https://www.qianxin.com

95015网络安全应急响应分析报告(2025)

THE REPORT

发布机构：

奇安信安服团队

发布时间：

2026.2

主要观点

- 2025 年，奇安信集团安服团队共接到应急服务需求 575 起。政府部门、制造业、金融机构的业务专网是 2025 年攻击者攻击的主要目标。
- 网络安全基础设施建设的不完善，网络安全运营能力的缺失，是当前国内绝大多数政企机构的通病。一方面，永恒之蓝、弱口令等基础漏洞仍然普遍存在，高危端口大量暴露；另一方面，仅有 14.2%的政企机构能够通过安全巡检提前发现问题，避免损失，而绝大多数政企机构只能在重大损失发生之后，或被第三方机构通报之后才能发现安全问题。
- 安全意识问题依旧是制约政企机构安全生产的根本性问题。近三成左右的应急事件与弱口令有关；内部人员违规操作引发的应急响应事件占 2025 年 95015 服务平台接报事件总量的五分之一；而因员工安全意识不足导致的各类风险更是层出不穷，包括遭受黑客钓鱼攻击、私自下载携带恶意软件的应用程序、滥用 U 盘引发系统瘫痪，以及随意开放端口感染勒索病毒等。值得注意的是，钓鱼邮件的利用占比呈现显著增长态势，从 2024 年的 4.7%快速攀升至 2025 年的 13.6%，增幅接近两倍。这一趋势进一步凸显了大中型政企机构亟需加强内部员工网络安全防范意识培训的紧迫性。
- 2025 年接收的安全事件中有小部分来自政企机构内部实战攻防演习活动，通过实际的攻击模拟和防御演练，企业可以更好地发现和识别可能存在的安全漏洞，能够尽早发现并修复潜在的威胁，防止实际攻击的发生，减少潜在的损失。

摘　　要

- 2025 年，95015 服务平台共接到全国政企机构网络安全应急事件报告 575 起。奇安信安服团队累计投入工时 4170.5 小时处置相关事件，折合 521.3 人天，处置一起应急事件平均用时 7.3 小时。
- 从行业分布来看，2025 年 95015 服务平台接报的网络安全应急响应事件中，政府部门报告的事件最多，为 76 起，占比 13.2%；其次是制造业、金融机构，均占比 12.5%。此外，事业单位、IT 信息技术等行业也是网络安全应急响应事件高发行业。
- 59.5%的政企机构，是在系统已经出现了非常明显的入侵迹象后，拨打的 95015 网络安全服务热线；21.0%的政企机构，是在被攻击者勒索之后进行的报案求助。而真正能够通过安全运营巡检，提前发现问题的政企机构仅占比 14.2%。
- 从网络安全事件的影响范围来看，50.6%的事件主要影响业务专网，而主要影响办公网的事件占比 49.4%。从受影响的设备数量来看，失陷服务器为 10349 台，失陷办公终端为 1498 台。业务专网、服务器是网络攻击者攻击的主要目标。
- 从网络安全事件造成的损失来看，造成生产效率低下的事件 157 起，占比 27.3%；造成数据泄露的事件 92 起，占比 16.0%；造成数据丢失的事件 77 起，占比 13.4%；此外，造成政企机构声誉影响的事件 56 起，造成数据被篡改的事件 18 起。
- 内部人员为了方便工作等原因进行违规操作，进而导致系统出现故障或被入侵，触发应急响应的网络安全事件多达 115 起。这一数量仅次于黑产活动（201 起）、超过了窃取重要数据（99 起）和敲诈勒索（65 起）等为目的的外部网络攻击事件。
- 以恶意程序为主要手段的网络攻击最为常见，占比 35.5%；其次是漏洞利用，占比 25.1%；钓鱼邮件排第三，占比 13.4%。Web 应用 CC 攻击、网页篡改、网络监听攻击、拒绝服务攻击等也比较常见。还有约 18.7%的安全事件，并非网络攻击事件。
- 应急事件分析显示，勒索病毒、银狐木马、挖矿木马是攻击者使用最多的恶意程序类型，分别占到恶意程序攻击事件的 11.3%、11.3%和 8.2%。此外，APT 专用木马、蠕虫病毒、DDOS 木马、网站木马等也都是经常出现的恶意程序类型。
- 在应急响应事件处置的勒索软件中，排名第一的是 Weaxor 勒索软件，全年触发大中型政企机构网络安全应急响应事件 9 次；其次是 Makop 勒索软件 5 次，RNTC 勒索软件和 Wannacry 勒索软件均为 3 次。这些流行的勒索病毒，十分值得警惕。
- 永恒之蓝漏洞是攻击者在 2025 年利用最多的网络安全漏洞，相关应急事件多达 145 起，占比 25.2%。其次是弱口令，相关利用事件为 140 起，占比 24.3%。

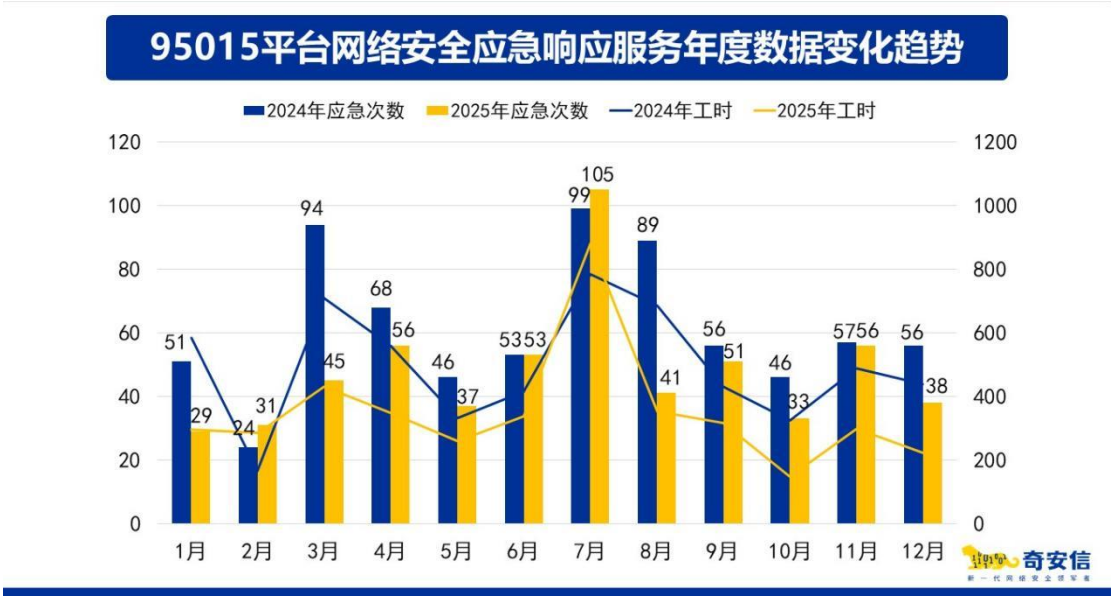
关键词：95015、应急响应、安全服务、永恒之蓝、内部违规、敲诈勒索、漏洞利用

目　　录

第一章　网络安全应急响应形势综述

2025 年 1~12 月，95015 服务平台共接到全国范围内网络安全应急响应事件报告 575 起，奇安信安服团队第一时间协助政企机构处置安全事故，确保了政企机构门户网站、数据库和重要业务系统等的持续安全稳定运行。

综合统计数据显示，在全年 575 起网络安全应急响应事件的处置中，奇安信安服团队累计投入工时为 4170.5 小时，折合 521.3 人天，处置一起应急事件平均用时 7.3 小时。



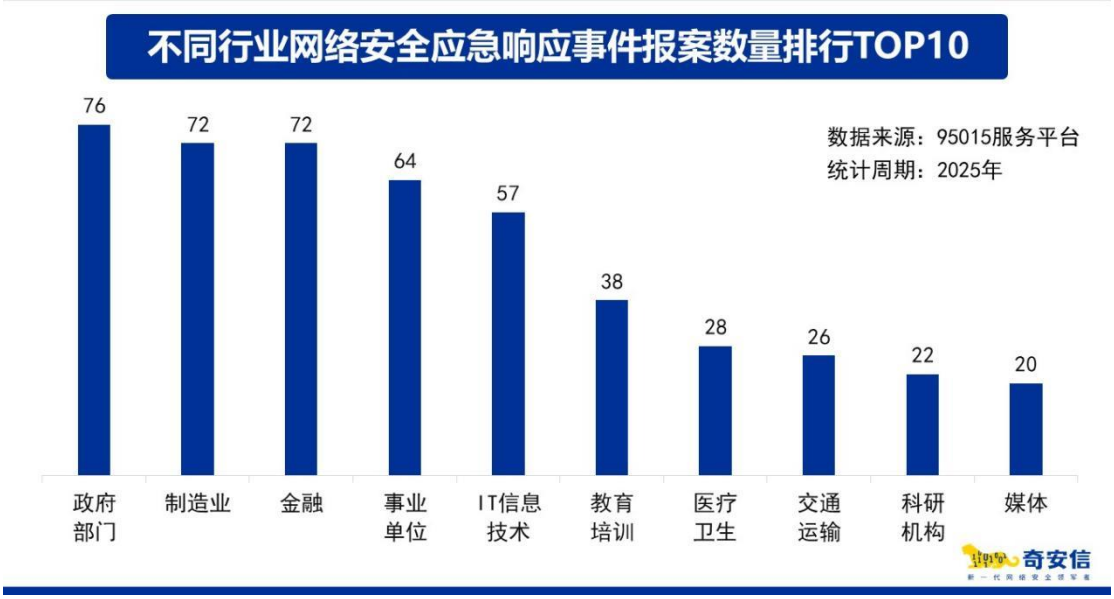
第二章　应急响应事件受害者分析

本章将从网络安全应急响应事件受害者的视角出发，从行业分布、事件发现方式、影响范围、以及攻击行为造成的影响等几个方面，对 95015 服务平台全年接报的 575 起网络安全应急响应事件展开分析。

一、　行业分布

从行业分布来看，2025 年 95015 服务平台接报的网络安全应急响应事件中，政府部门报告的事件最多，为 76 起，占比 13.2%；其次是制造业、金融机构，均占比 12.5%。此外，事业单位、IT 信息技术等行业也是网络安全应急响应事件高发行业。

下图给出了不同行业网络安全应急响应事件报案数量的 TOP10 排行。



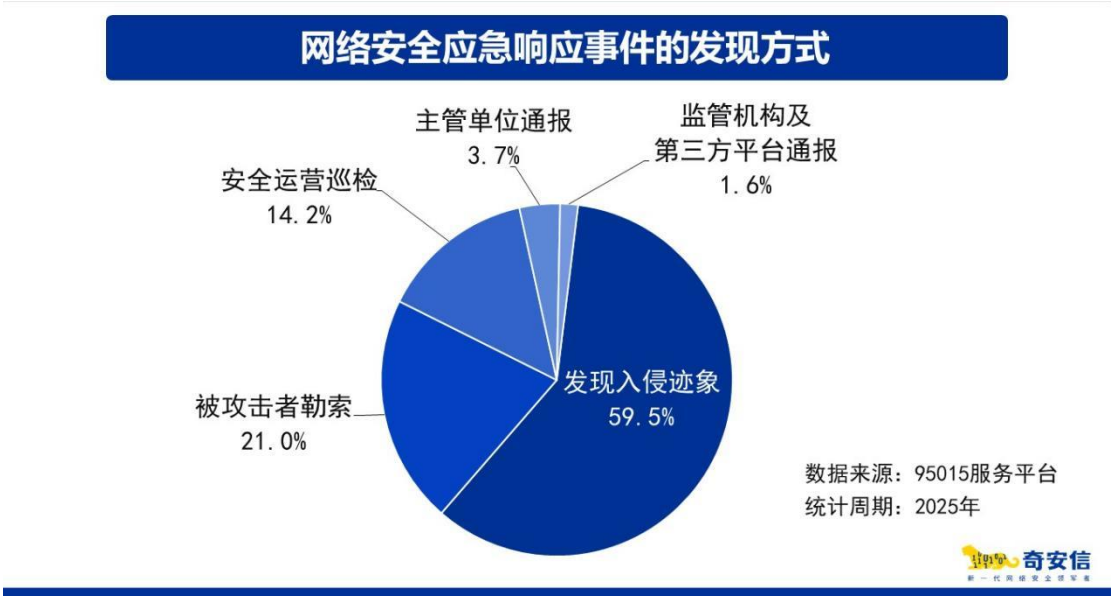
二、　事件发现

从安全事件的发现方式来看，59.5%的政企机构，是在系统已经出现了非常明显的入侵迹象后，拨打的 95015 网络安全服务热线；21.0%的政企机构，是在被攻击者勒索之后进行的报案求助。这二者之和为 80.5%。

也就是说，超过八成的大中型政企机构是在系统已经遭到了巨大损失，甚至是不可逆的破坏后，才向专业机构进行求助。而真正能够通过安全运营巡检，在损失发生之前及时发现问题并呼救，避免损失发生的政企机构，占比为 14.2%。

此外，还有约 5.3%的政企机构是在得到了主管单位、监管机构及第三方平台的通报后启动的应急响应。这些机构不仅严重缺乏有效的网络安全运营，也严重缺乏必要的威胁情报能力支撑，致使自己的主管单位或监管机构总是先于自己，发现自身的安全问题

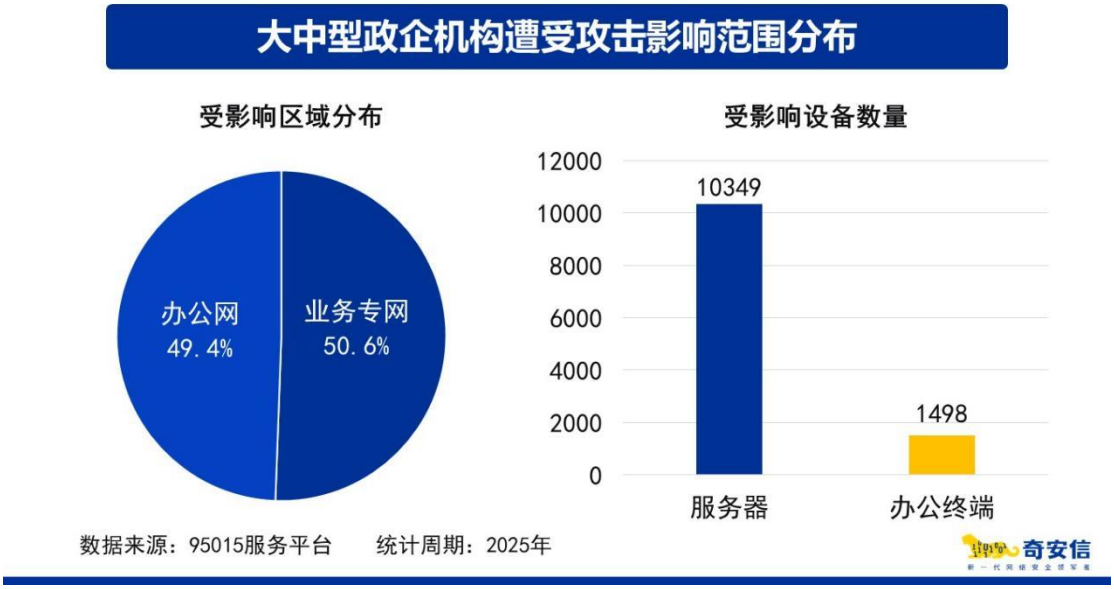
或被攻击的现象。其中，某些通报可能还会使相关单位面临法律责任及行政处罚。这些被通报的政企机构都是潜在的定时炸弹，随时都有可能爆发。



三、 影响范围

网络安全事件往往会对 IT 及业务系统产生重大的影响。在 2025 年 95015 服务平台接报处置的网络安全应急响应事件中，50.6%的事件主要影响的是业务专网，而主要影响办公网的事件占比 49.4%。从受网络安全事件影响的设备数量来看，失陷服务器为 10349 台，失陷办公终端为 1498 台。

2025 年大中型政企机构遭受网络攻击事件的影响范围如下图所示。



在本报告中，办公网是指企业员工使用的台式机、笔记本电脑、打印机等设备组成

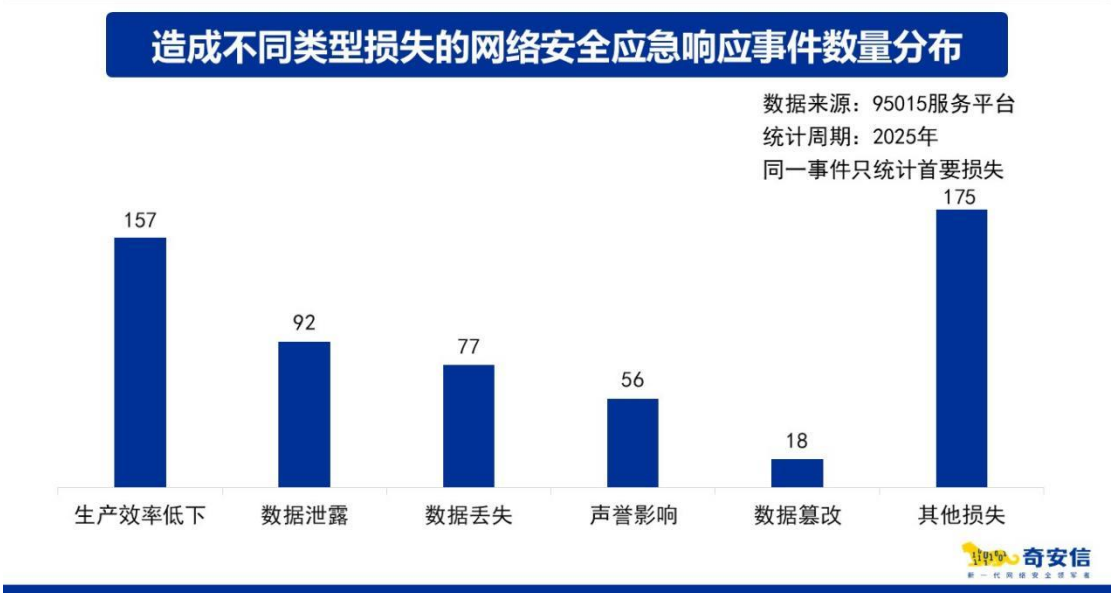
的基本办公网络，而业务专网泛指机构整体运行与对外支撑所需要的各种网络系统。

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、服务器是网络攻击者攻击的主要目标。

大中型政企机构在对业务专网进行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、 事件损失

网络安全事件通常都会引起政企机构不同程度、不同类型的损失。应急处置现场情况分析显示，在 95015 服务平台全年接报的 575 起报案中，有 157 起事件，造成了相关机构的生产效率低下，占比 27.3%，是排名第一的损失类型；其次是造成数据泄露的事件有 92 起，占比 16.0%，排名第二；造成数据丢失的事件 77 起，占比 13.4%，排名第三；此外，造成政企机构声誉影响的事件 56 起，造成数据被篡改的事件 18 起，造成其他损失的事件 175 起。



特别说明，在上述统计中，同一事件只计算一次，我们只统计每起事件造成的最主要的损失类型。

造成生产效率低下的主要原因是挖矿、蠕虫、木马等攻击手段使服务器 CPU 占用率过高，从而影响生产效率。也有部分企业是因为勒索病毒攻击造成了部分生产系统停产。

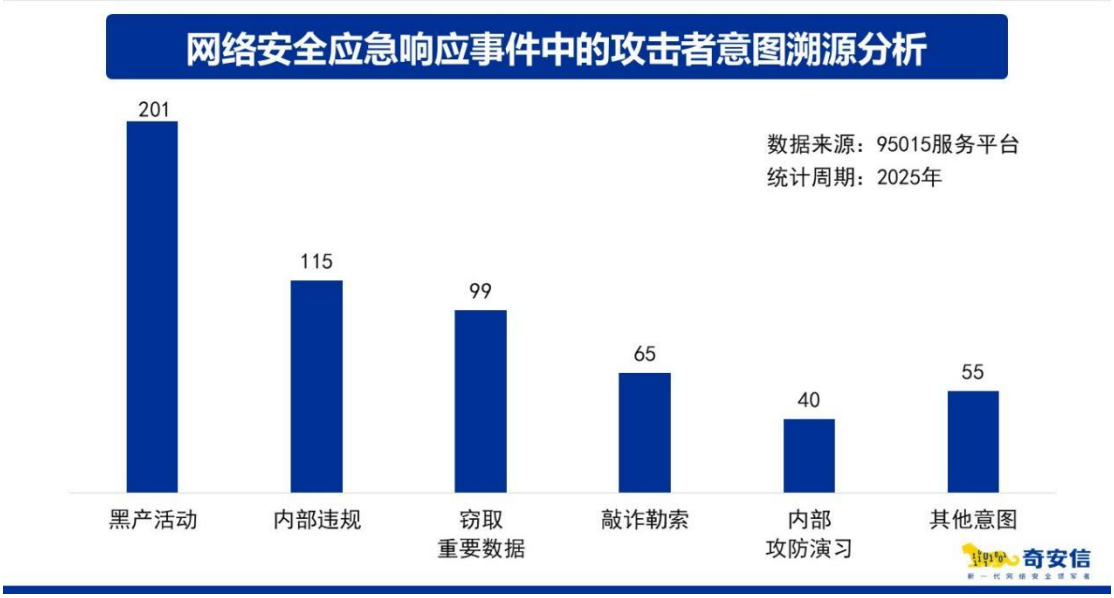
造成数据泄露的主要原因是黑客的入侵和内部人员的泄密。造成数据丢失的原因是多方面的，其中，因勒索病毒加密而导致数据无法恢复是首要原因。

第三章　应急响应事件攻击者分析

本章将从网络安全应急响应事件攻击者的视角出发，从攻击意图、攻击类型、恶意程序和漏洞利用等几个方面，对 95015 服务平台全年接报的 575 起网络安全应急响应事件展开分析。

一、　攻击意图

攻击者是出于何种目的发起的网络攻击呢？应急工程师在对网络安全事件进行溯源分析过程中发现，2025 年，内部人员为了方便工作等原因进行违规操作，进而导致系统出现故障或被入侵，触发应急响应的网络安全事件多达 115 起。这一数量仅次于黑产活动（201 起）、超过了窃取重要数据（99 起）和敲诈勒索（65 起）等为目的的外部网络攻击事件。



在这里，黑产活动以境内团伙为主，主要是指通过黑词黑链、钓鱼页面、挖矿程序等攻击手段开展黑产活动牟取暴利。

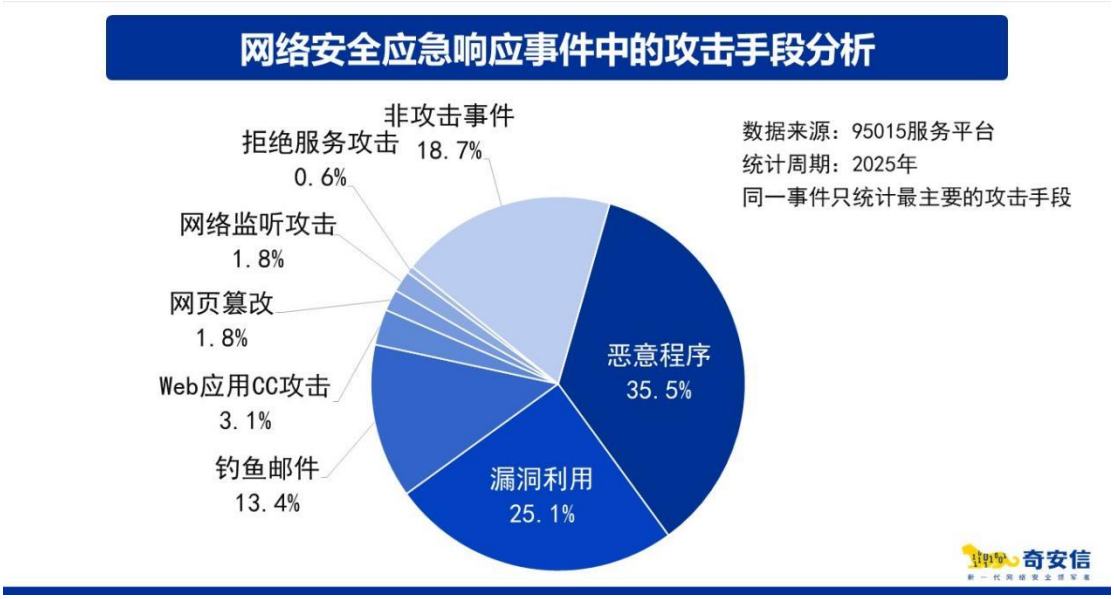
在 115 起内部违规事件中，内部人员为了方便工作或出于其他原因将内部业务端口映射至外网的违规操作需要引起大中型企业的重视。

以窃取重要数据为目的的攻击，一般分为两种：一种是民间黑客非法入侵政企机构内部系统盗取敏感、重要数据，如个人信息、账号密码等；另一种则是商业间谍活动或 APT 活动。从实际情况来看，第一种情况更为普遍，第二种情况偶尔会发生。

敲诈勒索，主要是指攻击者利用勒索软件攻击政企机构的终端和服务器，进而实施勒索。此类攻击几乎全部是由境外攻击者发起，打击难度极大。

二、 攻击手段

不同的安全事件，攻击者所使用的攻击手段也有所不同。对 2025 年全年的网络安全应急响应事件分析发现，以恶意程序为主要手段的网络攻击最为常见，占比 35.5%；其次是漏洞利用，占比 25.1%；钓鱼邮件排第三，占比 13.4%。此外，Web 应用 CC 攻击、网页篡改、网络监听攻击、拒绝服务攻击等也比较常见。还有约 18.7%的安全事件，最终被判定为非攻击事件。也就是说，由于企业内部违规操作，意外事件等原因，即便没有导致系统被入侵，但也同样触发了网络安全应急响应的事件不在少数，值得警惕。



三、 恶意程序

应急事件分析显示：勒索病毒、银狐木马、挖矿木马是攻击者使用最多的恶意程序类型，分别占到恶意程序攻击事件的 11.3%、11.3%和 8.2%。此外，APT 专用木马、蠕虫病毒、DDOS 木马、网站木马等也都是经常出现的恶意程序类型。还有 24.0%的恶意程序攻击事件与比较常见的，针对普通网民的互联网流行木马有关。

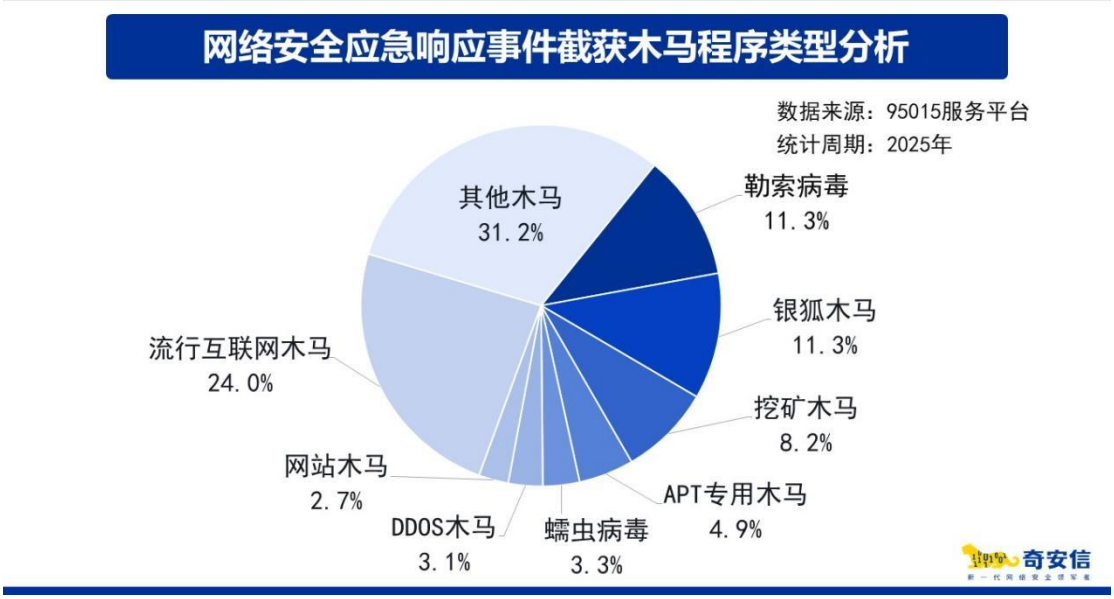


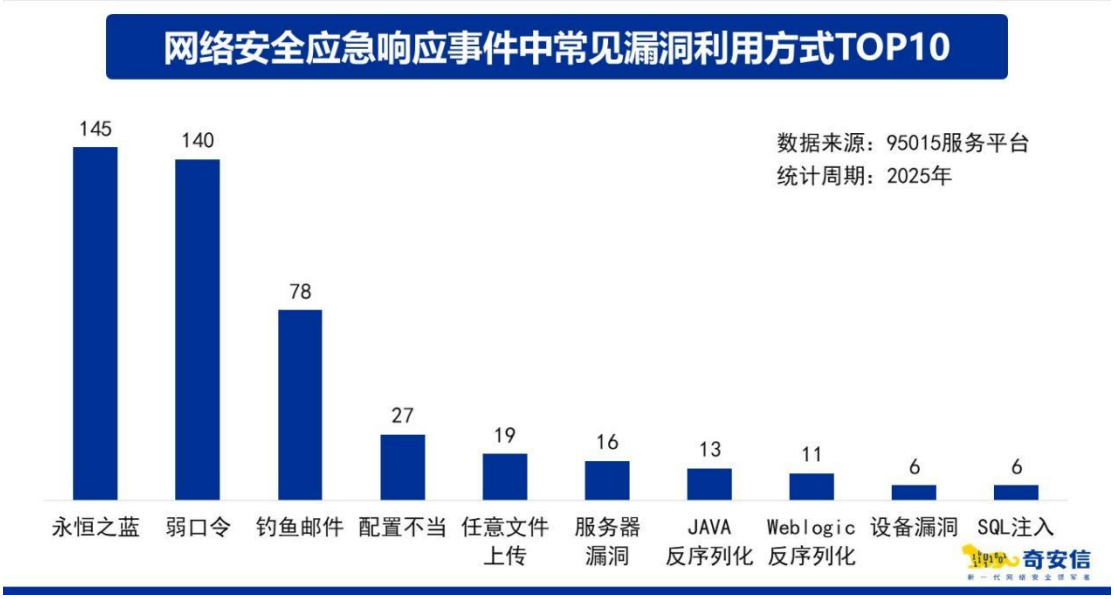
表 1 给出了 2025 年 95015 服务平台接报的网络安全应急响应事件中，出现频率最高的勒索软件排行榜 TOP10。可以看到，排名第一的是 Weaxor 勒索软件，全年触发大中型政企机构网络安全应急响应事件 9 次；其次是 Makop 勒索软件 5 次，RNTC 勒索软件和 Wannacry 勒索软件均为 3 次。这些流行的勒索病毒，十分值得警惕。

表 1 遭受攻击勒索软件类型 TOP10

勒索软件名称	应急次数
Weaxor 勒索软件	9
Makop 勒索软件	5
RNTC 勒索软件	3
Wannacry 勒索软件	3
Bixi 勒索软件	2
Mallox 勒索软件	1
Beast 勒索软件	1
BeijignCrypt 勒索软件	1
Phobos 勒索软件	1
BlackBit 勒索软件	1

四、 漏洞利用

应急事件分析显示：永恒之蓝漏洞是攻击者在 2025 年最为经常利用的网络安全漏洞，相关网络安全应急响应事件多达 145 起，占 95015 平台全年应急响应事件接报总数的 25.2%。其次是弱口令，相关利用事件为 140 起，占比 24.3%。排名第三的为钓鱼邮件，相关利用事件为 78 起，占比 13.6%。



永恒之蓝漏洞自 2017 年 WannaCry 病毒爆发后，已经成为广为人知，必须修补的安全漏洞。时至今日仍然有大量的政企机构倒在永恒之蓝的枪口之下，说明这些政企机构严重缺乏最基本的网络安全基础设施建设，缺乏最基本的网络安全运营能力。而弱口令的大行其道，完全是安全意识淡薄、安全管理松懈的体现。预计在未来相当长的时间里，永恒之蓝漏洞和弱口令仍将是国内政企机构亟待解决的、基础性的网络安全问题。

第四章　应急响应典型案例分析

2025 年，95015 网络安全服务热线共接到全国各地网络安全应急响应求助 575 起，涉及全国 31 个省市（自治区、直辖市）、2 个特别行政区，覆盖政府部门、制造业、金融机构、医疗卫生等 20 余个行业。本章将结合 2025 年的网络安全应急响应实践，介绍 6 起典型案例，希望能够为政企机构网络安全建设与运营提供有价值的参考。

一、　某学院信息遭泄露应急事件

（一）　事件概述

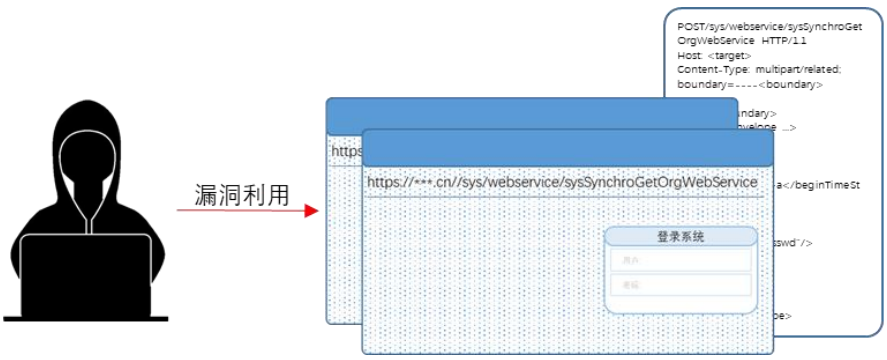
2025 年 1 月，奇安信安服应急响应团队接到教育培训行业某客户求助，客户反馈收到上级单位通报：存在非法登录，以及加密数据通讯，希望进行排查溯源。

应急人员抵达客户现场后，根据通报线索在流量监测平台进行筛查，确认存在符合通报信息的流量记录：可疑 IP：x.x.x.175 访问网关 x.x.x.186:443。

应急人员通过排查网关（x.x.x.186）的访问日志以及蓝凌 OA 服务器（x.x.x.224）的相关日志，确认攻击者通过利用/sys/webservice/sysSynchroGetOrgWebService 接口存在的任意文件读取漏洞以及 SQL 注入漏洞，拼接出配置文件路径并获取明文密码后，成功登录蓝凌 OA 服务器（x.x.x.224）进行了数据查询以及关键字全文搜索。

2025 年 3 月 3 日，客户反馈按照建议联系厂商进行漏洞修复并禁用 admin 账号后，再次收到上级单位类似通报。应急人员通过排查测试后确认 sys/webservice/sysSynchroGetOrgWebService 接口存在新的绕过方式被攻击者利用。应急人员通过排查蓝凌 OA 系统的登录日志及操作日志，未发现异常行为，判断攻击者未成功登录。在建议客户联系厂商对该接口进行二次修复后，此次应急结束。

根据以上排查信息，可确认，由于蓝凌 OA 系统的 sys/webservice/sysSynchroGetOrgWebService 接口存在任意文件读取漏洞和 SQL 注入漏洞，被攻击者利用成功获取 admin 账号密码。随后，攻击者登录蓝凌 OA 系统进行数据查询，获取用户信息。在客户禁用 admin 账号并联系厂商修复漏洞后，利用新的绕过方式再次尝试登录。



（二）　相关安全建议

1) 服务器定期维护，部署服务器安全防护系统，修复系统应用漏洞、中间件漏洞、组件、插件等相关漏洞，保障服务器安全；

2) 有效加强访问控制 ACL 策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员 IP 可对管理端口进行访问，如 FTP、数据库服务、远程桌面等管理端口；

3) 定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患；

4) 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。

二、 某企业中 Beast 勒索应急事件

(一) 事件概述

2025 年 3 月，奇安信安服应急响应团队接到医疗卫生行业某客户求助，客户反馈域内多台服务器被加密，导致近八成服务瘫痪，需要进行协助排查分析并溯源。

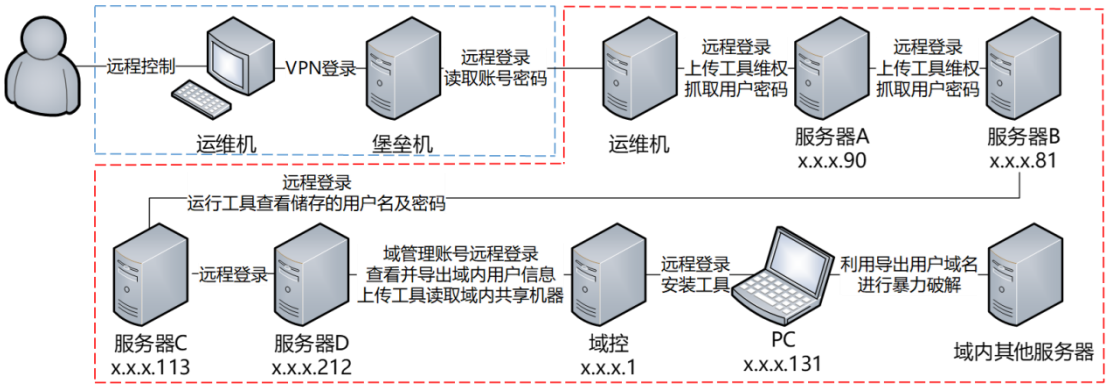
应急人员到达现场后，和客户现场人员沟通了解到 ESXI、域控服务器以及多台 Linux 和 Windows 机器被加密。其中，Windows 机器上的加密样本已被清理，而 Linux 机器上仍存在加密程序。通过分析该加密程序并结合勒索信等信息，确认客户服务器感染 Beast 勒索病毒，暂时无法解密。

应急人员通过查看运维服务商的堡垒机录像回放记录，发现攻击者通过堡垒机登录到客户的运维机器，并利用运维机上密码本中记录的账号密码远程登录至服务器 A（x.x.x.90）。随后，上传黑客工具进行权限维持、扫描内网以及密码抓取，不断横向登录至域控服务器（x.x.x.1），查看导出域内所有用户信息后，上传域内共享查询工具获取文件。通过域控服务器（x.x.x.1）登录到 PC（x.x.x.131），抓取到数据库密码和医院 Web 系统密码，并利用导出的域用户名进行 SSH 暴力破解。

应急人员通过上机排查其余失陷 Linux 机器，均发现在 C:\ProgramDate\目录下存在加密程序，并且在远程登录记录中存在 PC（x.x.x.131）成功登录记录。

最后，应急人员将排查结果与客户进行了同步，同时得到客户反馈：由于运维服务商的运维机器被控制，导致密码泄露，攻击者通过 VPN 登录到了堡垒机。

根据以上排查信息，可确认，攻击者通过获取运维服务商运维机器的控制权，在窃取到 VPN 凭证后登录到堡垒机，并登录至客户的运维机器。随后，利用在运维机器上密码本中获取到的账号密码，远程登录至服务器 A（x.x.x.90），并逐步渗透至域控服务器（x.x.x.1）获取域内所有用户名。最后，通过域控服务器（x.x.x.1）远程登录至 PC（x.x.x.131），利用导出的域用户名对 SSH 服务进行暴力破解，成功登录域内其他服务器获取权限后投放勒索病毒。



（二） 相关安全建议

1） 采用多因素认证（MFA）保护运维机器，避免仅依赖密码；

2） 限制运维机器的网络暴露面，仅允许特定 IP 或跳板机访问；

3） 有效加强访问控制 ACL 策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，采用白名单机制只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员 IP 可对管理端口进行访问，如 FTP、数据库服务、远程桌面等管理端口。

三、 某企业感染 kswapd0 挖矿病毒应急事件

（一） 事件概述

2025 年 4 月，奇安信安服应急响应团队接到制造业某客户求助，客户反馈单位内多台服务器感染挖矿木马，需要进行排查溯源。

应急人员抵达客户现场后，通过和运维人员沟通了解到，单位内多台服务器感染挖矿木马，其中服务器（x.x.x.1）对外开放 SSH 服务，疑似为最初失陷机器。

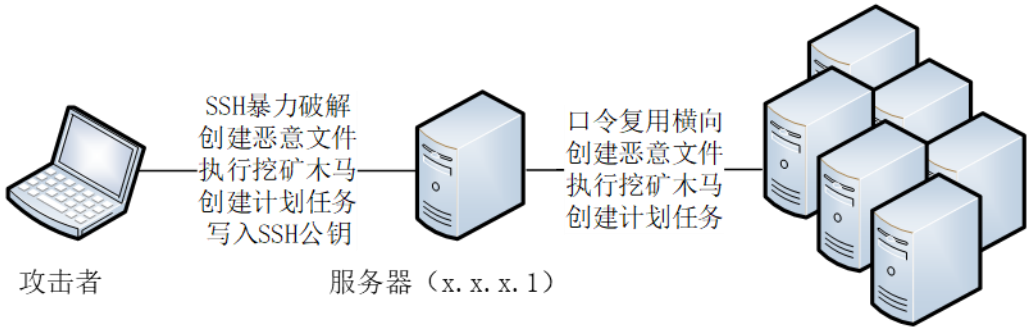
应急人员通过排查服务器（x.x.x.1），发现在/tmp 目录下存在挖矿木马文件 kswapd00；在/root/configrc7 目录下存在多个可疑文件。经分析确认其中 a 文件用于检测/清除挖矿僵尸网络，同时执行 run 文件来启动 kswapd00 挖矿程序，调用 stop 文件执行 init01 文件清理系统；b 文件用于执行 stop01 文件终止预设进程，同时执行 run01 文件进行端口扫描、DDOS 攻击、反向 Shell 以及状态回传。

应急人员通过进一步排查服务器（x.x.x.1），发现攻击者在/root/.ssh 目录下植入了 SSH 公钥，并添加了多个可疑计划任务，通过循环写入和执行机制维持挖矿进程，导致木马持续重启。在 SSH 登录日志中存在 IP（170.106.84.72）登录成功记录，并且在此之前半个小时内有多次登录失败记录。查询发现其为境外 IP 地址，并且被多个威胁情报平台标记为 SSH 暴力破解恶意 IP。

应急人员通过排查其余受害服务器发现：服务器上的恶意程序已于 2025 年 4 月 9 日被统一清除；每台服务器上均存在与服务器（x.x.x.1）相同的恶意计划任务；在/tmp 目录下均存在 up.txt 文件，其中记录的 root 用户 SSH 登录密码与服务器（x.x.x.1）的凭证一致，并且在

secure 日志中存在服务器（x.x.x.1）的 SSH 登录记录。

根据以上排查信息，可确认，由于服务器（x.x.x.1）对外开放 SSH 服务并且存在弱口令，攻击者通过暴力破解成功登录该服务器。随后，在服务器（x.x.x.1）上创建恶意文件、执行挖矿木马、创建计划任务、写入 SSH 公钥进行权限维持，并通过计划任务维持挖矿木马长期后台静默运行。最后，通过口令复用横向至其他服务器投放挖矿病毒。



（二） 相关安全建议

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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；

3) 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；

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。

四、 某企业员工遇钓鱼感染银狐木马应急事件

（一） 事件概述

2025 年 5 月，奇安信安服应急响应团队接到制造业某客户求助，客户反馈公司内某终端被远程控制，通过企业钉钉创建群聊并传播钓鱼文件，导致有员工被钓鱼造成财产损失，需要进行排查溯源。

应急人员抵达客户现场后，与客户沟通了解到被控终端为近期启用，并且使用者于 5 月 21 日在网上下载安装了多个办公软件，该行为疑似与此次事件有关。

应急人员根据该线索对被控终端的浏览器访问下载记录进行排查，发现存在访问网站：https://www.ddings.work，并下载文件：2025Dingding-05-18 下载.zip 的可疑记录，下载时间为 2025 年 5 月 21 日 15：39。通过对比分析，确认该网站为假冒的钓鱼网站，非钉钉官方网站。

随后，应急人员通过上机排查被控终端，发现通过钓鱼网站下载的文件：2025Dingding-05-18 下载.zip 已被移至回收站。通过提取分析该文件为银狐钓鱼样本，运行后会依次加载两段

自身携带的 payload，一部分是大小为 0xDD4 的 Raw Binary Shellcode，第二部分是大小为 948KB 的 PE 文件。Shellcod 用于将第二部分的 PE 文件加载到内存中并执行特定导出函数。PE 文件是一个用于维持权限以及启动后门进程的辅助模块，通过启动系统服务进程并注入远控模块，同时创建三个文件：SbieDll64.exe、SbieDll.dll、SbieDll.bin，并写入计划任务进行权限维持。被感染的常驻系统进程中的后门模块将回连攻击者，使其具备远程控制终端的权限。

应急人员通过进一步排查被控终端，在 C:\Program Files\Internet Explorer\目录下发现释放的恶意文件：SbieDll64.exe、SbieDll.bin，未发现其他异常。通过排查终端上安装的杀毒软件，在隔离区中找到恶意文件：SbieDll.dll，以及可疑计划任务。分析发现，该计划任务内容为：自动执行 C:\Program Files\Internet Explorer\SbieDll64.exe。

最后，应急人员协助客户对残留恶意文件进行清除，并建议对该企业钉钉账号做出封禁，此次应急结束。

本次事件，由于企业员工安全意识不足，在钓鱼网站中下载了捆绑有恶意程序的软件，安装后导致终端感染银狐木马。随后，攻击者通过远程控制该终端，通过企业钉钉创建多个群聊传播恶意文件进行钓鱼。

（二） 相关安全建议

1) 加强人员安全意识培养，强调网络安全重要性，禁止通过非官方渠道下载应用软件。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；

3) 配置并开启相关关键系统、应用日志，对系统日志进行定期异地归档、备份，避免在攻击行为发生时，导致无法对攻击途径、行为进行溯源等，加强安全溯源能力；

4) 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。

五、 某机构被植入 SEO 黑链应急事件

（一） 事件概述

2025 年 8 月，奇安信安服应急响应团队接到金融机构某客户求助，客户反馈被通报存在外联通信，希望进行排查溯源。

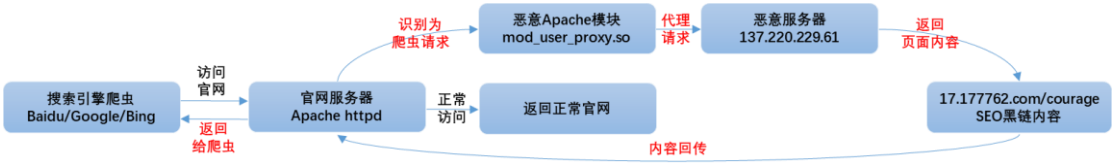
应急人员抵达客户现场后，通过排查 Linux 服务器网络连接，发现存在多个 Apache 进程连接 x.x.x.61:80 端口的记录。通过调试 Apache 的 httpd 进程，发现进程记录中存在 httpd 进程向 DNS 服务器（x.x.x.99）查询了 17.177762.com 的解析记录，并得到外部 IP 地址 137.220.229.61。随后，应急人员以该 IP 为线索进一步排查 Apache 目录，在./modules/mod_user_proxy.so 文件中发现异常字符。经过分析，发现该模块的工作逻辑为：当请求地址为爬虫时，返回 17.177762.com/courage 页面的内容。将 17.177762.com/courage 保存为文件后，其大小为 1326KB。

应急人员通过进一步排查发现，mod_user_proxy.so 模块于 4 月 4 日 21:32 被修改。在 Apache 目录中查找该模块时，发现 http.conf 配置文件于 7 月 11 日 10:44 被修改并加载了该模块。通过与客户沟通确认，7 月 11 日服务器曾出现网站无法访问的情况，管理员通过宝塔面板升级了应用程序，并于 7 月 11 日 10:48 重启了服务器。

经统计，8 月 18 日 Web 日志中共记录了 42589 次爬虫访问。若每次爬虫访问官网时均触发 mod_user_proxy.so 模块并返回 17.177762.com/courage 页面，则官网服务器将向 137.220.229.61 发起 42,589 次请求，对方累计返回约 55,149MB 数据。据此判断，官网服务器在当日被利用作为内容分发中转节点，其与 137.220.229.61 之间的通信内容主要为请求并转发 17.177762.com/courage 页面数据。

应急人员在服务器中发现，此前存在 Webshell 文件，但在本次应急响应前已被查杀。查看 4 月 4 日、7 月 11 日的 Web 日志，未发现访问后门的记录。2024 年 11 月 26 日，官网曾出现 SEO 黑链情况：访问 https://www.fsig.com.cn/yyds/8fy1kl/等网址时，链接至恶意小说网站。当时通过查杀发现多个 Webshell 文件，涉及时间跨度从 2019 年至 2023 年。

至此，应急人员判断，攻击者具备长期入侵服务器并获取高权限的能力。结合历史多次发现的 Webshell 及当前 Apache 核心模块被篡改的情况，推测攻击者可能利用此前遗留的 Webshell 或其他管理入口访问服务器，进而植入恶意 Apache 模块，并通过识别爬虫访问触发内容代理行为，利用爬虫流量发起大规模外联请求，最终导致异常网络通信。



（二） 相关安全建议

1) 管控服务器的端口：只对公网开放静态页面的访问端口（如 80，443），其余端口全部禁止在公网访问。网站后台等管理端只能在内网访问，且限制内网访问的来源 IP 或 IP 段；

2) 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；

3) 定期开展对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患；

4) 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。

六、 某企业 OldFox APT 应急事件

（一） 事件概述

2025 年 11 月，奇安信安服应急响应团队接到媒体行业某客户求助，客户反馈阿里云平台的态势感知发现服务器被植入恶意文件，同时存在权限维持的操作，需要进行应急排查。

应急人员抵达客户现场后，通过查看态势感知系统发现阿里云主机（x.x.x.150）存在异常告警。根据告警情况排查，发现存在后门程序/usr/local/lib/libluajit-5.1.so.2.0.0，更改时间为 2025 年 11 月 19 日 13:50。登录日志显示，服务器（x.x.x.120）于 2025 年 11 月 19 日 13:09 成功登录。

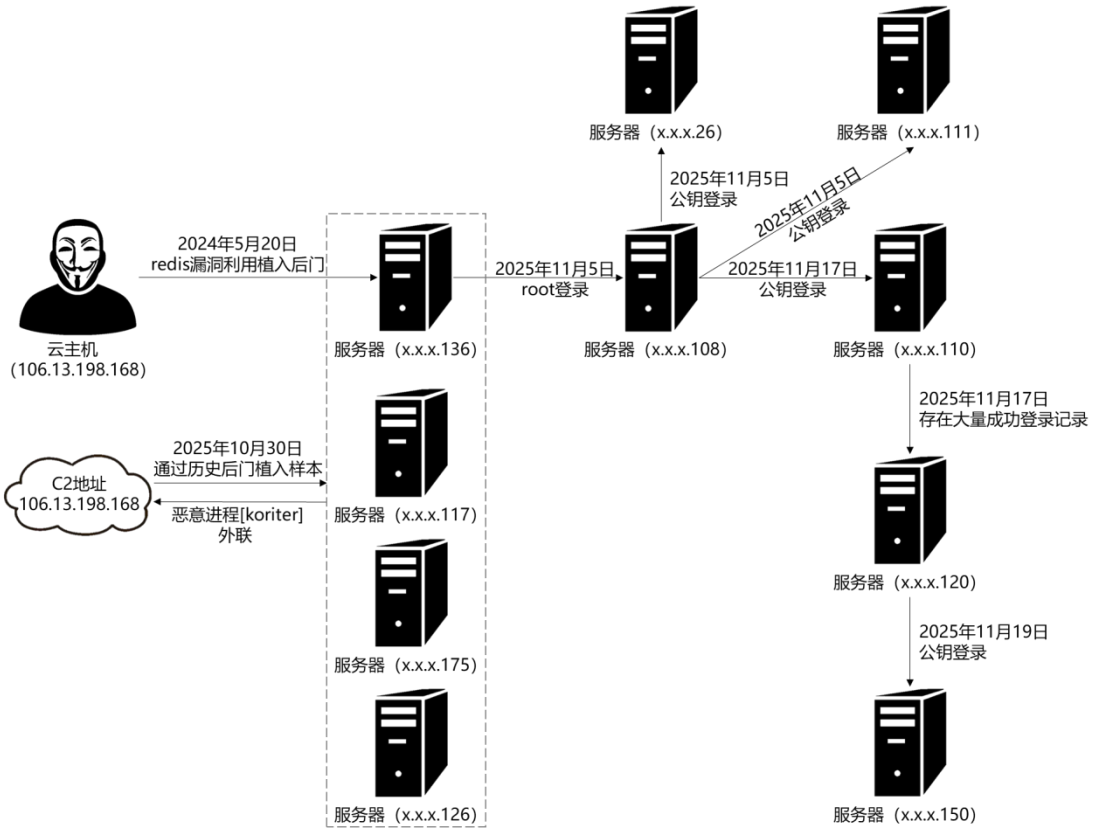
应急人员通过排查服务器（x.x.x.120）发现 init.d 目录下的 network 文件于 2025 年 11 月 17 日 15:09 被篡改插入恶意配置。系统文件中还存在以下可疑文件：/usr/lib/libthread、/usr/local/lib/libluajit-5.1.so.2.0.0、/usr/local/lib64/libpng.so.2。通过分析系统登录日志,发现在文件被篡改前登录日志中存在大量来自服务器(x.x.x.110)的异常登录尝试。

应急人员通过排查服务器（x.x.x.110）登录日志，发现存在服务器（x.x.x.108）于 2025 年 11 月 17 日 14:29 成功登录记录。排查服务器（x.x.x.108）发现 init.d 目录下 network 文件于 2025 年 11 月 5 日 14:56 被篡改；yum 安装日志显示在 2025 年 11 月 5 日 15:35 安装了可疑工具 nmap；登录日志显示服务器（x.x.x.136）于 2025 年 11 月 5 日 13:54 通过 root 账户登录成功。

应急人员通过排查服务器（x.x.x.136）发现 init.d 目录下 network 文件于 2025 年 10 月 30 日 13:13 被篡改插入恶意配置；存在恶意文件/usr/lib/libthread、/usr/local/lib/libluajit-5.1.so.2.0.0、/usr/local/lib64/libpng.so.2，落地时间为 2025 年 10 月 30 日；存在可疑进程 koriter 外联 IP 为 106.13.198.168，PID 为 18083。提取样本进行分析发现，该恶意样本连接域名 r3qr.fun，属于 APT 组织 OldFox。通过查看进程对应的服务，发现程序开始运行时间为 2024 年 5 月 20 日 18:44，已运行一年六个月。进一步排查其他文件，发现 ssh/ser/redis/redis-6379/dump.rdb/redis5.0.9 存在被恶意利用，配置计划任务反弹 shell 命令，文件更改时间为 2024 年 5 月 20 日 18:42。由于时间久远，无法确认当时部署情况。

应急人员通过排查其余存在恶意外联的异常服务器,在服务器(x.x.x.117)、(x.x.x.175)、（x.x.x.126）上均发现恶意进程 koriter 及相关文件/usr/local/lib64/libpng.so.2、/etc/rc.d/init.d/network,修改时间为 2025 年 10 月 30 日 16:35 至 16:41。由于无对应登录记录，判断为历史后门植入。在服务器（x.x.x.111）、（x.x.x.26）上均存在恶意文件/usr/local/lib64/libpng.so.2 更改时间分别为 2025 年 11 月 5 日 15:32、16:32，文件修改前存在来自服务器（x.x.x.108）的登录记录。

至此，应急人员判断，2024 年 5 月至 2025 年 11 月，攻击者通过利用 redis 漏洞成功入侵服务器（x.x.x.136）后进行长期潜伏，期间篡改系统文件、植入恶意文件并利用弱口令横向移动成功入侵服务器（x.x.x.108）、服务器（x.x.x.110）等十余台服务器。



（二） 相关安全建议

1) 在出口防火墙加入相关策略，封禁 106.13.198.168，四个随机字符串拼接.r3qr.fun 等恶意 IOC，并对服务器主动外联公网 IP 行为进行监控；

2) 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；

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、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；

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。

附录 1 95015 网络安全服务热线

2022 年 1 月 20 日，全国首个网络安全行业服务短号 95015 正式开通。95015 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 网络安全服务热线，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正式推出。在北京 2022 年冬奥会和冬残奥会期间，95015 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 网络安全服务热线将永久保留，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。

奇安信集团董事长齐向东表示，“95015 是我国第一个网络安全服务短号，是北京冬奥会网络安全保障指定号码，赛后，95015 将永久服役。95015 承载着网络安全行业的责任和使命，北京冬奥会期间，将作为网络安全保障工作的重要支撑平台，为网络安全事件的应急响应开辟一条绿色通道。全国的政企机构遇到任何网络安全问题，都可以拨打 95015，奇安信将提供 24 小时冬奥标准的应急响应服务。”

9 字头短号码是工信部统一管理的全国通用号码，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。

附录 2 奇安信集团安服团队

奇安信集团是北京 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 2018 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 6500 余起，累计投入工时 65000 多个小时，为全国超过 4000 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。奇安信集团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。