CAIS-Alerta [25/10/2017]: Ataque massivo do ransomware Bad Rabbit

Prezados,

O CAIS alerta para um novo ataque massivo de ransomware que tem afetado diversas organizações na Europa e Ásia. O ransomware Bad Rabbit afeta sistemas operacionais Windows cifrando os arquivos e se propagando para outros equipamentos que estejam conectados na mesma rede.

Descrição

O ransomware, aparentemente uma variante do NotPetya, infecta usuários que acessam sites comprometidos solicitando que seja realizado o download de uma atualização falsa do Adobe Flash Player, caso o usuário realize o download do arquivo e execute o mesmo, é realizado a cifragem dos dados.

Após a infecção, o ransomware tenta se propagar através da rede local via protocolo SMB, coletando credenciais locais da máquina infectada buscando acesso administrativo em outros computadores da rede.

Nos ambientes infectados é solicitado à vítima o pagamento de uma taxa para envio da chave que poderá decifrar os dados. Porém, de acordo com relatos conhecidos, o pagamento da taxa de resgate ao usuário malicioso não garante que o mesmo irá enviar a chave para decifrar os arquivos, o que torna importante realizar regularmente o backup dos arquivos para recuperação quando necessário.

Sistemas impactados

Windows XP
Windows Vista
Windows Server 2008
Windows 7
Windows 8.x
Windows Server 2012
Windows 10
Windows Server 2016

Recomendações de Proteção
1. Manter o backup dos dados atualizados;
2. Manter o sistema operacional atualizado com os patches de segurança;
3. Manter o sistema de proteção antimalware atualizado;
4. Restringir o acesso a porta 445;
5. Utilizar contas administrativas nos sistemas somente quando necessários;
6. Desabilitar o WMIC(Windows Management Instrumentation Command-line) caso o mesmo não esteja sendo utilizado;
7. Isolar computadores Infectados;
8. Realizar atualização do Adobe Flash Player somente no site oficial.

Identificadores CVE (http://cvw.mitre.org)

Não informado.

Mais informações

https://www.group-ib.com/blog/badrabbit
https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887/
https://blog.qualys.com/news/2017/10/24/bad-rabbit-ransomware

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricante.

Os alertas do CAIS também são oferecidos no Twitter:

Siga @caisrnp

Atenciosamente,

CAIS/RNP


```
#####################################################################
#   CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)          #
#       Rede Nacional de Ensino e Pesquisa (RNP)                    #
#                                                                   #
# cais em cais.rnp.br    http://www.rnp.br/servicos/seguranca       #
# Tel. 019-37873300      Fax. 019-37873301                          #
# Chave PGP disponivel   https://www.cais.rnp.br/cais-pgp.key       #
#####################################################################
```