极牛网络安全通讯 • 社群期刊 2024 年 1 月 第 31 期

网安观察

第31期
2024年1月

极牛网

极牛网 网络安全行业媒体

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

极牛众星计划

网安工程师品牌孵化

网安工程师品牌MCN孵化计划
工程师经纪服务平台

技术格局

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

管理之道

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

人才梯队

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

企业战略

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

产品运营

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

布道能力

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

2024网络空间安全趋势预测

随着2023年的结束，我们已经步入2024年。常见的关于网络安全趋势的评论更多地从网络钓鱼、勒索软件攻击、供应链攻击、意识培训、深度伪造风险等角度出发。让我们从更广的角度去对2024年全球将面临的一些复杂的网络安全挑战进行预测。

1）全球地缘政治不稳定和网络空间战争：

地缘政治紧张局势的升级越来越多地映射到网络空间，一些国家支持的网络活动导致破坏全球关键基础设施的稳定性。这一趋势超越了传统的网络攻击，更加针对能源、医疗健康、基础设施和金融系统。

预测：预计新形式的网络经济战(Cyber-Economic-Warfare)将更加突出，以最小的行动造成最大的影响，而且往往损害核心供应链。

2）人工智能、通用人工智能和网络安全风险：

人工智能和通用人工智能（AGI）的出现预示着网络威胁的新时代，它能进行复杂、自适应和难以检测的攻击。随着时间的推移，先进的"黑暗AI"可以熟练地处理大量不同的数据集，将来自各种相互排斥的数据泄露的信息联系起来。这种能力将能够对个人、行为和公司进行更复杂的分析。因此，它将为网络攻击铺平道路，网络攻击不仅更有针对性，而且具有高度个性化，有效载荷具有战略定时，专门适应其预定目标的特点。

预测：双重勒索的勒索软件案件的激增，以及前所未见的以某种方式由人工智能驱动的新一波复杂攻击方法将成为头条新闻。它会成为人工智能驱动的恶意软件的新形式吗?

3）量子计算、AGI和密码学：

量子计算和AI的交叉为密码学带来了重大的挑战和机遇。量子计算的快速发展，带来了破解当前加密算法的潜力，使现有的加密变得脆弱。同样，AGI以与前面提到的不同方式呈现了网络安全态势的另一个维度。利用AGI解决不同类型数学问题的全部潜能成为现在的一大热门话题。

预测：AGI不太可能很快解决高级密码/加密问题，但在2024年，我们也许会惊讶于AGI可能会解决一些我们没有预测到的初等数学问题。2024年AGI x密码学的发展将吓跑反对者。

总顾问
叶绍琛

2024 年2月1日

CONTEN

目录

安全态势

国际视野

ONTENTS

专题报道

第 3 1 期

《网安观察》编辑部

主办　极牛网

总　　编　　辑：陈鑫杰
总　　顾　　问：叶绍琛
副　　总　　编：王文彦
威胁情报主编：陈艇鑫
移动安全主编：蔡国兆
网安人才主编：林俊濠
涉网犯罪主编：胡铭凯
网安产业主编：张九史
网安态势主编：郑泽彬

公众号　小程序　网站

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

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

政策篇

国内，关基安全屏障建设再获进展。财政部、工信部联合发布施行 7 项政府采购标准，对政府采购操作系统、数据库、通用服务器等主流软 / 硬件产品，作出了安全可靠等要求；交通运输部公布《铁路关键信息基础设施安全保护管理办法》，对铁路领域关基保护作出了进一步要求；

国际上，美国国防部发布关于承包商网络安全合规计划 CMMC 的拟议规则，要求承包商必须获得 CMMC 认证才能获得订单，初步估算，美国国防工业企业每年将为此增加超 40 亿美元的网络安全支出。

国内

《网络安全信息报送指南》等 5 项网络安全国家标准获批发布

1 月 5 日全国信安标委公众号消息，根据 2023 年 12 月 28 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2023 年第 20 号），全国信息安全标准化技术委员会归口的 5 项网络安全国家标准正式发布。具体包括两项修订标准《信息安全技术 信息安全管理体系概述和词汇》《信息安全技术 射频识别（RFID）系统安全技术规范》，三项新标准《信息安全技术 网络安全信息报送指南》《信息安全技术 电子发现 第 1 部分：概述和概念》《信息安全技术 通用密码服务接口规范》。

十七部门联合印发《“数据要素 ×”三年行动计划（2024—2026 年）》

1 月 4 日国家数据局公众号消息，国家数据局、中央网信办、科技部等时期部门联合制定了《“数据要素 ×”三年行动计划（2024—2026 年）》，现公开印发。该文件共五章，包括背景介绍、总体要求、十二项重点行动、三项保障支撑举措、五项组织实施措施。该文件提出，到 2026 年年底打造 300 个以上示范性强、显示度高、带动性广的典型应用场景，数据产业年均增速超过 20%，推动数据要素价值创造的新业态成为经济增长新动力。在保障支撑举措“加强数据安全保障”中，该文件提出了落实数据安全法规制度、丰富数据安全产品、培育数据安全服务三方面内容。

《铁路关键信息基础设施安全保护管理办法》公布

1 月 3 日交通运输部官网消息，交通运输部公布了《铁路关键信息基础设施安全保护管理办法》，自 2024 年 2 月 1 日起施行。该文件共 6 章 30 条，包括总则、铁路关键信息基础设施认定、运营者责任和义务、保障和监督、法律责任、附则。该文件提出，铁路关键信息基础设施是指在铁路领域，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益的重要网络设施、信息系统等。铁路关键信息基础设施的网络安全保护等级应当不低于第三级。任何个人和组织不得实施非法侵入、干扰、破坏铁路关键信息基础设施的活动，不得危害铁路关键信息基础设施安全。

操作系统等 7 项政府采购需求标准发布施行

12 月 28 日财政部官网消息，财政部、工业和信息化部联合发布施行 7 项政府采购需求标准，分别是操作系统、数据库、通用服务器、工作站、一体式计算机、便携式计算机和台式计算机。该系列文件提出，对于既包含操作系统、数

据库、服务器等软 / 硬件产品也包含集成服务的采购项目，采购人应当合理划分采购包，尽可能将操作系统、数据库、服务器等软 / 硬件产品与集成服务分包采购。采购的操作系统、数据库、服务器等软硬件产品总额达到分散采购限额标准的，应当单独分包采购。该系列文件要求，乡镇以上党政机关，以及乡镇以上党委和政府直属事业单位及部门所属为机关提供支持保障的事业单位在采购相关产品时，应当将符合安全可靠测评要求纳入采购需求，其他单位可不在采购需求中提出此项要求。

十四部门联合印发《关于开展网络安全技术应用试点示范工作的通知》

12 月 18 日工信部官网消息，工业和信息化部、国家网信办、人力资源社会保障部等十四部门联合印发《关于开展网络安全技术应用试点示范工作的通知》，部署开展网络安全技术应用试点示范工作。该文件提出，将以新型信息基础设施安全、数字化应用场景安全、安全基础能力提升为主线，面向公共通信和信息服务、人力资源社会保障、水利、卫生健康、应急管理、广播电视、金融、交通运输、邮政等重要行业领域网络和数据安全保障需求，从基础网络安全、云计算安全、人工智能安全、大数据安全、信创安全、商用密码、车联网安全、物联网安全、中小企业数字化转型安全、网络安全共性技术、网络安全创新服务、教育技术产业融合发展联合体、网络安全“高精尖”创新平台等 13 个重点方向，遴选一批技术先进、应用成效显著的试点示范项目。

欧盟新《网络安全条例》正式生效

1 月 8 日欧盟委员会消息，欧盟新版《网络安全条例》于 1 月 7 日起生效。该条例规定了每个欧盟组织机构需要采取的相应措施，包括建立内部网络安全风险管理、治理和控制框架。该条例提出，设立一个新的机构间网络安全委员会（IICB）以监测和支持欧盟实体落实相关条例，并延长了欧盟计算机应急组织（CERT-EU）的任期。CERTEU 将作为威胁情报、信息交换和事件响应的协调中心、中央咨询机构和服务提供者。为了与其授权内容保持一致，CERT-EU 被重新命名为联盟内网络安全服务中心，其简称“CERT-EU”被保留。

美国防部发布关于承包商网络安全合规计划 CMMC 的拟议规则

2023 年 12 月 26 日美国联邦公报消息，美国国防部在《联邦公报》上发布针对网络安全成熟度模型认证（CMMC）计划的拟议规则，要求国防承包商必须获得 CMMC 认证才能获得订单。该规则确定了网络安全要求的分层模型，要求承包商根据信息的敏感性实施三级网络安全标准。其中，第 1 级针对涉及联邦合同信息（FCI）的合同，要求承包商必须遵守《美国联邦采购法规》52.204-21 规定的 15 项安全要求；第 2 级适用于涉及受控非机密信息（CUI）的合同，承包商除需遵守第 1 级要求外，还必须遵守《NISTSP 800-171 Rev2》中规定的 110 项安全要求；第 3 级旨在增强 CUI 抵御高级持续威胁的保护，承包商除在第 2 级基础上，还需遵守《NIST SP 800-172 Rev2》中选定的 24 项安全要求。据新规估算，美国国防工业企业每年将为此增加超 40 亿美元的网络安全支出。

美国 NASA 发布首版太空安全最佳实践指南

12 月 22 日 NASA 消息，美国国家航空航天局（NASA）发布首版太空安全最佳实践指南，以加强公共部门和私营企业太空活动的网络安全。太空安全最佳实践指南提供了安全实施任务的指导性原则和控制措施，旨在应对当今网络攻击者试图破坏任务所使用的战术、技术和程序（TTPs），保护航天器和地面段。指南采用美国国家标准与技术研究院 NIST SP 800-53 文件中“安全控制”的定义，并充当 NIST 术语与 NASA 飞行项目术语之间的翻译桥梁，适用于各种规模、范围和性质（国际、公司、大学）所有等级的任务、项目和计划。

事件篇

国家博弈与地缘政治交织下，网络对抗愈加激烈。俄罗斯安全公司卡巴斯基曝光，“三角行动”间谍软件利用了一个苹果硬件“后门漏洞”，俄情报部门认为攻击者为美国 NSA；我国国家安全部披露一起境外机构非法窃取我国航空数据活动，及时查获了数百套已在境内投放的设备。

美国证交会推特账号被黑并发布虚假市场消息

1 月 9 日 CyberScoop 消息，美国证券交易委员会（SEC）推特账号 @SECgov 当天下午约 4 点发布了一则虚假的市场消息，称批准比特币 ETF 上市交易。大约 15 分钟后，SEC 主席 Gary Gensler 在个人推特账号上声称，@SECgov 推特账号已被盗用，发布了未经授权的消息。SEC 发言人随后在一份声明中表示，在美国东部时间下午 4 点后不久，不明身份人士在短时间内对 SEC 的推特账号 @SECGov 进行了未经授权的访问和活动。目前黑客的访问“已被终止”。这则假消息发布后，比特币的价值暂时飙升至近 48,000 美元，然后又回落至 45,500 美元。

国家安全部披露境外机构非法窃取我国航空数据活动

1月6日国家安全部公众号消息，国家安全部发布文章《航空爱好者切莫变为“窃密志愿者”》称，发现多个境外机构以免费提供设备、共享航空信息为诱饵，依托网络社交平台面向境内航空爱好者精准招募“志愿者”，并跨境邮寄设备，指挥“志愿者”在我境内非法采集、向境外秘密传输我国飞行器飞行数据。这些境外机构在我国渤海、东海、南海周边省份大量投放此类设备，不仅窃取民用航空数据，甚至还能窃取军用航空器等敏感数据信息。经测算，每台设备每天可向境外发送约 1000 架次飞机的飞行数据和约 13 万条位置数据。按照覆盖半径 300 公里至 400 公里计算，仅需投放约 300 台设备，即可对我全空域飞机飞行数据实现监测覆盖。针对上述非法窃取我敏感数据的行为，国家安全机关会同有关部门在全国范围内开展了专项打击，及时查获数百套已在境内投放的设备，依法对有关人员进行处罚。

黑客攻击全国 21 个省市社保 / 医疗等系统，“爬取”公民信息获利 500 余万

1 月 5 日检察日报消息，四川省成都市新都区检察院公布了一起利用技术手段非法窃取公民个人信息案，法院近日以侵犯公民个人信息罪判处王某等人有期徒刑三年至十个月不等。经查，2021 年初至 2022 年 7 月，王某等人通过网络渠道委托黑客，利用搜集到的各种政府、企业网络平台的接口漏洞，通过对接口进行数据抓包、参数解析等，开发出 100 余款黑客软件。王某等人利用相关黑客软件，先后入侵全国 21 个省市的社保、医疗等共计 29 个行业的 51 个系统，“爬取”包括姓名、身份证号、手机号码、工作单位、家庭成员、社保缴纳等在内的公民个人信息，并贩卖给相关催债公司。被盗的公民个人信息被催债公司大规模用于数据画像，勾勒人物关系和活动轨迹，由此通过手机短信、微信、抖音等社交平台向欠款人的社会关系人发送催债信息。通过梳理固定涉案数据、司法鉴定意见及审计的获利情况，该院认定该团伙非法获利达 500 余万元。

电信巨头 Orange 西班牙公司关键账号被盗，导致国内大面积断网

1 月 3 日 Bleeping Computer 消息，国际电信巨头 Orange 西班牙公司的 RIPE 账号被盗，攻击者将其网络核心配置（BGP 和 RPKI）改为无效，导致全国互联网中断了大约 3 小时。Orange 是西班牙最大的移动运营商之一，此

次网络中断大约持续了 3 个小时。据悉，攻击者在信息窃取软件的数据集中发现了此次被利用的账号（未启用双因子认证），为了“找乐子”实施了此次攻击。

澳大利亚地方法院遭勒索攻击：敏感案件数据泄露 司法权威性被破坏

1 月 2 日 ABC 消息，澳大利亚维多利亚州法院系统遭受网络攻击，维多利亚州法院服务局（CSV）发言人表示，黑客侵入了法院系统的音视频存档区域。这意味着高度敏感案件的证人证词等听证录音可能已被访问或窃取。相关录音覆盖了 2023 年 11 月 1 日至 12 月 21 日期间的听证会，也可能包括 11 月之前的部分听证会。CSV 正在努力通知出庭记录遭黑客访问的人，并计划设立一个联系中心，向自认为受攻击影响者提供服务。有安全专家认为，攻击者是使用 Qilin 勒索软件的俄罗斯黑客。

杭州破获重大勒索病毒案：犯罪团伙借助 ChatGPT 进行程序优化

12 月 28 日新华社消息，杭州上城区网警近日破获一起重大勒索病毒案件，犯罪团伙成员均有网络安防相关资质，且在实施犯罪过程中借助 ChatGPT 进行程序优化。11 月 20 日，上城网警接到辖区某公司报案称，该公司名下相关服务器遭勒索病毒攻击，导致公司所有系统无法正常运行，对方勒索 2 万 USDT（泰达币）。警方随即组建技术攻坚团队开展侦查。专案组对被攻击服务器进行细致勘验、提取木马程序进行分析和对嫌疑人勒索使用的虚拟币地址进行多维度研判，成功抓捕 4 名犯罪嫌疑人。该团伙 4 人均有网络安防相关资质，且有供职大型网络科技公司经历。他们对分工负责编写勒索病毒版本、借助 ChatGPT 进行程序优化、开展漏洞扫描、渗透获取权限、植入勒索病毒、实施敲诈勒索的犯罪事实供认不讳。

卡巴斯基曝光疑遭 NSA 利用的苹果硬件“神秘后门”

12 月 27 日 Bleeping Computer 消息，卡巴斯基在年关时分披露了苹果处理器“后门漏洞”，为连载半年多的三角定位间谍软件行动收官。CVE-2023-38606 滥用苹果预留未公开的隐蔽硬件特性，绕过了系统保护措施，攻击者利用该漏洞对卡巴斯基、驻俄中国大使馆等多个组织实施了攻击。俄罗斯官方认为，美国 NSA 使用苹果提供的硬件后门发起了这次攻击，但尚无坐实这些指控的明确证据。卡巴斯基推测，这个未记录的硬件特性之所以包含在最终供消费者使用的 iPhone 版本中，可能是出于错误，或者是为了方便苹果工程师进行调试和测试。苹果通过更新设备树限制物理地址映射修复了这个漏洞。但是，仍然不清楚攻击者最初是如何发现这种如此隐蔽的可利用机制的。

意大利云服务商被勒索，导致上千个政府机构服务中断、数据丢失

12 月 19 日 Security Affairs 消息，意大利云服务商 Westpole 遭遇 Lockbit 3.0 勒索攻击，导致云上客户、政务服务商 PA Digitale 服务中断，PA Digitale 托管的大量地方政府组织和市政机构无法提供服务。有意大利媒体报道称，由于此次攻击，部分受影响政府机构将无法向员工发放 12 月工资。意大利国家网络安全局发布声明称，已恢复 700 多家与 PA Digitale 相关的国家和地方公共实体数据，但还有约 1000 家实体数据尚未恢复。

网络战场失利！伊朗全国大部分加油站数字崩溃，艰难转向手动运营

12 月 18 日路透社消息，伊朗石油部长 Javad Owji 表示，一起网络攻击导致境内约七成加油站无法提供服务，后来有一成多的加油站逐步恢复运营。据伊朗国家电视台报道，一家名为 Gonjeshke Darande 或“掠食麻雀”的组织声称他们是幕后黑手，以色列当地媒体也报道了这一声明。该组织在 Telegram 上发表声明：“我们以可控的方式实施这次网络攻击，避免对应急服务造成潜在伤害。”此前巴以冲突爆发后，“掠食麻雀”代表接受路透社采访，表示由于伊朗支持哈马斯，他们正在准备在未来对伊朗发动攻击，并“准备了一些攻击‘按钮’”。“掠食麻雀”组织此前曾网络攻击 UI；安加油站、铁路网络、钢铁厂等关基设施，并造成重大损害。

漏洞篇

热门产品 0day 漏洞在野利用猖獗。近一个月来，Google Chrome 浏览器两次披露有 0day 漏洞遭到在野利用，分别为 V8 越界访问、WebRTC 堆缓冲区溢出。Citrix 旗下 NetScaler Gateway 也曝出两个在野漏洞利用。建议用户尽快做好自查及防护。

Google Chrome V8 越界访问漏洞安全风险通告

1 月 17 日，奇安信 CERT 监测到 Google 发布公告 Google Chrome V8 越界访问漏洞 (CVE-2024-0519) 存在在野利用，攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而获取敏感信息或应用程序崩溃。目前，此漏洞已检测到在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

NetScaler ADC 和 NetScaler Gateway 多个在野漏洞安全风险通告

1 月 17 日，奇安信 CERT 监测到官方发布安全公告说明 NetScaler ADC 和 NetScaler Gateway 代码执行漏洞 (CVE-2023-6548) 与 NetScaler ADC 和 NetScaler Gateway 拒绝服务漏洞 (CVE-2023-6549) 存在在野利用。具有低权限的相邻网络的攻击者可通过管理界面访问 NSIP、CLIP 或 SNIP 后利用 CVE-2023-6548 在系统上执行代码；未经身份验证的远程攻击者利用 CVE-2023-6549 可以造成系统拒绝服务。鉴于这些漏洞影响范围较大，且已监测到在野利用，建议客户尽快做好自查及防护。

GitLab 密码重置漏洞安全风险通告

1 月 12 日，奇安信 CERT 监测到 GitLab 密码重置漏洞 (CVE-2023-7028)，未经身份验证的远程攻击者可利用该漏洞将用户账户密码重置电子邮件发送至任意邮箱。LDAP 用户不会受到影响，因为没有忘记 / 重置密码选项。此外，启用了双因素身份验证的用户很容易受到密码重置的影响，但账户不会被接管，因为需要第二个身份验证因素才能登录。鉴于该产品用量较大，建议客户尽快做好自查及防护。

Apache OFBiz 远程代码执行漏洞安全风险通告

12 月 29 日，奇安信 CERT 监测到 Apache OFBiz 远程代码执行漏洞 (CVE-2023-51467)，由于在 ofbiz 18.12.10 版本中官方仍未修复 CVE-2023-49070 漏洞中的权限绕过漏洞，导致未经身份认证的远程攻击者仍能够利用此漏洞绕过身份认证。远程未授权攻击者利用此漏洞结合后台相关功能可执行任意代码，接管目标服务器。目前奇安信 CERT 已成功复现该漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

金蝶 Apusic 应用服务器 JNDI 注入漏洞 (QVD-2023-48297) 安全风险通告

12 月 22 日，奇安信 CERT 监测到金蝶 Apusic 应用服务器 JNDI 注入漏洞 (QVD-2023-48297)，金蝶 Apusic 应用服务器是一款企业级应用服务器，支持 Java EE 技术，适用于各种商业环境。由于金蝶 Apusic 应用服务器权限验证不当，导致攻击者可以向 loadTree 接口执行 JNDI 注入，造成远程代码执行漏洞。利用该漏洞需低版本 JDK。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 1 月补丁日多个产品安全漏洞风险通告

1 月 10 日，微软共发布了 49 个漏洞的补丁程序，修复了 .NET、Microsoft Office、Windows Server 等产品中的漏洞。值得注意的是，微软在 2023 年 5 月 9 日停止了 Windows 10 20H2 的安全更新和技术支持，建议您尽快升级系统。经研判，以下 10 个重要漏洞值得关注（包括 2 个紧急漏洞、8 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-2024-20674	Windows Kerberos 安全特性绕过漏洞	紧急	未公开	较大
CVE-2024-20700	Windows Hyper-V 代码执行漏洞	紧急	未公开	一般
CVE-2024-20683	Win32k 权限提升漏洞	重要	未公开	较大
CVE-2024-20698	Windows Kernel 权限提升漏洞	重要	未公开	较大
CVE-2024-21307	Remote Desktop Client 代码执行漏洞	重要	未公开	较大
CVE-2024-20652	Windows HTML Platforms 安全特性绕过漏洞	重要	未公开	较大
CVE-2024-20653	Microsoft Common Log File System 权限提升漏洞	重要	未公开	较大
CVE-2024-20686	Win32k 权限提升漏洞	重要	未公开	较大
CVE-2024-21310	Windows Cloud Files Mini Filter Driver 权限提升漏洞	重要	未公开	较大
CVE-2024-21318	Microsoft SharePoint Server 代码执行漏洞	重要	未公开	较大

金蝶 Apusic 应用服务器 JNDI 注入漏洞 (QVD-2023-48476) 安全风险通告

12 月 22 日，奇安信 CERT 监测到金蝶 Apusic 应用服务器 JNDI 注入漏洞 (QVD-2023-48476)，金蝶 Apusic 应用服务器是一款企业级应用服务器，支持 Java EE 技术，适用于各种商业环境。由于金蝶 Apusic 应用服务器权限验证不当，导致攻击者可以向 createDataSource 接口执行 JNDI 注入，造成远程代码执行。利用该漏洞需低版本 JDK，且需要服务器上有数据库驱动。鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。

Google Chrome WebRTC 堆缓冲区溢出漏洞安全风险通告

12 月 21 日，奇安信 CERT 监测到 Google 修复 Google Chrome WebRTC 堆缓冲区溢出漏洞 (CVE-2023-7024)，该漏洞存在在野利用，攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而在应用程序上下文中执行任意代码或导致浏览器崩溃。目前，此漏洞已发现在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

金蝶天燕远程代码执行漏洞安全风险通告

12 月 20 日，奇安信 CERT 监测到金蝶天燕远程代码执行漏洞 (QVD-2023-48081)PoC 及 EXP 在互联网上流传，该漏洞允许未授权的远程攻击者上传任意文件，最终可能导致远程执行恶意命令，控制服务器等。目前，奇安信 CERT 已复现此漏洞，经研判，该漏洞攻击利用难度低，且 EXP 已公开，被恶意利用的可能性增大。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apache Dubbo 多个反序列化漏洞安全风险通告

12 月 18 日，奇安信 CERT 监测到 Apache Dubbo 发布新版本，修复了 Apache Dubbo 反序列化漏洞 (CVE-2023-46279) 与 Apache Dubbo 反序列化漏洞 (CVE-2023-29234)。攻击者通过向系统发送恶意数据包利用这些漏洞，成功后可以读取敏感信息或执行恶意代码。鉴于此产品用量较大，建议客户尽快做好自查及防护。

微软数据安全指数报告：自动化和 AI 是提升保护能力的可行途径

近日，微软和 Hypothesis Group 发布的《数据安全指数：趋势、见解和数据安全战略》报告显示，随着数字化的发展，网络安全漏洞也在不断增加，网络威胁、数据泄露和内部风险变得越来越常见，也给我们的企业带来了很大的风险。

结论一：决策者认为他们受到了保护，但事实并非如此

从表面上看，决策者对其数据安全解决方案展现出高度的信心和满意度。大多数单位、组织认为其数据安全控制措施在防止数据泄露方面是有效的，“他们知道自己的大部分数据放在哪里，并且可以检测与数据相关的大多数风险”。

但事实上，政企单位（单位组织）却持续遭遇大量的数据安全事件，在过去 的 12 个月中，平均每家公司经历了 59 起数据安全事件，其中 20% 被视为严重事件，可能带来高达 1500 万美元的年度成本。

除了这些成本，40% 的决策者还表示，为了从数据安全事件中恢复过来，以及挽回因声誉受损而造成的业务损失，需要花费的运营成本也是很高的。高达 92% 的受访者表示面临挑战，主要是在成本、集成和实施时间等方面。

结论二：拥有更多工具并不意味着能够提高数据安全性或效率，情况恰恰相反

虽然大多数人认为一体化的解决方案更好，但数据安全工具的使用仍然很分散。企业通常使用大约 10 种不同的数据安全工具来降低数据安全风险，而在员工人数超过 5000 人的公司中，这个数字还会更多。

拥有更多的数据安全工具并不总是意味着更高的安全性。事实上，情况可能恰恰相反。一项调查显示，那些拥有 16 种或更多数据安全工具的单位组织，在过去一年中经历的数据事件数量平均达到了 133 起。相比之下，使用较少工具的单位组织平均仅发生了 48 起数据事件，这意味着前者的事件数量是后者的 2.8 倍。

为何会出现这种情况？报告分析指出，首先，各种各样的数据安全工具可能会导致一些盲区，使得某些问

红帽人才工程

Cyber Crime Governance Talent Training Project

工程简介

在“全国网络警察培训基地”的指导下，中国下一代网络安全联盟牵头发起「红帽人才工程」，联合华云信安、美亚柏科、高联通信等知名网络安全企业，围绕“网络犯罪治理、涉网犯罪打击”等相关网络安全课题，持续挖掘、培养、资助、赋能网络安全人才，构建红色基因的网络空间安全人才防线。

申报流程

课题征集 → 课题公示 → 立项评审

研究课题计划征集

研究课题信息公示

研究课题立项评审

申报说明

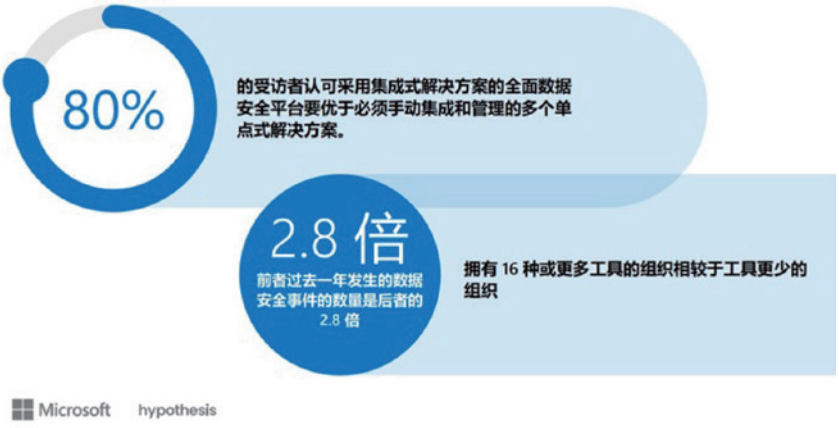
项目资讯

培养对象

政企单位在职人员、高校全日制在校生（含研究生）、互联网企业技术人员、网络安全企业技术人员以及社会网络安全人才...

核心课题

内网攻防、社工钓鱼、远控木马、免杀加壳、情报甄别、资金分析、调证溯源、取证固证、远程勘验、APP反编译、二进制逆向...



题无法被发现，同时也会产生大量的“影子数据”。其次，每种工具都需要专门的人员来进行安装、维护和操作，这会增加工作的复杂性和成本。最后，使用更多的工具也意味着需要花费更多的精力，来整合这些工具提供的信息，制定补救计划，而且在信息传递的过程中可能会有遗漏。

结论三：来自内外部数据（尤其是业务数据）安全事件的压力持续给单位组织带来困扰

尽管数据安全事件的来源可能多种多样，但恶意软件或勒索软件等外部威胁无疑是最常见的。在接受调查的企业中，有一半的企业表示他们在过去的一年里至少经历过一次这样的攻击。此外，还有 41% 的企业表示，他们对未来一年如何防范恶意软件或勒索软件的攻击并没有做好准备。

防止内部风险也是决策者的重要工作。35% 的受访者表示，他们需要更好地保护自己的公司和账户不受内部恶意人员的侵害，还有三分之一的人担心无意中造成的内部问题。虽然恶意内部事件不是数据安全的主要问题，但却是决策者觉得最没有准备好应对的问题之一。

展望未来，有 77% 的企业认为他们的业务数据（如知识产权和源代码）是最容易受到攻击的。这些数据在建立竞争优势和经济收益方面起着关键的作用。然而，识别和分类这些数据是具有挑战性的，因此企业需要更先进的技术来帮助他们发现和保护这些容易受到攻击的敏感数据。

结论四：单位组织需要云和 AI 来推动数字化转型，但它们也是最容易受到攻击的数据位置

云服务和 AI 技术对现在的公司来说非常重要。一般来说，每个公司都在使用大约 147 种云服务，有超过一半的公司已经有了人工智能的发展计划，其中大约三分之一已经开始实施。但是，因为这些技术在发展，所以我们很难搞清楚数据在哪里，这就带来了很多不确定性和风险。

在过去的一年里，有 42% 的企业报告了他们在云存储中遇到了安全问题，而有 31% 的企业报告了他们在使用电子邮件、即时消息或在线会议工具时遇到了安全问题。在这些工具的使用频率和协作程度较高的地方，这些问题似乎更为常见。

与其他领域相比，AI 被认为是最有可能发生数据安全问题的领域，有 27% 的企业在这个领域遇到了安全问题。尽管人们对 AI 有所担忧，但决策者还是看到了它的潜力，尤其是在市场上的供应商正在开发创新的方法来帮助企业通过负责任地使用 AI 提高能力的情况下。

结论五：自动化和 AI 是提升保护能力的可行途径

由于资源和人力的限制，以及工作分配可能不太合理，企业正在寻找技术来帮助他们有更多的时间进行主动性的活动。自动化是一个很好的选择，它可以帮助企业腾出时间来采取更主动的数据安全策略。

74% 的企业希望能够实现半自动化或全自动化的风险缓解机制，这样安全团队就可以在潜在的数据安全事件发生之前，将其影响降到最低，而不需要手动进行审核。通过自动化这些任务，企业可以减轻数据安全团队的负担，让他们能够采取更主动的策略。

将 AI 应用于数据安全也可以帮助企业提高战略意识，更智能地应对未来的威胁。这项技术可以加快对检测到的事件的响应速度，从而为数据安全专业人员赢得更多的时间进行调查。通过利用 AI 和自动化的优势，并转向更加集成的解决方案，企业可以采取更主动的数据安全策略，为打造一个更安全的未来做好准备。

最终结论

1、采用集成式平台，加强数据安全状况

一个集成的数据安全平台应该能够让安全团队，无缝地完成所有这些关键任务：首先是在数字环境中发现和保护敏感数据；其次是检测与此数据相关的重大风险；第三是防止未经授权使用敏感数据，同时不影响合法的业务活动。通过实施综合的数据安全战略，单位、组织可以实现更高级别的保护，同时简化其安全基础设施。

2、采用深度防御方法，由外而内和由内而外防范数据安全事件

单位、组织可以采取深度防御的策略来保护他们的数据，就像博物馆保护珍贵的艺术品一样。例如，博物馆会使用带有威胁智能防御功能的先进监控摄像头来监控访客，票务系统来管理身份和进入博物馆的权限，以及严格的安全措施来保护艺术品。这与保护企业宝贵数据的数据安全控制措施非常相似。无论是来自外部的恶意行为者，还是已经在企业环境中的个人，这些措施都可以阻止潜在的事件发生。

3、利用 AI 和自动化技术升级你的数据安全战略

自动化和 AI 可以帮助组织在数据安全方面变得更加积极主动。比如，利用 AI 帮助识别敏感数据和应用保护策略，包括加密和权限管理。利用 AI 的强大功能来确定与敏感数据相关的重大风险，并战略性地分配资源，以处理潜在的高风险事件。使用 AI 和自动化技术，根据评估的风险自动量身定制防护和缓解控制措施，从而实施适应性更强、更具前瞻性的数据安全战略。

组织更主动与更被动的结果对比	更主动	更被动
过去 12 个月的数据安全事件的平均成本影响	20.7 万美元	33 万美元
在平均不到一个月的时间内完成一项数据安全调查	80%	68%
相信防御控制措施足以防止数据泄露	77%	68%

《安全事件报告》新规解读：事后问责制升级为国家接管风险管理

12 月 8 日，国家互联网信息办公室发布了关于《网络安全事件报告管理办法（征求意见稿）》（以下简称《办法》），其中提到，运营者在发生网络安全事件时，应当及时启动应急预案进行处置。按照《网络安全事件分级指南》，属于较大、重大或特别重大网络安全事件的，应当于 1 小时内进行报告。

《办法》提倡并鼓励有关单位及时、完整、准确地报告网络安全事件，对于迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，应按照相关法律进行处罚，这对于网络安全事件发生后的报告工作具有重要意义，在很大程度上能够减少网络安全事件造成的实际危害。

具体而言，有以下四方面影响需要重点关注。

第一是界定了事件范围，并要求主动报告。

这里的网络安全事件并非狭义上所指的由网络攻击或者其他蓄意破坏所造成的安全事件，而是广义上所有对系统和网络安全造成影响的事件。《办法》第十二条规定，本办法所指网络安全事件是指由于人为原因、软 / 硬件缺陷或故障、自然灾害等，对网络和信息系统或其中的数据造成危害，对社会造成负面影响的事件。

《办法》第十一条规定，发生网络安全事件时，运营者已采取合理必要的防护措施，按照本办法规定主动报告，同时按照预案有关程序进行处置、尽最大努力降低事件影响，可视情免除或从轻追究运营者及有关责任人的责任。

因运营者迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，对运营者及有关责任人依法从重处罚。

第二是明确了报告对象，确立网信部门的监管作用。

《办法》第三条规定，国家网信部门负责统筹协调国家网络安全事件报告工作和相关监督管理工作。地方网信部

门负责统筹协调本行政区域内网络安全事件报告工作和相关监督管理工作。具体如下：

网络和系统归属中央和国家机关各部门及其管理的企事业单位的，运营者应当向本部门网信工作机构报告；网络和系统为关键信息基础设施的，运营者应当向保护工作部门、公安机关报告；其他网络和系统运营者应当向属地网信部门报告；有行业主管监管部门的，运营者还应当按照行业主管监管部门要求报告；发现涉嫌犯罪的，运营者应当同时向公安机关报告。

第三是强调了“1 小时”制度，安全事件应尽快上报。

显而易见的是，网络安全事件拖延时间越长，其危害性往往越大，后续的故障恢复及消除影响等工作也更加困难。因此对于网络安全事件报告的时效性要求非常高。

《 办法 》规定，运营者在发生网络安全事件时，应当及时启动应急预案进行处置。按照《 网络安全事件分级指南 》，属于较大、重大或特别重大网络安全事件的，应当于 1 小时内进行报告。

此外，《 办法 》还专门针对重大、特别重大网络安全事件做出了特别规定。《 办法 》第四条指出，属于重大、特别重大网络安全事件的，有关单位在收到报告后，应当于 1 小时内向上级部门报告。

第四是细化了报告内容，事件调查应全面、细致。

为准确评估网络安全事件造成的影响，为全面统筹后续的响应处置、溯源分析及故障恢复提供有力支撑，报告内容至关重要。《 办法 》第五条明确规定，运营者应当按照《 网络安全事件信息报告表 》报告事件，至少包括事发单位名称及发生事件的设施、系统、平台的基本情况；事件发现或发生时间、地点、事件类型、已造成的影响和危害；初步分析事件原因；下一步所需的线索及进一步采取的应对措施等。

值得一提的是，美国近 2 年也在制定相关法律法规。早在 2022 年 3 月，美国总统签署了《 2022 年关键基础设施网络事件报告法案 》(CIRCIA) ，要求网络安全和基础设施安全局 (CISA) 制定和实施法规，对关键基础设施部门发生的网络安全事件和勒索事件提出了明确的报告时间要求，其中网络安全事件要求在 72 小时内报告，涉及支付赎金的勒索事件在 24 小时内报告。根据法案要求，CISA 须在 24 个月内 (即 2024 年 3 月之前) 发布具体规则。

今年 2023 年 7 月，美国证券交易会员会 (SEC) 通过了网络安全事件披露规则，要求上市公司确定网络安全事件重大后 4 个工作日内提交。如果美国司法部长确定立即披露将对国家安全或公共安全构成重大风险，并以书面形式通知委员会该决定，则可以延迟披露。而就在今年 11 月初，ICBCFS 发生勒索攻击后，找美国安全服务厂商 MoxFive 进行帮助，并立即向执法部门进行了报告。

想要全面掌握上述网络安全事件相关细节、正确做出下一步处置行动并非易事。尤其是在某些高水平网络攻击中，攻击者通常会采用技术手段，隐藏甚至擦除入侵的路径、恶意样本、行为日志等，为事件调查带来非常大的挑战，要求运营单位必须具备准确的安全检测能力、全面的数据搜集能力、强大的关联分析能力。

前不久，奇安信发布的新版态势感知与安全运营平台 (NGSOC) ，可将相关联告警自动汇聚形成完整事件卷宗，自动补充上下文证据，自动映射 MITRE ATT&CK 攻击者战术和技术，自动解读攻击者意图、自动识别关键攻击痕迹、自动评估影响面并计算处置对象，1 分钟内即可完成事件定性、5 分钟完成影响面评估。

与此同时，奇安信威胁情报中心还拥有千万级终端的遥测数据、十亿级互联网资产及应用数据、万亿级历史 Passive DNS 数据及全量漏洞情报库，可进一步补充网络安全事件中有关的上下文信息，确保运营单位能在 1 小时内完成安全事件报告，并对运营单位下一步处置动作提供关键的技术支撑。

关于作者

汪列军

奇安信威胁情报中心负责人汪列军、网络安全事件响应专家，关注恶意代码分析、APT 攻击事件与团伙的跟踪与挖掘，实现安全威胁情报的运营与产品化。

CISO 的风险计算：划清偏执和警惕之间的界限

我在以色列出生和长大，至今仍清楚地记得第一次“冒险”去美国购物中心的情景。停车场停满了车，人们在转来转去，但我却找不到入口在哪里。我过了几分钟才意识到，美国的购物中心与以色列不同，并非所有购物中心的每扇门外都设有武装警卫和金属探测器。

我经常分享这件轶事，以此来阐明网络安全领域中的“健康偏执”概念。正如以色列的政治现实让其公民对人身安全保持持续警惕一样，今天的 CISO 也必须在其员工中培养类似的精神，以做好准备，并保护自己免受不断变化的数字威胁的影响。

CISO 本质上别无选择，只能对所有可能出错的事情保持偏执。相反，组织中的其他人通常不会偏执，直到坏事发生。

有用的警惕和令人衰弱的偏执之间的界限在哪里呢?

偏执需要一个目标

用户要始终保持警惕状态显然既不现实，还会适得其反。在心理层面上，持续的警觉可能会让人精神疲惫，常常导致疲劳和倦怠。当个人始终被要求保持高度警惕时，他们的认知功能可能会下降，生产力会下降，且更容易犯错误，这种警觉疲劳最终会抵消警惕的好处。

在零信任时代，这些趋势只会加剧，我们被要求“永远不信任，永远要验证”。有些人将这一要求发挥到极致，模糊了健康的怀疑主义和令人衰弱的不信任之间的界限。

网络安全中的零信任原则提倡严格的验证和监控，但至关重要的是要将这种战略方法和可能阻碍运营、协作和创新的偏执进行区分。

考虑一下组织在如何保护系统和数据方面，将偏执推进到不健康程度的一些方式。

- **繁重的密码要求：**密码的不足之处如今已为大多数用户所熟知，但密码依然被广泛使用。因此，多数大型组织都要求员工使用并定期更改字符、数字和符号组合的复杂密码。然而，此类安全协议往往忽视了一个现实，即许多身份验证相关安全事件，并不是由于密码被破解，而是通过相对简单的社会工程攻击来实现的。此外，如果强密码在暗网上被泄露，再复杂的密码也无法阻止攻击者执行撞库攻击。
- **追求“零风险”：**与许多战略努力一样，风险缓解往往会经历收益递减规律。过于严格的安全措施可能会降低工作效率，并使用户感到沮丧，导致用户寻找可能引入新漏洞的解决

> 许多身份验证相关安全事件，
> 并不是由于密码被破解，
> 而是通过相对简单的社会工程攻击来实现。

方案。追求绝对安全当然值得称赞，但将资源分配到对降低整体风险最有效果的领域往往更为实际。

· 恐惧驱动的决策：我们常常根据基于恐惧和不确定性的情绪反应做出决策，而不是客观分析和理性判断。比如，员工不小心点击了网络钓鱼邮件的恶意软件，由此导致的恐惧驱动反应可能是严格限制所有员工的互联网访问，阻碍生产力和协作，而不是通过更好的培训或更细致的访问控制来解决问题。

强化人类防火墙

有时，我们忘记了偏执和焦虑在物种集体生存中所发挥的关键作用。我们早期的祖先生活在充满掠食者和其他未知威胁的环境中，适量的偏执使他们更加警惕，帮助他们发现并避免潜在的危险。

当今时代的挑战是如何区分真正的威胁和无休止的虚假警报噪音，确保我们遗传的偏执和焦虑为我们服务，而不是阻碍我们发展。它还要求我们承认并解决安全计算中的人为因素。

正如已故知名黑客凯文·米特尼克（Kevin David Mitnick）所说，“随着开发人员不断发明更好的安全技术，利用技术漏洞变得越来越困难，攻击者越来越多地转向利用人的因素。破解人类防火墙通常更容易。”

安全领导者可以采取哪些措施来更有建设性地利用这些本能，以便能够帮助用户警惕并应对这些现实世界的危险，而不至于不知所措呢?

以下是一些可以提供帮助的策略。

· 拥抱安全从设计开始的策略：宣称安全是每个人的责任，并倡导普遍的安全文化是常见说法，但真正的挑战在于如何运用思维方式并将安全措施整合融入产品和系统开发的各个环节。为了真正实现这一目标，安全原则必须无缝嵌入到流程和实践中，确保其成为本能行为，而不仅仅是强制任务。

· 强调边缘情况：边缘情况是指在预期的系统边界之外发生的情况或用户行为。 比如，大多数 CISO 都会优先考虑防范数字威胁，但如果有人现场造访服务器机房会怎样？随着技术和用户行为的发展，今天被认为是边缘情况的，在未来可能会变得更加普遍。通过识别并应对这些异常情况，安全团队将能够更好地应对未来不确定的威胁。

· 安全培训必须持续：安全培训不应是一次性的举措。制定强有力的政策是至关重要的第一步，但指望人们会自动理解，并始终如一地遵守这些政策是不现实的。人的天性不能记住仅出现一次的信息并根据其采取行动。这不仅仅是提供信息，而是通过反复培训不断强化知识。时不时的推动或提醒，即使感觉像是唠叨，但对将安全原则放在首位，并确保长期合规，发挥着至关重要的作用。

正如作家约瑟夫·海勒在《第二十二条军规》中所写，“你偏执并不意味着他们不再攻击你。”这是一个很好的提醒，在这个不可预测的世界中，健康适度的偏执可能是防止自满的最佳方法。

关于作者

奥默·科恩

Descope 首席信息安全官，在网络安全、研究、软件开发和系统管理方面拥有深厚的背景。

CTFWAR.ORG

网络安全的本质是攻防对抗
讲百遍不如打一遍

---习近平

CTFWAR介绍

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

攻防答题模式

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

积分等级体系

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

极牛技术社群

网络安全技术社群

Cyber Security Technology Community

PLATFORM

网络安全技术社群

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

技术

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

管理

专注在帮助网安工程师在职业发展中，建立体系化的管理知识和技术管理转型路径。

圈子

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

极牛技术站

以沙龙、峰会、圆桌论坛等深度学习的形式进行，满足知识获取与社交需求。

管理加油站

面向管理者的闭门活动，前瞻性的思维和观点，成熟的管理模式与领导模型。

极牛知识变现

通过帮助工程师打造个人品牌，从出书、录课、企培等形式帮助知识变现。

极牛训练营

面向社群成员的线下课程，技术架构、团队管理、商业模式、塑造个人品牌等。

极牛众星计划

社群中优秀的工程师将会被受邀签约极牛众星计划，平台辅助进行品牌孵化。

更多内容敬请期待

境外认知战作战力量及技术装备分析

认知对抗诞生至今，经过了多轮演化，从最早实体空间的谣言散播、传单投送，到现在网络空间的视频图像伪造合成、虚假新闻传播、信息茧房构建等，充分体现了机器学习、大数据等技术带来的重大变革。

为了更好地了解和掌握境外认知作战体系，以美国、俄罗斯等国家及中国台湾地区为研究对象，梳理了其作战力量与主要技术装备，将为我国认知域积极防御提供借鉴和参考。

一、作战力量

美国、俄罗斯、英国等国家，以及中国台湾地区都成立了相应的认知战指挥机构和认知战部队，其职能各具特色，能够有效地与其他军种、兵种进行联合作战。

1. 美国

美军在目前世界各国军队中信息化程度最高，它一直将认知战作为信息化时代的核心作战样式，相关队伍建设也走在世界前列。2010 年 5 月，美军成立网络战司令部，整合分散在美军各军兵种中的网络战指挥机构，并将网络媒体战部队列为其麾下的重要作战力量之一，2018 年升级为第十联合作战司令部。以美海军为例，其网络媒体战部队在电子战、网络战、心理战、军事欺诈和作战安全 5 大信息建设核心综合能力中占据了 3 项，充分反映了其对认知战的重视。

2. 俄罗斯

俄军一直致力于建设一支专业性强、体系完整的信息战部队。2017 年 2 月，俄军宣称组建信息作战部队，其主要职能是保护私有计算机网络和军事指挥通信系统免遭网络攻击。此外，信息作战部队还负责开展舆论战，以增强俄军的网络舆论掌控能力。该部队的规模在 1 000 人左右。2018 年，俄罗斯设立军事政治管理总局，通过重塑军队政治文化、强化信息传播职能等手段，提升俄军心理战、舆论战、信息战的作战能力。

除上述官方作战部队外，俄军还通过“巨魔行动”和僵尸网络（克里姆林宫“巨魔军队”）来执行心理战、舆论战、信息战任务。每个“巨魔”拥有 6 个 Facebook 账户和 10 个 Twitter 账户，每天能够发布 50 条推文，此外，每天还能发布 50 篇新闻报道。

> 随着人工智能、社会科学、虚拟现实、ChatGPT 等新技术的发展，技术装备也朝着智能化、人机协同、无人化方向发展。

3. 英国

英国作为最早开展心理战的国家，长期维持着一支在境外从事心理战的队伍。英军成立第 15 心理作战群，其角色定位于国内外联合作战的支援力量，通过支援区域性和地方性的作战任务，协助开展战场心理作战活动。

英军对其认知作战力量按照战略、战役、战术的层级进行划分。其中，第 15 心理作战群属战略层级，主要负责招募、训练、指导、规划等活动。下辖的心理作战支援分遣队、战术心理作战小组分别属于战役和战术层级。

4. 中国台湾地区

中国台湾方面认为，未来高新技术条件下的心理战是一种集军事行为、政治攻势、电子干扰于一体的全新作战样式，必须依托健全、专业的心理战作战机构来组织、协调和实施。为此，在“台湾地区防务事务主管机关”设立了“信息战策略规划委员会”，负责对包括心理战在内的信息战实施整体指导，并效仿美军的做法，成立心理战研究机构——“陆军心战装备中心”，其下设“信息心战”“计划指导”和“后勤支援”3 个分队，隶属于“陆军总部政治作战部”。

台军心理作战由“台湾地区防务事务主管机关”直接领导，“总政战局”主任统筹规划，一名“总政战局”副主任督导执行。“总政战局”设有“心理战总队”“心理战电视台”“心理战播音大队”“心理战情报大队”等机构。“心理战总队”下辖 3 个心理战大队，每个大队包含 3 个中队 。

二、主要技术装备

从业务层面，可将网络空间认知作战装备分为态势感知类装备、鉴定识别类装备、内容创作类装备、引导干预类装备、仿真评估类装备。

从业务层面，可将网络空间认知作战装备分为态势感知类装备、鉴定识别类装备、内容创作类装备、引导干预类装备、仿真评估类装备。

1. 态势感知类装备

外国军方研制了多款态势感知和战略预警工具，通过实时监控全球新闻媒体、社交媒体等目标，全面获取互联网信息，利用大数据技术分析、挖掘热点事件及敏感信息，实现全球热点网络态势实时监控和热点冲突实时预警。

1.1 美军心理作战自动化管理系统

美军心理作战自动化管理系统主要为心理作战计划制订、心理战实施和心理作战效果评估提供所需的各种信息，具备信息存储、信息分析、信息处理、信息分发等功能。系统包括外国媒体分析、心理战外国地区数据和心理作战效果分析 3 个系统。外国媒体分析系统主要收集目标地区网络媒体信息，并针对该地区的重要事件、公共人物等，提供详细的分析报告。心理战外国地区数据系统能够处理超 1600 个地区的信息数据，并支持动态自动更新。该系统不仅为美国国防部心理作战组织提供外国地区数据，还为参谋长联席会议主席和心理作战指挥机构提供辅助决策。心理作战效果分析系统主要提供对心理作战效果的分析评估能力。

1.2 “社交媒体战略传播”项目

“社交媒体战略传播”项目由 DARPA 发起，通过研究基于新技术的社交网络信息获取，帮助美军实时掌握网络上的热点事件，并跟踪事件的产生、发展、演化全过程，挖掘事件规律，支撑美军进行战略宣传。

1.3 “数据驱动的模型发现”计划

“数据驱动的模型发现”计划目的是让机器学习如何通过数据驱动进行建模。研究用于高效仿真加速计算架构及支撑平台，开发专为大型复杂体系的演化计算所设计的独立仿真处理系统，提供社会化仿真计算能力；研究智能图像分析、反向图像搜索等深度媒体数据挖掘能力，为美国国家安全局（National Security Agency，NSA）等机构认知域分析提供决策支持。

1.4 “开源指示器”项目

“开源指示器”项目（Open Source Indicator，OSI）由美国情报高级研究计划局（Intelligence

Advanced Research Projects Activity，IARPA）发起，旨在开发对开源数据进行连续、自动分析的方法，以检测和预测政治危机、人道主义危机、大规模暴力骚乱、大规模迁移、疾病暴发等重大社会事件。研究人员通过融合来自多个公开数据源和类型事件的早期指标，来对现实世界中的事件进行评估和分析。

1.5 “X 关键得分”计划

“X 关键得分”计划（XKeyScore）是 2013 年覆盖范围最广的网络信息窃取计划，由 NSA 发起。NSA 通过在全球 150 个地区，设置 700 余台服务器实现对普通用户一切网上行为（如邮件内容、网络访问和搜索记录等）的监控 。NSA 人员只需输入目标对象的邮箱地址，就能对其网上行为进行实时监控。

1.6 “混合预测竞赛”项目

“混合预测竞赛”（Hybrid Forecasting Com petition，HFC）研究项目由 IARPA 于 2017 年 8 月发布。该项目旨在综合利用人与计算机系统各自的长处，改进世界范围内地缘政治问题预测的准确度。竞赛过程中，HFC 将尝试各种人－机混合策略，在政治选举、国家冲突、重大疫情等一系列涉及真实世界事件的场景中，将传统新闻报道、社交媒体和财经数据等信息源与人的判断加以融合，对预测结果进行综合分析，以提升准确率。

1.7 Maltego

Maltego 是 Paterva 公司开发的一款交互式社交网络拓扑情报挖掘工具。只需要一个域名，便可对互联网上的资源自上而下地搜索，它可以枚举网络和域的信息，包括域名系 统（Domain Name System，DNS）、互联网协议地址（Internet Protocol Address，IP）等，可以搜集目标的电子邮件、网站、电话号码、组织、公司等信息。

2. 鉴定识别类装备

鉴定识别类装备帮助外国军方对监测到的敏感信息进行检测、识别，并提供本地文化、语言等参考，帮助其正确理解事件。

2.1 “文化感知信息作战防御”项目

“文化感知信息作战防御”项目是 DARPA 提出的重点 AI 项目，旨在形成人类语言能力，使机器能够理解文化背景、社会和情感背景，从而加深对突发事件的态势感知 。该项目能够帮助参战人员快速了解变化的战场情况。

该项目在 2022 年有 3 个计划：一是引入社会和文化背景模型框架，包括共享的价值观、社会规范和跨文化情感表达的差异；二是为新的自然语言处理（Natural Language Processing，NLP）能力制定方法，例如，解释实体、情感和紧迫性的本地化参考，以及叙事和事件的文化意义；三是建立文化上的专业能力，以理解在稳定作业中通常遇到的紧急事件类型。

2.2 “计算文化理解”计划

2021 年 5 月，DARPA 发布“计算文化理解计划”项目，旨在利用人工智能技术，实现一种可以跨文化交流的自然语言处理技术，以协助美国国防部的海外行动。该技术不仅要阅读语言，还要能够理解和解释文化线索，并提供作战建议。

这项工作分为两个主要研究领域：一是解决目前限制人类语言和交流技术应用的一系列挑战，其中包括社会文化规范的发现、情绪识别和情绪变化的检测；二是开发对话协助服务，该服务可以自动检测社会文化背景并检测误解。

3. 内容创作类装备

外国军方综合运用虚拟现实、人工智能等技术，研制内容创作装备，生成多模态宣传制品，为信息引导提供“弹药”支撑。

3.1 动作捕捉系统

近年来，虚拟现实与增强现实技术被广泛应用于模拟各类极端、恶劣环境，提升军事训练环境的逼真度。与系统的行为交互由各类动作捕捉系统实现，其中 Facerig 软件能够实时读入用户的脸部表情和动作及音频输入；体感控制器有 Leap Motion、Kinect 等；Valve Index 手柄、诺亦腾 Hi5 手套等能实现手部动作捕捉；全身动作捕捉有 Xsens MVN 惯性动作捕捉系统，诺亦腾 Perception Neuron 动作捕捉系统等。

3.2 深度伪造系统

在 2022 年俄乌冲突中，DeepFake 首次被运用到军事活动中。由于 AI 技术日渐成熟，包括生成对抗网络（Generative Adversarial Network，GAN）的快速发展和网上各类深度伪造项目算法的开源，市面上大大小小的各种换脸 App 层出不穷，能达到以假乱真之效。

3.3 基于大语言模型的智能对话系统

以 ChatGPT 为代表的大语言模型对话系统，作为当前最强大的文本自动生成工具，凭借其强大的语言理解能力，不仅能够学习、理解人类的语言进行上下文互动聊天，还能够

根据上下文续写文章，并根据聊天内容进行逻辑推理，完成邮件撰写、代码编写、论文输出、图片生成等任务。除 OpenAI 公司的 ChatGPT 外，目前主流的大语言模型还包括 Google 公司的 T5，微软和英伟达公司的 MT-NLG，Meta 公司的 RoBERTa、LLaMA，BigScience 公司的 BLOOM，DeepMind 公司的 Chinchilla 等。

4. 引导干预类装备

外国军方在对目标身份定位的基础上，利用引导干预类装备，将定制化的“弹药”投送至特定的目标人群，实现认知“弹药”的精准释放。

4.1 社交网络舆论发布系统

社交网络舆论发布系统由美军中央司令部牵头研发，能够在社交媒体上以多个虚拟身份进行信息发布。通过伪造 IP 地址登录社交网站，制造虚拟网民是在不同国家和地区登录和发帖的假象，然后使用这些虚假身份发布信息，诱使极端分子接纳他们进入聊天室和论坛，从而渗透进一些组织（比如“基地”组织和塔利班等极端组织）中去散布假消息，干扰其行动。

4.2 “先进概念技术展示”计划

美军特种作战司令部“先进概念技术展示”计划（Advanced Concept Technology Display，ACTD）提出了研制综合信息推送系统，旨在解决禁入区域的心战制品分发问题，其中一项重要的研究内容就是开发基于不同通信设施的信息推送系统，包括卫星通信、手机、其他无线设备及国际互联网。

4.3 “剑桥分析”的政治竞选系统

“剑桥分析”公司在实际操作中融入心理学理论和影响模型，对各个不同的用户群体进行个性化推荐，进而做到悄无声息地影响用户选举行为。通过分析从社交媒体上获取的用户网络痕迹和发帖信息，分析用户行为，整合用户群体画像，分析出每个人的性别、年龄、宗教信仰、兴趣爱好、性格特征、政治理念、支持政党等。

在 2015 年美国总统大选中，“剑桥分析”公司利用数据模型挖掘中间选民，制造“共鸣信息”，实现广告的精准投放，长期向用户的社交媒体推送特定倾向性内容，从而影响他们的投票结果。

5. 仿真评估类装备

仿真评估类装备利用智能仿真技术对作战环境和作战场景进行模拟，并对各种决策效果进行评估，帮助指挥员进行决策。

5.1 “深绿”计划

“深绿”是 DARPA 研究的一套战前、战中一体，方案制订与分析评估一体的作战决策支持系统。“深绿”计划的技术本质是基于实时态势的动态仿真。

通过战场决策仿真和未来战场态势的超实时仿真，系统能够帮助指挥员针对性做出超前决策。

5.2 心理作战效果分析系统

心理作战效果分析系统属于美军心理作战自动化管理系统的一部分。通过分析信息接收者的抽样调查数据，实现对信息制品和作战计划的评估。

三、结语

作战力量的演进、技术装备的发展都是认知作战体系不断完善的过程，随着人工智能、社会科学、虚拟现实、ChatGPT 等新技术的发展，技术装备也朝着智能化、人机协同、无人化方向发展。本文通过归纳总结境外认知对抗综合情况，希望为我国认知防御体系构建提供参考和借鉴。

（选自《信息安全与通信保密》2023 年第 5 期）

关于作者

肖　宁

高级工程师，主要研究方向为网络空间安全。

曾华圣

高级工程师，主要研究方向为网络安全。

第三次网攻断电：配合俄大规模袭击的乌克兰电网攻击

美国网络安全公司曼迪昂特 11 月 9 日发布报告称，隶属于俄罗斯联邦武装力量总参谋部情报总局（GRU）的 APT 组织“沙虫”（Sandworm）在 2022 年对乌克兰一处能源设施发动了复杂的攻击，导致其暂时停电，随后乌克兰各地的关键基础设施遭到广泛的导弹袭击。曼迪昂特表示，此次攻击是破坏目标设施物理运行的网络事件的罕见事例，入侵活动还包括一种前所未见的破坏工业控制系统（ICS）和操作技术（OT）的技术。

曼迪昂特公司新兴威胁和分析负责人内森 · 布鲁贝克表示，此次事件不仅是自俄乌战争开始以来第一起已知的因网络攻击导致断电的公开案例，而且还是首次与导弹袭击同时发生的此类事件。乌克兰政府网络官员曾就俄罗斯此前与导弹袭击协调进行的网络攻击发出警告，但从未详细说明这些行动是如何进行的或影响了哪些设施。曼迪昂特未透露目标能源设施所在位置、停电时间及受影响人数。

> 此次事件不仅是自俄乌战争开始以来第一起已知的因网络攻击导致断电的公开案例，而且还是首次与导弹袭击同时发生的此类事件。

一、伴随大规模导弹袭击的针对乌克兰变电站的网络攻击

曼迪昂特公司表示，2022 年年底该公司处置了一起破坏性网络物理事件，其中与俄罗斯有关的威胁组织“沙虫”针对乌克兰关键基础设施机构开展了攻击；该事件是一次多事件网络攻击，利用一种影响工业控制系统（ICS）/ 操作技术（OT）的新技术；攻击者首先使用 OT 级“离地攻击”（LotL）技术可能使受害者的变电站断路器跳闸，导致意外停电，同时乌克兰各地的关键基础设施遭到大规模导弹袭击；“沙虫”组织随后在受害者的 IT 环境中部署了恶意数据擦除软件 CADDYWIPER 的新变种，从而实施了第二次破坏性事件。

曼迪昂特表示，此次攻击代表了俄罗斯网络物理攻击能力的最新演变，自俄罗斯入侵乌克兰以来，这种攻击能力变得越来越明显；事件期间使用的技术表明俄罗斯进攻性 OT 武器库日益成熟，包括识别新的 OT 威胁向量、开发新功能，以及利用不同类型的 OT 基础设施执行攻击的能力；通过使用 LotL 技术，攻击者可能减少了开展网

络物理攻击所需的时间和资源；虽然无法确定最初的入侵点，但分析表明，此次攻击的 OT 部分可能是在短短 2 个月内开发出来的，表明威胁行为者能够快速开发针对来自全球不同原始设备制造商的其他 OT 系统的类似功能。

二、“沙虫”的网络物理攻击

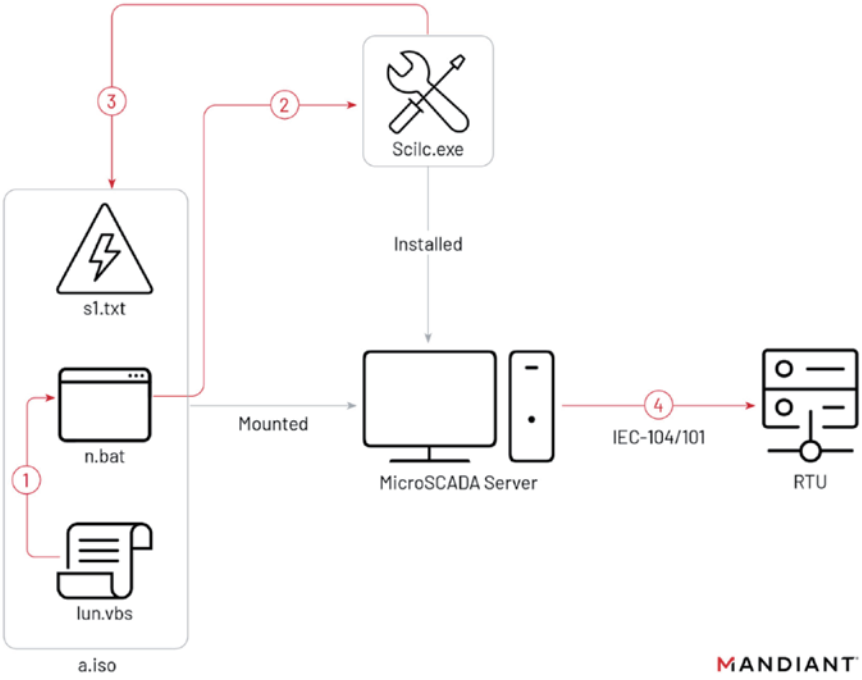
根据曼迪昂特的分析，此次事件的入侵始于 2022 年 6 月或更早，并在 2022 年 10 月 10 日和 12 日导致两次破坏性事件。虽然无法识别进入 IT 环境的初始访问向量，但“沙虫”通过虚拟机管理程序获得了对 OT 环境的访问权限，该虚拟机管理程序为受害者的变电站环境托管了监督控制和数据采集（SCADA）管理实例。根据横向移动的证据，攻击者可以访问 SCADA 系统长达 3 个月。

10 月 10 日，攻击者利用名为“a.iso”的光盘（ISO）映像执行本机 MicroSCADA 二进制文件，试图执行恶意控制命令来关闭变电站。ISO 文件至少包含以下内容：

- “lun.vbs”，运行 n.bat
- “n.bat”，运行本机 scilc.exe 实用程序
- “s1.txt”，包含未经授权的 MicroSCADA 命令

根据“lun.vbs”的 9 月 23 日时间戳，从攻击者首次访问 SCADA 系统到开发 OT 功能，大概有 2 个月的时间段。尽管曼迪昂特无法完全恢复二进制文件实现的 ICS 命令执行，但可以确定攻击导致了意外断电。

事件发生 2 天后，“沙虫”组织在受害者的 IT 环境中部署了恶意数据擦除软件 CADDYWIPER 的新变种，以造成进一步的破坏，并可能会删除取证工件。但是，曼迪昂特注意到该恶意软件部署仅限于受害者的 IT 环境，不会影响虚拟机管理程序或 SCADA 虚拟机。曼迪昂特表示，这是不寻常的，因为威胁行为者从 SCADA 系统中删除了其他取证工件，试图掩盖其踪迹，而恶意数据擦除软件活动会增强这种踪迹，这表明参与攻击的不同个人或操作团队间缺乏协调。

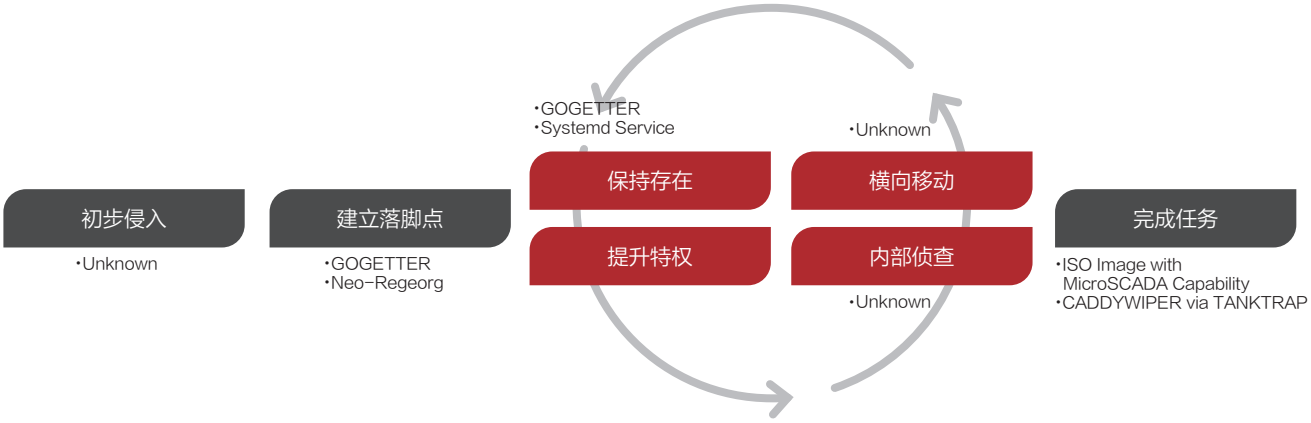


破坏性 OT 事件执行链

三、对俄罗斯进攻性网络能力的洞察

曼迪昂特表示，“沙虫”的变电站网络攻击揭示了俄罗斯持续致力发展面向 OT 的进攻性网络能力和攻击 OT 系统的总体方法；此次事件和 2022 年的 INDUSTROYER.V2 事件均显示出通过简化的部署功能来简化 OT 攻击能力的尝试，在分析一系列详细说明增强俄罗斯进攻性网络能力的项目要求的文件时也发现了同样的尝试。

曼迪昂特称，同样，疑似由俄罗斯联邦武装力量总参谋部情报总局（GRU）发起的 OT 攻击的演变表明，每次攻击的破坏性活动范围有所缩小；2015 年和 2016 年乌克兰断电事件均针对 OT 环境发生了多个离散的破坏性事件，例如，禁用 UPS 系统、破坏串行以太网转换器、对 SIPROTEC 继电器开展 DoS 攻击、擦除 OT 系统等；相比之下，INDUSTROYER.V2 事件



事件攻击活动周期

缺少许多相同的破坏性组件，并且该恶意软件不具有原始 INDUSTROYER 中的恶意擦除模块；同样，“沙虫”在 OT 网络中的活动似乎已简化为仅执行未经授权的 ICS 命令消息，而恶意数据擦除器活动仅限于 IT 环境。虽然这种转变可能反映了战时网络行动节奏的加快，但也揭示了 GRU 在 OT 攻击中的优先目标。

“沙虫”使用本地“离地攻击”二进制文件（LotLBin）来破坏 OT 环境，这显示了技术上的重大转变。使用比此前 OT 事件中观察到的工具更轻量级和通用的工具，攻击者可能减少了开展网络物理攻击所需的时间和资源。LotLBin 技术还使防御者难以检测威胁活动，因为他们不仅需要对引入其环境的新文件保持警惕，而且还需要对已安装的 OT 应用程序和服务中已存在的文件的修改保持警惕。还观察到“沙虫”在其更广泛的操作中采用 LotL 策略，以同样提高其操作的速度和规模，同时最大限度地减少检测的可能性。

曼迪昂特注意到此次网络攻击的时间与俄罗斯的动能行动重叠。“沙虫”可能早在事件发生前 3 周就开发出了破坏性能力，这表明攻击者可能一直在等待特定时刻来部署该能力。最终网络攻击的执行恰逢对乌克兰多个城市的关键基础设施进行了为期多天的协调导弹袭击，包括受害者所在城市。

四、“沙虫”攻击乌克兰变电站技术分析

1、初始渗透和维持存在

目前，尚不清楚“沙虫”最初是如何接触到受害者的。2022 年 6 月，“沙虫”首次在受害者环境中被观察到，当时攻击者在面向互联网的服务器上部署 Neo-REGEORG Webshell。这与该组织此前的活动扫描和利用面向互联网的服务器进行初始访问是一致的。大约 1 个月后，“沙虫”部署了 GOGETTER，这是一个用 Golang 编写的隧道器，使用基于 TLS 的开源库 Yamux 代理其命令和控制（C2）服务器的通信。

在利用 GOGETTER 时，“沙虫”使用 Systemd 服务单元来维护系统的持久性。Systemd 服务单元允许程序在某些条件下运行，在本事例中，它用于在重新启动时执行 GOGETTER 二进制文件。“沙虫”利用的 Systemd

```
[Unit]
Description=Initial cloud-online job (metadata service crawler)
After=
Requires=
[Service]
RestartSec=240000s
Restart=always
TimeoutStartSec=30
ExecStart=/usr/bin/cloud-online
[Install]
WantedBy=multi-user.target
```

Filename	Hash	Purpose
a.iso	Unknown	Contains attacker's files
lun.vbs	26e2a41f26ab885bf409982cb823ffd1	Runs n.bat
n.bat	Unknown	Likely runs native scilc.exe utility
s1.txt	Unknown	Likely contains SCIL commands

配置文件使该组织能够在系统上保持持久立足。在部署 GOGETTER 时，“沙虫”利用 Systemd 服务单元，伪装成合法或看似合法的服务。

2、横向移动到 SCADA 虚拟机管理程序和 OT 攻击执行

“沙虫”利用一种新颖的技术来影响 OT 环境，方法是在产品寿命结束（EOL）MicroSCADA 控制系统中执行代码并发出影响受害者连接变电站的命令。鉴于攻击者使用了反取证技术，无法恢复入侵中的所有工件。

为影响 OT 系统，“沙虫”访问了为受害者变电站环境托管 SCADA 管理实例的虚拟机管理程序，并利用名为“a.iso”的 ISO 映像作为虚拟 CD-ROM。系统配置为允许插入的 CD-ROM 自动运行。ISO 文件至少包含以下文件:“lun.vbs”和“n.bat”，因为这两个文件都在 D 卷中引用，因此包含在“a.iso”中。插入的 ISO 至少导致以下命令行执行:

- wscript.exe “d:\pack\lun.vbs”
- cmd /c "D:\pack\n.bat"

3、部署新 CADDYWIPER 变体破坏 IT 环境

OT 攻击活动 2 天后，“沙虫”在整个 IT 环境中部署了 CADDYWIPER 的新变体。此 CADDYWIPER 变体于 2022 年 10 月编译，包含一些较小的功能改进，使威胁行为者能够在运行时解析功能。

在俄乌战争期间，CADDYWIPER 被部署在乌克兰的多个垂直领域，包括政府和金融部门。CADDYWIPER 是一款用 C 语言编写的颠覆性恶意数据擦除软件，专注于使数据无法恢复并在环境中造成最大程度的损害。

“沙虫”在此次操作中使用 TANKTRAP 从域控制器通过两个组策略对象（GPO）部署了 CADDYWIPER。TANKTRAP 是一个用 PowerShell 编写的实用程序，它利用 Windows 组策略来传播和启动恶意数据擦除软件。

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。

极牛·产业生态

网络安全产业生态平台

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

四大引擎

产服

以产业基地为载体
提供产业生态服务
助力产业发展

产孵

以产业加速器为载体
孵化优质企业
与ToB业务的合作

产投

以产业生态投资
为重要抓手
构建产业生态体系

产研

构建产学研体系
聚焦底层技术创新
全面赋能网安产业

产业生态架构

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

华云信安

以人才梯队为依托，以自主创新为核心，深耕网络空间安全产业

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

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

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

网络犯罪研究中心

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

极牛攻防实验室

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

涉网犯罪对抗　护网重保服务　安全咨询服务　安全保障服务　安全培训服务

丰富的解决方案

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

专业的团队服务

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

众多的行业案例

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

深入的厂商合作

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

全国范围的服务

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

公众号 小程序 官网

网安观察

没有网络安全就没有国家安全

7436084028