Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Recomendação de Segurança 002/2019 - Cogetic/VPGDI

Em 12 de fevereiro de 2019

Para: Gestores de TI das unidades da Fiocruz

Assunto: Behavior Monitoring

Prezados Gestores de TI,

O *Behavior Monitoring* é um módulo de prevenção que analisa alterações incomuns ou não solicitadas no sistema operacional ou em arquivos, sendo uma das principais linhas de defesa do OfficeScan contra Ransonwares. A boa prática de configuração da aplicação diz que o módulo deve estar habilitado por padrão nas máquinas.

Contudo, em situações bem específicas, o módulo pode estar suscetível a falsos positivos. Assim, caso ocorra de uma aplicação legítima encontrar problemas em seu funcionamento devido ao *Behavior Monitoring*, basta criar uma exceção apontando para o caminho da aplicação impactada.

Procedimentos para habilitação do módulo *Behavior Monitoring* do OfficeScan XG e para a tentativa de recuperação de arquivos.

Procedimento para habilitar o Behavior Monitoring

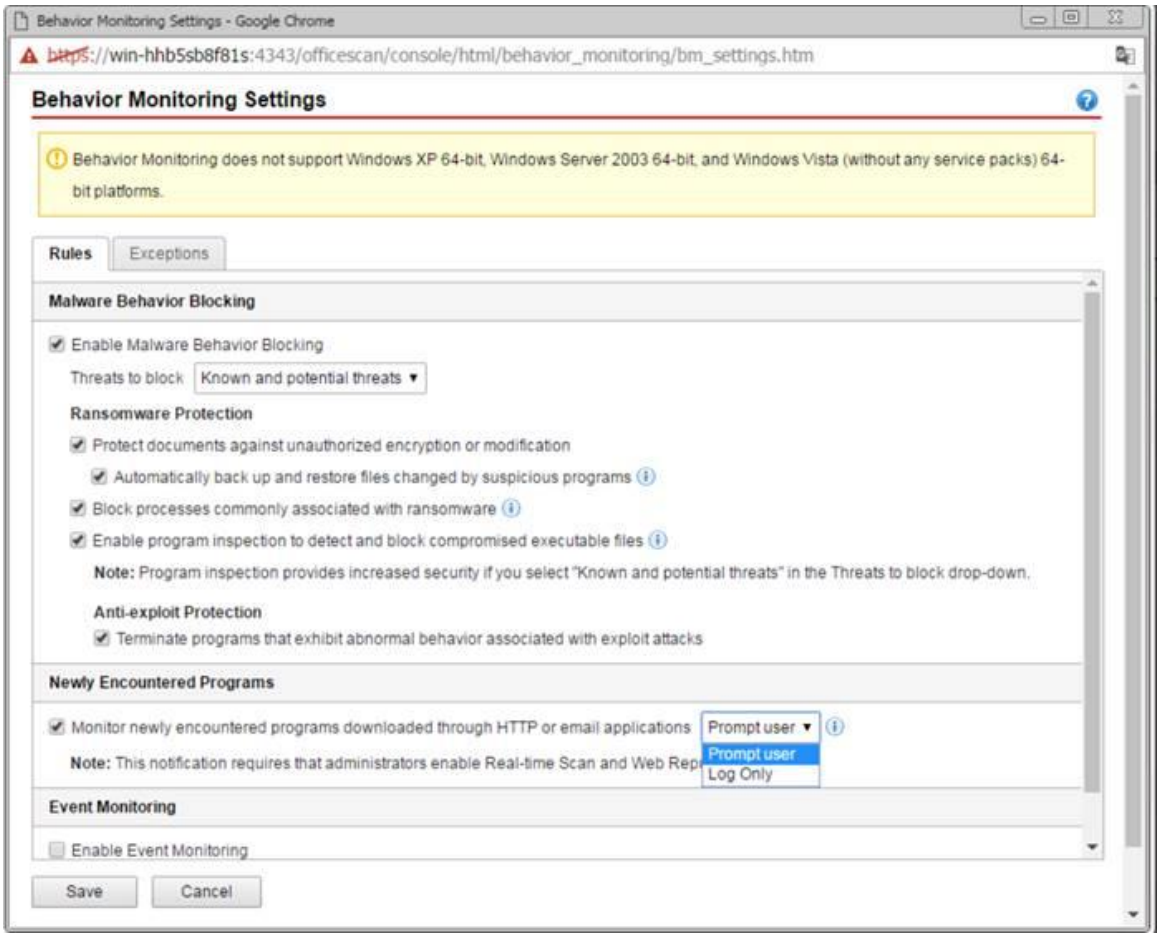
1. Logar na console do OfficeScan;
2. Vá até Agents > Agent management;
3. Clicar em Settings e depois em Behavior Monitoring Settings;
4. Marcar a opção “Enable Malware Behavior Blocking” e selecionar “Known and Potential Threats”;
5. Em Ransonware Protection, marcar as seguintes opções:

    - Protect documents against unauthorized encryption or modification & Automatically back up files changed by suspicious programs.
    - Block processes commonly associated with ransomware.
    - Enable program inspection to detect and block compromised executable files.

- Terminate programs that exhibit abnormal behavior associated with exploit attacks.

6. Em Newly Encountered Programs:

- Marcar a opção “Monitor newly encountered programs downloaded through HTTP or email applications”;
- Selecionar "Prompt user";



Procedimento para a tentativa de restore de arquivos criptografados

Caso o agente do OfficeScan não tenha feito o *restore* de maneira automática, é necessário seguir os passos abaixo:

1. Vá até a localização do backup de arquivos no *endpoint*.

a. O agente do OfficeSCan armazena o backup dos arquivos no seguinte diretório: <Agent_installation_folder>\CCSF\module\DRE\data\Backup

2. Localizar o arquivo a ser restaurado.

   a. O agente do OfficeScan retém o nome original do arquivo, mas altera a extensão com a data e a hora.

   b. Por exemplo, se o nome do arquivo original é teste_1.doc, o arquivo de backup se chamará teste_1.doc0120160822074710336_2.

3. Mudar a extensão do arquivo para a extensão original.

4. Copiar o arquivo.

5. Verificar se o arquivo está legível.

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações