Ms. Suzanne R. Sene
Office of International Affairs
National Telecommunications and Information Administration
1401 Constitution Avenue, N.W.
Room 4701
Washington, DC 20230

Response to Department Of Commerce, National Telecommunications and Information Administration Midterm Review of the Joint Project Agreement Request for Comments by Project KnujOn.

Reason for This Report

This report is in direct response to Request for Comment item number 5 on the *Federal Register Notice:* **The Continued Transition of the Technical Coordination and Management of the Internet's Domain Name and Addressing System: Midterm Review of the Join Project Agreement,** Docket No. 071023616-7617-01. The request for comment is quoted as:

> "5. In the JPA, ICANN agreed to undertake the following with respect to TLD management: ICANN shall maintain and build on processes to ensure that competition, consumer interests, and Internet DNS stability and security issues are identified and considered in TLD management decisions, including the consideration and implementation of new TLDs and the introduction of IDNs. ICANN will continue to develop its policy development processes, and will further develop processes for taking into account recommendations from ICANN's advisory committees and supporting organizations and other relevant expert advisory panels and organizations. ICANN shall continue to enforce existing policy relating to WHOIS, such existing policy requires that ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing and administrative contact information. ICANN shall continue its efforts to achieve stable agreements with country-code top-level domain (ccTLD) operators." What progress do you believe ICANN has achieved with regard to this Responsibility since October 1, 2006? If you believe that progress has been made, please explain how and why? Could more be done by ICANN in this area?"

Project KnujOn has had significant experience with ICANN's compliance structure, specifically in terms of the InterNic Whois Data Problem Reporting System (WDPR). Our evaluation of ICANN's compliance system is that current processing and staffing levels are not designed to meet the size and scope of today's Internet. Various illicit enterprises have subverted the current domain name system by taking advantage of poor accounting standards and a lack of oversight on the part of the registrars. For the reasons cited here we do not feel it is an appropriate time to end the JPA. Before any institutional changes can be made to ICANN, the mandated procedures need to be strengthened.

In a June 11, 2007 meeting at ICANN we expressed our concern that the organization was unable to process the volume of WDPR reports KnujOn was anticipating. We made several suggestions that are detailed in the last section. We have offered our assistance to ICANN in resolving the issues detailed in this report and hope that an improved compliance structure will secure industry, consumer and government trust. Since this meeting we have been encouraged by the progress made in this area, but more needs to be done. It is our belief that the problems sited by many ICANN critics are actually endemic to the registrar community and that improved registrar oversight will fix what may be broken.

Brief of KnujOn and Results

KnujOn is transforming the "unsolvable" spam problem into a situation that can be understood, managed, minimized and defeated. Spam filtering and blocking isn't working, in fact spam has increased in the last two years, flooding the global network. At KnujOn (http://www,knujon.com) we are providing consumers with a no-nonsense way to report junk mail. In return they receive feedback and action they are not getting from the Internet community. Through persistent policy enforcement, KnujOn is reducing the value of junk email by eliminating the transaction platforms (websites) and increasing the operational costs for the illicit networks.

We have been soliciting junk email from the public and running it through a process called the Policy Enforcement Engine (Patent Pending). We look at each piece of email and try to determine what the best course of action is. We actually go after the website owners and shut them down through legal, procedural methods. So far our work has led to the shutdown of tens of thousands of sites. We have individual users and small networks feeding us their junk email, many automatically. There are several major areas where our work is having an impact and continues to help:

- Counterfeit or unlicensed prescription drug sales on the Internet
- Traffic in knockoff, diverted, pirated, and stolen merchandise
- Predatory lending in the sub-prime and refinance mortgage industry
- Vacation scams
- Identity theft

In addition to developing an array of technical tools, we work to generate big picture thinking by exploring the complex issues driving spam, illustrating the impact on individual victims as well as the burden on the economy, and by using spam to create a “map” of transnational crime. At KnujOn we challenge beliefs, for example the current assumption that there is too much junk email to process effectively. We empower consumers by accepting junk email submissions from thousands of official and non-official clients as the starting point for our procedures. And we use the current policy structures to address the problem in order to reveal breakpoints and bottlenecks in Internet compliance.

Our perspective in the report is concerned with criminality on the Internet, its effects on consumers and business, and the role ICANN plays in related issues.

KnujOn is:

Garth Bruen, CTO
http://www.knujon.com
gbruen@knujon.com

Dr. Robert Bruen, CEO
http://www.coldrain.net
bruen@coldrain.net

Detailed white paper available at: http://www.knujon.com/KnujonWP.pdf

Limitations of ICANN WDPR System

Our experience with the ICANN Internic Whois Data Problem Report system has revealed limitations that require immediate address. To summarize, these limitations fall into 2 major categories: (1) the daily submission/processing limits of the WDPR system are fare bellow the volume of reports submitted by Knujon, and (2) the volume of these reports is placing increasing strain on ICANN's compliance system causing follow up delays.

1. Knujon accepts about 20,000 items from the public for processing each day. Some are individual messages and some are bulk compressed files containing thousands of emails. From these items our process yields on average 14,000 unique URLs. Between 1 and 2 thousand of these are immediately identified as having invalid Whois records. Additional short-term research usually finds 2 to 3 thousand more are in violation by the end of a daily processing run. KnujOn attempts to report all of these violations through the ICANN WDPR system but we estimate that ICANN can process fewer than 3000 in a 24 hour period. At the end of a typical week KnujOn records nearly 10,000 additional or repeat violations not covered in the daily reports. It can take several days to process all of these items through the ICANN WDPR.

2. The WDPR system is following up at slower rates. When Project KnujOn first started the WDPR follow-ups were issued after 15-30 days of initial submission. This time frame gradually crept to 45 days. Most recently a WDPR KnujOn submitted on November 5, 2007 was returned by ICANN on January 20, 2008 which is a 76-day turn around. Obviously additional resources are required to process the growing number of reports.

The WDPR system appears overloaded at the moment. This is of serious concern when contrasted with the speed and ability of Internet abusers to register and populate illicit websites. In an era when criminal enterprises may register new websites with fake information, complete illegal transactions, and disappear within 48 hours the 76-day follow-up only serves to help the criminals vanish. Adding resources to this critical ICANN process will help significantly.

Examples of Possible False Reporting to ICANN by Registrars

KnujOn has found evidence that some registrars may be reporting to ICANN that a site has been terminated when in fact it has not. Under current guidelines a registrar has 15 days to reply to a WDPR report and indicate if the erroneous Whois record has been corrected or if the site has been terminated.

Recently KnujOn has discovered the practice of providing different Whois query results to the ICANN WDPR. We have observed what appear to be two different sets of data released by BIZCN regarding Whois records. For example a recent WDPR follow up on ekvosoft.com contained this response to the standard Whois query:

```
              WHOIS DATA AS OF 2007/09/03 01:15:00

REGISTRAR WHOIS:

No match for ekvosoft.com

REGISTRY WHOIS:

Whois Server Version 1.3

 Domain Name: EKVOSOFT.COM
 Registrar: BIZCN.COM, INC.
 Whois Server: whois.bizcn.com
 Referral URL: http://www.bizcn.com
 Name Server: NS1.SOBAKA-SOFT.COM
 Name Server: NS2.SOBAKA-SOFT.COM
 Status: clientTransferProhibited
 Status: clientDeleteProhibited
 Updated Date: 26-apr-2007
 Creation Date: 26-apr-2007
 Expiration Date: 26-apr-2008

Registrar: BIZCN.COM, INC.
Whois Server: whois.bizcn.com
```

However, a standard Whois query at BIZCN.COM revealed the full record and the domain itself was and is active on the Internet. There could be a technical reason why the query returned to the WDPR would be different from the standard Whois query, but it seems unusual. It is important to note that BIZCN was used as an example here and this practice has been observed elsewhere.

Examples of Registrars Limiting Record Access to ICANN

Knujon has noted the increasing practice of restricting ICANN's access to Whois records through the WDPR system. With more frequency WDPR follow up reports from Registrars arrive with no Whois information. The section of the standard follow-up that usually contains the Whois record in question instead contains one of the following messages:

> **"Too many connection!"**
>
> **"You have reached your daily query limit"**
>
> **"We have restricted access because of excessive queries"**
>
> **"Whois server unavailable"**
>
> **"Query limit exceeded"**

While we understand that registrars have reasons for restricting access to their WhoIs queries, we assume that ICANN would be exempt from these limits. This issue has been reported to ICANN.

We are aware that ICANN conducted audits of the response rates of registrar port 43 Whois services by testing 5 domains at each registrar. While this test did show that a significant number of registrars did not have an active public Whois service functioning (105 of 850 or 12% of all registrars), we do not believe this test goes far enough. As explained above some registrars seem to be selective in the type of queries or number of queries allowed. In order to better understand this problem hundreds of domains would need to be tested at each registrar and on a regular basis.

Lack of Pre-registration Verification

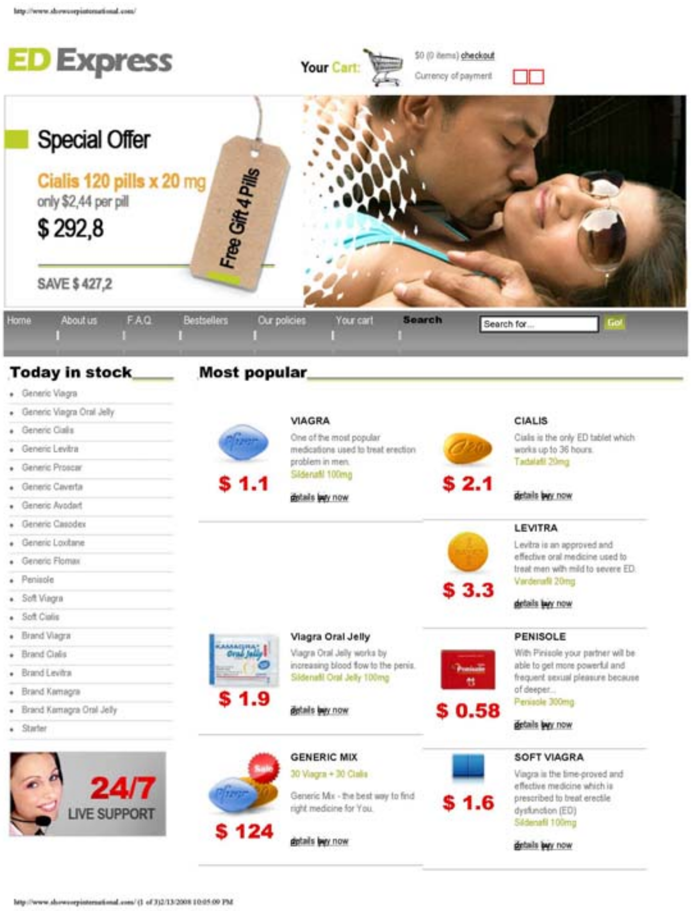
There is apparently little or no verification of data submitted by registrants at certain registrars. Knujon has found tens of thousands of blatantly falsified Whois records, most of which contain false information but some contain *impossible* information. For example, the following administrator or registrant email address were provided for some sites:

aa@aa.aa, colo@no.ana, dan@masih.lah, espy8yolk@yahoo.comm, ificould@tell.you, jika@hara.jika, just@one.lef, private@nospam.xxx, registres@intergrid.cat, shark@tv.asd, sharp@sur.ice, some@one.coe, welcome@was.boy, video@pop.up, work@tis.up

Since none of the above contain real Top Level Domain extensions, they are precluded from being real email addresses. None of the sites registered should have been allowed to complete their applications with this obviously false data. Most of these issues could be resolved by standard ASP/JavaScript/PHP form validation.

We believe these issues could be prevented by periodic audits of registrars and a more comprehensive vetting process for registrar certification.

The following fake pharmacy was registered with "colo@no.ana":



http://www.showcorpinternational.com/

Special Offer

Cialis 120 pills x 20 mg
only $2,44 per pill
$ 292,8

SAVE $ 427,2

Today in stock

- Generic Viagra
- Generic Viagra Oral Jelly
- Generic Cialis
- Generic Levitra
- Generic Proscar
- Generic Caverta
- Generic Avodart
- Generic Casodex
- Generic Loxitane
- Generic Flomax
- Penisole
- Soft Viagra
- Soft Cialis
- Brand Viagra
- Brand Cialis
- Brand Levitra
- Brand Kamagra
- Brand Kamagra Oral Jelly
- Starter

Most popular

VIAGRA
One of the most popular medications used to treat erection problem in men.
Sildenafil 100mg
$ 1.1
details buy now

CIALIS
Cialis is the only ED tablet which works up to 36 hours.
Tadalafil 20mg
$ 2.1
details buy now

LEVITRA
Levitra is an approved and effective oral medicine used to treat men with mild to severe ED.
Vardenafil 20mg
$ 3.3
details buy now

Viagra Oral Jelly
Viagra Oral Jelly works by increasing blood flow to the penis.
Sildenafil Oral Jelly 100mg
$ 1.9
details buy now

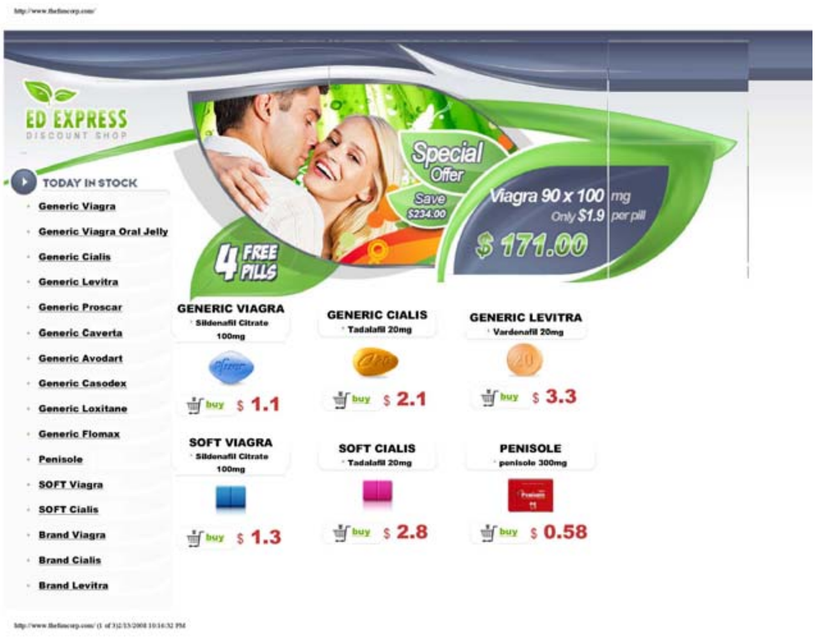
PENISOLE
With Pinisole your partner will be able to get more powerful and frequent sexual pleasure because of deeper...
Penisole 300mg
$ 0.58
details buy now

GENERIC MIX
30 Viagra + 30 Cialis
Generic Mix - the best way to find right medicine for You.
$ 124
details buy now

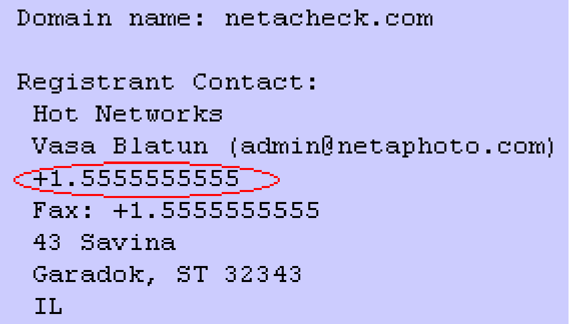
SOFT VIAGRA
Viagra is the time-proved and effective medicine which is prescribed to treat erectile dysfunction (ED)
Sildenafil 100mg
$ 1.6
details buy now

http://www.showcorpinternational.com/ (1 of 3)2/13/2008 10:05:00 PM

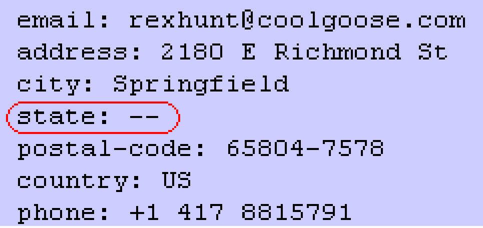
This one was registered with “jika@hara.jika” :



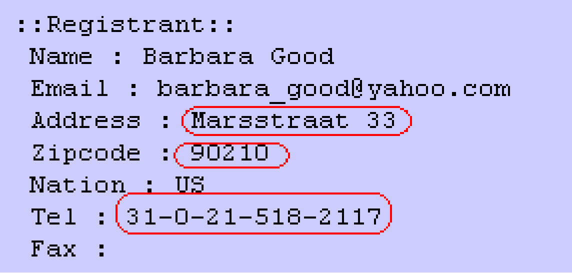
The following are real examples that could have been prevented by simple application form validation on the registrar’s website, beyond any actual verification of the data itself.



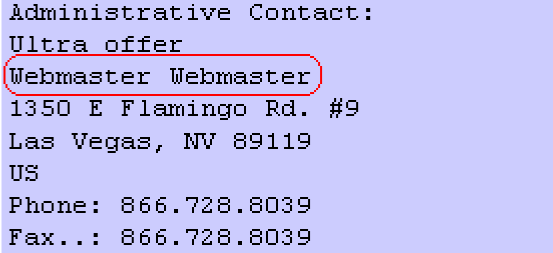
```
Domain name: netacheck.com

Registrant Contact:
 Hot Networks
 Vasa Blatun (admin@netaphoto.com)
 +1.5555555555
 Fax: +1.5555555555
 43 Savina
 Garadok, ST 32343
 IL
```



```
email: rexhunt@coolgoose.com
address: 2180 E Richmond St
city: Springfield
state: --
postal-code: 65804-7578
country: US
phone: +1 417 8815791
```



```
::Registrant::
 Name : Barbara Good
 Email : barbara_good@yahoo.com
 Address : Marsstraat 33
 Zipcode : 90210
 Nation : US
 Tel : 31-0-21-518-2117
 Fax :
```



```
Administrative Contact:
Ultra offer
Webmaster Webmaster
1350 E Flamingo Rd. #9
Las Vegas, NV 89119
US
Phone: 866.728.8039
Fax..: 866.728.8039
```

So-Called Privacy Records

While there is great and valid concern for personal privacy in today’s digital society, so-called privacy and proxy services have become a haven for various types of illicit activity. Personal individual website registrants and domain owners who may be targets of violence for political reasons have much to fear from public disclosure. However, privacy protections should not be extended to business websites selling regulated drugs, licensed software, trademarked merchandise, or sites engaged in financial transactions (mortgages, loans, banking, credit cards). While privacy registration services claim to be protecting their customers against identity theft, spam and harassment, our research has shown that the bulk of business using privacy services are engaged in spamming and selling illicit products.

ICANN exists to serve as an Internet authority and dispute mediator but services like Privacyprotect.org have assumed a certain amount of authority by adding a layer of anonymity. While Privacayprotect.org and others have electronic forms on their sites that allow anyone to “contact the real owner” of websites using the privacy service this in effect bypasses the purpose of the Whois structure and invalidates the existence of ICANN. This type of privacy service is a misuse of the Whois system and does not actually meet the basic requirements of public registration records.

Proxy vs. Privacy

In theory a proxy service is supposed to accept and handle communications from the public on behalf of a website owner. Email, phone calls and post mail are handled by the service and passed to the true registrant. A privacy service does none of these things. In the case of Privacyprotect.org all registration records have the email address of “contact@privacyprotect.org”. While this is an “active” email address it does not contact the registrant. Abuse complaints never reach the actual owner. All Privacyprotect.org registrations contain the following street address:

```
P.O. Box 97
All Postal Mails Rejected visit Privacyprotect.org
Moergestel
null 5066 ZH
```

If, as this Whois record claims: “All Postal Mails Rejected”, then this is not a valid registration by its own admission.

An additional contradiction arises because the Whois record clearly states:

```
Registrant:  PrivacyProtect.org
```

But Privacyprotect.org claims that: “We are NOT the actual owner of the domain name.” Given these facts we must assume that either: Privacyprotect.org is the registrant, OR Privacyprotect.org has falsified the Whois record, OR Privacyprotect.org has been given some sort of special authority by ICANN not afforded to any other domain registrant. Either way this highly questionable arrangement that presents serious problems for the Internet consumer.

While Privacyprotect.org claims that “Privacy Protection Service is not meant to be used for spam, abuse or any illegal/unlawful activities.” We have to wonder at the sincerity of this when they provide privacy services for sites like: your047pharmacy.com, usadrugs0nline235.com, us-pharmacy20436.com, us490pharmacy.com, uk325pharmacy.com, 105-cheaponlinepills.com, 40-elitebestpills.com. Sites like these should never have been allowed to use the service if Privacyprotect.org was serious about preventing misuse. Privacyprotect.org does have an interface for reporting abuse but there is little or no transparency for this process.

Coincidentally, the company Privacyprotect.org does not in fact provide any information about who owns it or where they are located. Considering that one completely anonymous company is providing anonymity for a host of illicit services, it is clear that the system has failed to protect the consumer in this case.

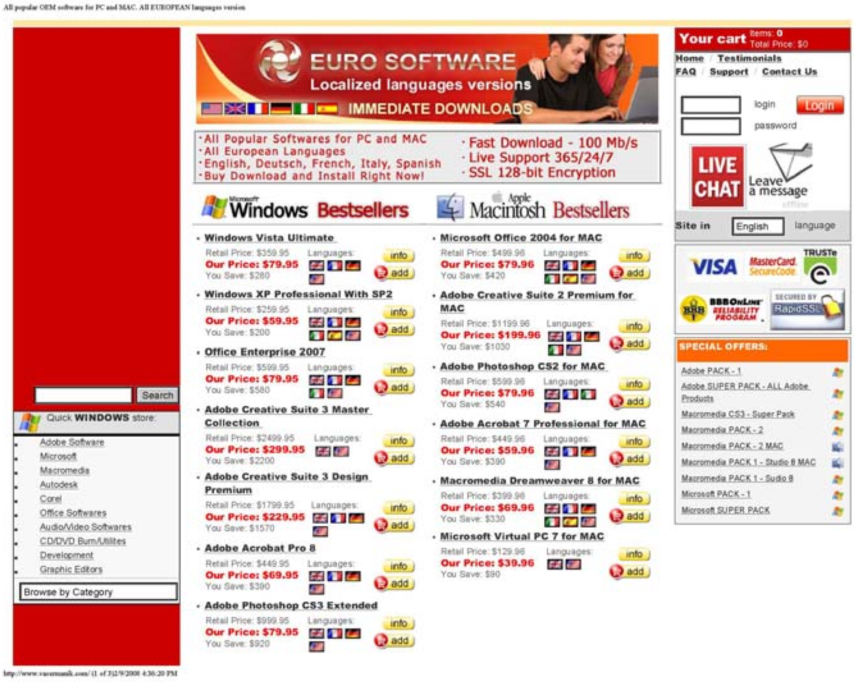
Another privacy service called FreePrivateRegistration.com responds to every email with the message:

> This domain registrant has opted to not receive unsolicited email correspondence. If you would like to contact this domain registrant or domain administrative contact, please use postal mail sent to the mailing address listed on the Whois record of this domain registration. Please ensure that you include reference to the domain name to which the correspondence is about.

Once again, providing an email address on registrations that does not actually reach the registrant is not a legitimate response and bypasses the real purpose of the Whois system. This situation also excludes millions of Internet users around the world who cannot afford to send international postal mail that will likely never be read or handled properly.

Privacy protection services have in essence set themselves up a separate authority from ICANN and made a mockery of the Whois system.

The following are samples from two sites using privacy protection, one is a typical software piracy site and the second sells pharmacuiticals and pornography, both were advertised with Unsolicited Commercial Email ("spam"):



All popular OEM software for PC and MAC. All EUROPEAN languages version

EURO SOFTWARE
Localized languages versions
IMMEDIATE DOWNLOADS

- All Popular Softwares for PC and MAC
- All European Languages
- English, Deutsch, French, Italy, Spanish
- Buy Download and Install Right Now!

- Fast Download - 100 Mb/s
- Live Support 365/24/7
- SSL 128-bit Encryption

Microsoft Windows Bestsellers

- Windows Vista Ultimate
  Retail Price: $359.95 Languages:
  Our Price: $79.95
  You Save: $280
- Windows XP Professional With SP2
  Retail Price: $259.95 Languages:
  Our Price: $59.95
  You Save: $200
- Office Enterprise 2007
  Retail Price: $599.95 Languages:
  Our Price: $79.95
  You Save: $580
- Adobe Creative Suite 3 Master Collection
  Retail Price: $2499.95 Languages:
  Our Price: $299.95
  You Save: $2200
- Adobe Creative Suite 3 Design Premium
  Retail Price: $1799.95 Languages:
  Our Price: $229.95
  You Save: $1570
- Adobe Acrobat Pro 8
  Retail Price: $449.95 Languages:
  Our Price: $69.95
  You Save: $390
- Adobe Photoshop CS3 Extended
  Retail Price: $999.95 Languages:
  Our Price: $79.95
  You Save: $920

Apple Macintosh Bestsellers

- Microsoft Office 2004 for MAC
  Retail Price: $499.96 Languages:
  Our Price: $79.96
  You Save: $420
- Adobe Creative Suite 2 Premium for MAC
  Retail Price: $1199.96 Languages:
  Our Price: $199.96
  You Save: $1030
- Adobe Photoshop CS2 for MAC
  Retail Price: $599.96 Languages:
  Our Price: $79.96
  You Save: $540
- Adobe Acrobat 7 Professional for MAC
  Retail Price: $449.96 Languages:
  Our Price: $59.96
  You Save: $390
- Macromedia Dreamweaver 8 for MAC
  Retail Price: $399.96 Languages:
  Our Price: $69.96
  You Save: $330
- Microsoft Virtual PC 7 for MAC
  Retail Price: $129.96 Languages:
  Our Price: $39.96
  You Save: $90

Quick WINDOWS store:

- Adobe Software
- Microsoft
- Macromedia
- Autodesk
- Corel
- Office Softwares
- Audio/Video Softwares
- CD/DVD Burn/Utilites
- Development
- Graphic Editors

Browse by Category

Your cart Items: 0 Total Price: $0

Home / Testimonials
FAQ / Support / Contact Us

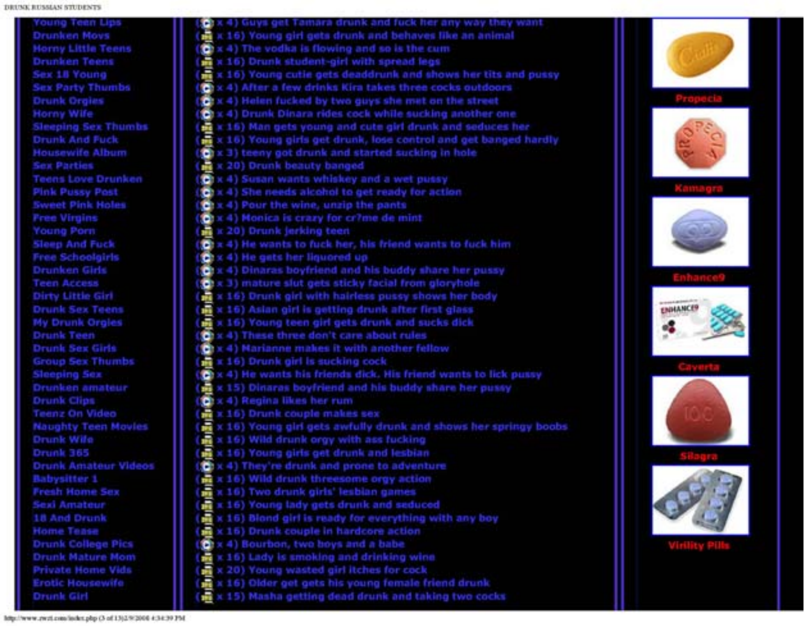
login
password

Site in English language

SPECIAL OFFERS:

- Adobe PACK - 1
- Adobe SUPER PACK - ALL Adobe Products
- Macromedia CS3 - Super Pack
- Macromedia PACK - 2
- Macromedia PACK - 2 MAC
- Macromedia PACK 1 - Studio 8 MAC
- Macromedia PACK 1 - Sudio 8
- Microsoft PACK - 1
- Microsoft SUPER PACK

http://www.[illegible].com/ (1 of 3)2/9/2008 4:36:20 PM



DRUNK RUSSIAN STUDENTS

Young Teen Lips
Drunken Movs
Horny Little Teens
Drunken Teens
Sex 18 Young
Sex Party Thumbs
Drunk Orgies
Horny Wife
Sleeping Sex Thumbs
Drunk And Fuck
Housewife Album
Sex Parties
Teens Love Drunken
Pink Pussy Post
Sweet Pink Holes
Free Virgins
Young Porn
Sleep And Fuck
Free Schoolgirls
Drunken Girls
Teen Access
Dirty Little Girl
Drunk Sex Teens
My Drunk Orgies
Drunk Teen
Drunk Sex Girls
Group Sex Thumbs
Sleeping Sex
Drunken amateur
Drunk Clips
Teenz On Video
Naughty Teen Movies
Drunk Wife
Drunk 365
Drunk Amateur Videos
Babysitter 1
Fresh Home Sex
Sexi Amateur
18 And Drunk
Home Tease
Drunk College Pics
Drunk Mature Mom
Private Home Vids
Erotic Housewife
Drunk Girl

(x 4) Guys get Tamara drunk and fuck her any way they want
(x 16) Young girl gets drunk and behaves like an animal
(x 4) The vodka is flowing and so is the cum
(x 16) Drunk student-girl with spread legs
(x 16) Young cutie gets deaddrunk and shows her tits and pussy
(x 4) After a few drinks Kira takes three cocks outdoors
(x 4) Helen fucked by two guys she met on the street
(x 4) Drunk Dinara rides cock while sucking another one
(x 16) Man gets young and cute girl drunk and seduces her
(x 16) Young girls get drunk, lose control and get banged hardly
(x 3) teeny got drunk and started sucking in hole
(x 20) Drunk beauty banged
(x 4) Susan wants whiskey and a wet pussy
(x 4) She needs alcohol to get ready for action
(x 4) Pour the wine, unzip the pants
(x 4) Monica is crazy for cr?me de mint
(x 20) Drunk jerking teen
(x 4) He wants to fuck her, his friend wants to fuck him
(x 4) He gets her liquored up
(x 4) Dinaras boyfriend and his buddy share her pussy
(x 3) mature slut gets sticky facial from gloryhole
(x 16) Drunk girl with hairless pussy shows her body
(x 16) Asian girl is getting drunk after first glass
(x 16) Young teen girl gets drunk and sucks dick
(x 4) These three don't care about rules
(x 4) Marianne makes it with another fellow
(x 16) Drunk girl is sucking cock
(x 4) He wants his friends dick. His friend wants to lick pussy
(x 15) Dinaras boyfriend and his buddy share her pussy
(x 4) Regina likes her rum
(x 16) Drunk couple makes sex
(x 16) Young girl gets awfully drunk and shows her springy boobs
(x 16) Wild drunk orgy with ass fucking
(x 16) Young girls get drunk and lesbian
(x 4) They're drunk and prone to adventure
(x 16) Wild drunk threesome orgy action
(x 16) Two drunk girls' lesbian games
(x 16) Young lady gets drunk and seduced
(x 16) Blond girl is ready for everything with any boy
(x 16) Drunk couple in hardcore action
(x 4) Bourbon, two boys and a babe
(x 16) Lady is smoking and drinking wine
(x 20) Young wasted girl itches for cock
(x 16) Older get gets his young female friend drunk
(x 15) Masha getting dead drunk and taking two cocks

http://www.zwzt.com/index.php (3 of 13)2/9/2008 4:34:39 PM

Some Proxy Services are not private

While Proxy services offer to protect their customers at a price, they are not offering any real privacy. For example, while Privacyprotect.org provides immediate anonymity on Whois records, it is fairly trivial to discover where the site is hosted and registered. In some other cases, as with GKG.NET proxy services, if an email is sent to a proxy address and the final destination mailbox is full or unavailable, the system rejection message will contain the real address.

The entire practice of private registrations is questionable. There seem to be few standards in this area and only a minority are benefiting from it. Our recommendation for addressing this is in the last section.

Connection Between Inaccurate WI, Illicit Traffic and UCE

At the odds are in the favor of the sophisticated Internet criminal. The small number of arrests and lawsuits represent a tiny fraction of a very large and complex criminal underground. The average Internet consumer or email user has little or no recourse against the mass of fraud and abuse because the compliance system, such as it is, has failed the public. The technical knowledge and wherewithal required for the individual follow through with abuse complaints is unattainable to most. Internet service providers are generally unconcerned with the minority who take the time to report abuse. Police agencies are restricted by jurisdiction and “real” crime priorities. The software industry has provided few real tools to the public or government. While ICANN does not have the authority to monitor website content or pursue criminal activity the Internet, they do have the mandated responsibility to police the registrars. The lack of enforcement up to this point has created an enormous loophole that allows illicit product traffickers to conduct business with impunity.

There are clear links between inaccurate registrations, unsolicited email, and illicit product transactions. The lack of screening and monitoring of registrars has created a wide loophole for illicit networks to exploit. This loophole needs to be closed soon.

Statistics

Of the 247,615 unique domains (not sub-domains) review by KnujOn in 2007 that were advertised through unsolicited commercial email 113,130 (46%)have been found to have inaccurate or blatantly falsified Whois records. The rest are still being investigated. Approximately 80% of all these sites fall into one of four categories: 1. Unlicensed Pharmacies; 2. Media Piracy (software, movies, music); 3. Unlicensed Lending Organizations (Mortgages, Loans), or 4. On-line stores offering luxury or general name-brand consumer goods that are unlikely sanctioned by the true manufacturers (“knockoffs”). It is impossible to tell if all of these sites offer a real product of service. Some have been know to merely collect credit card, banking or other personal information for the purposes of fraud.

The remaining 20% of the sites advertised are pornographic, vacation offers (many have been found to be unlicensed travel agencies with multiple BBB and FTC complaints), “dating” services, and many other uncategorized offers.

These illicit networks are often made up of several thousand domain names which are used in rotation. As one set of sites is shutdown, a second array of sites is ready to be released. We have observed that some registrars will temporarily comply with ICANN by suspending sites for a few days only to reinstate them without correcting the registration records. We have also observed illicit networks terminated at one registrar reappearing at another registrar with the same invalid information (a “bulk” transfer).

Site Types and WI abuse

Counterfeit products

Brand-name companies already face an uphill battle in combating counterfeit, substandard products. The lack of Whois scrutiny has added an additional layer of anonymity for knockoff distributors. Counterfeits are usually produced by organized criminal groups. Purchases of these goods can fund other criminal activities down the line like narcotics, human smuggling, weapons sales and terrorism. Fake products are often manufactured in "sweatshop" or slavery-like conditions, including child labor and possibly prison labor. Some fake products have been known to explode or poison users. Global illicit traffic is now a $600 Billion industry, representing 7-9% of all global trade, a considerable increase from previous decades. This increase is being partially driven by the growth in Internet commerce and electronic fraud.

Prescription Drugs

Registration fraud is rampant in the case of fake pharmacies. Prescription drugs are expensive, controversial and dangerous even if obtained legally. Prescription drugs are complex chemicals that alter body functions. Like many scams this one targets the elderly, who are less likely to report the crime and more likely to suffer adverse effects from the toxins. Deaths from painkiller overdoses have exceeded those from heroin and cocaine in recent years. In 2005 drug poisonings were second only to automobile accidents for unintended deaths. Counterfeit drug investigations by the FDA have increased 10 times since 2000. Steroids are much easier for young athletes to obtain and even licensed pharmacists and physicians have been implicated in high-profile scams. This has been the most common type of spam observed by KnujOn and it has moved beyond the erectile dysfunction and now includes cancer, blood pressure, heart, arthritis, and diabetes medication as well as anti-depressants and psychotropics.

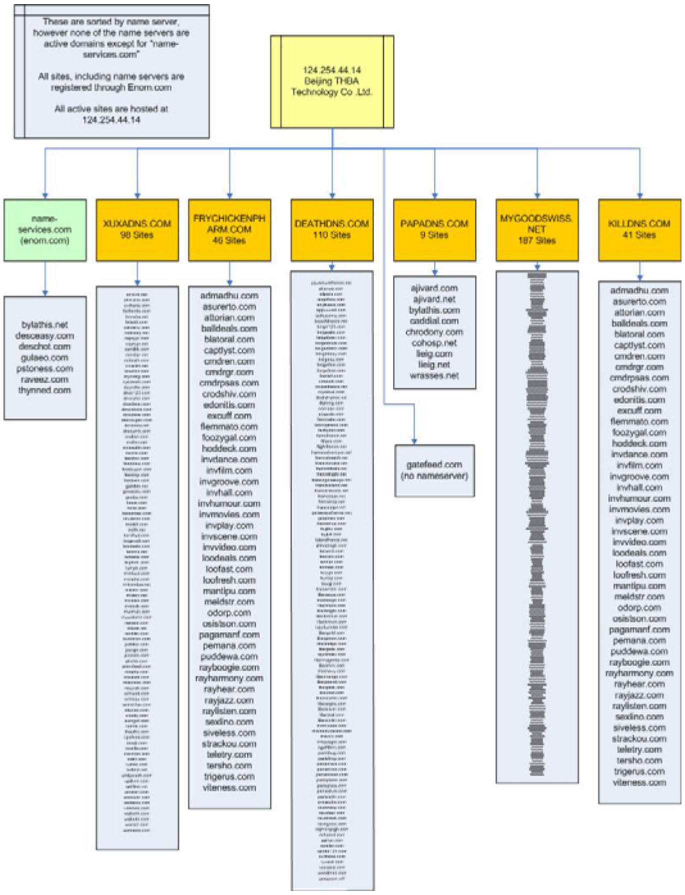
Pirated Software

Forged registrations are fairly standard for software piracy sites. Considering that the use of pirated software is estimated at 50% worldwide and that some developing countries have nearly 90% piracy rates there is a secondary threat looming. With private citizens, small business and even some governments purchasing and downloading pirated software there is a potential for a “big hack”. The person who is the source of pirated software can insert whatever they want into that installation bundle. The consumer of pirated software probably does not know their new office package contains pre-configured malware.

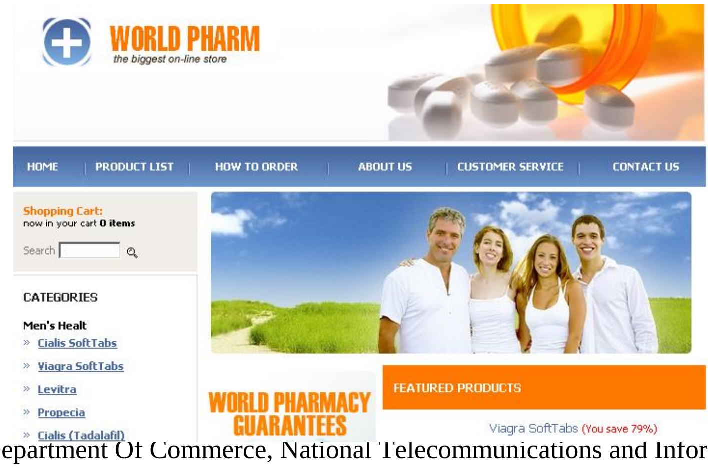
Mortgages/Loans

Forged registrations play an important role in the complex world financial transactions. There were 600 cases of mortgage fraud in 2004 and 21,971 in 2005 totaling over $1 Billion in losses(FBI). While the FBI reports that mortgage fraud cases are increasing, convictions, seizures, and recovered funds are declining. Some mortgage spams are just phishing/ID Theft attempts, others are “referrals”. Reverse Mortgages, “Teaser” ARMs, and “flipping” schemes are conducted by skilled industry insiders. Targets are often the elderly or people on a fixed income. While spam and domain fraud play a small part in the sub-prime mortgage crisis it is important to note that this is where the illicit networks are collecting money by preying on ignorance and fear.

The problems outlined here are complex and extend beyond the Internet. However, ICANN has an opportunity reduce the prevalence of illicit networks by expeditiously processing complaints and proactively enforcing compliance. For example, the following is a chart of a network of 518 fake pharmacy sites, all owned by one group, all registered through one registrar, and all using forged registrations:



“Kits” developed by illicit networks allow for quick registration and deployment of hundreds of domains at once. Most of the sites listed above were populated with the identical content:



Recommendations for ICANN

- ICANN should not allow privacy or proxy registrations for businesses. Especially businesses like banking and pharmaceuticals that are heavily regulated and are generally legally bound to disclose owner information. Whois privacy could be allowed for personal sites, advocacy groups, local organizations not involved in large commerce. This would be easy to determine on a registration application form. The registrant would have to disclose if the domain is being registered for commercial purposes. Failure to disclose commercial intent would be cause for suspension.

- ICANN should add a pharmacy disclosure on Whois records. The registrar need not verify that the registrant actually has a lawful pharmacy license. The registrant would be required to affirm that they do have a pharmacy license issued by some authority. Illegal pharmacy sites that do not disclose this can be immediately suspended. The pharmacy disclosure would make law enforcement investigations much simpler in this area. Considering the proliferation of fake Internet pharmacies, adding his disclosure could halt an enormous amount for fraud and poisonings.

- The Whois Data Problem Report System needs an upgrade. The inability to accept and process a large volume of reports is a serious concern. The lag in response time and follow up is unacceptable. It is evident that there is a lack of attention to this process and not enough resources dedicated to it. Expanding this department to be in proportion with size and growth of the Internet is imperative.

- Registrar applications require more scrutiny. Considering how many registrars are failing to meet their contractual agreements, a more thorough application process should be instituted to prevent inadequate and questionable companies from becoming registrars.

- Current registrars are either un-policed or self-policed. There are few repercussions for registrars who continue to sponsor illicit websites. Regular audits are not enough. Registrars who are clearly involved assisting illicit Internet networks need to be placed on a progressive path that leads to Accreditation Revocation. We understand that revocation of a registrar’s accreditation is a serious matter that would generate many hours of work for ICANN and severe inconvenience for registrar customers. Our recommendation is that registrars who fail to meet compliance requirements would be prevented from accepting new customers until the issue is resolved. Further non-compliance could result in money penalties and a full disclosure to their customers indicating that they are not in compliance. The final step would be revocation.

- If a domain has been terminated for inaccurate Whois data, the registrant should not be allowed to transfer the site to a new registrar with the same inaccurate data.

- Registrants with a history of bulk-registering inaccurate domain records should be banned from bulk-registering for some specified time, say six months.

- The ICANN audit of registrars should include a review of how they accept data from applicant registrants. Specifically, whether basic data form validation is employed by registrars.