NOTA MAKLUMAN GCERT BIL. 1/2017
PADA 9 MAC 2017

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**Ancaman Serangan Siber Dari Luar Negara**
Tarikh Dikesan	**9 Mac 2017**
Bilangan Agensi Terlibat	**Semua**

Sistem Pengoperasian/Aplikasi Berisiko

- Semua, terutamanya sistem pengoperasian Ms Windows.

Keterangan Serangan

- Penyerang akan menggunakan kod jahat (*malware*) untuk melumpuhkan sistem ICT agensi; dan/atau
- Penyerang akan mengambil peluang terhadap kelemahan pada sistem ICT agensi bagi menceroboh dan memuat naik kod jahat untuk mendapatkan kawalan penuh ke atas sistem ICT agensi.

Kaedah Serangan

- Penceroboh menyebarkan kod jahat (*malware*) melalui kaedah e-mel. Pengguna yang melayari laman web tertentu (yang di akses melalui link dalam e-mel) akan memuat turun kod jahat ke komputer pengguna. Kod jahat berkenaan seterusnya akan memuat turun lain-lain aplikasi yang berbahaya yang boleh digunakan oleh penceroboh untuk mendapatkan maklumat Kerajaan dan/atau mengawal sepenuhnya aset ICT Kerajaan.

Cadangan Tindakan Pengukuhan

- Melaksanakan pengemaskinian *patches* terhadap semua peranti dan sistem pengoperasian.
- Memastikan perisian *antivirus* dilengkapi dengan virus *signature* yang terkini dan menjalankan *full system scanning*.
- Memastikan semua storan mudah alih (*removable storage*) di imbas terlebih dahulu sebelum digunakan; cth: USB *drive*, *mobile hard disk*, dll.
- Memaklumkan semua pengguna agar tidak melayari laman web melalui pautan di dalam e-mel.
- Membuat konfigurasi *firewall* seperti berikut:
  a. *Block all outgoing traffic to* IP 196.202.33.106 *and* 161.139.39.234 *port* TCP\8443;
  b. *Block all outgoing traffic to* IP 203.113.122.163, 41.21.201.107 *and* 62.0.79.45 *port* TCP\443; dan
  c. *Block all outgoing traffic to* IP 158.69.115.115 *and* 192.99.223.115
- Memasang IPS/IDS/WAF/MyGSOC agen & WSM (sekiranya ada).
- Membuat konfigurasi IPS agar menghalang trafik yang mengandungi *payload* ñASDASDADSAò
- Aktifkan sistem log bagi semua sistem yang ada.