UCLOUD

悟有所值 Ucan 下午茶
Ucan Afternoon Tea

虚拟货币安全

陈顺航

UCloud高级安全工程师

目录

01

数字货币安全事件概览与现状

交易所被盗情况

Poloniex

Bitfinex

NiceHash

Tradefortress

LocalBitcoins

Coincheck

8.64亿美元

Youbit4

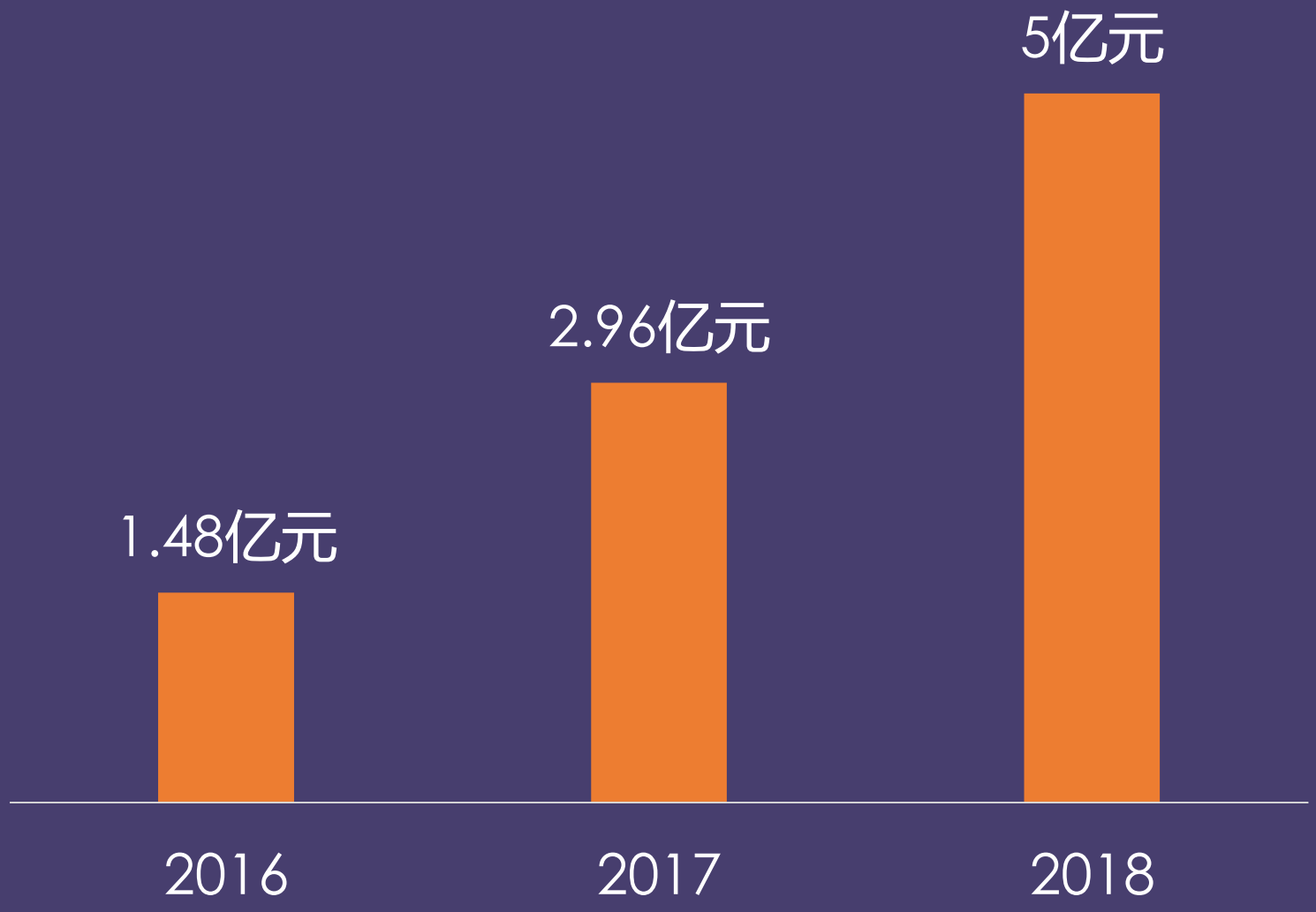
CoinDash

Enigma

Coincheck

Mt.Gox

yapizon


5亿元
2.96亿元
1.48亿元
2016
2017
2018

Botnet 从 ddos 转移到挖矿

UCloud通过安全产品共捕获到30+种样本

ddg20xx木马：合计挖矿90w到150w美元（三个钱包地址如下）

- 4AxgKJtp8TTN9Ab9JLnvg7BxZ7Hnw4hxigg35LrDVXbKdUxmcsXPEKU3SEUQxeSFV3bo2zCD7AiCzP2kQ6VHouK3KwnTKYg
- 45XyPEnJ6c2STDwe8GXYqZTccoHmscoNSDiTisvzzekwDSXyahCUmh19Mh2ewv1XDk3xPj3mN2CoDRjd3vLi1hrz6imWBR1
- 44iuYecTjbVZ1QNwjWfJSZFCKMdceTEP5BBNp4qP35c53Uohu1G7tDmShX1TSmgeJr2e9mCw2q1oHHTC2boHfjkJMzdxumM

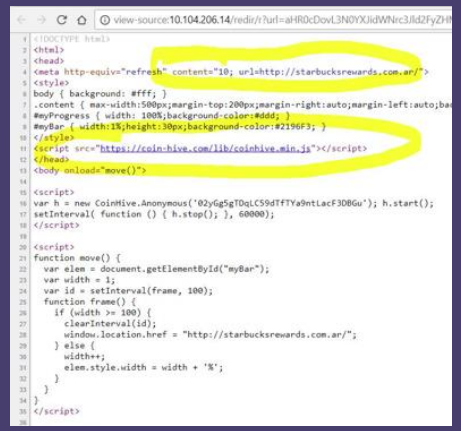
其他黑产方式

黑客门槛的降低

新的变现方式，让以往复杂的攻击方式变得更加简单，更加容易变现

恶意软件加入

原本由弹窗和广告构成的pc端恶意软件，加入了挖矿产业



星巴克WIFI挖矿

免费的公告WIFI是黑客的绝佳场所

软件中捆绑挖矿代码

uTorrent当中嵌入了挖矿代码，改现象也出现在手机端的盗版app

南方周刊官网挖矿

利用大流量的网站和漏洞大面积挖矿

不可调和的矛盾!!!

高回报 + 匿名性 + 不可溯源 = 高价值目标

悟有所值
Ucan Afternoon Tea

02

数字货币面临的安全风险

数字货币行业安全问题三大类

- 行业发展迅猛，准入门槛低带来的风险
- 传统安全存在依旧的老问题
- 新兴安全风险

交易所现状

规模小

- 69%的钱包开发商总员工数不到10人
- 交易所员工人数中位数为12

成立时间短

- 2017年下半年发行了4000+代币

门槛低

- 全球共成立了500+交易所，分布全球各个地方

来自visa和剑桥商学院的联合报告

数据来源:GLOBAL CRYPTOCURRENCY BENCHMARKING STUDY

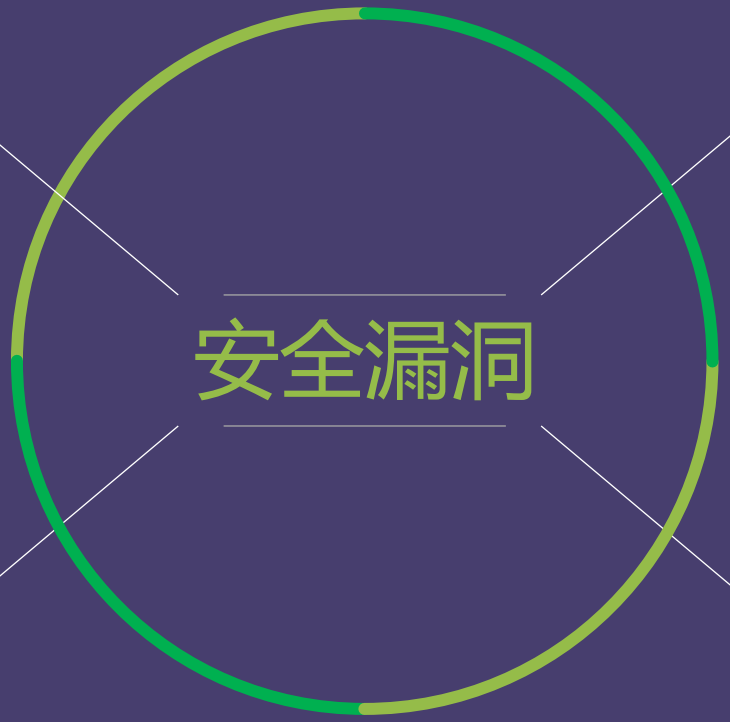
- Eclipse attack
- 51%攻击

新的安全问题

新的安全问题确实有效案例效果待观察

安全漏洞

传统攻击手段依然攻击效果依然非常好，并已出现多起case



钱包漏洞

Parity多重签名漏洞

假冒网站钓鱼

伪造假网站或者通过劫持，让用户访问黑客的网站，从而实现盗取

Coindash一个wordpress博客被上传webshell导致损失700w美元

网站web漏洞

币安钓鱼，通过伪造的地址，受害者点击之后即产生交易

业务安全

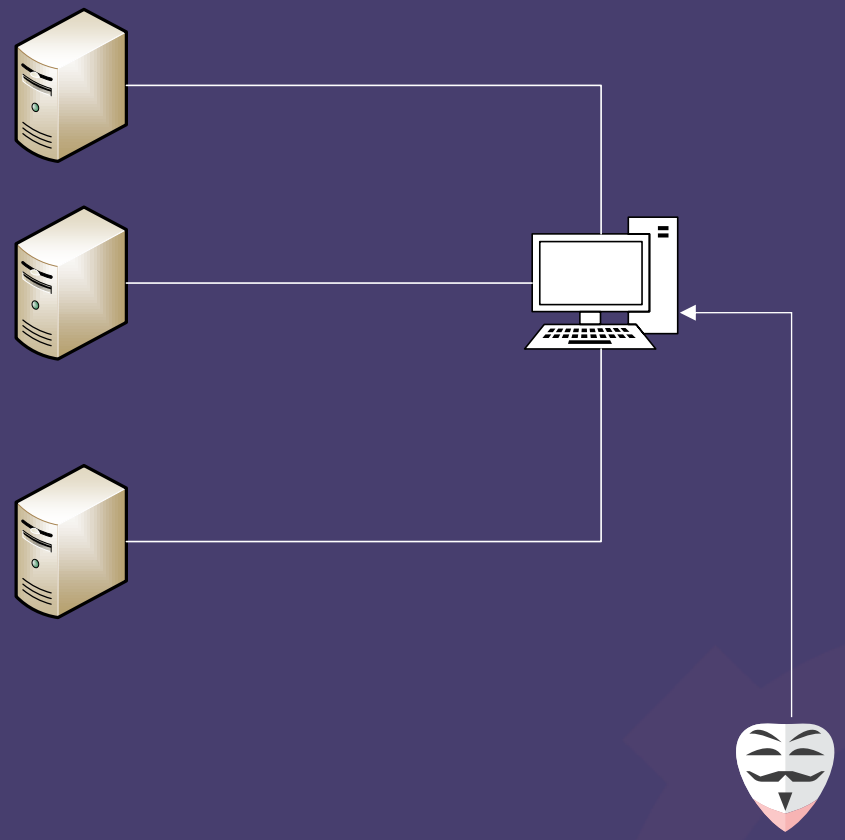
病毒木马

- **日本Coincheck：**

  员工电脑存在而已软件，损失约5.3亿美元

- **韩国Bithumb：**

  员工电脑被入侵，损失数10亿韩元



03

解 决 方 案

解决方案

传统安全厂商非常成熟可直接咨询，云上体系完善成本更低

建立正确的安全意识

正确的安全意识，不要相信绝对的安全，区块链带来的安全技术革命并不能解决所有安全问题

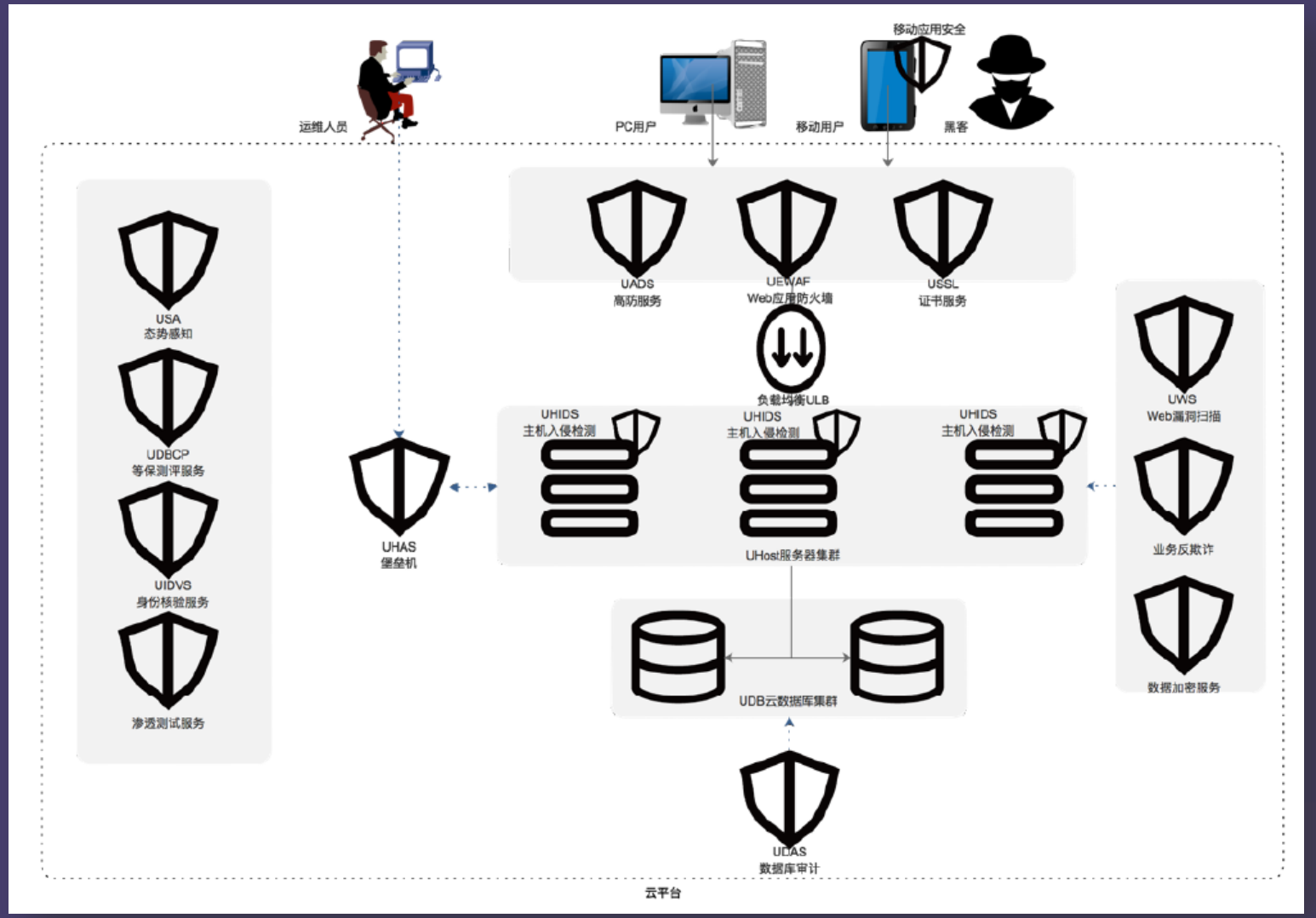
上云

云上有完整的基础设施，有成熟的基础防护体系，有配套的解决方案。其成本远远小于自己建设安全团队

使用第三方安全产品

传统安全产品已经在各个领域做的非常成熟，Visa报告中，全球最大的交易所中，使用的安全服务商均大于3家。同时也应该使用成熟的基础组件，比如钱包

解决方案架构图


运维人员
PC用户
移动应用安全
移动用户
黑客
UADS
高防服务
UEWAF
Web应用防火墙
USSL
证书服务
负载均衡ULB
USA
态势感知
UDBCP
等保测评服务
UIDVS
身份核验服务
渗透测试服务
UHAS
堡垒机
UHIDS
主机入侵检测
UHIDS
主机入侵检测
UHIDS
主机入侵检测
UHost服务器集群
UWS
Web漏洞扫描
业务反欺诈
数据加密服务
UDB云数据库集群
UDAS
数据库审计
云平台

悟有所值
Ucan 下午茶
Ucan Afternoon Tea

关注“UCloud技术公告牌”，更多分享与交流