Moving Beyond Legacy Approaches to Network Security and Getting Ahead of Targeted and Zero-Day Malware

Eddie Schwartz
CSO, RSA, The Security Division of EMC²

MENA Information Security Conference 2011

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Agenda

- Current thinking and better thinking
- Four Techniques, and why removing hay is the way to go
- An example or two

© Copyright 2011 EMC Corporation. All rights reserved.

Advanced Adversaries and Threats

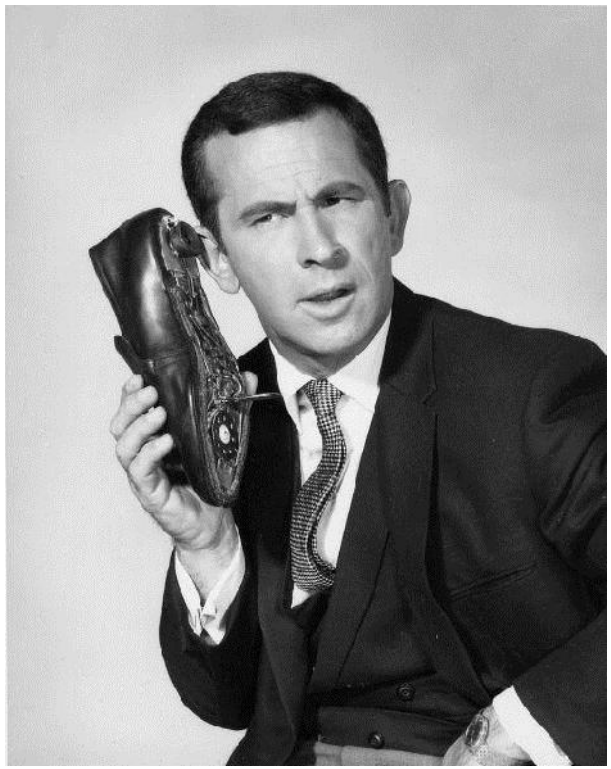
Two “general” schools of thought:

The APT

- Get in!

- Stay in!

- Steal information that leads to competitive or intelligence advantage!



NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Advanced Adversaries and Threats

Two “general” schools of thought:

Mass Malware / Cyber Crime

- Build BotNets!
- Make Money!
- Repeat!

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Advanced Adversaries and Threats

- Goals, motivations, capabilities, etc. may be different, but there are similarities:

Mass Malware / Cyber Crime

1) Mass spam campaign with social engineering hook.
2) Download of malware to establish foothold
3) Capture and exfiltration of interesting data
4) Rinse and Repeat

The APT

1) Targeted Spear-phish against specific targets.
2) Download of malware to establish foothold.
3) Hash dump and lateral movement.
4) Exfiltration of data

We'll come back to this!

© Copyright 2011 EMC Corporation. All rights reserved.

Incident investigation in practice

- Traditional
  - IDS / IPS
  - Log management
  - Pcap / wireshark
  - Even “malware protection systems”

NETWITNESS

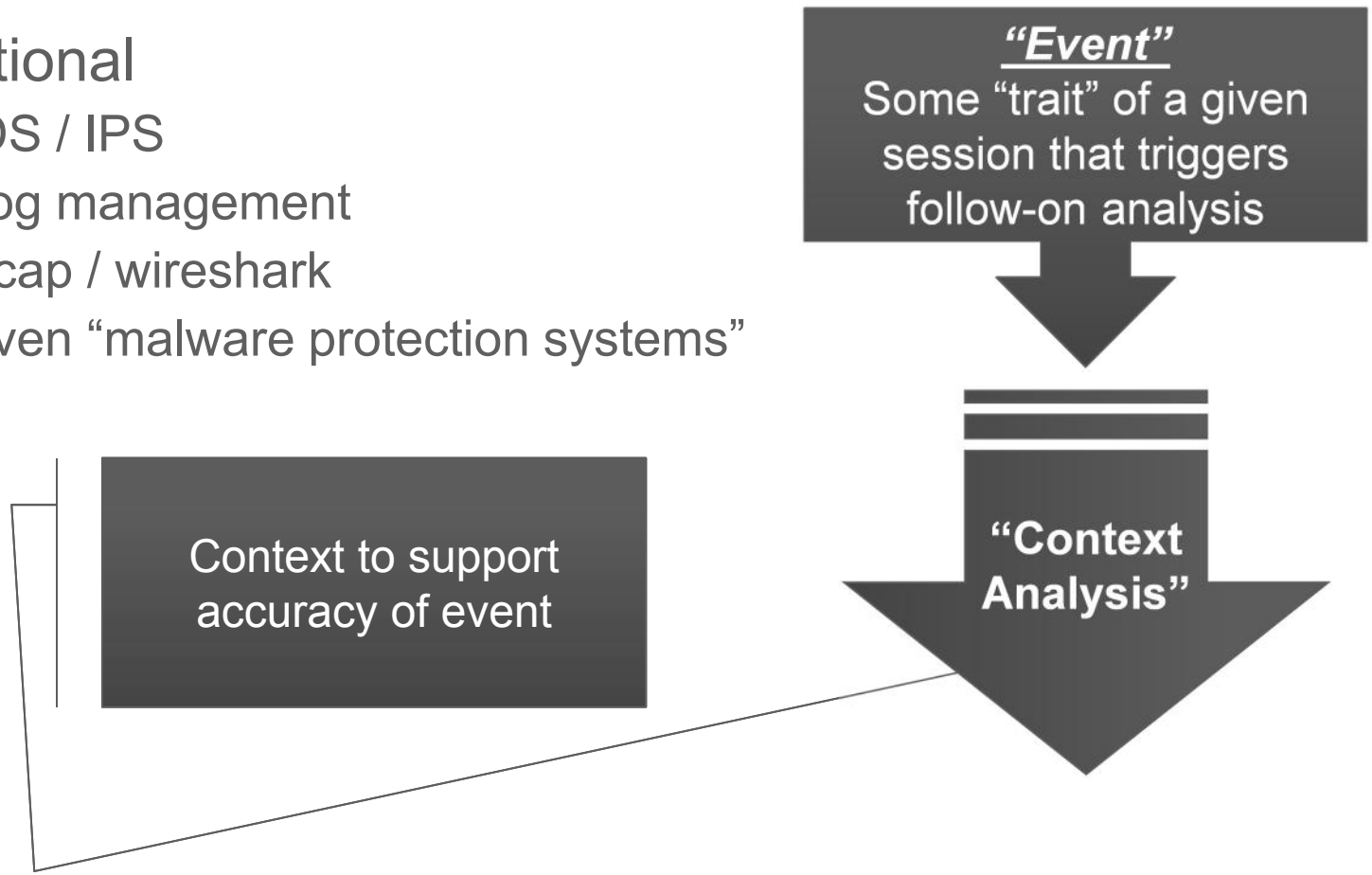
RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Incident investigation in practice

- Traditional
  - IDS / IPS
  - Log management
  - Pcap / wireshark
  - Even “malware protection systems”



NETWITNESS

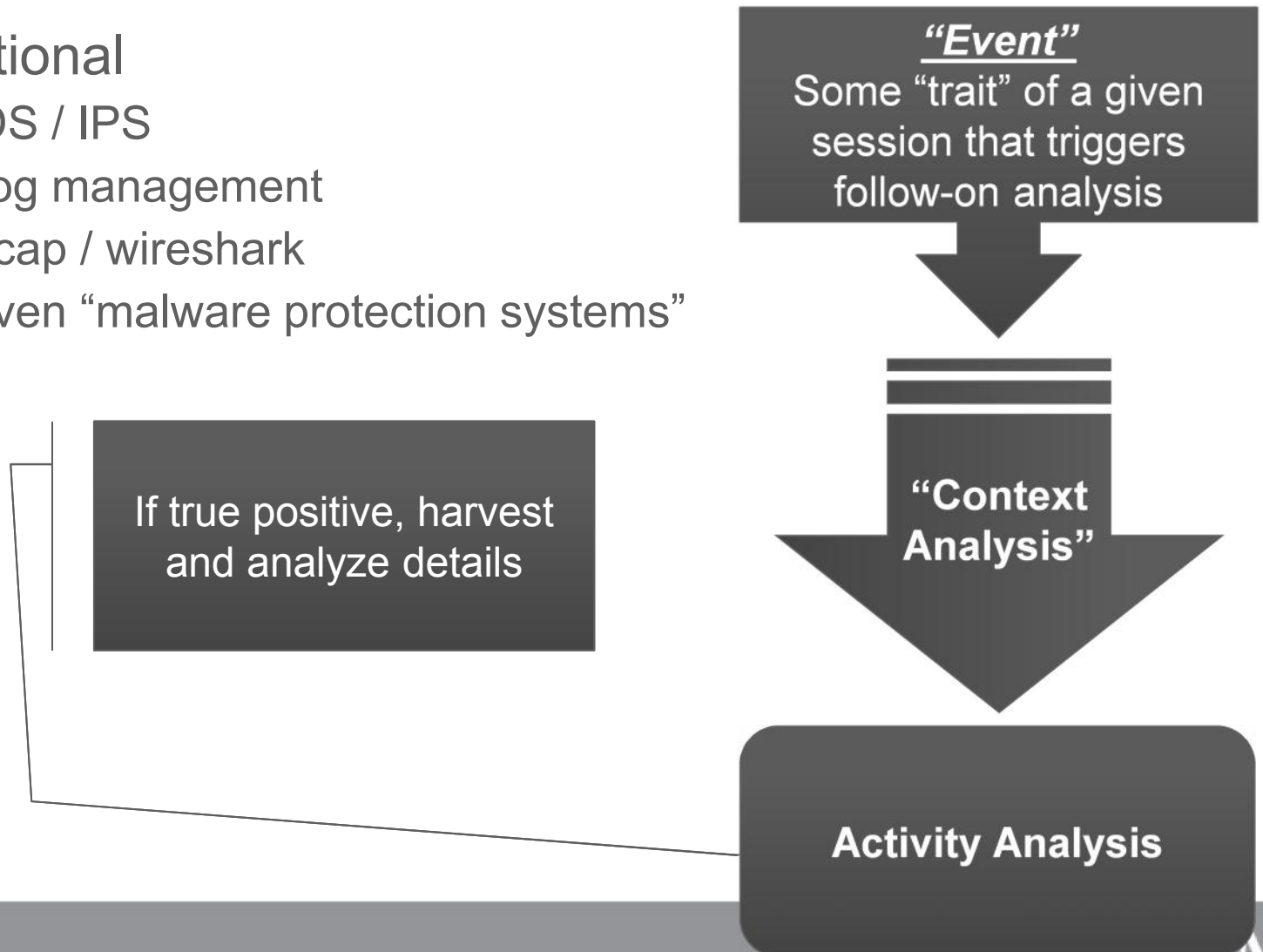
RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Incident investigation in practice

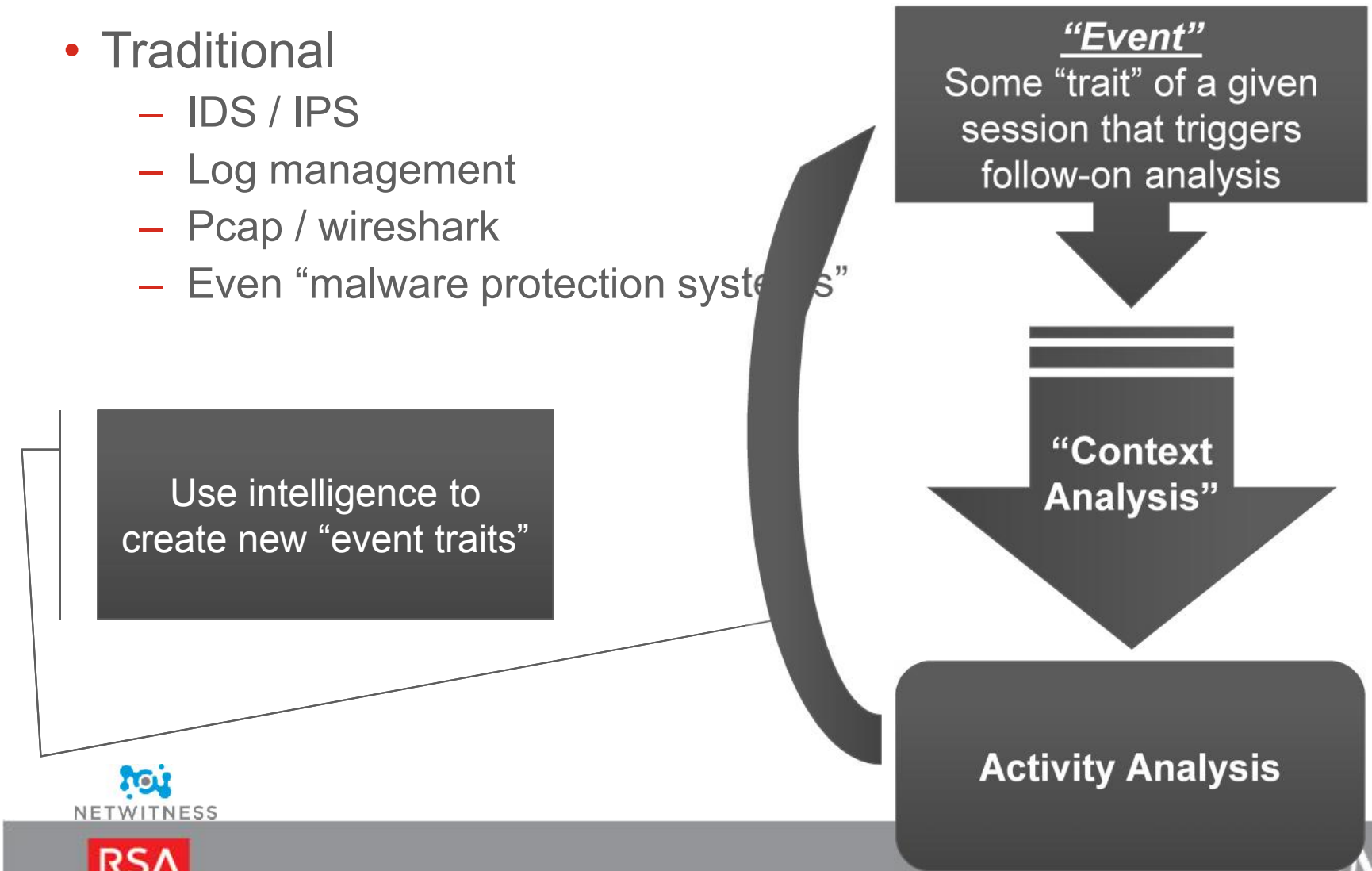
- Traditional
  - IDS / IPS
  - Log management
  - Pcap / wireshark
  - Even “malware protection systems”



© Copyright 2011 EMC Corporation. All rights reserved.

Incident investigation in practice

- Traditional
  - IDS / IPS
  - Log management
  - Pcap / wireshark
  - Even “malware protection systems”



NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Incident investigation in practice

- Traditional
  - IDS / IPS
  - Log management
  - Pcap / wireshark
  - Even “malware prote

© Copyright 2011 EMC Corporation. All rights reserved.

Gaps

- Current approaches that use this methodology are missing lots of problems
- But, before we dissect the reasons why, let's look at a forensics-based process, as performed on the host...

© Copyright 2011 EMC Corporation. All rights reserved.

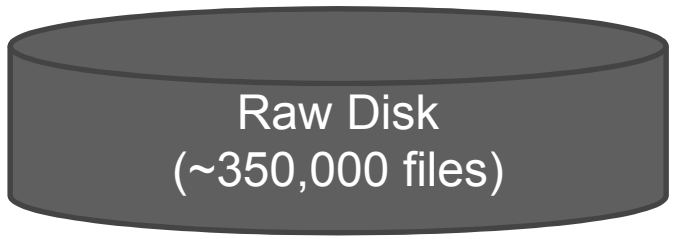
Analogy: Host-Based Forensics

- Find malware

© Copyright 2011 EMC Corporation. All rights reserved.

Analogy: Host-Based Forensics

- Find malware

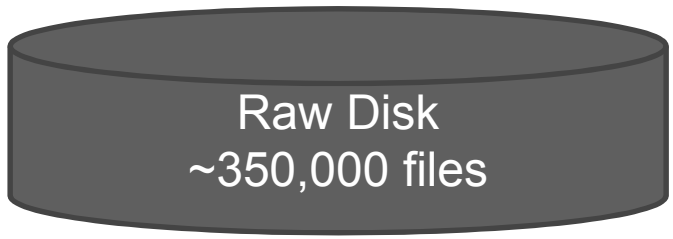


100% of Total

© Copyright 2011 EMC Corporation. All rights reserved.

Analogy: Host-Based Forensics

- Find malware



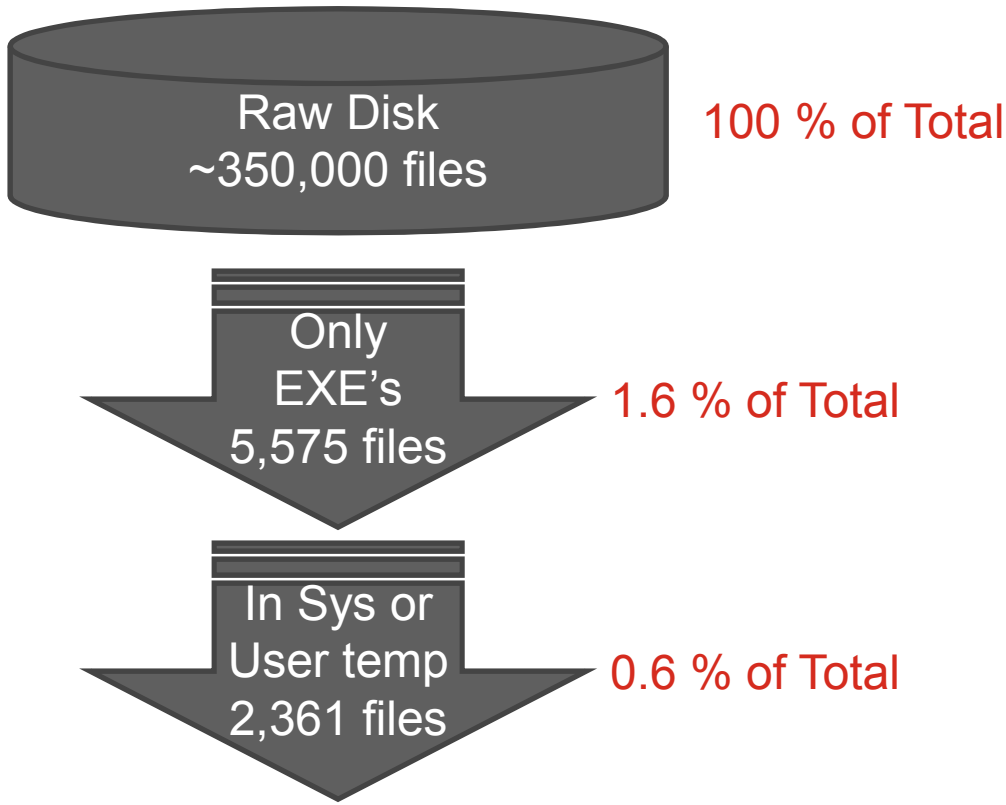
100 % of Total

1.6 % of Total

© Copyright 2011 EMC Corporation. All rights reserved.

Analogy: Host-Based Forensics

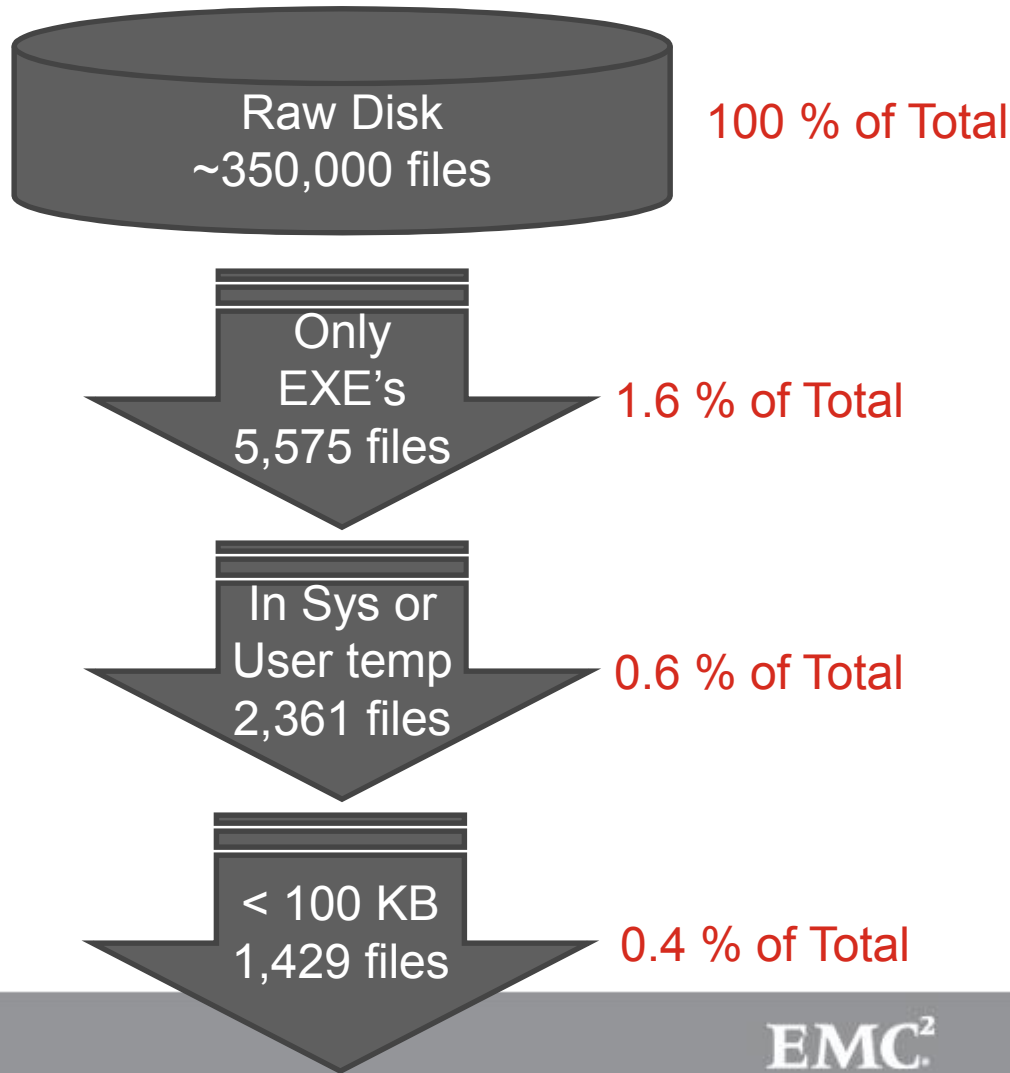
- Find malware



© Copyright 2011 EMC Corporation. All rights reserved.

Analogy: Host-Based Forensics

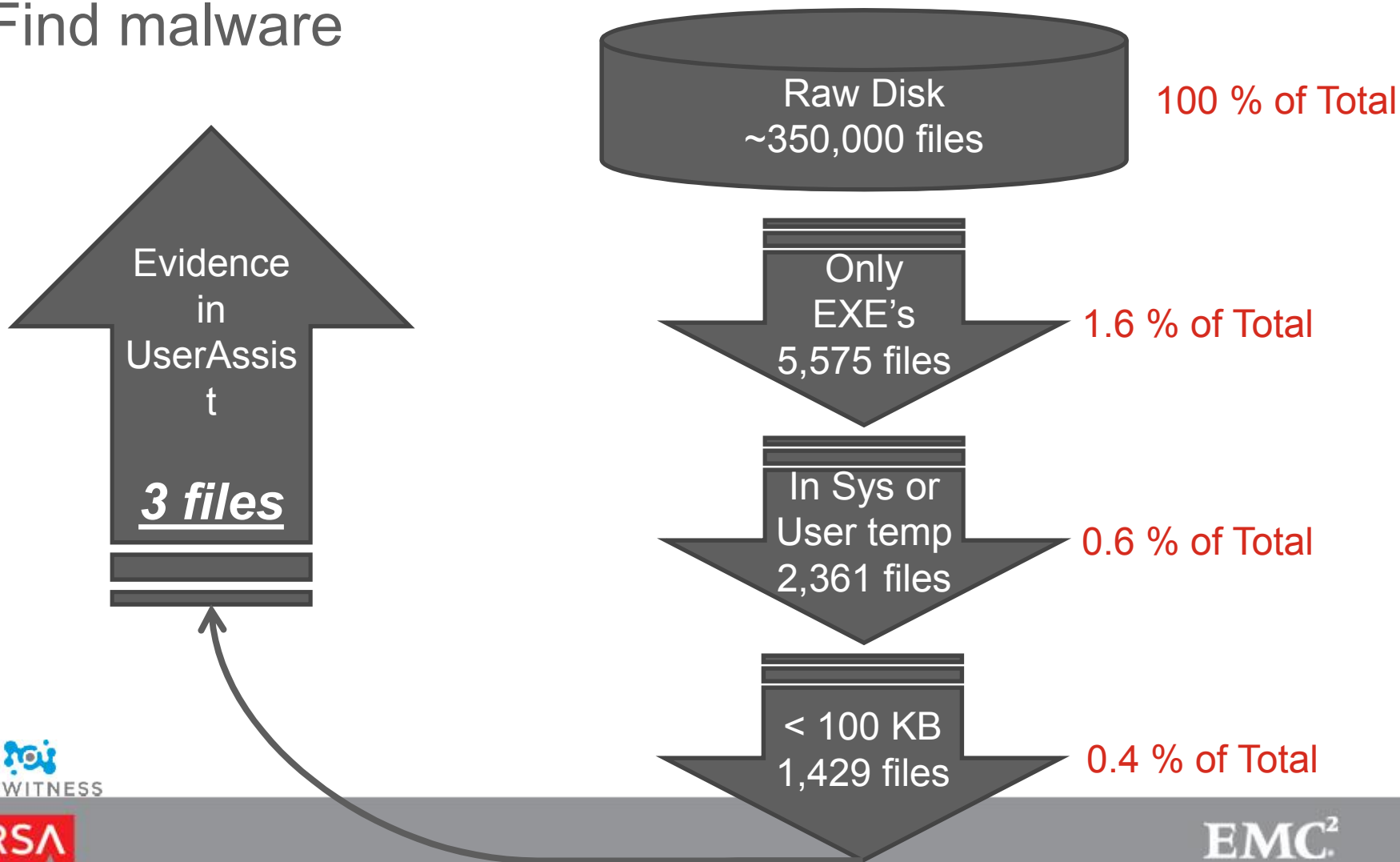
- Find malware



© Copyright 2011 EMC Corporation. All rights reserved.

Analogy: Host-Based Forensics

- Find malware



© Copyright 2011 EMC Corporation. All rights reserved.

What just happened there???

We found malware...

...by NOT looking for malware!!!

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Example: Good network visualization

- Find Compromises

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Example: Good network visualization

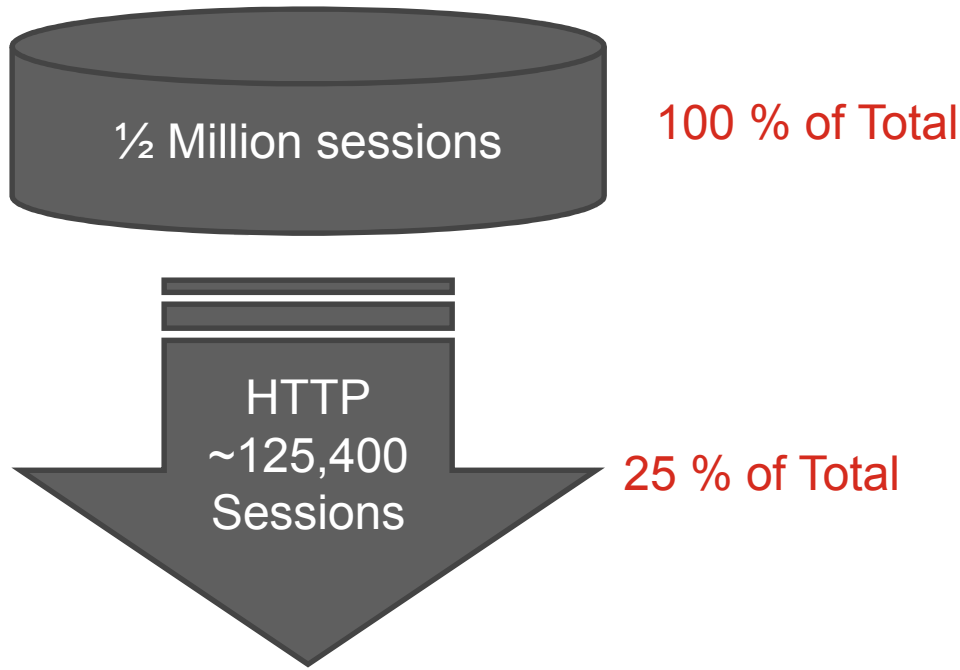
- Find Compromises

100 % of Total

© Copyright 2011 EMC Corporation. All rights reserved.

Example: Good network visualization

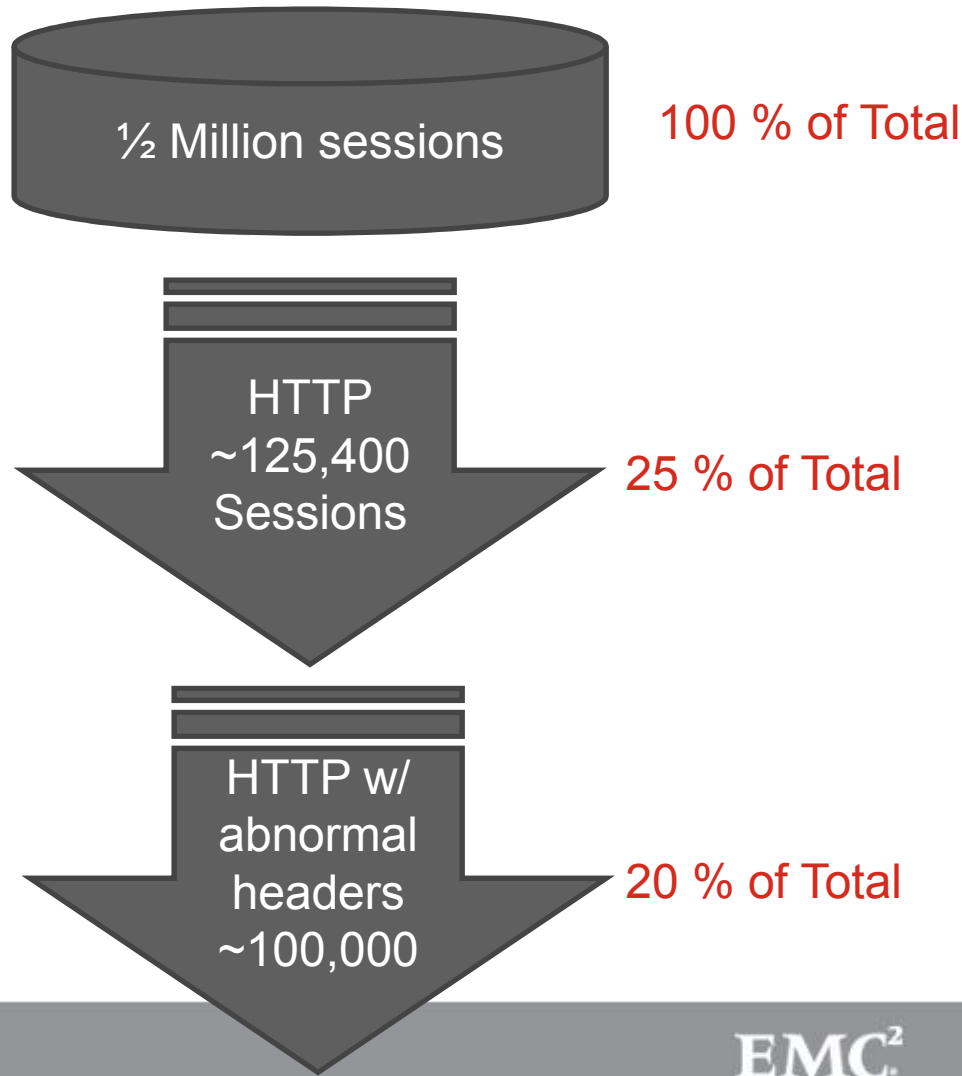
- Find Compromises



© Copyright 2011 EMC Corporation. All rights reserved.

Example: Good network visualization

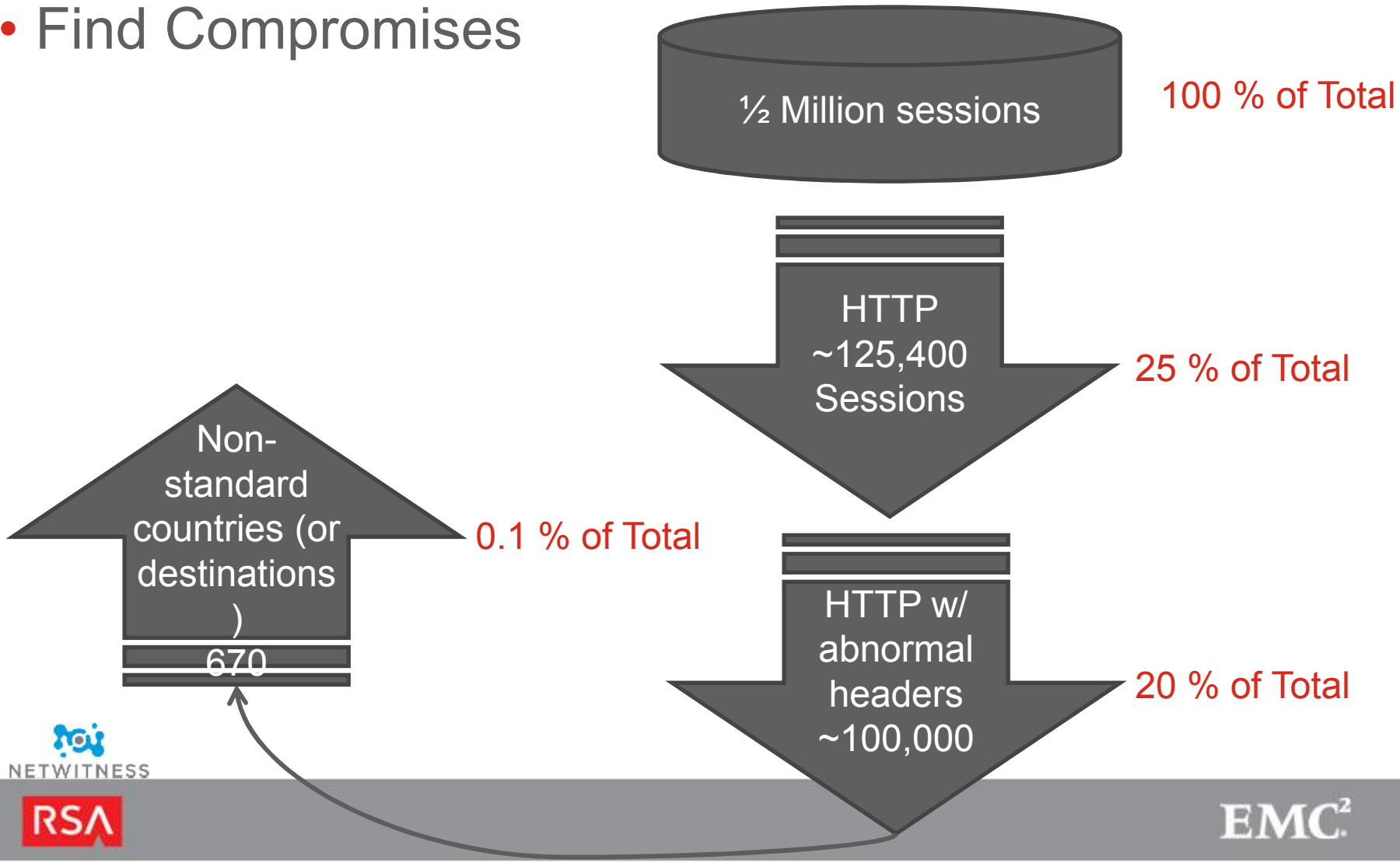
- Find Compromises



© Copyright 2011 EMC Corporation. All rights reserved.

Example: Good network visualization

- Find Compromises



NETWITNESS

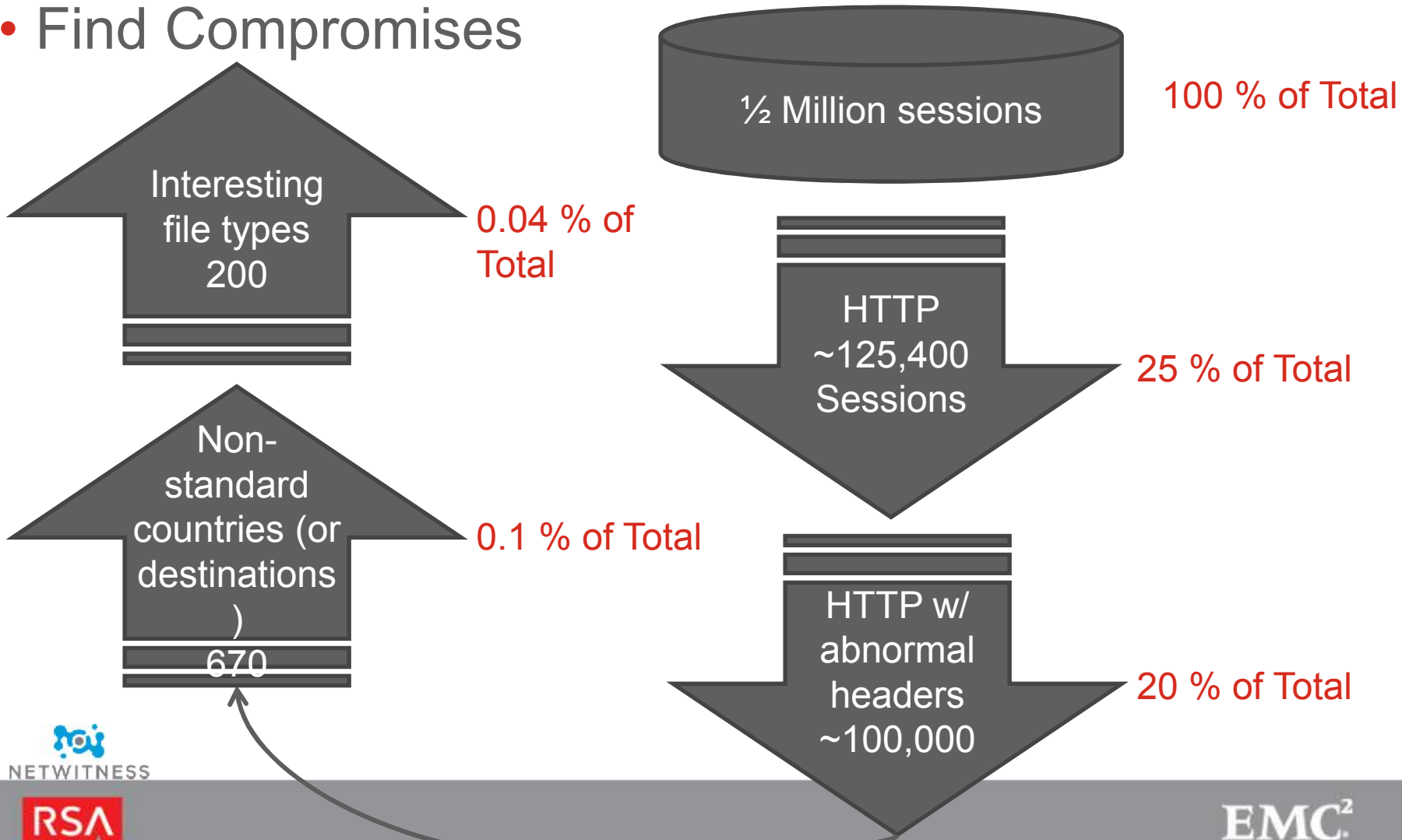
RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Example: Good network visualization

- Find Compromises



NETWITNESS

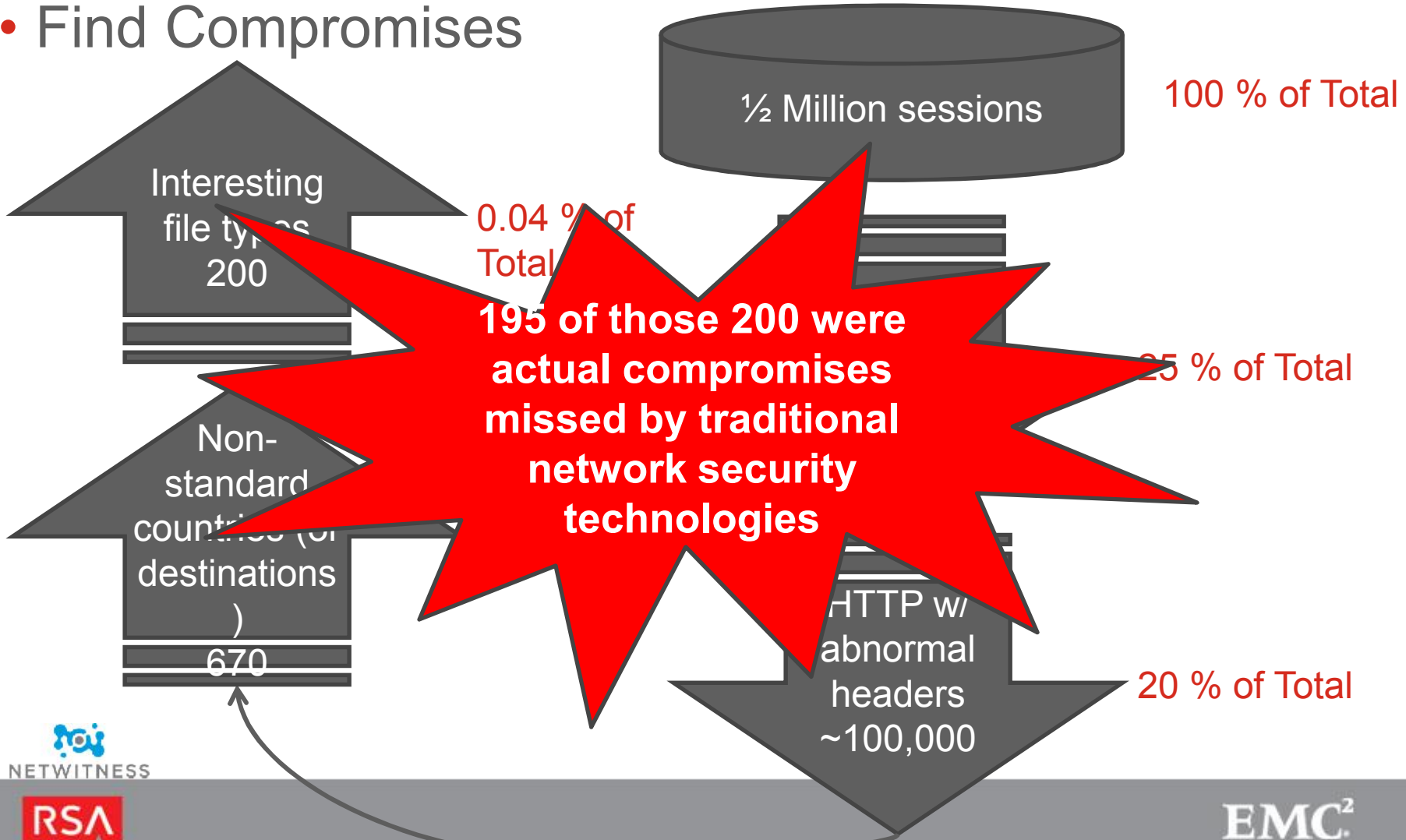
RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Example: Good network visualization

- Find Compromises



NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

- Traditional methods

NETWITNESS

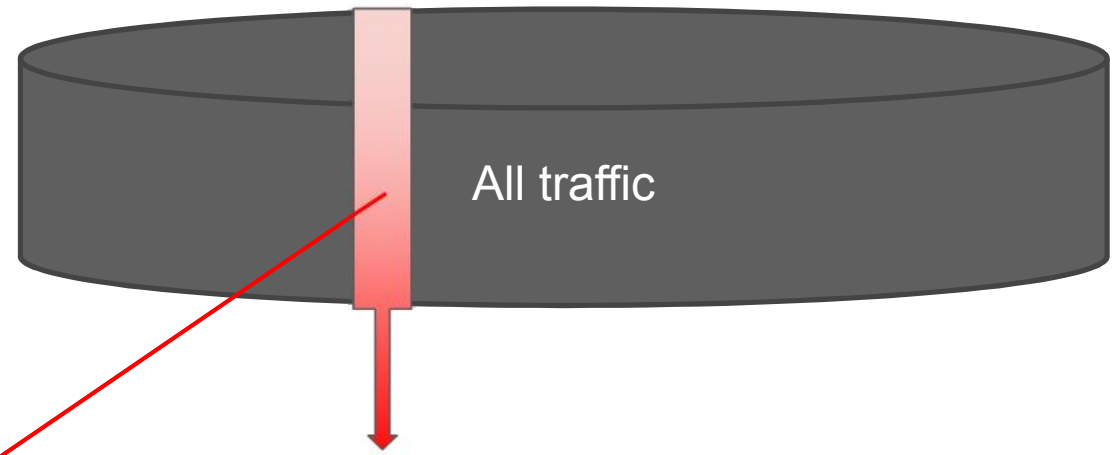
RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

- Traditional methods



"Events"
VERY small subset of all activity

NETWITNESS

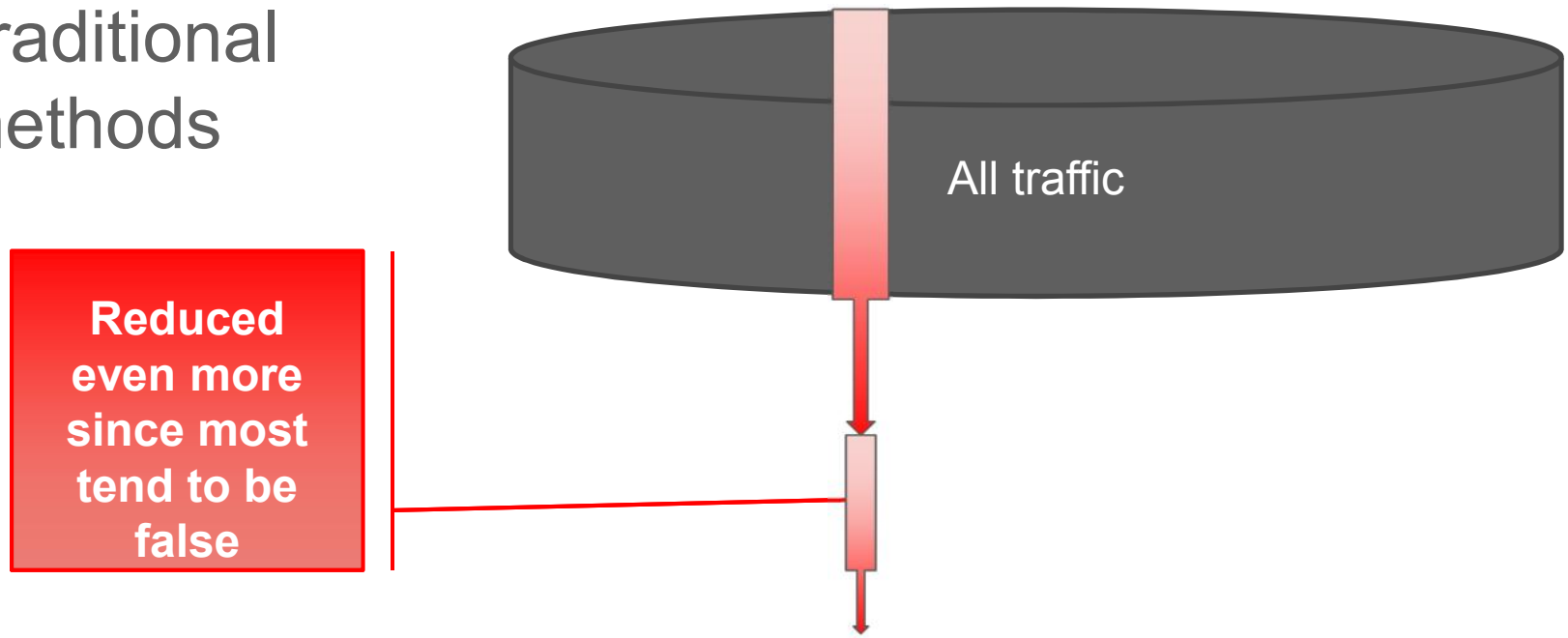
RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

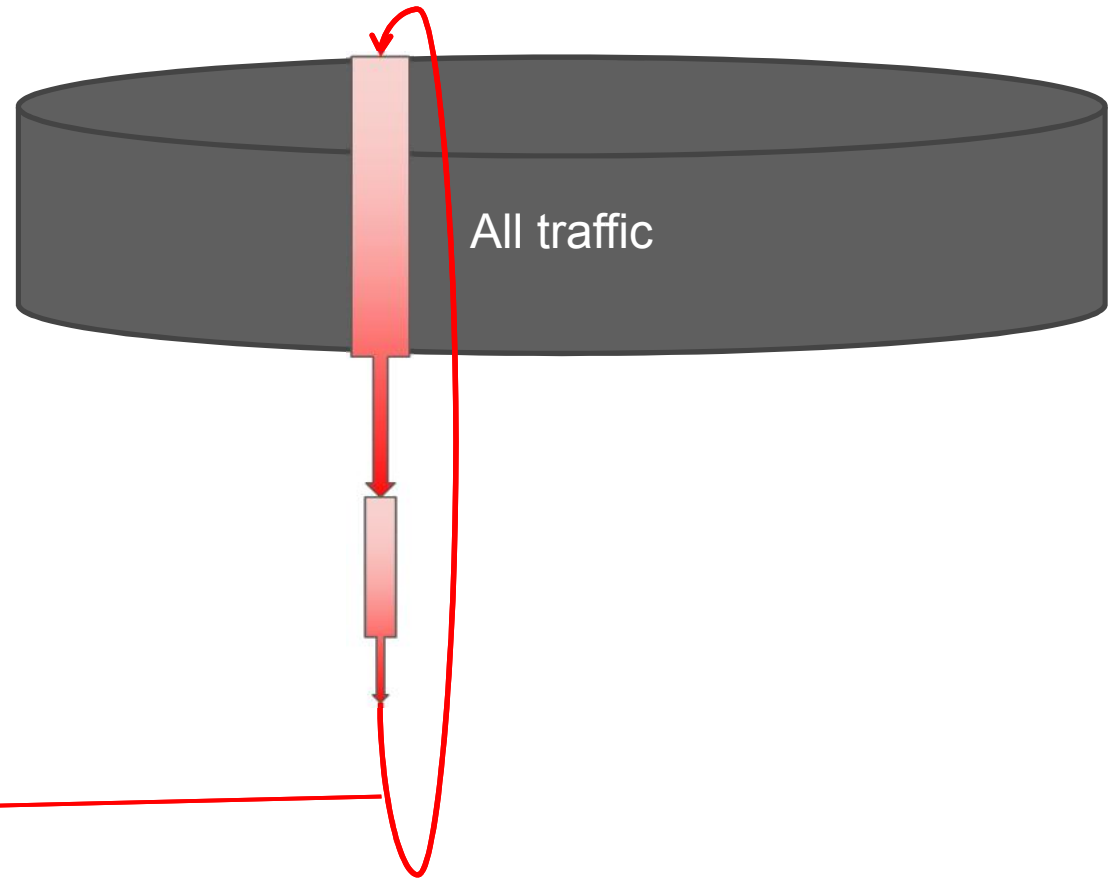
- Traditional methods



© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

- Traditional methods



"New intelligence" is nothing more than variations of the initial intelligence.

There really is *NO* NEW

© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

- Traditional methods

"New intelligence" is nothing more than variations of the initial intelligence.

There really is *NO* NEW

This is why accuracy of security today has been on a rapid decline over the past decade

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

- Real network analysis and visibility

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

- Real network analysis and visibility

NETWITNESS

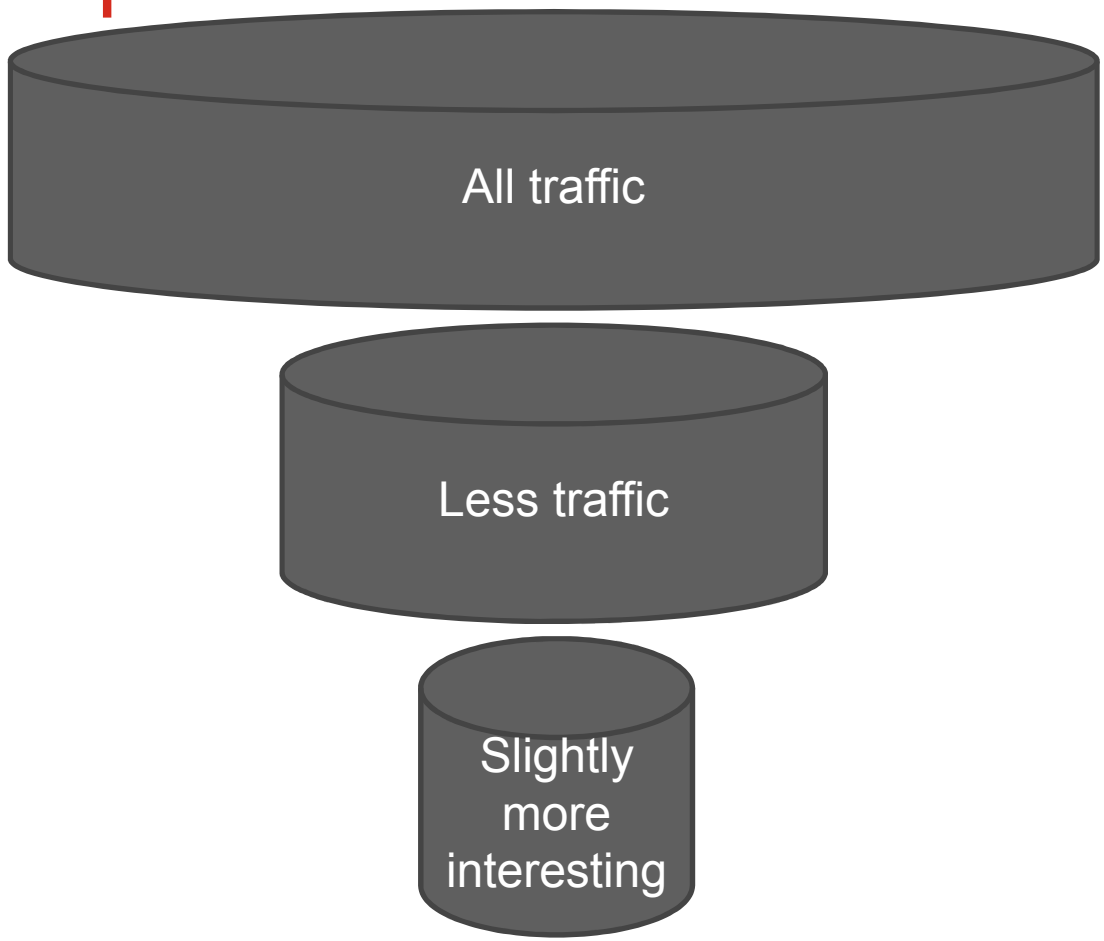
RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

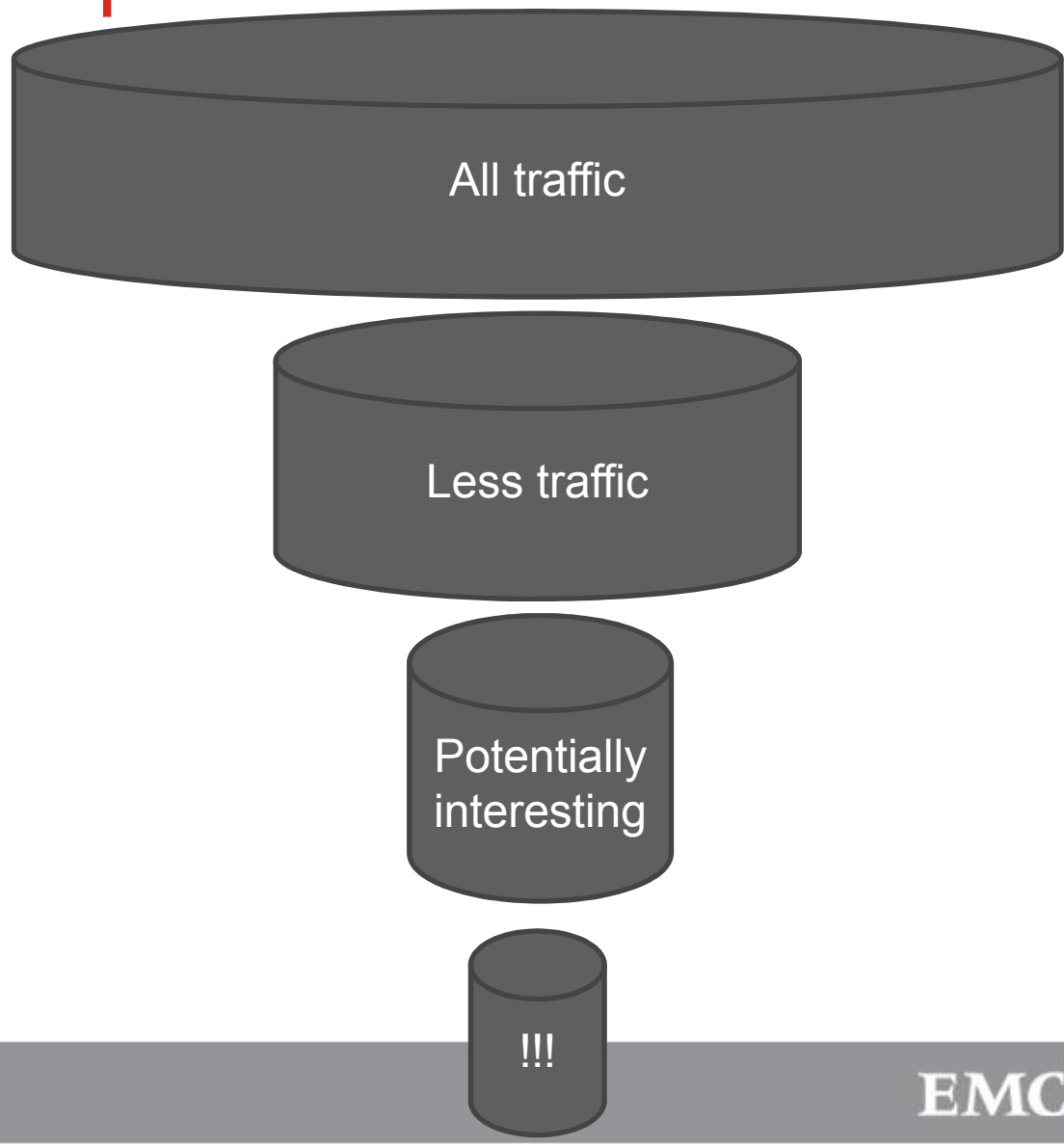
- Real network analysis and visibility



© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

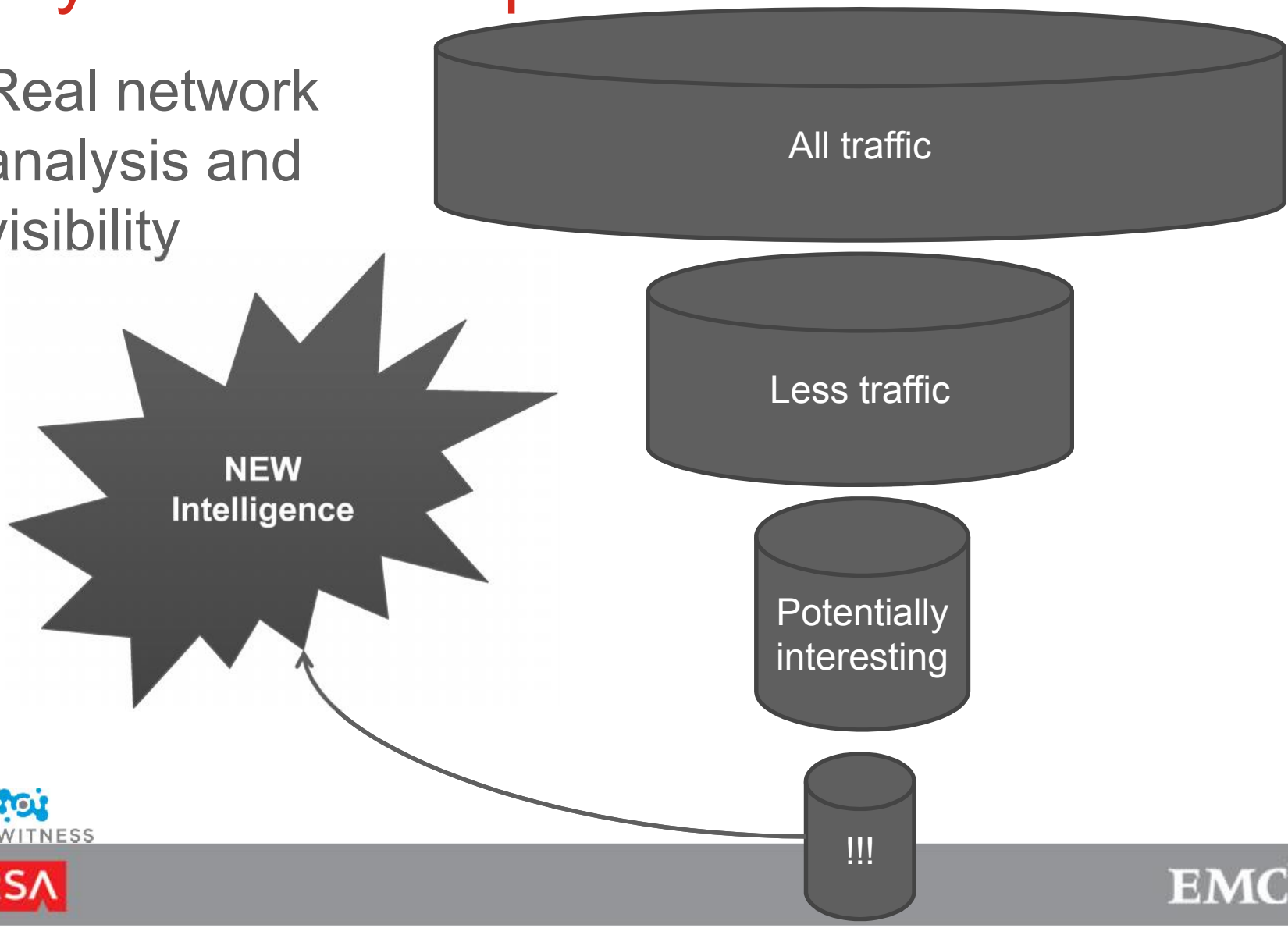
- Real network analysis and visibility



© Copyright 2011 EMC Corporation. All rights reserved.

Why this is so important

- Real network analysis and visibility



© Copyright 2011 EMC Corporation. All rights reserved.

The No B.S. Take-aways

- **The new best practice in incident management is to become information-centric and work with ALL the data.**
- This work can be tedious when you begin to do this – get over it.
- You can't buy a turnkey solution to do it all for you – so stop believing vendor lies.
- You should NOT be repeating the same processes to find the same things.
- New intelligence is used to automate finding those [now] known threats in the future (which is not investigative or detective at that point).
- **You need to think about preventive and detective approaches differently.**

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

A new goal for incident management

Separate “regular” activity and behavior to discover “interesting” activity and behavior - for the *primary* purpose of generating new threat “intelligence.”

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

How to Remove Hay

AKA – new visualization processes and technologies

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Goals

- The idea is to guide your thinking about a problem rather than provide you with a definitive answer
- Form a set of principles and procedures for qualitative and quantitative analysis for dealing with the unknowns of network visibility
- The zen of incident discovery and threat intelligence

© Copyright 2011 EMC Corporation. All rights reserved.

What can you tell us about finding....

- Alureon
- Autoit
- Bredolab
- Buz
- Conficke
-

» F Bean

»

» Piptea

» enos

rm

irut

» Zlob

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Stop focusing on specific families of malware

- If you focus on a specific type of malware, at the very best you will:
  - Be able to detect the specific variant you analyzed, and most likely not detect the thousands of others of the same version of the same family of malware
  - Be doing just as crappy of a job as the IDS space has done for over a decade now
  - WILL DEFEAT THE ENTIRE POINT OF ADVANCED VISUALIZATION: **GENERATING NEW INTEL**

© Copyright 2011 EMC Corporation. All rights reserved.

But WAIT you say?!?

- Don't we want to detect **both known and unknown** malware?!?!
- All that's required to detect known malware is "patterns." Generating patterns is simple. Analyzing patterns is simple. That's why 99.9% of the industry does it (including the new folks making claims about zero days)
- Separate these concepts in your head – once you can figure our how to detect known threats – that should move into your preventive realm

© Copyright 2011 EMC Corporation. All rights reserved.

A new best practice:

- Using “the needle in the haystack” analogy...

World-class threat analysts

remove hay until only needles remain

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Let's start separating some hay…!

- Group Question:
- ***When looking at HTTP sessions, what should you expect to see inside normal sessions?***

- Html
- Images (gif, jpg, etc)
- Other Files (pdfs, docs, exes, etc)
- Client application headers
- Web server headers

© Copyright 2011 EMC Corporation. All rights reserved.

The GET

- Here is a “normal” HTTP header from a “normal” web client

```
GET /Protocols/rfc2616/rfc2616.html HTTP/1.1
Accept: image/jpeg, image/gif, image/pjpeg, application/x-ms-application, application/xaml+xml,
application/x-ms-xbap, */*
Referer: http://www.w3.org/Protocols/rfc2616/rfc2616-sec19.html
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: www.w3.org
Connection: Keep-Alive
```

  - » And from our traffic in question

```
GET /1/helloworld.bin HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.4; Media Center PC
3.0; .NET CLR 1.0.3705; .NET CLR 2.0.50727; InfoPath.2)
Host: 193.219.5.200
Cache-Control: no-cache
```


© Copyright 2011 EMC Corporation. All rights reserved.

The GET

- Here is a “normal” HTTP header from a “normal” web client

```
GET /Protocols/rfc2616/rfc2616.html HTTP/1.1
Accept: image/jpeg, image/gif, image/pjpeg, application/x-ms-application, application/xaml+xml,
application/x-ms-xbap, */*
Referer: http://www.w3.org/Protocols/rfc2616/rfc2616-sec19.html
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: www.w3.org
Connection: Keep-Alive
```

  - And from our traffic in question

```
GET /1/helloworld.bin HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.4; Media Center PC
3.0; .NET CLR 1.0.3705; .NET CLR 2.0.50727; InfoPath.2)
Host: 193.219.5.200
Cache-Control: no-cache
```

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

The GET

- Here is a “normal” HTTP header from a “normal” web client

```
GET /Protocols/rfc2616/rfc2616.html HTTP/1.1
Accept: image/jpeg, image/gif, image/pjpeg, application/x-ms-application, application/xaml+xml,
application/x-ms-xbap, */*
Referer: http://www.w3.org/Protocols/rfc2616/rfc2616-sec19.html
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: www.w3.org
Connection: Keep-Alive
```

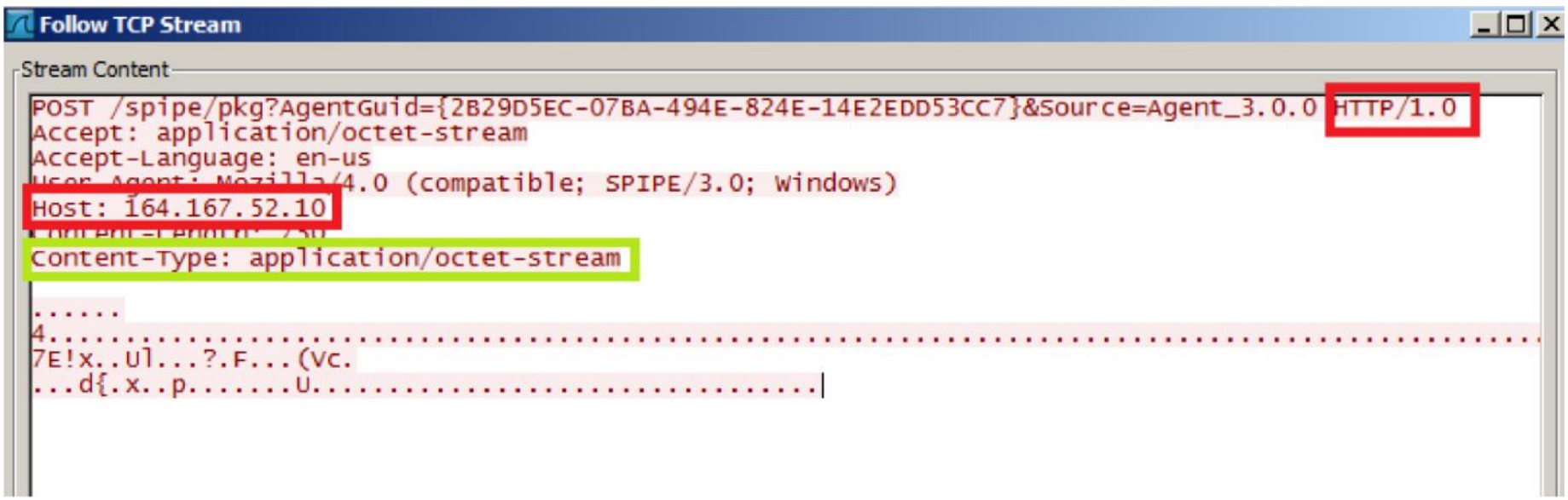
  - » And from our traffic in question

```
GET /1/helloworld.bin HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.4; Media Center PC
3.0; .NET CLR 1.0.3705; .NET CLR 2.0.50727; InfoPath.2)
Host: 193.219.5.200
Cache-Control: no-cache
```


© Copyright 2011 EMC Corporation. All rights reserved.

The POSTs

- Even poorly implemented protocol handlers from legitimate software has less obvious abnormalities



NETWITNESS

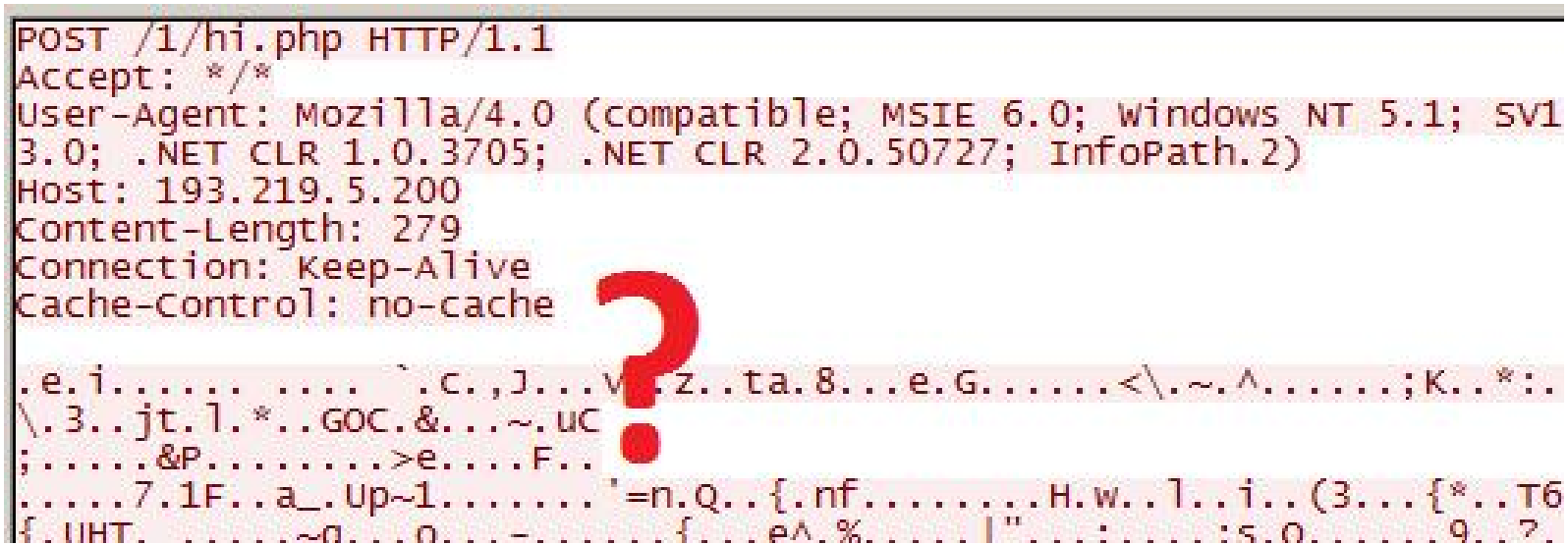
RSA

EMC²

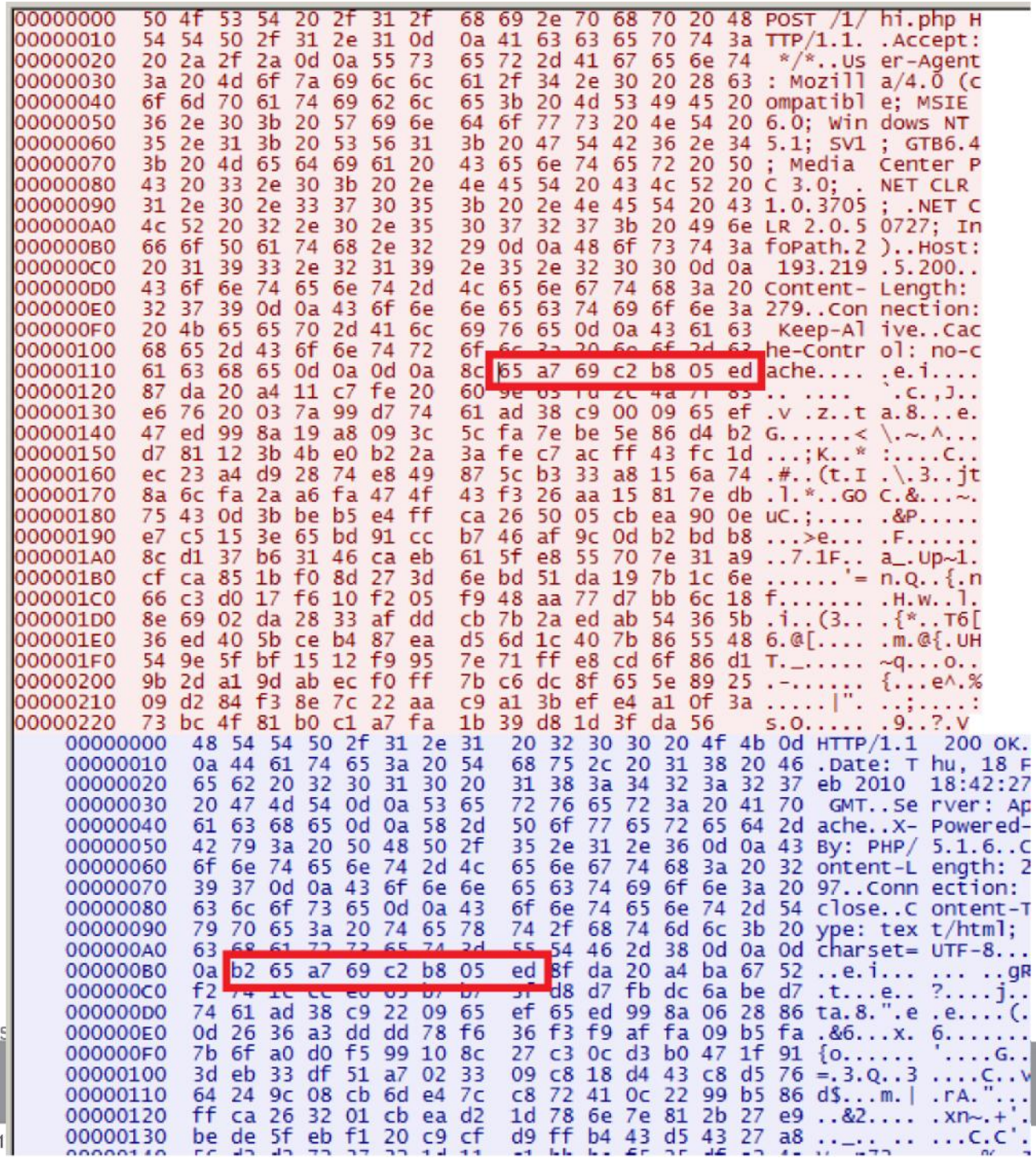
© Copyright 2011 EMC Corporation. All rights reserved.

The POSTs

- A POST without a Content-Type?



© Copyright 2011 EMC Corporation. All rights reserved.



```
00000000  50 4f 53 54 20 2f 31 2f  68 69 2e 70 68 70 20 48  POST /1/ hi.php H
00000010  54 54 50 2f 31 2e 31 0d  0a 41 63 63 65 70 74 3a  TTP/1.1. .Accept:
00000020  20 2a 2f 2a 0d 0a 55 73  65 72 2d 41 67 65 6e 74   */*..Us er-Agent
00000030  3a 20 4d 6f 7a 69 6c 6c  61 2f 34 2e 30 20 28 63  : Mozill a/4.0 (c
00000040  6f 6d 70 61 74 69 62 6c  65 3b 20 4d 53 49 45 20  ompatibl e; MSIE
00000050  36 2e 30 3b 20 57 69 6e  64 6f 77 73 20 4e 54 20  6.0; Win dows NT
00000060  35 2e 31 3b 20 53 56 31  3b 20 47 54 42 36 2e 34  5.1; SV1 ; GTB6.4
00000070  3b 20 4d 65 64 69 61 20  43 65 6e 74 65 72 20 50  ; Media  Center P
00000080  43 20 33 2e 30 3b 20 2e  4e 45 54 20 43 4c 52 20  C 3.0; . NET CLR
00000090  31 2e 30 2e 33 37 30 35  3b 20 2e 4e 45 54 20 43  1.0.3705 ; .NET C
000000A0  4c 52 20 32 2e 30 2e 35  30 37 32 37 3b 20 49 6e  LR 2.0.5 0727; In
000000B0  66 6f 50 61 74 68 2e 32  29 0d 0a 48 6f 73 74 3a  foPath.2 )..Host:
000000C0  20 31 39 33 2e 32 31 39  2e 35 2e 32 30 30 0d 0a   193.219 .5.200..
000000D0  43 6f 6e 74 65 6e 74 2d  4c 65 6e 67 74 68 3a 20  Content- Length:
000000E0  32 37 39 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a  279..Con nection:
000000F0  20 4b 65 65 70 2d 41 6c  69 76 65 0d 0a 43 61 63   Keep-Al ive..Cac
00000100  68 65 2d 43 6f 6e 74 72  6f [illegible]           he-Contr ol: no-c
00000110  61 63 68 65 0d 0a 0d 0a  8c 65 a7 69 c2 b8 05 ed  ache.... .e.i....
00000120  87 da 20 a4 11 c7 fe 20  60 [illegible]            .. .... `.c.,J..
00000130  e6 76 20 03 7a 99 d7 74  61 ad 38 c9 00 09 65 ef  .v .z..t a.8...e.
00000140  47 ed 99 8a 19 a8 09 3c  5c fa 7e be 5e 86 d4 b2  G......< \.~.^...
00000150  d7 81 12 3b 4b e0 b2 2a  3a fe c7 ac ff 43 fc 1d  ...;K..* :....C..
00000160  ec 23 a4 d9 28 74 e8 49  87 5c b3 33 a8 15 6a 74  .#..(t.I .\.3..jt
00000170  8a 6c fa 2a a6 fa 47 4f  43 f3 26 aa 15 81 7e db  .l.*..GO C.&...~.
00000180  75 43 0d 3b be b5 e4 ff  ca 26 50 05 cb ea 90 0e  uC.;.... .&P.....
00000190  e7 c5 15 3e 65 bd 91 cc  b7 46 af 9c 0d b2 bd b8  ...>e... .F......
000001A0  8c d1 37 b6 31 46 ca eb  61 5f e8 55 70 7e 31 a9  ..7.1F.. a_.Up~1.
000001B0  cf ca 85 1b f0 8d 27 3d  6e bd 51 da 19 7b 1c 6e  ......'= n.Q..{.n
000001C0  66 c3 d0 17 f6 10 f2 05  f9 48 aa 77 d7 bb 6c 18  f....... .H.w..l.
000001D0  8e 69 02 da 28 33 af dd  cb 7b 2a ed ab 54 36 5b  .i..(3.. .{*..T6[
000001E0  36 ed 40 5b ce b4 87 ea  d5 6d 1c 40 7b 86 55 48  6.@[.... .m.@{.UH
000001F0  54 9e 5f bf 15 12 f9 95  7e 71 ff e8 cd 6f 86 d1  T._..... ~q...o..
00000200  9b 2d a1 9d ab ec f0 ff  7b c6 dc 8f 65 5e 89 25  .-...... {...e^.%
00000210  09 d2 84 f3 8e 7c 22 aa  c9 a1 3b ef e4 a1 0f 3a  .....|". ..;....:
00000220  73 bc 4f 81 b0 c1 a7 fa  1b 39 d8 1d 3f da 56     s.O..... .9..?.V

    00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d  HTTP/1.1  200 OK.
    00000010  0a 44 61 74 65 3a 20 54  68 75 2c 20 31 38 20 46  .Date: T hu, 18 F
    00000020  65 62 20 32 30 31 30 20  31 38 3a 34 32 3a 32 37  eb 2010  18:42:27
    00000030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70   GMT..Se rver: Ap
    00000040  61 63 68 65 0d 0a 58 2d  50 6f 77 65 72 65 64 2d  ache..X- Powered-
    00000050  42 79 3a 20 50 48 50 2f  35 2e 31 2e 36 0d 0a 43  By: PHP/ 5.1.6..C
    00000060  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 32  ontent-L ength: 2
    00000070  39 37 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20  97..Conn ection:
    00000080  63 6c 6f 73 65 0d 0a 43  6f 6e 74 65 6e 74 2d 54  close..C ontent-T
    00000090  79 70 65 3a 20 74 65 78  74 2f 68 74 6d 6c 3b 20  ype: tex t/html;
    000000A0  63 68 61 72 73 65 74 3d  55 54 46 2d 38 0d 0a 0d  charset= UTF-8...
    000000B0  0a b2 65 a7 69 c2 b8 05  ed 8f da 20 a4 ba 67 52  ..e.i... ... ..gR
    000000C0  f2 [illegible]                                   ?....j..
    000000D0  74 61 ad 38 c9 22 09 65  ef 65 ed 99 8a 06 28 86  ta.8.".e .e....(.
    000000E0  0d 26 36 a3 dd dd 78 f6  36 f3 f9 af fa 09 b5 fa  .&6...x. 6.......
    000000F0  7b 6f a0 d0 f5 99 10 8c  27 c3 0c d3 b0 47 1f 91  {o...... '....G..
    00000100  3d eb 33 df 51 a7 02 33  09 c8 18 d4 43 c8 d5 76  =.3.Q..3 ....C..v
    00000110  64 24 9c 08 cb 6d e4 7c  c8 72 41 0c 22 99 b5 86  d$...m.| .rA."...
    00000120  ff ca 26 32 01 cb ea d2  1d 78 6e 7e 81 2b 27 e9  ..&2.... .xn~.+'.
    00000130  be de 5f eb f1 20 c9 cf  d9 ff b4 43 d5 43 27 a8  .._.. .. ...C.C'.
```

NETWITNESS
RSA
© Copyright 201
EMC²

At this point do we know this session is bad juju?

- We know because of all the abnormalities in the HTTP headers, the traffic appears to be crafted and coming from a “not normal” web client.
- We know there’s a pattern in the data exchange taking place that is typical of poorly implemented structured/encrypted information exchange schemes
- But... This only means it’s suspicious. We don’t KNOW it’s bad.

© Copyright 2011 EMC Corporation. All rights reserved.

Summary - Application Protocol Analysis

- "Normal" in most cases means "most sessions." "Abnormal" in most cases means outliers.
- Good outliers are not found though random searches, but rather intelligent combinations in logic, such as:
  - If looking at protocol X, I should see content Y
  - If looking at port A, I should see protocol B (and vise versa)
  - If looking at protocol Z, I should never see A, B, or C (we'll look at this next.)
- We just looked at web here, but the same logic applies to ALL other protocols.
- The more you know about the most common protocols, the more malware you'll be capable of finding! (They're good at hiding on endpoints – not so much on the network.)

© Copyright 2011 EMC Corporation. All rights reserved.

Examining the most obvious “needles” in the network haystack

The lost art of learning what the masses already know – information centricity through community

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Analysis goes beyond packets

- A single network session can contain 100's of points for analysis, but... Sometimes that's not enough to paint a good picture about the activity!
- Many times, trying to research the "suspicious traits" themselves consumes FAR more time than researching the more obvious traits (the ones most often overlooked by analysts too eager to play in the weeds)

© Copyright 2011 EMC Corporation. All rights reserved.

GET /images/update.jpg HTTP/1.1

Accept: */*

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)

Host: bataansurvivor.com

Cache-Control: no-cache

© Copyright 2011 EMC Corporation. All rights reserved.

Back to Bataan
A Survivor's Story

Written by Rick Peterson

Jump to: Home GO

Home
Foreword
Introduction

The Road to Bataan
The Bataan Death March
The San Fernando Train Ride
Camp O'Donnell
Clark Field Concentration Camp
Bilibid Prison
The Hell Ships
Japan
The Nomachi Express
Camp Nomachi

Home

"Courage is a quality God has seen fit to dispense with utmost care. The men of Bataan were His chosen favorites."

Major General Edward P. King, Jr., USA
Commanding General, Luzon Forces, 1942

This narrative is dedicated to my beloved wife Jane and to all United States of America military personnel who served in World War II on Bataan and Corregidor and endured the rigors of captivity inflicted on us by the soldiers of the Japanese Imperial Army.

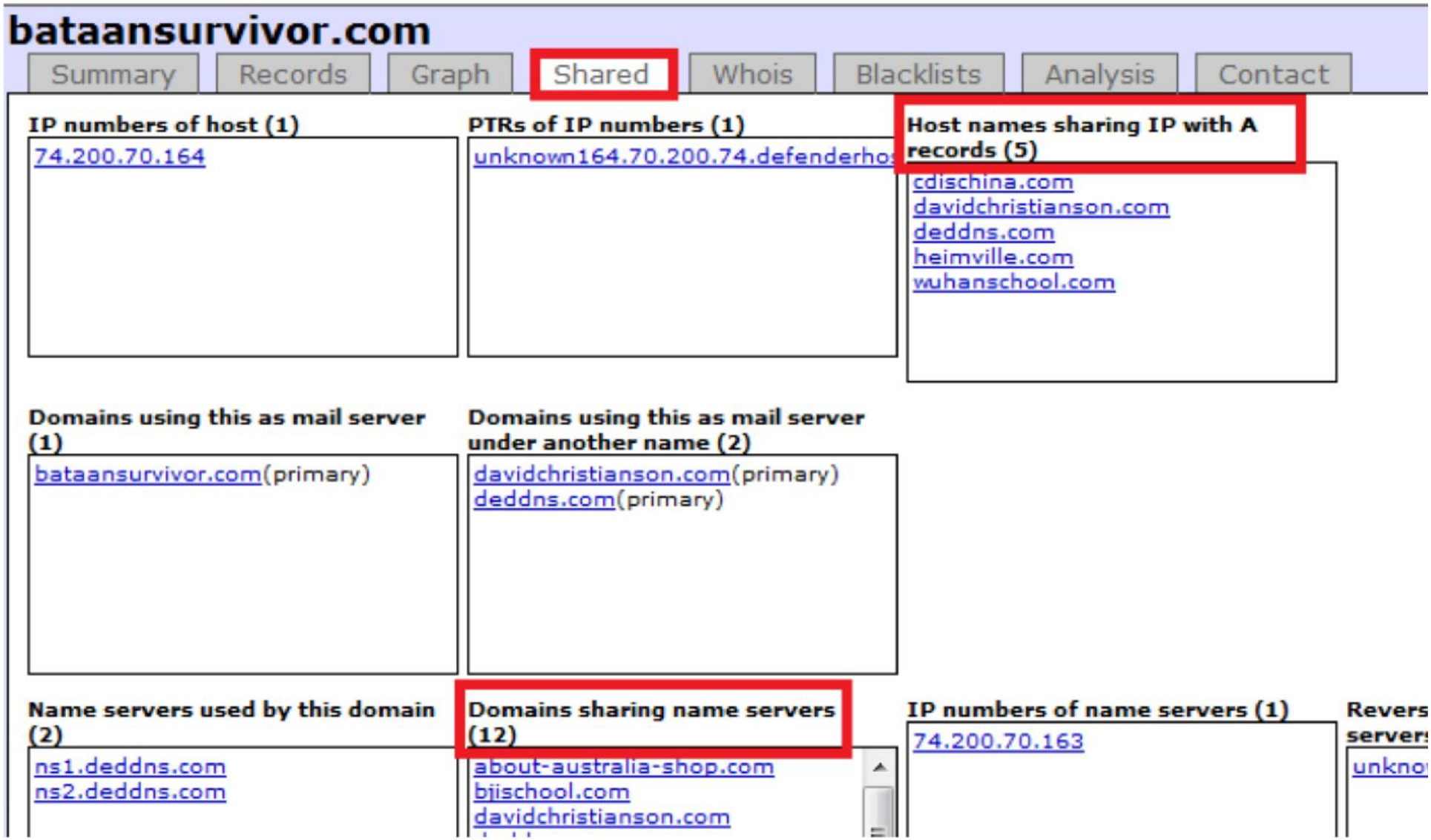
Alf R. Larson

© C

Robtex – DNS “Swiss army knife”

© Copyright 2011 EMC Corporation. All rights reserved.

Robtex – DNS “Swiss army knife”

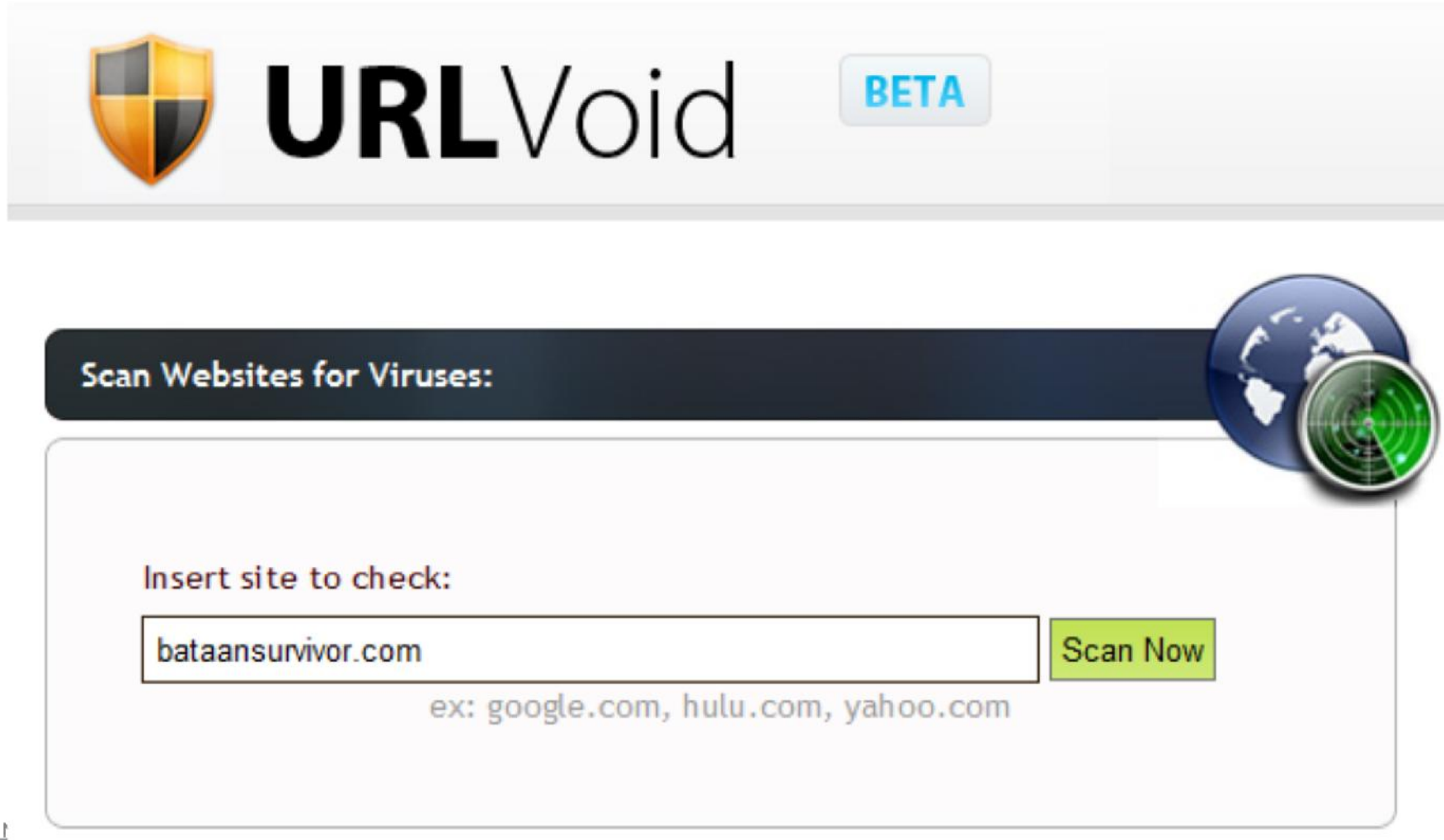


Malware Domain Lists

- AMaDa
- BrowserDefender
- Finjan
- Google Diagnostic
- hpHosts
- Malware Patrol
- MalwareDomainList
- MyWOT
- Norton SafeWeb
- ParetoLogic URL Clearing House
- PhishTank
- SURBL
- Threat Log
- TrendMicro Web Reputation
- URIBL
- Web Security Guard
- ZeuS Tracker

© Copyright 2011 EMC Corporation. All rights reserved.

URL Void



© Copyright 2011 EMC Corporation. All rights reserved.

URL Void

Report	2010-07-28 04:42:28 (GMT 1)
Website	**bataansurvivor.com**
Domain Hash	8c711caca70395acd5bb973b3dfae2be
IP Address	74.200.70.164 [SCAN]
IP Hostname	unknown164.70.200.74.defenderhosting.com
IP Country	US (United States)
AS Number	14383
AS Name	VCS-AS - Virtacore Systems Inc
Detections	5 / 17 (29 %)
Status	DANGEROUS

© Copyright 2011 EMC Corporation. All rights reserved.

URL Void

Scanning site with:	AMaDa	DETECTED
Scanning site with:	BrowserDefender	CLEAN
Scanning site with:	Finjan	CLEAN
Scanning site with:	Google Diagnostic	CLEAN
Scanning site with:	hpHosts	UNRATED
Scanning site with:	Malware Patrol	DETECTED
Scanning site with:	MalwareDomainList	DETECTED
Scanning site with:	MyWOT	CLEAN
Scanning site with:	Norton SafeWeb	CLEAN
Scanning site with:	ParetoLogic URL Clearing House	CLEAN
Scanning site with:	PhishTank	CLEAN
Scanning site with:	SURBL	CLEAN
Scanning site with:	Threat Log	CLEAN
Scanning site with:	TrendMicro Web Reputation	DETECTED
Scanning site with:	URIBL	CLEAN
Scanning site with:	Web Security Guard	UNRATED
Scanning site with:	ZeuS Tracker	DETECTED

© Copyright 2011 EMC Co

What does adding up all that info tell us?

- **It appears a legitimate site/domain was likely hacked and being used for C&C activity (based on the crafted appearance of the HTTP header that triggered our initial suspicion)**

© Copyright 2011 EMC Corporation. All rights reserved.

A smoking gun is nice. A smoking 50 Cal is WAY better

Bored of protocol anomalies? Then payload anomalies is just what you need...

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Goals

- Detect malware without a priori knowledge about it
- Integrate into existing workflow
- Low False Positive and low False Negative rate
- Take static analysis as far as possible without sandboxes, virtual machines, and similar runtime analysis technologies
- (Use sandboxing too, but don't over emphasize it…)

© Copyright 2011 EMC Corporation. All rights reserved.

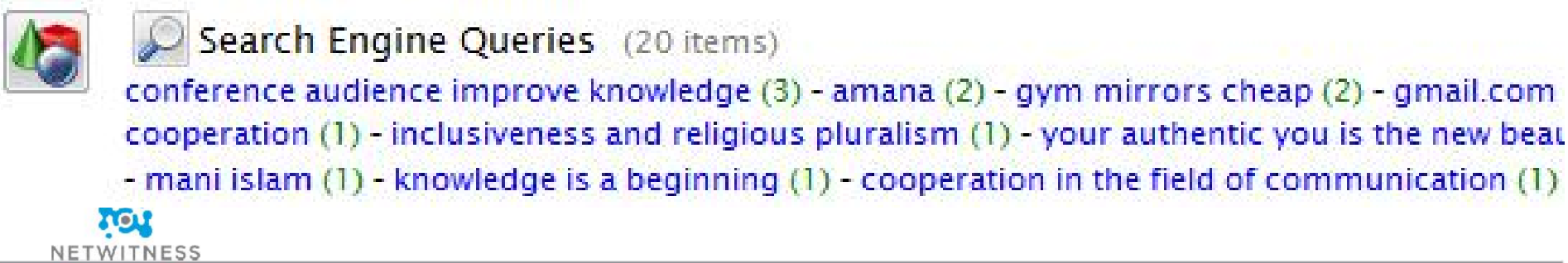
Network-Based Analysis Constraints

- Implementation must be FAST
  - Can only perform simple operations such as byte shifts and byte comparisons.
- Must compensate for highly “random” nature of traffic
  - Must validate that an array of bytes at any position in a stream of data

© Copyright 2011 EMC Corporation. All rights reserved.

Fully implemented as a *FlexParser*

- FlexParser
  - A syntax within NetWitness allowing you to tag sessions with new types of “meta” based on very granular examination and testing of the data contained within those sessions.



NETWITNESS

RSA EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Who cares about all this, you propeller-wearing nerd?!

- "...TSPY_ZBOT.BYZ also uses techniques designed to avoid automatic heuristics-based detection."
  - AV company blog October 13, 2010

Group	Rule	Notes
General Tests	CompressionTest	PE compression analysis found compressed sections
General Tests	Checksum	PE failed checksum validation.
Meta Strings	NoMetaFound	PE has been stripped of informational meta strings
Imports (Iteratively)	exact_match_test	Suspicious import fingerprint encountered. [callnexthookex imported from user32.dll]
Imports (Iteratively)	exact_match_test	Suspicious import fingerprint encountered. [createmutexa imported from kernel32.dll]
General Tests	FileSizeTest	This PE is abnormally small. Its size is: [178176 bytes]
Imports (Iteratively)	exact_match_test	Watchlist import fingerprint encountered. [changeserviceconfigw imported from advapi32.dll]
Imports (Iteratively)	exact_match_test	Watchlist import fingerprint encountered. [startservicew imported from advapi32.dll]
Imports (Iteratively)	exact_match_test	Watchlist import fingerprint encountered. [unhookwindowshookex imported from user32.dll]

© Copyright 2011 EMC Corporation. All rights reserved.

Our Challenge!

- Accurately identify when network sessions contain executables!

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

PE Identification on the network

4D 5A	MZ
COM, DLL, DRV, EXE, PIF, QTS, QTX, SYS	Windows/DOS executable file

- Ok for hosts, NOT for network!
- Chance of false positives: 1 in ~8k, or about 1 false positive in every 8 packets!

© Copyright 2011 EMC Corporation. All rights reserved.

PE ID on the Network, Snort/IDS Style

- sid:11192
- content:"application/octet-stream"; nocase; pcre:"/^Content-Type\x3a[\x20\x09]+application\/octet-stream/smi"; pcre:"/(\r?\n){2}MZ/sm";

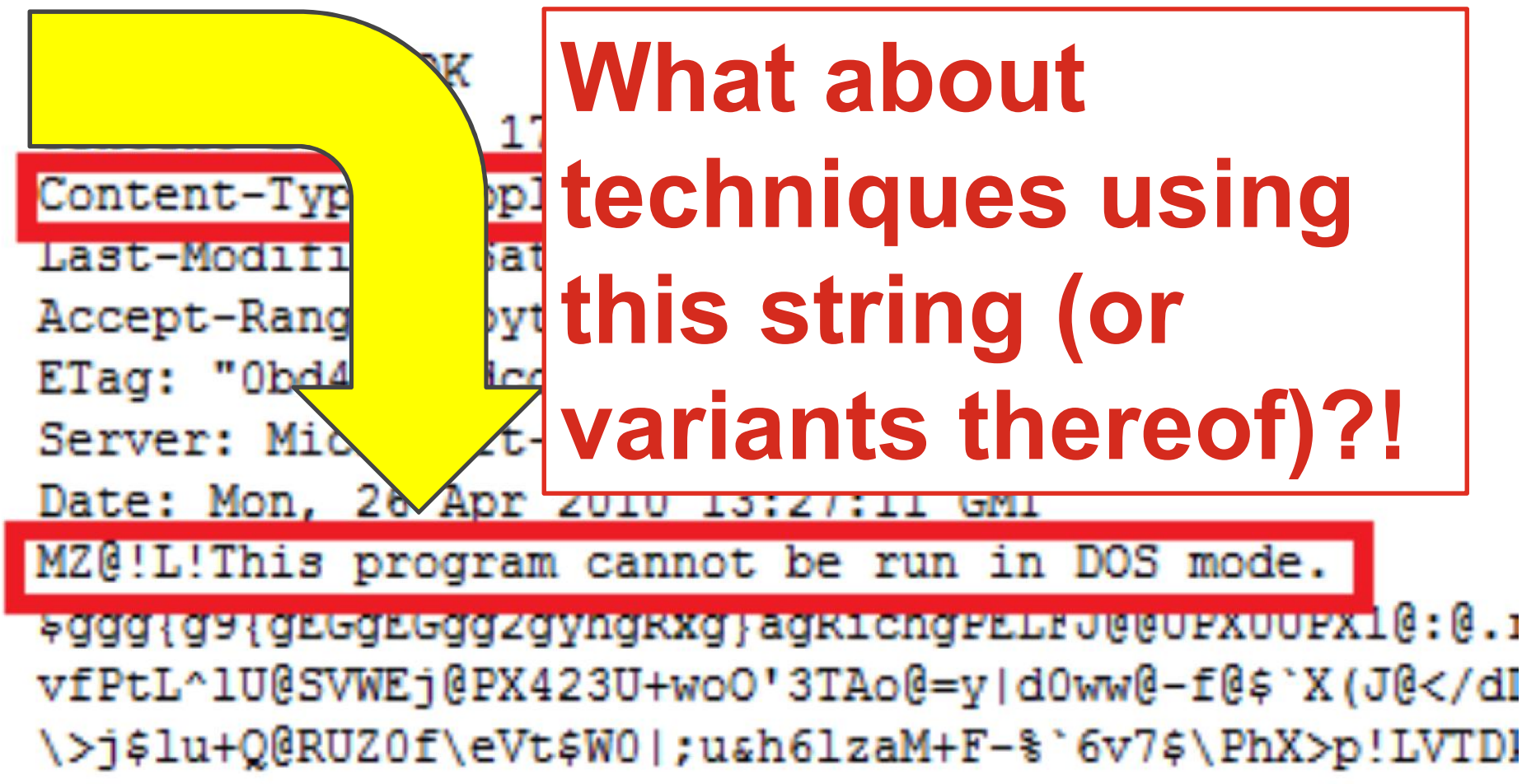
NETWITNESS

RSA

EMC²

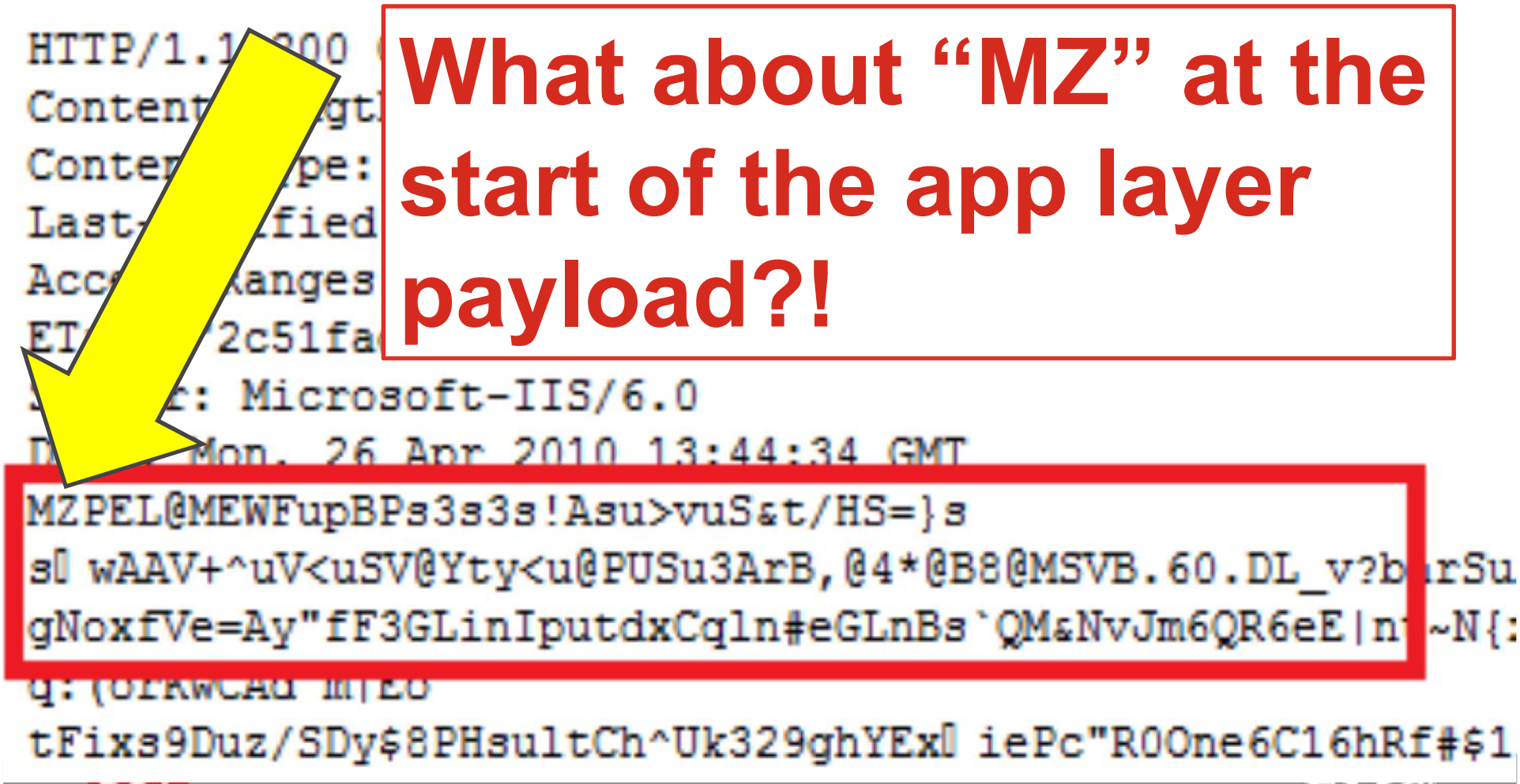
© Copyright 2011 EMC Corporation. All rights reserved.

Problem with static approaches…



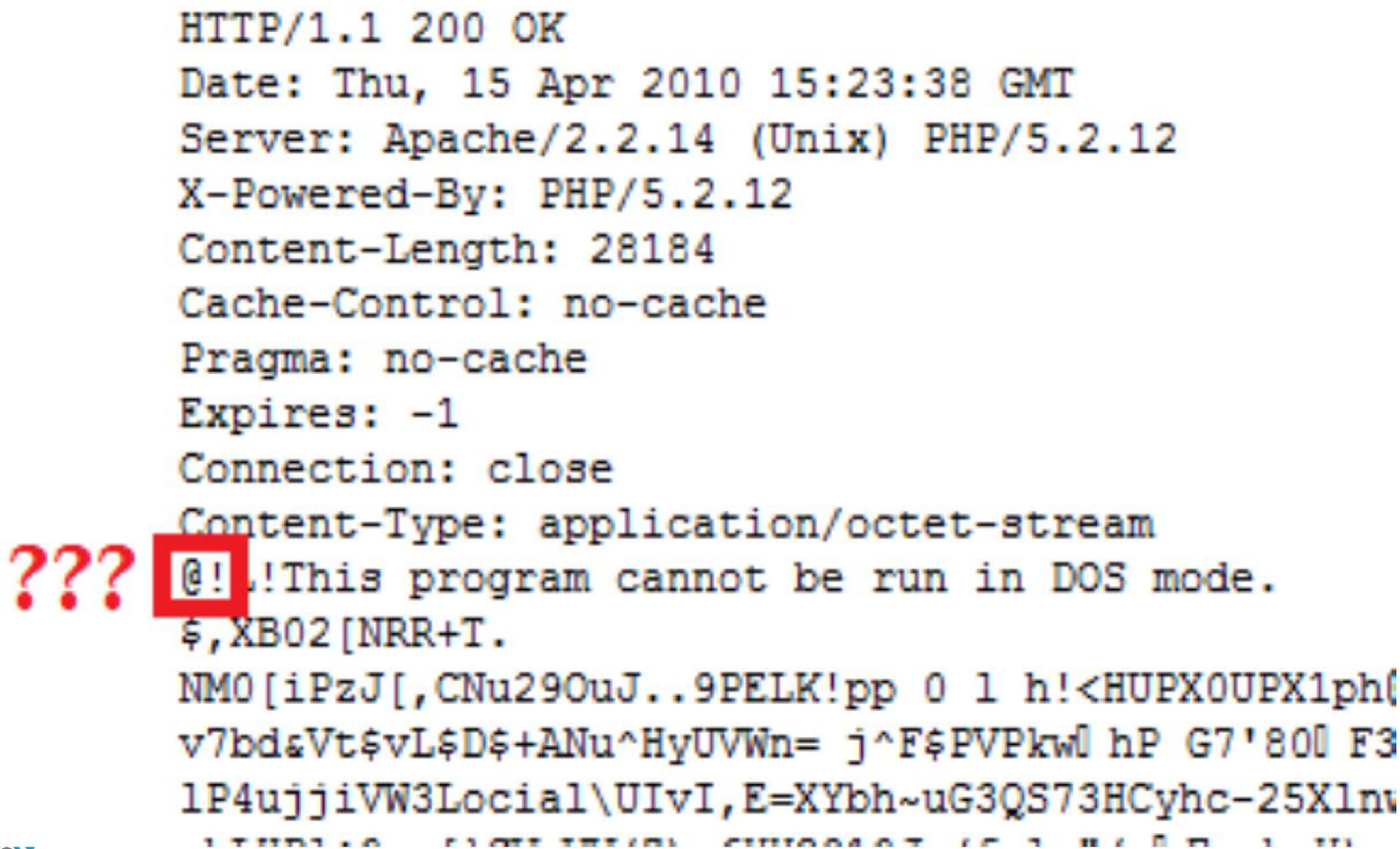
© Copyright 2011 EMC Corporation. All rights reserved.

Need to think in a data-centric way about each problem…



© Copyright 2011 EMC Corporation. All rights reserved.

Is no “MZ” that common?! Well…



NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

```
HTTP/1.1 200 OK
Content-Type: image/gif
Last-Modified: Sat, 11 Sep 2010 20:13:26 GMT
Accept-Ranges: bytes
ETag: "a4b29cbed51cb1:0"
Server: Microsoft-IIS/7.0
X-Powered-By: ASP.NET
Date: Sat, 11 Sep 2010 20:14:04 GMT
Content-Length: 55892
GIF87aqqquuuQQ}}  ee00eee   eA4<e0e000000000000e0e0ee0e00e0eeeee0eeeeee0eee0ee0e
ee0e0ee0eeeeee0e0ee0e0000e00eeeee0e,
H*\#JH3j '((S\0cp~4s@?l+NJXj"g^9;hlRA$<ZUS2=[pJXB"[W0_ ;0#G 3gF2"JBm6\:FijOMo'}|9
```

~ SNIP ~

```
{X8^6/L~{oOOk(h&6^QD(Vhfvug(C",(4h#+.<@)DiH&L6PFN/hXfm`)T]ih'<p)tix|*j&6YVjfv*j*;
MZE ELFSG!DT@p`pY}%AaUs3s3sAsu:SuS$t-HS;Cs
s wAAV+^^PS@xucPUS3Aru KERNEL32.dll @}Xp`0 SERVERr 8P@2$H"DQ%$CHOc"qD$H"D@R);$KH[q
"DS$Hq9"EDO[ i%'>E(].dl@user3R2;a9vpirecy^ N-N81tzBo9  qA2 @54E}\r1avyexM(
}t\.mpAUTORNIF:\ %cshe)(vpHo+xuCqmand+1!(&X)a opnDfa}uqt(1
```

Fingerprinting PE's

- We can use the previous diagrams to come up with a *simple* algorithm for fingerprinting PE's (*that start with "MZ"*).
  - We can fingerprint PE's attempting to evade detection by modifying the first few bytes of the file (no "MZ" fingerprint), but because of time constraints, that will not be discussed here.

© Copyright 2011 EMC Corporation. All rights reserved.

Pseudo example

IF pattern found == “MZ”

SHIFT 59 bytes forward

READ dword = *offset1*

SHIFT *offset1* from start of “MZ”

IF current offset pattern == “PE”

SHIFT 23 bytes

IF current offset pattern ==

0x010B OR 0x020B

BOOL isPE == true

© Copyright 2011 EMC Corporation. All rights reserved.

NetWitness (and ***Freeware)***: FlexParser Example

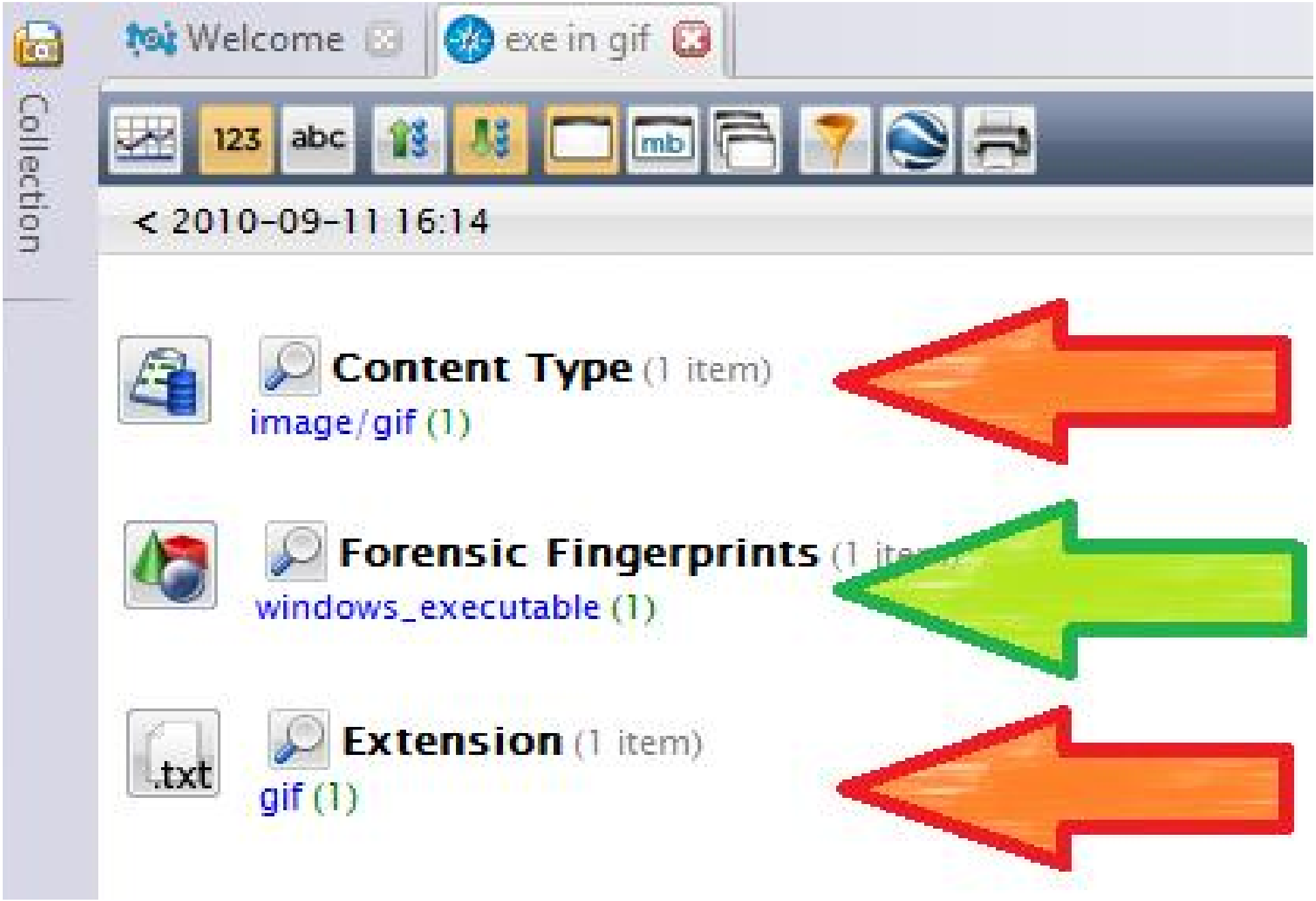
```
<match name="mz">
    <move direction="forward" value="58">
      <read length="4" name="pe_header_offset" endianess="little">
        <move direction="reverse" value="62">
          <move direction="forward" value="$pe_header_offset">
            <find length="2" name="num_temp_offset" value="PE">
```

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.


Collection
Welcome
exe in gif
123
abc
< 2010-09-11 16:14
Content Type (1 item)
image/gif (1)
Forensic Fingerprints (1 item)
windows_executable (1)
.txt
Extension (1 item)
gif (1)

Putting it all together

Forensic Fingerprints (10 items)

windows_executable (75) - windows_dll (28) - windows_installer (2) - office_95-2003 (2) - lnk (2) - javascript (2) -

Extension (20 items)

php (9) - auth (9) - z (6) - txt (4) - gif (4) - wat (2) - msi (2) - js (2) - htm (2) - bin (2) -

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

Putting it all together

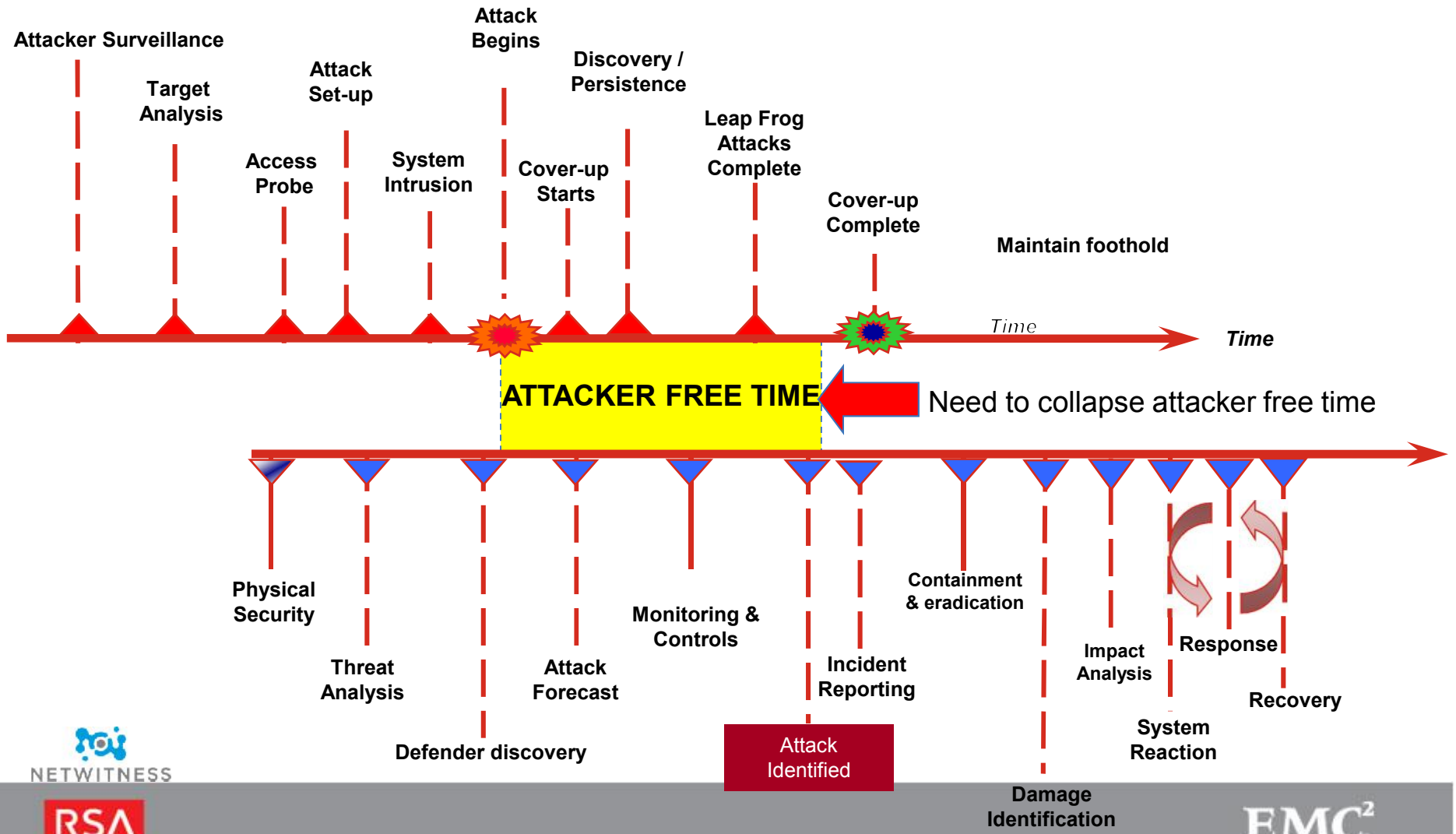
NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.

New Security Concept: "OFFENSE IN DEPTH"



Source: NERC HILF Report, June 2010 (http://www.nerc.com/files/HILF.pdf)

© Copyright 2011 EMC Corporation. All rights reserved.

Some initial conclusions

- Prevention and detection are different
- Dynamic security means information centric and a focus on threat intelligence (among other things)
- You need to capture and analyze everything
- We are just scratching the surface on what can be done – but you have to start doing it
- It's not easy, but it gets easier, so stop whining and get busy

© Copyright 2011 EMC Corporation. All rights reserved.

THANK YOU

eddie.schwartz@rsa.com
Twitter: @eddieschwartz
http://www.rsa.com

NETWITNESS

RSA

EMC²

© Copyright 2011 EMC Corporation. All rights reserved.