Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Alerta de Segurança 001/2017 – v2 – 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* – atualização

Prezados Gestores de TI,

Descrevemos a seguir recomendações complementares ao Alerta de Segurança 001/207.

No perímetro de rede:

- Bloquear o uso e download da aplicação TOR;
- Garantir que as funções de antimalware estejam habilitadas e atualizadas no Firewall, UTM ou NextGenFW;
- Bloquear o download de arquivos executáveis; (Certifique-se que o HTTPs está sendo inspecionado);
- Bloquear anexos de arquivos executáveis no filtro de E-mail (caso não utilizem o serviço antispam da Fiocruz);
- Garantir que o Filtro Web e Filtro de e-mail estejam com vacinas atualizadas;
- Bloqueio de urls e endereços IP que estão relacionadas ao Ransomware (171.25.193.9 | 95.130.11.147 | 82.223.21.74 | 51.15.48.254 | 91.121.230.218 | 62.210.125.130);
- Habilitar as regras no Network IPS para proteção da vulnerabilidade CVE -2017-0143;
- Garantir que as regras de firewall não permitam o redirecionamento de tráfego na porta 445 para redes protegidas;

Nas estações e servidores:

- Garantir que todos os computadores estão com o antimalware instalado e atualizado com a vacina hoje;
- Aplicar os patches de atualização relacionados à vulnerabilidade MS17-010;
- Garantir que o backup esteja atualizado e isolado do restante da rede;
- Habilitar regras de Host IPS para o CVE -2017-0143;
- Bloqueio de gravação de arquivos de extensão *.Wcry nas estações e servidores.

Informações adicionais:

- Realizar o monitoramento contínuo do ambiente em busca de atividades suspeitas;
- Em caso de suspeita de equipamento contaminado, é recomendado isolar o equipamento da rede imediatamente;
- Funcionamento do WanaCry de acordo com o Trend Labs: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/ransom_wcry.a
- Lista de IP's a serem bloqueados: 171.25.193.9 | 95.130.11.147 | 82.223.21.74 | 51.15.48.254 | 91.121.230.218 | 62.210.125.130
- Assinaturas de Host IPS disponíveis nas soluções Trend Micro: https://success.trendmicro.com/solution/1117192

Importante: no caso das unidades que utilizam serviços acima da Cogetic (IPS, filtroweb, appcontrol, antispam, etc.), as medidas acima já estão sendo implementadas pela própria Cogetic.

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações