**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 04/2017 – Ataques de *Ransomware Petrwrap/Petya*

## 1. Descrição do Problema

Temos recebido dos órgãos e de nossos colaboradores, alertas sobre ataques de *Ransomware Petwrap/Petya*, *tendo* como alvo o Leste da Europa, Rússia, Ucrânia, França, Espanha e Holanda. Esta variação de *Ransomware* é conhecida por Petrwrap/Petya.

O atacante explora as mesmas vulnerabilidades do *Ransonware Wanacry*, 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

Petwrap/Petya atua de forma um pouco diferente, em vez de criptografar arquivos individualmente, nega o acesso ao sistema atacando estruturas de baixo nível no disco, criando seu próprio *Kernel* com 32 setores.

O *Ransomware* atua no *Master Boot Record* (MBR) carregando o *Kernel* malicioso e criptografando o *Master File Table* (MFT) tornando o sistema inacessível.

Análise do arquivo petwrap.exe: (https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?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;
- 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**:


- https://www.us-cert.gov/ncas/current-activity/2017/06/27/Multiple-Petya-Ransomware-Infections-Reported.
- http://thehackernews.com/2017/06/petya-ransomware-attack.html?m=1
- http://blog.checkpoint.com/2017/06/27/global-ransomware-attack-spreading-fast/
- https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0205.html
- 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, 27 de junho de 2017.

Equipe do CTIR Gov