RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

了解并防范 Modern DDoS 威胁

会议 ID：MAN-W08

Stephen Gates

首席安全宣讲师
Corero Network Security
@StephenJGates

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

理解您容易受到攻击！

其他人准备得怎么样？

- **40%** 的企业完全或基本上没有准备
- **23%** 的受访者表示他们没有相关的计划
- **16%** 未意识到任何当前或未来的此类计划
- **26%** 仍依赖他们的运营基础架构
- **50%** 从未测试过他们的 DDoS 防御功能

访问整个报告：
www.corero.com/SANS-DDoS-Survey

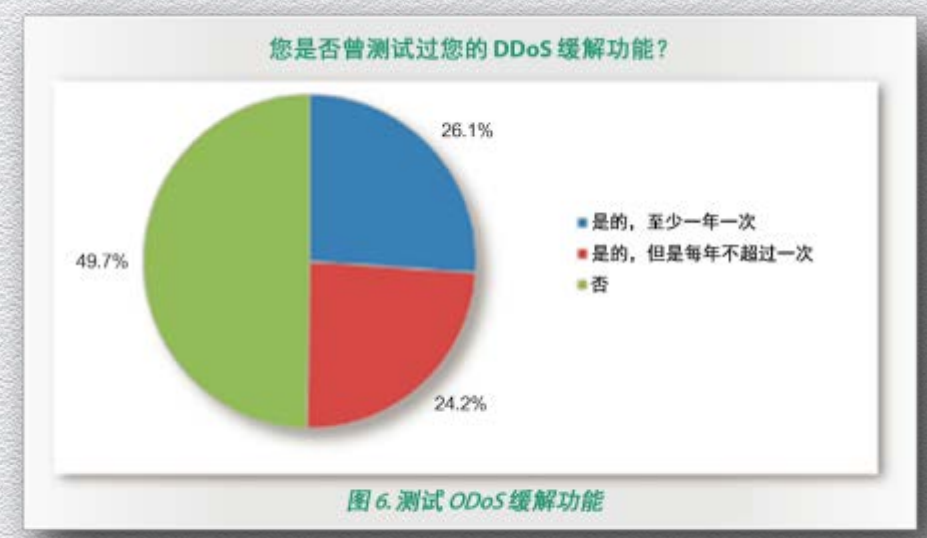


图 6. 测试 DDoS 缓解功能

corero
FIRST LINE OF DEFENSE

发起容易 — 停止难！

DDoS 攻击是否真的起作用？

The Phnom Penh Post

HOME | NATIONAL | BUSINESS | LIFESTYLE | SPORT | COLUMNS

Members of Anonymous Cambodia arres
Cambodia has sworn to up efforts to rec
assault on government websites. Photo

Anonymous vows re

Fri, 25 April 2014 Kevin Ponniah

Anonymous Cambodia has pledged
government websites in response
the international "hacktivist" gro

Akamai

By Jennifer LeCl
January 28, 201

In its State of t
year-over-year
performance c

» The Interne
slight decreas
there were m
in all of 2012.
Internet Repo
report offers
speeds, attac

Attacke
DDoS attacks

Candice So @candice_so
Published: March 28th, 2014

Distributed denial of service (DDoS) attacks are getti
becoming wise to the ways of DDoS threat preventio
from Incapsula Inc., a U.S.-based security solutions

XSS VULNERABILITY IN SOHU.COM LEVERAGED FOR LARGE-SCALE DDOS ATTACKS

28 Apr 2014 | DPC | Comments Off

DoS attack in
ps
ome 33 percent higher than last
ort's holder

May 28, 2014

SNMP reflection DDoS attacks on the rise, researchers find

Share this article:

Akamai's Prolexic Security Engineering Response Team (PLXsert) issued a threat advisory last week warning of an uptick in reflection distributed denial-of-service (DDoS) attacks using Simple Network Management Protocol (SNMP).

Dating back to April 11, PLXsert researchers observed 14 SNMP reflection DDoS campaigns that targeted the consumer goods, gaming, hosting, non-profit and software-as-a-service industries, according to the advisory, which indicates the threat is considered a "medium" risk.

Prolexic researchers have witnessed an uptick in the number of DDoS attacks using SNMP.

On May 14, 2014 by Matthew Broersma 0

US security firm Imperva has reported a massive DNS distributed denial-of-service (DDoS) attack on one of its customers – ironically, launched from the servers of two providers of anti-DDoS services.

The attack, far from being an isolated incident, is part of a dangerous emerging trend, according to the company – that of using DNS floods, which it says can bring down even highly resilient networks.

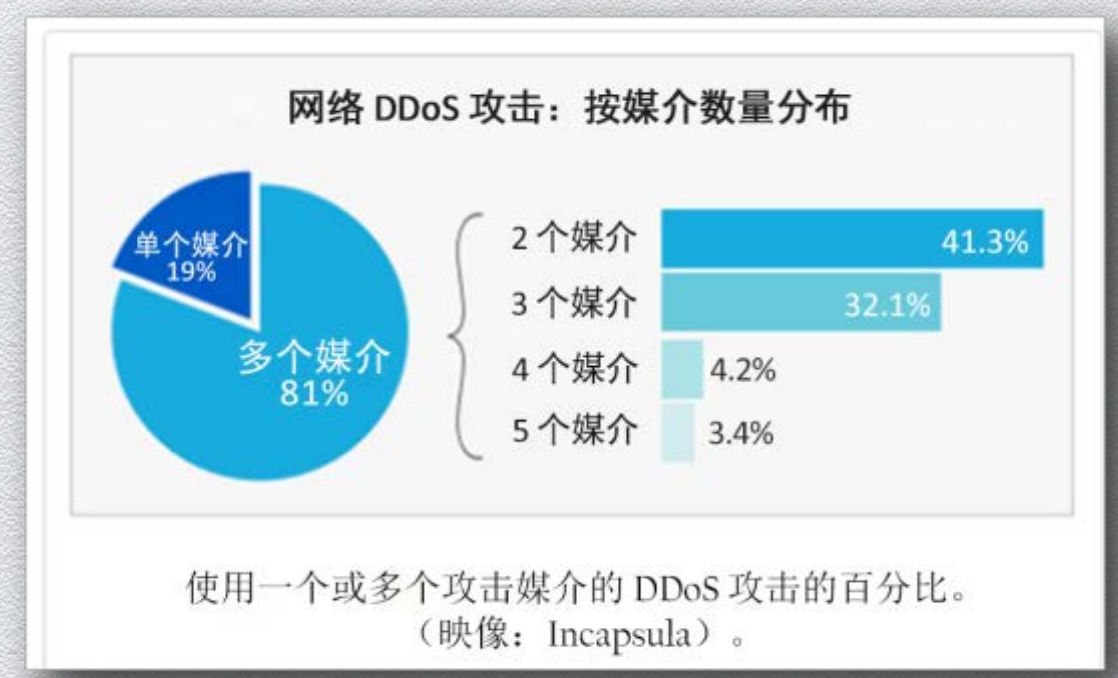
The research - which covers the whole of 2013 and the first two months of 2014 - says that 81 percent of DDoS attacks seen in 2014 are now multi-vectored, with almost one in every three attacks now above 20 Gbps in data volume

corero
FIRST LINE OF DEFENSE

#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

攻击者是否变得更加聪明？

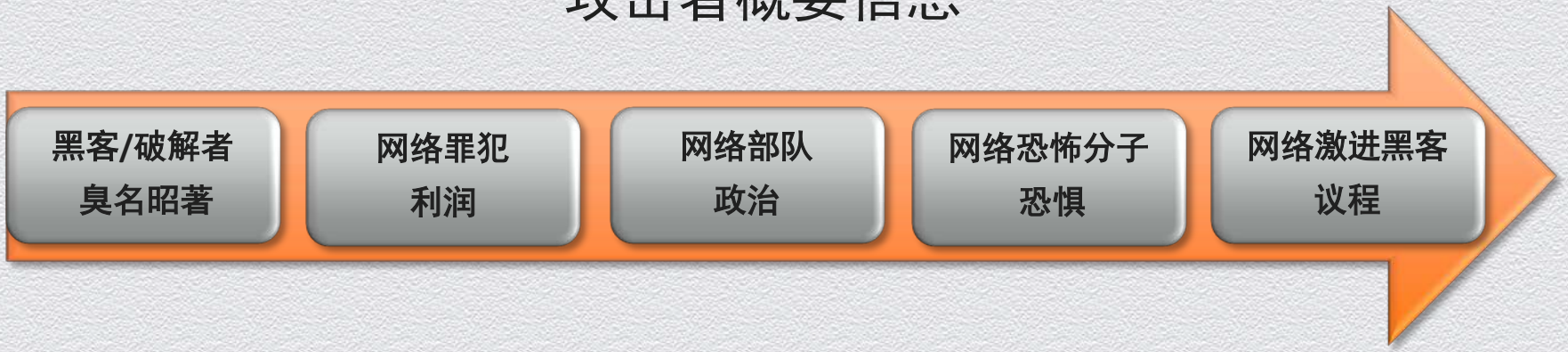
- 研究人员发现攻击者发起 DDoS 攻击的方式在增加
- 攻击者逐渐了解 DDoS 检测和防御*的方式*
- 攻击者在不断开发绕过传统防御的新方法



使用一个或多个攻击媒介的 DDoS 攻击的百分比。
（映像：Incapsula）。

攻击者的动机是否发生了变化？

攻击者概要信息



现在出现了一种新的黑客...

网络佣兵
为金钱不惜一切

不止一种！

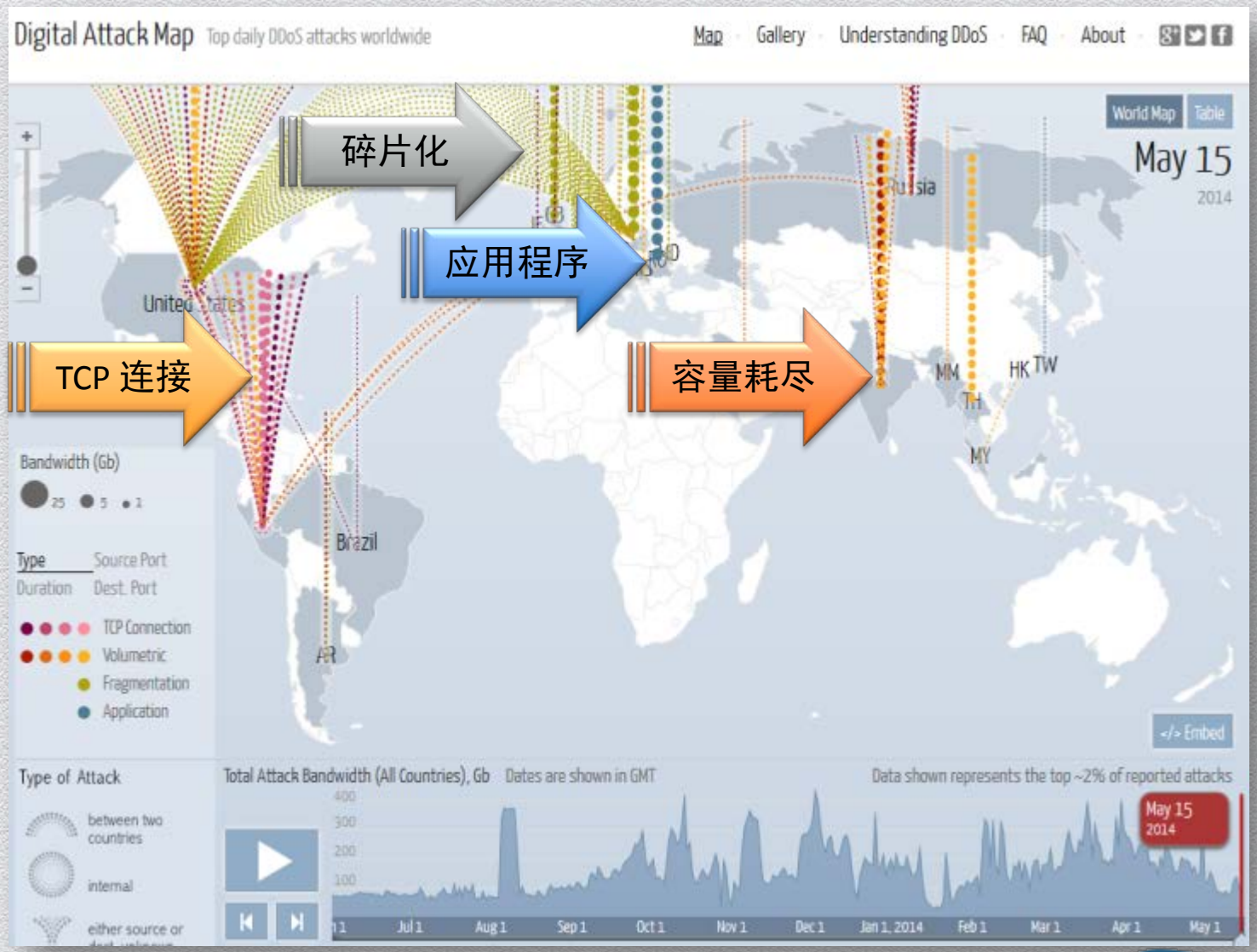
有哪些类/种 DDoS？

根据 SANS Institute 所做的最新调查 …

“多数破坏性 DDoS 攻击将容量耗尽攻击与有目标、针对具体应用程序的攻击混合在一起。”

DDoS 数字攻击映射

http://www.digitalattackmap.com/

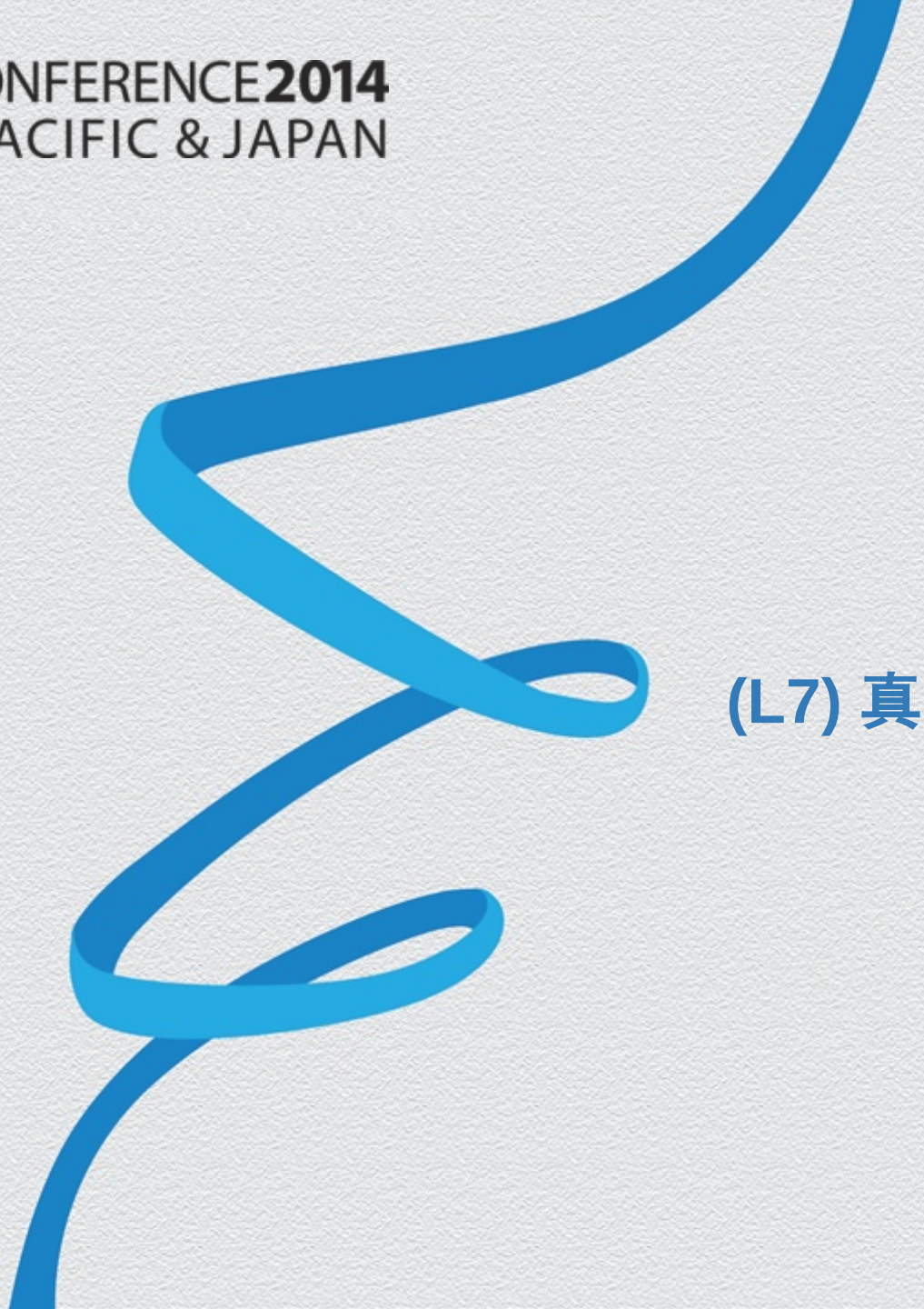


小心 (L7) 攻击！

能否举出一些 L7 攻击示例?

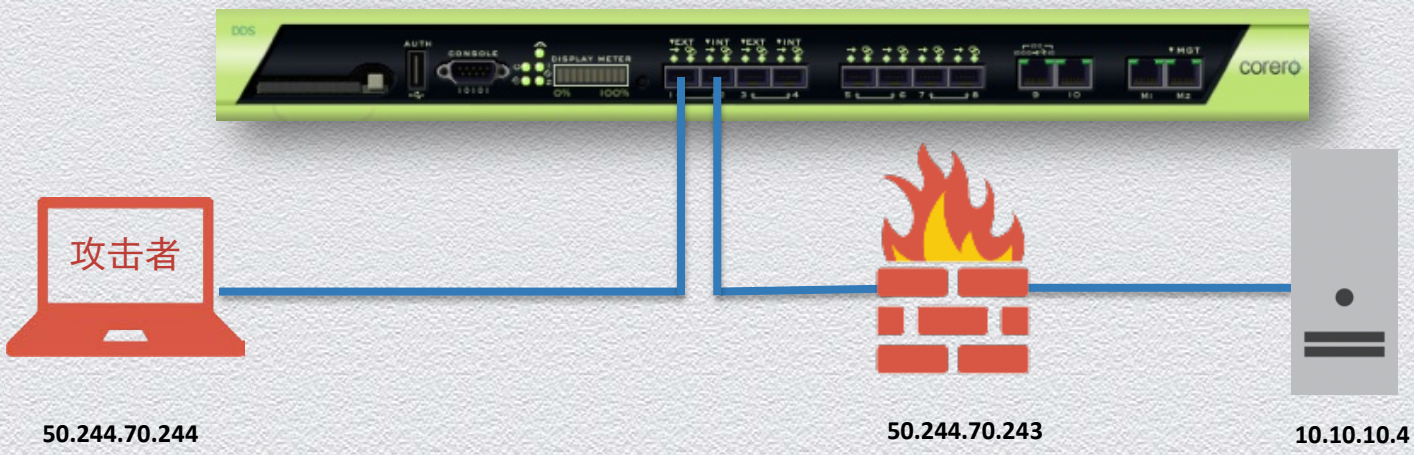
重复性:

- 主页、主页、主页
- 虚假登录尝试
- 忘记我的密码
- 随机关键字搜索
- SlowRead 下载
- 股票报价查询 1、2、3



(L7) 真实攻击演示

L7 攻击演示网络设置



50.244.70.244

攻击者

50.244.70.243

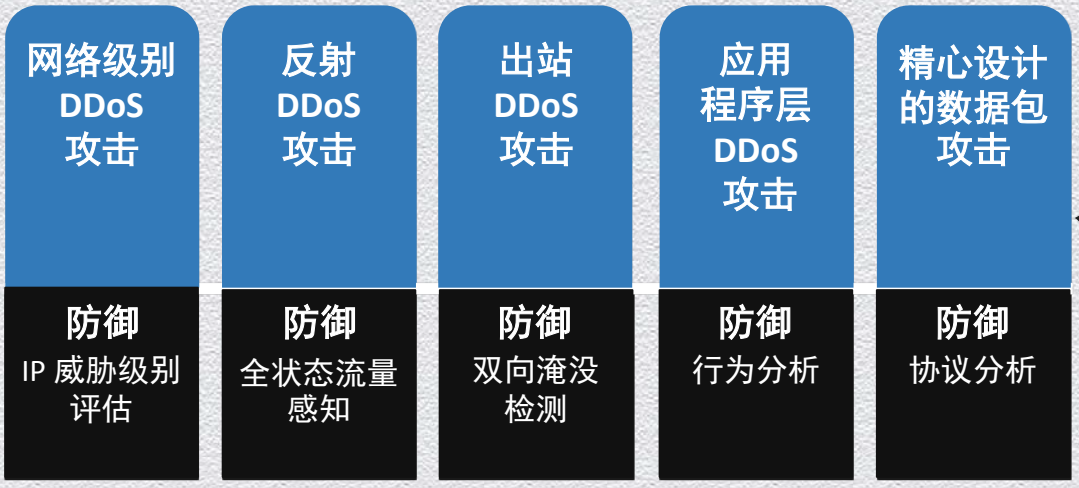
10.10.10.4

Apache Web 服务器

提前计划！

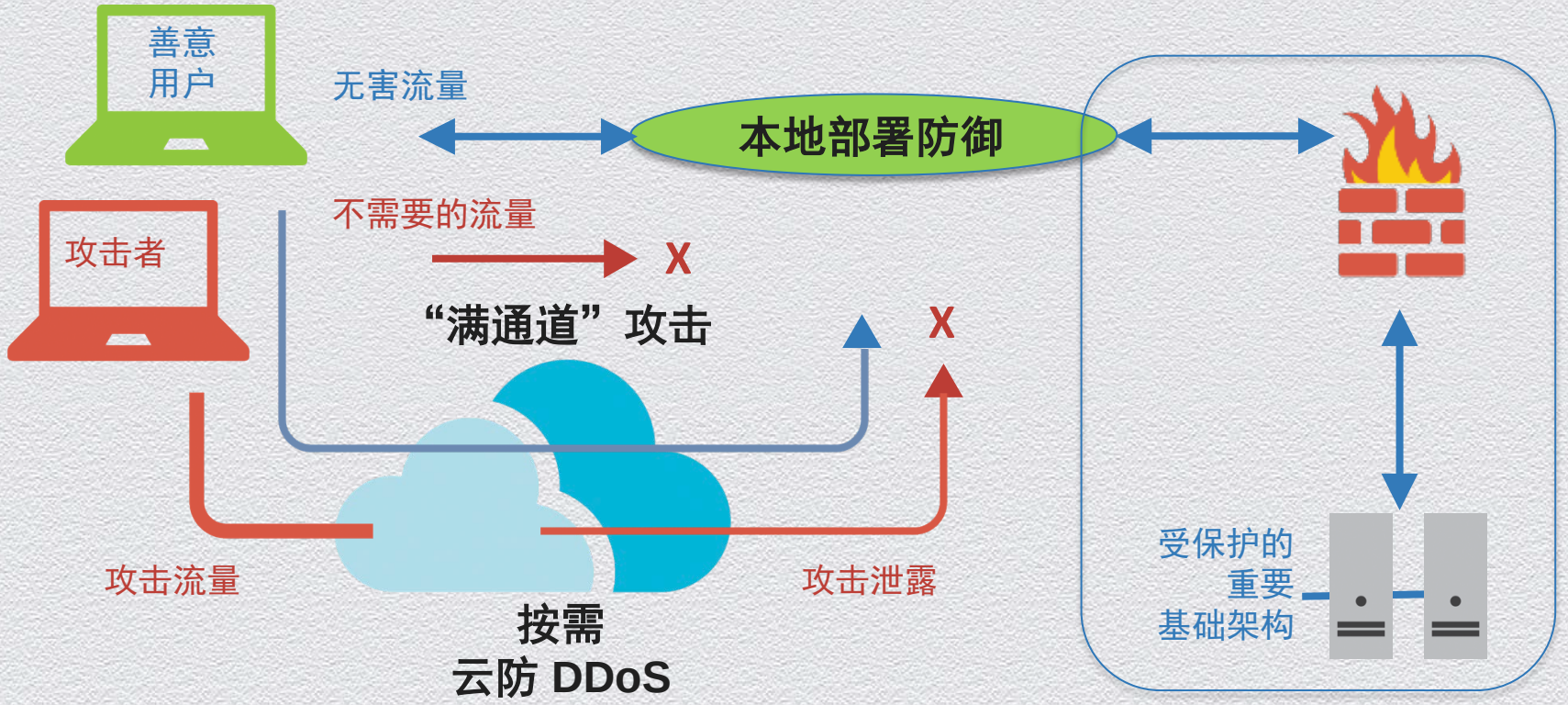
什么是最佳做法？

- 规划和回应 DDoS
- 评估 ISP“清理管道”服务
- 评估 DDoS“缓解为服务”选项
- 在本地部署 DDoS 检测和缓解设备



为何选择内部部署？

什么解决方案能应对所有 DDoS 攻击？



根据最新的 SANS 分析师调查：
混合解决方案的普遍程度是
本地或仅基于云的解决方案的四倍。

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

您阻止不了您所看到的东西！

#RSAC

您的可见性怎样？

- 部署具有以下功能的解决方案：
  - 提供全部的流量可见性
  - 监控所有传入连接
  - 监控所有传入请求
  - 阻止所有不需要的流量
  - 记录所有安全政策违反情况
  - 记录攻击流量 — PCAP
  - 收集攻击情报

小心混合式攻击！

混合式攻击是怎样的？

现在的老练 DDoS 攻击者会：

- 记录（概要描述）Web 存在
- 扫描基础架构和 Web 资源
- 启动网络级别容量耗尽攻击
- 维持淹没 — 假冒所有源 IP
- 启动低级而缓慢的应用程序攻击
- 启动精心设计的数据包攻击
- 启动 DNS 反射/放大攻击
- 尝试利用（破坏）下游服务器
- 尽可能同时启动多种攻击

组合攻击只是增加成功的几率！

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

来测试您的防御吧！

攻击者使用哪些手段？

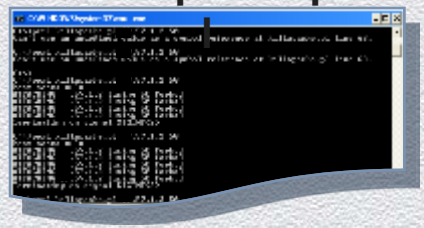
Hping3

NMAP

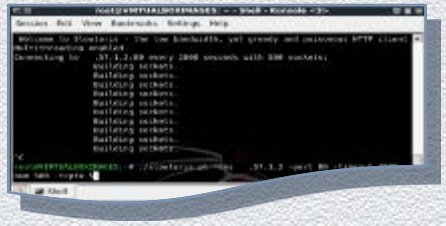
Low Orbit ION

High Orbit ION

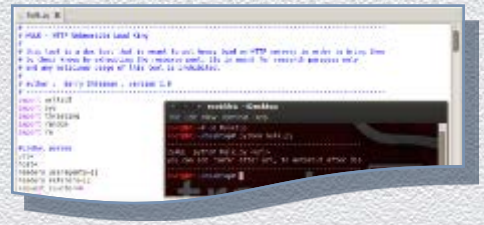
KillApache.p



Slowloris



HULK



Metasploit

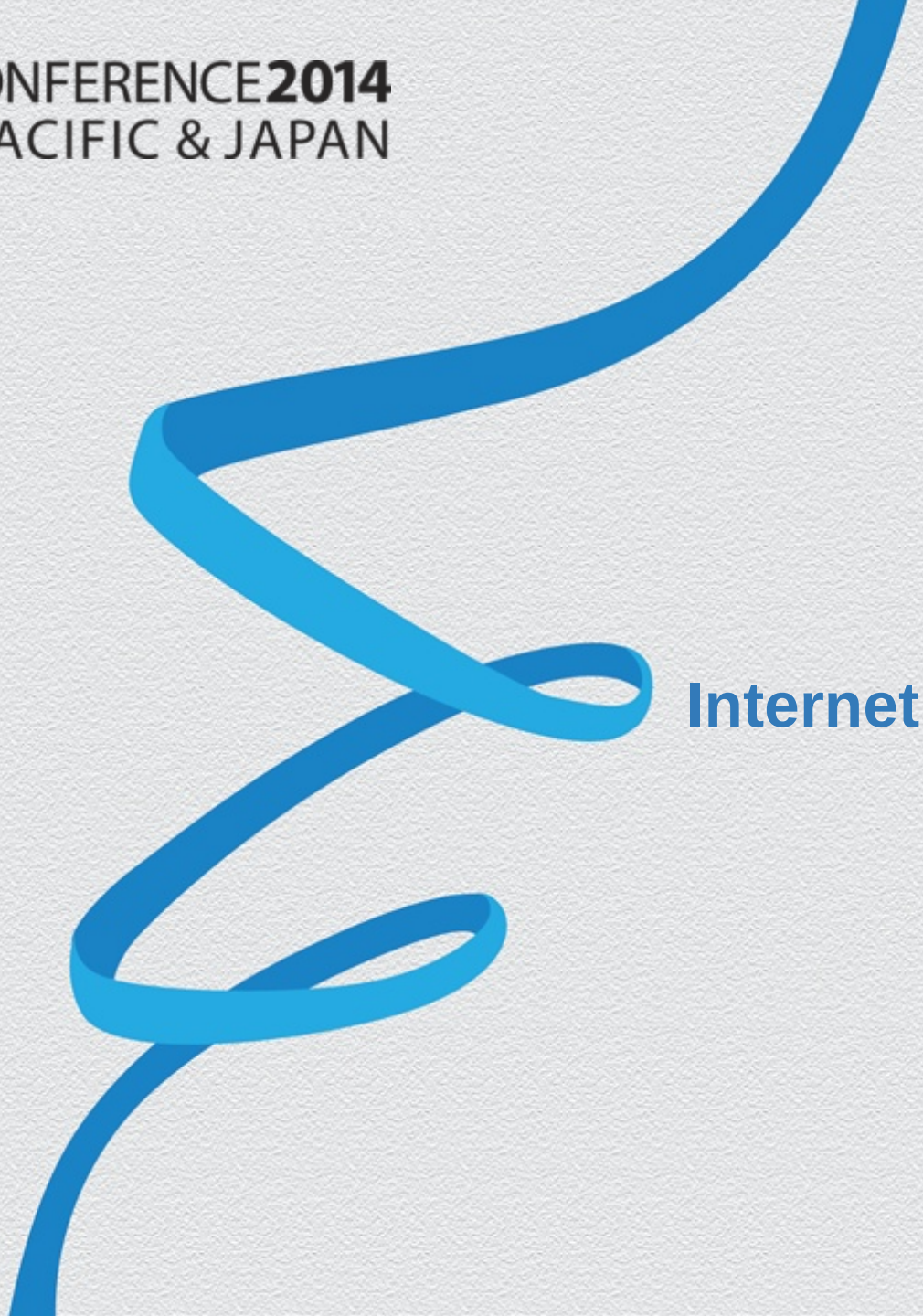
SlowHTTPtest

提出有价值的问题！

您是否知道您的 SLA 覆盖的范围？

- 确保您知道覆盖和未覆盖的范围
- 要求您的 ISP 根据新的攻击媒介和工具进行防御
- 要求您的 ISP 遵循最佳通用做法，例如 BCP-38/RFC 2827 http://www.rfc-base.org/rfc-2827.html
- 要求您的 ISP 做更多有助于解决 DDoS 和网络威胁问题的事情
- 要求您的 ISP 开始提供带宽清理选项
- 如果您不满意，那么考虑其他选项

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN



Internet 需要新的一线防御

我的 FW、IPS 或 SLB 无法抵御 DDoS?

问题

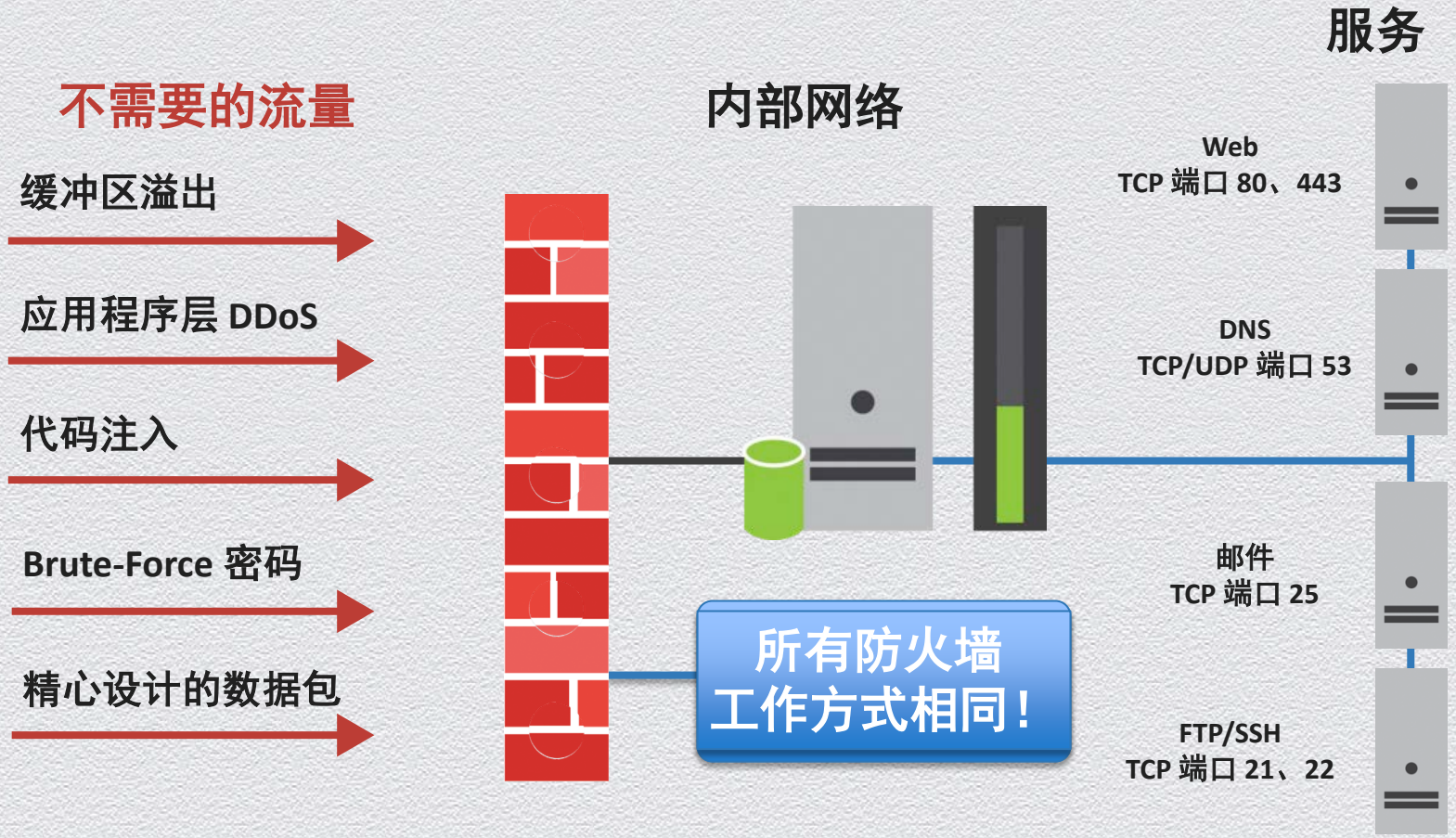
- 很多安全设备声称具有 DDoS 保护
- 大多数仅有单一的配置

建议

寻找有以下特点的解决方案：

- 特意设计的
- 具有极其精细的配置
- 能抵御所有攻击媒介
- 能处理负载
- 不能是 DDoS'd 自身
- 包括全天候支持服务

防火墙是否能阻止 L7 攻击？

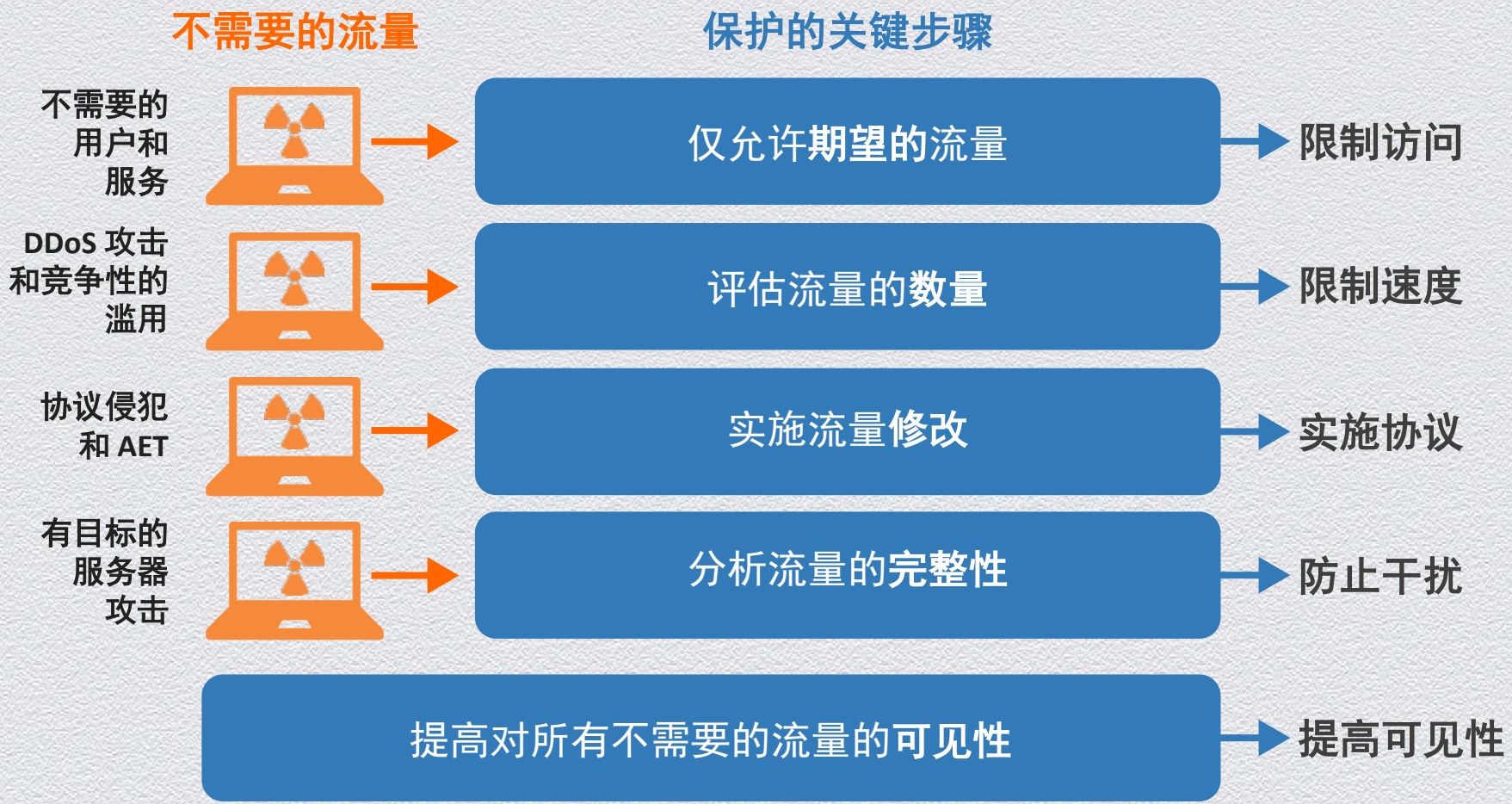


我的服务提供商无法阻止所有 DDoS？

某些服务提供商可能能够提供帮助！

- 但是，并非所有服务提供商有合适的：
  - 设备
  - 经验
  - L2-L7 可见性
  - 安全的服务方案

如何解决此问题？


不需要的流量
保护的关键步骤
不需要的用户和服务
仅允许期望的流量
限制访问
DDoS 攻击和竞争性的滥用
评估流量的数量
限制速度
协议侵犯和 AET
实施流量修改
实施协议
有目标的服务器攻击
分析流量的完整性
防止干扰
提高对所有不需要的流量的可见性
提高可见性

如何了解详细信息？

查看我们的网站

如果您需要今天演示的 PDF 副本，请发送电子邮件到 info@corero.com

有问题吗？请将问题转发到 stephen.gates@corero.com

查看我的博客 @ www.SecurityBistro.com

在 Linkedin 上联系我们 — www.linkedin.com/in/securitystephengates/

在 Twitter 上关注我们 — @Corero

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

谢谢大家！

Stephen.Gates@Corero.com