**Relatório de Levantamento de Situação**

**Problema:** Invasão do site [www.cpb.org.br](http://www.cpb.org.br), gerando páginas e comentários com phishing, causando a suspensão do site no servidor de hospedagem.

**Principais características encontradas:**

* Foi detectada a criação de comentários e “posts” no site, que ficavam disponíveis em sites de busca. Essas páginas, continham links maliciosos. As páginas e links são gravadas em banco. A invasão ocorreu somente na pasta do novo site (site2014), que é para onde o endereço principal aponta. Não foi identificado arquivo malicioso.
* Esse tipo de ataque ocorre por falha de segurança na senha do administrador do WordPress. Essa senha é definida pela equipe de desenvolvimento do site. Não foi identificado nenhuma invasão por FTP, o que descarta invasão direta do servidor.
* A pasta infectada é a site2014/ e o banco de dados cpb112
* Foi identificado como data marco, 29/11/2014 como início dos POSTs maliciosos, que duraram cerca de 3 semanas, de Batons da marca MAC, porém, após isso, os ataques cessaram.
* A suspensão foi um ato da Locaweb, visando segurança, de acordo com o informado.

**Relatório de ações para limpeza do site:**

* 24/04/2015 16:30:00 – Iniciado a análise do problema diretamente no servidor.
* 24/04/2015 17:00:00 – Identificado que todos os acessos do site estavam suspensos pela Locaweb, restando apenas o acesso ao Banco de Dados e FTP, o que dificultou o processo de identificação do problema.
* 24/04/2015 18:00:00 – Realizado o processo de backup do banco de dados
* 24/04/2015 18:15:00 – Iniciado Backup de todos os arquivos do servidor (57 Gigabites)
* 25/04/2015 14:30:00 – Concluído o backup dos arquivos do servidor
* 25/04/2015 14:30:00 – Iniciado o processo de limpeza do site
  + 14:40:00 – Recuperando o backup do banco de dados - Necessário o backup ser feito por tabela e em partes, tendo em vista q necessidade de limpar alguns dados maliciosos e falhas. Dessa forma, a recuperação do backup foi feito de forma manual, analisando blocos de registros. O backup possuía mais de 600mil registros de inserção.
  + 20:00:00 – Testando site em ambiente local
  + 20:50:00 – Identificado que instalação do site não roda localmente
  + 21:30:00 – Efetuado a limpeza de todos os arquivos e iniciado o upload para a hospedagem
* 25/04/2015 21:40:00 – Atualizado o chamado junto a Locaweb, solicitando urgência na liberação do ambiente, informando todos os passos feitos. Prazo dado: 27/04/2015