## Universidade Federal Rural de Pernambuco Sistemas de Informação Segurança e Auditoria de Sistemas Lhaíslla Eduarda Cavalcanti Rodrigues da Silva RECIFE-PE

2022

**Como um ataque utilizando BHO pode acontecer?**  
  
 Browser Helper Objects são DLLS que funcionam como plug-ins do Internet Explorer podendo ver(e alterar) todos os dados que trafegam entre o computador e um servidor web. Nem todos são, necessariamente, maliciosos, mas são muito usados para construir em cavalos-de-tróia e spyware  
 O ataque utilizando BHO normalmente acontece quando um BHO é instalado por um programa de terceiros para aprimorar a funcionalidade do navegador da web. Podem ser instalados sem o conhecimento do usuário e por serem programas, eles podem fazer qualquer coisa que outros programas fazem. O que pode permitir que um BHO seja utilizado para acessar informações sigilosas de um um usuário, que fica mais vulnerável uma vez que não há uma maneira fácil de listar os BHOs ​​instalados no PC.Um ataque utilizando BHO funciona da seguinte maneira: um BHO mal intencionado intercepta todas as comunicações entre o navegador do usuário e o servidor web de destino, em seguida altera, instantaneamente, as mensagens ou as transações web do usuário conforme elas ocorrerem.

**Exemplo de ataque BHO:**

* Quando o BHO fraudulento vê a página da conta onde o dinheiro está sendo transferido, ele registra um manipulador de eventos de botão.
* O BHO fraudulento envia o formulário corrompido para o servidor.
* Um usuário visita o site de seu banco e navega até a página de transferência de conta.
* Esse processo resulta na vítima, sem saber, autorizando uma transferência de dinheiro para a conta designada do hacker!
* A extensão BHO intercepta todas as solicitações e respostas que aparecem no site.
* Quando o usuário recebe um formulário de confirmação para aprovação, o BHO fraudulento analisa e troca os dados originais de volta no formulário.
* Quando o usuário finaliza uma transferência, a extensão extrai todos os dados dos campos das páginas da web e os substitui por informações e valores diferentes.
* O usuário aprova o formulário de confirmação, então o BHO fraudulento troca de volta às informações e o valor fraudulento.
* O BHO fraudulento envia o formulário corrompido para o servidor.
* O servidor processa a transferência com os dados corrompidos.

A ação de um ataque BHO se dá por meio de um módulo projetado para interceptar e substituir páginas no navegador internet explorer.Como identificado nos exemplos, todos os dados foram trocados pelo BHO fraudulento, o que torna muito difícil para a vítima provar que não é a transação que ele aprovou. Outro problema para a vítima é que essa transação foi hackeada antes da criptografia de transmissão SSL / TLS.

**Referências**

<https://minutodaseguranca.blog.br/usando-tecnicas-de-smokescreen-hacker-roubam-us10m-do-banco-do-chile/>

<https://www.mtitecnologia.com.br/seguranca-da-informacao-como-foi-o-ataque-dos-sistemas-de-um-grande-banco-chileno/>

<https://www.banrisul.com.br/bob/data/TiposdeAtaques.pdf>

<https://pt.wikipedia.org/wiki/Amea%C3%A7as_a_computadores#BHOs>