Como o punho Skype da ferramenta de segurança da Web de Cisco (WSA) trafica?

Índice

Pergunta:

Pergunta:

Como o punho Skype da ferramenta de segurança da Web de Cisco (WSA) trafica?

Ambiente: Cisco WSA, Skype

Skype é uma rede proprietária da telefonia pelo Internet (VoIP). Skype opera-se primeiramente como um programa peer-to-peer, assim não se comunica diretamente com um servidor central para operar-se. Skype pode ser particularmente difícil de obstruir, porque tentará conectar em muitas maneiras diferentes.

Skype conecta no seguinte ordem de preferência:

1. Pacotes de UDP diretos a outros pares que usam números de porta aleatórios
2. Pacotes de TCP diretos a outros pares que usam números de porta aleatórios
3. Pacotes de TCP diretos a outros pares que usam a porta 80 e/ou a porta 443
4. Os pacotes em túnel através de um proxy da Web que usa um HTTP CONECTAM à porta 443

Quando distribuídos em um ambiente de proxy explícito, os métodos 1-3 serão enviados nunca a Cisco WSA. A fim obstruir Skype, deve primeiramente ser obstruído de um outro lugar na rede. As etapas de Skype 1-3 podem ser utilização obstruída:

- Firewall: Use o NBAR para obstruir a versão 1 de Skype. Mais informação está disponível em http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
- Ips Cisco (ASA): Cisco ASA pode potencialmente detectar e obstruir Skype através das assinaturas.

Quando Skype cai de volta a usar um proxy explícito, Skype não fornece deliberadamente nenhum detalhe do cliente na requisição de conexão HTTP (nenhuma corda do agente de usuário tampouco). Isto faz difícil diferenciar-se entre Skype e uma requisição de conexão válida. Skype conectará sempre à porta 443 e o endereço de destino é sempre um endereço IP de Um ou Mais Servidores Cisco ICM NT.

Exemplo:

CONECTE 10.129.88.111:443 HTTP/1.0
Conexão de proxy: manutenção de atividade

A seguinte política de acesso obstruirá todas as requisições de conexão com o WSA que combina os endereços IP de Um ou Mais Servidores Cisco ICM NT e a porta 443. Isto combinará todo o tráfego de Skype. Contudo, os programas de NON-Skype que tentam escavar um túnel a um endereço IP de Um ou Mais Servidores Cisco ICM NT na porta 443 serão obstruídos também.

Obstruindo Skype - Ambiente explícito com proxy HTTPS desabilitado

Crie uma categoria do costume URL para combinar o tráfego IP e de porta 443:

1. Navegue ao “gerenciador de segurança” - > “categorias feitas sob encomenda URL” - > “adicionam a categoria feita sob encomenda”.
2. Complete da “o nome categoria” e expanda-o “avançou”.
3. Use "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" no indicador da expressão regular.

Ajuste esta categoria para negar nas políticas de acesso:

1. Navegue da “ao gerenciador de segurança Web” - > “políticas de acesso”.
2. Clique o link sob “a coluna das categorias URL” para o grupo de política apropriado.
3. “Na seção de filtração da categoria feita sob encomenda URL”, escolha o “bloco” para a categoria nova de Skype.
4. Submeta e comprometa as mudanças

Nota: As requisições de conexão explícitas podem somente ser obstruídas se o serviço de proxy HTTPS é desabilitado!

Quando a descriptografia WSA HTTPS é permitida, o tráfego de Skype pode muito provavelmente quebrar porque não é puramente tráfego HTTPS (apesar da utilização CONECTE e a porta 443). Isto conduzirá a um erro 502 gerado pelo WSA e a conexão será deixada cair. Todo o tráfego de web real HTTPS a um endereço IP de Um ou Mais Servidores Cisco ICM NT continuará a trabalhar (embora será decifrado no WSA).

Obstruindo Skype - Ambiente explícito/transparente com o proxy HTTPS permitido

Crie uma categoria feita sob encomenda para combinar o tráfego IP e de porta 443:

1. Navegue ao “gerenciador de segurança” - > “categorias feitas sob encomenda URL” - > “adicionam a categoria feita sob encomenda”.
2. Complete da “o nome categoria” e expanda-o “avançou”.
3. Use "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" no indicador da expressão regular.

Ajuste esta categoria para decifrar nas políticas de descriptografia:

1. Navegue da “ao gerenciador de segurança Web” - > “políticas de descriptografia”.
2. Clique o link sob “a coluna das categorias URL” para o grupo de política apropriado.
3. “Na seção de filtração da categoria feita sob encomenda URL”, escolha o “Decrypt” para a categoria nova de Skype.
4. Submeta e comprometa as mudanças.

Nota: Desde que o tráfego de Skype é enviado a um IP, considerar-se-á como parte “das URL Uncategorized”. O mesmo efeito que acima ocorrerá segundo se a ação deve decifrar ou transmissão.