内部发行 免费赠阅

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

抗击未来的勒索攻击

P14

第21期

2022 年 9 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

奇安信安全托管服务以威胁发现为基础、以分析处置为核心、以发现隐患为关键、以解决客户问题为目标，7*24小时全天候全方位守护客户网络安全。

两种模式
模式随心选择

- 直营服务模式：奇安信产品+MSS
- 合作服务模式：技术、产品、服务整体托管

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

- 集中服务化：统一监测、预警与通报
- 服务集中化：标准统一、质量可控、资源共享

首创“云地结合”模式

打破传统的托管仅限“云端监测”的认知开辟“云地结合”模式，云端+地端实现真正的闭环服务。

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

专家通过视频一对一的方式与您“面对面”沟通指导，不仅让您了解现状，还能防患于未然。

主动安全化解勒索攻击风险

9 月份，勒索软件组织 REvil 声称，对我国最大的某电器制造商进行了勒索攻击，窃取了数 TB 的数据。勒索软件组织 REvil 此前因对肉类供应商 JBS 和软件公司 Kaseya 的勒索攻击而闻名，对后者的攻击感染了数百个机构。我国这家电器制造商显然是其最新的勒索攻击受害者。

2022 年上半年，勒索组织创造了新的攻击方法，瞄准本已紧张的供应链，导致数百家企业的业务运营中断。此外，窃取勒索、三重勒索等勒索攻击技术出现。不断演进的攻击技术，越来越多的勒索攻击受害者，都在挑战我们的防御思维。

实际上，频发的攻击事件暴露出当前防御的缺陷，推动防御性思维逐渐发生变化：向主动安全演进或许才是应对网络攻击的有效方式。

2018 年，美国国防部发布的网络安全战略，将“主动防御”调整为更具进攻性的“防御前置”。基于主动安全理念的防御前置成为美军网络安全的指导战略。2022 年前后，美国网络国家任务部队（CNMF）在 18 个国家 / 地区开展了 35 次的狩猎行动，发现和消除网络与系统上的未知威胁。由美欧、中东非、亚太安全领导者组建网络防御者委员会建议，将“防御前置”战略用于指导私营机构安全防护。

主动安全防护强调攻击面的有效管理，部署零信任、动态监测等技术手段，提升人员安全意识，开展主动狩猎等主动安全策略。

攻击面的管理可以减少攻击入口。数字化推进，令机构拥有大量自身都不了解、不掌握的攻击面，其中可能隐藏大量的安全漏洞。通过网络测绘手段，发现和管理攻击面，可以缩减潜在的攻击入口；此外，通过模拟攻击、基于风险的漏洞管理技术，快速识别网络漏洞并确定漏洞优先级，可以立即部署解决方案，保护关键资产免受攻击。

开展威胁狩猎和动态监控可以在勒索软件攻击实施前进行阻止，这里涉及对于主要攻击组织及其最新攻击手段、工具和流程的主动了解。对于缺乏资金、技能的机构来说，可以考虑外包给托管检测和响应 (MDR) 专家。

零信任访问也被视为主动安全的重要措施。微隔离、持续验证、最小访问权限等零信任访问技术，可以有效终止异常的访问行为。

安全意识培训是经常被忽视却非常重要的措施。95% 的安全事件都与人为措施有关。目前钓鱼攻击与社工手段依然是攻击者经常采用、且非常有效的攻击手段。通过培训员工识别不良链接、恶意附件和可疑邮件，显然可以降低遭受攻击的概率。

转向主动安全意味着不再容忍安全事件的发生。越早启动这一转变，越能在应对网络威胁中把握主动。

总编辑

李建平

2022 年 9 月 1 日

CONTEN

目录

安全态势

P4 | 澳门健康码曾遭来自欧美地区网络攻击，达 300 多万次

P4 | 俄罗斯主要电视台再次播放“反战信息”：遭亲乌黑客劫持

P4 | 乌克兰网络攻击致 2400 多个俄罗斯网站瘫痪，含俄最大银行

P5 | 西北工业大学遭网络攻击，源头系美国国家安全局

P5 | 恶意黑客“操纵”网约车订单，在俄罗斯首都制造交通拥塞

P5 | 政务全瘫痪，电力转手动！黑山政府遭受超大规模网络攻击

P6 | Apple Kernel 本地权限提升漏洞安全风险通告

P6 | Chrome 浏览器沙箱逃逸漏洞在野利用风险通告

P6 | GitLab 安全漏洞 (CVE-2022-2884) 安全通报

P7 | 国内攻防演习 8 月态势：哪些薄弱点最易被利用?

P10 | 网信办《关于修改〈中华人民共和国网络安全法〉的决定》公开征求意见

P10 | 国家标准《信息安全技术 网络数据分类分级要求》公开征求意见

P10 | 《中华人民共和国反电信网络诈骗法》表决通过

P11 | 《公路水路关键信息基础设施安全保护管理办法》公开征求意见

P11 | 欧盟提出《网络弹性法案》，数字产品必须遵守安全基线

P12 | 《网络安全法》修改解读：加大违法处罚力度，提升全社会守法意识

月度专题

抗击未来的勒索攻击

P14

新的勒索形式、越来越多的附属团伙，重新塑造勒索软件攻击

攻防一线

P36

网络流量“指挥大师”是怎样炼成的?

安全之道

P40

护航三农金融天眼助力江苏省联社打造全行威胁感知大脑

安全叨客

P48

一次勒索，180 人
摧毁了一个 600 万人帝国

奇安信人

P44

与勒索黑产对抗，
星星之火，可以燎原

奇安资讯

P52 | 齐向东出席算力产业大会：以“零信任”为基础支撑“东数西算”安全发展
P52 | 亮相世界智能网联汽车大会：以“零事故”为目标 构建安全的车联网
P53 | 奇安信亮相 30 省 50 城市国家网络安全宣传周
P54 | 聚势赋能 奇安信集团投资生态大会举行
P55 | 吴云坤出席金砖国家数字经济对话会
P55 | 奇安信集团与东方通达成战略合作 共同构筑安全生态合作圈
P56 | “关基条例一周年”专题研讨会成功举办
P56 | 齐向东出席 2022 互联网岳麓峰会：数据大集中要谨防“蚂蚁搬家式盗窃”
P57 | 数据交易沙箱获 2022 年大数据产业发展试点示范项目
P57 | 奇安信天擎独家入选第二批 Windows 7 操作系统安全防护产品目录
P58 | 奇安信通过信通院 CWPP 云工作负载保护平台能力评估
P58 | “极盾 -2021”推荐名录出炉 奇安信 7 款产品上榜
P59 | 奇安信集团总裁吴云坤获 CSO 名人堂中国安全十大人物

《网安 26 号院》编辑部
主办 奇安信集团

总　　编　　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
攻防一线主编：魏开元
安全之道主编：张少波
奇安信人主编：孙丽芳
安全叨客主编：王梦琪
奇安资讯主编：陈　冲
研究报告主编：包世玉

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557
出版物准印证号：京内资准字 2122- L0058 号
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2022 年 9 月 26 日
发行对象：奇安信集团内部

事件篇

我国网络安全形势依然严峻，西北工业大学、澳门健康码均遭到过境外网络攻击，畅捷通财务软件漏洞被利用引发多起勒索攻击事件，俄乌冲突也导致部分国内用户数据遭牵连泄露。

澳门健康码曾遭来自欧美地区网络攻击，达 300 多万次

据环球时报 9 月 16 日消息，澳门保安司司长黄少泽在一场修改《维护国家安全法》咨询会上透露，去年 5 月初，澳门健康码连续两天遭受境外网络攻击，导致部分人无法转换粤康码，珠澳出入境大受影响，关口一度人流拥挤。经调查发现这是来自欧美地区的持续性攻击，多达 300 多万次。特区政府认为这并非普通的网络攻击，明显是想影响澳门的整体社会运作。澳门司警局局长薛仲明称，澳门每天都遭到大大小小的网络攻击，去年平均每分钟约受到 3.4 次攻击。

俄罗斯主要电视台再次播放“反战信息”：遭亲乌黑客劫持

据 TheRecord 9 月 13 日消息，亲乌克兰黑客团伙“hdr0”宣称入侵了俄罗斯电视频道并播放反战信息，Channel One Russia、Russia-24、Russia-1 等多个俄罗斯电视频道均受到攻击影响。被黑的电视频道播放了俄罗斯攻击乌克兰城市的暴力镜头，还播放了乌克兰总统泽连斯基及其他国家领导人对于俄开战行为的谴责。目前尚不清楚有多少观众看到了该团伙发布的反战信息。今年 5 月俄罗斯多个电视频道也遭到篡改，广电媒体已经成为俄乌冲突期间的网络攻击重点。

乌克兰网络攻击致 2400 多个俄罗斯网站瘫痪，含俄最大银行

据央视新闻 9 月 12 日消息，乌克兰数字化转型部当天宣布，8 月 29 日—9 月 11 日，乌克兰方面通过网络攻击致使 2400 多个俄罗斯网站瘫痪，其中包括俄罗斯媒体、俄罗斯最大银行和俄罗斯最大的汽车和零部件在线销售平台等。目前，俄罗斯方面尚未对相关说法作出回应。

中科大发 4 万封“免费送月饼”钓鱼邮件，超 3000 人中招信息被“骗取”

据上游新闻 9 月 8 日消息，正值国家网络安全宣传周之际，中国科学技术大学网络信息中心举行首次钓鱼邮件演练，向全校师生发送了超 4 万封“免费送月饼”主题、有较明显错误痕迹的钓鱼邮件，测试师生们的反诈骗能力。校方通报显示，有 3500 余人在假冒邮件的钓鱼链接中提交了个人信息，其中人数最多的是大一新生。策划老师称，下一步会着重对他们进行网络安全培训。

西北工业大学遭网络攻击，源头系美国国家安全局

据央视新闻 9 月 5 日消息，国家计算机病毒应急处理中心和 360 公司分别发布了关于西北工业大学遭受境外网络攻击的调查报告。技术团队先后从西北工业大学的多个信息系统和上网终端中提取到了多款木马样本，经综合研判分析，初步判明相关攻击活动源自美国国家安全局下属的“特定入侵行动办公室”。调查发现，“特定入侵行动办公室”多年来对我国国内的网络目标实施了上万次的恶意网络攻击，控制了数以万计的网络设备，窃取了超过 140GB 的高价值数据。

恶意黑客“操纵”网约车订单，在俄罗斯首都制造交通拥塞

据 Vice 9 月 3 日消息，恶意黑客在俄罗斯网约车应用 Yandex Taxi 上一口气预约几十辆出租车，直接导致首都莫斯科发生交通堵塞。社交媒体上流传的视频显示，大批出租车纷纷出现在一条原本就不太顺畅的道路上，造成了长时间交通堵塞。推特账号 @runews 分享了该视频，推文已被转发近万次。Yandex 公司发言人表示，该问题“在不到一小时内”得到解决。这是目前已知首批利用网约车应用造成交通混乱的案例之一。

政务全瘫痪，电力转手动！黑山政府遭受超大规模网络攻击

据美联社 9 月 1 日消息，欧洲国家黑山政府遭遇超大规模网络攻击，此次攻击为勒索软件与 DDoS 混合攻击，不仅扰乱了政府服务，导致国防部、财政部、内政部等主要政府网站均无法访问，还迫使该国电力系统转为手动控制。会说俄语的 Cuba 勒索软件团伙声称对此负部分责任，他们攻击了黑山议会办公室，要求支付 1000 万美元赎金。这起事件富含地缘政治色彩，该国认为攻击者可能是由俄罗斯相关部门控制的，并正在协同北约国家帮助他们做事件响应、防御和恢复。

畅捷通漏洞被勒索软件利用攻击国内企业！工业和信息化部漏洞平台发布预警

综合消息，国内多家安全厂商发布预警称，8 月 28 日起国内某企业财务软件 0day 漏洞可能遭到大规模勒索利用，已出现上千起使用该软件的企业勒索软件攻击案例，中招用户被勒索 0.2 比特币（约 2.7 万元人民币）。30 日，工业和信息化部网络安全威胁和漏洞信息共享平台发布预警称，畅捷通 T+ 软件存在远程代码执行的超危安全漏洞。该漏洞已被攻击者利用进行勒索病毒攻击，导致多起服务器因受到攻击，造成数据被加密的事件。建议受影响的单位和用户立即升级到最新版本。

俄罗斯流媒体巨头遭恶意攻击，210 万中国用户数据泄露

据 TheRecord 8 月 29 日消息，俄罗斯流媒体巨头 START 表示，其客户的个人信息在一次网络攻击中被泄露。根据最先爆料的俄罗斯 Telegram 频道“Information Leaks”透露，泄露数据库总计 72 GB 大小，包含 4400 万客户的数据（其中包括 745 万个唯一电子邮箱），有用户名、邮箱、哈希密码、IP、注册国、订阅时间等信息，其中有 210 万条用户信息注册国为中国。

漏洞篇

国内财务软件公司畅捷通旗下 T+ 软件存在远程代码执行漏洞，已被攻击者利用进行勒索病毒攻击，导致多起服务器数据被加密的事件。建议相关用户尽快升级至最新版。

Apple Kernel 本地权限提升漏洞安全风险通告

9 月 15 日，奇安信 CERT 监测到苹果公司发布了多个产品的安全更新，披露了已被在野利用的 Apple Kernel 本地权限提升漏洞 (CVE-2022-32917)。macOS Monterey、macOS Big Sur、iOS 和 iPadOS 存在权限提升漏洞。经过身份认证的本地攻击者可通过在目标系统上运行特制应用程序来利用此漏洞，成功利用此漏洞可在目标系统上以内核权限执行任意代码。目前，官方已监测到在野利用，鉴于此漏洞影响范围较大，建议用户尽快做好自查及防护。

Chrome 浏览器沙箱逃逸漏洞在野利用风险通告

9 月 4 日，奇安信 CERT 监测到 Google Chrome 官方紧急发布安全更新，修复了 Chrome 沙箱逃逸漏洞 (CVE-2022-3075)。由于 Mojo 中不恰当的数据验证，攻击者可通过多种方式诱导用户访问恶意的链接来利用此漏洞。这类漏洞通常需要配合其他远程代码执行漏洞使用，可突破浏览器沙箱限制在目标系统上执行任意代码。目前，官方已监测到在野利用，鉴于此漏洞影响范围较大，建议用户尽快做好自查及防护。

GitLab 安全漏洞 (CVE-2022-2884) 安全通报

9 月 2 日，国家信息安全漏洞库（CNNVD）收到关于 GitLab 安全漏洞（CVE-2022-2884）情况的报送。经身份验证的攻击者利用该漏洞可导入恶意制作的项目，进而导致在目标系统远程代码执行。GitLab（CE/EE）多版本受到漏洞影响。目前，GitLab 官方已发布新版本修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。GitLab 是美国 GitLab 公司的一款软件项目仓库应用程序。

畅捷通 T+ 软件存在任意文件上传漏洞的安全公告

8 月 30 日，国家信息安全漏洞共享平台（CNVD）收录了畅捷通 T+ 软件任意文件上传漏洞（CNVD-2022-60632）。未经身份认证的攻击者可利用漏洞远程上传任意文件，获取服务器控制权限。目前，已出现用户被不法分子利用该漏洞进行勒索病毒攻击的情况，厂商已发布安全更新完成修复。CNVD 建议受影响的单位和用户立即升级到最新版本。

对抗篇

国内攻防演习 8 月态势：哪些薄弱点最易被利用?

作者 奇安信安服团队

一、本月演习整体情况

2022 年 8 月，奇安信 Z-TEAM 团队共承接攻防演习服务 58 场，其中国家级攻防演习 1 场，行业级攻防演习 2 场，省级攻防演习 10 场，省级行业攻防演习 7 场，地市级攻防演习 17 场，本单位自主攻防演习 21 场。

本月攻防演习成果如下图:

二、本月任务目标特点

本月攻防演习和评估任务覆盖行业比较分散，涉及目标包括金融、政务、能源、医疗、交通、教育等，客户存在的主要安全问题为互联网侧应用组件存在漏洞、业务系统敏感信息泄露、内部人员对钓鱼攻击防范意识不足、内网网络功能区域缺乏安全隔离、弱口令及口令复用等。具体情况如下:

1、历史漏洞利用仍是主要突破手段

本月任务中针对多行业不同目标网络，互联网侧漏洞利用占据了主要部分。漏洞主要集中在协同办公 OA 系统、互联网业务平台和门户网站，漏洞利用类型主要包括未授权访问、远程命令执行、文件上传与下载、敏感信息泄漏与 SQL 注入等，这些漏洞仅有少数是未公开的 0day 漏洞，多以历史漏洞为主，历史漏洞基本都是由于没有及时升级、更新应用造成的。历史漏洞的存在是目标网络的重大安全威胁。

2、访问策略存在缺陷是外部成功突破的重要因素

本月任务中，多个行业网络的不同外部业务系统存在未授权访问问题，可以通过未授权访问漏洞直接访问这些外部系统后台，进而可以利用访问权限执行后台命令或获取后台配置文件、数据库配置等敏感信息。未授权访问多因对外部接入的安全配置或权限认证相关策略设置存在缺陷，且传统的授权认证体系无法根据用户属性、用户行为及环境状态进行用户权限动态控制，导致授权认证机制成为被外部攻击成功突破的重要因素。

3、弱口令和口令复用造成内网重大安全隐患

本月任务表现出弱口令和口令复用仍是目标网络的重大安全隐患。弱口令或口令复用会导致目标系统内网安全措施形同虚设，尤其是内网堡垒机、网管系统、域控和网关等核心网络节点。弱口令和口令复用的存在，为攻击者实现内网重要服务器、网关路由、网管系统和域控等核心网络节点的拓展控制带来极大便利，最终致使业务内网全面失陷。

4、钓鱼攻击是实现网络突破的得力手段

本月任务中，针对特殊行业目标系统网络，钓鱼攻击成为主要突破手段，攻击者通过伪装成可以信任的角色，利用电子邮件、微信或其他通信渠道向被攻击者发送植入木马的文档或恶意链接，并诱骗攻击者点击执行，从而实现对攻击者计算机的远程控制或恶意程序感染，并且具有较高的成功率，钓鱼攻击也成为了攻击者实现外部突破的高效手段之一。

本月攻防演习成果:

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	41	77	142	171	68	236	351	3271

5、敏感信息泄露让网络面临严重安全威胁

本月任务中目标外网敏感信息泄露较为严重，涉及敏感信息包括系统后台的登录地址、内网接口信息、数据库文件、账号口令信息、后台目录及目录下配置文件、日志文件、备份文件、后台操作系统、应用部署包、中间件、开发语言的版本等。这些敏感信息一旦被攻击者获取到，会为攻击者实施进一步攻击提供很大的帮助，甚至直接通过获取的账号口令信息获取接入权限。

6、内部关键业务网络纵深防御不足

本月任务中发现目标网络内部关键业务的纵深防御措施部署不足，缺乏对关键业务系统网络接入或系统访问的安全过滤措施，主要表现为：互联网侧业务系统被突破后，通过边界服务器或内部人员办公终端，即可触及一些重要的内网业务系统。内网纵深防御措施的缺乏，造成核心业务系统面临严重的安全隐患。

7、攻击行为无有效监测手段

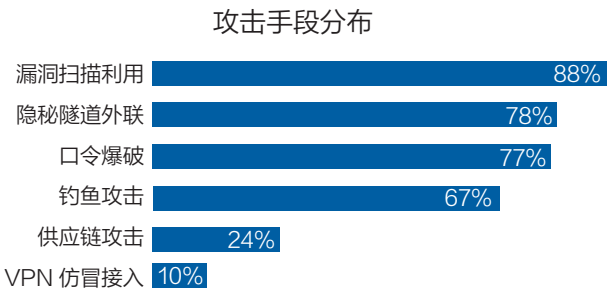
虽然各单位都部署了流量安全检测设备，但主要监测点分布于互联网边界及核心交换位置，普遍存在监测范围覆盖不够或加密流量无法监测的问题。一些内部网络子区域没有监测手段，通过控制子区域的一台服务器进行区域内攻击尝试时，监测能力消失，攻击成本大幅降低；部分应用系统采用了加密通信措施，攻击行为也会随之加密，流量监测设备无法监测。据此，多数单位尚未建成全覆盖全透明的监控体系。

8、供应链对网络安全至关重要

本月任务中多个目标网络通过供应链攻击实现突破，主要是针对目标网络平台或应用系统的供应商开展工作，通过获取产品源码，挖掘漏洞并最终实现漏洞利用，打开目标网络突破口。供应链安全是网络安全构建的重要组成部分，确保供应链安全对网络安全至关重要。

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果分析，对目标网络的外网突破多通过互联网侧业务系统漏洞利用和钓鱼攻击实现；内网横向拓展以弱口令、口令复用及内部应用漏洞为主。使用的主要技术手段分布如下：



1、漏洞扫描利用

本月任务中漏洞利用主要集中在互联网侧业务系统和门户网站，主要以敏感信息泄露、未授权访问、组件反序列化、文件上传执行等漏洞为主。这些漏洞主要是由于系统组件更新不及时、安全策略设置缺陷引起的，直接反映出客户网络运维人员对下辖网络资产动态跟踪不及时、网络运维缺乏常态巡检机制、对存在的漏洞及安全威胁缺乏应对等问题。

2、隐蔽隧道外联

本月任务中因大部分目标系统内网主机不能访问外网，需要借助端口转发、隐蔽隧道技术等手段实现网络穿透。尤其是政务、金融、能源等对内网业务防守较为严密的客户网络，对目标的一些核心业务系统、靶标数据库的渗透拓展，需要通过多层通信隧道转发才能实现。

3、口令爆破

本月任务中口令爆破主要体现在目标内网的弱口令和口令复用问题，比较典型的案例为仅使用弱口令即可实现某目标的外网突破及内网靶标控制。主要原因是目标网络没有依据安全规范要求进行账号口令设置和使用，缺乏对弱口令和通用口令的统一监管，如禁用弱口令、账号口令定期更新、首次登录要求修改默认账户密码等。

4、钓鱼攻击

本月任务中对可利用漏洞入侵成功率较小的目标，主要采取钓鱼攻击进行迂回突破。外部采用的钓鱼手段

为客服业务咨询、冒充内部管理人员等，内部钓鱼则以水坑攻击为主，重点在内网对网管、核心业务人员进行钓鱼突破。

5、供应链攻击

本月任务中的供应链攻击主要围绕目标网络外部业务系统开展，通过产品特征匹配供应商，围绕供应商进行信息收集，获取有关产品源代码、网络接口等关键信息，开展代码审计发掘安全缺陷，从而打开目标网络突破口。

6、VPN 仿冒接入

本月任务中目标网络内网多通过 VPN 实现分散网点入网访问，通过 VPN 仿冒接入，可实现对目标网络不同网段业务的渗透控制。在对 VPN 的攻击过程中，VPN 仿冒接入认证信息的获取是接入成功的关键环节，主要利用内网信息搜集、弱口令或口令复用等方式实现。

四、典型攻击手段实现案例

1、外部漏洞利用突破

（1）某目标网络互联网侧业务集成平台系统存在未授权访问和任意文件上传漏洞，通过未授权访问漏洞添加管理员账号，在其后台通过文件上传漏洞攻击获取集成平台系统服务器控制权限，实现外网突破，获取内网支点。

（2）某目标信息管理系统存在 SQL 注入漏洞，通过该漏洞利用获取到用户管理员权限，可进行角色管理、数据权限控制等行为。

（3）某目标家庭数字平台存在 CVE-2022-22947 漏洞，可通过漏洞利用获取服务器权限，突破网络边界，进入 DMZ 区。

2、口令爆破

（1）某目标人员管理服务中心系统存在弱口令漏洞，通过漏洞利用获取该系统管理员权限，可查看大量系统信息，如手机号、家庭住址、姓名、订单信息等。

（2）某目标运销管理系统存在弱口令漏洞，获取 Web 后台权限，通过该后台可查看该公司客户信息、合同信息、销售信息等数据。

（3）某目标云管理平台存在弱口令漏洞，通过漏洞利用获得后台管理员权限，可登录后台控制 105 台虚拟机，并通过计划任务获得服务器权限。

3、钓鱼攻击

（1）对某目标微信公众号在线客服以咨询业务为理由，进行钓鱼攻击，控制目标客服人员主机，从中获取大量内网系统关键信息。

（2）对某目标网络业务助手后台维护人员进行钓鱼，控制目标人员终端主机，并以此为支点对目标内网进行探测渗透。

（3）某目标网络外部业务平台突破后，通过水坑钓鱼针对内部网络运维人员进行定点攻击，获取关键运维人员主机控制权限，从中获取大量有关堡垒机、网管系统、服务器的安全管理信息，实现目标内网彻底渗透。

4、供应链攻击

（1）前期情报搜集过程中，确定某目标互联网业务系统开发商信息，利用某品牌 OA 漏洞控制开发商业务服务器，从中获取目标互联网业务系统源码，进一步通过代码审计挖掘出两处漏洞，最终通过挖掘的漏洞控制目标互联网业务系统后台服务器，打开目标网络突破口。

（2）通过前期搜集的情报，确定某目标管理中心信息平台网络安全服务商，对其开展工作，从安全服务商网络内获取目标管理中心平台管理账号、接口信息，成功接入目标内网。

5、VPN 仿冒接入

（1）某目标外网 VPN 网关存在命令执行漏洞，利用漏洞获取 VPN 网关控制权限，进一步通过 VPN 仿冒接入目标内网。

（2）通过口令爆破，成功登录外网 VPN 后台管理系统，通过 VPN 后台管理系统进行 VPN 账号添加、访问策略修改等操作，实现仿冒接入其他部门业务网络。

政策篇

国内，《网络安全法》实施五年后迎来首次修改，显著强化了网络安全违法行为的处罚力度，对于提升全社会特别是大型企业组织加强网络安全守法意识，具有极大的推动作用；

国际上，美国白宫发布备忘录，要求联邦机构采购软件需遵循安全软件开发框架，对推动安全软件开发具有较大示范意义。

国内

网信办《关于修改〈中华人民共和国网络安全法〉的决定》公开征求意见

9 月 14 日，国家互联网信息办公室发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》公开征集意见。该文件对《网络安全法》进行了四方面修改：一是完善违反网络运行安全一般规定的法律责任制度；二是修改关键信息基础设施安全保护的法律责任制度；三是调整网络信息安全法律责任制度；四是修改个人信息保护法律责任制度。

国家标准《信息安全技术 网络数据分类分级要求》公开征求意见

9 月 14 日，全国信息安全标准化技术委员会发布《信息安全技术 网络数据分类分级要求（征求意见稿）》公开征求意见。该文件给出了数据分类分级的原则和方法，包括数据分类分级基本原则、数据分类框架和方法、数据分级框架和方法等，用于指导各行业、各领域、各地方、各部门和数据处理者开展数据分类分级工作。数据分类分级需遵循科学实用、边界清晰、就高从严、点面结合、动态更新等原则。

《中华人民共和国反电信网络诈骗法》表决通过

9 月 2 日，十三届全国人大常委会第三十六次会议表决通过《中华人民共和国反电信网络诈骗法》。《反电信网络诈骗法》共七章五十条，包括总则、电信治理、金融治理、互联网治理、综合措施、法律责任、附则等。这部法律自 2022 年 12 月 1 日起施行。《反电信网络诈骗法》明确界定了电信网络诈骗的定义，法律的适用范围，电信、金融、互联网等重点领域的治理措施，以及综合性治理措施，为反电信网络诈骗工作构建了全方位的治理体系。

卫健委等三部门印发《医疗卫生机构网络安全管理办法》

8 月 29 日，国家卫生健康委、国家中医药局、国家疾控局联合发布《医疗卫生机构网络安全管理办法》。《办法》明确了各医疗卫生机构网络，以及数据安全管理基本原则、管理分工、执行标准、监督及处罚要求，共六

章三十四条。《办法》规定，各医疗卫生机构应成立网络安全和信息化工作领导小组，由单位主要负责人任领导小组组长，每年至少召开一次网络安全办公会，有二级及以上网络的医疗卫生机构应明确负责网络安全管理工作的职能部门。

《公路水路关键信息基础设施安全保护管理办法》公开征求意见

8月23日，交通运输部发布《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》公开征求意见。《征求意见稿》共六章四十八条，涉及公路水路关键信息基础设施认定、运营者责任和义务、保障和监督管理等内容。《征求意见稿》规定，运营者应当设立首席网络安全官，为每个公路水路关键信息基础设施明确一名安全管理责任人。首席网络安全官、专门安全管理机构负责人和关键岗位人员等公路水路关键信息基础设施从业人员每人每年网络安全教育培训时长不得少于30学时。

国际

欧盟提出《网络弹性法案》，数字产品必须遵守安全基线

9月15日，欧盟委员会发布《网络弹性法案》提案，要求具有数字元素的产品在生命周期内引入强制性网络安全要求，保护消费者和企业免受安全不足的产品侵害。

该法案要求，数字设备与软件需满足基本网络安全要求，公布软件物料清单，提供漏洞报告机制，开售后提供5年安全更新等。违反规定的企业将面临最高1500万欧元（约1.05亿元人民币）或全球营收2.5%的罚款。这是欧盟范围内首个此类立法。

美国白宫发布备忘录，要求联邦机构采购软件需遵循安全软件开发

9月14日，美国白宫管理与预算办公室发布M-22-18备忘录，名为《通过安全软件开发实践增强软件供应链安全性》。备忘录要求，各联邦机构采购软件产品需要供应商提供安全证明文档，表明该软件符合NIST发布的安全软件开发框架，并给出了各联邦机构落实要求的时间表。今年3月，管理与预算办公室发布命令，要求各联邦机构开始采用安全软件开发框架。

英国《电信（安全）法案》将通过立法，要求运营商严格遵循最佳安全实践

8月30日，英国数字化、文化、媒体和体育部发布《电信（安全）法案》公众咨询回复，称法案已确定最终文本内容，将于11月成为正式法律。该法案要求，电信运营商应在长期投资决策及网络与服务日常运行中嵌入网络安全，严格遵循最佳安全实践，以提高英国的网络弹性。英国数字基础设施部长马特沃曼议员表示，这将是世界上最严格的电信安全制度之一。

美国政府发布《准备将关键基础设施向后量子密码迁移》

8月24日，美国网络安全与基础设施安全局（CISA）发布《准备将关键基础设施向后量子密码迁移》，概述了关键基础设施利益相关者现在应该采取的行动。CISA建议优先考虑迁移的三个领域：一是支撑性国家关键功能，包括通信、身份管理、信息技术产品服务、保护敏感信息等；二是工业控制系统，需要在硬件替换成本高、地理分散等挑战下确保应对风险能力；三是要求长保密生命周期的国家关键功能。

政策解读

《网络安全法》修改解读：加大违法处罚力度，提升全社会守法意识

作者 奇安信战略推进中心

近日，中央网信办会同相关部门起草《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（以下简称《征求意见稿》），以便与 2021 年相继修订制定实施的《行政处罚法》、《数据安全法》、《个人信息保护法》等法律衔接协调。《网络安全法》是我国首部关于网络安全工作的基本大法，自 2017 年 6 月 1 日正式施行以来为我国网络空间安全治理提供了有力的法律保障。

本次修订主要针对《网络安全法》中“第六章 法律责任”部分条款进行了修订完善，是我国加强网络安全

工作的又一有力举措，将进一步完善我国网络安全法律法规体系。

本次修改主要有以下几点。

第一，顶格罚款金额激增，对企业罚款从最高 100 万提高到 5000 万或上一年度营业额的 5%，对直接负责的主管人员从最高 10 万元提高到 100 万元，直接与《 个人信息保护法 》接轨。

第二，新增禁业规定，对直接负责的主管人员和其他直接责任人员，可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

第三，新增通报批评，违法者除了被有关主管部门责令改正、给予警告，新增了通报批评的行政处罚形式。

具体而言，《 征求意见稿 》主要体现在以下五大变化。

一、增加与营业额挂钩的处罚措施，显著提升对大型企业组织的震慑力度。

现有《 网络安全法 》针对违法主体的处罚额度一般不超过 100 万，对于大型企业组织来说难以达到与之规模相匹配的惩戒力度。《 网安法修订稿 》针对违反网络运行安全一般规定的网络运营者、关键信息基础设施的运营者及违反网络信息安全义务的网络运营者，均增加了在特定违法情况下“处上一年度营业额百分之五以下罚款”的表述，与去年出台的《 个人信息保护法 》相关处罚措施相一致，这将对大型企业组织遵守《 网络安全法 》相关规定产生极大的震慑作用，有利于提升法律的权威性和威慑力。

二、增加禁业处罚措施，有力强化对涉及违法行为的相关管理人员的惩戒效果。

对于情节特别严重的违反网络运行安全一般规定的网络运营者和违反网络信息安全义务的网络运营者，除了保留对相关管理人员的罚款措施，《 网安法修订稿 》特别增加了“禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作”，有利于强化对涉及违法行为的相关管理人员的惩戒效果。

三、整合提升同一大类违法行为的行政处罚幅度，就高不就低。

例如，将原来的第五十九条、第六十条、第六十一条、第六十二条针对违反不同条款的行为的处罚种类和幅度合并为同一表述，将几类违法主体拒不改正或者情节严重的“处一万元以上十万元以下罚款”“处五万元以上五十万元以下罚款”“处十万元以上一百万元以下罚款”不同处罚额度统一合并提升到“处一百万元以下罚款”。

四、与其他法律法规处罚措施保持一致。

将原有关个人信息保护的法律责任修改为转致性规定：“网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十四条规定，侵害个人信息依法得到保护的权利的，依照有关法律、行政法规的规定处罚”，相关处罚主要参照《 个人信息保护法 》规定执行。将关键信息基础设施的运营者违反本法第三十七条规定（在境外存储网络数据，或者向境外提供网络数据的）的法律责任也修改为转致性规定，相关处罚主要参照《 数据安全法 》和《 关键信息基础设施安全保护条例 》规定执行。

五、增加兜底性条款，适应网络空间快速变化新形势。

针对《 网络安全法 》第七十条中“发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的”情况，对法律、行政法规没有规定的情形增加了兜底性罚则，在网络环境快速变化、信息安全违法犯罪形式层出不穷的背景下，兜底条款能够保证在出现一些新型违法行为都能对应罚则。

总体而言，本次修订工作明显强化了网络安全违法行为的处罚力度，对于提升全社会特别是大型企业组织加强网络安全守法意识具有极大的推动作用。 安

栏目主编　李建平

抗击未来的勒索攻击

新的勒索形式、越来越多的附属团伙，重新塑造勒索软件攻击

专题编辑　张少波　魏开元 王梦琪

2022: 勒索攻击的演进

自 1989 年首次出现以来，勒索软件一直稳步发展。在 33 年后的 2022 年，勒索软件成为各类机构面临的最大威胁之一。

2022 年上半年，勒索组织创造了新的攻击方法，瞄准本已紧张的供应链，导致数百家企业的业务运营中断，支付勒索赎金和恢复运营所支付的成本高达数百万美元。勒索软件即服务（RaaS）的出现，令网络犯罪可以获得更多的攻击工具和基础设施。

2022 年上半年，出现了超过 50 个活跃 RaaS 和勒索组织，超 1200 个机构受到勒索软件的攻击。

RaaS：降低攻击门槛

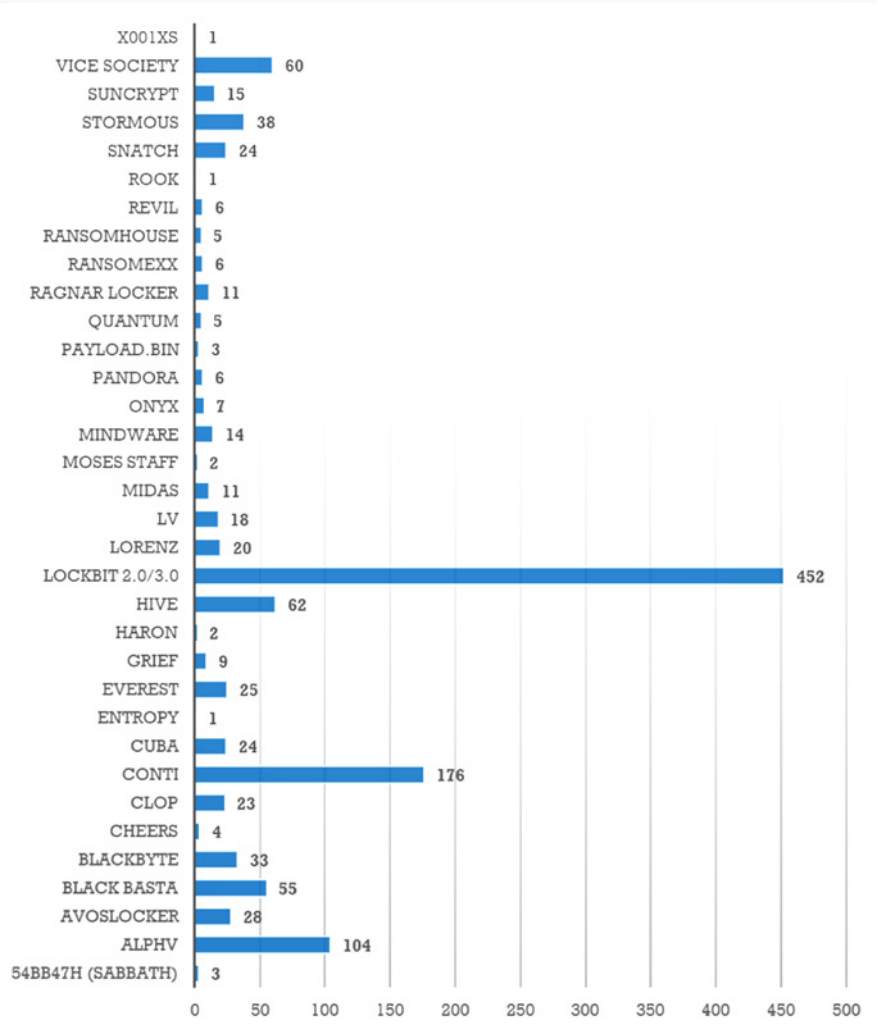
由于勒索软件即服务（RaaS）模式，攻击导致的攻

击规模越来越大、赎金越来越昂贵、攻击越来越频繁。RaaS 生态系统包括许多不同类型的参与者，目前定义的两种主要威胁参与者是勒索软件运营商及其附属团伙。

运营商是勒索软件开发商——制造和分发恶意软件，实施攻击并招募附属团伙的组织。附属团伙是较小的网络犯罪分子，会以一定的价格购买勒索软件运营商的恶意软件套件和基础设施。通常支付订阅费及与运营商分享利润。

目前拥有加盟招募计划的知名勒索软件运营商包括 REvil、DarkSide 和 LockBit。

IBM X-Force 研究主管约翰·德怀尔（John Dwyer）表示，加盟模式的兴起，表明勒索攻击已经建立起多种的经济形态。如果观察已发生的勒索攻击事件，就会注意到加盟模式和加密货币，以及访问代理（AB）等勒索经济的支撑。



勒索软件攻击活动（2022 年 1 月—6 月）

随着围绕特定网络犯罪组织建立起商业模式，攻击者的绝对数量不断增加，攻击机会也在增加。X-Force 负责人查尔斯·亨德森（Charles Henderson）表示，加盟模式使得“犯罪分子比网络安全行业更加合作”。因为任何管理红队或攻击性安全团队的人都知道，如果攻击者比防守者更好沟通，就会取得成功。红队进行测试攻击时，会有很多迹象显示防守出了问题。除非防守者能将这些迹象联系、拼凑在一起，否则整个攻击任务都可能难以被发现。在这方面，安全行业需要做得更好。

6 月初，X-Force 的一份报告发现，2019——2021 期间，企业勒索软件攻击的平均时间，从初始访问到恶意软件部署，下降了 94.34%。攻击时间从平均 2 个多月变为 3.85 天。报告称，对 ZeroLogon 等漏洞的快速利用是一个因素，另一个因素是勒索攻击目前的进入壁垒很低。

实施勒索攻击从未像现在这样容易。加盟团伙模式和相关机制通过租用基础设施和工具，用很小的投资就能够参与攻击了。LockBit、Conti 和 BlackCat 是 2022 年上半年 RaaS 领域的主要参与者。

攻击形式演变背后的核心

在过去十年的繁荣中，勒索软件经历了许多转折和变化，从现在无处不在的双重勒索技术到对关键基础设施的攻击。

勒索软件作为一个概念，已经存在了几十年。实际上，从消费者互联网诞生之日起就已出现。传统上，勒索攻击被定义为攻击者使用恶意软件加密受害者计算机上的文件，然后受害者支付赎金以解密文件。

近年来勒索软件发生了重大变化。经典的攻击仍在发生，但标准的企业勒索攻击现在涉及“双重勒索”技术：攻击者既会加密受害者数据，也会窃取数据，目的是在受害者不付款的情况下，公开泄露这些数据。

双重勒索技术已成为企业勒索软件攻击中的常态，但绝不是攻击团伙获取报酬的唯一途径。安全专家发现：一个新兴趋势是攻击者在未加密受害者文件的情况下窃取数据，这有时被称为窃取勒索（extortionware）。

现在说这会成为一种趋势还为时过早，但一些攻击组织开始关注数据勒索，一些攻击人员表示：“我们不会浪费时间加密数据，只会尽可能多地窃取数据，然后将其用作勒索赎金。”这种攻击方式的另一个好处是，它避免了医院等机构关键业务中断的可能性，而业务中断可能导致严厉的处罚。无论是否加密，数据都可以成为让受害者向勒索团伙付款的强大工具。芬兰的一家心理治疗机构在 2018 年经历了患者记录被盗事件，导致患者被直接勒索。

在其他情况下，加密仍是获得赎金的最有效武器。例如，工业环境中运营技术（OT）和工业控制系统（ICS）日趋普遍的互联网连接，经常成为勒索软件攻击的牺牲品。针对 CS/OT 系统攻击尤其残酷，因为工业和关键设施的性质意味着关键业务或服务可能中断。

此外，“三重勒索”技术也开始出现。在攻击中，网络犯罪分子加密数据、窃取数据并威胁对受害者进行 DDoS 攻击。

俄乌冲突引发网络犯罪组织的分裂

2022 年上半年，勒索软件领域出现了一些有意思的现象。最重要的事件之一是 Conti 勒索团伙的解散。

Conti 勒索组织是最知名的勒索软件团伙，成员来自俄罗斯或独立国家联合体（独联体）。俄罗斯和乌克兰之间的战争不仅影响了世界，也在网络犯罪组织中造成分裂。Conti 勒索软件集团在其数据泄露网站上宣布，在冲突中全力支持俄罗斯。这导致来自乌克兰的安全研究员泄露了 Conti 的内部通信，包括 6 万多条信息。揭示了该勒索组织如何处理赎金谈判，以及攻击期间使用的工具。 Conti 宣布于 2022 年 5 月结束运营。这可能直接与其沟通、工具和内部信息泄露有关。

另一方面，LockBit 勒索软件集团宣布保持中立，宣称不会“参与国际冲突”。 Evil Corp 勒索组织作为下游使用者与 LockBit 的勒索软件产生了关联。Mandiant 追踪名为 UNC2165（与 Evil Corp 集团有关）的威胁组织，观察到该组织部署了 LockBit 勒索软件变体。据报道，Evil Corp 组织是包括 Dridex、BitPaymer 和 DoppelPaymer 在内的知名勒索软件和恶意软件活动的幕后黑手。使用 LockBit 的勒索软件即服务（RaaS）让 Evil Corp 组织更难被识别。

LockBit 组织因发布其 LockBit 3.0 版本而再次登上头条新闻，这个版本包括新功能和 Zcash 加密货币支付选项。LockBit 组织启动了新的数据泄露网站，其中包括赎金要求，并允许其他攻击者购买被盗数据。

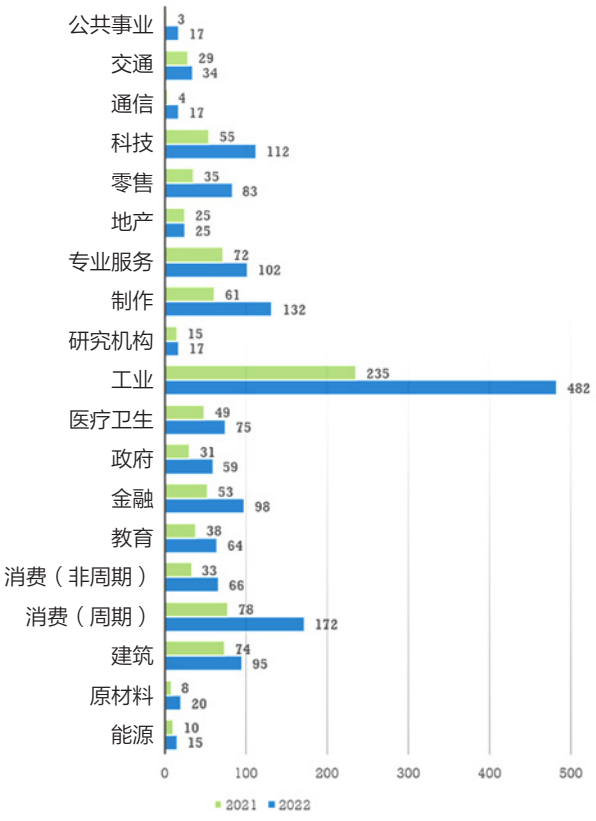
一切都表明，整个勒索软件经济仍在持续发展。

行业与地域：勒索目标大分解

工业领域是最主要的垂直目标领域。工业领域包括制造业、建筑工程、运输和工业服务业。这些行业的组织经常成为目标，因为它们无法承受长时间停机、客户和合作伙伴的敏感信息量大，以及支付赎金的可能性更大。

从 2021 年到 2022 年，周期性消费行业的勒索攻击增幅最大，约 125%（勒索事件由 33 起增至 66 起）。周期性消费品领域包括零售、汽车和零部件、消费品、旅游和休闲及媒体等。

零售业的勒索攻击增长了 86%，位于第二位。遭受勒索攻击的政府机构增加了 79%，这可能与 2022 年出现的许多政治性勒索软件攻击有关。此外，许多较小的政府机构，因缺乏资源或资金来阻止勒索组织的攻击，更可



勒索攻击行业分布（2022 年 1 月—6 月）

能成为受害者。

医疗卫生领域的勒索攻击受害者增加了 59%。医疗卫生领域相关设施无法承受大面积宕机，无法延迟个人医疗等关键特性，令其成为勒索攻击最有吸引力的目标领域之一。

从地域来看，北美是勒索数据泄露网站上列出的受害者人数最多的地区。2022 年上半年有 571 名受害者，与 2021 上半年相比下降了 8.5%。美国占北美所有受害者的 87%，占 571 个受害者中的 495 个，下降了 9.5%。

2021—2022 年间，非洲的攻击受害者增长最大，从 7 个增至 19 个，增长了 171%。其他增长包括亚洲（100%）、欧洲（57%）和南美洲（45%）。

未来

勒索软件可能在未来仍然是一种普遍的威胁。勒索软件事件高调发生，政府和执法部门密切关注，但目前勒索组织没有停止攻击的动机。

在 2021—2022 年间，勒索组织一直在持续运营和升级，继续构建基础设施和能力，打造一站式平台，减少对市场和论坛的依赖。

未来，重要垂直领域，包括医疗保健、能源、工业服务、政府在内，可能仍然是对勒索软件集团最有吸引力的领域。这些领域承载的信息价值高，无法承担长时间的宕机，并且有支付赎金的能力。

双重勒索方法很可能仍然是整个勒索软件威胁领域的主要过程。勒索软件集团可能会越来越多地与初始访问代理合作，以获得初始访问权并使用远程访问市场。远程访问市场是允许威胁参与者出售和交换访问凭证的自动化商店。

勒索组织历来使用网络钓鱼来获得对受害者网络的初始访问，并利用全球事件引诱受害者通过电子邮件进行互动。这种技术在未来可能仍是最主要的入侵手段。随着不确定性的持续，远程工作、经济不稳定等，勒索软件组织将继续使用这些技术，利用员工的恐惧和好奇心，吸引上钩。

勒索事件愈演愈烈，2021 年美国成立专门的勒索软件工作组，同时强调防御前置，加大对攻击组织的打击。在 RSAC 2022 上，工作组成员呼吁受害机构在遭遇勒索软件攻击后及时地报告。相比过去，提高网络攻击事件的透明度正在成为趋势和普遍意愿。“透明度意味着正在努力寻找正确的应对之道。”美国网络安全和基础设施安全局负责人则督促私营机构与政府部门加强合作，加强联合网络防御协作。

对于各类可能遭受勒索的机构而言，为防范勒索攻击则需要更密切关注攻击者的演变，包括其攻击方法和工具。

总体而言，需要采用主动安全防御模式，来应对不断演化的勒索攻击。比如，越来越多机构将网络安全保险作为事件响应计划的一部分。为了更符合保险要求，甚至对网络防御进行了优化，包括流程变革、部署新技术或服务、加强员工培训等。

解决方案

索取巨额赎金成为勒索攻击新常态 政企亟需提升四方面安全能力

作者 解决方案中心

2022 年 8 月 11 日，有网友爆料称某国内家电巨头工厂多处计算机感染勒索病毒，导致所有内部系统无法登陆，所有文件无法打开，被勒索要求 7 天汇 1000 万美金到指定账户；

2022 年 8 月 29 日，国内多家安全厂商发布预警，称 8 月 28 日起，国内某企业财务病毒 0day 漏洞可能遭到大规模勒索利用，已出现多起使用该病毒的企业勒索病毒攻击案例，有被勒索用户反馈，中了勒索病毒后要求是支付 0.2 比特币（约合 27,439 元人民币）；

2022 年 8 月 31 日，全球最大的图书馆书籍和电子资源分销商美国图书馆供应商 Baker & Taylor 公司披露，一周前曾遭到勒索病毒攻击，目前仍在努力恢复各业务系统。

……

仅仅 8 月份，国内外有关勒索攻击的重大事件频频曝出，凸显了当前网络安全的严峻形势。

勒索病毒，缘起数字货币

勒索病毒，是伴随数字货币兴起的一种新型病毒木马，通常以垃圾邮件、服务器入侵、网页挂马、捆绑病毒等多种形式进行传播，通过劫持用户的系统或数据资产，实现敲诈勒索的目的。

早期的勒索病毒通常通过隐藏目录、加密 C 盘文件名，或者给用户系统设置开机密码等方式进行勒索。这种情况下，只需显示文件或者去掉开机密码即可对勒索病毒破解。同时，这一阶段的勒索病毒赎金通常是汇入银行账户，追踪溯源较为方便，这也导致勒索病毒无法大规模使用。但是以比特币为代表的虚拟货币的出现，为勒索病毒的大规模扩散提供了基础。虚拟货币的匿名性特征保证了勒索犯罪无法通过支付进行追溯，因此犯罪分子开始重拾勒索病毒这一犯罪手段。

此时，勒索病毒已不再是通过隐藏目录这么简单的手段进行勒索了。主流的勒索方式已经变为通过加密数据或锁定系统的方式进行勒索。而近期发生的多起勒索攻击事件，则是明显带有针对性的商业攻击，勒索者在加密系统的同时，又宣布公开重要数据，这让受害者承受巨大的数据泄露压力，使得受害者被迫支付赎金的可能性大幅提高。且受害者在承受着支付赎金后数据仍有可能被公开的不确定性的同时，又面临监管机构对其数据泄露进行处罚的的压力，这在未来将会成为政府或企业面对勒索病毒攻击的“新常态”。

勒索病毒攻击案例剖析

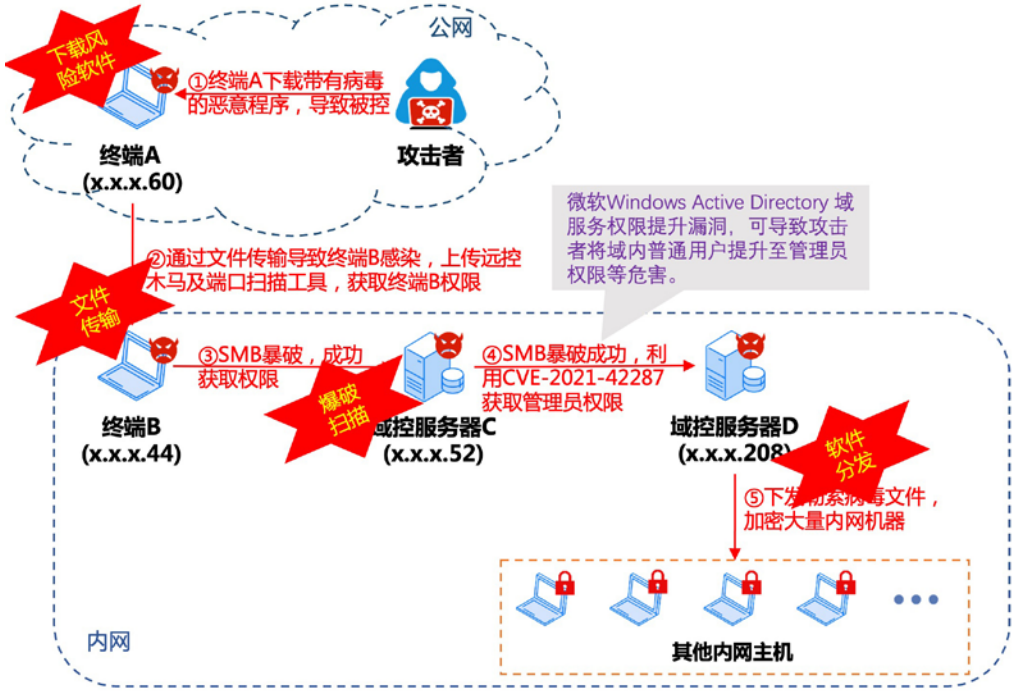
案例一：某日，奇安信应急响应团队接到某客户应急响应请求，内网数百台机器被勒索，要求进行溯源分析。通过攻击溯源分析发现攻击路径如下：

① 终端 A（x.x.x.60）使用者从非官方渠道下载带有病毒的恶意程序，导致终端 A（x.x.x.60）被攻击者控制；

② 攻击者利用终端 A（x.x.x.60）向内网终端 B（x.x.x.44）上传远控木马及端口扫描工具，获取终端 B（x.x.x.44）权限；

③ 终端 B（x.x.x.44）对域控服务器 C（x.x.x.52）进行 SMB 暴力破解，成功获取域控服务器 C（x.x.x.52）权限；

④ 攻击者继续利用域控服务器 C（x.x.x.52）为跳板，对域控服务器 D（x.x.x.208）进行 SMB 暴力破解并成功后，利用 CVE-2021-42287 域服务权限



提升漏洞获取管理员权限；

⑤ 攻击者利用域控服务器 D（x.x.x.208）管理员权限向内网下发勒索病毒文件，最终导致大量机器被加密。

从这起勒索攻击过程分析来看，终端可随意下载软件而不受限制，域控服务器作为重要集权类设备，但是安全监控和保护不到位，安全运行过程中安全监控、设备维护、分析研判等岗位未设置或未发挥作用，最终导致内网被勒索失陷。

案例二：某单位突然发现内部生产网业务系统瘫痪，通过拨打 95015 应急响应电话请求支援，经过应急团队排查发现企业遭受勒索病毒攻击，通过分析攻击路径如下：

① 该公司员工身份证、常用密码及工作邮箱等关键敏感信息泄露于多个社交网站，被某国外恶意组织发现，攻击组织利用员工邮箱和常用密码，成功登录该公司互联网边界云桌面；

② 攻击组织通过公司云桌面，获取到多个域账号信息，并对多个办公服务器、虚拟化平台进行远程登录，在成功定位到域控服务器后，攻击组织利用域控漏洞及社工密码等方式，获取到域控服务器账户凭证和密码；

③ 攻击组织对域控服务器配置计划任务，以定时执行加密任务的方式向全国域环境中机器投放 HIVE 勒索病毒，同时，攻击组织通过对 ESXI 平台进行 SSH 爆破，在获取到 ESXI 平台权限后，进行人工投毒，最终，该企业内部上千台服务器被加密，业务瘫痪。

从这起勒索攻击过程分析来看，员工敏感信息遭到泄露，密码重用或复用情况严重，域控服务器安全监控和保护不到位，安全运行未发挥有效作用，最终导致业务瘫痪。

勒索病毒排查思路

通过分析勒索病毒已知的攻击手段和攻击方式，并采取措施进行专项排查并整改，能够有效避免已知勒索病毒攻击事件的发生。

① 开展重点排查，通过对互联网入口暴露面梳理、账号生命周期管理、域控安全、集权平台安全、特权账号及访问管理、安全监测记录与分析、应急恢复能力验证等方面，开展重点排查；

② 开展红队评估，针对重要系统、人员、软件、硬件、设备、数据等执行模拟攻击，发现系统、技术、人员、基础架构和数据中的存在的隐患和风险；

③ 开展专项整改，针对重点排查和红队评估发现的问题和隐患，通过提升人员安全意识、优化纵深防御、优化主动监测体系等手段进行重点加固和加强，提升对勒索病毒的防护能力。

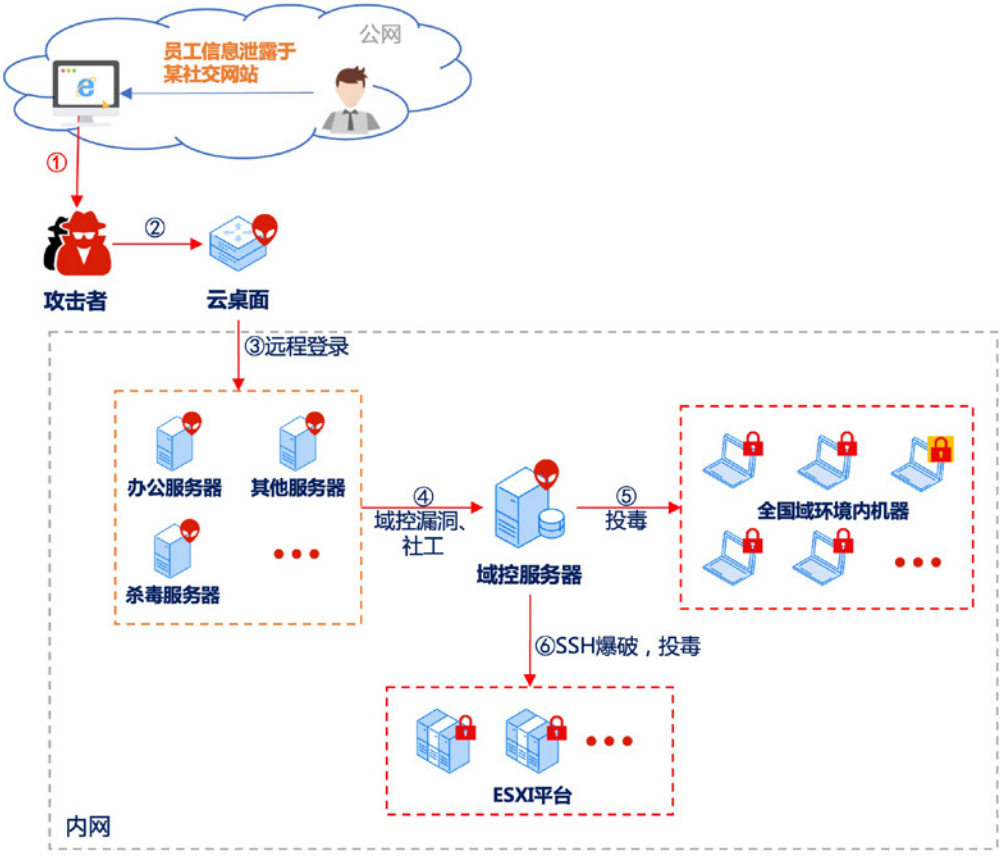
④ 开展重大事件应急响应，建立单位重大事件专项演练组织和机制，并配备专项资源进行协助。

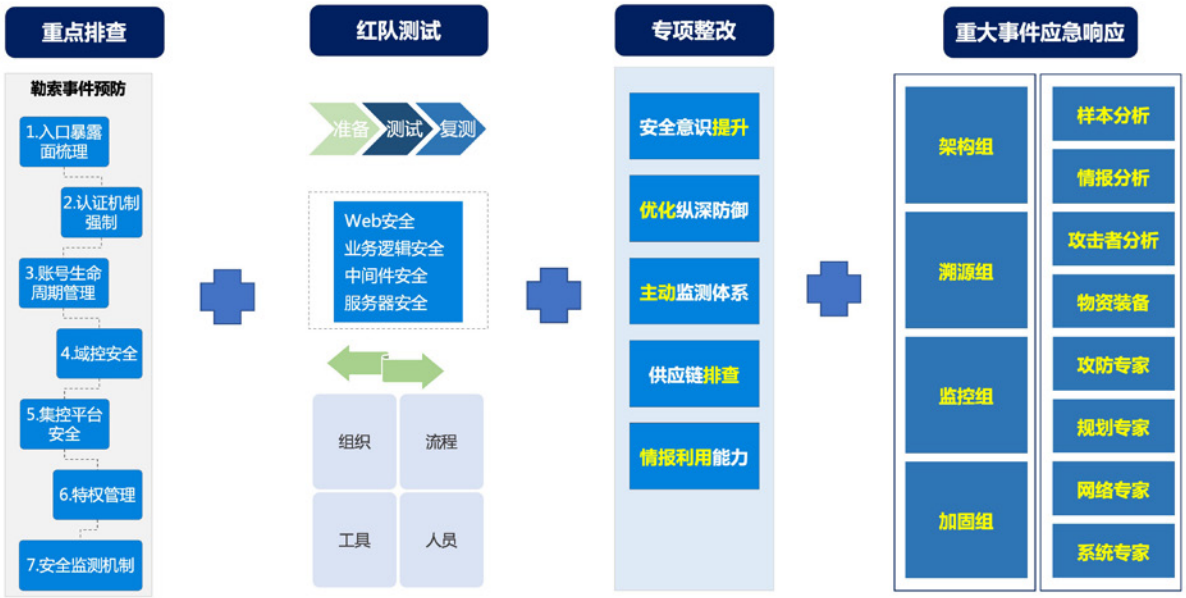
防治勒索攻击 期待强化四方面能力建设

目前，面对日益猖狂的勒索攻击，奇安信推出了勒索攻击防护解决方案，帮助政企单位加强自身网络安全防护建设，建立起完善的安全防护措施，构建自适应安全防御体系，实现对勒索病毒的有效检测和防护，保证内部网络及信息系统的安全。

在奇安信整体的勒索攻击解决方案中，将注重强化以下四方面的能力建设。

一、防御能力：该能力将通过一系列策略集、产品和服务，通过减少被攻击面来提升攻击门槛，并在受影响前拦截攻击动作。





该能力是指从网络入口到需要防御的目标均设置防御节点的方式，具体的能力来自奇安信的智慧防火墙、终端安全管理系统、终端安全准入系统、服务器安全管理系统构成。

二、检测能力：用于发现逃过防御网络的攻击，从而降低威胁造成的“停摆时间”及其他潜在的损失。

该能力主要通过在内部网络中部署奇安信天眼新一代安全感知系统，进行检测能力建设。可进行自动化挖掘获悉安全威胁，并根据专属威胁情报提升安全性。同时，天眼还能为后期研判与溯源提供重要依据。

三、响应能力：目标是实现高效调查和补救被检测分析功能（或外部服务）查出的安全事件，以提供入侵认证和攻击来源分析，并产生新的预防手段来避免未来的安全事件。

该能力将通过产品之间的联动响应及应急响应服务机制，实现响应能力建设。奇安信天擎 & 天眼、防火墙 & 天眼联动响应，可构建终端、网络层的多级深层次的安全防御能力，带来的安全事件应急响应机制的建立，将对安全事件进行检测、分析、协调、处理，保护资产安全属性的活动，并协同建立有效的防御策略来抵御网络安全威胁。

四、预测能力：通过对外部黑客行动的学习，主动锁定对现有系统和信息具有威胁的新型攻击，并对漏洞划定优先级和定位。该情报将反馈到预防和检测功能，从而构成整个处理流程的闭环。

该能力将通过奇安信云端海量数据的分析成果定期同步至方案中涉及到的产品，实现对 APT 攻击、勒索病毒、新型木马、特种免杀木马的规则化描述。同时，通过威胁情报解读定期推送分享服务，向政企单位分享 APT 攻击行为和事件情报、攻击团伙情报、恶意代码和漏洞利用情报、攻击团伙活跃态势情报等，建立预测预警能力。

总体而言，全面的勒索防御体系也并不是某一款单一安全产品就能完全解决的，威胁面不断加大的今天，安全产品也需要形成联动，并结合全面的安全服务，形成覆盖“边界 + 终端 + 云端”，基于威胁情报的多层次智慧检测、防御措施，并最终形成“自动化 + 人工响应”的有效处置机制，才能建立更强的安全优势。

终 端

2021 年终端被勒索攻击超 4000 万次，如何守住“第一防线”？

作者 研究员 张少波

尽管距离 2017 年 5 月 WannaCry 勒索病毒大规模爆发已经过去 5 年，但勒索攻击对终端的威胁依然有增无减。根据奇安信病毒响应中心的相关数据显示，2021 年被勒索攻击单位数量为 13,669 个，涉及 100.4 万终端，总计被攻击 4028.4 万次，遭受 10 次攻击以上的单位占比近 40%。尤其以不久前针对用友畅捷通 T+ 软件客户遭受勒索病毒攻击一事来看，中毒的终端数量多达数千台，这足以证明勒索攻击对于终端仍然构成着巨大威胁。

终端勒索威胁呈现三大特征

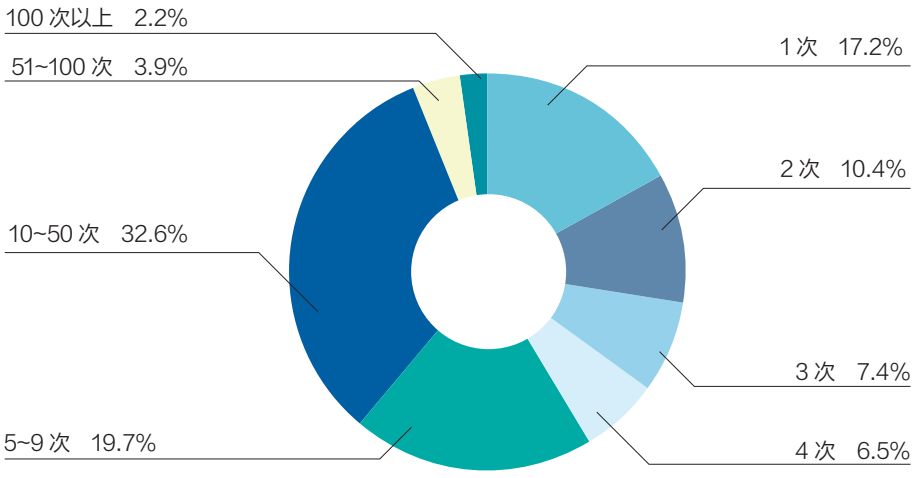
终端作为网络空间的“神经末梢”，处在网络安全防御的第一线。正如奇安信集团副总裁、终端安全 BG 负责人张庭所说，终端是必不可少的 IT 基础设施，更是数据和应用的重要载体，具有数量多、弱点杂、易利用等特点，一直以来都是勒索攻击的重点目标，更是安全管理的薄弱环节。

勒索病毒本质上是一种新型计算机病毒，主要以 RDP 爆破、漏洞利用、邮件、程序木马、网页挂马的形式进行传播。对于终端而言，勒索病毒的威胁存在着三大特征。

首先是影响范围广。2017 年 5 月 12 日爆发的 WannaCry 勒索病毒，席卷了全球 150 多个国家，至少 30 万台计算机中招。有数据显示，勒索软件攻击占所有网络攻击案件的三分之一以上。

其次是传播速度快。勒索病毒多属于“蠕虫”性质，传播和感染速度非常快，会在短短几个小时内造成大范围计算机中毒。同时，勒索病毒的变种衍生非常迅速，对常规的杀毒软件具有免疫性，同时攻击样本以 exe、js、wsf、vbe 等类型为主，对常规依靠特征检测的安全产品是一个极大的挑战。

被攻击单位被攻击频率



第三是造成损失巨大。这种病毒利用各种加密算法对文件进行加密，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。该病毒性质恶劣、危害极大，一旦感染，将给用户带来无法估量的损失。以 WannaCry 勒索病毒为例，仅爆发初期，所造成的经济损失就高达 80 亿美元。

企业如何从终端侧未雨绸缪

相关报告显示，2021 年平均每 11 秒就有一个企业受到勒索病毒攻击，勒索攻击一旦成功，平均停机时间为 21 天，平均恢复成本为 185 万美元，更为可怕的是，80% 支付赎金的受害者不久后会再次受到攻击。而且，为谋取更大的经济利益，提高勒索攻击得逞概率，攻击手段也在不断升级，会紧盯 0day 漏洞，执行供应链攻击，微调漏洞链，搜索废旧产品中的漏洞，不遗余力地使勒索软件武器化……要想免受勒索病毒困扰，奇安信终端安全专家建议广大政企客户从如下几方面入手。

1. 盘清终端资产

终端是数量最多也是最难纳管的 IT 设备，往往包括传统 PC 终端、国产化终端、移动终端、IoT 终端等多种类型，会安装 Windows、麒麟、Linux、UNIX、macOS、iOS、Android 等操作系统，并承载着各种各样的应用、业务和数据。只有盘清终端资产，才能明确保护对象，拒绝防护盲区。

2. 健全防御能力

面对日益精进的勒索病毒攻击，终端安全能力也需要不断升级或补充。建议广大政企客户构建体系化防御能力，通过终端类型全覆盖、安全能力全覆盖、联动场景全覆盖、部署管理全覆盖，打造更加牢固的防御体系，并通过终端安全运营确保能力持续有效。尤其要补充高级威胁分析能力，通过对勒索病毒的综合分析和全面溯源，更好地应对各类新兴威胁。

3. 做好补丁运营

漏洞是万恶之源，更是勒索病毒能够成功入侵终端的最大帮凶。建议广大政企客户做好补丁运营，在建立获得 / 订阅 / 整理漏洞情报的有效机制、正确评估漏洞影响范围、做好补丁测试和验证的基础上，更有针对性地下发补丁修复策略，并跟进补丁推送过程，直至漏洞修复完成。

4. 加强应用管理

终端是应用的载体，而应用则是人机交互、数据流转的介质，这就导致大部分终端在使用过程中离不开免费应用软件、U 盘类移动存储等应用。由于终端使用者的安全意识参差不齐，如果不对各类应用采取必要的管理措施，势必会给勒索病毒留下可趁之机。

5. 提高安全基线

掌握日常的安全配置技巧，例如，对共享文件夹设置访问权限，尽量采用云协作或内部搭建的 wiki 系统实现资料共享；尽量关闭 3389、445、139、135 等不用的高危端口，禁用 Office 宏等。

6. 备份重要文件

尽量建立单独的文件服务器，对重要文件进行存储和备份，即便条件不允许也应对重要的文件进行定期隔离备份，以免因为这些文件被勒索加密而造成不可挽回的损失。

7. 提升新兴威胁对抗能力

通过对抗式演习，从安全的技术、管理和运营等多个维度，对企业的互联网边界、防御体系及安全运营制度等多方面进行仿真检验，持续提升企业对抗新兴威胁的能力。

“四步走” 天擎全面防御勒索攻击

作为国内终端安全领域的领先者，奇安信天擎在

应对勒索病毒方面积累了深厚的经验。根据国际知名第三方机构赛可达的测评报告，奇安信天擎 EDR 对已知的勒索病毒家族和变种查杀率达到了 100%。对于终端肆虐的勒索攻击，天擎分别从入口防护、落地查杀、行为阻断、勒索解密四大步骤，提供全面的勒索防御体系。

第一步是勒索攻击入口防护。奇安信终端安全专家认为，勒索病毒不是凭空产生，需要有传播的途径。天擎实现了 U 盘防护、邮件防护、IM 防护、浏览器下载防护、局域网文件防护、网页安全防护等六种入口防御技术，结合网络入侵防护、远程登录防护等技术，从传播路径上阻断勒索病毒。

其中入口防护相关主防规则包括：RDP 爆破→云查及反馈中看到的远程登录进行勒索的最多；MSSQL 爆破→前段时间的 bluesky 勒索；Tellyouthepass →该家族会写 Powershell 计划任务持久化，并会通过永恒之蓝等漏洞进行内网渗透；PCHunter/ProcessHacker 等工具拦截→ 远程登录后常见的强杀天擎；内网渗透、Web 服务漏洞 → 最近的畅捷通漏洞，天马微电子通过域控、Psexec 分发勒索等。

第二步为勒索病毒落地查杀。对于勒索病毒样本，天擎拥有海量的样本库与广泛的威胁情报数据，可通过云查杀 +QOWL 本地查杀（针对已知家族），能够快速查杀新出现的勒索病毒。目前已有 1000 多已知勒索家族 + 变种的收录。

第三步为勒索行为过程阻断。该步骤包括勒索病毒免疫和勒索行为防御，其中勒索病毒免疫是指天擎利用病毒检测自身运行的机制，提前免疫某些家族的勒索病毒。原理为创建和病毒同名的内核对象，欺骗病毒阻断执行。

在勒索行为防御方面，当勒索病毒执行时，通过设置诱饵文档与加密行为的识别实现对勒索行为的发现与拦截。原理为监控关键文档、图片等经常会被加密的文件，当一个程序在一段时间内有多次对这些文件的修改行为，并且包含该进程的进程链有非白文件，会弹窗拦截。

第四步是勒索文件解密工具。勒索解密属于事后服务。勒索解密工具是一个独立发布的免费工具，并未不成在天擎客户端中，目前支持几十种勒索病毒的解密。

目前，天擎可以对大部分勒索病毒进行检测和查杀，并通过敲诈先赔服务免除客户后顾之忧。此外，天擎 EDR 模块能够与天眼威胁感知系统联动，准确检测内部的失陷主机，并通过天擎进行响应处置；天擎还可以与智慧防火墙联动，实现对内部风险主机或失陷主机进行安全管控。

总体来看，天擎通过和威胁检测、边界安全等产品的联防联控，针对勒索攻击，真正构建从精确检测到深度防御的纵深防范闭环体系，对终端实现固若金汤的安全防护。

天 眼

从 DarkSide 团伙看奇安信天眼如何做勒索病毒全生命周期检测

2021 年 5 月，勒索软件攻击切断半个美国的燃油管道的新闻传遍全网，该事件惊动了正在戴维营休假的总统拜登，迅速成为全球关注的焦点。据当时美联社报道，该事件是美国关键基础设施迄今遭遇的最为严重的网络攻击。很显然，基础设施正在成为网络攻击的首要目标。

事后调查显示，此次美燃油管道勒索事件的背后是来自母语为俄语的黑客团伙 DarkSide，该黑客团伙曾多次实施勒索攻击。奇安信天眼安全分析团队对其近期发起的攻击事件进行关联分析，大致攻击流程如下。

第一步，远程访问

根据 DarkSide 历来的攻击手段分析，此次攻击极有可能是收集了 TeamViewer 和 Microsoft Remote Desktop 等远程桌面软件的帐户登录详细信息，并以此为突破口建立初始访问权限，进行后续入侵。值得注意的是，在新冠肺炎全球大流行的社会背景下，越来越多的企业实施远程办公，允许工程师通过 VPN、RDP 和 TeamViewer 这样的远程连接工具访问企业内网，在一定程度上，提高了远程账号泄漏的可能性。

第二步，命令控制

在入侵的目标服务器上安装Tor客户端或者浏览器，并使用 Tor 进行 RDP 会话连接（RDP Over Tor），并且在远程控制方面会使用CobaltStrike进行后续操作。

第三步，横向渗透

以最初的失陷主机为跳板，使用 Active Directory 侦察工具收集有关用户、组和特权信息。其中使用内网渗透工具包括 advanced_ip_scanner.exe，psexec，Mimikatz。攻击者获得域管理员凭据后，即可访问域控。在后渗透阶段中，进行 DCSync 攻击，攻击者假装是合法的域控制器，并利用目录复制服务复制 AD 信息，从而获得了整个域（包括 KRBTGT HASH）的密码数据的访问权限。

第四步，加密勒索

在建立命令控制后门（Cobalt Strike）后，勒索软件会采取 PowerShell 脚本或者动态链接库 DLL 进行下发。其中涉及到的 Payload 会在域控制器的共享文件夹中进行暂时存储，并通过组策略调度任务指示主机获取并执行勒索软件。

值得注意的是，DarkSide 勒索软件活动在攻击前期使用多种隐蔽技术逃避网络安全设备和软件的检测，包括:

- 使用 Tor 网络隐蔽通信
- 检测 EDR 运行状态
- 为不同失陷主机定制攻击方式
- 混淆技术，如编码和动态库加载
- 痕迹清理

随着勒索软件无时无刻不在变化更新手段，通过各种不同恶意软件家族传播防不胜防。从 DarkSide 团伙的攻击手法来看，顶级勒索攻击能力甚至接近或达到 APT 水平。对企业来说，最好的防御措施就是敏锐发现变化多端的安全威胁，当受到攻击时迅速采取行动，并主动采用先进的安全解决方案。

天眼对关键基础设施安全领域持续关注并不断研究，利用自身技术优势，针对勒索病毒的“顽疾”开出了良方。

天眼针对勒索软件的全生命周期各阶段进行全面、持续的检测，采用多种检测技术相结合的方式，帮助用户及时发现威胁并定位失陷主机，尽可能将影响降到最低。同时利用本地的大数据平台对各阶段的检测结果进

覆盖高级威胁全生命周期的检测能力

行存储与分析，为完整回溯安全事件提供数据基础。

首先针对远程访问阶段，攻击者利用事先收集的 TeamViewer 或者 RDP 账号进入内网，天眼的流量传感器高并发流式处理引擎可实现对多种协议进行深度解码，可以监控 TeamViewer 或者 RDP 的登录行为。

其次，针对命令控制与横向渗透阶段，天眼流量传感器利用攻击模型检测技术，可检测网络协议中的攻击行为并发现内网横向渗透攻击行为。天眼传感器通过对网络流量进行解码还原出真实流量，提取网络层、传输层和应用层的头部信息，甚至是重要负载信息。同时，天眼传感器自主研发的攻击检测引擎可以实现流式匹配，达到高性能处理，预置了上万条攻击规则，覆盖了针对常见漏洞的攻击检测。

第三，针对加密勒索阶段，天眼文件威胁鉴定器利用虚拟执行检测技术能够识别恶意样本；与传统的采用基于恶意代码特征匹配的检测方法不同，虚拟执行检测技术所采用的规模化动态沙箱的方法可以对未知的恶意代码进行有效检测，这种利用对恶意代码行为进行动态分析的方法，可以避免因为无法提前获得勒索软件代码特征而漏检的问题，即在无需提前预知勒索软件样本的情况下仍然可以对勒索软件进行有效的检测，天眼文件威胁鉴定器可实现对勒索软件的若干变种进行检测。

天眼通过基于流量日志及针对勒索软件的威胁情报 IOC 进行关联分析，从而发现失陷主机。威胁情报主要来自云端威胁情报中心的分析成果，可对 APT 攻击、新型木马、特种免杀木马进行规则化描述，通过人工智能结合大数据知识及攻击者的多个维度特征，还原出攻击者的全貌，包括程序形态、不同编码风格和不同攻击原理的同源木马程序、恶意服务器（C&C）等，持续的发现勒索软件威胁，最终确保发现的未知威胁的准确性。通过威胁情报形式打通攻击定位、溯源与阻断多个工作环节，提升了对攻击回溯的能力。

同时，基于奇安信技术研究院星图实验室研发的全系统仿真动态分析框架，沙箱系统的分析过程对恶意样本完全透明，结合高仿真度的软件环境和数据环境，沙箱系统不仅可以根据加密磁盘文件、篡改引导扇区等典型操作识别勒索软件，还可以捕获并识别关闭系统服务、终止服务进程、删除卷影副本、清空回收站、释放勒索信、重启操作系统等勒索软件破坏过程的各个阶段行为，并报警。

近几年，随着关键基础设施的数字化程度不断提高，针对关键基础设施的威胁不断增加。而关键基础设施作为经济社会运行的神经中枢，一旦受到网络攻击陷入瘫痪，引起的连锁反应甚至会对一个国家 / 地区造成巨大损失。本次针对美国管道公司的重大勒索软件攻击，暴露出美国能源安全行业的网络脆弱性，同时为全球关键基础设施行业敲响警钟。

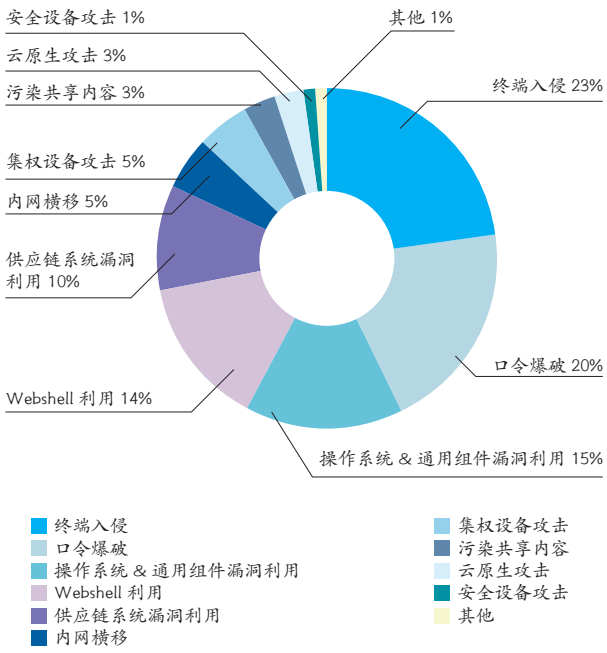
实际看来，这种高度定向的攻击本身已经等同于 APT 水准的攻击，我们必须构建高于攻击方的资源体系和能力。而只有持续的检测才能做到尽早发现、及时响应，有效防护减少受攻击的损失。天眼利用大数据分析技术，挖掘攻击线索，打通攻击检测、定位、回溯多个环节，最终提升对勒索病毒及高级威胁可测、可防、可溯源的能力。

服务器

勒索病毒事件频发 服务器安全防护刻不容缓

作者 奇安信云与服务器安全 BG 李栋

近年来，勒索病毒攻击事件呈快速上升态势，大型企业、医疗、软件供应链成为受攻击的重灾区，美国油管、Kaseya 云，以及国内多家知名企业均遭受过勒索攻击并造成严重后果。随着经济目标的转变，勒索的攻击目标也从终端逐渐扩展至服务器，定向攻击已经成为新的趋势，还在“裸奔”或是防护策略不严的服务器将面临严重的安全风险。



一、勒索病毒攻击分析

勒索病毒可以分为：病毒投放、病毒执行、病毒扩散三个阶段，每个阶段都可以多重攻击方式组合，还可以花式绕过现有的监控及防御措施，尤其是“0day 漏洞 + 变种勒索病毒”的攻击组合危害极大。

1. 病毒投放阶段

根据【奇安信云与服务器安全 BG】统计，常见服务器勒索病毒投放手段有数十种，常见的如右图：

终端入侵、口令爆破、漏洞利用、Webshell 利用、软件供应链攻击、内网横移是目前勒索病毒最常见的入侵手段，除此之外，域控 & 堡垒机等集权设备、安全管理设备、IoT 设备也成为高阶攻击者的新目标。同时，随着传统业务逐步向云原生环境迁移，API 攻击、容器镜像污染、编排工具利用、servermash 利用等在云原生场景下的勒索病毒入侵方式也开始逐

渐出现。

2. 病毒执行阶段

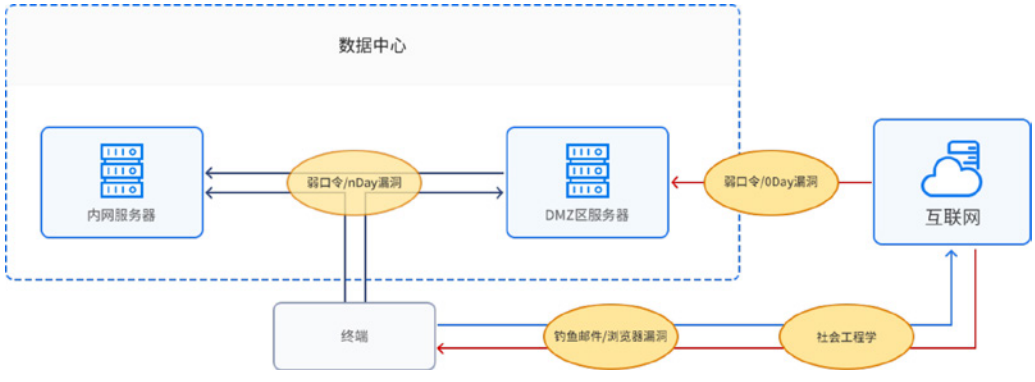
目前对抗勒索病毒在服务器本地执行的常用方式是杀毒软件，但频繁变形的旧病毒及不断出现的新病毒，都给依靠特征的查杀方式带来了巨大挑战，据奇安信统计，2022 年在国内活跃的勒索病毒家族有 PolyRansom、CONTI、GandCrab、Stop、Wanna 等近百个，每个勒索病毒家族都不断地有新型变种出现，因此即使部署了杀毒软件，服务器被上传了新型的勒索病毒后依然存在感染风险。

勒索病毒在成功执行后，会进行大量的文件扫描，并对数据类文件、系统关键文件进行加密，目前还衍生出无文件攻击的高级方式，即勒索病毒在本地无实体文件，而是以代码方式加载在 Powershell 等系统高权限应用中，并通过被感染的应用实现加密文件的操作，让病毒检测的难度进一步加大。

3. 病毒传播阶段

核心服务器一般部署在内部环境中，不容易被直接攻破，因此勒索病毒首次感染的服务器往往是边界服务器或者终端，而不是数据库、核心存储等勒索的最终目标，因此勒索病毒还需要通过自我增殖、横向移动的方式进行内网渗透，达到目标服务器后再进行加密勒索操作。

一个较为常见的“终端 – 服务器”的勒索病毒入侵轨迹如右图：



Step1： 利用弱口令 /0day 漏洞等方式直接入侵边界服务器；利用钓鱼邮件 / 浏览器漏洞突破终端边界，进一步渗透到边界服务器。

Step2： 入侵边界服务器成功后，利用弱口令 / nDay 漏洞 /IPC 横移等方式进行内网横向渗透，最终拿下目标服务器（数据库、核心存储等）。

二、服务器勒索病毒应对方式

发现勒索病毒说明服务器已经失陷，危害已经发生，因此服务器勒索病毒的应对思路应该由“事后补救”转变为“提前防御”，奇安信椒图服务器安全管理系统（以下简称：椒图）可以从“病毒投放 – 病毒执行 – 横向扩散”的攻击链上层层切断勒索病毒的传播途径。

对应勒索病毒的攻击链，其防御思路可以归纳为：防投毒（端口、漏洞、弱口令管理）、防执行（杀毒 – 已知病毒、白名单 – 未知病毒）、防扩散（微隔离）。

1. 防投毒

首先要切断勒索病毒所有的投放渠道，防治勒索病毒落地。

策略 1：屏蔽扫描

端口扫描是黑客攻击的第一步，攻击者利用扫描器可以获取服务器、开放端口和服务进程，并发现未修复的相关漏洞，再发起漏洞利用攻击。基于椒图防端口扫

描功能，可以有效阻止漏洞扫描的端口探测、Web 攻击行为。

策略 2：端口白名单 – 防危险端口暴露

椒图可以自动识别出暴露在互联网中的业务端口，帮助用户快速梳理整个业务信息系统的暴露面。并通过部署防护插件，配置端口控制策略进行管控。缩小企业暴露面，降低受攻击风险。同时支持用户自主添加端口进行入站 IP 的学习，形成可信 IP 列表，从而对异常访问进行告警或阻断。

策略 3：RASP– 防御 Web 类 0day

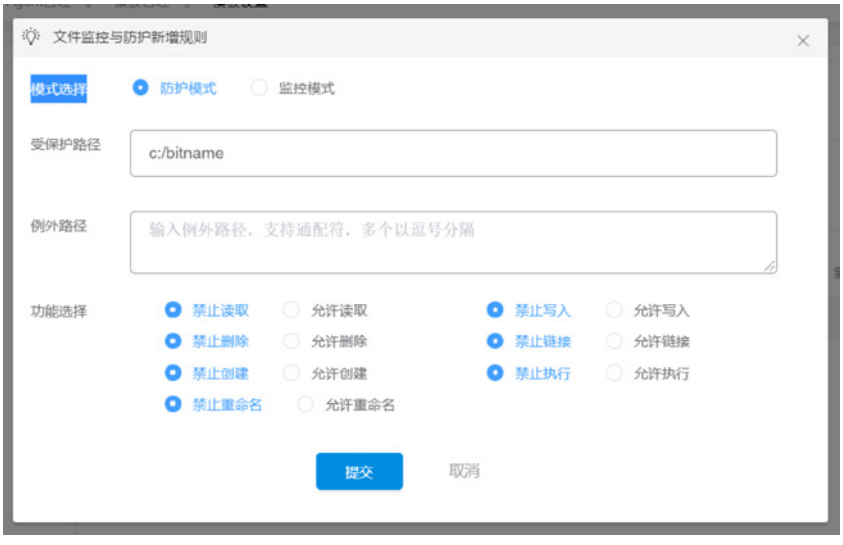
RASP（应用运行时自我保护，Runtime Application Self-Protection）工作于 ASP、PHP、Java 等脚本语言解释器内部，通过 HOOK 函数的方式，可以细粒度的监控应用脚本的行为及函数调用上下文信息，及时发现恶意代码和漏洞利用行为，RASP 通过“插桩”在语言解释器中，对流量转变为文件操作、命令执行、网络 IO 等运行时上下文进行检测，可以有效发现 WAF 规则外的 0dAY 利用，如 log4j 漏洞，涉及的应用和服务器很多，在短时间内难以完成升级攻击，通过部署 RASP 就能直接防御 log4j 漏洞利用，无需重启或者升级引用，能有效防止攻击者利用漏洞上传勒索病毒。

2. 防病毒执行

勒索病毒落地后的文件操作有三个特征：对文件进行大量原地读 / 写、创建同名但不同拓展名文件、对大量文件增加后缀，对这些行为进行实时监控和防护，可以有效阻断勒索病毒的执行。

策略 1：文件监控与防护

椒图文件监控与防护功能，可以保护整个目录、网页或文件不被恶意修改，支持监控 / 防护两种模



式，因为采用驱动级文件监控保护改功能，即使拥有管理员权限也无法实现恶意修改，权限可细粒度配置包括：文件的读取、写入、删除、创建、执行、重命名、链接等详细权限。可以有效限制 Webshell、勒索病毒落地。

策略 2：应用白名单 – 防勒索病毒执行

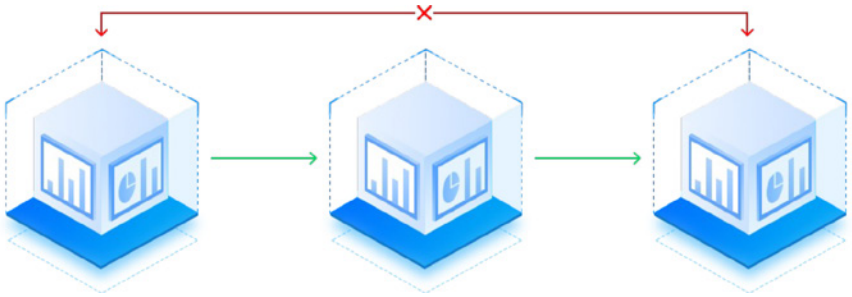
椒图自动学习已启动应用清单，根据威胁情报、病毒告警等信息，可快速识别出可信应用白名单。启用白名单防护策略后，勒索病毒及其他未知应用程序等非白名单应用将无法运行，直接免疫勒索病毒。

3. 防病毒扩散

类似于新冠肺炎的隔离政策，发现“感染者”应该快速做隔离处理，将危害控制在最低范围内。

策略 1：外连白名单

椒图限制服务器的对外服务进程只能访问特定的 IP



或域名，有效执行服务器中勒索病毒后链接 C2 服务器传输数据，或者进一步横向移动。

策略 2：端口暴露控制

椒图可以一键禁止服务器的内 / 外网访问，实现失陷服务器的快速隔离。

三、产品优势

奇安信椒图云锁服务器安全管理系统（椒图）依据云工作负载保护平台 CWPP 框架打造，是一款深扎服务器攻击面管理和运行时防护的实战型服务器安全产品。椒图基于资产与风险管理，提前发现安全薄弱点，实现攻击面的有效管理；通过 In-App WAF 探针、RASP 探针、内核加固探针等运行时防护技术，有效检测与抵御木马后门、暴力破解、无文件攻击、漏洞利用、SQL 注入等恶意攻击。在服务器端构筑事前加固、事中对抗、事后溯源的全程防线，实现网络层、系统层、应用层一体化防护，可有效保护服务器、虚拟机、云主机、容器等工作负载免受黑客及恶意代码攻击，满足实战攻防要求。

除了“打铁还需自身硬”，椒图也逐步实现与奇安信集团威胁情报、态势感知、零信任、终端等其他优势产品的协同联动，为客户提供更全面的整体安全方案。同时，椒图广泛应用于政府、能源、运营商、金融、制造、云计算及互联网领域，成功打造了多个千万级行业标杆。

服 务

遭遇勒索攻击后，一场教科书级别的自救指南来了！

作者 公关部 王梦琪

世界上大概有两种 CIO，一种是遭遇勒索攻击后选择支付赎金的，一种是不支付赎金的。前者为了业务正常运行而妥协，后者誓要与“绑匪”硬刚到底，找出自己的薄弱点赶紧修复。

一时损失真的可以换得长久安稳吗？一份国外调查机构 Censuswide 的数据显示，大约 80% 选择支付赎金的组织会遭到第二次攻击，其中 46% 有可能来自同一个团伙。

即使受害者支付了赎金以重新获得其加密文件的访问权，也经常会出现问题。46% 的支付者发现一些数据已被破坏，51% 的人重新获得了访问权，但没有数据损失；3% 的人根本没有拿回他们的数据。

时至今日，勒索攻击，这一网络安全世界的“流行病”，并没有随着安全技术水平的提升而销声匿迹，反而愈发猖獗，或针对企业系统，或针对数据资产，以敲诈勒索为目的，横行网络空间。面对勒索攻击，究竟怎样做才是完美答案？

当日 9:00am A 省某企业总部

上午九点，在 A 省某公司上班的小张刚打开电脑，就发现桌面弹出一张类似对话框的画面，文件名称显示异常。紧接着，小张试图打开桌面上的文件，但文件无一能打开。种种信息表明，这台电脑被“勒索”了！

不仅仅是小张，周围其他同事的电脑亦是如此。单位网络安全部门的工作人员进一步排查受影响的网络资产情况，同时发现部分对外业务系统也受到了勒索，工作人员立即切断网络，关闭远程服务端口。

经过对比、检索勒索信和被加密文件信息表明，这次攻击来自近年来十分活跃的 HIVE 勒索病毒家族。

面对公司内部众多受到攻击的终端和只有几个人的手下，网络安全负责人当机立断选择向专业力量寻求外援。


Hive

Hive Ransomware

Hive Doxware

(шифровальщик-вымогатель, публикатор) (первоисточник)

Translation into English

Этот крипто-вымогатель шифрует данные компаний и бизнес-пользователей с помощью AES+RSA, а затем требует выкуп в # BTC, чтобы вернуть файлы. Угрожает опубликовать данные. Оригинальное название: в записке не указано. На файле написано: encryptor_win32.exe.

Вымогатели, распространяющие Hive Ransomware, могут публиковать украденные данные с целью усиления давления на жертву (отсюда дополнительное название — **публикатор**). Для этого операторы-вымогатели начинают кражу данных ещё перед шифрованием файлов с помощью программных средств (**doxware**).

Обнаружения:

DrWeb -> Trojan.Siggen14.9462
ALYac -> Trojan.Ransom.Filecoder
Avira (no cloud) -> TR/Crypt.XPACK.Gen
BitDefender -> Gen:Variant.Razy.853199
ESET-NOD32 -> WinGo/Filecoder.V
Kaspersky -> Not-a-virus:HEUR:RiskTool.Win32.Generic
Malwarebytes -> Malware.AI.4245506271
Microsoft -> Trojan:Win32/Tiggre!rfn
Rising -> Malware.Heuristic!ET#94% (RDMK:cmR*
Symantec -> ML.Attribute.HighConfidence
Tencent -> Win32.Risk.Generic.Syhw
TrendMicro -> TROJ_GEN.R002H0CFP21

（图片来源于网络）

当日 9:30am 奇安信应急响应中心

“老大，A 省有多个企业报告遭遇了勒索攻击！”在接到 95015 应急电话后，奇安信应急响应中心的工作人员快步走向负责人，向上级报告了这两起都与 HIVE 勒索病毒相关的勒索攻击。话音未落，热线电话再次响起——

“B 省、C 省也有企业相继中招 HIVE 勒索病毒！”“还有 D 省……”

对于来势汹汹的勒索攻击而言，这仅仅是个开始。

从陆续接到各省企业组织的告警电话开始，奇安信应急响应中心立即成立了专项小组，选出应急响应总指挥和现场应急总指挥坐镇，并迅速成立溯源组、监控组、架构组、加固组和设备保障组，形成覆盖全局的应急响应体系。

这次勒索攻击，让奇安信集团安服应急响应负责人张永印不禁想起了此前一个类似的案例，仅仅两天时间，那场勒索攻击迅速席卷全国 10 个省份、20 个余城，各单位感染数量达上百个。想要赢得这场面对勒索攻击的战役，必须与黑客比“快”，抢占黄金救援时间。

于是，一线专家火速赶往现场，开始了争分夺秒的“救援”工作。

当日 10:00am A 省某企业总部

上午十点，安服专家与企业网络安全部门工作人员在现场共同开展后续处置与溯源工作。

在隔离中招主机的基础上，安服专家全面排查网络资产，进行全网病毒查杀、封禁恶意源 IP、修改服务器与主机密码等一系列处置动作后，开始了溯源分析。

综合文件、补丁、账户及网络连接、进程、计划任务、日志、流量等多个维度的搜证与排查，专家从中找到了攻击痕迹。但由于溯源涉及的样本数量巨大、现场困难较多，奇安信应急响应中心又增派了几名专家赶往现场增援。

当日 17:00am A 省某企业总部

下午五点，经过现场多名专家的连续奋战，终于初步理清了此次勒索攻击的大致情况。

经过排查发现，在遭受勒索的主机中均有受到同一 IP 地址机器的 RDP 登录事件，通过 RDP 登陆源锁定了一台对外业务服务器，并快速分析攻击发生的时间及手法，发现该业务服务器存在远程命令执行漏洞，最终将其串连在一起形成完整的攻击链。

随后，现场工作人员对已发现的利用工具进行清除，对使用的漏洞与业务系统进行核实漏洞是否存在，并升级最新版本。同时，专家协助企业网络安全负责人撰写好对外公告、管理相关舆情，直到此时，大家才稍微松了一口气。

在“黄金时间”内勒索攻击已初步得到抑制，专家们摸清了对手的套路，接下来才是响应处置的“重头戏”。

次日至第三日 A 省某企业总部

翌日上午，各方领导针对此次勒索攻击召开会议，考虑到奇安信应急响应以往丰富的处置经验和冬奥零事故经验，决定后续加固整改与持续运营仍然由奇安信负责。

会议结束后的两天时间里，一方面，现场专家仍在抓紧恢复受到攻击的设备，明确漏洞修复时间、清除问题文件、冻结问题账号，还原上线被勒索的主机，逐步取消临时策略、恢复正常业务运行；另一方面，在专家的指导下，制定符合当前业务和网络环境的关键措施要求，以加强全流量检测能力为后续目标进行整改。

受攻击单位紧急部署了更多奇安信天眼这类的流量检测产品。同时，正在进行的关键加固整改措施还包括减少业务系统端口的暴露，对服务器进行安全加固升级，杜绝弱口令，开启防护软件防爆破功能等。

短短三天时间，这场由 HIVE 勒索病毒带来的震荡已经渐渐平息，后续整改效果究竟如何？能否扛得住勒索攻击再次来袭？面对种种疑问，讲一百遍不如打一遍，以 A 省受攻击企业为首的单位率先开展了内部实战攻防演习。

第四天至第十天 A 省某企业总部

攻击发生后的第四天，第一轮实战攻防演练开始了，

这是对安全加固有效性和实战运营水平的真实考验。

与此同时，奇安信安服团队加派人员开展流量监测工作，先后投入安全监测人员超过 20 人，7×24 小时开展监测。

攻击发生后的第九天，第二轮实战攻防演练开始，一线专家协助企业网络安全工作人员继续优化监测处置流程。

攻击发生后的第十天，在前两轮攻防演习结果无异常的情况下，应急响应阶段工作初步结束，安全监测进入过渡阶段，开始转入常态化建设运营工作。

在这场席卷全国的勒索攻击下，A 省该企业的应急响应处置堪称应对勒索攻击的“满分答案”，为各省受攻击的企业组织处置做出有效示范，及时抑制了勒索攻击进一步扩散，在有限的时间内及时止损。

后记：专家支招勒索攻击的处置与防护

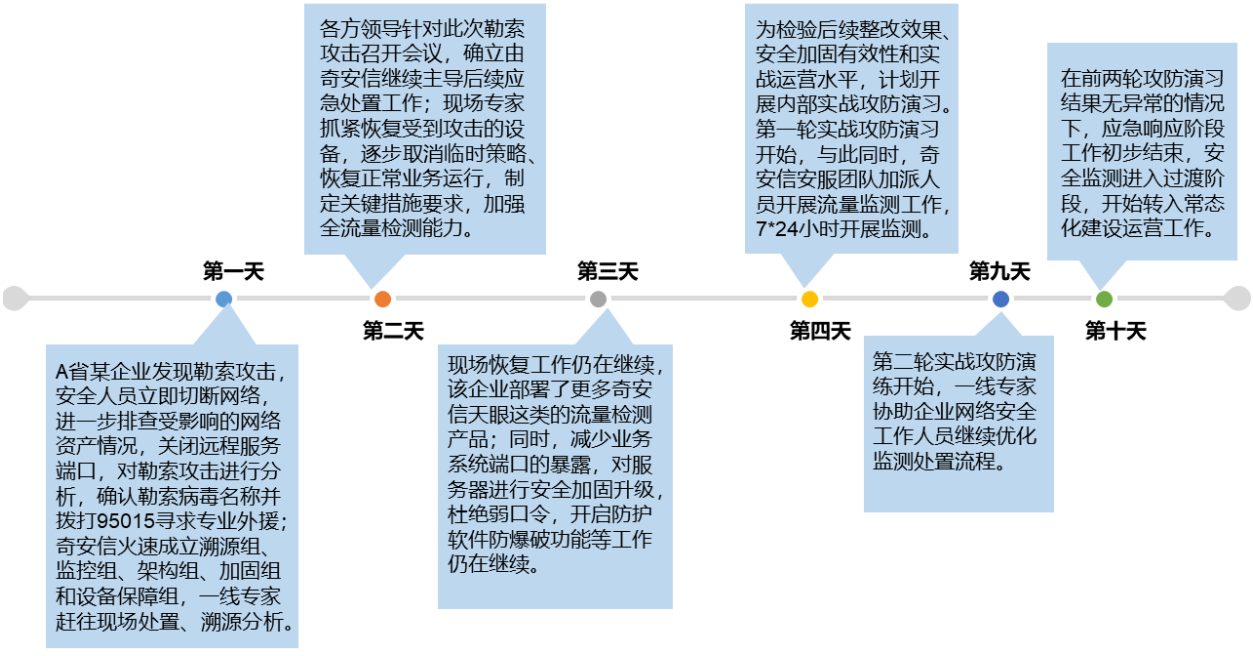
2022 年 8 月 10 日，思科证实，Yanluowang 勒索软件集团在今年 5 月下旬入侵了公司网络，攻击者试图以泄露被盗数据威胁索要赎金。攻击者声称已经窃取了 2.75GB 数据，大约有 3100 个文件，其中很多文件涉及保密协议、数据转储和工程图纸。2022 年 5 月，印度航空公司系统遭到勒索软件攻击，导致 25 日上午多个航班延误，数百名旅客滞留机场。2022 年 4 月，哥斯达黎加遭 Conti 勒索攻击，政府和经济遭遇打击，其新任总统 Rodrigo Chaves 宣布进入国家网络安全紧急状态……

国内外勒索攻击频频发生，给多国带来机密数据泄露、社会系统瘫痪等重大危害，严重威胁了国家安全。面对来势汹汹的勒索攻击，政企组织该怎样自救？奇安信安全专家归纳了以下几点建议。

一、重视常态化安全运营

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；

2. 定期开展对系统、应用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；

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

二、打造体系化与细粒度的安全防护，加强溯源能力

1. 部署全流量监测设备，及时发现恶意网络流量，同时进一步加强追踪溯源能力，为安全事件发生时提供可靠的追溯依据；

2. 部署高级威胁监测设备；

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. 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；

5. 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；

6. 重点建议在服务器上部署安全加固软件，并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。

三、提升勒索攻击发生后的快速响应、处置能力

1. 对于已中招的服务器应下线隔离，使用杀毒软件对中毒服务器进行全盘查杀，避免病毒的残留；

2. 对于未中招的服务器，在网络边界防火墙上全局关闭 3389 端口或 3389 端口，只对特定 IP 开放，远程连接类访问只允许白名单内 IP 连接；

3. 开启 Windows 防火墙，尽量关闭 3389、445、139、135 等不用的高危端口；

4. 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。

网络流量“指挥大师”是怎样炼成的?

通常情况下，不同的网络安全设备之间，有着不同的分工。

比如，防火墙按照最小化白名单原则，通过安全策略，仅对外开放有限服务，减小攻击面；

再如，Web 应用防火墙（WAF）可以阻止针对 Web 应用程序的恶意命令执行；

又如，入侵防护系统（IPS）可以阻止部分网络流量中的恶意攻击代码；

……

所有这些设备或多或少组合在一起，成为了企业网络边界的防守大闸。

鉴于网络攻击变得越来越复杂，安全设备也随之越来越多。

安全设备与“糖葫芦串”

不过，新的问题很快出现了。

网络安全目的本来是要保证组织不会因为网络攻击而导致数据丢失或者业务中断，但过多的安全设备有时会适得其反。

至于原因嘛，还要从大家小时候都吃过的甜品糖葫芦串说起。

众所周知，糖葫芦是用签子将一个个山楂球串起来制作而成的。吃的时候，一般都是从上到下按顺序一个个“消灭掉”。

为了吸引消费者，商家有时候还会将山楂球换成不同种类的水果，如葡萄、桔子等，但如果不喜欢某种水果，想要跳过它吃下一个，并不是一件容易的事，上面的冰糖会粘得满嘴都是，一个不小心还会将相邻的山楂球弄掉在地上。

安全防护架构也大抵如此，就像这样。

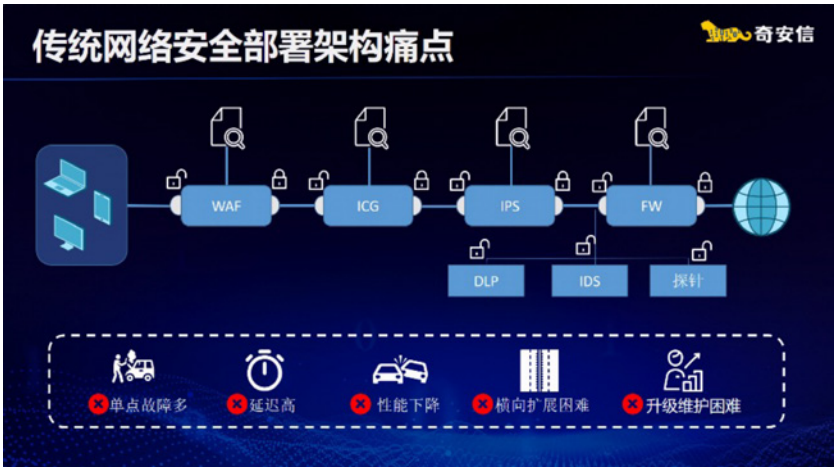
安全设备就像糖葫芦一样串成一串，等着检查访问服务器的网络流量是不是有问题。

想要跳过谁都不成。

尽管不同的安全设备在部分功能方面有所重合，但没有任何一款产品能够包打天下，各自专注在最擅长的领域，是最高效的做法。

但在这样一个糖葫芦串式的架构中，各个设备相互耦合，就像一个山楂球粘着另外一个山楂球，彼此影响。

“所有设备穿糖葫芦式的接进来，所有流量就会流经所有安全设备。”奇安信集团副总裁、首席架构师吴亚东在 9 月 13 日的奇安信流量解密编排器发布会上说，



这样一来就会出现三个问题。

第一，访问服务器的流量都要被一条链路上的所有安全设备检查。

个人 PC 会因为装了各类安全软件导致运行缓慢，其主要原因在于这些软件在保护计算机的同时，消耗了过多的内存、CPU 等硬件资源。

网络安全设备也一样。事实上不同类型的专业设备检测的流量并不相同，并不需要检查所有流量，即使检测也检测不出个子丑寅卯。而且，过度检测只会导致非必要的性能损耗，从而影响业务系统的运行效率。

第二，一旦单一设备出现故障，会导致整个链路不通。

学过物理的都知道，在一个串联电路中，任何一个元器件出现断路，整条电路就都断了，这就相当于开关没有闭合。

网络也是一样，任意一个网络节点发生拥塞或故障，都可能导致业务访问延迟大或业务中断。而且，一旦故障发生，想要迅速找出故障点。逐个设备排查，费时费力，想要第一时间恢复纯靠运气。

另外，对安全设备进行升级维护，都要提前通知预留割接窗口，且通常都在晚上或周末，非常耽误时间。

第三，扩展性差，难以对安全设备进行横向弹性扩容。

随着企业业务量的扩张，旧的安全设备一定会遇到性能瓶颈的难题。

比如，一台防火墙吞吐量为 1Gbps，但业务访问流量如果增长到 2Gbps，就会面临着扩容的问题。

常见的扩容方式包括横向扩容和纵向扩容两种。

举个例子。一所高校想要扩招，现有的宿舍楼肯定是不够住的，必须得扩建。

所谓纵向扩容就是指在原有宿舍楼基础上，纵向往上加盖几层，得到一栋能容纳更多学生的宿舍楼；

横向扩容是指重新选址，多盖几栋宿舍楼，大有“横向发展”的意思。

但网络设备不是宿舍楼，不可能往上加盖几层，想要纵向扩容，只能换一个更好的。

在糖葫芦串的网络安全部署架构下，向糖葫芦串中不断串接设备这种横向扩容方式并不适用，和木桶效应类似，流量处理能力取决于最小的那个设备，接再多的设备也无济于事。

最窄的地方“堵上了”，整条路也就“堵上了”。

因此最理想的横向扩容形式为 HA 双主（即两台机器同时独立运行，互不影响，流量处理能力约等于两台机器之和），但流量一旦超过其处理能力，还是得纵向扩容，将原有设备换成性能更高的型号。

这样一来，旧的设备就失去了用武之地，原有投资无法得保护。

而且，更换设备会导致断网，断网也意味着业务中断，这是所有组织都难以接受的，也不是网络安全防护所想看到的结果。

流量调度室

其实不难看出，所有问题的症结都在于这个“糖葫芦串”上——这是流量到达访问目标的唯一路径，不管流量要在哪个设备上接受检查，都得一个个过。

想要解决这个问题，就得从根上解决“穿糖葫芦”

式的安全设备部署方法，让特定流量只经过特定设备。

这和处理城市内涝的思路是一样的，积水需要通过遍布全城的下水道网，引流到该去的地方，而不是仅仅依靠一个大的河渠。

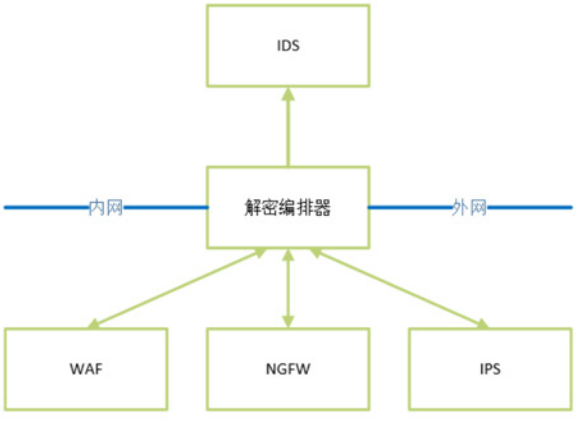
不过，网络流量不像积水一样，会在重力的引导下自动由高处流向低处。

所以，奇安信在 9 月 13 日发布的流量解密编排器上，引入了智能化服务链编排技术。

听起来有点晦涩，但实际上就是给网络流量造了一个“调度室”：让从哪条路走，就从哪条路走，而不是都挤在主干道上。

服务链编排做的第一件事情，就是基于细粒度智能引流策略。包括对主干路经过的流量进行分类，然后将流量引流到由安全网元组构成的服务链上，如需要进行漏洞检测的转发至 IPS；需要进行 Web 防护的分流至 WAF 进行检测；需要旁路检测的，通过串联链发送给相关设备，如探针、IDS 等。

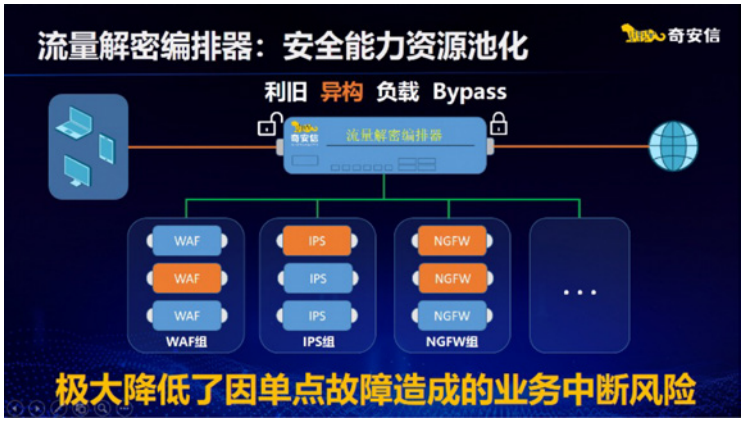
这样一来，过去“串糖葫芦”式的架构就不复存在了，取而代之的是一种“旁挂式”的架构，简单理解就是下图的样子，即编排器基于智能引流策略，按照服务链中定义的安全网元组顺序，引导流量依次通过。



这样做最大的好处就在于不同的安全设备再也不用检测所有流量，而是根据业务安全需要，通过个性化的引流策略让安全设备分工合作各司其职，从而大大降低了安全设备无效的工作负载，提升了整个网络的运行效率。

第二件事情就是实时探测各个安全设备的运行状态。

这么做的好处有两个：第一个是在探测到发生故障的安全设备时，可以启动 Bypass 机制跳过故障设备，将原本需要经过该设备的流量，自动转发至相同网元组内的其他同类型设备，保障业务持续运行；



第二个是对安全设备的运行状态进行实时可视化展现，一旦设备运行出现问题，工程师可第一时间定位到故障点并修复，避免排障“全靠运气”的尴尬局面。

第三件事情是安全设备的资源池化。

与传统架构最大的不同是，资源池能够实现安全工具和网络架构的解耦，按需个性化智能引流，以及横向弹性伸缩，安全资源利用率最大化。

如前文所述，串糖葫芦式的架构是很难新增设备的，想要扩容只能将原有的设备换成一个更高端的，导致客户 TCO（总体拥有成本）持续增加。

但服务链编排技术可以将旧的和新增的安全设备放入相同资源池，按照流量负载算法将流量牵引至不同设备处理，不但让原有的安全设备仍然可以持续发挥作用，更重要的是带来了动态横向扩容的便利。

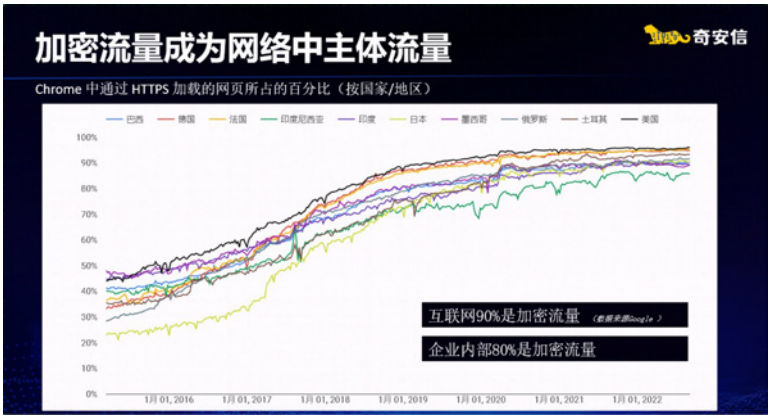
想要扩容，新增设备就完事了，流量解密编排器会把该过去的流量调度过去。

当然，这三件事情对第三方的安全设备同样有效，并不会因为采购了不同厂商的不同型号设备，出现服务链编排效果大打折扣的现象。

一次解密，多次检测

有一点需要注意的是，服务链编排技术在如今加密流量时代显得尤为重要。

众所周知，流量加密的本意是为了防止数据在传输过程中被监听或者被劫持，但这同样给了攻击者隐藏自己的机会。



互联网超过 90% 的流量是加密流量，企业内部超过 80% 的流量是加密流量，95% 的企业声称遭受过加密流量攻击……

这几个数据非常直观地展示了针对加密流量检测的紧迫性。

通常情况下，加密流量检测最直接也最有效的方法，就是将密文流量解密成明文。不过，解密过程所消耗的 CPU 资源是非常惊人的，可以达到明文流量检测的 100 倍之多。

用一句话来形容，解密是 CPU 密集型操作。

如此巨大的消耗，如果再让所有安全设备都来一遍，导致 CPU 资源无故浪费不说，还势必给系统网络带来极大的延迟。

如果用简单的算式计算，“糖葫芦串”上串了多少个设备，就还会在 100 倍算力消耗的基础上，再增加多少倍的算力消耗。这对任何组织来说，都是一件非常不划算的事情。

而且，如此多的加密流量，经常大大超出安全设备的解密能力上限。

为了保障业务的连续性，网络安全只能有所妥协，使得加密威胁成为企业当前面临的重大问题之一。

如果使用奇安信流量解密编排器则大有不同。流量解密编排器搭载的高性能解密能力，能够在完成流量解密之后，依托服务链编排技术将明文流量按需分发至既定的安全设备中，实现一次解密多次检测，从而避免了 CPU 资源的浪费。

从这个角度上看，服务链编排技术称得上是一位顶尖的网络流量“指挥大师”。安

护航三农金融
天眼助力江苏省联社打造全行威胁感知大脑

作者 安全攻防 BG 云娟

在数字经济浪潮席卷全球的今天，网络信息安全问题日益突出。银行机构作为关键基础设施单位，直接或间接地影响了国家经济发展和人民生活，其信息安全的重要性不言而喻。而作为我国银行业的重要组成部分，全力支持三农金融发展的主力军，农村信用社的网络安全也应引起高度重视。

“今天的江苏省农村信用社联合社（简称：江苏省联社）及所属 60 家农村商业银行的 IT 系统，承载着非常丰富的金融业务。而随着信息化应用范畴的不断扩展，其安全风险也正慢慢从保护人、财、资金安全的范畴向网络安全、信息安全、病毒防护、防御黑客攻击等多方位延伸。如何保证总部和农商行业务系统的稳定运行、保证业务持续的运转，是我们要加强的功课。”江苏省联社信息科技部相关负责人表示。

江苏省联社是全国农村信用社首家改革试点单位，也是国内成立规模最大的一家省级农村信用社联社。为了满足客户的服务需求，联社不断提升网络信息安全管理，不断加强网络信息安全建设，但也不可避免地存在一些问题。为了应对不断变化的安全问题，江苏省联社于 2018 年建设全行态势感知平台，将省联社内外部漏洞、威胁、攻击等安全事件及信息融合贯通，全天候、全方位感知全行网络安全态势。

2019 年，为了将省联社的安全服务能力下沉到 60 家农商行，建立全省农商系统的安全流量监测系统，江苏省联社选择了在威胁检测与响应领域有丰富实践和服务经验的天眼作为合作伙伴，在原有态势感知平台的基础上，进一步丰富安全情报收集能力，实现全省农商行安全信息共享，增强对未知、重大网络安全威胁的监测、处置和溯源能力，为全省网点的各类业务正常有效地运转提供安全保障。

同时，通过部署实战化防御指挥系统，江苏省联社实时掌握全省网点的网络攻击预警情况，大大提升威胁事件处置能力，降低威胁应对时间和工作人员的运维压力。

值得一提的是，江苏省联社天眼、实战化防御指挥平台项目的成功建设，开创了全国联社体系之“首”：打造了全国首家全流量威胁分析平台体系化覆盖省联社，也覆盖地市一级农商银行的标杆案例；开启了全国首家省联社从实战角度出发，构建农信体系常态化网络安全综合防控系统的先例。

全面提升威胁应对能力，下沉金融安全能力

“信息化发展越快，银行所面临的网络安全风险也就越多。面对攻击时，我们无法有效地进行实时检测和阻断，更无法知晓总行和分行的整网信息安全态势，不能形成立体的、有效的防护。”江苏省联社信息科技部相关负责人表示，在江苏省联社推进金融创新的同时，网络安全的问题也日渐突出，省联社及所辖农商行仅依

靠单一的网络安全防护技术已经不能满足网络安全的需求，更不能及时发现网络中的异常事件，尤其是高级可持续性的 APT 威胁。

而且各农商行的不同防护设备之间的数据相对割裂，形成信息孤岛，只能获取局部的攻击信息，无法构建出完整的攻击链条，难以发现并追踪真实的攻击行为和攻击者身份。在新形势、新业态下，急需建设一套覆盖全网，具备全面深度威胁检测、感知全网安全态势的全省统一信息安全防御系统，抵御 APT 攻击，降低金融数据泄露风险。

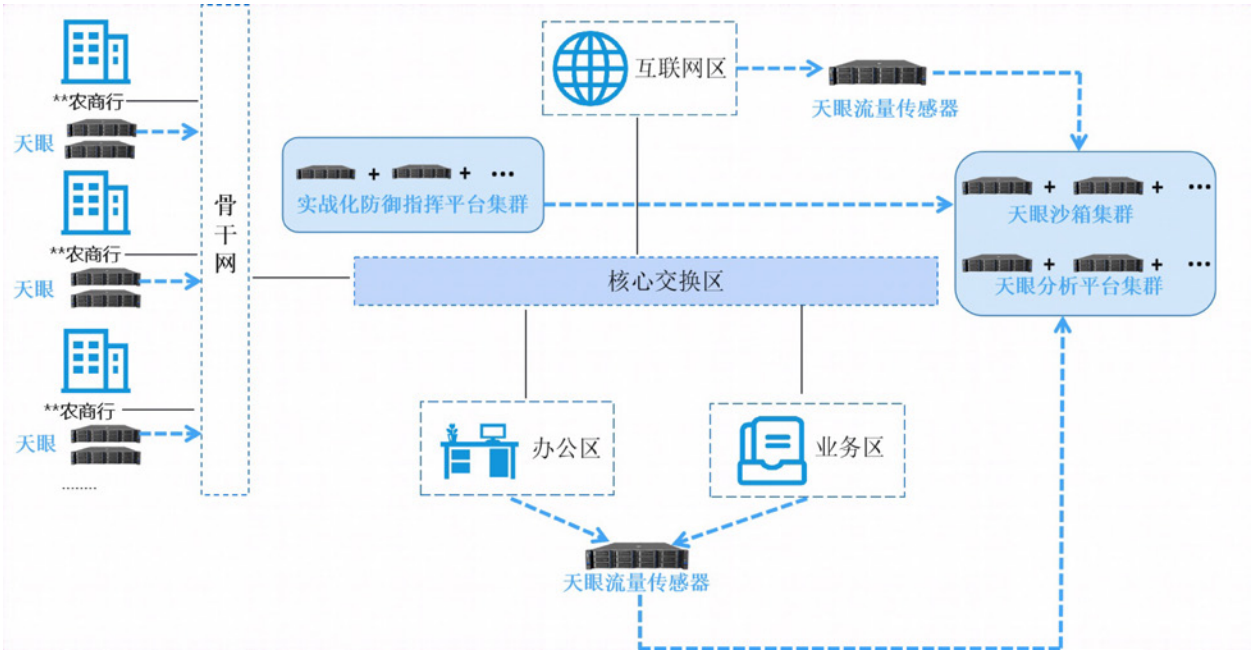
江苏省联社及所属农商行在部署了天眼系统后，不仅增加了省联社现有态势感知平台流量采集和分析能力，并将所属农商行天眼解析后的流量原始数据和日志数据传输到省联社态势感知平台，进行综合关联分析，完全可以感知 APT、勒索病毒、恶意文件、挖矿病毒等各类已知及未知类型的复杂攻击，全面掌握规模群体性事件的感染路径，让攻击链条在追溯中呈现的更加完整清晰。

与部署天眼系统前的较低感知率相比，江苏省联社部署后的威胁感知率实现了从量到质的提升。在参与客户攻防演习及重大活动保障过程中，在全网流量中发现数千次攻击和攻击源 IP 地址。

同时，利用省联社威胁攻击研判与协同化响应处置方面的能力，协助所属农商行实现快速精准的威胁检测与响应处置，真正做到将省联社的安全服务能力下沉到家农商行，实现所属农商行与省联社威胁情报共享，达到全省农商行系统安全威胁“一点发生，多点响应”，降低安全威胁检测和响应时间，增强全省农商行应对威胁的能力。

集约化建设降本增收，安全态势感知不留死角

随着数字化进程的深入，银行对数据需求将越来越大，数据成为江苏省联社数字化转型的基础。依托江苏省联社大数据基础平台和平台数据接口的开放性，天眼系统的部署，帮助省联社建设了内部安全数据的“总线”，提升了安全数据的复用和共享能力，提升安全态



势感知系统应用开发与集成的便捷性和开放性，真正达到“一次建设，长期受用”的目的。一方面，避免了全省农商银行重复建设，取得了较好的网络安全投入建设效果；另一方面，在节约成本的同时又提高了资源利用率和工作效率，走出了一条集约化的网络安全态势感知建设之路。

“每家农商行的情况都不一样，专职从事网络安全工作的员工素质也参差不齐、工作内容也很复杂、人员数量也少，很难保证各类业务不出现安全问题。而这条数据安全的总线每天都在全省农商行发挥着积极的作用。”江苏省联社信息科技部的负责人表示在没上天眼系统之前，各农商行面临的棘手问题之一就是威胁感知能力弱、感知面窄。

而部署天眼系统之后，全省农商行实现了对本地安全日志数据的采集和富化，对银行生产网、办公网、互联网出口的流量进行全面的采集分析，基本做到了 100% 覆盖业务网络安全，全省农商行的态势感知能力上了新台阶。

同时，省联社通过利用关联规则与威胁情报，实时从行为数据中识别各类威胁，并将威胁事件与银行业务对象结合，直观地感知银行内部的安全态势，快速的定位存在风险的内部资产，并进行响应和处置。

安全协同运营，实现一体化安全防控

在部署天眼系统前，江苏省联社网络中已经部署了防火墙、入侵检测、防病毒网关、网络审计、网络流量分析、威胁检测、服务器安全管理、攻击诱捕等大量安全设备，而且 60 家农商行分散在全省的各个位置，要进行统一安全管理和维护，是很大的挑战。

部署天眼系统后，每天天眼系统实时处理日志量超过亿条，告警归并之后，大约有 2000 多条告警，这些告警还包含大量误报告警，给安全运维再次造成巨大的困扰和压力。

“原来部署在农商行各业务出口的各类威胁监测设备，需要人工单独将告警信息转化成工单，并进行层层流转发给总行省联社，才能对事件进行处置，无法形成

闭环，不仅效率低、处置效果差，而且也无法通过各类安全问题洞察全局风险。”江苏省联社信息科技部负责人表示，彼时他们亟需一套统一的威胁事件汇聚平台，来将省联社和分行进行协同运营，以此来提升总行及分行信息化安全防御能力。

而天眼家族旗下“实战化防御指挥平台”的部署，真可谓实实在在帮助江苏省联社解决了安全运营效率和效果的难题。

在效果上，江苏省联社可实时掌握全局网络攻击预警情况，实时预警发现网络安全案件线索，掌握有关情报和情况信息，协同下属银行通报预警重大网络安全威胁，并针对处置情况进行跟踪归档化闭环处置。

通过与天眼系统联动，实战化防御指挥平台预置多种处置场景应对常见类型的告警事件，对应不同告警事件调用预置的处置流程，下发处理动作完成对告警事件的处置，提升业务系统的安全系数。

在效率上，通过实战化防御指挥平台，江苏省联社完成安全防护产品威胁事件的集中分析、分析，响应处置和决策建议一整套流程，缩短告警事件分散处置流程链长，提高预警效率。

同时，实战化防御指挥平台通过自主编排功能，可根据实际业务需求添加任务脚本、联动服务及工作流程，实现省联社及各大分行根据银行业务需求量身打造处置流程，提升了响应处置的速度与准确性。

农村信用体系不仅支撑着农村金融的健康发展，也对激发农村地区市场活力、促进农民增产增收起到重要的推动作用。在谈及银行未来的网络安全规划时，江苏省联社信息科技部负责人表示，“十四五”开局之年，江苏省联社将继续加强网络安全整体态势感知，在天眼和实战化防御指挥平台持续赋能下，加强省联社安全运营管理，提升银行整体风险防控能力，从网络安全的角度为全省农商银行数字化改革发展、为推动乡村振兴战略落地生根保驾护航。安

与勒索黑产对抗，星星之火，可以燎原

——走近应急响应负责人张永印

作者 公关部 包世玉

“其实做应急响应和散打很像。”聊起自己一直在做的应急响应工作，张永印想起了自己练习散打多年的经验，大部分人认为散打的出招似乎无章法可循，但他说，虽然散打不讲究花式和好看，但其实综合了各个流派的打法，讲求克敌制胜为主，很接地气。”

其实张永印说的不错，在勒索发生得越来越频繁的今天，作为集团安全服务应急响应负责人，他每天都在解决五花八门的应急响应事件。而奇安信的冬奥网络安全应急响应 95015 公共服务平台遍布全国 30 多个省份，7X24 小时待命，每年处理事件千余起。若无章法可言，恐怕是一盘散沙，但若团队协作顺畅，合力出拳，则是无往而不胜的。

开拓建制，克敌制胜，张永印和团队与勒索的“对抗”得心应手。

兴趣指引，与“勒索”过招

“我真的是喜欢技术，也喜欢搞事儿。”张永印提起自己最开始接触攻防，是在上高中的时候。2000 年初，QQ 作为新时代的聊天软件一下子火爆了起来，一直拥有好奇心的张永印也不例外，注册了 QQ 号，每天出入聊天室，探索互联网这个新世界。

然而没过多久，QQ 号突然登录不上去了，一研究才知道，原来号码还会被盗取。天生不服输的他开始自己研究起来，每天泡在论坛里看帖子、研究攻防，甚至后来自己录制视频传到网上，收“学生”，认识了一帮圈内的“黑客”朋友，也就此入了门。

这样一段经历，对张永印有很深的影响。甚至到后来入行，入职奇安信很久，张永印都走在了研究技术、开拓创新的路上。

2018 年，我国 H 城市的海关和高法行业陆续遭遇了勒索攻击，彼时，张永印刚刚接手应急响应团队。

说起在奇安信这几年，张永印前后负责过十几个业务，“孵化”了不少事儿——

2017 年和同事玉山一起打造了一款工具，这也成为了后来应急响应工具箱的雏形；2017 年年中接手大客户的态势感知项目，结束后把态势感知运营方案规划出来；2017 年到 2018 年，他负责安全运营团队，随之搭建起来一个 200 多人的团队。

2018 年的这两件勒索事件，H 市海关的事件发展很快，而高法行业的事件则是潜伏时间久、影响广。

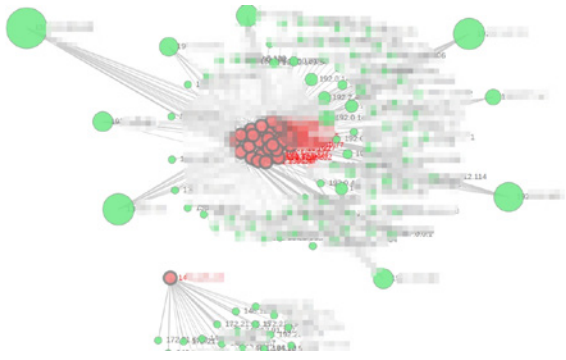
安服在 8 月 13 日 12 时 13 分接到 H 市海关的应急需求，当时已知被感染的服务器有十几台。应急团队在

13 时 30 分到达客户现场后，已知被感染的服务器就达到了 29 台，翻了一倍。

“就像散打，应急响应工作争分夺秒，对手出招都是出其不意的，这也是为什么我们 95015 应急响应热线都是 7X24 小时服务的原因。”经溯源调查发现，黑客首先攻击并控制了一台与 X 城保税区有关联的供应商的服务器，随之由此作为跳板分别控制了 X 城保税区和 H 城海关的两台服务器，紧接着再利用此为跳板暴力破解了 H 城海关其他的内网服务器，并投放运行勒索病毒 GandCrab，对服务器文件进行了加密操作。

在了解情况后，团队开始进行相应的应急处置，在事件发现后第三天的凌晨 3:55 分，业务全部恢复上线，并在 9:30 分客户上班后进行了汇报。两天半的时间内，张永印与团队共计 7 人，解决了 H 城海关的勒索事件。

紧接着在 9 月，高法行业勒索事件爆发，应急响应团队快速出动，共计为 20 多家客户单位进行取证溯源，最终发现受感染数量几十台。与上次不同的是，这一次最主要的勒索病毒是 GlobeImposter，而这两个病毒，正是 2018 年勒索病毒活跃榜前两名。



也正是在这一年，勒索病毒经过爆发式增长，奇安信接收到的大中型政企机构应急响应服务数量从 2017 年的 199 件陡增到了 2018 年的 717 件，翻了将近 3.5 倍，而整个勒索也呈现了产业化、链条化的特征。

虽然两件事情解决地快速且顺利，但观察着越来越多勒索事件密集发生，张永印心里对应急响应的工作，也有了更多的想法和要求。

一年建体系，快速提升效率

最有效的防守，就是进攻。在散打中，张永印是一个喜欢进攻的人，而在面对勒索的攻防对抗中，防守是最重要的一环。而这一环如何守住，要靠紧密的团队合作和先进的团队机制。

在 2018 年的两次大规模应急事件处理后，张永印和团队进行了一个全面的复盘，“开总结会的时候，吴总给我提了要求——把应急响应系统 IT 化，拉通各个环节，提高效率，让资源有效地利用起来。”

说起“搞事情”，张永印来了兴致，撸起袖子，便投入进了对应急响应进行体系化规划与建设的工作中。

从 2018 年开始对应急响应体系进行规划，到 2019 年 BCS 大会应急响应体系正式上线，张永印和团队用了一年的时间。他们首创的网络安全“120”应急响应全流程服务模式，国内唯一、国外未见。

应急响应服务模式中包含了机制与平台。应急响应机制，对整个应急响应的处理流程进行了整体地、体系化地规划，而应急响应平台通过“指挥中心 – 调度平台 – 应急资源”的三级体系对资源进行整体地规划和调度。

“之前十几个项目的经验很有用，应急响应工具箱就是安服从之前的一个项目之中孵化出来的。”张永印的团队在集团的指挥调度中心负责调度全国的应急资源，其中就包括了应急相应人员和这款应急响应工具箱。

“好马配好鞍，当我们的人冲到前线，这款能够覆盖多场景的应急响应工具箱融合了多场景溯源分析能力等一系列功能，为应急处置的现场解决了不少难题。”

好的体系搭建起来，效率提升自然就是快速的。

从 2020 年 1 月 1 日到 2021 年 11 月 30 日，奇安信应急响应平台共处置了全国应急事件 1640 起，平均每单处置耗时 7.19 小时，比 2019 年平均每单减少 3 小时，平均处置时间减少 30%。其中“外卖式”“可跟踪”“可评价”的服务体系，让整个工作形成了闭环。

由于高危漏洞数量的逐年上升，虽然张永印团队在应急响应处置上面的耗时逐渐减少，但待处置的需求却在上升。

张永印心里知道，是时候再整点“事儿”了。

两个创新，再上一个台阶

“勒索只是恶意行为的其中一种呈现形式，而很多有潜在危害的攻击行为也一直存在于发生勒索行为之前。为了更好地防守，往往研究如何有规划的前期准备，也是‘进攻’。储备足够的人才就是一种准备。”张永印不想只是“应急”，更想要有充分准备地“制动”。

在奇安信集团拿下了北京冬奥的保障工作之后，张永印的应急响应团队也需要打造一套配合冬奥的全新的应急响应体系。同时，随着勒索事件的快速增多，应急响应需求增加，对专业人才的需求也增加了不少——于是，应急响应联盟应运而生。

“其实联盟在做的事情我们很早就在做了，不过成立了联盟，一是为了更好地将专业人员资源合理调配进行平台化、体系化的建设，二是我们的培训机制可以真正地培养出来更多的人才。对抗勒索，组织、机制很重要，人才也同样重要。尤其是冬奥期间，专业的应急响应人才是稀缺的。”

是的，冬奥的应急响应95015公共服务平台也是张永印和团队落地执行的。平台在延续了以往的三体系外，95015作为全国第一个网络安全行业服务短号，于2022年1月20日正式开通，成为了北京冬奥会网络安全保障指定号码。

在冬奥期间，平台为全国政企机构提供7X24小时服务的同时，规模覆盖了全国31个省市、2个特别行政区，有2000多名具备攻防能力的应急响应工程师，和100多名资深安全专家，7X24小时随时待命，2小时内可到达现场处置。而这其中，都少不了足够的专业人员储备。

“为了应对冬奥，2021年4月，中国电子应急响应中心正式挂牌成立了。而将应急响应联盟真正一次拉入大规模实战的，就是冬奥成立的‘冬奥央企网络安全救援队’。” 在冬奥会期间，由国资委指导、中国电子集团牵头，联合中国电信、中国移动、中国联通、国家能源、国家电网等30家中央企业组成的几百人的救援队，为冬奥的应急响应贡献了不少的力量，而这也都得益于联盟成立后的整体机制设立和培训成果。

2022年1月23日—2月27日冬奥保障期间，救援队共参与和处置了全国范围内70多起网络安全应急响应事件，全国19个省份。经统计发现，攻击者针对的大中型政企机构的攻击意图排名第一的就是勒索，35.1%遭受到了勒索病毒的攻击。

经过三年多的发展，目前应急响应联盟已覆盖全国20个省份，联盟成员单位62家，目前拥有100位资深安全专家。

经过冬奥实战，应急响应95015公共服务平台经过了打磨后更加成熟，应急响应联盟也由此上了一个台阶。

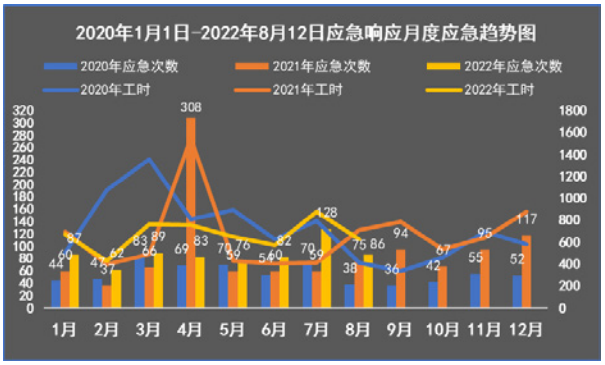
闲不住，心里有一团搞“事儿”的火

“我是真的喜欢工作，能在一个靠谱的公司，和靠谱的团队，做一些有意义且正确的事，我很满足。虽然应急响应工作有时是累的，但我也闲不住，成长更让我兴奋。”

近年来，政企机构面临的网络安全威胁越来越多，高危漏洞的数量也在逐年上升，看来张永印是“闲”不下来的。

根据CNCERT对CNVD收录的安全漏洞数量分析显示，近几年安全漏洞数量呈逐年上升趋势，自2016年以来，年均增长率达17.6%。通过奇安信应急响应服务次数进行对比也印证了这一点， 2017年至今应急响应次

数，也呈逐年上升趋势。截至今年 8 月份，应急响应团队共处置政企机构网络安全应急响应事件 4000 余起，累计投入工时 40000 多个小时，为全国超过 2000 家政企机构解决了网络安全问题。



“这都过去了，是团队合作的成果，我们要看以后。”说起团队，张永印表示自己很喜欢和大家没事儿“杠一杠”。

别看张永印在私下是一个随和的东北人，说话风趣幽默，但工作中却是实打实地“较真”：“做应急的都是实在人，处置事件也都是和勒索病毒、黑产‘真刀真枪’地拼，平时多和同事杠一杠，一来二去之间，也许一个新方法就杠出来了。大家也了解我的脾气，都是为了工作。”

提起未来对于对抗勒索和应急响应的工作，张永印想要做的更多，“其实现在看起来形式严峻，但还是有很多客户没有真正对网络安全上心。勒索团伙的投资回报比很高，他们一刻不停手，我们就要一直跟他们‘打’下去。”要说之前在公司经手的十几个项目，负责应急响应是张永印做的最久的一项，可能也正符合了他的性格，一刻都“闲”不下来，每一刻都在“战斗”，一直都在创新。

“按照目前的数据来看，今年的应急事件数量一定会超过去年。我们所经受的事件也越来越复杂、越来越紧急。我们根据客户特征、客户需求对处理方案做了全面升级。”提起要做的事，张永印已经给自己订好了 KPI，“升级应急响应处理方案的这件事儿已经在做了，今年即将到来的重要保障工作我们也在陆续筹备和推进过程中，另外应急响应联盟也要继续发展壮大，未来联盟的人员数量是一定会持续增加的……”

对于张永印来说，似乎真的很难让他“闲”下来。

有想法、正能量、接地气，最主要的是有追求，心里有一团求胜的火。

可能应急响应这种不断追求如何能“打败对手”的工作性质，让他想起了以前在散打比赛中的感觉，又或是让他回忆起当初坐在计算机前录制攻防视频的少年时光。他内心始终存着一股力量，让他乐于了解“对手”，乐于挑战不可能。

与勒索的对抗是不可能停歇的，应急响应工作可能是夜以继日的，也许让他心里那团求胜的“火”不断燃烧的，是散打擂台上的另一个人、是计算机另一端的黑产，也可能是张永印心里的另一个跟他说“不可能”的声音。

但张永印不相信“不可能”。安

一次勒索，180 人摧毁了一个 600 万人帝国

作者 公关部 张少波

要摧毁一个 600 多万人口、8 万军队的强盛帝国，需要多少兵力？有人给出了答案，180 人！

这是人类历史上发生的真实事情，也创造了冷兵器时代双方实力最悬殊、以少胜多的记录。

故事发生在 1532 年 11 月，主人公名叫弗朗西斯科 · 皮萨罗，是一位西班牙冒险家。这个人从小没念过什么书，不按常理出牌，就是俗话说的，“社会我皮哥，人狠话不多”。

如果放到今天，可能就是一个街头混混，混好的话得是个黑社会小头目。但是人家赶上的时代好呀，赶上了风云激荡的大航海时代。哥伦布、麦哲伦们，是他的前辈，不断冒险和征服是这个西班牙人的乐趣。南美新大陆，就是他的征服目标。

在他的征服生涯中，最“辉煌”也是最臭名昭著的，就是 180 人毁灭了 600 万人口印加帝国的事迹。1532 年 11 月，皮萨罗带领约 180 人的军队到达印加帝国的卡哈马卡城。他的征服对象，军队有 8 万之众，人口 600 多万。180 VS 600 万，即便是一个人杀 1 万人，也不可能摧毁这个国家。但是结果却令人瞠目，几乎不费吹灰之力，印加帝国就被灭国。

那么，究竟皮萨罗是如何打赢了冷兵器时代，这场实力最悬殊的战役的呢？

答案是，勒索。

图：西班牙人皮萨罗

要知道，凭借区区 180 人，去和数万印加帝国军队死磕，即便是每个西班牙人装备精良、武力超群，也不可能杀光数万军队。况且他们是远洋作战，没有后勤补给。

因此，皮萨罗的第一步，是让对方放下戒心，假说要“交流”。

结果，思想“单纯”的印加帝国国王阿塔瓦尔帕果然上当，不仅未加戒备，还在为皮萨罗等人的到来欢呼。

在阿塔瓦尔帕本看来，皮萨罗等人身着铠甲，骑着骏马，威风凛凛，犹如神灵下凡。经过

与皮萨罗等人的“交流”，他们得知皮萨罗等人是来结交朋友，向他们传播先进技术的，否则他们也不会只派100多人。

第二步，就是不宣而战，擒贼擒王。

兵家有云：擒贼先擒王，西方叫斩首行动。西班牙人将这个战术发挥到了极致。

图：西班牙人擒获阿塔瓦尔帕

为了表示诚意，国王听从了皮萨罗的要求，只带了5000名手无寸铁的士兵出城迎接。皮萨罗抓住机会，命令部队向国王发起疯狂进攻。可怜的阿塔瓦尔帕本的军队，只靠血肉之躯，根本无法对抗皮萨罗的骑兵和火枪。

几轮进攻，皮萨罗活捉了阿塔瓦尔帕本。阿塔瓦尔帕原本是印加帝国的“神”。他一旦被俘，全国都不敢反抗。

第三步，挟天子以令诸侯，发起巨额勒索。

皮萨罗接着把印加帝国国王关押了8个月，同时勒索历史上最高的一笔赎金以换取释放他的承诺。这笔赎金是黄金，要足足装满一间长22英尺、宽17英尺、高过8英尺的房间。另外还勒索两屋子的白银，装满另外两个小一些的房子。

印第安人没有办法，只好从全国各地运送黄金白银。最终，印第安人在奉送了富可敌国、价值数亿黄金白银之后，仍然没有换来国王的一条命。阿塔瓦尔帕惨被撕票，死于绞刑。

国王死后，印加帝国很快就陷入了分裂与混乱……不到一年的功夫，印加帝国这个拥有600万人口的王国就基本灭亡了，沦为了西班牙殖民地，大量印加史料和文明失传；许多珍贵的文明遗迹被毁；印加帝国人口竟从600万下降到不足50万……

印加帝国之所以突然崩塌，不得不说，国王被俘虏，沦为勒索筹码，是最大的转折点。

史上额度最大、最不讲信义、危害最大的勒索事件，印加国王被绑架勒索事件应属第一。

在不讲信义、恃强凌弱的古代，通过勒索人质索取钱财的事件，屡见不鲜。而在现代，随着治安水平提高，现实世界中绑架勒索的事件，越来越少了，但是在虚拟的数字世界中，勒索攻击的事件，却此起彼伏，呈现暴增趋势。

2017年席卷全球100多个国家的“永恒之蓝”，让大众领教到了勒索攻击的威力。近年来，各种勒索攻击有增无减。5月23日，Verizon发布的Verizon Business 2022数据泄露调查报告（DBIR）显示，勒索软件在2022年同比增长13%，增幅超过过去五年的总和。仅以2022年上半年来说，就有多起影响或损失重大的勒索事件。

1月5日，美国新墨西哥州伯纳利洛县政府遭到勒索软件攻击，多个城市的政府大楼和公共办公室关闭；

2月23日，英伟达（Nvidia）遭Lapsus$组织攻击，涉及1TB机密数据泄露；

3月1日，丰田汽车供应商遭勒索攻击，14家本土工厂暂时关闭；

3 月 21 日 , 征信巨头 TransUnion 数据泄露，对 90% 南非人造成影响；

4 月 22 日，里约财政系统遭勒索攻击，420GB 数据被盗；

5 月 2 日 , 印度航空公司 SpiceJet 遭勒索软件攻击，导致乘客滞留机场；

5 月 8 日，哥斯达黎加政府因勒索攻击宣布进入“国家紧急状态”；

5 月 11 日，意大利多个重要政府网站遭 DDoS 攻击致瘫痪；

6 月 25 日，美国出版业巨头 Macmillan 遭勒索软件攻击后关闭系统；

8 月 29 日 , 用友畅捷通等管理软件遭勒索软件攻击，中毒终端数量达数千台。

……

奇安信集团董事长齐向东曾指出，当前，勒索攻击成为“流行病”：2020 年，勒索软件的平均赎金已高达 31 万美元；2021 年，预计每 11 秒将发生一次勒索攻击，全年超过 300 万次。零售、通信、能源、食品、工业等诸多行业均未能幸免。

然而这些数字只是冰山一角，九成以上的企业因为害怕对自己的品牌造成伤害，都在支付赎金以后选择了静默。

支付了巨额赎金，就能够息事宁人、花钱买平安么？答案当然是 No！

根据市场调查机构 Censuswide 公布的最新数据，大约 80% 选择支付赎金的组织会遭到第二次攻击，其中 46% 被认为是来自同一个团伙。一家在遭遇勒索软件事件后支付了数百万美元的公司，在交出加密货币后的两周内，又被同一黑客攻击了。

而且，即使受害者支付了赎金以重新获得其加密文件的访问权，也经常会出现问题。有 46% 的支付者发现一些数据已被破坏；3% 的人根本没有拿回他们的数据。

这 3% 的人，和印加帝国国王的命运一样，赔付了真金白银，却只换来一个寂寞。

事实证明，中招的客户，大多和印加帝国国王犯过类似错误。

事前：安全意识薄弱

害人之心不可有，防人之心不可无。当初，印加帝国国王对西班牙人完全没有戒备心，没有做好相应的安全防护，导致被轻松俘虏。当一家企业的网络安全意识不足，平时不注重防范，勒索攻击基本就是每击必中。

事中：技术实力不足

印加帝国国王带领的 5000 人，都手无寸铁或兵器简陋，在 180 个西班牙人面前可以说是战五渣，实力悬殊，导致整个过程非常被动。

如果企业仅是精神上重视网络安全，但技术跟不上，缺乏专业团队和专业安全运营，依然会被轻松勒索。

事后：应急响应措施跟不上

当国王被抓获之后，该如何止损，避免完全被动的任人宰割？是否应该设立临时国王（类似于明朝皇帝朱祁镇被瓦剌俘获后，临时立的皇帝朱祁钰），启动备份，主持大局。

同样，勒索发生之后，如果能借助专业团队，自己解密文件，而不是单纯缴纳赎金，势必就能避免损失。

对此，奇安信给出了针对勒索攻击的应对之道。

事前，建立“一中心两体系”的内生安全。

其中态势感知与管控中心是监管、运营、攻防态势的三合一，确保安全能力行之有效；安全防护体系是安全能力的落地，与态势感知和管控中心有效协同；由零信任机制提供的动态授信体系，在用户的整个网络活动过程中不断检查凭证，以此帮助企业实现对安全系统的动态掌控。

在这个环节，集传感器、文件威胁鉴定器、分析中心、威胁情报等于一体的奇安信天眼（新一代安全感知系统），可以兼任哨兵和指挥员的角色。它通过 APT 威胁检测、未知威胁检测、恶意文件检测、威胁情报联动等功能，

提前发现勒索病毒样本及 APT 投递途径，及早发现异常攻击行为，联动椒图云锁、天擎、防火墙等快速响应处置勒索病毒攻击。

事中，需建立起安全运营和应急响应机制。

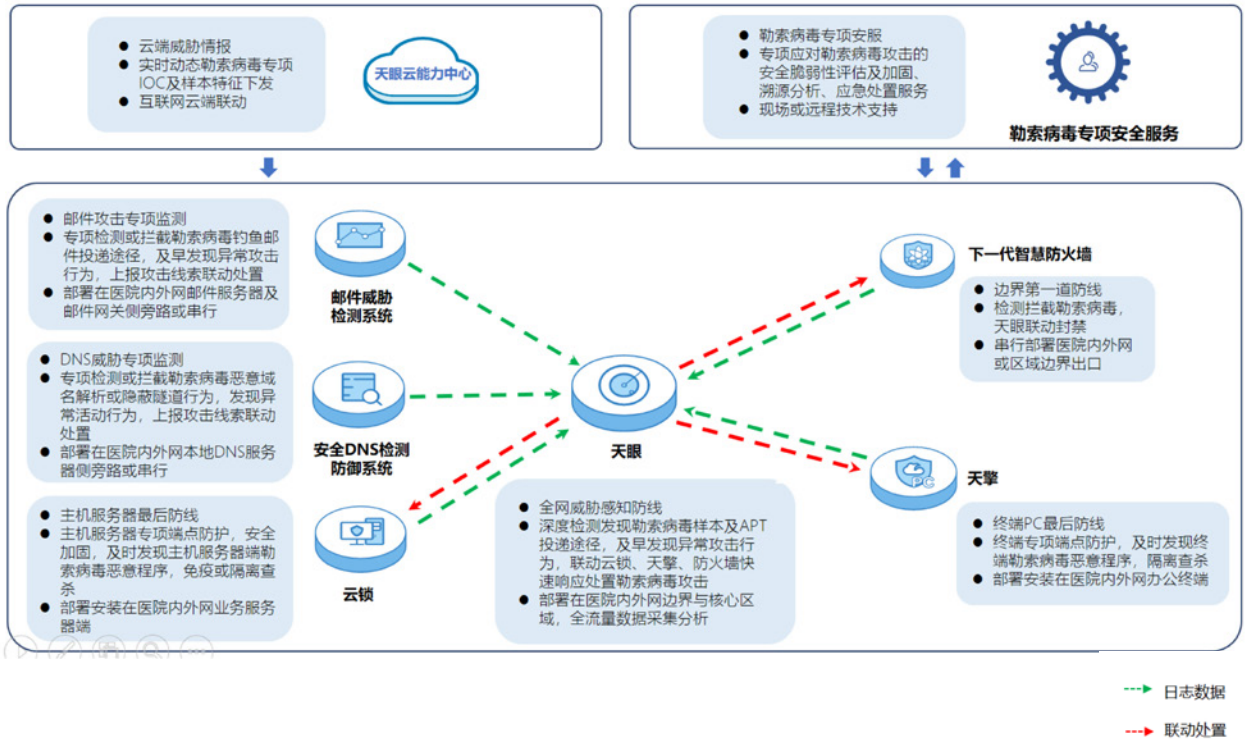
首先，要重视以网络资产为核心的系统安全建设，做好资配漏补的运营；其次，应通过恶意程序落地前的 4 重主动防御和恶意程序落地后的 3 重处置手段，做好“4+3”防护技术运营；当发现勒索病毒，说明服务器已经失陷，危害已经发生，可通过奇安信椒图服务器安全管理系统，从“病毒投放 – 病毒执行 – 横向扩散”的攻击链层层切断勒索病毒的传播途径。

事后，一旦不幸“中招”，也应及时采取事后补救。

奇安信勒索病毒搜索引擎支持解密 100 多种勒索病毒，且解密能力持续更新，可快速解密被感染的文件；同时，要尽快采取网络安全加固措施，如加强网络安全隐患修补、更新网络安全管理措施等；更重要的是，需要加强人员安全意识培训。

结束语：

“在绝对实力面前，任何计谋都是无效的。”正如齐向东预测的，“勒索攻击将与数字世界长期共存，企业要抵御勒索攻击流行病”。唯一的方法，不是妥协退让、破财消灾，而是应该练好内功，建立完整的网络安全体系，将勒索攻击威胁拒之门外。安



图：奇安信勒索病毒应对方案

大事记

齐向东出席算力产业大会：以“零信任”为基础支撑“东数西算”安全发展

9 月 15 日，由宁夏回族自治区人民政府主办，以“数聚宁夏 · 算领未来”为主题的首届“西部数谷”算力产业大会在银川开幕。奇安信集团董事长齐向东表示，在算力就是核心生产力的数字时代，算力基础设施的网络安全防御水平亟需全面提升，建立以“零信任”为基础的集约化大数据中心安全体系，可以有效降低被攻击的风险，解决我国“东数西算”10 大数据中心集群与 8 大算力枢纽面临的数据安全防护难题。

亮相世界智能网联汽车大会：以“零事故”为目标 构建安全的车联网

车联网提速发展，车联网安全边界进一步扩大。要以“零事故”为目标，护航智能网联汽车发展。9 月 16 日，2022 世界智能网联汽车大会上，奇安信集团副总裁孔德亮在主题演讲时表示，保障智能网联汽车发展安全，应做到“行驶不出事、数据不泄露、合规不踩线”。

围绕车联网云、路、网、车的不同层面，奇安信已开展大量研究和安全实践。本次大会上，奇安信也展出了车联网态势感知与应急响应平台、车联网安全合规检测一体化集成柜、车路协同安全“哨兵”、汽车信息安全靶场等多个安全产品和解决方案。其中，“智能网联汽车态势感知与应急响应平台”是首次正式对外展示。

国内首款流量解密编排器在京发布

9 月 13 日，奇安信集团在京举办流量解密编排器新品发布会。在发布会上，奇安信集团董事长齐向东表示，奇安信基于鲲鹏平台的高效研发能力，正式发布国内首款集高性能解密和智能编排技术于一体的边界安全新品——流量解密编排器，解决 DT 时代客户面临的加密攻击威胁，以及对弹性部署架构和动态扩容能力的需求。

奇安信集团副总裁、首席架构师兼边界安全 BG 负责人吴亚东介绍，该产品具备高性能解密、一次解密多

次检测、智能策略引流、安全能力资源池化等四大优势，已经在 2022 北京冬奥网络安全保障及国家级实战攻防演习中，获得了很好的实战验证，并为北京冬奥网络安全保障“零事故”立下了汗马功劳。

奇安信亮相 30 省 50 城市国家网络安全宣传周

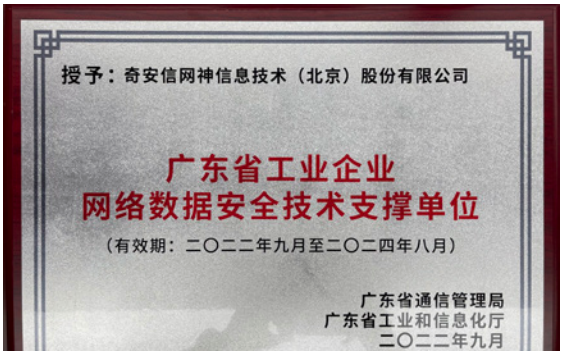
9 月 5 日至 11 日，以“共建网络安全，共享网络文明”为主题的 2022 年国家网络安全宣传周在全国范围广泛开展，奇安信充分发挥网络安全行业领军企业的社会责任，面向网信、教育、交通、卫生、传媒、通信等十多个行业的不同人群进行网络安全宣传推广，深入全国近 30 个省市自治区、50 余个城市，共筑网络安全防线。

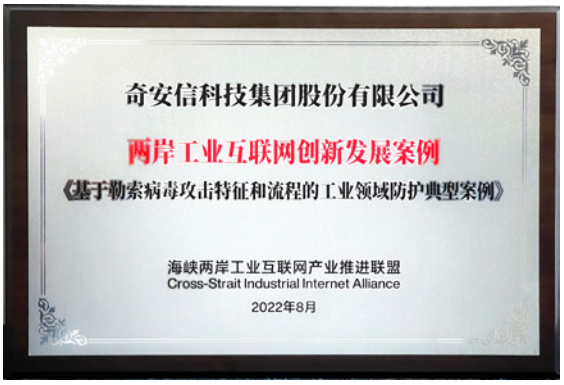
在重庆网络安全高峰论坛上，奇安信集团总裁吴云坤表示，数字化时代，网络安全不再是可选项，而是企业生存和发展的基础和前提，“零事故”应该成为数字化保障安全体系建设新目标。

在河南网络安全宣传周主论坛上，奇安信集团副总裁韩永刚分享了数字化时代网络安全趋势研判、保障与监管思路。他表示，应构建“网络安全保障与网空对抗”的双体系，在“双体系”间形成协同与帮扶，支撑关基保护与有效的网络空间安全监管治理。

在 2022 年国家网络安全宣传周汽车数据安全论坛上，奇安信集团副总裁孔德亮表示，针对智能网联车的网络安全和数据安全问题，“补短板”是当务之急。

网安周期间，奇安信集团获评北京市委网信办网络安全技术支撑单位；2021~2022 年度重庆市网络安全优质服务企业；广东省工业企业网络数据安全技术支撑单位；奇安信“基于勒索病毒攻击特征和流程的工业领域防护典型案例”，入选了 2022 年《两岸工业互联网创新发展案例集》。





奇安信盘古石电子取证系统获 2022 网络安全优秀创新成果大赛二等奖，入选首届法律科技成果案例，并入编由中国互联网协会、中国政法大学指导，中国政法大学数据法治实验室和《互联网天地》杂志社共同编制的《法律科技成果案例选》。


获奖证书

奇安信科技集团股份有限公司：

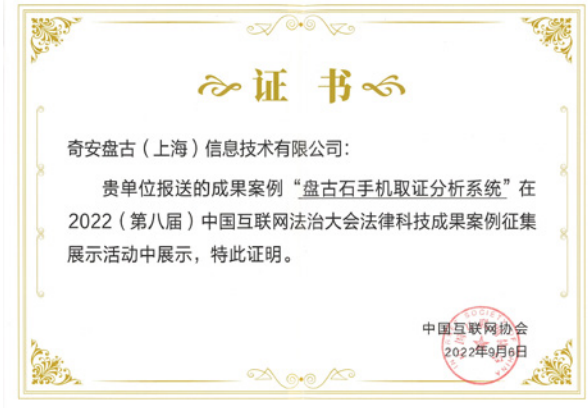
贵公司“盘古石手机取证分析系统”在2022年网络安全优秀创新成果大赛中荣获

二等奖

特发此证，以资鼓励。

中国网络安全产业联盟

2022年9月


证书

奇安盘古（上海）信息技术有限公司：

贵单位报送的成果案例“盘古石手机取证分析系统”在2022（第八届）中国互联网法治大会法律科技成果案例征集展示活动中展示，特此证明。

中国互联网协会

2022年9月6日

为更深入地分析网络安全威胁和人才情况，网安周期间，奇安信联合多家校企机构发布网安人才报告，首次提出了网络安全人才市场规模指数等多项创新指数，受到了监管机构领导、政企客户的高度关注；围绕企业邮箱安全性，奇安信联合 Coremail 发布了《2021 中国企业邮箱安全性研究报告》，指出了带毒邮件高速增长的发展趋势，为广大政企机构敲响了警钟。

聚势赋能 奇安信集团投资生态大会举行

9 月 15 日，奇安信集团投资生态共创汇暨创企成长导师团成立仪式，在奇安信安全中心举行。30 余家网络安全创业公司的高管 50 余人齐聚安全中心多功能厅，参加本次活动。

本次活动充分利用外部资源，整合协同集团优势，邀请集团内外部产业专家和专业投资人成立导师团，提供业务、采购、渠道、产品、融资、内控、财务、法务、税务等专业技能辅导和赋能。为奇安信投资生态圈的各家企业在发展的不同阶段提供帮助，建立良性、健康的泛网络安全生态圈，协助网安创业企业发展壮大。

吴云坤出席金砖国家数字经济对话会

9 月 8 日，金砖国家数字经济对话会在厦门举行。奇安信集团总裁吴云坤表示，随着数字化的深入发展，网络安全在全球范围内面临的挑战不断升级，金砖国家也发生多起重大网络安全实践，“零事故”应该成为数字化经济保障安全体系建设的新标准。

当前金砖国家都在大力发展具有各自国家特色的数字经济，对网络安全保障也有着强烈的需求。吴云坤表示，奇安信也希望与金砖国家共同交流合作，在中国方案基础上，形成基于“零事故”标准的“金砖国家方案”，保障金砖国家数字经济发展。

奇安信集团与东方通达成战略合作 共同构筑安全生态合作圈

9 月 8 日上午，奇安信集团与东方通签署战略合作协议。双方将在解决方案、人才培养、商机拓展、市场宣传等方面开展深度合作。

此前，在 BCS2022 数字安全产业发展论坛上，奇安信与东方通及 20 余家生态伙伴共同发起成立“数字产业生态共同体”，共筑“安全基座”。 本次战略合作的达成将与东方通打造紧密型战略合作伙伴关系，结合各自业务优势，进行能力融合。共同联动产业上、下游构筑安全生态合作圈，协同安全产品等发展标杆客户，形成示范效应。

奇安信与麒麟软件举办合作交流高层座谈会

9 月 2 日，麒麟软件有限公司一行到访奇安信，参观了奇安信安全中心展厅、工控实验室、司法鉴定所及党建室后，双方围绕安全操作系统、浏览器、安全防护产品、市场活动联合推广，以及协助麒麟建设产品安全研制体系等方面的合作进行了会谈交流。

接下来，针对双方主要产品的融合、浏览器、培训认证、市场活动联合推广、操作系统的安全保障，以及协助麒麟打造产品安全研制体系和生产安全的防护业务等方向，双方将分别成立联合专项小组，由各业务负责人牵头联合推进。

奇安信城市网络安全运营总部在长沙揭牌

9 月 1 日，奇安信城市网络安全运营总部暨长沙研发中心在湖南湘江新区国家网络安全产业园区正式揭牌成

立。这标志着奇安信在华中地区最大研发中心，树立起了城市网络安全运营“长沙模式”的金字招牌。

2020 年，奇安信与长沙市政府合资成立奇安星城网络安全运营服务（长沙）有限公司，并由该公司运营国家网络安全产业园区（长沙）城市网络安全运营中心。目前，长沙城市网络安全运营中心的运行已经得到广泛认可，经权威机构评测，长沙的 2021 年城市数字化网络安全指数第六，位居全国前列，并入选 2022 年 IDC 亚太区智慧城市大奖（中国区），长沙城市安全运营中心荣获“IDC 中国 20 大杰出安全项目”。最新发布的星城——城市网络安全运行平台 2.0，已在长沙城市网络安全运营中心落地应用。

“关基条例一周年”专题研讨会成功举办

2022 年 9 月 1 日，《关键信息基础设施安全保护条例》正式实施一周年之际，由《中国信息安全》杂志社与奇安信虎符智库联合主办的“关基条例一周年”研讨会今日在奇安信安全中心举行。多位产、学、研领域一线专家、研究学者、科技企业等专业人士参加，一同围绕关基安全保护工作推进的相关问题进行沟通与交流。

供应链安全是本次会议的热点问题之一，多位嘉宾认为实现自主可控将成为保障我国关键基础设施的重要着力点，针对这项议题，嘉宾就如何提升供应链安全能力，应对高端产品或组件的垄断与断供、组件投毒等问题进行了探讨。此外，与会嘉宾还围绕国内外关基政策、等保实施、中美竞合面临的关基挑战等议题进行了沟通与交流，并分享了条例实施后的实践经验与推进中遇到的问题与发现。

齐向东出席 2022 互联网岳麓峰会：数据大集中要谨防“蚂蚁搬家式盗窃”

在 2022 互联网岳麓峰会上，奇安信集团董事长齐向东表示，应对数字技术带来的网络安全风险，要以“零事故”为目标，建设更加具有纵深防御能力的内生安全体系。

其中，相较于更易触发系统告警的集中式大规模数据泄露，“蚂蚁搬家式”的数据盗窃策略更需要增强防范。政企机构可通过联合作战、精准防护、深度运营构建的纵深防御的内生安全体系，能快速封堵攻击行为，确保对内、对外的业务不受影响，做到业务不中断、数据不出事、合规不踩线，实现网络安全和数据安全“零事故”。

荣誉墙

数据交易沙箱获 2022 年大数据产业发展试点示范项目

近日，工信部对外发布了 2022 年大数据产业发展试点示范项目名单，奇安信“基于数据沙箱技术的数据安全流通平台”项目成功入选。

据悉，本次申报围绕“数据要素市场培育试点示范”“大数据重点产品和服务试点示范”和“行业大数据应用试点示范”3 大领域 8 个重点方向，其中，“大数据重点产品和服务试点示范”领域共入选 48 个项目，安全项目仅有 4 个，本项目是其中之一。

领域二：大数据重点产品和服务试点示范（共 77 项）

方向四：大数据重点产品方向（48 项）

1	国家电网有限公司	基于能源大数据中心的电力看双碳大数据应用	国家电网有限公司
2	奇安信科技集团股份有限公司	基于数据沙箱技术的数据安全流通平台	北京市
3	中兴通讯股份有限公司	基于大数据技术的面向金融交易场景的数据库产品和应用	深圳市
4	浪潮软件股份有限公司	多源多模态医疗大数据全栈式智能管理平台	山东省
5	天津卓朗科技发展有限公司	基于“海量分布式存储与弹性高性能计算一体技术”的大数据平台开发及应用	天津市
6	智网安云（武汉）信息技术有限公司	网络安全大数据分析和响应平台	湖北省

奇安信天擎独家入选第二批 Windows 7 操作系统安全防护产品目录

9 月 8 日， 中国网络安全产业联盟（CCIA）公布了第二批《实践指南》标准的 Windows 7 操作系统安全加固防护产品目录。经由第三方评测机构检测，奇安信天擎终端安全管理系统独家入选。


中国网络安全产业联盟
China Cybersecurity Industry Alliance

关于公布Windows 7操作系统安全防护产品目录（第2批）的通知

CCIA 秘〔2022〕055 号

各有关单位：

为有效应对 Windows 7 操作系统停止更新后带来的安全风险，中国网络安全产业联盟牵头编制发布了《网络安全标准实践指南—Windows 7 操作系统安全加固指引》（TC260-PG-20222A），为便于用户选择 Windows 7 操作系统安全防护产品，现将经第三方测评机构检测，符合《网络安全标准实践指南—Windows 7 操作系统安全加固指引》的 Windows 7 操作系统安全防护产品目录（第 2 批）公布如下：

序号	产品名称	版本号	生产厂家
1	奇安信天擎终端安全管理系统	V10.0	奇安信网神信息技术（北京）股份有限公司

作为网络安全行业的领军企业，针对用户关心的 Win7 停服后所面临的安全问题，奇安信在停服前就已立足 Win7 客户升级、过渡、切换三大应对场景和安全运营的长效机制，提供了系统性的综合解决方案，帮助客户顺利升级、安全过渡和平稳切换。

其中，奇安信天擎终端安全管理系统的“停服系统加固”模块，主要解决系统停服后的漏洞利用攻击防护问题，防止针对系统 RCE、浏览器、Office 等应用的漏洞利用攻击。

奇安信入选工信部大中小型企业融通创新典型模式案例集

9 月 8 日，工信部、国资委、工商联正式发布大中小企业融通创新典型模式案例集，奇安信集团入选“生态圈融通模式”。

2020 年，奇安信成功上市，在强化自身网络安全行业领军地位的同时，还充分利用当前网络安全行业的良好发展环境和政策支持，通过建立资本赋能平台，努力扶持优质中小型被投企业公司快速成长，支持其对外融资和资本运作。

在 BCS2022 大湾区网络安全峰会上，奇安信集团董事长齐向东表示，作为行业的龙头企业，奇安信将持续贡献新技术、新产品、新方案，夯实网络安全底座，并实现资源共享，加速开拓网络安全市场，拥抱千亿级蓝海机遇。协同上下游企业，打造合作共赢的生态，开辟产业发展新局面。

融通模式	案例名称	案例单位
生态圈融通	立体赋能 深度耦合 共建智能互联产业生态	小米科技有限责任公司
	多维融合铸生态 以链促转强优势	仪征经济开发区
	立足八大赋能体系打造“枝繁叶茂”的网安全景生态	奇安信科技集团股份有限公司
供应链融通	组建工程机械“同盟军” 聚力强链共进退	徐州经济技术开发区
	发挥引领作用 构建“整零”协同网络	中国兵器装备集团有限公司
创新耦合融通	全链协同共破技术难题 集中发力加速产业创新升级	维信诺科技股份有限公司
	链接全球 川流入海 构建“热带雨林”融通创新生态	海尔集团

奇安信通过信通院 CWPP 云工作负载保护平台能力评估

近日，奇安信网神云锁服务器安全管理系统（简称：椒图）在主机安全能力、容器安全能力、微隔离能力方面顺利通过中国泰尔实验室的评测，获得了由中国信息通信研究院颁发的“云工作负载保护平台能力检测证书”。


TRUSTED SECURITY
可信安全
CAICT 中国信通院
证书编号：IY2022750854
报告编号：V22Y75854
云工作负载保护平台能力检验证书
奇安信网神信息技术（北京）股份有限公司
北京市西城区西直门外南路 26 号院 1 号楼
奇安信网神云锁服务器安全管理系统
产品型号：V8.0
符合性描述：“经中国信息通信研究院的评估，贵单位的奇安信网神云锁服务器安全管理系统产品通过了 Q/KXY CS023—2022《云工作负载保护平台能力要求》的检验，达到主机安全能力、容器安全能力、微隔离能力要求，特发此证。”
【由于该检验是针对测试日期前产品情况进行核算，用户依然应留意在具体使用过程中可能发生的风险。因技术快速发展，产品/服务不断升级迭代，标准规范修订更新等原因，当产品或检验标准有较大变化时，建议进行重新检验。中国信通院将在 2023 年 8 月组织新一轮检验。】
云计算开源产业联盟
中国泰尔实验室
中国信息通信研究院
授权签字人：
2022 年 8 月 30 日
扫码查询证书

近年来，椒图在 CWPP 领域屡获殊荣，根据 IDC《中国云工作负载安全市场份额，2021：云原生与安全左移驱动技术持续创新》报告，奇安信以 17.2% 的市场份额位列中国第一；赛迪《中国服务器安全市场研究报告（2022）》，奇安信椒图的市场地位、发展潜力和部署总量均为中国第一，已经成为 CWPP 领域名副其实的领跑者。

“极盾 -2021”推荐名录出炉 奇安信 7 款产品上榜

近日，首届“极盾”众测活动（“极盾 -2021”）推荐名录正式发布，奇安信集团工业互联网安全领域 7 款产品通过审核及测试，被收录在网络安全软硬件产品推荐名录。目前，该名录已被收入《极盾专刊 -2021》，可通过“国家先进技术转化应用公共服务平台”查看详细介绍。

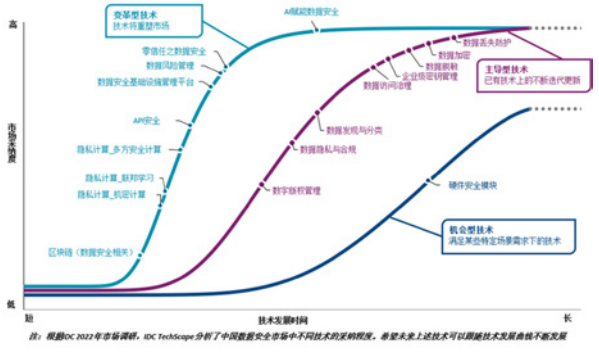
奇安信安全专家介绍，基于多年来在大数据、威胁情报、漏洞、安全攻防、态势感知等方面的突出优势，奇安信已构建了层次清晰、定位明确、融合联动的工业互联网安全产品体系和解决方案，并成功应用于能源电力、轨道交通、智能制造、钢铁、水务等垂直行业，打造了多个行业标杆案例。

极盾-2021推荐名录（排名不分先后）	
1	蓝海星主机管理系统
2	奇安信网神工业控制安全网关系统
3	奇安信网神工业安全隔离与信息交换系统
4	奇安信网神工业主机安全防护系统
5	奇安信网神工业安全监测系统
6	奇安信网神工业安全审计系统
7	奇安信网神工业入侵检测系统
8	奇安信网神工业安全管理与分析系统
9	长扬科技工控主机卫士
10	长扬科技工业防火墙

奇安信获评数据访问、隐私合规两项领域推荐厂商

IT 市场研究和咨询公司 IDC 发布《IDC TechScape: 中国数据安全技术发展路线图，2022》，根据技术的市场影响及各技术的发展阶段，将技术分为变革型技术、主导型技术及机会型技术三大类别。

其中，奇安信在主导型技术的数据访问治理和数据隐私与合规两个细分维度被列为推荐厂商。



注：根据IDC 2022年市场调研，IDC TechScape分析了中国数据安全市场中不同技术的关键程度。希望未来上述技术可以跟随技术发展曲线不断发展

奇安信集团总裁吴云坤获 CSO 名人堂中国安全十大人物

8 月 26 日，2022 CSO 全球网络安全峰会首次落地中国，并评选出中国安全十大人物（CSO 名人堂），以表彰本年度为中国网络安全市场做出重大贡献的十大杰出人物，奇安信集团总裁吴云坤入选。

据悉，本次中国安全十大人物（CSO 名人堂）是 IDG/IDC 在中国区首次公开征集网络安全领域的权威奖项，未来将成为 IDG/IDC 全球网络安全奖项的重要组成部分，并将设置为终身荣誉制。

奇安信荣获 2021 年度北京市科学技术奖一、二等奖

近日，2021 年度北京市科学技术奖评审结果正式公布。奇安信集团荣获一等奖 1 项、二等奖 2 项，成为获得 2021 年度北京市科学技术进步奖数量最多的网络安全企业。

其中，奇安信参与的“移动应用黑灰产溯源技术及应用”项目获科技进步一等奖，奇安信参与的“大规模数据安全深度检测识别关键技术与应用”和“知识驱动的高级复杂网络威胁发现及时空关联推理技术与应用”2 个项目获科技进步二等奖。

奇安信 Q-SASE、零信任获信通院年度奖项

8 月 25 日，由中国通信标准化协会算网融合产业及标准推进委员会（CCSA TC621）、中国信息通信研究院共同主办的“2022 年算网融合产业发展峰会”上，奇安信集团申报的 2 个案例，“中国电子基于 SD-WAN 的 SASE 落地与服务化实践”与“基于 PKS 的大数据环境零信任动态授权体系”，成功分获 2021 年度“SASE 优秀方案”和“零信任最佳方案”两大奖项。

奇安信
新一代网络安全领军者

聚焦安全运营，构建智能平台

奇安信网神态势感知与安全运营平台（简称NGSOC）以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，帮助政企客户持续监测网络安全态势，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置的安全运营工具。

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

国内首款具备分布式关联分析能力的安全运营平台，提供多元异构数据关联分析、灵活威胁建模、丰富的告警上下文信息展示及分布式横向扩展能力，已获得数十个相关专利。

将平战结合进行落地

演练态势监测攻防演练中防守方管理信息、系统建设、威胁运营等信息的总体状况，平战结合，全面提升安全防御能力。

重大安全事件的威胁预警

当出现重大网络安全事件时，帮助用户第一时间掌握是否遭受到攻击？首个被攻击的资产？影响部门？影响面趋势？事件处置情况？

专业的安全运营服务

奇安信集团具有专职产品运营服务团队，可提供原厂一线驻场、二线分析、运营方案咨询及培训服务，帮助客户解决无人运营困难。

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证
态势感知解决方案市场领导者——IDC认证
态势感知技术创新力和市场执行力双第一 ——数世咨询认证

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

网络安全 中国代表队 | 奇安信

2022年北京冬奥会胜利闭幕

“零事故”

奇安信圆满完成冬奥会网络安全保障任务

奇安信蝉联“中国网安产业竞争力50强”第一名

6月23日，中国网络安全产业联盟（CCIA）
揭晓“2022年中国网安产业竞争力50强”榜单。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信蝉联第一名。

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	深信服科技股份有限公司
3	启明星辰信息技术集团股份有限公司
4	天融信科技集团股份有限公司
5	华为技术有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	阿里云计算有限公司
9	新华三技术有限公司
10	杭州安恒信息技术股份有限公司
11	360政企安全集团
12	亚信安全科技股份有限公司
13	成都卫士通信息产业股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司