Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Recomendação de Segurança 001/2019 - Cogetic/VPGDI

Em 5 de fevereiro de 2019

Para: Gestores de TI das unidades da Fiocruz

Assunto: Exposição de serviços

Prezados Gestores de TI,

Dando continuidade à análise dos eventos relacionados a atividade de Ransomware nos últimos dias, foi possível verificar que se trata do malware Crysis (Dharma), que possui como característica comum a infecção através da exploração de serviços expostos (SMB, RDP, FTP, etc.). Através de uma rápida busca na ferramenta Shodan é possível identificarmos diversos serviços FTP e RDP, por exemplo, expostos para a Internet. Tal exposição aumenta consideravelmente a chance de exploração desses protocolos por ameaças diversas. Desta forma, recomendamos seja analisado urgentemente a necessidade destes serviços serem acessados externamente. Quando for inevitável a exposição de um serviço para a Internet, recomendamos que, sempre que possível, o mesmo seja realizado sempre através de uma VPN.

Referências

— https://www.fortinet.com/blog/threat-research/dharma-ransomware--what-it-s-teaching-us.html

— https://www.shodan.io/

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