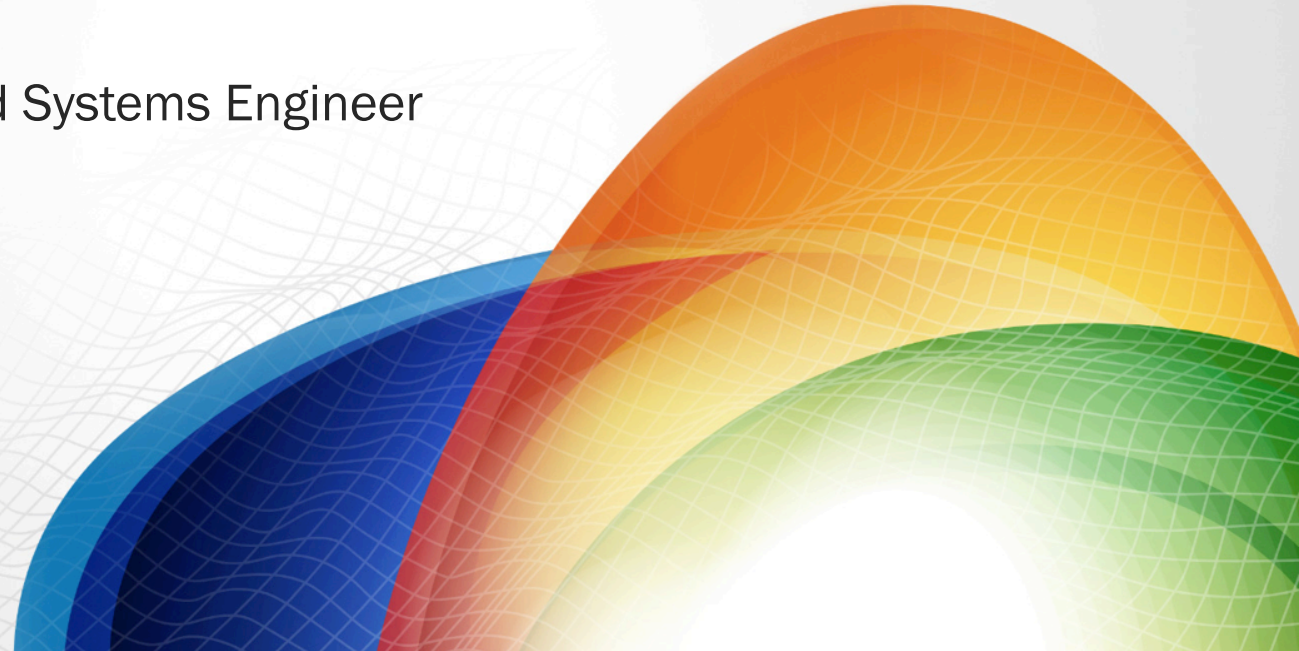
Herding Cats

Carl Brothers, F5 Field Systems Engineer



Agenda

- Introductions
- Security is easy, right
- Trivia
- Protecting your apps, one layer at a time
- How to survive an Attack – Time permitting

Securing applications can be complex

Attack visibility
Is often lacking details to truly track and identify attacks and their source, and ensure compliance and forensics

Ownership
Challenges with security team making the dev team fix vulnerabilities

Webification
Impossible to build safeguards into applications in a timely manner

Changing threats
increasing in complexity that requires intelligence and on-going learning

Scalability and performance
Needed to ensure services are available during the onset of aggressive attacks

Common attacks on web applications

CSRF
OWASP top 10
Forceful browsing
Web scraping
SQL injections
Field manipulation
Cross-site scripting
Command injection
Bots
Cookie manipulation
Brute force attacks
Buffer overflows
Parameter tampering
Information leakage
Session high jacking
Zero-day attacks
ClickJacking
Business logic flaws

Quick Trivia – the Cuckoo's Egg

Trivia Question 1

- What do the following have in common?
  1. 2600, the Hacker Quarterly
  2. Captain Crunch
  3. Blue Box

Trivia Question 2

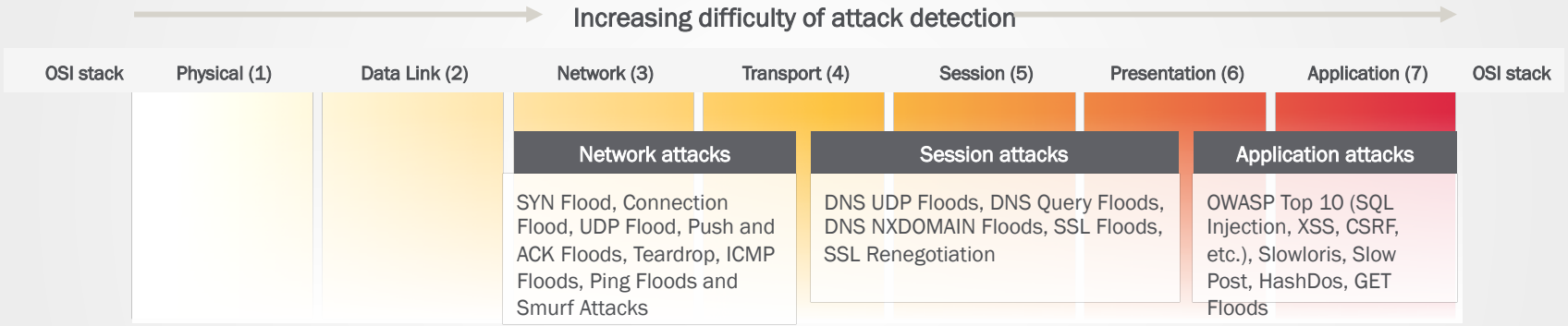
- What do these things have in common?
  - Waste of computer time at Harvard
  - One of Homer's greatest works
  - Doggonit, it's hard to compute

Trivia Question 3

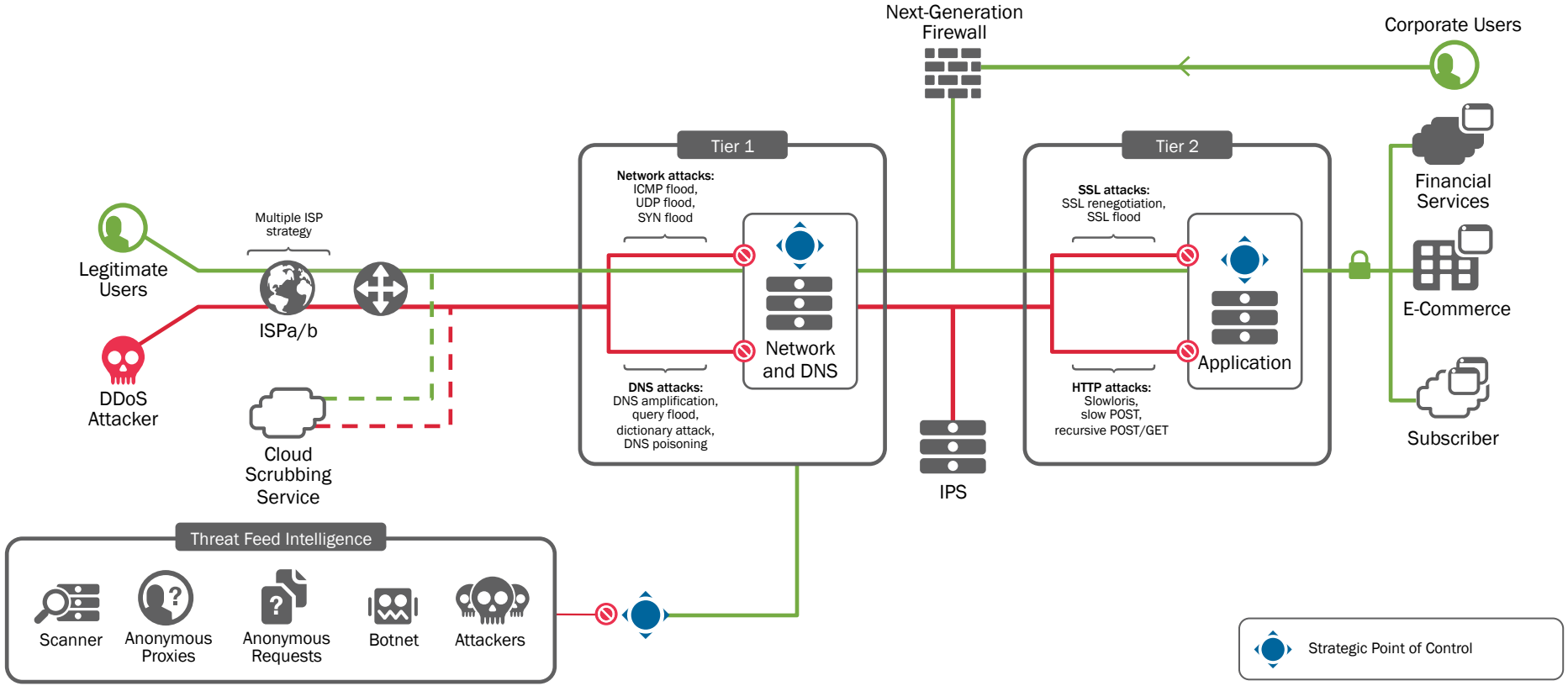
- Band who sang the song Low Rider?

Protecting your apps, one layer at a time

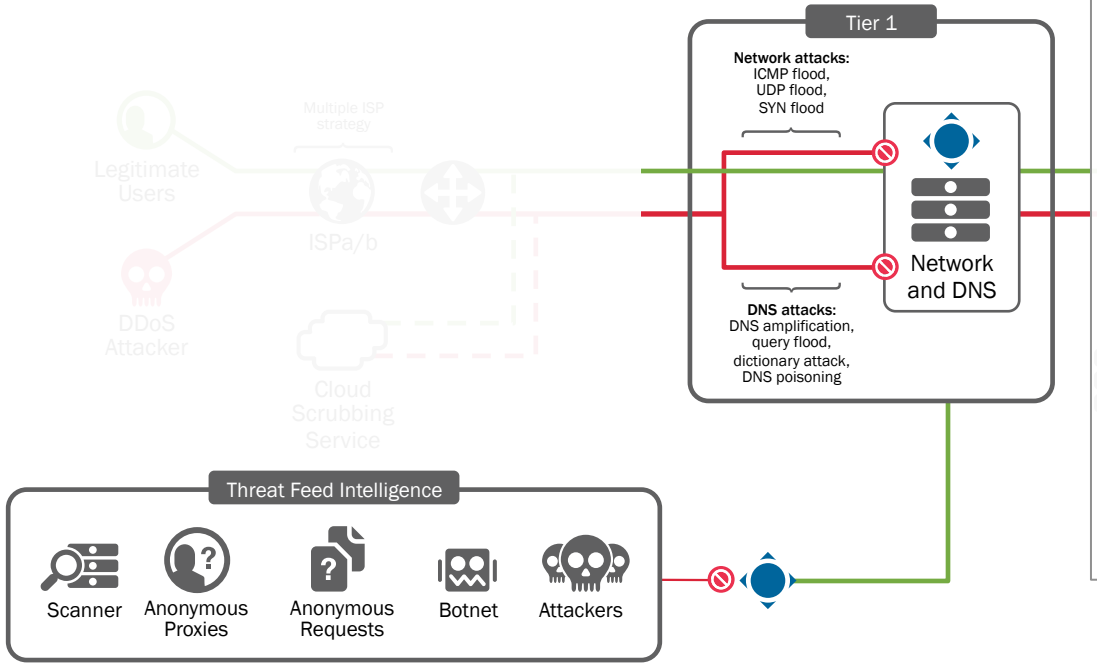
Attacks by the Layer



Reference Architecture



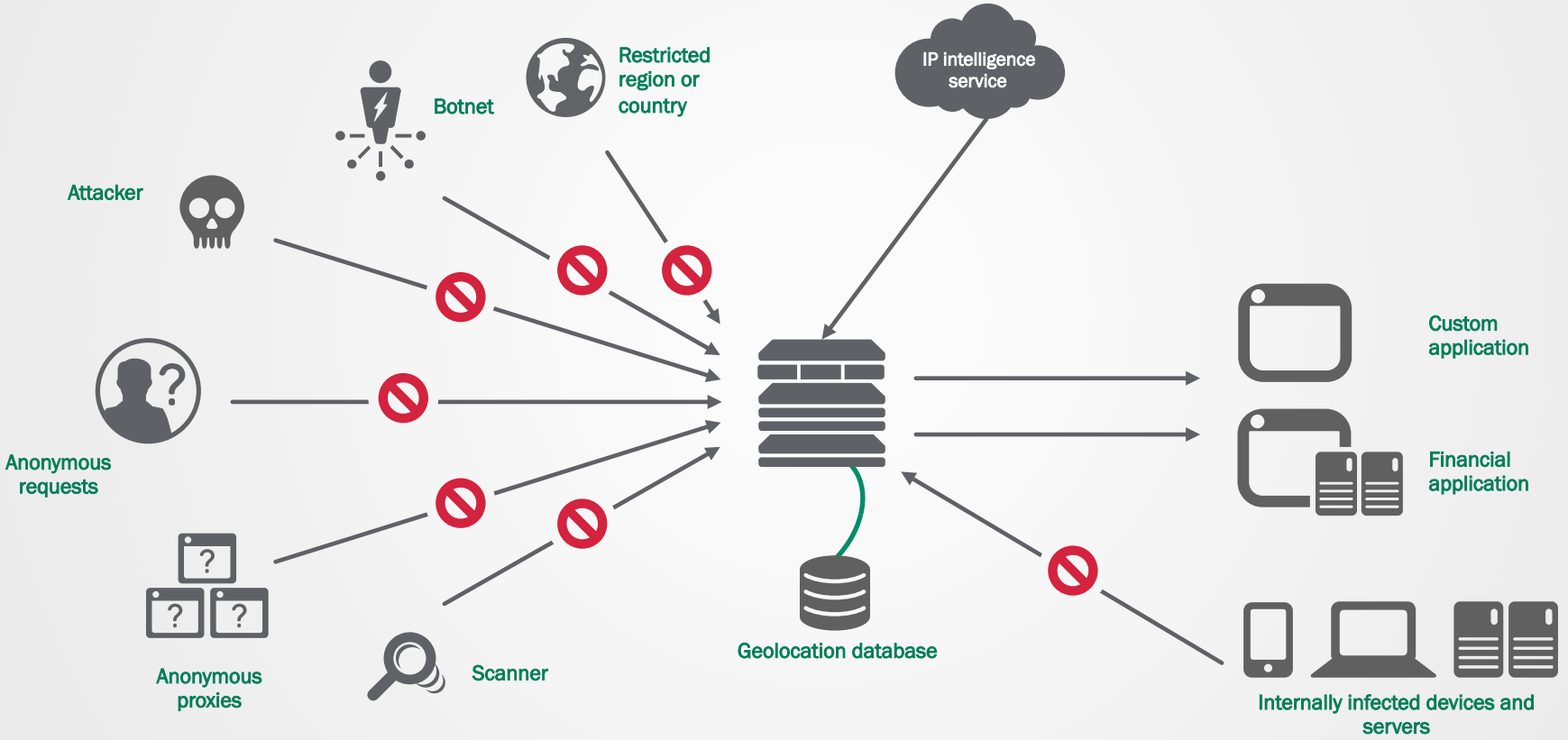
Reference Architecture



TIER 1 KEY FEATURES

- The first tier at the perimeter is layer 3 and 4 network firewall services
- Simple load balancing to a second tier
- IP reputation database
- Mitigates volumetric and DNS DDoS attacks

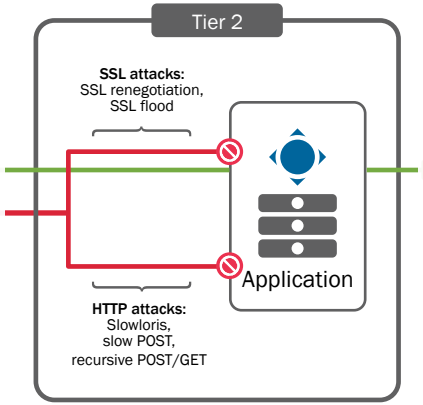
Threat Feed intelligence



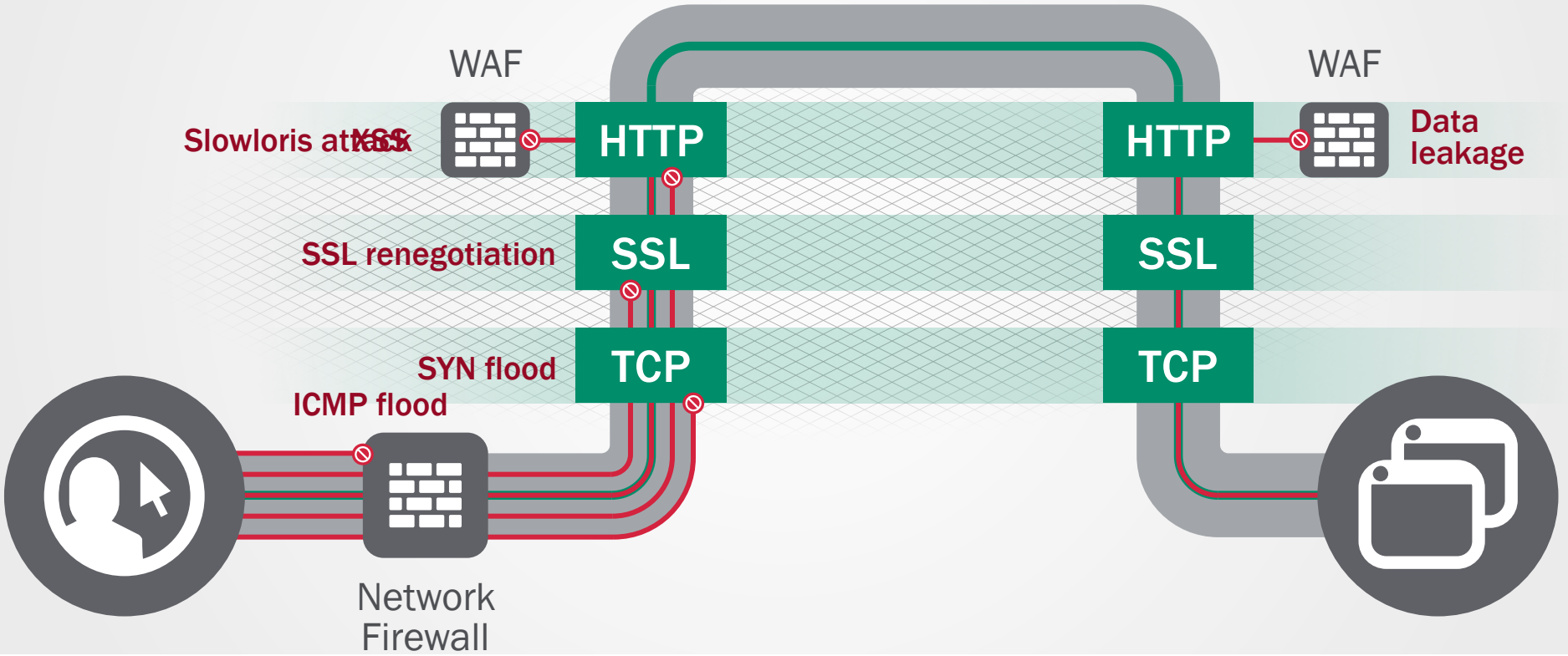
Reference Architecture

TIER 2 KEY FEATURES

- The second tier is for application-aware, CPU-intensive defense mechanisms
- SSL termination
- Web application firewall
- Mitigate asymmetric and SSL-based DDoS attacks



Using a full-proxy architecture



Layer 7 Attack Examples

Attacks	Slowloris	XerXes DoS	LOIC/HOIC	Slow POST (RUDY)	#RefRef DoS	Apache Killer	HashDos
Active (Since)	Jun 2009	Feb 2010	Nov 2010	Nov 2010	Jul 2011	Aug 2011	Dec 2011
Threat /Flaw	HTTP Get Request, Partial Header	Flood TCP (8 times increase, 48 threads)	TCP/UDP/ HTTP Get floods	HTTP web form field, Slow 1byte send	Exploit SQLi for recursive SQL ops	Overlapping HTTP ranges	Overwhelms hash tables of all popular web platforms – Java, ASP, Apache, Tomcat.
Impact	Attack can be launched remotely, Denial of Services (DOS), Resource Exhaustion, tools and script publicly available						

Which technology to use?

CLOUD/HOSTED SERVICE

Content delivery network

Communications service provider

Cloud-based DDoS service

ON-PREMISES DEFENSE

Network firewall with SSL inspection

Web application firewall

On-premises DDoS solution

Intrusion detection/prevention

The Answer:

“All of the Above”

"The kid's good."

How to survive an Attack

To the uninitiated, an attack can be a scary, stressful ordeal. Sometimes the first attack can appear randomly. Sometimes a competitor knows exactly the right (or wrong) day to take your high-value service offline. An outage like this can cause panic and force people into making decisions that they normally wouldn't make – such as paying a high ransom to stop an attack.

Prework

There are 5 worksheets to complete that will assist in repelling a DDoS attack.

If you have not recorded this information prior to your first attack, record it as you collect it. Then you can laminate these worksheets and keep them on the datacenter wall.

Worksheets

- Contact List – fill it out as you initiate contact.
- Whitelists – map your partners, users and services.
- Application Triage – know your own applications
- Device Map – Create a device map.
- Attack Log – Note the attack details

Ten Survival Guidelines

1. Verify the Attack
2. Contact the Team Leads
3. Triage Applications
4. Identify the Attack
5. Protect remote Users and Partners

Ten Survival Guidelines

6. Evaluate Source Address Mitigation Options
7. Mitigate Specific Application Attacks
8. Increase Application-Level Security Posture
9. Constrain Resources
10. Additional Considerations

Contact me for the full 15 page source document.

Contact Info:

Carl Brothers
www.f5.com
c.brothers@f5.com

Solutions for an application world.