-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

CAIS-ALERTA[27/06/2017]:Ataque massivo do ransomware NotPetya

O CAIS alerta para um recente ataque massivo de ransomware a várias organizações na Europa, Estados Unidos e América Latina que se afeta sistemas Windows e cifra
o registro de inicialização do sistema(MBR), podendo se propagar a outros computadores que estejam na mesma rede.

Descrição

O ransomware, batizado como NotPetya, afeta computadores Microsoft Windows e se propaga a outros computadores em uma rede local através de uma vulnerabilidade no
serviço SMBv1, a mesma utilizada pelo ransomware WannaCry.Após a infecção, o ransomware cifra a tabela de arquivos mestre(MTF), utilizada por sistemas de arquivos
NTFS e se instala na partição de inicialização do disco(MBR).O malware ainda agenda uma reinicialização forçada do sistema entre 10 e 60 minutos, e, após o reinício, trava o acesso do usuário ao sistema em uma tela solicitando pagamento de uma taxa para liberação do computador.

Além do ransomware NotPetya explorar a vulnerabilidade no serviço SMBv1 para se propagar pela rede local, ele também pode utilizar as ferramentas PSEXEC e WMIC,funções do Windows que permitem a administradores a capacidade de gerenciar computadores remotamente e em massa.A propagação do malware usando essas ferramentas é realizada usando as credenciais acesso do usuário, usando-as como vetor de infecção em outros sistemas, mesmo aqueles nos quais já tenham sido aplicados o patch de correção da vulnerabilidade referente ao serviço SMBv1(MS17-010).

Caso você seja o administrador do ambiente, uma das formas de identificar se o sistema foi afetado é verificar no Agendador de Tarefas do Windows(AT) a existência
indevida de alguma tarefa de reinicialização do sistema.

O CAIS recomenda a aplicação das correções disponíveis no comunicado "CAIS-Alerta:Vulnerabilidades no serviço SMBv1 da Microsoft" enviado pelo CAIS em 19/04/2017.
Além disso, recomenda a desativação das chamadas remotas via wmi e psexec, quando o mesmo estiver instalado e a verificação das atualizações das soluções antimalware com as últimas versões fornecidas pelo desenvolvedor.

O CAIS também recomenda a todos os administradores de redes e sistemas que verifiquem a integridade das cópias de segurança dos arquivos das suas respectivas instituições, assim como as rotinas de backup.

Sistemas Impactados

Windows XP (todas as versões)
Windows Vista (todas as versões)
Windows Server 2003 (todas as versões)
Windows Server 2008 (todas as versões)
Windows Server 2012 (todas as versões)
Windows Server 2016 (todas as versões)
Windows 7 (todas as versões)
Windows 8 (todas as versões)
Windows 8.1 (todas as versões)
Windows 10 (todas as versões)

Correções disponíveis

Aplicar as correções recomendadas no alerta "CAIS-Alerta: Vulnerabilidades no serviço SMBv1 da Microsoft" enviado pelo CAIS em 19/04/2017.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:

http://www.techtudo.com.br/noticias/2017/06/petya-ou-notpetya-novo-ransomware-usa-mesma-falha-do-wannacry.ghtml
https://blog.varonis.com/petya-ransomware-outbreak-what-you-need-to-know/
https://virustotal.com/en/file/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745/analysis/
https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100
https://www.extremetech.com/internet/251711-notpetya-ransomware-locking-computers-across-world
https://gist.github.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759
https://isc.sans.edu/diary/22560
https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know
https://msdn.microsoft.com/en-us/library/aa822854%28v=vs.85%29.aspx
https://securelist.com/schroedingers-petya/78870/

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.

```
#################################################################
#   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

iQCVAwUBWVMDhekli63F4U8VAQIIggP9EXIeyppaDI63lEz+02dNszFXLSCZaBM0
ELcAQKYrd2aLrN02eCl45HoPBGhsMM0GrhQKCNaCOT3uqpZiYAYk8nBjKFLS719S
bqhqsY2JbMqHPTw2q2bXfXGGBdvFyIeqW5xndSn3N3hQ2rmqUXJxQ6wQge4atXHq
WaMCNao7RqE=
=Jf1x
-----END PGP SIGNATURE-----
```