17º WRNP
Workshop RNP
30 | 31 MAIO
SALVADOR | BA

GT – ACTIONS
SeVen - *Selective Verification in Application Layer*

Iguatemi Eduardo da Fonseca

Laboratório de Redes (LaR)
Universidade Federal da Paraíba

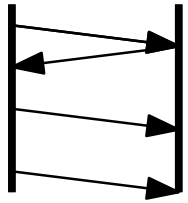
RNP

Sumário

- Ataques DDoS da Camada de Aplicação
- Objetivos do GT-ACTIONS
- Parceiros e equipe
- Produtos, Inovações e Resultados alcançados
- Público alvo e casos de uso
- Melhorias tecnológicas ainda em investigação

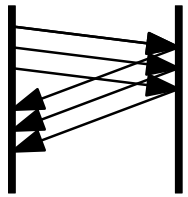
Ataques DDoS da Camada de Aplicação

Ataques DDoS da Camada de Aplicação



Slowloris / POST

- Pouco tráfego: um computador indisponibiliza um servidor Web;
- Tráfego similar a um usuário honesto;
- Indisponibilizar somente um serviço, deixando os outros disponíveis;
- Ferramentas de geração de ataques disponíveis e de fácil uso (até por amadores);
- Poucas defesas: filtrar IPs, negar serviços para clientes lentos, etc.



TCP SYN Flood

- Grande quantidade de tráfego;
- Indisponibiliza todos os serviços;
- Existem métodos de identificação e tratamento.

Application

⋮

Transport

Network

⋮

Physical

- Não é possível usar ferramentas de defesa baseadas em análise de fluxo e volume de tráfego
- Em 2015, ataques explorando o HTTP corresponderam a mais de 30% do total de ataques

G1 Tecnologia e Games

Editorias | Economia | Sua região | Na TV | Serviços | VC no G1 | Princípios editoriais

22/06/2011 19h19 - Atualizado em 22/06/2011 19h33

Ataque hacker foi o maior já sofrido por sites do governo na internet

Servidores na Itália teriam sido ponto de partida para ação de grupo. LulzSecBrazil reivindicou autoria de ataque de 'negação de serviço'.

Do G1, em São Paulo

O ataque hacker às páginas da Presidência da República, Portal Brasil e da Receita na madrugada desta quarta-

Ministério da Defesa
Exército Brasileiro
BRAÇO FORTE MÃO AMIGA
Ministério da Defesa | Marinha | Força A

Resenha
Informex
Reserva pró-Ativa
Ingresse no Exército
Quartéis por Estado
Rádio Verde-Oliva

PUBLICADOR DE CONTEÚDO WEB

GUERRA ANÔNIMA

OS HACKERS DE GRUPOS COMO ANONYMOUS E LULZSEC DOMINAM A ATENÇÃO DO MUNDO AO ATACAR DA SONY À CIA, DA PETROBRAS À PRESIDÊNCIA. MAS O QUE

Enem

GABARITO OFICIAL | CORREÇÃO COMENTADA | FOTOS | NOTÍCIAS | MANDE SUA

Enem 2013 tem 7,8 milhões de inscritos; MEC admite ataque hacker

Yara Aquino
da Agência Brasil, em Brasília 28/05/2013 | 12h24 > Atualizada 28/05/2013 | 16h50

SITES DO GOVERNO FEDERAL BRASILEIRO, INCLUISIVE DO EXÉRCITO BRASILEIRO, SÃO ATACADOS NOVAMENTE PELOS LULZSEC

10/04/2012 | Vinícius Vieira | One comment

info EXAME

NOTÍCIAS | BLOGS | GAMES | REVIEWS | GADGETS | DOWNLOADS | DICAS | MULTIMÍDIA | TÓPICOS | INFO@Vagas

Últimas / Bit no Carro / Carreira / Ciência / Internet / Mercado / Cultura Nerd / Segurança / Tec. Pessoa

OFERTAS TAM
Passagens Aéreas com os Melhores Preços. Acesse o Site e Con

Notícias > Segurança

11/06/2014 16h57 - Atualizado em 11/06/2014 16h57

Hackers atacam sites voltados à Copa no Brasil

Reuters

Edição do dia 28/12/2012
29/12/2012 00h47 - Atualizado em 29/12/2012 00h51

MEC tirou site do Enem do ar após ataque de hackers

Segundo técnicos do governo, o ataque veio de fora do país. Ministério da Educação diz que acesso foi normalizado rapidamente.

13/01/2015 20h32 - Atualizado em 13/01/2015 20h32

Página do Inep apresenta lentidão após divulgação das notas do Enem

Presidente do Inep diz que site foi alvo de hackers ao longo do dia. Lentidão deve prosseguir nos próximos dias, segundo o instituto.

Sites ligados à Copa e ao governo são alvos de ataques cibernéticos

DE SÃO PAULO
COM REUTERS

12/06/2014 12h29 - Atualizado às 13h18

RNP participa da operação de monitoramento do Sisu

[21.1.2015]

SiSU SISTEMA DE SELEÇÃO UNIFICA

abranet Associação Brasileira de Internet
Home

NOTÍCIAS

Ataques DDoS se multiplicam e sobem mais de 207% no Brasil

Por: Roberta Prescott - 14/05/2015

Puxado pelo crescimento dos ataques distribuídos de negação de serviços (DDoS), o número de incidentes reportados ao CERT.br alcançou 1.047.031 em 2014, contra 352.925 em 2013 e 466.029 em 2012.

Hackers derrubam páginas de administradoras de cartões de crédito

| Agência Brasil

Depois de atacar *sites* do Banco Central (BC), da Federação Brasileira de Bancos (Febraban) e de mais três bancos, o grupo de *hackers* Anonymous Brasil derrubou a páginas das administradoras de cartões Cielo e Redecard. As páginas das duas empresas na *internet* estão fora do ar.

Segurança

Ataques no Brasil chegam a serviços de nota fiscal eletrônica

Depois dos bancos, ciberativistas derrubaram nesta semana redes das Secretarias de Fazenda do estado de São Paulo e da Bahia.

Recomendadas

Malware bancário Escelar já atacou 100 mil brasileiros no país e nos EUA

terra | NOTÍCIAS | ECONOMIA | ESPORTES | DIVERSÃO | MÚSICA | VIDA E ESTILO | TERRA TV | SHOPPING
TECNOLOGIA

IDGNOW! | PCWorld | Macworld | COMPUTERWORLD | CIO

COMPUTERWORLD

Tópicos | News | Cloud Computing | Big Data | Mobilidade | Segurança | Carreira | Tecnologias Emergentes | Recursos/White Papers | Newsletters

Segurança
Cibercrime | Criptografia | Privacidade | Segurança de Aplicação | Segurança de Cloud | Segurança de Da
Segurança Móvel | Vírus e vulnerabilidades

Segurança > Cibercrime, Rede, Vírus e vulnerabilidades

Brasil é o terceiro maior alvo de ataques DDoS do mundo

Objetivos do GT-ACTIONS

- Desenvolver uma plataforma computacional, metodologias e técnicas para mitigação de ataques DDoS da camada de aplicação
  - **Modelo matemático e perfil dos ataques:** Identificar o perfil dos ataques DDoS da camada de aplicação e modelar formalmente os seus aspectos fundamentais
  - **Metodologia:** Criar uma metodologia para o desenvolvimento de algoritmos e técnicas de mitigação dos ataques DDoS
  - **Algoritmos e técnicas:** Desenvolver e validar técnicas e algoritmos para neutralizar ataques DDoS.
  - **Plataforma computacional:** Implementar plataforma computacional para a **defesa em tempo real** contra ataques DDoS

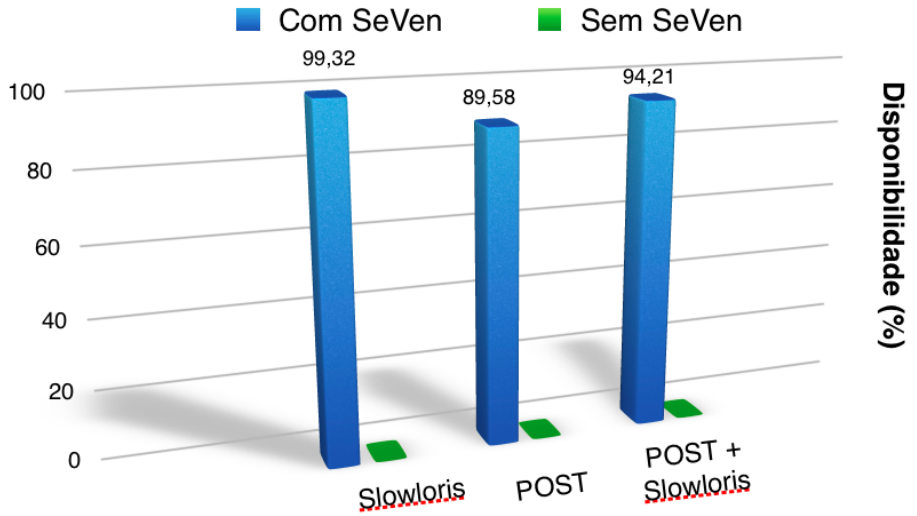
Parceiros e Equipe

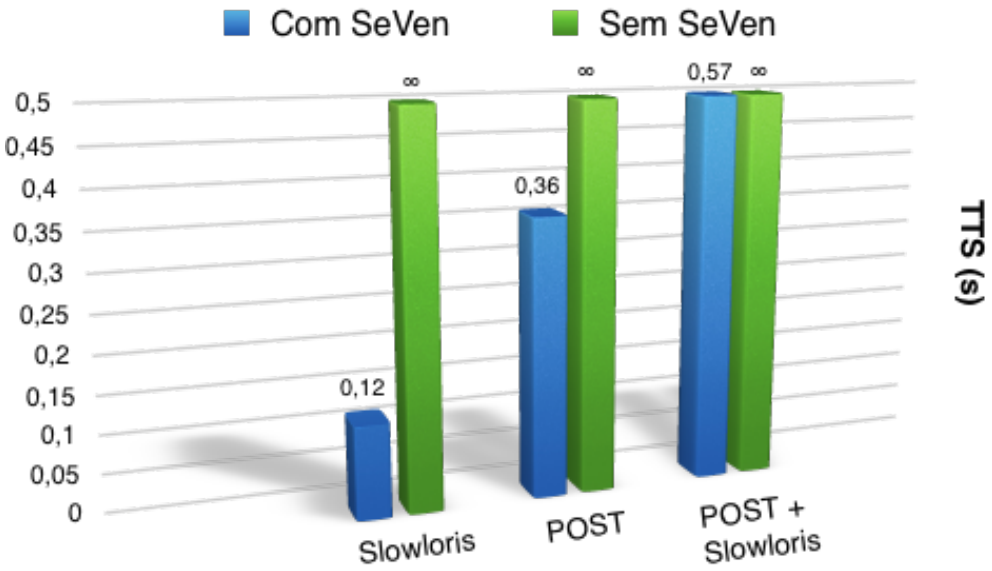
- **UFPB**: Iguatemi E. Fonseca, Vivek Nigam, Marcílio Lemos, Eduardo Gama, João Correa, Túlio Pascoal, Rafael Brayner, Roberto Júnior, Lucas Aversari
- **UFES:** Moises R N. Ribeiro, Isabella Albuquerque, Sabrina Felix
- **UNICAMP/UFABC**: Hélio Waldman
- **Parceiros:**
  - UniSul
  - UEPG
  - Fone@RNP
  - *Flexa Information Technology*
  - NTI/UFES
  - STI/UFPB

Produtos, Inovações e Resultados alcançados

- **Estratégia inédita na literatura,** chamada **SeVen,** para a mitigação de ataques DDoS na camada de aplicação. Características gerais: *configurável, independente do tráfego legítimo e do ataque, baixa complexidade computacional, modular*
- **Modelagem formal** do **SeVen** usando métodos formais e a simulação de diversos cenários de ataque
- **SeVen** implementando em C++, funcionando como *Proxy* ou módulo do Apache. 100% desenvolvido pela equipe
- **Validação por meio de experimentos na rede Ipê**. **SeVen** consegue garantir até 98% de disponibilidade em servidores Web (Apache, Nginx, Tom Cat) sob ataques DDoS (*Slowloris, HTTP POST, Slowread*, "*Slowloris ressussitado*")
- **Interface/Interação** com o usuário**, Escalabilidade, Estabilidade e Extensibilidade**
- **Produção acadêmica e inovação tecnológica:** Artigos científicos, registro(s) de software e patente(s)

✳ Experimentos com o SeVen na Rede Ipê da RNP: 24 horas de duração



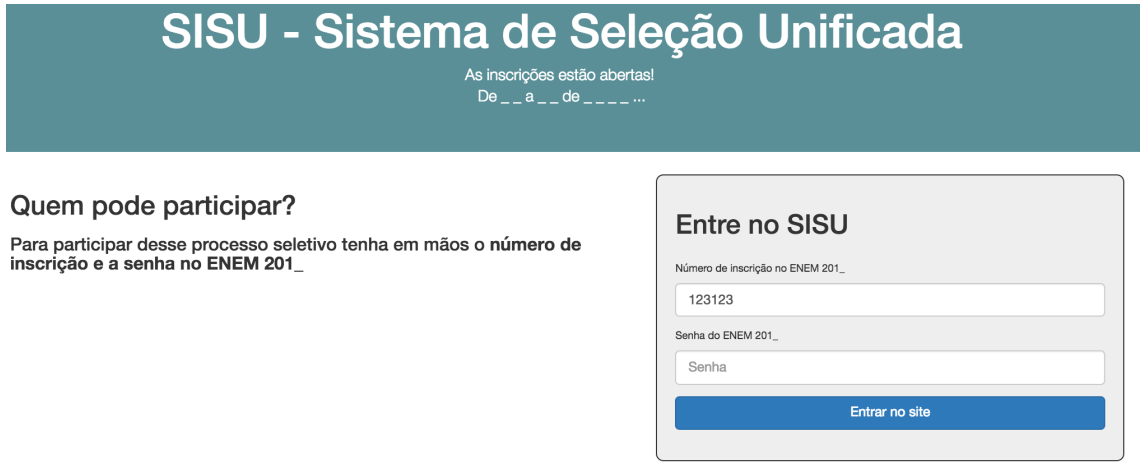


✳ Experimentos com o SeVen: diversos ataques em Servidores Nginx e Apache

Attack	Apache		Apache with SeVen		nginx		nginx with SeVen	
	Success Rate	TTS	Success Rate	TTS	Success Rate	TTS	Success Rate	TTS
Slowloris	0.0%	∞	98.7%	0.15s	15.3%	0.00s	81.4%	0.01s
HTTP POST	0.0%	∞	97.3%	0.14s	–	–	–	–
Slowread	13.8%	1.99s	94.4%	4.68s	5.2%	1.29s	97.9%	3.33s
Resurrected Slowloris	31.9%	1.28s	95.6%	0.58s	4.3%	0.00s	81.7%	0.01s
Slowloris + HTTP POST	0.0%	∞	95.2%	0.20s	–	–	–	–

✳ Servidor executando SeVen usou 3% da CPU e em torno de 8 Mbytes de RAM

✴ Experimentos com o SeVen: formulário SiSu + servidor *Web* Tomcat



Rate of 10 Robots per Minute

Attack	Tomcat		Tomcat with SeVen	
	Successful Robots	Failed Robots	Successful Robots	Failed Robots
Slowloris	0	1000 (2/998)	1000	0
HTTP POST	204	796 (21/775)	1000	0
Slowread	121	879 (9/870)	1000	0
Resurrected Slowloris	20	980 (12/968)	1000	0

Rate of 25 Robots per Minute

Attack	Tomcat		Tomcat with SeVen	
	Successful Robots	Failed Robots	Successful Robots	Failed Robots
Slowloris	0	1000 (4/996)	1000	0
HTTP POST	174	826 (27/799)	999	1 (1/0)
Slowread	121	879 (9/870)	1000	0
Resurrected Slowloris	4	996 (8/988)	1000	0

Rate of 50 Robots per Minute

Attack	Tomcat		Tomcat with SeVen	
	Successful Robots	Failed Robots	Successful Robots	Failed Robots
Slowloris	0	1000 (1/999)	1000	0
HTTP POST	104	896 (21/873)	997	3 (3/0)
Slowread	148	852 (6/846)	1000	0
Resurrected Slowloris	10	990 (3/987)	921	79 (0/79)

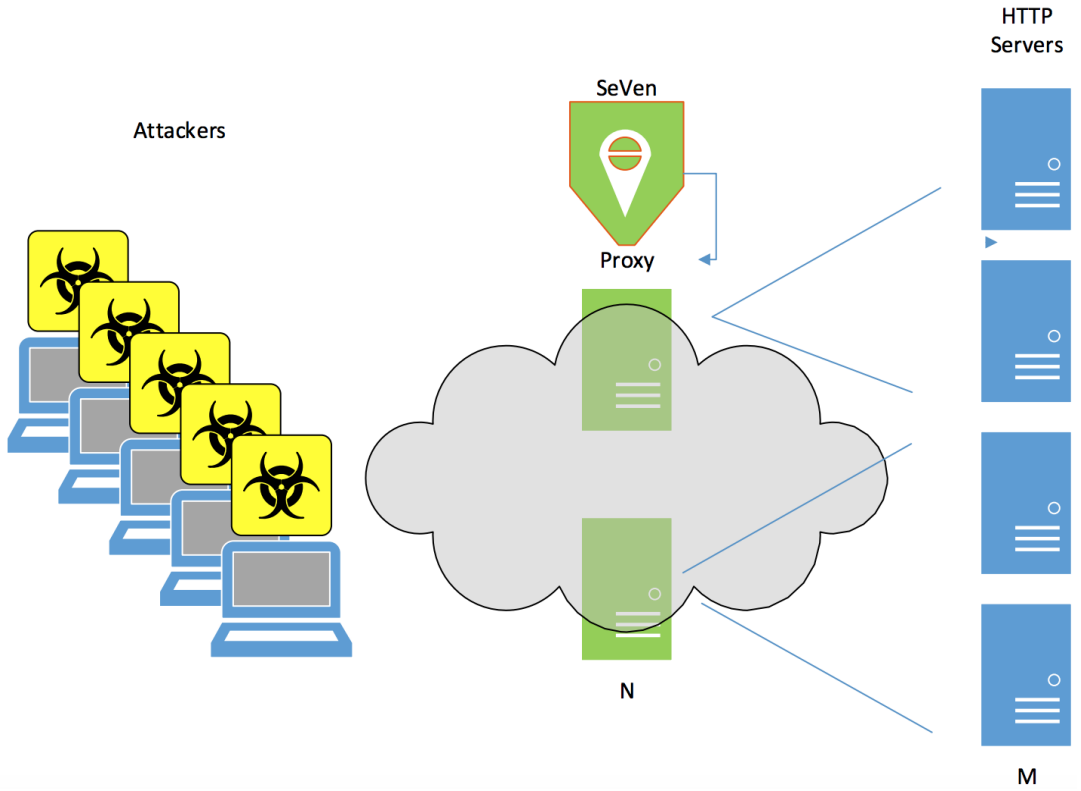
Público Alvo e Casos de Uso

- **Serviços e/ou servidores Web`s em qualquer cliente/usuário da RNP**, como por exemplo, as Universidades e Institutos Federais
  - *Atualmente a RNP não possui ferramenta de mitigação de ataques DDoS da camada de aplicação*
- **Serviço Fone@RNP**
  - *Ataques TDoS (Telephone DoS) - investimento dos EUA*
- **Sistema de matrículas das Universidades Federais**
  - *Pode ser um piloto para um futuro uso nos sistemas do SiSu/MEC*
- **Sites e Aplicações *Web* do Governo Federal**
  - *Sisu/MEC, Receita Federal, Polícia Federal, Exército Brasileiro, Gabinete da Presidência da República, Bancos, dentre outros*
- **Empresas interessadas em proteger suas aplicações e servidores *Web***

Melhorias tecnológicas ainda em investigação

Escalabilidade

- **Relação N/M:** Testar combinações e arquiteturas de número de proxy (N) versus número de servidores Web (M). A ideia é encontrar relações/configurações entre N e M que são necessários para manter o serviço Web disponível em diversos cenários de ataques.



Extensibilidade

- **Adaptação para o Fone@RNP:** tratamento de ataques *TDoS (Telephone DoS)*
- **Testes com o outros Servidores (IIS da Microsoft,**
- **Novos ataques da camada de aplicação ("Slowloris ressuscitado", Goloris, outros)**

Attack	Apache		Apache with ReqTimeOut		nginx	
	Success Rate	TTS	Success Rate	TTS	Success Rate	TTS
Slowloris	0.0%	∞	93.8%	1.13s	15.3%	0.00s
Resurrected Slowloris	31.9%	1.28s	7.6%	1.60s	4.3%	0.00s

17º WRNP
Workshop RNP

Obrigado! Visite o estande do GT-ACTIONS.

Iguatemi E. Fonseca

iguatemi@ci.ufpb.br