Panorama e Melhores Práticas de Segurança na Rede Acadêmica de Santa Catarina

Rede Nacional de Ensino e Pesquisa

Ponto de Presença da RNP em Santa Catarina

Rodrigo Pescador - rodrigo.pescador @ pop-sc.rnp.br

Seminário de Atualização 2016 – POP-SC/RNP

[4-6] de Outubro de 2016

REMEP Florianópolis

PoP-SC

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

Agenda

- MESEG 2016
- Panorama e estatísticas dos incidentes de segurança em Santa Catarina
- SGIS/RNP no gerenciamento de incidentes de segurança
- Ataques de amplificação usando UDP
- Tipos de incidentes de segurança mais comuns e como tratá-los
- Importância do *log* na identificação e resolução de incidentes
- Importância da resolução dos incidentes
- Importância de manter um software atualizado
- Boas práticas a serem adotadas (BCPs da IETF)
- Ferramentas interessantes

Para refletir

Veja se você sabe responder a esta questão:

- Sua instituição já foi alvo de uma tentativa de ataque, seja ele bem sucedido ou não? Com que frequência isto ocorre?

MESEG 2016 - RNP

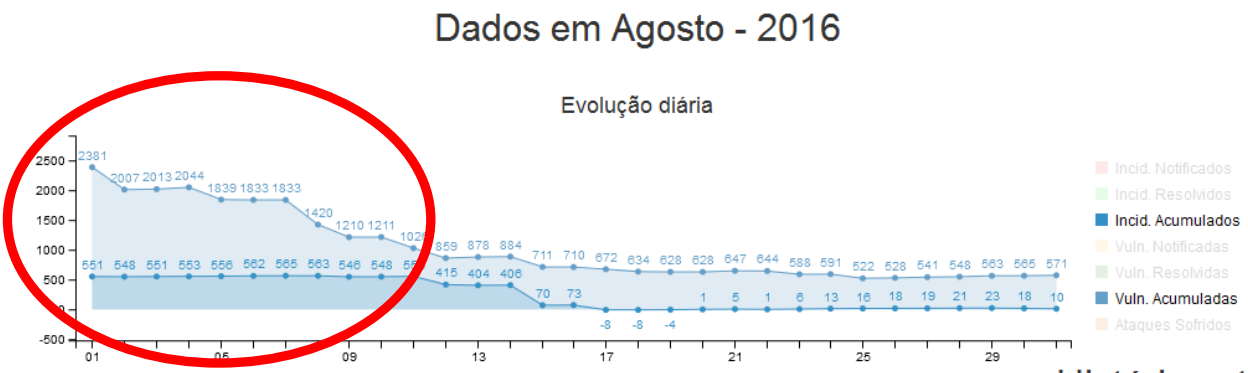
O Mês de Segurança é promovido pela Rede Nacional de Ensino e Pesquisa, por meio do seu Centro de Atendimento a Incidentes de Segurança (CAIS), como um conjunto de celebrações que acontecem anualmente durante todo o mês de outubro, com o intuito de fomentar a cultura de segurança da informação e divulgar amplamente as ações promovidas pelas instituições que aderirem.

A celebração do Mês de Segurança busca criar oportunidades para as instituições discutirem sobre as boas práticas no uso da tecnologia em suas instituições e comunidades locais.

Maiores informações: https://meseg.rnp.br/home

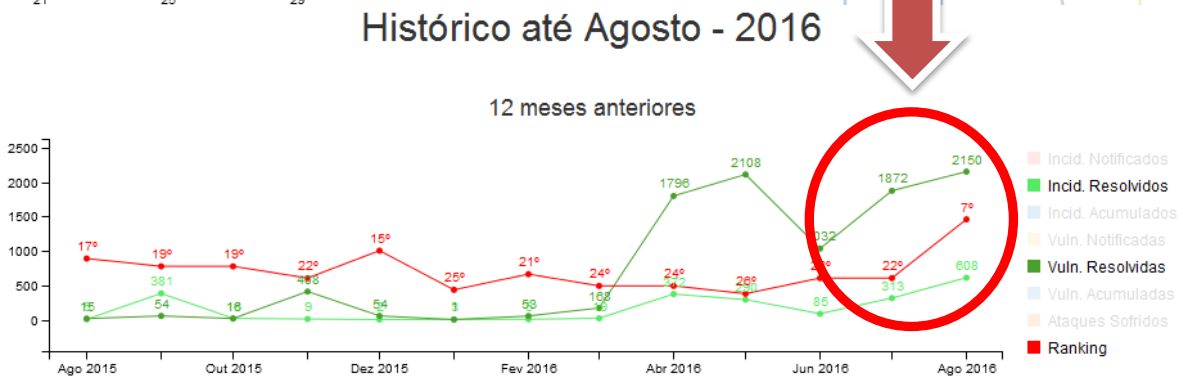
Panorama e estatísticas dos incidentes de segurança em Santa Catarina

- Contato mais próximo do PoP-SC com as instituições reduziu o número de incidentes consideravelmente
  - Apoio na resolução dos problemas
  - Identificação das causas e ações corretivas e preventivas



Ações efetivas a partir dos primeiros dias de Agosto – 2016: diminuição dos indicadores acumulados

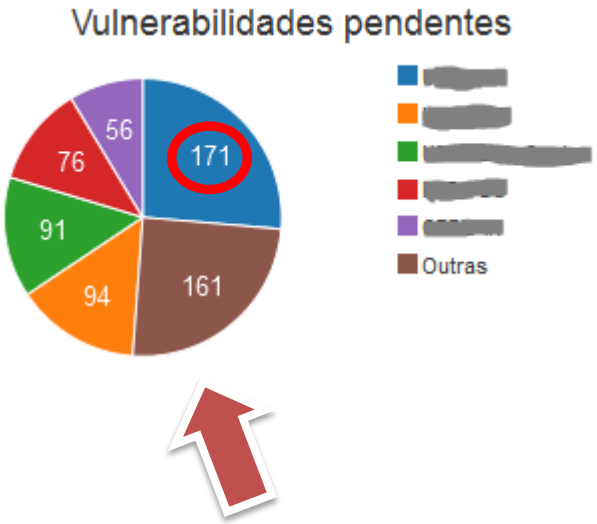
Reflexo no ranking nacional do número de incidentes



Fonte dos gráficos: SGIS/RNP

Panorama e estatísticas dos incidentes de segurança em Santa Catarina

- Distribuição por organização (dados de Agosto – 2016)
  - É Possível observar que poucas instituições concentram a maioria das vulnerabilidades pendentes de resolução

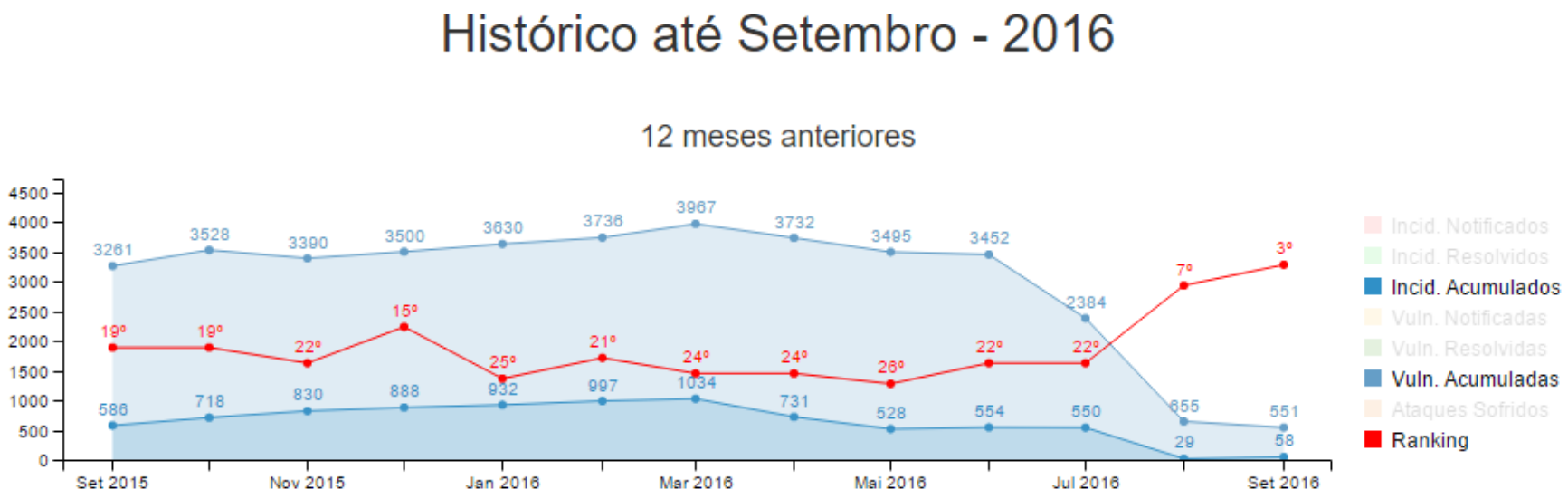


Neste caso, somente uma das instituições concentra mais vulnerabilidades pendentes do que o somatório de “Outras” não listadas

Fonte dos gráficos: SGIS/RNP

Panorama e estatísticas dos incidentes de segurança em Santa Catarina

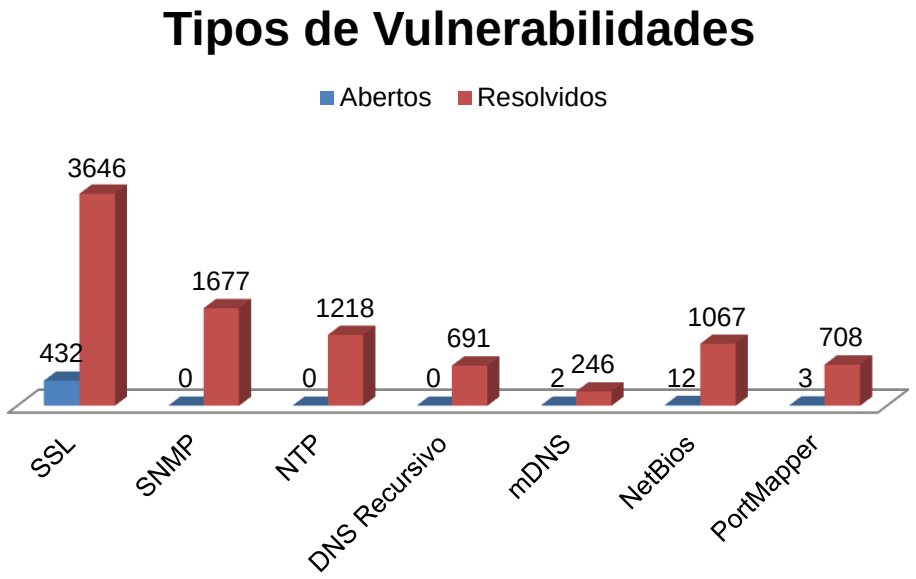
- Números até Setembro – 2016

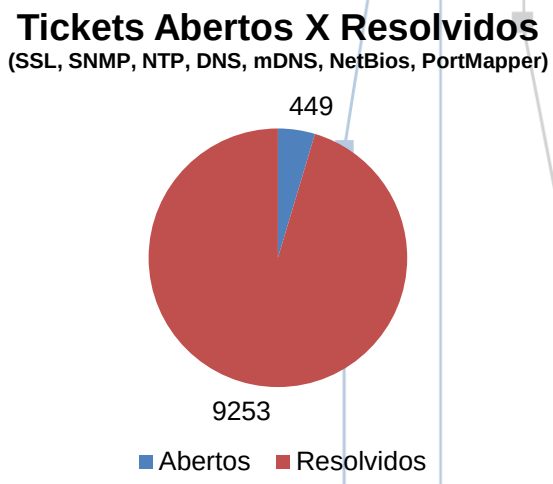


Fonte dos gráficos: SGIS/RNP

Panorama e estatísticas dos incidentes de segurança em Santa Catarina

- **Total de vulnerabilidades notificadas em SC**
  - Desde a implantação do SGIS: 10716
- **Tipos de vulnerabilidades mais notificadas**
  - As 7 categorias abaixo representam cerca de **90,54%** do total de vulnerabilidades registradas no SGIS desde a sua implantação





Fonte dos dados: SGIS/RNP – 27/09/2016

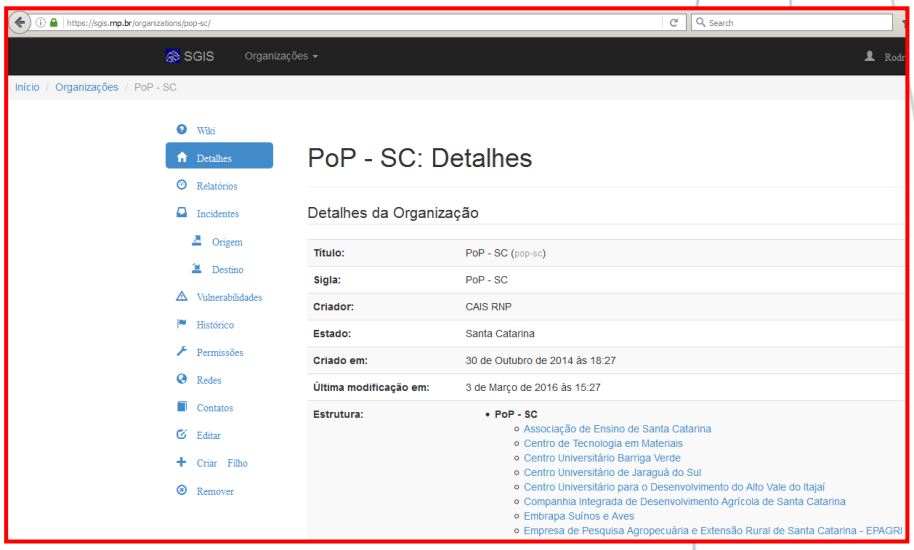
SGIS/RNP no gerenciamento de incidentes de segurança

- **Motivadores**:
  - Permitir que as instituições gerenciem através de uma interface web os seus incidentes/vulnerabilidades notificados pelo CAIS
  - Permitir que o CAIS faça mais iniciativas de controle e erradicação dos problemas enfrentados pelos clientes com base nas informações obtidas do sistema
  - Oferecer indicadores claros relacionados aos clientes da Rede Ipê

- **Algumas funcionalidades do sistema:**
  - Reporte de incidentes de segurança para a instituição e acompanhamento até sua resolução final
  - Geração de estatísticas
  - Solicitação de apoio na resolução de incidentes

Acesso através da URL: **https://sgis.rnp.br**

CAIS Centro de Atendimento a Incidentes de Segurança



SGIS/RNP no gerenciamento de incidentes de segurança

Sistema SGIS
(números nacionais)

653.093 notificações / ano

1.789 notificações / dia

74 notificações / hora

84 parsers

12 fontes de detecção

7 servidores

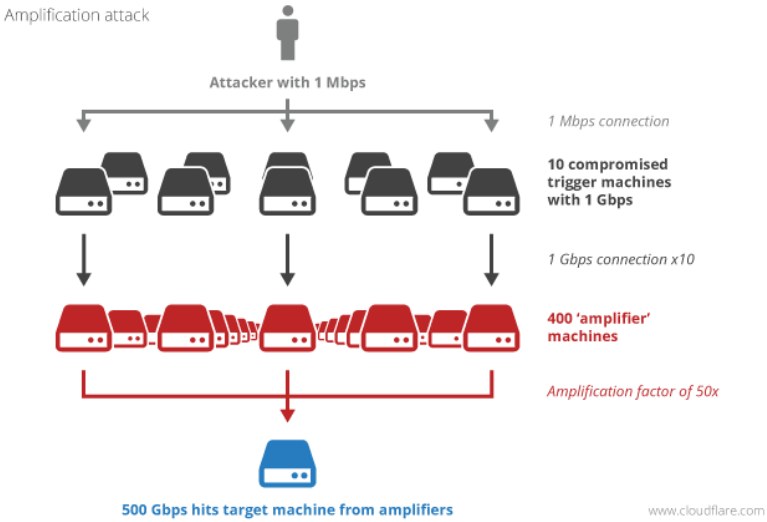
Dados de 2015

Ataques de amplificação usando UDP

- Alguns dos protocolos que permitem ataques de amplificação

Protocolo
DNS, mDNS
NTP
SNMP
NetBIOS

- Como ocorre a amplificação



Fonte: CloudFlare

Algumas formas de detecção de ataques de amplificação:

- Monitoramento de requisições de grandes pacotes UDP
- Monitoramento do número de conexões UDP a um serviço
- Análise de fluxos para detectar possíveis pacotes *de spoofing*

Algumas formas de mitigação de ataques de amplificação:

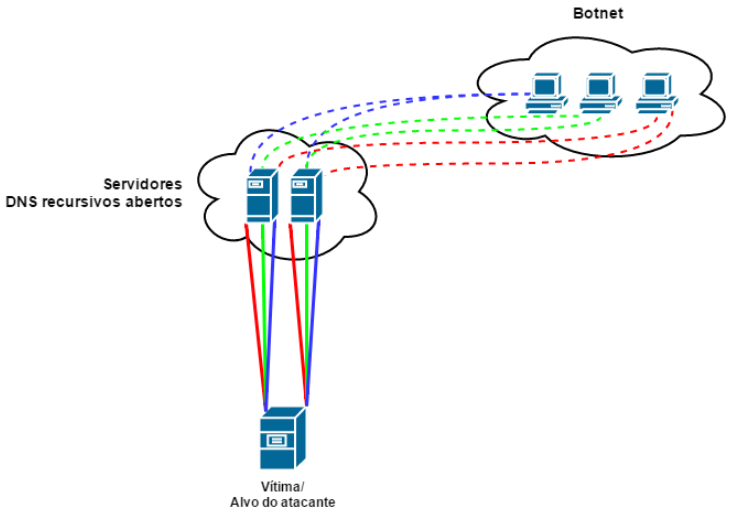
- Manter o software atualizado e com as correções de segurança em dia
- Implementar boas práticas na configuração de serviços
- Desabilitar qualquer serviço não utilizado que esteja disponível na Internet
- Habilitar *rate-limit* para os serviços legítimos disponibilizados na Internet
- Implementação da BCP 38

Tipos de incidentes de segurança mais comuns e como tratá-los

- **DNS recursivo aberto**
  - Servidor que permite ser utilizado por qualquer *host* na Internet para resolver nomes
- **NTP aberto**
  - Um servidor que permite consultas de qualquer host da Internet, especialmente as do tipo "*monlist*"
- **SNMP**
  - Dispositivo que responde a consultas SNMP para qualquer host na Internet, especialmente com comunidades padrão "*public*"
- **SSL vulnerável**
  - SSLv3 vulnerável permite acesso a dados sensíveis como senhas, alteração de cookies, etc...
- **Violação de Copyright**
  - Detentores de direitos autorais, principalmente estúdios de filmes, reclamam da violação de direitos

Tipos de incidentes de segurança mais comuns e como tratá-los

- **DNS recursivo aberto**
  - O atacante envia uma requisição ao servidor DNS aberto com um endereço de origem forjado (da vítima que sofrerá o ataque de DDoS). Com a resposta de diversos servidores ao mesmo tempo, a vítima facilmente ficará sobrecarregada das respostas
  - Uma requisição DNS de 60 bytes pode facilmente alcançar o tamanho de 4000 bytes na resposta para a vítima. Neste caso, o fator de amplificação é de aproximadamente 70:1



Como verificar a vulnerabilidade (rede externa):

dig ANY rnp.br @"IP"

Ação principal: Configurar corretamente os servidores DNS para que respondam a consultas recursivas somente de redes autorizadas e não para qualquer *host* da Internet

Tipos de incidentes de segurança mais comuns e como tratá-los

- **NTP aberto**
  - Através do comando "*monlist*" é possível listar os últimos 600 *hosts* que realizaram consultas no servidor
  - O atacante envia uma requisição ao servidor NTP solicitando a lista de *hosts* ("*monlist*") com um endereço de origem forjado (da vítima que sofrerá o ataque de DDoS). O fator de amplificação neste caso pode ser de 20:1 até 200:1

Como verificar a vulnerabilidade (rede externa):

ntpdc -n -c monlist "IP"

ATENÇÃO: Ao ativar a sincronização de tempo por NTP em equipamentos rede, muitos deles se tornam um servidor NTP e respondem a consultas externas. Neste caso, é importante implementar ACLs de proteção.

Ações principais:

- **Atualizar a versão do NTPD para NTP-4.2.7p26 ou posterior (retirada do comando "*monlist*")**
- **Implementar ACLs de proteção para evitar consultas da Internet ao servidor NTP (se for utilizado somente como um servidor interno)**

Tipos de incidentes de segurança mais comuns e como tratá-los

- **SNMP**
  - Comunidade "*public*" aberta para consulta na Internet
  - Assim como outros ataques de amplificação, o atacante envia requisições com IP forjado para os dispositivos que respondem a SNMP para que as respostas sejam direcionadas ao alvo do ataque
  - Ataques de amplificação utilizando SNMP foram vistos com fator de amplificação de 600 a 1700 vezes

Como verificar a vulnerabilidade (rede externa):

snmpget -c public -v 2c "IP" 1.3.6.1.2.1.1.1.0

ATENÇÃO: Muitos dispositivos de rede vem com SNMP ativado de fábrica utilizando a comunidade "*public*".

Ações principais:

- **Se não utilizar SNMP, desabilite o serviço**
- **Configure uma comunidade privada e utilize autenticação. NÃO UTILIZE A COMUNIDADE "PUBLIC"**
- **Aplique ACLs de proteção para restringir as consultas somente para a rede interna**

Tipos de incidentes de segurança mais comuns e como tratá-los

- **SSLv3**
  - SSL, e seu sucessor TLS, são utilizados para comunicação segura em navegadores WEB (HTTPS)
  - Nenhuma versão do protocolo SSL é segura, todas elas possuem algum tipo de vulnerabilidade
  - O atacante, através da vulnerabilidade do SSLv3 chamada POODLE, pode interceptar os dados em uma comunicação criptografada
  - De acordo com a CloudFlare, somente 0,09% dos usuários utilizam navegadores sem suporte a TLS

Como verificar a vulnerabilidade:

nmap -sV --version-light --script ssl-poodle -p 443 “IP”

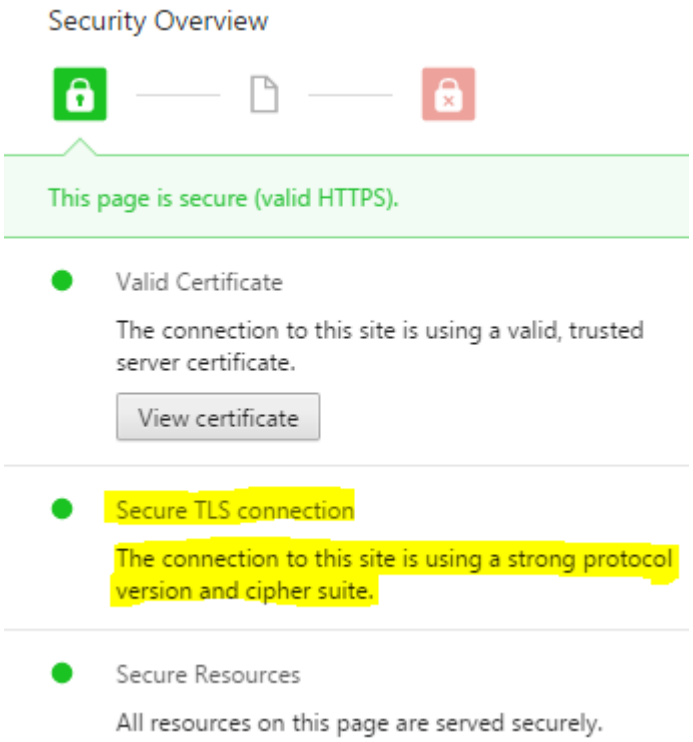
```
Nmap scan report for 154.[redacted] ([redacted].154)
Host is up (0.0033s latency).
PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http Oracle GlassFish 3.1.2.2 (Servlet 3.0; JSP 2.2; Java 1.7)
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  OSVDB:113251
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and
|           other products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       http://osvdb.org/113251
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
```

Ações principais:

- **Desabilitar o SSLv3 dos servidores (usuários não poderão mais utilizar este protocolo para se conectarem ao servidor e terão que utilizar um protocolo mais seguro)**
- **Utilize somente o protocolo TLS para comunicação criptografada**

Tipos de incidentes de segurança mais comuns e como tratá-los

- **SSLv3**
  - Acesso ao site da Caixa utilizando o Google Chrome: Negociação da criptografia entre o servidor e cliente utilizando TLS



Tipos de incidentes de segurança mais comuns e como tratá-los

- **Violação de Copyright**
  - Detentores de direitos autorais, principalmente estúdios de filmes, reclamam da violação de direitos
  - Toda reclamação é enviada ao administrador da rede, via SGIS/CAIS, para análise e resposta ao reclamante
  - De acordo com a Política de Uso da RNP, não é permitido distribuir conteúdo protegido por direitos autorais "*transgressão dos direitos do autor.*"

https://www.rnp.br/sites/default/files/politica-uso-rede-ipe_0.pdf

Evidentiary Information:
Protocol: BITTORRENT
Infringed Work: South Park: Bigger Longer & Uncut
Infringing FileName: South Park - Filme (1999) 720p Legenda Embutida ramonTPB
Infringing FileSize: 705277671
Infringer's IP Address: 200.135.X.X
Infringer's Port: 3792
Initial Infringement Timestamp: 2016-09-23T00:07:53Z **(horário UTC)**

Ações principais:

- **Ao usar NAT, é importante registrar os *logs* de conexões para relacionar o usuário, IP, porta e protocolo utilizado juntamente com o horário**
- **Criação e Divulgação de uma Políticas de Uso da Rede**
- **Firewalls de mercado com Deep Packet Inspection podem identificar, através de assinatura, uma comunicação Torrent e bloqueá-la**

Importância do *log* na identificação e resolução de incidentes

O monitoramento de *logs* do firewall (ou outro dispositivos) é muito importante para identificar atividades suspeitas na rede ou um comportamento anômalo:

- Máquinas comprometidas na rede interna
- Tentativas de invasão de agentes externos (*scan*, força bruta, etc)
- Traduções de NAT (identificação do responsável por incidentes)

Os logs devem ter o principal propósito de alertar para ações preventivas que devem ser tomadas, porém também servem para análise posterior de problemas e incidentes.

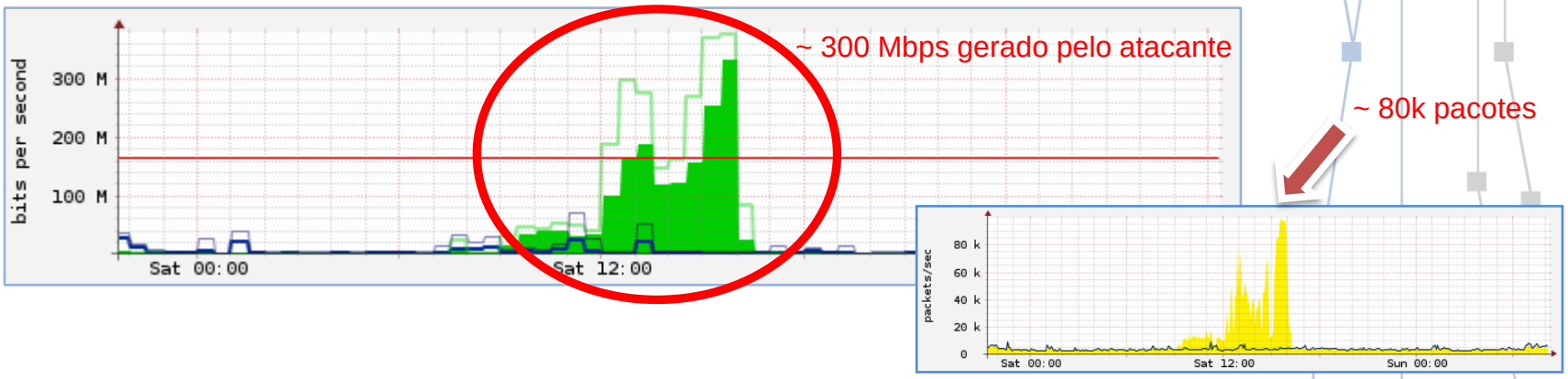
Quando você sabe o que é normal em sua rede, é possível identificar facilmente eventos anômalos.

Dica: enviar os *logs* de firewall, roteador, switch, servidor, etc para um ambiente centralizado, via *syslog,* para possibilitar a análise, tratamento e geração de alertas.

Importância da resolução dos incidentes

Ao receber a notificação de que um *host* na rede está vulnerável, é importante que sejam tomadas as medidas para correção do problema. A inobservância deste fato pode trazer grandes problemas para a instituição, desde a indisponibilização de serviços até roubo de informações.

Abaixo um exemplo onde uma máquina foi comprometida pelo atacante e serviu para realização de ataques de negação de serviço.



Date first seen	Duration	Src IP Addr	Dst IP Addr	Dst Pt	Proto	Packets	Bytes	bps	Bpp	Flows
2016-09-17 13:13:06.712	1205.102	200.135.X.Y	109.236.X.Y	48213	UDP	27.6 M	13.3 G	88.5 M	481	592
2016-09-17 13:13:06.712	1205.102	200.135.X.Y	109.236.X.Y	49305	UDP	21.9 M	10.6 G	70.2 M	481	447
2016-09-17 13:13:05.712	1206.102	200.135.X.Y	109.236.X.Y	57811	UDP	20.7 M	10.0 G	66.3 M	481	428

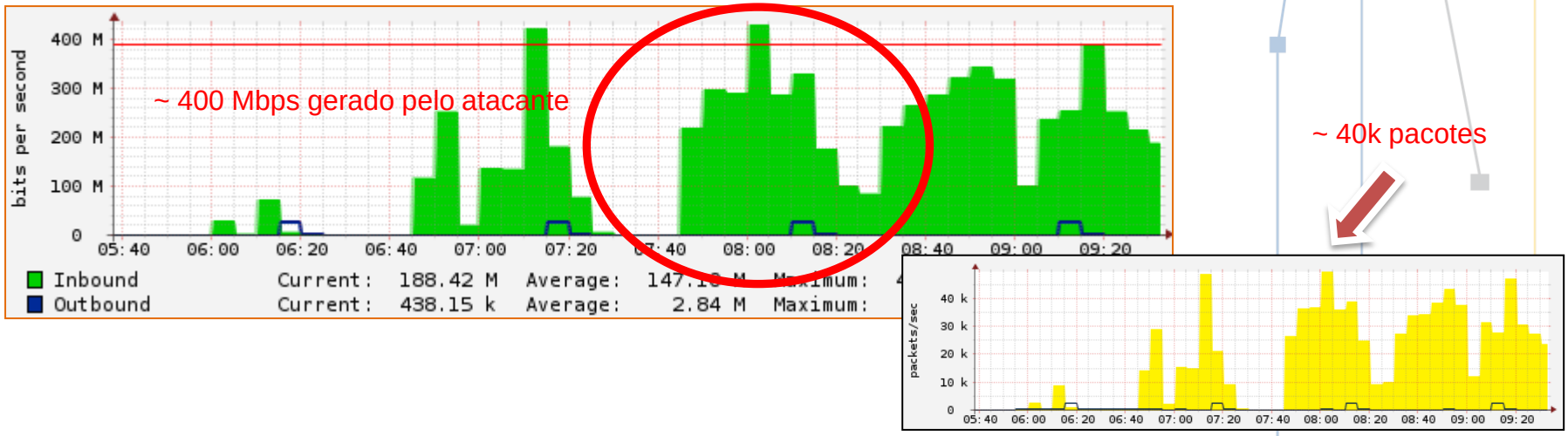
Os dados acima foram anonimizados

Importância de manter um software atualizado

Vulnerabilidades de aplicações WEB também são bastante comuns. Neste incidente, foi verificado que havia uma brecha no Zabbix 3.0.1 que permitia a injeção de código malicioso por SQL injection:

- [ZBX-11023] fixed SQL injection vulnerability in "Latest data" page; thanks to 1N3 at Early Warning Services, LLC

Através da interface de administração do Zabbix, foi executado SQL Inject de forma a conseguir acesso à interface de administração. Com acesso à área de administração, o Zabbix permitiu a execução de comandos no console. A partir do momento que o invasor teve acesso ao console, implantou então um binário e iniciou a geração de tráfego para ataques de DDoS.



Os dados acima foram anonimizados

Ataque DDoS e a internet das coisas

- Ataque ao site KrebsOnSecurity em 20/09/2016
- Tráfego aproximado gerado neste ataque: 665 Gbps
  - Utilizando principalmente câmeras, DVRs, etc
  - Não foi utilizado o método de amplificação
- *Akamai* mitigou o ataque e manteve o site em operação

21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

Fonte: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos

Boas práticas a serem adotadas (BCPs)

- BCP 38 - Impedindo ataques de negação de serviço que utilizam falsificação de endereços IP de origem (*spoofing*)
- BCP 55 - Diretrizes para coleta e armazenamento de provas
- BCP 162 - Recomendações de armazenamento de logs em servidores conectados à Internet
- BCP 140 - Prevenindo o uso de servidores de nomes recursivos em ataques de amplificação
- BCP 194 - Operações de BGP e Segurança
- BCP 199 - DHCPv6: Protegendo contra servidores DHCPv6 não autorizados

Maiores informações: **www.pop-sc.rnp.br e https://tools.ietf.org/html**

Ferramentas interessantes

- Log de NAT
  - Linux: http://conntrack-tools.netfilter.org
  - pfSense: https://github.com/italovalcy/pfnattrack
- Ferramentas de monitoramento de ameaças
  - IDS/IPS
    - Snort
    - Suricata
- Análise de fluxos
  - NTOP
  - NFDump
- Scan
  - NMAP

Conclusão

- Para manter uma rede segura:
  - Ações preventivas (implementação de políticas de segurança, atualização de softwares, regras de firewall, *logs*, etc...)
  - Ações corretivas (correção de vulnerabilidades, etc)
  - Monitoramento da rede (sensores de ataque, análise de fluxos, *logs* de sistema, etc)

“A segurança de toda a rede depende de cada um fazer a sua parte”

“Uma corrente é tão forte quanto seu elo mais fraco”

Caso de uso

- IFC Videira
  - Identificação do responsável por infringir direitos autorais de filme

Próximas Apresentações

http://www.pop-sc.rnp.br/seminarios/agenda.php

(**05/10/2016**) – Quarta-Feira

Horário	Descrição	Apresentador
09:00	**RCT/FAPESC - Panorama, Ações e Investimentos**	Juarez Lopes (FAPESC)
10:30	**REMEP - Panorama, Ações e Investimentos**	Edison Tadeu Lopes Melo (UFSC/REMEP)
14:00	**Iniciativas Instituições - Panorama, Ações e Investimentos**	Várias Instituições
16:30	**Serviços RNP**	Helder Vitorino / Jean Carlo Faustino (RNP)

Obrigado!

Rodrigo Pescador

Rede Nacional de Ensino e Pesquisa – RNP

Ponto de Presença da RNP em Santa Catarina - PoP-SC

Universidade Federal de Santa Catarina – UFSC

REMEP Florianópolis

PoP-SC

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**