COMUNICADO DE IMPRENSA

Lisboa, 25 de outubro de 2017, 16h - O Centro Nacional de Cibersegurança (CNCS) tomou conhecimento pelas 21h30min de 24 de outubro de 2017, através das redes de cibersegurança que integra, de uma nova campanha de ransomware, a que foi atribuído internacionalmente o nome de Bad Rabbit.

Os serviços técnicos do Departamento de Operações (DO) do CNCS de imediato aumentaram o seu nível de alerta, por forma a avaliar o impacto e lançar um comunicado para as redes nacionais de confiança em cibersegurança com os indicadores de compromisso e possíveis medidas de mitigação.

Este ransomware caracteriza-se pela propagação em modo de «drive-by download» (download não intencional por parte do utilizador) no momento que visita um website, fazendo-se passar por uma atualização do Adobe Flash. A vítima tem de executar manualmente o ficheiro. Após a execução do ficheiro, o computador reinicia e começa o processo de cifra sendo colocada uma nota de resgate. Visitando o website sugerido é possível verificar a quantia a pagar no momento (0.05฿). Após os ficheiros estarem cifrados, a extensão é alterada para .encrypted.

A propagação lateral é feita por SMB, não sendo a vulnerabilidade Eternal Blue, mas sim um ataque de força-bruta ou recolha de credenciais com software apropriado.

Como forma de contenção o CNCS recomenda a atualização dos antivírus e o alerta a todos os utilizadores para não efetuarem atualizações do Adobe Flash de fontes não fidedignas.

Ainda neste contexto, o CNCS partilha ainda indicadores de compromisso e a informação de que, ao serem criados os ficheiros c:\windows\infpub.dat e c:\windows\cscc.dat e ao serem removidas todas as suas permissões, fará com que o ataque não se consiga efetuar.

Esta nova campanha está diretamente ligada aos ataques sentidos durante o dia de ontem no aeroporto de Odessa e no metro de Kiev, sendo o governo Russo apontado como atacante pelo governo da Ucrânia.

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt

É ainda importante relacionar esta nova campanha com as notícias, saídas dias antes, da necessidade de fazer a atualização do Adobe Flash por existir uma vulnerabilidade explorada pela APT28.

No final da noite de ontem estas eram as estatísticas dos países mais infetados:

- Rússia: 65%
- Ucrânia: 12.2%
- Bulgária: 10.2%
- Turquia: 6.4%
- Japão: 3.8%
- Outros: 2.4%

Centro Nacional de Cibersegurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 049 74 00 | Fax (+351) 21 303 17 11 | cncs@cncs.gov.pt