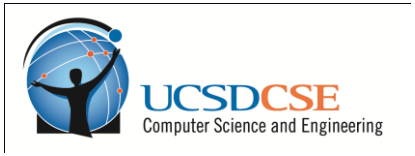
On the Effects of Registrar-level Intervention



He (Lonnie) Liu
Kirill Levchenko
Geoffrey M. Voelker
Stefan Savage

UC San Diego

Mark Felegyhazi
Christian Kreibich

UC Berkeley
ICSI

Spam


Free Plane Tickets
Two Free JetBlue Airlines Tickets – Details Inside
me
»
liulonnie Rolex.com For You -86% - Dear liulonnie@g
Microsoft® Corporation UK
Congratulation Winner No2 - Dear Winner. Attached t
Buy Cialis Online - $1.79 per Dose
No Prescription Required. Free Combo Pack with Order. No tablet splitting hassle!
Click here for 10mg Cialis, 20 for $48, 36 for $88, 60 for $106 10-20% Bonus on ReOrders.
Printer Ink Savings
Printer Ink Discounted - Save up to 75%OFF Today!
Mr. Kevin Momoh
(no subject) - My name is Mr. Kevin Momoh, a politicia
Medical Assistant
Restart Your Career, Become a CMA Today!
Josie Necole
»
No Prescription Required. Free Combo Pack with O

Spam Infrastructure

- Mail address harvesting
- Botnet mail senders
- Domain names
- Proxies and redirections
- Web hosting
- etc.

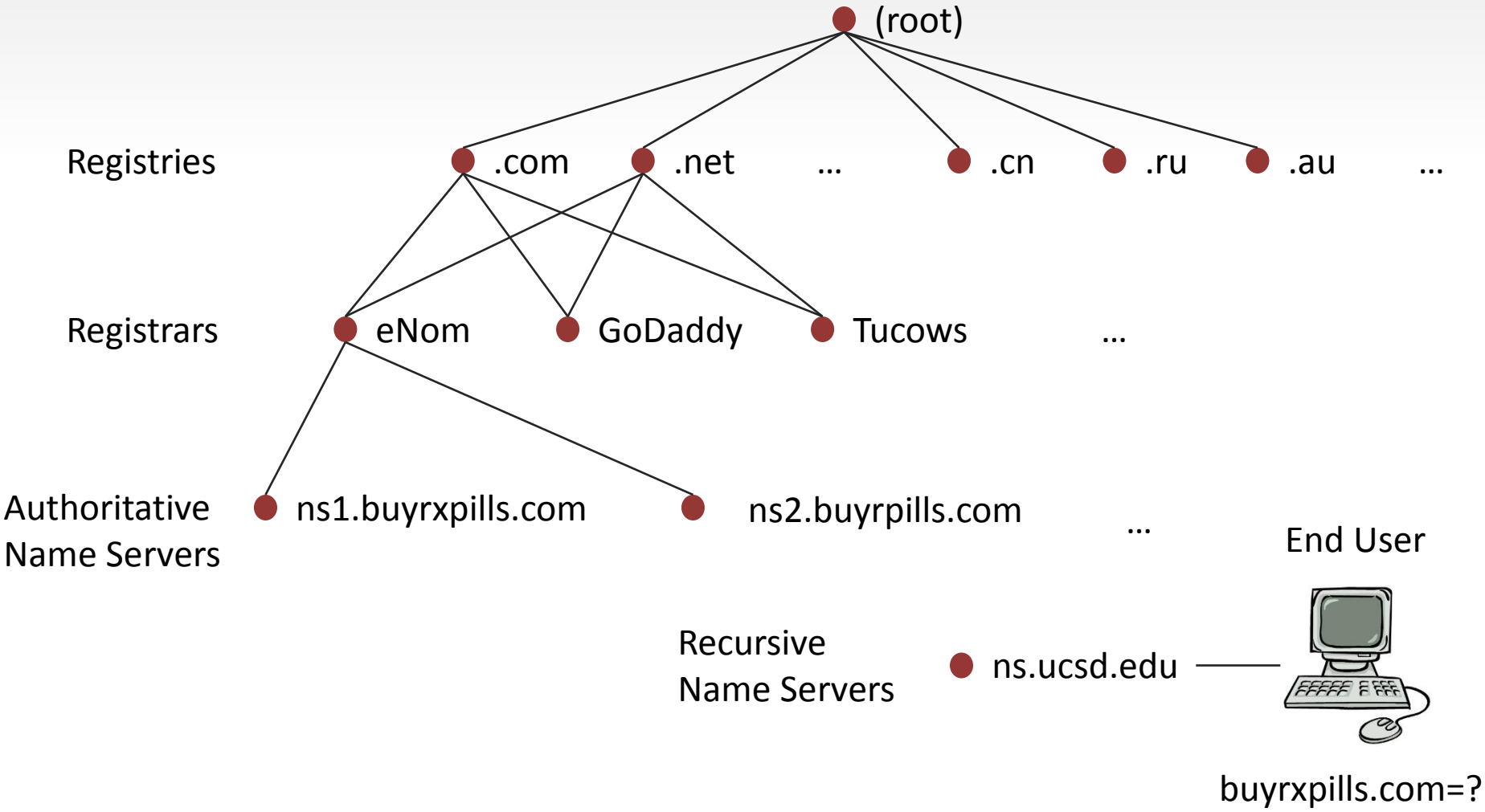
Spam Infrastructure

- Mail address harvesting
- Botnet mail senders
- **Domain names**
- Proxies and redirections
- Web hosting
- etc.

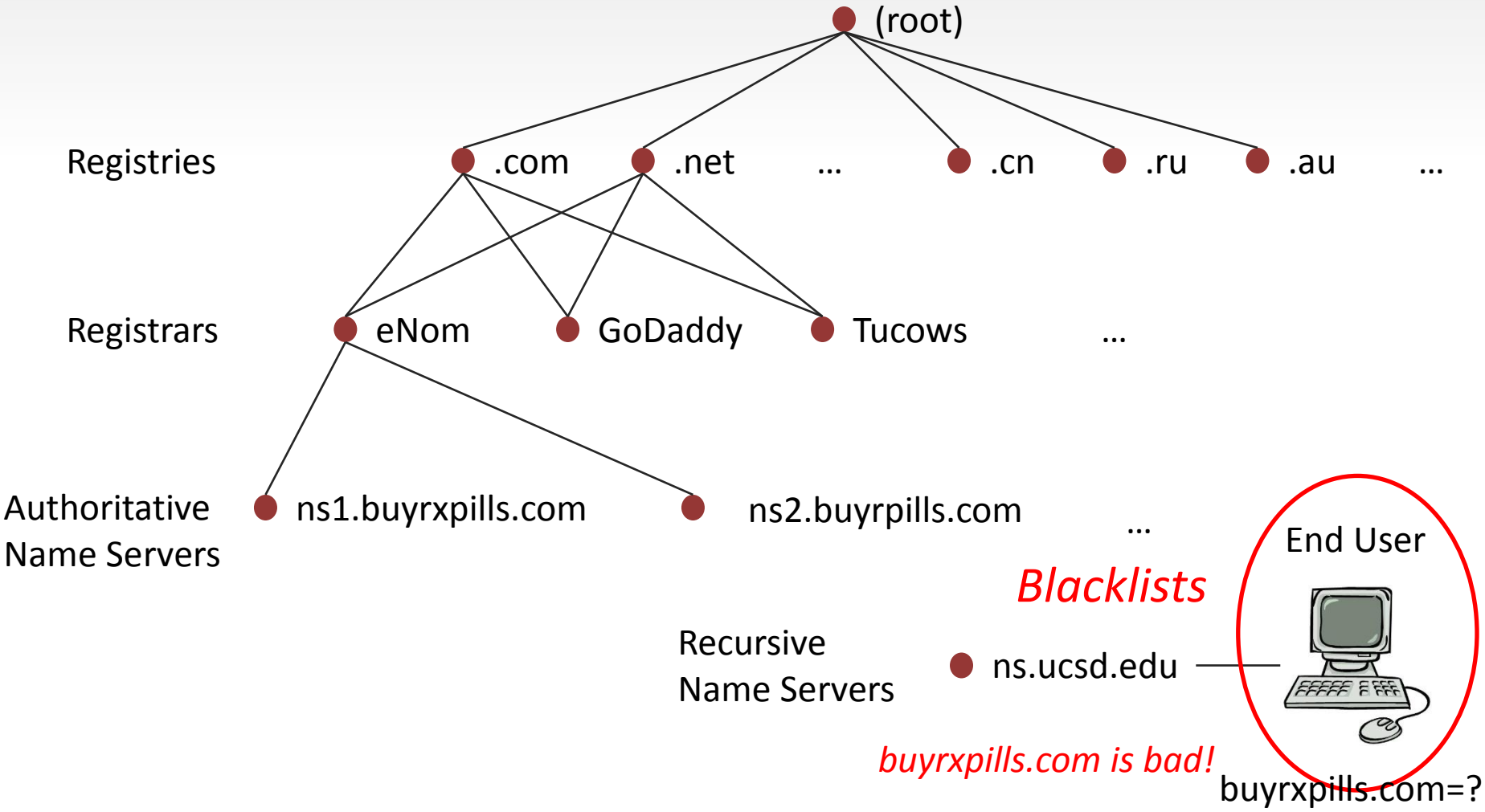
Spam


Free Plane Tickets
Two Free JetBlue Airlines Tickets – Details Inside
me
»
liulonnie Rolex.com For You -86% - Dear liulonnie@g
Microsoft® Corporation UK
Congratulation Winner No2 - Dear Winner. Attached t
Buy Cialis Online - $1.79 per Dose
No Prescription Required. Free Combo Pack with Order. No tablet splitting hassle!
Click here for 10mg Cialis, 20 for $48, 36 for $88, 60 for
http://buyrxpills.com/
Printer Ink Savings
Printer Ink Discounted - Save up to 75%OFF Today!
Mr. Kevin Momoh
(no subject) - My name is Mr. Kevin Momoh, a politicia
Medical Assistant
Restart Your Career, Become a CMA Today!
Josie Necole
»
No Prescription Required. Free Combo Pack with O

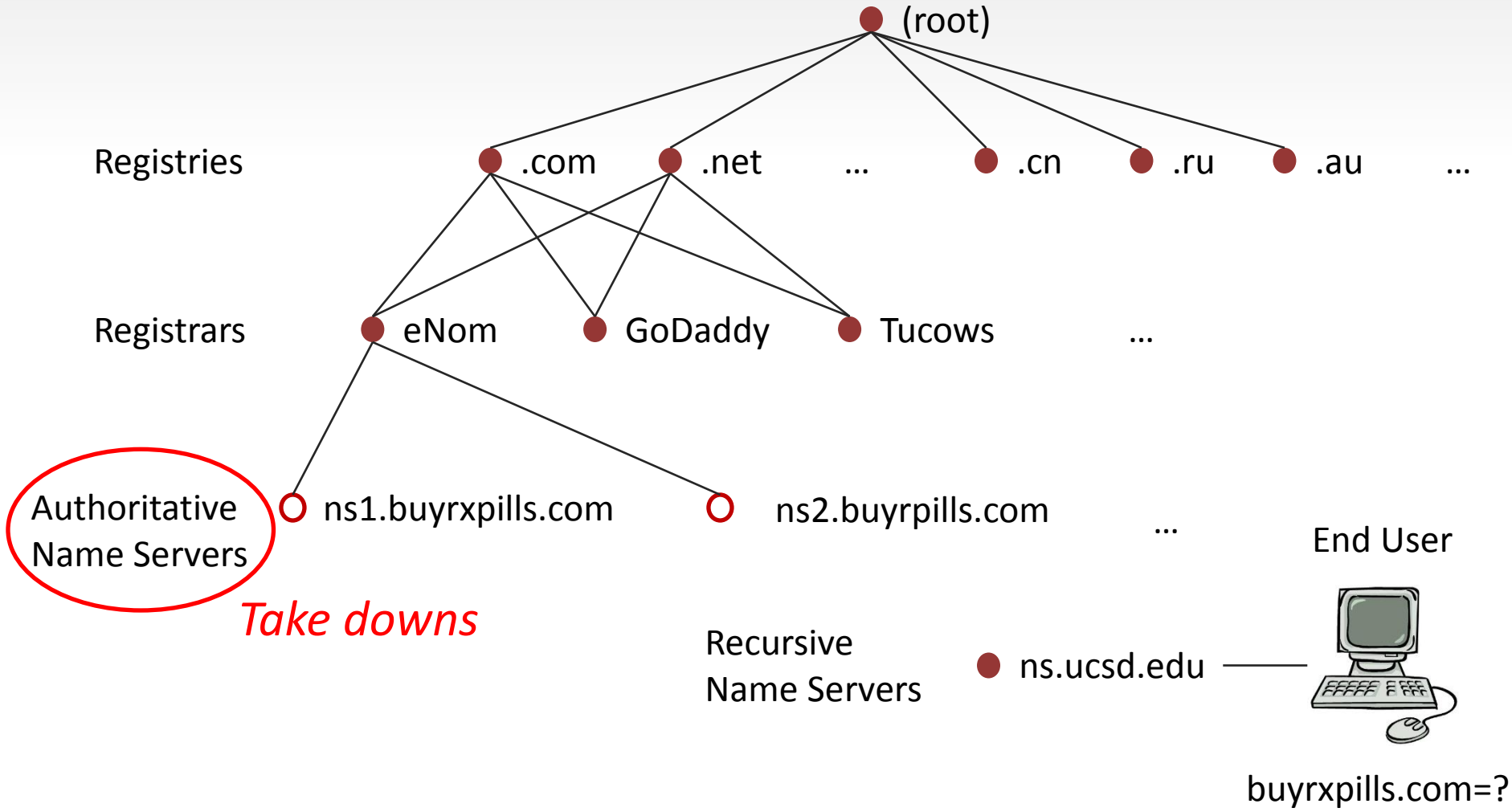
Domain Name System (DNS)



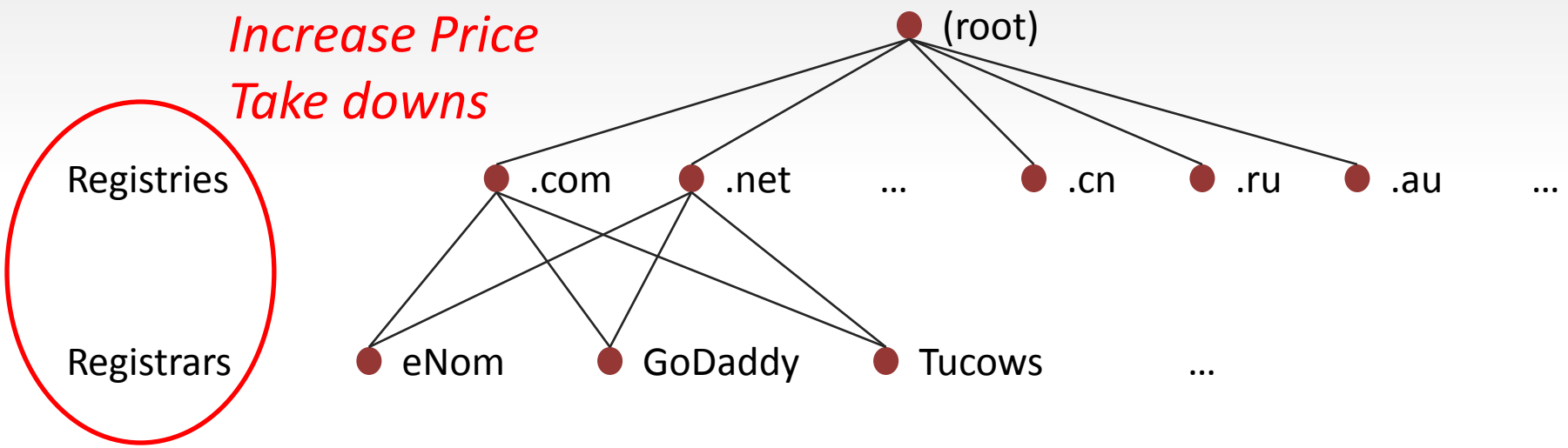
Domain Name System (DNS)



Domain Name System (DNS)



Domain Name System (DNS)



Authoritative Name Servers

ns1.buyrxpills.com

ns2.buyrpills.com

…

End User

Recursive Name Servers

ns.ucsd.edu

buyrxpills.com=?

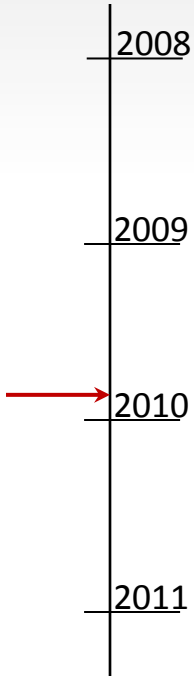
Two Registration Policy Changes

Two Registration Policy Changes

Dec. 2009

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

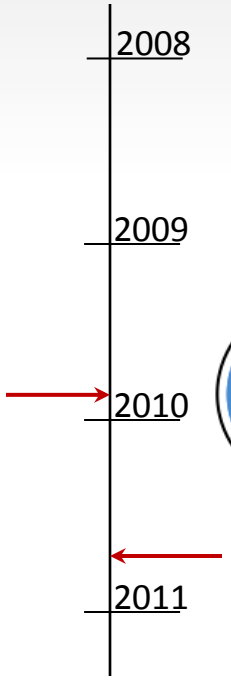
.cn



Two Registration Policy Changes

Dec. 2009

.cn



Sep. 2010

Our Approach

- Collect spam domains from spam feeds
- Track DNS name server activities
  - Zone files
- Track registration info
  - WHOIS, DomainTools.com (historic WHOIS service)
- Tagged pharmacy domains
  - Click Trajectory (Oakland ‘11)

December, 2009

.cn

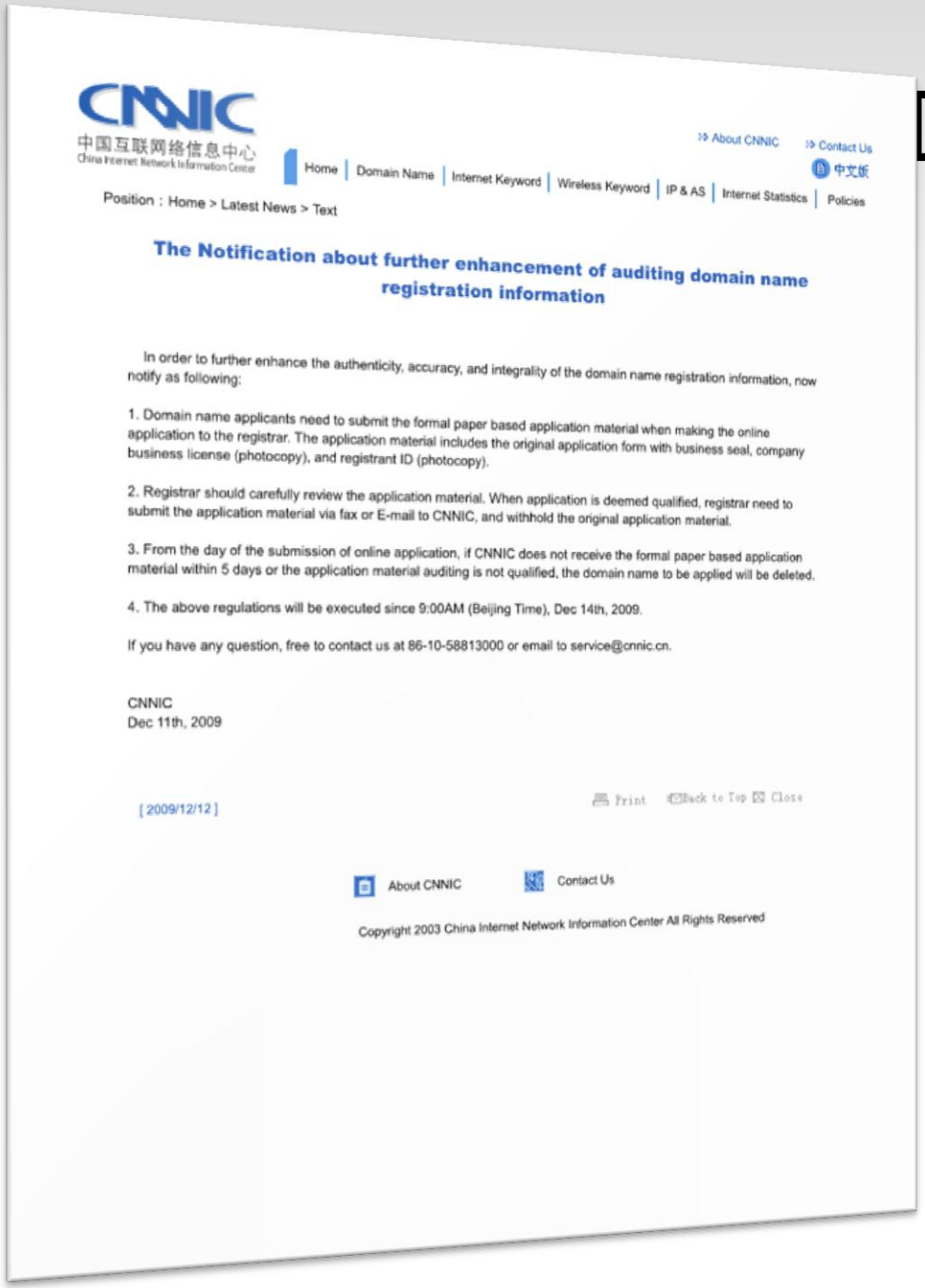
Cost of a .cn Domain

2007-2008

=

(15 cents)

Domain



中国互联网络信息中心
China Internet Network Information Center

About CNNIC | Contact Us | 中文版

Home | Domain Name | Internet Keyword | Wireless Keyword | IP & AS | Internet Statistics | Policies

Position : Home > Latest News > Text

The Notification about further enhancement of auditing domain name registration information

In order to further enhance the authenticity, accuracy, and integrality of the domain name registration information, now notify as following:

1. Domain name applicants need to submit the formal paper based application material when making the online application to the registrar. The application material includes the original application form with business seal, company business license (photocopy), and registrant ID (photocopy).

2. Registrar should carefully review the application material. When application is deemed qualified, registrar need to submit the application material via fax or E-mail to CNNIC, and withhold the original application material.

3. From the day of the submission of online application, if CNNIC does not receive the formal paper based application material within 5 days or the application material auditing is not qualified, the domain name to be applied will be deleted.

4. The above regulations will be executed since 9:00AM (Beijing Time), Dec 14th, 2009.

If you have any question, free to contact us at 86-10-58813000 or email to service@cnnic.cn.

CNNIC
Dec 11th, 2009

[2009/12/12]

Print Back to Top Close

About CNNIC Contact Us

Domain

CNNIC
中国互联网络信息中心
China Internet Network Information Center

About CNNIC | Contact Us | 中文版

Home | Domain Name | Internet Keyword | Wireless Keyword | IP & AS | Internet Statistics | Policies

Position : Home > Latest News > Text

The Notification about further enhancement of auditing domain name registration information

In order to further enhance the authenticity, accuracy, and integrality of the domain name registration information, now notify as following:

1. Domain name applicants need to submit the formal paper based application material when making the online application to the registrar. The application material includes the original application form with business seal, company business license (photocopy) and registrant ID (photocopy).

2. Registrar shou... refully review the application material. When application is deemed qualified, registrar need to submit the applicatio... terial via fax or E-mail to CNNIC, and withhold the original application material.

3. From the day of the sub... online application, if CNNIC does not receive the formal paper based application material within 5 days or the ... material auditing is not qualified, the domain name to be applied will be deleted.

4. The above regulations will be ex... 0AM (Beijing Time), Dec 14th, 2009.

If you have any question, free to contact ... 00 or email to service@cnnic.cn.

CNNIC
Dec 11th, 2009

[2009/12/12]

business license (photocopy)

About CNNIC | Contact Us

中华人民共和国
增值电信业务经营许可证

经营许可证编号: 苏 B2-20060151

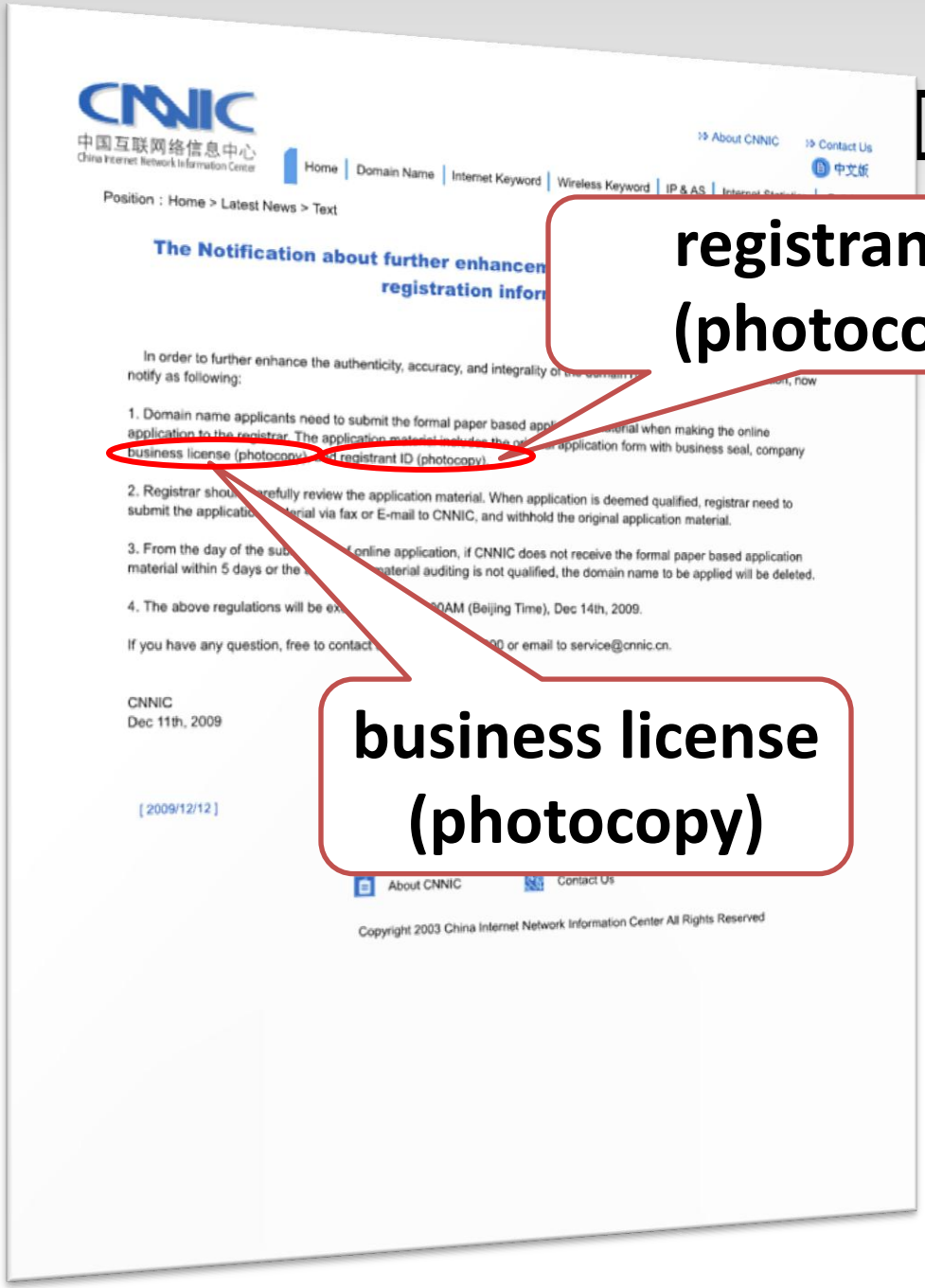
根据《中华人民共和国电信条例》及国家有关规定，经审查，准许你公司按照本经营许可证（正文和附件）载明的内容经营增值电信业务，特颁发增值电信业务经营许可证。

公司名称: 南京迅虎科技有限公司
法定代表人: 丁前胜
注册资本: 100 万元人民币
注册住所: 南京市雨花台区西善桥街道梅山村中心路 81 号
业务种类: 第二类增值电信业务中的信息服务业务（不含固定网电话声讯服务）
业务覆盖范围（服务项目）: 江苏省。

签发人: 发证机关(盖章):

发证日期: 2006 年 09 月 15 日
有效期至: 2011 年 09 月 15 日

Domain



registrant id (photocopy)

business license (photocopy)

Domain

CNNIC
中国互联网络信息中心
China Internet Network Information Center

About CNNIC | Contact Us | 中文版

Home | Domain Name | Internet Keyword | Wireless Keyword | IP & AS | Internet Statistic

Position : Home > Latest News > Text

The Notification about further enhancen
registration infor

In order to further enhance the authenticity, accuracy, and integrity of the domain n… …ion, now notify as following:

1. Domain name applicants need to submit the formal paper based appl… …terial when making the online application to the registrar. The application material includes the ori… …application form with business seal, company business license (photocopy) … registrant ID (photocopy).

2. Registrar shou… …refully review the application material. When application is deemed qualified, registrar need to submit the applicati… …terial via fax or E-mail to CNNIC, and withhold the original application material.

3. From the day of the sub… …online application, if CNNIC does not receive the formal paper based appl… material within 5 days or the … …material auditing is not qualified, the domain name to be appl… …be deleted.

4. The above regulations will be ex… …0AM (Beijing Time), Dec 14th, 2009.

If you have any question, free to contact … …90 or email to service@cnnic.cn.

CNNIC
Dec 11th, 2009

[2009/12/12]

About CNNIC | Contact Us

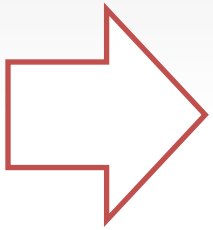
registrant id (photocopy)

Dec 14, 2009

business license (photocopy)

Cost of a .cn Domain

2007-2008



Dec 14, 2009

=

(15 cents)

Cost of a .cn Domain

2007-2008

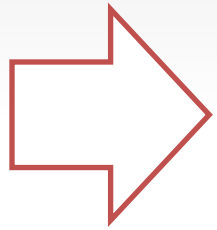
(15 cents)

Dec 14, 2009

(10 dollars)

Cost of a .cn Domain

2007-2008



Dec 14, 2009

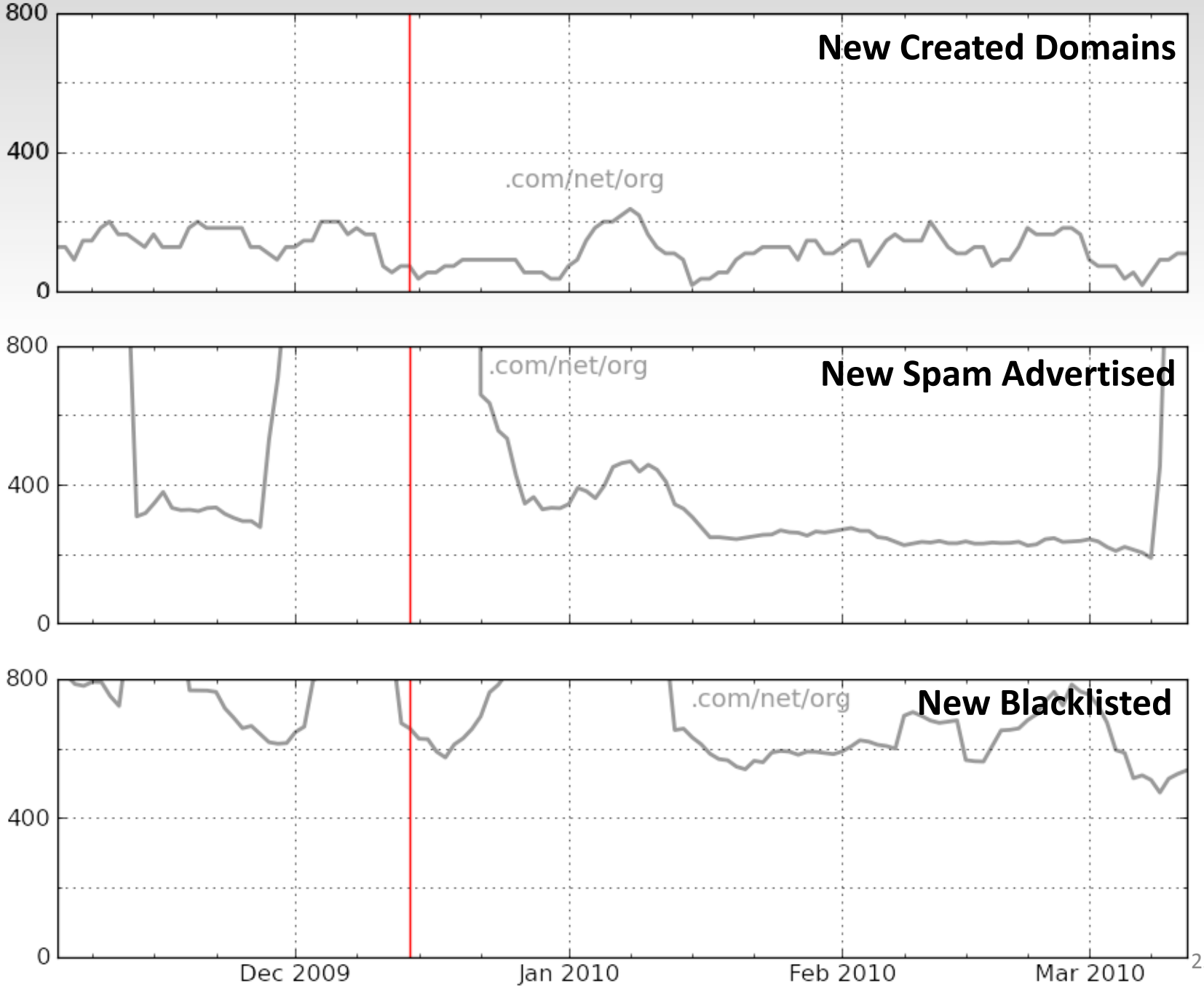
=

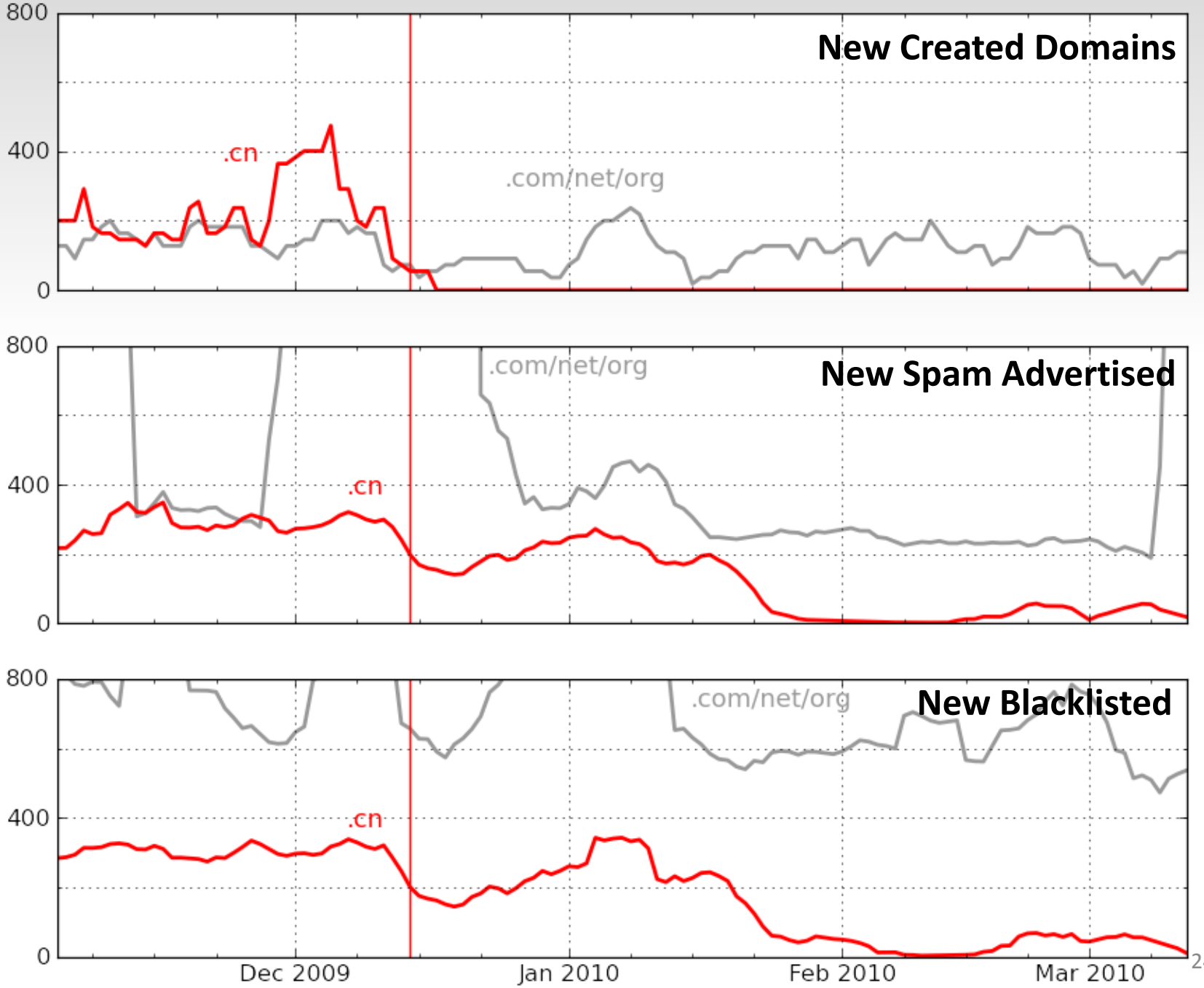
(15 cents)

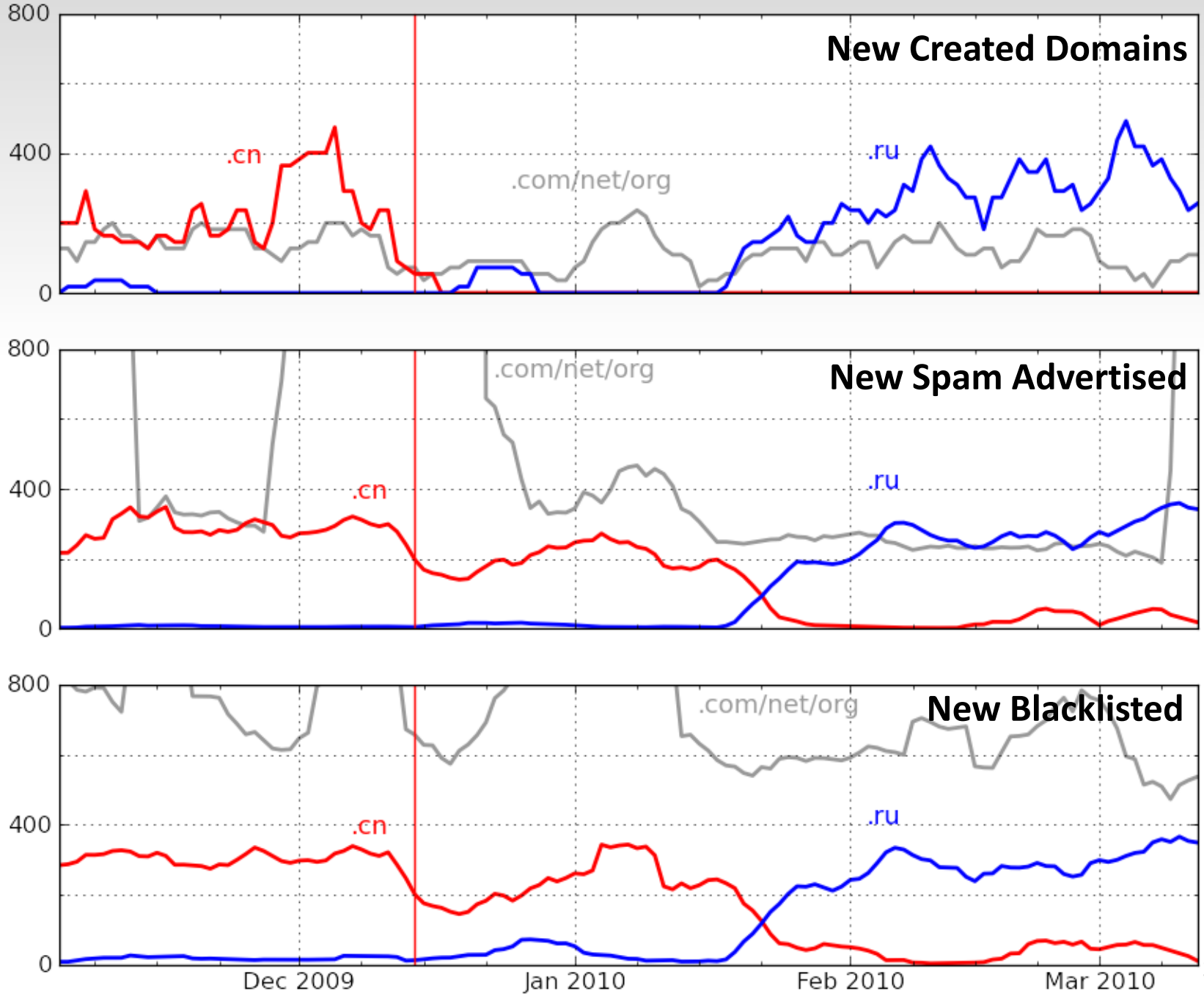
=

(10 dollars)

+6800%


New Created Domains
.com/net/org
800
400
0
New Spam Advertised
.com/net/org
800
400
0
New Blacklisted
.com/net/org
800
400
0
Dec 2009
Jan 2010
Feb 2010
Mar 2010


New Created Domains
800
400
0
.cn
.com/net/org
New Spam Advertised
800
400
0
.com/net/org
.cn
New Blacklisted
800
400
0
.com/net/org
.cn
Dec 2009
Jan 2010
Feb 2010
Mar 2010


New Created Domains
800
400
0
.cn
.com/net/org
.ru
New Spam Advertised
800
400
0
.com/net/org
.cn
.ru
New Blacklisted
800
400
0
.com/net/org
.cn
.ru
Dec 2009
Jan 2010
Feb 2010
Mar 2010

CNNIC Policy Change

- Spam domains are sensitive to prices
- Spammers abandoned .cn domains
- And start using .ru domains instead
- Quickly adapted the changes

September 21, 2010

September 21, 2010

LegitScript.com

enom

Internet Pharmacy
Verification & Enforcement

September 21, 2010 08:00 AM Eastern Daylight Time

eNom and LegitScript LLC Announce Agreement to Identify Customers Operating Illegal Online Pharmacies

SANTA MONICA, Calif.--(BUSINESS WIRE)--eNom, Inc., the world's largest ICANN accredited domain name wholesaler, and LegitScript LLC, an Internet pharmacy verification and monitoring service recognized by the National Association of Boards of Pharmacy, today announced an agreement by which LegitScript will assist eNom in identifying customers who are violating eNom's terms of service by operating online pharmacies in violation of U.S. state or federal law.

"As the largest domain name wholesaler, we take our role and responsibility very seriously. As such, it is our policy to cooperate with law enforcement agencies, and where we have evidence of illegal conduct from law enforcement or another trusted source, we take appropriate action, including terminating domain name registration services," said Taryn Naidu, senior vice president and general manager at eNom. "Our partnership with LegitScript provides us with a trustworthy source of information regarding the illegal sale of pharmaceutical drugs."

"LegitScript was created to fill a void in the monitoring and verification of the online pharmacy market, and our service has helped the investigative efforts of government agencies in the US and abroad"

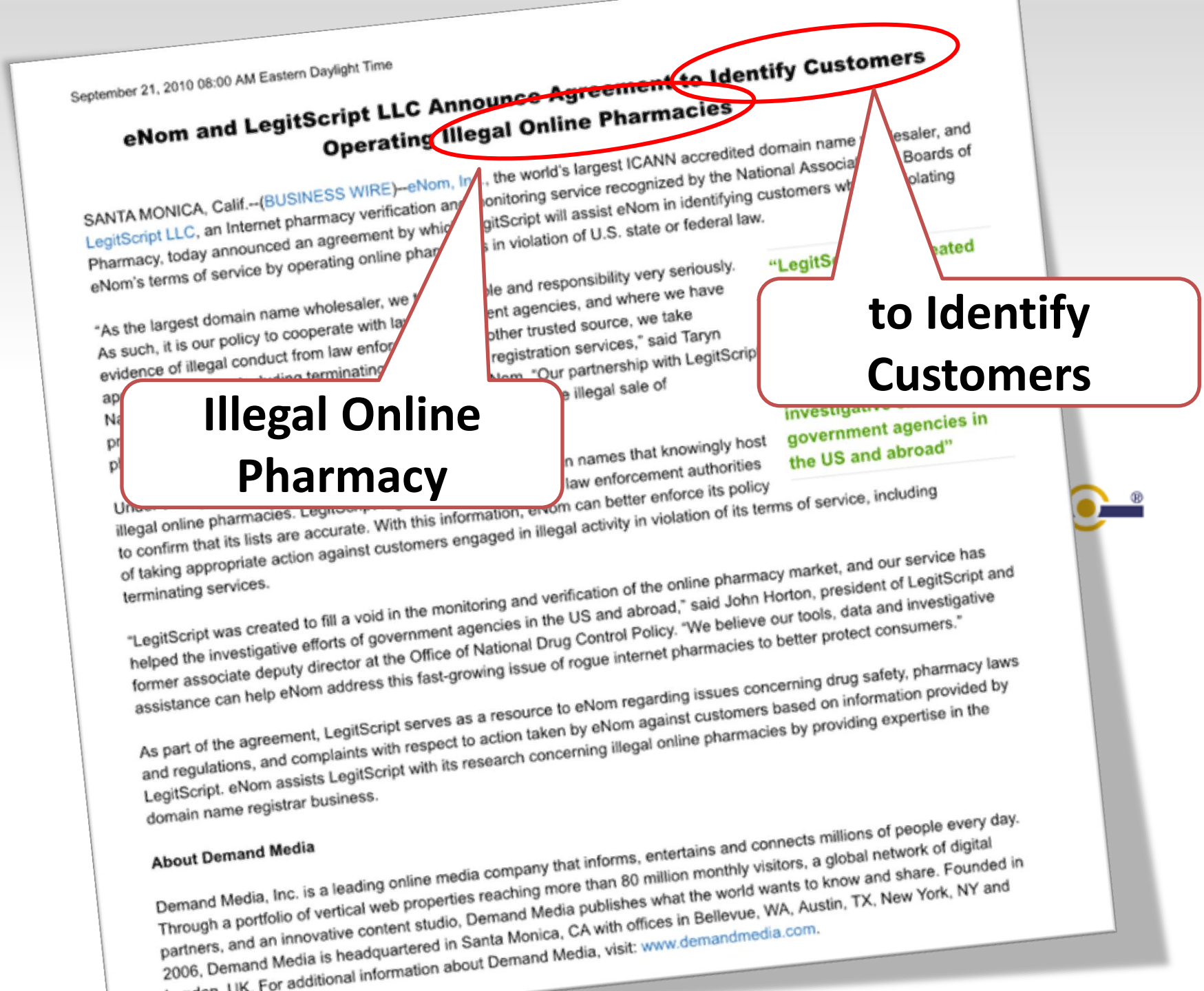
Under the agreement, LegitScript provides eNom a list of domain names that knowingly host illegal online pharmacies. LegitScript regularly coordinates with law enforcement authorities to confirm that its lists are accurate. With this information, eNom can better enforce its policy of taking appropriate action against customers engaged in illegal activity in violation of its terms of service, including terminating services.

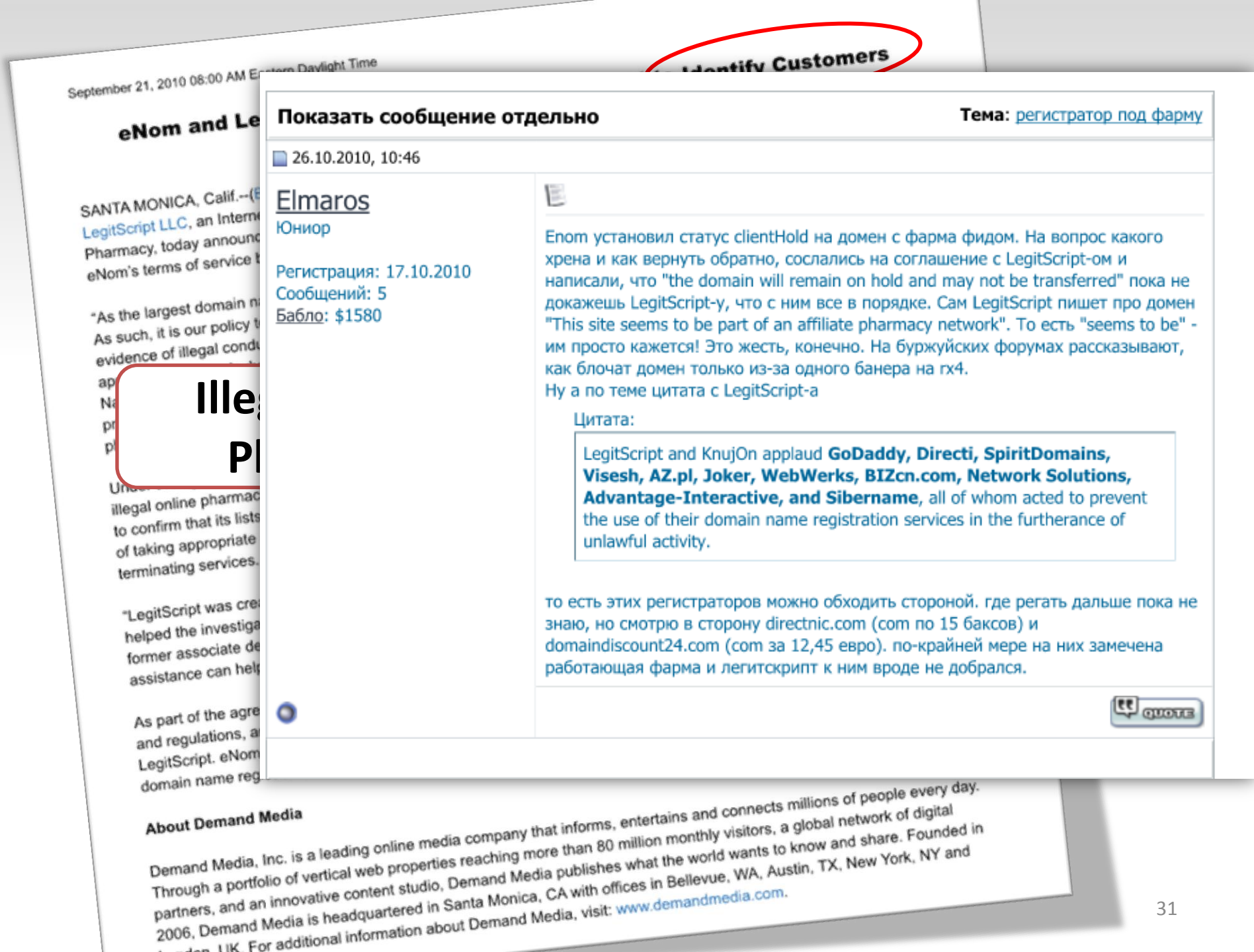
"LegitScript was created to fill a void in the monitoring and verification of the online pharmacy market, and our service has helped the investigative efforts of government agencies in the US and abroad," said John Horton, president of LegitScript and former associate deputy director at the Office of National Drug Control Policy. "We believe our tools, data and investigative assistance can help eNom address this fast-growing issue of rogue internet pharmacies to better protect consumers."

As part of the agreement, LegitScript serves as a resource to eNom regarding issues concerning drug safety, pharmacy laws and regulations, and complaints with respect to action taken by eNom against customers based on information provided by LegitScript. eNom assists LegitScript with its research concerning illegal online pharmacies by providing expertise in the domain name registrar business.

About Demand Media

Demand Media, Inc. is a leading online media company that informs, entertains and connects millions of people every day. Through a portfolio of vertical web properties reaching more than 80 million monthly visitors, a global network of digital partners, and an innovative content studio, Demand Media publishes what the world wants to know and share. Founded in 2006, Demand Media is headquartered in Santa Monica, CA with offices in Bellevue, WA, Austin, TX, New York, NY and [illegible], UK. For additional information about Demand Media, visit: www.demandmedia.com.


September 21, 2010 08:00 AM Eastern Daylight Time
eNom and LegitScript LLC Announce Agreement to Identify Customers Operating Illegal Online Pharmacies
SANTA MONICA, Calif.--(BUSINESS WIRE)--eNom, In
LegitScript LLC, an Internet pharmacy verification an
Pharmacy, today announced an agreement by whic
eNom's terms of service by operating online phar
"As the largest domain name wholesaler, we
As such, it is our policy to cooperate with la
evidence of illegal conduct from law enfor
illegal online pharmacies.
to confirm that its lists are accurate. With this information,
of taking appropriate action against customers engaged in illegal activity in violation of its terms of service, including
terminating services.
"LegitScript was created to fill a void in the monitoring and verification of the online pharmacy market, and our service has
helped the investigative efforts of government agencies in the US and abroad," said John Horton, president of LegitScript and
former associate deputy director at the Office of National Drug Control Policy. "We believe our tools, data and investigative
assistance can help eNom address this fast-growing issue of rogue internet pharmacies to better protect consumers."
As part of the agreement, LegitScript serves as a resource to eNom regarding issues concerning drug safety, pharmacy laws
and regulations, and complaints with respect to action taken by eNom against customers based on information provided by
LegitScript. eNom assists LegitScript with its research concerning illegal online pharmacies by providing expertise in the
domain name registrar business.
About Demand Media
Demand Media, Inc. is a leading online media company that informs, entertains and connects millions of people every day.
Through a portfolio of vertical web properties reaching more than 80 million monthly visitors, a global network of digital
partners, and an innovative content studio, Demand Media publishes what the world wants to know and share. Founded in
2006, Demand Media is headquartered in Santa Monica, CA with offices in Bellevue, WA, Austin, TX, New York, NY and
For additional information about Demand Media, visit: www.demandmedia.com.
Illegal Online Pharmacy
to Identify Customers



September 21, 2010 08:00 AM Eastern Daylight Time

eNom and Le

SANTA MONICA, Calif.--(B
LegitScript LLC, an Interne
Pharmacy, today announc
eNom's terms of service t

"As the largest domain n
As such, it is our policy t
evidence of illegal condu
ap
Na
pr
pl

Illeg
Pl

illegal online pharmac
to confirm that its lists
of taking appropriate
terminating services.

"LegitScript was cre
helped the investiga
former associate de
assistance can help

As part of the agre
and regulations, a
LegitScript. eNom
domain name reg

Identify Customers

About Demand Media

Demand Media, Inc. is a leading online media company that informs, entertains and connects millions of people every day. Through a portfolio of vertical web properties reaching more than 80 million monthly visitors, a global network of digital partners, and an innovative content studio, Demand Media publishes what the world wants to know and share. Founded in 2006, Demand Media is headquartered in Santa Monica, CA with offices in Bellevue, WA, Austin, TX, New York, NY and London, UK. For additional information about Demand Media, visit: www.demandmedia.com.

Показать сообщение отдельно **Тема:** регистратор под фарму

26.10.2010, 10:46

Elmaros
Юниор

Регистрация: 17.10.2010
Сообщений: 5
Бабло: $1580

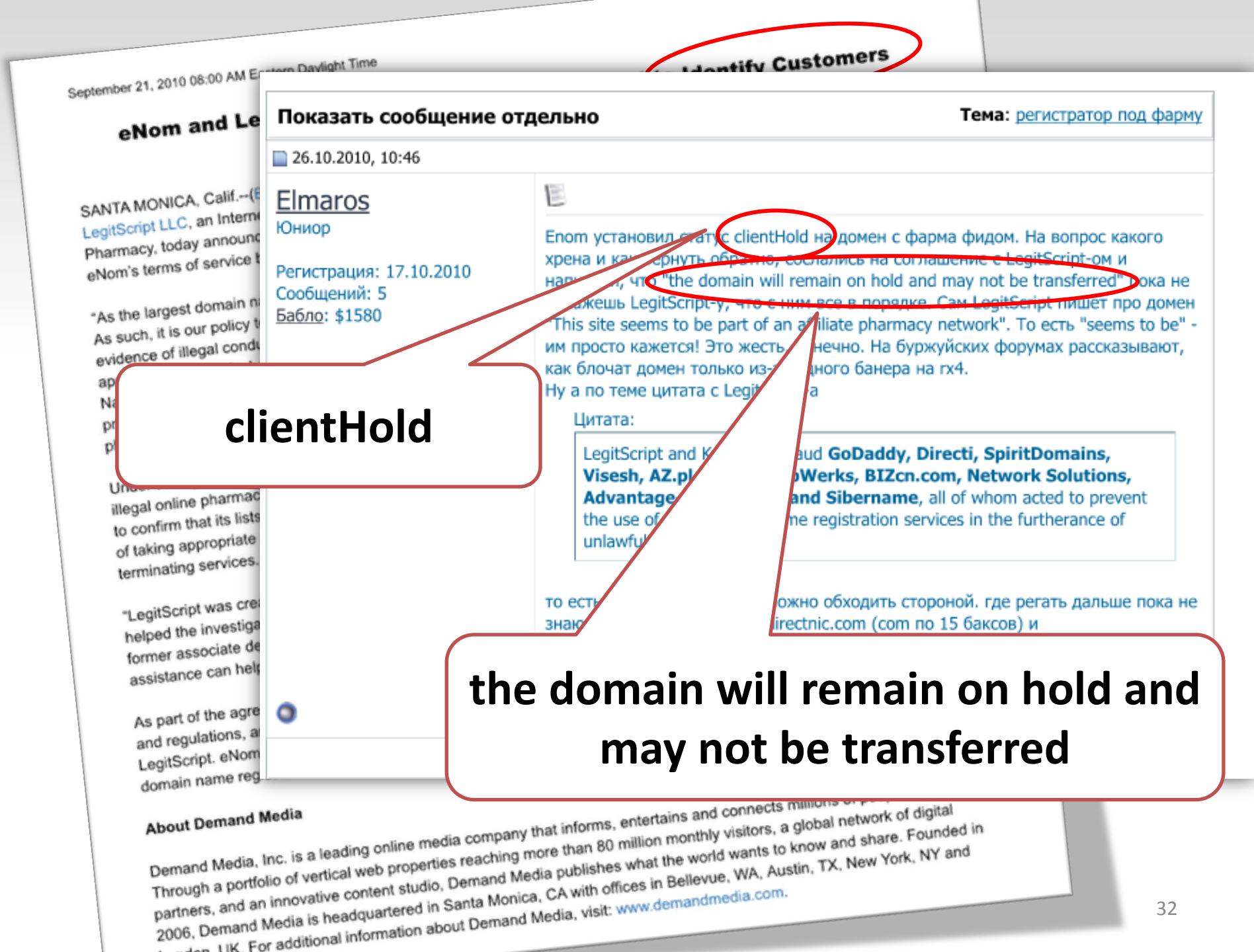
Enom установил статус clientHold на домен с фарма фидом. На вопрос какого хрена и как вернуть обратно, сослались на соглашение с LegitScript-ом и написали, что "the domain will remain on hold and may not be transferred" пока не докажешь LegitScript-у, что с ним все в порядке. Сам LegitScript пишет про домен "This site seems to be part of an affiliate pharmacy network". То есть "seems to be" - им просто кажется! Это жесть, конечно. На буржуйских форумах рассказывают, как блочат домен только из-за одного банера на гх4.
Ну а по теме цитата с LegitScript-а

Цитата:

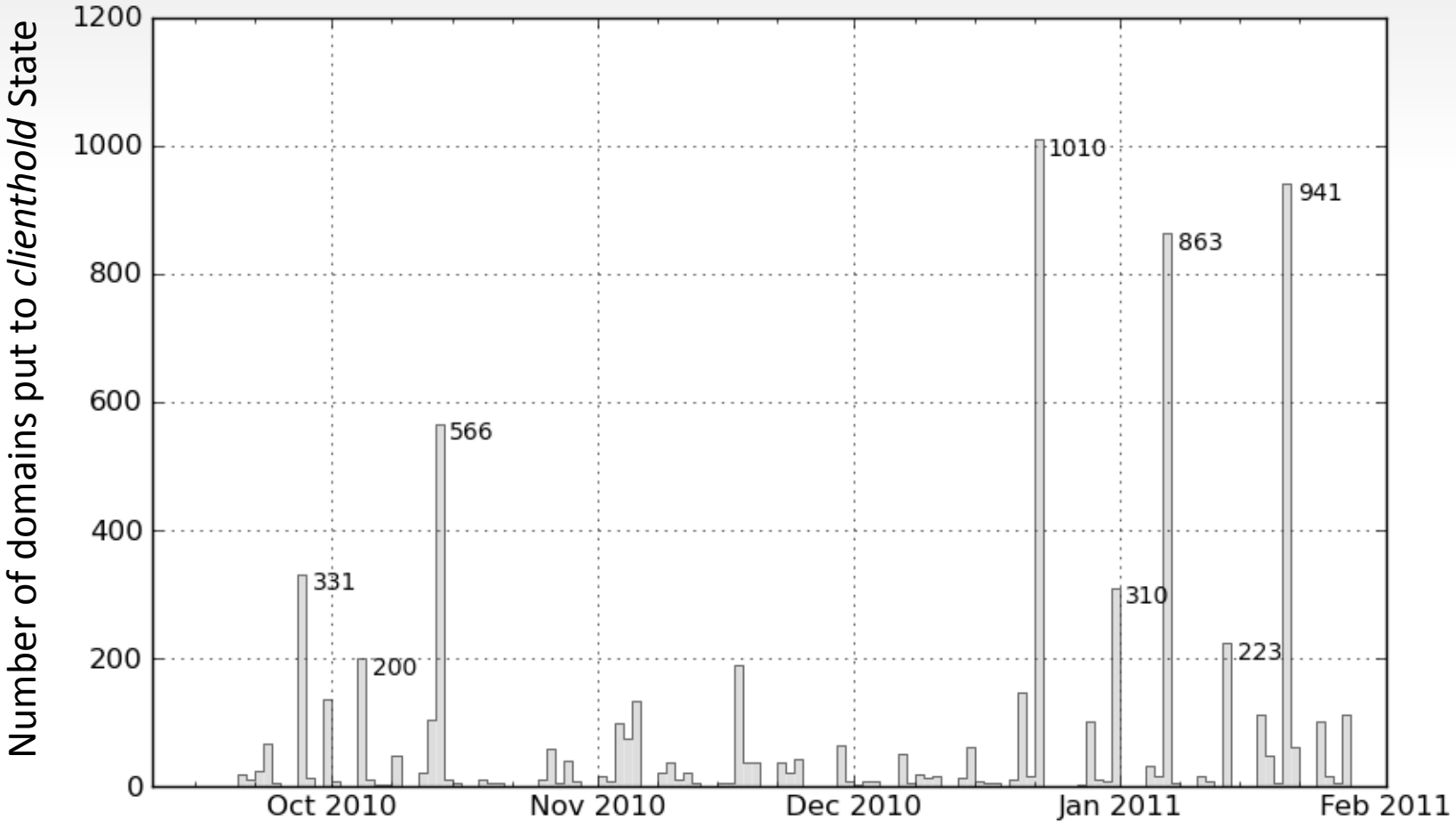
> LegitScript and KnujOn applaud **GoDaddy, Directi, SpiritDomains, Visesh, AZ.pl, Joker, WebWerks, BIZcn.com, Network Solutions, Advantage-Interactive, and Sibername**, all of whom acted to prevent the use of their domain name registration services in the furtherance of unlawful activity.

то есть этих регистраторов можно обходить стороной. где регать дальше пока не знаю, но смотрю в сторону directnic.com (com по 15 баксов) и domaindiscount24.com (com за 12,45 евро). по-крайней мере на них замечена работающая фарма и легитскрипт к ним вроде не добрался.

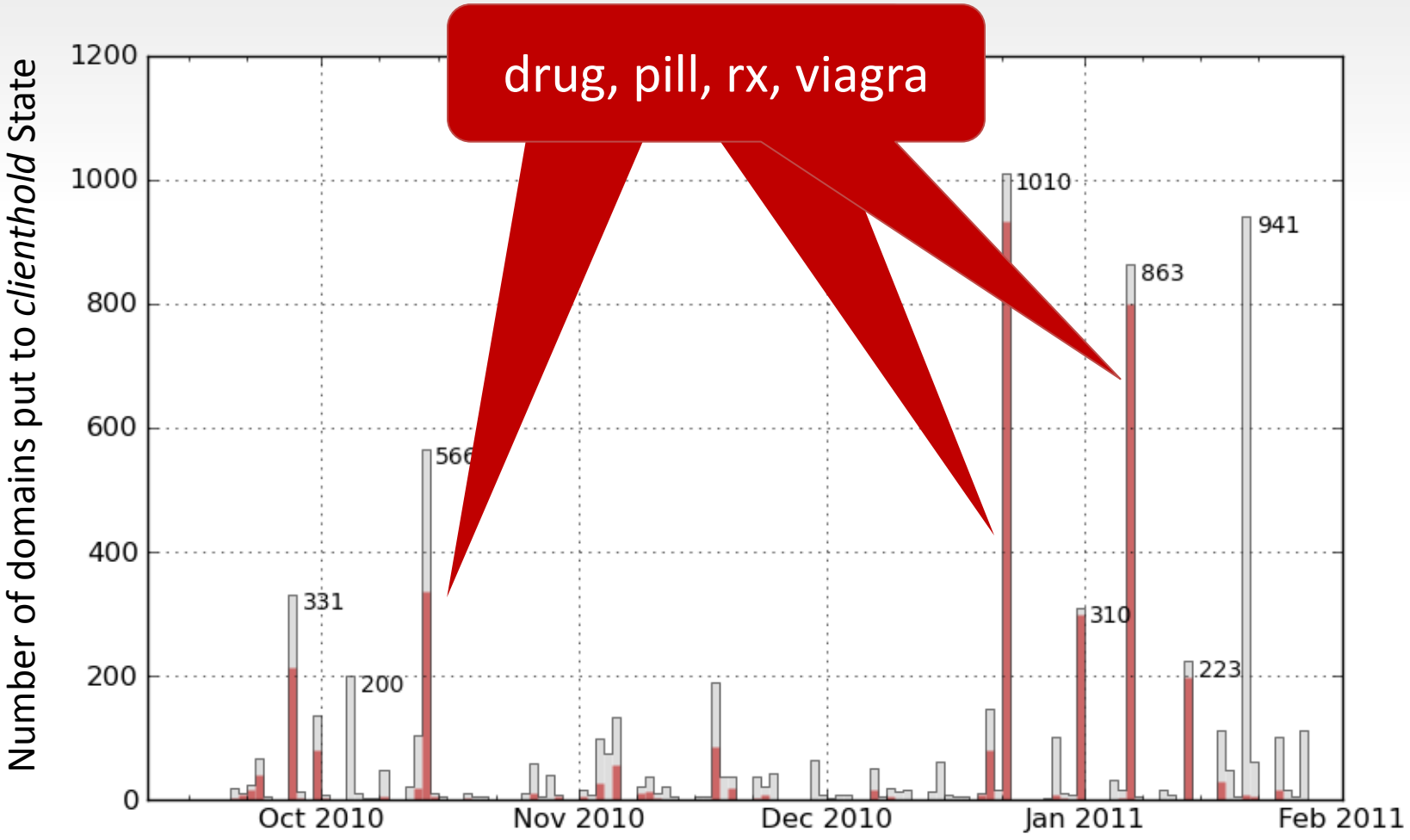
QUOTE


Показать сообщение отдельно
Тема: регистратор под фарму
26.10.2010, 10:46
Elmaros
Юниор
Регистрация: 17.10.2010
Сообщений: 5
Бабло: $1580
Enom установил статус clientHold на домен с фарма фидом. На вопрос какого
"the domain will remain on hold and may not be transferred"
This site seems to be part of an affiliate pharmacy network". То есть "seems to be" -
Цитата:
GoDaddy, Directi, SpiritDomains,
Visesh, AZ.pl
Advantage
and Sibername, all of whom acted to prevent
clientHold
the domain will remain on hold and may not be transferred
About Demand Media
Demand Media, Inc. is a leading online media company that informs, entertains and connects
Through a portfolio of vertical web properties reaching more than 80 million monthly visitors, a global network of digital
partners, and an innovative content studio, Demand Media publishes what the world wants to know and share. Founded in
2006, Demand Media is headquartered in Santa Monica, CA with offices in Bellevue, WA, Austin, TX, New York, NY and
www.demandmedia.com.

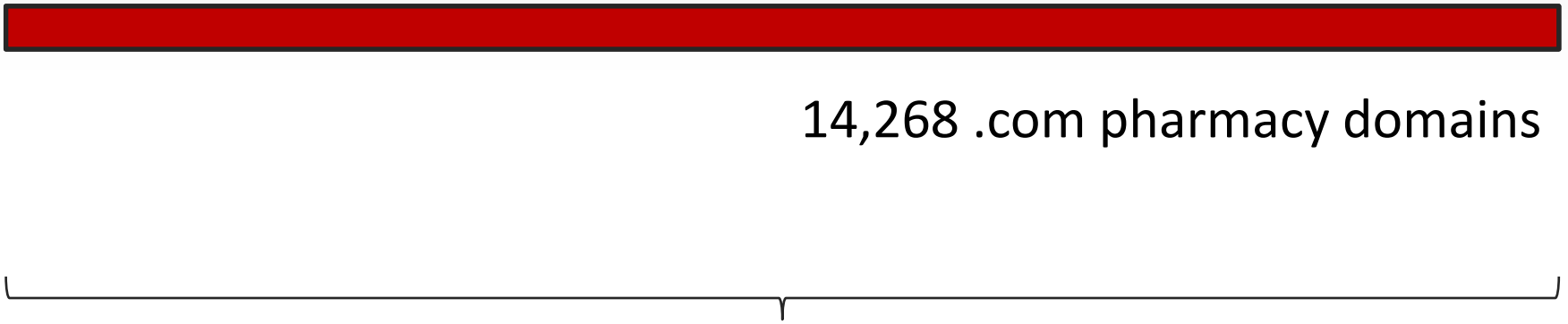
clientHeld eNom .com Domains



clientHeld eNom .com Domains



Global Impact



14,268 .com pharmacy domains

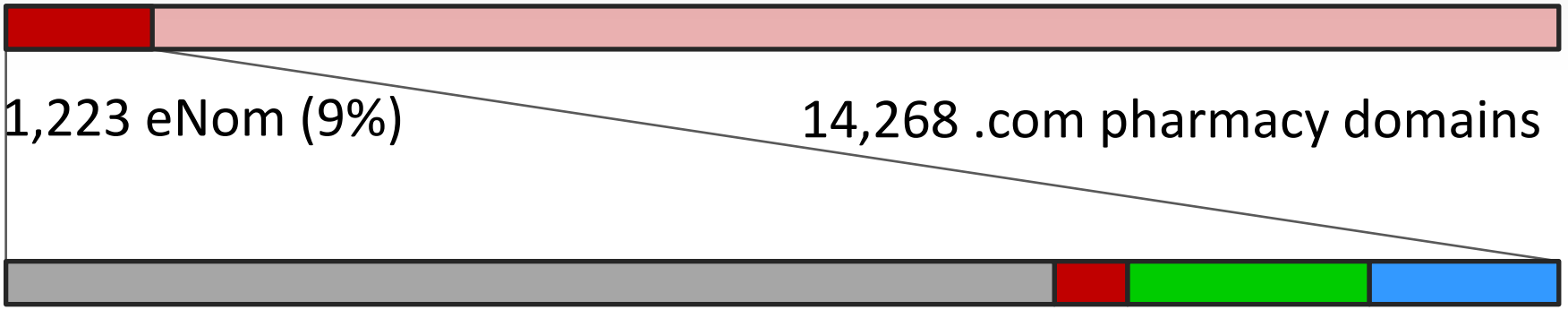
From our spam feeds, identified by webpage contents

Global Impact

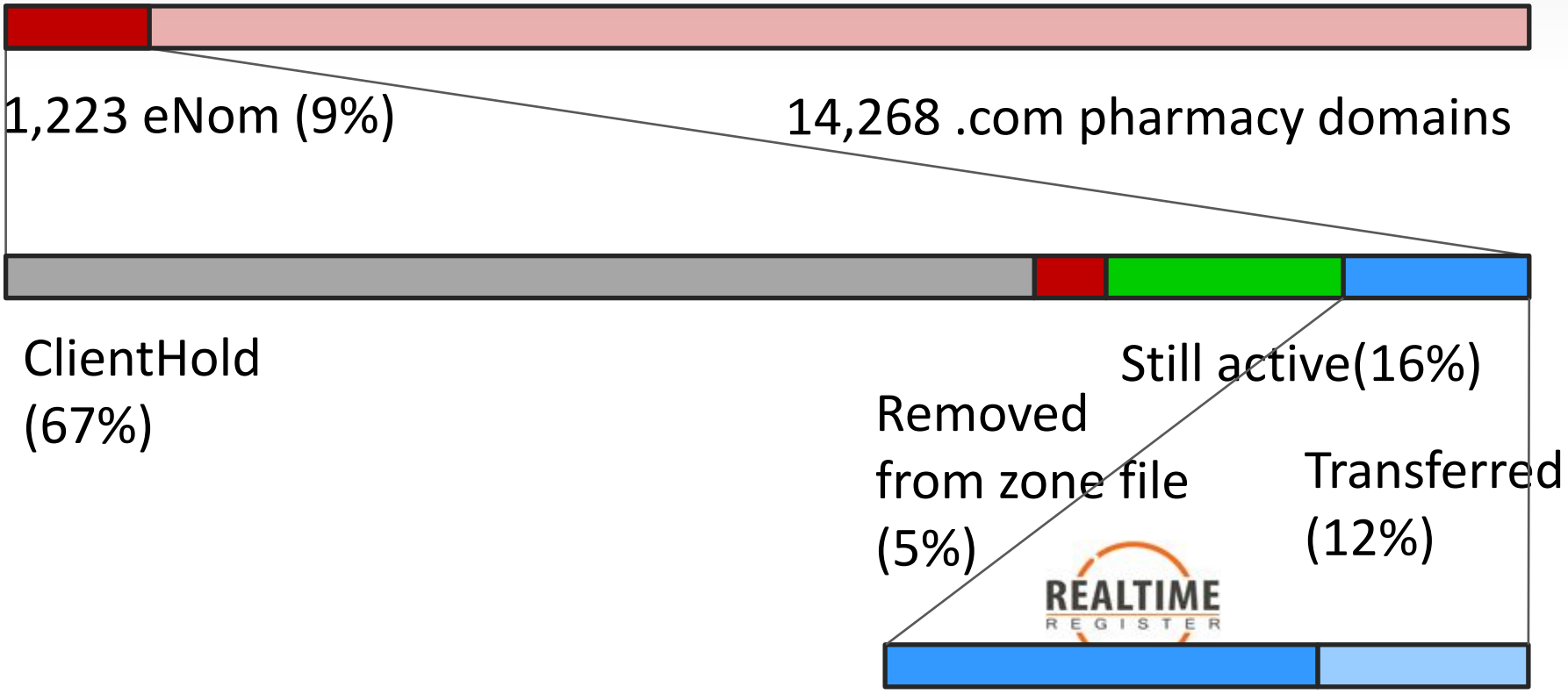
1,223 eNom (9%)

14,268 .com pharmacy domains

Global Impact



Global Impact



LegitScript - eNom Agreement

- Noticeable effects on eNom domains
  - 7000+ domains put to clientHold
  - Scammers transferred to other registrars
- The scale limits the global effects
  - 9% affected

Discussion: Defend at Registrar Level

- Economic way: increase the price (CNNIC)
  - Significant effect, but alternatives available
  - Affects all .cn users, including legal ones
- Social way: take down domains (LegitScript)
  - Similar to other takedowns,
    effects depends on scale and speed

Questions & Comments

Thank you