Procedimento para remoção do worm Downadup/Conficker

Informações do laboratório F-Secure:

http://www.f-secure.com/v-descs/worm_w32_downadup_al.shtml

Inicialmente é preciso verificar se o computador está abrindo conexões, normalmente um número muito elevado, para vários sites externos utilizando a porta 445 (RPC).

Se isto estiver acontecendo possivelmente este computador está infectado com alguma variante do worm Downadup/Conficker. Este worm pode, inclusive, derrubar os serviços de Proxy e firewall pelo número elevado de requisições que chegam a estes servidores.

Este worm explora uma vulnerabilidade do Windows, portanto é necessário instalar uma correção crítica da Microsoft desenvolvida para esta situação.

Você deve procurar pelo arquivo correspondente ao seu sistema operacional.

http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx

Após instalar esta correção o computador deve ser reinicializado e então prosseguir com o procedimento abaixo.

Primeiro passo, como impedir a queda dos serviços de firewall e Proxy para começarmos a desinfecção?

1. Impedir que conexões com destino à porta 445 (TCP e UDP) sejam originadas dos hosts. Para isto é necessário criar uma regra no firewall do F-Secure Client Security para bloquear tais conexões.
2. Acima desta regra de negação é preciso verificar quais serviços de rede utilizam esta porta e criar uma regra liberando as conexões para estes servidores, por exemplo, Active Directory e MS Exchange.

Esta ação fará com que a rede não sofra o impacto destas conexões, permitindo que os serviços normais sejam restaurados.

Após estabilizar os serviços de rede é preciso verificar as atualizações das assinaturas de vírus, pois estas podem ter sido atrasadas devido à sobrecarga na rede. Verifique se o F-Secure Policy Manager Server está com as últimas atualizações e as estações também.

Uma vez que tudo está atualizado faça download da ferramenta de remoção do worm Downadup/Conficker no seguinte endereço:

JAR: para distribuição através do Policy Manager Server

ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup_unsigned.jar

EXE: para instalação manual

ftp://ftp.f-secure.com/anti-virus/tools/beta/f-downadup.zip

Esta ferramenta auxilia na remoção do worm, em servidores é necessário rodar localmente com o executável.

A partir deste momento as infecções foram removidas das máquinas e as mesmas protegidas de novas infecções pelas assinaturas de vírus instaladas.

Daniel Salazar

Suporte F-Secure

suporte@f-secure.com.br