



26th annual **FIRST** conference



BOSTON

M A S S A C H U S E T T S

JUNE 22-27, 2014

Back to the 'root' of Incident Response

Boston Park Plaza Hotel | June 22-27, 2014



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

Gonzalo Romero

CSO - .CO Registry

© .CO Internet - COLOMBIA



BOSTON



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 *counterfeited 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
 - Details: <http://legitscriptblog.com/2010/01/new-rogue-internet-pharmacies-it%E2%80%99s-a-33-drugs-day/>
- 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, 2.012**

- IPv4 hosting “33DRUGS.CO”:
92.61.148.75
- IPv4 listed in **SPAMHAUS** since **January, 2.011**, associated with an *Ukrainian* Registrant

92.61.148.75/32 is listed on the Spamhaus Block List (SBL)

2011-01-17 19:54:58 GMT SR02 | [servage.com](#)

ROKSO Register Of Known Spam Operations (ROKSO)

Spam Operation: Yambo Financials

92.61.148.75/32 is listed on the SBL as being assigned to, being under the control of, or being otherwise connected with a known spam operation listed on the ROKSO database as: [Yambo Financials](#)

med-store.org etc.

med-store.org A 92.61.148.75
www.med-store.org A 92.61.148.75
33drugs.co.uk A 92.61.148.75
33drugs.info A 92.61.148.75

92-61-148-75.static.servage.net

Domain ID:D25703726-LRMS
Domain Name:33DRUGS.INFO
Created On:30-Jul-2008 08:45:43 UTC
Last Updated On:05-Mar-2010 12:10:00 UTC
Expiration Date:30-Jul-2011 08:45:43 UTC
Sponsoring Registrar:Internet.bs Corp. (R457-LRMS)
Status:CLIENT TRANSFER PROHIBITED
Registrant ID:INTE4b0ef106dbc7
Registrant Name:Private Whois Service

[whois.nic.uk]

Domain name:
33drugs.co.uk

Registrant:
Andrew Tsyplakov

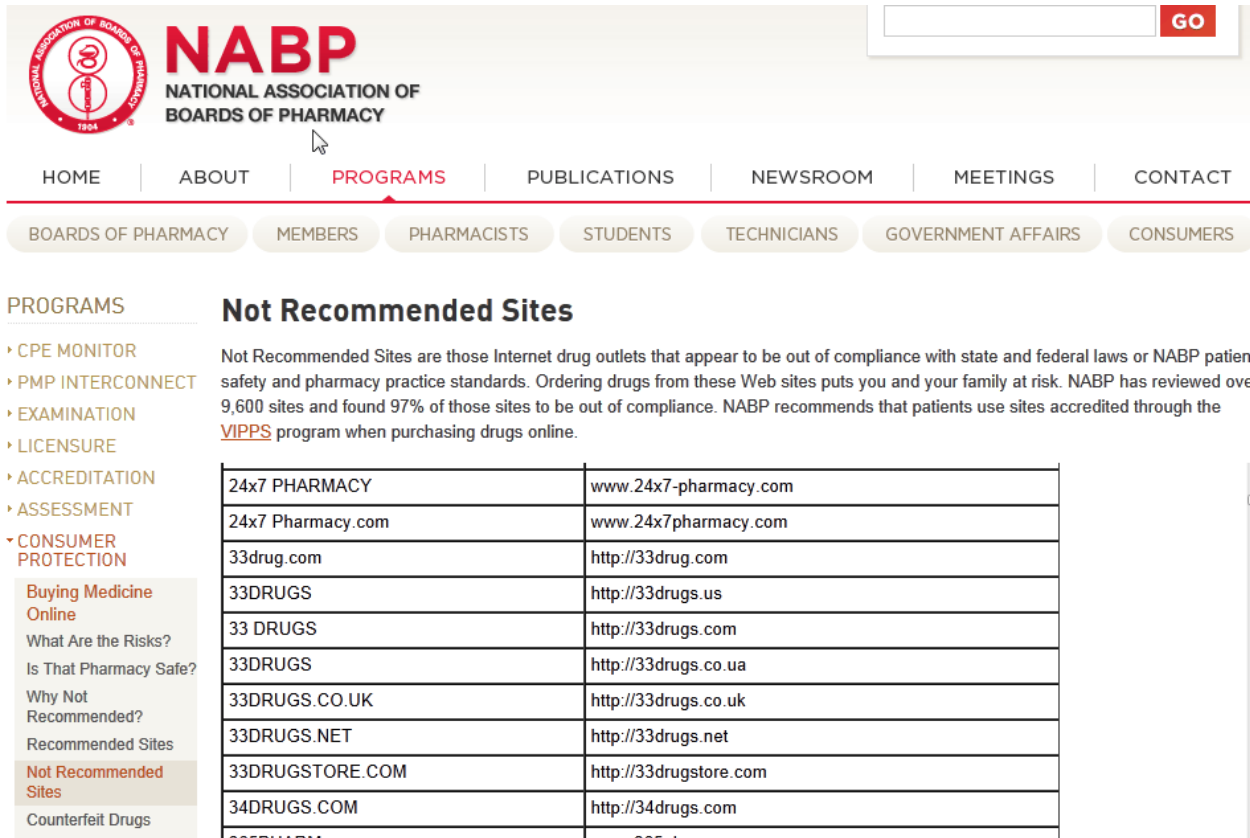
Registrant type:
Unknown

Registrant's address:
Berislavskoe shose 10d of59
Kherson
73008

“33DRUGS”



- [NABP](#) (USA) – warns consumers against visiting.



NABP
NATIONAL ASSOCIATION OF
BOARDS OF PHARMACY

HOME | ABOUT | **PROGRAMS** | PUBLICATIONS | NEWSROOM | MEETINGS | CONTACT

BOARDS OF PHARMACY | MEMBERS | PHARMACISTS | STUDENTS | TECHNICIANS | GOVERNMENT AFFAIRS | CONSUMERS

PROGRAMS

- ▶ CPE MONITOR
- ▶ PMP INTERCONNECT
- ▶ EXAMINATION
- ▶ LICENSURE
- ▶ ACCREDITATION
- ▶ ASSESSMENT
- ▶ CONSUMER PROTECTION
 - Buying Medicine Online
 - What Are the Risks? Is That Pharmacy Safe?
 - Why Not Recommended? Recommended Sites
 - Not Recommended Sites**
 - Counterfeit Drugs

Not Recommended Sites

Not Recommended Sites are those Internet drug outlets that appear to be out of compliance with state and federal laws or NABP patient safety and pharmacy practice standards. Ordering drugs from these Web sites puts you and your family at risk. NABP has reviewed over 9,600 sites and found 97% of those sites to be out of compliance. NABP recommends that patients use sites accredited through the [VIPPS](#) program when purchasing drugs online.

24x7 PHARMACY	www.24x7-pharmacy.com
24x7 Pharmacy.com	www.24x7pharmacy.com
33drug.com	http://33drug.com
33DRUGS	http://33drugs.us
33 DRUGS	http://33drugs.com
33DRUGS	http://33drugs.co.ua
33DRUGS.CO.UK	http://33drugs.co.uk
33DRUGS.NET	http://33drugs.net
33DRUGSTORE.COM	http://33drugstore.com
34DRUGS.COM	http://34drugs.com

“33DRUGS”



- ★ 33Drugs Store
- ★ Order Status
- ★ FAQ
- ★ Testimonials
- ★ Newsletter
- ★ Refer a Friend
- ★ Shipping Terms
- ★ Terms of Use
- ★ Request Callback
- ★ Contact Us

Get 4 Sildenafil Drugs FREE!

Men's Health drugs

- 36Plus
- Apcalis
- Avodart
- Casodex
- ED Discount Pack #1
- ED Discount Pack #2
- ED Discount Pack #3
- ED Discount Pack #4
- ED Trial Pack
- Eulexin
- Fiomax
- Herbal Sildenafil
- Himalaya Speman
- Kamagold
- Kamagra Effervescent
- Kamagra Soft
- Kamagra Soft Flavored

Call us Toll FREE
1-866-33-DRUGS

COMPARE ED

Details

Browse by drug first letter: ABCDEFGHIJKLMNOPQRSTUVWXYZ

You \$0.00

33Drugs Sildenafil Description



Sildenafil

Quality generic

Sildenafil is used for treatment of ED in men. Sildenafil increases the body's ability to achieve and maintain an erection during sexual stimulation.

Brand and Other Name(s): Viagara, Sildenafil Citrate, Sildenafil Tablets, Ruagra, Kamagra, Caverta, Silagra

[Large product images](#)

Sildenafil 25mg

Package	Per Pack	Per Item	Save	Order
10 Tabs + Free Sildenafil	\$19.00	\$1.90		Buy online
20 Tabs + Free Sildenafil	\$35.00	\$1.75	\$3.00	Buy online

• “Generic Viagra” (?)

- PFIZER patent for Viagra expires in 2.019

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”



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): Lowegra, Lovegra, Womenra

- “Female Viagra”/“Lovegra” (?)
 - PFIZER do NOT produce such drugs

Female Sildenafil **50mg**

Package	Per Pack	Per Item	Save	Order
30 Pills	\$54.00	\$1.80		Buy online



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”



33drugs.com https://secure.33drugs.com/cart/checkout.php?_session_id=452dad1d Startpage

Extra Information

Date of Birth: *

Your Height: *

Your Weight: *

Your Sex: * Male Female

Is your Personal Healthcare Practitioner aware that you are requesting this medication? * Yes No

Have you been prescribed this medication before? * Yes No

Have you had a physical exam in the last 12 months? * Yes No

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? * Yes No

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.

PLACE ORDER NOW

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

“33DRUGS”



Domain Name	33DRUGS.CO
Domain ID	D4439476-CO
Registrar-Reseller Name	INTERNET.BS CORP.
Sponsoring Registrar	CENTRAL COMERCIALIZADORA DE INTERNET PANAMA S.A.
Sponsoring Registrar IANA ID	1607
Registrar URL (registration services)	http://my.co
Domain Status	clientTransferProhibited
Registrant ID	INTEZVV90N7BINK2
Registrant Name	DOMAIN ADMINISTRATOR
Registrant Organization	FUNDACION PRIVATE WHOIS
Registrant Address1	ATTN: 33DRUGS.CO
Registrant Address2	APTDS. 🇵🇦 0850-00056 📞
Registrant City	PANAMA
Registrant Postal Code	ZONA 15
Registrant Country	Panama
Registrant Country Code	PA
Registrant Phone Number	+507.65995877
Registrant Email	m3f5z4u4f80838125dbb@t02cduv4f7f99a255f64.privatewhois.net
Administrative Contact ID	INTE4HRBMNA7UUDV
Administrative Contact Name	DOMAIN ADMINISTRATOR
Administrative Contact Organization	FUNDACION PRIVATE WHOIS

- 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, 2.012)
 - Moved operations from Bahamas to Panama in 2.011
 - At the time of this research, *there was no contact information in their website.*

“33DRUGS”



- **August 9, 2.012** – After officially forwarding the case to Colombian Police, we notify our **Registrar** (BCC'ing them) regarding “T&C”

33DRUGS.CO : ROGUE PHARMACY - We need your cooperation A.S.A.P. [ref:_00D30ZFj._50070NoB2y:ref] [Gmail](*) MAM - RD/CP/OLD - MAM/2012 - 08 x

.CO INTERNET Support - Neustar cosupport@neustar.biz via upd0n4g14kmc.3-zfjeam.7.bnc.salesforce.com

8/9/12 ☆

to gerardo, aristizabal, juancamilo, co-cert, gonzalo, cocert

Greetings CCI REG S.A.

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 (320) 899 25 99 (Español) | CO-CERT@COInternet.CO | Follow us @DotCO

"33DRUGS"



• August 22, 2.012 – Colombian Police case progress?

FW: 33DRUGS.CO : ROGUE PHARMACY - We need your cooperation A.S.A.P. [ref:_00D30ZF]_50070NoB2y:ref]



[Gmail](*) MAM - RDCP/OLD - MAM/2012 - 08 x

Gonzalo ROMERO <Gonzalo@cointernet.co>
to felix.miranda, fredy.bautista, eduardo ▾

8/22/12 ☆



Saludos, Teniente Miranda.

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](#)

Gonzalo A Romero B | Chief Security Officer | [.CO Internet S.A.S.](#) | [Gonzalo@COInternet.CO](#) | [www.COInternet.CO](#) | WTC - Calle 100 No. 8A-49 (B-507) – Bogota - COLOMBIA | [+57 \(320\) 899.25.99](#) | [@DotCO](#)

From: GERARDO ARISTIZABAL [<mailto:gerardo@my.co>]
Sent: Tuesday, August 14, 2012 5:53 PM
To: Marco Rinaudo - Internet.bs Corp.; pavel.ciocan@internet.bs
Subject: Re: [33DRUGS.CO](#) 🟡 : ROGUE PHARMACY - We need your cooperation A.S.A.P. [ref:_00D30ZF]_50070NoB2y:ref]

Marco, Pavel,

Do you have any updates on the issue below?

Let me know and thanks!

Gerardo

On Thu, Aug 9, 2012 at 6:31 PM, GERARDO ARISTIZABAL <gerardo@my.co> wrote:
Dear Marco, Pavel,

For your information.

Gerardo

----- Forwarded message -----

From: [.CO INTERNET Support - Neustar](#) <cosupport@neustar.biz>
Date: 2012/8/9

“33DRUGS”



- **August 26, 2.012** - **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>
 - “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

"33DRUGS"



- **August 29, 2.012** – *Registrar* put the domain in “ClientHold” (Terms and Conditions)

Fwd: 33DRUGS.CO : ROGUE PHARMACY - We need your cooperation A.S.A.P. [ref:_00D30ZFj._50070NoB2y:ref]

[Gmail](*) MAM - RDCCPOLD - MAM2012 - 08 x



GERARDO ARISTIZABAL <gerardo@my.co>

8/29/12 ☆

to Gonzalo ▾

----- Forwarded message -----

From: Pavel Ciocan <pavel.ciocan@internet.bs>

Date: Wed, Aug 29, 2012 at 5:26 PM

Subject: Re: 33DRUGS.CO : ROGUE PHARMACY - We need your cooperation A.S.A.P. [ref:_00D30ZFj._50070NoB2y:ref]

To: GERARDO ARISTIZABAL <gerardo@my.co>

Cc: "Marco Rinaudo - Internet.bs Corp." <marco.rinaudo@internet.bs>

Hi Gerardo,

We have suspended the domain. It was not in violation of our terms and conditions till 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. ¿Do you have any 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 <gerardo@my.co> wrote:

Marco, Pavel,

Do you have any updates on the issue below?

Let me know and thanks!

Gerardo

“33DRUGS”



- **August 29, 2.012** – [WHOIS](#) for the 33DRUGS.CO domain:

Registrar-Reseller Name [INTERNET.BS](#) CORP.
Sponsoring Registrar CCI REG S.A.
Sponsoring Registrar IANA ID 1607
Registrar URL (registration services) <http://my.co>
Domain Status **clientHold**
Domain Status clientTransferProhibited
Domain Status clientUpdateProhibited
Domain Status inactive
Registrant ID INTEZVV90N7BINK2
Registrant Name SUSPENDED DOMAIN
Registrant Organization SUSPENDED BY REGISTRAR
Registrant Address1 98 HAMPSHIRE STREET
Registrant Address2 SUSPENDED DOMAIN
Registrant City NASSAU
Registrant Postal Code 4892
Registrant Country Bahamas
Registrant Country Code BS
Registrant Phone Number +1.23456789
Registrant Email suspended.domain@topdns.com

“33DRUGS”



- **May 31, 2.013** – Web site “active” again (Registrar: PDR / DIRECTI)
- **May 31, 2.013** – 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](#)

Sponsoring Registrar IANA ID 303

Registrar URL (registration services) [www.PublicDomainRegistry.com](#)

Domain Status clientDeleteProhibited

Domain Status clientHold

Domain Status clientTransferProhibited

Domain Status clientUpdateProhibited

Registrant ID DI [14418420](#)

Registrant Name Andrew Tsyplakov

Registrant Organization promo

Registrant Address1 Mira 25a of.59

Registrant City Kherson

Registrant State/Province Kherson Oblast

Registrant Postal Code 73008

Registrant Country Ukraine

Registrant Country Code UA

Registrant Phone Number [+38.552444524](#)

Registrant 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





Teléfono gratuito EE.UU. / Canadá: 1-866-33-DROGAS
Internacional: +44 20 8133 8455
Fax: +44 20 8711 5898
* Nota: Las tarifas internacionales aplicables.

ESTADO DEL PEDIDO

CONTÁCTENOS

PETICIÓN DE CALLBACK



TRANSACCIONES 100% SEGURAS

[Click here to chat](#)

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 obligatorias

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

Rogue-Pharma: The *Good* News

Sept 3rd, 2.013 - <http://x.co/239Fy>



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



BOSTON

