极牛网络安全通讯 • 社群期刊

2022 年 6 月 第 12 期

网安观察

P12 RSA2022峰会主题
安全的转型与未来

P11
俄罗斯通过《保护关键信息基础设施国家政策基本原则》草案

P17 RSAC 十大热点安全议题解读

P25 RSAC2022 24款热门安全产品

P28 APP违规收集个人信息风险分析报告

第12期
2022年6月

极牛网

极牛网 网络安全行业媒体

致力于促进中国网络安全行业创新思维的交流与碰撞，搭建中国网络安全技术社区和交流平台



技术格局

网安工程师的成长，需要锻炼开阔的技术视野和统筹全局的战略高度，能够着眼现在思考未来，做懂业务懂策略的工程师。

管理之道

网安工程师随着职业发展，必然面临着向技术总监、CTO等管理角色转型，改变管理思维，建立属于自己的管理哲学。

人才梯队

作为技术管理者，如何建立一个稳固、高效的人才队伍是核心任务，更应该从人才梯队的角度，关注人才的培养的更迭。

企业战略

技术管理者应该建立技术以外的格局，经济形势、商业模式、投融资等等，才能助力企业发展，做与创始人同频的CTO。

产品运营

敢于拥抱和应对变化，敢于创新，在创新的基础框架下，寻找创新的实践方法论，激发技术人员创新能力，推动业务发展。

布道能力

作为技术工程师，需要重点培养自己的布道能力，能将自己的技术成果和理念传播出去，才能拓宽和升级自己的认知边界。

中国共产党建党101周年暨《网安观察》创刊一周年

从明确提出“没有网络安全就没有国家安全”，到突出强调“树立正确的网络安全观”，再到明确要求“全面贯彻落实总体国家安全观”。党的十八大以来，以习近平同志为核心的党中央高度重视网络安全工作，就做好网络安全工作提出明确要求，为筑牢国家网络安全屏障、推进网络强国建设提供了根本遵循。

2022年6月1日，《中华人民共和国网络安全法》正式实施五周年。作为我国网络安全领域的基础性法律，《网络安全法》是我国网络空间法治建设的重要里程碑。

自1994年全功能接入国际互联网以来，我国就不断探索和推进互联网立法。近年来，我国加快推进网络安全领域顶层设计步伐，在深入贯彻落实《网络安全法》的基础上，针对各界关注、百姓关切的突出问题，制定完善了网络安全相关战略规划。

相继颁布了《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》等法律法规。出台《网络安全审查办法》《云计算服务安全评估办法》《汽车数据安全管理若干规定（试行）》等政策文件，建立了一批重要制度。

其中，由中央网信办等13部门联合修订的《网络安全审查办法》有力维护了网络安全和数据安全，为防范和化解国家安全风险保驾护航。

《网络数据安全管理条例》《数据出境安全评估办法》等配套实施细则正在制定并已公开征求意见，数据安全和个人信息保护法律法规体系框架已初步确立。

自《网络安全法》落地以来，我国不仅构建了切实有效的网络安全保障体系，还在推动网络安全人才培养方面，采取系列举措。在前期设立网络空间安全一级学科基础上，国家组织实施一流网络安全学院建设示范项目。截至目前，国内有60余所高校设立网络安全学院，200余所高校设立网络安全本科专业，每年网络安全毕业生超过2万人。

值此中国共产党建党101周年，以及《网安观察》创刊一周年之际，我们来回顾总结我国网络空间安全力量的发展，网络安全战略一步步稳健推进，网络安全产业也呈现蓬勃发展的态势，在未来的3年将是我国网安产业发展的黄金期，作为网络安全人，未来可期！

总顾问

叶绍琛

2022年 6 月28 日

CONTEN

目录



安全态势

P4 | 非洲最大连锁超市遭勒索团伙敲诈，600GB 数据被窃取

P4 | Mirai 变种 Miori 僵尸网络在国内大规模传播，浙江受影响最严重

P4 | 数万个开源项目开发账户遭大规模泄露：超 7.7 亿条日志暴露

P5 | 意大利第五大城市遭勒索软件攻击，导致全城断网近一周

P5 | 富士康墨西哥工厂遭勒索软件攻击，业务运营受干扰

P5 | 南非总统的个人信贷数据泄露：该国已沦为“黑客乐园”

P6 | Windows SMB 拒绝服务漏洞安全风险通告

P6 | Linux Kernel eBPF 权限提升漏洞风险通告

P6 | Confluence 远程代码执行漏洞安全公告

P7 | 国内攻防演习 5 月态势：哪些薄弱点最易被利用?

P10 | 国家能源局修订两项电力行业网络安全政策公开征求意见

P10 | 网信办修订《移动互联网应用程序信息服务管理规定》发布施行

P10 | 市场监管总局、网信办发布《数据安全管理认证实施规则》

P11 | 《零信任参考体系架构》等 4 项国家标准公开征求意见

P11 | 美国参议员提出《健康和位置数据保护法》，治理数据交易乱象



国际局势

P11
俄罗斯通过《保护关键信息基础设施国家政策基本原则》草案

ONTENTS



专题报道

P13
RSAC：安全的转型与未来

P17
RSAC十大热点议题解读

P28
APP违规收集个人信息风险分析报告



第 1 2 期

《网安观察》编辑部

主办　极牛网

总　　编　　辑：陈鑫杰
总　　顾　　问：叶绍琛
副　　总　　编：王文彦
威胁情报主编：乔跃春
移动安全主编：蔡国兆
网安人才主编：林俊濠
网安产业主编：张　程
网安赛事主编：余　浩
网安态势主编：王　震

公众号　小程序　网站

电子版请访问　www.geeknb.com　阅读或下载索阅、投稿、建议和意见反馈，请联系极牛网期刊编辑部。

E m a i l：hi@geeknb.com
地　　址：深圳市龙岗区天安云谷2栋2层
邮　　编：518000
电　　话：0755-33228862
印刷数量：1000 本
印刷单位：深圳彩虹印刷有限公司

版权所有 ©2021 极牛网，保留一切权利。
非经极牛网书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。

无担保声明
本资料内容仅供参考，均“如是”提供，除非适用法要求，极牛网对本资料所有内容不提供任何明示或暗示的保证，包括但不限于适销性或者适用于某一特定目的的保证。在法律允许的范围内，极牛网在任何情况下都不对因使用本资料任何内容而产生的任何特殊的、附带的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉或预期节约的损失进行赔偿。

事件篇

非洲地区网络威胁形势日益严峻。最大连锁超市遭遇数据勒索攻击，多国受影响。南非总统个人信息泄露，有黑客团伙指责该国已经成为黑客乐园，任何人都能轻松绘制出南非数字基础设施分布。



非洲最大连锁超市遭勒索团伙敲诈，600GB 数据被窃取

据 BleepingComputer 6 月 15 日消息，非洲最大连锁超市 Shoprite 披露，近期遭遇了一起安全事件，部分国家的客户可能受影响，姓名、身份证号等信息泄露。勒索软件团伙 RansomHouse 声称对此负责，称已窃取 600GB 数据，要求支付赎金。RansomHouse 还毒舌“点评”了 Shoprite 差劲的安全意识，如用明文文本和原始图片保存大量个人数据。Shoprite 在非洲 12 个国家经营近 3000 家门店。

Mirai 变种 Miori 僵尸网络在国内大规模传播，浙江受影响最严重

据 CNCERT 6 月 14 日消息，国家互联网应急中心（CNCERT）和奇安信近期监测发现一个新的且在互联网上快速传播的 DDoS 僵尸网络 Mirai_miori，传播方式主要为弱口令爆破及 1 day 和 N day 漏洞。监测分析发现，今年 4 月 6 日至 6 月 6 日 Mirai_miori 僵尸网络日上线境内肉鸡数最高达到 1.1 万台，累计感染肉鸡数达到 4.4 万。肉鸡排名前三位的省份为浙江省（37.2%）、云南省（10.9%）和河南省（6.2%）。

数万个开源项目开发账户遭大规模泄露：超 7.7 亿条日志暴露

据 TheHackerNews 6 月 14 日消息，安全研究人员发现，流行的持续集成开发工具 Travis CI 存在 API 漏洞，导致大量开发账户敏感数据暴露，超过 7.7 亿条 Travis CI 免费版用户日志数据以明文方式泄露，其中包含大量敏感机密信息（开发令牌、云服务凭证等），包括 Github、Docker 的数以万计的开源项目开发账户受到影响。Travis CI 是一种被称为持续集成的越来越流行的敏捷开发工具，通常缩写为 CI，它使开发和测试代码变更的过程自动化，已经成为现代开发和云原生应用程序管道的重要组成部分。

俄罗斯知名媒体电台遭黑客攻击：奏响乌克兰国歌

据 HackRead 6 月 9 日消息，俄罗斯生意人报电台（Kommersant FM）的播报在 8 日出现中断，转而

播放乌克兰国歌和其他反战歌曲。之后，广播很快中止。官方发布声明称，遭到黑客攻击，将尽快恢复播报。被黑客篡改的是生意人报电台的午间播报节目，该电台是俄罗斯知名私营媒体生意人报的广播版。英媒 BBC 记者 Francis Scarr 在推文中提到，当时生意人报电台播放了乌克兰著名爱国民歌、曾经的国歌《哦，草地上的红荚蒾》。

意大利第五大城市遭勒索软件攻击，导致全城断网近一周

据 BleepingComputer 6 月 9 日消息，意大利南部巴勒莫市 3 日（周五）遭受网络攻击，导致全城断网、IT 系统瘫痪近一周，给当地旅游业和城市运营带来灾难性影响。据当地媒体报道，受影响的系统包括公共视频监控管理、警务及市政府的所有（网络）服务。市民的出生证明、结婚证明及户籍和居住证明等文件都无法办理或变更，也无法使用网络进行交流或获取服务。Vice Society 勒索软件组织声称对此负责。巴勒莫拥有约 130 万人口，是意大利人口第五大城市。

富士康墨西哥工厂遭勒索软件攻击，业务运营受干扰

据 BleepingComputer 6 月 2 日消息，富士康公司确认其位于墨西哥的一家生产工厂在 5 月下旬受到勒索软件攻击的影响。富士康没有提供任何有关攻击者的信息，但勒索软件组织 LockBit 声称对此负责。被攻击的富士康工厂位于墨西哥蒂华纳，是美国加州消费电子产品的重要供应中心，被认为是一个战略设施。富士康在官方声明中表示，勒索软件攻击对其整体运营的影响较小，工厂正在逐步恢复。这不是富士康第一次被勒索攻击，此前 2020 年 12 月，公司另一处墨西哥工厂也遭遇过类似事件。

南非总统的个人信贷数据泄露：该国已沦为“黑客乐园”

据 MyBroadband 5 月 29 日消息，黑客团伙 SpiderLog$ 公开了南非总统 Cyril Ramaphosa 自 2000 年在国内四大银行之一的贷款详细记录，这批数据来自另一黑客团队，为其入侵征信机构 TransUnion 所窃取。SpiderLog$ 称，南非已经成为“黑客乐园”，任何人都能轻松绘制出南非数字基础设施分布，甚至包括国防 / 国安等敏感系统。此次曝光使得大众意识到了南非信息系统的显著漏洞，特别政府 / 国防 / 国安等部门的系统安全性。

印度第二大航司遭勒索软件攻击，大量乘客滞留在机场

据 BBC 5 月 25 日消息，印度第二大航司香料航空（SpiceJet）遭勒索软件攻击，内部系统受影响离线，导致多个航班延误数小时，大量乘客滞留在机场。此次针对香料航空运营体系的网络攻击，直接影响到飞往印度及海外各国的众多乘客，数小时的延误将转化为巨大的经济损失。这是近期又一起网络攻击影响航班运转事件，此前 4 月，加拿大老牌航空公司阳翼航空遭网络攻击，致使航班严重延误近一周时间，大量乘客在机场滞留多日。

俄最大银行遭到最严重 DDoS 攻击，普京称正经历“信息空间战争”

据 BleepingComputer 5 月 20 日消息，俄罗斯最大银行联邦储蓄银行（Sberbank）官网披露，在 5 月 6 日成功击退了有史以来规模最大的 DDoS 攻击，峰值流量高达 450 GB/ 秒。该行安全负责人表示，俄罗斯网络安全发生了结构性转变，过去 3 个月来企业遭受的网络攻击呈现爆炸性增长，攻击实力大幅提升。普京称俄罗斯正在遭受“信息空间战争”，他提出了三项关键任务，以确保俄关键信息基础设施安全。

漏洞篇

5月末，多家安全公司披露，微软支持诊断工具远程（MSDT）的代码执行漏洞（代号 Follina，CVE-2022-30190）遭到多个攻击团伙在野滥用，微软在6月补丁日正式发布修复补丁。



Windows SMB 拒绝服务漏洞安全风险通告

6月16日，奇安信 CERT 监测到 Windows SMB 拒绝服务漏洞细节及 PoC 在互联网公开，Windows SMB 在处理请求的过程中存在空指针引用缺陷，未经身份验证的远程攻击者可通过向 Windows 域控制器发送特制请求来利用此漏洞，从而导致目标系统拒绝服务。经验证，此漏洞公开的 PoC 稳定有效，未经身份验证的攻击者可利用此漏洞攻击默认配置的域控制器，攻击普通 Win10、Win11 主机用户需要经过身份认证。值得注意的是，微软已于 2022 年 4 月份修复了此漏洞，并于6月补丁日公开。

Linux Kernel eBPF 权限提升漏洞风险通告

6月13日，奇安信 CERT 监测到 Linux Kernel eBPF 权限提升漏洞 (CVE-2022-23222) 的 PoC 在互联网上公开。由于内核在执行用户提供的 eBPF 程序前缺乏适当的验证，攻击者可利用这个漏洞提升权限并在内核上下文中执行代码。要利用此漏洞，攻击者首先需要获得在目标系统上执行低权限代码的能力。大多数 Linux 发行版本默认禁用非特权运行 BPF 程序。经验证，此漏洞 PoC 有效。鉴于此漏洞影响范围较大，危害较大，建议客户尽快做好自查及防护。

Confluence 远程代码执行漏洞安全公告

6月3日，国家信息安全漏洞共享平台（CNVD）收录了 Confluence 远程代码执行漏洞（CVE-2022-26134）。未经身份验证的攻击者利用该漏洞可在目标服务器执行任意代码。目前，漏洞细节信息尚未公开，厂商已发布漏洞缓解建议，暂未发布修复补丁。Confluence 是一款专业的企业知识管理与协同软件，常用于企业 wiki 的构建。

微软支持诊断工具 MSDT 远程代码执行漏洞安全公告

5月31日，国家信息安全漏洞共享平台（CNVD）收录了微软支持诊断工具远程（MSDT）代码执行漏洞（CVE-2022-30190）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。目前，漏洞利用代码已公开，且已出现在野利用的情况。微软公司已发布漏洞缓解指南，CNVD 建议受影响用户按照临时防范措施缓解漏洞攻击威胁。



CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

CTFWAR攻防战争平台是CTFWAR网络安全攻防对抗联赛的官方平台，是由中国网络安全攻防大咖联合发起的创新型学习平台，以游戏的形式融入多种网络攻防场景进行答题、竞赛、互动。CTFWAR攻防靶场分为初级新手区、中级进阶区、高级挑战区，同学们可根据自身技术能力及技术方向进行筛选，整个学习过程将有全面的数据化呈现。

攻防答题模式

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

积分等级体系

CTFWAR攻防战争平台采取主流的CTF夺旗赛和AWD攻防赛的答题模式，提供云端的攻击终端，同学们在云端攻击平台上进行攻防实战操作，通过 Flag 判定和操作用时进行综合评分，以获得积分升级和金币奖励。

极牛众星计划

下一代网络安全新形态教材





对抗篇

国内攻防演习 5 月态势：哪些薄弱点最易被利用?

一、本月演习整体情况

2022 年 5 月，奇安信 Z-TEAM 团队共承接攻防演习服务 36 场，其中行业级攻防演习 2 场，省级攻防演习 1 场，地市级攻防演习 10 场，客户自主攻防演习 23 场。

本月攻防演习成果如下：

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	44	58	67	92	21	112	237	2491

二、本月任务目标特点

本月攻防演习和评估任务行业比较分散，覆盖目标面比较广，涵盖了政务、金融、电力、互联网、企业等目标，客户存在的安全问题主要涉及互联网侧业务系统组件存在历史漏洞、内部人员对钓鱼攻击防范意识不足、内网功能区缺乏安全隔离、内网口令复用及弱口令普遍等。具体情况如下：

1、历史漏洞仍是实现外部渗透的主要突破口

本月任务中针对多行业不同目标网络，漏洞利用仍是实现外部渗透的主要突破口。被攻陷目标互联网侧应用漏洞以平台组件历史漏洞为主，如外部应用中未授权访问、Shiro 反序列化、Weblogic 反序列化、SQL 注入、任意文件上传漏洞等，多因外部应用及系统组件缺乏日常安全巡检机制、对爆出漏洞的组件未及时升级更新造成的，这些问题的存在致使目标网络防线有随时被攻破的风险。

2、钓鱼攻击具有较高成功率

本月任务中目标的核心业务网络安全防护相对严密，针对外部系统难以直接突破的情况，钓鱼攻击成为了另一种外部突破的主要实现手段，并且具有较高的成功率。钓鱼攻击主要选择目标内部网络安全意识相对薄弱的人员。通过冒充同事或客户身份，以内部业务交流或客服咨询为由发送木马打开突破口。

3、访问策略缺陷是重大安全隐患

本月任务中发现多个行业目标的外部业务系统存在未授权访问的问题，可以通过未授权访问，直接访问这些外部业务系统后台，进而可以利用访问权限执行后台命令及获取后台配置文件、数据库等敏感信息。未授权访问多因对外部接入的安全配置或权限认证相关策略设置存在缺陷，导致对外部用户的访问地址、访问权限缺乏限制，为网络安全埋下了重大安全隐患。

4、 弱口令是内网严重安全隐患

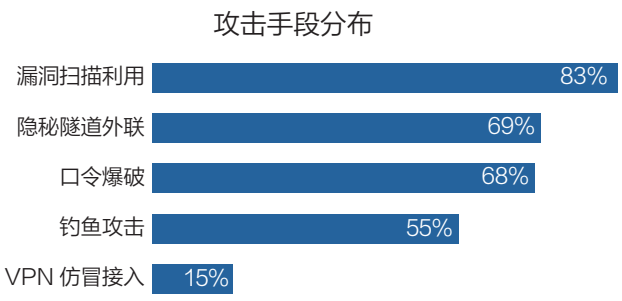
本月任务中口令爆破主要通过弱口令和口令复用实现，互联网侧口令爆破很少成功，在目标内网则成功率很高，是内网横向拓展的主要手段。通过搜集目标网络中各种设备的默认口令、弱口令来分析其密码组合规律，从而实现对目标内网相关网络应用、安全设备和服务器的快速爆破。

5、目标网络缺乏纵深防护机制

本月任务中目标网络普遍缺乏纵深防护机制，存在互联网侧服务器和核心内网未进行边界隔离的情况，内网的安全设备部署缺少功能域划分、vlan 隔离等措施。主要表现为突破互联网侧应用服务器后，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，多采用互联网侧系统漏洞利用和钓鱼攻击等方式进行，内网横向拓展则以隐蔽隧道外连、内网漏洞利用、弱口令和口令复用等手段为主。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集中在互联网侧业务系统和门户网站，以未授权访问、组件反序列化、任意文件上传

执行等漏洞为主。这些漏洞主要是由于系统组件更新不及时、安全策略设置缺陷引起的，直接反映出客户网络运维人员对下辖网络资产动态跟踪不及时、网络运维缺乏常态巡检机制、对存在的漏洞及安全威胁缺乏应对等问题。

2、隐蔽隧道外联

本月任务中大部分目标内网无法通过外网直接访问，需要借助端口转发、隧道技术等手段实现对内网的渗透拓展。以金融目标为代表的网络功能区划分严格、核心业务隔离措施完善的关键领域业务网络，则需要两到三层的通道转发实现对目标核心业务内网的渗透拓展。

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、钓鱼攻击

本月任务中针对不同目标，根据其业务特点，在钓鱼目标选择、钓鱼木马素材及话术组织方面均做了针对性的准备工作。比如，针对客服人员和人事部门目标，采取业务咨询、第三方合作或网络应聘等方式；针对管理人员和职能部门目标，则采取业务申请或报告提交等方式进行钓鱼突破。

三、典型攻击手段实现案例

1、外部漏洞利用

（1）某电力目标招聘官网存在任意文件上传漏洞，通过任意文件上传漏洞获取该机器上的登录凭证，登录后控制 96 台主机、2 台数据库、5 个 Web 后台。

（2）某目标域控存在 CVE-2021-42287、CVE-2021-42278 漏洞，通过该漏洞获得主域控权限，并抓取域管密码获取到域控权限，可接管控域终端 1912 台。

（3）某目标管理平台系统存在 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。

（4）某目标综合服务平台系统存在 CVE-2022-22947 漏洞，通过该漏洞获取到服务器权限。

2、口令爆破

（1）某目标动态仓储系统存在弱口令，可通过口令爆破直接登录该系统后台，获取后台管理权限。

（2）某目标数据库存在弱口令漏洞，通过漏洞利用获取到数据库权限，可查看某部门人员姓名、身份证、电话、地址等敏感信息。

（3）某目标内网域控服务器存在弱口令漏洞，通过弱口令获得域控权限后，可同时控制内网域控、域内主机和域内用户等。

（4）某目标 Web 控制台存在默认口令漏洞，通过该漏洞登录 Web 控制台后，可对监控主机下发脚本执行命令等。

3、钓鱼攻击

（1）通过浏览某目标政务外网 VPN 页面发现页面上可查询到 VPN 问题反馈人员的电话号码，通过微信搜索加为好友后，发送带有钓鱼木马的“VPN 申请单”，用户成功点击上线。

（2）通过搜索 QQ 群，申请加入某目标的 QQ 群后进行定点人员钓鱼，使用 QQ 临时会话发送木马文件，利用文件名诱导相关人员打开，进行钓鱼攻击，成功获取主机终端控制权限。

（3）以邮箱异常处理问题为由，对某目标的技术支持人员发送木马文件进行钓鱼攻击，成功上线并获取某系统服务器权限。

（4）通过对某目标内网投资系统运维人员进行水坑钓鱼，成功上线 4 台个人终端，并获取到内网 5 台数据库权限、2 台服务器权限、2 台 Web 后台权限。

政策篇

国内，国家能源局修订《电力行业网络安全管理办法》，首次要求设立首席网络安全官，网络安全预算不低于信息化总投入的5%；

国际上，美国商务部发布规定，要求向中国政府相关的最终用户进行漏洞披露等活动，需申请许可。



国内

国家能源局修订两项电力行业网络安全政策公开征求意见

6月15日，国家能源局公布了《电力行业网络安全管理办法（修订征求意见稿）》《电力行业网络安全等级保护管理办法（修订征求意见稿）》，公开征求意见。《电力行业网络安全管理办法（修订征求意见稿）》要求，电力行业关键信息基础设施运营者的主要负责人对关键信息基础设施安全保护负总责，要明确一名领导班子成员（非公有制经济组织运营者明确一名核心经营管理团队成员）作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作。

网信办修订《移动互联网应用程序信息服务管理规定》发布施行

6月14日，国家互联网信息办公室发布新修订的《移动互联网应用程序信息服务管理规定》。新《规定》要求，应用程序提供者和应用程序分发平台应当履行信息内容管理主体责任，建立健全信息内容安全管理、信息内容生态治理、数据安全和个人信息保护、未成年人保护等管理制度，确保网络安全，维护良好网络生态。新《规定》自2022年8月1日起施行。

市场监管总局、网信办发布《数据安全管理认证实施规则》

6月9日，市场监管总局、网信办宣布开展数据安全管理认证工作，并发布《数据安全管理认证实施规则》。《实施规则》以《信息安全技术 网络数据处理安全要求》及相关标准规范为认证依据，规定了对网络运营者开展网络数据收集、存储、使用、加工、传输、提供、公开等处理活动进行认证的基本原则和要求。《实施规则》明确，认证模式为“技术验证+现场审核+获证后监督”。认证证书有效期为3年。

《“中国+中亚五国”数据安全合作倡议》发布

6月8日，“中国+中亚五国”外长第三次会晤举行，会晤通过了《“中国+中亚五国”数据安全合作倡议》。倡议提出，在遵守国内法和国际法基础上，各方建议各国及各主体：就防范全球信息安全所面临的挑战和威胁，保障数据安全，开展协调行动与合作；应以事实为依据，全面客观看待数据安全问题，积极维护全球信息技术产品和服务的供应链开放、安全、稳定；各国应尊重他国

主权、司法管辖权和对数据的安全管理权，未经他国法律允许，不得直接向企业或个人调取位于他国的数据。

《零信任参考体系架构》等 4 项国家标准公开征求意见

综合消息，近一个月来，信安标委发布了 4 项国家标准的征集意见稿文件。包括《信息安全技术 互联网平台及产品服务隐私协议要求》《信息安全技术 零信任参考体系架构》《信息安全技术 移动智能终端的移动互联网应用程序（APP）个人信息处理活动管理指南》《信息安全技术 应用商店的 APP 个人信息处理规范性审核与管理指南》。



美国参议员提出《健康和位置数据保护法》，治理数据交易乱象

6月15日，美国参议员Elizabeth Warren提出了《健康和位置数据保护法》法案要求，禁止数据经纪人出售或传输位置数据和健康数据，并要求联邦贸易委员会颁布规则，在 180 天内实施该法律。同时，对符合 HIPAA 的活动、受保护的第一修正案言论和有效授权的披露作出例外规定。通过授权联邦贸易委员会、州检察长和受害者提起诉讼以执行法律规定，确保该法案的规定得到强有力的执行。

美国商务部发布《信息安全控制：网络安全条目》，强化漏洞信息管控

5 月 26 日，美国商务部工业和安全局发布《信息安全控制：网络安全条目》细则最终版，并生效执行。该文件要求，美国实体进行漏洞披露等跨境网络安全活动时，如最终用户与 D 组国家（包括中国）的政府有关，须申请许可才能发送潜在网络漏洞等信息。非政府用户不受影响。微软公司认为，这一审查制度将阻碍与安全研究人员和漏洞奖励计划参与者的跨境合作。

意大利发布《2022 至 2026 年意大利国家网络安全战略》

5 月 25 日，意大利政府发布《2022 至 2026 年意大利国家网络安全战略》及《2022 至 2026 年意大利国家网络安全战略实施计划》，公开了意大利未来几年的网络态势路线图。《战略》提出三大基本目标：通过旨在管理和减轻风险的系统性方法保护国家战略资产，通过部署增强的国家监控、检测、分析和响应能力及启动涉及国家网络安全生态系统中所有利益相关者的流程加强响应，有意识和安全地发展能够响应市场需求的数字技术、研究和产业竞争力。

俄罗斯通过《保护关键信息基础设施国家政策基本原则》草案

5 月 20 日，俄罗斯联邦安全委员会会议通过了《保护关键信息基础设施国家政策基本原则》草案。该草案定义了在信息技术部门实施国家政策的目的和机制，特别是计划通过使用国产信息技术提高关键信息基础设施的安全水平。草案决定运用国家力量组织研发人工智能、量子计算技术，创建富有竞争力的电子元件基地和高科技生产区，并开发用于检测、预防和消除网络攻击后果的国家信息系统。此外，草案还将特别关注信息安全领域的专家及技能培训。

P12

RSA2022峰会主题：安全的转型与未来

数字化转型加速，网络安全成生存必需。网络安全行业面临持续创新需求，RSAC 有哪些明确的方向?

RSAC 2022：安全的转型与未来

Talon Cyber Security 夺得 RSAC 创新沙盒冠军，让不少业内人士出乎意料，这其实代表着现实的真实需求与未来方向。RSA 公司 CEO Rohit Ghai“唯一的永恒”主题演讲，诠释了在不断变化的外部环境下，安全行业主动转型与变革的必要性。

普及的新兴技术、不断扩大的攻击面、频发的漏洞，对安全行业来说，唯一不变的是变化。行业推进转型转变的经验将决定下一个常态。

安全的转型与未来

RSA 公司 CEO Rohit Ghai 在演讲“The Only Constant”中为主题“转型”（Transform）做出了解读。Transform 是去年年中确定的 2022 年 RSAC 主题，在当前引起了广泛共鸣。

在开幕主题演讲中，Rohit Ghai 鼓励网络安全领导人主动进行转型——以达到比以往更强大、更好的状态。“安全转型需要重新定位我们的思维。”

Rohit Ghai 提出了三大推动转型的建议：重新思考身份；真相很重要；便利性不应牺牲安全。他认为未来应弄清楚如何以身份为中心进行访问，而不依赖传统访问机制（即密码），这是未来的方向。此外，他认为，保护信息的真实性将成为未来数年网络安全的关键任务。假新闻和错误信息已成为摧毁机构的有力武器。最后，他呼吁该行业放弃其旧的“教条”，不应为了便利而放弃安全性。



RSA 公司 CEO Rohit Ghai 在主题演讲中呼吁行业转型

RSAC 的“转型”主题，反映出机构在面临疫情流行加速的数字化转型所面临的巨大安全挑战。疫情之下，使用云服务的数字化转型成为企业生存的关键。网络安全比以往任何时候都更加重要，网络安全领导者需要进行转型，以保护通过云交付的应用。

实现转型、解决安全挑战的答案就在于创新，创新让蛋糕变大并带来新的好处。

网络安全行业正出现新的变化。业界不断寻找新的技术方法来改善网络安全状况或减少攻击次数。安全投资从强调“预防”转向“检测和响应”，现在这一重点正在再次转移。

首席安全官发现，要减少事件数量和团队负担，需要更好地了解和管理攻击面。现在业界对预防或“威胁与攻击面管理”重新产生了兴趣（Gartner《2022 年安全运营入门》）。在 RSAC 2022 上，攻击面管理是许多参观者最关心的问题。行业客户与安全同行强调考虑由外而内的外部攻击面管理 (EASM) 和网络资产攻击面管理 (CAASM)，来获得目前缺乏的安全可见性。

IBM 收购外部攻击面管理 (EASM) 领域领导厂商 Randori 可以反映出这种趋势。对攻击面和网络资产管理兴趣的增长表明，安全领导者已认识到，要降低网络风险，需要更好地了解网络环境及安全态势。但这并不意味着对安全响应投资不再重要，它与攻击面管理相辅相成。

思科执行副总裁兼安全与协作总经理 Jeetu Patel 表示，“我们需要确保对漏洞管理采取基于风险的方法。对入侵事件的处理，不是依据发生的时间，而是依据构成的风险量。”

业内人士认为，安全产品的创新，应该提高整个软件生命周期的效率，帮助安全团队成为转型的推动者，而不是阻碍者。例如，减少部署到云端的代码漏洞数量，并在应用运行时快速响应出现的问题。

攻击者的速度并未放慢

与会业界人士认为，在某种程度上，我们处于网络军备竞赛中。对供应链、云基础设施和物联网网络的攻击持续增长。SolarWinds 攻击与 Log4j 漏洞等重大安全事件表明：攻击的频率和规模不断增加。

根据 Sophos 在 RSAC 发布的《2022 活跃攻击者报告》，入侵者停留时间比 2021 年增加了 36%，中位数从 11 天增加到 15 天。近一半 (47%) 的攻击是漏洞被利用的结果。例如，ProxyLogon 和 ProxyShell 等容易被利用的漏洞占据显著位置。此外，今年主要趋势是利用面向外部服务的漏洞进行初始访问。这不仅包括 ProxyLogon 和 ProxyShell 漏洞，还包括影响 VPN 和防火墙部署的漏洞。另一个趋势是攻击者依赖通过远程服务进行初始访问。由于缺乏多因素身份验证 (MFA)，攻击者能在不被发现的情况下侵入系统。

索软件攻击几乎无处不在。大量受害者成为勒索软件犯罪分子的牺牲品。这种永远存在的威胁正在发生战术上的一些转变，但没有减弱的迹象。《2022 年度勒索软件状况报告》发现，勒索软件攻击的影响巨大。支付超 100 万美元赎金的受攻击组织增长了 3 倍。

SANS 研究所发布的最危险攻击技术简报是 RSAC 上最受欢迎的活动之一。SANS 研究所专家称，被窃取身份验证令牌、云滥用和易受攻击的备份都是企业在未来需要解决的问题。

以下是 SANS 研究所今年描述的五种最危险的攻击技术：

- **攻击在云端。**随着组织越来越多地使用基于云的服务来存储数据、在互联网上提供应用及开展业务运营，攻击者不仅将云服务作为攻击目标，还利用云产品作为攻击平台。

SANS 研究所情报总监 Katie Nickels 建议组织注意正常的云行为，并寻找潜在的异常值来发现风险。

- **多重身份验证绕过。**多因素身份验证 (MFA) 是一种非常强大的安全力量，但它越来越多地被攻击者滥用。攻击者能够通过几种不同的方法绕过 MFA。Nickels 建议组织有多种 MFA 备份选项来限制风险。
- **备份漏洞。** SANS 研究所研究主任 Johannes Ullrich 认为备份是一种潜在的危险攻击媒介。备份系统

可以访问整个企业的端点和服务器，对攻击者来说是有吸引力的目标。攻击者正在寻找备份系统中的已知漏洞进行利用。Ullrich 建议组织要勤于修补，确保对备份系统的访问是安全的。

● **跟踪软件和蠕虫仍有风险。**SANS 研究所高级讲师 Heather Mahalik 警告说，跟踪软件和蠕虫仍然是用户关注的问题。随着飞马软件（Pegasus）的出现，用户跟踪软件 Stalkerware 再次成为一大安全问题。

在防范跟踪软件和蠕虫方面，Mahalik 建议坚持基本的网络安全要求，包括定期修补、备份和反恶意软件工具。她还建议用户有效地使用多因素身份验证。

● **风险来自太空 。**SANS 研究所首席课程主任 Rob Lee 警告说，新出现的风险来自于非地面互联网通信。在俄乌冲突中，最早攻击目标之一是地面互联网基础设施。马斯克提供星链互联网服务后，攻击者将越来越多地瞄准支持互联网和地面系统的卫星系统。

关基防护需要联合防御模式

在 RSAC 2022 的主题演讲中，美国联邦政府的网络安全领导人鼓励政府和非政府实体之间开展更多合作。

网络安全和基础设施安全局 (CISA) 主管伊斯特利（Jen Easterly）表示，“ 2022 年的网络安全格局看起来并没有太大不同，但确实看到国家黑客和网络犯罪分子变得更加老练。网络安全成为国家安全的当务之急。”她强调将私营和公共部门联合打击恶意网络行为的重要性，因为私营部门通常“拥有更多的可见能力”。SolarWinds 事件不是由美国政府发现的，而是由安全企业 Mandiant 发现的。”

美国国家网络总监克里斯 · 英格利斯表示，这种合作“不是锦上添花，而是锦缎本身。”美国国家安全局 (NSA) 网络安全局局长罗伯特 · 乔伊斯表示，俄乌冲突之后，恶意网络活动增加，进一步证明了在联邦机构和关键基础设施部门的网络安全工作上加倍努力的必要性。

私营部门的合作伙伴关系是建立网络防御的必要组成部分。美国公共部门与私营机构的伙伴关系的重大举措是 2021 年 8 月成立联合网络防御合作组织 (JCDC)。JCDC 是一项开始领导美国网络防御计划发展的倡议。成员包括联邦机构、企业、州和地方政府等。



CISA 主管伊斯特利认为私营安全机构具有更强可见能力。

长期以来，美国政府官员一直主张在网络安全方面建立更强大的公私合作伙伴关系。2022 年与私营部门的协调与合作有所增加。伊斯特利表示：“自从俄乌冲突以来，我们已经开始一起工作、规划和实施运营协作模式，通过技术工具 Slack 近乎实时地共享信息。我们以政府和私营部门以前从未做过的方式真正分享见解、信息和分析。”

SolarWinds 公司 CEO Sudhakar Ramakrishna 呼吁政府和行业在安全情报共享方面加强合作，并承诺派驻员工与美国网络安全和基础设施安全局 (CISA) 密切合作。

Ramakrishna 说，能够有效应对不断变化的威胁形势的唯一方法，是加强公共部门和私营部门之间的真正伙伴关系。 他呼吁“整个软件行业加入这一努力，美国每一家软件或技术公司都委派一名全职员工在 CISA 的指引和指导下工作，以支持威胁情报和信息分享。”

白宫国家网络主管 Chris Inglis 表示，这种合作关系下，不同机构的技能能够相互补充，从攻击者的角度来看，“必须击败所有人方能击败我们中的每个人。”

思科安全与协作执行副总裁 Jeetu Patel 则强调网

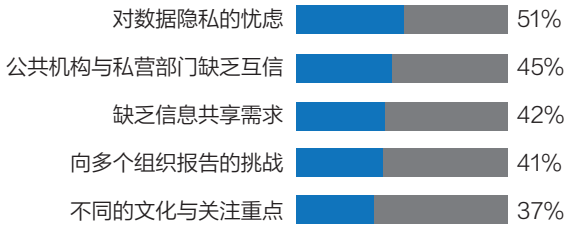
络安全贫困线的理念：由于软件依赖性、共享数据、混合工作等原因，不同机构更加相互联系和依赖，将所有企业提升到安全贫困线以上很重要。

“我们应该考虑保护整个供应链和生态系的安全，而不是单个组织。” 这延伸到为非营利组织和非政府组织提供免费或低成本安全服务，以及大公司帮助小型机构改善安全状况。

与会嘉宾强调，实现公共机构与私营企业的有效合作，建立彼此间的“信任”尤为重要。数据隐私问题和信任问题影响了这种合作伙伴关系的效力。根据 MeriTalk 和 RSAC 的研究，93% 的网络安全决策者认为政府与私营机构合作对国家安全防护至关重要，但只有 34% 的人认为非常有效。92% 的机构积极与合作伙伴共享信息，但 43% 的机构认为，私营部门与政府共享信息比反过来更常见。高达 69% 的网络安全决策者表示，其所在机构对网络安全信息共享保持沉默。

大多数与会者同意，以政府为主导的伙伴关系是前进的方向，但在最佳方法上却没有共识。但改善公共机构和私营部门间的沟通和信任，无疑是降低网络安全风险的关键。

公共机构与私营部门的合作障碍



创新是持续的需求

RSAC 第一天，Talon Cyber Security 夺得了创新沙盒的冠军，让不少业内人士都觉得出乎意料。TalonWork 专为企业打造安全的企业级浏览器：为浏览器提供身份验证、数据丢失预防、零信任控制等原生功能，使组织能够简化其安全防护。

Talon 仿照谷歌提出的浏览器即 OS 的概念，打造出的安全浏览器，其创新点在于加入了上网行为管理等功能，同时为一些线上编辑的文档进行加密处置等。

Talon 并不是唯一一家扩展对安全未来理解的初创公司。本届 RSAC 上另一关键主题是安全工具整合。ESG 高级首席分析师 Jon Oltsik 的新研究表明，组织正在朝着产品集成和多产品安全的方向发展。工具过载和人才短缺将使安全企业在端到端解决方案和安全自动化中脱颖而出。

目前每个安全需求都有单点解决方案，给安全从业者带来一系列新挑战。在过去几年中，CISO 对网络安全工具进行大量投资，给安全运营团队造成信息过载。投资太多不同的工具也给安全团队造成潜在的信息孤岛风险。

安全团队不可避免地必须集成各种工具，来实现全面的安全策略。当务之急是整合、连接和自动化孤立的安全解决方案，以帮助安全团队将时间和精力集中在最高优先级的威胁上。

在本届 RSAC 上，扩展检测响应 (XDR) 得到许多安全人员的关注。扩展检测响应 (XDR) 集成 SIEM、EDR 和 SOAR 解决方案，可连接和分析不同来源的数据，可以将安全工具统一到有效的威胁检测、调查和响应 (TDIR) 工作流程中。扩展检测和响应 (XDR) 为企业整合供应商提供了可行的路线图。

网络安全正迎来有史以来的最高光时刻。网络攻击处于历史最高水平，攻击者针对所有关键部门进行攻击。网络安全不再仅仅是组织的竞争优势，而是生存的必需品。

过去数年中，安全解决支出的增长已超过其他 IT 细分领域。根据 Pitchbook 的数据，2021 年网络安全投资达创纪录的 264 亿美元，比 2020 年增长 2.4 倍。2022 年，全球网络安全预算预计将同比增长 10~13%，而 IT 总预算同比增长 4~5%。

面对激增的安全支出，我们需要思考全球知名安全专家 Mikko Hypponen 在接受采访时的发言：复杂性是安全的最大敌人。代码越多，错误就越多，漏洞就越多。我们应该降低复杂性，但现在这并没有发生，而且恰恰相反。

极牛技术社群

网络安全技术社群

Cyber Security Technology Community

PLATFORM

网络安全技术社群

极牛网旗下面向网络安全工程师的社群平台，汇聚行业中网安工程师的知识和社交平台，围绕『技术』『管理』和『圈子』三个核心能力，将前沿的技术内容、技术管理成长感悟、技术圈子社群平台等向优质的网安工程师开放，每月定期组织社群会员线下活动，强调内容分享的体系化和活动内容的多样性，为中国网络安全工程师打造专属的全方位综合赋能的社群平台。

技术

聚焦前沿技术、热点技术、难点技术，提升网安在企业架构中的决策能力和迭代能力。

管理

专注在帮助网安工程师在职业发展中，建立体系化的管理知识和技术管理转型路径。

圈子

建立精准的技术方向圈子，针对不同的职业发展阶段，组成技术成长小组一起结伴同行。

极牛技术站

以沙龙、峰会、圆桌论坛等深度学习的形式进行，满足知识获取与社交需求。

管理加油站

面向管理者的闭门活动，前瞻性的思维和观点，成熟的管理模式与领导模型。

极牛知识变现

通过帮助工程师打造个人品牌，从出书、录课、企培等形式帮助知识变现。

极牛训练营

面向社群成员的线下课程，技术架构、团队管理、商业模式、塑造个人品牌等。

极牛众星计划

社群中优秀的工程师将会被受邀签约极牛众星计划，平台辅助进行品牌孵化。

更多内容敬请期待

极牛·产业生态

网络安全产业生态平台

极牛网络安全产业生态平台，通过产服、产孵、产投、产研四大引擎，打通技术、产品、平台能力以及B端G端场景和服务体系，构建产业核心生态圈，与合作伙伴共生共赢，助力网安产业智慧升级。



四大引擎

产服

以产业基地为载体
提供产业生态服务
助力产业发展

产孵

以产业加速器为载体
孵化优质企业
与ToB业务的合作

产投

以产业生态投资
为重要抓手
构建产业生态体系

产研

构建产学研体系
聚焦底层技术创新
全面赋能网安产业

产业生态架构

与生态伙伴一起持续加大资本 、资源 、 技术 、 能力和商机投入，助力科技创新驱动网络安全产业升级，为社会创造更大价值



RSAC 十大热点议题解读

RSAC 2022 年以“转型”（Transform）为主题，被认为是去年主题（Resilience，弹性）的延伸和拓展。从弹性到转型，RSAC 的主题变化透露出网络安全产业的持续变革。

RSAC 2022 的 170 余个主题演讲，主要围绕 10 大热门主题，其中包括：数据与隐私安全（热度 14 ）、身份安全与零信任（热度 14 ）、软件供应链安全（热度 10 ）、勒索软件（热度 10 ）、AI 安全（热度 10 ）、威胁分析及狩猎（热度 10 ）、风险管理（热度 9 ）、云安全（热度 6 ）、物联网及工业安全（热度 6 ）、基础设施安全（热度 4 ）。

从本届 RSAC 的热点议题，可以看出网络安全的多个细分领域都在发生变革。

1 数据与隐私安全

数据与隐私安全是近 5 年来的热点议题。随着数字经济的发展和数据流通需求的增长，其热度持续升高。数据与隐私安全融合了传统安全技术应用和创新技术应用，产生了新的需求和应用场景。数据治理、隐私计算、隐私合规成为数据安全的创新驱动力。

本届 RSAC 的数据安全议题集中在数据保护，如云上行业（如医疗）数据保护、企业数据保护、数据本地化保护政策，以及政府数据交易与授权访问等。在隐私安全方面，热点议题则集中在如何保障基础设施（如 5G ）、设备（如汽车），以及应用（如 AI、区块链）的隐私安全方面。



具有代表性的数据安全议题包括：

在“云安全：如何保护云上医疗数据”的议题中，专家以 AWS、Azure 和 DevOps 平台为例，将云上医疗数据包括概括为三点：（1）安全设计，包括身份验证、DevOps、标准、流程。（2）安全执行，包括通道、扫描、策略、受限访问角色。（3）安全运营，包括环境扫描、可用性管理和补丁管理等。最后，专家提出了三条建议：（1）使用云原生配置控制工具控制安全性和成本。(2)通过代码使基础设施和通道民主化。（3）实施透明的 DevOps 文化。

在“让企业员工保护高价值的数据”的议题中，专家从企业内部风险的视角，提出改变了内部风险的 3 个关键驱动因素：（1）数字化转型正在改变我们的合作方式；（2）知识型工作者随时随地展开工作；（3）人们正在频繁换工作，比以往任何时候都快。因此，从控制企业内部风险的角度保护高价值数据，需要做到 3 个 T：透明度（Transparency）、培训（Training）、技术（Technology）。

在“你能抓到我么：保护 5G 中的移动用户隐私”议题中，来自可信连接联盟（TCA）的专家关注的重点围绕国际移动用户身份 (IMSI) 的安全漏洞，以及保障用户身份隐私的方法，提出基于 SIM 卡的加密是唯一可行的方法，包括消费者和工业物联网用例。

在“隐私和区块链悖论”议题中，专家比较了区块链的优点与劣势，提出了区块链用于隐私保护及 GDPR 合规的四个注意事项：（1）一项技术和一项法规——数字世界中的隐私并非仅靠技术就能解决的问题。在技术方面，区块链正在通过在食品信托、集装箱、贸易融资和国际支付等不同领域提供价值的网络取得巨大进步。 尊重数据和交易的隐私是这些项目的核心。（2）起点相反，但基本原则相同——区块链和 GDPR 共享数据隐私的共同原则。 两者都希望监督我们自己的数字私人数据交易和支付（在比特币的情况下），或在 GDPR 的情况下需要与他人共享的个人数据。（3）公共网络中的隐私——隐私并不一定意味着用户需要一种私有区块链网络方法，可以在 GDPR 框架下实现满足公共网络隐私需求的区块链网络。（4）删除权——GDPR 要求之一是个人要求组织及时删除的权利，拥有他们的个人数据以完全删除该数据。

2 身份安全与零信任

身份安全是传统的赛道，零信任理念和云业务应用的发展为身份安全注入新的活力。

随着零信任框架和谷歌零信任应用的出现，零信任成为身份安全领域的新理念与创新热点。随着云应用的发展，云访问安全成为热点。疫情下远程办公的需要使得身份安全再度成为热点。“弹性” 是 2021 年 RSAC 大会的主题，零信任则被认为是建设“弹性”网络的安全基础设施。

本届 RSAC 的身份安全议题集中在多云环境的身份认证、生物识别技术应用，以及身份认证机制面临的风险等。在零信任方向，热点议题包括传统零信任的缺点、新的零信任机制，以及零信任在工业系统中的应用。

具有代表性的身份安全议题包括：

在“为什么零信任网络访问被破坏，以及如何修复它”议题中，来自 Palo Alto 的专家指出基于零信任的 ZTNA1.0 方案存在诸多缺陷，包括违反最小特权原则、没有对用户行为进行持续的跟踪和授权、没有流量检测、没有数据保护、无法保障应用程序安全等。专家提出了 ZTNA2.0 的方案，以解决上述问题。通过在第 7 层基于 App-ID 识别应用程序充分实现最小权限原则；一旦授予对应用程序的访问权限，就会根据设备姿势、用户行为和应用程序行为的变化不断评估信任度；提供对所有流量的深入和持续检查，甚至是允许的连接以防止所有威胁，包括 0day 威胁；跨企业使用的所有应用程序提供一致的数据保护，包括私有应用程序和 SaaS，具有单一 DLP 策略；始终如一地保护整个企业使用的所有应用程序，包括现代云原生应用、传统私有应用和 SaaS 应用。

在“零信任架构的构建”议题中，来自 NIST 的专家分享了国家卓越网络安全中心 NCCoE 实施 ZTA 零

信任架构项目。部署方式包括增强的身份治理 (EIG)、微分段、软件定义边界 (SDP)。整个架构包括 ZT 内核组件、终端安全、数据安全、安全分析及 ICAM。应用场景包括员工访问公司资源、员工访问互联网资源、承包商访问公司和互联网资源、企业内的服务器间通信、与业务合作伙伴的跨企业协作、利用企业资源提高信任评分 / 信心水平等。

在“为工业控制系统带来零信任”议题中，专家分析了工业控制系统面临的风险点，提出了在工业控制系统中部署零信任的方法：（1）OT 和 IT 边界：在企业网络、工厂系统和现场之间建立边界，分割网络。（2）OT 资产：屏蔽和监控无法运行安全软件或打补丁的工业端点。（3）OT 网络：使用适应现场网络中使用的工业协议和技术的网络安全。（4）离线操作：保护为维护而引入的可移动媒体和外部设备。（4）SOC/CSIRT：监控整个环境以简化威胁检测和事件响应。

在“面对 / 关闭：使用生物识别技术进行身份验证的战斗”议题中，来自思科的专家提出了 DeepFake 等技术对人脸识别和身份认证带来的技术风险，以及相应的法律风险，并提出改善的建议：（1）了解有关人脸识别和人工智能的更多信息，盘点 FR 认证和其他应用程序。（2）对 FR 申请进行法律风险评估，将 FR 整合到安全风险评估 / 管理流程中。（3）建设完整的治理体系，实施治理控制。



3 软件供应链安全

受贸易战和供应链攻击事件影响，软件供应链安全成为热点。美国商务部和国土安全部的软件供应链安全规范、代码安全和软件开发安全被高度重视。代码安全与开发过程已深度结合，强调软件供应链的安全监管与协同。开发安全和代码安全是软件供应链安全的主要抓手，并呈现融合发展的趋势。

本届 RSAC 的软件供应链安全议题集中在供应链的脆弱性，相关法律和政策等。在技术方面，热点议题则集中在软件开发安全，如 DevSecOps。

具有代表性的软件供应链安全议题包括：

在“安全的软件供应链是否可行”的议题中，专家提出当前世界软件供应链已经是高度发达的网状结构，威胁可能来自供应链的任何层面，包括恶意供应商、错误 / 易受攻击的软件、未经授权擅自修改开发或交付等。为应对软件供应链安全威胁，需要采取的措施包括供应链体系认证、供应商文件、软件测试、连续的提升、对开源软件的检测等。具体包括：对供应链软件的成熟度进行现实评估，制定安全计划以及可达到和可扩展的目标。确定对阻碍者的加速监控 / 响应，了解企业内部软件组织的安全态势。在开发和第三方代码方面获得供应链指导委员会的批准。获得对安全软件的内部承诺，在所有合同中增加供应链安全要求，对供应商的软件进行抽查等。

在“构建企业级 DevSecOps 基础架构：经验教训”的议题中，专家指出软件开发安全面临的挑战，包括：（1）对应用程序的安全状态缺乏统一的看法和理解。（2）如何实现代码分析管理及保障安全信息源的多样性。（3）开发者缺乏支持，开发团队之间缺乏信息共享。

为应对挑战，专家提出了企业级 DevSecOps 解决方案，包括：（1）由库存组件和开源构建的软件框架，将软件扫描工具打包成 docker 镜像的统一方式，Docker 化的扫描工具可以插入到许多不同的 CI 管道中。（2）存储库 / 项目与产品和团队之间的衔接。基于团队添加项目和数据，确保代码 / 工件 / 程序集 / docker 图像 / 云帐户可以链接到产品和团队。（3）为所有安全漏洞提供通用数据模型和统一 GUI。允许根据需要添加新的扫描工具或安全信息源，实现漏洞的标准化展示。（4）提供部门 / 产品级别汇总报告。包括存储库 / 工件级别的细粒度漏洞报告，在部门 / 产品级别汇总漏洞，展示跨部门 / 产品的安全成熟度等。

4 勒索软件

勒索软件成为 2021 年美国首要的网络安全威胁。根据 FBI 统计，2021 年勒索软件攻击了至少 649 个美国关键基础设施，其中包括美国最大燃油、燃气管道运营商科洛尼尔公司遭到黑客网络攻击勒索，导致供应中断和燃料短缺的事件。2021 年美国成立了勒索软件工作组（RTF），由来自行业、政府、执法部门、民间社会和国际组织的 60 多位专家组成，倡导统一、积极、全面、公私合营的反勒索软件运动。

本届 RSAC 的勒索软件议题集中在对勒索软件的分析、防护，以及应对勒索攻击的恢复能力等方面。

具有代表性的勒索软议题包括：

在“勒索软件现实清单：防止攻击的 5 种方法”议题中，专家提出了防止勒索软件攻击的 5 种方法，包括：（1）封堵漏洞。勒索软件团伙通常利用过去两年内的 CVE，目前了解到被利用最多的包括 MS Exchange、SolarWinds Serv-U、Log4J、Accellion、SonicWall、PrintNightmare 和 SMBv1。（2）知道何时丢失了密钥。核心关注点包括凭据盗窃和初始访问代理（IAB）。凭据盗窃常用的手段包括 AZORult、Predator the Thief、Kpot、MARS、Redline、Racoon、Mars Stealer。应对 IAB 的措施包括 IAB 出售对多个威胁参与者 inc. 的访问权限。 勒索软件团伙在实际勒索软件攻击之前，通常通过地下论坛出售对公司的访问权早期识别可以节省数百万美元；通过 ZoomInfo 或 RocketReach 类型工具识别受害者等。（3）了解网络犯罪分子，学

习他们的常用手段。例如，Conti 小组正在积极利用 Scripts Github repos、Cobalt Strike、CVE PoC 等，经常使用非恶意工具来获得他们的目标。这些资源是开放的，防御者也可以学习同样的资源。（4）深入了解勒索软件机制，发现恶意软件爆发之前的行为痕迹。攻击者严重依赖非恶意工具，而传统的网络安全控制关注过多的恶意文件，却忽略了行为才是关键。因此应重点关注攻击者使用工具的行为。（5）创建减速带和检查点。采取包括多因素身份验证、网络分段、限制浏览器 cookie 寿命、活动目录安全等措施，加强纵深防御使得攻击者横向移动更加困难。

5 AI 安全

本届 RSAC 的 AI 安全议题集中在 AI 训练和应用中的数据与隐私安全、AI 开源工具安全、AI 测试安全等 AI 自身安全，以及将 AI 技术用于威胁分析和 0day 网络攻击。

随着海量数据的积累、计算能力的发展、机器学习技术创新，图像识别、语音识别、自然语言翻译等人工智能技术得到普遍部署和广泛应用。AI 对于传统计算机安全领域的研究也产生了重大影响，除了利用 AI 来构建各种恶意检测、攻击识别系统，黑客也可能利用 AI 达到更精准的攻击。

同时，AI 自身的安全性变得前所未有的重要，如果应对利用数据投毒、深度伪造等技术干扰破坏 AI 的正常学习与应用，也成为网络安全领域面临的新课题。

具有代表性的 AI 安全议题包括：

在“AI 的隐私和合规性——开源工具和行业看法”议题中，来自 IBM 的专家分析了面向 AI 应用的隐私保护技术，如差分隐私、匿名化、分布式计算和加密技术等，以及各种技术的优缺点。IBM 专家认为，从行业视角看，AI 隐私保护应具备以下特点：（1）防御应该是非破坏性的。大多数组织已经拥有复杂的机器学习设计和运营流程，解决方案应该以最小的中断集成到这些流程中。（2）产品应设计成人工智能隐私工具包，“一键式”解决方案更易于学习，具有良好的默认参数有助于入门，以及可解释的可视化首选项。（3）可扩展性和性能。一些隐私保护方法非常适合学术工作，但不要扩展到企业工作负载，工具需要自动化和高效的算法，和基于风险评估的模型优先级。在此基础上，IBM 推出了用于 AI 隐私的开源工具，能够实现模型匿名化和数据最小化，并展示了相关的应用案例。

在“利用人工智能和深度学习对抗 0day 网络攻击”议题中，来自 Check Point 的专家认为面对当前网络威胁困境，基于 AI 的安全技术表现出高效阻断攻击、最佳威胁捕获率、接近零误报的特点，只有 AI 才能保证网络安全。Check Point 搭建了威胁云 ThreatCloud，通过 30 多个 AI 引擎实现不同的安全功能，主要包括：（1）检测未知恶意软件 – 受感染主机检测、沙盒静态分析、沙盒动态分析引擎；（2）检测网络钓鱼 – 邮件静态分析、移动零钓鱼检测、反钓鱼 AI 引擎；（3）提升准确性 – 网络 AI 引擎聚合器、移动 AI 引擎聚合器、机器验证签名引擎；（4）异常检测 – 云网络异常检测引擎；（5）战场狩猎 – 活动狩猎引擎；（6）揭露隐形漏洞 – 分析师头脑、恶意活动检测引擎；（7）分类 – 文档元分类器矢量化家族分类器、机器学习相似度模型、MRAT 分类器等。

6 威胁分析及狩猎

网络攻击技术和方法不断升级换代，攻击者从脚本小子、黑产犯罪团伙向国家级组织演进，攻击能力不断提高，攻击技术不断升级；威胁利用从已知到未知不断发展变化。

威胁狩猎是一种主动识别攻击痕迹的方法，由威胁猎人利用威胁分析工具、威胁情报和实践经验来积极筛选、分析网络和端点数据，寻找可疑的异常或正在进行的攻击痕迹。近年来威胁狩猎工具的自动化水平不断提高，逐渐成为应对高级持续威胁的重要手段。

本届 RSAC 的在威胁分析及狩猎议题集中在全球网络威胁态势、基于 AI 的自动化威胁分析技术，以及

威胁狩猎实践。

具有代表性的威胁分析及狩猎议题包括：

在“2022 年网络安全状况：从大离职到全球威胁”议题中，ISACA 专家分享了 2022 年网络安全状况报告。根据 ISACA 的研究，在网络威胁态势方面，2021 年企业最关注的五大网络安全影响包括：组织的声誉、数据泄露对客户造成的伤害、供应链攻击造成业务中断、商业秘密的丢失、组织的股票价格、财务状况。五大网络安全威胁分别为：网络犯罪、黑客、内部威胁、国家威胁、内部误操作。五大网络攻击方式分别为：社会工程学、APT 攻击、安全配置错误、勒索软件、未打补丁的系统等。在人力方面，当前全球网络安全从业人员数量严重不足。在 2021 年有 63% 的企业网络安全职位有空缺，五分之一的企业表示需要六个月以上才能找到合格的空缺职位的网络安全候选人。其中空缺最大的细分领域包括云安全（52%）、数据保护（47%）、身份安全（46%）、应急响应（43%）、DevSecOps（36%）。

在“CHRYSALIS：人工智能增强的威胁猎手和法医时代”议题中，专家介绍了将数据科学和人工智能引入威胁狩猎和数字取证进该领域的进步的技术：（1）ML&TH 联结学习用于异常分析的技术；（2）机器学习用于恶意软件分析并实现检测和分类的技术；（3）基于机器学习揭露恶意软件的技术，包括使用带有预训练模型的 ML 进行恶意软件检测、使用 SqueezeNet 和逻辑回归模型、使用卷积过滤器提取特征以将其分类为恶意软件；（4）基于机器学习实现内存取证的技术，包括用于识别受损数据集中的特定模式，使用 Volatility 3 输出应用 ML 算法来寻找可疑行为，并可以与 pslist、psscan、pstree、malfind、netscan 等一起使用；（5）基于机器学习实现深度日志分析的技术，包括从标记的数据中学习以分类为异常或正常条目，在大量系统日志中使用 LSTM 识别异常， IDS/防火墙日志以检测 DDoS 和端口扫描等；（6）基于机器学习实现流量分析的技术，包括远超传统系统能力的定制化深度监控、执行聚类以发现异常并区分异常值、在大型数据集中发现未知威胁等。

7 风险管理

网络威胁是利用电子信息和系统中的漏洞的恶意攻击，而安全风险管理旨在降低网络攻击的可能性和影响。通过识别、评估和减轻企业电子信息和系统的风险，实施安全控制以防止网络威胁。

面向关键基础设施和重要行业的高级持续威胁日益严重，企业必须建立风险评估机制，使用威胁情报界定风险，开展安全测试等一系列风险管理措施，从而实现体系化的网络安全防护。

本届 RSAC 的风险管理议题集中在网络风险分析及风险管理的合规模型等方面。

具有代表性的风险管理议题包括：

在“有针对性、统一和协调的服务，以更好地降低风险”议题中，专家认为由于新冠疫情带来的居家工作和“大离职”使得云服务提供商必须加速开展安全托管业务，而急于通过 MSSP 解决这些挑战是以牺牲其他领域的资源 / 风险为代价的，在许多情况下，企业过度补偿检测和响应领域的新工具和服务，而牺牲了他们的识别、预防和恢复策略，因此需要开展相应的评估和规划，评估的内容主要包括识别、防护、检测、响应、恢复。评估的过程包括：（1）需求评估，包括明显被忽视的领域、目前资源不足且风险太大的地区、存在明显技能差距的领域、您可能在现有工具或服务中有重叠的领域、内部资源可能不可行或不建议的领域；（2）使用安全框架来指导评估；（3）将调查结果与 MSSP 服务进行比较。

8 云安全

云应用的普及导致相关安全问题的热度持续增强。云安全赛道在一直演进，细分领域、技术方向不断演化，从以容器安全为代表的基础设施安全，到平台层面 API 安全，再到 SaaS 层面业务安全。基于云原生的



威胁管理，数字调查取证，云安全管理平台，资产管理等成为今年云安全的重点议题。

本届 RSAC 的云安全议题集中在云上的数据安全、身份安全等方面，以及多云环境的安全架构。

具有代表性的云安全议题包括：

在“安全左移：现代云安全的十大最具颠覆性的想法”议题中，专家提出安全左移的思想，认为在当前云安全响应太慢、太晚、缺少应用程序上下文、无法修复的现状下，应重新考虑以运行时为中心的云安全方法，主要包括：（1）以开发人员为中心，安全性必须集成到开发者平台中，包括代码库、业务流程等（GitHub、GitLabs、Jenkins、Jira……）。（2）拥抱 IaC 安全性，IaC 安全性将成为云安全的基石（VM、CSPM、CIEM 全部基于 IaC 扫描左移）。（3）补丁即代码：采用基于 IaC 和拉取请求的不可变运行时原则和补丁作为代码。（4）AppSec 的回归：不能忽视 SAST 和 SCA 的 AppSec 规则，它们是云安全策略中最重要的部分。（5）无代理方法：云安全供应商必须利用云 API 来实现无代理和持续的云安全，例如，将 VM 转换为基于 API 的云原生 VM。（6）运行时安全仍然很重要，并且 EPP 供应商必须采用云架构（如 eBPF）。（7）微分段 /ZTNA、的 IAM 策略

非常复杂，应寻求自动化解决方案。（8）持续部署安全网关，并考虑整个云应用程序生命周期的变化。（9）策略即代码，用一个单一的策略即代码统一， 考虑开放标准而不是以供应商为中心。（10）了解自身现状，大型企业将持续部署混合云，而中小企业则通常选择单一公有云。

9 物联网及工业安全

物联网及工业安全由于其庞大的终端规模及潜在的安全威胁而受到关注。近年来物联网技术正在加速向各行业渗透，智慧工业、智慧城市、智慧交通、智慧健康、智慧能源等将成为产业物联网连接数增长最快的领域。利用物联网终端的挖矿、设备劫持事件频发，智能医疗、交通、家居产品不断爆出安全漏洞，并且造成不可逆的生命财产损失，从而使得物联网及工业安全成为热点议题。

本届 RSAC 的物联网及工业安全议题集中在终端设备的漏洞检测、可信机制及安全模块方面。

具有代表性的物联网及工业安全议题包括：

在“防篡改元件如何保护物联网”议题中，来自可信连接联盟（TCA）的专家指出，到 2025 年，物联网连接数将达到 240 亿，而对物联网连接的安全防护能力则严重不足，这既包括对单个设备的近距离攻击，也包括云端的远程攻击。而防篡改元件可以实现基于 SIM、eSIM、eSE 的快速认证与数据安全传输能力。

10 基础设施安全

在前几届 RSAC 上，基础设施安全话题相对冷门，今年热度有所回升。一方面因为过去两年美国的重要基础设施大规模遭受勒索软件和供应链攻击的威胁，此外 5G 和工业互联网的建设进入到应用阶段，以能源互联网为代表的产业应用引起了更多的重视。

本届 RSAC 的基础设施安全议题集中在关键基础设施的网络攻防和安全运营方面。

具有代表性的基础设施安全议题包括：

在“分布式能源基础设施的入侵与防护”议题中，专家提出到 2024 年能源互联网市场将达 2000 亿美元。能源互联网安全是一个新的领域，需要不同的网络安全架构：保护系统 / 平台（例如 DERMS、ADMS），确保公用事业和第三方发电资源的连接，验证第三方发电源、聚合器和逆变器供应商的数据的完整性，检测第三方电源上的异常和潜在恶意活动并预测潜在的下游影响。因此需要建立供应链安全防护机制，检测并防御来自供应链上下游的攻击，以应对类似 SolarWinds 事件的攻击。

结语

从本届 RSAC 的热点议题可以看出，网络安全的许多细分领域都在发生变革。

数据与隐私安全在寻求具体应用场景的解决方案以实现产业落地；身份安全与零信任在寻求新的架构以弥补实践中发现的不足；软件供应链安全在尝试构建企业级开发安全架构；应对勒索软件则有了体系化的组织和方法；AI 安全在探讨自身的安全合规以及在对抗零日网络攻击中的应用；云安全在探索安全左移的运营商安全。

今年热点议题是对 RSAC2021 的网络安全“弹性”主题的回应，也是在网络安全行业进入深水区，如何解决诸多不确定性问题的积极尝试，对于我国网络安全建设和产业发展具有重要的参考价值。

RSAC 2022 24 款热门产品

RSAC 2022大会自疫情爆发以来首次恢复线下活动，全球网络安全厂商携最新安全产品在展会亮相。 网络安全产业处于高速发展中，各种极具创新精神和价值的新产品、新技术层出不穷，进一步丰富了网络安全行业的产品图谱。

今年参展的产品主要围绕身份和访问安全、应用安全、SaaS 服务和安全运营中心 (SoC) 增强功能。此外，语音欺诈监控工具、攻击面管理平台、人工智能电子邮件安全平台等也引入瞩目。

下面盘点一下 RSAC 2022 的热门的网络安全产品。

1 AppGate 零信任网络访问方案（SDP 6.0）

SDP 6.0 是 AppGate 的零信任网络访问 (ZTNA) 解决方案的最新版本。增加了新的风险模型功能，可让用户扩展其现有企业安全工具的价值和范围，以简化和加速零信任部署。Appgate SDP 6.0 的新风险模型功能使客户能够将高 / 中 / 低敏感度级别分配给特定的工作负载和资源。基于用户已有的安全工具，针对被访问资源的敏感性，SDP6.0 为用户提供一种简单、灵活的方法来衡量登录时的用户 / 设备风险。然后，风险模型根据风险评分动态调整访问权限。

2 Armis 资产漏洞管理（AVM）

Armis 资产漏洞管理 (AVM) 是一种端到端资产漏洞生命周期管理解决方案，支持 IT、OT（运营技术）、ICS（事件指挥系统）、IoMT（医疗物联网）和 IIoT（工业物联网）。在 RSA 会议上，Armis 展示了 AVM 中包含的更新功能，它提供了组织环境的完整资产和漏洞视图、基于风险的优先级及通过自动化和跟踪漏洞管理生命周期的综合仪表板减少平均修复时间。

3 BigID 数据安全解决方案（SmallID）

SmallID 是一种云原生的数据安全按需解决方案，可帮助客户减少攻击面，识别高风险数据，并自动识别“暗”数据（已收集但未用于分析的数据）跨云。SmallID 使用 BigID 专有的机器学习技术来自动发现和分类敏感数据，识别影子和暗数据，并简化合规。

4 Checkmarx 应用安全视图（Fusion）

Checkmarx Fusion 为应用、组件交互和材料清单提供了单一的集成视图。该平台会在软件生命周期的所有阶段生成安全扫描结果，以关联漏洞并确定漏洞的优先级，从而首先指导最关键问题的修复。Checkmarx Fusion 是应用安全 (AST) 平台 Checkmarx one 的一部分。Checkmarx Fusion 支持多引擎扫描关联和跨引擎扫描结果的基于上下文的风险优先级。

5 DNSFilter 数据导出工具（Data Export）

数据导出是一种新工具，旨在让安全团队加快整体威胁检测和响应策略。它自动将 DNSFilter 查询日志数据导出到领先的 SIEM（安全信息和事件管理）和安全监控解决方案，以便通过多个数据源进行聚合、分析和操作。这将有助于减少手动任务并提供对 DNS 的可见性，从而为组织创建完整的安全图景。

6 Forinet 数字风险保护服务 (Fortirecon)

Fortirecon 是一种数字风险保护服务 (DRPS)，它使用机器学习、自动化和人类智能来提供对组织外部攻击面的可见性。Forinet 表示，Fortirecon 有三重功效，包括外部攻击面管理 (EASM)、品牌保护 (BP) 和以对手为中心的情报 (ACI)，用于在侦察阶段检测和反击攻击，以帮助安全人员节省大量时间和降低风险。

7 Gurucul 安全运营和分析平台

Gurucul 安全和运营分析是一个云原生的模块化平台，它将 UEBA、NTA、SOAR 和 IAA 等安全运营中心 (SoC) 解决方案整合到一个单一的访问中，并增加了身份威胁检

测和响应 (ITDR)。该平台强调身份安全，旨在对抗与网络钓鱼、社会工程、凭证盗窃和供应链攻击相关的复杂攻击。

8 Hunters SoC 平台

Hunters SoC 平台推出了新的升级，以推进和简化安全运营工作流程。新功能包括整个安全运营工作流程的自动化、引入风险评分的威胁优先级、数据规范化及对无限数据注入的降噪支持。这种常见 SoC 任务的自动化预计将使数据和安全工程师能够专注于更高价值、领域和组织特定的威胁。

9 Mandiant：MDRP

Mandiant Digital Risk Protection (MDRP) 使用专有的扩展检测和响应 (XDR)，它与来自多个供应商的安全系统一起使用，以提供组织攻击面的情报支持视图。此次发布的产品与 Mandiant Advantage 数字威胁监控的普遍可用性相结合，该监控将与 MDRP 一起安装在 Mandiant Advantage 中。MDRP 将提供对外部暴露以及威胁分析和风险识别的可见性。

10 Noname API security platform 3.0

Noname API 安全平台的最新版本为遵守任何环境、市场和法规要求提供了全球支持。全球支持为该解决方案提供跨各种云和区域的 API 可见性，并识别跨区域的问题和模式，不受流量和环境复杂性影响。它还支持遵守各个地区的现行法规，包括 PCI-DSS、PII 和数据驻留要求。

11 Optiv：网络恢复解决方案 (CRS)

网络恢复解决方案 (CRS) 为组织提供战术建议和技术，以保护并从网络攻击中快速恢复。该解决方案通过自动化工作流程识别并优先处理业务关键资产。该公司将在 RSA 上展示它如何使用上下文关键技术通过数据仓库、数据隔离、物理隔离备份解决方案来备份基本数据、应用程序和系统。

12 RSA 身份和访问管理方案（ID Plus）

ID Plus 是一种基于 SaaS 的身份和访问管理 (IAM) 解决方案，为客户提供云、本地和混合部署的选择。ID Plus 是一款内置于 DS100 的新工具，该工具是 RSA 的新硬件验证器，专为 RSA 的零信任客户而设计。DS100 是一种无密码身份验证器，它使用 FIDO（快速在线身份验证）协议和一次性密码解决方案。该身份验证器是一款基于云的产品，可插拔使用。

13 SentinelOne 漏洞扫描修复工具

Singularity Vulnerability Mapping 是 SentinelOne 为 Ivanti 提供的集成工具，利用后者的统一 IT 平台和 Sentinel 自己的 Singularity XDR 提供自主网络和漏洞扫描及快速修复。Singularity Vulnerability Mapping 可以与 Ranger 的 IoT 网络发现系统和 SentinelOne 的 Storyline Active Response (STAR) 自动威胁搜寻、检测和响应工具一起使用，以帮助分析师确定补丁的优先级并降低风险。

14 BlackBerry 零信任网络访问 工具

黑莓展示了 CylanceGateway 零信任网络访问 (ZTNA) 工具，可为用户提供网络和设备监测，上下文关联和持续身份验证，以限制对受信任、经过身份验证和已知用户、设备的访问。工具可以保护任何网络、任何设备的访问、使用 Cylance 人工智能来降低风险并提供 0day 网络钓鱼检测，从而有效降低勒索软件和其他网络安全威胁。此外，还为自带设备 (BYOD) 部署提供安全连接，并使用 Mitre Att&ck 框架规则检测横向移动攻击。

15 Cisco Security Cloud

思科详细介绍了新的总体安全战略，重点推出酝酿依旧的 Cisco Plus 产品，用于统一安全访问服务边缘 (SASE)。思科安全云平台将在思科产品体系中占据重要地位，基于开放标准的统一平台将确保跨混合云和多云环境的安全性，并具有安全连接位于任何地方人员、应用和设备的能力，实现大规模的威胁预防、检测、响应和补救措施。

16 Palo Alto Networks

Palo Alto Networks 展示的 Prisma 云原生安全产

品的新功能，引起业界的广泛关注。近段时间，Palo Alto Networks 不断推出安全产品：3 月公布一款供应链安全领域的产品，用以寻找软件供应链中的潜在漏洞或错误配置；2 月推出针对托管服务提供商 Prisma SASE 新功能，包括分层多租户云管理平台和开放性 API 框架。

17 SailPoint 身份安全产品

身份安全公司 SailPoint 展示了两款新产品——SailPoint Identity Security Cloud Business 和 SailPoint Identity Security Cloud Business Plus，后者提供更多产品来发现、保护和管理整个混合基础架构中的身份。SailPoint 身份安全云业务包可以为用户提供必要的身份安全功能，并利用人工智能和机器学习来构建更强大的身份安全。

18 Pindrop 语音安全产品

语音防欺诈提供商 Pindrop 展示了最新产品。其语音安全技术的新功能包括预测年龄范围、预测口语和监控语音验证欺诈的方法。Pindrop 发展趋势迅猛，美国多家大型银行成为其客户，保护数亿用户免受基于语音的欺诈和攻击。



19 Orca 云安全

Orca Security 最近的产品开发动作主要是“上下文感知安全”，被用于开发早期识别和预防云应用安全问题，以及针对云原生应用的攻击路径分析和业务影响评分。该产品考虑了当前的运行环境和部署的代码，以提高准确性，并通过上下文和优先级警报等措施监控生产环境的风险。

20 Randori 攻击面管理服务

IBM 宣布收购的 Randori 在攻击面管理和攻击性网络安全服务上有着独到优势，IBM 计划将 Randori 的 ASM 平台与其扩展检测和响应 (XDR) 产品 IBM Security QRadar 集成，从而就能够保持攻击面的实时可见性。此外，IBM 还将使用 Randori 的持续红队攻击测试 (CART) 来改进 X-Force Red 进攻性安全服务。

21 Abnormal Security

Abnormal Security 主要业务包括保护企业和机构组织避免受到针对性的电子邮件攻击，旗下云电子邮件安全 (ICES) 平台可以和 Microsoft 365 集成，产品的创新之处在于结合当前云原生环境的发展和需求，孵化出了基于 AI 人工智能技术的电子邮件安全防护机制。

22 DoControl

DoControl 是一家美国数据访问控制服务商，展示了 SaaS 应用程序数据访问监视，编排和修复所需的自动化自助服务工具。公司采用独特的，以客户为中心的方法来应对流行的 SaaS 应用程序中的劳动密集型安全风险管理和数据泄露防护挑战。

23 Snyk 开发者安全平台

网络安全独角兽公司 Snyk 独特的“安全智能”工具帮助开发者持续监测可能发生的漏洞，并不断自动化安全性能升级。Snyk 帮助开发者在开发生命周期中一以贯之地查找、修复和监测代码的脆弱性，让开发者更好地应对纷繁复杂的微服务、API，以及日益增长的复杂性。

24 Fortanix 区块链安全产品

初创公司 Fortanix 展示了两个区块链安全产品：Fortanix Non-Custodial Warm Wallet 通过双因素身份验证令牌，确保数字资产不会在未经同意的情况下被钱包提供商滥用。Fortanix Ignite One-Time Signer 有助于验证区块链交易的合法性。新工具与 Fortanix 数据安全管理器集成，这是一套专为区块链、加密货币和去中心化金融业务设计的服务。

APP 违规收集个人信息风险分析报告

概要

2022 年第一季度，奇安信病毒响应中心共收录全国应用市场新增APP活跃样本近30万个。本报告依据《APP违法违规收集使用个人信息行为认定方法》等内容要求，使用奇安信自研安卓动态引擎 QADE 对新增 APP 样本进行抽样检测，重点评估“无提示收集个人信息”和“高频次收集个人信息”两种最为常见、影响较深的合规性问题。

报告发现，APP 违规收集个人信息的现象仍然十分普遍，平均每 5 个 APP 中，就有一个存在违规收集个人信息的风险。部分存在违规收集个人信息风险的 APP 社会影响面巨大，网上购物、生活休闲、办公商务等常用 APP 的违规风险问题最为突出。此外，八成以上的违规个人信息收集行为是由于 APP 集成了某些不规范的第三方 SDK，或者是没有对第三方 SDK 收集个人信息的行为进行声明造成的。

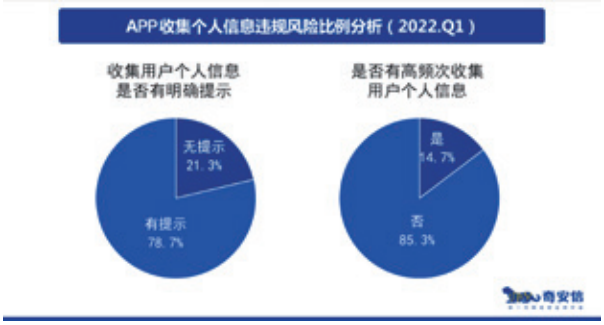
第一章 流行 APP 违规风险形势分析

随着互联网和移动设备的发展，手机已成为人人都拥有的设备，APP 的流行使人们对 APP 违规收集个人信息的风险更加担忧。为切实加强用户个人信息保护，工业和信息化部为此发布了一系列的相关法律法规和监管标准通知，并在全国范围内组织开展 APP 违法违规收集使用个人信息专项治理工作。

一、 存在违规风险的 APP 规模

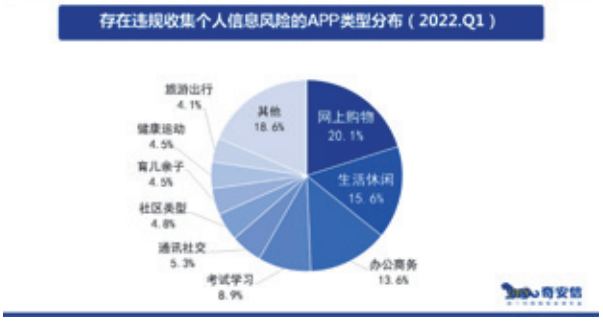
2022 年第一季度，在针对近 30 万个新增活跃 APP 样本的抽样检测中，存在“无提示收集个人信息”风险和“高频次收集个人信息”风险的 APP，分别占到检测样本总量的 21.3% 和 14.7%。总体来看，平均每 5 个 APP 中，就会有一个存在个人信息收集方面的违规风险。

本季度检出的所有存在违规风险的 APP 中，至少有 1 款下载量超过 1 亿次，4 款下载量超过 1000 万次，19 款下载量超过 100 万次。仅这 24 款 APP 就至少影响国内超过 2 亿用户。



二、存在违规风险的 APP 类型

从 APP 类型来看，在 2022 年第一季度的检测中，存在违规风险最多的 APP 是网上购物类 APP，约占所有存在违规风险 APP 总数的 20.1%。其次是生活休闲类，占比为 15.6%。办公商务类排名第三，占比 13.6%。

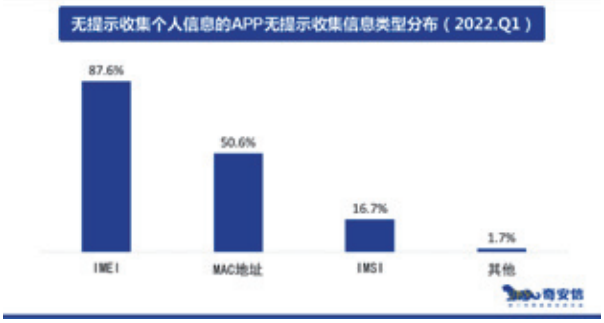


第二章 典型 APP 违规风险形势分析

一、无提示收集个人信息类型分析

在所有存在“ 无提示收集个人信息”风险的APP 中，IMEI、MAC 地址和 IMSI 是 APP 静默收集个人信息最主要的 3 个类型。其中，87.6% 会无提示收集 IMEI 信息，50.6% 会无提示收集 MAC 地址，16.7% 会无提示

收集 IMSI 信息，而无提示收集其他个人信息的情况，仅占 1.7%。



二、高频次收集个人信息情况分析

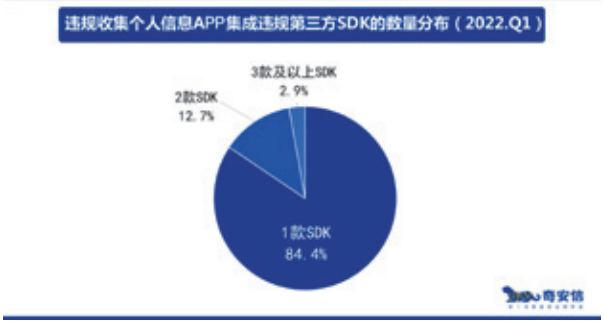
在 2022 年第一季度检测的所有新增活跃 APP 样本中，一百秒内收集用户个人信息超过 2 次（包含 2 次）的 APP 占到了所有被检测 APP 总量的 14.7%。在所有存在高频次收集个人信息风险的 APP 中，每一百秒收集个人信息次数大于等于 2 次，但低于 5 次的 APP 约占 44.0%；6~10 次的占比 28.7%，11~20 次的占比 18.8%，大于 20 次的占比 8.5%。

在本季度的检测中，发现某款收集个人信息最为频繁 APP，在一百秒内对 IMEI 信息收集了 138 次，平均每秒 1.38 次。

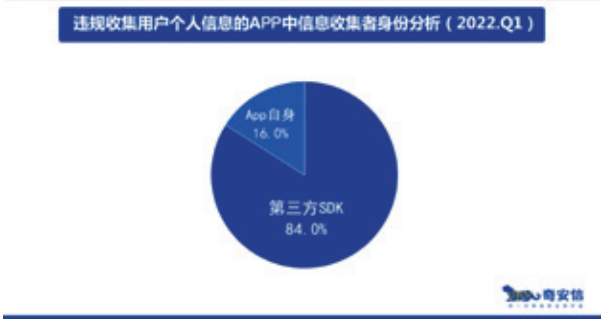


第三章 违规个人信息收集者分析

APP 对于用户个人信息的收集，未必都是由 APP 自身来完成的，很多时候是因为 APP 集成了第三方 SDK，而第三方 SDK 存在个人信息收集行为。统计显示，在所有存在“无提示收集个人信息”和“高频次收集个人信息”风险的 APP 中，对用户信息进行违规收集的，84.0% 属于第三方 SDK 行为，仅有 16.0% 属于 APP 自身行为。检测还发现，有两款知名的第三方 SDK，分别覆盖了存在违规行为的 APP 总量的 29.0% 和 21.0%。



统计显示，在所有集成了违规收集个人信息 SDK 的 APP 中，只集成了 1 款违规 SDK 的 APP 占比为 84.4%，集成了 2 款违规 SDK 的 APP 占比为 12.7%，另有 2.9% 的 App 集成 3 款及以上的违规 SDK。



附：发布机构介绍

奇安信病毒响应中心是奇安信集团旗下的专业病毒鉴定及响应团队。中心以奇安信核心云平台为基础，拥有每日千万级样本检测及处置能力、每日亿级安全数据关联分析能力。结合多年反病毒核心安全技术、运营经验，基于集团自主研发的 QOWL 和 QDE 引擎，形成跨平台木马病毒查杀能力与漏洞修复能力，并且具有强大的大数据分析能力，可以实现全平台安全和防护预警能力。

华云信安·产业教育中心

网安人才培养新模式
打造产业人才成长圈

产教融合

INTEGRATION OF PRODUCTION AND EDUCATION

- 共建产业学院
- 共建合作专业
- 共建联合实验室
- 共建人才/师资培养基地
- 1+X证书合作
- 教育部协同育人项目合作

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

华云信安(深圳)科技有限公司（简称 华云信安™ ）成立于2016年，是一家深耕于网络空间安全领域，拥有自主研发能力及核心知识产权，提供网络安全解决方案与技术服务的高新技术企业。华云信安™总部位于深圳，在广州、上海、武汉设有分支机构，公司核心团队来自奇安信、网易、华为、绿盟、思科等国际知名科技企业，具有深厚的网络安全技术实力和管理经验。

华云信安™目前拥有数十项计算机软件著作权和十余款自主研发产品，具备“风险评估类”和“安全工程类”两项信息安全服务资质，通过ISO9001质量管理体系认证，现为深圳市信息安全行业协会理事单位和深圳市信息网络安全管理协会会员单位。

华云信安™凭借创新的网络安全产品体系、深厚的网络安全服务能力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、政务等领域的广大客户，提供专业优质的网络安全产品、网络安全解决方案和网络安全技术服务。

网络犯罪研究中心

华云信安·网络犯罪研究中心，是专注于打击网络犯罪的安全服务部门，致力于打击涉网新型犯罪领域的安全技术研究与产品研发，包括涉网犯罪案件技术支撑、网络诈骗案件技术支撑、涉众型经济犯罪案件技术支撑等，以攻防实验室和极牛技术社群组成创新型的安全研究团队，为国家及各省市公安机关提供高效专业的打击涉网犯罪情报分析服务和实战解决方案。

极牛攻防实验室

华云信安·极牛攻防实验室，由内部成员及外部知名技术专家团队组成，致力于最前沿网络安全技术的研究和调研，以指导技术研发路径和产品发展方向。其职责除开展传统的网络安全技术研究外，还跟踪国内外网络安全技术趋势并进行相关技术研究。现已协助国家互联网应急中心(CNcert)发现并修复数百个安全漏洞，获得数十张高危原创漏洞证明证书。

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

我们提供卓越、丰富的信息安全产品及各行业解决方案、信息安全技术服务和基础架构咨询服务。

专业的团队服务

我们拥有资深、专业的服务团队，按需为用户提供多元化、多级别的咨询规划服务和技术实施服务。

众多的行业案例

我们拥有众多行业应用案例，包括制造、快消、航空、金融、物流、建筑、服务、互联网等行业。

深入的厂商合作

我们与多家国内外知名厂商建立战略合作关系，共同致力于优质解决方案及相关服务的推广落地。

全国范围的服务

我们公司总部在深圳，同时在上海、广州、武汉等设有分支机构，具有全国范围内的业务服务能力。

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全



7436084028