MCK主机加固解决方案

数据安全解决方案专家

CNSINDA

CONTENT

PART 01
公 司 简 介

关于我们

苏州深信达成立于2008年，是国家高新技术企业和国家软件企业，是国内数据安全解决方案供应商，拥有国内顶尖的安全研发团队，在操作系统内核级纵深防御技术、虚拟沙盒技术、外设端口过滤等专业级技术方面，在国内，拥有绝对的领先优势。

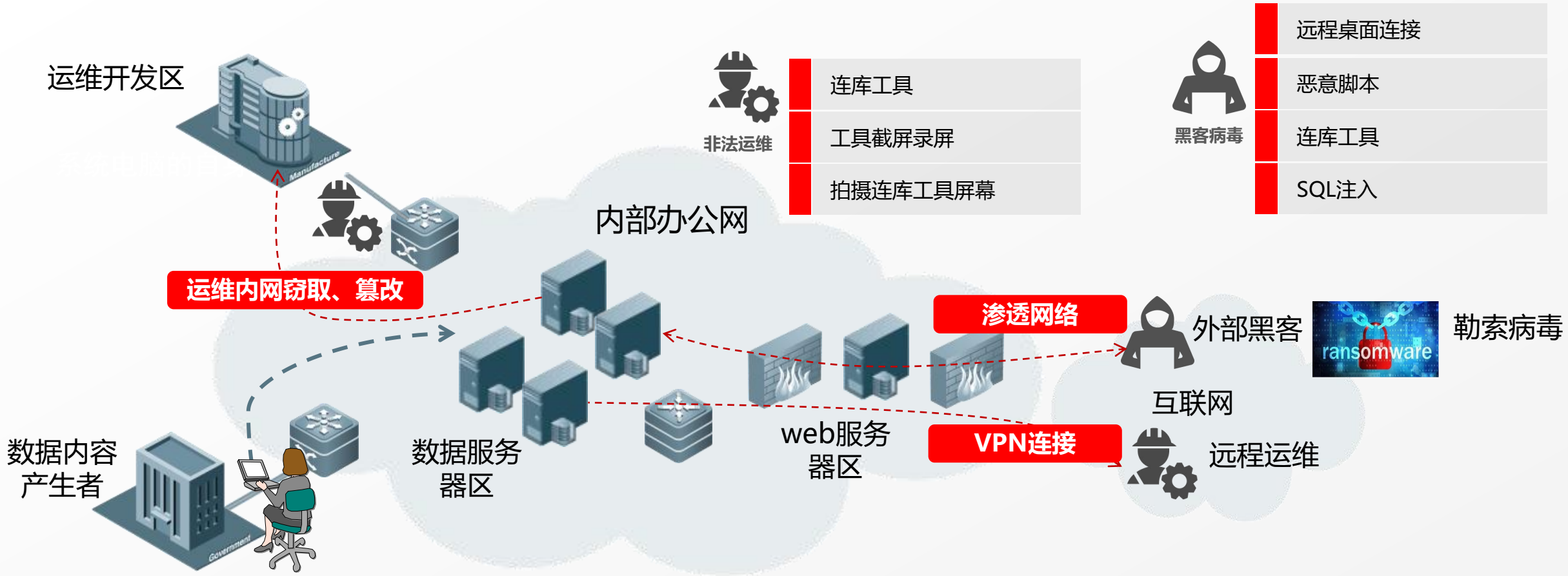
公司自2008年创立至今，专注数据加密和主机加固领域，从服务器安全、到用户终端安全，再到工业互联网安全，打造了一套完整的数据安全解决方案。

公司产品先后获得了公安三所检测和国家保密局检测，获得了公安部信息安全产品专用销售许可证和保密资质。旗下的研发数据防泄漏、服务器数据安全、智能终端数据安全、智联网的数据安全、智能工业设备终端安全、智能仪器仪表数据安全等安全产品，获得广泛用户认可和好评。

PART 02

安 全 现 状

数据安全主要面临三类威胁：泄密、篡改、损毁。



勒索病毒横行

2019年3月份

全球最大铝制品生产商之一的Norsk Hydro遭遇勒索软件攻击，公司被迫关闭多条自动化生产线，震荡全球铝制品交易市场。

2018年8月3日

台积电被曝出在台湾地区的三大厂区遭病毒入侵，直到8月6日台积电官方才发表声明称已经恢复生产。

2019年6月

全球最大飞机零件供应商ASCO遭遇勒索病毒攻击，生产环境系统瘫痪，大约1000名工人停工，四国工厂被迫停产。

2020上半年

勒索病毒依旧十分活跃。但总体感染情况较去年略有下降。从勒索病毒攻击的地区分布看，广东、浙江、山东、河南、上海等经济较发达地区成为重点目标，其它省份也遭受到不同程度攻击。从勒索病毒影响的行业看，数据价值较高的传统企业、教育、医疗、政府机构遭受攻击最为严重，互联网、金融、能源行业紧随其后，也遭到勒索病毒攻击影响，同时黑客攻击更精准，不交赎金立即公开敏感数据。

内部运营泄密

2018年10月

西二旗某科技公司发生代码泄露。陈某是该科技公司原运维主管，通过非法手段提高自己系统操作权限，从而获取大量自己本无权限接触到的核心代码，并通过自己的账号进行下载。

2019年2月24日

微盟官方发布公告表示：SaaS业务数据遭到一名员工“人为破坏”，故障发生后排查发现大面积服务集群无法响应，生产环境及数据遭受严重破坏。经查，本次故障是微盟核心运维人员贺某因个人精神、生活等原因，通过个人VPN登入公司内网跳板机，对微盟在腾讯云上的线上生产环境进行了恶意破坏。

2019年3月

阿里云发生因隐私权限设置错误而导致的大规模用户资料泄露事件，涉及40余家企业、200余项目，只要登录阿里云旗下的云校平台，就能够浏览很多公司的“内部”代码，而这些内部代码中就包含一些用户的个人隐私信息，如身份证号、手机号、手持身份证照片等，以及企业的重要商业秘密，如销售人员报表。

徐州市云龙区人民检察院诉被告人吴某某侵犯公民个人信息罪一审刑事判决书

发布日期：2020-04-17　　浏览：72次

江苏省徐州市云龙区人民法院
刑 事 判 决 书

（2019）苏0303刑初517号

公诉机关徐州市云龙区人民检察院。

被告人吴某某，女，1989年5月16日生，汉族，大学文化，凯芙曼（上海）贸易有限公司员工，现住上海市宝山区，户籍地上海市松江区。2019年1月25日因涉嫌侵犯公民个人信息罪被抓获并被临时羁押于上海市浦东新区看守所，2019年1月26日被刑事拘留，2019年3月1日被取保候审。

2019年4月

B站的网站后台工程源码也遭恶意泄露，被一个名为“openbilibili”的用户放到了开源项目平台Github上。“哔哩哔哩 bilibili 网站后台工程源码”的repo，内容包含了项目规范和负责人信息两部分，后者还涵盖了详细的业务、具体负责人等信息。

PART 03

产 品 介 绍

方案介绍

深信达公司研发的MCK主机加固解决方案，可以完美的解决服务器的数据安全风险，方案的核心是通过安全容器中间件技术，建立内核级纵深立体防护体系，保障服务器的安全稳定运行。系统设计理念颠覆了传统的系统管理员权限最大的理念，即使是木马病毒或黑客掌握了系统的管理员权限，仍然能有效保持服务器的稳定运行，确保存储的业务数据免受篡改和偷窥风险。

核心功能：

可信系统

场景白名单

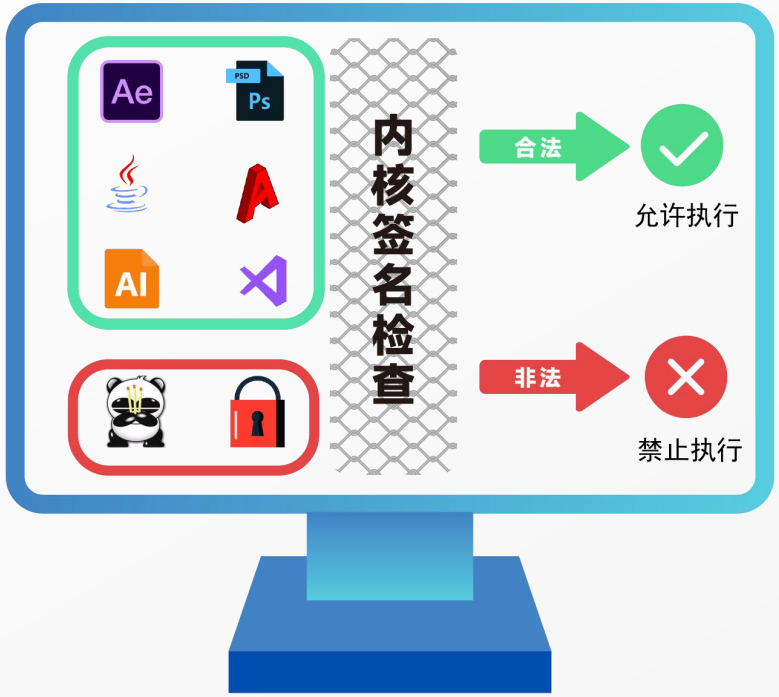
数据库保护

文件保护

四个防御功能模块，各功能模块既能相互独立搭配组合使用，几何级提升主机的安全级别。

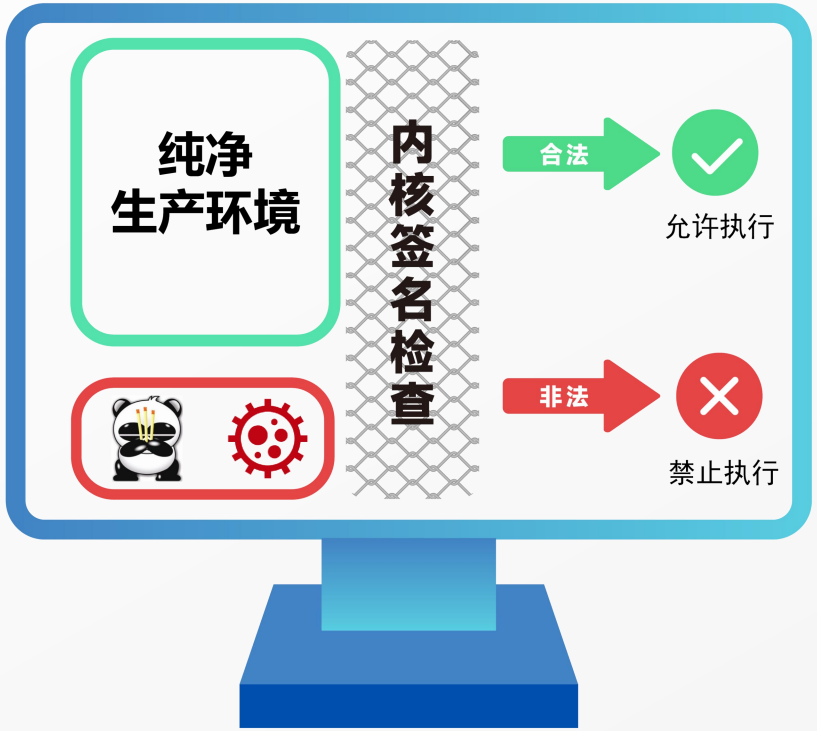
可信系统

通过独有的内核级签名校验技术，对操作系统启动及后续过程中的加载模块进行可信认证。并通过签名机制对加载的模块进行签名授权，未经签名的进程及可加载模块无法运行，根源上杜绝病毒，木马的运行机会，确保OS层安全。需要说明的是，即使管理员权限，也无法启动未经签名认证的程序，确保主机安全。



场景白名单

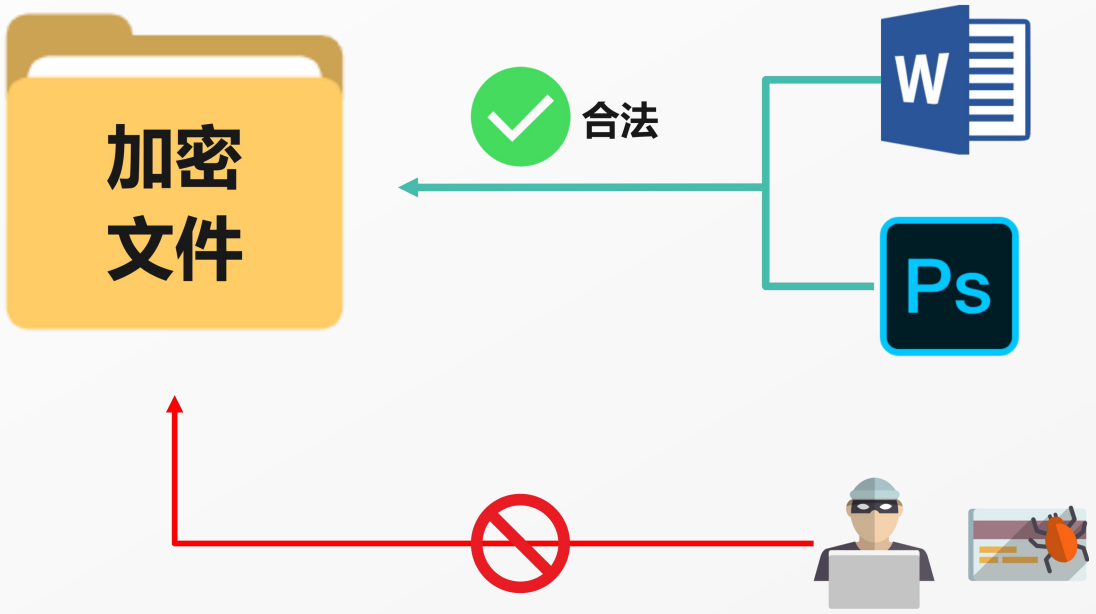
对主机进行深度学习，对业务程序、加载的模块，数据读写，网络行为等行为，建立数学算法模型，形成业务场景白名单，场景白名，只允许做业务相关的事情，其他行为一律禁止，此时业务系统稳定运行，但非业务需要的，即使一个命令行或脚本都无法运行，确保主机稳定运行。



关键文件防护

根据最小化权限原则，对主机内业务数据进行加密和权限访问控制，只允许指定的业务程序读/写指定的数据和文件，确保数据和文件的安全。同时通过数据文件的访问控制、定时监控以及数据对比还原功能，防止数据被篡改和偷窥。

例如，对指定目录下文件进行保护，或对指定格式的文件(如.docx、.pptx等格式的文件进行保护，只允许合法的安全的访问，禁止非信任访问，不给病毒木马和黑客任何机会。通过数据文件保护，对指定格式文件进行定期备份，确保数据随时可恢复，可以有效杜绝病毒等文件篡改或偷窥行为。



对于网络内的数据库，可以进行三层保护

数据库

文件保护

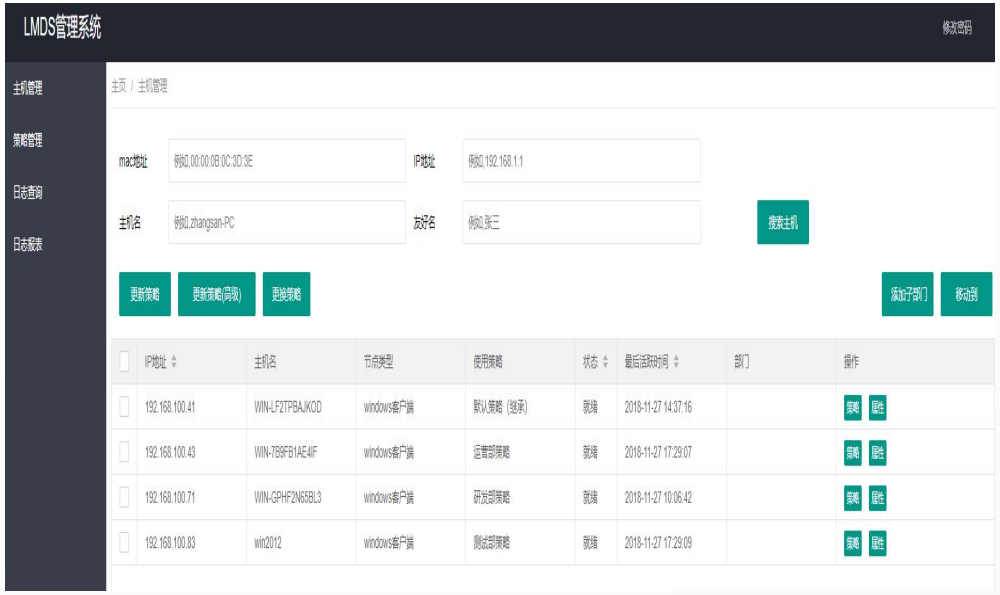
数据库文件禁止陌生程序访问和篡改。确保数据库文件级安全。

身份识别

数据库端口访问可信过滤，只允许业务程序进行数据库端口通信连接，在连接字符串的IP+端口+账号密码中，追加进程身份识别。

智能过滤

数据库连接SQL文进行智能过滤，防止关键数据被检索和访问，防止数据库内数据被非法访问，防止数据库表单的危险操作行为。



其他功能

1、客户端上传通信可选择走加密的网络隧道通信。

2、主机加固客户端，可通过Web管理控制台进行可视化管理。

3、通过集中安全监控报警平台，可以处理发现的安全事件。

分项名称	功能描述
总体要求	★采用主动防御机制，使用基于操作系统内核级的安全加固技术。国产品牌，具备自主知识产权，全中文操作界面。系统支持C/S架构，有统一控制平台，平台除了可以对各服务器进行集中统一管理、策略下发、日志审计外，还具有实时告警、状态分析处理等功能。
自身安全要求	★具有自我保护机制，对产品自身文件、重要敏感信息进行安全隔离保护，禁止对产品自身的非法操作；具备防非法卸载的能力。（提供操作界面截图证明）
执行程序控制	★采用白名单方式对执行程序启动进行实时的hash值校验，校验不通过拒绝启动，阻止非授权程序运行。（提供操作界面截图证明）
	对Windows系列操作系统，执行程序控制类型包括：PE格式文件、脚本文件。
	对类Linux系列操作系统，执行程序控制类型包括：ELF格式文件、脚本文件。
	★提供程序安装接口，控制程序安装行为，禁止非授权的程序安装行为。（提供操作界面截图证明）
	★提供增量扫描接口，可通过对系统新增或变更的程序或脚本文件进行扫描。（提供操作界面截图证明）
文件强制访问控制	支持配置进程对文件和目录的访问控制策略，权限包括读、写、所有权限、禁止所有操作。
基于工作场景的安全管控	可以限制由于业务应用程序(如tomcat/iis等)本身的漏洞对系统造成的危害。
	可以限制由于操作系统的0day漏洞对系统造成的危害。
网络控制机制	支持对系统出入栈的网络数据包进行过滤，包括IP/端口/数据包内容过滤。
产品资质要求	★《计算机信息系统安全专用产品销售许可证》、《计算机软件著作权登记证》、《涉密信息系统产品检测证书》。（提供证明材料复印件加盖原厂商公章）
	★提供产品原厂商出具的三年售后服务承诺函盖章原件。
主机实时监控	支持实时监控部署了操作系统安全加固软件的主机遭受攻击的情况。
安全审计管理	★支持对部署了操作系统安全加固软件的主机用户、文件、进程、策略加载、管理平台的操作行为审计。（提供操作界面截图证明）
管理功能要求	能够对系统中的所有服务器进行统一策略配置；支持策略实时更新、策略导入和导出功能。（提供操作界面截图证明）
	能记录运维员、系统管理员在安全管理中心上的操作行为。

PART 04

应 用 案 例

成功案例介绍

内蒙古某电力有限公司

项目需求： 2020年1月，内蒙古某电力有限公司出现“关键目录中文件/权限变更”告警信息，要求监控主机、五防主机、光功率预测等主机进行安全加固工作，防止并网电厂网络危险蔓延，确保电力监控系统安全可靠运行。

部署情况： 1期已完成验收：

Windows服务器部署 MCK安全加固软件。

所有linux 服务器部署MCK安全加固软件。

实施效果： 系统经测试安全稳定运行，免受勒索病毒攻击威胁。

成功案例介绍

贵州某流域开发公司

项目需求： 2020年6月根据国电投安全需求，公司需组织实机内部安全攻防演练，主要针对蠕虫，勒索病毒攻击，要求有效阻止外部存储设备携带病毒对服务器主机的攻击，以及勒索病毒对重要服务器的数据攻击，要求保证数据服务器安全可靠运行。

部署情况： 1期已完成验收：服务器部署MCK安全加固软件

实施效果： 经过内部攻防演练对抗，目前稳定运行，有效防止勒索病毒威胁。

客户案例


HUAWEI
mindray 迈瑞
大疆创新
Hytera 海能达
宇通客车
TRANSSION 传音控股
Sefonsoft 四方伟业
MGI 华大智造
国家电网 STATE GRID
商汤 sensetime
BOSCH
Midea
CONTEC 康泰医学
GSK 广州数控
魔视智能 MOTOVIS
中国邮政储蓄银行 POSTAL SAVINGS BANK OF CHINA
ZLG 致远电子
WEIHONG 维宏数控
投哪网 touna.cn
索菲亚 全屋定制
中国矿业大学
YUE
KONKA 康佳
LEXY 莱克 It's KingClean
鸿业科技 HONGYE TECHNOLOGY
天海 TIANHAI
树根互联 ROOTCLOUD
国泰君安证券 GUOTAI JUNAN SECURITIES

感谢您的观看

CNSINDA

深信达