Departamento 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 06/2018 - Ataques para Mineração de Criptomoedas - *CryptoJacking*.

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

1. Descrição

Tem sido observada a migração de ataques *Ransomware*, para ataques *Criptojacking,* que se trata do uso dos recursos de processamento de CPU para minerar criptomoedas, sem o consentimento ou autorização prévia de seus usuários. As duas principais formas de infecção por *Cryptojacking são* por *malware, ou por JavaScript* de mineração no navegador, o preferido entre os atacantes, principalmente por não requerer instalação do arquivo malicioso.

2. Sistemas Afetados

- Sistemas que utilizam o JavaScript sem filtro de conteúdo;
- Sistemas vulneráveis a execução maliciosa de arquivos.

3. Impacto

Este ataque, sendo efetivo permite:

- Uso excessivo de processamento do CPU para mineração de criptomoeda;
- Participação em *Botnets* maliciosas;

4. Recomendações

- Usar extensões que bloqueiam domínios que se associam a scripts de criptografia e restringem a permissão para que extensões não autorizadas do navegador obtenham acesso ou executem processos;
- Restringir a sites que entregam *scripts* para evitar o uso de *cryptojacking* na navegação;
- Desabilitar privilégios de rede para qualquer site / *script* de *cryptojacking* detectado;
- No caso de queda do desempenho da máquina, identificar o processo que estiver sobrecarregando a memória e verificar se há relação com processos de mineração.
    - Caso positivo, interromper o processo e o incluir em *blacklist*, suspendendo sua execução.
- Manter os sistemas, o *antivírus*, aplicação de "*Patchs*" de segurança e a "*blacklist*" (filtro "*antispam*") de *e-mail* atualizados para a versão mais recente possível ou aplicar os *patch* conforme orientação do fabricante.
- Na impossibilidade de atualizações em sistemas legados, avaliar a implantação do *Virtual Patching* (https://cipher.com/br/2017/08/04/virtual-patching-isto-e-para-voce/)
- 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;
- Rever a política de privilégios administrativos nas máquinas clientes, a fim de restringir a instalação /execução de binários e ou executáveis desconhecidos; e
- Realizar campanhas internas, alertando os usuários a não clicar em *links* ou baixar arquivos de *e-mail* suspeitos ou de remetentes não reconhecidos.

5. Referências

- https://computerworld.com.br/2018/04/04/cryptojacking-como-detectar-e-evitar-o-malware-de-mineracao-de-criptomoedas/http://dsic.planalto.gov.br/legislacao/RequisitosMnimosSIparaAPF.pdf
- https://www.fireeye.com/blog/threat-research/2018/02/cve-2017-10271-used-to-deliver-cryptominers.html
- https://www.symantec.com/security_response/attacksignatures/detail.jsp?asid=30358