SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

奇安信品牌代言人
速度滑冰世界冠军
宁忠岩

奇安信品牌代言人
单板滑雪世界冠军
蔡雪桐

P23

奇安信品牌代言人

第7期
2021年7月

规划快一步

奇安信 | BEIJING 2022

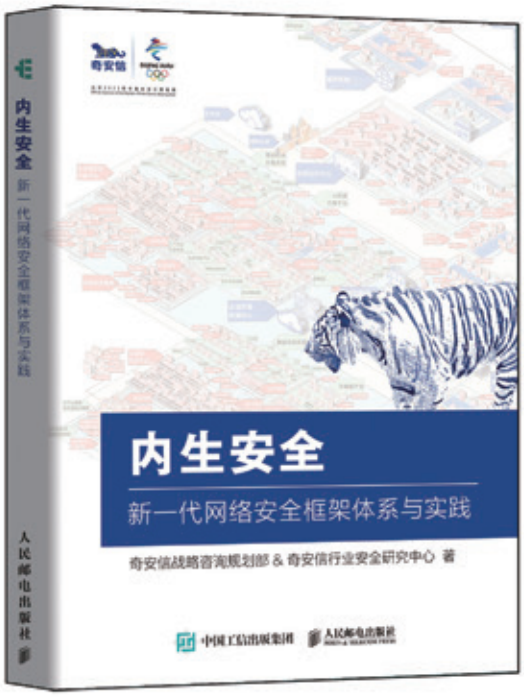
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

新书发布

内生安全权威解读

19支团队、37位专家倾力打造

政企“十四五”网络安全规划必读书籍



- 什么是内生安全
- 内生安全从何而来
- 为什么要内生安全
- 内生安全如何落地
- 新一代网络安全框架
- “十工五任”建设要点

扫描二维码
专享内购价

全球网络安全，倾听北京声音

眼下，第32届夏季奥运会正在东京举办。再过七个月，北京将敞开怀抱，迎来2022年冬奥运会和冬残奥会。届时，全球目光将汇聚在北京。

奥运是世界的奥运，网络空间是全球的空间。奥运会的圆满举办是全人类的共同愿望，确保全球网络空间的和平与稳定是我们网络安全工作者的共同使命。

去年新冠疫情的爆发，按下了全球数字化转型的加速键，带来了更为严峻的网络安全威胁。今年7月，瑞士远程IT管理软件服务商Kaseya被勒索，导致800多家零售门店被迫停业；6月，美国多家电视台遭勒索攻击，导致直播被中断；全球最大肉类加工企业JBS，因为网络攻击停产；5月，美国最大燃油管道运营商遭勒索攻击，17个州和华盛顿特区采取紧急措施……网络攻击导致的“断零售”“断播”“断肉”“断油”，正在现实生活中真实上演。

维护全球网络空间的安全与稳定任重道远，需要凝聚各国政府、企业、社会组织和机构的智慧。北京是中国的北京，也是世界的北京。倾听北京声音，读懂中国，对推动全球网络空间治理、共建网络空间命运共同体至关重要。2019年，奇安信携手中国电子举办北京网络安全大会（BCS大会），就是希望通过世界级的网络安全产业交流平台，促进全球政、产、学、研、用各界的沟通与合作，推动网络安全产业向更宽领域、更深层次、更高质量发展。

BCS大会是国际的。过去两年，BCS邀请了900多位顶尖学者、业内专家和世界级白帽黑客，来自30多个国家、地区和组织，促进国际社会建立更多信任、开展更多合作。

BCS大会是开放的。两年来，我们一共举办了10多场大型国际峰会，100多场高水平论坛和特色活动。每一场都是知识的交流、思想的碰撞，为行业发展提供了更广阔的视角。

BCS大会是前沿的。我们聚焦网络安全前沿技术，探讨网络风险应对策略，共同推动全球网络空间健康发展。2019年我们提出内生安全，2020年提出“内生安全，从框架开始”。这两年，内生安全框架得到了业界广泛认同，并快速落地实施。

立足当下，放眼未来，数字化转型正在全面铺开。“让网络更安全，让世界更美好”一直是奇安信的初心和使命，我们将为此不断努力，凝聚网络安全行业创新合力，推动全球网络安全产业共赢发展。

“全球网络安全，倾听北京声音”，8月10日-8月12日，期待与您在国家会议中心相见！

BCS大会主席、奇安信集团董事长

CONTEN

目录

安全态势

P4 | 网络安全审查办公室对“滴滴出行”等互联网平台启动网络安全审查

P4 | 首个软件供应链勒索攻击：美国两个城镇离线，上千组织被袭击

P5 | 今年第三次了！ LinkedIn 6 亿用户资料被兜售

P5 | 伊朗国家铁路遭网络攻击，各地车站大屏传播虚假延误信息

P6 | SonicWall SRA/SMA SQL 注入漏洞安全预警

P6 | Apache Tomcat HTTP 请求走私漏洞预警

P7 | 国内攻防演习 6 月态势：哪些薄弱点最易被利用?

P10 | 工信部、网信办、公安部联合印发《网络产品安全漏洞管理规定》

P10 | 工信部发布《网络安全产业高质量发展三年行动计划 (2021-2023 年) (征求意见稿)》

P11 | 工信部发布《关于加强车联网（智能网联汽车）网络安全工作的通知（征求意见稿）》

P11 | 美国参议院推进政府供应链和中小学网络安全立法

P11 | 美国科罗拉多州颁布《科罗拉多州隐私法案》

P12 | 《网络安全审查办法（修订草案征求意见稿）》修订要点与影响分析

月度专题

P16

奥运网络安全：赛场背后的高手暗战

奥运会吸引全球攻击者的目光，奥运网络安全保卫战，注定是一场高手的较量。

P21

疫情之下东京奥运与黑客赛跑

P23

奇安信与冬奥的故事

TS

攻防一线

P26

攻击者每发动一次网络攻击，
身份信息就可能暴露亿点点

安全之道

P30

勒索攻击已成“流行病”
医院如何打造闭环式安全运营?

奇安信人

P36

他不仅是位“读书人”

第 7 期
《网安 26 号院》编辑部
主办 奇安信集团

总　　编　　辑：李建平
副　　总　　编：裴智勇
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
奇安资讯主编：陈　冲
安全意识主编：李建平

奇安信集团　虎符智库　安全内参

电子版请访问 www.qianxin.com 阅读或下载
索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

Email: 26hao@qianxin.com
地 址：北京市西城区西直门外南路 26 院 1 号
邮 编：100044
电 话：（010）13701388557
出版物准印证号：京内资准字 2021- L0058 号
印刷数量：45000 本
印刷单位：北京七彩虹印刷有限公司

奇安资讯

P42 | 齐向东：数字经济要做好红线意识和安全流动两篇文章
P42 | 教育行业合作伙伴大会召开 共建教育行业生态
P42 | “责任之星”——奇安信亮相中国互联网大会
P43 | 奇安信韩永刚：应基于数字化业务流转建立数据安全防护体系
P43 | 《网络产品安全漏洞管理规定》独家解读
P43 | 吴云坤：保护数据和应用安全是保障智能系统的关键
P44 | 资源占用降低 50% 奇安信安全防护软件冬奥版率先适配 Windows11
P44 | 构建网络安全第一道防线 奇安信发布“安全 DNS”公共服务 QDNS
P44 | 全面适配鸿蒙 OS 奇安信移动办公安全产品和解决方案护航政企客户
P45 | 奇安信发布云天眼 全力提升云上实战攻防安全感知能力
P45 | 北京市政协委员齐向东：做好数字化时代网络安全的守护者
P45 | 奇安信圆满完成“2021 建党 100 周年”网络安全保障工作
P46 | 奇安信成为重庆市网络安全应急支撑单位
P46 | 奇安信终端安全两项方案入选工信部“2020 年信息技术应用创新解决方案”

事件篇

滴滴出行、BOSS直聘等多家互联网平台接受网络安全审查，数据安全关乎国家安全；美国爆发首个软件供应链勒索攻击，上千组织被袭击；伊朗交通部门连续遭到网络攻击，各地车站大屏传播虚假延误信息，道路和城市发展部网络服务中断……

网络安全审查办公室对“滴滴出行”等互联网平台启动网络安全审查

2021年7月，国家网信办接连发布公告称，网络安全审查办公室在7月2日宣布对滴滴出行，7月5日宣布对运满满、货车帮、BOSS直聘等4家互联网平台启动网络安全审查，要求审核期间停止新用户注册，其中运满满、货车帮为满帮集团旗下的货运平台。据悉，上述审查对象均于6月在美国上市。中国信息安全研究院副院长左晓栋接受媒体采访时表示，“我认为这次审查主要关注的是，重要数据和公民个人信息的出境安全风险。”

首个软件供应链勒索攻击：美国两个城镇离线，上千组织被袭击

2021年7月，综合外媒消息，美国IT管理软件厂商Kaseya 7月2日披露，遭遇利用零日漏洞的复杂网络攻击，导致内网沦陷，旗下VSA平台的更新包被篡改为REvil勒索软件，由此引发下游多级上千家组织被袭击。受害者包括至少8家托管服务商及下游更多组织，直接导致瑞典最大零售连锁店Coop至少800家门店关门、美国两个城镇IT系统离线等。美国网络安全与基础设施安全局将其定性为“软件供应链勒索攻击”，攻击者为REvil勒索软件团伙。

石油巨头沙特阿美发生数据泄露：1TB数据在暗网兜售

据BleepingComputer 7月19日消息，有攻击者从国际石油巨头沙特阿美石油公司盗窃1TB敏感数据，开价500万美元在暗网上出售，并声称5000万美元可以获取这批数据的独占权。具体数据包括近1.5万名员工的个人信息、多个炼油厂内部系统项目文件、客户名单与合同等。沙特阿美将此次数据泄露归因于第三方承包商，并表示事件未对公司的日常运营造成影响。

厄瓜多尔国家电信遭勒索攻击，运营被迫中断

据BleepingComputer 7月17日消息，厄瓜多尔国内最大的电信运营商国家电信遭遇RansomEXX勒索软件攻击，业务运营、在线支付及客户支持全部陷入瘫痪，无法访问。勒索团伙宣称已经拿到190 GB数据，并在数据泄露页面上分享了部分文档截图，包括联系人列表、合同及支持日志等信息。国家电信则表示，客户数据非常安全，不存在泄露情况。RansomEXX勒索软件过去

曾经攻击过许多知名机构，包括巴西政府网络、美国得克萨斯州交通部、柯尼卡美能达等。

今年第三次了！ LinkedIn 6 亿用户资料被兜售

据cybernews 7月12日消息，黑客论坛有用户发帖，兜售6亿份LinkedIn用户的个人资料，包括姓名、性别、出生日期、所在地、工作经历、邮箱、电话号码、各社交平台账号等，疑似爬虫抓取泄露，销售价格暂未公开。这意味着短短4个月以来，社交巨头LinkedIn已经经历了三轮大规模用户个人资料恶意抓取泄露，规模均为数亿级别：5亿、7亿、6亿。LinkedIn此前回应称不属于数据泄露，拒绝将恶意抓取视为安全问题，但这令犯罪分子更加肆无忌惮，收集越来越多用户的数据。

伊朗国家铁路遭网络攻击，各地车站大屏传播虚假延误信息

据SecurityAffairs 7月10日消息，伊朗法尔斯通讯社报道，伊朗国家铁路7月9日遭遇网络攻击，攻击者在国内各地车站的显示屏上发布关于车次延误或取消的虚假信息，并留下疑似伊朗最高领导人的办公室电话，敦促旅客拨打查询信息；同一天稍早，伊朗各地火车突然爆发电子跟踪系统失灵；次日，伊朗道路和城市发展部的内部计算机系统遭到网络攻击，使得该部网站和旗下其他网站中断服务。近年来，伊朗曾多次发生网络基础设施遭破坏事件，凸显了网空对抗下关基设施抗风险能力的薄弱。

摩根士丹利遭遇供应链攻击，客户个人信息泄露

据BleepingComputer 7月8日消息，美国金融巨头摩根士丹利披露，攻击者通过入侵第三方供应商的Accellion FTA服务器，窃取了属于其客户的个人信息，导致数据泄露。为摩根士丹利旗下股权业务提供账户维护服务的第三方供应商Guidehouse，在今年1月因Accellion FTA漏洞被入侵，3月发现了这一情况，5月在发现对摩根士丹利客户有影响并通知对方。Accellion官方曾表示，有接近100家企业因Accellion FTA漏洞被入侵。

网络攻击“扰乱”了俄罗斯总统普京的年度直播连线

据SecurityWeek 6月30日消息，俄罗斯国营电信运营商Rossiya 24表示，当日午间普京总统在电视直播连线时，遭受了“强有力”网络攻击的冲击，各方通话多次遭遇连接问题。俄罗斯总统普京举行了2021年“视频直播连线”活动，实时回答民众的提问。在为期近四个小时的直播连线中，各方通话多次遭遇连接问题，从偏远地区发起的呼叫受影响尤其明显。一位来自西伯利亚西南部地区库兹巴斯的来电者就遇到通话连接问题。此前在普京总统的2019年“直播连线”现场，也遭遇了境外大规模网络攻击，但均被阻止。

东京奥运会筹备期间，日本奥委会曾遭到网络攻击

据NHK 6月25日消息，日本奥委会日前披露，2020年4月底，东京奥运会宣布延期举办约1个月后，日本奥委会遭到疑似勒索软件攻击，被迫暂停业务。秘书处约100台服务器中，大约70%可能感染病毒的服务器不得不被更换，耗费约3000万日元。日本奥委会表示没有证据表明内部信息泄露，未公布损失情况和共享信息，这引发了较大质疑。日本内阁官房长官加藤称，“有必要仔细研究当时的情况，以确定没有及时分享信息是否合适。”

漏洞篇

7月，知名防火墙厂商 SonicWall 旗下安全产品爆出 SQL 注入漏洞，可未授权窃取内部敏感信息；YAPI 接口管理平台远程代码执行零日漏洞已遭在野利用，国内较多知名互联网企业在使用；奇安信 CERT 研判发现，近期需重点关注 24 个高风险漏洞……

SonicWall SRA/SMA SQL注入漏洞安全预警

2021年7月15日，国家信息安全漏洞库（CNNVD）收到关于Sonicwall SRA/SMA SQL注入漏洞（CNNVD-202107-1057）情况的报送。成功利用漏洞的攻击者可在未授权的情况下窃取内部敏感账户信息，进而控制目标设备。SonicWall 旗下远程访问、移动访问产品多个版本均受到漏洞影响。目前，SonicWall 官方已发布版本更新修复了漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

Apache Tomcat HTTP 请求走私漏洞预警

2021 年 7 月 14 日，网络安全威胁和漏洞信息共享平台发布漏洞预警，Apache 官方发布漏洞通告，修复了 Tomcat 中的一个 HTTP 请求走私漏洞 (CVE-2021-33037)。攻击者可利用该漏洞导致 HTTP 请求走私。目前官方已发布安全版本修复该漏洞，建议受影响用户及时升级。Apache Tomcat 是美国阿帕奇基金会的一款轻量级 Web 应用服务器。

Philips Vue PACS 医学诊断系统多个安全漏洞预警

2021 年 7 月 14 日，飞利浦官方近日发布多个安全漏洞的公告，包括 Philips Vue PACS 安全漏洞（CVE-2021-33020）、Philips Vue PACS 加密问题漏洞（CVE-2021-33018）等。成功利用漏洞的攻击者可以对 Philips Vue PACS 医学诊断系统发送恶意请求、获取用户敏感信息，导致系统无法正常工作，最终控制目标系统。VUE 系列多款产品多个版本均受到漏洞影响。目前，飞利浦官方已经发布更新修复漏洞，建议用户尽快采取修补措施。

YAPI 开源接口管理平台远程代码执行零日漏洞预警

2021 年 7 月 8 日，网络安全威胁和漏洞信息共享平台发布漏洞预警，互联网披露了 YAPI 远程代码执行 0day 漏洞，该漏洞已遭在野利用，并正在扩散。攻击者可利用该漏洞实现远程代码执行。建议用户通过临时防护措施缓解该漏洞风险，以免遭受黑客攻击。YAPI 是国内某旅行网站研发的接口管理服务开源项目，目前被较多知名互联网企业所采用。

奇安信 CERT：近期需重点关注的 24 个高风险漏洞

2021 年 6 月，奇安信 CERT 监测到新增漏洞 2753 个。经人工研判，本月值得重点关注的漏洞共 78 个，其中高风险漏洞共 24 个，包括多个遭在野利用的 Windows 代码执行和提权漏洞、多个开源 Java 框架 Apache Dubbo漏洞等，超7成高风险漏洞可被远程利用。

（关注公众号“奇安信 CERT”，发送“202106”可查看 6 月需重点关注的漏洞完整清单）

对抗篇

国内攻防演习6月态势：哪些薄弱点最易被利用？

作者 奇安信安服团队

2021年6月，奇安信Z-TEAM团队共承接攻防演习服务67场，其中包括行业级攻防演习1场，省级攻防演习12场，地市级攻防演习20场，本单位自主攻防演习任务34场。

一、本月任务目标特点

本月攻防演习评估任务主要以省、地市级为主，涉及的目标业务以政务、金融为主，其中政务行业通用系统平台较多，可利用的漏洞通用性较强，且内网依然存在安全域未隔离、弱口令及口令复用等安全风险问题，主要表现在以下几个方面：

1、应用更新不及时导致较多历史漏洞

本月任务中发现，被攻陷目标互联网侧应用漏洞以历史漏洞为主，比如，外部应用中48个Shiro组件漏洞多为Shiro-550漏洞、21个Weblogic组件多为CVE-2020-2551漏洞、16个OA系统漏洞也多是因为没有及时升级更新造成的，这些漏洞在外网突破中均被成功利用，成为目标网络的重大安全威胁。

2、行业通用平台组件漏洞导致被通杀

主要表现在行业平台分布部署通用性较强，同一业务使用的平台大多相同，导致同一漏洞通杀的情况出现，以某省政务网络为例，其中一个业务系统，多个地市均使用同一平台，存在相同的Shiro反序列化漏洞，导致同一漏洞通杀的情况出现。

3、内网弱口令和口令复用安全隐患严重

本月任务中，75%的防守单位的业务内网存在弱口令和口令复用情况，导致安全部署形同虚设。其中，内部堡垒机、网管系统和域控多存在弱口令和口令复用的情况，致使业务内网的安全风险非常严重。

4、目标网络缺乏纵深防护机制

本月任务中，80%的目标网络普遍缺乏纵深防护，存在互联网侧服务器和核心内网之间没有逻辑隔离，内

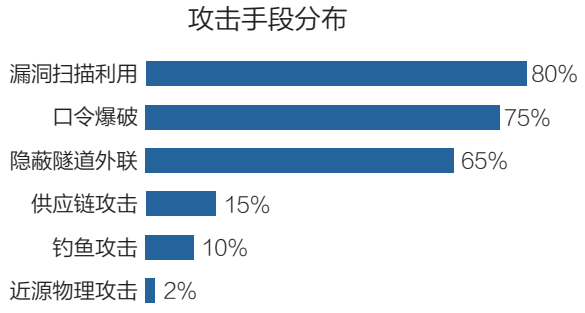
本月攻防演习成果：

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
攻陷数量	62	59	62	376	23	146	443	8036

部网络业务缺乏安全域划分、Vlan 隔离等措施，主要表现在从外网突破互联网侧应用后台服务器后，可直接对内网业务进行扫描探测，很容易实现对内网核心业务的横向渗透。

二、主要攻击手段分析

基于实战成果分析，由于目标网络互联网侧 OA 办公系统和业务应用较多，外网突破以此类漏洞利用为主，内网突破则以弱口令和漏洞利用为主。使用的主要攻击手段分布如下：



1、漏洞扫描利用

本月任务中，发现的漏洞主要集中在行业通用平台系统组件未授权访问、反序列化漏洞与敏感信息泄露，此类漏洞主要由内网防护策略不严导致未授权访问、对存在漏洞的系统组件更新不及时导致，直接反映出行业客户网络安全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。

2、隐蔽隧道外联

本月任务中，多数目标网络需要借助端口转发、隧道搭建等技术手段实现对内网的渗透拓展，以金融目标为例，网络安全域划分相对严格、核心业务隔离措施相对完善，所以突破过程中需要两到三层的隧道转发来实现对目标核心业务内网的横向渗透。

3、口令爆破

随着各行业业务人员网络安全意识逐步提升，互联网侧系统应用弱口令情况越来越少，但内网弱口令、口令复用等情况依然严重，本月任务中的弱口令或默认口令问题主要存在于内网，例如，某内网中就有超过 200

台的服务器使用了同一口令，导致这种情况的原因还是人员安全意识薄弱，对此类问题的危害严重性认识不足。

4、供应链攻击

本月任务中，供应链攻击以系统 Git 源码泄露为主，可从中获取外网重要账户名密码信息、内网数据库安全部署信息，且获取的信息可直接用于网络渗透，另有对泄露的 Git 源码进行代码审计发现系统漏洞，并通过漏洞利用实现管理员仿冒登录突破。

5、钓鱼攻击

钓鱼主要针对安全体系建设比较完善、防护相对严密，从外部很难直接突破的金融业务网络。钓鱼采用仿冒其内部人员，以交流业务为由套取关键认证信息，或以领导身份督查工作获取信任，以此打开网络突破口，从而进一步对目标网络进行渗透。内部钓鱼则以水坑攻击为主，重点在内部网络对网管、核心业务人员进行钓鱼突破。

6、近源物理攻击

本月任务中，针对某客户采取了近源攻击的方式，并取得了较好成果，攻击者利用假的工作证冒充内部工作人员进入目标办公区域，在办公区内利用暴露的公用主机直接对目标内网开展渗透攻击，充分暴露了目标单位对人员和终端设备安全管控能力不足导致的重大安全风险。

三、典型攻击手段的实现案例

1、外部漏洞利用突破

1) 多个地市政务类某系统统一开发的云平台存在 Shiro 反序列化漏洞，可被利用控制平台后台服务器；

2) 某机构 OA 系统存在文件上传漏洞，可被利用获取 OA 服务器管理权限和多个后台数据库权限；

3) 某目标在线点播系统存在 Struts2 漏洞，可被利用获取目标广播网服务器控制权限，直接突破逻辑内网隔离；

4) 某集团外网系统存在 0day 漏洞，可被利用反弹 Shell 获取系统控制权限；

5) 某职能部门视频网站大数据平台存在未授权访问漏洞，可直接控制多台大数据平台终端和数据节点；

6) 某单位目标业务内网，利用 ms17-010 漏洞一次扫描出近百台存在漏洞的Windows主机，均可利用拓展。

2、口令爆破

1) 某目标培训平台存在弱口令漏洞，可登录业务后台并进一步拓展控制平台服务器；

2) 某机构 sso 认证平台，通过口令复用可控制 22 个相关子系统；

3) 某职能部门内网华为 AR 路由器存在管理员弱口令，可控制 7 台 AR 路由器，实现跨网段拓展；

4) 某机构内部网络 SSH 弱口令，单个网段就有 40 余台 Linux 服务器为弱口令。

3、供应链攻击

1) 某目标业务系统 Github 源码泄露，直接从中获取管理认证信息，可进一步拓展利用；

2) 某目标 FMS 系统在外网发现 Gogs git 管理平台，利用 CVE-2018-18925 漏洞，伪造管理员 session 获取系统管理员权限；

3) 某目标系统 Github 源码泄露，从中获取多个专线网数据库账号密码、内网部署信息和开发人员信息，可用于进一步拓展。

4、钓鱼突破

1) 某企业的攻防演习中，经信息收集，确定某安全职能部门领导真实信息，通过利用领导照片修改微信头像冒充领导督查工作，获取关键业务系统账户名口令；

2) 某目标内网钓鱼管理员，在控制目标 ideal 系统后，通过 ideal 注册账号找到管理员邮箱，向该邮箱发送钓鱼邮件，成功上线管理员；

3) 某目标内部网络水坑钓鱼，通过修改已控的 Web 应用后台文件，加入 js 钓鱼代码，实现在内部人员点击访问时获取目标人员终端权限。

政策篇

国内，三部门联合印发《网络产品安全漏洞管理规定》，明确了网络产品漏洞各方参与者的责任和义务；工信部发布《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》，提出到2023年，网络安全产业规模超过2500亿元。

国际上，俄罗斯总统普京签署新版《国家安全战略》，将信息安全作为国家利益、战略性优先事项；NIST发布“总统行政令－关键软件”的定义、使用安全指南，为保障关键软件安全提供了指引。

工信部、网信办、公安部联合印发《网络产品安全漏洞管理规定》

2021年7月13日，工信部、网信办、公安部联合印发《网络产品安全漏洞管理规定》，将于9月1日起施行。《规定》旨在维护国家网络安全，保护网络产品和重要网络系统的安全稳定运行；规范漏洞发现、报告、修补和发布等行为，明确网络产品提供者、网络运营者，以及从事漏洞发现、收集、发布等活动的组织或个人等各类主体的责任和义务；鼓励各类主体发挥各自技术和机制优势开展漏洞发现、收集、发布等相关工作。

工信部发布《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》

2021年7月12日，工信部发布《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》，公开征集意见。《行动计划》提出，到2023年，网络安全产业规模超过2500亿元，年复合增长率超过15%。电信等重点行业网络安全投入占信息化投入比例达10%。一批网络安全关键核心技术实现突破，达到先进水平。进一步优化数据安全管理、分类分级安全防护等产品功能和性能，提升数据安全智能防护和管理水平。大力推进安全多方计算、联邦学习、可信计算等技术的研究攻关和部署应用，促进数据要素安全有序流动。

网信办发布《网络安全审查办法（修订草案征求意见稿）》

2021年7月10日，网信办会同有关部门修订了《网络安全审查办法（修订草案征求意见稿）》，公开征集意见。《修订草案》在网络安全审查工作机制成员单位增加了中国证监会；规范的行为在“关键基础设施运营者采购网络产品和服务”基础上，增加了“数据处理者开展数据处理活动”。《修订草案》还对赴国外上市公司作了特殊规定，要求掌握超过100万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查，且在申报材料中应提供拟提交的IPO材料。

中办、国办印发文件：压实境外上市公司信息安全主体责任

2021年7月6日，中共中央办公厅、国务院办公厅印发《关于依法从严打击证券违法活动的意见》。《意见》提出，加强跨境监管合作。要求完善数据安全、跨境数据流动、涉密信息管理等相关法律法规。抓紧修订关于加强在境外发行证券与上市相关保密和档案管理工作的规定，压实境外上市公司信息安全主体责任。加强跨境信息提供

机制与流程的规范管理。

工信部发布《关于加强车联网（智能网联汽车）网络安全工作的通知（征求意见稿）》

2021 年 6 月 23 日，工信部发布《关于加强车联网（智能网联汽车）网络安全工作的通知（征求意见稿）》，公开征集意见。文件指导基础电信企业、车联网运营企业、智能网联汽车生产企业加强车联网（智能网联汽车）网络安全管理工作，加快提升网络安全保障能力。内容包括加强车联网网络安全防护、加强平台安全防护、保障数据安全、强化安全漏洞管理四部分。

美国参议院推进政府供应链和中小学网络安全立法

据 MeriTalk 7 月 14 日消息，美国参议院国土安全与政府事务委员会批准了两项法案。《供应链安全培训法案》希望为负责服务及设备采购的联邦政府雇员提供一套网络培训计划，帮助他们识别可能对国家安全构成风险的产品。《K-12 网络安全法案》要求网络安全与基础设施安全局对中小学 (K-12) 面临的网络安全风险开展研究，并提出相应解决建议，发布一个供 K-12 学生使用的在线工具包。

美国科罗拉多州颁布《科罗拉多州隐私法案》

据 ZDNet 7 月 9 日消息，美国科罗拉多州州长签署颁布《科罗拉多州隐私法案》，使科罗拉多州成为继加利福尼亚州和弗吉尼亚州之后第三个颁布全面隐私立法的美国州，法案将于 2023 年 7 月 1 日生效。法案内容要点包括适用范围、消费者权利、数据处理者义务、法案执行 4 部分。该法案没有明确具体罚则，但违反《消费者权益保护法》的行为受该法案管辖，由此分析，针对违法企业单次罚款最高可达 20,000 美元。

NIST 发布“总统行政令 – 关键软件”使用安全指南

2021 年 7 月 8 日，美国国家标准与技术研究所（NIST）发布“总统行政令 – 关键软件”使用安全指南。该文件是总统行政令（E.O. 14028）的后续落地文件，聚焦关键软件使用环节的安全，给出了一系列的安全措施，包括应用最小权限、网络分段、正确配置等。此前 7 月 2 日，NIST 发布“总统行政令 – 关键软件”定义文件，对关键软件进行定义，并发布了初步的 11 类软件类型，包括 Web 浏览器、端点安全、网络控制、网络防护、远程扫描等。

俄罗斯总统普京签署新版《国家安全战略》

2021 年 7 月 2 日，俄罗斯总统普京签署命令，批准出台新版《国家安全战略》。《国家安全战略》是俄国家安全领域最高战略指导文件，上一版于 2015 年年底出台。新版《战略》包含总则、现代世界中的俄罗斯：趋势和机遇、国家利益和国家战略性优先事项、保障国家安全、战略实施的组织框架与机制 5 大部分。《战略》将信息安全作为国家利益、战略性优先事项，提出了 16 项任务加强俄罗斯在信息空间的主权。

政策解读

《网络安全审查办法（修订草案征求意见稿）》修订要点与影响分析

作者 虎符智库

在网络安全审查办公室宣布对滴滴出行等互联网平台实施网络安全审查数日后，国家互联网信息办公室在7月10日发布了《网络安全审查办法（修订草案征求意见稿）》（简称《征求意见稿》），结合刚刚颁布的《数据安全法》对《网络安全审查办法》（简称《审查办法》）的内容进行相应调整。

《征求意见稿》的多处修改均体现着对数据安全问题的高度重视。其主要修订要点如下：

- 增加《数据安全法》作为立法依据及处罚依据。
- 扩大网络安全审查范围，对于数据处理者开展数据处理活动，影响或可能影响国家安全的，纳入网络安全审查审查范围，落实《数据安全法》的数据安全审查制度。
- 新增网络安全审查适用情形，掌握超过100万用户个人信息的运营者赴国外上市，须申报网络安全审查。
- 网络安全审查重点从网络安全扩展至数据安全，增加对“核心数据、重要数据或大量个人信息”以及“关键信息基础设施”可能遭遇的数据安全风险因素的考量。
- 将中国证券监督管理委员会纳入网络安全审查工作组。
- 变更申报材料及审查时间，增补申报网络安全审查应提交的材料，特别审查程序由45个工作日延长为3个月。

下文对《征求意见稿》的主要变化与影响进行简要评述。

一、增加《数据安全法》作为法律依据

《网络安全审查办法》于2020年6月1日生效，这次修订有上位法发生变化的大背景，即我国《数据安全法》已经通过并即将于2021年9月1日生效。

《征求意见稿》第一条增加了《数据安全法》作为法律依据。根据即将生效的《数据安全法》相关规定，对原《网络安全审查办法》进行修订，增加了网络安全审查中需要根据《数据安全法》规定予以配套的内容。

因此，本次修订从根本上是为了落实《数据安全法》第二十四条“建立数据安全审查制度”的要求：“国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查”。

此外，《征求意见稿》第二十条增加了《数据安全法》作为处罚依据：“运营者违反本办法规定的，依照《网络安全法》《数据安全法》的规定处理”。

《数据安全法》将在 2021 年 9 月 1 日实施，《审查办法》的修订表明《数据安全法》进入实施前紧锣密鼓的准备阶段，法律中设立的重大制度将逐步通过法规和细则予以落实。

《网络安全法》与《数据安全法》通过不同角度立法，共同完善覆盖网络信息和数据领域，两者互相补充配合使用。

二、扩大网络安全审查的适用范围

（一）审查范围扩大至包括数据处理者

根据《网络安全法》和《审查办法》，网络安全审查制度审查的重点对象是关键信息基础设施运营者（CIIO）采购网络产品和服务（《审查办法》第二条），但相关监管部门可以依职权将其认为有可能影响国家安全的网络产品和服务纳入审查（《审查办法》第十五条）。

在《审查办法》基础上，《征求意见稿》第二条规定，扩大了适用网络安全审查的范围，明确将数据处理者（“运营者”）开展数据处理活动，影响或可能影响国家安全的，纳入了网络安全审查范围。

《征求意见稿》第二条规定：

- 关键信息基础设施运营者采购网络产品和服务。
- 数据处理者开展数据处理活动，影响或可能影响国家安全的，应当进行网络安全审查。

后者可涵盖的对象可能远远大于前者。根据《数据安全法》的规定，所谓数据处理包括数据的收集、存储、使用、加工、传输、提供、公开等。

（二）审查要点和标准从网络安全扩展至数据安全

《审查办法》主要针对 CIIO 采购特定网络产品和服务相关的供应链安全风险，而《征求意见稿》明确将《数据安全法》补充为立法依据，且将审查范围扩展至 CIIO、数据处理者数据处理活动以及赴国外上市相关的国家安全风险，特别是“核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险；国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险”。

“核心数据”和“重要数据”均系近期出台并将于 9 月 1 日正式实施的《数据安全法》提出的重要概念，目前均未界定其具体范畴。

（三）明确掌握 100 万用户个人信息的运营者赴国外上市的强制网络安全审查申报义务

《征求意见稿》第六条规定：掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办

公室申报网络安全审查。

这意味着，即使不属于非关键信息基础设施运营者的企业，如果处理个人信息达到规定的数量要求，其在赴国外上市前亦必须申报网络安全审查。

国家标准 GB/T 35273 - 2020《信息安全技术个人信息安全规范》中规定，企业在“处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息”应当设立专职的个人信息保护负责人和个人信息保护工作机构，《征求意见稿》似乎参考了此项个人信息数据标准。

此外，《征求意见稿》中使用的是“掌握”而非《数据安全法》《个人信息保护法（草案）》（第二次审议稿）中的“处理”概念，可解释范围更广。

根据第六条的规定，仅“赴国外上市”的行为触发强制的网络安全审查。从文义解释的角度看，由于香港和澳门特别行政区不属于“国外”的范围，拟赴香港上市的企业应不会受到本条的限制。

三、增加证监会作为网络安全审查的成员单位

为应对新增的审查范围，《征求意见稿》明确将证监会纳入中央网络安全和信息化委员会领导网络安全审查工作机制的范畴，与此前的网信办等十二部委联合开展审查。

就在数日前，中共中央办公厅、国务院办公厅印发了《关于依法从严打击证券违法活动的意见》（“简称《意见》”），明确提出“完善数据安全、跨境数据流动、涉密信息管理等相关法律法规”“压实境外上市公司信息安全主体责任”“加强跨境信息提供机制与流程的规范管理”的工作要求。

《征求意见稿》将证监会纳为工作机制成员单位，有助于证监会在贯彻落实《意见》的过程中发现影响或可能影响国家安全的国外上市行为，并根据《征求意见稿》第十六条的规定，依职权主动申请发起网络安全审查。

全球主要国家上市的信息披露和合规要求各有不同，但都有通过行政执法、投资者发起证券民事诉讼，甚至刑事追责等手段，强制上市企业必须强调真实、完整、准确披露拟上市公司的信息。

高科技企业掌握的科技数据、用户数据、业务涉及的敏感数据，关系到所在国家的网络数据安全甚至是国家安全。对企业来说，如何平衡好上市信息披露等法律合规和监管要求与业务属地的业务合规与监管要求，是企业面临的重要课题。

四、新增审查要点

《征求意见稿》第十条进一步增加了网络安全审查中考虑的国家安全风险因素，即“（五）核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险”，以及“（六）国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险”。

《征求意见稿》第十条规定了网络安全审查重点评估采购活动、数据处理活动以及国外上市可能带来的国家安全风险，主要考虑以下因素（注：新增的考虑因素已经突出提示）：

- 产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏的风险；
- 产品和服务供应中断对关键信息基础设施业务连续性的危害；
- 产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；
- 产品和服务提供者遵守中国法律、行政法规、部门规章情况；
- 核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险；
- 国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险；
- 其他可能危害关键信息基础设施安全和国家数据安全的因素。

五、特别审查程序期限延长

总体而言，《征求意见稿》的审查流程总体沿用了现行《审查办法》确定的审查材料和审查流程，只是将在出现网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门意见不一致情况下，需征求有关部门意见并报中央网络安全和信息化委员会批准的特别审查流程期限由45个工作日延长至3个月，且情况复杂的仍可以延长。

无论是主动申报的审查，还是面临网络安全审查办公室依职权发起的审查，有关企业均应将3个月的期限考虑在内，以免实质性地影响商业计划的进程。

六、明确“重要通信产品”属于“网络产品和服务”

《征求意见稿》在“网络产品和服务”中新增了“重要通信产品”，但仍然没有对网络产品和服务的具体范围给出进一步的说明。

目前，网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。

由于网络安全审查工作办公室有权根据《征求意见稿》第十六条，直接对“影响或可能影响国家安全的”网络产品和服务，以及数据处理活动和国外上市行为启动审查，如某项网络产品和服务在行业属性上具备敏感性且已经或可能进入关键信息基础设施运营者的供应链体系，或者其数据处理规模较大、处理的数据性质较为敏感，将有可能被认为“影响或可能影响国家安全”而面临审查，同样值得企业关注。

七、相关建议

若企业相关业务涉及处理个人信息或核心数据、重要数据，特别是掌握了大量个人信息数据的基础互联网服务企业，应当重视网络安全审查的相关规定，应当按照《网络安全法》《数据安全法》以及未来出台的《个人信息保护法》等相关法律规定做好个人信息保护及数据安全、网络安全工作；同时，组织或委托专业机构对数据处理的合规性，特别是数据处理是否可能影响国家安全，抓紧开展自评估。

奥运网络安全：赛场背后的高手暗战

奥运会吸引全球攻击者的目光，奥运网络安全保卫战，
注定是一场高手的较量。

本文 由奇安信公关部 包世玉整理

2021 年 7 月 23 日，2020 东京奥运会正式开幕。开幕式规模由最初计划的 1 万人缩减为 950 人。已经推迟一年的东京奥运会仍面临新冠疫情反弹的严峻考验。

但这仅是东京奥运会的多重考验之一，其网络安全的“疫情”也不容忽视。

就在开幕前的 7 月 19 日，美国联邦调查局（FBI）发布警告称: 恶意攻击者很可能将矛头指向东京奥运会，发动分布式拒绝服务（DDoS）攻击、勒索软件攻击、社会工程、网络钓鱼活动或内部威胁等多种攻击。最终影响甚至中断奥运赛事直播，入侵 IT 系统、泄露和加密敏感数据，或者冲击支持奥运会运营的数字基础设施。

东京奥运会已多次遭遇网络安全威胁

东京奥运会之所以更吸引恶意攻击者的“关注”，是因为在新冠疫情的影响下，这是全球首届专门以数字平台或电视广播为载体的体育盛会。

网络威胁联盟 (CTA) 的首席分析官尼尔詹金斯曾警告说：“民族国家看到了攻击的机会。东京奥运会的网络威胁态势严峻，不容忽视。”

7 月 21 日，日本政府官员称奥运门票网站遭入侵，购票信息被泄露。在 2021 年 6 月的发布会中，日本奥委会透露，东京奥运会秘书处在 2020 年 4 月底曾受到了勒索攻击，导致秘书处的计算机和服务器感染病毒，服务器上存储的数据被改写，导致服务器暂时无法访问。在 100 台服务器中有约 70% 感染病毒，最后被迫更换，总耗费高约 3000 万日元。日本奥委会在遭到袭击后曾被黑客索要赎金。

然而，这仅是针对东京奥运会网络攻击的严重事件。

2019 年 12 月，日本东京奥运会组委会称，发现一组假冒奥运会和残奥会东京组织委员会的钓鱼电子邮件攻击活动。

2020 年 2 月，一家伪装成能购买东京奥运会门票的虚假倒卖网站出现，目的是为了窃取购票者信用卡信息。同月，黑客通过第三方平台入侵了奥运会官方推特账号和国际奥委会 (IOC) 媒体事务的推特账号。

2021 年 5 月，受到富士通安全事件的余波影响，东京奥运会组委会的大量相关人员信息遭到泄露。原本为应对 2021 年东京奥运会可能出现的网络攻击，日本国家网络安全中心曾召集约 170 位安全管理人员参与演习。在此次攻击后，其中约 90 个组织的参与者的姓名、职级与隶属关系，奥运会与残奥会组委会、日本各部委、东京与福岛县等赛事举办地当地政府及多家奥运会赞助商的个人信息均遭泄露。

日本设想为东京奥运会打造世界级智能城市的体验。因此，在筹备期间大力推进政务数字化，希望借此推动整个社会的数字化进程。分析人士称，推进过程的新旧交替反而暴露了大量薄弱面。日本曾在疫情期间出现大量的机构和个人数据泄露，再加上其薄弱的数字基础设

施，很容易被攻击方利用，成为潜在的攻击入口，对东京奥运会活动造成严重影响。

奥运已成网络攻击战场

作为世界最高级别的体育赛事，奥运会不仅世界瞩目，同时也备受全球黑客“关注”。进入新世纪以来，随着网络普及率及使用率的日渐增加，网络攻击也随之增多，黑客攻击手段也随之增强。

2010 年温哥华冬奥会 影响轻微病毒感染

2010 年加拿大温哥华冬奥会首次设立网络安全指导委员会，网络安全成为核心关注领域之一。

在奥运会期间，加拿大计算机事件响应中心收到过一系列攻击报告：乌克兰出现了假冒的温哥华组委会网站；奥林匹克主题的搜索引擎被毒化，将用户指向到发布恶意软件的网站。

整体威胁主要为钓鱼网站、搜索引擎毒化、病毒感染等恶意网络活动，并有许多轻微的病毒感染事件上报。

2012 年伦敦奥运会 未成功的大规模 DDoS 攻击

伦敦奥运会被誉为第一届数字奥运会。在智能手机时代背景下，随着 Wi-Fi 的使用和移动服务的增加，随之而来的网络攻击暴露面也在增加。

奥运会期间，出现了数项对运动会举办带来影响的网络安全事件。包括：开幕前，东欧黑客对伦敦奥运会的 IT 基础架构进行了约 10 分钟的漏洞扫描；开幕当日，奥林匹克场馆电力系统遭受了 40 分钟大规模 DDoS 攻击，但并未成功；此外，多家媒体机构曾遭到网络攻击，还发生了笔记本电脑盗窃、高价值 IT 和通信设备盗窃、病毒蠕虫感染等事件。

此次奥运会中，黑客主要瞄准了奥运会的 IT 基础架构、电力系统、媒体机构等进行了一系列攻击活动。

2016 年里约奥运会 APT 攻击窃取大量隐私数据

巴西一直被视为网络犯罪活动高发之地，智能时代背景下，网络使用率逐渐增加。

奥运会期间，APT28 组织对奥运会相关的反兴奋剂组织发起了攻击，获取并公开该组织账号、运动员测试结果、相关人员隐私等数据。与此同时，还发生了大量针对奥运会的邮件欺诈、网站篡改、网站仿冒、贩卖假门票、伪造 Wi-Fi 网络、勒索病毒等的网络安全事件。除此之外，针对奥运会相关网站、巴西和里约政府相关网站、赞助商相关网站的 DDoS 攻击，其流量曾高达 300 ~ 500Gbps。还有报告发现，有些虚假网站未经授权进行奥运会门票销售。

此次奥运会中主要出现了 APT 攻击泄密虚假网站、破坏性攻击、数据泄露，以及针对政府和赞助商网站的 DDoS 攻击等行为。

2018 年平昌冬奥会 世界级网络安全事故

相比起来，平昌冬奥会则没那么幸运，在其奥运会期间曾遭遇世界级的网络安全事故。网络、广播系统中断，官网瘫痪数小时直接导致观众无法进场，Wi-Fi 无法使用导致直播信号中断，媒体集体“失声”……

在奥运会开幕前，安全研究人员就发现有黑客盯上了平昌冬奥会，不少冬奥会相关组织经常收到恶意钓鱼邮件。随后在开幕式期间，种种混乱出现：互联网和广播系统中断；奥运会网站瘫痪数小时，导致门票销售和下载被中断，甚至有些观众无法打印出门票，导致很多人无法参加开幕式，场馆内出现大量空位；奥林匹克场馆周围的本地 Wi-Fi 短时无法使用，开幕式直播信号中断。

影响范围广，事件影响力大，平昌冬奥会可以说排在了历届受网络安全攻击事件的奥运会之首。

奥运网络攻击“逐届加剧，危害倍增”

在近几届奥运会中，黑客从未缺席。奥运会的网络安全威胁“规范化”，危机逐步累积，攻击矢量、数量、影响范围和威胁等级也不断上升，攻击态势也呈现“逐届加剧，危害倍增”的趋势，不少专家评价攻击目的或与地缘政治有关。

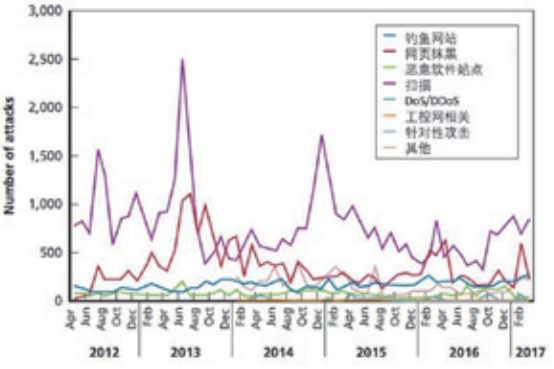
1、四大类威胁攻击影响奥运网络安全

目前分析看来，奥运会面临的威胁逐渐升级，攻击手法甚至逐渐“规范化”，目前主要的威胁攻击分为以下四大类：

- 针对性攻击：针对高价值奥运资产和个人或组织。
- DDoS 攻击：针对奥运会基础设施和网络。DDoS 的攻击者可以是国家黑客这样的高级攻击者，也可以是黑客独狼和技术爱好者。关注的重点是 DDoS 方法，以及基于物联网的僵尸网络。
- 勒索软件攻击：勒索软件攻击将影响甚至瘫痪大面积的设备、服务和基础设施，包括交通、会议电子设备和销售终端。
- 网络谣言与舆论误导：网络谣言和舆论操纵不但能给个人、组织和国家造成巨大声誉损失，甚至可能导致奥运会本身被中断。

根据日本计算机应急响应小组（JPCERT/CC）提供的 2012—1016 年网络威胁报告（上图）中可以看出，钓鱼网站呈现明显的上升势头。此外，JPCERT 的报告还指出，近年来，专门针对日本的针对性黑客攻击组织主要有三个：Daserf APT、Operation Dust Storm 和 Operation Quantum Entanglement，分别瞄准的是日本的电力、石油天然气、建筑、金融和交通等关键基础设施。

日本网络防御专家 Toshio Nawa 表示，尽管东京奥组委及网络安全行业内已全面分析了近三届奥运会期间的网络攻击事件，东京奥组委也已制定采取了相应的对策。但 2021 年距上一次奥运会已有三年之久，黑客



的网络攻击手段不断发展，逐渐“规范”，面对史上网络安全形势最为严峻的一届奥运会，预计将出现超出想象的网络攻击方式。

2、奥运网络安全威胁数量、涉及范围与攻击手段呈矢量升级

根据美国的知名综合性战略研究机构——兰德的《2020 年奥运会威胁评估报告》提到，在 2012 年之前的奥运会中，在线攻击仅限于欺诈和普通黑客行为；但从 2012 年开始，发生了电力系统曾遭受长达 40 分钟的拒绝服务攻击，黑客从 90 个 IP 地址对奥运会服务器发起洪水般的攻击。最近一次针对 2018 年平昌冬奥会的攻击，使奥运会网站瘫痪时间长达 12 小时，威胁影响范围涉及众多。

在后期的调查中发现，造成此次史诗级事件的攻击者很早就利用钓鱼邮件投递恶意代码进入内网，获取部分组委会工作人员的计算机权限。开幕式当天早上，攻击者向这些计算机中投放了以破坏为目的的蠕虫病毒，窃取用户密码、在内网进行爆破传播，投放后很快便控制了数百台电脑。开幕式启动时，蠕虫病毒开始大肆破坏控制计算机系统，数据中心的服务器被破坏至系统崩溃，网络、Wi-Fi、电视直播、楼宇门禁、网站、APP 等服务均陷入瘫痪。在技术人员找到对抗蠕虫病毒的方法，紧急关闭所有服务，从备份数据成功重建服务器系统时，距离攻击开始已过去 12 个小时。

从这个过程可以看出，目前针对奥运会的黑客攻击

拥有非常成熟的网络攻击技能、高超的网络隐藏能力，其精心设计的特种蠕虫病毒，通过平昌奥委会域账号进行内网横向移动，窃取所有被控设备上的凭证信息并再次爆破传播，保证了可以精准控制、最大化控制奥委会内部设备。专门设计的系统毁灭和持续感染机制，令技术人员难以快速解决问题，迫使奥委会只能“休克式”重建系统，让攻击持续了 12 个小时。

兰德报告中提到，目前预见到的攻击很可能是数据泄露和虚假信息的结合。

CTA 的尼尔詹金斯表示，由于大量潜在受害者利用在线系统开展业务，因此，在此次东京奥运会中最有可能的威胁是在线欺诈、钓鱼等犯罪活动。其中涉及的各个方面，不仅仅是奥运会的网络安全相关部门，甚至包括运动员、观众、赞助商和官员在内，都必须保持警惕并注意以奥运会为诱饵的骗局，网络钓鱼电子邮件和欺骗性网站。


Russia planned cyber-attack on Tokyo Olympics, says UK

Foreign secretary condemns 'cynical and reckless' bid to disrupt Games, before they were postponed

3、网络攻击威胁来源多样 涉及地缘政治目的

兰德在关于奥运会威胁的报告中强调，奥运会不只是国与国之间的体育竞技舞台，政治紧张局势下各方势力的“角力”往往也会蔓延到网络空间战场。

前日，一个来自多方的调查报告中体现，目前赛事面临的网络安全威胁主要来源于三个方面：

一是国家支持的 APT 组织。国家支持的 APT 组织可能对奥运会和奥运会附属实体构成最重大的威胁，其中俄罗斯 APT 团体可能最有动机攻击并扰乱东京奥运会。二是网络犯罪分子。从网络犯罪的角度来看，勒索软件可能对与奥运相关的组织构成最大威胁。勒索软件团伙很可能将赛事视为勒索攻击的有利可图的目标，因为关键基础设施的长期停运可能会对活动产生高度破坏性的影响。三是黑客行为主义者。出于爱国或特定道义动机，黑客行动主义者可能将奥运会视为表达其特定信息的显著机会。

企业数据安全公司 SecureAge 的首席运营官杰里·雷曾说，俄罗斯黑客很可能会攻击奥运会，因为在其与日本发生领土纠纷以及与世界反兴奋剂组织 WADA 的长期交锋后，俄罗斯不仅有相关的网络攻击能力，并且有破坏东京奥运会的意愿和动机。

并且，俄罗斯情报集团 GRUUnit74455 被认为是平昌奥运会黑客攻击的幕后黑手，安全公司 FireEye 曾在报告中强调此结论。FireEye 情报分析高级主管约翰·霍尔特奎斯特在一次声明中指出：“我们认为值得注意的是，他们（俄罗斯情报集团 GRUUnit74455）没有因试图破坏奥运会而受到公开谴责，我们担心这些攻击者的下一个目标是今年的东京奥运会。”

据悉，东京奥运会筹办期间，已有黑客长期进行盯梢。《卫报》报道，英国国家网络安全中心披露，俄罗斯 APT 组织沙虫曾准备对原定 2020 年夏天举办的东京奥运会和残奥会发起网络攻击，攻击目标包括赛事主办方、后勤服务和赞助商。沙虫，被指曾策划了平昌奥运会“最糟糕开幕式”的袭击行动，据称该组织已经对东京奥运会相关官员和组织进行了“网络侦察”。2019 年针对东京奥组委钓鱼邮件的一系列攻击手法，正是沙虫组织袭击平昌奥运会时所用的。

对此，东京奥运会组委会回应称，已注意到相关报道，将采取网络安全措施确保奥运会顺利举行。

疫情之下东京奥运与黑客赛跑

在疫情反弹的阴影之下，日本先后举办两项重大体育赛事：7-8月的东京奥运会、8-9月的残奥会。全球的目光汇聚到日本，赛事也成为黑客极佳的展示舞台。

作为“有史以来数字化应用程度最高的一届奥运会”，东京奥运会的数字媒体及云技术应用数量为历届之最：东京奥运的比赛运营和记录涉及100套以上的系统。此外，因严格的防疫控制，东京奥运会将是历史上首次观众席接近“空场”的奥运赛事，奥运期间将借助云上转播等技术形式，是全球首届以数字平台或电视广播为载体的体育盛会。这些使东京奥运会更吸引恶意攻击者的“关注”，网络风险显著增加。

日本情报机构警告称，针对2020东京奥运会和残奥会的网络攻击将是日本面临的最大威胁之一。美国联邦调查局（FBI）也在奥运会举办前夕警告称，恶意攻击者很可能将矛头指向即将召开的东京奥运会。

事实上，日本奥运会早已通过成立指挥中心、制定网络安全战略、组织网络救援队、培养白帽黑客和展开攻防演练来应对可能发生的网络攻击。

网安忧虑推动安全建设

随着网络空间的对抗愈发激烈，日本对于网络能力的重视程度不断提升，多次在防卫计划、规划中提及网络安全的重要性，并加快建设网络安全队伍体系。东京奥运会也成为日本展示安全能力的重要舞台。

早在2017年7月，为应对2020年东京奥运会和残奥会的网络攻击，日本政府召开由官房长官菅义伟亲自挂帅的网络安全战略总部会议，在2018年度结束前后成立名为“网络安全应对协调中心”的政府指挥中心。

一旦在电力、通信、交通和医疗等重要服务系统发生网络攻击，“网络安全应对协调中心”将立即建议应对方法，与奥组委携手把损失控制在最小程度。

日本还加强与其他国家的双边合作，并加强了现有的伙伴关系。例如，日本与美国国土安全部合作，研究如何改善其网络安全，为2020年东京奥运会做好准备。

日本能源公用事业公司还与以色列电力供应商以色列电力公司(IEC)合作，应对在奥运会期间管理关键基础设施的网络安全问题。

持续培训解决人才挑战

网络安全人才不足是全球性的问题，2021年有350万人才缺口，但日本在安全人才资源方面遇到独特的挑战。2016年，日本国内网络安全领域的专业人才不到26.5万人。此外，日本政企机构习惯于将IT与网络安全外包，仅自有28%雇用网络安全人才，而美国为65.4%，德国为61.4%，英国为53.9%。

为弥补安全人才缺口，日本政府建立基于网络安全的国家级“情报处理安全保护”等级考试制度，日本加紧网络安全人才的培训。据日本共同社报道，东京奥组委以发生大规模系统故障的平昌冬奥会为教训，假象开幕式遭到攻击等情景，针对性开展安全人才培养，以保障赛事运营。

为避免出现平昌冬奥会遭遇，自2019年起，日本政府网络安全指挥中心——国家网络就绪准备和战略安全中心(NISC)就与奥运重点服务提供商开展应对培训，包括电力、电信和医疗机构，这些机构对于奥运会顺利进行必不可少。截至2021年6月，已有来自约600家企业的2000余人次参加培训班。

距离东京奥运会和残奥会开幕约半年的时间，东京奥组委培养了220名“白帽黑客”，作为应对网络攻击的工作人员，希望打造更加安全的东京奥运会。

奥组委的白帽黑客主要从NTT（日本电信电话）和NEC（日本电气）等民间企业借调。日本国立研究开发法人“情报通信研究机构”通过名为“Cyber Colosseo”的训练项目等进行人才培养，课程包括20个科目，演习采用在网络攻击中保卫系统等实战形式以掌握应对方法。

大胆的计划：入侵联网设备

此外，日本还启动了一项大胆的计划：入侵本国的联网设备，找出并修复这些互联网上的薄弱点。自2019年5月开始，日本在18个月内开展实网测试，以确保橄榄球世界杯和2020年东京奥运会举办期间的网络安全。

日本信息通信技术研究所（NICT）被授权扫描国内互联网，对国内近2亿台物联网设备进行测试性攻击，包括摄像头、数字电视、灯具、冰箱等其他家用电器，以寻找不安全的家庭和办公室联网设备。NICT使用常用凭据、用户名和密码测试性攻击，成功获取设备访问权后，NICT将联系设备所有者建议其改进安全措施。

日本政府在应对物联网威胁的方法上大胆创新，其首要任务是奥运会的网络弹性能力。非技术方面的因素也应发挥作用，如塑造社区个人和组织为实现共同安全目标而努力的形象，促进合作和建立信任。

对东京奥运会和残奥会网络安全的担忧，推动日本加强网络安全建设，但来自智库的报告认为，日本的网络弹性依然“相当有限”。在网络安全这场持续的攻防对抗中，安全建设也永无止境。

奇安信与冬奥的故事

2021年7月27日，距离北京2022冬奥会开幕不到200天，北京冬奥会安全保障工作进入“备战倒计时”，“网安一哥”奇安信宣布签约两位品牌代言人——速度滑冰世界冠军宁忠岩，单板滑雪世界冠军蔡雪桐。

宁忠岩来自冬奥会中国王牌之师——速滑队，他的主要参赛项目是速度滑冰、短距离团体追逐赛，主要成绩有速度滑冰1500米首个世界冠军，是亚洲1500米纪录保持者，全国1000米、1500米纪录保持者。

蔡雪桐来自冬奥会中国冰雪新骄傲——单板滑雪队，她的主要成绩有2017年国际雪联单板滑雪世锦赛女子U型场地冠军，2019-2020赛季单板滑雪U型场地世界杯美国猛犸山站女子组冠军，2019/2020赛季单板滑雪U型场地世界杯总积分冠军，以成绩高度稳定著称。

两位品牌代言人的加入，为奇安信提供了参加冬奥具体项目的实际运动经验和各项数据。“网安一哥”奇安信作为中国顶尖网络安全企业，将冬奥项目运动与具体安全防护产品一一映射，制定针对性强的系统化、实战化冬奥保障计划。

北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商发布会

奇安信结缘冬奥会

2019 年 12 月 26 日，奇安信正式成为北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商。奇安信为安全而生，在诞生之初就树立“让网络更安全，让世界更美好”的使命，立志成为全球第一的网络安全公司。

网络安全攻防对抗和冬奥赛场的激烈角逐大有相通之处，都是不断挑战困难、勇敢拼搏、超越自我的过程。

奥运会追求 “更快、更高、更强”，而网络安全推崇更快的应急响应速度、更高的监测发现视角、更强的对抗突破能力。网络安全人和体育健儿，二者相通之处在于，一方面都基于强大的内在驱动力和自律性，一方面都依靠在“对抗赛场”上艰苦训练和全力拼搏，最终为国家和集体的目标，坚韧不拔、勇敢向前！

作为北京 2022 年冬奥会和冬残奥会官方网络安全服务和杀毒软件赞助商，奇安信以更快一步、更高标准、更强防护的安全能力，为政府、企业用户提供新一代企业级网络安全解决方案、产品和服务，凭借以实战攻防、平台创新、规划咨询为代表的全面领先的优势，通过七年积累，发展成为企业数字化转型与升级的全天候、全方位安全顾问。

北京冬奥或将面临最复杂网安挑战

为切实做好北京冬奥会的网络安全服务，奇安信集团与北京奥组委认真研究分析近四届奥运会经历的网络安全威胁事件，总结历届奥运会网络安全防护经验教训。

北京冬奥会网络信息系统规模大、结构复杂、风险点多，安全防护任务十分艰巨，对网络安全提出了更高的要求。此外，北京冬奥会实现了全球首次5G全覆盖——冬奥场馆、高铁地铁将 5G 全覆盖。

结合当前我国面临的网络安全严峻形势，专家认为，2022 年 2 月 4 日举办的第 24 届冬季奥林匹克运动会将面临的历史上最复杂的网络安全挑战。

奇安信安全中心

奇安信科技集团总裁吴云坤

北京冬奥组委专职副主席兼秘书长韩子荣致辞

六全防护体系

奇安信集团专门成立奥运运营中心，组建冬奥红云战队，齐向东董事长亲自担任总指挥，启动冬奥百千万计划，百人奥运专项团队投入总体规划。

2022年冬奥网络安全保障组负责人（奇安信集团总裁）吴云坤认为，“要解决北京冬奥会网络安全面临的实际问题，需要用工程化思想、体系化规划建设面向科技冬奥的网络安全体系。”

在总结历次国家重大活动网络安保的经验基础上，奇安信为北京冬奥运专门打造了“六全防护体系”：全维度管控、全网络防护、全天候运行、全领域覆盖、全兵种协同、全线索闭环，确保北京冬奥会关键系统万无一失，“零事故”运行。

截至目前，安全体系已经初见成效，形成了一套覆盖“技术、管理、运营”的实战化综合防御体系，赛事期间，北京奥组委与奇安信集团将动员核心技术力量，为冬奥会的顺利召开保驾护航。

奇安信安全防护软件冬奥版发布

2021年4月29日，奇安信安全防护软件冬奥版正式发布。该软件优先保证给各个国家参加冬奥的工作人员、运动员、志愿者，以及奥运会举办城市的城市志愿者使用，同时将面向个人用户开放。

奇安信安全防护软件冬奥版不仅保留了奇安信天擎业界领先的强安全能力，还重点强化了个人终端关注的隐私保护、卡慢追踪、网络连接管理、攻击溯源、无广告打扰等功能。在查杀病毒方面，冬奥版基于猫头鹰（QOWL）反病毒引擎、深度学习（QDE）引擎、云规则（QCE）引擎三大自研引擎保驾护航，覆盖样本超100亿，分钟级响应全网突发事件。

奇安信集团董事长齐向东

会上，韩子荣高度肯定了奇安信为守护冬奥安全所作的前期筹备工作。她表示，“2019年12月，奇安信成为北京冬奥会官方网络安全服务与杀毒软件赞助商，积极发挥专业优势，主动对接冬奥会网络安全需求，提供了精准可靠的网络安全技术、产品和服务，为筹办工作提供了有力保障。”

东京奥运会之后，奥运周期即进入北京时间。随着两位代言人的加入，“网安一哥”奇安信希望汇聚更多力量，为北京冬奥会构筑最坚固的网络安全防线。安

攻击者每发动一次网络攻击，身份信息就可能暴露亿点点

作者 公关部 魏开元

在《猫和老鼠》这部动画片里的其中一集，汤姆为了抓住涂抹隐形墨水的杰瑞，使用了两种办法：第一种如图一，杰瑞仗着隐形效果，明目张胆地坐在那里吃水果，结果被汤姆利用它的影子发现了行踪；第二种如图二，汤姆在地上洒满了面粉，杰瑞只要走过，必定留下满地的脚印。其实无论汤姆用什么方法，他的目的就只有一个，找出杰瑞。

图一

图二

网络攻防也是一个“猫和老鼠”的游戏。攻击者也会使用加密的攻击流量、加密的木马或者其他恶意文件，达到让自己“隐形”的目的。

对于防守方而言，他们需要借助一些工具，让原本隐形的痕迹暴露出来，从而挖出幕后的攻击者。

奇安信态势感知与安全运营平台 NGSOC 就是其中之一。说起来，NGSOC 可是政企机构实战化安全运营的一款利器，能够通过收集多元、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。

直白点说，NGSOC 能够记录内部 IT 系统产生的所有日志数据（当然包括攻击者的），一旦发现异常，就会产生告警，为安全运营提供决策支持。理论上说，只要攻击者敢进来，NGSOC 都能记下来。言外之意，想要不暴露，还是别进来了。

案发现场：一次标记“已失陷”的告警

叮叮叮，叮叮叮……墙上的挂钟响了八声，刺眼的阳光透过窗户照在了计算机屏幕上，又到了和值夜班的兄弟交接班的时间。刚从洗漱间走出来的奇安信安全运营工程师航哥，对着满是黑眼圈的哥们儿说：“昨晚没什么事情吧？”在得到对方肯定的答复之后，航哥又说：“包子给你们放茶几上了，洗把脸吃两口，去隔壁屋睡一会儿吧。”

说罢，航哥接过了这哥们儿的位子，熟练地登录上 NGSOC 管理后台。在这个不大不小的防守方值守办公室里，倒计时牌上的“1”字格外显眼。今天是 A 公司内部网络攻防演习的最后一天，作为奇安信 NGSOC 产品和安全运营服务的采购方，A 公司邀请到了奇安信安全

运营工程师，共同组成了本次演习的防守队。

经过 9 天的激烈对抗，攻防双方的得分一直咬的非常紧。

就在航哥心中不断默念上天保佑今日平安的时候，一条标记为“失陷”的告警信息，让他惊出了一身冷汗。告警信息显示，攻击者使用冰蝎工具（一种 Webshell 管理工具，主要用于执行攻击命令），连接了其植入的 Webshell 文件 common.jsp（一种常见的网页后门文件）。

一瞬间，无数种可能在航哥脑海中闪过，根本来不及仔细思考。在失陷信息上报之后，他立即通过 NGSOC 调用防火墙，封禁了攻击 IP。暂时阻止攻击者在内网的进一步渗透。

很快裁判组传来了消息，按照演习规则，由于内网服务器被攻陷，防守方被扣掉了一些分数，让原本紧咬的比分一下子被拉开了。

虽然在心里直呼“凉凉”，航哥还是将心情快速平复了下来。他不停地思考：到底是谁在这么重要的时刻，给我来这么一手?

想要做到这一步，就得看看 NGSOC 到底能记录多少攻击者的相关信息，再从这些相关信息中，分析出幕后的攻击者到底是谁。

线索搜集：“受害人”调查走访

线索搜集工作千头万绪，但经验老道的航哥知道，所有头绪都得从“受害人”和留在受害人身上的“凶器”开始理，找到了这些，施害人也就离他不远了。

这里的受害人就是被黑客攻陷的服务器，而凶器自然就是攻击者上传的 Webshell。

很快，攻击者就留下了第一条线索。在 NGSOC 事件调查模块，航哥轻易定位到了失陷服务器，并找到了最近一段时间内访问或连接该 Webshell 文件的 5 个外网 IP 地址。这就是说，攻击者同时使用了 5 台机器，对“受害者”发动攻击命令。

为了进一步查清攻击者到底对“受害人”做过什么，航哥决定从 NGSOC 平台导出这五个攻击 IP 的所有流量日志，看看能不能从中找出和攻击者相关的蛛丝马迹。

果不其然，攻击者的信息开始一点点的暴露在航哥面前。

流量日志分析的结果表明，估计是怕“打草惊蛇”，攻击者在渗透初期，在服务器里提前埋了一个经过免杀处理但功能非常简单的恶意文件 ***239538548.jsp，为后续的入侵动作“打前站”。时机成熟后，攻击者便利用 ***239538548.jsp 这个“潜伏者”，从自己的服务器上将 common.jsp 这个可以执行攻击命令的“凶器”带了进来。

与此同时，航哥还获取了一个非常关键的信息，攻击者自己服务器的域名是 **0101.com。这就等于找到了施害人经常活动的窝点，这里一定有能表明攻击者身份的证据。

可他还没来得及高兴，里屋俩值夜班的哥们儿却突然跑了出来说：“航哥，听说系统被打了？”

“是啊，你们咋知道的。”航哥突感诧异，“这俩哥们而不是在睡觉么？”

“这么大事儿能不知道么，群里一直在说这个，这不我们也被吵醒了。听群里师傅们分析，说是有 0day 漏洞？”

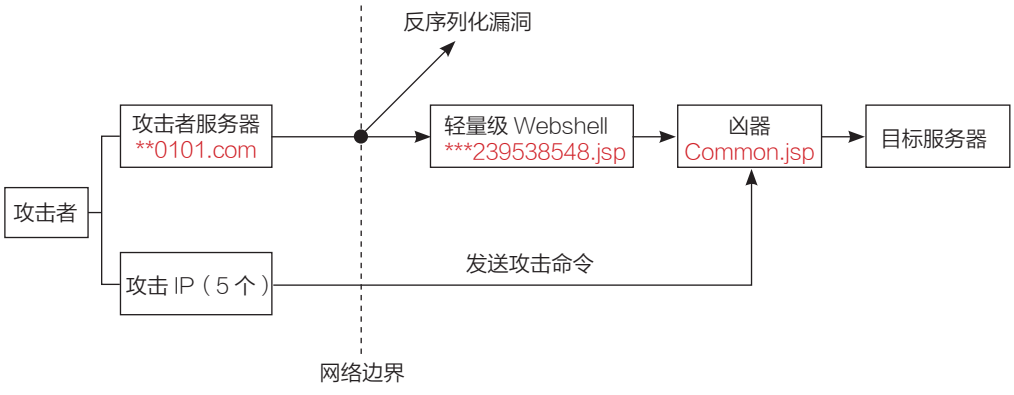
“额！”航哥心里一紧，“是啊，防火墙、IDS、WAF，该有的边界防护都有了。这么严密的防护，这个‘雷’是怎么提前埋进来的呢？刚才流量分析也没查出个所以然。”

8 成是挖出了什么 0day 漏洞。不过想要知道漏洞出在哪里，还得从“凶器”开始查。

顺着“凶器”这条线索，航哥仔细审计了文件写入相关的流量日志，终于定位到了漏洞点：攻击者利用某系统页面的反序列化漏洞，在演习开始的第一天，就写入了一个轻量级的 Webshell 文件，躲过了边界防护设备的拦截。

经漏洞研判组的同事确认，该反序列化漏洞为 0day 漏洞。

至此，航哥已经理出一条完整的攻击链条，如下图所示。



踩点蹲坑：挖出幕后“施害人”

至此，“受害人”的调查走访就告一段落，剩下的恶意文件分析、影响面分析、漏洞修复和相关的安全风险梳理工作，交给其他更专业的同事就可以了。

现在，航哥满脑子都是怎么才能找到幕后攻击者是谁。按照演习规则，只有这样，才能逆转分数暂时落后的局面。

现在摆在他面前的有两条路。第一条是以 NGSOC 记录的攻击者 IP 地址为基础，进行情报收集和关联分析，从而判断对方到底是谁。但在攻防演习的场景下，攻击者使用的攻击 IP 往往是主办方提供的固定 IP 地址，和攻击者并没有强相关性，因此很难挖掘出有用的线索。

第二条就是顺着“**0101.com”这条线索，对施害人的一个窝点，也就是攻击者用于上传 Webshell 的服务器进行蹲守，搜集攻击者的身份信息。

想到这儿，航哥掏出了另外一个“大宝贝”——奇安信威胁情报中心威胁分析平台。该平台可以对恶意文件、恶意域名以及恶意 IP 地址等相关威胁信息进行关联搜索。比如，用户输入一个杯子，这个平台就能告诉你这个杯子是不是航哥的；当用户再输入“航哥”，平台还能告诉你除了杯子，他还使用了什么样的碗、什么样的筷子，等等。

这次的收获倒是不小。**0101.com 这个域名对应的 IP 地址为 **.**.95.47，注册时间是 2016 年，至今仍在使用。用航哥的话说，只知道人家“窝点（服务器）”叫什么名字（域名）还不行，你得知道人家服务器在哪（IP 地址），这样才能去蹲守。

按照威胁分析平台的导航，航哥找

最早看到	最近看到	域名
2016/06/20	2021/04/27	[illegible]
2021/04/15	2021/04/15	[illegible]
2017/06/15	2021/04/06	[illegible]
2016/06/20	2021/03/21	[illegible]
2020/06/29	2020/11/03	[illegible]
2020/08/03	2020/08/03	[illegible]
2020/07/18	2020/07/18	[illegible]
2017/06/22	2020/06/17	[illegible]

到了攻击者经常活动的窝点。经过一段时间的蹲守（对 **.**.95.47 进行关联搜索），航哥发现 **.**.95.47 这个 IP 地址，在 4 年内关联了 8 个域名，这意味着这个 IP 曾部署过多个网站。

一瞬间，航哥的兴趣来了，所幸随便登录了其中一个网站域名，看看这些网站上到底都有些什么东西。Surprise！这竟然是某火爆全球的 MOBA 类游戏的脚本网站，航哥笑了，看来这个攻击者跟自己有同样的兴趣爱好，都喜欢打这款网游啊。

不过，让航哥气愤的是，这人玩游戏“不讲武德”，打不过就开脚本，一定得把他抓出来，以后玩游戏要拉黑他。

通过网站备案号，航哥很快就在工信部域名信息备案系统的网站上查到了攻击者的姓名，并进一步确认从 2016 年至今该域名、和 IP 地址为同一人使用。

“哈哈哈，你终于还是漏出了‘狐狸尾巴’。”

恰在此时，恶意文件研判组的同事传来消息，经过对攻击者经营的网站上外挂脚本文件逆向分析之后，发现了源代码中多次出现一个类似姓名的拼音以及社交账号等可以表明身份的信息。他们怀疑，这应该就是攻击者自己的姓名和社交账号。

经过与自己所掌握的信息进行比对，航哥确认了这一条重要的线索。

不过事情到这里还没结束，姓名和社交账号信息还不够，按照攻防演习的要求，航哥还应该获取更精确的信息，才能提交一份完整的攻击者溯源报告。

想到这，航哥决定用小号加这哥们儿的好友，看看从这里能不能找到一些有用的信息。不过很快航哥就失望了，尽管好友申请很快就通过了，但这个人几乎从来不发动态，头像也不知道是从哪个动漫里截的，一点有用信息也没有。

路走到这里，似乎再也走不下去了。可时间仍在一分一秒流逝，演习已经到了最后关头。

就在航哥冥思苦想解决方法的时候，他无意间在搜索框内输入了攻击者的名字，有趣的事情出现了，竟然搜索到了和攻击者有关的新闻，照片和公司名称都赫然在列。

就这样，一份完整的攻击者溯源报告就完成了。在报告提交之后，航哥低头看了看手表，时间定格在了下午四点五十八分。

“好险，只差两分钟。”

随着防守方取胜的消息从裁判组传来，防守方值守办公室里终于响起了掌声。安

勒索攻击已成“流行病” 医院如何打造闭环式安全运营?

作者 公关部 张少波

医院，是治病救人的场所，然而面对勒索病毒这一肆虐网络世界的“流行病”，医院几乎束手无策，甚至成为主要受害者。

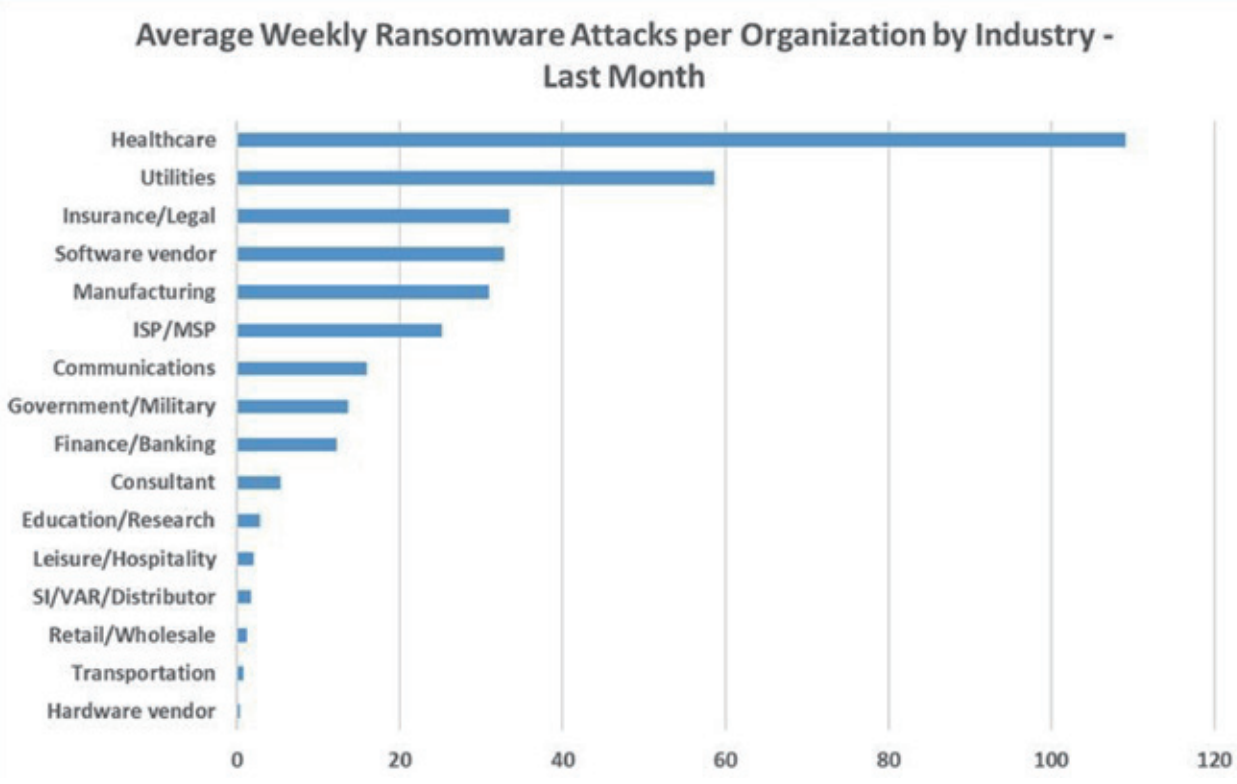
“网络攻击的形式手段有很多，但让我们医院最有切肤之痛的，当属勒索病毒攻击。”虽然事隔数年，安徽医科大学第二附属医院信息中心主任王慧姮仍然对当年的“永恒之蓝”勒索病毒攻击事件心有余悸。而正是这场席卷全球 150 个国家近 20 万台电脑的勒索病毒，让包括医疗在内的各行各业，对网络攻击有了空前的认知。

据王慧姮主任回忆，在 2017 年 5、6 月份，安徽省各主要医院大范围中招，“虽然没有给我们造成灾难性伤害，但我们用了两周时间、二三十人去清理，包括更换了部分电脑，才彻底清除了这轮勒索病毒的影响。还有些医院花了几乎三四年的时间，才恢复了丢失的数据，其业务和人力损失无法估算。”

前事不忘，后事之师。在经历过勒索攻击等事件之后，安徽医科大学第二附属医院（简称：安医大二附院）、安徽医科大学第四附属医院（简称：安医大四附院）这两家兄弟医院，充分意识到要保障医院业务平稳运行，提升网络安全防护水平迫在眉睫。

日益猖獗的勒索攻击 成了扑不灭的“流行病”

勒索攻击，最早出现于 1989 年，AIDS trojan 是世界上第一个被载入史册的勒索病毒，从而开启了勒索病毒的时代。



时至今日，勒索攻击愈演愈烈，美国最大的燃油管道运营商科洛尼尔 (Colonial Pipeline)、全球最大肉类加工商 JBS 公司、美国最大传媒集团之一考克斯媒体集团（Cox Media）等巨头近期纷纷中招，断油、断肉、断播……勒索攻击造成的危害屡次占据媒体头条，以至于美国政府将其与恐怖袭击并列。

由于医疗行业的重要性与特殊性，以及对信息化的高度依赖，使其经常成为勒索攻击的目标。2020 年 9 月，德国杜塞尔多夫的一家医院遭勒索软件攻击，该医院的关键入院和病人记录系统被离线，导致一位紧急入院病人在被迫转院途中耽误救治时间而亡；2021 年 5 月，爱尔兰公共资助医疗系统 HSE 受到勒索病毒攻击，700GB 重要数据被窃，导致该国家多家医院的服务取消和中断，新冠病毒检测工作受到影响……尤其是去年新冠疫情全球蔓延以来，针对医院的网络攻击急速增加。根据 Check Point Research（CPR）最新报告显示，医疗行业成为勒索软件攻击的头号重灾区，每个组织平均每周遭受 109 次攻击。

“我们是三甲医院，拥有 2000 多个各种终端，仅机房就有 53 个应用系统，但 IT 加上网络安全人员仅 7 个人，人手非常紧缺，安全力量比较薄弱。” 王慧姮主任谈到，“我们迫切需要实现网络安全管理和技术水平‘双提升’，避免遇到勒索攻击时手忙脚乱。”

安医大二附院信息中心工程师朱全回忆了这样的细节：2019 年，医院更新服务器被病毒感染，导致医院的 exe 文件全部隐藏起来，并生成一个同名的、文件大小只有几十 K 的 exe 文件，结果所有更新软件的计算机，都不能正常使用应用程序，严重影响医院业务。当时因为没有态势感知与安全运营平台（NGSOC），查找起来很麻烦，最后还是在更新服务器上抓包找到了源头，

才把问题彻底解决。

“我们需要提前感知危险在哪里，及早预警和处置，而非事后的亡羊补牢。”安医大四附院信息中心主任杨爱民也有同样的感受。从 2017 年的永恒之蓝，到后续屡次发生的安全事件，都加速了两家医院的网络安全建设进程。

仅靠产品堆砌还不够 医院网络安全建设面临三大痛点

王慧姮主任认为，在网络安全建设的道路上，合规驱动和业务需求，两个力量缺一不可。2017 年《网络安全法》颁布，从政策法规上，要求医院对网络安全工作加倍重视。因此，两家医院都上线了边界安全、准入、终端安全、上网行为管理、审计类等各类安全产品，然而在实际工程中，这种安全产品堆砌类的方式，效果并不尽如人意，集中表现在以下几个方面。

首先是“孤岛”作战、缺少联动，安全防护能力没有充分发挥出来。

在部署 NGSOC 之前，两家医院都遇到一个普遍问题：虽然已经部署了大量的安全设备，包括边界安全、终端安全、上网行为管理、漏扫、审计等，但各设备之间相互孤立、单兵作战，日常运维、事件回溯更是因设备太多而无从下手。

杨爱民主任谈到了安医大四附院面临的困惑：面对层出不穷的新攻击手法与高度组织化的黑客行为，医院的内网安全产品还停留在“孤岛”作战的状态。在流量侧，对于加密流量缺乏有效的检测与防御方法；在终端侧，对于基于 0day 漏洞、高度定制化的恶意应用缺乏有效的查杀手段，因此在解决此类高级威胁方面，协防联动已经成为两家医院的共同诉求。

其次是检测和响应滞后，导致风险激增。

勒索病毒是“自我进化能力”最强的网络安全威胁之一，不仅在持续产生新的变种，其攻击手法也在不断变化，从钓鱼邮件攻击，到网站恶意代码入侵，再到社会工程学，各种高级威胁的技术手段在勒索攻击得到复合型应用。而传统的安全技术手段，大多是利用已知攻击特征进行静态规则匹配，因此对于勒索攻击等高级威胁，现有的安全防护体系无论是在威胁的检测、发现还是响应等方面，都存在严重不足。

杨爱民主任特别指出，在处置响应环节，由于边界防护设备分布在不同的安全域和分支机构，不同的运维审计类产品部署在不同的安全域，还有端点的防病毒和安全准入，以及数以千计的资产，通过人工处置告警显然是困难重重、容易遗漏，这些都造成了巨大的潜在风险。

第三是缺乏可视化的管理手段，无法整体掌控态势。

网络安全攻防，唯有知彼知己，才能掌握主动。项目实施之前，在两家医院的安全体系中，大量的安全监测结果只是单一维度的反映某个系统存在相关问题，呈现的方式也多种多样，并没有针对海量的安全数据进行统一可视化展现，无法整体掌控网络安全的态势，给安全管理造成较大的门槛和成本。

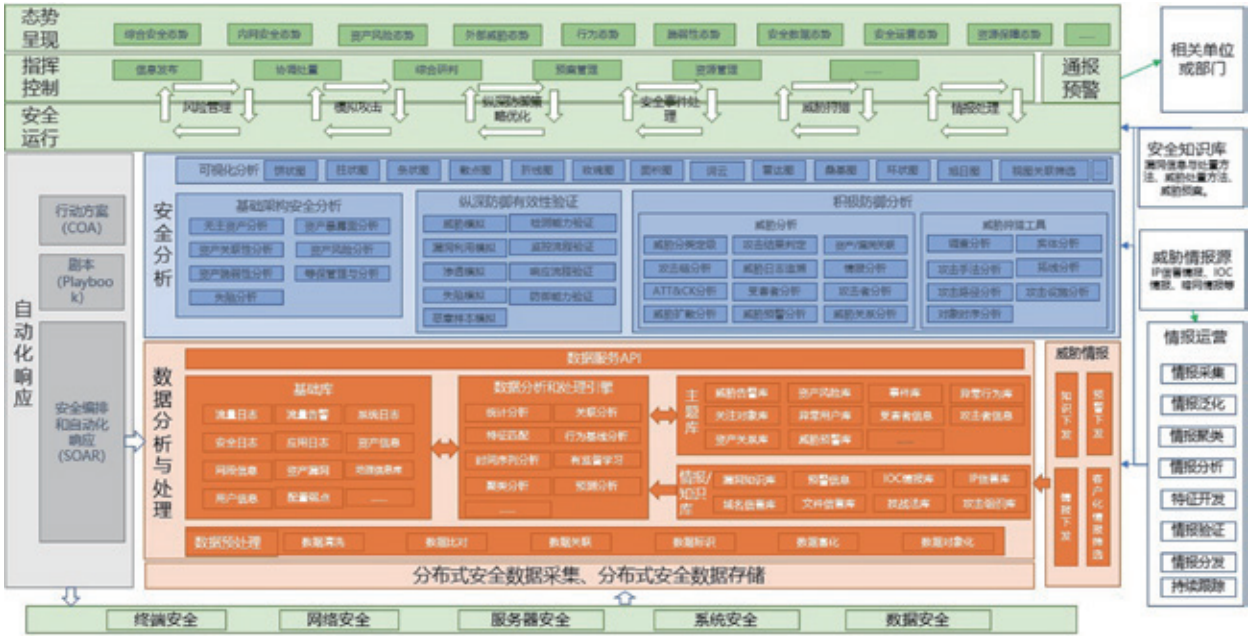
强联动、早处置、易管理 NGSOC 效果立竿见影

网络安全建设是一个长期的过程，随着 2020 年等保项目的实施，态势感知与安全运营被列上日程。两家医院本着“安全是第一位”的理念，以及高标准的要求，对多家安全厂商进行整体比较和严格评估，最终选择了综合实力更强且更适合医院业务现状的奇安信态势感知与安全运营平台（NGSOC）。

经过两家医院一年来的实践，NGSOC 很快在以下方面收到了立竿见影的效果。

第一是告别各自为阵，变被动防御为积极防御。

目前部分针对性的勒索攻击，从攻击手法上看完全是 APT 级别的，需要多个产品联动才能及时阻止。对于这种情况，NGSOC 能通过数据联动将内网各安全设备



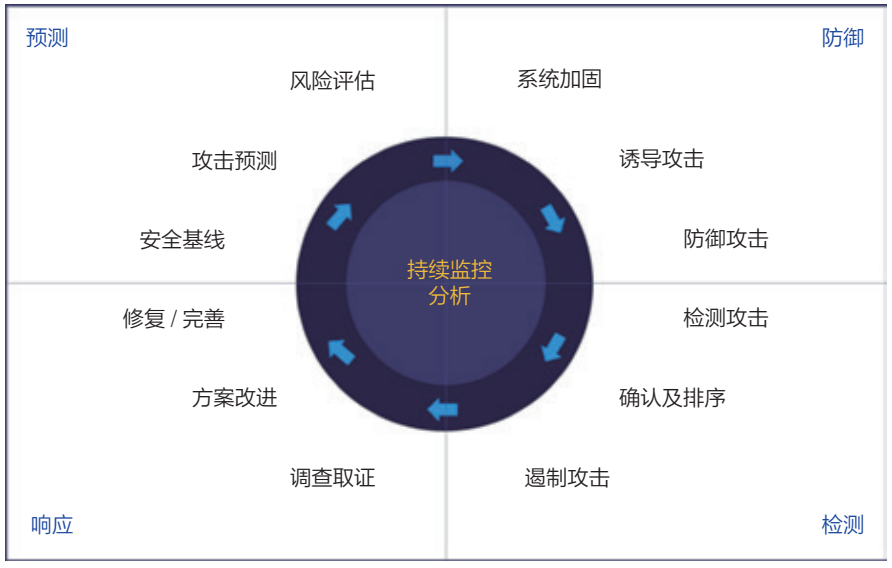
图：医院态势感知与安全运营方案总体架构

协同起来，实现内网安全的全面监测与防护，帮助用户及时发现感染勒索病毒的主机和服务器，尽可能将影响降到最低。

同时，NGSOC 还可利用本地的大数据平台对各阶段的检测结果进行存储与分析，为完整回溯安全事件提供数据基础，推动医院的安全建设从被动防御阶段向积极防御阶段演进。

第二是提前发现攻击，实现料敌于先，早处置降低风险。

“正所谓‘聪者听于无声，明者见于未形’，全天候、全方位感知网络安全态势，是安医大二附院网络安全管理建设的重要目标。”王慧姮主任谈到。面对勒索病毒等高级攻击形式，NGSOC 搭载的分布式关联分析引擎具备强大的数据分析能力，能够更快地发



图：基于 NGSOC 的威胁闭环管理

图：医院综合安全态势

现隐藏在各类日志中的安全问题。尽早发现威胁，可以为快速弥补安全问题提供宝贵的时间窗口，显著降低安全风险。尤其是对医院而言，勒索病毒无疑是潜在的炸弹。早一分钟解除威胁，就可能从死神手中多抢回一条生命。

第三是更友好的可视化界面，便于管理控制。

产品好不好，用起来是关键。朱全表示，“安全管理并不如网络、业务等内容更容易被管理者理解，因为安全所涉及的技术内容纷繁复杂，存在天然的技术屏障。因此，通过直观、清晰的图形展示，可以帮助管理者快速理解并判断当前安全态势。”

使用 NGSOC 后，医院可以直接通过态势感知大屏直观地查看医院网络内部不同资产组的风险分布，相关风险值会在逻辑拓扑上直接映射，以可视化的形式呈现在大屏幕上。外部威胁的攻击态势则能直接以地图展示的方式帮助管理者理解外部攻击的主要来源地、主要的外部攻击分类、本地最容易被攻击的资产等信息。所有态势感知的展示都可实时刷新，及时将最新的安全态势呈现在管理者眼中。

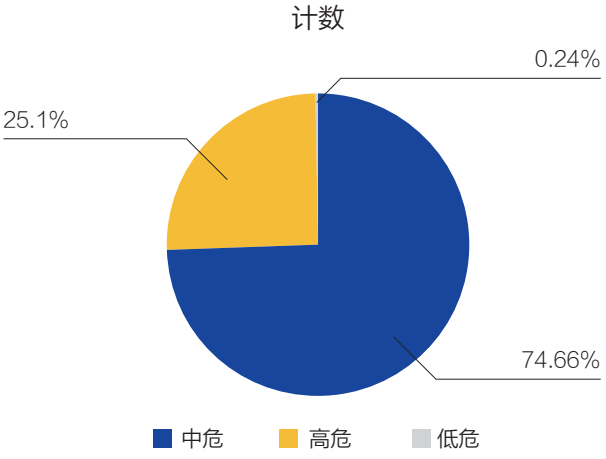
杨爱民主任也对 NGSOC 的可视化和易用性记忆深刻，“奇安信态势感知与安全运营平台设计符合我们的操作方式，界面很友好，功能很齐全，运行速度也很快，可以使我们对网络环境的安全态势一目了然。”

打造常态式、闭环式安全运营 将勒索攻击拒之门外

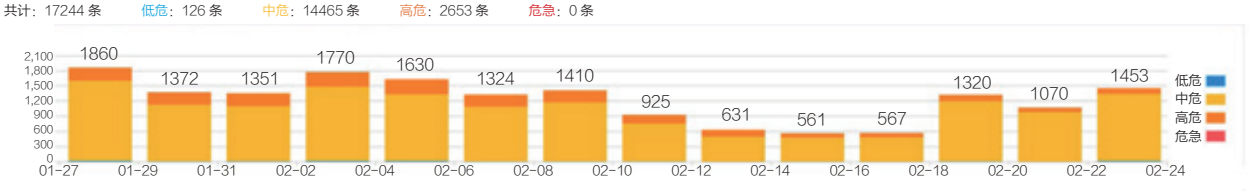
再先进的安全产品，也离不开专业的安全运营团队。对此，两家医院对奇安信的安全运营尤其是远程运营印象深刻，“奇安信每月提交一次态势感知与安全运营的安全分析报告，对于全网安全态势进行了详细的分析，总结了网内主要攻击源和高风险主机，这帮助我们加固

网络安全提供了很大的帮助。尤其在疫情期间，奇安信为医院提供远程运营服务，避免了高风险时期的直接接触，保障了医院在特殊时期系统的稳定运行。”

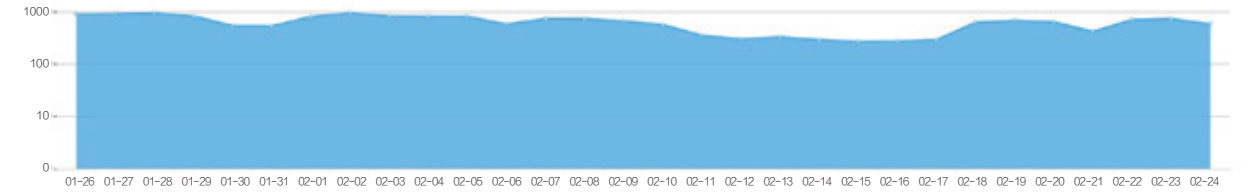
当今，勒索攻击已经成为网络空间的流行病。来自安全机构的一份预测，2021 年预计每 11 秒将发生一次勒索攻击，全年将超过 300 万次，造成损失或达数千亿美元。两家医院一致认为，要预防“勒索流行病”，仅靠产品还是不够的，只有将人、数据、工具和流程有机结合起来，建立常态化、闭环管理的安全运营体系，才能将勒索攻击等威胁拒之门外，保障医院业务的正常运转和数据安全。安



威胁等级占比



每日告警等级与数量分布



告警趋势图

图：医院安全运营报告之整体告警情况

他不仅是位“读书人”

——走近网络空间安全著名学者段海新

作者 公关部 孙丽芳

7 月 7 日，奇安信集团在京发布域名安全体系研究报告及“安全 DNS”公共服务 QDNS。一位面色白皙、身形清瘦、气质儒雅的学者两次走到台上，接连做了《域名体系安全及生态研究报告》《DNS 根节点测量》两次分享。

“我本来也可以安排我团队的人来讲，但我还是觉得，我来讲效果可能会更好一些。”

这位严谨的学者是清华大学网络科学与网络空间研究院教授，博士生导师，网络与系统安全实验室主任。国务院学位委员会第八届学科评议组成员，国际网络安全研究学术论坛（InForSec）发起人之一，清华大学 - 奇安信联合研究中心主任——段海新。

尽管早已是安全领域学术和工业界都非常知名的专家，段海新教授日常给人的感觉，却始终是谦虚有礼、温润如玉，很符合大家心目中对于“读书人”的定义。

这个理解确实正确，但又不完全正确。

孔孟故里走出的读书人

段海新教授来自孔孟故里——山东济宁的一个普通家庭，也许家人也没想到他在求学路上走了这么远，从哈工大到清华到美国加州伯克利，再回到清华。带领他越走越远的，正是互联网和网络安全。

多年前，李晓明教授（现在北大）赴美访问归来，带来了美国互联网发展的最新动态以及一些美国流行的互联网软件，引起了当时正在哈工大读书的段海新的兴趣。

“那时国内关于互联网的资料还十分匮乏，我从清华拷贝了一份 Linux，用李晓明老师带来的软件搭建了一台 Web 服务器和邮件服务器”。

以此契机，段海新开始在这个全新领域不懈钻研。后来，在北京听到清华大学李星教授关于互联网技术的一次学术报告，让段海新更深地“陷入”互联网的无穷魅力当中。

扎根校园的网络安全播种者

有了强烈的兴趣，加上不懈的努力，再后来赴京入读清华博士，开始网络安全的研究，并在这条路上渐入佳境，对段海新教授来说，就是水到渠成的事了。

也许为业界最熟知的角色，是段海新教授“网络安全播种者”的身份。

2010 年，网络安全教学界出现了一支生猛的“蓝莲花战队”，它正是由段海新教授和同事诸葛建伟副研

究员共同创建，是国内最早参与国际网络安全技术竞赛的队伍。而其名称正是段海新教授所起，寓意着他和学生们对网络安全技术纯粹的热爱与追求。当时的段海新教授亲身参与并带领学生们一起参加比赛，而这只战队随着比赛的磨练也不断声名显赫——“蓝莲花战队”于2013年成为华人世界首次闯入DEFCON CTF全球总决赛的队伍；2013年度在CTF TIME全球网络安全技术竞赛积分榜上排名全球第六、亚洲第一；此后两年连续入围DEFCON CTF 全球总决赛（2014-2015），并连续两年获得全球第五位的中国大陆最好名次。

被誉为“网络安全播种者”，除了带领学生在CTF竞赛中一展身手，更因为2006年至今，段海新教授一直任教清华本科和研究生班的网络安全课程。躬耕网络安全教学十多年，段海新教授注重培养学生的实践和创新能力，对我国网络安全人才培养发挥了重要作用。在段海新教授的课堂上，学生们感觉不到照本宣科的枯燥和乏味，取而代之的是在网络安全实战中汲取经验和技能。

学界与产业界间的摆渡人

除了课堂教学注重实战，段海新教授的研究一直紧贴现实。十多年来，段海新教授带领团队先后发现了互联网协议中域名系统、内容分发网络和Web协议等若干重大安全漏洞并提出了解决方案，促进了产品和标准的更新，产生了重要的国际影响；他长期从事互联网安全检测与应急响应，检测黑色产业、打击网络犯罪，为国家网络安全做出了重要贡献。

“产业界存在这样一个普遍的误解：学术圈的研究都只是理论，对于企业来说太过空泛，无法付诸实践。换言之，大家会觉得，‘书生’只会高谈阔论，实则‘百无一用。实际上，在网络和系统安全领域，国际顶级的学术研究很‘接地气’，特别是美国学术界研究的问题很多都是企业非常关心的，甚至也有很多企业界的人直接参与。另外，如果没有工业界真实的数据做支撑，单靠研究者自己搞个仿真来模拟一下，近年来已经得不到学术界的认可。我们的研究就一直是偏实践的，近年来的一些研究工作被国际学术届认可，主要也是发现了工业界实际的问题。”

一直以来，段海新教授和很多互联网公司、IT公司均有广泛的研究合作。2018年，段海新教授和工业界的深入交流与合作，迈出了更关键的一步——推动成立了清华大学（网络研究院）- 奇安信集团网络安全联合研究中心。

谈到为什么奇安信，段海新教授说：“奇安信是专注做网络安全的公司，体量也足够大，跟我的研究方向又非常契合。另外，因为这种校企合作给我的空间比较大，允许我用部分精力仍然继续原来学术上探索性的研究。”

当然，充当学界与产业界间的摆渡人，段海新教授也有过一段适应期。

“我没有在企业工作过，团队管理这方面也没有太多经验。学校里的团队主要是学生，他们基本上都有很强的自我驱动力，目标比较单一，就是取得学术成果，顺利毕业。公司里面可能就复杂一些，但我觉得总体来说还好，我们研究中心的技术骨干也多是从学校里刚出来的学生，有学术研究的背景，个人也都比较单纯、积极向上，所以也取得了不错的研究成果。”

联合中心利用清华大学网络研究院的学术研究和技术开发实力，结合奇安信集团的行业与产业优势，围绕互联网基础设施和协议安全、检测分析与数据驱动安全、物联网/车联网、5G等新兴网络安全、移动通信系统安全等重点课题开展深入研究，成为网络安全产学研深度融合的典范机构。

对科学用“套路”的研究者

无论是在校园，还是走出校园，段海新教授总能带领团队取得令人瞩目的学术成就，段海新教授却表示，其实得益于对科学方法和创新思维的理解，也许这就是别人说的“套路”。

“我的阅读面很广，经常反思一些甚至已经成为常识的一些所谓的传统认识。我理解科学最重要的是科学方法，它最核心的东西，其实就两条，一个是逻辑，一个是实证。这件事情后来又贯穿到我以后的研究当中。有人问我，你们发表顶级学术会议的论文，有没有什么套路？我觉得有，所有的套路就是这两条：你逻辑要清楚、严谨，你实验要充分。比如，我们关于根域名的测量，从逻辑上分析它的标准、它的源代码，然后我们在

2021年3月26日，清华大学（网络研究院）- 奇安信集团网络安全联合研究中心研究成果汇报暨管委会扩大会议在清华大学举行

实验室做实验，在现实的互联网上做大规模的测量实验。这就是逻辑分析再加实验证实。”

正是凭借“逻辑+实证”的“套路”，自成立以来，清华大学（网络研究院）- 奇安信集团网络安全联合研究中心在安全领域发表国际顶会论文10多篇，其中2篇获最佳论文奖；联合申请技术发明专利22项；出版专著《互联网基础设施与软件安全》；在互联网基础设施DNS和CDN安全、APT攻击及防御等方向支持国家重要需求，承担6项国家科研课题；联合组织两届大数据安全竞赛DataCon，吸引顶级高校和企业参赛并获奖；多次联合组队参加GeekPwn、天府杯、工业互联网安全技术大赛等安全竞赛，获重要奖项9次。

真正的知识分子

虽然治学非常严谨，但段海新教授并不是那种只沉浸在自己研究中的人。相反，他经常从研究中走出来，将视线放置在更无垠的时空里，也放置在周遭的事物上，思考、沉淀，再带着这些，回到自己的研究中。

工作之余，段海新教授喜欢读书、运动。他把很多思考和感悟，纪录在了自己的博客“段章取义”中。

“我自认为是个很有历史感的人，我希望用我的文字记录自己的感悟和经历，希望后来人能够看到。另外，多年来我一直觉得自己生活在两个世界中，一个是现实的世界，另一个是我自己的精神世界。现实的世界充满了世俗与无奈，‘长恨此身非我有，何时忘却营营？’总有一种想要出逃、‘小舟从此逝，江海寄余生’的冲动。在我的精神世界里生活着许多伟大的灵魂，比如，爱因斯坦、胡适、苏东坡等，阅读和写作让我觉得我在和他们进行超时空的对话，那种静谧、愉悦，一直在吸引着我。”

段海新教授表示，自己最欣赏苏轼所代表的理想人格。

从现实的角度，看不出段海新教授和苏轼有什么关联。和大部分人那样，段海新教授不曾经历苏轼那样离奇的起伏，没有像他那样，被命运几度高高举起，又重重摔落。但每一个人都有各自的精神樊笼，有理想与现实的矛盾。

“比如，社会上关于美国政府控制整个互联网、曾经让某个国家消失这类传闻非常多，这跟我了解的历史和事实有很大出入。作为学者，我非常欣赏胡适的那句话，有七分证据不说八分话。作为知识分子，我们应该独立于个人或者单位的利益，把客观事实说出来，让决策者根据客观事实作出决策和判断。我觉得，忠于事实真相，才是忠于我们的国家。”

苏轼的思想内核是儒家对人格自我完善的追求，在致君尧舜的思想影响下，苏轼不能身隐，对隐逸本质的深刻理解也使他无需身隐。苏轼在心隐中寻求到了人生解脱，居高位不邀君宠，处困厄不畏斧钺，在日常生活中，他为自己营造出了一个超然物外、闲适宁静的世界，达到了自由圆满的人生境界。

从这个角度看，段海新教授和苏轼又似有相通之处。

“我通常只是阐明我自己的观点，并不想说服任何人；如果有人愿意接受我的观点，我也希望他是经过独立思考之后的，那完全是他自己的选择。如果有人不同意我的看法，也尽可以提出批评或不同意见。如果发现我自己的认识有误，我会校正自己的观点，不以为这是‘自己打自己的脸’。”

读书人、播种者、摆渡人、研究者、真正的知识分子……虽然心怀“小舟从此逝，江海寄余生”的向往，但段海新教授从不曾有一日回避、脱离现实。相反，他牢牢扎根现实环境，解决现实问题，坚守内心，严谨治学、谦逊为人，活在当下。安

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

上海

南京

深圳云安宝

成都

沈阳


武汉


济南
安云


珠海


西安

7月22日，奇安信上市一周年。奇安信安全中心及各地分区举行了庆祝活动。

大事记

齐向东：数字经济要做好红线意识和安全流动两篇文章

“数字经济要做好红线意识和安全流动两篇文章。”在2021年中国网络安全年会上，奇安信集团董事长齐向东表示，数据泄露总量已超过前15年之和，平衡好数据利用与数据安全之间的关系，是数字经济平稳健康发展的关键。

其中，政企机构需要守住APP采集、数据跨境流动、数据存储和保护的三条“红线”，并通过安全体系有效防止破红线。

针对保护数据安全，齐向东介绍了奇安信的“九大板斧”：态势感知、零信任、云锁、特权账号安全管理、资配漏补的系统安全、邮件威胁检测系统、审查供应链、内生安全框架、隐私计算沙箱。

“九板斧”从制度、人员管理、系统防护、供应链上下游、数据交易等方面，对数据流动形成完整的安全防护体系，在保障安全的前提下，对数据价值进行充分挖掘利用，推进数字经济安全稳步发展。

教育行业合作伙伴大会召开 共建教育行业生态

7月16日，“2021奇安信教育行业合作伙伴大会”在奇安信安全中心举行。来自全国教育行业近百位合作伙伴齐聚一堂，共同探讨在当前国家产教融合战略机遇下，如何共筑教育行业合作生态。在会上，奇安信教育行业部发布了2021合作伙伴“大河计划”，并向合作伙伴详细介绍了奇安信OSM运营销售模式。

区别于其他企业的PSM渠道销售模式和CSM方案销售模式，OSM模式将通过产品BG、安全服务平台、战略规划中心、品牌营销中心联合，输出解决方案，赋能生态合作伙伴。奇安信也将提供一流的营销团队、产品团队、服务团队和生态公司，共同推动OSM框架方案落地，并提供持续的指导、帮助、支持、监督。

“责任之星”——奇安信亮相中国互联网大会

7月15日，在2021（第二十届）中国互联网大会闭幕式“星光盛典”上，奇安信凭借在抗击疫情及公益事业中的责任担当、党建工作及各类重保任务中的出色表现，以“责任之星”亮相。

主办方介绍，星光盛典旨在展现互联网人奋斗背后的精神内核，弘扬正能量，让“互联网之星”闪耀行业舞台，引领行业发展。主办方认为，奇安信在推进技术创新、勇担社会责任，弘扬正能量、引领行业发展及献礼建党百年等多个方面表现突出，对行业起到了表率作用。

奇安信韩永刚：应基于数字化业务流转建立数据安全防护体系

在 2021 中国互联网大会数据安全论坛上，奇安信集团副总裁韩永刚发表了“基于数字化业务视角的数据安全防御体系”主题演讲，指出《数据安全法》给安全行业带来了空前机遇，也给企业带来更高要求，安全企业需为客户尽快开展数据安全治理，建立数据安全保护体系与提升数据安全能力。

日前，奇安信已对外发布了“数据安全治理与保护体系建设路径图”，以及“数据安全能力框架”，为数据安全治理和保护体系，勾勒了面向未来的体系化建设路线。并以零信任、特权访问管理（PAM）、数据审计、数据泄露保护（DLP）、数据脱敏、APP 隐私卫士、数据交易沙箱等产品与服务为政企用户提供数据安全保障。

《网络产品安全漏洞管理规定》独家解读

工业和信息化部、国家互联网信息办公室、公安部联合印发《网络产品安全漏洞管理规定》（以下简称《规定》），并将于 2021 年 9 月 1 日起施行。

奇安信集团副总裁、补天漏洞响应平台主任张卓认为，该《规定》释放了一个重要信号：我国将首次以产品视角来管理漏洞，通过对网络产品漏洞的收集、研判、追踪、溯源，立足于供应链全链条，对网络产品进行全周期的漏洞风险跟踪，实现对我国各行各业网络安全的有效防护。

张卓认为，该《规定》重点解决了以下几方面问题：一、压实责任；二、明确流程；三、清晰指引；四、划清红线。

吴云坤：保护数据和应用安全是保障智能系统的关键

“数字化转型和智能化发展中，衍生了新的安全需求，保护数据和应用成为关键”。在世界人工智能大会（WAIC）的人工智能安全高端对话上，奇安信集团总裁吴云坤发表主题演讲时表示，需要打破安全与信息化之间的壁垒，将安全与信息化进行深度绑定，用内生安全框架指引数据智能系统的安全体系建设。

内生安全框架体系落地遵循统一规划、分布建设、重要先行、急用先行原则。针对智能化系统的保护，应重点建设“数据安全” 和“应用安全”工程和任务。其中数据安全应基于数据全生命周期及应用场景开展防护工作，而在保护应用安全方面，安全左移是本质，保护软件供应链安全是关键。

全国工商联党组副书记樊友山一行到奇安信开展调研

全国工商联党组副书记、副主席樊友山一行莅临奇安信，与奇安信集团党委书记、董事长齐向东等公司高管进行了深入交流。

樊友山一行实地参观调研了奇安信安全中心展厅、工控实验室及党建室，听取了奇安信“红色云展厅”及“红

云行动”等优秀党建工作的介绍，及奇安信业务发展技术研发成果的汇报，樊友山对奇安信党建引领企业发展、党建数字化建设、网络安全技术创新等工作表示赞赏。

资源占用降低 50% 奇安信安全防护软件冬奥版率先适配 Windows11

7 月 8 日，奇安信安全防护软件冬奥版已经率先完成了和 Windows11 系统的适配工作，并上线多项功能。对此，奇安信集团副总裁张庭表示，自 4 月 29 日开启内测以来，经过广大用户两个多月的内测体验，奇安信安全防护软件冬奥版在功能、性能等方面均有大幅度提升。

值得关注的是，奇安信安全防护软件冬奥版在更新至 Windows11 版本后，还提供了高性能模式和流畅模式，以满足不同机器性能的用户需要。

构建网络安全第一道防线 奇安信发布“安全 DNS”公共服务 QDNS

7 月 7 日，奇安信集团在京发布域名安全体系研究报告及“安全 DNS”公共服务 QDNS，为政府、企业以及个人用户提供全方位的域名安全防御服务与解决方案。

作为 DNS 安全威胁的缓解和解决方案，奇安信安全 DNS（QDNS）基于奇安信威胁情报中心商业威胁情报，能够对 APT 攻击、勒索软件、窃密木马、远控木马、僵尸网络、网络蠕虫、恶意下载、黑市工具、流氓推广等几十种网络威胁请求进行有效检测和阻断；产品使用的恶意域名库由多名安全专家、应急专家动态更新维护，保障了对最新威胁的实时防护能力；产品威胁请求阻断充分考虑域名解析过程，能有效阻断 DNS 隐蔽通信并防止用户信息泄露。

据介绍，在试运行阶段，仅 2021 年 6 月，奇安信安全 DNS 已对公众提供域名解析服务 570 亿次，解析域名近 2 亿，拦截威胁域名请求 1800 万次，涉及威胁域名 15 万。

全面适配鸿蒙 OS 奇安信移动办公安全产品和解决方案护航政企客户

奇安信旗下移动零信任、移动安全空间、移动终端安全管控、移动应用安全自防护和云手机等全线移动办公安全解决产品和解决方案，已完成与鸿蒙 OS 兼容性测试工作，为广大政企客户的移动办公保驾护航。

结合鸿蒙 OS 的分布式安全能力，奇安信能够为鸿蒙用户提供云网端一体化全链路移动办公安全能力，为政企机构提供移动安全态势感知，帮助客户打造移动安全监测、响应、预测和防御的闭环立体安全防御体系。截至目前，奇安信已为大量使用鸿蒙系统的政企客户，完成了相关移动办公安全产品的升级工作。

奇安信发布云天眼 全力提升云上实战攻防安全感知能力

近日，奇安信正式发布云天眼 · 新一代安全感知系统（简称云天眼）。云天眼以攻防渗透和数据分析为核心竞争力，面向安全服务和分析人员提供一套建在“云”上的监测预警、威胁检测、溯源分析和响应处置的高级威胁检测平台。

据介绍，在企业业务云化、互联网化的趋势下，云天眼完美“平移”了本地化天眼安全感知系统的各项攻防能力，能够支持阿里云、腾讯云、亚马逊 AWS、VMware 等主流云计算架构和虚拟化平台，与云上现有的防御体系构建起互补完整的安防体系，重点解决云上全网安全在东西向流量上监控盲区的问题，助力保障企业的云上安全。

北京市政协委员齐向东：做好数字化时代网络安全的守护者

奇安信集团党委书记、董事长齐向东在庆祝中国共产党成立 100 周年大会现场表示：“习近平总书记的讲话铿锵有力，振奋人心，让人热血沸腾。中国共产党带领中国人民告别了饱受欺凌的时代，建设了一个新世界。在新征程上，企业家要担起新使命。”

“我们做网络安全的，要深刻认识现在数字技术革命和产业革命的机遇期，以及错综复杂的国际环境带来的新矛盾、新挑战，逢山开道、遇水架桥，把网络安全核心技术牢牢掌握在自己手中，走出一条自主创新之路，做好数字化时代网络安全的守护者，为全面建成社会主义现代化强国、实现第二个百年目标不懈奋斗！”

奇安信圆满完成“2021 建党 100 周年”网络安全保障工作

2021 年 7 月 1 日，庆祝中国共产党成立 100 周年大会在北京隆重举行。作为网络安全领军企业，奇安信在网络安全主管部门的统筹部署下，圆满完成了此次网络安保任务。

为切实做好建党 100 周年系列活动期间网络安全稳定运行，奇安信成立了网络安全保障专项工作组，在全国范围内累计投入 5000 人 / 天，全面落实了各项安全工作和防护措施，保障了建党 100 周年系列活动的顺利进行，获得了主管部门的高度认可。在全体工作人员的共同努力下，活动期间未发生一起重大网络安全事件。

奇安信助力青海省 2021 年网络安全应急演练活动顺利举办

近日，由奇安信集团承办的 2021 年青海省网络安全应急演练活动在西宁顺利举行，演练活动旨在进一步加强青海省网络安全防护能力，检验应急处置队伍技术保障和协同处置能力水平。

演练活动由青海省委网信办主办，青海省交通运输厅、国家税务总局青海省税务局、青海银行、国家计算机网络和信息安全管理中心青海分中心 4 家单位协办，青海民族大学、奇安信集团承办。来自全省各市州委网信办、省直各部门、中央驻青各单位、各人民团体、各高等院校等 80 多家单位网络安全工作业务部门的负责人进行了现场观摩。

奇安信成为重庆市网络安全应急支撑单位

近日，奇安信科技集团入选了重庆市委网信办2021年度重庆市网络安全应急支撑单位，将参与重庆市委网信办相关网络安全保障及事件的应急处置工作。本次支撑单位的选拔，旨在进一步加强重庆市网络安全技术支撑体系的建设，强化网络安全事件应急处置能力，提升网络安全工作保障水平。

2020年，奇安信获得了“2020年重庆市网络安全优质服务企业”荣誉；在今年成立的重庆市网信事业发展专家咨询委员会上，奇安信集团总裁吴云坤受聘担任“网络安全专家咨询委员会”委员。


聘书
LETTER OF APPOINTMENT

荣誉墙

奇安信终端安全两项方案入选工信部“2020年信息技术应用创新解决方案”

2021年信息技术应用创新产业发展高峰论坛暨2020年信息技术应用创新典型解决方案发布会上，“2020年度信息技术应用创新解决方案”征集成果公布，奇安信“信创终端一体化终端安全解决方案”和“金融行业信创过渡期终端安全建设方案”成功入选。其中，金融信创过渡方案更是凭借“技术先进、应用示范、产业带动”的特性获评单项创新奖。

本次解决方案评选是在工业和信息化部信息技术发展司指导下，工业和信息化部网络安全产业发展中心（工业和信息化部信息中心）联合信息中心技术创新应用协作组启动开展，旨在以技术先进、应用示范、产业带动为创新指数考量，遴选单项指标突出、特征明显的解决方案。

奇安信也成为唯一一家入选两项解决方案的网络安全公司，同时也是唯一获得创新奖的网络安全公司，进一步验证了奇安信在信创终端安全领域的技术实力和市场领先地位。

进阶认证！奇安信荣获工业信息安全测试评估机构能力认定二级

近日，凭借自身在工业信息安全领域长期技术积累的优势，奇安信旗下网神被评选为“工业信息安全测试评估机构（二级）”，是当前该能力认定的最高等级。

工业信息测试评估机构根据机构规模、技术能力、服务水平等划分为三级，经企业自主申报、资格初审、专家认定等认定工作，旨在遴选一批能面向各类工业控制系统、工业互联网及相关系统和产品开展的安全技术测试、系统评估、产品检测、能力比对测试的企业。

2019年6月，在中国工业信息安全大会上，奇安信荣获首批“工业信息安全产业发展联盟－工业信息安全测试评估机构能力认定三级证书”，有效期2年。今年，依据工业信息安全产业发展联盟《工业信息安全测试评估机构管理办法》，奇安信获得了“工业信息安全测试评估机构”二级的认定等级，提升一级，同时也是当前该能力认定的最高等级。


NISIA
工业信息安全产业发展联盟
工业信息安全测试评估机构能力认定证书
（二级）
网神信息技术（北京）股份有限公司
符合工业信息安全测试评估机构管理办法二级要求
特发此证

奇安信

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

奇安信图书馆






网络安全科普系列




网络安全实战系列



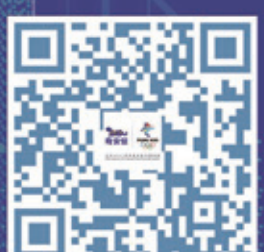
国际经验分享系列




网络安全认证系列




网络安全教育系列



扫码购书

奇安信致力于网络安全科普、教育、认证与实战，基于国内外先进实践及理念，编撰并翻译系列网络安全丛书。