SECURITY INSIDER

网安26号院

奇安信网络安全通讯 · 安全快一步

紧盯中国的全球APT组织

P14

第10期

2021 年 10 月

奇安信

敏感信息泄露情报服务

- 攻击队视角的全网敏感信息情报
- 急需补上的防守盲点
- 供应链安全的管控抓手
- 预防性进攻反制利器

纵深防御的马奇诺防线，为什么会被攻破？

- 完整的防御体系，既要考虑正面防御，侧翼的情报收集和对抗也必不可少！
- 忽视全网视角的情报，是防守的重大盲点！

服务定位 SERVICE POSITIONING

- **攻击队视角**：使用渗透专家交付，不是简单的信息收集。
- **全网视角**：核心功能是从外部探测全互联网第三方应用中的敏感泄露数据；而非只关心自己的网络和应用。
- **情报级**：专家梳理的情报级信息，而不是简单数据抓取：给出利用思路和可能的攻击链，更有详细的整改建议。

奇安信安服团队

从成本中心到价值创造

最近，在阅读一份报道时，有记者提出“安全价值”的问题。这可能是很多网络安全主管比较挠头的问题：说不清网络安全工作的价值。

通常情况，安全工作者说到安全的价值，往往会提到两个方面：减少数据泄露风险；避免对机构品牌声誉的损害（这里也包括对高管个人的影响）。这是网络安全价值的重要贡献，但并非全部。

长期以来，网络安全工作被视为只出不进的成本中心，对业务创新的掣肘和限制。面对后疫情的下一个常态，政企都在加快数字化转型的进程。要使任何数字化转型项目取得成功和实现价值，必须将网络安全视为基础。

在数字化转型深化之际，安全工作需要提升关键信息基础设施安全防护水平，做到增量同步建设和存量能力补课并举，以有效保障数字化转型。

安全主管可以按照风险管理方式，量化展现网络安全的工作价值：将网络安全工作构想为价值驱动要素和“利润中心”，超越“成本中心”思维，这可能是一个疯狂的想法，但却有助于赢得高层对安全工作的更多认可与支持。

对安全工作可以考核其对核心业务目标的影响，计算为企业节省的资金，避免的网络攻击经济损失——这可能比网络安全的建设成本高得多。

网络安全部门可以像 IT 服务管理一样，看作是内部服务提供者，来满足各个业务部门的需求。这样，网络安全服务可以根据使用情况分配成本，出现在每个业务部门预算中，而不是计入企业开销。网络安全投入决策由忽略所可能给业务造成的损失所驱动。

强大安全能力可以使企业更好地开展业务、更快更顺利地实现创新，从而在竞争激烈的市场中获得优势，产生真正的价值回报。尤其是越来越多的业务都与“数据”相关。维护了数据的安全，就等于赋能和推动了业务创新。用业务语言可以清楚地展示它如何帮助增加公司利润。

如果没有安全团队，企业经营状况会明显恶化。将网络安全从成本中心转变为利润中心，将是 CISO 所面临的领导力挑战：拥抱业务，基于业务战略与目标对安全定价，有助于更清晰展示安全价值。

总编辑

李建平

2021 年 10 月 1 日

CONTEN

目录

安全态势

月度专题

紧盯中国的全球APT组织 P14

2021 年上半年，国家级组织持续针对我国境内开展攻击活动，盘点一下针对我国的 APT 组织。

TS

第 10 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

事件篇

大型组织勒索攻击事件持续高发，美国媒体巨头辛克莱遭勒索攻击，旗下多个电视电台节目停播；英国工程巨头伟尔集团遭勒索攻击，运营临时中断致使损失超 4 亿元；美国一医院遭勒索攻击致使一婴儿死亡，涉事机构被起诉……

阿根廷政府公民数据库疑全部泄露，攻击者待价而沽

据 The Record 10 月 18 日消息，有匿名黑客在推特上泄露了阿根廷总统阿尔贝托 · 费尔南德斯、球星梅西和阿圭罗等数十位阿根廷名人的身份证信息，并在黑客论坛上发帖，兜售阿根廷公民身份数据查询权限。阿根廷内政部回应称，公民数据库 RENAPER 没有出现数据泄露事件。但匿名黑客随后表示，掌握了 RENAPER 的全部数据副本，并向记者展示了查询能力，称可能公布一批百万级的公民数据样本，将继续对外兜售数据访问权限。

美国媒体巨头辛克莱遭勒索攻击，旗下多个电视电台节目停播

据 The Record 10 月 17 日消息，美国最大电视运营商之一辛克莱广播集团遭遇勒索软件攻击，部分业务中断，涉及内部企业网络、邮件服务、电话服务、电视台广播系统等。受攻击影响，部分电视频道无法播放预定的节目，如早间节目、新闻节目及体育赛事等，只能替换为其他视频内容，以保证频道处于工作状态。大型电视台和广播电台遭遇勒索软件攻击、被迫中断节目播放的事件并不罕见，此前美国考克斯传媒集团、法国 M6 电视台等均遭遇过。

宏碁电脑今年第二次被黑，印度经销数据全泄漏

据 Bleeping Computer 10 月 14 日消息，在黑客论坛已经流出泄露数据后，宏碁电脑披露称，印度分部的售后服务系统被黑，正在应急响应，公司运营未受到重大影响。攻击者声称，窃取了宏碁超 60GB 内部数据，涉及数千家印度零售和分销商的财务数据、客户数据、登录凭证等商业秘密信息。这是宏碁今年第二次遭受重大网络攻击，今年 3 月，该公司遭 REvil 勒索软件攻击，对方索要了当时创纪录的 5000 万美元赎金。

挖矿木马盯上华为云，利用“配置错误”发动攻击

据 Bleeping Computer 10 月 11 日消息，趋势科技研究员发现，攻击者正使用新版 Linux 挖矿木马瞄准华为云用户。新版木马会禁用华为云 Linux 代理进程 hostguard、华为云用户重置密码的代理进程

cloudResetPwdUpdateAgent 等安全相关默认程序，并拥有较高的隐蔽和防删除能力。新版木马主要利用云服务配置错误发动攻击，如弱密码、未授权访问漏洞等。

英国工程巨头遭勒索攻击：运营临时中断至少损失 4 亿元

据 Bleeping Computer 10 月 8 日消息，英国工程巨头伟尔集团（Weir Group）披露，今年 9 月遭受了一起勒索软件攻击，导致出货、制造与工程系统发生中断。这起攻击令伟尔集团损失惨重，仅 9 月，因开销不足与收入延后带来的间接损失高达 5000 万英镑，预计下一财季业绩将受到影响。目前未发现任何数据泄露或加密情况。

披露：SolarWinds 黑客窃取了美国政府的绝密数据

据路透社 10 月 7 日消息，美国相关官员透露，最新调查显示，SolarWinds 黑客窃取的信息包括针对俄罗斯反情报（反间谍）调查情况、对俄个人的制裁政策及美国官方对新冠肺炎疫情的反应等内容。该官员认为，此次黑客事件最严重的损失，是针对俄罗斯的反情报活动被曝光，不过美国司法部发言人对此未予置评。

东京奥运会期间系统遭到超 4 亿次网络攻击

据共同社 10 月 6 日消息，东京奥组委透露，7 月 23 日—9 月 5 日东京奥运会和残奥会期间，约有 4.5 亿次针对奥运会官方网站及组委会系统的网络攻击被成功阻止。针对东京奥运会的网络攻击规模少于 2012 年伦敦奥运会和 2018 年平昌冬奥会，安全厂商认为可能与疫情期间没有门票和观众信息有关。据悉，伦敦奥运会期间共发生约 23 亿次网络攻击，平昌奥运会期间约发生 6 亿次网络攻击。

勒索攻击致使一婴儿死亡，涉事医疗机构被起诉

据 SecurityWeek 10 月 2 日消息，美国阿拉巴马州一名 9 个月大的女婴意外死亡后，婴儿母亲对接生的医院提起诉讼，声称医院没有披露其网络系统因网络攻击瘫痪，导致出生期间护理不足，最终致使婴儿死亡。她表示，如果知道该医院受影响的真实程度，她会去其他更安全的医院进行分娩。这是目前公开报道的第二起勒索软件致死案例，此前 2020 年 9 月，德国一家医院遭到勒索攻击，一名急诊病人错过最佳抢救时间，最终死亡。

美国重要港口计算机网络遭黑客入侵，但运营未受影响

据 CNN 9 月 23 日消息，美国海岸警卫队网络司令部的事件分析报告披露，墨西哥湾沿岸重要港口休斯敦港在 8 月曾遭受网络攻击，攻击者疑似有国家背景。幸运的是，官方早期调查发现了入侵者，尚未对港口的船运活动进行干扰。有传言称，休斯敦港事件是一起更大范围网络入侵的组成部分。据悉，入侵的黑客们把目标锁定在防务承包商、运输企业和其他组织身上。官方网站显示，休斯敦港每年的货物吞吐量可达 2.47 亿吨，是墨西哥湾沿岸最大的港口之一。

漏洞篇

10月，Oracle官方发布了2021年10月的关键安全补丁集合更新，修复多个WebLogic安全漏洞；缺陷修复引发新问题，Apache Tomcat披露拒绝服务漏洞；奇安信CERT研判发现，近期需重点关注23个高风险漏洞……

Oracle WebLogic多个组件漏洞安全风险通告

2021年10月20日，Oracle官方发布了2021年10月的关键安全补丁集合更新（Critical Patch Update），修复了多个存在于WebLogic中的漏洞，包括CVE-2021-35617、CVE-2021-35620、CVE-2021-35552。经过技术研判，奇安信CERT认为CVE-2021-35617（WebLogic Server远程代码执行漏洞）影响较为严重。由于漏洞危害性较大，奇安信CERT建议客户尽快应用本次关键安全补丁集合。

Apache Tomcat拒绝服务漏洞安全风险通告

2021年10月15日，奇安信CERT监测到Apache基金会公布了Apache Tomcat拒绝服务漏洞（CVE-2021-42340）。由于历史bug 63362的修复，一旦WebSocket连接关闭，用于收集HTTP升级连接的对象就不会针对WebSocket的连接释放，从而引发内存泄漏，恶意攻击者可以通过OutOfMemoryError利用该漏洞触发拒绝服务。鉴于漏洞危害较大，建议客户升级到最新版本。

微软10月补丁日多个安全漏洞预警

2021年10月14日，国家漏洞库CNNVD发布预警，微软官方发布了多个安全漏洞的公告，包括Exchange Server权限许可和访问控制问题漏洞（CVE-2021-26427）、Office代码注入漏洞（CVE-2021-40479）等多个漏洞，其中超危漏洞1个，高危漏洞41个。成功利用上述漏洞的攻击者可以在目标系统上执行任意代码、获取用户数据、提升权限等。微软多个产品和系统受漏洞影响。目前，微软官方已经发布了漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

Node.js多个HTTP请求走私漏洞安全风险通告

2021年10月12日，Node.js官方发布新版本v12.22.7，修复了两个HTTP请求走私漏洞。其中CVE-2021-22959是由于标头空格问题导致漏洞产生，CVE-2021-22960是解析正文中出现了HTTP请求走

私。Node.js 是一种可使 JavaScript 在浏览器中执行的服务器端技术。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 HTTP Server 目录遍历漏洞安全风险通告

2021 年 10 月 8 日，奇安信 CERT 监测到 Apache 基金会发布 Apache HTTP Server 2.4.51 版本，修复了 Apache HTTP Server 2.4.49 和 2.4.50 版本中存在的路径遍历和远程代码执行漏洞（CVE-2021-42013），官方定级为严重。目前，该漏洞的细节、PoC 及 EXP 均已在互联网上公开。据奇安信 Hunter 平台统计，国内受影响版本的服务器约 2000 台。鉴于其影响较大，建议客户尽快自查修复。

江森自控旗下 ExacqVision 视频监控系统高危漏洞风险通告

2021 年 10 月 7 日，国际知名建筑技术厂商江森自控披露了旗下 ExacqVision 视频监控系统两个高危安全漏洞。其中，CVE-2021-27664 是一个特权账号访问漏洞，CVSS 评分 9.8，未经授权的攻击者可以远程查看服务器信息乃至控制服务器；CVE-2021-27665 是一个拒绝服务漏洞，CVSS 评分 8.8，攻击者可远程发送特殊的请求包令服务器崩溃。目前，官方已经发布了漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

Chrome 浏览器多个漏洞遭在野利用风险通告

2021 年 9 月 30 日，谷歌官方发布了 Chrome 浏览器 v94.0.4606.71，修复了 4 个安全漏洞，其中有两个漏洞遭到在野利用，分别是 V8 引擎中的释放后使用缺陷（CVE-2021-37975）和内核信息泄露漏洞（CVE-2021-37976），建议用户尽快更新至最新版本。今年以来，Chrome 浏览器已经修复了 14 个遭在野利用的 0day 漏洞。

VMware vCenter Server 多个安全漏洞预警

2021 年 9 月 24 日，国家漏洞库 CNNVD 发布预警，VMware 官方发布了多个安全漏洞公告，包括 VMware vCenterServer 授权问题漏洞 (CVE-2021-22017)、VMware vCenterServer 权限许可和访问控制问题漏洞 (CVE-2021-21991) 等 9 个漏洞。VMware vCenterServer 6.5、VMware vCenterServer 6.7、VMware vCenterServer 7.0 版本均受漏洞影响。成功利用上述漏洞的攻击者无需用户交互及认证即可实现远程代码攻击，最终完全控制相关设备。目前，VMware 官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

奇安信 CERT：近期需重点关注的 23 个高风险漏洞

2021 年 9 月，奇安信 CERT 监测到新增漏洞 2658 个。经人工研判，本月值得重点关注的漏洞共 128 个，其中高风险漏洞共 23 个，包括多个 VMware vCenter Server 高危漏洞、多个 Apache Dubbo 高中危漏洞、遭在野滥用的微软 MSHTML 引擎漏洞等，约三成漏洞的细节和 PoC 已公开或遭到在野利用。

（关注公众号“奇安信 CERT”，发送“202109”可查看 9 月需重点关注的漏洞完整清单）

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

2021 年 9 月，奇安信 Z-TEAM 团队共承接攻防演习服务 20 场，其中，省级攻防演习 1 场，省级行业攻防演习 1 场，行业级攻防演习 1 场，地市级攻防演习 7 场，本单位自主攻防演习 10 场。

本月攻防演习成果：

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	14	25	98	45	4	42	113	213

二、本月任务目标特点

本月攻防演习和评估任务覆盖行业比较集中，以金融、教育、科研及运营商为主，客户存在的安全问题主要涉及互联网侧应用组件存在漏洞缺陷、内部人员对钓鱼攻击防范意识不足、内网功能区域缺乏安全隔离、内

网访问权限策略设置不严、内网口令复用及弱口令普遍等。具体情况如下：

1、漏洞利用是主要突破手段

本月任务中针对多行业不同目标网络，漏洞利用在外网突破中占据了主要部分。被攻陷目标互联网侧应用漏洞以平台组件漏洞为主，如外部应用中 Struts2 组件漏洞、SQL 注入漏洞、Shiro 反序列化漏洞、Apache solr 远程命令执行、Fastjson 命令执行漏洞等，多因外部应用及系统组件更新不及时造成，直接给目标网络带来了严重的安全隐患。

2、钓鱼攻击具有较高成功率

本月任务中针对特殊行业目标网络，钓鱼攻击在外网突破中占比有所提升，主要是由于金融、运营商、科研这类目标客户网络相比其他行业具有更高的安全要求，整体网络安全外部防护相对严密，对其内部网络安全意识比较薄弱的人员开展钓鱼攻击就成为了实现外部突破比较高效的手段。

3、弱口令仍是内网严重安全隐患

本月任务中目标内网弱口令和口令复用问题依旧比较突出，在内网横向拓展中仍是主要实现手段，通过弱口令或口令复用可轻易实现对内网重要服务器、网关路由、网管系统和域控等核心网络节点的拓展控制，致使业务内网毫无安全防护可言。

4、敏感信息泄露安全威胁严重

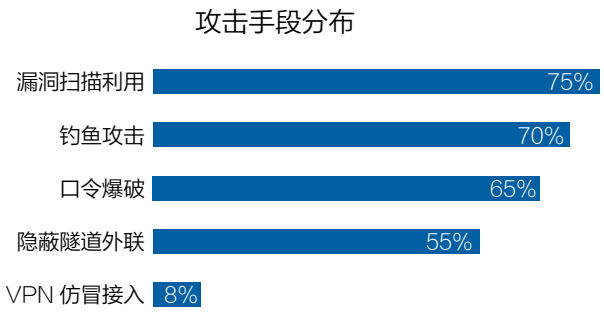
本月任务中目标网络敏感信息泄露较为严重，包括 URL 目录文件信息、Web 后台系统、应用开发平台及后台登录地址、内网接口、安全认证信息在内的敏感源码泄露等，这些敏感性信息泄露多是由于安全意识不足致使安全配置疏漏、平台审核不严导致的，此类敏感信息常常被用来实现针对性的快速突破渗透。

5、业务网络缺乏纵深防御机制

本月任务中目标网络关键业务安全防护缺乏纵深防御机制，存在互联网侧服务器和核心内网没有逻辑隔离的情况，内网安全部署缺乏功能域划分、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拓展渗透。

三、主要攻击手段分析

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



1、漏洞扫描利用

本月任务中漏洞利用主要集中在互联网侧 Web 应用或网络平台组件，主要以网络组件反序列化漏洞、敏感信息泄露、SQL 注入和未授权访问为主。这些漏洞主要是由系统组件更新不及时、安全策略设置缺陷引起的，直接反映出客户网络运维人员安全意识不足、网络运维缺乏常态巡检机制、对存在的漏洞及安全威胁实时应对不够高效等问题。

2、钓鱼攻击

本月任务中钓鱼攻击主要是针对金融行业目标人员，因金融行业安全体系建设比较完善、防护相对严密，互联网侧系统可利用漏洞和其他突破途径较少，所以外部主要从客户中安全意识相对薄弱的客服、人事及商务等内部目标人员实现钓鱼突破，内网钓鱼则主要针对网络运维、平台研发及核心业务人员等目标实现重点突破。

3、口令爆破

本月任务中口令爆破主要体现在弱口令和口令复用，目标网络外部应用认证入口通过弱口令爆破实现突破，内网横向拓展过程中弱口令、口令复用则较为普遍，主要原因是目标网络缺乏对弱口令和通用口令的统一治理，没有对账号口令设置和使用进行安全规范要求，如对密码复杂度提出要求、禁止使用通用账号口令、账号口令定期更新等。

4、隐蔽隧道外联

本月任务中因客户行业特殊，业务内网均无法直接从外网直连访问，虽然大部分目标网络缺少纵深防御部署，但依然需要借助端口转发、隧道技术等手段实现转发通信，对于网络功能区划分严格、核心业务隔离措施完善的内部网络，往往需要借助多层隧道转发才能实现对目标核心业务内网的渗透拓展。

5、VPN 仿冒接入

本月任务中行业目标网络核心业务相对集中，对 VPN 入网范围限制较严，只有少量目标业务网络通过 VPN 仿冒接入实现渗透，利用手段包括外网通过 VPN 网关漏洞利用、内网通过口令复用获取 VPN 认证信息等。

四、典型攻击手段实现案例

1、外部漏洞利用突破

（1）某目标互联网业务管理系统存在 Apache Struts2 远程代码执行（s2-005）漏洞，通过漏洞利用获取该管理系统权限。

（2）某目标 Web 平台系统存在 Shiro 远程命令执行漏洞，通过漏洞利用获取该系统后台服务器控制权限。

（3）某目标控制系统存在远程代码执行漏洞，通过漏洞利用获取数据库管理权限 5 个、内网服务器 7 台、敏感数据 1 万余条。

2、钓鱼攻击

（1）通过某目标官网招聘栏上找到的 HR 联系方式，添加微信向其投递木马文件，获取网站后台权限。

（2）直接针对某目标内部研发人员进行社工钓鱼，使用校招身份在 QQ 上发送文件，进一步获取内网服务器权限。

（3）针对某目标公众号中找到的投递稿件邮箱并进行投稿，利用钓鱼获取主机终端权限。

3、口令爆破

（1）某目标网络内网堡垒机存在弱口令，通过弱口令登录获取该堡垒机控制权限，可直接管控内网主机近 700 台。

（2）某目标 OA 系统存在弱口令，可直接登录 OA，并进一步获取内网办公业务、人员通信等敏感信息。

（3）某目标业务人事系统存在弱口令，可直接登录访问该系统，并对内部人员档案信息进行查询操作。

4、VPN 仿冒接入

（1）针对某客户网络内部人员成功钓鱼并控制该人员主机，从其主机上搜集敏感信息，获得目标内网 VPN 网络访问权限，成功进入目标内网。

（2）针对某客户网络，通过组合用户名与弱口令字典成功爆破控制目标网络边界设备，并获得 VPN 服务器访问权限，成功接入目标内网。

政策篇

国内，我国首次对打击治理电信网络诈骗进行专门立法，《反电信网络诈骗法》草案进入立法审议阶段；行业监管加力，工信部《工业和信息化领域数据安全管理办法（试行）》公开征求意见。

国际上，美国总统拜登签署《2021 年中小学（K-12）网络安全法案》，该法案是美国首部针对中小学的网络安全法案；新加坡网络安全局发布《2021 网络安全战略》，提出三大战略支柱和两大基础要素。

五部门联合发布《关于规范金融业开源技术应用与发展的意见》

2021 年 10 月 20 日，人民银行办公厅等五部门联合发布《关于规范金融业开源技术应用与发展的意见》。《意见》要求金融机构在使用开源技术时，应遵循“安全可控、合规使用、问题导向、开放创新”等原则。《意见》鼓励金融机构将开源技术应用纳入自身信息化发展规划，加强对开源技术应用的组织管理和统筹协调，建立健全开源技术应用管理制度体系，制定合理的开源技术应用策略；鼓励金融机构提升自身对开源技术的评估能力、合规审查能力、应急处置能力、供应链管理能力等。

《反电信网络诈骗法》草案已进入立法审议阶段

2021 年 10 月 18 日，全国人大常委会法制工作委员会举行记者会称，将于 10 月 19 日至 23 日在北京举行全国人大常委会第三十一次会议，包括反电信网络诈骗法草案在内的 9 件法律案将提请会议初次审议。这将是我国首次对打击治理电信网络诈骗进行专门立法。据悉，草案内容主要包括：完善电话卡、物联网卡、金融账户、互联网账号有关基础管理制度；建立电信网络诈骗反制技术措施，统筹推进跨行业、企业统一监测系统建设，为利用大数据反诈提供制度支持；加强对涉诈相关非法服务、设备、产业的治理等。

《工业互联网安全标准体系（2021 年）》公开征求意见

2021 年 10 月 9 日，在工信部网络安全管理局指导下，工业互联网产业联盟等多组织联合编制了《工业互联网安全标准体系（2021 年）》，现公开征求意见。工业互联网安全标准体系包括分类分级安全防护、安全管理、安全应用服务等 3 大类别、16 个细分领域及 76 个具体方向。该文件发布后，将加快建立工业互联网安全分类分级管理制度，指导工业互联网企业提升网络安全防护能力。

信安标委发布《汽车采集数据处理安全指南》

2021 年 10 月 8 日，全国信息安全标准化技术委员会发布了《汽车采集数据处理安全指南》。本文件规定了对汽车采集数据进行传输、存储和出境等处理活动的安全要求，包括汽车不应通过网络向外传输座舱数据，车外数据、座舱数据、位置数据不应出境，运行数据出

境需通过国家网信部门安全评估等。本文将适用于汽车制造商开展汽车的设计、生产、销售、使用、运维，也适用于主管监管部门、第三方评估机构等对汽车采集数据处理活动进行监督、管理和评估。

工信部《工业和信息化领域数据安全管理办法（试行）》公开征求意见

2021 年 9 月 30 日，工信部发布《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》公开征求意见。《办法》提出，工业和电信数据处理者收集数据应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。数据收集过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。

美英法等 30 余国共同发布反勒索软件联合声明

2021 年 10 月 14 日，由美国举办的反勒索软件倡议会议上，美英法等 30 余国发布联合声明，将共同采取行动，努力提高网络韧性，做好事件预防和响应；打击滥用金融机制洗钱或从事其他使用勒索软件获利的活动；通过执法合作破坏勒索软件生态系统，调查和起诉勒索软件参与者；利用外交手段消除勒索软件犯罪分子的避风港等。

美国总统拜登签署《2021 年中小学网络安全法案》

2021 年 10 月 8 日，美国总统拜登签署《2021 年中小学（K-12）网络安全法案》，使其正式生效。该法案是美国首部针对中小学的网络安全法案。法案指示网络安全和基础设施安全局（CISA）研究中小学面临的网络风险，并制定建议，协助学校面对这些风险。研究将评估学校在保护其系统和学生 / 雇员敏感数据上面临的挑战。CISA 有 120 天时间来完成审查并向国会报告。法案还要求联邦机构为学校官员开发在线培训工具。

美国管理与预算办公室发布备忘录，改进联邦系统网络安全漏洞和事件检测

2021 年 10 月 8 日，美国白宫管理与预算办公室（OMB）发布备忘录（M-22-01），通过部署端点检测与响应（EDR）改进联邦政府系统的网络安全漏洞和事件检测。该备忘录将为各联邦机构提供指引，加快推动部署 EDR 解决方案。具体而言，将通过集体努力实现第 14028 号行政令提到的三大目标：提高机构对其网络上网络安全事件的早期检测、响应和补救能力；实现机构内部跨部门 / 局 / 子机构的企业级可见性；通过 CISA 部署的集中式 EDR 实现整个联邦政府信息系统的主机级可见性、归因和响应。

新加坡网络安全局发布《2021 网络安全战略》

2021 年 10 月 5 日，新加坡网络安全局发布《2021 新加坡网络安全战略》。这是新加坡政府的第二份网络安全战略文件，上一份为 2016 年发布。新版文件剖析了当前技术环境，边缘计算、量子计算等潜在颠覆技术即将到来，威胁者手段越发老练，并擅长滥用泛在的联网设备。为此，文件提出三大战略支柱和两大基础要素，包括建设弹性基础设施、实现安全网络空间、加强国际网络合作及发展活力的网络安全生态系统、发展强健的网络人才通道。

奇安信

奇安信威胁情报中心

中国威胁情报行业领军者

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。

威胁情报中心

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

紧盯中国的全球APT组织

紧盯中国的全球 APT 组织

作者 奇安信威胁情报中心

2021 年上半年，网络武器威力和攻击规模持续增大，可能是近年来 APT 攻击活动最黑暗的半年。全球 APT 组织为达到攻击目的，不惜花费巨额资金和人力成本，使用的在野 0day 漏洞数量陡然剧增，出现的频次之高历年罕见。

在新冠疫情、地缘政治等复杂背景下，针对我国的高级威胁持续不断。2021 年上半年，毒云藤、蔓灵花、海莲花等国家级攻击组织，持续针对我国境内开展攻击活动。我们来盘点一下紧盯我国的全球 APT 组织。

南亚篇

1、摩诃草（APT-Q-36）

【组织概述】

摩诃草组织是 Norman 于 2013 年披露并命名的 APT 组织。其最早攻击活动可以追溯到 2009 年 11 月，该组织主要针对中国、巴基斯坦等亚洲地区和国家进行网络间谍活动。

在针对中国地区的攻击中，主要针对政府机构、科研教育领域进行攻击。具有 Windows、Android、Mac OS 多系统攻击的能力。

【攻击事件】

2018 年春节前后，某政府单位收到一些带有恶意下载链接的钓鱼邮件，邮件内容与其工作相关，一旦目标用户下载并打开 office 文档，则会触发漏洞 CVE-2017-8570 并执行恶意脚本，最终下载远控木马导致主机被控。

此外，摩诃草组织在本次攻击活动中注册了大量与我国敏感单位 / 机构相关的相似域名，以对我国特定的领域进行定向攻击。奇安信威胁情报中心通过对此次攻击活动中大量网络资产分析发现，其中一个 IP 地址曾在摩诃草历史的攻击活动中被披露使用，因此将此次攻击的幕后团伙判定为摩诃草 APT 组织。

2、蔓灵花（APT-Q-37）

【组织概述】

蔓灵花（Bitter）最早由国外安全厂商 Forcepoint 于 2016 年命名，研究人员发现其 RAT 变种在进行网络通信时往往包含有“BITTER”字符，故将行动命名为 BITTER。该组织至少自 2013 年 11 月开始活跃，长期针对中国及巴基斯坦的政府、军工、电力、核等部门发动网络攻击，窃取敏感资料。

【攻击事件】

2018 年 1 月，某工业大厂员工收到一份钓鱼邮件，

邮件声称来自该厂信息技术中心，提醒员工邮件账户登录异常，并要求员工通过“安全链接”验证邮件账户。该“安全链接”为高度仿造的企业邮箱登录页面，目标用户在此页面输入账号密码后将被攻击者收集用于向帐户内的其他用户发送带有病毒附件的邮件。附件被执行后将导致机器被种植后门木马。

奇安信威胁情报中心通过对钓鱼链接的域名跟踪分析，发现国内疑似被攻击的组织机构还包括中国 XXXX 集团有限公司、中国 XX 对外工程有限公司以及 XXXXXX 大学。

经过关联分析，奇安信威胁情报中心发现此次攻击活动中伪装成 JPG 图片的恶意样本释放的诱饵图片与蔓灵花组织在 2016 年的攻击活动中所使用的诱饵图片完全一致。此外，此次攻击活动发现的后门程序中查找 avg 杀软的相关代码片段与蔓灵花组织使用的相关代码片段也存在高度相似性。因此将此次攻击活动判定为蔓灵花 APT 组织所为。

3、魔罗纱（APT-Q-39）

【组织概述】

Confucius 组织是 Palo Alto Networks Unit 42 于 2017 年 10 月发现的攻击团伙，该团伙主要使用网络钓鱼邮件针对巴基斯坦目标实施攻击。

2017 年末趋势命名 Confucius 为 APT 组织，并分析了其与 Patchwork 存在一些联系。趋势科技表示，至少从 2013 年就发现该组织活跃，使用 Yahoo! 和 quora 论坛作为 C&C 控制器，该组织可能来自于南亚。该组织拥有对 Windows，Android 的攻击恶意代码，并常用 Delphi 作为其 Dropper 程序。

从奇安信威胁情报中心内部的威胁情报数据分析来看，这两个组织可以通过相似的 Delphi Dropper 程序使用的控制域名联系到一起。但其与摩诃草的主要不同在于攻击目标主要以巴基斯坦和印度为主，并通常伪装成俄罗斯的来源。

由于 APT-Q-39 属于攻击境内目标的境外组织，因此奇安信威胁情报中心对 APT-Q-31 组织的命名为魔株系——魔罗杪，“魔罗”出自该组织的地域教派神话，意为乱人事者。“杪”则象征该组织的地缘及文化特征。

【攻击事件】

2020 年 9 月，奇安信威胁情报中心披露了来自南亚地区的定向攻击：提菩行动。在此次活动中，攻击者使用了多种攻击手法例如：钓鱼邮件 + 钓鱼网站、钓鱼邮件 + 恶意附件、木马文件投放、安卓恶意软件投放，其中还包括部分商业、开源木马的使用以增加分析人员的溯源难度。

通过对提菩行动的攻击目标侧分析发现，此次活动主要针对中国、巴基斯坦、尼泊尔等地区的航空航天技术部门、船舶工业业、核工业 (含核电)、商务外贸、国防军工、政府机关 (含外交)、科技公司。其主要目的为窃取特定国家的核心国防军工技术。

奇安信威胁情报中心红雨滴团队基于内部大数据平台，对此次攻击活动中使用的恶意软件分析后发现，AsyncRat 回连的 C2 可关联到多个魔罗杪组织曾用特马，且部分样本曾被用于针对巴基斯坦缉毒部的攻击中。

此外，研究人员还追踪到此次攻击活动中的 SFX 类型样本与魔罗杪历史针对巴基斯坦 WIL 兵工厂活动中的样本同源。因此，奇安信对此次活动背后的组织判别为境外 APT 组织魔罗杪。

东南亚篇

4、海莲花（APT-Q-31）

【组织概述】

海莲花组织是奇安信于 2015 年披露并命名的 APT 组织。该组织自 2012 年 4 月起，针对中国政府、科研院所、海事机构、海域建设、航运企业等相关重要领域展开了有组织、有计划、有针对性的长时间不间断

攻击。

由于 APT-Q-31 属于攻击境内目标的境外组织，因此奇安信威胁情报中心对 APT-Q-31 组织的命名为魔株系——海莲花，“莲花”是表现了该组织的地缘及文化特征，“海”则主要表现了该组织以海洋领域为主要攻击目标的活动特征。

【攻击事件】

2020 年 12 月，奇安信态势感知与安全运营平台（NGSOC）在客户侧发现多台终端电脑与特定端口进行数据交互，研究人员在对交互数据分析后发现绑定在该端口通信的协议是一个没有验证加密的私有协议，对该协议数据进行逆向解密之后发现这是一些高危的指令，如修改管理员密码。

在经过层层分析和定位之后，奇安信研究人员发现这是一起供应链攻击，攻击者通过在安全终端管理软件中植入一段恶意代码，使得 18 年 9 月份之后的安全终端管理软件版本均有该代码块，且安装文件带有厂商数字签名。内网中任意 IP 的机器均可无需验证向安装了该终端软件的机器发送命令并执行。

这种源代码污染供应链攻击非常隐蔽，奇安信天擎在 2020 年 12 月更新病毒库之后扫描出了所有被植入木马的终端设备，经过供给链还原最终确认此攻击事件的发起组织为海莲花。

东亚篇

5、Darkhotel（APT-Q-10）

【组织概述】

Darkhotel 组织是 Kaspersky 于 2014 年披露的 APT 组织。该组织主要针对国防工业基地、军事、能源、政府、非政府组织、电子制造、制药和医疗等部门的公司高管、研究人员和开发人员。其因擅长使用酒店网络跟踪和打击目标而得名。

【攻击事件】

2019 年 7 月，攻击者针对国内多个重点单位网络资产进行信息收集，通过 WEB 漏洞入侵暴露在互联网上的内部系统后台登录页面并植入 IE 0day 漏洞以构造水坑攻击，相关单位网站管理员访问后台页面触发漏洞并被植入木马后门导致计算机被控、机密信息泄漏。

2020 年 2 月，奇安信威胁情报中心红雨滴团队监测到上述多个重点单位的内部系统管理登录页面被植入恶意代码以执行水坑攻击。研究人员在深入分析被植入的代码后，确认此次事件背后的攻击团伙为境外 APT 组织 Darkhotel。

通过奇安信威胁情报中心大数据关联分析后发现，攻击者使用的微软 IE 浏览器漏洞 CVE-2019-1367 利用代码在 2019 年 7 月 19 日就被上传至被攻击的服务器，而该漏洞微软在 2019 年 9 月份才修补，因此在攻击发生的当时漏洞还处于 0day 漏洞状态，因此研究人员推断，Darkhotel 最晚在 2019 年 7 月就利用 0day 漏洞对我国执行了针对性的攻击。

6、虎木槿（APT-Q-11）

【组织概述】

虎木槿是疑似来自东北亚的 APT 组织，使用的恶意代码有着很强的隐蔽性，且具备 0day 漏洞发掘利用能力。曾通过浏览器漏洞攻击国内重点单位。

2019 年，奇安信捕获境外 APT 组织虎木槿针对国内核心教育科研政府机构的攻击活动并将活动命名为“幻影”行动。

“幻影”行动意指虚幻而不真实的影像，取意于攻击者在浏览器漏洞利用过程中通过播放一个不存在的 Windows Media Video 影音文件来启动 MediaPlayer 插件，从而劫持执行下载的恶意 DLL 以达到执行木马获取控制的目的，体现了攻击者变幻莫测的攻击技巧和高超的技术能力。

由于 APT-Q-11 属于攻击境内目标的境外组织，因此奇安信威胁情报中心对 APT-Q-11 组织的命名为魔株系——虎木槿。“虎”与“木槿”均取自该组织地缘文化象征。

【攻击事件】

2019 年，奇安信威胁情报中心红雨滴团队结合天眼产品在客户侧的部署检测，在全球范围内率先监测到多例组合使用多个浏览器高危漏洞的定向攻击。此次活动目标包括多个国内核心教育科研政府机构和个人，被攻击目标只需使用某浏览器低版本打开网页就可能中招，被黑客植入后门木马甚至完全控制电脑。

7、毒云藤（APT-Q-20）

【组织概述】

毒云藤组织是奇安信于 2015 年 6 月首次披露的疑似有我国台湾地缘背景的 APT 组织，其最早的活动可以追溯到 2007 年。该组织主要针对国内政府、军事、国防、科研等机构，使用鱼叉邮件攻击和水坑攻击等手段来实施 APT 攻击。

由于 APT-Q-20 属于攻击境内目标的境外组织，因此奇安信威胁情报中心对 APT-Q-20 组织的命名为魔株系——毒云藤。“毒藤”意为该组织在多次攻击行动中，都使用了 Poison Ivy（毒藤）木马，“云”字取于该组

织在中转信息时，曾使用云盘作为跳板传输资料。

【相关事件】

2020 年 10 月，奇安信披露了华语情报搜集活动：血茜草行动。从 2018 年至 2020 年，毒云藤组织利用大陆最常使用的社交软件、邮箱系统、以及政府机构网站、军工网站、高等院校网站等进行了大规模的仿制，目的是尽可能多地获取目标的个人信息，为后续窃取我国情报信息做准备。

攻击主要分为钓鱼网站攻击以及钓鱼邮件攻击。在钓鱼邮件攻击中，毒云藤主要伪装成多种具有鲜明特色的角色如智库类目标、军民融合产业园、军事杂志、公务员类猎头公司等。

经过关联分析，奇安信威胁情报中心发现，此次攻击活动中使用的恶意代码同历史攻击活动一样利用 WinRAR ACE 漏洞 CVE-2018-20250 进行下发，且恶意代码中所使用的 API 函数以及使用 strrev 函数将字符串反序的特点也与历史代码几乎一致，最后木马回连的 C2 解析出的 IP 反查可得部分血茜草钓鱼网站域名。至此研究人员判定此次攻击活动与毒云藤组织相关。

8、蓝宝菇（APT-Q-21）

【组织概述】

蓝宝菇（APT-C-12）是奇安信率先公开和披露的 APT 组织。该组织从 2011 年开始持续至今，蓝宝菇（APT-C-12）对我国政府、军工、科研、金融等重点单位和部门进行了持续的网络间谍活动。该组织主要关注核工业和科研等相关信息。被攻击目标主要集中在中国大陆境内。

该组织常使用鱼叉邮件作为主要攻击手段，通过向目标对象发送携带 LNK 文件和恶意 PowerShell 脚本诱导用户点击，窃取敏感文件，安装持久化后门程序，并使用如阿里云盘、新浪云等云服务，把窃取的数据托管在云服务上。由于该组织相关恶意代码中出现特有的字符串（Poison Ivy 密码是：NuclearCrisis），结合该组织的攻击目标特点，奇安信威胁情报中心也将该组织的一系列攻击行动命名为核危机行动（Operation NuclearCrisis）。

在 2018 年期间，该组织针对我国政府、军工、科研以及金融等重点单位和部门发起多次针对性攻击，攻击手法相较于之前也有所升级，并且鱼叉邮件携带恶意文件也由原本的恶意 PE 文件首次更新为 PowerShell 脚本后门，以及采用云空间、云附件的手法接收回传的资料信息等都反映了蓝宝菇 APT 组织在攻击技术方面的更新。

【近期攻击事件】

2018 年 4 月以来，安全监测与响应中心和奇安信威胁情报中心在企业机构的协同下发现了一批针对性的鱼叉攻击，攻击者通过诱导攻击对象打开鱼叉邮件云附件中的 LNK 文件来执行恶意 PowerShell 脚本收集上传用户电脑中的敏感文件，并安装持久化后门程序长期监控用户计算机。该攻击过程涉及一些新颖的 LNK 利用方式，使用了 AWS S3 协议和云服务器通信来偷取用户的敏感资料。

继披露了蓝宝菇 (APT-C-12) 攻击组织的相关背景以及更多针对性攻击技术细节后，奇安信威胁情报中心近期又监测到该组织实施的新的攻击活动，在 APT-C-12 组织近期的攻击活动中，其使用了伪装成 " 中国轻工业联合会投资现况与合作意向简介 " 的诱导文件，结合该组织过去的攻击手法，该诱饵文件会随鱼叉邮件进行投递。

北美篇

9、Longhorn

【组织概述】

Longhorn 又名 Lamberts，APT-C-39 等。最早

由国外安全厂商赛门铁克在 Vault 7 泄漏间谍工具后命名[2]。Valut 7 是由维基解密从 2017 年 3 月起公布的一系列文件，在这些文件中主要披露了美国中央情报局进行网络监控和网络攻击的活动与攻击工具。

据分析，Longhorn 至少从 2011 年开始活动，Longhorn 感染了来自至少 16 个国家包括中东、欧洲、亚洲和非洲等的 40 个目标，主要影响金融、电信、能源、航空航天、信息科技、教育、和自然资源等部门。它使用了多种后门木马结合 0day 漏洞进行攻击。

奇安信威胁情报中心红雨滴团队对历史曝光的 CIA 网络武器及相关资料进行研究，并发现了多种网络武器文件，并且根据分析的结果与现有公开资料内容进行了关联和判定。红雨滴团队还发现这些网络武器曾用于攻击中国的目标人员和机构，其相关攻击活动主要发生在 2012 年到 2017 年（与 Vault 7 资料公开时间相吻合），并且在其相关资料被曝光后直至 2018 年末，依然维持着部分攻击活动，目标可能涉及国内的航空行业。

【相关事件】

2019 年 9 月，奇安信威胁情报中心红雨滴团队通过对曝光的 CIA 网络武器进行了国内安全事件的关联和判定，发现这些网络武器曾用于攻击中国的人员和机构，攻击活动主要发生在 2012 年到 2017 年（与 Vault7 资料公开时间相吻合），并且在其相关资料被曝光后直至 2018 年末，依然维持着部分攻击活动，其目标涉及国内的航空行业。

2020 年 3 月，360 根据奇安信威胁情报中心红雨滴团队的情报再次进行分析。360 表示中国航空航天、科研机构、石油行业、大型互联网公司以及政府机构等多个单位均遭到 Longhorn 不同程度的攻击。这些攻击活动最早可以追溯到 2008 年 9 月并一直持续到 2019 年 6 月，受害者主要集中在北京、广东、浙江等省市。该组织在针对中国航空航天与科研机构的攻击中，主要围绕系统开发人员来进行定向打击，这些开发人员主要从事的是：航空信息技术有关服务，如航班控制系统服务、货运信息服务、结算分销服务、乘客信息服务等。这项攻击不仅仅是针对中国国内航空航天领域，同时还覆盖百家海外及地区的商营航空公司。

10、Crypto AG

【公司概述】

2020 年 2 月 11，《华盛顿邮报》联合德国电视二台 ZDF 曝光，CIA 一直利用顶级通信加密公司 Crypto AG 设备破解上百个国家政府数十年来的绝密信息。

【相关事件】

Crypto AG 的加密算法从 60 年代开始就被 NSA 操控，可以秘密的在加密设备中植入漏洞从而截取机密情报。美国通过这种方式截取了大量秘密通信，包括其他国家政府大量军事行动、人质危机、暗杀和爆炸事件的通信。例如，在 1978 年美国前总统卡特与埃及前总统萨达特举行埃及 – 以色列和平协议会谈时，美国能够监听萨达特与开罗的所有通信；1979 年伊朗人质危机期间，CIA 和 NSA 也借此监听伊朗革命政府；在两伊战争的十年时间里，美国甚至截获了 19000 条加密机发送的伊朗情报。根据 CIA 的记录，在马岛战争期间，美国还利用阿根廷对于 Crypto 加密设备的依赖，将截获的阿根廷军事计划泄露给了英国。目前有 120 多个国家 / 地区购入过设备，客户包括伊朗、拉丁美洲的军政府、印度、巴基斯坦甚至梵蒂冈。

11、Equation（方程式）

【组织概述】

2015 年，卡巴斯基揭露史上最强网络犯罪组织——Equation Group，该组织被视为服务于美国情报部门 NSA 旗下。该团伙已活跃近 26 年，并且在攻击复杂性和攻击技巧方面超越了历史上所有的网络攻击组织。根据卡巴斯基实验室目前所掌握的证据，Equation Group 被认为是震网（Stuxnet）和火焰（Flame）病毒幕后的

操纵者。

从 2001 年到现在，Equation 已经在伊朗、俄罗斯、叙利亚、阿富汗、阿拉伯联合大公国、中国、英国、美国等全球超过 30 个国家感染了 500 多个受害者。这些受害者包括政府和外交机构、电信行业、航空行业、能源行业、核能研究机构、石油和天然气行业、军工行业、纳米技术行业、伊斯兰激进分子和学者、大众媒体、交通行业、金融机构以及加密技术开发企业等。

【相关事件】

2017 年 4 月 14 日，“影子经纪人”曝光的数据中包含一个名为 SWIFT 的文件夹，完整曝光了“方程式组织” 针对 SWIFT 金融服务提供商及合作伙伴的两起网络攻击行动—— JEEPFLEA_MARKET 和 JEEPFLEA_POWDER。 JEEPFLEA_MARKET 攻击行动是针对中东地区最大 SWIFT 服务提供商 EastNets，成功窃取了其在比利时、约旦、埃及和阿联酋的上千个雇员账户、主机信息、登录凭证及管理员账号。此次攻击以金融基础设施为目标；从全球多个区域的预设跳板机进行攻击；以 0Day 漏洞直接突破两层网络安全设备并植入持久化后门；通过获取内部网络拓扑、登录凭证来确定下一步攻击目标；以“永恒”系列 0Day 漏洞突破内网 Mgmt（管理服务器）、SAA 业务服务器和应用服务器，以多个内核级（Rootkit）植入装备向服务器系统植入后门；通过具有复杂的指令体系和控制功能平台对其进行远程控制，在 SAA 业务服务器上执行 SQL 脚本来窃取多个目标数据库服务器的关键数据信息的高级持续性威胁攻击事件。

JEEPFLEA_POWDER 攻击行动是主要针对 EastNets 在拉美和加勒比地区的合作伙伴 BCG（Business Computer Group），但此次行动并未成功。

12、Sauron（索伦之眼）

【组织概述】

Sauron 被认为与美国情报机构有关，长期对中国、俄罗斯等国进行 APT 攻击的组织，至少在 2011 年 10 月起就一直保持活跃。以中俄两国的政府、科研机构、机场等为主要攻击目标。

Sauron 使用恶意代码的难度和隐蔽性都与 APT 方程式相似，且与病毒火焰“Flame”有相似之处，因此被视为 NSA 旗下黑客组织，与“方程式”实力相当。

【相关事件】

2016 年 8 月中旬，赛门铁克和卡巴斯基实验室相继发布报告称，追踪到一个名为 Sauron（Strider）的 APT 组织。赛门铁克发现自 2011 年起，Sauron 凭借 Backdoor.Remsec 恶意代码，攻击了在中国，比利时，俄罗斯和瑞典的七个组织，包括：中国的一家航空公司、比利时的大使馆等。后门 Remsec 可以用来窃取 Windows 的用户信息，由 Lua 语言编写，模块化程度很高，不容易被发现。

目前已知该组织攻击过的目标包括中国、俄罗斯、比利时、伊朗、瑞典、卢旺达等 30 多个国家，主要以窃取敏感信息为主要目的。主要针对国防部门、大使馆、金融机构、政府部门、电信公司以及科技研究中心等。涉及国内组织包括科研教育、军事和基础设施领域，重点行业包括水利、海洋等行业。除了这些政府机构与企业，他们还在公用网络中各种开后门，针对个人进行键盘监听、窃取用户凭证或密码等个人隐私信息。

揭秘 APT 组织使用的 10 大类安全漏洞

作者 奇安信威胁情报中心

为了能够更加全面的了解全球 APT 研究的前沿成果，奇安信威胁情报中心对 APT 攻击中最重要的部分（APT 组织所使用的安全漏洞）进行了梳理，在参考了各类 APT 研究报告和研究成果、APT 攻击活动或 APT 组织最常使用的漏洞、以及漏洞的价值等几项指标后，并结合奇安信威胁情报中心对 APT 攻击这类网络战的理解，筛选出近年来 APT 组织所使用的 10 大（类）安全漏洞。

防火墙设备漏洞

防火墙作为网络边界设备，通常不属于攻击者攻击的目标，尤其在 APT 领域中针对防火墙设备的漏洞就更为少见，直到 2016 年第一批 Shadow Broker 泄露的工具中大量针对防火墙及路由设备的工具被曝光，方程式组织多年来直接攻击边界设备的活动才被彻底曝光，此处我们选择 CVE-2016-6366 作为这类漏洞的典型代表。

而方程式组织的 Quantum insert（量子植入攻击工具）则正是通过入侵边界防火墙、路由设备等来监听 / 识别网络内的受害者虚拟 ID，进而向被攻击者的网络流量中“注入”相应应用程序（比如 IE 浏览器）的漏洞攻击代码进行精准的恶意代码植入。

SMB 通信协议漏洞

SMB（Server Message Block）通信协议是微软（Microsoft）和英特尔（Intel）在 1987 年制定的协议，主要是作为 Microsoft 网络的通讯协议。

2017 年 4 月 14 日 Shadow Brokers 公布了之前泄露文档中出现的 Windows 相关部分的文件，该泄露资料中包含了一套针对 Windows 系统相关的远程代码利用框架（涉及的网络服务范围包括 SMB、RDP、IIS 及各种第三方的邮件服务器），其中一系列的 SMB 远程漏洞 0day 工具（EternalBlue，Eternalromance，Eternalchampoin，Eternalsynergy）之后被集成到多个蠕虫家族中，同年 5 月 12 日爆发的 WanaCry 当时就集成了 EternalBlue。

该泄露的工具本身出自 NSA 旗下的黑客组织 Equation Group，相关工具泄露后为大量的勒索，蠕虫所使用。

Office OLE2Link 逻辑漏洞

Office OLE2Link 是微软办公软件（Office）中的一个重要特性，它允许 Office 文档通过对象链接技术在文档中插入远程对象，在文档打开时自动加载处理。由于设计不当，在这个处理过程中出现了严重的逻辑漏洞，我们选择 CVE-2017-0199 为这类漏洞的典型代表。2017 年 4 月 7 日 McAfee 与 FireEye 的研究员爆出微软 Office Word 的一个 0-day 漏洞的相关细节（CVE-2017-0199）。攻击者可以向受害人发送一个带有 OLE2link 对象附件的恶意文档，诱骗用户打开。当用户打开恶意文档时，Office OLE2Link 机制在处理目标对象上没有考虑相应的安全风险，从而下载并执行恶意 HTML 应用文件（HTA）。

Office OLE2Link 逻辑漏洞原理简单，易于构造，触发稳定，深受 APT 组织的青睐，已经被大部分 APT

组织纳入攻击武器库。

Office 公式编辑器漏洞

EQNEDT32.EXE（Microsoft 公式编辑器），该组件首发于 Microsoft Office 2000 和 Microsoft 2003，以用于向文档插入和编辑方程式，虽然从 Office 2007 之后，方程式相关的编辑发生了变化，但为了保持版本的兼容性，EQNEDT32.EXE 本身也没有从 Office 套件中删除。而该套件自 17 年前编译之后就从未被修改，这就意味着其没有任何安全机制（ASLR，DEP，GS cookies…）。并且由于 EQNEDT32.EXE 进程使用 DCOM 方式启动而独立于 Office 进程，从而不受 Office 高版本的沙盒保护，所以该类漏洞具有天生“绕过”沙盒保护的属性，危害巨大。APT34 正是通过 CVE-2017-11882投递鱼叉邮件攻击中东多国金融政府机构。

OOXML 类型混淆漏洞

OOXML 是微软公司为 Office 2007 产品开发的技术规范，现已成为国际文档格式标准，兼容前国际标准开放文档格式和中国文档标准“标文通”，Office 富文本中本身包含了大量的 XML 文件，由于设计不当，在对其中的 XML 文件进行处理的时候，出现了严重的混淆漏洞，最典型的包括 CVE-2015-1641，CVE-2017-11826，这里我们选择近年来最流行的 OOXML 类型混淆漏洞 CVE-2015-1641 作为典型代表。

CVE-2015-1641 相关的利用技术早已公开，且该漏洞利用的成功率非常高，所以该漏洞在 Office OLE2Link 逻辑漏洞还未曾风靡之前是各大 APT 组织最常用的 Office 漏洞之一。

摩诃草 APT 组织自 2016 年以来针对我国的多起攻击事件大量使用了包含 CVE-2015-1641 的漏洞文档。

Chrome 浏览器漏洞

随着近年来 Windows 放弃自研浏览器 Edge，并宣布新版 Edege 将使用 Chrome 内核，Chrome 浏览器在 PC 产品浏览器产品中的使用比达到空前的地步，Chrome 浏览器也逐渐成为近三年来攻击者使用最多的在野 0day，2019 年 11 月 1 日，卡巴斯基在报告 "chrome-0-day-exploit-cve-2019-13720-used-in-operation-wizardopium" 中披露了疑似 Darkhotel 使用 Chrome 0day cve-2019-13720 进行水坑攻击的事件，随后大量的 Chrome 0day 开始被使用，2021 年被使用的 Chrome 0day 数量甚至已经超过 10 个。

Chrome 相关漏洞，由于 Chrome 浏览器本身包含沙箱且具备很高的安全性，此类漏洞的发现及利用都有很高难度，因此其往往都是定向性非常强的高价值目标攻击事件中出现。

Windows 提权漏洞

近年来针对 Windows 客户端的漏洞攻击越来越多，这直接导致各大厂商对其客户端软件引入了“沙盒”保护技术，其核心思想即是将应用程序运行在隔离环境中，隔离环境通常是一个低权限的环境，也可以把沙盒看做是一个虚拟的容器，让不是很安全的程序在运行的过程中，即便客户端软件遭受恶意代码的入侵也不会对使用者的计算机系统造成实际威胁。

引入了“沙盒”保护的常客户端程序有：IE/Edge 浏览器、Chrome 浏览器、Adobe Reader、微软 Office 办公软件等等。而客户端程序漏洞如果配合 Windows 提权漏洞则可以穿透应用程序“沙盒”保护。

相关的有针对日本和我国台湾的 APT 攻击以及 APT28 针对法国大选等攻击事件。

8 Flash 漏洞

Flash player 因为其跨平台的普及性，一直为各个 APT 组织关注，从 2014 年起，Flash 漏洞开始爆发，尤其到 2015 年，HackingTeam 泄露数据中两枚 0-day 漏洞 CVE-2015-5122/CVE-2015-5199，Flash 漏洞相关的利用技术公开，Flash 漏洞开始成为 APT 组织的新宠，尽管之后 Adobe 和 Google 合作，多个 Flash 安全机制陆续出炉（如隔离堆，vector length 检测），大大提高了 Flash 漏洞利用的门槛，但也不乏出现 CVE-2015-7645 这一类混淆漏洞的怪咖。这里我们选择不久前发现的在野 0-day CVE-2018-4878 作为这类漏洞的典型代表。

2018 年 1 月 31 日，韩国 CERT 发布公告称发现 Flash 0day 漏洞（CVE-2018-4878）的野外利用，攻击者通过发送包含嵌入恶意 Flash 对象的 Office Word 附件对指定目标进行攻击。

9 iOS 三叉戟漏洞

iOS 三叉戟漏洞是目前唯一一个公开披露的针对 iOS 系统浏览器的远程攻击实例，并真实用于针对特点目标的 APT 攻击中。

iOS 三叉戟漏洞是指针对 iOS 9.3.5 版本之前的 iOS 系统的一系列 0 day 漏洞，其利用了 3 个 0 day 漏洞，包括一个 WebKit 漏洞，一个内核地址泄露漏洞和一个提权漏洞。通过组合利用三个 0 day 漏洞可以实现远程对 iOS 设备的越狱，并且安装运行任意恶意代码。

三叉戟漏洞的最初发现是因为阿联酋一名重要的人

权捍卫者 Ahmed Mansoor 在 2016 年 8 月 10 日和 11 日，其 iPhone 手机收到两条短信，内容为点击链接可以查看关于关押在阿联酋监狱犯人遭受酷刑的秘密内容。其随后将短信内容转发给公民实验室 (Citizen Lab)，由公民实验室和 Lookout 安全公司联合分析发现，最后发现该三叉戟漏洞和相关恶意载荷与著名的以色列间谍软件监控公司 NSO Group 有关。

10 Android 浏览器 remote2local 漏洞利用

Android 浏览器漏洞利用代码的泄露揭示了网络军火商和政府及执法机构利用远程攻击漏洞针对 Android 用户的攻击和监控，并且该漏洞利用过程实现几乎完美，也体现了漏洞利用技术的艺术特点。

该漏洞利用代码几乎可以影响当时绝大多数主流的 Android 设备和系统版本。漏洞的相关利用情况没有在历史公开的事件报告中披露过，由于专注于向政府部门及执法机构提供电脑入侵与监视服务的意大利公司 Hacking Team 在 2015 年 7 月遭受入侵，其内部源代码和相关资料邮件内容被泄露，首次披露了其具有针对该漏洞的完整攻击利用代码。

APT 组织命名：读懂背后的信息与含义

——透过 APT 组织命名规则，掌控全球 APT 组织态势

给 APT 组织命名是安全研究的需要。我们看到某 APT 组织名称是这样的：“Strontium (APT28, Fancy Bear)”。某些 APT 组织的名称里，括号中的名字可能更多。这样名字包含什么信息呢?

如何命名 APT 组织? 为什么貌似同一个 APT 组织，却有很多不同的名字? 我们来探讨一下 APT 组织命名的影响要素及其之间的关系。

“Strontium (APT28, Fancy Bear)”，这三个名字分别来自微软、Mandiant 和 CrowdStrike 公司。根据这些公司的命名惯例，这三家公司都认为 APT 组织是具有国家属性的。例如，从“Fancy Bear”中，我们能从单词“Bear”（熊）联想到俄罗斯。了解研究人员如何对 APT 组织命名，有助于我们更好地了解全球网络威胁的态势。

APT 组织的命名与归因

名字是将想法固化为实体的标签。没有名字就没有真正的存在。研究人员首先检测客户出现的疑似恶意行为，并在其他客户寻找类似案例，由此组成恶意活动集——但目前仍是想法猜测。随着对恶意活动研究的深入，大量研究将恶意活动指向某一组织或者团伙，此时就需要对该组织进行命名了。

大多数安全厂商都有自己的安全研究团队，根据从客户电脑中采集的数据进行安全分析。这里我们需要认识到一点，即每个研究团队对都是基于自己客户数据进行整体威胁状况进行分析的，分析结果、结论是有局限性的。

根据相关安全产品的性能和特点，某一分析结果在某些地理区域（或垂直行业）可能是对的，而在其他地区则可能是不完全准确的，实际情况也是如此。任何两个安全研究团队的分析结果都不可能完全相同。

这个过程可以理解为多个安全研究团队在“管中窥豹”。每个安全团队看到真相的一部分。安全研究人员把这个过程比喻为每个团队使用不同望远镜观测宇宙的不同部分，都相信自己的望远镜看得更远，但仍不能观测到整个宇宙。

APT 组织的攻击活动往往突破安全厂商的安全产品边界，可能多个安全研究团队几乎同时检测到网络攻击活动，但都只是看到 APT 组织攻击活动的局部。如果大量攻击活动逐渐呈现出新的 APT 组织特征，目前的研究报告中都没有给攻击组织命名，安全研究团队就有权利和责任对攻击组织命名，为威胁活动打上标签。

不同的研究人员可能同时看到类似的攻击活动，但由于可见度有限，可能没有意识到其他研究人员也在进行研究。这导致在短时间内出现的新攻击组织具有不同名称，可能同一 APT 组织有三个不同名字，也可能三个 APT 组织使用相似恶意软件或通过同样的漏洞，攻击相

似目标。

主要研究团队的命名规则

不同公司的研究团队有不同的命名习惯。有的希望通过攻击组织名字提供清晰信息；有的仅仅进行没有任何归因的编号，甚至不遵循任何规则，完全取决于研究人员自身的喜好。

Mandiant

Mandiant 公司可能是 APT 组织命名的祖师爷。2013 年 2 月该公司发布了报告 APT1。APT n 是 Mandiant 对国家级攻击组织的命名法。

这种命名法的优势在于其比较清晰：马上可以看出是国家级攻击组织。它的弱点在于并没有提供其他信息：不知道涉及哪个国家——这些信息可以显示地缘政治目标和可能的垂直行业目标。

随着时间的推移，Mandiant 添加了其他前缀：UNC、TEMP 和 FIN。UNC 代表“未分类”攻击活动的内部名称。TEMP 是临时工作名称（仍然主要在内部），代表攻击活动明显归因于某组织。FIN（或 APT）是具有经济（或国家间谍）动机的威胁组织的前缀。因此，例如，UNC902 演变为 TEMPWarlock，最终公开命名为 FIN11。

FIN 不用于命名国家级攻击组织。对于攻击动机重叠的组织——例如具有经济动机的朝鲜网络攻击组织，优先采用 APT 命名方式。

CrowdStrike

CrowdStrike 公司采取了不同的命名方法：攻击组织的名字既富于想象又提供更多信息：首先是吸引人的前缀，然后是与国家有关、具有地理内涵的动物。最终将营销潜力与地理信息进行很好的结合——例如，用 Fancy Bear 命名据信为俄罗斯国家攻击组织，这个名字不容易遗忘，同时与 CrowdStrike 紧密联系起来。

根据 CrowdStrike 的命名习惯，用 Bear （熊）指代俄罗斯，Chollima（千里马）指代朝鲜、Kitten（小猫）

指代伊朗， Buffalo（水牛）指代越南。非国家攻击组织，则用 Spider（蜘蛛）指代网络犯罪组织，Jackal （豺）代笔黑客组织。

CrowdStrike 命名方法的突出风险（暗示特定国家参与）很容易理解：如果公司的归因错了怎么办？如果需要对 Fancy Bear 重新命名，将对公司声誉造成巨大打击。但目前还没有出现这样的更正。

卡巴斯基

2005 年前后，对攻击组织的命名是由政府机构完成的。政府机构对此有非常严格的流程：命名耗时较长，可能需要一年时间。只有少数机构参与，政府机构可以接受这种方式。

随后自由网络安全研究人员的加入，这一过程开始商业化。企业从研究牟利，就要想出自己的名字。这些企业过去没有，现在也不能一睹政府的研究成果，就只能完全依靠自己。这是产生不同的名字，并造成冲突的原因。

从那时起，网络安全研究员就不断讨论制定通用的命名公约，但一直没有成功。原因在于，不同研究机构对攻击活动都有不同的可见度。

现在达成的共识是，每个研究人员都应该坚持自己的命名，以进行归因。这会对客户造成困扰，对公众来说更是如此，但它使每个研究机构都保持自己研究的独特性。

卡巴斯基公司没有正式的命名规则。但它会确保使用的名称，不会有任何归因到某政府或现有组织的暗示，也就是回避了直接归因问题。

由于没有严格的命名规则，对攻击组织的命名一般

完全取决于卡巴斯基的研究人员个人。因此，通常不会遵循任何公约，一般名字都没有真正的含义。有时用恶意软件对攻击组织命名，或者是攻击组织所利用的基础设施的诙谐双关语。

微软公司

微软威胁情报中心（MSTIC）在内部已存在十多年，但直到 5 年前才正式对外宣布。由于 MSTIC 跟踪超过 140 个攻击组织，涵盖所有类别，很有必要确定命名规则，以便进行内部和客户沟通。

微软威胁情报中心尝试过多种命名方式，但没有试图将攻击组织归因到具体的地理位置或国家。早期曾使用过啤酒风味轮上的啤酒风味名称，甚至一度使用恐龙来命名，因名字长度和发音困难，最终放弃了这个想法。微软威胁情报中心需要确保名称不会违反任何许可协议，易被公众认知，同时能在相当长的一段时间的使用提供足够的信息。最终，微软威胁情报中心最终选择使用化学元素周期表、火山，和树木，以确保每个组织都有容易识别的名字。

研究人员用化学元素命名国家攻击组织，用火山命名网络犯罪组织，用树木命名私营机构的攻击，用 DEV 来命名仍处于调查中的新攻击活动。这些区别会有助于客户更好地了解不同攻击组织的威胁。MSTIC 的命名人员会考虑名称是否有任何文化的敏感性，尽量避免任何文化联想。

与其他研究小组不同，微软通过客户遥测技术对威胁全域有更广的视角。达尔曼说，“通常，我们观察到的网络攻击活动与其他研究人员重叠，对威胁全域的某些部分也有着共同的观点。因此，我们认为 Strontium 组织、APT28 组织、Fancy Bear 组织是同一网络犯罪团伙。”

奇安信

奇安信集团红雨滴团队 2015 年发布中国首个组织层面的 APT 事件揭露报告，开创了 APT 攻击类高级威胁体系化揭露的先河。持续发现包括海莲花在内的多个 APT 组织在中国境内的长期活动。截至目前，持续跟踪分析的主要 APT 团伙超过 46 个。

奇安信红雨滴团队对命名采取地域特征物品与 APT 编号结合的方式：对自己检测到的攻击组织及活动，会利用体现地理属性的编造植物、动物等进行命名；对于长期跟踪的其他组织，参考其他安全团队的命名。例如，摩诃草（APT-Q-36），摩诃草为体现南亚特征的（杜撰）植物。

APT 组织编号采用 APT-Q-N 的命名格式，其中 APT-Q- 为固定格式，代表奇（Q）安信 APT 组织编号。N 为独立数字，例如 APT-Q-1、APT-Q-27 等等。

在整体上，为了在 APT 组织编号上对各地缘背景下的 APT 团伙进行划分，按照历年来其对全球高级持续性威胁划分的 6 大地区，对 APT 组织的编号划分为了 6 组，包括：东亚、东南亚、南亚、中东、东欧和美洲地区。后续发现的来源于该地区的 APT 组织沿用对应地区的组织编号。

东亚地区	APT-Q-(1-30)
东南亚地区	APT-Q-(31-35)
南亚地区	APT-Q-(36-50)
中东地区	APT-Q-(51-75)
东欧地区	APT-Q-(76-90)
北美地区	APT-Q-(91-99)

研究机构看到同一组织多个名称造成的混乱，有意识地选择不再进行新的命名。只要有足够的重合证明合理性，就会使用现有的名字。

通常情况下，安全研究人员首先发现攻击者使用的恶意软件，但这就会容易带来混淆。谈及 DarkSide 时，就容易搞不清是指攻击组织还是恶意软件，REvil 也是同样的情况。

随着对恶意软件使用和发展研究的持续深入，对攻击组织有个更清晰认识。例如，CrowdStrike 将 DarkSide 组织称为 Carbon Spider，而 Revil 组织称为 Pinchy Spider。安

漏洞疯狂二十年之后，想“补天”的人出手了

作者 公共关系部 魏开元

20 世纪 70 年代末，当时年仅 15 岁的传奇黑客米特尼克，仅凭一台电脑和一部调制调节器，成功黑入了北美空中防务指挥部的计算机系统主机。

当时的他无论如何也很难想到，他攻破计算机系统所仰赖的漏洞，在短短数十年之后，竟变得和普通商品一样，在市场上买卖。

尽管在第二次社会大分工中，商品经济已然出现，不过在漫长的人类历史长河中，自给自足的自然经济长期居于核心位置。

直到 1492 年，航海家哥伦布“发现”美洲大陆之后，国际贸易一跃成为当时西欧的主要经济增长点，自此商品经济开始逐渐取代自然经济，成为了主要的经济活动形式。

从自给自足到“社会化大生产”

说起漏洞这把高悬在计算机系统上的达摩克里斯之剑，它最早记载于 1947 年：一只小飞蛾不慎飞进了 Mark II 计算机的继电器中，导致整个机器发生故障。

70 多年后的现在，计算机再也不可能飞进飞蛾，但漏洞却伴随着信息技术的应用飞速增长，从最底层的芯片到上层的 Web 应用，无一幸免。

有漏洞的地方就有江湖，行走江湖的人也有黑有白。

最开始这帮江湖人士或许并不想做点什么惊天地泣鬼神的“壮举”，漏洞从挖掘出来后，在他们手中也不过是一种“高级玩具”，用于炫耀谁的技术更加高明。

但商品经济的影响是方方面面的。

漏洞利用对信息系统的巨大破坏力，让一些不怀好意的人嗅到了金钱的味道：一枚关键的漏洞可以窃取到大量敏感数据，也可以篡改某些参数，甚至可以造成目标系统瘫痪，如果放到黑市上去买卖，应该有很大的市场空间。

借助暗网的保护伞，一笔笔非法漏洞交易裹挟着不可告人的目的，每天都在发生。交易的内容也不局限于漏洞本身，还包括黑客服务、攻击代码及恶意样本等。一个名为“TheRealDeal（真实交易）”的暗网黑市，就是地下漏洞产业的缩影。

在“TheRealDeal”黑市，所有漏洞都被明码标价，譬如前两年的时候，入侵 iCloud 账号的方法明码标价为 17,000 美金，一种在线 IE 浏览器的攻击方法价值 8000 美金的比特币。

而所有参与漏洞黑市交易的人群中，不乏网络犯罪团伙、APT 组织甚至是网络军火商的身影。

例如，以色列著名的网络军火商 NSO 一直都在做这么一件事情：从黑市中收购原始漏洞，然后开发漏洞利用工具，制作成网络军火再打包出售，从中攫取利润。前两个月臭名昭著的“飞马”恶意软件，就是出自 NSO 之手。

漏洞在黑市的广泛交易，大幅降低了网络攻击的门槛，网络攻击团伙不用从头开始进行漏洞挖掘，取而代之的是可以在黑市上购买一整套的漏洞利用工具，以自动化或者半自动化的方式，向目标发动网络攻击。

从最早的“bug”到后来的黑客职业化、漏洞攻击专业化、市场开拓产业化，漏洞带来了巨大的地下经济产业。这让本身就落后半拍的漏洞防护，更是雪上加霜。

在那个安全团队十分稀缺的年代，少数人小作坊式的漏洞挖掘能力，怎么可能与商品化的漏洞黑产相比。而且，漏洞的利用与反制永无止境，这是一场针尖对麦芒的对抗，这种对抗，不是现在才有，也不是未来才有，而是一直存在。

从这个角度来说，如果有一个平台，能把民间的白帽子给聚集起来，帮助企业找出其中潜在的漏洞，这样才能够最大程度上料敌于先。

于是乎，在黑产的另一面，有一帮正义的白帽子发

起了“漏洞赏金计划”，希望在黑产发现漏洞之前，就能够把它找出来并完成修复，我们不妨称之为白产吧。

补天平台正是在这种背景下成立的。白帽子可以把挖到的漏洞提交到补天平台上，补天平台再根据漏洞评级，给予白帽子一定的现金奖励，并把漏洞提交给对应的机构，协助他们完成修复。

“漏洞赏金计划”与漏洞响应平台的诞生，给了那些侠肝义胆的白帽子施展本领的舞台。

“大概从 2016 年开始，我就开始陆陆续续往补天平台提交漏洞了。对我来说，做白帽子挖漏洞是一个既可以锻炼技术，也可以获得收益的行为。”补天风云榜上排名靠前的一名白帽子 Kamelo（化名）说到。

从 2013 年 3 月收到第一个漏洞到现在，补天平台已经吸引了超过 8 万名白帽子，报送漏洞超过 60 万个。

黑白两道在漏洞挖掘领域的激烈对抗，让挖洞从少部分人的“自给自足”，朝着社会化大生产的方向迈进。

不平衡的漏洞博弈

尽管如此，但阳光不可能同时照亮世界上的每一个角落——你一定会在某些漏洞的挖掘中处于落后位置，导致那些不怀好意的人率先掌握某种不为人知的攻击方法。

即便是“撞洞”了（即黑白两道同时挖到同一个漏洞），在漏洞修补之前，黑产仍然处于绝对有利的攻击位置。

更何况，黑产的巨大经济诱惑，着实让不少心怀不轨的人蠢蠢欲动。

在所有漏洞中，最受欢迎的要属影响范围广并且触发方式简单的漏洞了，尤其是当它还是 0day 的时候。这样一枚漏洞动辄可以卖到数十万甚至上百万美元的价格。更要命的是，这枚漏洞可以在黑市中被反复交易 N 多次，直到大部分用户完成修复后失去利用价值。

2014 年 4 月首次曝光的 OpenSSL 心脏滴血漏洞，早在 2012 年就被引入到软件中，没人知道这两年间，这个漏洞被私下交易过多少次，也无法评估黑客利用这个漏洞，到底窃取了多少敏感数据。

但可以肯定，凭借心脏滴血的影响范围和破坏力，这枚漏洞在被挖掘出来后的首次交易价格，基本能够达到漏洞黑市的天花板级别。

正因如此，漏洞在黑产中的交易要更加广泛。或许是受其影响，或许还有其他什么原因，今年上半年 0day 的在野利用显得格外多。

据奇安信威胁情报中心发布的《全球高级持续性威胁（APT）2021 年中报告》显示，仅 2021 年上半年，APT 组织在野利用的 0day 漏洞数量超过 40 个，在网络安全历史上堪称空前。而且，这种攻击呈现出“以 Windows 平台为基础，Chrome/Safari 浏览器为主流向着多平台延伸”的趋势。

如果说所有的 APT 组织都会花费大量人力物力，去挖掘目标系统的 0day，这好像有点不太现实。

更让人头痛的是，黑产与白产之间，并没有一道特别明显的界限，总有人在黑白之间“反复横跳”。

毕竟同样一枚漏洞，放在黑市上交易与提交给补天平台获得的赏金，可能相差不少。

向钱看，无疑是商品经济时代最重要的参考准则之一。正是这样一条准则，让那个漏洞挖掘略显无序的时代，黑白双方的漏洞博弈出现了失衡。

面对这种情况，这几年，补天做了两件非常有意义的事情：

第一，通过漏洞奖励计划，众测平台为白帽子尽可能提供足够多的现金奖励；

第二，通过攻防社区、补天白帽大会、漏洞风云榜等，为白帽子提供交流展示的平台，同时营造正向的极客氛围。

在 9 月 17 日举行的的补天白帽大会，补天平台就邀请了各路白帽大神，分享他们开发或者惯用的渗透工具，通过工具化的方式更快的发现漏洞，帮助厂商更快速的建设防御体系。

“我相信，出于正义感，大多数的白帽子会把漏洞提交给 SRC 或者是补天平台，而不是为了利益交给黑产。”补天白帽子 Kamelo 坚定地说。

扭转软件供应链安全危机

话虽如此，这个事情还是需要一定的规范。

9 月 1 日，工业和信息化部、国家互联网信息办公室、公安部联合印发的《网络产品安全漏洞管理规定》（简称：《规定》）正式施行。

而《规定》的初衷之一，就在于禁止拿漏洞作恶。

《规定》特别强调，不得刻意夸大网络产品安全漏洞的危害和风险，不得利用网络产品安全漏洞信息实施恶意炒作或者进行诈骗、敲诈勒索等违法犯罪活动；不得将未公开的网络产品安全漏洞信息向网络产品提供者之外的境外组织或者个人提供。

说白了，白帽子在挖到漏洞之后，不能随便公开，尤其是不能交给境外人士。在网络军火商广泛参与的漏洞交易黑市，搞不好就被制作成了攻击我国的网络武器。

这样一来，《规定》就在很大程度上限制了漏洞的黑市交易。想搞事，你得自己有本事挖掘 0day。

在奇安信攻防社区，一名白帽子如此评论道：“《规定》的出台，与其说是强压责任，不如说是通过明晰权责，树立边界感，在合规的条件下，让白帽子的社会价值发挥至极致。”

与此同时，《规定》还释放了一个非常重要的信号。

奇安信集团副总裁、补天漏洞响应平台主任张卓认为，这是我国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。

基于软件供应链的攻击形式，正在变得愈加危险，

因此引起了全社会的高度重视。

根据奇安信威胁情报中心的监测，供应链攻击的主要目标更侧重于在供应链中负责提供服务的公司。就连网络安全公司，也很难幸免于难。

这就意味着，利用一枚漏洞，就有可能攻破在供应链下游的一片公司。

今年 4 月，黑客劫持了密码管理系统 Passwordstate 的更新服务器，并下发了添加了恶意代码的软件，该软件被 2 万 9 千个公司约合 37 万安全和 IT 人员使用。

从这个角度来看，《规定》的实施给了补天平台很大的机会，并且鼓励相关组织和个人向网络产品提供者通报其产品存在的安全漏洞，还“鼓励网络产品提供者建立所提供网络产品安全漏洞奖励机制。

为了尽可能覆盖更多品类的漏洞，在 2019 补天白帽大会上，补天平台发布了“补天五星计划”，将漏洞响应范围从原来的 Web 漏洞为主，升级化为 Web 应用、移动 APP、IoT、工控、操作系统等五大方向，成为国内少数覆盖全品类漏洞的第三方漏洞响应平台。

与此同时，这些年补天一直在优化自身的流程。从授权到漏洞定价、审核、验证再到漏洞提交及协助修复，补天把这段漏洞空窗期的时间，至少缩短了 90%。

对此张卓也曾表态，补天平台将根据规定要求，不断优化提升平台能力，也有意愿帮助各大网络产品厂商，建设和运营符合要求的产品漏洞收集平台，或者像服务现有 6000 多家入驻企业一样，为广大厂商代收漏洞。

落实《规定》的细则，尽可能帮助更多企业摆脱供应链安全危机，补天平台一直在路上。

与白帽子共成长

对于白帽子来说，他们把漏洞提交到补天平台之后，就可以坐等奖金了；但补天的使命还远远没有结束。

随着攻防对抗的不断升级，一方面，白帽子应当具备发现高级安全漏洞的能力，如浏览器、操作系统内核漏洞等；另一方面，除了漏洞挖掘，白帽子还必须具备在实战化的业务环境下实现漏洞有效利用的能力，这就要求白帽子具有社工能力、协作能力、业务分析能力等多种安全能力。

根据补天平台对数百名白帽子的调研显示，目前国内白帽子的实战化能力还很不全面，存在诸多短板。绝大多数白帽子的能力集中于 Web 漏洞的挖掘与利用这样的初级或中级能力，而对于系统层漏洞挖掘、CPU 指令集、编写 POC 或 EXP 等中高级能力，则存在明显的人才缺失。

巨量的人才缺口及缺乏进阶安全技能，也是造成漏洞博弈不平衡的重要原因之一。

在发布“五星计划”的同时，补天平台曾表示，过去、现在和将来，补天平台只做三件事情: 维护企业网络安全、降低漏洞被利用的风险、培养网络安全人才。

不过，人才培养从来不是一件非常容易的事情。

这些年，大量的白帽子一直在补天平台上活跃着、成长着，工作人员也热情的称他们为“带头大哥”。其背后的寓意是为网络安全带头冲锋。

“在域名扫描没什么发现之后，我想到了社会工程学的方法，伪装成一名在校生，借到了校内网的登录口令。我使用一个弱口令暴破进去后，就成功上传了木马，同时获取了一大堆内网 ip，紧接着我发现打印机、路由器这些设备都是弱口令……”回忆起在补天平台的初次渗透经历，Kamelo 如数家珍，“那时候我也刚成为大家口中的白帽子，技术比较菜，于是想到了用这种笨办法。”

尽管如今的 Kamelo 已经在补天平台上拥有一众忠实的粉丝，二进制、Web 应用无所不通，但他却依然比较谦虚。社会工程学在实战中的应用非常普遍，并不是什么笨办法。况且，谁还不是从菜鸟过来的呢。

“我很庆幸，在初入行的时候遇到了不少前辈大神，很多渗透技巧都是跟他们学的。” Kamelo 笑着说。

白帽众学、白帽社区、白帽大会，在这些补天平台搭建的学习场所，到处都有白帽子的身影。

当然，Kamelo 只是补天平台上八万多名白帽子的一个缩影，对于以 90 后甚至 00 后为主力的他们，补天还有很多事情要做。

只因有一点，漏洞黑产绝对不会停止。安

聚焦威胁，高效运营

——看深圳市第二人民医院如何用天眼构建一体化安全防御体系

作者 公关部 张少波 魏开元

2017 年 4 月，国务院办公厅印发《关于推进医疗联合体建设和发展的指导意见》，全面启动多种形式的医疗联合体建设试点，从此开始，全国各省掀起了一场医联体建设的浪潮。

“通过医联体建设，深圳市二院的医疗能力已经完成了向区级医院的下沉，但接下来的任务是推动安全能力的下沉，否则一旦区级医院被突破，整个集团内网的重要系统和数据，也会暴露在攻击者面前，后果不堪设想。”深圳市第二人民医院（简称深圳二院）信息科科长熊文举表示。

深圳二院，是深圳市综合实力排名前三的大型医院。2017 年 6 月，深圳二院牵头组建深圳市大鹏新区医疗健康集团（简称：大鹏新区医疗集团），对大鹏新区 3 家区级医院及所辖 21 家社区健康服务机构进行一体化管理，推进“以人为本”的市、区一体化医疗卫生服务体系建设。2020 年，深圳二院通过部署奇安信天眼（新一代安全感知系统），为大鹏医疗集团及其旗下的 3 家区级医院，实现了医联体信息化安全威胁检测、主动防御和全局安全态势可视一体化，树立了深圳集团化、医联体改革的样板工程。

医疗能力加速下沉 安全风险随之而来

2017 年 9 月 1 日，国家卫生计生委、国务院医改办在广东省深圳市召开全国医联体建设现场推进会，深圳的改革经验被充分肯定。

“病有良医”，是民生幸福的基础。近年来，深圳以改革创新为动力，着力推进以基层医疗集团为主要形式的紧密型医联体建设，引导医疗卫生工作重心下移、资源下沉。2017 年，作为深圳市首个市区合作的紧密医联体，大鹏新区医疗集团正式成立。目前，集团建立了“社

图：深圳市第二人民医院（深圳大学第一附属医院）

康机构 – 区级医院 – 市级医院”上下通畅的三级诊疗服务体系引导优质医疗资源下沉基层，让大鹏辖区居民足不出户即可享受市区三甲医院同质的医疗服务，并创下了全科诊疗服务公众满意度位居全市第一的口碑。

在医疗能力下沉的同时，大鹏新区医疗集团的网络安全问题也凸显出来。熊科长回忆在项目实施前，安全挑战主要在几个方面。

首先是地理分散，距离较远，统一管理防护的难度高。“深圳二院位于福田区，而其他 3 家区级医院都在数十公里之外。要进行统一安全管理和维护，都是很大的挑战。”

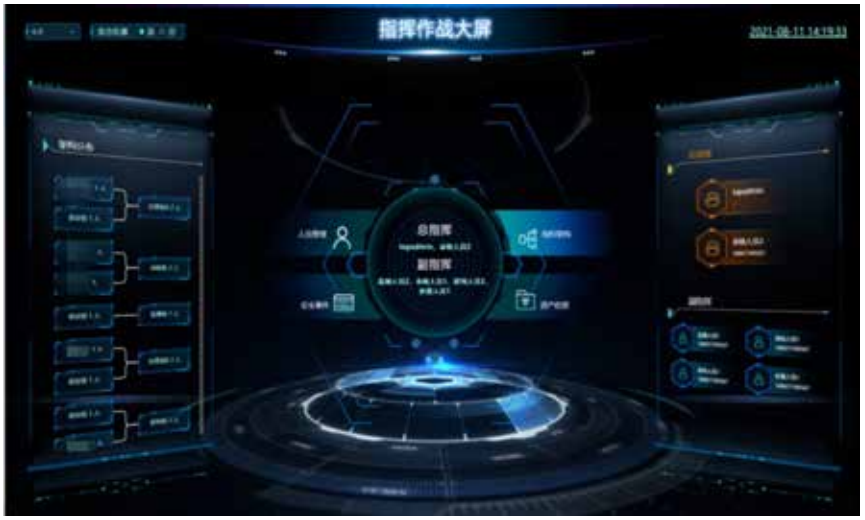


图 ：实战化防御指挥平台指挥作战大屏

其次是分支机构的网络安全建设基础非常薄弱。“当时有一些区级医院仅安装了简单的防火墙等边界设备，属于被动防御的措施，而且缺乏专业的人员进行配置和维护，在新型攻击面前很容易被穿透。”

同时，从市二院到各个区级医院，过去部署的网络设备和系统，基本上都是各自独立的，形成了一个个安全孤岛。对于一些复杂的攻击行为，依靠单一的安全设备，往往不是难以发现问题，就是产生过多误报。

第三是缺乏对未知及高级威胁攻击的主动发现与防御能力。未知威胁及高级持续性威胁（APT 攻击）是近年来非常猖獗的攻击行为，根据奇安信威胁情报中心《2020 年全球高级持续威胁 (APT) 年度报告》显示，2020 年，医疗卫生行业首次超过政府、金融、国防、能源、电信等领域，成为全球 APT 活动关注的首要目标，全球 23.7% 的 APT 活动事件与医疗卫生行业相关。

熊科长认为，APT 的目的性非常强，攻击目标明确，持续时间长，不达目的不罢休，对医院威胁很大。目前，主流的安全技术手段大多是利用已知攻击的特征对行为数据进行简单的模式匹配，只关注单次行为的识别和判断，并没有对长期的攻击行为链进行有效分析。

最后是不具备全局的安全态势监控和威胁追踪溯源能力。在上线天眼之前，从整个医疗集团到各机构部署的各类安全设备，会产生海量的日志，消耗大量存储和性能资源。但攻击发生之后，是谁攻进来过？做过哪些破坏？什么数据被拿走了？由于证据链不够全面，缺乏网络日志端回溯手段，无法跟踪溯源，能发现问题，但无法定位问题。

遵循“合规、全面、有效”三项原则

基于深圳二院医疗信息化系统的现状，以及大鹏新区医疗集团及其旗下其他医院的整体情况，集团在网络安全规划方面，遵循合规性、全面性、有效性三管齐下的原则。

“合规是基础要求，也是我们首要考虑的。”深圳二院信息科副科长潘军杰谈到。在合规性方面，深圳二院安全运营监管平台既是网络信息安全运营监管平台的基础，同时也是国家网络空间安全的组成部分，需严格符合国家关于网络与关键信息基础设施、云计算、大数据、等保 2.0 相关的安全政策标准、法令法规和指导文

图：深圳二院天眼系统整体建设方案

件的要求，在合规的基础上考虑整体安全保障方案设计，尤其符合国家《网络安全法》的要求。

在全面性方面，深圳二院兼顾集团的分支医院，将安全作为一个整体全面解决问题，继而构建完整的网络威胁态势感知系统。这与以往遇到安全问题后“头疼医头、脚疼医脚”的“创可贴”式，面向单一风险点、零散的、碎片化的安全产品叠加式的安全建设有本质不同。安全体系建设更强调规划思路，建设方案应坚持以面向问题、整体设计、支撑运营为原则，系统性解决各类安全威胁与安全问题，实现安全体系的可持续发展与迭代创新。

在有效性方面，深圳二院强调了安全运营监管的重要性。潘科长认为，安全运营监管是深圳二院实现一体化安全保障，有效解决安全问题的重要基础，在方案设计过程中需重点突出实战能力与保障能力，以动态安全保障中的感知发现、分析研判、响应处置、追踪调查、追踪溯源为核心，构建完整有效的一体化安全保障能力体系。

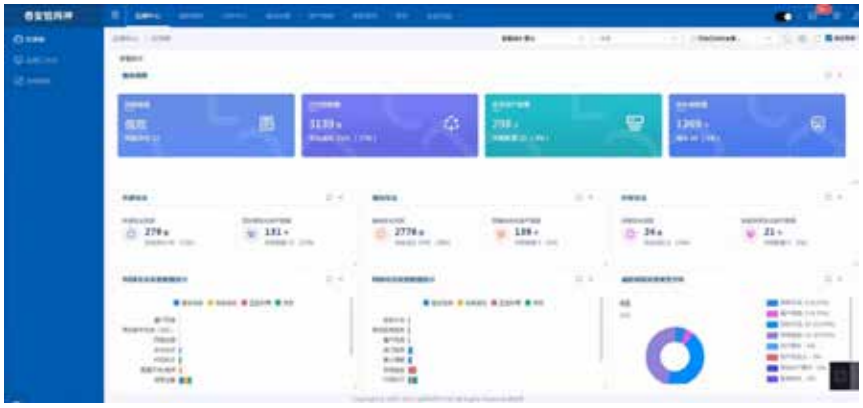
潘科长举了一个例子，“传统的安全防御体系就如同一个硬壳软糖，将安全性全部寄托于硬壳之上，一旦硬壳被砸碎，那么内部毫无二次抵御攻击的能力，而事实证明，天下不存在无坚不摧的管道硬壳。”因此，网络安全需要变被动为主动，只有快速追踪溯源，清晰掌握攻击过程全貌，才能迅速采取动作，遏制攻击扩散，实现积极防御。

构建 1+N 的威胁感知系统为集团实现“一体化”防护

2020 年，深圳二院立足规划的全局性和前瞻性，启动威胁感知系统的建设。奇安信提供的产品及解决方案更符合医院和集团的需求，双方达成了合作意向。

在具体实施方面，深圳二院按照循序渐进的原则推进整体方案建设。第一步，深圳二院基于分布式大数据架构，将天眼的流量传感器作为数据采集的原点，收集出深圳二院（内科楼、外科楼）、大鹏妇幼保健院、南澳人民医院、葵涌人民医院、大鹏医疗集团全网所有的流量数据，并利用数据标准架构来进行清洗、存储和计

图：天眼威胁感知系统



图：天眼“仪表板”界面

算分析，实现一体化的流量数据采集。

第二步，深圳二院将整个集团的数据归总在统一的展示层面，构建出“网络威胁感知系统”，即安全运营监管中心（威胁分析平台），从而对深圳二院的内、外科楼，以及大鹏医院集团内、外网，下属区级医院等的医疗信息化系统，实现一体化运营和监管，实现安全的态势感知、安全分析、安全评估、安全运营等大数据安全监管能力。

最后，整个大鹏新区医疗集团利用云端的安全大数据决策体系，提供威胁情报、失陷主机检测等各类 SaaS 安全服务，为本地的安全体系赋能，实现真正意义上的“云地协同、数据协同”的一体化效果。

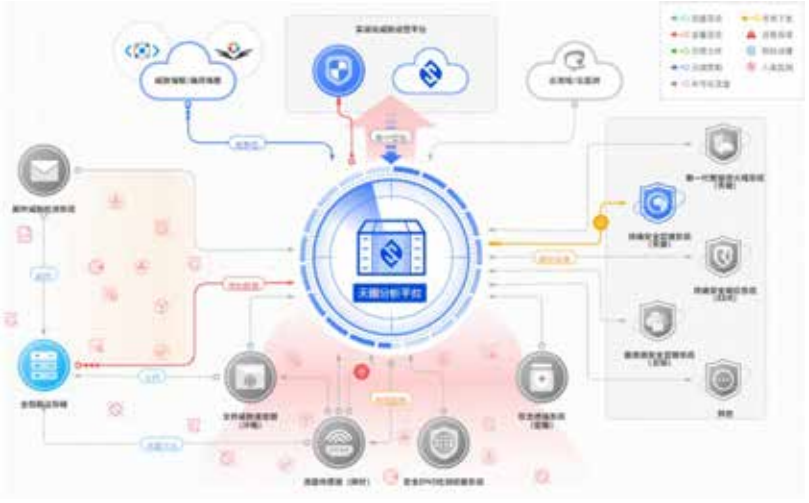
“在运行过程中，天眼在高级威胁检测、回溯分析、威胁情报等方面的能力，让我们印象深刻。”潘科长表示。同时，天眼还具备强大的协同联动能力，通过终端 EDR 联动、防火墙 NDR 联动与自动化编排处置，帮助用户快速定位感染主机和恶意软件，并及时的阻断威胁，提升网络攻击的响应和处置能力。

“以往网络安全和业务运营经常相互独立、缺乏协同，但基于天眼构建的网络威胁感知系统，最重要的就是将网络安全和业务运营紧密地融合到了一起。”潘科长总结道。

网络安全建设成果屡获肯定安全运营是未来重点

从实践效果来看，大鹏新区医疗集团的信息化和网络安全建设成果，获得了各大主管机构的肯定。“去年集团过了电子病历六级测评，今年正在通过互联互通评测，目前这些指标在全国一千多家三甲医院中名列前茅。而在信息化水平占据相当比重的国家卫健委三级公立医院绩效考核中，深圳第二医院连续两年全国前列、深圳市排名第一。”

在谈及医院未来的网络安全建设规划时，潘科长着重强调了安全运营的重要性，“部署网络安全设备只是打好基础，安全运营才是网络安全工作最为关键的一步。”据悉，未来医院及集团分支医院还将纳入天眼大家族中更多的产品成员，并将数据、技术、人员和流程等有效结合起来，形成面向实战的安全运营体系，为集团数字化转型保驾护航。 安



图：天眼的威胁感知家族体系

擅长的就是从无到有
奇安信高质量发展的践行者
——安服子公司“数据运营可视化信使” 桂文峥

作者 公关部 包世玉

在奇安信安全中心的一间会议室内，坐在面前的这个年轻人是奇安信安全服务子公司的桂文峥，“工作生活当中做事情不能总想着凭什么，不凭什么，不能只对有明确收益回报的工作感兴趣，而是应该对认为值得做、需要做的工作全力以赴。”他一改往日的随和，指着面前满屏的数字认真地说道。

安服子公司拥有同行业最大规模的专业队伍，业务范围覆盖全国各地。日常涉及的服务内容包含渗透测试、咨询规划、威胁检测、攻防演习、重保、应急响应等各类安全服务。

桂文峥解释到，在这样的一个庞大体系组织下，仅一个月就会产生各类海量数据。包含按周、按月、按区域、按行业生成的各个维度的数据表格就有几十个，而且还涉及商机、订单、留存、收入、工时、项目管理等方方面面，这样庞大的数据仅仅只是阅读这些数字就会陷入到一片混乱之中，若不进行有效处理，就很难发挥出数据应有的价值。

提起这个话题，桂文峥打开了话匣子。

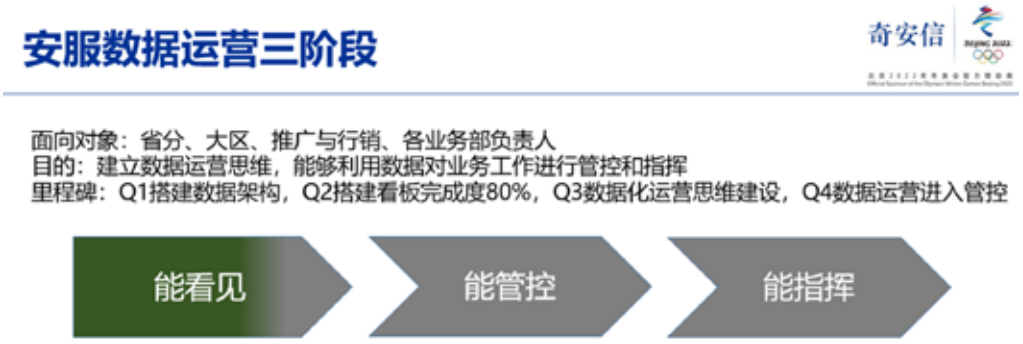
数据可视化初体验

“表格中原始的数据很多，但是有价值的内容都被深藏在里面，查看数据的人也无法快速高效地获取有价值的信息，更谈不上利用数据的价值助力业务成长。”说着，桂文峥打开了众多原始数据表格中的一个，每个类目下少说都有一万多条数据。

其实这个数据量从处理数据角度来讲不算多，但从数据运营的角度来说需要更多的提炼，通过挖掘数据进行不同视角、不同维度的内容分析与展现，能够帮助管理者更快速、更直接地获取到最重要的信息，进而通过数据进行管理和指挥，助力整个安服组织进入数字化、精细化管理的道路。

“基于齐总提出下一阶段的“高质量发展”目标，如何通过数据来助力这个目标，通过数据切片、层层抽丝剥茧地把各种维度的各种问题定位到具体的责任人，我与我的老师王凯开始从每个表中的每一个字段开始思考背后的价值。我们把数据运营分为了三个阶段：能看见、能管控、能指挥。”

于是，年初桂文峥接到了第一项新任务——对安服体系内庞大的数据进行清洗和提炼，要双手沾泥的深入



到数据和业务中去。

老师王凯跟他说过：“做事情重要的不是如何做，而是为什么做、价值是什么，要站在使用者视角思考，真正的解决业务痛点。让庞大的数据发出声音，整体数据可视化的第一步就是清洗。大量的表与表的逻辑关系、字段之间的不同解释方式曾经让我深陷数据的泥潭，但双手沾泥的精神始终激励着我，哪怕耗费再多时间，当厘清一条逻辑线就会让我的疲劳荡然无存。”

如果说老师提出的是整体的目标和要求，那么桂文峥要做的就是一步一步的将老师的设计落地实现，“当第一次了解到这个工作的时候，我就非常认同这个目标，想要满足公司对高质量发展的要求，就需要尽可能给管理者多配方便并锋利的武器——数据就是最好的武器。”

起点就是三阶段里的第一个，先让数据可以看到。看到不是单纯的可视化，更深层次的是能看懂。进一步能管控，最后做到能指挥，让数据呈现出它该有的价值，让数据说话。

但桂文峥明白，这条路是要先从第一张数据汇总表开始的。让公司直接投入大量的资源，去开发一个还尚未清晰的数据运营工具并不现实。于是桂文峥通过多个汇总表，最终像乐高一样累积成“数据看板”。

初步的尝试就通过最基础的 Excel 来实现，既方便修改迭代，也方便他人使用。从一张张的简易报表开始，“数据看板”开始快速搭起来。桂文峥从一个项目经理且 Excel 小白的身份开始了神奇的转身，每天思考如何利用 Excel 的功能做出大家需要的数据。他笑着说道：“甚至后来我在回家路上刷短视频，给我推送的全都是关于 Excel 使用技巧的，不过有些内容还真的让我用在了实战中。”

今年春节假期，在桂文峥持续七天的工作后，第一代基于 Excel 的——“安服数据运营看板 1.0.0”终于定稿诞生了。说着他打开了第一代看板， Excel 表内将汇总出的重点数据一一呈现，功能初见眉目。接着他打开如今正在使用的“安服数据运营看板 6.7.0”——数据逻辑严谨、布局规整清晰、维度整合全面，可以说是脱胎换骨地提升。若不是外面套着 Excel，还误以为是一个标准的 Web 页面，无论从观感还是使用上都可以媲美一款成熟的数据看板应用。

桂文峥说：“在近几个月的尝试中，每周必出一个小版本，有时甚至一天就有一版更新，把一个基于 Excel 的看板迭代，生生变成了软件开发的节奏。现在，部门管理者打开看板就能够看到整体各维度下的业绩完成进度情况，从订单到毛利、从项目状态到工时成本、从晨会到工单评价，基本覆盖了所有日常管理需要的信息，拉齐了安服体系内的信息。”

关于数据拉齐的重要性，桂文峥举了一个例子：比如说一个人拿到体检报告呈现的结果是肺不好，医生能得到的也只是“这个病人肺不好”这一个比较片面的信息。

如果这个时候还有另外一份报告写出这个病人还有 25 年的吸烟史，那么医生很容易回溯到了这个人肺不好的根源。如果这两个报告不结合起来看的话，医生获得到的信息是不对称的，用药也无法用到点子上。

同样，看板的作用就是将不同维度的数据汇总、处理、可视，保证最终安服系统内决策时信息的对称，这是安服体系内大量数据的价值，也是这套数据看板最初开始的初衷。

数据可视化之路

桂文峥说道，这套看板距离最终实现能管控、能指挥的目标还有很远的距离。这一路更新迭代中，也是一直在摸索中前进，没有任何同样的东西去对标。就像齐总说的，奇安信目前是规模最大的一家网络安全公司，这么庞大规模的安服体系也是罕见的，很多事情都是开天辟地第一桩。公司上一阶段实现了高速发展，那么下一阶段就要向高质量发展去发力。

持续不断的迭代下，数据运营看板才能有如今的效果，而如何迭代，正如前文所说，要看清需求与目标之间的差距。桂文峥说这还是要感谢很多领导的信任与支持、感谢各地方安服伙伴的沟通与帮助。

在数据运营的改进路上，还有另外一个问题：如何才能持续不断地了解需求，打通上下通路，改进看板？

桂文峥提到在这其中一件看似很小，却很重要的事情。因为安服在全国有数百名伙伴担当项目经理，很多时候信息难以及时同步。他的老师王凯与他讨论后，做了一个看起来难以实现的决定，他们向全国的项目经理承诺：“只要遇到了你们解决不了的问题，我们来兜底，负责联络所有部门直至问题的解决。做到事事有响应、件件有回音，确保所有的疑难杂症都有出口！”

虽然这种事情会占用大量的工作时间和精力，但正是这样的经历，让他快速地理解业务遇到的各种运营上问题，后期，同样也反哺了数据看板的迭代，促进了数据运营的进程。

从领导和同事的反馈中可以看到，安服体系内对于桂文峥的这套“安服数据运营看板”是高度认可的，效果大家有目共睹。但他自己还不满足于现在的成果，关于“数据运营的梦想”还有很多。在问题中迭代创新，正所谓老师领进门，桂文峥也在一次次的迭代中自我修行、升级打怪。

数据可视化的走出去

在短短几个月的尝试后，数据运营可视化这个理念，被桂文峥应用到了奇安信之外。他想，如果让服务的客户能够从单纯的只能听到奇安信工作内容，转变成每天每时每刻能获取奇安信的工作成果，是可以大幅度提高

客户体验的。

这项尝试要从一年一度的网络安全实战攻防演习说起。今年的演习期间，桂文峥被派入某客户现场，他发现，在以往的演习期间，大量的原始数据最后汇总到客户领导那边的就只有一个总数，更多的是最原始的数据，而这些数据背后可以挖掘的价值就浪费掉了，大量的数据堆积也不利于客户观看和使用。于是桂文峥想，那干脆将数据可视化也应用到这里来。

于是在演习正式开始之前，桂文峥就根据历史数据尝试做出一套数据可视化工具，应用到网络安全实战攻防演习中；演习开始前两天，通过数据间的交叉对比，不断完善工具模板；在演习第三天开始，“网络安全实战攻防演习项目数据可视化工具看板”正式投入使用。

桂文峥解释到，这套集合了所有现场运营数据看板的最终目的很明确——让客户随时能够获取演习中的运营数据展现，一眼看到他们最关心的内容。如果客户需要回看、对比数据进行分析，看板就可以提供数据回溯接口，起到通过储存数据观察链路的作用，大幅度解决了客户的需求。

毫无疑问，有了内部经验，加上痛点抓取准确、数据精炼符合客户刚需，数据看板一拿出来就得到了客户的好评。在客户期望之外，主动为客户提供超出其预期的数据运营服务，切实通过数据可视化为客户实现更多的价值，也是奇安信人的价值体现。

“我不怕困难，也很爱分享。”从交谈中可以看出，眼前这个温润儒雅、工作认真的年轻人是一个对工作有追求、对生活有期待的积极乐观的人。

“愿你内心山河壮阔，始终相信人间值得”是桂文峥在蓝信中的签名。

“成年人的世界没有童话，眼中既然是星辰大海，就无需惧怕路途荆棘，坚持走下去便是了。”这是桂文峥很久之前看到的一句话，也是他现在的座右铭。

在奇安信，这样有梦想有理想，低调谦逊做事，又无惧辛苦困难的年轻人不在少数。每一次交谈，认知的边界又拓了一程，获得的是信息、是成长、是故事，也是期待与希望。正是这样的一份份坚持和坚守、对工作的不懈追求成就了奇安信人卓绝的风采，也成就了一个个独自闪光的人生坐标。安

大事记

奇安信亮相 2021 全球工业互联网大会 与省政府、9 单位达成合作

10 月 18 日至 19 日，2021 全球工业互联网大会在沈阳召开。奇安信集团董事长齐向东在演讲时表示，传统工业相对封闭可信的生产环境被打破，网络攻击面不断扩大，这需要工业互联网平衡好开放和安全的关系，通过经营安全应对当前的网络安全威胁。而经营安全需通过“一中心两体系”构建起具有自适应、自主和自成长能力的安全系统，覆盖工业互联网全业务流程、各数据全生命周期，并通过不断循环升级，让安全能力与日俱增，实现对安全系统的动态掌控，守护工业互联网安全。

当日，奇安信集团与辽宁省人民政府签署协议，在网络安全领域达成全方位战略合作。齐向东表示，辽宁应用场景资源丰富、优势明显，奇安信将充分发挥企业技术和产业优势，积极参与辽宁产业发展和转型升级，助力数字辽宁、智造强省建设。

大会期间，奇安信还与中国工业互联网研究院、大连海事大学、沈阳航空航天大学、辽宁农业职业技术学院、沈阳市沈北新区政府、中国联通辽宁分公司、中国移动辽宁分公司、中国电信辽宁分公司、铁法煤业集团大数据运营有限责任公司分别签订了战略合作框架协议。

同时，在“工业互联网 + 网络安全”高峰论坛上，奇安信被工联院授予为“第一批网安技术支撑单位”。

张国清会见奇安信集团董事长齐向东

10 月 17 日，省委书记、省人大常委会主任张国清在沈阳会见奇安信科技集团股份有限公司董事长齐向东。

张国清说，辽宁高度重视网络安全和信息化事业发展，希望奇安信集团在提高辽宁网络安全水平上发挥更大作用，希望双方在网信领域深化产业合作、集聚人才。

齐向东表示，辽宁应用场景资源丰富、优势明显，奇安信集团将充分发挥企业技术和产业优势，积极参与辽宁产业发展和转型升级，助力数字辽宁、智造强省建设。我们对与辽宁合作充满信心。

31 个省、市、自治区，近百地……奇安信与各地伙伴共绘网安周“安全地图”

10 月 11 日至 17 日，2021 年国家网络安全宣传周在全国范围内广泛开展。奇安信集团与各地政府、行业及区域伙伴紧密合作，深入参与全国 31 个省、市、自治区，近百地网安周活动，面向全社会不同人群进行网络安全宣传推广，共同绘制覆盖全国各地、下沉至社区的“安全地图”。

政府、商会、校园 奇安信华北多领域交流分享

在首都北京，奇安信集团董事长齐向东受邀在全国工商联主办的德胜门大讲堂、水利部网安周宣传活动中进行分享，从网络安全行业领军企业的角度强调了“经营安全”的重要性：目前，勒索攻击正在成为“流行病”，企业需要通过对业务和系统安全的动态掌控，实现安全经营。

同时，奇安信作为财政部网络安全周连续三年的技术支持单位，为财政部本部筹划组织了 2021 网安周宣传活动；此外，奇安信还参与协办了北京市网安周校园日宣讲活动，特聘专家讲师杨天识就《网络安全发展形势与对策建议》主题，结合网络安全新法律法规，为学校师生分析解读当前网络安全发展态势，助力宣传普及网络安全知识和防护技能。

在辽宁大连，奇安信与大连海事大学联合共建船舶网络安全实验室，推出了国内首创的船联网安全舱应用场景演示，吸引了大批观众驻足。

揭牌、支撑、合作！奇安信西南之行硕果不断

在重庆，奇安信集团总裁吴云坤出席重庆网络安全宣传周活动中发表讲话，他从数据安全角度出发，建议企业重点围绕保护数据和应用，构建内生安全系统，通过经营安全落地形成实战化安全体系，实现对网络安全的动态掌控。

网安周期间，奇安信被评为 2020—2021 年度重庆

市网络安全优质服务企业。同时，由璧山区政府和奇安信集团共同建设的重庆市网络安全软件供应链安全检测中心也正式揭牌运行，该中心由重庆市委网信办领导，是全国首个专业从事软件供应链安全检测机构，开创了企业和政府在此领域合作的先河。

在贵州，奇安信独家协办 2021 年贵州省国家网络安全宣传周活动、独家承办 2021 年贵阳市国家网络安全宣传周活动。同时，奇安信作为独家网络安全企业与贵州省委网信办就助力贵州数字乡村发展签约战略合作协议。此外，奇安信还被遴选为贵阳市网信系统应急支撑单位。

在西藏，奇安信被国家计算机网络应急技术处理协调中心西藏分中心授予了 “网络安全应急服务（核心）核

心支撑单位”和“信息报送专项奖”两项荣誉。

数据安全与人才培养并重 奇安信华南多主题深入分享

广东作为试点首席数据官制度的先行者，对数据安全十分重视。在广东省网安周和广州市网安周的系列活动中，

奇安信副总裁韩永刚重点分享了数字化时代的数据安全建设思路。

由奇安信承办的广州市“数据安全与个人信息保护论坛”，邀请中国工程院院士沈昌祥，广东工业大学教授、哈尔滨工业大学（深圳）教授等专家学者，从《数据安全法》出发，深入交流数据安全与个人隐私保护的安全之道。

同时，在奇安信承办的“网络空间安全人才培养论坛”上，奇安信集团教育产品部负责人林雪纲做了《信息安全从业人员调研分析与奇安信人才培养模式实践》的主题报告，和多位高校、研究机构专家专家共同探讨人才培养模式的新模式、新经验。

冬奥安全、车联网安全、反诈互动 奇安信西北行全面科普网安知识

在西安 2021 年国家网络安全宣传周网络安全博览会上，奇安信携“冬奥网络安全运行指挥中心系统”模拟系统、“工业抽油机仿真沙盘”、态势感知和城市运营中心、车联网安全解决方案、反诈互动体验等多项内容亮相，一经亮相即吸引观众驻足观摩。

而在 10 月 12 日西安举办的汽车数据安全论坛上，奇安信集团首席战略官刘勇作为安全企业代表，分享了“四轮驱动”的车联网安全防护体系建设思路。

为进一步提高民众网络安全意识，奇安信还在官网上线了网络安全系列科普课程，通过 8 期不同的视频内容，更详细、深入的为广大网友科普个人网络安全、网络战、冬奥安全等网络安全概念。科普视频被全国近百家大型政企机构所引用，在各大平台上的累计播放量超过 10 万 +。

在新疆，网安周活动以线上 + 线下结合的模式展开，奇安信作为协办单位，设立展位，以专业、全面的安全能力协助开展相关宣传活动。

本届网安周期间，奇安信支持、参与了全国 31 个省、市、自治区，近百地的网安周主题活动，多位网络安全专家分赴各地，结合各主题日活动，上至部委机关，下至基层社区，面向各行各业及各年龄段进行网络安全宣传推广，点亮了一幅覆盖祖国大江南北的“安全地图”。

亮相天府杯 奇安信摘得天府杯破解大赛“皇冠上璀璨的明珠”

10 月 16 日至 17 日，2021（第四届）“天府杯”国际网络安全大赛暨天府国际网络安全高峰论坛在成都天府新区举行。

高峰论坛上，奇安信集团董事长齐向东在演讲时指出，所有网络攻击的核心都是利用漏洞，一点突破、层层渗透。只有通过经营安全来破解四大漏洞难题。而经营安全需要建立起“一中心两体系”，其中态势感知与管控中心是作战指挥平台，安全防护体系是一种协同作战体系，动态授信体系则可以破解“内鬼”信任难，以此逐一破解四大漏洞难题。

在产品破解赛期间，奇安盘古旗下盘古实验室在仅派出两位队员的情况下，不仅成功完成五大热门项目的破解挑战，还斩获 522500 美元（约合 3361765 元人民币）奖金。其中，在 16 日单项上完成了 iPhone 13 的全球首次公开远程越狱，1 秒钟取得手机最高控制权限，斩获了截至目前全球各类网络安全大赛中最高单项奖金——30 万美元。该破解项目还被主办方评选为“最具价值产品破解奖”。

在大赛期间，奇安信全新升级 MSS 安全托管服务，针对新形势下的网络安全问题，面向政企客户提供 7*24 小时全天候、全方位的综合服务，结合政企组织模式特点与实际情况，创新打造更具中国特色的安全托管服务。此次的全新升级，在重点打造中国特色的安全托管服务的同时，也有针对性的对服务内容进行升级改造，以更贴近政企客户的实际情况。

奇安信与贵阳市达成战略合作：助力贵阳成为“安全数谷”

10 月 16 日，贵阳市人民政府、贵安新区管委会与奇安信集团，贵阳经开区管委会与奇安信集团分别签订了《战略合作框架协议》。

未来，三方将在“中国数谷”贵阳，落地挂牌全国首个“数据安全开放及安全流通创新中心”、建设城市级大数据网络安全运营保障中心、建立大数据及网络安全运营工程师（西南）培训认证基地，从创新、技术、人才多方面进行示范性、先驱性合作，势将打造出国内网络安全领域领先的三大样板工程，为贵阳市数字产业化稳健发展做出新的贡献。

吴云坤出席第 36 次全国计算机安全学术交流会

“数据是数字化时代的生产资料，数据安全风险等同

于业务运营风险，数据安全更是关基保护的核心和关键。”10 月 15 日，奇安信总裁吴云坤在第 36 次全国计算机安全学术交流会上发表了以“面向关基保护的数据安全体系建设”为主题的演讲。

会上，专委会还特别授予了奇安信科技集团股份有限公司以第 36 次全国计算机安全学术交流会特别贡献奖。

接连中标移动、联通防火墙项目 与辽三大运营商签署战略合作

10 月 12 日，中国联通公布防火墙产品集中采购中标候选人名单，奇安信旗下网神智慧防火墙中标标包三（需求数量最多的防火墙品类），成为入围中国联通防火墙集采项目唯一的专业网络安全供应商。此次入围中国联通防火墙集采是奇安信在运营商行业的又一重大突破，标志着网神智慧防火墙在行业内已经取得了竞争优势。

不久前，奇安信还连续第二年入围中国移动硬件防火墙集采项目。“几大运营商的防火墙集采测试，向来被业内认为是中国含金量最高的防火墙测试，也是防火墙厂家综合实力的试金石。”奇安信边界安全负责人吴亚东表示，奇安信还将继续深耕运营商、电力、卫生、政府等安全市场，立足行业用户需求，持续提供高性能、高可靠的产品与解决方案。

在 2021 全球工业互联网大会上，奇安信分别与中国联合网络通信集团有限公司辽宁省分公司、中国移动通信集团辽宁有限公司、中国电信集团有限公司辽宁分公司签署了战略合作协议，奇安信将与三大运营商就信息基础设施、工业互联网安全、大数据与网络安全、智慧城市建设、船舶网络安全、人才培养等方面进行深入合作，共同构建辽宁省网络安全新格局。

北上广深 CA 厂商成为首批奇安信联合认证信任伙伴

日前，北京数字认证股份有限公司、上海市数字证书认证中心有限公司、数安时代科技股份有限公司和深圳市电子商务安全证书管理有限公司先后向《商用密码证书可信计划》提交证书入根申请，并均已通过奇安信、麒麟软件、统信软件联合认证，所提交的根证书将按计划预置于奇安信可信浏览器及银河麒麟操作系统、统信操作系统中。

这标志着国内主流 CA 厂商和奇安信、麒麟软件、统信软件将携手共同推动国产密码算法的应用，助力基于国产密码数字证书的信创环境安全访问体系持续完善，国密算法普及和发展工作将得到进一步提速。

北京市政协党组副书记、副主席杨艺文到奇安信集团走访调研

按照 2021 年度市区两级领导联系企业工作有关安排，日前，北京市政协党组副书记、副主席杨艺文围绕“完善‘服务包’制度 精准服务企业更好发展”主题，到奇安信集团走访调研。

杨艺文一行参观了奇安信安全中心展厅，并与企业负

责同志进行座谈交流。奇安信科团管理人员介绍了企业有关情况，提出服务诉求。相关部门负责同志介绍了北京市“服务包”制度相关情况，答复企业诉求并对企业在京发展提出建议。

奇安信集团牵头承担国家重点研发计划 “科技冬奥”重点专项启动会在京召开

9 日 30 日下午，奇安信科技集团股份有限公司牵头承担的国家重点研发计划 2021 年度“科技冬奥”重点专项项目启动暨实施方案论证会在北京奇安信安全中心召开。

奇安信集团董事长齐向东作为项目负责人，从项目简况、研究思路、实施计划、组织管理、成果及考核方式等五个方面对项目实施方案进行了详细介绍。清华大学诸葛

建伟、南开大学张健、中科院信工所刘玉岭、北京理工大学金福生、奇安信集团黄亮分别围绕课题研究任务、研究思路、单位分工、计划进度等四个方面对五个课题进行了详细介绍。

与会专家对实施方案给予了充分肯定，认为项目技术路线和考核指标明确；阶段目标和分工明确，计划安排合理；项目法人单位职责明确，交流及检查机制健全；实施方案合理可行。同时，重点围绕项目实施方案的细化分解和示范应用场景等方面提出了具体意见和建议。

奇安信“一中心两体系”护航全国第十四届运动会完美收官

2021 年 9 月 27 日，第十四届运动会闭幕。同时奇安信护航第十四届全运会的网络安全保障任务完美收官。

作为第十四届全运会组委会指定网络安全承建单位，自 2020 年 10 月开始，奇安信集团在赛事组委会统一安排下，全程参与了第十四届全运会的网络安全保障工作，并于 2021 年 5 月正式投入安全运营，为全运会云网平台、赛事管理系统、竞赛信息系统、竞赛专网、赛事互联网、全运村、开幕式、闭幕式场地和 60 个竞赛场馆的安全运行提供网络安全保障。

据统计，历时一年多网络安全重保工作，奇安信从安全建设、安全运营到值守保障共投入安全专家和技术骨干 450 余人，累计 8000 余人天，先后部署态势感知与安全运营平台、天眼新一代威胁感知系统、全球鹰互联网安全云监测系统、云锁服务器安全管理系统、天擎终端安全管理系统、虚拟化统一服务器安全管理系统、新一代智慧防火墙、Web 应用防火墙及抗拒绝服务系统（Anti-DDoS）等各类安全产品近 500 台套。

全球鹰网络空间测绘搜索平台正式发布

在 2021 中关村论坛国际技术交易大会上，奇安信正

式发布全球鹰网络空间测绘搜索平台，面向实战攻防演习、未知资产发现、互联网暴露面排查等多个场景，助力企业实现互联网资产的可查、可定位、可识别。该平台还入选了 2021 中关村论坛国际技术交易大会百项新技术新产品榜单。

据介绍，通过网络空间测绘技术，全球鹰测绘平台可以提供 IP、域名、开放端口、应用 / 组件、所属企业等关键安全信息，同时结合攻防场景绘制了资产画像与 IP 画像，实现互联网资产的可查、可定位、操作可识别的检索，助力企业日常的安全运营工作，如未知资产发现、风险识别、漏洞修复等。

圆满完成中关村论坛网络安全保障任务

以“创新发展”为永久主题的中关村论坛自 2007 年开始，历经十多年发展，已成为世界级、全面、开放的科技创新高端国际论坛。在网络安全主管部门的统筹部署下，奇安信圆满完成了此次网络安保任务。

奇安信此次重保负责人介绍，为切实做好 2021 年中关村论坛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，在服务范围内累计投入 42 人天，全面落实了各项安全工作和防护措施，保障了 2021 年中关村论坛活动的顺利进行，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。

齐向东出席 2021 世界互联网大会

“关键基础设施安全面临三大威胁：外部攻击、内部攻击、告警和处置。”在 2021 世界互联网大会“网络安全技术发展和国际合作论坛”上，奇安信集团董事长齐向东表示，关键基础设施作为国家网络安全战略的核心，可通过“一中心两体系”针对性解决三大安全威胁。

“企业要避免成为数字鸿沟的牺牲品。”在“一带一路”互联网国际合作论坛上，齐向东强调，数据代表信息、质量、生产力和生命线，企业要加快数字化转型，同时要守住数据流动的红线。

奇安信也在为缩小数字鸿沟做努力：一方面，加入“数字化转型伙伴计划”，推出“安全数据港”“安全虎符卫士”和“安全移动办公”三大项目，弥合中小企业和大企业间的数字鸿沟。另一方面，深入贫困乡镇，输送数字设备和资源，助力数字乡村建设，弥合城乡间的数字鸿沟。

与之江实验室达成战略合作 打造数字化网络安全样板

在 2021 乌镇世界互联网大会期间，之江实验室与奇安信集团宣布达成战略合作。此次合作，奇安信将与之江实验室共同打造三个样板：围绕浙江数字化改革，打造数字化网络安全的样板；围绕浙江共同富裕示范区，打造高质量发展的浙江样板；围绕浙江民营制造业创新，打造智

能制造的样板。双方将以此三个样板，为浙江省的数字化改革和共同富裕示范区建设提供全面的网络安全保障。

奇安信总裁吴云坤：落实数据安全法的三大举措

世界互联网大会期间，奇安信集团总裁吴云坤在数据治理实践论坛圆桌对话上表示，目前数据安全领域面临着三个挑战：从业者需要新概念、领域需要新理论、发展需要新技术。

吴云坤介绍，为落实数据安全法，奇安信一直在做三件事：一是建立体系化技术，二是奇安信一直在做规划，三是投资做研发。目前奇安信投入了营收的 40% 进行研发。奇安信已帮助涉及个人信息的机构、行业和企业构建数据安全保障体系，防御内外部威胁，保护其数据安全，避免信息泄露。

与云宏信息结成核心战略合作伙伴 致力虚拟化安全创新发展

9 月 24 日，奇安信科技集团股份有限公司与云宏信息科技股份有限公司战略合作签约仪式在广州举办。双方就网络安全建设、虚拟化安全领域等方面的合作达成共识，结成战略合作伙伴关系，并将开展长期合作。

奇安信与云宏信息将互相认定为彼此的核心生态合作伙伴，并在合作模式上进行深度融合：云宏信息将企业自身安全、自有产品安全完全依托奇安信安全体系进行建设，奇安信也将为云宏在打造“最安全的中国云”的征途上提供坚强有力的安全支撑。奇安信将依靠自身先进的安全理念、成熟的安全架构和安全运营，向云宏输出安全能力，并与云宏的自有产品进行深度融合，在保障云宏自身网络和产品安全的同时，更好地服务于云宏的客户。

年度最大白帽行业盛典！第五届补天白帽大会圆满落幕

9 月 17 日，面向全球白帽和技术精英的全球性安全行业大会——2021 补天白帽大会在北京举行。作为《网络产品安全漏洞管理规定》（以下简称“规定”）正式实施后的第一个白帽行业盛会，来自监管机构、安全团队、研究机构的嘉宾和顶级白帽近千人汇聚一堂。

齐向东出席中国信息化百人会 2021 峰会

“数智时代，保障数据安全成为网络安全的核心任务。”在中国信息化百人会 2021 峰会主论坛上，中国信息化百人会成员、奇安信集团董事长齐向东发表演讲时表示，需要构建内生安全系统，通过经营安全，实现对网络安全的动态掌控，以解决数智时代数据安全的复杂难题。

齐向东提出，可通过“网络安全建设三部曲”解决数智时代数据安全的复杂难题：把内生安全理念，用系统工程方法落地成完整的安全防护体系，最后通过经营安全做到对网络安全的动态掌控。

中国信通院发布《勒索病毒安全防护手册》 奇安信等 7 家单位共同编制

在工业和信息化部网络安全管理局指导下，中国信息通信研究院联合奇安信等 7 家单位共同编制了《勒索病毒安全防护手册》（以下简称《手册》），奇安信相关团队全程参与《手册》的编制工作，并提出了 13 条防护举措、45 条实操细则，指导防范和应对勒索病毒攻击风险。

为应对勒索病毒攻击的新特点，《手册》提出围绕“事前预防、事中应急、事后加固”三个环节，从管理、技术两个方面防范化解攻击风险。奇安信还在《手册》中给出 13 条防护举措、45 条实操细则，以切实可行的勒索病毒攻击安全防护措施，指导防范和应对勒索病毒攻击风险。

奇安信与南京信息工程大学达成战略合作

9 月，奇安信集团与南京信息工程大学在奇安信安全中心签署战略合作。根据协议，双方将充分发挥各自优势，在人才培养、科研创新、网络安全技能认证培训中心建设与校园网络安全运营体系建设等多方面开展深入合作。

齐向东受聘为车联网身份认证和安全信任工作专家委员会委员

“及时发现、修复漏洞对车联网安全至关重要。其中，身份认证成为影响车联网安全的关键因素。”在车联网试点工作启动会上，奇安信集团董事长齐向东作为安全企业代表，围绕“基于双证书体系融合应用的车云通信安全能力建设项目”介绍试点项目详情，并受聘为车联网身份认证和安全信任工作专家委员会委员。

此前，工信部在全国范围内开展车联网身份认证和安全信任试点工作，经过 2 个多月层层筛选和评估，最终评选出 61 个试点项目。奇安信作为主要参与单位之一，成

功入选 4 个项目。其中，“基于双证书体系融合应用的车云通信安全能力建设项目”由奇安信牵头申报，联合 8 家单位，围绕车联网服务平台车云通信场景开展试点应用工作，通过建立车云通信身份认证、数据加密等技术能力，实现各类车云通信场景下的身份认证、数据机密性和完整性保护，构建车云通信安全保障能力。

齐向东出席 2021 中国国际服务贸易交易会

“数字贸易没有‘数字海关’，企业想要安全经营，就得‘自证清白’。”在 2021 服贸会“数字贸易发展趋势和前沿高峰论坛”上，奇安信集团董事长齐向东表示，数据安全是企业安全经营的生命线，企业需要通过建设数据安全系统来守住数据安全红线。

“数据安全系统必须是内生安全系统”，齐向东表示，用“网络安全建设三部曲”：内生安全的理念、内生安全框架的方法，最后通过经营安全做到动态掌控，以此建立“自证清白”的内生安全系统。

“电商 APP 的数据覆盖面广、敏感度高，一旦泄露危害巨大。”在2021服贸会“2021中国电子商务大会”上，齐向东表示，面对频繁曝出的 APP 隐私数据泄露事件，需要针对“满足监管、发现问题、整改问题、促进发展”四大焦点有的放矢，保障 APP 隐私安全合规、健康发展。

“数字”成为今年服贸会的关键词。奇安信集团作为唯一一家网络安全厂商，亮相服贸会数字服务专题展区，以“冬奥标准奇安信，网络安全快一步”为主题，全面展示新一代网络安全框架。

服贸会期间，奇安信正式发布“数字城市网络安全运营中心”。 奇安信数字城市网络安全运营中心借助于奇安信自身强大的威胁情报、大数据安全技术，结合数据驱动的实战化安全运行模式，可实现对网络空间安全态势全面掌控，精准锁定安全事件的各个环节，全面深入保障智慧城市运行安全，预警通报重大网络安全风险，有效应对重大网络安全事件，守护城市网络安全运行。

圆满完成 2021 年服贸会网络安全保障工作

9 月 2 日至 9 月 7 日，2021 中国国际服务贸易交易会（以下简称：2021 服贸会）在北京召开。作为网络安全领军企业，奇安信圆满完成了此次服贸会的网络安全保障工作。

奇安信此次重保负责人介绍，为切实做好 2021 服贸会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，在服务范围内累计投入超过 300 人天，全面落实了各项安全工作和防护措施，保障了 2021 服贸会系列活动的顺利进行。

亮相 2021 智博会 奇安信工业互联网安全西南总部项目签约落户重庆

8 月 23 日，以“智能化：为经济赋能，为生活添彩”为主题的 2021 中国国际智能产业博览会在重庆开幕。奇安信携“冬奥标准奇安信 网络安全快一步”主题展示亮相智博会，通过签约合作、论坛演讲等多重形式，全面展示新一代网络安全解决方案。

在 2021 智博会的重大项目招商签约活动中，奇安信与重庆两江新区达成投资合作协议。根据协议，奇安信将在重庆两江新区成立全资子公司，建设区域总部项目，包括一总部一平台，即一个工业互联网安全西南总部、一个网络安全技术赋能支撑平台。

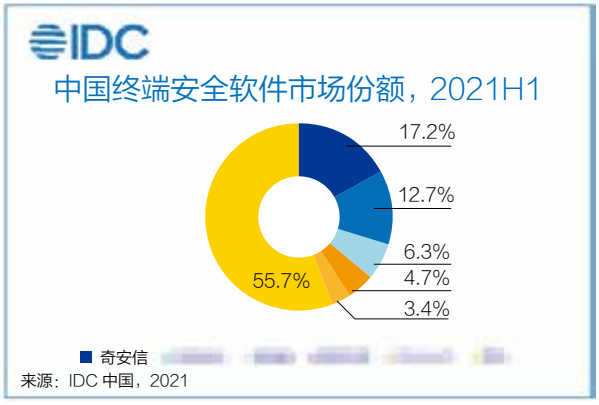
荣誉墙

双冠！奇安信终端安全、安全分析和情报牢据行业领先地位

国际权威咨询机构 IDC 正式发布《2021 上半年中国 IT 安全软件市场跟踪报告》中，奇安信在终端安全软件、安全分析和情报两个细分市场，凭借 17.2% 和 10.5% 的市场份额双居首位，牢牢占据行业领先地位。

针对终端安全领域，奇安信通过天擎终端安全管理系统（简称“天擎”）、服务器安全管理系统（简称“云锁”）聚焦终端安全保护。目前，天擎正在为 5000 万政企终端保驾护航，多次蝉联中国终端安全市场第一。

针对安全分析和情报领域，奇安信 NGSOC 综合安全感知能力、威胁情报、大数据分析技术和安全可视化等优势能力，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。此外，奇安信威胁情报中心已累计首发并命名 13 个国内外 APT 组织，监测到的针对国内发动 APT 攻击的黑客组织达 46 个。



奇安信荣获中国人民银行科技司“2021 年度优秀技术支撑单位”

日前，在国家网络安全宣传周期间的 2021 金融网络安全论坛上，奇安信获得中国人民银行科技司授予的“金融网络安全态势感知平台 2021 年度优秀技术支撑单位”荣誉。

在对中国人民银行科技司“金融网络安全态势感知平台”建设的支持过程中，奇安信充分发挥了威胁的发现定位能力，大大提升该平台的情报覆盖范围和共享信息能力，同时积极地支持金融网络的安全保障工作，充分地展示了优秀单位的社会责任感，也多次获得了中国人民银行科技司感谢函。

奇安信零信任项目入选 2021 人工智能安全典型实践案例

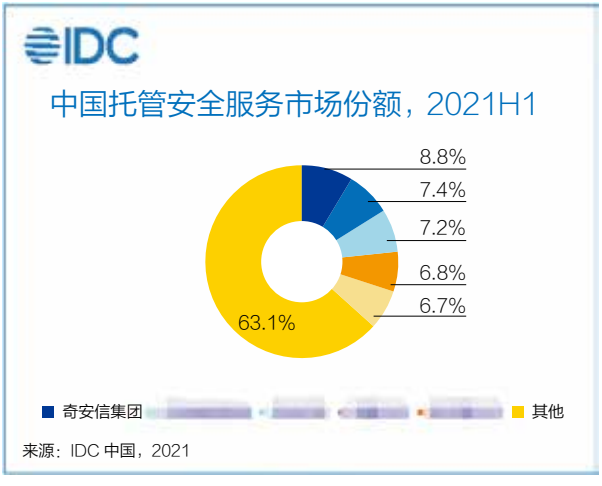
10 月 12 日，在国家网络安全宣传周人工智能安全产业发展分论坛上，奇安信提报的“支撑零信任安全架

构的人工智能信任决策系统”项目，在诸多优秀案例中脱颖而出，成功入选人工智能安全典型实践案例。

双细分领域第一 奇安信安全服务再获权威机构认可

国际权威咨询机构 IDC 发布的《2021 上半年中国 IT 安全服务市场跟踪报告》显示，在安全咨询服务和托管安全服务领域，奇安信分别以 5.1% 和 8.8% 的市场份额，双双位居细分领域第一名，领跑国内安全服务市场。

报告显示，2021 上半年中国 IT 安全服务市场厂商整体收入约为 11.1 亿美元（约合 71.5 亿元人民币），厂商收入规模较去年同期实现翻倍增长，涨幅高达 110%，较 2019 年同比增长 38%，中国 IT 安全服务市场正式进入需求全面爆发期。



来源：IDC 中国，2021

ATT&CK 攻击点覆盖第一 奇安信天擎 EDR 通过赛可达威胁检测能力测试

在国际知名第三方网络安全服务机构赛可达公布的最新一期测评报告中，奇安信天擎终端安全管理系统（EDR）（以下简称“天擎 EDR”）顺利通过赛可达实验室威胁检测能力测试，荣获“东方之星”证书。

赛可达实验室（SKD Labs）是国内外知名第三方信息安全测评认证机构，也是中国合格评定国家认可委员会 CNAS 认可实验室。本次测试共包含三个部分：ATT&CK 框架攻击技术覆盖面测试、基于场景的攻击链识别与深度检测及反病毒检出与防护测试。

测试结果显示，天擎 EDR 的 ATT&CK 框架攻击技术覆盖数量达到 164 个，可深度识别多种技术组合攻击的完整攻击链并生成攻击事件树，同时病毒查杀率达到了 99.2%，勒索病毒查杀率达到了 100%，病毒误报率为 0%。

奇安信四个项目入围工信部车联网身份认证和安全信任试点项目

近日，由奇安信集团牵头的四个项目成功入围由工信部网络安全管理局公布的车联网身份认证和安全信任

试点项目名单，分别是：“基于双证书体系融合应用的车云通信安全能力建设项目”、参与的“车云通信网络信任技术应用项目”“长沙车联网先导区身份认证和安全信任体系建设试点项目”“长安汽车车云通信身份认证和安全信任体系建设项目”。

据悉，“身份认证和安全信任试点项目”意在加快推进车联网网络安全保障能力建设、构建车联网身份认证和安全信任体系、推动商用密码应用、保障蜂窝车联网（C-V2X）通信安全。

奇安信获工信部移动互联网产品漏洞库特设组建设运维支撑单位称号

近日，工信部移动互联网 APP 产品安全漏洞库发布会暨安全漏洞管理特设工作组成立仪式在京举办，奇安信科技集团股份有限公司作为首批安全漏洞特设工作组成员单位之一，获“建设运维支撑单位”称号。

奇安信旗下补天漏洞响应平台报告漏洞数量超过 66 万个，平台白帽专家数量超过 85000 人，已成为重要机构和企事业单位漏洞响应的重要保障力量，先后被公安部、国家信息安全漏洞共享平台 (CNVD)、国家信息安全漏洞库 (CNNVD)，分别评定为技术支持先进单位、漏洞信息报送突出贡献单位和一级技术支撑单位。

奇安信连续三届入选 CNCERT 网络安全应急服务国家级支撑单位

日前，国家互联网应急中心（CNCERT）在 2021 年世界互联网大会上，为第九届 CNCERT 网络安全应急服务支撑单位颁发证书。奇安信同时入选国家级、APT 监测分析及反网络诈骗三项支撑单位名单。这也是奇安信连续三届入选 CNCERT 网络安全应急服务国家级支撑单位，体现了 CNCERT 作为国家网络安全重要支撑部门对奇安信安全能力的充分认可。

打造大数据安全保障标杆 奇安信零信任入选工信部示范项目名单

9 月 1 日，工信部正式公示了《2021 年大数据产业发展试点示范项目名单》，由奇安信参与的“面向垂直行业的零信任大数据安全访问平台建设及应用”项目，作为大数据安全保障标杆项目成功入选该名单。

奇安信身份安全实验室负责人张泽洲表示，该平台

能够帮助客户围绕数据分级分类构建防控重点，通过对用户访问数据过程持续评估，安全风险全程联防联控，实时应对外部攻击，有效防范内部泄密。该项目的建设及示范应用，能够帮助客户单位有效提升大数据平台安全防护能力，在历次重大活动的网络安全保障工作中取得了较好成绩。

奇安信四项产品全部入围 2021 年央采安全软件协议采购项目

近日，中央国家机关 2021 年安全软件协议供货采购项目成交公告发布，奇安信旗下网神安全分析与管理系统（NGSOC）、网神 SecVSS 3600 漏洞扫描系统、网神 SecFox 日志收集与分析系统 V5.0(LAS) 和天擎终端安全管理系统 V10（服务器端）参与的四款产品全部成功入围，成为本次央采安全软件采购项目的最大赢家之一。

根据中国政府采购网公示信息显示，本项目共 47 家响应人参与响应，评委会根据征集文件中确定的要求，从响应文件的有效性、响应人资质、实质性响应等方面对供应商的响应文件进行了符合性审查。此次四项入围充分体现了国家机关、政府行业专家及客户对奇安信产品能力的高度认可与肯定。

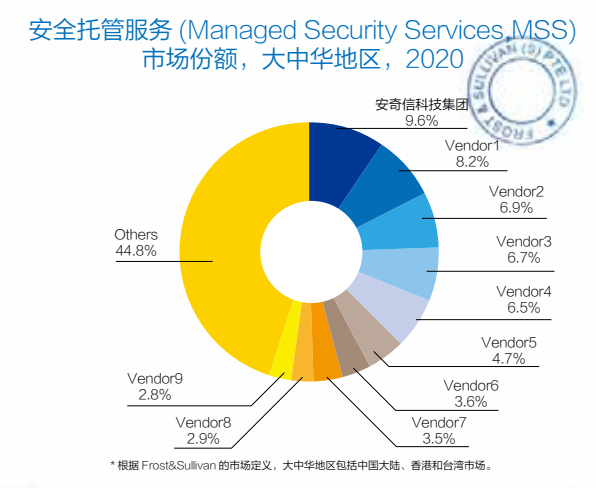
供应商名称	投标商品名称
福建深空信息技术有限公司	深空防篡改系统 V2.0
网神信息技术（北京）股份有限公司	奇安信天擎终端安全管理系统 V10（服务器端）
北京神州绿盟科技有限公司	绿盟终端安全系统 ESSV9.0（服务器端）
腾讯云计算（北京）有限责任公司	腾讯安全 - 零信任安全管理（iOA）系统终端安全软件（服务器端）
北京万里红科技股份有限公司	保密管理系统软件（服务端软件）

Frost & Sullivan 发布 MSS 报告：奇安信市场份额大中华区第一

近日，奇安信集团凭借技术优势和服务专业度，以 9.6% 的市场份额位列 2020 年大中华地区安全托管服务（Managed Security Services，MSS）第一名。此结论由全球权威分析机构 Frost & Sullivan 发布在《Asia-Pacific Managed Security Services Growth Opportunities》报告中。

报告数据显示，2020 年大中华区 MSS 市场年增长率高达 20.9%，政府部门和金融行业是该市场主要收入来源。奇安信作为主要领导者，在 2020 年通过扩展服务组合迅速进入安全托管服务市场，并从产品导向向服务导向转变，助力国内市场强劲增长。

作为领先的网络安全供应商，奇安信凭借专业的安全托管服务和管理团队，年增长率高达 51.1%，尤其是在政府部门和金融行业这两个主要领域具有强大的影响力。在 MSS 产品的可用性和完整性层面，奇安信拥有一系列采用率高于平均水平的服务产品，即拥有围绕端点安全、边界安全、云安全和 OT 安全的全面安全产品组合，可以利用其全面的专业知识来提供端到端的安全托管服务。



奇安信连续三年荣登“北京民营企业百强榜单”

9 月 16 日，奇安信荣登“民营企业百强”“科技创新”

及“社会责任”三大榜单，其中“社会责任”位列榜单第四，“科技创新”榜单位居网络安全领域第一。

中国最强“先进计算”网安企业 奇安信荣登“2021 中国先进计算企业百强榜”

9 月 17 日，在长沙举行的 2021 世界计算机大会发布“2021 中国先进计算企业百强榜”，奇安信荣登榜单，成为 2021 年度中国最强“先进计算”网安企业。

此次“先进计算企业百强榜”的评选，根据企业先进计算整体实力、企业参与先进计算程度、企业增长潜力和企业研发情况 4 大项一级指标和 20 项二级指标进行综合评估，是对中国企业界的数智化应用水平与创新能力的一次较全面呈现，将成为企业选择数智化转型路径的重要参考。

2021 年中国网络安全产业分析报告：奇安信“产业竞争力”第一

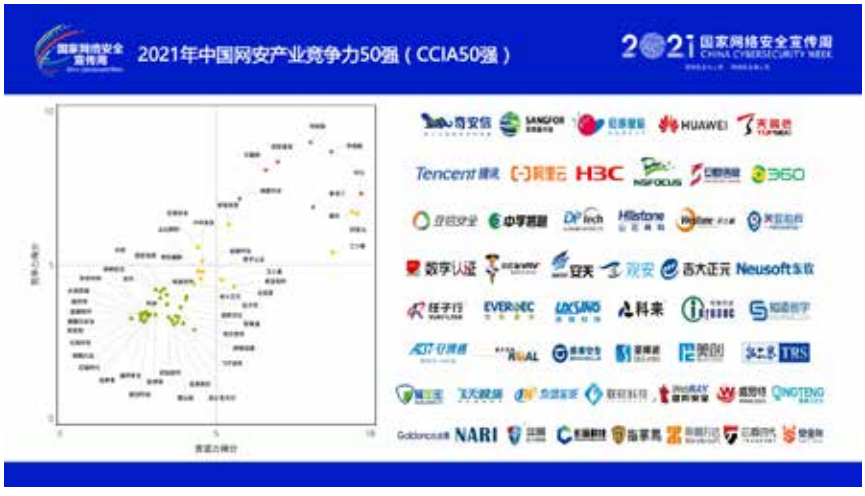
中国网络安全产业联盟日前发布了《2021 年中国网络安全产业分析报告》，报告显示，奇安信在 2021 年中国网安产业竞争力 50 强榜单中排名第一，成为产业竞争力最强的网络安全龙头企业。

报告同时认为，奇安信位于“产业领导者”象限，一方面是安全技术趋势和产业方向的引领者，同时又是安全领域投资并购主要的资金提供者和参与者，更是二级市场安全领域受广泛关注的热门标的。

国内唯一上榜 奇安信入围国际权威机构亚太安全咨询服务榜单

近日，国际权威咨询机构 Forrester 发布《Now Tech: Cybersecurity Consulting Services In Asia Pacific, Q3 2021》报告，奇安信作为亚太地区唯一入围的中国安全企业上榜。

在报告中，奇安信被划分为传统 MSSP 企业，主要覆盖银行、电信和企业组织等垂直领域。根据 Forrester 报告内容：“这类服务商通过技术、资源和产品帮助客户管理网络安全，主要擅长安全托管服务。”传统 MSSP 的特点是产品及服务的自动化、成熟度具备明显优势，在技术咨询与实施、安全团队支持、创新能力和灵活性等层面，水平相对较高。



奇安信

新一代网络安全领军者

聚焦安全运营，构建智能平台

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

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

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

将平战结合进行落地

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

重大安全事件的威胁预警

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

专业的安全运营服务

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

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证

奇安信

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。

奇安信位居“2021年中国网安产业竞争力50强”第一名

6月16日，中国网络安全产业联盟（CCIA）揭晓
“2021年中国网安产业竞争力50强”。
凭借在网络安全领域领先的技术实力以及突出的市场表现，
奇安信位居第一名。

“2021年中国网安产业竞争力50强”榜单

TOP15	公司名称	公司简称
1	**奇安信科技集团股份有限公司**	**奇安信**
2	深信服科技股份有限公司	深信服
3	启明星辰信息技术集团股份有限公司	启明星辰
4	华为技术有限公司	华为
5	天融信科技集团股份有限公司	天融信
6	腾讯科技(深圳)有限公司	腾讯
7	阿里云计算有限公司	阿里云
8	新华三技术有限公司	新华三
9	绿盟科技集团股份有限公司	绿盟科技
10	杭州安恒信息技术股份有限公司	安恒信息
11	三六零安全科技股份有限公司	三六零
12	亚信安全科技股份有限公司	亚信安全
13	中孚信息股份有限公司	中孚信息
14	杭州迪普科技股份有限公司	迪普科技
15	山石网科通信技术股份有限公司	山石网科