MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
7º CENTRO DE TELEMÁTICA DE ÁREA
(7º CCTA/1997)

DIEx nº 21-Stir/SSC/7ºCTA - CIRCULAR
EB: 64195.001780/2017-12

URGENTÍSSIMO

Brasília, DF, 15 de maio de 2017.

Do Chefe do 7º Centro de Telemática de Área
Ao Sr Chefe de Gabinete da Secretaria de Economia e Finanças, Chefe de Gabinete da Secretária Geral do Exército, Chefe de Gabinete do Comando Logístico, Chefe de Gabinete do Comando de Operações Terrestres, Chefe de Gabinete do Departamento Geral do Pessoal, Chefe de Gabinete do Departamento de Engenharia de Construção, Chefe do Estado-Maior do Centro de Comunicações e Guerra Eletrônica do Exército, Chefe do Estado-Maior do Comando Militar do Planalto, Chefe do Estado-Maior do Comando da 11ª Região Militar, Chefe do Estado-Maior do Comando da 3ª Brigada de Infantaria Motorizada, Chefe do Estado-Maior do Comando de Operações Especiais, Subchefe do Centro de Comunicação Social do Exército, Subchefe do Centro de Controle Interno do Exército, Subchefe do Estado-Maior do Exército
Assunto: prevenção contra ataque cibernético

1. Sobre o assunto em pauta, informo-vos que no dia 12 de maio de 2017 dezenas de países, incluindo o Brasil, foram vítimas de um ataque cibernético que atingiu o sistema operacional Microsoft Windows.

2. Por meio de uma falha de segurança do próprio sistema operacional, o *malware* é capaz de criptografar arquivos nas máquinas infectadas e se espalhar pela Internet e também por redes internas. O objetivo do ataque é exigir o resgate dos arquivos criptografados por meio de pagamento que deve ser feito em *Bitcoins*. Caso a vítima não pague o resgate dentro de um certo prazo, a chave para descriptografar os arquivos é deletada e a recuperação dos dados é praticamente impossível.

3. A correção para essa falha de segurança já foi disponibilizada pela própria Microsoft em março deste ano, mas ainda assim o ataque foi bem sucedido tendo em vista que muitos usuários não instalaram o *patch* de segurança em suas máquinas.

4. Como medida de segurança contra esse ataque, este Centro recomenda aos

administradores de rede que verifiquem o quanto antes, se os computadores sob sua responsabilidade estão devidamente atualizados. Caso algum computador tenha sido infectado com o *malware*, ele deve ser imediatamente isolado da rede e formatado. O mesmo procedimento também deve ser feito para servidores que utilizam o *Windows Server*.

5. Como orientação adicional contra esse tipo específico de ataque, este Centro reforça a necessidade da adoção de rotinas de *backup* para sistemas críticos. A partir dessas cópias de segurança os dados não serão perdidos em defintivo em caso de comprometimento por meio de criptografia.

6. É imprescindível também que haja, em âmbito interno, campanhas de conscientização voltadas aos usuários. As principais formas de proliferação dessas pragas virtuais são o uso descontrolado de mídias removíveis (*pen drives*, HD externo, celulares), desativação de controles básicos de segurança (*firewall* do *Windows*, antivírus) e *download* de arquivos de origem suspeita. Os usuários também devem ser orientados a jamais acessarem *links* ou fazerem *downloads* de arquivos enviados em anexos de *e-mail* por remetentes desconhecidos e com assunto suspeito.

7. Por fim, qualquer incidente de segurança envolvendo a rede corporativa do Exército pode ser relatado para a Seção de Segurança Cibernética do 7º CTA, por meio do *e-mail* stir@7cta.eb.mil.br.

EDÉSIO CESAR FARIAS DOS SANTOS - TC
Rsp pela Chefia do 7º Centro de Telemática de Área

"150 ANOS DA RETIRADA DA LAGUNA E DA RETOMADA DE CORUMBÁ: PERSEVERANÇA NA DEFESA DO TERRITÓRIO E NA INTEGRAÇÃO DO OESTE"