DNS Footprint of Malware

Ed Stoner
ers@cert.org
CERT Network Situational Awareness

Anexa

Automated Run-Time Analysis environment

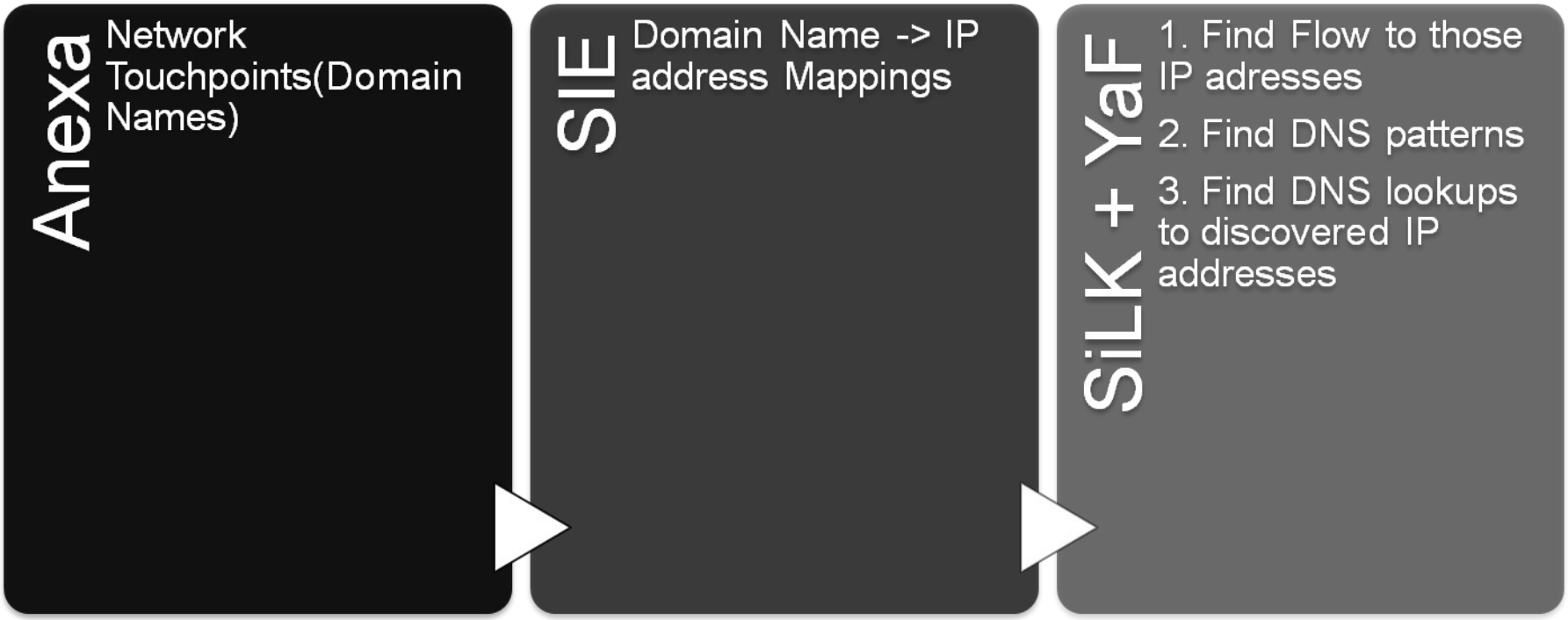
Malicious Software Catalog of millions of samples

~ 250,000 uniq md5s every 6 months

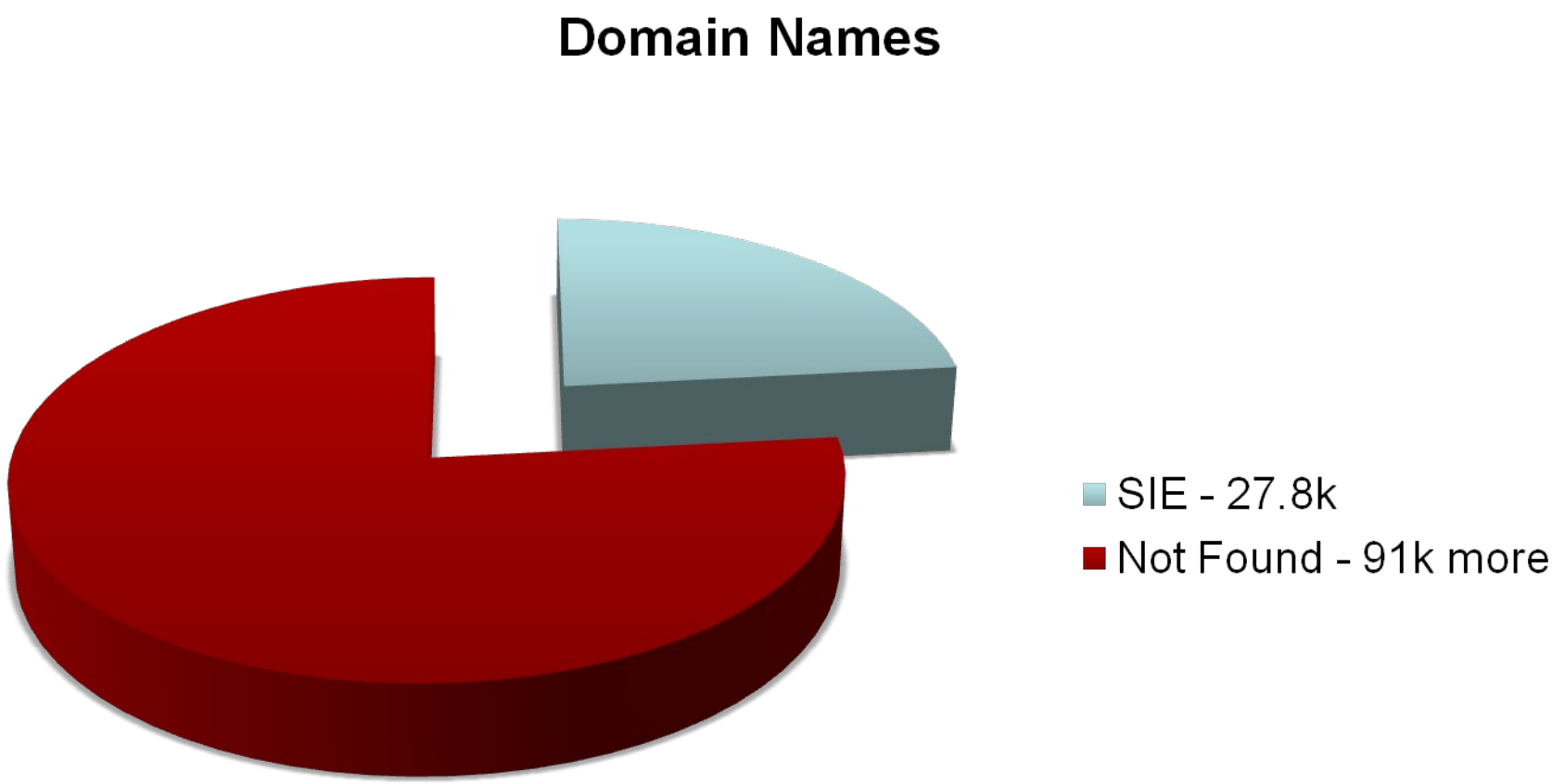
Network Touchpoints

- **Domain Names – 119,000 of them over 6 months**
- IP addresses

Malicious Domain Name Research

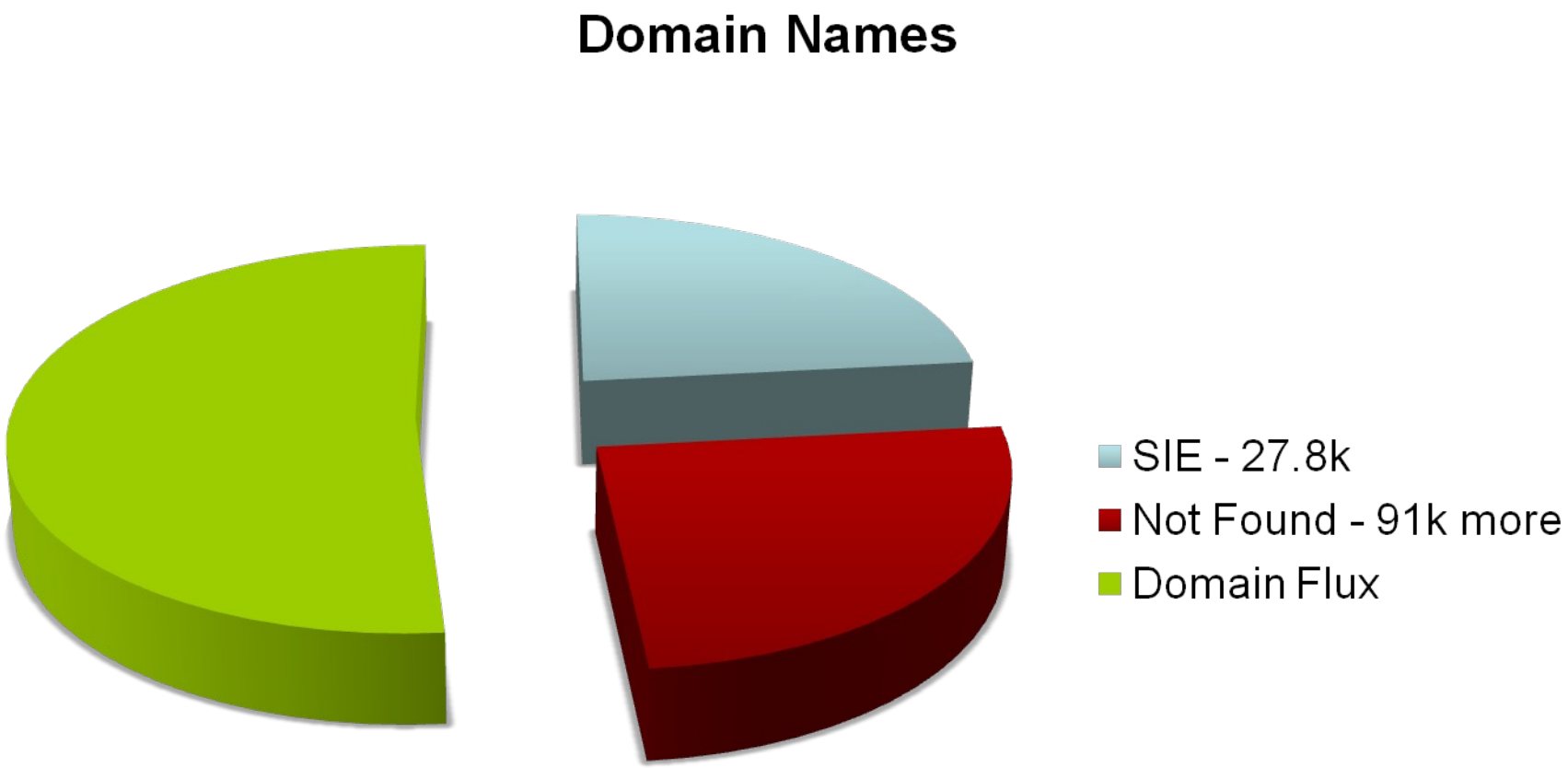


Data Set



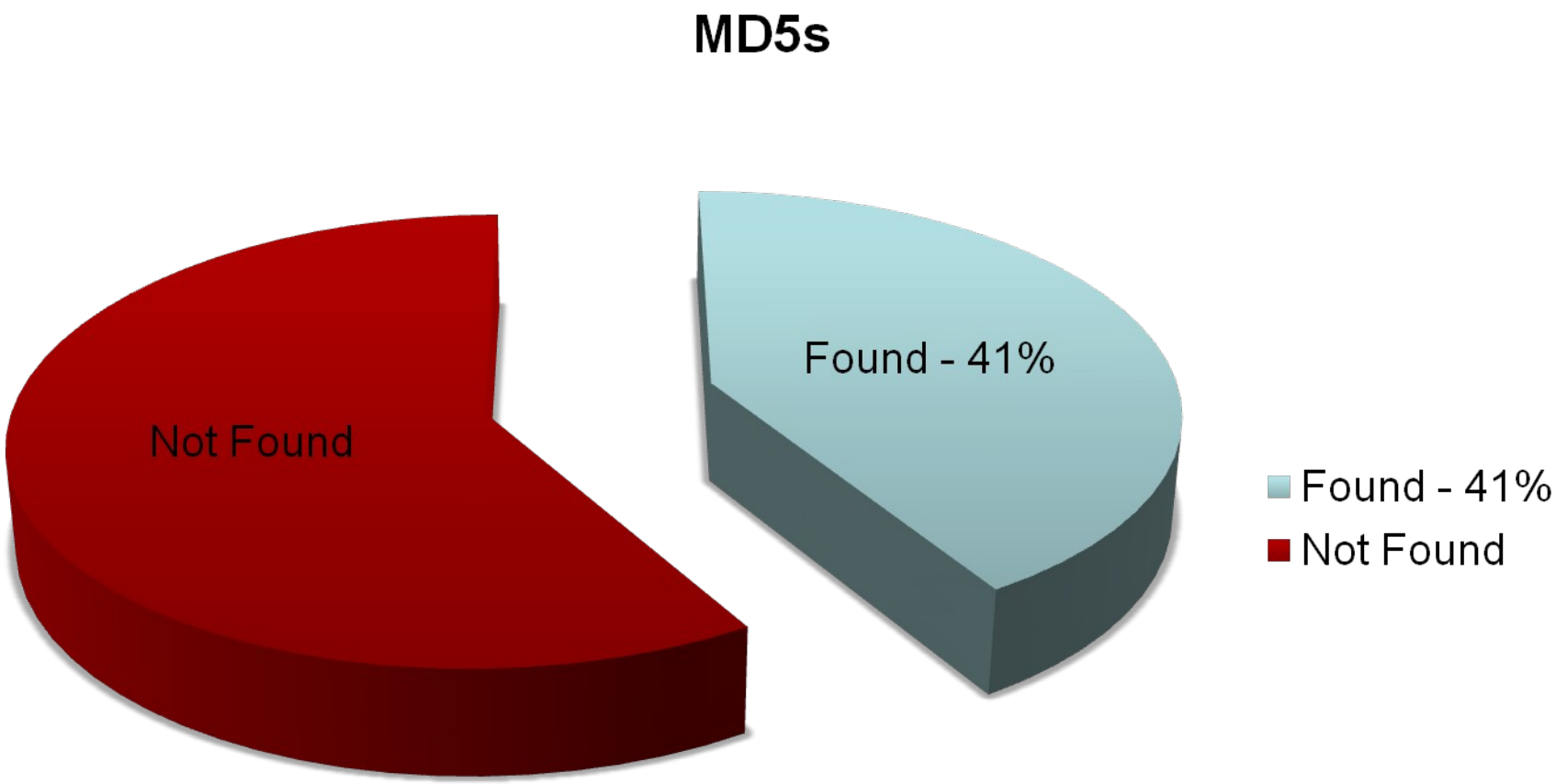
27859 domains -> 204931 IPs

Data Set



27859 domains -> 204931 IPs

Coverage by MD5

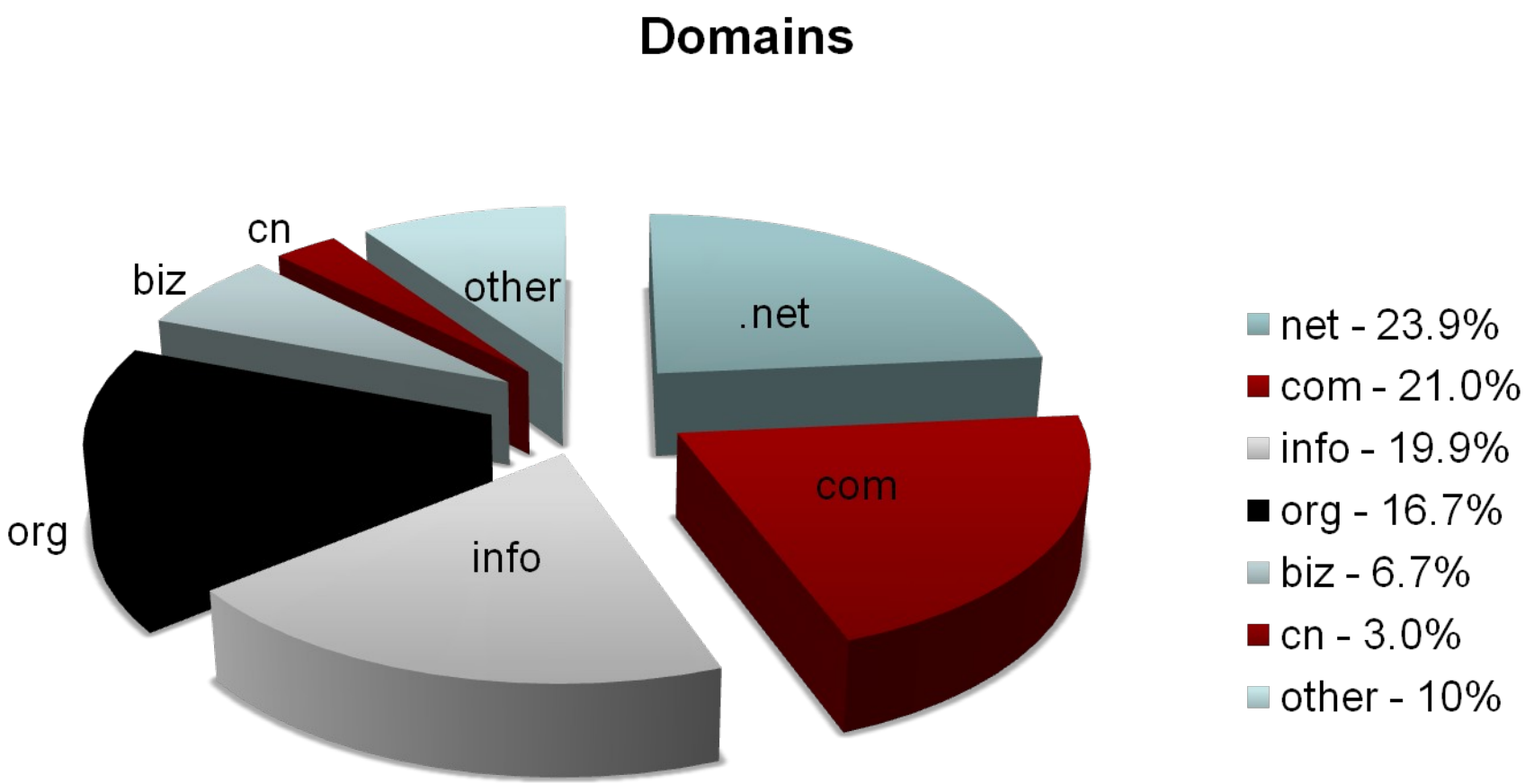


Control Case

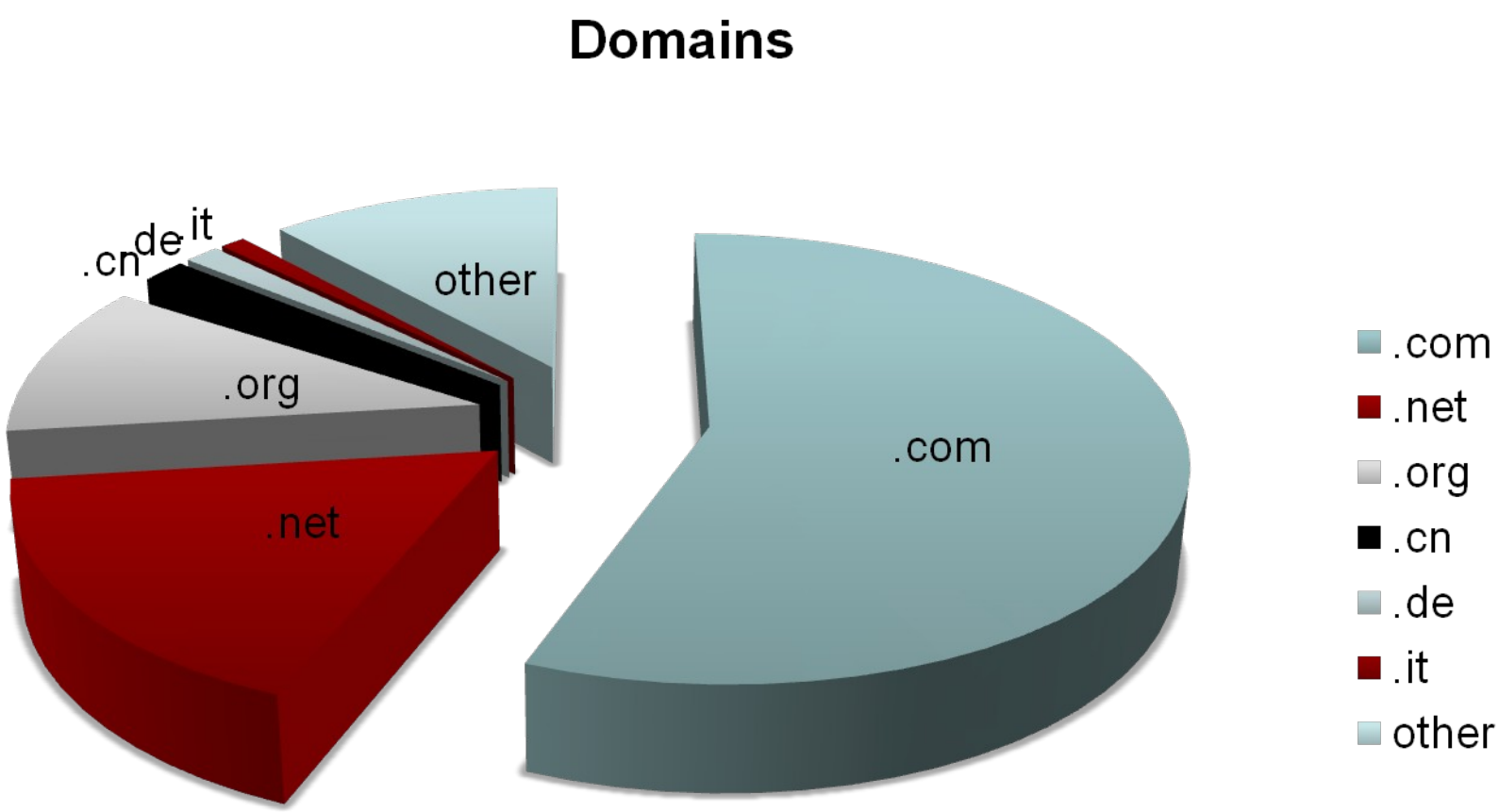
27859 Malicious Domains

27859 Random Domains

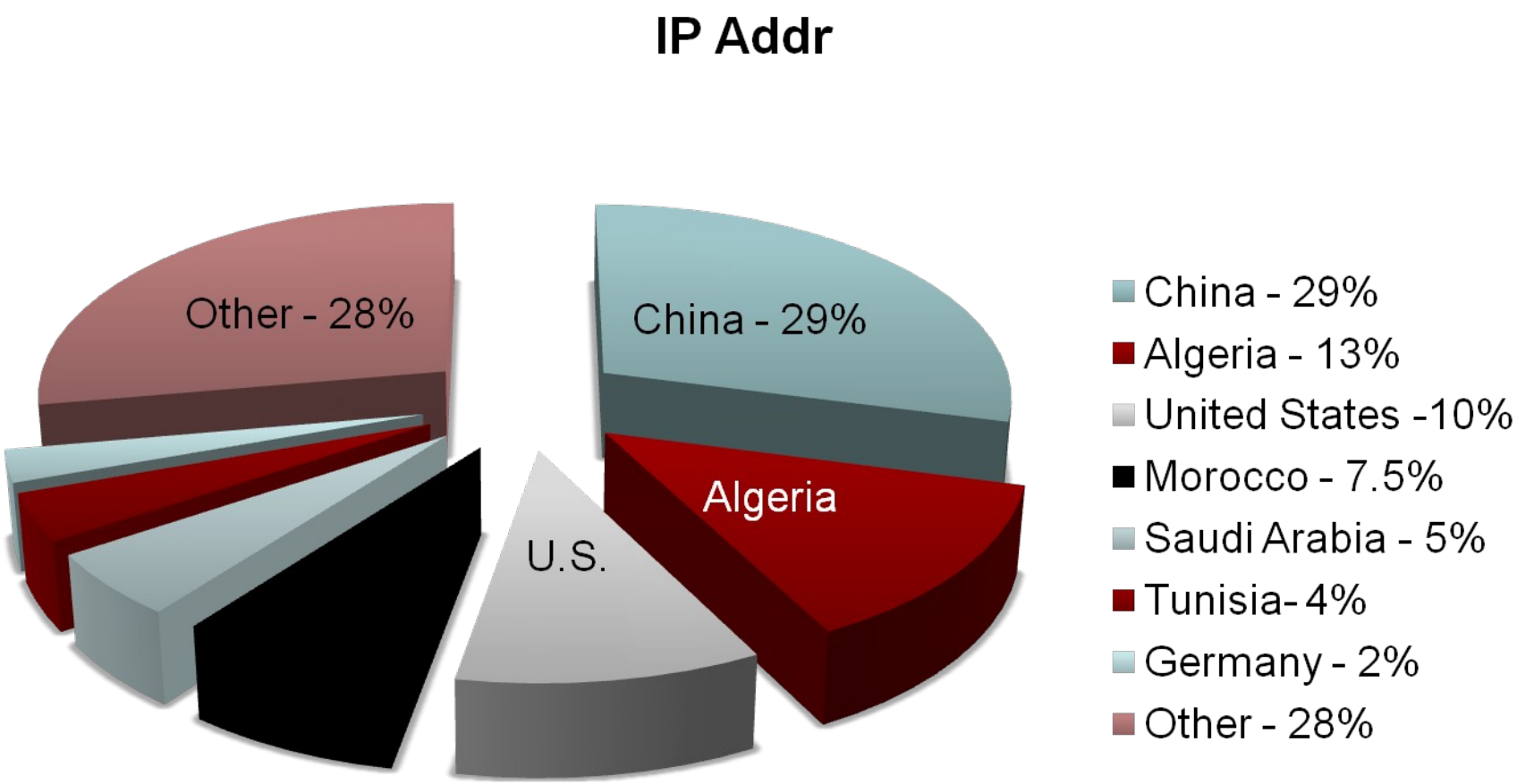
Top Level Domains - Malware



Random TLD distribution

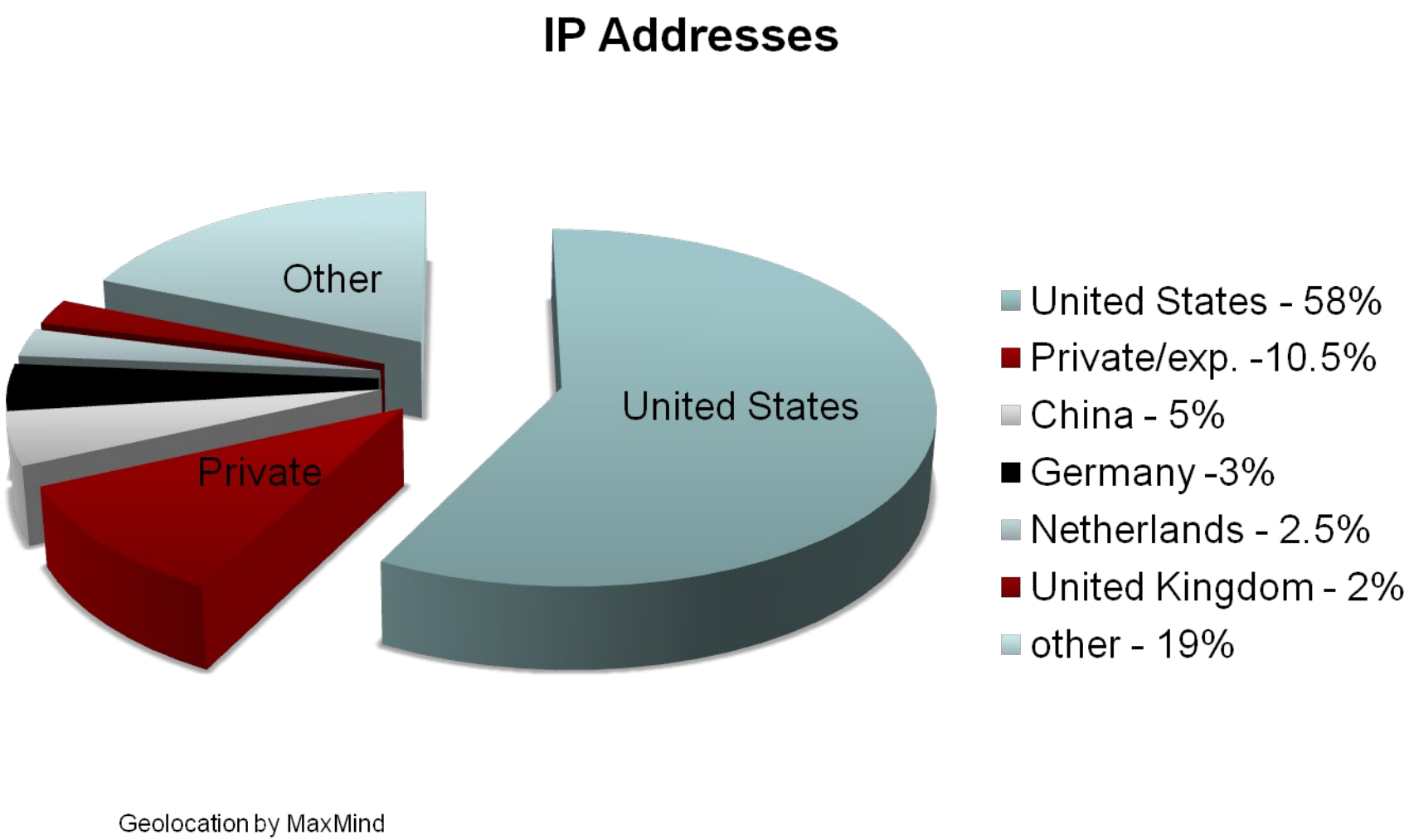


GeoLocation based upon IP address



Geolocation by MaxMind

Random GeoLocation distribution



Geolocation by MaxMind

Top domains (by md5)

2009-07-17 to 2010-02-10

auto.search.msn.com,23278
www.screenblaze.com,23152
www.wowchian.com,8333
www.fenomen-games.com,6999
www.gamecentersolution.com,4621
downloadfixandlove.com,4339
ads.netbios-local.com,2581
irc.zief.pl,2446
www.jcwz.net,2374
ayb.trinityacquisitions.com,2083
ayb.maximumexperience.com,2083
myart-gallery.com,1736
jet-arts-center.com,1716
videoporntrue.net,1645
freeavtest.com,1497
crystal-arts.net,1361
tubepornolive.com,1300
siteload.cn,1239
hostnsload.cn,1239
pornotube912.com,1225

2010-04-01 to 2010-09-27

mk.maxthon.cn,11516
google.com,8731
download.flvdome.com,7518
submit.flvdome.com,7278
www.jd9.net,7102
auto.search.msn.com,6435
www.screenblaze.com,6187
msn.com,5666
all-internal.info,4478
cfg.353wanwan.com,3987
crl.verisign.com,3950
csc3-2004-crl.verisign.com,3945
digitalartsaward.com,3608
cts.hotbar.com,3009
mediaartsplaza.com,2851
www.fenomen-games.com,2813
ayb.host255-255-255-0.com,2792
ayb.host192-168-1-2.com,2792
ayb.host127-0-0-1.com,2792
config.ie.sogou.com,2623

Top nameservers (by md5)

ns1-6.wingdns.net.	10937	ns1-2.nameself.com.	9012
ns1-4.trafficclub.com.	8986	ns1-4.google.com.	8976
ns1-5.byet.org.	8928	ns1-2.dns.com.cn.	8845
ns1-2.bluehost.com.	8795	dns1-2.uni5.net.	8779
dns1-4.kinghost.com.br.	8771	ns1-2.ukraine.com.ua.	8755
ns11-16.bigwww.com.	8752	ns,ns2,ns3.pipni.cz.	8744
ns1-3.surf-town.net.	8739	ns1-2.ignum.com.:	8738
dns,dns2.site5.com.	8737	ns1-4.cloudns.net.	8736
ns1-4.serveriai.lt.:	8735	ns1-3.cnchost.com.	8734
ns1-2.infobox.org.	8734		

Domain Name Characteristics

	Baseline Sample	All Malicious Domains
Two-Labels (example.com)	3227 (11% of)	67,398 (56% of)
Three-labels (www.example.com)	7204 (25% of)	45,944 (38% of)
Dynamic DNS	36 (0% of)	22,153 (18.5% of total, 50% of 3-label)

Registrars and Dynamic DNS

Dynamic DNS

- 22,153 out of 119,385
- 18.5% of total, but nearly 50% of the 3rd level domains)

Registrars (2nd Level Domains)

- 67,398 out of 119,385
- 56% of total

75% of malicious domains

Lifetimes

	Malicious Domains	Random Baseline
Lifetime	104 days	110 days
After Removal of Akamai, rbls, and cdns	105 days	165 days

RBLs – Remote Block Lists

CDNs – Content Distribution Networks

Parked Domains

Domains that are “parked” on a non-operational IP address

- Often unroutable IP space (192.168.1.1, 127.0.0.1)
- Sometimes strange IP addresses (1.2.3.4, 1.1.1.1)
- Other times popular IP address (google, akamai, microsoft)

Parked examples

- domains parked at google ip space:

a.emmai.info	ac3n.info	adslstats.net
boqeouti.org	bujozami.cn	custome.cn
dreamnaut.no-ip.info	f.unicat.org	forbes-2009.com
forrodesejomusical.com.br	google-resolve.servehttp.com	gooogle.com
hackhound.org	hurt23.mine.nu	lanzadorx.com
mail.xakep.ru	mgq2748586.s124.288idc.com	omfgitzpjx.info
ruvegaro.cn	sickshot.us.to	speedytorrents.net
vampire008tw.xxxy.info	viptrips.net	wmi.pho24.info
www.265.com	www.autokiemthe.com	www.cor.re.it
www.emilgiochi.it	www.lanzadorx.com	www.nepalsrl-italy.com
www.nuevaq.fm	www.opensc.ws	yc.shockwavesfx.com

Normal Parking

20091129	expired.domain.com	192.168.118.26
…	….	…
20091209	expired.domain.com	192.168.118.26
20091210	expired.domain.com	127.0.0.1
20091211	expired.domain.com	127.0.0.1
20091211	expired.domain.com	127.0.0.1
20091212	expired.domain.com	127.0.0.1
20091213	expired.domain.com	127.0.0.1
20091214	expired.domain.com	127.0.0.1
20091215	expired.domain.com	127.0.0.1
20091216	expired.domain.com	69.64.155.121
20091217	expired.domain.com	69.64.155.121
20091218	expired.domain.com	69.64.155.121
20091219	expired.domain.com	69.64.155.121

Normal Parking

20091129	expired.domain.com	192.168.118.26
…	….	…
20091209	expired.domain.com	192.168.118.26
20091210	expired.domain.com	
20091211	expired.domain.com	
20091211	expired.domain.com	
20091212	expired.domain.com	
20091213	expired.domain.com	
20091214	expired.domain.com	
20091215	expired.domain.com	
20091216	expired.domain.com	69.64.155.121
20091217	expired.domain.com	69.64.155.121
20091218	expired.domain.com	69.64.155.121
20091219	expired.domain.com	69.64.155.121

Example of Parking until Operations

20091129	badguy.com	255.255.255.254
…	….	…
20091209	badguy.com	255.255.255.254
20091210	badguy.com	123.117.77.10
20091211	badguy.com	125.34.77.52
20091211	badguy.com	255.255.255.254
20091212	badguy.com	255.255.255.254
20091213	badguy.com	255.255.255.254
20091214	badguy.com	255.255.255.254
20091215	badguy.com	255.255.255.254
20091216	badguy.com	97.67.118.26
20091217	badguy.com	97.67.118.26
20091218	badguy.com	255.255.255.254
20091219	badguy.com	255.255.255.254

Example of Parking until Operations

20091129	badguy.com	
…	….	
20091209	badguy.com	
20091210 - Thursday	badguy.com	123.117.77.10
20091211 - Friday	badguy.com	125.34.77.52
20091211	badguy.com	
20091212	badguy.com	
20091213	badguy.com	
20091214	badguy.com	
20091215	badguy.com	
20091216 – Thursday	badguy.com	97.67.118.26
20091217 - Friday	badguy.com	97.67.118.26
20091218	badguy.com	
20091219	badguy.com	

Fast Flux

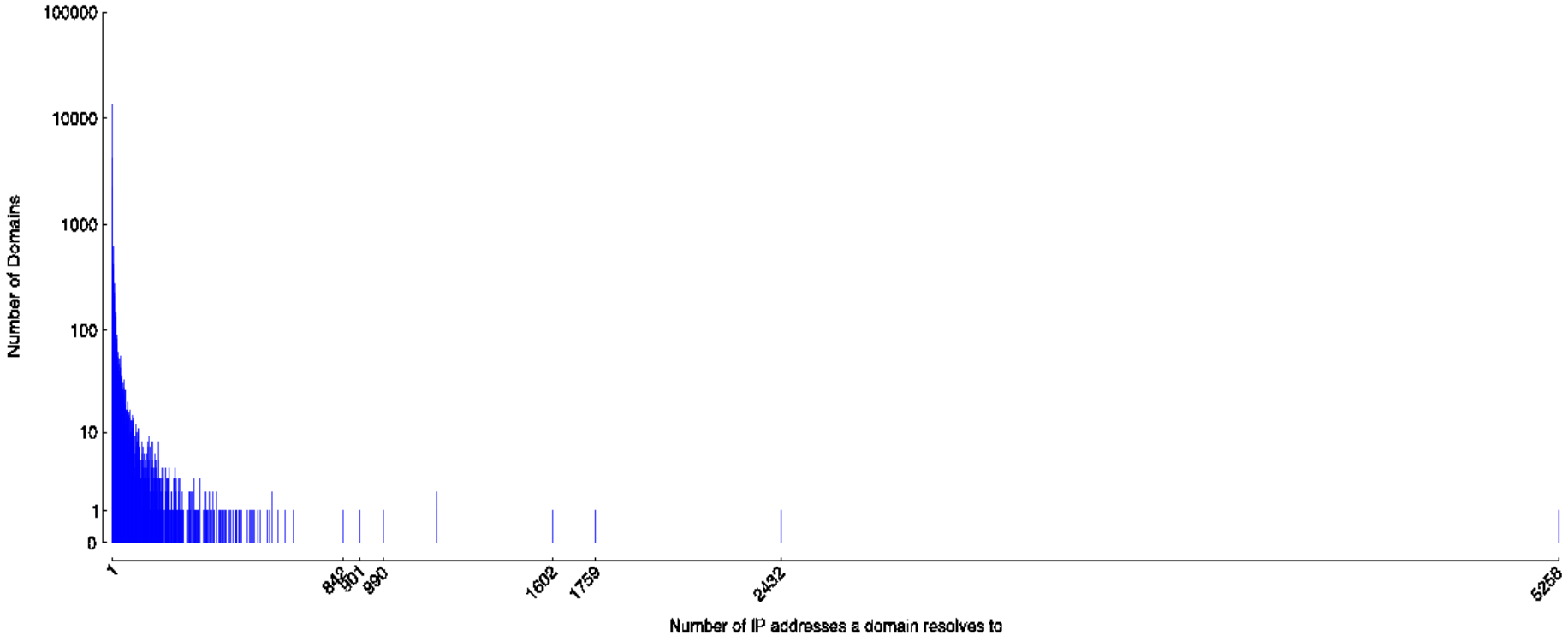
“fully qualified domain name (such as www.example.com) to have multiple (hundreds or even thousands) IP addresses assigned to it. These IP addresses are swapped in and out of flux with extreme frequency, using a combination of round-robin IP addresses and a very short Time-To-Live (TTL) for any given particular DNS Resource Record (RR)”

old FastFlux working definition

Previous definition:
20 different ASNs w/ 25 different IP-addresses

TTL of less than 2000 seconds

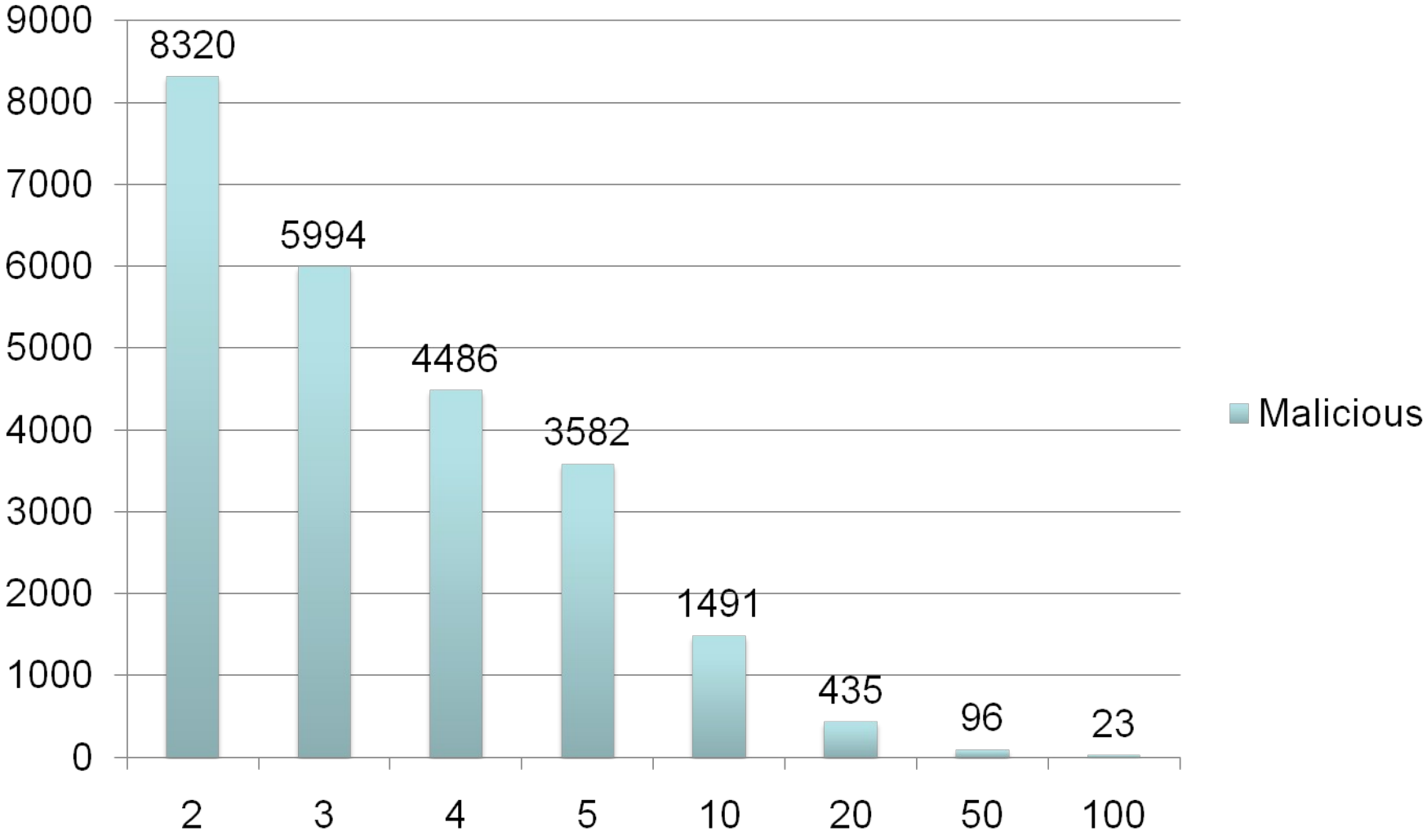
FastFlux Hosting



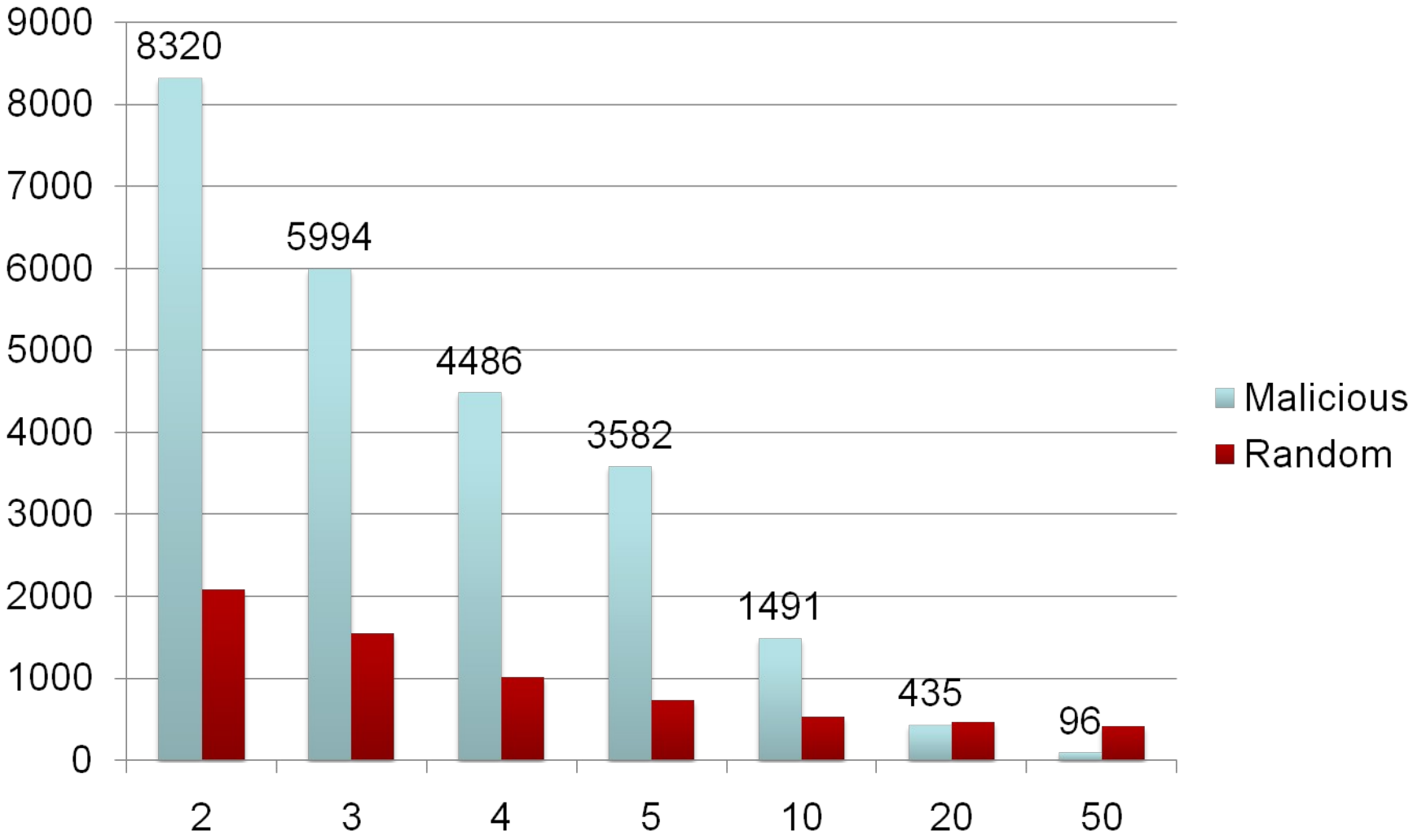
Most IPs per Domain – Unsophisticated Criminals

Domain	IPs	md5s	handle	Notes
02fgu145501.cn	4491	44	no	Unknown fastflux botnet c2
viotto.dyndns.org	1602	1	yes	discusses SpyNet 1.8 and 2.0
momo26.no-ip.biz	990	1	yes	ZeuS C2, momo.exe, not in virustotal
malchh.no-ip.biz	901	3	yes	Turkojan v1, discussing turkojan v4
spy-pc1.no-ip.biz	842	1	no	Poison/BiFrose
yousufshah.no-ip.biz	661	2	yes	discussing facebook passwords, CyberGate
souhil5.no-ip.info	632	1	yes	Poison/BiFrose, discussing biFrose
semao.myftp.biz	607	2	yes	biFrose Variant

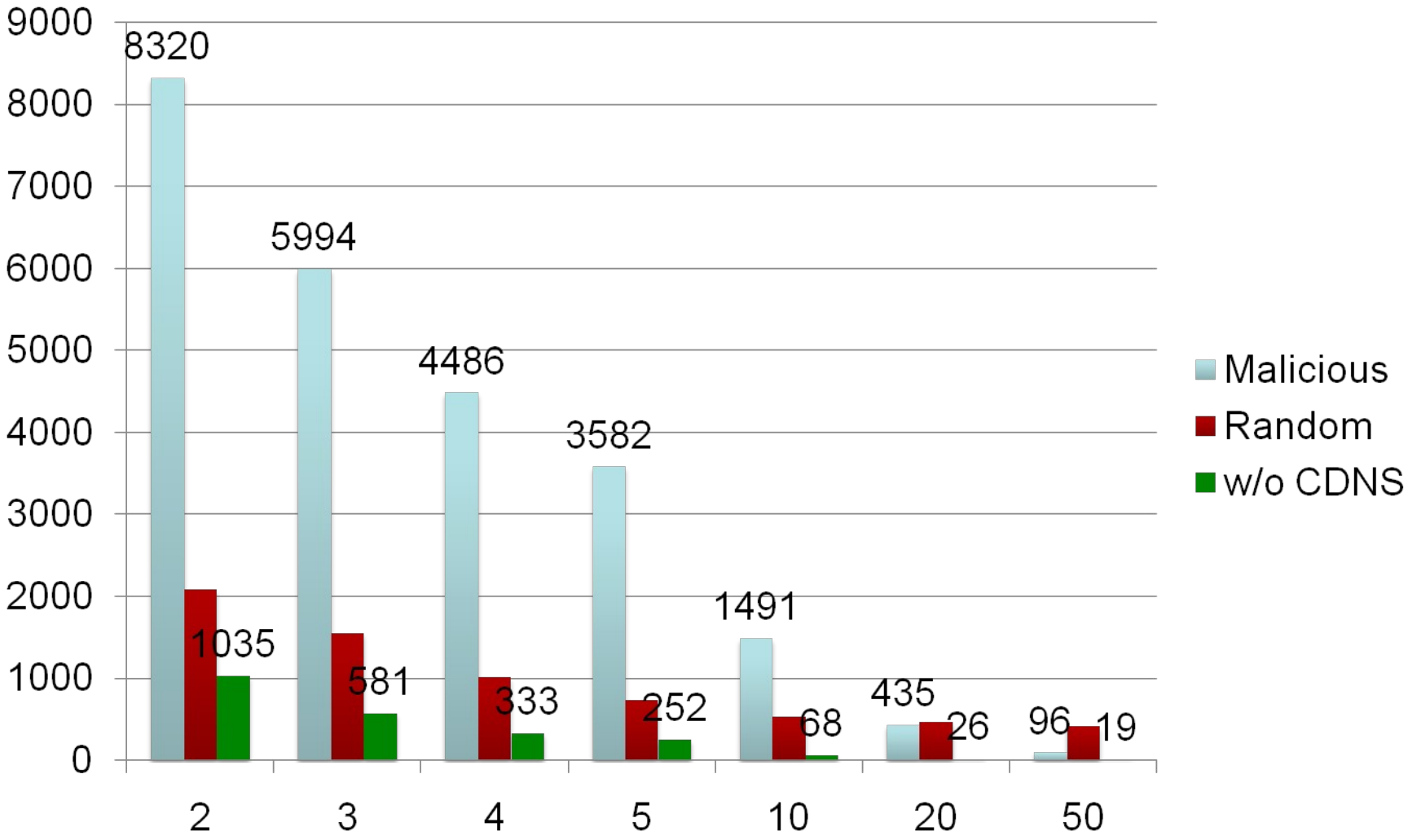
Flux Spread of Malicious Domains



Flux Spread w/ Random Sample



Flux Spread w/ CDNs removed



New Algorithm

- domains with:
  - 20 or more A recs
  - IPs are in 20 or more ASNs
  - of those domains:
    - find IP sets with more than 5 addrs in common
    - white list known CDNs

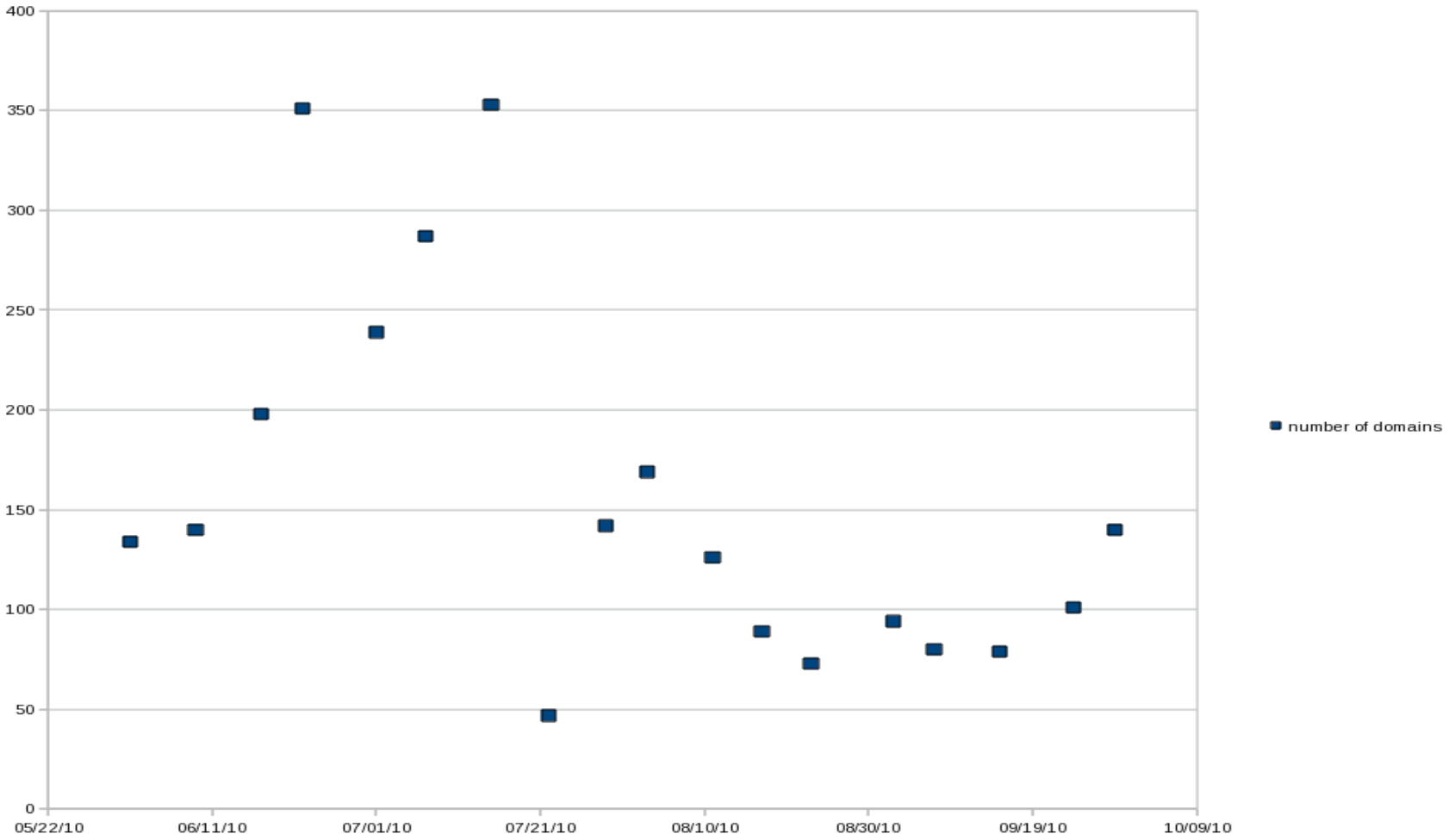
what we're finding

6/01/2010:
cc.allaboutc0ntrol,com.haijeihefoobeekahkohweto,net.jdhyh1230jh,
ru.mmjl3l45lkjbdb

7/15/2010:
com.drunkjeans,com.earlymale,com.hillchart,com.hugejar,com.roundstorm,
com.tightsales,ru.dealyak,ru.greedford,ru.heroguy,ru.jarpub,
ru.marketholiday,ru.pantscow,ru.problemdollars,ru.raceobject,ru.tintie

08/29/2010:
com.first-wave-aug,com.hotsku,com.iwfybfywi,com.mortalconbat,
com.qrtmpqpmlolpmu,com.uuvqvkoqrrdtli,net.instamfan,net.roundhome,
ru.adaichaepo,ru.aijohcolev,ru.dahzunaeye,ru.deilaeyeew,ru.hazelpay,
ru.iesahnaepi,ru.iveeteepew,ru.jocudaidie,ru.johgheejae,ru.kaithuushi,
ru.ohphahfech,ru.ootaivilei,ru.purplepron,ru.railuhocal

Flux Statistics



Domain Flux

Definition:

generation of a large number of pseudo-random domains using the same seed

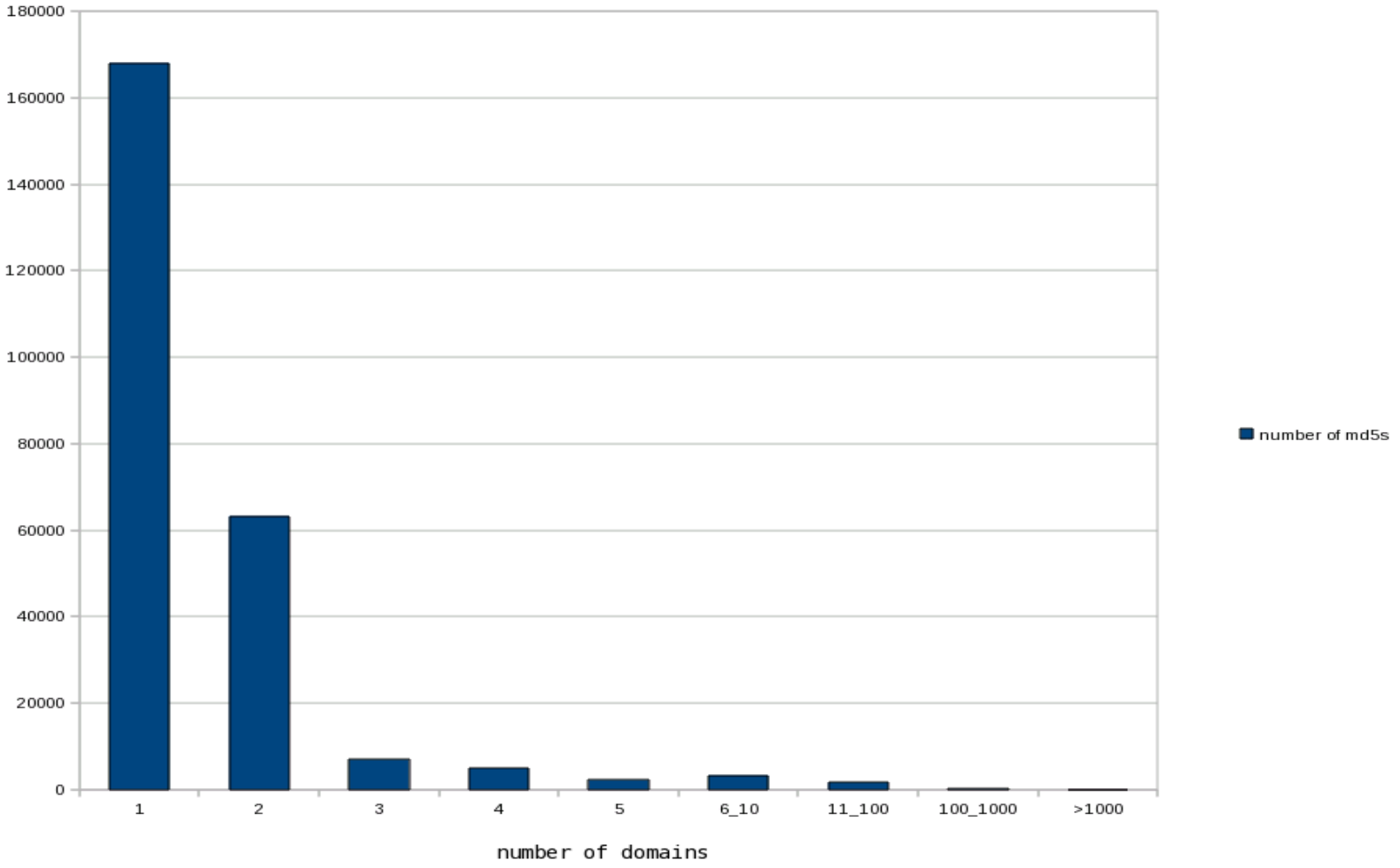
1.) to hide communication channel

2.) to prevent domains being blocked

looks like:

```
aabdykuiwcymao.biz,aaemxwiugkeq.info,aafueyeoya.biz,aaiahiiugkeq.biz,
aaiavsiugkeq.biz,aakmbsiugkeq.biz,aaonhaiugkeq.info,aapgpqeoya.info,
abahfodsholapet.cc,abcyxmnansnan.com,abdqbenansnan.com,acjybkdsholapet.org
OR:
ysggof.1dumb.com,yxnhwhmrckk.dynserv.com,yxrxopwfrvz.yi.org,
yybvnivcjei.3-a.net.,yzscnmh.afraid.org,zbttjqq.afraid.org,
zdhmosqbmuy.3-a.net,zeczrpsck.dynserv.com,zibjyomx.hn.org,zpkwnmip.hn.org,
zppkhkxsawq.yi.org.,zqptrlup.dynserv.com,zsbbrdwp.dynserv.com
```

Domains per MD5



NxDomain

need to capture to find:

1.) domain flux

2.) other domains seen for only one day

- 3096 different md5s (1.2%)

3.) What else are we missing?

YAF

yet another flowmeter

http://tools.netsa.cert.org/yaf

- initial public release Mar. 28, 2006
- processes packets from pcap or live capture
- exports flow to IPFIX format
- tcp reassembly, fragment reassembly
- widely deployed
- supports 10Gbs capture

IPFIX

RFC 5101,5102,5103 (previously Cisco Netflow v9)

abstract data types:

unsigned8,unsigned16,unsigned32,unsigned64,signed8,signed16,
signed32,signed64,float32,float64,boolean,macAddress,octetArray,
string,dateTimeSeconds,dateTimeMilliseconds,dateTimeMicroseconds,
dateTimeNanoseconds,ipv4Address,ipv6Address

over 200 Information Elements already defined

very widely supported in hardware and software

YAF current status

- as of Jul 27, 2010
  - now supporting:
    - udp-uniflow
    - FTP,HTTP,IMAP,RTSP,SIP,SMTP,SSH,DNS, IRC,NNTP,POP3,SLP,TFTP
    - custom protocol decoders as plugins
      - as C code or regex