



BlindElephant: Web Application Fingerprinting With Static Files

Patrick Thomas

7/28/10



Outline

- Web Apps & Security
- Intro to Fingerprinting
- Static File Approach
- Observations From A Net Survey

- Q & A

Well-Known Web Applications

- Every conceivable use...
- Content Management/Blogging
- Forums
- Email
- E-Commerce
- DB Admin
- Backup and File Storage Admin
- Device/System/VM Admin
- Version Control UI
- Intranet/Collaboration

Well-Known Web Applications



Theory of Fingerprinting

- Find some characteristic(s) that is...
 - ...always the same for a particular individual (implementation/version/person)
 - ...always different from other members of the population
- If there's one piece of info that fulfills both, great
 - If not, take several that pin it down
 - Tons of [interesting reading in information theory and entropy](#)
- OS & HTTP Server Fingerprinting: Lots of protocol-aware checks that rely on subtle differences in implementation

Existing Fingerprinting Approaches

- Labor intensive to add signatures
 - Manually locate version in files or build regexes for headers
- Decent hardening pretty much nukes them
 - Built-in options to remove identifiers (eg, meta generator)
 - Remove standard files
- Easy to lie to

Fingerprinters like this:

- Sedusa (in nmap), Wappalyzer, BackendInfo, Plecost, etc, etc...

More Advanced Tools

- Typically improve in one area
 - Resistant to hardening
 - Less labor intensive
- Have their own downsides
 - Less specific results
 - Some request massive amounts of data (> 20 megs!)
 - Some are less generic (Plecost = Wordpress Only)

Fingerprinters like this:

- [Sucuri](#), WAFP, WhatWeb, BackEndInfo (sortof),
-

Goals for a (WebApp) Fingerprinter

- Very Generic
- Fast
- Low resource usage
- Accurate (Low FP/FN)
- Resistant to hardening/banner removal
- Super easy to support new versions/apps

The Blind Men and the Elephant



Collect and Eliminate Possibilities



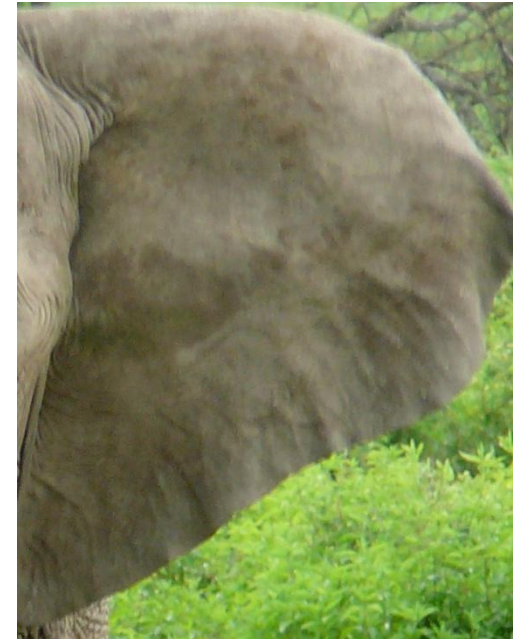
**Tree or
Elephant**

**Spear or
Elephant**



**Vine or
Elephant**

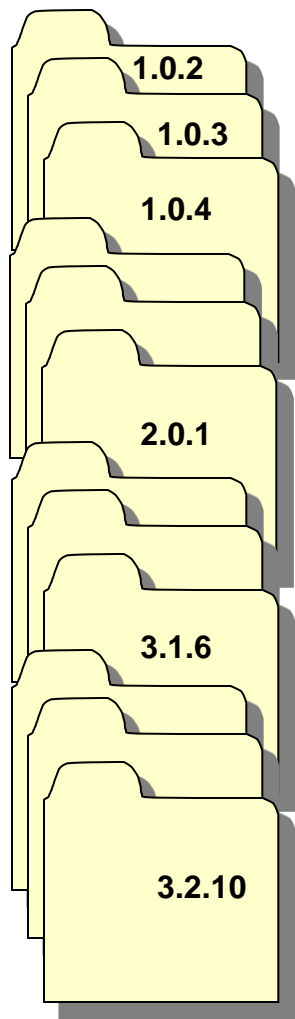
**Fan or
Elephant**



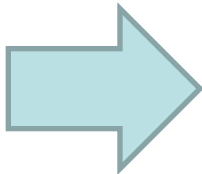
Intersect the Possibilities and...



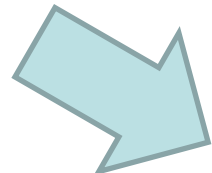
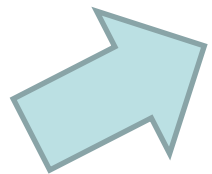
Preparing the Data



Web App Versions
(eg, Joomla-*.zip)



What files appear unchanged in multiple versions?



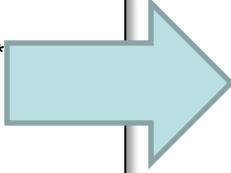
What versions will a path give me info on?



If I want to confirm or rule out a version/versions, what's a path that will do that?

Directory Tree

wordpress-0.71-gold/*/*.*
wordpress-0.72-beta-1/*/*.*
wordpress-0.72-RC1/*/*.*
wordpress-1.0.1-miles/*/*.*
wordpress-1.0.1-RC1/*/*.*
wordpress-1.0.2/*/*.*
wordpress-1.0.2-blakey/*/*.*
wordpress-1.0-platinum/*/*.*
wordpress-1.0-RC1/*/*.*
wordpress-1.2.1/*/*.*
wordpress-1.2.2/*/*.*
wordpress-1.2-beta/*/*.*
wordpress-1.2-delta/*/*.*
wordpress-1.2-mingus/*/*.*
wordpress-1.2-RC1/*/*.*
wordpress-1.2-RC2/*/*.*
...
wordpress-2.9/*/*.*
wordpress-2.9.1/*/*.*
wordpress-2.9.1-beta1/*/*.*
wordpress-2.9.1-beta1-IIS/*/*.*
wordpress-2.9.1-IIS/*/*.*
wordpress-2.9.1-RC1/*/*.*
wordpress-2.9.1-RC1-IIS/*/*.*
wordpress-2.9-beta-1/*/*.*
wordpress-2.9-beta-1-IIS/*/*.*
wordpress-2.9-beta-2/*/*.*
wordpress-2.9-beta-2-IIS/*/*.*
wordpress-2.9-IIS/*/*.*
wordpress-2.9-RC1/*/*.*
wordpress-2.9-RC1-IIS/*/*.*
wordpress-1.5-strayhorn/*/*.*
wordpress-2.0.7-RC2/*/*.*
wordpress-2.2.1/*/*.*
wordpress-2.5.1/*/*.*
...



HashesTable

f8fc944a02d28f61dc4cf719aa1194ce
('2.0.9', 'install/schemas/postgres_schema.sql', 'f8fc944a02d28f61dc4cf719aa1194ce')
('2.0.7', 'install/schemas/postgres_schema.sql', 'f8fc944a02d28f61dc4cf719aa1194ce')
('2.0.13', 'install/schemas/postgres_schema.sql', 'f8fc944a02d28f61dc4cf719aa1194ce')
('2.0.5', 'install/schemas/postgres_schema.sql', 'f8fc944a02d28f61dc4cf719aa1194ce')
('2.0.14', 'install/schemas/postgres_schema.sql', 'f8fc944a02d28f61dc4cf719aa1194ce')
('2.0.12', 'install/schemas/postgres_schema.sql', 'f8fc944a02d28f61dc4cf719aa1194ce')
('2.0.6', 'install/schemas/postgres_schema.sql', 'f8fc944a02d28f61dc4cf719aa1194ce')
('2.0.11', 'install/schemas/postgres_schema.sql', 'f8fc944a02d28f61dc4cf719aa1194ce')

7be360f53320de4bc9335738e8d02b20
('3.0.6-RC1', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.6', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.2', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.4', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.6-RC3', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.4-RC1', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.3', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.5', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.5-RC1', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.6-RC2', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')
('3.0.6-RC4', 'styles/subsilver2/template/index.htm', '7be360f53320de4bc9335738e8d02b20')

bdb4046baa012e90a01602199e60054f
('3.0.6-RC1', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.6', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.2', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.4', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.6-RC3', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.4-RC1', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.3', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.5', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('2.2b', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.5-RC1', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.6-RC2', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')
('3.0.6-RC4', 'adm/images/cellpic3.gif', 'bdb4046baa012e90a01602199e60054f')

HashTable

f8fc944a02d28f61dc4cf719aa1194ce	
('2.0.9', ..., 'f8fc944a02d28f61dc4cf719aa1194ce')	
('2.0.7', ..., 'f8fc944a02d28f61dc4cf719aa1194ce')	
('2.0.13', ..., 'f8fc944a02d28f61dc4cf719aa1194ce')	
('2.0.5', ..., 'f8fc944a02d28f61dc4cf719aa1194ce')	
('2.0.14', ..., 'f8fc944a02d28f61dc4cf719aa1194ce')	
('2.0.12', ..., 'f8fc944a02d28f61dc4cf719aa1194ce')	
Hash	94ce')
Version → File	194ce')
Version → File	38e8d02b20')
Version → File	d02b20')
Version → File	d02b20')
Version → File	d02b20')
Hash	38e8d02b20')
Version → File	38e8d02b20')
Version → File	d02b20')
Version → File	d02b20')
Version → File	38e8d02b20')
Version → File	38e8d02b20')
Version → File	d02b20')
Version → File	d02b20')
Version → File	38e8d02b20')
Version → File	38e8d02b20')
Version → File	38e8d02b20')

PathsTable

/templ...	
740	File
fc93	Hash → Version
7ec	Hash → Version
264	Hash → Version
/install	
b1fc	
10d	
112	File
8db	
560	Hash → Version
ad0	Hash → Version
590	Hash → Version
89e	Hash → Version
e06	
ce2	
efb00c11712011b0e0cc704ea10225394 [3.0.3]	
045634305e36af4fea75f3a95c415f49 [3.0.6-RC4]	

VersionsTable

bdb4046baa012e90a01602199e60054f	
('3.0.6-RC1', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.6', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.2', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.4', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.6-RC3', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.4-RC1', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.3', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.5', ..., 'bdb4046baa012e90a01602199e60054f')	
('2.2b', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.5-RC1', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.6-RC2', ..., 'bdb4046baa012e90a01602199e60054f')	
('3.0.6-RC4', ..., 'bdb4046baa012e90a01602199e60054f')	

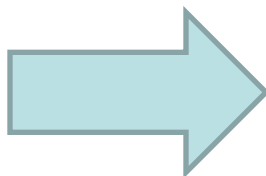
3.0.3,3.0.4,3.0.5	Version, Version, Version	5db...
('/styles/prosi	File → Hash	84bf4...
('/styles/subs	File → Hash	622')
('/adm/style/e	File → Hash	5aa6d..
('/styles/subs	File → Hash	2b8...
('/styles/prosi	File → Hash	8f379...
....		
2.0.20,2.0.21	Version	
('/language/la	File → Hash	7c68...
('/templates/s	File → Hash	
('/templates/s	File → Hash	850d...
('/language/la	File → Hash	596ad...
('/install/schemas/mssql_schema.sql', '045c0fcfaa4f89d771b07b66a74....		
('/contrib/README.html', '61f46292c72f73935bcc2b74403d8b74')		

How Many Files?

Wordpress	~80k files in 151 versions
phpBB	~17k files in 32 versions
MediaWiki	~56k files in 59 versions
Joomla	~83k files in 24 versions
MovableType	~140k files in 57 versions
Drupal	~30k files in 102 versions
... and many more	
Wordpress Plugins	~17k files in 358 versions
Drupal Plugins	~76K files in 983 versions

Fingerprinting

Best Candidates to Identify the Version

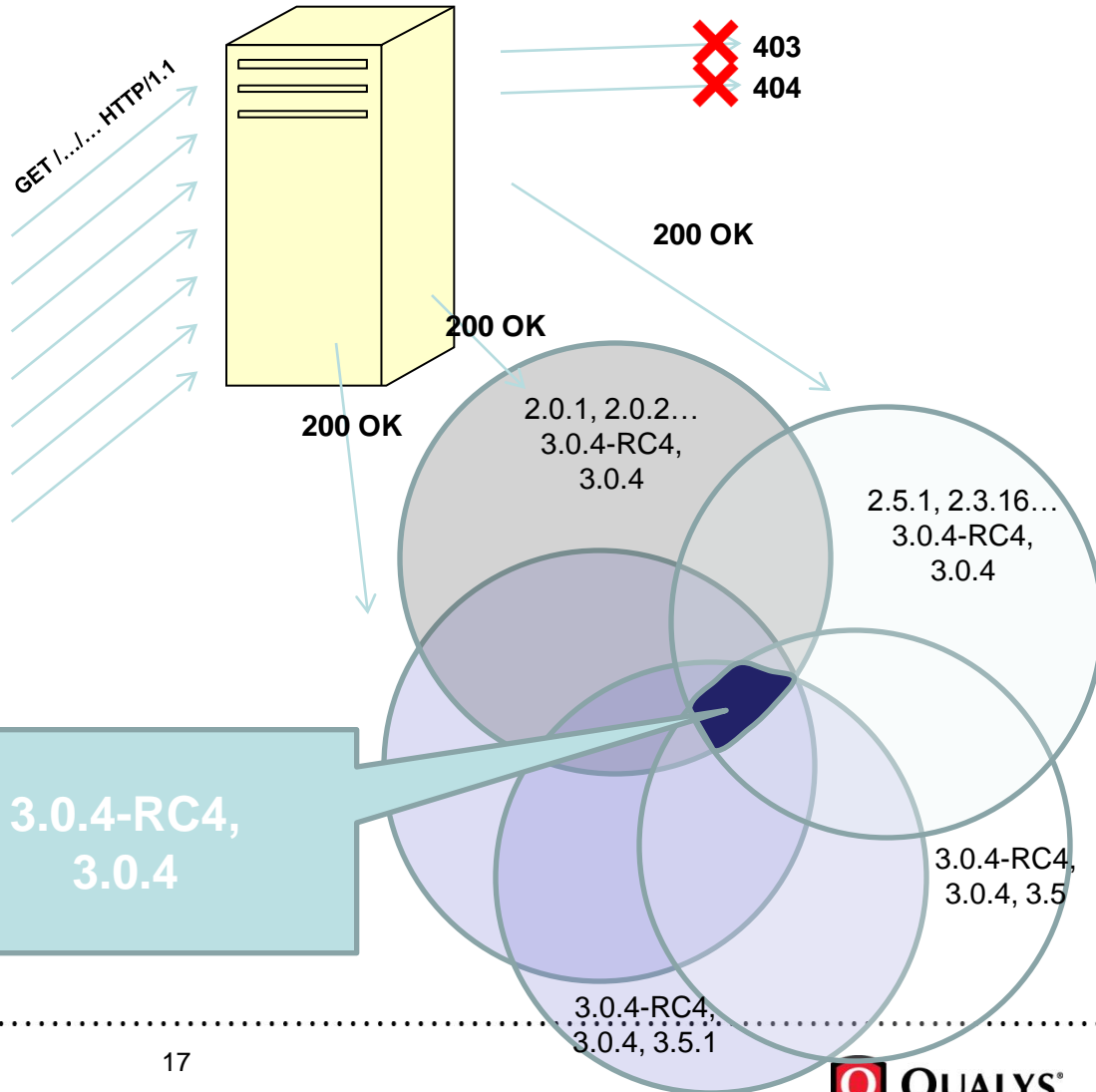


'/htaccess.txt', 14 hashes/31 versions, fitness=15.0
'/language/en-GB/en-GB.ini', 14 hashes/20 versions, fitness=14.64
'/language/en-GB/en-GB.com_content.ini', 13 hashes/20 versions, fitness=13.64
'/configuration.php-dist', 10 hashes/28 versions, fitness=10.90
'/includes/js/joomla.javascript.js', 8 hashes/28 versions, fitness=8.90
'/media/system/js/validate.js', 8 hashes/20 versions, fitness=8.64
'/media/system/js/caption.js', 8 hashes/20 versions, fitness=8.64
'/language/en-GB/en-GB.mod_feed.ini', 8 hashes/20 versions, fitness=8.64
'/media/system/js/openid.js', 8 hashes/20 versions, fitness=8.64
'/language/en-GB/en-GB.com_contact.ini', 8 hashes/20 versions, fitness=8.64
'/language/en-GB/en-GB.mod_breadcrumbs.ini', 7 hashes/20 versions, fitness=7.64
'/media/system/js/combobox.js', 7 hashes/20 versions, fitness=7.64
'/language/en-GB/en-GB.mod_search.ini', 7 hashes/20 versions, fitness=7.64
'/templates/rhuk_milkyway/css/template.css', 7 hashes/20 versions, fitness=7.64
'/media/system/js/switcher.js', 7 hashes/20 versions, fitness=7.64

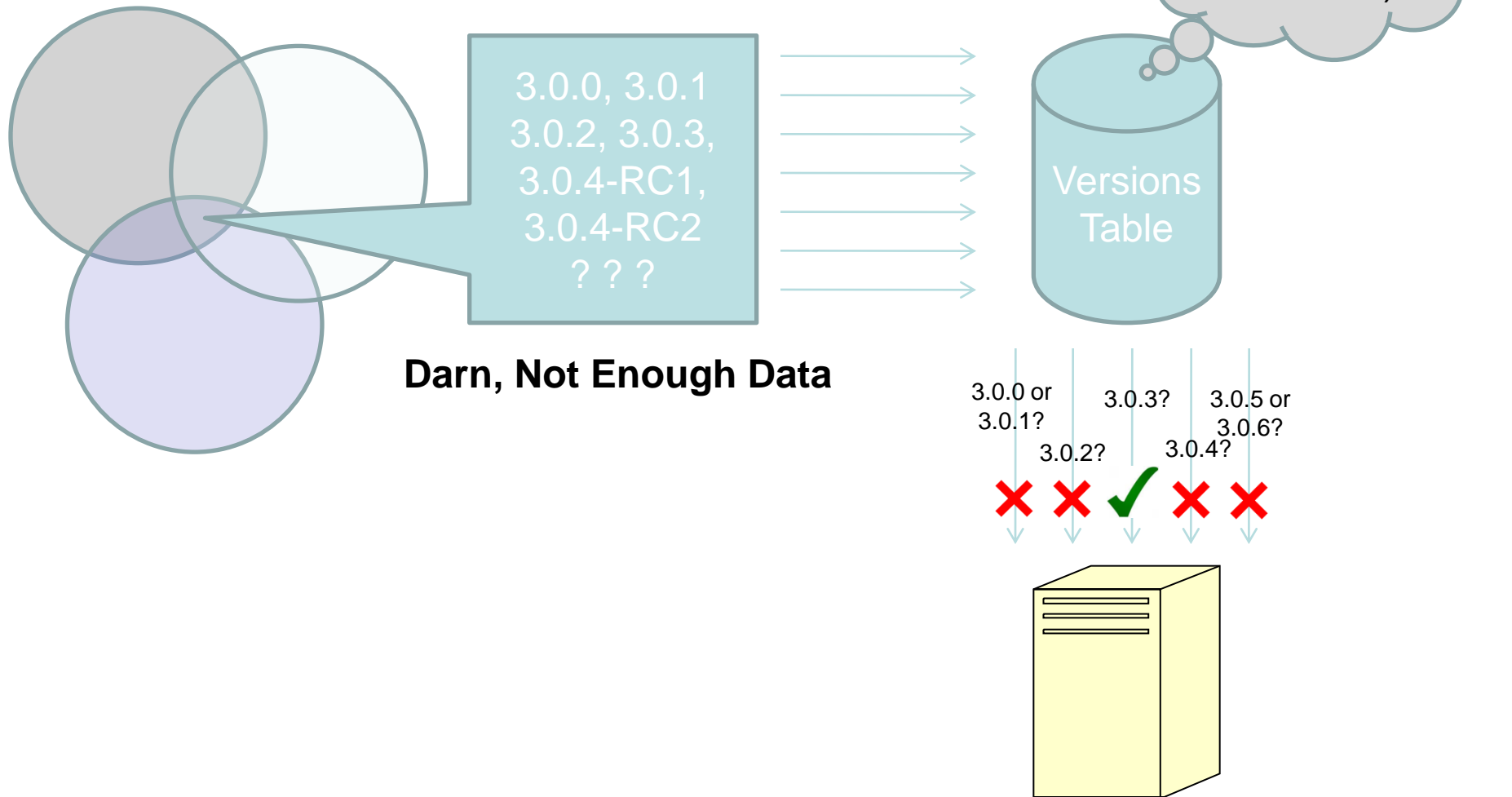
Fingerprinting

Best Candidates

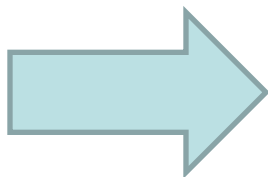
'/htaccess.txt'
'/language/en-GB/en-GB.ini'
'/language/en-GB/en-GB.com_content.ini'
'/configuration.php-dist',
'/includes/js/joomla.javascript.js'
'/media/system/js/validate.js'
'/media/system/js/caption.js'
'/language/en-GB/en-GB.mod_feed.ini'
'/media/system/js/openid.js'
'/language/en-GB/en-GB.com_contact.ini'
'/language/en-GB/en-GB.mod_breadcrumbs.ini'
'/media/system/js/combobox.js'
'/language/en-GB/en-GB.mod_search.ini'
'/templates/rhuk_milkyw/css/template.css'
'/media/system/js/switcher.js'



Winnowing



App Discovery / App Guessing



Indicator Files

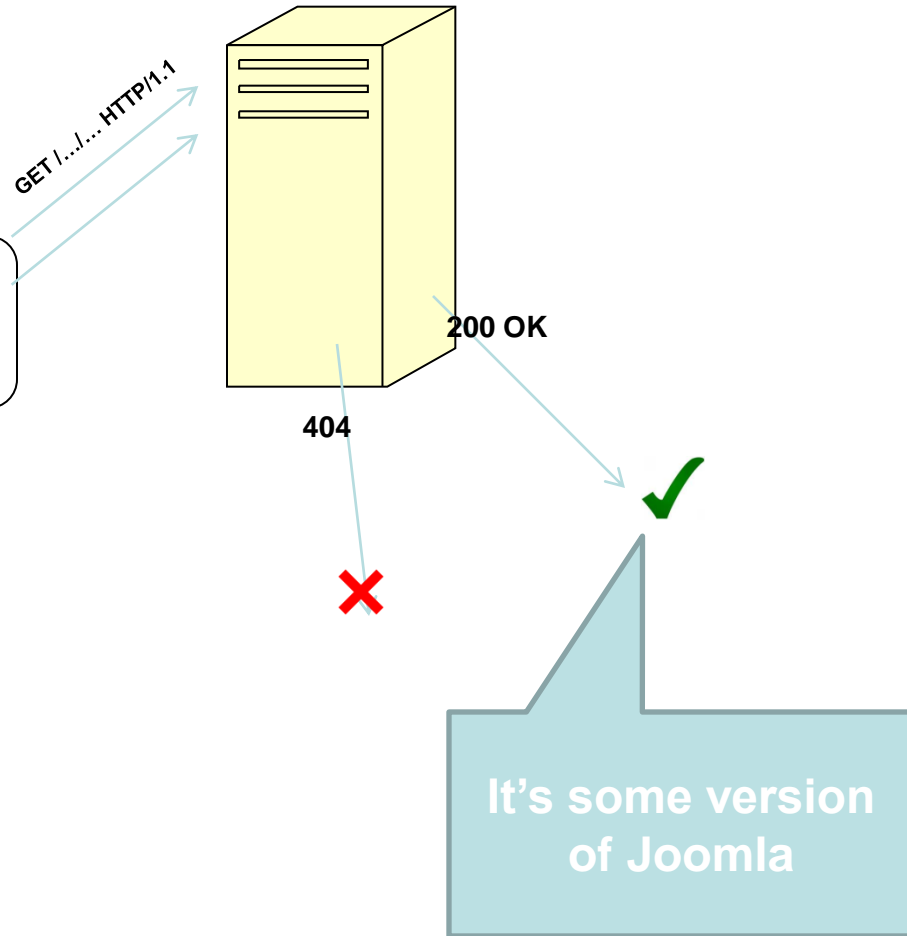
```
{'path': '/includes/js/dtree/img/frontpage.gif', 'versions': 29}  
{'path': '/images/banners/osmbanner2.png', 'versions': 33}  
{'path': '/media/system/js/mootools.js', 'versions': 18}  
{'path': '/includes/js/wz_tooltip.js', 'versions': 29}
```

Want a small set
of files with *at
least one* present
in every release

App Discovery / App Guessing

Indicator Files

```
{'path': '/includes/js/dtree/img/frontpage.gif', 'versions': 29}  
{'path': '/images/banners/osmbanner2.png', 'versions': 33}  
{'path': '/media/system/js/mootools.js', 'versions': 18}  
{'path': '/includes/js/wz_tooltip.js ', 'versions': 29}
```



Supporting a New App

- Gather every version you can find, dump them in a directory
- [Optional] Supply a regex to exclude directories/files from fingerprinting
 - (eg .php files, protected admin directory, .htaccess, etc)
- Use BlindElephant to build the datafiles
- Fingerprint!
- ...Profit?

Does it work?

`./BlindElephant.py http://laws.qualys.com` movabletype

Loaded movabletype with 96 versions, 2229 differentiating paths, and 209 version groups.

Starting BlindElephant fingerprint for version of movabletype at <http://laws.qualys.com>

Hit <http://laws.qualys.com/mt-static/mt.js>

Possible versions based on result: 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Hit <http://laws.qualys.com/mt-static/js/tc/client.js>

Possible versions based on result: 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Hit <http://laws.qualys.com/mt-static/css/main.css>

Possible versions based on result: 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM

Hit <http://laws.qualys.com/tools/run-periodic-tasks>

File produced no match. Error: Error code: 404 (Not Found)

Does it work?

Hit <http://laws.qualys.com/mt-static/js/tc/tagcomplete.js>

Possible versions based on result: 4.1-en, 4.1-en-CS, 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Hit <http://laws.qualys.com/mt-static/js/edit.js>

Possible versions based on result: 4.1-en, 4.1-en-CS, 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Hit <http://laws.qualys.com/mt-static/js/tc/mixer/display.js>

Possible versions based on result: 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Hit http://laws.qualys.com/mt-static/js/archetype_editor.js

Possible versions based on result: 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Does it work?

Hit <http://laws.qualys.com/mt-static/js/tc/mixer.js>

Possible versions based on result: 4.1-en, 4.1-en-CS, 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Hit <http://laws.qualys.com/mt-static/js/tc/tableselect.js>

Possible versions based on result: 4.1-en, 4.1-en-CS, 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

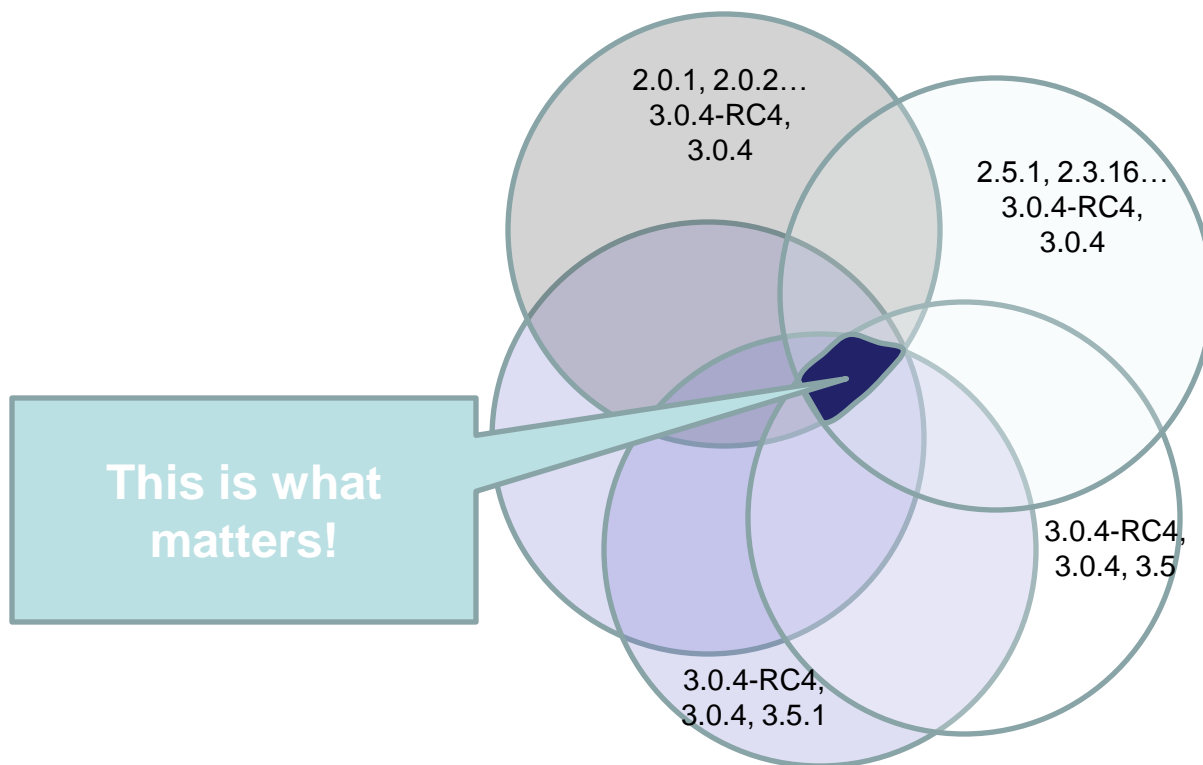
Hit <http://laws.qualys.com/mt-static/js/tc/focus.js>

Possible versions based on result: 4.1-en, 4.1-en-CS, 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Hit <http://laws.qualys.com/mt-static/js/tc.js>

Possible versions based on result: 4.1-en, 4.1-en-CS, 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Interlude



Does it work?

Hit <http://laws.qualys.com/mt-static/css/simple.css>

Possible versions based on result: 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM

Hit http://laws.qualys.com/mt-static/mt_ja.js

Possible versions based on result: 4.2-en, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.23-en-OS, 4.24-en, 4.24-en, 4.24-en-COM

Hit <http://laws.qualys.com/mt-static/js/tc/gestalt.js>

Possible versions based on result: 4.1-en, 4.1-en-CS, 4.2-en, 4.21-en, 4.21-en, 4.21-en-COM, 4.22-en, 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en, 4.23-en-COM, 4.24-en, 4.24-en, 4.24-en-COM

Fingerprinting resulted in: 4.22-en, 4.22-en-COM, 4.23-en, 4.23-en-COM

Best Guess: **4.23-en-COM**

Lets Pick on the Security Bloggers Network

`./BlindElephant.py` <http://www.andrewhay.ca/> wordpress

Loaded wordpress with 159 versions, 599 differentiating paths, and 226 version groups.
Starting BlindElephant fingerprint for version of wordpress at <http://www.andrewhay.ca>

Fingerprinting resulted in:

3.0-RC1

3.0-RC1-IIS

Best Guess: **3.0-RC1**

BTW: It Does Plugins Too

```
$ ./BlindElephant.py -s -p guess http://example.com drupal
```

Possible plugins:

```
['admin_menu', 'cck', 'date', 'google_analytics', 'imce', 'imce_swfupload',  
'pathauto', 'print', 'spamicide', 'tagadelic', 'token', 'views']
```

```
$. /BlindElephant.py -s -p imce http://example.com drupal
```

<snip>

Fingerprinting resulted in:

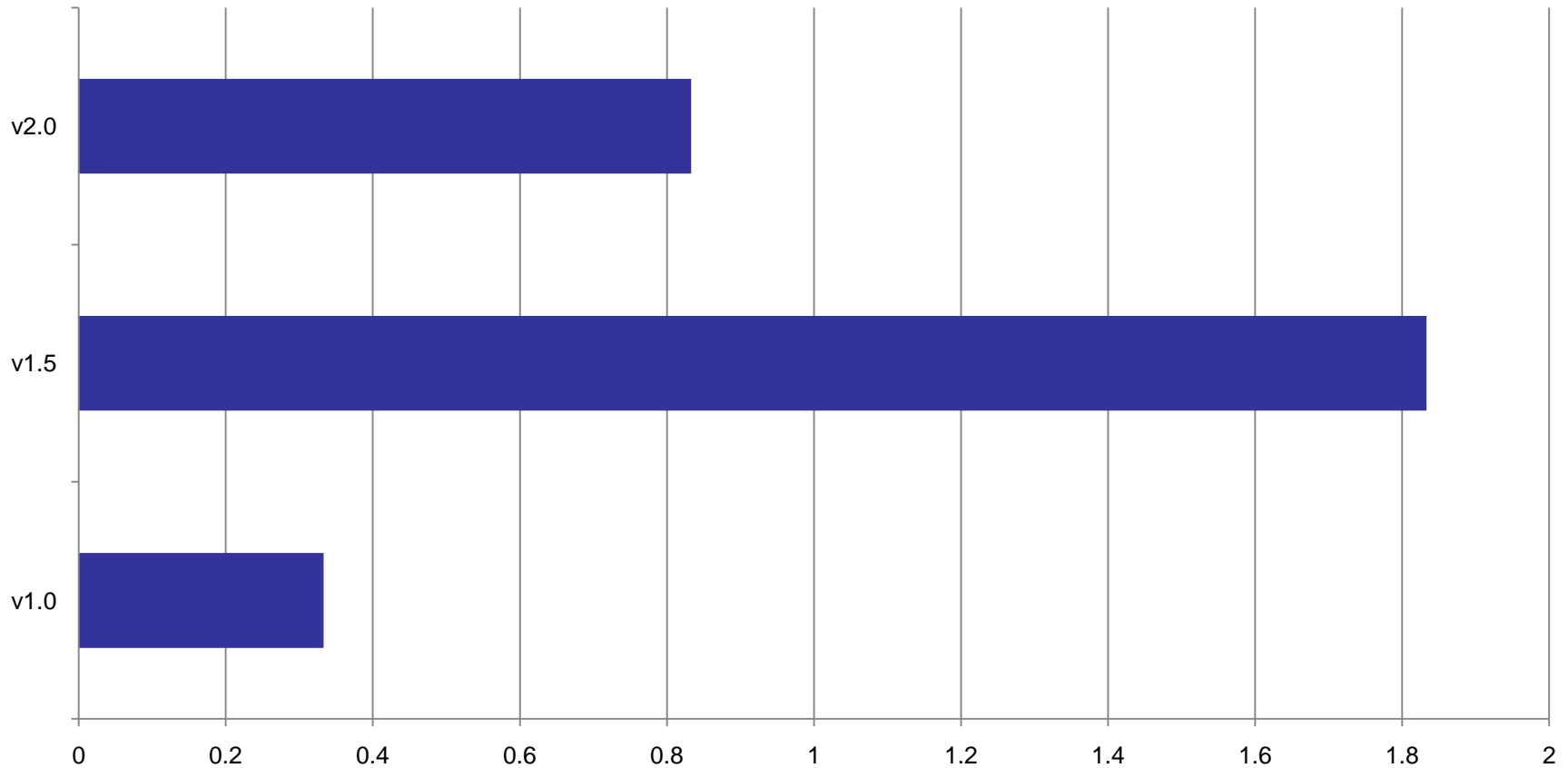
6.x-1.3

New Toy! Lets Play

- App ID & Fingerprinting on **1,084,152** hosts
- **34k** targeted scans for bug shakeout and calibration
 - Shodan = Really, really useful (kinda expensive though)
 - Is John here? I owe him a beer.
 - Slightly biased sample (skews to default installs, s'okay though)
- **50k** and **~1M** host random sample of 87M .com domains
 - Stats on accuracy and net-wide webapp population are from these

On To the Results...

Version Distribution: SomeApp

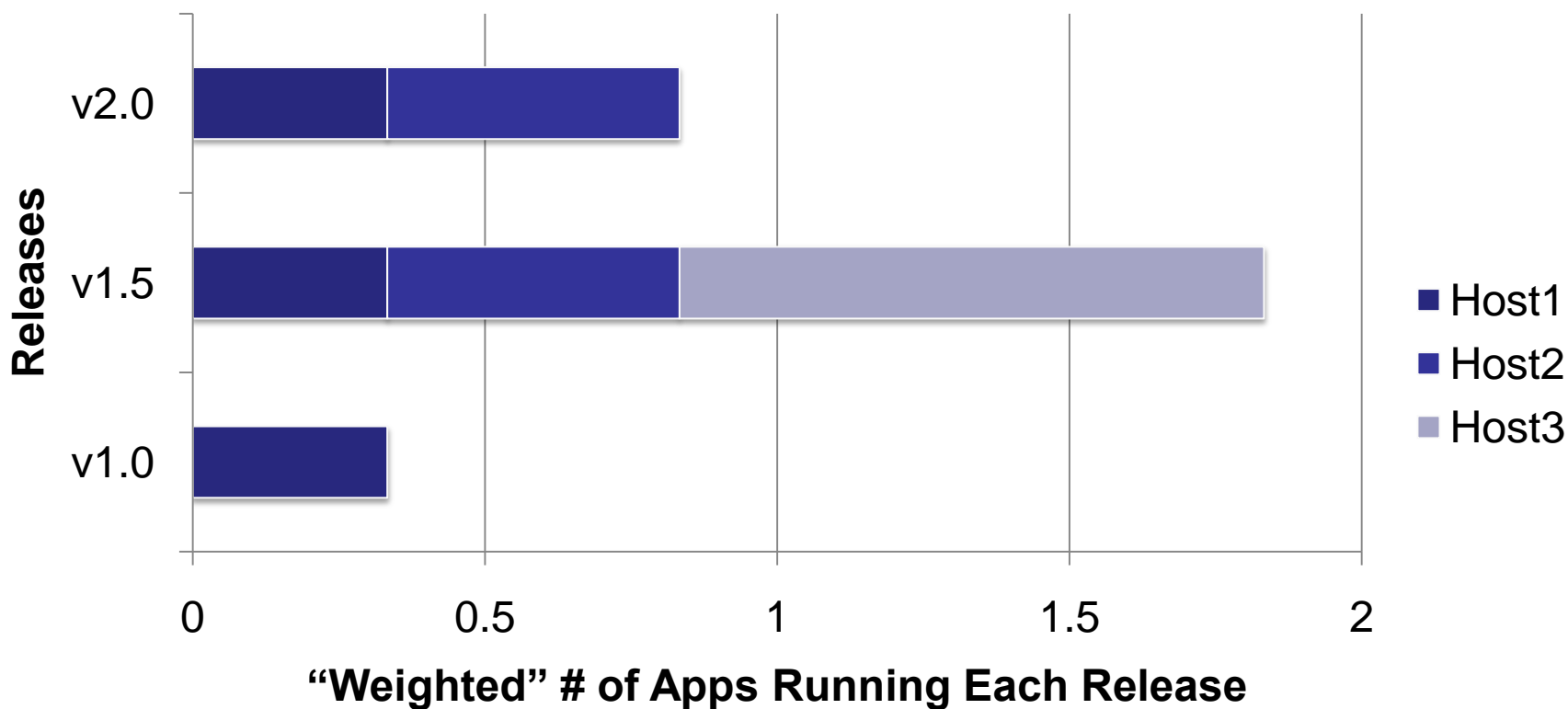


Graphing Sets of Possibilities

- Host1 Possible Versions: v1.0, v1.5, v2.0
 - .33 to three version columns
- Host2 Possible Versions: v1.5, v2.0
 - .5 to two version columns
- Host3 Possible Versions: v1.5
 - 1.0 to v1.5

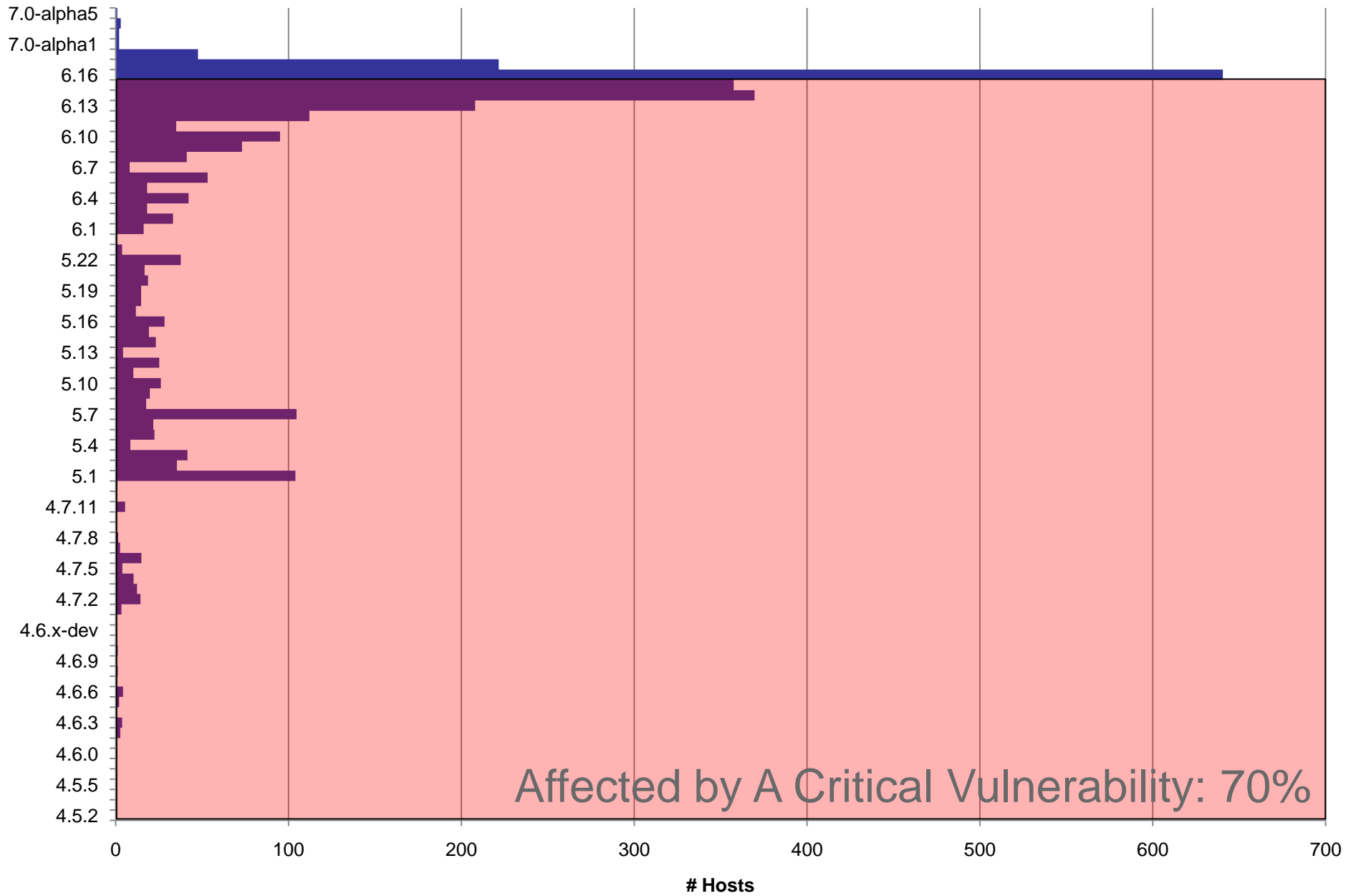
Graphing Sets of Possibilities

Version Distribution: Some App (6/18/10)



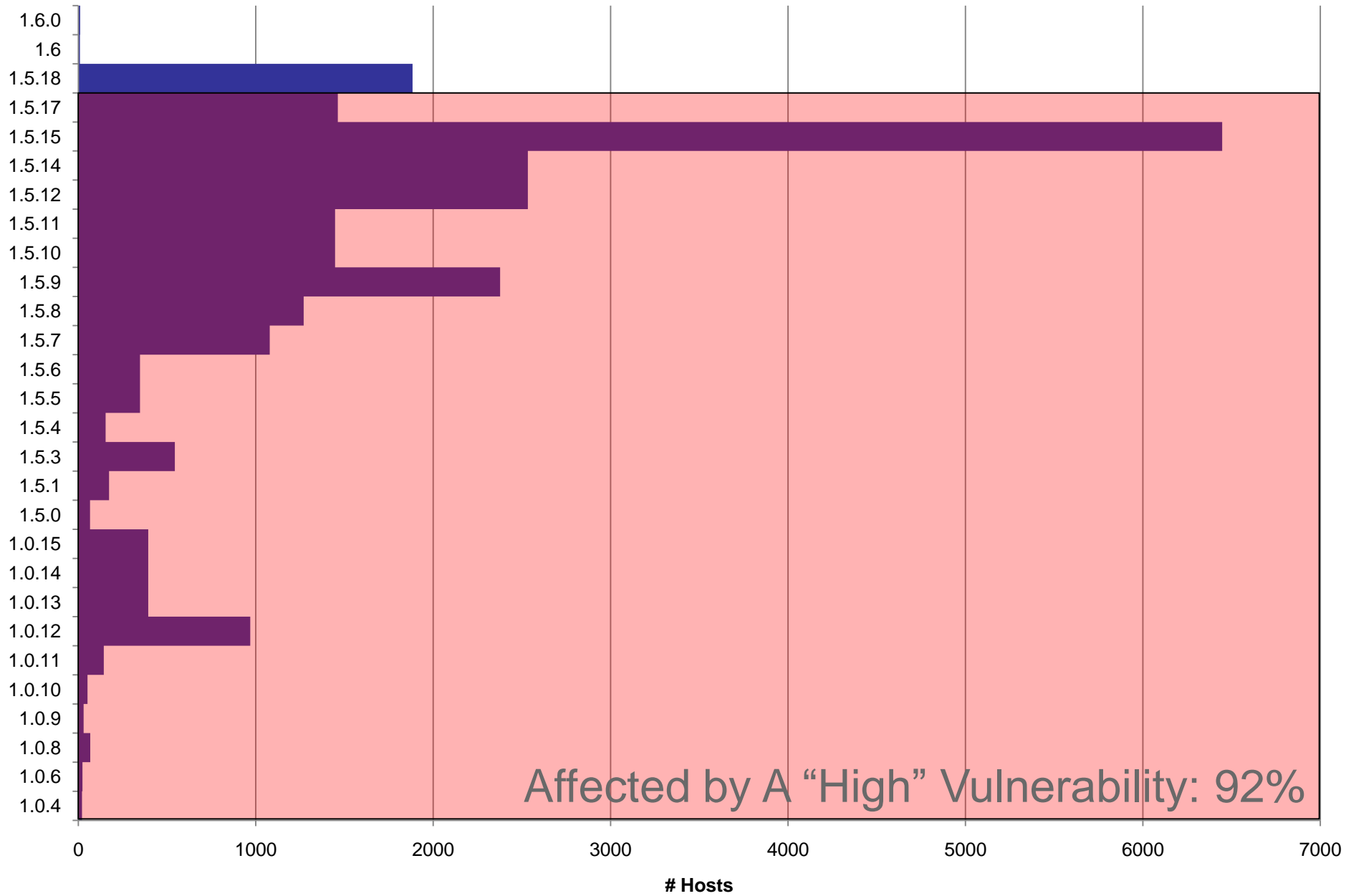
Version Distribution: Drupal

(June 18, 2010)



Version Distribution: Joomla

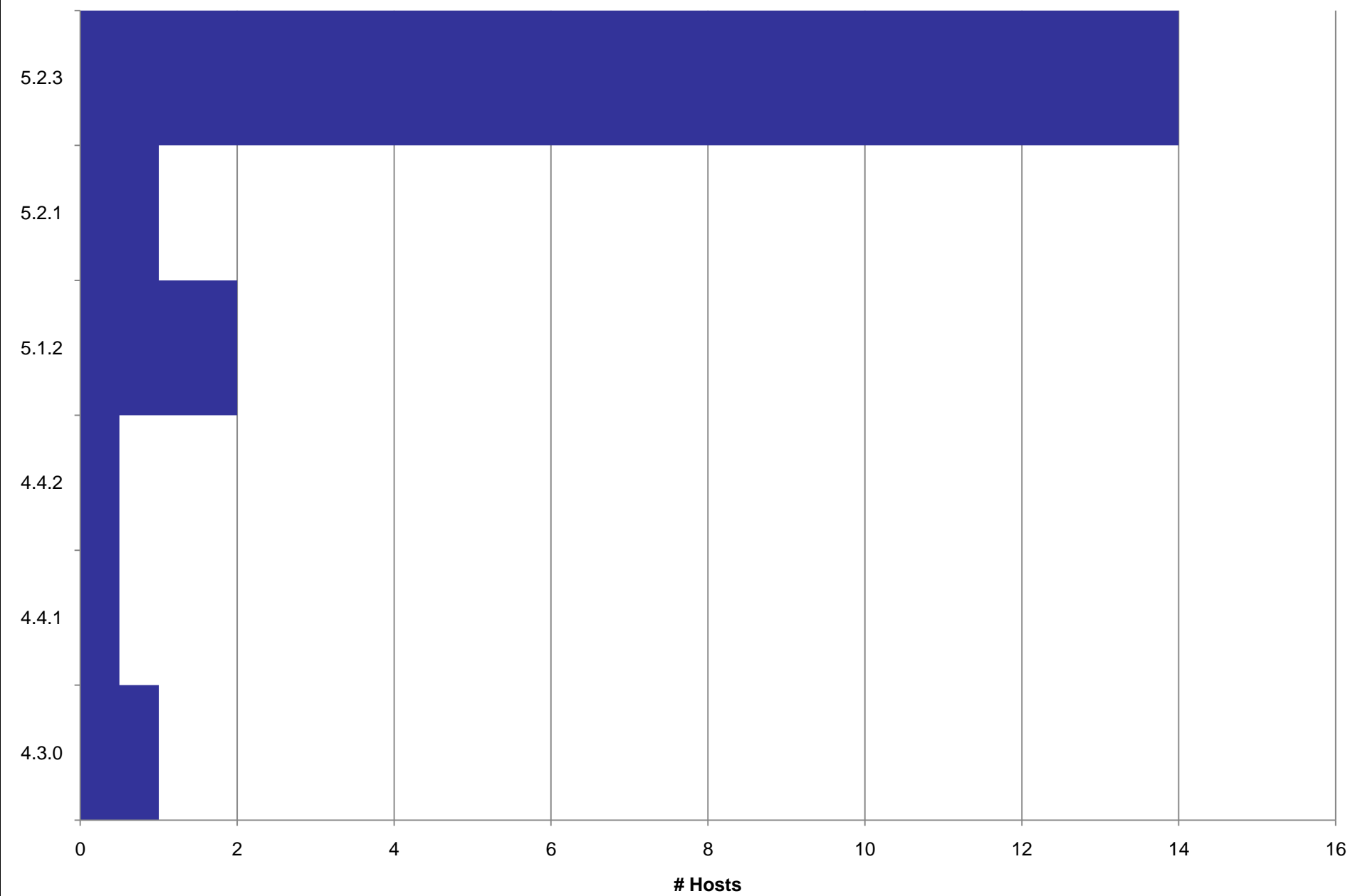
(June 18 2010)



Affected by A "High" Vulnerability: 92%

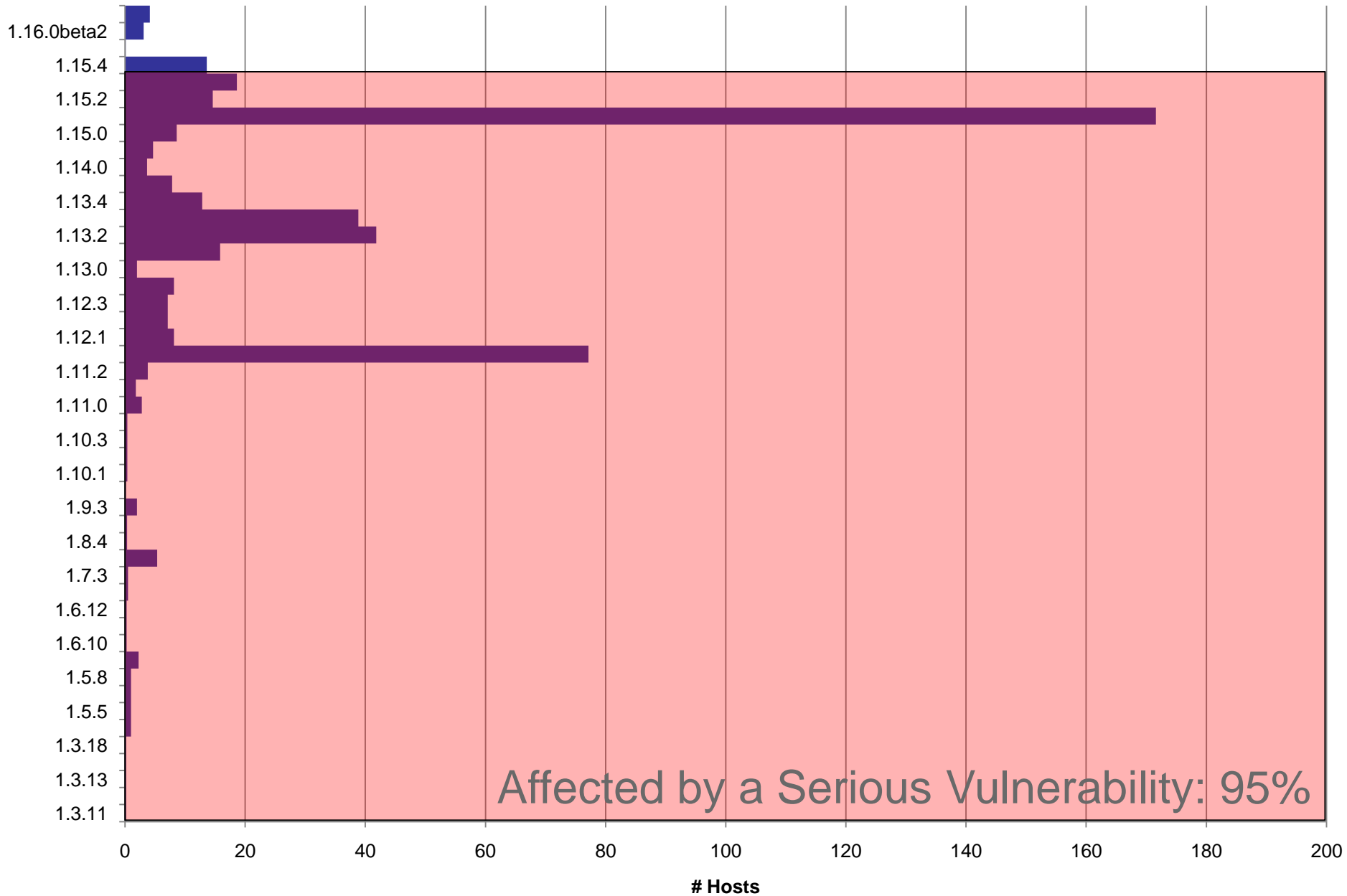
Version Distribution: Liferay

(June 18, 2010)



Version Distribution: Mediawiki

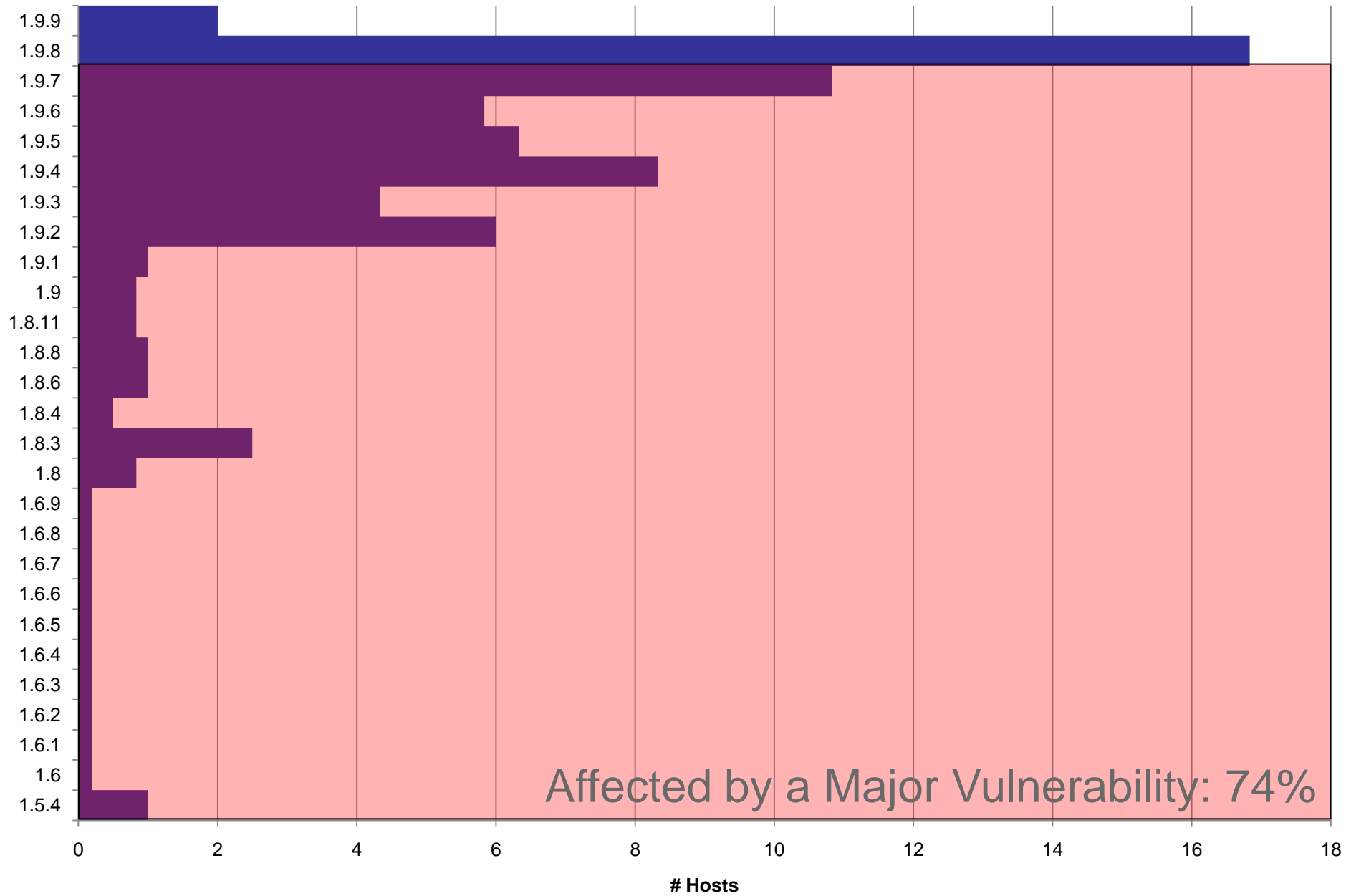
(June 18, 2010)



Affected by a Serious Vulnerability: 95%

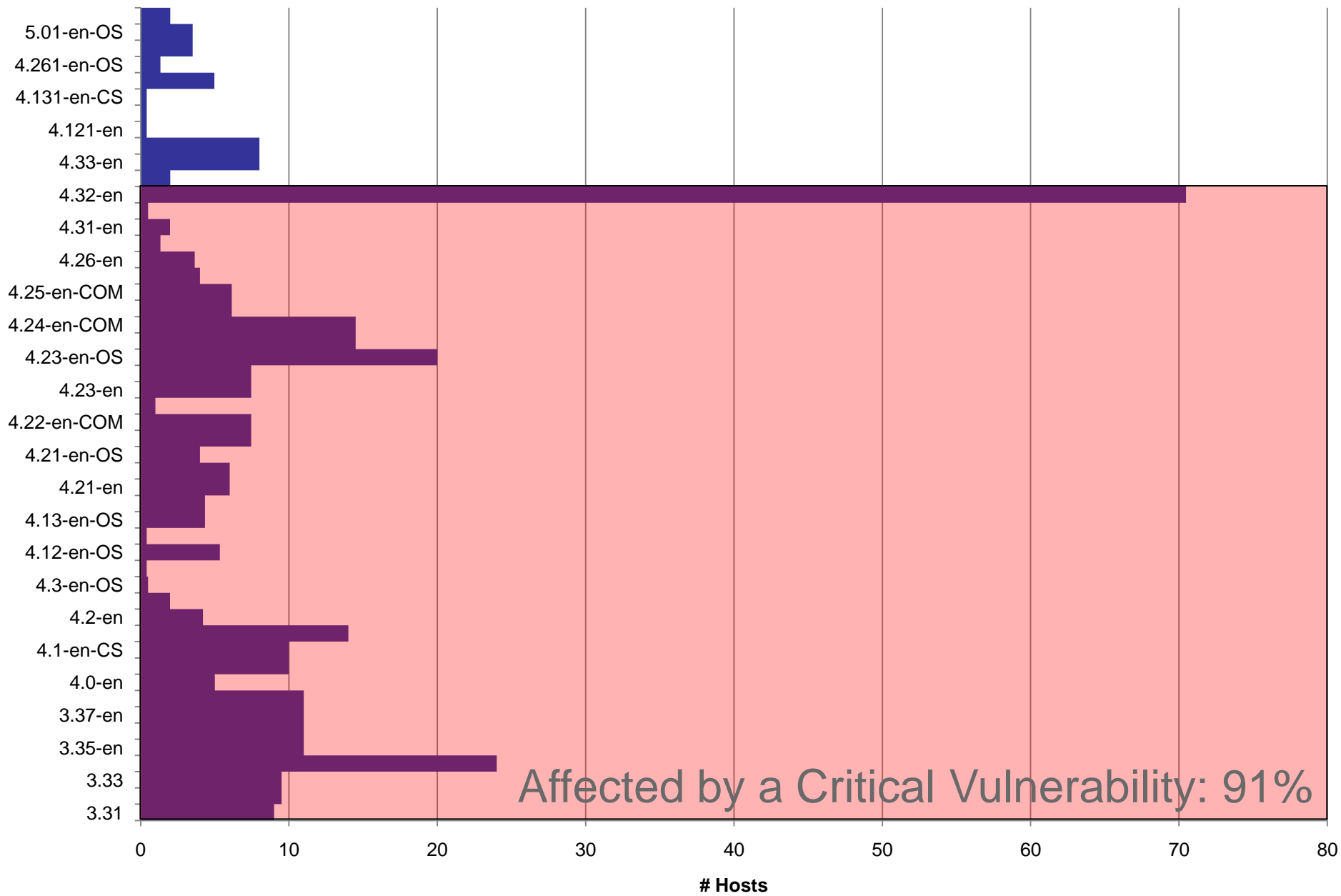
Version Distribution: Moodle

(June 18, 2010)



Version Distribution: MovableType

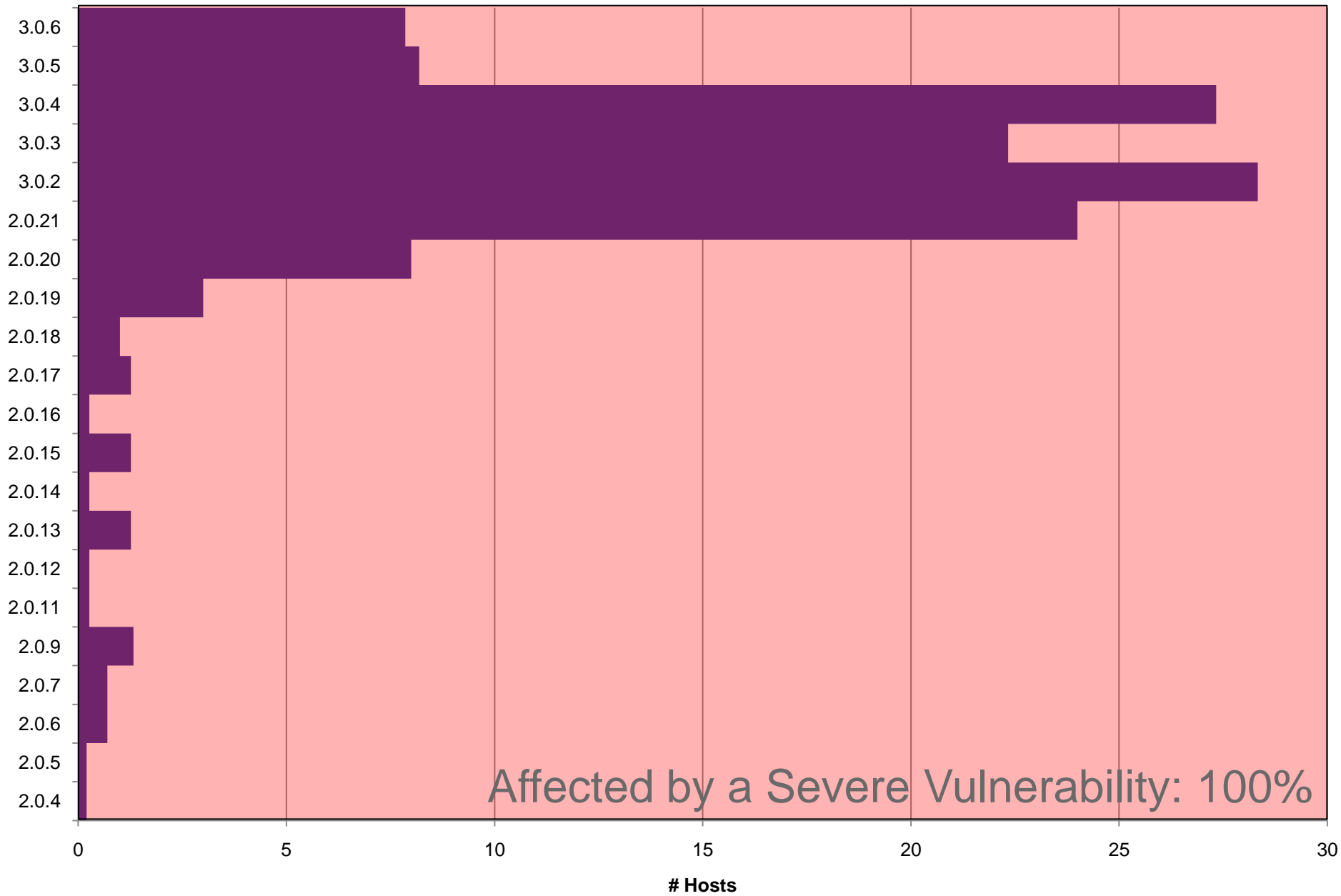
(June 18, 2010)



Affected by a Critical Vulnerability: 91%

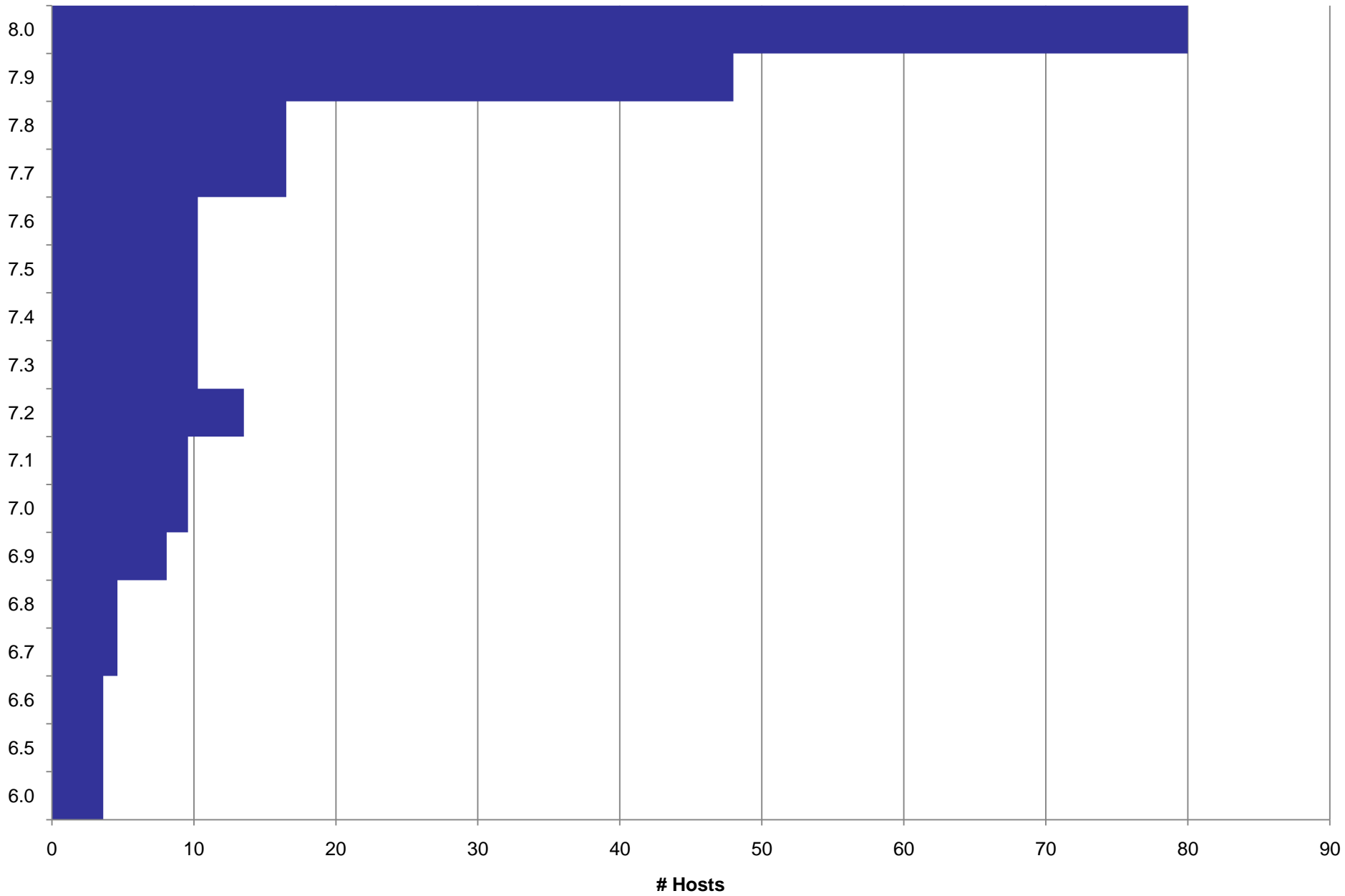
Version Distribution: phpBB

(June 18, 2010)

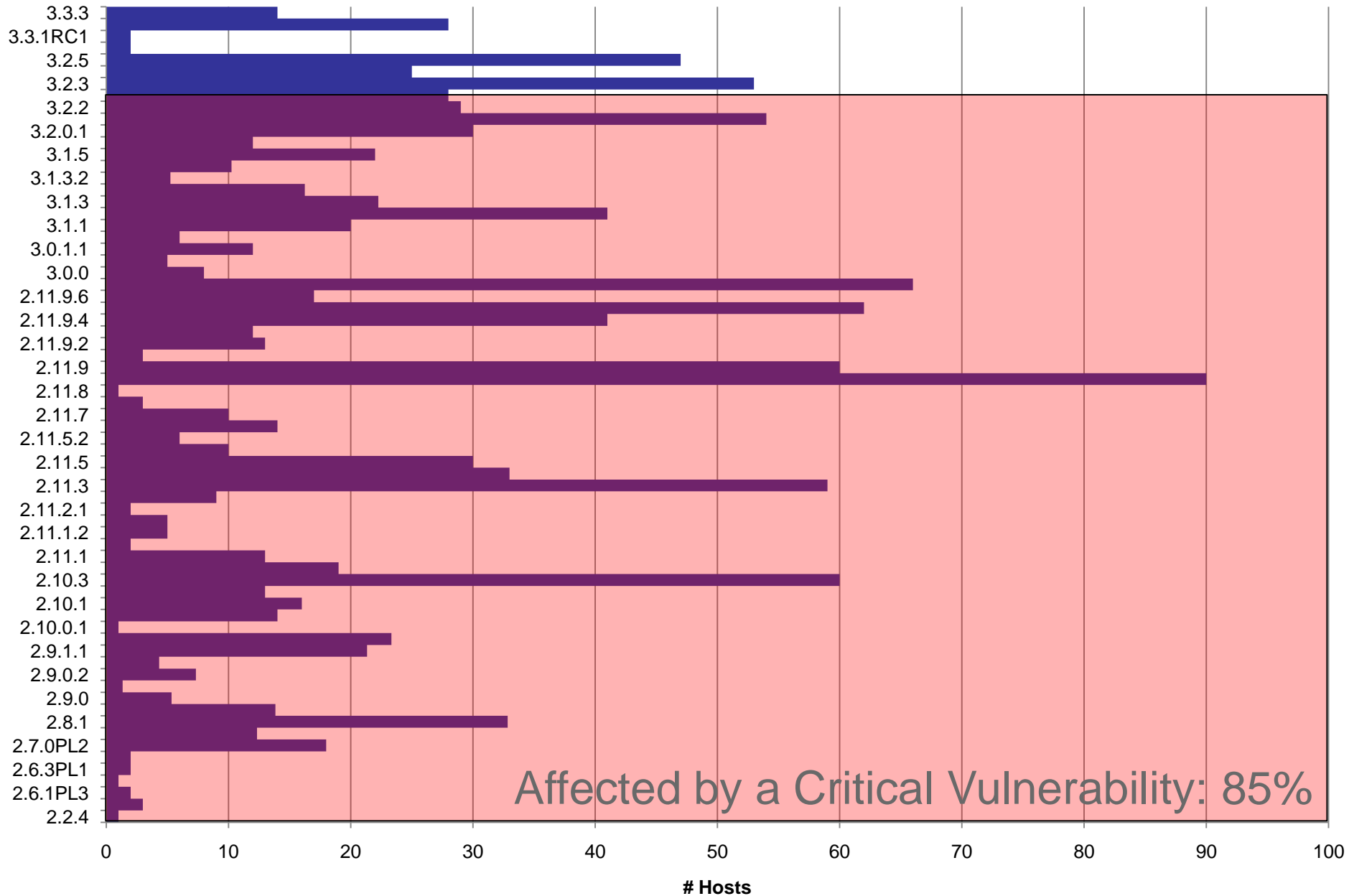


Version Distribution: PHPNuke

(June 18, 2010)



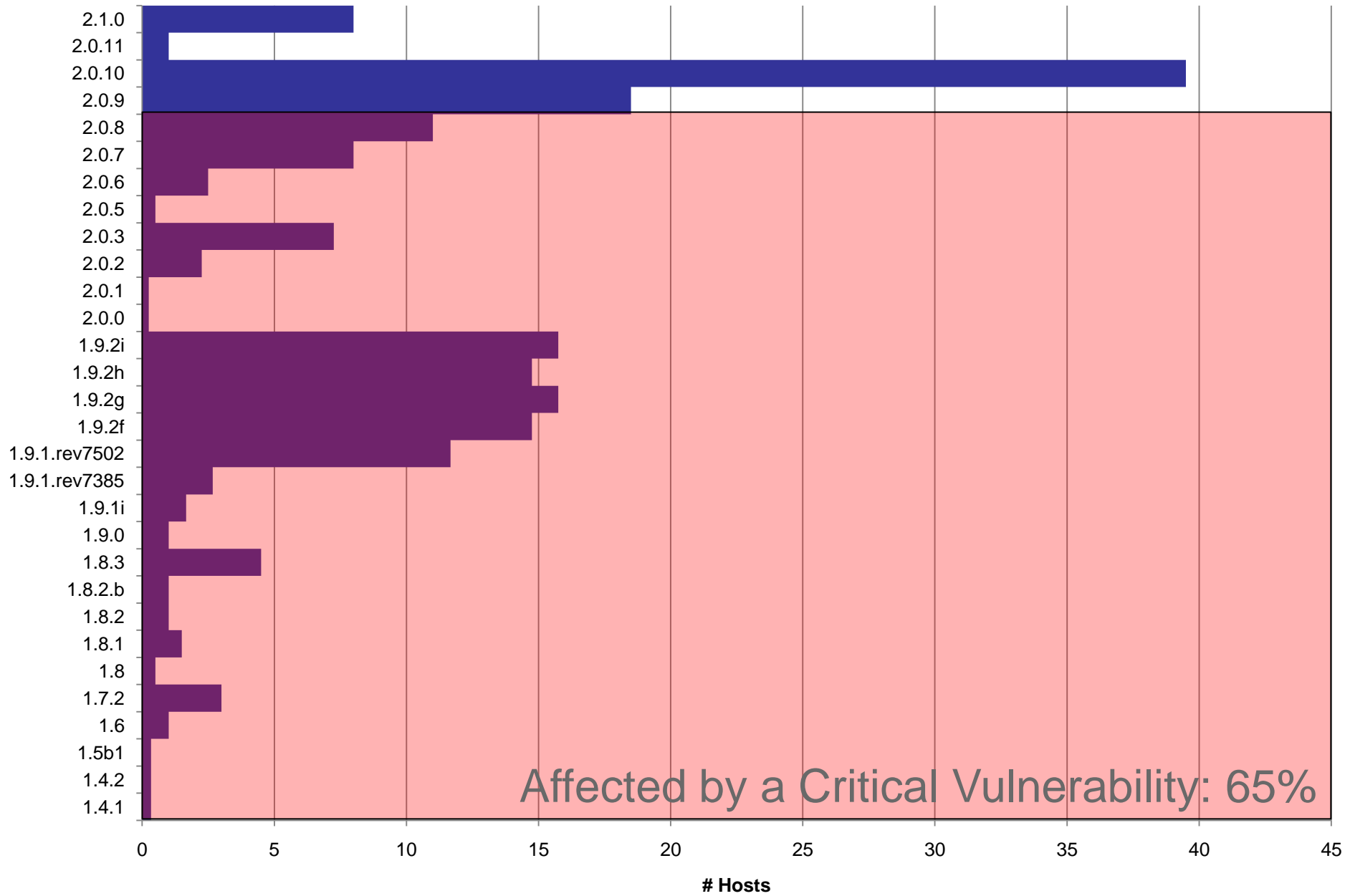
Version Distribution: phpMyAdmin (June 18, 2010)



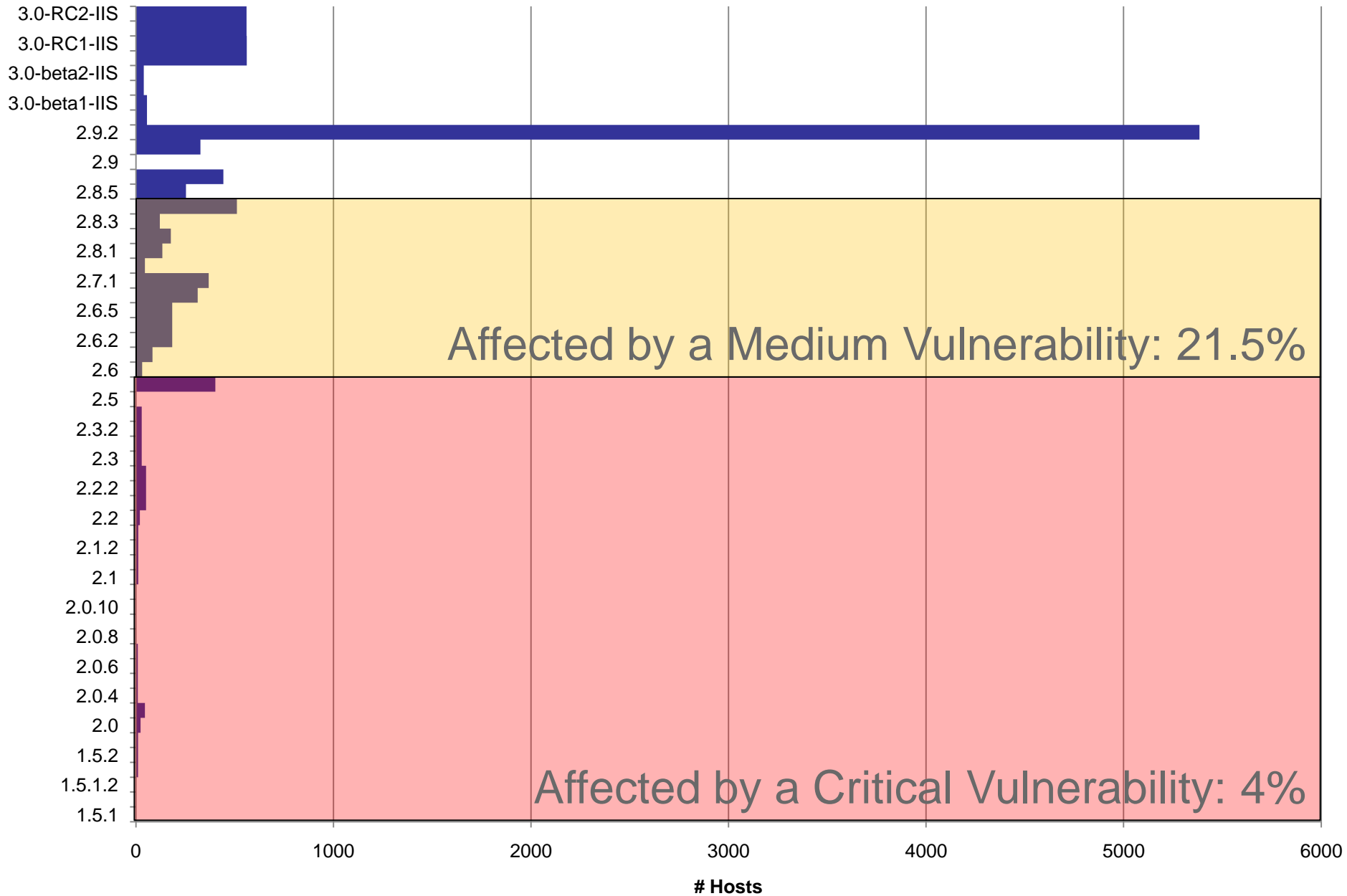
Affected by a Critical Vulnerability: 85%

Version Distribution: SPIP

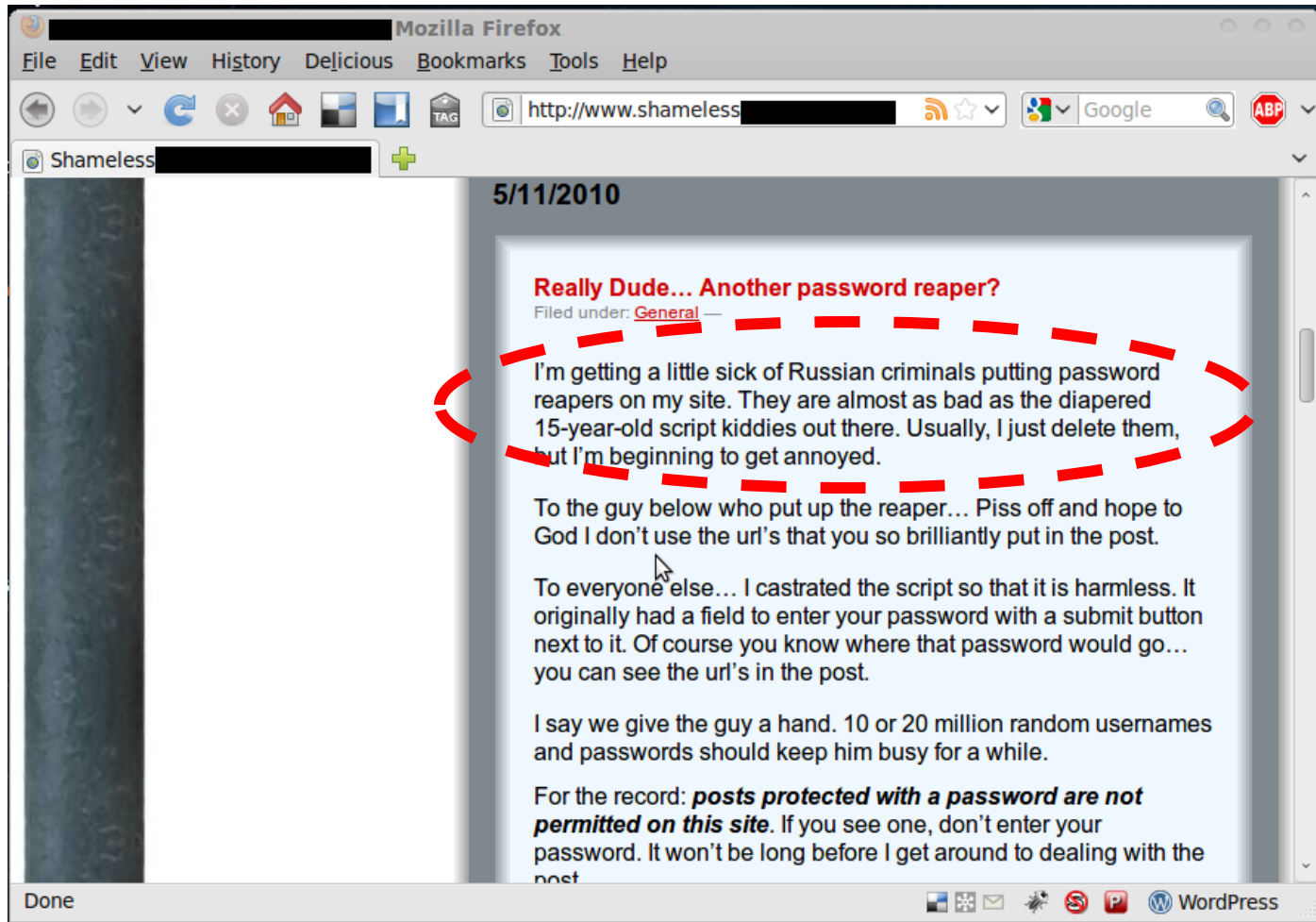
(June 18, 2010)



Version Distribution: Wordpress (June 18, 2010)



Lost: a Clue



Lost: A Clue

The image shows a screenshot of a Mozilla Firefox browser window. The browser's address bar contains the URL `http://www`. The page title is "Shameless". The main content area displays a blog post dated "5/11/2010" with the title "Really Dude... A [redacted] reaper?". The post text includes: "I'm getting [redacted] Russian criminals putting password reapers [redacted] they are almost as bad as the diapered 15-year-old kiddies out there. Usually, I just delete them, but [redacted] to get annoyed." Below this, there is a terminal window with the following output: "Fingerprinting resulted in 1.2.2 1.2-mingus Best Guess: 1.2-mingus". The browser's status bar at the bottom shows "Done" and various icons including a mail icon, a search icon, and a WordPress logo.

He's only 6 years and 60 releases behind...

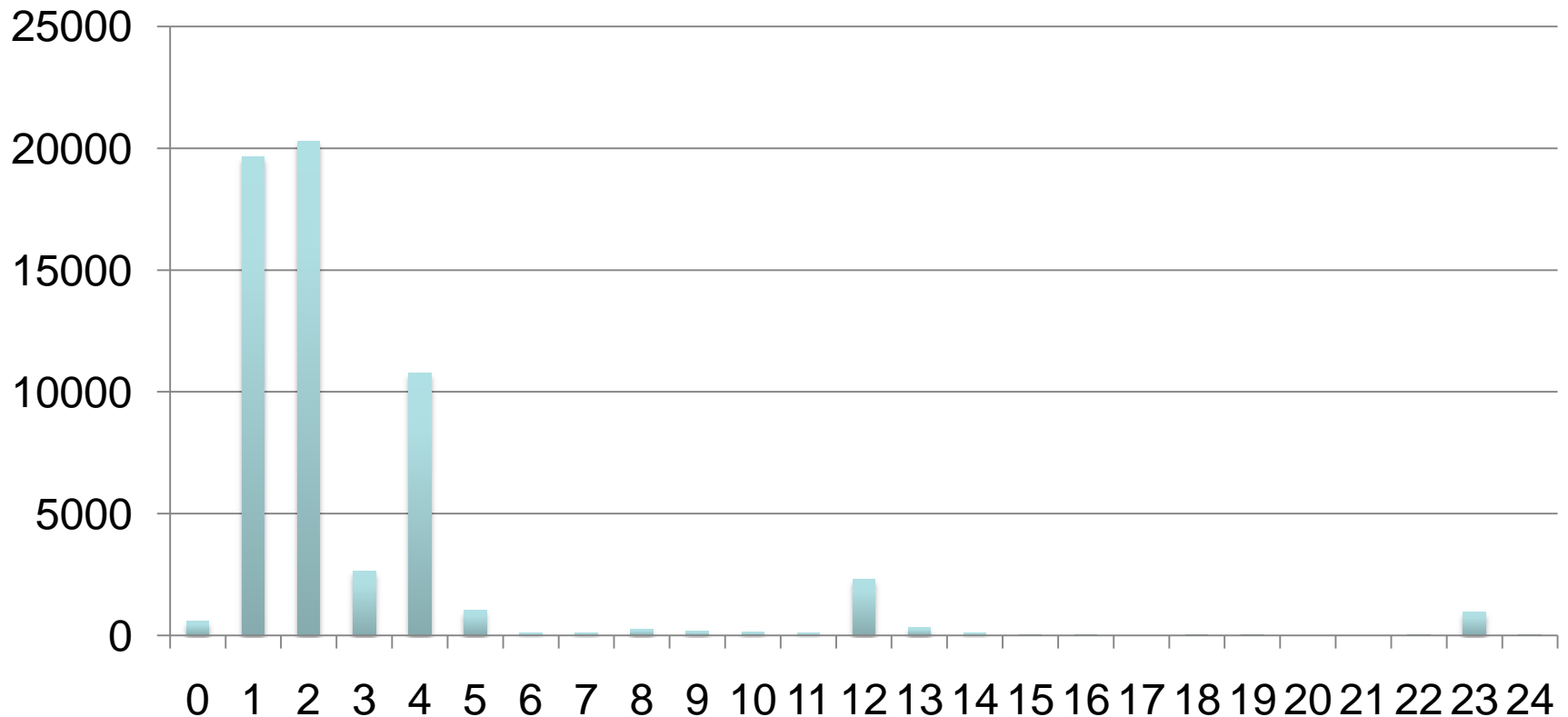
Observations

- Webapps actually doing pretty well update-wise
- Improperly removed webapps abound
 - Switch from CMS A to CMS B, but leave A lying around
- Net-visible test/QA sites

Precision

Fingerprint Precision

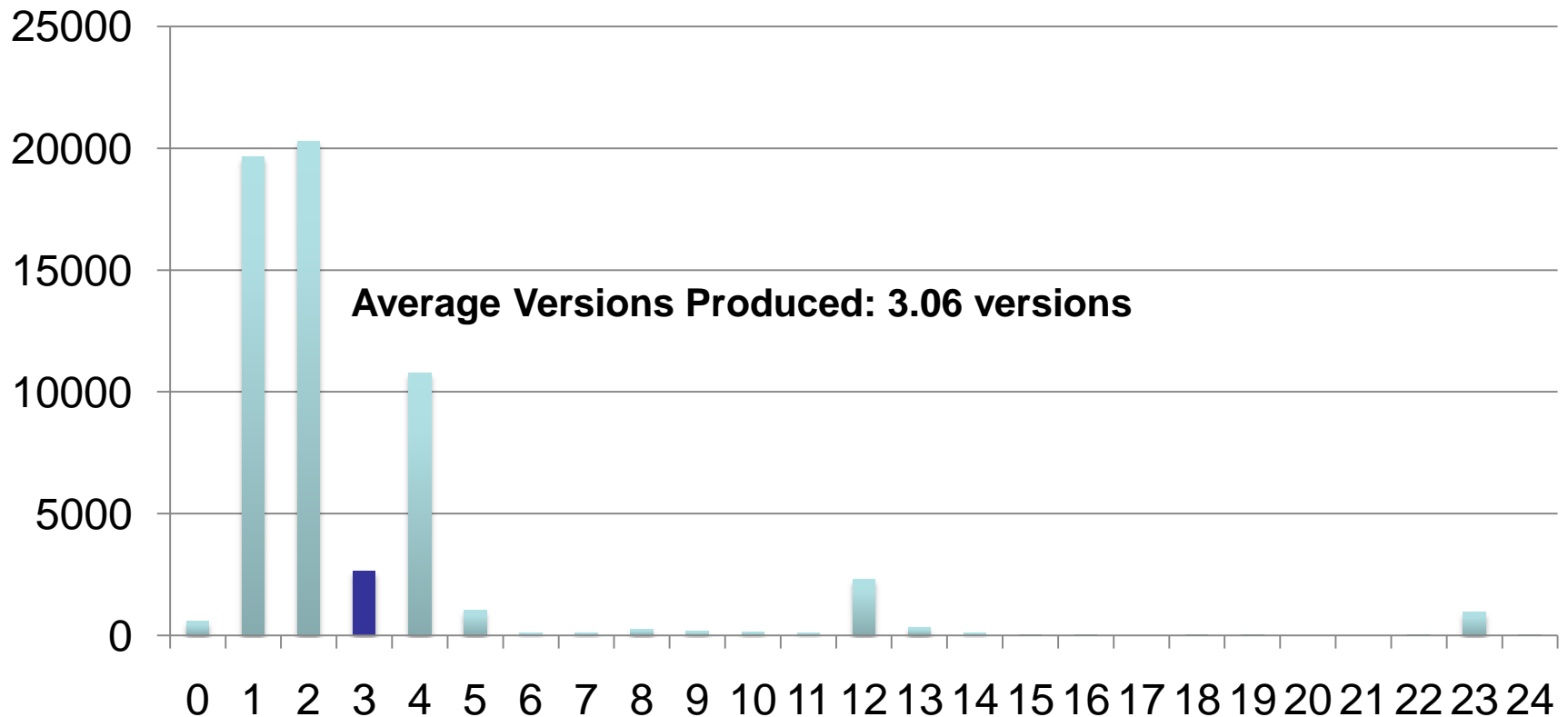
(# Versions Resulting from a Fingerprint (1 is best))



Precision

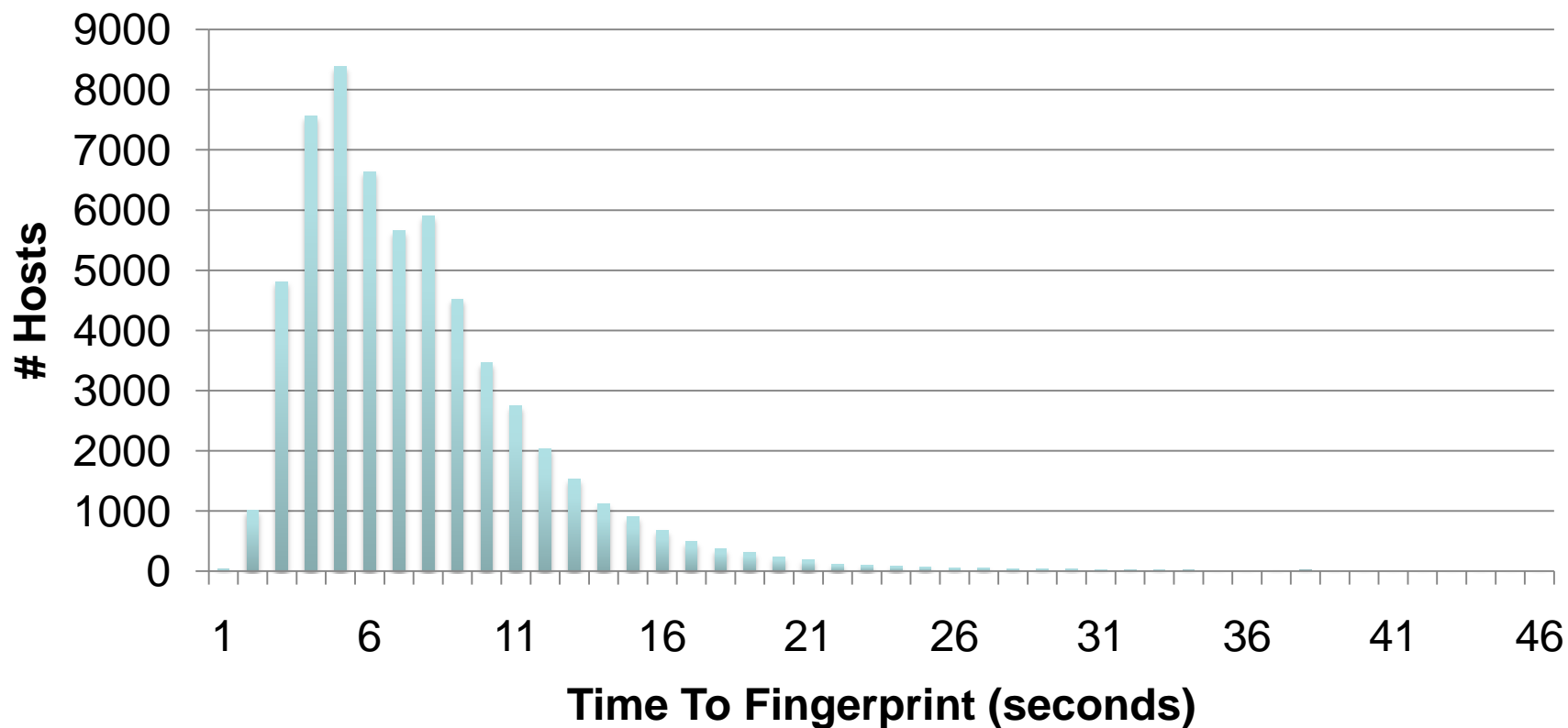
Fingerprint Precision

(# Versions Resulting from a Fingerprint (1 is best))



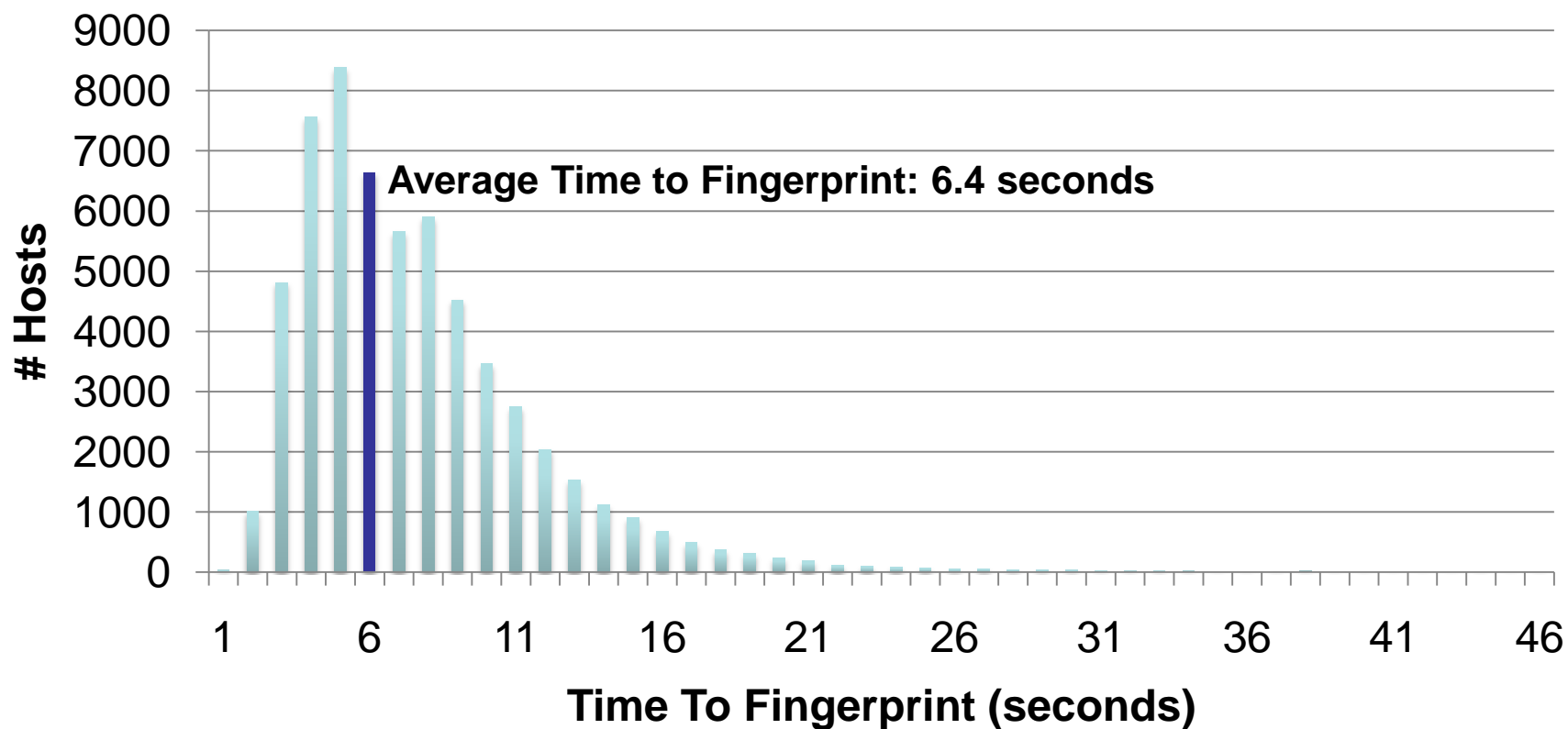
Speed

Fingerprinting Time (Quicker is better)



Speed

Fingerprinting Time (Quicker is better)



BlindElephant Scorecard

- Very Generic → Same code for all apps & plugins
- Fast → 1-10 sec, based on host (Avg 6.4)
- Low resources → Avg 354.2 Kb to fingerprint
- Accurate → Avg 1.66 versions & ID 98.0% of sites
- Resistant to hardening/banner removal
→ Yes
- Easy to support new versions/apps
→ ~2 hour to support all available versions of a new app (1 if they're packed nicely)

Sources Of Error

- WebApp Incompletely Removed
- Partial/Manual Upgrades
 - We tend to catch these though
- Changed App Root
- Static hosting on alternate domain (eg, Wikipedia)

- Fails completely if static files are trivially modified
 - But guess what? People don't do it

Release the Kra... Elephant



<http://blindelephant.sourceforge.net/>

To Do

- Web App Developers
 - Think about default deployments that resist fingerprinting
 - Help us create fingerprint files to recognize your app!
- Site Administrators
 - Fingerprint yourself – know what the attackers know
 - Harden to resist fingerprinting
 - Just... stay up to date
- Everyone Else
 - Try it out
 - Report bugs, contribute signatures, implement a pet feature

Questions?

pthomas@qualys.com

pst@coffeetocode.net

@coffeetocode

<http://coffeetocode.net>