Como você obstrui aplicativos desconhecidos na ferramenta de segurança da Web de Cisco?

Índice

Pergunta

Como você obstrui aplicativos desconhecidos na ferramenta de segurança da Web de Cisco?

Nota: Este artigo da base de conhecimento provê o software que não é mantido nem é apoiado por Cisco. A informação é fornecida como uma cortesia para sua conveniência. Para a assistência adicional, contacte por favor o fornecedor de software.

1. A primeira defesa é usar cordas do “agente de usuário” para obstruir tais aplicativos. Desde que nós não conhecemos todos os agentes de usuário para estes aplicativo, você precisará de procurá-los nos links abaixo.
   Nós podemos adicionar o “agente de usuário” sob <for da coluna do ***gerenciador de segurança > das políticas de acesso > dos protocolos e dos agentes de usuário da Web o*** policy> exigido do acesso.--**> Add a** corda do agente de usuário sob do ***“agentes de usuário feitos sob encomenda bloco: ”*** (um pela linha).

2. Se os controles da visibilidade do aplicativo (AVC) estão permitidos *(sob o > segurança GUI presta serviços de manutenção > reputação e Anti-malware da Web)*, a seguir nós podemos obstruir o acesso baseado em tipos de aplicativo como proxys, compartilhamento de arquivo, utilidades do Internet. Nós podemos fazer este sob o ***gerenciador de segurança > as políticas de acesso da Web > dos “<for da coluna aplicativos o policy> exigido do acesso***.
3. Se o agente de usuário não existe, você pode tentar adicionar o tipo MIMICAR (exemplo*:* aplicativos das torrentes do bit).
   Nós podemos adicionar “MIMICAMOS” tipos *sob o <for da coluna do* ***gerenciador de segurança da Web*** *> das* ***políticas*** *> dos* ***objetos do acesso à Web o*** *policy> exigido do acesso*.---o **>** Add no objeto/mime datilografa dentro o **“bloco que o MIME feito sob encomenda datilografa” a** seção como application/x-bittorrent (um pela linha).

4. Assegure-se de que as categorias como a vacância do filtro, atividades ilegais estejam obstruídas nas políticas de acesso. Se alguns aplicativos usam URL conhecidas ou endereços IP de Um ou Mais Servidores Cisco ICM NT para suas conexões, a seguir nós podemos obstruir suas categorias predefinidas assocaited URL ou configurar-las em uma categoria feita sob encomenda obstruída URL usando seu endereço IP de Um ou Mais Servidores Cisco ICM NT, FQDN, ou um regex que combina os domínios. Nós podemos fazer este *sob o* ***gerenciador de segurança > as políticas de acesso da Web > “***coluna das

categorias URL".

5. Alguns aplicativos podem usar o HTTP CONECTAM o método para conectar às portas diferentes. Reserve somente sabido que as portas ou as portas específicas necessárias em seu ambiente no HTTP CONECTAM domínios da configuração das portas.
   O HTTP CONNECT pode ser configurado *sob <for da coluna do* ***gerenciador de segurança > das políticas de acesso > dos protocolos e dos agentes de usuário da Web o*** *policy> exigido do acesso*.--**o > Add** permitido portas sob o **"HTTP CONECTA portas: "**

6. Para os aplicativos onde você sabe somente sobre os endereços IP de destino que estão sendo alcançados, você pode usar a característica do monitor de tráfego L4 para obstruir o acesso para o endereço IP de Um ou Mais Servidores Cisco ICM NT interessado. Nós podemos adicionar o ips de destino *sob o* ***gerenciador de segurança da Web > o monitor de tráfego L4 > endereços suspeitados adicionais do malware.***

Se você é de que o "agente de usuário" ou "mimica tipo inconsciente" está sendo usado por determinados aplicativos, a seguir você pode fazer qualquer um do seguinte para encontrar esta informação:

- Execute uma captura de pacote de informação com o WireShark (etéreo) na máquina e no filtro de cliente para o protocolo "HTTP".
- Execute a captação em WSA (sob o "apoio e a ajuda" > a "captura de pacote de informação"), filtrado no endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente.

Lista de agentes de usuário:
==========
http://www.user-agents.org/

Lista de tipos MIME:
==========
http://www.webmaster-toolkit.com/mime-types.shtml

http://www.microsoft.com/technet/isa/2004/plan/commonapplicationsignatures.mspx