勒索软件攻击威胁和零信任解决之道

一、网络勒索攻击频发

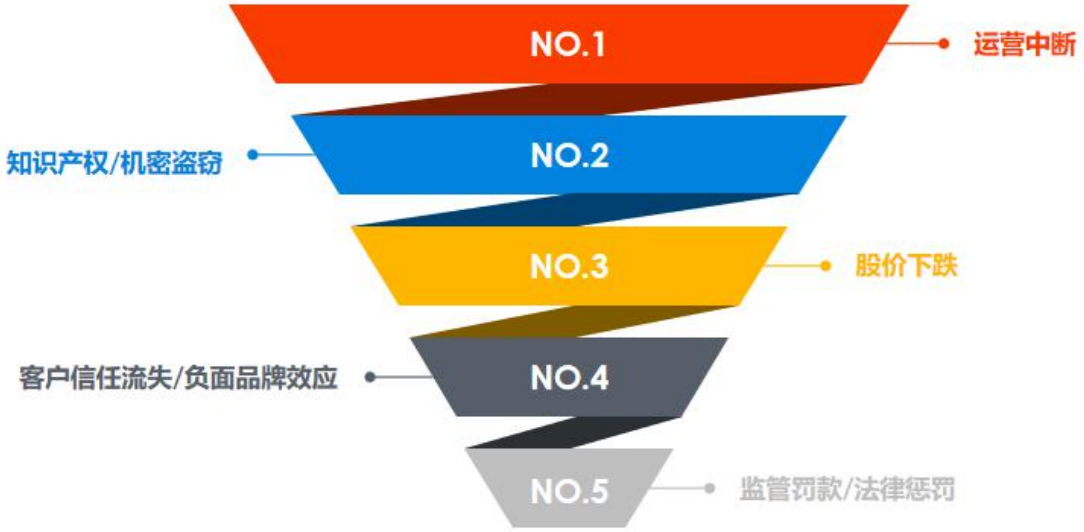
Covid-19 疫情仍在继续，而地缘政治对峙、区域战争爆发和全球经济低迷又添加了更多的不确定性，这一切造成了混乱不堪的局面，网络犯罪分子则有了可乘之机。近期，勒索软件攻击形势更加严峻，已经对全球制造、金融、能源、医疗、政府组织等关键领域造成严重影响。在某些事件中，攻击者挟持关键基础设施进而索要高额赎金，甚至可能影响国家的正常运作能力，如 2021 年 Darkside 对燃油管道运营商科洛尼尔的勒索攻击导致美国于 5 月 9 日宣布 18 个州进入国家紧急状态，最终以支付赎金了结，而 2022 年 5 月 8 日，受到 Conti 勒索攻击的哥斯达黎加政府多个机构陷入瘫痪，新当选总统宣布全国进入紧急状态。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。

排名 NO.1 的网络威胁

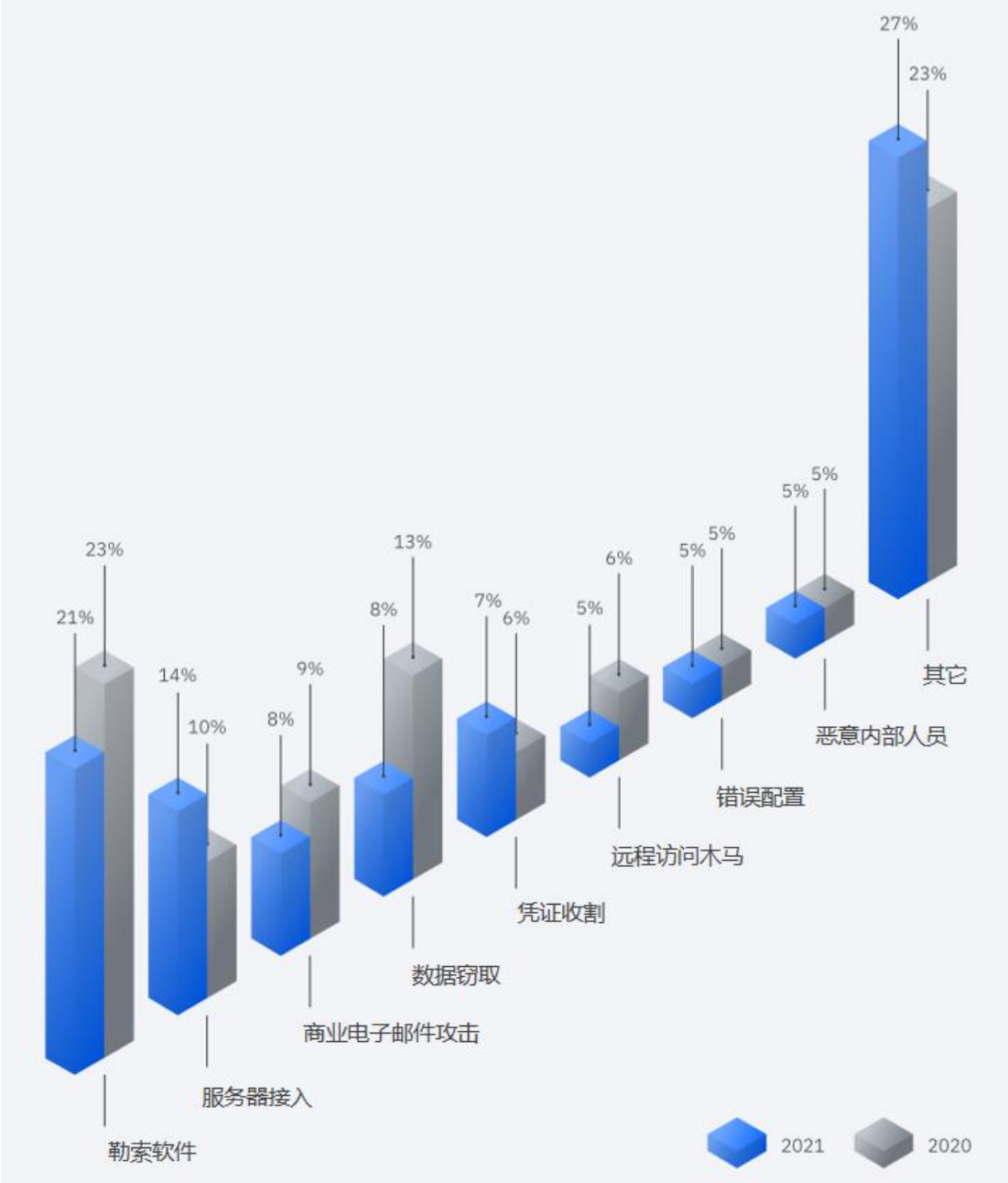
勒索软件是一种极具传播性、破坏性的恶意软件，黑客用来劫持用户资产或资源，旨在加密和盗窃数据以勒索钱财。勒索软件利用多种密码算法加密用户数据、更改系统配置等方式，使用户资产或资源无法正常使用，受害者必须向攻击者付费，才能获得解密密钥，重新获得数据，恢复系统正常运行。当然，即使受害者付款也有可能拿不到解密密钥。

勒索攻击在 2015 年后进入高发期，由于 2017 年 WannaCry 勒索攻击全球大爆发而广为人知，该次攻击事件至少有 150 个国家的 30 万名用户受害，共计造成超过 80 亿美元的损失，如今，随着暗网、虚拟加密货币的兴起，受害者通常需要支付无法追踪的加密货币，攻击者的行踪更加隐匿，使得这种网络犯罪更加猖獗。

勒索软件几乎总是以金钱为动机，对于个人而言，图片、视频或重要文件等个人事务、隐私如果被泄露可能会引起焦虑和纠纷，但对于企业而言，被勒索的内容包括专有信息、客户信息、账户和支付详细信息或其他有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。企业受到网络勒索攻击会遭受各个方面的损失，其中运营中断是最大的影响，平均停工时长为 21 天，其次是知识产权盗窃和股价下跌。



2021 年，在所有网络攻击中，勒索软件是数量占比最多的威胁类型，占比量虽然从 2020 年的 23%下降到 2021 年的 21%，但是超过 3 年来仍然稳居第一。



网络攻击占比分布，来源：IBM security X-Force

勒索软件攻击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%。

勒索攻击数量级，来源：2022 SONICWALL CYBER THREAT REPORT

REvil（又名 Sodinokibi）再次占据 2021 年最主要攻击类型的榜首，为 37% 的勒索软件攻击事件负责，而排在第二位的 Ryuk 占比只有 13%。REvil 勒索软件攻击实施者在 2020 年至少获利 1.23 亿美元，窃取了约 21.6TB 的数据。

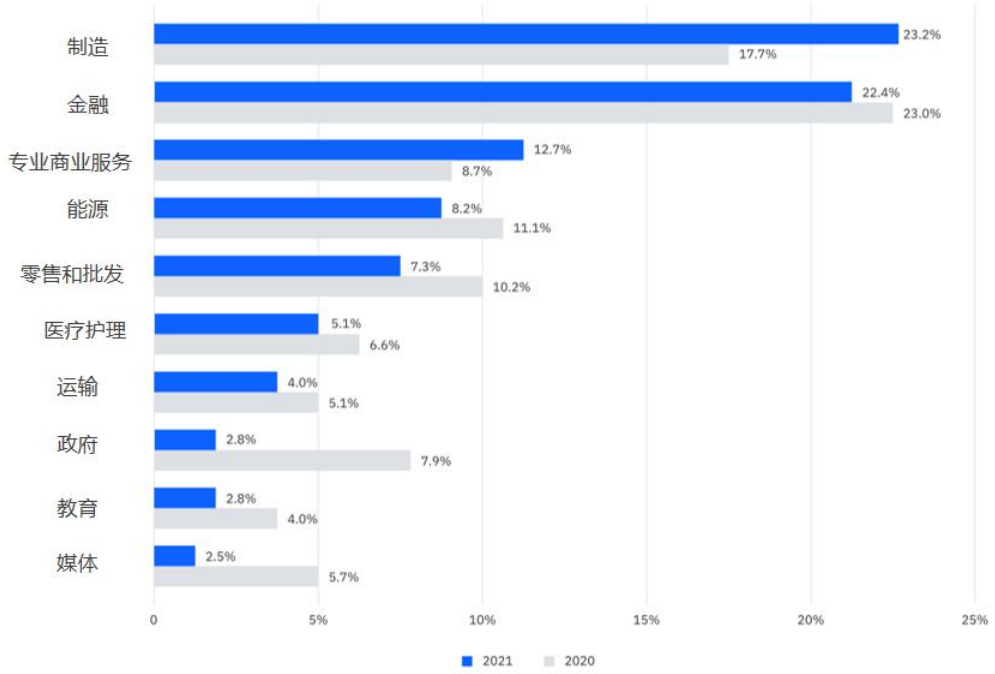
臭名昭著的 Conti 勒索组织过去两年来已涉入数百起勒索软件案件。FBI 估计截止到 2022 年 1 月，Conti 已经造成 1000 多家（大部分为企业）受害者，他们付出的赎金已超过 1.5 亿美元，这使得 Conti 成为有纪录以来造成最高开销的勒索软件。以致于今年 5 月 6 日美国政府宣布提供高达 1500 万美元的巨额悬赏奖金，奖励提供 Conti 勒索组织领导层和运营商关键信息的人。

勒索软件导致的数据泄露的规模、攻击的破坏效果都呈现扩大趋势，且在许多情况下直接攻击受害者关键设施组件致使业务中断，勒索软件攻击者对赎金的要求也越来越高。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动辄在几百万美元，REvil 勒索软件在 2019 年前后出现在中国时，索要金额仅 7000 元人民币，到了 2020 年，该团伙的勒索金额已动辄千万美元以上。

除不可预测的赎金费用外，平均估算，受到勒索软件攻击的企业还需要付出 462 万美元成本用于支付检测评估、多方通告、业务损失和响应成本，尽管近年许多企业采购了网络保险，但是仅能覆盖小部分损失。

制造业受到最多的攻击

制造业因为疫情原因饱受生产中断和供应延迟之苦，雪上加霜的是，该行业也是漏洞利用攻击的重灾区，是犯罪分子初始攻击方向的首选。2021 年，制造业取代金融服务业，成为受到网络攻击最多的行业，占攻击总数量的 23.2%。其中勒索软件是最主要的攻击类型，占到制造企业受到的攻击总数的 23%。



2021 年 VS 2020 年网络攻击排行，来源：IBM security X-Force

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。

触目惊心的勒索软件攻击事件

2021 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，以下回顾近期发生的典型的勒索软件攻击安全事件。通过这些事件，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。

•2022 年 4 月，哥斯达黎加多个政府机构遭到 Conti 组织的勒索网络攻击，政府程序、签名和邮票系统被破坏，财政部的数字服务无法使用，这影响了整个“生产部门”，总统罗德里戈·查韦斯（Rodrigo Chaves）宣布全国进入紧急状态。

•2022 年 3 月 8 日，三星证实源代码被窃取,科技巨头频陷勒索软件泥潭，黑客组织声称对芯片制造巨头英伟达进行了网络攻击，表示已窃取近 1TB 数据，并公开索要赎金。由于英伟达未满足其勒索要求，入侵者公布了包含英伟达 GPU 驱动、挖矿锁算力软件源代码等高度机密数据。

•2022 年 3 月 1 日，日本丰田汽车公司因零部件供应商受到“勒索软件”攻击，决定停止日本全国所有工厂运行，此次攻击导致丰田中断了约三分之一的全球生产。

•2022 年 2 月底，全球最大的轮胎制造商之一普利司通遭受 LockBit 勒索攻击，普利司通公司承认其一家子公司在 2 月份遭遇勒索软件攻击，导致其在北美和中美地区的计算机网络和

生产中断了约一周时间，攻击者威胁从普利司通公司系统中删除信息，并将这些信息予以公布，该组织提供给被勒索的公司一个在发布数据之前付款窗口，并添加了一个倒计时器，以此产生戏剧性效果。

•2022 年 02 月 20 日，全球十大物流公司之一的 Expeditors 遭勒索软件攻击，致全球业务受损。

•2021 年 11 月，丹麦风力涡轮机巨头维斯塔斯（Vestas WindSystems）于 19 日前后遭到网络攻击。此次事件中公司数据被挟持和加密，并且遭到勒索高额赎金，事件导致了尚未明确的数据泄露，部分受到攻击的设备正在恢复中，攻击事件发生后，维斯塔斯的股价跌至两周低点。

•2021 年 9 月，苏格兰跨国工程企业伟尔集团（Weir Group）遭受一起高复杂度的勒索软件攻击。伟尔集团在全球 50 多个国家/地区拥有包括采矿、基础设施、石油以及天然气等市场，本次攻击使集团的出货、制造和工程系统发生中断，仅 9 月份由于开销不足和收入延后造成的间接损失就高达 5000 万英镑，并且预计还会影响第四季度的正常运营。

•2021 年 7 月，攻击者利用托管服务软件供应链机制传播勒索软件，致瑞典连锁超市巨头 Coop 已关闭 800 多家商店服务。疑似 REvil 勒索软件攻击团伙利用安全漏洞，攻击入侵美国软件供应商卡西亚（Kaseya）软件补丁和漏洞管理系统 VSA 服务器设备，并利用软件更新机制传播 REvil 勒索软件。REvil 勒索软件攻击团伙声称在此次事件中锁定大量系统，并胁迫感染勒索软件的受害者支付价值约 7000 万美元的比特币赎金。

•2021 年 7 月，西班牙电信运营商 MasMovil Ibercom 遭 REvil 勒索软件攻击，数据遭到窃取。REvil 勒索攻击团伙在其专门的数据泄露网站中表示，已窃取该企业大量敏感信息，并公开备份文件、经销商名单等部分数据截图作为已成功实施网络攻击的证据。

•2021 年 6 月，北约“北极星”计划云平台供应商遭受勒索软件攻击，攻击者索要超 10 亿欧元（约合人民币 76 亿元）高额赎金。勒索软件攻击者入侵西班牙企业 Everis 及其位于南美洲的子公司，北约“北极星”计划云平台相关代码、文档等敏感信息可能遭到窃取。攻击者称有能力植入后门，攻击出于政治动机，威胁将数据发送到俄罗斯情报部门。

•2021 年 6 月，美国能源部核安全管理局（NNSA）的核武器分包商 Sol Oriens 遭受 REvil 勒索软件攻击。企业员工信息数据（包括姓名、社保号码、工资表以及员工培训计划等）遭窃取，内部信息被发布到 REvil 的暗网博客上，幸运的是，被泄露数据中似乎没有涉及高度军事机密，攻击者是否获取了美国和武器更敏感更秘密的信息有待调查。

•2021 年 5 月，美最大成品油管道运营商科洛尼尔遭 DarkSide 组织勒索软件攻击，导致美国东部沿海主要城市输送油气的管道系统被迫下线，成品油供应中断，美国于当地时间 5 月 9 日宣布进入国家紧急状态。科洛尼尔支付约 500 万美元（约合人民币 3200 万元）的加密货币勒索赎金，获得暗面组织提供的勒索软件解密工具，但由于该工具恢复数据速度缓慢，科洛尼尔已采用备份数据进行系统恢复。

•2021 年 5 月，巴西肉类制造巨头企业 JBS 遭受 REvil 病毒勒索攻击，导致其位于美国和加拿大地区的部分工厂暂停作业，其中，澳大利亚所有 JBS 肉类工厂停产。6 月 9 日，JBS 美国分部同意支付 1100 万美元比特币赎金，以防止黑客泄露公司数据。

•2021 年 5 月，安盛保险集团遭 Avaddon 勒索软件攻击，海量数据遭到窃取。Avaddon 在其数据泄露网站上称从安盛亚洲业务中窃取了 3TB 的敏感数据，包括客户的医疗报告、身份证

复印件、银行账户报表、索赔表格、付款记录、合同信息等。

•2021 年 5 月，位于挪威的欧洲能源及基础设施企业技术供应商 Volue 公司遭到勒索软件攻击。勒索软件攻击使得挪威 200 座城市的供水与水处理设施的应用程序关闭，导致挪威国内约 85%的居民生活受到影响。

•2021 年 3 月，CAN 保险公司遭勒索软件攻击，支付高额勒索赎金。美国最大的保险公司之一 CNA Financial 遭 Phoenix 勒索软件攻击，因无法自行恢复数据，CNA 支付 4000 万美元（约合人民币 2.57 亿元）高额赎金。CNA 在声明中拒绝就赎金发表评论，并提出在处理此事时已遵守美国相关法律、法规等。

•2021 年 3 月，宏碁遭 REvil 勒索软件攻击，攻击团伙索要高额赎金。REvil 勒索软件团伙在其数据泄露网站公布遭窃取文件的图片作为证据，包括财务电子表格、银行余额和银行通信等，索要赎金 5000 万美元（约合人民币 3.25 亿元），经谈判如提前支付赎金，勒索软件团伙可提供 20%的赎金折扣，提供解密工具、漏洞报告,并删除窃取到的文件。

•2021 年 2 月，起亚美国遭 DoppelPaymer 勒索软件攻击，导致长时间 IT 系统中断，影响应用程序、电话服务、支付系统的运行。攻击者要求起亚在两到三周内支付约 2000 万美元的比特币赎金（约合人民币 1.29 亿元），一旦延期支付，赎金将达到约 3000 万美元（约合人民币 1.93 亿元）。攻击者在其数据泄露网站威胁公布窃取的数据。

二、勒索攻击的技术手段分析

勒索方式和技术手段不断升级

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。无论大型还是小型企业，都在迅速变革工作环境，整个世界都转向线上活动，大量员工远程协作，其迁移速度和规模十分惊人。从云到 Shadow IT（影子 IT 设施）到 ICS（工业控制系统），均快速就位并准备好迅速扩张，但不太明显的是这种转变背后潜在网络风险，因为随之而来的就是网络暴露面大大增加，但企业往往很少甚至没有时间考虑安全问题。毫无意外，攻击事件频繁发生，各行业和各地区均是如此。

威胁实施者利用不断变化的局面，抓住机会采用各种手段和方法，成功渗透进世界各地的组织和企业中，勒索软件已经逐渐从“广撒网”误打误撞的手法转向定向攻击，表现出更强的针对性。攻击者瞄准能源、医疗等承载重要数据资源的行业信息系统作为勒索软件攻击“高价值”目标，摒弃传统利用钓鱼邮件、网页挂马等“广散网”无特定目标的勒索软件传播模式，攻击目标主要是大型高价值机构。同时，攻击技术呈现快速升级趋势，利用系统漏洞入侵以及随后的内网横向移动过程达到自动化、集成化、模块化、组织化的特点愈发明显。勒索方式也持续升级，勒索团伙往往在加密敏感数据同时将被数据文件窃取回传，并在互联网上或暗网的数据泄露站点上公布部分或全部文件，以胁迫受害者缴纳赎金。

(1) 定向 APT 攻击

传统勒索软件攻击者使用广撒网无差别攻击，这种方式很难预测受害者是谁，哪些受害

者有价值。同时，普通用户的数据价值相对不高，且缴纳赎金的意愿并不强烈。如今，勒索攻击定向精准攻击的趋势愈发明显，主要针对掌握大量数据的企业组织发起定向攻击，植入勒索软件并勒索超高额赎金。其攻击手段日趋 APT 化，形成涵盖探测侦察、攻击入侵、病毒植入等的精准化攻击链，如嗅探网络发现攻击入口、利用漏洞攻击入侵、精心设计的社会工程入侵等，攻击不计成本、不择手段，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，使受害者企业彻底瘫痪以有效勒索赎金。

(2) 强加密无法破解

勒索攻击使用的加密手段越来越复杂多样化，通常采用多种加密算法加密用户数据，一旦感染，极难进行数据恢复，业内专家普遍认为遭受勒索攻击之后，没有“特效药”。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难以进行解密，因为暴力解密往往需要上百年的时间，其时间成本已经使得破解失去意义。许多企业为了避免业务中断，往往选择支付巨额赎金。

(3) 双重/多重勒索

双重/多重勒索成为犯罪分子胁迫受害用户屈服的有效手段，一半以上的勒索软件采用双重勒索手段。勒索攻击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，攻击者通过甄别和窃取用户重要数据，以公开重要数据胁迫用户支付勒索赎金，这种新模式也被称为“双重勒索”。这样一来，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，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，使得受害企业同时承受数据公开、声誉受损、法律处罚等多重压力。

此外，在攻击者加密之前通过在受害者目标环境中安装具有 DDOS 攻击能力的后门程序，以“拒绝支付赎金则外泄数据或发动 DDOS 攻击”为威胁筹码，形成多重勒索，逼迫受害方支付赎金。

(4) 供应链攻击勒索

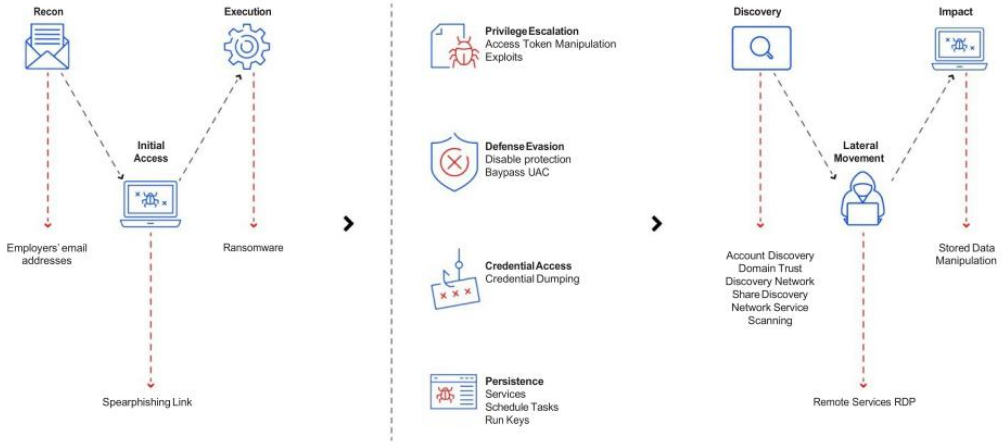
不同于攻击单一目标，供应链攻击指数级扩大入侵范围，通过入侵上游供应商，如通过软件补丁方式分布到众多使用该软件的企业 IT 设施内部，对于企业而言，其网络节点和上下游关联企业、供应商都成为潜在的攻击漏洞，产业链中安全薄弱环节均成为攻击者实现突破的关键点。

(5) 勒索攻击产业化平台化

不断扩大的市场规模触发了新的盈利模式，部分勒索软件攻击组织开发了 RaaS（勒索软件即服务）平台，面向“会员”提供开箱即用的勒索软件攻击服务。开发者可以提供一整套解决方案，如购买勒索软件程序、靶标系统访问权限，或订购针对特定目标的勒索软件攻击服务，甚至包括利用加密货币进行赎金支付等。同时，在病毒开发、攻击入侵等环节招募合作伙伴，分工协作增加勒索软件攻击成功率。依赖这种平台化模式，攻击者甚至不需要任何编程技术就可以开展违法犯罪活动，网络攻击的门槛大幅降低，理论上任何人只要支付少量费用就可以通过这类服务平台开展勒索攻击。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。

网络勒索攻击的实施过程

典型网络勒索攻击典型流程包括探测侦察、攻击入侵、病毒植入、实施勒索 4 个阶段。



1.探测侦察阶段

（1）收集基础信息。攻击者通过主动扫描、网络钓鱼以及在暗网黑市购买等方式，收集攻击目标的网络信息、主机信息、身份信息、组织信息等，为实施针对性、定向化的勒索攻击打下基础。

（2）发现攻击入口。攻击者通过漏洞扫描、网络嗅探等方式，发现攻击目标的网络和系统存在的安全漏洞，找到网络攻击的突破口。此外，攻击者同样可利用网站挂马、钓鱼邮件等方式传播勒索软件，建立内部立足点。

2.攻击入侵阶段

（1）部署攻击资源。根据发现的远程桌面 RDP 弱口令、信息系统漏洞等网络攻击突破口，部署相应的网络攻击资源，利用 MetaSploit、Cobalt Strike、RDP Over Tor 等网络攻击工具，在目标中部署攻击者可操纵的远程访问工具。

（2）侦查网络资产。攻击者持续扫描、侦查内部网络和资产，获取用户、群组、任务列表，同时获取域列表和域控制器信息、侦测企业 AD 域数据，获得主机名称、网络拓朴和数据资源清单，理解内部网络和资产分布，获取凭证和域管理员权限并准备后续横向扩展入侵。

（3）提升访问权限。采用合适的网络攻击工具，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。

3.病毒植入阶段

（1）植入勒索软件。攻击者通过恶意脚本、动态链接库 DLL 等部署勒索软件，并劫持系统执行流程、修改注册表、混淆文件信息等方式规避安全软件检测，确保勒索软件成功植入并发挥作用。

（2）破坏防御机制。攻击者往往在恶意程序中执行一系列动作以破坏安全检测机制和删除备份，攻击关闭安全程序、备份服务，甚至卸载已知的各种防毒软件和安全类程序，很多攻击会将卷备份删除、清零所有空闲磁盘空间、清除系统事件日志、关闭系统备份功能。

（3）扩大感染范围。攻击者在已经入侵内部网络的情况下，利用勒索软件本身类蠕虫的功能，通过文件共享协议 SMB 等方式在攻击目标内部横向移动扩大攻击范围，将恶意代码植入更多设备，并可以通过实施内部鱼叉式网络钓鱼进一步扩大勒索软件感染范围。

4.实施勒索阶段

（1）窃取机密数据。攻击者通过运行勒索软件，根据攻击目标类型，识别敏感、重要的文件，如关键业务数据、商业机密、知识产权等，使用 WinSCP、Rclone 等工具进行数据回传，后续对受害目标进行数据公开的威胁。

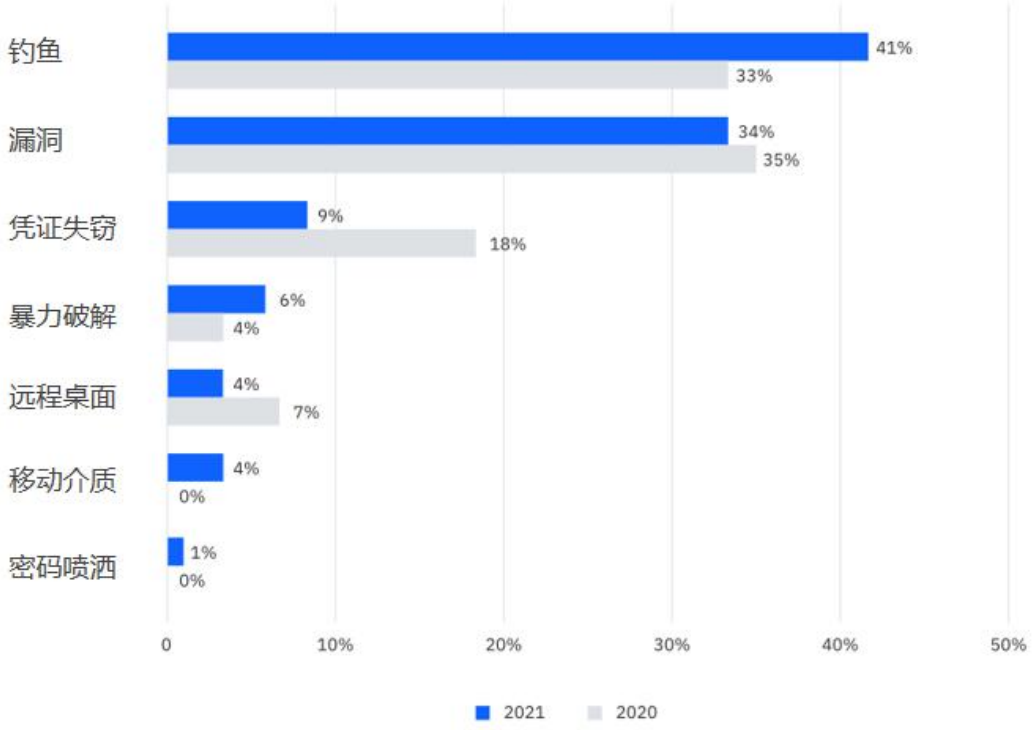
（2）加密关键数据。攻击者使用域管理凭证，通过 PsExec/SMB/组策略部署执行勒索软件，加密图像、视频、音频、文本等文件以及关键系统文件、磁盘引导记录等，导致受害者系统无法正常运行、业务无法开展。

（3）加载勒索信息。攻击者加载勒索信息，威胁攻击目标支付勒索赎金。通常勒索信息包括通过暗网论坛与攻击者的联系方式、以加密货币支付赎金的支付方式、支付赎金后获取解密工具的方式、警告受害者不要自行解密或修改数据名称等。

勒索攻击的初始入口途径

勒索软件有许多可行的途径入侵企业内部，网络犯罪分子在利用技术、社会工程和漏洞方面非常有“创意”。尽管企业对员工进行多年的安全意识培训，但危险的用户行为仍以极高的比率持续存在，导致对可疑链接的点击和考虑不周的应用程序/文件下载。

勒索软件主要的传播方式包括钓鱼邮件传播、水坑网站挂马传播、垃圾邮件、漏洞入侵、远程登录入侵传播、供应链传播和移动介质传播等，诱导受害者下载运行勒索软件。其中利用网络钓鱼获得初始访问权限的攻击的占比达 41%，成为 2021 年勒索软件攻击最主要的入侵途径。



2021 年 VS 2020 年勒索攻击媒介排行，来源：IBM security X-Force

1. 利用钓鱼邮件传播。攻击者发送带有恶意链接和恶意文件附件的针对性的网络钓鱼邮件，一旦用户打开邮件附件，或点击恶意链接，勒索软件将自动加载、安装和运行，实现实施勒索软件攻击的目的。

2. 利用安全漏洞传播。漏洞利用仍是攻击关键手段，引发勒索软件传播一点突破、全面扩散。攻击者主要利用已公布漏洞，通过漏洞扫描、端口扫描等方式主动发现未及时修补漏洞的设备，利用弱口令、远程代码执行等网络产品安全漏洞，攻击入侵用户内部网络，实施远程攻击入侵，获取管理员权限并在攻击目标内部网络横向移动，扩大勒索软件感染范围，实施勒索行动。同时，一些零日漏洞一直在被威胁实施者利用。

3. 利用远程桌面入侵传播。攻击者通常利用弱口令、暴力破解等方式获取攻击目标服务器远程登录用户名和密码，进而通过远程桌面协议登录服务器并植入勒索软件。同时，攻击者一旦成功登录服务器，获得服务器控制权限，可以服务器为攻击跳板，在用户内部网络进一步传播勒索软件。

4. 利用网站挂马传播。攻击者通过网络攻击网站，以在网站植入恶意代码的方式挂马，或通过主动搭建包含恶意代码的网站，诱导用户访问网站并触发恶意代码，劫持用户当前访问页面至勒索软件下载链接并执行，进而向用户设备植入勒索软件，攻击并且可以从浏览器发起内存空间无文件攻击，无需落地文件到磁盘驱动器，规避安全检测。

5. 伪造正规软件传播。仿冒或者篡改正常软件应用程序，通过虚假软件和虚假产品更新，诱导用户下载执行，隐藏在程序/可执行文件中的恶意程序加载勒索攻击病毒。

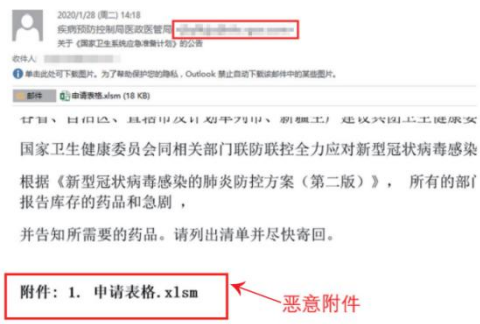
6. 利用移动介质传播。攻击者通过隐藏 U 盘、移动硬盘等移动存储介质原有文件，创建与移动存储介质盘符、图标等相同的快捷方式，一旦用户点击，自动运行勒索软件，或运行专门用于收集和回传设备信息的木马程序，便于未来实施针对性的勒索软件攻击行为。

7. 网络文件共享传播。攻击者将勒索攻击病毒植入 PDF、DOC 等文件中，利用网络共享平台、各类网盘等分发，用户下载后打开文档即触发勒索软件攻击，此类外表正常的文档隐含攻击代码，极具欺骗性。

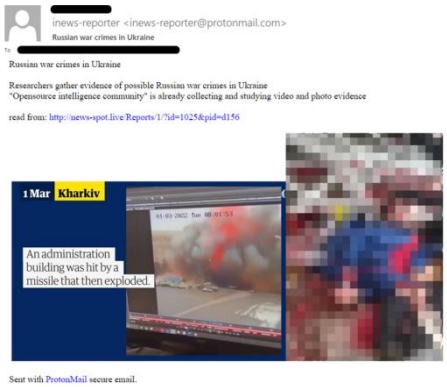
8. 利用软件供应链传播。攻击者利用软件供应商与软件用户间的信任关系，通过攻击入侵软件供应商相关服务器设备，利用软件供应链分发、更新等机制，在合法软件正常传播、升级等过程中，对合法软件进行劫持或篡改，规避用户网络安全防护机制，传播勒索软件。

钓鱼（包括钓鱼邮件、钓鱼网站、诱饵文档或程序伪装等）作为低成本的攻击方式一直被攻击者大量使用。邮件标题和内容往往采用吸引眼球的时事热点“疫情防控”“战争内幕”、利益诱饵的“限时福利”、“节假日礼包”、公事外观“项目申报”“升级补丁”等来诱使受害者点击链接访问恶意网站地址、打开附件恶意文档从而触发后续入侵和勒索软件植入。

例如，黑客将恶意文件、钓鱼链接、诱饵文档等攻击载体伪装成为新冠肺炎疫情相关官方通知、新闻资讯、政府文件、防疫建议等吸引目标下载并执行恶意代码。在邮件附以高度敏感的时事热点话题容易使受害者疏于防备，在毫无察觉的情况下遭到攻击。



攻击者模仿中国国家卫生健康委员会的钓鱼邮件



攻击者利用俄乌战争主题的钓鱼邮件

2020 年至 2021 年间由漏洞利用攻击导致的安全事件数量有所增加，在 2021 年，被犯罪分子利用的五个最主要漏洞中，有四个是新漏洞，包括 Log4j CVE-2021-44228，尽管它在 2021 年 12 月才被披露，但快速上升到排名第二位的被利用最多的漏洞，影响极其广泛，在 Log4j 漏洞公开后 48 小时，攻击量即达到 10 万，3 天内超过 100 万次攻击，截止 2022 年 1 月 31 日，SonicWall 组织记录到 1.422 亿针对 Log4j 的尝试攻击，这种波及面非常广泛的漏洞如果被成功应用到勒索攻击中，会带来新的波及全球的大型勒索攻击冲击波。

三、勒索攻击的防御响应机制

根据 NIST 计算机安全事件处理指南，勒索软件事件处理生命周期涵盖早期预防、探测事件和分析、遏制攻击和消除及恢复、事后复盘整改四个阶段。

全面的勒索软件防护需要同时在多个方面保持主动和警惕，安全必须涵盖在企业运作的每个方面。

事前预备：

(1) 员工培训教育，企业分部门、角色进行定期网络安全培训，提升网络管理员和普通用户的安全意识。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。

(2) 修复薄弱策略，针对文档宏的风险进行组策略配置，封禁互联网获取文件中宏的运行，去除邮件中可执行文件，限制 temp 目录中程序的执行，全局禁用 adobe Flash，限制 Windows Scripting Host 脚本执行，AD 管理入口不应直接暴露在互联网提供访问。

(3) 登录密码加固，用户应当及时修改默认密码，修改企业中重要资产、系统、组件和接口的默认密码，同时增加密码强度。

(4) 采用 MFA 机制，密码可能失窃或被暴力破解，企业应在尽可能多的登录入口采用多因子认证，保证攻击者即使获取密码也无法轻易突破系统。

(5) 激进补丁政策，攻击者大量利用已经公布的漏洞和 ODAY 漏洞，主动和定期修复操作系统、第三方程序的漏洞，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。

(6) 减少网络暴露面，避免关键信息系统在互联网上暴露，尽可能减少资产在互联网上暴露，特别是避免重要业务系统、数据库等核心信息系统在互联网上暴露。

(7) DNS 和流量过滤，增加 DNS 可见性，识别网络访问中恶意目标域名、IP 并进行封禁和告警，判断 DGA 形态可疑的 DNS 请求并进行处置，阻断连接攻击者的 C&C 服务器。

(8) 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，限制用户仅访问所需要的网络、系统和数据，限制其数据读写权限，限制用户本地设备 admin 权限。

(9) 程序和设备控制，监控终端环境情况，只允许运行所需的应用程序，只允许必要的 USB 连接系统，关闭自动播放功能，关闭或者修改 135～139、445 等高危端口。

(10) 执行安全域控制，对内网的安全域进行合理的划分，域之间通过访问控制列表（Access Control Lists，ACL）限制，对于域管理员账户和设备加固防护。

(11) 严格备份计划，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。

(12) 部署 EDR 工具，EDR 有助于尽早发现攻击并进行隔离，帮忙 IT 人员观察感染设备情况

和进一步的分析。

(13)制订响应计划，考虑周全的事件响应计划使企业在面对灾难级局面时，处于极度紧张的局面时，在各个层面、组织上进行协同和处置，减少最终损失。

检测响应和分析：

(1) 网络勒索攻击企业网络共享设施，用户工作中发现网络共享文件被加密不可用，应定位受感染用户设备并阻断其访问，抑制进一步对网络共享设施中数据的加密。

(2) 网络勒索攻击用户本地设备，用户工作中发现本地文件被加密不可用，应立即将设备关机以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。

(3) 企业 SIEM 系统发出文件大规模操作告警，对于部署 SIEM 监测的企业，有可能发出超出日常文件操作量的告警，从而引起 IT 人员注意，定位到已经发生勒索攻击。

(4) 网络勒索攻击者发出提示信息，勒索者在已经执行完对本地和网络文件的加密后，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，应当立即拍照以提供给安全专业人士进行分析，这有助于确定勒索攻击软件类型以寻找应对经验。

(5) 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。

(6) 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。

抑制、清除和恢复：

(1) 一旦发现攻击发生，应当立即隔离受感染设备，断开其网络连接或者关机，以防止攻击在内部的进一步扩散。

(2) 下线共享文件和数据，在无法明确定位到感染根因时，快速将已经部分加密的共享设备下线以阻止进一步数据破坏，包括各类开启 CIFS/SMB 协议的装置都应当进行检查。

(3) 清除网络设备中感染的勒索软件，包括各类本地设备和其它关键设备及服务，同时应当清除所有钓鱼邮件、屏蔽恶意网站，有策略地修改受影响的用户密码以阻断攻击者利用。

(4) 对于定位到是由系统漏洞攻入，则应当进行打补丁操作，阻止后续可能的再利用攻击，对于无法打补丁的情况则需要进行隔离，消除暴露面风险。

(5) 恢复遭到时破坏的数据，如果系统备份机制运行正常且备份数据未被加密、删除，则可以从备份库中恢复数据，应当检查确认备份库未被植入恶意攻击文档、代码。

(6) 由专业人士分析，寻求是否可能破解加密，或者从感染设备中打到解密密钥，当然，根据既往攻击事例，这些措施成功可能性较低。

(7) 按照合规和法律要求向相关机构报告勒索事件。

(8) 决策是否支付赎金，寻求专家建议，评估系统和数据的破坏程度、法律合规的要求、支付后是否保障恢复、获取到解密密钥进行恢复的时长成本等。

复盘和加固：

(1) 会议检讨事件处理过程，评估应急预案各项措施的执行情况，进而对事件响应预案进行修订优化。

(2) 系统检视和加固，由安全专家组织检视内部网络、安全架构的合理性，修补其中的漏洞，规划演进组织的安全机制、提高安全成熟度。

四、网宿零信任解决方案

零信任抑制网络勒索攻击

零信任概念自 2010 年由 Forrester 提出，直到 2017 年，谷歌对其内部网络进行基于零信任安全的改造成功后，验证了零信任安全在大型复杂网络环境中的落地可行性，业内开始关注零信任理念和实践，出现越来越多的零信任产品、平台及标准规范，2020 年 Covid-19 疫情爆发带来远程办公需求激增，将零信任热度推向一个新高度。

面对当前愈演愈烈的网络勒索攻击，部署零信任（Zero Trust）已然成为企业和组织 IT 安全架构转型中重要一环，在实施过程中，它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。

(1) 零信任是行为模式的转变，是解决安全问题的新方法，它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。

(2) 零信任核心理念是了解关键数据位于何处，以及谁有权访问这些数据，它在整个网络中建立强有力的验证措施，以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。

(3) 零信任构建企业组织软件定义的安全边界，当今新的网络架构演变形势下，传统边界防御机制已经失效，零信任模型提供了一种解决方案，它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。

(4) 零信任使用基于持续风险评估的实时访问决策替换简单的、静态的实体验证。

(5) 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，特别是勒索软件和 BEC，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。

(6) 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，但是实践证明 VPN 因为漏洞和暴露面容易受到攻击，而零信任网络访问（ZTNA）提供了安全性和可视化。

(7) 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，阻止发生进一步全局渗透攻击的严重后果。

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。传统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

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。据测算，部署零信任可为企业平均节省 28.7%-42.3%的安全事故成本。

网宿零信任有效应对勒索攻击

网宿安达 SecureLink 产品按照零信任(Zero-Trust)安全访问模型，将传统的基于边界“城堡与护城河式” 的安全管理方式，转变为按需在单个资源与客户之间构建信任的安全管理方式。在零信任模式下，用户将基于经不断重新验证的内外部因素建立可信连接，遵行零信任关键理念原则：

(1) 不自动信任网络的安全性(内网≠可信)；

(2) 对任何接入系统的人和设备都进行验证；

(3) 每次访问都要进行身份验证和行为审计；

(4) 细粒度访问控制策略 Need-To-Know(最小权限原则)；

勒索软件快速进化演变，新的变种和攻击策略层出不穷，勒索软件适应性强，经过精心设计，可避免被安全软件检测到。即使是很小的延迟检测，也可以为潜在的不可逆文件加密提供足够的时间。当企业组织检测到恶意的勒索软件时，往往攻击行动已经加密了部分目标数据，虽然仍有机会能够遏制住攻击进一步的扩散，但是此时想阻止全部的攻击的往往已经太迟了，所以对于企业组织而言，事前预防尤为重要，零信任通过提供在网络层面的暴露面收敛隐藏、身份 MFA 校验、密码加固、恶意访问威胁检测和设备环境安全感知、行为异常识别等能力，能够在勒索攻击的探测、远程连接阶段就进行安全防护和及时干预。

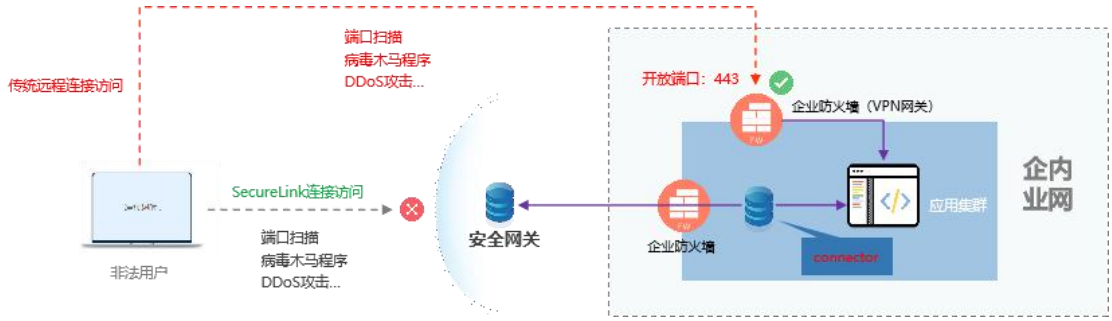
隐身网络遮蔽内部脆弱性

利用网络隐身技术构建一张隐形的网络，只对认证授权的可信任用户可见，对其他人完全不可见，并且该用户访问应用的行为可以进行严格控制和记录。这种模式很好地解决资产和应用暴露在公网的问题，同时也可以增强现有内网办公的安全性。由于网络资产被隐藏，攻击者无法嗅探、扫描到企业内部的服务，无法利用内部服务的漏洞，有效保护企业内部网

络、业务的脆弱性，遏制漏洞利用。

网宿安达 SecureLink 产品通过企业内网连接器由内向外建立安全隧道，企业应用无需映射端口于互联网，在用户侧看到的源站 IP 地址均为网宿的服务 IP，可以有效地把客户应用源站的真实 IP 隐藏起来。相比未部署网宿安达 SecureLink 产品前，源站 IP 可以通过访问直接获得的情况，可以有效地降低安全隐患。而且若黑客对平台发起攻击，网宿安达 SecureLink 平台也可快速启用安全策略，保障应用服务源站的安全。

同时，网宿安全网关支持采用单包认证授权的方案，只针对授权通过的用户开放访问连接通道，从而防止恶意扫描和非法数据进入，不再惧怕 IP、多端口对外开放。



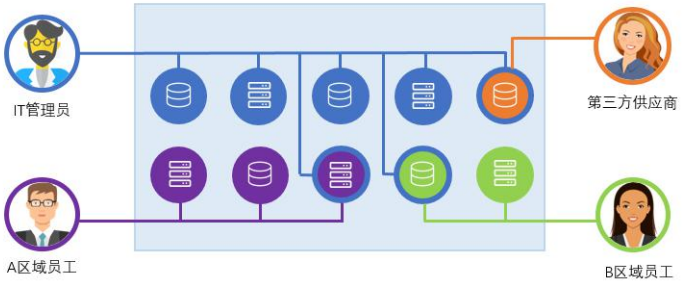
第一层隐身防护：网宿安达 SecureLink 通过企业内网连接器由内向外建立安全隧道，企业应用无需对外映射端口于互联网，实现第一层隐身防护。

第二层隐身防护：互联网用户获取到的应用域名及 IP 均为代理后（替换后），无法获取应用源站的真实位置，攻击无处发起，实现第二层隐身防护。

第三层隐身防护：网宿安全网关只针对授权通过的用户开放访问连接通道（SPA），实现第三层隐身防护。

MFA 机制保障身份安全

通过基于用户身份的认证、鉴权机制，确保合法用户才能接入内网。针对用户登录或敏感数据访问、敏感操作等场景，支持多因子认证（MFA）方式增强用户身份鉴定能力，提供短信、TOTP 等主流二次认证方式。实施 MFA 实际上改变了威胁态势，迫使威胁实施者寻找新的网络入侵方式，仅仅利用被盗的登录密码凭证无法攻破防线。MFA 降低了多种不同的攻击类型的风险，包括勒索软件、数据盗窃、BEC 和服务器访问等。

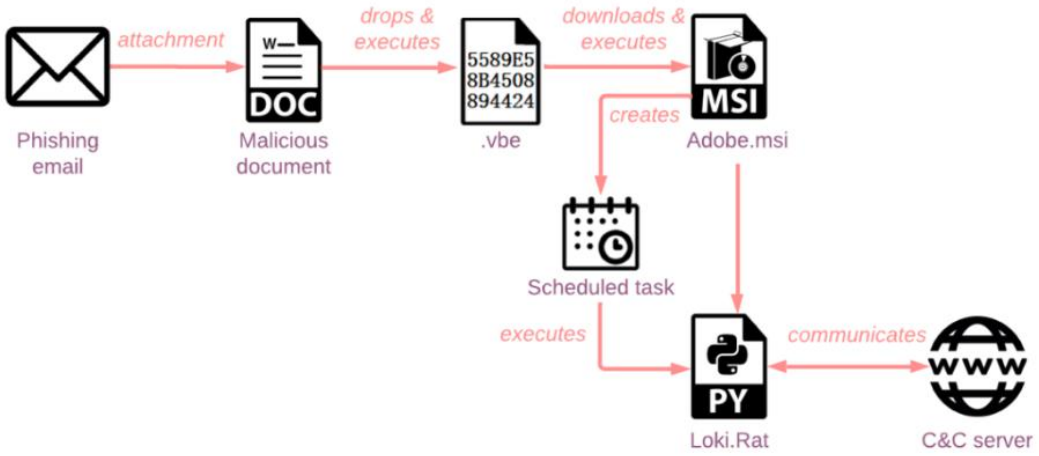


系统对用户进行身份标识和鉴别，保证身份标识具有唯一性、采用动态口令等两种或两种以上身份鉴别、具备防范口令暴力破解的能力、口令等身份鉴别信息符合复杂度要求并定期更换、推行口令定期强制修改等，识别发现并及时消除口令安全风险。

通过对用户身份进行管理，保障身份安全。管理员根据用户的身份和具体的需求，多维度制定用户访问策略，有效地控制不同部门不同角色用户的访问权限，降低网络攻击和员工泄密数据的可能。同时，在用户接入认证后，对终端及用户行为进行持续验证和动态授权，以保障访问的安全。

DNS 过滤阻断 C&C 连接

基于网络流量中 DNS 信令解析，对组织内部访问“风险网站”进行响应和阻断，降低由于下载和安装恶意软件，导致感染勒索软件的可能。勒索软件攻击中本地软件进程连接 C&C 服务器时，需要使用 DNS 解析其域名，此时平台实时进行识别和拦截，阻断勒索软件的攻击行动，从而降低遭遇网站挂马、网站钓鱼等安全风险的可能。



(1) 用户点击钓鱼邮件中恶意地址、挂马网站时，系统根据系统自带海量威胁情报，匹配判断其域名、IP 是否属于恶意地址，从而及时进行封堵，并可引导至 sinkhole 进行实时访问用户进行提示。

(2) 勒索软件连接远程 C&C 服务时，系统在收到 DNS 解析时，根据系统自带海量威胁情报，匹配判断其域名、IP 是否属于恶意地址，从而及时进行封堵。

(3) 勒索软件连接远程 C&C 服务时，有时会使用 DGA 方式产生大量域名来规避基于威胁情报的封禁，这种场景下，系统内置 DGA 域名智能识别模块，能够有效判断本地连接域名的可疑程度，从而进行告警或者阻断。

目前，网宿平台具备的威胁情报库日常量级达 3000 多万条目，可帮助企业屏蔽各类恶意域名和 IP ，识别、检测、阻断、告警及审计网络流量，防止勒索软件的攻击。

钓鱼攻击中，Microsoft、Apple 和 Google 是犯罪分子尝试假扮的前三大品牌。这些大品牌在网络钓鱼工具包中被反复使用，攻击者利用其热门程度，诱导消费者相信自己。某些情况下，攻击者利用同形异义词攻击，普通用户难于进行防范，平台则在 DNS 请求时识别流量中真实访问目标以进行相应处理。

此外，系统支持对利用 DNS 隧道构建 C&C 信道的恶意攻击进行检测和处置，DNS 隧道构建的隐蔽 C&C 信道较为隐蔽，因为 DNS 协议是当前网络中重要部分之一，大部分企业网络总会允许内网与指定 DNS 服务器(受信任)的查询、请求数据流量。检测机制主要包括：

(1) 对同一域名及其子域名的请求频次过于频繁

(2) DNS 数据包很大，占用带宽较高，可能在进行大数据量传输

(3) 截获数据包分析，有明显编码特征，而且时非正常 DNS 数据包

(4) 根据 DNS 查询类型、编码后传输、限制交互频率等进行限制

流量安全透视和处置威胁

NTA 流量分析，通过流量解析识别勒索软件攻击并处置告警，平台根据告警封禁攻击 IP 地址，通过还原流量中传播的勒索软件样本，联动威胁情报识别和阻断投递过程中勒索软件，从而检测和拦截各类通过邮件、网站传播的勒索软件。

(1) 平台 NTA 网络流量安全分析，对勒索软件、木马、蠕虫等入侵攻击以及敏感文件、敏感信息进行识别和处置。

(2) 支持基于 WAF 规则检测 SQL 注入、XSS、文件上传、命令执行、敏感文件下载、敏感目录访问、XXE、文件包含、跨目录、后门文件、扫描器、敏感信息泄露等 WEB 类流量。

(3) 支持内网渗透、端口攻击、病索病毒、间谍软件、网络钓鱼、挖矿、恶意脚本等非 WEB 类流量。

(4) 支持防暴力破解、端口扫描，防止攻击者进入敏感业务系统。

(5) 安全网关具备平台级的安全防护能力（DDoS、WAF 等），为企业应用消除来自互联网中的攻击风险。

(6) 流量全程加密保障通信安全，支持开启 SSL/TLS 加密能力，支持 IPsec 加密、国密算法加密，保障数据安全。

沙箱隔离工作安全空间

提供端侧沙箱，是与宿主机隔离的安全工作空间，保障接入和数据使用安全性，特别在远程办公形式下，数据脱离了企业内网和企业配发设备，数据泄漏隐患极大，安全沙箱则提供了在用户侧安全合规访问企业资源与数据的方法，有效保护企业核心资产安全，由于空间与宿主机的系统、网络、存储上进行隔离，数据加密存储，有效阻止宿主机中恶意勒索程序识别到其中的文件进行加密，也无法进入安全空间连接到企业敏感应用系统进行攻击传播。

(1) 采取最小权限控制，高敏感数据的访问提供安全沙箱隔离操作。

(2) 数据隔离，安全工作空间数据在本地空间中不可见。

(3) 白名单网络访问控制，阻止人员误点击攻击邮件、访问恶意地址引发入攻击入侵。

(4) 个人空间与工作空间隔离，安全与隐私兼顾。

(5) 设立应用软件、进程的白名单，排除恶意程序运行。

最小权限应用层限制可达

网宿安达 SecureLink 产品只允许应用级访问，不暴露内网。即使员工电脑上被安装了恶意软件也无法扫描，窃取内网上的资源。最小授权原则和基于身份确认授权，只授予员工所需的最小权限，细粒度访问控制，可以保证用户只能看到被授权的应用或资源。限制勒索软件的入侵和传播，降低由于单一设备感染勒索软件，导致勒索软件在内部网络进一步传播的可能。

终端设备绑定和安全基线检查

目前，65%的企业允许员工使用未受控的个人 BYOD 设备接入内部应用系统，端点安全建设至关重要，主要包括授信设备检测以及终端环境检测等，如检测设备唯一 ID 标识、病毒查杀、入域准入、弱密码检测等措施，同时在终端设备接入过程中，将根据安全基线实时监测用户终端设备的健康状态，判断终端是否授信准入。终端安全检测，保护用户设备安全性，防止攻击者利用作为内网入侵的入口。

- 终端序列号绑定：通过对终端设备物理特征计算出的唯一序列号进行绑定，确保用户账号只在被授权的终端上登录和访问，提升安全性
- 终端安全基线检查：针对终端设备的环境安全基线进行检查，如未入域、弱口令等不符

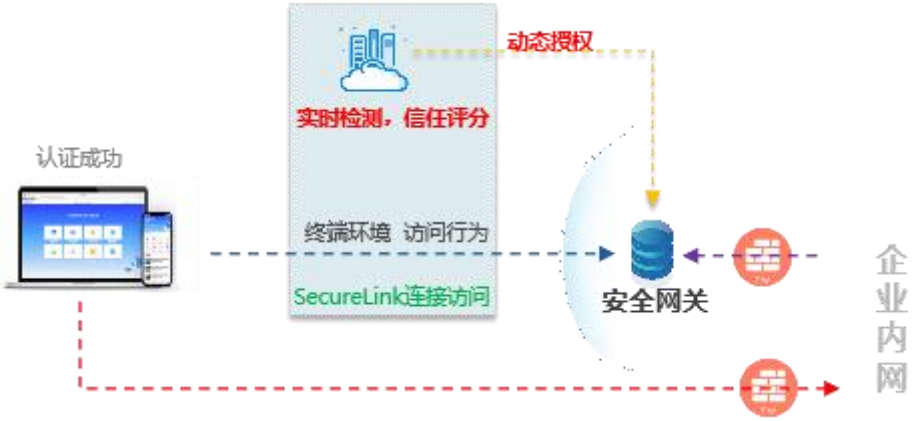
合安全基线的终端将不允许登录

- 终端杀毒软件检测：检测终端设备是否安装及运行指定的安全软件，如未安装或运行则控制访问
- 端侧运行进程检测：避免使用盗版或来路不明的软件，检测关键业务系统使用的相关软件版本，避免由于软件版本低引发安全风险。

网宿 SecureLink 同时支持联动流安全产品终端防御能力，对用户终端进行安全防护。终端防护产品集病毒查杀、实时防护、勒索软件、挖矿病毒防护、漏洞检测与修复、终端管理、主机防火墙、外设管控、EDR、资产管理、主机加固、文件分析、威胁处置等。

持续评估访问安全状态

用户登录认证成功并不代表对于用户的绝对信任和长期信任，平台对用户的每条访问和操作行为需要实时检测，主要通过用户行为分析、异常行为检测、网络流量安全检测等措施，根据检测结果动态调整该用户的权限，甚至关闭该用户的账号权限，来保障应用业务的安全。



对终端及用户行为进行持续验证，对检测到的异常行为、越权行为、威胁检测、终端环境等进行信任评分，根据检测结果动态调整用户的访问权限，保障应用业务的安全。使用 UEBA 智能模型机制来检测用户、设备的异常活动，自动化响应其威胁，告警和阻断。每个连接请求都根据一组上下文因素进行验证，从而得出基于风险的访问决策：

- 源连接是否来自经认证和授权的用户？
- 它是否来自已知且安全的设备？
- 该用户是否经常从该地理位置进行连接？
- 连接时间与该用户历史记录是否一致？
- 是否存在其他应在授予访问权限之前加以重视的信号或威胁情报？

全局风险监测示警和追溯

基于用户行为检测、终端检测、入侵检测等各种要素洞悉客户网络安全风险。网宿 SecureLink 平台对用户的异常访问和操作行为进行记录，同时，会将记录下的所有信息传

送到网宿安全管控平台，通过平台安全风险感知对大量数据进行统计分析，并在控制台展示检测到的入侵事件/异常事件/风险事件和对应数据呈现，如风险事件排名、高位用户排名、异常事件趋势图、最新风险展示及行为分析展示等等，对网络流量进行分析、识别、检测、告警及追溯审计可能的入侵行为，为管理员提供安全运维的决策依据。

踏上零信任之旅

借助零信任，现在我们可以将风险持续评估能力、动态访问控制、实时审查能力集成于复杂的安全架构。零信任不仅仅是一项技术解决方案，更是一次企业文化变革。零信任能够确保企业的业务融合创新及演进战略得以安全实施，沟通、员工专业培训、认知和运营流程调整等软因素是取得转型成功的关键要素，更会令每个人都意识到在推进数字化转型方面可带来的持续益处。

很多企业已经有意或无意地走上了“零信任”之旅，所采用方法因企业 IT 架构阶段而不同，其战术、架构或战略的选取也相应不同。任何零信任之旅都将面临各种阻碍，需要整个企业给予强有力的领导层支持、投资和认同才能确保成功。您需要考量与企业相关的业务驱动因素、现有流程功能和关键场景用例。建议从以下这些问题进行考虑：

企业的资产是否清晰？目前互联网暴露面状态？

企业重要资产在哪里？本地 IDC？公有云？您想要保护哪些资产？

远程工作的人员、角色范围？VPN 使用情况和威胁状态？

企业受管控设备比例？受控安全措施是否充分？

企业提供合作伙伴、供应链上下游访问的风险？

谁使用哪些设备能够访问哪些资产，必须满足哪些条件？

是否优先可用云化 ZTNA 能力，而无需在防火墙提供入站服务？

SASE 全局安全能力框架的规划？

要回答这些问题，企业需确定执行 IT 资产管理、安全基线规则和数据治理诉求，以了解自身资产和数据的类别和重要性，并由此创建访问控制和安全控制策略。确定您的目标并将其嵌入零信任系统端到端的策略机制中，并将数据业务服务和公共互联网的可见性进行隔离，这是实现所期望转型业务成果的最可靠起始路径，并逐步向安全接入服务边缘一体能力模型演进。

五、网宿零信任的概要简介

网宿安达 SecureLink 产品打破传统网络安全的固化边界概念，引导安全架构从网络中心化转向身份中心化，通过对用户、设备、网络、应用、数据的动态连接访问控制，建立应用层可视化、自动化、智能化的安全防护体系。其身份可信、终端可信、行为可信的核心特性能力，以及从传输加密、边缘防护、网络隐身打造的平台安全能力，为企业搭建安全访问体系，实现用户使用任意终端在任意网络环境中安全、高效、可靠、便捷地访问企业资源。

(1) SecureLink 产品通过信任评估引擎实时检测用户和设备的状态、网络连接信息、应用业务上下文、访问时空环境等多维数据，根据识别的风险动态调整用户的访问权限。

(2) 网络隐身，默认情况下服务端口全隐藏，业务全隐身，只有验证用户和设备身份的合法性后，才针对合法用户合规终端开放网络端口和业务访问权限,减少网络威胁面。

(3) 流量深度解析能力，实时分析、检测访问流量中的威胁攻击从而进行告警和阻断。

(4) 结合网宿云安全能力，提供分布式边缘防护，包括 DDoS 防护能力、WAF 安全能力等。

(5) 网宿全球网络加速能力,解决企业远程访问速度和稳定性问题,提供最佳客户连接体验。

(6) 管理便捷的一站式管理平台，可实现对用户操作行为的全面审计，通过平台实现全网业务态势感知，支持威胁探测和告警，满足企业运维及安全需求，提高管理效率。

(7) 凭借网宿全球分布式的安全传输网络的天然优势，建立起一张虚拟安全网络，为企业打造安全、高效的远程访问环境，提升业务敏捷性。

此外，所有行业和所有地理地域都处于勒索软件攻击的风险之中，针对勒索软件攻击制定响应计划十分重要，当勒索事件发生的紧张关键时刻，有效的预防手段、处置方案会对所花费时间和经济损失产生显著影响。网宿安全服务团队可以为贵组织开展勒索软件准备情况进行全面评估，对企业网络进行漏洞检测、渗透测试，提出整改加固建议，组织安全培训和演练，制定针对勒索软件攻击事件响应计划，同时考虑所需的业务和技术应对措施，帮助企业组织为勒索软件攻击做好充足应对准备。

网宿零信任平台对 IT 网络安全进行范式更新，因应当前云、大数据、物联网、移动化的网络架构演化趋势，针对各类网络威胁构建多层面立体防御，提供安全的统一业务可信接入平台，已成功为金融、政府、医疗、能源、教育等行业众多客户提供服务。

参考文献

[1] 2022 SONICWALL CYBER THREAT REPORT

[2] X-Force Threat Intelligence Index 2022，IBM Security

[3] 2021 网络安全前瞻调研报告，Deloitte

[4] Cost of a Data Breach Report 2021，IBM Security

[5] The definitive guide to ransomware，IBM Security

[6] 2020年中国互联网网络安全报告，CNCERT|CC

[7] 勒索软件安全防护手册，CAICT中国信息通信研究院

[8] Market Guide for Zero Trust Network Access 2020,Gartner