构建安全可信的数字世界
Build A Secure And Credible Digital World

安恒信息
DAS-security 安全中国

科创板：688023

2023年全球勒索软件
研究报告

猎影实验室

目　录

文档声明

本文档内容是杭州安恒信息技术股份有限公司对 2023 年全球勒索软件态势所编写的文档。文中的资料、说明等相关内容均归杭州安恒信息技术股份有限公司所有。本文中的任何部分未经杭州安恒信息技术股份有限公司许可，不得转印、影印或复印。

引言

勒索软件（Ransomware）是一种不断发展的恶意软件，旨在通过加密或其他方式更改系统的组成部分，从而完全阻止受感染系统的访问。勒索软件的主要目的是破坏目标系统的完整性，使其无法正常运行，并有效地锁定重要的数据。一旦系统被勒索软件感染，网络犯罪分子就会要求受害者支付赎金，以恢复系统的功能和访问权限。通常，赎金需要以加密货币的形式支付，这使得追踪攻击者和确定他们的身份变得困难。近年来，勒索软件已成为最突出和最具破坏性的恶意软件类型。

勒索攻击在 2023 年全年呈现出复杂化、范围扩大、目标精准化、技术升级和经济利益驱动等特点，总体攻击态势包括：

- 2023 年共披露 4832 起勒索攻击事件，较 2022 年相比大幅增长。2022 年平均每月攻击次数约为 220 次，而 2023 年则增至约为 402 次，增幅达 82.73%。
- 美国、英国、加拿大、意大利和德国仍是攻击的五个重要受害地区。服务行业、IT 行业和制造业是勒索攻击的主要目标行业。
- 2023 年最活跃的五个勒索团伙为 LockBit、BlackCat、Clop、Play 和 8Base，其中 8Base 是今年新出现的勒索团伙。
- 大型勒索组织持续加强漏洞武器化的能力，利用 GoAnywhere MFT、MOVEit Transfer 和 Citrix 等软件中的漏洞发起勒索攻击。
- 国际执法行动捣毁了包括 Hive、Ragnar Locker 在内的勒索团伙和

相关基础设施，但勒索威胁的不断演进仍然让网络安全面临着严峻挑战。

- 勒索软件团伙可能会利用人工智能（AI）技术扩展和改进攻击，追求攻击的自适应和智能化。

安恒研究院发布《2023 年全球勒索软件态势报告》，详细介绍 2023 年的勒索攻击整体情况、活跃团伙以及热点事件，分析研判勒索攻击的特点和预测 2024 年的勒索趋势，并提供防御措施，以帮助读者了解勒索软件生态的整体发展态势。

2023 全球勒索软件攻击态势

2023 年全球共公开披露 4832 起勒索软件攻击事件，较 2022 年的 2640 起相比，攻击次数整体呈现大幅增长。以每月攻击次数的平均值来看，2022 年平均每月攻击次数约为 220 次，而 2023 年则增至约为 402 次，增幅高达约 82.73%。

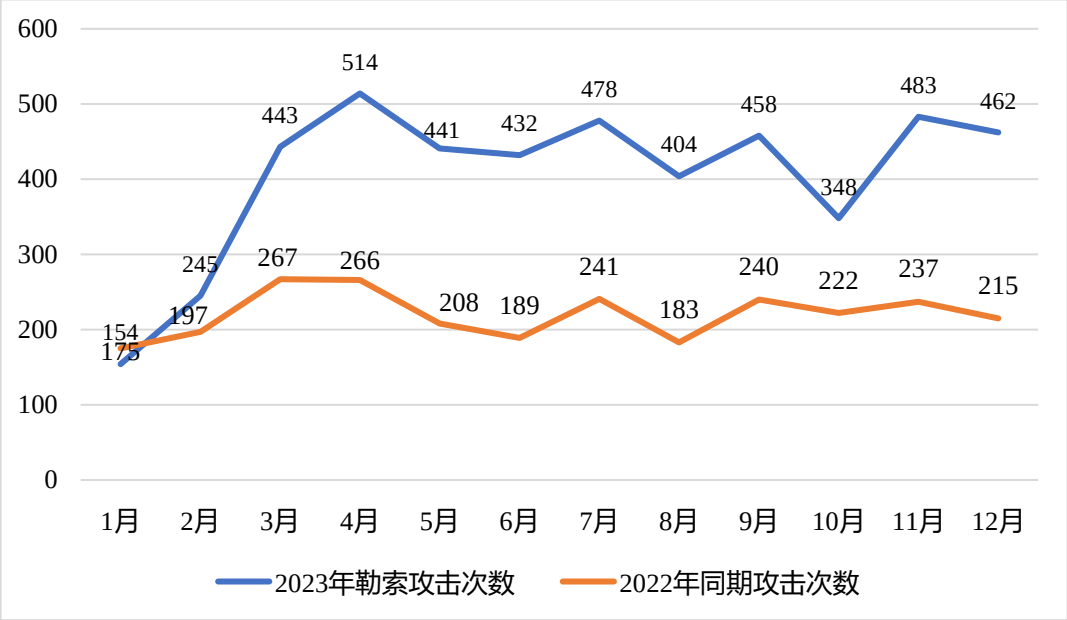


图 2023 年每月全球披露的勒索攻击次数统计

在全年 12 个月的时间跨度内，勒索软件攻击次数较去年相比每个月都呈增长趋势。年初增幅相对较小，随后在 3 月显著增长，增幅达 57.6%。后续连续 9 个月勒索攻击数量都在 300 起以上，月攻击次数全面超越 2022 年。

2023 年勒索软件攻击跨越国家和地域的限制，呈现出明显的全球蔓延趋势。数据显示，与 2022 年勒索攻击的整体情况一致，美国、英国、加拿大、意大利和德国仍是攻击的五个重要受害地区，其中美国是受攻击最

严重的地区，共发生了 2103 起攻击事件。

2023 年整年勒索攻击的受害者按地区划分的比例图如下：

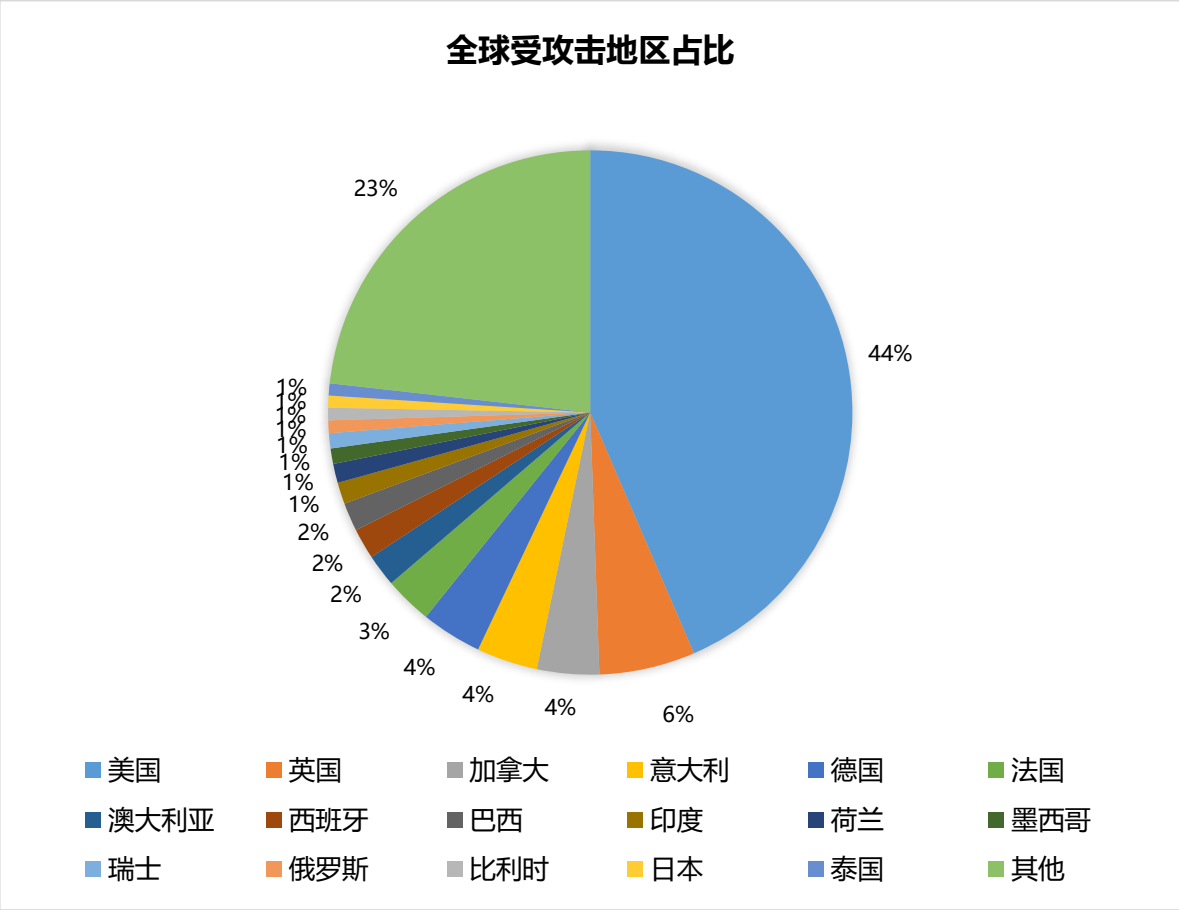


图 2023 年全球受攻击地区统计

上述几个受影响最严重的国家拥有庞大的经济规模和复杂的产业结构，所属地区运营着大量的跨国公司和大型企业。这些公司有着复杂的供应链和广泛的业务覆盖范围，且具备更多的资金和敏感数据，因此极易成为勒索团伙的目标。此外，这些国家在数字化程度方面相对较高，许多关键基础设施和产业都依赖于网络和信息技术，这也意味着可能存在更多的漏洞和安全隐患，攻击者更容易发现和利用网络的弱点进行入侵和勒索。

2023 年，服务行业、IT 行业和制造业成为勒索攻击的主要目标。服

务行业已披露的攻击次数最多，高达 1170 起，IT 行业和制造业分别遭遇了 454 次和 461 次的攻击。物流、零售、教育、医疗保健和科技行业等也属于受攻击占比较高的行业。这些行业具有重要性、数据丰富性等特点，并且有着潜在的经济影响，因此成为攻击者优先选择的领域。

2023 年勒索攻击受害者的行业分布比例图如下：

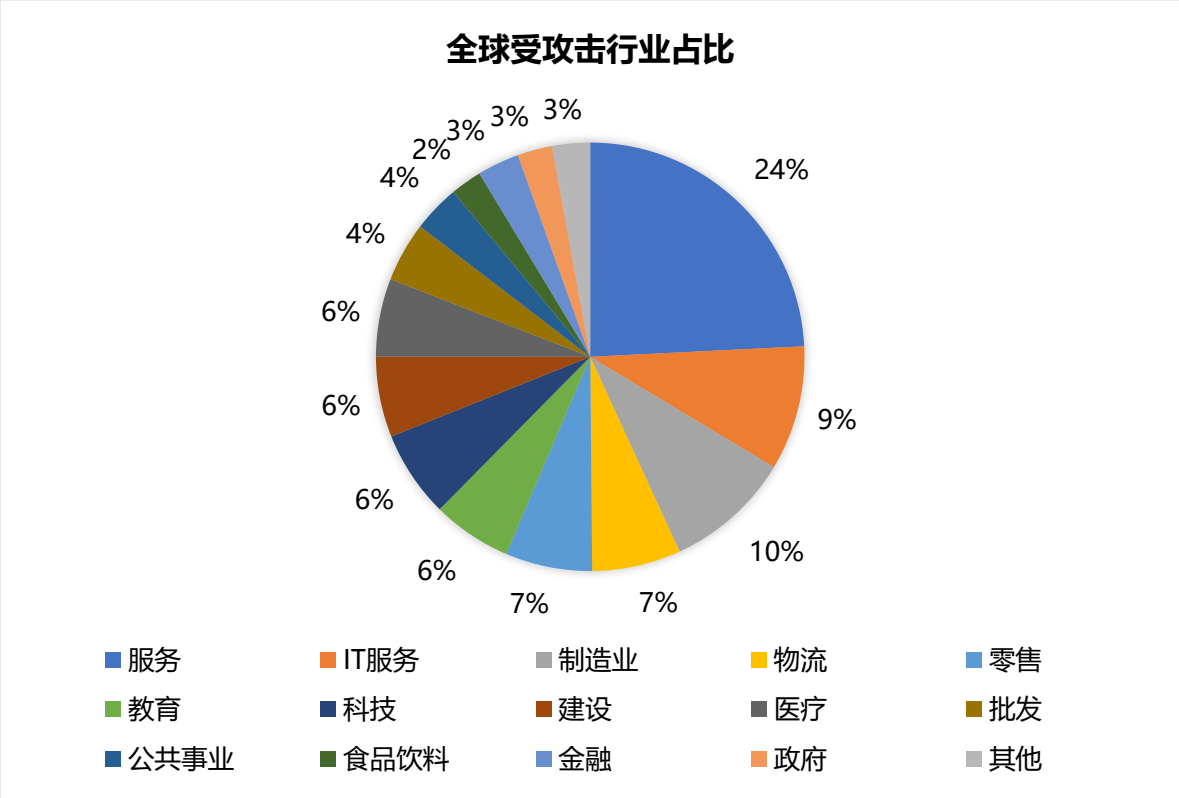


图 2023 年全球勒索攻击行业统计

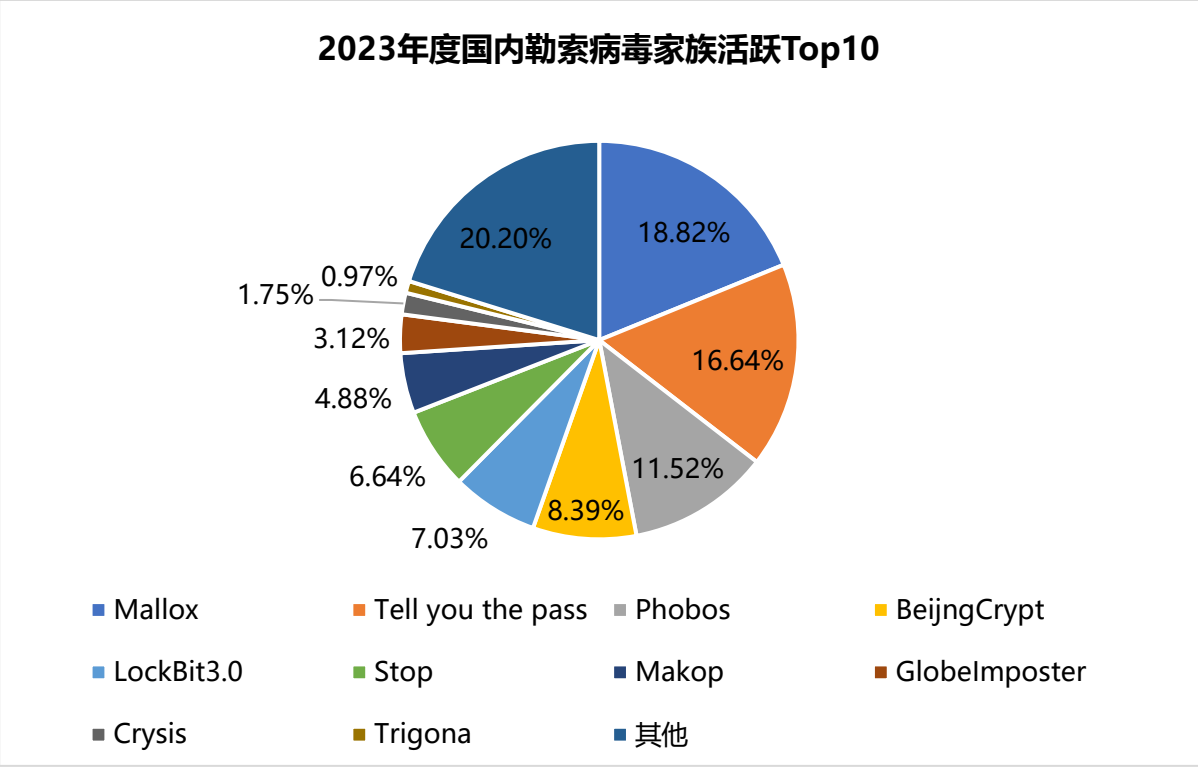
服务行业涉及餐饮、酒店、旅游等领域，IT 行业负责管理和维护信息技术基础设施，制造业涉及生产和供应链管理。攻击这些行业可能造成重要服务的停滞，影响居民所需的关键服务，对社会和经济运作产生较大的影响。这些行业通常拥有大量的用户数据、商业机密和敏感信息，攻击者可以通过勒索软件攻击获取这些有价值的数据，并将其用作勒索的筹码。

此外，服务行业、IT 行业和制造业涉及复杂的供应链，攻击其中的一个环节可能会对整个供应链产生连锁反应，对其他相关企业和行业造成影响。攻击者可能会利用这一点来实现更大范围的攻击和勒索。

2023 中国勒索软件攻击态势

自 2023 年以来，我国遭受勒索攻击的频率明显增加，由于网络攻击技术的不断演进以及 RaaS 运营模式的不断成熟，使得即便是技术素养相对较低的不法分子也能够轻松参与其中，并且成功渗透的可能性不断增大。加之不断有网络犯罪团伙加入到勒索生态当中，漏洞武器化利用速度加快。因此，以经济动机为基础的勒索攻击有可能进一步蔓延，对未来网络安全构成潜在的威胁。

2023 年度国内勒索病毒流行情况与 2022 年度相比变化不明显，Mallox、Tellyouthepass 和 Phobos 等勒索软件家族自 2022 年开始就是国内的主要危害来源。



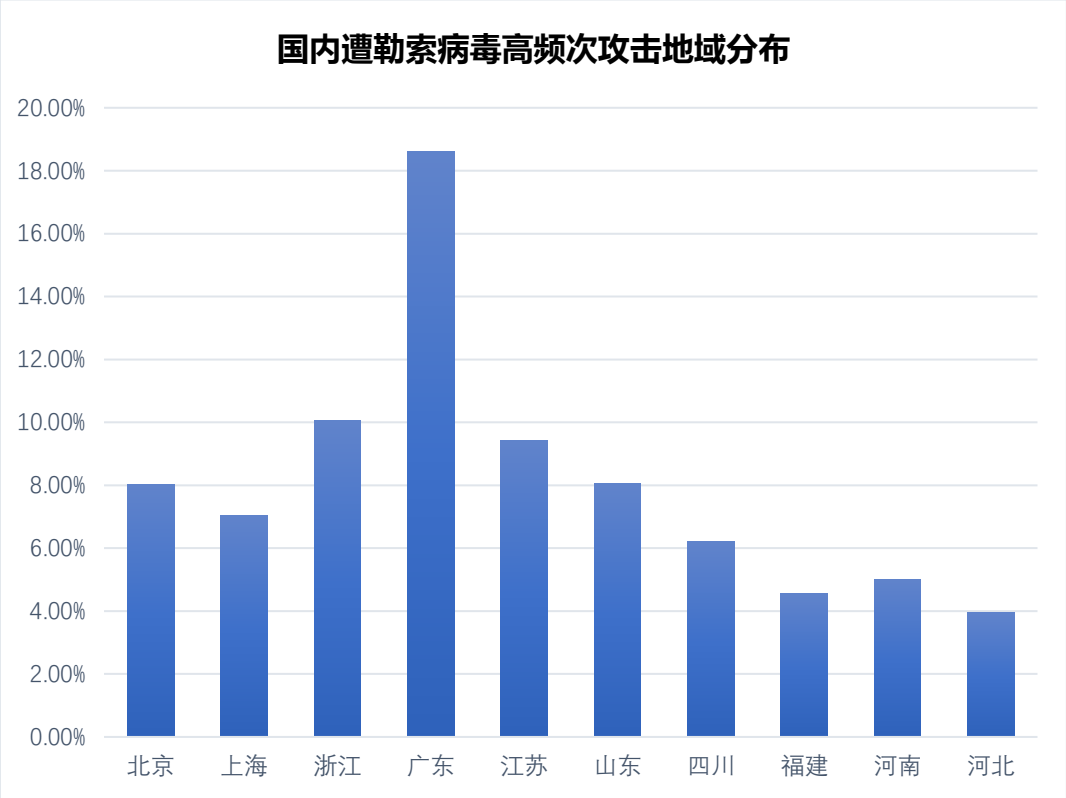
2023 年国内勒索病毒家族活跃 Top10

2023 年，针对我国的活跃勒索家族包括：

- Mallox：Mallox 别名 Target Company，于 2021 年 6 月被首次发现，2021 年 10 月在国内出现攻击事件。该勒索家族目前已有多个变种，采用 RAAS 的运营模式，主要针对包括 Spring Boot、通达 OA 等在内的 Web 应用系统。该家族使用多个渠道进行传播，包括匿隐的僵尸网络、横向渗透以及数据库弱口令爆破等。常用的加密文件算法为 Curve25519+ChaCha20。
- Tell you the pass：该家族主要通过各种软件漏洞、系统漏洞进行传播，例如之前广泛存在于 OA 系统上的 Log4j2 漏洞、某企业管理软件的反序列化漏洞、Apache ActiveMQ 远程代码执行漏洞（CVE-2023-46604）等。Tell you the pass 最早出现于 2020 年 7 月，长期活跃，主要目标集中在国内，使用 RSA+AES 的组合加密算法加密目标系统的文件。
- Phobos：Phobos 于 2019 年初开始传播，该勒索软件常见传播方式为暴力破解 RDP 登录，进行人工手动投毒。在国内长期活跃，并不断更新，至今已积累了多个变种，目标大多为中小企业。进入系统后往往会关闭防护软件，添加自启动，使用 AES+RSA 算法组合加密文件。
- BeijngCrypt：该家族主要通过暴力破解 RDP 或 SQL 服务器来传播，以.beijing 等作为扩展名，可以看出带有明显的地域针对性。该家族使用 RSA+AES 算法组合加密文件。

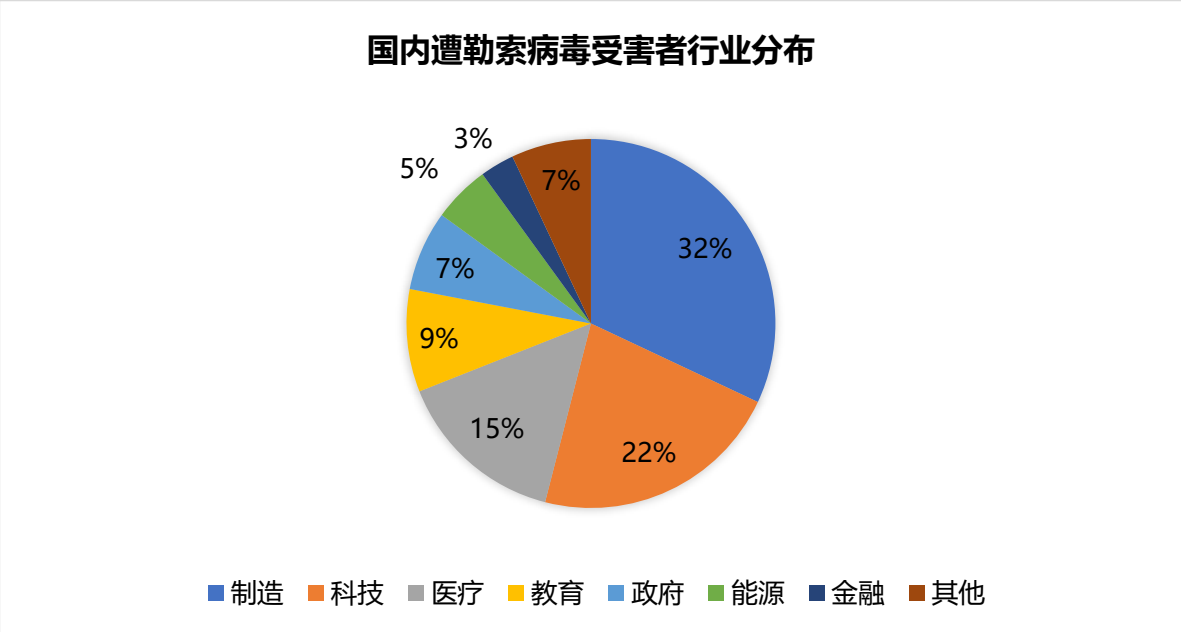
- LockBit3.0：这是 2023 年最活跃的勒索软件团伙。LockBit 勒索软件采用勒索即服务的运营模式，招募附属公司使用 LockBit 勒索软件工具和基础设施进行勒索软件攻击。
- Trigona：该家族是一种相对较新的勒索软件，自 2022 年 10 月下旬起一直保持高度活跃，普遍认为 Trigona 背后可能与 CryLock 勒索软件是同一组威胁行为者。2023 年 4 月，Trigona 开始通过暴力破解方法窃取凭据来针对受感染的 MSSQL 服务器。5 月，发现存在 Trigona 的 Linux 版本，它与 Windows 版本有相似之处。在 10 月份，该勒索组织的泄露网站服务器被乌克兰网络联盟攻陷被迫关闭，但不久，11 月下旬，安全研究人员发现 Trigona 更换了暗网博客的地址重新上线。
- Makop：Makop 勒索病毒家族最早于 2020 年 1 月被研究人员发现，该家族常使用暴力破解 RDP，获取登录凭证后手动投毒的方式进行传播，主要采用 RSA+AES 加密算法来加密文件。
- Stop：Stop 勒索家族，别名 Djvu，最早于 2018 年 8 月被发现，以伪装成破解软件或者激活软件作为捆绑，诱导用户下载运行作为主要的传播方式。该家族变种繁多，最近 2 年都广泛活跃在国内，使用 RSA+Salas20 算法加密文件。
- Crysis：又称为 Dharma，Crysis 于 2016 年首次出现，相关变种数量极多，该病毒主要通过垃圾邮件、RDP 远程桌面和弱口令爆破进行传播和感染，采用 AES+RSA 的加密方式。

根据 2023 年以来勒索攻击的应急响应数量，对遭受勒索病毒攻击的系统所属地域进行统计分析发现，数字经济发达地域是勒索病毒攻击的主要对象。同时，广东、浙江、江苏、山东等沿海和贸易港口较多的地区近年来受勒索攻击情况呈现逐年增长趋势，可见勒索攻击的目标区域正在扩大范围。



2023 年国内勒索病毒高频次攻击地域分布（统计区间：2023 年 1 月至 2023 年 12 月）

通过对 2023 年已知勒索攻击事件进行分析，制造业、科技和医疗等行业受勒索病毒影响最为严重，分别占比 32%、22%和 15%。教育和政府也较频繁的受到勒索病毒攻击。其中制造业和医疗行业对业务的连续性和系统的可用性具有较高的要求，被迫缴纳赎金的情况较多，因此成为勒索病毒的重灾区。



2023 年国内勒索病毒受害者行业分布（统计区间：2023 年 1 月至 2023 年 12 月）

对受害者使用的操作系统进行统计发现，桌面系统仍然是勒索病毒的主要感染目标，占比高达 56%。桌面系统中的 Windows10 和服务器系统中的 Windows Server 2008 是最易受到攻击的操作系统类型。国内容易受到影响的软件/系统包括：

软件名称	应用类型	攻击方式
Windows	操作系统	漏洞利用/RDP 暴力破解/网络钓鱼
MSSQL/MYSQL	数据库服务	漏洞利用/数据库弱口令暴力破解
Microsoft Exchange	邮件服务器	漏洞利用
QNAP 的 NAS 设备	数据存储服务	漏洞利用

软件名称	应用类型	攻击方式
Spring 框架	Web 服务	漏洞利用
OA/企业管理系统	办公/财务管理	漏洞利用
HIS 系统	医疗信息化系统	漏洞利用
Redis	数据存储服务	漏洞利用

勒索团伙介绍

全年勒索软件攻击占比

2023 年，勒索软件攻击呈现出多样化和动态演变的态势。2023 年全年最活跃的五个勒索团伙为 LockBit、BlackCat、Clop、Play 和 8Base，其中 LockBit 以 1089 次攻击稳居于首位。

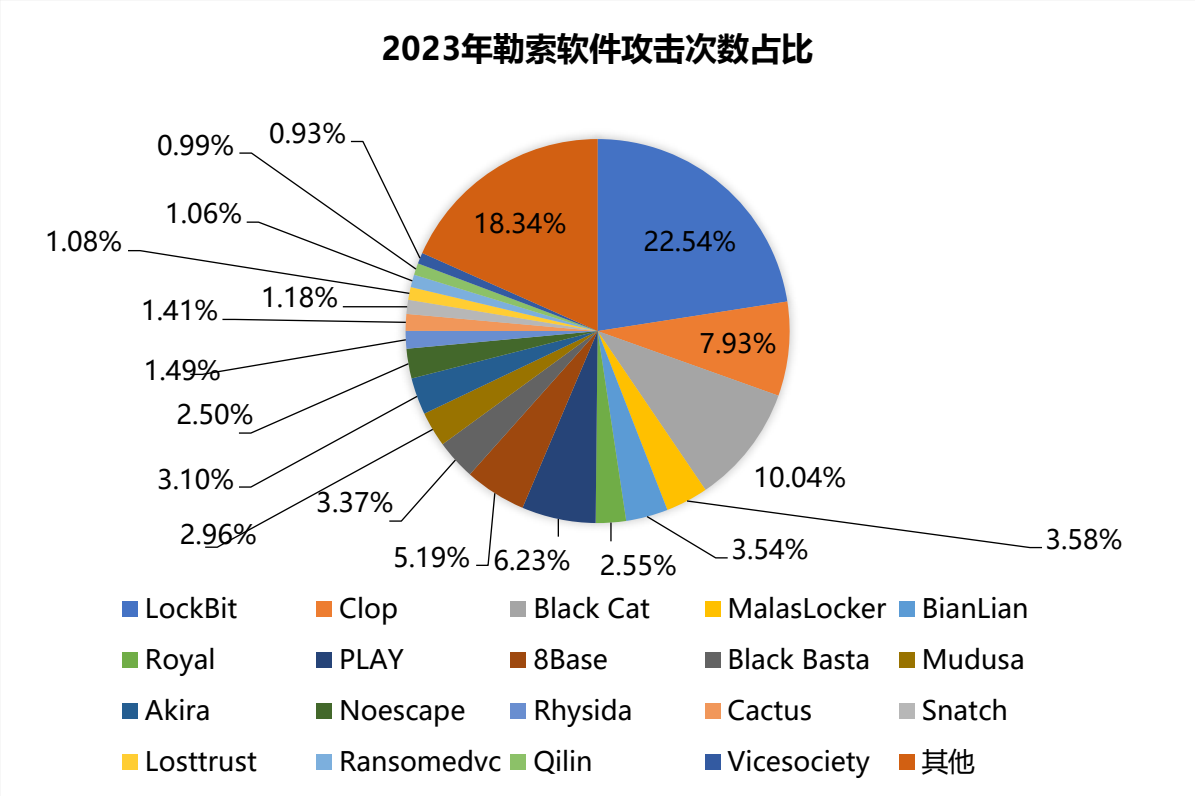


图 2023 年全球勒索软件攻击家族分布

相较于 2022 年，最活跃的勒索团伙发生了一定的变化。2023 年 1 月底，Hive 勒索团伙因国际执法行动而被瓦解，这成为勒索软件攻击态势的重要转折点。与此同时，MalasLocker、Akira、8Base、Rhysida 等新兴勒索软件团伙迅速崛起，填补了 Hive 团伙的空缺。此外，2022 年活跃的 Bl

ack Basta 团伙今年仍在发起勒索攻击，但攻击频率相较于去年有所下降。

LockBit、BlackCat 和 Clop 这三个勒索团伙过去几年中一直是勒索软件攻击领域的主要参与者。它们的长期存在和持续活跃性表明这些团伙具有高度的组织化、专业化和适应性。

2022 年，LockBit 是全球部署最多的勒索软件变种，其在 2023 年继续多产，依然保持高频次的勒索攻击活动，是今年最为活跃的勒索组织。2023 年，LockBit 不仅开发了基于 Conti 源码的 LockBitGreen 勒索变体，还定制了针对包括 MacOS 在内的多个操作系统加密程序的测试版本，进一步展示出该团伙强大的创新和持续开发能力。

Clop 勒索组织在 2023 年异军突起，利用 GoAnywhere（CVE-2023-0669）PaperCut（CVE-2023-27350）和 MOVEitTransfer（CVE-2023-34362）等漏洞，在全球范围内造成了严重的影响，受到了广泛关注。

值得注意的是，今年新出现的勒索组织占据攻击次数 Top20 的将近一半席位，新兴勒索表现十分抢眼，例如第五名的 8Base 勒索和紧随其后的 MalasLocker 勒索，攻击次数都达到了 150 以上，迅速跻身活跃勒索的前列。

季度攻击排行

2023 年最具活跃度的勒索团伙在不同时间段呈现一定程度的变化。为了更加清晰地呈现每季度的变化和趋势，我们将在接下来的内容中按季度逐一介绍当前季度最活跃的六个攻击团伙，帮助读者更深入地理解 2023

年勒索攻击态势的演变。

1. 第一季度

下图为 2023 年第一个季度最活跃的 6 个勒索团伙，星号标记的团伙为首次出现在榜单或占比排名有显著变化的团伙。

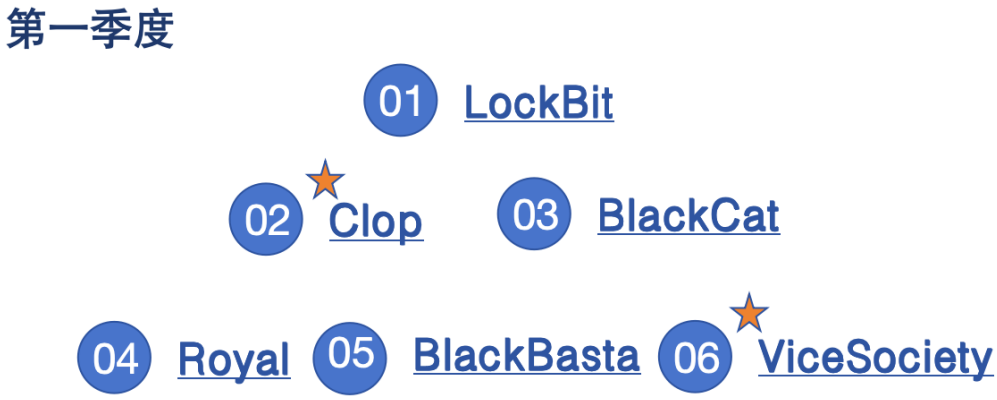


图 2023 年第一季度 TOP6 勒索家族

新年伊始，LockBit 依然位居最多产的勒索软件即服务(RaaS)的榜首。研究人员发现了 LockBitGreen 变体，这个最新的勒索软件版本是该团伙继 LockBit Red 和 LockBit Black 之后的第三个版本，其 89%的代码与 Conti v3 勒索软件共享，并且已被用来攻击至少 5 名受害者。

1 月，针对教育部门的勒索攻击占比排名第二，这与 Vice Society 团伙的活跃紧密相关。Vice Society 总部位于俄罗斯，攻击目标是大学、学院和 K-12 学校。Vice Society 于第一季度在其泄露网站上公布了九所学校的数据。

在 3 月，Clop 组织取代 LockBit 成为当月最多产的勒索软件团伙。这

一变化的根本原因在于，Clop 团伙利用 Fortra 的 GoAnywhere 软件中的漏洞发起大规模攻击，窃取了大量数据，影响约 130 个组织。这也彰显了漏洞利用在勒索攻击中的重要作用。

2. 第二季度

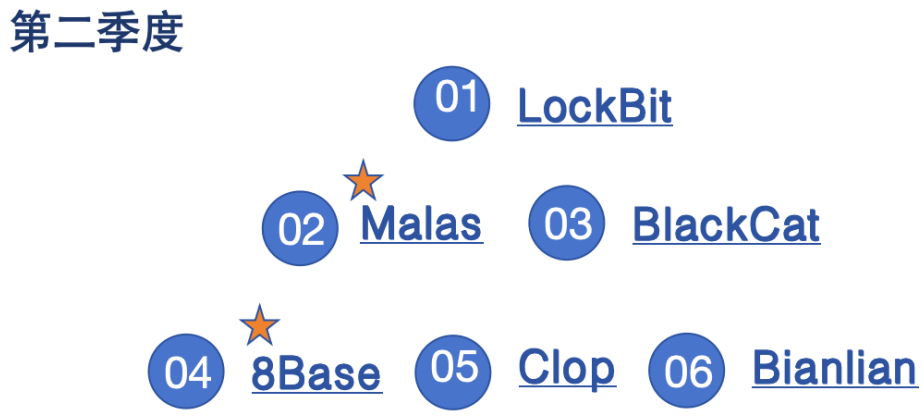


图 2023 年第二季度 TOP6 勒索家族

第二季度涌现了一批新的强劲勒索组织，其中 Malas Locker 和 8Base 勒索迅速拿下多名受害者，引人注目。

Malas Locker 首次出现于 3 月底，在 5 月针对 Zimbra 服务器以窃取电子邮件和加密文件，累计攻击了 170 多家单位，与一般勒索不同的是并没有要求支付赎金，而是声称要求受害者向慈善机构捐款。

8Base 勒索虽然于 2022 年 3 月就已经出现，但开始时保持相对安静，几乎没有明显的攻击，2023 年 5 月后勒索活动激增，针对各行各业的许多公司并进行双重勒索。

此外，其他新型勒索例如 Akira、Rhysida 和 Noescape 也在这一季度内开始崭露头角，受害者数量逐渐增加，蓄势待发。

3. 第三季度

图 2023 年第三季度 TOP6 勒索家族

第三季度全球的勒索攻击活跃程度不减，7 月 Clop 组织在 MOVEit Transfer 的 0day 漏洞的影响加持下新勒索了 170 名受害者，和 4 月份的 Malas Locker 攻击次数持平，达到全年当月勒索攻击次数最多的组织之一。随后的 8-9 月却消无声息，仅发布了很少的受害者,其背后原因可能是大多数单位都修补了该漏洞。

在 9 月，AKira 同样利用思科 VPN 设备中的 0day 漏洞 CVE-2023-20269 发起勒索攻击，该组织从 4 月被发现以来，持续到 9 月，已经积累了 100 多名受害者，是今年出现的代表性勒索组织之一。

4. 第四季度

图 2023 年第四季度 TOP6 勒索家族

在 2023 年的最后一个季度，勒索攻击迎来年底的狂潮，相继有大型跨国公司沦陷，例如在 10 月，LockBit 向全球知名 IT 供应商 CDW 要价八千万的赎金，此后又宣称入侵了美国波音公司，并在 11 月公布了窃取的数据，引人注目。11 月，Medusa 勒索组织将丰田公司旗下德国金融服务子公司加入受害者名单，要求支付 800 万美金。

今年出现的新勒索组织在第四季度也表现突出，例如 Rhysida 勒索相继攻陷了大英图书馆、斯洛伐克电力公司等重大目标单位和企业。Noeascape 勒索主要针对医疗保健行业进行勒索攻击，截止 12 月，今年已经发布了 120 多名受害者信息。

勒索团伙介绍

1. 活跃团伙

1) LockBit

LockBit（曾用名为 ABCD 勒索软件）是 2023 年最活跃的勒索软件团伙。自 2020 年 1 月以来，使用 LockBit 的附属公司攻击了一系列关键基础设施领域的不同规模的组织，包括金融服务、食品和农业、教育、能源、政府和紧急服务、医疗保健、制造和物流等。LockBit 勒索软件采用勒索即服务的运营模式，招募附属公司使用 LockBit 勒索软件工具和基础设施进行勒索软件攻击。

2019 年，研究人员首先观察到 ABCD 勒索软件的活动，这是 LockBit 的前身。2020 年 1 月，以 LockBit 命名的勒索软件首次出现在基于俄语的网络犯罪论坛。2021 年 6 月，LockBit2.0 出现（也称为 LockBitRed），推出 StealBit 信息窃取工具。LockBit2.0 勒索团伙随后于 2021 年 10 月引入 LockBitLinux-ESXiLocker1.0 版，将功能扩展至 Linux 和 VMwareESXi 的目标系统。

2022 年 6 月，勒索团伙推出 LockBit 3.0（也称为 LockBitBlack），其与 BlackMatter 和 BlackCat 勒索软件有相似之处，并且引入了勒索软件漏洞赏金计划，邀请安全研究人员提交漏洞报告，以换取 1000 美元至 100 万美元的奖金。此外，LockBit 3.0 在其赎金支付方式中添加了 Zcash 隐私币。

2022 年 9 月，一位名为“AliQushji”的新注册 Twitter 用户表示，其团队入侵了 LockBit 服务器，并找到了 LockBit 3.0 勒索软件的生成器。但团伙成员 LockBitSupp 声称并没有遭到黑客入侵，泄密者是 LockBit 勒索软件组织雇用的程序员，开发人员对 LockBit 的领导层心怀不满，所以泄露了生成器。

2023 年 1 月，安全研究人员发现 LockBitGreen 变体，分析后确定其结合了来自 Conti 勒索泄漏的源代码。2023 年 4 月，安全研究人员在 VirusTotal 上发现了一个 zip 存档，其中包含大多数可用的 LockBit 加密器，包括以前未知的 MacOS、ARM、FreeBSD、MIPS 等多种系统架构的加密器，后续分析表示这只是 LockBit 构建的测试版本，尚在开发阶段，未达到真正加密的功能，但这也揭示出该勒索团伙出众的创新开发能力和澎湃的野心。

时间	受害者	影响
1 月	洛杉矶住房管理局 (H	系统中断，15TB 的 HACLA 数据

时间	受害者	影响
	ACLA)	库图像被盗。
	英国皇家邮政	迫使国际邮政服务陷入停摆。
	日本电子产品制造商 Fujikura Global	泄露了 718GB 的机密和关键信息。
2 月	金融交易服务集团 ION	影响了包括一些全球最大银行、经纪公司和对冲基金在内的客户。
	全球电源产品制造商 Phihong	要求受害者支付 50 万美元的赎金。
	德克萨斯州 White Settlement 学区	2015 年或更早时间的文件被窃取。
3 月	佛罗里达州东北部华盛顿县治安官办公室	影响了部门应用程序，并破坏了财务和监狱网络。
	奥克兰市	非紧急系统处于离线状态。
	零部件制造商 Maximum Industries	窃取了 SpaceX 工程师开发的约 3000 个专有原理图。
4 月	新泽西州的 Pineland 学校	窃取了 65GB 数据的样本。
	委内瑞拉银行	窃取了部分数据。

时间	受害者	影响
5 月	Farmalink 处方药销售系统	联网计算机停止工作，管理虚拟机的软件也断开连接。
	非金融银行公司富乐顿印度公司	泄露了 600GB 的数据。
	印度尼西亚伊斯兰银行	窃取的 5TB 个人和财务信息。
6 月	印度制药巨头 Granules India	公布了被盗的部分数据。
	半导体制造商台积电	索要高达 7000 万美元的赎金。
7 月	日本名古屋港口码头	日本最大的港口名古屋港的所有集装箱码头运营均已中断
8 月	加拿大蒙特利尔电力服务委员会	被迫重建 IT 基础设施
9 月	西班牙塞维利亚市议会	要求的 150 万美元赎金。该事件影响了广泛的城市服务 IT 基础设施。
10 月	全球知名 IT 供应商 CDW	窃取数据索要八千万赎金
11 月	美国波音公司	窃取并公布了 43GB 内部数据

时间	受害者	影响
12 月	跨国零售商 Aldo	影响了特许经营合作伙伴的系统

2) Clop

Clop（Cl0p）于 2019 年 2 月出现，从 CryptoMix 勒索软件变体演变而来，安全研究人员认为与出于经济动机的威胁行为者 FIN11（也称为 TA505 和 Snakefly）有关。部署的 Clop 勒索软件变体在其加密的文件中附加新的文件扩展名。典型的文件扩展名包括“.Clop”，“.Cl0p”，“.C_L_O_P”，“.C_I_0P”等。

Clop 勒索软件组织在 2023 年 1 月至 6 月期间攻击了多个行业领域，最多的是商业服务，其次是软件和金融。目标地区主要是美国、加拿大和英国。亚洲、拉丁美洲、中东和非洲的企业也受到过攻击。

2023 年，Clop 勒索团伙利用多个漏洞入侵了全球众多组织，造成了严重的影响。1 月下旬，Clop 勒索软件组织利用 GoAnywhere0day 漏洞（现已编为 CVE-2023-0669）发起攻击，攻击者可以利用此漏洞在未修补的 GoAnywhere MFT 实例上执行远程代码，让管理控制台暴露在互联网上，被任意访问。Clop 团伙声称已经可以通过受害者的网络横向移动，并部署勒索软件载荷来加密系统，但他们决定不加密系统，只窃取存储在受攻击的 GoAnywhere MFT 服务器上的文件。该组织在其泄密站点上声称在 10 天内利用该漏洞攻击了 130 多家公司。

4 月，Clop 团伙利用了两个 PaperCut 漏洞 CVE-2023-27350 和 CVE

-2023-27351。Clop 利用该漏洞初步访问公司网络，部署 TrueBot 恶意软件和 Cobalt Strike，同时使用 MegaSync 文件共享应用程序窃取数据。

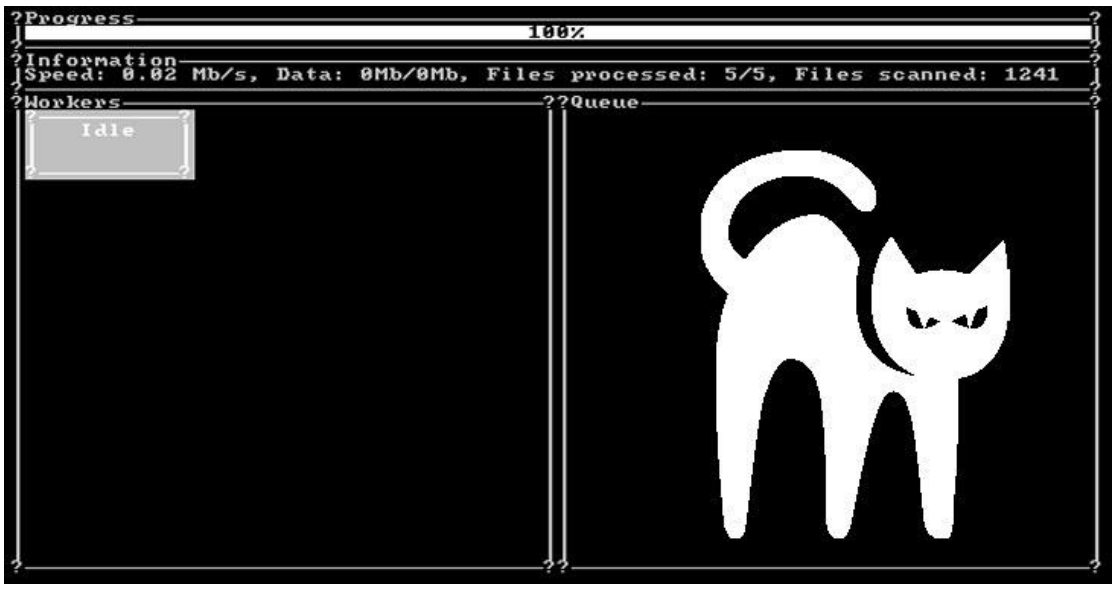
6 月，Clop 利用 MOVEit 平台中的 SQL 注入零日漏洞 CVE-2023-34362 进行攻击。攻击者利用 MOVEit 漏洞在服务器上释放特制的 webshell，从而允许他们检索存储在服务器上的文件列表、下载文件并窃取已配置的 Azure Blob 存储容器的凭证或密钥。利用 MOVEit 安全文件传输平台中的 0day 漏洞进行的数据盗窃攻击预计将影响全球数百家公司。Clop 勒索团伙很可能从 MOVEit 活动中赚取 7500 万至 1 亿美元。

时间	受害者	影响
1 月	纽约市酒吧	窃取了 1.8TB 数据。
3 月	澳大利亚赌博和娱乐公司皇冠度假村	声称从网络窃取了数据。
	云管理巨头 Rubrik	内部销售信息被窃取，包括客户和合作伙伴名称、业务联系人以及来自分销商的采购订单。
	Hatch Bank	窃取了 14 万个客户的社会安全号码。
6 月	雅诗兰黛	声称已经窃取了超过 131GB 的数据。
	西门子能源	声称窃取了数据。
	施耐德电气	声称窃取了数据。

时间	受害者	影响
7 月	丰田纺织欧洲有限公司	声称窃取了数据。
11 月	北卡罗来纳中央大学	在线课程受到影响暂停，可能泄露了敏感文件和信息。

3) BlackCat(ALPHV)

BlackCat 新型勒索软件于 2021 年 11 月出现，也称为 ALPHV，是第一个基于 Rust 编写的多平台勒索软件，支持在 Windows、Linux 操作系统（Debian、Ubuntu、ReadyNAS、Synology）和 VMWareESXi 系统上执行。BlackCat 使用三重勒索策略，在加密设备之前窃取数据，并且会发起 DDoS 攻击以威胁受害者，直到受害者支付赎金。



BlackCat 在勒索软件匿名市场（RAMP）和其他俄语黑客论坛发布广告，积极招募新的附属机构加入其团伙。BlackCat 团伙为其关联公司提供

非常可观的分成，高达受害者已支付赎金的 90%，远高于其他 RaaS 团伙为附属公司提供的报酬。攻击者在其附属计划的规则中规定，BlackCat 勒索软件不能用于攻击以下组织：

- 独立国家联合体或邻国
- 医疗保健行业或与之相关的组织
- 慈善或非营利组织
- 建议附属机构避免攻击教育和政府部门

BlackCat 在攻击中使用 ExMatter 工具自动执行数据泄露操作。ExMatter 是一种能够自我删除的自定义恶意软件,旨在从多个选定目录中窃取特定文件类型，并将其上传到攻击者控制的服务器，然后在受害者的网络上部署 BlackCat 勒索软件。此外，勒索团伙部署了一种名为“Eamfo”的新恶意软件，该软件明确针对存储在 Veeam 备份中的凭据。该软件通常用于存储域控制器和云服务的凭据，以便勒索软件攻击者可以利用它们进行更深层次的渗透和横向移动。

2023 年 2 月，BlackCat 组织发布了其勒索软件的新版本“Sphynx”，具有升级功能，旨在阻止防御措施。Sphynx 与以前的变体有显著的不同之处。例如，命令行参数已重新设计，以前的变体使用 -access-token 参数来执行。更新后的勒索软件删除了该参数，并添加了一组更复杂的参数。这使得检测变得更加困难。

BlackCat 在 2023 年是最活跃勒索软件家族之一，对全球组织造成严重破坏，其附属公司最近的攻击包括针对医疗保健、政府、教育、制造和

酒店业等组织。据美国联邦调查局 (FBI)称，截至 2023 年 9 月，ALPHV/ BlackCat 勒索软件团伙已向全球 1000 多名受害者支付了超过 3 亿美元的赎金。

不过在 2023 年 12 月 7 日至 12 日，BlackCat 遭受了为期 5 天的中断，其所有基础设施都处于离线状态，包括数据泄露和谈判站点。虽然该组织声称是由于硬件原因中断，但外界确认是受到执法部门的影响。12 月 19 日，美国司法部宣布对 Blackcat 勒索软件组织发起破坏活动，摧毁了相关基础设施，FBI 向全球 500 多名受害者提供解密工具。此外，顶级勒索组织 LockBit 试图招揽 BlackCat 旗下的附属机构，称如果他们有被盗数据的备份，他们可以利用 LockBit 的数据泄露网站和谈判小组继续勒索受害者。此次事件很可能对 BlackCat 造成无法挽回的损失，丢失大量附属机构的信任。

时间	受害者	影响
1 月	印度私人国防承包商 Solar Industries Limited	声称已窃取了 2TB 的数据。
	巴西公立教育机构 Instituto Federal Do Pará (IFPA)	BlackCat 发布了包含文件夹目录的屏幕截图。
2 月	美国快餐连锁店 Five	窃取了 2021 年的银行对账单、国际工资数据、招聘信息和审计信

时间	受害者	影响
	Guys	息以及其他类型的数据。
	爱尔兰蒙斯特理工大学(MTU)	属于该大学的数据已出现在暗网上。
	Wawasee 社区学校公司	勒索软件组织在其泄漏网站上泄露了 9.78GB 的文件。
	华盛顿州皮尔斯县莱克伍德市	超过 250GB 的数据被盗。
	美国天然气和石油生产商 Encino Energy	该勒索软件组织泄露了属于该组织的 400GB 数据。
3 月	孟买的制药公司 Sun Pharma	导致某些文件系统遭到破坏，影响了公司和个人数据。
	安全摄像头公司 Ring	声称窃取了数据。
4 月	西部数据	勒索 8 位数的赎金。
	肯尼亚 Naivas 连锁超市	声称窃取了超过 1TB 的数据。
	储罐公司 Vopack	边佳兰独立码头站点受到影响。
5 月	澳大利亚商业律师事务所 HWL Ebsworth	攻击期间 4TB 数据被泄露。被盗信息包括身份证、财务报告、会

时间	受害者	影响
		计数据、客户文件和信用卡详细信息。
	加拿大多元化软件公司 Constellation Software	声称窃取了超过 1TB 的文件。
	埃森医学协会	声称在攻击期间窃取了总计 2.6TB 的数据。
6 月	澳大利亚债券经纪商 FIIG Securities	385BG 数据被盗。
	法国企业 Automatic Systems	发布了数百个被盗数据样本，包括保密协议到护照副本。
	英国 Barts Health NHS Trust	声称窃取了超过 7TB 的敏感数据。
7 月	孟加拉国 Krishi 银行	获取了超过 170GB 敏感数据并使其运营瘫痪。
8 月	日本手表制造商 Seiko	声称窃取的敏感数据，包括护照扫描和新手表项目文件等。
9 月	米高梅酒店集团	宣称窃取了数 TB 的数据，并保持对米高梅部分基础设施的访问权限

时间	受害者	影响
10 月	ITM 和 ATM 解决方案提供商 QSI Inc	声称窃取了 5TB 数据
11 月	美国医疗保健巨头 Henry Schein	窃取了数十 TB 的数据，包括工资数据和股东信息
12 月	著名商业咨询和服务公司 Advantage Group International	在暗网上泄露 8TB 的数据，数据内容包含可口可乐、宝洁、百事可乐等客户的海量数据集，自世界顶级公司的庞大联系人名单，所有员工的浏览器密码等信息。
	全球知名服装公司 VF Corp	向美国 SEC（证券交易委员会）提交的表格披露中，VF 通报了 2023 年 12 月 13 日发生的勒索攻击，之后 BlackCat 将其列为受害者。

4) Royal

Royal 最初被称为“Zeon”，于 2022 年 1 月启动运营，被认为是 Conti 网络犯罪集团的一个分支，在 Conti 关闭其业务后崛起。在早期的活动中，Royal 部署了 BlackCat 的加密器，后来转向使用自己的加密器，该加密器会发出类似于 Conti 的勒索信息。

Royal 是 2022 年第四季度最活跃的勒索软件组织之一，针对众多的关键基础设施部门，包括但不限于制造业、通信、医疗保健以及教育等行业。Royal 的赎金要求从 25 万美元到超过 200 万美元不等。大多数 Royal 勒索软件受害者组织都是中小型企业，只有小部分是大型企业。

Royal 团伙使用回调钓鱼邮件进行针对性攻击，使用社会工程学手段，引诱受害者安装远程软件，以此获得初始访问的权限。在进入系统后，部署 CobaltStrike 进行持久性，获取凭据，利用 Netscan 和 PsExec 工具进行横向传播，窃取数据，并最终加密设备。加密文件时，Royal 加密器会将.royal 扩展名附加到加密文件的文件名中。赎金票据中包含一个指向受害者私人 Tor 协商页面的链接，受害者可以在其中进行谈判。2023 年 2 月，Royal 发布了针对 Linux 和 VMwareESXi 系统的勒索软件变种。

在 2023 年 7 月以后，Royal 并没有新增发布受害者，疑似已经进行品牌重塑。

时间	受害者	影响
1 月	亚利桑那州图森联合学区	关闭了该地区的互联网和网络服务，迫使学校离线工作。
3 月	英国怀蒙德姆学院	导致工作人员无法使用计算机资源，学生也无法访问文件。
4 月	克拉克县医院	包括 PII 在内的个人信息和一些健康信息可能已被未经授权的第三方获取。

时间	受害者	影响
5 月	蒙大拿州立大学	窃取了超过 100GB 的数据。
	达拉斯市	关闭了一些 IT 系统，包括警察局在内的多个职能领域受到影响。
	俄勒冈州南部的库里县	导致无法访问任何数字信息。
7 月	布伦特里公立学校	窃取了大量内部数据

5) BianLian

BianLian 勒索软件于 2022 年 6 月首次出现，其最初采用双重勒索模式，在从受害者网络中窃取私人数据后加密系统，然后威胁要泄露文件和数据。然而，自 2023 年 1 月以来，当 Avast 发布了勒索软件的解密器时，该组织转向基于数据盗窃的勒索，而无需加密系统。

BianLian 使用远程桌面协议（RDP）凭据入侵系统，这些凭据可能是从初始访问代理处购买的或通过网络钓鱼获得，采用 Go 编写的自定义后门，商业远程访问工具以及命令行和脚本进行网络侦察。最后一个阶段包括通过文件传输协议（FTP）、Rclone 工具或 Mega 文件托管服务泄露受害者数据。

BianLian 主要针对金融机构、医疗保健、制造、教育、娱乐和能源行业，根据分析受害者所在国家和地区的统计数据，主要针对美国、英国和

澳大利亚的组织和机构。

时间	受害者	影响
1 月	韦恩斯伯勒地方政府	窃取了 350GB 的文件，据称其中包括文件服务器数据、来自内部警察局文件服务器的文件、公共关系以及各种业务文件、笔记和手册。
2 月	Retina & Vitreous	一些个人和受保护的健康信息可能在未经授权的情况下被获取。
4 月	克拉克县医院	包括 PII 在内的个人信息和一些健康信息可能已被未经授权的第三方获取。
5 月	默弗里斯伯勒医疗诊所	窃取了 250GB 的文件，包括人力资源文档、财务数据、业务数据、法律案例和 SQL 数据库。
	巴塞尔教育部	窃取了约 1.2TB 的数据。
7 月	美国柯林斯航空航天公司	超过 20GB 的敏感个人数据泄露
9 月	救助儿童会	窃取了 6.8TB 的数据
10 月	加拿大航空	窃取了 210GB 数据。
11 月	印度国家证券交易所	声称获取了该公司超过 3TB 的

时间	受害者	影响
	信息技术 (NSEIT)	数据
12 月	乳制品蛋白制造商 AMCO Proteins	泄露数据大小为 4TB，包含个人资料、会计数据、财务数据、合同数据、SQL 备份等

6) BlackBasta

BlackBasta 是在 2022 年 4 月新出现的勒索团伙，由于具备在短时间内迅速执行多次攻击的能力，因此 BlackBasta 在出现不久后很快就恶名远扬。

BlackBasta 在短时间内产生的影响表明该组织具有一套经过实践且有效的战术、技术和程序 (TTP)，而其数据泄露博客、支付站点、恢复门户、受害者通信以及谈判方法与 Conti 团伙存在相似之处，因此被认为是 Conti 团伙的分支。

BlackBasta 的攻击一般从通过网络钓鱼攻击获得的初始访问权限开始，典型的攻击可能始于包含 zip 文件中恶意文档的电子邮件，提取后，文档会安装 Qakbot 银行木马以创建后门访问并部署 SystemBC，从而建立与命令和控制服务器的加密连接。之后安装 CobaltStrike 用于网络侦察和分发其他工具。

BlackBasta 的大部分受害者位于北美，其次是欧洲和亚太地区。受害者行业包括建筑、服务、零售、保险和制造业等。BlackBasta 勒索软件团伙在过去一年半的时间里从 90 多名受害者那里获得了超过 1.07 亿美元的

赎金。

时间	受害者	影响
2 月	KFI Engineers	1.1TB 的数据被盗，最终支付 30 万美元。
3 月	英国放大器和音箱制造商 Marshall	被添加到 BlackBasta 的泄露网站中。
4 月	加拿大目录出版商黄页集团	泄露的信息包括与员工有关的身份证件和税务文件、销售和购买协议以及公司财务信息。
5 月	Buckley King LPA 律师事务所	Black Basta 称有 110GB 的文件。最终受害者同意支付 15 万美元。
	德国汽车和武器制造商莱茵金属公司	窃取了保密协议、协议、技术原理图、护照扫描和采购订单。
10 月	多伦多公共图书馆	攻击导致多伦多公共图书馆停电

7) Medusa

Medusa 勒索于 2021 年 6 月开始，但活动相对较少，受害者很少，然而，在 2023 年，勒索软件团伙的活动却持续有所增加，并推出 tor 博客，用于曝光拒绝支付赎金的受害者的数据。

值得注意的是，许多恶意软件家族的名称都为美杜莎，包括具有勒索软件功能的基于 Mirai 的僵尸网络、美杜莎 Android 恶意软件和广为人知的 MedusaLocker 勒索软件。Medusa 勒索和 MedusaLocker 勒索软件并不是同一个勒索家族。MedusaLocker 于 2019 年作为勒索软件即服务推出，拥有众多附属公司，通常名为 How_to_back_files.html 的勒索信，以及各种加密文件的文件扩展名。

Medusa 勒索软件行动于 2021 年 6 月左右启动，使用 AES 和 RSA 加密算法对文件进行加密，加密后的文件扩展名.MEDUSA，并在目录下创建勒索信文件，名称为!!!READ_ME_MEDUSA!!!.txt。

时间	受害者	影响
2 月	汤加通信公司(TCC)	连接新客户、交付账单和管理客户查询的流程受到影响。
3 月	Bishop Luffa 学校	被盗数据包含教职员工、学生和家长的个人详细信息。
	田纳西州立大学	导致该大学的 IT 系统暂时无法

时间	受害者	影响
		访问。
4 月	Uniondale Union Free School District	网站上发布的文件包括学生的个人信息以及人事信息。
5 月	意大利自来水供应商 Alto Calore Servizi s pA	被盗数据的样本包括客户数据、合同、报告、扩展文档等。
	悉尼王妃玛丽癌症中心	10,000 多个文件被窃取。
6 月	阿根廷国家安全委员会	窃取了 1.5TB 的财务信息，并索要 50 万美元的赎金
9 月	菲律宾健康保险公司	近 750GB 信息被盗
10 月	德国丰田金融服务公司	窃取敏感数据要求 800 万美元的赎金
11 月	加拿大心理协会 (CPA)	窃取敏感数据要求 20 万美元的赎金

8) 8Base

8Base 勒索软件团伙于 2022 年 3 月首次出现，开始时保持相对安静，几乎没有明显的攻击，但在 2023 年 5 月后勒索活动激增，针对各行各业的许多公司并进行双重勒索，截至 12 月，已经有 200 多个组织遭受攻击。

通过网络钓鱼电子邮件或使用初始访问代理 (IAB)，主要目标行业包括但不限于商业服务、金融、制造和信息技术。

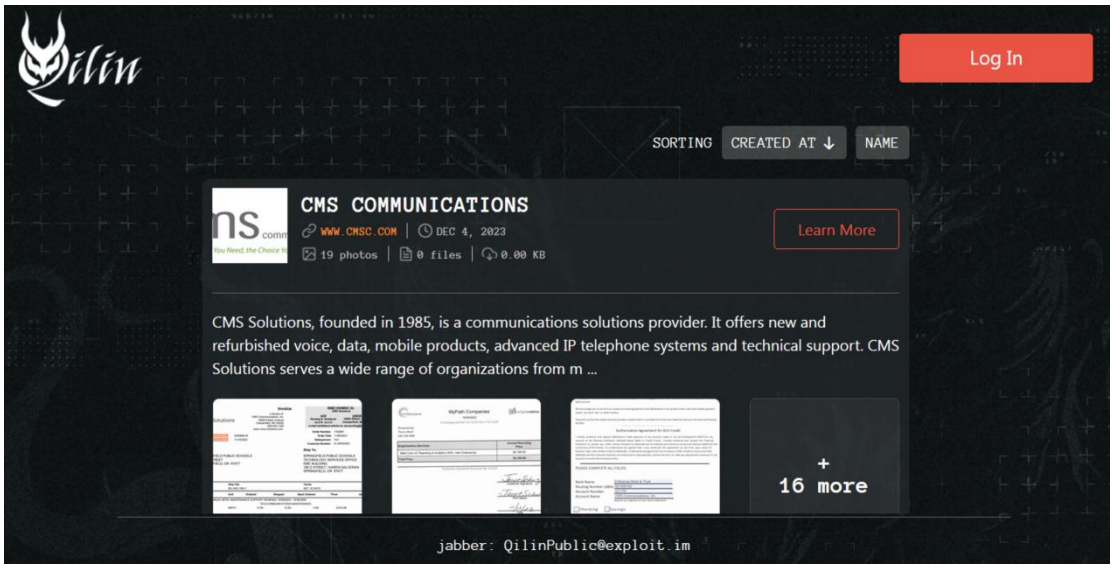
从 8Base 组织的运营成熟度分析，该组织并不像一个全新的勒索组织，VMware 的研究人员认为 8Base 与 Phobos、RansomHouse 这 2 个勒索团伙有着紧密关联。从勒索信和泄露网站分析，8Base 很有可能是 RansomHouse 的品牌重塑或者分支。此外，研究人员在搜索 8Base 使用的勒索软件样本时找到了“.8base”文件扩展名的 Phobos 样本，不排除 8Base 使用定制版本的 Phobosv2.9.1 勒索软件的可能性。

时间	受害者	影响
6 月	堪萨斯医疗中心	个人文件、身份证、健康保险信息、患者 PII、员工信息、内部文件、账户信息和其他财务文件被泄露。
	ClearMedi Health	被盗文件包括个人文档、患者数

时间	受害者	影响
		据、员工信息、财务文件等。
7 月	Anesco 能源公司	声称可以访问个人信件、财务报表、包含机密信息的文件等
9 月	福特经销商 COVESA	窃取敏感信息
11 月	西班牙 Ingenier í a F ULCRUM 公司	窃取敏感信息
12 月	西班牙雷乌斯市市政资本公司	泄露数据包含发票、收据、会计凭证、个人资料、证书、雇佣合同、大量机密信息、保密协议等，导致停车应用程序和市政停车网络的出入口发生故障

9) Qilin

Qilin 又名 Agenda 勒索，Windows 版本最早于 2022 年 8 月中旬被发现，2023 年重命名为 Qilin，8 月，Group-ib 公司揭露了 Qilin 勒索的 Raa S 策略，并表明 Qilin 拥有构建器可以生成针对 Windows 和 ESXi 的样本。在 2023 年 10 月底，安恒研究院猎影实验室捕获到 VT 检测数为 0 的 Qili n 勒索 Linux/ESXi 变体。该变体运行时允许配置多个命令行参数来启用和禁用特定功能，例如快照删除、进程终止等。



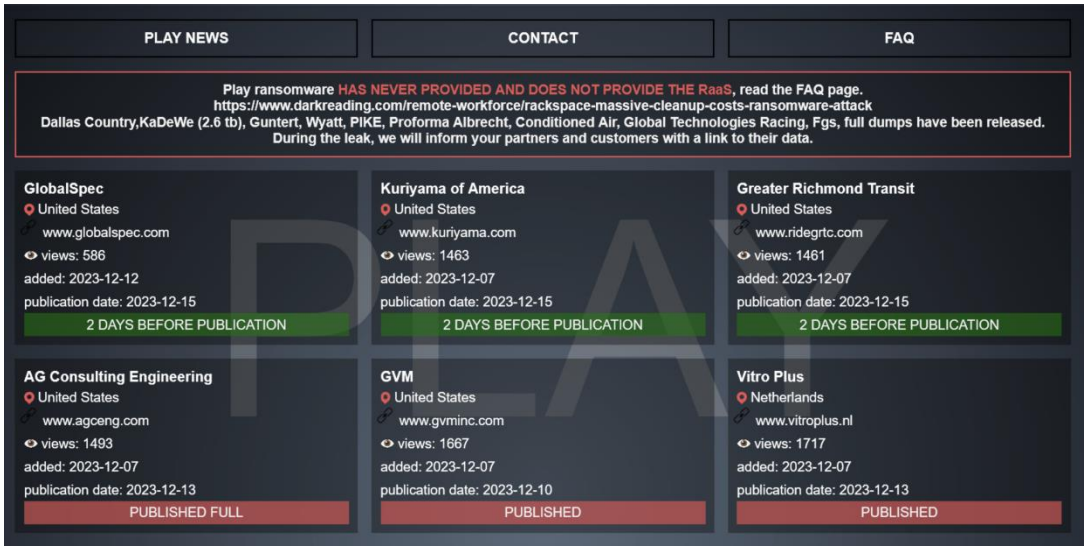
时间	受害者	影响
3 月	荷兰的医疗服务提供商 Attent Zorg Behandling	其网络遭遇未经授权的访问，导致其系统、电子邮件和电话无法访问。
5 月	哥伦比亚 Emtelco 公司	窃取了数百 GB 的数据。包括所有大客户（企业）数据、非公开文件等。
8 月	电池制造商 Thonburi Energy Storage Systems	针对 TESM 网络攻击的数据转储，窃取了大量内部数据。
11 月	汽车零件供应商延锋	影响多家汽车厂商的声称，直接迫使 Stellantis 汽车公司停止其北美工厂的生产。

时间	受害者	影响
12 月	美国内华达州神经病学中心	窃取了大量敏感数据

10)Play

Play 勒索软件于 2022 年 6 月被发现，当时受害者在 BleepingComputer 论坛中披露攻击。最初专注于拉丁美洲的组织，尤其是巴西，但之后很快就扩大了目标范围，受害者逐渐转移到了北美和欧洲地区。泄漏站点数据表明，IT 行业是 Play 攻击的最大目标，其次是运输，其他受影响的组织包括建筑和材料行业的组织以及政府实体等。

Play 勒索软件通常通过有效账户（包括虚拟专用网络（VPN）账户，而不仅仅是域和本地账户）实现初始访问，这些账户已在多个平台上重复使用、以前暴露或通过非法手段获得。为了在目标系统中建立立足点，他们还使用公开的远程桌面协议服务器。使用 Mimikatz 从内存中提取高特权凭据，然后将账户添加到特权组，包括域管理员组。为了躲避防护软件的检测，使用多种工具包括 ProcessHacker、GMER、IOBit 和 PowerTool 等禁用反恶意软件。它使用 Windows 内置工具 wevtutil 或批处理脚本来删除其日志信息来清除痕迹。Play 勒索软件可能会使用不同的工具在受害者的系统中横向移动，例如 CobaltStrike、SMBbeacon、Mimikatz 等。



Play 勒索软件组织是最活跃的团伙之一，以针对 MicrosoftExchange 漏洞获得远程代码执行并渗透受害者网络而闻名。使用许多工具和漏洞来增强其武器库，包括漏洞 ProxyNotShell，OWASSRF 和 MicrosoftExchangeServer 远程代码执行等。今年，它还开始使用新工具，如 Grixba，这是一种网络扫描工具，用于枚举域中的所有用户和计算机。以及开源 VSS 管理工具 AlphaVSS，它提供了一个用于与 VSS 交互的高级接口。该库通过提供一组受控 API 使.NET 程序更容易与 VSS 交互。开发人员可以使用这些 API 生成、管理和删除卷影副本，以及访问有关现有卷影副本的信息，例如大小和状态。

时间	受害者	影响
1 月	英国最大的汽车经销商网络阿诺德·克拉克 (Arnold Clark)	Play 勒索软件组织在网上发布了 15GB 的客户数据。
2 月	网络硬件制造商 A10	勒索团伙短暂获得了共享驱动器

时间	受害者	影响
	Networks	的访问权限以及与人力资源、财务和法律职能相关的数据。
3 月	荷兰海运物流公司 Royal Dirkzwager	发布了属于该公司的 5GB 数据。
	法国宝马	被盗数据包括私人和个人机密数据、合同、财务信息和客户文件。
4 月	萨克森州瓦莱州市	被盗数据包括机密、私人和个人数据、财务、人力资源、合同和员工文件。
5 月	马萨诸塞州洛厄尔市	该市计算机系统陷入混乱，电话线、电子邮件和其他系统因攻击而瘫痪。
	德国外贸机构 GTAI	攻击影响了其网站、电子邮件和电话服务。
6 月	瑞士 IT 公司 Xplain	使许多政府部门的数据面临风险。
	西班牙主要银行 Globalcaja	窃取了私人和个人机密数据，包括客户和员工文件、护照和合同。
	法国橄榄球联合会	邮件服务器受到严重攻击。

2. 新团伙

2023 年勒索攻击迅猛，除了往年活跃的勒索团伙，不断陆续有新的勒索家族出现，来势汹汹。据统计，今年最活跃的前 20 名勒索团伙中半数为新型勒索，侧面表现出勒索系统生态的进一步完善和不断发展的态势。

有些新型勒索团伙的影响力惊人，例如 MalasLocker、Akira，短时间内便拥有了众多的受害者。2023 年，针对 Linux 和 VMware ESXi 架构系统的勒索家族和变体也明显增加。一方面，出于利润最大化的目的，勒索软件团伙越来越多地开发 Linux 加密器来加密 VMware ESXi 服务器，另一方面，由于 Babuk 勒索组织泄露出的源码，这给众多勒索团伙提供了开发模板和思路，不断有类 Babuk 的新勒索软件涌现，尤其助长了以 Vmware ESXi 为目标的勒索软件开发。例如 Rorschach、RTM Locker、Cylance、Buhti、RaGroup、Rhysida、Abyss Locker 等。以下简要介绍部分今年出现的新型勒索团伙。

1) Cylance

2023 年 3 月，安恒研究院猎影实验室在日常监测运营中捕获了一种新型勒索软件 Cylance Ransomware。勒索软件执行后，快速加密文件并添加扩展名.Cylance，在目录下放置勒索信文件 CYLANCE_README.txt，并在信中自称 Cylance Ransomware。

Cylance 勒索信格式与 REvil 勒索组织高度相似，并都采用 Curve25519 和 salsa20 加密算法组合加密文件的方式，拥有快速加密和全加密两种加

密模式。但在整体功能上有所差异，例如参数配置更为丰富、针对数据库等特殊文件使用了间歇性加密模式，对于静态字符串没有 REvil 复杂的混淆加密处理，不涉及地区豁免等。

在加密策略上，Cylance 勒索默认无参数采用快速加密，即文件至多加密 1MB，不过特殊的文件类型采用间歇性加密，这类文件主要是数据库和压缩文件，攻击者认为此类文件具有重要的数据价值，所以在勒索中往往重点关注。

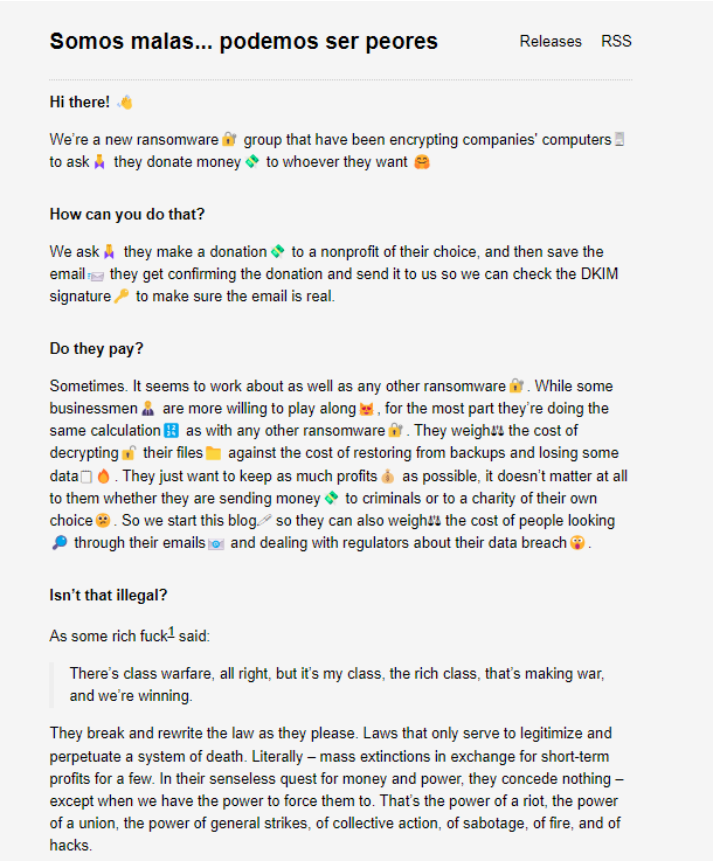
随后不久，Cylance Ransomware 的 Linux 变体样本被海外安全厂商发现，根据安全人员分析，Linux 变体的 Cylance 勒索基于已经泄露的 Babuk 源码改造开发而成，以 VMware ESXi 服务器为目标。

2) MalasLocker

MalasLocker 是一款新型勒索软件，通过入侵 Zimbra 服务器来窃取邮件并加密文件。和一般的勒索组织不同，攻击者并没有要求目标支付赎金，而是要求受害者向指定的非营利慈善机构捐款，以提供解密工具并防止受害者的数据泄露。

勒索团伙的活动始于 3 月底，针对全球中小型公司。MalasLocker 使用一种由 Google 的 Filippo Valsorda 开发的名为“Age”的加密工具。该工具使用 Curve25519、ChaChar20-Poly1305 和 HMAC-SHA256 加密算法。在加密电子邮件时，MalasLocker 不会在文件名附加额外的扩展名，但在每个加密文件的末尾都附加了一个“此文件已加密，请查看 README.txt

了解解密说明”的信息。



Somos malas... podemos ser peores Releases RSS

Hi there!

We're a new ransomware group that have been encrypting companies' computers to ask they donate money to whoever they want

How can you do that?

We ask they make a donation to a nonprofit of their choice, and then save the email they get confirming the donation and send it to us so we can check the DKIM signature to make sure the email is real.

Do they pay?

Sometimes. It seems to work about as well as any other ransomware. While some businessmen are more willing to play along, for the most part they're doing the same calculation as with any other ransomware. They weigh the cost of decrypting their files against the cost of restoring from backups and losing some data. They just want to keep as much profits as possible, it doesn't matter at all to them whether they are sending money to criminals or to a charity of their own choice. So we start this blog so they can also weigh the cost of people looking through their emails and dealing with regulators about their data breach.

Isn't that illegal?

As some rich fuck[1] said:

> There's class warfare, all right, but it's my class, the rich class, that's making war, and we're winning.

They break and rewrite the law as they please. Laws that only serve to legitimize and perpetuate a system of death. Literally – mass extinctions in exchange for short-term profits for a few. In their senseless quest for money and power, they concede nothing – except when we have the power to force them to. That's the power of a riot, the power of a union, the power of general strikes, of collective action, of sabotage, of fire, and of hacks.

MalasLocker 的主页

MalasLocker 勒索软件可能利用 CVE-2022-27924（Zimbra memcache 命令注入）、CVE-2022-27925（Zimbra 管理目录遍历）、CVE-2022-30333（UnRAR Linux/UNIX 目录遍历）和 CVE-2022-37042（Zimbra 身份验证绕过，远程代码执行）相关的漏洞。

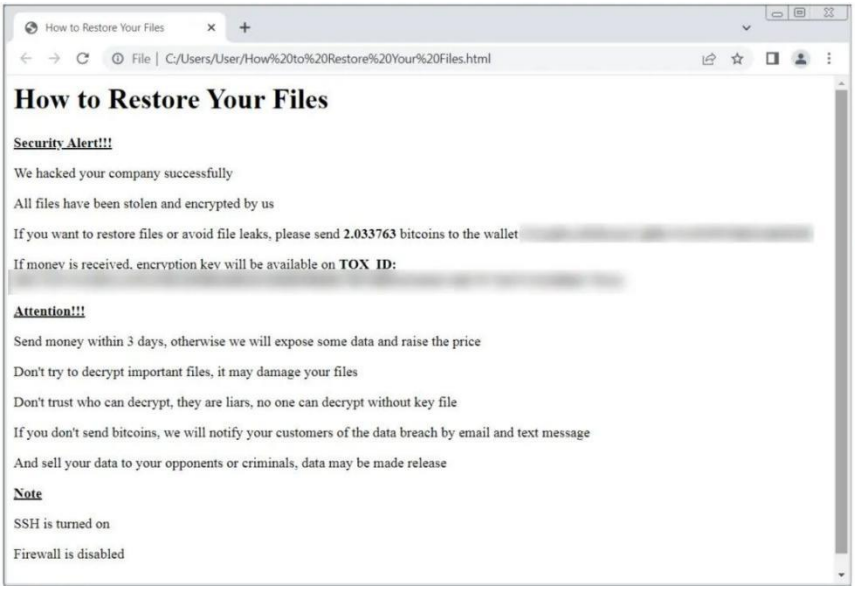
据统计，MalasLocker 出现后的一个季度里受害者数量达到了 171 位，主要针对意大利、俄罗斯和美国的公司。在目标行业上， MalasLocker 主要针对商业服务、制造业和零售业。

3) ESXiArgs

2023 年 2 月 3 日，针对 VMwareESXi 架构的新勒索软件 ESXiArgs 迅速席卷网络。ESXiArgs 使用 2 年前的 ESXi 远程代码执行漏洞（CVE-2021-21974）对未修补的 ESXi 服务器进行攻击，加密了全球 3000 多台暴露在互联网上的 VMwareESXi 服务器。该漏洞是由 OpenSLP 服务中的堆溢出问题引起的，可以被未经身份验证的攻击者远程利用。容易受到 ESXi Args 攻击的 VMware ESXi 版本包括：

- 6.7 之前的版本 6.x。
- ESXi70U1c-17325551 之前的版本 7.x。
- ESXi670-202102401-SG 之前的版本 6.7.x。
- ESXi650-202102101-SG 之前的版本 6.5.x。

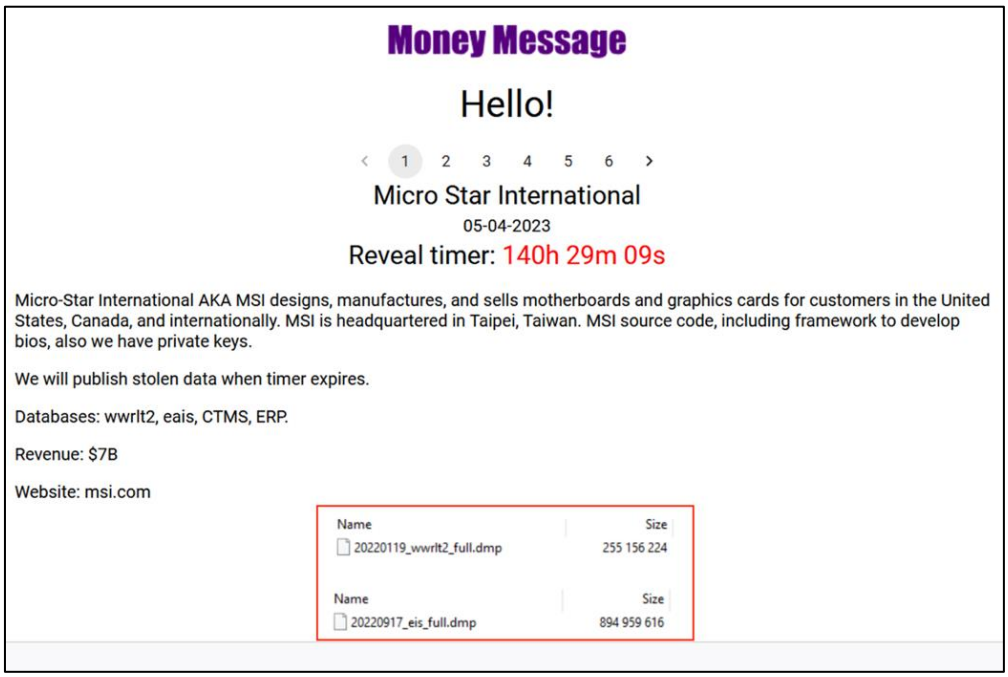
勒索软件在受感染的 ESXi 服务器上使用.vmxf、.vmx、.vmdk、.vmsd 和 .nvram 扩展名加密文件，并为每个包含元数据（可能需要解密）的加密文档创建一个.args 文件。对于每个找到的文件，脚本将在同一文件夹中创建一个 [file_name].args 文件，其中包含计算出的大小步长“1”和文件大小（例如，server.vmx 将有一个关联的 server.vmx.args 文件）。加密后，脚本将用赎金票据替换 ESXi index.html 文件和服务器的 motd 文件。最后，该脚本执行一些清理，删除疑似安装到/store/packages/vmtools.py 的后门。



ESXiArgs 赎金票据

4) Money_Message

2023 年 3 月 28 日，一款名为 Money_Message 的勒索软件大肆攻击全球知名企业，窃取数据并索要数百万美元的赎金。该勒索软件采用定向攻击的方式，目标主要针对大型企业实施勒索攻击，窃取和加密数据，包括孟加拉国家航空公司(BimanAirlines)，世界知名的计算机硬件提供商微星国际（MSI）等企业。



MoneyMessage 勒索采用 ECDH 和 ChaCha20 组合的方式加密受害系统上的文件，并嵌入 json 格式的配置文件来灵活设置加密策略。该种组合的加密方案若无对应的密钥，则无法解密。此外，MoneyMessage 勒索还通过内置的账户密码尝试登陆远程主机，并在内网进行横向感染，扩大勒索危害。该勒索加密执行结束后不改变加密文件的后缀名，但创建一个名为 money_message.log 的勒索信文件用于提醒受害者，在勒索信内容中包含了该组织的暗网博客链接，表示不支付赎金则在其数据泄露网站公布窃取的数据。

5) Akira

Akira 是 2023 年 3 月出现的新勒索软件，6 月底，安全研究人员发现 Akira 勒索开发出 Linux 变体样本，针对 VMware ESXi 服务器。截至 6 月，Akira 已经对 60 多家公司进行了攻击。这些公司涉及各个行业，包括教育、

金融、房地产、制造业和咨询等。

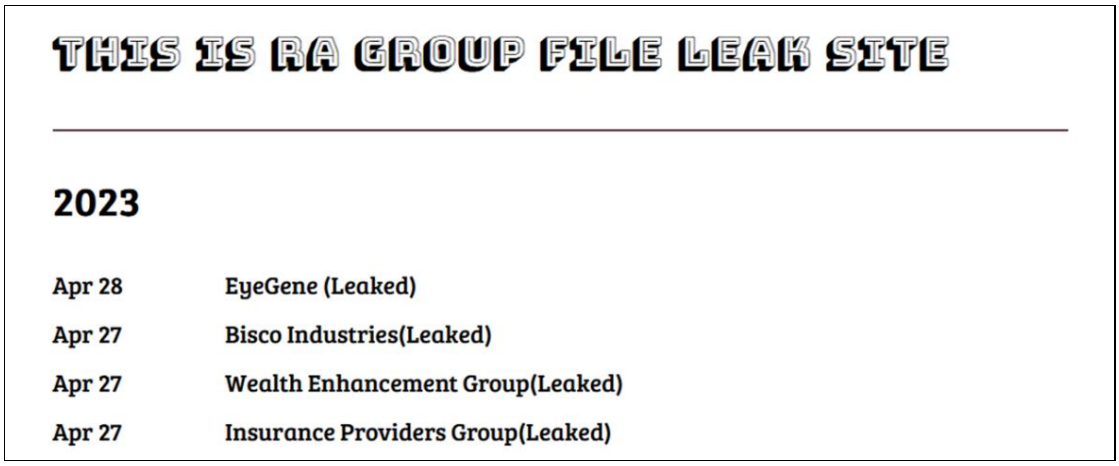
Akira 执行时，通过运行 PowerShell 命令删除设备上的 Windows 卷影副本。加密文件时，将.akira 扩展名附加到文件名中，释放名为 akira_readme.txt 的赎金记录，其中包括有关指向 Akira 数据泄露站点和谈判站点的链接。每个受害者都有一个唯一的协商密码，该密码输入到威胁参与者的 Tor 站点中。该谈判站点仅包含一个聊天系统，受害者可以使用该系统与勒索软件团伙进行谈判。

2023 年 8 月，Akira 勒索软件被发现滥用思科自适应安全设备(ASA)和 Firepower 威胁防御(FTD)产品，对许多组织发起勒索软件攻击，后续思科证实上述产品中存在 CVE-2023-20269 漏洞。在 2023 年，遭受 Akira 勒索攻击的受害者已经超过 150 名。此前安全研究人员称 AKira 勒索与消失的 Conti 之间存在关联，从勒索攻击规模也可以看出该勒索的非一般的技

术成熟度和运营能力。

6) RaGroup

RaGroup 勒索软件在 2023 年 4 月被首次发现，主要针对美国和韩国的制药、保险、财富管理和制造公司发起攻击，在不到一个月的时间里，已经入侵了美国的三个组织和韩国的一个组织。



RaGroup 实施双重勒索，运营着一个数据泄漏站点，若受害者未能在三天内联系，则在泄漏站点公布窃取的数据。该勒索软件基于泄露的 Babuk 勒索源码构建，加密扩展名为.GAGUP，勒索信文件 HowToRestoreYourFiles.txt。

7) BlackSuit

BlackSuit 是 2023 年 5 月出现的新的勒索病毒家族，其拥有 Windows 和 Linux/ESXi 版本的变体，采用 RSA 和 AES 组合加密，加密后更改文件扩展名为.blacksuit，放置勒索信文件 README.BlackSuit.txt。其含多种运行参数，可进入安全模式再进行加密，具有内网扩散功能。

针对 Linux 机器的 x64 VMware ESXi 版本的 BlackSuit 与 Royal 勒索软件之间存在明显相似之处，疑似为 Royal 的品牌重塑。在 2023 年下半年，该勒索目标主要针对于教育和医疗保健行业。例如，2023 年 10 月，Black Suit 攻击了印第安纳州的德堡大学，造成内部数据泄露。

8) INC Ransom

INC Ransom 是 2023 年出现的新型勒索组织，首次发现于 8 月，最早是通过泄漏网站而被发现，第一个在博客出现的受害者是奥地利酒店。加密文件的后缀名为.INC，勒索信文件为 INC-README.txt 和 INC-README.html，并且更改桌面背景图片，以及还会连接打印机打印勒索信文件，进一步警醒受害者支付赎金。其在勒索信中表明自己身份为 INC Ransom，并提供 tor 博客地址，在最后表示如果支付赎金，不仅可以解密，还提供信息安全建设方面的建议。

虽然该组织出现时间较短，但在其博客上已经拥有 40 多名受害者，比如雅马哈汽车菲律宾子公司在 11 月遭到 INC Ransom 的勒索攻击，导致包括重要的员工数据、IP、内部电子邮件以及客户信息数据泄露。

9) Moneybird

Moneybird 于 2023 年 5 月初被披露，疑似为伊朗国家支持的威胁行为者“Agrius”所部署，用来加密"F:\User Shares"文件夹中的敏感文件。至少自 2021 年以来，Agrius 一直在以多个别名积极瞄准以色列和中东地区的实体，同时在破坏性攻击中部署数据擦除器。

Agrius 从“ufile.io”和“easyupload.io”等合法文件托管平台获取 Moneybird 勒索软件可执行文件。启动后，Moneybird 将使用 AES-256 和 GCM 对目标文件进行加密，为每个文件生成唯一的加密密钥，并在其末尾附加加密的元数据。

在已知案例中，Moneybird 勒索软件仅针对“F:\User Shares”，这是企业网络上的一个常见共享文件夹，用于存储企业文档、数据库和其他协作相关文件。这种目标表明，Moneybird 的目的更多是造成业务中断，而不是破坏受影响的计算机。

10)Rhysida

Rhysida 最早在 2023 年 5 月 17 日被披露，其使用双重勒索策略，加密文件后缀为.rhysida。Rhysida 有多种部署方式，包括部署 CobaltStrike 或类似的命令和控制（C2）框架，通过网络钓鱼攻击和在受感染的系统上投放有效载荷来破坏目标的网络。

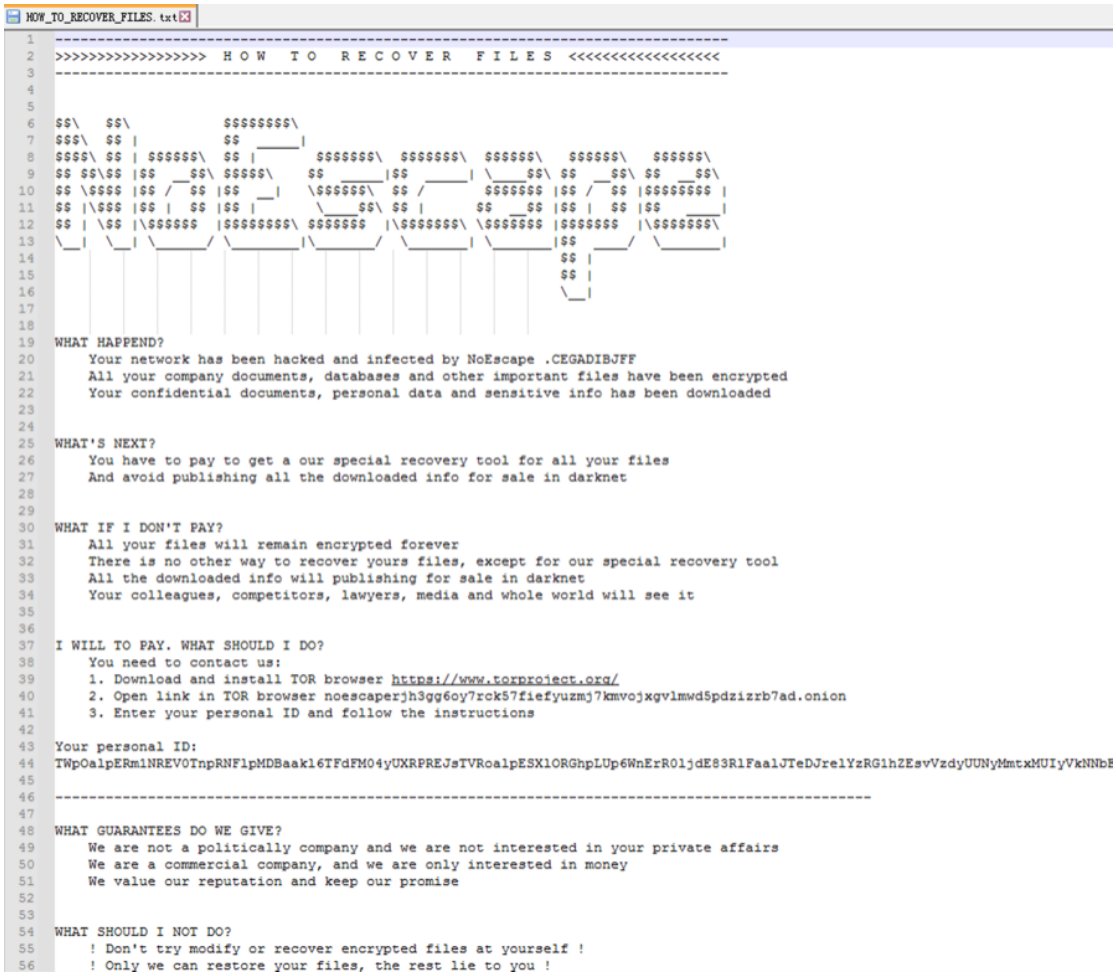
Rhysida 的勒索信以 PDF 文档形式写入目标驱动器上的受影响文件夹中，并更改受害者桌面壁纸。该团伙仅接受 BTC（比特币）付款，并向受害者提供有关在受害者门户上购买和使用 BTC 的信息。在向支付门户提供唯一的 ID 后，系统会提供一份附加表格，允许受害者向攻击者提供更多信息以进行身份验证和详细联系信息。

Rhysida 勒索软件标志

Rhysida 的受害者分布在西欧、北美、南美以及澳大利亚的多个国家，主要攻击教育、政府、制造、技术和托管服务提供商行业。Rhysida 勒索软件团伙将自己描述为一个旨在帮助受害者保护其网络的“网络安全团队”。

11)Noescape

最早于 2023 年 5 月被发现。该组织运行勒索软件即服务模式。开发人员为附属公司创建并提供必要的入侵工具，以执行恶意活动，例如数据泄露和加密器（勒索软件）部署。该组织已经成为多个行业的众多组织的受害者，包括政府、能源、医院和诊所。据称 NoEscape 勒索软件组织与现已解散的 Avaddon 勒索软件组织有关。


HOW_TO_RECOVER_FILES.txt

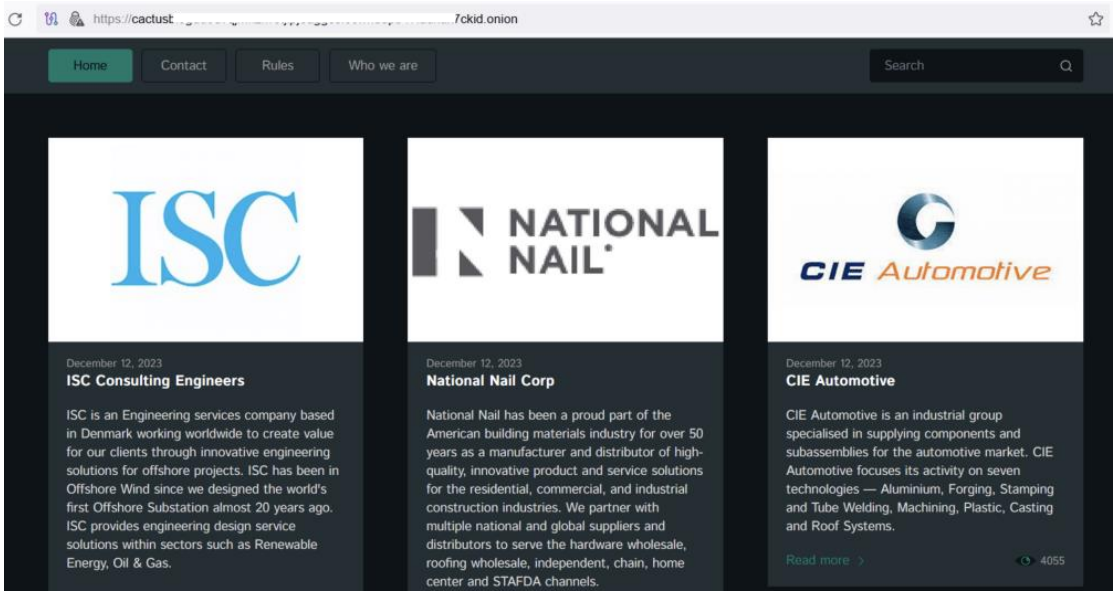
```
>>>>>>>>>>>>>>>>>> H O W   T O   R E C O V E R   F I L E S <<<<<<<<<<<<<<<<<<

WHAT HAPPEND?
    Your network has been hacked and infected by NoEscape .CEGADIBJFF
    All your company documents, databases and other important files have been encrypted
    Your confidential documents, personal data and sensitive info has been downloaded

WHAT'S NEXT?
    You have to pay to get a our special recovery tool for all your files
    And avoid publishing all the downloaded info for sale in darknet

WHAT IF I DON'T PAY?
    All your files will remain encrypted forever
    There is no other way to recover yours files, except for our special recovery tool
    All the downloaded info will publishing for sale in darknet
    Your colleagues, competitors, lawyers, media and whole world will see it

I WILL TO PAY. WHAT SHOULD I DO?
    You need to contact us:
    1. Download and install TOR browser https://www.torproject.org/
    2. Open link in TOR browser noescaperjh3gg6oy7rck57fiefyuzmj7kmvojxgvlmwd5pdzizrb7ad.onion
    3. Enter your personal ID and follow the instructions

Your personal ID:
TWpOalpERm1NREV0TnpRNFlpMDBaak16TFdFM04yUXRPREJsTVRoalpESXlORGhpLUp6WnErR01jdE83R1FaalJTeDJrelYzRG1hZEsvVzdyUUNyMmtxMUIyVkNNbE

WHAT GUARANTEES DO WE GIVE?
    We are not a politically company and we are not interested in your private affairs
    We are a commercial company, and we are only interested in money
    We value our reputation and keep our promise

WHAT SHOULD I NOT DO?
    ! Don't try modify or recover encrypted files at yourself !
    ! Only we can restore your files, the rest lie to you !
```

2023 年，Noescape 勒索组织攻击了 120 多个单位和组织，例如在 2023 年 11 月，入侵了美国一家私人医疗机构 PruittHealth，该组织威胁要公布 1.5TB 的泄露数据，要求谈判代表在三天内联系。12 月 9 日，Noescape

勒索软件运营商在黑客论坛上称勒索软件运营商已经退出跑路，窃取了数百万美元的赎金，并关闭了该运营商的网络面板和数据泄露网站。

12)Cactus

Cactus 勒索最早在 2023 年 3 月开始活动，于 2023 年 5 月被披露。该勒索使用加密自身的方法试图逃避检测。主要利用 VPN 设备中的漏洞来获得初始访问权限。进入网络后，Cactus 会尝试枚举本地和网络用户帐户以及可访问的端点，然后创建新的用户帐户并利用自定义脚本通过计划任务自动部署和启动勒索软件加密器。“Cactus”这个名字来源于赎金票据中提供的文件名 cAcTuS.readme.txt，以及赎金票据本身中自我声明的名称。加密文件附加了.cts1，后面的数字因样本而异。目前有 Windows 和 Linux 两个版本的变体，并且拥有自己的 tor 博客用于公布泄露数据。



勒索软件主要传播途径

2023 年勒索软件攻击最常见的访问媒介依然是网络钓鱼、远程访问和漏洞利用：

1、网络钓鱼：勒索软件组织通过网络钓鱼活动来获得对目标网络的初始访问权限。通过发送欺骗性电子邮件，诱使毫无戒心的用户点击恶意链接或下载受感染的附件。

2、远程访问：利用远程桌面协议（RDP），勒索软件组织利用弱口令或者配置错误的远程桌面协议（RDP）登录未经授权访问的系统。一旦进入，他们就可以在网络中横向移动，提升权限并部署勒索软件。

3、漏洞利用：利用软件漏洞仍是勒索软件团伙中最受欢迎的攻击向量。这一趋势不仅表现在漏洞利用的频率上有所增加，更突显了攻击者对新的、更为隐匿漏洞的持续追求，旨在提高攻击的成功率和持续性。在 2023 年，Clop 勒索团伙宣称利用 GoAnywhere MFT（CVE-2023-0669）漏洞入侵了 130 多个组织，此外，2023 年勒索软件攻击中还使用以下漏洞：

- PaperCut 打印机漏洞（CVE-2023-27350、CVE-2023-27351）
- IBM Aspera Faspex 文件共享软件漏洞（CVE-2022-47986）
- Windows 通用日志文件系统驱动程序提升权限漏（CVE-2023-28252）
- MOVEit Transfer SQL 注入漏洞（CVE-2023-34362）
- 思科 VPN 中的未授权访问漏洞（CVE-2023-20269）
- Apache ActiveMQ 远程代码执行漏洞（CVE-2023-46604）

- Citrix Bleed 漏洞（CVE-2023-4966）

随着勒索软件背后的威胁行为者试图扩大其运营范围并提高盈利能力，勒索软件攻击在技术和组织上都发生了变化。除了上述三种常见的访问媒介外，初始访问代理（IAB）也已成为 RaaS 运营中的关键环节，帮助攻击者发起有针对性的活动。IAB 是指专门未经授权访问内部网络和系统的威胁组织或个人，然后将其出售给勒索软件运营商或者勒索附属机构，其职责包括识别漏洞、破坏网络防御以及提供对目标的访问。IAB 的发展，一方面使具有渗透测试技能的威胁攻击者能够从他们的工作中获利，而无需具备进行全面勒索软件或无加密勒索攻击所需的专业知识，另一方面也节约了勒索团伙或者勒索附属机构的攻击成本和入侵效率。

2023 年勒索软件团伙利用的漏洞列表如下：

CVE 编号	漏洞描述	相关勒索家族
CVE-2023-27350	某些版本的 PaperCut NG 和 PaperCut MF 中，使未经身份验证的参与者能够在没有凭据的情况下远程执行恶意代码	Bl00dy、Clop、LockBit
CVE-2023-27351	可能允许未经授权的攻击者提取存储在客户的 PaperCut MF 和 NG 服务器中的用户账户信息	Clop、LockBit
CVE-2022-47986	IBM Aspera Faspex Yaml 反序列化漏洞	IceFire

CVE 编号	漏洞描述	相关勒索家族
CVE-2023-28252	通用日志文件系统驱动程序中的越界写入漏洞，成功利用可进行权限提升	Nokoyawa
CVE-2023-0669	GoAnywhereMFT 管理端存在反序列化漏洞，攻击者利用该漏洞无需登录便可以远程执行任意命令	Clop
CVE-2023-34362	SQL 注入漏洞，该漏洞可能允许未经身份验证的攻击者访问 MOVEit 传输的数据库	Clop
CVE-2023-24880	Windows SmartScreen 安全功能绕过漏洞	Magniber
CVE-2021-21974	OpenSLP 中存在堆溢出问题，从而导致远程代码执行	ESXiArgs
CVE-2021-27876	Veritas Backup Exec Agent 文件访问漏洞	ALPHV / BlackCat
CVE-2021-27877	Veritas Backup Exec Agent 不当认证漏洞	ALPHV / BlackCat
CVE-2021-27878	Veritas Backup Exec Agent 命令执行漏洞	ALPHV / BlackCat
CVE-2023-27	Veeam Backup & Replication 身	ALPHV / Blac

CVE 编号	漏洞描述	相关勒索家族
532	份认证绕过漏洞	kCat
CVE-2023-4966	未经身份验证的缓冲区相关漏洞，影响 Citrix NetScaler ADC 和 Gateway、用于负载平衡、防火墙实施、流量管理、VPN 和用户身份验证的网络设备，未授权的远程攻击者可通过利用此漏洞，窃取敏感信息。	LockBit
CVE-2023-20269	主要影响 Cisco ASA 和 Cisco FTD 的 VPN 功能，允许未经身份验证的远程攻击者暴力破解凭据来访问网络，通过访问帐户，可以在被破坏的网络中建立无客户端 SSL VPN 会话。	Akira
CVE-2023-47246	SysAid 中的路径遍历漏洞，该漏洞会导致 SysAid 本地软件中的代码执行。	Clop
CVE-2023-22518	Atlassian Confluence 身份验证绕过漏洞。	Cerber

重大勒索软件攻击事件

2023 年，勒索病毒威胁持续蔓延延至不同行业和规模的受害者，给个人用户、企业以及政府机构带来了不同程度的经济损失和声誉风险。这些攻击事件分布广泛，凸显了勒索软件威胁的普遍性以及持续演进的趋势。本章将着重介绍在 2023 年发生的一些勒索攻击相关事件。

黑客利用向日葵远程控制软件的漏洞部署勒索软件

时间	2023 年 1 月
勒索软件	Paradise
利用漏洞	CNVD-2022-10270
受害地区	中国

黑客团伙正在利用老版本向日葵远程控制软件的漏洞 CNVD-2022-10270 发起攻击，向对应设备中投放 Paradise 勒索软件。此次攻击最早发生于 2023 年 1 月 30 日，攻击者对网络中暴露的向日葵远程控制软件进行大范围扫描，并对存在漏洞的向日葵远程控制软件发起攻击，目前已经有数十个目标被攻破并投递勒索软件。

Paradise 勒索软件将文件加密后，修改文件后缀为“[id-xxxxxxxx].[main@paradisenewgenshinimpact.top].honkai”（xxxxxxxx 代指一个八位随机字符串），并展示勒索提示信息要求受害用户联系黑客支付赎金。此次传播的勒索软件样本面对部分后缀的文件并不会对其内容进行加密，而仅仅是

对文件进行重命名操作。

皇家邮政（Royal Mail）遭 LockBit 勒索软件攻击

时间	2023 年 1 月
攻击者	LockBit
目标实体	Royal Mail
受害地区	英国
所属行业	运输行业

1 月 12 日，英国皇家邮政声称，网络攻击事件迫使国际邮政服务陷入停顿。LockBit 勒索软件攻击者加密了用于国际运输的设备，并通过处理海关业务的打印机发送了巨额勒索赎金通知。此次勒索软件攻击在媒体上引起了巨大的轰动，因为皇家邮政拥有 500 年历史，被视为英国的“重要国家基础设施”，此次事件影响了英国群众的生活和中小型企业的运作。最终，英国皇家邮政拒付赎金，并聘请了第三方网络专家协助调查和恢复业务。

美国法警局遭到勒索软件攻击

时间	2023 年 2 月
攻击者	未知
目标实体	美国法警局
受害地区	美国

所属行业	政府部门

2 月 17 日，美国法警局 (USMS) 发现了一个影响其系统的勒索软件和数据泄露事件。受影响的系统包含执法敏感信息，法律程序相关信息，以及有关工作人员和逃犯的敏感信息。美国法警局（USMS）隶属于美国司法部，其职责是保护联邦法庭及确保司法体系的正常运作，向联邦司法系统的几乎所有部门提供支持。美国法警局将该次攻击行为认定为一起“重大事件”进行调查。

德国军工巨头遭勒索攻击，汽车业务敏感数据或泄露

时间	2023 年 4 月
攻击者	BlackBasta
目标实体	Rheinmetall
受害地区	德国
所属行业	制造业

德国汽车和武器制造商莱茵金属公司称其遭遇了 BlackBasta 勒索软件攻击，影响了汽车领域的民用业务，军用业务未受到影响。莱茵金属是一家德国汽车、军用车辆、武器、防空系统、发动机和各种钢铁产品的制造商，拥有超过 2.5 万名员工，年收入超过 70 亿美元。5 月 20 日，BlackBasta 在其勒索网站上发布了莱茵金属公司的信息，并附上了黑客窃取的数据样本，包括保密协议、技术原理图、护照扫描和采购订单。

Royal 勒索软件组织攻击达拉斯市

时间	2023 年 5 月
攻击者	Royal
目标实体	美国达拉斯市
受害地区	美国
所属行业	政府部门

美国德克萨斯州的达拉斯市证实，该市的一些服务器遭到勒索软件入侵，导致其关键服务瘫痪，包括 911 调度系统。达拉斯警察局的网站当天也宕机了一段时间。达拉斯是美国第九大城市，人口约 260 万。Royal 勒索软件团伙声称对此次攻击负责。

LockBit 攻击印度尼西亚伊斯兰银行

时间	2023 年 5 月
攻击者	LockBit
目标实体	伊斯兰银行
受害地区	印度尼西亚
所属行业	金融

LockBit 声称已经在暗网网站上传播了印尼伊斯兰教银行的 1.5TB 数据。此次勒索攻击并没有对银行的公共服务造成影响，但泄露了包括与约 1500 万客户和员工相关的个人和财务信息。在过去的几年里，印度尼西亚的公司和政府机构已经发生了多次数据泄露事件，一位网络安全专家认

为此次事件是该国金融机构最大的违规事件之一。

LockBit 团伙攻击台积电，索要 7000 万美元赎金

时间	2023 年 6 月
攻击者	LockBit
目标实体	台积电
受害地区	中国
所属行业	半导体制造业

6 月 28 日，一个名为 Bassterlord 的 LockBit 关联公司通过 Twitter 宣布攻击了全球最大的半导体制造商台积电，声称窃取了大量敏感信息。台积电否认被 LockBit 攻击，但证实该组织攻破了公司的一个 IT 硬件供应商 Kinmax Technology，该公司为台积电提供网络，云计算，存储和数据库管理等 IT 服务。LockBit 在其网站上列出了台积电公司的相关数据，并索要 7000 万美元（约 5.08 亿元人民币）赎金。

Tellyouthepass 发起多轮攻击，国内逾 2000 台设备中招

时间	2023 年 5 月
勒索软件	Tellyouthepass
受害地区	中国

自 5 月开始，Tellyouthepass 勒索软件卷土重来，频繁发动大规模的攻击。其攻击方式都集中针对企业的服务器或管理系统一类对外公共设备。

5 月 6 日某 NC 服务器软件遭受 Tellyouthepass 攻击，其利用 NC accept 接口文件上的漏洞，向受攻击的服务器上传冰蝎 WebShell，进而接收攻击者发送的恶意模块，并将恶意模块加载进内存中执行，然后释放勒索软件代码。5 月 15 日，亿赛通电子文档安全管理系统也同样遭到入侵，瞄准的还是已经被厂商修补却未及时安装更新补丁的程序。在同样的入侵方式后，Tellyouthepass 学会了避开很多传统安全软件检测的能力，进而造成结束特定服务器进程、删除用户备份、跳过某些关键目录等常规操作，最终通过 RSA+AES 两种算法实现对文件的最终加密行为，以实现勒索的目的。

值得注意的是，Tellyouthepass 是国内极具代表性的勒索软件家族，擅长利用 Web 应用漏洞对运行应用的服务器发起勒索攻击。Tellyouthepass 家族利用各种漏洞发起勒索攻击，给国内企业造成了惨重的损失。2023 年 10 月，发现 CVE-2023-46604 漏洞也被 Tellyouthepass 勒索组织利用，作为攻击的初始访问。

英国物流公司因 Akira 勒索攻击而破产

时间	2023 年 6 月
攻击者	Akira
目标实体	KNP Logistics
受害地区	英国
所属行业	物流

英国最大的私营物流集团之一 KNP Logistics 宣布自己资不抵债，并

将其归咎于 6 月份的勒索软件攻击。此次勒索软件事件影响了其关键系统、流程和财务信息，对集团的财务状况及其获得额外投资和资金的能力产生了不利影响，据报道，此次破产造成 760 人被裁员。

米高梅国际酒店集团遭遇 BlackCat/Alphv 勒索攻击导致损失近 1 亿美元

时间	2023 年 9 月
攻击者	BlackCat/Alphv
目标实体	MGM Resorts
受害地区	美国
所属行业	商业和服务业

2023 年 9 月，BlackCat/Alphv 勒索软件组织的一个附属组织攻击了米高梅酒店集团，对米高梅的运营造成了严重破坏，迫使客人等待数小时才能办理入住，并导致电子支付、数字钥匙卡、老虎机、自动取款机和付费停车系统瘫痪。根据海外媒体声称，该勒索软件团伙在 LinkedIn 上找到一名美高梅酒店的内部员工，然后致电服务台，数十分钟后就入侵成功。

米高梅公司估计 9 月份的网络安全事件对拉斯维加斯大道度假村和地区运营部门的 EBITDAR（税息折旧及摊销前利润）的负面影响约为 1 亿美元。

Dark Angels 定向勒索攻击跨国公司江森自控，索要 5100 万美元

时间	2023 年 9 月
攻击者	Dark Angels
目标实体	江森自控
受害地区	美国
所属行业	制造行业

2023 年 9 月，智能建筑领域的知名跨国公司江森自控遭受大规模勒索软件攻击，该攻击对公司的许多设备进行了加密，影响了公司及其子公司的运营。该公司最初是在其亚洲办事处遭到攻击，但这次攻击导致江森自控关闭了部分 IT 系统，其子公司在网站登录页面和客户门户上显示技术中断消息。

勒索信表明此次事件由勒索组织 Dark Angels 所为。随后该组织声称窃取了超过 27TB 的公司数据，并对公司的 VMWare ESXi 虚拟机进行了加密。该团伙提出 5100 万美元的赎金要求，以换取提供解密器并删除被盗数据。最近的报告表明，被盗数据可能包含美国国土安全部(DHS)的敏感数据。

斯洛文尼亚最大的电力供应商 HSE 遭受 Rhysida 勒索软件攻击

时间	2023 年 11 月

攻击者	Rhysida
目标实体	斯洛文尼亚电力公司
受害地区	斯洛文尼亚
所属行业	电力基础设施

斯洛文尼亚电力公司 Holding Slovenske Elektrarne (HSE) 遭受勒索软件攻击，其系统和加密文件受到损害，但该公司表示，该事件并未中断电力生产。HSE 是斯洛文尼亚最大的发电公司，约占国内产量的 60%，被认为是该国的关键基础设施。这次攻击归咎于 Rhysida 勒索软件团伙，该团伙最近一直很活跃，在 2023 年发起了包括对智利军队、大英图书馆、伦敦爱德华七世国王医院系统等组织的攻击。

国际执法行动

2023 年勒索态势复杂多变，一方面勒索攻击频率较于往年明显增加，全球范围内众多大型企业和组织都遭受到攻击，勒索团伙几乎无所畏惧。另一方面，国际执法部门采取高压态势，相继展开一系列行动，成功摧毁了一些具有代表性的勒索团伙及相关基础设施，为打击勒索攻击和网络犯罪赢得了关键的战果。这些国际执法行动的成功，不仅有效遏制了勒索攻击的活跃势头，也向网络犯罪分子发出了强烈的警告。

下面简要介绍 2023 年部分重点的国际执法行动。

Hive 组织的基础设施被关闭

2023 年 1 月 26 日，美国司法部和欧洲刑警组织共同宣布，经过长达 6 个月的渗透，臭名昭著的 Hive 勒索软件组织已被 FBI 和国际刑警控制。Hive 勒索软件是勒索生态中最活跃的组织之一，在 2022 年攻击占比排名第五。根据 FBI 的信息，截至 2022 年 11 月，Hive 勒索软件团伙已使全球 1300 多家公司受害，收取了约 1 亿美元的赎金。

Hive 组织的 IT 基础设施已经完全被破坏，Tor 支付和数据泄露站点被查封，警方获得两台服务器和一台虚拟专用服务器的访问权。Hive 勒索软件组织的核心成员依旧逍遥法外，但 FBI 局长表示此次执法行动仍在进行中，包括追踪攻击者的基础设施、加密货币，以及追踪与 Hive 团伙合作的人。2023 年 12 月，一名涉嫌帮助 Hive 勒索软件团伙“清洗”赎金的俄罗斯公民在巴黎被捕。据悉，法国反网络犯罪办公室(OFAC)将嫌疑人与

数字钱包联系起来，这些钱包根据他在社交网络上的活动从可疑来源接收了数百万美元。

黑客被指控参与部署三种勒索软件变体

2023 年 5 月，美国司法部宣布对 Mikhail Pavlovich Matveev 提出起诉，因为他涉嫌参与部署 LockBit、Babuk 和 Hive 勒索软件变体。这三种勒索软件攻击了美国和世界各地的数千名受害者，包括执法部门和其他政府机构、医院和学校。

据悉，2020 年 6 月 25 日左右，Matveev 针对新泽西州帕赛克县的一家执法机构部署了 LockBit 勒索软件；2021 年 4 月 26 日，Matveev 针对华盛顿特区的大都会警察局部署了 Babuk 恶意软件；2022 年 5 月 27 日左右，Matveev 针对总部位于新泽西州默瑟县的一家非营利行为医疗保

健组织部署了 Hive 勒索软件。

Matveev 被指控密谋传送赎金要求、密谋以及故意损坏受保护的计算机。如果罪名成立，他将面临 20 多年的监禁。

LockBit 3.0 附属机构被捕

6 月中旬，美国司法部宣布对俄罗斯国民 Ruslan Magomedovich Astamirov（20 岁）提出指控，罪名是他参与了针对美国、亚洲、欧洲和非洲系统的多次 LockBit 勒索软件攻击。如果罪名成立，他可能因电信欺诈而面临最高 20 年的监禁，因损坏受保护的计算机而面临最高 5 年的监禁。

据悉，Astamirov 是继米哈伊尔·瓦西里耶夫被捕和米哈伊尔帕夫洛维奇·马特维耶夫被起诉后，第三位因与 LockBit 攻击有关而被起诉的黑客。

Ragnar Locker 被欧洲刑警组织捣毁

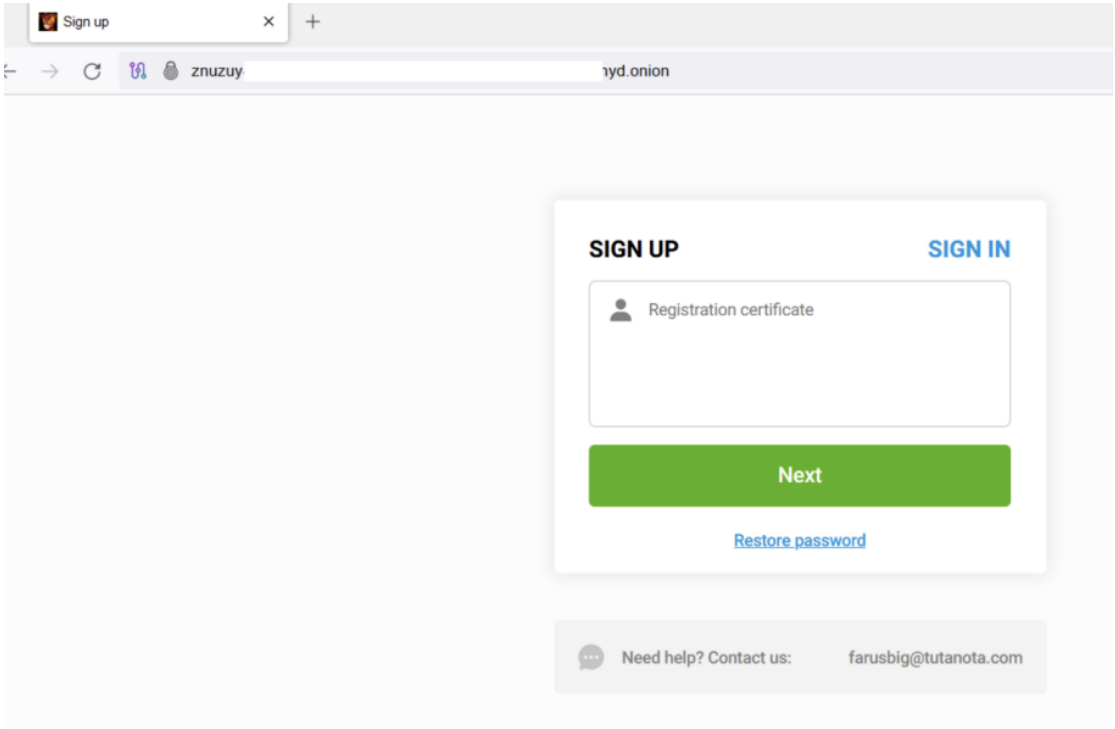
2023 年 10 月 19 日，国际执法机构小组查获了 Ragnar Locker 勒索组织的泄密地点。该勒索软件组织的基础设施也在荷兰、德国和瑞典被查封，相关数据泄露网站在瑞典被关闭。

Ragnar Locker 勒索最早于 2019 年 12 月首次被披露，常会利用远程桌面协议等暴露的服务来获取对系统的访问权限。其之前的受害者名单包括计算机芯片制造商 ADATA、航空巨头 Dassault Falcon 和日本游戏制造商 Capcom 等知名实体。

Trigona 遭遇乌克兰黑客攻击被迫关闭

乌克兰网络联盟(UCA)入侵了 Trigona 勒索软件组织，成功获取了服务器权限并清除了网络犯罪分子的数据。不过在 11 月，该组织使用新的 tor 链接重新上线并且已有新的勒索受害者出现。

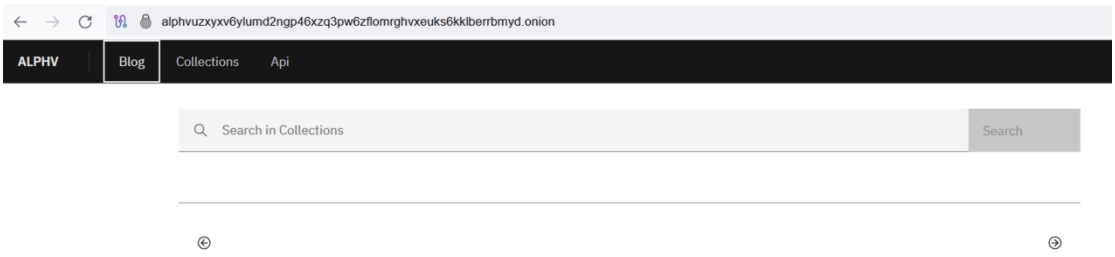
Trigona 于 2022 年 10 月下旬首次发现。从那时起，Trigona 的运营商一直保持高度活跃，一直在不断更新他们的勒索软件。2023 年 4 月，Trigona 开始通过暴力破解方法窃取凭据来针对受感染的 MSSQL 服务器。5 月，发现存在 Trigona 的 Linux 版本，它与 Windows 版本有相似之处。Trigona 由于工具、战术和程序（TTP）的相似性，认为 Trigona 背后可能与 CryLock 勒索软件是同一组威胁行为者。



BlackCat 服务器遭执法部门影响离线

在 12 月 7 日，BalckCat/Alphv 勒索组织其所有基础设施都处于离线状态，包括数据泄露和谈判站点。BalckCat/Alphv 管理员声称他们的中断是由硬件故障引起的，但网络安全公司 RedSense 称可以确认 BlackCat 勒索软件组织的网站已被执法部门关闭。

12 月 12 日，BlackCat 将其泄漏网站重定向到新的 URL 重新上线，但泄露站点没有显示之前的受害者信息。随后 LockBit 呼吁 BalckCat/Alphv 的附属机构，如果他们有被盗数据的备份，他们可以利用 LockBit 的数据泄露网站和谈判小组继续勒索受害者。此次事件可能对 BalckCat/Alphv 造成无法挽回的附属机构流失。



在 12 月 19 日，美国司法部宣布对 BlackCat 实施了执法行动，摧毁了相关基础设施并向全球 500 多名受害者提供解密工具。

勒索威胁新洞察

2023 年的勒索态势发展复杂且多变，勒索攻击威胁依然面临严峻挑战。安恒研究院猎影实验室长期持续跟踪全球勒索威胁变化，关注勒索组织战术、技术和程序的演化，以下简要介绍 2023 年勒索组织在演化过程中较为突出的 TTPs。

勒索团伙的演进——实施 BYOVD 技术

在 2023 年，不同的勒索团伙相继在勒索攻击过程中采用了 BYOVD 技术，这一现象呈上升趋势。BYOVD（Bring Your Own Vulnerable Driver）攻击技术，即攻击者在目标系统上加载已知包含安全漏洞的合法驱动程序，利用漏洞利用获取内核权限，利用成功后可以在内核级别运行任何恶意操作。这种攻击方式最初只有在一些顶级的 APT 组织活动中使用，而随着网络威胁态势的发展，攻击成本逐渐降低，近年来发现一些勒索组织也在利用该技术进行攻击，提升权限，逃避安全防护软件的检测，在 2023 年这一现象明显增加。

2023 年 1 月初黑客组织 Scattered Spider 利用已知的英特尔驱动程序漏洞以逃避 EDR 安全产品的检测。该组织后续在 10 月和 BlackCat 勒索组织关联在一起，是勒索攻击米高梅酒店集团的参与者。

此后，安全研究人员陆续发现多起利用 BYOVD 技术的勒索攻击事件。1 月 18 日和 2 月 14 日，攻击者使用 AuKill 终止 EDR 安全软件，然后部署 Medusa Locker 勒索软件。AuKill 是一款新型防御规避 EDR 检测的黑

客工具， 其利用 Process Explorer 16.32 版所使用的过时驱动程序版本，在目标系统上部署后门或勒索软件之前禁用 EDR 进程。后续还观察到攻击者在部署 Lockbit 勒索软件之前使用了 AuKill。

2023 年 5 月，BlackCat 利用 SpyBoy Terminator 终止安全防护程序。SpyBoy Terminator 同样是一款 BYOVD 工具，声称可以绕过包括 Sentinel One、Sophos、CrowdStrike 等在内的 24 种不同的 AV/EDR 和 XDR 安全防护设备。

网络威胁不断变化，2023 年的勒索攻击已然呈现出复杂的形势，勒索团伙近乎疯狂地在全球进行掠夺，远胜于 2022 年。勒索团伙势必也将在新的一年整合、创新已有的技术和策略，加强新一轮的勒索威胁。

Living off the Land(LOTL)攻击技术在勒索攻击中流行

Living Off the Land (LOTL)也称为 lolbins，是一种复杂的网络攻击技术，它利用受害者系统中已有的合法工具来执行和维持攻击。与依赖部署在受害者系统上文件的传统恶意软件攻击相反，LOTL 是无文件攻击。在 LOTL 攻击中，攻击者不需要在目标系统中安装任何代码或脚本。他们利用系统中存在的工具，包括二进制文件、脚本、库或驱动程序等，例如 certutil、regsvr32、schtasks、Mshta.exe、PowerShell 和 WMI 等。

由于使用的是合法的工具，LOTL 能长时间驻留在受害者系统内且不被察觉。这种更强的隐蔽性使攻击者有更多的时间来升级权限、窃取数据、横向移动、实施勒索软件攻击和设置后门。因此，LOTL 攻击越来越普遍，

也受到了勒索组织的追捧和热衷，例如 LockBit、Black Basta、Vice Society、Rhysida 和 BlackCat 等团伙在勒索攻击中常常使用该技术，屡试不爽。下面以 Rhysida 勒索组织为例，介绍该勒索组织在攻击中使用的合法工具列表:

工具名称	简单描述
cmd.exe	Windows 命令行实用程序
PowerShell.exe	用于在命令提示符窗口中启动 Windows PowerShell 会话的本机命令行工具。
PsExec.exe	PsTools 套件中包含的工具，用于远程执行进程。Rhysida 参与者大量利用此工具进行横向移动和远程执行。
mstsc.exe	与主机建立 RDP 连接的本机工具。
PuTTY.exe	Rhysida 参与者创建 Secure Shell (SSH) PuTTy 连接以进行横向移动。在一个示例中，对受感染用户帐户的 PowerShell 控制台主机历史记录的分析显示，Rhysida 攻击者利用 PuTTy 通过 SSH 远程连接到系统。
secretsdump	用于从系统中提取凭据和其他机密信息的脚本。Rhysida 使用此工具进行 NTDS 凭证窃取。
ntdsutil.exe	Rhysida 参与者使用此工具从域控制器中提取并转储 NTDS.dit 数据库，其中包含所有 Active Director

工具名称	简单描述
	y (AD)用户的哈希值。
AnyDesk	一种常见软件，可被威胁行为者恶意使用以获得远程访问并维持持久性，AnyDesk 还支持远程文件传输。
wevtutil.exe	用于查看事件日志的标准 Windows 事件实用工具。Rhysida 攻击者使用此工具清除了大量 Windows 事件日志，包括系统、应用程序和安全日志。
PowerView	用于获取 Windows 域态势感知的 PowerShell 工具。通过查看 PowerShell 事件日志，发现 Rhysida 攻击者使用此工具执行其他基于侦察的命令并获取凭据。

勒索组织利用 SEO 投毒获取初始访问

SEO 投毒即通过购买 Google/Bing 等搜索引擎的广告服务，当搜索关键词时可以向用户优先推送广告内容。

2023 年 1 月，微软报告称被追踪为 DEV-0569 的威胁行为者在广泛、持续的广告活动中使用 Google Ads 来传播恶意软件、窃取受害者的密码，并最终破坏网络进行勒索软件攻击。这些广告伪装成流行软件程序的网站，例如 7-Zip、FileZilla、LibreOffice、AnyDesk、WinRAR 等。研究人员认为

DEV-0569 是一个初始访问代理商，通过传播恶意软件破坏企业网络获取访问权限，然后将初始访问权限出售给其他黑客团伙，例如 Royal 勒索组织等。

2023 年 6 月，BlackCat/Alphv 勒索集团的附属机构利用 Google Ads 推送的新型 Nitrogen 恶意软件用于勒索软件攻击。当受害者在 Bing 或 Google 上搜索“WinSCP Download”会获得排名高于安全 WinSCP 下载站点的恶意结果引诱受害者点击进入模仿 Windows WinSCP 官方网站的虚假页面，然后下载恶意植入程序。

SEO 投毒广泛地被黑客团伙利用，此前安恒研究院猎影实验室也披露黑灰产团伙利用恶意广告诱使受害者访问伪装的 Telegram 钓鱼站点。今年以来勒索组织不断扩大目标范围，增加攻击频率，也在积极拓展获取初始访问的方式。

2024 年勒索攻击趋势预测

赎金支付总金额大幅上升

2021 年是勒索软件攻击领域迄今为止赎金交易额最高的一年，总支付金额高达 9.399 亿美元。2022 年，全球机构共同努力，采取了坚决的执法行动，有效地打击了勒索软件攻击的蔓延，受害者支付金额显著下降，赎金支付总规模低于 5 亿美元。

然而这一趋势并未延续至 2023 年，。根据区块链分析公司 Chainalysis 的数据，在 2023 年上半年受害者已向勒索软件团伙支付了 4.491 亿美元，预计 2023 全年的支付总额可能会达到 9 亿美元，与 21 年持平。

2023 年勒索赎金支付规模的增长与勒索团伙提出的极高初始赎金需求直接相关。2023 年针对大型企业的勒索攻击大幅增加，“大型游戏狩猎”攻击活动卷土而来，例如在第一季度，45%的勒索攻击初始金额要求超过 100 万美元。

在 2023 年，许多受网络攻击的组织仍选择不支付赎金，为了从那些仍愿意支付赎金的公司那里获取更多的赎金，攻击者提高了最初的赎金要求。

此外，据相关机构统计，2023 年，不包括赎金，从勒索软件攻击中恢复的平均成本是 182 万美元，勒索攻击对企业和组织造成的危害正逐步加深。我们预计在 2024 年，勒索软件攻击支付金额随着勒索组织的疯狂而进一步上升，受害组织遭受勒索攻击后的恢复成本也会相应提高。

勒索组织直接威胁受害个体

自 2021 年起，勒索病毒由单一的加密数据，演变为窃取公司数据、对被勒索公司发起 DDoS 攻击、售卖窃取到的信息等多重威胁。自 2022 年开始，国内已经有出现企业同时遭受勒索病毒攻击及数据泄露的情况。可以预见，双重甚至三重勒索攻击在国内也将成为常态。

为了更有效地获取经济利益，一些勒索团伙采取了更激进的方法，直接威胁受害公司或机构中的个人，迫使他们施压，要求公司支付赎金。2021 年 3 月，Clop 勒索软件团伙在加密并窃取受害公司数据后，向受害者的客户发送电子邮件，通知客户称，如果受害公司不支付赎金，攻击者将发布这些客户的个人数据。Clop 团伙敦促客户以保护隐私为由，致电受害公司，要求他们尽快支付赎金。

2023 年，针对曼彻斯特大学的攻击更加凸显了这一趋势带来的严重影响。除了联系校方之外，攻击者直接联系该校的教职员工和学生，告知他们关于大规模数据窃取的情况，警告称如果不满足勒索要求，他们的数据很快就会被泄露。据悉，攻击者窃取了 7TB 数据，包括教职员工和学生的机密个人信息、研究数据、医疗数据、警方报告、药检结果、数据库、人力资源文件、财务文件等。

如果学校被视为攻击目标，则会出现众多受害者。联系学生进行施压，学校会面临极大的舆论压力和声誉风险。媒体和公众对于大规模数据泄露的报道和批评可能对学校形象产生影响。

由于针对曼大的勒索攻击在国内外掀起了巨大的舆论风波，这可能会

引起更多的勒索团伙效仿，特别是针对拥有庞大用户群体的机构。因此，未来可能会看到更多类似的攻击事件。面对这一趋势，教育界和其他大规模组织必须采取更加严密和全面的网络安全措施。

二度受害：单一目标成为两个团伙的攻击对象

2023 年勒索软件领域呈现出“两个勒索组织攻击同一个目标”的新特点：

- 2 月，未经授权的攻击者访问并获取了存储在美国奥克兰市计算机服务器上的某些文件，影响了除 911 调度、消防应急服务和城市金融系统之外的所有网络系统。Play 勒索软件在 3 月初表示对此次网络攻击负责，随后泄露了声称为奥克兰市被盗数据的 10GRAR 档案，其中包含机密文件、员工信息、护照和身份证。3 月 21 日，LockBit 团伙也将奥克兰市列为受害者，并威胁要泄露从系统中窃取的文件。随后，奥克兰市政府发言人否认被 LockBit 入侵，称没有迹象表明系统存在其他未经授权的访问。
- 5 月，两个不同的勒索软件组织声称对总部位于美国纽约的奥尔巴尼耳鼻喉科和过敏服务中心（AENT）进行了成功的攻击。BianLian 组织首先声称对此攻击负责，并声称已泄露了 630GB 的文件。RansomHouse 随后声称渗透了内部系统，并窃取了 2TB 数据。AENT 未对这两个团伙声明的有效性发表评论。
- 6 月，全球最大的音乐设备生产商雅马哈公司被列入 BlackByte 勒

索软件团伙的泄密网站，而后于 7 月又被 Akira 组织列为受害者。雅马哈公司确认遭遇“网络安全事件”，表示黑客未经授权访问其系统并窃取数据，但并未指明攻击者的身份。

- 7 月，雅诗兰黛被 Clop 和 BlackCat 勒索团伙列为受害者。BlackCat 组织声称与 Clop 无关，并将其入侵描述为“完全独立”的攻击，并暗示泄露的数据可能会影响客户、公司员工和供应商。
- 11 月，勒索组织 Clop 和 Rhysida 接连将美国北卡罗来纳中央大学纳入受害者名单，该校在线课程因勒索攻击被迫暂停。
- 12 月，德国能源署 DENA 先后遭受两大顶级勒索组织 LockBit 和 BlackCat 的数据勒索。

对于这一特点，从受害者内因分析，可能有以下两个原因：

1. 目标的价值和重要性：如果两个勒索团伙都选择攻击同一个目标，很可能是因为该目标具有很高的价值和重要性。这样的目标可能是政府机构、大型企业或跨国公司。这些实体拥有大量敏感数据和财务资源，攻击造成的损失巨大且影响广泛。
2. 目标的脆弱性：同时被两个勒索团伙攻击，也有可能是因为该目标的网络存在多个薄弱环节，缺乏有效的安全防御措施。勒索软件攻击者通常会选择寻找容易渗透的目标，以确保成功侵入目标网络。

从攻击者外因分析，也可能存在不同勒索软件团伙与同一个附属机构（affiliate）合作的情况。此外，将受害者同时列入不同勒索软件组织的泄密网站或暗网中，能够获得更多的曝光率，扩大宣传效果，引起更广泛的

关注和社会议论，进而加大了受害组织的压力，促使其更快速地支付赎金。预测，在 2024 年，两次受害这一现象将会被扩大。

勒索团伙的漏洞利用能力增强

勒索软件团伙在 2023 年展现出了强大的漏洞利用能力。其中 Clop 勒索软件团伙尤为突出，该团伙在半年内利用 GoAnywhere MFT、PaperCut 和 MOVEit Transfer 等软件中的漏洞发起了大量攻击，造成了严重影响。

2023 年 1 月下旬，Clop 勒索软件组织利用 0day 漏洞（现已编为 CVE-2023-0669）发起了一场针对 GoAnywhere MFT 平台的活动。攻击者可以利用此漏洞在未修补的 GoAnywhere MFT 实例上执行远程代码，让管理控制台暴露在互联网上，被任意访问。Clop 团伙声称已经可以通过受害者的网络横向移动，并部署勒索软件载荷来加密系统，但他们决定不加密系统，只窃取存储在受攻击的 GoAnywhere MFT 服务器上的文件。该组织表示，从 GoAnywhere MFT 平台窃取的数据影响大约 130 名受害者。

2023 年 4 月，Clop 团伙利用了两个 PaperCut 漏洞传播勒索软件——CVE-2023-27350 和 CVE-2023-27351。攻击者利用 PaperCut 的漏洞，初步访问公司网络。一旦获得了访问服务器的权限，Clop 就会部署 TrueBot 恶意软件和 Cobalt Strike 信标，同时使用 MegaSync 文件共享应用程序窃取数据。

2023 年 6 月，Clop 利用流行的管理文件传输软件 MOVEit 中的 SQL 注入 0day 漏洞 CVE-2023-34362 进行攻击。MOVEit Transfer 是广泛使用

的托管文件传输软件，通过利用该漏洞，攻击者可以未经授权访问数据库，进而导致远程代码执行和数据泄露。攻击者利用 MOVEit 漏洞在服务器上释放特制的 webshell，从而允许他们检索存储在服务器上的文件列表、下载文件并窃取已配置的 Azure Blob 存储容器的凭证或密钥。利用 MOVEit 安全文件传输平台中的 0day 漏洞进行的数据窃取攻击预计将影响全球数百家公司。

2023 年 8 月，Akira 勒索软件利用思科自适应安全设备(ASA)和 Firepower 威胁防御(FTD)产品进行勒索攻击，后续思科证实上述产品中存在漏洞未授权访问漏洞（CVE-2023-20269）。

2023 年 10 月起，包括 Citrix Bleed 在内的多个漏洞相继被勒索组织利用，波音公司等大型企业和机构受到波及。

值得注意的是，Clop 团伙在之前也曾经利用 Accellion 文件传输设备和 GoAnywhere MFT 等软件中的漏洞进行攻击。这表明，0day 漏洞利用攻击对勒索团伙来说是一种有吸引力的作案手法，他们对这类漏洞的关注程度持续增加，且持续加强漏洞武器化的能力。面对勒索团伙漏洞利用能力的增强，各组织和企业应当高度重视网络安全防护措施，及时更新软件补丁，加强漏洞管理，以及备份重要数据，以确保网络和数据的安全。

AI 技术在勒索攻击中的潜在威胁

快速发展的网络安全格局给网络防御者带来了新的挑战，网络犯罪分子进军新兴的基于大型语言模型 (LLM) 的人工智能市场，试图利用 AI

技术创建、扩自动化和改进攻击。

日本专家的一项研究发现，生成式人工智能服务 ChatGPT 可以创建计算机病毒。ChatGPT 是美国初创公司 OpenAI 于 2022 年发布的人工智能聊天机器人，尽管 ChatGPT 被设置成拒绝用户“恶意或不道德地使用”，避免被用于犯罪目的，但如果输入伪装成开发者的指令，就能生成可用于网络犯罪的勒索病毒。经测试，生成的勒索病毒成功感染了一台测试用的电脑，加密了内部数据并显示索要赎金的勒索信。

虽然勒索软件团伙目前还没有推出人工智能驱动的勒索软件，但知名网络安全专家 Mikko Hyppönen 认为，考虑到近年来一些勒索软件团伙积累的财富，攻击者可能很快就会聘请人工智能专家，与合法安全公司争夺人工智能和机器学习方面的人才。

勒索软件团伙可能会通过以下方式利用人工智能（AI）技术：

- 定制的网络钓鱼攻击：借助人工智能驱动的勒索软件，黑客可以创建更具体、更有创意的电子邮件。钓鱼邮件是勒索团伙常用的媒介之一，攻击者可以利用 AI 技术抓取社交媒体网站并识别信息，将其传送回恶意软件团伙，用于定制的网络钓鱼攻击，从而实现社会工程策略。
- 快速扫描漏洞：勒索软件攻击的一个重要部分是渗透系统，恶意行为者可以利用 AI 技术快速分析大量的网络数据，并识别系统中可能存在的弱点和漏洞。
- 自动执行大规模攻击：恶意行为者可以使用人工智能工具来自动化

大规模勒索软件攻击，包括脚本编写、部署、系统分析等过程，快速创建恶意软件并将其同时部署到多个系统。

- 基于机器人的谈判：人工智能驱动的勒索软件可以自动化赎金谈判过程。过去，勒索软件攻击通常通过人工操作员与受害者沟通并协商支付赎金。而借助人工智能驱动的勒索软件，谈判过程可以实现自动化，使攻击者能够节省谈判时间，扩大其运营规模，并有可能获得更多赎金。

如果勒索团伙利用人工智能的应用，攻击会变得更加自适应和智能化。这些技术变化给防御措施带来了新的挑战。网络安全专家需要加强防御措施，提高系统的安全性，以有效应对不断演进的勒索威胁。

针对云服务的勒索攻击将增加

2023 年 2 月初，ESXiArgs 勒索软件破坏了未打补丁的云服务，对全球数千台服务器发起勒索软件攻击。攻击者利用 VMware ESXi 服务器中的已知漏洞，获取访问权限并部署 ESXiArgs 勒索软件，对 ESXi 服务器内配置文件进行加密并发送赎金票据。其中，受影响最严重的是过去将数据存储在物理服务器上，并仅简单地将数据部署在云端的公司。

重要的云服务提供商和云计算基础设施近期成为勒索组织关注的重点目标。随着全球数字化转型的加速，越来越多的服务和数据部署在云端，基础设施即服务（IaaS）作为数字经济的强力支撑，逐渐成为信息基础设施的重要组成部分。勒索组织也注意到云上资产的重要性，针对云系统量

身定制的勒索软件攻击（Cloud Ransomware）成为新型威胁。

随着云计算和存储的日益普及，勒索软件攻击者可能会开发针对云服务和工作流程进行优化的新型勒索软件。云环境受到损害可能会导致广泛的损害、业务中断和敏感数据被盗，从而同时影响多个用户或组织。这种可能性凸显了在基于云的环境中需要强大的安全措施和主动防御。

间歇式加密和无加密勒索模式持续发展

勒索病毒在发展中不断探索新技术来提高自身的加密能力，间歇性区块加密就是其中一种盛行的新技术。间歇性加密不会加密所选择的完整文件，而是选择性加密文件中的部分字节。

LockFile 勒索软件是 2021 年年中第一个使用间歇性加密的恶意软件家族，此后 Qyick、PLAY、Agenda、Black Basta、BlackCat 等勒索软件也开始采用这种模式。

对比全加密，间歇式加密的速度更快，能够尽可能的绕过安全软件检测和拦截。间歇性加密方式可以在很短的时间内加密较少内容但仍导致系统无法使用，从而为勒索团伙在速度方面带来了显著优势。

无加密勒索是 2022 年勒索生态最显著的变化之一，这一趋势在 2023 年仍在持续。无加密勒索始于 Babuk 和 SnapMC，随后在 2022 年又涌现出如 Karakurt、Donut、RansomHouse、Lapsus$等专注数据泄露勒索攻击的团伙。

BianLian 是 2023 年最为突出和典型的数据勒索网络犯罪组织。BianL

ian 最初采用双重勒索模式，窃取文件并加密受害者的系统。但 2023 年 1 月左右，BianLian 转为采取无加密勒索攻击模式。该组织通过有效的远程桌面协议 (RDP)凭据访问受害者系统，使用开源工具和命令行脚本进行发现和凭据收集，并通过文件传输协议 (FTP)、Rclone 或 Mega 窃取受害者数据。

自双重勒索攻击模式兴起以来，勒索攻击的核心逐渐从数据加密转变为数据泄露。数据泄露勒索攻击方式与传统的全面的勒索软件攻击相比，跳过了部署勒索软件的步骤，需要的时间更少，大大节省了时间成本，因此无加密勒索的趋势在勒索生态中将会持续存在。

出现更多的勒索源代码再利用

自 Conti 团伙解散以来，研究人员发现了多种基于 Conti 勒索软件泄露源代码创建的勒索软件毒株。LockBit 威胁组织也使用了泄露的 Conti 勒索软件源代码进行攻击，并将该特定变体称为 LockBitGreen。以下是一些已披露的基于 Conti 的新型勒索软件：

- BlueSky：BlueSky 勒索软件最初于 2022 年下半年出现。该勒索软件与 Conti 和 Babuk 勒索软件表现出一些相似之处和重叠之处。此勒索软件释放的赎金记录名为“# DECRYPT FILES BLUESKY #.txt”，其中包含解密文件的说明。
- ScareCrow：ScareCrow 是一种基于 Conti 勒索软件的新勒索变体。执行后，它会加密文件并附加 crow 作为扩展。该勒索软件会释放

名为“自述文件.txt”的赎金记录，其中包含三个用于联系威胁行为者的 Telegram 地址。

- Meow：Meow 变种基于 Conti 勒索软件，加密受害者的文件并附加.meow 作为扩展。它会释放一个名为“readme.txt”的赎金记录，其中包含四个电子邮件地址，以及受害者可以用来交互的两个 Telegram 地址。
- Putin Team：Putin Team 作为新出现的勒索软件组织，可能已经更改了 Conti 勒索软件泄露的源代码以生成勒索软件二进制文件。这个团体伪装成来源于俄罗斯，但目前没有有效的证据来证实这一点。

2023 年 3 月，研究人员首次观察到 Akira 勒索软件，该软件主要针对美国和加拿大，目标包括教育、金融、房地产、制造业和咨询等多个行业，已经危害了至少 63 名受害者。研究人员认为 Akira 恶意软件开发者受到了泄露的 Conti 源代码的启发。Akira 与 Conti v2 勒索软件的相似之处包括：

- 排除相同的文件类型和目录
- Akira 文件尾部的结构与 Conti 附加的文件尾部相同
- Akira 勒索软件使用的 ChaCha 算法的实现与 Conti 勒索软件相同。
- 密钥生成代码（两次调用 CryptGenRandom，然后调用 CryptEncrypt）类似于 Conti 的密钥生成函数。

此外，Akira 勒索软件交易与 Conti 攻击者之间存在“多次重叠”。区块链分析人员发现，在其观察到的三笔可疑交易中，Akira 勒索软件用户总共向 Conti 附属地址支付了超过 60 万美元。因此研究人员认为，虽然 C

onti 已经解散，但其前成员可能通过与 Akira 等其他勒索软件即服务组织的活动。

除了 Conti，Babuk 和 HelloKitty 源码也已经泄露，在 2023 年同样出现了大量复用的现象，预测未来会涌现更多代码复用的勒索家族，在 2024 年继续对目标实体造成破坏。

防御措施

针对日益增加的勒索软件威胁，企业和个人用户需要采取一系列有效的防御措施来保护数据和网络安全。以下是对勒索软件的防御措施建议：

- 定期备份数据：建立定期备份机制，将重要数据备份到离线存储介质，例如外部硬盘或云存储
- 更新和升级软件：及时更新操作系统、应用程序和安全软件，确保系统和软件的漏洞得到及时修补。
- 安装可信的安全软件：选择可信的防病毒和防火墙软件，及时检测和阻止恶意软件的入侵，加强对勒索软件的防范。
- 增强网络安全意识：对企业员工和个人用户进行网络安全培训，增强对勒索软件和其他网络威胁的认识，不点击来历莫名的邮件附件和链接。
- 使用强密码和多因素身份验证：采用强密码，定期更换密码，并使用多因素身份验证，增加账户的安全性，防止账户被入侵和勒索。
- 监控和检测：建立实时监控和入侵检测系统，安装防病毒软件定期对系统进行扫描，及时发现异常活动，追踪并预防潜在的攻击。
- 加强网络隔离：将关键系统和数据隔离于内部网络，限制用户权限，降低勒索软件扩散和影响范围。
- 建立应急响应计划：制定应急响应计划，明确应对勒索攻击的流程和责任，确保在遭受攻击时能够迅速做出反应。

总结

今年面临的勒索软件攻击形势较于以往更为复杂，在全球经济发展低迷和地缘政治波动的双重影响下，愈来愈多的网络犯罪团伙投身于勒索攻击以掠取丰厚的非法利润。经过多年来的发展，勒索软件生态逐渐丰富，RaaS 运营模式的成熟和 IABs 的兴起，大大降低了勒索攻击的门槛和成本。

2023 年多个新型勒索组织开始崭露头角，锋芒毕露，占据了今年将近一半的活跃度，在这些新兴勒索中不乏有老牌勒索的影子，例如 AKira 和逝去的 Conti 组织之间的关联，BlackSuit 勒索的出现和 Royal 在下半年的消失重塑有着密不可分的关系，这也透露出如今勒索软件生态中不同勒索组织可能存在千丝万缕的联系和高度复杂化。而作为顶级勒索组织的 LockBit、BlackCat 和 Clop 在 2023 年依旧跻身前列。他们在 RaaS 的运营模式、漏洞武器化利用和勒索软件开发能力等技术和战术方面上展现了出色的综合能力，凭此在全球收割了众多受害者，获取了巨额的利润。

在即将到来的 2024 年，新一轮的勒索攻防博弈已经拉开序幕。随着全球各个组织对网络服务的日益依赖，尤其是对关键信息基础设施的数字化依存程度不断提升，网络犯罪分子也同样已经将其目标锁定在这一趋势当中。在这样的背景下，制定和实施切实可行的网络安全战略显得至关重要。网络安全不再是单一组织的问题，而是需要全球范围内的协同合作来有效对抗勒索攻击的挑战。只有通过协同努力，共同应对不断演进的勒索攻击，才能够更好地保护网络空间的安全，维护数字化社会的可持续发展。

亚奥理事会官方合作伙伴
OFFICIAL PRESTIGE PARTNER OF THE OLYMPIC COUNCIL OF ASIA

安恒信息
DAS-Security

官网：www.dbappsecurity.com.cn
电邮：info@dbappsecurity.com.cn
客服专线：+86-400-6059-110

杭州总部

地址：杭州市滨江区西兴街道联慧街188号安恒大厦
座机：0571-88380999/28860999
传真：0571-28863666

安恒信息官方微信