奇安信
新一代网络安全领军者

95015
网络安全服务热线

https://www.qianxin.com

2023年
中国企业勒索病毒攻击态势分析报告

THE REPORT

发布机构：

奇安信行业安全研究中心

奇安信安服团队

奇安信
新一代网络安全领军者

摘　要

- ✧ 统计显示，医疗卫生行业是勒索病毒攻击的重灾区，报案数量占到勒索病毒攻击事件报案总数的 21.4%；制造业排名第二，占比为 17.5%；生活服务紧随其后，占比为 14.6%。
- ✧ 61.7%的勒索病毒攻击事件根本无法进行溯源，13.1%的中招机构，只能进行内网或局域网内的溯源，其余 25.2%的机构能够对互联网侧的勒索病毒攻击源 IP 进行追溯。5.8%的攻击源 IP 来自于境内，17.0%的攻击源 IP 来自境外，另有 2.4%的攻击者，同时使用了境外 IP 和境内 IP 进行勒索攻击。
- ✧ 在 206 起造成重大破坏或严重损失的勒索病毒攻击典型事件中，各类政企机构共有 1485 台设备感染了勒索病毒。平均每起勒索病毒攻击事件造成 8.6 台网络设备（含虚拟机）被感染。
- ✧ 2022 年 1 月至 2023 年 3 月，综合奇安信 95015 应急响应团队处理的所有勒索攻击事件中，排名前十的事件涉及勒索病毒/家族占所有勒索攻击事件的 51.0%。其中，phobos 勒索家族排名第一，有 22.8%的勒索事件受到该勒索软件的攻击；makop 勒索病毒排名第二，占比 5.3%；mollox 排名第三占比 4.9%。
- ✧ 完成一次勒索病毒攻击的平均时长为 105.7 小时、最短时长为 3 分钟、最长时长为 529 天。其中，17.6%的攻击者在一小时内即完成了从发起攻击至完成勒索的全过程，“0.5 小时”是勒索攻击发现后的“黄金救援期”，在发现攻击者攻击后的 0.5 小时内，拦截攻击失陷的成功率极高接近 90%。
- ✧ 52.6%的攻击事件使用了暴力破解，存在违规操作或使用钓鱼邮件攻击的事件分别占比 5.2%。
- ✧ 全国发生的勒索攻击重大事件中，49.5%的勒索攻击事件明确与弱口令有关。
- ✧ 从端口暴露情况来看，42.2%的攻击事件均涉及端口暴露。其中，暴露最多的端口 TOP5 分别为：3389（19.4%）、445（12.1%）、135（5.3%）、139（4.4%）、3306（2.9%）。

关键词： 勒索、暴力破解、弱口令、漏洞、端口暴露

主要观点

- 医疗卫生、制造业、生活服务行业是国内勒索病毒攻击的重灾区，相关行业单位应当对勒索病毒风险高度重视。从规模来看，安全防护能力相对较低的中小企业，相对更容易遭到勒索病毒的攻击。

- 遭到勒索病毒攻击的政企单位，绝大多数都是网络安全建设基础极其薄弱，存在显而易见的安全建设漏洞的单位。终端没有采取任何安全防护措施、内网服务器近乎裸奔、关键漏洞长期得不到修复等情况非常普遍。没有整体安全规划、没有全局安全策略、没有有效运营手段，都是勒索病毒受害机构的典型通病。有些单位虽有安全基础设施建设，但缺少安全运维，基础设施不更新、告警不看等原因导致基础设施应有的作用未充分发挥。

- 如果仅从入侵方式和渗透手法来看，勒索病毒的攻击与其他各类传统网络攻击相比并没有多少特别的“新花招”，极少有使用 0day 漏洞或高级攻击手法的情况发生。这也意味着，不论发病时的症状多么的可怕，勒索病毒依然是一种可防、可控、可阻断的“网络传染病”。

- 绝大多数的勒索病毒攻击，在攻击早期就会暴露出比较明显的“攻击信号”。从早期攻击信号出现后的 0~30 分钟，是勒索病毒攻击应急响应的“黄金救援期”，在这段时间内，系统生存率仍在 90%以上。而 9.8 小时，约 590 分钟是一个临界时间点，超过这个时间，系统被成功投毒的概率就会大于生存概率。因此，遭受攻击的机构必须要有能力在第一时间捕获攻击者的行动，并在有限的时间内采取有效的行动，才能成功阻止最终的投毒，在勒索病毒的攻击下存活。

- 在勒索病毒攻击事件中：有 49.5%与弱口令有关；在 52.6%使用了暴力破解；而能够被成功爆破的口令，理论上讲都属于弱口令。作为系统看门人，管理员使用弱口令，就等于是将库房钥匙交给了攻击者。这也就难怪攻击者可以“大摇大摆”的“破门而入”。

- 表面上看，弱口令问题是安全意识问题。但从本质上看，弱口令的存在本身就说明系统的身份认证机制不完整或者是存在重大的缺陷。采用零信任等新型身份安全机制，可以实现即方便、又安全的用户体验。对于尚不具备部署零信任系统条件，或者是安全预算

不足的政企机构，至少也应该在传统安全机制范围内，努力避免弱口令的存在，采取技术手段阻止暴力破解。

- 受害机构普遍严重缺乏威胁溯源能力。61.7%的受害机构完全不具备溯源能力，13.1%的机构仅能实现内部溯源，这二者的总和超过七成。溯源能力的缺失，也就意味着即便勒索病毒攻击已经给机构造成了重大的损失，我们也仍然无法“对症下药”，无法找到安全隐患点，不知道该具体采取哪些改进措施。白挨了一顿打，还没有学到任何教训。

- 想要有效应对勒索病毒的攻击，就要求政企机构必须具备实战化安全运营能力，以便能够在第一时间发现关键的攻击活动特征；同时，还要具备充分的应急响应能力，包括组织保障、技术方法、安全工具等多个方面，才能做到响应及时、响应有效。有条件的单位应积极建设异地备份系统，条件不足的单位应积极建设有效的本地备份机制和数据安全保护措施。

- 端口暴露问题是政企机构的基本安全问题。统计显示，在 206 起勒索病毒典型攻击事件中，共有至少 87 起事件涉及端口暴露问题，占比 42.2%。累计暴露端口 134 个，涉及端口号 27 个。存在不必要的端口暴露也就等于是为攻击者打开了一条入侵内部网络的绿色通道。

- 建设实战化、可运营的漏洞监测与预警能力，是政企机构安全运营能力建设的一大难点。同时，机构还应建立长期持续、动态运营的供应链安全管理办法，这涉及源码及开源组件安全检测、漏洞评估、漏洞发现处置等内容。

奇安信
新一代网络安全领军者

目　　录

研究背景

勒索病毒的出现，极大的改变了网络安全的基本环境和游戏规则，成为当今世界网络空间中最大的不确定因素。特别是勒索病毒一旦中招几乎无解的攻击特点，使得越来越多的政企机构被迫放弃了“事后补救”的幻想，转而采用以“预防为主”的积极防御策略来应对勒索病毒攻击的泛滥之势。

不过，国内外研究机构以往针对勒索病毒的研究，大多集中于样本分析、团伙分析和基于少数案例的具体攻击手法的分析，缺少对勒索病毒攻击特征、攻击路径和关键防御点的大样本、系统性研究，从而使得针对勒索病毒的各类解决方案大多缺少全面的科学依据，方案的有效性、性价比等关键问题，都难以得到客观评估。

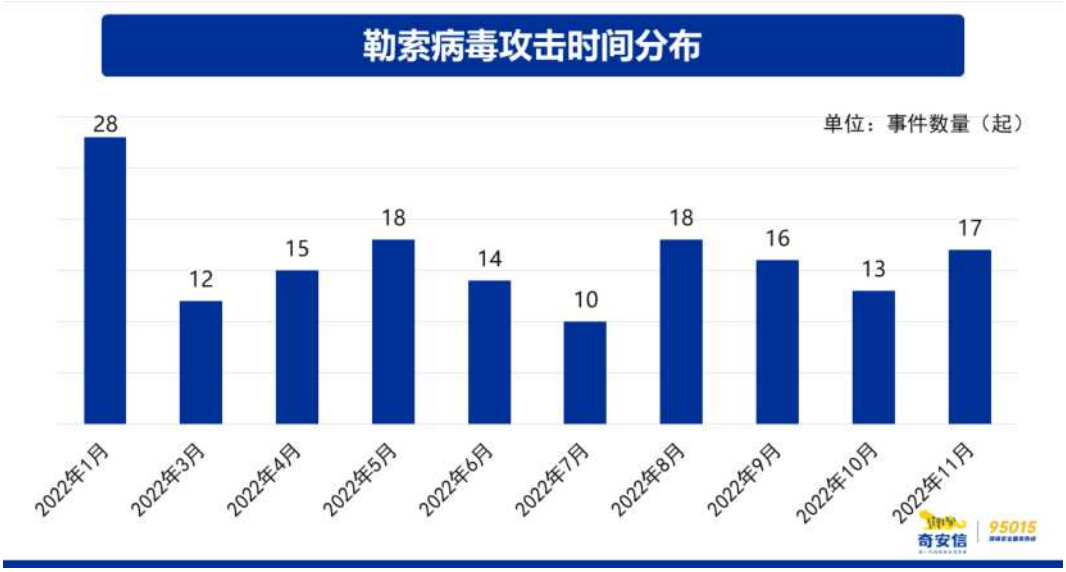
95015 网络安全应急响应服务平台，平均每年接到全国各地政企机构网络安全应急响应事件报告 1100 余起。其中，勒索病毒事件在所有恶意程序攻击事件中，占比近三成，已经连续多年排名恶意程序攻击类型的榜首。由于 95015 平台会对每一起应急响应事件做出详细的应急响应分析报告，并尽可能的进行溯源分析，从而为我们深入、全面、系统性的研究勒索病毒攻击特征提供了大量高价值的参考资料。

本次报告，从 2022 年 1 月至 2023 年 3 月的千余份网络安全应急响应分析报告中，甄选出了 206 起造成重大破坏或严重损失的勒索病毒攻击典型事件的应急响应分析报告为研究样本，分别从行业特征、攻击溯源、感染范围、病毒类型、攻击时长、攻击方式等方面展开深度分析，并首次给出了勒索病毒攻击的生存曲线。同时，报告还结合勒索病毒的攻击特征，深入分析了中招机构网络安全建设与运营方面的“通病”，为政企机构高效率的建设勒索病毒防范体系提供了重要的参考依据。

第一章　勒索病毒攻击态势综述

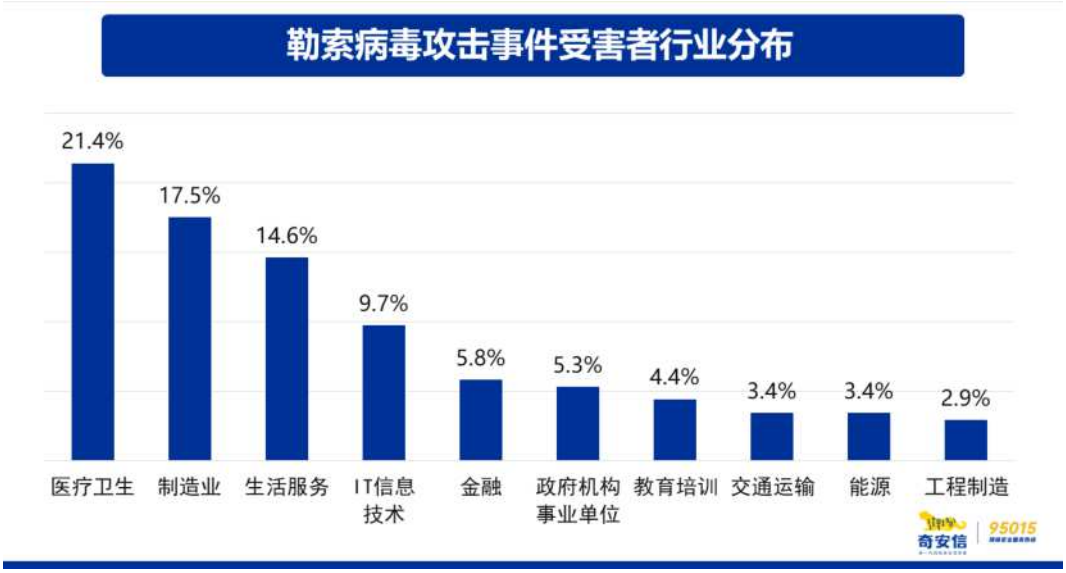
一、　月度分布

下图给出了 95015 服务平台 2022 年 1 月~2023 年 3 月接报的 206 起造成重大破坏或严重损失的典型勒索病毒攻击事件每月分布情况。其中，2022 年 1 月数量最多，为 28 起。



二、　行业分布

统计显示，医疗卫生行业是勒索病毒攻击的重灾区，报案数量占到勒索病毒攻击事件报案总数的 21.4%；制造业排名第二，占比为 17.5%；生活服务紧随其后，占比为 14.6%。



从规模来看，安全防护能力相对较低的中小企业，相对更容易遭到勒索病毒的攻击。

三、 攻击源 IP 分析

尽管攻击源 IP 的地域归属并不能代表攻击者的地域归属，但对攻击源 IP 的地域归属分析，却可以帮助我们了解攻击者最终发起攻击时的 IP 选择倾向。

然而，当我们攻击源 IP 归属地进行全面深入分析时，却十分惊讶、也十分遗憾的发现：竟有 61.7%的勒索病毒攻击事件根本无法进行溯源，甚至仅仅是在内网或局域网中进行攻击溯源都完全无法实现。这也就意味着，我们完全不知道攻击者从哪里进来，从哪里出去，访问过哪些系统、进行过哪些操作、利用过什么漏洞、是否埋下了后门。造成这种情况的原因，固然有攻击者事后主动擦除痕迹的因素，更为主要的是，中招政企机构的网络安全基础建设过于薄弱，没有采取任何针对网络攻击的监测或留痕措施，致使内部系统门户打开，几近裸奔。

除了完全无法溯源的机构之外，还有 13.1%的中招机构，只能进行内网或局域网内的溯源，而完全无法得知攻击者是通过什么互联网 IP 访问了系统。造成这种情况的主要原因，是相关机构对于来自互联网的访问信息没有进行必要日志存储，更没有对外部流量采取必要的威胁检测措施，只是对内部网络采取了一定程度流量监测与分析。此外，也有一小部分中招机构，是因为网络日志遭到了攻击者的破坏从而无法进行外部溯源。相比于完全对攻击活动进行无法溯源机构来说，能够进行内网溯源的机构，其网络安全基础能力要

略强一些，但也只能算是“聊胜于无”。

除了上述两种情况外，其余 25.2%的机构能够对互联网侧的勒索病毒攻击源 IP 进行追溯。分析显示，5.8%的攻击源 IP 来自于境内，17.0%的攻击源 IP 来自境外，另有 2.4%的攻击者，同时使用了境外 IP 和境内 IP 进行勒索攻击。

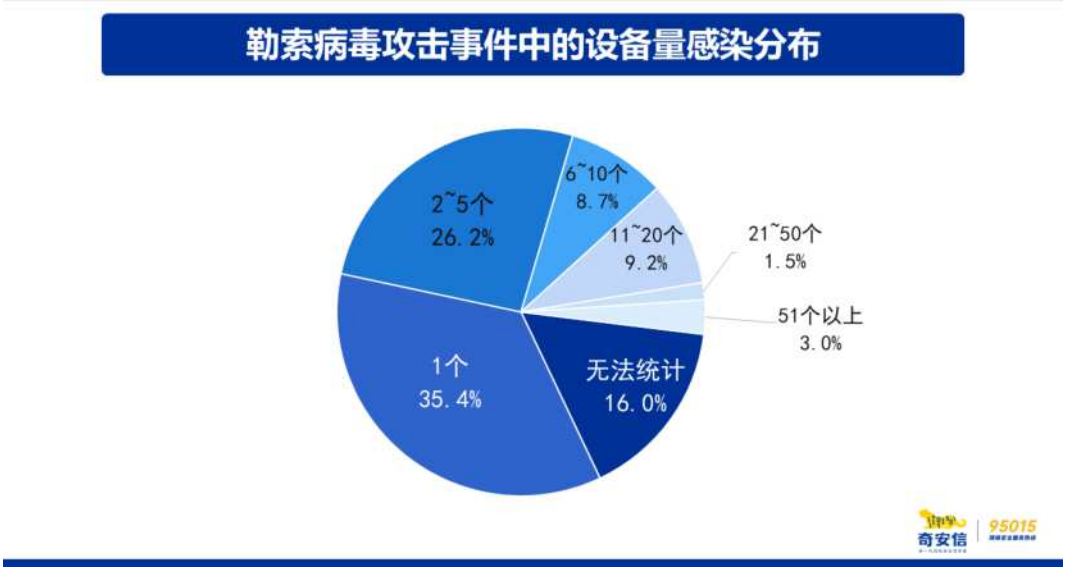
下图给出了勒索病毒攻击源 IP 的国别归属排行 TOP10。其中，无法溯源和仅能进行内网/局域网溯源的事件，不计入排行。由图可见，来自中国境内的攻击源 IP 最多，占比为 8.2%；其次是美国，占比 6.8%，排名第二；俄罗斯排名第三，占比 4.4%。注：同一攻击存在攻击者同时使用多个位于多国的 IP 发起攻击的情况，因此境外攻击占比之和会大于前文的 19.4%。

四、 感染量分析

统计显示，在 206 起造成重大破坏或严重损失的勒索病毒攻击典型事件中，共有 173 起案例的分析报告可以明确说明感染设备数。统计显示各类政企机构共有 1485 台设备感染了勒索病毒。平均每起勒索病毒攻击事件造成 8.6 台网络设备（含虚拟机）被感染。

下图给出了勒索病毒攻击事件导致的勒索病毒感染设备数量的分布。设备可能包括普通个人主机终端、工业系统终端、服务器、或虚拟机等。具体来看，35.4%的攻击事件感染/加密了 1 台设备，26.2%的勒索攻击事件感染/加密了 2~5 台设备，甚至有 3.0%的攻击事件影响设备超过 50 台。其中，某制造业企业遭到 phobos 勒索病毒攻击，通过单一跳板进

入内网攻击内网中主机超过 200 台，并投递勒索病毒。

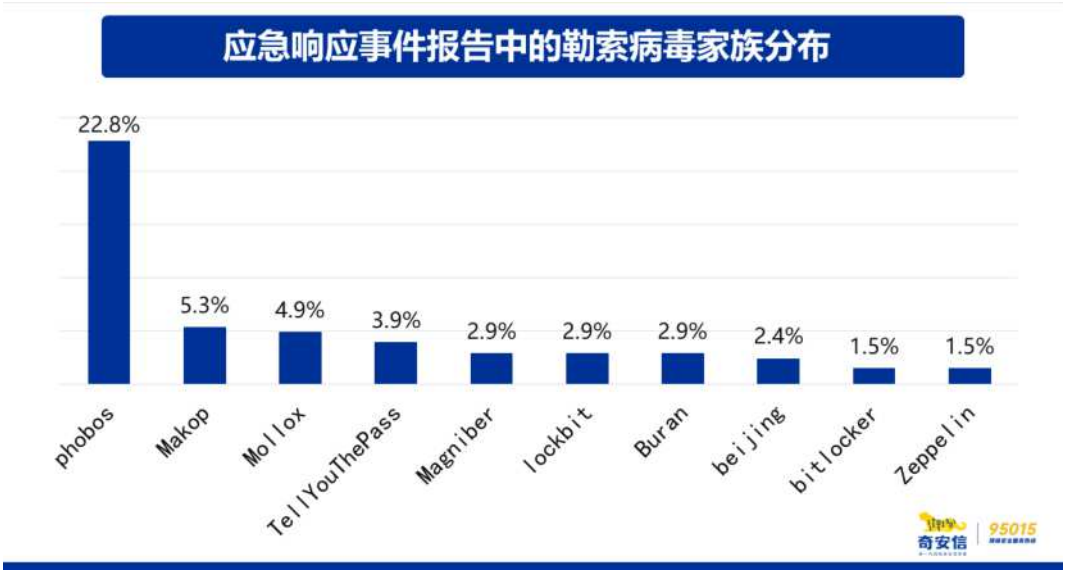


统计还显示，41%的勒索病毒攻击事件会导致虚拟机被感染，虚拟机感染量占设备感染总量的 13.2%。

第二章　勒索病毒家族分析

一、　勒索病毒家族分布

统计发现，2022 年 1 月至 2023 年 3 月，综合奇安信 95015 应急响应团队处理的所有勒索攻击事件中，排名前十的事件涉及勒索病毒/家族占所有勒索攻击事件的 51.0%。其中，phobos 勒索家族排名第一，有 22.8%的勒索事件受到该勒索软件的攻击；makop 勒索病毒排名第二，占比 5.3%；mollox 排名第三占比 4.9%，排在后面的分别为 TellYouThePass、Magniber 勒索病毒。具体分布如下图所示：



大多情况单起勒索事件受害者会被一种勒索病毒感染并加密，仅一起事件中发现某集团单位 50 余台服务器感染了 Pipikaki 家族勒索病毒与 WannaCrypt 勒索病毒程序两种病毒，但经分析发现，这是两个不同的团伙在相近的时间攻击所致。

下文整理了近一年来奇安信 95015 应急响应团队处理的勒索事件中，较频繁出现的几个勒索病毒家族，综合公开情报及内部资料，给出了基本的介绍、加密类型及经常利用的漏洞或端口等信息，内容较为精简，若想了解更详细的技术问题可联系对口销售。

二、 Phobos 勒索病毒

最早发现时间：2019 年

主要传播方式：RDP 暴力破解、钓鱼邮件

勒索加密算法：RSA+AES

加密文件后缀：无固定后缀

针对操作系统：Windows7、Windows10、Windows Server 等。

最常利用端口：3389、445

Phobos 勒索软件家族，于 2019 年初被发现，并不断更新病毒变种。其传播方式主要为 RDP 暴力破解或钓鱼邮件获取内网控制权后人工投毒。此勒索软件及变种会使用“RSA+AES”算法加密文件，暂时没有解密工具。程序运行后会关闭系统防火墙，添加注册表实现开机启动，而后将家族变种版本信息追加到加密文件中，不仅加密文档文件还会加密可执行文件，并在加密后创建两种类型的勒索信，一种为 txt 格式，另一种为 hta 格式。Phobos 勒索软件家族在全球多个行业扩散，感染面积大，变种更新频繁。

此新变种勒索信内容与以往的 Phobos 勒索软件勒索信内容有所不同，Phobos 勒索软件家族其它变种的勒索信中会告知受害者如何购买比特币支付赎金，但此变种的勒索信中并未体现，只表达了受害者的文件已被加密，并告知联系邮箱地址等信息。

三、 Makop 勒索病毒

最早发现时间：2020 年

主要传播方式：RDP、邮件、第三方软件下载源、木马

勒索加密算法：RSA+AES512

加密文件后缀：.makop

针对操作系统：Windows

Makop 勒索病毒是较新的恶意软件，发现于 2020 年，目前正在流行。Makop 勒索病毒

传播方式包括 RDP 传播、利用邮件引导受害者下载第三方软件、木马以及虚假的软件更新程序和“破解”程序等。Makop 勒索软件使用的是 RSA+AES256 密钥在运行时于内存中解密字符串，暂时没有解密工具。该勒索病毒指示用户/受害者通过即时消息协议 Tox 联系恶意软件作者。

该恶意软件会加密每个文件夹中的所有文件，并为每个文件添加扩展名 .makop。勒索者会在暴露的链接上找到具有弱口令的管理员帐户，并使用它们来渗透和传播 Makop 勒索病毒加密计算机。

四、 Mallox 勒索病毒

最早发现时间：2020 年

主要传播方式：漏洞攻击、钓鱼邮件、网站挂马、恶意软件、U 盘等

勒索加密算法：AES+RSA

加密文件后缀：.mallox

针对操作系统：Windows

最常利用端口：139、445、3389、135、1433

Mallox 勒索病毒于 2020 年被发现和披露。主要针对企业的 Web 应用和数据库服务器进行攻击，其中包括 Spring Boot、Weblogic、OA、财务软件等。该勒索软件主要使用 AES+RSA 加密算法，对设备攻击成功后，拿下目标设备的权限，还会在内网中横向移动，获取更多的设备权限，从而达到对其设备的加密程序执行目的。它通过获取数据库口令后，远程下发勒索病毒，并在被攻击设备的 Web 应用中大量植入 WebShell，然后使文件名中包含“kk”的特征字符。入侵成功后会在目标机器内尝试释放黑客工具，控制机器并创建账户，并尝试远程登录目标机器，获取更多内网中的设备权限，从而部署勒索病毒。

除此之外 Mallox 勒索病毒还会通过网站挂马传播、恶意软件传播、共享文件夹入侵、邮件传播、漏洞入侵、U 盘等形式传播，尤其是下载不可靠来源文件，它们会在其中会隐藏恶意软件，诱骗用户使用虚假安装程序，更新程序等方式从而被感染，因此日常工作运营中要注意细节，提前做好预防工作。

五、 TellYouThePass 勒索病毒

最早发现时间：2019 年

主要传播方式：漏洞利用、RDP 爆破、钓鱼邮件、僵尸网络等

勒索加密算法：RSA+AES

加密文件后缀：.locked

针对操作系统：Windows、Linux

最常利用端口：3389、445、139、135、5900

TellYouThePass 勒索病毒最早发现于 2019 年 3 月，至今一直在活跃。加密方式采用 AES+RSA，在没有私钥的情况下无法解密。该家族具有多种传播方式，包括 RDP 爆破、钓鱼邮件、僵尸网络、漏洞利用等。加密文件后缀通常为.locked。

在近期捕获的变种样本中，TellYouThePass 勒索病毒利用 log4j2 漏洞进行传播，并更新了 Linux 平台版本。病毒利用压缩工具打包的 exe 执行程序，将 ms16-032 内核提权利用模块、永恒之蓝内网扩散模块集成到勒索攻击包中，以实现内网蠕虫式病毒传播。黑客通过漏洞侵入（OA 业务漏洞，向日葵 RCE 漏洞），调用恶意文件下载执行勒索病毒。

TellYouThePass 勒索病毒攻击者的一系列工具中，包含永恒之蓝漏洞高危漏洞 MS17-010、log4j2 漏洞、CVE-2020-0796 等的攻击利用。

六、 Magniber 勒索病毒

最早发现时间：2017 年

主要传播方式：漏洞利用、文件更新

勒索加密算法：RSA+AES

加密文件后缀：.APPX、.msi、.js 等随机后缀

针对操作系统：Windows10、Windows11、Windows Server 等。

最常利用端口：445

Magniber 勒索病毒是一款臭名昭著的勒索软件，在 2017 年首次被发现,在韩国和亚太地区造成了较大影响。该病毒使用 RSA+AES 加密算法，最新的传播手法是伪装成 Windows 更新的 MSI 文件诱使用户下载，暂时无法解密。一旦感染 Magniber，磁盘上几乎所有格式的文件都会被加密，有极大外泄风险。与常见的 Hive 及 LockBit 等勒索家族相比，Magniber 也会针对个人进行勒索。此勒索病毒会在各种类型网站上大范围投放，企业、学校和个人用户需要特别小心。

Magniber 勒索病毒常利用的漏洞：CVE-2021-40444、CVE-2021-34527

七、 BeijingCrypt 勒索病毒

最早发现时间：2020 年

主要传播方式：远程爆破桌面

加密文件后缀：.360、.halo、.beijing 等

针对操作系统：Windows 服务器

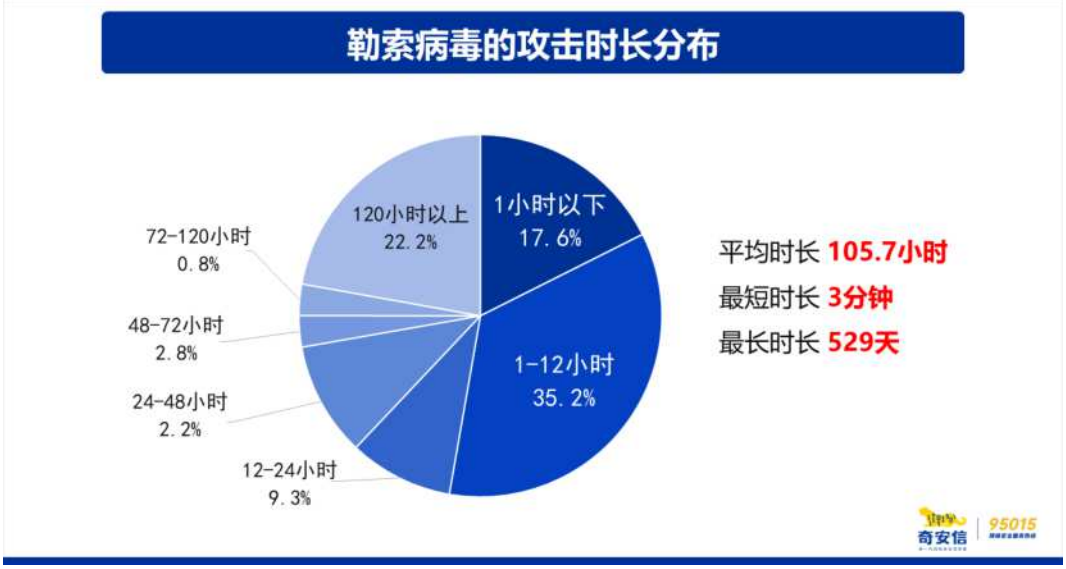
最常利用端口：3389、445

Beijing 勒索病毒（也为 BeijingCrypt 勒索病毒家族）最早发现于 2020 年。BeijingCrypt 后缀多为.360、halo 或.Beijing。该勒索病毒能够感染任何 Windows 计算机。它会在未经许可的情况下静默进入计算机，并隐藏在计算机中。成功安装和运行后，它将加密系统中存储的所有文件。成功加密后，它将自己的扩展名添加到所有文件的末尾。然后，.Beijing 勒索病毒将在计算机上留下赎金记录，以提供有关解锁数据的说明。赎金中包含一封威胁信，说您的所有个人信息均已加密，并且只能通过私钥解密，并要求您支付赎金以交换解密代码。不过，有很多感染者反馈，Beijing 勒索病毒的攻击者通常无意帮助受害者解密文件，而仅是为了勒索钱财。

第三章　攻击时长与生存曲线

在本次报告分析的 206 起勒索病毒攻击典型案例中，共有 108 起案例的分析报告中，能够找到明确的攻击“起止时间”记录，即最早的攻击时间记录和勒索病毒完成加密的时间记录，从而可以帮助我们分析勒索病毒攻击者的攻击时长。而其余 98 起案例，由于相关政企机构没有采取足够的安全防护措施和日志保存手段，导致事后完全无法进行有效的攻击溯源，无法回溯完整的攻击过程和攻击起止时间。

对有明确记录攻击起止时间的 108 起勒索病毒攻击事件的分析显示：完成一次勒索病毒攻击的平均时长为 105.7 小时、最短时长为 3 分钟、最长时长为 529 天。其中，17.6%的勒索病毒攻击事件是在 1 小时内完成的，超过半数是在 12 小时内完成的，24 小时内完成的攻击事件超过六成。具体攻击时长分布如下图所示：



特别值得反思的是，竟然有 22.2%的勒索病毒攻击事件，攻击时长在 120 小时以上。也就是说，相关单位在完全有能力发现攻击现象的情况下，仍然在至少整整 5 天以上的时间里，任由攻击者对自己的系统进行肆无忌惮的攻击，而没有采取任何有效的响应措施，足见其防御手段有名无实，严重缺乏基本的网络安全运营能力与安全事件处置能力。

勒索病毒的攻击是一个过程，而不是一个瞬时动作。有效的安全监测和实战化的安全运营，是完全有能力及时发现和阻止勒索病毒攻击的。为了能够更加精确的分析防范勒索病毒攻击所需要的响应速度，本报告以“攻击时长”数据为基础，绘制了勒索病毒攻击的

“生存曲线”，详见下图。在生存曲线图中，横坐标为“生存时间”，表示从攻击者发起攻击开始计算，受害机构系统能够生存的时间长度（即尚未被加密的时间长度）；而纵坐标为“系统生存率”，即表示到指定的生存时间为止，攻击者尚未完成勒索病毒的加密操作，相关机构的系统仍然处于“安全”或“存活”状态的概率。

统计显示，0~30 分钟是勒索病毒攻击应急响应的“黄金救援期”，因为到 30 分钟时，系统生存率仍在 90%以上。即如果系统运营者在发现诸如爆破、远程登录或漏洞利用等攻击现象后，第一时间采取有效的防御措施，那么到 30 分钟时，系统尚未被攻击者投毒，即系统仍然存活的概率为 90%。

而到了 5.5 小时，即 330 分钟时，系统存活率就已经下降到了 60%；而 9.8 小时，约 590 分钟是一个临界点，此时的系统存活率为 50%。过了这个临界时间点，系统被成功投毒的概率就会大于生存概率。

第四章　勒索病毒的攻击手法

勒索病毒攻击者究竟使用了哪些手段对系统进行渗透和入侵，是本次研究报告的重点关注，也是帮助政企单位防范勒索病毒攻击的重要参考依据。

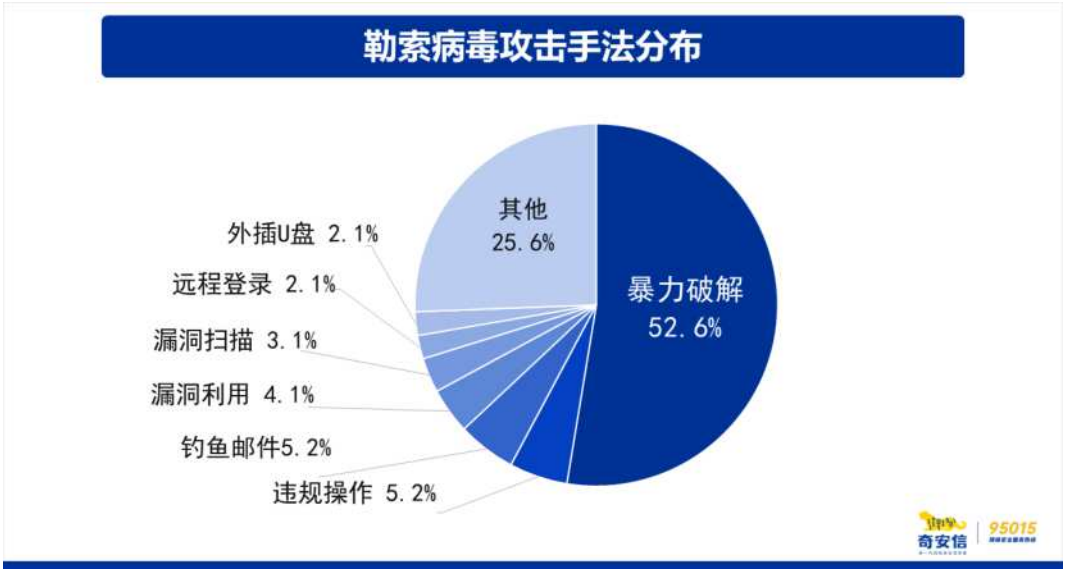
分析发现，绝大多数的勒索病毒攻击，在攻击早期就会暴露出比较明显的“攻击信号”，如：弱口令暴力破解、非法外联、远程登录、漏洞扫描等。而且这些“攻击信号”通常都没有经过特别高级的伪装，很多安全厂商都有比较成熟的安全产品或解决方案，可以实时监控相关攻击活动，及时发现并产生告警。极少有使用 0day 漏洞或高级攻击手法的情况发生。

客观的说，如果仅从入侵方式和渗透手法来看，勒索病毒的攻击与其他各类传统网络攻击相比并没有多少特别的“新花招”。这也意味着，不论发病时的症状多么的可怕，勒索病毒依然是一种可防、可控、可阻断的“网络传染病”。

本章将针对勒索病毒的攻击手法进行详细的介绍与举例。

一、　攻击手法综述

在本次报告分析的 206 起典型案例中，共有 97 起案例能够明确确认攻击者所使用的攻击手法。其中，52.6%的攻击事件使用了暴力破解，存在违规操作或使用钓鱼邮件攻击的事件分别占比 5.2%。此外，漏洞利用、漏洞扫描、远程登录和外插 U 盘，也都是比较常见的攻击方式。攻击手法的具体分布如下图。

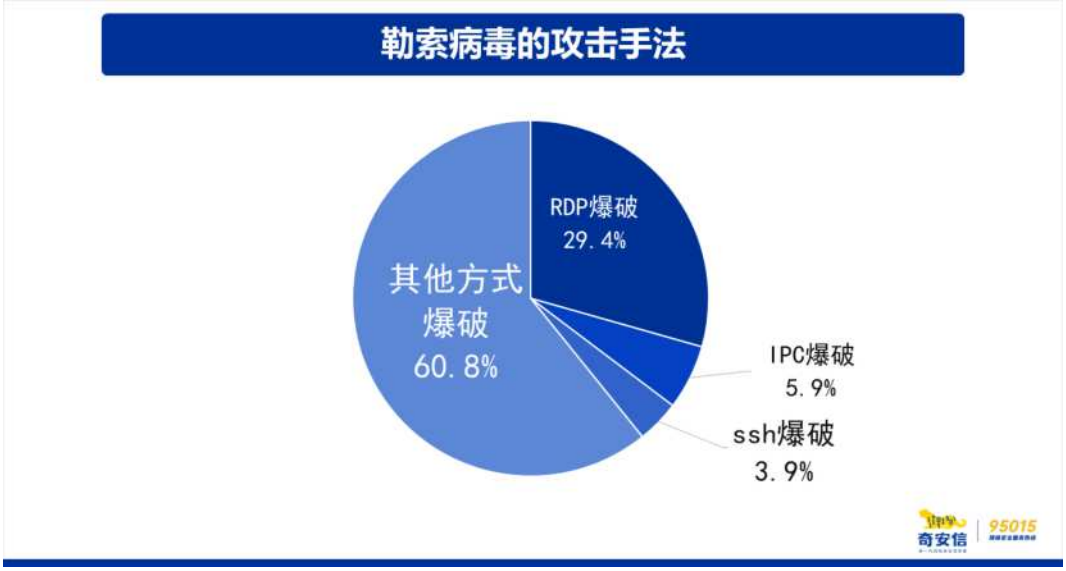


下面针对常见的勒索病毒攻击手法进行进一步分析。

二、 暴力破解与弱口令

尽管并非所有的暴力破解都取得了成功，但暴力破解确实是勒索病毒攻击者最爱使用的攻击方法，也是勒索病毒攻击可能发生的一个重要信号。

对暴力破解手法的进一步分析显示，被使用最多的爆破手法是 RDP 爆破，在所有勒索病毒攻击者发起的爆破攻击事件中，占比为 29.4%。另有 5.9%的勒索病毒攻击者选择 IPC 爆破，3.9%选择 SSH 爆破。而其他各类形式的弱口令爆破占比约为 60.8%。



RDP 爆破：利用“远程桌面登录协议”登录到受害终端/服务器上。要实现登录，大多必须知道被攻击终端的登录密码，所以常规方式是利用 RDP 协议来暴力破解远程终端的密码。

IPC 爆破：利用“共享文件服务”获取目标的文件管理权限，上传生成的木马后，建立任务实现横向渗透。

SSH 爆破：利用“安全外壳协议”的安全通道传输命令行界面和远程命令。以便用来直接登录系统，控制服务器所有权限。

从普遍意义上讲，凡是能够被爆破的口令都可以被认为是弱口令，或者至少这些口令是攻击者的口令库中已经存在的口令。在对 206 起典型勒索病毒攻击事件的分析中，我们发