内部资料 免费交流

出版物准印证号：京内资准字 2122- L0058 号

SECURITY INSIDER

网安26号院

奇安信网络安全通讯

数字工作新范式

P11

第33期

2023 年 9 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。

安全与数字化便利不能同时拥有?

数字技术的创新与应用目的是让工作与生活变得更加轻松，但越来越多的人数字体验质量正出现急剧下降。

一项由知名密码管理服务公司 NordPass 委托的研究发现，每个用户平均拥有大约 100 个密码，数量比上次调查的数字——70 ~ 80 个密码大约增加了 25%。这个数字从一角度看是积极的正面消息，人们的安全意识不断提高，不再像过去那样一个密码打天下。但工作需要使用多个应用，频繁的验证和复杂的密码，由此带来的糟糕体验，会给数字化带来抵触情绪，甚至引发更高的安全风险。为了便利，总会想办法绕开安全机制。这个时候，人——安全防护这最薄弱的一环，就真的可能引发巨大的风险。

对于网络安全团队来说，应对日益频繁和复杂的网络威胁，实施某些对业务部门来说并不方便的安全措施，或者以其他各种方式阻碍日常运营。这种恼火情绪，可能会从个人层面升级到业务部门层面。不妨考虑一下您自己对要求更改密码的反应——想出又一个既符合长度和复杂性要求，又容易记住的密码；值得关注的是，为了确保安全性而实施的实时验证措施，更是让员工为证明“我就是我”而经历各种令人沮丧的体验。

长期以来，网络安全与数字化便利成为组织内部势同水火、完全对立的两股势力。安全逐渐成为用户的烦恼，业务的障碍，而不是推动者。安全部门常常因为安全措施给业务部门造成的障碍而备受责难。另一方面，员工也往往因为种种不便，而尽量绕开安全措施。对外的数字化服务，也往往因为烦琐的验证而失去潜在的用户。

实际上，提供既安全又方便的数字体验会对客户满意度产生直接的影响。麦肯锡有项研究发现：提供卓越数字体验，同时客户数据安全的企业，可以将客户满意度分数提高 20% ~ 35%。

为了应对网络安全威胁，政企机构当然不能为了便利性而牺牲安全，必须考虑一种具有强大网络安全措施的解决方案，同时确保员工的便利性和生产力，并能够给自己的“客户”提供便利的服务。

奇安信站在业务视角重新思考网络安全挑战，尝试用零信任架构，去解决数字化工作面临的“繁、乱、险”难题。目前，奇安信发布的基于零信任构建的数字化工作入口，可以提供一站式访问、一站式协同工作和一站式保护，而不会影响用户体验或团队生产力，可以让企业告别繁复，拥抱简捷，让访问流程不再“重”。

无论是行政一姐，还是销售一哥，无论是员工还是高管，数字化体验未来将更加便捷、流畅和安全可靠。

安全与便利真的可以同时拥有。

总编辑

李建平

2023 年 9 月 1 日

CONTENTS 目录

安全态势

月度专题

数字工作新范式

在确保信任、保障安全的前提下，创造简捷流畅的数字化体验，让安全与便利不再对立，这就需要站在业务的视角，去重新思考网络安全挑战，让我们看一下奇安信是如何用零信任架构去解决数字化工作的难题的。

《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
攻防一线主编：魏开元
安全之道主编：张少波
安全叨客主编：魏开元
奇安资讯主编：陈　冲
报告速递主编：闫　延
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：2023 年 9 月 26 日

栏目主编　王彪

政策篇

国内，各部委发布产业政策均首倡发展与安全并重，近一月来元宇宙、国土空间规划、货币经纪等领域均有新文件；

国际上，英国两大监管机构达成合作，企业上报网络安全事件可减免监管处罚，这是全球首个实施此类规则的国家。

国内

《信息系统密码应用设计指南》等 4 项网络安全国家标准获批发布

9 月 15 日全国信安标委官网消息，根据 2023 年 9 月 7 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 9 号），全国信息安全标准化技术委员会归口的 4 项国家标准正式发布。具体包括两项修订标准、两项新标准，修订标准有《信息安全技术 网络安全服务能力要求》《信息安全技术 信息安全控制评估指南》，新标准包括《信息安全技术 信息系统密码应用测评要求》《信息安全技术 信息系统密码应用设计指南》。

深圳市人民检察院等五部门联合发布《深圳市企业数据合规指引》

9 月 12 日深圳市人民检察院公众号消息，深圳市人民检察院联合深圳市互联网信息办公室、深圳市司法局、深圳市发展和改革委员会、深圳数据交易所，11 日在“2023 年深圳市网络安全宣传周”启动活动上公开发布《深圳市企业数据合规指引》。该文件共计六章 77 条，包括：总则、数据安全合规管理组织体系建设、数据合规管理制度体系建设、数据全生命周期合规、数据出境合规和附则。该文件立足企业数据法治需求，引导企业开展数据合规管理，提高企业数据合规意识与数据保护水平，对涉及数据各场景制定了全面详细的规范指引。

五部门联合印发《元宇宙产业创新发展三年行动计划（2023-2025 年）》

9 月 8 日工业和信息化部官网消息，工业和信息化部、教育部、文化和旅游部、国务院国资委、国家广播电视总局等五部门联合印发《元宇宙产业创新发展三年行动计划（2023—2025 年）》，以构建工业元宇宙、赋能制造业为主要目标，提出了 5 方面 14 条重点任务。在构建安全可信产业治理体系方面，该文件要求完善元宇宙协同治理机制，强化安全保障能力建设。加强元宇宙安全技术研究，常态化开展安全风险评估，建立安全风险事件处置机制。指导元宇宙企业加强信息安全管理，建立健全违法信息监测、识别和处置机制，加强数据安全和出境管理，规范对用户信息的收集、存储、使用等行为，提升数据安全治理能力和个人信息的保护水平。

《全国国土空间规划实施监测网络建设工作方案（2023-2027 年）》印发

9 月 5 日自然资源部官网消息，自然资源部办公厅印发《全国国土空间规划实施监测网络建设工作方案（2023-2027 年）》，提出了 9 方面任务，指导全国国土空间规划实施监测网络建设。在任务九建立健全安全运维保障体系方面，该文件要求加强基础设施安全保护和网络安全能力建设，强化网络安全态势感知、监测预警、风险评估、事件处置、灾难恢复等能力，建立健全数据安全管理等基础管理制度，加强传输（区块链）加密、密钥管理、隐私计算、脱敏脱密等国土空间数据安全管理技术研发。

五部门联合发布《关于规范货币经纪公司数据服务有关事项的通知》

8 月 30 日国家金监总局官网消息，国家金融监督管理总局、中国人民银行、中国证券监督管理委员会、国家互联网信息办公室、国家外汇管理局联合发布《关于规范货币经纪公司数据服务有关事项的通知》。该文件指出，货币经纪公司应加强数据治理，确保数据安全；同时，规范提供数据标准，提高数据服务质量。该文件要求，经交易机构授权同意后，货币经纪公司可向市场提供交易机构的报价数据和成交意向数据，数据标准应秉承“最小必须、保护客户隐私、促进信息共享”的原则，涉及能够识别交易双方主体的信息不得提供。

《网络安全标准实践指南——生成式人工智能服务内容标识方法》发布

8 月 25 日信安标委官网消息，全国信息安全标准化技术委员会组织编制了《网络安全标准实践指南——生成式人工智能服务内容标识方法》。该文件围绕文本、图片、音频、视频四类生成内容给出了内容标识方法，可用于指导生成式人工智能服务提供者提高安全管理水平。该文件给出了两种内容标识方式，在交互界面内或背景中添加半透明文字的显式水印标识，通过修改图片、音频、视频内容，添加人类无法直接感知、但可通过技术手段从内容中提取的隐式水印标识。

国际

英国两大监管机构签署备忘录：企业上报安全事件可减免监管处罚

9 月 12 日 ICO 官网消息，英国信息专员办公室（ICO）与英国国家网络安全中心（NCSC）签署谅解备忘录，双方就制定网络安全标准和指南、对 ICO 监管的组织改进网络安全施加影响达成合作。备忘录规定，发生数据泄露事件的英国企业，只要不隐瞒事件，而是主动向 NCSC 报告，与 NCSC 合作处理事件，就有可能享受 ICO 罚款减免政策。备忘录强调，如未获得组织许可，NCSC 不得与 ICO 共享组织上报的敏感信息。

美国国防部发布《2023 年国防部网络战略摘要》

9 月 12 日美国国防部官网消息，美国国防部发布《2023 年国防部网络战略》非机密版摘要文件。该文件借鉴了美军基于“前沿防御”政策的大量网络空间行动和俄罗斯对乌克兰战争网络战场的现实经验，阐述了美国国防部为应对当前和未来的网络威胁将采取的四项总体优先事项，包括保卫国家、准备战斗并赢得国家战争、与盟友和合作伙伴协同保护网络领域、在网络空间建立持久优势。这是美国国防部第四次发布网络战略。

美国 NIST 发布 3 项后量子密码学标准草案

8 月 24 日 NIST 官网消息，美国国家标准与技术研究院（NIST）发布了 2022 年 7 月所选定的 4 种后量子密码学（PQC）算法中的 3 种算法的标准草案，公开征求意见。此次发布 3 种加密算法的标准化草案分别为 FIPS 203（CRYSTALS-KYBER，普通加密用途）、FIPS 204（CRYSTALS-Dilithium，数字签名）和 FIPS 205（SPHINCS+，数字签名），将替代易受量子计算机攻击的 3 项现行标准或指南文件 FIPS 186-5、NIST SP 800-56A 和 NIST SP 800-56B。NIST 表示，3 项新算法标准预计将于 2024 年投入使用，第 4 种算法 FALCON（数字签名）的标准化草案也将在 2024 年发布。

美国纽约州发布首个网络安全战略

8 月 9 日纽约州政府官网消息，美国纽约州州长 Kathy Hochul 推出一项全州网络安全战略，计划拨款 6 亿美元（约合人民币 43.53 亿元），用于保护该州数字和关键基础设施免受网络威胁。该战略提出，统一全州范围的网络安全服务，以保证关键基础设施、个人信息和数字资产免受恶意行为者攻击，同时提供一套框架来协调公共部门和非营利组织的行动与资源。该战略还在工业控制系统、医疗保健信息基础设施、市县政务共享服务等方面提出了网络安全要求。

事件篇

上海网信办披露一起“公民个人信息泄露遭境外兜售”案件。上海某政务系统承包商违规将政务数据置于互联网进行测试期间，相关存储端存在高危漏洞，导致大量公民数据遭泄露，相关公民个人信息去年 7 月在境外黑客论坛被披露兜售。

上海某政务系统承包商因公民个人信息泄露遭境外兜售被处罚

9 月 15 日网信上海公众号消息，上海市网信办发文称，某政府信息系统技术承包商违规将政务数据置于互联网进行测试期间，相关存储端存在高危漏洞，导致大量公民数据遭泄露，以致成为境外不法分子窃取政务数据的“供应链”入口，2022 年 7 月，相关公民个人信息在境外黑客论坛被披露兜售。经查，该公司在开展数据处理活动中未能有效履行数据安全和个人信息保护义务，没有建立全流程数据安全管理制度，未采取技术防护措施保障数据安全和公民个人信息安全，导致平台频繁遭受境外远程访问和数据泄露风险。日前，上海市网信办协调有关部门已要求该公司立即下线政府网站页面、关闭相关云服务端口、配合开展网络资产清查，并对该公司作出行政处罚。

美国博彩业巨头凯撒娱乐遭勒索攻击，支付超过 1 亿元赎金

9 月 14 日 Bleeping Computer 消息，号称美国最大连锁赌场的凯撒娱乐遭受勒索软件攻击，被迫支付 1500 万美元（约合人民币 1.09 亿元）赎金。凯撒娱乐披露称，在 7 日发现攻击者窃取了客户忠诚度计划（也叫会员）数据库，其中有大量的客户社会安全号码、驾照号码等身份数据，详细损害仍在调查中。《华尔街日报》报道称，攻击者最初索要 3000 万美元赎金，凯撒娱乐最终支付了一半金额，以避免业务中断和对方数据不外泄的“承诺”。外界对此事意见不一，此前美国政府警告企业不要支付赎金。该公司也是美国证交会实施网络安全事件报告制度以来首批执行的公司。

斯里兰卡国家政务云被黑，近 4 个月数据丢失

9 月 14 日 Infosecurity 杂志消息，斯里兰卡政府云系统“兰卡政府云”在 8 月 26 日遭受一次大规模勒索软件攻击，服务和备份系统被加密，所有使用“gov.lk”电子邮件域名的电子邮件地址（约 5000 个），包括内阁办公室在内都受到影响。系统和备份在遭受攻击后 12 小时内得以恢复，但由于系统在 5 月 17 日 ~8 月 26 日之间的数据没有可用备份，所有受影响的账户在这段时间内的数据都已永久丢失。斯里兰卡信息与通信技术局首席执行官 Mahesh Perera 表示，由于资金限制等原因，“兰卡政府云”使用的软件已经超出维护期，易受各类攻击。在遭受攻击后，该部门已经开始采取措施增强“兰卡政府云”安全性。

香港数码港遭勒索攻击：400GB 数据泄露，科技中心受打击

9 月 7 日南华早报消息，香港科创中心数码港在 8 月中旬遭遇网络攻击，部分数据被锁定。勒索软件组织 Trigona 日前声称，已从数码港窃取超过 400GB 数据，要求支付 30 万美元（约合港币 235 万元）赎金。据悉，被窃数据包括数码港高管的个人身份信息等。数码港表示，已关闭受影响的计算机设备，并启动彻底调查。数码港已就此事于 8 月 18 日上报当地隐私监管机构，但没有对数据泄露规模进行回应。

黑客入侵伊朗 APP 向数百万人推送反政府信息

9 月 1 日 Cyber Scoop 消息，以伊朗为主要目标的黑客组织“黑色奖励”（Black Reward）在 8 月 31 日宣称，针对数百万伊朗人使用的金融服务 APP“780”发起网络攻击，并通过该 APP 向所有用户推送了反政府信息，包括“打倒哈梅内伊！”“我们回到街头，因为革命仍在继续。为了女性、生命、自由。”部分内容还带有 #MahsaAmini 标签。这次网络攻击恰逢伊朗女子 Mahsa Amini 被警察拘留去世一周年纪念日，带有明显的借势迹象。“780”开发商声称拥有超过 600 万用户。

加拿大蒙特利尔市电力系统遭勒索攻击，被迫重建 IT 基础设施

8 月 31 日 The Record 消息，加拿大第二大城市蒙特利尔市的电力服务委员会（CSEM）遭到 LockBit 勒索软件攻击，被迫重建 IT 基础设施。CSEM 称在 3 日遭受攻击，但拒绝支付赎金，目前已重建信息技术基础设施，并联系了加拿大国家当局和魁北克省执法部门。CSEM 谴责了犯罪团伙公开被窃数据的行为，并表示这部分数据对公共安全和该组织运营带来的安全风险很低。CSEM 是一家拥有百年历史的市政组织，负责管理蒙特利尔市的电力基础设施。

全球多处天文台望远镜因网络攻击停运多周，天文科研遭受沉重打击

8 月 18 日美国科学杂志消息，8 月初以来，美国国家科学基金会负责协调国际天文学任务的工作中心发生一起网络攻击事件，导致位于夏威夷和智利的天文望远镜暂时停用。此次事件可能给设备带来物理危险，有 10 台天文望远镜已经完全停止运行，剩下数台也只能进行现场观测。由于天文望远镜无法远程控制，在智利现场工作的人员已经连续两周实际操作仪器。停运给天文科研活动造成巨大冲击，各个科研团队正在集中力量寻找替代方案，否则只能错过关键的观测时间窗口。一些团队可能会派遣研究生赶赴智利，替换这些疲惫不堪的工作人员。

计提 5.5 亿元成本！澳洲知名金融公司因网络攻击损失惨重

8 月 18 日 The Sentiment 消息，澳大利亚知名数字支付和贷款公司 Latitude 在财报中表示，公司因今年 3 月的安全事件损失惨重，不仅计提了 7590 万美元（约合人民币 5.53 亿元）的准备金，并且由于业务中断等原因，上半年净亏损近亿美元。当时 Latitude 报告称，在系统上发现了一些恶意活动，并表示“这些活动据信源自 Latitude 合作的一家主要供应商。”该事件导致 800 万客户的个人信息被窃取，公司业务被迫中断。

南昌某高校发生大量数据泄露案件，当地警方处以 85 万元罚款

8 月 17 日南昌网警公众号消息，南昌公安网安部门工作发现，南昌某高校 3 万余条师生个人信息数据在境外互联网上被公开售卖。南昌公安网安部门立即开展一案双查。经查，涉案高校在开展数据处理活动中，未建立全流程数据安全管理制度，未采取技术措施保障数据安全，未履行数据安全保护义务，导致学校存储教职工信息、学生信息、缴费信息等 3000 余万条信息的数据库被黑客非法入侵，其中 3 万余条教职工、学生个人敏感信息数据被非法兜售。南昌公安网安部门根据《中华人民共和国数据安全法》第四十五条的规定，对该学校作出责令改正、警告并处以 80 万元人民币罚款的处罚，对主要责任人作出人民币 5 万元罚款的处罚。

全球最大金矿和钼矿厂遭网络攻击，生产受到部分影响

8 月 14 日 Industrial Cyber 消息，美国矿业巨头自由港 · 麦克莫兰铜金公司在 11 日披露，正在调查一起影响其信息系统的网络安全事件。一位匿名的公司员工表示，攻击发生在 10 日夜间，导致公司计算机系统关闭。该公司表示，正在评估事件影响，积极采取解决措施，并与“第三方专家和执法部门密切合作”。该公司称，“事件对生产影响有限”。正在计划和实施过渡性解决方案，以尽快保护信息系统的安全。自由港是全球最大金矿、最大钼生产商、主要铜生产商。

漏洞篇

本月微软补丁日发布了 59 个漏洞的补丁程序，其中 CVE-2023-36761 Microsoft Word 信息泄露漏洞和 CVE-2023-36802 Microsoft 流式处理代理权限提升漏洞存在在野利用。经研判，有 16 个重要漏洞值得关注，建议相关产品用户尽快做好自查及防护。

Windows Themes 远程代码执行漏洞安全风险通告

9 月 16 日，奇安信 CERT 监测到 Windows Themes 远程代码执行漏洞 (CVE-2023-38146) 的技术细节和 PoC 已在互联网上公开。由于 Windows Themes 中的数据验证不当，当主题的版本为 999 时，校验 _vrf.dll 文件后会将其关闭再打开，产生竞争窗口，攻击者可以利用竞争窗口将已验证的文件替换为未签名的恶意文件。然后，将加载并执行该恶意 DLL。从而造成远程代码执行。目前，奇安信 CERT 已成功复现此漏洞。鉴于此漏洞影响较大，建议客户尽快做好自查及防护。

微软 2023 年 9 月补丁日多个产品安全漏洞风险通告

9 月 12 日，微软共发布了 59 个漏洞的补丁程序，修复 了 Microsoft Office、Microsoft Exchange Server、Microsoft Visual Studio 等产品中的漏洞，其中 CVE-2023-36761 Microsoft Word 信息泄露漏洞和 CVE-2023-36802 Microsoft 流式处理代理权限提升漏洞存在在野利用。经研判，以下 16 个重要漏洞值得关注（包括 4 个紧急漏洞、12 个重要漏洞），如下表所示：

编号	漏洞名称	风险等级	公开状态	利用可能
CVE-2023-36761	Microsoft Word 信息泄露漏洞	重要	已公开	在野利用
CVE-2023-36802	Microsoft 流式处理代理权限提升漏洞	重要	未公开	在野利用
CVE-2023-38148	Internet 连接共享 (ICS) 远程代码执行漏洞	紧急	未公开	较大
CVE-2023-36792	Visual Studio 远程代码执行漏洞	紧急	未公开	较少
CVE-2023-36793	Visual Studio 远程代码执行漏洞	紧急	未公开	较少
CVE-2023-29332	Microsoft Azure Kubernetes Service 权限提升漏洞	紧急	未公开	较少
CVE-2023-38142	Windows 内核权限提升漏洞	重要	未公开	较大
CVE-2023-38160	Windows TCP/IP 信息泄露漏洞	重要	未公开	较大
CVE-2023-36745	Microsoft Exchange Server 远程代码执行漏洞	重要	未公开	较大
CVE-2023-36756	Microsoft Exchange Server 远程代码执行漏洞	重要	未公开	较大
CVE-2023-36744	Microsoft Exchange Server 远程代码执行漏洞	重要	未公开	较大
CVE-2023-36804	Windows GDI 权限提升漏洞	重要	未公开	较大
CVE-2023-38161	Windows GDI 权限提升漏洞	重要	未公开	较大
CVE-2023-38143	Windows 通用日志文件系统驱动程序权限提升漏洞	重要	未公开	较大
CVE-2023-38144	Windows 通用日志文件系统驱动程序权限提升漏洞	重要	未公开	较大
CVE-2023-38152	DHCP 服务器服务信息泄露漏洞	重要	未公开	较大
CVE-2023-36777	Microsoft Exchange Server 信息泄露漏洞	重要	未公开	较大

Adobe Acrobat Reader 代码执行漏洞安全风险通告

9 月 13 日，奇安信 CERT 监测到 Adobe Acrobat Reader 代码执行漏洞 (CVE-2023-26369)。在 Adobe Acrobat Reader 中存在越界写入漏洞，攻击者可以制作恶意文档诱使受害者打开，成功利用该漏洞将在目标系统执行任意代码。目前该漏洞已存在在野利用事件，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 远程代码执行漏洞安全风险通告

9 月 12 日，奇安信 CERT 监测到 Google Chrome 远程代码执行漏洞 (CVE-2023-4863)。由于 Google Chrome 中的 WebP 组件存在边界错误，远程攻击者可以诱骗受害者访问恶意网站，触发基于堆的缓冲区溢出并在目标系统上执行任意代码。目前，奇安信 CERT 已监测到此漏洞在野利用。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

致远 OA 前台任意用户密码重置漏洞安全风险通告

9 月 8 日，奇安信 CERT 监测到致远官方发布了短信验证码绕过重置密码漏洞的补丁公告，修复致远 OA 前台任意用户密码重置漏洞 (QVD-2023-21704)。未经授权的远程攻击者在已知用户名的情况下，可通过发送 HTTP 请求来触发任意用户密码重置，最终可导致任意用户登录。鉴于此漏洞利用简单且影响范围较大，建议客户尽快做好自查及防护。

Apple 多个产品高危漏洞安全风险通告

9 月 8 日，奇安信 CERT 监测到 Apple 官方发布了多个产品高危漏洞，包括两个任意代码执行漏洞，分别是 CVE-2023-41064 和 CVE-2023-41061，这两个漏洞被称为 BLASTPASS 漏洞利用链，攻击者能够在不与受害者进行任何交互的情况下借助 PassKit 附件进行利用，从攻击者 iMessage 账户发送恶意图像给受害者从而执行任意代码。奇安信 CERT 监测到该利用链正在被 NSO Group 组织的 Pegasus 雇佣间谍软件所广泛利用，现实危害升级，建议客户尽快做好自查及防护。

VMware Aria Operations for Networks 身份认证绕过漏洞安全风险通告

8 月 31 日，奇安信 CERT 监测到 VMware Aria Operations for Networks 身份认证绕过漏洞 (CVE-2023-34039)。Aria Operations for Networks 中存在身份验证绕过漏洞，由于缺乏唯一的加密密钥，具有 Aria Operations for Networks 网络访问权限的攻击者可以绕过 SSH 身份验证访问 Aria Operations for Networks CLI，通过产品的命令行界面可能操纵数据，根据配置的不同，可能导致拒绝服务、配置修改、恶意软件安装或横向移动等。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Windows 错误报告服务权限提升漏洞安全风险通告

8 月 25 日，奇安信 CERT 监测到 Windows 错误报告服务权限提升漏洞 (CVE-2023-36874) 的技术细节和 PoC 已在互联网上公开。由于 Windows 错误报告服务对数据的验证不恰当，经过身份认证的本地攻击者可以构造恶意程序触发该漏洞，成功利用此漏洞可以提升权限至 SYSTEM。目前，奇安信 CERT 已成功复现此漏洞。鉴于此漏洞影响较大，且存在在野利用，建议客户尽快做好自查及防护。

WinRAR 代码执行漏洞安全风险通告

8 月 24 日，奇安信 CERT 监测到 RARLAB WinRAR 发布安全更新，修复了 RARLAB WinRAR 代码执行漏洞 (CVE-2023-38831)。WinRAR 在处理压缩包内同名的文件与文件夹时存在代码执行漏洞，攻击者构建由恶意文件与非恶意文件构成的特制压缩包文件，诱导受害者打开此文件中看似无害的文件（如 JPG 文件）后，将在受害者机器上执行任意代码。鉴于此漏洞影响范围较大，技术细节已公开且存在在野利用，建议客户尽快做好自查及防护。

奇安信 | BEIJING 2022

北京2022年冬奥会官方网络安全赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

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

在确保信任、保障安全的前提下，创造简捷流畅的数字化体验，让安全与便利不再对立，这就需要站在业务的视角，去重新思考网络安全挑战，让我们看一下奇安信是如何用零信任架构去解决数字化工作的难题的。

零信任工作系统：数字工作新范式

作者 | 张少波

在数字化之路上都会遭遇这样的苦恼：根据业务需求，快速上线很多应用，并匹配安全方案。问题随之凸显，比如应用访问入口众多，身份认证烦琐；现有安全方案未针对数字化业务设计，导致不同应用访问缺乏统一入口。满屏的办公软件错综复杂，就像蜘蛛丝一样，剪不断理还乱。完成一项业务审批，往往需要若干次登录、验证，操作烦琐，极易出错，让员工不胜其烦。

如何在确保信任、保障安全的前提下，确保简捷流畅的数字化体验？如何摆脱软件来源混乱、兼容性层次不齐的困境？奇安信给出的答案是：基于零信任构建安全、一站式的数字化工作入口。

一、打工人的数字化烦恼

10 个 ID 8 个难记，这里登录那里跳出，打工人走在崩溃道路……

自从上线新的数字化系统，打工人享受到现代化便利，却又陷入了新的包围圈，面临新的烦恼：公司的数字化系统，让员工又爱又恨。

烦恼 1: 傲娇的密码，考验记忆力

OA、人事系统、财务系统……打工人充实的一天，要和十多个系统与应用打交道，账号和密码就像生日一样要牢牢记住。但问题是，生日只有一个，账号密码却有那么多。

什么，“一码通用”不就好了？真是想的太简单。

平台设置密码的条件五花八门，位数、大小写要求都不一样，有的必须有特殊符号，有的不能有特殊符号……每当系统提示“这个密码太弱了”的时候，以至于有崩溃的打工人说：我的记忆力也很弱，求求你让我用这个吧！

久而久之，很多员工好像已经有了一套账号密码的排列组合，一系列账号和一系列密码。但问题是，常常记不得它们之间的对应关系，每每输错。这些时候，内心就会唱起：“黑

板上排列组合，你舍得解开吗？”

最可怕的是长假归来发现：休假只是一时爽，密码忘了不得了。一旦输入次数错误过多，就被自动判定为图谋不轨的人，于是这一天痛恨于自己设置的密码复杂又难记，苦闷于密码之间的相互打架和相互纠缠，最后都不要想着再登录这个系统了。

密码的傲娇程度，堪比最高冷的缅因猫。它们说失效就失效，有时这边登录那边就登出；还有的要求每过 90 天更换一次密码……这一天，不是在登录的路上就是在登错的路上，被账号密码治得服服帖帖。

烦恼 2: 内网验证，让内心很崩溃

更让人无语的，是内网对于“位置”的执迷。一旦离开了工位，拔下了网线，公司的各个系统，就不认识你了：内网 OA 登录不上了，什么提交审批权限都没了，有种被这个数字化系统给抛弃的感觉。

更有甚者，去外地出差，远程 VPN 听上去很美，可实际却是三步一卡顿，五分钟一认证，一问才知道，VPN 可扩展性有限，远程使用的人一多就容易掉线……打工人真有希望打个飞的回公司，三下五除二，将流程处理完成。

居家办公的时候也是喜忧参半。不用往返通勤，上班幸福感显著提升，可家里的 Wi-Fi 信号明明是满格，但连接内网就是经常掉线，看着流程处理到一半忽然崩溃的系统页面，打工人的内心也是崩溃的。远程找 IT 小哥支持，先是让查一下分配 IP 段的路由信息，再让看防火墙策略。以至于打工人纷纷吐槽：本职工作已是一团乱麻，哪有精力再去学计算机辅助技！

另外，让人崩溃的，还有可怕的神兽：“焰 (验) 狰 (证) 马 (码) ”。作为一个有血有肉的人，而不是一架命冰冷的机器。为了证明这一点，需要付出了很大的代价，全是因为验证码。

虽然公司数字化系统的验证码，比不上 12306 网站那么的花式复杂，在一堆乱码里找字母，在九张图片中找出三张红绿灯……这样的体验依然酸爽。“I 还是 1？ 0 还是 O？ 2 还是 Z？ 9 还是 q？ vv 还是 w？”每天打工人都受困于这样的斯芬克斯之谜。

所以很多人已经傻傻分不清，验证码到底是对抗机器还是对抗人类。

烦恼 3: 不知是内网，还是自投罗网?

自从开始数字化转型之后，公司也进行过不少次新系统使用培训和网络安全意识培训，员工当然也明白公司这些安全措施的制定都有其道理。

随着内网的管控措施越来越严格，防火墙、准入等配备齐全，业务网、生产网、运维网、信创域资源的访问有不同的措施。即使是在内网环境，访问不同的网络、域空间，还需要不同的验证手段，甚至有些业务系统，还必须只能用指定的办公电脑才能连接！

访问不同的业务，就要切换不同的网络地址、切换不同的设备，有时一天切换个五六次都是常事。切换得多了，手指老像是鸡爪一样在敲击着键盘，脑子也开始变成了浆糊。正常工作没累到哪去，却在不停切换中被耗光了精力耐心。打工人的日常，如坠云里雾里。

这样的“数字化”让员工苦不堪言。在数字化系统面前，打工人拥有了若干可能的前置身份：一个偷数据的贼、一个网络攻击犯……一天要证明十几次自己不过是个普普通通、勤勤恳恳的小职员，工作也变成了对记忆力、眼力、心力的极限拉伸。

二、CIO 的数字化烦恼

员工的真实吐槽让 CIO 怀疑人生！

作为 CIO，负责组织内部的业务数字化、网络基础搭建、安全应急响应等。平时花了很多时间倾听各部门需求，解决了一个又一个痛点，业务部门的人盛赞 IT 带来的效率与价值，让 CIO 颇感心安。可无意中听到一番吐槽，却将 CIO 自尊心打回原形。

CIO 烦恼 1：数字化如盘丝洞，软件多了，效率却低了。

数字化转型马不停蹄，但是软件太多了，加剧了来源、入口和使用的分散化，容易让员工找起来晕头转向、用起来不得要领，效率不增反降，与数字化的初衷目标南辕北辙。

“满屏的办公软件错综复杂，在这个盘丝洞里，一个个应用图标、访问入口、信息流、工作流，就像蜘蛛丝一样，剪不断理还乱。真的不清楚，这样的数字化改造究竟是公司的先见之明，还是蜘蛛已经修炼成精？”来自业务线的不时吐槽，让 CIO 压力山大。

更有员工认为，一篇名为《超全——七大类 64 款职场 APP 软件，做高效率“打工人”》的文章，介绍的看似都是打工人的高效利器，但面对满屏的办公软件、一个又一个的客户端，复杂得像进了盘丝洞，只能让人倒吸凉气，搞得没啥工作心情。兴许每一款软件都很高效，但它们“合体”绝对会造成集体低效，这真是对数字化莫大的讽刺。

工作软件多的确是惯常现象，根据一家叫 Okta 的公司的统计，去年企业平均配备了 89 个不同的应用程序，规模大一些的公司是 187 个。

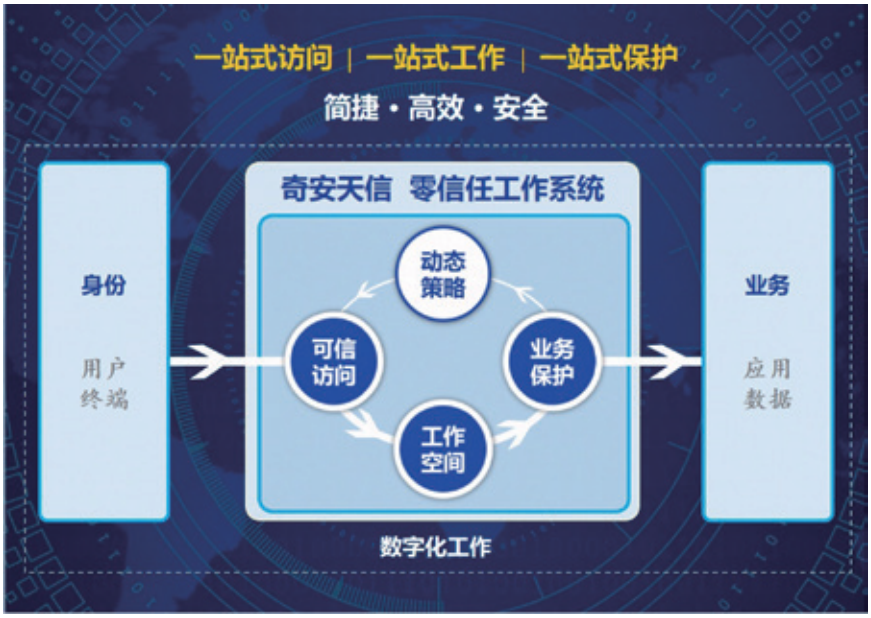
这些数量众多的软件，最后“互相踩踏”，反而影响了工作效率。

“第一是不能协同，不能共享。一个事情需要用好几个软件，做反复流程审批，难道共享信息、打通流程就那么难么？

第二是不同软件不断地切来切去，一天要在切换各种软件上浪费超过一小时，时间浪费还是其次，关键这是一种艰苦的‘情绪劳动’，有人把它概括叫作‘切换税’。

第三是每次访问不同的应用，都需要多次烦琐的认证。N 个应用 N 个入口，N 个系统 N 个密码，上班工作，如同进入无数个大门小门、暗藏若干机关的‘盘丝洞’，一不小心，就身陷其中，绕不出来。

最后就是每次上了新的业务系统，就要申请开通相应权限，有的需要层层审批，有的需要专门打报告，‘反射弧’都很长，一个环节卡在那里，就延迟了整体推进，最终受影响的还是业务办理。”



CIO 烦恼 2: 员工求方便，管理要安全。

业务的需求千差万别，员工的确需要灵活下载安装各种软件。如果全部统一安装，成本太高，耗时耗力；如果靠员工自主安装，其风险指数又会陡然上升，安全隐患难以控制。

尽管公司的 IT 部门已经非常努力，但来自业务线的需求肯定不能全都满足。工作中总要用到些新的办公软件，最后只能靠员工自行到网上搜索下载。很多时候，想要下载某一款软件，结果却看到一堆‘小兄弟’进来了，铺满了屏幕。

这让人想起银角大王的经典段子。银角大王将宝葫芦倒置，喊了一声“XXX！”XXX 应了一声，嗖的便被吸了进去。银角大王查看时，里面除了 XXX，还有 XX 杀毒、XX 压缩、XX 浏览器、XX 安全卫士、XX 游戏大厅等熙熙攘攘一干人。银角大王惊讶道：“怎的来了这么多？”宝葫芦开言：“我就只点了个‘下一步’。”

更危险的是，现在“软件刺客”不少，每次下载软件都战战兢兢，总要判断究竟是美丽善良的七仙女，还是暗藏杀机的七个蜘蛛精。

作为公司的 CIO，安全线就是我的生命线，不出事是基本盘。往年的实战攻防演习，就有一个部门员工被诱导下载了带有后门的软件，直接让对方攻击队轻而易举拿下了靶标。再不解决好工作软件下载来源混乱的问题，今年攻防演习估计成绩肯定好不了。

CIO 烦恼 3，管理需求和实际现状的脱节。

拿信创来举例，国家大力倡导，领导层给我下了死命令，国产化替代要尽快执行。很多国产化系统都以 PC 端为主，但是在数字化工作环境下，除了 PC，大家经常要使用手机等智能终端开展业务，这就意味着终端的碎片化日益严重，而很多系统难以兼容各类型的终端，能力不一致，更不用说体验平滑了。

领导层军令如山，认为实现数字化有助于效率倍增。但是，数字化带来的是大量劳动付出，甚至短期效果不明显，稍有不慎，又惹来业务部门滔滔怨言，我这个 CIO 夹在中间真是左右为难。

三、安全的一站式数字化工作入口

其实，每个公司，都会遇到类似以上的数字化苦恼。如何在确保信任、保障安全的前提下，提供简捷流畅的数字化体验？奇安信给出了答案：基于零信任构建安全、一站式的数字化工作入口。

在 2023 全球数字经济大会上，奇安信正式发布“奇安天信”零信任工作系统（简称“奇安天信”）。它通过“一站式访问、一站式工作、一站式保护”，解决数字化过程中的“重、乱、险”等问题，提供简捷、高效、安全的工作体验，实现业务安全与工作效率并举，构建数字化工作新范式。

奇安天信以身份为基石，充分利用手机令牌、生物特征认证等技术手

基于零信任构建安全、一站式的数字化工作入口，这是奇安信在保障信任、保障安全的前提下，打造简捷流畅数字化体验的新尝试。

段，先验证后访问，确保“可信”——自适应多维身份认证，确保人员可信；安全终端管控，持续环境感知估，确保设备可信；全场景业务流量代理，确保流量可信；动态最小权限业务访问，确保访问可信。

解决了信任问题，再融入“一站式访问”理念，效率问题便可迎刃而解。把各种应用访问的入口统一集成至奇安天信工作系统中，而这个系统的进入，则基于“零信任”的身份验证机制，形成一道闸门，在符合企业的信任策略机制下，无需重复登录，一次性解决了各个应用的信任问题。同时，工作系统提供多类网络流量代理技术，满足不同场景的业务需求，所有流量全部加密，全面收缩业务暴露面。基于此，业务访问的安全性与开放性同时得以保障。

在具体实现上，奇安天信通过“一站式”理念，解决企业数字化三大工作难题。

第一是通过一站式访问，告别繁复，拥抱简捷，让访问流程不再“重”。奇安天信以身份为基石，通过先验证后访问，动态最小权限访问，构建起业务安全新边界；通过自适应多维身份认证，确保人员可信；通过安全终端管控，持续环境感知评估，确保设备可信；通过全场景业务流量代理，确保流量可信；通过动态最小权限业务访问，确保访问可信。

第二是通过一站式工作，告别杂乱，拥抱高效，让工作协同不再“乱”。奇安天信基于场景化、集中式工作环境，实现化繁为简；而轻便化、一站式工作体验，让使用者举重若轻；通过统一资源访问门户，实现业务访问简便易用；而轻量化应用商店更让工作软件随手可得。在协同方面，通过对接业务信息流，实现业务协同高效便捷；通过对各类终端、各种操作系统的全面兼容，使得工作体验无缝跨屏，满足远程、移动等各种场景需求……一系列一体化、协同化的设计，让企业的数字化工作拥抱轻简、效率倍增。

第三是通过一站式保护，告别风险，拥抱安全，让数据资产不再“险”。奇安天信在业务保护方面，以数据为中心，围绕工作空间构建隔离、加固、纵深管控的全链条业务安全保护能力。包括通过工作空间环境隔离、工作软件安全加固等方式，实现数据安全存储、来源安全可控。通过精细业务权限管控、数据流转有效保护，实现敏感数据的识别、脱敏和加密。

同时，奇安天信还基于动态策略实现持续性的风险预警和响应。其中包括通过多属性、多卡点、多手段动态策略管控，快速实现风险闭环，同时满足业务平滑性需求。一旦出现潜在风险，动态策略迅速调整，将业务风险降至最低。这一系列多样化控制手段，能够满足业务平滑开展的需求，并且有效提升风险响应的实时性与有效性。

与和过去关注网络和边界的产品不同，奇安天信以身份为基石、以数据为中心，通过“可信访问、工作空间、业务保护、动态策略”四大核心能力，打造基于零信任的“一站式”安全工作入口，实现“身份化可信访问、工作开展不受限”“场景化工作空间、工作效率不打折”“体系化业务保护、工作数据不泄露”“一体化动态策略、工作风险不延误”等数字化目标。

总而言之，通过部署奇安天信，可以让企业数字化系统在“零信任”架构的保驾护航下，实现一站式访问，从而告别繁复，拥抱简捷，让访问流程不再“重”。无论是行政一姐，还是销售一哥，无论是员工还是高管，数字化体验将更加便捷、流畅和安全可靠。安

零信任：服务数字工作才是硬道理

作者 | 魏开元

自 2010 年提出，零信任的外延就在不断向外扩展。零信任要做的事情已经远不止其内涵强调的“从不相信，始终验证”这么简单。数字化工作成为新常态，零信任架构需要重点解决数字化工作的三大难题。

引发不小争议的论调

说起零信任，就不得不提统治网络安全数十年之久的边界信任。

网络边界将网络分割成内网和外网，内外网之间则通过部署防火墙、IDS、WAF 等安全设备，负责对所有通过的流量和数据进行检测。

通常情况下，内网只有内部员工才可以访问，因此被认为是安全可信的；而外网则充满了木马、病毒等威胁，因此并不被信任。

这种依靠内外网位置来区分信任度，并基于部署安全防护手段的安全模型，被称为边界防护模型。

2004 年，一个在当时明显超越时代的论调，从耶利哥论坛中传了出来：以防火墙为代表的传统边界安全设备已经成为网络发展的阻碍，应该将企业网中的边界消灭。

此言一出，立即引起了不小的争议。反对者始终认为，如果打开网络边界，黑客将肆无忌惮地攻击企业内部网络。

这话并无道理。

2004 年是个什么时间？

在美国，有着 SaaS 鼻祖之称的客户关系软件供应商 Salesforce 艰难上市，市值大约 11 亿美元，与现在可谓是云泥之别；在国内，用友创始人王文京正满世界吆喝，为 ERP 软件站台，向刚刚过去的会计电算化的时代说再见。

刚刚起步的企业信息细化系统就像温室里的花骨朵，这时候有人说应该把门打开，让其感受一下外面世界的风浪。

与此同时，IDC 于 9 月份首度提出“统一威胁管理”的概念，即将防病毒、入侵检测和防火墙安全设备进行全面整合，重新为企业边界树立起一道防守大闸。

一时间，UTM 风光无二。在广泛的质疑声中，取消边界这件事情也就不了了之了。

没有云计算，没有移动互联网，甚

> 自 2010 年提出，
> 零信任概念的外延就在不断向外扩展。
> 零信任要做的事情已经远不止其内涵强调的
> “从不相信，始终验证”这么简单。

至连信息化都是一个非常新鲜的玩意。企业内部网络就是一个封闭的局域网，上班老老实实来公司就行，远程办公？想都没想过。

至少在没有新技术可以取代的情况下，应当维持现状。然而，谁也没有意识到，就是这样一次短暂的争吵，让零信任命运的齿轮就此开始转动，这一转就是二十年。

信任危机：零信任魔盒就此打开

很快，全新的技术就出现了。

2006 年 8 月，在谷歌搜索引擎大会上，时任 Google 首席执行官埃里克 · 施密特首次提出了云计算的概念；同年，亚马逊推出了首款简单存储服务 Amazon S3 以及弹性计算服务 Amazon EC2，正式开启了云服务商用的道路。

如今，谷歌和亚马逊都成为了云计算领域的佼佼者。

云计算的大规模普及，意味着计算、存储等服务的使用，可以像使用水电一样自由，企业的 IT 应用完全可以托管在云端，而不用在内部自建机房。

从这一刻开始，IT 便一步一步地从内部向外部走去。

这还不算完。

2007 年，苹果公司发布了首款大屏智能手机 iPhone，它超越性的搭载了 iOS 操作系统和 App 应用商店，从而正式开启了属于智能手机的时代。

次年 9 月，谷歌正式发布了日后能够和 iOS 分庭抗礼的安卓操作系统 1.0 版本，之后的一个月内，世界上首款搭载安卓系统的智能手机 HTC G1 正式问世。同样是这一年，3G 通信技术开始大规模商用，从而开启了移动互联网的新纪元。

智能手机和移动互联网技术的飞速发展，让手机逐渐开始和计算机一样，成为了人们手中不可获取的多媒体计算终端，BYOD 的办公方式逐渐成为一种潮流。

这也就意味着，员工的手机和计算机拿到哪里，哪里就有可能是办公室。

如果把这两样技术综合起来看，那就是云计算改变了企业资源的部署习惯，移动互联网改变了员工的办公习惯，除特殊情况外（如涉密单位），试图依靠防火墙将二者锁在内网环境中，实际上已无可能。

不管是作为访问者的人，还是作为被访问者的核心业务系统或者数据，都在内外网之间“反复横跳”。

如果说新技术的发展只是让边界信任模型出现裂痕的话，那么接下来发生的事情就是推倒多米诺骨牌的开端。

2009 年，一次名为“极光行动”的网络攻击打疼了谷歌：攻击者利用钓鱼攻击等手段，向内部植入了木马软件，从而监听、窃取关键账户的登录凭证，攻击者则利用这些窃取到的凭证登录到了敏感系统中，执行最终的窃密工作。

这就像开自助餐厅的老板，只要顾客交钱（取得信任）就可以进来随便吃，至于食客有没有浪费食材、有没有私底

> “极光行动”网络攻击
> 引发了谷歌对于网络访问的信任危机，
> 并逐渐蔓延至网络上的各个角落。

下打包，这些事情确实很难限制。偶尔一次两次可以睁一只眼闭一只眼，数量多了餐厅非倒闭不可，必须加以限制。

但企业就不一样了，数据安全泄露事件有一次就受不了，这件事也在事实上引发了谷歌对于网络访问的信任危机，并逐渐蔓延至网络上的各个角落。

信任就像一面镜子，碎掉了是难以重圆的，零信任的魔盒就此打开。

> 所谓的零信任项目只是在网络访问上，
> 保证了内外网信任的一致性，
> 这就和传统 VPN 别无二致；
> 反复验证忽略了用户的实际使用体验，
> 使得员工对于零信任策略产生抵抗心理。

从不信任，持续验证

“网络攻击手段日新月异，针对身份和权限的攻击手段日渐成为主要形式。”奇安信零信任事业部总经理张泽洲表示，传统安全模型基于网络制定安全策略，难以应对针对身份、应用和数据的安全威胁。

在此之前，人们能想起来的网络攻击屈指可数，无非就是冲击波、熊猫烧香这种如今看起来并不高明的病毒，在当时绝对算得上顶尖。

可以这样说，极光行动的发现，揭开了以 APT 为代表的高级攻击模型的神秘面纱，这给边界防御带来了很大的压力。攻击者可以使用各种各样的手段，突破网络边界的重重阻碍。

人们意识到，这种依靠网络位置赋予的信任并不总是正确，总有人能够浑水摸鱼。

很快，时钟被拨动到 2010 年，这对网络安全而言是划时代的一年。

分析机构 Forrester 正式提出了零信任理念，其核心在于“从不信任，持续验证”，即不再以内外网来区分信任度，而是通过多种技术手段，建立访问主体与客体之间的动态信任关系。

有人说，零信任的出现，将网络安全历史分为了上下两部，上部还未结束，下部的画卷已经缓缓展开。

与此同时，谷歌绝对属于给力的行动派。“极光行动”之后，谷歌就一直在探索一种方法，以解决传统边界防御的不足。

功夫不负有心人。从 2011 年开始，谷歌花费数年时间，打造了其内部的零信任项目 BeyondCorp，成为了行业内第一家“吃螃蟹”的公司。

用户必须使用由谷歌提供且持续管理的设备，通过身份认证，且符合访问控制引擎中的策略要求，才能通过专门的访问代理访问特定的公司内部资源。

很难想象，一个 10 年前就上马的项目，时至今日依然是最成功的零信任落地项目之一，成为众多企业争相学习的对象。

后来，谷歌又在 BeyondCorp 的基础上，打造了另一个面向云原生的生产网零信任项目 BeyondProd，实现了更加细粒度的访问控制能力。

随着 BeyondCorp 与 BeyondProd 的成功，零信任作为保护企业网络安全的重要力量，正式登上了历史舞台。

经过数年的发展，到 2020 年 4 月，BeyondCorp 正式作为一个商业项目，出售给谷歌的客户。

破局：安全从 0 开始

谷歌在零信任领域的大获全胜，引起了业界的争相模仿，许多公司都试图复制 BeyondCorp 取得的巨大成功。

然而，在短暂的喧嚣过后，平静的市场似乎再也看不到半点水花。

或许除了未得谷歌成功法门，相比零信任，彼时安全圈有一个“更靓的仔”，叫检测与响应。

这是有原因的。实施零信任道阻且长，即便强如谷歌，前前后后也花费了数年时间，背后所投入的人力、物力更是不计其数。

相比之下，部署几台设备、安装几个软件要容易很多。

更何况，网络安全的本质是攻防双方的对抗，没有一位防守专家会认为，自己的技术就是不如攻击者，凭什么你的攻击手法我就检测不出来?

那几年，几乎所有的安全公司，都希望在检测与响应技术上取得突破，EDR、NDR、SOAR、威胁情报等如今最广为人知的检测与响应技术，都诞生于这个阶段。

尽管如此，业界对于零信任的追求

并没有就此停滞：2014 年，云安全联盟 CSA 发布了《SDP 标准规范 1.0》；2017 年，Gartner 发布了 CARTA 模型（持续自适应风险与信任评估）……这些理念都为零信任的发展指明了道路。

变化出现在 2018 年。

4 月，思科大手一挥，以 23.5 亿美元的巨资，收购身份安全公司 Duo Security，创下了当年网络安全圈的投融资之最；

同年 8 月，国内网络安全领域领军者奇安信正式下场，为零信任站台。

奇安信主要做了两件事情。

· 第一，提出安全从 0 开始，对于 0 的解释有很多，零信任就是其中一个，并正式面向市场发布了奇安信零信任安全架构与整体解决方案；

· 第二，旗下身份安全实验室翻译了《零信任网络：在不可信网络中构建安全系统》这本书，首次在国内全场景展现了零信任架构的独特魅力。

“零信任策略强调以数据为中心，以身份为基石，基于多维属性构建动态策略；同时实现多点精细检控，进行持续评估并实时调整。”作为 Forrester 认证的国内首位零信任战略专家，张泽洲的身影在内部培训、客户现场、会议中心之间“闪转腾挪”，为奇安信零信任战略站台。

奇安信的入局，仿佛推倒了第一块多米诺骨牌，打破了国内零信任市场的宁静，国内安全厂商纷纷下场。

与此同时，在太平洋的另一边，零信任市场的火热程度也不遑多让。

2019 年，RSAC 上主打零信任的厂商就逐渐开始增多，大致有 39 家。而到了 2020 年，RSAC 上打着零信任标签的厂商就已经有 91 家之多，零信任也因此成为了 RSAC2020 热度增长最快的热词之一。

分歧：谁才是零信任正统

很快，蜂拥而入的厂商们开始各显神通。

有人发现账号密码这种静态的身份认证方式不安全，所以打算在身份认证方面大做文章；有人觉得黑客在内网的横向渗透太过简单，所以希望在内网里，也应加入足够细颗粒度的隔离和信任机制，避免黑客入侵由点及面迅速扩散……

美国国家标准与技术研究院 NIST 在其发布的《零信任架构》中，对实施零信任的常见技术路线进行了总结。

第一是软件定义边界 SDP。早在 2013 年，云安全联盟 CSA 就提出了 SDP 的概念。SDP 强调在没有经过身份验证和授权之前，存储应用和数据的服务器都会隐藏在代理服务器后面，

与此同时，代理服务器可以进行动态授信，只有通过验证才可以与服务器建立通信。

第二是增强型身份认证。零信任强调总是验证。过去的身份验证偏向于静态单次验证，简单来说就是输入账密，验证通过后即可建立信任关系。增强型身份认证则不在局限于静态账号密码，而是基于大数据等技术，对用户的各类行为数据进行动态分析，综合判定用户身份是否合法。

第三是微隔离。通俗来讲，微隔离就是将隔离的颗粒度无限缩小，小到每一个应用、每一个进程之间都应该隔离开，而应用与应用之间的每一次通信，都应该被验证是可信的，从而确保加入某个应用被攻破，不会迅速传播至其他应用。

从市场来看，上述三种技术路线都涌现了大批追随者。

许多原本生产单一技术产品的厂商纷纷宣称自己为零信任产品供应商，而类似零信任就等于几种技术叠加之类的流言，让零信任市场还没有真正成熟就陷入到了不少争议之中。

总之，在铺天盖地的炒作下，迅速掀起了一股零信任替代的热潮。

首当其冲的就是 VPN。作为边界信任时代的产物，当企业对内外网一视同仁的时候，VPN 就成为了一个可有可无的角色。

2019 年 Gartner 就预测到 2023 年，60% 的企业将逐步淘汰大部分 VPN，转而使用 ZTNA（零信任网络访问）。想当年，谷歌在取得 BeyondCorp 的成功之后，在第一时间就干掉了 VPN。

或许是受到了这句预言的刺激，在相当一段时间内，用所谓的新技术、新产品搞 VPN 替代，成为了零信任的同义词，仿佛零信任的终极目标就是干掉 VPN。

干着干着，逐渐有人发现了问题。

比如，替换了传统的 VPN，却迎来了一个新的“VPN”，而所谓的零信任项目也只是在网络访问上，保证了内外网信任的一致性，并没有进一步根据实际业务需求，赋予动态的访问权限，这就和传统 VPN 别无二致；再如，过度追求对访问用户身份的反复验证，却忽略了用户的实际使用体验，使员工对零信任策略产生抵触心理……

“ZTNA 当然可以被说成是更好的网络访问产品，但 ZTNA 不等于就是零信任，而搞所谓的 VPN 替代，并不是零信任。”张泽洲说，“技术本身可以解决很多单点问题，但零信任是网络安全信任模型新范式，并不是单点技术问题，更不是搞所谓的 VPN 替代。”

被单点技术、单一产品一叶障目，零信任就变味了。

很多产品都声称可以帮助客户实现零信任，但事实上每家企业的业务相差甚远、IT 环境各不相同、工作方式也不一样，如果不能清晰了解自身的零信任建设需求，零信任项目自然难以取得成功。

说直白一点，技术是技术，业务是业务，这俩根本没穿一条裤子。技术再好，跟业务没穿一条裤子，也遮不住时代进步在业务身上留下的伤疤。

一位不愿透露姓名的 CSO 解释道：“我们实施零信任战略的目标，是为了解决边界信任模型下，因业务开放和内网的过渡信任所带来的安全风险，而不是向我们的员工展示，你看公司用的这个新技术到底有多炫酷。”

黎明：内生安全

为了解决这个问题，2019 年，奇安信在北京网络安全大会期间正式提出了内生安全，其核心就是业务安全和网络安全合一，确保业务持续稳定。

张泽洲认为，零信任架构聚焦身份、信任、访问控制、权限等维度的安全能力，而这些安全能力也是任何信息化业务系统不可或缺的组成部分，所以零信任本应该是内生的。

基于内生安全理念，奇安信形成了以身份为基石、业务安全访问、持续信任评估、动态访问控制这四大核心零信任能力。

就在内生安全提出后不久，一场席卷全球的和天鹅事件“不请自来”，新冠疫情的蔓延，让整个物理世界短暂的按下了暂停键。

然而对大多数人来说，对网络空间变革的切身体验从未像 2020 年新冠疫情爆发以来这般强烈。

首先是远程办公的常态化，彻底将传统网络边界打碎，那些坐在屏幕前上着网课的学生，在平行时空内或许从来都没用过视频会议系统。哪里有联网的人或者设备，哪里就是网络边界。

其次，以疫情之名的网络攻击愈加汹涌，这让以医疗卫生为代表的各行各业防不胜防。

站在网络安全的角度，每上线一个新的系统，就等于为攻击者多提供了一个攻击目标，尤其是因为远程办公导致业务系统不得不对外开放。

这对于尚未准备好公司来说，是一次艰难的选择：前进一步，网络安全没有保障；退后一步，正常业务难以为继。

而且，即便是有良好的网络安全和零信任网络访问基础，这事儿也不是一路绿灯。

比如以前只要管一朵云，现在需要适配多云和复杂终端环境；以前的业务应用相对单一，现在需要覆盖本地应用、小程序、API、微服务等复杂应用形态；以前业务系统上线时间以年计算，而现在需要按月甚至按周计算……

从这个角度来说，网络安全必须是与业务融合内生的，否则网络攻击还没怎么着，网络安全先把业务干崩溃了。

这一点正好为零信任的发展提供了肥沃的土壤。

从全球范围来看，疫情爆发以来，零信任保持着高速增长的势头。IDC 数据显示，2022~2026 年的零信任网络访问市场年复合增长率将达到 30.3%，大幅领先整体网络安全市场的增长速度。

在国内，2020 年 10 月，由奇安信牵头发起的国内首个立项的零信任国家标准《信息安全技术 零信任参考体系架构》正式启动。这意味着继美国 NIST 发布《零信任架构标准》之后，国内零信任也走上了标准化的道路。

数字工作，未来已来

时至今日，零信任的外延依然在不断向外扩展。数字化工作成为新常态，应用场景、IT 环境的变化，零信任要做的事情远不止其内涵强调的“从不相信，始终验证”这么简单。

当前，数字经济已成为推动中国乃至世界经济发展的重要引擎，而数字工作是撬动数字经济的重要砝码。

如果站在业务视角去重新思考网络

> 站在业务视角去重新思考网络安全挑战，零信任架构将重点去解决数字化工作面临的三大难题。

安全挑战，零信任架构将重点去解决数字化工作面临的三大难题。

首先访问流程太“重”。对于任何一家企业而言，一味追求反复的身份验证，只会使得身份认证流程过于“沉重”，员工登录不同的系统需要多次重复输入账号密码，用户体验极差。如果身份验证策略强度过高，会导致员工对相关制度的反感甚至抵触；而强度如果过低，则极易导致账户被破解。

其次工作协同太“乱”。不同的工作使用不同的软件，比如，报销使用财务系统、招聘使用人力系统、销售使用 CRM 系统……不同的员工使用不同的系统，其权限分配十分复杂；而且使用非可信来源工具、应用也屡见不鲜，员工自行下载安装各类工作软件，来源不明，容易导致恶意软件入侵，给企业数据造成极大的安全隐患。

最后数据资产太“险”。传统的边界信任模型自然不必多说，静态的安全策略、粗颗粒度的管控手段，很难对业务数据进行有效的管控和安全防护。而且，即便是企业采用零信任架构，如果不能全面覆盖新应用和新业务，如微服务、API 等，依然会导致企业面临着巨大的数据泄露风险。

所以奇安信发布了“奇安天信零信任工作系统”，基于零信任构建安全的数字化工作入口。作为以安全内生为根本的新一代零信任产品，奇安天信通过“一站式”理念，即一站式访问、一站式协同工作和一站式保护，解决数字化工作面临的上述三大难题。

“我们希望奇安天信能够打破业务和安全之间长期割裂的状况，将零信任很好地融入到数字化工作场景之中。”张泽洲说，奇安天信以身份为基石、以数据为中心，通过“可信访问、工作空间、业务保护、动态策略”四大核心能力，打造基于零信任的“一站式”安全工作入口，帮助客户实现“身份化可信访问、工作开展不受限”“场景化工作空间、工作效率不打折”“体系化业务保护、工作数据不泄露”“一体化动态策略、工作风险不延误”等数字化目标。

这正是数字工作的未来，未来已来。

据 IDC 发布的《中国零信任网络访问解决方案技术评估，2023》，奇安信零信任网络访问解决方案在所有六项关键技术能力评估中均取得最优成绩，成为所有入围企业中，唯一获得五个五星、技术评估雷达图最接近正六边形的企业。

在2023年北京网络安全大会上，奇安信集团董事长齐向东表示，数智安全要以内生为本，自我进化，从关注 IT 转变成关注业务、从关注设备转变成关注“人”、从关注建设转变成关注运营，而这正是零信任不断前进的方向。安

“钢铁长子”在数字化浪潮下的终端安全之路

作者 | 张少波

“共和国钢铁工业的长子”“新中国钢铁工业的摇篮”“雷锋同志唯一工作过的企业”……提到鞍钢集团，人们总能想到一连串沉甸甸的荣誉称号。作为中央直接管理的国有大型企业，鞍钢集团是新中国第一个恢复建设的大型钢铁联合企业和最早建成的钢铁生产基地，为国家经济建设和钢铁事业的发展作出了巨大贡献。新中国成立初期，曾为国家建设贡献了三分之二左右的钢材，并创造了我国钢铁工业无数个“第一”：新中国第一炉钢水、第一根钢轨、第一根无缝钢管……

近年来，伴随着人工智能等新科技革命浪潮，数字经济正在加速向千行百业渗透。党的二十大报告更是指出，“加快发展数字经济，促进数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群”。在钢铁行业步入高质量发展阶段背景下，数字化、智能化有助于产品质量的改善和生产效率的提升，已逐渐成为企业竞争力的重要指标之一。

图：鞍钢集团

鞍钢集团是中国首批“创新型企业”，也是中国首家具有成套技术输出能力的钢铁企业。近五年来，集团将数字化转型视为新一轮钢铁工业革命的核心竞争力，持续实施数字化、智能化项目，降低生产制造成本，提高全要素生产效率，提升经营管理水平，加快实现数字蝶变。然而，随着信息化建设和 IT 技术的快速发展，各种网络应用的日益增多，病毒、木马、蠕虫及黑客攻击等，不断威胁着鞍钢集团内部网络资源，使得企业网络的安全边界迅速缩小，开放的内部网络访问将影响企业 IT 基础设施的稳定运行和数据安全，因此需要构建新一代的内部终端准入安全防御体系。

对此，鞍钢集团通过牵手奇安信部署统一终端网络准入管理系统，实现对鞍钢内网终端进行准入管理，最终构建可信、可管、可视的终端安全防护体系，为数字化转型过程中的同行，打造终端安全准入建设的标杆示范。

图：数字鞍钢

制定五大目标，构筑终端安全防线

将钢铁、冶金等国民基础行业作为网络攻击目标，近年来可谓愈演愈烈，成为全球网络威胁新趋势。2022 年 6 月，伊朗国有钢铁寡头公司胡齐斯坦由于受到“网络攻击”后引发的“技术问题”，工厂不得不停工，造成了巨大损失。7 月，攻击三家伊朗钢铁制造企业的黑客组织 Predatory Sparrow 发布了近 20GB 绝密数据，其中包含该公司重要文件等。同年 10 月，欧盟最大铜矿公司德国铜生产商 Aurubis（中文名为奥鲁比斯）遭到网络攻击，IT 系统被迫中断服务。

“公开的事件仅是冰山一角，钢铁行业已成为数字化时代网络安全的新战场。” 鞍钢集团管理与信息化部副总经理蔡恒君认为，钢铁业不仅是国民经济的支柱性产业，也属于整个工业产业的核心基础，它关联着众多上下游企业，一旦遭受攻击破坏，将会影响整个产业链和生态，甚至关乎经济发展、社会稳定乃至国家安全。因此，随着钢铁行业数字化水平和生产效率的不断提高，对于鞍钢集团而言，亟待构筑更可靠的网络安全防线，来应对黑客、病毒、蠕虫等外部威胁，以及员工数据泄露等内部威胁。

据介绍，终端网络准入工作是鞍钢集团 2023 年推进的一项重点工作，集团的各二级单位，将该项工作列入重点任务清单，旨在对接入网络的终端设备进行实时监测和管理，保证网络安全和信息安全。

面对下属单位较多、网络层级不规范、交换机与要求不符等困难，集团发动各单位迎难而上，明确分工，落实责任，全力推进网络终端准入工作。

鞍钢集团管理与信息化部梁会霞表示，结合集团终端安全面临的威胁和现状，最终确立了五大目标。

第一个目标：实现端口级别的接入管控

在项目实施之前，任何外来人员或客户只要将计算机插入网线，就可以进入内部网络，进行散播病毒、网络攻击等操作，给集团内网造成极大的风险，因此需要实现端口级别的接入管控来解决以上问题。同时也满足了国家《网络安全法》等政策合规要求。

第二个目标：实现终端基线策略合规性检查与修复

项目实施前，终端上不能及时更新补丁，以及配置弱口令、开放高危端口等，这些情况均会给攻击者留下入侵机会，攻击者轻松获取低安全基线终端管理权限，从而对高价值目标发起攻击。如何在行政命令手段之外，能通过技术手来段提升内网终端安全软件覆盖率，提升终端策略安全级别，从而更好地抵御入侵。

第三个目标：实现不同网络访问权限限制

实施之前，缺乏基于用户身份的权限管理机制，不同身份的人都可以访问同样的服务器资源，往往导致隐私数据被窃取，泄密事件风险，故需要实现不同网络访问权限限制来解决以上问题。

第四个目标：实现人机对应，实名管理

实施之前，管理员不能准确掌握人员与终端资产的对应关系，更无法跟踪资产变更情况，例如硬件新增、丢失情况等。因此，集团需要一种方法关联人与终端资产的对应关系，以及对硬件变更准确和实时监控，并及时预警，方便管理部门审计。

第五个目标：全面掌握终端信息资产

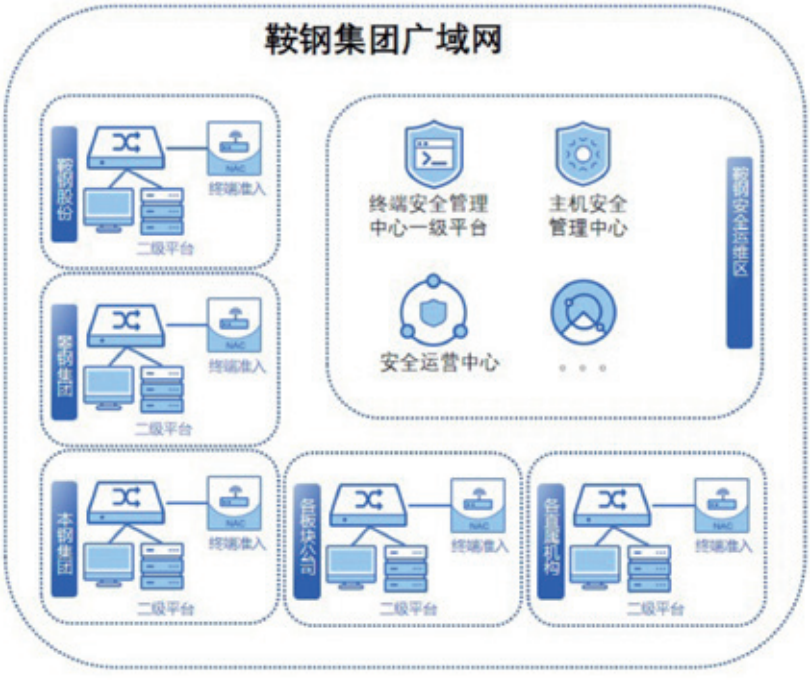
随着鞍钢集团的不断发展，计算机的数目在不断增加，海量终端的资产信息难免出现无法统计的现象，即使是管理部门所获取的资产信息也由于时间的差异无法实时统计。这就导致设备资产情况不清晰，无法做到统一接入安全管理，经常会发生资产信息不全、丢失等情况，更无法建立完善的设备规范化接入管理机制。因此，需要通过一种方法使管理员可以轻松把终端硬件资产信息实现全面的自动收集（如计算机硬件信

息、软件程序信息、操作系统配置等），快速统计分析（资产变更自动监控，及时反映企业资产变化状况），快速生成满足各个部门所需要的资产报表。

覆盖数万终端、核心二级单位，实现可防、可管、可视

针对各单位网络改造牵涉面广、技术复杂、问题排查难度高等不利因素，鞍钢集团管理与信息化部邢立刚组织集团各下属公司，分别建立准入专班团队，和国内领先的网络安全企业奇安信紧密合作，协同各单位全面梳理整改历史遗留问题，累计更换不合要求的网络交换机数百台，并借助准入平台验证功能对整改结果进行全网络合规性验收。

在终端准入建设中，如何将对业务的影响降至最低、实现无感知上线，是该项目最重要的挑战。由于单位分散、终端数量众多，网络终端准入项目在实施过程中重点考虑了不影响鞍钢集团各职能中心和基层单位的工作业务。对此，集团和奇安信紧密合作，充分利用节假日休息时间加班加点，做到了无感切换，顺利完成约数万台终端的网络终端准入工作，实现全覆盖。



图：鞍钢集团广域网

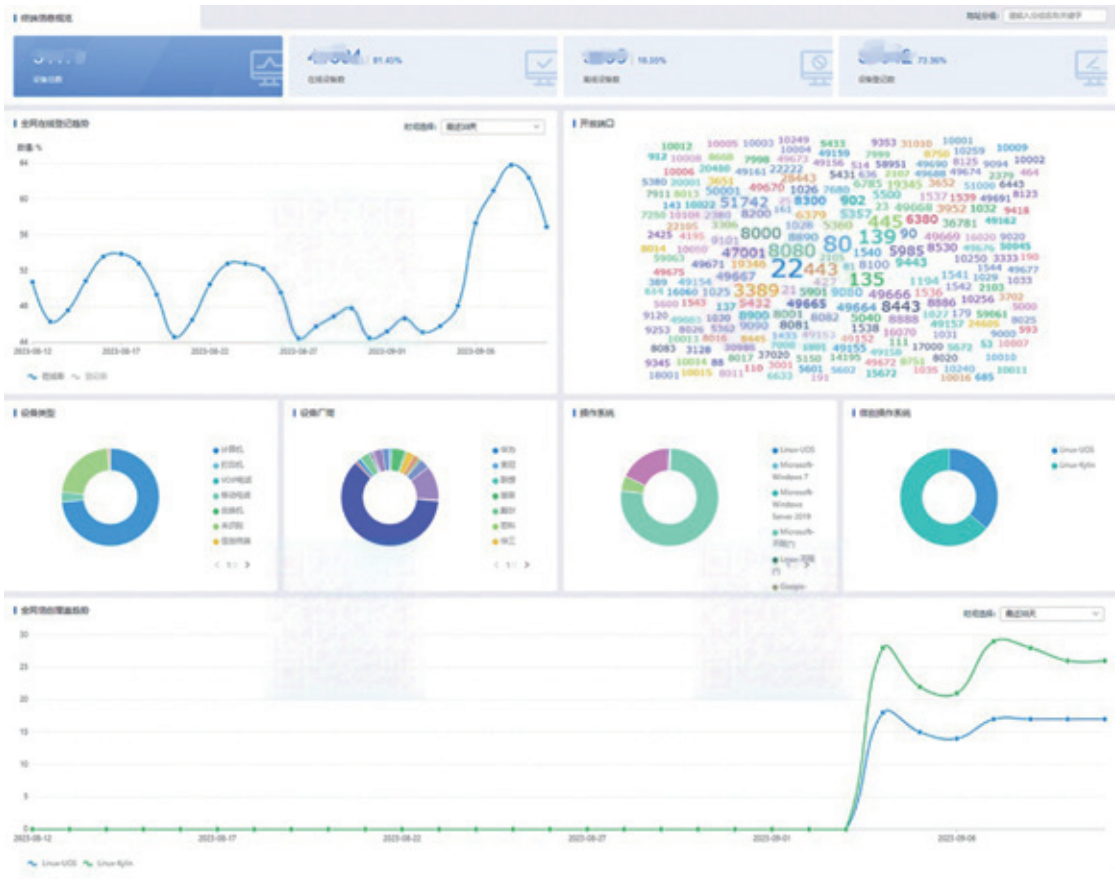
邢立刚表示，截至目前，鞍钢统一终端网络准入管理系统已部署一级平台及数个二级平台，全面覆盖鞍钢集团下属核心二级单位，几万台终端设备。新的准入系统在安全合规、可管理性、可视化等方面都作了很好的保障。

首先在安全保障方面，统一终端网络准入管理系统通过丰富的设备发现识别及准入控制手段，能够准确发现网络内接入终端，验证接入终端的身份，判断终端与用户的安全与合规，动态控制入网终端及用户的网络访问权限，从而确保整个内网环境的安全。

同时，统一终端网络准入管理系统通过对网内设备进行身份分析、合规检查及流量控制等安全检查或控制，协助集团及时发现网络内各类设备的异常并进行处置，提升内网设备抵抗入侵的能力。

其次在管理方面，统一终端网络准入管理系统使用各类手段强制终端入网时必须进行实名认证或登记，同时配合设备发现与识别功能对设备信息变更的实时感知，无论设备的 IP 如何变化，准入系统均能提供准确的设备与使用人关系记录。当监管部门提供特定时间段内的风险 IP，通过在准入系统上查找对应时段的认证记录，即可快速定位责任人。

最后在可视化管理方面，统一终端网络准入管理系统一级平台依托数据可视化技术，使集团内网终端整体安全态势一目了然，威胁和异常清晰可见，



图：统一终端网络准入管理系统可视化运营界面

还能将平台自有运营的终端病毒情报、终端漏洞情报等终端安全情报库与本地终端上的安全数据结合在一起，进行汇总分析，成为集团终端安全运营和安全分析的重要工具。

助力国产化平滑迁移，持续保障接入安全

据梁会霞介绍，鞍钢集团逐步将终端替换为国产化设备，安全准入系统提供各操作系统及国产化平台下的客户端软件，同时依靠准确识别的设备操作系统、准入系统可准确地向未安装客户端软件的各操作系统终端 / 信创终端推送对应的客户端安装页面，并通过多种手段准确识别网络中的各终端和信创终端，针对不同终端执行不同入网策略，保障国产化替代过程中的网络接入安全。

展望未来，鞍钢集团还将继续建设终端安全一体化管理平台。准入系统将与终端安全一体化管理平台联动，通过联动可强制内网中的 PC 机安装客户端。一体化管理解决终端杀毒补丁等安全需求的同时，通过杀毒软件安装、违规外联等基线策略的检查，有效管控内部资源违规访问和泄露的问题，防止违规终端访问核心业务资源，保障入网终端安全可信，合规入网。

不久前，工业和信息化部、国家发展改革委、财政部、自然资源部、生态环境部、商务部、海关总署等七部门近日联合印发《钢铁行业稳增长工作方案》，明确指出要加快推进数字化转型智能化升级，开展钢铁行业数字化转型三年行动，促进钢铁企业数字化、网络化、智能化改造升级，建设一批智能制造示范工厂，打造一批制造业数字化转型标杆，形成一批可复制可推广的典型案例。随着数字化转型、国产化替代等浪潮在钢铁行业的开展，安全成为不可忽视的重要组成部分，鞍钢集团联手奇安信打造的统一终端网络准入管理系统，很好地解决了国产化过渡期面临的复杂安全风险、合规准入、统一管控等难题，为同行开辟出一条值得业界借鉴的道路。安

数字化转型下中关村银行安全办公协同的探索与实践

作者 | 北京中关村银行　许伟涛　罗进权　翟栋男

2021 年 12 月和 2022 年 1 月，中国人民银行《金融科技发展规划（2022—2025 年）》（以下简称《发展规划》）和银保监会《关于银行业保险业数字化转型的指导意见》（以下简称《指导意见》）先后印发，将数字金融发展的目标指向对数字经济发展的支持，将金融科技定位在深化金融供给侧改革、更好地服务实体经济、实现高质量增长的重要创新力量。

中关村银行的“一体化链接中台”建设

中关村银行积极学习和贯彻落实监管部门《指导意见》，于 2022 年 1 月成立了以行领导和各部门负责人为主体的数字化战略领导小组，加强数字化转型统筹协调和组织实施。数字化转型工作是一个复杂系统工程，对银行而言，数字化建设走在各行业前列，大多数同业已实现计算软 / 硬件架构解耦、集中资源池共享及虚拟化建设，并大量采用自动化技术，形成较高的数字化能力，成效显著。而在日常办公运营领域，很多银行并未列为重点建设方向，认为其重要程度不高。北京中关村银行针对自身信息化建设现状分析，认为办公数字化转型可以整合资源，提升银行整体办公效率，降低成本，因此规划建设“一体化链接中台”。在数字化战略领导小组的领导下，中关村银行开始推动办公数字化转型“一体化链接中台”建设工作，并将该项目作为中关村银行数字化转型 1 号工程。

“一体化链接中台”定位办公系统中台，建立数字化门户入口集成各办公系统及工具，利用消息通知、在线会议、办公文档在线协同等功能触达员工，黏合各部门办公人员。此外，利用该平台的链接能力还可以进一步对外链接客户群体和关联企业，加强上下游沟通能力及效率，逐步建立完整生态。数字化协同智能安全管控平台方案作为“一体化链接中台”的安全部分，为中台提供安全支撑能力。

随着办公数字化转型不断深入，“一体化链接中台”跨网络域、跨系统，乃至打通客户和关联企业的特性对“分区

> 在数字化战略领导小组的领导下，
> 中关村银行开始推动办公数字化转型
> “一体化链接中台”建设工作，
> 并将该项目作为中关村银行数字化转型 1 号工程。

分域”的传统安全理念产生了挑战。如远程办公、业务处理、开发测试等场景均需要用户在不同网络间访问。数字化转型帮助中关村银行获得新的业务增长点，但同时也蕴含着巨大的网络安全风险，当前通过网络隔离、重边界的防护理念已经不能满足业务的发展需要。为保障“一体化链接中台”的安全性，中关村银行综合利用零信任技术、沙箱技术创新，寻求数字化协同智能安全管控平台方案。

为保障 “一体化链接中台”的安全性，
中关村银行综合利用零信任技术、沙箱技术创新，
寻求数字化协同智能安全管控平台方案。

开发建设过程面临的挑战

中关村银行现有网络按照功能区域划分为生产环境、开发测试环境和办公环境，相互之间隔离，形成不同的网络应用：生产环境使用专用终端访问；行内办公系统使用办公终端访问；开发测试环境使用云桌面，开发人员通过办公终端登录云桌面进行开发工作；远程办公使用 VPN 接入实现。

1. 传统网络边界隔离凸显不足

中关村银行的网络模型采用传统的网络分区和隔离的边界防护模型，随着“一体化链接中台”不断推进，意味着数据必须在多样化的业务、平台、设备、用户之间流动，导致网络安全边界变得模糊，难以通过边界防护实现灵活、动态的访问控制需求。

2. 接入设备多样性导致安全风险增大

数字化转型促使网络进一步开放，随时随地接入网络的人员、设备多样性导致安全可控性降低，大量业务数据存放在终端上，一旦发生敏感数据泄露，将会给金融机构带来巨大影响。

3.VPN+ 云桌面方式问题凸显

受疫情影响，远程办公大规模使用 VPN 和云桌面。近年来，VPN 不断被爆出安全漏洞，在中关村银行多次渗透测试中也发现了此类问题，攻击者利用 VPN 漏洞极易绕过 VPN 用户验证，直接进入 VPN 后台，将 VPN 作为渗透内网的跳板，进行肆意横向移动。

云桌面需要部署高性能服务器及虚拟化平台管理工具，每年需要采购云桌面维保服务及虚拟化授权许可，每年都需要花费大量资金。

持续创新，构建数字化协同智能安全管控平台

数字化转型驱动了系统集成的需求激增，数据流动性需求变大，传统的安全解决方案越来越不能满足业务需要。在当前新技术、新场景下，中关村银行立足于信息化和网络安全的双重定位，摒弃传统安全解决方案，尝试综合利用新技术，创新性地解决业务和安全需要。

1. 系统建设思路

调研过程中，中关村银行发现，很多企业将零信任定位为 VPN 的升级替换产品，作为远程访问使用。“一体化链接中台”作为链接远程办公、业务处理、开发测试等场景的平台，模糊了网络边界，零信任主流的远程访问场景不足以满足中关村银行的需要。中关村银行综合考虑后决定探索新的零信任使用场景。无企业网络特权的模式，用户和设备的访问都基于权限，与网络位置无关，所有对企业资源的访问都是基于设备状态和用户权限进行全面认证、授权和加密。在此种模式下，网络边界被模糊化，一切基于权限。此种思路符合中关村银行一体化链接中台建设目标，工作中打破壁垒，解决日常工作中沟通协同痛点。

零信任架构可以有效地解决传统基于边界的网络安全架构在数字化转型下面临的困境，对用户业务系统安全访问提供了强有力的保护。相比之下，终端作为零信任架构下“信任”关系链中重要的一环，目前只提供了身份认证、终端环境安全感知等能力，缺乏对落地业务数据的有效保护，成为了零信任方案下的安全短板。针对这一需求，中关村银行考虑在零信任方案基础上引入安全工作空间技术，用户在访问不同安全等级的业务系统时，通过安全工作空间，在终端建立相应的安全工作环境，通过

加密、隔离、管控等手段，保障落地业务数据的存储、使用和流转安全。

2. 项目建设平稳推进

基于上述建设思路，中关村银行设计了一套数字化协同智能安全管控平台方案，在全行部署一套包含可信代理网关、可信访问控制台和安全工作空间的安全系统，通过零信任技术实现网络层的访问控制，通过安全工作空间实现终端层面的隔离控制，使得同一台终端既可以从任意位置访问生产环境、开发环境、办公环境，而且不会因使用同一台终端造成各个环境间相互联通，同时能够满足监管对于生产环境、开发环境、办公环境隔离的要求。数据在各环境间流转需要审批，降低了数据泄露的风险。

（1）统一部署、集中管理

管理端层面，在互联网 DMZ 区和内网办公区部署零信任 TAP（零信任可信应用网关），分别处理来自互联网或内网的访问请求。内网部署 TAC（零信任可信访问控制台），统一控制部署在 DMZ 区、内网办公区的可信应用网关。内网部署一个安全工作空间策略服务器，用于安全工作空间策略的管理。

终端层面，在全行办公终端部署包含零信任和安全工作空间功能的统一客户端，零信任和安全工作空间权限及策略，按照用户及其所使用的终端类型的不同，分配对应的权限和策略。

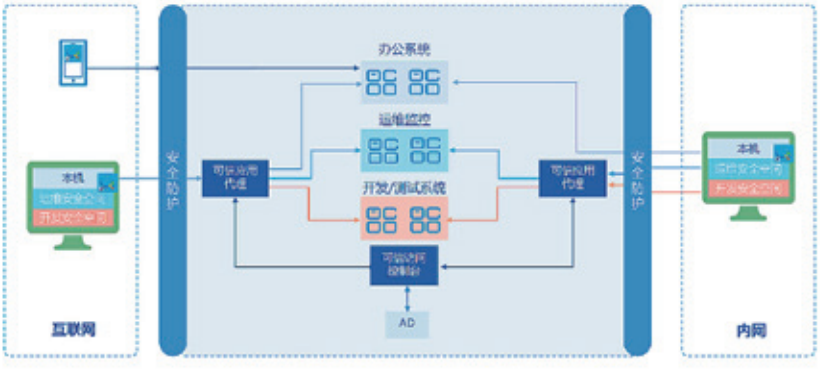


图 数字化协同智能安全管控平台架构图

零信任开启 SPA 模式，利用零信任较强的身份认证能力，实现内、外网的安全接入。利用零信任技术建立的网络通道实现内网的可信连接，提高了内网数据传输的安全性。利用内网 DNS 和内外网 TAP 配合，实现用户无需根据互联网或内网环境切换接入点，给予用户内外网一致的用户体验（如图所示）。

安全工作空间方面，中关村银行配发终端本机用于日常办公使用，通过用户组区分下发不同的安全工作空间策略，业务人员终端创建生产安全工作空间，开发人员终端创建开发测试安全工作空间。自有设备终端除根据角色创建生产安全工作空间或开发测试安全工作空间外，还会创建办公空间，用于日常办公使用，具备与中关村银行配发终端的本机相同的权限。通过这几个空间的灵活使用，实现在自有终端上安全访问中关村银行业务系统。

（2）策略管理灵活、兼顾效率和安全

依靠安全工作空间的隔离能力，将本机与安全工作空间彻底隔离。安全工作空间按角色访问对应的服务器资源，本机不能访问只有安全工作空间才能访问到的资源。在安全工作空间中创建的数据、文件、代码只能保存在安全工作空间中，导出时需要经过审批，防止了敏感信息泄露。为提高便利性，本机向安全工作空间导入数据无需审批，直接使用拖拽方式拖入安全工作空间即可。

为了进一步破除环境间数据不流通造成的协作障碍，中关村银行对员工数据导出需求进行了调研。调研发现，出于数据分析目的进行的数据导出，员工一般按照行内数据导出流程申请数据导

出，而终端层面跨环境导出数据场景，主要是办公协同沟通时展示数据能让对方更好地理解并解决问题。这种场景下申请导出的数据量不大，为此申请一次数据导出费时、费力。针对此情况，安全工作空间允许截屏、允许共享屏幕，这样员工就可以使用“一体化链接中台”的聊天、截屏功能和会议功能，高效地开展办公协同、讨论隔离在安全工作空间中的内容。为了保证安全性，所有的截屏都会带有水印、导出内容上传服务器，可以实现事后审计。通过这些举措实现了安全和高效之间的平衡。

由于“一体化链接中台”实现了各环境间通信和协调工具的统一，提高了全行的工作效率。为了保证安全性，防止数据通过“一体化链接中台”在不同等级的安全工作空间之间非法传递，“一体化链接中台”客户端只在本机运行，不允许在安全工作空间内运行。通过这种手段拉齐可传递数据的安全级别，防止利用“一体化链接中台”非法打通各隔离环境，造成数据泄露。

（3）特殊安全设计

数字化协同智能安全管控平台本身就有着很高的安全性设计，为了进一步提升安全性，中关村银行还做了特殊设计。

客户端首次接入系统时需进行认证，由管理员对终端进行人工识别，确认终端是否为已经批准接入的终端，并按照企业配发设备、自带设备为终端分组，便于后续管理。通过这种方式防范客户端被非法获取，从而接入中关村银行内网的情况。

此外，为进一步防范客户端被非法获取，中关村银行对客户端安装文件进行了分离，分解成安全工作空间安装文件和零信任安装文件，终端成功安装安全工作空间后，由安全工作空间到中关村银行内网指定路径拉取零信任安装文件静默安装，最终形成完整的客户端功能。公开渠道只能获取到安全工作空间安装文件，无法获取到零信任安全文件，再结合客户端首次接入系统认证，基本可以阻断非法获取客户端自行接入中关村银行网络的可能。

积极探索实践，完成多场景落地实践

目前，中关村银行在开发测试场景、生产访问场景、互联网访问场景已落地，数字化协同智能安全管控平台支持近400台终端的开发测试、生产访问使用。通过多维身份认证、动态权限控制、终端数据隔离等手段，确保用户终端访问开发环境、生产环境的精细化控制及数据安全。

1. 业务隐藏，访问加密，构建资源保护面

通过构建保护面实现对暴露面的收缩，要求所有资源默认隐藏，根据访问控制授权结果进行最小限度的开放，所有的资源访问请求都进行全流量加密和强制授权，有效地防止了黑客在内、外网窃听，获取登录账号和密码的可能性。

2. 数据隔离，安全流转，加强数据安全管控和审计

安全工作空间是一个加密的空间，存储在安全工作空间中的文件、代码都是加密存储，较终端上的明文存储更安全，而且安全工作空间支持国密算法、加密密钥丢失也可随时更换密钥，防止安全工作空间内的信息泄露。

数据导入行内环境更加开放，数据可以通过U盘拷入本机，然后再通过拖拽方式导入相应安全空间。整个得到导入过程不再需要摆渡盘和审批，效率提高。数据导出审批通过客户端即可完成，不再需要通过OA进行烦琐的审批，而且具备审计能力。

3. 降本增效，大幅提升工作效率

从使用效果来看，开发人员省去登录云桌面过程，开发终端配置可以根据需要增加内存或硬盘甚至更换新终端，不再受云桌面整体硬件资源上限的限制，升级成本大幅降低。同时，由于安全工作空间替代了云桌面，支持云桌面的计算资源被回收，也不会再产生新的软/硬件及带宽等维护费用，IT成本大幅下降。

监控类运维管理系统由专用终端登录改为由生产安全工作空间登录，对安全性要求不高的巡检类工作可直接在工位完成，不再依赖专用终端，大大提高了工作的灵活性。业务人员通过生产安全工作空间访问业务系统，保障工作便捷的同时提高了安全性。

4. 高效协同，科技创新助力服务“三创”

通过数字化协同智能安全管控平台落地，切实支持“一体化链接中台建设”，打通内外网。行内外交流统一，无需切换通信工具，数据流动更简便，同时提供文档协同、安全审计等能力，协同办公更高效，助力服务“三创”。

结语

数字化协同智能安全管控平台的上线，改变了中关村银行的管理模式和安全管控模式，在保障安全的前提下提高了沟通效率和工作效率。未来，中关村银行将按照数字化协同智能安全管控平台架构理念，逐步推进更多场景的落地实践，结合“一体化链接工程”建设，形成企业级网络安全能力，高效支撑中关村银行数字化转型和发展。安

请注意，这些文件可能包含木马病毒！

作者 | 魏开元

正文开始之前，先看看以下ABCD哪个或者哪几个文件有可能是恶意文件?

言归正传!

在日常的工作和生活中，大家总会在网站、论坛、社交软件、电子邮箱等各种渠道，收到许许多多各种类型的文件，尽管绝大多数情况这些文件都与人们秋毫无犯，但也有一小部分“坏人”试图混进人民群众的队伍，给广大用户造成不小的麻烦，轻则导致计算机、手机停摆、个人信息失窃，重则工厂停工、电厂停电甚至国家安全遭到破坏。

不过随着全民网络安全意识与技能的不断提升，如果恶意文件再以“真身”大摇大摆的出现，先不说能不能逃过杀毒软件的检测，就是普通用户一眼就能识破。所以，攻击者也花样百出，尽可能地为恶意软件穿上合法的外衣。

2023年国家网络安全宣传周活动刚刚结束，借着这个机会，下面盘点一下哪些文件最有可能是“人民群众中的坏人”。

首先，拥有一个“极具诱惑”的名字

用户对于文件类型的第一印象，大都来源于文件名，比如，压缩文件WinRAR、浏览器文件Google Chrome、Word文件张三个人简历等，一打眼看过去就知道这个文件是干嘛用的。

一个极具诱惑力的名字，总是能够吸引用户的眼球，这一点正是木马、病毒的初衷。至于诱惑力从何而来，笔者认为至少包括三个方面。

第一，和社会热点或者个人兴趣相关

任何时候都不要怀疑吃瓜群众的热情。对于圈内大瓜或者社会热点新闻的内幕，绝大多数用户都按奈不住内心的好奇，想要一探究竟。黑客就是利用了这一点，将恶意文件伪装成社会热点事件从而进行广泛传播。

在新冠疫情初期，奇安信威胁情报中心曾多次捕获与疫情相关恶意文件，如“口罩价格”“疫情防控”等，在当时那个背景下，这是与几乎每个人都息息相关的消息，极其容易诱导不明真相的吃瓜群众上当受骗。

下图是奇安信威胁情报中心根据攻击活动相关的诱饵热词制作的词云图，几乎每一个关键词都直击舆论的热点。

文件类型	样本名称示例
简历 / 招聘	*** 保险 Java 资深研发工程师招聘需求 简历 -***- 清华大学 个人简历 -***
通知 / 通告	关于集团调岗降薪通知详情 关于加强防范钓鱼邮件的通知 开展 OA 弱口令排查的紧急通知
数据信息 / 文件资料	团队个人业绩提成分红核对 中国 ***** 数据中心资产评估服务采购投标材料 数据脱敏在数据中台产品的实践与应用 -0814. 附件 4. 支撑性证明材料参考清单
问题反馈 / 投诉举报	中国 **** 交易所 - 业务流程审批问题 招标投诉反馈附件 .zip 20230815 投诉证据 (聊天记录 , 客服工号) 20230817** 航空收到客户投诉信息详情

表：实战攻防演习期间部分恶意样本文件名

第二，和钱相关

相较于吃瓜，金钱的吸引力只会有过之而不及。没办法，谁还不是个勤勤恳恳的打工仔，靠辛勤的劳动换取一份辛苦钱。天上掉馅饼这种事情，能接住还是接住吧。

所以，在看到“工资补贴”“退税”等字样的时候，“激动的心，颤抖的手”就已经按奈不住了。殊不知，前方早有一双“无形的黑手”，在等着人们上当受骗。

第三，和工作相关

如果上述两种情况，大家还能强忍好奇心将其抛之脑后的话，那和工作相关的文件就“由不得”打工人了，出于工作的惯性，很多人都会不假思索打开它。

比如，HR 收到了候选人简历、销售拿到了招标文件时，犹豫一分钟都是对工作的不尊重。

尤其是当这个文件是以“同事”的名义发过来的时候，为了欺骗目标，攻击者首先会盗取公司内部员工的身份作为伪装，从而显得更加真实。

其次，拥有一个以假乱真的“外衣”

除了文件名，用户对于文件的另一个直观印象就来源于图标了。俗话说人靠衣装马靠鞍，这个图标就好比是文件的外衣。一件好看的衣裳，对于用户眼中的文件而言，绝对是大大的加分项。

但木马病毒追求的并非华丽的外表，而是足够以假乱真。谁最能取得用户信任，木马病毒往往就“化妆”成谁。

常见的对象也可以分为两类。

第一类是穿上常见应用软件的外衣，利用搜索引擎、网站、手机应用市场等渠道进行传播。

今年上半年，奇安信威胁情报中心通过日常分析运营发现多款二次打包并携带木马后门的恶意安装包样本，恶意安装包内包含“向日葵远控”“钉钉”“WPS”等常用工具软件。

图：恶意安装包内部分文件截图

目前，绝大多数企业并没有统一的软件下载渠道，主要是员工在网上自行下载，这就给了攻击者以可乘之机。只要文件名、图标一换，如果杀毒软件再检测不出来，那就危险了。

尤其是很多小众的工具，这些工具来源于开源社区、论坛甚至是其他陌生用户，只在固定圈子内流行，相对而言，被中招的可能性要更高。

第二类是换上 Word、Excel、PDF 等办公文档的衣服，利用邮件、即时通信软件鱼目混珠。

作为日常接触最多的文件类型，打工人对各种各样的 Word 文档、Excel 表格可谓是倍感亲切，也更加信任，一个小小的 office 文档能干什么坏事呢？这种心里正是黑客想要的。

根据奇安信威胁情报中心的统计，Word 等办公文档的图标，是攻击者首选的伪装类型。

顺带说一句，不同类型的文件有着不同的后缀名，比如，Word 文档的后缀名是 .docx、PPT 文档的后缀名是 .pptx、常见的可执行程序的后缀名是 .exe……

由于绝大多数情况下，木马病毒属于可执行文件，所以当它伪装成办公文档时，一定会夹紧自己的“狐狸尾巴”，漏出来被人看到可就大事不妙了。

需要提醒用户注意的是，很多计算机的设置是默认隐藏后缀名的，导致普通用户并不能一眼看出后缀名的区别。

尤其是有些攻击者善用“阴招”，在原本的真后缀名前面，加上一个假后缀名，用于扰乱用户的注意力。这样一来，原本的 .exe 后缀被隐藏起来，而伪造的 .docx 却作为文件名的一部分，直接展现在用户的视野里。

就像下图这样。

最后，拥有“一招毙命”的非对称武器

即便是真正的办公文档，也并不是绝对安全的。

上述的两类主要伪装方式，无论是修改文件名，还是修改文件图标、后缀名这些方式，都很容易被肉眼看出或者其他相对简单的方式规避，决不能为结果兜底。

所以，高明的攻击者总会留一手“撒手锏”，在关键时刻给目标致命一击。想要突破防守方的层层围堵直达目标系统内部，就得拿出点绝活。

利用办公文档自身的功能或者缺陷，就是最好的手段，至少无论横看、竖看、斜看，这都是一个真正的办公文档，不是其他什么文件伪装的。

图：近期奇安信威胁情报中心捕获的部分恶意样本

绝活一：Office 宏

宏（Macro）是微软为 Office 软件包设计的一个特殊功能，是一种用来帮助用户完成一系列操作的记录器，它可以录制你操作的过程，当需要重复这样的操作时，可以通过录制的“宏”来自动完成。

攻击者利用这个功能，制作专门利用 Office 软件传播的宏病毒，一旦打开这样的文档，其中的恶意宏就会被自动执行，于是宏病毒就会被激活，并转移到目标计算机上。

这个过程，用户没有任何感知。而且不论是外表还是内容，携带宏病毒的文档，都与正常文档看不出任何差别。

尽管利用 Office 宏的方法看起来非常隐蔽，但由于普通用户对于宏这个功能的依赖度并不高，加之近些年来宏病毒日渐泛滥，因此宏通常会被企业用户默认关闭。

如此一来，宏病毒就失去了原有的效果。

绝活二：0day 漏洞

显而易见，攻击者还有绝活。

作为网络安全领域当之无愧的“武器之王”，0day 漏洞在任何时候出现都具有相当大的破坏力。

并且利用 Office 软件的 0day 漏洞，同样具备极强的隐蔽性，用户收到的同样是一个看起来再正常不过的文档。

在前不久结束的大型实战攻防演习期间，奇安信威胁情报中心率先捕获了一个利用 WPS 0day 漏洞的恶意样本。经测试，用户只需打开文档，就可以被攻击者远程控制，不需要其他任何操作。

有趣的是，尽管该恶意文档躲过了绝大多数恶意软件的检测，但却没逃过奇安信的追捕。

事情已经很明显了，奇安信威胁情报中心也有绝活——红雨滴云沙箱。（奇安信情报沙箱 (qianxin.com)）

红雨滴云沙箱是威胁情报中心红雨滴团队基于多年的 APT 高级攻防对抗经验、安全大数据、威胁情报等能力，使用软、硬件虚拟化技术开发实现的真正的“上帝模式”高对抗沙箱，每日可完成 20W 左右的样本处理量，可同时并行处理高达上千条的沙箱分析任务，面向客户提供 Web 服务和 API 接口服务，Web 端用户只需要在沙箱页面完成文件上传和分析配置，30s 即可生成专业分析报告。红雨滴云沙箱提供恶意软件详细的静态、动态行为分析及各类文件详情并提取 IOC 形成自己的威胁情报，同时支持 Windows、Android、Linux 等平台下的样本自动化分析。

红雨滴云沙箱依靠威胁情报中心自主知识产权的 APT 团伙静态分析引擎（RAS 引擎），基于 ALPHA 威胁分析平台完备的威胁情报和互联网基础数据，以及数据覆盖度、信息种类、数据的时间 / 空间跨度等多重优势，通过专家级的自动化日志分析，快速锁定真正有威胁的攻击者，快速进行画像、持续跟踪，揪出背后隐藏的攻击者，保障攻防期间研判分析的精准性。

回到文章开头的问题，您心里有答案了吗？ 安

报告：2023 年数据泄露成本达历史新高

近日，IBM 安全发布的《2023 年数据泄露成本报告》显示，2023 年数据泄露的全球平均成本上升至 445 万美元，达到历史新高，比 2022 年的 435 万美元增加了 2.3%，比 2020 年的 386 万美元增加了 15.3%。

《2023 年数据泄露成本报告》针对全球 553 个组织所经历的数据泄露事件进行深入分析研究，探讨数据泄露的根本原因，以及能够减少数据泄露的技术手段。

1、数据泄露成本继续攀升

报告中的主要发现包括数据泄露的成本攀升至新高、医疗保健行业的数据泄露成本仍为所有行业中最高，以及制造业成为网络犯罪分子最常攻击的行业等。

· 数据泄露的成本攀升至新高。数据泄露的全球平均成本已上升至 445 万美元，比 2022 年增加了 10 万美元。相较于 2022 年的 435 万美元，平均成本增加了 2.3%。自 2020 年以来，数据泄露的平均总成本为 386 万美元，平均总成本增加了 15.3%。

· 数据泄露的每条记录成本也达到新高。2023 年，数据泄露相关的每笔记录的平均成本为 165 美元，比 2022 年的平均成本 164 美元略有增加。这与 2021 年至 2022 年相对较小的增长相吻合，其中成本仅增长 3 美元。在过去七年中，每笔记录的平均成本最大增幅发生在 2020 年至 2021 年期间，平均成本从 146 美元上升到 161 美元，涨幅为 10.3%。这项研究调查了 2,200~102,000 笔记录规模不等的泄露情况。

· 医疗保健违规成本持续飙升。在各个行业中，医疗保健行业连续 13 年录得损失最高的数据泄露成本。医疗保健行业的数据泄露成本仍为所有行业中最高，从 2022 年的 1,010 万美元增加到 2023 年的 1,093 万美元，增幅为 8.2%。在过去三年中，医疗保健领域数据泄露的平均成本增长了 53.3%，与 2020 年的平均成本 713 万美元相比，增加了 300 多万美元。医疗保健行业受监管程度很高，美国政府始终将之视为关键基础设施行业。

· 行业排名发生变化。医疗行业之后，分别是金融、能源、工业、科技、服务、运输、教育等行业，其中金融机构的数据泄露平均成本为 590 万美元，能源行业的平均成本为 478 万美元，教育行业的平均成本为 365 万美元。科技行业跌出前五名，而工业部

主要发现包括数据泄露的成本攀升至新高、医疗保健行业的数据泄露成本仍为所有行业中最高，以及制造业成为网络犯罪分子最常攻击的行业等。

图 1：以百万美元为单位

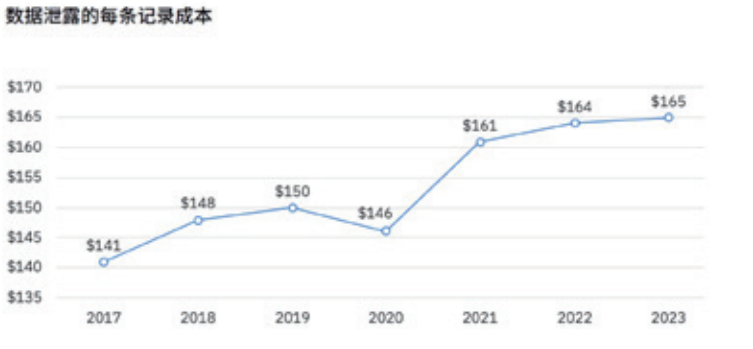
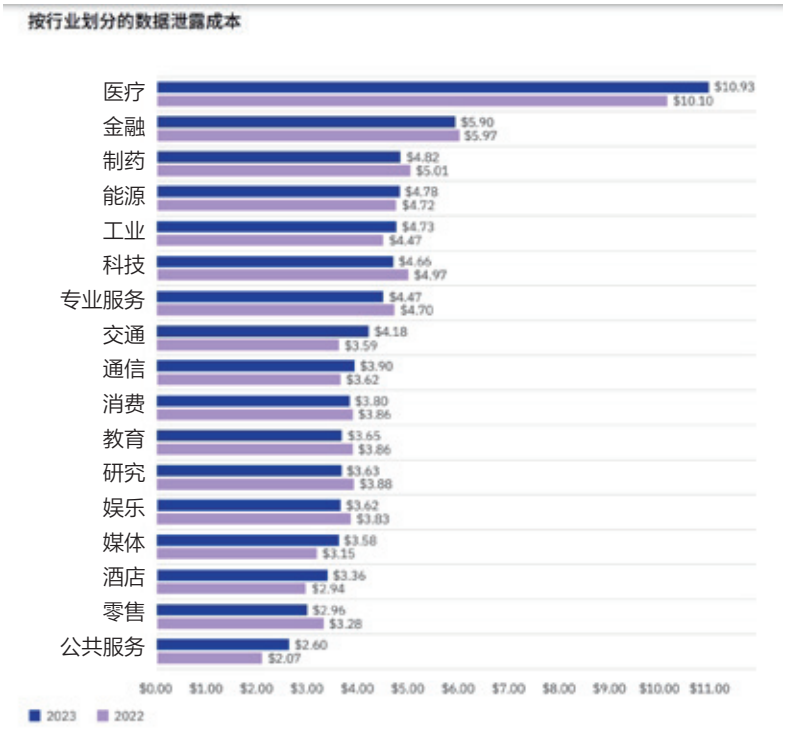


图 2：以美元为单位



门则递补上来，从第七位上升到第五位，增幅为 5.8%。制造业成为网络犯罪分子最常攻击的行业。

· 关基行业的数据泄露成本超过 500 万美元。关键基础设施组织包括金融服务、工业、科技、能源、运输、通信、医疗保健、教育及公共部门等行业的企业和机构。这些组织的数据泄露成本（504 万美元）比其他行业组织的平均成本（378 万美元）高出 126 万美元，比 2022 年报告的关键基础设施行业的数据泄露平均成本增加了 4.6%。

2、数据泄露检测能力亟待提升

IBM 全球安全服务部总经理 Chris McCurdy 表示：“对于防御者和攻击者来说，时间都是网络安全中的新货币。正如报告所示，早期检测和快速响应可以显著减少漏洞的影响。安全团队必须关注对手最容易得手的地方，并集中精力在他们实现目标之前阻止他们。对威胁检测和响应方法进行投资，以加快防御者的速度和效率；如人工智能和自动化，对于改变这种平衡至关重要。”

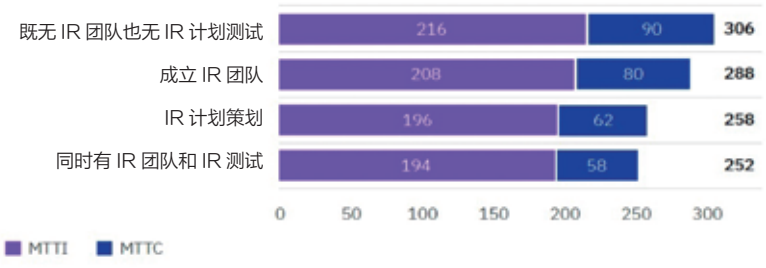
· 网络钓鱼与凭证被盗或泄露是两种最常见的初始攻击媒介。网络钓鱼与凭证失窃或泄露分别造成了 16% 和 15% 的数据外泄。其后则是云配置错误和商业电子邮件泄露，分别占 11% 和 9%。此外，在今年报告中首次将 0day 漏洞和已知未修补的漏洞进行研究，所调研的数据泄露中有 5% 以上源于尚未修补的已知漏洞。

· 组织发现数据泄露事件能力亟待提升。仅有三分之一的公司通过自己的安全团队发现数据泄露事件，这凸显了亟需更好的威胁检测手段。67% 的漏洞是由良性第三方或攻击者自己报告的。当攻击者披露漏洞时，相较于内部检测，组织会损失近 100 万美元。与自行发现数据泄露的研究组织相比，攻击者披露的数据泄露成本平均高出近 100 万美元（523 万美元 & 430 万美元），漏洞的生命周期也

按初始攻击媒介划分的数据泄露成本和频率

图 10：以百万美元为单位

通过 IR 团队的组建和测试来识别和遏制数据泄露所需的时间



使用 ASM 解决方案识别和遏制数据泄露所需的时间

延长了近 80 天（320 天 & 241 天）。

· 最有效的三个成本降低因素，分别是采用 DevSecOps 方法、员工培训及 IR 规划和测试。例如，采用 DevSecOps 方法的组织发生数据泄露所造成的平均成本约为 420万美元，比 2023 年的平均数据泄露成本（445 万美元）低 24.9 万美元。

· IR 战略和策略在减少数据泄露影响方面发挥了重要作。采用组建 IR 团队和 IR 计划测试的双重策略，识别和遏制数据泄露的时间更短（252 天），识别泄露事件的速度比二者皆无的组织要快 54 天。

· ASM 帮助将识别和遏制数据泄露的总时间缩短了近 12 周。部署 ASM 解决方案的组织在 193 天内成功识别泄露事件，并在 61 天内完成遏制操作。识别和遏制泄露的总时间为 254 天，相对缩短了 83 天（约 12 周），识别和遏制数据泄露所需的时间仅为未部署 ASM 解决方案的组织所耗费时间的 75%。

· 广泛使用安全 AI 和自动化可以大幅节省成本、缩短识别和遏制泄露的时间。广泛使用安全 AI 和自动化的组织所节省的成本最高，数据泄露的平均成本为 360 万美元，比不使用的组织减少了 176 万美元，相差 39.3%。与未部署这些技术的组织相比，广泛使用人工智能和自动化的组织的数据泄露生命周期缩短了 108 天。

3、降低成本的建议

在本部分概括介绍了组织可采取哪些措施来降低数据泄露事件造成的财务成本，并减少给组织声誉带来的不良影响。我们的建议包括成功的安全方法，这些方法可以帮助以更低的成本、更短的时间发现并遏制泄露事件。

· 将安全性融入到软件开发和部署的每个阶段，并定期进行测试；

· 跨混合云实现数据保护现代化；

· 使用安全 AI 和自动化来提高速度和准确性；

· 通过了解攻击面态势和实践 IR 来增强恢复弹性。安

大事记

全球上市公司 30 人智库论坛在京举行 齐向东应邀出席

9 月 17 日，由首都经贸大学、清华大学社会科学学院社会与金融研究中心、上海交通大学人文学院、亚洲数字经济科学院等发起的首届全球上市公司 30 人智库论坛在北京银行大厦举行，论坛以“全球上市公司治理与面向 2035 的世界一流企业”为主题，与会嘉宾纷纷就此解析政策动向、共话经济热点、把脉市场趋势，论坛现场思想激荡、精彩纷呈。

“有什么样的情怀，就有什么样的上市公司，上市公司要为国家发展战略服务。一流上市公司要以科技创新为驱动，没有科技创新就没有世界一流。”全国工商联副主席、奇安信党委书记、董事长齐向东在发言中强调，企业要持续投入研发，掌握核心技术，在国际市场占有一席之地。一流上市公司要有国际视野和格局，进行全球化经营，在全球产业链分工中取得优势。企业要主动融入世界科技创新舞台，提升全球竞争力。

存证、取证、鉴证全链条服务 奇安信推出奇证云及新一代数字司法解决方案

9 月 19 日，奇安信集团在京发布了奇安信数字证据云服务系统（简称“奇证云”）及新一代数字司法解决方案。针对电子证据采信低的问题，奇证云可提供覆盖事前存证、事中取证、事后鉴证的全链路服务，打破电子数据“自证难、存证难、他证难”的困境，为知识产权保护及行政监管提供全新的解决方案。

发布会现场，北京金融安全产业园、武汉华著科技有限公司分别与奇安信签约，成为奇证云的第一批合作伙伴。

齐向东出席香港网络警政国际论坛

9 月 13 日 ~15 日，香港特区政府警务处举办了网络警政国际论坛。会上，齐向东发表了“以‘零事故’为目标，护航数智时代警务建设”为题的演讲，分享了他对网络安全警务建设等话题的看法和思考。

齐向东认为，面对日益严峻的网络安全环境，警务部门也需要不断提升数字化系统的安全能力。他建议，要想确保数字化系统“零事故”，警务机构应该从五个方面提高网络安全能力：一是把纵深防御的内生安全体系融入警务系统建设；二是筑牢全链条的数据安全防线，让警务部门能真正看

清风险、防住攻击、管好“内鬼”；三是打造三级联动的网络安全运营中心，用一个中心解决各个警务机构的安全问题；四是用好智能化手段，精准打击网络犯罪；五是重点探索“AI＋安全”，促进警务工作提质增效。

2023 网安周：奇安信联动行业伙伴 共筑网络安全防线

9 月 11 日 ~17 日，2023 年国家网络安全周活动在全国范围内统一开展。奇安信与各地政府、区域合作伙伴紧密合作，深入全国 30 个省市自治区、近百地，面向网信、教育、工业、通信等十余个行业群体，进行网络安全宣传推广。

在福州，奇安信集团总裁吴云坤围绕关基领域网络安全防护，提出关基保护是一个系统工程，需要用系统工程方法体系化构建安全能力，用内生安全框架实现体系化、系统化建设和运行。

奇安信集团副总工程师兼数据安全首席科学家刘前伟在中国网络安全年会暨网络安全协同治理分论坛上，分享了如何通过“四个转变”、抓住“三个关键”实现数智时代的网络安全“零事故”目标。

在西藏自治区网安周活动上，奇安信集团副总裁罗海龙发表了《用城市级安全防护网筑牢数字经济的安全底座》主题演讲，分享了构建城市网络安全运营中心的核心能力及奇安信的相关建设经验，把智慧城市网络安全建设的先进理念和成果带到了雪域高原。

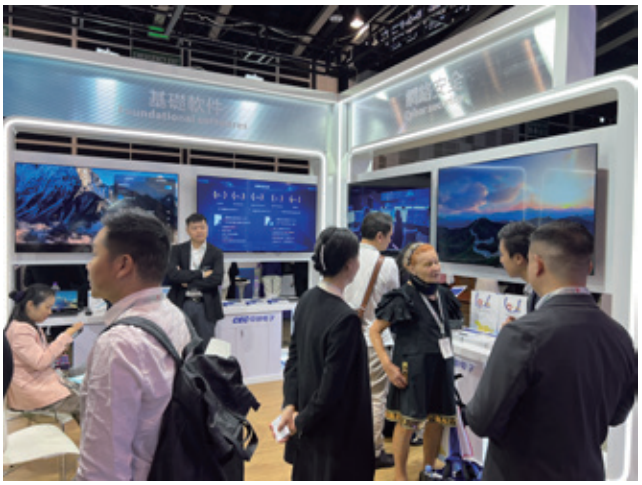
在贵州，奇安信集团副总裁、数据安全事业部总经理刘洪亮发表了《构建数字安全体系 护航数字经济发展》主题演讲，分享了数据安全系统治理的三大关键举措：盘清资产、精准防护、全局管控。

在雄安，奇安信集团副总裁张龙围绕“网络安全企业的工程化人才培养实践”进行主题报告分享，从课程体系、实践育人、产教融合多角度探讨网络空间安全专业人才培养创新机制。

奇安信最新发布的 Q-GPT 安全机器人和大模型卫士，在网安周期间，在全国各地进行了展示，吸引了大量关注，并登上央视新闻。

奇安信亮相香港“一带一路”高峰论坛 C-SOC 吸引海外客户关注

9 月 13 日 ~14 日，由香港特别行政区政府主办的第八届“一带一路高峰论坛”在香港会议展览中心举行。适逢共建“一带一路”倡议提出十周年，本届论坛以全实体形式回归，网络安全领军企业奇安信集团携 C-SOC 等产品亮相展区，向超过 80 个国家和地区的参会者展示网络安全中国实力。



南水北调集团联合奇安信等 12 单位共同成立水网数字化产业链创新联盟

近日，由水利部、国际水资源学会指导，中国南水北调集团有限公司主办的首届“国家水网及南水北调高质量发展论坛”在京举行。会上，由中国南水北调集团水网智慧科技有限公司牵头，奇安信与华为、百度、阿里云等 12 家企业、高校、科研院所共同发起的“水网数字化产业链创新联盟”正式启动。

奇安信作为联盟创始单位，将围绕产业链部署创新链，以水网数字化产业技术创新需求为基础，与联盟成员共同完善水网行业的网络安全解决方案，以确保智慧水网的可靠性

和可持续发展，促进水网数字化关键技术领域的科技进步及应用落地，推动国家水利行业网络安全建设发展。

齐向东：以“零事故”为目标 建设更高水平的平安中国

9 月 8 日，由中国友谊促进会主办的全球公共安全合作论坛（连云港）2023 年大会第二届数据安全分论坛在京举行。全国政协委员、全国工商联副主席、奇安信集团董事长齐向东受邀出席，并发表《以“零事故”为目标 建设更高水平的平安中国》主旨演讲。

他提出，建设更高水平的平安中国，既要用数智化手段促进发展，又要确保数智化社会安全无忧，杜绝网络和数据安全事故，也就是要做到“零事故”。要筑牢全链条的数据安全防线、“三级联动”的运营防线、精准打击网诈等新型网络犯罪的防线、用智能对抗智能的防线，让国家、社会更平安、人民生活更幸福。

北京联通总经理霍海峰调研奇安信集团：双方签署战略合作

9 月 8 日，奇安信集团与中国联合网络通信有限公司北京市分公司在奇安信安全中心签署战略合作协议并达成长期战略合作伙伴关系，双方将围绕“大联接、大计算、大数据、大应用、大安全”五大方向开展全方位合作，将奇安信的安全能力及北京联通的网络能力紧密结合，形成合力。

根据协议，双方将结合各自专业优势和影响力形成合力，在通信连接领域开展创新应用合作；在计算领域积极探索数据中心业务合作、云网一体、信创云等方面的能力合作；在大数据领域共同研究数据安全体系的建设及应用；在应用领域深入推进多场景应用系统建设；在安全领域，围绕政企安全产品、云安全、网络安全服务等内容展开合作。

签约赛力斯、城市级网络安全运营中心落地 奇安信亮相 2023 智博会收获满满

9 月 4 日 ~ 6 日，聚焦“智能网联新能源汽车”等年度主旨的 2023 中国国际智能产业博览会在重庆举行。奇安信携系列车联网安全产品及解决方案亮相智博会，通过签约合作、论坛演讲等多种形式，全面展示了奇安信在车联网、工业互联网、数字城市等领域的安全实力。

为进一步推进智能网联新能源汽车产业发展，会上，奇安信集团与赛力斯汽车签署战略合作协议，双方将在智能网联汽车、工业互联网等领域的网络与数据安全威胁检测防护、监测预警、威胁信息共享、应急处置协同等方面开展合作，建立长期稳定的战略合作关系。

在“车路云融合发展 50 人论坛”上，奇安信集团高级副总裁曲晓东表示，信息安全作为汽车的一个属性，需要建立在汽车内部网络架构的基础上，安全保障体系也需要与智能网联汽车应用同步部署。

在“2023 新能源汽车智能座舱生态论坛”上，奇安信集团工业互联网安全事业部总经理李小军表示，我国智能座舱市场快速发展，数据显示，到 2025 年市场规模预计将超过 1000 亿元，但安全部分并没有随着智能座舱一起同步发展，希望未来可以和更多智能座舱厂商、新能源汽车厂商一起，共同促进智能座舱安全、智能发展。

在“第六届智能制造和工业互联网创新发展论坛”上，奇安信集团副总裁孔德亮提出了“工业互联网‘零事故’网络安全一体化运营”的观点。他表示，工业互联网安全“零事故”是一项复杂的系统性工作，需要在技术支撑、管理制度、组织保障和安全运行等方面全方位落实，做到业务不中断、数据不出事、合规不踩线。

千万级安服大单 奇安信中标某大型银行 2023 年安全测试服务项目

近日，奇安信中标某大型银行机构 2023 年度安全测试服务采购项目，项目规模为千万级别。该项目是奇安信今年获得的又一个千万级安服大单，同时也是奇安信在银行业涉及安全检测类产品最全、覆盖业务系统最广的安全服务项目，对于金融业同类项目起到了很好的标杆示范作用。

齐向东：香港国际创新科技中心建设要突出重点

9 月 4 日，中国宏观经济暨大湾区融合论坛 2023 在香港举办，香港特别行政区行政长官李家超，香港特别行政区

财政司司长陈茂波，中美绿色基金管理有限公司董事长、原国家发改委财政金融司司长徐林，中国建筑国际集团执行董事兼行政总裁、可持续发展委员会主席王晓光，全国工商联副主席、奇安信集团董事长齐向东等数十位在政商学界有影响力的知名人士出席，共同为大湾区、香港经济发展建言献策。

齐向东发表主题演讲时表示，香港国际创新科技中心的建设要突出重点，网络数据安全将成为支柱产业，应该成为香港科技创新的重点，香港也应该成为中国网络安全企业全球化的支点。同时，香港要用好三大优势，建设国际科技人才港，这是建成国际创新科技中心的前提。

奇安信集团 2023“质量月”活动全面启动：产品质量是安全公司的生命

9 月 1 日，第 46 届全国“质量月”活动拉开帷幕。奇安信集团同步启动了主题为“持续优化流程、创造客户价值”的“质量月”系列活动。

奇安信已连续第六年举办集团“质量月”活动。本次活动面向全国各地员工，开展质量征文、质量培训、质量改进建议征集、质量专项稽核、质量技能大比拼、工厂质量标兵评选等一系列活动，通过线上和线下结合的形式，全面推进“质量月”活动。

奇安信司法鉴定中标北京市公交总队电子数据鉴定服务项目

近日，奇安信司法鉴定在多家司法鉴定机构中脱颖而出，以全场最高评分成功中标“北京市公安局公共交通安全保卫分局 2023—2024 年电子数据鉴定服务项目”，再次彰显了奇安信司法鉴定的专业实力和领先地位。

作为司法鉴定业务的核心支撑，奇安信集团拥有北京网神洞鉴科技有限公司司法鉴定所与盘石软件（上海）有限公司计算机司法鉴定所两家司法鉴定机构，是目前国内少数能够通过自主研发软件进行取证与分析的电子数据司法鉴定机构，具有独立的实验室场所。

齐向东：“零事故”是目标更是标准 构建安全的数智时代

在 8 月 28 日举行的区人民政府协办的首届网络空间安全（天津）高峰论坛上，全国政协委员、全国工商联副主席、奇安信集团董事长齐向东发表了“以‘零事故’为目标，构建安全的数智时代”的主题演讲。

他表示，人工智能为破解数智时代新盲区提供了方法，但面对严峻的网络安全形势，网络安全防护思路需要做到三个转变：从关注 IT 转变成关注业务、从关注设备转变成关注人、从关注建设转变成关注运营，这样才能做到业务不中断、数据不出事、合规不踩线的“零事故”。

齐向东出席 HICOOL2023 全球创业者峰会：网络安全是创新创业热门领域

8 月 27 日，由北京市政府、中华人民共和国教育部指导，北京市海外高层次人才协会主办的 HICOOL 2023 全球创业者峰会在京举行。全国政协委员、全国工商联副主席、奇安信集团董事长齐向东在主旨演讲中表示：网络安全作为创新创业的热门领域，需要具备三大能力，包括重视研发投入、以结果为导向、选好细分方向。

“深入开展网络安全创新创业，是时代机遇，更是时代使命。”他表示，在顶层设计、国际形势、新兴技术、投资市场、产业生态五大驱动力的推动下，网络安全产业将进入高速度、高质量发展的黄金期。数据安全、人工智能、软件供应链安全、身份安全将是网络安全产业发展的四条重点赛道。

Q-GPT 安全机器人和大模型卫士发布 京东方和吉利成为首批用户

8 月 25 日，奇安信集团在京发布了 Q-GPT（奇安信大模型）安全机器人和大模型卫士。京东方集团和吉利汽车集团等客户现场签约，成为国内首批 Q-GPT 安全机器人和安全大模型用户。同时，大模型卫士现场获得了国内多家客户的签约意向。

Q-GPT 安全机器人是基于奇安信大模型的“虚拟安全专家”，可以全天候工作，一台机器人等于 60 多位安全专家，可产生约 2000 万元的运营效益，极大提升了生产力。大模型卫士集安全风险发现、大模型访问控制、数据泄露管控、违法违规行为溯源、大模型应用分析等为一体，帮助企业更安全的向大模型要生产力。

广州燃气与奇安信达成战略合作

8 月 22 日，广州燃气集团有限公司与奇安信科技集团股份有限公司签署战略合作签约仪式。根据协议，双方将在数字化转型、数据安全、安全人才培养等领域开展战略合作，夯实广州燃气数字化转型安全底座、推动数字化转型目标有效落地。

荣誉墙

奇安信连续五年入选“民营企业百强”“科技创新”及“社会责任”三大榜单

9 月 21 日，北京市工商联在京召开 2023 北京民营企业百强发布会，发布了“北京民营企业百强榜单”。奇安信集团凭借在行业引领、技术创新、人才培养等多个方面的优异表现，连续五年入选“民营企业榜单”“科技创新”“社会责任”三大榜单。

连续四年位居网安企业头名！奇安信再登“中国先进计算企业百强榜”

9 月 15 日，2023 世界计算大会在湖南省长沙市召开。会上，赛迪顾问发布《2023 先进计算企业竞争力研究》报告，并揭晓“2023 中国先进计算企业百强榜”，奇安信凭借在先进计算领域整体实力、产业生态布局、产品领先性等方面的综合优势，连续四年以网络安全行业头名的身份入围该榜

排名	企业	排名	企业
TOP1	华为技术有限公司	26	英伟达半导体科技（上海）有限公司
TOP2	苹果（中国）有限公司	27	上海宝信软件股份有限公司
TOP3	中国电子信息产业集团有限公司	28	亚信科技控股有限公司
TOP4	浪潮集团有限公司	29	北京金山云网络技术有限公司
TOP5	阿里云计算有限公司	30	北京京东尚科信息技术有限公司
TOP6	深圳市腾讯计算机系统有限公司	31	中软国际集团有限公司
TOP7	中国移动通信集团有限公司	32	亚马逊（中国）投资有限公司
TOP8	中国电信集团有限公司	33	北京宇信科技集团股份有限公司
TOP9	用友网络科技股份有限公司	34	武汉达梦数据库股份有限公司
TOP10	微软（中国）有限公司	35	麒麟软件有限公司
11	英特尔（中国）有限公司	36	深信服科技股份有限公司
12	中芯国际集成电路制造有限公司	37	中国联合网络通信集团有限公司
13	小米科技有限责任公司	38	中国信息通信科技集团有限公司
14	国电南瑞科技股份有限公司	39	杭州海康威视数字技术股份有限公司
15	SK 海力士半导体（中国）有限公司	40	曙光信息产业股份有限公司
16	联想集团	41	超聚变数字技术有限公司
17	三星集团	42	海尔集团公司
18	奇安信科技集团股份有限公司	43	海信集团有限公司
19	超威半导体（中国）有限公司	44	甲骨文股份有限公司
20	深圳市大疆创新科技有限公司	45	金蝶软件（中国）有限公司
21	启明星辰信息技术集团股份有限公司	46	荣耀终端有限公司
22	百度在线网络技术（北京）有限公司	47	思爱普（中国）有限公司
23	戴尔（中国）有限公司	48	北京紫光展锐科技有限公司
24	中兴通讯股份有限公司	49	中科软科技股份有限公司
25	新华三技术有限公司	50	联通动力信息技术（集团）股份有限公司

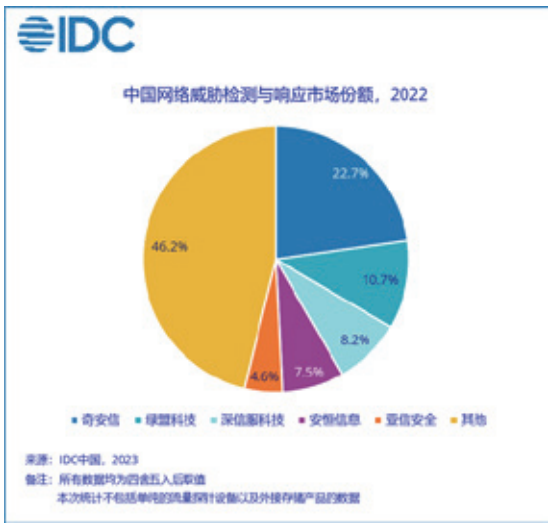
单，再次巩固了公司在算力、算法技术和市场表现等方面的领先地位。同时，奇安信还在软件领域排行第五。

助力中国企业走出去 奇安信入选 2023 年服贸会合规优秀案例

近日，中国国际服务贸易交易会“2023 中国企业国际合规论坛”在京举行。奇安信凭借在企业合规建设等方面取得的成就，入选了本次论坛合规优秀案例，同时案例被收录至《中国企业国际合规蓝皮书（2023）》，为大企业“走出去”提供实战经验。奇安信法律合规中心负责人、首席法律顾问马兰在论坛上表示，数据合规仅建立制度和管理层面的静态体系是远远不够的，必须借助技术手段，实现覆盖数据全生命周期和业务全流程的安全与合规管控，实现动态及持续性的实质性合规。

奇安信天眼连续两年位居国内 NDR 市场第一

近日，全球领先的 IT 市场研究和咨询公司 IDC 发布了《中国网络威胁检测与响应市场份额，2022：技术提升，市场下沉》（以下简称《报告》）。数据显示，奇安信市场份额占比达到了 22.7%，大幅领先第二、第三名市场份额总和，连续两年位居国内网络威胁检测与响应（NDR）市场第一位置。



广东省机场集团零信任安全访问平台获评“2023 安全守卫者计划优秀案例”

近日，由中国信息通信研究院、中国通信标准化协会主办的 SecGo 云和软件安全大会在京举办。大会上正式发布了 2023 年安全守卫者计划优秀案例，由奇安信建设的广东省机场集团零信任安全访问平台项目成功入选。

随着广东省机场集团数字化转型的深入，大量数据需要在集团各系统间流转，同时还需要满足员工远程访问、移动办公等需求。奇安信帮助广东省机场集团建设零信任安全访问平台，将业务与安全融合，实现了终端可信、用户可信、

流量可信，从信任链到运营管理闭环，达到了访问安全、动态、易用的良好效果。

奇安信云安全运营管理系统首批通过可信安全能力检测

近日，由中国信息通信研究院、中国通信标准化协会联合主办的“2023 SecGo 云和软件安全大会”在京召开。大会同期公布了 2023 年度可信安全最新评估结果，奇安信云安全运营管理系统（CSC）凭借优秀的云上资产发现能力、漏洞及风险检测能力，以及全流量高级威胁检测能力，在业界首批通过可信安全－安全运营中心能力检测。

社会责任

首个“留本基金”项目启动：清华之友－网络研究院奇安信奖助学金正式设立

9 月 14 日，“清华之友－网络研究院奇安信奖助学金”启动仪式在清华大学举行。此次捐赠模式为留本基金，并且是奇安信基金会“心安助学”项目捐赠的首个留本基金，将长期性地为清华大学网络科学与网络空间研究院学生提供社会实践支持、奖助学金等帮助。

“和美乡村计划”再出发 双坑村护栏修筑工程顺利竣工

近日，由北京奇安信公益基金会“心安助农 · 和美乡村计划”支持的广东省大埔县湖寮镇双坑村防护围栏项目顺利竣工，通往学校的临溪道路安全设施得到完善，双坑村 1168 名学生及村民的出行安全问题得到有效保障。

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，致力于支持乡村人居环境改善，推动乡村生态振兴，助力乡村生态宜居，重点支持乡村人居环境改善、环境污染治理、生态系统健康修复、资源高效利用等方面的工作。截至 2023 年 8 月，项目已经在四川、广东、北京、安徽等地开展，受益人数已接近 2.5 万人。

数据安全领域的创新方法、技术、产品和服务

作者 | Gartner

Gartner 在其发布的《 数据安全最酷供应商 》报告中，介绍了四家数据安全创新厂商的相关产品与服务，以期望帮助安全和风险管理领导者最大限度地提高共享数据资产的价值。

Gartner 认为，随着聚焦于数据保密和权限控制的技术加速创新，数据安全服务提供商可以支持实现对数据的细粒度高效控制。

报告中介绍的四家数据安全供应商的开拓性创新技术，可以对数据进行有效保护，免受未经授权的访问和滥用。无论是使用加密、主动数据防泄漏（DLP）还是扩展企业数字版权管理(EDRM) 控制技术，相关数据安全服务的目标就是使组织能够充分利用其数据，并确保不受信任的第三方或恶意内部人员，几乎没有攻击面可以利用。

主要发现

安全和风险管理 (SRM) 领导者希望通过提高数据的可用性和可访问性来获取更多的数据价值。然而，经常使用数据会导致攻击面增加，容易受到不太受信任的第三方和恶意内部人员的攻击。

为了解决这个问题，一些初创供应商正在基于当前学术科学进行产品创新或将成熟的商业产品进行扩展，以最大限度地减少攻击面，并降低数据泄露的风险。

相关产品可以做到如下创新：

· 扩展和简化对组织自身数据的传统数据控制，而无需控制人们使用的每个设备、网络和应用。

· 拥有已在关键环境中得到验证的、对在用数据的加密功能。

· 将在用数据保护扩展到设备和终端。

应对建议

为了缩小组织数据的攻击面，同时实现新的数据共享和数据处理用例，负责数据安全的 SRM 领导者必须：

（1）重新评估企业数字版权管理(EDRM) 产品，包括第三方扩展，以期通过加密保护内容，并在数据跨越公司边界后保留某种形式的应用控制。

（2）将创新的数据防泄漏 (DLP) 产品应用于更广泛的数据和选项。这是内部和外部使用和共享数据日益增长的需求所必需的。

（3）至少对最敏感的数据部署在用数据保护措施。

> 经常使用数据会导致攻击面增加，容易受到不太受信任的第三方和恶意内部人员的攻击。

> 无论是使用加密、主动数据防泄漏（DLP）还是扩展企业数字版权管理(EDRM)控制技术，相关数据安全服务的目标就是使组织能够充分利用其数据，同时免于攻击的风险。

最佳厂商概述

报告介绍的4家数据安全供应商，其中两家厂商Cyberhaven和ITsMine致力于优化目前数据控制方案，使其更易于实施和操作。此外还添加了客户经常要求的功能。例如，将EDRM的覆盖范围扩展到组织需要与之共享数据的第三方。

另外两家厂商Enveil和VectorZero Technologies提供在用数据加密功能，使组织能够在其控制之外的环境中对敏感数据进行运算。一个经常提到的用例，涉及对需要在计算云中处理的高度敏感数据实施在用数据加密。但在当今数据驱动的世界中，几乎所有系统或设备（不仅仅是用于云计算的系统或设备）都可能处于在用数据保护的范围内，以防御勒索软件等恶意软件。

1、Cyberhaven

创新优势：Cyberhaven提供对组织敏感数据环境的新见解，无论数据类型、文件类型、加密或数据来源如何，并解决客户在传统DLP方法中发现的常见限制。通过将对敏感数据的检测与对用户行为的洞察相结合，Cyberhaven的数据检测和响应(DDR)终端代理和SaaS应用的API连接器基于数据上下文构建数据沿袭，并提供用户培训，所有这些都通过单个控制台进行管理。Cyberhaven检测和减轻内部风险和数据丢失事件的方法及其提供的广泛保护通过终端代理了解用户行为，将其产品定位为传统DLP解决方案的下一代替代方案。Cyberhaven的方法构建了比传统DLP解决方案更广泛的检测网络，可以减轻敏感数据暴露带来的SaaS和内部风险威胁。在检测不受监管的数据类型时尤其如此，例如，知识产权(IP)和源代码等，通常难以使用传统DLP工具实施策略。

挑战：Cyberhaven使用DDR缩写的消息传递及其数据安全方法，可能会与现有终端检测和响应(EDR)及扩展检测和响应(XDR)技术的供应商造成竞争紧张，这些技术旨在通过收购或收购来实现产品多样化。制定数据安全控制措施。“DDR”作为一个术语也可能会引起数据安全市场的混乱，因为数据检测和响应没有标准化的定义。此外，Cyberhaven可能面临来自终端DLP市场当前领导者的压力，这些领导者正在构建类似的数据沿袭控制，并将其终端DLP功能与用户和实体行为互连起来分析(UEBA)控制。云优先组织可能会发现Cyberhaven针对SaaS应用程序的数据安全控制与现有安全服务边缘(SSE)产品重叠，但不涵盖基础设施即服务(IaaS)数据存储库，而Cyberhaven依赖于合作伙伴和补充技术。

受益人群：

· 急于从创建到删除，全流程保护组织知识产权的SRM领导者；

· 负责减轻内部风险造成的数据损失，以及敏感数据暴露而产生的更传统风险的SRM领导者。

2、Enveil

创新优势：Enveil将同态加密(HE)和安全多方计算(SMPC)结合在一个产品平台中，使企业能够提取见解、搜索和分析大量数据，而不会泄露搜索内容或底层数据元素。即使在资源有限的环境中，它也能以最小的延迟完成此操作。Enveil对内存中数据的HE使用不会超出流行的基于云的计算实例或商业现成硬件的资源或规格。Enveil的ZeroReveal技术旨在允许数据保留在其原始位置，无需重新定位即可跨不受信任的域进行安全分析。

挑战：Enveil完全专注于保护处理过程中的数据或使用中的数据，并设计了ZeroReveal Search和ZeroReveal AI产品来补充现有的静态数据和传输中数据加密。因此，最终客户需要构建一个由多种加密产品组成的技术堆栈，以在不受信任的环境中实现静态数据和使用中数据的保护。这是在组织希望整合尽可能少的产品的时候发生的。此外，使用中数据保护市场正变得更加拥挤且竞争激烈。其中包括一些全球最大的技术供应商，如英特尔和AMD。

受益人群：

· 负责保护人工智能或机器学习模型，或其他分析环境数据隐私的

SRM 领导者。

· 需要共享或处理可能包含专有或敏感信息的大量数据并允许协作者进行安全分析的组织。

· 受隐私和数据保护法规约束的企业，需要分析跨业务运营或第三方的多个数据集，其中可能包括敏感数据或个人数据。

3、ITsMine

创新优势：ITsMine 的 Agentless Beyond DLP 是一个数据保护平台，它通过将 EDRM 和 AI 驱动的威胁检测动态直观地结合起来，取代传统的基于策略的执行模型，从而简化 DLP。它通过将组织数据存储库中的文件夹转换为虚拟保管库来保护敏感数据免遭破坏、勒索软件及恶意或粗心的内部人员的侵害，虚拟保管库可以对数据进行审核、跟踪和管理，甚至可以超越公司边界。在 Microsoft 信息保护 (MIP) 的推动下，虚拟保管库中的文件配备了文件 GPS、一种可以跨存储应用程序提供数据可见性和控制力的技术，无论位置如何。ITsMine 通过使用 AI 战略性地部署实时诱饵文件 (SoftwareMines) 来保护数据。这些模仿客户存储库中的敏感数据，并在出现意外访问、加密或泄露这些数据的尝试时“引爆”，从而向安全团队发出警报并自动拒绝对相关文件的访问。

挑战：该平台的一些功能依赖于基于 API 的通信，这些通信会受到延迟和可用性的影响。API 延迟可能会延长接收日志所需的时间，进而会削弱阻止设备的能力。EDRM 是一种通常被认为难以大规模正确实施的控制措施。ITsMine 需要让潜在客户相信情况已不再如此。该平台的一些 EDRM 功能使用 MIP 作为后端。Microsoft 可能决定在其产品中包含类似的功能，并与 E3 或 E5 许可证一起提供它们。

受益人群：

· 希望为客户提供轻量级、无代理的 DLP 解决方案的托管安全服务提供商，最终可以满足托管和非托管设备上数据保护的法规要求。

· 负责实施适合远程员工 DLP 解决方案的 SRM 领导者。ITsMine 的平台可以跨多个存储应用程序，提供一致的 DLP。

· 正在寻求一种更主动的 DLP 方法的 SRM 领导者，与传统的基于策略的执行策略相比，该方法产生的误报更少。

· 想要在公司范围之外审核、跟踪和管理文件的 SRM 专业人员。

4、VectorZero

创新优势：VectorZero 的 Active Data Vault 是一个产品平台，它将静态数据和使用中数据的加密结合起来。据供应商称，它可以非常快速地部署在几乎任何设备上和几乎任何位置。它使用多种隐私增强技术（PET），包括机密计算、HE 和 SMPC 。它支持在其机密计算飞地内处理通过加密、SMPC 或 HE 保护的数据。或者，如果从此 enclave 导出文件，则可以自动加密，即使它们被视为飞地内的明文。数据仓库可以位于服务器上，也可以位于设备和终端上，这极大地扩展了 PET 的范围。VectorZero 还实现了加密敏捷性，以便使用新兴的后量子加密算法。它正在部署一套量子安全算法，可用于终端上的存储、数据处理和传输中的数据。

挑战：VectorZero 最近才推出其产品，其功能在未来几年内可能会发生重大变化。

Active Data Vault 由硬件安全模块 (HSM) 支持，或者可以与客户的 HSM 集成，但目前它只能与 AWS 的密钥管理服务集成。

尽管该产品具有足够的灵活性，可以在其机密计算飞地内集成各种加密算法，但数据发现和分类功能的省略限制了其在飞地内应用一致数据安全策略的能力。

受益人群：

· 需要在内部或与第三方合作确保敏感数据处理安全的 SRM 领导者，因为该产品使他们能够在机密计算飞地内部署适当的加密控制。

· 负责或对如下内容感兴趣的 SRM 领导者：

· 训练人工智能模型并与第三方共享。

· 在数据驻留限制下使用公共云平台。

· 开展内部和外部分析和商业智能活动。安

关于作者

Gartner 是全球领先的信息技术研究和顾问公司

自动移动目标防御（AMTD）：网络安全的新范式

作者 | Ronen Yehoshua

勒索软件变得日益猖獗，平均每 10 秒就有一次勒索软件攻击发生。到 2031 年，这一数字可能会缩减至仅 2 秒。当今的网络攻击者实力强大且经验丰富，足以成功劫持国家政府，勒索赎金。但这并不意味着国家级实体是他们的主要目标。

相反，由于具有吸引力的努力回报比，勒索软件组织越来越多地针对企业机构进行攻击。根据 2023 年《Verizon 数据泄露调查报告》，勒索软件是泄露事件中最常见的行为类型，占报告泄露数据事件的 24%。

Verizon 的报告表明，对于勒索软件受害者来说，从攻击事件中恢复的总体成本正在增加。潜在的和延长的系统宕机时间、可能的处罚，以及泄露的客户、合作伙伴或员工数据，都会带来长期和极具破坏性的后果。首先防止攻击已成为当务之急。

在勒索软件防护和攻击缓解方面，端点检测和响应 (EDR) 及扩展检测和响应 (XDR) 是行业标准，它们结合使用签名和基于行为的检测方法来防御已知和可检测的威胁。然而，网络攻击者已经适应并开发了可以成功逃避 EDR 和 XDR 系统的策略和技术，其中包括内存攻击、无文件恶意软件和其他防御规避技术。多项研究表明，这些恶意软件占野外恶意软件的 30% 以上。

最近的例子包括逃避 EPP 和 EDR 解决方案检测的 BlackBasta 勒索软件的新变体、GuLoader（针对法律和投资机构的高级威胁）及 InvalidPrinter（高度隐秘的加载程序）。ProxyShellMiner 则是针对 MS-Exchange ProxyShell 漏洞的另一变体。

攻击者在过去几年中不断改进技术，为大规模勒索软件攻击创造了条件。两项进步对攻击者极其有利。

· 无文件恶意软件的兴起：攻击者更喜欢设计无法检测的恶意软件。这是因为 EDR 和 XDR 技术依赖于静态和动态分析来查找和检测恶意活动。静态分析技术检查文件、代码或二进制文件以识别潜在威胁。然而，无文件恶意软件不使用传统文件，也不留

> 自动移动目标防御 (AMTD) 技术使用多态性对攻击面进行移动、改变、混淆和 / 或变形，并破坏对手的杀伤链。

下任何静态内容可供分析，这使得恶意软件的检测变得极其困难。动态分析观察软件或文件在执行过程中的行为，通常比静态分析更有效地检测无文件恶意软件。然而，动态分析是资源密集型的，通常在沙箱或虚拟机等受控环境中执行。此外，动态分析旨在监控执行期间的行为；如果分析工具不（或不能）监视内存中相关的活动，那么直接在内存中运行的无文件恶意软件将会逃避检测。一些恶意软件也使用多态技术来隐藏其在内存的存在。因此，恶意软件可以表现为合法进程，使其难以检测和阻止。

·生成式人工智能工具的可用性：生成式人工智能可能会为攻击者提供更复杂的技术和更难防御的变体，并且其速度和规模难以维持。防护人员还担心 EDR 和 XDR 系统的应对式特性，因为检测通常发生在入侵之后，补救措施并不是完全自动化的。在勒索软件场景中，这意味着攻击者可能已经在网络内进行了横向移动。根据 2023 年《IBM 数据泄露报告》，检测和遏制攻击行为的平均时间约为 322 天。广泛使用人工智能支持的安全工具和自动化有助于将检测和遏制时间缩短至 214 天。然而，这仍然为攻击者留下了重要的时间窗口，可在网络内建立持久立足点，并可能泄露有价值的信息。使用具有 AI 防御功能的 EDR 和 XDR 系统的组织必须确保其底层数据集、训练集及开展学习过程的机器的稳健性和安全性，以保护系统免受未授权和可能武器化的恶意代码的侵害。

是时候改变安全范式了

攻击者利用多态性来逃避检测，但防御者也可以应用此技术。考虑一下：在发生攻击时，如果目标资源不存在或不断变化（移动），则以系统为目标的攻击机会就会显著降低。

自动移动目标防御（AMTD）技术使用多态性对攻击面进行移动、改变、混淆和/或变形，并破坏对手的杀伤链。AMTD 通过增加复杂性、不确定性和预防策略来有效地防范攻击。它的起源与防御狙击手的军事战略有关，依靠掩护和隐蔽，以及保持移动来消除射击攻击的机会。

假如训练有素且极其聪明的狙击手，需要瞄准隐藏或持续移动的目标，狙击的成功机会就会减少。狙击手甚至可能会因为反复不正确的误射而暴露自己。

AMTD 技术在应用程序加载到内存空间时发挥作用；该技术改变进程结构和其他系统资源的形态，并进行隐藏，部署轻量级陷阱来欺骗攻击者。由于无法访问原始资源，恶意代码就会失败，从而阻止攻击，并记录攻击，从而提供完整的取证信息。

即使现有的基于人工智能的检测和响应工具被绕过，这种预防优先的方法也可以阻止威胁。由于攻击被阻止，安全团队获得了关键的时间来调查威胁，同时知道他们的系统是安全的。AMTD 的确定性还意味着它可以生成高保真警报，有助于确定安全团队工作的优先级，减少警报疲劳。

AMTD 技术不会取代检测和响应系统。相反，它提供了额外的防御层，并补充了 EDR 和 XDR 工具集。AMTD 利用深度防御功能增强能力并强化整体攻击面，阻止现有检测和响应解决方案无法阻止的未知攻击。

勒索软件和其他网络攻击的日益流行和复杂，凸显了加强和推进端点保护的重要性。防守者应该借鉴对手的战术：采用他们使用的战术。不仅要尝试检测并追溯性修复攻击，还要不断发展以先发制人地防止攻击发生。 安

关于作者

Ronen Yehoshua

网络安全初创企业 Morphisec 公司首席执行官

研究：四类恶意包持续攻击 npm 软件供应链

作者 | 奇安信技术研究院

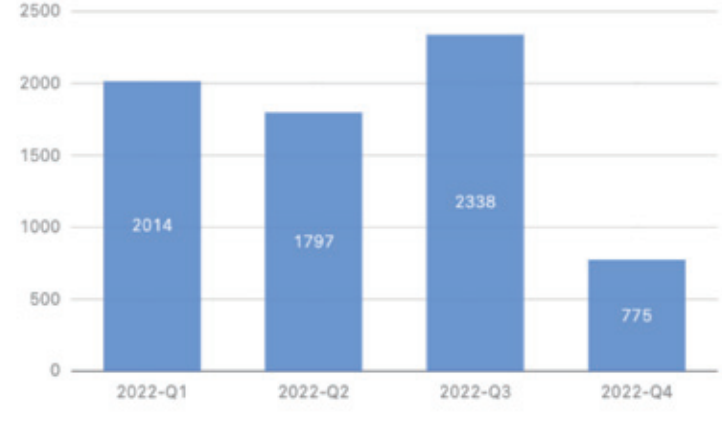
1、前言

在各种开源软件生态中，npm 生态是软件包数量最庞大、用户最为活跃的一个。得益于 node.js 等 runtime 的特性，Javascript 语言在后端系统等方面也可以发挥其作用，并随着 Typescript 的发展，这一趋势愈发明显。在如此庞大的生态之下，针对其进行的软件供应链攻击从未停歇过。

2022 年，奇安信技术研究院星图实验室研发的“天问”软件供应链安全分析平台对 npm 生态持续进行了多达 650 万次的安全分析，检测到了大量的恶意行为，发现了多起大型软件供应链攻击事件。

通过 2022 年一整年的监测分析，天问平台共计发现 6,924 个 npm 恶意包。通过深入分析这些恶意包，我们将其大致分为四类：信息窃取、反弹 shell、后门木马、挖矿病毒。

2022 年 4 个季度恶意包数量



2、整体趋势

在过去的一整年中，针对 npm 生态的软件供应链攻击呈现出持续化、自动化、隐蔽化的趋势。天问平台在 4 个季度分别发现了 2,014、1,797、2,338、775 个恶意包。其中 Q1、Q2、Q3 季度均发生了大型供应链攻击事件，由同一攻击者利用自动化手段上传了大量相似行为的恶意包，详细分析可见天问博客历史分析报告《【天问】Node.CuteBoi：大规模供应链挖矿攻击持续追踪》《【天问】滥用 Replit 服务进行自动化挖矿。Q4 季度未发现大型攻击事件》，所以恶意包数量较前三季度减少。

除此之外，针对 npm 生态的供应链攻击越来越隐蔽，从刚开始明显的恶意指令直接执行，到后面使用诸多类似代码混淆、通过依赖组合攻击、反沙箱检测、借助第三方平台隐蔽流量等手段来对恶意行为进行隐藏，企图绕过安全检测。

3、恶意包分析

通过对发现的 6,924 个恶意包的分析后，根据其最终恶意行为的目的，我们将其大致分为了四类：信息窃取、反弹 shell、后门木马、挖矿病毒。

3.1 信息窃取

针对 npm 生态的供应链攻击中，此类目的的恶意包最为常见，大约占据了 40% 的数量。这些包的内容大都非常简单，且有统一的模板。在安装完这些恶意包之后，会自动执行恶意代码所在的脚本，脚本会收集系统和用户信息并回传，这些信息包含用户目录、用户名、DNS 服务器等，有的恶意包还会将网卡信息、passwd 文件内容等一同回传。

这一类恶意包在刚开始时会使用非常简单直接的方式将受害者主机的信息进行回传，即在 npm 包的 script 字段直接执行系统命令。有关 script 字段的危害性和攻击手法的分析可见历史文章《【天问】两周 150+ 恶意包！npm 供应链攻击手法分析》。

上图中展示了一个简单的通过 script 字段执行命令的恶意包，攻击者通过 DNS 请求将获得的 hostname、passwd 内容进行 base64 编码后回传到攻击者的机器上。通过 DNS 回传相较于普通的 TCP 协议回传更具有隐蔽性，可以绕过许多通过流量分析进行的安全检测。在天问安全研究的历史文章中也对这部分内容进行过分析，详情可见《【天问】Node.DNS：基于 DNS 隐蔽信道的自动化供应链攻击分析》。

在这些信息窃取型的恶意包中使用了多种类型的回传地址接收信息，包括由第三方服务提供的信息接收平台，由 burpsuite 提供的代理网站，以及由攻击者自己搭建的服务及购买的域名等。通过对 6,924 个恶意包进行全面分析后，我们共发现了 70 个不同的回传地址域名，这些回传域名关联的恶意包数量如下图所示。其中使用最多的是 pipedream.net，共有 698 个恶意包使用该地址进行了信息回传。

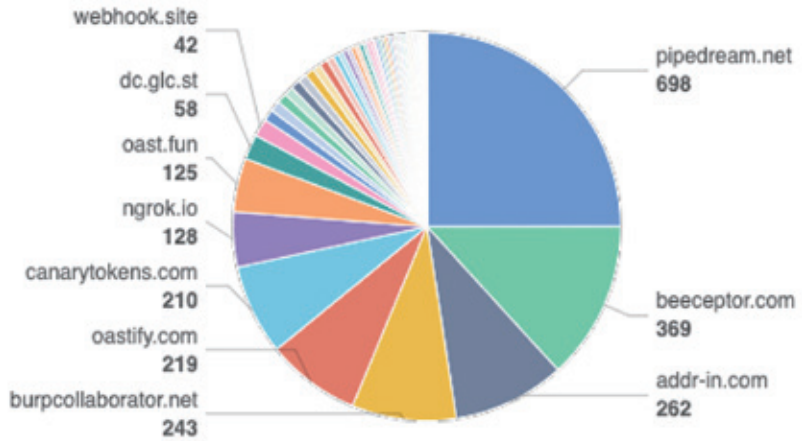
3.2 反弹 shell

这一类的恶意包行为危害性最大，一旦攻击成功，攻击者可以立即拿到机器当前用户的权限，并通过提权在机器上以最高权限执行任意命令。不过，这一类的恶意包也相对容易被检测到，其危害行为特征明显，不易于达到隐蔽攻击的效果。

3.3 后门木马

这一类的恶意包，主要目的是在用户机器上释放并执行已经精心制作好的后门木马。相较于前两种方式，这种攻击方式成本较高，因为后门木马一旦被使用后，很快就会被安全分

信息窃取回传地址使用频率



析人员逆向分析，提取其特征加入病毒库，下次再出现相同的木马很容易就会被识别出来。但这种攻击方式也有其优势，因为后门木马都是编译好的二进制程序，针对 js 及相关脚本的静态分析很难发现此类恶意行为。

在 2022 年年初，国外安全研究团队披露了一个跨 Windows、Linux、macOS 三个平台的恶意软件 SysJoker，并推测该恶意软件最初的攻击向量是一个受感染的 npm 包。通过天问软件供应链安全分析平台的分析，我们证明其最初的传播行为正是在 npm 生态中发生的。详细分析可见《【天问】SysJoker：以 npm 软件供应链为攻击入口的跨平台恶意后门分析》。

3.3.1 wsrcsv 攻击事件

在 2022 年和第四季度，我们发现了一个结合 typosquatting 在 npm 生态中进行后门木马传播的供应链攻击事件，因为这些恶意包最终都会释放恶意后门 wsrcsv.exe，我们称其为 wsrcsv 攻击事件。

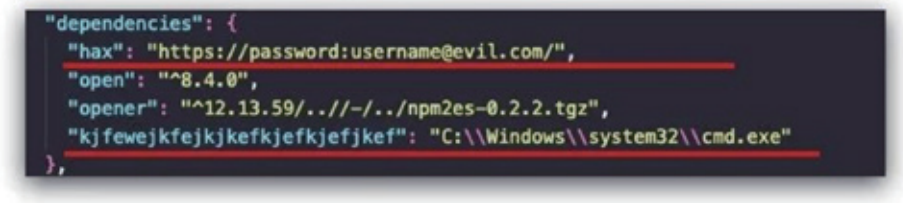
天问平台在 2022 年 10 月 2 日发现用户“nsrvmzuq”在 npm 生态中上传了 152 个 npm 包，这些包的名称大多与一些下载量较高的热门 npm 包相似，且都有相同的恶意行为。下表展示了部分仿冒包的名称和对应的热门 npm 包，可见两者包名极其相似，很多开发者往往无法准确识别，很容易误用恶意包而被攻击。

这些包安装的时候都会自动执行位于包内的 index.js 脚本，该脚本会从 Discord 下载一个 Windows 的快捷方式文件，并将其执行。所以这些恶意包的攻击对象都是 Windows 系统。所获得的快捷方式在运行时会执行其包含在其中的脚本代码，调用 Windows 系统中的 PowerShell 再次从第三方托管平台下载一个 vbs 脚本，用于下载最终的恶意后门 wsrcsv.exe 并进行提权和运行。

3.3.2 ByPTR 事件

2022 年 9 月 28 日，天问平台监测到一起软件供应链攻击事件，由攻击者 andlipoen 上传了一个名为 chameleonbasic 的恶意 npm 包，根据天问平台历史数据分析发现，该攻击者在同年 3 月也进行过攻击活动。由于攻击者在攻击时多次使用了

恶意包	正常的流行包	正常包周下载量
psotcss-value-parser、potscss-value-parser、posctss-value-parser	postcss-value-parser	30,402,449
micromathc、micromacth、micrmoatch	micromatch	38,910,761
estravesre、estraveres、estarverse	estraverse	45,017,510
glob-paretn、glob-parnet、glob-paernt	glob-parent	44,451,101
string-witdh、string-wdith、string-iwdth	string-width	58,958,116
tsilb、tlsib、tslbi	tslib	94,377,701
igonre、ingore、ignroe	ignore	31,252,902
unievrsalify、univesralify、univeraslify	universalify	35,887,945



“.ByPTR”这个独具标识性的字符串，所以我们称其为 ByPTR 攻击事件。

在这次攻击中，攻击者对下载后门 loader 的 js 脚本进行了代码混淆处理，所获取的 loader 脚本执行后会下载真正的后门文件，后门文件被下载到受害者机器上后会被立即执行，脚本等待 10s 确保后门成功执行之后会删除下载的后门文件，提高攻击隐蔽性。

3.4 挖矿病毒

这一类恶意包的目的主要是窃取计算资源，让受害者的机器成为一个算力节点，为攻击者的矿池持续提供算力。在 2022 年 6 月和 7 月，npm 生态中就发生了一起大规模的供应链挖矿软件投毒事件。不过与常见恶意包不同的是，这些挖矿软件利用了像 Replit 这种在线运行服务的系统资源来进行挖矿，其攻击手段更加巧妙，详细分析可见历史文章《【天问】Node.CuteBoi：大规模供应链挖矿攻击持续追踪》《【天问】滥用 Replit 服务进行自动化挖矿》。

4、攻击手法总结

除了较为常见的攻击手法，如代码混淆、通过 script 进行命令执行、利用 DNS 进行隐蔽信息回传等，在过去一年中，针对 npm 生态的供应链攻击中又出现了一些更为隐蔽和高级的攻击手段。

4.1 利用 DNS 获取攻击指令

2022 年 10 月 31 日，用户名为 michaljaz 的攻击者在 npm 生态中上传了一个名为 nodexda 的恶意包，该包会利用 Google 公开的 DNS 服务来解析一个域名，攻击者将恶意代码隐藏于域名的 TXT 类型解析的 data 字段中，由此达到隐蔽传输恶意指令的目的。

4.2 通过依赖包配合共同攻击

2022 年 9 月 17 日，攻击者上传了一个名为 jqdc 的恶意包。在安装恶意包 jqdc 的时候会执行一个包内的脚本，如果单独看这个包无法发现其恶意行为，因为它将恶意的执行代码通过包依赖的方式放在了另一个包内，且在这个依赖包内进行了加密处理，所以单独对这两个包进行静态分析都无法直接发现其恶意行为。

这种组合依赖的的攻击方式在我们团队最新发布的论文《Investigating Package Related Security Threats in Software Registries》中也有提到，其中提出的攻击点 R1（Package Reference Attack）就是对该攻击的系统性研究和测量。

4.3 利用 dependencies 进行网络请求

由于 npm 包中的依赖声明支持解析 http/https 的资源，在 dependencies 字段中写入一个位于网络的 tarball 也可以成功下载并作为一个依赖的包安装使用，所以攻击者利用这一点进行了一些测试行为。由此可见，这种攻击方式虽然较为明显，容易被发现，但确实可以用来在受害者的机器上发起 TCP 请求，获取受害主机的 IP 网段等敏感信息。

5、结语

综合本文对 2022 年 npm 生态供应链攻击的分析，我们可以看到，攻击者的攻击行为越来越隐蔽，攻击手法也越来越刁钻。攻击者更加偏好于使用现在飞速发展的云服务来达成攻击链，更好地隐藏其恶意行为。这对 npm 生态供应链攻击及恶意包的检测的要求越来越高。天问软件供应链安全监测平台对 npm 生态中上传的 npm 包进行持续且实时地监测分析，结合静态分析和天穹沙箱动态分析的优势，以及通过大量恶意包深入分析得来的长期规则沉淀，大幅度降低了恶意包检测的误报率，提高了分析的精准度。我们将持续关注 npm 生态的软件供应链安全问题，共同推动软件供应链安全的进步。安

关于作者

奇安信技术研究院是专注于网络空间安全相关技术的研究机构，聚焦网络空间安全领域基础性或前沿性的研究课题，结合国家和社会的实际需求，开展创新性和实践性的技术研究。

安全事件运营 SOP：蜜罐告警

作者 | 武鑫

本文将从基础概念、运营处置和反向攻击三个维度，对蜜罐应用和告警事件运营 SOP 进行阐述。

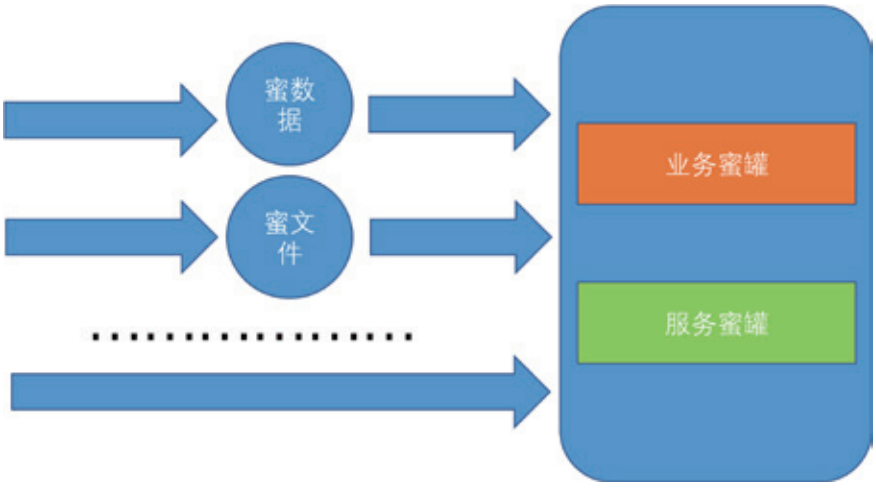
1. 蜜罐基础概念

1.1 什么是蜜罐

一种广泛用于企业安全建设中的入侵检测 / 威胁诱捕技术，从使用的角度来看，其实就是一个具备告警功能、甚至反制能力的陷阱。在不对称的攻防环境中，相对主动的帮助防守方发现攻击。蜜罐可以针对攻击者的攻击行为进行告警，一碰就报告；蜜罐可以伪装成攻击者感兴趣的目标（数据 / 服务 / 系统），吸引攻击者去触碰；蜜罐还可以藏着攻击武器，在攻击者连接之后，索要他的身份信息或进行攻击。

1.2 有哪些蜜罐

通常会按照交互程度分为低交互和高交互，交互程度越高、诱骗攻击者越深入，越有可能获取更多攻击者的信息。但仅从攻击检测来说，低交互的蜜罐足以使用，按功能可分为数据蜜罐、服务蜜罐和业务蜜罐。



- **数据蜜罐**：又叫面包屑，包括蜜数据、蜜文件、蜜邮件……洒落在内外网的各个角落，均是攻击者信息收集时关注的数据或文件，如在 GitHub 上传存在敏感蜜数据的代码、在内网服务器上存储蜜数据……引导攻击者访问蜜环境。
- **服务蜜罐**：对外开放 22、23、3389 等可能存在风险的高危端口及服务，部署在业务系统周边及全局设计部署在各网段，一触碰就产生告警，常见的工具或蜜罐系统有 opencanary（具备 Web 控制台进行管理）、HFish、Kippo、MHN、T-POT 等。
- **业务蜜罐**：伪装成业务系统（业务系统克隆），或业务系统的一个不常碰到的功能点，混淆攻击者的视听并起到告警作用。初级水平，常用 setoolkit 等工具进行目标系统静态资源提取，提取之后仍需修改网站源代码才能跑通；更高一点的水平已经实现流量重放，根据攻击者的请求重放 API 的 response，包括对一些攻击行为的响应。

1.3 蜜罐的应用

在重要系统旁部署蜜罐、在各内网网段部署蜜罐、在互联网上部署蜜罐（尤其需要注意安全性，单独规划蜜罐

网段，在网络层进行隔离，避免“引狼入室”），总之就是大范围部署上线、下线、卸载、测试、数据备份及恢复等对蜜罐的管理动作，故需统一管控平台进行日常运营。在整个过程中，至少需要考虑蜜罐等多样性和存活率。

- **蜜罐的多样性**：各类低交互的蜜罐（业务蜜罐 & 服务蜜罐），如 oa、crm 等攻击队关注的系统应该要有，ssh、rdp、tomcat 等系统及应用服务也需要覆盖，保持足够多的种类，可增加发现攻击的可能性。
- **蜜罐的存活率**：在管理平台设计时，加入对蜜罐存活的判断，定时去探活。解决蜜罐部署很多但面对攻击行为时不能告警的窘境。

2. 安全运营 SOP

蜜罐告警的场景比较简单，即一碰就响。在实际运营工作中，会遇到误报、不能直接找到源地址等问题。在介绍 sop 前，对误报原因进行了总结与分析，主要有系统误报、正常行为、违规行为，以及安全事件等下四类。

- **系统误报**：蜜罐管理系统出现问题，导致没有触碰蜜罐时，也产生告警。
- **正常行为**：用户在访问目标系统时输入错误、同网段 Windows 主机发现等可能会产生访问记录导致告警。
- **违规行为**：违反安全红线的行为可能产生告警，如业务方测试时，超范围漏洞扫描碰到蜜罐。
- **安全事件**：指攻击者在进行信息搜集、探测时触发的告警，也是蜜罐告警最主要关注和分析的类型。

2.1 找出攻击源

收到告警时，获得的 Sip 可能并不是真实的，有的是 NAT 或 LVS 的地址。此时就需要使用相关流量、日志、CMDB 平台等进行查询，找到真实的 Sip。

2.2 确定责任人

通过资产管理平台（cmdb/scmdb），查询 Sip 的资产 owner，包括归属人、运维人、安全责任人等。

2.3 判断告警场景

联系归属人（如果无归属人，则依次询问运维人、安全责任人）沟通 Sip 访问蜜罐的原因，以支撑接下来的处置动作。

2.4 执行处置动作

若是正常行为，则 close 告警；

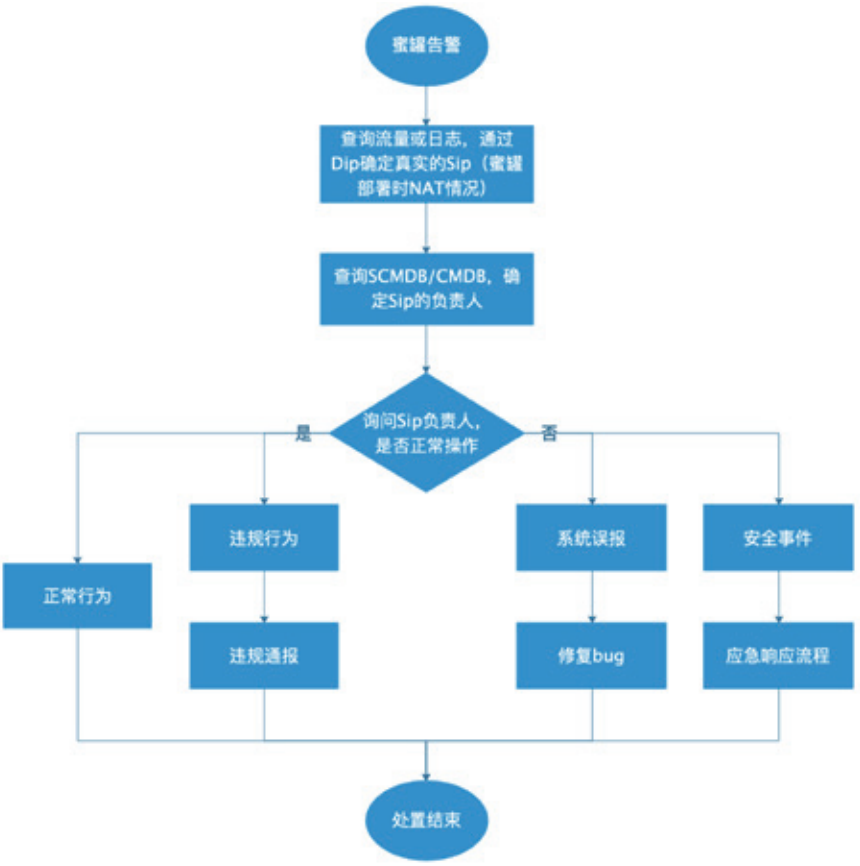
若是员工扫描行为，则根据是否报备等实际情况进行处理；

若是系统误报，则通知干系人排错修复；

若确认是安全事件，则立即开始应急响应流程。

2.5 SOP 流程图

2.1~2.4 描述的内容，如下图所示：



3. 蜜罐其他玩法

前面的章节主要聚焦在入侵告警

及处置，针对一个蜜罐收到告警、多个蜜罐收到告警聚合，均可以参照上述SOP进行处置，并且可部分实现（半）自动化。但蜜罐的应用已经不局限于被动的检测，更多的技术已经被应用到蜜罐上，实现了多元化的输出。

3.1 捕获 0day 漏洞

多用在互联侧进行大规模、工程化部署，以增加捕获0day漏洞攻击的可能性。这里提到的是可能性，说明实战场景中在该方面的收益并不大，也不适合于大多数公司。不过随着攻击识别和流量牵引技术的发展，在内网为攻击者准备一套特定的环境，已有可能让攻击者进入并引导其使用0day。

3.2 识别攻击者身份

在业务系统前端页面嵌入js脚本，获取攻击者社交账号信息，通过社工库碰撞出或工具指纹识别出攻击者身份。但这招需要储备存在敏感信息的API，需要攻击者登录过API所属网站并保持会话有效。

在国家级攻防演习活动中，防守队仅靠守住已经不能拿到很好的名次，需要溯源加分。面对经验丰富的攻击队员，这招大概率不生效，但谁又能保障他们每次都头脑清醒或者每个人都是高手呢?

3.3 反向控制攻击者

通过蜜罐引诱攻击者，在其不知情的情况下，控制其终端。通常可以利用已知漏洞进行攻击，最为常见的包括浏览器、MySQL反制、反向RDP攻击及伪造恶意程序等。

- **浏览器**：业务系统页面嵌入BeEF（浏览器攻击框架，The Browser Exploitation Framework Project）攻击代码，反向控制攻击者浏览器甚至拿到权限。
- **MySQL反制**：通过伪造MySQL报文来模拟服务；从客户端（攻击者终端）读取文件，可参照https://github.com/qigpig/MysqlHoneypot。
- **反向RDP攻击**：利用CVE-2018-20179、CVE 2018-20181、CVE 2018-8795等漏洞对rdesktop等软件进行攻击。
- **伪造恶意程序**：通过假装咬钩钓鱼邮件，将对方引入蜜网，散播存有后门的虚假敏感文件反击攻击者，如office文档木马、winrar压缩包等。

3.4 在攻防演习中应用

利用攻击者拿到终端据点后进行本地信息收集的招式，在员工终端存放蜜文件，引导攻击者去访问蜜系统，如:桌面上存放password.txt文件；内部IM聊天记录中收藏蜜环境地址与账密;浏览器中保存蜜环境域账密等。

4. 结语

利用攻击者拿到终端据点后进行本地信息收集的招式，在员工终端存放蜜文件，引导攻击者去访问蜜系统，可让防守方重新获得主动权，扭转坐等被动挨打的局面。安

关于作者

武鑫

虎符智库专家，奇安信产品安全负责人，兼负责公司内部蓝军工作。擅长从攻防视角进行甲方企业安全建设，在软件开发安全、供应链安全、攻防对抗方面有一定研究。

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。

“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