

2021上半年 勒索病毒趋势报告 及防护方案建议

WannaCry爆发四年后，
为什么还没有对付勒索病毒的“银弹”？

目 录

前言.....	1
一、 勒索病毒攻击最新趋势盘点	4
1.1 2020/2021 勒索病毒 1-4 月攻击态势对比.....	4
1.2 2021 年 Q1 最流行的勒索病毒家族.....	5
1.3 1-4 月勒索病毒受灾地域分布.....	8
1.4 1-4 月勒索病毒攻击行业分布.....	9
二、 十大典型勒索病毒案例分析	10
2.1 全球超 150 个国家和地区遭 WannaCry 攻击，损失高达数十亿美元.....	10
2.2 美国波音工厂遭 WannaCry 攻击，导致自动化组装生产线被迫停工.....	11
2.3 台积电芯片制造基地遭遇勒索病毒攻击，损失超 17 亿元.....	11
2.4 全球最大助听器制造商 Demant 遭勒索病毒攻击，损失高达 9500 万美元.....	12
2.5 法国最大商业电视台 M6 Group 惨遭勒索软件洗劫，集体被迫“罢工”.....	13
2.6 自动化设备生产巨头皮尔兹遭勒索攻击，网络被迫中断网络超一周.....	13
2.7 佳明遭勒索软件重创：业务瘫痪产线停运，被勒索千万美元赎金.....	14
2.8 佳能遭 Maze 勒索软件攻击，2.2GB 美国公司数据被“撕票”泄露.....	15
2.9 富士康工厂遭勒索攻击：上千台服务器被加密，索要 3400 万美元赎金.....	15
2.10 台湾 PC 巨头宏基(Acer)遭勒索攻击，赎金创 5000 万美元新纪录.....	16
三、 勒索病毒攻击分析.....	16
3.1 勒索病毒产业链中的五大关键角色.....	16
3.2 传播技术手段.....	18
3.3 勒索病毒的常规攻击路径.....	20

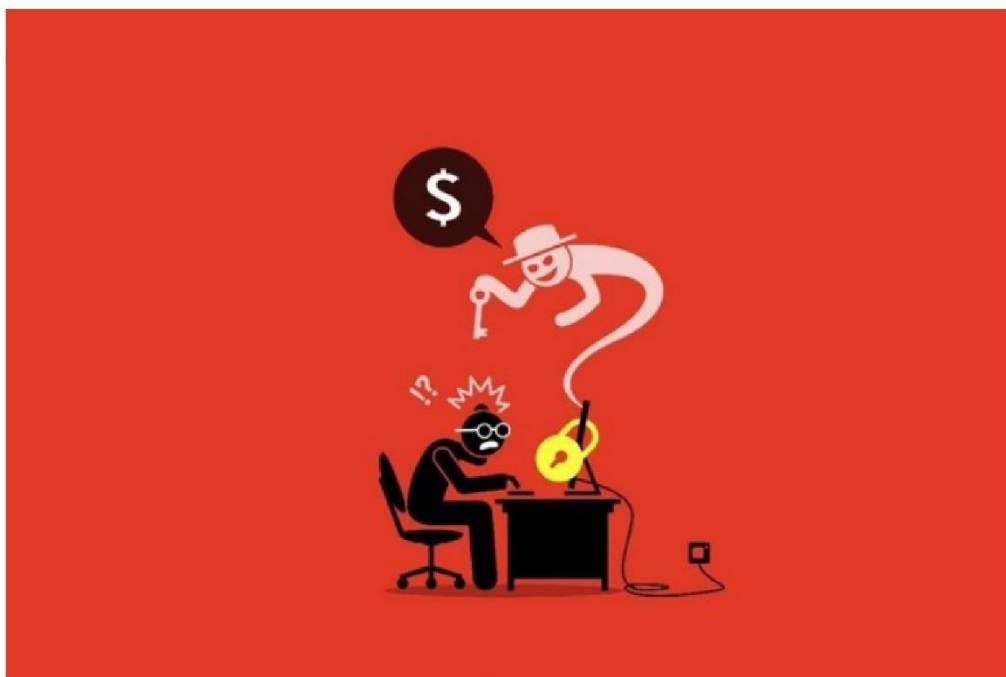
3.4	勒索病毒主要攻击特征.....	21
四、	勒索病毒未来发展趋势.....	22
五、	防御方案建议.....	23

前言

2017 年 5 月 12 日, WannaCry 勒索病毒通过 MS17-010 漏洞在全球范围爆发, 形成一场影响全球的蠕虫病毒风暴。伴随当前 AI、物联网、区块链、工业互联网等新技术的飞速发展, 以及各类加密数字货币在全球市场持续火爆, 勒索病毒也持续高发, 很多全球知名企业都曾因勒索病毒导致经济和声誉损失。勒索病毒也因此已成为近年来网络安全主要的威胁之一。

事实上, 勒索病毒最早可追溯到 1989 年, 哈佛大学学生约瑟夫·L·波普编写一款电脑病毒-AIDS 木马。这款木马的传输方式和加密手段包括支付赎金的方式都相对简单仅零星发生, 被归纳在恶作剧攻击并未构成较大威胁, 但这一病毒的出现可以说打开了勒索病毒的潘多拉魔盒, 自此勒索病毒如鬼魅一般, 频繁将魔爪伸向企业及个人用户。

2006 年, 国内出现首款勒索软件 Redplus, 勒索赎金从 70 元至 200 元不等; 从 2013 年的 CryptoLocker 开始, 黑客团伙开始利用比特币作为赎金, 这款软件为黑客团伙带来近 41000 枚比特币收入, 按照最新市值折算将近 10 亿美元之巨; 2020 年, 制造 Troldeh 病毒的黑客团队在 Github 上发表了声明宣布要金盆洗手, 公布团队 75 万多个解密密钥, 顿时引起业界一片哗然。



勒索病毒从零星恶作剧发展到频繁发生的主要原因包括三点：第一，勒索病毒加密手段复杂，解密成本高；第二，使用电子货币支付赎金，变现快追踪难；第三，勒索软件服务化的出现，开发者提供整套勒索软件解决方案，从勒索软件的开发、传播到赎金收取都提供完整的服务。攻击者不需要任何知识，只要支付少量的租金就可以开展勒索软件的非法勾当，大大降低了勒索软件的门槛，推动了勒索软件大规模爆发。

与此同时，随着不断有攻击者通过迫使受害者就范而获得非法收益，散在发生的勒索病毒攻击手法日益流行，其表现和传播手法也在不断升级。常见的攻击方式包括系统漏洞攻击、远程访问弱口令攻击、钓鱼邮件攻击、Web 服务漏洞和弱口令攻击、数据库漏洞和弱口令攻击等。值得一提的是，勒索病毒未来将呈

现勒索产业化、场景多样化、平台多元化等显著趋势，持续对公众网络安全造成极大的威胁。

而随着勒索病毒案例的不断涌现，不少企业在安全厂商的建议完善了数据备份方案。目前主流安全厂商积极响应，并推出各类防御产品及解决方案，为公众提供安全防护服务与信息。作为拥有二十余年安全能力沉淀经验的安全厂商，腾讯安全对全球勒索病毒深入分析及研判，挖掘其中涉及的安全漏洞、入侵手法和攻击工具，为个人及企业用户提供网络安全防护。目前，腾讯安全通过企业级杀毒软件内置的终端数据保护功能（如腾讯零信任 iOA、腾讯电脑管家已内置文档守护者自动备份）对数据进行备份，迫使勒索黑客仅靠破坏用户数据也难以让勒索得手。

WannaCry 的爆发让勒索病毒走进了大众视野，至今已经四年，这四年间勒索病毒又衍生出了多个变种，并且持续对企业网络安全造成威胁，仅 2021 年 1 季度就发生了多起国际知名企业被勒索的案件，并且赎金持续刷新纪录。目前尚未出现对付勒索病毒的“银弹”，应对勒索病毒的核心原则仍然是以事前防范为主。所幸的是，勒索病毒虽然无解，但是企业仍可以通过提升打预防针的方式获得更高的“免疫力”。

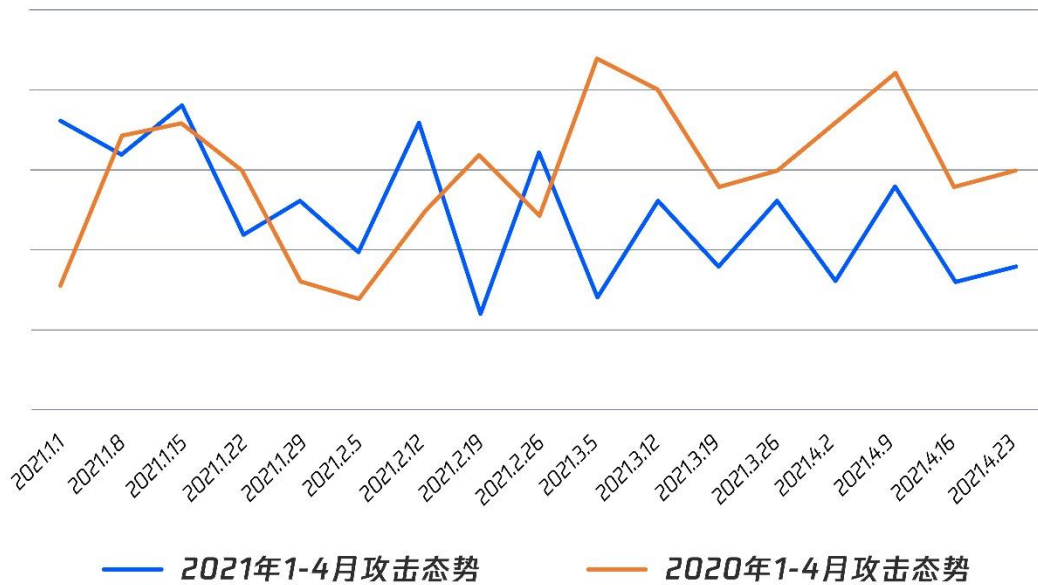
为了帮助更多企业和机构了解和尽可能规避勒索病毒的危害，腾讯安全联合南方都市报以安全事件告警工单数据为基础，基于勒索病毒的起源与演变，从数据概览、入侵特点、攻击手段、活跃家族排行榜等维度，剖析过去半年勒索病毒的攻击形势，通过分析勒索病毒的攻击路径及案例盘点，为广大个人用户防范信息泄露风险提供实用建议。

一、勒索病毒攻击最新趋势盘点

1.1 2020/2021 勒索病毒 1-4 月攻击态势对比

2021年，勒索病毒攻击态势在春节期间降至最低，观察其攻击态势，2021年相比去年同时期稍有下降。但勒索事件仍然频发，勒索金额屡创新高，勒索攻击愈发具备针对性。

2020/2021勒索病毒1-4月攻击态势对比



1.2 2021 年 Q1 最流行的勒索病毒家族

1.2.1 Globelmposter

Globelmposter 出现于 2017 年中，加密文件完成后会留下名为 HOW TO BACK YOUR FILES.(txt、html、exe), Decryption_Info.html 类型的勒索说明文件。该病毒加密扩展后缀繁多，其规模使用且感染泛滥的类型有 12 生肖 4444, 12 生肖/主神 666, 12 生肖/主神 865, 12 生肖/主神 865qq, C*H 等系列，由于该病毒出现至今仍然无有效的解密工具，各政企机构需提高警惕。

1.2.2 Phobos

Phobos 勒索病毒是 2019 年 8 月出现的一款新型的勒索病毒，主要通过 RDP 方式入侵，然后在受害者主机上运行勒索病毒加密文件。这款勒索病毒已出现最新变种样本，主要以 devos、devoe、devil、dever、dewar、actin、acton、actor、acuff、acute 等加密后缀为主，目前病毒变种的流行加密后缀已有几十个不同变种。

1.2.3 Crysis

Crysis 勒索病毒从 2016 年开始具有勒索活动，加密文件完成后通常会添加“ID+ 邮箱+ 指定后缀”格式的扩展后缀，例：“id- 编号.[gracey1c6rwhite@aol.com].bip”，其家族衍生 Phobos 系列变种在 2019 年 2 月开始也有活跃。该病毒通常使用弱口令爆破的方式入侵企业服务器，安全意识薄弱的企业由于多台机器使用同一弱密码，面对该病毒极容易引起企业内服务器的大面积感染，进而造成业务系统瘫痪。

1.2.4 Sodinokibi

Sodinokibi 勒索病毒首次出现于 2019 年 4 月底，由于之后 GandCrab 停止运营事件，该病毒紧跟其后将 GandCrab 勒索家族的多个传播渠道纳入自身手中。该病毒目前在国内主要通过 Web 漏洞和钓鱼邮件传播，也被国内厂商称为 GandCrab 的“接班人”，该病毒的特点之一是病毒加密完成后会把壁纸修改为蓝色背景壁纸，因此也得名“锁蓝勒索”。

该病毒攻击时也会使用内核提权漏洞 CVE-2018-8453 将自身提升到 SYSTEM 权限，已获得更多文件的读写权限，使得加密文件过程更加顺利。同时，该病毒也在不断的对国内系统做定制化的操作（中文支持，国内大软件目录判断），毫无疑问，国内是该病毒的重点打击目标之一。

1.2.5 Buran

Buran 勒索病毒从 2020 年上半年开始进入我国，因会在注册表和加密文件中写入“buran”字符串，故命名为 buran 勒索病毒。该病毒起初是以邮件形式进行传播，若用户下载邮件附件，启用宏代码，就会下载激活勒索病毒，导致磁盘文件被加密。而变种之后的病毒传播形式转为通过 RDP 爆破拿到远程桌面密码后手动投毒，感染量不断上升，对用户电脑及财产安全造成极大威胁。

1.2.6 Medusalocker

Medusalocker 该病毒出现于 2019 年 10 月，已知该病毒主要通过钓鱼欺诈邮件及弱口令爆破传播。该病毒早期版本加密文件完成后添加扩展后缀.encrypted 或者.ReadTheInstructions 后缀，近期传播病毒版本加密文件后添加.deadfiles .EG 扩展后缀，也看到有使用.shanghai 国内地域拼音的后缀类型。通常该团伙攻击者向受害者勒索 1BTC（比特币），当前市值约 6.4 万元。

1.2.7 Avaddon

Avaddon 勒索病毒出现于 2020 年 6 月上旬，病毒早期版本加密文件完成后会添加 avdn 扩展后缀，随后病毒加密文件扩展变更为随机字符串。加密文件完成后留下名为“随机-readme.html”的勒索信文档。该病毒出道即以大量的垃圾邮件传播，同时与 Phorpiex 僵尸网络合作。导致其一度感染量上升。

1.2.8 Lockbit

lockbit 勒索病毒出现于 2019 年末，传播方式主要利用 RDP 口令爆破，并使用 RSA+AES 算法加密文件，加密过程采用了 IOCP 完成端口+AES-NI 指令集提升其病毒工作效率，从而实现对文件的高性能加密流程。由于该病毒暂无有效的解密工具，被攻击后无法恢复文件。值得注意的是，该病毒此前主要活跃在国外，目前其已将狩猎目标拓展到国内。

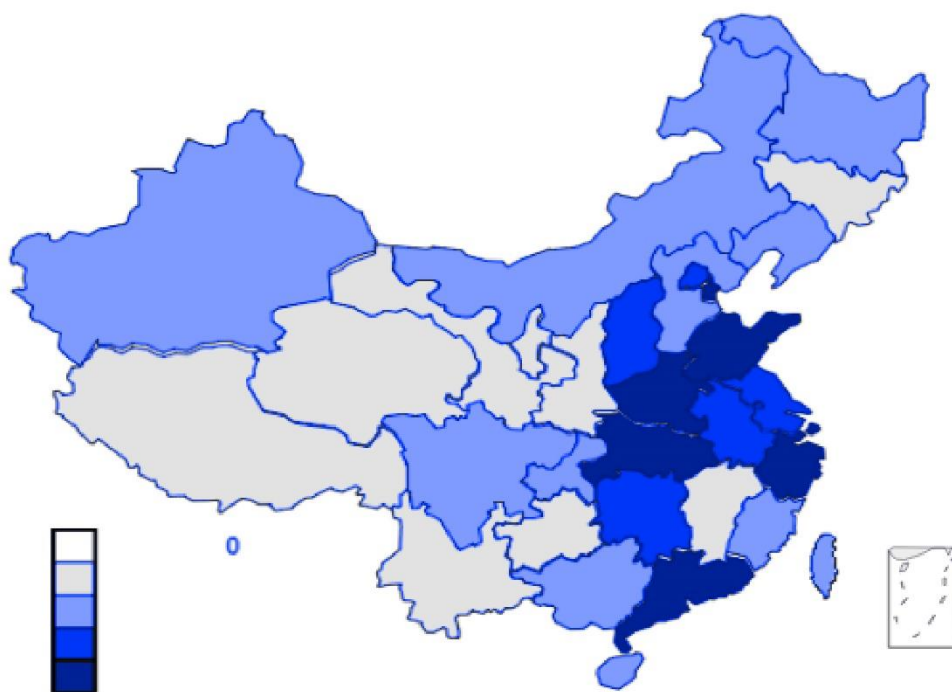
1.2.9 Ryuk

Ryuk 勒索病毒最早于 2018 年 8 月被首次发现，主要针对大型企业及组织进行定向攻击勒索，这款勒索病毒主要在国外较为流行。目前该病毒主要通过网络攻击手段并利用其它恶意软件进行传播，同时充当下载器功能，提供下载其它勒索病毒服务。

1.2.10 NEMTY

NEMTY 勒索病毒出现于 2019 年 8 月，该病毒早期加密文件完成后会添加 NEMTY 扩展后缀，也因此得名。该病毒在国内会依靠垃圾邮件，RIG EK（漏洞利用工具包）传播，最新变种加密文件完成后会添加._NEMTY_random 形式的随机扩展后缀。该病毒也与 Phorpiex 僵尸网络有着密切的合作，常借助僵尸网络扩散传播。

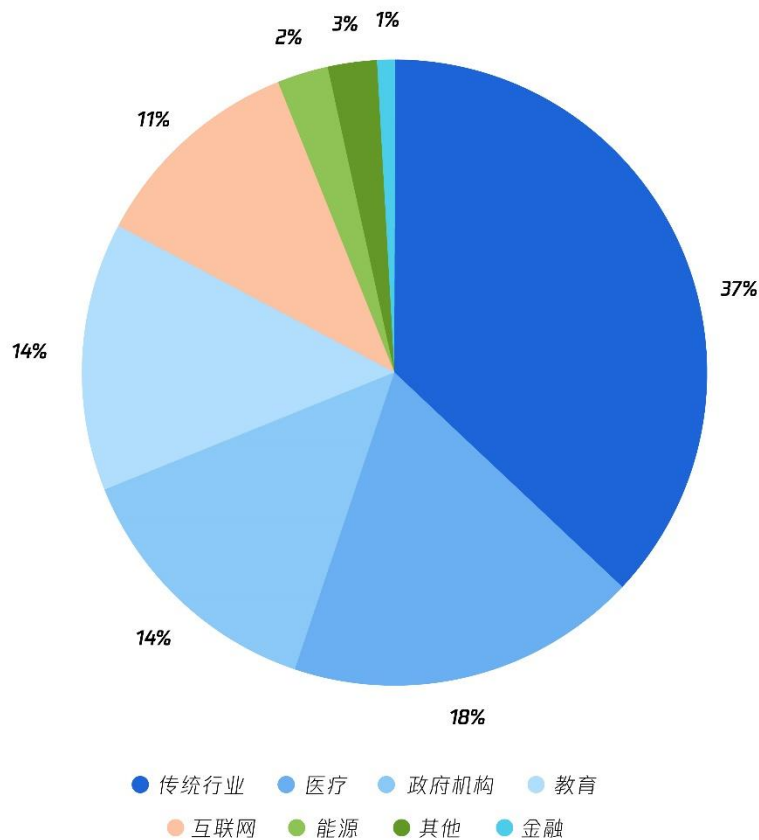
1.3 1-4月勒索病毒受灾地域分布



国内遭受勒索病毒攻击中，广东，浙江，山东，湖北，河南，上海，天津较为严重，其它省份也有遭受到不同程度攻击。

1.4 1-4月勒索病毒攻击行业分布

勒索病毒感染行业占比



从勒索病毒感染行业来看，数据价值较高的传统行业、医疗、政府机构遭受攻击较为严重，占比依次为 37%、18%、14%，总计占比高达 69%。

二、十大典型勒索病毒案例分析

2.1 全球超 150 个国家和地区遭 WannaCry 攻击，损失高达数十亿美元

2017 年 5 月 12 日晚，一场被命名为“WannaCry”的勒索病毒攻击首先在英国爆发，并以“蠕虫式”的传播速度迅速蔓延至全球 150 多个国家和地区（幸免国家要么没有电脑，要么没有网络）。“你的电脑已经被锁，文件已经全部被加密，除非你支付价值 300 美元的比特币，否则你的文件将会被永久删除”的锁定桌面，瞬间感染波及全球近 20 万电脑设备。全球多地发出告警，短短两日内，包括政府、医疗、学校甚至是公益机构在内的多个板块的大量电脑文件被加密，并均受到要求支付比特币以解密文件的威胁。

通过分析发现，WannaCry 勒索病毒是不法分子通过改造之前泄露的 NSA 黑客武器库中“永恒之蓝”攻击程序发起的蠕虫病毒攻击。攻击者利用了微软基于 445 端口传播扩散的 SMB 漏洞 MS17-010，实现远程代码执行。攻击成功后携带勒索软件功能的蠕虫病毒会对主机文件进行加密，并扫描网络内其他主机进行传播，从而实现对被攻击者实施勒索。据悉，数内网机器未及时更新微软于 3 月发布的漏洞补丁，是导致电脑大规模中招的重要原因。

WannaCry 勒索蠕虫是传统勒索软件与蠕虫病毒的结合体，同时拥有蠕虫扩散传播和勒索软件加密文件的双重功能。WannaCry 一旦进入目标电脑，就会通过检查硬编码的终止开关域来开展恶意活动。若未发现终止开关域，则会在加密文件的基础上，利用漏洞展开联机攻击，并向被攻击者发起 3 天或 7 天内，以加密比特币的方式，支付 300-600 美元的赎金要求。专家分析，这一攻击过程

不仅会带来图片、文档、压缩包、音频、视频、可执行程序等重要文件和数据信息的损失,同时也存在危及医疗设备、能源系统等公共安全设施的可能性。此外,比特币支付方式的不可追踪,更是让 WannaCry 病毒蔓延带来经济损失加码。

业内专家评称,修正了“永恒之蓝(EternalBlue)”的漏洞,同时发现了允许停止执行恶意软件的“杀死开关”,是帮助减缓这一恶意活动的两个主要贡献。然而,高达数十亿美元的损失总额,实为在全球范围内引发了史无前例的震动。

2.2 美国波音工厂遭 WannaCry 攻击,导致自动化组装生产线被迫停工

2018 年 3 月,据外媒报道,美国波音飞机位于南卡罗来纳州查尔斯顿的生产工厂遭到 WannaCry 勒索病毒攻击,导致 777 翼梁自动化组装生产线被迫停工,是 2018 年首例被媒体披露的 WannaCry 勒索病毒攻击事件。攻击者向波音索要价值 300 美元的比特币作为赎金以恢复数据和业务。

鉴于对攻击迅速转移态势的分析与担忧,波音公司总工程师 Mike VanderWel 第一时间在全公司范围内发布了相关备忘录,要求全体员工做好应对措施,避免病毒以攻击功能飞机测试设备为跳板,实现对飞机系统软件直接扩散、蔓延情况的发生。波音在对外声明中称,网络安全中心发现仅有少数设备系统遭到了入侵并已展开补救,且不影响生产交付。

2.3 台积电芯片制造基地遭遇勒索病毒攻击,损失超 17 亿元

2018 年 8 月,全球知名半导体厂商台积电营运总部和新竹科学园区的 12 英寸晶圆厂电脑被曝遭到勒索病毒攻击,造成竹科 FAB 12 厂、南科 FAB 14 厂、

中科 FAB 15 厂等三处主要高端生产基地的生产线短短几小时内全数停摆，直接导致台积电股价下跌，直接经济损失高达 17 亿元人民币。

据台积电对外声明称，此次事件中，设备感染的是勒索病毒“WannaCry”的变种，具体表现是电脑蓝屏、设备宕机、各类文档和数据库锁定等。感染的原因是员工在为新机台安全软件过程中，没有事先做好隔离和离线安全检查工作，导致新设备连接到公司内部网络后，病毒快速传播，并最终影响整个生产线。基于台积电相关电脑设备使用的都是 Windows 7 系统，业内人士也分析很可能或是没有及时升级系统补丁，或者没有关闭 445 端口，导致病毒的入侵与扩散。

幸运的是，台积电主计算机系统并未受到攻击影响，其也在第一时间采取措施弥补这一安全疏忽并加强了安全措施。但值得一提的是，诸如台积电这一生产设备和检测设备等都被勒索病毒同时攻击的情况还是前所未有的。

由此不难看出，从 2017 年到 2018 年，以 WannaCry 为首的勒索病毒攻击已经跳脱了对仅限于核心业务文件的加密，转而向企业服务器和业务系统的攻击拓展。通过感染企业关键系统，破坏企业日常运营，从而带来动辄停产的直接后果。

2.4 全球最大助听器制造商 Demant 遭勒索病毒攻击，损失高达 9500 万美元

2019 年 9 月，据外媒报道，全球领先的助听器制造商的迪曼特集团 (Demant) 遭遇 NotPetya 勒索软件攻击。尽管该公司已经备份了数据，但攻击的规模似乎对其恢复具有重大影响。该公司的 IT 基础架构受到网络攻击的影响，其通过关闭多个站点和业务部门中的 IT 系统来限制事件的进一步发酵，但

是整个价值链的关键业务流程仍然受到事件的影响，包括研发、生产和分销。这些中断的累积影响将对该公司 2019 全年造成高达 6 亿人民币的负面财务影响，该公司的之前购买的保险为公司减少了一部分损失。Demant 预计，本次直接损失将达 5000 万人民币。

据了解，该勒索病毒团伙曾导致航运巨头马士基和快递服务联邦快递等公司各自遭受超过 3 亿美元的损失。

2.5 法国最大商业电视台 M6 Group 惨遭勒索软件洗劫，集体被迫“罢工”

2019 年 10 月，法国最大商业电视台 M6 Group 惨遭勒索软件洗劫，公司电话、电子邮件、办公及管理工具全部中断，集体被迫“罢工”。事件发生后，其他电视台已禁止员工通过电子邮件与 M6 进行通信，以免受到感染。而此次事件很有可能是黑客使用了网络钓鱼电子邮件或利用了未打补丁的软件，从而使电视台网络被勒索软件感染至扩散。M6 集团在公开领域并未透露攻击者信息及是否交付巨额赎金。

2.6 自动化设备生产巨头皮尔兹遭勒索攻击，网络被迫中断网络超一周

2019 年 10 月，全球最大的自动化工具生产商之一皮尔兹（Pilz）遭受 BitPaymer 勒索软件攻击，该公司在全球范围内的所有服务器和 PC 工作站，包括通信设施，都受到了影响，公司被迫关闭其网络。Pilz 员工花了三天时间才恢复对其电子邮件服务的访问权限，又花了三天时间恢复国际电子邮件服务，直到

一周后才恢复对产品订单和交货系统的访问。该企业对外声称，其生产能力没有受到影响，但是无法检查订单，并且生产速度较慢。

2.7 佳明遭勒索软件重创：业务瘫痪产线停运，被勒索千万美元赎金

2020 年 7 月，健身追踪器、智能手表和 GPS 产品制造商 Garmin 遭受了 WastedLocker 勒索软件的全面攻击，主要产品服务和网站均瘫痪，攻击者向 Garmin 索要高达 1000 万美元赎金，威胁要删除服务器上的所有数据。

其中，Garmin Connect 网站和移动应用程序以及 Garmin Pilot、Connex 和 FlyGarmin，因数据无法同步更新，被迫大规模下架。Garmin Pilot 等商用航空产品被迫关闭停运。参考国际咨询机构 Canalys 对 2020 年第一季度全球可穿戴市场的评估，佳明在全球可穿戴市场的份额大概是 7.3%，整体用户数量为 7000 万，按照这个数字推算，此次 Garmin 遭受攻击将影响至少 1500 万用户。

面对勒索病毒的入侵，佳明的产业和业务一下子就遭遇了全面打击。跟最严重的后果比起来，用户服务的暂时停摆都不算什么。有台湾媒体援引知情人士信息，佳明的台湾工厂也已经停工，可见此次勒索病毒影响之深。

从目前已知的情况看，这次攻击是一次黑客组织长期策划、筹备的针对性攻击。甚至存在一种更糟糕的可能性：黑客组织很可能在实施勒索病毒攻击之前，已经将佳明的用户数据盗取，佳明想要恢复用户的云端数据，只能接受黑客组织的威胁。否则将因用户隐私数据泄露造成更大的损失。

2.8 佳能遭 Maze 勒索软件攻击, 2.2GB 美国公司数据被“撕票” 泄露

2020 年 8 月, 著名数码摄像机厂商佳能(Canon)被曝遭受 Maze 团伙勒索攻击, 影响电子邮件、微软团队、美国网站及其他内部应用程序。其中, 佳能 image.canon 云照片和视频存储服务的可疑中断, 导致其免费 10GB 存储功能的用户丢失数据。由 BleepingComputer 消息称, 佳能经历了“影响多个应用程序、团队、电子邮件和其他系统的广泛传播的系统问题, 目前可能不可用”。

随后, Maze 因未收到赎金, 在暗网泄露了佳能大约 2.2GB (据 Maze 团伙称仅为所有窃取数据的 5%) 的美国公司营销数据和视频文件, 从而导致佳能部分内部系统中断。但佳能全球网站和电子商务网站等在内的其他资产似乎不受影响, 这意味着佳能的网络安全措施有效防止了勒索软件损失的扩大化。同时, 也在一定程度上, 反映了传统“支付赎金”的应对策略正在失效。

2.9 富士康工厂遭勒索攻击: 上千台服务器被加密, 索要 3400 万 美元赎金

2020 年 11 月, 全球最大电子制造公司之一——富士康位于墨西哥的华雷斯城 CTBG MX 工厂设施被曝遭受“DoppelPaymer”勒索软件攻击, 导致 1200 台服务器被加密。据悉, 攻击者在对设备进行加密前已窃取了 100GB 的未加密文件(包括常规业务文档和报告, 但不可苦熬任何财务及员工个人信息), 并删除了 20-30 TB 的备份。随后, 攻击者发布了一个指向 DoppelPaymer 付款站点的链接, 要求富士康支付 1804.0955 比特币作为赎金(约 3486.6 万美元, 约 2 亿元人民币), 否则将把盗取数据在暗网出售。

随后，富士康对外声称，其网络安全团队已经完成了软件和作业系统的安全更新，并且提升了安全防护等级，受到影响的厂区网络已经逐渐恢复正常。

2.10 台湾 PC 巨头宏基(Acer)遭勒索攻击，赎金创 5000 万美元新纪录

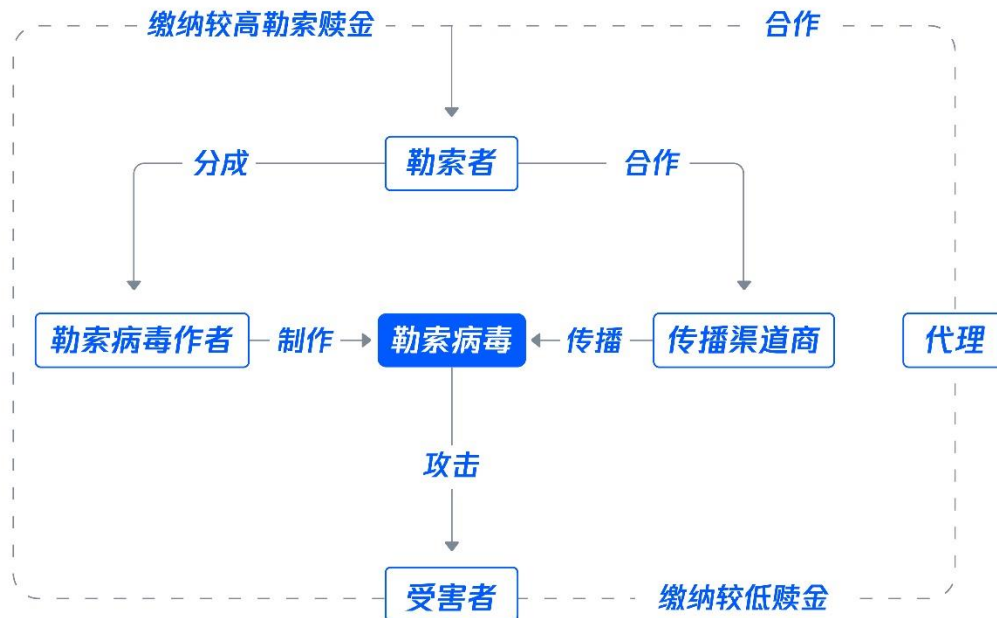
2020 年 3 月，台湾 PC 巨头宏基(Acer) 遭到勒索病毒组织 REvil 的网络攻击，并被索要支付高达 5000 万美元的赎金，刷新了勒索病毒有史以来的最高赎金纪录。同时，攻击者还在网站上公布了从宏碁窃取的部分财务电子表格、银行结余和银行往来邮件等数据，并提出只有支付赎金，才能提供解密工具、漏洞报告以及删除盗取的文件；此外，还对宏碁发出了“不要重蹈 SolarWind 覆辙”的含糊警告。

据外媒 BleepingComputer 分析，REvil 可能是通过瞄准宏碁域名上的一台 Microsoft Exchange 服务器上的漏洞，才得以成功发动了此次攻击，这也是针对大型目标实施勒索软件攻击的首次做法。目前，因宏碁并未支付赎金，REvil 已在暗网出售宏碁财务表格、银行结余、银行通讯文档等机密资料。

三、勒索病毒攻击分析

3.1 勒索病毒产业链中的五大关键角色

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网络勒索类型也是千姿百态。网络勒索具有匿名性、隐蔽性、便捷性等特点，深受黑产青睐。其中典型的勒索病毒作案实施过程如下，一次完整的勒索可能涉及 5 个角色（一人可能充当多个角色）。



勒索病毒作者：负责勒索病毒编写制作，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。

勒索者：从病毒作者手中拿到定制版本勒索病毒或勒索病毒原程序，通过自定义病毒勒索信息后得到自己的专属病毒，与勒索病毒作者进行收入分成。

传播渠道商：帮助勒索者传播勒索病毒，最为熟悉的则是僵尸网络，例 Necurs、Gamut，全球有 97%的钓鱼邮件由该两个僵尸网络发送。

解密代理：向受害者假称自己能够解密各勒索病毒加密的文件，并且是勒索者提出赎金的 50%甚至更低，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，勒索病毒产业链养活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，让勒索病毒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。

受害者：通过勒索病毒各种传播渠道不幸中招的受害者，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。

3.2 传播技术手段

总结市面较为高发的勒索病毒特征，可大致将勒索病毒的传播手段分为 6 个方向：

3.2.1 弱口令攻击

由于部分服务器会使用弱口令远程登录，不法黑客便利用这一弱口令登陆短板暴力破解远程登录密码，并手动下载运行勒索病毒。即使服务器安装了安全软件，不法黑客也可手动退出。这一手段隐蔽性、机动性均较高，极难被安全软件发现。

3.2.2 U 盘蠕虫

以 U 盘或移动设备作为介质，利用感染型病毒的特点，病毒运行过程中，大量占用系统资源，随后会开启后门功能，用户电脑中的所有隐私将完全暴露在黑客面前。随后黑客便可加密用户所有文档后再弹出勒索信息，而由于 PE 类文件被感染后具有了感染其他文件的能力，因此如果此文件被用户携带（U 盘、网络上传等）到其他电脑上运行，就会使得该电脑的文件也被全部感染加密。

3.2.3 软件供应链攻击

病毒制作者通过劫持正常软件的安装、升级服务，在用户进行正常软件安装、

升级时植入勒索病毒。这种传播方式利用了用户与软件供应商之间的信任关系，成功绕开了传统安全产品的围追堵截，传播方式上更加隐蔽。此前侵袭全球的 Petya 勒索病毒便是通过劫持 Medoc 软件更新服务进行传播。

3.2.4 系统/软件漏洞

2017 年 5 月全球爆发的 WannaCry 就是利用 Windows 系统漏洞进行传播，利用系统漏洞传播的特点是被动式中毒：用户即使没有访问恶意站点，没有打开病毒文件也会中招。利用系统漏洞传播的蠕虫病毒还会扫描同网络中存在漏洞的其他 PC 主机，只要主机没有打上补丁，就会被攻击。

3.2.5 “无文件”攻击技术

“无文件”攻击最常见的是利用恶意文本文档传播，多见通过邮件附件进行传播。勒索病毒通常会伪装成用户常查看的文档，如信用卡消费清单、产品订单等。附件中会隐藏恶意代码，当用户打开后恶意代码便会开始执行，释放病毒。不法黑客往往会将携带病毒的文件通过邮件批量发送给企业、高校、医院机构等单位，这些单位中的电脑中通常保存较重要的文件，一旦被恶意加密，支付赎金的可能性远远超过普通个人用户。

3.2.6 RaaS

RaaS 是 SaaS 模式的一个非法应用，网络犯罪分子开发出高度复杂的勒索软件并将其出售给想要发动攻击以换取经济利益的客户。RaaS 几乎使任何人都可以在不自己编写代码的情况下进行网络攻击。RaaS 使发动网络攻击牟利变得更加容易，这对于企业数据安全是一个巨大的威胁。

一旦网络犯罪分子破坏了一个系统并窃取了有价值的信息，他们就需要把目标对准一个买家——通常是企业——以谈判价格出售窃取到的信息。与 SaaS 应

用程序非常相似，RaaS 采用基于云的订阅模型。RaaS 开发者使用关联工作流收集受害公司支付的赎金的详细信息，然后从收到的赎金中抽取一定比例，再将剩余部分转交给软件购买者。

3.3 勒索病毒的常规攻击路径

第一步：入侵

惯用手法：RDP 爆破、SQL 弱口令爆破，网络钓鱼，恶意电子邮件（包括垃圾邮件广撒网与精准定向投放）及恶意附件投递（包括 Office 漏洞、Flash 漏洞、PDF 阅读器漏洞等），高危漏洞利用，无文件攻击等。也有部分勒索黑客会利用僵尸网络控制的肉鸡渠道分发。

第二步：扩散

勒索黑客入侵某一台主机之后，往往并不立即运行勒索病毒，而是尽可能的利用各种攻击手法在目标网络横向扩散以增加受控主机数量。勒索黑客在此阶段会通过下载各种攻击工具包，包括流行漏洞利用工具、密码提取工具、远程控制木马或后门、下载密码字典继续使用爆破入侵等等。

第三步：盗窃

攻击者会遍历已攻陷主机数据，筛选最有价值的攻击对象，窃取受控主机数据。

勒索病毒团伙在利用多种技术手段入侵目标系统后，会留置后门、安装多种远程控制软件（如 TeamView 破解版、RemoteUtilities 商业远控软件破解版、RemcosRAT、AgentTesla、SnakeKeylogger、AsyncRAT、Nanocore 等商业木马），勒索黑客会使用此类工具将失陷网络的机密数据上传到该团伙控制的服

服务器上。

第四步：勒索

下载一种或多种勒索病毒运行，瘫痪目标网络，留下勒索信件，在暗网渠道发布失陷企业数据，实施勒索。

攻击者利用 REvil 勒索软件攻击著名计算机厂商 Acer，勒索 5000 万美元，攻击者在暗网公布该公司的部分数据，截图包含一些财务报表、银行相关的文档。

3.4 勒索病毒主要攻击特征

3.4.1 针对企业用户定向攻击

勒索病毒在 2016 年爆发时，主要通过钓鱼邮件、挂马等攻击方式撒网式传播，导致普通用户深受其害。但随后黑客发现普通用户的数据价值相对更低，并不会缴纳高额赎金进行数据恢复，相反企业用户的资料数据一旦丢失，将会极大地影响公司业务的正常运转，因此企业用户往往会缴纳赎金来挽回数据。因此现在黑客基本针对企业用户定向攻击，以勒索更多的赎金。

3.4.2 以 RDP 爆破为主

通过腾讯安全御见威胁情报中心的数据统计，目前勒索攻击主要以 RDP 爆破为主（包括企业内网渗透），典型家族有 GlobeImposter 和 Crisis，也有其他家族的勒索病毒陆续加入端口爆破攻击方式。RDP 爆破成功后，黑客可以远程登录终端进行操作，这样即使终端上有安全软件的防护也会被黑客退出，攻击成功率高，因此备受黑客喜爱。

3.4.3 更多使用漏洞攻击

以往勒索病毒更多地使用钓鱼邮件、水坑攻击等方式进行传播，但随着用户

的安全教育普及，社工型的攻击成功率越来越低。因此勒索病毒现在更多地使用漏洞进行攻击，漏洞攻击往往令用户没有感知、并且成功率高。部分企业没有及时修复终端的高危漏洞，这就给了黑客可趁之机。

3.4.4 入侵企业内网后横向渗透

大多企业通过内外网隔离，来提高黑客的攻击门槛，但是一旦前置机有可利用漏洞，黑客依然可以入侵到企业内网。入侵成功之后，黑客往往会利用端口爆破、永恒之蓝漏洞等进行横向传播，来达到加密更多的文件、勒索更高额赎金的目的。

四、勒索病毒未来发展趋势

- 4.1 考虑到未来一段时间，PC 电脑上价值最高的依然为用户数据，故勒索病毒依然为用户面临的主要安全威胁之一；
- 4.2 企业用户数据价值较高，且内网环境复杂，依然是勒索病毒的重点攻击对象；
- 4.3 随着技术的普及、勒索病毒产业链的成熟，黑客加入勒索病毒的门槛越来越低，因此勒索病毒有可能变得更多样、更新更频繁；
- 4.4 目前受到的勒索病毒攻击主要是 windows 系统，但是管家也陆续发现了 MacOS、Android 等平台的勒索病毒，随着 windows 的防范措施完善，将来黑客也可能转向攻击其他平台。
- 4.5 由于勒索病毒和挖矿木马的攻击方式和传播渠道几乎完全一样，目前已有不法黑客，如 Satan 病毒团伙，同时采用勒索病毒和挖矿木马双重攻击，给用户带来更大的损失。

五、 防御方案建议

A、定期进行安全培训，日常安全管理可参考“三不三要”思路

1.不上钩：标题吸引人的未知邮件不要点开

2.不打开：不随便打开电子邮件附件

3.不点击：不随意点击电子邮件中附带网址

4.要备份：重要资料要备份

5.要确认：开启电子邮件前确认发件人可信

6.要更新：系统补丁/安全软件病毒库保持实时更新

B、全网安装部署终端安全管理软件，推荐企业用户使用腾讯零信任无边界访问控制系统(iOA)，个人用户使用腾讯电脑管家。同时，针对一些大中型企业，我们建议采用腾讯高级威胁检测系统(NTA)监测内网风险，企业管理员可以通过这些安全解决方案及时发现内网入侵风险，及时封堵弱点，修补漏洞，避免重要业务系统被勒索病毒破坏。

企业客户可通过订阅腾讯安全威胁情报产品，让全网所有安全设备同步具备和腾讯安全产品一致的威胁发现、防御和清除能力。



C、建议由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略、软件限制策略，以保证网络的动态安全。

D、建议对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促员工停止使用弱密码，或使用安全策略来强制规定密码长度和复杂性。

E、对网络资产进行核查，如果存在一些非必要开启的网络服务或端口，可以按照最小权限原则进行关闭或禁用，最大程度减少黑客入侵的攻击面。

F、企业应建设、培养专业的网络安全管理人才建设，密切关注网络安全动态，与安全厂商展开良好互动，仅仅依靠安全软件就解决网络风险是难以想像的，安全攻防需要长期的技术投入和人员投入。

G、建议对重要的网络服务进行远程访问策略配置、对管理节点进行限制，只限定允许的 IP 地址访问管理后台。数据库服务避免使用弱密码，配置最大错误登录次数，防止远程黑客进行暴力破解。

重要的关键业务系统必须做好灾备方案（备份 3、2、1 方案）


A、至少准备三份副本；

B、两种不同形式：将数据备份在两种不同的存储类型，如服务器/移动硬盘/云端/光盘/磁带等；

C、至少一份异地（脱机）备份：勒索病毒将联机的备份系统加密的事件发生的太多了。



nd. 南都传媒 **南方都市报**
办中国最好的报纸

 腾讯安全威胁情报中心