2018 THINK IN CLOUD BEIJING

# 数字货币安全杂谈

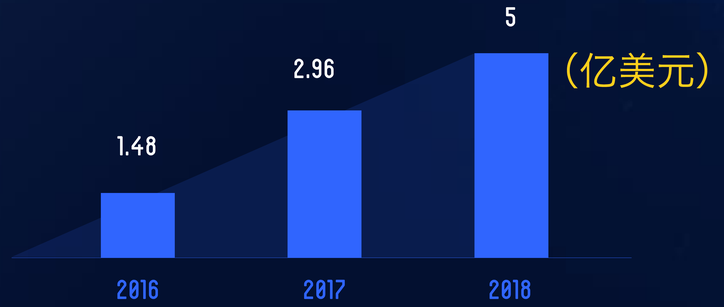
宗泽UCloud

# 数字货币黑产概览

# 攻击货币交易所


Tradefortress
Bitfinex
NiceHash
Poloniex
LocalBitcoins
8.64亿美元
CoinDash
Coincheck
Enigma
Mt.Gox
Youbit4
yapizon

被盗货币 损失



# Botnet 从 DDoS 转移到挖矿

- 利润高
- 变现快
- 安全隐蔽

# Ddg 挖矿木马　挖矿 90-150w 美元

- 4AxgKJtp8TTN9Ab9JLnvg7BxZ7Hnw4hxigg35LrDVXbKdUxmcsXPEKU3SEUQxeSFV3bo2zCD7AiCzP2kQ6VHouK3KwnTKYg
- 45XyPEnJ6c2STDwe8GXYqZTccoHmscoNSDiTisvzzekwDSXyahCUmh19Mh2ewv1XDk3xPj3mN2CoDRjd3vLi1hrz6imWBR1
- 44iuYecTjbVZ1QNwjWfJSZFCKMdceTEP5BBNp4qP35c53Uohu1G7tDmShX1TSmgeJr2e9mCw2q1oHHTC2boHfjkJMzdxumM

# UCloud 共捕获到 30+ 种样本

# 其他黑产方式

高回报 ＋ 匿名性 + 不可溯源 ＝ 高价值目标

# 数字货币安全风险剖析

# 行业发展迅猛，准入门槛低

500+交易所

员工平均数 12

半年 4000+ 种代币

数据来源：2017年全球加密货币研究报告

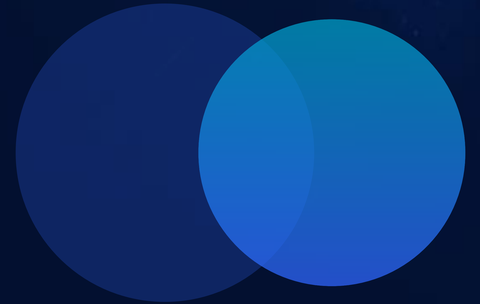
# 传统安全问题依然存在

# 安全漏洞

- 开源区块链软件漏洞：Solidity 漏洞
- 钱包漏洞：Parity多重签名钱包漏洞
- 交易所安全漏洞：coindash未修补的漏洞导致被上传webshell

# 病毒木马

- 日本Coincheck：员工电脑存在恶意软件，损失约5.3亿美元
- 韩国Bithumb：员工电脑被入侵，损失数十亿韩元



# 社工钓鱼

- 矿场NiceHash
- 2018年3月，币安钓鱼事件
- 2018年4月，MyEtherWallet遭DNS劫持攻击，用户被劫持到假冒网站

# 新形态安全问题

- 51%攻击
- Sybil Attack（女巫攻击）
- eclipse attack

# 数字货币交易安全解决思路

03

# 个人

## 离线钱包 VS 在线交易所

# 交易所

- 安全意识，设立安全团队
- 使用成熟的安全解决方案
- 上云

# THANKS