

Understanding and Defending Against the Modern DDoS Threat

SESSION ID: CLE-T09

Stephen Gates

Chief Security Evangelist
Corero Network Security
@StephenJGates



RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN

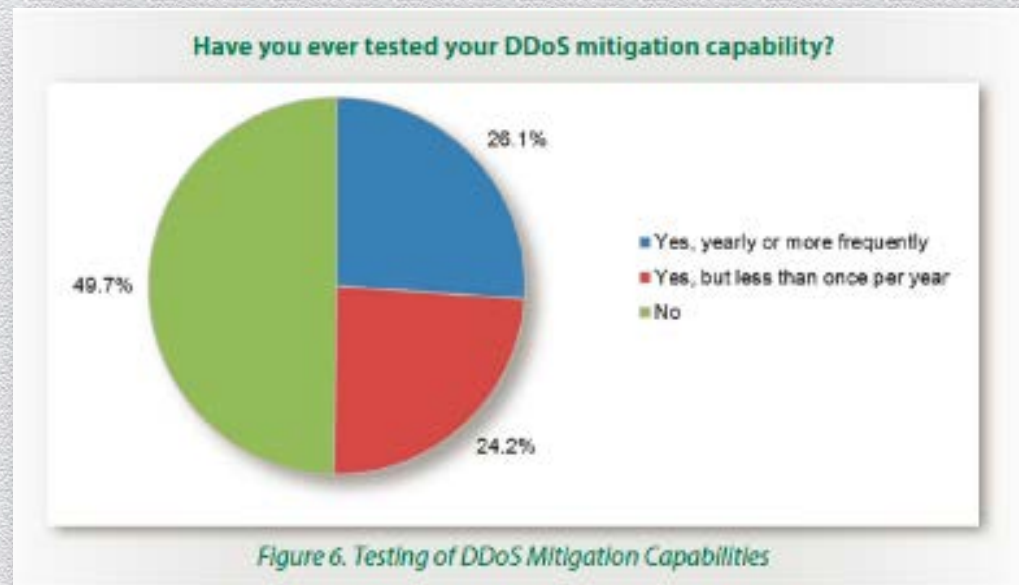


**Understand you're
vulnerable!**

How well are others preparing?

- ◆ **40%** of enterprises are completely or mostly unprepared
- ◆ **23%** of respondents indicated they did not have a plan
- ◆ **16%** were unaware of any such current or future plans
- ◆ **26%** are still relying on their operational infrastructure
- ◆ **50%** have never tested their DDoS defense capabilities

Access the entire report:
www.corero.com/SANS-DDoS-Survey



RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



**Easy to launch -
tough to stop!**

Do DDoS attacks really work?

Akamai

By Jennifer LeClair
January 28, 2014

In its State of the Industry report, Akamai reports a 10 percent year-over-year performance increase.

» The Internet's performance was slightly slower than last year, but there were many positives in all of 2012. Akamai's State of the Industry report offers a look at the future of the Internet speeds, attacks and more.



Attacker DDoS attacks



Candice So @candice_so
Published: March 28th, 2014

Distributed denial of service (DDoS) attacks are getting more sophisticated. Security researchers are becoming wise to the ways of DDoS threat prevention from Incapsula Inc., a U.S.-based security solutions provider.

The Phnom Penh Post

HOME NATIONAL BUSINESS LIFESTYLE SPORT COLUMNS



Members of Anonymous Cambodia arrested in Cambodia has sworn to step up efforts to respond to assault on government websites. Photo: Phnom Penh Post

Anonymous vows re

Fri, 25 April 2014 Kevin Ponniah

Anonymous Cambodia has pledged to step up efforts to respond to assault on government websites in response to the international "hacktivist" group's recent actions.

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

28 Apr 2014 DPC Comments Off

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.

On May 14, 2014 by Matthew Broersma

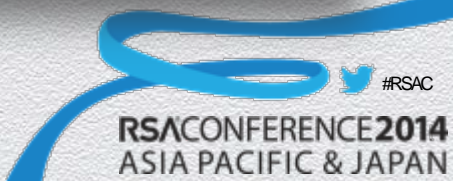
US security firm Imperva has reported a massive **DNS distributed denial-of-service (DDoS)** attack on one of its customers – ironically, launched from the servers of two providers of anti-DDoS services.

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.



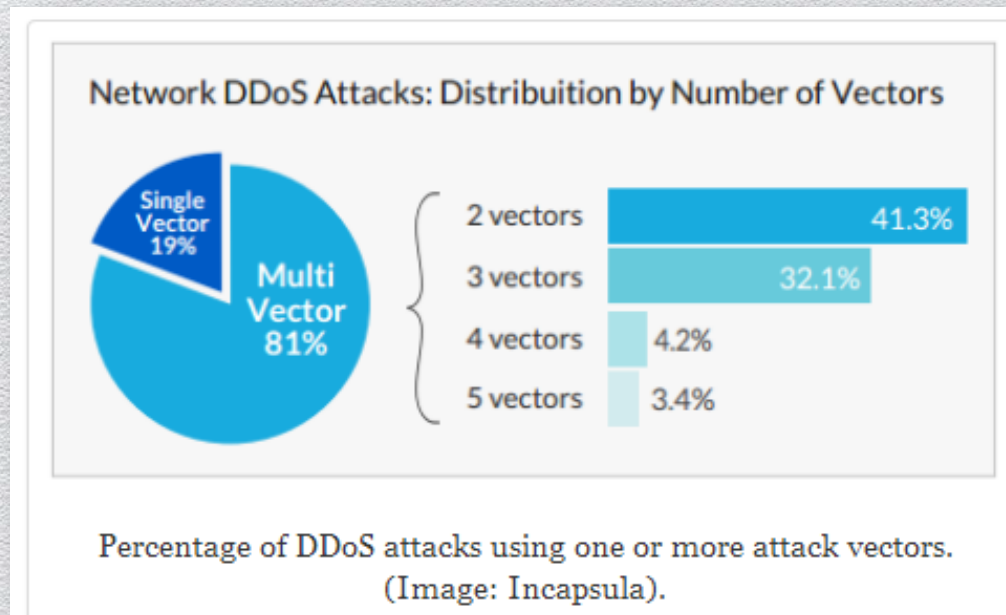
Prolexic researchers have witnessed an uptick in the number of DDoS attacks using SNMP.

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.



Are the attackers getting smarter?

- ◆ Researchers have spotted an uptick in the number of ways attackers are launching DDoS attacks
- ◆ Attackers are becoming *wise to the ways* of DDoS detection and defenses
- ◆ Attackers are developing new methods of bypassing traditional defenses



Have the attacker's motivations changed?

Attacker Profiles



Today there is a new category of attacker...

Cyber Mercenary
Anything for Money

RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



**There is more than
one type!**

What categories/types of DDoS are there?

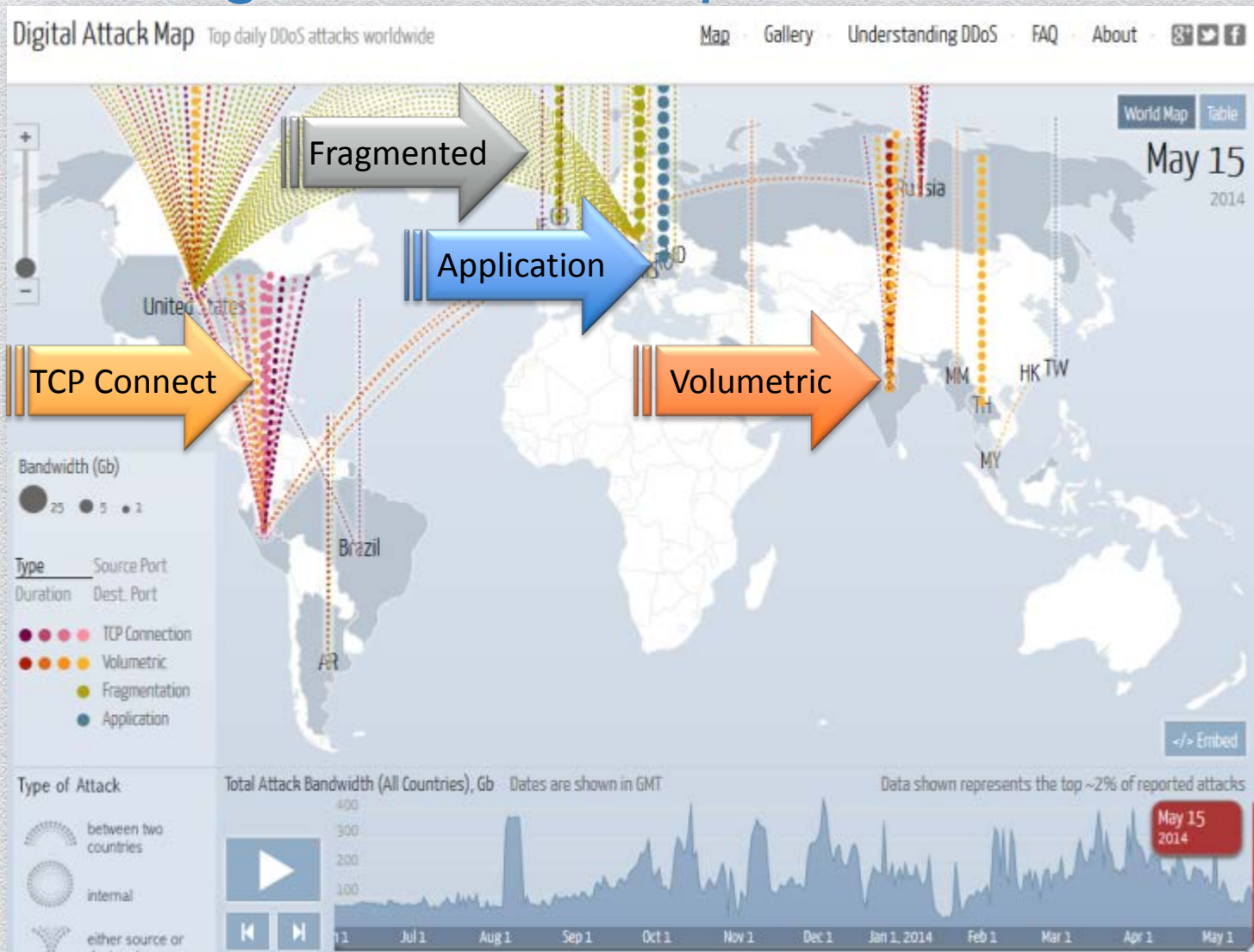
Network Level DDoS Attacks	Reflective DDoS Attacks	Outbound DDoS Attacks	Application Layer DDoS Attacks	Specially Crafted Packet Attacks
Defense IP Threat-Level Assessment	Defense Stateful Flow Awareness	Defense Bi-Directional Flood Detection	Defense Behavior Analysis	Defense Protocol Analysis

According to a recent survey conducted by the SANS Institute...

“The most damaging DDoS attacks mix volumetric attacks with targeted, application-specific attacks.”

DDoS Digital Attack Map

<http://www.digitalattackmap.com/>



RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



Beware of (L7) attacks!

What are some examples of L7 attacks?

Repetitive:

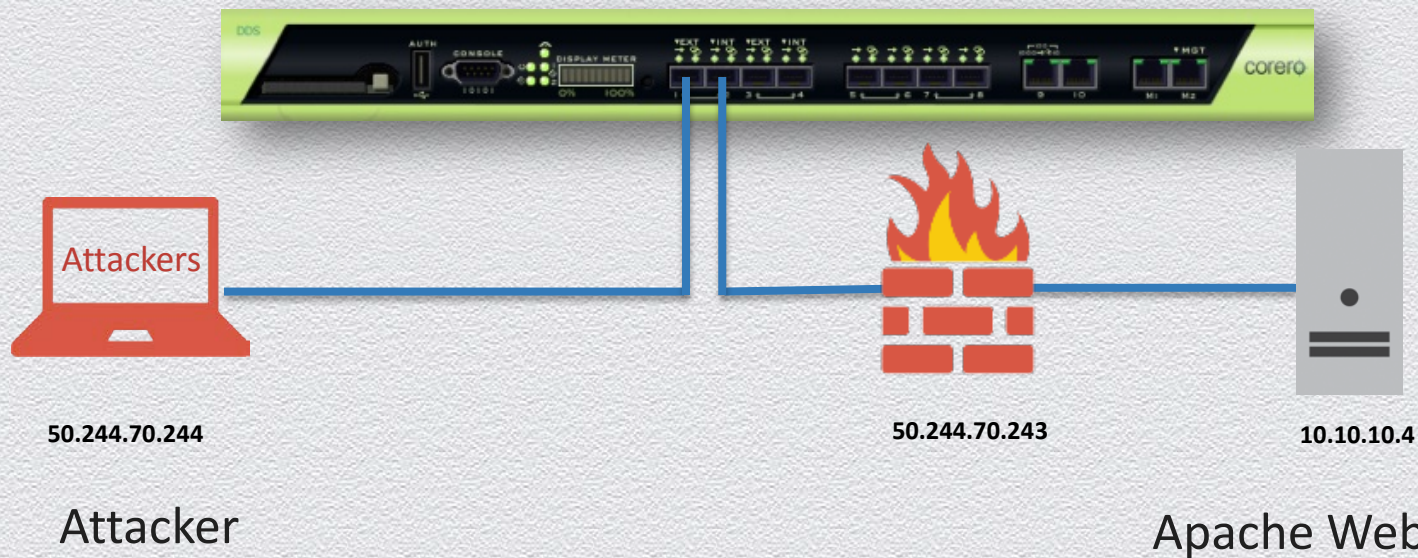
- ◆ Home page, home page, home page
- ◆ Bogus login attempt
- ◆ Forgot my password
- ◆ Random keyword search
- ◆ SlowRead downloads
- ◆ Stock quote lookups 1,2,3





**(L7) live attack
demonstration**

L7 Attack Demo Network Setup



RSAC CONFERENCE **2014**
ASIA PACIFIC & JAPAN



Plan ahead!

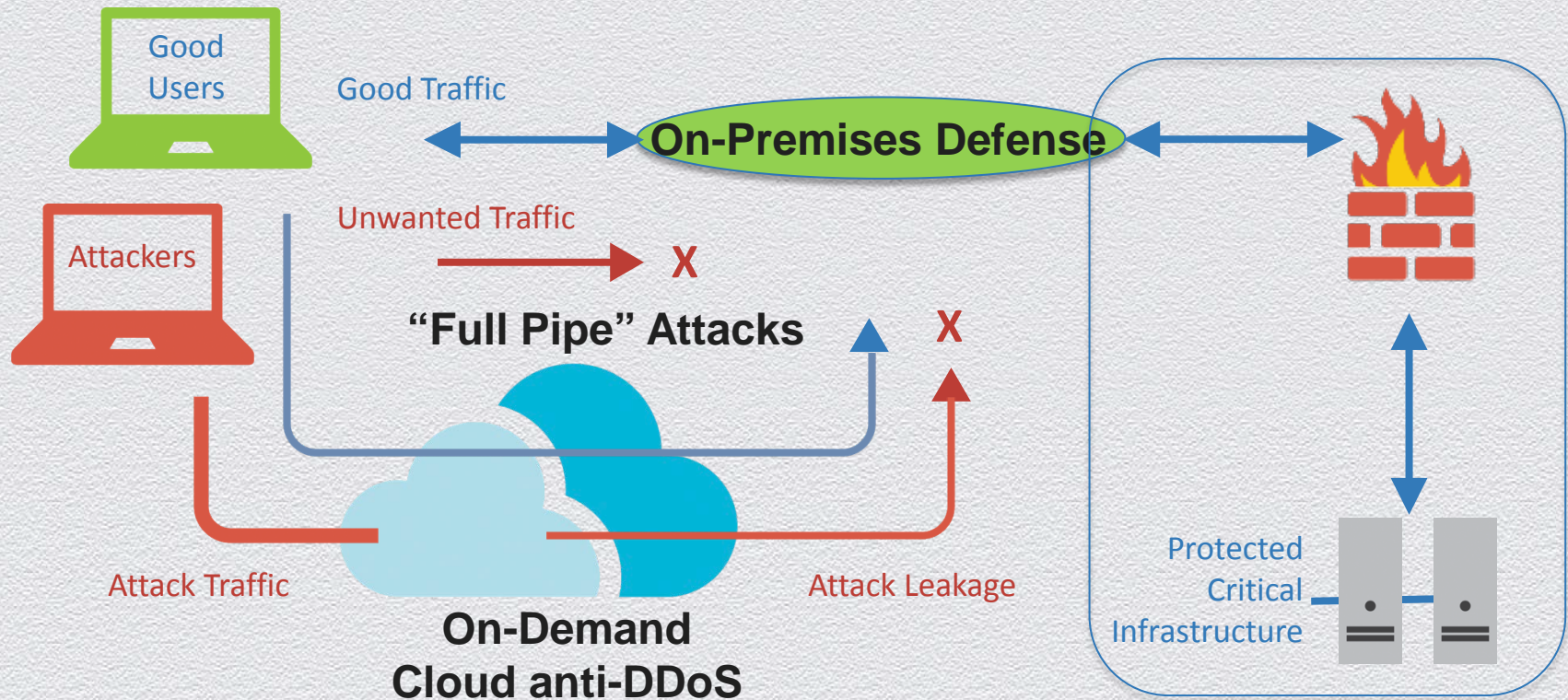
What are the best practices?

- ◆ Address Planning-for and Response-to DDoS
- ◆ Evaluate ISP "Clean Pipe" Services
- ◆ Evaluate DDoS "Mitigation as a Service" Options
- ◆ Deploy DDoS Detection and Mitigation Equipment on Premises

Network Level DDoS Attacks	Reflective DDoS Attacks	Outbound DDoS Attacks	Application Layer DDoS Attacks	Specially Crafted Packet Attacks
Defense IP Threat-Level Assessment	Defense Stateful Flow Awareness	Defense Bi-Directional Flood Detection	Defense Behavior Analysis	Defense Protocol Analysis

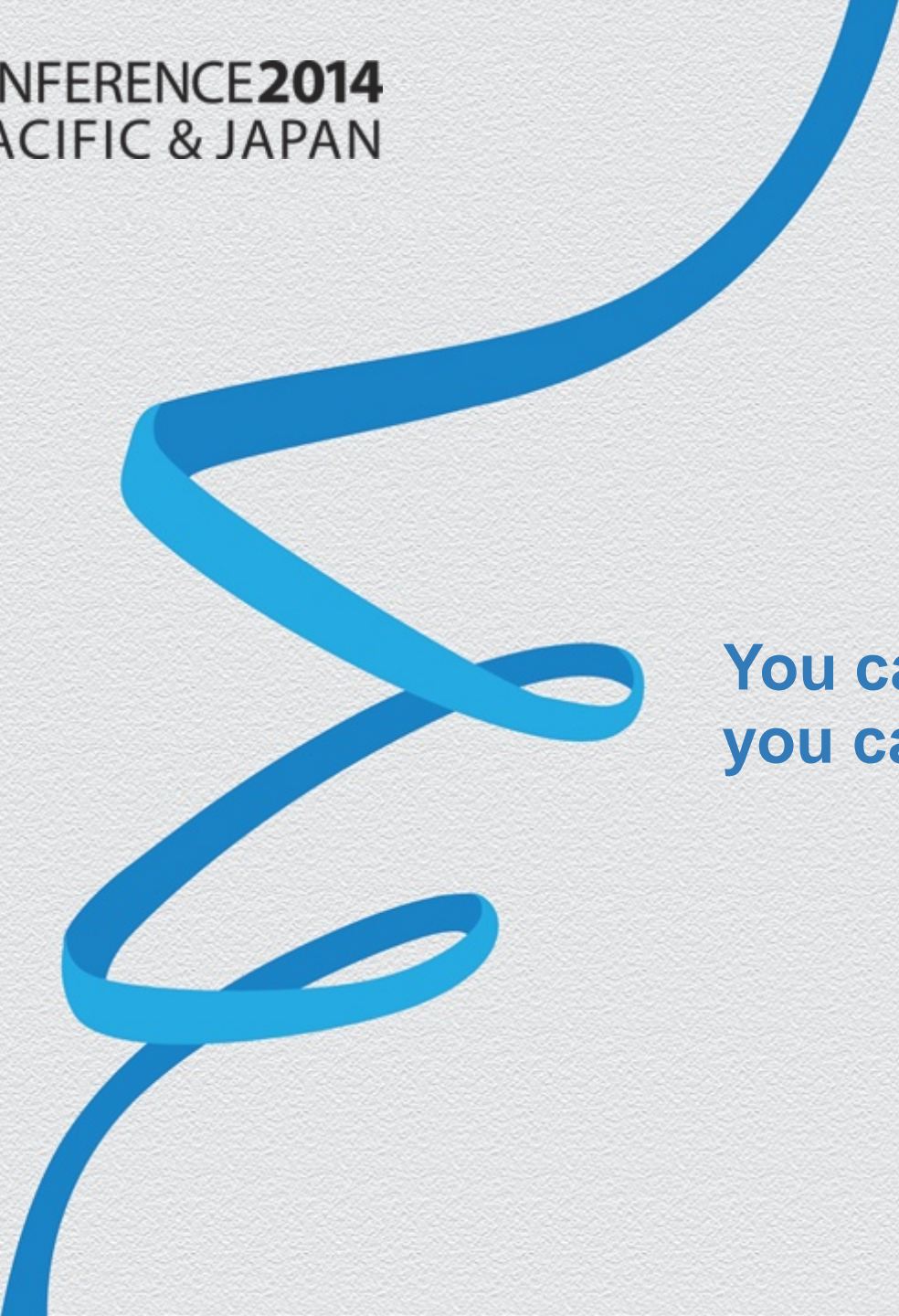
Why on-premises?

What solution addresses all DDoS attacks?



According to a recent SANS Analyst survey:
Hybrid solutions are nearly four times more prevalent than
on-premise or cloud-only solutions.

RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN




**You can't block what
you can't see!**

What does your visibility look like?

- ◆ Deploy solutions that:
 - ◆ Provide complete traffic visibility
 - ◆ Monitor all incoming connections
 - ◆ Monitor all incoming requests
 - ◆ Block all unwanted traffic
 - ◆ Log all security policy violations
 - ◆ Record attack traffic – PCAP
 - ◆ Gather attack intelligence



RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



**Watch for blended
attacks!**

What does a blended attack look like?

Today's sophisticated DDoS Attackers will:

- ◆ Footprint (profile) the Web Presence
- ◆ Scan the infrastructure and Web resources
- ◆ Initiate network-level volumetric attack
- ◆ Maintain Flood – spoof all source IPs
- ◆ Initiate low-and-slow application attacks
- ◆ Initiate specially-crafted packet attacks
- ◆ Initiate DNS reflective/amplified attacks
- ◆ Attempt to exploit (compromise) downstream servers
- ◆ Simultaneously launch as many types of attacks as possible



A combined attack simply increases the chances of success!

RSAC CONFERENCE **2014**
ASIA PACIFIC & JAPAN



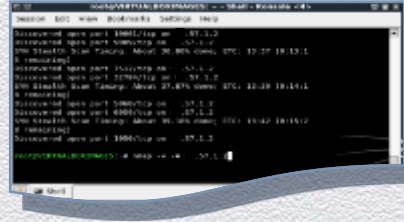
Test your defenses!

What are the attackers using?

Hping3



NMAP



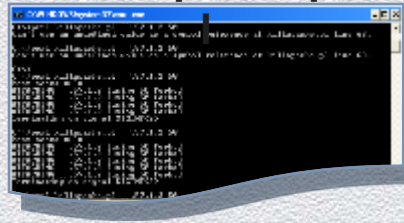
Low Orbit ION



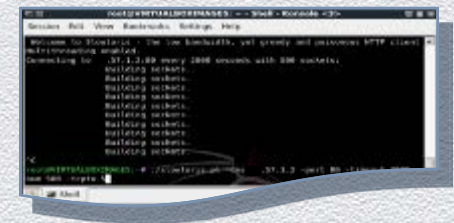
High Orbit ION



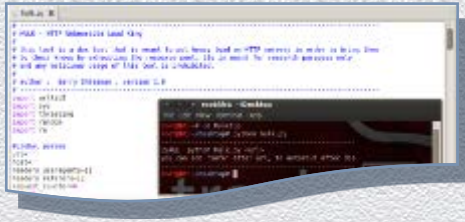
KillApache.p



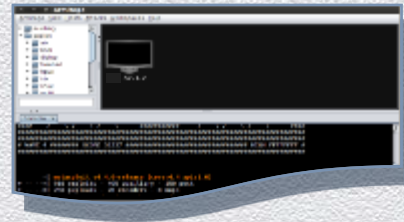
Slowloris



HULK



Metasploit



SlowHTTPtest



RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



Ask good questions!

Do you know what your SLA covers?

- ◆ Ensure you know what's covered & what's not
- ◆ Ask you ISP regularly about their defenses with regards to new attack vectors and tools
- ◆ Ask your ISP to adhere to Best Common Practices for example – BCP-38/RFC 2827 <http://www.rfc-base.org/rfc-2827.html>
- ◆ Ask your ISP to do more to help solve the DDoS and cyber threat issue
- ◆ Ask your ISP to start offering cleaner-bandwidth options
- ◆ If you're not satisfied then consider other options

RSAC CONFERENCE 2014
ASIA PACIFIC & JAPAN



The Internet Needs a New First Line of Defense

Can't my FW, IPS or SLB defeat DDoS?

Problem

- ◆ Many security devices claim to have DDoS protection
- ◆ Most have a single configuration

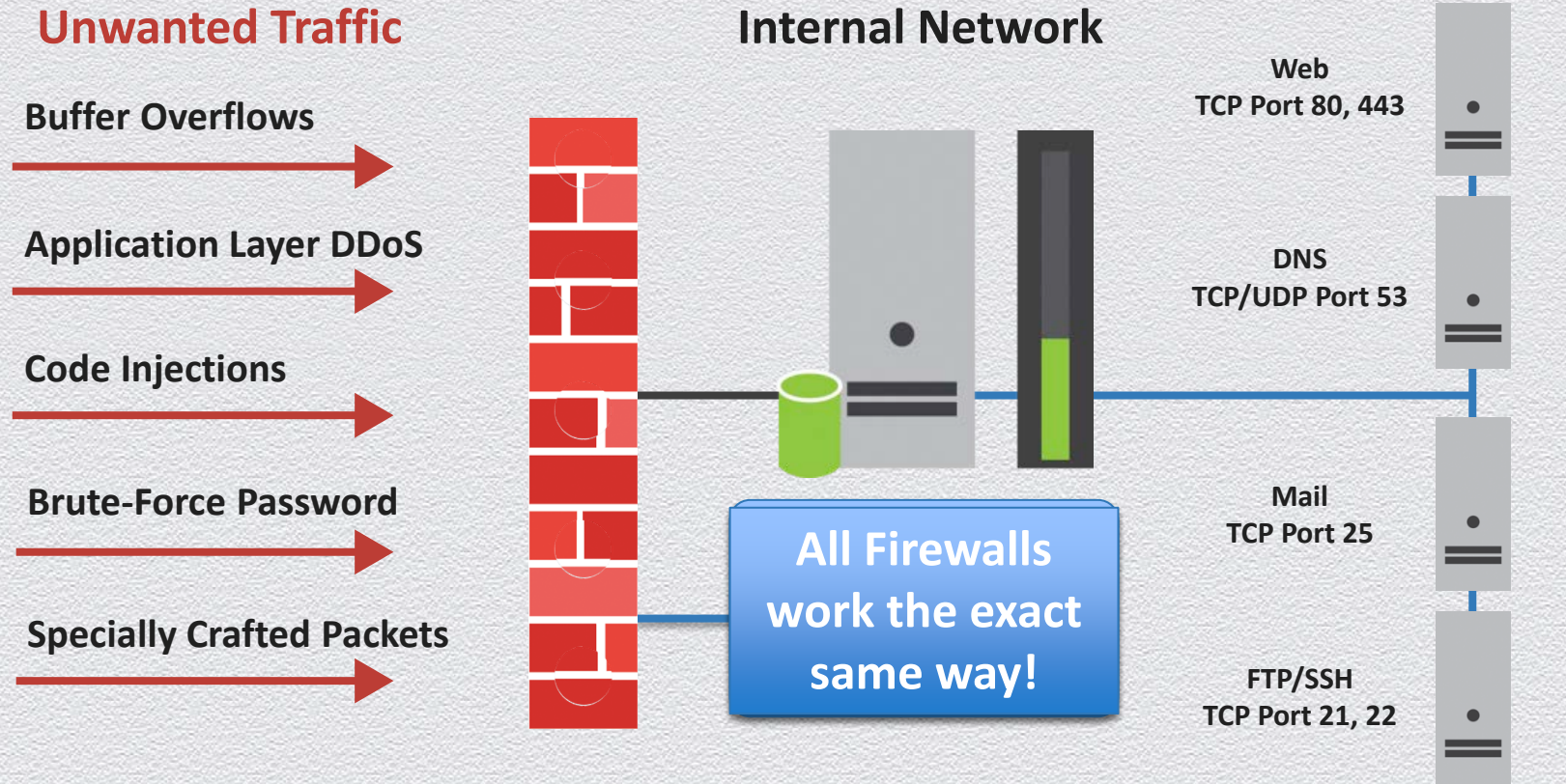
Recommendation

Find Solutions that:

- ◆ are purposely designed
- ◆ have extremely granular configurations
- ◆ can defend against all attack vectors
- ◆ can handle the load
- ◆ cannot be DDoS'd itself
- ◆ include 24x7 support services



Can firewalls block L7 attacks?



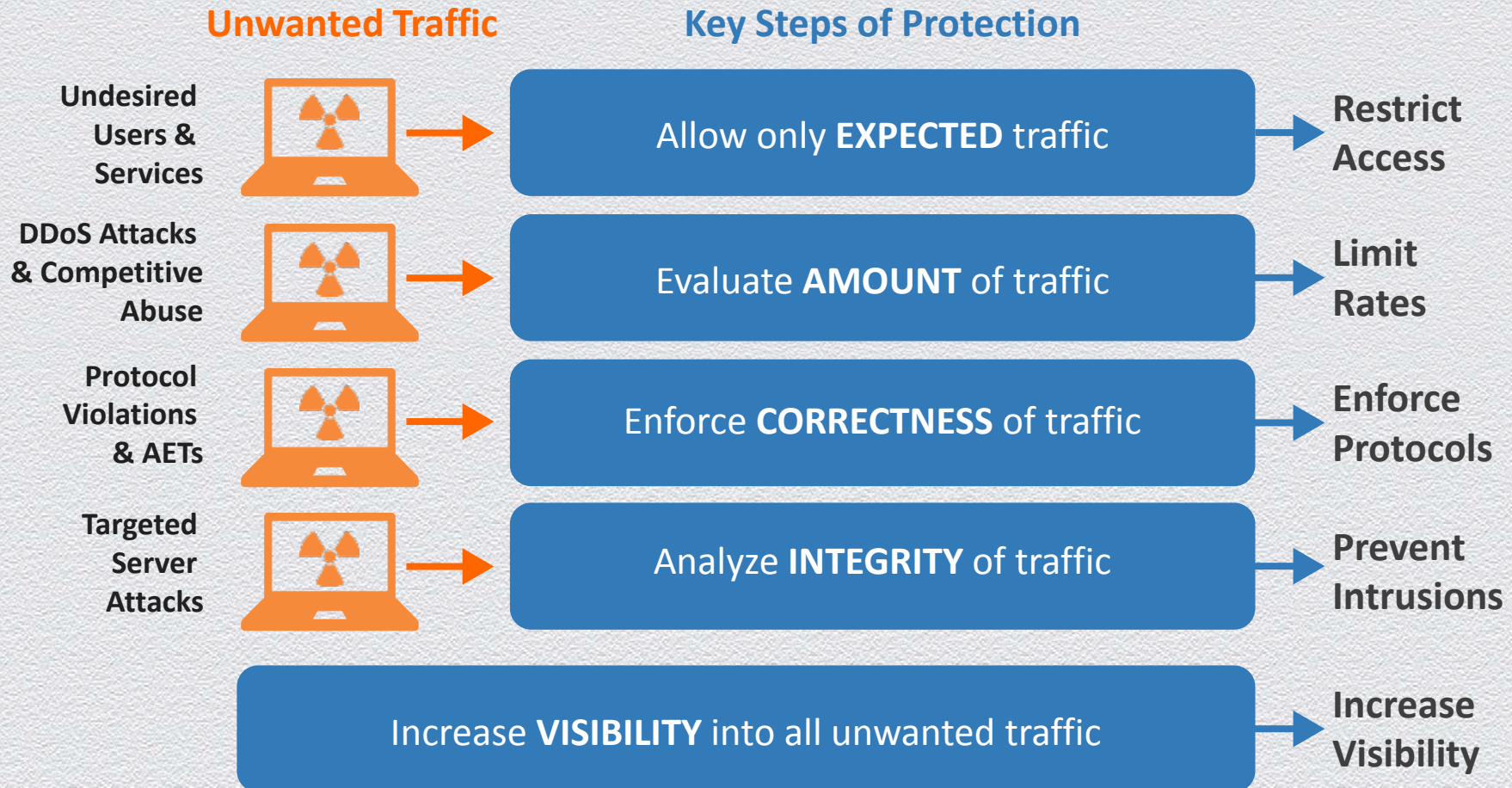
Can't my Service Provider Block all DDoS?

Some service providers might be able to help!



- ◆ However not all service providers have the right:
 - ◆ Equipment
 - ◆ Experience
 - ◆ L2-L7 Visibility
 - ◆ Secure service offerings

What's going to solve this problem?



How can I learn more?

Check Out Our Website

If you'd like a PDF copy of today's presentation, email info@corero.com

Questions? Please forward them to stephen.gates@corero.com

Check out my blog @ www.SecurityBistro.com

Connect on LinkedIn - www.linkedin.com/in/securitystephengates/

Follow us on Twitter - @Corero

Thank You!

Stephen.Gates@Corero.com



Enterprise



Hosting



Service Provider



MSSP