Como eu capturo e obstruo os hiperlinks encaixados que têm executáveis?

Índice

Pergunta

Como eu capturo e obstruo os hiperlinks encaixados que têm executáveis?

Resposta

Você pode usar um filtro da mensagem para fazer a varredura do corpo e de todos os acessórios HTML. Geralmente, estes email entram através dos email HTML. Para que o motor da exploração detecte-o, você deve usar corpo-contém a circunstância. Se você processa somente o correio de partida, a seguir você pode usar-se “somente-corpo-contém” a circunstância.

O filtro do seguinte mensagem procurará todo o hiperlink do comprimento esse extremidades com um executável. Uma vez que a circunstância é estada conforme, duas ações ativarão. A primeira ação será notificar o administrador local enviando um email a admin@example.com.

O segundo será uma ação final de deixar cair o email. O email não precisa de ser gota, mas pelo contrário pode ser quarantined. Removendo a ação abaixo do “`drop(); `” pode ser substituído com a ação “da `quarentena (“política "); ".`

A quarentena deve ser definida, se não o motor do filtro não permitirá o filtro. Você pode ou usar a quarentena da política padrão, ou crie sua própria quarentena (refira por favor quarentena no manual para criar ou suprimir de quarentena).

```
Block_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
notify ("admin@example.com");
drop();
}
```

Você pode igualmente usar esta versão que removeu as URL ruins do corpo e substituídas lhes com a URL REMOVIDAS.

```
remove_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
edit-body-text("://\\S*\\.exe(\\s|\\b|$)", "URL REMOVED");
}
```

Para instruções do detalhe em como entrar em um filtro da mensagem, reveja por favor como eu adiciono um filtro novo da mensagem a meu dispositivo de Cisco IronPort?

Refira por favor o GUIA de USUÁRIO AVANÇADO do de Cisco ESA AsyncOS para que o reforço de política chamado seção das ferramentas de segurança do email rever filtros da mensagem.