

2024 勒索软件攻击态势报告

- 新华三主动安全系列报告 -



目录

CONTENTS

1 概述	3
2 勒索攻击态势	4
2.1 全年勒索攻击频次分析	4
2.2 受害行业分析	5
2.3 受害地域分析	6
3 勒索组织分析	7
3.1 年度勒索组织盘点	7
3.2 入侵手段分析	8
3.3 索要赎金分析	10
4 勒索攻击发展趋势	12
4.1 AI 技术加持，勒索攻击态势加剧	12
4.2 目标行业重心转移，制造业跃居第一	12
4.3 勒索组织格局演变，由一家独大向多元化发展	13
4.4 攻击策略转变，中小企业面临更大风险	14

5 新华三勒索防御方案	16
附录一：年度勒索攻击大事件	18
附录二：新兴活跃勒索组织一览	20
Ransomhub	20
Fog	21
ElDorado(BlackLock)	22
Cicada3301	23
InterLock	24
附录三：安全建议和处置清单	26
安全建议	26
勒索软件应急处置清单	27
新华三聆风实验室	29

1 概述

在瞬息万变的数字化浪潮中，网络空间的勒索软件攻击日益显现出其严峻性和复杂性，成为全球网络安全领域备受瞩目的课题。作为一种极具破坏力的威胁，勒索软件通过其不断演变的技术手法，对各行各业持续发起新的挑战。新华三聆风实验室通过对全球范围内勒索攻击活动的长期持续观察与深入分析，以勒索软件攻击的总体态势为切入点，深入剖析其技术特点及演进趋势，总结 2024 年勒索攻击的主要特点如下：

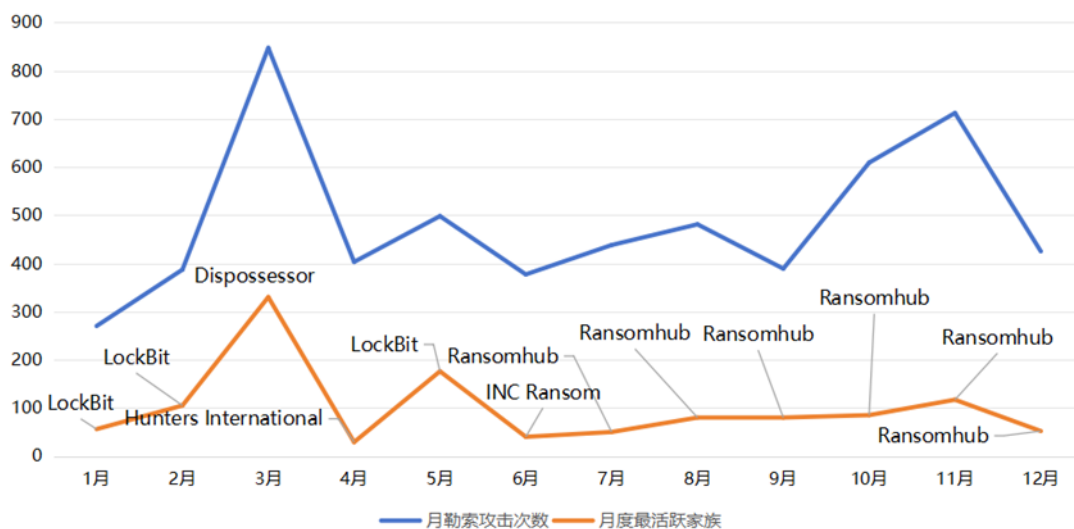
- 1、2024 年全球勒索攻击活动呈上升趋势，较 2023 年上升 47%；
- 2、从攻击数量来看，各月攻击数量存在一定的波动，但全年总体呈上升趋势，值得注意的是 Ransomhub 勒索攻击活动几乎霸榜整个下半年；
- 3、从受害行业来看，2024 年 TOP5 受害行业为制造、专业和法律服务、房产建筑、批发零售、信息技术等行业，共占比 58.37%；
- 4、从受害地域来看，北美、欧洲、亚洲位列前三，其中美国以 53%居于全球首位；
- 5、从活跃组织来看，2024 年共监测 96 个活跃勒索组织，其中有 46 个为新兴组织。活跃 TOP3 组织分别是 Ransomhub、Lockbit、和 PLAY，其中，Ransomhub 为今年新兴组织，其在 2024 年 2 月出现后迅速崛起，成为最活跃的勒索组织之一；
- 6、从入侵手段来看，漏洞利用、钓鱼邮件、弱口令仍是主要入侵手段，共占比 65%。2024 年有 85 个漏洞被勒索组织频繁利用，类型多为远程代码执行和提权漏洞，其中，零日漏洞(0day)造成的影响最为严重；
- 7、从赎金来看，勒索组织由于目标的营收规模不同和行业差异，索要赎金也存在差异。但最高支付赎金记录屡创新高，今年 2 月，DarkAngels 向美国知名药品公司 Cencora 发起勒索攻击，成功索要到赎金 7500 万美元，创造了历年来最高支付赎金记录；

2 勒索攻击态势

2024 年的勒索攻击态势呈现出诸多新变化。一方面，全年攻击数量较 2023 年显著攀升，呈现出明显的上升趋势；另一方面，勒索攻击在频次波动、受害行业偏好以及受害地域分布等方面，均展现出新的动向与规律。本章将从全年勒索攻击频次、受害行业、受害地域三个关键维度详细剖析勒索攻击在 2024 年的具体态势。

2.1 全年勒索攻击频次分析

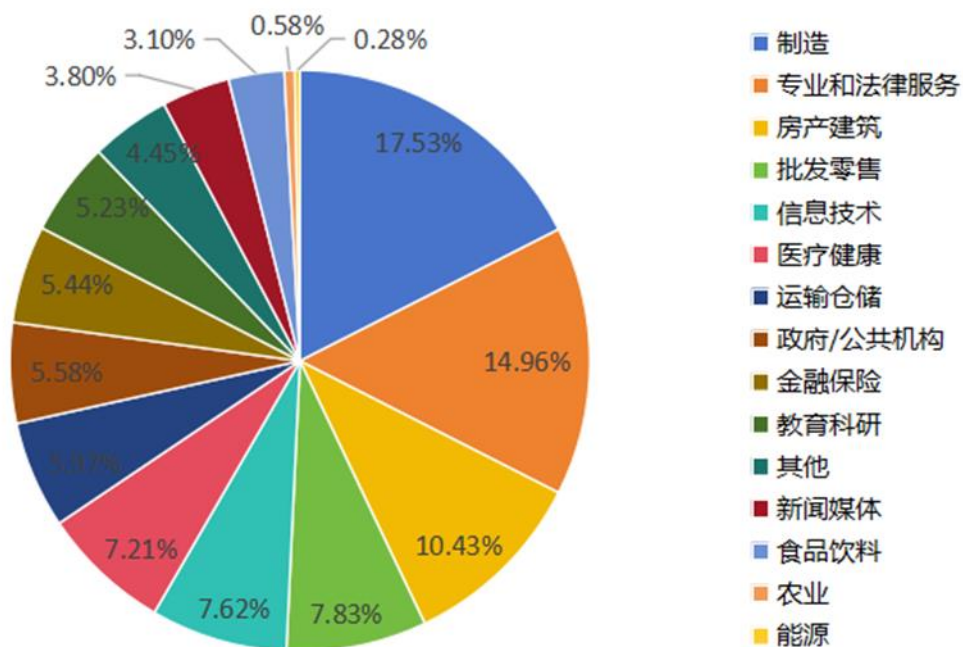
图 2-1 各月攻击数量及月度最活跃组织



根据图 2-1 统计，2024 年的 3 月和 11 月出现了两次勒索攻击事件的大规模爆发，除了这两个月份的集中增长外，全年勒索攻击事件总体上呈现出持续上升的趋势。在各个月份的攻击事件统计中，LockBit 在 5 月份之前三次荣登榜首，显示出其在年初的活跃程度。而从 5 月份开始，Ransomwarehub 则后来居上，六次登顶榜首，成为下半年勒索攻击的主要推手。

2.2 受害行业分析

图 2-2 2024 勒索攻击受害行业分布



根据最新的 2024 年勒索攻击受害行业分布统计图，勒索软件的目标行业带有明显的倾向性，由于制造业等实体行业对生产停机时间容忍度较低，导致以制造，批发，房产为主的实体行业仍是 2024 年的勒索重灾区。此外，数据价值和敏感度高的行业也是勒索攻击的重点倾向目标，如法律，信息技术，教育等行业。

2.3 受害地域分析

图 2-3 2024 勒索攻击全球地域分布

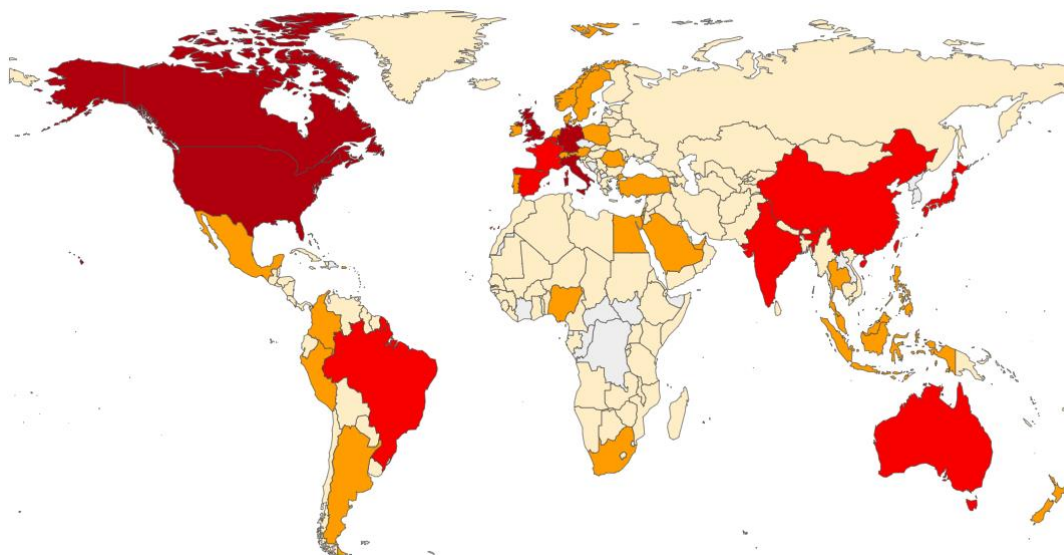


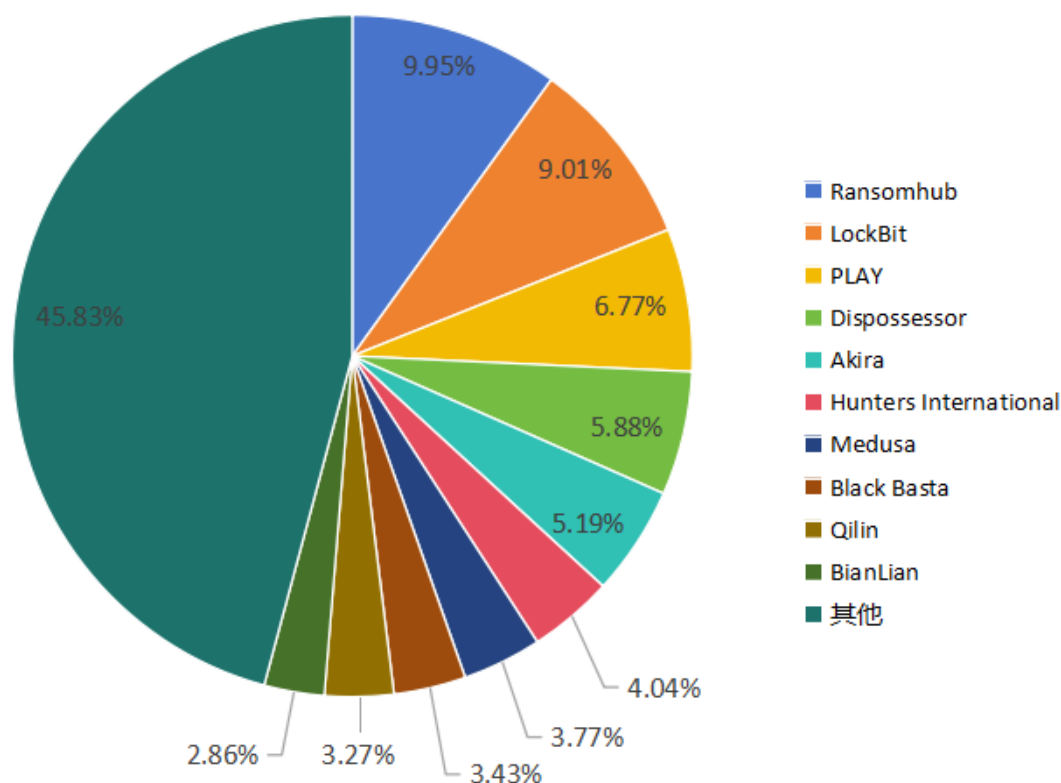
图 2-3 是 2024 年度全球勒索攻击地图，除俄罗斯外其余国家的排名变化不大，北美洲，欧洲，亚洲三个地区仍是受到攻击最严重的三个州。其中美国(53%)居于全球首位，加拿大(5.2%)排在第二。根据分布图和各地域发展情况可以看出，勒索组织更偏向经济发达，高度数字化和信息化的国家和地区，这与勒索组织追求利益最大化的目标一致。

3 勒索组织分析

勒索组织作为勒索攻击的幕后黑手，其发展动态和变化直接影响着勒索攻击的格局与走向。2024 年，勒索组织数量大幅增长，新兴组织不断涌现，与老牌组织彼此竞争，形成了复杂多变的勒索组织生态格局。从年度活跃组织的排名更替，到新兴组织的异军突起，再到入侵手段的持续演变，及索要赎金金额变化，本章将对这些勒索组织进行深入剖析。

3.1 年度勒索组织盘点

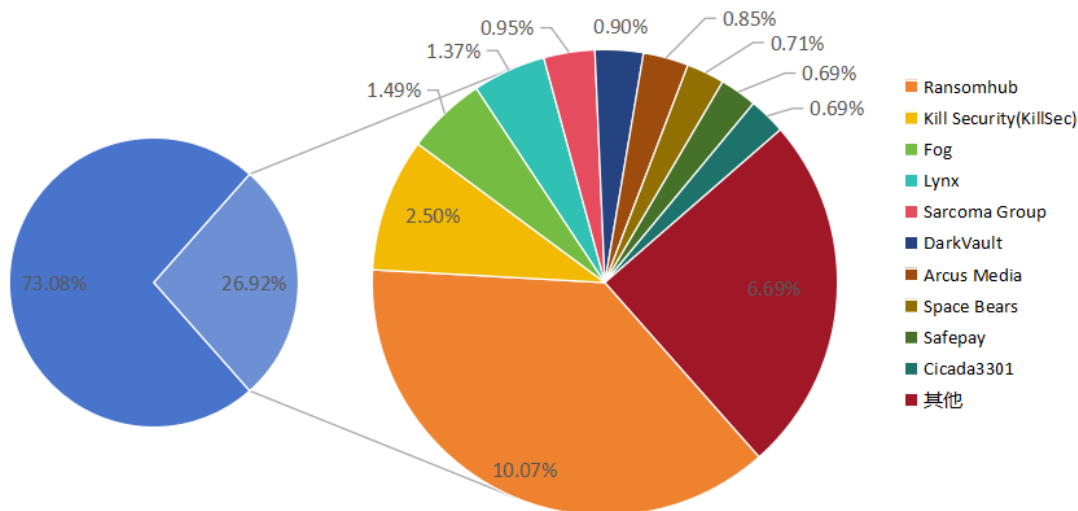
图 3-1 年度 TOP10 活跃勒索组织



据统计，2024 年共有 96 个勒索组织发起了不同程度的勒索攻击，与 2023 年的 62 个活跃组织数量相比有了大幅度的增长。2024 年头部组织 Ransomhub 相比 2023 年的 LockBit 勒索攻击事件数减少约 50%，但是总体事件数却比 2023 年增加了 47%，可见勒索组织数量的增加直接导致了勒索攻击事件数的上升。其中，2024 年

TOP3 活跃组织分别是 Ransomhub(18.3%)、LockBit(16.6%)和 PLAY(12.4%)。2024 年勒索组织更替明显, 新增 46 个新兴勒索组织, 这进一步展示了勒索软件生态系统的适应性和持续威胁。

图 3-2 新兴勒索组织 TOP10

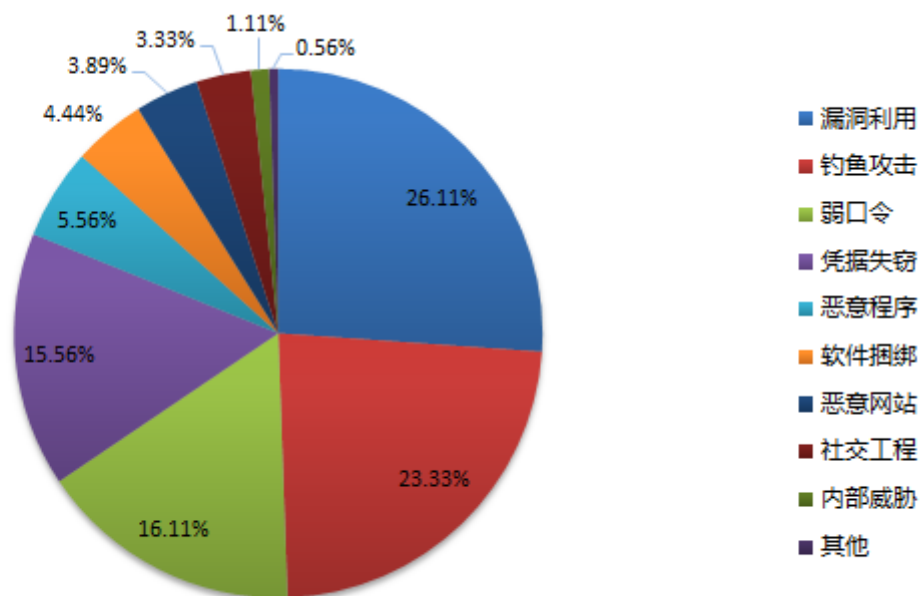


在所有组织中, 新兴勒索组织的活跃度占总体的 26.96%, 较去年 19.28% 有了明显增长。其中以 Ransomhub、Kill Security 和 Fog 为代表的新兴组织最为活跃, 24 年出现如此多的新兴勒索组织的一个重要原因是来自于执法部门的强力打压, 导致部分头部勒索组织重组为多个新的勒索组织。据相关报告表明, BASHE (APT73)、Safepay、Brain Cipher、SenSayQ、DarkVault 等勒索组织都与 LockBit 存在关联或相似性。

3.2 入侵手段分析

为了深入了解当前网络安全环境中的主要威胁向量, 我们对 2024 年活跃勒索组织常用入侵手段进行了统计, 结果如图 3-3 所示。与 2023 年相比, 漏洞利用、钓鱼攻击和弱口令依然是勒索组织的主要入侵方式, 分别占比 26.11%、23.33% 和 16.11%。这反映出企业在漏洞管理和安全教育等方面仍有待加强。

图 3-3 入侵手段统计



勒索组织频繁利用漏洞进行入侵，主要有以下几个原因。首先，随着各类软件和系统的快速迭代更新，新漏洞层出不穷，同时企业也不能及时修复旧漏洞，这为勒索组织提供了可乘之机。其次，成功利用漏洞可以帮助勒索组织快速绕过安全防护措施，直接获取系统或网络的访问权限，从而节省大量时间和资源。表 3-1 整理了 2024 年勒索组织常用的漏洞。

表 3-1 勒索组织常用漏洞统计

安全措施绕过	未授权访问	路径遍历	远程代码执行	命令注入	权限提升	SQL注入	文件上传	信息泄露	其他
CVE-2019-1338	CVE-2023-22069	CVE-2018-13379	CVE-2017-0144	CVE-2021-27102	CVE-2020-0787	CVE-2021-20028	CVE-2024-50623	CVE-2019-6693	CVE-2021-27103
CVE-2020-12812	CVE-2023-22515	CVE-2023-41266	CVE-2019-0708	CVE-2021-27104	CVE-2020-1472	CVE-2021-24465		CVE-2020-3259	CVE-2021-37606
CVE-2021-31207	CVE-2023-34362	CVE-2023-47246	CVE-2019-1068	CVE-2023-0669	CVE-2021-1732	CVE-2021-27101		CVE-2023-4966	CVE-2023-20263
CVE-2023-20269		CVE-2024-11667	CVE-2019-5544	CVE-2024-21887	CVE-2021-34523	CVE-2023-48788			CVE-2023-41265
CVE-2023-38035		CVE-2024-1708	CVE-2020-0618	CVE-2024-4577	CVE-2021-36942	CVE-2024-6670			CVE-2023-48365
CVE-2024-1709		CVE-2024-23334	CVE-2020-3992	CVE-2024-55956	CVE-2022-21999	CVE-2024-6671			CVE-2024-40711
CVE-2024-37085		CVE-2024-23897	CVE-2021-21972		CVE-2022-41040				CVE-2024-40766
CVE-2024-51378			CVE-2021-22986		CVE-2022-41080				
			CVE-2021-26855		CVE-2023-27532				
			CVE-2021-26857		CVE-2023-28252				
			CVE-2021-26858		CVE-2023-29357				
			CVE-2021-27065		CVE-2024-26169				
			CVE-2021-34473						
			CVE-2021-34527						
			CVE-2021-35211						
			CVE-2021-40444						
			CVE-2021-44228						
			CVE-2022-2294						
			CVE-2022-2295						
			CVE-2022-26500						
			CVE-2022-26501						
			CVE-2022-26504						
			CVE-2022-40684						
			CVE-2022-41082						
			CVE-2023-26360						
			CVE-2023-27350						
			CVE-2023-27997						
			CVE-2023-3519						
			CVE-2023-36884						
			CVE-2023-46604						
			CVE-2023-46747						
			CVE-2023-46805						



根据表 3-1 所示，勒索组织往往会使用一些超危、高危的漏洞发起攻击，这些漏洞往往存在于广泛使用的软件和系统中，影响范围较大。而且这些漏洞通常不具备复杂的利用条件，使得攻击者能够轻松加以利用，一旦成功，攻击者即可执行诸如远程代码执行和权限提升等关键操作，从而完全控制目标系统。

此外，勒索组织还会利用零日漏洞进行攻击，极大提高了攻击成功率，造成严重影响。例如，2024 年 12 月，Cleo 披露了其产品中的两个零日漏洞：CVE-2024-50623 和 CVE-2024-55956。Cleo 在全球拥有近 4000 家客户，ClOp 勒索组织利用这两个零日漏洞持续进行大规模数据泄露和勒索活动。近期，该组织在其网站上列出了 60 名受该漏洞影响的受害者，并要求他们在 48 小时内支付赎金。

3.3 索要赎金分析

2024 年，勒索组织索要的赎金也呈现出多样化与极端化的态势。索要赎金的范围极为广泛，从相对较低的数万美元到令人咋舌的数千万美元不等，随着目标的营收规模不同而变化。进一步来看，不同行业的企业所面临的赎金要求也大相径庭。数据敏感度高、业务连续性要求强的行业，如金融、医疗、信息技术等，往往被索要更高的赎金，因为勒索组织深知这些行业无法承受长时间的业务中断和数据泄露风险；而一些传统制造业或小型本地企业，虽然也会遭受攻击，但赎金要求相对较低。尤为引人关注的是，2024 年有记录的最高赎金支付金额飙升至 7500 万美元，这一惊人的记录由 Dark Angels 创造。他们向美国知名药品公司 Cencora 发起攻击，并成功索要到了这笔巨额赎金，这不仅刷新了历年来的赎金支付最高记录，也凸显了勒索攻击在经济利益驱动下的极端贪婪与破坏力，为全球企业和网络安全防护敲响了沉重的警钟。此外，加密货币（如比特币、门罗币等）因具有匿名性和难以追踪的特性，仍然是勒索软件攻击者要求的主要赎金支付方式。表 3-6 列举了 2024 年度被索要赎金 TOP10 的受害者及发起攻击的勒索组织和赎金金额。

表 3-2 2024 索要赎金 TOP10

勒索组织	受害者	所属行业	索要赎金
Dark Angels	Cencora	医疗健康	7500万美元
RansomHub	Mellitah	能源	5000万美元
Qilin	Synnovis	医疗健康	5000万美元
LockBit	London Drugs	批发零售	2500万美元
BlackSuit	CDK Global	制造业	2500万美元
Brain Cipher	RIBridges	政府/公共机构	2300万美元
BlackCat	Change Healthcare	医疗健康	2200万美元
LockBit	Majorca city Calvià	政府/公共机构	1100万美元
Trigona	Claro	信息技术	1000万美元
Hunters International	Hoya Optics	制造业	1000万美元

4 勒索攻击发展趋势

2024 年，勒索攻击呈现出诸多新趋势。AI 技术的加持使得勒索攻击的门槛与成本大幅降低，攻击速度与效率显著提升，给企业和组织带来了前所未有的挑战；目标行业的重心发生转移，制造业受到更多“青睐”；勒索组织格局也由过去的一家独大向多元化演变，新兴组织不断瓜分市场份额；攻击策略同样出现新变化，中小企业因安全防护薄弱而面临更大的风险。

4.1 AI 技术加持，勒索攻击态势加剧

自 2022 年底以 ChatGPT 为代表的生成式 AI 大模型产品问世以来，AI 技术快速发展，不断有各种 AI 大模型产品相继发布，攻击者接触和使用 AI 也更加方便。AI 技术在勒索攻击领域也产生了深远影响，不仅显著降低了勒索攻击的门槛和成本，还提高了攻击的速度和效率，致使勒索攻击更加频繁和复杂。企业和组织亟需高度重视这一趋势，积极采取有效的防御措施，以应对日益严峻的网络安全威胁。

（一）降低勒索攻击门槛和成本：

AI 技术的普及极大降低了勒索攻击的门槛和成本，使得即便没有任何 IT 基础的攻击者也能借助 AI 轻松制造出勒索病毒。2024 年 5 月，日本一名 25 岁的无业男子便利用生成式 AI 制作出了勒索软件病毒程序。此外，以 WormGPT 和 FraudGPT 为代表的恶意 AI 大模型受到攻击者的广泛青睐。这些模型操作简单、功能强大，能够用于创建、测试和优化各种恶意代码，涵盖恶意软件和勒索软件等诸多领域。

（二）提高勒索攻击速度和效率：

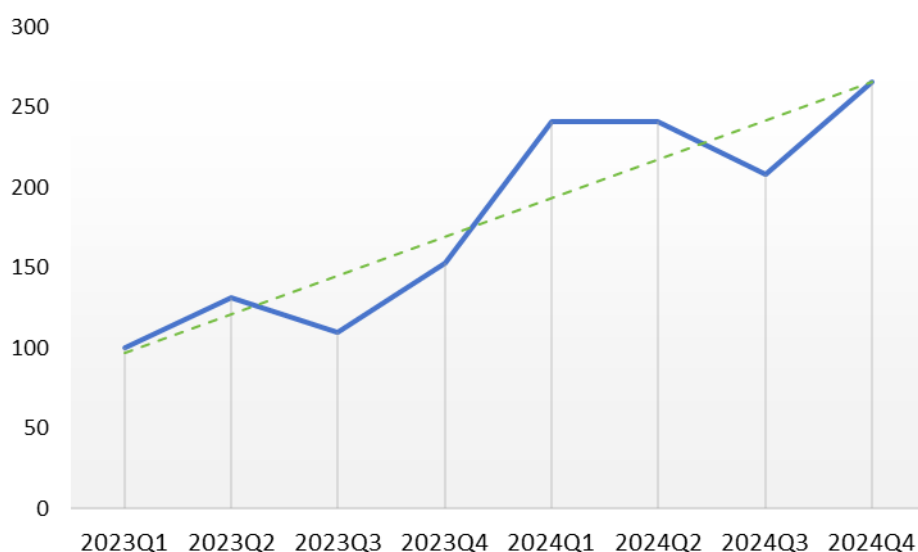
AI 技术还显著加快了勒索攻击的速度和效率。它能够迅速生成看似合理且难以甄别的欺诈性文本、电子邮件和网站。这些生成的内容常被用于制作钓鱼邮件和虚假网站，诱骗受害者点击链接或下载附件，从而实现勒索软件的传播。此外，AI 还可辅助攻击者高效寻找和挖掘目标系统中的漏洞。据 OpenAI 报告，伊朗黑客组织 Cyber Av3ngers 利用 ChatGPT 策划一系列针对可编程逻辑控制器（PLC）的网络攻击，他们借助 AI 来寻找目标系统可能存在的默认口令组合和漏洞，并改进用于探测网络漏洞的脚本。攻击者还可以利用 AI 技术快速生成和优化勒索程序，使其更具隐蔽性和破坏力。例如，2024 年 12 月开始活跃的勒索组织 FunkSec 就使用了 AI 来开发勒索软件和各种脚本程序，让其攻击手段更加难以防范。

4.2 目标行业重心转移，制造业跃居第一

在 2024 年，全球网络安全形势愈发严峻，勒索攻击事件频发，给各行业带来了巨大的挑战。与 2023 年相比，2024 年各行业遭到的勒索攻击次数总体呈上升趋势，其中制造业的受害情况尤为突出，攻击次数近乎翻倍，跃

居各行业之首。制造业作为全球供应链的核心环节，对生产停机的容忍度极低，一旦遭受攻击，不仅会导致生产中断，还会引发供应链的连锁反应，造成巨大的经济损失。此外，制造业面临的网络安全威胁也更为复杂，易受攻击的工业控制系统（ICS）、软件供应链安全威胁、物联网设备漏洞以及智能制造技术的复杂性，都进一步增加了其遭受攻击的风险，使其成为了勒索攻击的重点目标。从数据泄露到运营中断，勒索攻击已对全球制造业厂商造成了严重的财务损失和声誉影响。例如，2024 年 1 月，Cactus 勒索组织声称成功入侵全球能源与自动化行业的领导者施耐德电气，窃取了约 1.5TB 的数据。此次攻击主要影响了其可持续发展业务部门，导致资源顾问云平台的服务中断。虽然施耐德电气确认了数据泄露，但声明其他业务部门未受影响。为证明其攻击成果，Cactus 在其 Tor 泄密网站上发布了 25MB 的被盗数据样本，其中包括护照图像和公司文件。10 月，日本著名电子巨头卡西欧遭遇了 Underground 组织的勒索攻击，此次攻击导致卡西欧多个系统瘫痪，发表了暂停接收个人产品的维修服务的声明。同时 Underground 声称窃取了 204.9 GB 的数据，包括卡西欧员工的个人信息、合作伙伴的相关信息等。这些事件凸显了制造业和相关行业在网络安全方面面临的巨大挑战，也提醒了全球企业必须加强自身的网络安全防护能力，以应对日益复杂和频繁的网络攻击。

图 4-1 制造业受害者数量季度统计

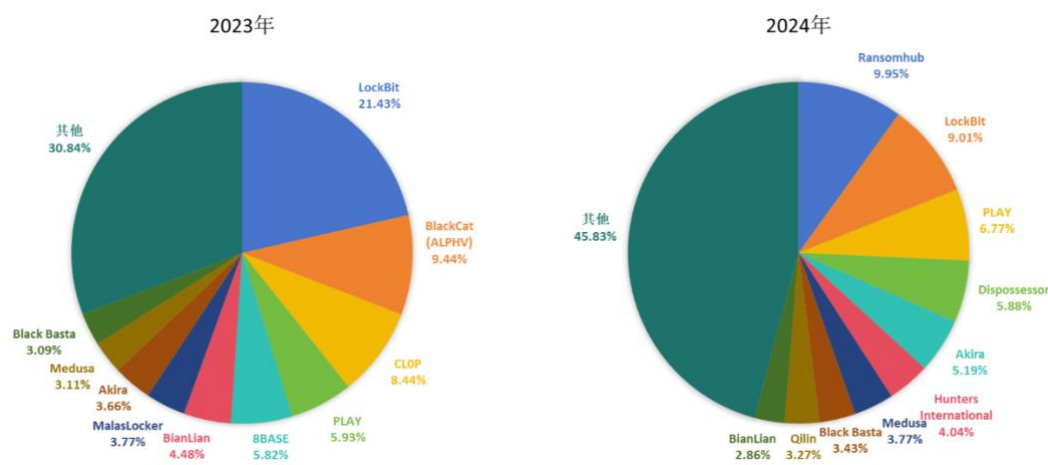


4.3 勒索组织格局演变，由一家独大向多元化发展

2024 年，勒索组织的生态格局正经历一场深刻的变革。过去，少数主要勒索组织凭借强大的技术实力和严密的组织架构，在勒索攻击领域占据主导地位，肆意攻击全球企业和机构，攫取巨额赎金。然而，国际执法部门的严厉打击以及自身内部矛盾的激化，使这些昔日“巨头”走向衰败甚至垮台。但应当警惕的是，这并未带来长久安宁，反而为新兴勒索组织的崛起创造了肥沃土壤。

新兴勒索组织如雨后春笋般涌现，采用更先进、复杂的技术手段和更具破坏性的攻击策略，迅速瓜分市场份额。2023 年，排名前十的勒索组织如 Lockbit、BlackCat、Cl0p 等发起的攻击事件占到了全年总事件的 69%，其中仅 Lockbit 一家就占 21%。而到了 2024 年，排名前十的勒索组织攻击事件占比下降至 54%，各组织之间的差距也变小，第一名 Ransomhub 仅占 10%。这其中主要的原因是 Lockbit、BlackCat 等勒索遭到了执法机构的严厉打击。2024 年 2 月，执法机构对 Lockbit 发起了代号“克罗诺斯行动”的执法活动，拆除了 LockBit 的基础设施，逮捕了其两名成员，并提供巨额赏金对其头目进行悬赏，导致其附属机构由 194 个锐减至 69 个。2024 年 3 月初，BlackCat 在收到美国医疗公司 Change Healthcare 的 2200 万美元赎金后关闭运营，此前在 2023 年 12 月，该组织遭到了美国执法机构的打击，被扣押了多个数据泄露和通信站点。在这些巨头倒下后，其附属机构或自立门户，或加入其他勒索组织。例如，BASHE (APT73)、Dispossessor、DarkVault 等新兴组织的泄露站点与 Lockbit 极其相似，BlackCat 的附属机构 Notchy 因 BlackCat 未能履行承诺，在 Change Healthcare 勒索事件中未获得其应得的赎金份额，携带窃取到的数据转投 RansomHub。据相关数据显示，2024 年新兴勒索组织数量相较于 2023 年近乎翻倍增长。这标志着勒索组织格局已从过去的一家独大，彻底转向多元化发展的新阶段。网络空间安全形势变得更加复杂严峻，给全球网络安全防护工作带来了前所未有的挑战。

图 4-2 2023 与 2024 勒索组织“市场份额”对比

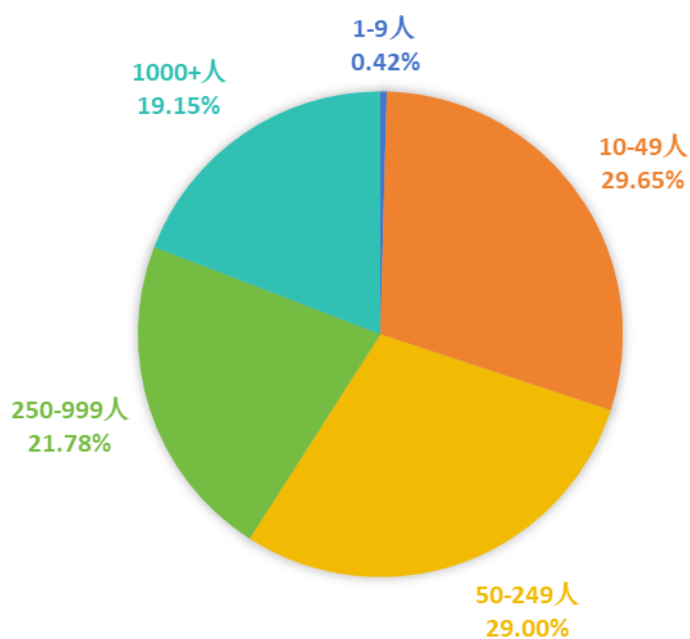


4.4 攻击策略转变，中小企业面临更大风险

在勒索攻击策略方面，2024 年出现了显著变化。虽然“大型狩猎 (Big game hunting)”依然受头部技术实力高超的攻击者青睐，仅针对少数高价值公司发起攻击，就能获取巨额赎金。例如，据 Zscaler ThreatLabz 的报告，Dark Angels 勒索组织 2024 年初攻击了美国药品分销巨头 Cencora，并获取到了 7500 万美元的巨额赎金，打破历史最高赎金支付记录。但随着勒索攻击门槛和成本的双双降低，大多数攻击者并没有很强的技术实力，他们更倾向于将目标锁定在中小企业。这一趋势在安全公司 Cyberdefense 发布的 Cy-Xplorer 2024 报告中得到了印证，数据显示，员工少于 1000 人的中小型企业遭受勒索攻击的可能性是大型企业的 4.2 倍。究其核心原

因，随着企业安全体系的不断完善，大型企业的攻击难度大幅增加，使得勒索组织不得不将注意力转向那些相对容易得手的目标。中小企业由于安全建设投入有限，安全防护措施不够完善，攻击难度较低，因此成为了勒索攻击的主要受害者。

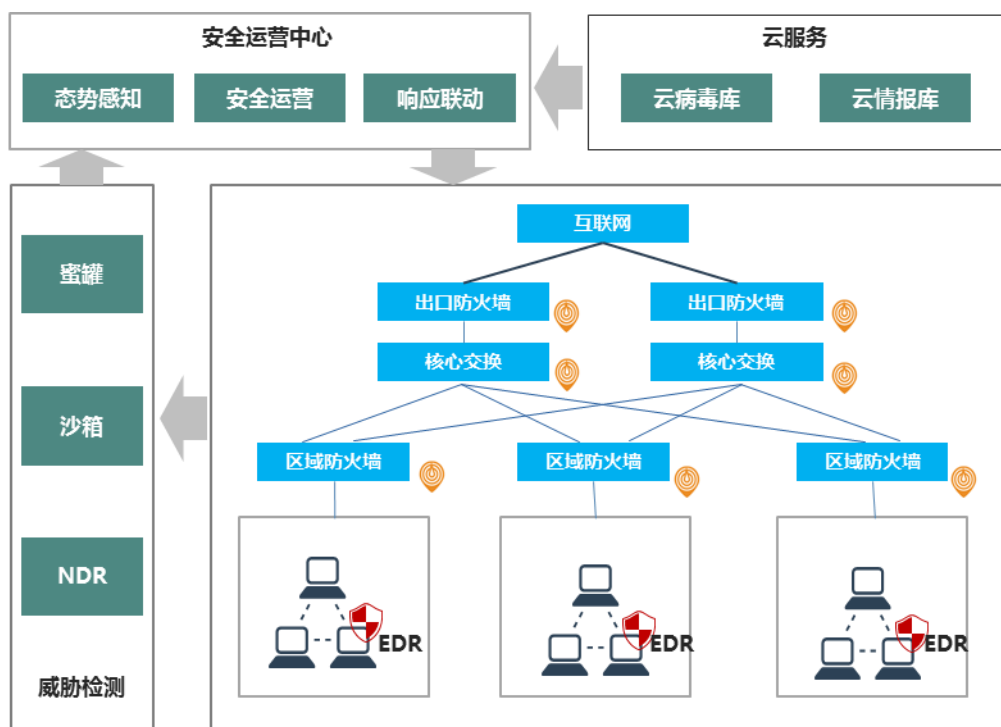
图 4-3 不同员工规模的企业遭受攻击占比



5 新华三勒索防御方案

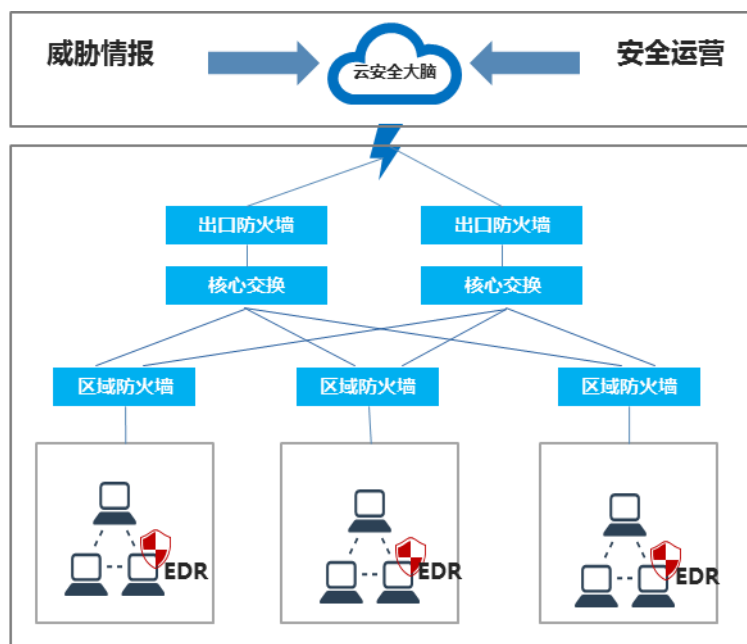
新华三依托“主动安全 3.0”，提供“云-网-边-端”一体化多层次协同防御解决方案，结合云端沙箱阵列、威胁情报库、海量病毒库，全面提升勒索病毒检测能力。本地搭载高性能动静态检测引擎，以及勒索组织常用的攻击工具指纹流量特征，结合加密流量检测、未知威胁分析模块，协同云端，全方位防范勒索病毒入侵。对于已经进入内网的病毒，可以回溯样本投递路径、预测内网传播趋势、及时全网联动阻断，自动及时止损。

图 5-1 新华三勒索防护安全解决方案



同时，新华三安全拥有 AI 全面加持的安全运营中心，依托专业安服与五大攻防团队，提供 7*24h 的防护服务，全面覆盖企业安全运营的技术与管理流程，也可结合用户业务提供定制化防勒索解决方案与实战演习，防范于未然，充分保障企业整体安全建设效果。

图 5-2 勒索防护轻量化解决方案



此外，在中小企业、普教等场景下，用户没有太多预算，但勒索防护攻击又非常频繁，如何低成本高质量进行勒索防护，是此类场景下的核心。新华三基于此场景，推出轻量化勒索防护防御方案。采用“本地产品+云服务”方式，本地轻量化部署，仅需要在出口和区域边界部署防火墙，端侧部署 EDR 产品。云端以安全大脑为核心，结合威胁情报，快速应对病毒变种，低成本实现专家级安全运营。

附录一：年度勒索攻击大事件

政府

1 月，LockBit 攻击美国富尔顿县政府系统，导致系统瘫痪数周，严重影响公用事业、法院和税务网络的运作，许多机构在此期间被迫采用手工办公。

医疗保健

2 月，BlackCat 向美国医疗巨头 Change Healthcare 发动勒索攻击，致使全美医院和药房的处方药交付连续中断达半月之久。此次攻击导致该机构 6TB 的敏感数据被窃取、100 多项服务受到影响，重创了美国医疗保健行业的报销、配药等流程系统。

休闲娱乐

3 月，Rhysida 勒索组织袭击了世界上最大的豪华游艇经销商 MarineMax，窃取了 225G 的数据，包括客户数据库、收益报告、银行账户转账、资产负债和其他财务文件。最终因 MarineMax 拒绝支付赎金，这些数据遭到泄露，影响超过 12.3 万人。

休闲娱乐

4 月，Daixin 勒索组织攻击了美国连锁酒店 Omni，导致其全国范围内的 IT 网络瘫痪，影响到酒店预订、房间锁和 POS 系统。该团伙声称已窃取 Omni 350 多万条客户数据，并索要 300 万美元的赎金。

医疗保健

5 月，Black Basta 勒索组织对美国最大的医疗服务提供商之一 Ascension 发起网络攻击，导致其电子健康系统业务停摆，该医院被迫暂停一些非紧急性手术，工作人员被迫切换到纸上办公。

制造业

6 月，美国汽车行业软件领军企业 CDK Global 遭遇了 BlackSuit 勒索组织攻击，导致 IT 系统中断，影响到北美近 15000 家汽车经销商，损失超过 10 亿美元。随着事件影响不断扩大，BlackSuit 索要赎金从 1000 万美元增加到 5000 万美元。

医疗保健

7 月，美国第三大连锁药店 Rite Aid 遭到 RansomHub 勒索攻击。RansomHub 称在此次攻击中窃取了 10GB 的数据，包括 220 万名客户患者的个人信息、身份证号码、地址等敏感信息。

政府

8 月，Rhysida 勒索组织对佛罗里达州政府发起攻击，入侵了警长办公室系统。Rhysida 窃取了超过 15 万公民的护照、社会保险号等隐私数据，要求该机构支付近 50 万美元的赎金。

医疗保健

9 月，Qilin 勒索团伙向伦敦国民医疗体系发动攻击，泄露了伦敦医院近 100 万患者的数据。其中包括患有癌症和性传播疾病等敏感疾病症状的个人信息。

制造业

10 月，日本著名电子巨头卡西欧遭遇了 Underground 勒索组织的勒索攻击，此次攻击导致卡西欧多个系统瘫痪，发表了暂停接收个人产品的维修服务的声明。同时 Underground 声称窃取了 204.9 GB 的数据，包括卡西欧员工的个人信息、合作伙伴的相关信息等。

物流运输

11 月，SafePay 勒索组织声称对英国远程信息处理供应商 Microlise 的网络攻击负责，并称其窃取了 1.2 TB 的数据。这次攻击导致 DHL 和 Serco 等主要客户的追踪服务中断，造成交付延误，并一度影响到囚犯运输的追踪系统。

公共服务

12 月，Brain Cipher 勒索组织攻击了美国罗德岛 “RIBridges” 社交服务平台，此次攻击将近 65 万人的信息被窃取，包括姓名、地址、出生日期、社会安全号码、银行信息等

附录二：新兴活跃勒索组织一览

Ransomhub

组织画像：

Ransomhub	
首次出现时间	2024-02
传播方式	钓鱼邮件、漏洞利用和密码喷洒攻击等
针对平台	Windows、Linux、VMware ESXi等
编写语言	C++、Go
加密算法	Curve 25519、HC-256、Chacha20
加密后缀	.[由字母+数字组成的随机6个字符]
目标行业	医疗保健行业
勒索模式	双重勒索

勒索信：

```

Hello!

Visit our Blog:

Tor Browser Links:
  http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.c

Links for normal browser:
  http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.c

>>> Your data is stolen and encrypted.

- If you don't pay the ransom, the data will be published on our TOR
appears on our leak site, it could be bought by your competitors at a
sooner you pay the ransom, the sooner your company will be safe.

>>> If you have an external or cloud backup; what happens if you don't

- All countries have their own PDPL (Personal Data Protection Law) re
with us, information pertaining to your companies and the data of you
internet, and the respective country's personal data usage authority
related to your company will be shared with potential competitors thr
you will incur damages far exceeding the amount we are requesting fro

>>> Don't go to the police or the FBI for help and don't tell anyone
    
```

Fog

组织画像：

Fog	
首次出现时间	2024-07
传播方式	漏洞利用、泄露的凭据
针对平台	Windows、Linux
编写语言	C++
加密算法	RSA+AES
加密后缀	.fog、.flocked
目标行业	教育、娱乐行业
勒索模式	双重勒索

勒索信：

If you are reading this, then you have been the victim of a cyber attack. We call ourselves Fog and we take responsibility for this incident. We are the ones who encrypted your data and also copied some of it to our internal resource. The sooner you contact us, the sooner we can resolve this incident and get you back to work. To contact us you need to have Tor browser installed:

1. Follow this link: xql562evsy7njcsngacphc2erzjfecwotdkobn3m4uxu2gthq26newid.onion
2. Enter this code: XXXXXXXXXXXXXXXXXXXXXXXX
3. Now we can communicate safely.

If you are decision-maker, you will get all the details when you get in touch. We are waiting for you.

ElDorado(BlackLock)

组织画像:

ElDorado	
首次出现时间	2024-03
传播方式	漏洞利用
针对平台	Windows、Linux
编写语言	Go
加密算法	RSA+Chacha20
加密后缀	.00000001
目标行业	医疗、教育、房地产
勒索模式	双重勒索

勒索信:

HOW_RETURN_YOUR_DATA.TXT


```
to the board of directors.

Your network has been attacked through various vulnerabilities found in your system.
We have gained full access to the entire network infrastructure.

All your confidential information about all employees and all partners and developments has been downloaded to our servers and is located with us.
-----

Our team has an extensive background in legal and so called white hat hacking.
However, clients usually considered the found vulnerabilities to be minor and poorlyr\n
paid for our services.
So we decided to change our business model. Now you understand how important it isr\n
to allocate a good budget for IT security.
This is serious business for us and we really don't want to ruin your privacy,r\n
reputation and a company.
We just want to get paid for our work whilst finding vulnerabilities in various networks.

Your files are currently encrypted with our tailor made state of the art algorithm.
Don't try to terminate unknown processes, don't shutdown the servers, do not unplug drives,
all this can lead to partial or complete data loss.

We have also managed to download a large amount of various, crucial data from your network.
A complete list of files and samples will be provided upon request.

We can decrypt a couple of files for free. The size of each file must be no more than 5 megabytes.

All your data will be successfully decrypted immediately after your payment.
You will also receive a detailed list of vulnerabilities used to gain access to your network.
-----

If you refuse to cooperate with us, it will lead to the following consequences for your company:
1. All data downloaded from your network will be published for free or even sold
2. Your system will be re-attacked continuously, now that we know all your weak spotsr
3. We will also attack your partners and suppliers using info obtained from your network
4. It can lead to legal actions against you for data breaches

-----
!!!!Instructions for contacting our team!!!!
-----
--> Download and install TOR browser from this site : https://torproject.org
--> For contact us via LIVE CHAT open our website : https://panel\[REDACTED\].onion/Url=
--> If Tor is restricted in your area, use VPN
--> All your Data will be published in 7 Days if NO contact made
--> Your Decryption keys will be permanently destroyed in 3 Days if no contact made
--> Your Data will be published if you will hire third-party negotiators to contact us
```

Cicada3301

组织画像：

Cicada3301	
首次出现时间	2024-06
传播方式	漏洞利用、弱口令爆破、泄露凭据
针对平台	Windows、Linux、VMware ESXi等
编写语言	Rust
加密算法	RSA+Chacha20
加密后缀	.bhk003m
目标行业	医疗、制造、科技
勒索模式	双重勒索

勒索信：

```

*****
***   Welcome to Cicada3301   ***
*****

** What Happened? **
-----
Your computers and servers are encrypted, your backups are deleted.
We use strong encryption algorithms, so you won't be able to decrypt your data.
You can recover everything by purchasing a special data recovery program from us.
This program will restore your entire network.

** Data Leak **
-----
We have downloaded more than %SIZE% GB of your company data.
Contact us, or we will be forced to publish all your data on the Internet
and send it to all regulatory authorities in your country, as well as to your customers, partners, and
competitors.

We are ready to:
- Provide you with proof that the data has been stolen;
- Delete all stolen data;
- Help you rebuild your infrastructure and prevent similar attacks in the future;

** What Guarantees? **
-----
Our reputation is of paramount importance to us.
Failure to fulfill our obligations means not working with you, which is against our interests.
Rest assured, our decryption tools have been thoroughly tested and are guaranteed to unlock your data.
Should any problems arise, we are here to support you. As a goodwill gesture,
we are willing to decrypt one file for free.

** How to Contact us? **
-----
Using TOR Browser:
1) You can download and install the TOR browser from this site: https://torproject.org/
2) Open our website:
http://cicadaxousmk6nbntd3ucxefmfgt2drhtfdvh7gmdeh3ttvudam6f2ad.onion

```

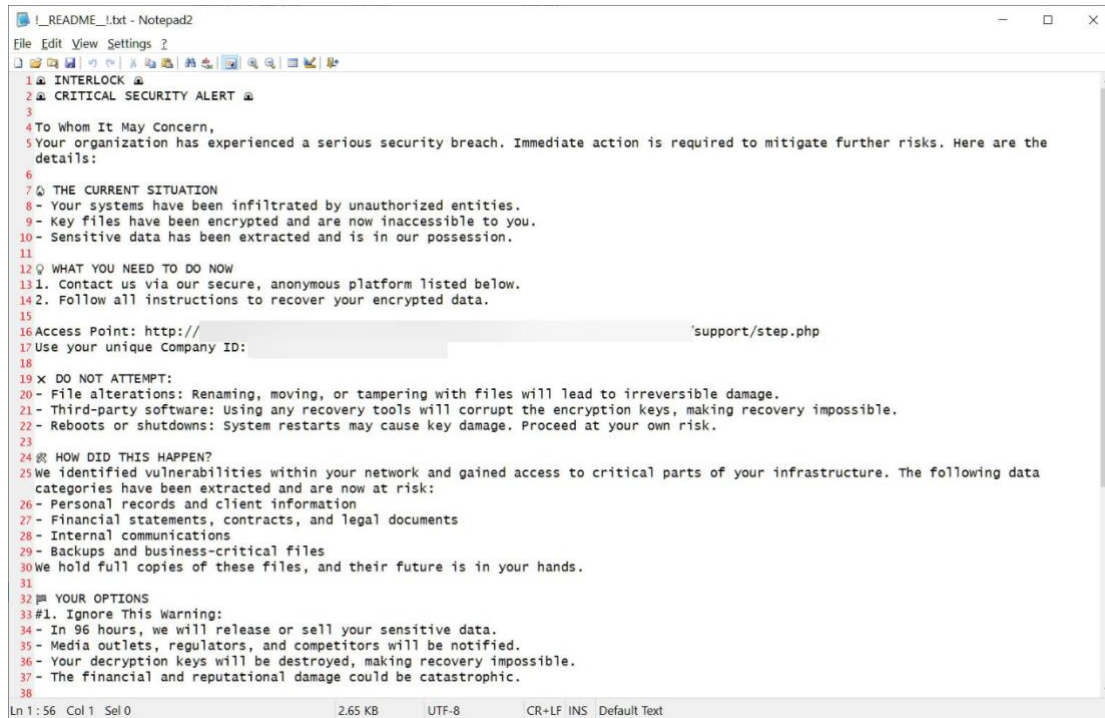
WARNING: DO NOT MODIFY or attempt to restore any files on your own. This can lead to their permanent loss.

InterLock

组织画像：

InterLock	
首次出现时间	2024-09
传播方式	钓鱼攻击、漏洞利用、泄露凭据
针对平台	Windows、Linux
编写语言	C++
加密算法	RSA+AES
加密后缀	.interlock
目标行业	医疗、金融、教育
勒索模式	双重勒索

勒索信：



```
1 1. INTERLOCK
2 2. CRITICAL SECURITY ALERT
3
4 To Whom It May Concern,
5 Your organization has experienced a serious security breach. Immediate action is required to mitigate further risks. Here are the details:
6
7 7. THE CURRENT SITUATION
8 - Your systems have been infiltrated by unauthorized entities.
9 - Key files have been encrypted and are now inaccessible to you.
10 - Sensitive data has been extracted and is in our possession.
11
12 8. WHAT YOU NEED TO DO NOW
13 1. Contact us via our secure, anonymous platform listed below.
14 2. Follow all instructions to recover your encrypted data.
15
16 Access Point: http://[redacted]support/step.php
17 Use your unique Company ID: [redacted]
18
19 9. DO NOT ATTEMPT:
20 - File alterations: Renaming, moving, or tampering with files will lead to irreversible damage.
21 - Third-party software: Using any recovery tools will corrupt the encryption keys, making recovery impossible.
22 - Reboots or shutdowns: System restarts may cause key damage. Proceed at your own risk.
23
24 10. HOW DID THIS HAPPEN?
25 We identified vulnerabilities within your network and gained access to critical parts of your infrastructure. The following data categories have been extracted and are now at risk:
26 - Personal records and client information
27 - Financial statements, contracts, and legal documents
28 - Internal communications
29 - Backups and business-critical files
30 We hold full copies of these files, and their future is in your hands.
31
32 11. YOUR OPTIONS
33 #1. Ignore This Warning:
34 - In 96 hours, we will release or sell your sensitive data.
35 - Media outlets, regulators, and competitors will be notified.
36 - Your decryption keys will be destroyed, making recovery impossible.
37 - The financial and reputational damage could be catastrophic.
38
```

Ln 1 : 56 Col 1 Sel 0 2.65 KB UTF-8 CR+LF INS Default Text

附录三：安全建议和处置清单

安全建议

企业建议

1. 注重员工安全意识培训

- (1) 建立定期的安全意识培训课程，了解勒索软件、网络钓鱼、恶意软件的特征与危害
- (2) 设立安全意识奖励机制，鼓励对可疑的电子邮件和网站进行上报
- (3) 定期举办网络安全模拟演习

2. 加强网络访问控制与身份验证

- (1) 实施多因素身份验证，如叠加验证码、生物识别技术等
- (2) 权限管理策略坚持最小权限原则，严格控制或关闭非必要的端口与功能
- (3) 使用零信任解决方案

3. 安全更新和数据备份

- (1) 及时对系统和软件进行补丁更新和漏洞修复
- (2) 对关键的数据应采取离线备份和加密存储等方式进行备份
- (3) 对安全设备、杀软也需定期更新，以保障防御方案的有效性和实时性

个人建议

1. 勒索软件我知道

了解勒索软件的常见攻击手段以及被勒索软件入侵后造成的危害，如财物损失、业务影响等，增强对威胁的认识和警惕性

2. 网络行为我负责

- (1) 避免随意点击来自电子邮件、社交媒体中未知或可疑的链接，点击之前要先验证链接的真实性和信任度，确保它们指向安全的站点或资源

- (2) 谨慎下载和安装软件，只从官方和可信的来源下载和安装软件，避免下载来自不明来源或未经验证的软件，这些软件可能携带恶意代码
- (3) 防止网络钓鱼攻击，避免在未经验证的网站上输入个人敏感信息，警惕仿冒的电子邮件、登录页面、社交媒体链接等
- (4) 避免在不安全或未加密的公共 Wi-Fi 网络上进行敏感信息的传输，如银行账户信息、密码等
- (5) 保持操作系统、浏览器和最新版本，并定期更新安全补丁，以修复已知的漏洞

3. 账户安全我先行

- (1) 创建复杂、独特好记且难以猜解的密码，包括字母、数字和特殊字符的组合，避免使用包含生日、姓名等常用词的密码
- (2) 定期更换密码，每三个月或更频繁进行更改，避免重复使用相同的密码

4. 数据备份我会用

- (1) 定期备份数据，并定期验证备份数据的完整性和可访问性，确保备份文件能够正常恢复和使用，同时在备份前要检查存储介质是否安全可靠，包括移动硬盘、U 盘等

5. 安全软件我不关

- (1) 使用防火墙和其他具有威胁防护能力的安全软件，用于检测和阻止病毒、恶意软件入侵，做到不随意关闭或退出这些安全软件，以及确保这些软件的及时更新

勒索软件应急处置清单

1. 立即隔离感染主机

- (1) 立即拔出感染主机的网线、禁用网卡，关闭无线网络和蓝牙连接，断开感染主机的外部硬盘、USB 驱动器等存储设备，将感染的主机从公司网络中隔离出去，防止对其他设备造成影响
- (2) 关闭远程桌面等服务，包括 3389、445、139、135、5900 等不必要的端口

2. 确定感染范围

- (1) 检查文件共享目录、内部和外部存储设备以及云存储服务中的文件，看是否已经被勒索软件加密，通常被加密的文件的扩展名都会被修改，并且无法正常打开，当发现机器上重要文件尚未被加密时，应立即终止勒索软件进程或者关闭机器，及时止损
- (2) 通过分析网络流量和日志，查找可疑的通信和数据传输，以确定感染是否进一步扩散到其他设备或网络区域

3. 感染溯源分析

- (1) 查看勒索软件在主机内是否留下勒索信，在勒索信中可以判断出感染的是哪一种勒索家族病毒
- (2) 收集主机的日志信息，通过查看日志信息有可能判断病毒植入路径
- (3) 收集病毒样本，后续提供给安全厂商作进一步分析

4. 排查加固

- (1) 关闭相应端口、网络共享、修改内网内主机的弱密码，修复相关补丁和漏洞
- (2) 安装高强度防火墙，防病毒软件进行全面扫描，防止二次感染勒索

5. 业务恢复

- (1) 如果主机上的数据存在备份，可以自行还原备份数据，恢复业务
- (2) 请专业公司进行数据和系统恢复工作

新华三聆风实验室

新华三聆风实验室专注于威胁狩猎、情报生产、高级威胁追踪等技术研究。基于对全球活跃恶意团伙的跟踪与分析、安全事件响应处置、海量恶意样本的自动化情报提取以及多元基础数据的关联分析等方法，结合人工+AI 研判策略和运营流程，实时产出多维度的威胁情报，为新华三安全产品和解决方案持续赋能。同时，实验室致力于高级威胁攻击的技术研究，包括跟踪、分析、监测与报告输出等。

主动安全

新华三以主动安全理念为核心

致力于成为客户业务数字化转型的助力者

融绘数字未来 共享美好生活



www.h3c.com

Copyright © 2025 新华三集团 保留一切权利

免责声明:

虽然新华三集团试图在本资料中提供准确的信息，但不保证本资料的内容不含有技术性误差或印刷性错误，为此新华三集团对本资料中信息的准确性不承担任何责任，新华三集团保留在没有任何通知或提示的情况下对本资料的内容进行修改的权利。

CN-170X30-20220422-BR-HZ-V1.0