-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Prezados,

O CAIS alerta para um recente ataque massivo de ransomware que tem afetado diversas organizações na Europa e America Latina. O ransomware afeta sistemas Windows cifrando diversos arquivos em discos rígidos, pendrives e unidades de rede podendo, assim, se propagar a outros equipamentos que estejam conectados na mesma rede.

Descrição

O ransomware, conhecido pelas variantes de WannaCry ou HydraCrypt, infecta computadores utilizando o sistema operacional Microsoft Windows através de uma vulnerabilidade no serviço SMB, utilizado para o compartilhamento de arquivos via rede. Quando o usuário executa um arquivo malicioso enviado pelo atacante, normalmente um arquivo compactado do tipo RAR, inicia-se um processo de cifragem de arquivos no computador da vítima. Além disso, conforme dito anteriormente, o ransomware pode propagar-se através da rede local podendo afetar também outras máquinas que executem o mesmo sistema operacional. Quando o computador é afetado, os arquivos cifrados passam a ser identificados pela extesão ".wcry". Após este processo, é solicitada 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.

A vulnerabilidade do serviço SMB já foi alvo de alerta publicado e enviado pelo CAIS em 19/04/2017, podendo ser visto no link:
https://www.rnp.br/sites/default/files/vulnerabilidade_servico_smbv1_da_microsoft.pdf

O CAIS recomenda a todos os administradores de redes e sistemas que verifiquem a integridade das cópias de segurança dos arquivos da suas respectivas Instituições, assim como as rotinas de backup. É recomendada também a aplicação das correções disponíveis no comunicado "CAIS-Alerta:Vulnerabilidades no serviço SMBv1 da Microsoft". Além disso, recomenda-se que as soluções antimalware estejam atualizadas com as últimas versões fornecidas pelo desenvolvedor.

Sistemas impactados

Windows Vista SP2
Windows Server 2008
Windows Server 2008 R2

Windows 7
Windows 8.1
Windows Server 2012
Windows Server 2012 R2
Windows 10
Windows Server 2016

Correções disponíveis

Aplicar as correções recomendadas no alerta "CAIS-Alerta:Vulnerabilidades no serviço SMBv1 da Microsoft".
Atualizar as soluções de antimalware para suas últimas versões disponibilizadas pelos desenvolvedores.
Realizar cópias de segurança de arquivos e sistemas e aplicar medidas para assegurar sua integridade e funcionamento.

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

Mais informações
https://isc.sans.edu/forums/diary/Massive+wave+of+ransomware+ongoing/22412/ - Regra Emerging Threats para identificar ransomware wannacry no seu IDS
http://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html
https://www.rnp.br/sites/default/files/vulnerabilidade_servico_smbv1_da_microsoft.pdf
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0147
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
https://www.virustotal.com/en/file/a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3/analysis/
https://www.hybrid-analysis.com/sample/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa?environmentId=100
https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

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

Os alertas do CAIS também podem ser acompanhados pelas redes sociais da RNP. Siga-nos!
Twitter: @RedeRNP
Facebook: facebook.com/RedeNacionaldeEnsinoePesquisaRNP.

Atenciosamente,

CAIS/RNP


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



-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1

iQCVAwUBWRYLcekli63F4U8VAQKOBQP/bhTi3amAr9kHttX7VO1exKL0i+stMClf
jyl1WFbV+PlK2rRpL4/0yuW4Y4OfKaPnBxfDShtiBVCO1WfFy0FRw4iD0vBax2b+
6nRhfvD2GUdD0ivQMoY2YT3cP0xYdBnbL/ipHJcvqLybOYmuvoTodmfav48Ub0IJ
8Z2G/87kdl0=
=aprG
-----END PGP SIGNATURE-----