Alerta de Segurança 002/2013 - CGTI/VPGDI

Em 2 de agosto de 2013

Prezados Gestores,

Recentemente foi descoberto um novo *malware* do tipo *Ransomware*, que utiliza uma técnica de sequestrar os dados das vítimas e comprimi-los em arquivos do formato .RAR criptografado com o algoritmo AES (*Advanced Encryption Standard*) . Após a infecção, os arquivos são liberados somente mediante o pagamento de "resgates".

Para realizar a infecção, os atacantes procuram por computadores com o sistema operacional Windows publicados na internet que estejam com o serviço Remote Desktop (RDP) habilitado e realizam um ataque de força bruta em tais computadores. Uma vez que conseguem o acesso, transferem a ameaça para o computador e a executam.

Por tanto, torna-se substancial tomar algumas medidas para mitigar esta ameaça:

1) Desativar o serviço RDP das máquinas que não necessitam, principalmente de computadores que estão publicados para internet. Para os computadores que necessitam desse recurso habilitado, recomenda-se filtrar os usuários que terão permissão para executar o recurso.

2) Utilizar-se de senhas fortes para dificultar o ataque de força bruta.

3) Manter os computadores com sistema operacional Windows atualizados, principalmente em servidores. As vulnerabilidades MS12-020 e MS13-029, por exemplo, são do protocolo RDP e permitem execução remota de código. A mais recente é de abril de 2013.

4) Para determinados tipos de ataques de *Ransonware*, a única solução para recuperação dos dados criptografados é através da restauração de backup, portanto é importante manter sempre o backup atualizado.

Coordenação de Gestão de Tecnologia da Informação

Segurança da Informação e Comunicações