Entre hackers e botnets: a segurança cibernética no Brasil

Oppermann, Daniel

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Observatório Político
Sul-Americano

O **Observatório Político Sul-Americano - OPSA** é um núcleo de referência destinado ao monitoramento e registro de eventos políticos nos planos interno e externo dos países sul-americanos. Suas atividades principais envolvem a coleta e sistematização de informações relativas aos processos políticos dos países da região, bem como a elaboração de análises pontuais sobre aspectos e problemas das conjunturas doméstica e internacional da área.

Coordenadora Acadêmica

Maria Regina Soares de Lima
Ph.D. em Ciência Política pela Vanderbilt University

Assistentes de Coordenação

Regina Kfuri
Tatiana Oliveira

Assistentes de Pesquisa

Clayton Cunha (Bolívia)
Daniel Oppermann (Indicadores)
Ana Carolina Vieira de Oliveira (Argentina)
Eduardo Heleno Santos (Paraguai)
Beatriz Thomaz Carvalho (Peru)
Fernanda Pernasetti (Equador)
Fidel Flores (Venezuela)
Pedro Benetti (Chile)
Athos Luiz dos Santos Vieira (Colômbia)
Francisco Josué Medeiros de Feitas (Brasil)
Suhayla Khalil (Uruguai)

Boletim OPSA

O Boletim OPSA reúne análises sobre acontecimentos de destaque na conjuntura política da América do Sul e tem periodicidade bimestral. A publicação é composta por editorial e textos dirigidos a leitores que querem ter acesso rápido a informações de qualidade sobre temas contemporâneos. As fontes utilizadas para sua confecção são resumos elaborados pelos pesquisadores do OPSA com base nos jornais de maior circulação em cada um dos países e documentos de autoria de pesquisadores ou agências independentes que complementam as informações divulgadas pela imprensa.

Este Boletim foi elaborado principalmente com base nas informações referentes aos meses de abril a junho de 2011.

O Boletim OPSA é publicado na segunda semana do mês seguinte aos dois meses a que se refere.

ISSN 1809-8827

Instituto de Estudos Sociais e Políticos
Universidade do Estado do Rio de Janeiro
IESP/UERJ

Rua da Matriz, 82 - Botafogo **-** Rio de Janeiro – RJ | Tel.: (21) 2266-8300 Fax: (21) 2286-7146

http://www.opsa.com.br
E-mail: observatorio@iesp.uerj.br

reage à plena submissão das relações internacionais às relações de poder.

A eleição de Graziano Silva para a FAO abre, pois, uma oportunidade para a definição de uma nova globalização e, mais do que isso, chama a atenção pela responsabilidade que enseja. Por marginais que sejam as agências da ONU no que diz respeito à realocação de poder no plano internacional essa eleição é simbólica. E o é porque, com ela, reitera-se a intenção de um desenvolvimento humano que promova a dignidade humana e não apenas o crescimento econômico desigual e excludente. Para o Brasil, é um ganho no sentido de que os brasileiros foram capazes de fazer da política um instrumento para a mudança social, num processo que teve início com a eleição de Lula em 2003. Para o mundo, uma esperança de que a pobreza e as desigualdades sociais arraigadas dentro e fora dos Estados possam vir a ter solução.

Referências bibliográficas

O Globo; Folha de SP; Valor Econômico.

Outras fontes

Observatório Político Sul Americano. *Banco de eventos.* Disponível em: www.opsa.com.br

Segurança da Informação

Entre hackers e botnets: a segurança cibernética no Brasil

Daniel Oppermann

Quando páginas de companhias ou instituições públicas são invadidas por hackers, o cenário sempre é o mesmo. Os representantes e porta-vozes das organizações prejudicadas declaram ao público que não foram afetados dados importantes, especialmente dados pessoais de usuários cadastrados. O Instituto Brasileiro de Geografia e Estatística (IBGE) e a Brigada Militar do Rio Grande do Sul reagiram dessa forma quando suas páginas sofreram ataques virtuais nos dias 24 e 25 de junho de 2011. Além dessas duas, várias outras páginas de instituições públicas foram atacadas na mesma semana. Entre elas, a da Presidência da República, do Senado, da Receita Federal, da Petrobras[18], do Ministério da Cultura, do Ministério do Esporte, diversas páginas da Polícia Militar e a da Universidade de Brasília, entre outros.

Segundo os jornais Folha de São Paulo e Estado de São Paulo uma

18 Na sexta-feira, dia 24 de junho de 2011, a Petrobrás negou ter sido vítima de um ataque virtual, mas não conseguiu explicar de onde vêm os dados privados dos seus funcionários publicados pelos hackers. No dia seguinte, foram divulgados mais dados pelos hackers dando acesso ao servidor da empresa, sendo assim possível acessar outros dados de funcionários e relatórios da empresa.

"série de ataques" virtuais no Brasil começou na quarta-feira, dia 22 de junho de 2011. Segundo o blog de um jornalista da Folha, a presidente "Dilma Rousseff declarou-se 'surpresa' com a vulnerabilidade dos sites oficiais" (Souza 2011). Na versão oficial apresentada pela mídia, o problema estava principalmente concentrado nos grupos de hackers chamados LulzSecBrazil e Fatal Error que estavam atacando sites governamentais a partir de um certo momento. Porém, o cenário era mais complexo.

A "série de ataques" que chamou a atenção pública brasileira nesses dias foi realizada por um grande número de atores independentes, incluindo indivíduos e grupos de hackers de vários países como Turkish Energy Team, Ashiyane Digital Security Team, MeGo, Havittaja, LatinHackTeam, IR4DEX, Sophia Hacker Group e outros. A impressão criada pela mídia de que o problema começou no dia 22 de junho não é correta. O LatinHackTeam é um grupo de hackers ativo há mais de três anos, sendo responsável por invadir pelo menos 250 páginas no Brasil e em Portugal. Embora a maioria das páginas seja privada, houve um aumento de invasões de páginas de instituições públicas nos últimos 12 meses. Entre elas, páginas governamentais dos estados de Goiás (junho 2010), Minas Gerais (julho 2010), Acre (agosto 2010) e Mato Grosso do Sul (maio 2011). Também a Ashiyane Digital Security Team vem aumentando o número de ataques a sites de instituições públicas no Brasil desde março de 2011. Exemplos são as invasões das páginas da Universidade Federal de Ceará (março 2011), da Secretaria Municipal da Saúde de Joinville (abril 2011) e da Universidade Federal do Maranhão (maio 2011). A Sophia Hacker Group é responsável por invasões em mais de 1000 páginas no Brasil desde 2009, principalmente sites particulares. O número de invasões feito pelo IR4DEX supera 1500 só no Brasil (principalmente sites de empresas e particulares). Segundo o chefe do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional (GSI) da Presidência da República, Raphael Mandarino Junior, o "Brasil tem 320 grandes redes no setor governamental, sob constantes ataques cibernéticos (…). Em 2009, foram registradas 45 mil tentativas de invasão e busca de informações estratégicas dessas redes - uma média de cinco por hora." (Estado de São Paulo 2011a)

Existem estratégias diferentes usadas pelos hackers. Grupos como o Turkish Energy Team, o Ashiyane Digital Security Team e o LatinHackTeam usam métodos como a *injeção de SQL* para entrar em um sistema e mudar a

aparência visual das páginas (*web defacement*). Muitas vezes os invasores deixam slogans, logos ou imagens nas páginas invadidas. Tutoriais para aprender como fazer injeções de SQL são disponibilizados pelos próprios hackers na internet. Em alguns casos, a restauração da página pode ser feita pelo administrador do sistema. Em caso de invasões agressivas, o sistema também pode ser seriamente danificado.

Outra estratégia é a realização de um ataque DDoS (distributed denial-of-service attack). Essa forma de atacar um servidor é muito comum não apenas por ser realizada com facilidade, mas também por ser um negócio muito lucrativo, capaz de gerar milhões de dólares por ano. Diferente das injeções de SQL, nos ataques DDoS os agressores não invadem o sistema, mas o atacam de fora, usando um alto número de computadores que estão conectados em redes chamadas botnets. Um botnet pequeno pode ser constituído por 10 ou 20 mil computadores, enquanto botnets grandes consistem em dois ou três milhões de computadores. Geralmente donos de botnets estão envolvidos em várias formas de crimes cibernéticos. Alguns delas são arrendamento de botnets para grupos criminosos e os ataques contra servidores com a intenção de extorsão financeira.

Segundo o Symantec Intelligence Quarterly Report de abril-junho 2010, o Brasil foi o país número cinco no ranking global de atividades de código malicioso. Além disso, sua infra-estrutura está entre as mais vulneráveis para botnets. Relatórios de segurança de informática da Microsoft (2010) e da Trend Micro (2010) confirmaram que o Brasil está sofrendo o segundo maior nível de infecção por botnets no mundo. Isso significa que uma parte essencial da infra-estrutura de TI do país está envolvida em atividades de crimes cibernéticos no mundo inteiro. Além disso, milhares de computadores localizados no Brasil participam atualmente em vários tipos de ataques DDoS em países diferentes.

Já em 2009, o Boletim OPSA informou sobre a necessidade de investigar a segurança cibernética no Brasil (Oppermann 2009). A "série de ataques" feita por hackers que prejudicaram diversas páginas do governo central em junho de 2011 é um problema sério que mostra a necessidade de melhorar a segurança das redes de informação do país. Ao mesmo tempo, esses ataques não são o único problema na segurança cibernética brasileira. A falta de informação da população sobre problemas como botnets e outras ameaças do ciberespaço é também um aspecto crucial. Grupos como LulzSec que, segundo informações

próprias do grupo, era formado por apenas 6 pessoas (e que se dissolveu após apenas 50 dias de existência no dia 26 de junho de 2011) existem em grande número. Eles costumam aparecer e desaparecer. O que fica são milhares de cidadãos mal informados sobre a proteção dos próprios computadores tanto em casa quanto no trabalho. Os botnets no Brasil consistem em computadores localizados em diversos lugares como escritórios, salas e escolas entre Boa Vista e Porto Alegre. A combinação entre crescimento acelerado no mercado de informática e falta de informações para os usuários sobre a necessidade de proteger seus próprios computadores cria um terreno perfeito para atores mal-intencionados no ciberespaço.

No seu Livro Verde "Segurança Cibernética no Brasil" (Presidência da República 2010), o governo brasileiro destacou a necessidade de uma Política Nacional de Segurança Cibernética. Nesse contexto, explicou a intenção de criar, entre outros, programas de "capacitação em segurança cibernética … nos níveis: básico, técnico, graduação, especialização, mestrado e doutorado". Além disso, anunciou o desenvolvimento de "material apropriado para os públicos: infantil; adolescentes e jovens; de baixa renda; da terceira idade; de educadores em todos os níveis de formação educacional; e de gestores e legisladores públicos". As invasões recentes corroboram a necessidade de realizar tais planos agora.

Referências bibliográficas

Estado de São Paulo 2011a: Brasil ainda não tem Política Nacional de Segurança Cibernética, Estadão.com.br, 08 de junho de 2011

http://www.estadao.com.br/noticias/nacional,brasil-ainda-nao-tem-politica-nacional-de-seguranca-cibernetica,729292,0.htm

acesso: 26 de junho de 2011

Estado de São Paulo 2011b: Governos e empresas estão igualmente vulneráveis a hackers, dizem especialistas, Estadão.com.br, 24 de junho de 2011

http://www.estadao.com.br/noticias/tecnologia,governos-e-empresas-estao-igualmente-vulneraveis-a-hackers-dizem-especialistas,736559,0.htm

acesso: 26 de junho de 2011

Folha de São Paulo 2011: Hackers divulgam dados pessoais de funcionários da Petrobras, Folha.com, 24 de junho de 2011

http://www1.folha.uol.com.br/poder/934449-hackers-divulgam-dados-pessoais-de-funcionarios-da-petrobras.shtml

acesso: 26 de junho de 2011

Microsoft 2010: Security Intelligence Report Volume 9, 2010

http://www.microsoft.com/sir

acesso: 26 de junho de 2011

Oppermann, Daniel 2009: A necessidade de investigar a segurança cibernética no Brasil, Boletim OPSA No. 6, nov/dez 2009, p. 17

http://www.opsa.com.br/pdfs/40_boletins_Boletim_06_nov_dez_2009.pdf

Presidência da República 2010, Segurança Cibernética no Brasil (Livro Verde), Gabinete de Segurança Institucional , Secretaria Executiva , Departamento de Segurança da Informação e Comunicações , Brasília, 2010

http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf

accesso: 26 de junho de 2011

Souza, Josias de 2011: Além da PF, Abin é acionada para investigar hackers, http://josiasdesouza.folha.blog.uol.com.br, 24 de junho de 2011

acesso: 26 de junho de 2011

Symantec 2010: Symantec Intelligence Quarterly (April-June 2010)

http://bit.ly/g8kpvz

acesso: 26 de junho de 2011

Trend Micro 2010: TrendLabs. Global Threat Trends 1H 2010

http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/tm101hthreat_report.pdf

acesso: 26 de junho de 2011

Instituições e Processos Políticos

Consulta Popular no Equador: uma vitória para abrir os olhos

Fernanda Pernasetti

Durante o primeiro semestre de 2011, o cenário político equatoriano foi marcado pelo debate acerca da grande consulta popular proposta pelo presidente Rafael Correa. Aprovada em janeiro pelo Conselho Nacional Eleitoral (CNE)[19], e realizada no dia 7 de maio, pode-se dizer que ela logrou

[19] O CNE é o órgão central do Poder Eleitoral, um dos cinco poderes da República do Equador, além do Executivo, Legislativo, Judiciário e de Transparência e Controle Social.