云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

TRUSTED SECURITY
可信安全

勒索软件防护发展报告

（2022年12月）

云计算开源产业联盟

云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

版 权 声 明

报告愿景及目标

随着数字化经济的飞速发展，网络安全法、数据安全法的颁布，数字化已成为国家和各行业发展的主旋律。企业在数字化转型的过程中，面临着包括勒索攻击、双重勒索等新型勒索软件带来的巨大威胁。勒索软件是攻击传播面极广、经济损失极大的一种攻击方式。无论是个人、企业还是组织，都可能成为勒索软件攻击的对象。

勒索软件针对企业核心业务系统、关键数据进行加密，导致核心业务系统中断、关键数据不可恢复，从而影响企业正常运作，带来严重的经济损失和声誉损失。因此为企业建立事前防护、事中持续监测、事后快速响应及安全加固的全流程勒索软件防护体系，成为企业防御勒索软件攻击的首要重点。

在此背景下，云计算开源产业联盟撰写了本报告，旨在通过对勒索软件发展情况、主要特点、攻击现状、发展态势以及防护体系建设、未来发展展望等多个方面进行梳理、总结和分析，帮助企业正确认识勒索软件，合理高效地防范勒索软件攻击，增强产业界信心。

编制组成员

卫斌、郭雪、孔松、李忆晨、饶帅、李飞、吕杨琦、黄超、李晓峰、丁立彤、陈绍良、何志彬、何柏宜、王振兴，安东冉，田苏维、李栋，梁伟，于忠臣、梁连燚、吕佳、陈东鹏，彭丽娟，聂永立、张永波、毛帅、杨志伟、延林朴、刘新新、周素华、王凤周、王亮、刘海粟、康罗、孙维伯、吴剑刚、黄海莲、刘沛、程进、张桐桐、王春晓、李文越、陈世亮、杨磊、杨梅、廖双晓、曹峰、毛立峰、孙涛、郭海骏、陈明阳、林建兴、张帅

目 录

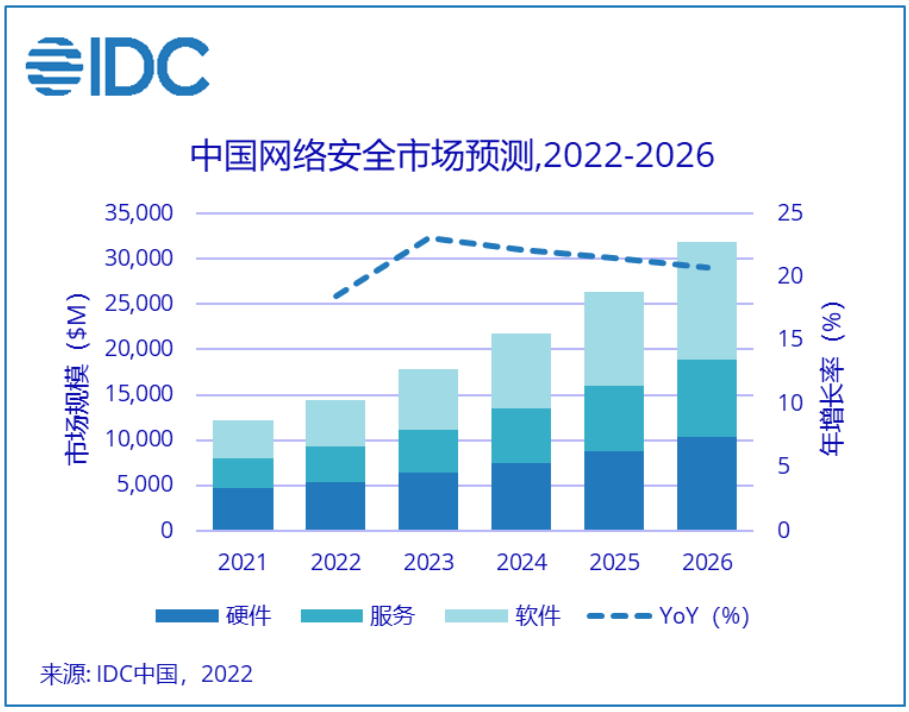
图目录

表目录

一、 勒索软件发展概述

（一）我国网络安全市场产业进展迈向新阶段

我国网络安全市场发展稳中向好，产业发展迈向新阶段。2022 年对中国和世界都是充满挑战的一年，我国数字经济进入快速发展时期，网络安全法律法规体系逐渐夯实完善，社会各方对网络安全的投入逐渐加大。根据《IDC Market Forecast: 中国网络安全市场预测，2022-2026》，中国网络安全市场总投资规模为 122 亿美元。IDC 预测，到 2026 年，中国 IT 安全市场投资规模将达到 319 亿美元。



数据来源：IDC 中国（2022）

图 1 中国网络安全市场预测，2022-2026

（二）勒索软件攻击已成为网络安全的最大威胁之一

勒索软件（Ransomware）攻击已成为网络安全的最大威胁之一。勒索软件攻击指的是网络攻击者通过对目标数据进行强行加密，导致企业核心业务停摆，以此要挟受害者支付赎金进行解密的行为。勒索软件是一种阻止或限制用户使用电脑系统的恶意程序，极具传播性、破坏性，攻击者用来对用户资产或资源进行劫持，旨在加密和盗窃数据以勒索钱财。勒索软件利用多种密码算法加密用户数据、更改系统配置等方式，使用户资产或资源无法正常使用，受害者必须向攻击者付费，才能获得解密密钥，重新获得数据，恢复系统正常运行。由于勒索攻击事件中被加密信息难以恢复，直接导致作为攻击目标的关键信息系统无法正常运转，攻击来源难以追踪，敏感信息的窃取和泄露导致极大的法律合规和业务经营风险，勒索软件对现实世界的威胁加剧，已经成为全球广泛关注的网络安全难题。

近年来，勒索软件攻击已成为无处不在的网络安全攻击手段。新型勒索攻击事件层出不穷，勒索软件攻击形势更加严峻，已经对全球制造、金融、能源、医疗、政府组织等关键领域造成严重影响。在某些事件中，攻击者挟持关键基础设施进而索要高额赎金，甚至可能影响国家的正常运作能力。根据 SonicWall 发布的 2022 年年中网络威胁报告，2022 年 1-6 月，全球共记录了 2.361 亿次勒

索软件攻击。世界经济论坛《2022 年全球网络安全展望报告》称，80%的网络安全领导者认为勒索软件是对公共安全的重大威胁。勒索软件损害预计将从 2015 年的 3.25 亿美元增长到 2031 年的 2650 亿美元。

勒索攻击事件在全球各地频频发生，可归因于几方面:

一是企业内部基础设施建设不完善，拥抱数字化转型后缺少有效的安全防护措施。根据美国国家标准与技术研究所（NIST）发布的数据显示，2021 年报告的漏洞数量为 18378 个，年度漏洞数据已经在五年内连续增长。根据《2022 上半年网络安全漏洞态势观察》，我国 2022 年上半年新增通用型漏洞信息共计 12466 条，超高危及高危漏洞占比超过 50%，存在大量暴露在互联网的设备和系统，存在高危漏洞的系统涉及诸多重点行业。

二是高额赎金已经成为网络攻击者极高的犯罪动力。根据《Akamai 勒索软件威胁报告 APJ 深入洞见 2022 年上半年》，勒索软件攻击在全球造成的损失已超过 200 亿美元。《Ransomware Uncovered 2021/2022》报告指出，2021 年的平均赎金要求增长了 45%，达到 24.7 万美元，比 2020 年高出 45%。

三是远程办公增加安全风险。新冠肺炎疫情期间，远程办公带来的安全漏洞，通过技术迭代，不断进化数据泄露、加密数据等攻击手法和方式，开辟新的攻击面，利用人们在危机期间的恐慌心理，勒索次数持续增加。

当前，随着云计算、大数据、人工智能等新技术的快速普及和应用，如今勒索攻击呈现出持续高发态势，网络攻击也变得更加组织化和系统化，攻击范围向行业、基础设施领域拓展，包括金融、交通、医疗等多个领域都成为新的攻击对象。一旦基础设施遭受攻击，将导致整个产业链的停摆或瘫痪，甚至影响社会稳定。

（三）勒索软件攻击影响呈扩大趋势，带来巨大威胁

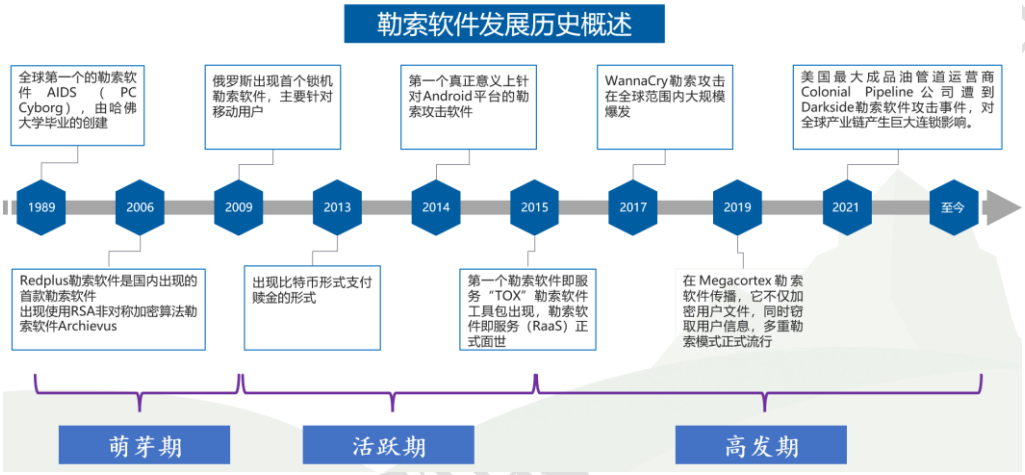
勒索软件攻击几乎总是以金钱为动机，已经成为重要的网络安全问题，对个人、企业乃至国家层面安全都面临着巨大的安全威胁。首先，对个人而言，文件、图片、视频等个人事务、隐私若被泄露可能会引起纠纷、焦虑以及恐慌。**其次，对于企业而言，一是破坏生产**，数据被加密，往往意味着业务系统崩溃、数据库宕机，如果被加密的数据包括生产控制系统、流程系统等，或者用户数据、订单数据等，则会造成企业生产的混乱，轻则减产，重则停工停产，销售停顿，会造成巨大的经济损失。**二是经营困难**，如果被加密的数据涉及企业的经营数据，则可能造成经营决策的混乱，如无法进行政策的财务审计，无法进行市场分析、用户画像等经营决策，打乱企业发展步伐，造成长期的经济损失。**三是数据信息丢失**，被勒索的内容包括企业信息、客户信息、账户和支付详细信息或其他重要价值的企业机密数据，一旦加密造成业务无法运行、数据泄露公布，将对企业造成巨大伤害；**四是持续攻击，**勒索软件清

楚不彻底，可能在信息系统中留有隐蔽通道，勒索组织会持续对企业进行攻击和袭扰，还有企业不胜其扰，定期向勒索组织缴纳赎金买平安，数据勒索从“拦路抢劫”模式，进入“收保护费”模式。**五是商誉损失，**数据勒索会造成客户对企业的信任危机，企业的商业信誉会降低，面临的法律风险会升高，经营管理能力面临质疑，面临巨大的无形资产损失风险。**最后，勒索软件攻击已在某些层面上直接或间接得影响了国家安全，**自 2022 年 4 月 17 日和哥斯达黎加勒索软件攻击爆发以来，已至少影响了哥斯达黎加 27 个政府机构，其中 9 个受到严重影响；2022 年 11 月，英国议会国家安全战略联合委员会（JCNSS）亦启动专项调查，调查其国家安全战略能否有效应对勒索软件威胁。

勒索软件攻击的规模、影响以及破坏效果都呈扩大趋势，可直接攻击关键基础设施导致企业组织关键业务中断，攻击者的赎金要求亦是逐年增高。根据公开报告收集的数据分析显示，2017 年在迅速蔓延的 WannaCry 勒索软件赎金仅为 300 美元，目前勒索软件要求企业支付的赎金则动辄在几百万美元；REvil 勒索软件在 2019 年前后出现，索要金额仅 7000 元人民币，次年该团伙的勒索金额已动辄千万美元以上。除逐年上涨、且不可预估的赎金费用外，被勒索攻击影响企业还需支付检测评估、多方通告、业务损失和响应成本等诸多费用，近年许多企业采购了网络安全类保险，可覆盖部分损失。

（四）勒索软件经历萌芽期、发展期，目前已正式进入高发期

勒索软件攻击发展过程可以大体分为三个阶段，萌芽期、活跃期高发期。



数据来源：公开材料整理

图 2 勒索软件攻击发展概述

一是 1989 至 2009 年，为勒索攻击的**萌芽期**。1989 年全球第一个的勒索软件 AIDS（PC Cyborg），由哈佛大学毕业的 Joseph Popp 创建，该木马会替换系统文件，隐藏磁盘目录，加密 C 盘的全部文件，从而导致系统无法启动，但因极易被破解，未引起过多关注。在随后 20 年中，勒索攻击处于起步阶段，勒索攻击软件数量增长较为缓慢，且攻击力度小、危害程度低。2006 年出现的 Redplus 勒索软件是国内出现的首款勒索软件，可隐藏用户文档，弹出窗口勒索赎金，金额从 70 元至 200 元不等。2006 年出现使用 RSA 非对称加密算法勒索软件 Archievus，使加密的文档更加难以

恢复。2009 年，俄罗斯出现首个锁机勒索软件，主要针对移动用户，并于 2010 年传播到世界其他地区。

二是 2010 年至 2015 年，勒索软件进入**活跃期**，几乎每年都有变种出现，其攻击范围不断扩大、攻击手段持续翻新。2013 年以来，越来越多的攻击者要求以比特币形式支付赎金；2014 年出现了第一个真正意义上针对 Android 平台的勒索攻击软件，标志着攻击者的注意力开始向移动互联网和智能终端转移。

三是 2015 年以后，勒索攻击正式进入**高发期**，勒索软件的影响力和破坏力都在不断增长，已经成为行业一致认可的最大的网络威胁之一。2015 年，第一个勒索软件即服务“TOX”勒索软件工具包出现，勒索软件即服务（RaaS）正式面世。2017 年 WannaCry 勒索攻击在全球范围内大规模爆发，使黑客认识到了将勒索软件与蠕虫病毒相结合可带来巨大破坏力，此后大量黑客开始研发和使用勒索软件，影响程度不断提高，至少 150 个国家、30 万名用户受害，共计造成超过 80 亿美元的损失，至此勒索攻击正式走入大众视野并引发全球关注。2018 年起勒索软件攻击技术逐渐成熟，出现了由病毒制作者、攻击实施者、传播渠道商、收款代理商组成的黑色产业链条。2019 年，Megacortex 勒索软件传播，它不仅加密用户文件，同时窃取用户信息，多重勒索模式正式流行。2021 年起勒索大事件频出，美国最大成品油管道运营商 Colonial Pipeline 公司遭到 Darkside 勒索软件攻击事件，对全球产业链产生巨大连

锁影响。

（五）勒索软件攻击流程各个阶段日益专业化

勒索软件攻击流程主要包括五个部分。

第一为初始访问阶段。勒索软件攻击最常见的访问媒介为存在漏洞的边缘设备，如虚拟化设备、VPN 和服务器等。攻击的账户来源于第三方数据泄露、网络钓鱼、针对远程桌面协议（RDP）的暴力凭证攻击以及从暗网中购买等手段获取的凭据等。根据初始访问向量，通过特定工具下载到设备上，建立交互式访问。

第二为扫描和获取凭证阶段。攻击者对受感染的系统扫描以更好地了解设备和网络，然后确定可以用于进行双重或三重勒索攻击的目标文件，攻击者还会利用各种攻击手法在目标网络**横向扩散**，以此将勒索软件传播到更多的设备。

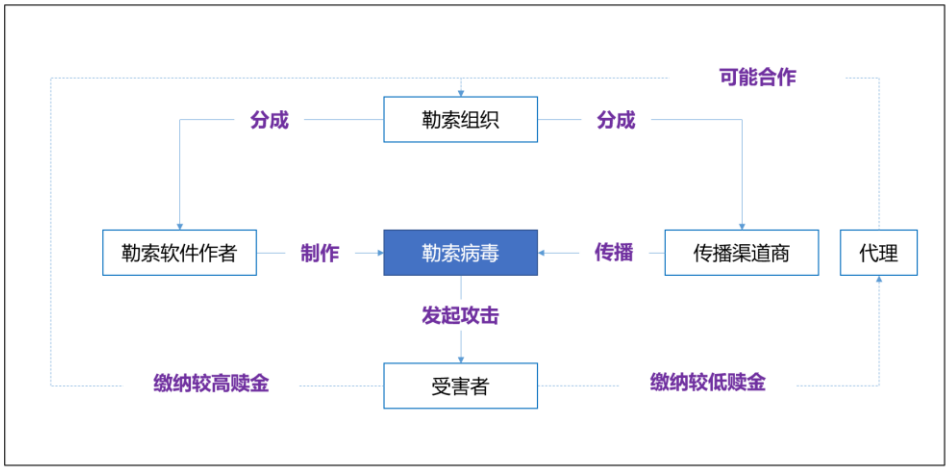
第三为部署攻击资源阶段。根据发现的网络攻击突破口，部署相应的网络攻击资源，在目标中部署攻击者可操纵的远程访问工具，获取攻击目标网络和系统的访问权限，并通过使用特权账户、修改域策略设置等方式提升自身权限，以渗透入侵组织内部网络。

第四为勒索软件运行阶段。勒索软件运行后，会对文件开始识别和加密，禁用系统恢复功能并删除或加密受害者计算机或网络上的备份数据，加密方式一般会采用非对称式加密方式，攻击者将保留私钥。

第五为实施勒索阶段。一旦文件被加密或设备被禁用，勒索软件就会向受害者发出感染警告，通常做法是在文件目录和计算机桌面上释放勒索信，勒索信将说明如何支付赎金，通常使用加密货币或类似的无法追踪的方法用于换取解密密钥或恢复数据。在多重勒索策略盛行的现行阶段，攻击者在此阶段会对有价值的数据进行加密和威胁。

（六）勒索攻击黑色产业链逐渐完善化，层次分明，分工明确

随着勒索产业的迅速发展壮大，通过围绕数据加密，数据泄露，乃至诈骗等核心元素展开的勒索软件攻击黑色产业链逐渐完善。其中典型的勒索软件作案实施过程如下，一次完整的勒索可能涉及 5 个角色，且一人可充当多个角色，包括勒索软件作者，勒索者，传播渠道商，代理，受害者。



数据来源：公开材料

图 3 勒索软件攻击黑色产业链

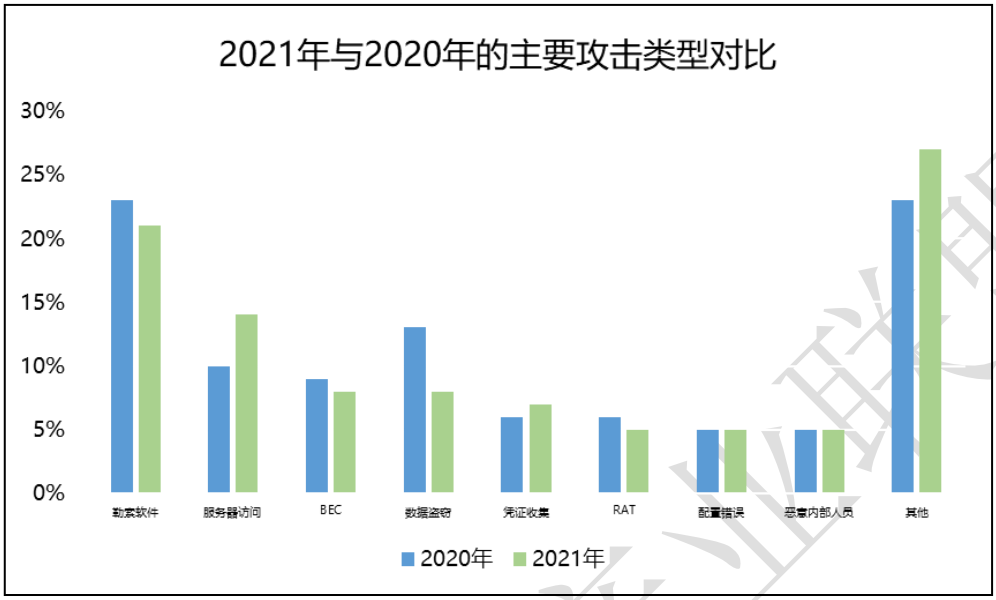
第一是勒索软件作者，负责勒索软件编写制作，与安全软件免杀对抗。通过在“暗网”或其它地下平台贩卖病毒代码，接受病毒定制，或出售病毒生成器的方式，与勒索者进行合作拿取分成。**第二是勒索组织，**从病毒作者手中拿到定制版本勒索软件或勒索软件原程序，通过自定义病毒勒索信息后得到自己的专属病毒，与勒索软件作者进行收入分成。**第三是传播渠道商，**帮助勒索者传播勒索软件，最为熟悉的则是僵尸网络。**第四是代理角色，**向受害者声称自己能够解密各勒索软件加密的文件，并且费用是勒索赎金的一半甚至更少，但实际上与勒索者进行合作，在其间赚取差价。从世界范围内看，勒索软件产业链衍生出了大量从事解密代理的组织，这些人直接购买搜索关键字广告，让勒索软件受害企业通过他们完成解密交易，解密代理充当了中间人的角色，从中获取大量利益。**第五是受害者，**通过勒索软件各种传播渠道不幸被勒索的受害者，如有重要文件被加密，则向代理或勒索者联系缴纳赎金解密文件。

二、 勒索软件攻击现状

（一）近期勒索软件攻击事件频发，已引起广泛关注

勒索软件攻击已成为网络安全得最大威胁之一。根据《X-Force 威胁情报指数 2022》，勒索软件攻击已成为网络安全中数量最多的攻击类型，但占比从前年的 23%下降到去年的 21%，但勒索软件攻击仍处于所有网络攻击中的第一位，并且攻击总量逐年上

升，2021 年已达 6.233 亿，自 2019 年以来上升比率达到 232%。



数据来源：X-Force 威胁情报指数 2022

图 4 2021 年与 2020 年主要攻击类型对比

2022 年勒索软件攻击持续活跃，有组织的勒索软件攻击愈发频繁，备受瞩目的勒索软件攻击事件，造成了巨大的金钱损失和负面社会影响。通过回顾近期发生的典型的勒索软件攻击安全事件。可以了解这一类型网络攻击导致的风险，从而更好地预见网络威胁的演变和发展趋势，以采取有效应对措施保障企业和组织的信息安全。勒索软件攻击事件汇总见附录 1 2022 年全球勒索软件攻击重要事件汇总以及附件 2 2022 年我国勒索软件攻击重要事件汇总。

（二）勒索软件攻击形式与传播渠道不断发生着变化

勒索软件发展至今，勒索攻击形式与传播渠道不断发生着变化。

1. 勒索软件攻击分类形式多样，日益进化

因产业内对勒索软件的分类方式较多，本报告对根据受害者采取的措施的主要分类方式进行阐述，不对各种分类形式进行赘述。根据勒索软件对受害者采取的措施进行分类，当前勒索软件分类主要有如下几种：加密勒索软件、锁机勒索软件、恐吓软件、MBR 勒索软件和擦除性勒索软件。

一是加密勒索软件，将加密个人文件和文件夹。受影响的文件一旦加密就会被删除，用户通常会在与现在无法访问的文件同名的文件夹中遇到带有付款说明的文本文件。**二是锁机勒索软件，**对计算机屏幕进行锁定并要求付款，阻止所有其他窗口，一般不会加密个人文件，锁定系统只允许有限的访问，以与攻击者进行交换。**三是恐吓软件，**恐吓软件可能会伪装成来自执法机构的信息，指控受害者犯罪并要求罚款，也可能伪造成合法的病毒感染警报，恐吓软件旨在说服用户下载无用的软件、破坏性的恶意软件或勒索软件。**四是主引导记录（MBR）勒索软件，**是计算机硬盘驱动器中允许操作系统启动的部分，将更改计算机的 MBR，以便中断正常的启动过程，赎金要求显示在屏幕上且防止操作系统的启动。**五是擦除或破坏性勒索软件，**将威胁被勒索用户若不支付赎金就破坏数据。

2. 勒索软件攻击传播渠道呈多样化不断发展

在勒索攻击传播方面，钓鱼邮件、安全漏洞、网站挂马、移动

介质是较为常见的方式，同时软件供应链、远程桌面也成为新的传播渠道。具体来看，**一是安全漏洞**，攻击者通过弱口令、远程代码执行等安全漏洞来入侵受害者内部网络，从而发起攻击。**二是钓鱼邮件，**攻击者把勒索软件内嵌在邮件文档、图片等附件中，或者将勒索恶意链接写入钓鱼邮件正文，诱发用户点击。**三是移动介质，**攻击者通过 U 盘、移动硬盘等移动存储介质，并创建移动介质盘符或图标等快捷方式，来骗过用户进行点击。**四是软件供应链，**攻击者利用用户对软件供应商的信任关系，通过软件供应链的分发和更新等机制来发起勒索攻击。**五是远程桌面，**攻击者利用弱口令、暴力破解等方式获取攻击目标服务器远程登录信息，进而通过远程桌面登录服务器植入勒索软件。

（三）勒索软件攻击不断演变发展进化，国内外存在一定差异

1. 勒索家族繁多，国内外活跃勒索团队存在差异化

全球勒索软件家族繁多，据不完全统计，目前有近 2000 个勒索软件家族，对于勒索软件防范工作带来巨大挑战。

全球方面，根据 Coveware 2022 年前三季度勒索软件事件响应趋势报告数据显示，按照勒索团伙赎金所占市场份额进行排名，国外勒索事件中，勒索软件家族主要有 BlackCat、Hive、Black Basta、Dark Angels、Phobos、Vice Society、AvosLocker、

Lockbit、Quantum、Conti、Karakurt、suncrypt、Deadbolt 等。

Most Commonly Observed Ransomware Variants in Q2 2022

Rank	Ransomware Type	Market Share %	Change in Ranking from Q1 2022
1	BlackCat	16.9%	+2
2	Lockbit 2.0	13.1%	-
3	Hive	6.3%	+1
4	Quantum	5.6%	New in Top Variants
4	Conti V2	5.6%	-3
5	Phobos	5%	+2

Most Commonly Observed Ransomware Variants in Q3 2022

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2022
1	BlackCat	15%	-
2	Hive	13.5%	+1
3	Black Basta	6%	+2
4	Dark Angels	3.8%	New in Top Variants
4	Phobos	3.8%	+1
5	Vice Society	3%	New in Top Variants
5	AvosLocker	3%	-

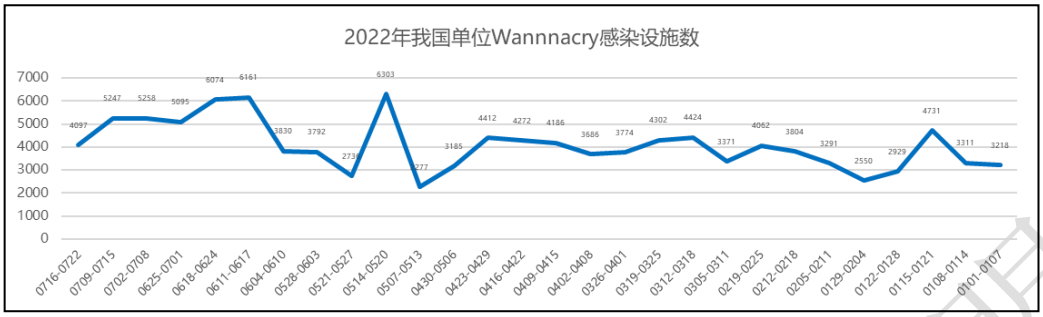
Most Common Ransomware Variants in Q1 2022

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2021
1	Conti V2	16.1%	-
2	LockBit 2.0	14.9%	-
3	BlackCat	7.1%	New in Top Variants
4	Hive	5.4%	-1
5	AvosLocker	4.8%	+1
6	Karakurt	4.1%	-
7	Phobos	3.0%	New in Top Variants

数据来源：Coveware

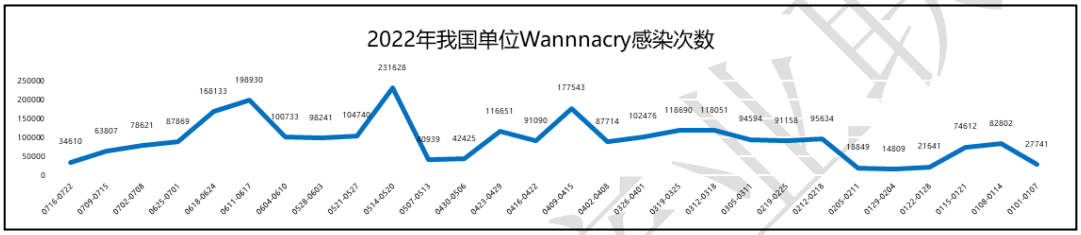
图 5 全球勒索软件家族市场份额排名（2022 年 Q1-Q3）

国内方面，根据公开资料对我国 1 月至 7 月的勒索软件防护动态整理，Wannacry 因“永恒之蓝”漏洞（MS17-010）始终占据勒索软件感染量的榜首，反映了当前仍存在大量主机没有针对常见高危漏洞进行合理加固的现象，在 2022 年 5 月感染量猛增达到峰值，我国单位累计 Wannacry 感染设施数超过 11 万个，累计 Wannacry 感染次数超过 250 万次。



数据来源：公开数据整理

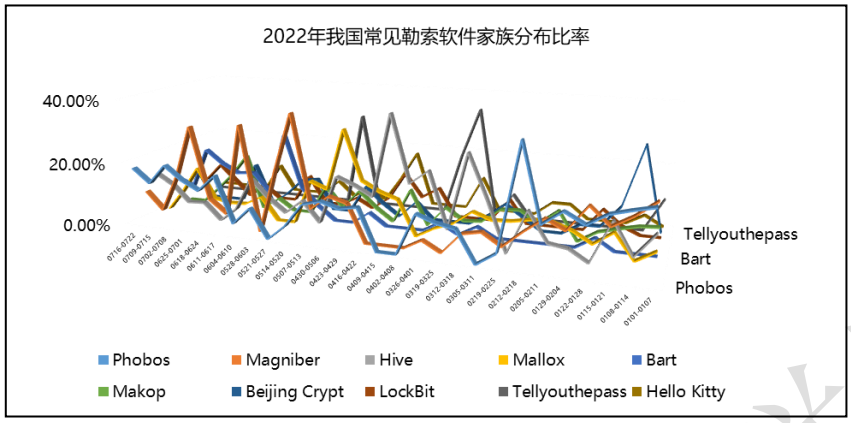
图 6 2022 年我国单位 Wannnacry 感染设施数



数据来源：公开数据整理

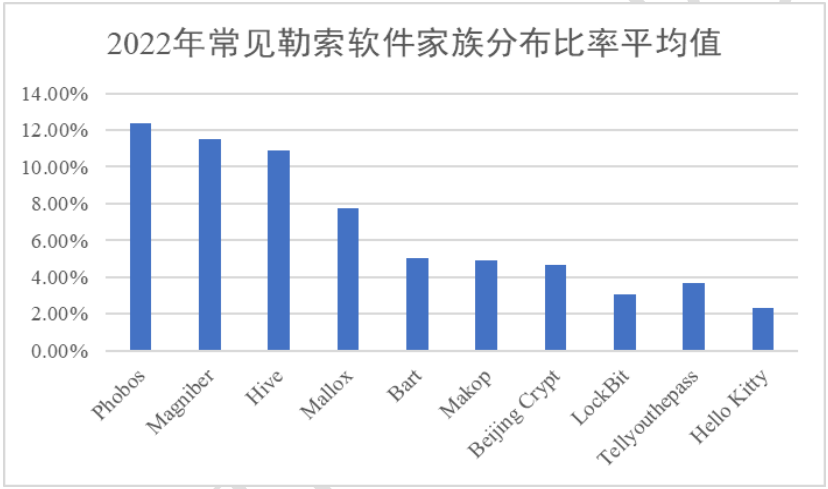
图 7 2022 年我国单位 Wannnacry 感染次数

国内其他勒索软件攻击情况，根据公开资料对我国 1 月至 7 月的勒索软件防护动态整理，2022 年常见勒索软件家族流行趋势时刻变化，如下图所示，分布比率较高的勒索软件家族为 Phobos、Magniber 、 Hive 、 Mallox 、 Bart 、 Makop 、 Beijing Crypt 、LockBit、Tellyouthepass、Hello Kitty。



数据来源：公开数据整理

图 8 2022 年我国常见勒索软件家族分布比率



数据来源：公开数据整理

图 9 2022 年我国常见勒索软件家族分布比率平均值

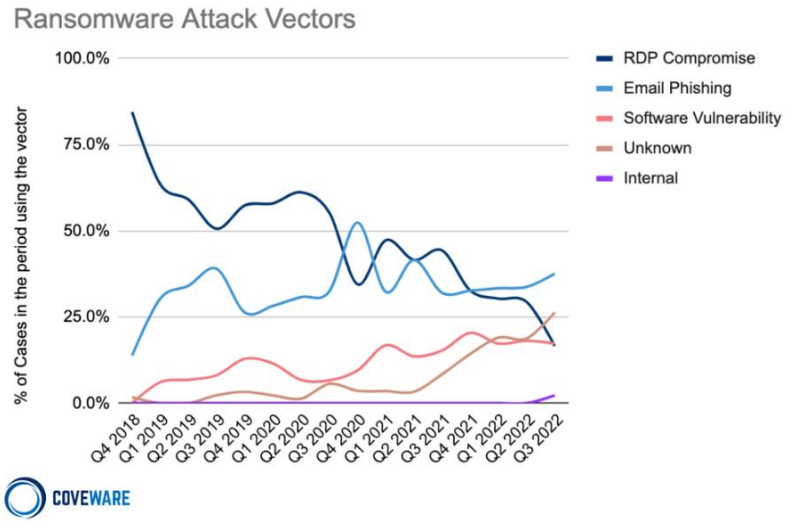
总体上境内外流行的勒索家族分布存在差异。差异表现在国内外活跃勒索家族不同，且分布占比情况存在差异。国外极其活跃的勒索家族 Conti 在国内并不活跃，Conti 组织一向以高赎金勒索闻名业内，由于境内外监管机制和虚拟货币环境等因素不同，使得境内外活跃勒索家族分布不同。

Phobos 因其攻击方式的通用性、系统的兼容性及传播的广泛性等综合因素得以在国内外流行。勒索软件 Phobos 在国内外均保

持着很高的活跃度。其不断推出新变种，并频繁通过 RDP 暴破、钓鱼邮件等方式进行攻击，windows 和 linux 系统均会受到影响。Phobos 传播性广，影响范围大，且无解密工具，危害性极大。

2. 攻击手段趋于多样化，钓鱼邮件逐渐取代 RDP 爆破成为主要入侵方式

全球方面，根据 Coverware 数据分析，钓鱼邮件、RDP 爆破、漏洞利用是目前全球范围内勒索软件攻击最主要的入侵方式。自 2021 年下半年至今，钓鱼邮件逐渐取代 RDP 爆破方式，成为勒索软件攻击的主要入侵的最主要方式。

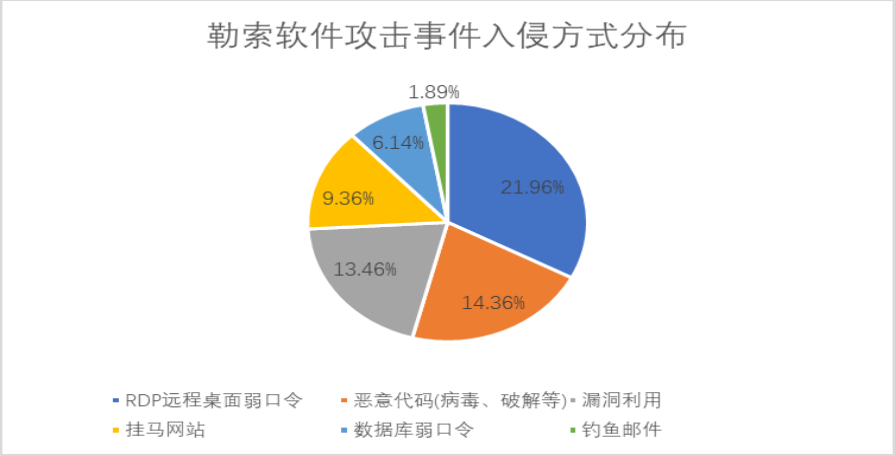


数据来源：Coveware

图 10 2022 年全球勒索软件入侵方式分布

根据公开资料显示，国内与国际上的勒索软件攻击入侵方式上存在一定差异，RDP 爆破的入侵形式在国内更为流行，其次为恶意代码、漏洞利用、挂马网站、数据库弱口令，其他入侵方式还包

括暴力破解、共享加密、Powershell 攻击、VPN 登录、Web 入侵等等。



数据来源：公开数据整理

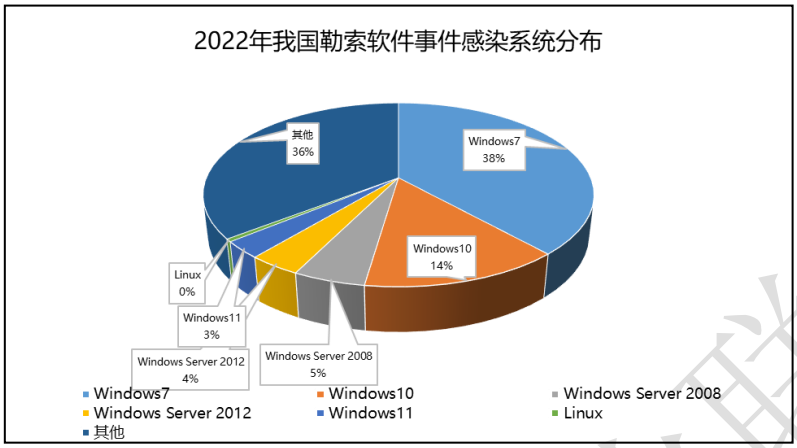
图 11 2022 年我国勒索软件入侵方式分布

3. 勒索软件攻击系统目前仍主要是 windows 系统，有转移上云的趋势

勒索软件攻击系统分布仍主要是 windows 系统。windows7 系统和 windows10 系统占比超过 40%，此外，Linux 系统也遭到一定程度的勒索软件攻击。

勒索软件攻击有转移云上的趋势。随着数字化转型的浪潮来临，越来越多的企业逐渐将业务上云，云上承载着企业的关键业务和重要数据，掌握着企业的命脉，其数据价值高，数据集中，往往成为勒索团伙攻击的首要目标。云上数据存储一般多使用 Linux 系统，也遭到了一定的勒索软件攻击。勒索软件攻击本质上为获利的一种方式，企业的关键业务所在即会成为犯罪团伙的攻击目标，勒

索团伙追求获利的本质，使得勒索攻击有着转移上云的趋势。



数据来源：公开数据整理

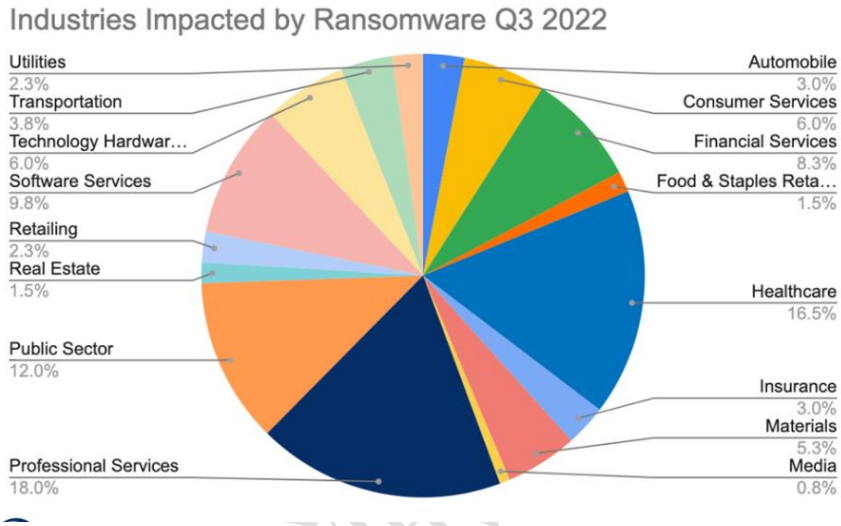
图 12 2022 年我国勒索软件事件感染系统分布

4. 国内与国际上的勒索软件重点攻击行业不尽相同，制造业等行业已成为我国勒索软件攻击的主要行业

勒索攻击者更倾向于针对那些在经济上对攻击有利的公司，而不分行业。勒索软件攻击者仍然主要针对小型/中型企业进行攻击。多数攻击团队试图找到一个平衡点，既不攻击巨头公司，导致影响过大从而被逮捕等额外的高风险，但也不攻击非常小型的公司，使他们无法获得足够的赎金收益。同时，因为中小型企业更有可能在网络安全方面投资不足，从而更容易成为勒索攻击目标。

全球方面，由 Coverware 数据分析，医疗健康、专业服务、软件服务业、金融行业、科技硬件为全球勒索软件攻击的主要目标行业。传统意义上来说，大多数勒索软件攻击目标与行业无关，勒索软件攻击更以从经济角度来讲有利于攻击的公司为目标，而

不将行业作为攻击的考虑维度。经过对 2022 年前两个季度的数据分析，一些 RaaS 团体会避开某些行业，例如某些医疗保健组织（如医院）。但是，在 2022 年第三季度，Hive 勒索软件的流行增加导致对医疗保健组织的攻击增加。



数据来源：公开数据整理

图 13 2022 年全球常见行业受勒索软件攻击分布图

国内方面，根据公开资料分析，国内与国际上的重点勒索软件攻击目标行业不尽相同，医疗行业、科技行业、制造业、电信行业、政府部门、教育科研机构、为我国勒索软件攻击的主要目标行业，勒索形式不容乐观。

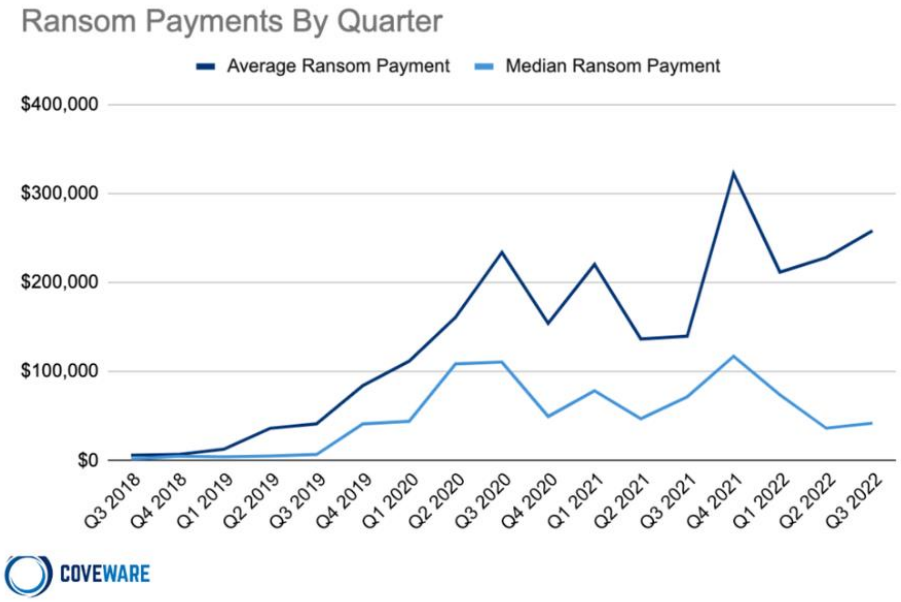
制造业已成为网络攻击的重灾区。根据《X-Force 威胁情报指数 2022》，制造业取代金融业，成为 2021 年遭受攻击最多的行业，占到 23.2%。勒索软件是其中最主要的攻击类型，占制造业组织所遭受攻击的 23%，这凸显了勒索软件正将制造业视为主要攻击目标。随着制造业数字化转型加快，其原本封闭的网络和业务系

统更加开放，以工业控制系统为例，由于设计之初没有考虑到海量异构设备以及外部网络的接入，随着物联网开放性日益增加、远程监控和远程操作加快普及，网络攻击者更容易利用系统漏洞发动远程攻击和针对运营管理中存在的薄弱环节发动入侵，一旦成功即可造成多达数十亿台设备的集体沦陷，导致生产中的海量数据被加密和盗取，并中断生产业务以达到勒索钱财的目的。

5. 勒索软件攻击平均赎金金额增加，但是中值减少

勒索软件攻击事件的赎金金额呈全面上升趋势。攻击者从他们认为有能力支付的企业索取高额金额，故不同的行业之间存在一定差异。

勒索软件攻击逐渐向中端市场转变。RaaS 附属公司和开发人员向中端市场转变，中端市场的攻击回报风险是比超高赎金类攻击的成功率更高且风险更低。大型组织在被索要超高赎金情况下拒绝支付的比率呈增长趋势。根据 Coveware 报告数据显示，2022 年第二季度与第一季度相比，平均赎金支付增加了 8%，达到 228,125 美元，赎金支付的中位数实际上下降到 36,360 美元，比 2022 年第一季度下降了 51%。2022 年第三季度与第二季度相比，平均赎金支付增加了 13.2%，达到 258,143 美元，但赎金支付的中位数实际上增加到 41,987 美元，比 2022 年第二季度增加了 15.5%。



数据来源：Coveware

图 14 2022 年勒索软件支付赎金均值及中间值折线图

三、 勒索软件发展态势

各行各业面临着网络安全风险的巨大挑战。新冠疫情不仅造成市场压力，还宣告着远程办公时代的到来。无论企业规模大小，都在迅速对工作环境进行着变革，绝大多数工作都转向线上活动，大量员工远程协作，其迁移速度和规模十分惊人，转变的背后潜在着巨大的网络风险，因为随之而来的就是网络暴露面大大增加，但企业往往很少考虑安全问题。攻击事件频繁发生，各行业和各地区均面临着巨大的风险。

随着勒索攻击专业化、团队化运作，勒索攻击逐渐发展出新的发展态势。后疫情时代，勒索攻击手段日趋成熟、攻击目标越发明确，模式多种多样，攻击愈发隐蔽，更加难以防范，危害也日益增

大。

（一）影响广泛：影响社会正常运转且难解密

首先，勒索软件攻击对社会正常运转带来较大挑战。一是在民生方面，大型企业遭到勒索攻击严重影响民众正常生活。2021 年 5 月全球最大的肉类供应商 JBS 遭到勒索软件攻击，部分牛羊屠宰加工厂停摆，美国肉类批发价格出现上涨，使得本就受到疫情冲击的全球食品供应链更受打击。**二是在医疗卫生方面，**勒索攻击不但造成巨额经济损失，同时也威胁到病人生命安全。2020 年 9 月，德国杜塞尔多夫医院 30 多台内部服务器遭到勒索攻击，一位前来寻求紧急治疗的妇女被迫转送至其他医院后死亡。这是公开报道的第一起因勒索攻击导致人死亡的事件。**三是针对关键信息基础设施与工控系统的攻击日逐显现，**关键信息基础设施一旦遭到破坏，丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益；工业企业网络环境中网络连接形成了暴露面，攻击者可通过企业信息网络侵入将勒索软件传播到工控网络中，进而导致工业控制系统无法运行。

其次，勒索攻击使用的加密手段越来越复杂多样。绝大多数勒索软件攻击事件不能被解密，因攻击所用的非对称加密算法的密钥长度长且很难被反向破解。受害者往往需要在支付巨额赎金和数据恢复重建中做出选择。即使一些勒索攻击采用的加密算法是公开

的，但是依靠现有算力或通过暴力破解的方式也难以进行解密，因为暴力解密往往需要极长的时间。

最后，勒索攻击者逐步将攻击范围向学校及儿童数据隐私领域拓展。根据公开数据统计，2021 年美国有 1200 多所学校的数据被勒索攻击团队窃取并公布。泄露的信息包括学生的出生日期、种族、社保号码、性别等，甚至还包括是否为移民、是否无家可归、是否家庭条件较差等更多信息。勒索攻击者利用学生的数据来尝试办理信用卡和申请汽车贷款等方式进行获利。

（二）隐蔽变异快：为勒索防护提出巨大挑战

自勒索软件攻击初次出现，便呈现出与传统网络攻击不同的特点，传统的网络安全防护措施在应对勒索攻击时略显无力。面对全球范围内爆发式增长的勒索攻击事件，熟悉勒索攻击的隐蔽性和变异性将有助于应对此类攻击。

一是隐蔽性强已成为勒索攻击的典型策略。勒索攻击善于利用各种伪装进行入侵，为保持高隐蔽性，部分勒索攻击还会采取智能攻击策略，攻击事件可能在潜伏一段时间之后再引入第一个恶意软件版本，潜伏时间较长也印证了勒索攻击的高隐蔽性。攻击方可利用尚未被发现的网络攻击策略、技术和程序，不仅将后门偷偷嵌入代码中，而且可以与被感染系统通信而不被发现。这些策略、技术和程序隐藏极深且很难完全从受感染网络中删除，为攻击活动细节

的调查取证和后续的清除工作带来巨大的挑战。

二是勒索软件变异较快且易传播。目前活跃在市面上的勒索软件种类繁多，而且每个家族的勒索软件也处于不断地更新变异之中。变体的增多除了借助信息技术的飞速发展以外，还与网络攻击者“反侦查”意识的增强相关。很多攻击者不断改进勒索软件变体以逃避侦查。此外，蠕虫式传播型勒索软件可进行自我复制、自主传播，传播速度更快，波及范围更广。例如，爆发于 2017 年的 WannaCry，在全球范围蔓延的同时也迅速出现了新的变种，变种不能通过注册“开关域名”来遏制传播，因而传播速度变得更快

三是勒索攻击路径和目标多元化发展。首先，勒索软件攻击路径正在由被动式攻击转为主动式攻击。随着远程办公场景加快普及并生产海量数据，网络攻击者更容易利用系统漏洞发动远程攻击。除了针对运营管理中存在的薄弱环节，勒索攻击还在设备安装过程中利用内置漏洞进行横向渗透。**其次，勒索攻击目标呈现多元化发展。一方面，**是从电脑端到移动端。勒索软件大多以电脑设备为攻击目标，其中 Windows 操作系统是重灾区。但随着移动互联网的普及，勒索攻击的战场从电脑端蔓延至移动端，并且有愈演愈烈的趋势。**另一方面，**是从个人用户到企业设备。个人设备在勒索软件攻击目标中一直占据较高比例，但随着传统勒索软件盈利能力的持续下降，对更高利润索取的期待驱使网络攻击者将目标重点聚焦在政府或企业的关键业务系统和服务器上。

（三）勒索攻击 SaaS 化：RaaS(Ransomware-as-a-service)勒索即服务模式兴起

勒索软件即服务（RaaS）商业模式的兴起使得从业者无需任何专业技术知识就可以发起勒索攻击活动。RaaS 模式大大降低了攻击的技术门槛，这也成为导致勒索软件攻击泛滥的重要原因。近年来，Lockbit、conti、DarkSide 和 Black Basta 等勒索软件即服务的成功，进一步推动了 RaaS 的发展。

勒索软件黑色产业层级分明，全链条协作。开发者只需要更新病毒，拓展传播渠道大肆释放勒索软件，各级分销参与者点击鼠标就能从中瓜分利润。这种黑色产业分销模式大大降低了勒索攻击的传播门槛，使网络安全风险快速扩散。总体来看，RaaS 商业模式下的攻击将带来三个方面的优势:

第一，攻击呈系统化发展，实现“开箱即用”的便捷性。勒索攻击从制作、传播、攻击到收益呈现系统化、便捷化，开发者可提供一整套解决方案，甚至可包括利用加密货币进行赎金支付等服务。犯罪分子获得勒索软件后，可通过多种渠道进行传播并获利，攻击模式更为便捷。

第二，攻击门槛大幅降低。攻击者往往并不需要任何编程技术就可以开展违法犯罪活动，理论上任何人只要支付少量费用即可通过 RaaS 服务开展勒索攻击，导致网络攻击的门槛大幅降低。

第三，实现价值多向变现，黑客团伙除自身发动勒索攻击外，还会借由暗网和虚拟货币技术，对外出租或售卖成熟的勒索软件产品和服务，促使勒索“产业链”逐渐形成，上下游相互协作配合，共同瓜分勒索收益。

第四，进一步增强勒索攻击能力和隐蔽性，不同勒索软件团伙之间开始着手构建具有精准配合关系的勒索商业联盟，通过共享受害者信息等手段，扩大勒索商业模式。

（四）跨平台勒索：提升勒索软件利用

勒索软件逐渐发展为可在不同的架构和操作系统组合上运行，提升勒索软件利用率，进而获得更多经济利益。在过往的攻击中，Windows 平台的勒索攻击依然是最为常见的。但是针对 Linux，MacOS 等其它操作系统的勒索攻击越来越频繁，而被打击的目标，也不再只局限于计算机，各种嵌入式设备、专用设备上也被曝出受到勒索软件攻击影响。近年来 Big Game Hunting (BGH)计划呈流行趋势，网络犯罪分子已经渗透到运行着各种系统环境中。随着环境的愈加复杂，为了造成尽可能多的损害并使恢复变得更加困难，攻击者尝试加密尽可能多的系统。例如：Rust 或 Golang 等“跨平台编程语言”编写勒索软件已然成为一种趋势；BlackCat 的 Linux 示例与 Windows 示例非常相似，在其运行的不同平台上仍然具有相同的功能。

（五）漏洞武器化：促进勒索软件发展

漏洞武器化已然成为勒索攻击的又一重要途径。攻击方对漏洞的掌握与防守方对漏洞的修补始终是一个相互追赶博弈的过程，每一次的大范围勒索事件大多伴随着一些新型漏洞利用工具，漏洞中除了 0day 漏洞外，不乏已知漏洞，甚至是披露很久的漏洞，它们能够被勒索攻击利用原因一方面是没有及时的进行修复，另一方面随着系统版本的更新、组件代码调整而导致新漏洞的出现，或者原先很难被利用的低危漏洞成为容易沦陷的关键点。勒索组织借助漏洞进行攻击，攻击面和攻击效率得到了较大提升。如 Log4j 漏洞的爆发，多个勒索组织利用该漏洞进行大规模攻击。

（六）加密货币普及：助推赎金快速增长

勒索攻击的制造者对赎金的要求越来越高。2017 年在全球 140 多个国家和地区迅速蔓延的 WannaCry 勒索软件赎金仅为 300 美元，4 年后勒索软件要求企业支付的赎金则大多在上百万美元，

加密货币一定程度上助推了赎金的快速增长。早期的网络攻击想要套现，需要冒险尝试很多不同的路径。但由于被盗取的数据往往很难找到支付意愿高的买家，这种模式运行起来并不理想。此外，多年前就有网络攻击者尝试勒索模式，但当时银行转账方式极易暴露其犯罪行为，成功率不高。随着加密货币成为近年来社会关注的焦点，尤其是加密货币的匿名化和难以追溯性导致监管部门很

难对其进行管理。犯罪分子利用加密货币这一特点，将其与网络勒索攻击结合起来，有效隐匿其犯罪行径，导致网络攻击门槛降低、变现迅速、追踪困难，一定程度上助推了网络犯罪快速增长。对于支付方式来说，目前越来越多的勒索团伙开始抛弃比特币，选择如门罗币、达世币等其它虚拟货币做替代，这一变化与各国对比特币的监管不无关系。

反之，区块链探索器可以帮助调查人员跟踪区块链内部的资金流动。因为重要的地址和交易已经确定。在尖端技术的帮助下，监管单位可以利用区块链取证技术从区块链中抓取交易数据并分析其是否存在非法活动，有效的打击勒索软件活动。

（七）APT 定向化：大型企业和基础设施是重点

近年来勒索软件攻击定向精准攻击趋势明显。传统勒索软件攻击者使用无差别攻击的形式，很难预测受害者的价值。近年来，勒索攻击对象涉及面越来越广，目前主要针对掌握大量数据的大型企业，且定向精准攻击趋势愈发明显，勒索攻击日趋 APT 化。APT 化指的是对目标企业进行“量身定做”，从低权限帐号入手，持续渗透攻击，直到控制企业核心服务器，再释放勒索软件，使巨型企业彻底瘫痪。

勒索对象主要集中于大中型企业和基础设施类组织。原因主要是两点：**一是**此类企业和组织对信息化依赖程度相对较高，而网

络安全能力相对不足，使得勒索成功率较高；**二是**遭受攻击后其受影响程度比较深，而支付意愿和能力较强，有更大的可能缴纳赎金。

（八）多重勒索：引发数据泄露风险

多重勒索模式已成为现今网络攻击者实施攻击的重要手段。勒索攻击已经从单纯的支付赎金即可恢复被加密的数据，逐渐演变成先窃取商业信息和内部机密，而后威胁企业不缴纳赎金将公开数据，在此基础上，攻击者还威胁受害者如果不支付赎金就会发动“拒绝阻断服务攻击”，使得受害者服务器超负荷运转，直至服务器瘫痪。这种新模式也被称为“多重勒索”。不仅使得勒索攻击杀伤性增强，被勒索企业缴纳赎金的可能性变大，诱使勒索攻击者发动更多攻击，而且极易引发大规模的行业内部数据泄露事件，使得受害企业同时承受数据公开、声誉受损、行政处罚等多重压力。这种情况下，如果受害者不支付赎金不仅仅数据难以解密，还将面临信息被公布或者被拍卖出去的危险，给企业或机构造成较为复杂的外部危害。尤其是随着互联网的大面积普及，大量企业的安全事件短时间内即可在网络中大肆传播开来。多重勒索的机制，在一定程度上，也改变了勒索攻防的游戏规则。以往注重时候查杀恢复，数据备份的思路，在多重勒索面前已经无法真正奏效。真正从源头预防，才能彻底化解勒索风险。

勒索软件产业链出现成熟的第三方数据泄露平台。勒索攻击者发现以加密数据为威胁获得的赎金，已经远不如以泄露数据相要挟而获得的赎金多。一方面是因为个人、企业或政府机构对于数据保密的重视程度逐年提升，另一方面是因为各国政府对数据泄露的惩罚越发严厉。而从威胁程度上来看，数据加密虽然难解，但还有可能通过备份等方式进行恢复；可一旦重要数据资料遭到泄露，对于某些受害者来说将会是毁灭性的打击，尤其是尚处在保密阶段的新产品、新研究成果相关的数据。于是，勒索软件的组织者们也开始调整策略，从加密向泄密“转型”。

（九）供应链渗透：成为勒索攻击重要切入点

供应链攻击作为一种新型攻击手段，凭借自身难发现、易传播、低成本、高效率等特点已成为最具影响力的高级威胁。一是供应链攻击涉及诸多企业，难以控制恶意软件波及的范围，无差别攻击成为供应链勒索攻击的重要特征。**二是大型软件供应商成为潜在被攻击对象。**当前受到攻击的软件供应商规模不大，一旦大型企业遭受到供应链勒索攻击，将造成难以想象的严重后果。**三是针对供应链的勒索攻击，目前难以找到有针对性的解决方案，**即使供应链企业本身，也很难通过软件更新来防御恶意攻击，尤其是对于已经遭受恶意攻击的用户，修复打补丁为时已晚。

供应链攻击引发连锁效应将威胁巨大。一般利用产品软件官网

或软件包存储库等进行传播，网络攻击一旦成功攻陷上游开发环节的服务器，便会引发连锁效应，波及处于供应链中下游的大量企业、政府机构、组织等。由于被攻击的应用软件仍然来自受信任的分发渠道，恶意程序将随着软件的下载安装流程悄无声息地入侵目标电脑，逃避传统安全产品检查的同时又可沿供应链发动向后渗透攻击，大大增加安全检测的难度。

未来，供应链攻击将成为勒索软件攻击的重要入口。随着产业链上下游企业数字化水平和效率的提升，更多企业打通上下游数据链条，合作程度加深，产业链安全防护能力取决于产业链中安全最薄弱环节或企业，安全风险开始向更广范围和更基础领域扩散。

如何阻止软件供应链攻击，是全球面临的共同挑战。根据公开数据整理，2022 年多起勒索事件因供应链攻击遭到重大损失，供应链涉及多个企业，攻击方为提高投资回报率，通过一次攻击获得多笔赎金。商品化的恶意软件泛滥和大量已知漏洞仍然是持续存在的问题。

（十）处置专业化：增强勒索攻击防护能力

伴随着勒索攻击的不断增长，国内的勒索处置逐步专业化。以往的勒索软件处置，多属于被攻击公司和安全公司应急响应的一部分，由安全运维团队兼职处理。随着勒索软件攻击事件的常态化，勒索处置团队已成为安全公司的必备团队，市面上也开始出现专项

代理处置勒索软件解密业务的解密公司。安全公司的处置业务也由之前的查杀病毒，逐步扩展为：协助企业恢复生产，溯源排查，安全加固，解密咨询等，服务更趋专业化。

勒索软件的防护能力，已成为企业和个人选择安全产品的一个重要关注点。在安全产品方面，不论是终端安全产品，还是网络监测产品，亦或是安全情报，数据备份产品，均突出了勒索防护功能。

在各类产品的配合加持下，勒索处置的规范化已有显著提升。部分厂商推出了勒索求助热线，反勒索服务，勒索软件查询引擎，解密大师等各类产品，勒索保险业务也在国内开始试点展开。用户不论是攻击前还是攻击后，均能够获取到有效的咨询和帮助。

（十一）全球治理：促进国际共同抵抗威胁

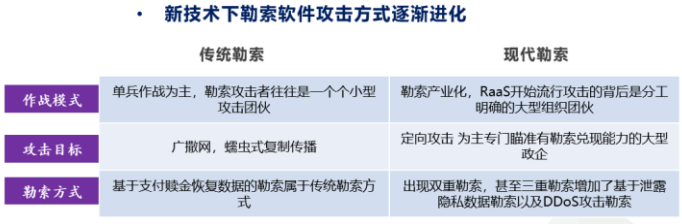
勒索软件威胁已经成为一个全球化的威胁，不是单独某个团体可以解决。网络攻击天然具有的国际化属性，勒索攻击也不例外。勒索软件的攻击目标从个别笔记本、个人电脑、服务器，到目前对医院、学校、政府机构和基础设施实施攻击，其影响力已经大大超越以往。勒索软件也已不单单是造成经济上的损失，它已经形成了对国家安全，公众生命健康安全的挑战。勒索软件攻击目标与意图也发生了复杂转变。勒索软件的这一变化，也使其受到了更多国家的关注，如美国已经连续举办两届国际反勒索大会。国内，主管部

门也发起过“勒索病毒的专项治理工作”，以加强机关单位对勒索病毒的重视程度与防护能力。

四、 勒索软件防护体系建设

（一）传统勒索软件攻击防护已效率不足，须推陈出新

传统备份式勒索防护软件对勒索软件的防护方式主要为从备份中恢复被攻击的系统。传统防护方式主要包括：**一是**缩短备份间隔，增加全备份次数，将备份存储在不同的介质上，并将其保留在不同的位置，至少一个副本位于异地，缺点为增加了资源、时间等各种成本，且效率不高。**二是**定期修补操作系统和应用程序，以关闭勒索软件可以利用的已知软件漏洞作为攻击媒介，缺点是增加了业务中断的可能性和停机时间。**三是**部署硬件防火墙等端点防御，以检测和阻止一些公开的勒索软件，缺点是增加了额外的部署成本。**四是**使用网络分段隔离技术（如 VLAN）阻止某些勒索软件变体在生产网络中传播蠕虫功能，缺点是增加了网络拓扑图的复杂程度。



数据来源：公开材料

图 15 新技术下勒索软件攻击方式逐渐进化

传统勒索软件防护方案已效率不足，须推陈出新。主要表现在以下四个方面。**一是单点防御难以抵抗多重攻击。**单点防御情况下，仅作用勒索软件攻击流程的某种方式，若突破或绕过防御则满盘皆输，病毒一旦进入内网可通过多种方式快速横向扩散。在遭受勒索软件的攻击后，检测、遏制、恢复、清理和攻击后取证、分析及报告期间，业务运营均会受到破坏性影响。**二是传统防护方案纵深防御差。**企业信息网安全纵深防御能力相对薄弱。如今勒索软件变种频繁，单纯依赖传统安全产品无法适应复杂多变的安全环境。极难应对人为攻击，找漏洞、打补丁的传统防御思路不利于整体安全。**三是防御措施未深入治根本。**终端的病毒攻陷现象只是表象，内在原因是因为病毒已经在内网扩散和蔓延，不阻止病毒的入侵和扩散，随着病毒内置杀软功能的普及，一旦终端防护软件失效，病毒肆虐只会更加猖獗，即使业务系统恢复后，也有可能导致再次感染。**四是缺少情报意识。**在当下安全形式瞬息万变，一条及时的情报足以改变战局。由于外部情报不及时、内部上下级情报不统一，导致系统存在安全短板，极大增加了被攻击的可能性。**五是应急响应滞后。**网络安全事件的损失通常与应急响应的反应速度是相关的，若因前期准备不足、员工安全意识缺乏导致中毒后没有意识到事件严重性，滞后的应急响应有可能导致二次损失。**六是产品堆叠使用，功能间无法有效联动。**产品集合不能从勒索软件的生命周期的原理入手，分析病毒的传播环节并定位所有感染主机，起到有效

防护。

数据来源：公开材料

图 16 勒索软件攻击防护常规流程

由于勒索攻击方法持续进化，以及勒索变种类型快速演进，传统数据备份、以及网络边界防护设备和依靠特征检测的传统杀毒软件在面对勒索攻击、APT 攻击等未知威胁时已经基本失效，网络安全安全行业应对勒索攻击要对其攻击形式进行全面且持续地研究，推出更适合企业自身特点的防御手段。

（二）勒索软件攻击防护体系日趋纵深防御发展

目前，勒索软件攻击防护体系主要为应基于事前、事中、事后，构建纵深的全流程防护体系，实现事前的防护、勒索事件发生后的持续监测、以及事后持续检测、快速响应以及安全加固。由于勒索软件攻击具有强对抗性，并没有一种方法可以单独有效解决，这也导致应对勒索攻击应是全面的防护体系才能予以应对。

注：由于报告篇幅限制，本报告将就勒索软件防护流程进行概

述分析，并会在下一年度的《勒索软件防护发展报告》2.0 以及后续《勒索软件攻击防护要求》相关标准中对此部分内容详细展开。

1. 事前防护体系建设

企业的事前防御体系建设主要包括员工培训教育与安全意识宣传、备份管理、主动防御、系统加固等多个部分。针对事前防御建设体系，本报告总结了几个关键词:

一是员工培训教育、安全意识宣传以及应急演练。第一，企业应分部门、角色进行定期网络安全培训，提升企业人员的安全意识。普通用户是各类钓鱼邮件、恶意软件攻击的入口，需要经常进行网络安全日常培训，甚至内部通过模拟方式进行演习强化。**第二，最好的防御措施是受过良好教育的用户。**尽管已具备软件限制策略和其他端点防御得多重保护机制，但恶意电子邮件或恶意链接的形式仍可入侵企业。在这种情况下，尽管措施仍然可以保护，但，能够识别可疑电子邮件并及时将其报告给 IT 部门进行调查。这种可疑的通信越早被报告，它们就越快可以被封锁在周边地区。**第三，日常应急演练可帮助企业在发生勒索软件事件后，做出正确响应的速度越快，遭受的损失越小。**开展模拟勒索攻击事件的应急演练工作，既能检验应急响应流程的合理性，又能让各协同相关部门和人员熟悉面对勒索事件发生时的应对方法，还能更好的优化落实物质条件、人力和技术支撑等保障措施。避免真实事件发生时处

理过程中出现混乱、无序状况，减少处理过程中错误的发生，从而避免不必要的损失。

二是加强备份管理，建立关键数据、系统的周期备份计划。创建勒索软件无法访问的防篡改备份副本，包括本地网络备份、离线备份、云备份。**其一是备份和恢复计划，**企业可为每个资产定义明确的恢复点、恢复时间目标。制定明确的政策和程序，以描述备份计划、数据应如何备份或恢复、谁负责备份和恢复等。**其二是配置存储快照，**以便在必要时可将卷回滚至受攻击前快照的先前状态。**其三是脱机备份，**为了在勒索软件事件后成功地从备份中还原数据，备份应进行脱机存储，以确保备份数据不会加密和不可恢复。磁带可用于存储环境中数据的多个历史时间点快照。**其四是备份和恢复测试，**备份和恢复应按常规计划进行成功测试，以确保所有系统正常工作，例行测试也会缩短恢复时间。**其五是对备份系统增加安全检测能力和恢复能力，**一方面对备份数据进行安全检测，确保备份数据本身的可用性、完整性、可恢复性，另一方面在恢复时应能快速恢复业务数据，企业业务连续连续性计划应能覆盖勒索软件攻击事件对各重要业务 RTO、RPO、响应流程等的要求。

三是主动防御。减少网络暴露面，使用最小权限原则对组织关键业务系统设置严格的访问权限和维护变更，在事前阶段保障对勒索软件的精准判断，利用多层次的主动防御对各种攻击方式的勒索软件进行有效拦截。**一方面通过边界防护**防止病毒从边界入侵，关

闭风险传输端口，更新防护规则，阻断传播。**另一方面通过终端防护**结合威胁情报自动对终端进行基线核查，检查终端是否存在可被利用漏洞、弱密码、不安全端口开放等风险，在安全事件发生前及时发现并修复潜在业务威胁风险。

四是系统加固、漏洞修复以及微隔离机制。针对系统注册表、关键配置项等有效保护，防止勒索软件的高危动作对系统造成的破坏；针对互联网环境、内外网隔离环境以及纯内网环境的不同场景提供不同的漏洞修复手段；通过 IP、协议、端口、方向等多个维度加强内网区域各个分组和各个终端之间的访问控制，实现主机东西向之间的网络防护。

五是补丁机制。对严重的高危漏洞，从网络层面与进程行为多个角度综合分析并识别漏洞攻击模型，有效阻止漏洞攻击行为，在系统没有打补丁的情况，完成漏洞热修复在网络层拦截勒索软件渗透威胁行为，维持快速和自动化的补丁机制有助于保护企业免受恶意攻击者进行漏洞利用入侵。

六是关键数据识别与数据保护机制。一方面是进行关键数据识别，关键数据应包括：对于有法律合规风险的数据，主要是个人信息；影响生产经营的数据，如：订单数据、财务数据、核心知识产权、生产控制数据等。对关键数据加强监控，可以更好的监控数据窃取和破坏行为，为关键数据的备份策略设置更高的 RPO 和 RTO，能更好的保证数据完整性。**另一方面是**能即时准确的找到丢

失数据并恢复是解决遭遇勒索软件后的最有效办法之一，所以企业针对核心数据需要实现网络弹性隔离保护，建立专用的隔离安全恢复环境，以物理和逻辑的方式从生产和备份网络隔离开来。关键数据采用不可变更的格式，在隔离存储区中受到保护，其留存期限被锁定。如果主备份受到损坏或者灾难恢复地点被入侵或感染，这样可提供最佳恢复机会。如果不具备网络恢复解决方案，企业会花费大量的时间、人力和费用恢复上一次并不确定是否准确的备份。

2. 持续监测体系建设

持续监测阶段需对全网进行持续监测，第一时间发现第一台失陷的主机，并进行应急处置，将勒索软件造成的损失降到最低。勒索软件版本更新频繁、入侵方式多变，仅靠事前防护必然无法保证完全安全，一旦勒索软件入侵会由点及面快速扩散，造成爆发式破坏。

其一，提高防御对抗能力。勒索软件逐渐向多样化和复杂化的趋势演变，传统意义上在网络边界部署防火墙产品或在主机部署杀毒软件的方式逐渐效率不足。为打破单一产品的防御模式，全面提升防御能力，可基于大数据和人工智能等新技术，构建网络边界、端点防护、云端协助相互联动的防御体系，有效提高与勒索软件的实时对抗能力。

其二，对业务系统进行排查。勒索攻击企业网络共享设施以及

用户本地设备后，企业发现网络共享文件及本地文件被加密不可用，应定位受感染用户设备并阻断其访问，阻止勒索软件进一步的攻击和内部扩散，交由 IT 专业人员处理。同时，攻击事件发生后，企业收到大规模告警，对于部署监测的企业，将收到大量告警，从而引起 IT 人员注意，定位到已经发生勒索攻击。

其三，对事件进行溯源分析。勒索者在已经执行完对本地和网络文件的加密后，发出提示信息，会在感染设备的界面中留下网页或者文档，告知受害者数据已经被加密，企业应当立即拍照以提供给安全专家进行分析，以帮助确定勒索攻击软件类型。安全专家通过分析勒索软件的变种类型，根据勒索软件的消息、攻击表现和路径，研判勒索软件的变种类型。

其四，安全专家追踪定位攻击者初始入口。如果是通过邮件钓鱼则需要扫描公司内邮件库以清除所有可能未被打开的攻击邮件，如果是访问恶意网站则立即进行防火墙屏蔽，如果是经由系统漏洞的攻击则需要立即进行补丁修复。

3. 快速响应及事后加固体系建设

针对已中毒主机，盲目查杀往往会造成查杀完反复感染、一边查杀一边扩散的问题，严重降低处置效率，造成更进一步的严重损失。因此勒索软件事件处置需要先快速摸清中毒主机数目和分布，接着隔离全部中毒主机，避免进一步扩散或遭受二次感染，最后通

过专杀工具或系统恢复等手段逐一处理，清除病毒文件，彻底解决病毒事件。为保证业务系统的安全防线完整，企业可以重新将重建的业务系统进行数据备份策略设置。

一是数据恢复。任何防御手段都没有绝对的安全，当出现勒索软件感染加密时，如何把经济损失降低到最小最为重要。数据通过自动备份，可以保障本地盘与云硬盘数据即使意外被勒索加密，也能在短时间内对数据进行恢复，大大降低由于勒索加密造成的经济损失。

二是购买保险。越来越多的公司正通过采取保险措施防止数据泄露，将部分网络风险转移给保险公司。具体内容请见**本章第四节网络安全保险为勒索软件攻击防护提供事后保障**内容。

4. 勒索软件攻击防护核心产品

由于勒索软件攻击具有强对抗性，并没有一种产品可单独有效解决。产业内勒索软件防护产品繁多，且防护功能会有交叉，本报告只列出部分重要勒索软件产品供参考。详见**附件 3 勒索软件攻击防护主要产品汇总**。

（三）勒索软件攻击防护关键技术能力蓬勃发展

当前，随着云计算、大数据、人工智能等新技术的快速普及和应用，数字化转型升级的关键信息基础设施依旧是勒索软件攻击的重点目标。同时，基于新技术的创新勒索软件攻击防护体系也将更

有效地保护客户免受勒索软件侵害。**本章节将对产业内的几个常见勒索软件防护技术应用进行探讨。**

1. 零信任将业务资源从互联网暴露面上进行隐藏，从而降低恶意软件的渗透风险

建立零信任安全防护机制，可弥补传统边界防护模式网络暴露面大和隐式信任问题以防护勒索软件攻击。零信任架构意味着每个试图访问网络资源的人和设备都要进行验证，其访问控制不仅能应用于用户，也适用于服务器设备与各类应用，以防止不必要的特权，并且将业务资源从互联网暴露面上进行隐藏，从而降低恶意软件的渗透风险。

面对当前愈演愈烈的网络勒索攻击，部署零信任已成为企业勒索软件防护架构转型中重要一环。在实施过程中，零信任是对网络生态系统的边界模糊的有效应对，它认为组织架构内每个组件都有弱点，每一层设施均需要保护。而得益于近期计算能力的提升，零信任架构已经在广泛的行业中得到应用。零信任不仅仅是一种技术修复，它是一套相互交织、洞悉敌对活动及相关业务风险、并致力于消减风险的方案集合。

零信任架构可帮助企业降低勒索软件攻击风险，主要表现在以下几个方面。**一是**零信任改变了用户行为模式，用新的方式解决安全问题。假设安全风险无处不在，通过各种方法加大攻击活动渗透

到整个网络的难度。**二是**零信任核心理念是了解关键数据的位置以及访问权限，运用验证措施确保只有具有权限的个人才能以适当的方式访问这些数据。**三是**零信任构建企业定义的安全边界，当今新的网络架构演变形势下，零信任模型相比传统边界防御机制提供了一种解决方案，要求对所有连接网络的用户、设备进行认证和授权，访问过程中进行持续验证。**四是**零信任方法相关的原则包括实施 MFA 以及最少特权原则，有助于降低组织中最主要攻击类型的脆弱性，特别是勒索软件，实施 MFA 会增加网络犯罪分子接管帐户的难度，仅仅盗取凭证无法攻破网络。**五是**零信任提供了对 VPN 脆弱性的替换，许多行业和公司依赖 VPN 来访问他们公司的内部网络，但是 VPN 因为漏洞和暴露面容易受到攻击，而零信任网络访问提供了安全性和可视化。**六是**零信任体系利用企业终端的 Agent，对每台电脑在访问过程中的环境进行监控。通过感知和收集到攻击者在不同的阶段实施的攻击行为，记录全链路的攻击轨迹，对系统环境的运行状态进行实时监控，发现异常行为后，Agent 可以实时进行阻断，从而对勒索软件攻击事件进行阻断。**七是**零信任体系有效阻止黑客入侵后在内网扩散。攻击者可能控制某些脆弱的单点，当其通过已攻击的终端向网络内部更重要系统横向渗透，零信任的安全机制可以及时检测到风险，阻止勒索软件在网络中进行横向移动，从而将勒索软件的影响从企业内网多台业务服务器和数据存储服务器降低至单一用户的电脑，从而帮助企业将风

险控制在最小限度，阻止发生进一步全局渗透攻击的严重后果。

2. WAAP 针对漏洞攻击进行有效防护，变被动为主动降低勒索软件攻击风险

现有安全防护技术在面临勒索软件攻击时面临巨大挑战。漏洞利用是勒索软件的主要攻击手段之一，攻击者通过漏洞探测工具扫描应用或者系统漏洞，同时利用零日漏洞快速渗透应用或者系统权限，从而发起勒索攻击。现有安全防护技术，大多基于签名或规则技术实现对已知攻击进行防护，这些防护技术都需要对已知的恶意行为进行分析，撰写攻击特征签名或行为规则；对于未知的攻击行为，现有安全技术必须等待签名或规则的更新才能有效防御，因而出现防御空窗期。然而零日漏洞攻击，由于攻击特征还没有发布，因此可以有效躲避签名与规则的侦测，已成为当前信息安全防御体系的重大缺口。勒索软件攻击已经让现有的安全防护技术捉襟见肘，然而更严峻的挑战是攻击者使用自动化攻击技术，不但可以在短时间内攻占大量的系统，也可以长期潜伏在企业信息系统中，持续窃取企业敏感信息，这对企业的信息安全来说是一个空前的挑战。

WAAP 可针对漏洞扫描以及零日漏洞进行有效防护，防止攻击者利用应用漏洞发起勒索攻击。Gartner 对 Web 和 API 保护提出了新的防护理念，即 WAAP，需要具备分布式拒绝服务（DDoS）

防御、机器人程序缓解（Bot Mitigation）、API 保护和 WAF 防护能力。其中 WAAP 防护中的 Bot 防护能力，具备针对各种自动化工具的主动防御能力，可以有效防护各种漏洞扫描和零日漏洞探测，防止攻击者利用应用漏洞发起勒索攻击。

动态安全技术已成为帮助企业变被动防御为主动防御的重要手段。动态安全技术变被动防御为主动防御、变静态防护为动态防护。无需依赖规则和补丁，以“动态安全”技术，增加服务器行为的“不可预测性”实时迷惑和干扰攻击，从而制止自动化攻击行为；高效甄别伪装和假冒正常行为的 Bots 机器人攻击，拦截已知和未知威胁，帮助企业安全团队突破被动防护的困局。

AI 技术已成为 WAF 防护提高检测率降低误报率的重要手段。在 WAF 防护能力上，引入 AI 技术，通过机器学习和行为分析技术，对攻击样本进行深入分析，结合第三方漏洞库、威胁情报等信息，进行了广泛训练和测试，从而发现高度隐蔽的攻击，有效提高检测率，降低误漏报。

3. 机器学习技术可有效提高识别、检测和处理勒索软件攻击的效率，降低企业面临的威胁与风险

机器学习技术的应用已成为近年来业界提高勒索软件防护能力的新趋势。相比手工分析，机器学习算法更加高效。但是机器学习方式受样本与特征提取限制，其结果的可靠性不是很高，还无法替

代静态检测法。基于机器学习的勒索软件查杀可通过深度学习与机器学习结合的方式进行样本的恶意动态行为检测。构建高性能、可扩展、高可用的恶意软件查杀能力，成为保障模型效果的根本。通过深度学习对恶意软件的行为序列进行智能分类，通过机器学习对局部特征进行二次校验，可大大提高检出的准确度。

4. 众多勒索软件防护技术合纵联合应用，共同提升企业勒索防护能力

众多勒索软件防范技术相互合纵联合使用，共同提升企业勒索防护能力，本章节将对勒索软件防护的其他主要核心技术进行分析和总结。

一是勒索诱饵防护技术可有效防范勒索攻击横向传播。勒索软件在入侵主机后，会进行横向传播扩散，影响范围广泛，一台终端中毒，全网业务瘫痪。使用包含已知漏洞的诱饵或部署一个几乎不可能人为或正常应用访问的文件作为引诱攻击的资源，并设定一个阈值进行监控，一旦某进程对该文件的访问超过这个阈值，则认为该进程为异常进程。勒索诱饵防护技术的优点是诱饵文件识别方法所利用的勒索软件行为特征是几乎所有勒索软件均具备的，具有较强的普适性，缺点为难以应对基于数据窃取的双重勒索或三重勒索攻击。

二是勒索行为监控技术可有效对勒索行为进行监控与定位。根

据勒索软件的特征，通过监控所有进程并 HOOK 系统内的 API 分析勒索软件发送消息、对系统文件进行加密等操作进行检测。在发现可疑行为例如频繁对文件进行读写并改变文件后缀，使用加密 API 等操作时，可以对产生该行为的进程进行阻断并将相关数据上报。勒索行为监控技术的优点为可以监控到大部分进程的可疑操作，并能够较精准地定位勒索软件所使用的进程。缺点是如运行在不同版本的操作系统中，防护程序的稳定性难以保障、实时监控对系统资源消耗较大。

三是病毒特征匹配技术可有效提高勒索识别效率。病毒特征匹配是当前最常见勒索软件查杀技术之一，通过对样本进行特征匹配，对于已知病毒来说，这种方法是最简单、最直接的方法。勒索软件特征库查杀分为云查杀和本地查杀两种方式。特征库查杀技术有着检测准确快速、可识别病毒的名称、误报警率低、依据检测结果等优点，但也存在不能检测未知病毒、网络/本地资源占用大等缺点。

四是病毒脱壳技术可解决攻击者加壳攻击。勒索软件攻击者在新技术的加持下，会给病毒程序加上一层“壳”，所谓加壳，即当加壳后的文件执行时，“壳”这段代码先于原始程序运行，把压缩、加密后的代码还原成原始程序代码，然后再把执行权交还给原始代码。对于加壳的病毒样本，常规杀毒手段无法有效发现与处理，通常采用虚拟机动态脱壳的方式来处理壳的问题，脱壳技术还可解决

包括病毒使用的自定义壳、代码混淆器在内的所有其他代码级对抗技术。

五是虚拟机沙箱技术通过模拟环境勒索攻击进行精准判断。勒索软件可伪装成为正常程序，基于特征的匹配很难发现该类勒索程序。虚拟沙盒技术设计完整的操作系统环境仿真，模拟千级数量 Windows API，涵盖绝大多数操作系统的核心机制，通过在沙箱中运行程序并观察程序行为来判断程序是否为恶意程序。

六是利用文件保险箱白名单技术提高重要资源安全性。计算机执行环境中以文件夹、磁盘等方式划分出安全空间用于存储重要数据，在此空间内的数据资产采用白名单的方式进行资产访问，同时对其中的数据进行加密保护，并可以将数据及文件备份到安全空间。该技术的优点是能够应对任何类型的勒索攻击，具有较高的安全性。但该技术会占用一部分系统内存、磁盘空间，并且只能对有限的数据资源进行防护，不能主动进行防御。

七是启发式病毒查杀技术主动防御减少防范滞后性。基于病毒库扫描的防伪为被动防范，具有滞后性，这也是杀毒软件的弊端之一。启发式查毒技术作为主动防御的一种，是当前对付病毒的主要手段，从工作原理上可分为静态启发和动态启发两种。**静态启发技术**指的是在静止状态下通过病毒的典型指令特征识别病毒的方法，是对传统特征码打描的一种补充。由于病毒程序与正常的应用程序在启动时有很多区别，通常一个应用程序在最初的指令，是检查命

令行输入有无参数项、清屏和保存原来屏幕显示等，而病毒程序那么通常是最初的指令是直接写盘操作、解码指令，或搜索某路径下的可执行程序等相关操作指令序列。静态启发式就是通过简单的反编译，在不运行病毒程序的情况下，核对病毒头静态指令从而确定病毒的一种技术。**动态启发技术**给病毒构建一个仿真的运行环境，诱使病毒在杀软的模拟缓冲区中运行，如运行过程中检测到可疑的动作，那么判定为危险程序并进行拦截。这种方法更有助于识别病毒，对加壳病毒依然有效，但如果控制得不好，会出现较多误报的情况。

八是指令序列检测技术可实现更细颗粒度权限管理。基于指令序列的细粒度权限控制技术，能够对所发现的漏洞代码、后门代码的权限从更细粒度的指令调用序列层次进行约束、实现同一进程拥有不同权限，控制漏洞与后门被利用所带来的风险，有效解决这类勒索攻击问题。在技术创新性和设计效果上具有领先性。简而言之，能够仅允许合法的“文件写指令序列”进行对文件的操作，其它非法指令则会被记录并拦截，从而达到防止利用攻击指令序列和后门指令序列对目标文件恶意篡改和勒索的问题。

（四）网络安全保险为勒索软件攻击防护提供事后保障

1. 勒索软件攻击行为助推网络安全保险发展

网络安全保险是一种新的网络安全风险管理方式。它把企业的网络安全风险转移给网络安全保险公司，以传统的网络安全保障为基础，旨在保护企业免受各种网络威胁和数据泄露造成的财物损失，在被保险企业因网络攻击而遭受损失时由保险公司进行赔付。

网络保险主要由第三方责任险和第一方责任险两个部分组成。根据 AdvisorSmith 研究显示，网络保险涵盖内容包括：数据泄露、黑客攻击、病毒、拒绝服务攻击和其他类似网络事件造成的经济损失。第一方责任险保护企业免受因数据泄露、黑客攻击或其他网络事件而遭受的财务损失。第三方责任险可防止客户或其他人因违反其安全或隐私而对企业提起诉讼。这些诉讼可能指控企业未能充分保护客户、员工、供应商或其他人的数据。第三方责任可能涵盖的一些索赔和费用包括：法律费用、网络安全声明、隐私声明、员工隐私责任和监管罚款。境外提供网络安全保险的公司主要有 Hiscox、Chubb、The Hartford、aig、CNA、Arch、Hanover、Intact、Beazley 和 Axis。

勒索软件推动网络安全保险的发展。勒索软件攻击频率和成本的增加使其成为企业面临的主要风险，并使网络保险行业面临极大压力。勒索软件攻击在一定程度上推动了网络保险行业的发展。2021 年拥有网络保险的企业更大概率遭到勒索软件攻击。原因可

能包括以下几点。**一是**是勒索软件事件的直接经验促使许多机构购买保险以帮助减轻未来攻击的影响。**二是**攻击方可能将他们的攻击目标放在已购买保险的企业上，以增加攻击方获得赎金的机会。**三是**一些组织购买了保险，以平衡其防御系统中的已知弱点。

2. 网络安全保险费用的大幅提升亦在促进提升企业网络安全能力

频发的勒索软件攻击已催生网络安全保险费用大幅增长。根据《2022 年全球网络安全展望报告》所示数据，勒索软件损害预计将从 2015 年的 3.25 亿美元增长到 2031 年的 26.50 亿美元。高额的网络攻击成本催生了对网络风险保险的庞大需求市场，根据预测，到 2025 年网络风险保险费用将从 2016 年的 32.5 亿美元上升到 200 亿美元。根据伦敦再保险经纪商数据，今年 7 月保单更新季，网络安全相关保险费率将迎来 40%的大幅增长。近年来，还专门出现了勒索攻击谈判公司，这些公司一般所属于保险公司，专门负责与攻击者进行谈判，期望将赎金压低。

网络保险正在促进网络防御的提升。目前可提供网络保险的保险公司数量不多，并且随着勒索赎金金额越来越高，网络保险价格也再上涨，网络保险服务提供商会去评估购买该项服务的企业的网络环境，根据不同的防御方式或安全人员的配置决定保险金额。很多企业为了提高他们的网络保险地位，已经对他们的网络防御进行

了改变，包含新的技术和服务、员工安全培训和教育活动等。同时，遭受受过勒索软件攻击的组织比那些未被攻击过的组织更有可能拥有网络保险和对网络安全的重视。随着网络保险价格的上涨，也促使企业都对他们的网络防御系统做出改变，以改善他们的网络保险状况。

3. 网络安全保险隐藏着恶行循环危机，变相提升犯罪成功率

网络安全保险隐藏着恶性循环危机，导致犯罪成功率提升。全球网络保险行业欣欣向荣的表象下，潜藏着巨大的恶性循环危机。由于最近几个月来全球几大公司接连遭到灾难性的勒索攻击，越来越多的企业向网络保险和再保险公司寻求帮助，网络攻击者特意挑选投保了网络保险的公司作为攻击目标，更加有针对性地实施勒索攻击，使得网络犯罪的成功率大幅提升，整体网络环境面临加速恶化的窘境。为遏制这一情况的继续恶化，已有多家公司开始缩减网络保险覆盖范围，例如法国正在考虑强制所有网络保险商停止报销赎金支出，以切断网络犯罪这一有利可图的途径。但到目前为止，大多数的保险公司并不准备取消针对勒索的保险。对于保险公司和购买了网络安全保险的企业来说，应当承担起更多的社会责任，避免在减轻单一企业在面对勒索软件的风险时，增加了其他企业的集体风险。

4. 我国网络安全保险发展处于高潜力的探索阶段

我国网络安全保险发展处于高潜力的探索阶段。我国网络安全保险产业处于起步阶段，在方案落地、发展过程、定损定责等多个方面都面临着多重阻力及挑战。保险公司、再保险公司、安全厂商以及企业用户也处于网络安全保险的探索阶段。随着《网络安全法》等法律法规的实施的推进以及一系列国内外安全事件的真实发生，已有越来越多的企业关注，网络安全保险逐渐突出在大众视野当中，企业提高了认识的同时，已引起了业内的广泛重视。2022 年 11 月，工信部公开征求对《关于促进网络安全保险规范健康发展的意见(征求意见稿)》的意见，意见稿提到建立健全网络安全保险政策标准体系，加强网络安全保险产品服务创新，强化网络安全技术赋能保险发展，促进网络安全产业需求释放，培育网络安全保险发展生态。

中国信通院科技保险团队深谙信息科技类保险相关工作多年，包括云保险，信息技术保险、网络安全保险、首版次保险等领域。2015 年，由中国信通院牵头，中国人民财产保险股份有限公司等公司组成的共保体与中国电信、中国联通、优刻得、万国数据等四大云服务商签订云计算保险合作签约云保险，意味着中国保险行业首次正式推出“云保险”这一专门针对云计算的科技类保险产品并落地。2015 年至今，中国信通院科技保险团队持续推进信息科技类

保险的落地工作，已为数十家企业提供了信息科技类保险的事前风险评估以及事后定损定则服务，同时，探索推进平台 ISV 服务商准入投保、云管理服务（MSP）风险保障计划、地方落地首版次保险补偿机制等多个创新商业模式。

五、 勒索软件攻防护发展展望

随着勒索软件的不断发展，勒索软件所造成的危害深度和攻击的广度也在不断扩大，勒索软件攻击事件以及防护也受到了业内的广泛关注。新形势下的勒索软件攻击的防护发展的未来展望包括以下几点。

一是提高人员安全意识。要认识到安全问题是我们自己人为生产的，增强人员安全意识，可以大幅降低安全风险。对从业人员的勒索软件安全意识、安全素养的训练是长久、持续的过程。

二是安全措施加强纵深防御策略。当前网络威胁已经发生了很大的变化，已经不是简单的破坏系统，让企业的 IT 系统不能正常运行，而是把关注度转向企业的核心数字资产。勒索软件的防范也需要从传统的防范策略演变到纵深防御策略上。纵深防御策略采用一个多层次的、高纵深的安全措施，最大限度的降低风险、防止攻击，来防范勒索攻击或将勒索攻击的危害降到最低。

三是提升安全前置能力。企业一旦被勒索后再进行勒索数据恢复难度很大，因此在这个防护过程中，就需要对安全防护前移，即

整个防护的重点在勒索发生之前要进行拦截或阻断。目前已知的针对勒索诱饵等技术都是将围绕事前开展防御，实现将安全左移，提升安全前置能力。

四是保障供应链安全。随着数字化程度不断加深，依靠单一企业的安全防御能力，不足以应对供应链安全威胁。勒索软件结合软件后门、软件投毒、供应商软件漏洞等供应链风险开展网络攻击，传统防护方案是很难应对。因此，需要提升供应链安全防护能力，建立供应链链威胁共享机制与协同防御、建立软件供应链生命周期，包括供应链上游、开发、编译、交付、供应链下游阶段的防护体系。

五是新技术赋能安全。尽可能提升关键安全技术效能，利用云计算、大数据、人工智能等技术赋能，提高对数据的处理、对威胁的识别效率，跟上黑客能力的进化速度，在智能化方面加强勒索软件攻击的端点对抗。攻击方亦在尝试通过人工智能等技术进行更具破坏性的攻击，因此构建具备新技术的安全侦测和防御体系，识别网络的勒索软件攻击流量，并减少误报，是提升整体安全防护防御能力的必经之路。

六是持续推进网络安全保险对勒索软件攻击风险的抵御。网络安全保险已成为网络安全风险的新型管理方式，事前投保可以有效降低企业在遭到攻击后的维护成本，且专业保险公司在风险管理与损失填补方面的经验，也有助于企业保障基本的防护要求，做好安

全规划。

七是勒索软件防护逐步规范化，推进标准化建设，深入实施高质量发展。构建并完善勒索软件防护标准体系。中国信息通信研究院云计算与大数据研究所相关团队，将联合业界众多勒索软件防护头部企业专家，共同编写勒索软件防护标准体系，标准将适用于对服务提供商在提供勒索软件防护服务时的功能设计、产品研制等方面进行指导和监督，同时适用于企业对自身勒索软件防护安全体系进行设计、管理和评价时进行参照使用。

附录 1 2022 年全球勒索软件攻击重要事件梳理

表 1 2022 年全球勒索软件攻击重要事件

数据来源：公开数据

2022 年全球勒索软件攻击事件		
时间	**事件**	**事件详情**
1 月	美国头部 HR 系统供应商 Kronos 遭勒索软件攻击	国头部 HR 系统供应商 Kronos 私有云平台遭勒索软件攻击超过 1 个月仍未恢复，数千家公司因勒索攻击无法发放工资，供应商瘫痪超 1 个月。
1 月	印尼央行(印度尼西亚银行)遭 Conti 组织袭击，超 13GB 数据外泄	印尼央行内部网络十余个系统遭到勒索软件攻击，已超过 13GB 的内部文件数据被窃取。勒索团伙称，如印尼央行不支付赎金，将公开泄露数据。
1 月	教育行业云服务提供商 FinalSite 遭受勒索软件攻击	FinalSite 是一家教育行业云服务提供商，为全球 115 个国家逾 8000 所学校提供 SaaS 服务。FinalSite 遭到勒索软件攻击，导致约 5000 所学校网站被迫关停。
1 月	国防承包商 Hensoldt 遭 Lorenz 勒索软件攻击	Hensoldt 是一家总部位于德国的跨国国防承包商。其英国子公司的部分系统感染了 Lorenz 勒索软件。声称网络中窃取了大量敏感文件。
1 月	美国新墨西哥州伯纳利洛县遭勒索软件攻击	美国新墨西哥州伯纳利洛县政府的 IT 网络遭到勒索软件攻击，导致多个城市的政府大楼和公共办公室关闭，还致使该县拘留中心的安全摄像头和自动门脱机，囚犯被限制在牢房内。
2 月	英伟达（Nvidia）遭 Lapsus$组织攻击，涉及 1TB 机密数据	全球知名的半导体芯片公司英伟达被爆遭到 Lapsus$勒索团队攻击。攻击者表示可访问 1TB 的企业数据，若拒绝支付赎金，将公开泄露数据。
2 月	全球最大的轮胎制造商之一普利司通遭受 LockBit 勒索攻击	LockBit 勒索软件团伙声称已经破坏了最大的轮胎制造商之一普利司通美洲公司的网络，并窃取了该公司的数据。若拒绝支付赎金，将公开泄露数据。

2 月	航空服务企业 Swissport 遭受 BlackCat 勒索软件攻击	Swissport 在 50 个国家的 310 个机场开展业务的航空服务企业，近日该企业遭受勒索软件攻击，其位于全球的多个 IT 基础设施被入侵或破坏，对公司运营造成严重影响，并导致多个航班延误。BlackCat 勒索团伙随后宣布对此次攻击事件负责，并威胁将窃取的 1.6TB 敏感数据出售给潜在买家。
3 月	意大利铁路公司 Trenitalia 遭勒索攻击	Hive 勒索软件组织攻击了意大利铁路公司 Trenitalia 的计算机系统，影响了公司员工电脑和系统的正常运行。此外，与其连接的票务系统 Trenord 也受到了黑客攻击的影响。若拒绝支付赎金，将翻倍赎金。
3 月	丰田汽车供应商遭勒索攻击，14 家本土工厂暂时关闭	丰田汽车公司表示，其零部件供应商因受到了勒索软件攻击，从而导致系统瘫痪。受此影响，丰田日本 14 家工厂，28 条生产线停工一天。
3 月	罗马尼亚石油公司 Rompetrol 遭勒索攻击	罗马尼亚最大的石油公司 Rompetrol 遭到 Hive 勒索组织的攻击，关闭了其网站和加油站的会员卡服务，不过顾客可以选择用现金或银行卡付款。据了解，这次攻击影响了该公司的大部分 IT 服务。若拒绝支付赎金，将公开泄露数据。
3 月	征信巨头 TransUnion 数据泄露，对 90%南非人造成影响	征信巨头 TransUhnion 的南非公司遭巴西黑客团伙袭击，5400 万消费者征信数据泄露，绝大多数为南非公民，南非总人口约 6060 万人。事件将为受影响的消费者免费提供身份保护年度订阅服务，预计成本将超过 114 亿元。
4 月	里约财政系统遭勒索攻击，420GB 数据被盗	巴西里约热内卢州财政部门系统遭到勒索软件攻击。随后勒索软件团伙 LockBit 宣称为此次事件负责。LockBit 入侵了接入政府办公室的系统，并窃取到约 420GB 数据。
4 月	风力涡轮机公司 Nordex 遭受 Conti 勒索软件攻击	德国风电整机制造商巨头 Enercon 受到了勒索软件攻击。事件中欧洲卫星通信受到大规模中断，直接影响了中欧和东欧近 6000 台装机容量总计 11GW 的风力发电机组的监控和控制。
4 月	哥斯达黎加政府多个部门遭受勒索攻击	此事件为 2022 年最受关注的攻击事件，为一个国家首次宣布进入“国家紧急状态”以应对勒索软件攻击。从 4 月中旬到 5 月初，27 个政府机构成为第一波攻击活动的目标。国家财政部 800 多台服务器受到影响，数字税务服务和海关控制 IT 系

		统瘫痪，不仅影响了政府服务，还影响了从事进出口的私营部门。勒索软件组织 Conti 声称对此轮攻击负责，并要求哥斯达黎加政府支付赎金 5 月 31 日开始，另一波攻击使该国的医疗保健系统陷入混乱。
4 月	美国利福尼亚州一医疗保健组织遭 Hive 勒索软件攻击	Partnership HealthPlan of California 是一个帮助美国加州数十万人获得医疗保健服务的非营利组织，受到 Hive 勒索软件团伙的攻击。攻击导致其遇到技术困难，某些计算机系统中断。勒索软件团伙称其窃取了超过 85 万人的个人信息，还声称从该组织的服务器上窃取了 400GB 的文件。
5 月	美国农业机械巨头爱科遭到勒索软件攻击，造成重大的供应链影响	美国农业机械巨头爱科遭到勒索软件攻击，部分生产设施运营受影响并持续多天。FBI 在 4 月警告称，勒索软件攻击正逐渐将矛头指向美国农业部门。
5 月	意大利多个重要政府网站遭 DDoS 攻击致瘫痪	意大利多个官方网站遭到黑客大规模 DDoS 攻击致服务器瘫痪，包括参议院、国防部、国家卫生所等 7 家重要机构官网临时宕机长达 4 个小时，用户无法访问。
5 月	加拿大空军关键供应商遭勒索攻击，疑泄露 44GB 内部数据	加拿大、德国军方的独家战机培训供应商 Top Aces 称，遭到 LockBit 勒索软件攻击。LockBit 团伙的官方网站已经放出要求，如不支付赎金将公布窃取的 44GB 内部数据。
5 月	印度航空公司 SpiceJet 遭勒索导致乘客滞留机场	印度香料航空公司系统遭到勒索软件攻击，内部系统受影响离线，导致多个航班延误数小时，大量乘客滞留在机场，直接影响到飞往印度及海外各国的众多乘客，数小时的延误或造成巨大的经济损失。
5 月	奥地利卡林西亚州政府遭勒索攻击	Black Cat 勒索组织声称获取了奥地利卡林西亚州政府的敏感数据和解密软件访问权限，并向其索要价值 500 万美元的比特币来解锁加密的计算机系统。攻击者加密了数千个政府机构的工作站，导致政府服务严重中断。最终政府拒绝了支付赎金。
6 月	意大利比萨大学（University of Pisa）遭勒索攻击	意大利的比萨大学被 Black Cat 勒索组织攻击。攻击者要求学校管理层支付 450 万美元来恢复对已锁定数据的访问权限，如果规定时间内未受到赎金，赎金金额将增加。

6 月	意大利巴勒莫市遭遇 Vice Society 组织攻击	意大利南部巴勒莫市遭受 Vice Society 勒索攻击，据报道，受影响的系统包括公共视频监控管理、市警察行动中心以及市政府的所有服务。同时威胁如不支付赎金将会泄露政务数据。
6 月	Lockbit 勒索软件团伙称入侵网络安全公司 Mandiant	近日，LockBit 勒索软件团队宣称从 Mandiant 窃取了 356841 份文件，并计划将这些文件泄露到网上。
7 月	美国乔治亚州的蒂夫特地区医疗中心遭到 hive 攻击	Hive 团伙窃取了该医疗中心约 1TB 的数据，其中包括诊疗记录、员工工资记录和机密商业信息。
7 月	Macmillan 遭到勒索软件攻击导致系统关闭	据报道，出版业巨头麦克米伦（Macmillan）遭到勒索软件攻击，该公司关闭了其所有 IT 系统，以防止攻击蔓延。
7 月	法国电话运营商 La Poste Mobile 遭勒索软件攻击	法国虚拟移动电话运营商 La Poste Mobile 遭到勒索软件攻击，导致行政和管理服务瘫痪，攻击行为者可能已经访问了其客户的数据。
7 月	建材巨头可耐福遭到 Black Basta 勒索软件攻击	德国建材巨头可耐福集团(Knauf Group)宣布已成网络攻击目标。其业务运营被攻击扰乱，迫使全球 IT 团队关闭了所有 IT 系统以隔离事件影响。随后，Black Basta 勒索软件组织在其网站上发布公告将其列为受害者。
8 月	CHSF 医院遭勒索软件攻击，急诊被迫停业	法国巴黎的一家医院（CHSF）遭遇网络攻击，急诊被迫停业，并推迟了多台手术。CHSF 为当地 60 万居民提供诊疗服务，因此其运营中断，给病患造成严重的健康甚至生命威胁。此次网络攻击致使医院的业务软件、存储系统（特别是医学影像）及与部分患者信息系统暂时无法访问。勒索软件团伙要求医院支付 1000 万美元以换取解密密钥。
8 月	美国麦岭市（City of Wheat Ridge）公共市政系统遭勒索攻击	美国科罗拉多州麦岭市的市政服务系统遭遇 Black Cat 勒索组织攻击，致使电话、电子邮件系统和其他市政服务系统关闭了一个多星期。攻击方索要 500 万美元来解锁麦岭市的市政数据和计算机系统，并要求以加密货币 Monero 来支付。
8 月	多米尼加共和国政府机构遭遇 Quantum 攻击	多米尼加共和国的多米尼加农业研究所遭到了 Quantum 勒索软件攻击，加密了整个政府机构的多项服务和工作站，导致部分工作暂

		时停滞。攻击者索要 60 万美元赎金，否则泄露数据。
9 月	欧洲国家黑山政府部门和国家议会遭遇勒索攻击	欧洲国家黑山的多个政府部门遭遇超大规模勒索攻击，致使超过 10 个政府机构的 150 多个工作站均无法访问。此次攻击采用了勒索软件与分布式拒绝服务（DDoS）相结合的方式，不仅扰乱了政府服务，还迫使该国的电力系统转为手动控制。Cuba 勒索软件组织宣称对此次攻击负部分责任。
9 月	法国服装公司 Damart 遭勒索攻击	法国服装品牌 Damart 遭到 Hive 勒索组织的攻击，并索要 200 万美元的赎金。这次攻击访问了 Damart 的活动目录，尽管 Damart 主动关闭了系统以保护它们，但这次网络攻击还是影响了 92 家商店，并影响到这些门店处理订单服务。
9 月	澳洲电信运营商 Optus，1120 万用户数据被窃	澳大利亚电信公司 Optus 遭遇勒索组织攻击，1120 万用户的数据被窃，可能泄露的信息包括客户的姓名、出生日期、电话号码、电子邮件地址，住址等信息。攻击者要求 Optus 支付价值 100 万美元的门罗币（Monero），否则将公开数据。
10 月	印度最大的综合电力公司子公司 Tata Power 遭到 Hive 勒索软件攻击	勒索软件组织 Hive 在其数据泄露网站上公布了塔塔电力公司（TataPower）的数据。月初，该公司遭遇攻击发生数据泄露，勒索软件组织 Hive 宣称对此次攻击负责。据报道，勒索软件组织 Hive 发布了他们声称从 Tata Power 窃取的数据，这意味着赎金谈判已经失败。
11 月	LockBit 勒索团伙入侵德国跨国汽车零部件制造公司	LockBit 勒索软件组织声称已经入侵了跨国汽车集团 Continental，并威胁要泄露被盗数据。

附录 2 2022 年我国勒索软件攻击重要事件梳理

表 2 2022 年我国勒索软件攻击重要事件

数据来源：公开数据

2022 年我国勒索软件攻击事件	
时间	**事件**
1 月	北京某金融企业员工终端感染 Magniber 勒索软件
1 月	安徽某医院运维服务器感染 Phobos 勒索软件
1 月	山西某企业服务器感染 Zeppelin 勒索软件
1 月	重庆某企业服务器感染 Makop 勒索软件
1 月	河北某医院多台云服务器感染 BeijingCrypt 勒索软件
1 月	南京某企业遭 Mallox 勒索软件攻击
1 月	浙江某药企遭勒索软件攻击
1 月	内蒙古某企业遭勒索软件攻击
2 月	福建某企业内网多台主机感染 BeijingCrypt 勒索软件
2 月	浙江某高校办公终端感染 Coffee 勒索软件
2 月	江苏某企业遭遇 Magniber 勒索软件攻击
2 月	浙江某企业遭 Mallox 勒索软件攻击
3 月	安徽省某企业服务器感染 TellYouThePass 勒索软件
3 月	深圳某医疗行业单位办公终端感染 TargetCompany 勒索软件

3 月	重庆某医院服务器感染 Phobos 勒索软件
3 月	浙江某运营商遭勒索软件攻击
3 月	南京某企业遭遇 LockBit 勒索软件攻击
3 月	济南某企业遭到 TellYouThePass 勒索软件攻击
3 月	深圳某医疗行业单位办公终端感染 TargetCompany 勒索软件
4 月	天津某企业遭 RushQL 勒索软件攻击
4 月	郑州某企业遭遇 Makop 勒索软件攻击
4 月	贵州某单位服务器遭 Zeppelin 勒索软件攻击
4 月	上海某企业遭勒索软件攻击
4 月	浙江某厂商遭勒索软件攻击
4 月	江苏某企业遭 Mallox 勒索软件袭击
4 月	浙江某企业遭 Phobos 勒索软件攻击
5 月	福建某企业遭 Makop 勒索软件攻击
5 月	某医院遭 Phobos 勒索软件攻击
5 月	上海某企业遭 Phobos 勒索软件攻击
5 月	浙江某企业遭 Mallox 勒索软件攻击
5 月	沈阳某公司遭 7Locker 勒索软件攻击
6 月	山东某企业遭到 TellYouThePass 勒索软件攻击
6 月	广西某企业遭勒索软件攻击

6 月	深圳某制造业单位遭 Makop 勒索软件攻击
6 月	浙江某企业遭遇 Globeimposter 勒索软件攻击
6 月	浙江某学校遭 Phobos 勒索软件攻击
6 月	福建某生活服务行业单位遭勒索软件攻击
6 月	山西某医院遭 Phobos 勒索软件攻击
6 月	山东某制造业单位遭勒索软件攻击
6 月	某大学遭境外网络攻击
7 月	江苏某企业遭 Makop 勒索软件攻击
7 月	苏州某企业遭 ViodCrypt 勒索软件攻击
7 月	上海某企业遭遇 Phobos 勒索软件攻击
7 月	SafeSound 勒索软件通过多款网络游戏外挂进行传播。
7 月	深圳某企业遭 Phobos 勒索软件攻击
7 月	深圳某企业遭 Phobos 勒索软件攻击
7 月	山东某制造业单位遭勒索软件攻击
8 月	上海某科技公司遭 Phobos 勒索软件攻击
8 月	安徽某企业遭 Lockbit 勒索软件攻击
8 月	辽宁某企业感染 Phobos 病毒
8 月	广东某制造业遭 Sodinokibi 勒索软件攻击
8 月	山东某企业遭遇 TellYouThePass 勒索软件攻击

8 月	TellYouThePass 针对中小微企业用户发起大规模勒索攻击
9 月	湖南某制造业遭 Babuk 勒索软件攻击
9 月	山东某企业遭遇 TellYouThePass 勒索软件攻击
9 月	上海某企业遭 Phobos 勒索软件攻击
9 月	浙江某企业遭 Mallox 勒索软件攻击
9 月	陕西某企业遭 Phobos 勒索软件攻击
9 月	Makop 勒索软件攻击广东某企业
10 月	上海某集团遭遇 GlobeImposter 勒索软件攻击
10 月	浙江某医疗单位遭 BeijingCrypt 勒索软件攻击
10 月	深圳某企业遭 Sodinokibi 勒索软件攻击
10 月	成都某企业遭受勒索软件攻击
11 月	贵州某医院遭 Phobos 勒索软件攻击

附录 3 勒索软件攻击防护主要产品梳理

由于勒索软件攻击具有强对抗性，并没有一种产品可单独有效解决。产业内勒索软件防护产品繁多，且防护功能会有交叉，本报告只列出部分重要勒索软件产品供参考。

表 3 勒索软件攻击防护核心产品

数据来源：公开数据

产品	主要防护手段与功能
1. 事前抵御勒索软件攻击入侵	
勒索拦截产品	对已知、未知的勒索软件进行监测、诱捕、防范和阻断并进行快速响应，对业务进行保护，同时对核心数据进行保护。
防火墙产品	在传统防火墙的基础上集成众多应用层安全功能，为用户提供 L2-L7 层网络的全面安全防护能力，应对传统网络攻击和未知威胁攻击的创新网络安全产品。集成机器学习和大数据分析等创新安全技术，增强安全检测与防控能力，保障网络的正常运行，实现业务的稳定运营，阻断勒索软件利用与异常外联。
杀毒软件产品	杀毒软件是目前应对勒索软件攻击最有效的安全产品，通过在操作系统上安装 agent 软件对勒索软件实时动态检测，利用传统病毒特征库、病毒基因库识别技术等识别不同勒索软件，对已知各类勒索软件及其变种病毒进行精准查杀。同时还可通过虚拟沙盒技术，利用恶意代码行为分析能力，解析勒索软件的本质特征，实时阻断未知勒索。针对勒索软件加密文件的特殊动作，采用勒索诱捕技术，对加密动作实时捕获并阻断。
存储备份产品	备份产品可以对文件、数据库、虚拟机进行备份，在勒索软件攻击发生前对数据进行备份、攻击发生后对数据进行恢复，最大程度降低由勒索软件加密、窃取数据造成的数据丢失。
WEB 应用防火墙产品	保护核心网站的漏洞不被勒索软件利用，进而避免核心网站被勒索攻击。
漏洞扫描产品	及时发现网站漏洞和主机系统的漏洞，避免漏洞被勒索利用。
主机安全及管理产品（EDR）	EDR 通过多种杀毒引擎配合，能防止大部分已知的病毒、木马和勒索软件侵入系统；一旦系统被侵入，EDR 通过外联检测发现勒索软件和木马建立的隐蔽通道，从而定位病毒和木马；通过诱饵引擎，诱使勒索软件主动加密文件，从而隔离病毒；EDR 通过端口监控和漏洞管理，也能防止病毒横向扩散和蔓延。
邮件威胁防护产品	防垃圾邮件系统通过检查邮件源拦截常见僵尸网络发送的钓鱼邮件和垃圾邮件，防垃圾邮件系统通过对邮件主题、正文和附件的检查，可以拦截带毒邮件和钓鱼邮

	件。
XDR 产品	随着人工智能技术的快速融入，新一代网络技术使攻击变得更加隐蔽和快速，对传统安全防御体系更是建立起“降维打击”的优势。XDR（扩展威胁检测与响应）产品作为更主动的安全方案，能跨网络、端点以及云基础架构提供数据的可见性，从而可快速检测威胁并能够快速响应。
主机加固产品	系统基线配置不当、弱口令、端口违规开发、RDP 协议违规开放均为勒索软件攻击的直接原因。当应用系统急剧增加时，由主机自身安全导致的勒索软件传播概率将大幅提升。主机加固产品支持主机入侵防护、操作系统基线检测、等级保护基线检测、中间件基线检测及自定义检测基线等，定期对主机进行信息安全风险评估，通过自动化的安全配置检查，及时发现主机中存在的安全隐患，并在第一时间定制安全加固策略，保证主机系统的安全。
2. 事中阻断勒索软件攻击横向扩散	
入侵防护产品	检测勒索攻击横向扩散中对其他主机的勒索攻击、弱密码攻破及病毒加密复制行为，提供动态的、深度的、主动的安全防御。
网络流量分析产品	提供告警策略分级，针对全局、业务域、业务 IP 组进行分级策略配置等功能。通过智能流量学习、告警检测，全面实现从网络流量侧进行勒索攻击防护。
安全审计产品	安全审计通过信息资产（网络设备、安全设备、主机、应用及数据库）的日志获取，基于预置的解析规则实现日志的解析、过滤及聚合，对非法访问、可疑入侵 、病毒爆发、数据库口令猜测、漏洞攻击和数据大量下载、高危操作的异常行为进行监控。安全审计可将数据访问行为发送给用户行为分析系统进行周期分析，尽早发现勒索软件的入侵。
蜜罐产品	针对数据勒索搭建的数据库蜜罐系统，将自身伪装成 CRM 数据库、HR 数据库、ERP 数据库等高价值目标，诱使勒索组织进行攻击。一方面，所有对数据库蜜罐系统的访问都是高危访问，可快速准确的定位攻击来源，另一方面，数据库蜜罐系统还能分散勒索组织的精力，为及时做出响应争取更多时间。
APT 攻击预警产品	勒索组织在内网踩点和横向渗透阶段，都会尝试进行网络扫描和服务扫描，会利用服务漏洞进行权限获取和提升，会通过建立隐秘通道与勒索组织服务器建立控制连接，并传输窃取到的数据，APT 攻击预警系统采用安全沙箱、DGA 等技术能够发现以上的行为异常，定位勒索渗透的主机，阻断勒索攻击链。
用户行为分析产品（UEBA）	基于大数据平台，运用 AI 技术和机器学习，对采集到的数据访问行为、告警信息，终端日志、应用日志、运维日志进行大数据分析，基于访问行为建模，能够发现隐蔽更深的数据勒索。
数据分析处置产品	大数据分析平台对海量数据进行高速、准确的提取和分析，从大量事件中发现攻击线索，结合威胁情报和专家分析，对数据勒索和攻击行为进行长效监测。安全运维人员在对安全事件研判分析确认安全事件之后，流转至安全事件处置响应模块进行安全事件信息联动处置。对已经确认的攻击，可以通过人工的处置流程剧本编排，

	使响应流程尽量实现标准化、智能化，从而做到快速正确的响应和处置。
3. 事后数据恢复还原	
磁盘快照产品	为云硬盘数据盘提供快照能力，当数据被勒索加密时可通过快照恢复数据。
数据恢复产品	保障业务数据即使意外被勒索加密，也能完整恢复数据。
云灾备产品	采用云灾备模式，用户可利用服务提供商的优势技术、灾备经验和运维管理流程，快速实现用户的灾备目标，降低客户的运维成本和工作强度，同时也降低灾备系统的总体成本。云灾备的备份介质可以选择云服务商的对象存储，结合对象存储的云灾备服务，是勒索软件攻击应急恢复的重要措施。
应急响应服务	咨询安全专家进行应急响应，快速恢复系统的保密性、完整性和可用性，阻止和降低数据勒索造成损失。对事件情况出具专业完整的应急响应报告，包括对事件的描述和判断，以及安全加固建议、应急处置办法，将整个系统恢复至安全状态，防止二次侵害发生。
谈判专家服务	谈判专家团队是对数据勒索产业充分了解，并对勒索链条中各环节角色的心理进行充分的分析。当勒索事件发生时，谈判专家能够与勒索组织沟通，得到勒索的更多线索，如：数据泄露情况、勒索者对企业的了解程度、数据恢复的可能性等，便于企业进行研判。

致谢

本报告得到以下单位的大力支持，特此表示感谢。限于编写时间、知识积累与产业尚未完全定型等方面的因素，内容恐有疏漏，烦请不吝指正。

中国信息通信研究院、腾讯云计算（北京）有限公司、北京联合大学智慧城市学院、中国联通西安软件研究院、用友网络科技股份有限公司、戴尔科技集团、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、奇安信科技集团股份有限公司、北京天融信网络安全技术有限公司、中兴通讯股份有限公司、北京知道创宇信息技术股份有限公司、网宿科技股份有限公司、北京神州绿盟科技有限公司、三六零数字安全科技集团有限公司、北京持安科技有限公司、瑞数信息技术(上海)有限公司、优刻得科技股份有限公司、杭州默安科技有限公司、山石网科通信技术股份、中电信数智科技有限公司、亚信安全科技股份有限公司、苏州美天网络科技有限公司、上海安钛飞信息技术有限公司、深圳市智安网络有限公司、高颂数科（厦门）智能技术有限公司、北京网际思安科技有限公司

云计算开源产业联盟
OpenSource Cloud Alliance for industRy,OSCAR

TRUSTED SECURITY
可信安全

CONTACT US

若您对本报告有任何建议，请与我们联系：
weibin@caict.ac.cn / 18618259777

可信安全