Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Alerta de Segurança 001/2017 - Cogetic/VPGDI

Em 12 de maio de 2017

Para: Gestores de TI das unidades da Fiocruz

Cc: Vice-diretores de Gestão das unidades da Fiocruz

Assunto: *Ransomware*

Prezados Gestores de TI,

Alertamos as unidades da Fiocruz em relação aos ataques relativos a Ransomware ocorridos no dia de hoje, atingindo diversas empresas e hospitais na Europa, e já com alguns casos de ataques a empresas brasileiras.

A criticidade dessa campanha de Ransomware ocorre devido a utilização do exploit EternalBlue/DoublePulsar para uma vulnerabilidade descoberta no dia 14/3 e que está descrita no MS17-010 (https://technet.microsoft.com/en-us/library/security/ms17-010.aspx).

O ataque usa uma variante do Ransomware denominada "WannaCry" (detectada pela Trend Micro como RANSOM_WCRY.*). A nova versão 2.0 ganhou força e se alastrou em poucas horas, causando danos ao longo do dia 12/05 de forma sem precedentes.

Os principais fabricantes, como Trend Micro e Fortinet já estão disponibilizando vacinas para algumas variantes.

Recomendamos a aplicação imediata das seguintes ações:

— Manter o WSUS atualizado.

— Garantir que todos os hosts com Microsoft Windows tenham o patch MS10-017 instalado.

— Garantir que todos os *patterns* de seus produtos estejam atualizados para a última versão disponível. A *pattern* "Smart scan" versão 13.399.00 já detecta esta ameaça e já está disponível.

— Depois de atualizar as *patterns*, executar um *scan* manual programado nos dispositivos.

— Ativar a proteção Smart Scan do Officescan, caso ainda não esteja ativa.

— Implementar mecanismos de detecção de ameaças desconhecidas (Ransomware, APTs, etc) para aqueles que já tem o Officescan XG (*Machine Learning*) instalado.

— Quando possível, restringir acesso à porta 445.

— Evitar acesso através de VPN.

Acompanhe os alertas de segurança em seu ambiente, detecções relacionadas a: Ransom_Wana.a, WannaCrypt, Wcry, WanaCrypt, WannaCrypt,

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações