“Rogue-Pharma” in .CO
The “33DRUGS” case

Gonzalo Romero
CSO - .CO Registry
© .CO Internet - COLOMBIA
Agenda

• .CO Internet – About us
• Rogue-Pharma ?
• “33DRUGS”
• 33DRUGS.CO
• Learned Lessons
• Q & A
.CO Internet – About us

• A **NEUSTAR** subsidiary in Colombia
  • Launched 2.010 to *promote* and *manage* the ccTLD
  • Concession contract with Colombian government (ITC Ministry)

• **.CO Statistics and Milestones**
  • 1.7M domains registered in +200 *countries* world-wide (60 registrars / resellers
  • 2.010: **28K** only *Colombian* registrations (.CO was delegated in 1.991)

• **Credibility and Awareness**
  • T.CO used by *Twitter* (~110M tweets a day), G.CO by *Google*, A/K/Z.CO by *AMAZON* as official “URL Shorteners”
  • 85% Top-100 Colombian enterprises use “.CO” as their *primary* online domain
  • All government agencies have at least one (1) .CO domain name.
Rogue-Pharma

• “Rogue Sites”
  • “On-line pharmacies” (no license) commercializing narcotics, anti-depressants, stimulants, steroids, counterfeited / adulterated medicines, without any medical prescription
  • Sell counterfeit drugs, manufactured in countries like China and India, under questionable hygienic conditions
  • **Violate** Colombian Law
    • Colombia is part of global anti-drug and patent protection treaties
  • **Violate** laws of countries to which they sell/send their products
    • USA: **Ryan-Haight Act** – sale to minors, don’t meet medicines import standards set by DEA
  • Often load credit cards from buyers and don’t send the purchased products.
Rogue-Pharma

• “Rogue Sites”
  • Sites highly promoted by spam campaigns generated by botnets
  • Content misleading (false WHOIS data) with fake licenses and accreditations, and located in different countries than they publish

• “Pharma Networks”
  • Recognized as criminal organizations by Law Enforcement Authorities (LEA’s) and regulation entities
  • Operate in East-Europe countries

• INTERPOL – “PANGEA” Operation
  • 2.011: LEA’s and organizations from 88 countries participated in an operation which suspended 13,500 “Pharma” related sites/domains
Rogue-Pharma

• “Rogue Sites”
  • Colombia is part of the “UN Convention against illicit traffic in narcotic drugs and psycotropic substances” (1.988)
    • Regulates the traffic of controlled substances commercialized in these sites
    • Convention created the “International Narcotics Control Board (INCB)”

• Colombia is part of the three (3) main international patent Treaties (which includes drugs): Paris, PCT, TRIPS

• Are NOT part of our “.CO Malicious Activities Monitoring (MAM)”
  • As for e-piracy, content, CP, we forward related cases to in-country LEA’s for their research and action.
“33DRUGS”

- Operation associated with
  - “Yambo Financials”, “EvaPharmacy” and/or “DrugRevenue”
  - One of the major known cyber-crime operations on the Internet

- Web sites “falsely imply” to be located in UK/USA, with “legitimate” e-commerce and operations license
  - *Illegal* operations
    - Drugs, IT [Spam, IP’s, servers]
  - Mostly operated by *Russians* and *Ukrainians*. 
“33DRUGS”

- **July 15, 2012**
  - IPv4 hosting “33DRUGS.CO”: 92.61.148.75
  - IPv4 listed in SPAMHAUS since January, 2011, associated with an Ukrainian Registrant
“33DRUGS”

- **NABP** (USA) – warns consumers against visiting.
• “Generic Viagra” (?)
  • PFIZER patent for Viagra expires in 2019

33Drugs FAQ

What does Generic stand for?
Generic drugs means using a different name for the same ingredients. The contents of the pills are absolutely the same in our generic version and the branded analogue.

Why is your ED drugs so cheap?
There is a number of reasons for that. We do not spend anything on marketing, there are no taxes to be paid as the product comes into the country unregistered, the manufacturer is located in an offshore zone and the production costs are way lower. No child labor is used.

Read all questions »
Facts about generic drugs »
33Drugs Female Sildenafil Description

Female Sildenafil
Quality generic

Lovegra provides intense sexual satisfaction for women seeking ultimate pleasure. It increases genital blood flow which intensifies pleasure during sexual activity.

Brand and Other Name(s): Lovegra, Lovegra, Womenra

Female Sildenafil 50mg

<table>
<thead>
<tr>
<th>Package</th>
<th>Per Pack</th>
<th>Per Item</th>
<th>Save</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 Pills</td>
<td>$54.00</td>
<td>$1.80</td>
<td></td>
<td>Buy online</td>
</tr>
</tbody>
</table>

Mega Viagra Pack

Mega Viagra Pack includes 4 pills each of Viagra 100mg, Female Viagra 100 mg, Viagra Caps 100 mg, Viagra Oral Jelly, Viagra Professional 100 mg, Viagra Soft 100 mg, Viagra Soft...
“33DRUGS”

- Sale of drugs without any medical prescription
- “Web Form” with no major restrictions

Extra Information

- Date of Birth: (Month, Day, Year)
- Your Height: 
- Your Weight: 
- Your Sex: Male/Female

Is your Personal Healthcare Practitioner aware that you are requesting this medication?

Have you been prescribed this medication before?

Have you had a physical exam in the last 12 months?

Please state the medical condition requiring you to use this medication IMPORTANT: your order will not be approved unless this question is answered fully:

Do you suffer from any seasonal allergies?

Please list in detail any allergies you have to medicines:

Terms & Conditions

I have Read and Agree with the 33drugs.co Terms & Conditions:
I have Read and Agree with the 33drugs.co Refund Policy:
I have Read and Agree with the 33drugs.co Notice of Privacy Practices:

By pressing the PLACE ORDER NOW button on the right, I agree to pay 33drugs.co
“33DRUGS”

- WHOIS.CO protected data *(privacy)*
- Internet.BS (Reseller)
  - Has only 0.2% of the global domain name market
  - BUT sponsors more than 40% of all Rogue Pharma sites
    - [LegitScript Report](#) (March, 2012)
  - Moved operations from Bahamas to Panama in 2011
    - At the time of this research, *there was no* contact information in their website.
August 9, 2012 – After officially forwarding the case to Colombian Police, we notify our Registrar (BCC'ing them) regarding “T&C”.

As you know, .CO INTERNET is the Registry and administrator of the .CO domain. As managers for the domain, we have a “Malicious Activities Monitoring”, which includes monitoring of .CO domains and performing any corrective actions for any issues found with domains that may affect the stability and security of .CO domains, the Registry, Registrars, Registrants, Partners or any other Internet users.

As part of our monitoring process, we’ve detected the following domain has been identified as a rogue pharmacy:

33DRUGS.CO

LegitScript has identified this as being in violation.
http://www.legitscript.com/pharmacy/33drugs.co

We politely request you to review if this site violates the registration agreement and terms and conditions you have with your customer.

We appreciate your help and support to maintain the highest standards of security for the .CO domain.

Sincerely,

Security Team

.CO INTERNET
+1 (866) 123 1234 (English) | +57 (020) 000 25 00 (Español) | CO-CERT@COInternet.CO | Follow us @DotCO
Gonzalo ROMERO <Gonzalo@cointernet.co>

Hemos tratado de gestionar el tema a través de la cooperación con el Registrador de este dominio y este a su vez con su revendedor (INTERNET.BS), pero no hemos recibido respuesta.

Agradecemos por favor sus noticias en relación con este incidente.

Atte.,

//Gonzalo

---

Gerardo ARISTIZABAL <gerardo@my.co>

Marco, Pavel,

Do you have any updates on the issue below?

Let me know and thanks!

Gerardo

---

Gerardo ARISTIZABAL <gerardo@my.co> wrote:

Dear Marco, Pavel,

For your information,

Gerardo

-------- Forwarded message --------
From: COINTERNET Support - Neustar <cssupport@neustar.biz>
Date: 2012/6/9
• **August 26, 2012** - *Internet.BS* proactively cooperated with us updating “**Terms and Conditions**” of their “**Registrar Agreement**” (ICANN)

• **URL:** [https://internetbs.net/en/domain-name-registrations/termsandconditions.html](https://internetbs.net/en/domain-name-registrations/termsandconditions.html)

• “Domain names registered with Internet.BS Corp. **may not be used to facilitate the sale of drugs in violation of Applicable Laws.** This expressly includes, but is not limited to, the sale of prescription drugs without a prescription based on a prior in-person examination, except where such is expressly permitted by Applicable Laws, or selling unapproved drugs (e.g., falsified medicines, counterfeit drugs, or drugs unapproved for sale)”

• These **Terms and Conditions** notify you that Internet.BS Corp. acts on notices from **LegitScript** about domain names that violate this section of our policy. If you have any questions about the basis for your website’s LegitScript classification, please contact **LegitScript** at [legitscript.com](http://legitscript.com)
August 29, 2012 – Registrar put the domain in “ClientHold” (Terms and Conditions)

Hi Gerardo,

We have suspended the domain. It was not in violation of our terms and conditions until the 26th when our new terms and conditions are in effect. Now it is in breach of our updated terms and conditions and we were able to suspend it.

Best regards,
Pavel Ciocan
Internet bs Corp.
http://www.internetbs.net

On 30-Aug-12 1:07 AM, GERARDO ARISTIZABAL wrote:

Marco, Pavel,

Sorry to be bothering again with this issue. I've had no updates on this case. Please send me some kind of information to know where this process is standing.

Thanks!
Gerardo

On Tue, Aug 14, 2012 at 5:53 PM, GERARDO ARISTIZABAL wrote:

Marco, Pavel,

Do you have any updates on the issue below?
Let me know and thanks!

Gerardo
**August 29, 2012 – WHOIS for the 33DRUGS.CO domain:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registrar-Reseller Name</td>
<td>INTERNET.BS (CORP)</td>
</tr>
<tr>
<td>Sponsoring Registrar CCD REG S.A.</td>
<td></td>
</tr>
<tr>
<td>Sponsoring Registrar IANA ID 1607</td>
<td></td>
</tr>
<tr>
<td>Registrar URL (registration services)</td>
<td><a href="http://my.co">http://my.co</a></td>
</tr>
<tr>
<td>Domain Status</td>
<td>clientHold</td>
</tr>
<tr>
<td>Domain Status clientTransferProhibited</td>
<td></td>
</tr>
<tr>
<td>Domain Status clientUpdateProhibited</td>
<td></td>
</tr>
<tr>
<td>Domain Status inactive</td>
<td></td>
</tr>
<tr>
<td>Registrant ID</td>
<td>INTEZVY00N7BINK2</td>
</tr>
<tr>
<td>Registrant Name</td>
<td>SUSPENDED DOMAIN</td>
</tr>
<tr>
<td>Registrant Organization</td>
<td>SUSPENDED BY REGISTRAR</td>
</tr>
<tr>
<td>Registrant Address 1</td>
<td>98 HAMPSHIRE STREET</td>
</tr>
<tr>
<td>Registrant Address 2</td>
<td>SUSPENDED DOMAIN</td>
</tr>
<tr>
<td>Registrant City</td>
<td>NASSAU</td>
</tr>
<tr>
<td>Registrant Postal Code</td>
<td>4892</td>
</tr>
<tr>
<td>Registrant Country</td>
<td>Bahamas</td>
</tr>
<tr>
<td>Registrant Country Code</td>
<td>BS</td>
</tr>
<tr>
<td>Registrant Phone Number</td>
<td>+1.23456799</td>
</tr>
<tr>
<td>Registrant Email</td>
<td><a href="mailto:suspended.domain@topdns.com">suspended.domain@topdns.com</a></td>
</tr>
</tbody>
</table>
“33DRUGS”

- May 31, 2013 – Web site “active” again (Registrar: PDR / DIRECTI)
- May 31, 2013 – Notification to the Registrar (Terms and Conditions), BCC’ing National Police
  - Immediately put the domain on ClientHold (CH)

Domain Name: **33DRUGS.CO**
Domain ID: D44663811-CO
Sponsoring Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Registrar URL: www.PublicDomainRegistry.com
Domain Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Registrant ID: DI_14418420
Register Name: Andrew Tsyplakov
Register Organization: promo
Register Address: 1 Mira 25a of 59
Register City: Kherson
Register State/Province: Kherson Oblast
Register Postal Code: 73008
Register Country: Ukraine
Register Country Code: UA
Register Phone Number: +38 552444524
Register Email: promopharmacy@googlemail.com
Name Server: NS1.SUSPENDED-DOMAIN.COM
Name Server: NS2.SUSPENDED-DOMAIN.COM
Created by Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Last Updated by Registrar: PDR LTD. D/B/A PUBLICDOMAINREGISTRY.COM
Domain Registration Date: Thu May 16 14:59:29 GMT 2013
Domain Expiration Date: Thu May 15 23:59:59 GMT 2014
Domain Last Updated Date: Fri May 31 21:05:19 GMT 2013
33DRUGS.COM

ESTADO DEL PEDIDO

Si desea comprobar el estado de su pedido, puede hacerlo escribiendo su dirección de correo electrónico y número de tarjeta de crédito o ID del pedido en el siguiente formulario. Los campos marcados con * son obligatorios.

- **Su correo electrónico** *
- **Tarjeta de Crédito #**
- **OR** *
- **ID del pedido**
- **Verification code** *

Verificación Try a new code

Asegúrese de utilizar el mismo número de tarjeta de crédito que utilizó al hacer su solicitud, de lo contrario nuestro sistema no será capaz de encontrar su orden. Los campos obligatorios están marcados con un *.
Learned Lessons

• Strong cooperation action from “Registry channel” (Registrar, Resellers) and Law Enforcement
  • While our channel may have compromised/malicious sites, they cooperate with us by updating their customer’s “Terms and Conditions”

• Having well-defined “Baselines”, “Policies” and “Terms and Conditions” is key for research and getting successful cases

• Proactive domain name registrations monitoring and follow-up: another key for success.
Igor Artimovich has been linked with a prolific illegal network of virus-infected computers that send spam worldwide. *Photo: James Hill/New York Times*

Pavel Vrublevsky, centre, the owner of the online payment settlement business, ChronoPay, with Igor Artimovich, right, and Dmitry Artimovich, a freelance programmer. *Photo: James Hill/New York Times*
¡Thank you!

Gonzalo Romero

G@Go.CO

@GonzaloARomeroB | @DotCO