Os clientes que usam o proxy transparente devem ativamente decifrar o tráfego a fim distinguir entre YouTube.com e Google.com

Índice

Problema

Os clientes que usam o proxy transparente devem ativamente decifrar o tráfego a fim distinguir entre YouTube.com e Google.com.

Ambiente

Desenvolvimento do proxy transparente, proxy HTTPS permitido

Sintomas

Previamente, Google usou Certificados de servidor SSL diferentes para cada um de seus Domain Name preliminares. Assim se você conectou a https://www.google.com e a https://www.youtube.com, você veria certificados de servidor diferentes, cada um especificando que são válidos para um daqueles dois domínios.

Recentemente, Google comutou a usar um único certificado de servidor SSL para todas suas propriedades da Web, assinado por sua própria em-casa CA. Assim se você consulta aos dois domínios alistados acima de usar o SSL, você obterá o mesmo certificado. Que o certificado usa uma extensão ao X.509 chamou “SubjectAltName” para alistar alguns dúzia domínios como válidos para esse certificado. Uma lista completa dos domínios de Google que são válidos para este certificado novo está abaixo.

Isto trabalha muito bem para navegadores: seu navegador sabe que está tentando conectar a youtube.com, vê um certificado que seja válido para youtube.com (e outras dúzia coisas), e deixa a conexão ir completamente sem nenhuns avisos.

Como isto impacta o WSA

Para algum servidor proxy, a primeira coisa que você precisa de fazer quando você vir que um pedido de um cliente é determina que destino da Web a que o cliente está tentando ir. Para o HTTP liso, é consideravelmente fácil: olhe o encabeçamento do host no pedido do HTTP.

Para o SSL, é mais difícil. No modo de proxy explícito, o navegador diz-nos na requisição de conexão, de modo que seja fácil. A dificuldade vem no modo transparente. Com a descriptografia permitida no WSA, nós precisamos de determinar onde o usuário está tentando consultar antes realmente a decifrar a conexão.

Hoje, nós fazemos este olhando o endereço IP de Um ou Mais Servidores Cisco ICM NT que o cliente está tentando conectar a, conectando a esse IP nós, e olhando o certificado, em particular, no campo do CN. Isto trabalha bem quando um hostname original tem seu próprio certificado de servidor SSL. Igualmente permite que os clientes executem alguma quantidade de reforço de política para o tráfego SSL sem decifrar qualquer coisa, e assim sem distribuir o CERT de CA do WSA a seus clientes. Um cliente pode permitir https://www.google.com mas o bloco https://www.youtube.com ajustando o primeiro “reserva, não decifra” e o segundo “a deixar cair” na política de descriptografia.

Agora, youtube.com e google.com servem acima o mesmo certificado de servidor. Isto significa que a fim distinguir entre os dois, WSA tem que procurar algo a não ser apenas o certificado servido acima no endereço IP de Um ou Mais Servidores Cisco ICM NT a que o cliente está tentando conectar.

A solução a esta edição está sendo seguida como a identificação de bug Cisco 74969.

Solução

Se você tem uma configuração afetada por esta, a seguir a solução imediata é girar sobre a descriptografia ativa do tráfego SSL. Para os clientes que não têm distribuído previamente o certificado de CA do WSA, precisarão de começar fazer assim. Esta é a melhor solução geral ao problema.

Apêndice

Lista de domínios para que o certificado novo de Google é válido:

Nome de DNS: *.google.com
Nome de DNS: google.com
Nome de DNS: *.atggl.com
Nome de DNS: *.youtube.com
Nome de DNS: youtube.com
Nome de DNS: *.ytimg.com
Nome de DNS: * .google.com.br
Nome de DNS: * .google.co.in
Nome de DNS: *.google.es
Nome de DNS: * .google.co.uk
Nome de DNS: *.google.ca

Nome de DNS: *.google.fr
Nome de DNS: *.google.pt
Nome de DNS: *.google.it
Nome de DNS: *.google.de
Nome de DNS: *.google.cl
Nome de DNS: *.google.pl
Nome de DNS: *.google.nl
Nome de DNS: * .google.com.au
Nome de DNS: * .google.co.jp
Nome de DNS: *.google.hu
Nome de DNS: * .google.com.mx
Nome de DNS: * .google.com.ar
Nome de DNS: * .google.com.co
Nome de DNS: * .google.com.vn
Nome de DNS: * .google.com.tr
Nome de DNS: *.android.com
Nome de DNS: *.googlecommerce.com