Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 02/2017 – Ataques de *Ransomware* *Wncry* através de Vulnerabilidade no Windows

1. Descrição do Problema

Temos recebido dos órgãos de nossos colaboradores, Alertas sobre ataques de "*Ransomware*" tendo como alvo os domínios da Administração Pública Federal. O atacante explora vulnerabilidades dos sistemas Windows, alertado no Boletim MS17-010 da Microsoft, bloqueando acesso aos arquivos e cobrando o "resgate" em *bitcoins*.

1.1 O que é um Ransomware?

Pode ser entendido como um código malicioso que infecta dispositivos computacionais com o objetivo de sequestrar, capturar ou limitar o acesso aos dados ou informações de um sistema, geralmente através da utilização de algoritimos de encriptação (*crypto-ransoware*), para fins de extorsão.

Para obtenção da chave de decriptação, geralmente é exigido o pagamento (ransom) através de métodos online, tipo "*Bitcoins*"**.**

2. Métodos de Ataques

A mais severa das vulnerabilidades, conforme Bolentim MS17-010 da Microsoft, permite ao ataquente a execução remota de código por um atacante através de envio mensagens especialmente criadas a um 1.0 servidor Microsoft Server Message Block (SMBv1).

3. Ameaças

- Recentemente, recebemos a informação sobre um ataque de *Ransomware* Wncry, o qual está sendo amplamente usado em ataques desse tipo.
- O CCN-CERT elaborou um comunicado "Identificado ataque de ransomware que afecta a sistemas Windows" (https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html).
- A recuperação dos arquivos infectados é quase impossível, sem a chave de encriptação, devido ao tipo de criptografia forte utilizada, portanto a política de Backup é a medida mais eficaz para evitar a perda de dados.
- Não é recomendável, em nenhuma hipótese, o pagamento de valores aos atacantes.

4. Sugestões para Mitigação Problema

- Isolar a rede infectada e aplicar o patch conforme Bolentim MS17-010 da Microsoft – Crítico.
- Manter os sistemas atualizados para a versão mais recente ou aplicar os patch conforme orientação do fabricante.
- Bloquear as portas UDP 137, 138 e TCP 139, 445 até solucionar o problema.
- Realizar campanhas internas, alertando os usuários a não clicar em links ou baixar arquivos de e-mail suspeitos ou não reconhecidos como de origem esperada;
- 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;
- Isolar a máquina da rede, ao primeiro sinal de infecção por malware;
- Verificar o tráfego de máquinas internas para domínios não usuais ou suspeitos. (vide relação anexa);

- Monitorar as conexões internas e não usuais entre máquinas da rede, a fim de evitar o movimento lateral de propagação do malware; e
- Por fim, manter o antivírus, aplicação de "*Patchs*" de segurança e a "*blacklist"* (filtro "antispam") de e-mail atualizados.

Referências:

- https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
- https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Brasília-DF, 12 de maio de 2017.

Equipe do CTIR Gov