The Wild West

DerbyCon 2012

HD Moore

RAPID7

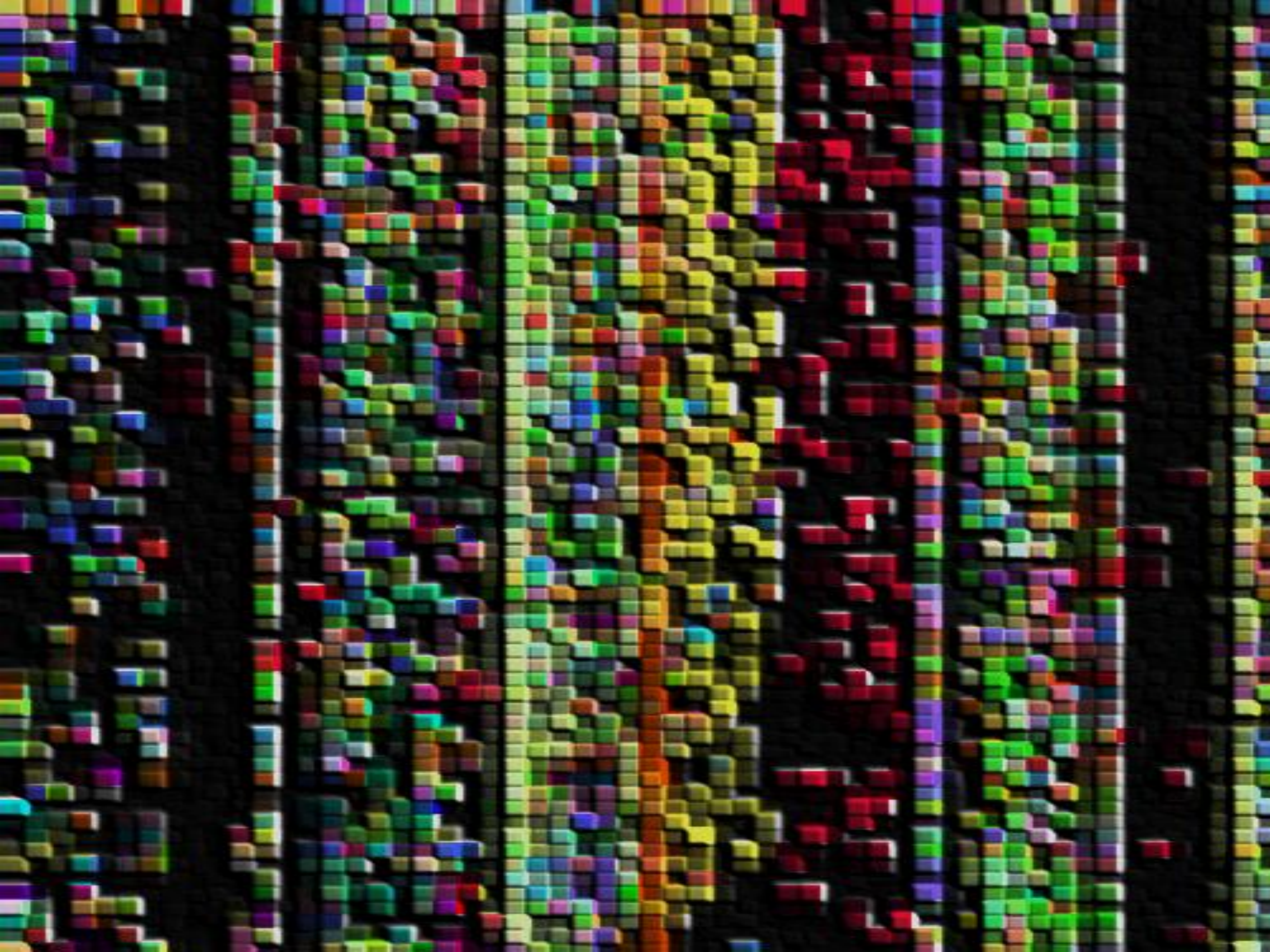
Credit: http://www.flickr.com/photos/flowers-of-the-sea/7044155641/

Credit: http://www.flickr.com/photos/cld/15103741/

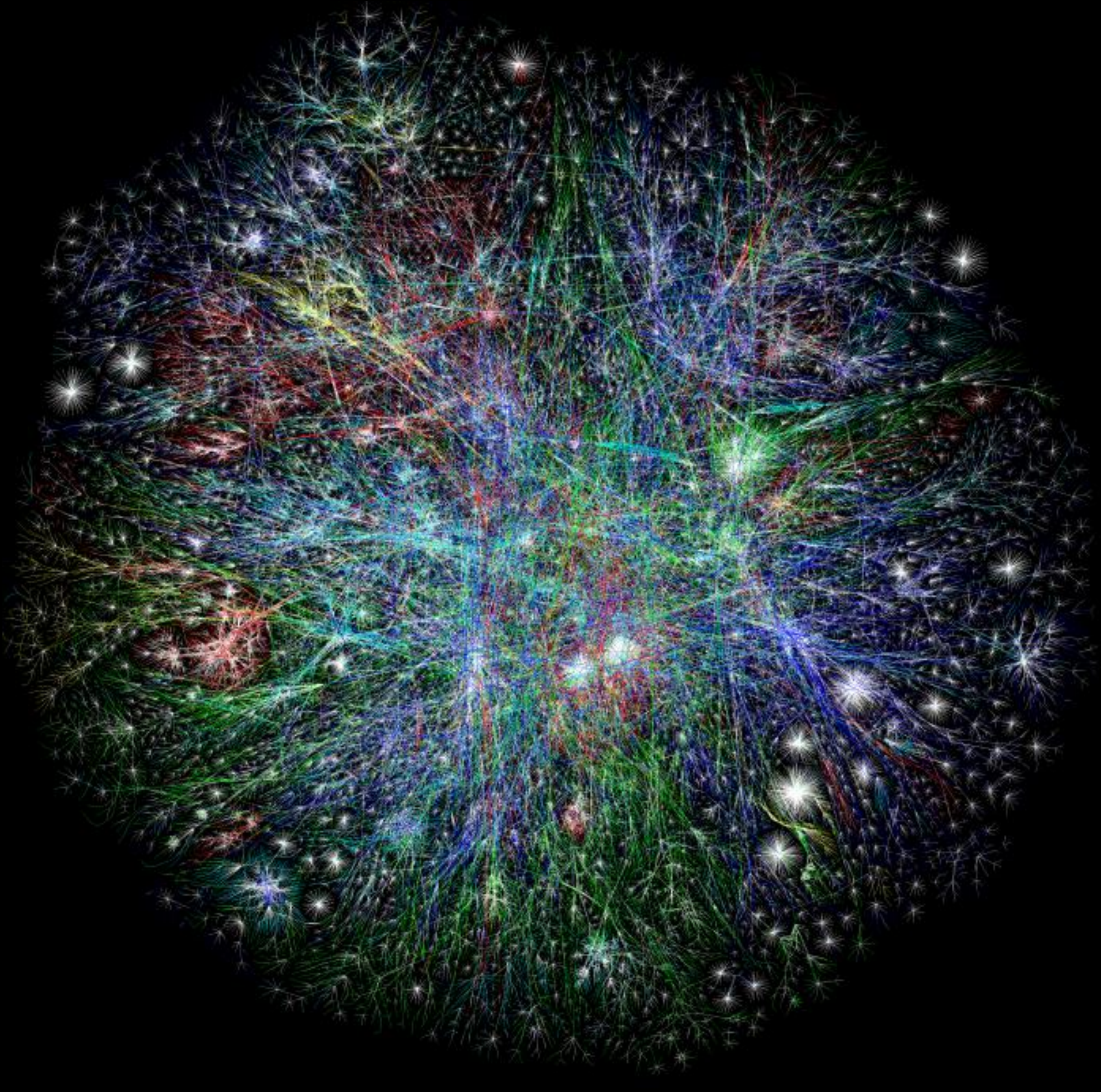
Otis
EMERGENCY STOP
RUN
EMERGENCY OPERATION
LIGHT SWITCH
ON

Credit: http://www.flickr.com/photos/nomadic_lass/6469849701/

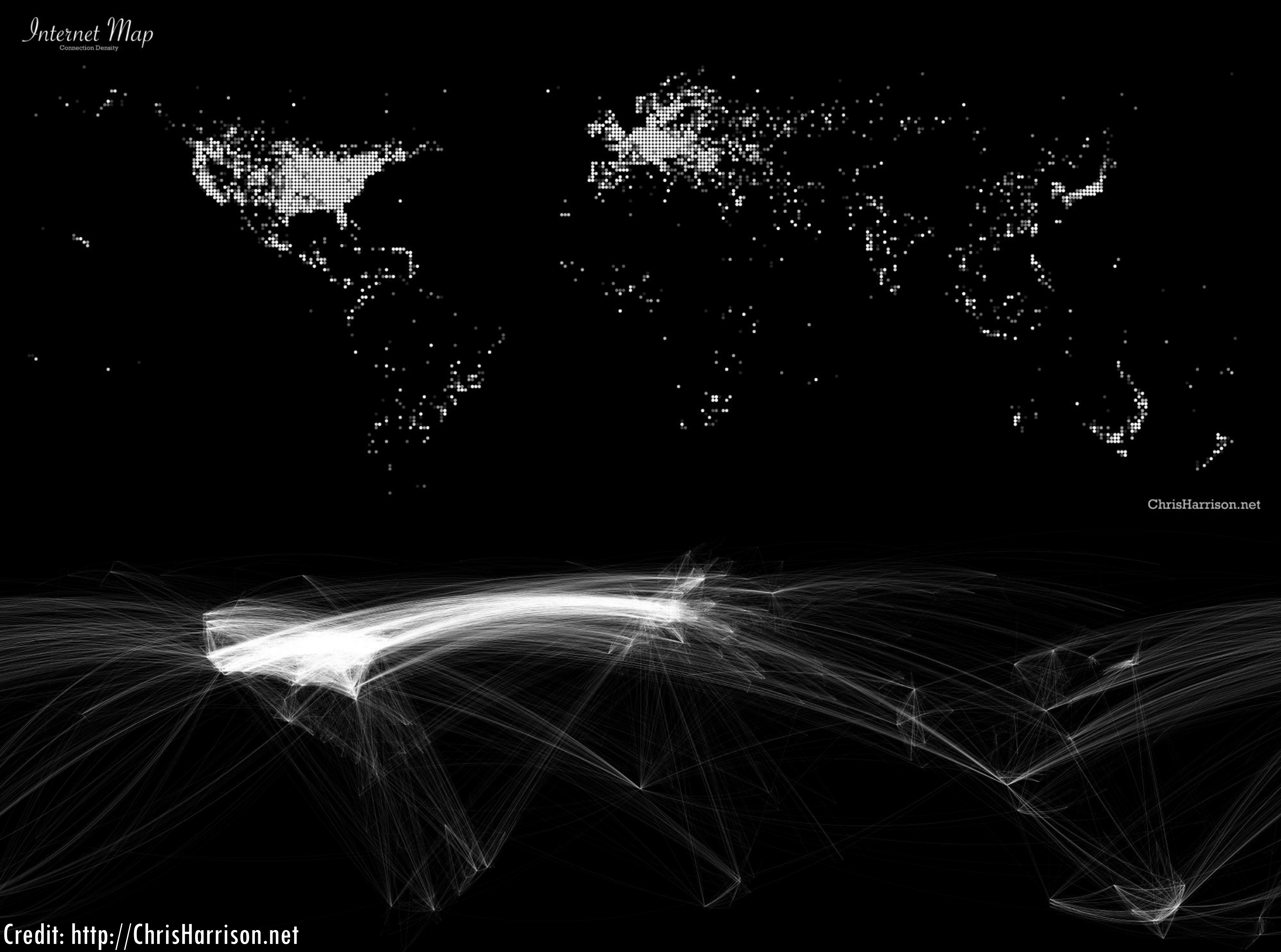
Credit: http://www.flickr.com/photos/getbutterfly/6317955134/



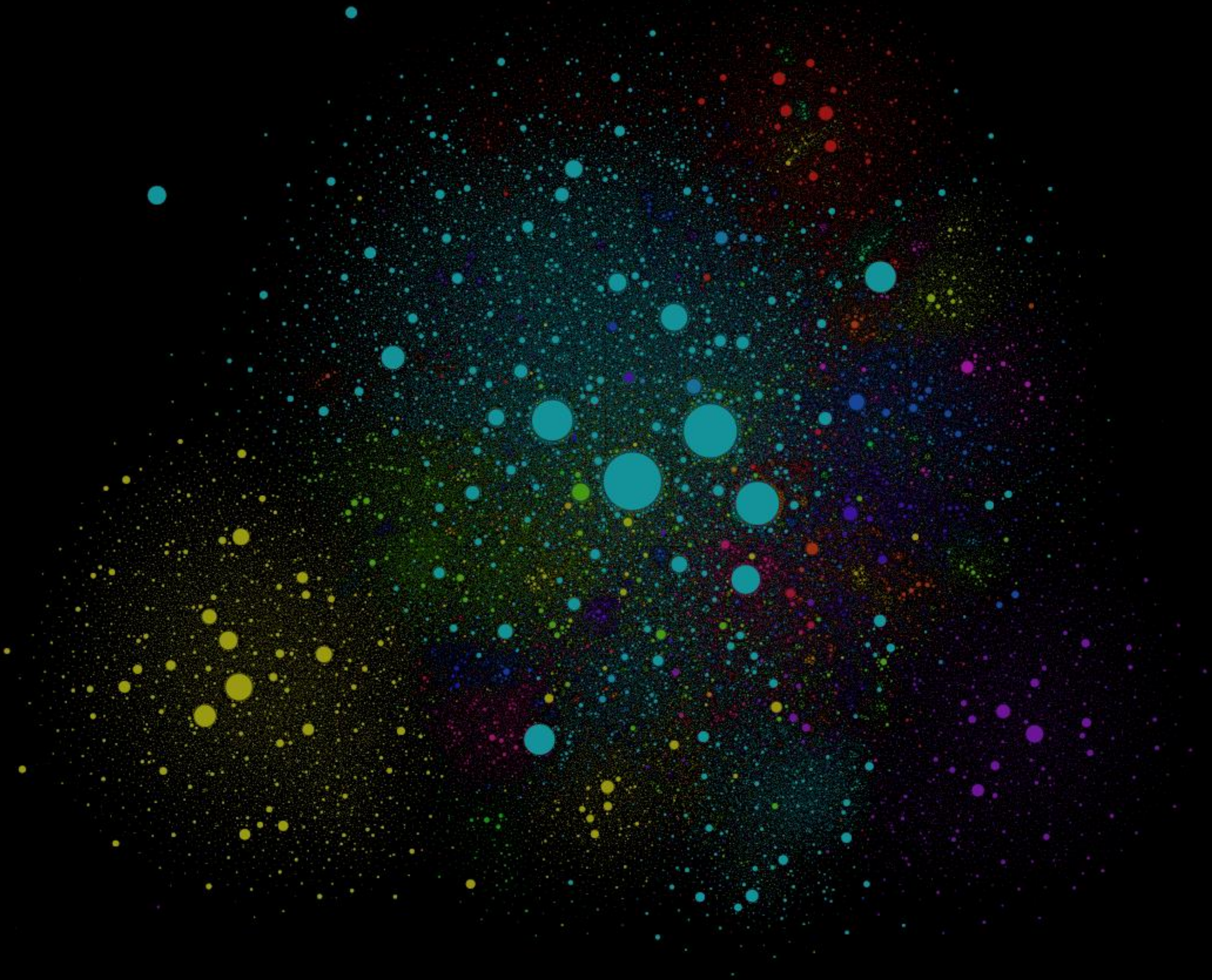
Credit: http://www.flickr.com/photos/cali4beach/7637828650/



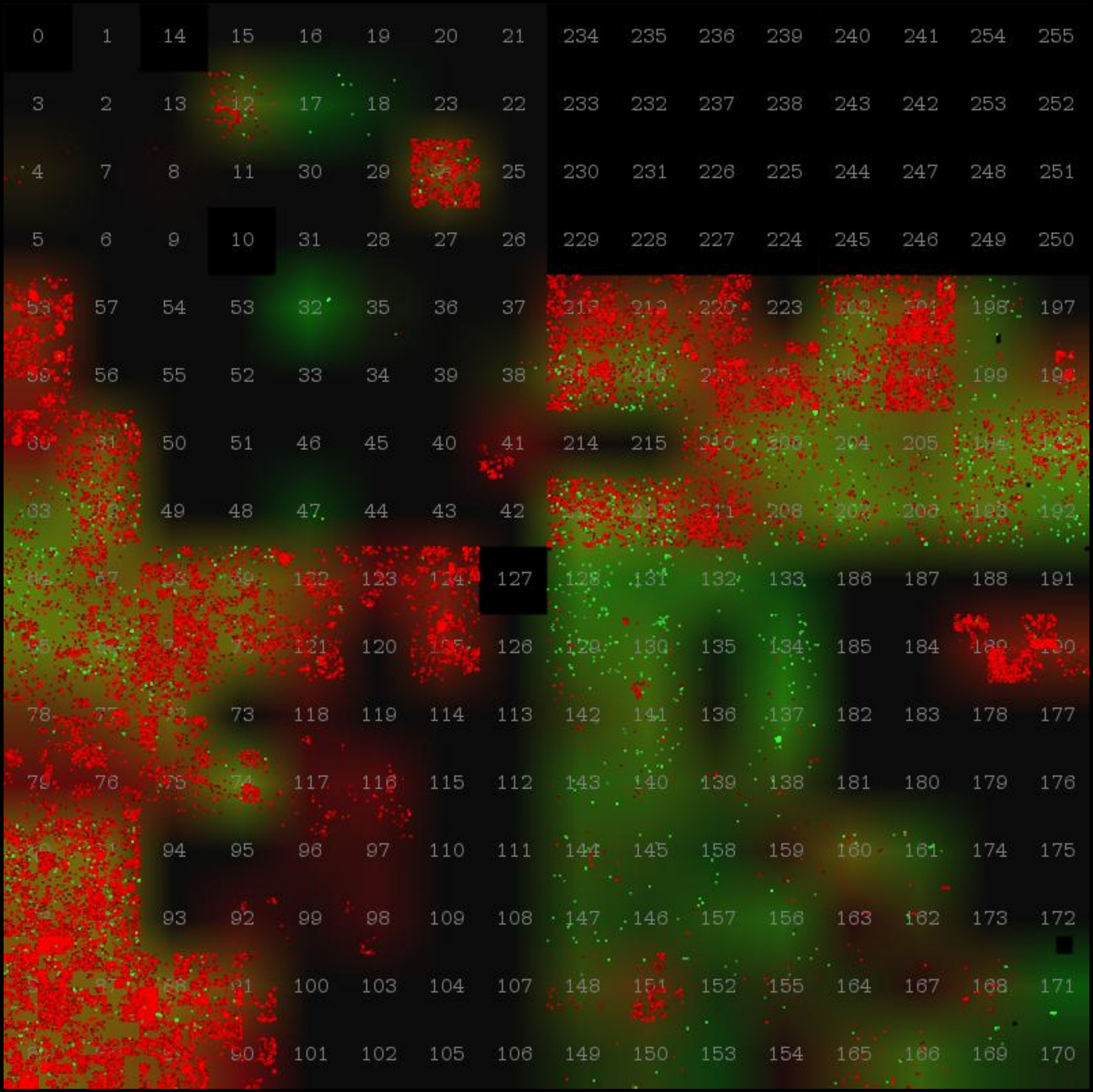
Credit: http://www.opte.org/maps/



Credit: http://ChrisHarrison.net



Credit: http://internet-map.net/



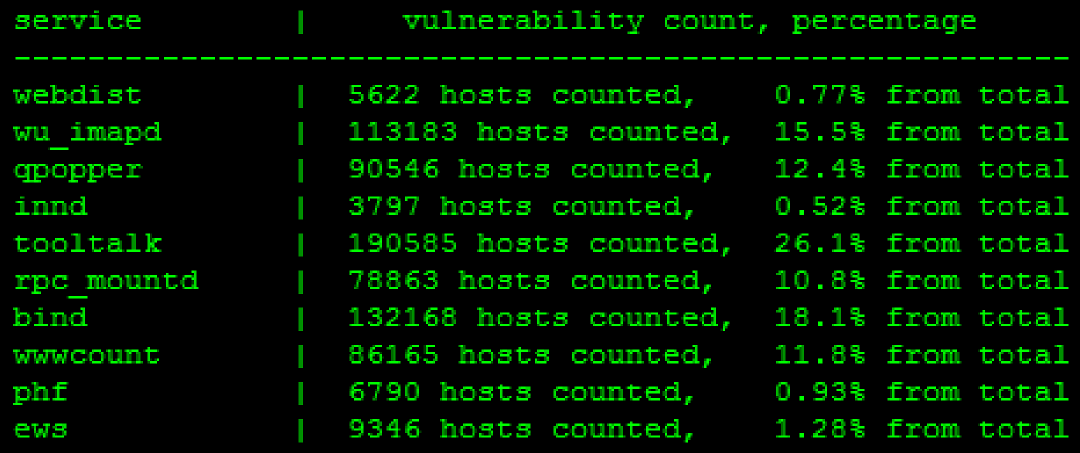
Credit: http://www.seehuhn.de/pages/internet

Credit: http://www.opte.org/maps/ (magnified)

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



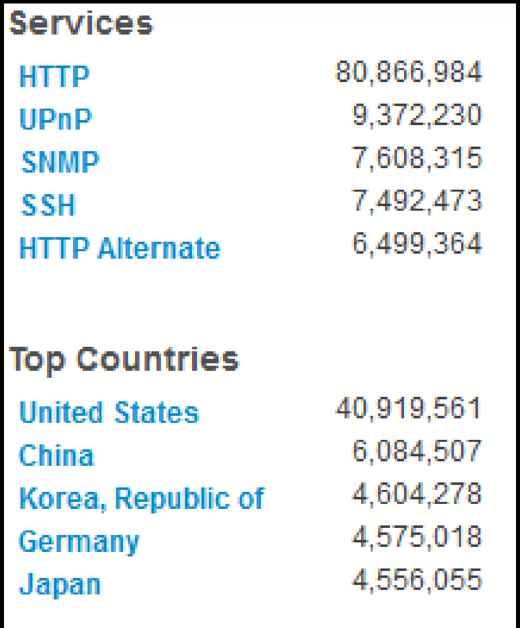
```
service         |     vulnerability count, percentage
---------------------------------------------------------
webdist         |  5622 hosts counted,    0.77% from total
wu_imapd        |  113183 hosts counted,  15.5% from total
qpopper         |  90546 hosts counted,   12.4% from total
innd            |  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
```

IAP / BASS: http://www.decuslib.com/decus/vmslt99a/sec/bass.txt

Modern

2010+ – SHODAN: The computer search engine

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

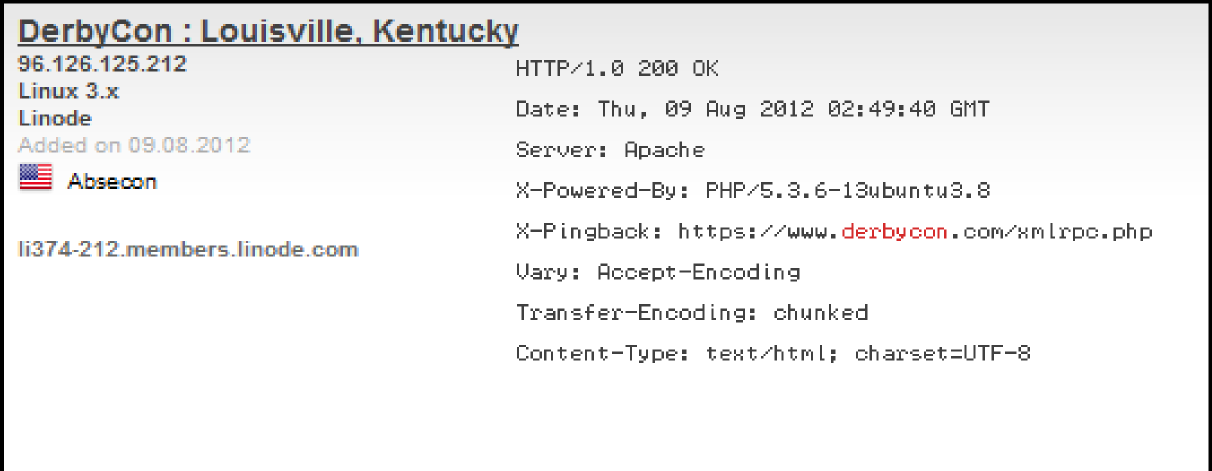


Services

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



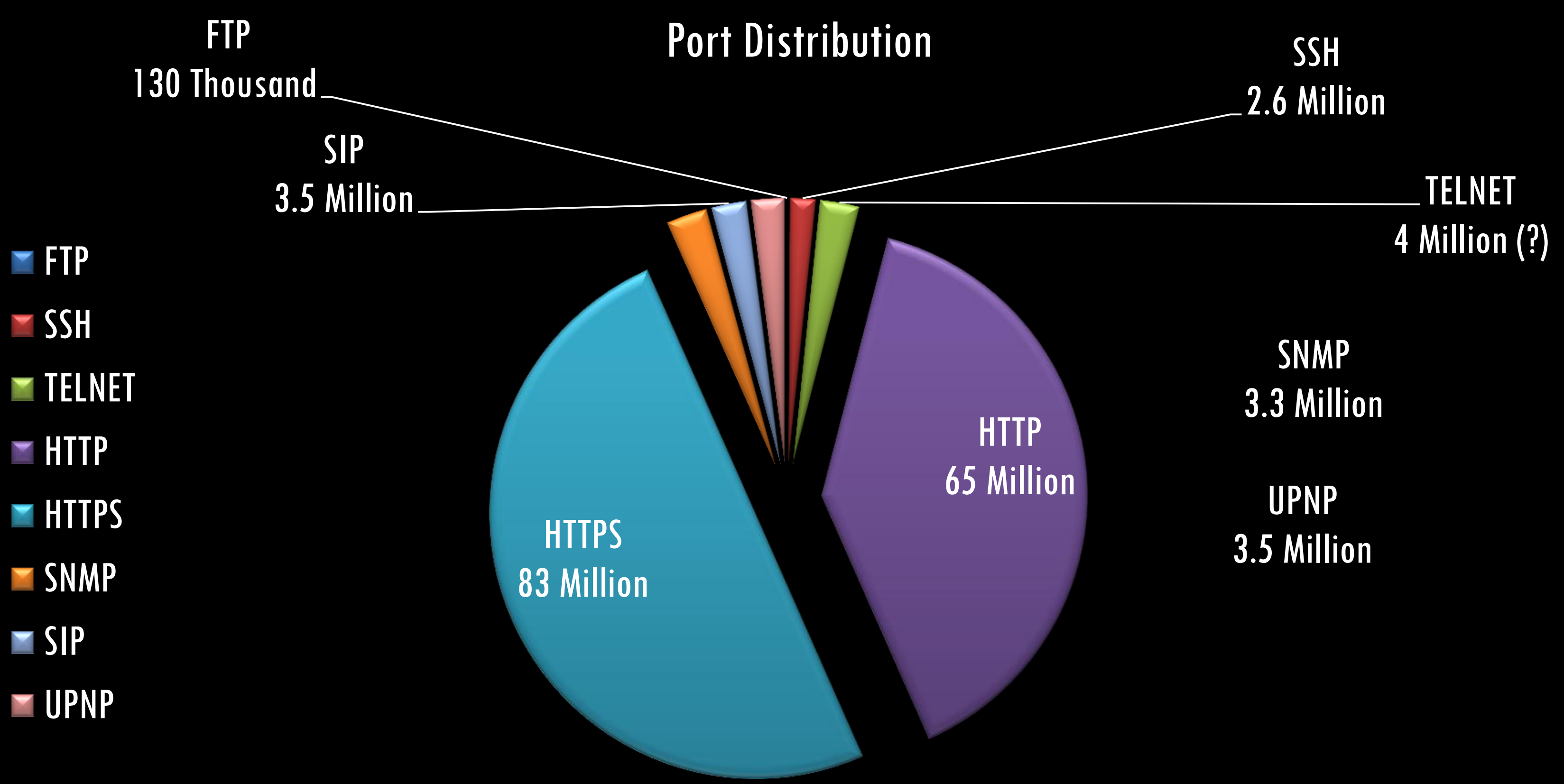
DerbyCon : Louisville, Kentucky

96.126.125.212
Linux 3.x
Linode
Added on 09.08.2012
Absecon

li374-212.members.linode.com

```
HTTP/1.0 200 OK
Date: Thu, 09 Aug 2012 02:49:40 GMT
Server: Apache
X-Powered-By: PHP/5.3.6-13ubuntu3.8
X-Pingback: https://www.derbycon.com/xmlrpc.php
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

SHODAN was 90% HTTP and HTTPS*

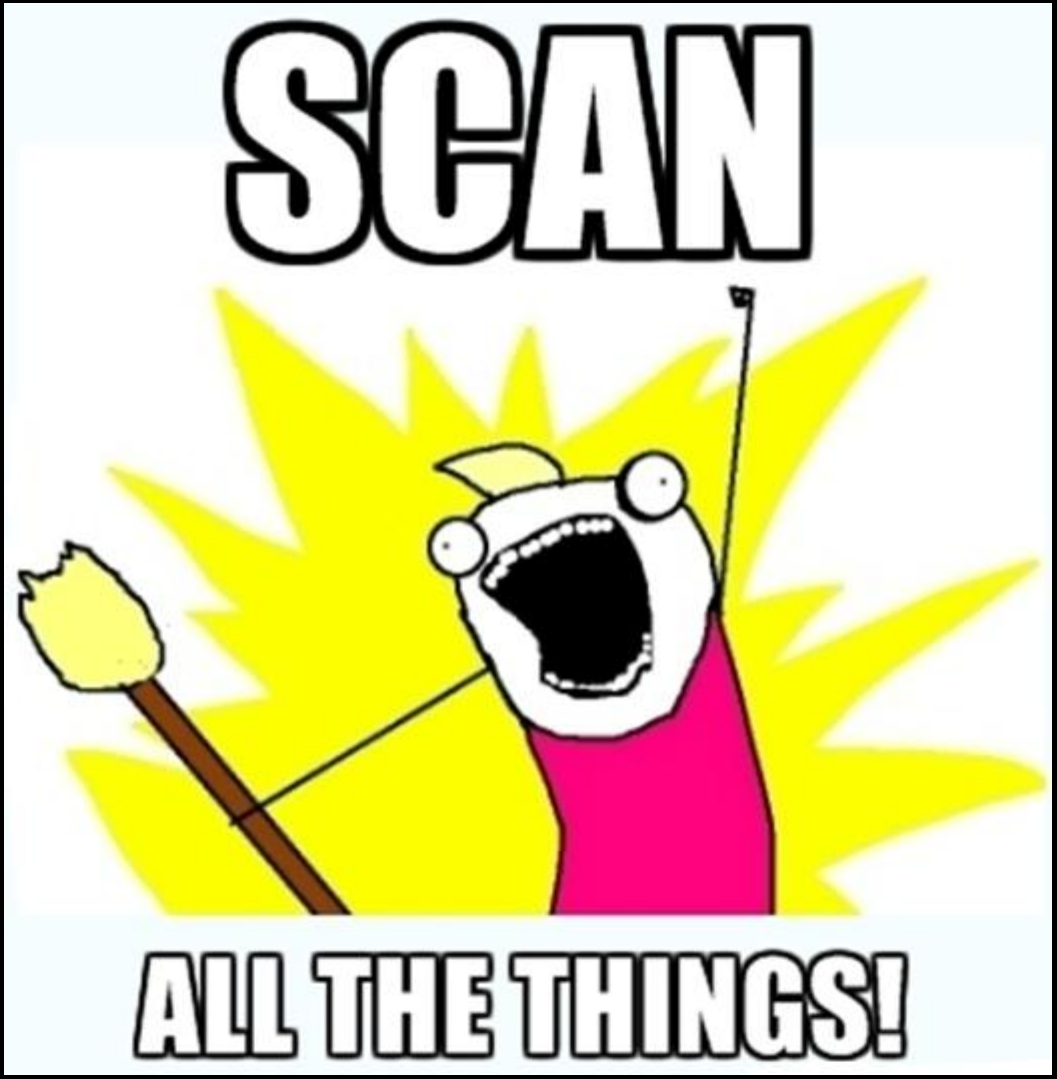


* Shodan has massively expanded coverage since my project was started

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://digitaloffense.net/tools/banner-plus.nse

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

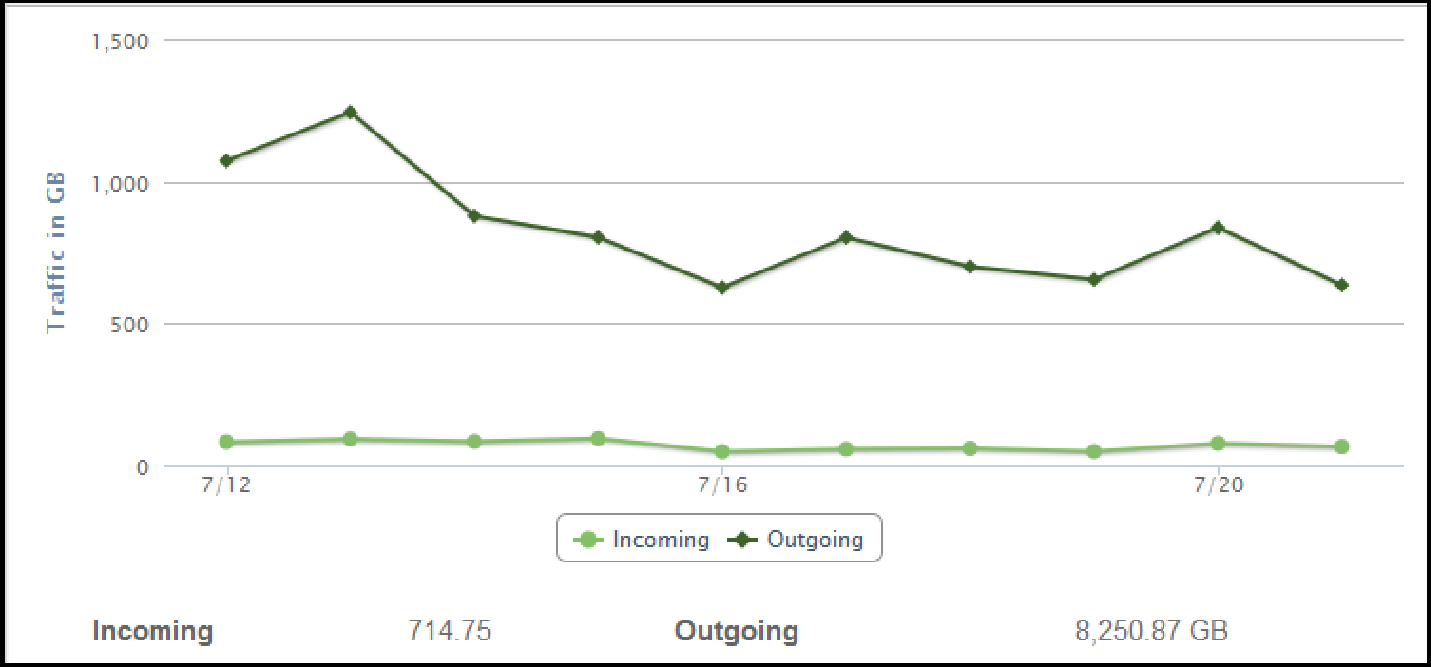
- Runs well on 128Mb RAM VPS nodes in Russia

Scanning UDP Services

Scan the entire Internet with one probe in about 7 hours

Easily push 1.2Gb of traffic per day

- http://digitaloffense.net/tools/udpblast.c

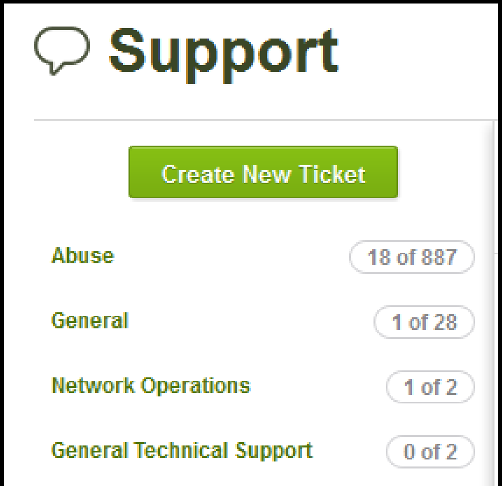


Incoming 714.75 Outgoing 8,250.87 GB

Scanning the Internet Annoys People

Visible on the DShield “top attackers” list

- Over 1,700 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



Support

Create New Ticket

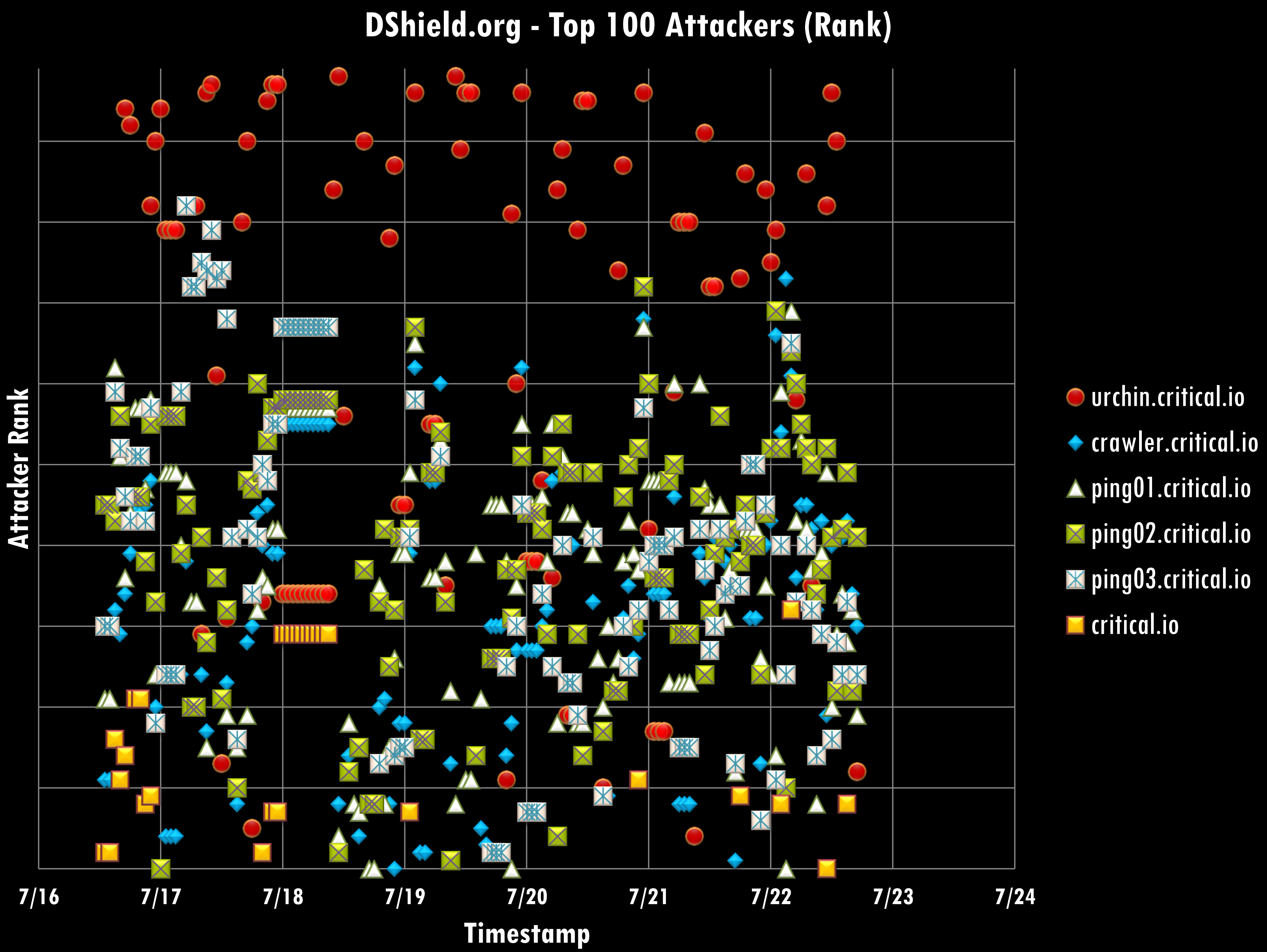
Abuse	18 of 887
General	1 of 28
Network Operations	1 of 2
General Technical Support	0 of 2

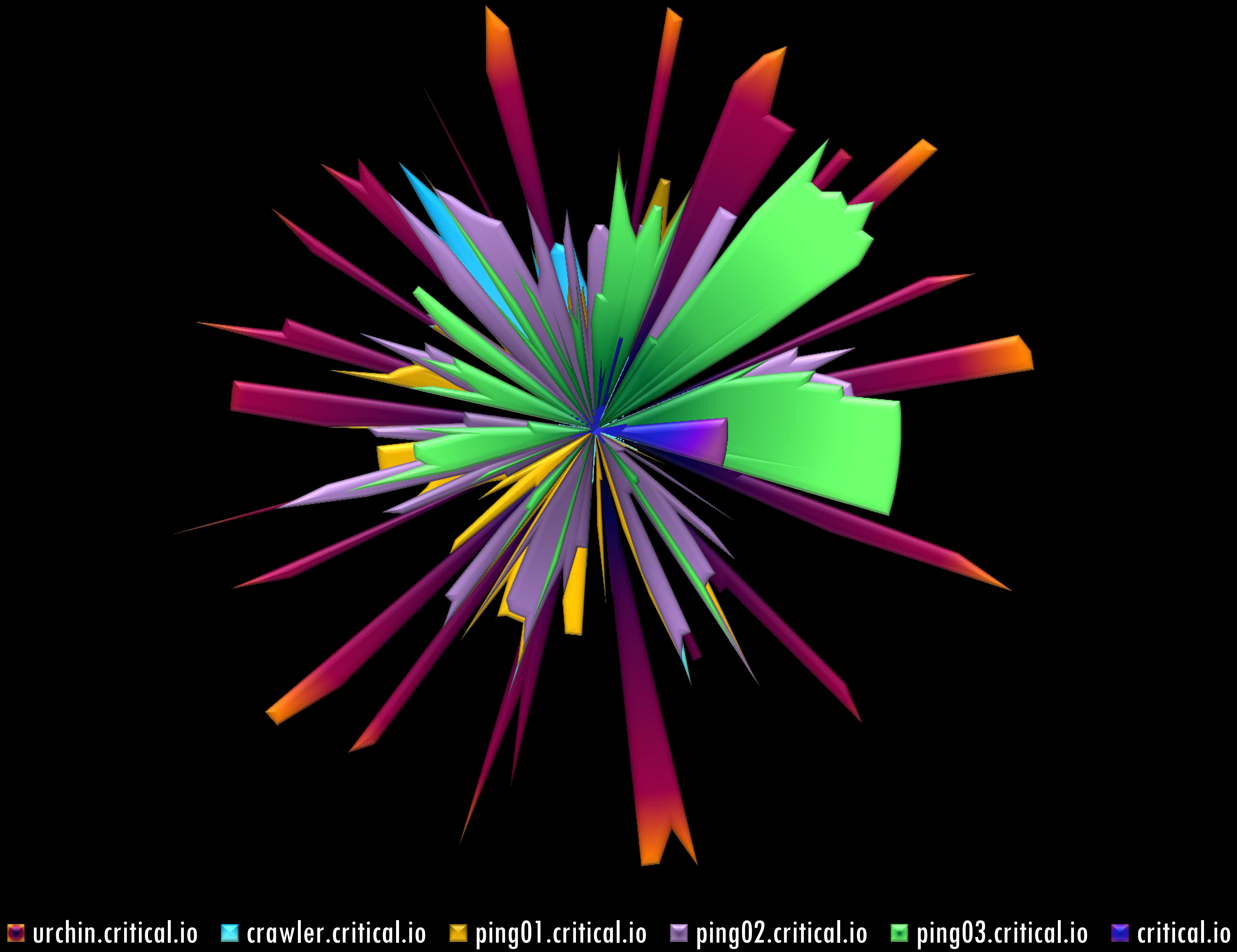
Please identify your customer operating from the above address at the time mentioned, and terminate immediately his hacking activities. Please prevent him from continuing his hacking activities in the future as well.

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?

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.

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?**


DShield.org - Top 100 Attackers (Rank)
Attacker Rank
Timestamp
7/16
7/17
7/18
7/19
7/20
7/21
7/22
7/23
7/24
urchin.critical.io
crawler.critical.io
ping01.critical.io
ping02.critical.io
ping03.critical.io
critical.io


urchin.critical.io
crawler.critical.io
ping01.critical.io
ping02.critical.io
ping03.critical.io
critical.io

Storage and Processing

Generates about 5Gb of data per day

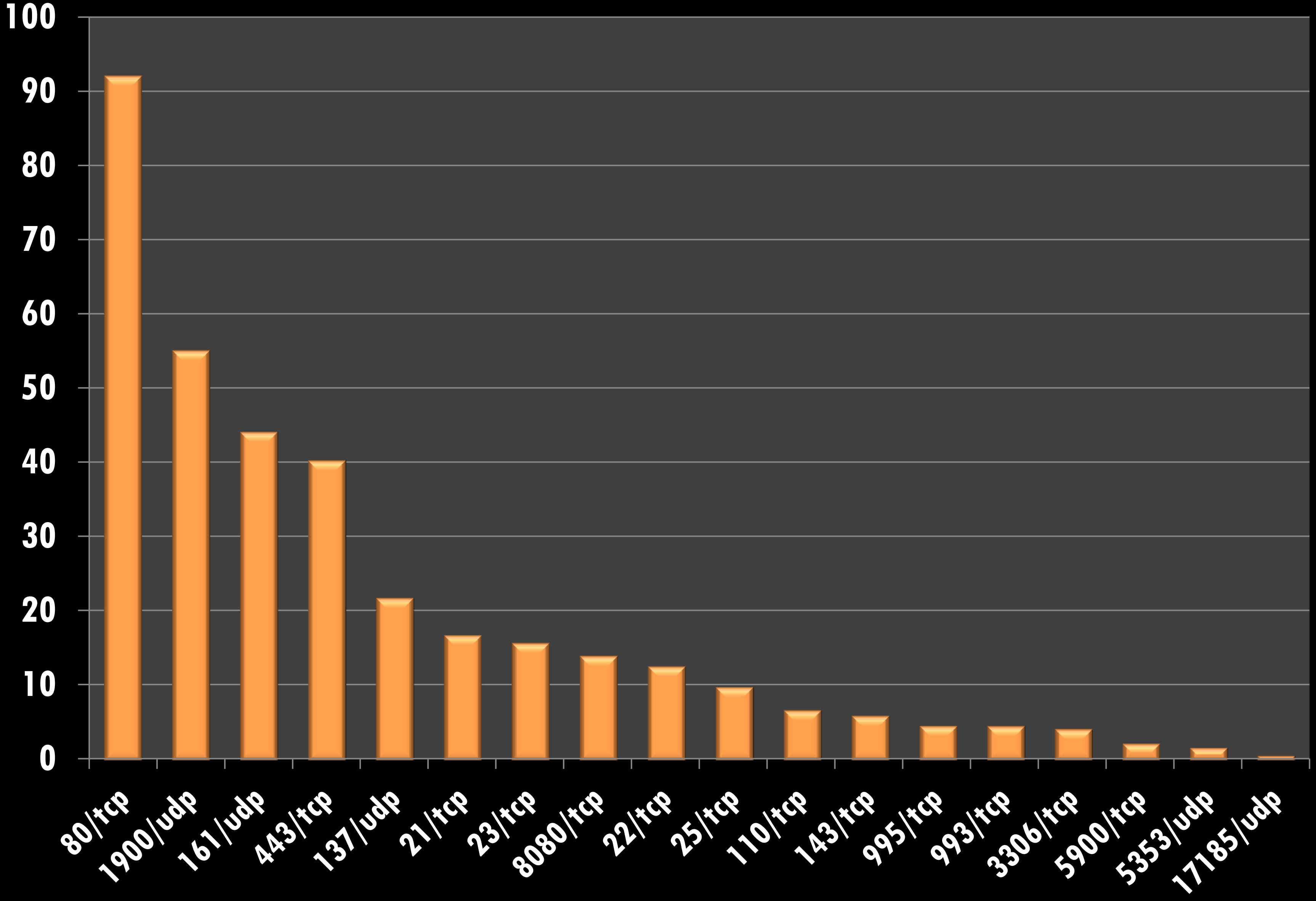
- Around 700GB of raw data over four months
- Normalized to 330GB of Bzip2 record streams

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

UDP Scanning Packet Statistics

```
root@urchin:~# ifconfig eth0
    RX packets:       36,493,188,599
    TX packets:      570,585,376,832
      RX bytes:   4,050,663,016,927 (4.0 TB)
      TX bytes:  57,845,505,035,755 (57.8 TB)
```

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

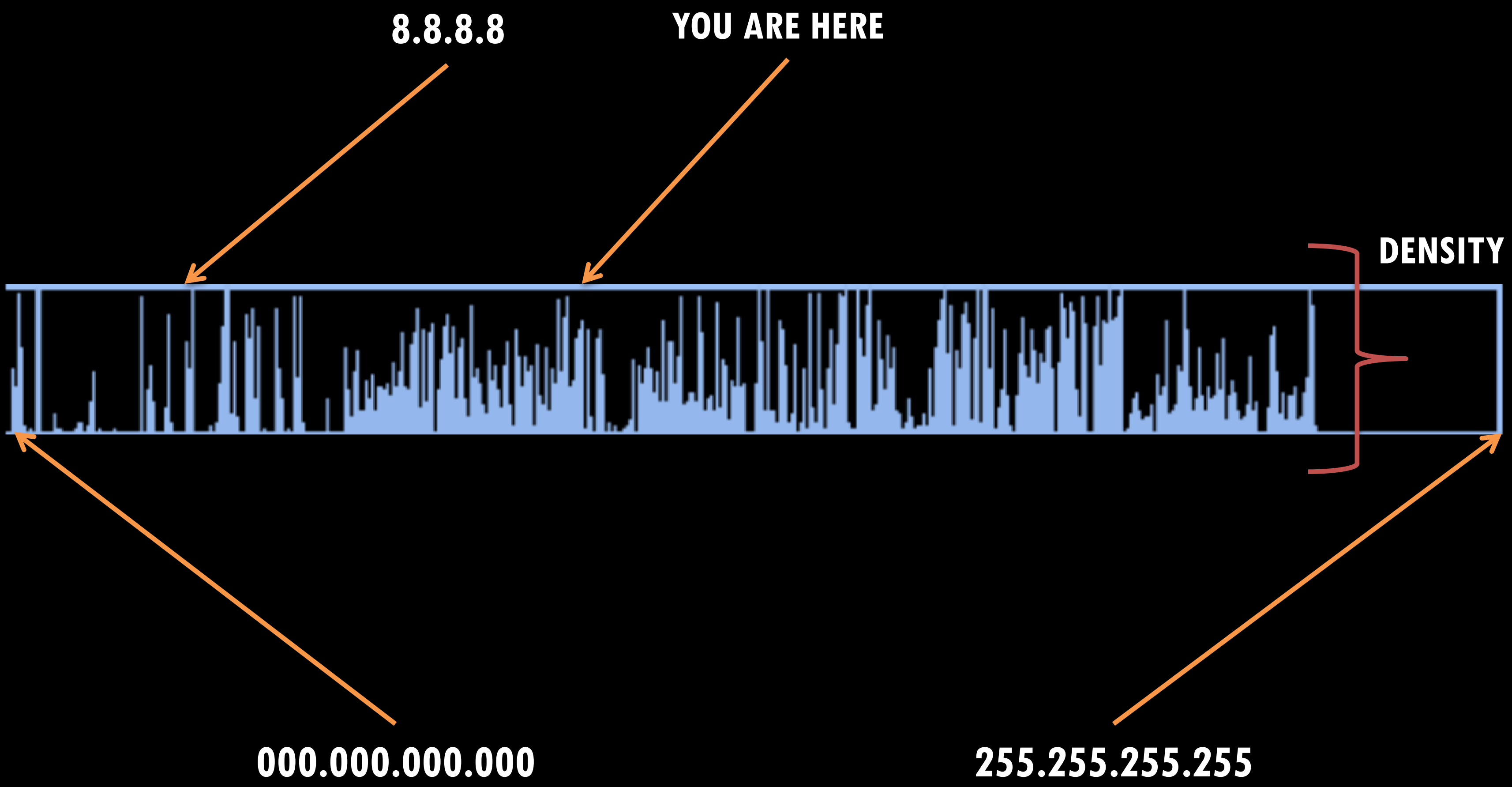
UPNP Services

Over 54 million devices respond to UPNP / SSDP probes

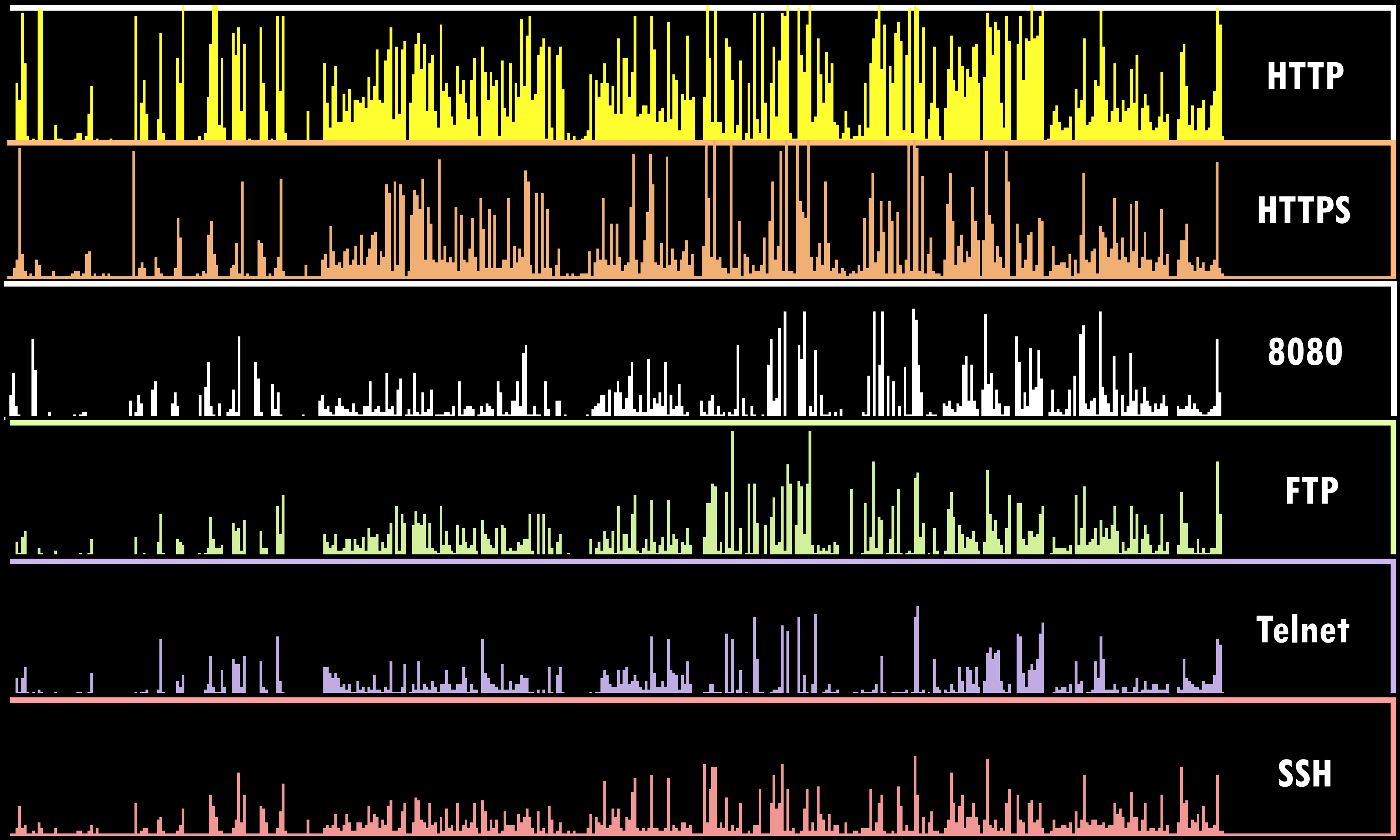
- Close to a dozen unique UPNP SDKs represented
- Quite a few expose the SOAP service externally
- Almost half based on the Intel SDK (1.2)

Service Density

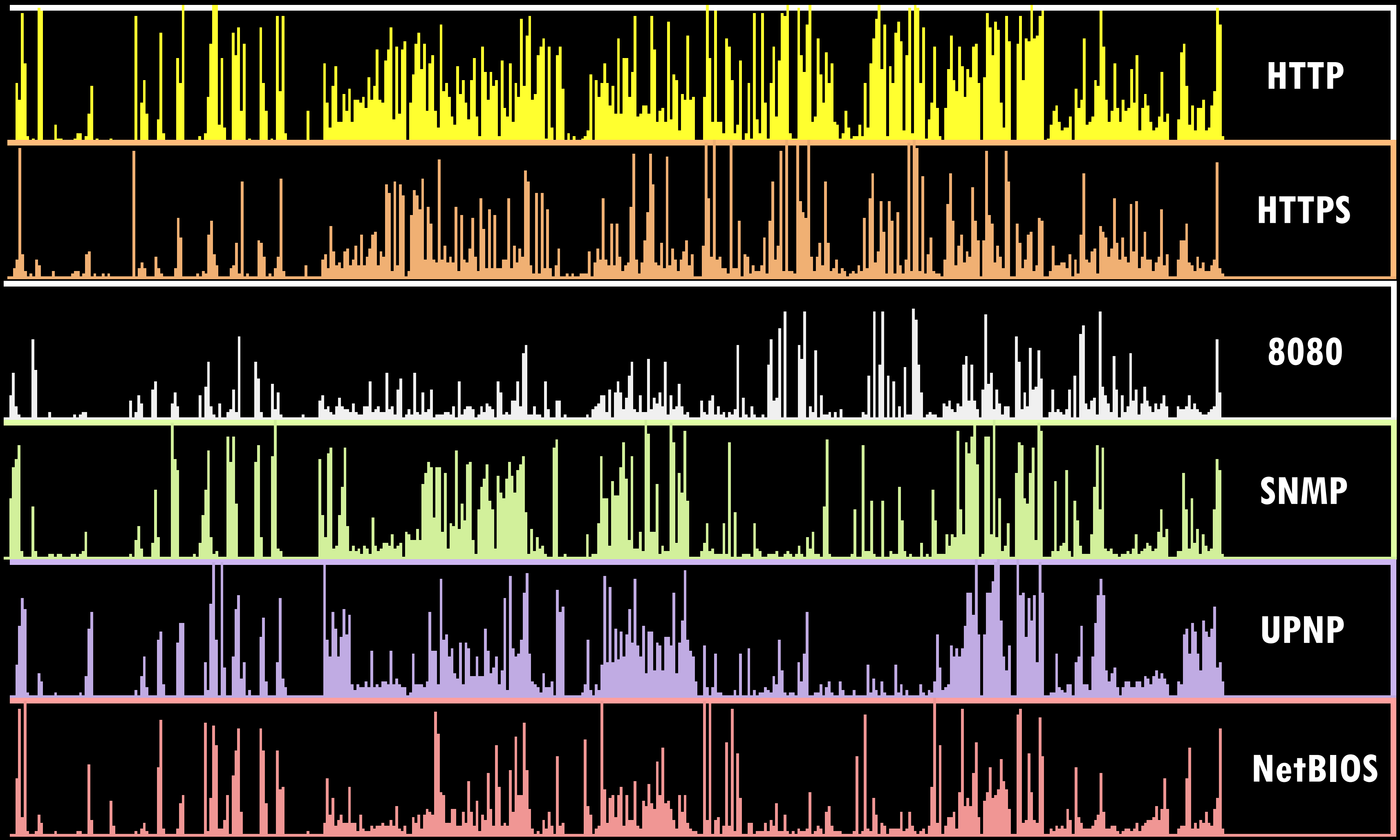
Internet Sparklines



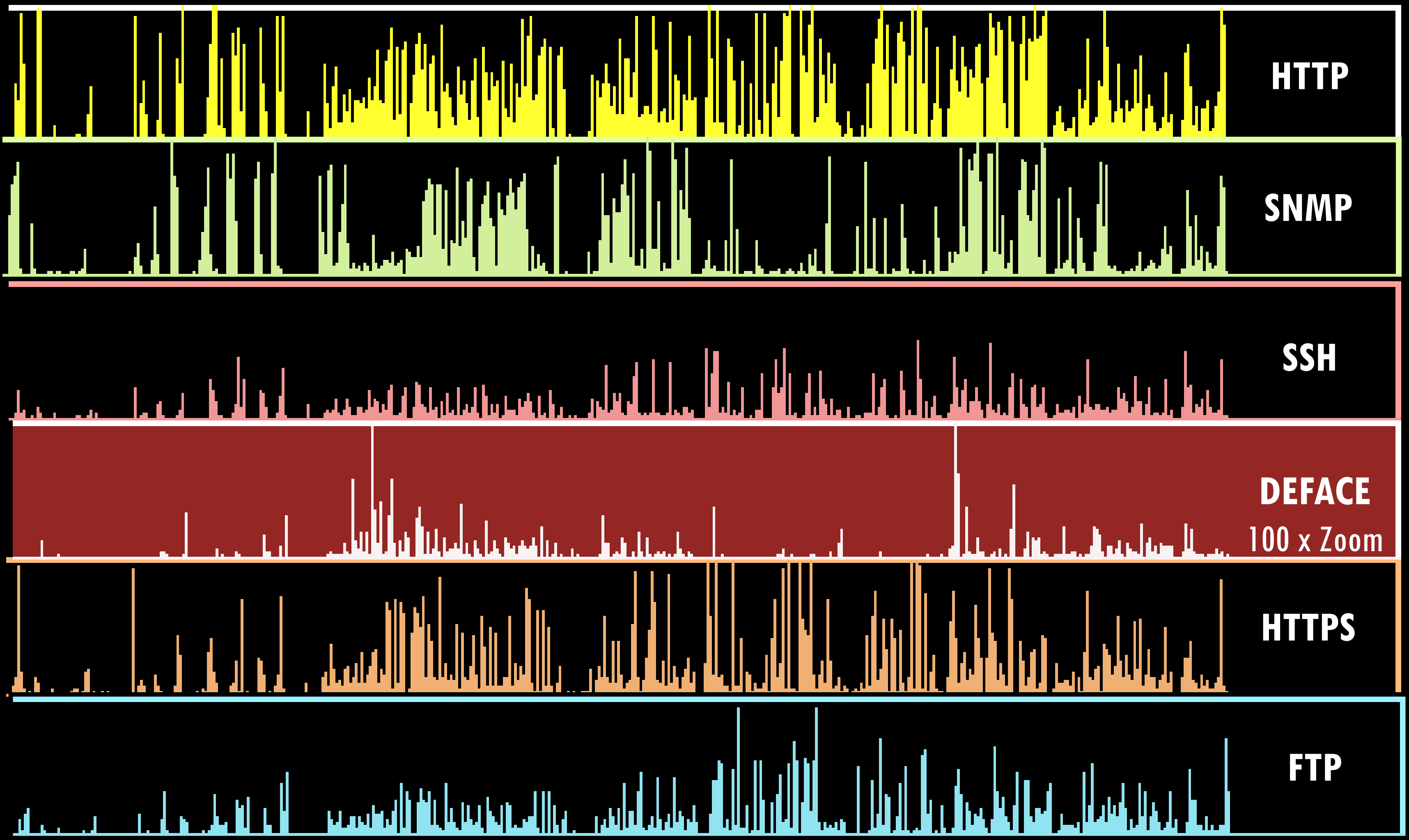
Web, FTP, Telnet, and SSH



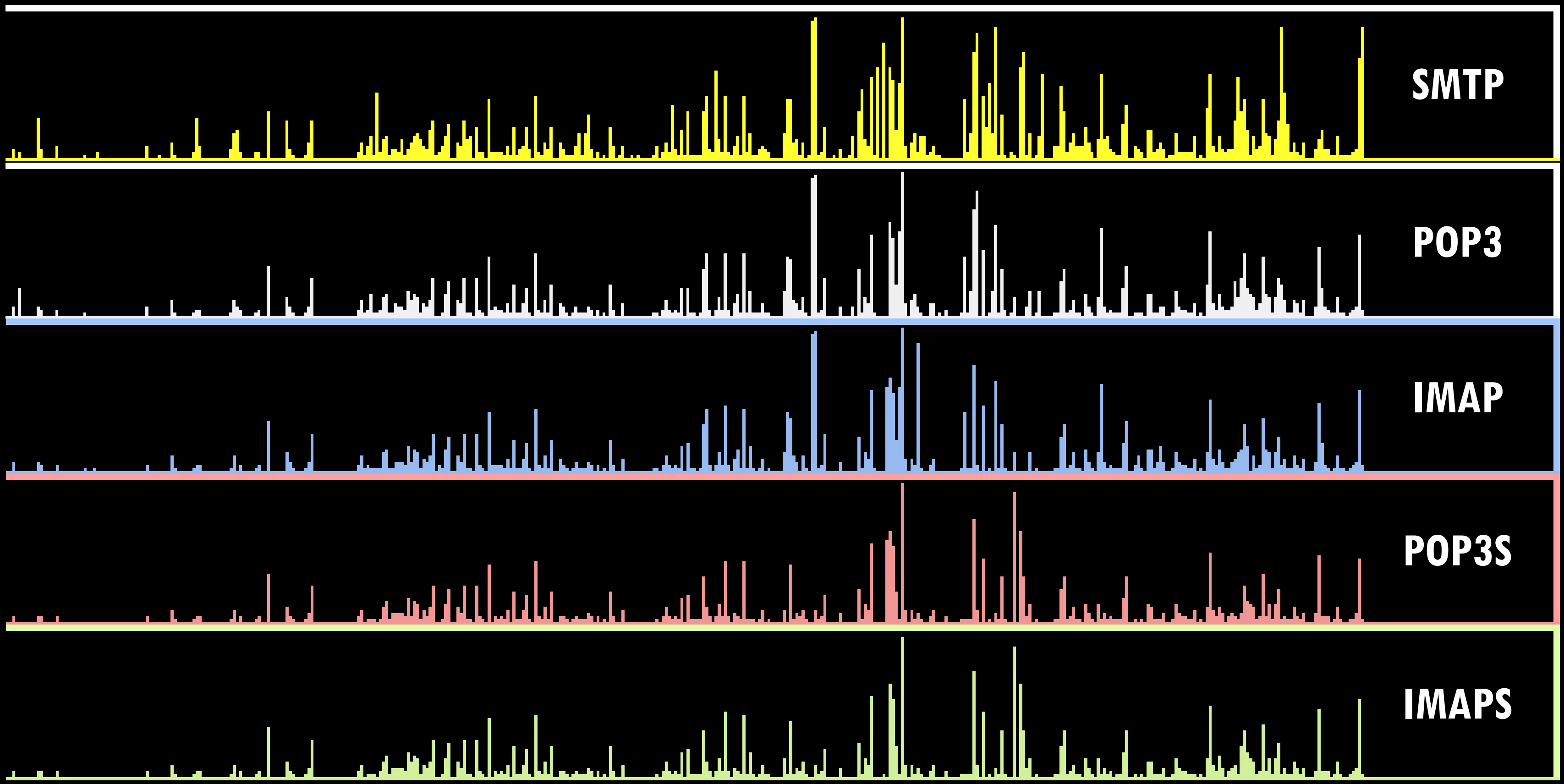
Web, SNMP, UPNP, NetBIOS



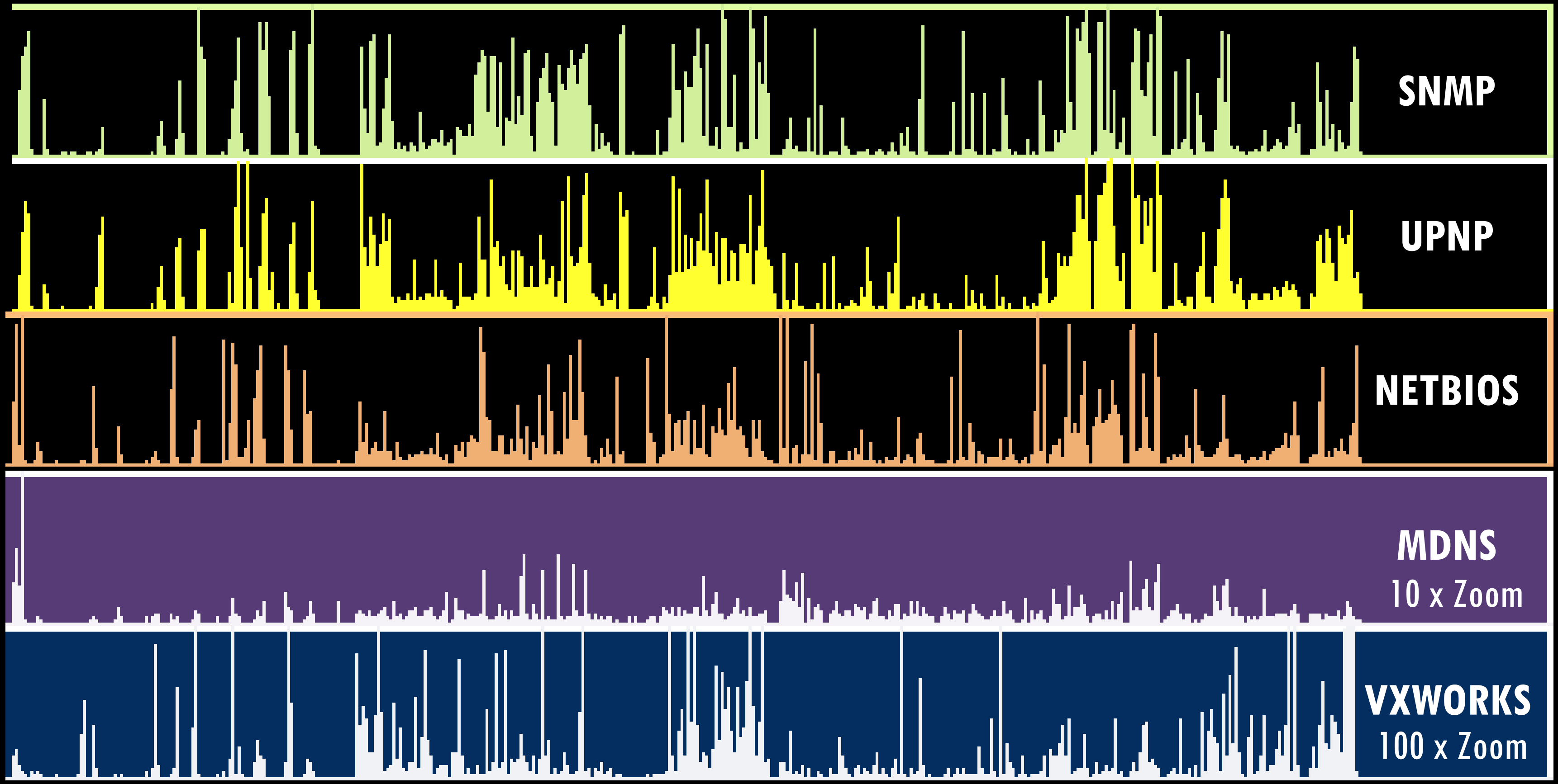
Defacements (Zone-H)



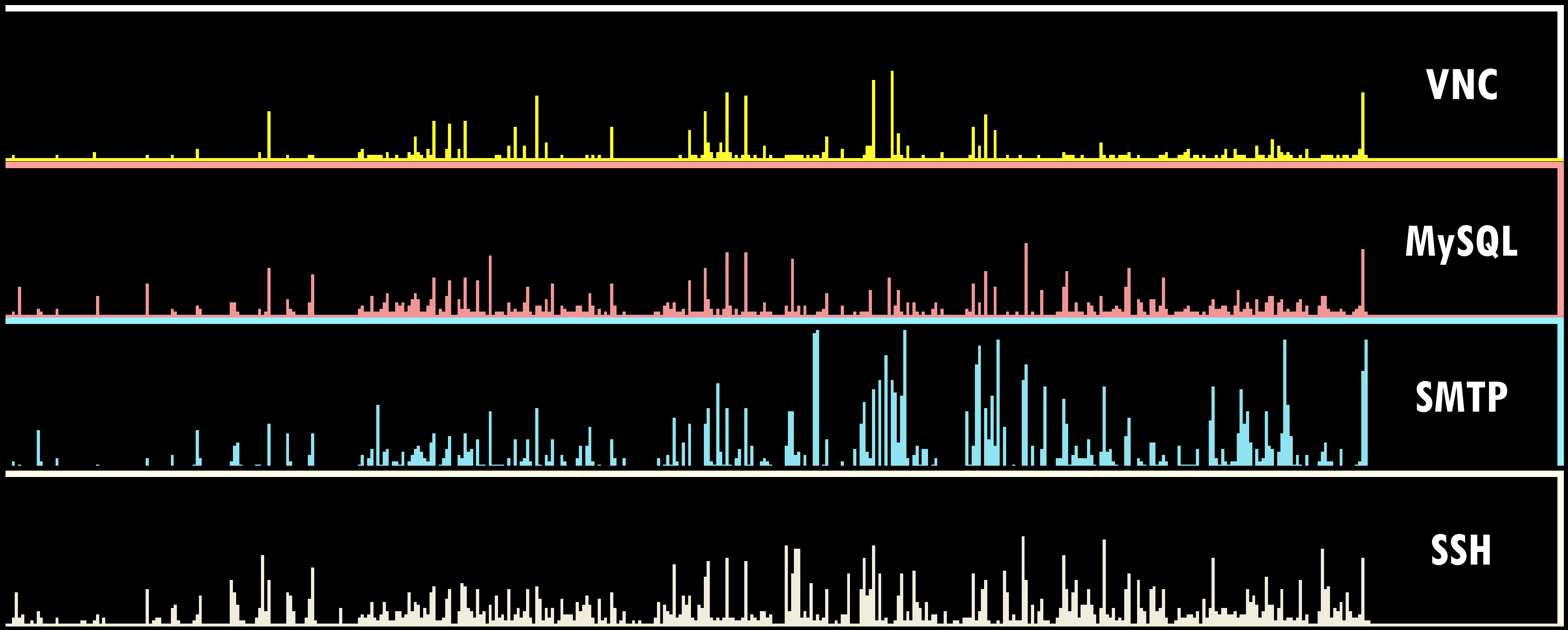
Email Services



UDP Services



VNC vs MySQL vs SMTP vs SSH



Measuring Exposure

VxWorks Debug Service

Remote debug service on UDP port 17185

- Exposes hundreds of different devices
- Planes, Mars rovers, VoIP phones
- Read, write, execute memory
- Over 250,000 found in July of 2010…

2012: **200,000**

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%]

Cisco Routers

Cisco Router Vulnerabilities

Cisco releases about 40 advisories per year

- How often do you flash your routers?
- Average router has over 60 flaws
- Most exploitable version?

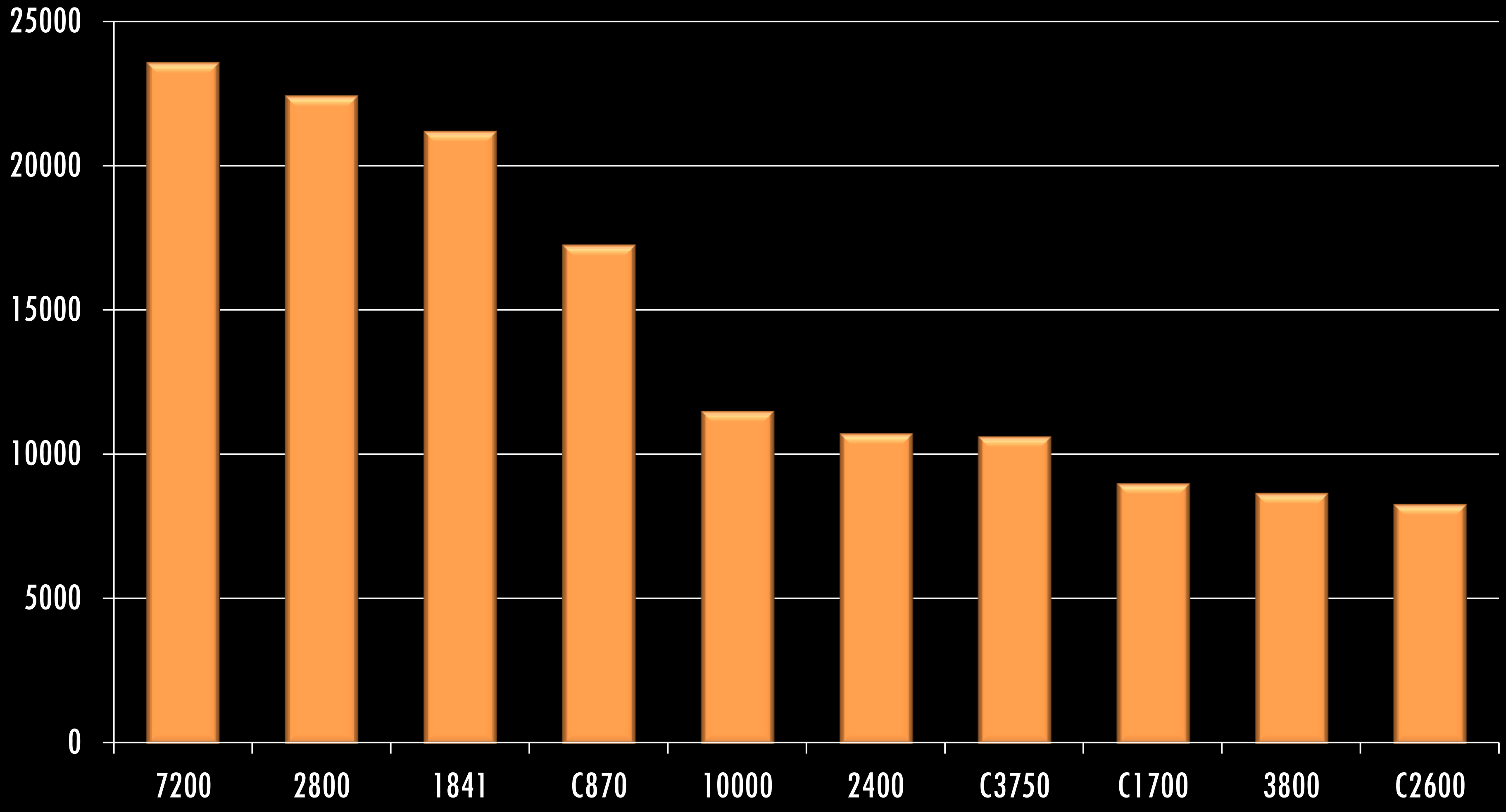
Cisco IOS 12.2

Cisco Exploit Tuning

Remote Cisco IOS exploits are fragile

- Magic numbers required
- Hardware and RAM specifications
- Runtime configuration
- IOS version
- Build

Cisco Devices by Hardware



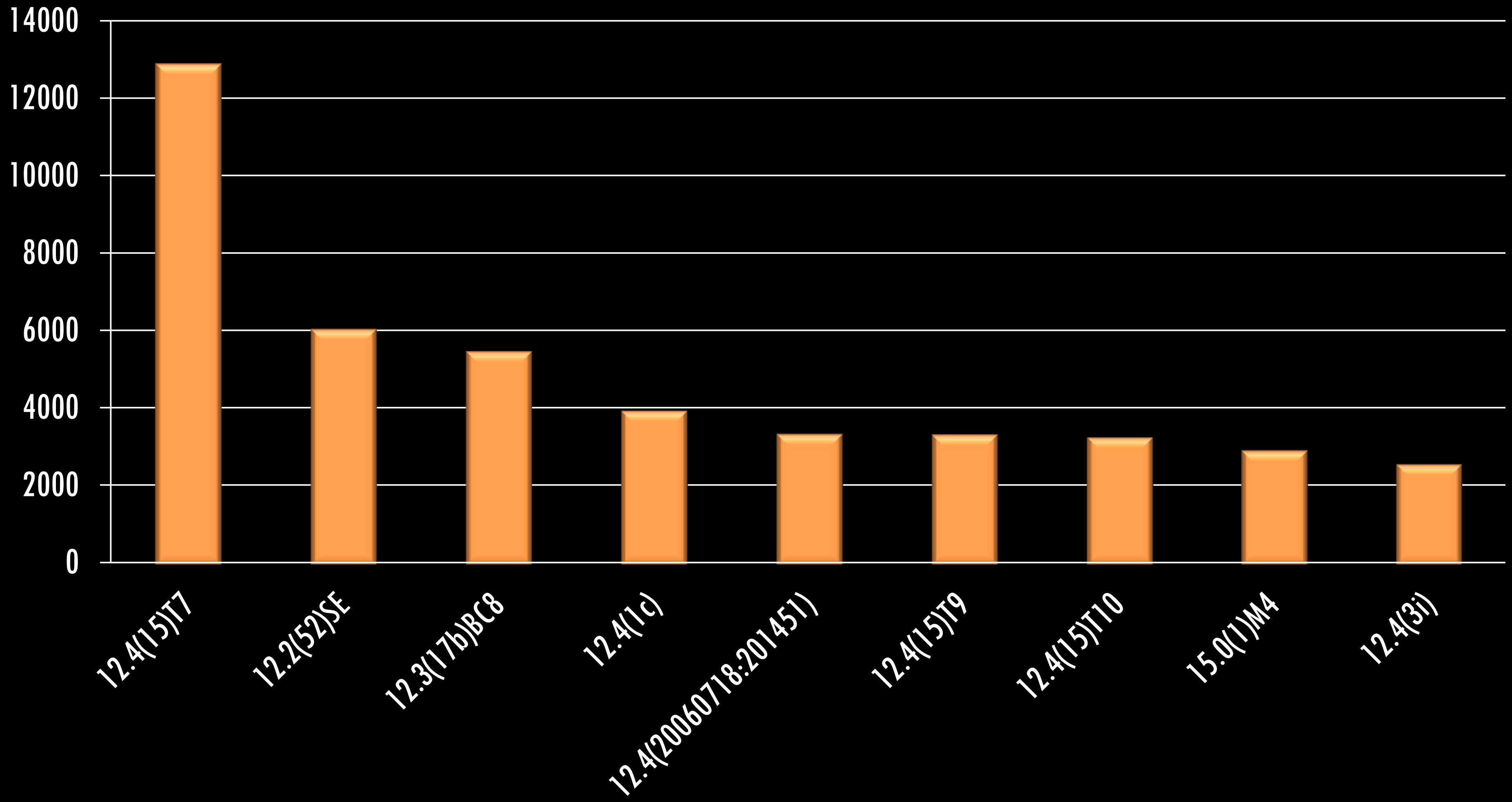
Cisco Exploitation

Crunch SNMP data for the optimal target

- Most common combination of HW, Version, Image
- Hardware is one of 7200, 2800, 1841, or C870
- What version has the most flaws?

Optimized Targets

12.4(15)T7 is on 12,842 routers



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

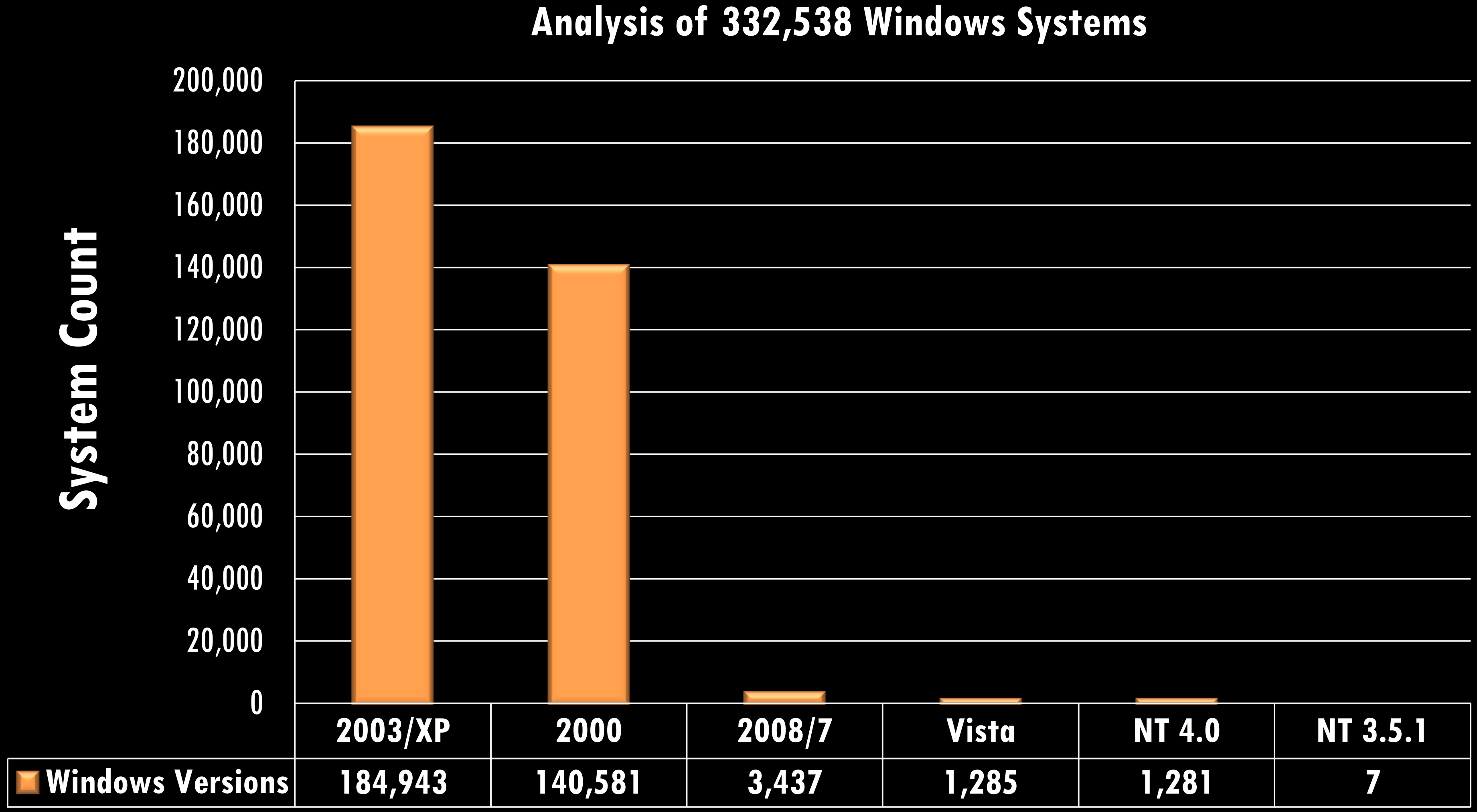
Windows SNMP

Windows SNMP Services

SNMP exposes sensitive data on Windows

- Standard networking and interface MIBs
- Installed software and security patches
- Windows domain & account names
- Arguments to service processes

Windows SNMP Services



Analysis of 332,538 Windows Systems

	2003/XP	2000	2008/7	Vista	NT 4.0	NT 3.5.1
▨ Windows Versions	184,943	140,581	3,437	1,285	1,281	7

Common Process Names

263,552	string: "svchost.exe"
58,980	string: "csrss.exe"
51,287	string: "winlogon.exe"
35,841	string: "snmp.exe"
35,442	string: "services.exe"
35,439	string: "lsass.exe"
35,407	string: "smss.exe"
35,209	string: "system idle process"

Less Common Processes

- 1 string: "90.txt"
- 1 string: "8-mergab_animvip.exe"
- 1 string: "8-mergab2_animvip.exe"
- 1 string: "88.exe"
- 1 string: "888111xpsp2.exe"
- 1 string: "88755.exe“
- 1 string: "87.exe“
- 1 string: "86husiji3w.exe"

- 1 string: "867.tmp"
- 1 string: "866.tmp"
- 1 string: "865.tmp"
- 1 string: "854.exe"
- 1 string: "84.exe"
- 1 string: "80.exe"
- 1 string: "8082.exe“
- 1 string: "8634iji3w.exe"
- 1 string: "86h3jiiw.exe"

Interesting Processes

- 444.470
- 4b07d.com
- 6c51e.com
- 865.tmp
- a2.tmp
- acetsfsl.386
- acpgui.dll
- acqhidcl.dat
- **adobe online.com**
- **adobe update.com**
- adskcleanup.000
- ameliecafe2.ifn
- amwin.ovl
- atbptoolbarssb aua.bin
- audio.run
- ayagent.aye
- ayagentsrv.aye
- aydblog.aye
- aypatch.aye
- aypatchv.aye
- aytask.aye
- **blackcipher.aes**
- bservice.srv
- c16_serv_dba_w32.dll
- c16_serv_mgr_w32.dll
- c16_serv_svc_win.dll
- c1e8a.com
- calcfeetool.101
- cdshookloader.dll
- **cgibin.sys**
- cilevbw.com
- cks1a.tmp

Windows SNMP Service Arguments

Over 1000 passwords found exposed

- ○ 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"
```

NetBIOS Oddities

NetBIOS Services

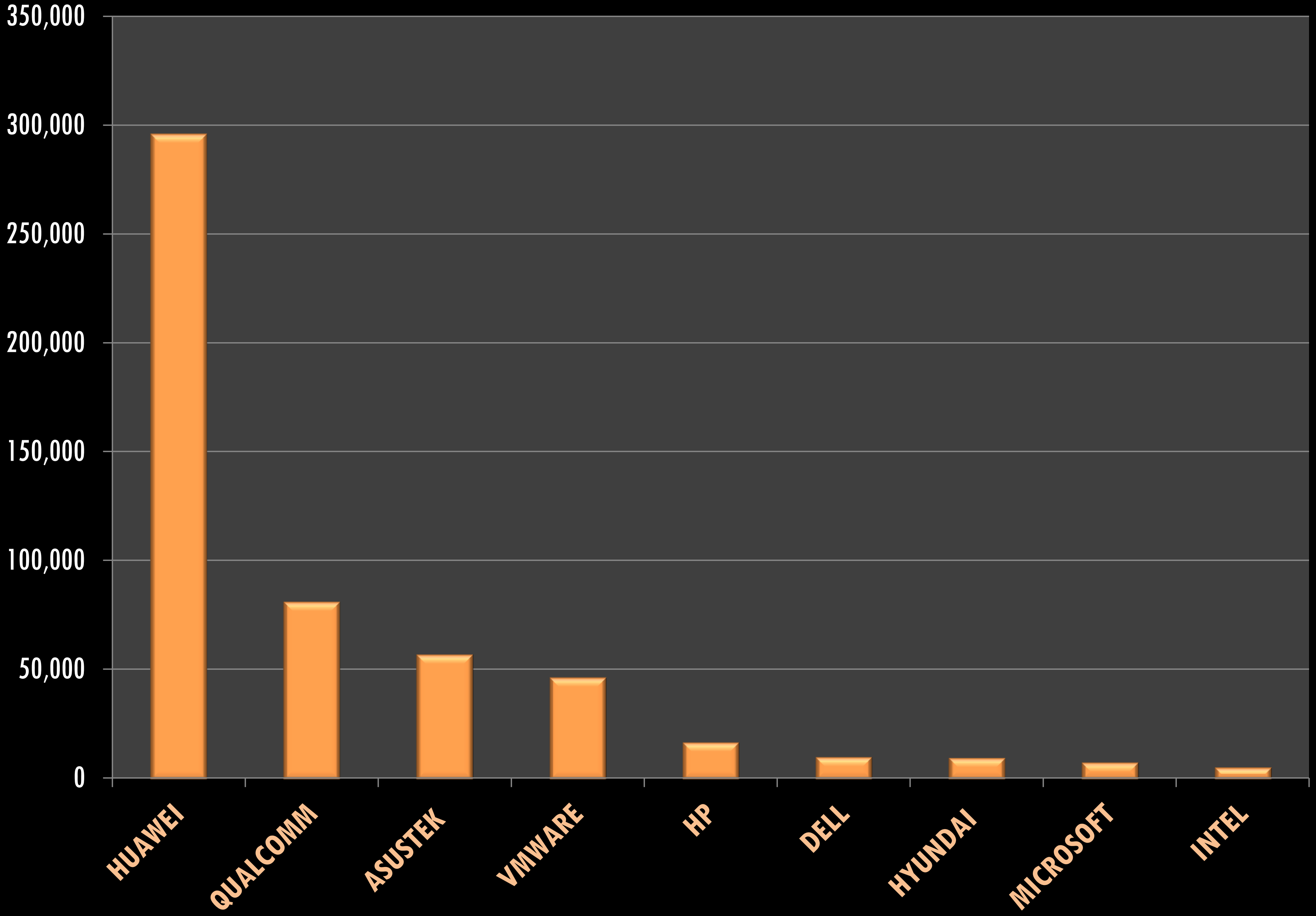
NetBIOS (137/udp) responses incredibly useful

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

Over 21 million NetBIOS services found

- MACs are globally unique? Right?

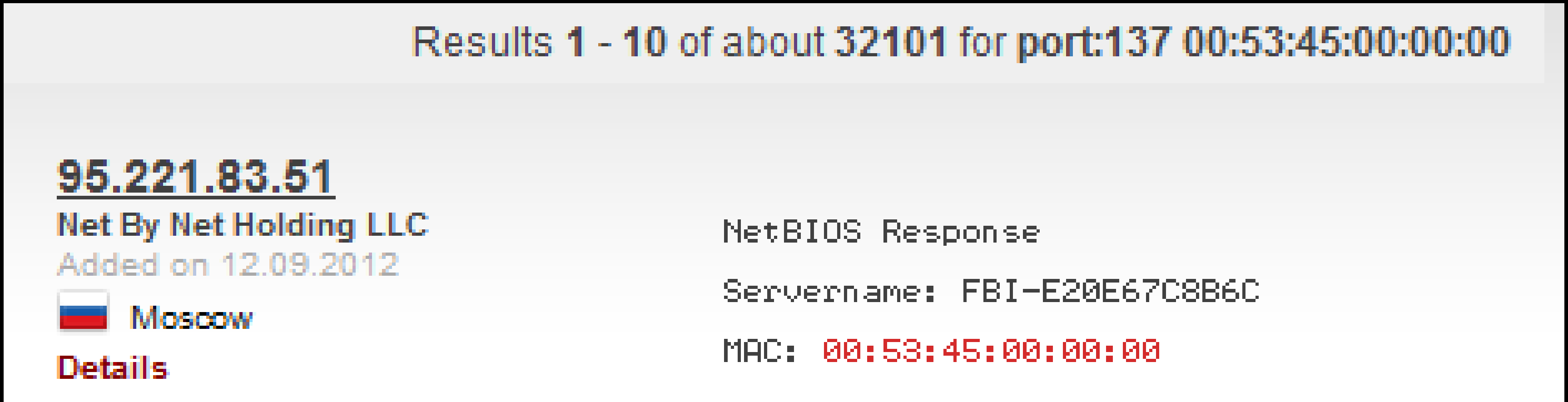
Duplicate MAC Addresses by Vendor



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

Servername: FBI-E20E67C8B6C

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

NetBIOS Names

Names must also be locally-unique on the network

- A unique name can be tracked across networks
- Domain names often unique to a company

HTTP Cookie Analysis

HTTP Cookie Repetition

HTTP session cookies are generally unique

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

25	ASPSESSIONIDCARCTTQQ	APPKDOOAEHOEIPJJIFPKHAGI
25	ASPSESSIONIDCARCTTQQ	LOELDOOALLKGBBDKKIMNBPCA
26	ASPSESSIONIDCARCTTQQ	EDCLDOOAPCBIBMCFBGCOLCMH
133	ASPSESSIONIDQACDDRAQ	NMELPFDCKCAKKNPAHIDCICMJ
296	ASPSESSIONIDAATTDQBT	FGMAJHOAJJEAGLFNFJKFDANP

Duplicate Cookies Indicate 0-Day

More broken cookies

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

58	rack.session	BAh7BjoOX19GTEFTSF9fewA%3D%0A
54	_Federal_session	BAh7BiIKZmxhc2hJQzonQWN0aW9uQ29udHJvbGxlcj
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

Questions?

Thanks!

Email	hdm@rapid7.com
Twitter	@hdmoore
IRC	hdm@freenode