居安思危，洞见未来

——四叶草互联网安全服务创新案例

随着信息技术和网络的快速发展，物联网、大数据、人工智能等新技术得到广泛应用，网络安全威胁的范围和内容不断扩大和演化，网络安全形势与挑战日益严峻复杂。西安四叶草信息技术有限公司，简称“四叶草安全”，成立于2012年8月3日，是一家以安全服务及产品开发为主的互联网安全企业，秉承“居安思危，洞见未来”的发展理念，专注于为客户提供网络信息化安全服务，致力于帮助用户先于黑客发现并及时解决安全问题，是国内安全行业发展最快的创新型企业之一，是国内外安全检测领域的领军企业，拥有全球最快最准的分布式漏洞检测能力和产品，拥有最接近实战环境的黑客攻防靶场和人才培养体系。

一、四叶草互联网安全服务创新的背景

中国网络安全形势面临复杂化、多元化和新型化的安全新形势，网络威胁全球化特征也日益明显。网络安全是一个生态系统，需要互联互通，深度融合，加强合作，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。目前无论是党政军以及一些大型企业，面临的数据跟踪、商业竞争背后黑客的驱动力越来越大，客户需求慢慢变成刚需。再加上《中华人民共和国网络安全法》推出，企业安全投入开始增多。对于企业来说，安全并非产出服务，但它可以保障企业不被黑客行为伤害造成商业损失。

四叶草安全成立于2012年8月，立足西安、服务全国，目前在北京、杭州、成都、重庆、郑州、兰州等地成立办事处和售后服务机构。凭借着在网络安全领域的专注与创新，为客户提供更专业的网络安全产品、网络安全服务、网络安全解决方案、网络安全认证培训及网络安全赛事支撑等。业务范围覆盖政府、运营商、互联网、教育、金融、能源、企业等。

经过6年的发展，四叶草安全已是国家高新技术企业、硬科技优秀企业、培育独角兽企业，CNCERT技术支持单位、CNNVD技术支撑单位、CNVD技术组单位，拥有数十项技术专利和完善的网络安全服务资质证书；是国内多所高校的人才实践单位；与华为、百度、腾讯、阿里、蚂蚁金服等达成战略合作；服务过3100+安全服务项目，20多个省份的运营商和近百家地方银行；保障过党的十九大、“一带一路”高峰论坛、金砖国家峰会、G20、文博会、贵阳大数据等大型政府活动的网络信息安全。

四叶草安全坚持自主创新和掌握核心技术，让安全风险可控，防御更简单。研究领域涉及渗透测试、代码审计、逆向分析、移动终端安全、物联网安全、黑客行为分析、智能算法、漏洞数据的建模和安全人工智能等。

二、四叶草互联网安全服务创新的主要做法及成效

（一）主要做法

四叶草安全基于丰富的安全经验、完备的专业团队、扎实的行业基础可实时跟踪国内外最新安全动向，专注于Web安全、软件安全、移动终端和IoT/物联网/工控安全，覆盖渗透测试、代码审计、逆向分析、漏洞研究、移动端安全、工控安全、智能化物联网安全、App安全评估、软件安全性测试等多个领域，向客户提供高效专业的全方位安全服务工作。四叶草安全的创新业务主要包括：

1. 全时风险感知平台Bugfeel，简称“感洞”（Bugfeel），是国内首款基于插件模式的分布式在线扫描平台，该平台基于黑客视角，拟黑客攻击手法，利用智能匹配算法还原攻击路径并进行漏洞风险建模，对可能引发网络安全风险的资产进行全面、快速和准确的实时感知，实现漏洞无缝全自动实时监测，第一时间、先于黑客发现产品存在的漏洞安全隐患，使漏洞在被利用攻击前已经被修复，做到用户先于黑客发现并解决自身安全问题。该平台包括漏洞可视化、漏洞风险感知、可用性检测、专业风险监测报告、风险通报预警五大功能，开启了主动安全防御时代。

2. 四叶草安全实验室（CloverSec Labs）。实验主要负责安全漏洞研究，最新安全资讯跟踪，安全事件病毒木马分析，知名漏洞提交平台提交相关漏洞与申请CVE和漏洞资质，在各SRC平台提交相关漏洞。实验室下设四个研究方向分别是二进制软件漏洞挖掘、Web漏洞挖掘、移动终端漏洞挖掘和IoT设备漏洞挖掘方向，其中二进制软件漏洞挖掘主要负责0day级漏洞挖掘与分

析；Web 漏洞挖掘负责最前沿的 Web 框架漏洞研究与大型 CMS 的审计；移动终端漏洞挖掘主要负责 Android 和 IOS 的系统与 App 的漏洞挖掘；IoT 设备漏洞挖掘主要负责 IoT 设备的安全研究。另外实验室还负责攻防实验搭建、CTF 赛事组织、安全培训等。

3. 漏洞插件社区 Bugscan（bugscan. net）。是为广大信息安全爱好者打造的学习、交流、分享信息安全资源，集中提供信息安全工具的综合平台。社区由资源区、论坛区、工具区、文档区、商城区、擂台赛区六大板块组成，资源区供用户提交查看最新漏洞、插件、特征等，社区成员通过提交资源可以获得相应的贡献值；论坛区与文档区提供了各种安全技术的普及文章，最新安全技术的研究文章，安全资源收集的教学文章，漏洞检测插件的学习教程等，是用户交流学习信息安全最新热点话题的平台；商城区与工具区为社区成员提供众多优秀的安全工具，这些工具可以在社区成员进行安全测试或编写漏洞检测插件过程中提供帮助，同时社区成员可以将自己编写的安全工具在社区内分享；擂台赛区定期举行与渗透、逆向等技能相关的夺旗赛，旨在训练参阅人员的实战经验，培养渗透及逆向技能的人才。六大板块紧密结合，将漏洞检测插件、实用安全工具等众多的安全资源收集整理，为安全爱好者提供最新、最全的安全资源支持。同时，该社区聚集的众多安全人才和资源，为全时风险感知平台提供了最新的、准确的、高效的漏洞检测插件，实现了安全资源的最大化利用。

4. CLS - ADP 四叶草安全攻防平台。该平台借助虚拟化技术，模拟安全研究与渗透评估中可能遇到的环境，构建攻防私有云平台和各式各样的网络攻防环境。该平台集网络安全基础学习、网络攻防实训、网络安全实验、攻防竞赛训练场、网络安全场景、单兵作战、红蓝对抗和团队对抗等功能于一体的网络安全攻防实验室，实现教学、实验与实操一体化。

（二）主要成效

四叶草安全发现苹果 AirPlay 协议认证漏洞、独立技术承办 SSCTF 全国信息安全挑战赛、独立技术承办宁夏回族自治区全国信息安全挑战赛、独立技术承办“华山杯”全国信息安全技能赛、参加互联网嵌入式漏洞挖掘比赛，对某知名厂商提供的设备进行漏洞挖掘，提交了 5 个高危漏洞、多次参与各网络安全与安全竞赛的培训。已拥有 18 项软件著作权和 2 项发明专利，服务 20 多个省份的运营商和近百家地方银行，与百度、腾讯、阿里、360、蚂蚁金服等知名互联网企业结为战略合作伙伴，完成超过 2100 个安全服务项目，保障过党的十九大、G20、文博会、贵阳大数据等大型政府项目和活动的网络信

息安全，是国内多所高校的人才实践单位，业务范围覆盖政府、运营商、互联网、教育、金融、能源、企业等。

自2014年起举办多届SSCTF全国网络安全大赛，大赛旨在为中国安全行业塑造更为强劲的后备力量。2016年、2017年连续主办SSC（全称：CloverSec Security Conference）安全峰会，会聚了全国行业大咖、网络安全精英及白帽子近千余人参会，是中西部规模最大、规格最高、影响力最广的网络安全盛会。

三、四叶草互联网安全服务的政策启示

古往今来，很多技术都是“双刃剑”，一方面可以改变我们的生活，造福人类，另一方面也可以被一些人利用从而危害社会，危害人民。尤其是互联网时代的快速发展，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。

2018年11月初，《人民日报》刊发题为《引领网信事业发展的思想指南》文章，阐述了习近平总书记就网络安全和信息化工作作出一系列重大决策，提出一系列重大举措。“金融，能源，电力，通信，交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。不出问题则已，一出就可能导致交通中断，金融紊乱，电力瘫痪等问题，具有很大的破坏性和杀伤力”。网络安全一时引发我们的思考和探讨。

“时至今日，网络信息安全早已超出了电脑中毒，网站被黑，数据丢失的程度，而是达到了会威胁生命的地步。”马坤，西安四叶草信息技术有限公司的创始人，开门见山地道出了当今网络信息安全的重要性。从2012年开始创业至今，四叶草安全从未停下创新的脚步，将捍卫网络信息安全作为己任，誓与攻击网络安全的黑暗力量对抗到底。

从明确提出“没有网络安全就没有国家安全”，到突出强调“树立正确的网络安全观”，再到明确要求“全面贯彻落实总体国家安全观”，网络信息安全的重要性与日俱增。

互联网无处不在的当今，大到国家关键基础设施，小到每个人的衣食住行，都与网络信息安全息息相关。同时，伴随着网络技术的日新月异，信息化渗透进每个人的工作与生活。带来前所未有的舒适与便捷体验感的同时，隐患也如影随形。

在大数据时代，安全只会变得越来越重要。可以说，网络信息安全与军工、航空航天、交通物流、能源电力，以及医院、学校各个领域紧密相关。“高铁，地铁的运行信息系统，家中的指纹锁，虹膜识别系统，购物消费时存储在云端的数据……只要有联网的信息化系统，就需要坚实的网络信息保障后盾。”关键核心技术的薄弱，让互联网产业的繁荣发展仿佛一株缺失土壤的盆景。

每个行业都像是一棵树。枝叶越向高处攀长，根脉也必将更深一分。对于网络信息安全行业而言，攻击手段与防御手段亦是如此，此消彼长，需要持续相互动态制衡。在信息化突飞猛进的今天，网络安全通过不断加固地基的方式应对攻击，该行业的技术创新永远都在路上。

四、四叶草互联网安全服务创新的下一步工作思路

四叶草安全研究院将坚持核心技术的研发及产品创新，运用具有自主知识产权的安全产品和掌握自主可控、安全可信的网络安全核心技术，助力网络强国建设。

作为聚焦 Web 以及应用层面检测的四叶草在这轮融资之后也将对产品进行一些细分。比如可能按照行业去划分，或者为客户进行定制，做出不同的版本。

目前主要客户是政府运营商、金融、互联网企业，未来会按照现有的几个行业进行划分。因为每个行业用户使用的操作系统、数据库，以及它的网络环境、资产种类是不一样的，而有了很多客户案例之后，有利于做这种产品的划分。同时，有竞争也会有合作。对于主机层面的漏洞扫描，更为需要特征，而对应用层面的漏洞扫描，行为则更为重要，所以四叶草也会与同行进行互补，联合做项目。

四叶草安全将继续坚持技术创新，掌握核心技术，秉承“居安思危 洞见未来”的发展理念，携手合作伙伴共同守护亿万网民的网络信息安全、共同携手构建一个安全的网络环境，共同营造一个安全的互联网生态。

【实践者说】

在四叶草安全公司创立者马坤看来，自家的“娃娃”是有个性的，这种个性更多是在行为层面发现用户的漏洞，而不单纯地依靠特征。“传统厂商的漏洞扫描平台多依靠特征发现一些漏洞，即针对一条条呆板的规则进行比对发现，可以把它理解成杀毒软件扫描病毒的方式。而四叶草通过多年的安全

服务项目和社区，集成了大量的黑客行为模型，并把这种模型加之以特有算法，初步实现了一些人工智能，然后让产品自动化地模仿人的行为，发现用户漏洞。”

模型的搭建少不了数据支持，马坤在接受采访时说道：“四叶草得到的这些数据依托之前搭建的分布式漏洞扫描社区，目前注册人数超过两万，每天活跃人数500—1000人。这些白帽子会在社区发布如何验证漏洞的插件，而这些插件即四叶草所收集的数据，也就是黑客行为模型。每天所能收集到的二三十个插件就是模型更新迭代的‘原料’。”马坤也将这种方式比作“互联网的众筹模型”。

【案例点评】

“四叶草安全”专注于为客户提供网络信息化安全服务，致力于帮助用户先于黑客发现并及时解决安全问题，是国内安全行业发展最快的创新型企业之一，是国内外安全检测领域的领军企业。“四叶草安全”携手合作伙伴共同守护亿万网民的网络信息安全、共同携手营造一个安全的网络环境，对于共同打造一个安全的互联网生态具有重要意义。

四叶草安全