

# **RSA<sup>®</sup>CONFERENCE2014**

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.  
Learn.  
Secure.

Capitalizing on  
Collective Intelligence

## **Harnessing Big Data for Application Security Intelligence**

SESSION ID: SPO1-T08

**Or Katz - Principal Security Researcher**  
**Tsvika Klein - Product Manager**  
Akamai Security BU



# It All Started When...



**RSA**CONFERENCE**2014**



**Hello Akamai, We're Under  
Attack...**

**RSA CONFERENCE 2014**

# So We Analyzed this Attack



**RSACONFERENCE2014**



# WordPress Remote File Inclusion Vulnerability

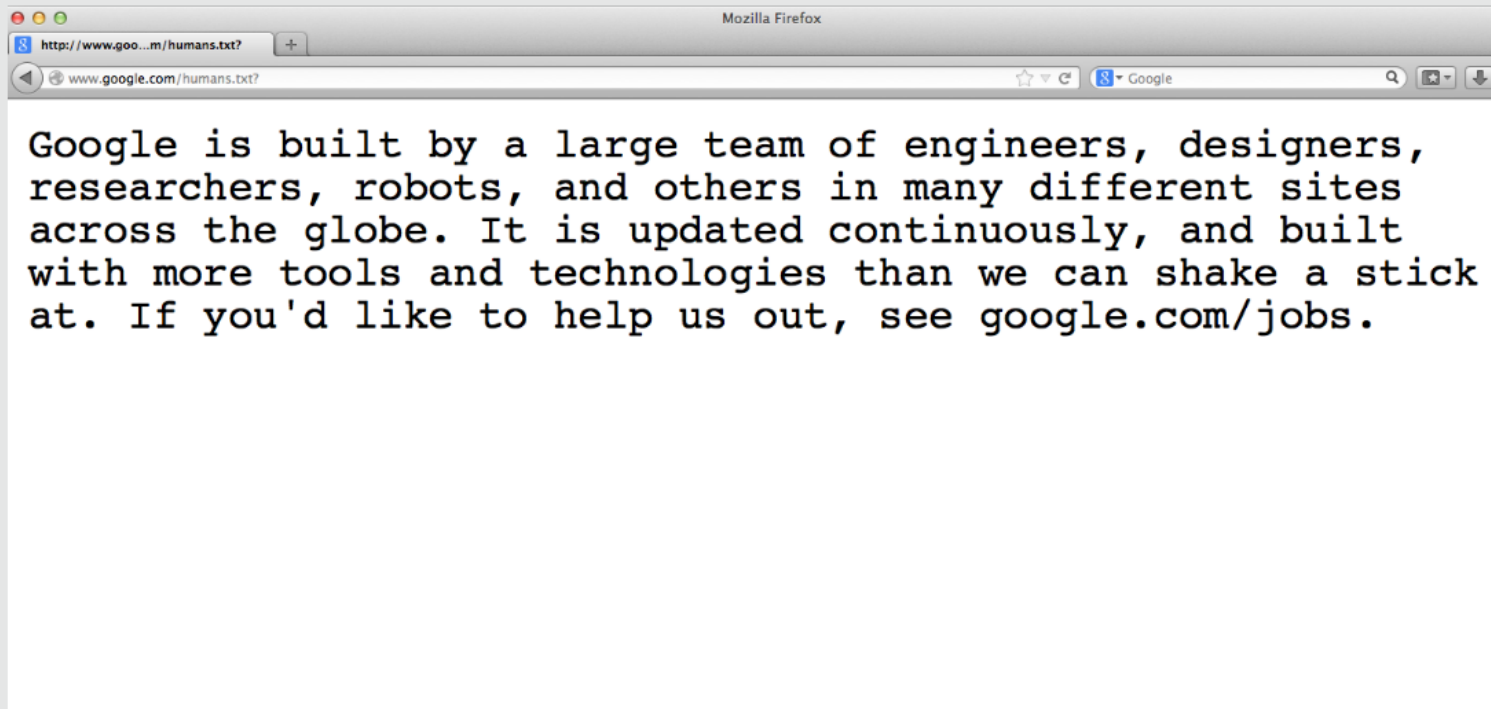
```
GET /wp-content/plugins/wordtube/wordtube-button.php?wpPATH=http://www.google.com/humans.txt? HTTP/1.1  
Host: www.test.com  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like Gecko)
```

Trying to inject to this HTTP parameter **wpPATH**

The content of this URL <http://www.google.com/humans.txt?>

**RSACONFERENCE2014**

## Content of hummans.txt



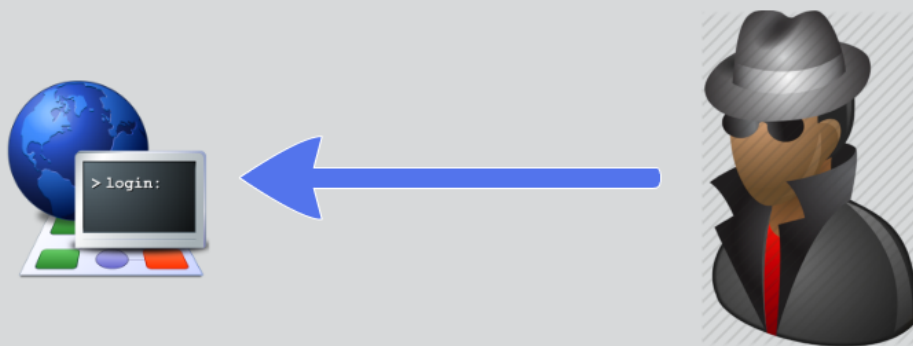
**RSACONFERENCE2014**

## Some Question that Crossed Our Minds:

- Why RFI exploit from 2007?
- Why trying to exploit PHP inclusion on .NET application?
- Why including a legitimate page?

**RSA CONFERENCE 2014**


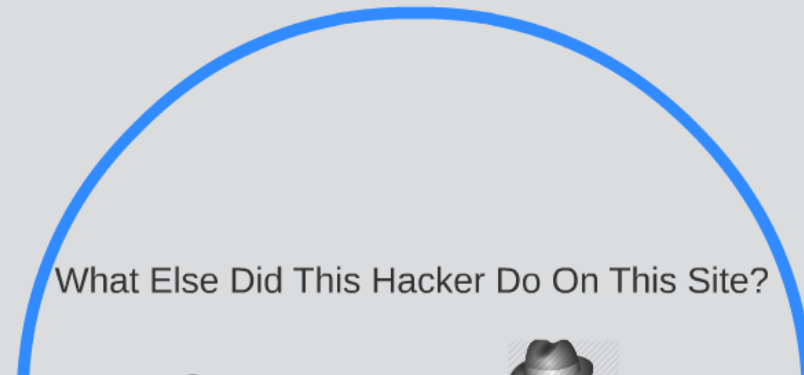
What Else Did This Hacker Do On This Site?





Sending **2212** different RFI exploits



Any Other Akamai Customers Hit by This Hacker?



What Else Did This Hacker Do On This Site?



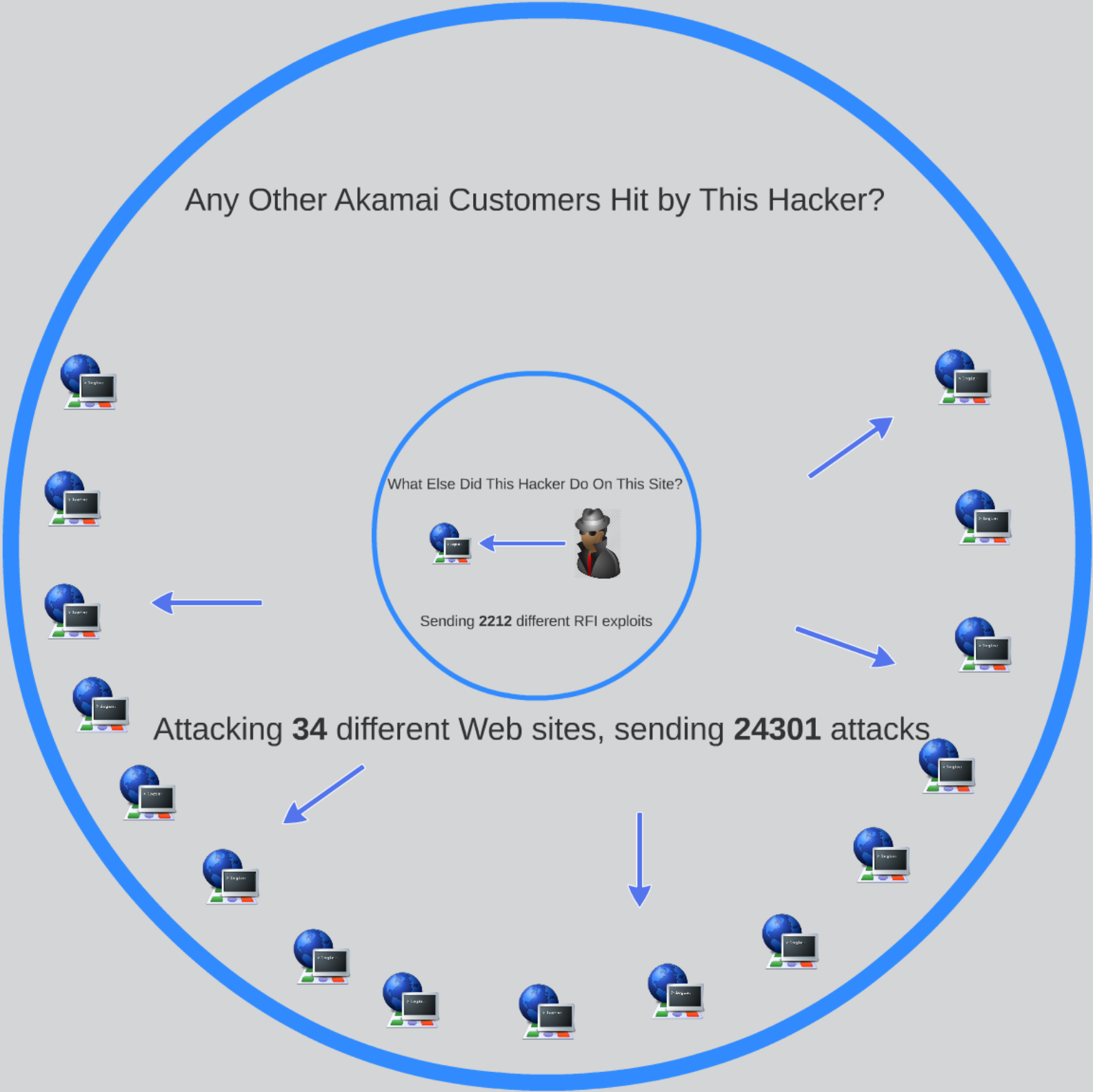
Any Other Akamai Customers Hit by This Hacker?

What Else Did This Hacker Do On This Site?



Sending **2212** different RFI exploits

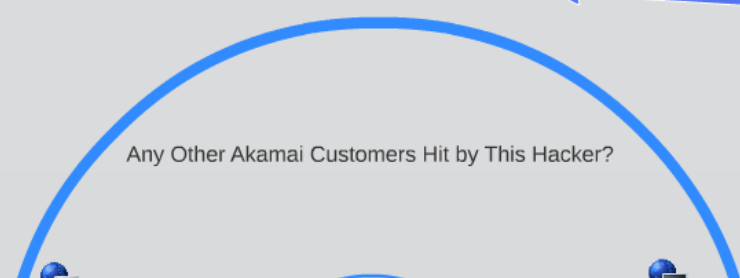
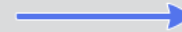
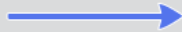
Attacking **34** different Web sites, sending **24301** attacks





Lets find similar activity across the internet...

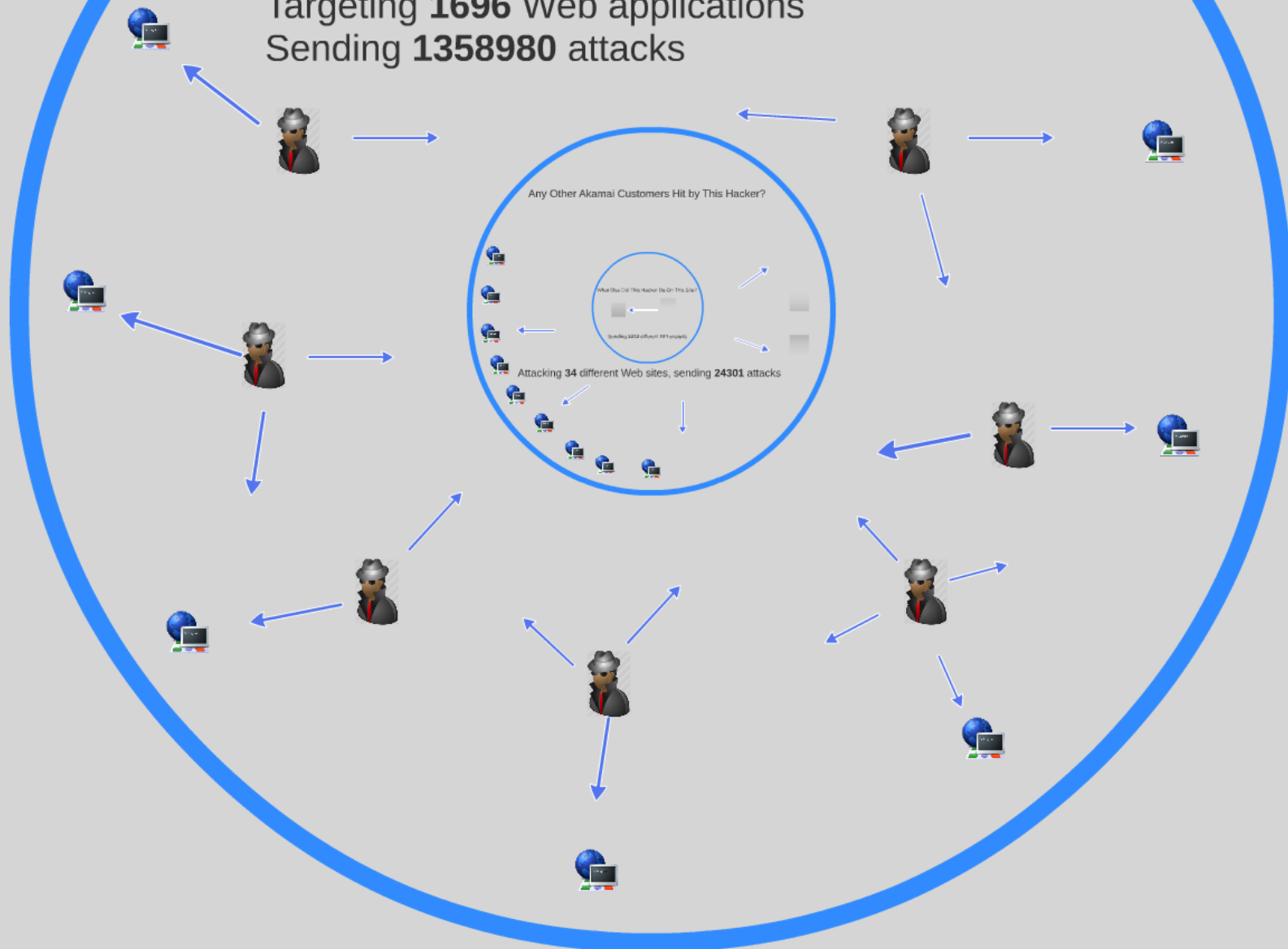
Bot Network that include **272** machines  
Targeting **1696** Web applications  
Sending **1358980** attacks



Any Other Akamai Customers Hit by This Hacker?

Lets find similar activity across the internet...

Bot Network that include **272** machines  
Targeting **1696** Web applications  
Sending **1358980** attacks





# Still Some Questions that Need to be Answered...



## Why RFI Exploit from 2007?

Hacker trying to be lucky  
using old exploits

## **Why Including a Legitimate Page?**

Hacker checking exploit feasibility



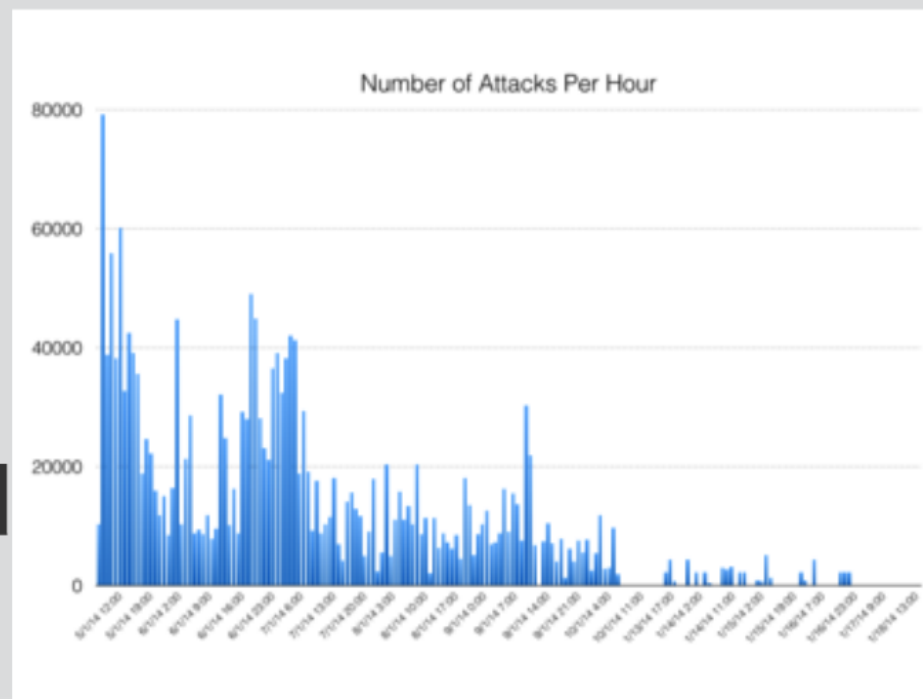
## Why trying to Exploit PHP Inclusion on .NET Application?

Hacker is just shooting all over the place



# Attack Summary

- Distributed attack campaign.
- 200 compromised web servers
- Lasting over more than a month.



**RSACONFERENCE2014**

# Big Data at Akamai

120,000+  
Servers

2,000+  
Locations

750+  
Cities

82  
Countries

1,100+  
Networks

## Highlights:

- 100 million page views per second and 500 billion hits per day
- 734 Million IP addresses seen quarterly
- 260+ Terabytes of compressed daily logs
- **30%** of all internet traffic



# Cloud Security Intelligence

2 Petabytes of security data

10 Terabytes of daily attack traffic

600K log lines per second

140K concurrent connection

800 queries daily

45 days retention

**RSACONFERENCE2014**



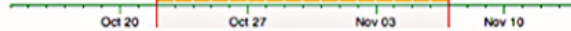








# Security Big Data Challenge #1






# Security Big Data Challenge #2



 xxxx\_8862 ▾ 2.2.6 Scoring ▾Load  Rule Name ▾Drill   10/22/2013  12:00 AM  -  11/07/2013  12:00 AM 

Drill Path &gt; Rule Name

Distribution 

RULE NAME (29 OF 29)

ALERT

DENY

TOTAL

DISTRIBUTION IN DAYS

System Command Injection

~1.62B

0

~1.62B



Request Indicates an automated program explored the site

~10.14M

0

~10.14M



Request Missing / blank User-Agent and Accept Headers

~9.15M

0

~9.15M



The application is not available

~8.79M

0

~8.79M



Detected request from anonymous proxy

~3.86M

0

~3.86M



LOIC 1.1 client detected

~2.42M

0

~2.42M



Invalid character in request

490,060

0

490,060



HTTP Response Splitting Attack


409,427

0

409,427



Raw Log

Raw Data 



## Market Trends

Forecast intent before exploitation

Filter malicious client

Shift to context aware security



**RSACONFERENCE2014**

# Client Reputation

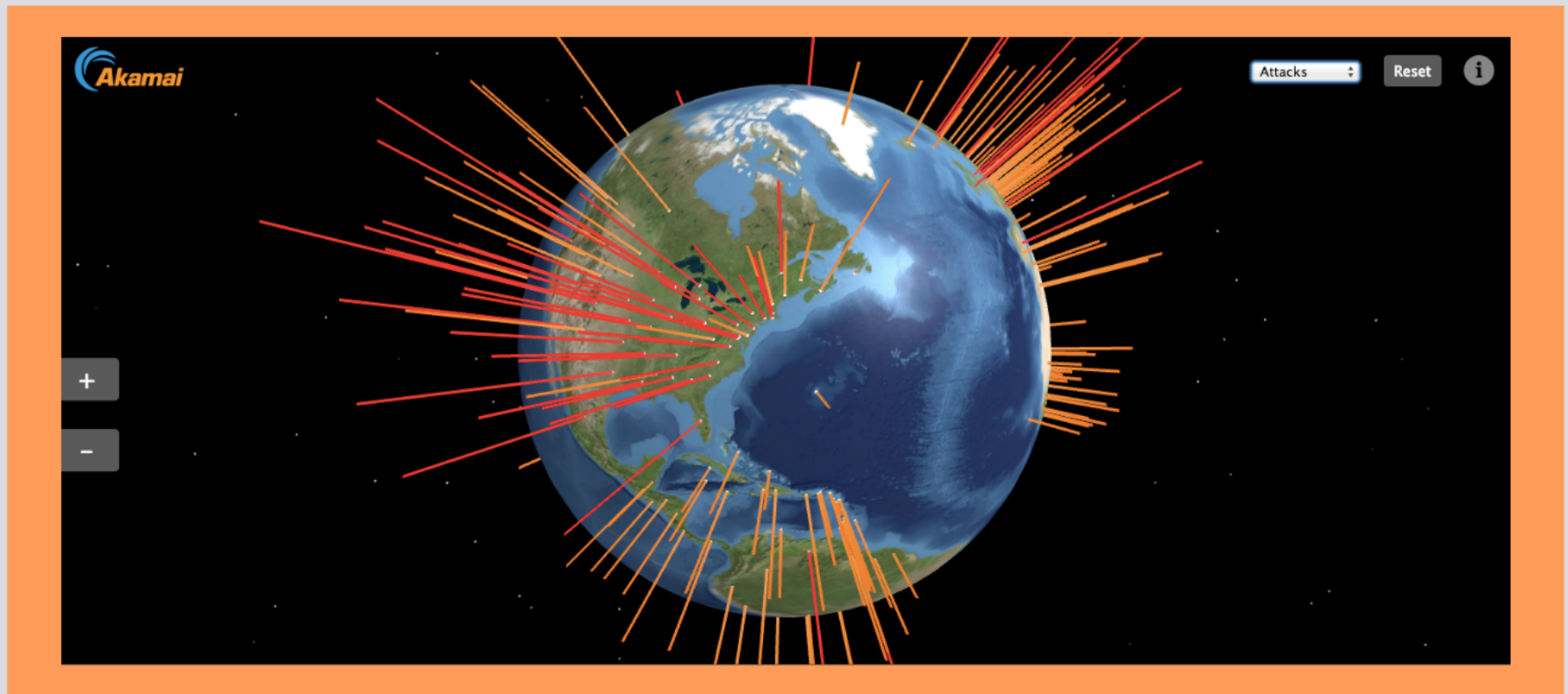
- Identify malicious clients
- Block access to web application



# Reputation Considerations



# Data

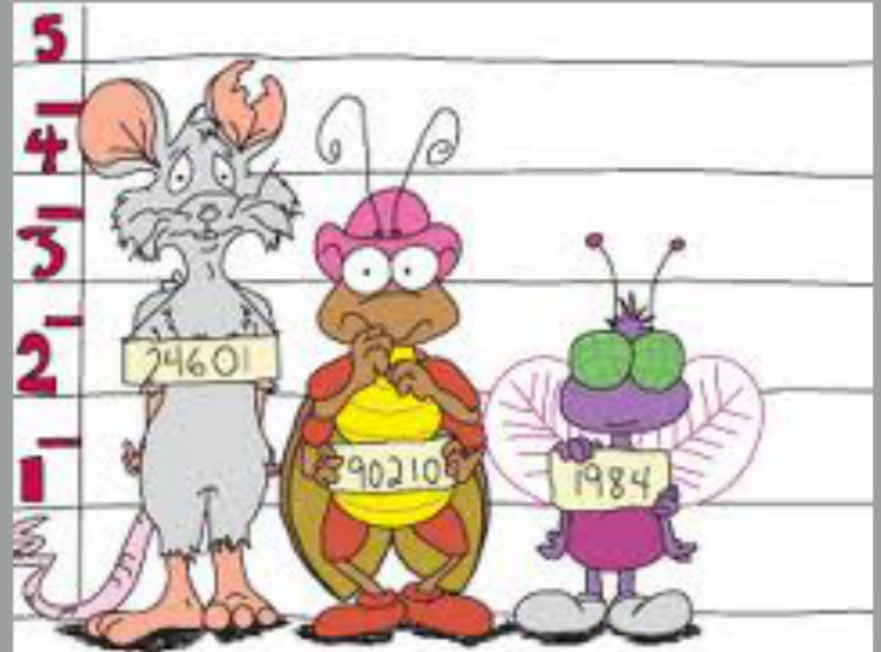


# User identification

IP address

Passive fingerprinting

Active fingerprinting



# Algorithms

Distribution

Magnitude

Behavior

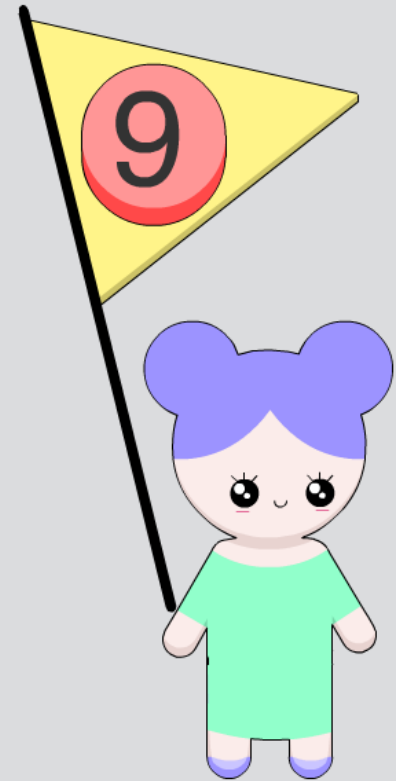
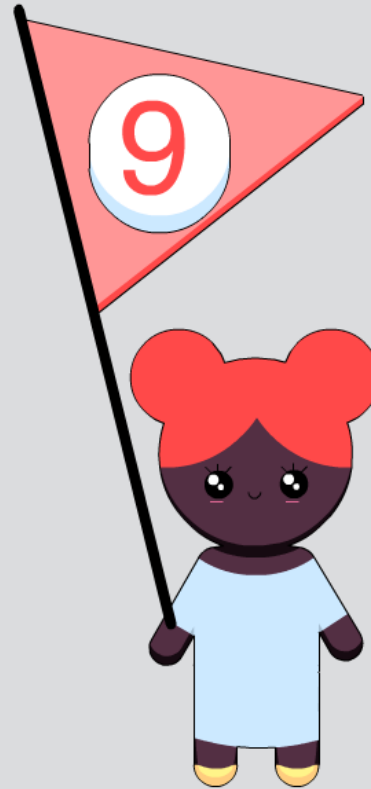
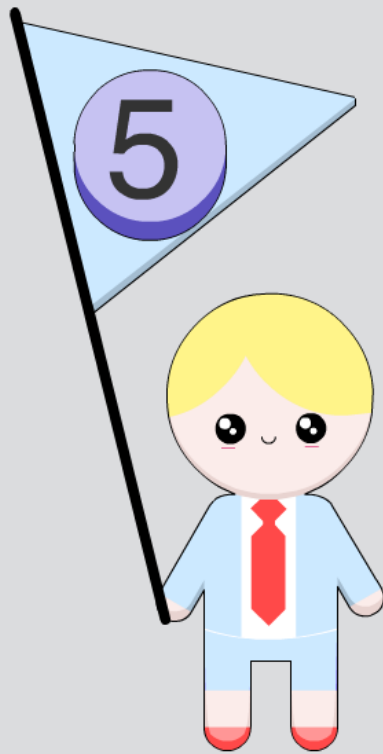
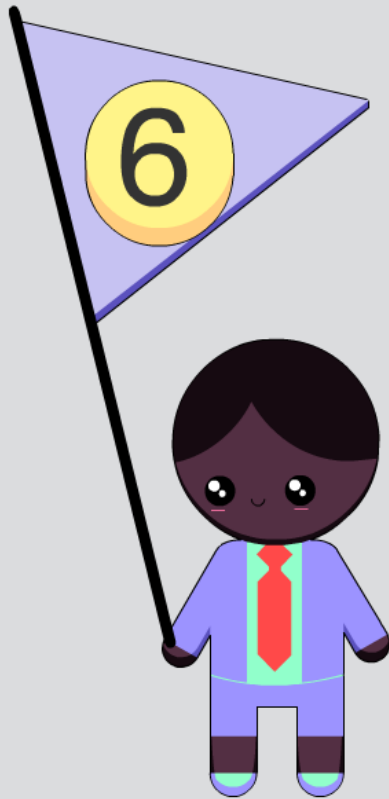


Duration

Sources  
similarity



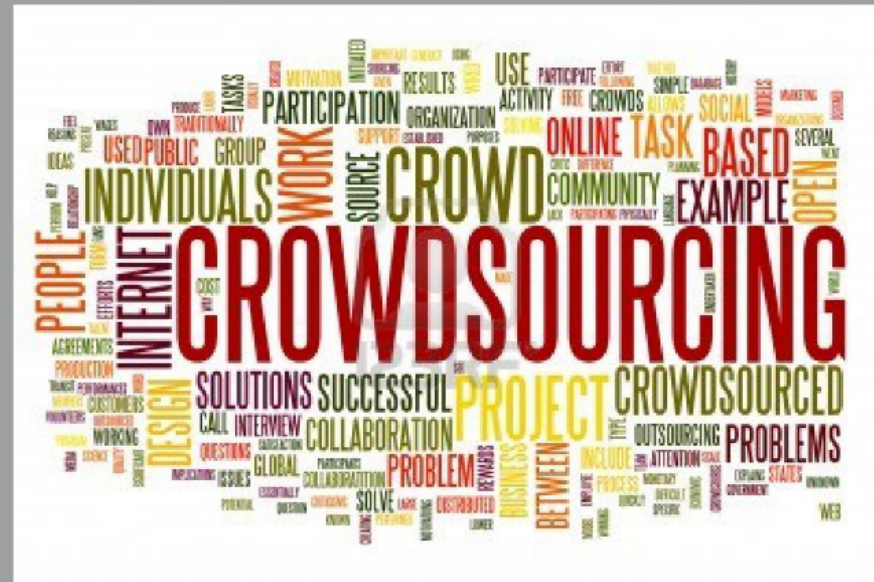
# Scores



Decay scores  
when malicious  
activity stops



# Crowdsourcing



# Reputation Use Cases

- Block access
- Enrichment
- Challenge
- Incorporate with additional controls

**RSA** CONFERENCE 2017

# Big Data Analysis for Client Reputation



**RSACONFERENCE2014**

# Client reputation

A mean to detect malicious clients...

WAF Triggers

Web attacks behavioral profiling

RSACONFERENCE2014

RSACONFERENCE2014

# WAF Triggers

**RSA**CONFERENCE**2014**



Web attacks behavioral profiling

**RSA<sup>®</sup>CONFERENCE 2014**



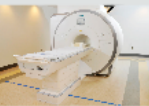
# Where can Behavioral Profiling Complement Traditional Protections?

Distributed Activity



RSAC/USENIX 2014

Reconnaissance



RSAC/CONFERENCE 2014

Targeted Attacks



RSAC/CONFERENCE 2014

**RSAC**CONFERENCE2014

# Distributed Activity



**RSACONFERENCE2014**

# Reconnaissance



# Targeted Attacks



**RSA CONFERENCE 2014**

# Behavioral?!

Clients



RSACONFERENCE2014

Applications



RSACONFERENCE2014

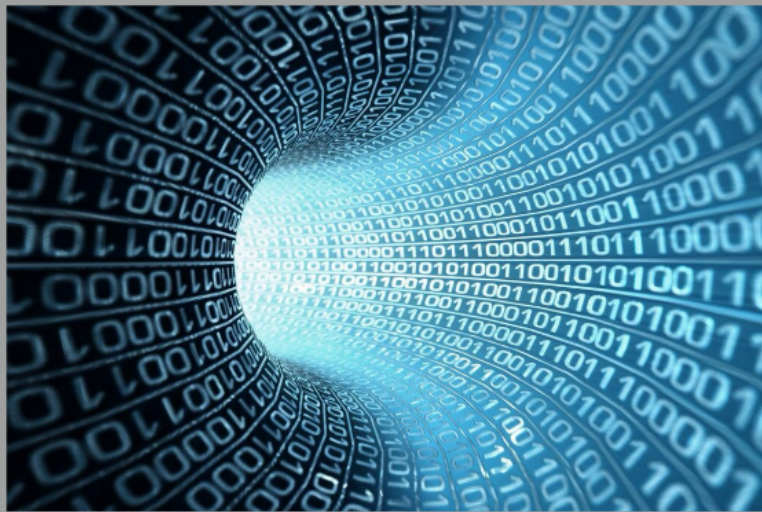
WAF Big Data



RSACONFERENCE2014

**RSACONFERENCE2014**

# WAF Big Data



**RSACONFERENCE2014**

# Applications



**RSA CONFERENCE 2014**

# Clients



**RSACONFERENCE2014**



# Case Study: Detecting Malicious Clients That are Targeting PHP Applications



## Objective

Find attackers that send PHP attacks

RSACONFERENCE 2014

## 3 Steps Technique

Step 1: Identify malicious requests  
Log entries with suspicious IP  
IPs

Step 2: Filter data by IP  
Obtain requests in documents based  
on the number of log entries  
IPs

RSACONFERENCE 2014

RSACONFERENCE 2014

## Objective

Find attackers that send PHP attacks

**RSACONFERENCE2014**

# 3 Steps Technique

## Step 1 - Analyze Applications' Behavior

Fingerprint platform behind each app (e.g. PHP)

RSACONFERENCE2014

## Step 2 - Analyze Client Behavior

Look for clients that try to access PHP URLs on ASP.NET apps

RSACONFERENCE2014

## Step 3 - Big Data Analysis

Calculate clients maliciousness based on the number of apps scanned

RSACONFERENCE2014

RSACONFERENCE2014

## Step 1 - Analyze Applications' Behavior

Fingerprint platform behind each app (e.g. PHP)

**RSACONFERENCE2014**

## Step 2 - Analyze Client Behavior

Look for clients that try to access PHP URLs on ASP.NET apps

## Step 3 - Big Data Analysis

Calculate clients maliciousness based on the number of apps scanned

**RSACONFERENCE2014**

# Let's Test Drive This Approach...

950

Malicious clients were detected over one week

RS&A CONFERENCE 2014

~9

The average amount of applications scanned by client

RS&A CONFERENCE 2014

236

Highest number of scanned applications by one client in one hour

RS&A CONFERENCE 2014

We analyzed 10% of Akamai traffic over a 1-week time period

7.2

The average score that represents clients maliciousness

RS&A CONFERENCE 2014

43%

Of the detected clients are web servers

RS&A CONFERENCE 2014

4 days

The average amount of time client was maliciously active

RS&A CONFERENCE 2014

# 950

Malicious clients were detected over one week

**RSACONFERENCE2014**



~9

The average amount of applications  
scanned by client

**RSA<sup>®</sup>CONFERENCE2014**

# 236

Highest number of scanned applications  
by one client in one hour

**RSACONFERENCE2014**

# 7.2

The average score that represents clients  
maliciousness

**RSA**CONFERENCE**2014**

# 43%

Of the detected clients are web servers

**RSACONFERENCE2014**

# 4 days

The average amount of time client was  
maliciously active

**RSACONFERENCE2014**

## Further Analysis of Clients Traffic

- PHP known vulnerabilities - RFI, XSS, SQLi, Path traversal...
- Brute force attacks - looking for WordPress and Joomla login pages
- Comment spamming
- And in the future: Zero day exploits...

**RSACONFERENCE2014**

## Summary

- Big data != Analytics/Reporting
  - Huge potential for active defense
- Big Data complements traditional detection techniques
- "Fight fire with fire" - distributed attacks call for "distributed detections"

**RSA CONFERENCE 2014**



# Q&A

**RSA** CONFERENCE 2011