nic.br cgi.br | cert.br

4º Fórum Brasileiro de CSIRTs
São Paulo, SP
18 de setembro de 2015

Perspectivas e Desafios para 2016

Cristine Hoepers
cristine@cert.br

Klaus Steding-Jessen
jessen@cert.br

cert.br nic.br cgi.br

O que mudou em 2015?

Como isso pode afetar 2016?

Como NÓS podemos

fazer o cenário melhor?

Cenário de *Malware*

- **RAT (*Remote Access Trojan*) se tornou o tipo mais comum de *malware* usado**
- ***"Government Grade Malware for the Masses"***
  - **Com o vazamento do *Hacking Team*, o código fonte ficou disponível para todos os tipos de atacantes**
  - **Código multiplataforma:**
    - ***"Windows*, *Windows Phone*, *Windows Mobile*, *Mac OSX*, *iOS*, *Linux*, *Android*, *BlackBerry OS*, and *Symbian*"**
- ***Ramsomware* em amplo uso**
  - **agora também para Android**
- **Descoberta de vulnerabilidades em ampla expansão para dispositivos móveis**
  - **Exemplo: StageFright**

Roteadores Domésticos (CPEs)

- **Enorme base vulnerável**
  - **sem instalação de *patches***
  - **configurações padrão de fábrica com serviços com senha padrão, serviços como Telnet habilitados, etc**
  - **serviços UDP permitindo abuso para amplificação**
    - **como SNMP, SSDP, DNS recursivo aberto**

- **Usados para todos os tipos de ataque**
  - ***botnets* para DDoS**
  - ***botnets* para mineração de *bitcoins***
  - **comprometimento para alteração de DNS**
    - **via CSRF ou via Telnet**
    - **alteração leva a ataques de *phishing* ou para induzir a baixar *malware***

DDoS

- **Ataques com amplificação são triviais**
- **Ataques dificilmente são menores que 50Gbps**
  - **vários ocorrendo no Brasil**
  - **internacionalmente DD4BC atacando instituições financeiras, realizando extorsão com pagamento via *bitcoin***
- **Mitigação é realmente difícil**
  - **técnicas de mitigação tem que levar em conta questões de privacidade e possibilidade de descarte de tráfego legítimo**

- **Lições aprendidas da Copa 2014, que nos apontam para desafios adicionais em 2016**
  - **Olimpíadas/Manifestações**
  - **Alvos difusos**
  - **Criminosos se transfiguram em "*hacktivistas*"**

Como NÓS podemos fazer o cenário melhor?

cert.br nic.br cgi.br

Precisamos um ecossitema mais saudável

Nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança ou a resposta a incidentes - todos possuem um papel

- **administradores de redes e sistemas**
  - **não emanar "sujeira" de suas redes e adotar boas práticas**
  - **Exemplo: implementar BCP38 (http://bcp.nic.br/), implementar gerência de porta 25; notificar usuários sobre infecções e indícios de comprometimento**
- **usuários**
  - **entender os riscos e seguir as dicas de segurança**
  - **manter seus dispositivos atualizados e tratar infecções**
- **desenvolvedores**
  - **precisam pensar em segurança desde o início**

Ainda assim incidentes ocorrerão

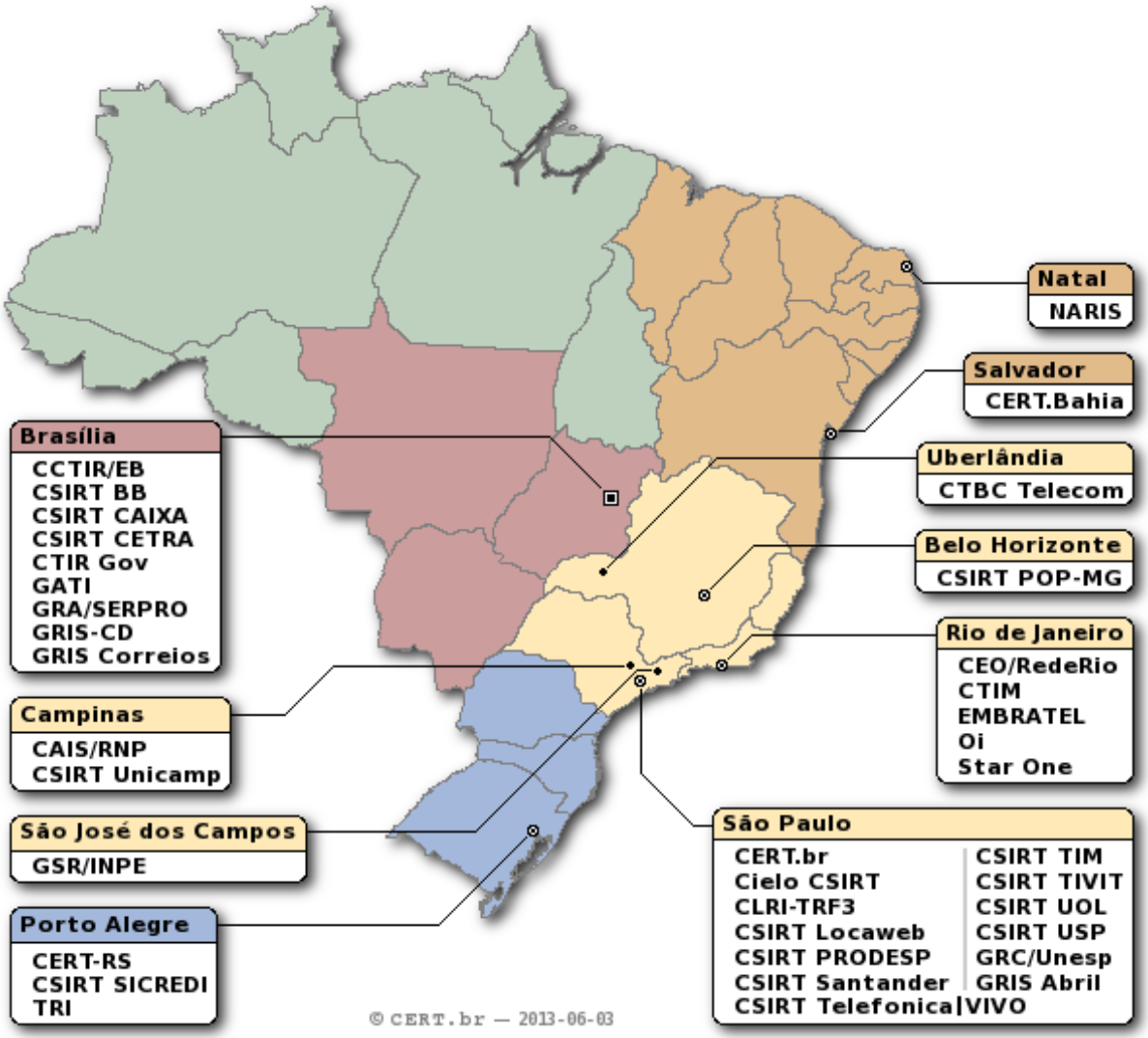
Cooperação no Tratamento de Incidentes

- **Redução de impactos é grande se a atuação é rápida**
- **Necessários profissionais habilitados e CSIRTs estabelecidos**
- **Cooperação é fundamental**
  - **nacional e internacionalmente**
- **Publique os dados de contato para notificações de incidentes**
- **Compartilhe sempre que possível**
  - **técnicas**
  - **tendências**
  - **dados anonimizados**

Grupos de Tratamento de Incidentes Brasileiros

37 times com serviços anunciados ao público

Público Alvo	CSIRTs
Qualquer Rede no País	CERT.br
Governo	CTIR Gov, CCTIR/EB, CLRI-TRF-3, CSIRT PRODESP, GATI, GRA/SERPRO, GRIS-CD, CSIRT CETRA, GRIS Correios
Setor Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, CSIRT Telefonica|VIVO, CSIRT Locaweb, CSIRT TIM, CSIRT UOL, StarOne, Oi,
Academia	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CEO/RedeRio, CERT.Bahia, CSIRT USP, GRC/UNESP, TRI
Outros	CSIRT TIVIT, GRIS Abril



http://www.cert.br/csirts/brasil/

Materiais de Apoio para Todos

cert.br nic.br cgi.br

www.cert.br/docs/whitepapers/notificacoes/

Ir para o conteúdo

Núcleo de Informação e Coordenação do Ponto BR

English

CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTRO.br - W3C.br

Imprensa

cert.br 15 anos

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

- Sobre o CERT.br
- CSIRTs
- Estatísticas
- Cursos
- Projetos
- Publicações
- Palestras
- Links
- FAQ
- Mapa do site
- Contato
- Twitter
- RSS

Busca

ok

Buscar em CERT.br

W3C XHTML 1.0 W3C CSS

Acessibilidade do site

Você está em: CERT.br > Publicações > Recomendações para Notificações de Incidentes de Segurança

Recomendações para Notificações de Incidentes de Segurança

Autor: CERT.br
Versão: 1.0 -- 09/06/2015

Sumário

1. Importância da notificação de incidentes de segurança
2. O que notificar
3. A quem notificar
4. Buscando contatos
5. Formas e formato de notificar
6. O que incluir na notificação
7. Exemplos de consultas WHOIS

8. Modelos de notificações
   - 10 casos típicos de incidentes
   - variáveis de texto para simples substituição
   - download de arquivo .txt para diversos *encodings*
   - nos idiomas pt-br e en-us

Cartilha de Segurança para Internet

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

- **Livro (PDF e ePub) e conteúdo no *site* (HTML5)**
- **Dica do dia no *site*, via *Twitter* e RSS**
- **Impressões em pequena escala enviadas a escolas e centros de inclusão digital**
- **Uso por instituições para treinar funcionários**

http://cartilha.cert.br/

Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- Redes Sociais
- Senhas
- Comércio Eletrônico
- Privacidade
- Dispositivos Móveis
- *Internet Banking*
- Computadores
- Códigos Maliciosos
- Verificação em Duas Etapas
- Redes

Acompanhados de *slides* de uso livre para:

- ministrar palestras e treinamentos
- complementar conteúdos de aulas

Outros Materiais para Usuários Finais

Portal Internet Segura

- Reúne todas as iniciativas conhecidas de educação de usuários no Brasil, que possuam material *online*

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/

Iniciativas de Incentivo a Boas Práticas

- **Recomendações para Notificações de Incidentes de Segurança**

  http://www.cert.br/docs/whitepapers/notificacoes/
- **Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos**

  http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/
- **Sugestões para defesa contra ataques de força bruta para SSH**

  http://www.cert.br/docs/whitepapers/defesa-forca-bruta-ssh/
- **Práticas Anti-Spam**

  http://antispam.br/admin/
- **DNSSEC, para segurança do sistema de nomes (DNS)**

  http://registro.br/tecnologia/dnssec.html?secao=dnssec
- **Cursos de IPv6 e de boas práticas em administração de sistemas autônomos**

  http://ipv6.br/calendario/
- **Cursos de Tratamento de Incidentes**

  http://www.cert.br/cursos/

Eventos para Fomentar a Cooperação

Eventos gratuitos organizados pelo NIC.br:

- **Grupo de Trabalho de Engenharia e Operação de Redes (GTER)**
- **Grupo de Trabalho em Segurança de Redes (GTS)**
- **Fórum da Internet no Brasil**
- **Seminário de Proteção à Privacidade e aos Dados Pessoais**
- **Fórum Brasileiro de CSIRTs**
- **Conferência Web W3C Brasil**
- **Semana de Infraestrutura da Internet no Brasil**
  - **PTT Fórum - Encontro dos Sistemas Autônomos da Internet no Brasil**
  - **Fórum IPv6**
  - **GTER/GTS**

http://nic.br/eventos/agenda/organiza/

Obrigado

www.cert.br

cristine@cert.br jessen@cert.br @certbr

18 de setembro de 2015

nic.br cgi.br

www.nic.br | www.cgi.br