Spam, Domain Names and Registrars

Joe St Sauver, Ph.D. (joe@uoregon.edu)
Senior Technical Advisor
Messaging Anti-Abuse Working Group

MAAWG 12th General Meeting, San Francisco
February 18th-20th, 2008

http://www.uoregon.edu/~joe/maawg12/

Disclaimer: all opinions expressed in this talk are solely those of the author, and do not necessarily represent the opinion of MAAWG or any other entity. Recognizing that conditions are continually evolving over time, please carefully re-evaluate this data yourself before drawing any conclusions from it or taking any action based on it. This analysis is not intended to be used for operational purposes. It is offered as is, where is, with no warranty or assertion of fitness for any purpose whatsoever

Attacking Spam By Focusing on the Resources That Spammers Need

- In order to spam, spammers require access to a variety of resources.
- For example, let's assume that in order to send spam, a spammer needs (at a minimum):

  -- spam sending software
  -- addresses to spam
  -- hosts on unblocklisted IP addresses through which to route their spam (these may be compromised consumer hosts on a rented botnet, for example)
  -- hosting for spamvertised web sites (whether on so-called bullet proof hosting, fast flux hosting, or whatever), and
  -- domain names for that hosting, among other things.
- **If we can cut off spammer access to at least one those required resources, <u>spamming becomes harder</u>.**

Domain Names Are One Fundamental Component of the Internet Ecosystem

- Domain names are a fundamental part of the Internet, and it would be hard to imagine the Internet working without them.
- **Those who abuse email unquestionably depend on the continued availability of domain names.**
- For example, in a typical pillz spam, the spam message may urge the spam recipient to visit a given domain name (e.g., web page "URL" or "URI") to buy a controlled substance.
- Just a single pillz spam campaign might use **dozens or even hundreds** of domain names.
- You might wonder, "Why would a spammer use **so many** domain names? Why not just spamvertise the address of **one** web site and be done with it?"
- There are actually many reasons. A few of those are...

The Many Reasons for Spamvertising Many Different Domain Names

- **Avoiding SURBL/URIBL Filtering:** Let's assume that a foolish spammer only spamvertised a single URI for weeks (or months!) on end. Once that URI got identified, it would be a trivial task to filter messages referring to that URI. Clearly, spammers need to continually introduce new domains as their old domains get identified and SURBL or URIBL listed.
- **Trying to Stay Off Law Enforcement (LE)'s Radar:** Prioritization of official anti-spam efforts also is often volume-related: "let's go after the worst of the bad guys first; we'll deal with all the little guys later." If a spammer spamvertises multiple domain names (rather than just one domain name), it becomes at least marginally harder for LE to mechanically aggregate all that spam traffic, thereby potentially reducing a spammer's chance of being targeted for prosecution.

The Many Reasons for Spamvertising Many Different Domain Names (2)

- **Load Balancing and/or Enhanced Survivability:**
  Use of multiple domain names also makes it possible for the spammer to do load balancing and/or to increase the survivability of his/her web site. For example, spamvertised domains A, B, and C might be configured to go to backend server farm #1, while spamvertised domains D, E, and F might get sent to backend server farm #2. Any attempt to take that spammer down would require hitting both of those backend server locations more or less simultaneously – and you'd also need to tear down all of those domain names so the spammer couldn't simply repoint that set of domains to some third backend server location. Clearly spamvertising multiple domain names increases a spammer's ability to manage his/her traffic and to survive attempts at interference

The Many Reasons for Spamvertising Many Different Domain Names (3)

- **Market Segmentation:** Use of multiple domain names also facilitate spammer market segmentation. For example, a pillz spammer might use some domain names to route potential benzodiazepine customers directly to pages selling benzodiazepines, while customers for erectile dysfunction medications might be sent to different pages offering those medications, instead.
- **Tracking/Crediting Affiliate Traffic:** Spamvertising multiple domain names also makes it easy for spammers to track and credit affiliate traffic. The spammer assigns a different set of domain names to each affiliates, and then checks the referrer logs, watching to see which of those assigned domains ends up referring traffic to the spammer's real web site or sites.

Some of The Hassles of Having to Operate In A "Many Domain World"

- There are some **disadvantages** to spammers having to operate in a "many domain world," including (among others):

  -- purchasing large numbers of domains may contribute to the erosion of spammer profits (unless the spammer owns or effectively controls his/her own registrar)

  -- using many different domains increases operational complexity, and creating and efficiently managing large numbers of spam-related domains may require automated domain name provisioning software or other assistance

  -- effectively re-contacting customers who respond to spam via a spamvertised web site may require special steps (such as polling customers by phone or by email for "refills"), since the spamvertised domain the customer used last time may no longer be operational this time

Spamvertised URIs and URI Block Lists

- Even though spammers may continually introduce new domains to be spamvertised, URI block list operators have done a **very good** job of keeping up with the spammers as new spammy domains have been created.
- Because of the extreme effectiveness of URI-based block lists, some spammers have been forced to resort to sending:
  -- spam which doesn't use or need a URI (such as stock pump-and-dump spam),
  -- spam which attempts to use image files in an effort to keep embedded URIs from being mechanically "read",
  -- spam which attempts to channel responses via an email drop box address or a VoIP phone number (as is the case in many 4-1-9 advance fee fraud scam spam), or
  -- spam which attempts to hide spamvertised URLs behind web redirector pages, search engine search strings, etc.

Spammers Also Need Domain Names for Other Purposes

- While spammers need domain names to spamvertise, they also need domain names for other operational purposes.
- For example, they need domain names to use to name their servers, so that when that server connects to a remote mail server, it has a domain name, not just a raw IP address. Why is this important? Well, Some ISP have published email technical standards which require connecting hosts to have rDNS (http://postmaster.aol.com/guidelines/standards.html states that "AOL's mail servers will reject connections from any IP address that does not have reverse DNS (a PTR record")), and having rDNS requires having a domain name.
- Spammers also need domain names for use in HELO/EHLO and in message headers (such as in From: headers). Things like SPF/SenderID may limit their ability to use others'!

Okay, So Spammers Need Domain Names. Where Do They Get Them?

- The get them from registrars (or registration service providers), just like anyone else. Well, *almost* just like everyone else….
- Some registrars really don't like spammers, and if they find they've unintentionally sold a domain name to a spammer, or they've got a domain name that has bogus whois data, they'll promptly suspend that domain (yes, this is allowed, see Spamhaus' discussion of this at http://www.spamhaus.org/faq/answers.lasso?section=Generic%20Questions#127).
- If **enough** registrars became intolerant of spam-related domains, domain non-availability could become a critical spam choke point. Registrars and registration service providers thus have the potential to play a crucial role in the fight against spam.

Not All Registrars May Be Willing to Help

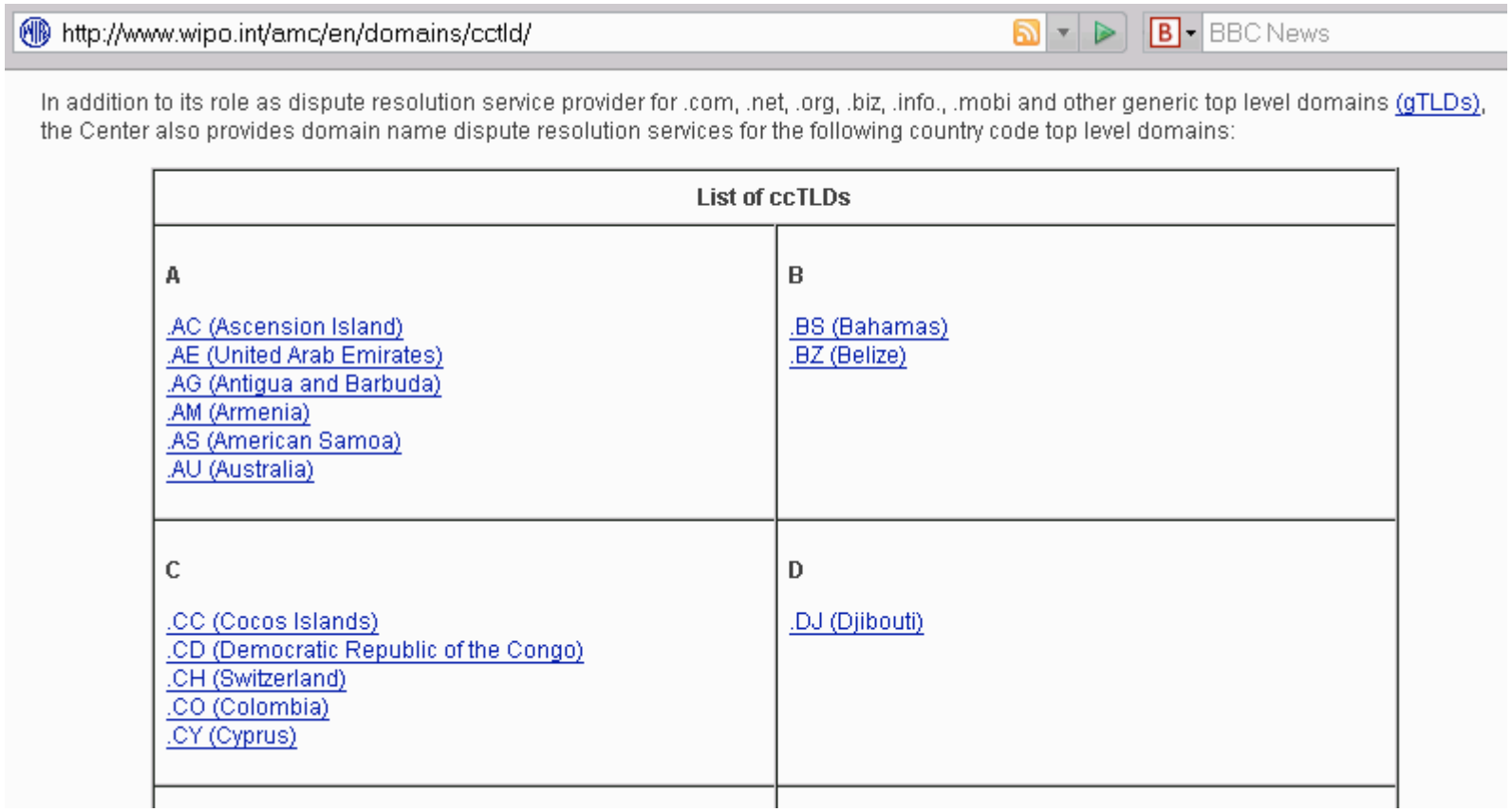
- We know, for example, that there are some registrars or registration service providers who offer so-called *bullet proof domain names* (check for that phrase in your favorite search engine to see some examples).
- Of course, if you're a bad guy and need a domain name that won't be shut down in response to complaints, you should plan to pay a premium for that privilege (~$100/domain?).
- I recognize that those "bulletproof" registrars may be unwilling to refrain from selling domains to spammers, since that may be their targeted/primary customer base. That may seem worrisome, but it's actually okay -- IF we're able to identify those registrars and the domains they've sold
- We also need to recognize that we don't live in just a dot com/dot net/dot org world. We also need to think about other top level domains, such as ccTLDs.

Margins for Some TLDs May Be Thin, Limiting Resources for Abuse Handling

- For example: see '"Experience .CN Domain Name for One Yuan Campaign" will extend till 31st December, 2008,' http://www.cnnic.cn/html/Dir/2007/12/27/4953.htm
- For those of you who don't routinely memorize foreign exchange rates, 1 Yuan = US$ 0.139 as of 2/10/2008
- At $0.139/domain, there's NOT going to be a lot of money available to investigate .cn domain name abuse complaints.
- For example, I bet you didn't know that "your" company's domain name may already be registered by someone in .cn, e.g., maawg.cn is currently at 218.244.140.62
- Rebuttable hypothesis: at just $0.14/domain, domain name speculation and squatting may now be fairly rampant in the dot cn TLD. So how do domain name disputes get resolved?

For Example, Does the Normal WIPO Dispute Resolution Process Apply?

- The gTLDs, and many ccTLDs, use the WIPO framework (http://www.wipo.int/amc/en/domains/cctld/) but .cn does not:



http://www.wipo.int/amc/en/domains/cctld/

BBC News

In addition to its role as dispute resolution service provider for .com, .net, .org, .biz, .info., .mobi and other generic top level domains (gTLDs), the Center also provides domain name dispute resolution services for the following country code top level domains:

List of ccTLDs	
A .AC (Ascension Island) .AE (United Arab Emirates) .AG (Antigua and Barbuda) .AM (Armenia) .AS (American Samoa) .AU (Australia)	B .BS (Bahamas) .BZ (Belize)
C .CC (Cocos Islands) .CD (Democratic Republic of the Congo) .CH (Switzerland) .CO (Colombia) .CY (Cyprus)	D .DJ (Djibouti)

If You'd Like To Read About The Rules Which DO Apply to .cn Domains...

www.cnnic.net.cn/html/Dir/2006/02/14/4008.htm states:

- "Article 2. The policy is applicable to disputes result from registration or usage of domain names. [...] the Dispute Resolution Service Providers do not accept the Complaint regarding domain names with registration term of over (including) **TWO years**. [emphasis added]

www.cnnic.net.cn/html/Dir/2006/03/15/3655.htm states:

- "Article 8: Unless otherwise agreed by the Parties or determined in exceptional cases by the Panel, the language of the domain name dispute resolution proceedings shall be **Chinese**. The Panel may order that any documents submitted in languages other than Chinese be wholly or partially translated into Chinese." [emphasis added]

And Speaking of Dot cn Domains...

- We're entering a brave new world where English language domain information (or even Roman character sets!) shouldn't even be presumed in whois data:

.CN Registry WHOIS Data

Domain Name	maawg.cn
Domain Status	ok
Registrant Name	测试
Administrative Email	cnreg@hichina.com
Registrar	北京万网志成科技有限公司
Name Server	dns15.hichina.com
Name Server	dns16.hichina.com
Creation Date	2007-05-30 09:08
Expiration Date	2008-05-30 09:08

.cn .com.cn .net.cn .org.cn .gov.cn .ac.cn .bj.cn .sh.cn .tj.cn .cq.cn
.he.cn .sx.cn .nm.cn .ln.cn .jl.cn .hl.cn .js.cn .zj.cn .ah.cn .fj.cn
.jx.cn .sd.cn .ha.cn .hb.cn .hn.cn .gd.cn .gx.cn .hi.cn .sc.cn .gz.cn
.yn.cn .xz.cn .sn.cn .gs.cn .qh.cn .nx.cn .xj.cn .tw.cn .hk.cn .mo.cn

Go on query

Quick "Quiz"

- Pronounce the registrant's name from the preceding slide.
- What's his/her snail mail postal address? Phone number?
- Is this a "domain name privacy" registration where hichina.com has done a proxy registeration of this domain for someone else? A domain owned by hichina.com itself?
- I showed you the .cn registry whois. Is there a referral to a registrar whois server with more detail? If so, what's the name of the registrar's whois server you should check?
- How many .cn domains can you query per hour/day/ whatever before your IP address gets rate limited/blocked?
- How many provincial and other subdomains are available below dot cn addition to the "top level" dot cn domain? (I'll stipulate and agree that you may not be allowed to register domain names in some of them, e.g., gov.cn for example)

And If You're Still Not Interested In China

- I'd encourage you to look at Google's February 2008 tech report, "All Your iFRAMEs Point to Us," by Niels Provos, Panayiotis Mavrommatis, Moheeb Abu Rajab, and Fabian Monrose, which is available online at http://research.google.com/archive/provos-2008a.pdf
- Specifically, note the comments on pdf page 9 of that report: "One noteworthy result is the geographic locality of web based malware. […] The results show that a significant number of Chinese-based sites contribute to the drive-by problem. Overall, 67% of the malware distribution sites and 64.6% of the landing sites are hosted in China."
- See also report page 13, stating that "malware distribution sites are concentrated in a limited number of /8 prefixes. About 70% of the malware distribution sites have IP addresses within 58.* -- 61.* and 209.* -- 221.* network ranges." <cough>

But Let's Move On: What About gTLD Domain Names With Bad Whois Data?

- gTLD domains are required, pursuant to the registrar's accreditation agreement with ICANN, to maintain accurate whois data for their domains (see http://www.icann.org/whois/whois-data-accuracy-program-27apr07.pdf).
- From time to time, however, particularly if you're looking at spamvertised domain names, you may run into names with bad or incomplete whois data.
- For instance, when you check whois for a domain you may find that the street address given for the domain registrant (or administrative contact or technical contact) may be missing, incomplete, inconsistent, or otherwise invalid (www.usps.gov/zip4 is great for checking US addresses)
- The General Accounting Office has previously investigated the issue of bad whois data for Congress.

The 2005 GAO Whois Data Study

- In November 2005, the General Accounting Office released, GAO 06-165, "INTERNET MANAGEMENT: Prevalence of False Contact Information for Registered Domain Names" (see http://www.gao.gov/new.items/d06165.pdf)
- That study estimated that 8.65% of all .com/.net/.org domains had at least one patently false or incomplete required fields in whois.
- The study also found that when they looked at a random sample of 900 domains (300 each from .com, .net and .org) and identified and reported 45 of those domain names for identified inaccuracies or omissions, a month later 33 of the 45 domains (73%+) did **not** have their inaccuracies or omissions corrected despite having been reported.

A Concrete Example From This Month

What Does the Whois Data Look Like For That Domain?

```
[whois.dns.com.cn]
Domain Name.......... mrbobjones.com
Creation Date........ 2008-01-27 13:53:12
Registration Date.... 2008-01-27 13:53:12
Expiry Date.......... 2009-01-27 13:53:12
Organisation Name.... Ruby Diamond Bhd
Organisation Address. Brail City  } not much of an
Organisation Address.             } address, eh?
Organisation Address. Brazil      }
Organisation Address. 45123       }
Organisation Address. WG          }
Organisation Address. BR          }
```

[continued next slide]

What Does the Whois Data Look Like For That Domain? (2)

```
Admin Name.......... Ruby Diamond Bhd
Admin Address........ Brail City
Admin Address........
Admin Address........ Brazil
Admin Address........ 45123
Admin Address........ WG
Admin Address........ BR
Admin Email.......... brazil@gmail.com
Admin Phone.......... +86.452133
Admin Fax............ +86.5457331
[etc]
Name Server.......... ns4.jokens.com [116.199.138.24]
Name Server.......... ns3.jokens.com [116.199.135.168]
Name Server.......... ns2.jokens.com [58.20.84.92]
Name Server.......... ns1.jokens.com [221.122.64.14]

[All of those name server IP's are on the SBL]
```

Reporting Inaccurate Whois Data

- If you do run into a gTLD domains with bad whois data, you can file a complaint about it via http://wdprs.internic.net/
- According to http://www.icann.org/whois/whois-data-accuracy-program-27apr07.pdf , there were about 6.35 non-duplicative reports made per 10,000 .com domains (.com domains accounted for nearly 75% of all complaints).
- That same report notes that a relatively small number of reporters, **just 20 people** (<1% of all those who filed reports) **accounted for over 87% of all 50,189 inaccuracy reports,** and just *one* person accounted for approximately 40% of all inaccuracy reports. Quoting from the report, *"From both anecdotal information received by ICANN and text accompanying the body of WDPRS reports received, we conclude that most, if not all, of the high volume reporters are driven by a concern about abuses involving email."*

Those Are Fascinating Statistics And Ones Which Raise Some Questions

- Why are just twenty reporting parties carrying the lion's share of the burden when it comes to reporting domain names with bad whois data to Internic? Why isn't everyone who's here today reporting domain names with bad whois data when they run into them?
- Would a bulk-reporting interface help, so that multiple domains all sharing the same whois data defects can be reported en-masse, instead of onesie-twosie style?
- Why aren't leading providers pressing ICANN to deal more aggressively with accredited registrars who aren't fulfilling their obligations with respect to maintaining whois data accuracy? If a domain has bad whois data, there's no reason why it should still be up/uncorrected months later.
- There are other domain/whois-related issues, too…

For Example: The Glue Record Problem

- Glue records are static name server records in the TLD created to help bootstrap access to that domain
- So if a bad domain name gets taken down, what happens to the name server glue records which may be associated with that domain? Do they also go away?
- The answer is, "It depends." It is not uncommon to run into situations where a particular domain name no longer exists, but glue records associated with that domain remain active (and usable!) in conjunction with other potentially abused domains.
- Does this mean that we should we work towards eliminating all glue records? No. For example, if there were to be a requirement that glue records be present and correct for all domains, things like double fast flux domains would become extremely difficult for the bad guys/bad gals to implement.

ICANN SSAC Comments to the GNSO Regarding WHOIS Studies (7 Feb 2008)

[see http://www.icann.org/committees/security/sac027.pdf]

- The ICANN Security and Stability Advisory Committee recently provided comments on whois related issues to the ICANN Generic Names Supporting Organization, noting in part:

  -- "The GNSO should continue current and proposed work to resolve legal and privacy issues within the existing WHOIS framework."

  -- "ICANN should take aggressive measures with respect to improving registration data accuracy and integrity. Future agreements should include data accuracy and integrity (e.g., archival and restoration) guidelines and should include provisions for sanctions or other penalties for those who do not comply with these guidelines."

ICANN SSAC Comments to the GNSO Regarding WHOIS Studies (continued)

-- "The ICANN community should adopt an Internet standard directory service as an initial step toward deprecating the use of the WHOIS protocol in favor of a more complete directory service."

-- 'ICANN should work with all TLD registry operators to develop a timeline and transition plan for migrating from the current WHOIS service to a successor Internet “domain” directory service.'

- Clearly I'm not the only one frustrated by the current state of affairs with respect to the accuracy of domain name data in whois. :-)

Of Course, If Domains Are Registered Via A Proxy Registration Service...

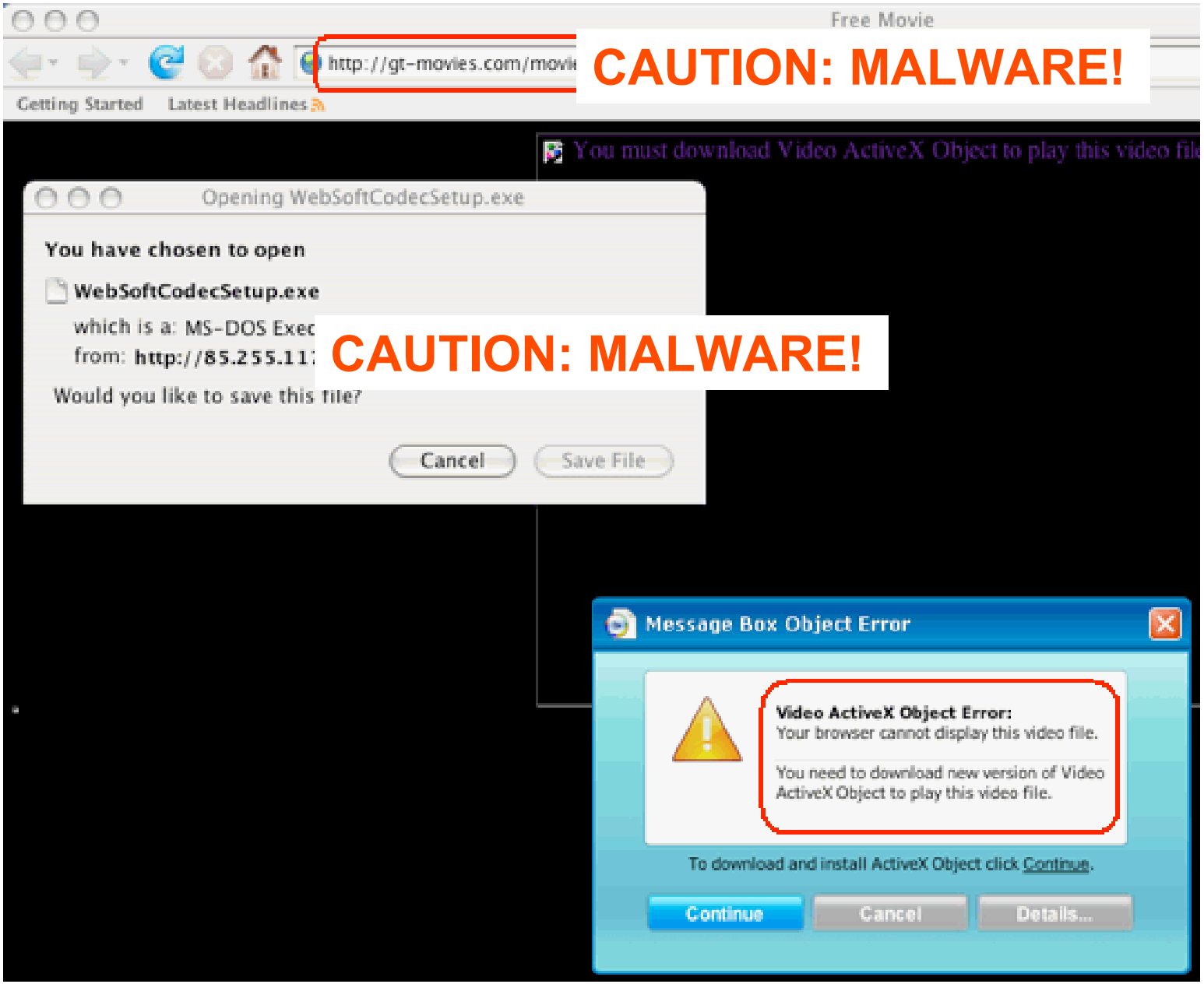
- ... then you won't see much in the way of the underlying domain owner's contact data to validate and/or to report.
- While people may have perfectly valid and legitimate reasons for wanting to use a proxy registration service, it is unfortunate that many abusive domains are also registered via proxy registration services.
- As a result, at least one DNS-based whois service, **www.openwhois.org**, has begun to offer a service which will allow you to check to see if a domain of interest has been registered with a proxy registration service, and if it has, well, then you have the option of taking whatever action you deem appropriate. That type of test can be easily integrated into a spam scoring system such as SpamAssassin, etc

Why Are Some Proxy or Private Domain Registrations Problematic?

- **Proxy registrants may be effectively impossible to map to a real person or company**. Proxy registration services may initially shield the identity of their customer, and if/when a court order or other legal paperwork compels them to disclose the underlying identity of the customer, that data may be turn out to be completely bogus since it is subject to review only by the proxy registration service provider itself.
- **Proxy registrations make it more difficult to accumulate reputation across domain names.** That is, if I find that domains A, B, C, D, and E all are registered to a particular individual, and all are spammy, if I find additional domains F or G or H, I might be predisposed to assuming those domains are spammy too, until proved otherwise. Proxy registrations make it impossible to do that sort of thing...

Some Proxy Registration Providers Do A Good Job Of Handling Abuse

- For example, some proxy registration service providers are well known for their policy of cancelling a domain's proxy registration status if a proxy registered domain is used for spam or otherwise unacceptable purposes, "outing" (publishing) the customer's normally withheld contact details at that time. Good job!
- Other registrars (or proxy registration service providers) may be less aggressive in dealing with problematic domain names. A prime indication that problems may exist may be restrictive proxy registration complaint communication policies (such as only accepting complaints via certified mail, or only accepting complaints via email, or only accepting complaints made by telephone, or only accepting complaints made via a web form). Again, let's consider an example...


Free Movie
http://gt-movies.com/movie
CAUTION: MALWARE!
Getting Started
Latest Headlines
You must download Video ActiveX Object to play this video file
Opening WebSoftCodecSetup.exe
You have chosen to open
WebSoftCodecSetup.exe
which is a: MS-DOS Exec
from: http://85.255.11
Would you like to save this file?
Cancel
Save File
CAUTION: MALWARE!
Message Box Object Error
Video ActiveX Object Error:
Your browser cannot display this video file.
You need to download new version of Video ActiveX Object to play this video file.
To download and install ActiveX Object click Continue.
Continue
Cancel
Details...

File **WebSoftCodecSetup.exe** received on **02.16.2008 22:59:12 (CET)**

Current status: **finished**

Result: **8/32 (25%)**

Compact | Print results

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.2.16.10	2008.02.15	-
AntiVir	7.6.0.67	2008.02.15	TR/Crypt.XPACK.Gen
Authentium	4.93.8	2008.02.16	-
Avast	4.7.1098.0	2008.02.16	-
AVG	7.5.0.516	2008.02.16	-
BitDefender	7.2	2008.02.16	-
CAT-QuickHeal	None	2008.02.16	(Suspicious) - DNAScan
ClamAV	0.92.1	2008.02.16	-
DrWeb	4.44.0.09170	2008.02.16	-
eSafe	7.0.15.0	2008.02.14	Suspicious File
eTrust-Vet	31.3.5541	2008.02.15	-
Ewido	4.0	2008.02.16	-
FileAdvisor	1	2008.02.16	-
Fortinet	3.14.0.0	2008.02.16	W32/Stration!tr.dldr

F-Prot	4.4.2.54	2008.02.16	-
F-Secure	6.70.13260.0	2008.02.15	-
Ikarus	T3.1.1.20	2008.02.16	-
Kaspersky	7.0.0.125	2008.02.16	-
McAfee	5231	2008.02.15	-
Microsoft	1.3204	2008.02.16	TrojanDropper:Win32/Nuwar.gen!lds
NOD32v2	2880	2008.02.15	-
Norman	5.80.02	2008.02.15	-
Panda	9.0.0.4	2008.02.16	-
Prevx1	V2	2008.02.16	-
Rising	20.31.50.00	2008.02.16	-
Sophos	4.26.0	2008.02.16	Mal/EncPk-CG
Sunbelt	2.2.907.0	2008.02.16	-
Symantec	10	2008.02.16	-
TheHacker	6.2.9.222	2008.02.16	-
VBA32	3.12.6.1	2008.02.14	MalwareScope.Worm.Nuwar-Glowa.1
VirusBuster	4.3.26:9	2008.02.16	-
Webwasher-Gateway	6.6.2	2008.02.15	Trojan.Crypt.XPACK.Gen

Additional information

File size: 88080 bytes

MD5: 0773804a68f0f94945bd43d81122b76d

SHA1: 3d2dace8353f96a4f648aa6e042a6f2110e86dc3

PEiD: -

packers: PEP, PEP

[whois.estdomains.com]
Registration Service Provided By: ESTDOMAINS INC
Contact: +1.3027224217
Website: http://www.estdomains.com

Domain Name: GT-MOVIES.COM

Registrant:
PrivacyProtect.org
Domain Admin (contact@privacyprotect.org)
P.O. Box 97
All Postal Mails Rejected, visit Privacyprotect.org
Moergestel
null,5066 ZH
NL
Tel. +45.36946676

Creation Date: 10-Feb-2008
Expiration Date: 10-Feb-2009

Domain servers in listed order:
ns2.gt-movies.com
ns1.gt-movies.com

So In That Example…

- We have a domain name which is associated with malware
- The domain name is hidden behind a privacy service reg
- The privacy service has chosen to severely constrain how they will accept complaints about their customers' domains
- Because the owner of that domain is concealed, it is harder for us to identify other domains which may exhibit similar misbehavior
- These factors make it hard(er) for us to combat the malware associated with that site or set of sites.
- I would assert that as this sort of thing becomes more common, a growing number of sites will begin to pay attention to things like www.openwhois.org's list of proxy/private registration service providers
- In fact, some sites may begin to scrutinize registrars and their associated characteristics more closely in general.

Some Accredited Registrars May Be Working From IP Addresses On The Spamhaus SBL and DROP Lists

- For example, what about www.estdomains.com, as seen in the preceding example?

  1) www.estdomains.com ==> 216.255.186.100
  2) 216.255.186.100 is on the Spamhaus SBL at SBL53319
  3) SBL53319 is on the Spamhaus DROP list

  If you wish to review that SBL listing, it is at http://www.spamhaus.org/sbl/sbl.lasso?query=SBL53319

  You can also review the listing criteria for DROP at http://www.spamhaus.org/drop/index.lasso

So Does This Mean You Want ICANN to Use Spamhaus Listing Status As An Accreditation/Reaccreditation Criteria?

- Not necessarily. What ICANN chooses to use or not as a gating criteria for accreditation or reaccreditation decisions is up to them, and I wouldn't presume to attempt to dictate policy to them or to the registrar community, except to note that registrars do have special access to critical community resources, and that special access implies (or should imply) a broad level of community confidence and trust.
- On the other hand, if an accredited registrar is broadly blocklisted, it will be operationally very hard for them to send email to many potential recipients, including registration-related emails for things such as verifying domain whois email points of contact, etc. *That* **may** be an issue which merits discussion in the ICANN community.

Accumulating Registrar Reputation Data

- As you check domain after spam-related domain with bad or hidden whois data, you may begin to notice registrar reputation-related data patterns emerge. For example, some registrars routinely and promptly suspend domains associated with bad whois data or with spam issues, while others may not.

- Castlecops has actually begun to formally track registrar performance when it comes to removing domains in response to complaints, tracking the results on a registrar-by-registrar basis for selected registrars. See the report on the following slide (sorry about the sideways orientation of that page).

Registrars

```
BILT     - BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD. DBA DNS.COM.CN
BIZCN    - BIZCN.com
Todaynic - Todaynic.com
XIN NET  - XIN NET TECHNOLOGY CORPORATION
```

Overall results

BILT Removals - 30%

Reported: 1,958

Suspended: 591

BIZCN Removals - 80%

Reported: 745

Suspended: 595

Todaynic Removals - 24%

Reported: 2,431

Suspended: 581

XIN NET Removals - 0%

Reported: 2,178

Suspended: 4

Castlecops Even Gives You A Breakdown of Domains Reported by "Brand" and Domain Names

http://wiki.castlecops.com/XIN_NET_Removals

XIN NET Removals

Contents [hide]

Canadian Pharmacy (651)

Reported on 2007-12-24 and 2007-12-27
alwaysor.com
bluedouble.com
bgrgld.com

But What of Other Registrars?

- I was curious about **all registrars**, not just the handful of Chinese registrars that Castlecops tracked (although I must say that I **do** find their work exceptionally interesting).

- The operators of the URIBL block list do look at the top 250 registrars associated with the domains they list, see http://rss.uribl.com/nic/

- The spacing of their report makes it hard for me to show it to you onscreen, so I've excerpted and slightly reformatted that data to show you on the following slide.

- Note, too: you can click on a link on http://rss.uribl.com/nic/ to see the hosts which are URIBL listed for that registrar

[Excerpted and slightly reformatted rendition of http://rss.uribl.com/nic/ data]

Rank	Registrar	Listed	Active	Percent
1	MONIKER ONLINE SERVICES, INC	2488	3007	82.74%
2	ENOM, INC	2197	3468	63.35%
3	TODAYNIC.COM, INC	1220	1228	99.35%
4	GO DADDY SOFTWARE, INC	947	3378	28.03%
5	XIN NET TECHNOLOGY CORPORATION	790	848	93.16%
6	DYNAMIC DOLPHIN, INC	486	489	99.39%
7	SPOT DOMAIN LLC DBA DOMAINSITE.COM	333	362	91.99%
8	BLOG.COM DIGITAL COMMUNICATIONS INC	327	334	97.90%
9	BIZCN.COM, INC	238	260	91.54%
10	BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD. DBA DNS.COM.CN	237	276	85.87%
11	INTERCOSMOS MEDIA GROUP, INC DBA DIRECTNIC.COM	191	373	51.21%
12	DIRECT INFORMATION PVT LTD DBA PUBLICDOMAINREGISTRY.COM	179	295	60.68%
13	PLANET ONLINE CORP	169	173	97.69%
14	GKG.NET, INC	152	216	70.37%
15	TUCOWS INC	147	1412	10.41%
16	REGISTER.COM, INC	144	683	21.08%
17	NETWORK SOLUTIONS, LLC	109	4433	2.46%
18	NUCLEAR NAMES, INC	80	81	98.77%
19	DOTSTER, INC	58	271	21.40%
20	DOMAIN CONTENDER, LLC	49	65	75.38%

The URIBL is *NOT* The Only URI Block List Out There. What Do We See for the SURBL URI Blocklist?

- I decided to see who was the registrar of record for the domain names listed on the SURBL (www.surbl.org), another publicly available and widely used URI block list
- The SURBL folks were good enough to give me rsync access to their list of domains for this purpose, thank you very much! As of 2/16/2008, the multi.surbl.org.rbldnsd zone is roughly 1.24 million entries long.
- If you've not seen a copy of the SURBL zone file, some of the URI hosts in the SURBL include numeric IP addresses, as well as domains from diverse TLDs. Obviously we're not going to be looking at any domain registrar data for numeric IP's. There are a few other domains we also can't process,..

Omitted SURBL Listed Domains

- Some SURBL'd domains were from TLDs (such as some ccTLDs) which don't offer whois service
- Other TLDs offer whois service, but severely limit the maximum number of whois queries which one can make per querying IP per day.
- An additional group of SURBL listings were domains which appeared to have been already suspended or deleted (that list of domains has been provided to the SURBL folks for their review).
- Finally, some domains, because of how they format their whois data, will not be included in this preliminary report (for example, co.uk domains put their registrar data on a separate line from the Registrar: field name, and as a result I ended up missing collecting data from that TLD)

What We Were Left With...

- After considering the previously mentioned factors, we ended up with a data set of right around 600,000 SURBL'd domains and their associated registrars.

- In my opinion, that's still enough domains to be worth a look.

- What do we see as we look at that data?

A Small Number of Registrars Have The Potential To Be Hugely Influential When It Comes to Combating Abuse

- Looking at the domains on the SURBL for which it was possible to identify a responsible registrar (just under 600,000 listed domains):

  -- 4 registrars account for 50% of listed domains

  -- 24 registrars account for 80% of listed domains

  -- 69 registrars (all of the ones with more than a tenth of a percent of all listed domains) cover roughly 92% of listed domains

  See the following table...

REGISTRAR	Freq	%	Cum Freq	%
ENOM INC	108,965	18.34	108,965	18.34
MONIKER ONLINE SERVICES INC	92,765	15.61	201,730	33.95
DIRECT INFORMATION PVT LTD DBA PUBLICDOMAINREGISTRY.COM	50,180	8.44	251,910	42.39
GODADDY.COM INC	49,309	8.30	301,219	**50.69**
TUCOWS INC	17,045	2.87	318,264	53.56
MELBOURNE IT LTD DBA INTERNET NAMES WORLDWIDE	15,369	2.59	333,633	56.14
SPOT DOMAIN LLC DBA DOMAINSITE.COM	13,750	2.31	347,383	58.46
BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD DBA DNS.COM.CN	13,444	2.26	360,827	60.72
COMPUTER SERVICES LANGENBACH GMBH DBA JOKER.COM	12,833	2.16	373,660	62.88
DYNAMIC DOLPHIN INC	11,594	1.95	385,254	64.83
NETWORK SOLUTIONS LLC	11,480	1.93	396,734	66.76

REGISTRAR	Freq	%	Cum Freq	%
XIN NET TECHNOLOGY CORP	10,207	1.72	406,941	68.48
WILD WEST DOMAINS INC	9,529	1.60	416,470	70.08
ESTDOMAINS INC	9,499	1.60	425,969	71.68
THE NAME IT CORPORATION DBA NAMESERVICES.NET	9,435	1.59	435,404	73.27
INTERCOSMOS MEDIA GROUP INC DBA DIRECTNIC.COM	7,155	1.20	442,559	74.47
REGISTER.COM INC	6,827	1.15	449,386	75.62
BIZCN.COM INC	6,357	1.07	455,743	76.69
GKG.NET INC	5,283	0.89	461,026	77.58
DOTSTER INC	4,662	0.78	465,688	78.37
TODAYNIC.COM INC	4,588	0.77	470,276	79.14
DSTR ACQUISITION VII LLC	4,569	0.77	474,845	79.91
ONLINENIC INC	4,450	0.75	479,295	**80.66**
SCHLUND+PARTNER AG	4,413	0.74	483,708	81.40
PARAVA NETWORKS INC DBA REGISTRATEYA.COM NAAME.COM	4,144	0.70	487,852	82.10

REGISTRAR	Freq	%	Cum Freq	%
INNERWISE INC DBA ITSYOURDOMAIN.COM	4,074	0.69	491,926	82.78
ABSYSTEMS INC	3,740	0.63	495,666	83.41
BASIC FUSION INC	3,074	0.52	498,740	83.93
DOMAIN CONTENDER LLC	2,712	0.46	501,452	84.38
NAME.COM LLC	2,241	0.38	503,693	84.76
NAMEKING.COM INC	2,153	0.36	505,846	85.12
IP MIRROR PTE LTD DBA IP MIRROR	2,087	0.35	507,933	85.48
PLANETDOMAIN PTY LTD	1,962	0.33	509,895	85.81
KEY-SYSTEMS GMBH	1,889	0.32	511,784	86.12
MYDOMAIN INC	1,838	0.31	513,622	86.43
NAME.NET LLC	1,588	0.27	515,210	86.70
DOMAINDISCOVER	1,471	0.25	516,681	86.95
COMPANA LLC	1,415	0.24	518,096	87.19
PLANET ONLINE CORP	1,407	0.24	519,503	87.42
ULTRARPM INC DBA METAPREDICT.COM	1,404	0.24	520,907	87.66

REGISTRAR	Freq	%	Cum Freq	%
DOMAINDOORMAN LLC	1,331	0.22	522,238	87.88
RED PILLAR INC	1,308	0.22	523,546	88.10
BELGIUMDOMAINS LLC	1,305	0.22	524,851	88.32
CSC CORPORATE DOMAINS INC	1,157	0.19	526,008	88.52
RUCENTER-REG-RIPN	1,145	0.19	527,153	88.71
OMNIS NETWORK LLC	1,090	0.18	528,243	88.89
HICHINA WEB SOLUTIONS (HK) LTD	1,003	0.17	529,246	89.06
NUCLEAR NAMES INC	1,000	0.17	530,246	89.23
FABULOUS.COM PTY LTD	934	0.16	531,180	89.39
TLDS LLC DBA SRSPLUS	920	0.15	532,100	89.54
CAPITAL NETWORKS PTY LTD	867	0.15	532,967	89.69
CAPITOLDOMAINS LLC	837	0.14	533,804	89.83
MELBOURNE IT LTD	833	0.14	534,637	89.97
1-877NAMEBID.COM LLC	813	0.14	535,450	90.11
DYNADOT LLC	742	0.12	536,192	90.23
ANSWERABLE.COM (I) PVT LTD	727	0.12	536,919	90.35

REGISTRAR	Freq	%	Cum Freq	%
NICREG LLC	725	0.12	537,644	90.48
PSI-USA INC DBA DOMAIN ROBOT	682	0.11	538,326	90.59
NETFIRMS INC	681	0.11	539,007	90.70
ENOMAU INC	679	0.11	539,686	90.82
DOMAINPEOPLE INC	662	0.11	540,348	90.93
ENOMX INC	656	0.11	541,004	91.04
VISESH INFOTECNICS LTD	655	0.11	541,659	91.15
ENOMMX INC	640	0.11	542,299	91.26
MONIKER ONLINE SERVICES LLC	639	0.11	542,938	91.37
WEBAIR INTERNET DEVELOP.	635	0.11	543,573	91.47
FASTDOMAIN INC	630	0.11	544,203	91.58
ABACUS AMERICA INC DBA NAMES4EVER	629	0.11	544,832	**91.68**

[all remaining registrars individually represented 1/10th of 1% of the total or less]

Caution: Glancing at That Raw Table May Give You A Misleading Impression

- Domain names are not equally distributed across all accredited registrars. There are some accredited registrars who have a huge share of the market, while others are quite a bit smaller. We therefore should adjust that listing according to relative registrar market share.
- Some registrars may also have multiple independent accredited registrar units. For example, in addition to ENOM INC, the top registrar in our dataset, there are also additional potentially related registrar entities such as ENOMAU INC, ENOMX INC, ENOMMX INC, ENOMTEN INC, ENOMTOO INC, ENOM CORPORATE INC, ENOM1 INC, ENOM3 INC, ENOMNZ INC, ENOMEU INC, ENOM4 INC, ENOM5 INC, ENOM GMP SERVICES INC, ENOM WORLD INC, etc., etc. Potentially related registrars have NOT be aggregated.

More Cautions

- We also need to recognize that some registrars may have many domains for which we could not get registrar whois data, so for now let's just focus on .com and .net domains for comparability purposes.
- Dot com and dot net account for > 95% of the "registrar-attributable" SURBL domains in our dataset anyway...

TLD	Frequency	Percent	Cumulative Frequency	Cumulative Percent
com	498642	82.04	498642	82.04
net	82664	13.60	581306	95.64

- Focusing on dot com and dot net also makes it easy to get registrar market share statistics from Verisign's monthly registry reports (see www.icann.org/tlds/monthly-reports/). The most recent registry data available is from October 2007.

What's In The Table On The Next Slide?

- For registrars with at least 0.2% of the .com+.net SURBL dataset, the spreadsheet on the next slide shows some initial results, namely:
  - Registrar Name
  - Number of .com+.net SURBL'd domains associated with that registrar
  - Total .com domains for that registrar as of October 2007
  - Total .net domains for that registrar as of October 2007
  - Sum of those October 2007 .com + .net domain counts
  - Ratio of (.com and .net SURBL listed domains associated with this registrar)/(all .com+.net domains associated with this registrar)*100
  - Ratio of (the % of all SURBL domains for this registrar)/(the % of all .com+.net domains for this registrar); entries in the table are sorted by this column.

    Note: one registrar (MYDOMAIN INC) did not appear in the Verisign Monthly report; the whois server associated with at least a couple of MYDOMAIN INC domains showed a whois server of whois.namesdirect.com but for now I've simply omitted that registrar

Registrar	SURBL Domains	COM Domains	NET Domains	COM+NET Domains	(SURBL Domains/ Total Domains) *100	(% of all SURBL Domains)/ (% of all COM+NET Domains)
RED PILLAR INC	1308	1403	149	1552	84.278	116.014
PLANET ONLINE CORP	1407	1883	117	2000	70.350	96.841
DYNAMIC DOLPHIN INC	11594	36050	1051	37101	31.250	43.017
ABSYSTEMS INC	3740	0	14905	14905	25.092	34.541
IP MIRROR PTE LTD DBA IP MIRROR	2087	7278	1571	8849	23.585	32.465
PARAVA NETWORKS INC DBA REGISTRATEYA.COM NAAME.COM	4144	40511	7583	48094	8.616	11.861
TODAYNIC.COM INC	4573	44998	9919	54917	8.327	11.463
ESTDOMAINS INC	8936	85564	22935	108499	8.236	11.337
THE NAME IT CORPORATION DBA NAMESERVICES.NET	9435	131617	17429	149046	6.330	8.714
DOMAIN CONTENDER LLC	2712	53045	6829	59874	4.530	6.235
MONIKER ONLINE SERVICES INC	92741	1956780	204067	2160847	4.292	5.908
DIRECT INFORMATION PVT LTD DBA PUBLICDOMAINREGISTRY.COM	49199	1064697	159588	1224285	4.019	5.532
BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD DBA DNS.COM.CN	13444	306100	45961	352061	3.819	5.257
SPOT DOMAIN LLC DBA DOMAINSITE.COM	13744	285248	77780	363028	3.786	5.212
GKG.NET INC	5270	134210	27469	161679	3.260	4.487
COMPUTER SERVICES LANGENBACH GMBH DBA JOKER.COM	12833	420766	96638	517404	2.480	3.414
BIZCN.COM INC	6355	223728	35493	259221	2.452	3.375
ENOM INC	107689	6179440	883538	7062978	1.525	2.099
XIN NET TECHNOLOGY CORPORATION	10192	697360	102374	799734	1.274	1.754
NAME.COM LLC	2240	157168	19488	176656	1.268	1.745
PLANETDOMAIN PTY LTD	1951	136426	19295	155721	1.253	1.725
NAME.NET LLC	1588	131267	6764	138031	1.150	1.584
ULTRARPM INC DBA METAPREDICT.COM	1404	180306	9141	189447	0.741	1.020
INNERWISE INC DBA ITSYOURDOMAIN.COM	4025	574666	60315	634981	0.634	0.873
INTERCOSMOS MEDIA GROUP INC DBA DIRECTNIC.COM	7009	994670	131489	1126159	0.622	0.857
DSTR ACQUISITION VII LLC	4569	745611	99949	845560	0.540	0.744
CSC CORPORATE DOMAINS INC	1157	193505	42874	236379	0.489	0.674
DOTSTER INC	4655	895368	123440	1018808	0.457	0.629
BASIC FUSION INC	3072	681211	29506	710717	0.432	0.595
WILD WEST DOMAINS INC	9206	1956922	248300	2205222	0.417	0.575
ONLINENIC INC	4437	931566	153062	1084628	0.409	0.563
MELBOURNE IT LTD DBA INTERNET NAMES WORLDWIDE	15298	3825219	510778	4335997	0.353	0.486
TUCOWS INC	16734	4552986	755560	5308546	0.315	0.434
REGISTER.COM INC	6789	1992806	279522	2272328	0.299	0.411
GODADDY.COM INC	47984	15295392	2181820	17477212	0.275	0.378
NAMEKING.COM INC	2153	788110	46064	834174	0.258	0.355
COMPANA LLC	1415	638764	22818	661582	0.214	0.294
BELGIUMDOMAINS LLC	1304	574568	40366	614934	0.212	0.292
DOMAINDOORMAN LLC	1328	590618	40202	630820	0.211	0.290
NETWORK SOLUTIONS LLC	11407	5046746	781814	5828560	0.196	0.269
DOMAINDISCOVER	1470	624960	140631	765591	0.192	0.264
KEY-SYSTEMS GMBH	1786	776138	245799	1021937	0.175	0.241
SCHLUND+PARTNER AG	4411	2713201	471701	3184902	0.138	0.191

How Do I Read The Values In That Chart?

- Looking at the two ratios shown for each registrar:

  -- The first of those two ratios is essentially the percent of .com and .net domains (for that registrar) which are listed on the SURBL list. Lower values are better.

  -- The second of those two ratios is the percent of SURBL listings associated with a given registrar divided by the market share of that ratio. If a registrar has just "its proportionate share" of SURBL listings, it would have a ratio of 1.0. If the registrar appears to have more than "its proportionate share" of SURBL listings, it will have a ratio that's **greater than** 1, and conversely, if it appears to have less than its proportionate share of SURBL listings, it will have a ratio of **less than 1.** (Again, lower values are better.)

Interpretive Cautions/Disclaimers

- Just like earlier tables, the table on slide 55 also needs to be interpreted carefully. For example, because the most recent com/net domain market share data available was from October 2007, if a registrar listed in that table experienced growth between October 2007 and the end of January when I obtained SURBL data for this study, they might show higher ratios than they should; conversely, if registrar share dropped during the period while SURBL listings remained unchanged, they might show undeservedly low ratios.
- Those ratios are also just a "snapshot" in time; any registrar can develop a temporary infestation of abusers, or have a temporary clean streak. :-) The correct thing to watch is what happens to SURBL listing counts over time. Do the counts associated with providers go up (as infestations get worse), or do they go down as problematic domains get terminated?

Interpretive Cautions/Disclaimers (2)

- While these statistics are derived from dot com and dot net domains listed in the SURBL data, replacing the SURBL data with a different unwanted domain data source, or inclusion of other TLDs (such as dot org), just to name two factors among many, might dramatically change individual registrar rankings for the better (or for the worse).
- While I've attempted to exercise all due care, I may have made some yet-to-be-identified error so I would urge you to carefully re-evaluate this data yourself before drawing any conclusions from it or taking any action based upon it.
- The preceding analysis is meant to illustrate **one** possible analysis which one might do, and is intended to stimulate further discussion. This data should NOT be used for operational purposes, and comes with no warranty.
  If you use this data for anything, you do so at your own risk.

Conclusion/Summary

- Spammers need a variety of resources in order to be able to send spam. If denied access to those resources, their ability to continue to be able to spam will be diminished.
- Domain names are one such resource, which means that registrars can potentially play a critical role in fighting spam.
- A relatively small number of registrars control a significant fraction of the addresses listed on the SURBL. Other registrars may have a high concentration of domains associated with abuse, and may (or may not) be willing to take action to deal with those problematic domains.
- Proxy/private registration services may exacerbate the problems associated with abused/abusive domains.
- The status of any registrar at any single point in time is not as important as what happens over time -- are the number abused/abusive domains increasing or decreasing?

Are There Any Questions?

- Thanks for the chance to talk today, and thanks to those who contributed suggestions/comments on a draft version of this talk!