epartamento de Segurança da Informação e Comunicações – **DSIC** - *dsic.planalto.gov.br/*
Centro de Tratamento de Incidentes de Redes do Governo – **CTIR Gov** - *www.ctir.gov.br/*

Alerta nº 05/2018 – Ataques de *Ransomware CrySis*.

Data de Atualização: 23/08/2018
Data de Publicação: 23/08/2018

1. Descrição do Problema

Temos recebido de nossos colaboradores, Alertas sobre possível campanha de infecção por *Ransomware CrySis a Órgãos e Entidades da Administração Pública Federal –APF.*

O *CrySiS* (MSIL/Kryptik.NUQ) é um código malicioso do tipo *Filecoder* que surgiu em setembro de 2015. O *CrySis* possui um encapsulamento para se ocultar das principais ferramentas de antivírus. Ele efetua o comprometimento do protocolo da área de trabalho remota (*Remote Desktop protocol* – RDP), bloqueando com algoritmo AES256, combinada com criptografia assimétrica RSA1024, o acesso aos arquivos. Após o comprometimento uma mensagem é exibida cobrando o "resgate" em *bitcoins* para o desbloqueio dos arquivos.

Os arquivos criptografados têm muitas extensões diferentes, incluindo:

.xtbl, .crysis, .crypt, .lock, .crypted e .dharma.

1. Sistemas Afetados

- Sistemas vulneráveis a execução maliciosa de arquivos.

2. Impacto

Este ataque, sendo efetivo permite:

- Impedimento de acesso aos dados (dados criptografados e sequestrados);

3. Recomendações

- Não abrir e-mails suspeitos;
- Evitar visitar websites para downloads de programas obscuros e suspeitos;
- Mesmo não sendo comprovada existência de vulnerabilidades, manter os sistemas atualizados para a versão mais recente possível ou aplicar os patch conforme orientação do fabricante;
- Isolar a máquina da rede, ao primeiro sinal de infecção por Malware;
- Garantir o backup atualizado dos arquivos locais e dos Armazenados em Servidores de Arquivos;
- Rever a política de privilégios administrativos nas máquinas clientes, a fim de restringir a instalação /execução de binários e ou executáveis desconhecidos; e
- Por fim, realizar campanhas internas, alertando os usuários a não clicar em links ou baixar arquivos de e-mails suspeitos ou não reconhecidos como de origem esperada.

4. Referências

- https://www.welivesecurity.com/2016/11/24/new-decryption-tool-crysis-ransomware/
- https://tecnologia.uol.com.br/noticias/redacao/2018/07/18/novo-golpe-de-sequestro-de-arquivos-afeta-principalmente-o-brasil.htm?cmpid=copiaecola
- https://semvirus.pt/virus-ransomware-crysis/