极牛网络安全通讯 • 社群期刊

2021 年 12 月 第 6 期

网安观察

P21 阿帕奇 Log4j2 组件曝出“核弹级”漏洞

P12
CTFWAR 2021网络安全攻防对抗联赛总决赛圆满收官

P14 美国"加强软件供应链安全实践指南"解读
P25 软件供应链安全：开源软件安全再受拷问
P29 经营安全推动网络安全技术变革

第 6 期
2021年12月

极牛网

极牛网 网络安全行业媒体

致力于促进中国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



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。

开源漏洞风险显现
软件供应链安全挑战巨大

2021年12月，本以为今年的网络安全行业再无重大消息了，只等着安心跨年之时，横空出世影响全球的Apache Log4j2组件"核弹级"安全漏洞让安全工程师们陷入紧张地排查和修复工作中。

阿帕奇(Apache) Log4j2 组件曝出严重安全漏洞，令开源软件的安全问题再受关注。开源软件加速创新，目前已大行其道，主流软件都会使用大量开源代码。但开源软件是否比闭源软件更安全的争论却一直没有终结。

数年前，开源拥趸者就宣称，开源软件相比于商业闭源软件更安全，原因包括开源软件具有代码公开、易获取、可重用的特点，比闭源软件能够获得更多开发者的关注，因而修复漏洞和发布补丁的速度更快，从而针对所遇见的问题提供相应的解决方案，因此，开源软件宣称提供了真正的透明度、更快的安全更新。

从全行业来看，我们需要在国家、企业、用户、检测机构等 4 个层面着手，体系化应对开源软件的安全风险。

（一）国家层面组织开展开源软件源代码检测工程

建议国家相关部门组织有业务基础的科研机构开展开源软件源代码检测工程，并将检测的成果以一种安全可控的方式向商业软件制造商及关键岗位的企业共享，尽可能降低开源软件漏洞对社会各行各业的影响。

（二）企业层面建设开源软件安全治理体系

对于明确需要引入的开源软件，在加强版本控制的基础上，一方面，开展安全风险评估检测；另一方面，持续跟踪相关的漏洞情报，时刻提防软件供应链攻击。

（三）用户侧建立软件安全渗透测试机制

企业在开展软件采购时，应向供应商明确要求提供软件中包含的开源组件，"用了什么，什么版本，软件来源"，并在验收时进行细致核查。

信息安全产品是重要信息系统安全防护的重要组成部分，其自身的安全性将影响重要信息系统的安全。开源软件安全性的争论显然短时无法终结，而其安全性的维护则要依靠开发者与使用者等多方协作来实现。

总顾问

叶绍琛

2021年12 月31日

CONTEN

目录



安全态势

P4 | 北美天然气供应商 Superior 遭勒索攻击，部分系统下线
P4 | 菲律宾两大银行遭黑客入侵，部分客户存款被盗
P4 | 印度总统莫迪推特账号被盗，发布加密货币推广消息
P5 | 北京冬奥会测试赛期间处理网络安全事件 300 余个
P5 | 国际连锁超市 SPAR 遭勒索攻击，超 300 家门店支付系统中断
P6 | 谷歌 Chrome 浏览器安全漏洞预警
P6 | Apache Log4j2 存在远程代码执行漏洞安全公告
P6 | Grafana 任意文件读取 0day 漏洞安全风险通告
P7 | 国内攻防演习 11 月态势：哪些薄弱点最易被利用?
P10 | 国家标准《信息安全技术 网络安全信息共享指南》公开征求意见
P10 | 中国首次就规范人工智能军事应用问题提出倡议
P10 | 《2021 年工业互联网安全标准体系》正式发布
P11 | 工信部发布《“十四五”大数据产业发展规划》
P11 | 美澳签署 CLOUD 法案双边协议，将跨境获取敏感数据
P11 | 俄罗斯拟修订信息法，公开移动通讯数据打击犯罪
P11 | 美国运输安全管理局发布铁路行业网络安全指令

赛事报道

P12
CTFWAR 2021网络安全攻防对抗联赛总决赛圆满收官

P14
美国“加强软件供应链安全实践指南”解读



CONTENTS



专题报道

P25
软件供应链安全：开源软件安全再受拷问

P29
攻与防的角力，经营安全推动网络安全技术变革

P33
奇安信椒图：我赌你的服务器里没有恶意文件



第 6 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
安全态势主编：乔跃春
网络攻击主编：王新睿
漏洞情报主编：黎治声
移动安全主编：蔡国兆
安全人才主编：林俊濠
安全产业主编：张　程

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：深圳市龙岗区江灏科技园1栋西座
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。

事件篇

Log4j2 组件严重漏洞在网上流传后引发全球震动，遭到网络犯罪分子疯狂滥用，已有一家行业龙头疑似被勒索软件攻陷；针对政治敏感人群的攻击频发，美国务院多名官员的手机被间谍软件入侵，印度总统莫迪的推特账号第二次被劫持。



北美天然气供应商Superior遭勒索攻击，部分系统下线

据 inforisktoday 12 月 15 日消息，北美天然气供应商 Superior 在上周日遭遇勒索软件攻击，暂时下线了计算机系统和应用程序。公司初步调查显示，没有任何客户和个人受到损害。有安全专家认为，虽然勒索攻击的规模尚不清楚，但是 Superior 因攻击而被迫下线系统，意味着此次勒索攻击已经取得了一定成果。据悉，Superior 提供天然气、石油蒸馏等相关产品和服务，在美国和加拿大拥有超过 78 万的客户。

菲律宾两大银行遭黑客入侵，部分客户存款被盗

据东博社 12 月 13 日消息，菲律宾社交媒体上日前盛传，菲律宾最大银行金融银行（BDO）一些客户的存款被黑客盗取，有报道称这些钱被转移到友联银行（UBP）的一些账户上，并用以购买虚拟货币。菲律宾中央银行行长陆诺表示，央行正在监控社群媒体用户投诉银行帐户遭黑客入侵事件激增的现象，并与相关银行合作，以补偿等方法解决问题。目前，涉事银行尚无法估计有多少资金遭到移转。

印度总统莫迪推特账号被盗，发布加密货币推广消息

据环球网 12 月 12 日消息，印度总理办公室称，莫迪的个人推特账号目前暂时被盗，已进入保护模式，并提醒人们忽略在此期间该账号发布的任何内容。莫迪账号被盗期间曾发推文称，政府要给全国民众发加密货币。推特公司表示，目前此账号已恢复使用。这已经不是莫迪的推特账号第一次被黑客盯上，去年 9 月，该账号也曾被盗，并呼吁印度民众就新冠肺炎疫情捐款。

Log4j2 严重漏洞引发全球震动：网络犯罪分子疯狂滥用

12 月 9 日，Java 日志记录组件 Apache Log4j 任意代码执行漏洞（CVE-2021-44228）曝光，在国内外互联网上引发了腥风血雨。奇安信司南平台监测发现，漏洞曝光后几个小时就有了规模攻击流量，并陆续

涌现多个僵尸网络、勒索软件、挖矿木马家族滥用传播。全球范围也出现了受害案例，有勒索软件疑似利用该漏洞攻击了美国大型人力资源供应商 Kronos（内部使用 Java 技术栈），导致薪资服务下线，恢复需要数周时间，数千家公司面临暂时无法计算和发放员工工资的窘境。

北京冬奥会测试赛期间处理网络安全事件 300 余个

据人民网 12 月 7 日消息，工信部官网发布消息称，为营造北京冬奥会测试赛安全稳定的网络环境，工信部网安局组织相关单位 1 万余人全力协同进行值班值守和应急处置等保障工作。期间，持续开展网络安全漏洞、移动恶意程序、恶意 IP 地址、僵尸网络等网络安全威胁监测与处置，累计屏蔽恶意程序发送端 IP 地址 9000 余个，组织修复漏洞隐患 200 余个，处置网络安全事件 300 余个。

国际连锁超市 SPAR 遭勒索攻击，超 300 家门店支付系统中断

据天空新闻 12 月 7 日消息，国际连锁超市 SPAR 遭遇勒索软件攻击，收银和 IT 系统被迫关闭。位于英格兰北部的大约 330 家 SPAR 商店受到影响，这些商店很多不得不选择关闭或转为仅使用现金支付。攻击发生后，SPAR 发布声明称正在尽快解决问题，但没有告知系统恢复所需的预期时间。今年 7 月，因收银和自助服务机遭攻击被关闭，瑞典连锁超市 Co-op 超 500 家门店也大面积暂停营业。

美国务院多名官员的手机被以色列公司间谍软件入侵

据海外网 12 月 4 日消息，一名身份不明的攻击者使用总部位于以色列 NSO 集团开发的间谍软件，侵入了 9 名美国国务院官员的苹果手机。过去几个月发生的这起黑客行动，影响了在乌干达的美国官员及其要处理的相关问题。此次报告的黑客攻击事件，代表了首次通过 NSO 技术对美国官员进行的最广泛的黑客攻击。NSO 集团次日表示，没有迹象表明其工具已被使用，但集团已取消相关账户，并将根据报道进行调查。

以色列和伊朗网络战范围扩大，无辜平民成攻击目标

据澎湃新闻 11 月 28 日消息，以色列和伊朗的数百万普通民众被两国之间近期的一系列网络战波及。在伊朗，燃油分配系统受到网络攻击。在以色列，一些普通公民的私生活细节被公布在网上。近几周，伊朗全国燃油分配系统遭到网络攻击，造成该国 4300 个加油站瘫痪，耗时 12 天才恢复正常，导致许多加油站前大排长龙。有美国国防官员将此次网络攻击归咎于以色列。燃油系统遭袭的几天后，以色列一家医疗设施和一个流行 LGBTQ（指性少数群体）约会网站遭到网络攻击，特拉维夫一位著名播音员的私生活细节被上传到社交媒体。

中国台湾最大券商遭黑客攻击：客户自动买入港股，瞬间亏掉 33%

据券商中国 11 月 27 日消息，包括中国台湾最大券商元大证券在内的多家券商的交易系统，疑似遭到黑客的“撞库攻击”，大量客户的证券账户被自动“下单”、批量买入港股。其中，更有投资者账户被动买入深蓝科技控股（01950.HK），当天股价遭遇闪崩暴跌，单日跌幅高达 33%。随后，中国台湾证期局证实，确实收到了部分券商的通报信息，客户的账户被盗自动下单买入港股。

漏洞篇

近日，Apache Log4j2 组件暴出严重安全漏洞，可能导致设备远程受控，进而引发敏感信息窃取、设备服务中断等严重危害。Log4j2 被广泛用于 Java 业务系统开发，为降低漏洞风险，国内多个监管机构发布安全预警。



谷歌 Chrome 浏览器安全漏洞预警

2021年12月16日，国家信息安全漏洞库（CNNVD）收到关于谷歌 Chrome 浏览器安全漏洞（CVE-2021-4102）情况的报送。攻击者可利用该漏洞在未授权的情况下，对远程服务器执行恶意代码，最终获取服务器最高权限。Chrome 96.0.4664.110 之前版本受此漏洞影响。目前，谷歌官方已发布新版本修复了漏洞，请用户及时确认是否受到漏洞影响，尽快采取修补措施。

Apache Log4j2 存在远程代码执行漏洞安全公告

2021年12月10日，国家信息安全漏洞共享平台（CNVD）收录了 Apache Log4j2 远程代码执行漏洞（CNVD-2021-95914，CVE-2021-44228）。攻击者利用该漏洞，可在未授权的情况下远程执行代码。经综合研判，该漏洞具有危害程度高、利用难度低、影响范围广的特点。目前，漏洞利用细节已公开，Apache 官方已发布补丁修复该漏洞。CNVD 建议受影响用户立即更新至最新版本，同时采取防范性措施避免漏洞攻击威胁。

Grafana 任意文件读取 0day 漏洞安全风险通告

2021年12月7日，奇安信 CERT 监测到 Grafana 未授权任意文件读取 0day 漏洞信息在互联网上公开。经验证，未经身份验证的远程攻击者可利用此漏洞读取服务器上的任意文件。鉴于此漏洞目前处于 0day 状态，建议客户尽快采取措施防护此漏洞。Grafana 是一个跨平台、开源的数据可视化网络应用平台。

奇安信 CERT：近期需重点关注的 18 个高风险漏洞

2021年11月，奇安信 CERT 监测到新增漏洞 1449 个。经人工研判，本月值得重点关注的漏洞共 98 个，其中，高风险漏洞共 18 个，包括多个微软产品组件高危漏洞、Hadoop 身份认证远程绕过漏洞、泛微 E-Office 文件上传漏洞等，约一半漏洞已遭在野利用或 PoC 已公开。

（关注公众号“奇安信 CERT”，发送“202111”可查看 11 月需重点关注的漏洞完整清单）



对抗篇

国内攻防演习 11 月态势：哪些薄弱点最易被利用?

作者 奇安信安服团队

一、本月演习整体情况

2021 年 11 月，奇安信 Z-TEAM 团队共承接攻防演习服务 19 场，其中，省级攻防演习 1 场，地市级攻防演习 2 场，本单位自主攻防演习 16 场。

本月攻防演习成果见下表。

二、本月任务目标特点

本月攻防演习和评估任务行业比较分散，覆盖目标面比较广，涵盖了政务、金融、能源、教育、医疗、互联网企业等目标，客户存在的安全问题主要涉及互联网侧业务系统未授权访问、系统平台历史漏洞、内部人员对钓鱼攻击防范意识不足、内网功能区缺乏安全隔离、内网口令复用及弱口令普遍等。具体情况如下。

1、漏洞利用仍是主要突破手段

本月任务表现出漏洞利用依旧是实现外网突破的主要手段。突破利用的漏洞以平台组件历史漏洞为主，如外部应用中非授权访问、Weblogic 反序列化、Shiro 反序列化、任意文件上传漏洞等，多因外部应用及系统组件缺乏日常安全巡检机制、对爆出的漏洞组件未实时升级更新造成，这些漏洞的存在使得目标网络有随时被入侵的严重安全风险。

本月攻防演习成果：

目标系统	靶标	强隔离内网	核心业务网	网站	堡垒机	安全设备	业务系统	服务器
数量	31	39	54	47	29	67	135	416

2、访问策略缺陷是重大安全隐患

本月任务中，多个行业网络的不同外部业务系统存在未授权访问问题，可以通过未授权访问漏洞直接访问这些外部系统后台，进而可以利用访问权限执行后台命令或获取后台配置文件、数据库等敏感信息。未授权访问多因对外部接入的安全配置或权限认证相关策略设置存在缺陷，导致对外部用户的访问地址、访问权限缺乏限制，未授权访问漏洞利用成为了外部突破的重要途径之一。

3、钓鱼攻击是实现突破的有力辅助

本月任务中，针对特殊行业目标系统网络，钓鱼攻击成为主要突破手段，并且具有较高的成功率，主要由于金融、教育、医疗这类目标业务具有较大的开放性，并且内部业务人员网络安全意识不强，这些人员就容易成为钓鱼的重点对象，钓鱼攻击也成为了攻击者实现外部突破的高效手段之一。

4、弱口令和口令复用是内网重大安全隐患

本月任务表现出弱口令和口令复用仍是目标网络的重大安全隐患。弱口令或口令复用会导致目标系统内网安全措施形同虚设，尤其是内网堡垒机、网管系统、域控和网关等核心网络节点。弱口令和口令复用的存在，为攻击者实现内网重要服务器、网关路由、网管系统和域控等核心网络节点的拓展控制带来极大便利，最终致使业务内网全面失陷。

5、敏感信息泄露安全威胁严重

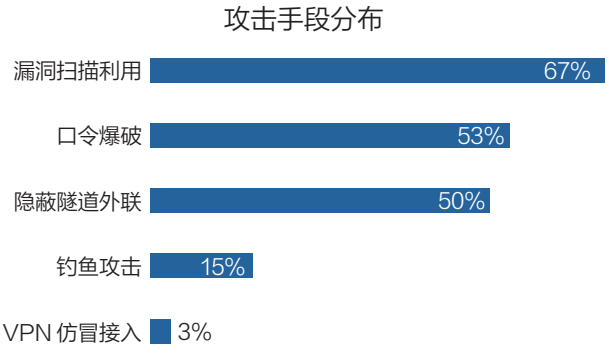
本月任务中目标外网敏感信息泄露较为严重，以 Gitlab 开发源码库为主，这些源码多包含重要的业务系统、应用平台的关键逻辑架构、函数调用实现和数据处理流程等关键信息，甚至包含一些极其敏感的认证信息，这些信息的泄露极容易被攻击者利用，进行有针对性的攻击，给目标网络带来严重的安全危险。

6、内部关键业务网络纵深防御不足

本月任务中发现目标网络内部关键业务的纵深防御措施部署不足，缺乏对关键业务系统网络接入或系统访问的安全过滤措施，主要表现为：互联网侧业务系统被突破后，通过边界服务器或普通内部人员主机即可触及一些重要的内网业务系统。内网纵深防御措施的缺乏，造成核心业务系统存在严重的安全隐患。

三、主要攻击手段分析

基于本月奇安信 Z-Team 团队实战成果分析，对目标网络的外网突破多通过互联网侧业务系统漏洞利用和钓鱼攻击实现，内网横向拓展以弱口令、口令复用及内部应用漏洞为主。使用的主要技术手段分布如下：



1、漏洞扫描利用

本月任务中漏洞利用对象主要集中在互联网侧 Web 应用和网络业务平台组件，涉及非授权访问、Weblogic 反序列化、Shiro 反序列化、任意文件上传及注入等漏洞。这些漏洞主要是由于目标系统网络接入安全策略设置缺陷、平台组件更新不及时引起的，直接反映出客户网络运维人员安全意识不足、网络运维缺乏常态巡检机制、对存在的漏洞及安全危险的应对不够高效等问题。

2、口令爆破

本月任务中口令爆破问题主要体现在目标内网的弱口令和口令复用，比较典型的案例为仅使用弱口令即可实现某目标的外网突破及内网靶标控制。主要原因是目

标网络没有依据安全规范要求进行账号口令设置和使用，缺乏对弱口令和通用口令的统一监管，如禁用简单弱口令、修改默认账户名口令、账号口令定期更新等。

3、隐蔽隧道外联

本月任务中因大部分目标系统网络无法通过外网直接访问，需要借助端口转发、隐蔽隧道技术等手段实现网络穿透。尤其是政务、金融、能源等对内网业务防守较为严密的客户网络，对目标的一些核心业务系统、靶标数据库的渗透拓展，需要通过多层通信隧道转发才能实现。

4、钓鱼攻击

本月任务中钓鱼攻击主要是针对金融和互联网企业目标人员，这些行业网络安全体系建设比较完善，防护相对严密，互联网侧系统可利用漏洞和其他突破途径较少。钓鱼攻击主要向安全意识相对薄弱的客服或商务等人员展开，实现外部突破。

5、VPN 仿冒接入

本月任务中目标网络内网多通过 VPN 实现分散网点入网访问，通过 VPN 仿冒接入可实现对目标网络不同网段业务的渗透控制。在对 VPN 的攻击过程中，VPN 仿冒接入认证信息的获取是攻击的关键环节，主要利用内网信息搜集、内网弱口令或口令复用等方式实现。

四、典型攻击手段实现案例

1、外部漏洞利用突破

（1）某目标网络互联网侧业务集成平台系统存在未授权访问和任意文件上传漏洞，通过未授权访问漏洞添加管理员账号，在其后台通过文件上传漏洞攻击获取集成平台系统服务器控制权限，实现外网突破，获取内网支点。

（2）某目标外网 E 企赢平台系统存在未授权访问漏洞，从中发现系统未授权访问接口和敏感认证信息，进而对 E 企赢后台服务器的控制，进一步实现内网接入。

（3）某目标外网泛微 E-mobile 存在反序列化漏洞，通过漏洞利用获取泛微 E-mobile 后台管理权限，进入目标内网。

2、钓鱼攻击

（1）某目标网络外网防护比较严密，以业务投诉为理由对其微信客服进行钓鱼， 控制目标客服人员主机，从中获取大量内网系统信息。

（2）对某目标网络业务助手后台维护人员进行钓鱼，控制目标人员终端主机，并以此为支点对目标内网进行探测渗透。

（3）某目标网络外部业务平台突破后，通过水坑钓鱼针对性围绕内部网络运维人员定点攻击，获取关键运维人员主机控制权限，从中获取大量有关堡垒机、综控系统、服务器的安全管理信息，实现目标内网彻底渗透。

3、口令爆破

（1）某目标网络内外网关键系统均存在弱口令，通过弱口令获取外网智慧办公平台（OA）的后台控制权限，并进一步通过弱口令获取内网堡垒机、核心业务靶标系统、Docker 管控平台及大量内网服务器的控制权限。

（2）某目标网络内网弱口令问题比较突出，外网突破内网后，内网 IT 运维系统、防火墙、虚拟管理服务器、VPN 网关、网络入侵防护系统、网络安全审计系统、数据库服务器、内网域控和综合业务系统等均存在弱口令，通过口令爆破，轻松实现权限控制。

（3）某目标内网 Exchange 邮件服务器存在口令复用情况，通过口令爆破获取邮件服务器控制权限，进而可查阅所有 Exchange 邮件服务器用户邮件。

4、VPN 仿冒接入

（1）某目标外网 VPN 网关存在命令执行漏洞，利用漏洞获取 VPN 网关控制权限，进一步通过 VPN 仿冒接入目标内网。

（2）通过口令爆破，成功登录外网 VPN 后台管理系统，通过 VPN 后台管理系统进行 VPN 账号添加、访问策略修改等操作，实现仿冒接入其他部门业务网络。

政策篇

国内，工信部发布《“十四五”大数据产业发展规划》，要求筑牢数据安全保障防线，并提出了数据安全铸盾行动；《湖南省网络安全和信息化条例》发布，成为全国首部网络安全和信息化地方性法规。

国际上，美国 CLOUD 法案获重要进展，美澳签署敏感数据跨境执法双边协议；俄罗斯拟修订信息法，公开移动通信数据打击犯罪。



国内

国家标准《信息安全技术 网络安全信息共享指南》公开征集意见

2021年12月17日，信安标委发布《信息安全技术网络安全信息共享指南》〈征求意见稿〉，公开征集意见。《指南》给出了网络安全信息共享活动要素、基本原则、共享范围和活动过程。《指南》指出，网络安全信息共享使网络安全信息资源价值最大化，更有利于对威胁和事件的获取、分析、研判、预警，增强组织的威胁认识和主动防御能力，减少威胁带来的影响和可能造成的损失。

中国首次就规范人工智能军事应用问题提出倡议

2021年12月13日，中国特命全权裁军事务大使李松出席联合国相关会议，提交了《中国关于规范人工智能军事应用的立场文件》。这是中国首次就规范人工智能军事应用问题提出倡议。文件聚焦人工智能军事应用涉及的研发、部署、使用等重要环节，并就如何在军事领域负责任地开发和利用人工智能技术提出解决思路。该文件是中国因应国际安全和新兴科技发展形势，积极引领国际安全治理进程的一项重要努力。

《2021年工业互联网安全标准体系》正式发布

2021年12月10日，在工信部网安局指导下，多个行业联盟、标准组共同发布《工业互联网安全标准体系（2021年）》。工业互联网安全标准体系包括分类分级安全防护、安全管理、安全应用服务等3个类别、16个细分领域及76个具体方向，对于发挥标准规范引领作用、推动建立网络安全分类分级管理制度、强化工业互联网企业安全防护能力、促进网络安全产业高质量发展，具有重要支撑作用。

《湖南省网络安全和信息化条例》发布

2021年12月3日，湖南省十三届人大常委会第二十七次会议表决通过《湖南省网络安全和信息化条例》，成为全国首部网络安全和信息化地方性法规。《条例》提出省内重要信息系统全部实行重点保护，明确了县级以上网信部门和有关部门依法履行网络信息安全监督管理职责。针对紧急状态下的数据使用、数据处理活动中应当注意的个人信息保护问题，《条例》也进行了制度设计。

工信部发布《“十四五”大数据产业发展规划》

2021 年 11 月 30 日，工信部发布《“十四五”大数据产业发展规划》，要求坚持安全与发展并重，筑牢数据安全保障防线，包括完善数据安全保障体系、推动数据安全产业发展。《规划》还提出了数据安全铸盾行动，分别从加强数据安全管理能力、加强数据跨境安全管理、建设数据安全监测系统三个方面展开进行。



美澳签署 CLOUD 法案双边协议，将跨境获取敏感数据

2021 年 12 月 15 日，澳大利亚和美国签署了一项 CLOUD 法案协议，允许美澳双边敏感数据跨境执法。该协议旨在防止严重犯罪、恐怖主义、勒索软件攻击、关键基础设施破坏和儿童性虐待方面作出努力。这是第二个在《澄清境外合法使用数据法案》(CLOUD Act) 框架下达成的双边协议。此前在 2019 年，美英签署了首份 CLOUD 法案协议。

俄罗斯拟修订信息法，公开移动通信数据打击犯罪

2021 年 12 月 11 日，俄罗斯经济部公布信息法修正案，提出公开用户通信连接、流量和支付信息，这样将允许运营商在征得用户同意的情况下将信息转给第三方，如银行用于信用评级或打击诈骗。目前，运营商只能根据法庭裁决或以不记名形式传递信息。修正案规定，公开的完整信息清单及提供这些信息的规程将由政府确定。俄经济部在解释性说明中说，根据目前用户数据库管理规程规定，企业不能随意使用掌握的信息，包括提供综合服务框架内的信息。

美国运输安全管理局发布铁路行业网络安全指令

2021 年 12 月 2 日，美国国土安全部运输安全管理局发布了两项安全指令，要求客运 / 货运铁路和轨道交通行业的组织采取措施加强自身网络安全，包括指定一名网络安全协调员、24 小时内向联邦政府报告网络事件、制定和实施网络安全事件响应计划、实行漏洞评估等。该指令将于 12 月 31 日生效，相关组织将有 90 天的时间进行网络安全漏洞评估，180 天的时间实施网络安全事件响应计划。

联合国教科文组织发布全球首份人工智能与伦理协议

2021 年 11 月 25 日，联合国教科文组织正式通过了首份有关人工智能伦理的全球框架协议，旨在促进人工智能为人类、社会、环境及生态系统服务，并预防其潜在风险。《建议书》包含规范人工智能发展应遵循的原则及在原则指导下人工智能应用的领域，包括确保透明度、行动力和对个人数据的控制来保证个体得到更多保护，改善数据保护和个体对自身数据的了解和控制权的行动，并明确禁止使用人工智能系统进行社会评分和大规模监控。

英国政府提出新法案，禁止联网智能设备设置默认密码

2021 年 11 月 24 日，英国政府提出《产品安全和电信基础设施法案》，要求禁止联网智能设备设置默认密码，需披露获得重要安全更新和补丁的最短时间，必须提供公开漏洞报告联系方式等。新法案覆盖了几乎所有智能家居产品和联网消费电子产品，不遵守规定的企业将面临最高 1000 万英镑或全球年营业额 4% 的巨额罚款。

政策解读

CTFWAR 2021网络安全攻防对抗联赛总决赛圆满收官

2021年正值建党100周年，深入贯彻习近平总书记关于网络强国的重要思想特别是关于国家网络安全工作"四个坚持"的重要指示精神，落实网络空间的竞争，归根到底是人才竞争的指示要求，举办2021年CTFWAR网络安全攻防对抗联赛。



本次大赛深入贯彻习近平总书记关于网络强国重要思想，秉承「公平、公开、公正」的赛事原则，旨在选拔优秀网络安全人才，促进网络安全技术交流，提高全民网络安全意识，筑牢网络安全基石。

本次大赛设置线上赛、线下赛、精英赛和青少年专项赛4个部分，面向网络安全从业人员、技术爱好者、院校学生和青少年等各类群体开展。通过由浅入深的赛制，培养参赛选手的网络安全攻防实战能力，推动建设创新实战型网络安全人才队伍，为国家网信事业高质量发展提供更有力的人才保障。

指导单位：国家网络空间安全人才培养基地
主办单位：CTFWAR网络安全攻防对抗联赛组委会
承办单位：华云信安(深圳)科技有限公司
媒体支持：极牛网-中国网络安全行业门户
赛事官网：www.ctfwar.org.cn/2021/



CTFWAR网络安全攻防对抗联赛，是国际范围的知名网络安全攻防对抗赛事，由CrashCTF攻防赛发展而来，CTFWAR联赛采取线上攻防对抗选拔赛结合线下全场景仿真攻防赛的形式。

CTFWAR攻防战争平台是知名的网络安全攻防靶场练习平台和竞赛平台，也是CTFWAR网络安全攻防对抗联赛的官方平台，以游戏的形式融入多种网络攻防场景，采取主流的CTF夺旗赛和AWD攻防赛的答题模式。

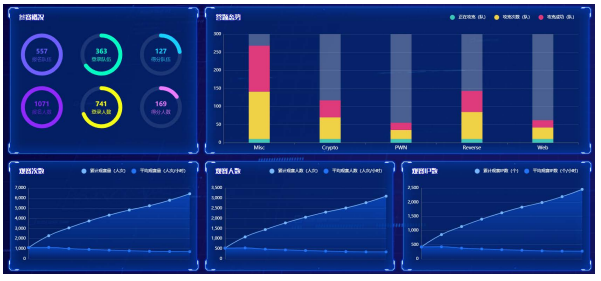
在CTFWAR2021总决赛的华中地区分站赛现场，中央电视台教育频道对本次赛事进行了全面的跟踪报道，在现场记者采访了CTFWAR网络安全攻防对抗联赛的创办人、

知名网络安全技术专家陈鑫杰。



陈鑫杰表示，网络空间已经成为继海、陆、空、天之后的第五空间域，保障网络空间安全，就是保障国家安全。网络安全的本质就是攻防对抗，而攻防对抗的核心关键就是安全人才。现如今，我们国家的网络安全人才非常紧缺，通过与高校联合举办CTFWAR这样的攻防赛事，能够让更多在校学子关注并从事安全行业，一起推动网络安全事业发展。





在总决赛现场，选手们紧锣密鼓地开始攻克赛题，摇光安全战队率先拿下签到题关卡一血，其余战队势如破竹，紧追不舍。



CTFWAR攻防战争赛事平台通过云攻击终端的形式让选手快速获取攻防环境，能够实现对赛事全程攻防数据的全量回收和实时AI分析，通过云终端的形式能更好地实现对武器化级别工具的管理，更好地在赛事中体验实战程度更高的攻防技战法。



排名	队伍名	总分	Misc			Crypto		PWN		Reverse		Web	
			签到	猜圈	进入	Cr	Cr	Li	Ha	Li	cm	Yo	Be
1	摇光安全	1734	69	278		152	228	334	286	130			257
2	AhiSec	1506	69	278		152		334	286	130			257
3	1024	1448	69	278		152	228	334		130			257
4	酸菜棒棒鱼二号机	1347	69	278		152	228	334	286				
5	雷神之锤	1336	69			152	228			130		500	257
6	NFSCE	1249	69	278		152		334	286	130			
7	思而听TaL小队	1228	69			152		334	286	130			257
8	数字丹青	1228	69			152		334	286	130			257
9	Spirit	1199	69			152	228	334	286	130			
10	红刃安全	1143	69	278		152	228		286	130			

CTFWAR2021总决赛在2021年12月31日17点圆满落下帷幕，经过紧张的角逐，最终“摇光安全”战队摘下了CTFWAR2021总决赛的一等奖桂冠。

一等奖：摇光安全

二等奖：AhiSec、1024、酸菜棒棒鱼二号机

三等奖：雷神之锤、NFSCE、思而听TaL小队、数字丹青、Spirit

◎ **极牛网 专题报道**

政策解读

美国“加强软件供应链安全实践指南”解读

2021年5月12日，美国总统拜登签署了“关于改善国家网络安全(EO 14028)”的行政命令，其中第4节“加强软件供应链安全”的(e)条款要求：初步指南发布90天内(不迟于2022年2月6日)，NIST应发布加强软件供应链安全实践的指南，并明确了指南需包含的10余项具体内容(表3一二列)。

对此，NIST修订了其2020年4月发布的《安全软件开发框架(SSDF) V1.0》，形成V1.1草案，并于2021年9月30日至11月5日完成公开征求意见。

1、SSDF基本原则

“安全左移”的理念已得到广泛共识，软件供应链安全保障也常基于软件生命周期模型，但明确详细处理软件安全的SDLC模型却很少，大多是将安全实践添加其中。

SSDF描述了一组基于已有标准、指南和安全软件开发实践的基础可靠的高层级最佳实践，可帮助使用者实现安全软件开发的目标。实践直接或间接(如保护开发环境)涉及软件本身，即框架考虑了软件供应链安全应包括的软件自身及相关生产要素的安全。

SSDF的重点在于实现安全软件开发实践的结果，而没有明确实现它们的工具、技术和机制。SSDF并不要求所有组织具有相同的安全目标和优先级，框架中的建议恰恰反映了软件生产者可能的独特安全预期和软件使用者可能的独特安全需求。每个实践实现的程度和形式根据生产者预期的变化而变化。

2、SSDF实践分类

SSDF是关于安全软件开发的一组实践，呈现为一张描述实践的表格，可根据需要方便地进行扩充、调整或删减。SSDF V1.1草案共包含4类19项实践(表1一二列)。

· **组织准备(PO)：**此类实践用来确保已准备好组织层面执行安全软件开发的人员、过程和技术(某些情况下针对单独的项目)，共5项，根据行政令要求，新增了实践“软件开发安全环境(PO.5)”；

· **保护软件(PS)：**此类实践用来保护软件的所有组件不受篡改和未授权访问，共3项；

· **生产安全性良好的软件(PW)：**此类实践用于尽量减少软件发布版本中的安全漏洞，共8项。新草案将原实践“验证第三方软件是否符合安全要求(PW.3)”合并到了PW.4中；

· **漏洞响应(RV)：**此类实践用来识别软件版本中的剩余漏洞，适当响应以解决它们，并防止未来发生类似漏洞，共3项。

表 1 SSDF V1.1 草案中所有实践和任务

分类	实践	任务
组织准备 (PO)	PO.1：定义软件开发的安全需求	PO.1.1：识别并记录组织的软件开发基础设施和过程的所有安全需求，并随时间维护这些需求
		PO.1.2：识别并记录组织开发的软件满足的所有安全需求，并随着时间的推移维护这些需求
		PO.1.3：与所有将向组织提供商业软件组件的第三方沟通需求，以供组织自己的软件重用
	PO.2：实施角色和职责	PO.2.1：创建新角色，根据需要改变现有角色职责。定期检查已有角色和职责，根据需要更新
		PO.2.2：为安全开发者提供基于角色培训。定期检查熟练程度和岗位培训，按需更新培训内容
		PO.2.3：获取上层管理对安全开发的承诺，并将该承诺传达给所有与 SSDF 相关的角色和职责
	PO.3：实现支持工具链	PO.3.1：指定各工具链须或应包含哪些 (类) 工具，以减少已识别风险，及工具链组件如何集成
		PO.3.2：按照推荐的安全实践部署和维护工具和工具链
		PO.3.3：配置工具以生成支持组织定义的安全软件开发实践的证据和工件
	PO.4：定义和使用软件安全检查标准	PO.4.1：在 SDLC 中定义软件安全检查和跟踪的标准
		PO.4.2：执行过程、机制等，以收集和保护支持标准的必要信息
	PO.5：实施和维护开发的安全环境	**PO.5.1：分离并保护软件开发中涉及的每个环境**
		PO.5.2：保护和加强开发终端，使用基于风险的方法执行与开发相关的任务
保护软件 (PS)	PS.1：使代码免受未授权访问和篡改	PS.1.1：以最小权限原则存储所有形式的代码，包括源代码和可执行代码，只有经过授权的人员、工具、服务等才有必要的访问形式
	PS.2：提供验证软件发布完整性机制	PS.2.1：使软件购买者和使用者能够获得完整性验证信息
	PS.3：对软件的每个版本存档和保护	PS.3.1：为每个软件版本保留安全存档必要文件和其他数据 (如完整性验证信息、来源数据)
		PS.3.2：收集维护共享各软件版本所有组件和依赖项的来源数据 (如软件材料清单 [SBOM] 中)
生产安全性良好的软件 (PW)	PW.1：设计符合安全要求及降低安全风险的软件	PW.1.1：使用风险建模的形式，如威胁建模、攻击建模或攻击面映射，帮助评估软件安全风险
		PW.1.2：记录软件的安全需求、风险和设计决策
		PW.1.3：适当时，构建使用标准化安全特性和服务的支持，而非创建安全特性和服务专有实现
	PW.2：审核软件设计以核实符合安全要求和风险信息	PW.2.1：有资格但未参与设计的人员或自动化、流程实例化的工具链 (或两者结合) 审查软件设计确认和执行，它符合所有的安全需求并很好的定位识别的风险信息
	PW.4：在可行的情况下重用现有的、安全的软件，而不是复制功能	PW.4.1：从商业、开源和其他第三方开发人员获得安全可靠的软件组件，以供组织的软件使用
		PW.4.2：在内部创建维护安全可靠组件，满足第三方组件无法更好满足的常见内部开发需求
		PW.4.4：验证所获得的商业、开源和所有其他第三方组件在其生命周期中符合组织定义的要求
		PW.4.5：在为组织自己的软件重用所有内部和第三方组件之前，验证其完整性并检查其来源
	PW.5：根据安全编码实践创建源代码	PW.5.1：遵循所有适合开发语言和环境的安全编码实践，以满足组织的要求
	PW.6：配置环境、编译、构建过程等	PW.6.1：使用编译器、解释器和构建工具来提高可执行文件的安全性
		PW.6.2：确定应使用的编译器、解释器和构建工具特性及配置方法，实现和使用经批准的配置
	PW.7：检查并分析可读代码，以识别漏洞并验证符合安全需求	PW.7.1：根据组织的定义，确定是否应该使用代码审查或代码分析 (使用工具发现代码中的问题，以完全自动化的方式，或与人工结合的方式)
		PW.7.2：执行基于组织的安全编码标准的代码审查和代码分析，并在开发团队的工作流或问题跟踪系统中记录和分类所有发现的问题和建议的补救措施
	PW.8：测试可执行代码以识别漏洞并验证符合安全需求	PW.8.1：确定进行可执行代码测试否，识别消除之前未覆盖的漏洞类别，如是，确定测试类型
		PW.8.2：设计测试，执行测试，并记录结果，包括记录和分类所有发现的问题，并在开发团队的工作流程或问题跟踪系统中，建议补救措施
	PW.9：开启软件默认安全设置	PW.9.1：定义安全基线，使默认设置是安全的，不会削弱平台、网络设施或服务的安全功能
		PW.9.2：实现默认设置 (或默认设置组，如果适用)，并为软件管理员记录每个设置

漏洞响应(RV)	RV.1：持续的识别和确认漏洞	RV.1.1：收集关于软件和软件使用的第三方组件的潜在漏洞的信息，并调查所有可信的报告
		RV.1.2：检查、分析和测试软件代码，以识别或确认之前未检测到的漏洞
		RV.1.3：制定策略以解决漏洞的公开和修复，并实现支持该策略所需的角色、职责和流程
	RV.2：评估、确定优先级和修复漏洞	RV.2.1：为制定漏洞修复计划而对其进行分析，以收集足够的信息
		RV.2.2：为每个漏洞制定和实施修复计划
	RV.3：分析漏洞以确定其成因	RV.3.1：分析所有已识别的漏洞，确定每个漏洞的成因
		RV.3.2：随着时间的推移，分析根本原因以识别模式，如未遵循特定安全编码实践的情况
		RV.3.3：检查软件中相似漏洞，并主动修复它们，而不是等待外部报告
		RV.3.4：评审 SDLC 过程，适当时更新，缓解漏洞成因在软件更新或新开发软件中重复的可能

分析草案所有实践可知，19 项实践覆盖了软件供应链安全应包含的软件自身及其生产要素的安全内容，整体框架较为全面：

(1) 框架中实践涉及软件开发生命周期的需求、设计、集成第三方软件、编码、构建、测试源代码和可执行码、漏洞修复响应和分析等各个阶段的安全要求。

(2) 框架中实践考虑到了人员、工具链、开发环境、授权访问、完整性、安全配置等软件生产要素方面的安全和防护手段。

3、SSDF 实践细节

SSDF 对每项实践的详细描述包括 4 个方面：

· **实践：**实践的简介、唯一标识符和解释等；

· **任务：**完成实践所需的一个或多个动作。V1.1 草案中共 43 个 (表 1 第三列，其中粗体的为新增任务，斜体的为从 V1.0 的其他实践中调整来的任务)；

· **实现示例：**可用于实现相应实践的工具、过程或其他方法的示例；

· **参考：**对美机构已有标准指南中相关信息的引用。



表 1 中新增和调整的任务主要涉及开发环境安全、记录维护安全需求和风险设计决策、与第三方沟通需求、维护组件和依赖项的来源数据、使用标准化安全特性和服务、验证第三方组件等。这些进一步加强了对第三方元素、开发环境的安全管理和对安全实践的复用。

表 2 以 PW.4 为例，给出了实践的完整描述示例，可看出 SSDF 的编制参考了较为丰富的文献。

4、与行政令要求的对应关系

SSDF V1.1 草案中实践任务与行政令 4(e) 要求的指南应包含的具体内容之间的详细对应关系如表 3 所示。可以看出：

(1) 软件供应链安全保障中，使用自动化工具检查已知和未知漏洞并修复依然是核心工作。它涉及框架中

表 2 实践详细描述示例

实践	任务（见表 1）	实现示例	参考
PW.4：在可行的情况下重用现有的、安全的软件，而不是复制功能。降低开发成本，加速开发，并通过重用已检查过安全状态的软件模块和服务，降低向软件中引入额外漏洞的可能。这对实现安全功能（如加密模块和协议）的软件尤其重要	PW.4.1	· 检查评估第三方组件的预期用途。如将来要以完全不同的方式使用，再次检查评估时需注意新上下文 · 获取每个组件来源信息（如 SBOM、组成分析），并分析该信息，以更好评估组件可能引入的风险 · 建立组织软件资源库，以托管批准和审查的开源组件 · 维护批准的商业软件组件、版本及其来源数据清单 · 指定要开发的软件中必须包含的组件	**BSAFSS:** SM.2; **BSIMM:** SR1.1; **SCTPC:** 维护；**CNCFSSCP:** 确保材料安全－验证；**IDASOAR:** 19; **IEC62443:** SM-9, SM-10; **MSSDL:** 6; **NISTCSF:** ID.SC-2; **SCSIC:** 供应商采购完整性控制；**OWASPASVS:** 1.1.6; **OWASPSAMM:** SA1-A; **OWASPSCVS:** 4; **SP80053:** SA-4, SA-12; **SP800181:** K0039
	PW.4.2	· 创建维护组件时，遵循组织建立的安全软件开发实践 · 为这些组件维护一个组织范围的软件存储库 · 指定要开发的软件中必须包含哪些组件	**BSIMM:** SFD1.1, SFD2.1, SR1.1; **SCTPC:** 维护；**IDASOAR:** 19; **OWASPASVS:** 1.1.6; **SP800181:** SP-DEV-001
	PW.4.4	· 确定软件模块和服务中是否存在供应商尚未修复的已公开漏洞 · 使用商业服务的现有结果来审查软件模块和服务	**BSAFSS:** SC.3-1, TV.2, TV.3; **CNCFSSCP:** 确保材料安全－验证、自动化；**IDASOAR:** 21; **IEC62443:** SI-1, DM-1; **SP800181:** SP-DEV-002; K0153, K0266; **MSSDL:** 7; **NISTCSF:** ID.SC-4; **NISTDVS:** 2.11; **OWASPASVS:** 10, 14.2; **OWASPMASVS:** 7.5; **OWASPSAMM:** TA3-A, SR3-B; **OWASPSCVS:** 4, 5; **PCISSLC:** 3.2, 3.4, 4.1; **SCAGILE:** 需要安全专家帮助的任务 8; **SCFPSSD:** 管理第三方组件使用中固有风险；**SCSIC:** 供应商采购完整性控制，同行评审和安全测试；**SCTPC:** 维护、评估；**SP80053:** SA-9, SA-12, SR-3; **SP800160:** 3.1.2, 3.3.8
	PW.4.5	· 确保每个软件组件仍在维护，并未结束不用；这应该包括正在修改的软件中发现的新漏洞 · 为不再维护或不久后将不用的软件组件确定行动计划 · 通过数字签名或其他机制确认软件组件的完整性	**BSAFSS:** SM.2-1, SM.2-2, SM.2-3; **SCSIC:** 供应商采购完整性控制；**CNCFSSCP:** 确保材料安全－验证、自动化；**IEC62443:** SM-9, SM-10; **NISTCSF:** PR.DS-6; **NISTDVS:** 2.11; **OWASPASVS:** 14.2.4, 14.2.5; **SP80053:** SR-4; **OWASPSCVS:** 4, 6; **SP800181:** S0298

18 项任务，包括定义检查标准、设计、集成、编码、构建、代码审查和漏洞分析、基线配置、漏洞信息收集、修复等各环节、各要素中与漏洞相关的工作。其中 PW.4.4、PW.5.1、PW.7.1、PW.7.2 和 PW.8.2 是检查漏洞的主要任务，多由有经验的安全人员在 SAST、SCA、IAST 等类型工具的辅助下完成。

(2) 实践“复用安全软件 (PW.4)”的任务包括获取或维护安全可靠的内部和第三方组件、验证第三方组件符合组织要求、验证第三方组件的完整性和来源等。这些任务多用于供应链来源、控制和完整性方面安全要求 (3、4、6、10) 的应对方案中。其中，第三方组件的验证可以使用 SCA 工具进行。

(3) 新增“开发的安全环境 (PO.5)”的两项任务可用于行政令多项要求 (1(1)–(6)、2、3、5、6) 的应对方案中。这说明在供应链安全中，软件开发环境已成为重点考虑的因素之一。

表 3 SSDF 任务与行政令要求的对应关系

条款	EO 14028 4(e) 要求指南包含的具体内容	SSDF V1.1 草案任务
1	安全的软件开发环境	
(1)	独立的构建环境	PO.5.1
(2)	审计信任关系	PO.5.1
(3)	企业内建立多因素、基于风险的认证和有条件的访问	PO.5.2
(4)	记录并尽量减少对那些作为开发、构建和编辑软件的环境一部分的企业产品的依赖	PO.5.1
(5)	对数据进行加密	PO.5.2
(6)	监测操作并对企图或实际发生的网络事件做出响应	PO.3.2, PO.3.3, PO.5.1, PO.5.2
2	留存并在购买者要求时提供证明符合条款规定的要求	PO.3.2, PO.3.3, PO.5.1, PO.5.2
3	用自动化工具或相似程序维护可信的源代码供应链	PO.3.1, PO.3.2, PO.5.1, PO.5.2, PS.1.1, PS.2.1, PS.3.1, PW.4.5
4	用自动化工具或相似程序检查已知和潜在漏洞并修复，这些工具或程序应定期运行，或至少在产品、版本或更新发布之前运行	PO.4.1, PO.4.2, PS.1.1, PW.2.1, PW.4.4, PW.5.1, PW.6.1, PW.6.2, PW.7.1, PW.7.2, PW.8.2, PW.9.1, PW.9.2, RV.1.1, RV.1.2, RV.2.1, RV.2.2, RV.3.3
5	购买者要求时提供执行上述两条款的工件，并公开提供这些活动的摘要信息，包括评估和缓解风险的摘要	PO.3.2, PO.3.3, PO.4.1, PO.5.1, PO.5.2, PW.1.2, PW.2.1, PW.7.2, PW.8.2, RV.2.2
6	保持准确最新数据、代码或组件的来源，内部和第三方组件、工具和服务的控制，对控制进行经常审计和执行	PO.1.3, PO.3.2, PO.5.1, PS.3.1, PS.3.2, PW.4.1, PW.4.5, RV.1.2
7	向购买者提供产品 SBOM，或将其公布在网站上	PS.3.2
8	参加漏洞披露计划	RV.1.1, RV.1.2, RV.1.3, RV.2.1, RV.2.2, RV.3.3
9	证明符合安全的软件开发实践	所有实践和任务
10	可行范围内确保证明所用开源软件的完整性和来源	PO.1.3, PS.3.2, PW.4.1, PW.4.4, PW.4.5



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·产业生态

网络安全产业生态平台

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



四大引擎

产服

以产业基地为载体
提供产业生态服务
助力产业发展

产孵

以产业加速器为载体
孵化优质企业
与ToB业务的合作

产投

以产业生态投资
为重要抓手
构建产业生态体系

产研

构建产学研体系
聚焦底层技术创新
全面赋能网安产业

产业生态架构

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



阿帕奇 Log4j2 组件曝出“核弹级”漏洞

12 月 17 日，国家工信部发布公告，通报阿帕奇 Log4j2 组件的重大安全漏洞。工信部在公告中表示，这一漏洞可能导致设备远程受控，进而引发敏感信息窃取、设备服务中断等严重危害，属于高危漏洞。

奇安信公司安全专家研判，这一漏洞影响范围极大，90% 以上基于 Java 开发的应用平台都会受到这一漏洞影响。Log4Shell（Log4j2 组件漏洞名称）的破坏力和 ShellShock、Heartbleed 和 EternalBlue 属同一级别，堪称“核弹级”漏洞。

截至 12 月 13 日，奇安信安服中心收到 10 多起利用该漏洞进行勒索攻击的应急响应需求。奇安信专家预计，由于 Apache Log4j2 漏洞影响面大，利用门槛低，未来几天会有更多的僵尸网络、挖矿病毒、勒索软件等利用此漏洞发起攻击，其危害不容忽视。

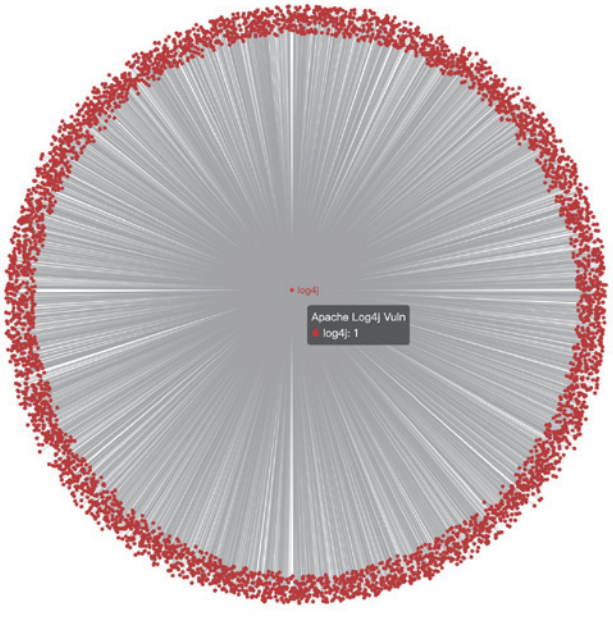
工信部提醒有关单位和公众密切关注阿帕奇 Log4j2 组件漏洞补丁发布，排查自有相关系统阿帕奇 Log4j2 组件使用情况，及时升级组件版本，以降低网络安全风险。

数万组件依赖 Log4j2

Apache Log4j 作为阿帕奇(Apache)的开源项目，是基于 Java 语言的开源日志框架。

Log4j2 是 log4j 的后继者，被大量用于业务系统开发、记录日志信息，广泛应用于 Java、C、C++、.Net、PL/SQL 等程序中。通过各种第三方扩展，可将 Log4j 集成到 J2EE、JINI 及 SNMP 应用中。很多互联网公司及耳熟能详的企业系统都在使用该框架。

奇安信安全专家认为，Log4j 作为日志组件，位于软件供应关系的较底层。供应链对此漏洞的放大效应将逐渐显现，相关厂商、用户需密切关注其威胁发展情况。



奇安信开源卫士评估数万组件依赖于 Log4j2



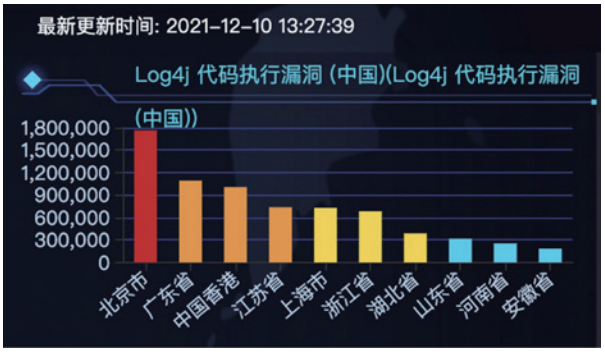
奇安信提供的漏洞在国内的威胁和影响情况

在漏洞威胁方面，根据奇安信网络空间测绘平台（Hunter）截至 2021 年 12 月 10 日的测绘数据，依据排名前十的 Java 组件统计分析，受 Apache Log4j 代码执行漏洞影响的前十大省级单位（含直辖市、自治区、特别行政区）分别为北京市、广东省、香港特别行政区、江苏省、上海市、浙江省、湖北省、山东省、河南省、安徽省。其中，北京市受该漏洞影响最大，暴露在公网上的资产总数为 1,763,977 个，占北京市 Web 资产总数比例大于 10%。

在实际生产环境中，很多系统并未使用 Java，但后台的服务中，大量使用了 ElasticSearch、Kafka、Estorm、Logstash 等 Java 实现的开源组件，也会通过前台的输入产生实际影响，实际影响面远超想象。

如果被攻击，影响的范围堪比 2017 年“永恒之蓝”病毒，致使美国、英国、俄罗斯、中国等至少 150 个国家，30 万名用户中招。

据悉，Log4j2 远程代码执行漏洞已被攻击者利用并公开扩散。截至 12 月 13 日，奇安信应急响应中心已接到十余起重要单位的漏洞应急响应需求。据补天漏洞响应平台负责人介绍，12 月 9 日深夜，仅一个小时内就收到白帽黑客提交的百余条该漏洞的信息。



几乎所有行业都受到波及

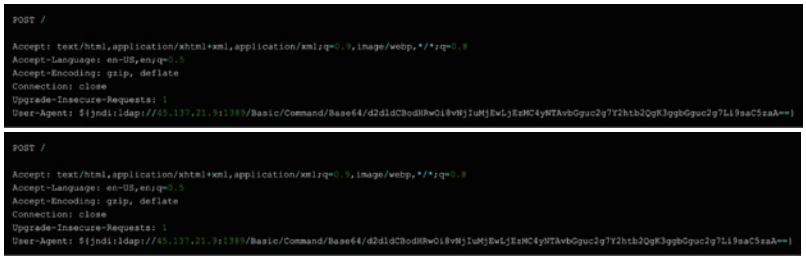


图 Mirai 家族利用 Apache Log4j2 漏洞的攻击流量

根据司南平台监测发现，针对 Apache Log4j2 漏洞，第一次攻击事件高峰出现在 12 月 10 日凌晨 0 点左右，随后在上午 9 点、12 点再次出现两次攻击高峰。其攻击源主要分布在荷兰、中国、

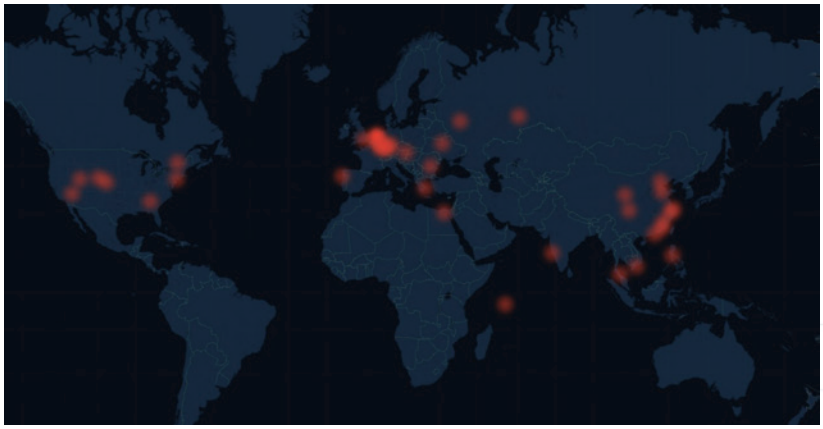


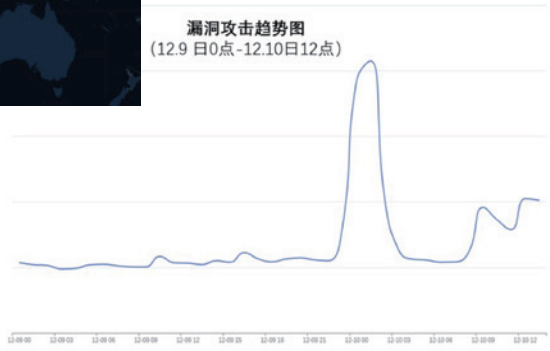
图 全球恶意扫描源分布图

德国、美国、奥地利等国家地区。目前，新西兰计算机紧急响应中心（CERT）、美国国家安全局、德国电信 CERT、中国国家互联网应急中心（CERT/CC）等多国机构相继发出警告。

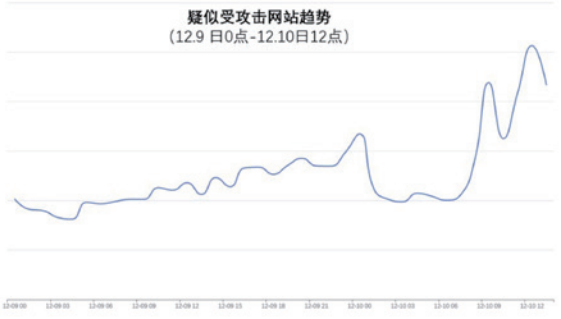
奇安信发现，Log4j2 漏洞已被多个僵尸网络家族利用，12 月 11 日 10 点 25 分，Mirai 家族利用 Apache Log4j2 漏洞进行样本传播。随后，于 10 点 58 分，Muhstik 家族也开始利用此漏洞进行传播。同时，Minerd、LifeCalendarWorm、HSMiner、BigWolf、SnakeMiner、HideShadowMiner、BlueHero 等数十个挖矿病毒家族也在利用该漏洞从事挖矿活动。

截至 12 月 13 日，奇安信安服中心收到 10 多起利用该漏洞进行勒索攻击的应急响应需求。奇安信专家预计，由于 Apache Log4j2 漏洞影响面大，利用门槛低，未来几天会有更多的僵尸网络、挖矿病毒、勒索软件等利用此漏洞发起攻击，其危害不容忽视。

在利用该漏洞的攻击数量方面，根据奇安信司南平台监测数据显示，首次攻击量级波动出现在 12 月 9 日下午 16 点，随后趋于平静。到 10 日凌晨 0 点开始，攻击数量出现大幅度增加，并持续 2 个多小时。 到 10 日上午 9 点和 12 点，攻击数量再次出现两个高峰。



对于疑似受到攻击的网站数量，在 12 月 9 日下午开始增加，凌晨达到一次高峰，10 日早晨 9 点左右，量



级再次激增，10 点达到第二个高峰，12 点达到第三个高峰，也是全天的最高峰。被攻击的网站数量和攻击次数的波峰时间基本吻合。

奇安信司南平台还显示，本次受到攻击行为的客户分布非常广，IT 通信（互联网）、高校、工业制造、金融、政府、医疗卫生、运营商等几乎所有行业都受到波及，全球知名科技公司、电商网站等也未能幸免。其波及面和威胁程度，均堪比 2017 年的“永恒之蓝”。

精准防护漏洞

针对 Log4j2 开源漏洞，首先需要梳理自身产品中所使用的软件资产，检测其中是否使用了开源组件、影响哪些资产、影响程度如何，判断受影响资产应修复到哪个版本，其他关联组件是否受影响，最后着手修复和防御后续类似攻击。用户可通过奇安信开源卫士等工具系统化地应对此类漏洞。

奇安信安全专家建议，广大客户请联系厂商获取修复后的官方版本，或者用以下解决方案来精准防护该漏洞：

◎ **奇安信网站应用安全云防护系统已更新防护特征库**

奇安信网神网站应用安全云防护系统 已全面支持对 Log4j 任意代码执行漏洞的防护。

◎ **奇安信网神智慧防火墙产品防护方案**

奇安信新一代智慧防火墙（NSG3000/5000/7000/9000 系列）和下一代极速防火墙（NSG3500/5500/7500/9500 系列）产品系列，已通过更新 IPS 特征库完成了对该漏洞的防护。建议用户尽快将 IPS 特征库升级至” 2112092130” 及以上版本，并启用规则 ID: 4347001 进行检测。

◎ **奇安信天眼新一代安全感知检测方案**

奇安信天眼通过对攻击手法的多维度分析，基于已有规则，已经可以发现此漏洞，最新版本新增规则可以对该漏洞进行更精准的发现与检测。

◎ **奇安信开源卫士已更新**

奇安信开源卫士 20211209.907 版本已支持对 Log4j 任意代码执行漏洞的检测。

◎ **奇安信网神统一服务器安全管理平台更新入侵防御规则库**

奇安信网神虚拟化安全轻代理版本将于 12 月 10 日发布入侵防御规则库 2021.12.10 版本，支持对 Log4j2 代码执行漏洞的防护，届时请用户联系技术支持人员获取规则升级包对轻代理版本进行升级。

◎ **奇安信椒图服务器安全管理系统防护方案**

方案一： 奇安信椒图服务器安全管理系统可通过 RASP 高级防护功能直接防护该 0day 漏洞，无需更新规则，通过安装 RASP 插件，在 Agent 管理 – 功能设置 – 高级防护功能，进行监控或防护阻断。

方案二：对于无法部署 RASP 插件的用户，同时加入了虚拟补丁防护规则，可通过安装 WAF 插件，在 Agent 管理 – 功能设置 – 虚拟补丁功能，开启监控或者防护模式。

◎ **奇安信天擎终端安全管理系统防护方案**

针对可以连接互联网的终端，将云查模式修改为“直接连接公有云鉴定中心”，即可实现对该漏洞的拦截。对于无法连接公有云的终端，请保持病毒更新最新版本（可将病毒库更新设置为小时级）

◎ **奇安信态势感知与安全运营平台（NGSOC）检测方案**

奇安信 NGSOC 已具备该漏洞的监测能力，规则名为：预置 – 网络探针检测到代码执行事件，所有版本均无需升级规则库即可支持。但需要将 NGSOC 流量传感器的 IPS 规则库升级至 2112100956 或以上版本。

◎ **奇安信天问软件供应链安全分析系统**

奇安信天问软件供应链安全分析系统已全面支持 Apache Log4j 任意代码执行漏洞的检测，用户可以通过将待测的二进制软件上传到天问平台，查看漏洞检测结果，检查是否受漏洞影响。同时，天问平台还提供离线分析工具，可以使用工具离线分析待测软件生成分析日志，然后将分析日志上传到天问平台查询待测软件的检测结果。

此外，补天漏洞响应平台已收到大量关于该漏洞的报告，并开展专项众测活动，让补天平台众多白帽子为客户提供及时专业的安全漏洞检测服务。全球鹰每日进行全网扫描，同步更新测绘数据，并对数据做持续跟踪分析，及时发现存在的漏洞和问题。

软件供应链安全：
开源软件安全再受拷问

安全专家认为，Apache Log4j 漏洞之所以影响范围极大，其核心仍然是开源软件供应链安全问题。由于组件应用范围十分广泛，所有使用该组件的产品都会受到漏洞影响，对其下游造成的软件供应链安全隐患影响巨大，这再次引爆对开源软件安全问题的关注。

实际上，开源安全风险已经成为行业焦点。攻击者越来越多地开始利用开源组件漏洞发动供应链攻击。当前几乎所有的技术巨头都在使用该开源组件，它所带来的危害就像多米诺骨牌一样。安全机构 Sonatype 的报告显示，开源供应链攻击事件比 2020 年增长了 650%。

奇安信安全专家认为，开源软件安全治理是一项任重道远的工作，需要国家、行业、用户、软件厂商都重视并投入进来才能达到良好的效果。

一、开源代码供应量呈指数级增长

Gartner 报告指出，在当前 DevOps 之类的开发模式下，应用程序中大部分代码是被“组装”而不是“开发”出来的。据统计，有超过 95% 的组织在业务关键 IT 系统中都主动或被动地使用了重要的开源软件(OSS) 资产；Forrester Research 研究也表明，应用软件 80% ~ 90% 的代码来自开源组件。2021 年，各地开发者预计从第三方生态系统中借用超过 2.2 万亿个开源包或组件，原因有两个：开源软件开发者的生活更轻松，并加快了创新的步伐。

根据 Sonatype 发布的《2021 年软件供应链状况报告》，2021 年全球开放源代码库供应量继续呈指数级增长，目前，排名前四的开源生态系统总共包含 37,451,682 个组件和包。2020 年共发布了 6,302,733 个新版本的组件 / 包，推出了 723,570 个全新项目，以支持全球 2700 万开发人员。

2021 年 6 月，奇安信代码安全实验室发布的《2021 中国软件供应链安全分析报告》，对 2188 个企业软件

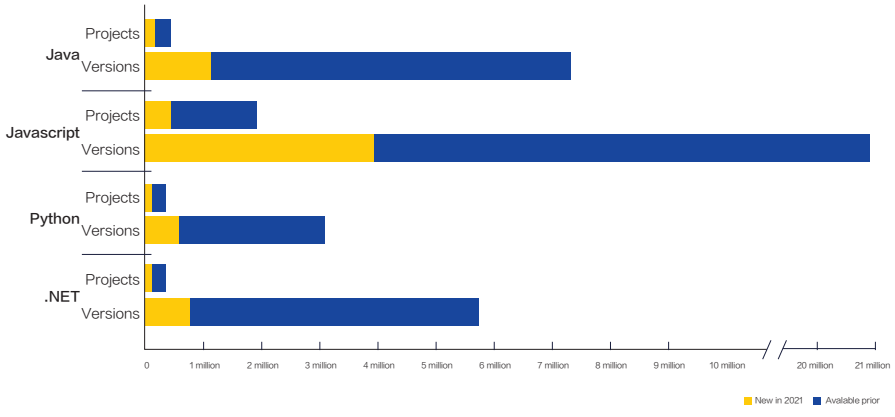


图 2021 开源可用资源

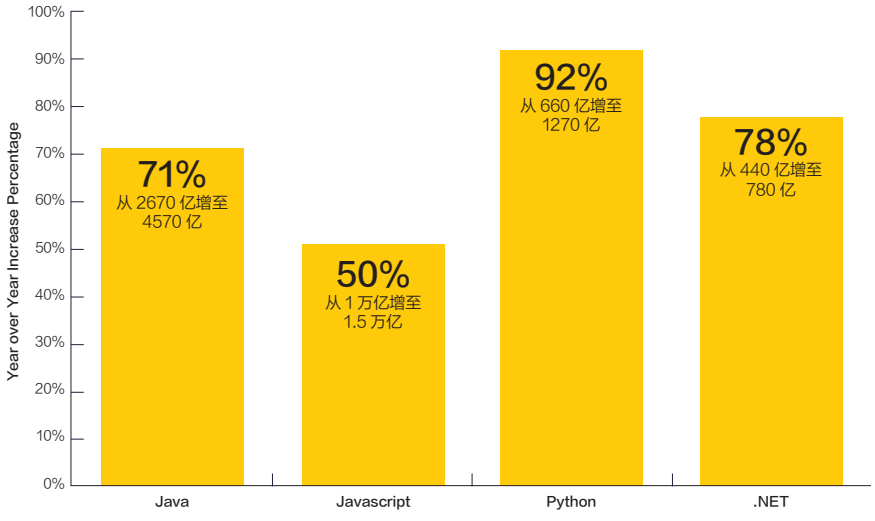


图 2020 年至 2021 年下载量逐年增加

项目的检测结果进行分析。报告显示，所有软件项目均使用了开源软件，平均每个项目使用开源软件数量达 135 个，使用最多的开源软件出现在 581 个项目中，渗透率达到了 26.6%。

2021 年前七个月，Java 从 Maven 中央存储库下载了 2670 亿个 Java 组件。按照这个速度，2021 年 pypistats.org 的第 3 季度预计将超过 4570 亿，同比增长 71%。

JavaScript：2021 年的交易量预计将达到 1.5 万亿，同比增长 50%。

Python：2021 年全年，PyPi 下载量预计为 1270 亿包，同比增长估计为 92%。

.NET ：2021 年，开发者将下载超过 780 亿个软件包，同比增长 78%。

二、开源软件安全存在认识误区

使用开源软件的核心理由之一是开源软件相比于商业闭源软件更安全。这样的结论源自于这样的认知：开源软件具有代码公开、易获取、可重用的特点，比闭源软件能够获得更多的开发者和关注，从而针对所遇见的问题提供相应的解决方案。

开源组件的安全性直接关系到信息系统基础设施的安全，开源安全性不容乐观，它已成为软件供应链安全问题增长的重要因素。

随着开源软件的广泛使用，安全漏洞给开发、安全团队带来严峻的挑战。开源漏洞信息往往散落分布在各大社区，很多漏洞信息不能及时被官方收录。同时，软件使用者缺少漏洞信息跟踪能力，漏洞修复具有滞后性，提升了软件被攻击的风险。

（一）开源软件等于免费软件

开源软件指源代码可以被公众使用的软件，源代码公开是开源软件的主要特点之一。虽然大部分的开源软件可以免费获得，但是开源软件并不是全都免费，仍有大量的开源软件对用户是收费的。

开源软件要求软件发行时附带源代码，但并不意味着它就一定是免费的；同样，免费软件也只是软件免费提供给用户使用，但并不一定是开源的。

（二）开源软件可以随便使用

每一个开源软件都需要包含开源许可证去规定开源软件的使用范围和权利义务，开源软件并非完全没有限制，可以随意使用，其最基本的限制就是开源软件强制任何使用和修改该软件的人承认发起人的著作权和所有参与人的贡献。

开源软件的许可证比较烦杂，经常遇到的开源许可证主要有 GPL 和 BSD 两种。如果不恰当地使用开源软件，未能充分理解和研究许可证规定的权利和义务，往往会埋下知识产权的风险隐患，甚至会被强制要求公开自家产品的私有代码。

（三）开源软件比闭源软件安全

近年来开源软件安全性事件频发，打破了传统观念中的“开源等于安全”的认知。专家认为，开源组件高危漏洞频发、松散的开源社区管理难以有效推动漏洞修复，以及开源代码的漏洞补丁部署状况混乱，是造成开源代码漏洞威胁巨大的三个主要原因。

奇安信代码安全实验室发布的《2021 中国软件供应链安全分析报告》显示，平均每个软件项目存在 52.5 个开源软件漏洞，存在开源软件漏洞、高危开源软件漏洞和超危开源软件漏洞的项目分别为 1695 、1559 、1319 个，占比分别为 77.5%、71.3%、60.3%。影响面最大的开源软件漏洞（Spring FrameWork 漏洞）出现在 973 个项目中，渗透率高达 44.5%，一旦该漏洞被攻击者利用，将影响近半数的企业软件，波及的企业数量更加不计其数。

此外，开源软件的开放、共同参与、自由传播等特性也会带来更多安全风险：一方面，开发者自身安全意识和技术水平不足，易产生安全漏洞，另一方面，无法避免恶意人员向开源软件注入木马程序，进行软件供应链攻击等安全风险行为。

三、开源软件漏洞激增背后

随着开源需求的增加，开源攻击增加了 650%，攻击者不再等待公开的漏洞披露来进行漏洞利用，而是主动将新漏洞注入为全球供应链提供支持的开源项目中，通过将攻击转移到“上游”，可以获得影响力和关键的时间优势，使恶意软件能够在整个供应链中传播，从而对“下游”用户进行更具扩展性的攻击。

由于开源软件使用与获取的便利性，加之部分软件开发人员的安全意识淡薄，可能导致忽略开源软件带来的风险。

总体来看，开源软件存在的安全问题比较严重，安全漏洞是主要的问题，软件供应链攻击呈现上升趋势，同时缺少系统的安全审查机制。

以下三个原因造成开源软件漏洞与攻击激增。

（一）开源项目维护者的安全意识和技术能力参差不齐

Snyk 公司通过扫描数以百万计的 Github 代码库和程序包，对超过 500 个开源项目的维护者进行调查发现：只有 8% 的开源项目维护者自认为有较高的信息安全技术，接近半数的开源项目维护者从来不审计代码，只有 11% 的维护者能做到每季度审核代码。另据 Linux 基金会发布的《开源软件供应链安全报告》显示，大量开发人员在开发软件时并未遵守应用程序安全最佳实践。开源项目维护者对代码安全质量重视不够和技术能力水平不足，是当前造成开源软件安全漏洞的主要原因。

奇安信代码安全实验室发起的“开源项目检测计划”，通过对 3000 余款使用比较广泛的开源项目进行检测，发现所有检测项目的总体平均缺陷密度为 14.22/KLOC，高危缺陷密度为 0.72/KLOC。路径遍历、空指针相关、密码管理、跨站脚本 XSS、注入类缺陷、XML 外部实体注入、缓冲区溢出、资源管理、HTTP 响应截断、日志伪造等是开源软件主要的安全风险。

2019 年，Unit42 安全团队分析了 24,000 多个公开的 GitHub 开源项目，共识别出 2328 个硬编码密码，2464 个 API 密钥和 1998 个 OAuth 令牌。对于关系社会安全稳定的企业单位，如银行等金融机构，信息系统中如果采用了上述的开源组件将会对社会经济安全造成恶劣的影响。

在密钥管理中最常见的错误，就是将密钥硬编码在代码里。一旦攻击者获得密钥，再通过审计分析支付系统的加密算法，就可以破译所有的加密数据。

（二）越来越多的黑客组织开始盯上开源软件

在软件生产过程中，代码复用程度越来越高，各种开发包、核心库的应用越来越广泛。很多黑客组织也意识到了这一点，逐渐把目光放在了开源软件上，利用开源代码植入后门。这些代码的复用度越高，后门影响范围就越广，从而实现对软件供应链上游的攻击。

2019 年 8 月，Webmin 被曝存在高风险远程命令执行漏洞，根据 Webmin 开发人员的说法，该漏洞不是编码错误的结果，而是“恶意代码注入受损的构建基础架构中”导致的。Webmin 是一个用于管理 Linux 和 UNIX 系统的基于 Web 的开源软件，互联网上大约有 13 万台机器使用 Webmin。根据 Shodan 搜索引擎收集到的统计数据显示，有近 10 万台服务器曾运行过存在“后门代码”版本的 Webmin 软件，对整个互联网安全造成了巨大的影响。

（三）开源软件缺少系统的代码安全审查机制

美国是最先认识到开源软件安全问题的重要性的，早在 2006 年美国国土安全部就开展过“开源软件代码测试计划”，对大量开源软件进行安全隐患的筛选和加固。

根据 Snyk 公司的报告显示，37% 的开源开发者在持续集成（CI ）期间没有实施任何类型的安全测试，54 % 的开发者没有对 Docker 镜像进行任何的安全测试。

开源代码中不断发现新的安全漏洞，而很多项目没有查找并修复漏洞的响应机制。开源项目的安全记录方式也没有明确的标准可以遵循，GitHub 上排名前 40 万的公共代码库中，仅 2.4% 的项目有安全文档。

开源软件在实际的流通过程中，各个环节间缺乏系统的安全审查机制，部分企业内部也缺少必要的安全检测要求和规范，导致一旦底层开源组件出现安全漏洞，这些问题组件将传染给哪些商业产品、影响哪些业务领域，没人能给出一个准确的答案。

四、全方位应对开源软件安全风险

从全行业来看，我们需要在国家、企业、用户、检测机构等 4 个层面着手，体系化应对开源软件的安全风险。

（一）国家层面组织开展开源软件源代码检测工程

随着开源趋势的不可逆，以及开源软件在商业软件中的占比越来越高，开源软件俨然已经成为软件开发的关键基础设施，因此开源软件的安全问题应该上升到国家安全的角度来对待。

建议国家相关部门组织有业务基础的科研机构开展开源软件源代码检测工程，并将检测的成果以一种安全可控的方式向商业软件制造商及关键岗位的企业共享，尽可能降低开源软件漏洞对社会各行各业的影响。

（二）企业层面建设开源软件安全治理体系

企业应建立开源软件安全治理体系，明确开源软件使用的安全准入条件，从软件开发阶段就建立开源软件使用的统一策略，实现开源软件引入和使用的标准化、规范化和合规化。

对于明确需要引入的开源软件，在加强版本控制的基础上，一方面，开展安全风险评估检测；另一方面，持续跟踪相关的漏洞情报，时刻提防软件供应链攻击。

（三）用户侧建立软件安全渗透测试机制

从已经发生的软件供应链攻击案例来看，非常有必要开展软件上线前的渗透检测。通过采用良性的攻防渗透的方法、思路和手段，及时发现软件系统中存在的安全漏洞和隐患，降低新软件上线给系统带来的风险。

企业在开展软件采购时，应向供应商明确要求提供软件中包含的开源组件，“用了什么，什么版本，软件来源”，并在验收时进行细致核查。

（四）检测机构加强对安全产品中开源组件的检测

信息安全产品是重要信息系统安全防护的重要组成部分，其自身的安全性将影响重要信息系统的安全。检测机构应要求软件供应商准确提供产品中包含的开源组件等信息，并针对开源组件开展专门的安全检测。这样，一旦某个开源软件被曝出重大的安全漏洞，产品检测机构可以及时迅速地发布安全预警，并要求相关产品厂商尽快开展修复，甚至对修补不力的产品予以禁用处置。

华云信安·产业教育中心

网安人才培养新模式
打造产业人才成长圈

产教融合

INTEGRATION OF PRODUCTION AND EDUCATION

- 共建产业学院
- 共建合作专业
- 共建联合实验室
- 共建人才/师资培养基地
- 1+X证书合作
- 教育部协同育人项目合作

雷锋网

BCS 2021 技术峰会：攻与防的角力 经营安全推动网络安全技术变革

作为 BCS 2021 三大峰会（战略峰会、产业峰会、技术峰会）中的压轴峰会，技术峰会吸引了全球网络安全技术爱好者的热切关注。在今年峰会上，Forrester 副总裁、集团研究总监 Laura Koetzle（劳拉·科茨勒），北京赛博英杰科技有限公司董事长谭晓生，Kryptos Logic 高级威胁情报分析师与恶意软件研究员，WannaCry 破解者 Marcus Hutchins（马库斯·哈钦斯），复旦大学计算机科学技术学院副院长杨珉，美国俄克拉荷马大学助理副校长、讲席教授 David S. Ebert（大卫·伊尔伯特），北京大学大数据分析与应用技术国家工程实验室常务副主任袁晓如，蚂蚁集团副总裁韦韬，清华大学－奇安信集团联合研究中心主任段海新等发表了主题演讲。安全牛总编辑、国际信息系统审计协会（ISACA）中国专家委员会副主席陈伟作为主持人出席了技术峰会。

勒索病毒、供应链攻击，威胁侧的变化莫测

2021 年似乎一开始就是不平静的一年，在全球网络安全领域也充满了变化和挑战。从去年年底 SolarWinds 供应链攻击事件开始，有两个关键词一直充斥着人们的眼球，一个是供应链攻击，另一个是勒索攻击。值得关注的是，奇安信威胁情报中心已监测到多起安全公司被入侵造成的供应链攻击事件。

甚至，这二者开始出现了结合。今年 7 月 2 日，企



Forrester 副总裁、集团研究总监 Laura Koetzle（劳拉·科茨勒）

业管理软件供应商 Kaseya 被曝出旗下产品 KASEYA VSA 软件存在漏洞，已被 REvil 黑客勒索组织利用攻击，并造成其大量客户因此关闭服务。

“他们并不在乎黑进了哪家公司，他们只在乎能够花费最少的代价获取最多的收益。” 劳拉 · 科茨勒在演讲中一语道出了供应链攻击流行的原因，由于攻击目标往往处于供应链的上游，因此通常具备“攻其一点，伤及一片”的特点，尤其是攻击那些使用较为广泛的软 / 硬件产品。

劳拉 · 科茨勒说，SolarWinds 事件告诉我们，不要觉得供应链攻击离你很远，即便你不知名，但如果你有很多知名的客户，你依然具备极高的攻击价值。并且，攻击者为了达成攻击目标，通常会在目标中潜伏很长时间，从而植入恶意代码。为了应对这种攻击方式，组织机构应该尝试使用零信任架构，用于将每一次访问的安全风险降至最低，同时应当建立软件资产清单，便于清晰掌握软件供应链所面临的风险，即便发生攻击，也能在最短的时间内做出正确的响应。

但遗憾的是，大多数组织机构并没有明确掌握他们所使用的软件面临的风险，尤其是在引入开源软件的时候。由于开源软件使用的广泛性，给了大量攻击者以可乘之机。

根据奇安信发布的《2021 中国软件供应链安全分析报告》显示，在奇安信代码安全实验室分析的 2557 个国内企业软件项目中，平均每个软件项目存在 66 个已知开源软件漏洞，最多的软件项目存在 1200 个已知开源软件漏洞。其中，存在已知开源软件漏洞的项目占比高达 89.2%；存在已知高危开源软件漏洞的项目占比为 80.6%；存在已知超危开源软件漏洞的项目占比为 70.5%。

“多项开源组件受到高危漏洞影响、松散的开源社区管理难以有效推动漏洞修复，以及开源代码的漏洞补丁部署状况混乱，是造成开源代码面临的漏洞威胁巨大三个主要原因。”杨珉解释到，“面对这些不足，我们希望通过挖掘开源组件漏洞、增强开源漏洞信息，以及评估漏洞补丁状态等方面的工作去解决，尽管在这个过程中我们遇到了漏洞挖掘效率低、漏洞库信息不完整、补丁部署管理混乱等方面的困难。”

当然，饱受漏洞问题困扰的绝非只有普通的开源软件或者其他商业软件，互联网核心协议的漏洞问题同样不可小觑，由于使用更为广泛，其危害性甚至更加巨大，2014 年曝出的 OpenSSL 心脏滴血漏洞仿佛就在昨日。

“互联网基础协议的小问题常是互联网的大问题。”清华大学 – 奇安信集团联合研究中心主任段海新强调，



清华大学 – 奇安信集团联合研究中心主任段海新

作为互联网基础协议领域的安全专家，段海新又一次在技术峰会上，分享了他在该领域的最新研究成果。他说：“经过长期的研究和攻防实践，我们发现了互联网基础协议漏洞的一些显著特征，基础协议的漏洞影响范围很广，但想要运用自动化的方法来挖掘或者寻找漏洞却十分困难。并且，这些互联网协议漏洞绝大多数都是逻辑漏洞，甚至许多漏洞是多个系统组合在一起才出现的，需要多个系统组合在一起才能发现。”

与此同时，作为近年来威胁侧的另外一个“明星”，勒索病毒也一直保持着很高的活跃度，甚至是触发企业应急响应流程的最主要威胁。“勒索软件通常不再侵扰消费者系统，而是企图感染整个企业网络。”马库斯·哈钦斯介绍了近年来勒索病毒攻击的变化趋势。这主要是因为感染一家企业，要比同时感染数十万台设备要容易得多，并且相对个人消费者而言，企业支付赎金的意愿更强。马库斯·哈钦斯强调，勒索病毒的防范不仅仅是一个技术问题，仅靠提高安全性、增加安全预算是无法解决的，需要在金融、法律及网络安全等领域开展多方合作。



Kryptos Logic 高级威胁情报分析师与恶意软件研究员、WannaCry 破解者 Marcus Hutchins(马库斯·哈钦斯)

AI 可视化与平行切面，防护侧的技术变革

魔高一尺，道高一丈。奇安信集团董事长齐向东在 26 日战略峰会上谈到，只有煞费苦心地经营安全系统，才能保障经营活动安全运转。经营安全是对网络安全的动态掌控，只有让安全能力动起来，不断循环升级，才能破解复杂难题。

对于网络安全技术的发展趋势，谭晓生针对端点安全、网络安全、应用安全等网络安全所有技术领域，展开了非常深入细致的分析。从防火墙到下一代防火墙、从 IPDS 到 NTA 和 NDR、从 SD-WAN 再到 SASE，以及安全管理和安全服务，推动了整个网络安全防护水平向前发展。

在所有用于网络安全的技术中，机器学习、可视化与平行切面等技术的应用，逐渐走进了大众的视野。

大卫·伊尔伯特表示，尽管深度学习已经在很多领域取得了成功，但它不是万能的灵丹妙药，目前也还没能最大化发挥它的价值，因此很多人都认为深度学习远



北京赛博英杰科技有限公司董事长谭晓生

比现在大有可为。他说，人们需要创造可视分析、可视化和人机协同决策环境，来帮助大众充分利用现有的所有数据源，并且把垂直领域的知识整合到可视分析系统中，改进分析流程，并且基于数据和先进分析，做出更高效的决策。

袁晓如也表达了这样的观点。他认为，智能新时代的可视分析是沟通数据、人与社会的桥梁。虽然机器初步具有分析、预测能力，但人类在复杂事物认知、常



北京大学大数据分析与应用技术国家工程实验室常务副主任袁晓如

识和创意的能力机器不能匹敌。他通过情报文本报告、舆情传播以及与奇安信团队合作的媒体新闻转载分析等可视化案例，指出通过设计有针对性的可视化界面，把人和机器结合起来，可以大大提高人类的知识认知能力。安全领域面临复杂的博弈，可视分析可以更好地帮助决策者理解复杂的数据场景，作出相应的对策。大数据、人工智能和计算能力是计算机科学拉动社会前进的三架马车，可视化可以帮助人类更好地驾驭计算和数据。

同样是与数据打交道，数据治理在拥有海量数据的今天显得更加重要。随着网络安全与数据安全逐渐深入到业务本身，数据安全治理与日常业务的开展经常会出现冲突。如果有一个平行空间，能够让业务部署维度与安全部署维度做到正交融合——两者既能融合为一体，又能独立解耦，各自独立发展，对于安全行业的发展来说将会是一个重要变革。

“安全平行切面体系（安全切面）是一个安全基础设施，通过嵌入在端管云内部的各层次切点使得安全管控与业务逻辑解耦，并通过标准化的接口为安全业务提供内视和干预能力。”韦韬给出了安全切面的概念。能够预见的是，在数据爆炸的 DT 时代，安全平行切面体系的引入，能够有效地推动数据感知覆盖、数据链路血缘高精度分析上产生新的突破，以解决数据治理面临的精确度、覆盖度、保鲜度等深水区的严峻挑战，并且在 App 隐私管控、数据分类分级、数据主体确权，以及数据输出防泄露等数据治理关键工作中起到重要作用。



蚂蚁集团副总裁韦韬

奇安信椒图：我赌你的服务器里没有恶意文件

1876 年，时年 33 岁的德国农业化学家麦尔，发现了一个很严重的问题。

很多种植烟草的农民都遇到了一个困惑：烟草长出的深绿叶子上会莫名其妙地出现浅绿色斑纹，致使烟叶的产量和质量都受到严重的影响。

为探明该烟草疾病的产生原因，麦尔自 1879 年开始对烟草的种植展开了长时间的观察与实验研究，并于 1882 年将这种烟草疾病命名为“烟草花叶病”。

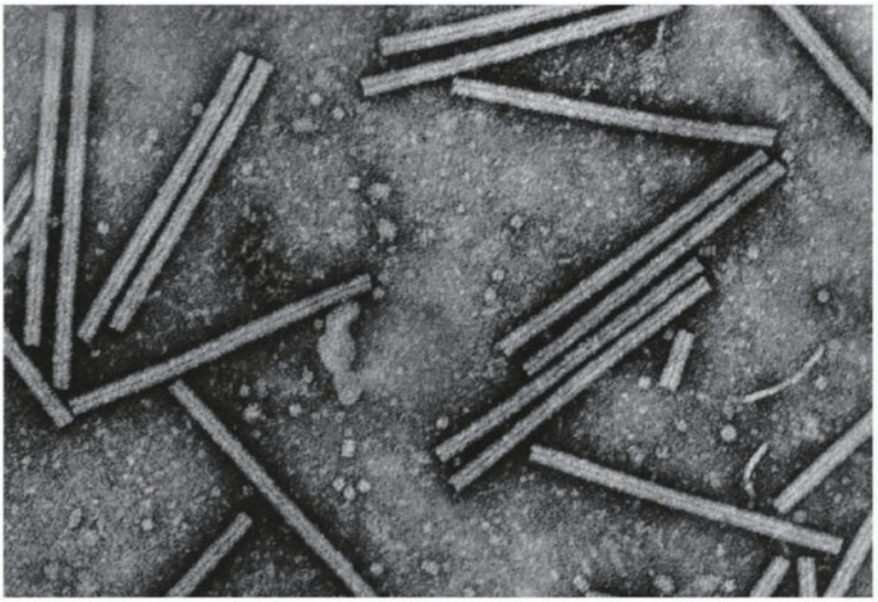
尽管麦尔仔细研究了气温、光照、土壤及细菌、真菌等病原体的影响，但始终没有找到“烟草花叶病”的真正病因，无奈的他只好将其归咎于某种尚未发现的细菌上。

直到 1892 年，“烟草花叶病 " 的研究取得了突破性的进展。一位名叫伊万诺夫斯基的俄国植物生理学家发现，有病的烟叶汁即使用过滤器过滤后，擦在无病的烟叶上仍能使好叶子生病。他由此推断：一定有一种更小的，能通过细菌过滤器的微生物存在。

毋庸置疑的是，伊万诺夫斯基的研究成果，打开了人类研究病毒世界的大门。伴随着 1939 年第一台商用电子显微镜的问世，科学家终于观察到了这个直径约为 15



纳米、长度约为 300 纳米的杆状病毒。



图：电子显微镜下的烟草花叶病毒

拉手风琴

病毒的发现改变了人们对于微生物的认知：病毒体积微小、结构简单，甚至没有完整的细胞结构，仅仅是一个蛋白质外壳包裹着核酸链。不同于寄生类细菌，病毒必须将遗传物质注入到宿主细胞内，依靠宿主细胞的物质和能量，才能完成自我复制和增殖。

可怕的是，这种导致人类近 80% 传染病的东西，令当时所有外界的检测和防护手段近乎失灵，人们只能寄希望于强大的免疫系统。

病毒实在是太小了，小到最小的病毒直径还不到 10 纳米，细菌过滤器根本无法对其实施有效拦截，即便是最先进的光学显微镜也无法观测到；曾经拯救千万士兵生命的抗生素，在面对这类非细胞生物时，也发挥不出任何作用。即便是在医学已经相对发达的今天，人类唯一战胜的病毒也仅只有天花一种（下一个有希望的是脊髓灰质炎）。

很快，病毒出现了另外一层含义：1987 年，一对来自巴基斯坦的兄弟发明了另一种“病毒”，它的感染目标并不是细胞生物，而是计算机系统，能够耗尽计算机的存储空间。

计算机病毒就此诞生，并很快成为危害计算机安全的头号杀手，在网络空间大肆传播。它和普通的细菌、病毒等寄生生物一样，具有传播、复制和破坏宿主正常功能的能力。

最开始的计算机病毒拥有完整的文件结构，没事的时候就独立存储在硬盘里，执行的时候再写入内存，释放恶意代码。

这时候的计算机病毒更像是细菌，有着完整的细胞结构，可以独立寄生在表皮黏膜、肠道、血管等位置，当然某些细菌也可以寄生在细胞内部。

为了阻止计算机病毒的传播，人们发明了反病毒软件，它工作在计算机终端或服务器终端上，能够扫描所有磁盘空间，把那些病毒文件找出来。

同样，为了对抗反病毒软件的检测，计算机病毒也在不断“变异”，产生对杀毒软件的“耐药性”，让你检测不到、删除不了，甚至可以反过来把杀毒软件卸载掉。不得已之下，人们只好不断提升反病毒引擎的检测能力……

这个过程是不是似曾相识？人们从青霉菌的分泌物中提取出了盘尼西林，成为了第一种能够治疗细菌感染的特效药，从而拯救了成千上万的生命；抗生素的广泛使用，使得细菌耐药性不断提升，尤其是超级细菌的出现，让大家意识到了抗生素滥用的巨大危害；为了对抗细菌

的抗药性，人们又不得不研发新的抗生素。

用麦克阿瑟送给李奇微的一句话来说，这场拉手风琴式的战争永远都不会结束。

猝不及防

说实话，李奇微针对志愿军后勤特点制定的这种“磁性战术”非常有效。但正如麦克阿瑟所说，靠这种手风琴式的打法，“联合国军”想要快速结束战争的愿望却很难实现。

所以，麦克阿瑟想要实施第二次仁川登陆，幻想一举击溃志愿军和朝鲜人民军（未能如愿，麦克阿瑟也因为狂妄而被撤销一切职务，有兴趣可以查看抗美援朝第五次战役）。

那么有没有一种“病毒”，能够一劳永逸摆脱反病毒软件的检测呢?

来做一下类比。抗生素的杀菌机制总共有四种，包括抑制细菌细胞壁的合成、改变细胞膜的渗透性、干扰蛋白质的合成及抑制核酸的复制和转录。但无论哪种杀菌机制，它的作用对象都是拥有完整细胞结构的细菌，而不会对非细胞生物起任何作用。

同理，传统的反病毒软件检测的对象是存储在磁盘中的文件，那是不是有病毒可以不把文件留在磁盘中，从而一劳永逸摆脱反病毒软件的检测了呢?

这个还真有。

2012 年，卡巴斯基在一份安全报告中，提到了一个新型木马：Lurk 木马非常独特，它不会存储在受害者的计算机硬盘中，而是利用漏洞把恶意代码写入 javaw.exe 进程的内存中执行。

这就是无文件恶意软件的样子。下面举个形象的例子来区分有文件攻击和无文件攻击。

通常情况下，你要想刺探敌方情报，就得派遣特工化妆渗透，但特工无论再怎么乔装打扮，他还是你们这边派过去的；但现在不一样了，你可以趁对方的人不注意的时候，往他身上装一个窃听器或者微型摄像头，这样无论怎么查，他都是对面自己人。

可以这么说，无文件恶意软件的出现让当时所有的反病毒软件猝不及防，依靠病毒文件签名进行特征匹配的方法肯定不行。

而根据谷歌的一项数据统计显示，大概是在 2014 年开始，无文件恶意软件开始逐渐活跃在搜索引擎中，成为受人们关注的安全话题之一。

可以这么说，无文件恶意软件才开始真正的像微生物病毒一样，没有完整的细胞结构，在入侵的时候会将遗（恶）传（意）物（代）质（码）注入到宿主细胞中，甚至逆转录病毒会将自己的基因整合到宿主细胞的 DNA 上，完成自身的复制和增殖，最终裂解宿主细胞后再横向感染其他目标。

核酸检测

时至今日，人们对于病毒的检测已经有了比较科学的方法，比如，大家所熟知的新冠肺炎病毒核酸检测，无论是咽拭子还是肛拭子，都能够有效采集并检测到病毒核酸。

同理，无论无文件攻击再怎么花里胡哨，只需要检测到恶意代码它就再也无路可逃。

所不同的是，计算机并不会新陈代谢，无文件恶意软件也只会写在内存里，感染合法进程，而不会跑到其他地方。想要检测到恶意代码，只能在内存里做文章。

众所周知，不管是捅喉咙还是捅鼻子，新冠肺炎病毒核酸检测有一个必不可少的工具——棉签，用于采集样本。如果这个“棉签”放在计算机系统里，就被称作“HOOK”，中文翻译为钩子。

椒图就是用这个“钩子”把恶意代码钩出来。

椒图是奇安信集团旗下的服务器安全软件，能够从事前的服务器加固、事中的检测与响应、事后的溯源分析等维度，实现服务器安全的闭环。（详细介绍可以参考《服务器保卫战：它在网络空间里坚守最后一道防线》）

为了实现对无文件恶意软件的精准检测，椒图内置了一款强大的无文件攻击检测引擎。

该引擎总共包含了三个模块。

第一，INJECT 注入模块负责把 HOOK 模块第一时间加载到新建进程内。这个过程就如同护士把棉签放到你的咽部。

第二，HOOK 钩子模块是整个无文件检测引擎的核心，负责修改进程内的指令，用于在命令执行之前，拿到需要关心的函数调用参数或者 Com 方法中的参数。HOOK 函数可以理解为一段消息处理的程序，每当消息发出，在没有到达目的窗口前，HOOK 函数就先捕获该消息，即钩子函数先得到控制权。

这里再科普一下。程序猿朋友都知道，每一个应用程序都包含大量的变量和函数。在数学中，函数可以把各种不同类型的变量，按照一定的计算关系组合起来，如二次函数、三角函数等。这里也一样，函数可以把变量组合起来，执行既定的操作或命令。钩子钩住了关键参数，接下来就能够判断程序到底会执行什么样的操作，这个操作是不是恶意的。

这个过程就如同护士拿着棉签对你的咽部一顿操作，采集关键样本。

第三，CHECK 检查模块会将钩子捕捉到的关键参数进行检查，判断是否为恶意。这个模块内置了大量的业务逻辑规则，用于和钩住的参数进行匹配，如脚本特征匹配、拦截逻辑判断、白名单放行逻辑、写入事件、写入日志等操作。如果发现有什么不对的地方，就可以产生告警。

这个过程就相当于护士将采集到的咽拭子或肛拭子样本，送到检测中心去检测。

这三个模块赋予了椒图基于内存指令集的检测能力，说直白点就是深入到内存里面，检测恶意代码到底感染了哪些进程，从而摆脱了对具体文件特征和漏洞防护规则的依赖，对各种类型的无文件恶意软件和 0day 漏洞利用行为，都有较高的检出率。

除了无文件攻击检测引擎，椒图还有一些功能模块也能够检出部分类型的无文件攻击。

椒图在新版本中引入了全新的龙息 Webshell（一种网页后门，常用于远程控制 Web 服务器）检测引擎，它工作于 Web 中间件内部，对于内存马（常通过 Apache 等 Web 中间件漏洞写入内存的无文件 Webshell）就有很好的检测效果。

基因突变

我们应当注意到，病毒是非常容易发生变异的。由于缺乏细胞结构的保护，病毒的核酸链非常容易在复制的过程中发生改变。

这就是大家口中的基因突变。

同理，对于较为稳定的有文件结构，无文件恶意软件也很容易产生新的“变种”，尤其是在椒图等能够防御无文件攻击的产品问世之后，新变种产生的速度更快。并且，新的变种无论是在隐蔽性还是在功能性、传播性等方面，往往都会大大增强。

从理论上说，这种基于内存指令集的检测能力，肯定能够发现内存中的恶意代码。因为无论它再怎么变异，也逃脱不了计算机的设计逻辑，总归会进入到内存中运行起来，从而在内存中留下“浓墨重彩的一笔”。就像普通新冠毒株也好，德尔塔毒株也罢，总之是逃脱不了白衣天使的棉签。

但说句实在话，把宝全部压在机器的自动化检测上，并不是一个非常明智的做法。况且，针对无文件攻击的检测和处置，绝对是一个技巧性很强的工作。

所以在公司的一手安排下，椒图和安服团队完成了深度整合。基于“人 + 机器”的模式，在数千场攻防演习的过程中，积累了海量的恶意样本特征库、攻击工具特征库，以及实战化基线检查模板，这些数据的加持将产品的实战化能力大幅度提升，能更好地满足服务器的攻防需求。

继天眼（奇安信旗下针对网络流量的高级威胁检测产品）之后，椒图也将被打造为服务器上一款实战攻防的必需品。

不过，无文件攻击尚未成为攻击服务器的最主要方式。但在将来的某一天有人和你打赌，就赌你中招的服务器上没有恶意软件，你就得掂量掂量再下注了。

“浙江全域数字法院”加速跑
网络安全如何实现体系化防御？

司法是维护社会公平正义的最后一道防线，而网络安全无疑是数字化社会的防线和底线。

人民法院，代表国家独立行使审判权的国家审判机构，肩负着司法正义的光荣使命。在人们的印象中，到法院“打官司”是一件程序烦琐的事情。然而在浙江省，依托数字化改革的推动和“智慧法院”建设，法官、原告、被告三方可以在线上，相隔千里之遥，只要有部手机，就能把官司打了，极大地提升了效率，无需往返奔波。

这一切，要归功于浙江省政府数字化改革的成效。群众和企业到政府办事，“最多跑一次”是浙江省数字化建设的目标。尤其在数字司法方面，2020 年浙江全省法院无纸化办案率达到 98%。2020 年最高法院发布的《智慧法院建设评价报告（2019 年）》显示，浙江法院智慧法院建设综合指数为 97.24，居全国第一。

优异成绩的背后，是浙江省政法体系在数字化改革和网络安全建设的不断探索和突破。2021 年开始，浙江省高院印发《关于推进建设“浙江全域数字法院”重大改革的实施方案》（简称《方案》），进一步推动浙江全省法院进入数字化、智能化升级的快车道。

“浙江全域数字法院”加速跑 安全红线不可或缺

“‘浙江全域数字法院’不是一个信息化项目，也不是一家实体法院，而是整个法院审判执行、办案办公等各项工作全面、彻底的数字化，并在此基础上展开业务流程再造、诉讼制度创新，以及法院组织架构、管理模式的彻底重塑，进而打造全业务平台通办、全时空泛在服务、全流程智能辅助、全省域资源整合、全方位制度变革的现代化法院。”在今年 7 月浙江省高院召开的全域数字法院改革推进会上，浙江省高院党组书记、院长李占国对进一步深化全域数字法院改革，赋予了极高的定位和期望。

“浙江省是数字经济的大省，省政府在数字化转型方面更是走在全国前列，这给政法系统数字化改革提供了良好的条件。”浙江省高院副院长朱新力表示，为响应“十四五”规划和 2035 年纲要中“加快数字化发展，建设数字中国”的号召，深入贯彻省委数字化改革决策部署，浙江省高院从 2021 年开始，积极推进建设“浙江全域数字法院”重大改革，实现互联网法院新模式从“风景”到“全景”的转变。

全域数字法院是浙江法院的数字化改革的重要工程，具有“全域化、一体化、智能化、制度变革”四大特征。而网络安全无疑是保障全域数字法院建设的重要基石。朱新力副院长强调，“推进数字法院建设是一项系统性、全局性、引领性的改革工程，各法院要加强组织领导，大力推进落实，强化安全保障。”

勒索攻击肆虐 对全域数字法院构成严重威胁

“在数字化改革的过程中，由于信息架构更加复杂，数据量更加庞大，各种安全威胁也层出不穷，给全域数字法院带来严峻挑战。” 浙江省高院大数据处长李国毫表示。

李国毫回忆道，2017 年肆虐全球的勒索病毒，几乎波及所有信息化行业，法院也无法幸免；2018 年 8 月，多地法院感染“勒索病毒”；中国裁判文书网遭受过数以亿计的网络攻击，利用“爬虫技术”抓取裁判文书信息的情况也令人触目惊心。

李国毫分享了一个故事：2018 年，某省法院专网中

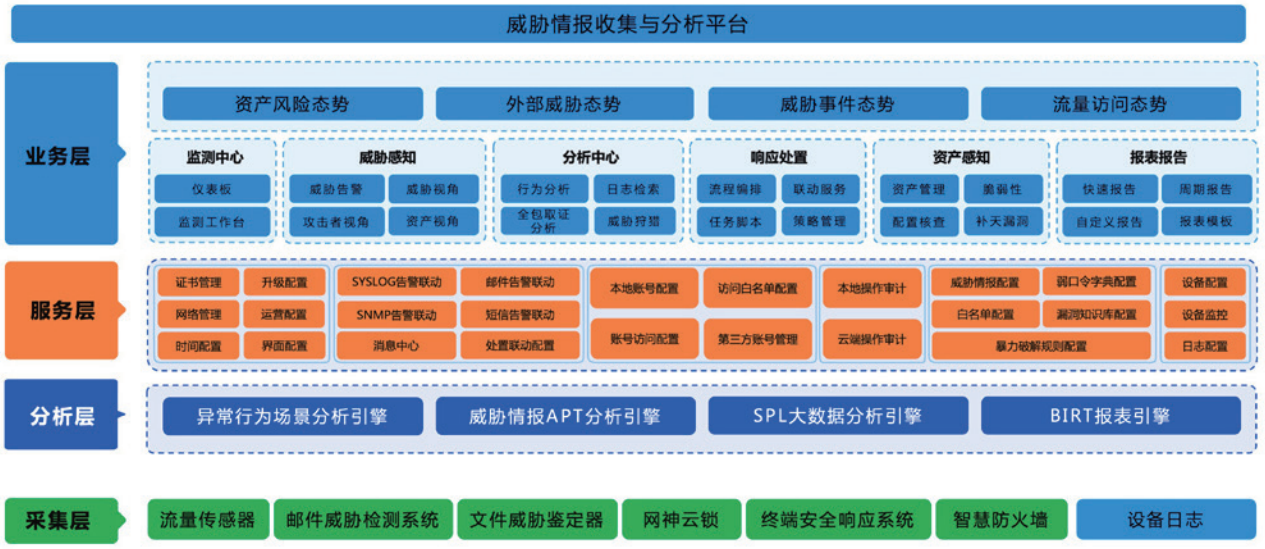


图 1：浙江高级法院威胁情报收集与分析平台能力框架

大量服务器被加密，通过安全专家的分析，判断该勒索攻击的样本为某勒索病毒变种。其攻击原理，就是黑客通过人工 RDP 爆破法院暴露在互联网的服务器密码，并使用黑客工具抓取其他服务器密码，当成功入侵服务器后，通过黑客工具结束杀毒软件进程，并使用扫描工具继续进行渗透，从而实现横纵向扩散，进而投递攻击载荷（勒索软件），达到加密文件、实施勒索的目标。

“对于法院系统而言，文件加密、数据不可用的危害可以说是不可承受的，不仅会造成直接经济损失，而且会导致业务停摆，严重影响司法业务乃至政府形象。”攻击事件频发，让浙江省高院提升了网络安全意识，并加快对法院专网的深度自查。

经过分析，浙江省高院发现全省法院专网几方面的安全需求比较迫切：首先是各地法院的网络安全水平希望整体提升，补齐安全短板；其次是针对多平台数据的汇聚和统一；然后是构建起协同联动的整体防御体系；最后是增强网络攻击（尤其是新型网络攻击）的检测发现能力、溯源分析、响应处置等能力。更深层的需求是强化顶层设计，改变重建设轻运营的局面，充分发挥安全防护技术的效能，进而满足法院网络安全体系化防护的需求。

基于天眼建立威胁运营平台 为浙江省高院实现四个“统一”

为解决上述问题，浙江省高院于 2019 年，选择了和业界领先的网络安全公司奇安信进行了接触，后者业内首创的“数据驱动安全”理念，引起了浙江省高院的浓厚兴趣，双方在威胁情报收集与分析、实战化威胁运营等方面达成合作。

在具体实施方面，浙江省高院部署了天眼威胁情报分析平台和实战化威胁运营平台，杭州市中级人民法院旁路部署分析平台和探针在专网核心交换机，桐乡县人民法院旁路部署探针，构建“省 – 市 – 区县”三级部署模式。部署架构如图 2 所示。

“部署这两个平台的效果是显而易见的，凭借天眼的威胁发现能力，以及威胁运营平台的、新的系统实现四个‘统一’，真正达到了数据驱动安全的目标。” 浙

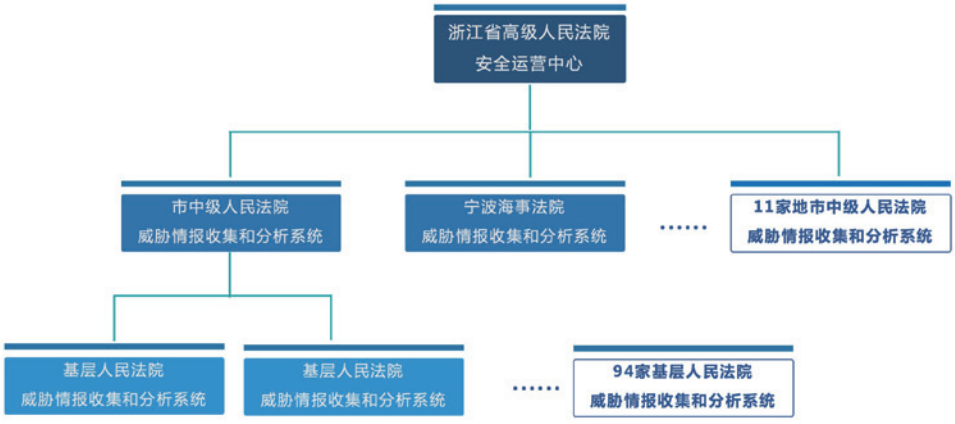


图 2：浙江高级法院实战化威胁运营总体架构

江省高院信息科科长毛林斌表示。

第一是上报数据格式统一。

网络流量数据包括网络协议、文件协议、数据库协议、会话流量等各类数据类型，不同数据类型又有不同格式，如上报数据类型、格式不同，会影响省高院安全运营平台的分析结果。通过上报数据格式的统一，大幅提升了各地市人民法院威胁情报收集和分析系统的效率和有效运转。

第二是实现威胁情报收集和分析系统管理统一。

威胁监测类系统的“统采”可实现对分布全省的近百台威胁监测类系统的统一管理，包括策略批量下发、平台统一升级、状态统一监控、平台统一运维等，可有效提升威胁情报收集和分析系统的运行效率，减轻各级人民法院的运维工作量。威胁情报收集与分析平台的统一管理见图 3.

第三是监督和安全考核机制的统一。

安全考核要基于数据，考核标准要统一，前提是数据要统一。通过实现各地市人民法院威胁情报收集和分析系统的上报数据类型、格式及告警的统一，有利于建立全省统一的网络安全考核机制，进而验证并提升各单位的网络安全水平。

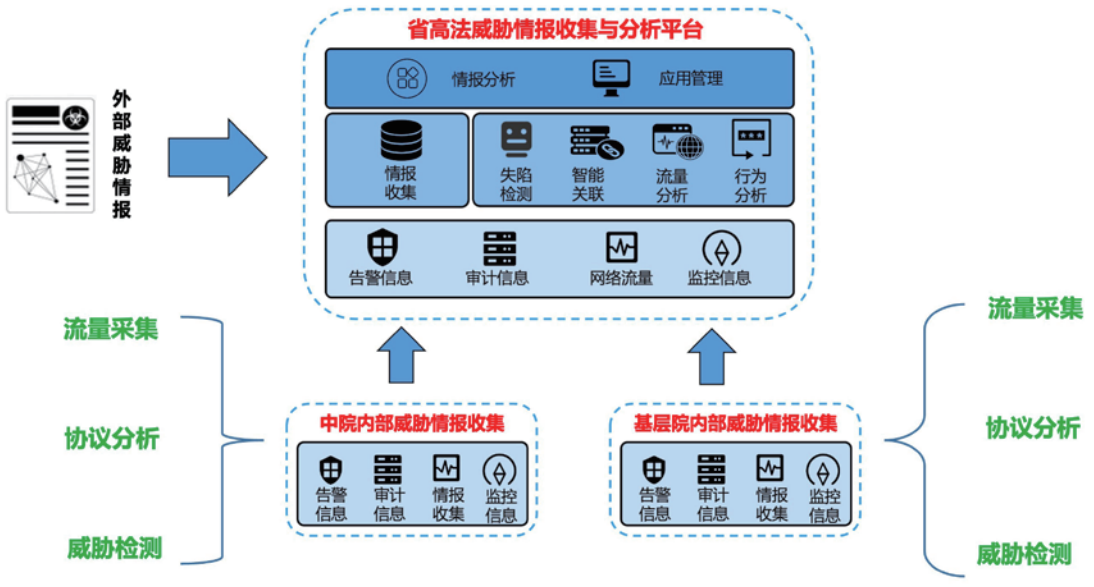


图 3：威胁情报收集与分析平台的统一管理

第四是安全防护水平的统一。

威胁情报收集与分析系统“统采”有利于避免网络安全的“短板效应”。毛林斌认为，法院专网是“全省一张网”，即使全省 99% 的法院的网络安全都做得非常完善，如果存在某一个法院的网络安全水平较低，那么黑客就可以通过该薄弱环节渗透进法院专网，并攻击网内的信息系统。

目前，杭州市、湖州市、嘉兴市等四个地市已经部署了分析平台，嘉兴市全市八个部署了探针，从省高院到嘉兴市到桐乡等四级成一线，从总部到地区实现无缝联动、充分拉齐安全能力，避免单点被突破、导致满盘皆输的情况。

“网络安全是‘三分靠技术，七分靠管理’。” 毛林斌感叹道，2020 年，浙江省高院购买了奇安信安全服务，组建了专业的驻场安全工程师团队，制定了网络安全管理制度，并成立安全运营小组，分析法院面临的安全威胁，其中涉及账号弱口令、应用软件漏洞等安全风险。

“参考网络安全滑动标尺模型，浙江法院体系已经从架构安全 – 被动防御 – 积极防御 – 威胁情报逐步建设，形成了初级威胁可防御，高级威胁可监测的动态安全能力，同时兼顾防御、检测、响应和预防四个方面，安全能力有了质的飞跃。”毛林斌总结道。

这些成果在实战中也获得了验证。通过法院专网威胁告警监测及处置，浙江法院发现并处置专网威胁达 39035 个，对法院的网络环境、各类办公业务起到有效防护。2021 年，在网信办、公安厅牵头的攻防实战演习中，浙江省高院取得了零失陷的出色成绩。威胁情报收集与分析平台展示大屏见图 4。

率先实施 2+2 零信任体系 护航“全域数字法院”

在网络安全的道路上，只有起点，没有终点。为了解决全域数字法院在建设过程中，因滥用账号、异地登录、仿冒，以及数据通道未加密等导致的数据泄露风险，浙江省高院在法院行业率先建设基于“零信任”的“2+2”安全运营体系，并成功入选了《法治日报》2021 政法智能化建设智慧法院创新案例。

展望未来，浙江省高院将继续贯彻落实安全与业务统一谋划，安全和发展同步推进的原则，为‘全域数字法院’构筑坚实的网络安全底座。



图 4：威胁情报收集与分析平台展示大屏

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

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”，HuaYunSec）成立于2016年，是一家深耕于网络信息安全领域，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，在上海、广州、苏州、武汉设有分支机构，公司核心团队来自腾讯、网易、阿里巴巴、思科等国际知名科技企业，具有丰富的技术积淀和管理经验。

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。

华云信安基于业内领先的网络安全解决方案、雄厚的技术实力以及丰富的服务经验，为互联网、金融、能源、制造、交通、医疗、零售等行业的广大用户，提供优质多元的网络信息安全解决方案、网络信息安全技术服务和基础架构实施服务。

服务实施组

华云信安安全服务团队主要由具有多年安全经验的业界专家、咨询顾问及攻防安全研究员组成，多名成员获得CISSP/CISP/COBIT/ITIL 等安全相关认证。服务团队现有数十人并在持续壮大中，凭借专业的素养、高超的技术和丰富的经验，为众多客户提供安全咨询、安全评估、安全培训、安全审计、安全检查、安全保障等服务，赢得高度赞誉和广泛认可。

攻防实验室

华云信安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。

安全咨询服务　安全评估服务　安全检查服务　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