腾讯研究院 Tencent Research Institute | 腾讯安全 Tencent Security | 中国信息安全 China Information Security | 中国产业互联网发展联盟 Internet+ Development Association of China

2021年「勒索攻击」特征与趋势研究白皮书

2021.11

顾　问

丁珂、司晓、张显龙、陈胜喜

编委会

李刚、刘琼、柳雁军、张雪琴、王融、董文辉、程虎

编写组

腾讯研究院

翟尤、宋扬、秦天雄、刘金松、袁媛、吴朋阳、周丹、窦淼磊、白惠天

腾讯安全

李铁军、胡龙、黄佩钰、谢飞、恒海涛、刘颖、谭昱、付蓉洁、陈娟娟、王成、张靓

《中国信息安全》杂志社

王丹娜、向继志、袁胜、李鑫、邱辰杰、彭琳、张婷

CONTENTS

目录

序言

勒索软件又称为“赎金木马”，勒索软件攻击是指网络攻击者通过锁定设备或加密文件等方式阻止用户对系统或数据的正常访问，并**要挟受害者支付赎金的行为**。如同我们把钱放在保险箱，小偷没有撬开保险箱偷钱，反而把放保险箱的房间加了把锁。如果没有房间的钥匙，我们依然拿不到保险箱里的钱。

如今，新型勒索攻击事件层出不穷。**勒索攻击事件在全球各地频频发生，可归因于三个方面：一是企业内部基础设施建设落后，联网后缺少有效的安全防护措施。**美国国家漏洞库 NVD 资料显示，仅在 2020 年上半年就发现了多达 365 个工业控制系统相关的漏洞，比 2019 年上半年增长 10.3%，其中，超过 75% 的漏洞被认定为严重等级，这些漏洞涉及 53 个厂商。而我国的情况也不容乐观，《2020 年上半年我国互联网网络安全监测数据分析报告》数据显示，我国工业控制系统的联网信息持续遭受境外不法分子的窥探，日均扫描超 2 万次，能源、制造、通信等行业的基础设施及控制系统成为主要目标。**二是对于网络攻击者来说，高额的赎金成为他们实施犯罪的极大动力。**美国网络安全公司 Palo Alto Networks 公布的数据显示，发生于 2020 年的勒索攻击事件赎金平均为 312,493 美元，较上年增加 171%。区块链分析公司 Chainalysis 的报告也提到，2020 年市面上各类活跃的勒索软件共计获利 3.7 亿美元，较上年增长 336%，其中仅

DarkSide 一家就获得超过 9000 万美元的赎金。**三是远程办公增加安全风险。**新冠肺炎疫情期间，犯罪分子利用远程办公带来的安全漏洞，通过技术迭代、数据泄露、加密数据等方式不断进化攻击手法，开辟新的攻击面，利用人们在危机期间的恐慌心理，持续增加勒索次数。例如，2020 年 6 月，斯洛伐克安全公司发现了通过伪装成“新冠病毒跟踪应用程序”加密 Android 设备上文件的勒索软件。

2021 年，勒索攻击事件此起彼伏。例如，以色列 Hillel Yaffe 医疗中心遭到勒索攻击。日本著名企业奥林巴斯遭遇 2021 年度的第二次勒索攻击导致美洲地区的网络系统被迫下线。中国台湾知名电脑企业宏碁公司也遭遇了两次勒索。最令人不可思议的是，在已经遭遇过勒索攻击后，却没见宏碁和奥林巴斯的网络防御能力变得强大。其中，奥林巴斯两次遭劫前后仅仅间隔一月有余。

随着 AI、5G、物联网等技术的快速普及和应用，以及加密货币的持续火爆，如今勒索攻击呈现出持续高发态势。勒索攻击已经成为未来一段时期网络安全的主要威胁之一，如何有效防范勒索攻击成为当前网络安全领域关注和讨论的焦点。

各国都认识到，勒索软件是一种不断升级的全球安全威胁，会造成严重的经济和安全后果。勒索软件对关键基础设施、基本服务、公共安全、消费者保护和隐私构成重大风险，例如，勒索软件针对当地卫生服务提供者的恶意操作，危害了病人护理；针对限制其向公众提供燃料、生活用品或其他商品能力的企业的操作，影响了企业运营。与其他网络威胁一样，勒索软件的威胁是复杂的、全球性的，需要各国共同应对。

第一章
勒索攻击成为全球新挑战

数字技术应用的泛在化、融合化意味着更多终端暴露在网络攻击范围之内，网络攻击随时随地可能发生，攻击频次和深度逐步加大。基础设施逐渐成为被攻击的主要对象，导致国家经济社会安全受到挑战。总的来看，数字经济时代我们将面临以下三个方面的安全挑战。

一、科技竞争对国民经济安全带来挑战

后疫情时代，贸易、技术、人员流动面临更多限制，区域性、双边性投资和贸易安排更加频繁，全球产业链布局区域化特征凸显。与此同时，为科学划分国家经济安全边界、保障产业链安全，全球主要经济体纷纷加快基础性技术主导权战略布局、构建产业安全边界，抢占新一轮科技革命制高点。

一方面，各国持续增厚科技实力“安全垫”。随着科学技术体系日益复杂，单一技术难以引领新一轮科技革命。为维护国家安全，提高竞争实力，发达国家加快重大科技战略制定成进程。例如，英国发布《未来科技贸易战略》，对数字经济、科技创新投资进行战略部署[1]。美国发布《改善国家网络安全的行政命令》，明确指出要增强软件供应链安全、成立网络安全审查委员会，同时要求美国政府部门制

美国发布
《加强国家网络安全的行政命令》

英国发布
《未来科技贸易战略》

印度加快研究发布
《新网络安全战略》

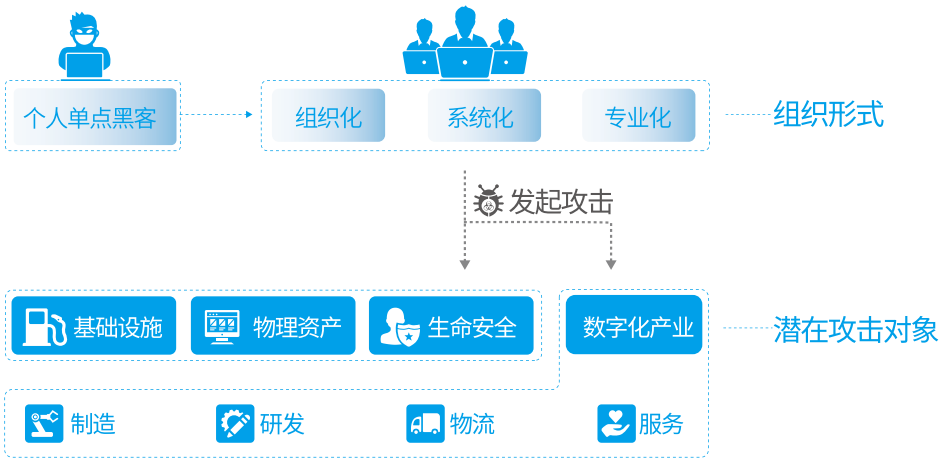
1 引自 https://baijiahao.baidu.com/s?id=1669290498915404046&wfr=spider&for=pc

定实施零信任架构的计划、加快云服务安全化的步伐等具体措施[2]。印度加快研究发布《新网络安全战略》，旨在确保安全、可靠、有弹性、充满活力和值得信赖的网络空间[3]。

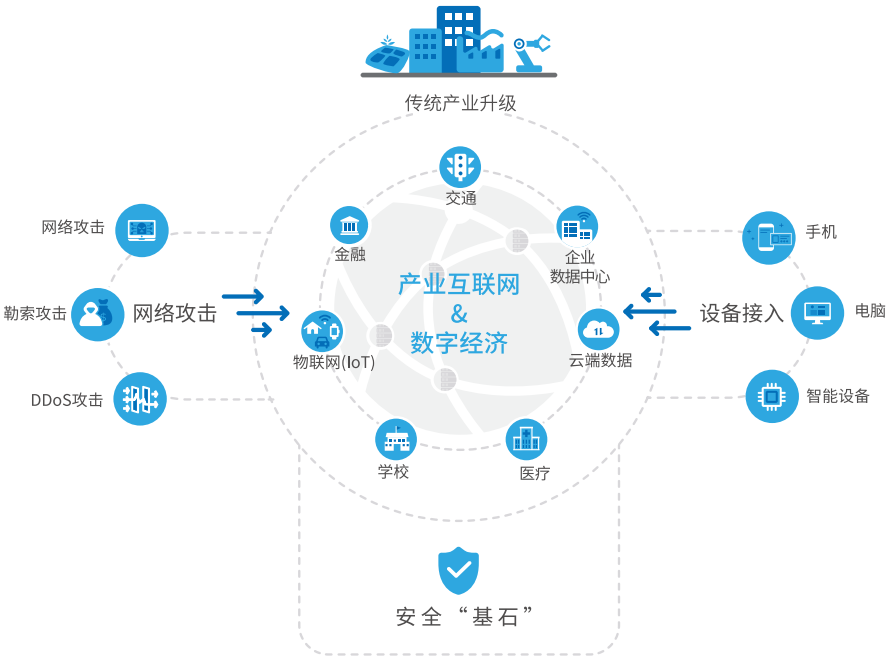
另一方面，细分领域技术优势影响产业链安全。部分核心技术和专利集中在少数国家或企业手中，对其他国家经济安全带来较大影响。以芯片产业为例，韩国总统文在寅在参与“K—半导体战略报告大会”时表示，半导体竞争已经超越公司层面，成为国家角力的战略领域[4]。

二、产业数字化转型带来安全挑战

产业互联网时代，安全范畴进一步扩大。攻击发起方已经从过去个人、单点黑客行为向组织化、系统化、专业化方向快速蔓延。一方面基础设施、物理资产、生命安全都将成为比特世界的潜在攻击对象，安全保障能力成为行业发展的“生命线”。另一方面，数字化贯穿企业研发、制造、物流、服务等全流程，安全需求覆盖全部环节，安全能力的强弱程度逐渐成为企业持续发展的“天花板”。



2 引自 https://xueqiu.com/6430922966/180728305
3 引自 https://www.secrss.com/articles/32558
4 引自 https://m.gmw.cn/baijia/2021-05/28/34883896.html



（一）安全是产业互联网的基石

数字经济时代，数字化加快推动传统产业转型升级。一方面，产业数字化促使数字经济加快进入高级阶段，生产效率的提高更加依赖数据深度挖掘和全流程打通。另一方面，传统产业安全防护能力参差不齐，海量设备接入网络当中，网络安全、数据安全在全流程应用场景中均涉及。因此，网络攻击、勒索攻击、DDoS 攻击逐渐增多，攻击面逐渐扩大化。以智能网联汽车行业为例，智能化、网联化、共享化、电动化成为行业主要发展趋势，伴随而来的是大量安全漏洞和远程控制风险。攻击者利用车辆自带的安全系统漏洞对汽车软硬件部分实施攻击、窃取并发送信息甚至远程控制车辆。一旦发生安全事故，将对消费者人身安全产生重大风险。

（二）基础设施成为攻击重点

当前，网络攻击更加组织化、系统化、专业化，攻击范围向行业、基础设施领域拓展，金融、交通、医疗、城市管理等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。以医疗卫生行业为例，医疗数字化一直

是社会关注焦点，随着大量数字化设备和医疗设备的广泛应用，医疗效率、就医体验、服务精准度都有大幅提升，但也给安全防护和医疗数据安全保护带来新的挑战。

据媒体报道，2020 年，法国有 11% 的网络攻击目标是医院系统。2021 年 2 月，法国两家医院连接遭到大规模勒索攻击，造成医院信息系统瘫痪，部分外科手术被迫推迟，甚至需要手工绘制医院排班图表 [5]。

（三）恶意攻击实时化全面化

恶意攻击不分时间和地点，随时对目标发起攻击，因此，安全投入资源不足、安全监测能力较低、安全防御碎片化的企业和机构，将面临较大风险。安全防护需要做到前置和未雨绸缪，不论是个人、企业、还是民用设施、基础设施都可能成为恶意攻击的跳板，链条中的薄弱环节将成为攻击的重要突破口。

美国燃油运输管道商科洛尼尔遭到勒索攻击

来源：Colonial Pipeline Company

2021 年 5 月，美国最大的燃油运输管道商科洛尼尔公司遭到勒索攻击，导致 5500 英里输油管系统被迫停运，该管线供应了美国东海岸 45% 的燃料。网络攻击者在短时间内获取企业约 100G 数据，并锁定相关服务器等设备要求支付赎金。能源运输管道作为国家重要基础设施，成为越来越多犯罪分子攻击对象。安全风险逐步从小范围局部向基础设施大范围进行扩散。

5 引自 https://new.qq.com/omn/20210406/20210406A00LHJ00.html

三、技术破坏式创新带来安全挑战

一方面，技术创新在造福民众和提升经济社会效率方面发挥牵引作用；另一方面，新技术也是一把双刃剑，容易引发新的安全风险，给现有安全保障措施带来巨大挑战。数字经济时代，安全的价值和重要性愈发突出，安全的内涵也在不断丰富。

（一）海量终端与网络虚拟化带来更多攻击面

一方面，海量多样化终端接入网络。智能终端设备的接入规模、技术架构的异质化带来了安全管理难度和复杂度的提升。另一方面，新型网络架构导致安全边界模糊。SDN、NFV、云计算和边缘计算等技术和技术框架的应用带来了新的攻击面，在这些新技术研发中广泛使用开源代码，带来了新的安全设计缺陷和安全漏洞。同时，基于网络切片端到端逻辑虚拟网络技术的垂直领域应用，在资源共享、跨领域安全、身份认证和权限控制等方面出现新的安全风险。例如5G 的开放性网络容易遭受攻击、虚拟化模糊了物理边界、海量数据连接带来安全风险。

（二）破坏式技术创新带来负面影响

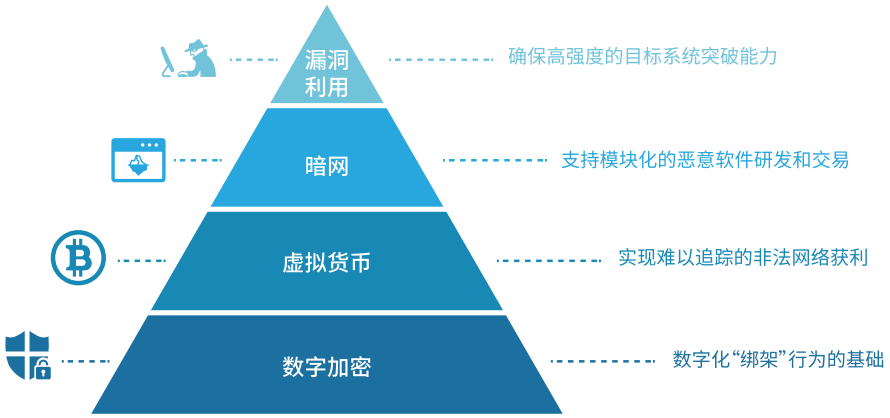
技术在给经济社会带来大量便利和效率提升的同时，破坏式创新也带来不利影响。一方面，犯罪分子使用新技术工具逐渐增多，对个人、企业和政府部门带来损害。根据世界经济论坛发布的《2021年全球技术治理报告：在疫情时代利用第四次工业革命技术》，比特币支付占 2019 年第一季度全球勒索事件赎金交付方式的 90%以上，尤其是区块链技术的匿名性使得监管部门难以溯源打击违法犯罪分子。另一方面，新技术应用安全风险难以界定。例如，随着自动驾驶技术的进一步普及，相关技术落地后产生的安全风险难以界定。自动驾驶汽车发生交通事故，如何判断责任方是一个较为复杂的过程，其中涉及汽车制造商、软件研发人员、网络服务商、汽车所有者、使用者以及乘客等多方。

（三）隐私保护与数据共享面临挑战

当前，数据已经成为企业的重要核心资产。能否对数据进行有效运用和深度挖掘，成为衡量一家企业能否创造价值的重要依据之一。需要意识到，数据安全在企业价值体现面前具有“一票否决”权。技术溢出带来的风险、算法难解释性与黑箱性、数据质量导致计算结果可控性差、用户权益与隐私屡遭侵犯等是当前数据安全面临的巨大挑战。同时，隐私保护和信息共享缺乏统一技术标准和治理框架。

四、勒索攻击带来的安全风险和挑战

如果勒索攻击没有得到有效解决，将会带来大量潜在风险。一是监管风险，以欧盟《通用数据保护条例》（GDPR）为例，备份和灾难恢复是 GDPR 的必选项，如果被攻击的机构没有按照法规定期对数据进行备份，将会面临罚款等惩罚措施。二是服务风险，数据或文件被加密或泄露，机构将被迫停止其经营活动，如果受害机构没有可以恢复正常运营的备份数据，可能会导致客户的投诉和不满，最终失去客户。三是经济风险，数据恢复流程长、复杂度高，费用昂贵。恢复已遭破坏的数据时需要重新收集数据，这使得机构信誉受到质疑，对机构品牌带来较大损害。



重大威胁勒索软件应用到的关键技术 [6]

6 赵子鹏、张奇 . 解读重大勒索攻击事件下的网络安全态势及应对 [J]. 中国信息安全，2021(6):64-67.

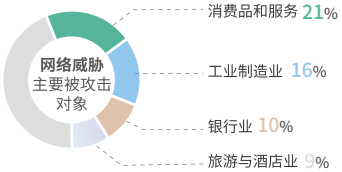
第二章
勒索攻击演进路径与特征

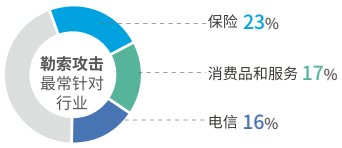
从 20 世纪 80 年代首个勒索病毒 AIDS 出现到 2021 年的 30 余年间，勒索攻击经历了萌芽期、活跃期和高发期三个阶段。已经形成了分工明确的产业链条，受害用户和造成的损失与日俱增。世界范围内，勒索攻击主要针对能源、电信、医疗、教育等国民经济重要行业，已经成为网络安全的主要威胁。

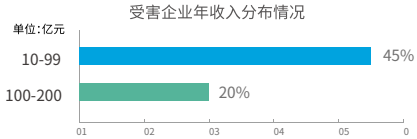
一、从勒索病毒向勒索攻击的转变

1989 年，哈佛大学学生约瑟夫·L·波普制作了全球首个勒索病毒—AIDS 木马。这位哈佛高材生将勒索病毒隐藏在软盘中并分发给国际卫生组织艾滋病大会的参会者。此款勒索病毒会记录用户设备重启次数，一旦超过 90 次就会对设备中存储的文件进行加密，并要求邮寄 189 美元才能解密重新访问系统。虽然**“名牌大学生恶作剧 + 邮寄支付赎金”**的标签在今天看来既没有多大危害，也不够专业，但是，该勒索病毒所建立的对经济社会的攻击模式，在此后的 30 多年中逐渐演变为让人闻之色变的网络攻击浪潮。

根据咨询机构埃森哲调查显示，2021 年上半年，全球网络威胁活动较去年增长 125%。其中，消费品与服务、工业制造业、银行业和旅游与酒店业成为主要被攻击对象，占比分别为 21%、16%、10%、9%。聚焦在勒索攻击领域，勒索攻击最常针对的行业是保险、消费品和服务、电信，占比分别为 23%、17%、16%，三者总计占比达到 56%。受害企业按照年收入分布来看，10-99 亿美元的公司占比超过 45%，年收入在 100-200 亿美元的企业占比 20%。







勒索攻击发展历程并不长，在 30 多年的发展过程中，主要经历三个阶段：

1. 萌芽期。1989 至 2009 年是勒索攻击的萌芽期。在这 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 年甚至更早，出现了使用 RSA 非对称加密算法的勒索病毒 GPcode，其密码长度更长，在此基础上还衍生出诸如 Gpcode.AK 的变种，使得勒索病毒的破解难度急剧增加。同年，中国大陆首次遭到名为“Redplus”的勒索病毒的入侵，勒索金额从 70 到 200 元不等。

2. 活跃期。2010 年以后，勒索攻击进入活跃期，几乎每年都有勒索软件的变种出现，其攻击范围不断扩大、攻击手段持续翻新，此阶段的勒索攻击事件大多分散发生，勒索软件本身并不具有主动扩散的能力。2013 年 9 月，Cryptolocker 勒索病毒的出现标志着以比特币为赎金支付方式时代的来临，此后很长一段时间内没有有效的解密被感染文件的手段，黑客团伙据此赚取近 41000 枚比特币（市值为 10 亿美元）。自此之后，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。

3. 高发期。勒索攻击在 2015 年后进入高发期，此阶段勒索攻击已呈现产业化、家族化的特点，勒索软件作者、勒索者、传播

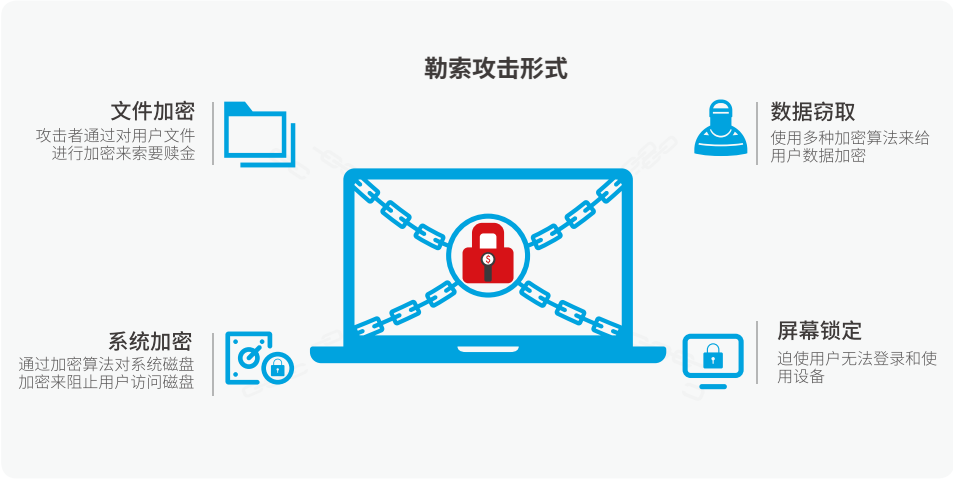
渠道商和解密代理四个角色分工明确，共同发起一次完整的勒索攻击事件。2017 年，WannaCry 勒索攻击在全球范围内大规模爆发，至少 150 个国家、30 万名用户受害，共计造成超过 80 亿美元的损失，至此勒索攻击正式走入大众视野并引发全球关注。

2015
高发期

WannaCry勒索攻击在全球大规模爆发
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

二、勒索攻击形式与传播渠道的变化

在勒索攻击形式方面，目前主要有文件加密、数据窃取、系统加密和屏幕锁定等四种主要的形式。一是文件加密，这是最典型的攻击形式，攻击者通过对用户文件进行加密来索要赎金，文件一旦被感染极难恢复。二是数据窃密，数据窃密与文件加密相类似，即使用多种加密算法来给用户数据加密，攻击者以威胁公开重要数据来胁迫受害者支付赎金。三是系统加密，主要是通过加密算法对系统磁盘主引导记录、卷引导记录进行加密来阻止用户访问磁盘，影响用户正常使用设备。四是屏幕锁定，相对其他三种攻击形式，屏幕锁定危害较轻，主要迫使用户无法登录和使用设备，数据具备可恢复的可能。

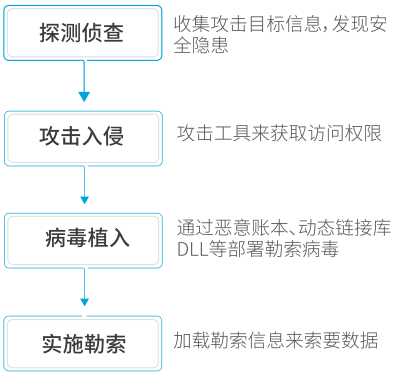


在勒索攻击传播方面，钓鱼邮件、安全漏洞、网站挂马、移动介质是较为常见的方式，同时，软件供应链、远程桌面也成为新的传播渠道。具体来看，一是安全漏洞，攻击者通过弱口令、远程代码执行等安全漏洞来入侵受害者内部网络，从而发起攻击。二是钓鱼邮件，攻击者把勒索软件内嵌在邮件文档、图片等附件中，或者将勒索恶意链接写入钓鱼邮件正文，诱发用户点击。三是移动介质，攻击者通过 U 盘、移动硬盘等移动存储介质，并创建移动介质盘符或图标等快捷方式，诱导用户进行点击。四是软件供应链，攻击者利用用户对软件供应商的信任关系，通过软件供应链的分发和更新等机制来发起勒索攻击。五是远程桌面，攻击者利用弱口令暴力破解等方式获取攻击目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

勒索攻击传播

安全漏洞	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
钓鱼邮件	把勒索软件或勒索恶意链接内嵌在邮件文档、图片等附件中
移动介质	通过U盘、移动硬盘等移动存储介质并创建快捷方式
软件供应链	通过软件供应链的分发和更新等机制来发起勒索攻击
远程桌面	通过远程桌面登录服务器植入勒索病毒

勒索攻击实施阶段



在勒索攻击实施阶段方面，探测侦查、攻击入侵、病毒植入和实施勒索 4 个方面是主要的攻击阶段。一是探测侦查，攻击者首先需要收集攻击目标，一般通过主动扫描、网络钓鱼以及暗网购买等方式，来收集攻击目标信息，从而发现被攻击者存在的安全隐患。二是攻击入侵，攻击者根据发现的漏洞作为网络攻击突破口，并部署相应的攻击资源。同时，采用合适的攻击工具来获取访问权限。三是病毒植入，攻击者通过恶意账本、动态链接库 DLL 等部署勒索病毒，以此来规避软件监测，并利用文件共享协议等方式来横向移动，扩大感染范围。四是实施勒索，攻击者通过加载勒索信息来索要数据，勒索信息包括联系方式、支付赎金等内容。

三、勒索攻击事件数量不断增加

如今，勒索软件已经成为一个全球性问题，而且勒索攻击事件的数量也不断攀升，自2018 年以来，勒索软件攻击数量猛增了 350%。根据澳大利亚信息专员办公室 （OAIC）的一份报告，与 2020 年下半年相比，2021 年上半年，由勒索软件攻击引起的数据泄露事件增长了 24%。勒索攻击不仅带来了代价高昂的服务中断，还直接威胁政治安全、经济安全、科技安全等各个方面。

近年来全球典型勒索攻击汇总表

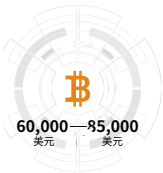
名称	出现时间	特点	典型受害企业
WannaCry	2017.5	蠕虫扩散传播和勒索软件加密文件双重功能，比特币支付	全球 150 多个国家和地区的 20 万台电脑设备受感染。美国波音飞机生产工厂、全球知名半导体厂商台积电
NotPetya	2017.6	加密和锁死整个硬盘，从内存提取密码	全球领先的助听器制造商 Demant、航运巨头马士基、快递服务商联邦快递、俄罗斯最大石油企业 Rosneft
BitPaymer	2017	针对大型公司，攻击行业的供应链解决方案提供商	全球知名自动化工具生产商之一皮尔兹（Pilz）、苏格兰医院、美国阿拉斯加自治市政府、美国饮料供应商 - 亚利桑那饮料公司
Ryuk	2018.8	对大型企业定向攻击	全球知名自动化工具生产商之一皮尔兹（Pilz）、苏格兰医院、美国阿拉斯加自治市政府、美国饮料供应商 - 亚利桑那饮料公司
Ryuk	2018.8	对大型企业定向攻击	美国通用健康服务公司、法国 IT 巨头 Sopra Steria
Maze	2019.4	针对专业部门，攻击北美和欧洲组织	美国跨国 IT 服务商 Cognizant、美国军事承包商 Westech Internationl、佳能
Sodinokibi	2019.5	通过混合方式发动攻击，对国内系统做定制化操作	阿根廷电信公司、美国烈酒和葡萄酒行业 Brown-Forman 公司
NetWalker	2019.8	针对政企、医疗组织和远程办公员工，利用系统内工具攻击	阿根廷移民局
Ekans	2019.12	依靠钓鱼邮件传播	澳大利亚航运及物流公司
WastedLocker	2020.4	针对高价值企业	健身追踪器、智能手表和 GPS 产品制造商 Garmin

名称	出现时间	特点	典型受害企业
Avaddon	2020.6	以垃圾邮件传播	保险巨头安盛集团
Revil	-	加密所有文件，通过比特币支付赎金	智利国家银行、中国台湾 PC 巨头宏基 (Acer）、全球最大肉制品供应商 JBS、美国核武供应商 Sol Owriens 公司、日本富士、美国 IT 管理软件开发商 Kaseya
Darkside	2020.8	以 RaaS 模式运作，具有 Windows 和 Linux 双平台攻击能力，只针对大型盈利性公司	美国最大的燃料管道运营商 Colonial
RansomEXX	2020.6	通过购买凭证、暴力破解 RDP 服务器、利用安全漏洞等方式入侵，出现 Linux 版本	巴西政府网络、得克萨斯州交通部（TxDOT）、柯尼卡美能达、IPG Photonics、Tyler Technologies、厄瓜多尔最大网络运营商 CNT

数据来源：根据公开信息整理

2021 年以来，勒索攻击事件频发。以美国为例，2021 年 5 月以来，美国频繁遭遇勒索病毒攻击，有媒体甚至用“嚣张”两个字形容这一现象。而且，勒索的攻击对象范围不断扩大，医院、交通、食品、管道运输等行业和领域，都成为其攻击的对象。

2021.01



2021 年 1 月，首款 2021 年面世的勒索软件 Babuk Locker 在新年伊始攻击了 5 家企业。其开出的赎金价格（要求以比特币支付）在 60,000 美元到 85,000 美元之间。

2021.02

2021 年 2 月，据 BleepingComputer 报道，起亚汽车美国公司（KMA）疑似遭受了 DoppelPaymer 团伙的勒索软件攻击，攻击者要求提供 2000 万美元赎金解密数据，以及防止被盗数据泄露。此前， BleepingComputer 报道起亚汽车美国正在遭受全国性 IT 系统中断，受影响系统包括移动 UVO Link 应用程序、电话服务、支付系统、用户门户以及经销商使用的内部站点。

2021.03

2021 年 3 月，REvil 勒索软件团伙在其数据泄露站点上宣布，他们已经成功入侵宏碁电脑公司的系统，并同时公布了几张作为证据的被盗文件截图，包括关于财务电子表格、银行结余以及银行往来信息的文档等。3 月，澳大利亚最大的电视网络之一九号电视台，在官方网站上披露遭受网络攻击，导致生产系统被迫下线。

2021.04

2021 年 4 月，荷兰 Bakker Logistiek 公司遭遇勒索软件攻击，业务网络上的设备被对方加密，食品运输与配送体系也随之瘫痪，多地超市发生食品断货。4 月，Babuk Locker 勒索团伙宣称，他们已经从美国哥伦比亚特区警局的服务器上总计下载到超过 250GB 数据。该团伙随后主动联系警局，要求对方三天之内回应勒索要求。如果不支付赎金，他们将对外公布该警局的秘密档案。4 月，REvil 勒索软件团伙向苹果公司提出赎金要求，否则就将机密信息发上暗网。REvil 团伙称，他们已经成功入侵中国台湾广达电脑公司。遵循勒索活动的一贯套路，REvil 团伙在某暗网门户网站上发表帖子，表示广达电脑拒绝赎回这批失窃数据，因此 REvil 决定转而将矛头指向信息内容涉及的各家主要客户。REvil 团伙共发布了 21 张 MacBook 产品设计图，并威胁除非苹果或广达电脑支付赎金，否则他们将每天披露更多新数据。此外，该勒索软件团伙还暗示，他们有意将这批数据出售给多家公司。4 月，英国城市铁路运营商默西铁路（Merseyrail）证实，遭受勒索软件攻击。攻击方甚至使用该公司内部电子邮件系统，向员工及记者发送了关于勒索活动的说明邮件。

2021.05

2021 年 5 月，美国最大燃油管道商 Colonial 遭受勒索攻击后被迫关闭。5 月，美国水务公司 WSSC Water 称，其系统遭到了勒索软件攻击。5 月，专为欧洲能源及基础设施企业提供技术方案的挪威公司 Volue 遭遇勒索软件攻击。勒索软件关闭了挪威国内 200 座城市的供水与水处理设施的应用程序，影响范围覆盖全国约 85% 的居民。

2021.06

2021 年 6 月，据美国华盛顿“福克斯 -5”电视台报道，华盛顿大都会警察局（MPD）的服务器被名为 Babuk 的黑客团伙入侵。Babuk 向警方索要 400 万美元的赎金，否则将公布 250GB 的 MPD 机密文件。6 月，全球最大肉类生产商巴西 JBS 集团美国分公司的 CEO 表示，该公司向网络犯罪分子支付了价值 1100 万美元的比特币赎金，以解决所遭受的网络攻击，这次攻击迫使该公司暂时关闭了加工美国约五分之一肉类产品的工厂。6 月，中国台湾内存和存储制造商威刚表示，在 5 月下旬网络被攻击后，勒索软件的再次攻击迫使其系统脱机。6 月，美国最大传媒集团之一考克斯媒体集团（Cox Media）旗下广播和电视台遭遇勒索软件攻击，导致直播流被迫中断。这次事件影响到考克斯媒体资产中的内部网络与实时流媒体功能，令网络流媒体与移动应用业务无法正常运转。6 月，勒索软件攻击令美国马萨诸塞州的最大轮渡服务商 Steamship Authority 遭遇班次延误与中断，扰乱了马撒葡萄园岛与楠塔基特群岛同美国大陆之间的轮渡交通。6 月，日本富士公司宣布正在调查勒索软件攻击，并关闭了部分网络以防止攻击蔓延。

2021.07

2021 年 7 月，为 4 万多家组织提供服务的美国 IT 管理软件厂商 Kaseya 披露，它们已经沦为“复杂网络攻击”的受害者。这导致包括瑞典最大杂货零售品牌在内的全球数百家企业，启动紧急应急响应，以应对潜在的违规漏洞。7 月，英国地方公共铁路运营商北方铁路（Northern Trains）遭遇服务宕机，自助售票亭无法正常运行，官方称遭到了勒索软件的突然袭击。7 月，厄瓜多尔最大的网络运营商国家电信（CNT）遭遇勒索软件攻击，业务运营、支付门户及客户支持全部陷入瘫痪。

2021.08

2021 年 8 月，勒索软件团伙 LockBit 发布公告称，已攻破咨询巨头埃森哲内网，窃取了一批内部数据；埃森哲随后承认，确实遭到勒索软件攻击，但公司运营未受到影响，相关系统已通

过备份副本恢复。8 月，日本跨国保险公司东京海上控股（Tokio Marine Holdings）披露称，新加坡分公司新加坡东京海上保险（TMiS）遭受勒索软件攻击。8 月，巴西政府发布声明称，巴西国库（National Treasury）遭遇勒索软件攻击。巴西经济部表示，他们立即采取了相关措施，以遏制网络攻击引发的影响。8 月，美国医疗连锁机构Memorial Health System遭遇勒索软件攻击，致使 IT 系统瘫痪，旗下三家医院无法正常运营。8 月，中国台湾电脑巨头技嘉遭勒索软件攻击，上百 GB 数据失窃。

2021.09

2021 年 9 月，南非司法与宪法发展部所有系统被勒索软件攻击者加密，所有系统被锁死，内部员工及公众均无法使用，运营陷入“手动”。9 月，欧洲呼叫中心巨头 Covisian 的西班牙与南美洲分部 GSS 遭勒索，多个关基组织客服中断。9 月，美国第二家农业合作社 Crystal Valley 系统遭遇到勒索软件攻击，位于爱荷华州的农场服务供应商 NEW Cooperative 也遇到勒索软件攻击。9 月，日本科技巨头奥林巴斯遭到勒索攻击导致部分网络关闭。

2021.10

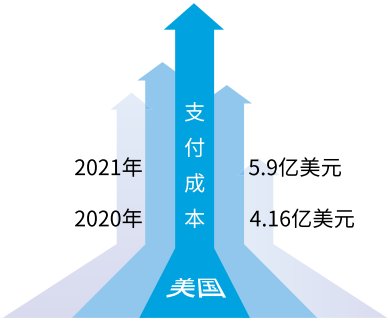
2021 年 10 月，苏格兰跨国工程企业伟尔集团（Weir Group）披露了一项“勒索软件攻击企图”，称该事件导致了今年 9 月的“重大临时中断”。

从上述勒索攻击事件可以看出，勒索攻击事件发生的频率不断攀高，其所涉及的行业和领域也不断扩展，例如金融领域已经成为勒索攻击的重灾区之一。根据美国财政部当地时间 2021 年 10 月 15 日发布的一份报告，截至 2021 年 6 月，金融机构已经向金融犯罪执法网络报告了 635 起与勒索软件相关的可疑活动，比 2020 年报告的所有活动增加了 30%。

四、勒索攻击事件支付成本大幅攀升

勒索软件攻击不仅变得越来越频繁，而且成本也越来越高。遭遇勒索攻击的当事方出于各种原因，不得不选择交付赎金以重新恢复正常的秩序。

勒索攻击交易数额导致受攻击对象支付成本增加。根据美国财政部当地时间 2021 年 10 月 15 日发布的一份报告，2021 年报告的总价值为 5.9 亿美元，平均每月 6640 万美元，而 2020 年全年的总价值为 4.16 亿美元。网络保险公司的数据表明，勒索软件攻击不仅变得越来越频繁，而且成本也越来越高，遭勒索且索赔的案件也呈上升趋势。



据报道，今年 5 月， REvil 公司因攻击全球肉类供应商 JBS 公司获得了 1100 万美元赎金收入。随后，该组织在 7 月攻击了软件公司卡西亚（Kaseya），导致这家公司数百名客户无法工作，有些甚至长达数月。另一个组织“黑暗面”（DarkSide）的黑客敲诈了美国燃料供应商科洛尼尔（Colonial Pipeline）数百万美元，引发了对可能出现的天然气短缺的恐慌。

勒索攻击事件增加促使各国加大应对勒索攻击财政投入。勒索攻击事件导致的支付成本增加，促使各国政府不得不考虑通过增加财政投入改善网络安全状况，甚至考虑帮助受到勒索攻击方恢复正常秩序。

澳大利亚

《2020 年网络安全战略》

- 16.7 亿澳元（12.3 亿美元）投资
- 雇佣AFP特工

《2021年监视立法修正案》

- 610万澳元(450万美元)帮助企业
- 培训中小企业

为应对风险，澳大利亚政府已通过澳大利亚《2020 年网络安全战略》批准了为期十年的 16.7 亿澳元（12.3 亿美元）的投资，其中勒索软件计划是该项投资的一部分。在这部分投资中，有大约一半的份额用于雇佣另外 100 名 AFP 特工。新的工作组将承担识别、调查和锁定网络犯罪分子的角色。在澳大利亚政府寻求通过的《2021 年监视立法修正案》中，在支持受害者内容方面，还包括 610 万澳元（450 万美元），用于帮助企业从灾难性的网络攻击中恢复，并培训中小企业如何改善其网络安全状况。

五、各国加速调整反勒索相关立法

勒索软件造成的数据安全事件频发，成为各国共同面临的挑战，对勒索软件进行立法规制的需要已经刻不容缓。

（一）美国

2016 年 9 月，美国加州通过参议院第 1137 号法案（Senate Bill No. 1137- Chapter 725），修订了《刑法典》第 523 节，在法律层面明确了实施勒索软件行为的刑事责任，规定以获取钱财或其他利益为目的，直接放置或感染勒索软件，或者指使、引诱他人这样做，从而将勒索软件感染到计算机、计算机系统或计算机网络中，在获取利益后为受感染者提供移除或其他方式的恢复服务的，将视情节处以 2 至 4 年的监禁。

2016.09
美国加州通过
参议院第 1137 号法案（Senate Bill No. 1137- Chapter 725）
修订了《刑法典》第 523 节

2017 年 9 月，美国国家标准技术研究院（National Institute of Standards and Technology，NIST）发布了帮助遭受勒索软件攻击的企业制定数据恢复计划的专门指南，提供了包括高级架构、实现案例、安全特性分析等正确处理勒索软件攻击的方法建议。

2017.09
美国国家标准技术研究院发布
帮助遭受勒索软件攻击的企业制定数据恢复计划的专门指南

2020 年 9 月，NIST 发布了新的《数据完整性恢复指南（SP）1800-11》[7]，帮助组织制定从影响数据完整性的攻击中恢复的策略，恢复并维持运营及管理企业风险。

2020.09
NIST 发布了
新的《数据完整性恢复指南（SP）1800-11》

在遭遇“太阳风”（SolarWinds）大型供应链安全事件后，美国又紧急出台了一系列有关供应链安全的政策法规。2021 年 3 月，美国商务部《确保信息和通信技术及服务供应链安全》（Securing the Information and Communications Technology and Services Supply Chain）[8] 生效，要求对半导体芯片等四类供应链产品开展审查，并在一年内完成对美国国防、通信科技、能源等六大部门的生产供应链进行风险评估，提出改善措施。

2021.03
美国商务部
《确保信息和通信技术及服务供应链安全》

7 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-11.pdf
8 https://www.govinfo.gov/content/pkg/FR-2021-01-19/pdf/2021-01234.pdf

2021.04

美国网络安全基础设施安全局和 NIST 联合发布

《防御软件供应链攻击》

2021.05

美国总统签署

《关于改善国家网络安全的行政命令》

2021.06

美国参议院通过

《2021 年美国创新和竞争法案》网络安全的行政命令》

美国白宫针对企业发布避免勒索软件备忘录

美国司法部提交

《关于勒索软件和数字勒索调查和案件的指导意见》备忘录

2021.07

美国众议院通过

1 《国土安全部工业控制系统能力增强法案》

2021 年 4 月，美国网络安全和基础设施安全局（Cybersecurity and Infrastructure Security Agency，CISA）和 NIST 联合发布《防御软件供应链攻击》（Defending Against Software Supply Chain Attacks）[9] 报告，描述了与软件供应链攻击相关的信息、关联风险及缓解措施。

2021 年 5 月，美国总统签署的《关于改善国家网络安全的行政命令》（Executive Order on Improving the Nation’s Cybersecurity）[10] 要求，联邦政府采取行动确保软件供应链的安全性和完整性，其中包括要求向政府出售的软件必须符合基准安全标准，并引入软件物料清单。2021 年 6 月，美国参议院在通过的《2021 年美国创新和竞争法案》（The United States Innovation and Competition Act of 2021）[11] 也提到要推进“弹性供应链战略”、帮助美国公司“获得稳定可控的全球供应链”等，从而确保美国在供应链安全方面的领导地位，减少网络攻击的产生。同月，美国白宫针对企业发布避免勒索软件备忘录，总统府助理、负责网络和新兴技术的副国家安全顾问安妮·诺伊伯格（Anne Neuberger）指出：“所有组织都必须认识到，任何公司都不能成为勒索软件的目标”，敦促商界领袖“立即召集他们的领导团队讨论勒索软件的威胁”，并在他们受到攻击时加强安全措施和连续性计划，并列出了一系列最佳实践和建议，从创建数据备份到及时的系统补丁、第三方网络安全审查和分段网络。同月，美国司法部提交《关于勒索软件和数字勒索调查和案件的指导意见》备忘录，旨在通过一系列安全指令实践来阻止勒索软件感染、数据盗窃和向网络犯罪集团支付巨额款项等违法行为。

2021 年 7 月，美国众议院通过了一系列涉及反勒索软件的立法。一是《国土安全部工业控制系统能力增强法案》（HR1833-DHS Industrial Control Systems Capabilities Enhancement Act of

9 https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf

10 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

11 https://www.democrats.senate.gov/imo/media/doc/USICA%20Summary%205.18.21.pdf

2 《网络安全漏洞修补法案》

3 《CISA 网络演习法案》

4 《州和地方网络安全改善法案》

5 《国土安全关键领域法案》

2021）[12]。目前，该法案已在参议院获得两党支持。该法案要求国土安全部的网络安全和基础设施安全局（CISA）带头更好地识别和减轻对 ICS 基础设施的威胁。二是《网络安全漏洞修补法案》（HR2980-Cybersecurity Vulnerability Remediation Act）[13]，重点关注关键基础设施。该法案旨在授权美国国土安全部（DHS）的网络安全和基础设施安全局 (CISA) 协助关键基础设施的所有者和运营商制定针对严重漏洞的缓解策略。该法案涵盖了 IT 和 OT 系统中的漏洞，以及不再被支持的硬件或软件中的安全漏洞。它还授权国土安全部为识别 IT 和 ICS 产品漏洞的补救方案引入竞争机制。三是《CISA 网络演习法案》（HR3223-CISA Cyber Exercise Act）[14]。该法案在 CISA 内部建立了一个项目，旨在促进对针对关键基础设施的网络攻击的准备和恢复能力的定期测试和评估。演习将模拟网络攻击对政府或关键基础设施网络的重大影响，并将帮助组织提高准备和事件响应能力。四是《州和地方网络安全改善法案》(HR3138-State and Local Cybersecurity Improvement Act)[15]。该法案将创建一个每年 5 亿美元的拨款项目，由国土安全部运营，以帮助各州和地方政府改善网络安全。该法案还将创建一个州和地方网络安全弹性委员会，以确保国土安全部的网络安全和基础设施安全局与州、地方、部落和地区政府之间就其网络需求进行持续的对话。五是《国土安全关键领域法案》（HR3264-the Domains Critical to Homeland Security Act）[16]。该法案授权国土安全部识别对经济安全至关重要的领域的供应链风险。虽然它没有特别提到网络，但它可能适用于这个领域。该法案的摘要解释说，“该法案将美国经济安全的关键领域定义为对美国经济安全至关重要的关键基础设施和其他相关产业、技术和知识产权，或它们的任何组合。”

2021.08

美国国土安全部 CISA 发布

《保护敏感信息和个人信息免受勒索软件导致的数据泄露》

2021 年 8 月，美国国土安全部 CISA 发布有关如何防止勒索软件数据泄露的指南，名为《保护敏感信息和个人信息免受勒索

12 https://docs.house.gov/billsthisweek/20210719/BILLS-117hr1833-SUS.pdf
13 https://docs.house.gov/billsthisweek/20210719/BILLS-117hr2980-SUS.pdf
14 https://docs.house.gov/billsthisweek/20210719/BILLS-117hr3223-SUS.pdf
15 https://docs.house.gov/billsthisweek/20210719/BILLS-117hr3138-SUS.pdf
16 https://docs.house.gov/billsthisweek/20210719/BILLS-117hr3264-SUS.pdf

软件导致的数据泄露》[17]。该文件建议公司如果成为勒索软件攻击的目标，不要支付赎金。根据该机构的文件，为防止成为勒索软件攻击的受害者，企业应采取如下步骤：解决面向互联网的漏洞和错误配置，减少攻击者利用这一攻击面的可能性；制定、维护和行使基本的网络事件响应计划、弹性战略和相关的通信计划；保持数据的离线、加密副本，并定期验证备份；减少收到网络钓鱼邮件的可能性；坚持正确的网络健康准则。

2021.10

美国参议员提出

《赎金披露法草案》

2021 年 10 月，美国参议员伊丽莎白·沃伦（Elizabeth Warren）和众议员德博拉·罗斯（Deborah Ross）提出《赎金披露法草案》（Ransom Disclosure Act）[18]。草案要求勒索软件受害者（不包括个人）在支付赎金之日起 48 小时内披露有关赎金支付的信息，包括要求和支付的赎金金额、用于支付赎金的货币类型以及有关勒索软件的任何已知信息；要求赎金的实体；要求国土安全部公开上一年披露的信息，不包括支付赎金实体的身份信息；要求国土安全部建立个人可以自愿报告赎金支付情况的网站；指示国土安全部部长对勒索软件攻击之间的共性以及加密货币促进这些攻击的程度进行研究，并为保护信息系统和加强网络安全提供建议。

（二）澳大利亚

2021.05.24

澳洲政府

公开表示正在考虑制定政策

2021 年 5 月 24 日，澳洲政府公开表示正在考虑制定政策，要求因遭到网络攻击而支付赎金的企业向政府报告。

2021.08.12

澳大利亚工党

在参议院重新提出《勒索软件法案》

2021 年 8 月 12 日，澳大利亚工党在参议院重新提出《勒索软件法案》[19]，如果该法案获得通过，将要求企业和政府在为应对网络攻击而支付勒索软件费用之前通知澳大利亚网络安全中心。

为了进一步加强调查和破坏勒索软件攻击的能力，澳大利亚

17 https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf

18 https://www.warren.senate.gov/imo/media/doc/DUN21766.pdf

19 http://www.anquan419.com/knews/24/1140.html

政府还在寻求通过《2021 年监视立法修正案》以获得新的权力。根据这项新立法，澳大利亚联邦警察（AFP）和澳大利亚刑事情报委员会（ACIC）将有权删除或删除与涉嫌犯罪活动有关的数据，允许访问设备和网络，甚至允许为了调查目的接管在线账户。这些新权限将允许执法部门删除在勒索软件攻击中窃取的数据，以及存储在攻击者操作的服务器上用于双重勒索的数据。通过删除这些数据，执法部门希望在受害者不支付赎金的情况下防止潜在的数据泄露。

（三）中国

针对敲诈勒索

信息网络技术支持和帮助、制作传播计算机病毒等危害网络安全方面的规定较为完善

在我国，勒索攻击事件频发，对人民生产生活造成了严重的影响。从法律法规角度，完善的相关法律法规是打击勒索攻击的第一步。目前，我国现行法律没有针对勒索软件的专门性规定，但是，针对敲诈勒索、信息网络技术支持和帮助、制作传播计算机病毒等危害网络安全方面的规定较为完善。

1997.03

《刑法》及后续历次修正案

1997 年 3 月的《刑法》及后续历次修正案，在第 274 条规定了敲诈勒索罪，第 285 条规定了非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪、非法控制计算机信息系统罪和提供侵入、非法控制计算机信息系统程序、工具罪；第 286 条将计算机病毒作为破坏性程序的一种，第 287 条之一规定了非法利用信息网络罪，287 条之二规定了帮助信息网络犯罪活动罪。

2000.04

《计算机病毒防治管理办法》

2000 年 4 月，《计算机病毒防治管理办法》明确规定，任何单位和个人不得制作、传播计算机病毒，并规定了相应的警告、罚款、没收非法所得等行政处罚。

2005

《治安管理处罚法》第 29 条

2005 年，《治安管理处罚法》第 29 条规定故意制作、传播计算机病毒等破坏性程序，影响计算机信息系统正常运行的，可予以十日以下拘留。

2011 年 8 月，《最高人民法院、最高人民检察院关于办理

2011.08

《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》第 5 条

危害计算机信息系统安全刑事案件应用法律若干问题的解释》第 5 条界定了破坏性程序的范围，包括：（1）能够通过网络、存储介质、文件等媒介，将自身的部分、全部或者变种进行复制、传播，并破坏计算机系统功能、数据或者应用程序的；（2）能够在预先设定条件下自动触发，并破坏计算机系统功能、数据或者应用程序的；（3）其他专门设计用于破坏计算机系统功能、数据或者应用程序的程序。

2013.04

《最高人民法院、最高人民检察院关于办理敲诈勒索刑事案件适用法律若干问题的解释》

2013 年 4 月，《最高人民法院、最高人民检察院关于办理敲诈勒索刑事案件适用法律若干问题的解释》明确了量刑标准，并在第 7 条规定：明知他人实施敲诈勒索犯罪，为其网络技术支持等提供帮助的，以共同犯罪论处。

2016.11

《网络安全法》

2016 年 11 月，《网络安全法》出台，促进了网络安全等级保护制度的全面开展。该法规定，网络运营者应当按照网络安全等级保护制度的要求，履行多项安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。明确要求任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。同时，要求网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。该法建立了较为全面的管理制度遏制勒索病毒。

2021.06

《数据安全法》

2021 年 6 月，《数据安全法》公布，进一步加强了数据安全领域基础性制度的建设，其中第三十二条规定：“任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据”。同时，第五十一条规定：“禁止以窃取

或者其他非法方式获取数据，违反者，将依照有关法律、行政法规的规定处罚”。

2021 年 7 月，工信部、国家互联网信息办公室、公安部联合发布《网络产品安全漏洞管理规定》，其中明确了网络产品提供者、网络运营者，以及从事漏洞发现、收集、发布等活动的各类主体的责任和义务，推动了网络产品安全漏洞管理工作的制度化、规范化、法制化。同月，国家互联网应急中心发布了《勒索软件防范指南》，其中规定了防范勒索软件要做到九要、四不要，包括要备份重要数据和系统、要设置复杂密码并保密、要做好身份验证和权限管理、要制定应急响应预案等九项建议，以及不要点击来源不明邮件、不要打开来源不可靠网站、不要安装来源不明软件，以及不要插拔来历不明的存储介质等四项建议。

2021.07

工信部、国家互联网信息办公室、公安部联合发布

《网络产品安全漏洞管理规定》

国家互联网应急中心发布

《勒索软件防范指南》

2021年8月，国务院发布《关键信息基础设施安全保护条例》。《条例》对《网络安全法》所确立的关键信息基础设施安全保护制度作了进一步细化完善，明确了国家网信部门、国务院公安部门以及重要行业和领域的主管部门、监督管理部门等相关职能部门的责任边界和职责要求，明确了关键认定原则和认定机制，细化了运营者的主体责任和义务，形成了关键安全保护工作相关各方的法律责任体系。同月，《个人信息保护法》正式公布。《个人信息保护法》是我国个人信息保护领域的专门立法和基础性立法，进一步建立健全了个人信息保护制度，其明确要求任何组织、个人不得侵害自然人的个人信息权益，并不得通过误导、欺诈、胁迫等方式处理个人信息。同时，任何组织、个人也不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；不得从事危害国家安全、公共利益的个人信息处理活动。该法全面禁止了涉及个人信息的诸多违法行为，为打击涉及勒索软件等侵犯公民、组织个人信息的行为提供了更加坚实的法治保障。

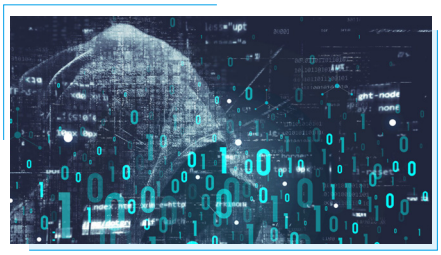
2021.08

国务院发布

《关键信息基础设施安全保护条例》

《个人信息保护法》

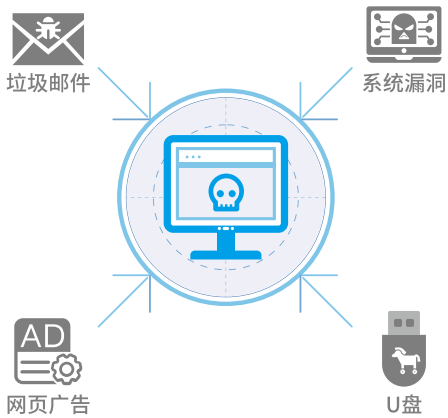
第三章
勒索攻击主要特点



自诞生之日起，勒索攻击便呈现出与其他形式网络攻击大相径庭的特点，正是因为这些独特之处，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，熟悉勒索攻击的惯用手段和趋势特点将有助于我们更加从容地应对此类攻击。总的来看，勒索攻击有以下主要特点。

一、勒索攻击行为隐蔽性强且危害显著

隐蔽性是勒索攻击的典型攻击策略。勒索攻击善于利用各种伪装达到入侵目的，常见的传播手段有垃圾邮件、网页广告、系统漏洞、U 盘等。例如，2019 年 2 月出现的勒索病毒 Clop，能够通过携带有效数字签名的方式躲避系统和防毒软件的防御，进而达到入侵目标计算机的目的。为了保持高隐蔽性，部分勒索攻击还会采取智能攻击策略：在入口选择上，攻击者以代码仓库为感染位置对源代码发动攻击；在上线选择上，宁可放弃大量的机会也不愿在非安全环境上线；在编码上，高度仿照目标公司的编码方式和命名规范以绕过复杂的测试、交叉审核、校验等环节。



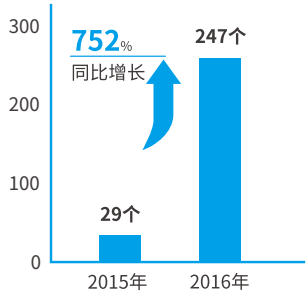
此外，攻击者往往在发动正式攻击之前就已控制代码仓库，间隔几个月甚至更长时间才引入第一个恶意软件版本，其潜伏时间之长再一次印证了勒索攻击的高隐蔽性。

调查发现，某些勒索攻击事件的制造者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。

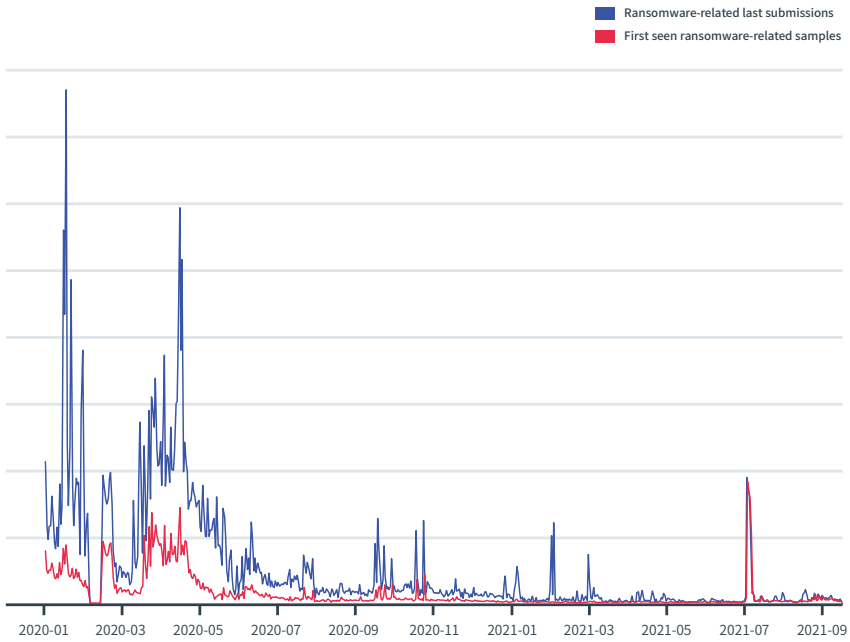
此外，勒索攻击一般具有明确的攻击目标和强烈的勒索目的，勒索目的由获取钱财转向窃取商业数据和政治机密，危害性日益增强。例如，2021 年 5 月，爱尔兰卫生服务执行局（HSE）遭遇勒索攻击，犯罪分子窃取多达 700GB 的未加密文件，致使全国多家医院电子信息系统无法访问，新冠病毒检测工作受阻。爱尔兰方面表示，此次网络攻击可能是爱尔兰遭受的最严重网络攻击。我国国内也出现过类似的勒索攻击事件，例如，某建筑设计院遭遇勒索病毒攻击，数千台电脑文件被加密，工程图纸无法访问，损失惨重；某网约车系统遭遇勒索病毒攻击，导致所有用户无法使用网约车服务；某医院遭遇勒索病毒攻击，导致医院就诊服务全面崩溃等。

二、勒索病毒变异较快且易传播

目前，活跃在市面上的勒索攻击病毒种类繁多，而且每个家族的勒索病毒也处于不断地更新变异之中。2016 年，勒索软件变体数量达 247 个，而 2015 年全年只有 29 个，其变体数量比上一年同期增长了



752%[20]。变体的增多除了借助飞速发展的先进网络技术以外，还与网络攻击者“反侦查”意识的增强相关。很多勒索软件编写者知道安全人员试图对其软件进行“逆向工程”，从而不断改进勒索软件变体以逃避侦查。以下是 VirusTotal 对勒索样本更新速度的追踪趋势图[21]，由此可见大部分时候，勒索软件作者都实现了对样本的快速更新，总是使用新的样本进行攻击投递，以躲避检测。



VirusTotal 对勒索样本更新速度的追踪趋势图

此外，蠕虫式传播型勒索病毒可进行自我复制、自主传播，传播速度更快，波及范围更广。近年来，勒索攻击席卷全球，几乎所有国家的政府、金融、教育、医疗、制造、交通、能源等行业均受到影响，与勒索病毒的强感染力和易传播性密不可分。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——WannaCry 2.0，与之前版本的不同是，这个变种不能通过注册“开关域名”来遏制传播，因而传播速度变得更快。使用“加密病毒勒索软件”攻击技术的勒索软件攻击愈加受到关注。目前，比较受关注的勒索软件及运营团伙见下表。

20 引自国家保密局官网 http://www.gjbmj.gov.cn/n1/2019/0319/c411145-30983492.html
21 https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf

比较受关注的勒索软件及运营团伙

名词	简介	工作原理	目标受害者	归因
Cerber	Cerber 是一个 RaaS 平台，于 2016 年首次出现，并且在当年 7 月为攻击者净赚 200,000 美元。	Cerber利用Microsoft漏洞感染网络，其功能与其他勒索软件类似，主要使用 AES-256 算法对文件进行加密，攻击覆盖多种文件类型，包括文档、图片、音频文件、视频、档案和备份。	似乎没有针对任何特定实体。	Cerber 的创作者在一个私人俄语论坛上出售服务。
Conti	Conti RaaS 平台于2020年5月首次出现，被认为是 Ryuk 勒索软件的后继产品。目前至少发现了三个新版本。	Conti 使用双重威胁策略，即保留解密密钥并出售或泄露受害者的敏感数据。Conti 通过使用多线程来快速加密文件。	2021 年 1 月的最新一轮感染似乎针对政府组织，但作为 RaaS 行动，对任何组织 / 个人都构成威胁。	Conti 是独立团伙运作，其成员身份不明。
Crypto Locker	CryptoLocker 于 2013 年首次被发现，开启了现代勒索软件时代，并在其高峰期感染了多达 500,000 台 Windows 计算机，也被称为 TorrentLocker。	CryptoLocker 是一种木马程序，在受感染的计算机、任何内部或网络连接的存储设备中搜索要加密的文件。通常通过网络钓鱼电子邮件进行分发，邮件带有包含恶意链接的文件附件。一旦打开文件，就会激活下载程序，从而感染计算机。	似乎没有针对任何特定实体。	Crypto Locker 是由犯罪团伙成员创建的，该犯罪团伙还开发了银行木马 Gameover Zeus。
Crypto Wall	又名 CryptoBit 或 CryptoDefense，于 2014 年首次出现，并在 CryptoLocker 关闭后开始流行。	通过垃圾邮件或漏洞，利用工具包进行分发。CryptoWall 的开发人员似乎避免使用复杂的方法，更倾向于简单但有效的经典勒索软件方法。在运营的前六个月，它感染了 625000 台电脑。	该勒索软件已经损害全球数以万计的组织，但避开了俄语环境的国家。	CryptoWall 开发人员很可能来自讲俄语的国家。
CTB-Locker	CTB-Locker 于 2014 年被首次报道，以高感染率而闻名。2016 年，以 web 服务器为目标的新版本的 CTB-Locker 发布。	勒索软件会员必须向 CTB-Locker 开发人员支付月费，才能访问托管的勒索软件代码。该勒索软件使用椭圆曲线密码来加密数据。它还以多语言能力而闻名，这使潜在受害者遍布全球。	鉴于其 RaaS 模式，CTB Locker 对任何组织都是威胁，尤其是来自西欧、北美和澳大利亚等国家。	

名词	简介	工作原理	目标受害者	归因
Doppel Paymer	DoppelPaymer 于 2019 年 6 月首次出现，至今仍然活跃。	DoppelPaymer 团伙使用不同寻常的战术，即通过伪造的美国电话号码打给受害者，要求支付赎金，一般赎金为 50 比特币左右（最初为 60 万美元）。他们声称自己来自朝鲜，并威胁会泄露或出售被盗数据。在某些情况下，他们还会威胁受害公司的员工。	医疗保健、紧急服务和教育等关键行业。	疑似由 Dridex 特洛伊木马背后的一个分支 TA505 负责。
Egregor	Egregor 出现在 2020 年 9 月。2021 年 2 月 9 日，美国、乌克兰和法国当局在联合行动中逮捕了 Egregor 的集团成员和附属机构成员，使其网站下线。	Egregor 遵循“双重勒索”趋势，既加密数据又威胁如果不支付赎金就泄露敏感信息。它的代码库相对复杂，并且能够通过使用混淆和反分析技术来避免检测。	Egregor 破坏了全球 19 个行业的至少 71 个组织。	Egregor 的崛起与 Maze 勒索软件团伙的关闭相吻合，因此判断 Maze 的分支机构转移到 Egregor。
FONIX	FONIX 是一种 RaaS 产品，于 2020 年 7 月首次被发现。经历了多次代码修订后于 2021 年 1 月突然关闭，且 FONIX 运营团伙随后释放了主要密钥。	FONIX 运营团伙在网络犯罪论坛和暗网上宣传其服务。FONIX 的购买者向该团伙发送电子邮件地址和密码。然后，该团伙将定制的勒索软件有效载荷发送给买方，攻击成功后，运营团伙收取 25% 的赎金作为报酬。	似乎没有针对任何特定实体。	未知
Gand Crab	GandCrab 可能是有史以来最赚钱的 RaaS 产品。GandCrab 于 2018 年 1 月首次被发现。	该恶意软件通常通过网络钓鱼电子邮件发送的恶意 Microsoft Office 文档进行分发。目前，GandCrab 的变体通过利用 Atlassian’s Confluence 等软件中的漏洞注入恶意模板，从而完成远程代码执行。	GandCrab 已经在全球多个行业感染了系统，但避免在俄语地区的活动。	俄罗斯网络犯罪组织
Golden Eye	GoldenEye 出现在 2016 年，疑似基于 Petya 勒索软件的变种。	GoldenEye 最初瞄准人力资源部门，以投递虚假的求职信和简历发动攻击。一旦其有效负载感染计算机，就会执行一个宏来加密计算机上的文件，并在每个文件的末尾添加一个随机的 8 个字符扩展名。然后，勒索软件使用自定义启动加载程序修改计算机的硬盘主启动记录。	以说德语的用户为目标。	未知

名词	简介	工作原理	目标受害者	归因
Jigsaw	Jigsaw 于 2016 年首次出现，但很快研究人员就公布了解密工具。	Jigsaw 最特别之处在于它加密了一些文件后会索要赎金，然后逐步删除文件，直到受害者支付赎金为止。基本每小时删除一个文件，一般持续 72 个小时，超过这个时间，将删除所有剩余文件。	不针对特定目标	未知
KeRanger	2016 年发现的 KeRanger 被认为是第一个旨在攻击 Mac OS X 应用程序的可运行勒索软件。	通过合法但受感染的 BitTorrent 客户端进行分发，该客户端具有有效的证书，能够逃避检测。		
Leather locker	Leatherlocker 于 2017 年在两个 Android 应用程序中被发现，Booster & Cleaner 和 Wallpaper Blur HD。	当受害者下载似乎合法的应用程序后，该应用会请求权限，以授予执行所需的恶意软件访问权限。该勒索软件不加密文件，而是锁定设备主屏幕禁止受害者访问数据。	下载受感染应用程序的 Android 用户	未知
Locker Goga	LockerGoga 在 2019 年针对工业公司的攻击中活跃。	LockerGoga 使用包含恶意文档附件的网络钓鱼活动来感染系统。有效负载使用有效证书签名，从而使它们可以绕过安全性。	欧洲的制造业公司，其中最著名的受害者是 Norsk Hydro 公司，攻击导致该全球 IT 系统的瘫痪。	
Locky	Locky 于 2016 年开始传播，并使用类似于银行恶意软件 Dridex 的攻击模式。Locky 激发了包括 Osiris、Diablo6 在内的多个变种。	向受害者发送一封带有 Microsoft Word 文档的电子邮件，声称为发票，其中包含恶意宏。	早期针对医院，后期没有针对性。	Locky 背后的网络犯罪组织疑似隶属于 Dridex 背后的组织。
Maze	Maze 是一个相对较新的勒索软件组织，于 2019 年 5 月被发现。2020 年 9 月，Maze 宣布将关闭其运营。	Maze 攻击者通常使用可以通过网络钓鱼活动来猜测或获取有效凭据，远程进入网络。然后，该恶意软件会使用开源工具扫描网络，以发现漏洞。接着会在整个网络中横向移动，以寻找更多可用于特权升级的凭据。找到域管理员凭据后，就可以访问和加密网络上的任何内容。	遍及全球所有行业。	拥有共同专长的多个犯罪集团，而非单一团伙。

名词	简介	工作原理	目标受害者	归因
Net walker	Netwalker 自 2019 年以来一直活跃，它使用双重威胁，即扣留解密密钥和出售或泄露被盗数据。2021 年 1 月，美国司法部宣布一项全球行动，扰乱了 Netwalker 的运作。	从技术角度来看，Netwalker 是相对普通的勒索软件，利用网络钓鱼电子邮件获得据点，对数据进行加密和渗漏，并发送赎金要求。据悉，该公司发布被盗数据的方法是将数据放在暗网上的受密码保护的文件夹中，然后公开释放密钥。	医疗保健和教育机构	由 Circus Spider 运营
NotPetya	首次出现于 2016 年，实际上是数据破坏类恶意软件（“刮水器”），但其伪装成了勒索软件。	NotPetya 与 Petya 类似，都会加密文件并要求以比特币支付赎金。但不同的是，Petya 要求受害者点击恶意邮件，从而启动恶意软件并获取管理员权限，但 NotPetya 可以在没有人工干预的情况下进行传播。	据称，集中在乌克兰	据称俄罗斯 GRU 内的 Sandworm 小组
Petya	Petya 恶意软件的初始版本于 2016 年 3 月开始传播。这个名字来自于 1995 年 007 电影《黄金眼》中的一颗卫星。而一个疑似该恶意软件作者的推特账号使用了扮演反派的演员艾伦 - 卡明的照片作为头像。	Petya 通过一封声称是求职者简历的邮件发送，其中包含两个文件：一个年轻男子的图像和一个可执行文件。当受害者点击该文件时，Windows 用户访问控制警告会告诉他们，该可执行文件将对计算机进行更改。一旦受害者接受更改，恶意软件就会加载，然后通过攻击存储介质上的低级结构拒绝访问。	任何 Windows 系统都是潜在的目标，但乌克兰是这次攻击的重灾区。	未知
Pure locker	在 2019 年发现的 PureLocker RaaS 平台，目标是运行 Linux 或 Windows 的企业生产服务器。因为它是用 PureBasic 语言编写的，因此得名。	PureLocker 依靠 more_eggs 后门恶意软件获得访问权，而非钓鱼尝试。攻击者针对已经被入侵的计算机，有选择地对数据进行加密。	只有少数犯罪团伙能够负担得起 PureLocker 的费用，因此更针对高价值目标。	恶意软件即服务提供商可能是 PureLocker 的幕后黑手。
Robbin Hood	RobbinHood 是使用 EternalBlue 的勒索软件变体。	RobbinHood 最独特的地方在于其有效载荷如何绕过终端安全。它有五个部分：杀死安全产品的进程和文件的可执行文件、部署有签名的第三方驱动和恶意的无签名内核驱动的代码、有漏洞的旧版本 Authenticode-signed 驱动、杀死内核空间的进程和删除文件的恶意驱动，以及一个包含要杀死和删除的应用程序列表的文本文件。	Baltimore 和 Greenville 的地方政府是重灾区。	未知

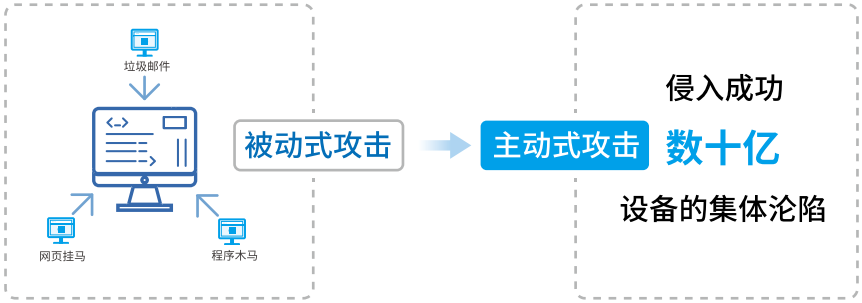
名词	简介	工作原理	目标受害者	归因
Ryuk	Ryuk 于 2018 年 8 月首次出现，是基于 2017 年在地下网络犯罪论坛上出售的一个名为 Hermes 的旧勒索软件程序开发的。	通常与 TrickBot 等其他恶意软件结合使用。Ryuk 运营团伙以使用手动黑客技术和开源工具在专用网络中横向移动，并在启动文件加密之前获得尽可能多的系统管理访问权而闻名。	企业、医院和政府组织	最初归因于朝鲜拉撒路集团（Lazarus Group）。
SamSam	SamSam 自 2015 年以来活跃至今，主要针对医疗保健组织，并在接下来的几年中大幅提升。	SamSam 的控制器探测预选目标的弱点，利用从 IIS 到 FTP 到 RDP 的一系列漏洞。一旦进入系统，攻击者就会升级特权，以确保在开始加密文件时，攻击具有极大的破坏性。	医疗保健和政府组织	最初被认为起源于东欧。2018 年底，美国司法部起诉两名伊朗人，声称他们是攻击的幕后黑手。
Simple Locker	2014 年出现的 SimpleLocker 是第一个广泛针对移动设备（尤其是 Android 设备）的勒索软件。	当受害者下载恶意应用程序时，SimpleLocker 会感染设备。随后，恶意软件会在设备的 SD 卡上扫描某些文件类型，并进行加密。最后，显示赎金和有关付款方式的说明。	由于赎金票据是俄文并要求以乌克兰货币付款，因此推测攻击者最初的目标是该地区。	由开发其他俄罗斯恶意软件（例如 SlemBunk 和 GM Bot）的同一位黑客编写的。
Sodinokibi /REvil	Sodinokibi 是一个 RaaS 平台，于 2019 年 4 月首次出现，并在 2019 年除夕关闭了英国货币兑换服务 Travelex。该勒索软件与 GandCrab 有关，并且代码不在俄罗斯和几个邻国以及叙利亚执行。	Sodinokibi 以多种方式传播，包括利用 Oracle WebLogic 服务器或 Pulse Connect Secure VPN 中的漏洞 。它的目标是微软 Windows 系统，并对除配置文件外的所有文件进行加密。如果受害者不支付赎金，他们的敏感数据将被出售或公布在地下论坛上。	其所排除地区以外的全球不同组织。	Sodinokibi 在 GandCrab 关闭后崭露头角。一名据称是该集团成员的人，证实该勒索软件是建立在一个旧的代码库之上。
Tesla Crypt	TeslaCrypt 是 Windows 勒索软件木马，2015 年首次出现，主要针对计算机游戏玩家。2016 年 5 月，开发者关闭了运营并发布了主密钥。	在受害者访问了运行漏洞工具包的黑客网站之后，TeslaCrypt 会查找并加密游戏文件，如游戏保存、录制的重播和用户配置文件。然后索要价值 500 美元的比特币来解密文件。	电脑游戏玩家	未知

名词	简介	工作原理	目标受害者	归因
Thanos	Thanos 出现在 2019 年末，是第一个使用 RIPlace 技术，可以绕过大多数反勒索软件策略的勒索软件。	Thanos 一般在地下论坛和其他封闭渠道发布广告，作为一个定制的工具，其附属机构使用它来创建勒索软件有效载荷。		
WannaCry	由于美国国家安全局（NSA）开发的永恒之蓝漏洞被黑客窃取，2017 年 5 月，WannaCry 蠕虫通过计算机网络迅速传播，感染了数百万台 Windows 电脑。	WannaCry 由多个组件组成，以 dropper 的形式到达受感染的计算机。dropper 作为一个自带程序，可以提取嵌入自身的其他应用组件。一旦启动，WannaCry 将尝试访问硬编码的 URL。	攻击影响了全球范围的公司，但在医疗保健、能源、运输和通讯领域企业受到打击更为严重。	据称为朝鲜的拉撒路集团（Lazarus Group）。
Wasted Locker	WastedLocker 于 2020 年 5 月开始攻击。该勒索软件相对复杂，且其创作者以索要高额勒索费而闻名。	该恶意软件使用基于 JavaScript 的攻击框架 SocGholish，该框架在一个感染的网站上以虚假更新的方式，通过 ZIP 文件形式进行分发 。	最有可能支付高额赎金的目标，主要针对北美和西欧。	知名的犯罪团伙 Evil Corp。
WYSIWYE	WYSIWYE（所看到的就是所加密的）是针对 Windows 系统的 RaaS 平台，于 2017 年被发现。	在网络上扫描打开的远程桌面协议（RDP）服务器，然后使用弱凭据执行登录尝试。购买所见即所得服务的犯罪分子一般可以选择要加密的文件类型以及加密后是否删除原始文件。	最初出现在德国、比利时、瑞典和西班牙。	未知
Zeppelin	Zeppelin 首次出现在 2019 年 11 月，是 Vega 或 VegasLocker RaaS 产品的后代。	Zeppelin 拥有丰富的功能（尤其是在可配置性方面），可以通过多种方式部署，包括作为 EXE、DLL 或 PowerShell 加载程序进行部署。	Zeppelin 比 Vega 更具针对性，即不在俄罗斯、乌克兰、白俄罗斯或哈萨克斯坦运行的计算机上执行，更多针对北美和欧洲的医疗保健及技术公司。	疑似来自俄罗斯的攻击者通过 Vega 的代码库开发了 Zeppelin。

数据来源：《CSO 指南：全球最危险也最有名的勒索软件清单》， 以上内容，不代表白皮书观点。

三、勒索攻击路径和目标多元化发展

早期大部分勒索软件以垃圾邮件、程序木马、网页挂马等方式进行传播，然而，近年来，越来越多的攻击事件表明，勒索攻击正在由被动式攻击转为主动式攻击。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，随着开放性日益增加，设备中普遍存在的高危漏洞给了勒索攻击以可乘之机，一旦侵入成功即可造成多达数十亿台设备的集体沦陷。随着远程监控和远程操作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，实现盗取数据、中断生产的目的。为了成功绕过外部安装的防火墙等安全设施，不少勒索攻击诱导企业内部员工泄露敏感信息。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，一旦发现系统已有漏洞则立即感染侵入。



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。勒索病毒大多以电脑设备为攻击目标，其中 Windows 操作系统是重灾区。但是，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。卡巴斯基俄罗斯实验室检测发现，2019 年，针对移动设备用户个人数据的攻击达 67500 个，相比 2018 年增长了 50%。同年，卡巴斯基移动端产品共检测到 350 多万个恶意安装软件包，其中包含近 7 万个新型移动端银行木马和 6.8 万多个新型移动端勒索软件木马 [22]。

22 引自 https://www.163.com/dy/article/F732DQ350511CJ6O.html

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，但是，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。例如，在今年 7 月 16 日发生的国家级勒索事件中，厄瓜多尔最大网络运营商 CNT 遭遇勒索软件 RansomEXX 的攻击，致使其业务运营、支付门户及客户支持全部陷入瘫痪，犯罪团伙声称取得 190GB 的数据，并在隐藏的数据泄露页面上分享了部分文档截图。

四、受勒索攻击领域更加宽泛

勒索软件攻势愈演愈烈，受到勒索攻击的领域和行业也覆盖关键基础设施等，涉及金融、医疗、教育、食品等行业。2021 年的几次勒索攻击事件致使关键燃料管道、大型肉类加工企业以及其他对于民众日常生活与安全至关重要的基础设施陷入瘫痪。这也使越来越多的普通民众可以感受到勒索攻击造成的影响。美国网络与基础设施安全局网络安全执行助理主任艾瑞克·戈德斯坦（Eric Goldstein）表示，“随着恶意网络攻击者不断将大型与小型企业、组织及政府部门作为目标，越来越多的美国民众开始切身体会到勒索攻击流行带来的现实后果。”

（一）关键基础设施

今年以来，美国科洛尼尔油管公司遭遇勒索软件攻击，并引发一场全美有史以来规模最大的输油管线停摆事故。专为欧洲能源及基础设施企业提供技术方案的厂商挪威公司 Volue 遭遇勒索软件攻击，被迫疲于奔命。这两次勒索攻击凸显出能源与关键基础设施公司已成为勒索软件攻击的头号目标。美国国家安全局网络安全主管罗伯·乔伊斯（Rob Joyce）曾经发出警告，勒索攻击活动背后的网络犯罪分子，长期以来一直在紧盯包括国防工业在内的各类关键基础设施。

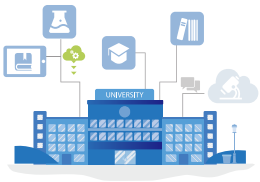
（二）医疗系统

今年以来，医院与诊所的沦陷，标志着勒索攻击又找到了新的攻击对象。美国 Check Point 公司的安全报告指出，医院

45%

和医疗机构已经成为越来越多勒索软件攻击的目标。自 2020 年 11 月份以来，平均每个医疗机构每周遭到 626 次网络攻击，攻击方法主要包括勒索软件、僵尸网络、远程代码执行和分布式拒绝服务（DDoS）攻击，全球针对医疗机构的攻击数量增加了 45%，是同期全球其他行业遭受网络攻击次数的两倍多。2021 年 5 月，美国 FBI 在发布的一份报告中强调，在上报的 400 起攻击活动当中，至少有 16 起指向美国医疗保健服务商与急救网络。

（三）学校网络



网络防护薄弱

学校网络防护的薄弱给攻击者可乘之机，这也是黑客一直把学校视为常规攻击目标的原因。近年来，不断加剧的勒索软件攻势让这一问题进一步恶化，致使学校网络成为网络攻击的重要目标之一。而且，常常发生的情况是，如果被勒索的校方不付款，黑客经常会在自己的网站上发布受害者信息。2021 年 2 月，在俄亥俄州托莱多公立学校遭遇勒索软件攻击后几个月，黑客们在网上公布了学生的姓名和社保号码。2020 年 12 月，有黑客闯入得克萨斯南部边境附近的韦斯拉科独立学区。工作人员迅速采取行动，向超过 48000 名家长及监护人发出警报。他们听从了 FBI 的建议没有向黑客付款，并利用应急备份恢复了校方系统。但是，由于拒不付款，黑客最终将窃取到的文件转储到了泄密网站上。目前，网络上仍然公开一个名为“学生基本信息”的 Excel 电子表格，其中包含约 16000 名学生的基本情况，相当于韦斯拉科当地 20 所学校一年招生人数的总和。

（四）食品与农业

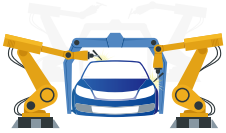
影响社会生产生活

在涉及民生的食品供应和农业生产供应链上，如果一个环节出现问题，则会影响正常的社会生产生活。2021 年 9 月 1 日，美国 FBI 曾经发布一份通报，警告食品与农业企业关注针对供应链的勒索软件攻击。FBI 指出，“面对勒索软件侵害，食品与农业企业可能因支付赎金、丧失生产力、后期补救成本等情况承受重大经济损失。企业也可能泄露专有信息与个人身份数据，或因勒索软件攻击而遭受声誉损失。”自 2020 年 11 月以来，

已经发生了多起针对食品与农业部门的勒索攻击，包括对美国面包供应商的 Sodinokibi/REvil 勒索软件攻击、针对全球肉类加工商 JBS 的攻击、针对美国饮料企业的攻击以及针对美国一家农场的攻击。这些攻击不仅给被攻击方造成损失，例如 JBS 最终向 REvil 勒索软件团伙支付了 1100 万美元赎金，也影响了社会生活，例如由于勒索攻击导致美国、澳大利亚及其他多国出现肉类短缺。

（五）保险行业

2021 年，保险公司已经成为勒索攻击者眼中极具吸引力的目标，已有多家大型保险公司遭到勒索软件毒手。2021 年 3 月，美国第七大商业保险公司 CNA Financial Corporation 遭遇 Phoenix CrypotoLocker 勒索软件攻击，攻击方还窃取了包含客户信息的文件。5 月，Avaddon 勒索软件团伙攻击了 AXA 在泰国、马来西亚、香港及菲律宾的多家分支机构，并宣称成功窃取到 3 TB 数据。



100 家
最大汽车制造商

50%
受到勒索攻击软件影响

17%
可能收到攻击

（六）汽车行业

随着自动驾驶、电动汽车、联网汽车和共享汽车的迅猛发展，正处于转型期的汽车行业，也成为网络犯罪的目标。继能源和物流业之后，汽车行业是过去一年中全球受攻击最严重的行业之一。根据一份勒索软件趋势报告，在全球 100 家最大的汽车制造商中，有近 50% 受到勒索软件攻击的严重影响。此外，超过 17% 的汽车供应商最有可能遭受勒索软件攻击。汽车制造商遭到勒索软件攻击重创的典型例子是 2017 年 WannaCry 病毒爆发。这次攻击影响了 150 多个国家的 20 多万台计算机，其中包括雷诺在法国、斯洛文尼亚和罗马尼亚的制造厂都受到严重影响，导致所有的工业生产都被关闭，并连续数日处于停工状态。2021 年，汽车制造公司受到攻击的例子是，大型汽车制造商大众（Volkswagen）和奥迪（Audi）成为 Conti 勒索软件的受害者。在美国和加拿大，超过 330 万客户和潜在买家受到了这次攻击的影响。

第四章 勒索攻击七大发展趋势

在后疫情时代，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。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攻击趋势。

一、影响社会正常运转且难解密

勒索攻击对社会正常运转带来较大挑战。

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 遭到勒索病毒攻击，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雪上加霜。

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。2021 年 8 月，美国医疗连锁机构 Memorial Health System 遭到勒索攻击，导致 IT 系统瘫痪，分布在美国西弗吉尼亚州和俄亥俄州的三家医院和数十家诊所被迫取消手术预约，并将患者转移至其他医疗机构。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。

> **业内专家普遍认为，遭受勒索攻击之后，没有“特效药”**

勒索攻击使用的加密手段越来越复杂多样，绝大多数不能被解密，因其所采用的非对称加密算法的密钥长度长且很难被反向破解。业内专家普遍认为遭受勒索攻击之后，没有“特效药”。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，但是依靠现有的算力或者是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上百年的时间。极少数报道中提到的可解密案例主要是以下两种情况：一是出于各种各样的原因，勒索病毒的制作者会泄露病毒的内部资料。二是勒索病毒自身存在的漏洞大大降低了破解难度。但是，这种情况越来越少，勒索病毒的运作已经演进到标准化甚至专业化的程度，病毒制作者往往有成套、完整的代码可以参考。

同时，需要注意的是，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 Emsisoft 统计数据，2021 年美国有 1200 多所 K-12 学校的数据被勒索攻击团队窃取并公布。大部分学校并没有意识到数据泄露，公立学校在保护学生数据免受攻击方面，远远不及私营企业，主要原因在于学校没有足够多预算聘用网络安全专家或者采购保护服务。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。

美国

1200+

K-12学校

攻击范围向学校及儿童数据隐私领域拓展

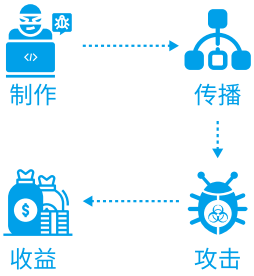
二、勒索软件即服务成为网络攻击新模式

随着云计算、人工智能等新技术的快速普及和应用，勒索软件即服务（SaaS）成为当前网络攻击的新模式。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病毒，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。例如，依靠这种黑产模式，某勒索攻击软件仅用一年多时间就敛财 20 亿美元。

当前网络攻击的新模式

勒索攻击从制作、传播、攻击到收益呈现系统化、便捷化趋势，开发者可以提供一整套解决方案，甚至包括利用加密货币进行赎金支付等服务。这些解决方案具有“开箱即用”的便捷性，犯罪分子获得勒索病毒后，可以通过多种渠道进行传播并获利，攻击模式更为便捷。此外，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就可以通过这类服务开展勒索攻击，导致网络攻击的门槛大幅降低。

系统化、便捷化趋势



三、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 150 多个国家和地区迅速蔓延的 WannaCry 勒索病毒赎金仅为 300 美元。四年后，勒索病毒要求企业支付的赎金则大多在上百万美元。Sodinokibi 勒索病毒在 2019 年前后出现在中国时，索要金额仅 7000 元人民币，到了 2020 年，该团伙索要的勒索金额已动辄千万美元以上。2020 年 3 月，计算机巨头宏碁公司遭到勒索软件 Revil 攻击，被要求支付 5000 万美元赎金；2020 年 11 月，富士康墨西哥工厂受到勒索病毒 DoppelPaymer 的攻击，被要求支付超过 3400 万美元赎金。

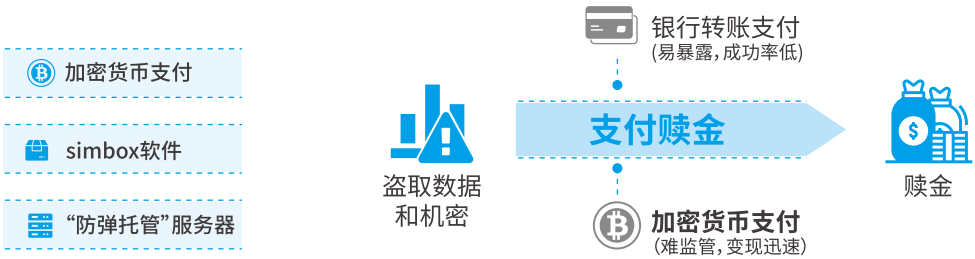
300美元

5000万美元

3400万美元

高额赎金不仅让网络攻击者赚得盆满钵满，同时，勒索攻击者可以借此招揽更多人铤而走险加入勒索攻击行列。对于网络攻击者来说，勒索模式和网络入侵相结合是一种较为便利的套现模式。早期的网络攻击想要套现，需要冒险尝试很多不同的路径，例如“偷数据、卖数据”的模式。但是，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，一定程度上让加密货币成为网络犯罪快速增长的“助推剂”。

除了加密货币之外，其他技术也被网络攻击者充分利用。例如，可以隐藏电话来源的 simbox 软件，被攻击者用来发送垃圾邮件或者短信；“防弹托管”服务器具有较好的安全性和私密性，攻击者的犯罪信息可以在这里快速转移。



四、基础设施成为攻击重点

传统勒索病毒攻击者使用广撒网、误打误撞的手法，这种无差别攻击很难预测受害者是谁，哪些受害者有价值，如果受害者是普通用户，则其数据价值相对不高且缴纳赎金的意愿也不强烈。同时，早期勒索攻击大多以病毒的形式发动，攻击者将制作好的恶意软件投放出去，而后由勒索病毒自行发起入侵。但是，这种模式很难保证持续性，如 WannaCry 病毒的大规模爆发正是钻了“永恒之蓝”系统漏洞的空子。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。所谓 APT 化，即攻击不计成本、不择手段，从低权限账号入手，持续渗透攻击，直到控制企业核心服务器，

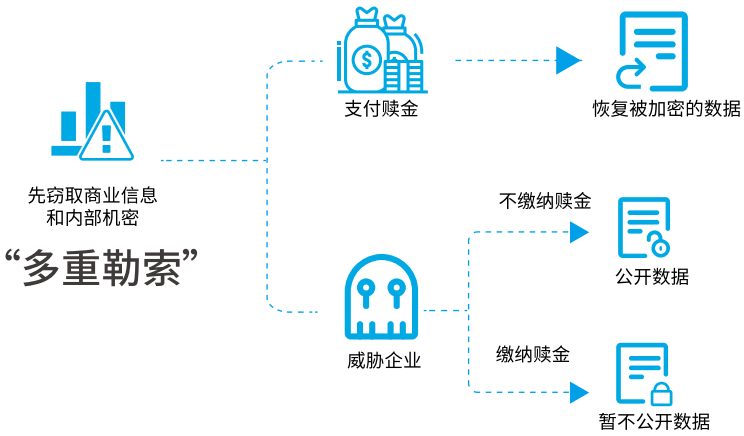
再释放勒索病毒，使巨型企业彻底瘫痪。此外，勒索攻击 APT 化还意味着病毒的入侵过程由人工操控完成，入侵后的数据加密等环节则由勒索病毒自动完成，攻击者入侵后会首先窃取该企业的核心数据，即使企业使用备份恢复系统，核心机密泄露也会导致极其严重的损失。

波音公司、台积电、富士康、全球最大的助听器制造商 Demant、法国最大商业电视台 M6 Group 都曾成为被攻击对象。有报告显示，2020 年，美国有约 2400 家医疗机构、学校和政府部门遭受勒索攻击，新冠肺炎疫情导致越来越多的人依赖远程办公，这在某种程度上进一步增加了勒索攻击的频次和概率。网络隐私保护软件公司 BlackFog 研究发现，2020 年，勒索攻击呈现集聚化发展态势，其中针对政府部门、制造业、教育和医疗保健等行业的勒索威胁最为严重。由此看来，勒索对象主要集中于大中型企业和基础设施类组织，背后原因有两点：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。

同时，攻击者开始针对特定企业制定攻击策略，哪些企业掌握大量有价值的数据，哪些企业就越容易遭到攻击。针对目标企业，攻击者手法更加多样化、对高价值目标的攻击进行“量身定做”，形成一整套攻击“组合拳”。对于大型企业来讲，网络节点和上下游关联企业与供应商都成为潜在的攻击漏洞，产业链中安全薄弱环节均成为攻击者实现突破的关键点。许多企业为了避免业务被中断，往往选择支付巨额赎金。

五、“多重勒索”模式引发数据泄露风险

时至今日，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”。这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，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。在这种情况下，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。



据不完全统计，自 2019 年 11 月首次公开报道勒索病毒窃取数据的事件以来，不到一年时间里，有超过 20 个流行勒索病毒团伙加入到数据窃取的行列中。以迷宫（Maze）勒索攻击为例，它不仅最先开始系统性地窃取数据，还以泄露数据相逼要挟用户缴纳赎金。越来越多的勒索攻击事件表明，“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。

> **“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**

六、供应链成为勒索攻击重要切入点

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。2020 年 12 月，知名 IT 公司 Solars 旗下的 Orion 网络监控软件更新服务器遭到网络攻击并被植入恶意代码，由于其客户群体覆盖大量重要机构和超过 90% 的世界 500 强企业，导致美国财政部、商务部等多个政府机构用户受到长期入侵和监视。

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、高效率等特点成功跻身最具影响力的高级威胁之列：

难发现

一是供应链攻击涉及诸多企业，即使是网络黑客也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。

易传播

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，尤其是和互联网巨头如谷歌、苹果及微软等企业相比较知名度不高。然而作为数字时代的重要建设者和参与者，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，对数字社会的破坏将不再局限在一家公司、一个国家，而是覆盖全球。

低成本

三是针对供应链的勒索攻击，目前来看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。

高效率

供应链攻击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。2017 年 6 月，一家不知名的乌克兰软件公司

遭受勒索攻击，勒索病毒通过软件公司服务器传播到数家全世界大企业，令其运营陷入瘫痪，造成全球范围内约 100 亿美元的损失。2021 年 7 月，美国软件开发商 Kaseya 遭勒索攻击，网络攻击团伙索要高达 7000 万美元的赎金。有评论称，此次事件可能成为 2021 年影响最大的供应链攻击事件。

七、引发网络保险行业的恶性循环

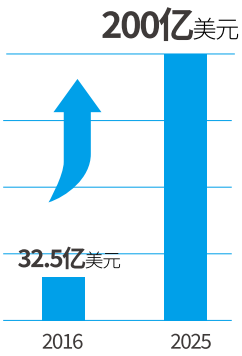
美国战略与国际研究中心与杀毒软件供应商迈克菲联合发布的一份报告指出，估计每年全球网络攻击所带来的损失将达 9450 亿美元，再加上约 1450 亿美元的网络防护支出费用，总经济成本将超过 1 万亿美元[23]。高额的网络攻击成本催生了对网络风险保险的庞大需求市场，根据预测，到 2025 年，网络风险保险费用将从 2016 年的 32.5 亿美元上升到 200 亿美元。伦敦再保险经纪商 Willis Re 透露，2021 年 7 月保单更新季，网络安全相关保险费率将迎来 40% 的大幅增长。近年来，还出现了勒索攻击谈判公司，这些公司专门负责与攻击者进行谈判，期望将赎金压低。这些公司通常是保险公司找来的。

9450亿美元
网络攻击损失

+

1450亿美元
网络防护支出

超过1万亿美元

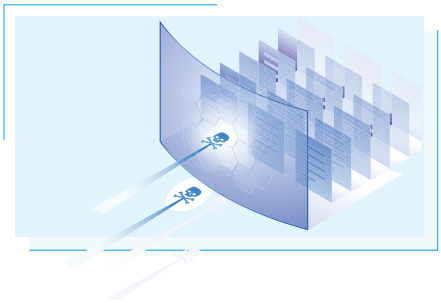


网络风险保险费用

然而，网络保险行业欣欣向荣的表象下，却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。同时，保险公司也成为勒索攻击的受害者。仅 2021 年就有多家公司中招。2021 年 3 月，美国第七大商业保险公司遭受勒索攻击，攻击者窃取了包含客户信息的文件；5 月，世界 500 强安盛保险公司在泰国、马来西亚、菲律宾等多个机构遭到勒索攻击，有 3TB 数据遭到窃取。攻击者层公开表示，保险公司是勒索攻击者眼中极具吸引力的目标。

23 引自 https://www.163.com/dy/article/F732DQ350511CJ6O.html

第五章 防范勒索攻击建议与思考



由于勒索攻击具有高强度加密算法的难破解性，勒索赎金数字货币交易方式的隐蔽性，无论是政府机构网络主体，还是非国家行为体的各类组织和企业，一旦遭遇网络勒索攻击，其损失和后果则都是不可预知的，因此，防范勒索攻击的重点应在事前防御环节而不是放在遭受攻击后的解密环节。从企业和个人层面看，防范勒索攻击需要提升网络安全能力、进行数据备份、提高人员意识等多个方面，从总体上不断提升安全防护能力，不给勒索攻击以可乘之机。

一、聚焦安全前沿技术，提高防护能力

从技术层面讲，网络安全的前沿技术，如云原生安全、零信任等，可以及时检测到风险、更早识别勒索攻击，同时，帮助企业在受到攻击后通过数据备份减少损失。

1．构建云上安全，提升安全防御能力

产业互联网时代，企业在应对勒索攻击时，数据备份和恢复的重要性进一步凸显。云原生安全所具备的开箱即用、自适应等显著优势，将成为保障云平台和云上业务安全的重要基础。

一方面，云原生安全将构建安全服务全生命周期防护，伴随云上业务发展全过程。

另一方面，云上安全产品将向模块化、敏捷化和弹性化演进，为用户提供差异化服务，成为兼顾成本、效率和安全的“最优解”。例如，客户主机出现高负载、高 CPU/ 磁盘占用等异常行为时，系统会发出自动告警，甚至直接阻断。这些措施都是基于云端实施、部署的，交付成本低。

安全之道在云端，企业上云，一方面，可以利用云服务提供商过往积累的安全能力与经验，更早识别勒索攻击。另一方面，云应用使数据加密和备份工作更加充分、及时，即使出现问题，也可采取多种数据恢复手段。

2．通过零信任，降低被攻击风险

零信任假定所有身份、设备和行为都是不安全的，即使曾经有过被“信任”的经历，也要一视同仁，在接入时需要进行全程安全验证和检查。攻击者使用窃取到的账号信息登录 VPN 或其他内部业务平台时，由于零信任采用多因子用户验证（即只有账号密码还不够，需要配合短信验证码、token、人脸识别等），即使攻陷了企业的一台服务器，也无法致使勒索攻击扩散到其他服务器。零信任体系还能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渗透时，零信任的安全机制可以及时检测到风险，从而帮助企业将风险控制在最小限度，不至于发生全网崩溃的严重后果。

需要指出的是，零信任是防守方武器库里一个比较新的武器，和其他武器一样，都不是万能的，必须与整个安全体系紧密结合才能充分发挥作用。

二、构建安全前置能力，提升“免疫力”

在勒索攻击防御方面，很多企业还存在误区：

一方面，是“银弹”误区，即很多企业期待用一种办法或一套系统彻底解决网络安全问题，但实际上，安全问题是动态演进的过程，不存在一劳永逸的手段，需要持续投入、运营、升级和关注。

另一方面，很多企业把网络安全仅仅定义为 IT 技术层面的问题，并没有意识到网络安全对企业来说是制约企业发展的天花板与生命线。

鉴于以上几个误区，从**企业层面来讲，**

> **解决勒索攻击的核心是构建“安全能力前置”，提升自身的“免疫力”**

1．安全能力前置成为企业必选项

企业数字化程度越高，潜在的安全风险也就越大，甚至会有致命风险。早期从业者大多在软件运行和业务运营过程中才考虑安全的问题，此时的安全防御思路明显是偏后的、被动的，难以应对多样化、动态化的网络攻击。如今，整个行业已经形成共识，安全贯穿于整个系统生命周期，需要进行全生命周期的守护。

因此，对于企业来说，一方面，要利用人工智能、大数据、云计算等新技术实现安全能力在业务环节的前置，提前预判潜在安全风险；加快数据资产梳理与管理，掌握不同信息系统和设备间数据流动情况，识别内部系统和外部第三方系统的连接关系，降低勒索攻击从第三方系统进入的风险；识别关键业务和系统之间的依赖关系，确定应急响应优先级。另一方面，要对安全专家或人才能力进行量化，使过往积累的安全经验与能力标准化、流程化，以实现安全能力的量化部署；定期开展风险评估，及时修复安全漏洞，定期更新杀毒软件，关停不必要的服务和端口。

2．打好保障供应链安全“组合拳”

供应链安全是保障网络安全的重点。随着数字化程度不断加深，依靠单一企业的安全防御能力，不足以应对大规模网络攻击，需要在产业链企业间形成威胁情况共享机制，协同防御。

一方面，须加强代码审计与安全检查。机构组织可向供应商索要清单，列明其使用的所有代码组件，以识别与开源组件漏洞有关的潜在风险。此外，还可以考虑在实施代码前，增加额外的自动化或手工检查，并利用第三方工具对软件及相关产品源代码进行详细的安全分析。

另一方面，加快推动建立零信任架构等安全防护机制。供应链攻击暴露出网络安全架构最大的缺陷就是过于信任。而零信任架构意味着每个试图访问网络资源的人都要进行验证，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，以防止第三方供应商获得不必要的特权，从而降低恶意软件的渗透风险。

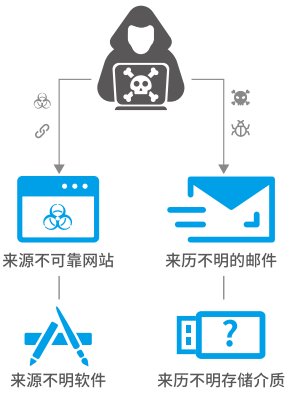
三、增强人员安全意识，降低攻击风险

应对勒索攻击，增强员工安全意识与加强数据备份同等重要：对从业人员的安全意识、安全素养的训练是长久、持续的过程。

1．增强安全意识

企业要加强安全知识的宣传力度，使从业人员对各种可能出现的可疑情况保持高度警惕。

一是不点击来历不明的邮件。勒索攻击者常利用受害者关注的热点新闻发送钓鱼网站，甚至会利用攻陷的受害者单位邮箱发送钓鱼网站。二是不打开来源不可靠网站。色情、赌博等不良网站是勒索攻击者发起钓鱼、挂马的主要地点。三是不安装来源不明软件。不安装来历不明或者陌生人发送的软件，警惕伪装成正常软件升级更新的勒索软件。四是不插拔来历不明存储介质。不随便使用来历不明的 U 盘、移动硬盘或者闪存卡等移动存储设备。同时，使用高强度且无规律登录密码，对于同一局域网内设备杜绝使用同一密码。加强网络隔离，限制不必要的访问通道。



2．加强数据备份

对于使用了非对称加密算法加密的文件，目前尚未找到有效的破解方法，一旦计算机遭到此类新型勒索病毒的攻击只能坐以待毙，因而，必须在平日里就做好重要数据的备份工作，且最好使用本地存储和云端双备份的策略。同时，应严格限制对备份系统的访问权限，防止勒索攻击横移对备份数据进行加密。

参考文献

[1] 张晓玉 , 陈河 . 从 SolarWinds 事件看软件供应链攻击的特点及影响 [J]. 网信军民融合 ,2021(04):37-40.

[2] 瑞星 2020 年中国网络安全报告 [J]. 信息安全研究 ,2021,7(02):102-109.

[3] 李江宁 , 覃汐赫 . 工业领域的勒索攻击态势与应对思路 [J]. 自动化博览 ,2021,38(01):86-90.

[4] 张宝移 . 计算机勒索病毒及防治策略分析 [J]. 技术与市场 ,2020,27(10):109-110.

[5] 高红静 . 近年勒索软件威胁分析及防范策略综述 [J]. 保密科学技术 ,2018(12):21-28.

[6] 李易尚 . 勒索软件 : 过去、现在和未来 [J]. 北京警察学院学报 ,2017(06):99-104.

[7] 李建平 . 供应链安全 : 防不胜防的软肋 [J]. 保密工作 ,2021,{4}(04):58-59.

[8] 嵇绍国 .2020 年勒索软件攻击情况及趋势预测 [J]. 保密科学技术 ,2020(12):33-43.

[9] 2021 上半年勒索病毒趋势报告及防护方案建议 , 南方都市报 ,2021-5-10

[10] 门嘉平 . 勒索病毒防治策略浅析 [J]. 网络安全技术与应用 ,2020(06):23-24.

[11] 吴崇斌 , 成星恺 . 勒索软件发展现状及应对 [J]. 通讯世界 ,2019,26(08):111-112.

[12] 盘点 2019 年勒索病毒灾难事件 [J]. 电脑知识与技术（经验技巧）,2019(12):88-90.

[13] 孟庆莉 . 面对愈演愈烈的网络勒索，美国怎么破 [J]. 廉政瞭望，2021(8):52-54.

[14] 郝俊慧 . 勒索病毒猖獗，运营商躲得过吗？ .IT 时报，2021-7-30.

[15] 孟佳惠 . 数字时代，应对“勒索软件”攻击任重道远 [J]. 中国信用，2021(6):121-123.

[16] 赵子鹏、张奇 . 解读重大勒索攻击事件下的网络安全态势及应对 [J]. 中国信息安全，2021(6):64-67.