Desafios no Tratamento de Incidentes de Segurança

Klaus Steding-Jessen
jessen@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto br
Comitê Gestor da Internet no Brasil

Sobre o CERT.br

Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil

FIRST Improving Security Together MEMBER

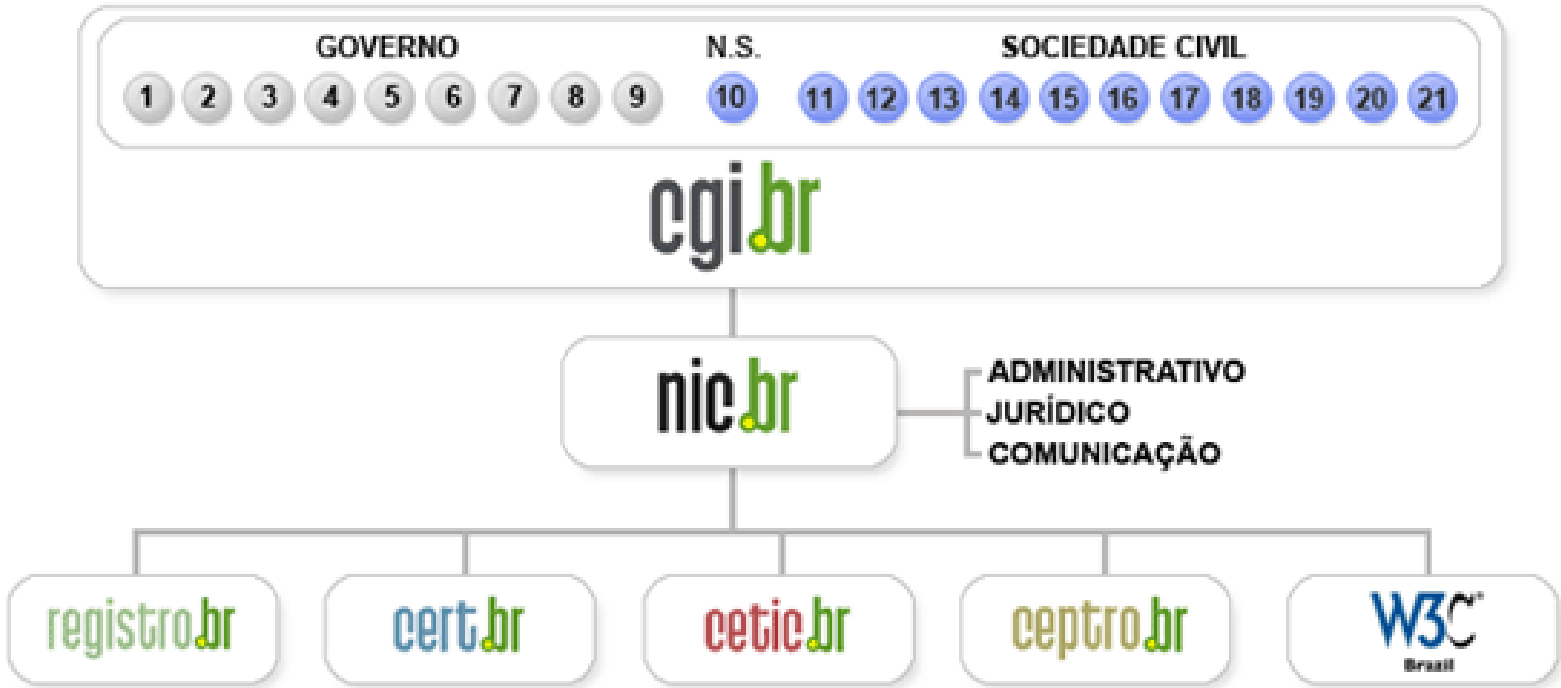
APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner CERT Courses

The Honeynet PROJECT

http://www.cert.br/sobre/

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério do Planejamento, Orçamento e Gestão
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério da Defesa
07- Agência Nacional de Telecomunicações
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando `<.br>`
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas**

Agenda

Motivação

Fraude com Geolocalização

NAT

IPv6

Referências

Motivação

Motivação

Alguns desafios atuais no tratamento de incidentes:

- Ataques mais complexos
  - ferramentas (complexas) prontas
  - grande número de máquinas servindo de base de ataques
  - atacantes usando ofuscação
- Volume de trabalho
- Riscos do excesso de automatização
  - perda de credibilidade
- Mudanças na Internet
  - CGNs
  - IPv6

Fraude com Geolocalização

Fraude com Geolocalização

Uso de Geolocalização na fraude:

- Prover diferentes conteúdos em função da rede de origem
- Por exemplo, se a vítima acessa uma página de um IP alocado para o Brasil, a fraude é visível
- Para outras redes (inclusive a rede hospedando o conteúdo) a fraude não é visível
- Dificulta o processo de remoção do conteúdo

Geolocalização: Exemplo de htaccess (1/2)

```
<limit GET POST PUT>
order deny,allow
deny from all
allow from 187.0.0.0/8
allow from 189.0.0.0/8
allow from 200.0.0.0/8
allow from 201.0.0.0/8
allow from 177.0.0.0/8
allow from 188.0.0.0/8
allow from 202.0.0.0/8
allow from 199.0.0.0/8
</limit>
```

Geolocalização: Exemplo de htaccess (2/2)

```
<Files 403.shtml>
order deny,allow
</Files>
ErrorDocument 404 /misc/404page.php
allow from 139.82.0.0/16
allow from 143.54.0.0/16
allow from 143.106.0.0/16
allow from 143.107.0.0/16
allow from 143.108.0.0/16
allow from 144.23.0.0/16
allow from 146.134.0.0/16
allow from 146.164.0.0/16
allow from 147.65.0.0/16
allow from 150.161.0.0/16
allow from 150.162.0.0/16
allow from 150.163.0.0/16
allow from 150.164.0.0/16
allow from 150.165.0.0/16
allow from 152.84.0.0/16
allow from 152.92.0.0/16
allow from 155.211.0.0/16

[mais 255 redes omitidas...]
```

Geolocalização: Phishing e Trojans

- 20% dos phishings tratados pelo CERT.br já usam algum esquema de geolocalização
- O time de abuse não consegue “visualizar” a página e não se convence do problema
- Requer um esforço maior de notificação
  - explicar o problema de geolocalização
  - ênfase no sistemas de arquivos, não no que está visível online
- Começando a ficar comum em trojans também

Geolocalização: Sugestões

- É fundamental um texto claro de notificação que explique o problema
- Uma infraestrutura de proxies com:
  - IPs alocados para o Brasil
  - IPs no exterior

NAT

NAT: problemas

- Dificuldade em identificar máquinas comprometidas:

  “Esse IP é o do meu NAT: não tenho como chegar na máquina infectada, vou bloquear a rede do reclamante. . .”

- Falsa sensação de segurança

- Falta de estímulo para adoção de soluções mais robustas: AS próprio, conexão com PTTs, maior espaço de endereçamento, independência de operadoras

IPv6

IPv6: Treinamento da Equipe

- Familiarização com o protocolo
- Entender possíveis riscos para a organização:
  - túneis “automágicos” (Vista, Windows 7, etc)
  - comportamento IPv4 diferente do IPv6. Por exemplo, firewall IPv4 ativo, mas desativado para IPv6
  - funcionalidade IPv6 inexistente. Por exemplo, netflow v5 suporta apenas IPv4

IPv6: Tratamento de Incidentes

```
# begin logs
xxxx:xxxx:2019::141:29 - - [26/Aug/2012:07:19:14 -0300] \
"GET /awstats/awstats.pl HTTP/1.0" 404 7488 "-"
# end logs
```

Questões como:

- scripts / ferramentas / etc
- validação de “endereço IP”
- contatos de redes IPv6
- banco de dados (por exemplo, MySQL x PostgreSQL)

IPv6: Logs com Porta de Origem (1/2)

- Cenário de transição IPv4 $\rightarrow$ IPv6
  - serão necessários mecanismos de tradução IPv4 $\rightarrow$ IPv6 e IPv6 $\rightarrow$ IPv4
  - mecanismos de tradução implicam no compartilhamento de endereços IP entre diversos usuários
  - teles planejam usar CGNs (*Carrier Grade Nats*) no espaço IPv4 restante
- **Problema**: não será suficiente apenas a informação de data/hora e IP de origem. Será necessário também a porta de origem.
- Necessidade de registrar porta de origem em todos os serviços online

IPv6: Logs com Porta de Origem (2/2)

Realizou-se uma reunião em 11/07 com Operadores da Justiça, teles, e provedores para discutir esse cenário

Documentos adicionais:

- RFC 6302: Logging Recommendations for Internet-Facing Servers
  http://www.ietf.org/rfc/rfc6302.txt

- RFC 6692: Source Ports in Abuse Reporting Format (ARF) Reports
  http://www.ietf.org/rfc/rfc6692.txt

Referências

- Esta apresentação pode ser encontrada em:
  http://www.cert.br/docs/palestras/
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.nic.br/
- Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil – CERT.br
  http://www.cert.br/