奇安信

BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

95015
网络安全服务热线

https://www.qianxin.com

2021
网络安全应急响应分析报告

THE REPORT

发布机构：
奇安信安服团队

主要观点

- 2021 年，奇安信集团安服团队共接到应急服务需求 1097 起。政府部门、医疗卫生行业和事业单位的业务专网是 2021 年网络安全应急响应事件的高发区。
- 2021 年，政企机构通过安全运营巡检发现攻击事件占比为 18.0%。这说明，国内仅有不到五分之一的政企机构具备在重大事件发生之前及时阻止的能力。有 37.7%的机构是在被勒索后才寻求应急响应，但此时往往已对机构造成了一定的影响和重大的损失，日常安全运营建设水平仍然需政企机构持续提高。
- 2021 年，攻击者攻击目标仍以业务专网，服务器为主，然办公终端问题也不容小觑。与去年相比，服务器受感染台数较去年增加 20987 台，办公终端受感染台数较去年增加 8217 台。受影响服务器、终端数量的明显增加，预示着不仅是服务器安全问题，日益凸显的终端安全问题也需要引起我们的关注。
- 2021 年应急响应安全事件中，木马病毒攻击仍然是大中型政企机构服务器、数据库失陷的重要原因，除常见的勒索病毒攻击外，下半年出现的“Magniber 勒索病毒”以及“Apache Log4j2 漏洞”也成为大中型政企机构业务中断和数据泄露的重要原因。这也就意味着，政企机构应在日常运营建设中增加对外部事件，情报的监测能力，一旦发现威胁事件，应立即进行自查修复，保障业务的正常运营，将经济损失最低化。
- 2021 年，钓鱼邮件仍然是攻击者热衷利用手段之一，员工安全意识培养仍需政企机构关注并提升。员工为方便工作，使用高危端口外连公网、弱口令等导致勒索病毒蔓延、数据泄露甚至服务器失陷事件。可见，员工安全意识亟待提升。

摘　　要

- ✧ 2021 年全年奇安信集团安服团队共参与和处置了全国范围内 1097 起网络安全应急响应事件。
- ✧ 2021 年全年应急响应处置事件行业 TOP3 分别为：政府部门行业（243 起）、医疗卫生行业（112 起）以及事业单位（108 起），事件处置数分别占应急处置所有行业的 22.2%、10.2%、9.8%。
- ✧ 2021 年全年奇安信安服团队参与处置的所有大中型政企机构的网络安全应急响应事件中，由行业单位自行发现的安全攻击事件占 95.3%，其中有 37.7%的政企机构是在遭受勒索攻击后才发现系统被攻击；而另有 4.7%的安全攻击事件则是由监管机构及第三方平台通报得知。
- ✧ 2021 年全年应急响应事件的影响范围主要集中在业务专网，占比 66.7%；办公网占比 33.3%。
- ✧ 2021 年全年应急响应事件中，攻击者对系统的攻击所产生的影响主要表现为生产效率低下、数据丢失、数据篡改。
- ✧ 2021 年全年应急响应事件中，黑产活动、敲诈勒索仍然是攻击者攻击大中型政企机构的主要原因。
- ✧ 2021 年全年大中型政企机构安全事件攻击类型，排名前三的类型分别是：恶意程序，占比 44.7%；漏洞利用，占比 30.6%；网络监听攻击，占比 4.4%。
- ✧ 2021 年全年应急响应事件中，弱口令、永恒之蓝漏洞仍是大中型政企机构被攻陷的重要原因。

该报告所有分析数据来源于奇安信安服全年的 1097 次应急响应数据整理，可能存在一定的局限性，报告结论和观点仅供用户参考。

关键词：应急响应、安全服务、弱口令、敲诈、勒索病毒、漏洞利用

目　　录

第一章　2021 年全年应急

2021 年 1-12 月，奇安信集团安服团队共参与和处置了全国范围内 1097 起网络安全应急响应事件，第一时间协助政企机构处理安全事故，确保了政企机构门户网站、数据库和重要业务系统的持续安全稳定运行。

2021 年应急响应服务月度统计情况具体如下：

2021 年，奇安信安服共处置应急响应事件 1097 起，投入工时为 7932.4 小时，折合 991.6 人天。其中，2021 年 4 月，因全国多地举行网络安全实战攻防演习活动，应急响应处理量大幅增加。

从上述数据可以看出，2021 年前三季度（除 4 月）大中型政企机构应急数量趋于平稳，第四季度应急数量基本呈逐月递增趋势。通过对大中型政企机构发生网络安全事件类型进行分析，第四季度全国范围内出现“Magniber 勒索病毒”事件和“Apache Log4j2 漏洞利用”事件，导致第四季度应急需求增多。

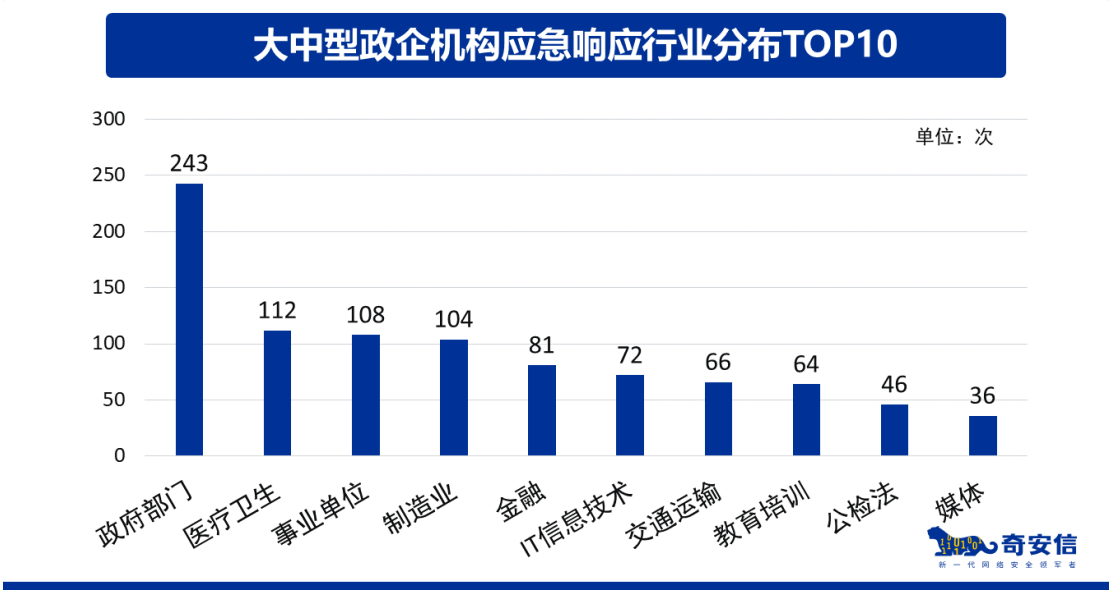
第二章　应急响应事件受害者分析

为进一步提高大中型政企机构对突发安全事件的认识和处置能力，增强政企机构安全防护意识，对 2021 年处置的所有应急响应事件从被攻击角度、受害者行业分布、攻击事件发现方式、影响范围以及攻击行为造成的影响几方面进行统计分析，呈现全年政企机构内部网络安全现状。

一、　行业现状分析

2021 年应急响应处置事件排名靠前的行业 TOP3 分别为，政府部门（243 起）、医疗卫生行业（112 起）、事业单位（108 起），事件处置数分别占 2021 年应急处置事件的 22.2%、10.2%、9.8%。

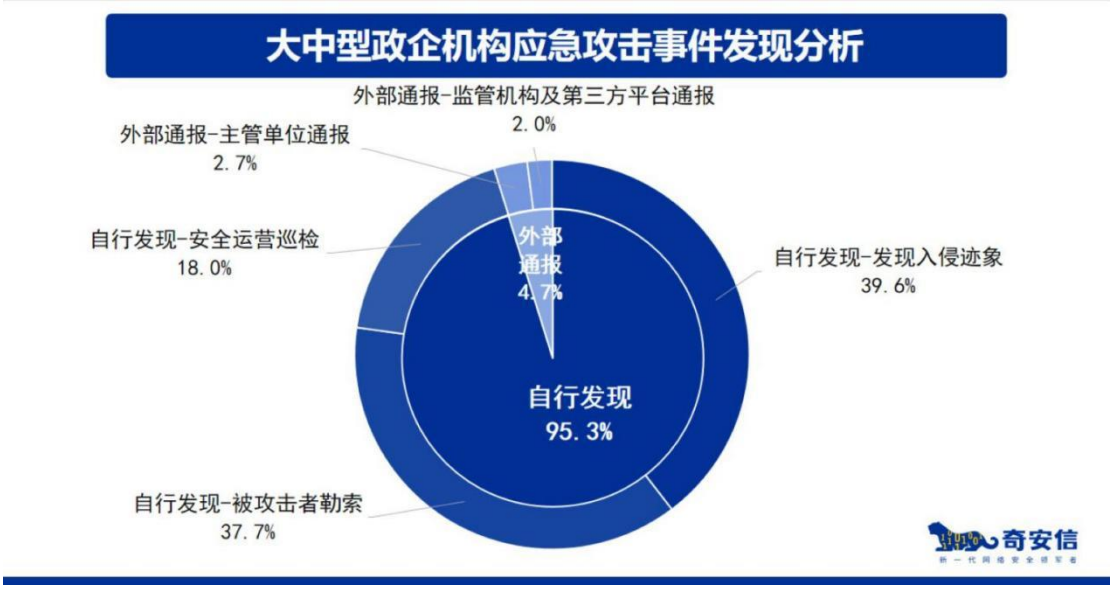
大中型政企机构应急响应行业分布 TOP10 详见下图：



从行业排名可知，2021 年攻击者的攻击对象主要分布于政府机构、医疗卫生行业和事业单位。

二、　事件发现分析

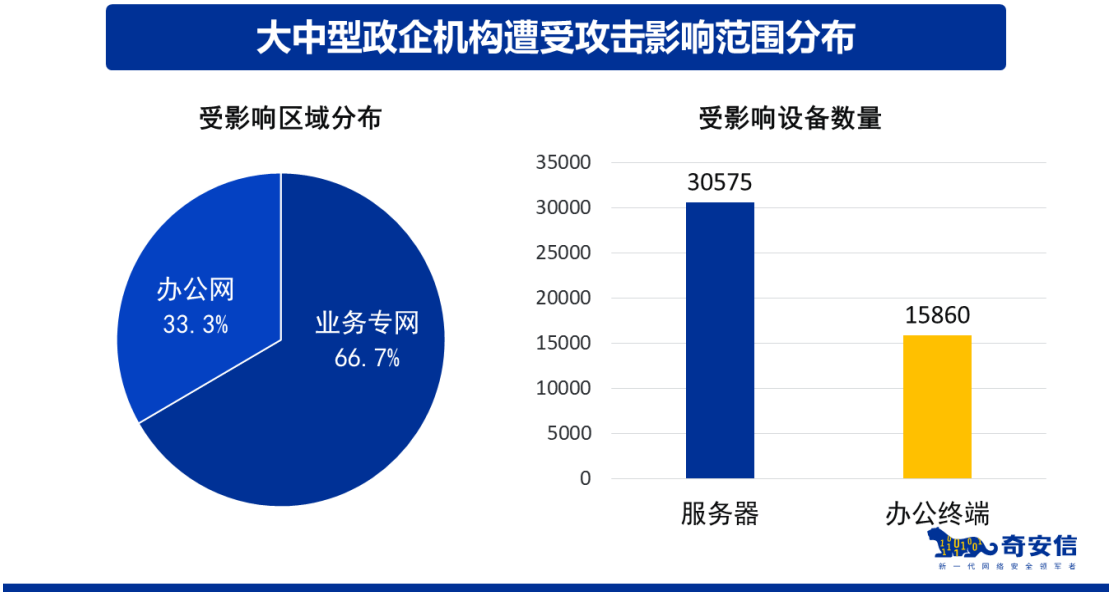
2021 年奇安信安服团队参与处置的所有政企机构网络安全应急响应事件中，由行业单位自行发现的攻击事件占 95.3%，其中发现入侵迹象的事件占比 39.6%，被攻击者勒索后发现的攻击占 37.7%，安全运营巡检发现的事件占比 18.0%。另有 4.7%的攻击事件政企机构是在得到了监管机构及第三方平台的通报后，才得知自己已被攻击。



三、 影响范围分析

2021 年应急响应事件的影响范围主要集中在业务专网，占比 66.7%；其次为办公网，占比 33.3%。根据受影响区域分布对受影响设备数量进行了统计，2021 年失陷的设备中，30575 台服务器受到影响，15860 台办公终端被攻陷。与去年相比，受影响服务器数量增加 20987 台，受影响终端数量增加 8217 台。2021 年大中型政企机构遭受攻击影响范围如下图所示。

本文中办公网指企业员工使用的台式机/笔记本电脑、打印机等设备，而业务专网泛指机构整体运行与对外支撑所需要的各种网络系统。



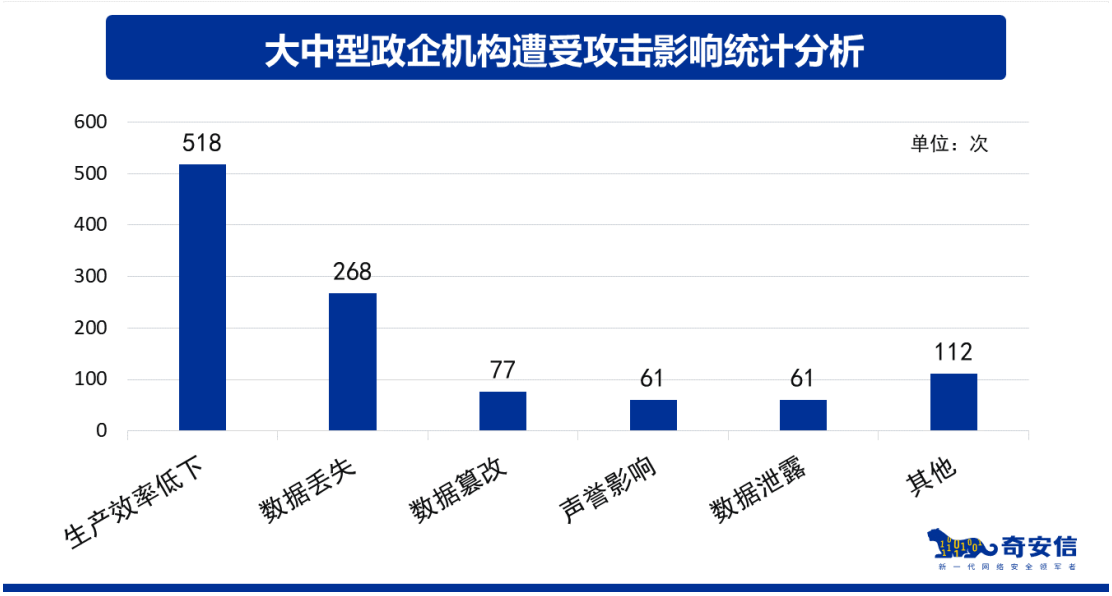
从影响范围和受影响设备数量可以看出，大中型政企机构的业务专网、服务器为攻击者攻击的主要目标。

大中型政企机构在对业务专网的安全防护建设的同时，还应提高内部人员安全防范

意识，加强对内网中办公终端、重要服务器的安全防护保障和数据安全管理。

四、 攻击影响分析

2021 年，从大中型政企机构遭受攻击产生的影响来看，攻击者对系统的攻击所产生的影响主要表现为生产效率降低、数据丢失、数据篡改等。下图为大中型政企机构遭受攻击后的影响分布。



在上述数据中，有 518 起应急响应事件导致生产效率低下，占比 47.2%，攻击者主要通过挖矿、蠕虫、木马等攻击手段使服务器 CPU 占用率异常高，造成生产效率降低。

有 268 起应急响应事件导致数据丢失，占比 24.4%，攻击者通过对大中型政企机构重要服务器及数据库进行攻击，导致数据被破坏或丢失。

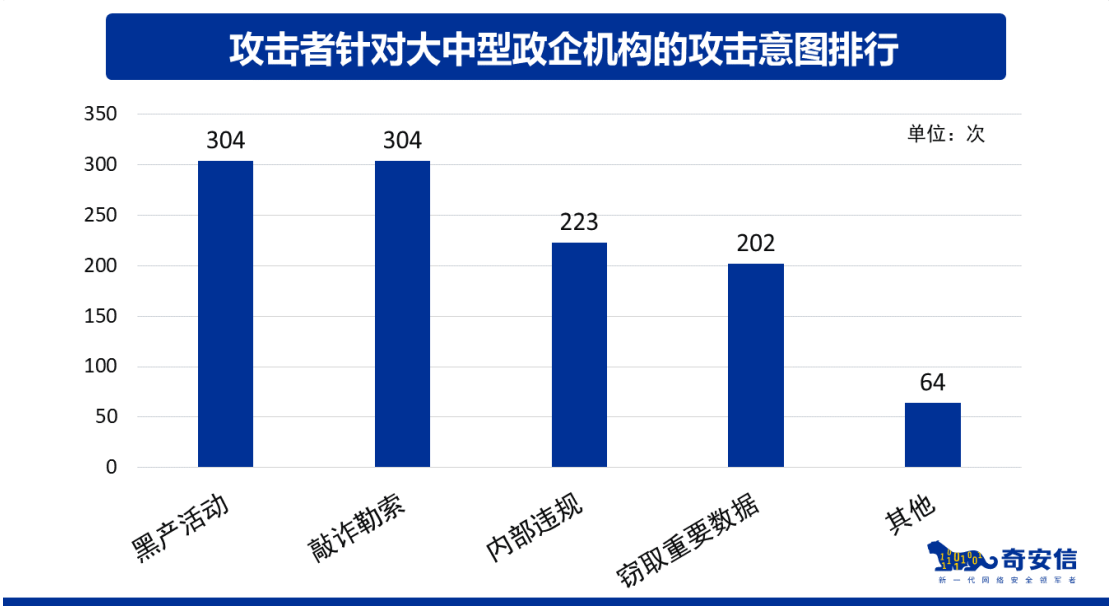
有 77 起应急响应事件导致数据篡改，占比 7.0%，攻击者在非法读取数据后，对数据进行篡改，损坏数据可读性，使用户无法获得真实信息。同时，声誉影响和数据泄露等也是政企机构被攻击后产生的结果，同样会造成非常严重的后果。

第三章　应急响应事件攻击者分析

应急响应事件攻击者分析以 2021 年大中型政企机构所有应急数据为支撑，从攻击者角度对攻击者攻击意图、攻击类型、攻击者常用恶意程序以及常见漏洞利用方式进行分析，为各政企机构建立安全防护体系、制定应急响应处置方案提供参考依据。

一、　攻击意图分析

在 2021 年的应急响应事件中，攻击者攻击意图主要为黑产活动、敲诈勒索、内部违规和窃取重要数据操作。



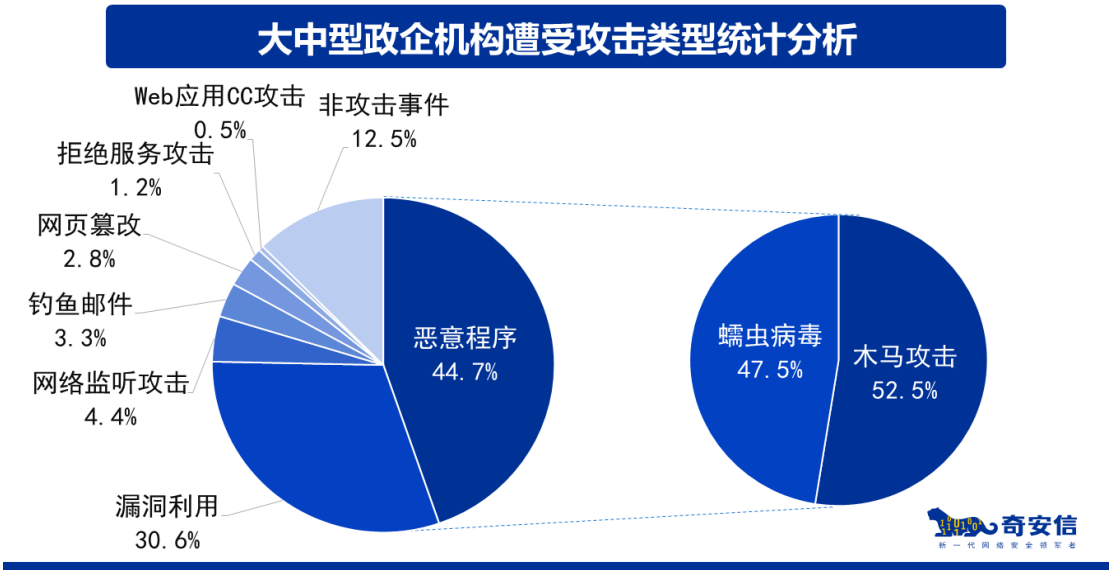
在 2021 年应急响应事件中，304 起事件的攻击原因为黑产活动，占比 27.7%，攻击者通过黑词黑链、钓鱼页面、挖矿程序等攻击手段开展黑产活动牟取暴利。

304 起事件的攻击原因为敲诈勒索，占比 27.7%，攻击者利用勒索病毒感染政府机构、大中型企业终端、服务器，对其实施敲诈勒索。对于大部分攻击者而言，其进行攻击的主要原因是为获取暴利，获取自身利益。

在 223 起内部违规事件中，内部人员为了方便工作或出于其他原因将内部业务端口映射至外网的违规操作需要引起大中型企业的重视。

二、　攻击类型分析

通过对 2021 年大中型政企机构安全事件攻击类型进行分析，排名前三的类型分别是：恶意程序占比 44.7%；漏洞利用占比 30.6%；网络监听攻击占比 4.4%。在恶意程序中，木马攻击（非蠕虫病毒）占比 52.5%，蠕虫病毒攻击占比 47.5%。



蠕虫病毒和木马，由于传播速度快、感染性强等特征成为最受攻击者青睐的攻击手段，攻击者利用病毒、木马对办公系统进行攻击，通常会产生大范围感染，造成系统不可用、数据损坏或丢失等现象；利用如 11 月出现的“Magniber 勒索病毒”对服务器和系统进行攻击，导致系统不可用，从而谋取利益。

漏洞利用则是攻击者利用政企机构网络安全建设不完善的弊端，使用常见系统漏洞、Web 漏洞等，例如 21 年 12 月发现的“Apache Log4j2 漏洞”，对服务器进行的破坏性攻击，通常会导致重要数据丢失、泄露、内部投毒、敲诈勒索等严重后果。

除此之外，网络监听攻击、钓鱼邮件、网页篡改等也是较为常见的攻击类型。如 21 年 12 月份发现的 emote 木马钓鱼邮件，一旦中招，对政企机构产生的影响是不小的。因此，大中型政企机构应做好员工安全意识培训工作，定期内部巡检，及时发现威胁并有效遏制。

三、 恶意程序分析

在 2021 年，大中型政企机构遭受攻击恶意程序类型，占比较多的木马病毒分别为勒索病毒总占比 28.8%，挖矿木马占比 18.4%，以及一般木马占比 10.8%。

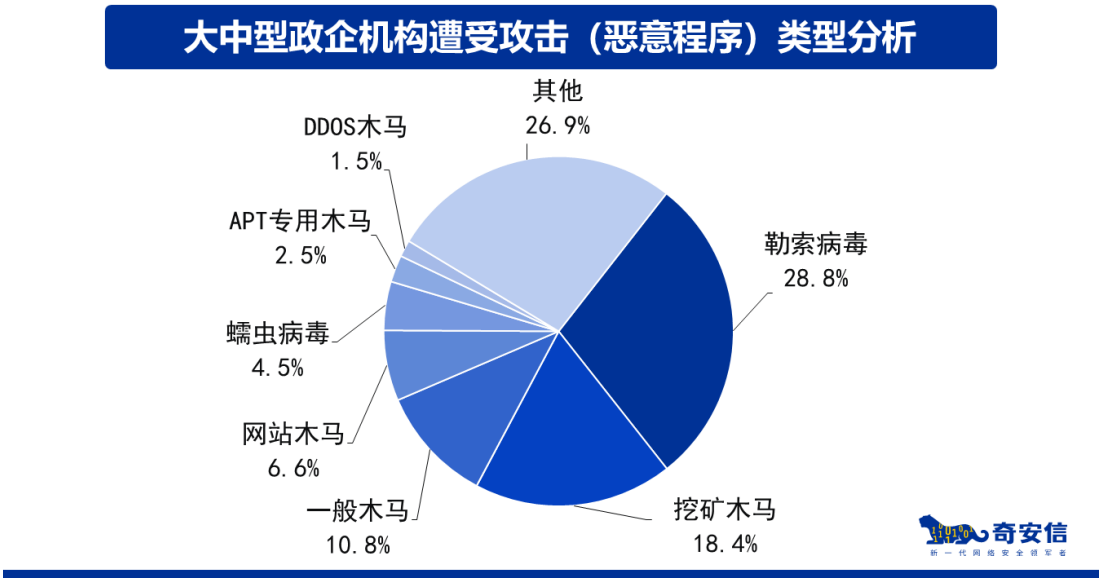


表 1 遭受攻击勒索软件类型 TOP10

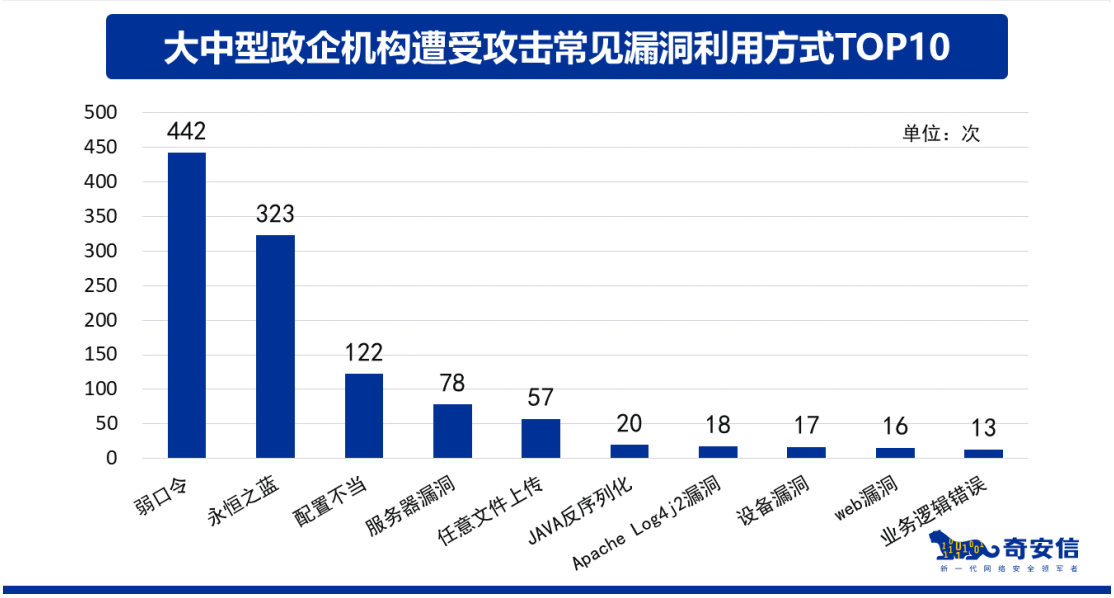
勒索软件名称	应急次数
Phobos 勒索软件	62
Wannacry 勒索软件	29
LockBit 勒索软件	18
Buran 勒索软件	17
GLobeImposter 勒索软件	16
Sodinokibi 勒索软件	12
Magniber 勒索软件	10
Makop ransomware 勒索软件	5
YourData 勒索软件	5
Crysis 勒索软件	5

2021 年最常见的勒索病毒是 Phobos 勒索病毒、Wannacry 勒索病毒、LockBit 勒索病毒、Buran 勒索病毒以及下半年新出现的“Magniber 勒索病毒”。大中型政企机构应更清楚地认识到木马病毒对我们的服务器、数据库所造成的严重损害，加强内部网络安全建设，针对多变种勒索病毒、挖矿木马以及随时可能出现的新型病毒制定完善的应急方案和安全防护措施，将应急响应常态化。

四、 漏洞利用分析

在 2021 年应急响应事件攻击类型中，对漏洞利用部分进行统计分析，发现弱口令、永恒之蓝漏洞是大中型政企机构被攻陷的重要原因；其次，服务器配置不当、服务器漏

洞也经常作为攻击者利用的方式（其中，在单起网络安全事件中，存在多个弱点的情况）。



弱口令、永恒之蓝漏洞需要引起政企机构关注，全面的安全管理策略、内部漏洞检测和日常修复动作不容忽视。除弱口令、永恒之蓝漏洞、服务器配置不当以及服务器漏洞外，21 年下半年发现的“Apache Log4j2 漏洞”对全国政企机构的影响也是非常大的，攻击者通过利用这一漏洞入侵系统，传播病毒，获取重要数据以达到敲诈勒索、牟取暴利等意图。

政企机构应加大内部巡检力度，定期对设备、终端进行漏洞扫描、修复。定期更换服务器、终端登录密码，加大密码复杂度。

第四章　应急响应典型案例分析

2021 年奇安信安全服务团队共接到全国各地应急求助 1097 起，涉及全国 33 个省（自治区、直辖市），近 30 个行业，包括医疗卫生、大中型政企机构、事业单位等。发生的安全事件包括各种变种勒索病毒、挖矿木马、漏洞利用等不同事件类型，均不同程度地给大中型政企机构带来经济损失和恶性的社会影响。下面介绍 10 起 2021 年典型的网络安全事件。

一、 制造业某客户遭遇恶意邮件传播应急事件处置

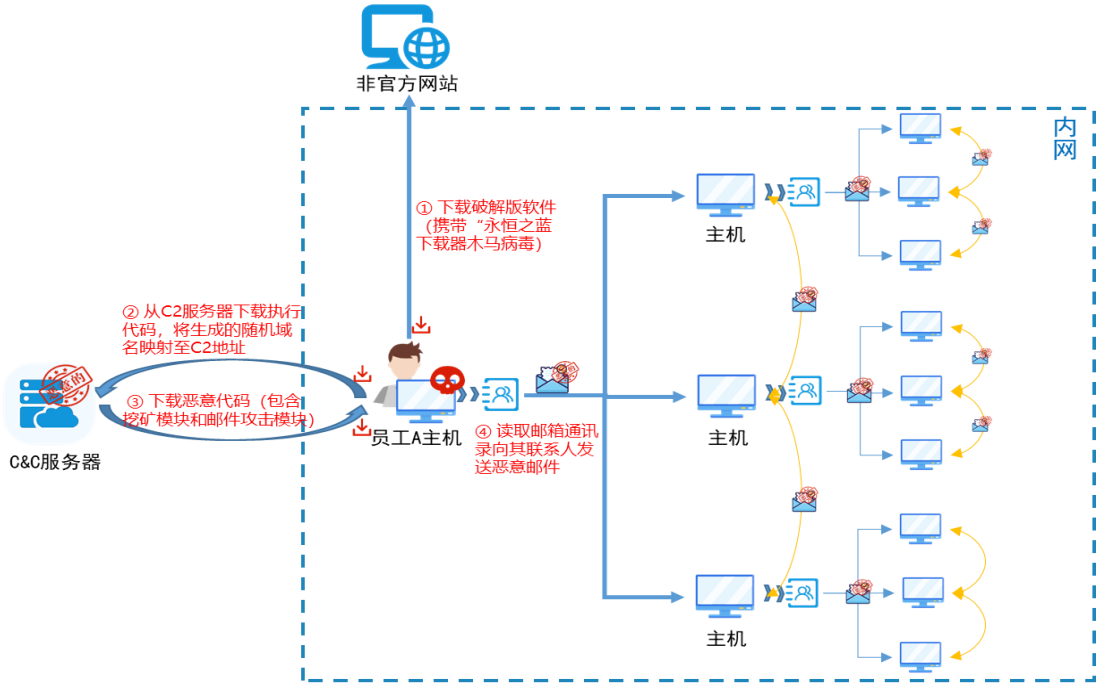
（一） 事件概述

2021 年 3 月，安服应急响应团队接到制造业某企业应急响应请求，其内网中多个终端出现自动发送恶意邮件行为，希望对该事件进行分析排查处理。

应急人员抵达现场后对邮件样本进行分析，判断该病毒为“永恒之蓝下载器木马”家族的最新变种。分析邮件日志发现，第一封恶意邮件于事发当天 15:32 由员工 A 邮箱发出。对员工 A 主机进行分析发现，该主机中安全软件存在多个“永恒之蓝下载器木马”恶意文件拦截记录。继续对其系统日志及计划任务分析发现，事发当天员工 A 主机曾成功执行永恒之蓝下载器木马恶意计划任务。

应急人员与员工 A 沟通了解到，他半年前曾通过第三方渠道下载某破解版软件，从安装该软件之后，安全软件就曾有相关拦截提示。事发当天，因误操作，对安全软件弹出的拦截提示点了“允许请求”。

经过最终分析研判确定，因员工 A 安全意识不足，安装了携带木马的破解版软件，导致个人主机感染“永恒之蓝下载器木马”病毒，后又因误操作对安全软件弹出的告警点击了“允许请求”，导致病毒下载执行了挖矿模块和邮件攻击模块，并以员工 A 主机为源头，通过读取邮箱通讯录，向其联系人发送恶意邮件导致了内网大范围传播。



（二） 防护建议

1） 禁止或限制个人 PC 接入内网，如业务需要，增加访问控制 ACL 策略，采用白名单机制只允许对个人 PC 开放特定的业务必要端口，其他端口一律禁止访问；

2） 禁止通过非官方渠道下载应用软件，不随意点击来历不明的链接，加强内部人员安全意识；

3） 浏览网页或启动客户端时注意 CPU/GPU 的使用率，出现异常时，及时排查异常进程，找到挖矿程序并清除；

4） 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

二、 某政府部门编辑器漏洞致网站黑页应急事件处置

（一） 事件概述

2021 年 4 月，奇安信安服团队接到某政府部门的应急响应求助，其官网被上传黑页，需要进行排查分析并溯源。

应急人员抵达现场后，对网站 Web 目录进行排查，成功定位黑页位置，同时发现网站备份文件 www.zip，并在备份文件中发现版本为 v4.1.3 的 kindeditor 编辑器。对 Web 日志进行分析发现，该日志中存在某公网 IP（x.x.x.62）对失陷网站上传黑页文件、压缩文件 63.zip 的记录，以及对 www.zip 文件的扫描记录。应急人员对 63.zip 进行分析发现，该压缩文件中包含 Webshell 文件，但无法解析成功。

应急人员协助删除黑页，恢复网站正常运行，并最终确认，攻击者首先对网站进行扫描，发现网站备份文件 www.zip 并进行分析，获取了网站目录结构和配置信息，同时在备份文件中发现版本为 V4.1.3 的 kindeditor 编辑器，攻击者利用该版本编辑器存在的文件上传漏洞，上传了包含 Webshell 的压缩文件 63.zip，但未能解析成功，继而上传黑页文件，对网站进行了恶意篡改。为了进一步获取网站权限，攻击者还对该网站进行 SQL 注入、敏感路径扫描、XSS 攻击等操作，但均未成功。

（二） 防护建议

1) 升级 kindeditor 编辑器到最新版本，或者在不影响业务的情况下关闭相关文件上传功能；

2) 建议部署网页防篡改设备，对网站文件、目录进行保护，拦截黑客的篡改操作，实时监控受保护的文件和目录，发现文件被篡改时，立即获取备份的合法文件并进行文件还原；

3) 对网站根目录文件上传功能，采用白名单上传文件，不在白名单内的一律禁止上传，上传目录权限遵循最小权限原则；

4) 加强日常安全巡检工作，定期对系统配置、网络设备配置、安全日志以及安全策略落实情况进行检查，定期安装补丁、更新病毒库，常态化信息安全工作；

5) 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，安全事件发生时可提供可靠的追溯依据。

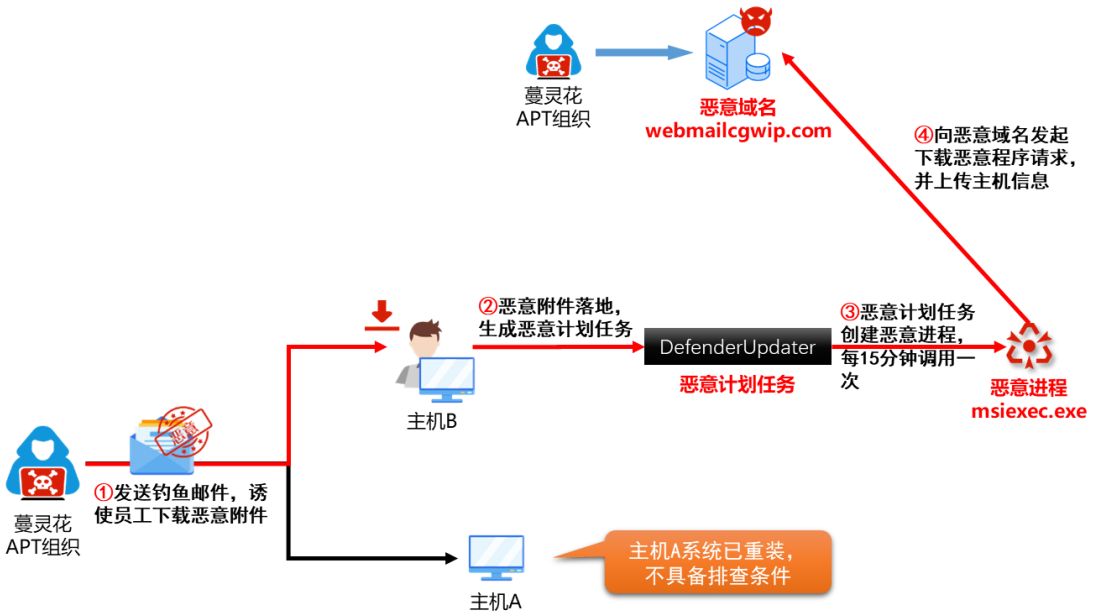
三、 制造业某客户蔓灵花 APT 应急事件处置

（一） 事件概述

2021 年 6 月，奇安信安服团队接到制造业某企业应急响应求助，该企业反馈办公网疑似被 APT 组织攻击，要求协助进行排查并溯源。

应急人员抵达现场后，对其中一台受害主机（x.x.x.103）日志进行排查发现，受害主机（x.x.x.103）每隔 15 分钟就会对恶意域名（webmailcgwip.com）发起 DNS 解析请求。对恶意域名（webmailcgwip.com）进行威胁情报查询，显示为蔓灵花 APT 团伙。应急人员利用进程监控及子父进程关系，成功定位到相关恶意进程 msiexec.exe 和恶意计划任务 DefenderUpdater。

最终，应急人员删除恶意计划任务、恶意进程、木马文件，对失陷主机进行全盘查杀，并溯源攻击路径：蔓灵花 APT 团队使用 songxxx@mfa.xx.cn 邮箱账号向该单位内网发送钓鱼邮件，受害主机（x.x.x.103）使用者下载并运行了钓鱼邮件中的木马文件。木马文件落地后在主机中创建恶意计划任务 DefenderUpdater 及恶意进程 msicexec.exe，使受害主机每隔 15 分钟向 APT 恶意域名 webmailcgwip.com/xingsu/asp.php 发送下载恶意程序请求，同时将发起请求的主机名和用户名信息上传。



（二） 防护建议

1) 定期进行内部人员安全意识培训，禁止点击来源不明邮件附件，禁止将敏感信息私自暴露至公网等；

2) 安装杀毒软件并定期更新病毒库，开启杀毒软件对邮件附件的扫描功能，有效识别恶意附件；

3) 禁止或限制个人 PC 接入内网，如有业务需要，加强访问控制 ACL 策略，采用白名单机制只允许对个人 PC 开放特定的业务必要端口，其他端口一律禁止访问；

4) 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；

5) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

四、 交通运输行业某客户感染门罗币挖矿病毒应急事件处置

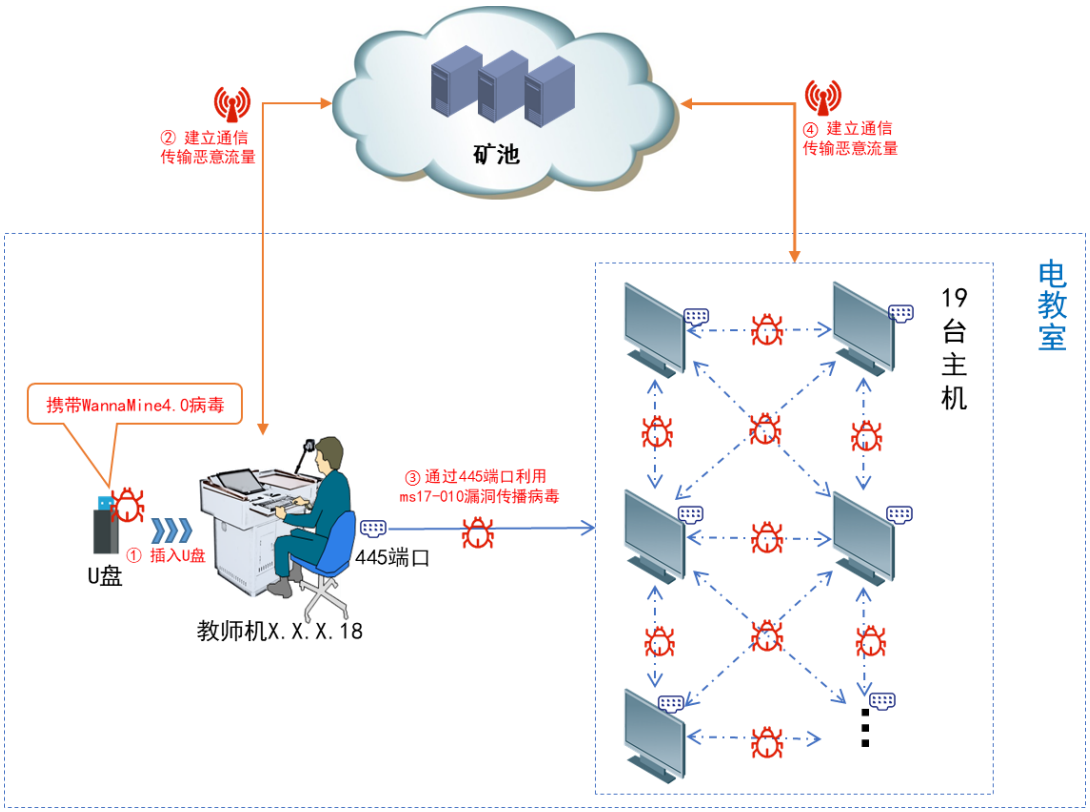
（一） 事件概述

2021 年 2 月，奇安信接到交通运输行业某单位应急响应请求，现场办公网内大量主机感染病毒，并且存在大量国外地址通讯行为，希望对办公网内失陷主机进行排查分析并溯源。

应急人员到达现场后，结合天眼告警及日志进行分析研判，确认失陷范围为多媒体教室的 20 台主机。应急人员对病毒样本进行分析，确认该病毒为新型 WannaMine4.0 变种，同时确认该病毒中毒时间的唯一性特征是病毒向注册表新建 LastBackup 键值的时间，并追踪到最早感染病毒的主机为教师机（x.x.x.18）。因中毒时间段失陷主机无法访问互联网，失陷主机所在网段为独立网段，可排除主机自身上网下载恶意文件或通过局域网内传播感染的可能性，对教师机（x.x.x.18）系统使用痕迹进行分析确认该主机的病毒来源为 U 盘传播。应急人员对失陷主

机进行系统运行环境检测分析发现，失陷主机均为 windows xp 系统，且基本未安装漏洞相关补丁和杀毒软件。

应急人员通过对排查结果分析研判，确认本次安全事件是因为该单位在多媒体教室的教师机上使用了携带木马病毒的 U 盘造成主机感染门罗币挖矿病毒（WannaMiner），利用 ms17-010 漏洞横向传播，最终导致 20 台主机失陷。



（二） 防护建议

1) 建议部署病毒防护软件，对移动存储设备进行查杀，在确定无病毒的情况下，再进行其他操作；

2) 非业务需要，禁止未授权移动存储设备接入主机，应使用白名单的方式只允许可信任移动存储设备接入；

3) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化；

4) 禁止服务器主动发起外部连接请求，对于需要向外部服务器推送共享数据的，应使用白名单的方式，在出口防火墙加入相关策略，对主动连接 IP 范围进行限制。

五、 某政府部门下属单位外连国外恶意 IP 应急事件处置

（一） 事件概述

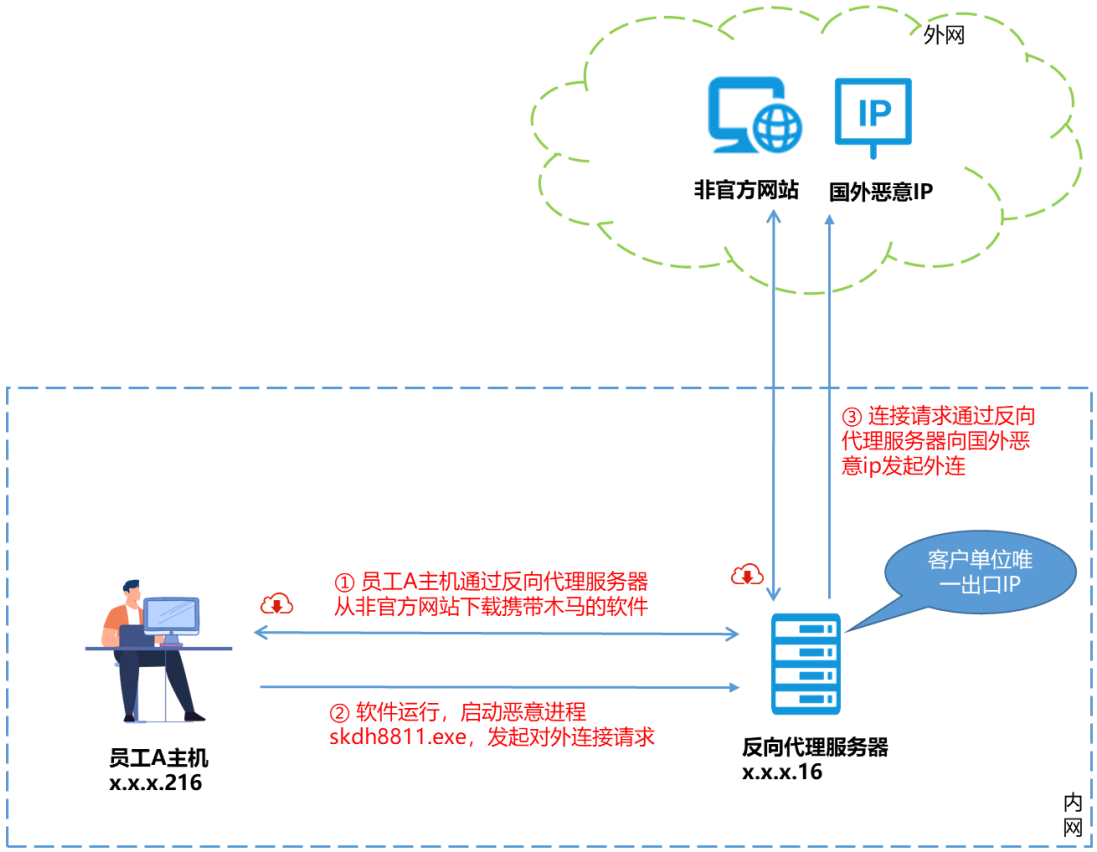
2021 年 8 月，奇安信安服团队接到某政府部门应急响应求助，其下属单位出口 IP 有外连

国外恶意 IP 流量，需要进行排查分析并溯源。

应急人员到达现场后发现，客户处上网行为管理设备中存在反向代理服务器（x.x.x.16）外连国外恶意 IP 记录，应急人员对该服务器分别进行了系统排查、日志排查、内存扫描以及 Webshell 扫描，均未发现异常。继续排查发现，服务器（x.x.x.16）与内网 6 台机器有网络连接，通过逐台断开网络连接查看外连是否断开，应急人员成功定位到发起外连的主机（x.x.x.216）。

应急人员对主机(x.x.x.216)进行排查，成功定位对外发起连接的恶意进程 skdh8811.exe，该进程启动后会加载同目录下的恶意动态库文件 skhooks.dll，然后加载内置 shellcode，解密出 metasploit-framework 生成的后门模块，执行对外发起连接的操作。此外，应急人员发现主机（x.x.x.216）安装有大量从互联网下载的软件，在与主机（x.x.x.216）的使用者员工 A 沟通后了解到，与恶意进程 skdh8811.exe 捆绑的软件是员工 A 通过非官方渠道下载的。

经最终研判分析确认，因员工 A 安全意识不足，通过非官方渠道安装并使用了携带木马的软件，导致个人主机（x.x.x.216）被感染，软件运行后启动恶意进程 skdh8811.exe 对外发起连接，从而导致本次外连事件发生。



（二） 防护建议

1） 禁止通过非官方渠道下载应用软件，加强内部人员安全意识；

2） 对于需要向外部服务器推送共享数据的，应使用白名单的方式，在出口防火墙加入相关策略，对主动连接 IP 范围进行限制；

3) 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；

4) 安装相应的防病毒软件，及时对病毒库进行更新，并且定期进行全面扫描，加强服务器上的病毒清除能力。

六、 互联网行业某客户感染 phobos 勒索病毒应急事件处置

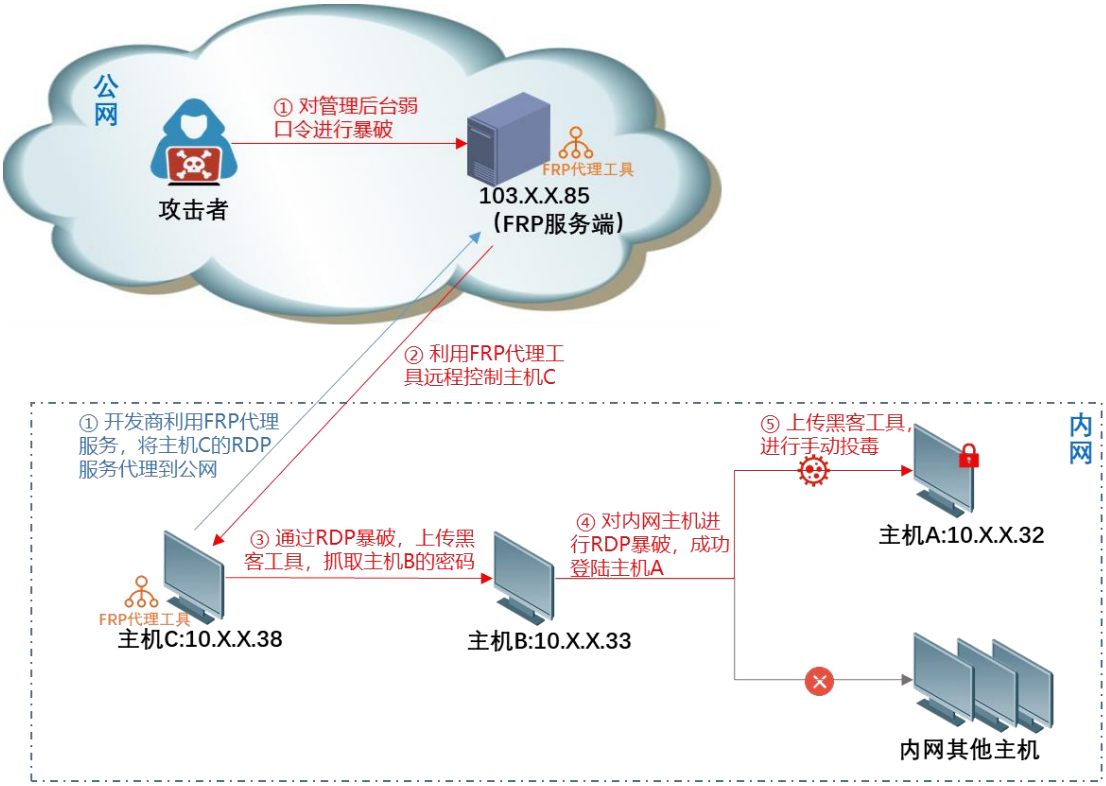
(一) 事件概述

2021 年 7 月，安服应急响应团队接到互联网行业客户应急响应请求，现场服务器被勒索，内网存在暴力破解攻击行为告警，客户希望对此事件进行排查溯源。

应急人员到达客户现场对受害主机 A（10.x.x.32）中加密文件进行分析，确认感染 phobos 家族勒索病毒，暂时无法解密。对主机 A（10.x.x.32）日志及系统进行排查发现，主机 B（10.x.x.33）曾远程 RDP 登录主机 A（10.x.x.32），并且在断开 RDP 连接 1 分钟后主机 A（10.x.x.32）被勒索。

应急人员对主机 B（10.x.x.33）中 RDP 登录日志进行排查，定位到首台被攻击的主机 C（10.x.x.38），并且客户内网主机系统账号存在弱口令及内网密码复用的情况。此外，应急人员发现，主机 C（10.x.x.38）中存在运行中的 FRP 代理工具进程。经与客户沟通，该 FRP 服务为客户 OA 系统开发公司所使用，应急人员排查发现，位于公网的 FRP 服务端（103.x.x.85）管理后台账号存在弱口令。

经过一系列排查分析，应急人员确认本次事件因客户 OA 系统开发公司为方便管理，将内网主机 C（10.x.x.38）的 RDP 服务违规代理至公网，并且管理后台账号使用弱口令所导致。攻击者利用暴力破解成功获取 FRP 服务端（103.x.x.85）权限，从而远程控制主机 C（10.x.x.38），随后以主机 C（10.x.x.38）为跳板，对主机 B（10.x.x.33）进行 RDP 暴破，成功后在内网进行横向渗透，最终成功登录主机 A（10.x.x.32），上传黑客工具，关闭防火墙，手动投放勒索病毒。



（二） 防护建议

1) 系统、应用相关用户杜绝使用弱口令，应使用高复杂强度的密码，尽量包含大小写字母、数字、特殊符号等的混合密码，加强管理员安全意识，禁止密码重用的情况出现；

2) 建议安装相应的防病毒软件，及时对病毒库进行更新，并且定期进行全面扫描，加强服务器上的病毒清除能力；

3) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化；

4) 建议在服务器上部署安全加固软件，通过限制异常登录行为、开启防暴破功能、禁用或限用危险端口（如 3389、445、139、135 等）、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵。

七、 交通运输业某客户感染 Magniber 勒索病毒应急响应事件

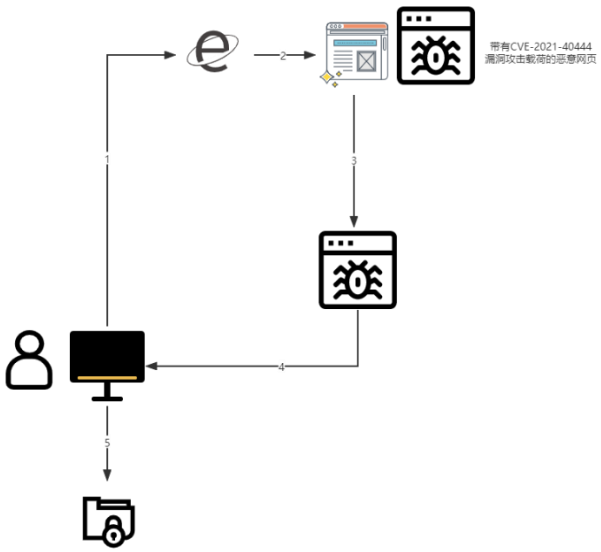
（一） 事件概述

2021 年 12 月，奇安信安服应急响应团队接到交通运输业某客户应急响应请求，现场一台终端感染勒索病毒，客户希望对受害机器进行排查并溯源。

应急人员到达客户现场对受害终端进行排查，结合加密文件后缀、勒索信以及内部威胁情报等内容，确定该终端感染 Magniber 勒索病毒，暂时无法解密。应急人员查看现场行为审计设备发现，受害终端在事发之前访问了一个钓鱼网站 http://xxxpig.com，该钓鱼网站域名与某常用生活服务网站仅差一个字符，极易发生混淆。

应急人员使用虚拟机中的 IE 浏览器访问钓鱼网站域名 http://xxxpig.com 发现，页面加载成功后会自动跳转到一个新的网页 C，将网页 C 保存并上传至 VT 进行查杀，识别出该网页为 CVE-2021-40444 漏洞利用代码。随后，应急人员根据威胁情报中描述的目录，在虚拟机中发现了恶意.inf 文件，将.inf 文件上传至 VT 分析，被识别为 Magniber 勒索病毒。

经过一系列排查分析，最终应急人员成功复现攻击路径：攻击者通过构造带有 CVE-2021-40444 漏洞攻击载荷的恶意网页，并使用与常用生活服务网站相似的域名，诱使用户进行访问。客户员工使用 IE 浏览器误访问该恶意网页，触发 CVE-2021-40444 漏洞利用代码，该代码执行后，在受害终端自动下载并执行病毒样本，导致受害终端感染 Magniber 勒索病毒，被加密。



（二） 防护建议

1) 加强人员安全意识培养，访问网站前认真核对网页域名，不要点击来源不明的链接，不从不明网站下载软件；

2) 对业务系统及数据进行及时备份，并定期验证备份系统及备份数据的可用性；

3) 安装杀毒软件、终端安全管理软件并及时更新病毒库；

4) 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；

5) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

八、 服务业某客户 100+台服务器感染挖矿病毒应急事件处置

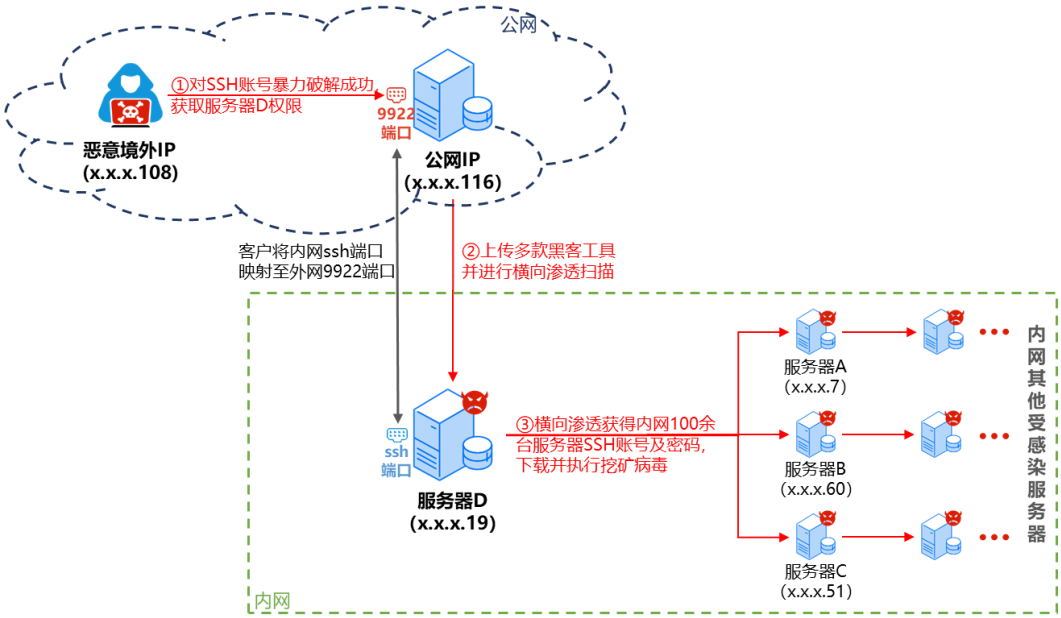
（一） 事件概述

2021 年 9 月，奇安信安服团队接到服务业某客户应急响应求助，公司内网 100 余台服务器感染挖矿病毒，已严重影响到企业正常运作，客户希望对挖矿病毒进行清除，并溯源入侵途径。

应急人员对受害服务器进行分析发现，存在异常进程 mysql 大量占用服务器资源，导致服务器卡死不可用，继续排查发现名为 go 的文件会尝试连接矿池 pool.supportxmr.com，应急人员对矿池地址进行分析，确认客户现场感染的是门罗币挖矿病毒。

应急人员对多台受害服务器进行系统排查发现，服务器历史执行命令中均有使用 wget 下载挖矿程序的记录，并且在受害服务器目录中均存在多款黑客工具和存有 ssh 账号及密码信息的 txt 文件。根据 ssh 登录日志记录，应急人员定位到服务器 D（x.x.x.19）是第一台被恶意境外 IP（x.x.x.108）登录的内网服务器。

应急人员对服务器 D（x.x.x.19）的端口开放情况进行排查发现，该服务器的 ssh 端口被映射到公网 IP（x.x.x.116）的 9922 端口上，并且包括服务器 D（x.x.x.19）在内的本次所有失陷主机 ssh 账号密码均为弱口令，至此应急人员判定本次事件是由于客户方将 ssh 端口映射至公网，并且账号密码使用弱口令所导致。



（二） 防护建议

1) 系统、应用相关用户杜绝使用弱口令，应使用高复杂强度的密码，尽量包含大小写字母、数字、特殊符号等的混合密码，加强管理员安全意识，禁止密码重用的情况出现；

2) 建议安装防病毒软件，及时对病毒库进行更新，并且定期进行全面扫描，加强服务器病毒预防、抑制及清除能力；

3) 建议在服务器上部署安全加固软件，通过限制异常登录行为、开启防爆破功能、禁用或限用危险端口（如 3389、445、139、135 等）、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；

4) 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；

5) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

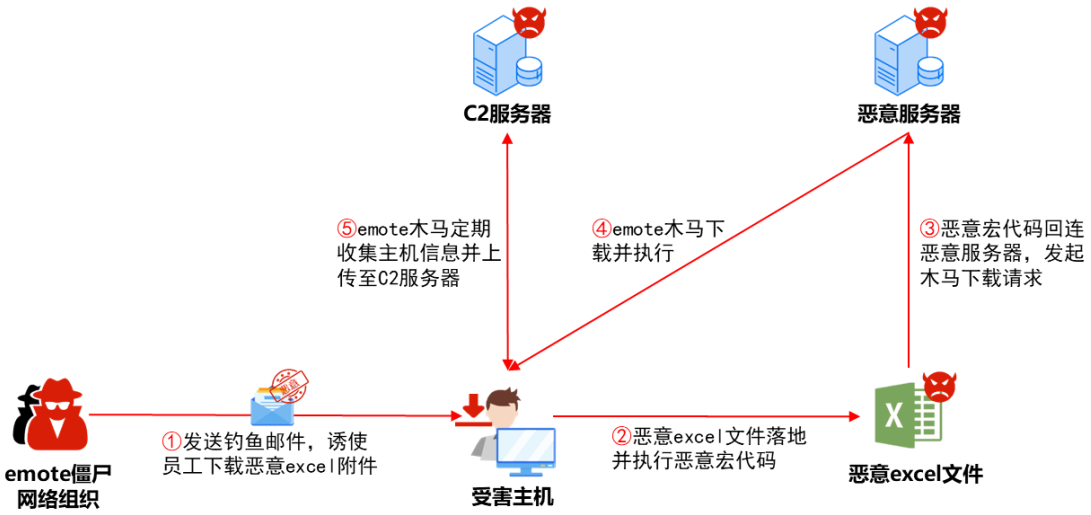
九、 能源行业某客户内网收到钓鱼邮件应急事件处置

（一） 事件概述

2021 年 12 月，奇安信安服团队接到能源行业某客户应急响应求助，公司内部收到数千封钓鱼邮件，客户期望对钓鱼邮件内容进行分析并排查疑似感染终端情况。

应急人员抵达现场后，对钓鱼邮件内容进行查看发现，邮件所带附件是一个压缩包，应急人员将其下载至沙箱并解压，发现压缩包内为多个带有恶意宏代码的 excel 文件，打开后会诱导用户启动宏功能，为自身恶意宏代码创造执行条件。恶意宏代码运行后，会调用 powershell 回连恶意服务器将 emote 木马病毒下载至本地并执行。emote 木马会定期收集主机信息并将数据加密上传至 C2 服务器，使服务器沦为 emote 僵尸网络中的一员。

根据客户反馈，应急人员对疑似点击了钓鱼邮件的 3 台员工电脑进行病毒查杀及特征排查，均未发现其它异常。至此，应急人员确认，本次攻击并非针对单一用户的定向攻击，是 emote 僵尸网络在全网范围的钓鱼邮件投递。投递的钓鱼邮件附件内包含带有恶意 excel 4.0 宏代码的 excel 文档，功能为下载并执行 emote 木马，进而控制受害终端。



（二） 防护建议

1) 加强人员安全意识培养，不要点击来源不明的邮件附件，不要从不明网站下载软件。对来源不明的文件包括邮件附件、上传文件等要先杀毒处理；

2) 部署邮件安全检测设备，对外部邮件进行安全检测，提高垃圾邮件、恶意邮件识别及过滤能力；

3) 建议安装防病毒软件，及时拦截病毒落地，并且定期进行全面扫描，加强服务器病毒预防、抑制及清除能力；

4) 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，在安全事件发生时可提供可靠的追溯依据；

5) 加强日常安全巡检制度，定期对系统配置、系统漏洞、安全日志以及安全策略落实情况进行检查，及时修复漏洞、安装补丁，将信息安全工作常态化。

十、 某客户遭遇 Apache Log4j2 漏洞攻击应急事件处置

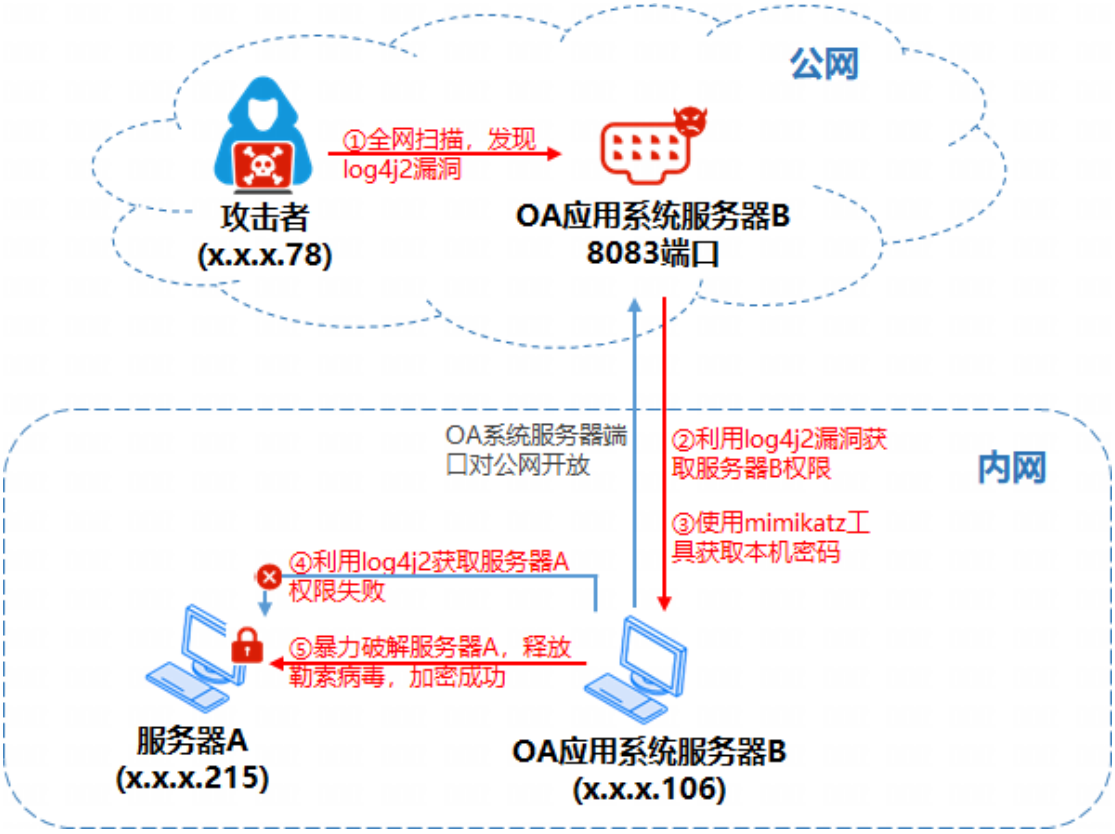
（一） 事件概述

2021 年 12 月，奇安信安服团队接到某客户应急响应求助，公司服务器感染勒索病毒，所有文件被加密，客户希望对受害服务器进行排查，溯源入侵途径。

应急人员抵达现场后对被加密的服务器 A（x.x.x.215）进行排查发现，确认客户服务器感染 Tellyouthepass 家族勒索病毒，该家族使用 RSA+AES 的方式对文件进行加密，无法解密。

应急人员对服务器 A（x.x.x.215）的日志和系统进行排查发现，应急前一天服务器 B（x.x.x.106）曾远程 RDP 登录服务器 A（x.x.x.215）。经与客户沟通，服务器 B（x.x.x.106）为 OA 应用系统服务器，对服务器 B（x.x.x.106）系统进行排查发现，OA 应用系统端口 8083 对公网开放。

最终确认，客户将含有 log4j2 远程代码执行漏洞的 OA 应用系统开放在公网，攻击者利用 log4j2 远程代码执行漏洞（CVE-2021-44228）获取 OA 应用系统服务器 B（x.x.x.106）权限及密码信息，利用密码复用技术暴力破解服务器 A（x.x.x.215）RDP 账号并成功登录，下载并运行 Down.class 恶意文件，释放勒索病毒文件 debug.exe，导致服务器 A（x.x.x.215）被加密。



（二） 防护建议

1） 为服务器升级到最新的安全补丁，部署服务器安全防护系统，及时打补丁并做好网站服务目录权限控制；

2） 服务器、操作系统启动密码策略，杜绝使用弱口令，应使用高复杂强度的密码，如包

含大小写字母、数字、特殊符号等的混合密码，加强管理员安全意识，禁止密码重用的情况出现；

3) 建议在服务器上部署安全加固软件，通过限制异常登录行为、禁用或限用危险端口（8083、445、139、135 等）、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；

4) 建议在服务器或虚拟化环境上部署虚拟化安全管理系统，提升防恶意软件、防暴力破解等安全防护能力；

5) 建议安装相应的防病毒软件，及时对病毒库进行更新，并且定期进行全面扫描，加强服务器上的病毒清除能力；

6) 加强日常安全巡检制度，定期对系统配置、网络设备配合、安全日志以及安全策略落实情况进行检查，常态化信息安全工作。

附录 1 奇安信集团安服团队

奇安信是北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商，作为中国领先的网络安全品牌，奇安信多次承担国家级的重大活动网络安全保障工作，创建了稳定可靠的网络安全服务体系——全维度管控、全网络防护、全天候运行、全领域覆盖、全兵种协同、全线索闭环。

奇安信安全服务以攻防技术为核心，聚焦威胁检测和响应，通过提供咨询规划、威胁检测、攻防演习、持续响应、预警通告、安全运营等一系列实战化的服务，在云端安全大数据的支撑下，为客户提供全周期的安全保障服务。

应急响应服务致力于成为“网络安全 120”。自 2016 年以来，奇安信已积累了丰富的应急响应实践经验，应急响应业务覆盖了全国 31 个省（自治区、直辖市），2 个特别行政区，处置政企机构网络安全应急响应事件超过三千起，累计投入工时 37000 多个小时，为全国超过两千家政企机构解决网络安全问题。

奇安信还推出了应急响应训练营服务，将一线积累的丰富应急响应实践经验面向广大政企机构进行网络安全培训和赋能，帮助政企机构的安全管理者、安全运营人员、工程师等不同层级的人群提高网络安全应急响应的能力和技术水平。奇安信正在用专业的技术能力保障着企业用户的网络安全，最大程度地减少了网络安全事件所带来的经济损失，并降低了网络安全事件造成的社会负面影响。

应急响应 7×24 小时热线电话：95015。

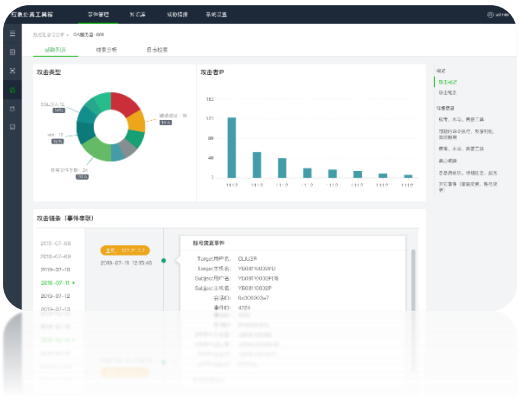
附录 2 应急响应工具箱介绍

奇安信应急响应工具箱是一款集成了奇安信安全情报及专家分析经验的自动化应急响应工具，旨在解决应急响应人效低、应急处置标准化程度低、处置人员能力不足等痛点。应急响应工具箱源于实战、用于实战，是真正解决客户痛点的产品箱，而不是常见工具的简单集成。

应急响应工具箱在产品设计阶段就引入了大量的应急响应专家，也经过了安服团队多年来的实战使用和不断改进，在应急响应服务、攻防演习服务、重要时期安全保障服务等业务中都发挥了不可或缺的作用。

依托奇安信行业领先的攻防研究能力，应急响应工具箱内置了威胁情报、专家知识库、分析模型和众多检测工具（日志关联分析工具、APT 检查工具、恶意代码检查工具、Webshell 后门检查工具、漏洞检查工具、暗链检查工具等），保障了检测、分析的效率和准确度。奇安信将应急响应工具的自动化分析能力，提升到一个新的高度，能够进行多维度的线索关联分析、基于情报的事件溯源，以及多场景的线索分析。

应急响应工具箱在最大程度上实现了自动化的威胁检测和关联分析，并经过了奇安信安全服务团队多年来的实战检验，能够降低应急响应的技术难度，赋能用户。同时，其具有高集成化的特点，覆盖了应急响应全过程所需要的各类支撑功能并简化了操作，还内置了应急流程，并配套了相关模板，将应急响应工作规范化。



附录 3 95015 冬奥网络安全应急保障服务热线

95015 是全国首个网络安全行业服务短号，是为全国各地政府、企业、相关机构提供网络安全应急响应、合作与咨询服务的电话专线。“安全快一步，95015”。

95015 服务短号，由北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商奇安信集团，在北京冬奥会开幕前夕，即 2022 年 1 月 20 日正式推出。在北京 2022 年冬奥会和冬残奥会期间，95015 服务短号是承载全国各地政企机构网络安全保障工作的重要支撑平台，同时也是全国各地重大网络安全事件应急响应的绿色通道，是全国冬奥网络安全保障工作中的关键一环。北京冬奥会结束后，95015 服务短号将永久保留，持续为全国各地政企机构提供网络安全应急响应、合作与咨询服务。

95015 服务短号，整合了原有的 4009-727-120 应急响应专线、4009-303-120 客户服务热线和 4006-783-600 合作伙伴热线三条 400 电话专线，实现了“一号全通”。同时，更短的号码也意味着更快的响应速度，更加优质、更加便捷的平台服务，标志着网络安全行业在线服务能力与服务方式的一次重大升级。

报告二维码

（扫码获取全文）

应急响应

7×24小时热线电话：95015