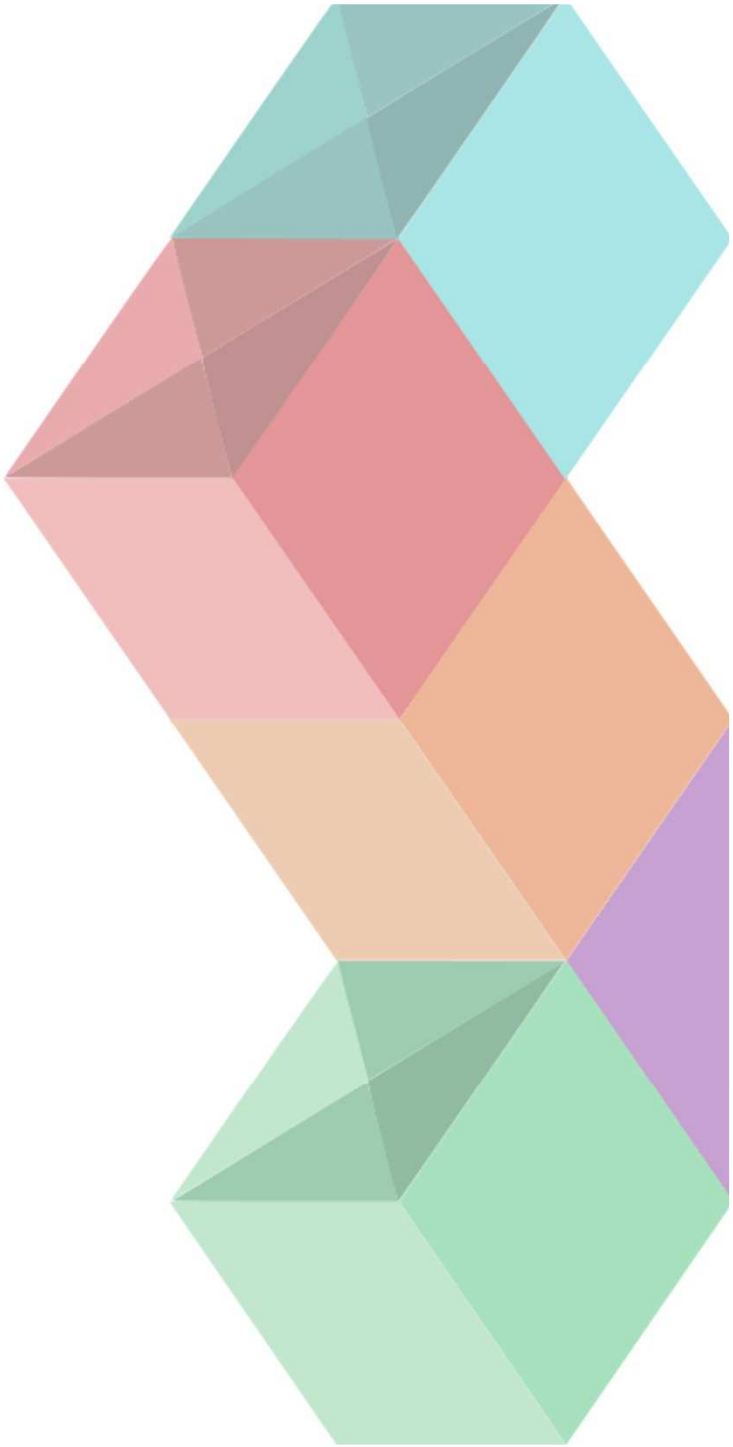
# Ustore

**Rodrigo Assad**
assad@usto.re

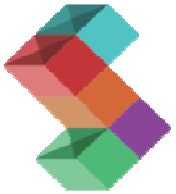
# novas tecnologias, legislação e a nova governança da Internet estão a favor do empreendedor



# O CAPITAL INTELECTUAL NACIONAL

33 colaboradores sendo:
7 PHDs
5 Mestres
2 Pos-Graduados
10 Graduados
Totalizando 33 Nerds

4 parceiros de negócios
5 anos de pesquisa
+ 15 anos de experiência no mercado
Investimento em P&D: 1 Patentes e 2 submetidas



Referência Governamental para Segurança Cibernética
5 falhas de segurança descobertas em ambientes de terceiros
Parceiro de confiança do EB
Experts nas linguagens principais linguagens : Java, Pyton, .Net

Compromisso com o meio-ambiente
Soluções desenvolvidas com foco em gestão para economia de energia e recursos computacionais


Não, obrigado!
Deus, vai me ajudar

TECNOLOGIA

06 de Junho de 2013 • 19h25 • atualizado em 06 de Junho de 2013 às 21h34

# Governo dos EUA acessaria dados do Facebook, Google e outros

13 Tweetar

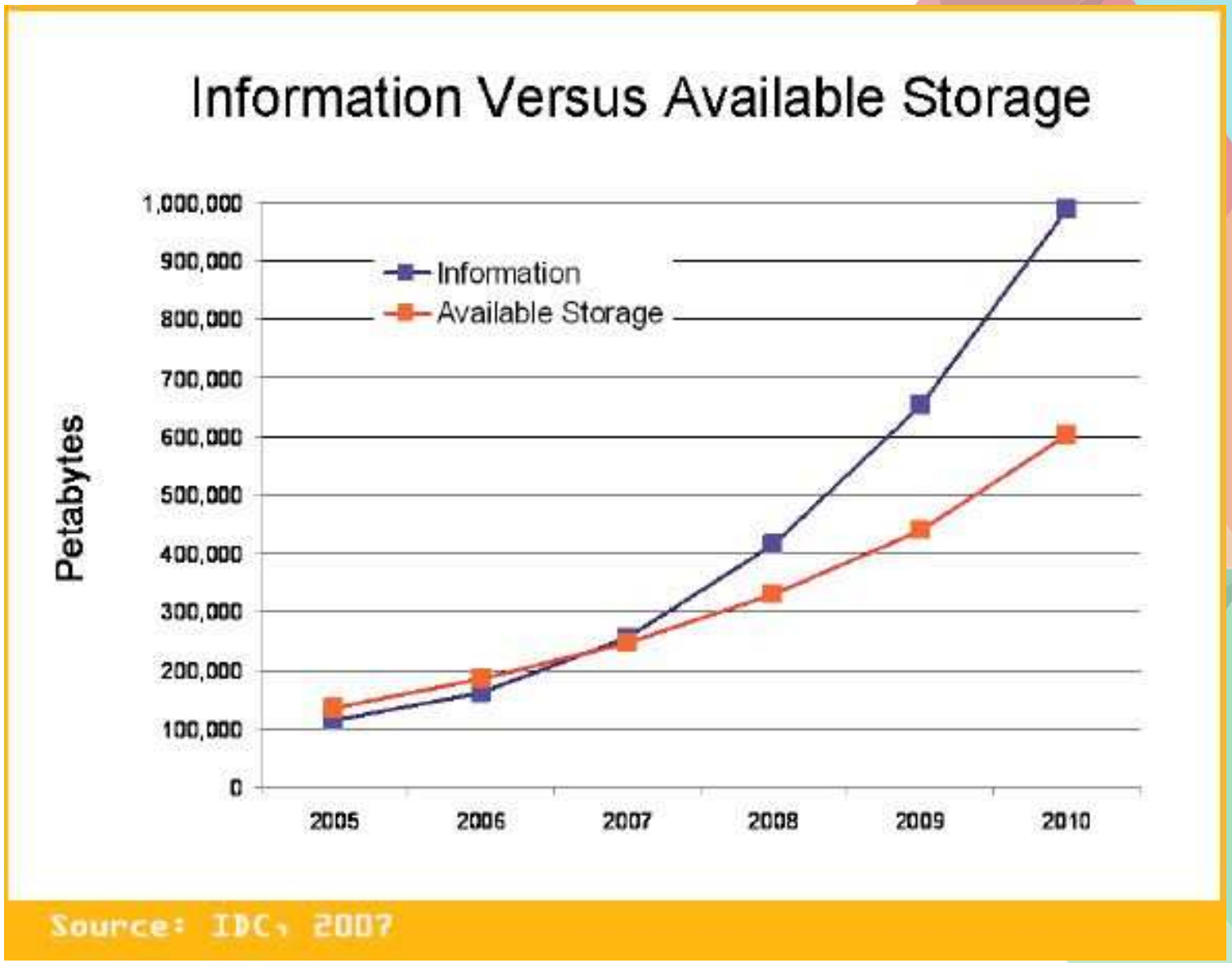
224 Curtir


O jornal britânico The Guardian publicou nesta quinta-feira que a agênci segurança nacional dos Estados Unidos teve ace aos dados de sites com Facebook, Google, Yaho outras empresas de tecnologia. Segundo a publicação, o acesso às informações fazem parte um programa batizado d PRISM, no qual os oficiais do governo americano coletam dados como histórico de navegação, conteúdo de e-mail, transferência de arquivos, histórico de chats e outros documentos virtuais

http://tecnologia.terra.com.br/governo-dos-eua-acessaria-dados-do-facebook-google-e-outros,f7e5c4179831f310VgnCLD2000000ec6eb0aRCRD.html


2001:
3.000.000.000.000
2011:
10 anos depois, foram
1.800.000.000.000.000.000.
000
[zetta] [exa] [peta] [tera] [giga] [mega] [kilo]

# Há como armazenar tanta informação?

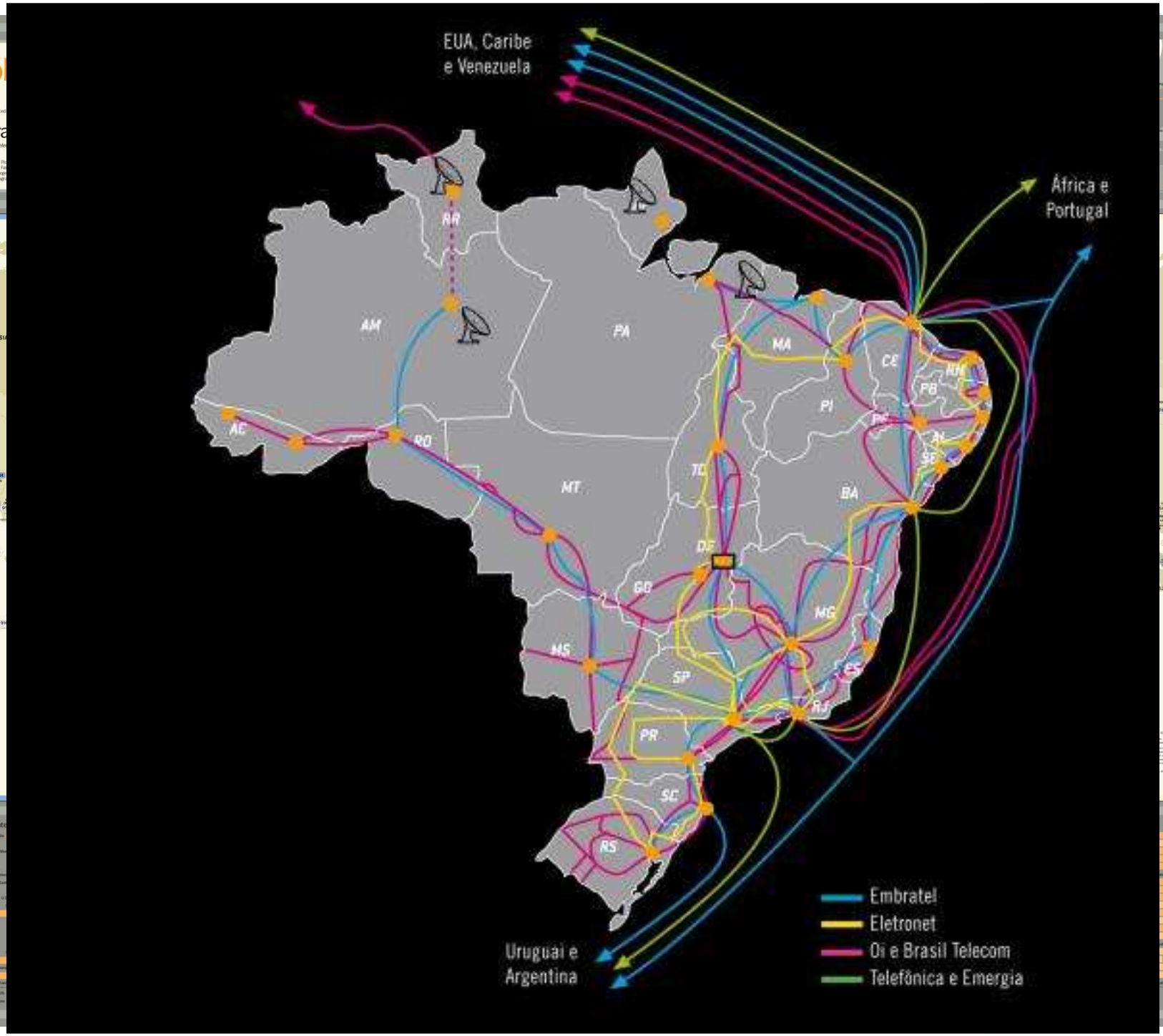


# Quais os impactos disso?

# Mudanças nas formas de relacionamento …


**“Computing Means CONNECTING.”**

Wade Roush (2006)


EUA, Caribe
e Venezuela
África e
Portugal
RR
AM
PA
MA
CE
RN
PB
PE
AL
SE
PI
AC
RO
MT
TO
BA
DF
GO
MG
MS
SP
ES
RJ
PR
SC
RS
Uruguai e
Argentina
Embratel
Eletronet
Oi e Brasil Telecom
Telefônica e Emergia

# O MERCADO DAS VULNERABILIDADES

| | |
|---|---|
| ADOBE READER | $5,000–$30,000 |
| MAC OSX | $20,000–$50,000 |
| ANDROID | $30,000–$60,000 |
| FLASH OR JAVA BROWSER PLUG-INS | $40,000–$100,000 |
| MICROSOFT WORD | $50,000–$100,000 |
| WINDOWS | $60,000–$120,000 |
| FIREFOX OR SAFARI | $60,000–$150,000 |
| CHROME OR INTERNET EXPLORER | $80,000–$200,000 |
| IOS | |

Os mais sofisticados estão no setor energético

Who's paying these pric
says the Grugq, who hir
the American and Europ
ethical concerns, but als
Russian mafia guarante
money," he says, explaining that he has no contacts in the Russian government. "Russia is flooded with criminals. They monetize exploits in the most brutal and mediocre way possible, and they cheat each other heavily."

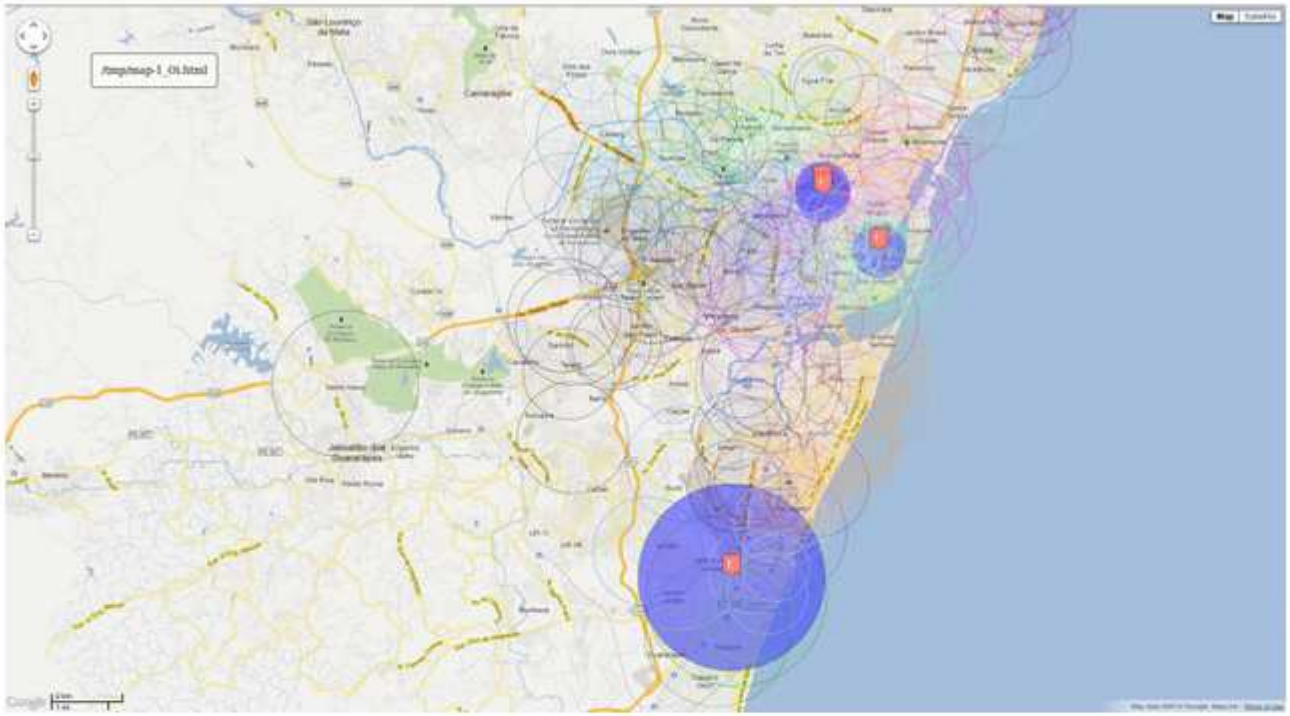
Even more importantly, the new market for security vulnerabilities results in a variety of government agencies around the world that have a strong interest in those vulnerabilities remaining unpatched. These range from law-enforcement agencies (like the FBI and the German police who are trying to build targeted Internet surveillance tools, to intelligence agencies like the NSA who are trying to build mass Internet surveillance tools, to military organizations who are trying to build cyber-weapons.

As for China, he says that the country has too many hackers who sell only to the Chinese government, pushing down prices. "The market is very depressed," he says. Other regions like the Middle East and the rest of Asia can't match Western prices either.

# Mobilidade

Depending on your HLR provider, the informa
illustrated in the example bellow.

```
5[redacted]7
[success] => 1
[status] => HLR_STATUS_OK
[number] => +5[redacted]
[imsi] => 72402
[mcc] => 724
[mnc] => 02
[msin] =>
[servingmsc] =>
[servinghlr] =>
[originalnetworkname] => Oi - TM
[originalnetworkprefix] => 8187
[originalcountryname] => Brazil
[originalcountrycode] => BR
[originalcountryprefix] => +55
[roamingcountryname] =>
[roamingcountrycode] =>
[roamingcountryprefix] =>
[roamingnetworkname] =>
[portednetworkname] => TIM Brasi
[isported] => 1
[iscorrect] => 1
[isroaming] =>
[charge] => 0.010
```



| Operator | Number of tested cells | Smallest | | Biggest | | Mean coverage radius |
|---|---|---|---|---|---|---|
| | | Coverage radius | CID | Coverage radius | CID | |
| Vivo | 369 | 772m | 22381 | 3476m | 21502 | 1469.37669377m |
| Oi | 290 | 774m | 30712 | 2652m | 33271 | 1350.62068966m |
| TIM | 241 | 779m | 811 | 2398m | 212 | 1223.94537815m |
| Claro BR | 208 | 771m | 10436 | 4258m | 40175 | 1188.98557692m |
| **Summary** | 1108 | 771m | 10436 | 4258m | 40175 | 1338.8032491m |

"Temos uma grande embaixada em Brasília e um consulado no Rio de Janeiro. A NSA opera nesses prédios. Antenas nas embaixadas podem interceptar sinais de micro-ondas e telefones celulares", diz James Bramford.

# Casos em empresas da APF

- Detectado um dispositivo Samsung Galaxy SIII com Android 4 fazendo parte da botnet Plankton.
- Houve mais de 4.000 comunicações entre este dispositivo e o servidor de C&C hospedado nos EUA nas duas semanas analisadas.

DeviceHostName = [redacted] | DeviceRiskConfidenceLevel = 3 | EventCategory = Callback |
EventID = 100119 | EventName = SECURITY_RISK_DETECTION | FinalAction = Unblocked | InterestedIP = 10.1.5.94 |
LogID = e6217a40-cf16-[redacted]-000c2918e7c5 | MalwareType = Malware | PeerCountry = United States | PeerIP = 217.65.36.4 |
PeerLocation = United States | ProductComponent = NCIE | ProductName = Deep Discovery | ProductVersion = 3.2.1028 |
ProtocolGroup = HTTP |
RequestClientAgent = Mozilla/5.0 (Linux; U; Android 4.1.2; pt-br; GT-I9300 Build/JZO54K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
| RequestURL = http://www.[redacted]/protocol/commands | RuleID = 541 |
RuleName = PLANKTON (Android) HTTP request - Class 1 | Severity = 8 | Sou[redacted]
SourceIP = 10.1.5.94 | SourceMAC = [redacted] | SourcePort = 42780

## Plankton Android Trojan found in 10 apps on Android Market

Posted on 09.06.2011

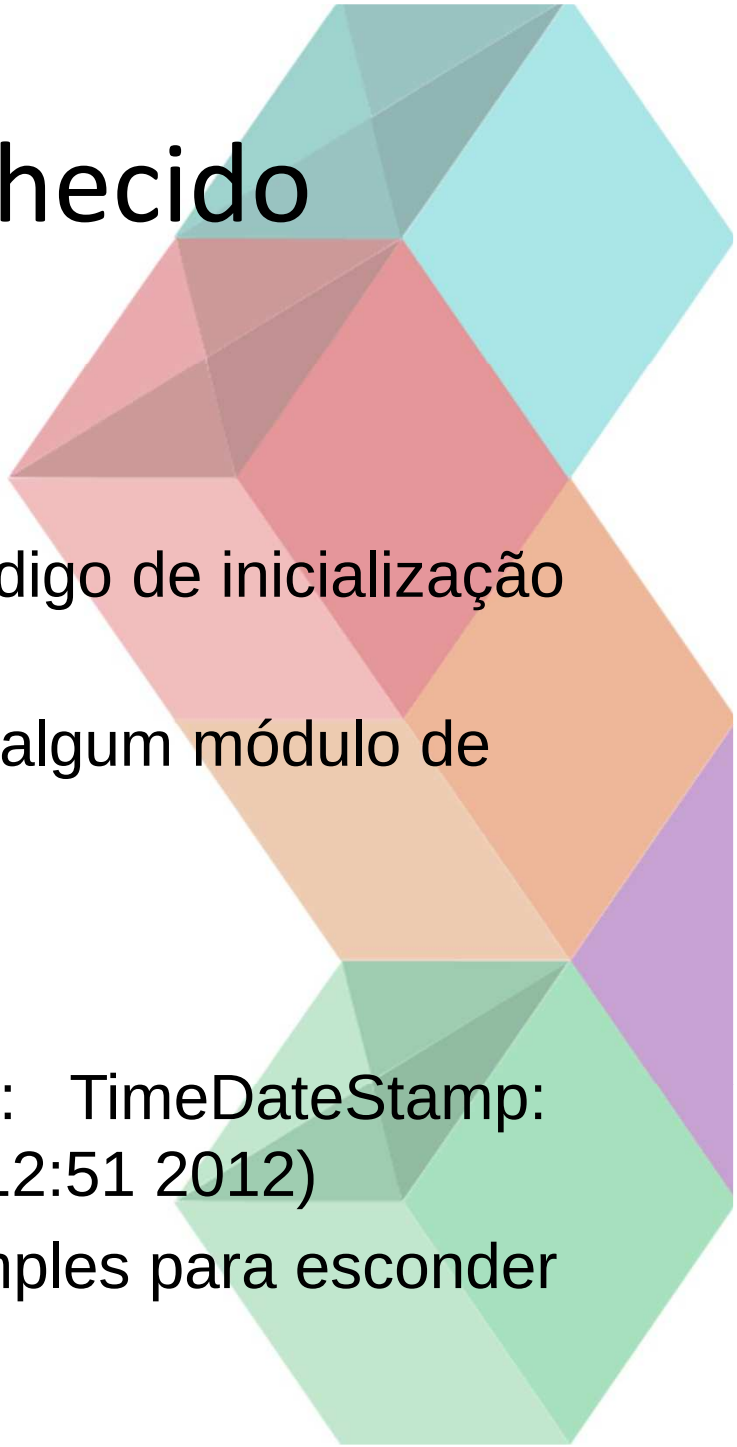
BOOKMARK

Ten more applications have been pulled from the Google's official Android Market following a notification that they contained a new kind of Android malware.

The malware was discovered by Xuxian Jiang, an assistant professor at the NC State University,

# Artefato desconhecido

- Detalhes técnicos:
  - Possui cerca de 100 Kbytes
  - Não contém qualquer tipo de código de inicialização automática
  - Possivelmente é utilizado como algum módulo de outro(s) software(s)
  - Não contém ícone
  - Não é compactado
  - Data da compilação do malware: TimeDateStamp: 0x4FAA5F43 (Wed May 09 12:12:51 2012)
  - Possui uma criptografia bem simples para esconder strings



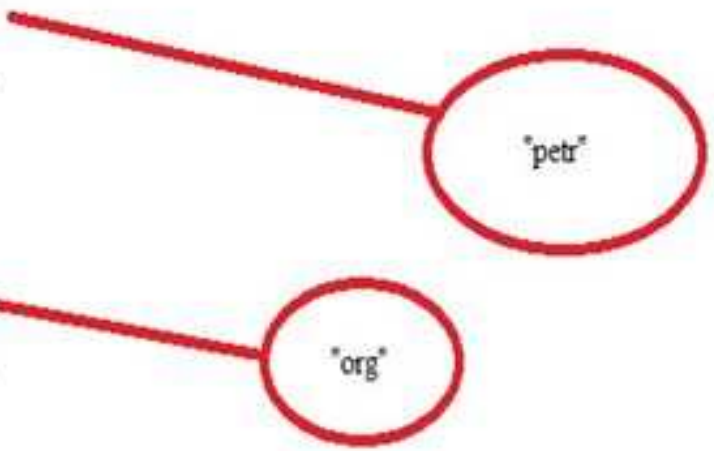
# Artefato desconhecido

- Ao iniciar, o malware tenta ler o conteúdo das variáveis de ambiente: USERDOMAIN e LOGONSERVER, para tentar obter o nome do domínio ou workgroup:

```
stosw
push    1000h           ; nSize
push    ecx             ; lpDst
push    offset Src      ; "%USERDOMAIN%"
xor     bl, bl
stosb
call    esi ; ExpandEnvironmentStringsA
```

- Em seguida é feita uma checagem por um dos seguintes textos: petr, org, gov ou br

```
push    offset aOdsq    ; "odsq"
call    sub_401A50
push    eax             ; SubStr
push    esi             ; Str
call    _strstr
add     esp, 10h
test    eax, eax
jnz     short loc_401499
push    offset aNqf     ; "nqf"
call    sub_401A50
push    eax             ; SubStr
push    esi             ; Str
call    _strstr
```



# Artefato desconhecido

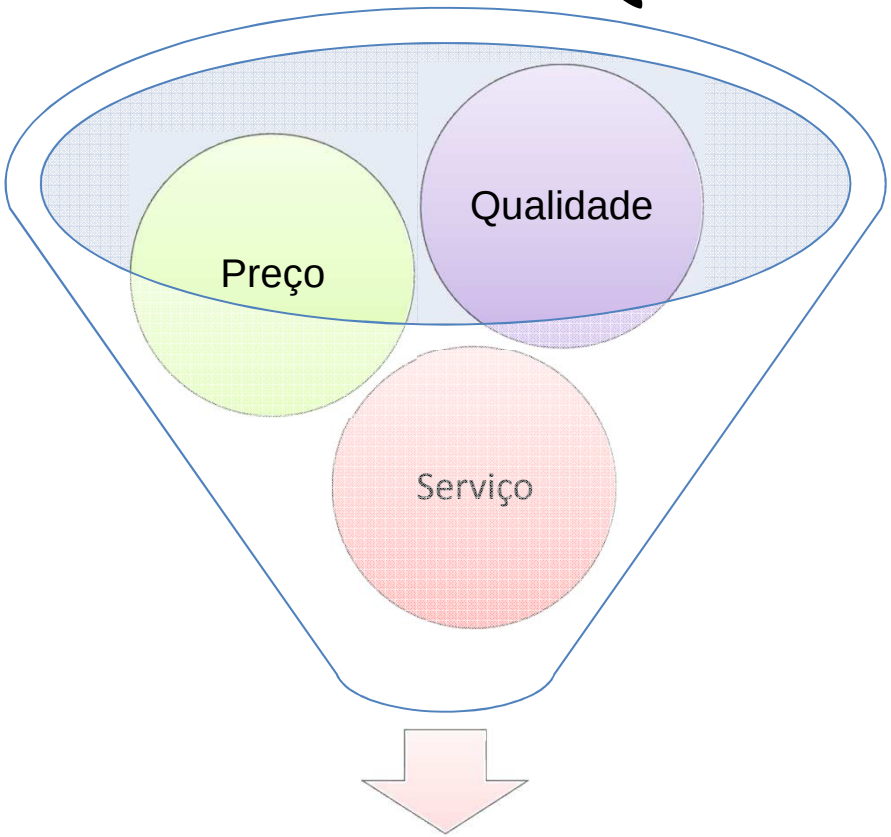
- Caso encontre nomes do tipo GOVerno, ORGanizacao, PETRoleo, PETRobras, BRasil, ele verifica as unidades de disco de C: ate Z: em todas as pastas e subpastas, por arquivos das seguintes máscaras: *.doc*, *.ppt*, *.xls*, *pass*.*, *senha*.*

```
mov     ax, word_415174
mov     cl, byte_415176
mov     word ptr [esp+1008h+FileName], ax
mov     [esp+1008h+var_FFE], cl
mov     ecx, 3FFh
xor     eax, eax
lea     edi, [esp+1008h+var_FFD]
push    offset aCnb     ; ")-cnb)"
```


- Se algum arquivo for encontrado, ele faz uma copia o arquivo para uma extensao .txt e envia para o seguinte email: NIASC@nsa.gov via porta 587

```
lea     ecx, [ebp+var_12C]
push    ebx             ; char
push    esi             ; Str
push    eax             ; int
call    sub_4040B0
push    offset aMh@rb?mrFnu ; "MH@RB?mr`-Fnu"
mov     [ebp+var_1C], ebx
```

# O QUE FAZER?




TCO

Prodest
Tecnologia da Informação

Ustore

# LEGISLAÇÃO

- Lei Federal 4.150 de 1962
- Lei 8.666/93
- Estratégia Nacional de Defesa
- Lei no 10.176, de 11 de janeiro de 2001.
- Norma Complementar 14, de 30 de Janeiro de 2012
- Decreto nº 3.505, de 13 de junho de 2000.
- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação.
- Instrução Normativa GSI Nº 1, de 13 de junho de 2008, e respectivas Normas Complementares.
- Lei da Inovação
- Decreto Nº 8.135, de 4 de novembro de 2013 da presidência da república
- Bem como consiste de peça fundamental de suporte aos procedimentos definidos nos acórdãos do TCU que versão sobre segurança da informação e sua propriedade.
  - 1603/2008 - ac-1603-32/08-p : levantamento de auditoria. Situação da Governança de Tecnologia da Informação - TI na Administração Pública Federal. Ausência de planejamento estratégico institucional. Deficiência na estrutura de pessoal. Tratamento inadequado à confidencialidade, integridade e disponibilidade das informações. Recomendações.
  - 019.230/2007-2: fiscalização de orientação centralizada. Tema de maior significância "Terceirização na Administração Pública Federal". Subtema "Terceirização em TI". Execução descentralizada de auditorias. Relatório de consolidação de informações obtidas nas auditorias. Falhas diversas detectadas. Determinações. Recomendações.
- Marco Civil da Internet

**A PRESIDENTA DA REPÚBLICA**, no uso da atribuição que lhe confere o art. 84, **caput**, inciso IV, da Constituição, e tendo em vista o disposto no art. 24, **caput**, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, ouvido o Conselho de Defesa Nacional,

**D E C R E T A :**

Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.

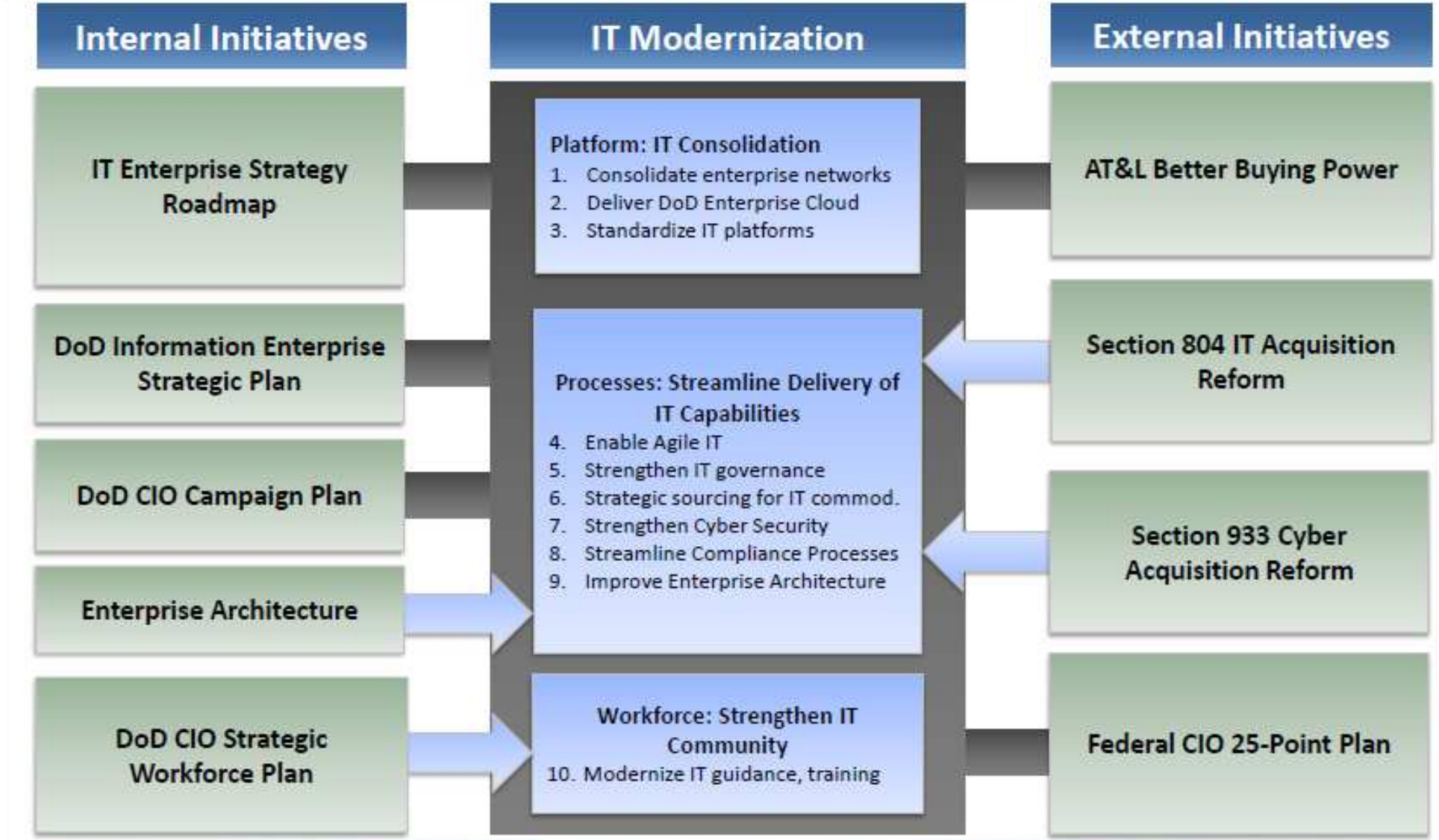
§ 1º O disposto no **caput** não se aplica às comunicações realizadas através de serviço móvel pessoal e serviço telefônico fixo comutado.

§ 2º Os órgãos e entidades da União a que se refere o **caput** deverão adotar os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da administração pública federal.

§ 3º Os programas e equipamentos destinados às atividades de que trata o **caput** deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.

§ 4º O armazenamento e a recuperação de dados a que se refere o **caput** deverá ser realizada em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal.

# Alignment with Other Initiatives



# DOD IT MODERNIZATION

## BENEFITS OF SUCCESSFUL IT MODERNIZATION

- Increase Mission Effectiveness
- Strengthen Cyber Security
- Improve Outcomes of IT Acquisition
- Faster Capability Deliveries
- Improve Interoperability
- Save Billions Through Cost Efficiencies

## CONSOLIDATE INFRASTRUCTURE

### 1. Consolidate Enterprise Networks

- Consolidate data centers and network operations
- Optimize to a joint enterprise architecture with secure access

### 2. Deliver DoD Enterprise Cloud

- Develop and execute a strategy and standards for a secure DoD cloud environment.
- Leverage commercial clouds that meet cyber security requirements

### 3. Standardize IT Platforms

- Minimize program-unique platforms
- Drive DoD use of standard platforms
- Design platforms that ensure a secure cyber environment

## STREAMLINE PROCESSES

### 4. Enable Agile IT

- Lead the development of an Agile IT development methodology
- Provide Guidance to DoD On Agile IT Best Practices

### 5. Strengthen IT Governance

- Restructure IT governance boards for enterprise view
- Improve DoD IT decisions, strategies, investments
- Streamline compliance processes

### 6. Leverage Strategic Sourcing for IT Commodities

- Implement an enterprise approach for the procurement of common IT H/W & S/W
- Establish a DoD Commodity Council

### 7. Strengthen Cybersecurity

- Develop enterprise cyber situational awareness including authentication
- Leverage automated tools and continual assessments
- Streamline certification and reinforce reciprocity

### 8. Strengthen IT Investments

- Obtain transparency of IT investments
- Align IT Investments to DoD strategies
- Review performance of major investments

### 9. Improve Enterprise Architecture Effectiveness

- Transition document based process to decision support model
- Develop EA Implementation Plan and Instruction

## STRENGTHEN WORKFORCE

### 10. Modernize IT Guidance and Training

- Provide guidance to DoD on adoption of Agile IT best practices
- Leverage ongoing workforce initiatives
- Develop a robust IT acquisition community

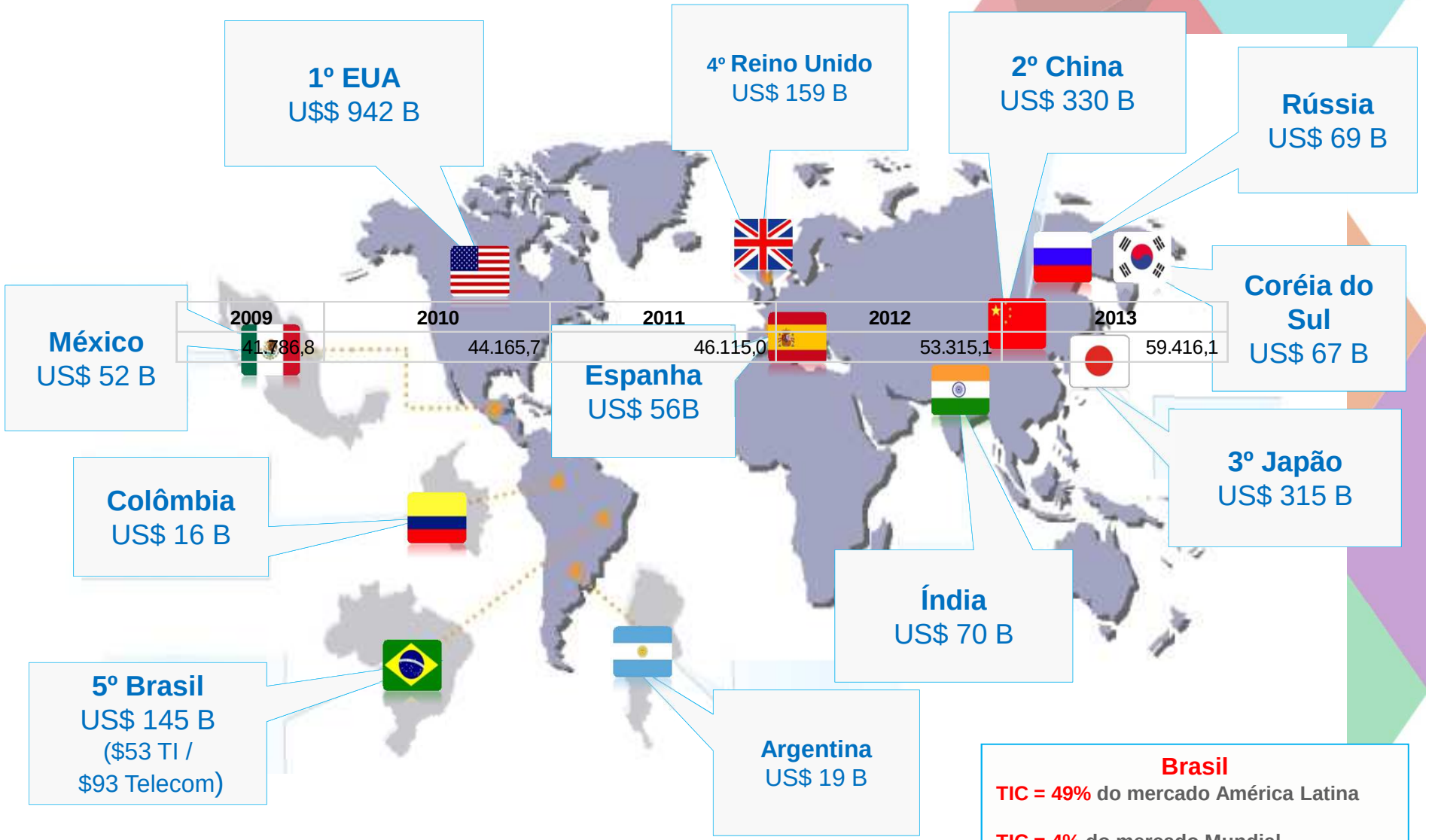
# MERCADO MUNDIAL DE TI & TELECOM 2012

## WW – Mercado de TI & Telecom – Receitas 2012 = US$ 3.6 T


Fonte: IDC Worldwide Black Book, Q4 2012

# Receitas de TI e Telecom em 2013

## Mercado Mundial de TI e Telecom em 2013 = US$ 3,5 T




**Brasil**

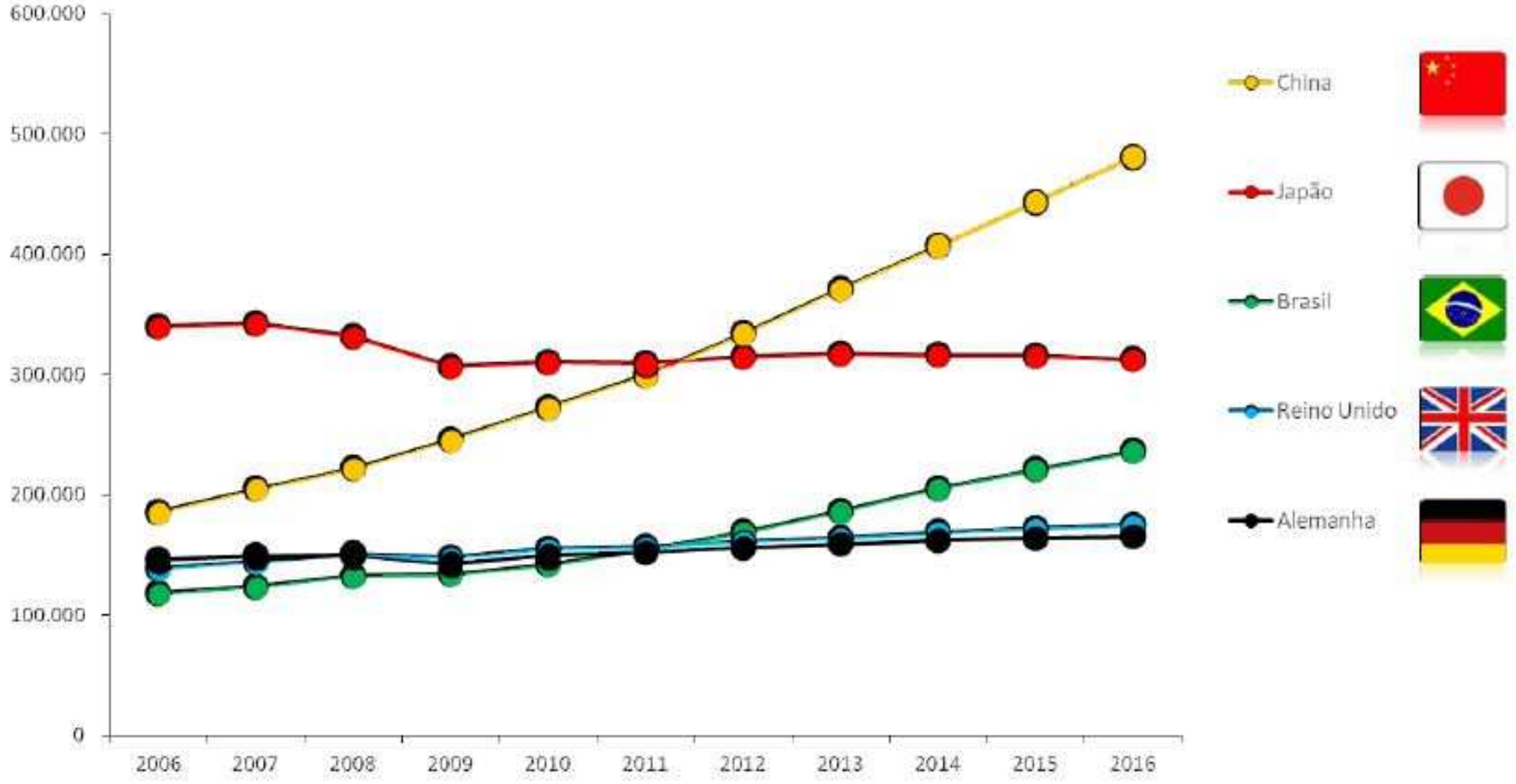
**TIC = 49%** do mercado América Latina

**TIC = 4%** do mercado Mundial

**Fonte: IDC Worldwide Black Book, 2013**

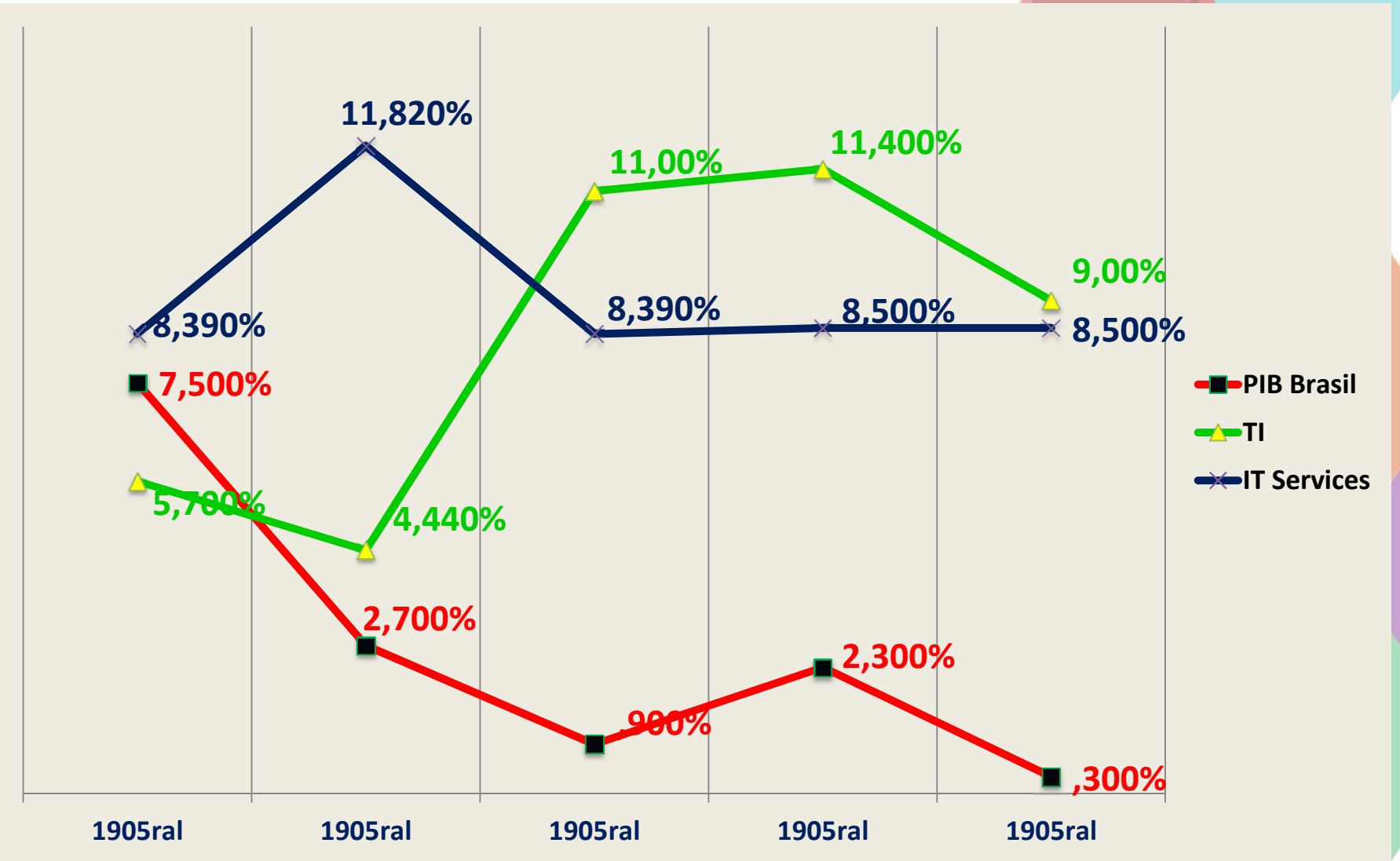
# O BRASIL ENTRE OS MAIORES MERCADOS DE TIC

## Ranking dos Maiores Mercados de TIC (2006-2016), exceto EUA

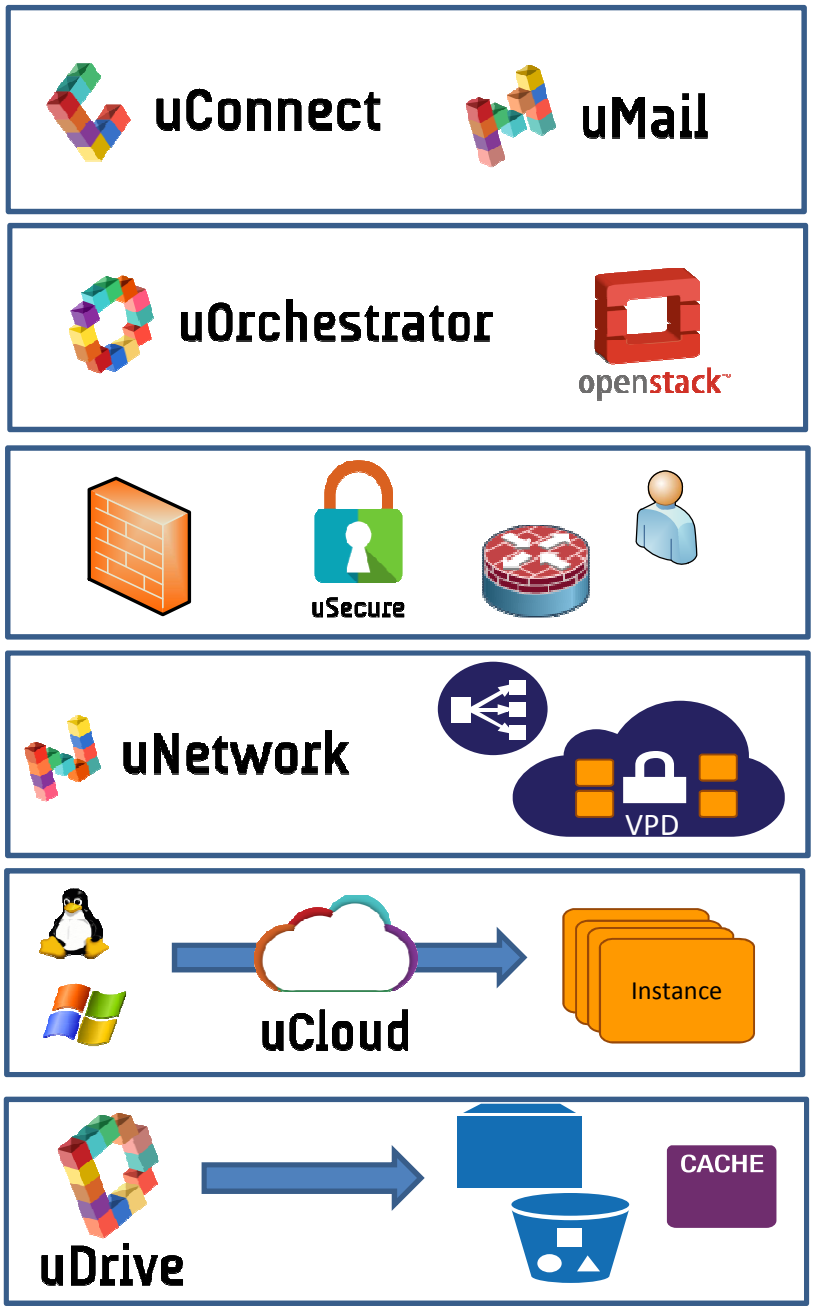



Fonte: IDC Worldwide Black Book, Q4 2012

# PIB / IT / IT Services




Fonte: IDC IT Services Tracker 1H2014




Plataforma de mail, agenda, calendário, chat e voz integrada

Plataforma aberta, multivendor, escálavel, pronta para interconectar com aplicações webservice,

Data Ceter As as Service DaaS

Gestão, Orquestração e provisionamento dos recursos de segurança de rede, inspecionando e garantindo segurança em Cloud

Gestão, Orquestração e provisionamento dos recursos de rede

Gestão, Mensuração, Orquestração e provisionamento de servidores e data centers

Gestão, orquestração, replicação e armazenamento de dados desestruturados, banco de dados, indexação para Big data,

# Servidores/Performance

**/dev/sda: SATA**
**Timing buffered disk reads: 476 MB in 3.00 seconds = 158.48 MB/sec**
**/dev/sdc: SSD**
**Timing buffered disk reads: 1288 MB in 3.00 seconds = 428.88 MB/sec**
**/dev/fioa: FUSION IO**
**Timing buffered disk reads: 2848 MB in 3.00 seconds = 949.06 MB/sec**

**1 Gbps e 190 IOPS**

EB-DRIVER

- Base de Dados MySQL
  Base de Dados
- Hibernate
- Jetty
- JXTA
- H2
- Spring
- Lucene
- J-SCSI
- ISE


Visite nosso site:
www.usto.re

# CONTATO

**Rodrigo Assad**

**assad@usto.re**