Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Redes do Governo

Alerta nº 02/2017 – Ataques de *Ransomware Wanna Decryptor*

1. Descrição do Problema

Temos recebido dos órgãos e de nossos colaboradores, Alertas sobre ataques de *Ransomware* tendo como alvo os domínios do governo brasileiro. Esta variação de *Ransomware* é conhecida por *Wanna Decryptor, WannaCry, WCry, WanaCrypt ou WanaCrypt0r*.

O atacante explora vulnerabilidades do Microsoft Server Message Block 1.0 (SMBv1), alertado no Boletim MS17-010 da Microsoft, ou através do comprometimento do protocolo da área de trabalho remota (Remote Desktop protocol – RDP), bloqueando o 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

O *Ransomware Wanna Decryptor* explora a mais severa das vulnerabilidades informada através do Bolentim MS17-010 da Microsoft, permitindo ao atacante a execução remota de código através de envio de mensagens especialmente criadas para um servidor Microsoft Server Message Block 1.0 (SMBv1), ou através do comprometimento do protocolo da área de trabalho remota (Remote Desktop protocol – RDP). O Atacante envia um *loader* contendo uma dll criptografada em algorítimo AES e chave de 128bits, sendo indetectável até então, aos anti-virus. Durante a execução um arquivo copiado no disco pelo malware se encarrega de descriptografar a dll enviada, que por sua vez, começa a criptografar os arquivos alvos. O *Ransomware Wanna Decryptor* também tenta utilizar informações sobre compartilhamentos ativos disponíveis na IPC$ (Inter Process Communication), para poder se propagar na rede através do protocolo SMBv1 (Server Message Block 1.0), infectando todos os sistemas vulneráveis. Os arquivos infectados passam a ter as seguintes extensões: .wnry, .wcry, .wncry e .wncrypt. Sendo necessária uma chave de 128bits-AES para restaurar os arquivos alvos.

Análise do arquivo wannacry.exe (https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100)

3. Recomendações

- Manter os sistemas atualizados para a versão mais recente ou aplicar os patch conforme orientação do fabricante.
- Isolar a máquina da rede, ao primeiro sinal de infecção por malware;
- Verificar o tráfego de máquinas internas para domínios não usuais ou suspeitos;
- Monitorar as conexões internas e não usuais entre máquinas da rede, a fim de evitar o movimento lateral de propagação do malware;
- Garantir o backup atualizado dos arquivos locais e dos Armazenados em Servidores de Arquivos;
- Manter o antivírus, aplicação de "*Patchs*" de segurança e a "*blacklist"* (filtro "antispam") de e-mail atualizados;
- 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-mail suspeitos ou não reconhecidos como de origem esperada.

4. Sugestões para Mitigação do Problema

- Isolar a rede infectada e aplicar o patch conforme Bolentim MS17-010 da Microsoft – Crítico;
- Bloquear as portas UDP 137, 138 e TCP 139, 445 até solucionar o problema;
- Alguns usuários identificaram arquivos @Please_Read_Me@.txt ou com a extensão .WNCY;
- 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; e
- Não é recomendável, em nenhuma hipótese, o pagamento de valores aos atacantes.

Referências:

- http://www.ctir.gov.br/arquivos/alertas/2016/ALERTA_2016_02_AtaquesRansomware.pdf
- 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://www.us-cert.gov/ncas/alerts/TA16-091A
- https://www.us-cert.gov/ncas/alerts/TA17-132A#revisions
- https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Brasília-DF, 12 de maio de 2017.

Equipe do CTIR Gov