RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Whose IP Is It Anyways: Tales of IP Reputation Failures

SESSION ID: SPO-T07

Michael Hamelin

Lead X-Force Security Architect
IBM Security Systems
@HackerJoe

What is reputation?

GAME OF THRONES


HEAR
ME
ROAR
LANNISTER
HBO GAME OF THRONES

Game of Thrones	Today on the Internet
• You wear crests and carry banners	• We communicate via IP addresses
• Reputation is often learned by word of mouth	• We cannot look at a web connection and see a “family crest”
• Reputation might also be called Gossip	• We lookup reputation in third-party systems

We have been conditioned to use IP reputation

We have assigned reputation since we started network security

Trusted	**Untrusted**
Inside	**Outside**
DMZ	**Partner Network**
Good Actors	**Bad Actors**

Script Kiddies, Activists, State Sponsored Adversaries

Our first exposure to IP reputation

We deployed firewalls and created our first IP Reputation System

Fighting SPAM with reputation

A good taste of success with IP Reputation

- Dynamic IP Blocking
- Real Time Blackhole Lists
- Trusted Senders
- Domain Keys
- Sender Policy Framework

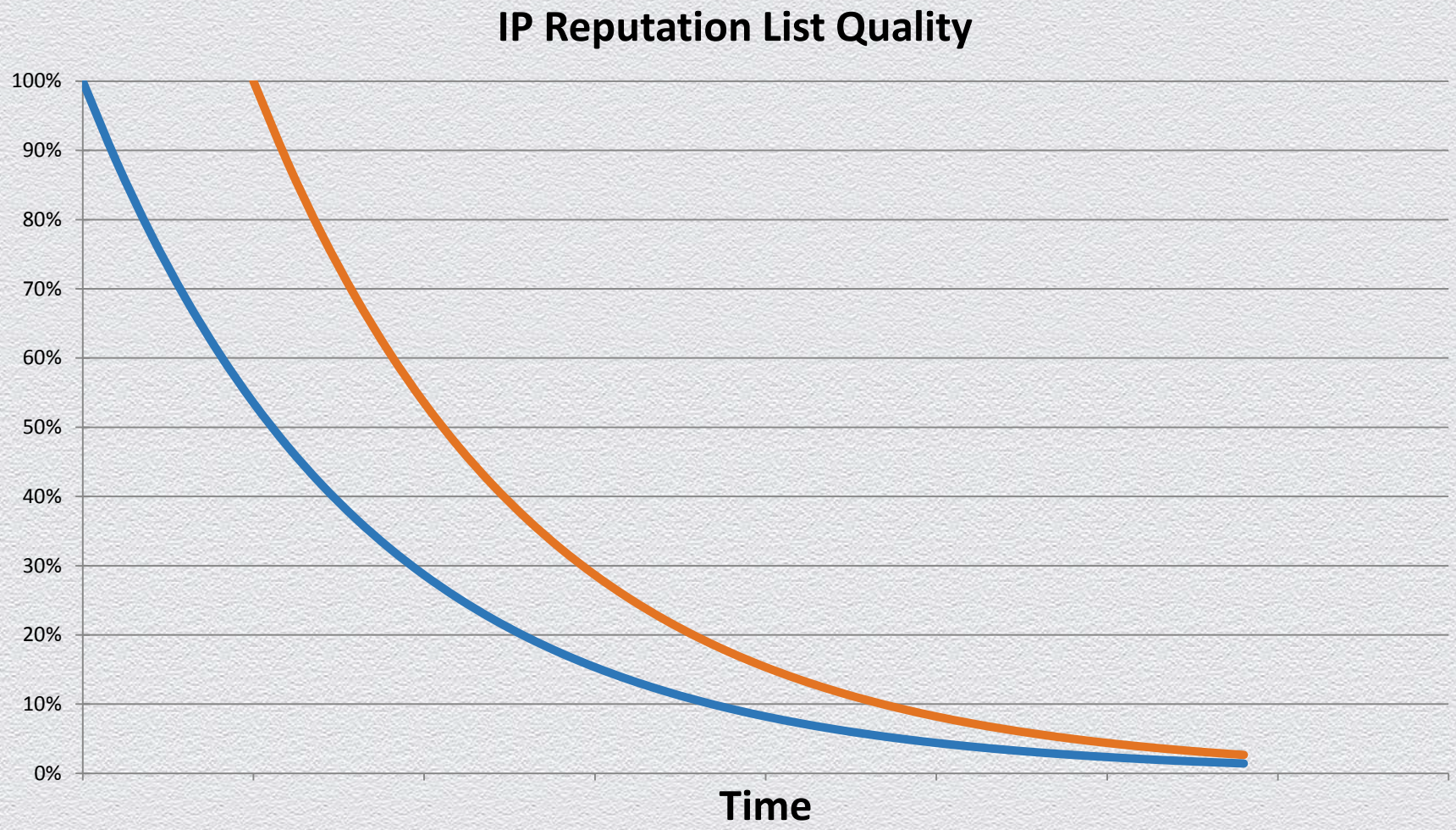
IP Reputation can improve security

- Browsing the web
  - Visit a site that downloads an executable
  - Process alert based on an AV engine
  - Blacklist the IP Address
- Good candidate for IP Reputation blacklist

Reputation solves everything

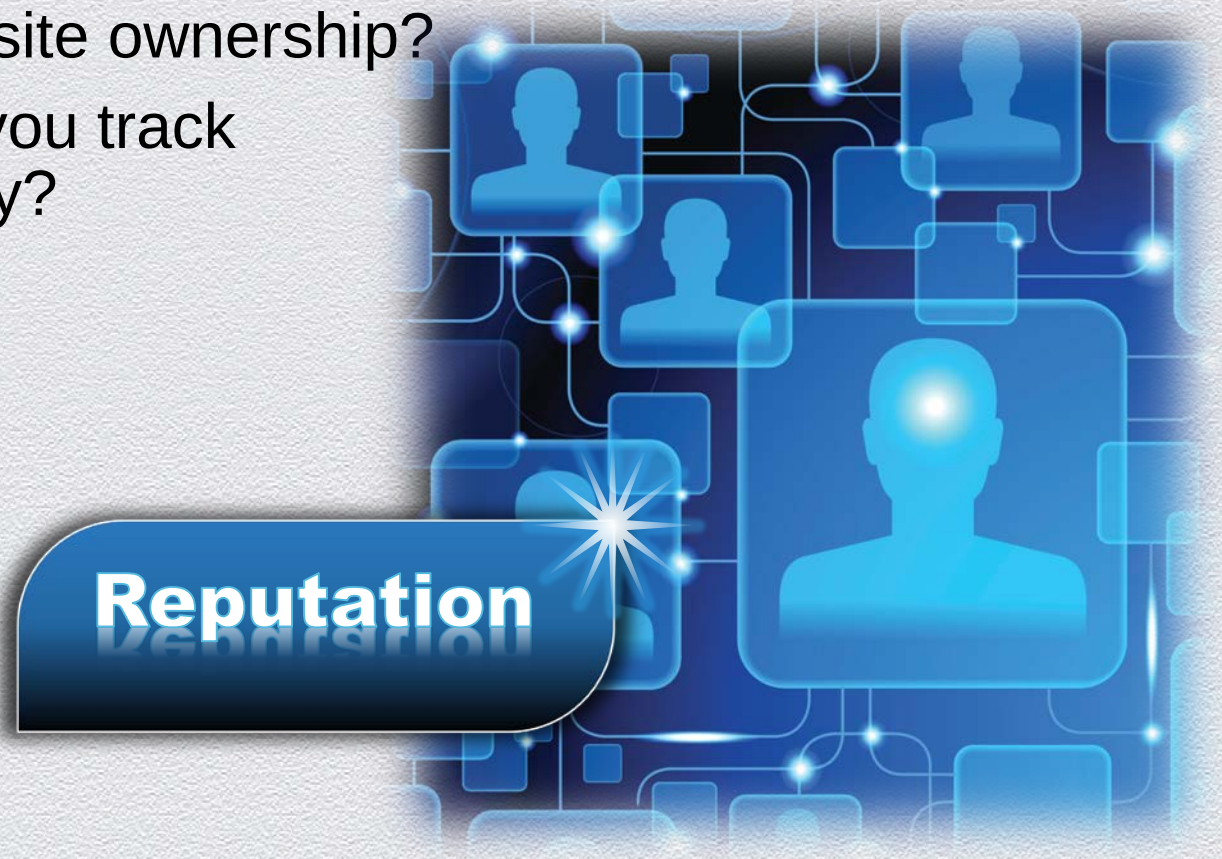
…It's not so easy

List effectiveness decays with age



So what else is complicating IP reputation?

- How about website ownership?
- How often can you track ownership easily?



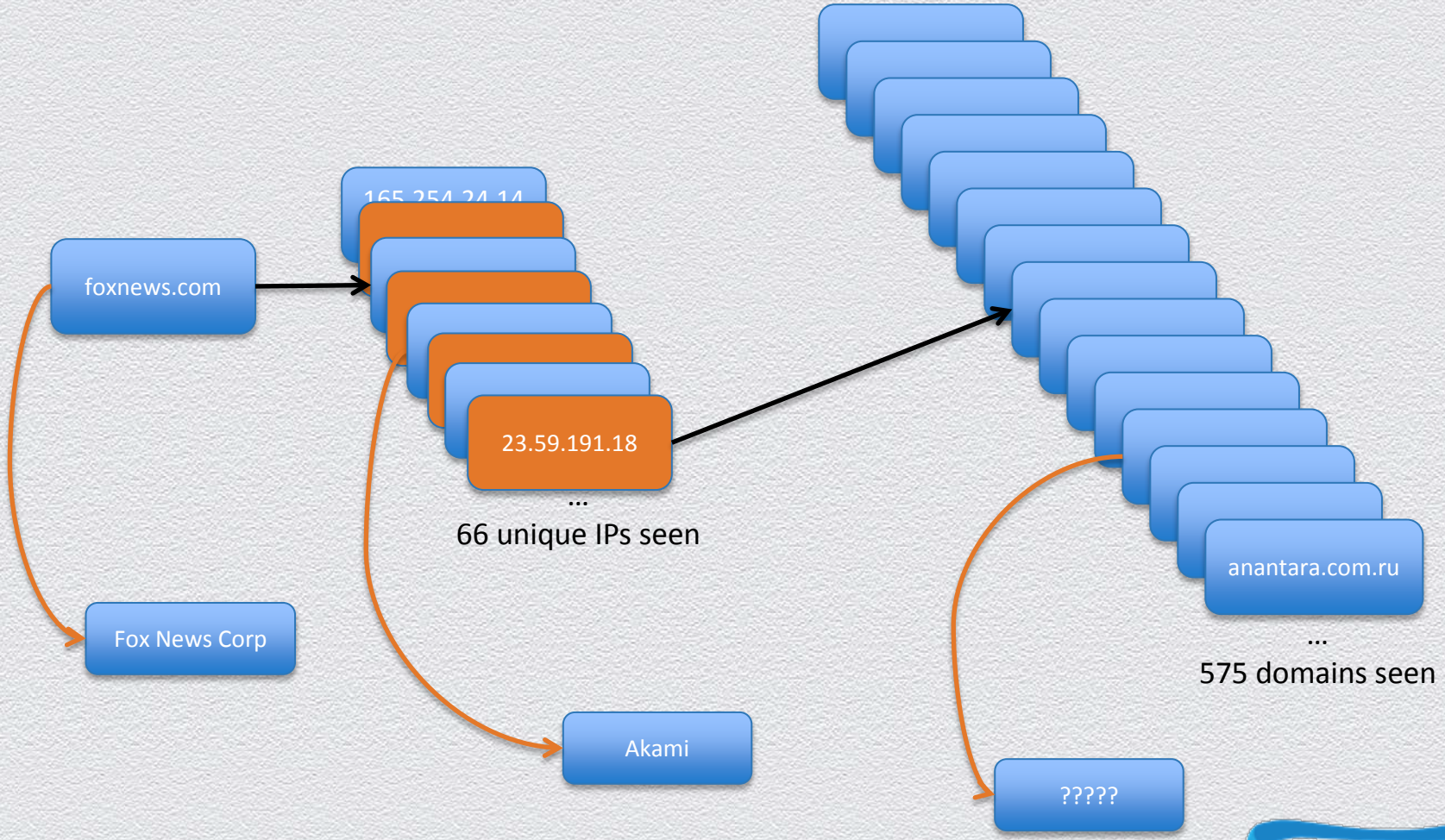
Case study #1

- We used an IP Reputation feed on our outbound web traffic
  - Malicious sites, anonymous proxy sites, botnet sites, etc.
- We found we had thousands of ‘false positives’
- We have 6K+ reports for foxnews.com

What is really happening

- Start with the 6K reports for Fox News
- Examine the DNS resolution for foxnews.com
- Generated a list of IP's that change over time with very short TTL
  - 20 second TTL

Why were some IP addresses flagged



Welcome to CDNs

- So whose IP's are these?
- Akamai owns all the IP's
- So it's not Fox's IP Addresses

- So the new question, whose reputation am I looking at?

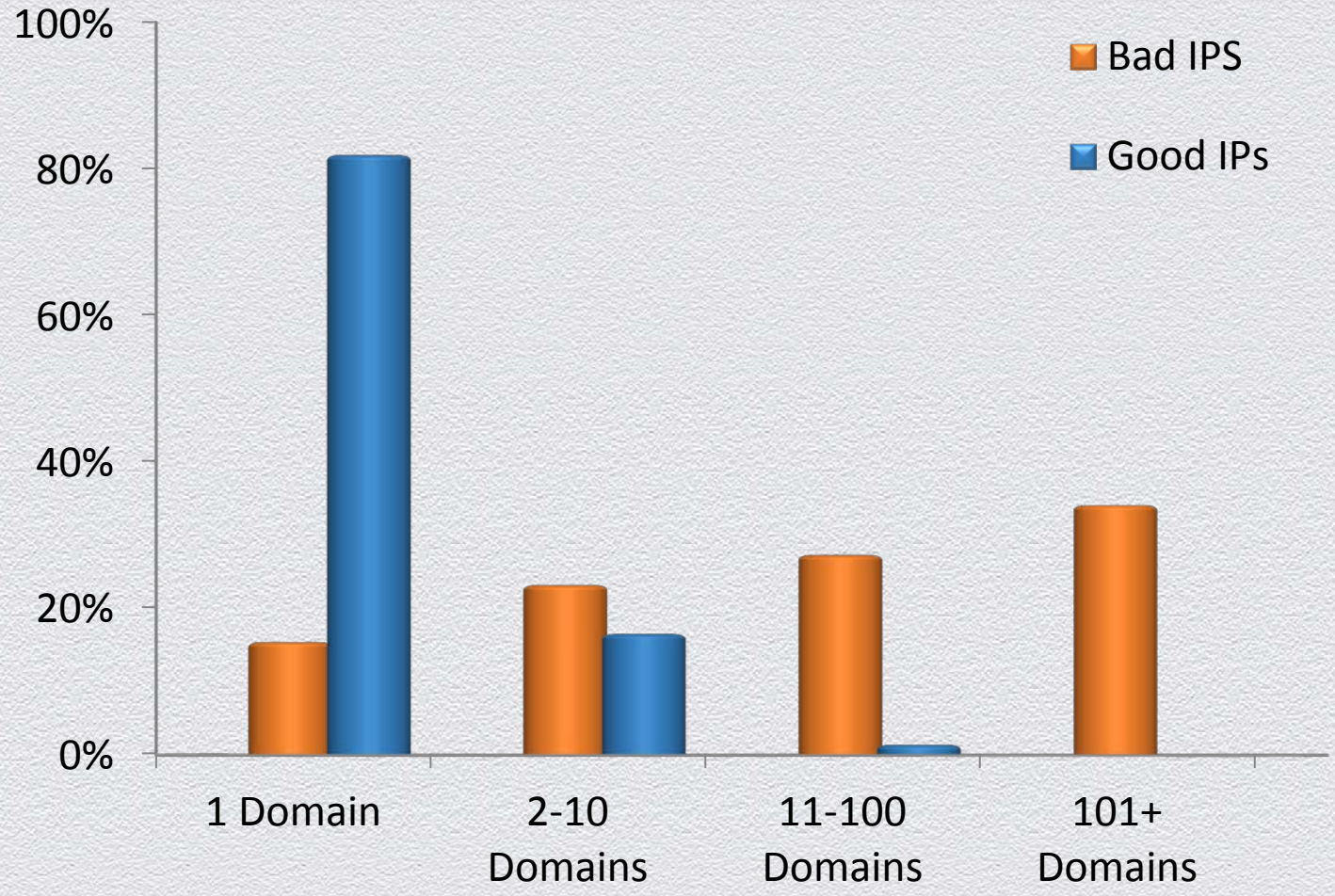
So do you trust this traffic?

- There are going to be several answers in the room today
- If you are hyper sensitive
  - These IPs have records of nefarious activity
- If you are an average site
  - My users didn't go to a nefarious domain

Lesson learned

- You need to understand **How** you want to use IP Reputation Feeds
- You should expect to have false positives on round 1
  - If not, someone else made your risk assessment and filtered them out
- Decide on your own whitelisting
  - i.e. allow Alexia top 1000
  - Easy for domains, harder for IPs

IPs with multiple domains hide more risk



Alert on all botnet activity from firewall logs

- Sounds like a reasonable IP Reputation problem
- Botnets communicate with Command & Control (C&C) Servers
- Buy some feeds on Botnet C&C activity and save the day

Case study #2

- We used the Botnet IP Reputation feed with our SIEM
- We created automatic alerts on all outbound connections that matched an IP in the reputation feed
- We got thousands or email alerts and they are all false positives

Botnet C&C and IP Reputation

- Large group of false positives pointing to Google
- Specifically many alerts to a few IPs used by App Engine

Yep, it's the cloud's fault

- SaaS presents a new problem for IP reputation
- Again, many domains behind just 1 IP address
- In this case an email relay used by several botnets lives on Google App Engine

Lesson Learned

- SaaS providers present a new complication to IP Reputation
- Bad Guys have been using the cloud for years
- We can whitelist SaaS providers but is that the right solution?

Aggregate IPs from malware monitoring sites

- Many sites publish malware DNS and IP lists
- Many solutions will provide local IOCs from malware samples
- We can take these aggregate lists and filter against our logs

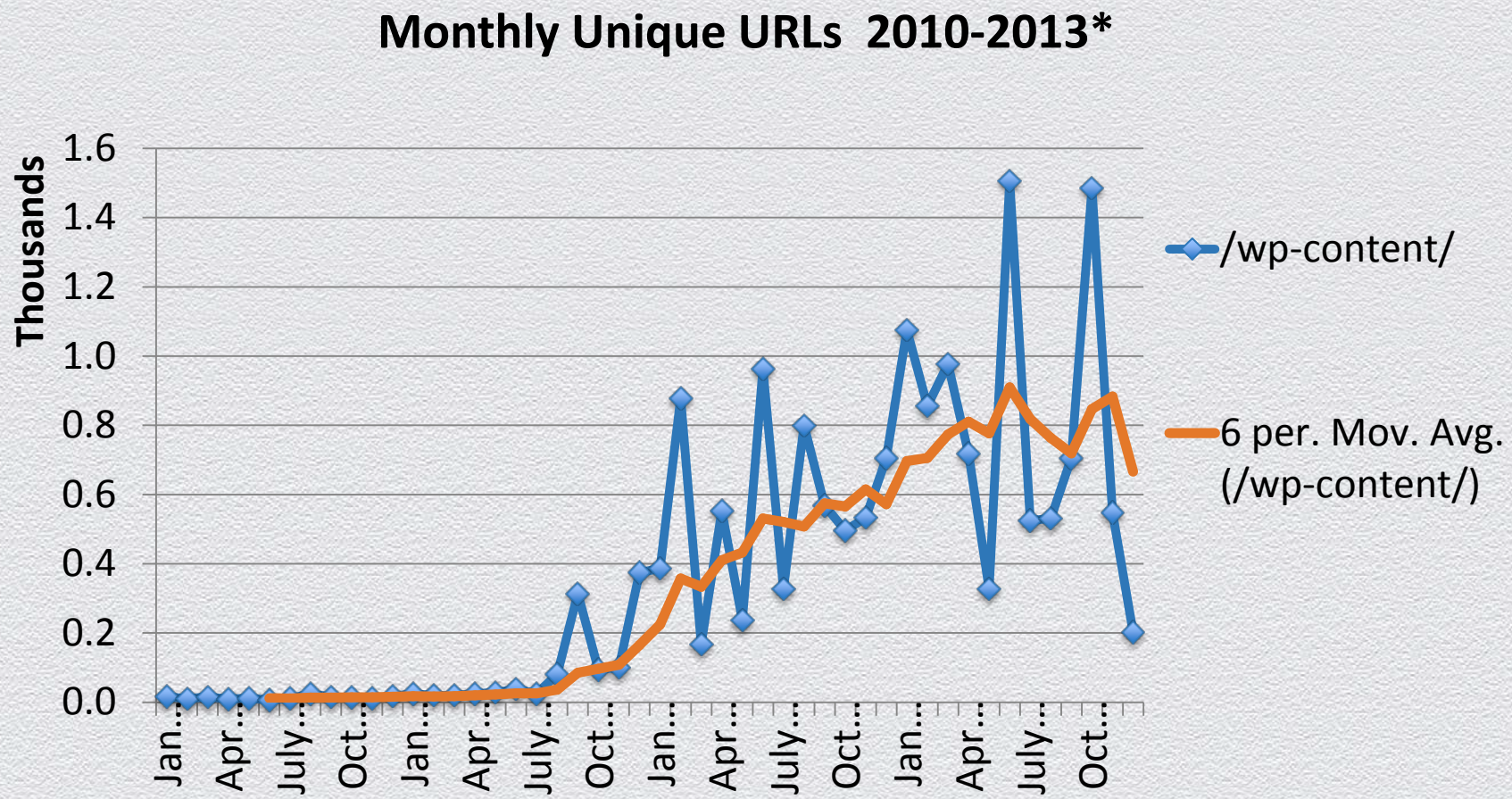
Case Study #3

- Apply IP Reputation from malware feeds to firewall logs
- SIEM sends an endless stream of alerts from many users browsing activity
- Desktop AV reports no issues
- Desktop investigations find no issues

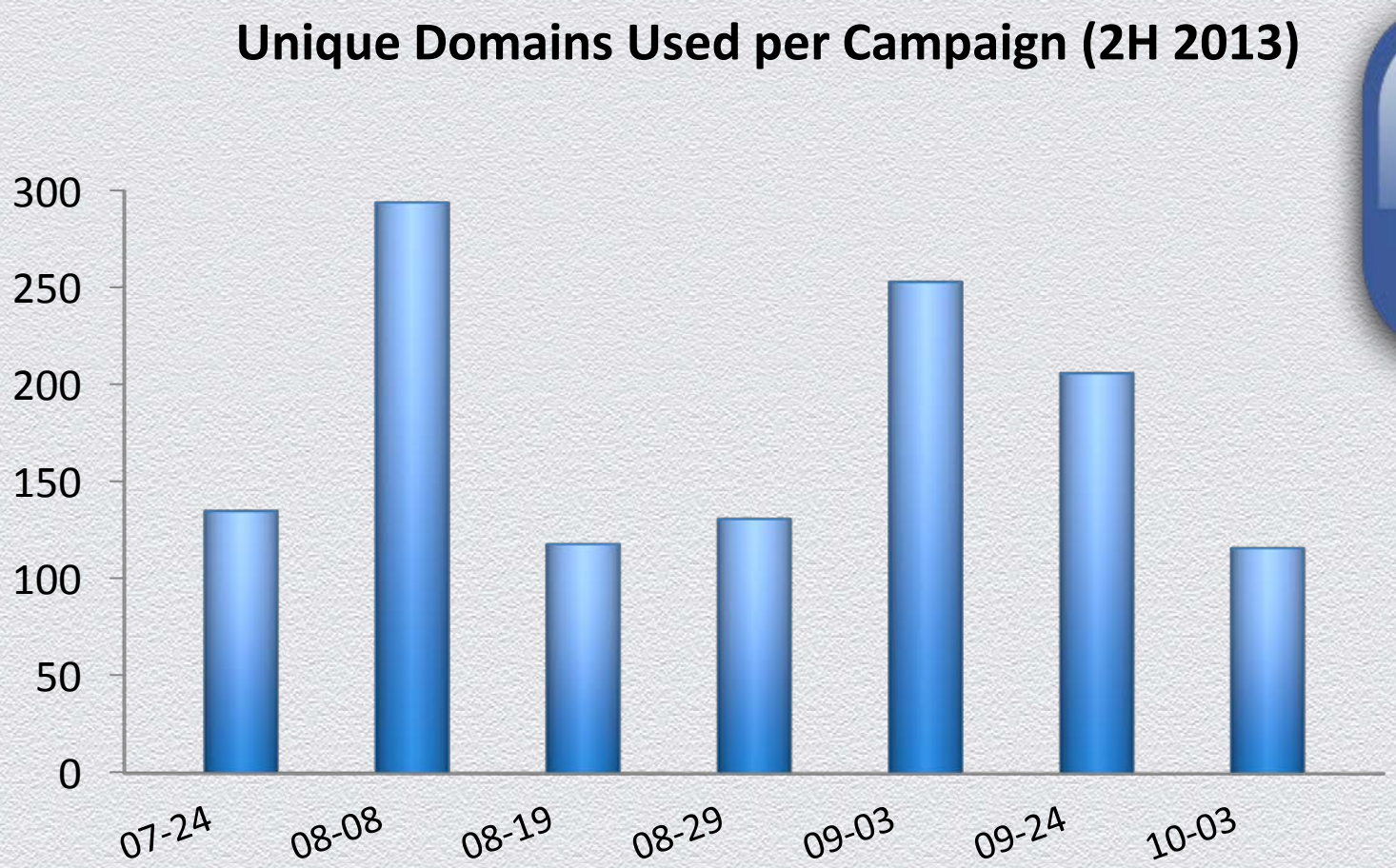
Stolen reputation

- What went wrong?
- We applied an IP based malware alert
  - The same Domain *versus* IP Address problems arise
- Many malware samples are delivered via compromised sites
  - Some are delivered only via one unique URI

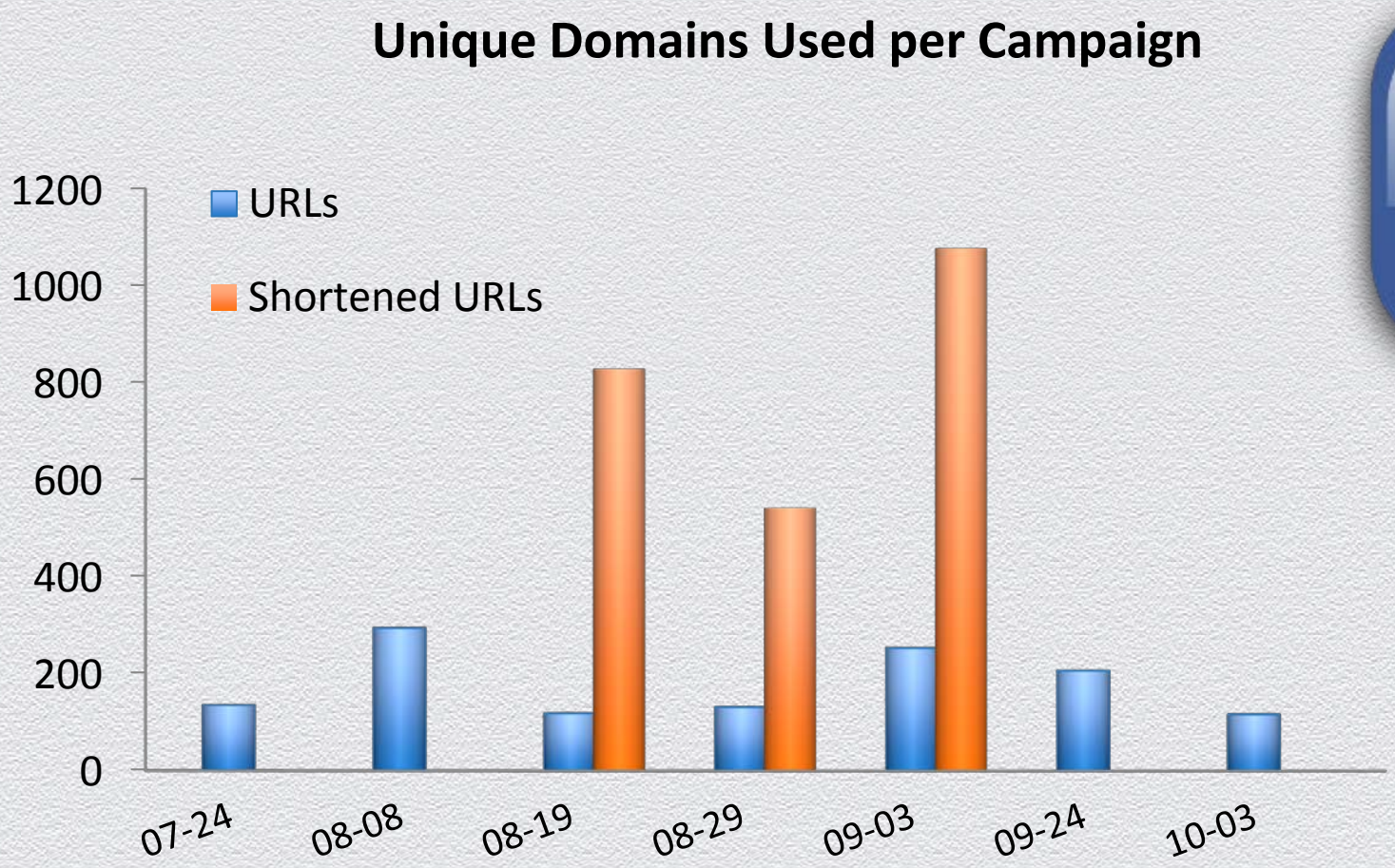
Phishing using compromised WordPress sites



Phishing campaigns can use hundreds of domains



They are even experimenting with URL Shorteners



Lesson Learned

- The Bad Guys know we are using IP Reputation
- They are continually looking for ways to get around our controls
- They have found it is relatively easy to **Steal** some **Good Reputation**

Can we implement IP Reputation correctly?

- That depends…
- We need to ask the question differently
- How can Reputation improve security?

Better ways to get there

- Domain Reputation
  - More specific than IP Reputation
  - False negative for the paranoid/sensitive

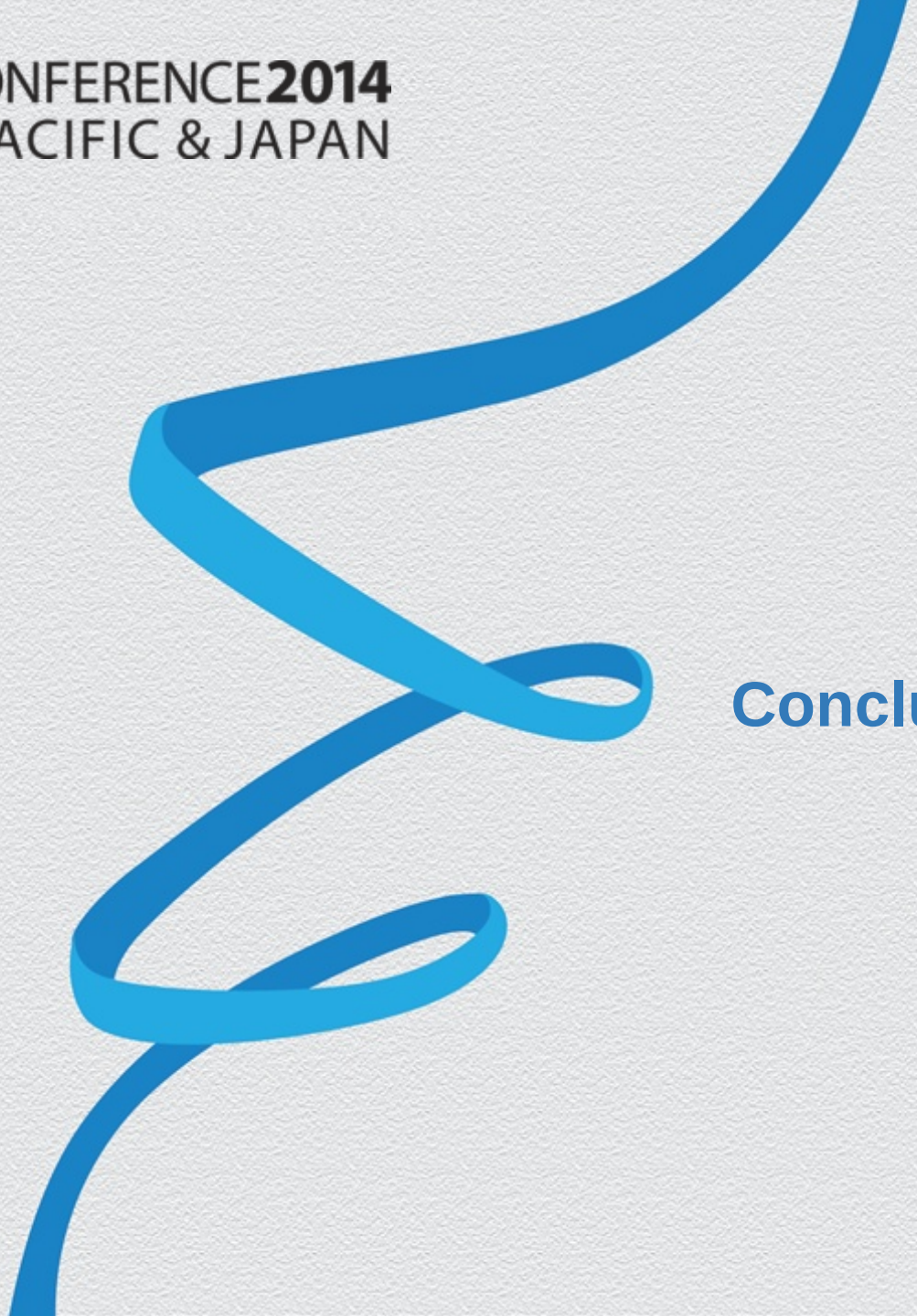
  - Partial solution for CDN issue
  - Partial solutions for SaaS issues
  - No help in stolen reputation
    - Full URL blocking will block legitimate site

We need dynamic reputation systems

- Since …
  - IP Reputation and Domain Reputation are less than perfect
  - Reputation get stale fast
  - The Bad Guys move very fast

Reputation Best Practices

- Reputation isn't black and white
  - It's very grey and thus a confidence score is needed on all results
- Reputation systems need to be active, reach out and touch the net
- Reputation systems need to be real-time
  - Age is very important
- System that use Reputation need to query for reputation and confidence scores
- Reputation scoring must factor in the use case



Conclusions

Q & A

Michael Hamelin
michael.hamelin@us.ibm.com