届毕月刊

特刊

2018

知道创宇

本期看点

编委 黑哥 刘光旭 李伟辰 孙蕾 王宇 张毅
美工 徐文征 郭莎莎
出品 知道创宇市场部

投稿邮箱：tg@knownsec.com。同时欢迎您提出各种意见和建议。

北京知道创宇信息技术有限公司
Beijing Knownsec Information Technology Co., Ltd.

北京市朝阳区阜安西路望京 SOHO T3 A 座 15 层
15th Floor, Unit A, Tower 3, Wangjing SOHO, Fu'an West Road, Chaoyang District, Beijing
010-57076191
010-57076117（FAX）

赛博世界推进现实世界的不断融合，让信息安全成为时代的必需品。踏浪而来的我们有望在数年后成为世界一流的安全企业，这个梦想值得每一位创宇人为之奋斗！不忘初心、坚定信念，锐意创新、精诚协作，我们不仅要最酷，我们还要 No.1！

——赵伟

希望酷月刊能办成有内容、有干货、有人文、有情怀的刊物。

——杨冀龙

CONTENTS 目录

创宇 2018

领军云防御

安全保障

产品动态

行业合作

重磅活动

安全研究

创宇生活

创宇 2018

知道创宇登陆纳斯达克大屏 向世界展示中国网络安全力量

美国纽约时代广场（Times Square）位于美国纽约市曼哈顿区第 43 大街、弗洛德街跟第 7 路交叉的三角地带，是财富与文化双雄交汇的“世界十字路口”。在这里，年均客流量数千万人次、人员流量上亿人次。

纳斯达克大屏幕则是纽约时代广场的标志性建筑物，高 36.5 米，宽 25.5 米，其屏幕面积之大及世界影响之广泛，被誉为“世界第一屏”。作为全球最受瞩目的商业核心地段，全球高端品牌长期在这里传播品牌形象；而这里播出的信息多次引起 BBC、路透社、新华社等传媒巨头的关注，成为名副其实“吸引世界目光”的最佳窗口之一。

今年 3 月份，知道创宇公司在纳斯达克广告大屏的亮相。这与知道创宇在 3 月份以前对外宣布加大海外云防御节点的部署有极大关系，这意味着未来知道创宇不仅能保障客户在国内市场的安全需求，如果客户渴望走出国门，去拓展海外业务，我们同样也能提供相应的安全保障。

2018 年伊始，知道创宇已经在国家品牌这个重磅级大舞台亮相了两次——《大国重器第二季》中露脸的“网络正义者联盟”——安全联盟，是由知道创宇联合业界发起、并由知道创宇长期运营的；而作为《CCTV 国家品牌计划》代表中国网络安全行业的形象展示在纳斯达克大屏，则是第二波。

除了在纳斯达克大屏亮相之外，无巧不成书的是证券行业当时正疯传相关部门即将对“独角兽”企业提供上市便利，而知道创宇又幸运地被权威创业媒体评选为国内网络安全行业唯一进入 TOP100 企业的“独角兽”，一系列现象是否预示着知道创宇即将 IPO 呢？反正投资界都十分关注。

总之，在十年磨砺之后，这家一向行事低调的企业终于开始不低调起来：它为中国超过 90 万网站提供安全服务，云防御市场占有率第一；还为国家重要职能部门长期提供网络安全服务，并在国家各种重大会议活动中承担网络安保的重要责任。作为当前网络安全行业里技术方向、发展潜力、公司及客户规模都属于国内业界 TOP 级别的一家企业，知道创宇有能力也有责任为中国的网络安全力量代言，成为名副其实的国家品牌！

知道创宇数次上榜权威媒体“独角兽”榜单

创业媒体创业家 &i 黑马从互联网、人工智能、智能制造、生物医药等前沿领域，综合企业行业地位、融资情况等条件，筛选出《最有可能穿过 A 股快速通道的 100 家“独角兽”》名单，网络安全领域仅有北京知道创宇信息技术有限公司榜上有名。

“在“没有网络安全，就没有国家安全”的基本战略指导下，国内的网络安全领域迎来了发展的春天，目前国内活跃的网络安全企业已经达到数百家，可以说是当前最具潜力的一个市场。”一位投资界人士表示，“但是行业属于刚刚进入高速期，真正具备独角兽潜质的公司还是较少，独角兽企业需要有一定的市场占有率和具备良好潜力。而且，还能够为客户提供较为全面的产品和服务，来解决客户的痛点，目前网络安全企业数量多但是大多只能解决单一痛点，像知道创宇这样能够提供全面安全解决方案的企业还为数不多。”

中科院《互联网周刊》& 科技媒体 eNet 硅谷动力以“发展迅猛、勇于创新”的新价值观定义并筛选出“2018 最具潜力独角兽企业 Top150”，北京知道创宇信息技术有限公司再次榜上有名。

据报告分析，多数因估值超过百亿美元而成为“超级

企业服务	猎聘网	D轮	10亿美元	2006年	北京
	Testin	C轮	/	2011年	北京
	知道创宇	C轮	10亿美元	2007年	北京
	猪八戒网	C轮	超120亿元人民币	2005年	重庆

独角兽”的初创企业离不开集团的支持和资本的助力，而在众多垂直细分领域，还有更多业内拔尖的企业值得关注。新价值观定义下的独角兽榜单挖掘和传达了一批优秀企业的目标、使命、价值观，向世人和资本市场展示这那些代表未来、助力中华民族伟大复兴的互联网力量。而作为资本市场非常青睐的网络安全领域，知道创宇是榜单中唯一一家网络安全企业。

5 月 19 日，由人民网和成都市政府主办的“2018 全球独角兽企业高峰论坛”在蓉举行，人民创投、人民网舆情数据中心和四川天府新区成都管委会战略研究局联合发布了《中国独角兽和瞪羚企业价值榜》，北京知道创宇信息技术有限公司荣誉入选瞪羚企业价值榜单。

人民创投总经理赵亚辉表示，瞪羚企业的特点是在特定领域具备技术领先性，业务积极正向，创新驱动，成长迅速，产品符合国家战略和美好生活的需要，企业展现出较大的发展潜力。企业是尚未独立上市或被收购，非其他企业的全资企业，有公开融资纪录；具备很好的投资价值，收入和市场份额高速成长。作为资本市场非常青睐的网络安全领域，知道创宇得以从投资价值、技术潜力、政策环境、市场前景、舆论口碑等多个评选维度脱颖而出，成为业界肯定与关注的瞪羚企业。

4 月 24 日，由创业黑马、创业家 APP 主办的“2018 独角兽峰会”在京举行。会上，创业黑马正式发布了《中国硬独角兽 TOP100（春榜）》。北京知道创宇信息技术有限公司再次以唯一一家网络安全企业的身份入选该“独角兽”榜单。

创业黑马表示，此次发布的硬独角兽榜单是指那些拥

2018最具潜力独角兽企业Top150

企业	业务
梨视频	资讯短视频平台
拼好货	C2B水果拼单社交分享电商
知道创宇	网络安全服务商
图森未来	城际物流自动驾驶解决方案提供商
缤果盒子	智能零售便利店

有把科技落地实业的硬实力，位居产业龙头，规模营收可持续，处于准上市阶段的企业。此榜单旨在挖掘深藏各个产业、城市的硬独角兽，展现硬独角兽独特的价值。榜单中出现的企业多以技术驱动型为主，同时模式创新带来强有力的企业升级发展。

9 月 1 日，南京软博会鼓楼专场暨中国独角兽（秋季）峰会召开，本次峰会不仅围绕大数据＋产业的主题，展开主题演讲、高峰论坛，更是首次揭晓由创业黑马评选出的充满力量的“中国大数据硬独角兽榜”。北京知道创宇信息技术有限公司成功入选该“独角兽”榜单。

创业黑马表示，大数据产业硬独角兽企业是最能代表大数据产业未来的公司，经过全网公开征选、投票与专业评委评选，首次揭晓，让独角兽企业站在产业变革的中央，引领产业升级的浪潮，更好的服务于实体经济。

知道创宇今年先后被多家媒体、行业组织评选为“独角兽”企业，同时也多次以唯一一家网络安全企业身份入选。作为国内最早从事云防御的网络安全企业，根据第三方市场调研，其云防御市场占有率方面高居榜首。在技术驱动方面，知道创宇云防御由多款安全产品序列组成，云安全平台先后三次重大升级，围绕云技术、人工智能、大数据的开发与利用，为客户在线业务提供一整套先进的安全解决方案。技术的利用和模式的创新，已令知道创宇在云防御市场上占据了领跑龙头企业地位。

安全联盟被央视《大国重器》高度褒奖为“国之重器”

中央电视台与工业和信息化部联合制作的大型纪录片《大国重器第二季》一开播，便成为央视剧王并持续热播，每一个国人都因为国家所获得的成就所震撼和骄傲。值得注意的是，“国之重器”已不仅仅是现实世界的工业制造，在更广阔的虚拟世界中建设网络强国，中国需要构筑起网络空间的铜墙铁壁。在刚刚播出的《大国重器第二季》第六集中，就演绎了一场惊心动魄的网络攻坚战，而为国家网络安全而奋斗的安全从业者们，被该剧赞扬，同样被授予“大国重器”的荣誉。

而其中，一个“中国互联网上的正义者联盟”跃然屏幕，激发了笔者的无限好奇，节目中这样介绍：

“这是中国互联网上的正义者联盟，他们不仅包括腾讯的七大实验室、还包括国内顶级网络安全公司，以及重大基础设施的网络安全部门。他们与政府部门信息共享、协同作战，共筑中国网络安全的钢铁长城。”

原来，早在 2012 年，国内知名安全公司知道创宇就联合腾讯、百度、金山等互联网企业发起了一个公益组织，旨在促成一个中立、公正、权威的第三方平台，团结有实力的企业进行资源共享，共同建立行业公认的互联网安全标准，联合企业、机构、网民一起构建有效的网络安全社会化治理体系，优化中国互联网使用环境。截止到目前，已经有超过百家国内互联网头部企业、国家机构及媒体等

加入这一正义者联盟。

联盟成员们从共享和协同的态度出发，倡导共享数据、共享标准、协同防治。集各安全厂商之所长，开放安全数据给全社会，互通有无，共筑防护长城。以实践为先导，共同建立网络安全标准，履行中立与公正。跨行业、跨厂商、跨平台联合推动安全基础建设，协同对抗网络攻击与犯罪。

公开数据显示，安全联盟目前已建成国内最大的第三方网络安全数据共享交换平台，拥有超过 8.9 亿条恶意网址、电话数据。长期以来，这些恶意数据向全网开放，应用到其合作伙伴的搜索引擎、浏览器、IM、社交平台、路由器 OS 等互联网终端，每天为网民提供超过 30 亿次恶意风险提醒，极大程度地帮助网民远离各类网络攻击。

据安全联盟负责人介绍，除了在底层建立防护网，遏制恶意网址、病毒的传播，民众安全意识的培养同样是打击网络攻击的重要手段之一。一方面，安全联盟通过与各地网警、网信部门以及各企业单位合作，开辟举报专区（如：青岛互联网违法信息举报中心、58 同城虚假兼职举报专区等），开展全民举报；另一方面，安全联盟持续于线上线下进行网络安全公益宣传，仅 2017 年曝光量就超过 1 亿次，大面积普及安全常识。通过从打击端和防范端双向发力，安全联盟践行着“让用户安全上网”的宗旨，发动安全部门、安全企业、普通民众共同参与到网络安全的治理中来，并取得了良好的效果。

◢ *安全联盟恶意数据库已应用于腾讯电脑管家*

“中国网络正义者联盟”——安全联盟开创性地打破了互联网各平台信息不能互通的孤岛效应，并发动全民以及社会机构参与到“网络打黑除恶”这一场人民斗争中，让网络坑蒙拐骗偷可以瞬间被中国互联网行业集体“封杀”，充分说明了国人已经逐渐认识到了网络安全的重要性。

大数据、云计算、移动互联网，新一代信息技术为代表的科技革命风起云涌，它们正以前所未有的力量，改变着人类的思维、生产、生活和学习方式，建设网络强国的愿景已经织就，信息装备和技术正成为这个东方大国赢得未来的强大驱动力。正如《大国重器》所畅言，“互联网上的战役，明天还将继续，但中国人守护全球互联网安全的决心，不会改变。”网络安全，总是在路上，不断精进与汇聚的安全力量，就是中国在互联网世界的“国之重器”。

习总书记 419 讲话两周年 知道创宇演绎安全企业责任与担当

两年前的 4 月 19 日，习近平总书记主持召开网络安全和信息化工作座谈会并发表重要讲话。今天我们再次回顾总书记讲话全文，着眼于新时代的发展，可以清晰的看到总书记的高瞻远瞩，以习总书记“4•19”重要讲话为标志，我国网信事业在习近平网络强国战略思想指引下，进入了迈向网络强国的新时代。

与此同时，作为参与中国网信事业建设的你我，也要担负历史赋予我们的责任与担当。在总书记发表 4•19 重要讲话两周年之际，我们来看一下安全企业知道创宇付出的责任与担当。

营造一个风清气正的网络空间

习近平在讲话中曾强调，网络空间是亿万民众共同的精神家园。网络空间天朗气清、生态良好，符合人民利益。网络空间乌烟瘴气、生态恶化，不符合人民利益。我们要本着对社会负责、对人民负责的态度，依法加强网络空间治理，加强网络内容建设，做强网上正面宣传，培育积极健康、向上向善的网络文化，用社会主义核心价值观和人类优秀文明成果滋养人心、滋养社会，做到正能量充沛、主旋律高昂，为广大网民特别是青少年营造一个风清气正的网络空间。

【创宇在行动】：知道创宇高度重视网络空间健康治理工作，早在 2012 年，由知道创宇发起，联合国内多家知名互联网企业、行业组织成立的公益平台安全联盟，过去一直为国家治理网络空间发挥重要作用。安全联盟运营理念是全民参与的网络社会化治理。目前安全联盟已积累诈骗、病毒等恶意网址 10 亿条，而这些安全大数据再通过无偿的共享给百余家互联网合作平台，编制起了一幅巨大的网络空间过滤网。

现在，安全联盟每日通过各平台协同共享风险提醒网民次数近 30 亿，避免网民访问了海量的经过人工审核的恶意网址，挽回经济损失难以预估，这种安全企业、互联网企业牵头建立的“全网”反恶意网址工作体系，在全民“皆兵”的参与体制下，起到了前所未有的网络空间治理功效。

同时安全联盟最近几年还不断的与外界权威机构、公安及社区单位，开展线上举报、投诉（与消协合作）、宣讲等活动，积极发挥平台自身效应，开展安全意识宣传教育工作。2017 年，安全联盟还上线了“网络谣言”举报专项，前不久该功能以小程序形式现身微信端，更加方便了网民查阅。

互联网核心技术是我们最大的“命门”

习近平在讲话中着重指出，一个互联网企业即便规模再大、市值再高，如果核心元器件严重依赖外国，供应链的“命门”掌握在别人手里，那就好比在别人的墙基上砌房子，再大再漂亮也可能经不起风雨，甚至会不堪一击。我们要掌握我国互联网发展主动权，保障互联网安全、国家安全，就必须突破核心技术这个难题，争取在某些领域、某些方面实现“弯道超车”。

【创宇在行动】：知道创宇 CEO 赵伟之前接受中国网信网采访时就曾表示：“总书记对于核心技术对于企业的影响用词非常准确，对于企业来说，产品的核心技术同样是‘命门’。知道创宇云防御服务处于行业领先地位，靠的就是核心技术，比如说抗 DDoS、CC 攻击，这个不是说你投入多少物理资源就可以搞定的，而是要底层的防御引擎要非常有效才行。过去我们业务问过我这样一个问题，他说为什么别的厂商防不住的攻击我们就能防住呢，讲到底就是‘核心技术’的问题。”

赵伟强调称，想要获取“核心技术”，没有什么捷径，知道创宇在过去的十年时间里，在资金投入上非常大，这才有了可以左右自己命运的核心技术，有了核心技术也才有会用户的高度认可，也才会赢得云防御市场占有率第一的地位，这种投入还要持续下去。

国家关键信息基础设施面临较大风险隐患

习近平在讲话中指出，从世界范围看，网络安全威胁和风险日益突出，并日益向政治、经济、文化、社会、生态、国防等领域传导渗透。特别是国家关键信息基础设施面临较大风险隐患，网络安全防控能力薄弱，难以有效应对国家级、有组织的高强度网络攻击。这对世界各国都是一个难题，我们当然也不例外。面对复杂严峻的网络安全形势，我们要保持清醒头脑，各方面齐抓共管，切实维护网络安全。

【创宇在行动】：知道创宇是一家拥有 10 年历史的创新型网络安全公司，其看家本领除了提供最为专业的云防御之外，还在多领域里有深度涉及。在 2013 年，知道创宇重磅推出了国内首款网络空间测绘类产品“ZoomEye 网络空间雷达系统”，利用这一系统，可对未知网络空间进行资产测绘普查。

▲ ZoomEye 可对全球网络空间进行资源探测

知道创宇贯彻国家顶层安全思维，在 ZoomEye 基础之上，于 2017 年推出了“雷达星图”威胁检测态势感知系统。该系统可对重要关键信息基础设施实施全面的脆弱性普查，构筑关键设备“防御备战图”，对国家提供网络安全等级可发挥重要作用。

同时，因知道创宇全面的网络安全保障能力，也受邀参与到了多项国家关键信息基础设施网络安全大检查工作当中，去年 9 月，在党的十九大召开前期，知道创宇还被授予北京市政务信息安全应急队伍，即是对其全面的安全保障能力的高度肯定。

感知网络安全态势，知己知彼，才能百战不殆

习近平在讲话中强调，网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。

全天候全方位感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险。网络安全具有很

强的隐蔽性，一个技术漏洞、安全风险可能隐藏几年都发现不了，结果是“谁进来了不知道、是敌是友不知道、干了什么不知道”，长期“潜伏”在里面，一旦有事就发作了。

【创宇在行动】：知道创宇是国内最早推出成熟的态势感知系统的安全企业，利用“创宇星图”态势感知系统，可以对网络空间所有的资产进行统一管理，它集监控告警及分析防护于一身，基于知道创宇海量基础大数据，可对攻击事件进行回溯，对攻击者进行溯源，同时预测即将发生的安全事件，为管理者提供策略帮助。

该系统在去年中信集团信息化年会上有过代表性应用，作为中信云的安全合作伙伴，系统现场展示了为中信云用户提供云防御的整体网络安全态势，某一时间段内的攻击源，攻击手段、攻击对象等等，均可一一展现。

◢ 赵伟于“创宇星图”发布现场进行讲解

按照知道创宇 CEO 赵伟的指示，在过去一年时间内知道创宇在态势感知体系建设方式有了更为深层的提高。知道创宇在 2017 年推出了数款态势感知系统，其中“雷达星图”、“创宇云图”，与“创宇星图”三者联合应用，再辅以知道创宇对大数据全新的分析与纵横利用，其态势感知能力更是不可同日而语，这也是落实赵伟早日前提及的防范“GPT1”攻击的具体举措。

建立统一高效的网络安全风险报告共享机制

习近平在讲话中指出，要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改。要建立统一高效的网络安全风险报告机制、情报共享机制、研判处置机制，准确把握网络安全风险发生的规律、动向、趋势。要建立政府和企业网络安全信息共享机制，把企业掌握的大量网络安全信息用起来，龙头企业要带头参加这个机制。

【创宇在行动】：知道创宇一直以来就是 CNCERT/CC 的网络安全应用服务支撑单位，同时还积极参与国家漏洞共享计划，是国家信息安全漏洞共享平台的成员单位，长期为国家通报知道创宇的漏洞研究成果，以及安全应急发现，也多次因此受到荣誉表彰。

网络安全为人民，网络安全靠人民

习近平在讲话中强调，网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

【创宇在行动】：可以说知道创宇是最早贯彻总书记指示的网络安全企业，在实际行动中不仅体现在了公益组织安全联盟的不断加大投入上，更是不断的以身作则的通过创新研发，通过站出来、协同合作的形式，给予网民更全面的保护。

知道创宇在 2017 年联合腾讯公司推出了定制化的电信诈骗解决方案，通过与公安机构、运营商的能力合作，已于数个省市落地部署。系统的底层方案基本知道创宇及腾讯公司的安全大数据，通过网络层访问入口识别恶意网址的形式，通过阻断和风险提醒的形式避免网民直接访问，避免了经济财产的损失。该方案识别成功率达 99% 以上，通过部署上线之后的数据对比发现，当地的关于电信诈骗的案发率已下降 88%。

同时，“网络安全为人民，网络安全靠人民”也是最近几年国家网络安全宣传周的主题，知道创宇也连年参与到该项公益的宣传活动当中。这几年，知道创宇均与腾讯一道以超大规模展台的形式，并辅以生动的展示，对参观民众宣讲网络安全防范常识。去年，知道创宇展示的网络钓鱼诈骗就受到了参观群众的高度评价。

网络攻防要做到“魔高一尺、道高一丈”

习近平在讲话中指出，网络安全的本质在对抗，对抗的本质在攻防两端能力较量。要落实网络安全责任制，制定网络安全标准，明确保护对象、保护层级、保护措施。哪些方面要重兵把守、严防死守，哪些方面由地方政府保障、适度防范，哪些方面由市场力量防护，都要有本清清楚楚的账。人家用的是飞机大炮，我们这里还用大刀长矛，那是不行的，攻防力量要对等。要以技术对技术，以技术管技术，做到魔高一尺、道高一丈。

【创宇在行动】：在国家级的重要会议、活动的前期筹备中，知道创宇均被甄选为安全应急保障单位，而在过去的几年时间内，由知道创宇云防御产品提供防护的国家政府重要网站，在保障期间无一被黑，这已成为所有知道创宇人的自豪与荣耀，同时也是鞭策的动力。所今，知道创宇云防御产品“创宇盾”、“抗 D 保”等产品在一如既往的持续投入研发之外，均配备了充足的保障运维人员，技术人员通过不断的攻击大数据分析，不断的夯实着平台的防御等级。

◢ 创宇盾历届保障，无一被黑

同时，云防御平台拥有 90 万国内网站用户，也在为国家经济建设发挥着重要作用。互联网 + 计划的持续推进，网络安全强国的建设，都必须要有安全保障作为前提，知道创宇将坚决捍卫国家网络安全。

另一方面，知道创宇还成立了全资子公司——北京知道未来信息技术有限公司，作为新一代网络攻防一体化安全企业，知道未来从诞生起，便以承载和保障国家信息安全为己任，为国家持续输出一流的网络安全产品、服务和整体解决方案。知道未来专注于为国家提高网络安全监测、

预警及攻防整体能力。

企业做得越大，社会责任、道德责任就越大

习近平在讲话中指出，一个企业既有经济责任、法律责任，也有社会责任、道德责任。企业做得越大，社会责任、道德责任就越大，公众对企业这方面的要求也就越高。我国互联网企业在发展过程中，承担了很多社会责任，这一点要给予充分肯定，希望继续发扬光大。

【创宇在行动】：知道创宇 CEO 赵伟在参加“北京网络媒体红色故土·甘肃行”活动时曾表示：“知道创宇从成立之初就以成就更高社会价值为目标，安全不仅要为国，也要为民，这是知道创宇的核心价值体现。我们所面临的网信事业注定艰巨，但知道创宇愿在其中扮演‘特种兵’这一角色，在关乎‘国家安全’这一重大问题上，满怀信心，绝不含糊，我国网信事业必将成功。”

在履行社会负责方面，知道创宇连年被评为国家级“国家网络与信息安全信息通报机制先进技术支持单位”，知道创宇一直以来履行安全企业应尽的社会负责，多次向国家上报漏洞信息威胁、安全事件威胁，并适时的对外界社会公布漏洞应急及安全研究成果。同时在过去几年里，几次重大的国家级会议背后都有知道创宇参与其中的网络安全保障工作，全部以“满分”成绩完成，并多次获得上级部门“点赞”。

培养网信人才，要下大功夫

习近平在讲话中指出，互联网主要是年轻人的事业，要不拘一格降人才。要解放思想，慧眼识才，爱才惜才。培养网信人才，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院。互联网领域的人才，不少是怪才、奇才，他们往往不走一般套路，有很多奇思妙想。对待特殊人才要有特殊政策，不要求全责备，不要论资排辈，不要都用一把尺子衡量。

【创宇在行动】：知道创宇在过去的一年多时间内，在保障技术稳定研发的基础上，还在内部推行了一项实习生培养计划。知道创宇 COO 兼 CTO 杨冀龙认为，网络安全人才的培养，不仅仅要靠高等院校，拥有实力的网络安全企业最应站出来，来承担一部分历史赋予给我们的责任，现在国家高等院校培养出来的安全人才与市场规模相比有着较大的缺口，所以我们安全企业要在这个历史时期发挥重要作用，多为国家承担一些责任。

知道创宇的实习生培养计划面向的范围将更加广泛，不仅仅面向专业对口的即将走向社会的学生，凡是对网络安全有高度兴趣的非本专业学生均可争取得到实习机会，其内部丰厚的学术氛围，以及课业培养计划，正在为国家网络安全人才培养做出积极贡献，同时该计划也正不断的吸引着未来安全人才的加入，对于国家和企业需要来说都是双赢。

【1】. GPT（God Persistent Threat）上帝模式的持续威胁。“赛博空间内的上帝模式意味着你已经拥有赛博空间绝对的控制和主宰能力，你可以洞察一切表象、洞悉一切内幕、洞穿一切防御。拥有这种能力，就必须要拥有超级大数据能力，可以掌握赛博空间所有节点上的信息并分析，让所有信息在主宰者面前无所遁形，主宰者可以形式上帝力度对所有目标进行高纬度打击。”

封面人物 | 创新、创业与责任——知道创宇 CEO 赵伟谈网络安全

来源：《中国信息安全》杂志 2018 年第 4 期

赵伟，北京知道创宇信息技术有限公司创始人、CEO，中国反病毒联盟资深专家、安全联盟创始人，中国信息安全标准委员会委员、院士工作站特聘专家。

2015 年赵伟在业内首提 GPT 概念（God Persistent Threat 上帝模式的持续威胁），超越了行业对以往的防御认知。

由赵伟创立的知道创宇，专注于云监测与云防御，经过十年发展，已成行业龙头企业，旗下云监测、云防御平台共服务百万余用户，知道创宇公司当前也是国家漏洞库、公安部以及其他省市等政府机构的主要技术支撑单位。在国家网络安全大战略背景之下，知道创宇坚持“侠之大者，为国为民”的信仰，致力于打造“更好的互联网环境”，为国家及企业提供一流的网络解决方案。

从提出 GPT 概念，到“侠之大者，为国为民”，知道创宇 CEO 赵伟一直在推行其独到的网络安全理念。作为一个知名“白帽”，网络安全的先行创业者，赵伟对产业和技术有着敏锐的把握，率领知道创宇在云安全上不断前行。在采访中，赵伟阐述了他对当前安全产业的看法、建议、对创业者的忠告，以及知道创宇如何切实践行为国为民的做法。

一、您如何看待我们和信息发达国家之间网络安全方面的差别？怎样解释您提出的 GPT 的概念？我们有哪些短板需要补足？

赵伟：近几年在国家的高度重视和大力推动下，我们的网络安全产业得到了显著的发展，但从产业环境和整体水平上，我们和国外信息发达国家还存在明显差距。这种差距类似著名的科幻小说“三体”里描述的那样——是高维度同低维度之间的差距，是一种极度不对称的能力差距。

通过斯诺登事件曝光的一系列信息窃取计划，让我们见识到了某些国家对网络空间的掌控能力。我们用钟馗之眼 (ZoomEye) 网络空间搜索引擎扫描了全球网络空间，发现我国网络防御能力在世界上排名在百名开外。为此，我在 2015 年提出了 GPT 概念（God Persistent Threat 上帝模式的持续威胁），不同于业界常说的 ATP（Advanced Persistent Threat 高级持续性威胁），GPT 不再是仅仅关注技术层面的威胁，而是将眼光看得更高更远，从整体网络防御能力来看待安全威胁，包括大数据安全、风险意识、法律环境等。

GPT 意味着你已经拥有网络空间绝对的控制和主宰能力，可以洞察一切表象、洞悉一切内幕、洞穿一切防御。拥有这种能力，就必须要拥有超级大数据能力，可以掌握网络空间所有节点上的信息并分析，让所有信息在主宰者面前无所遁形，主宰者可以开启上帝模式对所有目标进行高纬度打击。

这种能力差距主要是我们和国外对安全的理解不同所导致的。我们理解的攻击，往往都认为是明刀明枪的方式，防御也是针对这种模式来应对。但现在潜在的对手早已经进化到大数据的维度，在这个级别上，它不用通过 APT 来入侵目标的邮箱或者数据库，就可以得到所需的信息。这是一种柔性攻击，本质是通过更高维度的大数据层面收集分析，以极高水平的 APT 配合驱动。通常这些国家的数据治理和跨数据的融合都做得非常好，这是他们高纬度数据分析和攻击的基础。

从这个角度看，就能意识到我们还在手工撒网打鱼，而别人已经用声呐拉网高科技作业。该如何防御？现实的情况是这种威胁暂时无解。这对知道创宇和整个安全产业都是个长期的挑战和鞭策，驱动我们加紧进行技术创新和组织创新，重点发展以大数据驱动的动态防御和态势感知技术，用上帝的视角来感知这种威胁。

只有意识到这种高级威胁的存在，意识到这种能力差距的存在，我们才会痛定思痛，迎头追赶，不断锐意创新，加快网络安全产业的发展，提升自身的各种安全能力，提升国家网络空间安全的实力，真正成为网络强国。

二、知道创宇为何提出“侠之大者，为国为民”的理念？是否可以看作是对国家乃至个人的社会责任？具体是怎么落实到实践上的？

赵伟：“侠之大者，为国为民”是知道创宇的企业信条。作为一个中国网络安全产业的见证者，我经历了从传统的单纯追求技术上极致的“黑客”到如今 “网络安全白帽子”的转变。黑客是一种精神，对技术钻研到底并举一反三，能够用技术改变产业格局，推动产业发展，这是真正的黑客所追求的。但同时我们也意识到，保护互联网的安全是我们最重要也是最终的责任。

互联网是我国在发展中弯道超车的绝佳机遇，但如果被网络安全问题所影响，会减缓甚至拖累其发展速度。作为一直能看到网络阴暗面的安全从业者，我们必须站出来解决这些实际问题，保护国家、企业、个人的信息安全和健康发展。

落实到实践上，首先知道创宇积极参加了国家各项重要安保工作，调动了最好的资源和人力去参与，很多都是无偿付出。其次我们输出优秀的产品和技术，如知道创宇 ZoomEye 网络空间搜索引擎，协助网信主管部门进行对关键信息基础设施的网络安全检查工作。再次，我们和很多地方合作，建设反欺诈平台，帮助执法部门更好地打击电信诈骗。以上这些工作都得到了相关单位的认可甚至表扬，我们也很高兴自身所积累的安全能力能奉献给国家。

为企业方面，知道创宇开发了创宇盾、抗 D 保、加速乐等多款云安全产品和服务，为中国百万余家企业网站提供防黑客入侵、抵御 DDoS 攻击、网站 CDN 加速等服务。很多服务都是免费使用，宗旨是保护众多中小企业不被网络安全所困扰，专注企业发展。

为民众方面，“网络安全为人民，网络安全靠人民”，在网络社会化治理方面，维护网络正义、打击网络犯罪、保障网络空间和谐必须号召全社会的力量进行参与。为保护老百姓上网的安全，知道创宇联合业界有担当的企业和行业组织，共同建立了“安全联盟”——第三方网络安全数据共享交换平台。作为一个公益性的平台，安全联盟定义了数据共享的标准，我们将各家收集到的恶意数据汇集整合，再推送给各家，对恶意网站做到最大范围的拦截。迄今为止安全联盟已经积累了近 10 亿条恶意网址、电话数据库，有效地降低了涉及网址诈骗、电话诈骗的案发率。因为这项工作，在 2016 年，我被评为 3·15“十大最美消费维权人物”，这是对安全联盟切实维护消费者权益所做工作的肯定。

三、您如何评价当前网络安全产业的法规和政策环境？还有哪些地方需要加强？

赵伟：国家对网络安全的大力推动有目共睹，现在网络安全的整体环境比以前好得太多。《网络安全法》和相关配套实施条例的正式出台，使得很多以往模糊的层面有法可依，有章可循。而且针对互联网犯罪中一些常见多发亟需解决的问题，如域名劫持、DDoS 攻击、信息窃取等，司法部门还颁布了指导性案例，给出了具体的司法参考。

具体到安全产品上，以前安全行业同质化竞争特别激烈，各家企业都想做全做多，主要都集中在合规性产品方面。现在随着安全意识的进步，政府和社会的需求不断地提升，需要能解决实际痛点的产品，出现了一些针对这种需求的非合规的安全防御产品，安全市场的细分更加明显，催生了更多的创新企业和技术。这对产业的发展是个实在的推动。

当然，安全形势的大好非一日之功，全民安全意识的教育普及，整个产业的蓬勃发展，都需要一点一滴的积累，预计在未来的三到五年整个产业环境会有一个明显的转变，知道创宇会在其中积极奉献自己的力量。

如果说有一些建议，首先是借鉴国外的经验，在网络安全领域加强军民融合。如美国、以色列的安全企业在国家网络安全中是重要的参与者，有着不可替代的作用。军民融合已是我国的一项重要国家战略，现在我们所面临的网络安全挑战已经超越了军民界限，技术也越来越通用化，民间的网络安全企业能够更多地参与到一些军民融合的项目中，对军民协同、信息共享、技术创新、人才培养等方面都是双赢的效果。

其次，网络安全行业面临的都是国际一流的技术竞争和对抗，对于一些资质性的门槛可以适度降低，鼓励更多有志于网络安全的企业和创业者进入。在国家信息化采购中加大网络安全产品和服务的比例，以及国产化率，扩大产业发展空间，激励企业积极研发先进技术而非只注重盈利，促进产业的创新发展。

四、近些年的行业热点是云计算、大数据，知道创宇十年来在云防御上不断发力，卓有成效，为什么从创立之初就选择云安全作为主攻方向？对新的技术热点如人工智能在网络安全上的应用，知道创宇有何实践？

赵伟：云计算已经火热发展了多年，从开始我们就非常看好这个领域，不仅是云计算技术在安全里的应用，云

计算自身的安全需求也非常明显。一方面云造成了数据的集中，更容易成为攻击者的目标，二来云带来了防御边界的变化，使得过去的安全手段频繁失效。

这种全新的网络态势下，攻防两端的发展趋势一定是“用云攻击云，用云防御云”。传统的鱼叉式的单点攻击已经落伍，现代化的网络安全威胁来自于利用大数据的撒网式的威胁攻击。攻击者利用云的优势、大数据的能力，对政府、企业、广大网民发动一轮又一轮越来越强、频次越来越高、范围越来越广的攻击，传统的安全防御早已力不从心。

云的安全问题还是要用云来解决，就像大数据安全需要用大数据分析等技术手段来解决一样。所以知道创宇长期以来一直把云安全作为主攻方向，将安全技术也用云的手段实现。通过长期的漏洞挖掘研究，将知识库应用于云安全监控防御；通过云防御分析和捕获的攻击大数据，又应用于云防御，构成了知道创宇独特的三位一体的云安全防御体系。在安全就是服务的理念下，形成了创宇盾、抗 D 保、加速乐等一系列云安全服务产品。这些产品正服务于百万余家政府、企业等用户，让他们安全上云。

人工智能的概念其实业界很早就有提出，并已开始应用，例如云计算的实现背后就有大数据和人工智能的支撑。现在所说的人工智能其实就是早已应用的深度学习，只是换了一个说法。深度学习在安全行业应用广泛，国外有一份报告指出人工智能在安全领域有 40% 的使用率。我们在 2008 年开始做云防御时，就用到一些深度学习的技术，然后不断地增加和深化，现在我们的整个产品技术体系已经是基于自动化深度学习的架构。但深度学习也不是万能的，目前行业中对基于特征的拦截，再去匹配一些潜在的同类未知威胁可以做到，但到了 GPT 层面这种错综复杂的柔性攻击，或者说是完全新型的攻击，还需要更深度的人工智能来分析。

五、产业界近年来协同联合的提法较多，您是怎么看待的？知道创宇做了哪些工作？

赵伟：我们深知能力有多大，责任就有多大。前面所说的安全联盟就是我们在产业联合上所做的一个实践，推动产业共享信息，共同解决实际安全问题。

同时，我们还开源自己的软件核心代码，如基于漏洞与 PoC 的远程漏洞验证框架 Pocsuite，可以让有一定开发基础的人就能开发出对应漏洞的观点证明或者漏洞利用代码。开放我们验证过的学习方法和体系，如知道创宇研发技能表，给整个产业更多的助力。在我们的 KCon 黑客大会上请来行业内的“大牛”来做演讲交流，通过“兵器谱”展示推荐同行优秀的安全产品和技术。

安全行业需要大家一起努力，目光放长远，共同把产业做强做大。

六、知道创宇从成立到现在的规模，是一条典型的创业之路。在此过程中您最深的感受是什么？对于当前网安行业的创业者，您有何建议？

赵伟：创业是个打铁的过程，是对自我的修炼。在创业的过程中，我总结了几个陷阱：

第一是机会陷阱。互联网机会和热潮很多，但风口上失败的例子也比比皆是。机会陷阱会把人带偏，使人误入歧途。我们没有盲目追互联网的热点、潮流，找到自己该做的落地点，坚定地做网络安全，做好自己的事情。

第二是技术陷阱。我们属于技术创业，曾经以为技术能解决一切问题，客户应该为好的技术买单。但这是技术人员的一种狭隘和偏执，做出了屠龙刀，没有龙怎么办？偏离用户的需求，是很容易踩上的技术陷阱。而且安全更多的是一个成本问题，要站在整个安全的商业模式上来考虑问题，不是单纯的技术能解决的。

第三是销售陷阱。销售陷阱的本质是生存与发展，在找了很多销售大牛来加盟后，我发现销售的目标是完成业绩，不会有创业者的前瞻性和理想，会带偏公司的发展，无异于饮鸩解渴。销售陷阱涉及的是人性，事实上是最难跨越的陷阱。

第四是资本陷阱。资本是顺水推舟的放大器，如果业务非常稳定，框架、结构好，资本的加持会让企业发展得更好；反之会让企业加速走下坡路。安全行业选择资本一定要慎重，要选择能够长期配合共同发展的资本方，而不是以企业为目标来盈利的资本投资，因为安全行业很难短期盈利，它是长期的一个事业。所以我们选择了腾讯，知道创宇走到今天腾讯的支持功不可没。

网络安全创业的一大特点是爆发性不突出，不同于互联网的各种风口，要靠高投入获得将来的爆发性高产出。相对于其他产业，网络安全的盈利水平较为一般，没有真正的情怀和理想做不了网络安全这个事业。网络安全行业的发展是稳步进行的，如果说互联网创业是冲浪，那么网络安全创业就是爬山，有着清晰的目标，一步一步渐行渐远，只要勤奋、努力、坚持，成功就会越来越近。

知道创宇落地安徽铜陵 凸显未来市县网络安全战略布局

7 月 18 日上午 9 点 18 分，作为铜陵市重点招商引资的高新技术企业，知道创宇当日正式入驻铜陵创新小镇，并举行了一场隆重而又不失简朴的开业庆典，铜陵市政府副市长黄化锋、信息化管理办公室主任胡振南，及市属相关单位领导出席庆典，见证了铜陵知道创宇公司成立和正式开业，北京知道创宇执行副总裁陆海、安徽黄河信息科技有限公司董事长黄河出席开业活动。

黄化锋副市长出席活动致辞时表示，铜陵正处于转型升级、超越发展的关键阶段，铜陵过去一直是工业城市，但是 100 万铜陵人民更期待铜陵的天更蓝、水更清，铜陵这样一个美丽的小城一旦踏上信息化高速发展的列车，一定会迸发出无穷的动力。最后，黄化锋副市长代表市委、市政府对铜陵知道创宇成立和开业表示了热烈的欢迎和祝贺，并对未来市信息化安全建设充满期待。

▲ *铜陵市政府副市长黄化锋发表讲话*

▲ *北京知道创宇执行副总裁陆海发表开业致辞*

陆海在庆典活动致辞时首先代表北京知道创宇创始人兼 CEO 赵伟欢迎各界来宾出席活动见证铜陵知道创宇开业，陆海表示，网络安全已经成为国家重要战略，不管是大到国家、还是小到县市，在当前互联网经济蓬勃发展的大背景下，保障好当地范围内的网络安全不仅有助于国家的安全建设和社会信息化发展，还能够帮助维持社会的稳定，更好地保护人民的生命和财产安全。

陆海强调，知道创宇公司一直以“侠之大者，为国为民”作为企业信条，为国家政府、企业和民众奉献自己的力量，与当地的合作伙伴一起成立铜陵知道创宇，这意味着我们能够将服务于全国其他地区的能力，也能够在铜陵更好地落地。并且，成立铜陵知道创宇，也意味着我们将针对铜陵地区的网络安全建设，提供更多优质、快捷的服务，将服务的本地化做到最优，为铜陵信息化发展提供强力保障。

▲ *北京知道创宇运营总监詹兴豪代表铜陵知道创宇完成战略签约*

在铜陵知道创宇开业庆典上，铜陵知道创宇还与铜陵市公安局网络安全保卫支队、铜陵职业技术学院、铜陵理工学校现场签订了战略合作协议，合作内容包含网络安全赋能落地，及校企联合人才培养等方面，并联合成立了“打击新型网络犯罪实验室”、“网络空间安全实验室”、“网络安全实践基地”。

▲ *铜陵知道创宇开业仪式*

铜陵知道创宇是北京知道创宇信息技术有限公司与安徽黄河信息科技有限公司在铜陵市政府双招双引下成立的信息技术有限公司，铜陵知道创宇将以“知道创宇”在云计算和大数据方面的行业领先能力，提升政府、企业、金融等行业在网络安全监测、预警、防御、溯源及态势感知等方面提供全方位的技术支撑。铜陵知道创宇将始终以专业的技术能力及不断提升的服务质量，为客户提供国际一流的网络安全服务。

喜迁新址 | 知道创宇武汉研发中心入驻腾讯武汉软件研发中心

▲ *创始人兼 CEO 赵伟与大家共享喜悦*

11 月 12 日，知道创宇武汉研发中心迎来了发展历程中的重要时刻，研发中心迁至位于江夏区庙山开发区汤逊湖畔的腾讯武汉软件研发中心。

知道创宇创始人兼 CEO 赵伟、EVP 陆海、SVP 汤周华、VP 陶晨锐等总裁办高层管理团队悉数来到武汉，共同启动了知道创宇武汉研发中心乔迁仪式，与知道创宇武汉研发中心的各位同事一起分享了乔迁新楼的喜悦。

腾讯武汉软件研发中心是腾讯在华中最大的研发中心和人才基地，位于江夏庙山开发区，占地面积 80 亩，总建筑面积 70000 多平方米。

腾讯武汉软件研发中心是腾讯为有效聚集移动互联网产业人才、技术、资本等创新要素，吸引相关产业集聚而建立的一个以移动互联产业为主导的创谷，也是一个集生产、生活、生态融合发展的综合部创新创业活力社区。

作为腾讯战略投资的高新技术网络安全企业，知道创宇得到了腾讯在资金、人才、资源等多个方面提供的有力的支持。本次知道创宇武汉研发中心能够入驻腾讯武汉软件研发中心，也再次得到了腾讯提供的优渥条件和大力支持。

在乔迁仪式上赵伟表示，自武汉研发中心成立以来，武汉研发团队不断取得优异的成绩，团队规模也不断扩大，吸收了大量优秀人才。今天， 武汉研发中心搬迁至腾讯武汉软件研发中心，办公环境将得到大幅改善，希望大家能够将这里当做一个全新的起点，开创更辉煌的成绩，祝大家工作顺遂，生活开心。

在入驻腾讯武汉软件研发中心后，知道创宇武汉研发中心将会继续深耕网络安全领域，立足网络空间对抗一线，为客户提供最专业的产品和快速响应服务，为各位伙伴提供最专业的安全保障。

知道创宇党支部荣获 2017 年度先进党组织

2018 年 6 月 29 日下午，中共首都互联网协会委员会 2017 年度表彰会举办。会上，对在 2017 年度首都互联网党建工作中涌现出的先进集体、优秀个人和党建创新品牌进行了隆重表彰。知道创宇党支部荣获 2017 年度先进党支部，党支部书记毕宁被评选为 2017 年度优秀党组织书记。

2017 年，知道创宇党支部在上级党委的正确领导下，坚持围绕中心工作抓党建，抓好党建促发展的工作思路，紧密联系实际，持续深入开展支部建设活动，扎实推进党组织建设，不断转变思想观念，完善工作思路，充分发挥党组织战斗堡垒作用，进一步提升基层党组织凝聚力、战斗力。

一、深入学习贯彻党的十九大精神

知道创宇党支部高度重视党员的理想信念教育，将其作为深入贯彻落实习近平新时代中国特色社会主义思想和党的十九大精神、推进“两学一做”学习教育常态化制度化的重要抓手。开展观看十九大开幕式、“学习新党章，践行十九大”、“紧跟时代脉搏，持续学习和贯彻十九大精神”主题学习活动 3 次。建立支部书记讲党课 2 次，认真学习《中国共产党第十九次全国代表大会报告》、《中国共产党章程》学习体系。全体党员手抄党章 19 份，深刻领会、学习十九大报告精神和习近平新时代中国特色社会主义思想的精神实质和丰富内涵。

二、夯实基础，强化基层组织建设

知道创宇党支部根据协会党委要求，严格按党内相关规定和流程开展换届选举工作、民主评议党员工作。支部书记统筹支部常规工作，定期召开支委会议 12 次，总结布置党建工作、通报党建工问题、商讨党员反映的难点问题及解决处理的办法和措施。建设党员活动室 1 间，设立党员示范岗 19 个，充实党员读物 20 余册，按时订阅党报党刊 4 类。

三、健全管理制度，规范支部运作

依照协会党委编印的《党支部工作手册》和《党支部规范》，以“一规一表一册一网”规范化建设为目标，认真贯彻落实。

1、健全完善制度。支部制定完善各项组织制度，坚持“三会一课”、组织生活、民主评议、主题党日等制度，定期开展支部活动。重新制定《党员管理条例（试行）》制度。党支部书记对支部党员开展谈心谈话 2 次，做到“了解、交流、批评、整改”四步走。

2、制定党员考评体系，做好党员纳新、转正工作，按时转正党员 2 名。

3、支部制定主题党日活动方案、“学习贯彻十九大精神”主题教育方案，结合重大节日、纪念日和重要事件节点开展活动，支委会决定每月 21 日为支部的党日活动时间。

4、规范台账管理。明确支部台账管理责任人，责任人负责党员、积极分子和申请人材料的统计、分类、整理、归档，分别建立电子台账和纸质台账，并做到及时更新。

四、开展支部精品活动、举办主题党日活动

知道创宇党支部开展主题党日活动 6 次，结合公司反欺诈业务，打造党建创新品牌，深入翠微南里社区，开展了一场防范电信网络诈骗宣传活动，向社区居民发放了《防骗秘籍》200 余册。 党的 96 周岁生日到来之际，开展“追寻英雄足迹，传承英雄精神”的狼牙山五勇士纪念馆参观活动。为纪念中国人民解放军 90 周年华诞，开展了“普及射击技能，增强国防意识”主题爱国主义教育活动，组织观影活动 2 次。教育引导党员时刻铭记党员身份，履行党员义务，不断增强党性意识，躬身力行做好表率。

知道创宇一直以来以国家利益为先，由党员带队，多次在战胜利 70 周年、国家两会、G20 峰会、世界互联网大会（乌镇峰会）、国家网络安全宣传周等等国家重大会议、活动义务提供安全保障，由知道创宇提供应急保障的工作部分，均以零被黑、零事故顺利完成保障工作。在接下来的工作中，知道创宇党支部定会在习近平网络强国战略思想的指导下，发挥党员先进带头作用，带领全体员工，为国为民做出自己的贡献。

领军云防御

知道创宇云安全防御平台首批获得国际顶级云安全认证

6 月 25 日，在公安部网络安全保卫局的指导下，由公安部第三研究所主办的网络安全标准论坛（暨云计算安全与通用评估标准培训会）在北京召开。在本次大会上，知道创宇云安全防御平台同时将公安部第三研究所安全防范与信息安全产品及系统检验室验室颁发的云计算产品信息安全认证证书（SaaS 增强级认证），以及全球顶级认证 CSA CSTR 云安全标准认证收入囊中，成为首批同时通过“双标认证”的云防御安全厂商之一。

此次国内只有四家一线网络安全企业获得了“双标认证”，也可以看得出该标准的要求严格程度是极高的。据介绍，该“双标认证”是一种综合了安全专用产品销售许可和网络安全等级保护优势的测评，其不仅考虑了产品提供的安全能力，也能保证在线系统自身的安全性，在全球云防御大势所驱的大背景下，认证充分体现了知道创宇云安全防御平台的极高可靠性。

云等保测评 2.0 和云计算安全相关政策最近频繁被宣讲和阐述，也体现了云防御在未来的安全价值。从解读上讲，以前的传统的认证，都是偏重于针对软件和硬件形态产品，对于新兴的服务形态的产品，比如云安全平台则没有针对认证，公安三所此次联合国家权威安全认证机构，将彻底解决云防御之前遭遇的尴尬处境问题

出席会议的知道创宇相关负责人表示，知道创宇从 2011 年开始着手建设云安全防御平台，在过去数年时间内，保障用户总量已近百万，并且在保障周期内无一用户被黑，平台具有极高的安全价值，作为首批双标云计算产品信息安全认证的安全厂商之一，知道创宇将继续提升安全能力，并努力丰富细化产品矩阵，持续输出安全、高速、稳定的云安全服务能力。为中国云安全、云防御领域的发展进一步贡献力量。

群雄逐鹿时代，百万级用户的云防御打造

“光顾着埋头苦干，真的没有发现我们已经取得了这样的成绩。”5 月 24 日，在腾讯云 + 网络安全专场的演讲台上，知道创宇创始人、CEO 赵伟指着第三方行业报告统计的云防御市场占有率排名说道。根据数据显示，知道创宇在互联网金融、政府网站两端的云防御市场上，分别以 49.77%、42.18% 占有率均高居榜首。

当天，知道创宇创始人、CEO 赵伟带来《群雄逐鹿时代，百万级用户的云防御打造》主题演讲，在演讲过程中他对知道创宇完整的云防御体系做了全面的讲解，并就云防御厂商和公有云之间的关系，以及目前安全市场局面提出了自己的见解，同时还道出了云防御未来的发展之路。

赵伟表示，知道创宇成立 10 余年间一方面在取得了不俗的成就同时，也在不断思考如何迎合用户更为细化的需求。基于此，知道创宇云防御平台历经三次进化。第一次进化，即 2011 年加速乐产品的推出；第二次进化，则是 2015 年创宇盾、抗 D 保产品融入云防御平台；第三次进化，知道创宇推出云防御 2.0，推出了大量的针对业务安全的服务和产品。

“第一阶段，我们切入点以加速和安全为主。”赵伟表示，当知道创宇在云还没有广泛发展和应用时，以云防御切入时最先做的是解决当时用户最大的痛点，就是加速，而这一迎合用户细化需求的做法也在市场上收获了巨大的成功。但是他也感慨当时用户对安全还没有明显强烈的需求，总是把安全放到最后。而在市场表示出强烈的安全需求时，创宇盾、抗 D 保相继的推出，又使平台得到了一个高速的增长。

产品同用户刚需紧密结合，这是知道创宇云防御平台发展上的典型特征。赵伟认为，现阶段，用户的刚需则是以客户为中心的量身安全服务，用赵伟的话就是“为用户量身定制盔甲”。知道创宇云防御平台也在前不久迎来重大升级，云安全 2.0 重磅推出，围绕着客户在线业务安全的数款产品和服务已经上线，知道创宇也再次迎来了高速的市场增长。

如何细化用户需求？赵伟表示，知道创宇云防御平台深入了解了客户企业的初创期、成长期、稳定期，分析了客户的每一步的具体需求，围绕需求在时代不断演变的同时做出了及时的应变，并且充分拓展外部资源，比如与腾讯之间的合作，依托于双方的安全大数据，打造出了全方面的安全服务体系。

在谈到云防御厂商与公有云之间的关系时赵伟表示，两者之间并不是竞争关系，而是一种垂直的生态，是共同发展、共同成长的关系。赵伟发现，公有云已越加要第三方安全云来保证它的生态安全，又以腾讯云来说，也一直是知道创宇最为重要的合作伙伴，也在为知道创宇的安全产品提供着更强的“动量”，相互已形成反哺关系。

赵伟表示，安全产业潜在市场份额一直虚高，他并不认同朋友口中国内能达到 600 亿左右的市场规模，而在市场规模有限的现状下，赵伟更希望能看到大家联合起来，共同做大市场，把产品和客户服务做大，而不是相互恶意竞争。

在谈到云防御未来发展时赵伟表示，知道创宇在成功打造服务百万级客户的云防御平台之后，其实平台正在走向一个完整的生态系统。“大家可以看到知道创宇云安全官方网站，我们已经有上线合作伙伴的产品，我们也希望跟更多的友商合作，联合打造更全面的云防御安全生态。”

“云鼎奖”花落知道创宇 国内首家云安全企业获行业高度认同

5 月 10 日，第六届全球云计算大会·中国上海站迎来第二天议程，同时当天还有另外一项大会的核心活动尤为引人关注，那就是一年一届的“云鼎奖”（Top Cloud Connect Awards）颁奖盛典活动。当天下午，大奖在层层评选之下终于花落，知道创宇揽获“云鼎奖”2017-2018 年度中国领先品牌奖。

“云鼎奖”自 2014 年设立以来，已成功举办四届，共有 500 余家企业申请过该奖项。“云鼎奖”旨在表彰年度对中国云计算产业做出突出贡献和具有创新精神的集体、个人和产品，进而促进云计算在中国健康、快速、有序发展，并助推中国企业走向世界舞台。换言之，能够荣获此奖，也是对知道创宇的高度认可。

主办单位认为，知道创宇作为国内首家利用云计算技术来保障云安全的网络安全企业，当用户还在考量业务上云所带来的安全性问题时，知道创宇就已提供了一整套成熟而且便利的安全解决方案，这种全面的安全支撑，对国内云计算产业的发展也起到了助推作用。

同时，知道创宇云安全在历时近十年的发展中，一直处于国内云防御市场引领者地位，也带动了云防御市场的高速增长，而对云本身发展的贡献也早已转换为企业知名度，高达 90 余万网站用户选择知道创宇云防御，也是对知道创宇品牌本身的高度认可。

知道创宇在国内缔造了云安全的商业模式，如今利用云技术实现网络安全保障已成为最为流行的安全部署方式，不仅新兴的安全企业跟随着知道创宇的步伐进入云安全市场，甚至一些传统网络安全企业也在改变自身的商业模式，新增云安全业务。其中甚至不乏完全的商业模式抄袭者。

而知道创宇云安全正以多年积攒的技术优势、不断投入的资源优势、应对不同安全需求的产品优势，以及对高风险网络安全的极限保障，越来越被政府单位、商业企业所认同，服务网站用户量高达 90 余万，具相关的市场调研显示，知道创宇云防御市场占有率第一。

年初，知道创宇还宣布加大了对海外云防御节点的部署，这也意味着未来知道创宇不仅能保障客户在国内市场的安全需求，如果客户要开展全球化业务，拓展海外市场，知道创宇同样能提供相应的安全保障，这一点上也与“云鼎奖”评选标准助推中国企业走向世界舞台高度契合。

一个全新时代的开启，必须解决时代高速变革所带来的种种安全难题。作为引领者，全新的知道创宇云安全 2.0 于 5 月份上线，平台深度融合了旗下 4 条产品线包括 14 个安全产品及服务，除了集成创宇盾、抗 D 保等明星产品，还新增了诸如业务反欺诈产品——羊毛盾、企业征信查询产品——企信查等业务安全领域的产品，以及企业安全验证、SSL 证书等商业安全领域的产品，也提供渗透测试、代码审计、应急响应、威胁速报等细分需求下的安全服务，同时还发布了综合行业解决方案。

2018 开年以来，知道创宇持续受到外界关注和认同，此次将“云鼎奖”核心奖项收入囊中，这也督促着知道创宇在未来自身发展的同时，对国家网络安全、及行业发展的提升做出更多的贡献。

安全保障

知道创宇圆满完成两会网络安全保障工作

第十三届全国人民代表大会第一次会议、全国政协第十三届一次会议（以下简称两会）在圆满完成各项议程后，分别于 3 月 20 日、3 月 15 日在北京胜利闭幕。作为保障两会网络稳定安全运行的核心力量，知道创宇圆满完成了会议期间国内重要网站的网络安全保障工作。知道创宇云防御明星级防入侵产品“创宇盾”再次交上了一幅完美答卷，防护期间由“创宇盾”所防护的网站，无一例被黑事件发生。

免费开放 政府网站接入创宇盾

为全方位保障各级政府网站安全稳定运行，知道创宇于会前推出免费安全保障服务。两会期间凡政府网站均可申请安全保障，免费接入创宇盾进行最高级别的安全防护。秉承“侠之大者，为国为民”的企业信条，知道创宇已多次为国家网络安全贡献自身力量，帮助各级党政机关网站有效避免网站被黑客入侵，网页被篡改、信息被窃取，网站无法访问等情况发生。

会前备战 严阵以待迎接两会

与此同时，知道创宇云防御平台组织召开两会安全保障会议，随即成立多个保障小组，要求调动最优资源、以最高的安全标准进入两会重保时间。并依据各级政府网站的安全需求，制定专属防护策略，为各级网站提供军工级安全防护，坚决完成两会网络安全保障工作。

零被黑零事故 圆满完成保障

据知道创宇云防御检测平台数据显示，重保期间，创宇盾共为接入防护的各级政府网站、国家重要信息系统抵御 23.3 亿次攻击，保障小组在两会期间 7*24 小时不间断为各地政府网站提供支撑上千次，由创宇盾防护的网站

无一例被黑事件发生。同时，创宇盾大数据平台利用云防御全网感知，协同防御的机制，为客户动态优化防护策略 25.8 万次，创宇监控共发送近百万次预警，通过创宇监控观测创宇盾防护网站可用性超过 98.8%。

两会期间，创宇盾网站安全舆情监测平台发现并预警数百起政府网站被入侵，被篡改事件。针对上述安全事件，知道创宇安全应急响应团队已在第一时间配合各地监管部门将安全威胁全部杜绝。

安全保障需要主动防御未攻击

“安全保障不是说发生了攻击我们再去揪出骇客，修复网站，而是要在对方发起攻击前就检测到痕迹并斩断它。”在两会胜利闭幕后，一名参与应急响应的安全专家这样表示。传统的被动防御技术无法对未知攻击进行有效检测，而两会等重保期间容易造成网络安全事故的，恰恰是网络空间中各种未知的、潜在的威胁。创宇盾通过汇集知道安全大数据分析平台和安全舆情检测平台，能主动、实时追踪整体态势，动态调整防护策略，及时响应安全事件，并独创站锁功能，为各级网站提供多维度的整站防护，保障万无一失。

没有网络安全 就没有国家安全

历年来，知道创宇多次参与到国家重大会议、活动的网络安全保障工作中，为国家级活动提供坚实防护，收获数次致谢肯定。这一次，创宇盾再以“零被黑、零事故”的优异成绩抵御全部攻击，完满完成防护，再次证明了其防御能力的扎实可靠。没有网络安全就没有国家安全，知道创宇将继续肩负起网络安全企业的责任，深耕于浩瀚的网络空间，为建设网络强国奉献力量。

知道创宇云防御产品创宇盾强势保障“强网杯”挑战赛成功举办

创宇盾

第二届“强网杯”全国网络安全挑战赛于 3 月 24 日、25 日举行。据了解，本次赛事堪称“国赛”标准，一方面赛事由中央网信办指导，并且线上赛报名战队高达 2622 余支，报名参赛人数更是高达 13250 人，均达到国内相关赛事新高。

为保障大赛顺利举办，“强网杯”赛事支持平台 i 春秋学院引入了全面的安全保障，一方面引入反作弊系统，同时赛事平台更是全面接入知道创宇云安全平台，由云防御明星级产品创宇盾负责提供网络安全支撑，以保障不受外界攻击干扰。

制定专属策略
创宇盾轻松应对赛事平台初期流量攻击

24 日上午 9 时，本次赛事正式打响，并不出乎意料的是，外界对赛事平台的攻击也随之而来。据知道创宇云安全平台创宇盾产品的实时监控数据获悉，当天上午，黑客调用了 3000 余台肉鸡资源，对赛事平台共计发起了百万次 CC 攻击，希望借以瘫痪平台响应，造成比赛中断。

为保障赛事顺利进行，创宇盾在触发原有拦截机制有效防护赛事平台稳定使用的同时，另一方面积极沟通赛事保障技术人员，进一步制定专属防御策略，并提供了相应的攻击数据，以便赛事保障人员以赛事需要、并保障赛事平台稳定使用的前提下，进一步开展具有针对性的安全防护。

“本次保障的 CC 攻击量级远远没有达到知道创宇的防御上限，本身其实无需人工干预即可以由系统完成自主防御，但考虑赛事环境的复杂性，我们还是进一步沟通制定了专属的防御策略，以便做到 100% 的安全防御。”知道创宇云安全相关保障负责人表示。

创宇盾严密监视防护
警惕暗度陈仓保障平台及数据安全

借助于创宇盾产品有效的防御，以及 i 春秋多年来举办网络安全竞赛的安防经验，很快黑客便意识到了攻击的无效。但黑客并未彻底放弃攻击，当天至 25 日晚间，CC 攻击仍保持着一定的量级。此时，技术人员在原有流量攻击防御的基础上，开始更加关注可能伴随着的漏扫入侵。

“网络安全需要提供多样化的防御方案及策略，知道创宇云安全平台就是依托于此为客户提供的 100% 安全保障，而不断受到客户信赖。鉴于流量攻击并不是不断飙升，云安全保障团队即刻开始着重分析是否存在漏扫渗透攻击，以便及时做出防范。” 知道创宇云安全相关保障负责人表示。

一方面，创宇盾开始发挥着其重要的看家本领，为赛事平台提供了军工级的防入侵服务，对攻击扫描行为实时拦截。汇集了 30 余万黑客攻击指纹并且具有不断自我学习能力的创宇盾，轻松应对了本次可能出现的入侵攻击；另一方面，云安全保障团队积极联手赛事保障团队，进一步分析加固了平台自身安全性，以便彻底杜绝黑客入侵的可能性。

创宇盾过往保障无一被黑
人性化防护安全体验不断提升

知道创宇明星级云防御产品创宇盾自 2015 年发布以来，多次为国家重大会议、活动，以及重要政府网站、商业网站提供安全防护，在过往的服务防护期内，无一例被黑事件发生，坚决保障和捍卫了国家网络安全，以及民间商业企业的信息安全，也因此多次受到相关部门、单位的一致好评和致谢。

“创宇盾产品本身具有自主防御能力，完全不需要人工干预，但是我们从产品发布之日起，就不断加大自身保障团队的建设，如本次‘强网杯’赛事的保障工作，除了创宇盾的自主防御，我们还大量投入了人工参与的保障工作，这有助于细致化安全需要的同时还能进一步提升安全体验。” 知道创宇云安全相关保障负责人表示。

知道创宇为上合峰会成功举办贡献安全力量

6 月 9 日 -10 日，上海合作组织成员国元首理事会第十八次会议在中国青岛举行。作为上合组织扩员后召开的首次峰会，青岛峰会具有承前启后的重要意义。为保障会议顺利有序进行，应上级部门安排，知道创宇作为网络安全支撑单位之一参与到本次盛会的网络安全保障工作当中，为大会顺利举办贡献了力量。

相关单位高度重视本次盛会网络安全保障工作，在会议前期，知道创宇即全面参与到“齐鲁护网行动 2018”当中，作为会议前期集中安排的网络安全专项攻防演练活动，知道创宇三次参与其中，派出强大技术团队，并在活动之后多次荣获“突出贡献奖”。另外知道创宇还多次参与到了地市一级的攻防演练活动，夯实了网络安全底层防御能力。

在会议举办期间，知道创宇则作为现场技术支撑团队之一保障会议网络安全，利用创宇雷达、WebSOC 等安全产品实时监控会议期间网络环境安全，二款安全产品可对新接入网络的设备、资产进行安全检测，防范之万一。同时知道创宇还参与了会议网络安全态势感知技术平台保障工作，提供重要数据支撑网络安全。

与此同时，知道创宇云安全防御平台在会议举办前后进入 24H 值守保障，抽调各技术小组核心成员成立保障工作组，对接入平台的华东地区政府网站执行重点防御，创宇盾、抗 D 保等产品以最优资源为千余政府网站提供 100% 安全保障服务，值守期间，由知道创宇提供防御的政府网站无一例被黑事件发生。

“侠之大者，为国为民”是知道创宇的企业信条，知道创宇公司成立已来，多次为国家网络安全贡献自身之力，为网民上网安全保驾护航。在国家级重大会议活动的网络安全保障支撑方面，抗战胜利 70 周年、国家两会、G20 峰会、世界互联网大会（乌镇峰会）、国家网络安全宣传周等，都可以看到创宇人在背后提供网络安全保障的身影。

在过去历届国家级盛会、活动中，所有由知道创宇提供应急保障的工作部分、以及利用创宇盾提供安全防御的政府网站，均以零被黑、零事故顺利完成保障工作，未来，我们同样有能力也有信心再次肩负重责。

产品动态

全新突破 ZoomEye 2018 强势发布

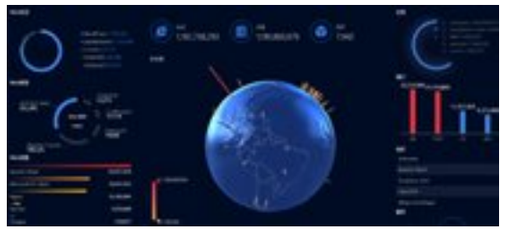
2013 年，知道创宇基于互联网大数据基础测绘的理念，打造了“ZoomEye”（钟馗之眼）网络空间安全搜索引擎，针对全球网络空间基础设施、网络设备进行指纹特征检索，开创了国内网络空间资源测绘工作的先河。

自发布以来，ZoomEye 形成并不断丰富全球网络空间的互联网基础态势，构建了互联网安全基础态势测绘底图。无论是“心脏出血”漏洞的全球摸查，还是近年来不断涌现的物联网安全威胁，ZoomEye 一直以洞悉的视角输出强大的全面的安防能力，帮助及时了解漏洞爆发全球影响面，黑产作恶的动向，以及如何对应开展互联网漏洞安全应急响应工作等。

事实上，基于 ZoomEye 的能力，在国家有关部门指导下，知道创宇已进行了百余次重大漏洞爆发时的资产检查、应急处置、安全保障、网络空间安全应急响应等工作，为我国网络疆域的安全防护做出了重要贡献，得到高度评价。

作为中国第一大网络空间安全搜索引擎，同时也是全球著名的两大网络空间安全搜索引擎之一，ZoomEye 一直在不断进化，在经过开发以及优化调整之后，全新的 ZoomEye 2018 于 2018 年 10 月正式上线！

ZoomEye 2018 在视觉交互、内容呈现、数据探索及商务功能上均带来重大突破。首先不管是搜索时新增可选的热门 Dork 还是搜索结果中数据类型的集成汇总，都让使用 ZoomEye 更加方便友好，新增的移动端适配让更是让探索 ZoomEye 不再受限。其次，搜索单页面中新增的统计报告、全球视角、相关漏洞标签页以及分词、Dork 贡献及下载功能，使得网络空间资产的数据信息呈现更加清晰、丰富和具象化。再者，探索功能中加入了多维度的数据统计和开放组件，以及新增了贡献榜单功能，动手探索便可以汲取 ZoomEye 更强大更优异的能力，获得 ZoomEye 海量的归类的网络空间数据。最后，商务方面新增的掘金计划和充值服务让 ZoomEye 以满足不同用户多样化的个性需求。



如今，基于 ZoomEye 强大的网络空间测绘能力，并进一步结合知道创宇不断积累的海量安全大数据，以及 Seebug 漏洞社区的运营，探测全球互联网空间上的节点分布情况和网络关系索引正愈加完善全面。随着 ZoomEye 2018 更加强大的功能上线，以及更加开放的合作心态，知道创宇将继续走在不断致力于维护国家网络安全的道路上，协助有效应对网络空间各领域里的现实威胁，维护国家网络安全，保障国家壮大发展。

“暗网雷达”出世：破深网暗尘 知山鬼暗啼

在网络空间更深层的地方，有一处阴暗且鲜为人知的阴暗区域，它匿名，隐蔽，搜索引擎无法搜索，监管机构难以触及，它就是“暗网”。

暗网缔造黑市天堂

▲ *媒体报道安全周知道创宇“暗网专区”相关展示*

这一富含神秘色彩的词汇，随着频频爆发的数据泄露事件和数字货币的火爆逐渐进入大众视野，它总与各种令人胆颤、诡异阴暗的话题相关，是想象中的犯罪份子和霸凌者的领地。今年国家网络安全宣传周期间，知道创宇通过设立暗网专区向民众普及暗网基本知识和危害，受到大量公众与媒体的广泛关注。总体来说，暗网在目前仍然是一个未被探索且鲜有人理解的世界，现实也只有极少部分人越过这条界，深入网络空间的幽深之处。

暗网统称只能用特殊软件、特殊授权、或对计算机做特殊设置才能连上的网络，使用一般的浏览器和搜索引擎找不到暗网的内容，例如 Tor、I2P 等。正是由于高度匿名、虚拟的特性，在没有法律和舆论的监视下，暗网成为了网络上的黑市，它明码标价着各种犯罪服务，各色人种在上

▲ *知道创宇在“天府杯”态势感知论坛分享暗网研究*

面从事着各种非法的交易，没有限制的信息泄露和欺诈充斥其中。而且，暗网也被用于传递政治、经济等敏感信息和实施网络攻击，甚至是危害国家安全的犯罪，这些风险一直在威胁着社会、企业和国家的安全。

暗网监测急需解决

针对暗网空间中的数据信息，如何索引与检测，是一个值得不断思考与探索的问题，全球执法机构也在尽力捣毁各类危害巨大的暗网服务。2017 年 7 月，美国和欧洲多个执法部门联手，关闭了暗网上以毒品交易为主的最大黑市网站 AlphaBay；另外荷兰警方同期在暗网上另一个主要毒品交易网站 Hansa 钓鱼执法，成功锁定一批嫌疑人

建立暗网空间搜索引擎，完成对暗网入口、链接、内容检测采集，并尝试对暗网进行主动嗅探，对暗网交易数据进行跟踪，以及对暗网网络结构及数据资源进行合理掌握，让网络监管机构获取知己知彼的能力，变得非常重要。

▲ *暗网雷达正式发布*

暗网雷达洞悉黑暗空间

知道创宇作为国内最早进行网络空间测绘的安全企业，五年前，发布了 ZoomEye 网络空间搜索引擎，持续进行着对明网（表层网络）的测绘、侦测工作。在今天（11 月 17 日）召开的“天府杯”网络空间态势论坛上，知道创宇正式对外发布“暗网雷达”，将对于网络空间的探测分析能力纵深到更神秘的暗网空间。

这是一款面向暗网的情报监测系统，以威胁情报线索挖掘为导向，通过构建分布式暗网节点监控、服务发现、内容采集、弱点探测、智能监测、情报研判、证据保存等平台，提供暗网服务的发现、识别、分类、采集、监测功能，旨在为相关业务人员提供高效的情报监测和分析服务。

暗网雷达覆盖了暗网的 Tor、I2P、ZeroNet（零网），收录其中的设备、内容、机器使用服务、组件等信息，通过强大的暗网节点接入能力，及独创的暗网引擎爬虫技术，实现全暗网的信息采集及监测。

根据持续的扫描监测，暗网雷达目前已收录 Tor 服务地址超过 12 万个，峰值总量约 13 万，截止目前存活服务 1 万余个，I2P 地址超过 1000 个，零网 P2P 网络超 1700 个。已发现 53 种语言的暗网网站，其中中文网站 641 个，内容集中在违法交易，政治谣言，色情暴力等，英语网站 2 万余个，俄语、阿拉伯语网站也不在少数。这些网站主要涉及黑市交易、政治宗教和匿名通讯，此外有大量的比特币地址和 Email 地址收录其中。

就在今年中旬，知道创宇也对外发布了《2018 上半年暗网研究报告》，从暗网雷达的实时监测数据来看，暗网还在呈现缓慢增长的态势，随着暗网用户的增多，黑市及加密数字货币的发展，更多的恶意黑客在利益的的驱动下开展各种活动，把之前通过表层网传播的非法交易更多的转移至暗网，通过各种技术手段躲避追踪监管，对取证调查带来更大的挑战。

面对日益增长的暗网威胁，知道创宇将会持续通过技术手段来测绘暗网，挖掘威胁情报，追踪和对抗来自暗网的威胁，尽力帮助相关执法机构挖掘潜伏的网络犯罪，并连同 ZoomEye 2018 更强大的测绘能力和安全大数据，持续构建更安全的网络空间。

知道创宇推出国内首个 IPv4/IPv6 双栈云防御服务

11 月 20 日，知道创宇正式对外发布国内首个 IPv4/IPv6 双栈云防御服务。该服务的推出可以帮助企业极大的加快业务系统向 IPv6 升级的进程，从 IPv4 向 IPv6 的改造方案到 IPv6 业务系统安全防御上向企业提供了一站式的解决方案。

知道创宇云防御产品经理邓金城对此介绍，IPv4/IPv6 双栈云防御服务只需要 2 分钟即可帮助客户做到业务系统支持 IPv6 并且可以有效防御黑客入侵、DDoS 网络攻击，整个过程不需要客户业务系统做任何改造。

2017 年 11 月 26 日，中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》，根据该计划要求，到 2018 年末，国内 IPv6 活跃用户数要达到 2 亿，国内用户量排名前 50 的商业网站及应用户、省部级以上政府和中央企业外网系统、IDC 数据中心等均要完成 IPv6 支持。据阿里巴巴发布的公告，今年双 11，天猫进行了国内首次 IPv6 大规模商用实战，IPv6 在国内的普及势在必行。

而对企事业单位来说，各种系统往往承载着重要业务数据，系统改造升级慎之又慎，往往因为担心影响业务稳定而放弃升级，这还包括即使支持了 IPv6 但原有防火墙设备不支持 IP v6，网站无疑陷入巨大安全风险中。然而国内的 IPv6 升级已经正式大规模开展，如何抢先一步，而不是 IPv4 用户向 IPv6 升级后，网站客户流失，成为一个两难的问题。知道创宇 IPv4/IPv6 双栈云防御服务的推出刚好可以解决这个燃眉之急。

海外 CN2 专线防护 助力业务无忧出海

随着一带一路建设的推进和互联网的不断发展，越来越多的中国企业开始走出国门，国内对海外 IDC 服务的需求正在日益增加。但是，海外 Web 系统却时常面临着访问速度慢、稳定性差、易遭受攻击等多重困扰。

据相关业内人士反映，由于地理因素，国内访问海外服务器需要经过多个路由节点，网络高延迟导致访问速度变慢，用户体验度变差，致使客户大量流失。在国内访问海外服务器时，经常出现瞬断现象或者访问量过多、带宽不足造成线路拥堵，稳定性变弱，影响业务正常进行。同时，国内与海外服务器的访问过程中容易遭受到恶意攻击和恶意入侵行为，大量消耗服务器资源以及泄露敏感信息，影响系统正常运作。

复杂的海外网络运用需求，催生了互联网第二平面——CN2 的落地。CN2 是相关网络运营商的下一代多业务的承载网，主要用于海外地区，采用 IP/MPLS 核心技术，海底光缆直连大陆，省去了跳转国际网络的延迟，具有高弹性，高冗余性和低延迟的特性，属于专线通道，速度更快更稳定。

长期为国内互联网企业提供云防御服务的安全厂商知道创宇通过与 China Telecom Global 等大陆运营商广泛合作，早在 2013 年便在中国香港部署了数据中心，开启国际化战略布局后后于中国台湾、新加坡、韩国、日本等多地部署了多个大型 CN2 数据中心。目前已拥有多条海外 CN2 专线直连中国大陆，其 PING 值低至 30ms，几乎等同于国内服务器的访问速度。

据了解，海外 CN2 线路在 IP 层，实现平均小于 500ms 的快速路由收敛；在 MPLS 层，核心节点之间 50 条链路部署了 FRR，实现 50ms 的保护切换。知道创宇在国内 PING 值低至 30ms，欧美 PING 值约为 100~200ms 之间，极大缩短网络访问延迟。网络结构完善，因此传输速度更快。

CN2 承载的是网络运营商具有 QoS 保证的 SLA 业务，可同时支持语音、数据、视频、专线、国际互联等多业务，知道创宇提供 CN2 带宽升级服务，保障充足的带宽资源，满足多业务的需求。并且，若 CN2 线路遭受到 DDoS 攻击时，知道创宇将会临时调 Anycast 进行抗 D，完美防御 SYN Flood、ACK Flood、ICMP Flood、UDP Flood、NTP Flood 、SSDP Flood、DNS Flood、HTTP Flood、CC（ChallengeCollapsar）攻击，确保线路连接正常。

通过 CN2 线路接入知道创宇云防御平台的抗 D 保、创宇盾和加速乐等安全产品和服务，将保障业务快速稳定并且安全无忧，特别对于国际性贸易在中国大陆的业务开展有无与伦比的优势。

近十年以来，创新型的品牌在世界范围的影响力日渐深远，多数企业开放海外业务，参与全球范围的市场竞争。在这个过程中， IT 架构和业务需要应对越来越大的业务需求。基于服务响应速度、节点布局、安全实力、跨域网络以及丰富的解决方案等整体资源和技术实力，走出国门的中资企业和海外企业在拓展全球业务时更需要优质云服务来添足马力。

知道创宇推出资产风险管理解决方案 风险态势全面感知

长期以来，企业在资产管理方面都存在着梳理资产困难、资产评级不明、资产风险不明等难题，寻求一种高效健全的资产风险管理解决方案是行业亟待解决的难题。

面对传统安全管理平台无法解决的安全状况不详、安全问题不明、紧急漏洞应急响应困难，安全工作无法跟踪等问题，知道创宇针对企业资产的风险脆弱性，基于 PDCA 提出完整的资产风险管理解决方案（ScanV-VM）。从发现问题、分析问题、解决问题等角度入手，层层递进，实现管理闭环，协助安全管理，辅助安全决策。

方案介绍

知道创宇资产风险管理解决方案（ScanV-VM）) 针对脆弱性风险管理提出完整方案，实现了资产风险发现与监控、内部资产管理、1 day 漏洞快速响应。方案提供风险管理的全过程支撑，安全工作进度全程跟踪监督，应急响应机制完善。

资产风险管理闭环

ScanV-VM 中利用内置资产扫描引擎实现资产梳理，获取资产信息。并基于时间维度持续监控资产变化情况，以便运维人员及时应对资产环境变化。

通过部署扫描设备，主动检测资产存在的漏洞风险，辅以人工参与，发现漏洞、验证漏洞、修复漏洞、漏洞复查，实现漏洞全生命周期管理，实现漏洞闭环。

1 day 漏洞快速响应

ScanV-VM 针对刚刚爆发的新型漏洞提供快速通报预警功能，通过微信、短信、邮件等多种方式通知用户，并利用内置 POC 脚本实现快速检测，及时应对新型威胁。

安全状况综合可视

ScanV-VM 内置关联引擎，将各级数据做关联统计处理，最终呈现多维度的安全态势展示图表。平台从漏洞、资产等相关数据的产生、处理和可视化展示，将多个视图整合在仪表盘中，突出显示和筛选数据，展现关系，突破视野的局限性，方便决策者对业务的发展规划作出科学的决策。

专业服务团队助力安全建设

ScanV 安全技术团队，拥有丰富的安全运维经验，为用户提供周期性和响应式的专家漏洞报告分析服务，降低漏洞验证和管理的成本，提高漏洞修复的效率。协助企业梳理安全现状，提供安全建议，助力企业安全体系建设。

用户收益

漏洞风险持续优化

基于资产的漏洞管理，资产与漏洞关联分析，准确定位漏洞。根据资产权重和漏洞危害来确定安全事件的重要程度。资产漏洞扫描、验证、修复建议一体化处理，形成闭环漏

洞管理流程。漏洞持续减少，风险持续降低，安全态势持续优化。

紧急漏洞快速处置

1day 漏洞及时预警，配合提供快速的响应和深度的检测服务，实时高效的保障企业业务系统的安全。结合漏洞发现，漏洞处理和处理反馈等不同业务需求，形成企业独特的紧急漏洞处理流程，促进应急机制的完善。

工作成果清晰可查

资产信息与漏洞信息结合处理，统计数据大屏展示，安全报告实时导出。工作过程全记录，安全工作成绩清晰可查。

工作进度全面跟踪

安全状态、安全工作全方位记录展示，工作进度、工作结果全面跟踪。多维度数据分析，为安全决策提供强有力的支撑依据。

智能锁安全暗流涌动，小黑盒只是冰山一角…

科技改变生活，如今智能家居时代的来临，智能门锁作为智能家居窗口级的门类和用户追求智能化生活的入门产品，从进入人们视野起就备受欢迎。

我们再也不用带钥匙或者因为忘带钥匙而烦恼，智能门锁可以通过密码、指纹等方法打开。如果不幸密码也被忘记，手机 iPhone 的 iOS 平台或者 android 系统平台还可以对门锁进行远程控制，手机输入指令，门会为你自动打开。

各厂商看准其中的商机，广告频出，宣传方式五花八门，更有多重专利技术加持，为了让消费者了解到自家产品的高效便利和智能使出浑身解数。

然而，2018 年 5 月 26 日，第九届中国（永康）国际门业博览会上的“小黑盒”3 秒破锁事件让人们意识到，以便利性制胜的智能门锁，其安全性却存在很大问题。

普遍认为应用了先进的生物识别技术、对数据进行加密就能保障安全的智能门锁应用，在真正别有用心的歹徒面前不堪一击。

小黑盒只是智能门锁被攻破的方式之一，智能门锁开锁方式的多样性导致其受到攻击的方式也是多种多样，比如通过利用管理 App 的漏洞而对智能锁进行攻击、通过入侵智能门锁网关而实施攻击等。装了智能门锁的门可能在很短的时间内被打开，同时智能门锁中保存的密钥、个人信息等隐私数据也存在泄漏的风险。

不速之客的入侵使得暴露在外面的不仅仅是你家的模样，更是你生活的模样。这才是智能门锁安全问题最令人感到不安的地方。

智能门锁发展迅速，其中的问题不容忽视，急需有人有所作为，为智能门锁用户的建立信心。

目前知道创宇推出针对智能门锁的安全检测服务，从物理终端、管理平台、智能锁供能、传输链路、数据存储、生物识别等方面对智能设备展开安全检测，对安全性检测合格的产品出具权威检验报告。协助智能门锁生产商知晓安全风险所在，针对性整改，提高产品安全技术能力，增加用户信任度，提升品牌的行业竞争力。

一把智能锁被攻破，并不值得我们去过度恐慌，否定这个新兴行业。安全始终都是相对的，全球知名的科技巨头，依然会不时被黑客爆出漏洞。支付宝刚兴起时，质疑声比今天智能锁遇到的质疑更多，但随着阿里巴巴对平台安全的完善和保障，质疑最终烟消云散，支付宝逐渐成为了大家日常生活中必不可少的一环。

智能门锁的健康发展，需要消费者予其信心，国家予其支持，社会予其协助，更需要厂商自己有担当。知道创宇愿与智能门锁厂商一起共同努力，促进行业健康发展，共同守护消费者的人身和财产安全。

创宇信用企业认证：全方位打造安全可信企业形象

过去一年，遭受网络诈骗的用户人均损失超 1.4 万元，比前一年增长五成多，其中钓鱼网站成为主要的诈骗渠道。

最新数据显示，中国市场上的 app 已超过 406 万个，微信月活高达 10.4 亿，QQ 月活突破 8.05 亿，移动设备流量已远超 PC 端流量。

如今，超 80% 的传统企业正跨过 PC 时代，将主营业务进驻平台电商、微信等移动平台。

在移动互联网高速发展的今天，在每一个企业和个体都触网的当下，企业如何把握住移动端的洪荒流量，传递自己的品牌信誉？用户又如何辨别官方与山寨，避免假冒伪劣等网络欺诈？曝光是一切的开始，信用是未来的基石。

为了解决当下“企业获客成本高、用户信任门槛高”的难题，8 月 1 日，知道创宇盛大召开“创宇信用”新产品发布会，映客、花椒、斗鱼三大平台同步直播，宣布全面升级旗下的安全认证产品及服务，为广大企业提供更广阔的流量渠道和更权威的品牌形象，以促成更健全的互联网征信体系。与此同时，创宇信用新官网也在这一天正式上线，登陆官网（xinyong.yunaq.com）还可参与新品优惠活动。

创宇信用企业认证是一个中立、公正、权威的企业信息认证审核服务平台，通过社交工具、浏览器、搜索引擎等近 20 种覆盖全网的网络终端，将企业的品牌信誉传递给 9 亿网民，帮助企业快速提升品牌形象、网站流量和交易转化。为优化中国互联网使用环境，促进共建互联网征信体系而努力，最终实现企业可信、网站可信及商务可信的健康互联网产业。

▲ *创宇信用产品经理王字*

早在 2013 年，为积极响应国家十一五规划互联网征信体系建设号召，知道创宇通过中国电子商务网址安全评估委员会指导的互联网安全标准，建立起第三方认证评级机构，为各互联网企业、安全厂商提供安全认证评级服务，在行业内拥有非常高的知名度和良好的口碑，获得了合作伙伴和用户的高度认可。到如今，知道创宇已经累计为超过 436 万家厂商进行过企业认证，累积传播 10 亿次可信网址与电话信息，已帮助超过 95% 的用户提升网站流量 5 倍，平均降低网站跳出率 36%。此次全新升级的创宇信用，将带来怎样的突破？

以企业为认证主体 八大权威平台展示

创宇信用将原有的网址认证纬度升级为企业认证，以经营内容、运营方信息、行业经营资质、企业网站安全、网站等级为基础建立起独有的动态信用评级数据模型，以细分行业的认证评级深入各垂直行业领域，对企业进行多维度立体信用评级，并将认证结果输出至 QQ 名片、微信企业名片、站长之家、企查查、搜狗浏览器、QQ 浏览器、搜狗搜索、腾讯电脑管家等多家主流平台，为企业提供更多的流量入口，更好地传递信用价值。

▲ *企业微信名片展示*

此次升级新增独有的企业微信名片功能，让用户在微信端就能直接查看到企业的认证展示及相关介绍信息，不仅可帮助用户快速识别企业及网站的真伪，还能让用户对企业有更深层次的了解，在微信生态中更精准触达目标客户，彰显企业实力，提高品牌可信度。

不仅如此，创宇信用认证结果展示平台还同步新增企查查、站长之家以及行业信息查询平台 5118。据悉，企查查是目前国内用户量最大、数据最全的企业信用信息查询平台，企业认证通过后的网址将被企查查收录，帮助提高网站权威。站长之家已覆盖 2000 万站长专业用户，通过企业认证后的安全徽标彰显可信身份，将帮助企业在行业用户中拔得头筹。

至此，创宇信用企业认证数据将广泛应用于各类流量端口及业务场景，累积覆盖超过 91% 的流量入口，最大范围内解决企业与用户之间的互信关系，从而促成交易转化，并有力打击对企业有侵害的网络欺诈、假冒商品、商标侵权等行为，双向保护用户和企业的权益。

联手公安三所 权威鉴证企业信誉

在创宇信用实名认证、行业认证、官网认证的基础上，知道创宇联合国家网络与信息系统安全产品质量监督检验中心（公安部第三研究所，以下简称“公安三所”）在网站安全保障方面做了有益的探索，推出网站安全权威认证，全新优化安全服务，让企业认证服务能够在网络安全保驾护航中发挥不可或缺的作用。

结合知道创宇领先的安全实力，对于用户提交的网站信息，创宇信用权威认证会分别对网站的漏洞与安全风险进行检测，定期提供专业的安全报告，一方面阻止各类网络攻击，另一方面协助预防及处理潜在安全风险，同时还计划增加内容安全检测能力，通过智能内容识别引擎对页面中可能存在的非法敏感信息进行智能检测，有效防止网站被利用，注入不良信息进行传播，损害企业自身形象以及面临法律法规的风险

公安三所对此表示，中国 526 万个互联网网站是企业面对用户的“桥梁”，每年大量的网站攻击让网站成为国家重点安全监管的对象，目前针对网站管理者、运营者和使用者提出各种安全问题亟需一款产品为之解决。作为网络安全的引领者和建设者，公安三所从安全合规、监测预警、安全防护和应急响应四个方对网站进行动态评估，通过网站安全认证评估规范为网站安全防护能力进行打分，依据评分获取相应的星级证书，让网站安全状况可量化、可视化、常态化及可监督。

▲ 权威认证展示

开放数据共享 建立企业全网通行证

为了让企业的信用认证信息得到最大化的展示和通用，创宇信用将秉持开放的心态将已认证的企业信息数据和可信网址数据作为第三方认证数据进行公开共享，开放给第三方网站、产品和网络平台进行使用，真正发挥统一企业诚信信任机制，让用户浏览与交易更放心。

比如针对 SaaS 企业应用平台，为了确保平台所提供的服务为真实的企业所用，避免用户盗用其他企业的资料来申请服务，平台往往需要开发一个申请入口，接收企业的营业执照、对公帐号、法人信息、授权公函等，并组建审核团队对上述资料进行审核，同时还面临着审核标准制定和升级的巨大成本。

创宇信用将免费为各大 saas 商业平台开放认证结果数据，平台只需接入创宇信用第三方认证接口，通过授权即可使用创宇信用的认证结果，避免虚假资料和信息盗用风险。

▲ *创宇信用为第三方提供企业认证验证*

网络空间的信用与安全是虚拟社会化环境可持续发展的保证，创宇信用的全新升级，不仅可以为网民创造强有力的网络保障，在最大程度上维护网民的利益，更是最大化地将企业信誉传递给全网，连接信用，创造价值。今后，创宇信用会以更加开放的姿态为广大商用平台、社交平台开放企业验证结果，同时为企业和用户起到桥梁与沟通的作用，为建立更安全的网络防护体系，促进共建互联网征信体系而不断努力。

知道创宇推出智能名片工具——创宇微名片

在微信成为主要社交场合的今天，绝大部分商务交流都基于微信开展，在用户注意力越来越稀缺的当下，社交关系也已经从纸质名片、电话转移到微信。在这个流量巨大但信息纷扰的平台中，打破传统的信息传递、展示方式以及销售观念，对于企业和个人，都变得尤为重要。

10 月，知道创宇推出一款智能名片工具——“创宇微名片”，以小程序为载体，通过个人名片与企业名片功能，帮助企业连接到微信端 10 亿用户流量，全面提升企业销售和品牌输出能力，并集成创宇信用认证的企业可信验证信息，颠覆传统名片和企业官网，多维度输出企业品牌，提升客户信任，形成移动互联网时代企业营销推广的全新力量。（微信小程序搜索“创宇微名片”即可体验）

背靠微信社交关系链 轻松传递品牌

据统计，全球每年有 120 亿张纸质名片被交换，其中有超过 90% 不久就被丢失，只有 10% 可能被浏览并妥善保存，这其中 9% 被遗忘在抽屉的角落里，真正转化为商业价值的名片不到 1%。

“创宇微名片”可以更好地解决传统信息传递和销售链条中拓客难、触达难、易流失的痛点。

首先小程序门槛低、操作简单、便捷高效、交互友好、兼容多种名片交换场景。智能名片随手机微信自动生成，一键即可分享，再也无需像纸质名片那样互相交换和保存，可轻松覆盖潜在客户，却又无需重复介绍，用低廉的本钱和灵活的方法收割最大的流量红利，完成企业品牌与销售人员的最大化辐射。

同时，智能名片支持个性化定制，同时具备浏览量、人气值等社交信息展示，可以根据不同的业务场景需要制作不同的名片，向更精准的人群推广，更好的拓展人与人之间的关系，打开更广泛的社交圈、客户圈。

移动平台展示 企业信息可验证

企业员工向客户递出名片的同时，客户不仅可以看到员工的联系方式及相关资料，还可以通过对应的企业名片查看员工所属企业的基本信息、产品信息、社交媒体资料、企业工商信息、股东高管、经营信息、分支机构、变更、舆情等等，是企业在社交平台多维度展示品牌形象的绝佳场所。

员工认证与企业认证的加 V 展示，使信息传递变得真实可信且高效，避免山寨、虚假等钓鱼欺诈行为，让用户在微信端就能直接查看到企业的认证展示，不仅可帮助用户快速识别企业及网站的真伪，还能让用户对企业有更深层次的了解，在微信生态中更精准触达目标客户，彰显企业实力，提高品牌可信度。

企业员工管理 批量操作裂变推广

同时，智能名片提供企业员工管理后台，可批量完成员工管理操作，在电脑端、移动端同步认证审核，免去了企业为员工制作纸质名片的成本与周期。通过一张张电子智能名片，就可以全面输出个人、企业产品、品牌形象，通过微信的社交裂变属性，进行裂变推广。

名片作为商务活动的必需品和消耗品，智能名片顺应着社交场景的变化和互联网的发展已逐渐成为企业服务的标配，在拥有 10 亿用户的微信环境内，转发一张名片，客户一旦点击，其品牌信息和个人信息就被“捕获”，并长期留存，在科技愈加发达的未来，“互联网 +”的商业模式将会变得普遍，智能名片也将具有更广阔的应用前景。

知道创宇 APT 检测产品——“创宇云图”获赛可达实验室“东方之星”认证

11 月，知道创宇 APT 检测产品—“创宇云图”大数据安全威胁分析系统（以下简称创宇云图）顺利通过赛可达实验室各项严格的测试之后，获得该实验室颁发的“东方之星（Starcheck）”安全认证。

赛可达实验室是全球知名安全软件测评机构西海岸实验室旗下的中国测评认证机构，西海岸实验室认证目前是全球网络安全业界衡量产品水平的标杆，认证标准被全球认可为最值得信赖的指标之一。赛可达实验室在测试中严格采用西海岸实验室的测试标准体系和技术，特别强调产品在真实环境中特别是在中国实际互联网环境下的性能表现。本次赛可达实验室再次秉承“公平、中立、科学、严谨”的原则，为“创宇云图”颁发认证，代表着“创宇云图”的安全能力和安全水平已经达到了国际一线标准，也代表了“创宇云图”在技术上得到了网络安全业界的高度肯定和认可。

据介绍，今年 9 月，“创宇云图”在对某市公安授权监管出口进行网络安全威胁情况进行检测分析时，检测发现该市图书馆管理系统存在大量 DDoS 远控木马通信行为。

发现威胁信息后，“创宇云图”迅速对攻击来源进行了深入的数据挖掘与溯源取证。并对该市提供了全面不间断的威胁信息监测，和强有力的安全保障。

据知道创宇安全专家介绍，“创宇云图”上可对网络中的异常行为、数据外发、钓鱼邮件、网络应用攻击、Webshell 后门、是否感染僵尸网络，病毒木马，内部业务系统、员工主机的 Web 访问、Windows 系统、Office 办公文件等各类网络中传输文件，进行全方位安全检测。“创宇云图”采用机器学习及全面沙箱分析与入侵指标（IOC）确认技术，通过 BDE 行为检测引擎及 SDE 规则检测引擎实时分析网络流量，深度监控链接所有可疑活动。通过在沙箱（Sandbox）中运行（行为激活 / 内容“引爆”）各种文件和内容的功能，并观察虚拟机中的一些入侵指标，识别出未知威胁，以便进一步采取相关措施，将 APT 攻击消灭在萌芽状态。

知道创宇态势感知产品荣获 CCIA“2018 年网络安全创新产品优秀奖”

今年五月，中国网络安全产业联盟（以下简称“CCIA”）组织开展了“2018 年优秀网络安全解决方案和网络安全创新产品”评选活动。经过严格评审，在 CCIA 近日公布的评选结果中，知道创宇旗下网络资产信息普查和风险感知系统荣获“2018 年网络安全创新产品优秀奖”。

在网络安全产品同质化日趋严重的今天，只有技术先进并且模式创意的产品才能更好地支撑网络安全建设。因此网络安全创新产品的评选标准是产品的创新点具有较高的水平，在技术、设计方法、功能实现等等方面有创新突破，并且关键技术指标达到国内领先或国际先进水平，为网络安全产品开辟了重要的新应用领域。

知道创宇网络资产普查和风险感知系统，是基于知道创宇多年来从事网络安全相关技术研究以及网络安全产品的不断演进积累，并融合大数据情报收集、聚类及分析的技术资源而打造的全网安全威胁态势感知系统，可实时、准确的进行可视化传递，为用户呈现全网及特定目标网络的全部网络设备资产信息、漏洞威胁及影响范围等安全风险信息。

早在 2012 年底，知道创宇便开始对全球 42 亿 IP 地址进行持续的网络空间资源信息普查工作，目的就是在于为了让我国拥有与世界同等的网络安全水平，并研发出足够优秀的安全防护产品。2013 年，知道创宇于国内率先推出 ZoomEye 网络空间搜索引擎，在此基础上，结合知道创宇的漏洞发现检测技术和大数据情报分析能力，于 2015 年研制出 ZoomEye 网络空间雷达系统，通过对网络空间资产、漏洞侦测实现对网络空间测绘。

知道创宇一直致力于为用户掌握并呈现全网网络空间中的关键信息基础设施资产信息、特定目标范围内的网络资产信息以及针对网络空间资源进行漏洞预警与监察，通过持续累积演进，于 2016 年正式发布网络资产信息普查和风险感知系统，实现对网络空间资产及风险的普查、感知与呈现。

十八大以来，党中央对网络安全工作高度重视，《国家安全法》、《网络安全法》、《国家网络空间安全战略》在内的多项重磅政策密集出台，为网络安全产业健康发展提供了良好的政策环境和法律依托，网络安全产业处于快速发展的历史机遇期。

CCIA 此次评选，旨在为促进我国网络安全产业自主创新能力，推进产业结构化升级，帮助网络安全企业塑造品牌形象和拓展市场，为广大用户选择网络安全解决方案和网络安全产品提供参考依据。知道创宇网络资产信息普查和风险感知系统可为政府、企事业及军工单位客户建设全球网络空间测绘提供技术支持及产品支撑，进一步推动行业网络安全技术手段建设，进一步提升我国网络安全保障能力和水平。

行业合作

打造最强云生态 知道创宇携手中信集团共创新可能

4月3日，中信集团在四季酒店召开主题为“共生共享”品牌战略发布会，发布“共生共享”品牌核心定位和“共创新可能”品牌主张。知道创宇作为中信重要战略合作伙伴，为其提供了全面的云防护服务，中信云网成立之后，知道创宇首批入驻平台，全面保障中信集团“互联网+转型”战略，品牌战略升级之后，知道创宇将携手中信，在已经吹响的新时代号角下，迎接和创造无限新的可能。

中信认为，未来经济的持续繁荣和社会的持续发展，并非依赖于单一个体的带动，而是依托多方的合力。中信此次品牌战略发布之后，也同步打开了开放共享的时代窗口，将致力于与所有利益相关方共同打造一个有机向上、空间无限的“共生体”。作对外开放窗口和经济改革试点的中信，也用本次品牌理念的发布，为改革开放40周年庆祝献礼！

知道创宇创始人、CEO赵伟对中信“共生共享”品牌战略发布表示祝贺和高度赞同，他表示“知道创宇与中信集团之间的合作堪称行业典范，中信云网成立之后知道创宇是首批且当时唯一一家入驻的网站安全服务提供商，过去以来一直在为集团及集团各大子公司、以及中信云全生态用户提供全面的云防御服务，未来双方将基于更加开放的理念，在网络安全领域里不断拓展新的可能。”

新时代下的开放共享 共创新可能

2016年8月，中信集团正式启动“互联网+转型”战略，运用物联网、区块链、大数据等互联网技术，做连接，聚用户，生数据，重构下属产业的商业模式，推动其转型升级，打造“新金融、新零售、新制作、新建造、新仓储”五大生态，建设有中信特色的产业互联网。

基于上述战略，中信此次提供了“共生共享”的品牌核心定位。既体现了中信的综合经营特点，也体现了中信以开放共享的理念推动互联网+转型的战略内涵。更重要的是，这一定位契合了国家提供的“创新、协调、绿色、开放、共享”的五大发展理念，也与构建人类命运共同体理念一致，具有鲜明的时代特色。

“共生”带来三种结果，一是创造价值，二是创建生态，三是带来无限可能。中信更加看重后者，认为这将充满想象。中信拥有显著的品牌效应和强大的整体优势，在市场上具有强大的资源整合能力和资源聚集效应，在创造新可能方面具有独特禀赋。

中信提出“共创新可能”品牌口号，并给出如下诠释：“在一个复杂多元且快速变革的时代，全力前行，方能致远。未来不仅需要单一个体的带动，更要依托于各类发展资源的开放与协同，让隐性的价值显性化，让分散的价值链条关联起来，进而创造更大价值与更多新的可能。

合作共赢 布局全产业生态安全

在去年的中信集团年度信息技术工作会议上，知道创宇集中展示了入驻中信云网的安全成果，云防御平台在为集团及各大子公司、以及中信云安全生态用户提供全面保障，通过大数据萃取及威胁情报分析生动的通过态势感知系统得以展现，中信集团董事长常振明在会间参观时也给予了高度评价。

而展示平台背后，则是数款已经入驻中信云平台的知道创宇云防御产品实时予以提供的重要支撑。创宇盾，专为网站提供军工级防入侵服务；抗D保，则专为抵御大流量DDoS、CC攻击而生。入驻中信云平台之后，两款云防御（云安全防护平台）产品正在坚决捍卫中信云网用户网站数据及业务安全。

知道创宇云防护平台登陆中信云平台，对中信集团建立统一的网站安全管理体系、提升网站安全事件的防范和应急处置能力具有积极的影响。知道创宇云防护平台将用充足的资源保障、持续的研发投入，为中信集团“互联网+转型”战略提供信息网络安全保障，保障中信云网用户的信息网络安全。

“中信集团是超大型国有综合企业集团，拥有庞大的自身产业链，业务布局多元化且全球化。同时中信一直以来也是一家开放的企业，此次品牌战略发布之后更加让人看到这种开放的态度和决心，知道创宇也愿意在原有与中信集团的合作框架下，在全新品牌主张的指引下，在更多的产业生态安全领域全面开展合作。” 知道创宇创始人、CEO赵伟表示。

创宇盾助力东方航空 打造空港网络安全体系

五月，中国东方航空集团与北京知道创宇信息技术有限公司达成深度合作。

据悉，东方航空旗下网站群接入知道创宇云安全平台产品—“创宇盾”，创宇盾将对东航旗下网站群开展包括网站应用防护、页面防篡改、数据防泄密、漏洞速递、重点时期保障等在内的多项服务，形成一站式立体空港网络安全体系。

东航是国内前三、全球第七大航空公司，现有机队规模近650架，2017年承运旅客超过1.1亿人次，网络通达全球177个国家和地区的1074个目的地。东航一直注重将最先进的互联网技术应用于安全运行管理领域，提升飞行风险管控能力。

知道创宇是国内最早提出云监测与云防御理念的网络安全公司，十年能力积累，实现了为客户提供具备国际一流安全技术标准的可视化解决方案，网络安全监测、预警及防御能力。

旗下核心产品“创宇盾”自发布以来，参与过中国共产党第十九次全国代表大会、世界互联网大会、国家网络安全宣传周、金砖峰会（厦门）、一带一路峰会（北京）、国家两会、G20峰会（杭州）、贵阳数博会等会议的网络安全保障工作，“创宇盾”所防护的网站均无一例被黑事件发生，其强大的安全防护能力经受住了长久的实战考验。多次受到相关部门、单位的一致好评和致谢。

目前，网络安全已迅速成为航空运输业面临的首要任务之一，随着越来越多新技术的采用，提高效率的同时不可避免的增加了网络安全的风险，创宇盾拥有丰富的成功案例、专家资源及本土的专业信息安全人才，助力东方航空应对网络安全挑战，携手共进，互惠共赢。

十年耕耘 不负重托——知道创宇 6 款安全产品入围央采名录

7 月 24 日，中央政府采购网公布了 2018-2019 年中央国家机关信息类产品（硬件）和空调产品协议供货采购项目中标公告，知道创宇旗下创宇盾、抗 D 保、WebSOC、创宇云图、创宇雷达、创宇智图等 6 款安全产品共计 18 个型号通过了专家论证，全部入围中央政府采购网协议供货名录。

中央政府采购是整个政府采购中的最高级别，协议供货目录面向中央直属近万个机关单位，同时辐射地方政府采购中心。候选厂商必须经过专家组的多次集体评审，对产品从品质、口碑、技术含量、售后服务等方面层层筛选、多重把关，入选门槛相当之高。入围 2018 央采信息类产品协议供货采购目录，是中国政府采购权威评审机构对知道创宇认可度和信任度最高的体现，是企业硬实力的表现。

入围采购名录的 WebSOC(立体监控) 是一款高性能、周期性网站集中安全监测硬件产品，可多维度、全方位监控大批量网站，并提供全局统计和趋势分析。

创宇盾通过军工级 Web 业务系统防护服务，提供网页防篡改、防拖库窃密、防挂马等服务，帮助政府机构等建立全方位防御体系。

抗 D 保拥有全球 Anycast 清洗技术及多个自主知识产权的攻击清洗专利技术，专注于特大流量 DDoS 攻击防御，防御能力超过 4Tbps。

创宇云图威胁感知系统采用机器学习及全面沙箱分析与入侵指标确认技术，通过行为检测引擎及规则检测引擎实时分析网络流量，识别出未知威胁，将 APT 攻击消灭在萌芽状态。

ZoomEye 网络空间雷达系统针对目标进行漏洞侦测，实现网络资产的风险感知。可实时监测存活网络资源和设备资产受漏洞影响的情况，并可根据需要进行漏洞筛查和验证等工作。

创宇智图数据库审计与防护系统是知道创宇自主研发完成的业界首创智能自动学习、自动建模、风险自识别、细粒度审计、精准化行为告警、全方位的数据库安全审计产品。

此次顺利入围，知道创宇以 6 款产品 18 个型号的巨大优势在众多优秀的供应商中拔得头筹，对于知道创宇进一步拓展政企市场具有重大意义，使其产品在市场上更具优势，同时也体现出客户对知道创宇品牌“侠之大者 为国为民”基本信仰的认可和信任。

多年以来，知道创宇立足网络空间攻防对抗一线，为政企客户提供最专业的产品和快速响应服务，在用户中赢得良好的口碑。也正是长久的技术积淀让知道创宇成长为国家网络安全背后的坚实力量，多次参与了各项国家级会议、活动的网络安全保障工作中，均以“零被黑，零事故”的优异成绩切实守护着国家的网络空间安全。

今后，知道创宇将继续发挥自身技术优势，始终保持高度的责任感，为政府、公安、金融、能源等企事业单位网站系统和国家关键信息基础设施提供全方位的安全防护，为建设网络强国奉献力量，为更好更安全的互联网而奋斗。

知道创宇联合腾讯安全中标招商局
一体化终端安全方案护航央企网络安全

近年来，以高级持续性威胁、勒索病毒、数据黑产等新型攻击技术为代表的网络安全事件频繁发生，严重损害了企业利益。如何加强信息安全建设成为社会各界共同面临的挑战，尤其对于中央企业而言，安全问题更是不容忽视。

为全面提升企业信息安全防护水平，保障全集团终端安全，实现终端统一安全管理，招商局向安全业界广泛咨询，寻找技术领先的方案提供商，腾讯安全与知道创宇凭借技术驱动智慧安全的理念，以腾讯御点终端安全管理系统（以下简称“腾讯御点”）及其所拥有的海量安全大数据，高级威胁终端检测与响应能力，精准的病毒查杀能力，全面的一体化终端安全管理能力和极致服务模式成功中标。

腾讯御点由具备全球顶尖攻防及病毒研究能力的腾讯和知道创宇“7+1”联合实验室支持，依托双方多年安全实践和经验积累，采用了百亿量级云查杀病毒库、引擎库以及独有的腾讯 TAV 杀毒引擎、系统修复引擎，可有效防御针对企业内网终端的病毒木马和漏洞攻击，为企业级用户提供终端病毒查杀、漏洞修复和统一管控等全方位的终端安全管理方案，帮助企业管理者更好地了解内网终端安全状况，保护内网终端安全。

同时，在面对招商局十万级终端安全防护任务的挑战上，腾讯御点充分发挥了其在适配大型企业网络环境中多地域、多级构架的能力，采用集群架构的模式，把原本运行在同一台服务器上的业务拆分到不同的服务器，用以支持跨地域的十万级终端，从而建立全面的终端安全防护体系。

知道创宇相关负责人进一步介绍，腾讯御点以更准、更轻、更快、更易用为首要研究方向，基于腾讯安全和知道创宇联合大数据，能够与流量检测和态势感知联动，并提供便捷的终端安全一体化管理。此次与招商局合作，将全面体现腾讯御点终端防护以及管理的价值，即“快速有效系统解决终端安全问题”，通过灵活的配置迅速反应，为集团系统建立完整的防护体系，在遭遇攻击时，快速应急并形成完整的防御机制。

在安全成绩方面，腾讯御点的安全能力备受瞩目，屡获国际评测认证，全球七大权威机构病毒查杀能力评测大满贯，100 次 + 最高评级。

招商局终端安全保障项目已成为腾讯御点在央企行业的标杆项目之一，后续，招商局、腾讯安全和知道创宇三

方将在彼此配合下，精诚合作，全面助力企业终端安全从单一防护向体系化防护，从被动防御向主动防御，从局部静态防御向整体动态防御，为国家关键信息基础设施安全和集团网络安全保驾护航。

据了解，在该项目的产品测试阶段，腾讯御点就已表现出远超国内安全行业业界平均水准的强势安全能力。随着国家信息安全意识增强，政府、央企采购杀毒软件已倾向和支持国产化，尖端技术生来便具备国家属性，腾讯 TAV 引擎作为国产反病毒引擎和腾讯御点的核心引擎之一，无疑是为我国的杀毒软件注入了一针强心剂，将推进国产信息安全领域进入下一时代。

为树立新时代的网络安全观，知道创宇一直提倡“技术驱动 智慧安全”的安全体系架构。在企业内网面临全面的高等级攻击威胁的当下，传统以卡断离为表现的刚性防护思想已不能适应新时代企业网络安全的需要。知道创宇提供以技术实用性驱动的柔性整体防护体系，防御和威慑并重，并与企业态势感知和其他安全体系在数据和操作层面上融合一体，形成整体安全能力。此次中标，正是对知道创宇服务和以实战出发整体防御体系的高度认可。

依托腾讯公司近 20 年为互联网 10 亿级海量用户提供安全防护的成功经验，腾讯安全积累了先进安全的大数据平台和 AI 等核心技术实力，并形成了云、管、端协同的智慧安全防护体系。此次腾讯御点的中标，腾讯安全也再次拓展了业务体系，将帮助更多超大型国企、政府机构高效抵御高等级的安全威胁，从而进一步推动产业数字化、智能化升级。

国防科工局信息中心与知道未来签署战略合作协议

为了推动国防科技工业系统网络安全和军民整合产业的发展，5 月，国家国防科技工业局信息中心与北京知道未来信息技术有限公司正式签署战略合作协议，双方将本着“协同推进、共赢未来”的原则，全面推进国防科技工业体系信息安全行业军民融合深度发展。

据介绍，接下来双方将在工业系统网络安全军民融合各领域展开战略合作，如共同推进《国防科技工业系统网络信息安全采购规范白皮书》及行业相关制度及目录的制定工作等，同时知道未来 K 学院还将重点参与配合举办 2018 国防科技工业体系网络安全攻防演练活动。

知道未来相关人员表示，知道未来成立之初即以保障国家信息安全为己任，致力于建设新一代网络攻防一体化安全企业，为捍卫国家网络空间主权贡献力量，双方合作开展之后，将投入优先资源以保障相关工作顺利有序开展。

知道未来
Known Future

关于“知道未来”：

北京知道未来信息技术有限公司成立于 2014 年，是北京知道创宇信息技术有限公司的全资子公司。作为新一代网络攻防一体化安全企业，公司以保障国家信息安全为已任，提供一流的网络安全产品、服务和整体解决方案，并主动开展网络空间安全前瞻性技术研究与探索，为捍卫国家网络空间主权贡献力量。

联通集团边缘云生态合作伙伴公布 安全企业仅此一家

6 月 13 日上午，2018 中国联通边缘云生态合作伙伴大会在北京国际会议中心举行，现场联通集团为国内二十家生态合作伙伴授牌。在现场宣读的合作伙伴名单中，可以看到 BAT 三巨头、华为、新华三等置身其中，而知道创宇则是其中唯一一家网络安全企业。

出席会议的知道创宇 EVP 陆海表示，知道创宇随后将与联通集团就边缘云生态全面开展相关合作，目前正在对现有试点及未来规划进行相关安全测试，未来将量身定制一系列安全服务，以保障联通集团边缘云生态安全落地健康发展。

下一代网络、未来安全，是网络安全公司知道创宇的技术定位。从国内最早的云防御公司，引领国内云防御大力发展；到提出大数据安全概念；以及率先开展网络资源测绘；打造人工智能安全技术；再到全面的态势感知体系的建立，知道创宇一直处于网络安全行业浪头。

云计算的出现到成熟改变了整体互联网业态，重塑了企业 IT 服务架构，边缘云技术的诞生，到利用，以及更多的同 5G 技术产生关联，已经具备了它应有的“催化”气质，更将为下一代主网带来翻天覆地的商业变革。此次知道创宇与联通集团的合作，也是自身企业发展的顺势推进。

重磅活动

知道创宇承办首届“赛博地球杯”工业互联网安全大赛暨论坛成功举办

由北京知道创宇信息技术有限公司和南京赛宁信息技术有限公司联合承办的“赛博地球杯”工业互联网安全大赛暨论坛于 1 月 28 日成功举办，该赛事活动由网信军民融合发展联盟网络空间工作委员会与工业和信息化部国家工业信息安全发展研究中心联合主办，旨在推进网络强国建设，落实国务院关于建立工业层次安全保障体系，提升“设备安全、控制安全、网络安全、平台安全、数据安全”的工作要求，建设攻防兼备的国家工业互联网安全体系。

中国工程院信息与电子工程科技发展战略研究中心、移动互联网发展中心、中关村信大网络信息军民融合研究院和《网信军民融合》杂志协办参与了本次赛事活动。

本次大赛由“赛博地球杯”工业互联网安全大赛、工信部工业互联网安全闭门研讨会、工业互联网安全论坛及工业精选创新项目投资洽谈会四部分内容组成，工信部、网信办、公安部等部门相关领导出席了赛事及会议活动，大赛开幕式、论坛及颁奖活动由中央电视台军事频道主持人主持。

中国电子科技集团副总经理、总工程师、中国工程院院士吴曼青、国家工业信息安全发展研究中心主任尹丽波于当天上午 9 时宣布大赛正式开始，线上赛入围的 12 支战队和主办方特邀的 8 支战队共 20 支战队一同角逐当天线下决赛。截止至当天下午 17 点，线上入围组排行由 Nu1L 战队夺得冠军，解出 7 道题，得分 4665.7；第二名 ChaMd5 安全团队，解出 6 道题，得分 3877.07；第三名天枢战队，解出 5 道题，得分 2719.13。

线下特邀组战队实力也不容小觑，最终排行该组第一名的是护网先锋战队，解出 6 道题，得分 3651.92 ；排行第二名的是朝阳群众战队，解出 6 道题，得分 3571；第三名是 BOI 战队，解出 4 道题，得分 2173.69。

本次赛博地球杯工业互联网安全大赛为解题闯关赛，定位国内首个军民融合主题的云防护实战技能对抗赛，中国电科提供龙云平台云安全相关赛题，知道创宇 K 学院提供工控安全相关赛题、工业仿真环境，赛宁网安提供竞赛平台支持。

其中，我国自主研发的新一代信息系统基础服务平台“电科龙云”作为靶标，供来自国内的 20 支优秀团队自行突破，历时 8 小时总计 7042 次攻击，截至比赛结束仍未被攻破，展现出了其自主可控、安全可靠的产品内在基因。

本次比赛为体现攻防的实战价值，由承办单位知道创宇精心布置了工业互联网的典型场景，并与赛题进行充分融合。参赛团队需通过逐步渗透，完成题目闯关，并借以评估其技术能力。赛题中分别设置了火力发电（火电工艺监控系统）、电网调度（城市电力系统）、军工制造（砷化镓单晶炉监控）等工控场景，选手需先通过突破工业互联网络后方可进入工业生产控制网络。

本次比赛赛题设计源于实践，集合了多次国内外大型工控安全事件的背景原因分析，体现了当下工业互联网的脆弱性和后果的复杂、严峻性。例如，在对在工业生产环境中借助入侵生产商能源关键系统账号，搜索到工厂生产排程计划并找到工厂单晶炉工艺参数，最终获取单晶炉现场监控主机登录密码。此后选手可通过迫使煤运皮带停止转动、修改单晶炉生产工艺、修改生产现场控制程序等手段最终破坏城市供电系统。

本次工控赛题设计巧妙，将工业互联网与传统安全攻防技术充分融合，呈现出如 web 渗透、qemu 逃逸、docker 逃逸、云 waf 绕过、逆向工程、本地提权、漏洞利用等多种赛题形式，对选手的综合攻防能力是一次全面检验，这一设计也得到了观赛专家和参赛选手的一致好评。

“赛博地球杯”工业互联网安全大赛也成功首创国内以攻促防的比赛机制。以此次比赛起点，逐步形成创新型

常态化比赛机制，由产业界提供自有产品和系统作为靶标，为发布靶标的企业建立“漏洞发现奖励制度”，以众测方式为企业打造更加安全的产品、系统、平台。在促进产业界网络安全升级的同时，推动形成网络安全人才社区，鼓励网络安全人才和产业界形成互相促进、良性发展的产业生态。

当天下午，工业互联网安全论坛如期召开，论坛特邀相关部委领导、中国工程院院士、以及网络安全产业的领军人物出席论坛活动并发表了主旨演讲。中国电子科技集团副总经理、总工程师、中国工程院院士吴曼青致辞时表示，工业互联网时代需要建立协作共享的工作机制，才能更好的解决来自工业互联网可能会面临的风险问题，需要大家一同努力提高我们的工业互联网安全能力。

工业和信息化部信息化和软件服务业司任利华副司长在致辞时表示，工业互联网快速发展、健康发展、安全发展归根结底要靠我们掌握关键核心技术、培养一支强大的科技人才队伍，需要产学研用方方面面共同参与，协同推进。今天“赛博地球杯”工业互联网安全大赛暨论坛的召开正是响应国家在工业互联网发展上的具体部署要求，是行业发现工业互联网安全人才的重要平台和举措，希望在不断创新的基础上越办越好，为夯实我国工业互联网安全体系做出更多更大的贡献。

国家创新与发展战略研究会副会长郝叶力少将在论坛致辞时表示，发展工业互联网已经成为主要国家抢占全球产业竞争新的制高点，对于建设制造强国、网络强国都具有重大的深远意义。当前我国工业互联网正处于起步阶段，总体发展水平、基础与发达国家仍有不小差距，迫切需要政府、企业、产业协同连动，才能实现安全保障能力的体系化布局，切实的提升工业互联网整体的安全防护能力。

在论坛主旨演讲环节，国家数字交换系统工程技术研究中心主任邬江兴院士、中国工程院倪光南院士、国家工业信息安全发展研究中心何小龙副主任、中国网络空间安全协会理事长，中国工程院方滨兴院士、赛迪安全咨询和评估中心刘权主任、中国电子科技集团青年千人廖勇先后发表了精彩的话题演讲，就赛博空间、工业互联网安全发展做出了精彩解读。

网络安全企业知道创宇技术副总裁李伟辰演讲则从专业角度对广域互联网的安全威胁如何做好防范做出了解读，他重点解读了基于知道创宇核心的安全能力，如云防御对工业互联网的安全意义，以及 Seebug 漏洞社区的运营、ZoomEye 网络空间探测引擎探测全球 42 亿 IP 对工业互联网安全保障所能做出的贡献做出了进一步解读。

论坛最后，由吴曼青院士和郝叶力少将先后对“赛博地球杯”工业互联网安全大赛线下决赛最终战绩优胜的队伍进行颁奖，也宣告了“赛博地球杯工业互联网安全大赛暨论坛”的圆满举办。

▲ *吴曼青院士、郝叶力少将为优胜队伍颁奖*

首届中国区块链安全高峰论坛召开 号召关注生态安全

6 月 21 日，首届中国区块链安全高峰论坛在北京国家会议中心成功召开，大会由中国技术市场协会主办，北京知道创宇信息技术有限公司承办，会议吸引了众多国家权威机构领导、区块链行业大咖、安全行业大佬以及众多行业顶尖媒体及海外权威人士共同参与。

大会由一段短视频作为开场，视频展现了近年来区块链领域相关的安全事件，以及暴露的社会化安全问题，可以说件件惊心。种种因安全问题所造成的动辄千万、上亿经济损失的事件，及广泛存在的假借区块链名义施诈骗、传销之实，已成为区块链生态圈的心头痛点，并引发各界警惕与关注。

在区块链技术受到世界广泛关注的同时，伴随其自然发展的道路上，网络安全及社会化安全问题已经成为区块链良性发展的绊脚石，这也是本次大会举办所要表达的核心意义所在，大会呼吁关注区块链生态安全，合力探寻区块链未来健康发展之道。

▲ *圆桌讨论区块链安全*

大会受到了国家及社会各方的高度重视，多个国家部门相关领导出席会议并发表致辞，来自腾讯公司副总裁马斌、知道创宇创始人兼 CEO 赵伟、中国区块链应用研究中心理事长 - 星合资本董事长郭宇航、比特大陆副总裁葛越晟也先后登台致辞，表达了对区块链生态安全的关切。

当天上午，大会发起了中国区块链安全联盟筹备的倡议活动，活动由中国反流氓软件联盟发起人董海平主持。据介绍，联盟由中国技术市场协会、腾讯安全、知道创宇、中国区块链应用研究中心等，含政府指导单位、网络安全企业、区块链相关机构及媒体等二十余家机构、单位联合发起，这一活动将建立区块链生态良性发展长效机制，着重打击一切假借区块链名义进行变相传销、诈骗等敛财行为。

大会共邀请到国内外区块链生态领域相关专家共十余位到场发表主旨演讲，分享如何利用技术打造更好更安全的区块链生态，以及区块链技术的创新应用，高质量的议题分享也受到了参会嘉宾的称赞与热议。在大会的圆桌论坛环节，相关专家还共同就如何推动区块链产业的安全健康发展展开了集中讨论，并且不乏劲爆观点被抛出。

首届中国区块链安全高峰论坛得到了相关行业及媒体的广泛关注，会议报名通道开通仅一天即已爆满，会议当天现场座无虚席，上百家专业媒体当天列席会议并对会议进行了报道。

KCon 2018 黑客大会在京圆满召开

2018 年 8 月 24-26 日，KCon 2018 黑客大会在北京市 751D·PARK 东区故事 D·live 生活馆召开，这场由国内一线安全公司知道创宇主办的黑客大会由首日两场闭门培训和为期两天的干货黑客议题分享组成。

KCon 的口号是汇聚黑客的智慧，在 KCon 2018，我们再次见证了全球黑客的热情，大家齐聚一堂，用攻破之精神、探索之成果向安全行业及整个互联网传递着正义黑客应该具有的价值观和人生观。

在 KCon 2018 开幕式上，知道创宇 CEO 赵伟说道，KCon 定位于干货和品位，聚焦于有价值的技术内容以及真正的黑客精神，这个平台聚集着黑客们的智慧结晶，这样有意义的交流也让安全行业发展更具生机。KCon 走到第七年，除了顶尖前沿的技术分享，各互联网公司的 SRC 平台、白帽子们、安全自动化工具开发者等等群体都加入进来，散发着无穷的能量。赵伟表示，“当大家不认为我们办了一场商业会议，而是一场有品位的黑客会议时，我们就成功了。”

▲ *知道创宇 CEO 赵伟开幕致辞*

会前闭门培训再度升级

KCon 认为，能力越大者，责任也就越多，安全行业从来就不是一个轻松的行当，只有当一个人有了敬畏和规则，有了技能与实力，才能在这条路上走的更远。KCon 从

▲ *KCon 2018 演讲日现场*

▲ *KCon 2018 演讲日现场*

2015 年和 2016 年相继引入安全入门培训和安全进阶培训，旨在为不同层次的安全技术人员带来心灵上的洗礼或是技能点的专攻提升。

在 KCon 2018 上，两场闭门培训皆采取了更加细化的方式，分为上下午两场，为参会者带来更好的培训体验。安全入门培训邀请到知道创宇 K 学院资深培训讲师周家豪，带来黑客技术及案例分享，为年轻学子打开黑客世界的大门。另一位培训导师是来自听潮盛世（北京）科技有限公司创始人杨凡，他通过渗透测试技术讲解，带领大家感受渗透实战的魅力，受到与会者一致好评。

▲ *KCon 2018 安全入门引导培训现场*

在安全进阶培训方面，讲师 hyperchem 通过实战方式引导学员对现行主流游戏平台的破解方式进行深度剖析，引得众多游戏机爱好者和硬件发烧友大呼过瘾。而去年深受好评的进阶培训讲师 xwings 也再次到来，带来《物联网系统安全实战—PartII》培训，更深入地开展物联网通用设备全过程分析，并将拆解设备送给现场学员供研究。

18 大议题分享干货依旧 不负众望

KCon 黑客大会重磅环节，自然是为期两天的 18 个干货议题分享。本届 KCon 主题是「聚·变」，当 KCon 经历七年轮回后，再次回到“黑客精神”的原点，聚焦当下最新、最热门的攻防研究方向与技术，涵盖汽车安全、智能家居安全、工业网络安全、智能合约安全、数字钱包安全等领域，用技术实力引领业界未来的变革。

KCon 提倡以极客精神探索攻防技术、实践安全之道，谢绝商业演讲，致力打造纯技术分享会议。正是长期以来的严格要求和精益求精，才让 KCon 成长为中国网络安全圈最年轻、最具活力与影响力的前沿网络安全攻防技术交流平台。

不断创新 丰富 KCon 参会体验

除了保持高水准的议题分享，KCon 连年都在推陈出新，KCon 2018 保留了往届推出的经典环节，如兵器谱展示、周边售卖、合作伙伴展示等，今年还新设置了“SRC 英雄榜”，向众多致力于维护互联网健康环境的漏洞收集及应急响应平台，以及背后默默付出的白帽子致以敬意。腾讯、京东、美团、小米、唯品会、陌陌等国内一流互联网公司的安全平台均有上榜，主办方也希望借由 KCon 的平台加强业内各界的安全沟通及合作，共同打造互联网的安全生态。

▲ *KCon 2018 Rocking Live Show*

同时，让历届参会者印象深刻的摇滚表演也全新升级为 Rocking Live Show，贯穿于两天演讲日的每一场茶歇时刻，让黑客与摇滚更紧密地结合在一起。一名真正的黑客，正如摇滚乐所要表达的那样，向往自由，善于创新，充满正能量。KCon 2018 Rocking Live Show 由陌陌 SRC 独家冠名赞助，在走唱团队激情表演下，点燃了大家的内心激情。

致谢合作伙伴与朋友们

从 2012 年到 2018 年，KCon 从一个小小的安全论坛成长为中国网络安全圈最年轻、最具活力与影响力的前沿网络安全攻防技术交流平台。每一年 KCon 黑客大会的成功举办，都离不开给予我们帮助和支持的行业伙伴们。

KCon 2018 黑客大会得以圆满举办，在此感谢黑钻赞助腾讯安全，金牌赞助腾讯安全应急响应中心、安赛 AISEC、椒图科技，Rocking Live Show 独家赞助陌陌安全应急响应中心，礼品赞助唯品会安全应急响应中心，独家中英同传支持搜狗同传，安全客、IT168、链闻三家战略媒体及十余家合作媒体的鼎力支持。

▲ KCon 2018 会务组

KCon 所做的努力是在建立一个安全氛围，团结所有正义的黑客，共同创造和维护更安全的网络空间，正是有了你们的帮助和支持，我们所共同向往的那个世界才会在不远的前方。

KCon 2018 黑客大会圆满落幕，难舍再见，但这也更让我们期待来年，正义的黑客们，我们 KCon 2019 再约！

CSS2018 FP50 分论坛：
首创安全界奥斯卡颁奖礼 发掘未来安全行业新锐力量

数字经济时代，新兴网络安全企业如雨后春笋般地蓬勃发展，面对更加复杂细分的领域以及更加多元化的市场需求，究竟谁才能成为未来行业的新锐力量？这些都成为第四届互联网安全领袖峰会 (Cyber Security Summit，简称 CSS)Future Power 50 安全新锐力量分论坛（以下简称 FP50）聚焦的重点。

2018 年 8 月 28 日下午，由北京知道创宇信息技术有限公司及腾讯安全主办的 FP50 安全新锐力量分论坛在北京望京凯悦酒店召开。北京知道创宇信息技术有限公司创始人、CEO 赵伟发表致辞中提到，FP50 安全新锐力量分论坛更希望打造安全新锐企业交流，合作的平台，从而吸引更多的企业加入，推动行业发展，为行业不断造血。

会上，XIO 基金亚洲区主管兼合伙人乔飞与极客邦科技创始人兼 CEO 霍泰稳围绕新兴安全技术创业者所面临的难题进行了两大主题演讲。由 10 位业内大咖组成的专家评审团经过多维度的考量，最终评选出 30 家安全新兴企业，并在首创的安全界奥斯卡颁奖礼上为入围企业颁奖，最终成立安全新锐力量俱乐部。

两大主题演讲为技术创业者指点迷津

当经济增长放缓遇上技术革新，数字时代下，新兴安全企业如何屹立于浪潮中不倒？ XIO 基金亚洲区主管，合伙人乔飞围绕 “当前市场情况下科技互联网行业投资的关注要点”这一主题带来了主题演讲。

乔飞认为，在当前复杂的网络形势下，科技创新企业

应坚持完善科技，以科技去驱动创新，以创新成为核心竞争力，用核心竞争力创造最终的商业价值。他还指出，我们应给予安全创业公司更多的关怀和信心，当今时代，通过安全技术创造美好世界并不是梦想，而是可以成为认真切实的选择。

众所周知，技术创业是所有类型创业中风险最大的一种，安全创业公司会面临无法及时融资导致资金条断裂，无法控制固定成本导致收支出现极大差异等诸多挑战，极客邦科技创始人兼 CEO 霍泰稳结合自身多年创业经验，为我们带来了“技术创业者的三大纪律”。

他奉劝各位技术创业者，不要因为自己赶上了创业的好时代，就心头一热，去追赶估值高、投资踊跃的领域，一定要审时度势，居安思危。而安全创业公司面临的最大危机就是没钱，通常，一个技术创业公司如果没有足够的现金流，而一旦资金断裂，工资发不出来，造成人才流失，公司也就只能在濒死的边缘挣扎。对此，他提出了一个“固定成本”概念，就是通过认真并提前融资做到“开源”，再通过控制支出达到“节流”，两个方向双管齐下，最终控制好“固定成本”，避免资金出现问题。

首创安全“奥斯卡”颁奖盛典 重磅评审团汇集业内大咖

作为 CSS2018 的一大亮点，FP50 安全新锐力量分论坛引入了技术大拿、业界领袖企业高管、专业媒体及第三方调研机构、创投领域意见领袖等组成专家评委团队。

评委团队包括知道创宇信息技术有限公司创始人、CEO 赵伟，《中国信息安全》杂志社副社长、主编崔光耀，北京未来安全信息技术有限公司 CEO 王英键，极客邦科技创始人兼 CEO 霍泰稳，创头条副总裁李茂达，“数说安全”创办人于江，北极光董事总经理张朋，腾讯安全云鼎实验室负责人董志强（Killer），飞天诚信副总经理闫岩，启明星辰副总裁潘重予。

大咖们齐聚一堂，聆听“新锐力量”们探讨尖端技术新趋势、企业责任、未来产业方向、传统企业转型中的科技助力，对入围的企业就业务范围、发展规模、成立年限、年营收等进行了全方位多维度的考量，秉着开放、公开的态度，最终通过慎重地评审，推选出 30 支安全新锐力量。

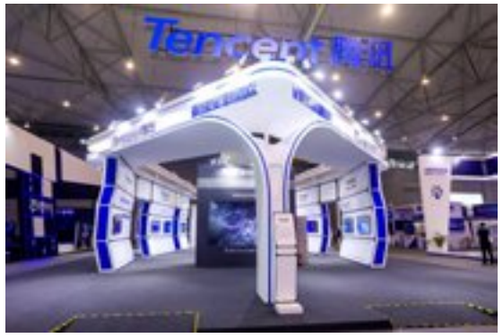
随后，入围的 30 支安全企业代表悉数登台，评审团对企业们做出了中肯的点评，并表示希望 30 家企业再接再厉，汲取更多的技术创新，不断进步，共同推动中国网络安全产业。FP50 首创的安全界“奥斯卡”颁奖典礼正式开始，以下为获奖企业名单：

FP50入围企业
北京长亭科技有限公司
北京娜娜安全科技有限公司
杭州默安科技有限公司
北京安华金和科技有限公司
北京极图科技有限公司
上海斗象信息科技有限公司
北京安赛创想科技有限公司
苏州棉佰安信息技术有限公司
北京指掌易科技有限公司
深圳永安在线科技有限公司
北京卫达信息技术有限公司
武汉极意网络科技有限公司
北京升鑫网络科技有限公司
瀚思安信（北京）软件技术有限公司
南京赛宁信息技术有限公司
贵州白山云科技有限公司
杭州美创科技有限公司
杭州世平信息科技有限公司
成都无糖信息技术有限公司
北京元支点信息安全技术有限公司
芯盾（北京）信息技术有限公司
北京未来安全信息技术有限公司
北京金睛云华科技有限公司
四维创智（北京）科技发展有限公司
北京上元信安技术有限公司
北京锦龙信安科技有限公司
北京红山瑞达科技有限公司
西安讯蜂科技有限公司
北京海泰方圆科技股份有限公司
上海弘积信息科技有限公司

评选出的 30 家企业随后成立了安全新锐俱乐部，旨在通过企业联合，扩大行业价值，促进行业内核心技术进步，提高共同抵御安全风险的能力。同时，FP50 安全新锐力量分论坛更希望通过安全新锐俱乐部，为更多的新兴企业提供一个平台，吸引更多的企业加入进来，推动行业发展，为行业不断造血。

包括 Future Power 50 安全新锐力量分论坛在内，本届 CSS2018 还设置了腾讯安全探索论坛（TSec）、金融安全分论坛、人工智能安全分论坛、AE50 网络安全产学研论坛、数字支付分论坛、云安全分论坛、工业互联网安全分论坛以及 P16 基础设施安全领袖圆桌等九大分论坛，聚焦各领域的安全趋势与技术研究成果，与国际重磅大咖一同助力数字安全新生态的建设。

知道创宇盛装亮相 2018 安全周：最强生态舰队，护航网络安全



2018 年 9 月 17 日，第五届国家网络安全宣传周如期举行，直到当月 23 日，全国范围内将迎来为期一周的网络安全盛会，围绕“网络安全为人民 网络安全靠人民”这一主题，通过成果展示、高端论坛、极客赛事、互动体验等多种活动形式，提升全民网络安全意识和相关技能培训，共建网络安全。

在主会场成都，由中央网信办、四川省人民政府指导，成都市人民政府主办的 2018 年网络安全博览会也于今日盛大开展。博览会设置了优秀网络安全解决方案和网络安全创新产品展，展示网络安全领域新技术新理念新方案，让广大观众在参观博览会过程中更好地了解网络安全、参与网络安全。

在 2018 网络安全博览会，中国最具影响力的互联网巨头腾讯、中国一线网络安全企业知道创宇以及前沿国际化智能安全社区 GeekPwn，再次强强联手，推出“最强生态舰队，护航网络安全”主题展，展览内容全面涵盖各自网络安全领域最强能力及生态影响力，积极推动网络安全新生态建设。

最强生态舰队 护航网络安全

今年的安全周，腾讯、知道创宇、GeekPwn 联合展厅化身未来科技感“生态舰队”，由动力平台组建的超级引擎、强大科技编程的操控系统和攻防兼备的尖端战斗武器精密组合而成。在腾讯品牌超级引擎下，腾讯安全象征着强大科技产品矩阵构建的操控平台，知道创宇、GeekPwn 则是这支网络安全战舰中最强大的武器，三方对应不同安全能力及生态，构建起空天地一体的网络安全护航舰队。

在网络安全领域，腾讯安全拥有腾讯公司长达 19 年的专业领先能力、海量安全大数据经验积累，是中国最为领先的互联网安全产品、安全服务提供者，和安全生态建设者；而知道创宇则拥有专业网络安全领域超 10 年的深耕能力积淀，在以不断创新研发能力的保障，及服务中国 90 余万家网站的海量大数据经验积累下，已成为中国最具代表性和领先的网络安全企业；GeekPwn 则是全球首个关注智能生活的安全极客赛事平台，一直关注未来智能生活安全。

此次联合参展，也向行业和社会传递一个概念，做好网络安全，仅靠自身力量远远不够，需要整个安全产业联合起来，通过产业合作，实现开放、联合、共享的安全新生态环境。

保障国家民众网络安全 知道创宇永不停歇

随着网络信息技术的迅猛发展和广泛应用，特别是我国国民经济和社会信息化建设进程的全面加快，网络信息系统的基础性、全局性作用日益增强。习总书记倡导“总体国家安全观”，网络安全是整体的而不是割裂的，网络安全对国家安全牵一发而动全身，同许多其他方面的安全都有着密切关系。

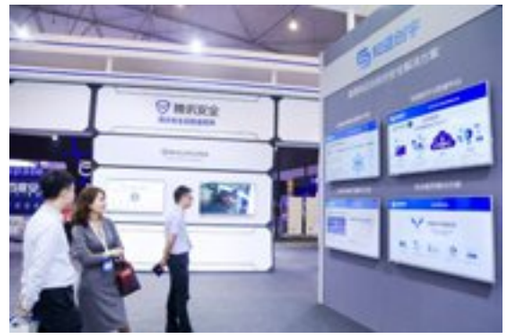
知道创宇自成立之初就以“侠之大者，为国为民”作为企业发展的核心信念，致力于为国家和人民提供网络安全保障。在国家层面，长期为政府国家重要信息系统提供安全防护，并积极参与到各项国家级会议、活动的网络安全保障行动中，均以“零被黑，零事故”的优异成绩切实守护着国家的网络空间安全。与此同时，知道创宇还为国内超过 90 万家政府及企业网站提供网络安全服务，为各行业线上业务的稳健运行和健康发展提供了强有力的保障，为我国经济稳定发展做出了极大贡献。

捍卫国家网络核心资源安全、保护企业网上业务安全的同时，知道创宇也致力于公民用网安全保障，不断加大力度打击电信网络欺诈。作为国内最大网络安全公益组织“安全联盟”的主要发起及参与单位，知道创宇技术贡献网络平台级反欺诈行业标准，并将数以亿计的恶意网址黑名单共享至各级互联网平台，用于底层打击电信网络诈骗，并联合腾讯安全，配合各地公安机关、运营商，建立电信网络诈骗拦截系统，为国家打击防范电信网络欺诈犯罪贡献了力量，帮助民众有效避免各类网络风险。

安全产品悉数亮相 展现全能攻防实力

在此次安全周网络安全博览会上，知道创宇展示了多领域的网络安全研究成果和协同防治经验。

基于 AI 和大数据的驱动，知道创宇已经形成了从区域资产，到漏洞威胁，再到攻击态势全面的获取能力。自主研发的 ZoomEye 新一代网络空间雷达系统、网络空间威胁态势感知系统创宇星图、针对特殊高危领域的威胁情报感知系统创宇云图集体亮相，为探知深层次网络空间安全提供了绝佳窗口，通过可视化数据，将网络空间的资产分布、弱点漏洞、风险态势、威胁活动等信息一一掌握，将 APT 攻击消灭在萌芽状态。



伴随着基础设施、传统企业与互联网的高速融合，网络安全和信息化是一体之两翼、驱动之双轮，政府及企业的网络安全建设也在不断完善。知道创宇展示的政府 & 企业网络安全综合解决方案，以云安全防御平台为主体，由创宇盾、抗 D 保、WebSOC 等安全产品组成，配合渗透测试、代码审计、应急响应等安全服务，形成了从风险识别、到安全防御、到安全响应、再到安全恢复的一整套安全保障体系。

另外，针对今年以来层出不穷的勒索病毒和区块链安全事件，在展台也可以看到知道创宇的最新相关研究。由创宇云图、腾讯御点、应急服务组成的反勒索病毒快速解决方案，通过防病毒感染+感知病毒传播+应急响应的模式，为各关键信息基础设施系统提供覆盖云管端的立体防护。而区块链安全整体解决方案，通过打通、整合知道创宇云防御、安全服务的各项能力和大数据，建立起了从业务系统到办公网络的全生态安全保障。

同时为了提升民众的网络安全意识，现场还设置了网络安全知识科普和互动体验专区。这是知道创宇首次在国家级展会上向民众普及关于暗网的基本知识及危害，呼吁民众远离暗网，保护个人信息。展区的互动模块，则通过手机接入被恶意改装的公共充电桩，展示窃取手机通讯录、通话记录、短信、控制摄像头、远程定位等攻击过程，以直观的感受达到安全警示的目的，并针对性地采取必要防范措施。

网络安全为人民 网络安全靠人民

自 2014 年网络安全周举办以来，知道创宇也已经是第五年参展。“网络安全为人民，网络安全靠人民”是习总书记历年来重要讲话所体现的新时代网络安全观的重要内涵之一，网络安全与人民是密不可分的，每年举行的网络安全周系列活动，能够帮助民众更好地了解网络安全风险，增强网络安全意识，提高网络安全技能，保护全民合法权益，共同维护国家网络安全。

身为安全企业，也更有责任、有义务成为先行者，加强网络安全建设、加强网络安全法制宣贯，加强全民安全意识教育，加强网络安全人才培养，让网络安全的信念真正传递到你我心中。

“天府杯”网络空间态势感知论坛：发展态势感知建设 铸造网络空间国之重器

11 月 16 日，为期两天的 2018 国际网络安全大赛暨 2018 天府国际网络安全高峰论坛在成都天府新区中国西部国际博览城鸣锣开战，多场议题重磅、主题多元的行业论坛及现场招聘等活动也同期展开。

11 月 17 日上午，由知道创宇与腾讯安全共同主办的“天府杯”网络空间威胁态势感知论坛召开，数位国内顶尖安全专家出席，分享态势感知建设的宝贵经验和技术研究成果，共同探讨利用态势感知系统促进网络安全行业发展的有利之道。

▲ *“天府杯”网络空间威胁态势感知论坛现场*

网络空间威胁持续升级 态势感知渐成国之重器

网络空间威胁与挑战无处不在，建立态势感知系统来应对变化的安全变的愈加重要。公安部网络安全保卫局总工程师郭启全先生在大会致辞中表示，应习总书记关于“加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力”的重要工作指示，态势感知大平台已成为新时代整体安全观下的“国之重器”，公安主导，建立由职能部门、部委、央企、监测机构、电信运营商、互联网企业、信息安全企业、研究机构多方参与的协同防御机制体系，各司其职、各负其责，以解决我们共同面临的安全生态问题。

腾讯公司副总裁马斌先生在讲话中提到，在数字化转型这一大背景下，IT 基础设施正在发生变化，安全运营思路甚至是安全体系，也应重新构建。这一点，所有的厂商都有了共同的认知，那就是通过应用态势感知技术，对来自内外部的安全威胁进行研判和溯源，变被动受害为主动防御。腾讯安全不断通过 AI 和大数据技术驱动安全防护能力升级，推出灵鲲、麒麟、鹰眼、神荼、神侦等一系列安全产品，并持续开放安全能力，形成“智慧共治平台”，贯通态势感知能力。

知道创宇创始人、CEO 赵伟先生进一步指出，在面对新形势下的网络安全威胁，我们需构建具有高维度的上帝视角（GTP）网络攻防体系，涵盖洞察一切（认知）、洞悉一切（预判）、洞穿一切（反制）的能力，才能避免网络攻击和潜在安全风险。知道创宇凭借实时安全大数据集成了情报收集分析能力，研发网络空间雷达系统建立起网络空间作战地图，并配合云防御平台提供坚实有力的全局防御，先知先觉，捍卫国家安全。

安全行业合力深耕 五大议题指点迷津

在论坛议题分享环节，来自知道创宇的安全专家陈庆先生首先在《大数据技术驱动智慧安全感知》演讲中分享了知道创宇基于大数据技术的态势感知体系建设。依托知道创宇云防御平台、ZoomEye 网络空间搜索引擎、

Seebug 漏洞社区等，为态势感知平台提供了安全大数据支撑。应国家《网络安全法》、“十三五”规划等监管要求，以等保为起点，从数据基础赋能、监测管理赋能、案件打击赋能、综合平台赋能全面提升监管安全感知能力。

中国电科首席专家、中国网安总工程师饶志宏先生发表《以态势感知为核心的大型企业网络安全整体保障服务》主题演讲，他表示，随着大数据、人工智能、物联网等新信息技术的普及和推广，中央企业信息资产快速泛在化，受攻击面也同步扩张，防护难度急剧增加。多元融合、多核驱动的态势感知平台将开启中央企业网络安全保障“新纪元”。

中科院软件所研究员连一峰先生在其《网络安全态势感知关键技术解读》的演讲中强调，基于监测、通报、应急、追踪、监督闭环的态势感知目标定位，需要重点突破数据采集、数据治理、机器学习、知识图谱等相关关键技术，把握住业务驱动的人工智能和协同联动的技术体系要点。

来自腾讯智慧安全产品总监张鹏飞先生则带来了《腾讯安全威胁情报系统分享》主题分享，他表示，当下网络安全正在发生深刻变化，企业安全的重心正在从传统的“边界防御”到如今的“检测和响应”转移。基于 20 年技术沉淀，腾讯建立起完备的安全威胁情报库，以安全大脑为中心，输出感知、溯源、预测能力。

亚信网络安全产业技术研究院技术总监罗翔先生最后发表了《态势感知助力等保 2.0 建设的探索与实践》主题演讲，他认为，网络安全等级保护的核心是保证不同安全保护等级的对象具有相适应的安全保护能力。态势感知建设重点在于构建“外部感知、内部监管、安全可视”的“态势感知能力”，实现“威胁识别、精准监管、整体协同、预警响应”的一体化管理能力。

暗网雷达神秘发布 洞悉黑暗网络空间

在网络空间更深层的地方，暗网空间因其匿名、虚拟的特性，充斥着大量非法交易和犯罪服务，严重威胁社会、企业和国家的安全。在论坛压轴环节，知道创宇正式发布了自主研发的针对暗网空间的搜索引擎——暗网雷达，以威胁情报线索挖掘为导向，通过构建分布式暗网服务发现、内容采集、弱点探测、证据保存等平台，提供暗网服务的发现、识别、分类、采集、监测。

据暗网雷达产品总监介绍，暗网雷达旨在为相关业务人员提供高效的情报监测和分析服务，从暗网雷达的实时监测数据来看，暗网如今呈现缓慢增长的态势，随着更多的非法交易转移至暗网，监管机构获取对于暗网知己知彼的能力将变得更加重要。

当前，以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的态势感知技术，已经成为我们抵御未知威胁最锋利的武器。“天府杯”网络空间态势感知分论坛的举办，正是意在落实国家网络安全战略思想，搭建态势感知相关领域新技术交流平台，探索这项关键技术应用实践的前沿方向，以助力全方位应对网络安全威胁、保障数字经济快速发展。

安全研究

404 团队出品

助力构建安全生态，知道创宇 404 实验室多次获厂商官方致谢

知道创宇 404 实验室，国内黑客文化深厚的知名安全公司知道创宇神秘而核心的部门，长期致力于 Web、IoT、工控、区块链等领域内安全漏洞挖掘、攻防技术的研究工作，在业内享有非常高的声誉。

2018 年，知道创宇 404 实验室共跟进漏洞与安全事件应急 150 多起，发布原创分析文章 60 多篇，全部漏洞都已收录到 Seebug 漏洞平台，共获得包括 AWS、 百度云、华为云、网易云、金山云、Adobe、Oracle、Evernote 等大厂商的多个致谢。

Adobe 官方于 5 月和 7 月均发布了针对 Adobe Reader 和 Adobe Acrobat 的安全公告，并提供了安全更新指引。在具体的漏洞方面，Adobe 官方致谢了多名安全研究人员与团队，知道创宇 404 安全实验室发现并提交六个漏洞，获得了 Adobe 官方致谢。

在 5 月 14 日更新的安全公告中，知道创宇 404 实验室提交的 Use-after-free 漏洞（编号为 CVE-2018-4958 和 CVE-2018-4983），其危害性被 Adobe 定义为严重（critical）级别。

在 7 月 10 日更新的安全公告中，知道创宇 404 实验室提交的 Out-of-bounds write 漏洞（编号为：CVE-2018-5021），其危害性被 Adobe 定义为严重（critical）级别；另外三个 Out-of-bounds read 漏洞（编号为：CVE-2018-5022, CVE-2018-5025, CVE-2018-5026），其危害性被 Adobe 定义为重要（Important）级别。

10 月 4 日，Adobe 发布了 AdobeAcrobat 和 ReaderforWindows 和 MacOS 的安全更新，解决了一系列重要或高危的任意代码执行漏洞，同时 Adobe 官方致谢了多名安全研究人员与团队，知道创宇 404 安全实验室再次上榜，获得了 Adobe 官方致谢。本次获得致谢的漏洞为

8 月底的 KCon 黑客大会，由来自神秘的安全组织 0x557 的 安全大神 Bo Qu(Swan) 和 知道创宇 CSO 周景平 (黑哥) 的压轴议题《PDF JS 引擎交互式 Fuzzing》中公布的，通过一套 Fuzz 神器，结合新颖的自动化测试策略，发现一大批 Adobe Reader 的安全问题。这些安全问题在本次的安全更新中均得到了体现，Swan 与黑哥提交的漏洞，均得到了 Adobe 官方的确认并致谢。

10 月中旬，Oracle 官方也于 17 日发布了安全公告，更新包含 WebLogic 等产品在内的多个安全补丁，并提供了安全更新指引。同时 Oracle 官方致谢相关安全研究人员与团队，知道创宇 404 安全实验室榜上有名，获得了 Oracle 官方致谢。

知道创宇 404 安全实验室此次发现并提交的漏洞在该公告中的编号为 CVE-2018-3245(9.8), CVE-2018-3250(6.1)。其中 CVE-2018-3245 是存在 WebLogic T3 协议的反序列化漏洞，该漏洞评分为 9.8 分，属于高危漏洞。

2018 上半年 暗网研究报告

作者：知道创宇 404 实验室

知道创宇基于公司产品“暗网雷达”对暗网的测绘及分析编写的《2018 上半年暗网研究报告》从 Tor 节点分布，Tor 网络数据统计，以及暗网 Web 服务，开放端口及语种的可视化分析数据，以及暗网的威胁风险 等微观及宏观的数据分析和统计，阐述了我们知道创宇 404 安全研究团队在通过技术手段来测绘暗网，追踪和对抗来自暗网的威胁方面的研究成果，该报告在圈内引起广泛的关注和传播。

Weblogic 反序列化漏洞 (CVE-2018-2628) 漫谈

作者：Badcode@ 知道创宇 404 实验室

2018 年 4 月 18 日，Oracle 官方发布了 4 月份的安全补丁更新 CPU（Critical Patch Update），更新中修复了一个高危的 WebLogic 反序列化漏洞 CVE-2018-2628。攻击者可以在未授权的情况下通过 T3 协议对存在漏洞的 WebLogic 组件进行远程攻击，并可获取目标系统所有权限。

本文总结了几年内 Oracle WebLogic 反序列化的相关漏洞，梳理了 Oracle WebLogic 反序列化漏洞的攻击与防御的历程，并且着重分析了 CVE-2018-2628 反序列化漏洞，最后根据以往的漏洞利用方式，给出了另外一种绕过补丁的攻击方式。

摄像头漏洞挖掘入门教程（固件篇）

作者：fenix@ 知道创宇 404 实验室

据 IT 研究与顾问咨询公司 Gartner 预测，2017 年全球物联网设备数量将达到 84 亿，比 2016 年的 64 亿增长 31%，而全球人口数量为 75 亿。2020 年物联网设备数量将达到 204 亿。

而与如此快的发展速度相对应的，物联网的安全问题也日趋凸显，尤其是网络摄像头、路由器等常见设备。我们可以从以下两个案例大致感受一下物联网设备严峻的安全形势。

♦ 抓住“新代码”的影子 —— 基于 GoAhead 系列网络摄像头多个漏洞分析

♦ 全球 2.5 万网络摄像机被黑，用于构建 DDOS 攻击僵尸网络

物联网设备数量的快速增长和其安全性的严重滞后形成了鲜明对比。同时也给恶意攻击者和安全研究人员提供了新的土壤，这场正邪的博弈在新的战场上正激烈上演。

这是一篇详细的入门级别的教程，献给众多想入门智能设备安全的爱好者们。

从补丁到漏洞分析 -- 记一次 joomla 漏洞应急

作者：LoRexxar'@ 知道创宇 404 实验室

2018 年 1 月 30 日，joomla 更新了 3.8.4 版本，这次更新修复了 4 个安全漏洞，以及上百个 bug 修复。

为了漏洞应急这几个漏洞，我花费了大量的时间分析漏洞成因、寻找漏洞触发位置、回溯逻辑，下面的文章比起漏洞分析来说，更接近我思考的思路，希望能给大家带来不一样的东西。

印象笔记 Windows 客户端 6.15 本地文件读取和远程命令执行漏洞 (CVE-2018-18524)

作者：dawu@ 知道创宇 404 实验室

2018 年 9 月，我当时的同事 @sebao 告诉我印象笔记修复了他的 XSS 漏洞并登上了名人堂，碰巧国庆的时候考古过几个客户端 XSS 导致命令执行的案例，就想在印象笔记客户端也寻找一下类似的问题。

在之后的测试过程中，我不仅发现原本的 XSS 修复方案存在漏洞、利用这个 XSS 漏洞实现了本地文件读取和远程命令执行，还通过分享笔记的功能实现了远程攻击。

以太坊网络架构解析

作者：0x7F@ 知道创宇 404 区块链安全研究团队

区块链的火热程度一直以直线上升，其中以区块链 2.0 —— 以太坊为代表，不断的为传统行业带来革新，同时也推动区块链技术发展。

区块链是一种分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式，这是一个典型的去中心化应用，建立在 p2p 网络之上；本文以学习和分析以太坊运作原理为目的，将以太坊网络架构作为一个切入点，逐步深入分析，最终对以太坊网络架构有个大致的了解。

通过学习以太坊网络架构，可以更容易的对网络部分的源码进行审计，便于后续的协议分析，来发现未知的安全隐患；除此之外，目前基于 p2p 网络的成熟的应用非常少，借助分析以太坊网络架构的机会，可以学习一套成熟的 p2p 网络运行架构。

本文侧重于数据链路的建立和交互，不涉及网络模块中的节点发现、区块同步、广播等功能模块。

以太坊智能合约 OPCODE 逆向之理论基础篇

作者：Hcamael@ 知道创宇 404 区块链安全研究团队

在我们对 etherscan 等平台上合约进行安全审查时，常常会遇到没有公布 Solidity 源代码的合约，只能获取到合约的 OPCODE，所以一个智能合约的反编译器对审计无源码的智能合约起到了非常重要的作用。

目前在互联网上常见的反编译工具只有 porosity，另外在 Github 上还找到另外的反编译工具 ethdasm，经过测试发现这两个编译器都有许多 bug，无法满足我的工作需求。因此我开始尝试研究并开发能满足我们自己需求的反编译工具，在我看来如果要写出一个优秀的反汇编工具，首先需要有较强的 OPCODE 逆向能力，本篇 Paper 将对以太坊智能合约 OPCODE 的数据结构进行一次深入分析。

以太坊智能合约审计 CheckList

作者：知道创宇 404 区块链安全研究团队

在以太坊合约审计 checkList 中，我将以太坊合约审计中遇到的问题分为 5 大种，包括编码规范问题、设计缺陷问题、编码安全问题、编码设计问题、编码问题隐患。其中涵盖了超过 29 种会出现以太坊智能合约审计过程中遇到的问题。帮助智能合约的开发者和安全工作者快速入门智能合约安全。

本 CheckList 在完成过程中参考并整理兼容了各大区块链安全研究团队的研究成果，CheckList 中如有不完善 / 错误的地方也欢迎大家提 issue.

由于本文的目的主要是 CheckList，所以文中不会包含太详细的漏洞 / 隐患信息，大部分漏洞分析在扫描报告中会有所提及。

金钱难寐，大盗独行——以太坊 JSON-RPC 接口多种盗币手法大揭秘

作者：知道创宇 404 区块链安全研究团队

2010 年，Laszlo 使用 10000 个比特币购买了两张价值 25 美元的披萨被认为是比特币在现实世界中的第一笔交易。

2017 年，区块链技术随着数字货币的价格暴涨而站在风口之上。谁也不会想到，2010 年的那两块披萨，能够在 2017 年末价值 1.9 亿美元。

以太坊，作为区块链 2.0 时代的代表，通过智能合约平台，解决比特币拓展性不足的问题，在金融行业有了巨大的应用。

通过智能合约进行交易，不用管交易时间，不用管交易是否合法，只要能够符合智能合约的规则，就可以进行无限制的交易。

在巨大的经济利益下，总会有人走上另一条道路。

古人的盗亦有道，在虚拟货币领域也有着它独特的定义。只有对区块链技术足够了解，才能在这场盛宴中偷到足够多的金钱。他们似那黑暗中独行的狼，无论是否得手都会在被发现前抽身而去。

2018/03/20, 在《以太坊生态缺陷导致的一起亿级代币盗窃大案》和《揭秘以太坊中潜伏多年的“偷渡”漏洞，全球黑客正在疯狂偷币》两文揭秘以太坊偷渡漏洞（又称为以太坊黑色情人节事件）相关攻击细节后，知道创宇 404 团队根据已有信息进一步完善了相关蜜罐。

2018/05/16, 知道创宇 404 区块链安全研究团队对偷渡漏洞事件进行预警并指出该端口已存在密集的扫描行为。

2018/06/29, 慢雾社区里预警了以太坊黑色情人节事件（即偷渡漏洞）新型攻击手法，该攻击手法在本文中亦称之为：离线攻击。在结合蜜罐数据复现该攻击手法的过程中，知道创宇 404 区块链安全研究团队发现：在真实场景中，还存在另外两种新型的攻击方式：重放攻击和爆破攻击，由于此类攻击方式出现在偷渡漏洞曝光后，我们将这些攻击手法统一称为后偷渡时代的盗币方式。

本文将会在介绍相关知识点后，针对偷渡漏洞及后偷渡时代的盗币方式，模拟复现盗币的实际流程，对攻击成功的关键点进行分析。

创宇生活

春风吹，战鼓擂，全能 PM 我怕谁！
——2018 创宇大学 PM 训练营圆满结束

2018 年 7 月——11 月，为了提升公司产品能力，经过部门推荐和认真筛选，创宇大学开办“全能 PM 训练营”，邀请 XX 名创宇产品人共同学习共同提高。和以往培训不同的是，本次训练营采用行动学习的方式，可不是听完就完了，每个小组都要完成自己产品的商业计划书，为期五个月的学习旅途，从《品牌营销》、《商业画布》到《产品规划》、《产品管理》，先打开思路再落地规划，中间贯穿老杨的点评和传授，不断打磨自己产品的商业计划，在最后的模拟路演中去争取总裁办的投资。

第一次集结，我们一起打开了商业思路和视野，《品牌营销》和《商业画布》的课程我们记忆犹新。

第一次汇报，BOSS 们百忙中为大家点评指导，小伙伴们聚集智慧，发散思维，互相沟通交流。IC 和老杨还为大家分别讲述了《新时代的网络安全观》、《赋予产品灵魂》。小伙伴们都表示受益匪浅。

第二次课程 《产品规划与设计》，大家一起学习产品需求规划和管理，深刻把握客户需求并快速实现。

模拟路演开始啦 ~ 汇报中明显感受到了大家的变化和成长，每个人都更加重视市场和需求的分析了。

各位投资人，每人 100 万的资金，为心仪产品投资。最终王字同学获得胜利，登上了最高的领奖台，独自捧获 5000 奖金和奖杯 ~

虽然今年的全能 PM 训练营已经结营啦，但我们的学习之旅还在继续。产品能力是公司的核心竞争力，产品能力建设是关乎公司生死存亡的问题。相信我们的 PM 们会为提升公司产品能力而共同努力，期待你们成为赋予产品灵魂的人。

让知道创宇越来越好，让互联网更好更安全。春风吹战鼓擂，全能 PM 我怕谁！

匠心 11 周年 知道创宇 11 岁生日快乐

2018 年 8 月，正值七夕佳节之际，知道创宇迎来了自己的 11 岁生日。

11 年的发展离不开全体伙伴的努力，在前进道路上，我们遇到了越来越多的创宇同路人，至此 11 周年，让我们感恩为创宇辛勤工作努力奋斗的伙伴们。特别有这样一群人，他们加入创宇后，得到了成长与发展，他们感恩着平台赋予的机会，创宇也感恩他们的付出和努力。

星星之火可以燎原，点点星火光可照亮夜空，为了传承创宇文化，公司启动星火计划。在创宇，有这样一群人，一直以来信守并践行创宇文化，是文化的代表者。公司任命一些小伙伴为创宇文化星火，授予他们星火币，佩戴星火专属工牌，希望他们可以将星火的力量传递给创宇小伙伴中去。

2007 年，在北京回龙观的一个三居室里，知道创宇成立了。发展至今，知道创宇已经从最初的几个人成长为销售和技术服务体系覆盖全国的专业网络安全公司。

这十一年的技术积淀，让知道创宇成长为国家网络安全背后的坚实力量，作为国家及多省市地区多部门及行业组织的网络安全技术支撑单位，知道创宇连续多年参与到各项国家级会议、活动的网络安全保障工作，全部以“零被黑，零事故”的优异成绩切实守护着国家的网络空间安全。

匠心 11 年，精彩因你一路同行。

2018“启航”系列培训完美收官，创宇大学助你展翅高飞

17 年末创宇大学发起“启航”初级领导力培训第一期，收到了参加培训的小伙伴的一致好评。18 年“启航”“启航”初级领导力培训相继在成都和北京开班，再次得到了大家的热情报名。接下来一起回顾一下创宇大学“启航”初级领导力培训小课堂吧 ~

“用心主动”的态度，“以终为始”的愿景，"要事第一”的把握，“双赢思维”的互赖，“知彼解己”的沟通，“统合综效”的合作，“不断更新”的创造，会使每一个人走向世成功的彼岸。

启航项目完美收官

▲ *全程打卡的伙伴获得了创宇大学初级领导力资格认证，作为职级晋升的加分项*

“启航”是创宇大学针对一线管理者的领导力培养项目。有些伙伴初级登上管理岗位，从个体贡献到团队领导，如何完美转型？有些伙伴有一定带领团队经验，但都是自己的实践总结的“野路子”，科学规范高大上的方法工具是什么，如何寻求突破？

“启航”希望可以满足这两类伙伴的需求。

第一课，17 年 Q4，《管理角色认知》。改变从心开始，管理者的角色究竟是什么？有哪些取得成功的黄金法则？

第二课，18 年 Q1，《目标与绩效管理》。如何设定目标并管理过程？如何有效地做出绩效评估和辅导反馈？

第三课，18 年 Q2，《团队建设》。如何分工授权？如何激励批评？如何打造一支有凝聚力的团队？

第四，18 年 Q3，《高效能人士的七个习惯》。不断提高自我，才能让团队越走越高。高效能的习惯是什么？如何养成？

四门课程，为时一年的学习旅程，武装知识和技能，在实际工作中不断磨砺提升。

今年度的“启航”落幕了，管理道路上的升级打怪不会停止。愿所有参加过启航培训的学员们，卓有成效，一起共创创宇未来。

创宇大学明年继续“启航”，新任 LEADER 们，等待你们整装出发。

▲ *优秀学员*

各部门采风

▲ 线下大客户部

▲ 市场部

▲ 云安全事业部网销一部

▲ 云安全事业部网销二部

▲ 云安全事业部运营管理部

▲ 人力行政部

▼ *PTC 部*

▲业务安全产品线 - 业务支撑团队

▼ *方案解决部 & 新业务部*

▲ *PTC 部*

▲ *ScanV 团队*

▲政企事业部华东区

▲ 在线产品线


俠之大者
為國為民