NOTA MAKLUMAN SgCERT BIL. 5/2017
PADA 25 Oktober 2017

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**: Ancaman *ransomware 'Bad Rabbit'*** Sejenis variasi daripada *ransomware WannaCry* dan *Petya*
Tarikh Dikesan	**: 24 Oktober, 2017**
Bilangan Agensi Terlibat	**: Semua Penjawat Sektor Awam dalam Rangkaian SabahNet**

Sistem Operasi/Aplikasi Berisiko

- Semua Sistem Operasi berasaskan *Microsoft Windows.*

Kaedah Serangan

- Modus operandi hampir sama dengan serangan WannaCry (sgcert-2-2017[WannaCryRansomware]) dan Petya (sgcert-3-2017[Petya-Ransomware]) iaitu meminta wang tebusan.
- Melalui laman sesawang yang dikompromi dimana pelawat laman tersebut akan diminta memuatturun dan seterusnya menginstal perisian palsu Adobe Flash dan dengan itu akan menjangkiti komputer sendiri.

Impak Serangan

- Impak sepenuhnya belum diketahui pada masa nota makluman ini ditulis.
- Namun yang telah diketahui, 'Bad Rabbit'' telah menular ke beberapa negara iaitu Russia, Ukraine, Turkey dan Germany.
- Komputer yang berjaya ditembusi oleh *'Bad Rabbit'* akan dikunci dan tidak dapat dibuka/diakses kecuali setelah wang tebusan sebanyak 0.05 Bitcoin (lebih kurang RM1185.00) dan untuk memulihkan komputer tersebut.

Tindakan Penyelesaian

Tindakan Pengukuhan:

- Pastikan perisian antivirus komputer masing-masing mempunyai *'pattern update'* terkini.
- Sila rujuk ***blog cybereason***[1] yang tercatit dalam **Maklumat Lanjut** untuk langkah-langkah tindakan pengukuhan.

Amalan yang Digalakkan:

- Selalu membuat salinan (backup) kepada data-data penting.
- Tidak digalakkan untuk membayar wang tebusan kerana tiada jaminan komputer anda akan dilepaskan.

Maklumat Lanjut

- http://www.bbc.com/news/technology-41740768
- https://techcrunch.com/2017/10/24/badrabbit-notpetya-russia-ukraine-ransomware-malware/?ncid=mobilenavtrend
- [1]https://www.cybereason.com/blog/cybereason-researcher-discovers-vaccine-for-badrabbit-ransomware?hs_amp=true
- Untuk Pertanyaan: *Sila hubungi melalui alamat e-mel Keselamatan.JPKN@sabah.gov.my*

Hasil Penyelidikan oleh:
Donald Monjohi
Head of Research and Development Team, sgCERT
Urusetia sgCERT, Bahagian Keselamatan
Jabatan Perkhidmatan Komputer Negeri