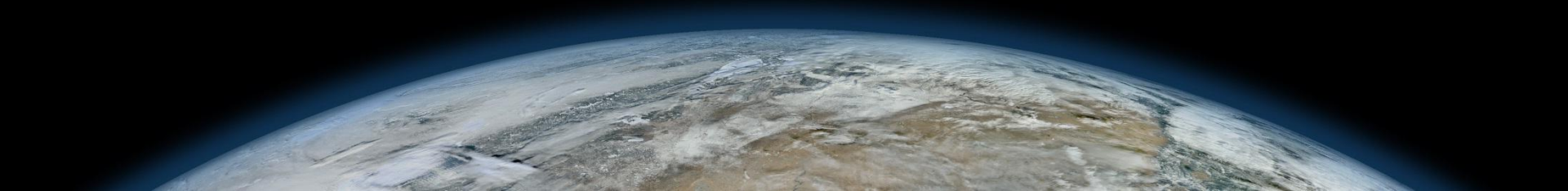


Four Axes of Evil

Austin, TX

October 26th, 2012

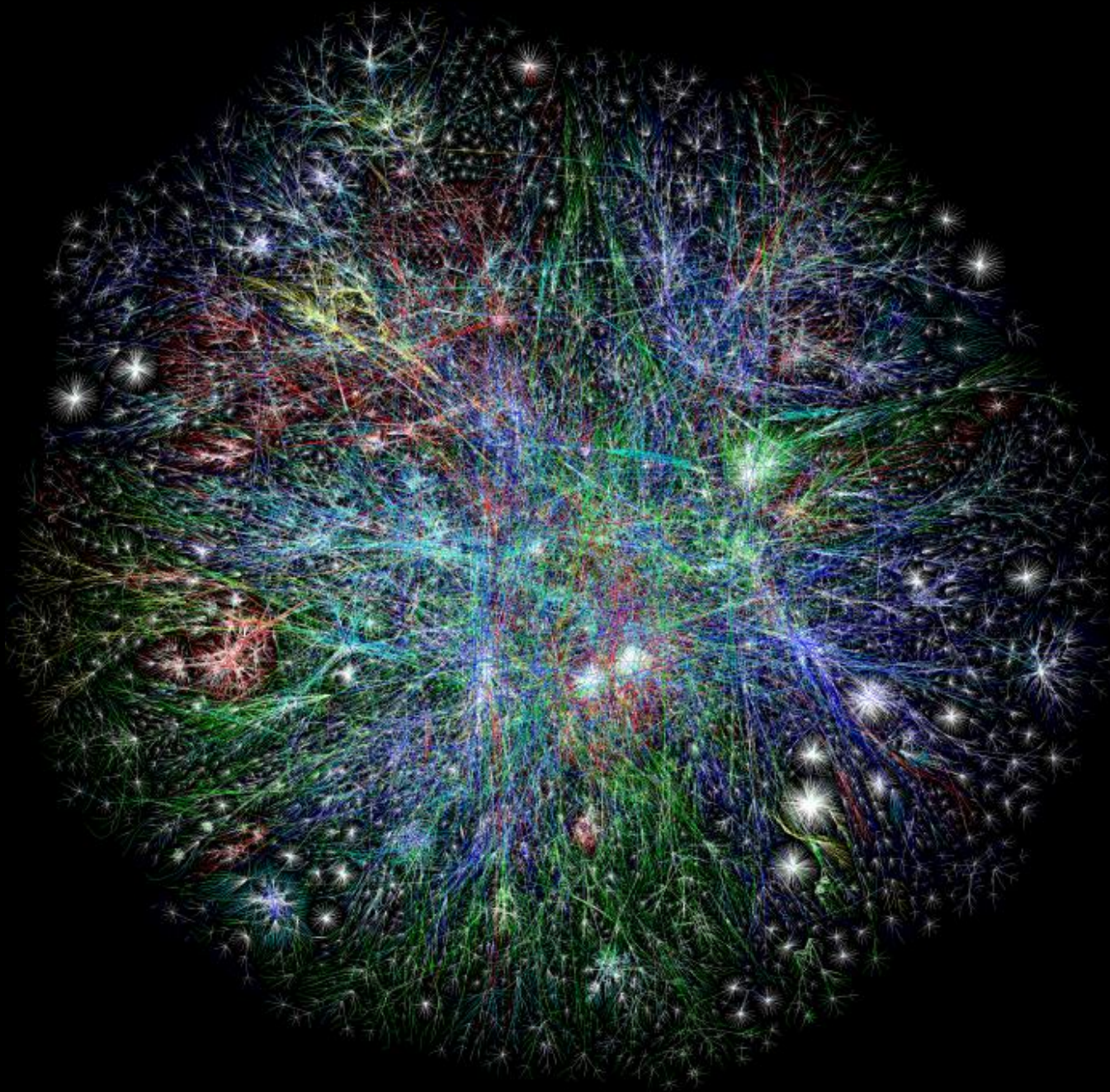


http://1224396017/

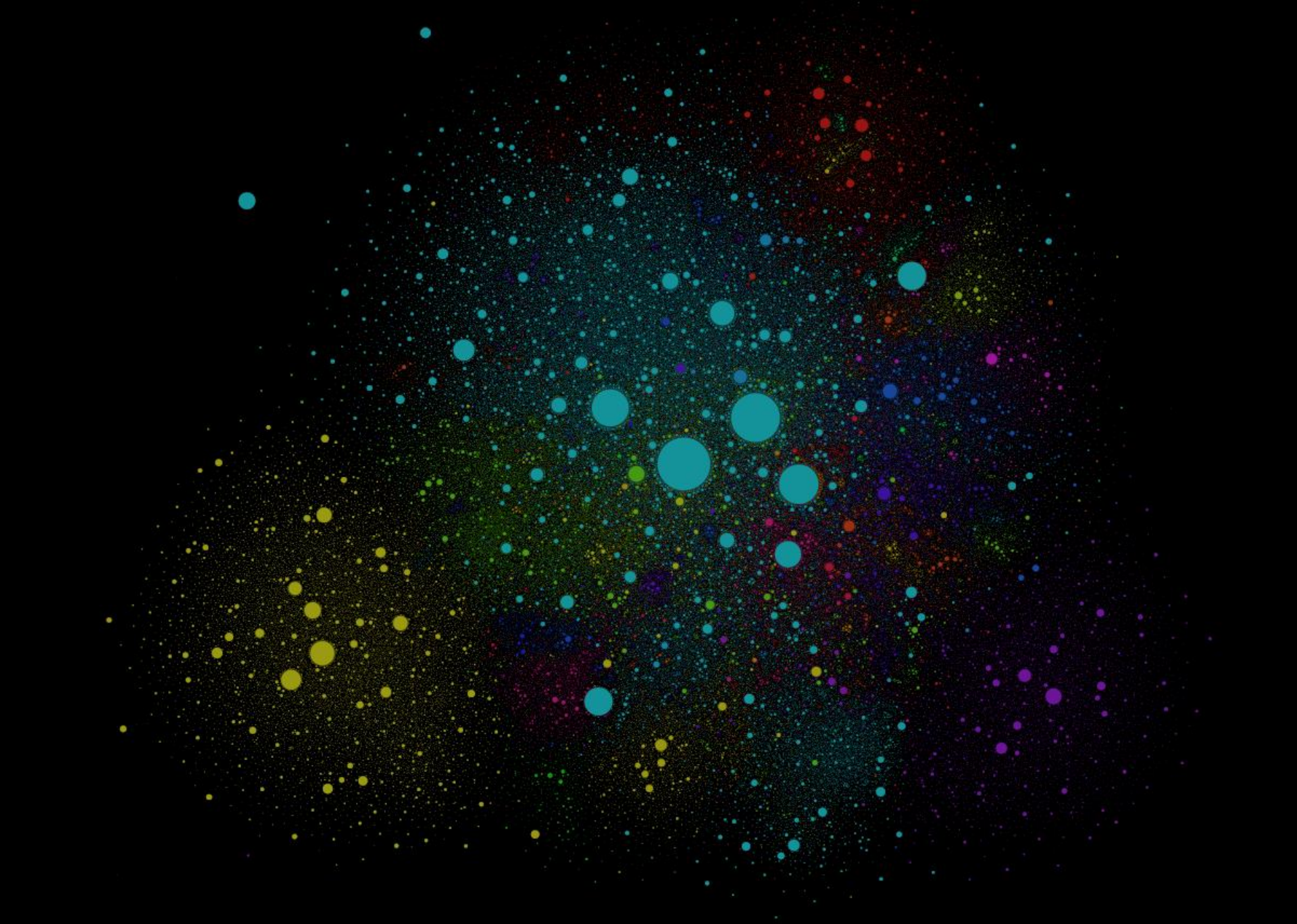
IPv4 addresses are 32 bits, a fairly small range to manage

0 — 4,294,967,295

0.0.0.0 — 255.255.255.255









Gathering Data

Ancient

1998 — BASS: Bulk Audit Security Scanner

- Scanned 36.4 million hosts over the course of 20 days
- Tested 18 vulnerabilities and confirmed 730 thousand
- Over 450,000 thousand hosts found vulnerable

service		vulnerability count, percentage
webdist		5622 hosts counted, 0.77% from total
wu_imapd		113183 hosts counted, 15.5% from total
qpopper		90546 hosts counted, 12.4% from total
innd		3797 hosts counted, 0.52% from total
tooltalk		190585 hosts counted, 26.1% from total
rpc_mountd		78863 hosts counted, 10.8% from total
bind		132168 hosts counted, 18.1% from total
wwwcount		86165 hosts counted, 11.8% from total
phf		6790 hosts counted, 0.93% from total
ews		9346 hosts counted, 1.28% from total

Modern

2010+ — SHODAN: The computer search engine

- Collected data on approximately 120 million hosts
- <http://shodanhq.com/>


Services

HTTP	80,866,984
UPnP	9,372,230
SNMP	7,608,315
SSH	7,492,473
HTTP Alternate	6,499,364

Top Countries


United States	40,919,561
China	6,084,507
Korea, Republic of	4,604,278
Germany	4,575,018
Japan	4,556,055

302 Found

137.78.99.39
Linux recent 2.4
National Aeronautics and Space
Administration
Added on 25.09.2012
 Pasadena
education.jpl.nasa.gov

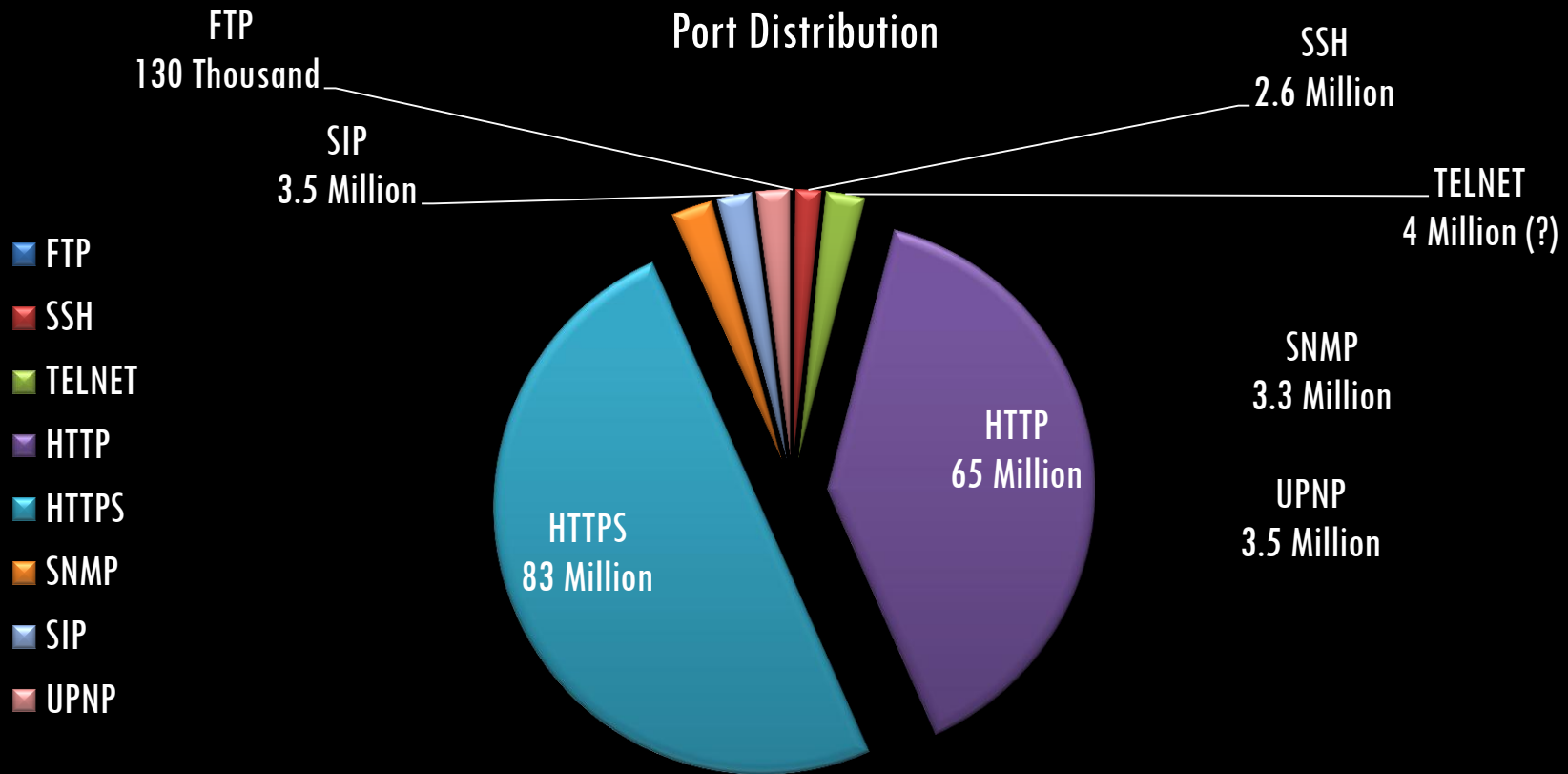
HTTP/1.0 302 Found
Date: Mon, 24 Sep 2012 16:57:19 GMT
Server: Apache/2.2.22 (Unix) PHP/5.3.16 mod_jk/1.2.32 JRun/4.0
Location: <http://www.jpl.nasa.gov/education/>
Content-Length: 218
Content-Type: text/html; charset=iso-8859-1

302 Found

137.78.38.109
National Aeronautics and Space
Administration
Added on 24.09.2012
 Altadena
mipl.jpl.nasa.gov

HTTP/1.0 302 Found
Date: Mon, 24 Sep 2012 17:50:46 GMT
Server: Apache/2.2.21 (Unix) mod_ssl/2.2.21 OpenSSL/0.9.7d DAV/2 PHP/5.3.14
Location: <https://mipl.jpl.nasa.gov/>
Content-Length: 210
Content-Type: text/html; charset=iso-8859-1

SHODAN was 90% HTTP and HTTPS*



* Shodan has massively expanded coverage since my project was started

More Data / More Services

- TCP Services

- FTP, SSH, Telnet
- SMTP, POP3, IMAP
- MySQL
- VNC
- HTTP
- HTTPS

- UDP Services

- SNMP
- NetBIOS
- MDNS
- UPNP
- WDBRPC

SCAN



ALL THE THINGS!

Quick Internet Maths

IPv4 is about four billion IP addresses

- 4Gb of RAM can hold 256 states per IP
- Only 3.2 billion are actually used

Sending a single packet to everything online

- 50,000 pps per cheap server, 24 hours == 4 billion IPs
- \$7 dollars (or less)

Scanning TCP Services

Leverage Nmap 6.0 and NSE support

- Uses `--min-rate=5000 -m 256 --min-host-group=50000 -PS -p`
- Match `--min-rtt-timeout` to `--max-rtt-timeout`

Hacked up the existing Nmap banner.nse script

- Collect raw banners, negotiate telnet, SSL, send probes
- Code: <http://github.com/criticalr/scan-tools/>

Scanning UDP Services

Bare bones UDP blaster

- Take a list of IP addresses from standard input
- Take a packet data file, port, and packet rate
- Spray packets into the ether & print output

Happy with limited processing resources

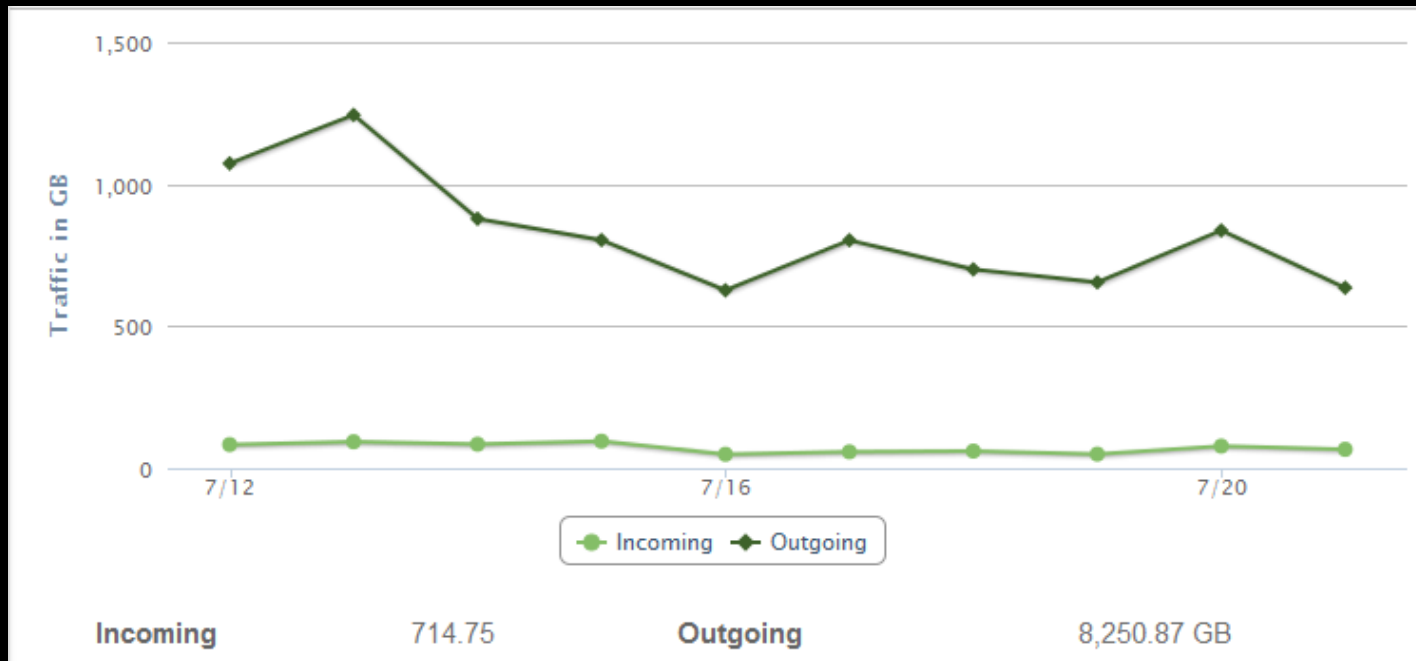
- Runs well on 128Mb RAM VPS nodes in Russia

Scanning UDP Services

Scan the entire Internet with one probe in about 7 hours

Easily push 1.2Gb of traffic per day

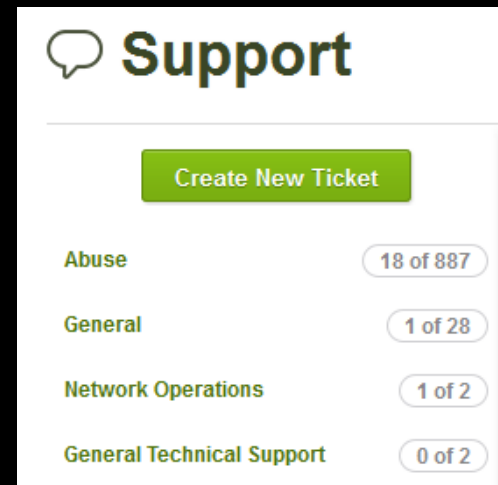
- <http://github.com/criticalr/scan-tools/>



Scanning the Internet Annoys People

Visible on the DShield “top attackers” list

- Over 2,300 abuse complaints to date
- Created an opt-out program: <http://critical.io/>
- 1 of 5 ISPs formally shut me off
- Huge thanks to two ISPs
 - SingleHop.net
 - Linode.com



Please identify your customer operating from the above address at the time mentioned, and terminate immediately his hacking activities. Please prevent him from continuing his hacking activities in the future as well.

Due to the potential severity of this incident, we have reported it to the Computer Emergency Response Team (CERT) in United States (US) and Denmark.

Ironically, since the days you have begun your independent scans we have received a few DDOS attacks using udp_app port 53 traffic.....**any correlation?**

So what your saying is I should just ignore the excessive amount of port snooping coming from your system(s), and I should allow this on your word alone? Since when did you become my big brother? **Are you related to Obama?**

Storage and Processing

Generates about 5Gb of data per day

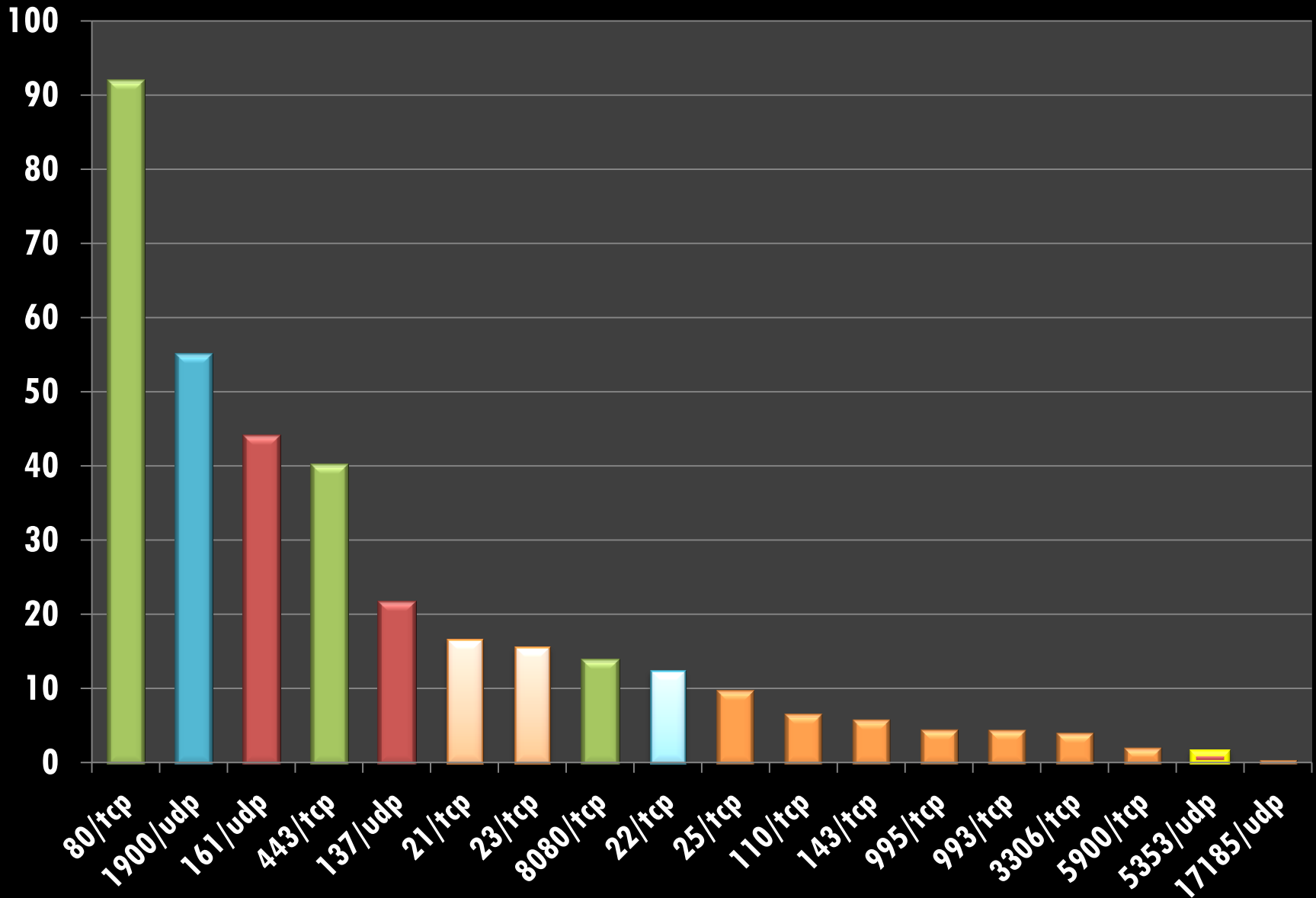
- Around 830GB of raw data over five months
- Normalized to 450GB of Bzip2 record streams

Data is loaded into MongoDB & ElasticSearch

- Mongo: State table of last data for every IP:Port
- Elastic: Every unique record indexed (MD5 data)
- Mongo: Every record on its own

Data Overview

Services Overview



Basic Statistics

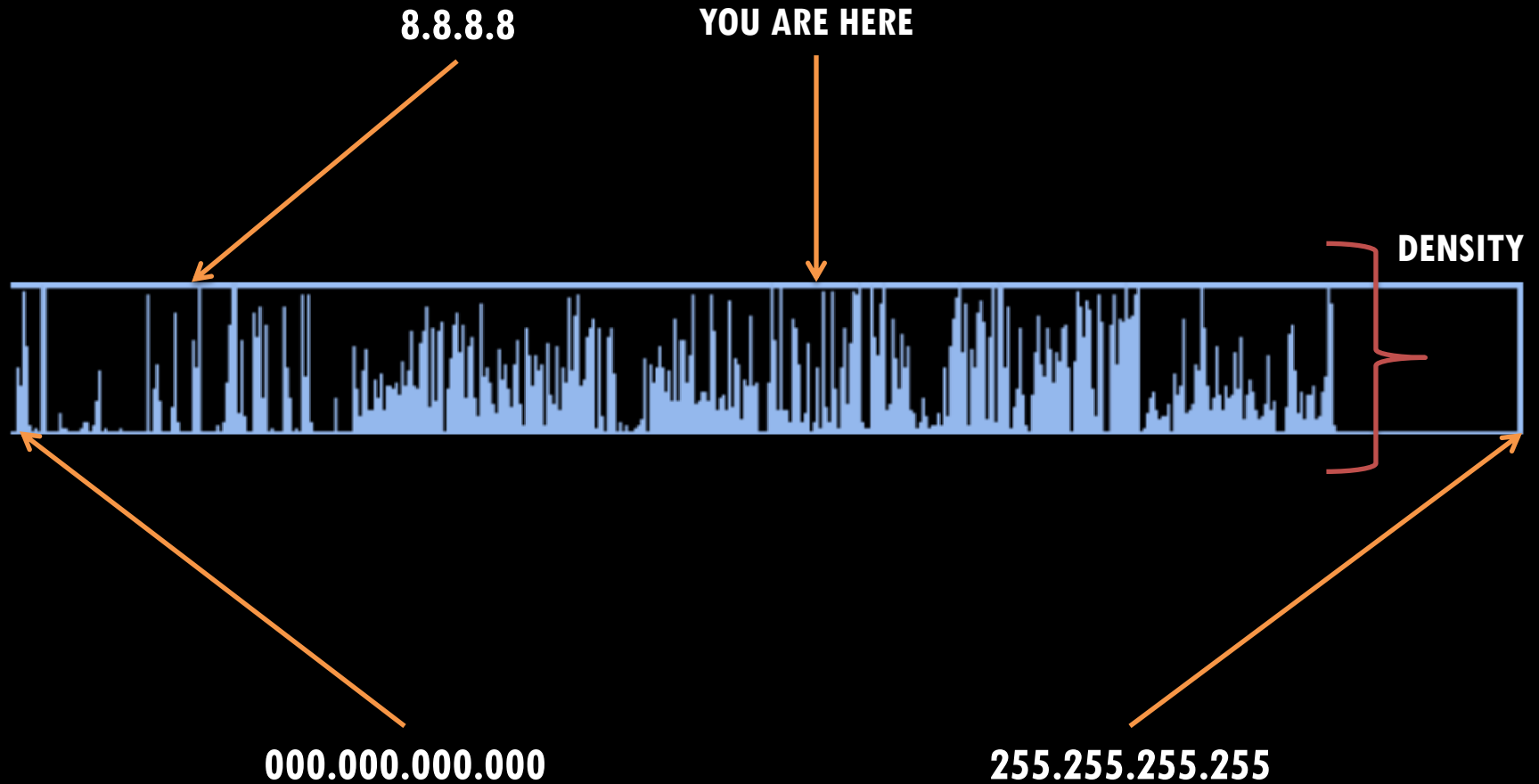
Results obtained for 227 million unique IPs

- Over 550 million unique TCP & UDP service banners
- Scanned ALL addresses for UDP services
- Random sampling for TCP services

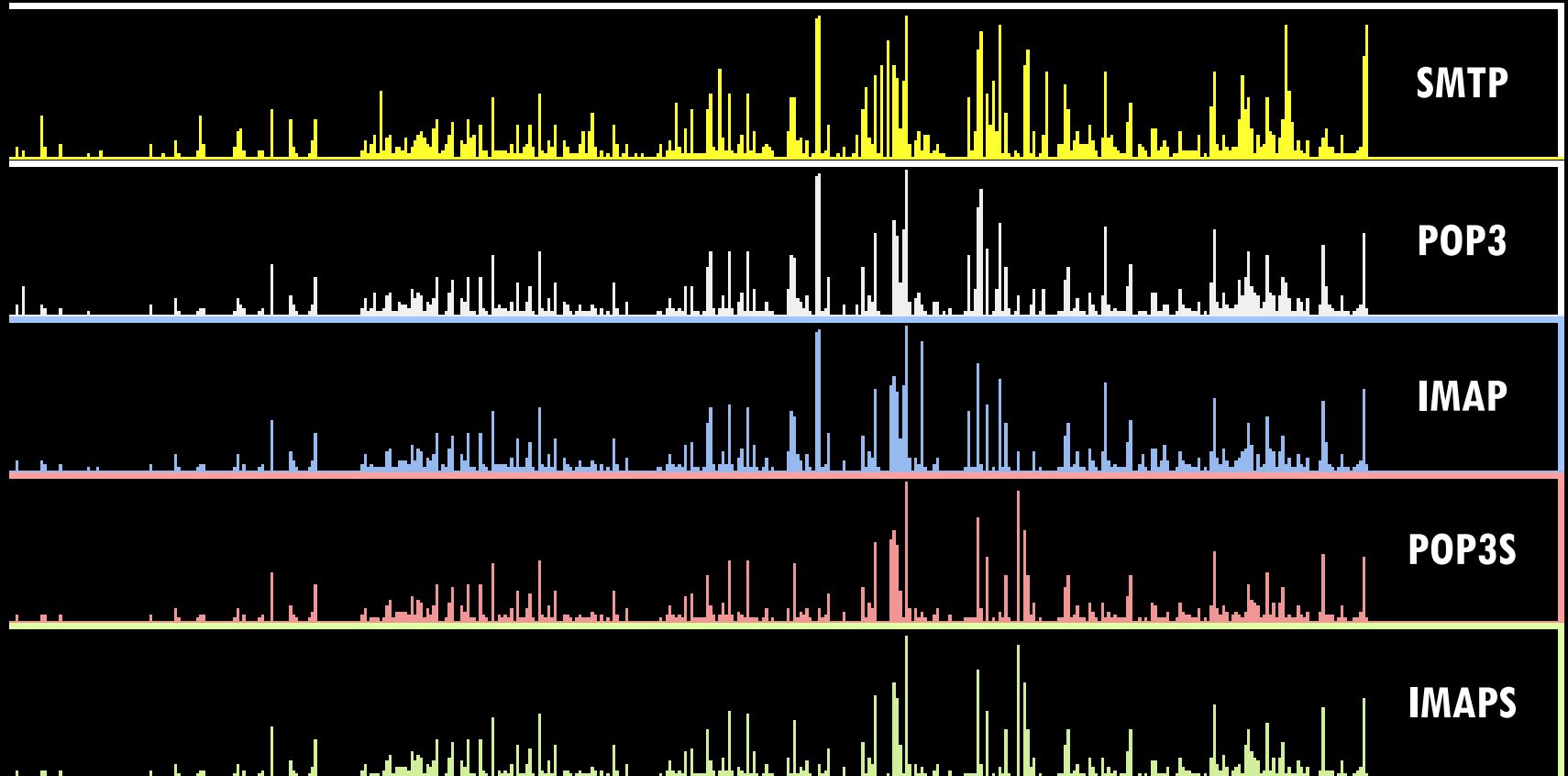
Web services are the most commonly found banner

- 145 million over ports 80, 8080, and 443

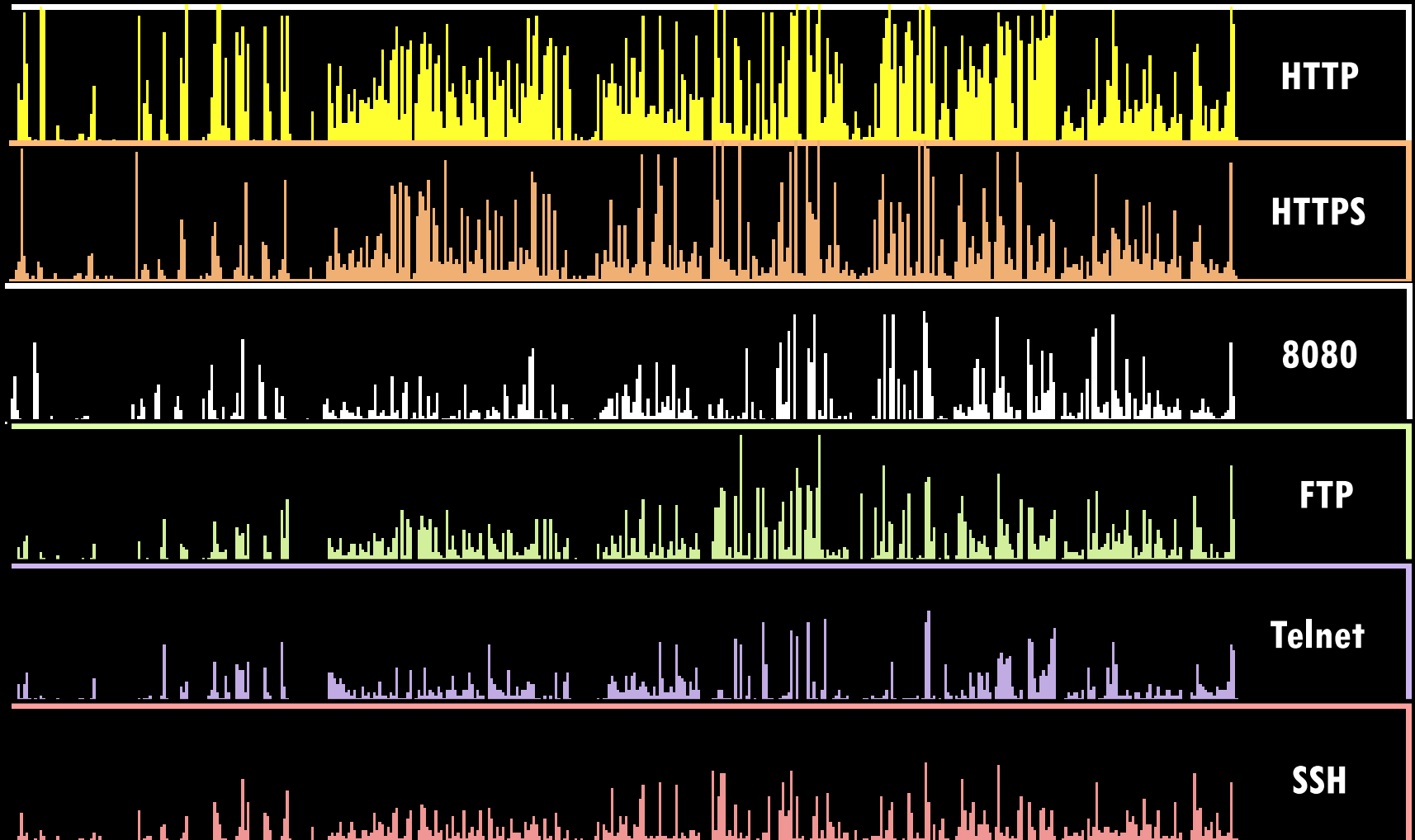
Internet Sparklines



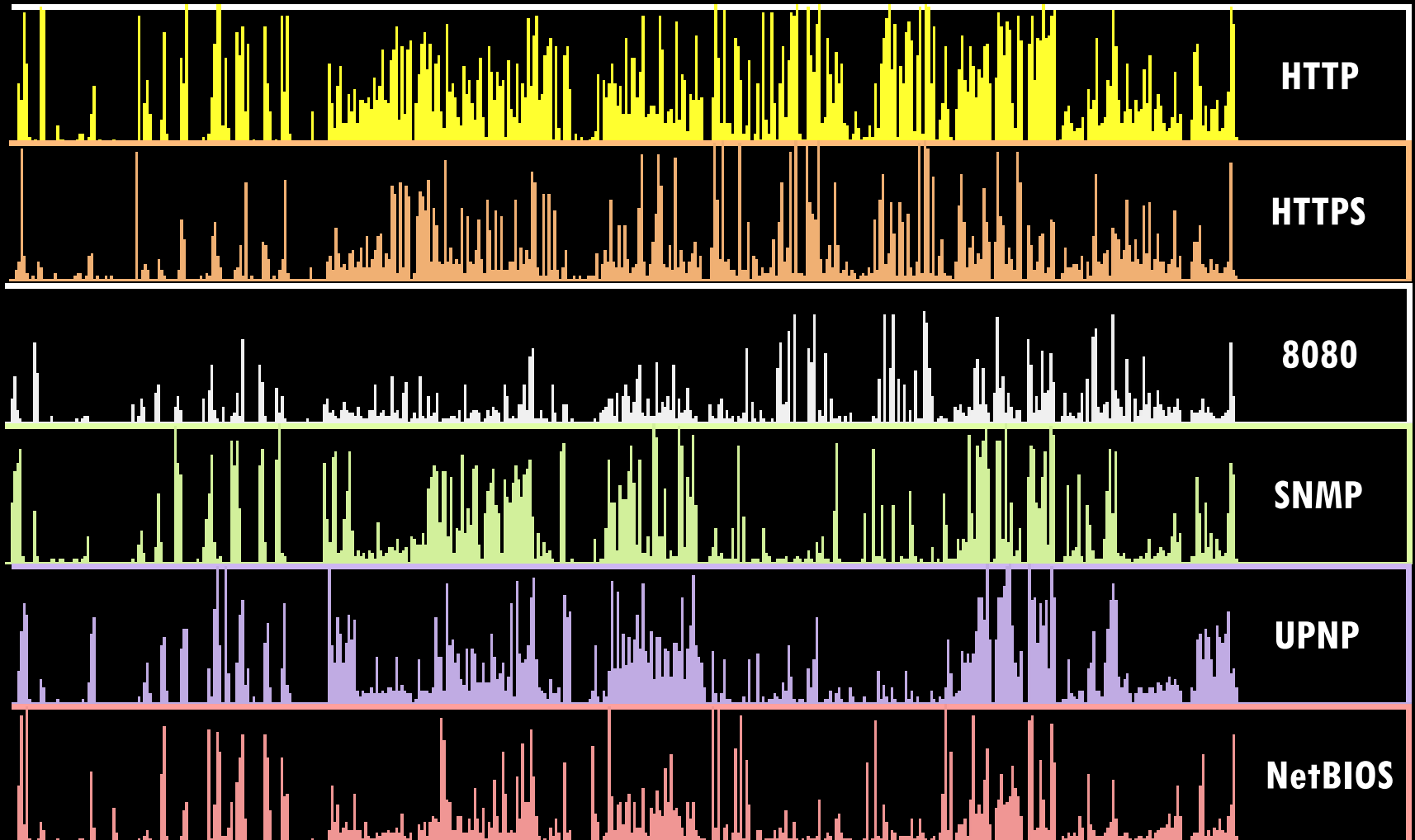
Email Services



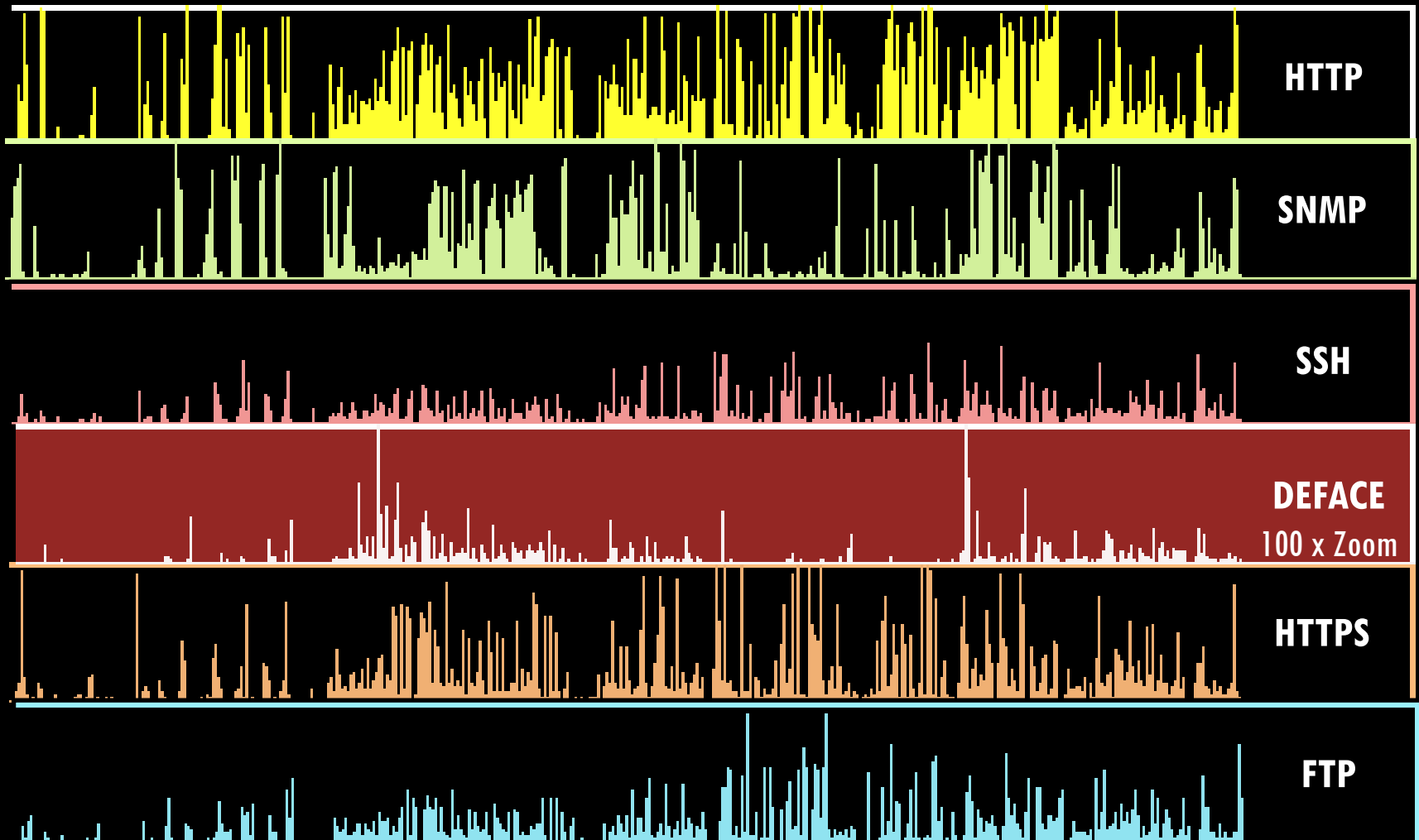
Web, FTP, Telnet, and SSH



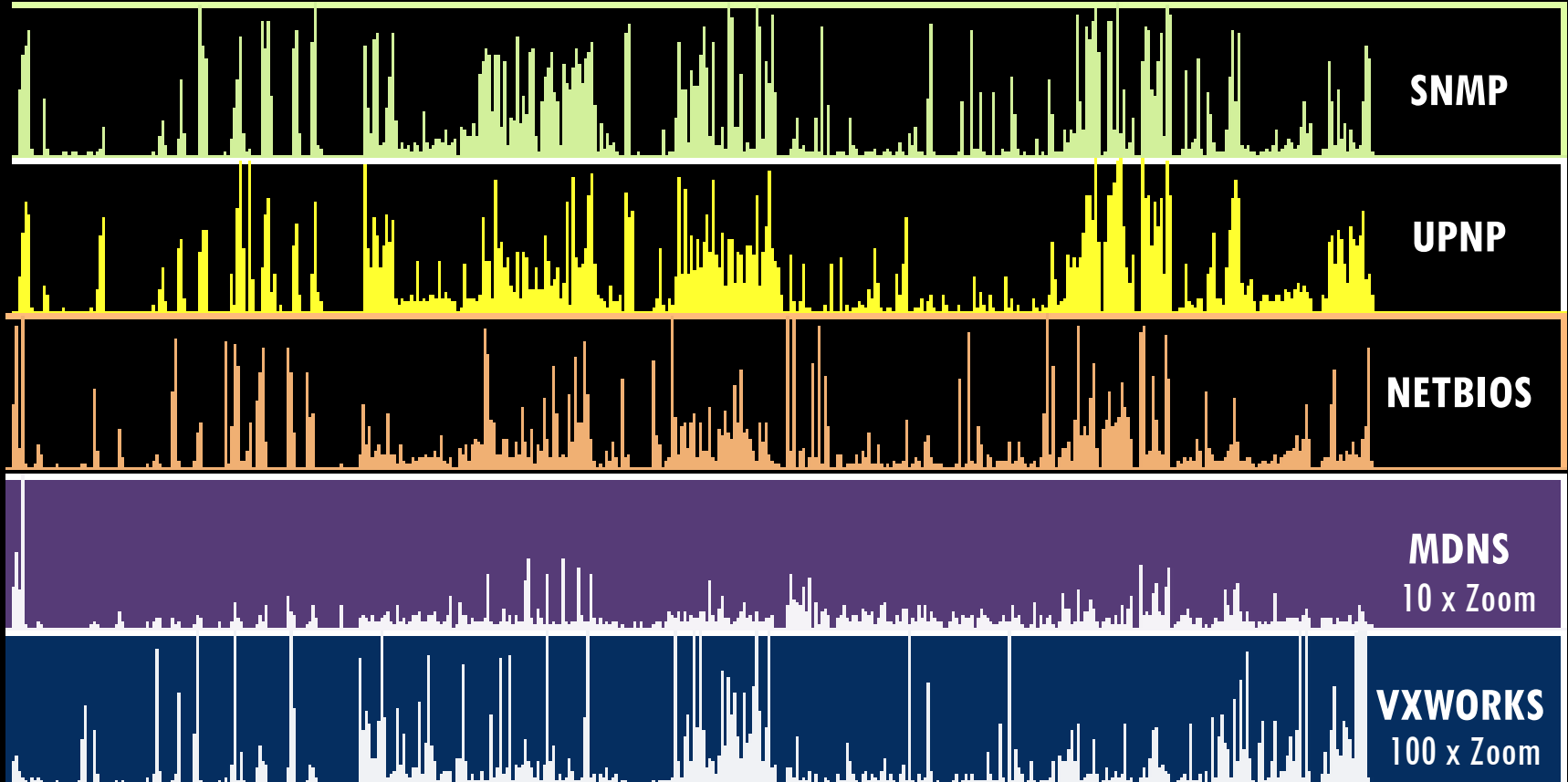
Web, SNMP, UPNP, NetBIOS



Defacements (Zone-H)



UDP Services



VNC vs MySQL vs SMTP vs SSH



Measuring Exposure

SNMP Services

Over 43 million devices expose SNMP with “public”

- Routes, addresses, listening ports
- Running processes and services
- Installed software and patches
- Accounts and group names
- DDoS via amplification

Cisco SNMP Services

Over 268,000 Cisco IOS devices with “public”

Over **18,000** of these with “private”

- Write access provides full control
- Read and write running config
- Extract passwords
- Enable services
- Rootkit
- Sniff

Huawei / H3C Routers

Over 135,000 Huawei/H3C devices exposed via “public”

- Kurt Grutzmacher published an advisory on 2012-10-24
- List usernames and passwords via read-only only comm
- Ignore FX's awesome exploit work for now...

Huawei / H3C Usernames

Sampled 16,065 routers, globally distributed

9842 "admin"	310 "krzysztof"
1862 "root"	310 "confbackup"
1471 "lyzdm"	310 "ciacho"
1471 "lywli"	309 "sb"
1471 "lymr"	309 "michal"
1471 "lyjy"	309 "mateusz"
1470 "lyzwm"	298 "ysnetcom"
1467 "lyys"	264 "lyct"
1460 "jlllyli"	224 "hedongtx"
1429 "lygsg"	223 "lanshan"
1291 "lyjrw"	221 "pingyi"
1276 "lyyys"	221 "lylz"
1261 "lysw"	220 "lzwhb"
1259 "lygmb"	192 "tcnet"
1001 "lyfyh"	192 "szbin"
427 "huawei"	192 "lyzhf"

Huawei / H3C Passwords

Clear Text

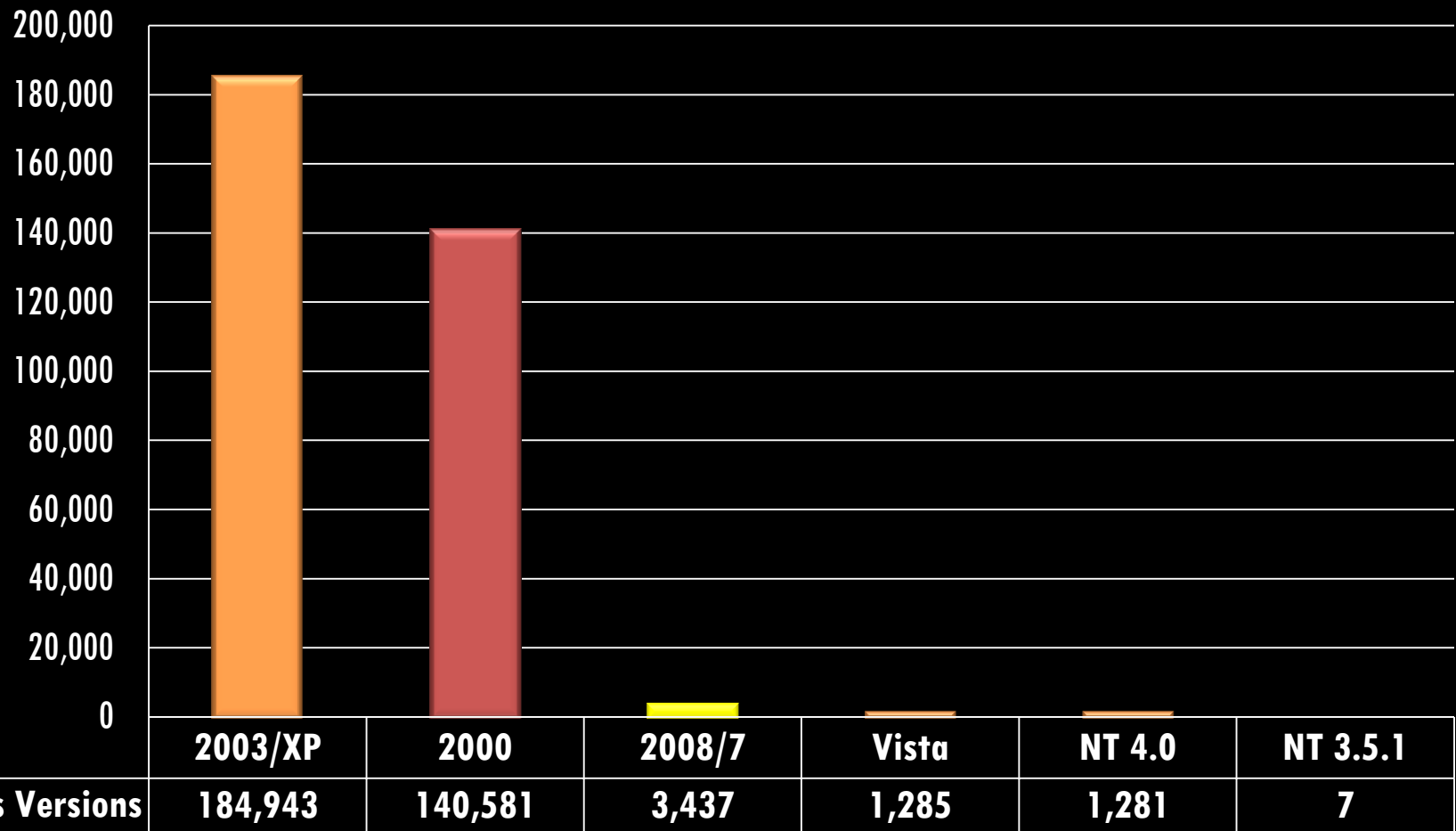
3152 "12345"
2244 "h3capadmin"
363 "xialiang!@#"
349 "nhkhlwlwhz"
334 "admin"
282 "1234"
225 "szwx@ah"
163 "huawei"
154 "itms123456"
147 "AAA888###"
137 "0662"
119 "abc123!"
100 "zch3capadmin"
89 "123456"
87 "apadmin"
78 "password"

Hashed Passwords

866 "_v9@i>_ux)_Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
866 \"T-F-7<]9/7KQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
866 \"RM&/;XGT>L[Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
866 \"PRS.@'[4FG_Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
866 \"99j\\7\\PR:10Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
866 \"\\\"#^0-JaY_COQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
854 \"13&-Z#aG'T)/a!1\$H@GYL\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
850 \"K9F'F&UDZN3Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
831 \"IJ95`F=NXa`Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
819 \"\$2IVD&U[G[Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
813 \"/=X=>T_NU:+Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
779 \"56(AH6*1Z;CQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
777 \"3P;\\Z5\"&[K;Q=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
625 \"13&-Z#aG'T)/a!1\$H@GYA!!\"
621 \"O[[]-LQZ\\]aQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<<\"TX\$_S#6.NM(0=0\\)*5WWQ=^Q`MAF4<1!!\"
604 \"_v9@i>_ux)_Q=^Q`MAF4<1!!\"
604 \"RM&/;XGT>L[Q=^Q`MAF4<1!!\"
604 \"PRS.@'[4FG_Q=^Q`MAF4<1!!\"
604 \"99j\\7\\PR:10Q=^Q`MAF4<1!!\"
604 \"\\\"#^0-JaY_COQ=^Q`MAF4<1!!\"
600 \"T-F-7<]9/7KQ=^Q`MAF4<1!!\"
600 \"\$2IVD&U[G[Q=^Q`MAF4<1!!\"
578 \"K9F'F&UDZN3Q=^Q`MAF4<1!!\"
497 \"56(AH6*1Z;CQ=^Q`MAF4<1!!\"

Windows SNMP Services

Analysis of 332,538 Windows Systems



Windows SNMP Service Arguments

Over 1000 passwords found exposed via “public” SNMP

- Database drivers, email clients, point of sale
- Retail, B2B, and e-commerce

```
1 : "username=sa password=Masterkey2011 LicenseCheck=Defne"
1 : "DSN=sms;UID=XXX;PWD=XXXsys; DSN=GeoXXX;UID=XXX;PWD=XXXsys; 8383 1"
1 : "-password h4ve@gr8d3y"
1 : " --daemon --port 8020 --socks5 --s_user Windows --s_password System"
1 : "/XXXX /ssh /auth=password /user=admin /passwd=admin_p@s$word"
1 : "a.b.c.d:3389 --user administrator --pass passw0rd123"
1 : "a.b.c.d:3389 --user administrator --pass Password"
2 : "http://a.b.c/manage/retail_login.php3?ms_id=14320101&passwd=7325"
```

UPNP Services

Over 54 million devices respond to UPNP / SSDP probes

- Close to a dozen unique UPNP SDKs represented
- Quite a few expose the SOAP service externally
- Almost half based on the Intel SDK (1.2)
- A major gap in security auditing

VxWorks Debug Service

Remote debug service on UDP port 17185

- Exposes hundreds of different devices
- VoIP phones, routers, planes, spacecraft
- Read, write, execute memory
- Over 250,000 found in July of 2010...

2012: **200,000**

Obtaining IP Address...



© 2005 i2 Link Systems, Inc.
All Rights Reserved

MySQL Exposed

Approximately 3 million MySQL servers found

- About half of these have no host ACLs
- 1.5 million exposed to password attacks
- Vulnerable to known flaws
- Authentication bypass

MySQL Authentication Bypass

Estimating the impact of authentication bypass

- Requires specific versions and architectures
- Combined versions with OS fingerprint
- Around **90,000** servers vulnerable (August 15th 2012)
- Instant data loss

F5 BigIP SSH Exposure

A total of 13,500 BigIP appliances identified

- Over 50% of these configured with SSH open
- Static and exposed SSH private key
- Remote root in one SSH attempt
- Published June 6th, 2012

F5 BigIP SSH Exposure

Scanned these with the `ssh_identify_pubkeys` module

- Does a “half-auth” using the public key only
- Does not actually attempt authentication
- **721 machines** still exposed (2012-08-15) [10%]

Randomness

NetBIOS Services

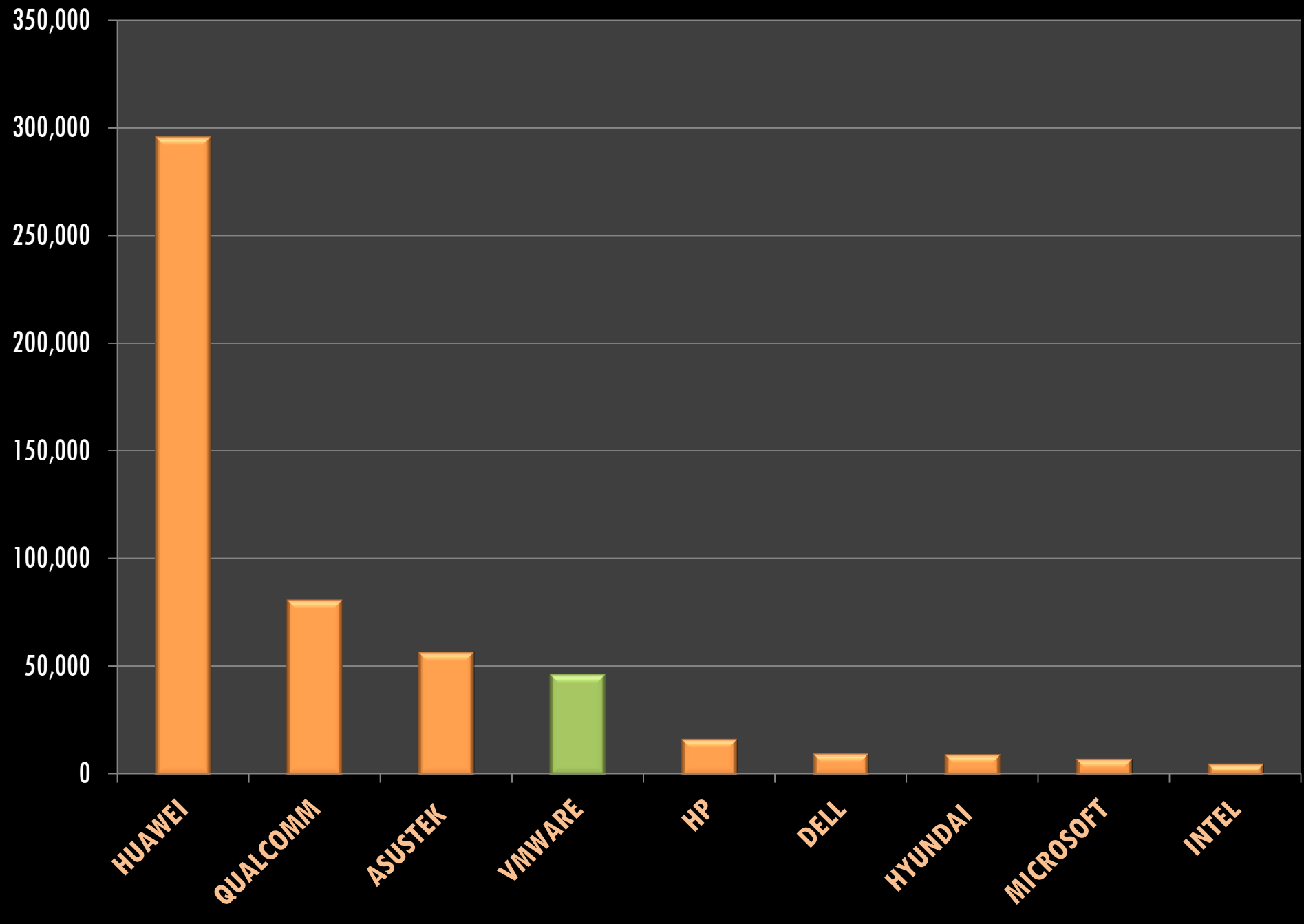
NetBIOS (137/udp) responses incredibly useful

- Exposes system name and domain name
- MAC address & interface detection

Over **21 million** NetBIOS services found

- MACs are globally unique? Right?

Duplicate MAC Addresses by Vendor



NetBIOS MAC Addresses

Duplicate MACs also used for dial-up connections

- 00:53:45:00:00:00 is Windows XP
- 44:45:53:54:42:00 is Windows 98

Results 1 - 10 of about 32101 for port:137 00:53:45:00:00:00

95.221.83.51

Net By Net Holding LLC

Added on 12.09.2012



Moscow

[Details](#)

NetBIOS Response

Servename: FBI-E20E67C8B6C

MAC: 00:53:45:00:00:00

HTTP Cookie Repetition

HTTP session cookies are generally unique

- Are these unique across 145m servers?
- Mostly...

25	ASPSESSIONIDCARCTTQQ	APPKDOOAEH0EIPJJIFPKHAGI
25	ASPSESSIONIDCARCTTQQ	LOELDOOALLKGBBDDKKIMNBPCA
26	ASPSESSIONIDCARCTTQQ	EDCLDOOAPCBIBMCFBGCOLCMH
133	ASPSESSIONIDQACDDRAQ	NMELPFDCKCAKKNPAAHIDCICMJ
296	ASPSESSIONIDAATTDQBT	FGMAJHOAJJEAGLFNFJKFDANP

Duplicate Cookies = Security Issues

More broken cookies

- Ruby on Rails and Rack
- Python's Twisted Framework

58	rack.session	BAh7BjoOX19GTEFTSF9fewA%3D%0A
54	__Federal_session	BAh7BilKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcj
3	TWISTED_SESSION	f8de4a91e96417ad61fd2a6cc3b8ef85
4	TWISTED_SESSION	170ce9e0f1718e940aaf9456d3ef52a6
4	TWISTED_SESSION	755e9c715d5fdfdeb750864ae3b82ee1
4	TWISTED_SESSION	7a07e0d0babaeff72c5655eaebea45d7
5	TWISTED_SESSION	06d804074586da3252d19a53c82b2f85
5	TWISTED_SESSION	3cf983f5596c034576066f1495db18fa
5	TWISTED_SESSION	64747149955706972aeff4aaa8826646
5	TWISTED_SESSION	ee57575fa42eaaf719f9bc1496830973

HTTP Cookies from Embedded Devices

Cable & ADSL Modem

7	rg_cookie_session_id	633223718
7	rg_cookie_session_id	679341132
8	rg_cookie_session_id	278907688
9	rg_cookie_session_id	1567459416
10	rg_cookie_session_id	2111951218

Cisco Application Control Engine

20	ACE_COOKIE	R3834094051
23	ACE_COOKIE	R3834058114
52	ACE_COOKIE	R1627792095
65	ACE_COOKIE	R1318094141
103	ACE_COOKIE	R3283128030
130	ACE_COOKIE	R3283163967

More Odd Duplicates

• 85.111.21.17	1341054537	PHPSESSID=63-bc793a3c54473b008fae521fc328fe0f-cf9139d54445c8957e750210ba377b2e
• 61.122.213.22	1341056470	sid=cf9139d54445c8957e750210ba377b2e
• 220.158.68.208	1341058809	sid=cf9139d54445c8957e750210ba377b2e
• 117.109.247.83	1341063277	sid=cf9139d54445c8957e750210ba377b2e
• 133.5.138.13	1341074475	sid=cf9139d54445c8957e750210ba377b2e
• 217.114.76.220	1341096516	cf9139d54445c8957e750210ba377b2e=4gioab4am9auv4qv3glshedbdmq08aa1k
• 116.0.236.183	1341102102	sid=cf9139d54445c8957e750210ba377b2e
• 221.133.80.197	1341103294	sid=cf9139d54445c8957e750210ba377b2e
• 61.89.16.61	1341116604	sid=cf9139d54445c8957e750210ba377b2e
• 221.246.228.28	1341119469	sid=cf9139d54445c8957e750210ba377b2e
• 120.51.194.113	1341126768	sid=cf9139d54445c8957e750210ba377b2e
• 157.82.132.14	1341144508	sid=cf9139d54445c8957e750210ba377b2e
• 173.192.168.113	1341143853	0b2c2ec429192f7eb70429aa3a2da9b1=cf9139d54445c8957e750210ba377b2e
• 180.61.68.126	1341145575	sid=cf9139d54445c8957e750210ba377b2e
• 85.111.21.13	1341147049	PHPSESSID=63-14b42c0bffe71dff9bf74567842c425-cf9139d54445c8957e750210ba377b2e
• 119.47.102.10	1341151661	sid=cf9139d54445c8957e750210ba377b2e
• 133.54.155.204	1341158575	sid=cf9139d54445c8957e750210ba377b2e
• 77.55.75.209	1341171169	cf9139d54445c8957e750210ba377b2e=ef8fa6bcc8dda8d5121557994715c27

More Odd Duplicates

• 85.111.21.17	1341054537	PHPSESSID=63-bc793a3c54473b008fae521fc328fe0f-cf9139d54445c8957e750210ba377b2e
• 61.122.213.22	1341056470	sid=cf9139d54445c8957e750210ba377b2e
• 220.158.68.208	1341058809	sid=cf9139d54445c8957e750210ba377b2e
• 117.109.247.83	1341063277	sid=cf9139d54445c8957e750210ba377b2e
• 133.5.138.13	1341074475	sid=cf9139d54445c8957e750210ba377b2e
• 217.114.76.220	1341096516	cf9139d54445c8957e750210ba377b2e=4gioab4am9auv4qv3glshedbdmq08aa1k
• 116.0.236.183	1341102102	sid=cf9139d54445c8957e750210ba377b2e
• 221.133.80.197	1341103294	sid=cf9139d54445c8957e750210ba377b2e
• 61.89.16.61	1341116604	sid=cf9139d54445c8957e750210ba377b2e
• 221.246.228.28	1341119469	sid=cf9139d54445c8957e750210ba377b2e
• 120.51.194.113	1341126768	sid=cf9139d54445c8957e750210ba377b2e
• 157.82.132.14	1341144508	sid=cf9139d54445c8957e750210ba377b2e
• 173.192.168.113	1341143853	0b2c2ec429192f7eb70429aa3a2da9b1=cf9139d54445c8957e750210ba377b2e
• 180.61.68.126	1341145575	sid=cf9139d54445c8957e750210ba377b2e
• 85.111.21.13	1341147049	PHPSESSID=63-14b42c0bffe71dff9bf74567842c425-cf9139d54445c8957e750210ba377b2e
• 119.47.102.10	1341151661	sid=cf9139d54445c8957e750210ba377b2e
• 133.54.155.204	1341158575	sid=cf9139d54445c8957e750210ba377b2e
• 77.55.75.209	1341171169	cf9139d54445c8957e750210ba377b2e=ef8fa6bcc8dda8d5121557994715c27

HTTP ETag Header

The ETag header in HTTP/1.1 identifies unique content

- Browsers check this against their cache to save bandwidth
- ETag generation is not specified by the RFC
- Most ETags are unique

HTTP ETag Duplication

Duplicate ETag values predict identical content

46467	"f4b198fff9fcc81:0"	IIS 7.0
38658	"3a24cbe86088cb1:0"	IIS 7.5
34879	"083b42ac730cc1:0"	IIS 7.5
31997	"-518385442"	KL DSL Modem
30307	"153-48d2e9eea2640"	Apache
17550	"3d00a8-2c-3e9564c23b600"	Apache
15117	"dd8094-2c-3e9564c23b600"	Apache
13039	"94a519-a7-4ba744b4aab40"	Apache
12379	"4013-585-603a4ec0"	Apache
11091	"3685c3-b1-4b7b54582b480"	Apache
11020	"7b8027-8b-4a76d6b668f80"	Apache
10181	"8080c09dde19c51:5897"	IIS 6.0
9745	"15bd5-e1-4a40c24b13a40"	Apache

Web Server Header Popularity

Examining 35 of 200 million web server records

```
8124109 RomPager/4.07 UPnP/1.0
3968077 AkamaiGHost
2828545 Apache
2064499 nginx/1.0.11
1673137 micro_httpd
1230114 Apache/2.2.3 (CentOS)
1214596 GoAhead-Webs
958521 Microsoft-IIS/6.0
597482 RomPager/4.51 UPnP/1.0
552849 cisco-IOS
437144 Microsoft-IIS/7.5
403239 Microsoft-HTTPAPI/2.0
379864 httpd
349979 mini_httpd/1.19 19dec2003
336207 Mini web server 1.0 ZTE corp 2005.
```


Powered-by Popularity

18127	PHP/4.3.2-RC1
15923	ASP.NET
5340	Servlet/2.5 JSP/2.1
3322	Express
2133	Servlet/2.4 JSP/2.0
1112	PHP/4.3.4
339	PHP/5.3.10
282	PHP/5.2.17
263	PHP/5.2.3
263	PHP/4.3.3
194	PHP/4.3.1
168	PHP/5.1.6
163	Servlet 2.5; JBoss-5.0/JBossWeb-2.1
120	HPHP web server records

Powered-by Hilarity

“Economic growth, fair trade coffee and the letter T”

“The Red Badger Team”

“Secret Namics rocket technology”

“Bananas and Rum”

“Teeny Tiny Organic Cage Free Hamsters”

Summary

Conclusions

- A global perspective helps identify unknown vulnerabilities
- Internet-wide reconnaissance is cheap and relatively easy
- The Internet as a whole is not in a healthy condition
- Entropy problems can be identified through large data sets

Questions?

Thanks!

Email	<code>hdm@rapid7.com</code>
Twitter	<code>@hdmoore</code>
IRC	<code>hdm@freenode</code>