安天周观察

安天官方微博　安天官方微信

主办：安天　2020 年 10 月 26 日 (总第 251 期) 试行　本期 4 版　微信搜索：antiylab　内部资料 免费交流

2020 社会责任榜单 网安行业安天领跑

10 月 16 日，第二届中国互联网企业社会责任高峰论坛暨《2020 中国互联网企业社会责任报告》（下称“报告”）发布会在京举行。报告由北京师范大学互联网发展研究院、互联网司法治理研究中心联合光明网、中国经济网、中国日报网、中国网、北师大中国教育与社会发展研究院权威发布，系统评价了中国互联网企业社会责任发展现状，为进一步强化社会责任意识，改进社会责任管理，更好地促进经济效益与社会效益的统一，实现企业和行业健康、有序地发展提供依据。

《2020 中国互联网企业社会责任报告》考察的 18 个互联网行业中，筛选 240 个分析对象，从“社会价值”“产品 / 服务责任”“企业家责任”“责任管理”“企业公益”“负面影响”六个维度设置具体指标，评价其社会责任发展现状，特别是重点考察了疫情期间互联网企业的社会责任表现。

行业	第一名	第二名	第三名
电子商务	阿里巴巴（淘宝、天猫）	苏宁易购	京东
医疗健康	微医	阿里健康	丁香园
网络教育	作业帮	新东方	掌门 1 对 1
网络安全	安天	360	中孚信息
人工智能	百度（人工智能）	科大讯飞	海康威视
社交平台	新浪微博	微信、QQ	百度贴吧
视频	快手	秒拍	爱奇艺
交通出行	美团打车	嘀嗒出行	曹操出行
移动智能终端	华为	小米	中兴
智能搜索	QQ 浏览器	UC 浏览器	搜狗浏览器
知识付费	百度文库	QQ 阅读	豆瓣
网络音乐	QQ 音乐	酷我音乐播放器	酷狗音乐
互联网金融	蚂蚁金服等	微信支付等	平安口袋银行
旅游	携程网	飞猪	同程艺龙网
房地产服务	链家网	我爱我家	贝壳找房
招聘	58 同城（赶集网）	智联招聘	猎聘
汽车服务	途虎养车	汽车之家	淘车二手车
网络游戏	腾讯游戏	三七互娱	完美世界

安天位列网络安全行业第一名

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势。构筑由铸岳、智甲、镇关、探海、捕风、追影、拓痕、智信组成的产品方阵，可以为客户构建资产运维、端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置等安全基础能力。安天通过为客户建设态势感知平台体系，形成网络安全运行的神经中枢，提升客户统一安全运维能力，并通过快捷精准的威胁情报持续完成客户赋能。安天的产品和解决方案保障客户从办公内网、私有云、混合云到工业生产网络的全面安全，保障客户关键数据资产安全和业务运行连续性。使客户能有效应对从病毒传播感染、网络勒索乃至情报级别的攻击窃密的不同层级的威胁，为客户数字化转型保驾护航。

安天以达成客户有效安全价值为企业使命；坚持法治诚信，致力于维护良好的产业生态；坚持以人为本，积极承担社会责任。安天不断将网络安全技术和理念推广至整个社会和重要的行业。在此之前安天就多次获得主管部门、相关媒体评选出的“践行社会责任”、“互联网行业自律贡献企业”等多次表彰。

历经 20 年的发展，安天已经成为我国网络安全应急支撑的重要企业节点，以第一时间启动，同时应对多线威胁，三体系联动，四作业面协同为导向，构筑了应急分析与响应支撑体系。安天已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，安天进行了先发预警或全面应急响应，有力支撑了国家和政企机构的应急响应工作。安天持续监测跟踪了数百个威胁行为体的活动，特别是针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（APT 组织）进行了攻击活动、攻击装备、支撑体系和作业手法的深度解析，分析成果在第一时间向主管部门报送，并按照相关规范要求，进行负责人的公开信息披露。在去年 6 月 1 日，安天发布长篇分析报告，完整复盘了美国情报机构 NSA 入侵中东金融机构的全过程。

安天为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。参与了 2005 年后历次国家重大政治社会活动的安保工作，并多次获得杰出贡献奖、安保先进集体等称号。

安天通过安全中间件授权模式，推动了基础威胁检测防护能力向供应链侧的原生融合，安天安全引擎已经累计为超过 21 亿部手机终端和其他移动安全设备，提供了出厂预置的安全能力，有效遏制了手机病毒的泛滥，也为系统安全环境治理提供了基础支撑能力。安天坚守“安全的技术必须转化有效安全价值”的理念，坚持网络安全的契约价值，探索了不同于“互联网免费安全”的价值模式。在网络安全业 TOP10 的安全企业有一半以上选择安天为反病毒引擎合作伙伴，亦为支撑良性协同产业生态做出了贡献。

新冠疫情发生后，安天迅速启动重大社会事件网络安全应急值守制度，研判安全风险。各地研发中心和应急响应站第一时间启动工作，有效支撑客户网络安全保障。并为卫生医疗系统提供了智甲终端防御系统医疗行业版、智信零信任移动安全接入的免费服务，并紧急发布三款免费专业处置分析工具支撑疫情期间远程安全响应需求。安天快速跟进分析与疫情相关的 APT 攻击、科研成果窃取等安全风险，向有关部门呈递了长篇分析报告，系统分析了疫情期间威胁行为体对我国卫生防疫部门攻击情况、关联衍生风险情况、个人信息和隐私的次生灾害等问题，获得好评。安天发挥自身在数据分析、安全可视化等方面的技术优势，在春节期间，为部委和政企机构免费提供了分析员工分布与防控风险、有效安排返程的可视化分析工具。2020 年 2 月，安天入选了工信部疫情防控重点保障企业名单。

面对社会运行高度依赖互联网基础设施，远程办公成为普遍模式，重要信息资产暴露面增加，防御难度加大等问题。安天将继续把习近平总书记关于“关口前移，防患于未然”的要求落到实处。承担起网络安全企业的责任与担当，赋能客户，共筑网络安全防线。

每周安全事件

类 型	内 容
中文标题	Adobe 发布 Adobe Media Encoder 带外更新
英文标题	Adobe releases out-of-band security update for Adobe Media Encoder
作者及单位	Lawrence Abrams
内容概述	Adobe 已发布 Adobe Media Encoder 的带外安全更新，该更新修复了三个“重要”安全漏洞。这三个漏洞被归类为“信息泄露”，这可能会使敏感信息在活跃用户的安全情况下被泄露。该更新修复了可能导致信息泄露的越界读取漏洞，这些漏洞的优先级为“3”，这意味着它们不是攻击者的目标，也没有使用它们的主动攻击。用户应安装 Adobe Media Encoder 14.4 来修复这三个漏洞。
链接地址	https://www.bleepingcomputer.com/news/security/adobe-releases-out-of-band-security-update-for-adobe-media-encoder/

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 3 个活跃的漏洞以及 7 个活跃的恶意代码家族值得关注

恶意代码类别	名称	威胁等级	简要描述
活跃漏洞	Microsoft Windows Hyper-V 远程代码执行漏洞（CVE-2020-16891）	高	Microsoft Windows Hyper-V 中存在安全漏洞。当主机服务器上的 Windows Hyper-V 无法正确验证来宾操作系统上经身份验证的用户的输入时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。
	Microsoft Windows TCP/IP 远程代码执行漏洞（CVE-2020-16898）	高	Microsoft Windows TCP/IP 中存在安全漏洞。当 Windows TCP/IP 堆栈不当处理 ICMPv6 Router Advertisement 数据包时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以获取在目标服务器或客户端上执行代码的能力。
	Microsoft GDI 远程代码执行漏洞（CVE-2020-16911）	高	Microsoft GDI 中存在安全漏洞。Windows 图形设备接口 (GDI) 处理内存中对象的方式中存在远程代码执行漏洞。成功利用此漏洞的攻击者可能会控制受影响的系统。
较为活跃样本家族	Trojan[Banker]/Win32.Emotet	中	此威胁是一个具有窃取银行账户行为的木马家族。该家族木马在执行后会在后台对进程进行监控，监视登陆银行页面的进程并记录信息，回传攻击者服务器。
	Trojan/Win32.SelfDel	中	此威胁是一种对恶意木马家族。该家族木马的主要功能是对抗反病毒软件或安全工具，通常会关闭反病毒软件或安全工具的进程。该家族木马同时还具有删除反病毒软件的病毒库、文件或安全工具的功能。
	Trojan[Banker]/Win32.Banbra	中	此威胁是一中专门用于盗取银行信息木马家族。该家族木马运行后能够感染硬盘的主引导记录，对包括使用 EV-SSL 的 HTTPS 在内所有类型的网络流量进行监控，在被窃取的信息发送到金融网站之前就被传送到远程服务器上。
	Trojan[Dropper]/Win32.Dinwod	中	此威胁是一种具有释放或捆绑行为的木马类家族。该家族木马在感染用户系统之后，会自动释放并安装其它恶意程序。该家族的部分变种还具有强制关闭杀毒软件的能力。
	Trojan[Packed]/Win32.Katusha	中	此威胁是一种木马家族。该家族木马通常伪装成常用软件的更新程序，通过电子邮件传播，伺机感染用户计算机。利用社会工程学诱骗用户执行附件程序。该家族木马还会自动下载其它恶意软件，伪造虚假警报提示，以欺骗用户进行付费。
	Trojan[Backdoor]/Linux.Mirai	中	此威胁是一种 Linux 平台上的僵尸网络家族。该家族样本主要是利用漏洞传播并组建僵尸网络，并利用僵尸网络传播相关恶意软件。
	Trojan/Android.Hqwar	中	此威胁是安卓平台上一种间谍类木马家族。该家族木马运行后，伪装成系统应用，联网上传用户短信、通讯录、通话记录、录音、位置信息等隐私信息，私自发送指定短信，造成用户隐私泄露和资费消耗。

Gartner：2021 年战略技术趋势

迈克尔·库尼 / 文　安天技术公益翻译组 / 译

研究公司 Gartner 每年都会公布下一年企业需要关注的重要战略技术趋势。今年，Gartner 指出，企业需专注于构建弹性并接受“颠覆性变革是常态”的观点。

Gartner 研究副总裁布莱恩·伯克（Brian Burke）表示：“企业各职能部门对运营弹性的需求从未如此强烈”。

伯克以这些概念为背景，预测了 2021 年的重要战略技术趋势。

行为互联网（IoB）

伯克说，使用人脸识别、位置跟踪和大数据，并将数据与相关行为事件（例如现金购买或设备使用情况）相关联的技术不断发展。企业使用这些数据来影响“人的”行为——Gartner 称之为“行为互联网”。例如，为了在疫情期间监控对健康规定的遵守情况，企业可以使用 IoB 计算机视觉来查看员工是否佩戴口罩，或者通过热成像来识别发热者。

Gartner 预测，到 2025 年末，全球一半以上的人口将至少参与一项私人、商业或政府 IoB 项目。伯克说：“虽然 IoB 在技术上有可能实现，但是对影响行为的各种方法仍会有广泛的伦理和社会学讨论。”

隐私增强计算

伯克说，到 2025 年，将有 50％的大型企业采用隐私增强计算，以便在不受信环境和多方数据分析用例中处理数据时保持机密性或隐私性，并保护使用中的数据。Gartner 分析师说，企业需要评估个人数据传输、数据货币化、欺诈分析等高度敏感数据用例的数据处理活动，以确定隐私增强计算的候选对象。

网络安全网格

伯克说，网络安全网格使任何人都可以安全地访问任何数字资产，无论资产或人员位于何处。它通过云交付模型将策略执行与策略决策分离，并使身份成为安全边界。伯克说，到 2025 年，网络安全网格将支持超过一半的数字访问控制请求。

伯克指出：“疫情加速了企业的数字化变革。我们已经越过了一个转折点——大多数企业的网络资产都已超出传统的物理和逻辑安全边界。随着‘随处运营’的不断发展，网络安全网格将成为从非受控设备安全访问和使用云应用与分布式数据的最实用方法。”

分布式云

Gartner 已连续数年将分布式云服务列入技术趋势清单。Gartner 说，分布式云是指将公有云服务交付到不同的物理位置，公有云提供商负责服务的运营、监管和更新。对于需要低延迟、降低数据成本和数据驻留的企业来说，分布式云能够提供灵活的环境。它还能使云计算资源更靠近发生数据和业务活动的物理位置。到 2025 年，大多数云服务平台都能够提供“按需执行”的分布式云服务。“分布式云可以代替私有云，为云计算提供边缘云和其他新用例，代表了云计算的未来。”伯克说。

超级自动化

Gartner 指出，超级自动化将多种机器学习（ML）、打包软件和自动化工具组合起来以交付工作。虽说在过去的几年中，超级自动化也在不断发展; 但是疫情导致任何事物的“数字优先”使该需求激增。业务利益相关者所积压的需求已促使 70% 以上的商业机构实施了数十种超级自动化计划。伯克说：“超级自动化是不可避免和不可逆的，所有能够而且应该自动化的事物都会实现自动化。”

随处运营

伯克说，“随处运营”是一种为全球客户提供支持、为全球各地员工赋能并管理各类分布式基础设施业务服务部署的 IT 运营模式。到 2023 年底，40％的企业将采用“随处运营”，以提供优化和混合的虚拟和物理客户与员工体验。

全面体验

Gartner 在去年的趋势报告中指出，到 2028 年，“用户体验将在用户如何看待数字世界以及与数字世界交互的方式上（多重体验）发生重大转变。”改善了语音和对话管理功能的会话平台将改变人们与数字世界交互的方式。今年，多重体验发展为全面体验（TX）。该策略将多重体验与“客户、员工和用户体验联系起来”。非接触式界面等技术改变了数字体验；随着交互更加移动、虚拟和分布式，企业需要 TX 策略。

智能可组合业务

智能可组合业务可以通过获取更好的信息并对此做出更敏锐的响应，来彻底改变决策。例如，借助丰富的数据和见解，未来的机器将具有更强大的决策能力。智能可组合业务将为重新设计数字业务时点、新业务模型、自主运营以及新产品、各类服务和渠道铺平道路。伯克说：“为提高效率而建立的静态业务流程非常脆弱，以至于在疫情冲击下分崩离析。CIO 和 IT 领导者努力收拾残局，他们开始了解适应业务变革步伐的功能的重要性。”

AI 工程化

伯克说，随着更多自动化需求的增长，AI 将在多个学科中成熟。但 Gartner 的研究表明，只有 53％的项目能够从 AI 原型转化到生产。这意味着，要想将 AI 转化为生产力，必须转向 AI 工程化，这是一门专注于各种可操作 AI 和决策模型（例如机器学习或知识图）的监管和生命周期管理的学科。

原文名称	Gartner: Top strategic technology trends for 2021
作者简介	迈克尔·库尼（Michael Cooney）。迈克尔·库尼是 Network World 资深编辑。
原文信息	2020 年 10 月 19 日发布于 Network World 原文地址 https://www.networkworld.com/article/3586571/gartner-top-strategic-technology-trends-for-2021.html
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。

安天智甲有效防护 Woodrat 勒索软件

勒索软件名：Woodrat 勒索软件
传播方式：垃圾邮件
加密算法：AES+RSA
后缀：.woodrat
支付与金额：通过勒索信中的门罗币钱包地址
免费解密工具：暂未发现

近日，安天 CERT 在梳理网络安全事件时发现一个名为 Woodrat 的勒索软件。该勒索软件最早发现于 2020 年 10 月，主要通过垃圾邮件进行传播，邮件附件为勒索软件程序，邮件内容诱使用户执行该程序。该勒索软件运行后，将在短时间内完成对计算机文件的加密操作。经验证，安天智甲终端防御系统（简称 IEP）的勒索软件防护模块可有效阻止 Woodrat 勒索软件的加密行为。

Woodrat 勒索软件样本运行后，创建多个线程，在短时间内完成对计算机上相关文件的加密，在被加密文件的后缀名后追加以“.woodrat”命名的后缀；加密完成后，该勒索软件在每个被加密文件的同一文件夹下创建一个名为“LOCKED_README.txt”的勒索信，该勒索信由中英文书写，具体内容包含了勒索说明、联系邮箱、USER_ID、门罗币购买教程和勒索者门罗币钱包地址，其中强调了勒索金额随时间变化，具体为 3 天内加密的支付 1.5xmr、3 天 -7 天内加密的支付 3xmr、一个月内加密的支付 10xmr 可解密和超过一个月加密的永不解密。

▲Woodrat 勒索信

Woodrat 勒索软件采用“AES+RSA”加密算法，目前被加密的文件在未得到密钥前暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的密码；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。目前，安天追影产品已经实现了对该类勒索软件的鉴定；安天智甲已经实现了对该勒索软件的查杀。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、字符串分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、信标检测鉴定器、关联分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆概要信息

文件名	woodrat.exe
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	5.97 MB
MD5	127E7DCE984CC0ACEA750746B485C101
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan/Win32.Zudochka
判定依据	反病毒引擎

◆操作系统

操作系统	内置软件
Win7 x86 6.1.7600 Build 7600	默认、IE9、Google Chrome、Firefox、Office 2007、Flash、WPS、FoxitReader、Adobe Reader

◆危险行为

行为描述	危险等级
内联钩子	★★★★
查询系统硬盘大小	★★★
延时	★★★
文件篡改	★★★★★

◆常见行为

行为描述	危险等级
获取系统信息（处理器 版本、处理器类型等	★
加载运行时 DLL	★
壳行为填充导入表	★★
设置调试器权限	★
访问文件尾部	★
DNS 请求	★
检索系统内存信息	★
扫描磁盘类型	★★
根目录下创建 EXE 文件	★★

◆扫描二维码查看完整报告