SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Cyber Attacks and Application - Motivation, Methods and Mitigation

Alfredo Vistola

a.vistola@f5.com

Solution Architect – Security, EMEA

Attacks are Moving “Up the Stack”

Network Threats

90% of security investment focused here

Application Threats

75% of attacks focused here

Source: Gartner

Example 1

Statement - SONY Playstation

http://blog.us.playstation.com/author/pseybold/

- We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised…
- … we believe that an unauthorized person has obtained
  - name, address , email address, birthdate, PSN/Qriocity password (hashed) and login, profile data, including purchase history…
- While there is no evidence at this time that encrypted credit card data was taken, we cannot rule out the possibility.

  - Comment: SONY Playstation has about 77Mio customers

Statement - SONY Online Entertainment

http://blog.eu.playstation.com/

- On April 16th and 17th, 2011….. Personal information from approximately 24.6 million SOE accounts may have been stolen…,
  - Name, e-mail, login, hashed password,…
- As well as certain information from an outdated database from 2007 for 10.700 customer in EU
  - Name, bank account number, address,…

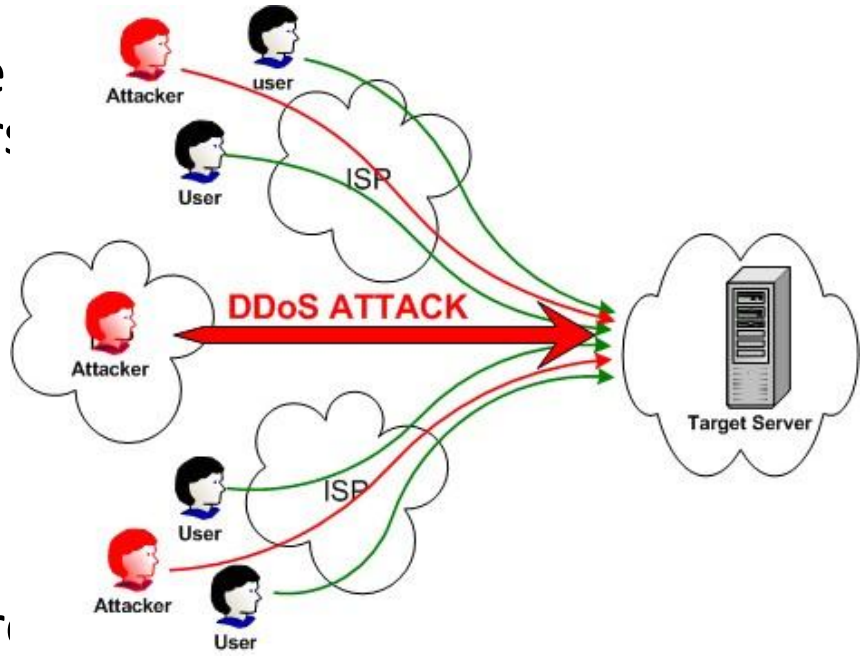
Example 2

What happened to WikiLeaks

- Several companies stopped the service for WikiLeaks although it is not proven that WikiLeaks violates the existing law
  - Amazon removed all WikiLeaks content from their servers
  - EveryDNS switched off the DNS resolution for wikileaks.org
  - Several financial institutes locked up donation accounts

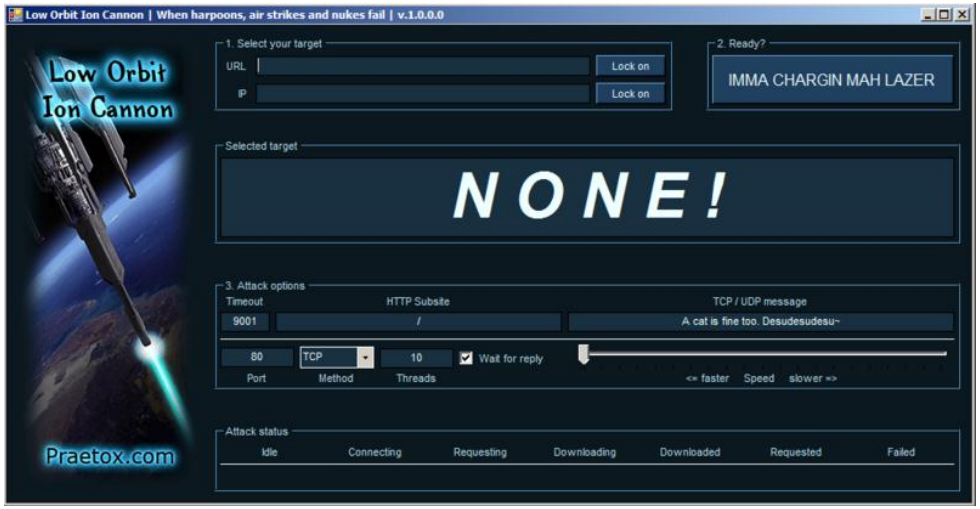
Finally…

- Thousand of internet users unloaded their accumulated anger starting 7th Dec 2010
  - Web servers of Swiss Postfinance bank were down for several hours
  - Credit card companies like Mastercard and VISA where not accessible for several hours/day over several days
  - Paypal's transaction network were slow but not taken down completely



Behind the scenes

- „Operation Payback“ admitted to this attack. They are also known as „Anonymous“ from previous attacks
- They used a modified version of the tool called LOIC
  - Originally developed for load tests
  - Nearly 50,000 people downloaded it to “join voluntary a botnet”
  - It performs a DoS or DDoS on a target site by flooding the server with TCP packets
    UDP packets or HTTP requests
    to disrupt the service of a host



Slowloris, Slow POST attack

How to choke a web server slowly...

- Takes down a web server with minimal bandwidth
- Slowloris begins by sending a partial HTTP request...
  - ...Followed by subsequent HTTP headers...

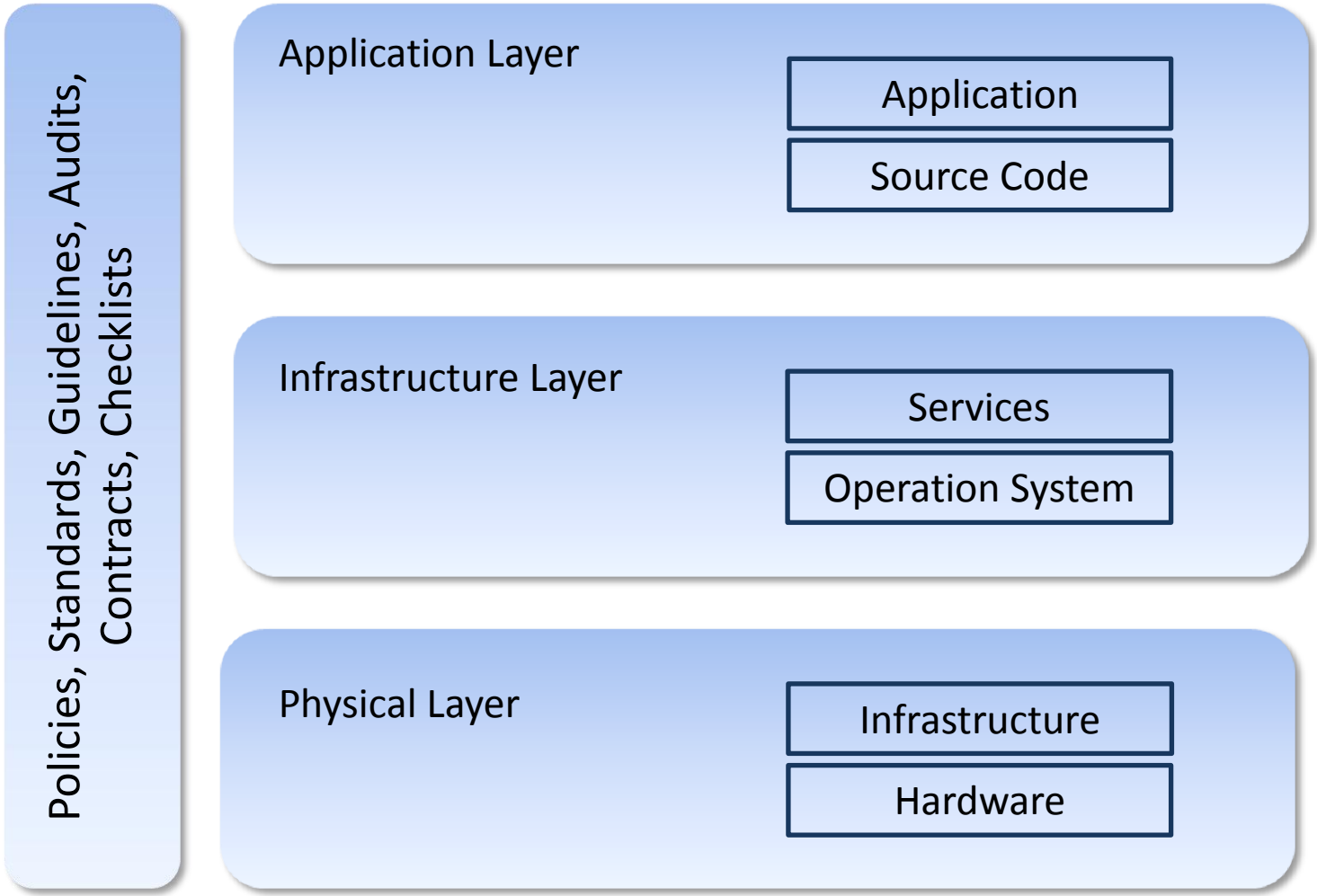
...One at a time

..Very slowly...

...and never ends...

- Slow POST attack
  - The data are sent very slow
- Server holds connection open and runs out of available connections
- Result – server is unavailable with no errors in the logs

All Levels need to be covered



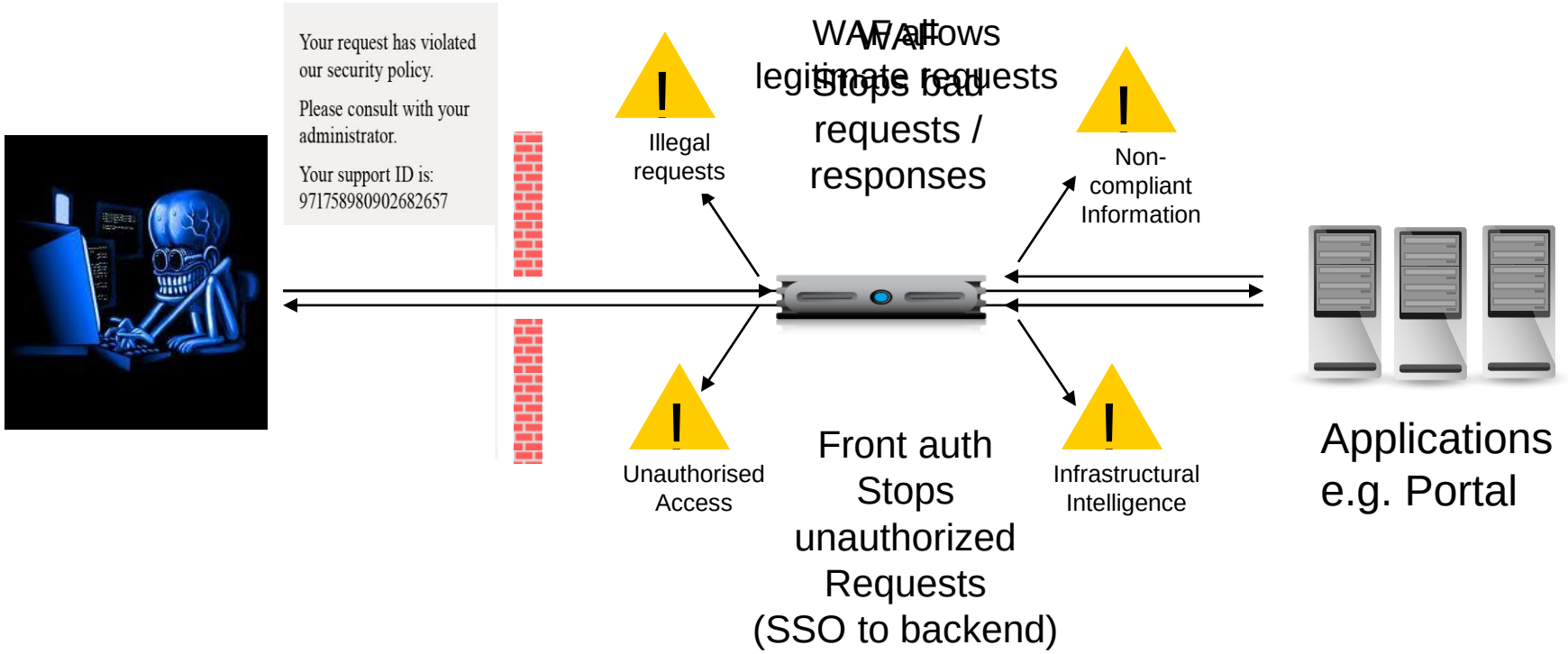
OWASP Top 10 for 2010

A1: Injection
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object References
A5: Cross-Site Request Forgery (CSRF)
A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards

Value of the Web Application Firewall

- Allows immediate protection against new vulnerabilities
  - Virtually patch vulnerabilities in minutes without changing application code
- Application visibility and reporting
  - Comprehensive logging and reporting
- Reduce operation costs
  - Ensure high application availability by stopping application based attacks and application based DoS/DDoS
  - Reduce the expenses of meeting PCI security compliance requirements by showing clean scans
- Get out-of-the-box application security policies with minimal configuration
- Authentication and authorization with SSO at the edge of the network
- Cut your infrastructure costs with consolidation and reduce latency
  - High availability, scalability, SSL acceleration, caching, compression, rate limiting, optimization, ...

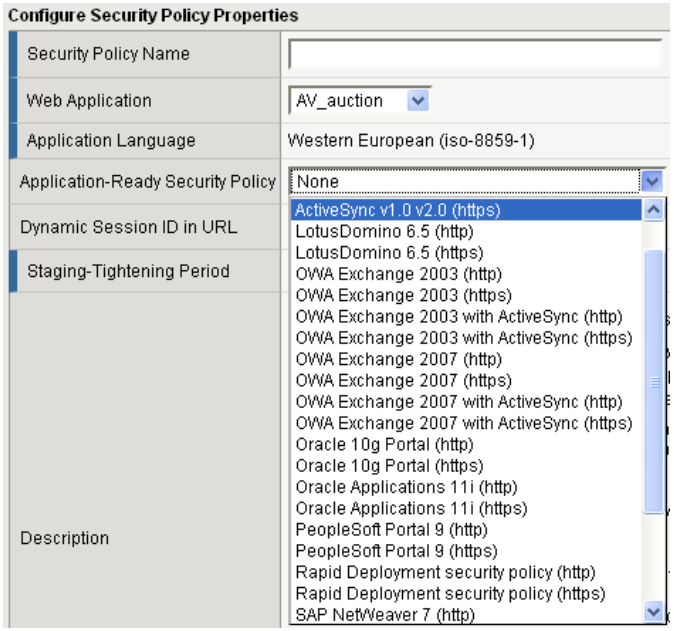
Application Security with the WAF



Reduces the attack vector because only authenticated, authorized and legal requests are permitted to the relevant application servers

Deploy WAF Policies without false

- Predefined Policy Templates
  - Pre-configured security policies
- Learning mode
  - Automatic or manual
- Application Scanner integration
- Gradual deployment
  - Transparent / semi-transparent / full blocking



Example: App scanner integration

Vulnerabilities Found And Verified By QualysGuard

QualysGuard Vulnerability Name	ASM Attack Type	Resolvable	Occurrences
Browser-Specific Cross-Site Scripting (XSS)	Cross Site Scripting (XSS)	Yes	3
Reflected Cross-Site Scripting (XSS) Vulnerabilities	Cross Site Scripting (XSS)	Yes	25
SQL Injection	SQL-Injection	Yes	23
SQL Injection In HTTP Header	SQL-Injection	Yes	11

Total Entries: **4**

Browser-Specific Cross-Site Scripting (XSS) Vulnerabilities List

URL	Parameter	ASM Status	Load Time
http://172.29.38.211/help.php?topic=%3cscript%20src%3dhttp%3↵ a%2f%2flocalhost%2fj%20	topic	Mitigated	2012-02-07 22:53:18
http://172.29.38.211/sell.php	suggested_category	Pending	2012-02-07 22:53:18
http://172.29.38.211/japanese_test.php?charset=	string	Pending	2012-02-07 22:53:18

Resolve and Stage | Resolve | Ignore | Cancel Ignore

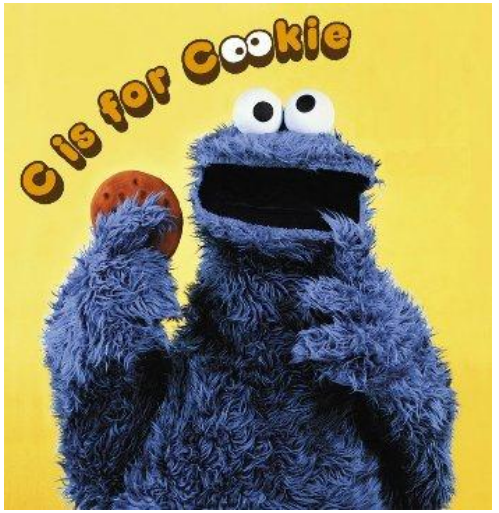
Total Entries: **3**

WAF Security Services

- Attack signatures (staging, update service)
- Information leakage prevention
  - E.g. CC# 3568-4298-9764-7690

WAF Security Services

- Attack signatures (staging, update service)
- Information leakage prevention
  - E.g. CC# ****-****-****-****
  - Block MS-Office files, PDFs, ...
- Cookie signing and encryption
  - Cookies are used to maintain the user state
- Detailed granular positive protection for every entity
  - Protocol, URI, parameters, headers
  - Protection for hidden field and dynamic parameter manipulation
- Access flow and login page enforcement
  - E.g. restrict URL Access or mitigate broken authentication



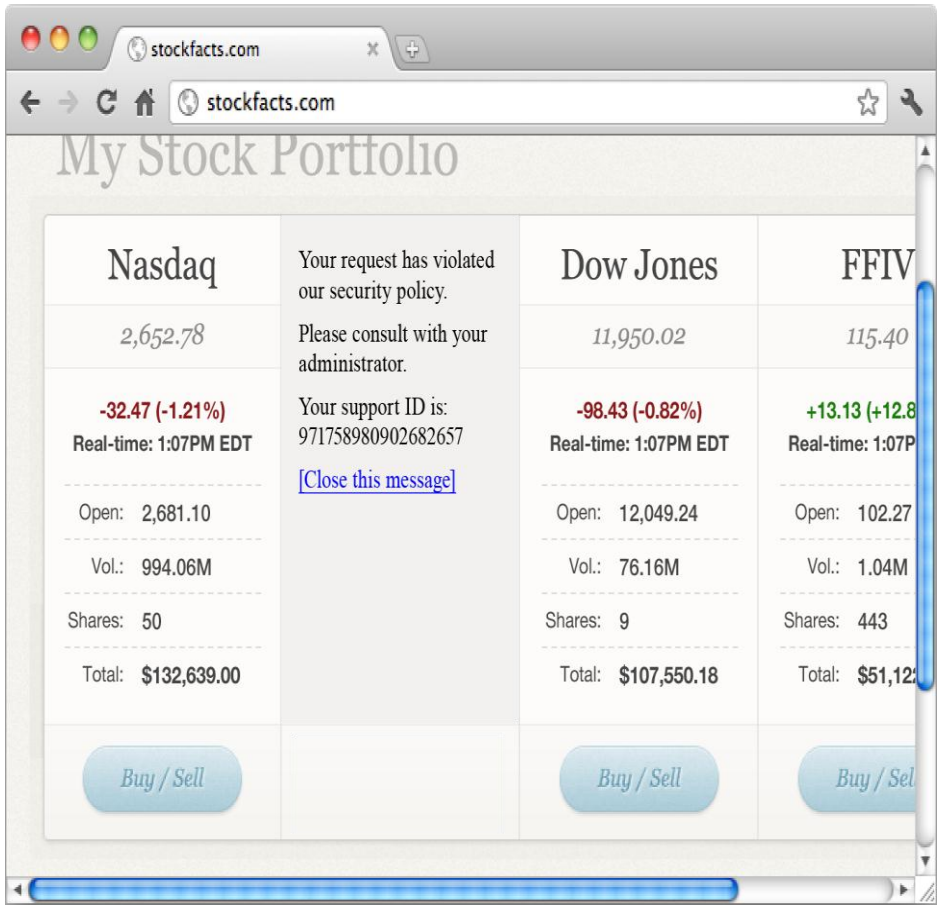
WAF Security Services

- CSRF Protection
- Slowloris and Slow POST attack mitigation
- Bot and scanner detection and risk mitigation
  - Layer 3 and Layer 7 DoS attacks
  - Brute force attacks
  - Web scraping
    - ASM differentiates between a BOT which runs a script and a real user who uses the keyboard and moves the mouse
- ICAP support for http uploads, SOAP or SMTP attachments
- …

AJAX/JSON Support for Web 2.0

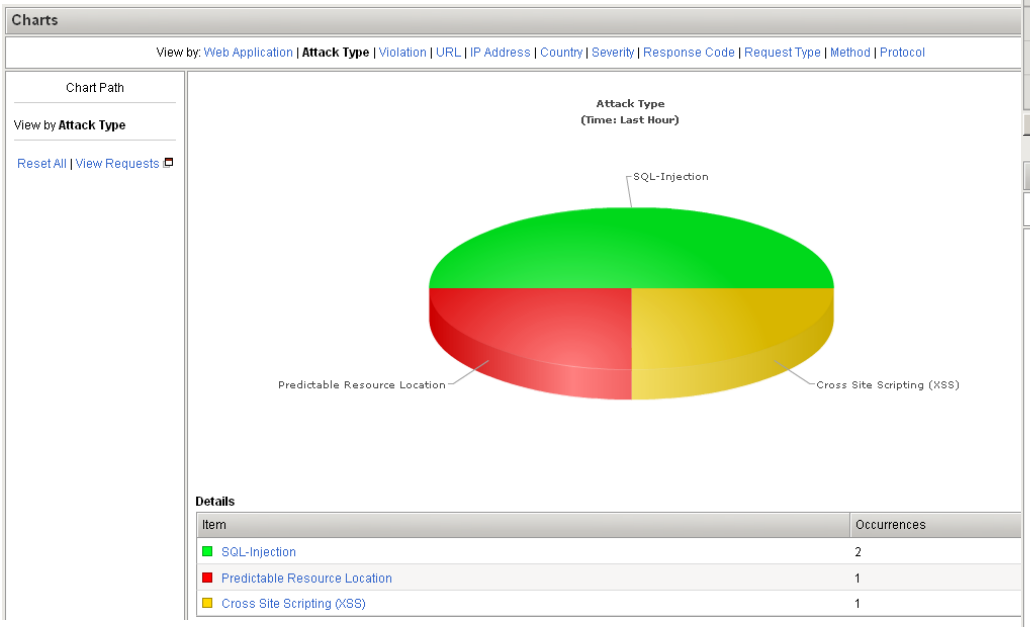
- Support AJAX apps or JSON payloads
- Parse JSON payloads
- Same attack vectors as http apps

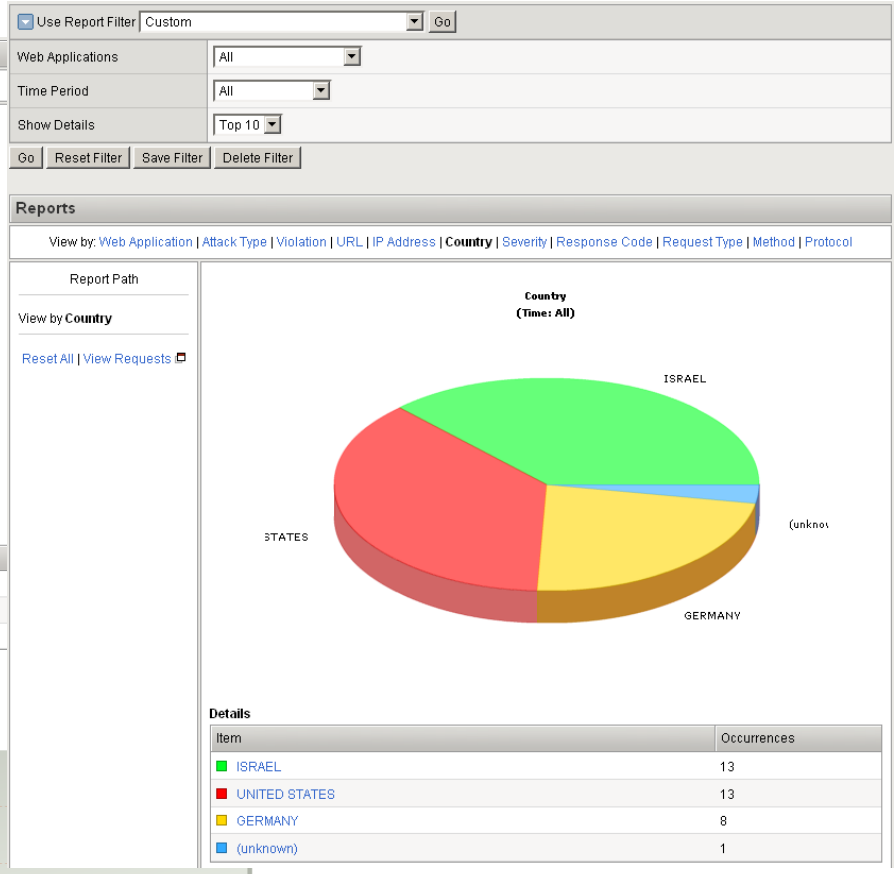
Easily Secure JSON Payloads

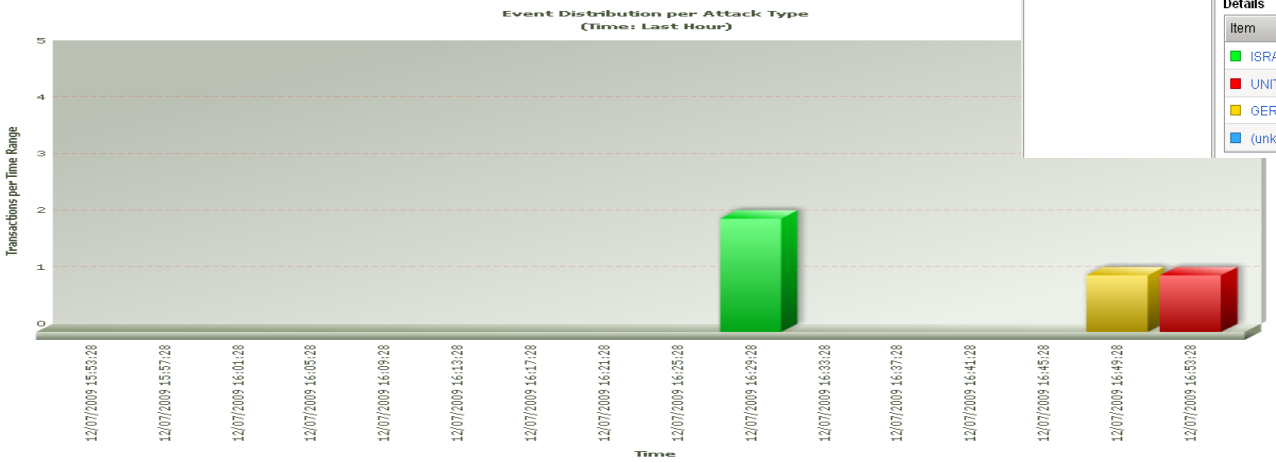


- Protect from JSON threats
- Ability to present a unique blocking page to an AJAX widget
- User informs admin with support ID for resolution

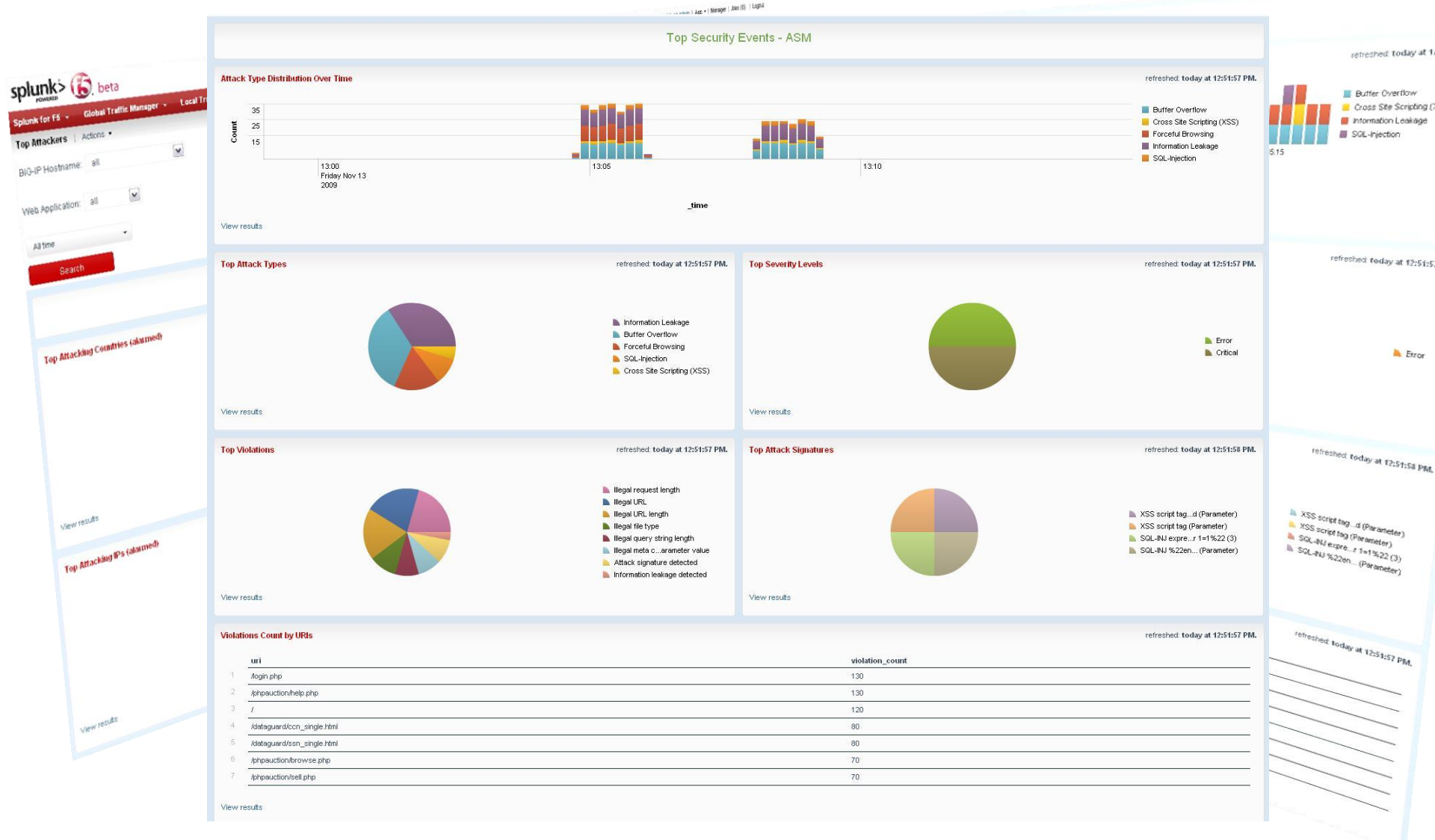
Logging/Reporting





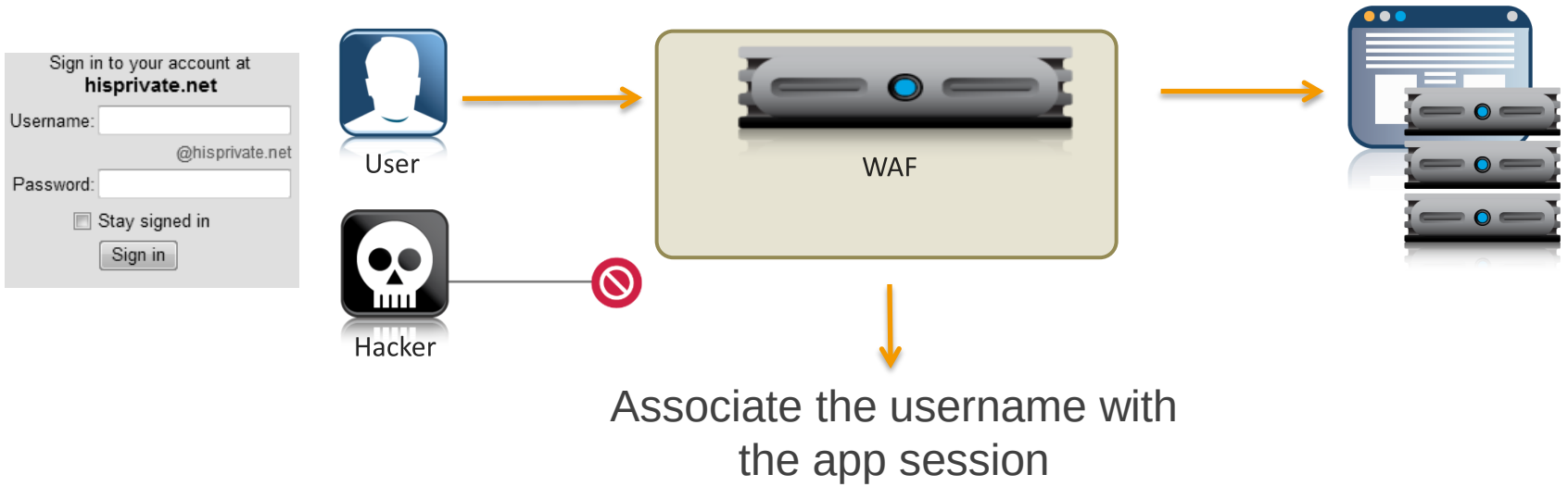


Centralized Reporting Examples



Track and Control User Behavior

Session Awareness



- Integrate user context within Logs
- Rules can be applied based on user behavior

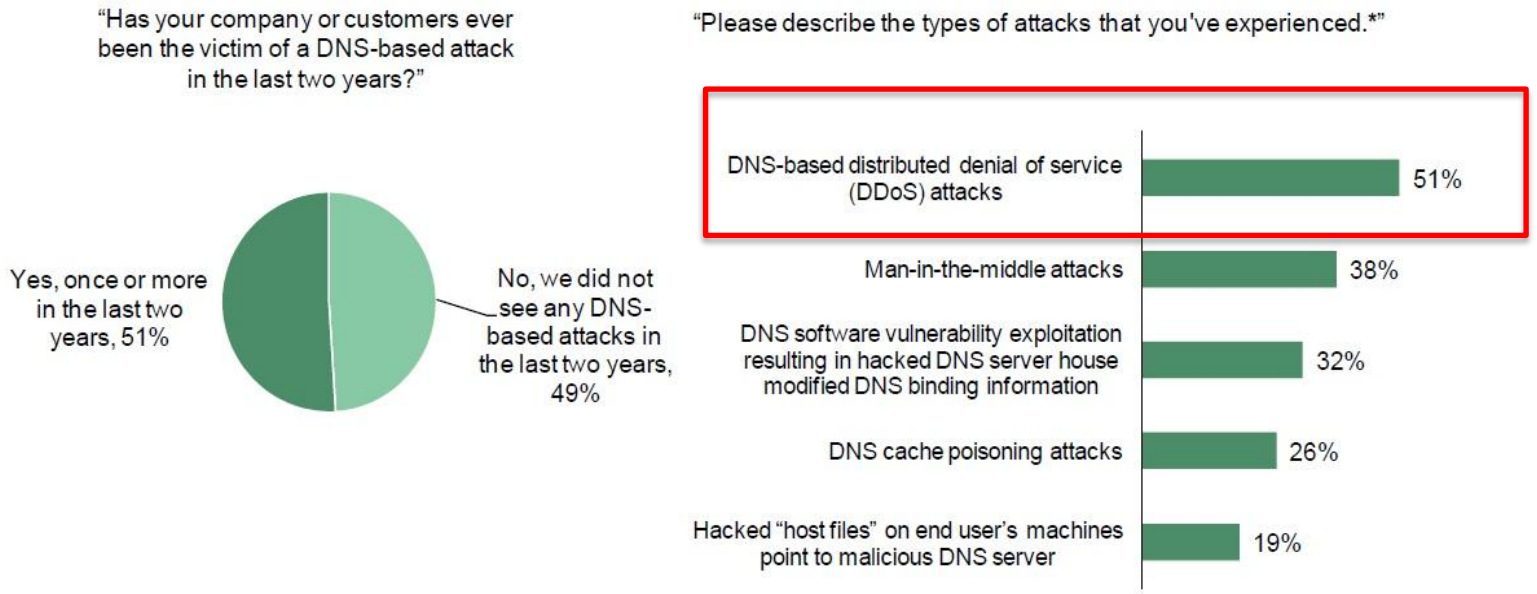
XML/Web Services Firewall

- Well formatted validation
- Schema/WSDL validation
- WSDL Method selection (SOAP)
- Attack signatures for XML platforms
- Backend XML parser protection
- Full request logging
- WS-security message level encryption and digital signature support
- XML content based routing (built into LTM)

DNS Attacks Are Common

Figure 3

More Than Half Of Our Respondents Have Seen At Least One DNS-Based Attack In The Past Two Years

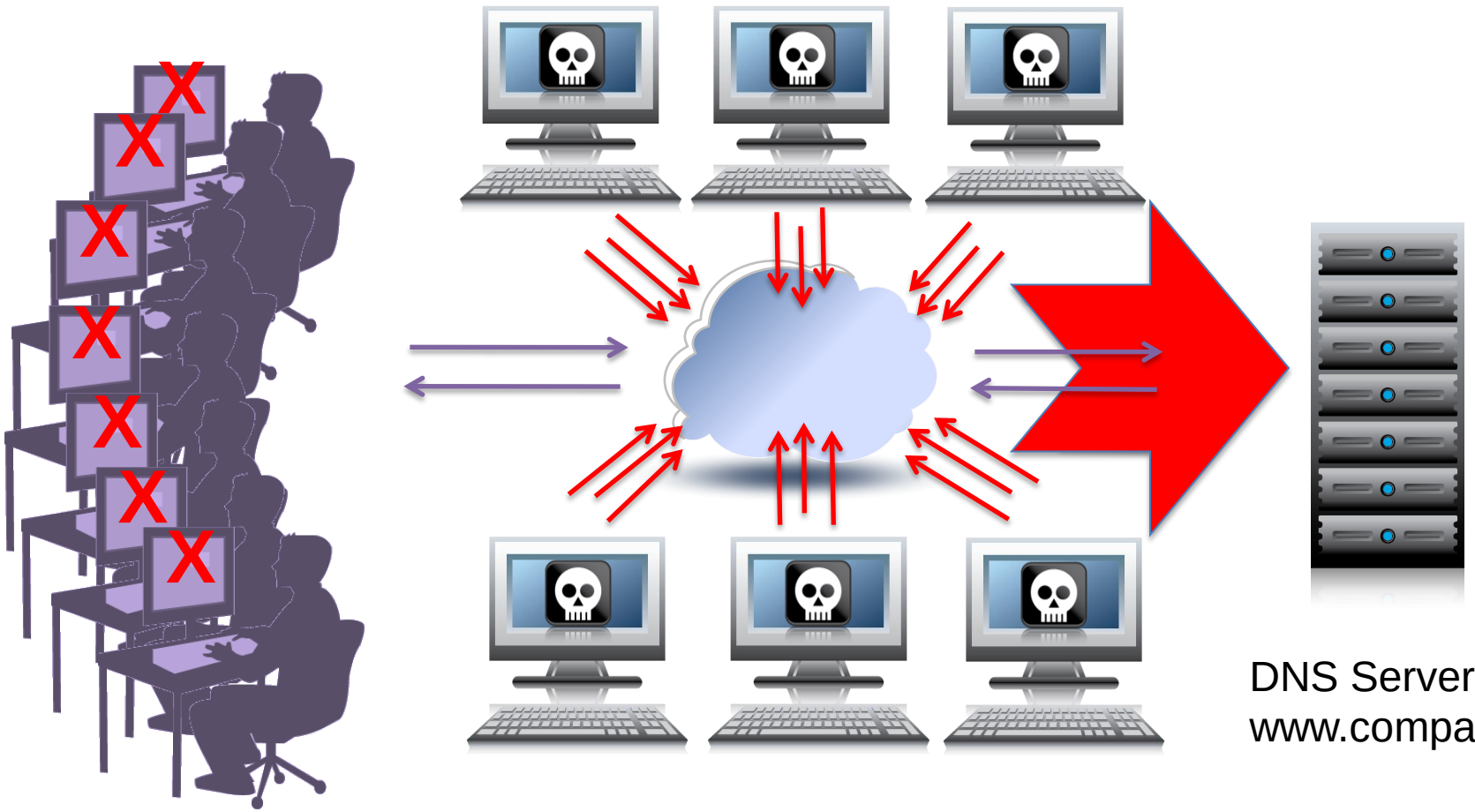


Base: 297 global network operations or IT security influencers/decision-makers

*Base: 151 global network operations or IT security influencers/decision-makers whose company or customers have been a victim of a DNS-based attack within the last two years (multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of VeriSign, June 2010

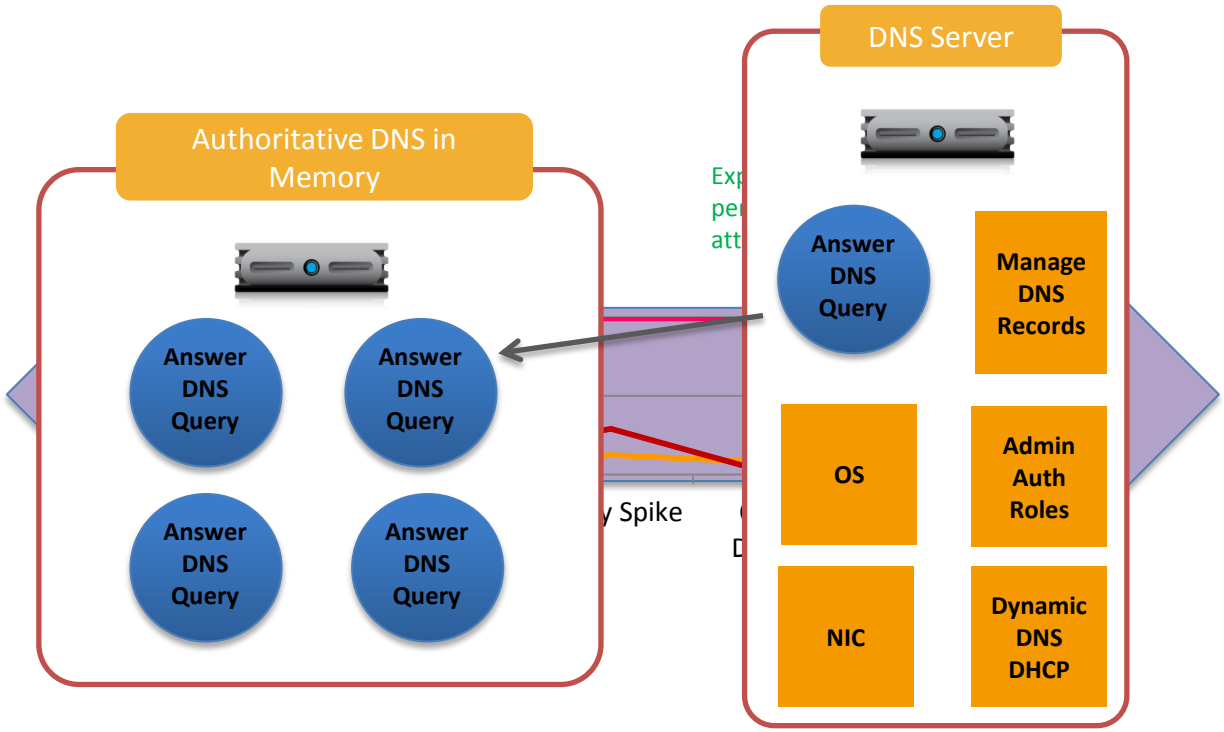
Problem: DNS is Vulnerable to Attacks



DNS Servers
www.company.com

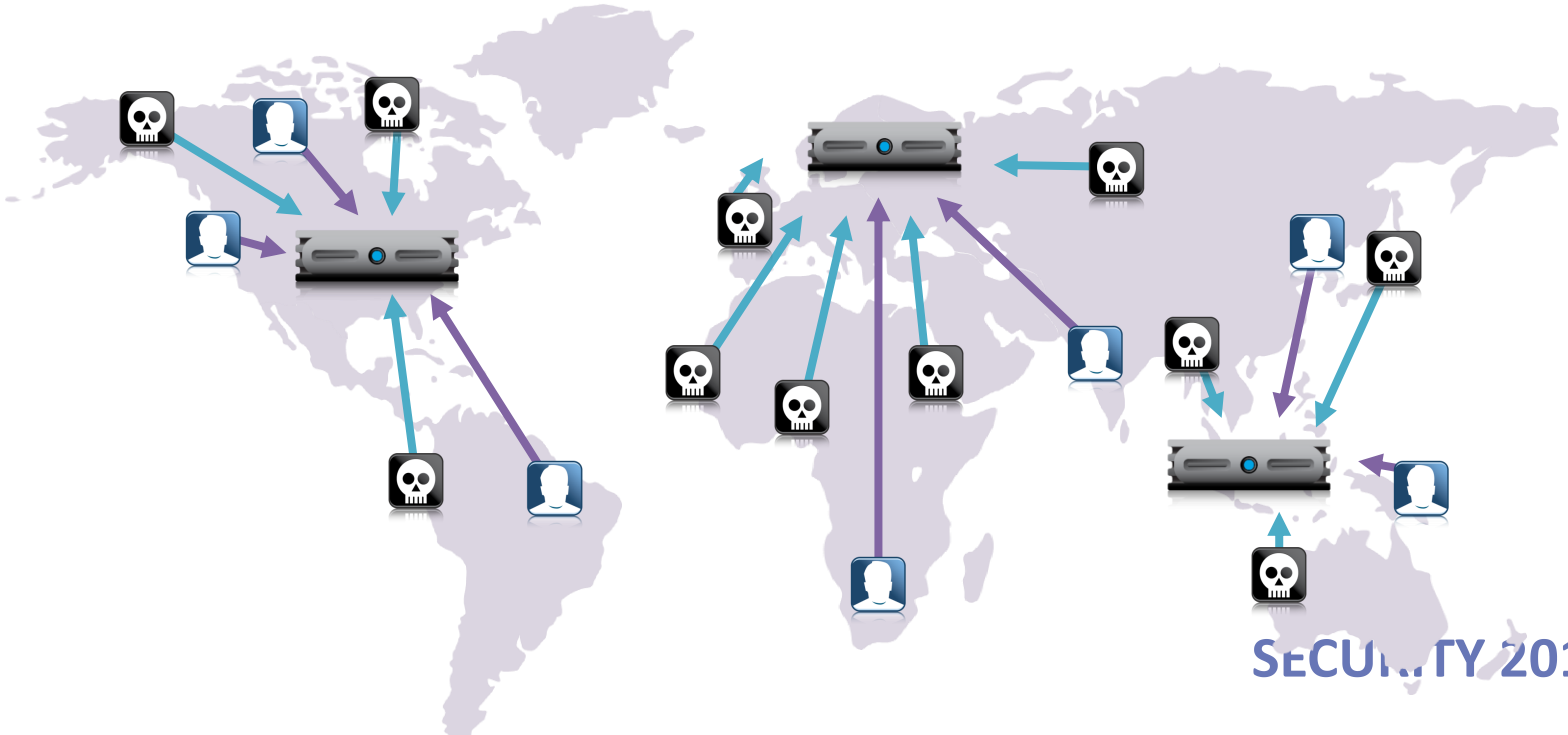
Solution: Handle All DNS Requests

- ✓Scalability
- ✓Authoritative DNS in Memory



Solution: Handle All DNS Requests

- ✓Scalability
- ✓Authoritative DNS in Memory
- ✓IP Anycast Integration

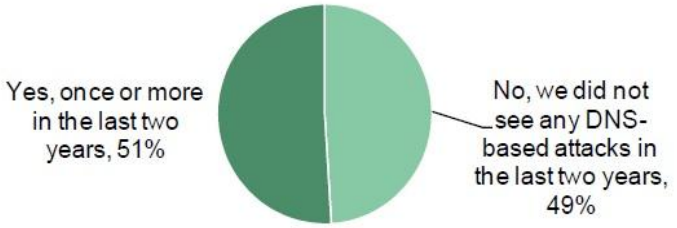


DNS Attacks Are Common

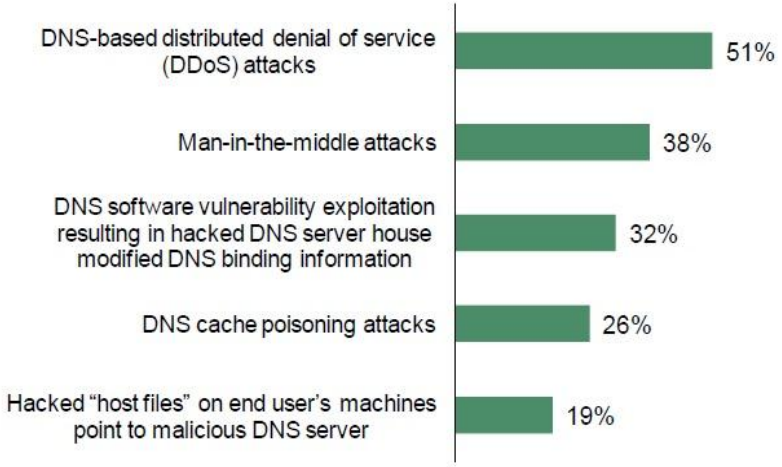
Figure 3

More Than Half Of Our Respondents Have Seen At Least One DNS-Based Attack In The Past Two Years

"Has your company or customers ever been the victim of a DNS-based attack in the last two years?"



"Please describe the types of attacks that you've experienced.*"



Base: 297 global network operations or IT security influencers/decision-makers

*Base: 151 global network operations or IT security influencers/decision-makers whose company or customers have been a victim of a DNS-based attack within the last two years (multiple responses accepted)

Source: A commissioned study conducted by Forrester Consulting on behalf of VeriSign, June 2010

DNS Session Hijacking

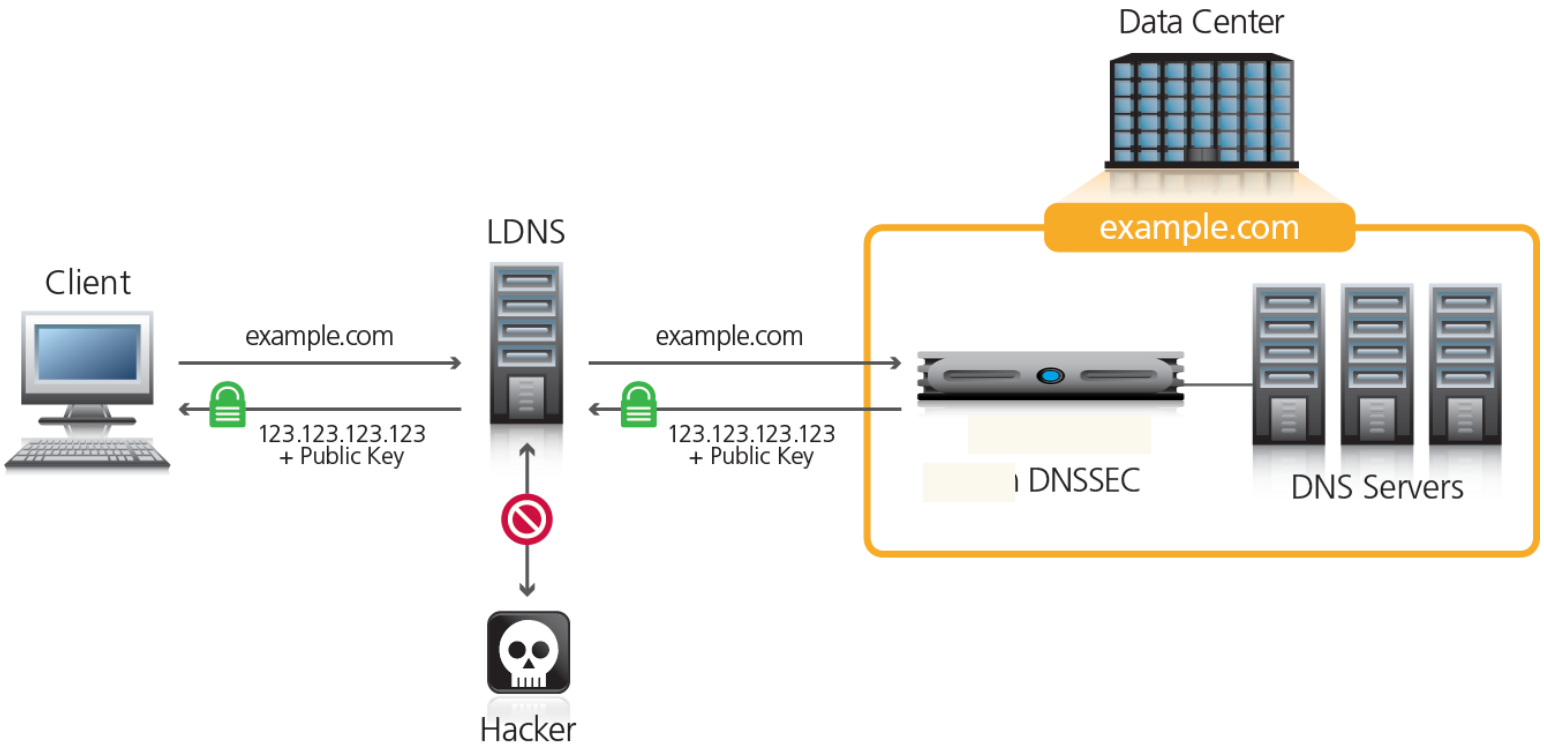
- What is DNS Hijacking?
  - Subscriber initiates a DNS request which is through a resolver to an authoritative DNS server
  - Instead of arriving at the authoritative DNS server for that specific hostname, another DNS server "Hijacks" the request and sends a false authoritative answer to the subscriber
  - The subscriber is then directed to a wrong IP for the hostname requested

- Solution? **DNSSEC**

DNSSEC

- What is DNSSEC?
  - DNSSEC is a standardized method of signing authoritative DNS responses. This signing ensures the identity of the authoritative DNS answering the request
- Where is the standard?
  - There are multiple RFC's that define different elements of DNSSEC. (Not all are listed here, only the main RFC's)
  - RFC4033 – Introduction to DNSSEC
  - RFC4034 – DNSSEC Records
  - RFC4035 - DNSSEC Protocol

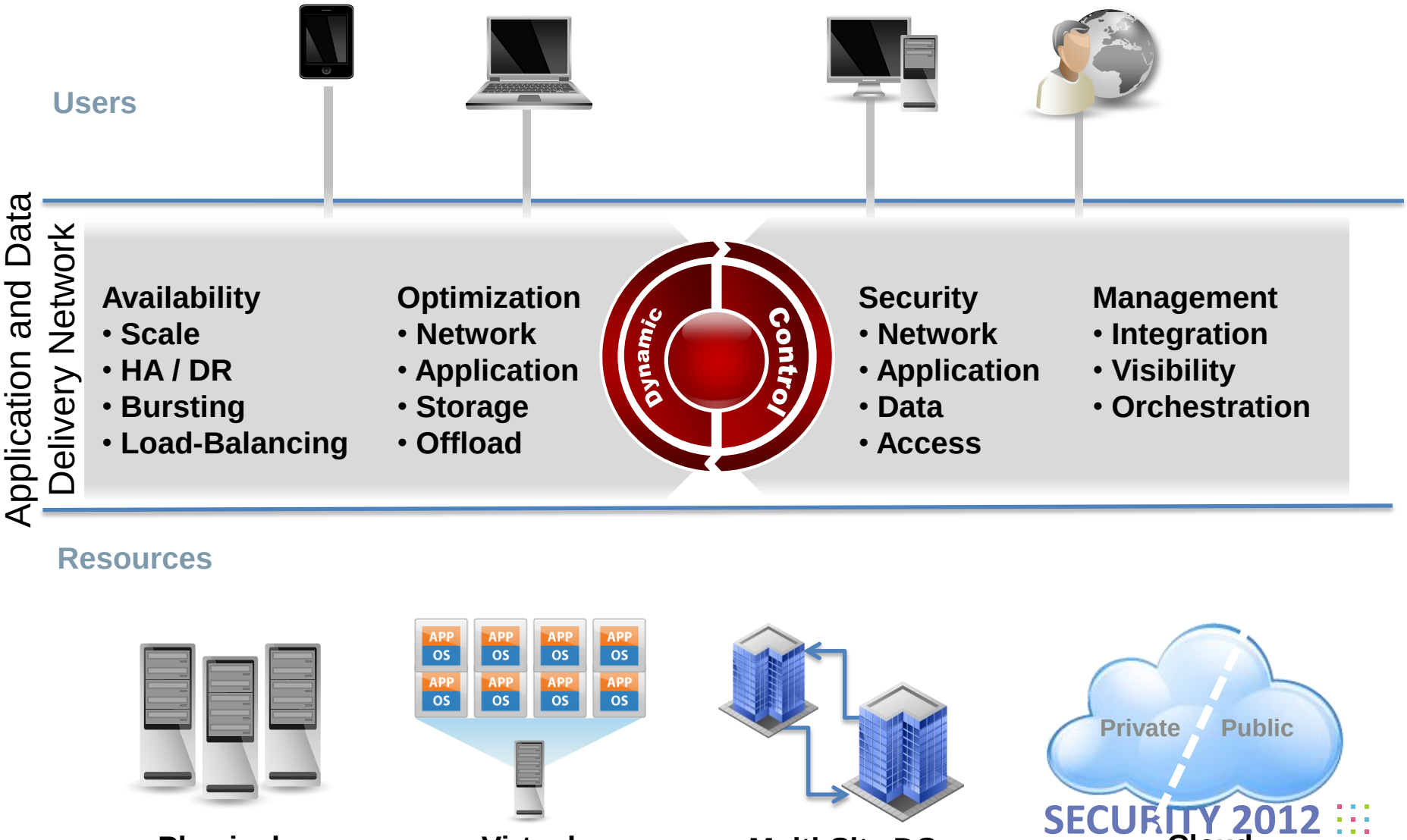
Secure Your DNS Infrastructure



Simple DNSSEC compliance:

- E.g. implement DNSSEC in front of existing DNS servers
- Ensure trusted DNS queries with dynamically signed responses

F5's Dynamic Control Plane Architecture



SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Alfredo Vistola

a.vistola@f5.com

Security Architect, EMEA @ F5