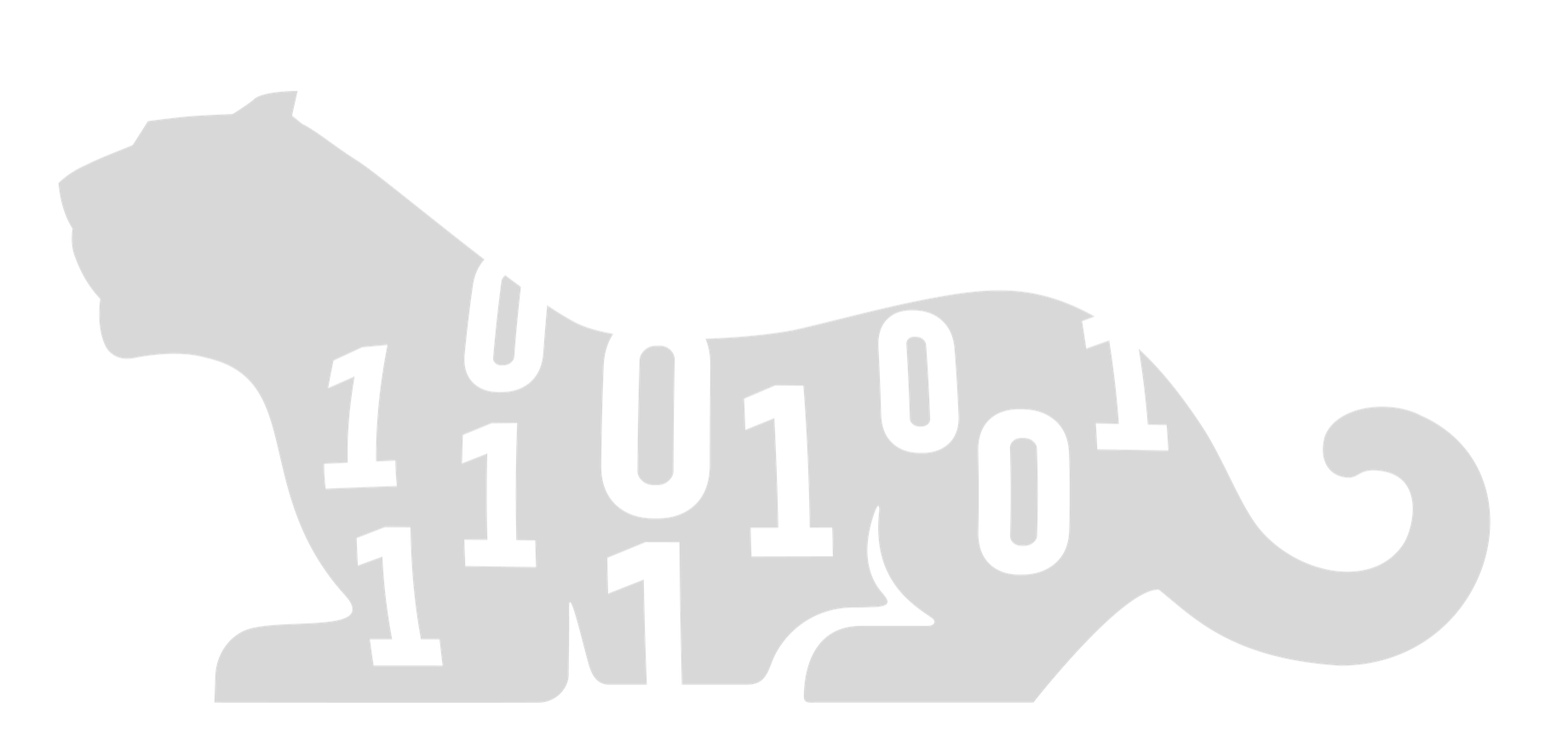
应急响应典型案例集（2021）



奇安信安服团队

2021年7月

前言

应急响应是网络安全工作中的重要组成部分，当政企机构发生重大网络安全事件时，往往意味着其背后存在着诸多的危险和隐患，应急响应事件的发生是长期网络安全监测不足，大量安全隐患未得到有效的及时处置等一系列安全问题最终隐患的集中爆发。就像一起火灾的爆发，映射着长期的消防建设不足。通过应急响应往往能够快速地发现政企机构网络安全建设中的典型不足。从应急响应事件来看，每次在应急响应结束后我们都会给政企机构提供很多的整改意见，政企机构在这些安全建议的基础上也会进行大量的建设和提高，从而避免应急事件的反复发生。我们在本书当中为大家整理了奇安信历年来处置过的几千起应急响应中精选的50个典型的案例，一方面通过网络安全应急响应事件来分析机构的安全隐患，另一方面，我们也可以通过应急响应案例来帮助更多企业，一旦发生安全事故、安全风险时有更多的经验和参考方法进行应急响应的处置，希望通过案例的分享能够帮助我们的广大政企机构提前防御、提早发现、及时处置。

通过近6年的应急响应工作，我们发现以下几个典型特点。第一，勒索病毒的攻击愈演愈烈，包括在国外发生的多起重大事件，国内也不断有相关攻击案例的发生。同时，挖矿木马也越来越流行；第二，政企机构在网络安全建设中网络安全防护存在短板，常见如：弱口令、永恒之蓝漏洞补丁下载不及时、员工缺乏安全意识等问题尤其明显；第三，应急响应事件受影响范围主要集中在业务专网，平均占比可达60%以上，其次是办公终端；第四，敲诈勒索、黑产活动是攻击者攻击政企机构的主要原因，而对政企机构所产生的后果也尤为严重，主要表现为导致生产效率低下，数据丢失和系统/网络不可用等，对政企机构日常工作和运营造成了较大影响；第五，攻击者除利用病毒和木马攻击外，利用漏洞攻击和钓鱼邮件攻击的事件也在不断增多，常见漏洞如永恒之蓝漏洞、任意文件上传、weblogic反序列化漏洞；第六，通过对这6年政企单位应急响应事件发现数据进行对比，政企机构单位自行发现能力虽逐年上升，然而，其中被攻击者勒索后才发现事件的占比却高于政企机构日常安全运营巡检发现入侵迹象的占比，这说明国内政企机构的日常安全运营建设水平仍有待大幅提高。

本书主要分为两个部分，第一部分结合2021年最新的应急响应事件通过数据来表现当前网络安全应急响应的基本形势；第二部分一共分为十个章节，分别对勒索类、挖矿类、蠕虫类、篡改类等10种类型的典型案例进行介绍，希望能够通过应急响应数据和典型案例为政企机构的日常安全建设提供参考，使应急响应事件发生的越来越少，一旦发生安全事件时响应越来越快，损失降到越来越低，这也是我们应急响应工作的主要意义。

目 录

[第一章 网络安全应急响应形势综述 1](#_Toc77865308)

[一、 应急响应事件受害者分析 2](#_Toc77865309)

[（一） 行业现状分析 2](#_Toc77865310)

[（二） 事件发现分析 2](#_Toc77865311)

[（三） 影响范围分析 3](#_Toc77865312)

[（四） 攻击影响分析 4](#_Toc77865313)

[二、 应急响应事件攻击者分析 5](#_Toc77865314)

[（一） 攻击意图分析 5](#_Toc77865315)

[（二） 攻击类型分析 5](#_Toc77865316)

[（三） 恶意程序分析 6](#_Toc77865317)

[（四） 漏洞利用分析 7](#_Toc77865318)

[第二章 勒索类事件典型案例 8](#_Toc77865319)

[一、 服务器存漏洞感染勒索病毒 8](#_Toc77865320)

[（一） 事件概述 8](#_Toc77865321)

[（二） 防护建议 8](#_Toc77865322)

[二、 终端电脑遭遇钓鱼邮件感染勒索病毒 8](#_Toc77865323)

[（一） 事件概述 8](#_Toc77865324)

[（二） 防护建议 9](#_Toc77865325)

[三、 工业生产网与办公网边界模糊，感染勒索病毒 9](#_Toc77865326)

[（一） 事件概述 9](#_Toc77865327)

[（二） 防护建议 9](#_Toc77865328)

[四、 服务器配置不当感染勒索病毒 9](#_Toc77865329)

[（一） 事件概述 9](#_Toc77865330)

[（二） 防护建议 10](#_Toc77865331)

[五、 专网被攻击，58家医院连锁感染勒索病毒 10](#_Toc77865332)

[（一） 事件概述 10](#_Toc77865333)

[（二） 防护建议 11](#_Toc77865334)

[六、 OA服务器远程桌面映射公网，感染勒索病毒 11](#_Toc77865335)

[（一） 事件概述 11](#_Toc77865336)

[（二） 防护建议 12](#_Toc77865337)

[七、 内网主机使用弱口令致感染勒索病毒 12](#_Toc77865338)

[（一） 事件概述 12](#_Toc77865339)

[（二） 防护建议 12](#_Toc77865340)

[八、 8003端口映射在公网感染勒索病毒 13](#_Toc77865341)

[（一） 事件概述 13](#_Toc77865342)

[（二） 防护建议 13](#_Toc77865343)

[九、 私自下载破解软件致服务器感染勒索病毒 13](#_Toc77865344)

[（一） 事件概述 13](#_Toc77865345)

[（二） 防护建议 14](#_Toc77865346)

[十、 服务器补丁安装不及时感染勒索病毒 14](#_Toc77865347)

[（一） 事件概述 14](#_Toc77865348)

[（二） 防护建议 14](#_Toc77865349)

[十一、 擅自修改网络配置致服务器感染勒索病毒 14](#_Toc77865350)

[（一） 事件概述 14](#_Toc77865351)

[（二） 防护建议 15](#_Toc77865352)

[十二、 用户名口令被暴力破解感染勒索病毒 15](#_Toc77865353)

[（一） 事件概述 16](#_Toc77865354)

[（二） 防护建议 16](#_Toc77865355)

[第三章 挖矿类事件典型案例 17](#_Toc77865356)

[一、 官网存在上传漏洞感染挖矿木马 17](#_Toc77865357)

[（一） 事件概述 17](#_Toc77865358)

[（二） 防护建议 17](#_Toc77865359)

[二、 误点恶意链接感染挖矿木马 17](#_Toc77865360)

[（一） 事件概述 18](#_Toc77865361)

[（二） 防护建议 18](#_Toc77865362)

[三、 软件升级包携带“永恒之蓝下载器”致专网感染挖矿木马 18](#_Toc77865363)

[（一） 事件概述 18](#_Toc77865364)

[（二） 防护建议 20](#_Toc77865365)

[四、 “永恒之蓝下载器”致内网挖矿木马 20](#_Toc77865366)

[（一） 事件概述 20](#_Toc77865367)

[（二） 防护建议 20](#_Toc77865368)

[五、 安全防护不到位致终端和服务器感染挖矿木马 21](#_Toc77865369)

[（一） 事件概述 21](#_Toc77865370)

[（二） 防护建议 21](#_Toc77865371)

[六、 SSH私钥本地保存致虚拟机感染挖矿木马 22](#_Toc77865372)

[（一） 事件概述 22](#_Toc77865373)

[（二） 防护建议 22](#_Toc77865374)

[七、 网站存漏洞致服务器感染挖矿木马 22](#_Toc77865375)

[（一） 事件概述 23](#_Toc77865376)

[（二） 防护建议 23](#_Toc77865377)

[八、 服务器使用弱口令导致感染挖矿木马 24](#_Toc77865378)

[（一） 事件概述 24](#_Toc77865379)

[（二） 防护建议 24](#_Toc77865380)

[九、 应用服务平台使用弱口令导致感染挖矿木马 24](#_Toc77865381)

[（一） 事件概述 24](#_Toc77865382)

[（二） 防护建议 25](#_Toc77865383)

[十、 U盘未管控导致主机感染挖矿木马 25](#_Toc77865384)

[（一） 事件概述 25](#_Toc77865385)

[（二） 防护建议 25](#_Toc77865386)

[第四章 蠕虫类事件典型案例 27](#_Toc77865387)

[一、 服务器弱口令导致感染蠕虫病毒 27](#_Toc77865388)

[（一） 事件概述 27](#_Toc77865389)

[（二） 防护建议 27](#_Toc77865390)

[二、 浏览恶意链接感染蠕虫病毒 28](#_Toc77865391)

[（一） 事件概述 28](#_Toc77865392)

[（二） 防护建议 28](#_Toc77865393)

[三、 U盘未合理管控导致感染蠕虫病毒 28](#_Toc77865394)

[（一） 事件概述 28](#_Toc77865395)

[（二） 防护建议 29](#_Toc77865396)

[第五章 篡改类事件典型案例 30](#_Toc77865397)

[一、 Redis未授权访问漏洞致官网被植入黑链 30](#_Toc77865398)

[（一） 事件概述 30](#_Toc77865399)

[（二） 防护建议 30](#_Toc77865400)

[二、 网站WEB漏洞致网站被挂马 30](#_Toc77865401)

[（一） 事件概述 31](#_Toc77865402)

[（二） 防护建议 31](#_Toc77865403)

[三、 网站后台程序漏洞致网站被植入黑链 31](#_Toc77865404)

[（一） 事件概述 31](#_Toc77865405)

[（二） 防护建议 32](#_Toc77865406)

[四、 Tomcat中间件漏洞致官网被上传博彩页面 32](#_Toc77865407)

[（一） 事件概述 32](#_Toc77865408)

[（二） 防护建议 32](#_Toc77865409)

[五、 Weblogic WLS组件漏洞致网页被篡改 32](#_Toc77865410)

[（一） 事件概述 33](#_Toc77865411)

[（二） 防护建议 33](#_Toc77865412)

[六、 weblogic反序列化漏洞致网页被篡改 33](#_Toc77865413)

[（一） 事件概述 33](#_Toc77865414)

[（二） 防护建议 34](#_Toc77865415)

[七、 官网存在SQL注入漏洞致网页被篡改 34](#_Toc77865416)

[（一） 事件概述 34](#_Toc77865417)

[（二） 防护建议 35](#_Toc77865418)

[八、 编辑器漏洞致网站被挂黑页 35](#_Toc77865419)

[（一） 事件概述 35](#_Toc77865420)

[（二） 防护建议 36](#_Toc77865421)

[第六章 APT类事件典型案例 37](#_Toc77865422)

[一、 APT组织利用弱口令进行攻击 37](#_Toc77865423)

[（一） 事件概述 37](#_Toc77865424)

[（二） 防护建议 37](#_Toc77865425)

[二、 APT组织利用"白+黑"技术进行攻击 38](#_Toc77865426)

[（一） 事件概述 38](#_Toc77865427)

[（二） 防护建议 38](#_Toc77865428)

[三、 APT组织利用外泄的账号密码进行攻击 38](#_Toc77865429)

[（一） 事件概述 38](#_Toc77865430)

[（二） 防护建议 39](#_Toc77865431)

[四、 APT组织利用钓鱼邮件进行攻击 39](#_Toc77865432)

[（一） 事件概述 39](#_Toc77865433)

[（二） 防护建议 40](#_Toc77865434)

[第七章 DDOS类事件典型案例 41](#_Toc77865435)

[一、 某部委遭遇CC攻击 41](#_Toc77865436)

[（一） 事件概述 41](#_Toc77865437)

[（二） 防护建议 41](#_Toc77865438)

[二、 某证券公司遭遇DDoS攻击 41](#_Toc77865439)

[（一） 事件概述 41](#_Toc77865440)

[（二） 防护建议 42](#_Toc77865441)

[第八章 漏洞利用类事件典型案例 43](#_Toc77865442)

[一、 内网防护不到位致大量主机失陷 43](#_Toc77865443)

[（一） 事件概述 43](#_Toc77865444)

[（二） 防护建议 43](#_Toc77865445)

[二、 网站存在任意文件上传漏洞，致多台主机沦陷 44](#_Toc77865446)

[（一） 事件概述 44](#_Toc77865447)

[（二） 防护建议 44](#_Toc77865448)

[三、 服务器因SQL注入漏洞被攻陷 44](#_Toc77865449)

[（一） 事件概述 44](#_Toc77865450)

[（二） 防护建议 45](#_Toc77865451)

[四、 机顶盒配置不当致堡垒机被攻陷 45](#_Toc77865452)

[（一） 事件概述 45](#_Toc77865453)

[（二） 防护建议 46](#_Toc77865454)

[五、 公网应用平台因Shiro反序列化漏洞被攻击 46](#_Toc77865455)

[（一） 事件概述 46](#_Toc77865456)

[（二） 防护建议 46](#_Toc77865457)

[第九章 钓鱼邮件类事件典型案例 48](#_Toc77865458)

[一、 利用钓鱼邮件，伪造打款信息 48](#_Toc77865459)

[（一） 事件概述 48](#_Toc77865460)

[（二） 防护建议 48](#_Toc77865461)

[二、 破解管理员弱密码，发起钓鱼邮件攻击 48](#_Toc77865462)

[（一） 事件概述 48](#_Toc77865463)

[（二） 防护建议 49](#_Toc77865464)

[三、 下载破解软件，导致内网终端自动发送恶意邮件 49](#_Toc77865465)

[（一） 事件概述 49](#_Toc77865466)

[（二） 防护建议 50](#_Toc77865467)

[第十章 数据泄露类事件典型案例 51](#_Toc77865468)

[一、 账号信息上传公网，致内网20多台机器受感染 51](#_Toc77865469)

[（一） 事件概述 51](#_Toc77865470)

[（二） 防护建议 51](#_Toc77865471)

[二、 系统漏洞造成数据泄露 51](#_Toc77865472)

[（一） 事件概述 51](#_Toc77865473)

[（二） 防护建议 52](#_Toc77865474)

[第十一章 僵尸网络类事件典型案例 53](#_Toc77865475)

[一、 安全设备弱口令致内网被僵尸网络控制 53](#_Toc77865476)

[（一） 事件概述 53](#_Toc77865477)

[（二） 防护建议 53](#_Toc77865478)

[附录1 奇安信集团安服团队 54](#_Toc77865479)

[附录2 应急响应工具箱介绍 55](#_Toc77865480)

1. 网络安全应急响应形势综述

2021年1—6月，奇安信集团安服团队共参与和处置了全国范围内590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年上半年应急响应服务月度统计情况具体如下：**

2021年上半年，奇安信安服共处置应急响应事件590起，投入工时为3964.5小时，折合495.6人天。

（2021年4月为全国实战攻防演习期间，应急数量大幅增加。）

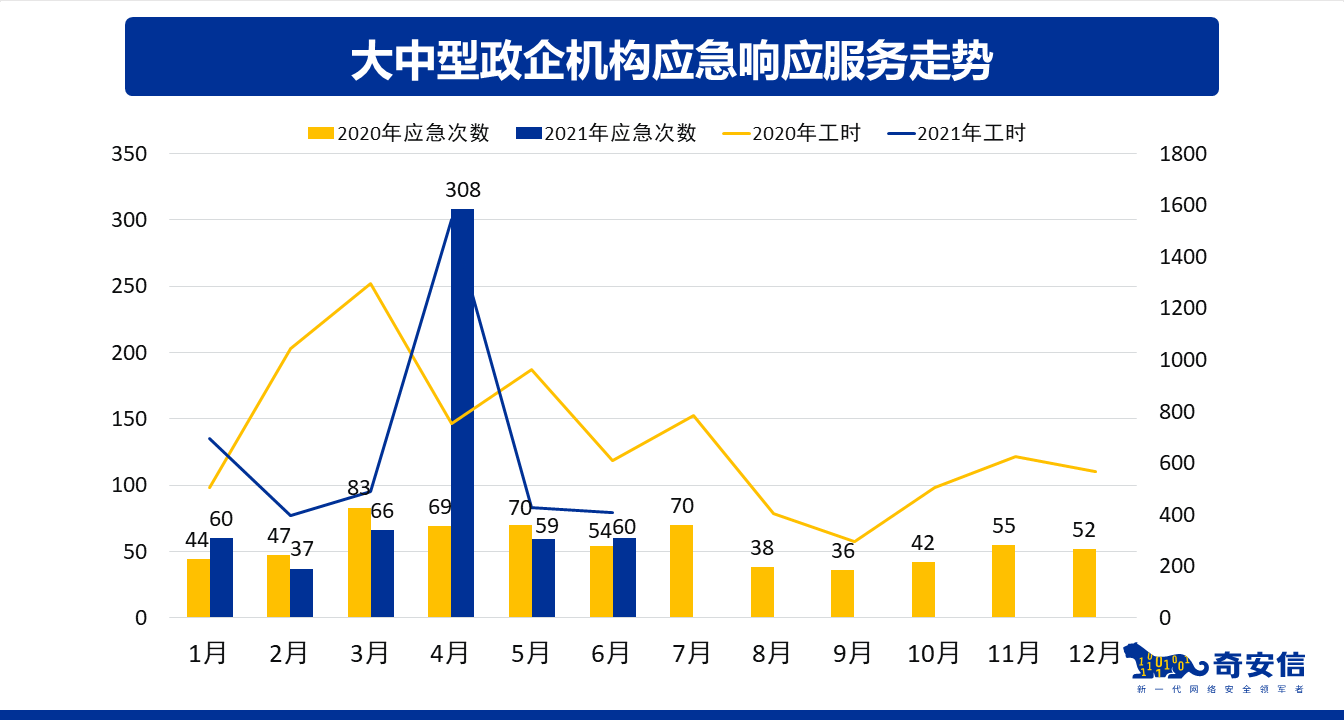


图1-1：大中型政企机构应急响应服务走势

1. 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年上半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，呈现上半年政企机构内部网络安全现状。

### 行业现状分析

2021年上半年应急响应处置事件排名靠前的行业分别为，政府部门（140起）、医疗卫生行业（58起）以及金融行业（49起）和事业单位（49起），事件处置数分别占上半年应急处置事件的23.7%、9.8%、8.3%和8.3%。

大中型政企机构应急响应行业分布TOP10详见下图：

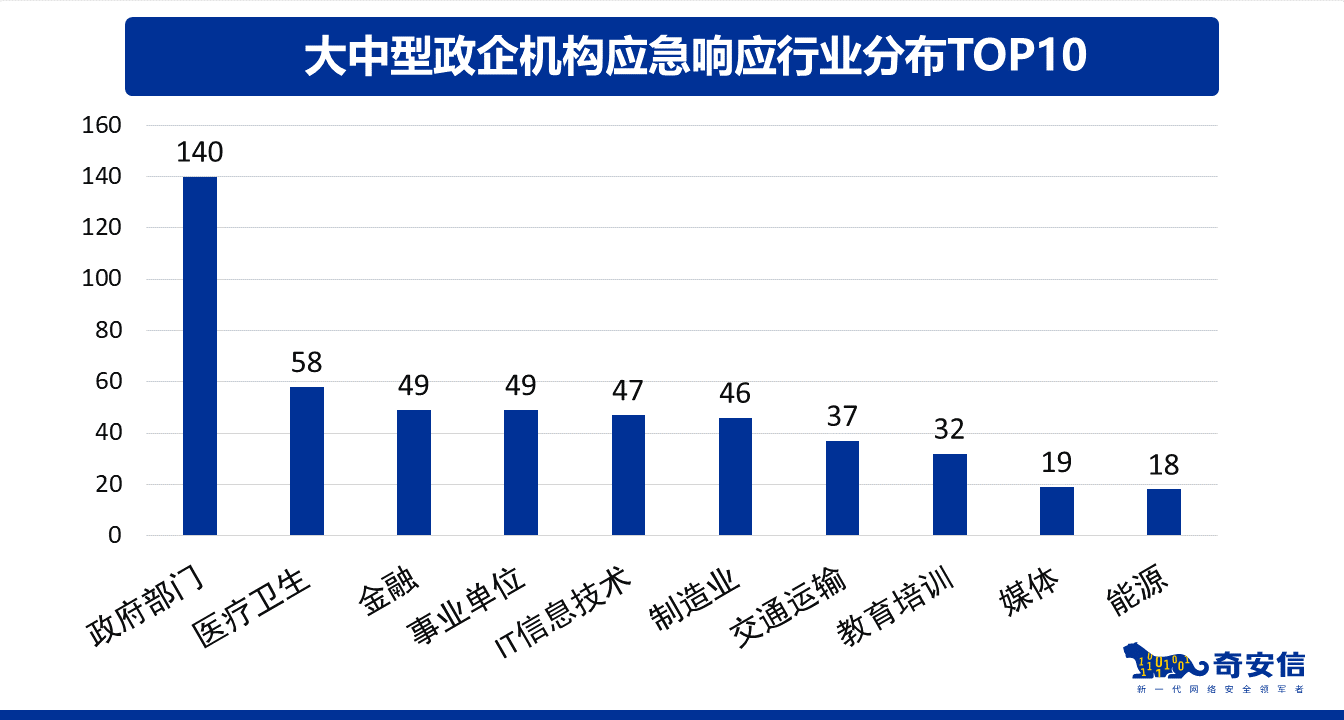


图1-2：大中型政企机构应急响应行业分布

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

### 事件发现分析

2021年上半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95.2%，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35.1%，安全运营巡检发现的事件占比20.5%。另有4.8%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。

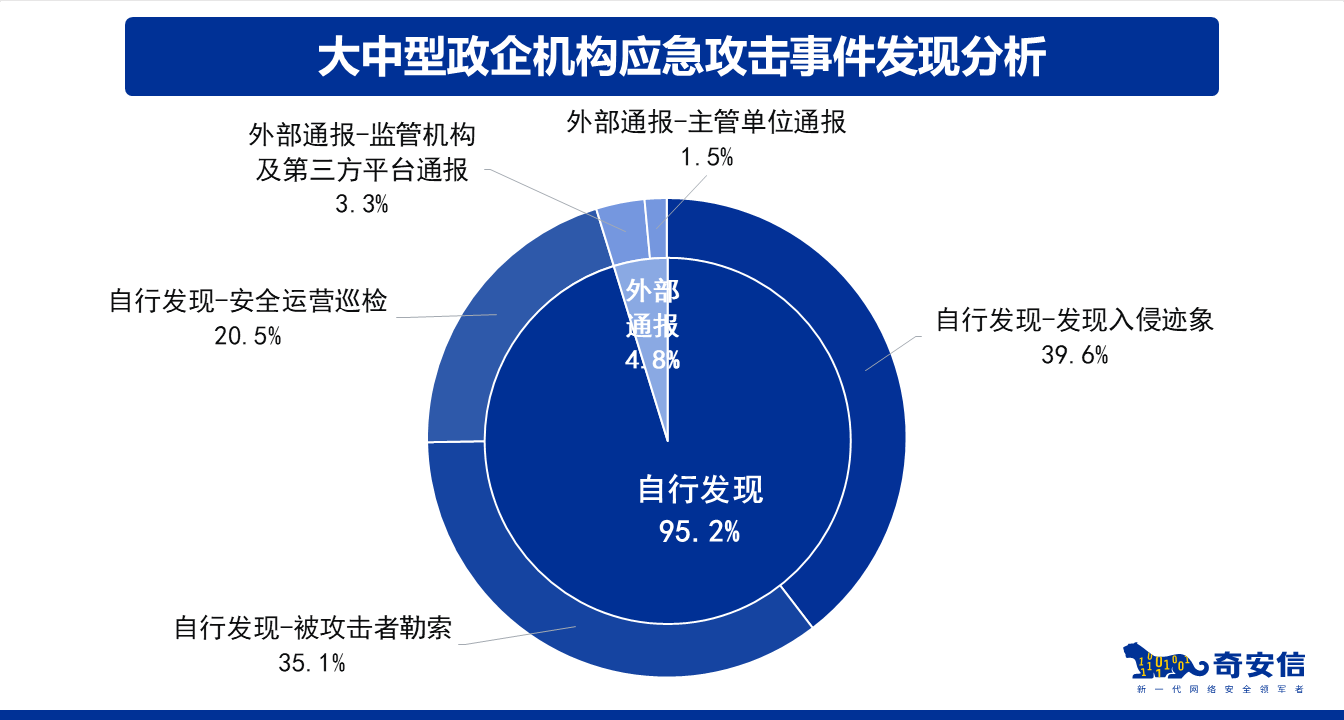


图1-3：大中型政企机构应急攻击事件发现分析

### 影响范围分析

2021年上半年应急响应事件的影响范围主要集中在业务专网，占比67.9%；其次为办公终端，占比32.1%。根据受影响区域分布对受影响设备数量进行了统计，上半年失陷的设备中，9284台服务器受到影响，2373台办公终端被攻陷，如下图所示。

本文中办公终端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。

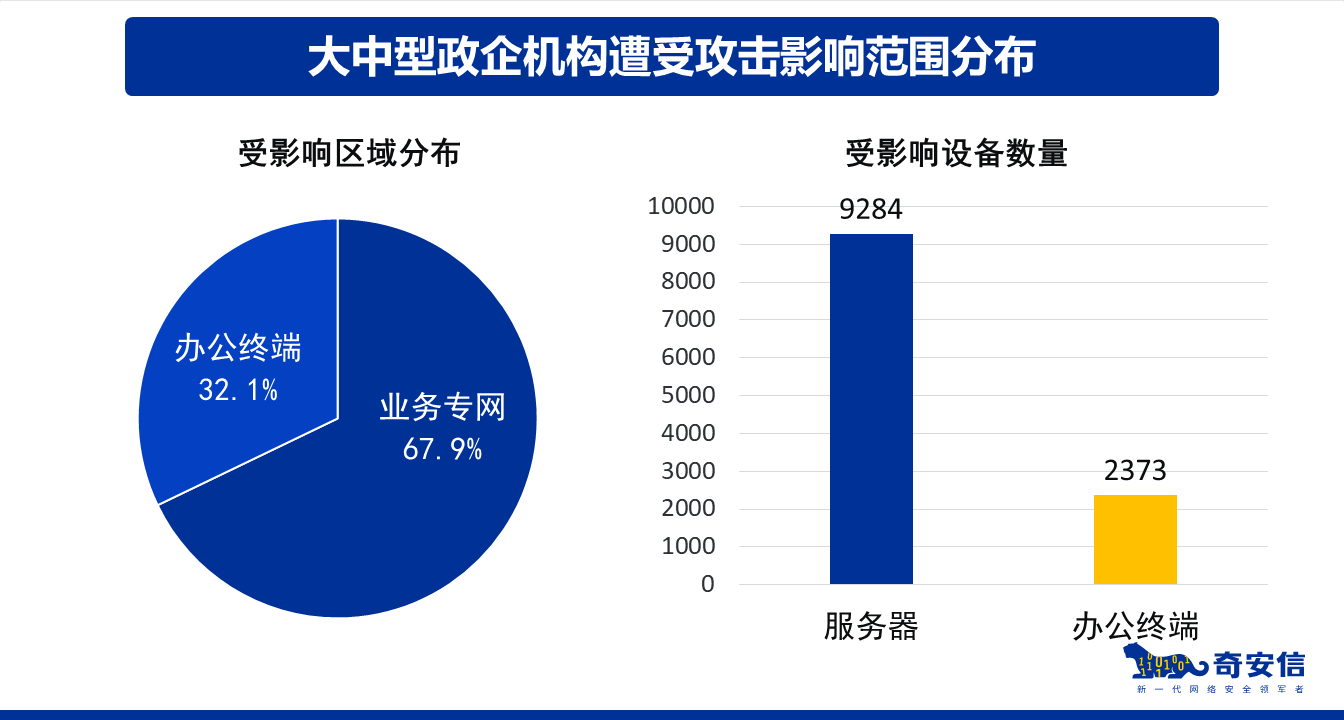


图1-4：大中型政企机构遭受攻击影响范围分布

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，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。

### 攻击影响分析

2021年上半年，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、声誉影响等。下图为大中型政企机构遭受攻击后的影响分布。

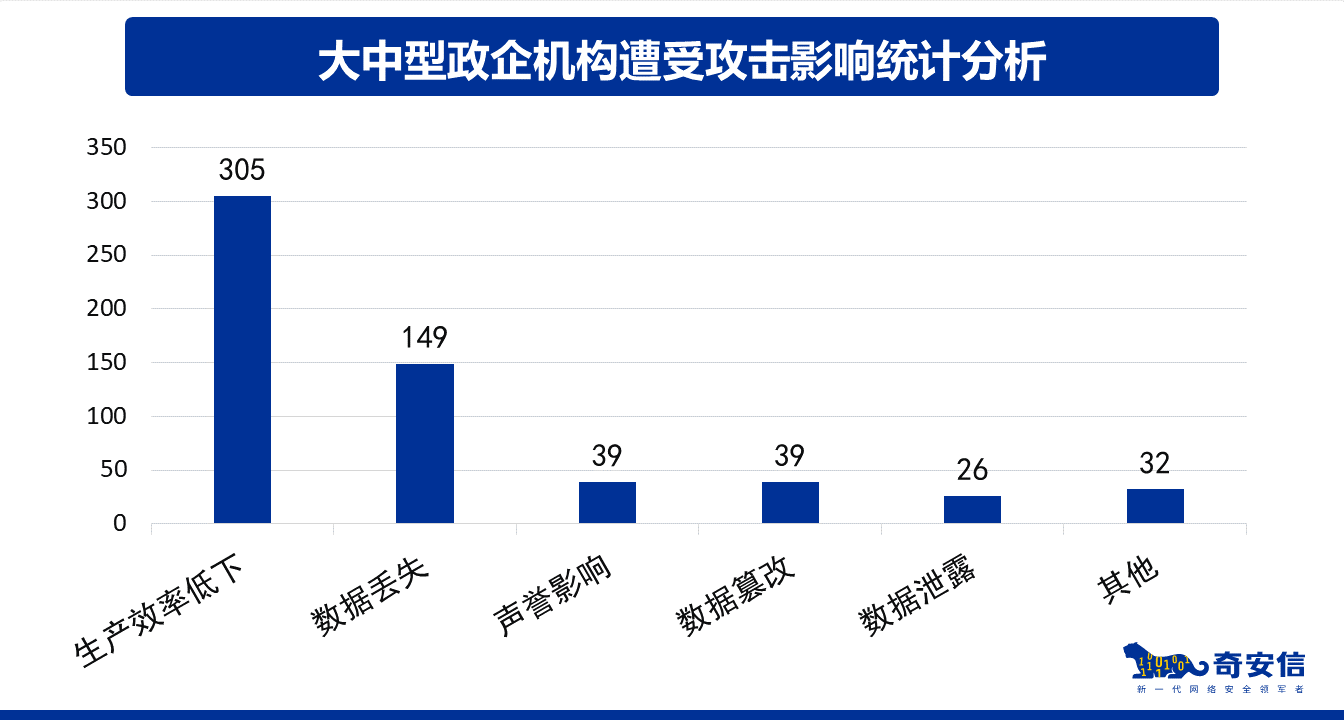


图1-5：大中型政企机构遭受攻击影响统计分析

在上述数据中，有305起应急响应事件导致生产效率低下，占比51.7%，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149起应急响应事件导致数据丢失，占比25.3%，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。

还有39起应急响应事件导致声誉受到影响占比6.6%。同时，数据被篡改、数据泄露等也是政企机构被攻击后产生的结果，造成的后果也是非常严重的。

1. 应急响应事件攻击者分析

应急响应事件攻击者分析以2021年上半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。

### 攻击意图分析

在2021年上半年的应急响应事件中，攻击者攻击意图主要为敲诈勒索、黑产活动、窃取重要数据和内部违规操作。

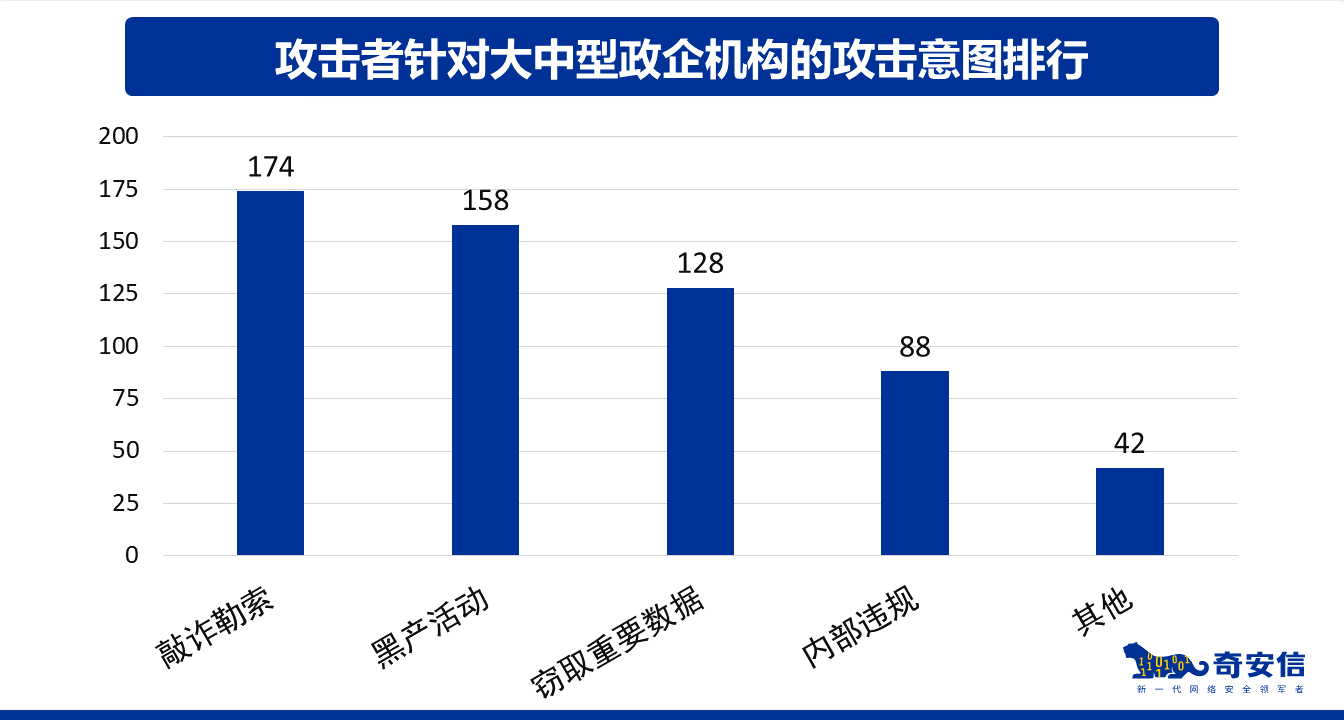


图1-6：攻击者针对大中型政企机构的攻击意图排行

在2021年上半年应急响应事件中，174起事件的攻击原因为敲诈勒索，占比29.5%，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，实现自身最大利益。

158起事件的攻击原因为黑产活动，占比26.8%，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；另外还有128起应急响应事件会导致重要数据被窃取，占上半年应急响应事件的21.7%。

在88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。

### 攻击类型分析

通过对2021年上半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48.8%；漏洞利用占比29.8%；网络监听攻击占比8.0%。在恶意程序中，木马攻击（非蠕虫病毒）占比53.0%，蠕虫病毒攻击占比47.0%。

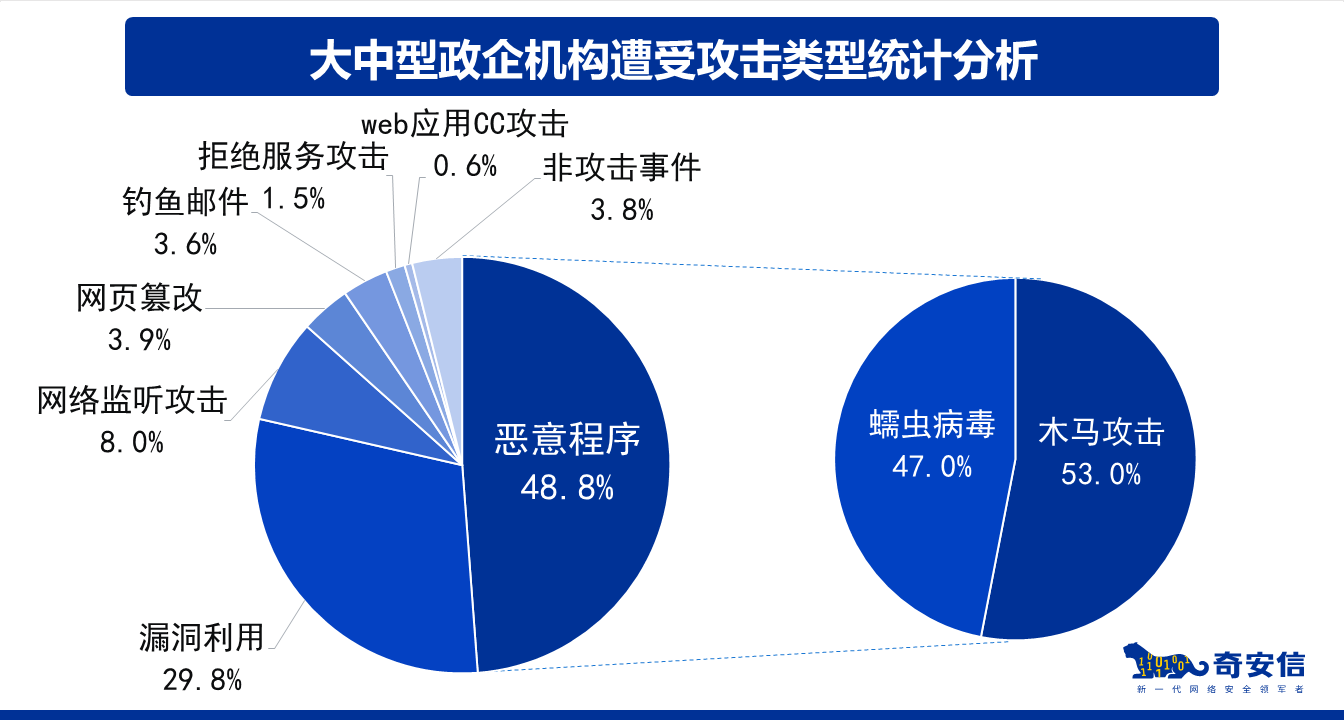


图1-7：大中型政企机构遭受攻击类型统计分析

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。

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，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、网页篡改、钓鱼邮件等也是较为常见的攻击类型。因此，大中型政企机构应做好日常安全防范工作，定期巡检，及时发现威胁并有效遏制。

### 恶意程序分析

在2021年上半年，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30.4%，挖矿木马占比18.8%，以及一般木马占比17.3%。

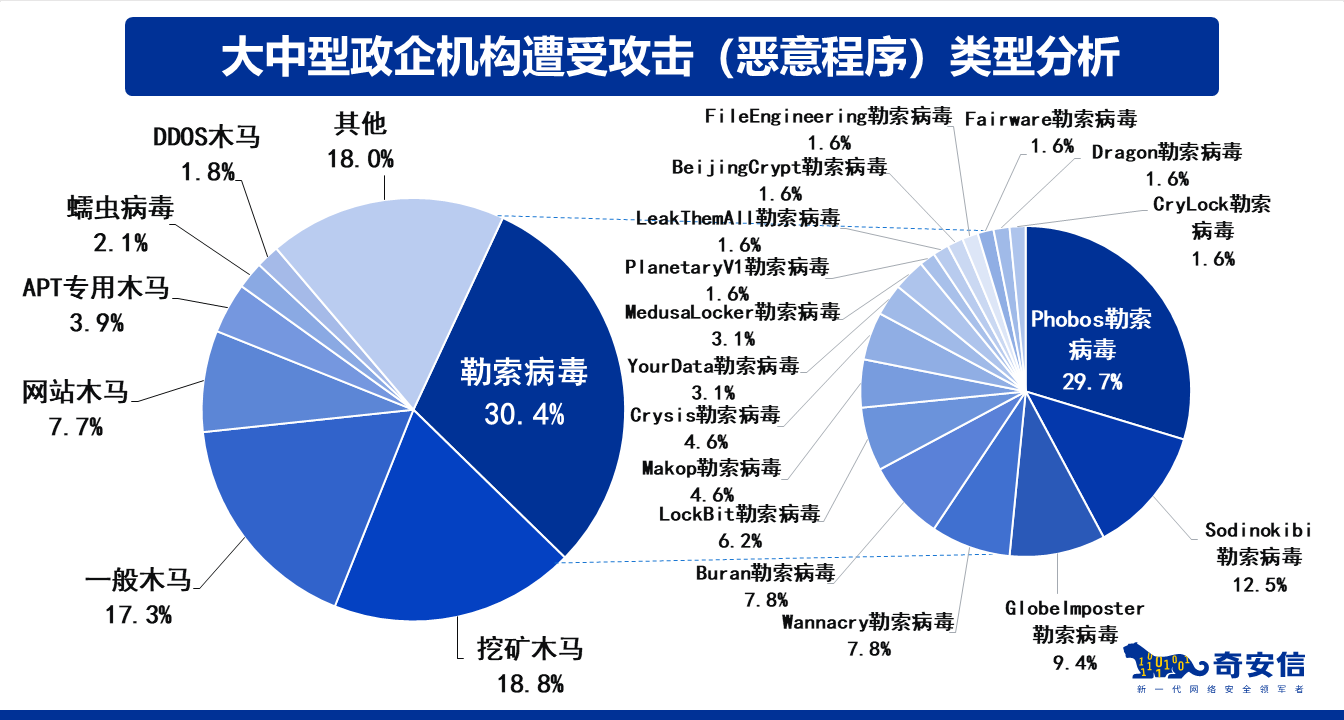


图1-8：大中型政企机构遭受攻击（恶意程序）类型分析

2021年上半年最常见的勒索病毒是Phobos勒索病毒、Sodinokibi勒索病毒、GlobeImposter勒索病毒、WannaCry勒索病毒以及相关变种病毒。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。

### 漏洞利用分析

在2021年上半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日常利用的方式（其中，在单起网络安全事件中，存在多个弱点的情况）。

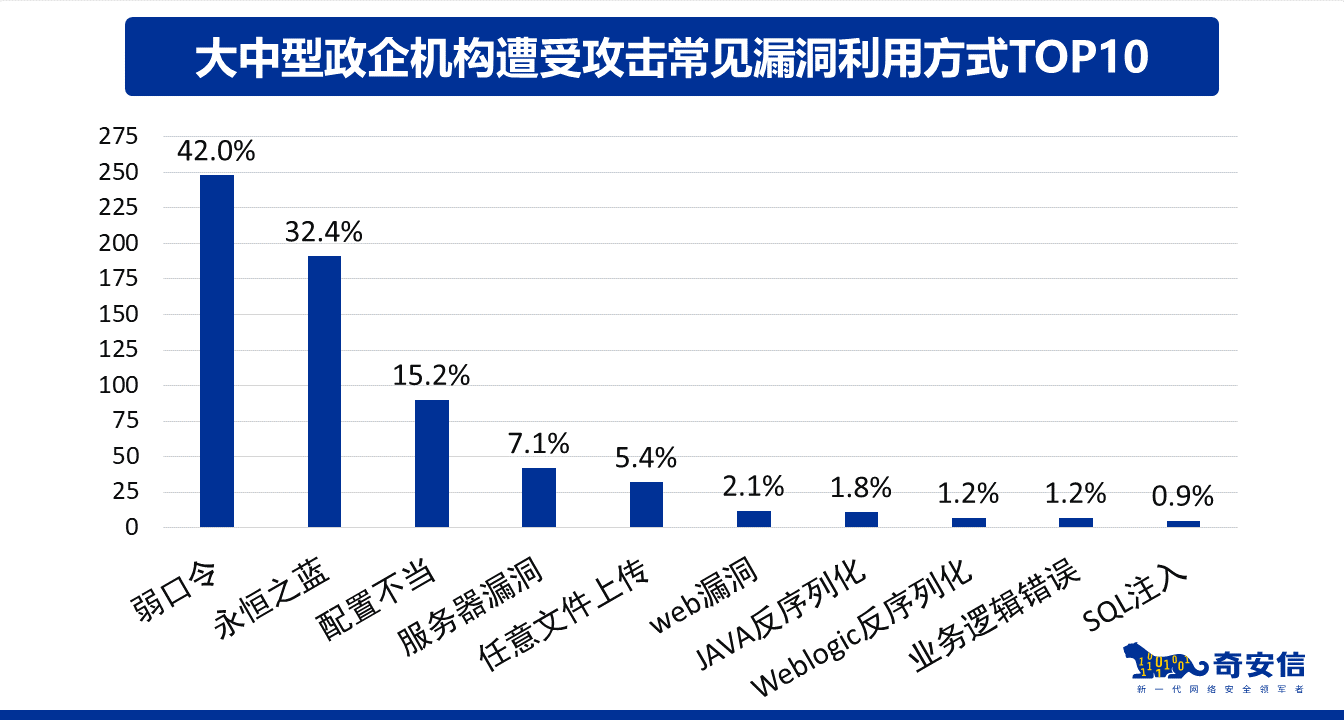


图1-9：大中型政企机构遭受攻击常见漏洞利用方式

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，任意文件上传也是攻击者最常利用的漏洞，攻击者通过利用某一漏洞入侵系统，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，不给攻击者任何可乘之机。

1. 勒索类事件典型案例

自2017年“永恒之蓝”勒索病毒事件之后，勒索病毒的花样也越来越多，不同类型的变种勒索病毒层出不穷，从近几年的应急响应数据来看，因感染勒索病毒的应急每年都占应急事件的五成以上，利用方式也多以“永恒之蓝”漏洞，暴破和弱口令空口令等方式，受害者一旦感染勒索病毒，重要文件被加密，产生的影响和损失巨大。

1. 服务器存漏洞感染勒索病毒

### 事件概述

2018年1月，奇安信集团安服团队接到某医院的服务器安全应急响应请求。该机构反馈有几台服务器出现重启/蓝屏现象，应急响应人员初步判定为感染了勒索病毒。

应急响应人员对重启/蓝屏服务器分析后，判定均遭受“永恒之蓝”勒索病毒，同时遭受感染的服务器中部分文件被加密。通过对服务器进行漏洞检查发现服务器存在MS17-010漏洞，同时发现服务器开放了445端口。

通过本次安全事件，医院信息系统暴露了诸多安全隐患，包括未定期开展安全评估工作，导致内部服务器存在严重高危漏洞；安全域划分不明确，较为混乱；安全意识仍需加强等。

### 防护建议

* 1. 周期性对全网进行安全评估工作，及时发现网络主机存在的安全缺陷，修复高风险漏洞，避免类似事件发生；
  2. 系统、应用相关的用户杜绝使用弱口令；
  3. 有效加强访问控制ACL策略，细化策略粒度，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；
  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；
  5. 加强安全意识，提高对网络安全的认识，关注重要漏洞与网络安全事件。

1. 终端电脑遭遇钓鱼邮件感染勒索病毒

### 事件概述

2018年4月，奇安信集团安服团队接到某电网公司的终端安全应急响应请求，有几台办公终端出现部分Office文档、图片文档、pdf文档多了sage后缀，修改后变成乱码。

应急响应人员接到请求后，通过对感染勒索病毒的机器样机进行分析得知，此次感染的勒索病毒的类型为sage2.2勒索病毒。对于感染过程，响应人员分析该勒索病毒可能使用了包含欺骗性消息的恶意电子邮件，消息可以是各种类型，目的皆在使潜在受害者打开这些电子邮件的恶意.zip。

### 防护建议

* 1. 对受感染的机器第一时间进行物理隔离处理；
  2. 部署终端安全管控软件，实时对终端进行查杀和防护；
  3. 对个人PC中比较重要的稳定资料进行随时备份，备份应离线存储；
  4. 继续加强网络与信息安全意识培训教育。意外收到的或来自未知发件人的电子邮件，不要按照文字中的说明进行操作，不要打开任何附件，也不要点击任何链接；
  5. 操作系统以及安装在计算机上的所有应用程序（例如Adobe Reader，Adobe Flash，Sun Java等）必须始终如一地更新。

1. 工业生产网与办公网边界模糊，感染勒索病毒

### 事件概述

2019年2月，某大型制造企业的卧式炉、厚度检测仪、四探针测试仪、铜区等多个车间的机台主机以及MES（制造执行系统）客户端都不同程度地遭受蠕虫病毒攻击，出现蓝屏、重启现象。该企业内部通过处理（机台设备离线、部分MES服务器/客户端更新病毒库，更新主机系统补丁）暂时抑制了病毒的蔓延，但没有彻底解决安全问题，因此紧急向工业安全应急响应中心求救。

工业安全应急响应中心人员到达现场后，经对各生产线的实地查看和网络分析可知，当前网络中存在的主要问题是工业生产网和办公网网络边界模糊不清，MES与工控系统无明显边界，各生产线未进行安全区域划分，在工业生产网中引入了WannaMine3.0、“永恒之蓝”勒索蠕虫变种，感染了大量主机，且勒索蠕虫变种在当前网络中未处于活跃状态（大部分机台设备已离线）。

### 防护建议

* 1. 制定MES（制造执行系统）与工控系统的安全区域，规划制定安全区域划分；
  2. 隔离感染主机：已中毒计算机关闭所有网络连接，禁用网卡，未进行查杀的且已关机的受害主机，需断网开机；
  3. 切断传播途径：关闭潜在终端的网络共享端口，关闭异常的外联访问；
  4. 查杀病毒：使用最新病毒库的终端杀毒软件，进行全盘查杀；
  5. 修补漏洞：打上“永恒之蓝”漏洞补丁并安装工业主机安全防护系统。

1. 服务器配置不当感染勒索病毒

### 事件概述

2019年3月，奇安信安服团队接到某交通运输行业的应急响应请求，某重要服务器感染勒索病毒，导致业务系统无法正常运行。

应急响应人员抵达现场后，通过对受感染服务器进行分析，发现服务器感染Crysis勒索病毒变种，操作系统桌面及启动项目录中发现病毒样本payload1.exe，系统大部分文件被加密。同时2个境外IP在勒索时间节点利用administrator账号远程桌面登录到了目标主机，人工投毒并进行横向扩散。

通过对现场情况进行分析和对事件进行推断，本次事件主要是由于服务器配置不当，直接对外映射了远程桌面端口，进而攻击者有针对性地对rdp远程登录暴破、人工投毒执行的勒索攻击。

### 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. 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；
  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. 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. 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；
  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；
  7. 加强人员安全意识培养，不要点击来源不明的邮件附件，不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。

1. 专网被攻击，58家医院连锁感染勒索病毒

### 事件概述

2019年3月，某地骨科医院爆发勒索病毒，不到一天，全省另外57家医院相继爆发勒索病毒，每家医院受感染服务器数量为3-8台不等，受灾医院网络业务瘫痪，无法正常开展诊疗服务。奇安信安服团队收到求助后，第一时间到达该医院进行排查。

现场排查显示，此次事件可认定为人工投毒，感染的病毒为Globelmposte家族勒索病毒，受感染医院专网前置机因使用弱口令而被暴破，在成功感染第一家医院后，攻击者利用卫生专网暴破3389登录到各医院专网前置机，再以前置机为跳板向医院内网其他服务器暴破投毒，感染专网未彻底隔离的其他57家医院。

通过本次安全事件，医院信息系统暴露了诸多安全隐患，包括未定期开展安全评估工作，导致内部服务器存在严重高危漏洞；安全域划分不明确，较为混乱；安全意识仍需加强等。



图2-1：攻击路径图

### 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. 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；
  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；
  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. 后续完善强化安全域划分与隔离策略；修改弱密码；关闭防火墙一切不必要的访问端口；配置完善全流量采集分析能力；
  6. 构建安全行业生态合作，有效利用威胁情报和应急服务，提升安全防护和处置水平。

1. OA服务器远程桌面映射公网，感染勒索病毒

### 事件概述

2020年2月，安服团队接到某地热电企业应急响应请求，该企业现场包括收费系统、化检站远程监测系统、用户室温检测系统、邮件系统等23个系统被加密。该企业属于大型政企机构，停产后果难以估量，因此发出应急响应请求。

应急人员抵达现场后，对受害主机初步分析，确定病毒为Sodinokibi勒索病毒，且主机日志大多被清除。

通过对多台主机残留日志关联分析，配合上网行为系统访问日志分析，确认感染源头为部署在虚拟化区域的OA服务器。黑客入侵后取得了管理员权限，又以此为跳板攻击其他主机。经现场调研发现，除管理疏忽存在漏洞外，该企业为了方便运维将OA服务器远程桌面映射到了互联网上，并且有弱口令甚至是空口令的情况，导致遭受此次攻击。

### 防护建议

* 1. 定期进行内部人员安全意识培养，禁止将敏感信息、内网端口私自暴露至公网，所有账号系统必须设置口令且禁止使用弱口令；
  2. 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。

1. 内网主机使用弱口令致感染勒索病毒

### 事件概述

2020年3月，安服应急响应团队接到某国有企业应急响应请求，该企业感染勒索病毒、多个主机文件被加密，要求协助对攻击路径进行溯源。

应急人员通过对主机/服务器的进程、文件、日志等排查分析，发现主机审核策略配置存在缺陷，部分审计未开启，系统被植入恶意程序等现象，确认多台机器感染Hermes837勒索病毒，被病毒加密后的文件后缀为“Hermes837”。

攻击者利用IPC暴力破解，成功登录内网主机和办公主机，在办公主机进行安装TeamViewer，创建ProcessHacker服务，修改密码等一系列操作，以内网主机为跳板，在SMB服务器安装恶意程序KProcessHacker 。最终导致多台机器感染Hermes837勒索病毒，文件被加密。

### 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，加强内部人员安全意识，禁止密码重用的情况出现；
  2. 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；
  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；
  4. 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；
  5. 建立安全灾备预案，一旦核心系统遭受攻击，需要确保备份业务系统可以立即启用；同时，需要做好备份系统与主系统的安全隔离工作，避免主系统和备份系统同时被攻击，影响业务连续性。

1. 8003端口映射在公网感染勒索病毒

### 事件概述

2020年5月，安服应急响应团队接到某医疗卫生行业应急响应求助，现场发现一台服务器被加密，希望对加密服务器进行排查，并追溯攻击来源。

应急人员接到应急请求抵达现场后排查发现，内网2台服务器和11台终端感染Phobos家族最新变种勒索病毒。应用服务器B的应用系统8003端口映射在公网上，内网多台设备均未安装任何补丁，且开放445、3389等常被攻击者利用的端口。

经过一系列排查分析，最终确认攻击者利用应用服务器B存在的已知漏洞，上传webshell后门获得服务器B的应用权限，进行提权后，关闭终端安全软件，上传恶意程序mssecsvr.exe。并以应用服务器B作为跳板机，对内网发起扫描，通过暴力破解获取服务器A的3389端口的账号、密码，远程登录服务器A，上传勒索病毒程序mssecsvr.exe，利用内网开放的445端口将病毒进行横向扩散，最终导致内网多台设备感染勒索病毒被加密。

### 防护建议

* 1. 服务器、操作系统启用密码策略，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；
  2. 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；
  3. 关闭服务器3389、445、139、135等不必要的高危端口，建议内网部署如堡垒机等类似的设备，并只允许堡垒机IP访问服务器的远程管理端口（如445、3389、22等）；
  4. 对内网开展安全大检查，检查的范围包括但不限于恶意进程、恶意服务、异常账号以及后门清理、系统及网站漏洞检测等；
  5. 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。

1. 私自下载破解软件致服务器感染勒索病毒

### 事件概述

2020年9月，某公司十余台服务器感染勒索病毒，文件遭勒索加密，因此向奇安信安服团队发起应急响应请求，查询中毒原因。

应急人员抵达现场后，查看加密文件后缀及勒索病毒界面，判断该病毒是Phobos家族勒索病毒。通过现场对多台受害服务器进行日志分析，并与相关工作人员沟通，发现公司内部员工曾使用个人电脑通过非官方渠道下载各类破解版软件，导致个人电脑感染勒索病毒。同时内网多台服务器均开放3389远程桌面服务端口，勒索病毒进入内网后对内网服务器进行RDP暴破，暴破成功后释放勒索病毒，加密文件。

### 防护建议

* 1. 加强内部访问策略，禁止或限制个人电脑进入内网，如业务需要，增加访问控制策略；
  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；
  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，禁止通过非官方渠道下载应用软件，及时修复漏洞、安装补丁，将信息安全工作常态化。

1. 服务器补丁安装不及时感染勒索病毒

### 事件概述

2021年2月，某药业公司一台服务器遭受勒索病毒攻击，紧急向奇安信工业安全应急响应中心求助，希望尽快排查并溯源。

工业安全应急响应中心专家通过对受感染服务器进行日志分析，排查确认感染fair勒索病毒。分析中发现文件最早加密时间为2021-02-26 15:20 左右，排查此时间段前登录记录，发现存在大量国外IP登录的记录。对登录IP进行威胁情报排查，发现大多IP都为恶意IP，其中有恶意IP通过windows登录类型10：远程交互（远程桌面或远程协助访问计算机）的方式登录过受害服务器。

通过对现场情况进行分析发现，该药业公司服务器存在补丁安装不及时、多张网卡情况、根据以上排查信息、也不排除攻击者扫描到相关漏洞进行攻击的可能性。

### 防护建议

* 1. 对已被感染勒索病毒的服务器进行断网处理，并进行隔离，以免进一步感染其他主机。对于未中招服务器，尽量关闭不常用的高危端口；
  2. 有效加强访问控制策略，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，在服务器部署工业主机安全防护系统，使用白名单的机制只允许业务必要端口开放；
  3. 部署工业安全监测系统，进行镜像流量分析和威胁检测，及时发现网络中的安全风险，同时加强追踪溯源能力，提供可靠的追溯依据。

1. 擅自修改网络配置致服务器感染勒索病毒

### 事件概述

2021年4月，奇安信安服团队接到医疗行业某机构应急响应求助，现场一台刚上线服务器感染勒索病毒，所有文件被加密。

应急人员通过对加密文件进行查看，确认受害服务器感染的是Phobos勒索病毒，文件加密时间为事发当日凌晨3点。应急人员对受害服务器日志进行分析发现，从事发前一周开始，公网IP（x.x.x.75）持续对受害服务器RDP服务进行账号密码暴力破解，并于事发前一晚22点第一次登录成功。事发当日凌晨1点，公网IP（x.x.x.75）再次登录RDP服务账号，使用黑客工具强制关闭服务器中安装的杀毒软件，向内网进行了横向渗透、端口扫描及RDP暴破等行为，但均利用失败，并于事发当天凌晨3点向受害服务器释放勒索病毒。

最终发现，正常运维人员访问RDP服务需要通过堡垒机访问，运维人员为了方便管理，将RDP服务8735端口的网络流量通过netsh端口转发到服务器3389端口到公网，导致RDP服务开放至公网被攻击者利用。

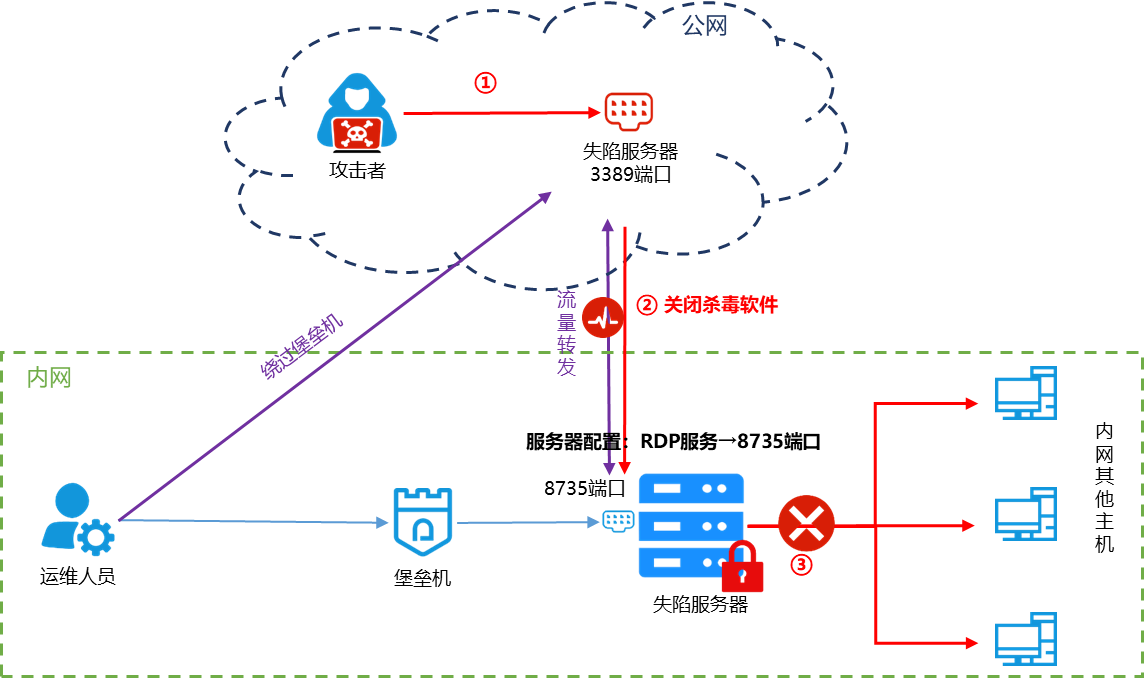
****

图2-2：攻击路径图

### 防护建议

* 1. 定期进行内部人员安全意识培训，禁止擅自修改服务器配置，禁止使用弱密码等；
  2. 服务器、操作系统启用密码策略，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、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；
  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。

1. 用户名口令被暴力破解感染勒索病毒

### 事件概述

2021年5月，奇安信安服团队接到某政府部门的应急响应求助，要求对被勒索服务器进行排查分析并溯源。

应急人员通过查看加密文件，确认感染VoidCrypt勒索病毒。对多台被感染服务器进行日志分析，发现存在大量用户名口令暴破并暴破成功的记录。查看服务器C主机进程发现存在FRP代理程序，与运维管理员沟通了解到，运维管理员为了方便管理将服务器C的3389远程桌面端口映射到了公网。

经排查研判后最终确定，攻击者利用服务器C对外开放的3389端口对用户名和密码进行暴力破解，并成功获取服务器C的控制权，进而以服务器C作为跳板，对内网进行小规模扫描暴破获取服务器B的权限，再进一步以服务器B作为跳板，继续对内网进行扫描暴破获取服务器A的权限，利用服务器A为跳板机进行内网暴破攻击，在获得其他主机用户名口令后，通过远程登录执行勒索程序。

### 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；
  5. 对内网的安全域进行合理划分，各个安全域之间限制严格的ACL，限制横向移动的范围；
  6. 建立安全灾备预案，一旦核心系统遭受攻击，需要确保备份业务系统可以立即启用；同时，需要做好备份系统与主系统的安全隔离工作，避免主系统和备份系统同时被攻击，影响业务连续性。

1. 挖矿类事件典型案例

近几年，除勒索病毒外，挖矿木马也越来越流行，多为利用漏洞利用、“永恒之蓝下载器”、弱口令暴破等手段完成攻击，由于其具有较强的隐蔽性，会利用一些手段避开受害者活动时间，利用受害者空闲时间进行挖矿，长此以往，服务器、主机显卡或CPU长期占用过高，导致电脑性能降低，同时攻击者会利用已控制的挖矿主机攻击其他设备，导致业务中断甚至更严重的网络安全事件的发生。

1. 官网存在上传漏洞感染挖矿木马

### 事件概述

2017年6月，某汽车集团发现网络异常，影响正常使用，奇安信安服团队接到应急响应申请，应急响应专家1小时内到达现场。

应急响应专家登录到异常服务器排查分析，发现该恶意程序通过PowerShell脚本执行，并会从C&C地址拉取PayLoad和远控程序，故判定为感染挖矿木马，进一步分析，发现该恶意软件具有蠕虫特点，能够通过网络自我复制传播，该木马的传播途径主要通过使用MS17-010（永恒之蓝）漏洞进行传播或使用在本机抓取的账号密码信息，登录其他机器进行传播。通过查看内部机器发现均未安装MS17-010补丁，且所有服务器均采用统一密码。

综上，攻击者利用该集团官网页面上传漏洞获取了服务器权限，投放挖矿木马，连接矿池并从C&C服务器中下载恶意payload，利用内部服务器未安装MS17-010以及所有服务器均采用同一密码的弊端，对其他服务器进行攻击，导致内网多台服务器中招，分别连接矿池，下载恶意payload，导致网络受到严重影响。

### 防护建议

* 1. 避免使用弱口令，应该在服务器登录账户和开放端口上的服务使用强密码；
  2. 定期更新电脑补丁，使用正确渠道，下载对应漏洞补丁；
  3. 应定期维护服务器，内容包括但不限于：查看服务器操作系统CPU使用率是否异常、是否存在可疑进程、计划任务中是否存在可疑项；
  4. 对系统文件上传功能，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；
  5. 部署高级威胁监测设备；
  6. 建议在服务器上安装相应的防病毒软件或部署防病毒网关，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。

1. 误点恶意链接感染挖矿木马

### 事件概述

2018年11月，奇安信集团安服团队接到某公司的挖矿木马事件应急响应请求，其内网多台终端被挖矿木马攻击，服务器卡顿、进程缓慢，无法正常运行。

应急人员到达现场后，对内网服务器、终端进程、日志等多方面进行分析，发现内网服务器、终端CPU被powershell进程占满，服务器、终端均开放135、139、445等服务端口，且均未安装“永恒之蓝”补丁。

经过分析排查，应急人员成功找到问题根源，并对病毒进行抑制、根除。本次事件主要是由于内部工作人员安全意识较低，点击恶意链接感染终端，然后通过被感染终端对服务器SMB弱口令进行暴破获取服务器账号和密码，并利用服务器作为突破口，对内网中有“永恒之蓝”漏洞的主机进行攻击，种植挖矿木马，并横向传播，意图感染内网其他终端。

### 防护建议

* 1. 系统、应用相关的用户杜绝使用弱口令，同时，应该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，尽量避免一密多用的情况；
  2. 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；
  3. 关闭内网远程服务、共享等危险性服务端口；
  4. 定期更新电脑补丁，使用正确渠道，如微软官网，下载对应漏洞补丁；
  5. 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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
  6. 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；
  7. 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；
  8. 加强人员安全意识培养，不要点击来源不明的邮件附件，不从不明网站下载软件。

1. 软件升级包携带“永恒之蓝下载器”致专网感染挖矿木马

### 事件概述

2019年2月，制造行业某企业遭受“永恒之蓝下载器”感染事件，专网近10家下属单位中毒，因病毒爆发导致正常业务中断。奇安信安服团队接到求助后，第一时间与该企业进行沟通，并协助进行处理。

1）现象为从2月11日windows服务器开始出现被恶意添加计划任务情况，多次删除后仍被添加，并且系统防火墙被无故开启影响企业自有系统运行；

2）上机查看后发现被新建的三项计划任务名称分别为：Ddrivers、DnsScan、WebServers，并在服务器上找到了对应的三个程序；

3）与此同时在C:\windows\temp\目录下发现存在两个可疑文件，分别是名为“m.ps1” 的Powershell文件及名为“mkatz.ini”的配置文件。经分析“m.ps1”为经混淆的mimikatz，而“mkatz.ini”则是通过mimikatz抓取出的本机操作系统账号密码等认证信息；

4）查看网络连接发现temp目录下的svchost.exe正在向内网10.\*.196.\*及外网170.\*.239.\* C段IP地址发起大量一对多的445端口的主动连接动作，疑似存在扫描攻击行为；

5）通过对操作系统排查，自2018年12月起，有大量IPC登录日志产生，甚至登录成功与失败的次数相当，其中10.\*.196.\*（SU\*\*\*NG）存在大量失败及成功的次数，行为与暴力破解一致。并在2月10日计划任务起始时间前的早上5:53分仍有大量登录失败及少量登录成功的IPC登录动作；

6）通过文件威胁情报碰撞检测到进程中存在wannacry勒索病毒相关的样本程序正在运行，该恶意程序发起大量向各个互联网IP地址的445端口连接行为，存在可疑的永恒之蓝漏洞攻击行为；

7）通过沙箱对该程序进行检测发现该程序为10分恶意程序，主要标签为“下载者”、“漏洞利用”、“检测沙箱”、“加壳程序”。高危动作包括：安装自身来实现自启动、创建一个可疑的Powershell进程、创建一个可疑文件、创建m.ps1文件、创建可疑进程等动作；

8）其中，temp目录下的m.ps1文件由该程序svchost.exe所生成，同时发现存在WannaMiner挖矿蠕虫病毒，对恶意程序进行分析，获取到该程序发起部分固定链接的访问；

9）通过TI威胁情报大数据检测到i.haqo.net和p.abbny.com等链接与前期大面积爆发的黑客利用某第三方软件升级通道下发病毒木马感染传播有关；

10）采样了多台服务器，在另两台服务器上发现存在木马、挖矿蠕虫、漏洞利用程序。发现了前期黑客通过某第三方软件升级渠道传播病毒的行为及对应的恶意程序。

经过分析发现，是文件下发器在进行某第三方软件升级后，将该软件升级包进行全国下发，该第三方软件升级包携带的“永恒之蓝下载器”木马，具有外连矿池下载病毒木马、扫描暴破等功能，导致该企业内网及其专网近10家单位部分服务器、终端感染挖矿，蠕虫等病毒，正常业务中断。应急人员通过对该事件进行分析溯源，定位问题关键点，部署虚拟化杀毒平台进行病毒管控，帮助其降低损失。经过7个小时的事件应急处置，专网内下属单位业务已恢复正常。

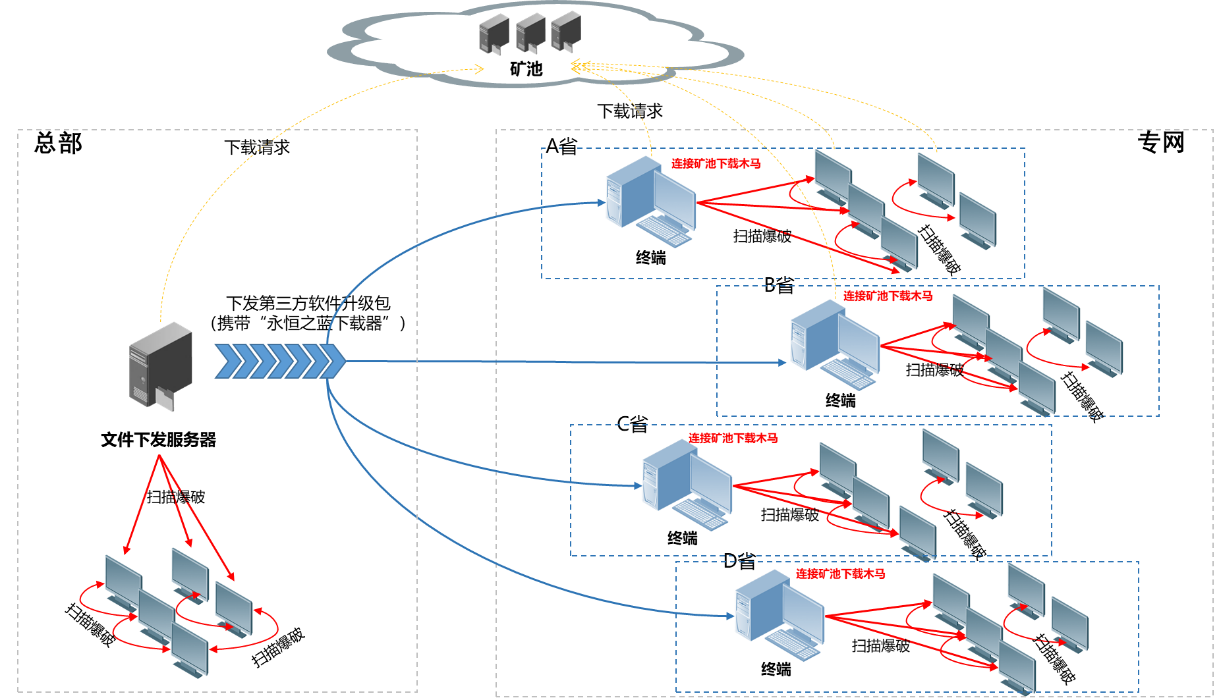


图2-3：攻击路径图

### 防护建议

* 1. 对于重点服务器和主机，做好网络安全域划分并及时打MS17-010漏洞补丁，防止利用此漏洞的横向攻击；
  2. 开启Windows防火墙，尽量关闭3389、445、139、135等不用的高危端口；
  3. 每台服务器设置唯一口令，且复杂度要求采用大小写字母、数字、特殊符号混合的组合结构，口令位数足够长；
  4. 部署全流量监测设备，及时发现恶意网络流量，进一步追踪溯源。

1. “永恒之蓝下载器”致内网挖矿木马

### 事件概述

2019年3月，奇安信安服团队接到某政府单位“永恒之蓝下载器”挖矿事件应急响应请求，其内网大量服务器出现服务器内存、CPU等资源被恶意占用，导致部分服务器业务中断，无法正常运行。

应急人员到达现场后与该单位沟通得知，服务器于一周前存在大量445连接，随时间增长，服务器资源被耗尽，导致业务无法正常工作。通过对内网服务器、终端进程、日志等多方面进行分析，根据应急响应人员现场排查的结果，判定内网服务器所感染病毒为“永恒之蓝下载器”挖矿蠕虫病毒，该病毒会利用永恒之蓝漏洞在局域网内进行蠕虫传播，窃取服务器密码进行横向攻击，并且会创建大量服务耗尽服务器资源。通过使用奇安信安服团队编写的批量查杀脚本，对网内机器进行查杀病毒，大大降低网内恶意流量与病毒对资源的占用，恢复了正常业务。

### 防护建议

* 1. 对检测阶段发现的攻击源IP地址进行重新查杀，条件允许情况下重装系统重新部署业务；
  2. 安装天擎最新版本（带防暴破功能）和天擎服务器加固防止被黑；
  3. 建议部署全流量监控设备，可及时发现未知攻击流量以及加强攻击溯源能力，有效防止日志被轮询覆盖或被恶意清除，有效保障服务器沦陷后可进行攻击排查，分析原因；
  4. 建议对内网开展安全大检查，检查的范围包括但不限于后门清理、系统及网站漏洞检测等；
  5. 尽量关闭3389、445、139、135等不用的高危端口，建议内网部署堡垒机类似的设备，并只允许堡垒机IP访问服务器的远程管理端口（445、3389、22）；
  6. 对系统用户密码及时进行更改，可并使用LastPass等密码管理器对相关密码进行加密存储，避免使用本地明文文本的方式进行存储。

1. 安全防护不到位致终端和服务器感染挖矿木马

### 事件概述

2019年4月，安服应急响应团队接到应急请求，医疗行业某单位网内约1000多台终端和服务器存在大量病毒，客户机不定时重启、蓝屏，严重影响业务系统的正常运行。

应急人员通过对相关进程、文件、服务进行排查分析后，判断该单位内网失陷是由于感染“永恒之蓝下载器”木马，导致病毒泛滥。通过检查现场内网失陷主机，发现现场主机系统均未安装杀毒防护软件，C:\Windows目录下存在大量以随机字符命名的.exe文件，并在系统服务中发现大量该exe对应的服务。在分析天眼设备抓取流量时，发现内网共存在11种病毒，包括蠕虫病毒、挖矿病毒、勒索病毒、远控木马、僵尸网络等多种病毒，且发现主机高危端口如135、137、138、445端口均为开启状态并存在传播病毒的行为。除此之外，应急人员在检查过程中发现sqlserver数据库管理员账户密码与网内所有服务器均使用同一种密码，且该数据库服务器未安装任何安全防护设备，使得木马快速在内网扩散，并存在大量外连行为，导致大量机器沦陷。

### 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. 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. 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. 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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
  5. 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；
  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。

1. SSH私钥本地保存致虚拟机感染挖矿木马

### 事件概述

2019年9月，安服应急响应团队接到某互联网公司请求，其安全部门发现公司内网数万台虚拟机感染挖矿木马，应急人员立即赶往现场进行排查和溯源工作。

应急人员对受害服务器进行分析，发现内网多台受害主机本地均存有内网其他机器的ssh私钥，并可以免密登录Ansible服务器。攻击者首先利用Consul组建远程命令执行漏洞进入内网，下载并运行挖矿木马，并利用保存在本地的ssh私钥进行横向扩散，感染Ansible服务器后，通过ansible/salt/knife进行大量传播，最终导致内网数万台虚拟机均受影响。应急人员立即采取行动，对挖矿木马产生的密钥认证文件、可疑计划任务项、木马守护进程以及挖矿木马创建的恶意文件进行清理。

Ansible是一种可批量管理服务器的开源自动化工具，管理员可以通过 Ansible 在成百上千台计算机上同时执行指令（任务）。本次事件中，数万台虚拟机受到感染，Ansible服务器的沦陷是导致挖矿木马大量传播的主要因素，企业应当对此类重要服务器进行充分的保护和隔离，避免其被攻击者掌控，造成不必要的损失。

### 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、密码本地保存等情况出现；
  2. 重要业务系统及核心数据库应设置独立的安全区域，做好区域边界的安全防御工作，严格限制重要区域的访问权限并关闭不必要、不安全的服务；
  3. 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；
  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. 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；
  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。

1. 网站存漏洞致服务器感染挖矿木马

### 事件概述

2020年6月，安服应急响应团队接到某大型企业的应急响应请求，该企业服务器存在被种植挖矿木马病毒程序，态势感知出现病毒告警，要求对服务器后门进行排查，同时对攻击来源进行追溯。

应急人员经过排查，发现该企业内部有70台服务器受到SystemdMiner挖矿木马最新变种病毒的感染，存在内网横向传播的情况，且服务器中均未安装杀毒软件。通过对病毒样本和受感染机器的日志分析，确定攻击者利用该企业官网服务器漏洞获得网站服务器控制权限，通过扫描暴破获得堡垒机主机权限，并对内网多台服务器安装FRP反向端口代理工具，并上传SystemdMiner挖矿木马程序，配置计划任务，定时连接矿池域名，又利用Consul rce /Hadoop rce /Jenkins rce/PostgreSQL rce、主机系统弱口令漏洞入侵IDC机房其他主机操作系统，利用自动化运维工具（salt/ansible/chef-knife）横向传播，利用失陷主机本地保存的 SSH 密钥传播自身。

最终，确定攻击者通过官网漏洞获得网站服务器控制权限，通过扫描暴破获得堡垒机权限，并部署Frp代理工具。通过堡垒机登录多台服务器，部署扫描工具进行内网扫描，并通过“自动化运维服务器”下发挖矿程序， 利用“自动化运维服务器” 部署Frp代理作为跳板横向传播，最终控制近70台服务器。

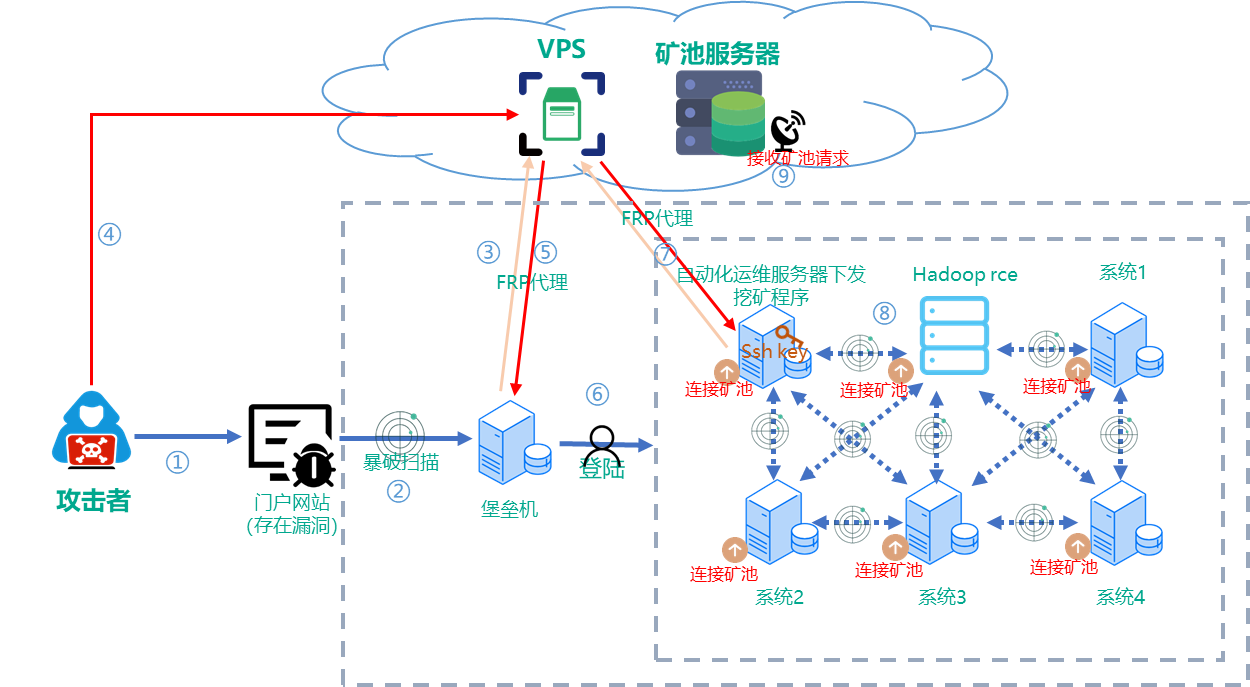


图2-4：攻击路径图

### 防护建议

* 1. 将已检测到的矿池相关非法域名，通过安全防护设置将其加入黑名单列表，并设置安全策略为阻断访问；
  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，加强内部人员安全意识，禁止密码重用的情况出现；
  3. 增强内部人员密码管理意识，禁止将密码进行本地保存；
  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，加强服务器上的病毒发现及清除能力；
  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。

1. 服务器使用弱口令导致感染挖矿木马

### 事件概述

2020年8月，某大型煤矿集团一台服务器发现感染挖矿蠕虫病毒，往同段其他服务器445以及6379端口发送大量感染数据包，服务器自身CPU利用率较高，机器卡顿，严重影响正常业务的使用。奇安信安全服务人员紧急向该煤矿集团进行现场应急响应服务。

安全专家发现受感染的服务器向内部某网段发送大量攻击数据包，并不断连接外部矿机地址，结束进程后会自动重启，相关病毒文件删除后会自动生成，存在守护进程。采集受感染服务器的系统日志并获取挖矿病毒文件的落地时间分析发现，攻击者使用通用弱密码123.com对服务器发起暴破行为并暴破成功，通过某台服务器进行暴力破解服务器RDP服务进行工具自动化投毒，导致服务器被挖矿蠕虫病毒感染。

### 防护建议

* 1. 对已受感染的主机清理病毒进程，删除相关病毒文件，停止恶意服务；
  2. 加强资产上的服务口令复杂度，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；
  3. 有效加强访问控制策略，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；
  4. 部署工业主机安全防护系统，采用基于智能匹配的白名单管控技术、基于ID的USB移动存储外设管控技术、以及入口拦截、运行拦截、扩散拦截关卡式病毒拦截技术，防范恶意程序的运行、非法外设接入，从而进行全面的工业资产、安全风险集中管理，实现对工业主机/服务器的安全防护。

1. 应用服务平台使用弱口令导致感染挖矿木马

### 事件概述

2020年10月，安服团队接到某政府部门应急请求，其安全设备检测到挖矿木马外连告警，内部多台服务器感染挖矿木马，需要进行排查分析并溯源。

安服应急人员到达现场后，通过排查安全设备告警日志、受害主机日志以及对木马样本进行分析发现，内网多台Web应用服务器对外开放SSH服务22端口并且使用相同的弱口令、多台受害服务器均被植入SSH扫描暴破脚本和挖矿木马程序，并设置为开机自启动。

经过最终研判分析确定，攻击者首先对网站应用服务平台进行端口探测，发现开放22端口SSH服务，对SSH服务进行弱口令暴破成功登录服务器，随后植入挖矿木马和SSH扫描暴破脚本并添加至服务器自启动项，攻击者采用相同的密码利用SSH扫描暴破脚本对内网服务器进行暴破，并植入挖矿木马，最终导致内网多台服务器沦陷。

### 防护建议

* 1. 封禁攻击者服务器IP、修改失陷机器的用户密码；
  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. 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；
  4. 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。

1. U盘未管控导致主机感染挖矿木马

### 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，其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。

### 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。

1. 蠕虫类事件典型案例

蠕虫病毒也是一种常见的计算机病毒，具有较强独立性，可以不依赖宿主程序独立运行，具有传播更快更广以及更好的伪装和隐藏的特点，通常利用恶意链接、电子邮件附件、U盘携带以及弱密码暴破的方式发起攻击，受害者一旦点击包含有被蠕虫感染的链接和邮件附件，蠕虫病毒会立刻被激活，并迅速感染其他主机，窃取重要信息，严重时会导致网络系统瘫痪，服务器系统资源遭到破坏。

1. 服务器弱口令导致感染蠕虫病毒

### 事件概述

2016年，奇安信集团安服团队接到某银行应急响应请求，其发现内网有服务器出现工作异常，并发现网络中存在扫描行为，应急响应专家1小时内到达现场。

应急响应专家通过现场进行检测分析，发现大量来自A省分行的服务器可疑远程桌面暴破行为，进一步远程检测发现A省分行服务器上均存在恶意进程，正在批量扫描暴破内网3389端口，其中B省某重要业务系统已被暴破成功，并对全国至少19家分行进行扫描。通过对样本进行分析，确认该银行内网中感染了Morto家族系的蠕虫的最新进化版本，主要实现远控目的。对A省被攻陷终端的日志分析，攻击者早在2015年就已进入到A省分行内部网络区域，对整个银行内部网络的暴破攻击长达1年以上。

此外，不同省分行主机均存在以下问题：

1、用户名均为User ，密码为 111111；

2、均开启远程桌面服务，同时对其他开启远程桌面服务的资产产生大量连接（暴破行为）；

3、开始－运行中存在 rundll32 \\tsclient\a\a.dll a 的命令执行记录；

4、服务均存在名为 FastUserSwitchingCompatibility以及 Ias 的异常服务。

### 防护建议

* 1. 所有服务器、终端应强行实施复杂密码策略，杜绝弱口令；
  2. 对服务器进行安全加固，关闭远程桌面功能、定期更换密码、禁止使用最高权限用户运行程序、使用HTTPS加密协议等；
  3. 建立安全灾备预案，一旦核心系统遭受攻击，需要确保备份业务系统可以立即启用；
  4. 对服务器定期维护，内容包括但不限于：查看服务器操作系统是否存在可疑进程、计划任务中是否存在可疑项等；
  5. 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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
  6. 安装杀毒软件、终端安全管理软件并及时更新病毒库。

1. 浏览恶意链接感染蠕虫病毒

### 事件概述

2018年11月，奇安信集团安服团队接到某部委蠕虫病毒事件应急响应请求，其发现内网多台终端外连恶意域名并下载恶意软件。

应急人员到达现场后，对内网服务器文件、服务器账号、网络连接、日志等多方面进行分析，发现内网主机用户浏览带有恶意链接的Web页面，并于内嵌链接中触发对该异常域名的访问，导致服务器被感染飞客蠕虫病毒，并外连下载恶意软件。该病毒会对随机生成的IP地址发起攻击，攻击成功后会下载一个木马病毒，通过修改注册表键值来使某免费安全工具功能失效。病毒会修改hosts文件，使用户无法正常访问安全厂商网站及服务器。

### 防护建议

* 1. 配置并开启操作系统、关键应用等自动更新功能，对最新系统、应用安全补丁进行订阅、更新。避免攻击者通过相关系统、应用安全漏洞对系统实施攻击，或在获取系统访问权限后，对系统用户权限进行提升；
  2. 限制服务器及其他业务服务网可进行访问的网络、主机范围。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，限制公网主机对139、445端口等访问；
  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. 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；
  5. 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；
  6. 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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
  7. 加强人员安全意识培养，不要点击来源不明的邮件附件，不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。

1. U盘未合理管控导致感染蠕虫病毒

### 事件概述

2019年1月，某工业集团为了便于各测试系统中测试数据的统一采集、存储和管理，各测试系统将陆续接入TDM系统（测试数据管理系统），当前仍然有部分测试设备、系统未接入。由于移动介质的交叉使用、相关使用规范的缺失，当前未入网的设备/系统中存在大量病毒，因此该工业集团请求工业安全应急响应中心进行应急响应。

工业安全应急响应中心人员到达现场后，经对现场情况的了解及设备的检测，发现当前设备、系统、网络中存在的主要问题是由于U盘的不合理使用使得TDM系统中感染了“Conficker” 蠕虫、矢网仪感染了“FakeFolder”蠕虫病毒。

病毒可通过移动介质、网络大范围传播，由此形成恶性循环；同时，病毒感染后可进行各种恶意操作，如安装后门、窃取敏感数据、篡改数据等，数据可通过被感染的移动介质和主机传播外泄，由此造成敏感数据丢失、测试数据不准确，最终导致产品出现功能、性能问题的可能性；缺乏对U盘使用的基本管理制度，亦无技术管控措施；安全意识有待提高，安全制度建立有待完善。

### 防护建议

* 1. 在工业终端、服务器等安装工业主机安全防护系统，建立安全基线，对U盘使用进行策略配置；
  2. 对于TDM系统，可在控制主机和数据中转主机之间配置工业网关设备，保证数据的安全、单向传输，在TDM网络边界处部署工业防火墙。除此之外，做好应急准备，将安全处置风险降到最低或可控。

1. 篡改类事件典型案例

篡改类事件主要包括网页篡改，网站黑链、网站挂马等类型，攻击者通常利用漏洞利用、木马病毒程序等方式对网页内容进行篡改，植入违法信息、暗链、挂黑页等，借以达到炫耀自己的技术能力、非法获利、刻意抹黑等目的。

1. Redis未授权访问漏洞致官网被植入黑链

### 事件概述

2017年，奇安信安服团队接到某出版社应急响应请求，官网出现黑链急需溯源排查，应急响应专家30分钟到达现场。

应急人员抵达现场后，通过对系统分析发现在WEB负载服务器WEB01中确实存在黑链，对Web01进行排查发现后门文件，溯源分析后发现攻击者是通过TRS服务器登入Web01系统，获取了Web01系统权限，通过对TRS服务器Web日志分析发现攻击者利用TRS漏洞，植入WebShell后门，攻击IP经调研后发现为内部Redis服务器，通过对Redis服务器进行分析发现该机器存在RootKit程序，该程序会自动连接到攻击者服务器，植入时间为：2017/03/17 ，且在该机器上发现了攻击者利用Redis未授权获得本机SSH管理权限的行为和内网扫描行为。

综上，攻击者通过利用Redis未授权漏洞获取了Redis服务器本机SSH管理权限，并对同网段进行扫描，发现TRS服务器存在漏洞，并对该漏洞进行利用，获取TRS服务器权限并植入Webshell后门文件，由于TRS服务器与WEB负载服务器均使用相同密码，攻击者通过密码登录到WEB负载服务器，植入后门文件，并在官网首页文件中插入恶意代码。

### 防护建议

* 1. 系统、应用相关的用户杜绝使用弱口令，同时，应该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. 禁止外部访问Redis服务端口，禁止使用root权限启动redis服务，配置安全组，限制可连接Redis服务器的IP；
  3. 安装webshell检测工具，根据检测结果对已发现的可以webshell痕迹立即隔离查杀，并排查漏洞；
  4. 加强权限管理，对敏感目录进行权限设置，限制上传目录的脚本执行权限，不允许配置执行权限等；
  5. 日常要多维护，并注意服务器中是否有来历不明的可执行脚本文件；
  6. TRS服务升级为最新版本。

1. 网站WEB漏洞致网站被挂马

### 事件概述

2018年5月，奇安信集团安服团队接到某集团网站挂马事件应急响应请求，其门户网站被挂马，非域名或IP直接访问跳转色情网站。

应急人员到达现场后，对网站系统、服务器文件、账号、网络连接、日志等多方面进行分析，网站网页被植入恶意JS脚本代码，同时网站系统存在DOTNETCMS 1.0 版本漏洞。

经过分析排查，本次事件中黑客主要通过对网站进行扫描，发现网站系统存在SQL注入、登录绕过、任意文件上传等漏洞，黑客通过利用漏洞获取系统权限，并在网页中加入恶意JS脚本，并为了不被内部管理维护人员发现，以达到更长时间的黑帽SEO流量，黑客限制只从百度等搜索引擎跳转，其他则不跳转。

### 防护建议

* 1. 平时运维过程中应当及时备份重要文件，且文件备份应与主机隔离，规避通过共享磁盘等方式进行备份；
  2. 尽量避免打开来源不明的链接，给信任网站添加书签并通过书签访问；
  3. 对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；
  4. 定期用专业反病毒软件扫描系统.及时对服务器的补丁进行更新；
  5. 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；
  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。

1. 网站后台程序漏洞致网站被植入黑链

### 事件概述

2018年5月，奇安信集团安服团队接到某大学信息中心的网站安全应急响应请求，其官网上出现大量黑链、赌博、游戏外挂等违规关键词。

应急响应人员到达现场后，对网站服务器文件、服务器账号、网络连接、进程信息、服务信息、日志信息等多方面进行分析，发现文件中包含大量aspx木马及gif图片伪装成木马，发现存在多个无效账号，以及向外连接的可疑IP地址。

经过分析排查发现，本次事件中所使用的黑链手法为黑产行业惯用手法，利用搜索引擎对大学院校网站发表内容收录快、排名高等优势，利用网站后台程序漏洞对网站进行攻击，上传webshell木马文件至服务器，获取网站管理权限并篡改服务器原有文件，插入黑链恶意脚本，达到控制搜索引擎网页访问跳转，实现搜索引擎“黑帽SEO”。在获取权限后克隆服务器管理员账号以达到长期控制服务器的目的。

### 防护建议

* 1. 建议部署操作系统及相关应用并生成快照，进一步落实口令管理；
  2. 建议使用独立的、随机生成的满足强度要求的口令，严禁使用弱口令、统一口令管理服务器，及时销毁临时、测试账户；
  3. 修改后台管理员密码为复杂密码，修改后台管理目录为复杂路径防止被攻击者猜到，禁用或删除后台模板功能；
  4. 服务器运行环境部署需要进行加固处理，关注各个应用系统所使用程序、组件、第三方插件等安全现状，及时更新相应的补丁版本；
  5. 加强对敏感服务器、配置文件、目录的访问控制，以免敏感配置信息泄露；加强信息系统安全配置检查工作。

1. Tomcat中间件漏洞致官网被上传博彩页面

### 事件概述

2018年5月，奇安信安服团队接到某政府部门应急响应请求，客户官网被植入博彩页面，希望协助恢复官网正常业务，并追溯攻击来源。

应急人员抵达现场后，分别对WCM后台编辑管理平台、iGuard网页防篡改系统、Linux WEB前端服务器进行排查，成功定位博彩页面及Webshell文件。在运维人员对服务器镜像进行备份后，将博彩页面、Webshell文件进行删除，网站恢复正常工作。

应急人员经过分析排查，成功还原攻击路径：攻击者利用WCM系统的Tomcat中间件漏洞上传Webshell文件，获得了WCM系统管理员权限，继而将博彩页面上传至WCM服务器。之后，WCM服务器上的博彩页面被iGuard推送至iGurad服务器和前端WEB服务器，造成了“网站被挂博彩页面暗链”的情况。此外，攻击者还留下了其它的webshell以便对WCM服务器实现长期控制。

### 防护建议

* 1. 及时进行中间件版本更新，对已知漏洞进行补丁修复；
  2. 安装服务器防护软件，及时更新病毒库，对发现的威胁文件立即隔离查杀，并排查漏洞；
  3. 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，立即获取备份文件并进行还原；
  4. 对服务器开展安全大检查，包括但不限于恶意IP封禁、恶意文件以及后门清理、网站漏洞检测及修复等。

1. Weblogic WLS组件漏洞致网页被篡改

### 事件概述

2020年6月，安服应急响应团队接到某事业单位应急响应请求，其官网首页被篡改挂有违法图片，希望对该官网系统业务服务器进行排查分析，并追溯攻击来源。

应急人员抵达现场后，与现场运维人员沟通了解到，业务服务器通过99端口对互联网提供WEB应用服务。

应急人员通过对该服务器Web日志进行排查分析发现，该服务器对互联网还开放9001和9002端口，并发现攻击者在凌晨6点上传一句话木马s.jsp文件。应急人员通过关联s.jsp文件名，检索access.log 和 WLS\_REPORTS.log 日志最终确定攻击者ip，并筛出该攻击ip所有访问日志。通过对访问日志进行排查分析发现，该日志中有大量针对9002端口的Weblogic WLS 组件漏洞攻击的痕迹，由于无法通过Web应用日志确认是否存在Weblogic WLS组件漏洞，因此，应急人员利用Weblogic WLS组件漏洞进行攻击测试，最终确认存在该漏洞。根据日志中攻击者利用Weblogic WLS 组件漏洞攻击时间与官网首页篡改时间比对，攻击成功时间和官网首页被篡改时间相近，由此推断攻击者利用Weblogic WLS 组件漏洞代码进行攻击，成功进入服务器。

攻击者利用Weblogic反序列化漏洞，对开放9002端口的服务器进行攻击，获得该服务器权限并上传一句话木马s.jsp文件。通过查看服务器web目录发现，该服务器对外开放的99端口下部署有该公司官网系统，随后向该系统上传违法图片，修改官网首页。

### 防护建议

* 1. 对系统文件上传功能，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；
  2. 加强权限管理，对敏感目录进行权限设置，限制上传目录的脚本执行权限，不允许配置执行权限等；
  3. 关注官方漏洞发布信息，及时安装漏洞补丁，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，常态化信息安全工作；
  4. 关闭不必要的高危端口，对服务器开展安全大检查，包括但不限于恶意IP封禁、恶意文件以及后门清理、网站漏洞检测及修复等；
  5. 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。

1. weblogic反序列化漏洞致网页被篡改

### 事件概述

2020年9月，奇安信安服团队接到某政府部门应急请求，其网站首页被篡改挂有违法标语，需要进行排查分析并溯源。

奇安信安服应急人员到达现场后通过了解现场网络架构及应用部署情况，分别对应用web应用文件排查、系统日志分析以及防火墙日志分析排查发现web应用服务网站http://11.xx.xx.1与http://11.xx.xx.2 网站首页被篡改、网站存在weblogic反序列化漏洞、服务器存在恶意文件及图片。

经过最终研判分析，黑客首先通过IP:198.xx.xx.21对网站应用平台进行扫描攻击，通过扫描发现网站http://11.xx.xx.1与http://11.xx.xx.2存在weblogic反序列化漏洞。攻击者通过利用该漏洞默认路径下可提交恶意的XML格式的数据，提交的数据在服务器端反序列化时实现远程命令执行，进而获得服务器的权限。最后通过获取到的服务器权限来修改网站首页文件index.jsp，加载恶意图片1.jpg，成功篡改网站首页，并在违法黑客网站进行炫耀其攻击成果。

### 防护建议

* 1. 封禁攻击者服务器IP、删除服务器上恶意文件及图片；
  2. 对应用平台漏洞进行补丁修复，修复相关组件进行重启；
  3. 加强安全运营监控力度，针对告警事件分析研判与处置；
  4. 优化主机、网络安全设备安全策略；
  5. 如非必须禁止内网服务器出外网；
  6. 有效加强访问控制ACL策略，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。

1. 官网存在SQL注入漏洞致网页被篡改

### 事件概述

2020年11月安服应急响应团队接到某教育机构应急响应求助，教育机构官网遭到恶意篡改，部分页面自动跳转至违法网站，希望进行分析排查溯源。

应急响应人员抵达现场后，通过了解现场网络架构及应用部署情况，对受害页面以及Web应用文件进行排查，发现网站目录中存在已被利用的Webshell文件，创建时间为事发前一晚23点，应急人员通过测试，发现网站后台图片上传处存在任意文件上传漏洞。通过提取网站Web应用日志进行分析，发现在事发前一天下午3点，有境外IP（x.x.x.119）对网站A发起SQL注入攻击，并成功获取到了网站后台管理员账号及密码。

经过一系列排查分析，应急人员成功溯源攻击途径，攻击者（x.x.x.119）在事发前一天下午3点发现网站A存在SQL注入漏洞，并对其进行利用，成功获取网站后台管理员账号及密码。事发前一晚23点，攻击者假冒管理员身份登录后台，发现后台页面存在任意文件上传漏洞，利用该漏洞成功上传Webshell文件。事发当天，攻击者利用已上传的Webshell对网站源代码进行修改，将网站部分页面跳转至违法页面。

### 防护建议

* 1. 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；
  2. 对服务器开展安全大检查，包括但不限于恶意IP封禁、恶意文件以及后门清理、网站漏洞检测及修复等；
  3. 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；
  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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
  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，对安全事件发生时可提供可靠的追溯依据。

1. 编辑器漏洞致网站被挂黑页

### 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。



图2-5：攻击路径图

### 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。

1. APT类事件典型案例

APT攻击，即高级可持续威胁攻击,也称为定向威胁攻击，具有极强的隐蔽性和针对性，通常会利用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击，常见如利用账号密码外泄，钓鱼邮件等方式，借以达到监听、窃取重要信息的目的。

1. APT组织利用弱口令进行攻击

### 事件概述

2018年12月，奇安信集团安服团队接到某法院遭到APT攻击事件应急响应请求，其发现天眼存在APT告警行为，服务器存在失陷迹象，因此要求对服务器进行排查，同时对攻击影响进行分析。

应急人员到达现场后，对内网服务器文件、服务器账号、网络连接、日志等多方面进行分析，发现内网主机和大量服务器遭到APT组织lazarus的恶意攻击，并被植入恶意Brambul 蠕虫病毒和Joanap 后门程序。

经过分析排查，本次事件中APT组织所使用的是通过植入恶意Brambul 蠕虫病毒和Joanap 后门程序，进行长期潜伏，盗取重要信息数据。黑客通过服务器ssh弱口令暴破以及利用服务器“永恒之蓝”漏洞对服务器进行攻击，获取服务器权限，并通过主机设备漏洞对大量主机进行攻击，进而植入蠕虫病毒以及后门程序，进行长期的数据盗取。

### 防护建议

* 1. 内网主机存在入侵痕迹，并存在可疑横向传播迹象，建议对内网主机做全面排查，部署终端查杀工具做全面查杀；
  2. 内网服务器存在未安装补丁现象，建议定期做补丁安装，做好服务器加固；
  3. 整个专网可任意访问，未做隔离，建议做好边界控制，对各区域法院间的访问做好访问控制；
  4. 服务器运行业务不清晰，存在一台服务器存在其它未知业务的现象，建议梳理系统业务，做好独立系统运行独立业务，并做好责任划分；
  5. 失陷服务器存在异常克隆账号风险，建议全面排查清理不必要的系统账号；
  6. 需严格排查内外网资产，做好资产梳理，尤其是外网出口做好严格限制；
  7. 应用服务器需做好日志存留，对于操作系统日志，应定期进行备份，并进行双机热备，防止日志被攻击者恶意清除，增大溯源难度；
  8. 系统、应用相关的用户杜绝使用弱口令，同时，应该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；
  9. 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；
  10. 重点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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
  11. 部署全流量监测设备，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。

1. APT组织利用"白+黑"技术进行攻击

### 事件概述

2019年6月，奇安信安服团队接到某事业单位应急请求，其内网有四台机器疑似被海莲花APT组织控制，该单位要求提取对应样本，以确认事件的真实性。

应急响应人员通过对4台疑似受控机进行分析，判定确为海莲花受控机器。攻击者利用海莲花常用的“白加黑”技术，通过在主机目录下植入恶意文件AdobeFlash.exe、goopdate.dll，其中，AdobeFlash.exe是具有google签名的伪造的GoogleUpdate.exe，goopdate.dll是精心伪造的恶意文件，AdobeFlash.exe（GoogleUpdate）程序启动时，会自动加载动态链接库goopdate.dll执行。

海莲花使用典型的"白+黑"方式伪装释放文件，用于迷惑用户以及安全防护产品，达到免杀的目的。并且每个"黑"文件样本的变换后的数据也不相同，主要是由于加密密钥不同，在运行时先进行解密，然后在内存中执行解密后的shellcode。

### 防护建议

* 1. 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；
  2. 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；
  3. 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；
  4. 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；
  5. 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。

1. APT组织利用外泄的账号密码进行攻击

### 事件概述

2020年3月，奇安信安服团队接到某科技公司应急响应请求，其疑似内网受到海莲花APT组织的攻击，请求溯源和应急处置。

应急人员到达现场后发现该公司所使用的云桌面目录下存在恶意木马DLL文件，通过大量日志分析发现存在海外IP登录记录，该海外IP经奇安信红雨滴实验室分析确认，属于海莲花常用的跳板机IP，确认该公司受到了海莲花APT攻击。通过流量分析找到最先入侵的A主机，并且此机器上存在某系统相关服务器的SSH登录用户名及密码，可以成功登录服务器B。

最终确认攻击途径，由于账号密码外泄，攻击者利用信息收集，成功从海外控制A主机，又因A主机无法出网，且存有服务器B的SSH登录用户名及密码，攻击者成功登录服务器B，并以服务器B作为跳板进行端口转发，实现A主机外连。

### 防护建议

* 1. 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；
  2. 定期进行内部人员安全意识培养，增强内部人员密码管理意识，禁止将密码进行本地保存，禁止将敏感信息私自暴露至公网等；
  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. 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；
  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。

1. APT组织利用钓鱼邮件进行攻击

### 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。

### 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。

1. DDOS类事件典型案例

DDOS攻击，即分布式拒绝服务攻击，其目的在于使目标电脑的网络或系统资源耗尽，使服务暂时中断或停止，导致其正常用户无法访问。CC攻击使用代理服务器向受害服务器发送大量貌似合法的请求（通常为HTTP GET），通常会导致网站出现了无法进行操作的情况，不仅仅影响了用户的正常使用，同时造成的经济损失也是非常大的。

1. 某部委遭遇CC攻击

### 事件概述

2018年3月，奇安信集团安服团队接到某部委的网站安全应急响应请求，网站存在动态页面访问异常缓慢现象，但静态页面访问正常，同时WAF、DDoS设备出现告警信息。

应急响应人员通过对现场技术人员所提供WAF告警日志、DDoS设备日志、Web访问日志等数据进行分析，发现外部对网站的某个动态页面全天的访问量多达12万次，从而导致动态页面访问缓慢。

根据本次攻击事件的分析，造成网站动态页面访问缓慢的原因主要是攻击者频繁请求“XXX页面”的功能，同时该页面查询过程中并未要求输入验证码信息，大量频繁的HTTP请求以及数据库查询请求导致CC攻击，从而使服务器处理压力过大，最终导致页面访问缓慢。

### 防护建议

* 1. 对动态页面添加有效且复杂的验证码功能，确保验证码输入正确后才进入查询流程，并每次进行验证码刷新；
  2. 检查动态页面是否存在SQL注入漏洞；
  3. 加强日常监测运营，开启安全设备上的拦截功能，特别对同一IP的频繁请求进行拦截封锁；
  4. 建议部署全流量的监测设备，从而弥补访问日志上无法记录POST具体数据内容的不足，有效加强溯源能力；
  5. 相关负载设备或反向代理上应重新进行配置，使Web访问日志可记录原始请求IP，有助于提高溯源分析效率；
  6. 开启源站保护功能，确保只允许CDN节点访问源站；
  7. 定期开展渗透测试工作以及源代码安全审计工作。

1. 某证券公司遭遇DDoS攻击

### 事件概述

2018年6月，奇安信集团安服团队接到某省网安的应急响应请求，本地证券公司在10日7:00-8:00遭受1G流量的DDoS攻击，整个攻击过程持续了1个小时，造成证券公司网站无法正常访问。同时，多个邮箱收到勒索邮件，并宣称如不尽快交钱会把攻击流量增加到1T。

应急响应人员通过利用奇安信集团大数据平台对网站域名进行分析，发现了Top10 IP地址对被攻击地址进行了DDoS攻击，并发现其攻击类型为NTP反射放大攻击。通过后端大数据综合分析，准确定位了攻击者的真实IP地址。

### 防护建议

* 1. 针对重要业务系统、重要网站等，建立完善的监测预警机制，及时发现攻击行为，并启动应急预案及时对攻击行为进行防护；
  2. 建议部署类似于奇安信集团安域等的云安全防护产品，云端安全防护产品对常见的DDoS、Web行为攻击等进行有效防护。

1. 漏洞利用类事件典型案例

漏洞利用主要是指攻击者利用计算机程序中的某种漏洞，来达到控制计算机权限的目的，从近几年应急数据中，弱口令、WEB常见漏洞、中间件漏洞、服务器漏洞等经常成为攻击者利用的常用攻击方式。同时，设备配置不当和代码编写中存在的逻辑漏洞也成为攻击者高频利用发起攻击的常见手段，造成的经济损失也是非常大的。

1. 内网防护不到位致大量主机失陷

### 事件概述

2019年9月，安服应急响应团队接到某公检法机构应急请求，该机构内网疑似被渗透，3000多台主机失陷，导致业务系统和内部网络瘫痪。

应急人员对受害服务器进行排查，发现网络环境未做全面的防护策略，并且受害服务器版本过低，对外网开放了包含常用端口，如80端口、21端口等，和危险端口，如1433端口等在内的21个服务端口，甚至部分端口存在目录遍历等漏洞。攻击者利用上述系统问题，早在2017年就将webshell木马上传至受害服务器，并获取了该服务器的控制权。之后，攻击者对受害服务器上传了暴力破解工具和字典，并将受害服务器作为肉鸡，成功暴破了内网3575个服务器或终端。

通过本次安全事件，该机构系统暴露了诸多安全隐患，包括未定期开展安全巡检工作，导致内部服务器于2017年就已被攻陷；对外开放端口过多，且包含部分高危端口；员工安全意识不足，大量服务器使用弱密码等。

### 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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
  3. 建议对内网开展安全大检查，检查的范围包括但不限于后门清理、系统及网站漏洞检测等；
  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. 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；
  6. 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；
  7. 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。

1. 网站存在任意文件上传漏洞，致多台主机沦陷

### 事件概述

2020年3月，安服团队接到某医院应急请求，医院服务器被入侵。

应急响应人员通过网站的安全性检测以及系统日志分析发现，网站http://xxx:999存在任意文件上传漏洞，同时发现内网多台主机存在MS17-010漏洞，并且存在被暴力破解的记录。

最终通过对系统的检查和分析确定，攻击者首先对网站http://xxx:999进行访问，在该网站中发现了任意文件上传漏洞，并对其进行利用，通过上传ASP类型的Webshell获取了服务器的管理员权限，进而以该沦陷服务器为跳板机，利用内网多台主机中存在的MS17-010漏洞、RDP弱口令等对其进行攻击，导致多台内网终端沦陷。

### 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. 对系统文件上传功能，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；
  3. 加强权限管理，对敏感目录进行权限设置，限制上传目录的脚本执行权限，不允许配置执行权限等；
  4. 建议对内网服务器及主机开展安全大检查，检查的范围包括但不限于系统漏洞检测（如MS17-010漏洞、任意文件上传漏洞等）、后门检测，并及时进行漏洞修复、补丁安装、后门清理等工作；
  5. 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。

1. 服务器因SQL注入漏洞被攻陷

### 事件概述

2020年6月，安服应急响应团队接到某政府单位应急响应请求，该单位员工发现天眼存在SQL注入告警，需要上机排查服务器是否存在异常。

应急人员在到达现场后，根据天眼SQL注入告警，首先对数据库服务器进行排查，发现该服务器存在大量“powershell.exe”和“mshta.exe”进程。通过对“powershell.exe”进程进行解密，确定该进程为攻击者的远控进程。结合天眼流量分析，确定攻击者于1天前凌晨3时11分左右，利用SQL注入漏洞，对该服务器进行命令执行攻击。查询服务器用户，发现可疑隐藏账户。对业务服务器进行排查发现有Webshell后门脚本文件“1.aspx”和“index.aspx”。

最终确定攻击者利用业务服务器登录处的SQL注入漏洞，进行任意命令执行，并创建隐藏账户、上传后门文件。因该业务服务器和数据库服务器为站库分离设计，故导致业务服务器和数据库服务器均被攻陷。

### 防护建议

* 1. 对用户输入内容进行检查与验证。检查所输入字符串变量的内容，使用白名单，只接受所需的值，拒绝包含二进制数据、转义序列和注释字符的输入内容，限制用户输入内容的大小和数据类型，对输入内容进行强制转换等；
  2. 重要业务系统及核心数据库应设置独立的安全区域，做好区域边界的安全防御工作，严格限制重要区域的访问权限并关闭不必要、不安全的服务；
  3. 禁止重要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；
  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. 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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵。

1. 机顶盒配置不当致堡垒机被攻陷

### 事件概述

2020年8月，某运营商的安全设备监控到一台堡垒机前置机对内网其他服务器发起攻击行为，怀疑服务器已沦陷，向奇安信安服团队发起应急响应请求，希望对其内网服务器进行排查。

应急响应人员抵达现场后发现有两台服务器遭受不同程度地攻击，通过对可疑服务器进行排查溯源后发现，攻击者利用机顶盒配置不当连接本地机顶盒网络，从而访问堡垒机前置机等多台内网服务器。攻击者一方面利用前置机远程桌面服务端弱口令获取前置机权限，投放恶意程序及勒索病毒，然后在内网内横向移动传播恶意程序；另一方面在取得堡垒机控制权后利用Weblogic反序列化漏洞对端到端诊断系统实施多种敏感命令执行及漏洞探测行为，掌握系统敏感数据。

通过进一步地对服务器进行溯源后发现，早在事件发生前一个半月，攻击者就已经对服务器暴露在公网的3389端口发起大量暴力破解攻击，尝试获取服务器权限，但均登录失败，暴露身份信息。

应急响应人员立即排查全网资产，封禁恶意IP地址，关闭不必要的公网危险端口，增强访问策略，部署安全加固软件。

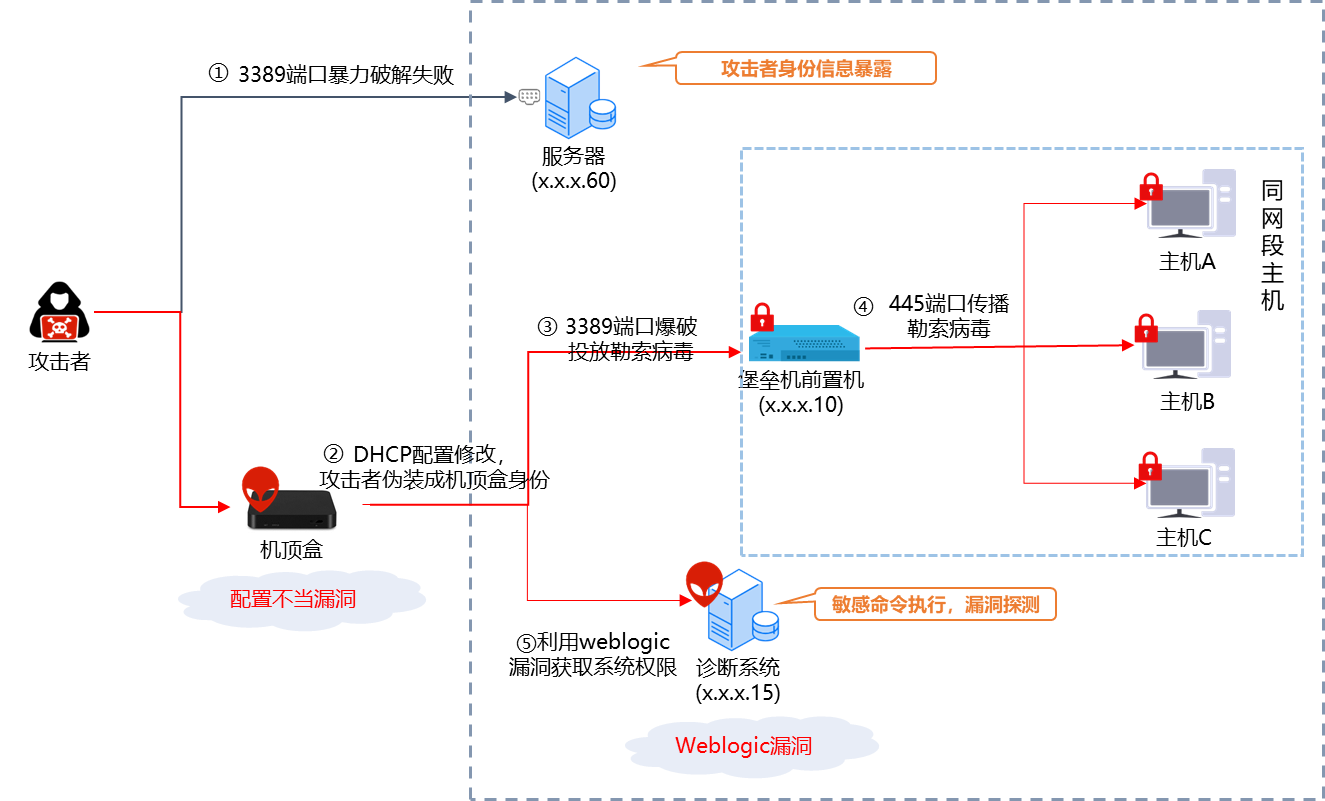


图2-6：攻击路径图

### 防护建议

* 1. 加强内部访问策略，增加访问控制策略。
  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；
  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（如MS17-010漏洞等）、安装补丁，将信息安全工作常态化。

1. 公网应用平台因Shiro反序列化漏洞被攻击

### 事件概述

2020年8月，奇安信安服团队接到某政府部门应急请求，该部门安全设备发现服务器反弹shell告警，需要进行排查溯源。

奇安信安服应急人员通过天眼告警与系统日志分析对受害资产梳理发现，其公网应用平台http://115.xx.xx.1/xx/采用Apche Shiro框架存在Shiro反序列化漏洞，内网做负载均衡的两台服务器被上传有webshell记录、frp内网穿透代理工具，公网出口地址与外网攻击者vps进行连接通信。

经最终分析研判确定，攻击者首先通过收集网上Shiro框架默认密钥，多次对应用平台http://115.xx.xx.1/xx接口利用Shiro RememberMe反序列化漏洞进行攻击，攻击成功后执行whoami、ifconfig等系统命令，然后利用远程命令执行使两台内网服务器从公网vps1下载webshell，访问webshell发现未解析随后删除webshell，进而下载frp内网穿透代理客户端并运行，最终将shell反弹至公网vps2服务器上面实现内网穿透并进行远程控制。

### 防护建议

* 1. 封禁攻击者服务器IP、公网vps1、公网vps2；
  2. 对应用平台网站进行关闭或者使用白名单方式访问；
  3. 对Apache shiro框架进行版本更新，删除默认密钥，生成随机密钥方式登录；
  4. 加强安全运营监控力度，针对告警事件分析研判与处置；
  5. 优化主机、网络安全设备安全策略；
  6. 如非必须禁止内网服务器出外网；
  7. 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。

1. 钓鱼邮件类事件典型案例

钓鱼邮件攻击是指攻击者通过利用伪装的电子邮件，欺骗、诱使收件人点击下载达到窃取账号密码、执行恶意程序的目的。攻击者结合社工手段，利用政企机构人员安全意识薄弱的特点，进行有针对性的、较高目标价值的精准打击，用以骗取账号密码信息进行进一步投毒等操作，造成更大的危害。

1. 利用钓鱼邮件，伪造打款信息

### 事件概述

2019年9月，某能源行业企业发现黑客伪造邮件，试图欺骗项目方打款到非项目银行账户中。由于发现及时，该企业已紧急与项目方进行联系，提醒项目方注意防范伪造邮件，未造成严重后果。应急人员前往现场进行溯源工作。

应急人员对邮件服务器进行分析，发现邮件网关日志授权已经过期，导致日志记录时间较短，无法获取有用信息。此外，邮箱系统中存在大量垃圾邮件及恶意邮件，对其中一封恶意邮件进行分析，发现黑客以OA系统升级为由，欺骗用户点击制作好的域名网站，从而获取用户账号及密码。之后，应急人员对伪造邮件进行查看，发现黑客为了不使项目方察觉，在邮件中假装抄送了原邮件中的项目组成员，但将真实邮箱的后缀xx.com全改为xxj.co进行伪造，企图蒙骗收件人相信邮件内容，从而将项目资金汇入黑客账户中。

最终，应急人员通过对以上内容进行分析，认为黑客可能是通过以下方式对内部进行攻击：①项目组邮箱、企业邮箱及邮件中抄送或转发的邮箱中存在弱口令，被黑客暴力破解登录；②项目组及企业相关人员点击了钓鱼邮件导致邮箱密码泄露，或执行了恶意文件导致电脑被控制；③企业项目伙伴邮件服务器存在漏洞，被黑客利用获取邮件内容。

### 防护建议

* 1. 定期进行内部人员安全意识培训，禁止点击来源不明的邮件附件，禁止将敏感信息私自暴露至公网等；
  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，加强内部人员安全意识，禁止密码重用的情况出现；
  3. 公私邮箱分离，禁止使用办公邮箱注册游戏、购物、社交和论坛等第三方应用账户及公共网站的服务，禁止用工作邮箱发送私人邮件；
  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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵。

1. 破解管理员弱密码，发起钓鱼邮件攻击

### 事件概述

2019年11月，安服应急响应团队接到某科研集团应急需求，其邮箱系统遭受钓鱼邮件攻击，邮箱系统超级管理员账户被盗，导致集团组织架构，以及包含集团领导在内的近200名员工信息泄露。

应急人员抵达现场后对邮件服务器进行排查，发现邮箱系统超级管理员账户admin密码为弱口令，攻击者利用SMTP暴破获取了超级管理员账户admin的控制权。之后，攻击者使用该账户向集团180名员工邮箱发送可盗取用户账号及密码的钓鱼邮件，并成功钓鱼了至少4名集团员工的邮箱账户，删除了邮箱中网管人员发送的预防钓鱼事件的邮件。最终，导致了集团组织架构信息，以及包含集团领导在内的近200名员工信息泄露。

综上所述，超级管理员用户邮箱使用弱口令，以及集团内部员工安全意识不足是导致本次安全事件的主要因素，可见增强员工网络安全意识对企业网络安全至关重要。

### 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. 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. 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. 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；
  5. 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；
  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。

1. 下载破解软件，导致内网终端自动发送恶意邮件

### 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，该主机中天擎存在多个“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，天擎就曾有相关拦截提示。事发当天，因误操作，对天擎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，后又因误操作对天擎弹出的告警点击了“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。

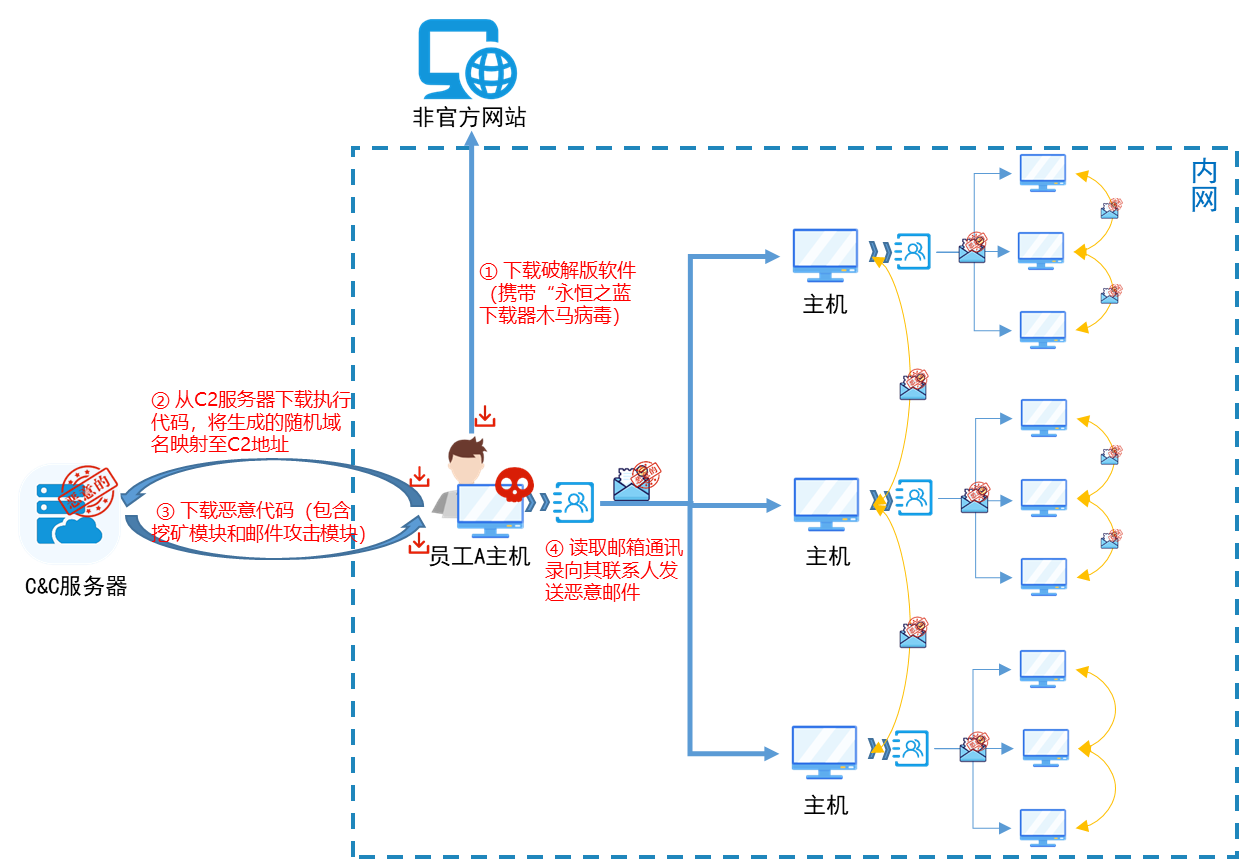


图2-7：攻击路径图

### 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。

1. 数据泄露类事件典型案例

数据泄露指将机密信息、私人信息或其他敏感信息发布到不安全的环境中。数据泄露分为外部泄露和内部泄露两种，外部泄露典型如攻击者通过漏洞利用等方式获取了主机账号密码进行的数据窃取，内部泄露典型如员工安全意识薄弱将敏感信息上传至公网、使用带病毒的U盘或非正规的软件导致的数据泄露。数据泄露会导致敏感信息以及重要信息的外泄，一旦被不法分子所利用，造成的危害是非常严重的。

1. 账号信息上传公网，致内网20多台机器受感染

### 事件概述

2020年2月，安服团队接到某运输公司应急请求，该公司通过天眼发现存在服务器失陷的危急告警。

应急人员通过分析天眼发现，该公司内部环境中20余台服务器出现失陷告警，其中两台重要服务器上发现被植入后门，服务器已沦陷，同时多台服务器上均发现Frp代理、CobaltStrike上线脚本与漏洞利用工具使用痕迹，攻击者正在通过Frp代理对内网服务器进行SQL注入漏洞攻击。

通过人工排查，发现该公司内部某员工上传敏感信息到GitHub中，导致敏感数据泄露，攻击者利用该员工账号登录VPN对该公司某重要服务器发起攻击，并利用Redis未授权访问漏洞获得权限，上传Frp代理工具、MS17-010等漏洞利用工具，进行内网横向渗透，成功攻下内网服务器、主机20余台，并利用已攻陷机器在内网中进行横向攻击。

### 防护建议

* 1. 定期进行内部人员安全意识培养，禁止将敏感信息私自暴露至公网，禁止点击来源不明的邮件附件等；
  2. 为Redis服务添加密码验证，为Redis服务创建单独的user和home目录，并且配置禁止登录，低权限运行Redis服务；
  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（如MS17-010漏洞等）、安装补丁，将信息安全工作常态化；
  4. 建议配置VPN登录的双因素认证，如增加手机短信验证码认证等，严格控制用户登录，防止账号信息被盗用。

1. 系统漏洞造成数据泄露

### 事件概述

2020年3月，安服应急响应团队接到某市医药公司应急请求，公司DMZ服务器区出口地址存在外连行为。

应急人员排查分析，发现对外攻击的IP为该公司内网某系统的出口地址，因该系统供应商要求对系统进行远程维护，特将服务器的3389端口映射到出口地址的3389端口。通过对IPS、负载均衡、防火墙以及服务器系统日志进行分析排查，发现内网某系统存在多个地区和国家的IP通过3389端口远程登录记录和木马文件。对该服务器系统部署文件进行排查，发现此服务器存在任意文件写入漏洞，并且发现两个Webshell后门。

经分析研判最终确定，攻击者通过内网某系统映射在公网的3389端口进行远程登录，并上传Webshell后门1，用于执行系统命令；利用该系统任意文件写入漏洞，上传Webshell后门2，用于上传任意文件，写入恶意木马文件，对外网发起异常连接，进行数据传输。

### 防护建议

* 1. 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；
  2. 加强设备权限管理，对敏感目录进行权限设置，限制上传目录的脚本执行权限，不允许配置执行权限等；
  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；
  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；
  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。

1. 僵尸网络类事件典型案例

僵尸网络是指采用一种或多种传播手段，将大量主机感染病毒，从而控制被感染主机，形成可一对多控制的僵尸网络。近几年的应急中，也不乏合法网站被僵尸网络侵害的案例。攻击者通常利用漏洞攻击、口令暴破或邮件病毒等方式发起攻击，在内网中进行窃取信息、发起DDOS攻击或僵尸网络挖矿等行为，使网络安全受到严重威胁，危害巨大。

1. 安全设备弱口令致内网被僵尸网络控制

### 事件概述

2019年4月，安服应急响应团队接到某大学僵尸网络事件的应急请求，现场多台终端发现疑似黑客活动迹象，重要网站系统遭到黑客攻击，无法正常运行。

应急响应人员通过对重要网站系统进行排查分析，发现该业务系统存在大量IPC暴破登录行为，内网多台主机被多次登录成功，且存在数个僵尸网络远控IP登录行为，其中，某一控制端存在大量国外IP连接行为。同时，应急人员发现其网站运维管理审计系统暴露于公网，并存在弱口令现象，攻击者通过该系统可取得大量服务器的控制权限，且很多敏感安全设备均暴露在公网上，包括WEB应用防火墙、日志中心、漏洞扫描系统、超级终端等。攻击者通过暴露于公网的审计系统弱口令暴破登录进入内网，并以此为跳板，对内网多台服务器、主机进行暴破、投毒并进行横向扩散，组成僵尸网络。

### 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. 重要业务系统及核心数据库应设置独立的安全区域，做好区域边界的安全防御工作，严格限制重要区域的访问权限并关闭不必要、不安全的服务；
  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. 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、防范漏洞利用等方式，提高系统安全基线，防范黑客入侵；
  5. 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；
  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：4009-727-120。

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。

