Como faz o whitelist I manualmente um Web page na ferramenta de segurança da Web de Cisco (que executa 5.2.0 e acima) de modo que a exploração WBRS, de Webroot ou de McAfee seja contorneada?

Índice

Pergunta:

Como faz o whitelist I manualmente um Web page na ferramenta de segurança da Web de Cisco (que executa 5.2.0 e acima) de modo que a exploração WBRS, de Webroot ou de McAfee seja contorneada?

Sintomas:

O usuário está tentando alcançar um local legítimo, mas está sendo devido a uma baixa contagem WBRS (infecção do vírus do web server, do Spam sendo enviado através do IP etc. do web server) ou obstruído devido a um dos motores do anti-malware que provocam nessa página.

Se o usuário é obstruído devido a um baixo WBRS o usuário está vendo uma mensagem do bloco MALWARE_GENERAL. A mostra dos accesslogs um WBRS abaixo do ponto inicial de obstrução (o padrão é -6.0).

Para uma solução permanente, contacte por favor o tac Cisco de modo que a página possa ser revista a fim ajustar o WBRS ou relatar falsos positivos aos vendedores anti-vírus e do anti-malware.

Você pode igualmente contactar o tac Cisco para recolher mais informação em porque o local é obstruído de modo que o contato ou o administrador técnico do Web site possam ser notificados e possam tomar as etapas necessárias.
Certifique-se fornecer os códigos de obstrução e as linhas relevantes do accesslog ao contactar o tac Cisco

Para contornear WBRS:

4. Clique sobre o link da “na coluna de filtração da reputação e do Anti-malware Web” de sua política recém-criado do acesso à Web (deve ler “a política global” até aqui).

5. Seleto “defina configurações personalizadas da reputação e do Anti-malware da Web
Nota: Se você ajusta a ação “permita” na categoria URL, isto conduziria a contornear a exploração do Anti-malware/vírus.

Para contornear a exploração WBRS e de anti-malware:

Nota: A exploração de desabilitação do anti-malware (Webroot e/ou McAfee) poderia ser um risco de segurança potencial. Isto deve somente ser feito para os locais que podem ser confiados para não conter o malware.