Filtração falsificado do correio ESA

Índice

Introdução

Este documento descreve um problema que seja encontrado na ferramenta de segurança do email de Cisco (ESA) quando o Spam e o email fraudulento participam na rede.

Problema

Tentativa dos defraudador de encarnar o email. Quando o email encarna (sentidos ser de) um membro de seu pessoal da empresa, pode ser particularmente decepcionante e tem o potencial causar a confusão. Na tentativa de resolver este problema, os administradores do email puderam tentar obstruir o correio de entrada que parece originar de dentro da empresa (correio *falsificado*).

Pôde parecer lógico que se você obstrui o correio de entrada do Internet que tem o endereço do remetente da empresa no Domain Name, resolve o problema. Infelizmente, quando você obstrui o correio desta maneira, pode igualmente obstruir o email legítimo ao mesmo tempo. Considere estes exemplos:

- Um empregado viaja e usa um provedor de serviço do Internet (ISP) do hotel que reoriente transparentemente todo o tráfego do Simple Mail Transfer Protocol (SMTP) aos server do correio ISP. Quando o correio é enviado, pôde-se parecer que passa diretamente pelo servidor SMTP da empresa, mas está enviado realmente através de um servidor SMTP da terceira antes que esteja entregado à empresa.

- Um empregado subscreve a uma lista de discussão do email. Quando as mensagens são enviadas à lista de email, estão retornadas a todos os assinantes, aparentemente do autor.

- Um sistema externo é usado a fim monitorar o desempenho ou a alcançabilidade de dispositivos externo-visíveis. Quando um alerta ocorre, o email tem o Domain Name da empresa no endereço do remetente. Os provedores de serviços da terceira, tais como o WebEx, fazem este razoavelmente frequentemente.

- Devido a um erro de configuração da rede temporária, o correio do interior da empresa é enviado através do ouvinte de entrada, um pouco do que o ouvinte de partida.

- Alguém fora da empresa recebe uma mensagem que encaminhe de novo na empresa com um agente de usuário do correio (M.U.A.) esse linhas de cabeçalho novas dos usos um

pouco do que o cabeçalho original.

- Um aplicativo Internet-baseado, tal como as **páginas do transporte de** Federal Express ou Yahoo **enviam por correio eletrónico esta** página do **artigo**, criam o correio legítimo com um endereço do remetente esses pontos de volta à empresa. O correio é legítimo e tem um endereço de origem do interior da empresa, mas não origina do interior.

Estes exemplos mostram que se você obstrui o correio de entrada baseado na informação de domínio, pode conduzir aos falsos positivos.

Solução

Esta seção descreve as ações recomendadas que você deve executar a fim resolver este problema.

Aplique filtros

A fim evitar a perda de mensagens de Email legítimos, não obstrua o correio de entrada baseado na informação de domínio. Em lugar de, você pode etiquetar a linha de assunto destes tipos de mensagem enquanto incorporam a rede, que indica ao receptor que as mensagens estão forjadas potencialmente. Isto pode ser realizado com filtros da mensagem ou com filtros satisfeitos.

A estratégia básica para estes filtros é verificar as linhas de cabeçalho para trás-aguçado do corpo (dos dados é o mais importante), assim como o remetente do envelope do RFC 821. Estas linhas de cabeçalho o mais geralmente são mostradas em MUAs e são essas que são mais provável ser forjado por uma pessoa fraudulenta.

O filtro da mensagem no exemplo seguinte mostra como você pode etiquetar as mensagens que são encarnadas potencialmente. Este filtro executa diversas ações:

- Se a linha de assunto já tem **"{forjado possivelmente}" n**ele, a seguir uma outra cópia não está adicionada pelo filtro. Isto é importante quando as respostas são incluídas no fluxo de mensagem, e uma linha de assunto pôde mover-se com o mail gateway diversas vezes antes que uma linha da mensagem esteja completa.

- Este filtro procura pelo remetente do envelope ou do encabeçamento que tem um endereço esse extremidades no Domain Name **@yourdomain.com.** É importante notar que correio-da busca é automaticamente não diferenciando maiúsculas e minúsculas, mas de - a busca do encabeçamento não é. Se o Domain Name é encontrado em um ou outro lugar, o filtro introduz "**{forjado possivelmente}" na** extremidade da linha de assunto.

Está aqui um exemplo do filtro:

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
   {
       if (mail-from == "@yourdomain\\.com$") OR
          (header("From") == "(?i)@yourdomain\\.com")
       {
           strip-header("Subject");
           insert-header("Subject", "$Subject {Possibly Forged}");
```

```
    }
}
```

Medidas adicionais

Porque não há nenhuma maneira simples identificar o correio falsificado do correio legítimo, não há nenhuma maneira de eliminar inteiramente o problema. Consequentemente, Cisco recomenda que você permite a exploração do Anti-Spam de IronPort (IPA), que identifica eficazmente o correio fraudulento (phishing) ou o Spam e o obstrui positivamente. O uso deste varredor do anti-Spam, quando acoplado com os filtros descritos na seção anterior, fornece os melhores resultados sem a perda de email legítimo.

Se você deve identificar os email fraudulentos que entram sua rede, a seguir considere o uso da tecnologia identificada chaves do correio do domínio (DKIM); exige mais estabelecido, mas é uma boa medida contra o phishing e email fraudulentos.

> Nota: Para obter mais informações sobre dos filtros da mensagem, refira o **Guia do Usuário de AsyncOS na** página de suporte da ferramenta de segurança do email de Cisco.