

站在云端看企业安全

乌云 章华鹏

关于我

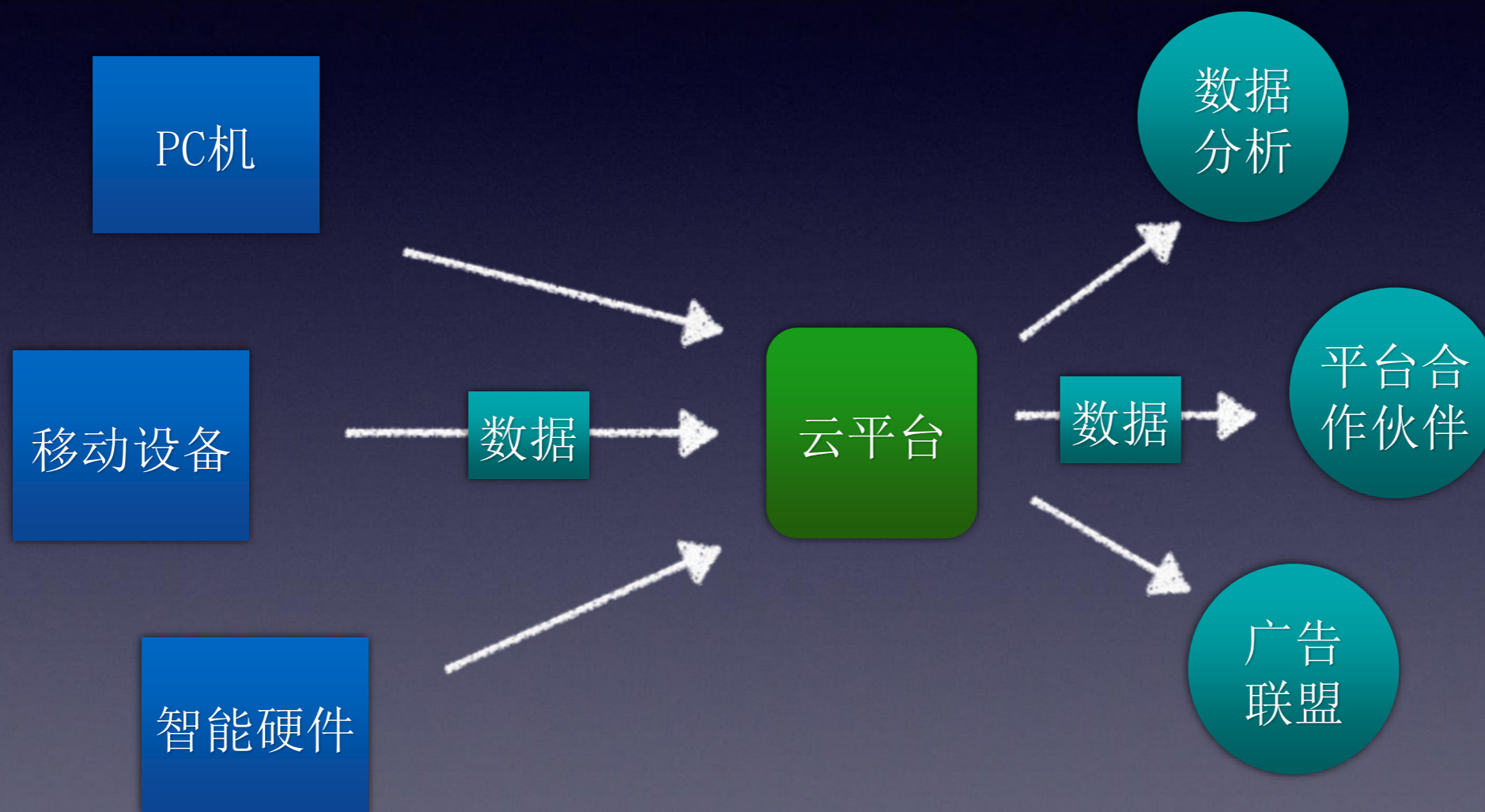
- 独立思考的白帽子黑客，boooooom
- 前百度高级安全工程师
- 乌云，唐朝安全巡航产品负责人
- <http://www.tangscan.com>

“企业安全的本质是数据安全”

“云给企业&安全带来的变化”

“数据边界正在消失”

用户



“用户数据边界消失带来什么样的问题？”

用户数据泄露

当前位置 : [WooYun](#) >> [漏洞信息](#)

漏洞概要

关注数(131) [关注此漏洞](#)

缺陷编号 : **WooYun-2013-44069**

漏洞标题 : 任意用户密码修改 (危急 手机卫士、云盘、浏览器云同步, 可泄露通讯录、短信、通话记录等)

相关厂商 :

漏洞作者 : **JiuShao**

提交时间 : 2013-11-26 17:00

公开时间 : 2014-01-10 17:00

漏洞类型 : 设计缺陷/逻辑错误

危害等级 : 中

自评Rank : 10

漏洞状态 : 厂商已经确认

漏洞来源 : <http://www.wooyun.org>

Tags标签 : [逻辑错误](#) [安全意识不足](#) [认证设计不合理](#) [平行权限](#)

分享漏洞 : [分享到](#) [+](#) [0](#)

21人收藏 [收藏](#)

用户数据泄露

- 云端任意用户密码重置

- http://i.***.cn/findpwd/set%2Fw1jiqD9WGv%2FwDyS93Bghve1cnSDZP3qIW4deYwnCpkdbCSZ3I2FBXxk6qo5oABIr6ZrywAoPB8D2%3D&qid=507290669



用户数据泄露

当前位置：WooYun >> 漏洞信息

漏洞概要

缺陷编号：**WooYun-2016-174070**

漏洞标题：智能快递柜安全之武汉智码开门域名+服务器沦陷（我来帮你取快递）

相关厂商：**武汉智码开门电子科技有限责任公司**

漏洞作者：**路人甲**

提交时间：2016-02-01 10:53

公开时间：2016-03-14 15:10

漏洞类型：用户资料大量泄漏

危害等级：高

自评Rank：10

漏洞状态：未联系到厂商或者厂商积极忽略

漏洞来源：**<http://www.wooyun.org>**，如有疑问或需要帮助请联系 help@wooyun.org

企业

- HR
- CRM
- 财务
- ...



“企业数据边界消失带来的安全风险？”

企业数据泄露

- https://crm.***.com/json/oa_profile/card.action?uid=xxxxxx
- 把uid改成六位数，即可以查看客户信息

行业

- 医疗
- 金融
- 出行
- ...

“传统行业互联网+带来的新的威胁”


传统行业互联网+风险

当前位置 : [WooYun](#) >> [漏洞信息](#)

漏洞概要

关注数(5) [关注此漏洞](#)

缺陷编号 : **WooYun-2015-101807**

漏洞标题 : 市肿瘤病例报告卡管理系统存在弱口令 (可影响3.8W多名肿瘤患者的个人信息)

相关厂商 : **cncert**国家互联网应急中心

漏洞作者 : **机器猫**

提交时间 : 2015-03-19 10:04

公开时间 : 2015-05-04 17:24

漏洞类型 : 后台弱口令


危害等级 : 高

自评Rank : 12

漏洞状态 : 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源 : <http://www.wooyun.org> , 如有疑问或需要帮助请联系 help@wooyun.org

Tags标签 : 无

分享漏洞 :  0

0人收藏  收藏

存在弱口令 admin admin 即可登录。


传统行业互联网+风险


当前位置: [WooYun](#) >> [漏洞信息](#)

漏洞概要

关注数(40) [关注此漏洞](#)

缺陷编号: **WooYun-2015-109734**

漏洞标题: 某站未授权访问+命令执行导致十几亿资金可随意操作

相关厂商: 贷

漏洞作者: [杀器王子](#) ▾

提交时间: 2015-04-22 20:43

公开时间: 2015-06-08 18:20

漏洞类型: 命令执行


危害等级: 高

自评Rank: 20

漏洞状态: 已交由第三方合作机构(cncert国家互联网应急中心)处理

漏洞来源: <http://www.wooyun.org>

Tags标签: 无

分享漏洞: [分享到](#)  0

5人收藏 [收藏](#)

互联网+的风险分析

- 互联网业务起步阶段
- 安全作为一个高阶的需求
- 能力的缺失

“新的解决方案”

—唐朝安全巡航的实践

新的解决方案的思考

- 资产管理：全面了解企业的数据流向
- 风险发现：深度挖掘企业的业务&数据存在的风险
- 事件处理：发现问题并有能力及时解决
- 持续管理：应对业务迭代更新带来的风险

资产管理

- 域名
- IP
- 服务
- 网站
- 应用



基础资产发现

- 企业内部资产梳理
 - 服务器上线流程控制
- 外部
 - 子域名暴力枚举
 - DNS解析数据
 - 第三方数据接口&爬虫

精细化的资产发现

- 指纹识别技术
 - 服务指纹识别
 - Nmap
 - mysql、redis、ssh
 - 应用指纹识别
 - 应用指纹: cookie, 文件MD5, html...
 - Blog、cms、oa

风险发现

- 基础服务风险检测
 - 服务通用漏洞检测
 - 相关配置风险
- 应用风险
 - 自研应用风险
 - 第三方应用通用漏洞检测

核心检测能力

- 核心是检测策略
 - 安全是动态的
 - 策略也应该是动态的
- 依托于开放平台&社区的力量
 - 基础引擎架构支撑+社区参与建设
 - 社区运营（激励策略）
 - 检测策略的持续更新
- 乌云社区二十万漏洞，两万白帽子的安全能力输出

事件处理

- 安全事件处理
 - 通告
 - 修复方案
 - 复查
- 全球威胁情报预警

高效问题处理能力

- 安全事件处理
 - 平台API对接产品生命周期管理流程
 - 安全专家全流程跟进服务
- 全球威胁情报收集
 - 威胁是动态的
 - 依托于社区&开放平台

持续风险管理

- 周期性检测
 - 对应业务迭代更新频率
 - 防止回滚导致修复失效
- 风险管理
 - 风险趋势分析
 - 指导基础安全建设

高效管理实践

- 自动周期安全巡检
 - 周期可配置
- 自动化分析报告
 - 自定义策略导出
 - 自动生成周报&月报&年报

谢谢

