Alerta de Segurança - 001/2012 CGTI/VPGDI

Em 23 de março de 2012

Aos Gestores de TI da Fiocruz

Assunto: Alerta de vírus - Conficker/Downadup

Prezados gestores,

Nos últimos dias temos recebido várias notificações do Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP), relatando que hosts pertencentes à rede da Fiocruz realizaram acessos a URLs maliciosas. Essas URLs são utilizadas por malwares para controle e execução de ações diversas em sistemas infectados. A notificação aponta para a possibilidade de infecção do vírus Conficker/Downadup, que através de algoritmos complexos criam uma lista diária de domínios que sofrerão o ataques, gera com os hosts infectados uma grande rede de bots para que, em algum momento, seus criadores possam enviar spams, roubar informações pessoais e direcionar os usuários a sites maliciosos para o download de outros malwares ou phishing.

Os primeiros exemplares datam de 2008 com variações a partir de 2009. O vírus explora vulnerabilidades do Windows e desativa os serviços de segurança, impede que computadores infectados acessem sites de segurança e faz o download de um cavalo de Troia. Ele também busca infectar outros computadores através dos serviços de comunicação ponto-a-ponto e inclui um algoritmo para atualizar os hosts infectados.

Assim, tendo em vista o tratamento adequado das vulnerabilidades e manutenção de níveis aceitáveis de segurança, recomendamos as seguintes ações:

1- Instalar o patch crítico MS08-067, que corrige a vulnerabilidade do Windows permitir a execução de um código remoto;

2- Manter um sistema de antivírus instalado e atualizado;

3- Realizar uma varredura em todos os computadores na rede da unidade e analisar os logs para confirmação da detecção e remoção do “Conficker/Downadup”;

4- Desativar o recurso de "execução automática" para evitar infecções dos drives USB;

5- Adotar o uso de senhas fortes e trocá-las com frequência;

Fundação Oswaldo Cruz – FIOCRUZ - CGTI - Av. Brasil, 4365 – Manguinhos, RJ. CEP: 21040-900
Castelo Mourisco, Sala 105. Tel.: 3885-1724 Site: http://cgti.fiocruz.br