

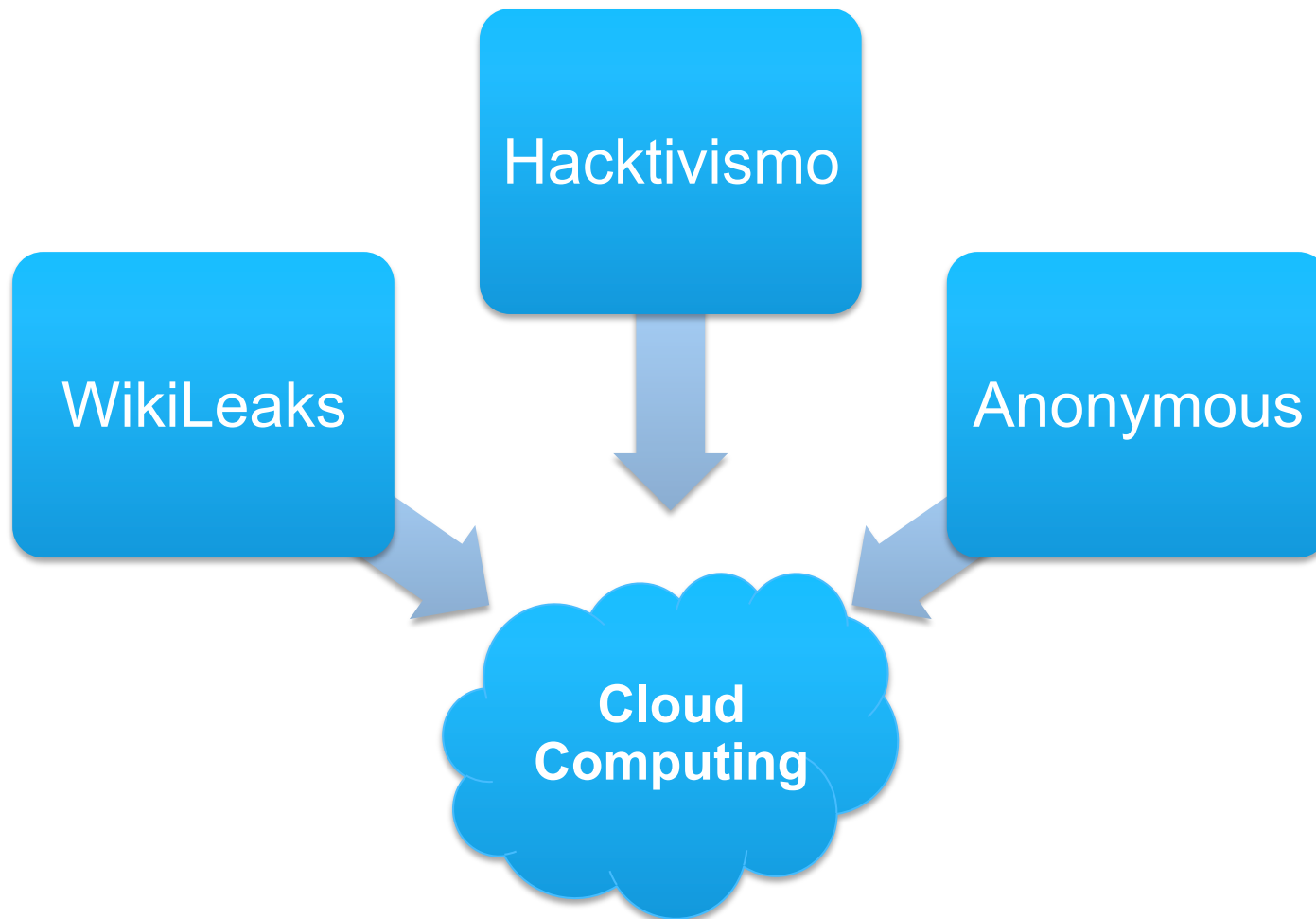
Hacktivismo e Segurança em Cloud Computing

Anchises M. G. de Paula

iDefense Cyber Intelligence Analyst

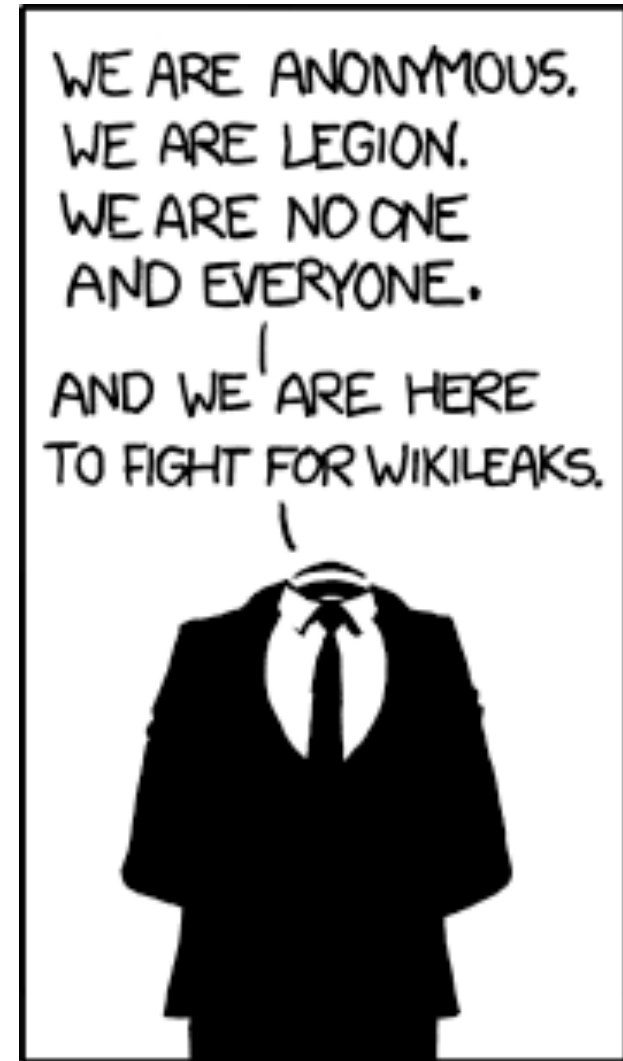
14 de Maio de 2011

Agenda



Hacktivismo

- 2010: Wikileaks e Anonymous redefinem o Hacktivismo
 - 90's: Defacement
 - Hoje:
 - Roubo e vazamento de Dados
 - DDoS como forma de protesto
 - Botnets
 - Low Orbit Ion Cannon (LOIC)
- Princípios
 - Transparência
 - Contra censura online
 - Liberdade de expressão
 - Movimentos sociais



Picture source: xkcd.org

Diversas operações ao redor do mundo



#OpPayback



01/Abr./2010
Wikileaks publica o
vídeo “Colateral Murder”



Picture source: collateralmurder.com

**Abril
2010**

Maio

Jun.

Jul.

Ago.

Set.

Out.

Nov.

Dez.

Jan.
2011

Fev.

Mar.

28/Nov./2010

Cablegate

Wikileaks publica cartas
secretas do Dept. de
Estado dos EUA



Picture source: xkcd.org

Abril
2010

Maio

Jun.

Jul.

Ago.

Set.

Out.

Nov.

Dez.

Jan.
2011

Fev.

Mar.

twitter

Login Join Twitter!

www.wikileaks.org - TANGO DOWN -
for attempting to endanger the lives of
our troops, 'other assets' & foreign
relations #wikileaks #fail

12:34 AM Dec 1st, 2010 via web
Retweeted by 3 people



th3j3st3r
Jester

28/Nov./2010
Th3j3st3r DDoS
Wikileaks website

Abril
2010

Maio

Jun.

Jul.

Ago.

Set.

Out.

Nov.

Dez.

Jan.
2011

Fev.

Mar.



01/Dez./2010
Wikileaks move seu
website para a Amazon

Abril 2010	Maio	Jun.	Jul.	Ago.	Set.	Out.	Nov.	Dez.	Jan. 2011	Fev.	Mar.
---------------	------	------	------	------	------	------	------	-------------	--------------	------	------



*"No soup
for you!"*

01/Dez./2010
Amazon cancela o site
do WikiLeaks

Abril
2010

Maio

Jun.

Jul.

Ago.

Set.

Out.

Nov.

Dez.

Jan.
2011

Fev.

Mar.

E o que isso significa para a Nuvem ?

- Mesmo estando na Nuvem, seu site pode evaporar !



Picture source: sxc.hu

E o que isso significa ?

- **Motivos inesperados**
 - Pressão de terceiros
 - Falência do provedor
 - Falhas do provedor
 - Localização Geográfica

Mar. 13, 2010

Car

Pov

By D

Amaz

servi

outag

some

losin

incide

crash

the c

trans

mana

shift

facili

Apr. 29, 2011

Amazon cloud outage was triggered by configuration error

By Computerworld

Amazon has released a detailed postmortem and mea culpa about the **partial outage** of its cloud services platform last week and identified the culprit: **A configuration error made during a network upgrade.**

During this configuration change, a traffic shift "was executed incorrectly," Amazon said (...).

Mitigação

- Revisar o histórico e a saúde financeira do provedor
- Garantias contratuais
 - SLA
- Plano de Contingência
 - Seu site
 - Provedor secundário
 - Portabilidade
 - Políticas de Backup
 - Off-the-cloud backup



Picture source: sxc.hu

Mitigação

Domínio 2: Governança e Gestão de Risco Corporativo

Domínio 6: Portabilidade e Interoperabilidade

Domínio 7: Segurança Tradicional, Continuidade de Negócios e Recuperação de Desastres





Picture source: sxc.hu

01/Dez./2010
Visa, Mastercard,
Paypal cancelam o
recebimento de doações
para o WikiLeaks

Abril 2010	Maio	Jun.	Jul.	Ago.	Set.	Out.	Nov.	Dez.	Jan. 2011	Fev.	Mar.
---------------	------	------	------	------	------	------	------	-------------	--------------	------	------

twitter

Login Join Twitter!

TARGET: WWW.VISA.COM: FIRE
FIRE FIRE!!! WEAPONS
<http://bit.ly/e6iR3X> ::: SET YOUR
LOIC TO irc.anonops.net ::: #PAYBACK
#WIKILEAKS #anonops

6:02 PM Dec 8th, 2010 via web
Retweeted by 6 people



anonops
AnonOps

#OpPayback

Anonymous faz DDoS
em empresas contra o
Wikileaks

- 04/Dez: Paypal
- 08/Dez: Visa,
Mastercard

Abril
2010

Maio

Jun.

Jul.

Ago.

Set.

Out.

Nov.

Dez.

Jan.
2011

Fev.

Mar.



09/Dez./2010
#OpPayback
Anonymous não
consegue derrubar
Amazon

Abril 2010	Maio	Jun.	Jul.	Ago.	Set.	Out.	Nov.	Dez.	Jan. 2011	Fev.	Mar.
---------------	------	------	------	------	------	------	------	-------------	--------------	------	------

E o que isso significa ?

- Cloud Computing pode ajudar na estratégia de Segurança



Picture source: vidadeprogramador.com.br

E o que isso significa ?

- Confiabilidade do Provedor de Cloud Computing
 - Resistência a cyber ataques
 - Mão de obra especializada
 - Suporte investigativo



Picture source: sxc.hu

Conclusões

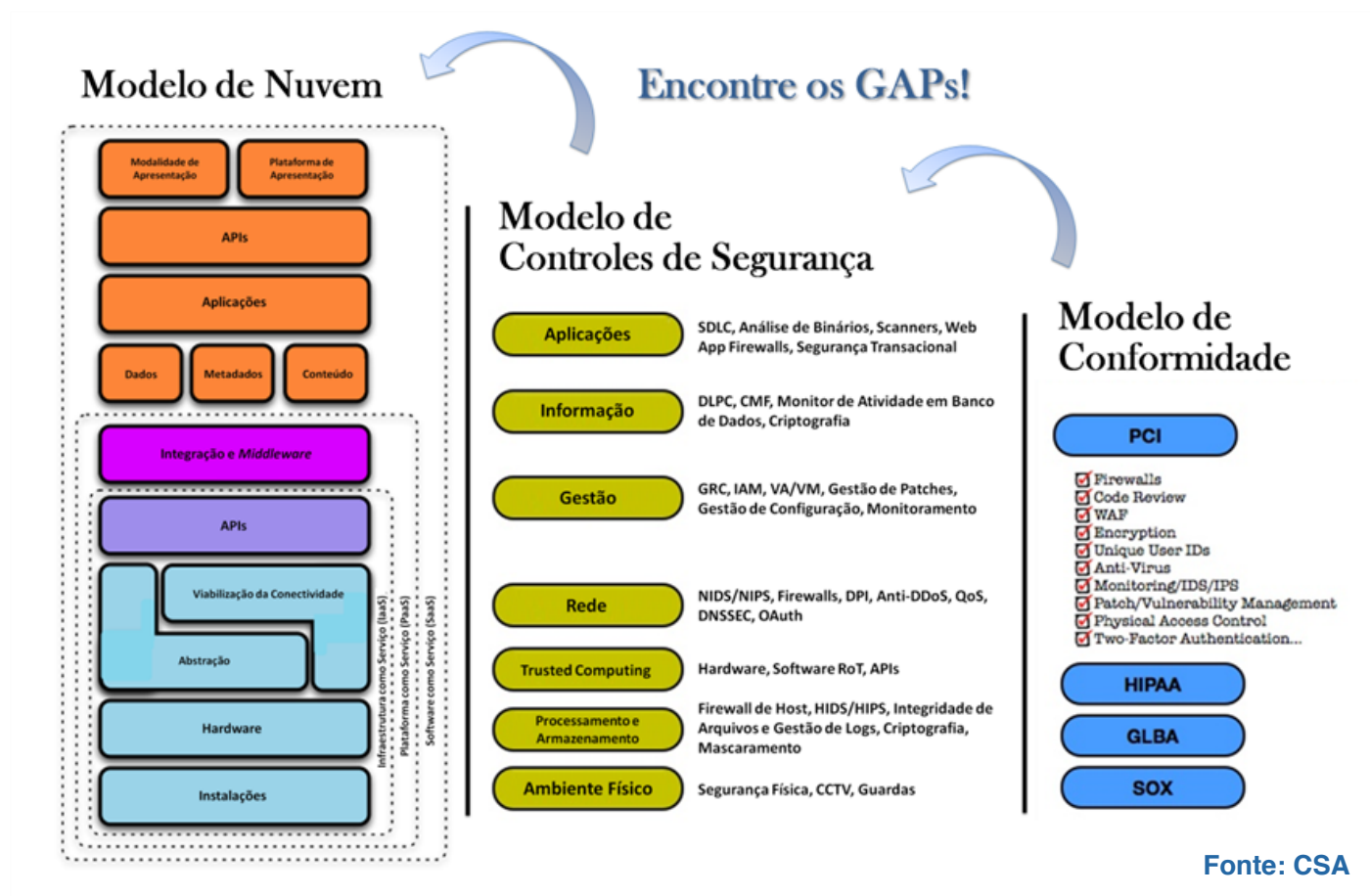
- Computação em Nuvem cria novos **riscos** e novas **oportunidades**
- Análise de Riscos é fundamental



Picture source: sxc.hu

Segurança na Computação em Nuvem

Mapeando o Modelo de Nuvem para o Modelo de Controles de Segurança & Conformidade



Referências

Security Guidance for Critical Areas of Focus in Cloud Computing v. 2.1

- <http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>
- <http://br.cloudsecurityalliance.org>



Top Threats to Cloud Computing V1.0

- Sete principais riscos
<http://www.cloudsecurityalliance.org/topthreats.html>

“It’s the great irony of the Information Age that the very technologies that empower us to create and to build also empower those who would disrupt and destroy”
(Barack Obama)



Source: Whitehouse



VERISIGN™

Thank You

Anchises M. G. de Paula
iDefense Security Intelligence Services
@anchisesbr
adepaula@verisign.com
www.verisigninc.com
www.idefense.com