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%。

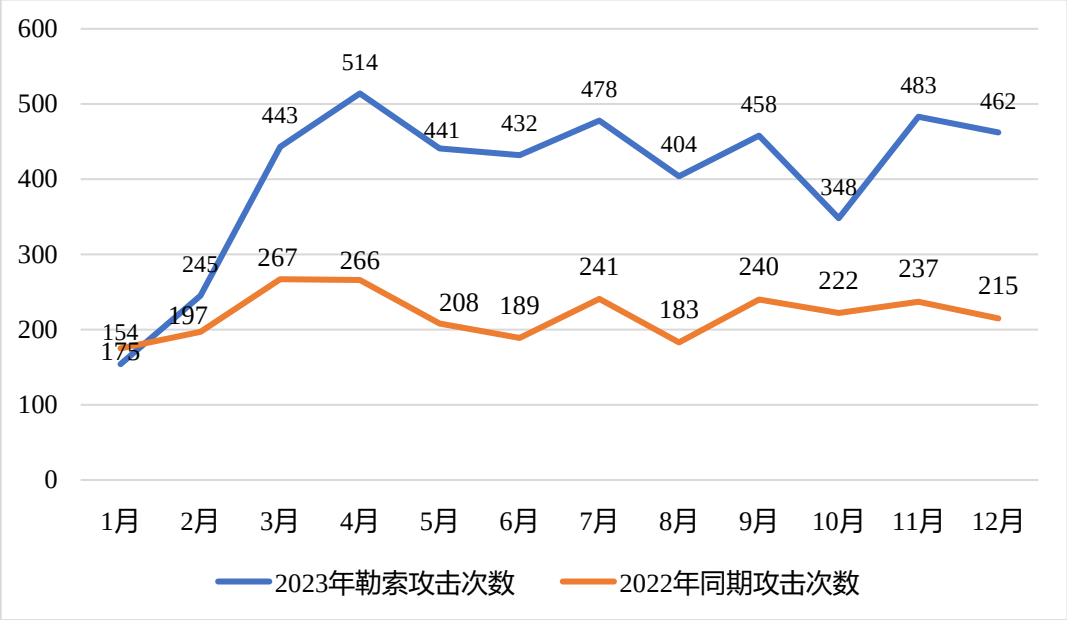


图 2023 年每月全球披露的勒索攻击次数统计

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：

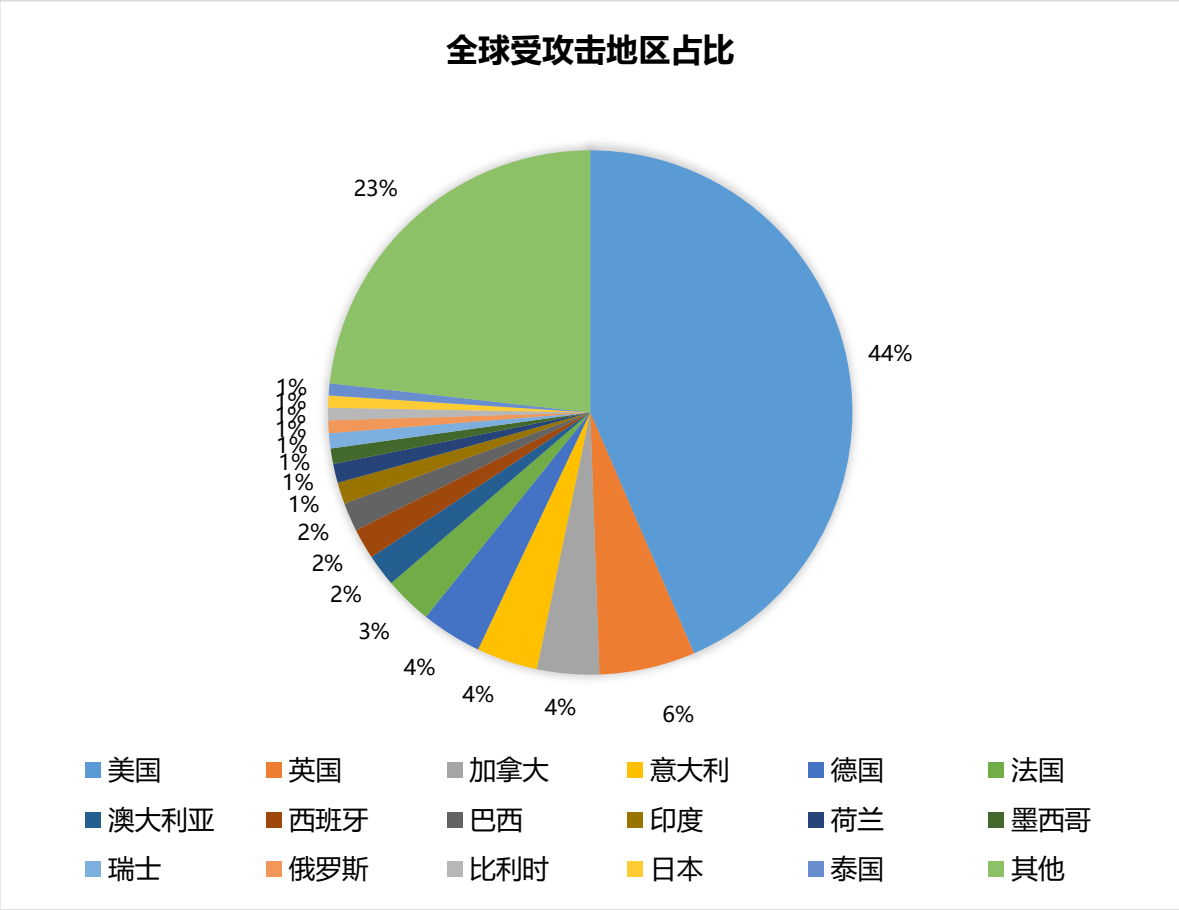


图 2023 年全球受攻击地区统计

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：

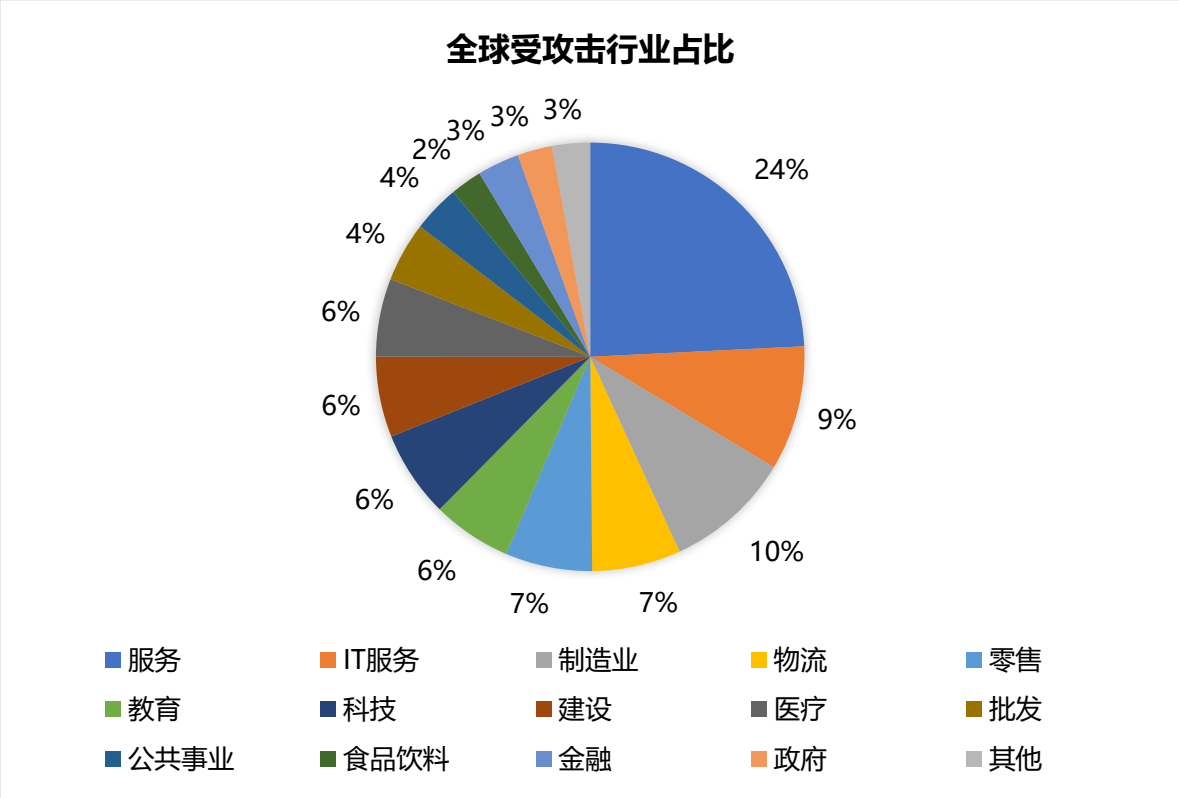


图 2023 年全球勒索攻击行业统计

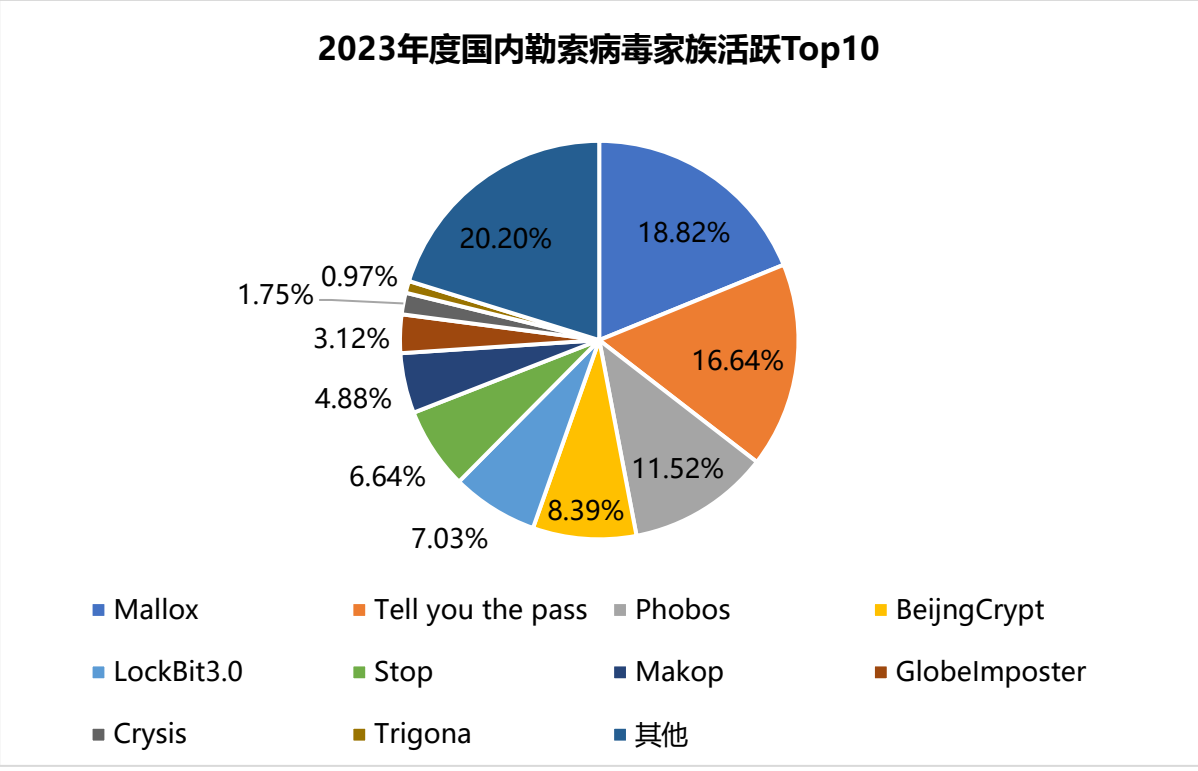
服务行业涉及餐饮、酒店、旅游等领域，IT 行业负责管理和维护信息技术基础设施，制造业涉及生产和供应链管理。攻击这些行业可能造成重要服务的停滞，影响居民所需的关键服务，对社会和经济运作产生较大的影响。这些行业通常拥有大量的用户数据、商业机密和敏感信息，攻击者可以通过勒索软件攻击获取这些有价值的数据，并将其用作勒索的筹码。

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。



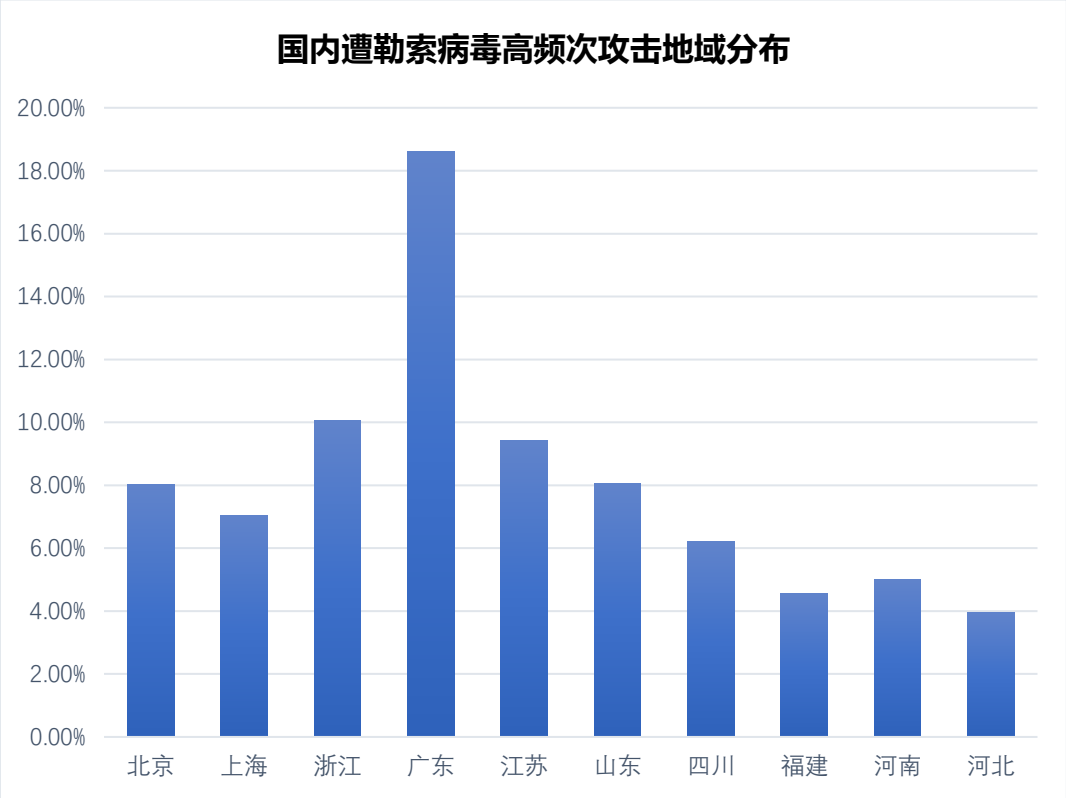
2023 年国内勒索病毒家族活跃 Top10

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。

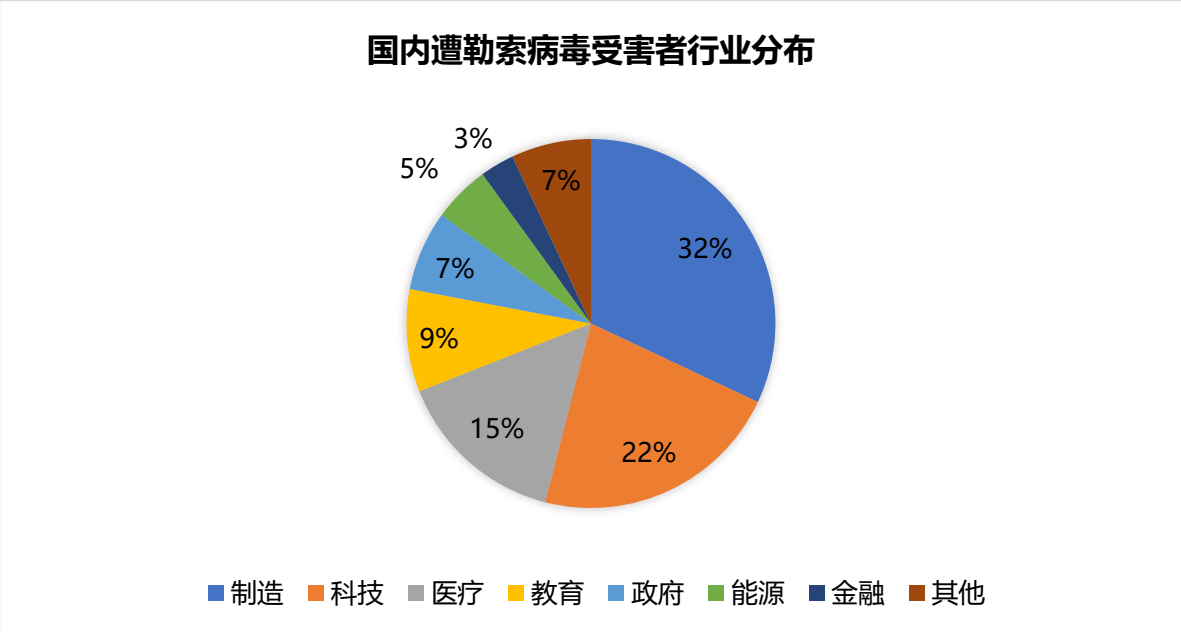
- LockBit3.0：这是 2023 年最活跃的勒索软件团伙。LockBit 勒索软件采用勒索即服务的运营模式，招募附属公司使用 LockBit 勒索软件工具和基础设施进行勒索软件攻击。
- Trigona：该家族是一种相对较新的勒索软件，自 2022 年 10 月下旬起一直保持高度活跃，普遍认为 Trigona 背后可能与 CryLock 勒索软件是同一组威胁行为者。2023 年 4 月，Trigona 开始通过暴力破解方法窃取凭据来针对受感染的 MSSQL 服务器。5 月，发现存在 Trigona 的 Linux 版本，它与 Windows 版本有相似之处。在 10 月份，该勒索组织的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