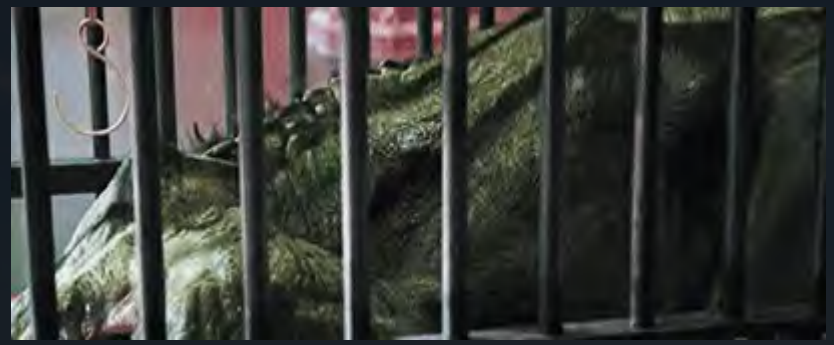

唯一集团
互联网综合服务提供商
.COM DDOS
唯一网络
郑可君
让世界更安全！
Make the world safer !
2017GOPS全球运维大会 深圳站

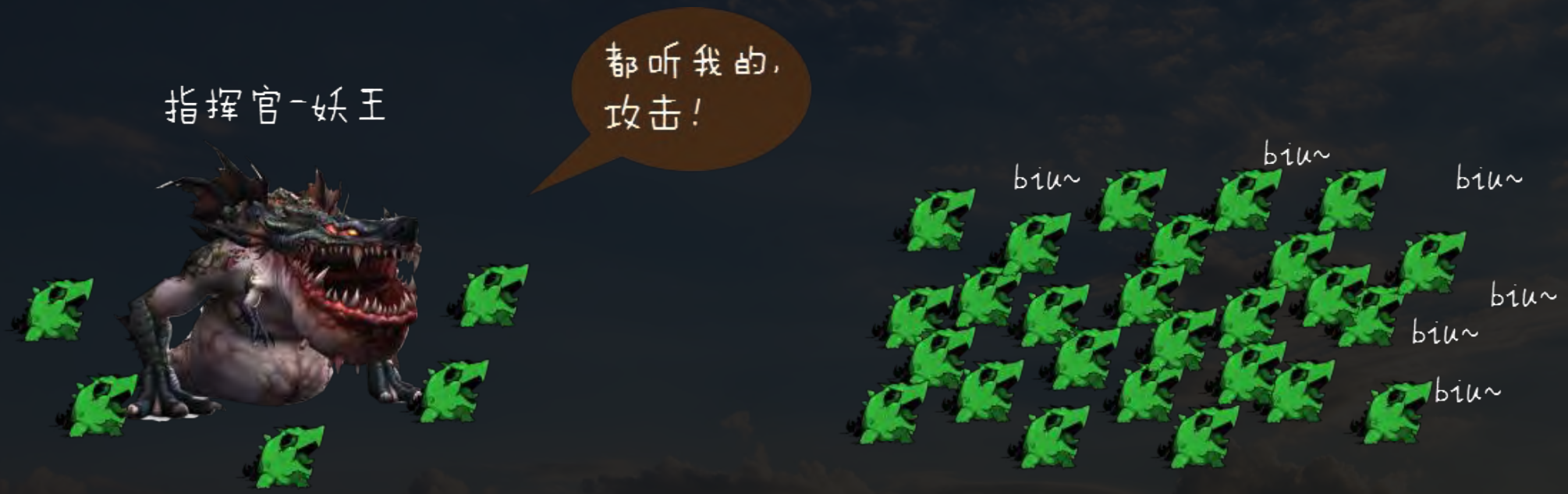
电影 长城——细思极恐的DDoS攻击

饕餮 (tāo tiè)



电影 长城——细思极恐的DDoS攻击

电影 长城——细思极恐的DDoS攻击

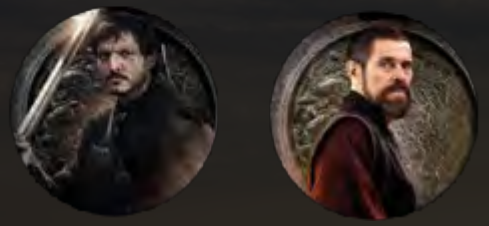


电影 长城——细思极恐的DDoS攻击

长城
只是防火墙的硬件

虎军 鹿军 熊军 鹤军 鹰君

无影禁军
是防火墙软件能力



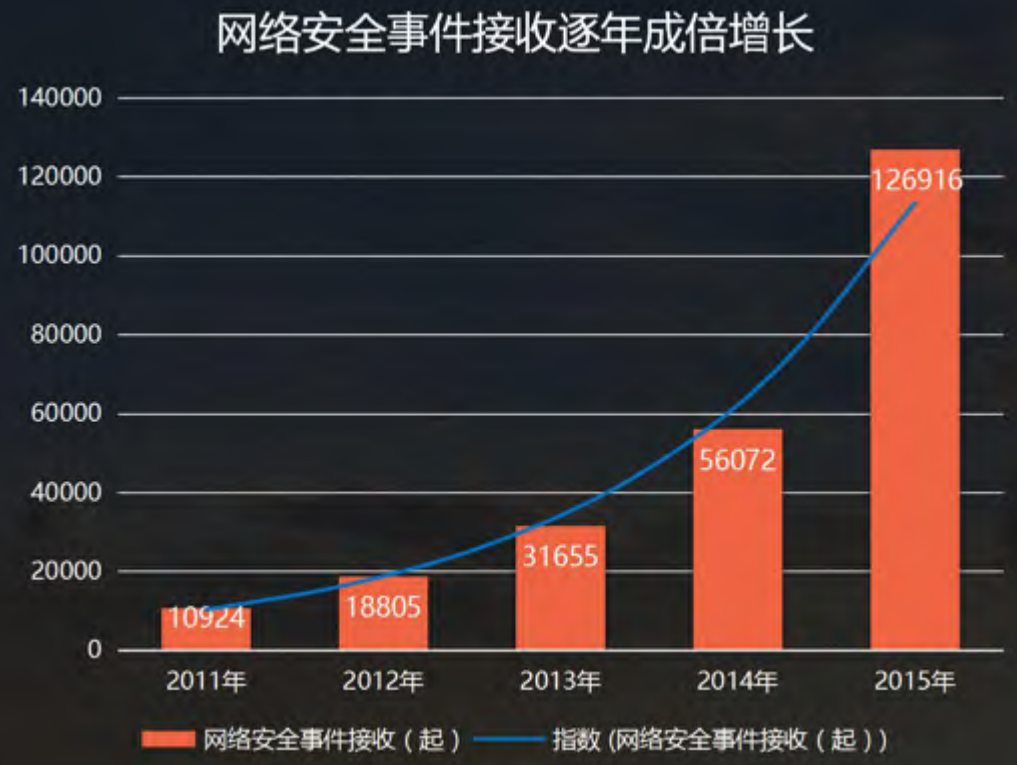
洋人组合
软件能力注入，使得
防火墙升级为NGFW

CONTENTS


01
互联网安全形势简析

1.1 中国互联网安全形势

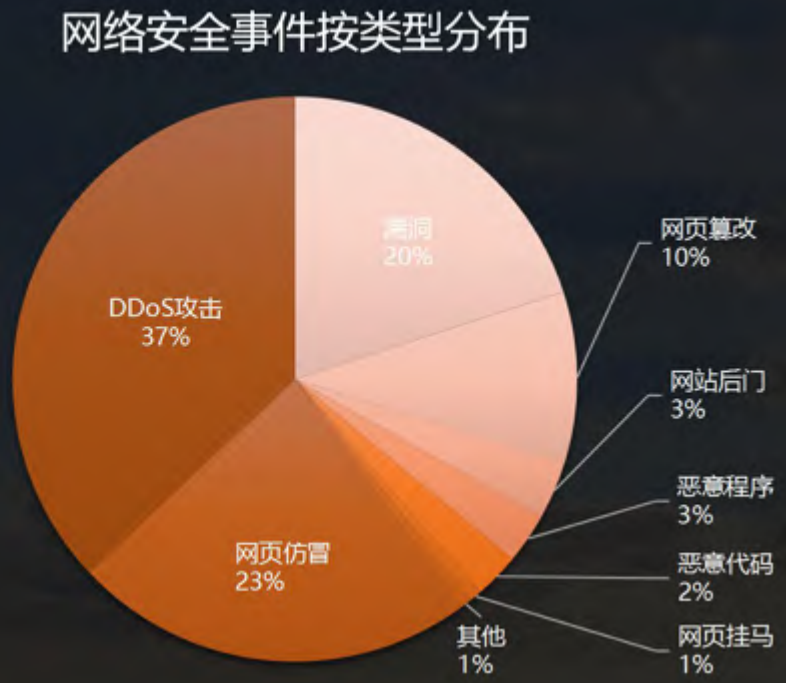
中国互联网安全事件接收呈现逐年成倍增长态势。2015年，CNCERT/CC共接收境内外报告的网络安全事件126916起，较2014年增长了125.9%。事件类型主要包括网页仿冒、漏洞、网页篡改、DDoS攻击、网站后门、恶意程序等，互联网安全形势日趋严峻。



数据来源：《CNCERT/CC——2011年-2015年 CNCERT/CC网络安全事件接收数量年度统计》

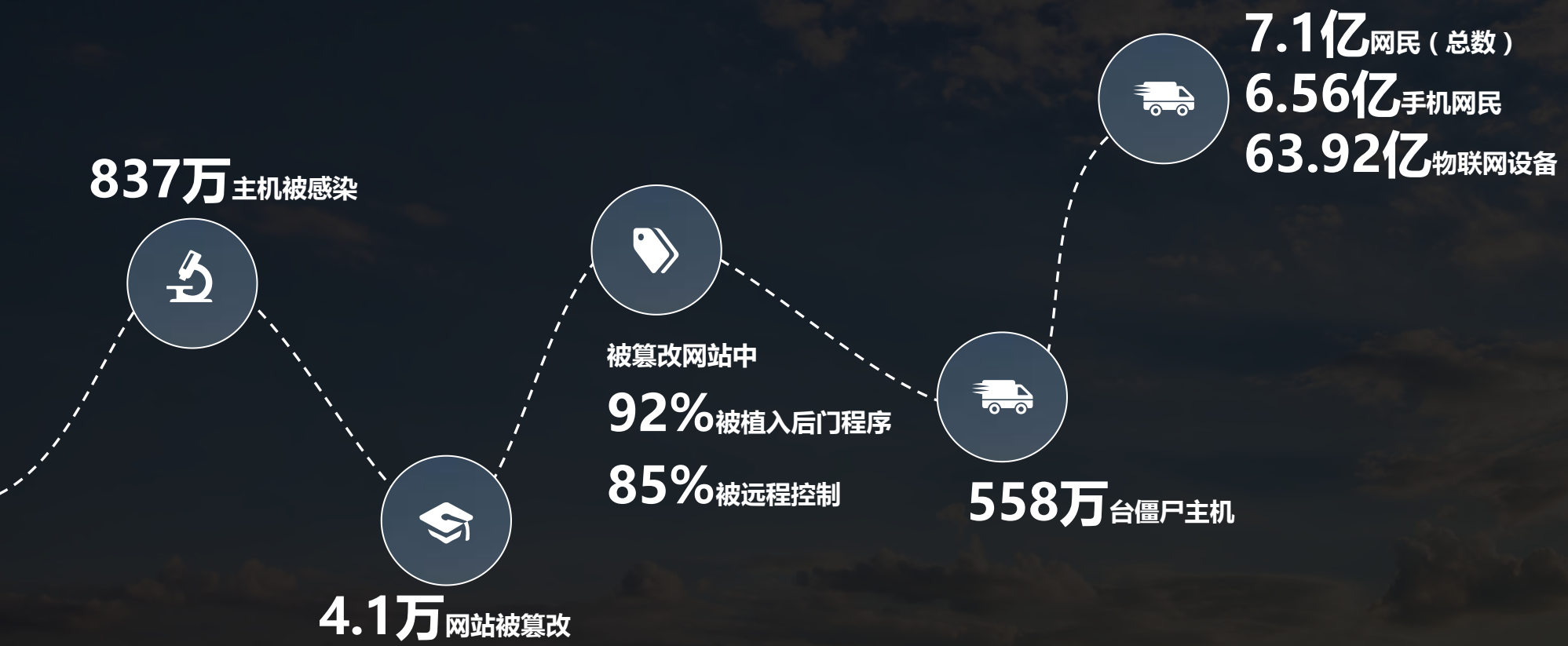
1.1 中国互联网安全形势

中国互联网安全事件接收呈现逐年成倍增长态势。2015年，CNCERT/CC共接收境内外报告的网络安全事件126916起，较2014年增长了125.9%。事件类型主要包括网页仿冒、漏洞、网页篡改、DDoS攻击、网站后门、恶意程序等，互联网安全形势日趋严峻。



数据来源：《CNCERT/CC——2011年-2015年 CNCERT/CC网络安全事件接收数量年度统计》

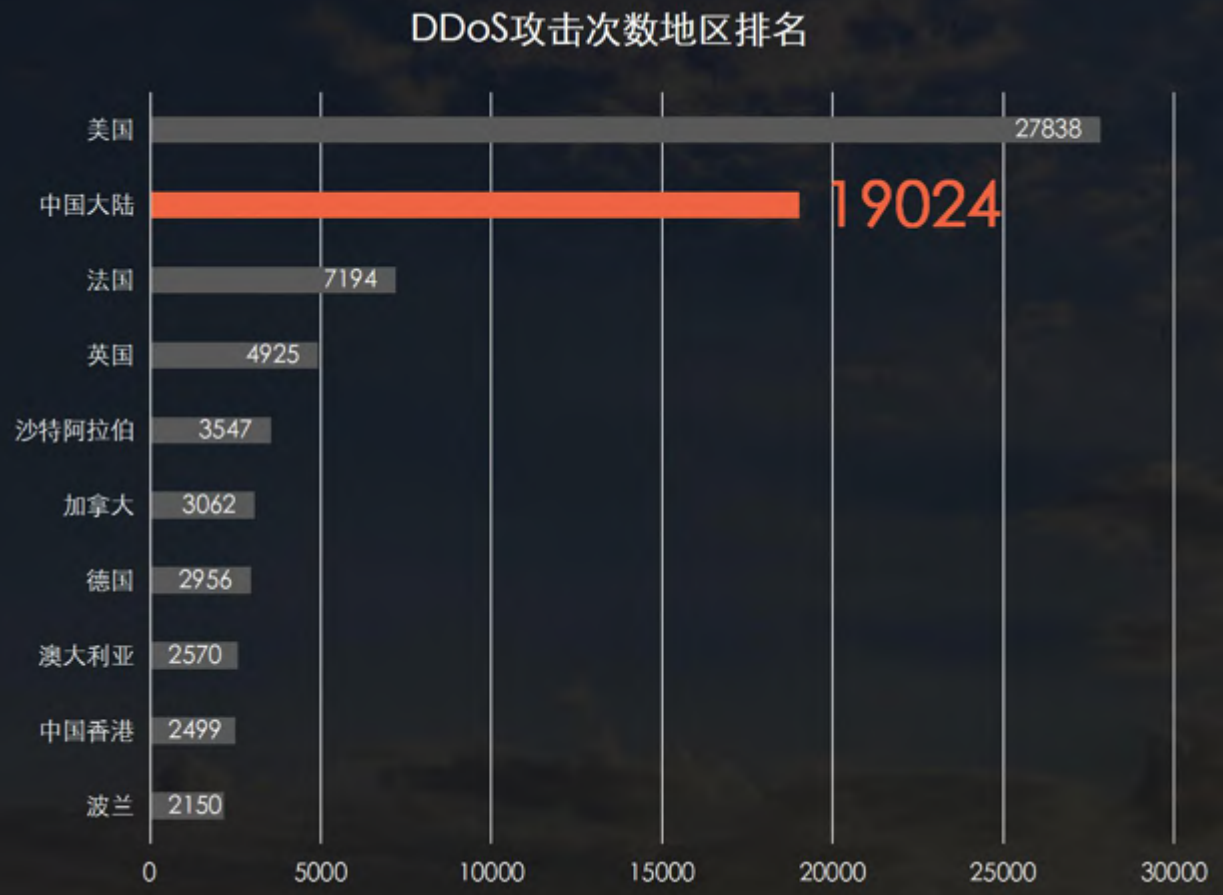
1.2 中国已成为“著名”攻击源国家



- 2016年第三季度网络安全态势
- 不排除还有更多隐秘性高的事件未在官方平台统计。

数据来源：《2016第三季度阿卡迈互联网安全报告》《中国互联网站发展状况及其安全报告（2016）》《2016年中国物联网市场规模及行业发展趋势》

1.2 中国已成为“著名”攻击源国家

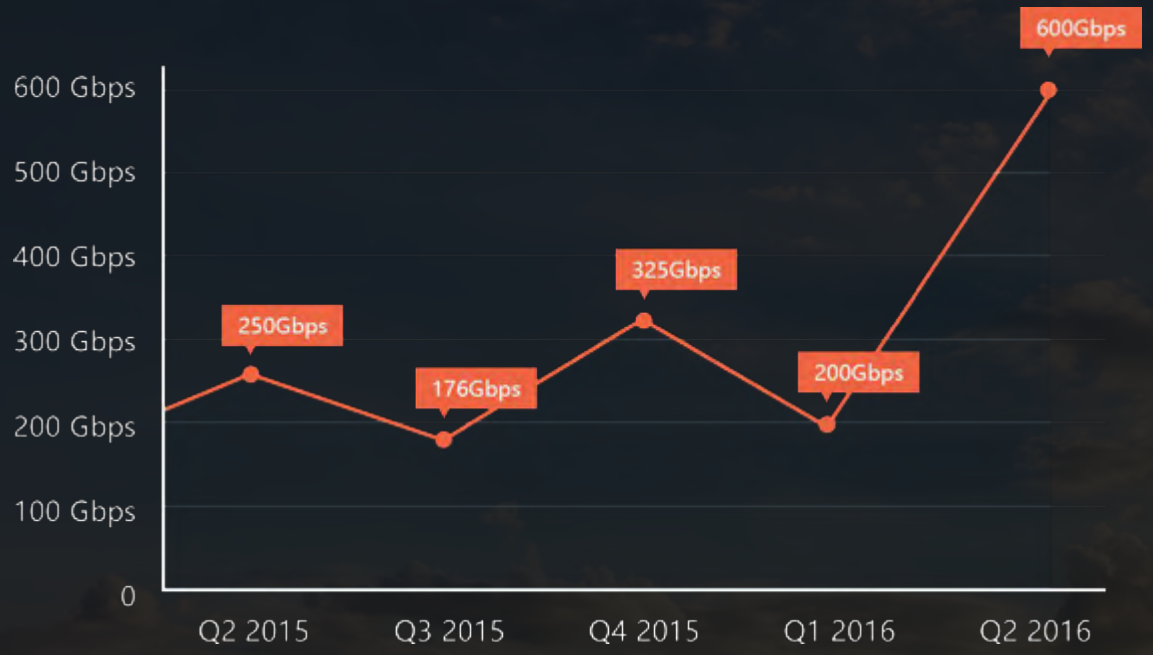


- **2016年第三季度网络安全态势**
- **不排除还有更多隐秘性高的事件未在官方平台统计。**

数据来源：《2016第三季度阿卡迈互联网安全报告》《中国互联网站发展状况及其安全报告（2016）》《2016年中国物联网市场规模及行业发展趋势》

1.3 网络攻击趋势

攻击规模



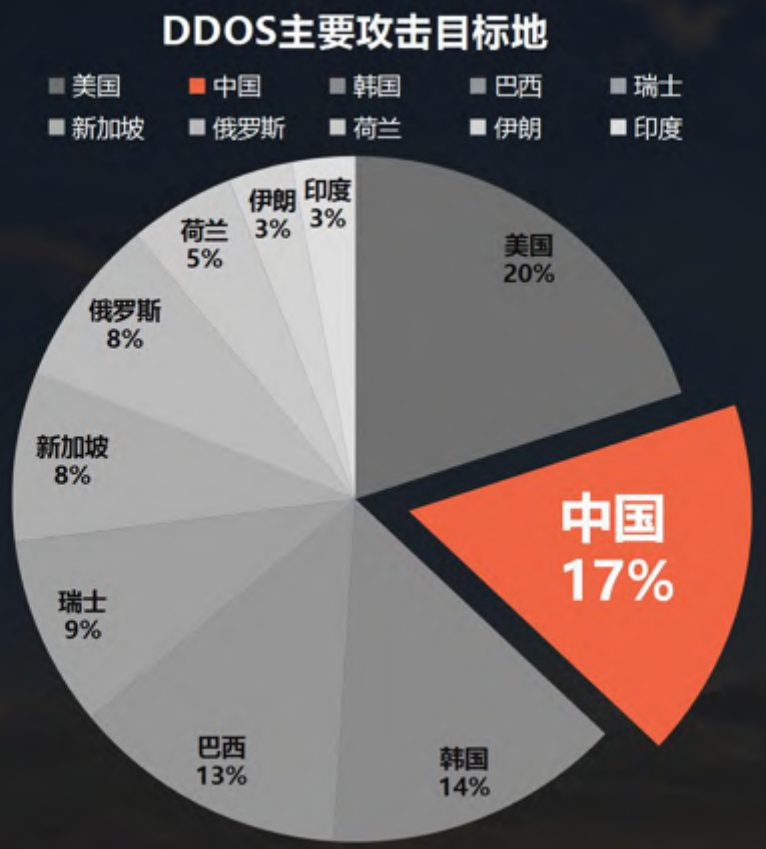
《Arbor Networks Releases Global DDoS Attack Data for 1H 2016》

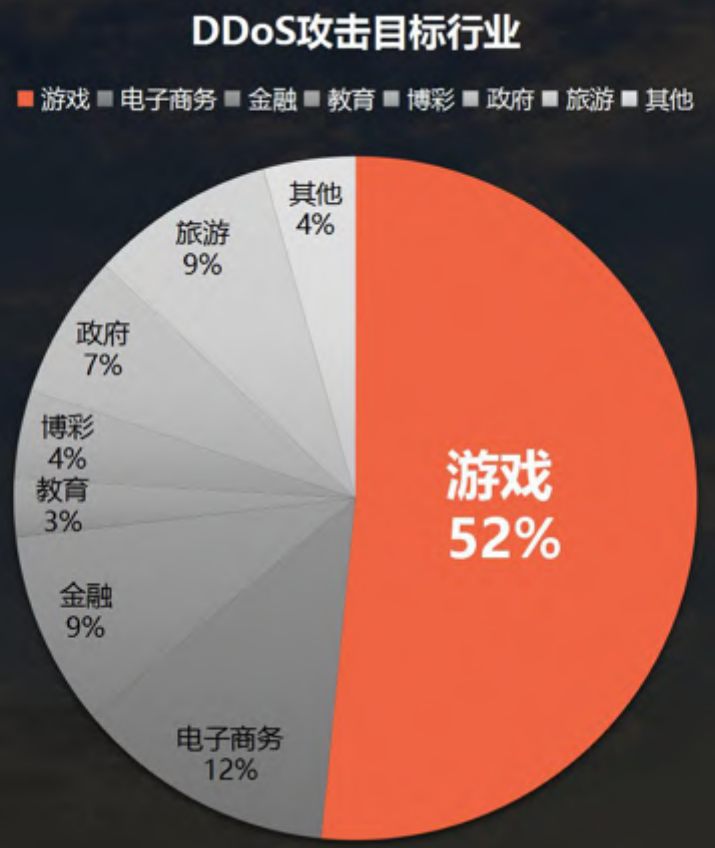
1.3 网络攻击趋势

- 2015年至2016年7月，平均每周发生**12.4万次**安全事件
- 攻击规模增长了73%，最高超过**600Gbps**
- 2016年上半年超过100Gbps的攻击事件高达**274起**，而2015年全年223次
- 2016年上半年超过200Gbps的攻击事件超过**46次**，而2015年全年仅16次

《Arbor Networks Releases Global DDoS Attack Data for 1H 2016》

1.4 中国处于攻击目标地的“第一梯队”





数据来源：《2016第三季度阿卡迈互联网安全报告》《中国互联网站发展状况及其安全报告（2016）》


02
网络安全世界的野蛮人
——DDoS

2.1 为何称DDoS为野蛮人？

动机

恶意竞争

敲诈勒索

实施报复

目的

从中获利

技术炫耀

政治立场

攻击特征

快速高效

种类繁多

隐蔽性高

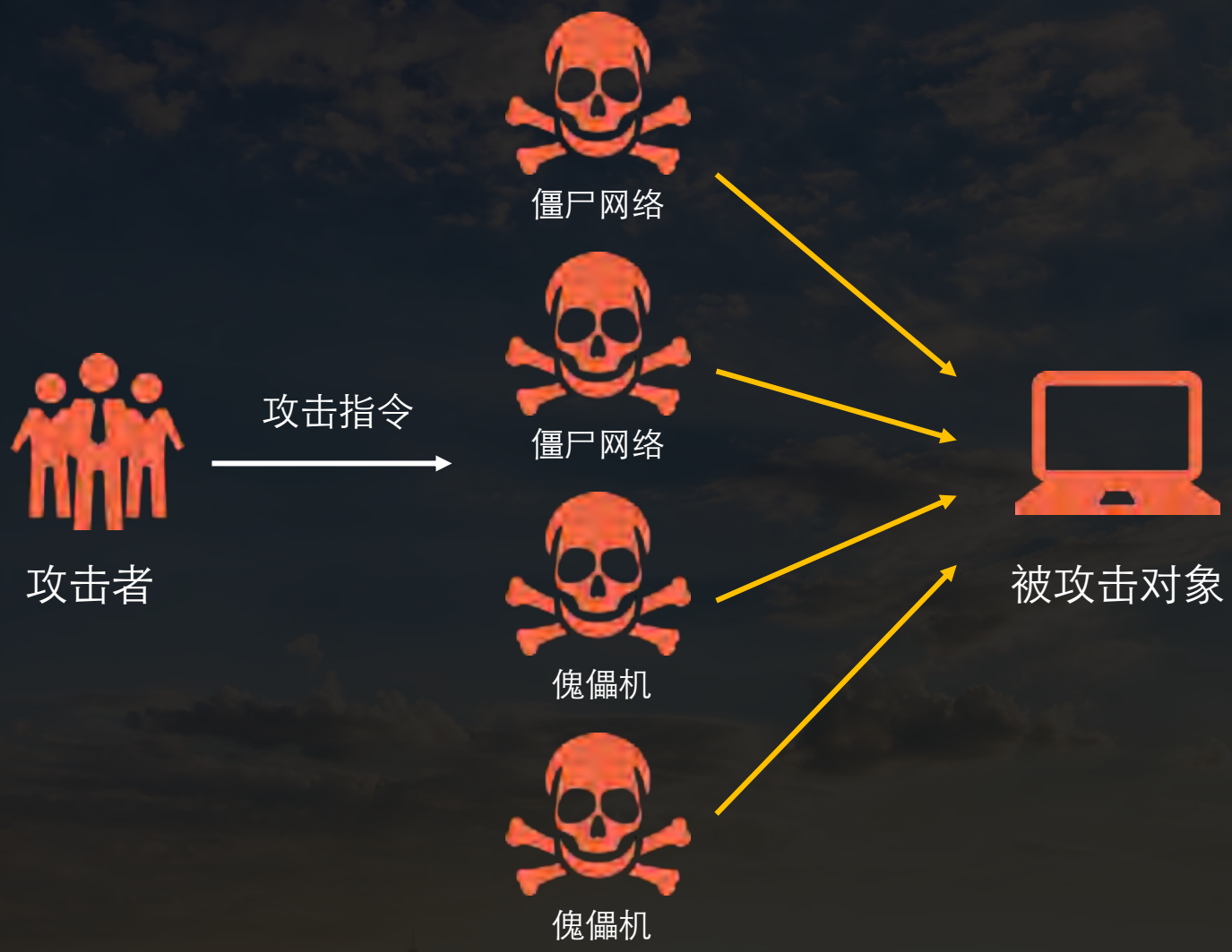
《Arbor Networks Releases Global DDoS Attack Data for 1H 2016》

2.2 为何称DDoS为野蛮人？

原理

分布式拒绝服务攻击

- 黑客利用大量僵尸机/傀儡机同时对目标发起请求，导致目标的网络出口链路拥塞或者忙于应付攻击请求无法响应正常的服务。



2.2 为何称DDoS为野蛮人？

原理

分布式拒绝服务攻击

黑客利用大量僵尸机/傀儡机同时对目标发起请求，导致目标的网络出口链路拥塞或者忙于应付攻击请求无法响应正常的服务。

攻击特点

攻击指令

- **易实施**
- **攻击类型多**
- **攻击手段多样**
- **攻击源设备多样**
- **攻击源数量庞大**
- **溯源困难**

攻击类型

畸形包攻击

远程溢出拒绝服务攻击

利用协议栈漏洞攻击

流量型攻击

TCP Flood　　ICMP Flood
UDP Flood

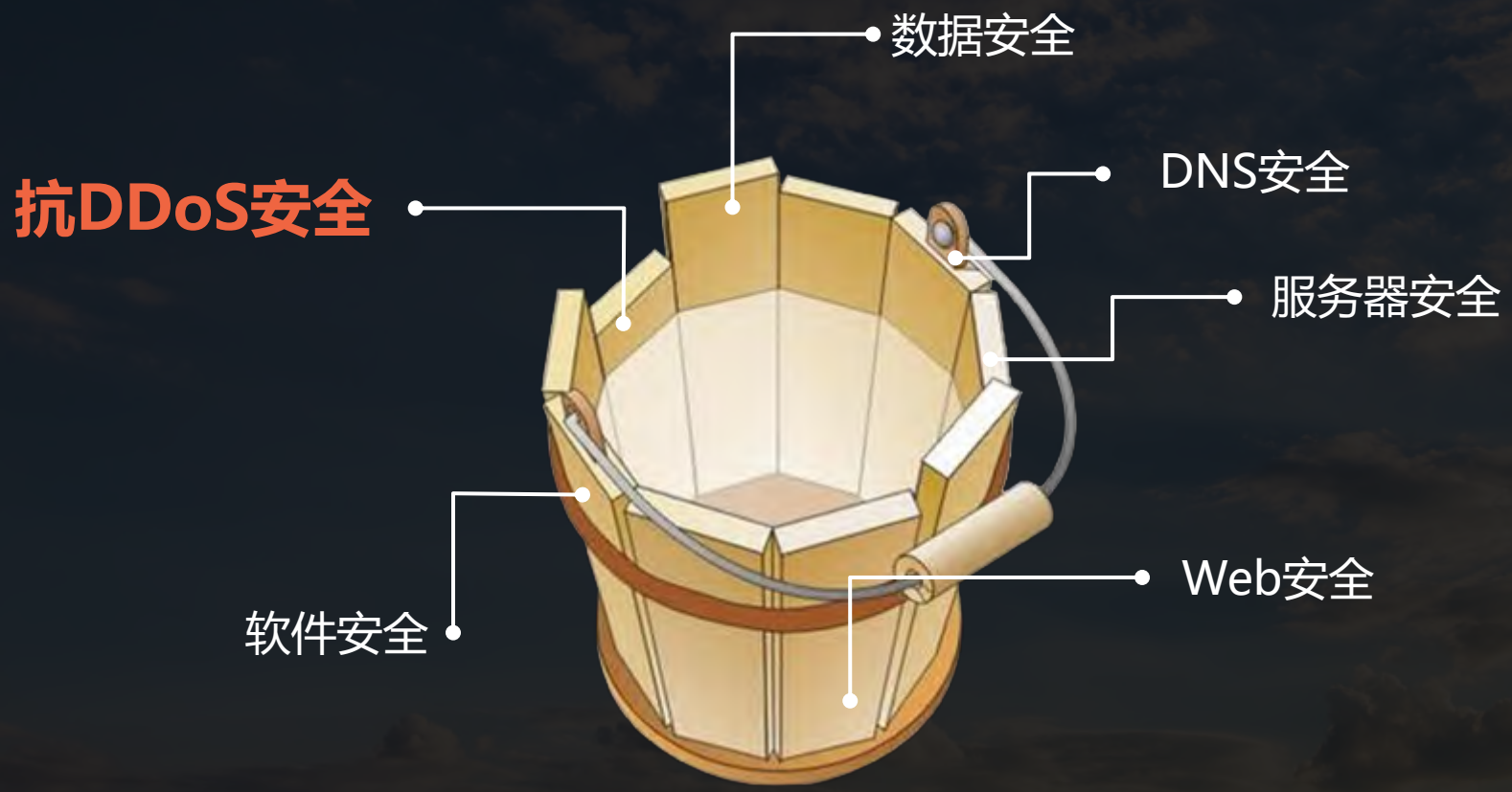
应用型攻击

DNS Query Flood　　Connection Flood
HTTP Get Flood　　CC攻击
HTTP 半开　　HTTP 错误
基于会话的攻击

03

DDoS攻击与防御
实例分析

3.1 安全观点：互联网安全的立体性



在信息安全中的防护强度取决于**“马奇诺防线”**中最为薄弱的一环

3.2 攻击案例

收入2000万/年

安全投入 30万/年

中断1小时

损失12万

8 万 / 年 DDoS云防护服务

3.3 著名攻击案例1

KrebsonSecurity
In depth security news and investigation

攻击者 | Mirai僵尸网络

时间 | 2016年9 月 20 日

目标 | 安全研究机构 KrebsonSecurity

攻击特点

1、十万数量级别的僵尸网络发起

2、物联网IOT设备构成

3、665G大规模DDoS攻击

攻击影响

Akamai

KrebsonSecurity
In depth security news and investigation

3.3 著名攻击案例2

Dyn

2016年10月

DYN.COM（美国最大的DNS服务商）

24小时内三波攻击

最长持续2个小时

攻击特点

1、数十万僵尸网络

2、物联网IOT设备

3、1T+攻击带宽

4、DNS放大攻击

攻击影响

airbnb

NETFLIX

Spotify


04
抗DDoS攻击解决方案

4.1 关于我们

1

全网防御带宽1T+
单点600G

5

全国5大抗D数据中心

10

10年网络安全
经验团队

100+

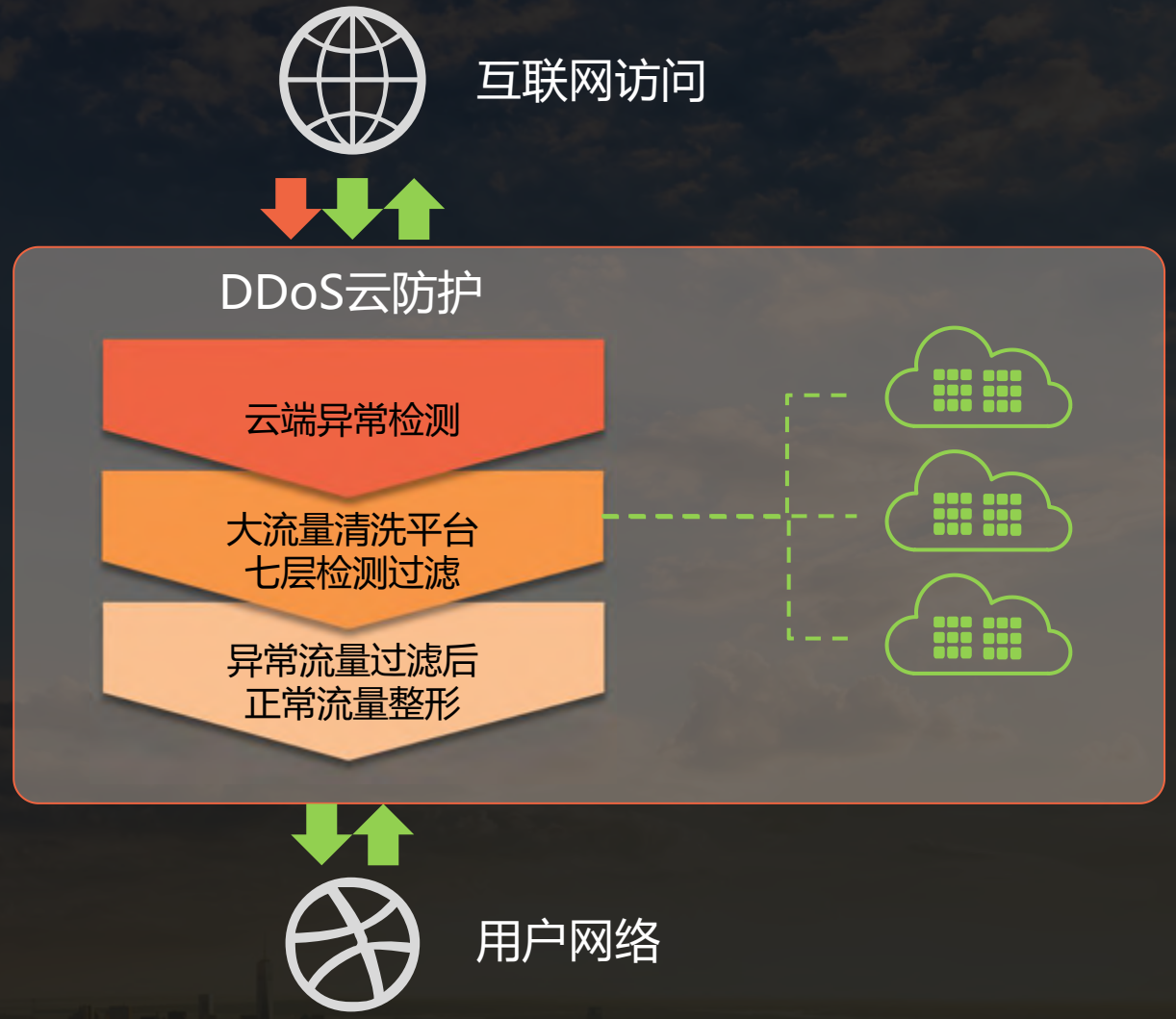
抗D服务客户
超100家

365

365*7*24小时
运维支撑服务

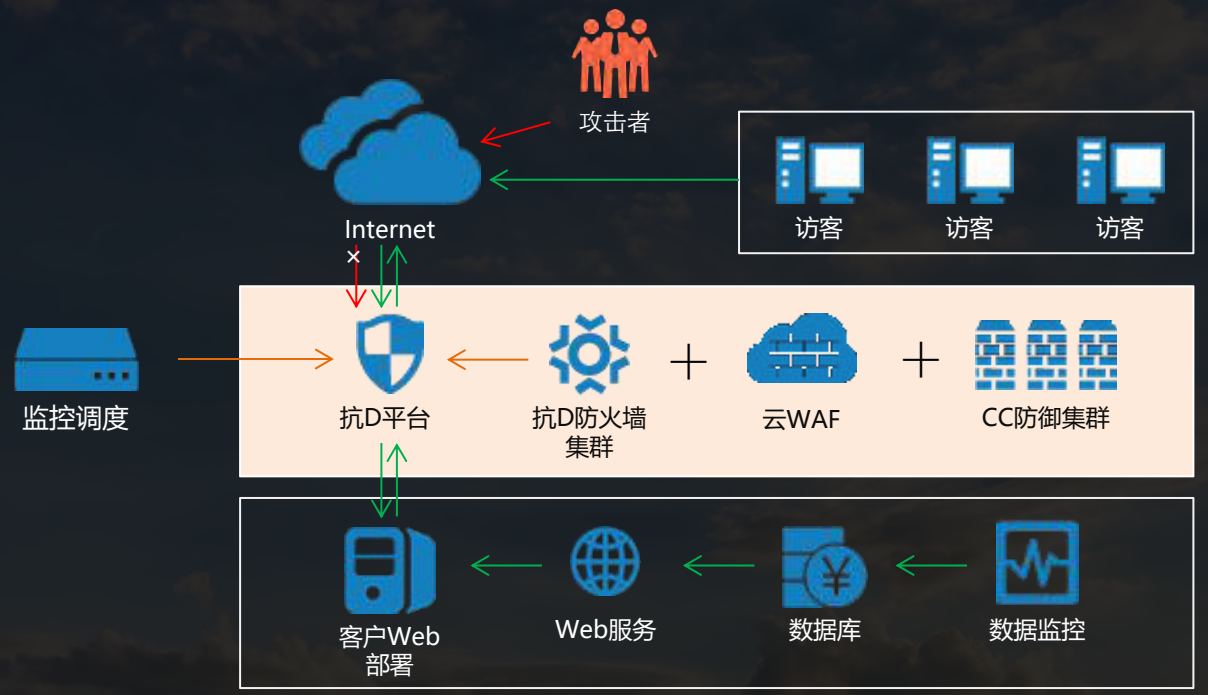
4.2 抗DDoS攻击解决方案

DDoS云防护



4.2 抗DDoS攻击解决方案

4.2 抗DDoS攻击解决方案



4.3 增值服务

全网覆盖

覆盖主流运营商
异地多节点接入

负载均衡

高性能服务器集群
路由协议负载均衡

可视化态势感知

全息监控，高可用保障
可视化攻击报表查询

实时告警

发现异常，秒级告警
支持短信、邮箱等方式

缓存加速

缓存网站静态内容
提升网站访问速度

4.4 客户案例


广州红盾信息网
广州文史
恒安集团 HENGAN
ChinaCache
网宿科技 ChinaNetCenter
小牛在线 xiaoniu88.com
分期乐 fenqile.com
桔子理财 juzilicai.com
金瑞龙 ruilongjin.com
拉拉财富 www.lalacaifu.com
中国IDC圈 idcquan.com
597人才网 www.597.com
500wan.com
可付集团 kefuempire
团贷网 www.tuandai.com
37.游戏.com
4399 最大的休闲娱乐平台
多玩游戏 duowan.com
9377.com
飞鱼科技
Letv乐视网
爱奇艺
YIKA
社区动力 DISCUZ!
懒人听书 www.lrts.me
22.cn 爱名网
易名中国 NAME www.ename.cn
4.CN金名网
HON-Logistics 弘信物流
YOUKU 优酷
健客
东莞国药
39健康网 www.39.net
风行网
Skyworth 创维

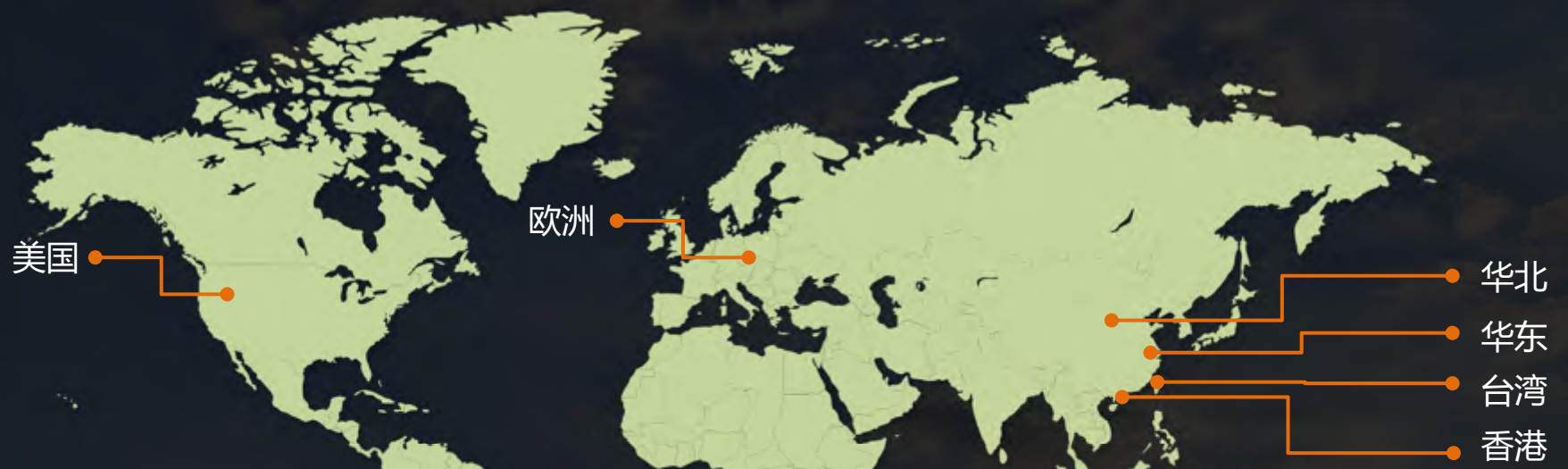
4.5

打造互联网信息安全核心生态圈

一站式安全服务体系

协同输出能力

为用户解决安全问题



打造互联网信息安全核心生态圈

让世界更安全！

唯一集团
互联网综合服务提供商

DDOS.COM

Thanks

郑可君　唯一集团