MODULO Solutions for GRC
Governance, Risk and Compliance | 25 Years

Reunião GTS-15
Maio 2010

Identificando a existência de páginas falsas na Internet.

Alexandre Domingos
adomingo@modulo.com.br

Edney Gará
egara@modulo.com.br

Agenda

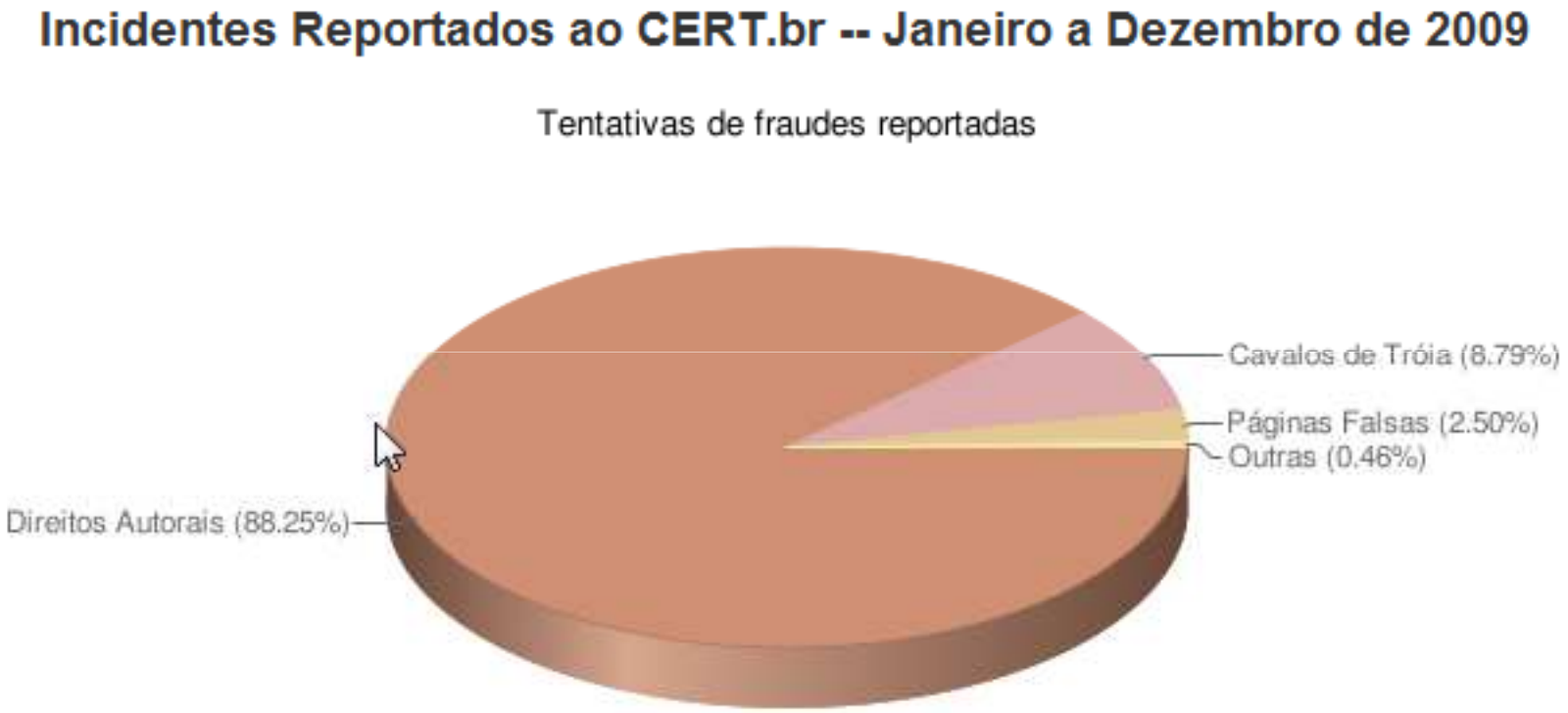
- Qual o objetivo de uma página falsa?
- Panorama das fraudes
- Anatomia de uma página falsa
- Análise de logs para identificação de páginas falsas
- Apresentação de um resultado prático
- Automatizando a identificação de páginas falsas
- Considerações finais

Qual o objetivo de uma página falsa?

Furto de Identidade → Fraudes

Fonte: http://info.abril.com.br

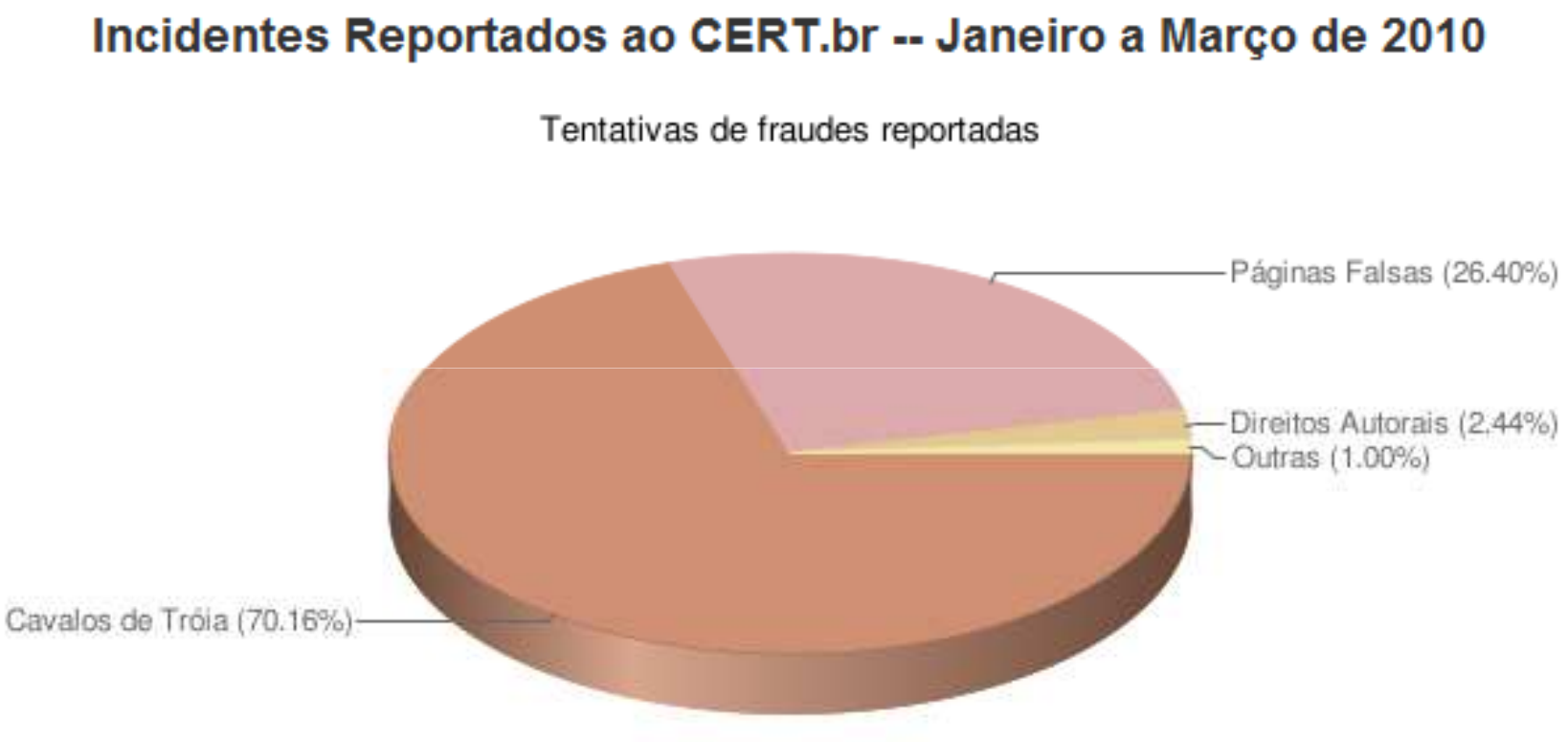
Panorama das fraudes



Aproximadamente 5007 páginas falsas reportadas

Fonte: cert.br

Panorama das fraudes



Aproximadamente 2180 páginas falsas reportadas

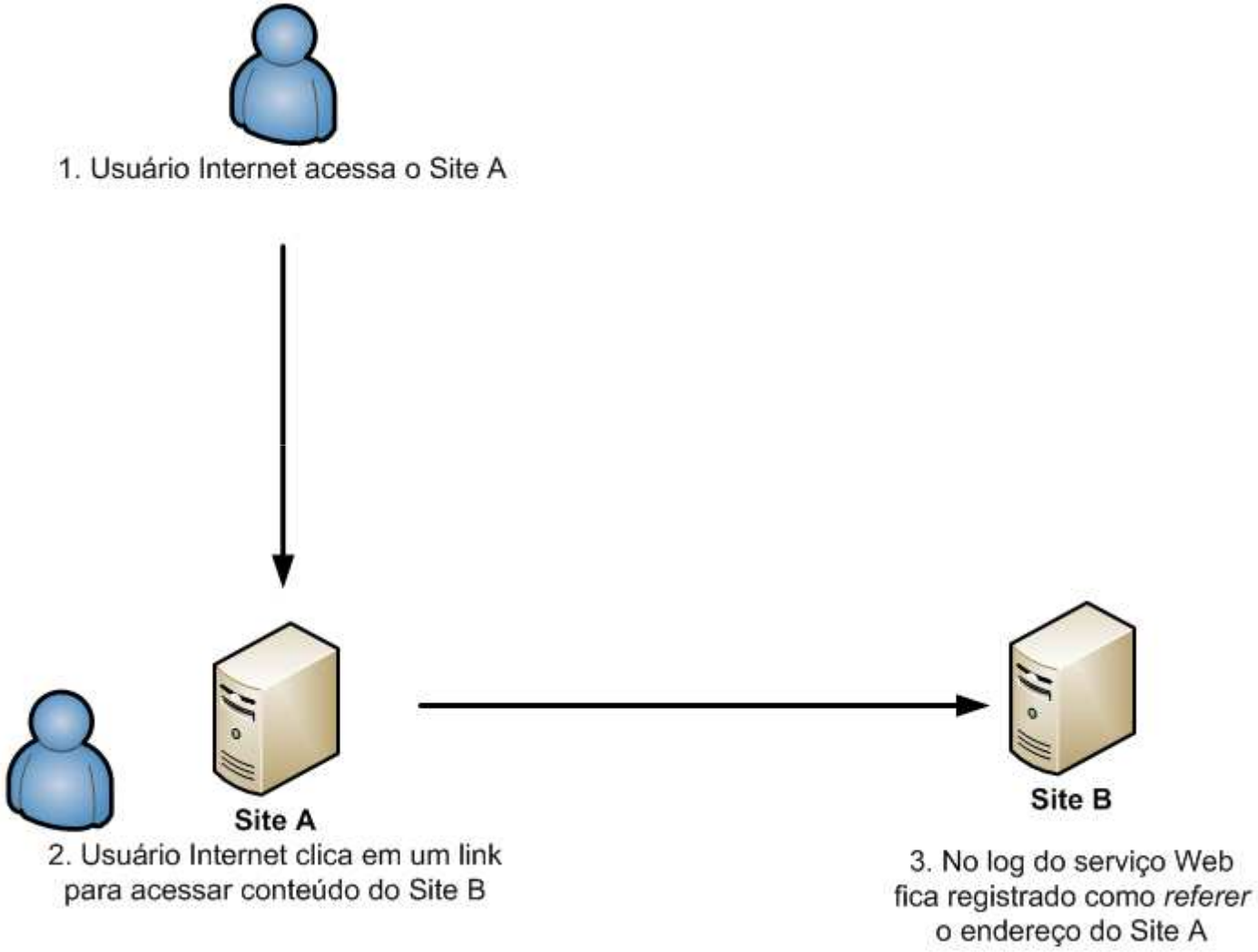
Fonte: cert.br

Em que momento você é notificado da existência de uma página falsa da sua empresa ou instituição?

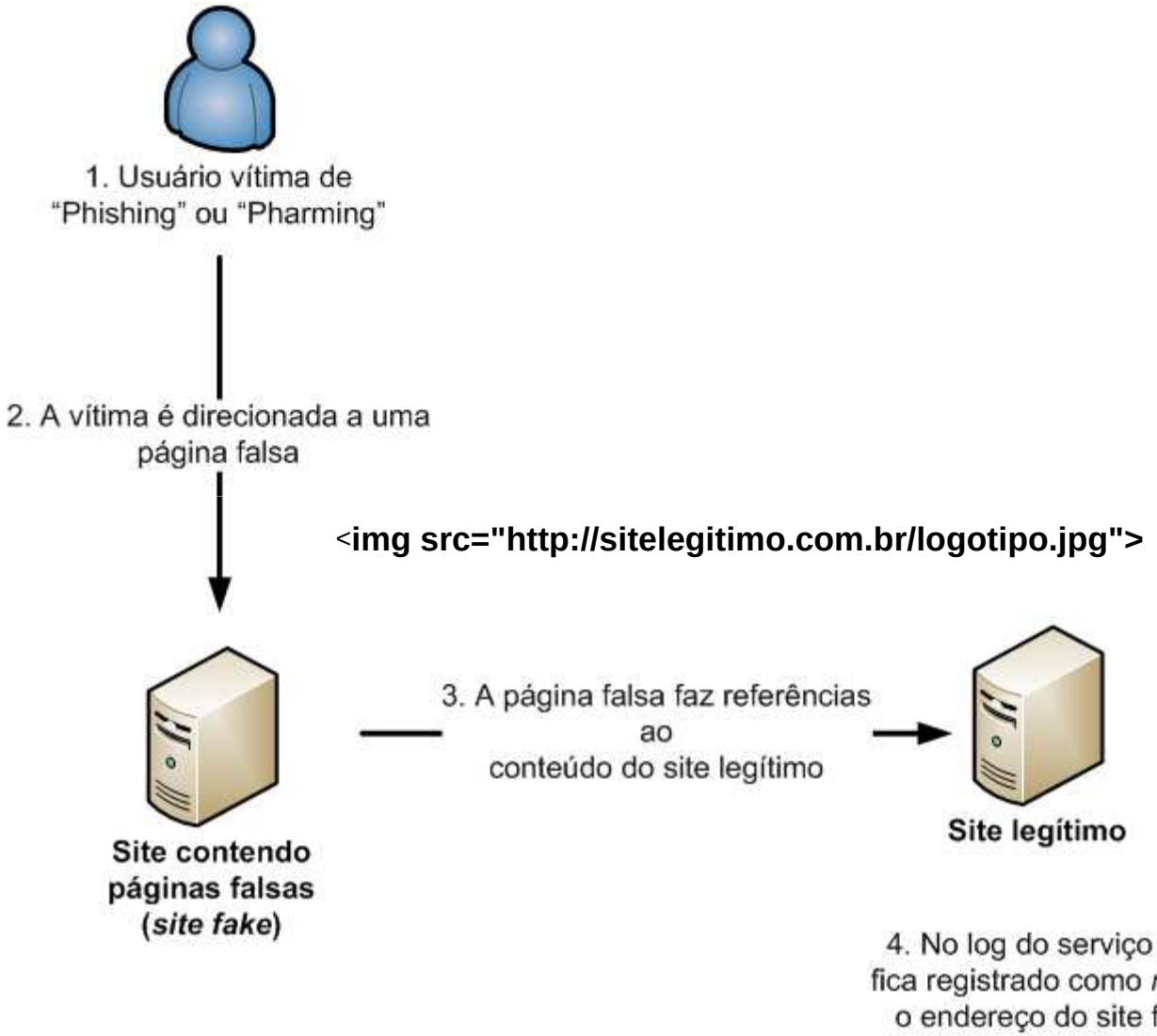
MODULO Solutions for GRC
Governance, Risk and Compliance
25 Years

Como identificar a existência de páginas falsas de forma pró-ativa?

Como funciona o “HTTP Referer”



Anatomia de uma página falsa



Analisando os logs para identificação de páginas falsas

- Foco no campo *referer:*
  - Páginas falsas: tráfego excessivo a partir de um único endereço IP.
- Refinar a busca:
  - Vários sites confiáveis podem fazer referência ao logo do seu site, a conteúdo específico;
  - Páginas falsas referenciam conteúdo, figuras, *flash*,de forma diferenciada;
  - Avaliar o comportamento do tráfego, definindo-se um *baseline* do comportamento normal de acesso ao seu site;
  - Tudo que for diferente do *baseline*, do normal, é suspeito e deve ser devidamente tratado.

Resultado de uma aplicação prática

- Identificação de uma média de 10 *sites fakes*/mês.
  - Não consideramos nessa média os casos de reincidência, ou seja, aqueles fraudadores que, uma vez tendo seu site indisponibilizado, hospedaram em outro provedor.
- Identificação de *sites fakes* em tempo de desenvolvimento.
  - Em tempo de desenvolvimento, o desenvolvedor "fraudador" fazia referência ao site alvo, identificado antes de colocar em "produção".
- **A identificação pró-ativa das páginas falsas, antes dos usuários alvos, contribuiu para a redução de fraudes.**

Automatizando a identificação de páginas falsas

- Avalie o que você tem em casa:
  - Analisadores estatísticos de *log:*
    - Webtrends;
    - AWSTATS;
    - Outros.
  - Ferramentas SIEM (correlação de logs):
    - Vantagem de uma identificação on-line.

- Desenvolva scripts para automatizar as análises dos logs, gerando contadores para o *referer,* refinando o script para diferenciar tráfego normal de tráfego suspeito.

Como habilitar o *referer*

- Por default, o *referer* não é habilitado para ser registrado no log.

- Para habilitar o *referer*:
  - Microsoft IIS: selecionar o campo *Referrer* nas configurações do log.
  - Apache: ativar o *Combinet Log Format*, que inclui o campo Referrer.

Considerações finais

- Analisar o *referer* está longe de ser a solução final para identificação de páginas falsas.
- A proposta apresentada visa somar a outros controles, aproveitando em muitos casos, uma infraestrutura existente como analisadores e correlacionadores de logs.
- Os logs dos serviços Web são fontes valiosas de informações que devem ser muito exploradas pelas áreas de monitoração de segurança.
- Identificar mudanças no comportamento do tráfego de forma pró-ativa, contribuirá sempre para uma resposta mais eficiente dos incidentes de segurança.

Referências bibliográficas

- Header Field Definitions
  - http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html
- CANTINA: A Content-Based Approach to Detecting Phishing Web Sites
  - www2007.org/papers/paper557.pdf
- Cert.br - Estatísticas de incidentes
  - www.cert.br
- APWG - Global Phishing Survey: Domain Name Use and Trends in 2H2009
  - http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf

Perguntas?

MODULO Solutions for GRC
Governance, Risk and Compliance | 25 Years

Reunião GTS-15
Maio 2010

Identificando a existência de páginas falsas na Internet.

Alexandre Domingos
adomingo@modulo.com.br

Edney Gará
egara@modulo.com.br