Matveev和LockBit勒索软件合谋在新泽西州帕赛克县的一个执法机构的网络上部署了LockBit勒索软件；
- 2021年4月，Matveev与Babuk勒索软件合谋在华盛顿特区大都会警察局的系统上部署了恶意载荷。
- 2022年5月，Matveev同Hive勒索软件团伙成员加密了总部位于新泽西州默瑟县的一家非营利性行为医疗保健组织的系统。
- Matveev还因对美国实体（包括美国执法部门和关键基础设施组织）发起网络攻击而受到财政部外国资产控制办公室（OFAC）的制裁。

Matveev在网上的知名度非常高。他经常与网络安全研究人员和专业人士进行交流，并使用他的Twitter帐户“RansomBoris”公开讨论他的网络犯罪活动。而在受到美国制裁后，Matveev还曾公开嘲讽美国执法部门，并在推特上发布了一张T恤上的通缉海报照片。



# 附录2

# 360终端安全产品反勒索防护能力介绍

P115

P127

# 360终端安全产品反勒索防护能力介绍

## 一

## 远控与勒索急救功能

360在2023年下半年，新推出了远控与勒索急救功能，用来解决用户在已经感染或怀疑感染远控木马或勒索病毒的场景下，帮助用户快速建立一个临时的安全场景，我们的防护功能将运行在一个严格监控的模式下，阻止一切可能的破坏行为，避免系统和数据进一步被攻击活动破坏。作为一个后置方案，它还将一些排查处置策略、溯源方法制作成了一键排查功能，协助管理员快速应对勒索攻击。


**远控 · 勒索急救功能界面**

360在2024年对该产品新增了渗透痕迹检测功能，覆盖了勒索攻击、挖矿植入、远控木马等流行威胁的攻击链检出。同时根据当下勒索软件与流行木马同安全防护软件的攻防对抗趋势，率先覆盖了全球主流安全厂商的防护致盲检测。支持九大类渗透痕迹检测，累计检出项目超过600项。

**远程控制权限**：将对一些远控的关键功能进行限制，如屏幕读取，键盘记录，键盘鼠标操作等，以及提供对一些重要敏感进程与文件的保护。

**访问权限**：将对系统中，常见的文档、数据库、音视频等数据文件提供保护，避免被篡改或删除。对进程的运行，联网也将进行严格的限制。

一键扫描功能，可以检出是否存在高风险的启动项、系统账户的弱口令、黑客工具、高危的远控软件并进行相应处理。


**远控·勒索急救扫描界面**

“被攻击查询”功能，可看到各类攻击信息，其中“系统日志”的“远程桌面登录”项完整记录了成功登录的ip与账户信息及时间信息。同时提供了勒索攻击常见的“数据库登录”、“SMB共享登录”、“痕迹清理记录”查询，方便进行攻击时段的溯源排查。


**远程桌面暴破记录查询界面**

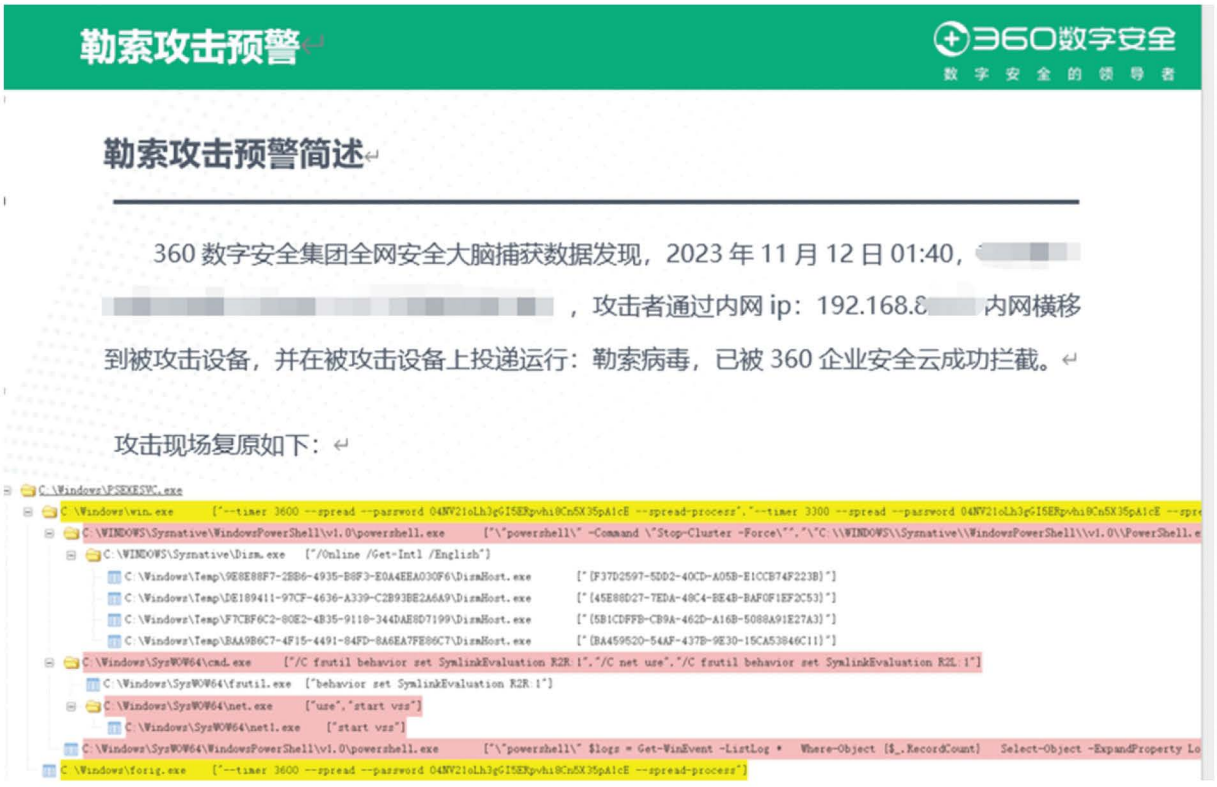
2024年新增的“渗透痕迹记录”可看查看系统中，出现过的攻击链痕迹，用于辅助判断是否存在黑客攻击。


**渗透行为记录界面**

# 二

# 勒索预警服务

2024年，通过我们的勒索预警订阅服务，基于360全网安全大数据视野，监测勒索攻击的多个环节，在勒索攻击的准备阶段，以及病毒初始投递阶段，对监管、企业用户提供勒索预警订阅服务。希望在勒索的前期阶段，进行阻断，避免造成受害单位的进一步损失。2024年共计捕获勒索攻击事件线索5863起，涉及受害单位2148家，确认勒索病毒家族59个，攻击IP来源地涉及境外54个国家或地区，配合监管输出勒索攻击事件线索658起，覆盖全国多个地区。




勒索攻击预警服务

# 三

# 弱口令防护能力

弱口令攻击一直是勒索软件最重要的传播手段，360安全卫士自2017年开始提供弱口令攻击防护，为亿万用户提供了安全保护。在与勒索软件对抗的过程中，产品也一直在提升安全能力，保证了可以应对最新攻击手法，为用户提供更好的体验。

下图是2024年防黑加固功能每月所防御的攻击量，2024年，360防黑加固共保护近270万台设备免遭入侵，拦截各类弱口令入侵共计超过43.1亿次。


数据来源：防黑加固统计数据

以下是360提供弱口令攻击防护的重要更新时间轴：

●2017年-2018年：新增对远程桌面弱口令防护支持。

●2018年-2019年：新增SQL Server暴破、VNC暴破、Tomcat暴破的防护支持。

●2019年：

◆新增RPC协议弱口令暴破防护

◆SMB协议暴破拦截优化版正式上线

◆新增对金万维、瑞友管理软件的支持。

◆对MYSQL、SQL Server、Tomcat等服务器常用软件也加入了多方位的拦截防护。

●2020年：

◆用户登录提醒：如果机器在未登录阶段受到攻击，在用户下次登录时，会提醒用户之前发生攻击的概况，提醒用户加强安全防护。

◆弱口令提示：对正在使用弱口令的账户主动做出提醒，建议用户及时修改口令。

◆登录IP黑名单：通过云端安全大数据，动态配置IP黑名单，保护用户电脑免受攻击。

◆账户黑名单：由于各种条件限制，有部分设备无法修改内置账户和口令，造成设备被攻击，360安全卫士提供了账户黑名单功能，记录了各类数据库和应用系统的内置账户密码和已经泄露的一些账户密码。限制这类账户密码组合使用的远程登录情况，保障用户设备免受攻击。

●2021年：

◆支持拦截时间段控制

◆来自风险地区的ip拦截

●2023年：

◆增加暴破日志查询

◆企业安全云增加远程接入策略，实现IP白名单功能

●2024年

◆企业安全云高级功能增强，支持更丰富防御定义

# 四
# 数据库保护能力

数据库文件是勒索软件攻击的头号目标，数据库被加密，也是企业面临的最严重勒索风险，一旦数据库被攻破，会直接对用户造成严重的数据泄露或损坏。

360终端安全针对数据库面临的勒索风险问题，也推出了数据库加强保护功能，在常规的勒索保护之外，增加了针对数据库特有情况的专门保护。针对数据库常见的SQL注入，数据库爆破等攻击，360的数据库防护功能，对恶意SQL语句进行识别和拦截。同时还加强了对数据库服务的保护，避免勒索软件对数据库服务与文件本身的破坏。

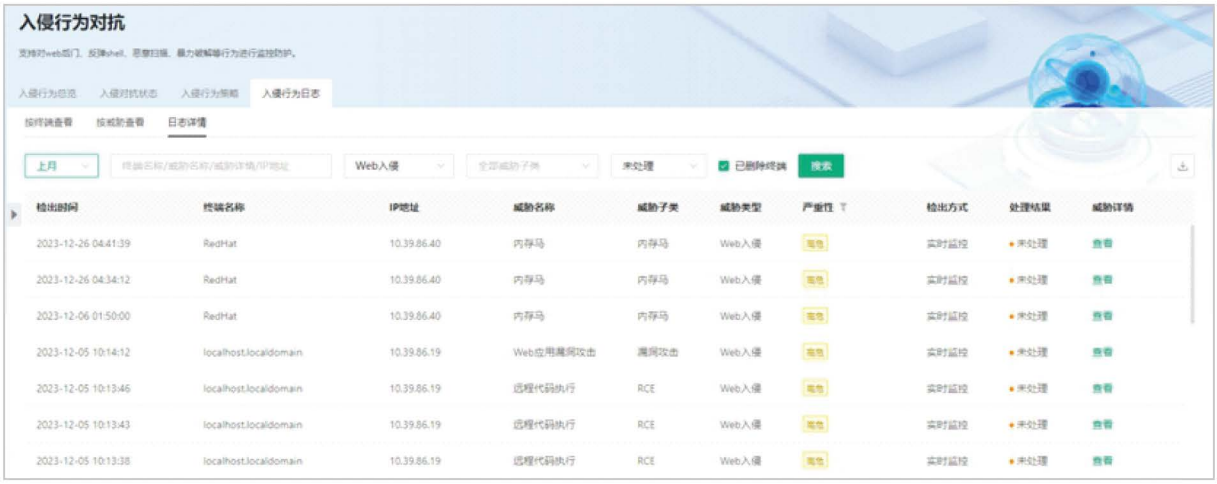

**数据库攻击防护弹窗**

# 五
# Web服务漏洞攻击防护

Web服务类漏洞攻击，是目前最常见的一类针对服务器的勒索攻击手段。部署在服务器中的各类Web应用，如OA系统、财务系统经常成为勒索团伙的攻击目标。

360 RASP可以实现对Web资产的梳理和实时防护。通过应用程序执行上下文，语义分析，ASM栈帧分析，并结合360在C端庞大的用户量和多年攻防实战经验制定的安全规则和算法。有效防护RCE漏洞，文件上传漏洞，反序列化漏洞，内存马攻击等，实现NDay漏洞的防护和0Day漏洞的告警，具备更深度的监控和威胁感知能力。RASP基本适配所有Java版本和主流的操作系统，所有防护插件使用独立的ClassLoader加载，灵活启停，支持热更新，对现有业务无影响，稳定性高，目前已在数十万服务器终端上稳定运行，目前已经支持超过280个Nday漏洞告警。

还有针对.Net漏洞的专项防御DNRSP，支持.Net Framework 4.0及其以上的主流.Net版本，具有广泛的适用性。DNRSP的原生SDK基于系统原始API设计，提供统一的防护和识别接口，对系统运行无额外负担，除此之外，考虑到.Net应用的场景已经使用问题，DNRSP支持热更新，在不影响业务运行情况下实现防护功能的动态更新与防护能力的增强。




Web服务漏洞攻击防护界面

# 六
# 横向渗透防护能力

横向渗透目前是针对企业内网攻击的关键技术手段之一，而针对横向渗透的防护能力则是360高级威胁防护体系中的一项重要能力。勒索软件攻击团伙，在对企业发起攻击后，往往利用该技术扩大影响范围，获取更多设备的控制权，乃至控制整个企业网络。

在我们处置的企业被攻击案例中，几乎都可以见到横向渗透攻击的身影。为此360安全卫士推出了体系化的横向渗透防护方案，从攻击源头、攻击方法、攻击资源、技术素材等多维度入手，全方位的阻断横向渗透攻击。下面列举了其中部分防护能力：

- 共享文件访问控制
- 远程WMI执行控制
- 远程计划任务控制
- 远程MMC控制
- 远程DCOM控制/远程RPC调用防护
- 远程服务创建控制
- 远程注册表操作控制
- 远程WINRM监控
- 远程PSEXEC防护
- 共享文件写入监控
- 域环境下的组策略拦截

这些防护能力，结合对无文件攻击防护和LOLBAS（Living Off The Land Binaries and Scripts）防护能力，有效阻断了攻击者在企业内网的刺探和攻击扩散。


360安全卫士防护横向渗透防护模块

# 七

# 提权攻击防护

勒索软件执行过程中，为了提升其权限，尽可能多的加密系统中的文件，会尝试利用各种方法去提升程序的运行权限，针对这一攻击方式，360安全卫士对其进行了严格的行为侧。


360安全卫士提权攻击防护功能

# 八

# 挂马网站防护能力

针对包括勒索软件在内的各类木马病毒攻击，更早的防护往往能取得更好的效果。360安全卫士致力于在病毒木马攻击的早期就将其遏制，遏制传播渠道便是早期防御的一个重要部分。挂马网站是传播勒索软件的重要渠道之一，针对这一情况360安全大脑能第一时间监控并识别该网站的恶意行为并做出拦截。


360安全卫士拦截挂马站点

# 九
# 钓鱼邮件附件防护

针对从邮箱中下载回来的附件，360安全大脑精准识别邮件附件中潜藏的病毒木马，替用户快速检测附件中是否存在问题。


360安全卫士拦截钓鱼邮件附件

# 附录3

# 360解密大师

P128

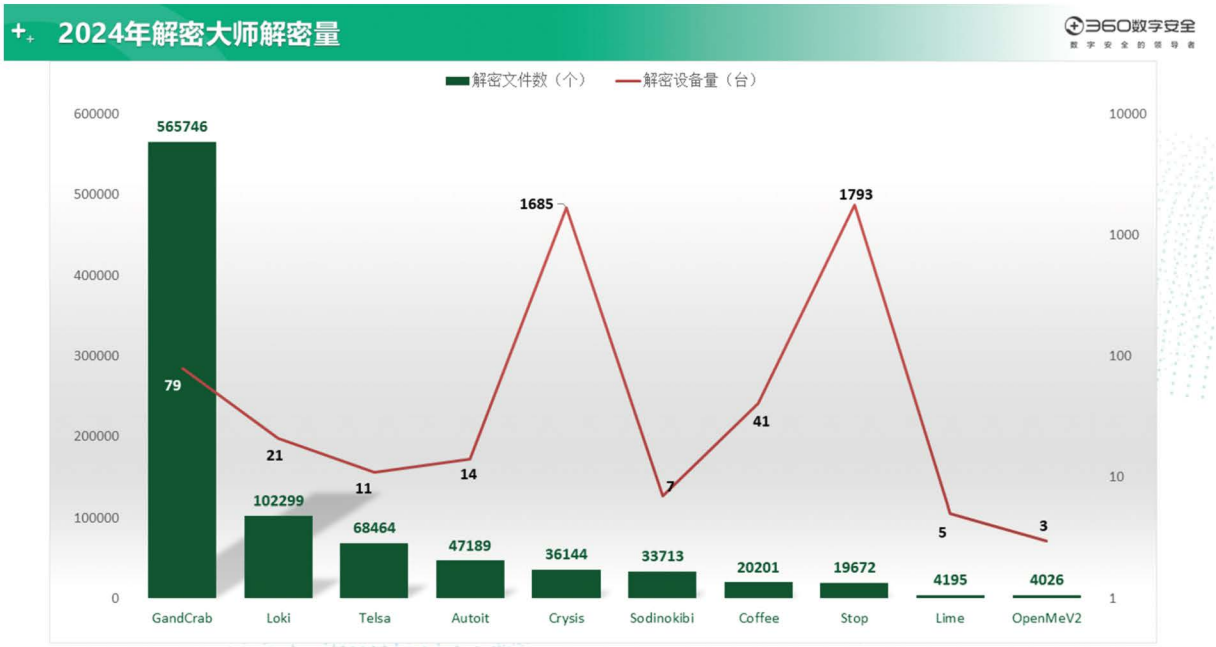
P129

# 360解密大师

360解密大师是360终端安全产品提供的勒索软件综合解密工具，是目前全球范围内支持解密类型最多的一款解密工具。

2024年360解密大师依然继续对最新出现的勒索软件保持着持续响应，解密大师功能累计支持解密勒索软件共计超过360种。2024年全年服务用户超3996台次。

下图给出了360解密大师在2024年全年，成功解密被勒索软件感染的文件和机器数量的Top10。其中，解密量较大的有Stop和Crysis，都属于历史遗存的勒索家族。




数据来源：解密大师统计数据

附录4

# 360勒索软件搜索引擎

P130

P133

# 360勒索软件搜索引擎

该数据来源lesuobingdu.360.cn的使用统计。（由于WannaCry、AllCry、TeslaCrypt、Satan、GandCrab、WannaRen、Sodinokibi等几个家族在过去曾出现过大规模爆发，之前的搜索量较高，长期停留在推荐栏里，对结果有一定影响，故在统计中去除了这几个家族的数据。）


360勒索软件搜索页面

通过对2024年全年勒索软件搜索引擎热词进行分析发现，搜索量排前十的关键词情况如下：

- rmallox、hmallox、mallox

  属于TargetCompany(Mallox)勒索软件家族，由于被加密文件后缀会被修改为mallox而成为关键词。该家族的传播渠道通常有：暴力破解远程桌面成功后手动投毒，暴力破解获取到数据库口令后远程投毒，若在内网环境中，还会尝试横向移动。2024年4月起新增软件漏洞利用方式进行传播。

●locked

locked后缀经常被不同勒索软件家族作为加密文件新增的扩展名，在国内最为流行的是TellYouThePass勒索软件家族。主要通过各种软件漏洞、系统漏洞等进行传播。

●mkp、svh、wis

属于Makop勒索软件家族，由于被加密文件后缀会被修改为mkp而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。同时存在加密共享目录的行为。

●faust

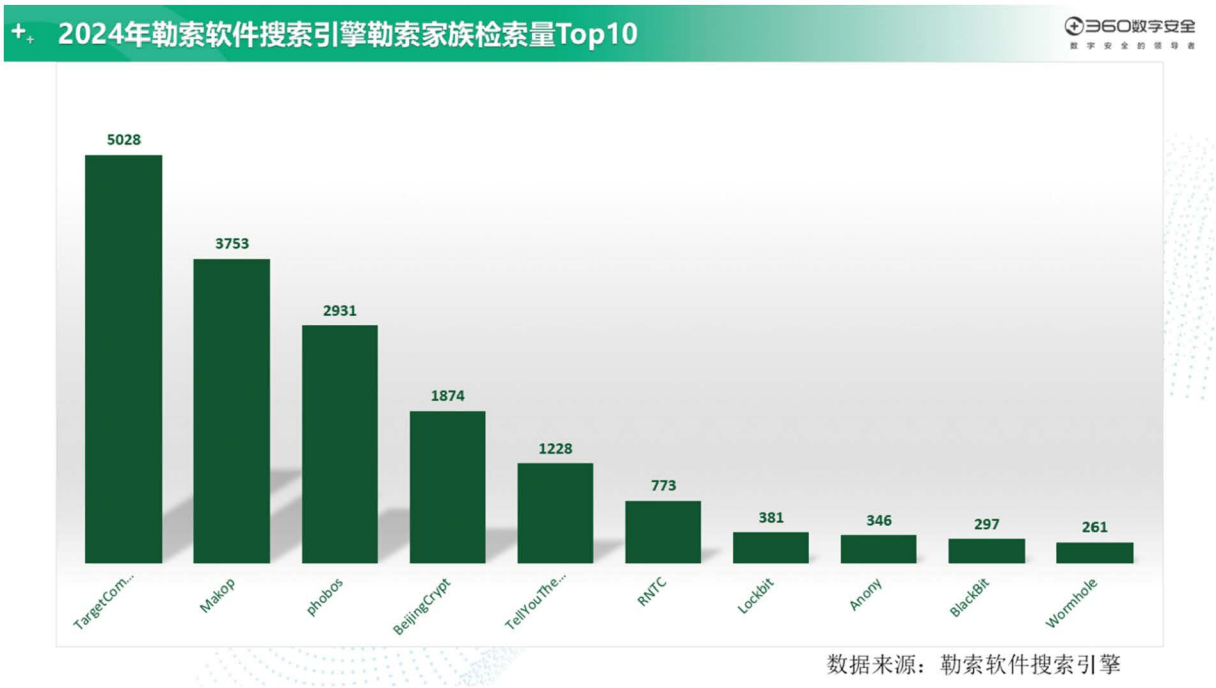
属于phobos勒索软件家族，由于被加密文件后缀会被修改为devos而成为关键词。该家族主要的传播方式为：早期在国外出现过利用激活工具破解软件进行传播，但在国内几乎都是通过暴力破解远程桌面口令成功后手动投毒。

●wstop

属于RNTC勒索软件家族，由于被加密文件后缀会被修改为rntc而成为关键词。该家族主要的传播方式为：通过暴力破解远程桌面口令成功后手动投毒。同时存在加密共享目录的行为。


数据来源：勒索软件搜索引擎

360勒索软件搜索引擎在2024年为用户提供了近6万次查询服务，对这近6万次关键词的搜索结果进行详尽分析后发现，与第一章勒索软件攻击形式的勒索家族分布相比，整体占比基本一致。然而，显著的差异在于Wormhole与BlackBit进入了TOP10的搜索结果中。Wormhole是利用瑞友天翼漏洞发起攻击的典型家族，自4月起发动了大范围传播。BlackBit是基于Loki家族的一个修改版本，主要通过远程桌面登录投毒。




数据来源：勒索软件搜索引擎

# RANSOMWARE THREAT REARCH REPORT 2024

# 2024年勒索软件流行态势报告


360数字安全 360安全大模型

360安全能力中心反病毒部

2025年1月