Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Alerta de Segurança 001/2016 - CGTI/VPGDI

Em 23 de março de 2016

Para: Gestores de TI das unidades da Fiocruz
Assunto: Vírus "Qakbot" associado à *botnet* "Qbot"

Prezados Gestores,

Encaminhamos, na íntegra, o alerta emitido pela Coordenação-Geral de Tratamento e Incidentes de Redes / Departamento de Segurança da Informação e Comunicações sobre o vírus "Qakbot" associado à botnet "Qbot".

1. Descrição do Problema

O Referido malware é capaz de roubar as credenciais do usuário e outras informações confidenciais digitados no navegador "web" usando "*keystroke logging*" (*keylogger*) e "*Webinjects*".

O Qakbot possui a capacidade de propagação muito rápida, a partir de compartilhamento de redes (C$ e Admin$), mídias removíveis e Websites infectados. Portanto, pode ser necessário desativar temporariamente todos os compartilhamentos e interromper qualquer comunicação entre estações de trabalho dentro do ambiente afetado.

Os dados capturados são enviados para Servidores FTP controlados pelo atacante. No entanto, foi observado, em máquinas afetadas, tráfego nas portas 21, 22, 443, 65200 e 65400 para os respectivos servidores de Comando e Controle (C2).

2. Sugestões para Mitigação do Problema

O US-CERT recomenda as seguintes ações para conter ou mitigar possíveis infecções pelo Qakbot:

a) Desabilitar o "AutoRun" de mídias removíveis (https://www.us-cert.gov/ncas/alerts/ta09-020a.);
b) Considerem a hipótese do bloqueio de acesso de suas respectivas redes aos IP/domínios associados ao Qakbot, conforme listagem constante do arquivo "MAR-10050053-Update-1" anexo;
c) Prevenir que novas tarefas sejam adicionados aos perfis dos usuários no agendador de tarefas do Microsoft Windows até que o malware seja contido, e modificar todas as senhas do sistema afetado.
d) Por fim, julgamos importante reforçar juntos aos administradores de TI, a necessidade de manter os sistemas e antivírus atualizados, bem como a aplicação dos "patches" de correção.

3. Informações complementares

Informações adicionais podem ser obtidas no relatório de análise de malware "MAR-10050053-Update-1.pdf" em anexo

Atenciosamente,

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