安全快一步

2021年1月 创刊号

网安26号院

SECURITY INSIDER

透视

最严重 APT 供应链攻击 P10

兴业数金
CIB FINTECH

首家银行系金融科技子公司

兴业数金 系兴业银行集团旗下金融科技子公司，成立于2015年12月。面向集团，作为集团高科技内核和创新孵化器，全面负责兴业银行集团科技研发和数字化创新工作。对外，兴业数金致力于运用云计算、人工智能、开放API、流程机器人等前沿科技，为商业银行数字化转型提供解决方案，输出科技产品与服务。

更多业务交流与咨询，可联系寿先生：13774399844，欢迎垂询。

共建网络安全 共享网络文明

——写在《网安26号院》创刊之际

栉沐寒风，俏迎瑞雪。

2021年岁首，奇安信迎来了新的家庭成员——《网安26号院》。

在信息泛滥的时代，理性是这个时代的稀缺。我期待，《网安26号院》能成为中国网络安全领域的一个价值坐标，有自己的思考，不盲目跟风，散发出理性的光芒。

坐标的原点是“安全”。在刚刚过去的2020年，未来从未如此未知，安全从未如此不安。尽管中国迅速控制疫情，市场回暖经济复苏，但全球疫情形势依然极为严峻，不确定不稳定因素显著增多，国际现实一片魔幻。现实与虚拟相互交织，网络空间的边界加速消亡，安全问题首当其冲：“海莲花”“蔓灵花”“白象”“绿斑”等多个黑客组织攻击异常活跃，窃取机密情报、劫持重要网站、对企业勒索攻击、破坏关键基础设施的稳定运行……监测安全事件，捕捉网络漏洞，防范网络攻击，促进数字产业发展，是奇安信的责任和价值所在，也是《网安26号院》立刊的核心。

坐标的横轴是技术。奇安信作为行业领军者，将努力围绕产业链短板和薄弱环节，持续加大研发投入，突破一批基础性、通用性、前沿性、颠覆性网络安全核心技术，打造多方协同融合发展的网络安全产业生态，改变当前网络安全“小零同”现状。《网安26号院》是一个汇聚观点、洞察趋势的平台，是各种技术思想交流碰撞的载体，将推进技术研究和创新，成为网络安全新技术、新理论、新思想的汇聚场，成为弥合争端达成共识的辩论场，成为激发灵感、共同创新的竞技场。

坐标的纵轴是人。事业之所始者，以人为本。2020年，奇安信人勇敢前行，与祖国共克时艰、携手抗疫。近万名兄弟姐妹奋战在网安一线，一诺千金、披荆斩棘。在火神山，在雷神山，在小汤山，在遥远的西藏、新疆，在祖国的心脏……奇安信人用信念、责任和担当，筑起了一道网络安全屏障；2020年，奇安信人不断创新，锐意进取，在取得一系列领先成果的同时，磨练了意志，增强了内功；2020年，奇安信的人才队伍不断壮大，“五五制”凝聚精英力量，锻造了一支高素质的干部专家队伍，近千名校招生通过“扬帆计划”快速起航。我相信，《网安26号院》将成为奇安信人共同的文化驿站、心灵港湾。在未来的岁月里，《网安26号院》将记录奇安信人编程的生活、经历的成长和朝气蓬勃奋进的模样。

刊物初创，当如旭日之升；刊物精神，当如皓月之恒；刊物虽小，当心怀网络天下。作为一份初创的企业刊物，或力有不逮，但应勠力求之，全力以赴为未来的网络安全行业提供一份助力。

让我们携起手来，共建网络安全，共享网络文明。

奇安信集团董事长

齐向东

2021年1月1日

CONTEN

目录

安全态势

月度专题

TS

攻防一线

安全之道

奇安信人

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
副总编	裴智勇
安全态势主编	王彪
月度专题主编	李建平
攻防一线主编	魏开元
安全之道主编	张少波
奇安信人主编	孙丽芳
奇安资讯主编	陈冲
安全意识主编	李建平

奇安信集团　虎符智库　安全内参

投稿邮箱 26hao@qianxin.com

联系电话 13701388557

事件篇

美政府被指遭俄黑客大规模供应链攻击，全球近两万个组织受影响

2020年12月综合消息，12月14日，美国公司SolarWinds旗下网管软件被曝光遭到供应链攻击，发布了受污染的更新版本，导致美国财政部、商务部等多家联邦机构被黑，邮件被监控数月。据SolarWinds披露，其3.3万个客户中，有约1.8万个客户安装了被污染版本。

后期经调查，美国国务院、国防部、能源部、国土安全部、司法部、多个州政府、微软、思科、VMware、FireEye等关键政企机构均遭受不同程度的攻击，内部机密邮件、源代码、特权账号、网络武器库等被窃取。美国政府认为，俄黑客组织主导了这一攻击。（注：本期专题板块刊登了该事件的深度分析）

美国物流巨头 Forward Air 遭勒索软件攻击，业务被迫中断

据BleepingComputer 2020年12月21日消息，美国物流巨头Forward Air遭到Hades勒索软件攻击，迫使公司关闭内部系统以防止扩散，据称海关放行文件存放在离线系统中，处于不可用状态，该公司业务已经中断。Forward Air在2019年收入为14亿美元，有4300余名员工。

公民实验室：32 名记者的 iPhone 手机遭最高级别 0day 攻击

据Ars Technica 2020年12月22日消息，加拿大多伦多大学公民实验室周日发布报告称，在今年7-8月，有32名记者的iPhone手机被黑，聊天记录和密码被盗。攻击者使用了iMessage零交互0day漏洞，无需受害者做操作也可以感染手机。报告称攻击者采购了间谍软件公司NSO Group的Pegasus网络武器，不过NSO否认了这一指控。

芬兰议会遭网络间谍攻击，多位国会议员邮箱账号被破坏

据BleepingComputer 2020年12月28日消息，芬兰议会今日透露，由于发生网络攻击，多位国会议员的邮箱账号遭到破坏。芬兰议会的安全团队在今年秋季发现了这次攻击，目前正由国家调查局进行调查。议会议长Anu Vehviläinen说，这次事件是对芬兰社会和民主的严重攻击，需要在国内、欧盟以及其他国际合作中采取积极行动。芬兰国家调查局发布声明称，该案正作为涉嫌间谍活动进行调查。在此之前，挪威议会曾在今年8月遭到攻击，后被归因为俄APT28组织；德国联邦议会曾在2015年被黑，后也被归因为APT28组织；欧盟还因此在今年10月还宣布对多个APT28成员实施制裁。

家电巨头惠而浦遭勒索软件攻击，内部数据被公开

据Security Affairs 2020年12月28日消息，美

国知名家电巨头惠而浦在12月初遭到Nefilim勒索软件攻击，攻击者窃取了内部数据并索要赎金，由于勒索谈判失败，该团伙放出了惠而浦的内部数据，包括员工福利、医疗信息请求、住宿要求等相关内容。Nefilim勒索软件在近期比较活跃，曾经破坏了意大利眼镜和眼保健巨头Luxottica、网络运营商Orange、技术服务商SPIE Group等大型机构的数据。

马来西亚武装部队确认受到网络攻击：未影响运行

据Straits Times 2020年12月29日消息，马拉西亚武装部队（MAF）今日公开确认，12月28日（周一）曾遭到试图窃取内部数据的网络攻击。武装部队负责人Affendi Buang表示，网络攻击未能影响系统的运行，仅在一开始成功入侵了少数外围网段，武装部队内部的网络与电磁防御部门、网络防御运营中心两个部门均跟进了事件响应处置。据称，周一中午，武装部队门户网站上出现了不雅图片。

台湾合勤科技旗下安全设备被爆后门账号，现遭黑客规模滥用

据Ars Technica 2021年1月5日消息，12月23日，中国台湾合勤科技（Zyxel）旗下防火墙、VPN、统一安全网关等多款安全设备被荷兰安全公司Eye Control曝光，存在隐藏的最高权限账号zyfwp，密码写死且无法修改（CVE-2020-29583）。本周一安全公司GreyNoise的创始人Andrew Morris称，已检测到利用该漏洞的自动化攻击流量，攻击者正大批量尝试登录攻击。

交通银行辟谣：网传“客户信息泄露”不实，与真实用户信息不符

2021年1月11日消息，交通银行官网发布声明称，前几日网传“暗网贩卖所谓交行客户信息”消息不实。官方表示，经系统核查比对，确认与银行真实客户信息不符，

交通银行不存在客户信息泄漏，已就相关违法行为向公安部门报案，依法追究损害其商誉行为的法律责任。

美国右翼社交平台 Parler 超 70TB 数据泄露，已被下载扩散

据 HackRead 2021 年 1 月 11 日消息，美国右翼社交平台 Parler 由于被美国主流数字基础设施苹果、谷歌、AWS 等封杀，平台安全性受到了极大打击。有用户声称在 1 月 6 日下载了 Parler 大约 70-80TB 的数据，包括帖子、照片、视频、消息等。由于 Parler 的电话和邮件验证服务被封杀后已不可用，该用户使用之前的管理员账户创建新的特权账号，并用新账户下载了平台数据。Parler 平台在特朗普支持者中非常受欢迎。

“格格病毒”潜伏十余年发作，上半年还将“爆发”19 次

2021 年 1 月 14 日消息，奇安信 CERT 监测到格格病毒（incaseformat）在 1 月 13 日发作，表现为电脑中招后，除系统 C 盘以外其他文件全部被删除。经研判，该病毒为多年前的老病毒，不具网络传播性，通过 U 盘等移动存储介质传播，具备定时删除文件的能力，会在特定时间定时发作，最近的一次发作日期是 2021 年 1 月 23 日，后续在 2021 年上半年还至少 19 次发作日期。由于该病毒隐蔽性强，难以根除，奇安信强烈建议用户“应检尽检”，全面在终端上安装天擎等集中式安全管理软件，构筑无死角的防线。

漏洞篇

Apache Airflow 错误会话漏洞（CVE-2020-17526）预警

2020 年 12 月 29 日，工信部网络安全威胁信息共享平台发布漏洞预警，Apache 发布的邮件通告中披露 Apache Airflow 错误会话漏洞（CVE-2020-17526），攻击者可利用该漏洞进行未授权访问。目前，Apache 已发布安全版本修复该漏洞，建议受影响用户及时升级至 1.10.14 及以上版本，并做好资产自查以及预防工作，以免遭受黑客攻击。Apache Airflow 是一套用于创建、管理和监控工作流程的开源平台。

Oracle WebLogic XXE 漏洞安全风险通告

2021 年 1 月 4 日，奇安信 CERT 发布漏洞风险通告，收到补天漏洞响应平台报告的 Oracle WebLogic Server XXE 漏洞，攻击者可以在未授权情况下对目标系统发起 XML 外部实体注入攻击。成功触发该漏

洞需要目标开启 T3 或 IIOP 协议。鉴于此漏洞影响较大，目前尚无补丁，建议用户尽快采取紧急修复措施。Oracle WebLogic Server 是基础中间件中的融合中间件服务。

国家漏洞库关于 Apache Flink 安全漏洞的通报

2021年1月7日，国家信息安全漏洞库（CNNVD）收到关于 Apache Flink 安全漏洞（CVE-2020-17519、CVE-2020-17518）情况的报送。成功利用漏洞的攻击者，可在未授权的情况下，构造恶意数据执行任意文件读取或文件写入攻击，最终获取服务器敏感性信息或权限。Apache Flink 1.5.1 - 1.11.2 版本均受此漏洞影响。目前，Apache 官方已经发布了版本更新修复了该漏洞，建议用户及时确认产品版本，尽快采取修补措施。Apache Flink 是美国 Apache 基金会的一款开源的分布式流数据处理引擎。

国家漏洞共享平台预警：致远 OA 系统存在文件上传漏洞

2021 年 1 月 11 日消息，国家信息安全漏洞共享平台（CNVD）官网发布致远 OA 系统存在文件上传漏洞（CNVD-2021-01627）的安全公告。近日，有安全人员披露了致远 OA 系统高危漏洞。未经身份验证的攻击者利用该漏洞，可通过精心构造恶意脚本文件，使用 POST 方法向目标服务器上传文件，继而通过远程代码执行植入网站后门，控制目标服务器。目前，漏洞细节已公开，厂商已发布版本补丁修复。致远 OA 是由北京致远互联软件股份有限公司开发的一款协同办公产品。

Windows Defender 严重漏洞被滥用，微软发布修复补丁

2021 年 1 月 13 日消息，奇安信威胁情报中心监测发现，微软在今日的例行补丁日修复了一个严重级别的 Windows Defender 远程代码执行漏洞（CVE-2021-1647）。攻击者可通过向目标受害者发送邮件或恶意链接等方式诱导受害者下载攻击者构造的恶意文件，从而使 Windows Defender 在自动扫描恶意文件时触发利用该漏洞，最终控制受害者计算机。微软官方披露目前已发现在野利用，奇安信威胁情报中心分析认为：该漏洞确认可被利用，不过 Windows Defender 联网后会自动升级补丁，故目前可造成的影响已经不大。Windows Defender 是 Windows 系统内置默认杀毒软件。

政策篇

工信部印发《电信和互联网行业数据安全标准体系建设指南》

2020 年 12 月 25 日消息，工信部印发《电信和互联网行业数据安全标准体系建设指南》。《指南》提出，

到 2021 年，研制数据安全行业标准 20 项以上，初步建立电信和互联网行业数据安全标准体系，到 2023 年，研制数据安全行业标准 50 项以上，标准的技术水平、应用效果和国际化程度显著提高，有力支撑行业数据安全保护能力提升。电信和互联网行业数据安全标准体系包括基础共性、关键技术、安全管理和重点领域等标准。

四部门发文：加快构建全国一体化大数据中心协同创新体系 强化大数据安全防护

2020 年 12 月 28 日消息，发改委、网信办、工信部、国家能源局四部门联合发布《关于加快构建全国一体化大数据中心协同创新体系的指导意见》，加强全国一体化大数据中心顶层设计。《意见》提出，加快提升大数据安全水平，强化对算力和数据资源的安全防护，形成“数盾”体系；推动核心技术突破及应用，加强对关键技术产品的研发支持，加快科技创新突破和安全可靠产品应用。

我国《国防法》修订通过：要求维护网络空间的活动、资产和其他利益的安全

2020 年 12 月 27 日消息，《中华人民共和国国防法》经全国人大正式修订通过，将于 2021 年 1 月 1 日起施行。该法首次提出，国家采取必要的措施，维护在太空、电磁、网络空间等其他重大安全领域的活动、资产和其他利益的安全。

网信办《互联网信息服务管理办法（修订草案）》公开征求意见

2021 年 1 月 8 日消息，网信办会同工信部、公安部起草《互联网信息服务管理办法（修订草案征求意见稿）》，向社会公开征求意见。修订草案相比现行《办法》，条文数量由 27 条增加至 54 条，进一步细化和完善了互联网信息服务的监管要求。《办法》明确了国家网信部门对全国互联网信息内容实施监督管理执法；国务院电信主管部门对互联网信息服务的市场准入、市场秩序、网络资源、网络信息安全等实施监督管理；国务院公安部门负责维护互联网公共秩序和公共安全，防范和惩治网络违法犯罪活动。

工信部印发《工业互联网创新发展行动计划（2021-2023 年）》

2021 年 1 月 13 日消息，工信部印发《工业互联网创新发展行动计划（2021-2023 年）》，提出到 2023 年，我国工业互联网新型基础设施建设量质并进，新型基础设施进一步完善、融合应用成效进一步彰显、技术创新能力进一步提升、产业发展生态进一步健全、安全保障能力进一步增强。《行动计划》明确将开展网络体系强基行动、标识解析增强行动、安全保障强化行动等 11 项重点任务。

欧盟委员会发布《数字十年的欧盟网络安全战略》

据 europa.eu 2020 年 12 月 16 日消息，欧盟委员会发布《数字十年的欧盟网络安全战略》，旨在增强欧洲抵抗网络威胁的集体应对能力，确保所有公民和企业都能从可信赖、可靠的数字服务中充分受益。新《战略》的核心是信任与安全，包含三个具体建议：加强弹性、技术主权和领导力；建立预防、制止和应对网络攻击的

能力；通过加强合作促进全球开放的网络空间。

英国国家网络安全中心发布《农业网络安全指南》

据 gov.uk 12 月 22 日消息，英国国家网络安全中心（NCSC）与英国农民联盟联合发布《农业网络安全指南》，帮助农业界保护自身免受最常见的网络攻击。电子邮件、在线会计工具、在线支付系统及自动耕作设备等越来越多的使用，使得农业界网络风险日益增长，亟需做好保护措施。该《指南》编写清晰易懂，以提示的形式提供建议，可以帮助用户轻松实施安全措施。

美网络安全与基础设施安全局发布远程用户网络安全指南草案

据 fedscoop 2020 年 12 月 23 日消息，美国网络安全与基础设施安全局（CISA）周二发布可信互联网连接（TIC 3.0）的远程用户网络安全指南草案，旨在保障联邦机构网络与外部连接的安全。CISA 官员 Matt Hartman 表示，新的用例可以帮助联邦机构提升远程办公环境的应用性能，减少使用专线来降低成本，并通过与可信云服务连接来改善体验。该草案的征集意见时间截止于 2021 年 1 月 29 日。

美国政府推出《国家海事网络安全计划》

据 The Hill 2021 年 1 月 5 日消息，美国白宫今日推出《国家海事网络安全计划》，以保护美国海事领域免受可能危害国家安全的网络安全威胁。该计划于 12 月编制，本周公布。海事领域约占美国国内生产总值的四分之一。该计划的三个目标包括：一是建立定义对海事领域威胁的国际标准；二是增强针对上述威胁的情报和信息共享；三是增加美国在海事领域的网络劳动力。该计划旨在应对行业中越来越多应用新信息技术和运营技术系统所带来的新威胁。

美国众议院通过《联邦风险评估和管理计划授权法案》

据 MeriTalk 2021 年 1 月 5 日消息，美国众议院于 1 月 5 日通过了《联邦风险评估和管理计划（FedRAMP）授权法案》。该法案将 FedRAMP 编为法律，并每年拨款 2000 万美元用于该计划及其维护。FedRAMP 计划为云服务和产品的安全评估、授权和连续监视提供了一种标准化方法。该授权法案旨在弥补计划中的不足，并提高认证过程的效率。FedRAMP 始于 2011 年，但目前没有标准化的认证框架。该法案旨在创建“一次认证、多次重用”的模型，还将建立一个联邦安全云咨询委员会，以确保行业、总务管理局、机构网络安全和采购官员之间的对话。安

奇安信
新一代网络安全领军者

奇安信营销体系
招募精英

党政大客户部总经理

1.负责中央部委及二级单位市场的全年销售任务达成；
2.制定年度销售计划及预算，分解销售任务，推动并确保相应计划、目标的达成；负责团队的建设、管理、指导与激励；
4.重要客户中高层关系维护，项目运作与把握；潜在客户的市场拓展，制定增量目标，计划并达成；
5.进行市场调研与分析，研究同行业界发展状况，为公司战略制定、产品规划等方面提供相应建议。

大客户销售经理

党政/网信/电子政务/审计行业

1.根据公司及本行业销售任务开展销售工作，完成各项销售指标；
2.开拓、积累、夯实客户基础；
3.挖掘客户需求，为客户提供整体解决方案；
4.负责组织开展行业市场活动，加强公司在行业内的品牌影响力；
5.挖掘、反馈所负责行业的市场信息及客户需求，促进产品体系优化，构建有竞争力的市场策略。

售前技术专家

党政大客户部

1.负责国家党政机关头部客户的售前技术工作，协同党政大客户部销售拓展客户商机及业务布局，配合销售挖掘项目机会、引导客户需求
2.负责党政大客户部客户技术交流、项目技术文档编写、项目招投标等售前支撑工作；
3.负责党政大客户部技术策略梳理、技术资料整理，并能在党政机关头部客户进行技术和解决方案推广。

解决方案专家

党政/网信/电子政务/审计行业

1.协助行业技术负责人完成行业级解决方案、营销技术策略、行业技术资料整理，并能在行业进行技术和解决方案推广；
2.协同行业销售拓展客户商机及业务布局，配合销售挖掘项目机会、引导客户需求；
3.完成行业市场典型客户调研，不断提升解决方案竞争力，能洞察行业趋势、参与行业规范制定。

扫码联系我们

奇安信
新一代网络安全领军者

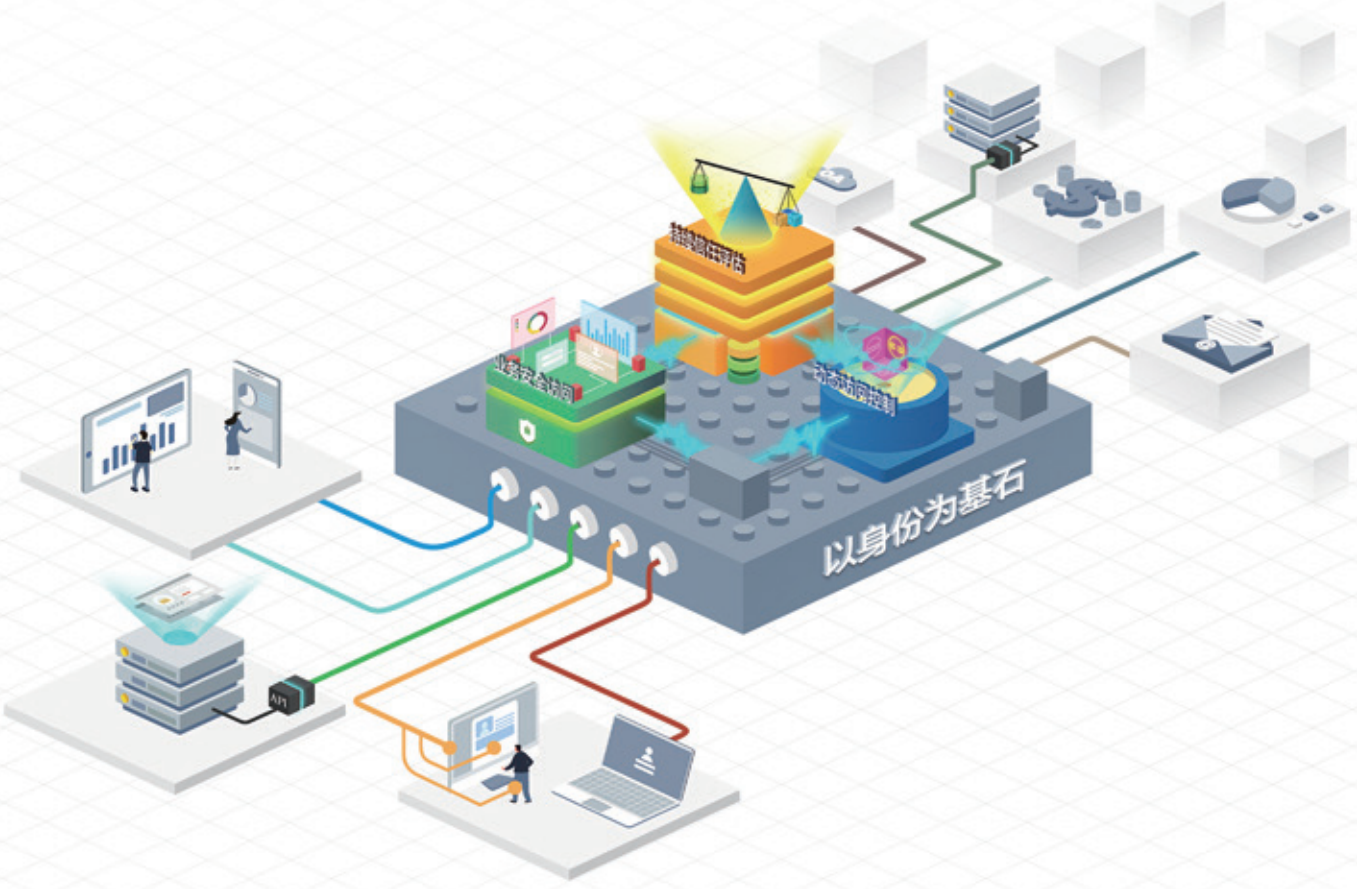
让网络更安全 让世界更美好

云计算和大数据时代

网络安全边界逐渐瓦解，内外部威胁愈演愈烈

传统安全架构正在失效

零信任安全 新身份边界



以身份为基石

- 为人和设备赋予数字身份
- 为数字身份构建访问主体
- 为访问主体设定最小权限

业务安全访问

- 全场景业务隐藏
- 全流量加密代理
- 全业务强制授权

持续信任评估

- 基于身份的信任评估
- 基于环境的风险判定
- 基于行为的异常发现

动态访问控制

- 基于属性的访问控制基线
- 基于信任等级的分级访问
- 基于风险感知的动态权限

构筑基于身份的动态虚拟边界

全面身份化 | 授权动态化 | 风险度量化 | 管理自动化

www.qianxin.com

kefu@qianxin.com

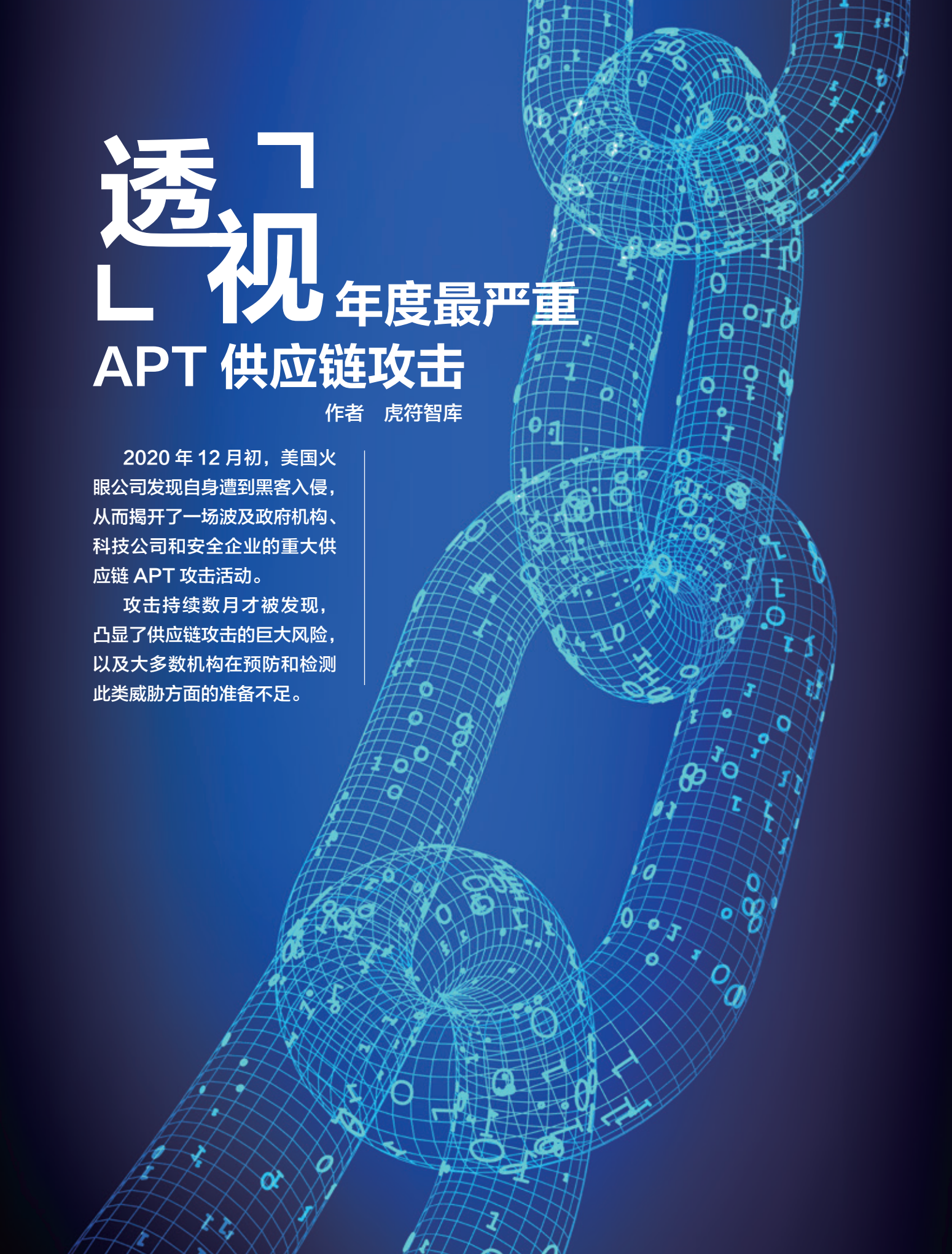
400-930-3120

透视 年度最严重 APT 供应链攻击

作者　虎符智库

2020 年 12 月初，美国火眼公司发现自身遭到黑客入侵，从而揭开了一场波及政府机构、科技公司和安全企业的重大供应链 APT 攻击活动。

攻击持续数月才被发现，凸显了供应链攻击的巨大风险，以及大多数机构在预防和检测此类威胁方面的准备不足。



一场影响全球大型机构的攻击

攻击的冰川一角

12月8日，美国安全公司火眼发布通告称，公司网络被“拥有一流网络攻击能力”的国家黑客组织所突破：攻击组织利用前所未有的技术组合，渗透进入火眼公司内网，盗取了火眼的网络武器库——红队测试工具，可被用于在世界范围内入侵高价值的目标。

对于攻击者所展示出的攻击能力，火眼首席执行官凯文·曼迪亚（Kevin Mandia）甚至用“25年所遭遇的顶级攻击”来形容：从攻击者的行为、操作的隐蔽性和使用的技术来看，攻击的背后无疑是国家背景的黑客组织。

但令人想不到的是，火眼被入侵事件只是一场重大APT攻击活动的冰山一角。

12月14日，路透社和《华盛顿邮报》报道，因知名IT公司SolarWinds旗下的网络监控软件Orion的更新服务器遭黑客入侵并植入恶意代码，导致美国众多政府机构和企业用户遭到入侵，火眼公司只是首个被曝光的受害者。

黑客正是通过这种供应链攻击，获得了"后门"访问权，窃取了火眼公司的客户网络安全测试工具（红队工具）。针对SolarWinds的攻击发生在数月前，但直到其客户——火眼公司调查自己的入侵事件时才被发现。

SolarWinds在向美国证交会提交的文件中表示“大约有18,000个客户下载了木马化的SolarWinds Orion版本”。奇安信CERT分析，被污染的SolarWinds软件带有公司签名，这表明SolarWinds内部很可能已经被黑客完全控制。

攻击者入侵的SolarWinds是全球流行的网络管理软件，客户包括美国财富500强中的425家、美国十大电信公司、美国五大会计师事务所、美国军方所有部门、五角大楼、国务院以及全球数百所大学和学院，全球机构用户超过30万家。

《华尔街日报》等多家媒体报道，如果将网络间谍活动按严重性和对国家安全的影响划分1–10个等级，此次行动的等级能达到10级。

图1　攻击至少影响了七个美国联邦政府机构。

美国国家安全委员会甚至专门召开紧急会议。美国国家安全事务助理罗伯特 · 奥布莱恩则缩短了出访行程，紧急返回以协调处理“美国政府机构遭遇网络攻击”事件。

CISA 代理主管布兰登 · 威尔斯（Brandon Wales）表示：“SolarWinds 公司 Orion 网络管理产品的失陷，对联邦机构的网络安全构成不可估量的风险。”

据《纽约时报》的最新报道，攻击影响多达 250 个政府机构和企业。受害名单包括微软，思科和 VMware 等大型科技公司，以及国务院，商务部，财政部，国土安全部和美国国立卫生研究院等美国政府机构。微软则承认攻击者可能访问某些源代码。

攻击始于 1 年前

对于此次网络攻击活动，安全专家有了初步了解，但对这项攻击行动的计划和何时开始实施尚不完全了解。要弄清楚网络攻击的危害程度以及哪些数据被窃取，可能要花费数年时间。

此次攻击事件中最与众不同、且引人注目的地方是：间谍行动背后的实体能掌握众多网络权限，并在如此长的时间内保持隐蔽。

SolarWinds 攻击未利用任何被入侵用户获得最初的立足点。相反，攻击完全在后台发生。如果寻找可疑用户行为、用户设备的恶意软件下载以及异常网络活动等失陷指标 (IOC)，可能将一无所获。

实际上，只是在攻击者试图使用窃取的凭据注册新设备，以进行多因素身份验证时，火眼公司才发现了此次黑客入侵。

2020 年 12 月 13 日，火眼公司发布了关于 SolarWinds 供应链攻击的通告，网络管理软件供应商 SolarWinds Orion 软件更新包中被黑客植入后门，火眼将其命名为 SUNBURST（日爆），与其相关的攻击事件被称为 UNC2452。

SolarWinds 在随后发布的安全通告中称，受影响的产品为 2020 年 3 月至 2020 年 6 月间发布的 2019.4 到 2020.2.1 版本的 SolarWinds Orion 管理软件：“根

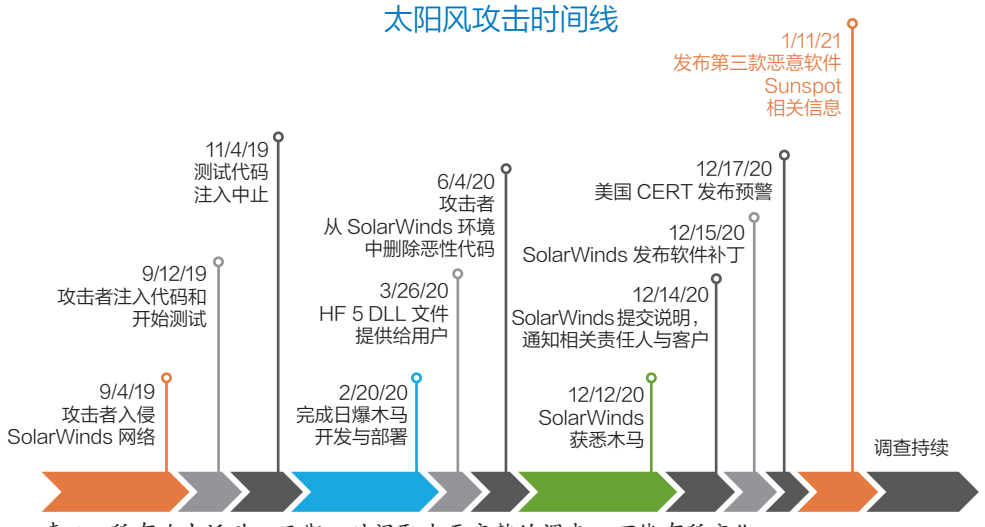


表 1　所有攻击活动、日期、时间取决于完整的调查，可能有所变化

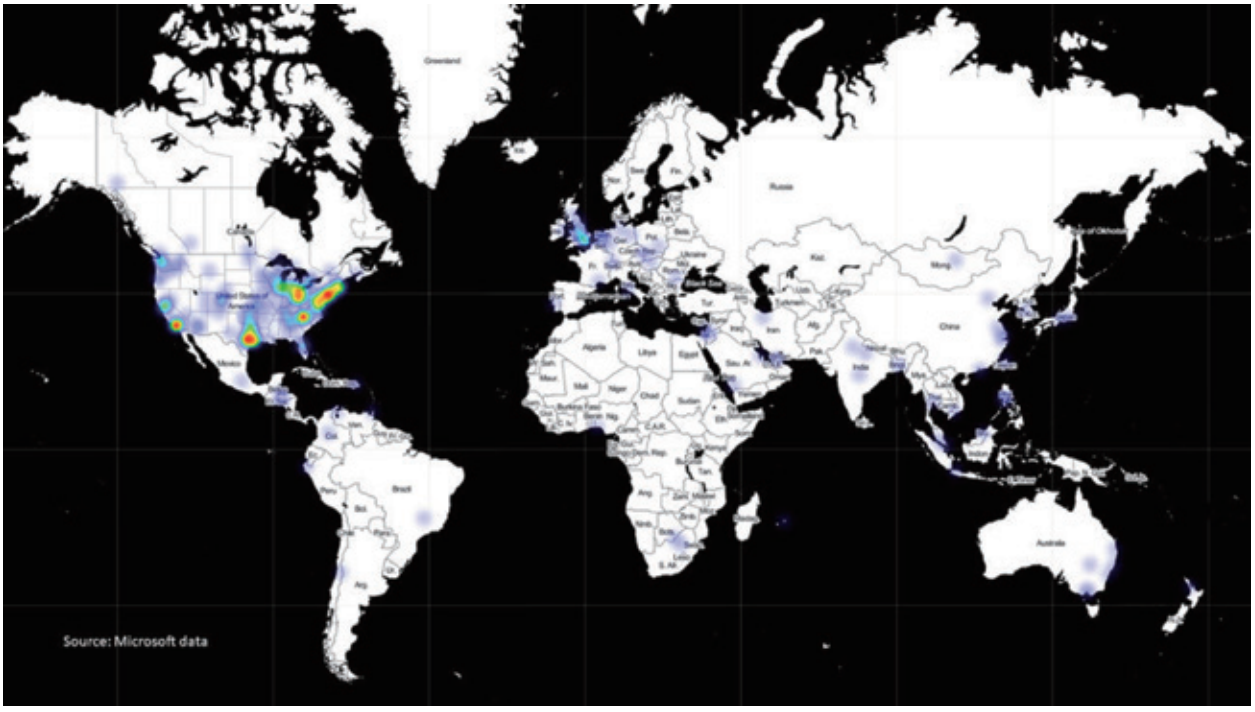


图 2　受影响系统的全球分布

据监测，今年 3 月和 6 月发布的遭污染 Orion 产品可能已被秘密地安装在大量高度复杂的、有针对性的目标中。”

通过分析相关的 DGA 数据获取的信息，奇安信 A-TEAM 认为，本次行动的供应链攻击环节由 2020 年 3 月份开始并在 7 月份达到顶峰，随后成逐渐下降的趋势并于 10 月份消失在视野之中。（DGA，即域名生成算法，是 Domain Generation Algorithm 缩写，是利用随机字符生成 C&C 域名，逃避域名黑名单检测的技术手段）。

对 SolarWinds 软件的分析显示，最早在 2019 年 10 月，攻击者就实施了代码修改，但直到 2020 年 3 月才发布了首个武器化软件更新，即被称为 SUNBURST（日爆木马）恶意软件。

Palo Alto Networks 旗下 Unit42 威胁情报团队发现，攻击者使用的的命令与控制 (C2) 服务器早在 2019 年 8 月就已建立。

SolarWinds 新任 CEO Sudhakar Ramakrishna 证实，攻击者于 2019 年 9 月 4 日首次进入了 SolarWinds 网络，8 天后注入了测试代码并对攻击进行试运行。测试代码注入于 2019 年 11 月 4 日结束，2020 年 2 月 20 日开始将恶意代码插入 Orion Platform 版本中。2020 年 6 月 4 日黑客从 SolarWinds 的环境中删除了恶意代码。

从 2020 年 6 月开始，SolarWinds 对 Orion 平台中的漏洞进行调查，并采取补救措施。但直到 12 月，SolarWinds 才发现被称为 SUNBURST 的后门木马。

根据 SolarWinds 提供的材料：大约有 18,000 个客户下载了木马化的 SolarWinds Orion 版本，但攻击者并未对所有使用者采取进一步的攻击行动，而仅选择感兴趣的目标开展后续攻击活动。

如此大体量，攻击过去 9 个月才被发现，主要原因在于，攻击者会对感染了受影响版本的受害者进行筛选，并在后续仅对特定目标进行指令下发，以便进行后续的攻击，这可以看出供应链攻击的高精度性。

奇安信 CERT 分析认为，SolarWinds 供应链攻击（金链熊）事件，是一场由专业 APT 组织进行谋划，由基础建设团队提供链路与武器，由供应链团队经过至少两年的踩点与渗透，由分析团队进行目标确认，由后渗透团队实行深入控制，通过供应链打击的实质形式，有组织、有目的、成建制进行的网络攻击行动。

攻击远比我们想象的严重

美国参议院情报委员会代理主席马可·鲁比奥（Marco Rubio,）认为，这是美国历史上遭遇的最严重的网络攻击。

奇安信CERT安全专家rem4x@A-TEAM也指出，这是一场足以影响全世界大型机构的软件供应链攻击。

SolarWinds 公司网络管理软件的全球 18000 家用户，成为全球技术供应链最脆弱的环节，波及了除俄罗斯之外的诸多国家，而且数量正在不断增加。

奇安信威胁情报中心与奇安信 CERT，通过对公开的 DGA 域名解码后发现大量中招的知名企业和机构。截至 12 月 16 日，发现至少有 200 家以上的机构被该 APT 组织采取了行动，受害者遍及北美、欧洲、亚洲和中东地区的政府、科技公司和电信公司，覆盖军工、能源等多个涉及国家安全的行业。遭到攻击的美国机构占比 62%。

美国火眼公司也证实了这一结论。该公司已在全球多个机构中检测到攻击活动：" 受害者包括北美，欧洲，亚洲和中东的政府、咨询、科技、电信和采矿业机构。

从波及范围上来看，这起网络攻击事件受害者不仅包括政府机构，也包括网络安全公司、科技企业以及非政府组织，造成的影响目前还无法估计。《纽约时报》在此后的报道称，攻击已影响多达 250 个政府机构和企业。

网络安全公司

作为美国政府的网络安全服务公司，火眼成为这起网络攻击事件中的首个曝光受害者。邮件与 Web 安全提供商 Mimecast 在 1 月份也确认遭到攻击，成为受攻击事件影响的另一家安全公司。

科技企业

贝尔金、思科、英特尔和英伟达等美国科技公司也是攻击的受害者。

微软和 VMware 也透露遭到攻击。微软承认攻击者可能访问了其某些源代码，但声称他们无法对该代码进行任何修改。VMware 在声明中说： 在公司的内部环境中发现了易受攻击的 SolarWinds Orion 软件，但调查并未发现任何被利用的迹象。

美国联邦政府机构

商务部：商务部首先确认高官邮件帐户遭入侵。

国防部：五角大楼部分机构受到攻击影响，但影响程度尚不清楚。

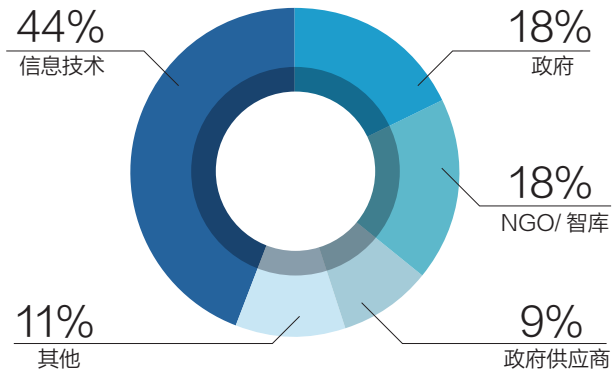
能源部：黑客进入了能源部国家核安全局的网络。

国土安全部：国土安全部官员向媒体证实，已受到攻击的影响。

表 2　SolarWinds 事件受害者行业分布

44% 的攻击目标集中在信息技术领域，包括软件公司、IT 服务和设备提供商。

针对美国政府机构的攻击主要集中在金融、国防、医疗和通信管理机构；遭到攻击的政府供应商则主要是为国防和网络安全提供支持的机构。



司法部： 司法部 于1月6日确认是攻击的受害者。3%的微软 Office 365 电子邮件帐户可能已被侵入。

国务院：《华盛顿邮报》报道说，国务院是违规行为的受害者之一。

财政部：数十个财政部邮件账户被入侵。目前还未确切知道被盗信息。

美国国立卫生研究院：《华盛顿邮报》报道说，美国国立卫生研究院被攻击所困。

奇安信 CERT 安全专家 rem4x@A-TEAM 表示，“还有多少未被发现的‘SolarWinds’，谁会是下一个被发现的‘SolarWinds’？隐藏在冰山下的APT攻击，规模究竟有多大，辐射范围有多广？”这一切问题，尚无法知晓。“唯一确定的是，APT 攻击安全威胁，比我们想象要严重的多。我们看到的远远少于所有的可能性。”

政府与企业携手应对

在攻击事件发生后，美国情报部门（FBI）、国土安全部网络安全和基础设施安全局（CISA）和国家情报总监办公室（ODNI）联合成立了网络统一协调小组，协调应对这一跨多机构的重大安全事件。

- 联邦调查局（FBI）负责调查并收集情报，确定威胁者身份，并进行追查和拦截。
- 网络安全和基础设施安全局（CISA）将向联邦、私营部门和国际合作伙伴传递技术援助和指导，旨在识别和减轻危害。
- 国家情报总监办公室（ODNI）则负责调集所有相关情报界资源，在政府内部共享。

美国国土安全部 CISA 发出紧急指令，要求政府机构检查自己的网络是否存在木马组件，并进行汇报。使用 SolarWinds 软件的民用机构被要求立即断开连接，以阻止危害蔓延，限制泄露的访问权限。

微软公司宣布，从北京时间 12 月 17 日 0 点开始，微软 Defender 软件开始阻止已知恶意 SolarWinds 安装文件。同时，据外媒 ZDNet 报道，微软已查封在本次事件中扮演核心角色域名所在的服务器。火眼、微软和注册商 GoDaddy 携手，夺取 avsvmcloud[.]com 域名，成功阻止攻击者访问一些运行 Orion 木马版的终端。奇安信 CERT 分析发现，核心域名被指向微软公司拥有的 IP 地址，根据攻击样本的预制指令，所有受害者的相关攻击活动都被即刻终止。

这些举措无疑可以能阻止危害蔓延，并限制之前由于软件更新泄露的访问权限。大西洋理事会网络治理计划主任特雷·赫尔（Trey Herr）认为，作为行动的第一步，这些举措并无不妥。各机构还应该开始检查网络日志，并请 CISO 和安全领导层共享最敏感环节的供应商产品列表。

谁是攻击的幕后黑手?

一些安全专家认为，这次攻击具有俄罗斯黑客攻击活动的特征，但尚未得到证实。

美国四大联邦机构：联邦调查局（FBI）、网络安全和基础设施安全局（CISA）、国家情报局局长办公室（ODNI）以及国家安全局（NSA）发表的联合声明称，SolarWinds 攻击“的源头很可能来自俄罗斯”。

《华盛顿邮报》报道称，此次事件的幕后攻击组织是俄罗斯对外情报局 SVR 的黑客部门——APT29（又名 The Dukes”、“Cozy Bear” 和“Cozy Duke”）。俄罗斯安全公司卡巴斯基在分析 Sunburst 后门时发现，与已知后门 Kazuar 在代码上有一定重叠之处。Kazuar 为 2017 年披露的俄罗斯 APT 组织 Turla（又名毒熊 Venomous Bear、毒蛇 Venomous Snake）所使用的的 .NET 后门程序。

奇安信 CERT 分析认为，目前还不能确定背后攻击组织，但执行该攻击行动的是一个数百人的集团化组织，并将其命名为“金链熊”。奇安信 CERT 分析发现，这

是一个数百人的集团化 APT 组织。该组织系统庞大、分工明确、纪律性强、攻击隐蔽，在执行该次任务中，至少包括三个不同职能的行动组织。

奇安信 CERT 根据他们的攻击手法、样本分析，勾画出该 APT 组织的作战路线图：“这次攻击有三个作战任务，分别由三个独立的行动组织来完成。”安

作战任务一：入侵供应商，大范围撒网

SolarWinds 软件在全球有超过 200,000 个组织中使用，客户包括美国军方的所有五个分支机构、五角大楼、国务院、司法部、美国国家航空航天局、总统执行办公室和国家安全局。

奇安信 CERT 此前分析，这次 APT 攻击首先是对 SolarWinds 旗下的 Orion 网络监控软件更新服务器进行黑客入侵，并植入恶意代码。目前被污染的 SolarWinds 软件带有该公司签名，这表明 SolarWinds 公司内部很可能已经被黑客完全控制。

作战任务二：实施供应链攻击，精准筛选重点目标

奇安信 CERT 发现，该组织具有极强的纪律性，对于攻击时机、攻击目标的选择，极富耐心，极其谨慎。

奇安信 CERT 认为，完成该目标的团队至少需要数十人。这些人员具有高超的代码仿冒能力，植入的恶意代码与 SolarWinds 产品的代码风格完全一致，完全不同于黑客所写的代码风格，从而成功绕过 SolarWinds 公司复杂的测试、交叉审核、校验等多个环节将恶意代码植入发布的软件版本之中。

恶意样本植入后，至少要通过 8 个步骤进行复杂的校验、检查工作才会正式开启供应链攻击。接下来，该组织会根据回传的受害者信息，判断是否进行下一步行动，分为终止、等待、行动三个类别，再按照不同对象，分配不同的行动团队。

执行该作战阶段的团队至少需要数十人，他们需要完成基础设施维护、攻击框架设计开发、目标甄别筛选等工作。

作战任务三：针对特定目标的渗透，完成收网

目前，根据奇安信 CERT 的统计，已经完成作战任务二的目标机构，至少有 200 多家。一旦发起第三阶段作战，就意味着他们拥有这 200 个组织的“上帝之手”……

这 200 多家受害的重点机构，覆盖了美国、加拿大、日本、比利时、荷兰、澳大利亚等，多为发达国家。在行业分布上，包括国防科技、政府、医疗服务、教育、金融、食品等关键基础商业。

奇安信 CERT 测算，针对 200 家重点机构进行定点渗透，就代表着有 200 个攻击小组。保守估计，第三阶段的作战人数可能为数百人。

供应链安全警钟再度敲响

历史上最严重的网络攻击引发对供应链安全的关注

作者 奇安信公关部 李建平

在 SolarWinds 攻击事件中，攻击组织通过在软件更新中植入木马后门，就影响到高达 18000 家政企用户，连知名网络安全厂商也被入侵。攻击者活动持续数月才被发现，大量的美国联邦政府机构成为受害者，造成的损失难以估量。

SolarWinds 攻击事件再次敲响了供应链攻击的巨大风险：安全专家多年来一直警告供应链攻击是最难防范的威胁类型，它利用了供应商和客户之间的信任关系，以及机器与机器之间的通信渠道（如软件更新机制），而渠道本身受到用户信赖。只要攻陷单单一家供应商，攻击者就可以访问这家供应商的所有客户。

供应链风险管理是一项极其复杂的工作，大多数机构都没有能力进行有效的管理。

供应链攻击成攻击重要突破口

太阳风（SolarWinds）事件可能是影响美国政府和网络安全界的轰动性网络安全事件，但不是我们见过的第一起重大供应链攻击。

2017 年爆发的 NotPetya 勒索病毒，最初是通过流行于东欧的 M.E.Doc 会计软件，发布含有后门的软件更新发起的攻击。全球 59 个国家的政府部门、医院、银行、机场，以及多家跨国公司的系统受到影响，严重扰乱了业务运营，造成超过 100 亿美元的损失。此次攻击甚至被定义为网络战的一部分。

供应链攻击已经成为黑客攻击的重要突破口。与日益猖獗的网络攻击形成对照，供应链的安全状况不佳，某些方面甚至出现恶化。在政企机构报告的直接攻击减少的同时，通过供应链发起的“间接攻击”却呈上升趋势。根据知名智库“大西洋理事会”发布的报告，2010–2020 年的 10 年间的公开报道中，具有较高影响力的软件供应链相关的攻击和泄露事件呈现逐年递增趋势。（注：2020 年尚未结束，因此并非全年数据）

从复杂性上来看，太阳风（SolarWinds）事件反映了复杂的软件供应链安全问题。相对于传统软件漏洞的攻击相比，供应链攻击将攻击面由网络边界扩大到软件自身以及内部的所有代码、模块和服务的边界，以及与这些模块相关的供应链上游供应商的开发过程，开发工具和设备的边界。

未来软件供应链攻击的数量很可能会持续增加，尤其是该类攻击的成功和影响力有目共睹。在 2017 年的 WannaCry 和 NotPetya 攻击之后，针对组织的勒索软

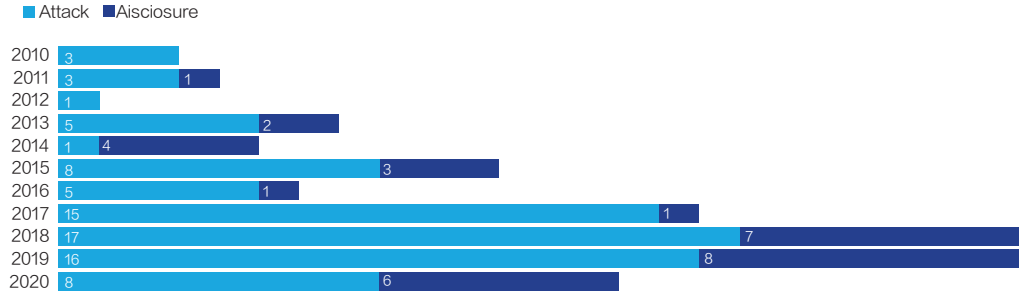


表 3　2010–2020 年软件供应链攻击和泄露事件的时序分布

件攻击数量爆炸性增长，它们向攻击者表明，企业网络并不像他们认为的那样具有抵抗此类攻击的弹性。许多网络犯罪团伙开始采用先进的技术，使他们可以与民族国家的网络间谍行为者比肩。

ICT 供应链网络安全成全球性挑战

如果说 SolarWinds、NotPetya 攻击事件，还都是集中在软件供应链方面，在新兴技术迅速推出，行业数字化和智能城市建设如火如荼之际，5G 互联设备逐步部署，云计算应用深入，整个 ICT 供应链的安全性已经成为全球性的挑战。

从手机到云存储、卫星连接，ICT 供应链涉及硬件、软件和服务的整个生命周期，以及各种第三方服务商。ICT 产品的全球流通和相互连接的特征意味着，供应链的漏洞可对多个关键基础设施领域造成巨大的损害或影响。

国土安全部网络安全和基础设施安全局（CISA）警告，ICT 的每个阶段都存在供应风险：设计，开发和生产，流通，购置和部署，维护和处置。

专家认为， 信息和通信技术（ICT）系统的运行依赖于分布在全球相互联系的供应链生态系统，包括制造商、供应商（网络供应商和软硬件供应商）、系统集成商、采购商、终端用户以及外部服务商等各类实体，产品和服务的设计、研发、生产、分配、部署和使用、以及技术、法律、政策等软环境。

信息和通信技术（ICT）供应链安全无疑是一项复杂、充满挑战的工作。信息和通信技术（ICT）供应链的设计、开发和生产、分配、获取和部署、维护以及处置阶段非常容易受到恶意或无意引入的漏洞（例如恶意软件和硬件）；假冒组件；以及不良的产品设计、制造流程和维护程序等多种因素的影响。

针对信息和通信技术（ICT）供应链的漏洞利用可能会导致：系统可靠性问题，数据窃取和操纵，恶意软件传播以及网络内部持续性的未经授权访问行为。因此，CISA 认为 ,ICT 供应链安全对于美国技术领先以及经济和国家网络安全的未来至关重要。

ICT 供应链三大网络安全风险

总的来看，ICT 供应链包括软件供应链风险、硬件供应链风险，以及第三方服务商风险等主要三大风险。

软件供应链攻击

软件供应链攻击并不是新生事物，安全专家多年来一直警告说它们是最难防范的威胁类型，因为它们利用了供应商和客户之间的信任关系，以及机器与机器之间的通信渠道（如软件更新机制），而这些渠道本身就受到用户信赖。

软件供应链攻击目前主要包括：1）通过绕过代码签名滥用用户信任；2）通过劫持软件更新破坏供应链；3）攻击开源软件在井里投毒；4）攻击应用商店进行攻击。

早在 2012 年，网络间谍恶意软件 Flame 背后的攻击者就利用针对 MD5 文件散列协议的密码学攻击，使恶意软件看起来好像是由微软合法签署，并通过 Windows 更新机制向目标分发。

软件分为开源软件和专有软件。近些年来，对开源软件的攻击越来越频繁，并且开源项目经常默默地打补丁而不通知用户，使得嵌入补丁的恶意代码在用户意识打补丁到之前依然保持攻击。

据 Sonatype 发布的《2020 年软件供应链状况》报告显示，当前超过 90% 的现代应用融入了开源组件，平均每个应用包含超过 124 个开源组件，其中 49% 的开源组件存在高危漏洞。

据 Sonatype 调查显示，通过渗透开源项目、植入被黑组件的下一代软件供应链攻击，较上一年猛增了 430%，有愈演愈烈之势。

硬件供应链攻击

SolarWinds 遭受的攻击针对软件，硬件中的供应链攻击也同样危险，同样易受高级攻击组织和国家黑客威胁的影响。攻击者可能以 ICT 物理基础设施为目标，例如制造过程中的微芯片和路由器，以安装秘密芯片或漏洞利用程序，因为它们处在供应链的下游，因为硬件已由制造商进行电子签名，很难进行检测。

在任何环境中，恶意入侵硬件堆栈（包括固件，BIOS 和 UEFI）都是巨大的威胁。但它们通常处于低优先级。当硬件被全局系统所依赖并存储敏感数据时，潜在数据泄露风险将呈指数级增长。

对硬件供应链的威胁不是理论上的。目前，供应链攻击在 IC 界受到了广泛关注，硬件木马等安全威胁日益凸显。安全专家认为，IC 供应链的所有阶段都可遭受攻击，包括 RTL 设计和片上系统（SoC）中第三方 IP（3PIPd）的集成。

在其发布信息和通信技术（ICT）供应链风险中，CISA 提到硬件设计和生产制造阶段的攻击风险。

设计阶段的攻击可能会影响组件的所有用户。网络攻击者会将漏洞集成到各种组件上，最终被安装在数百万设备中。2016 年，一家公司为美国手机制造商设计的固件，导致手机记录的文本和通话记录、电话联系信息的加密记录，被固定发送到外部服务器。

开发和生产阶段引入的漏洞，即便是设计良好的产品可能会以难以识别的方式在制造和组装过程中引入恶意组件。2012 年，一家负责为美国公司生产开关的工厂，在生产过程中安装了受感染的闪存卡。导致受感染的组件可能损害系统，并在网络中横向传播恶意软件。

最知名的硬件风险可能是两大 CPU 漏洞：Meltdown（熔断）和 Spectre（幽灵）。从个人电脑、服务器、云计算机服务器到移动端的智能手机，都受到这两组硬件漏洞的影响。

第三方服务商风险

与第三方有关的安全攻击不断增长。Gartner 2019 年的数据显示，83% 的被调查机构在进行审慎调查后发现第三方风险。

第三方服务商是那些提供支持服务，经常可以访问、共享或维护对机运营至关重要数据或设备的机构。第三方服务商范围广泛，包括数据管理公司、律师事务所、电子邮件提供商、网络托管公司、供应商、服务提供商、分包商，基本上是那些可以访问机构系统或数据的服务

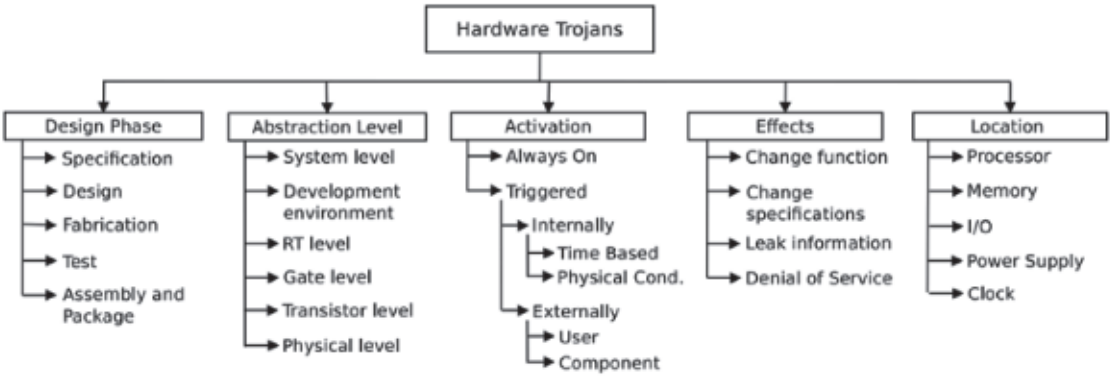


表 4　硬件木马的分类

机构。

第三方服务商造成的重大网络入侵事件层出不穷。2014 年美国百货巨头塔吉特用户信用卡数据泄漏事件，起因是由于第三方 HVAC（供热通风与空气调节）承包商对安全的疏忽。

2017 年，一份被称为“天堂文件”(Paradise Papers) 的财务报告被曝光，泄露了超过 1300 万份详细记录大型企业、政界人士和名人离岸避税行为的文件。其泄露源头正如“巴拿马文件”（Panama Papers）事件，是一家律师事务所。

根据波耐蒙研究所（Ponemon Institute）在 2018 年秋季进行的一项调查，56% 的组织机构遭遇过由某个供应商造成的网络入侵。同时，每个组织机构中，能够接访问敏感信息的第三方服务商平均数量由 378 增加到了 471。

供应链攻击应对建议

如前所述，供应链风险管理是一项极其复杂的工作，大多数机构都没有能力进行有效的管理。那政企机构真的无能为力，被动挨打吗?

由于 ICT 供应链涉及环节广泛，仅仅靠企业本身很难对每个环节进行审查，实现安全的保障。美国已将 ICT 供应链安全置于国家安全战略层面来考虑，提升 ICT 供应链安全管理的地位。

2012 年，美国土安全部发布首份国家层级的战略报告《全球供应链安全国家战略》。此后，各相关机构出台一系列文件，如国家标准和技术研究院（NIST）的《联邦信息系统与机构供应链风险管理实践》（2013）、国土安全部的“供应链风险管理计划”（2017）、白宫的《联邦信息技术供应链风险管理改进法案》（2018）。2019 年 5 月，特朗普签署《确保信息通信技术与服务供应链安全》行政令，禁止交易、使用可能对美国构成特殊威胁的外国信息技术和服务。

前 CISA 负责人 Chris Krebs 近期表示，供应链风险管理一直是 CISA 关注的重点。2018 年 CISA 牵头成立了供应链风险管理工作组，包括 20 家 IT 公司、20 家通信公司和 20 家联邦机构。不久前，CISA 发布了 ICT 供应链风险管理工作组第二个年度报告，对加强 ICT 供应链管理提出了多项建议。

2020 年 4 月 27 日，国家网信办等 12 个部门联合发布了《网络安全审查办法》，要求关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查。但目前 ICT 供应链安全相关配套标准仍需完善，管控能力有待提升。

从国家层面，应该从三大方面着手，推动建立 ICT 供应链安全管理制度和体系。

1、建立 ICT 供应链安全管理制度与标准

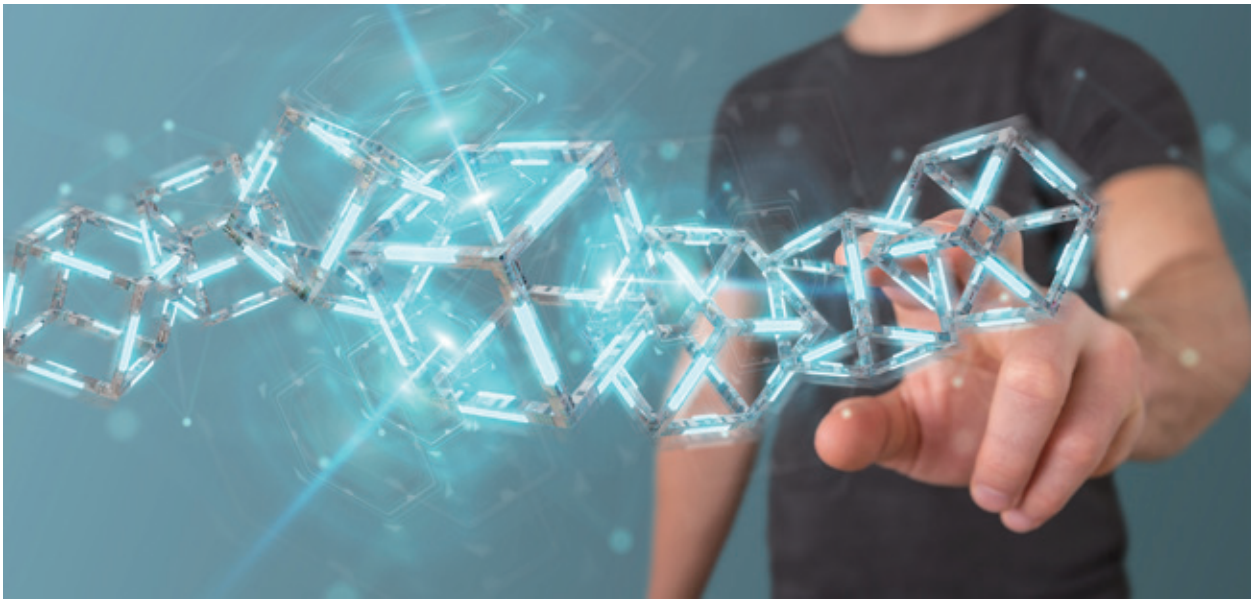
强化供应链安全管理，要制定相关政策法规，提升供应链安全管理的战略地位；同时建立健全 ICT 供应链安全管理的相关制度和标准。引导全产业关注供应链安全。

2、完善 ICT 供应链管理与评估体系

ICT 供应链中最有价值的风险信息往往是由企业（而不是政府）首先发现的，加强政府与企业之间的风险信息共享十分必要。安全评估是网络安全保障的重要组成部分，是网络安全防御的前提和基础条件。可以确定 ICT 供应链中存在的安全隐患，提供切实可行的安全增强措施，从而确保 ICT 供应链的安全性。

3、提升 ICT 供应链安全基线。

提高 ICT 供应链安全标准成为趋势。美国国防部认为，NIST 等网络安全控制类标准不能满足网络防御要求，要求供应商须符合 2020 年发布的网络安全成熟度模型认证 (CMMC) 框架，将信息数据安全的要求提到最重要的维度。



对企业机构来说，应该从三大方面着手，降低 ICT 供应链攻击的风险。

1、制定更强大的安全策略

提升供应链安全需要在各个层面上进行。确保供应链成为机构威胁模型的一部分。对与供应链相关的风险有很好的了解，可能会改善业务相关风险。如果没有将 ICT 供应链安全要求纳入合同，就缺乏基本机制来确保供应商（及其上游供应商）能够充分应对与 ICT 产品和服务相关的风险。

2、加强代码审计与安全检查

政企机构可以向供应商索要“材料清单”，列出该供应商使用的所有代码组件，以识别与开源组件漏洞有关的潜在漏洞。高风险厌恶机构可以考虑在实施代码之前审核代码。

例如，SolarWinds 新任 CEO 就决定，增加额外的代码自动化和手工检查，确保编译后的发布版本与公司源码匹配。同时，利用第三方工具对其软件及相关产品源代码进行详细安全分析。

针对硬件风险，除了采用分体制造和和逻辑障碍，加强硬件木马检测也是安全专家的重要建议。

3、推动建立零信任等安全防护机制

供应链攻击暴露出 IT 网络安全架构的最大缺陷：就是信任。不是信任不够，而是过于信任。零信任架构意味每个试图访问网络资源的人都需要进行验证。不仅将零信任网络原则和基于角色的访问控制应用于用户，还应当应用于应用和服务器。安全专家认为，作为一系列解决方案的集合，零信任可以防止第三方供应商工具获得不必要的特权，能够削弱恶意软件的传播能力。

SolarWinds 攻击的巨大成功，无疑会推动攻击组织更多采用。2021 年可能会出现更多供应链攻击事件，显然任何机构都无法忽视它的发展。安

奇安信
新一代网络安全领军者

补天漏洞响应平台

工业和信息化部网络安全技术应用试点示范项目

补天众测

网络安全漏洞领域唯一以安全厂商身份入选

企业商务合作请扫我

精英白帽子报名请扫我

官网：https://zhongce.butian.net　　邮箱：g-butian-deliver@qianxin.com　　公众号：补天漏洞响应平台

奇安信
新一代网络安全领军者

云安全管理平台

云安全的智慧大脑

运用软件定义安全的设计思路，将云的属性赋能给安全体系

在公共服务云安全建设中，协助云服务商搭建可按需交付、分权管理和业务增值的云安全资源池。在行业私有云安全建设中，使安全具备敏捷上线、集约化部署和易于统一监管的能力。云安全管理平台为各行业客户提供安全产品服务化、安全能力一体化、安全运营自动化 三大核心价值，为云保驾护航。

“一条 IOC”的 APT 阻击

作者 奇安信公关部 魏开元

蔓灵花（BITTER），国外著名 APT 组织，因该组织常用的特种木马数据包头部为“BITTER”而得名，近一两年持续针对我国重点行业单位进行钓鱼攻击，其中攻击方式较多样，横跨 PC 端到移动端，通常采取的手段为钓鱼邮件攻击，其中邮件中搭载的可能是钓鱼网站，也可能是恶意附件。

在疫情爆发以来，蔓灵花组织从 2020 年初就开始制作防疫诱饵，攻防双方的战斗仍在继续。

一次告警，蔓灵花组织漏出了狐狸尾巴

2020 年 10 月的某天深夜，一台办公电脑收到了一封合作公司发来的业务邮件。

“合同终于发过来了。”大李端起咖啡杯轻抿了一口，兴奋地说。为了这一次合作，大李一个月来都没怎么好好休息过。

就在大李打开附件后不久，电脑上安装的奇安信天擎终端安全管理系统弹出了一个窗口，疑似发现木马文件。

“中病毒了？不能啊，我也没干啥啊，难道是？”想到这里，大李不寒而栗，迅速关上电脑并将网线拔掉，拨通了公司网络安全负责人老 K 的电话。

“嗯，我知道了。”老 K 甚至来不及洗把脸，往公司飞奔而去。盯着天擎管理后台的告警记录，老 K 心里咒骂着，稍有平复，拨通了 4009-727-120。窗外，夜

已深了。

“喂，您好！这里是奇安信应急响应中心……”

恰在此时，南亚地区 APT 组织蔓灵花的总部也“热闹非凡”。

“拿下多少台终端了？”一个中年男人从里屋走出来说。

“还没。这轮攻击刚开始，钓鱼邮件发出去没多久，估计还需要一段时间。”

“嗯，注意盯着点，我估摸着鱼饵很快就能看到效果。”中年男人看了一眼旁边的机房，“这一次，绝对能挖到一些我们意想不到的东西。”

“放心吧，这几年哪次不是手到擒来。来了，C2（命令与控制，Command And Control）服务器后台有反应了……”

还原作案现场，蓄谋已久的社会工程学攻击

“嚯！这蔓灵花组织又来了。”收到客户求助电话后，奇安信第一时间启动了应急响应程序，威胁情报中心随即针对样本和攻击手法展开了溯源分析工作，最终锁定了蔓灵花 APT 组织。

自 2016 年首次披露以来，奇安信威胁情报中心与蔓灵花组织已经较量了多达数十次。

“从这几年和蔓灵花交手的经验来看，我们发现了他们攻击手法的几个特点。”奇安信威胁情报中心负责人 Star 称。

第一类是以发送伪装成目标单位邮箱登录界面的钓鱼网站为主，通过钓鱼网站控制目标用户的邮箱账户，从而窃取敏感信息。

第二类主要是发送带毒附件，释放专用下载器下载其特种木马。蔓灵花组织会利用自有的 C2 服务器，远程控制木马完成敏感信息窃取任务，并回传至自有的服务器中。

为了提升目标的中招几率，蔓灵花组织非常善于伪装。他们会把诱饵加上一个当前热点事件的“外壳”，从而吸引目标的注意力。正如本文开头所说，在今年疫情爆发后，蔓灵花组织就多次利用疫情热点话题，向攻击目标发送钓鱼邮件，直到现在依然没有停止。

后来，业界习惯把这种利用人性好奇或者其他弱点的攻击方式，叫做社会工程学攻击。这和某些新型毒品伪装成跳跳糖、邮票、奶茶等形象，从而诱骗不知情人士染上毒瘾的原理，非常相似。

收集证据链，威胁情报的进击

“第一次面对 APT 攻击的时候，真的很难。”Star 笑着说，“你的对手完全是陌生的，你不知道他使用的攻击手法、恶意样本、基础设施资源的情况，甚至你不能判断这个行为是否合法。”

这就像一名拳击手站在擂台上面对一个完全陌生的对手，你不知道对方的力量到底多大、速度多快，也不知道对方习惯使用上勾拳还是下勾拳。

一切都得从 0 开始。

时间拉回到蔓灵花组织首次被披露的 2016 年，威胁情报方兴未艾，这为高级威胁检测提供了一种全新的思路。

“每一个 APT 组织都有自己的招牌，也可以称之为

仪式感。比如蔓灵花组织使用的特种木马，它的数据包头部就有‘BITTER’字样。”

看过武侠剧的朋友也都知道，很多高手都有自己的仪式，比如《神探狄仁杰》中的杀手蝮蛇会在杀人后留下一方绣有蝮蛇的手帕。

威胁情报分析师就是要从海量数据中，找到这些显著特征，为攻击检测和后续的溯源分析提供有力证据。

基于这些特征，一条条 IOC（全称为失陷检测情报，是威胁情报的一种）便被生产出来了。通俗理解，IOC 就是攻击者所使用工具的‘招牌’，包括攻击者使用的恶意文件签名、恶意 IP 地址以及服务器域名等等。

失陷检测情报就是用来检测已经失陷（被入侵）终端和服务器的。

举个例子，当通过 IOC 与异常流量进行匹配，防火墙发现公司内网的一台电脑正在尝试与蔓灵花组织经常使用的 C2 域名连接，那么这台电脑就很可能已经感染蔓灵花组织植入的木马了，安全人员就可以及时设置，让防火墙阻断所有非法连接。就像在古龙的武侠小说里，六扇门的捕头发现有人被灵犀一指杀死了，马上就能想到这很有可能是陆小凤干的。

时至今日，IOC 的应用已经非常广泛。SANS 历年的威胁情报调研报告都显示，最受欢迎、应用最多的威胁情报类型始终是 IOC；在卡巴斯基发布的应急响应手册里，IOC 的匹配是触发应急响应流程的最主要入口。

但 IOC 的生产绝非一日之功。就像你了解一个人一样，必须要常年累月的与其接触。

经过长时间对蔓灵花组织的追踪，奇安信威胁情报中心掌握了大量有关蔓灵花组织的 IOC，例如蔓灵花组织所使用的键盘记录器、文件上传、远程控制等插件的 MD5 值（通俗理解为文件信息经过加密算法得到的一串十六进制字符，可认为具有唯一性），域名为 162.0.229.203 的 C2 服务器等等信息，一旦安全设备检测到了与 IOC 匹配的异常信息，则基本可以判定受到了蔓灵花组织的攻击，并及时阻断非法通信和删除病毒文件。

后续更深入的关联分析，就可以交给专业的威胁情报分析师来处理了。

收网！ QOWL 反病毒引擎“一锤定音”

为了帮助防守方快速分析攻击者所使用的攻击手法，美国研究机构 MITRE 于 2014 年推出了 ATT&CK 框架。通俗理解 ATT&CK 框架是一个不断完善的知识库，能够将已知攻击者的攻击手段、木马类型、破坏行为等总结成一个列表，用于全面呈现攻击者的技战术水平，从而给防御措施提供依据。

听起来十分有用，只要这个知识库足够丰富，遇到攻击只要往里面套就没错了。但 Star 却“泼了一盆冷水”。

“理论上是这样没错，但在实际的 APT 分析过程中，价值不大，因为现有的 ATT&CK 框架只能让你了解大致上的攻击手法和过程，并不能作为判断攻击来源的依据。APT 分析的核心在于能够看见的细节，我称之为‘元数据为王’。”

所谓元数据可以简单理解为强特征。举个例子，说一个人两米二六你能想到谁？我想所有人都会异口同声的回答：姚明。因为放眼全世界，大家所熟知的也就只有姚明是两米二六。所以，两米二六就是姚明的强特征。但如果你说一个中国篮球队员长的非常高，这恐怕得在中国篮球队所有的中锋里，慢慢挑了。

APT 分析也是如此。比如蔓灵花组织，他们所使用的 C2 服务器就是 162.0.229.203，发现这个域名再结合其他关联信息，基本就能判断出就是蔓灵花组织所发起的攻击。

不过，元数据的获取并不容易，需要专业的分析师，利用专业的工具，对攻击行为、攻击样本开展深度分析。

针对网络流量的分析和元数据提取，当时业界有不少专业的产品，比如奇安信天眼新一代威胁感知系统、科莱的全流量分析系统等等。但受限于传统反病毒引擎对可疑文件的解析能力不足，往往难以做到细粒度精确度高的查杀和追踪。这也是所有安全厂商在防御 APT 攻击时所面临的难点。

“既然现在没有合适的反病毒引擎，我们干嘛不研发一款呢？”Star 琢磨着。

于是，QOWL 反病毒引擎应运而生，这个 APT 狩猎的独门绝技，为文件元数据提取、APT 样本挖掘及检测，立下了汗马功劳。

在此次攻击活动中，蔓灵花组织依旧使用了其常用的攻击手法，企图释放执行其常用的下载者进行恶意软件部署，威胁情报分析师生产的 IOC，结合 QOWL 反病毒引擎的深度检测分析，蔓灵花组织这次失算了。

这个世界上，每天都有数以万计的“IOC”被生产出来。“把它用在最合适的地方，就是 APT 阻击战的战士。”Star 说。安

内生安全护航“智慧大理” 打造数字时代的城市名片

作者 奇安信公关部 张少波
奇安信营销九群云南分区 方楚臣

“网络安全不受重视、没地位。”“安全建设不成体系，零敲碎打、缺乏管控。”“在信息化总盘子里占比太小，预算少的可怜。”“运维时安全人手严重不足，疲于奔命”……

在很多信息化建设中，网络安全负责人经常要面对缺地位、缺方法、缺钱、缺人手的“四缺”矛盾。这些问题解决不好，其引发的安全风险，就会成为悬在信息化头上的达摩克利斯之剑。

2020 年 7 月，奇安信中标“智慧大理”云计算中心安全加固采购项目。该项目的意义，不仅在于涵盖了态势感知与安全运营（NGSOC）、云安全管理平台、上网行为管理、下一代防火墙、终端安全响应系统（EDR）等多达 12 款产品，更在于它颠覆了过去“事后补救”的局部整改建设模式，转变为“事前防控”型建设思路。尤其是通过基于内生安全框架的四大工程两大任务（4+2 模块），将安全能力内置到业务系统当中，解决了“四缺”难题，使之成为内生安全框架落地的一个标杆典范。

“智慧大理”：数字时代的城市名片

苍山之麓，洱海之滨！大理，这座因金庸武侠而家喻户晓的城市，如今不仅成为网红打卡的旅游胜地，更被评为中国首批十大魅力城市之首。

在当今数字化转型、智慧城市建设的浪潮之下，大

理再次走到时代的前列。早在2013年10月，“智慧大理”项目正式启动，并成功申报为“国家智慧城市试点”和“国家信息消费城市试点” 。在2017年亚太智慧城市发展高峰论坛评选中，大理荣获“中国智慧城市创新奖”。

经过多年来的积极实践与探索，“智慧大理”取得显著的成效，其建设涵盖了平安大理、智慧社区、智慧旅游、智慧城管、智慧教育、智慧交通、智慧环保、智慧医疗等项目。真正将大理建设成了百姓生活幸福、环境优美和谐、适宜投资居住、城市管理睿智的国际化旅游城市，成为数字时代最亮丽的城市名片。

据“智慧大理”承办方和运营方大理市信息化发展有限责任公司负责人表示，目前项目在多个方面取得丰硕成果。例如通过建立云计算中心，避免了重复建设各类小机房，大量节约各部门的信息化建设、运维成本。而依托云计算中心建成全市统一的视频监控云平台，显著提升城市管理能力。将全市各部门分散、独立、零乱的信息资源进行整合，形成统一的政务信息资源库和应用服务平台，实现信息资源高度共享和深入应用。

在服务社会方面，“智慧大理”更是做到了便民、惠民、利民。带上一张市民卡，就能完成金融支付、公交乘车、占道停车缴费、食堂、医院就诊、新农合、图书馆、门禁、公共事业缴费、旅游年卡、出租房门禁管理、校讯通等各种应用。“到家边的乡镇卫生院就诊，就能享受市级医院待遇，省时又高效。”

此外，投资1.1亿建成的大理洱海流域生态环境智慧监管系统，更为科学治理洱海、保护洱海提供保障。智慧旅游可以一站式了解大理景区、旅游路线、度假等信息，一个手机玩遍大理。

高度重视安全风险 确立责任“一把手”制

近年来，国内外网络安全形势愈发恶劣，境内外攻击者及黑客组织对我国重要信息系统的攻击渗透更加频繁，智慧城市体系作为城市运转的核心，其重要基础网络、信息系统的网络安全防护成为重中之重。尤其“智慧大理”是一个集成了金融、民生、医疗、交通等领域协同合作、关键业务高度互联的融合平台，一旦遭到网络攻击，极有可能对城市运转形成严重影响。为此，客户上上下下都对网络安全给予极高的重视。

作为“智慧大理”的承办方和运维方，大理市信息化发展有限责任公司负责人表示，“等保2.0从国家标准层面为网络安全提供了指导作用和推动作用。但对于‘智慧大理’而言，网络安全不仅要符合合规需求，更要和信息化、业务系统实现深度融合，满足现在和未来业务升级的安全需求。因此，我们在选择合作伙伴时，不仅要方案符合等保要求，更需要从信息化角度明确目标，从顶层设计、全局规划等方面，建立适应业务发展的安全防护体系。”

尽管存在着资金紧张、缺人手等困难，但从业务建设之初，大理市委、市政府，以及承办方大理信息化发展有限公司，从上到下非常重视网络安全，确定了安全责任一把手制度，响应总书记“安全是发展的前提”的要求，配好刹车再上路，将安全放在最优先的地位。

落实内生安全框架 将安全能力“理清楚”、“建起来”

“智慧大理”对于网络安全建设的思考和需求，是全国各个信息化项目的缩影。作为国内网络安全的领军企业，奇安信很早就意识到，要改变困扰网络安全“四缺”的问题，就需要破旧立新，将安全建设模式从“局部整改外挂式”走向“深度融合体系化”，在数字化环境内部建立无处不在的网络安全“免疫力”，实现内生安全。

从2019年开始，奇安信专门成立了工作组，与20多个一线部门紧密协同，用系统工程的思想，构建了一个能够适应形势变化的网络安全框架，来支撑内生安全体系建设。2020年3月，面向新基建的内生安全框架正

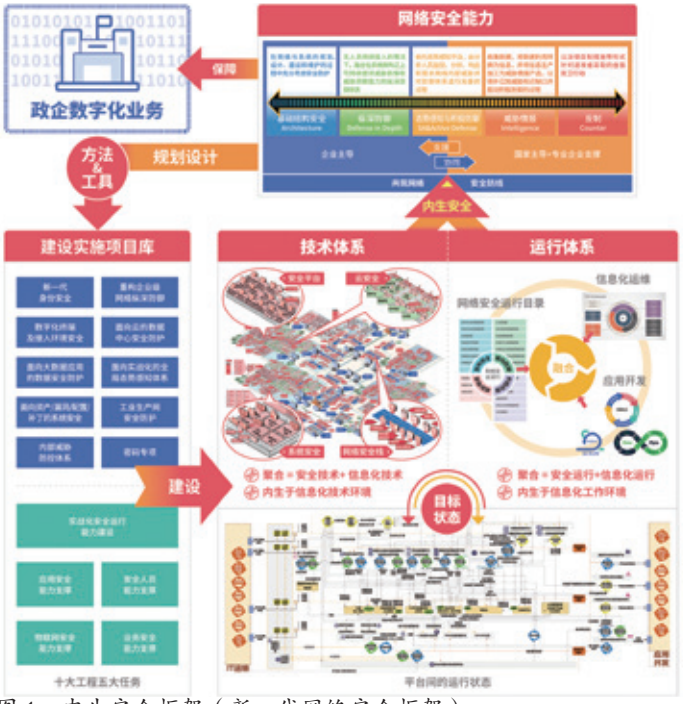


图 1：内生安全框架（新一代网络安全框架）

式推出，与此同时，基于该框架的“十工五任”手册也正式出炉。

2020 年 4 月，奇安信助理总裁陈明、奇安信云南省技术总监方楚臣以及销售经理李扬、安全顾问鲁成等一行团队向“智慧大理”的领导进行了方案汇报。通过“十工五任”手册的介绍，包括内生安全框架具备的“1+1>2”的涌现效应，让众人耳目一新，特别是面向新基建，面向十四五规划，非常符合“智慧大理”网络安全建设的定位和目标。

双方一致认为，“智慧大理”的信息化与网络安全极其重要与复杂，必须以顶层设计思想、结构化的思维、体系化的方法才能做到“化繁为简”。为此，奇安信结合“智慧大理”的现状和需求，创新提出了四大工程两大任务的内生安全框架，即 4+2 模块。其中四个工程包括：面向网络安全架构的纵深防御体系、面向云的数据中心安全防护、面向实战化的全局态势感知体系、面向大数据应用的数据安全防护；二大任务包括：实战化安全运行能力建设、安全人员能力支撑。

一直困扰“智慧大理”的是安全预算与安全人员投入不足，而 4+2 模块的内生安全框架是在大理十四五与新基建这个契机上指导“智慧大理”的规划工作，帮助“智慧大理”明确目标、方向和任务，使后期项目建设有足够的资源和政策推动力。

内生安全框架能在“智慧大理”顺利落地，陈明归纳了五个核心要素。

一是模式的转变，网络安全应避免“以偏概全”的传统模式，转而以全覆盖、层次化思路进行规划设计。

二是体系化规划、设计和建设，需要以系统工程方法论来指导网络安全体系的规划、设计和建设工作。

三是叠加演进提升，以围绕网络的纵深防御体系为基础，进一步围绕数据确定防御重点。

四是实战化的运行，通过将人防和技防相融合，围绕人员开展面向实战的安全运行，持续运行保障业务。

最后是打破“紧平衡”，规划出预置的可扩展的能力，预留出必要的应急资源，应对重大不确定性风险。

构筑安全管理新格局 助力“智慧大理”“跑得赢”

奇安信云南省技术总监方楚臣表示：实践是检验真理的唯一标准。安全系统建起来之后，接下来最重要的就是要“跑得赢”。在“智慧大理”项目中，4+2 模块的内生安全框架在管理和运营方面的优势，体现的淋漓尽致。

首先是安全产品服务化，让“智慧大理”实现合规和高效两者兼得。项目方通过 SecFV 安全功能虚拟化，

提供丰富的安全防护手段，让客户无需担忧上云安全问题。同时从东西向、南北向、主机层、应用层等全方位进行新等保技术对标，形成全面安全防护能力，并保障安全合规。

其次是安全能力一体化，推动“智慧大理”真正实现智慧易管。通过 SDS 软件定义安全，为客户打造可编排、易管理的云安全管理平台。让客户通过云安全态势感知、天眼联动等监测手段，让云安全防护更及时、高效。依托集中管理多个分布式部署的安全资源池，让多云融合场景下的安全防护无忧。

最后是实现了安全运营自动化，帮助客户实现增值共赢。通过 BPM 业务流程管理实现自服务、订单审批、计量计费等，将安全资源服务化，为云服务商提供业务增值，从而构建安全生态合作，为“智慧大理”提供开放的、丰富的、可持续输出的安全能力。

在整个项目中，奇安信的顶层设计、框架落地和全产品线优势得到充分体现。例如云安全管理平台结合了奇安信领先的云端防护能力和大数据未知威胁检测能力，从而构建一套真正属于“智慧大理”的安全防护框架。而先进的信息安全防御体系下可以构建“智慧大理”态势感知与保障平台，如新一代检测技术、云计算安全技术、大数据安全分析技术等。在安全能力一体化方面，通过云安全态势感知、天眼、天擎联动等监测手段，让云安全防护更及时、高效。

“如此复杂的产品线，快速整合实施的难度无疑是超出想象的。” 奇安信助理总裁陈明感叹道。“得益于公司大规模的设备生产供货能力，以及覆盖全国各省、自治区、直辖市的备品备件保障，强大的项目实施队伍，完善的项目实施计划，丰富实施经验的队伍，确保了庞大复杂的产品线，得到很好的整合和落地。”

未来，“智慧大理”规划建设还将全面落地“十工五任”中的其他项目，包括新一代身份安全、终端及接入环境安全、数据安全防护、内部威胁安全管控等等，让“智慧大理”真正具备内生安全的能力，成为数字时代古城大理的一张时尚城市名片！（本文首发于中国新闻网）安

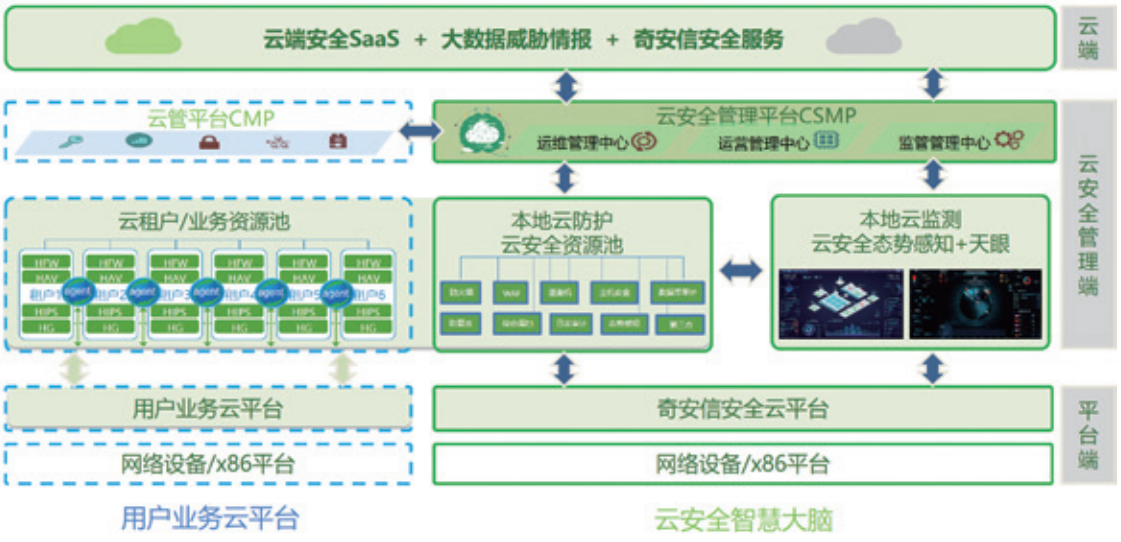


图 2：云安全管理平台产品架构图

前方到站奇安信

作者 奇安信公关部 孙丽芳

2020 年 12 月 28 日早上 9 点，北京地铁四号线动物园站正是繁忙。C 出站口走出不少双肩电脑包、仔裤、球鞋，IT 人打扮的年轻人。华北电力大学计算机专业 2020 届硕士毕业生董玲是其中一员。

“来这么多年轻人好像是三四月开始的”地铁引导员李阿姨对此还有些印象。“以前少，以前在这站下的，很多都是家长带着孩子去逛动物园的，要么就是去周边市场买衣服的”。直接带来这个变化的是地铁口 200 米外，奇安信西直门安全中心 2020 年的启用。它由原万容天地市场升级改造而成，一亮相，就成为从前的“动批”区域，如今的国家级金融科技创新示范区新地标，也把附近变成了继中关村、后厂村、望京之后，北京又一处 IT 人的聚集地。董玲正是在这个时候入职奇安信。

选对行业更要选对企业

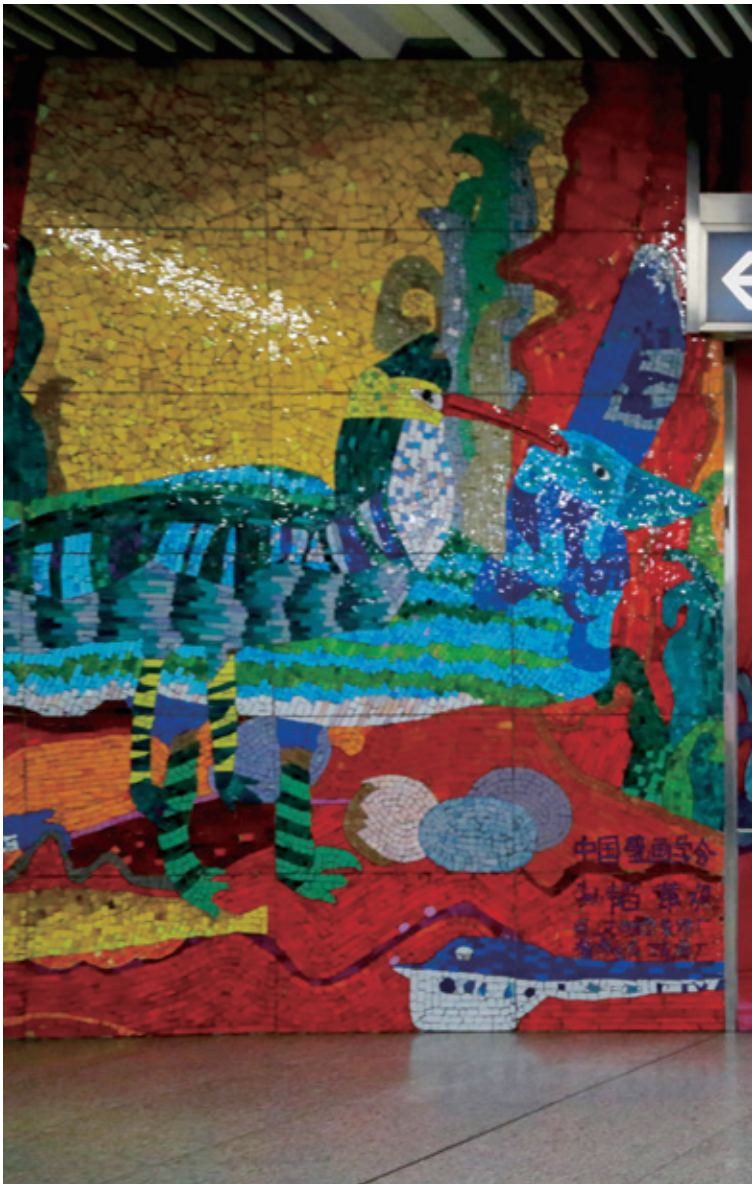
“这也是我 2020 年最大的收获。”

事实上，董玲的同班同学大都把进入电力系统的研究机构作为首选。“那就有点像考公务员，比较稳定，但是我更想去企业，企业要不断适应市场的需求，技术的更新会更快”。对新技术充满渴求的董玲没有参加电力系统的考试，一心想进入企业。工作找得也很顺利，2019 年 9 月，还在校就读的董玲就和一家在京企业签约了，但是 10 月又接到了奇安信的面试通知。

“我是学计算机的，除了找份工作，更想选一个应用方向长期发展。网络安全不是最热门的方向，但我觉得随着互联网对传统行业的改造深入，人们对网络的依赖程度越来越高，网络安全未来肯定也就越来越重要。当然，当时我对网络安全的理解还很有限，但是我知道，这个领域里奇安信是最领先的”。

虽然橄榄枝伸得稍晚，面对自己最心仪的网络安全公司，董玲还是非常用心地准备着，最终收到了 OFFER。“很开心，算是梦想成真了。但顾虑还是有的，因为当时我已经和另一家公司签约了，如果解约要支付不菲的违约金”。

董玲担心的违约金问题，后来在奇安信校招组的全力协助下，得到了圆满解决。2020 年 7 月，走出校门的董玲正式成为奇安信应用技术研发一中心的一员，所在的小组主要支持公司的云安全产线。这是一条非常重要的产线，随着政企单位的数字化进程，各种服务上云或者云化已成为趋势。



用内部 GPS 导航系统不走弯路

现代化的办公场地、便捷的上下班通勤，奇安信优越的硬环境显而易见，但公司良好的软环境让董玲感受更深。扬帆训练营的开展使董玲快速了解了公司文化，一对一导师制则让董玲拥有了奇安信内部“GPS 导航仪”。导师由本部门资深业务专家担任，全程负责校招生培养期的职业发展，帮助校招生快速了解业务内容，适应工作平台，完成自我定位，全身心地投入到工作中。

“我的导师是冯鹏，大家都喊他大师，因为他的技术水平很牛。在他的指导下，我学到了很多。我经常提交 Merge Request（合并请求），等待着大师合并。尽管很忙，但是每次他都会认真审查代码，并对相应问题提出修改意见，包括命名不规范、方法可合并等很多细节问题。大师严谨的工作态度，督促我在未来的开发中注重细节、遵守代码规范。”

“如果没有导师制，我即使有心指导，责任感也不会太强。现在因为有师徒关系，我会着重地给徒弟多一

些业务指导。而且，说实话，在带徒弟过程中，业务上自己会自觉地高标准要求自己。这种“绑定”会让师徒在教学相长中互相促进。”导师冯鹏觉得自己也很有收获。

有了内部“GPS”，董玲没有走弯路，有了更多时间“练内功”。“第一份工作，不排除有的人可能有跳板心理，但更多人非常重视走出的这职场第一步。比起薪资或者工作舒适度，他们更看重自己的成长，看重未来。”校招组的范馨觉得这个群体的共性明显。

“来了之后我发现，网络安全和我之前理解的有所不同，我学到了很多从未见过的东西，而且是成体系的学习”。和所有研发线的校招生一样，部门和董玲一起，制作了详细的中期学习计划，学习内容从前端研发基础，包括 JavaScript、CSS 等到独立听需求，进而可以独立承担项目研发等。

得益于这些为校招生量身订造的机制，董玲顺利完成了从学生向职场人的转换，逐步能根据指导完成项目中的工作，先后参与了蜜罐、虚拟化重构部分模块、CSC、Luban 等项目。

“董玲的基础很好，进步也非常明显。 在 Luban 项目的开发中，产品概念有些抽象。每每多理解了一些产品或得到了反馈，她都能回顾之前的实现并加以更正或改进。不满足于实现功能，有意愿且有行动地往更好的方向发展，这是难能可贵的”。导师冯鹏对自己的这个徒弟非常认可。

每一行代码都关系客户的满意度

7 月 22 日，奇安信成功登陆科创板。早上 8 点，董玲在地铁里通过手机观看了上市仪式直播。“觉得非常骄傲，这是公司发展很重要的一个里程碑，我很希望公司未来的发展里有我的努力”。

经过几次项目历练，迅速成长的董玲，愿望很快变成了现实。2020 年 11 月初，董玲开始独立负责云网安全分析系统的新一轮迭代。云网安全分析系统是云安全管理平台创新组件，提供混合云场景下的云网全流量采集分发及轻量级的流可视化解决方案。本轮迭代是继续

增强系统采分功能运行时的各项指标监控，通过引入可视化的监控面板，帮助客户快速及时定位问题。同时，优化策略模块，从前端入手进一步简化配置逻辑及展现组织形式，降低上手难度，提升客户体验。“总的来说，就是要让这个系统更聪明、更简洁、更好用”。

加班明显多了起来，不过董玲觉得很充实。“大家普遍认为 90 后比较自我，责任心差，服务意识差。但是在工作中我真正体会到了当责奋斗、客户优先的意义。这八个字很平常，却绝不简单。最初我只是参与项目，做完了手头工作就提交，下班回家，现在我会反复确认研发过程中的每一个功能点，尽量通过更多的测试用例自测出相应的问题，降低 bug 率。除此之外，我会时常翻看自己的代码，发现之前代码中的不足，从而进行优化，提升代码质量。我是程序员，但我不仅是简单面对代码，我还是一个重要的节点，要对过程负责，也要对结果负责。每一行代码都可能关系到客户的最终体验，我多想一步，多做一步，客户就能多一分满意。”目前，云网安全分析系统的本轮迭代基础研发工作已经结束，进入测试阶段。

“我最喜欢的就是公司浓厚的技术氛围，让我这种研发小白也有独立上手的机会，而且研发的成果将直接面对客户，这是最好的学以致用”。从研发小白到独立负责项目，2020 届校招生董玲的成长并不是个案。2016 届校招生马培月已成长为重庆区域负责人和汽车行业部负责人；2018 届校招生霍东焱因技术水平过硬，入选天眼团队出征阿曼的队伍；2018 届校招生孙健因工作业绩突出，受邀参加了公司上市仪式分会场仪式；2020 届校招生曾丽阁迅速融入公司，担任了部门年会主持人，还获得公司校招答辩 TOP 1。

后生可畏亦可爱。2020 年年末，奇安信 2021 届校招生收到了来自公司的惊喜礼盒。之所以称为惊喜，是因为校招组以发放 " 入职材料 " 为由收集了所有同学的地址，礼物也是量身定制。礼盒盒面印有每位同学的名字和专属祝福，盒内装有专属工卡、奇安信定制款鼠标和

随机一款冬奥吉祥物。这份用心在这个格外寒冷的冬天尤其温暖，同学们纷纷在校招群里晒出自己的专属礼盒，分享自己的个性祝福语。很多同学还守在跨年的零点零分发出了 2021 年第一条朋友圈，送给了他们昵称为“虎厂”的奇安信。红红火火的好不热闹！

作为职场新人，校招生距离取得骄人的工作成绩也许还有一段较长的路要走。但当这条路上有关怀指导的引领者、有相互帮助的同行者，当个人的奋斗与公司的愿景相结合，个人能收获成长与当下，公司能收获进步与未来。当责奋斗，无奋斗不青春。

动物园站是北京超大型的市内通勤枢纽。每天，四通八达的轨道交通把像董玲这样的年轻人，送到公司。更多有新鲜方案思路、活跃技术想法的小伙伴，欢迎搭乘，前方到站奇安信。安

荣誉墙

奇安信一科研项目荣获中国通信学会科技奖

2020 年 12 月，中国通信学会公示的 2020 中国通信学会科技奖名单中，由奇安信集团、清华大学和云盾智慧联合完成，奇安信集团董事长齐向东作为第一完成人的“基于云边情报协同的智能威胁检测和分析技术攻关及规模应用”项目，荣获 2020 通信学会科技奖二等奖。项目凭借在边缘计算与云计算相结合的体系结构、威胁情报自动提取技术、攻击知识图谱智能提取技术等多项技术创新得到了中国通信学会的充分肯定。

该项目主要为各类网站提供安全防护，创新地将边缘计算与云计算进行了有机结合，采取两级检测机制；在威胁情报应用面，采用多字符串中的攻击语义子串提取、同源（同 IP/ 子网）威胁情报提取、基于关联分析的行为序列情报提取等多项自动化威胁情报提取技术，改变了人工提取模式下，效率低，工作量大、门槛高等诸多短板，让威胁情报的提取与应用进入了自动化时代。

目前，该项目已经成功用于奇安信安域（网站云防护系统）和云盾智慧旗下相关产品中，结合 GSLB、人工智能、去规则化防护等技术，提供网站漏洞攻击防护、DDoS 攻击防护、CC 攻击防护、反爬虫、安全 CDN 等安全能力，已经在部委、央企、金融、医疗等数十万家单位取得了良好的实践效果，有效保障了这些单位网站的安全运行，为十九大、全国两会、国庆、阅兵、一带一路峰会、达沃斯论坛等重要活动提供了安全保障。

奇安信集团总裁吴云坤荣获 2020 年（第四届）国家“杰出工程师奖”

2020 年 12 月 23 日，2020 年（第四届）杰出工程师奖获奖名单在京揭晓，奇安信集团总裁吴云坤荣获第四届中华国际科学交流基金会“杰出工程师奖”，成为今年网络安全行业唯一一位获此殊荣的工程师、企业家。

杰出工程师奖由中华国际科学交流基金会发起，经科技部和国家科学技术奖励工作办公室批准，是我国目前涵盖领域最广、最具权威性的工程技术人员奖项。奖项分为“杰出工程师奖”、“杰出工程师青年奖”。“杰出工程师奖”每届奖励人数不超过 30 名，“杰出工程师青年奖”每届奖励人数不超过 40 名。


中华国际科学交流基金会

中科金[2020]029号

关于第四届杰出工程师奖
推荐人选获奖的通知

奇安信科技集团股份有限公司：

第四届中华国际科学交流基金会杰出工程师奖（以下简称杰出工程师奖）评选工作，经推荐机构（人）推荐、科基会科技公益奖励形式审查、专业领域专家评审组初评、评审委员会专家终评、媒体和所在单位公示以及奖励委员会审批等程序，已评选出第四届“杰出工程师奖”获奖人70位，其中40位“杰出工程师奖”获奖者、30位“杰出工程师青年奖”获奖者。

贵单位 吴云坤 同志获“杰出工程师奖”，特表示祝贺！

第四届杰出工程师奖颁奖活动因受疫情影响将推迟举办，届时另行通知。获奖人员将在明年初按地区分片召开小型座谈会，介绍科基会主要工作内容、杰出工程师专家委员会开展的主要活动，以及颁发证书、证书、登记奖金发放信息等相关事宜。届时科基会将分别通知有关人员参会，请各位获奖工程师根据通知积极参加。

2020 年 12 月 23 日

1

大力支持教育系统网络安全 奇安信获教育部致信感谢

2020 年 12 月，因积极参与教育系统网络安全攻防演习工作，提供演习支撑系统并赞助优秀攻击队的资金，保障了教育系统攻防演习的顺利开展，奇安信集团获得了来自教育部科学技术司的致信感谢，对奇安信一直以来对教育系统网络安全保障工作给予的大力支持表示衷心的感谢。

党的十九届五中全会明确提出了建设高质量教育体系、建成教育强国的奋斗目标。奇安信也将持续发挥企业排头兵作用，进一步与教育部门增进沟通，加强政企联动、夯实合作基础、拓宽合作领域，继续大力支持教育系统网络安全工作，为中国教育事业的发展做出新的贡献。

自 2016 年国家级大型实战攻防演习开展以来，奇安信作为中坚力量全面支撑主管机构及行业客户的实战攻防演习工作。在 2020 年的国家级大型实战攻防演习任务中，奇安信已累计参与监管单位和政企机构的各类实战攻防演习超过 220 场，在攻击、防守、沙盘推演、产品抗攻击等方面均有优秀表现。

教育部司局函件

感谢信

奇安信科技集团股份有限公司：

2020年，是极其关键特殊的一年，是全面建成小康社会目标实现之年。贵公司秉承高度的社会责任感，积极参与教育系统网络安全攻防演习工作，提供演习支撑系统并赞助优秀攻击队伍的资金，保障教育系统攻防演习顺利开展。在此，我司代向贵公司一直以来对教育系统网络安全保障工作给予的大力支持表示衷心的感谢。

党的十九届五中全会明确提出了建设高质量教育体系，建成教育强国的奋斗目标。希望贵公司继续发挥企业排头兵的作用，进一步与教育部门增进沟通，加强政企联动，夯实合作基础，拓宽合作领域，继续大力支持教育系统网络安全工作，为中国教育事业的发展做出新的贡献！

教育部科学技术司
2020年12月28日

奇安信荣获 CNVD 漏洞信息报送突出贡献单位等四项殊荣

2020 年 12 月，国家信息安全漏洞共享平台（CNVD）召开 2020 年工作会议，对漏洞信息报送和处置突出贡献单位进行表彰。奇安信集团旗下网神信息技术（北京）股份有限公司运营的补天平台，凭借强大的漏洞挖掘和响应处置能力，获得“2020 年度漏洞信息报送突出贡献单位”和“CNVD 协作特别贡献单位”称号。

截至 11 月底，补天平台在 2020 年共向 CNVD 报送 34481 个原创漏洞，位列国内前茅。其中，奇安信网神自主发现报送的漏洞（漏洞编号：CNVD-2020-59797）被评为“2020 年度最具价值漏洞”。

同时，凭借强大的实战化漏洞攻防能力，奇安信网神还在 2020 年被授予“CNVD 技术组支撑单位”称号。

奇安信集团荣获第八届 CNCERT 网络安全应急服务国家级优秀支撑单位

2020 年 12 月 2 日，国家互联网应急中心 CNCERT 公布第八届 CNCERT 网络安全应急服务支撑单位考核结果，奇安信集团旗下网神信息技术（北京）股份有限公司作为国家级支撑单位和唯一三个资质大满贯企业（国家级 / 省级、反网络诈骗领域、工业控制领域），获得“优”级考评。

附：本次考评等级为优的部分单位列表。

编号	单位名称	级别	考评等级
CNCERT-2019-20210701 GJ007	北京天融信网络安全技术有限公司	国家级	优
CNCERT-2019-20210701 GJ004	网神信息技术（北京）股份有限公司	国家级	优
CNCERT-2019-20210701 GJ001	恒安嘉新（北京）科技股份公司	国家级	优
CNCERT-2019-20210701 SJ034	上海斗象信息科技有限公司	省级	优

CNCERT 网络安全应急服务支撑单位旨在遴选出一批优秀的网络安全应急服务单位，配合 CNCERT 为国家网络安全应急提供支撑服务工作。

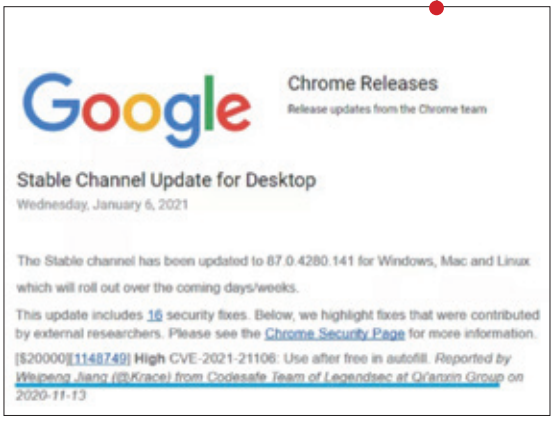
奇安信集团坚持为 CNCERT 国家中心及北京、天津、上海、江苏、江西、湖南、河南、广东、陕西、四川 、辽宁、青海、河北、西藏等各分中心提供安全漏洞信息报送、网络安全事件报送、重大安全事件响应、专项支撑，以及交流培训、产品测试等多个维度的应急服务支撑。

数据显示，2019 年以来，奇安信网神运营的补天平台累计向 CNVD 报送漏洞超过 8 万条，行业内遥遥领先。在 CNCERT 发起的各类专项支撑活动中，奇安信集团的网络安全漏洞、事件等报送任务和应急服务工作，均得到了 CNCERT 的高度认可。

奇安信代码安全实验室报告并协助修复高危漏洞 获谷歌官方致谢

北京时间 2021 年 1 月 7 日，谷歌发布补丁更新公告以及致谢公告，公开致谢奇安信代码安全实验室研究人员。

此前，奇安信代码安全实验室研究员为谷歌 Chrome 发现一个“高危”级别的沙箱外漏洞 (CVE-2020-21106)，第一时间报告并协助其修复漏洞。该漏洞位于浏览器沙箱外，易被攻击者利用。未认证的远程攻击者可构造恶意网页，诱骗受害者访问，从而在受害者系统上执行任意代码。如遭成功利用，该漏洞可使易受攻击的系统遭攻陷。



Google Chrome Releases

Release updates from the Chrome team

Stable Channel Update for Desktop

Wednesday, January 6, 2021

The Stable channel has been updated to 87.0.4280.141 for Windows, Mac and Linux which will roll out over the coming days/weeks.

This update includes 16 security fixes. Below, we highlight fixes that were contributed by external researchers. Please see the Chrome Security Page for more information.

[$20000][1148749] High CVE-2021-21106: Use after free in autofill. Reported by Weipeng Jiang (@Krace) from Codesafe Team of Legendsec at Qi'anxin Group on 2020-11-13

大事记

奇安信内生安全框架荣膺“世界互联网领先科技成果”

在2020年浙江乌镇召开的“2020世界互联网大会 · 互联网发展论坛”上，包括奇安信新一代企业网络安全框架（内生安全框架）在内的15项闪耀全球的世界互联网领先科技成果正式发布，这些成果有望为人类生活、科技进步、经济发展、社会变革赋予强大动力。

据悉，2020年“世界互联网领先科技成果发布活动”聚焦产业恢复与协同发展、数字化社会治理、全球公共危机应对、人工智能云生活、绿色数字公益实践五大应用领域，展现全球互联网领域最新科技成果。

“数字化时代的到来，彻底打破了网络世界和物理世界的边界，带来了新的安全风险。以前的静态边界防护思路，不再适应新时代的需求，数字化时代的保障需要内生安全。”在领先科技成果发布会上，奇安信集团董事长齐向东介绍称，内生安全是指在信息化环境下，内置并不断自我生长的安全能力。通过“一个中心五张滤网”，从网络、数据、应用、行为、身份五个层面，建立无处不在的网络安全“免疫力”，从而极大降低网络攻击风险，真正保证业务安全。

为推动政企机构能够快速建立起适应数字化时代的网络安全防御能力，2020年8月，奇安信基于“内生安全”理念，用系统工程的方法，把网络安全能力映射成为可工程建设的安全能力组件体系，并给出一套方法论，构建出能够适应形势变化的新一代企业网络安全框架（内生安全框架）。

齐向东表示，政企机构按照新一代企业网络安全框架（内生安全框架），投入三至五年实践，就能建立起完善的网络安全协同联动防御体系，真正实现内生安全。

国际权威咨询机构 Forrester 最新报告显示：奇安信领跑国内威胁情报市场

国际权威咨询机构 Forrester 发布了《Now Tech: External Threat Intelligence Services,Q4 2020》报告，详细盘点了全球主要威胁情报供应商（包括CrowdStrike、IBM、FireEye等）。奇安信凭借海量的威胁情报样本、精准的威胁情报检测能力和强大的APT组织追踪能力，成为少数入围该报告的中国厂商之一，再次证明了奇安信威胁情报在国内的领跑地位。

作为国内首个商用威胁情报中心，奇安信威胁情报中心通过强大的大数据能力，实现全网威胁情报的即时、全面、深入的整合与分析。其产生的海量情报数据，不仅直接赋能自身安全体系产品，而且基于攻击链路径特征和各行业多场景的业务需求，进行有针对性地产品化开发。

近百人的奇安信威胁情报研究分析团队，在威胁分析的各环节，包括公开情报收集、数据处理、恶意代码分析、网络流量解析、线索挖掘拓展，都有专才覆盖，为威胁情报安全服务产品研发和能力提升提供了强大的基础数据、威胁研判支撑。

截至目前，奇安信威胁情报中心已累计首发9个国内外APT组织，监测到的针对国内发动APT攻击的黑客组织达到44个。

奇安信与腾讯安全达成战略合作 筑牢互联网安全底座

奇安信与腾讯云计算（北京）有限责任公司签署协议，双方达成战略合作伙伴关系，约定在信息安全市场中紧

密合作，充分融合双方的优势资源、能力、技术，共同打造行业领先的安全解决方案，为产业互联网发展筑牢安全底座。

根据协议内容，腾讯安全与奇安信不仅将聚焦安全技术创新和安全产品研发，还将共同针对政企、金融、医疗、教育、交通、能源及其他信息安全需求高增长行业，提升安全服务效率和质量。

随着产业数字化的高速推进，“上云用数赋智”已成为数字经济强劲发展和产业互联网高质量发展的必然，而网络安全则是数字经济的“底座”，是新基建的基础工程。此次合作，不仅为双方在市场业绩高速增长注入强劲动力，也势必通过双方技术优势互补和深度融合，为整个数字经济社会转型升级，打造出最安全的“数字化助手”。

吴云坤出席 2020 中国城市数字经济论坛：数字经济需重视防范黑客

2020 年 12 月 8 日，主题为“数智共享 驱动未来”的 “中国城市数字经济论坛 · 2020”在上海举办。奇安信集团总裁吴云坤出席此次论坛。

在“构建数字未来 共享数字空间”平行论坛现场，奇安信科技集团总裁吴云坤表示，防范黑客是数字经济中不可或缺的一项工作。

吴云坤指出，从 2015 年开始，黑客的关注焦点从最初的网络诈骗，到用户上网遭到攻击，到攻击金融机构，再到攻击实体工业企业。随着数字化的深入发展，已转移至“智慧城市”，这将影响水电气等关乎老百姓生活品质的领域，因此数字经济必须重视防范黑客。

用奥运标准培养网络安全尖兵 十支警院队伍问鼎第四届“蓝帽杯”

2020 年 12 月 26 日，第四届 " 蓝帽杯 " 全国大学生网络安全技能大赛举办颁奖典礼，为在比赛中取得优异成绩的战队以及人气教师获得者颁发奖项。

作为面向全国警院的高规格、强影响力的实战技能大赛，第四届“蓝帽杯”吸引了全国 6 家地方院校、26 家警察院校，共 201 支战队，603 名警院学生参赛。经过专家评委会的最终审定，来自全国 8 所院校的 10 支战队获得了一等奖。

此前，" 蓝帽杯 " 已连续举办三届，统计显示，已累计有 194 支战队，582 位选手参赛，持续强化中国的网安力量。目前，这些网络安全的 " 尖兵 "，已在公安网络安全领域担任重要的工作岗位，为网络安全、国家安全保驾护航。同时，比赛还促进了各大学院校的网络安全攻防人才培养，建立专业学科、建设靶场实验室，拉动了网络安全教育素质的提升。

北京市政协主席吉林带领政协科技委赴奇安信集团调研

2020 年 12 月 7 日，北京市政协主席吉林带领政协科技委部分委员赴奇安信集团调研，深入了解奇安信的网络安全业务和近期发展规划。奇安信集团董事长齐向东等公司相关高管陪同并参加了交流座谈会。

吉林主席对奇安信的发展表示了肯定，并对奇安信成功登陆科创版表示祝贺。吉林表示，当前数字技术与实体经济深度融合，不断提高数字化、网络化、智能化水平，信息网络已经成为重要载体，因此网络安全关系到国计民生的方方面面，奇安信经过几年的快速发展，在国家网络安全维护和保障中已经起到越来越重要的作用。

奇安信与中国电信安徽分公司达成战略合作 开创“1+X+1”合作模式

2020 年 12 月 4 日，奇安信集团与中国电信安徽分公司达成战略合作，双方开创性地建立网安行业“1+X+1”合作模式，共同探讨研究内生安全体系在网络安全、云安全、5G 安全、工业互联网安全等领域的实践落地，共同打造战略协同、优势互补、资源共享、共赢发展的安全服务业务生态链。

双方联合成立“安徽电信－奇安信安全联合创新中心”，共同开展创新课题研究。奇安信集团董事长齐向东和中国电信安徽公司党委书记、总经理刘颖为创新中心揭牌。

本次合作开创性建立的“1+X+1”的合作模式，包括一套内生安全体系和一个安全联合创新中心，X 代表着双方在实战攻防、5G 安全、云安全、工业互联网安全等方面的全面合作。奇安信将用内生安全框架，帮助中国电信安徽分公司建立“事前防控”的内生安全体系。

图书推荐

奇安信出版《走进新安全》专为初学者量身打造

知识是最好的礼物，奇安信集团近期全新出版一部网络安全专业类书籍《走进新安全》，专为不太懂网络安全的“萌新”量身打造。

该书是由奇安信集团联合 30 余位一线网络安全专家共同参与创作，可让“外行人”通过通俗易懂的文字，顺畅理解看起来非常晦涩难懂的网络安全术语或基础知识，零门槛走进新的网络安全世界。

本书面向领导干部、管理人员和网络安全爱好者，将从安全基础、安全建设和安全发展三个方面将网络安全的各项要点与读者一一道来，并首次将“新”思想、理念和方法以图书形式呈现在大众面前。

亮点速览：

安全基础篇

1、全面介绍了网络安全威胁、思想、技术、政策的发展过程

2、现在的网络威胁到底有哪些，给我带来了什么影响？

3、当前主流的网络技术有什么？

安全建设篇

1、现代网络安全建设的思想和方法论有哪些？

2、如何进行网络安全体系的规划、建设和运营？

3、如何进行网络安全实战攻防演习？

安全发展篇

1、网络安全人才应该如何培养？

2、网络安全朝着哪些新方向发展？

奇安信

防范钓鱼邮件

• 网络安全部温馨提示

- ☆ 钓鱼邮件一般利用人们使用习惯、焦急心理等因素进行钓鱼攻击
- ☆ 收到可疑邮件需要仔细观察邮件有没有异常提醒或提示，核对发件人信息与邮件所显示的是否一致
- ☆ 谨慎面对邮件中的链接，不相信任何弹出的要求输入账号密码的页面
- ☆ 遇到公司部门发送需要收集信息的通知邮件，要通过蓝信聊天 / 必读号核实
- ☆ 附件先用天擎杀毒再打开
- ☆ 除了邮件外警惕二维码、社交软件聊天、加微信等社会工程学钓鱼。你以为的交友，可能是为了套取你的信息
- ☆ 警惕上下文关联的钓鱼邮件
- ☆ 保护好公司和个人的信息、权限、不确认不提供，遇到问题及时联系网络安全部（g-sec@qianxin.com）

奇安信 | BEIJING 2022

北京2022年冬奥会官方网络安全赞助商

奇安信威胁情报中心

中国威胁情报行业领军者

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

威胁情报中心

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

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

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

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

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

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

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

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

奇安信

新一代网络安全领军者

聚焦安全运营，构建智能平台

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

国内领先的威胁情报能力

奇安信威胁情报中心在情报数量及数据覆盖度方面国内第一。

首款分布式关联分析引擎 - Sabre

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

将平战结合进行落地

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

重大安全事件的威胁预警

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

专业的安全运营服务

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

市场占有率NO.1

连续2年中国安全管理平台市场占有率第一——赛迪顾问认证

态势感知解决方案市场领导者——IDC认证

态势感知技术创新力和市场执行力双第一——数世咨询认证