



---

2016乌云白帽大会·不插电

# 威胁情报联盟

# Who Am I ?

- 瞌睡龙
- 乌云合伙人、知识库负责人

威胁情报是针对已有或新型的威胁或风险采取响应的一种实证知识，  
包括背景、运作机制、标识、启示性的和可操作性的建议。

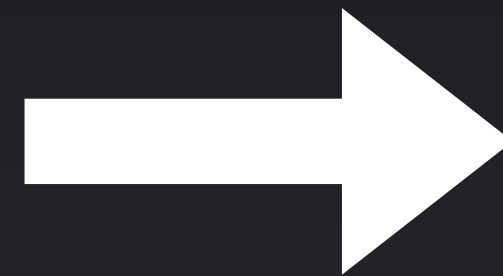
— Gartner（全球最具权威的IT研究与顾问咨询公司）

# 我们理解的威胁情报

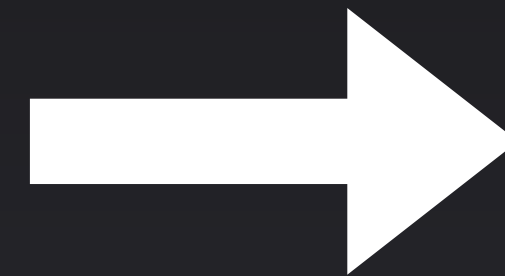


# 我们理解的威胁情报

数据安全



服务器安全  
交换机安全  
数据库安全  
员工PC安全  
等.....



Web应用防火墙

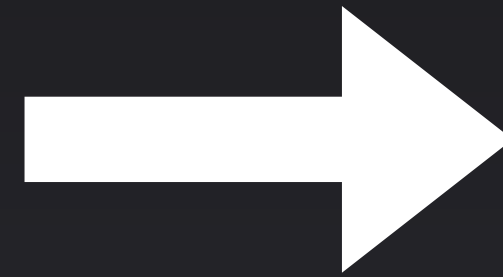
IDS、IPS

端点监控

等.....

# 我们理解的威胁情报

业务安全



DDoS攻击  
CC攻击  
被薅羊毛  
被撞库  
等.....



网络防火墙  
业务安全产品  
自身业务数据分析  
等.....



# 我们所做的事情

## 数据安全

- ThreatKey蜜网监控

## 业务安全

- 互联网风控基础数据



乌云 WooYun



乌云白帽大会 · 2016  
不插电

# ThreatKey简介

- 基于Docker的高交互蜜罐系统
- 部署脚本一键安装
- 蜜罐网络安全限制
- 云端直接管理蜜罐（新增、启动、重置）
- 多样化日志收集、查询、分析



ThreatKey.com

ThreatKey

🏠 首页

☁ 节点 ▼

查看所有节点

创建节点

📖 接口介绍&文档

Install path:

Node name:

Node description:

Node description

Vul type:

☐ SSH ☐ Redis\_SSH

☐ Telnet

☐ Joomla ☐ WP ☐ Shellshock

☐ Jboss ☐ Jenkins ☐ struts2\_032

☐ ES

☐ vsftp

Add

🔔

wooyun ▼

H

乌云 WooYun

乌云白帽大会 · 2016

不插电

ThreatKey.com

ThreatKey

首页

节点

查看所有节点

创建节点

接口介绍&文档

Attack

Nodes

Attacked Honeypots

55474

details

Today

6668

Yesterday

10769

8

Running

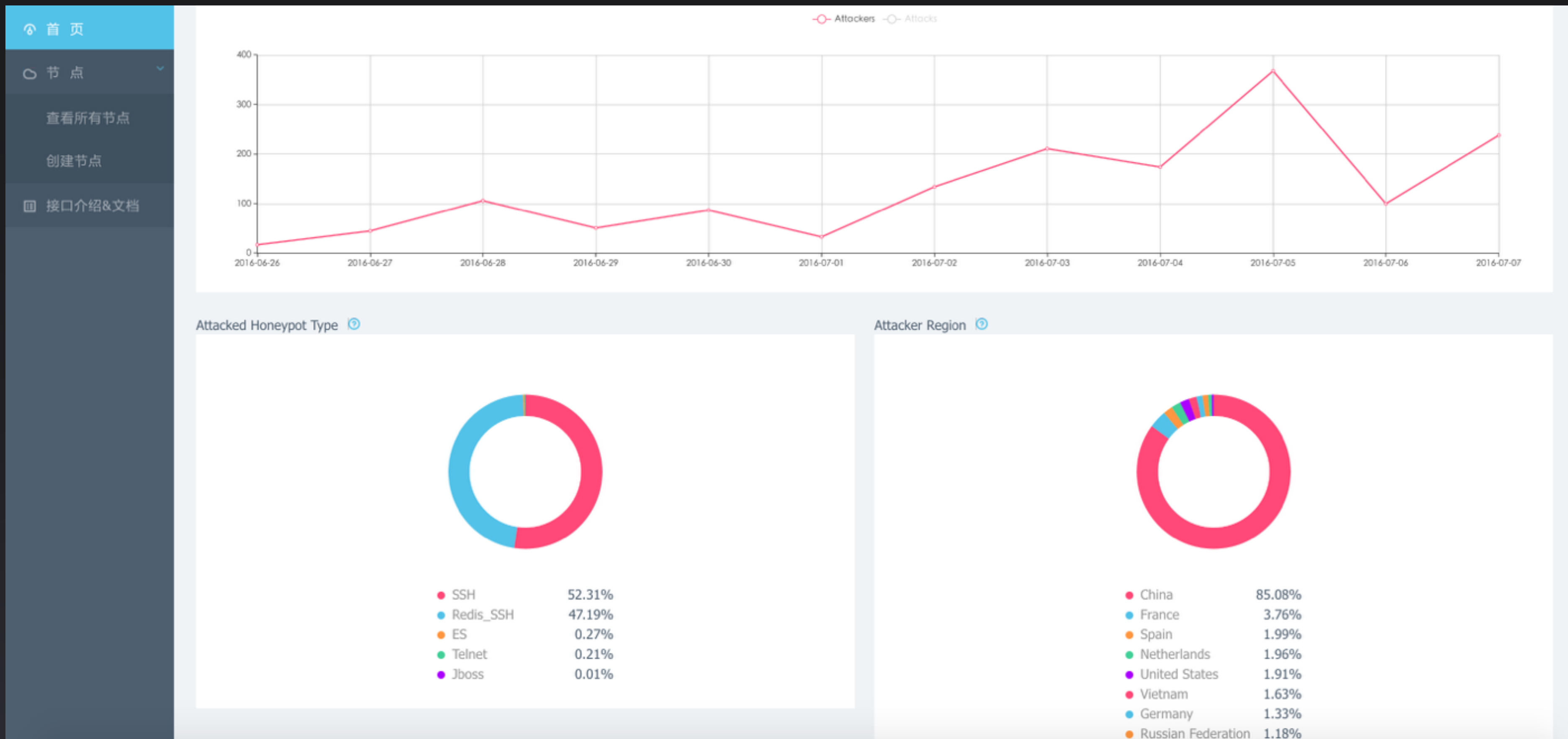
10

Totals

Vul Type	Node Name	Attacks	Attackers
Redis_SSH	dgo_Bangalore	6226	2
SSH	dgo_London	228	6
SSH	dgo_Toronto	134	4
SSH	dgo_Singapore	60	4
SSH	aws_Beijing	17	3
SSH	tencent-shanghai	2	1
Telnet	aws_Beijing	1	1

more

# ThreatKey.com



乌云 WooYun



乌云白帽大会·2016  
不插电

ThreatKey.com

ThreatKey

首页

节点

查看所有节点

创建节点

接口介绍&文档

搜索时间2015-12-31 23:552016-07-07 00:00

搜索范围File Log (999+)Http Out (294)DNS Log (999+)Access Log (999+)Bash Log (112)IRC Log (122)全选

搜索关键词

不包含关键词

2016-07-06T15:59:56.871489+00:00auth

dst\_ip:178.62.220.128  
vid:4757eba5686b5d97  
service:ssh  
src\_ip:163.172.166.222  
user:magnos  
pass:magnos  
is\_attack:1

2016-07-06T15:59:56.871489+00:00auth

dst\_ip:178.62.220.128  
vid:4757eba5686b5d97  
service:ssh  
src\_ip:163.172.166.222  
user:magnos  
pass:magnos  
is\_attack:1

2016-07-06T15:55:07.866580+00:00

dst\_ip:178.62.220.128  
vid:4757eba5686b5d97

# 互联网风控基础数据

Risk.WooYun.org

- 羊毛党手机号
- 被钓鱼银行卡号
- 代理IP地址

# 互联网风控基础数据

Risk.WooYun.org



乌云 WooYun



乌云白帽大会 · 2016  
不插电



# 互联网风控基础数据

Risk.WooYun.org

● 管理控制台

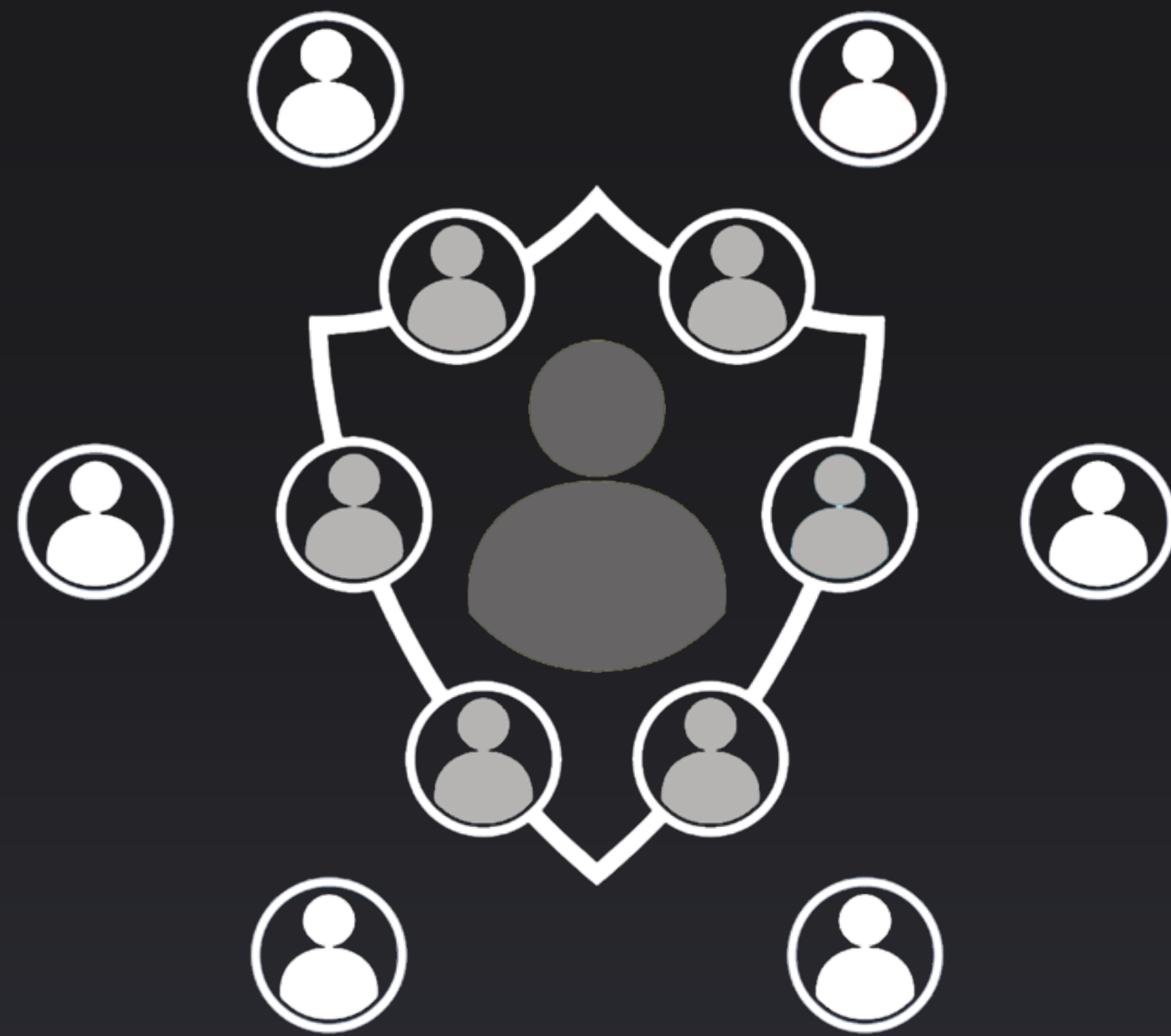
AccessKey帮助文档账户管理

API 实例名称 / ID	接口地址		命中总数 / 请求总数	详情说明
帐号安全	https://apirisk.wooyun.org/V1/account/verify	复制	41 / 62	查看
业务安全	https://apirisk.wooyun.org/V1/common/verify	复制	5 / 27	查看

WooYun

乌云知识库乌云众测合作咨询

我们希望未来的安全



# THANKS



乌云 WooYun



乌云白帽大会 · 2016  
不插电