NOTA MAKLUMAN GCERT BIL. 5/2017
PADA 25 OKTOBER 2017

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**Bad Rabbit Ransomeware**
Tarikh Dikesan	**25 Oktober 2017**
Bilangan Agensi Terlibat	**Semua CERT agensi dibawah Sektor Perkhidmatan Kerajaan di mana MAMPU (GCERT) bertindak sebagai Ketua Sektor**

Pengenalan

GCERT telah menerima maklumat daripada National Cyber Coordination and Command Centre (NC4) di mana, berkemungkinan berlaku pencerobohan laman web yang mensasarkan laman web Malaysia.

Kesan Serangan

Kebocoran maklumat, kehilangan maklumat, gangguan perkhidmatan dan integriti maklumat dikompromi.

Penerangan Ringkas

- Bad Rabbit Ransomware telah dikesan di Russia, Ukraine, Turki dan German.
- Berdasarkan kajian dari Laman Web Virus Total, majoriti antivirus yang ada tidak dapat mengesan Malware tersebut.
- Kebanyakan firma keselamatan menyatakan bahawa Malware ini tersebar melalui pengemaskinian Adobe Flash yang palsu.
- Bad Rabbit akan menuntut bayaran wang tebusan melalui Bitcoin untuk menyahsulitkan fail yang telah dijangkiti.
- Oleh itu, organisasi digesa mengambil tindakan yang diperlukan untuk menghalang organisasi anda menjadi mangsa serangan ini.

Sistem Pengoperasian/Aplikasi Berisiko

Semua versi sistem pengoperasian Ms Windows

Cadangan Tindakan Pengukuhan

1. Memastikan semua sistem pengoperasian Ms Windows dikemaskini dengan tampalan keselamatan terkini;
2. Memastikan pengguna emel tidak membuka lampiran atau klik pada pautan di dalam e-mel yang diragui;
3. Memastikan *signature* anti-virus / anti-malware adalah terkini dan berfungsi;
4. Menyekat akses setiap *port* dan *services* yang tidak berkenaan;
5. Memantau persekitaran anda dengan teliti dari sebarang anomali;
6. Tidak sesekali mengikut arahan bayaran wang tebusan;
7. Jangan sesekali mengemaskini Adobe Flash dari sumber yang mencurigakan.
8. Memastikan sekatan capaian kepada laman sesawang berikut:
    - **http://1dnscontrol.com/**
9. Jika disyaki bahawa *server* anda telah dikompromi, *reset* semua nama pengguna dan kata laluan dengan segera; dan
10. Laporkan sebarang insiden berkaitan ke GCERT.