NOTA MAKLUMAN GCERT BIL. 2/2017
PADA 14 MEI 2017

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**WannaCry Ransomware**
Tarikh Dikesan	**12 Mei 2017**
Bilangan Agensi Terlibat	**Semua CERT agensi dibawah Sektor Pentadbiran Kerajaan yang MAMPU (GCERT) bertindak sebagai Ketua Sektor**

Sistem Pengoperasian/Aplikasi Berisiko

- Sistem pengoperasian berasaskan Windows

Kaedah Serangan

- *WannaCry Ransomware* adalah sejenis *malware* yang menggunakan kelemahan fungsi perkongsian fail melalui ***SMB Windows TCP Port 445*** yang dibocorkan oleh *ShadowBrokers.*
- Malware ini mungkin disebarkan menerusi kelemahan sistem Windows yang telah dipatch oleh *Microsoft MS17-010* yang dikeluarkan untuk menampung kelemahan SMB.
- Terdapat enam jenis kelemahan MS17-010 dengan aktiviti eksploitasi kod *'EternalBlue'* yang memberi kesan kepada SMBv2
- *WannaCry Ransomware* disebarkan melalui pelbagai cara termasuk *spam* email dengan penyebaran secara pautan (*link)* dan fail kepilan *(attachment*)
- Komputer yang telah dijangkiti *WannaCry Ransomware* menggunakan keupayaan mengimbas *TCP Port 445 (Server Message Block),* menyebarkan virus dengan membuat penyulitan keatas fail dalam hos sehingga menyebabkan pengguna gagal membuka fail tersebut, mungkin berlaku kehilangan data atau gangguan kepada operasi dan menjejaskan imej organisasi.
- *Ransomware* ini akan menuntut bayaran wang tebusan melalui Bitcoin untuk menyahsulitkan fail tersebut.

Kesan Serangan

- Mengganggu/Melumpuhkan sistem penyampaian perkhidmatan Kerajaan
- Menjatuhkan imej Kerajaan
- Kehilangan data/maklumat jika tiada sandaran (backup) di buat sebelum ini

Cadangan Tindakan Pengukuhan

- Memastikan sekatan alamat IP berikut:
  - 205.186.153.200
  - 96.127.190.2
  - 184.154.48.172
  - 200.58.103.166
  - 216.145.112.183
- Memastikan sekatan terhadap alamat email alertatnb@serviciobancomer.com
- Memastikan sekatan capaian kepada laman sesawang berikut:
  - www.rentasyventas.com/incluir/rk/imagenes.html?retencion=081525418

    - http://www.ren tasyventas.com/incluir/rk/imagenes.html?retencion=081525418
    - https://graficagibin.com.br/loja/q.hta
- Memastikan sistem operasi Windows dikemaskini dengan *patches* terkini
- Bagi sistem pengoperasian yang tidak lagi disokong oleh pihak Microsoft (Windows Server 2003, Windows XP, Windows Vista dan Windows 8), tampalan keselamatan hendaklah dimuat turun dan dipasang secara manual dari laman web Microsoft Update Catalog
- Memastikan fail-fail penting telah dibuat salinan *backup,* diuji integriti backup tersebut dan boleh direstore semula jika diperlukan serta memastikan backup ini disimpan offline
- Memastikan *anti-virus dan anti-malware* organisasi telah dikemaskini dengan *patches* terkini
- Menyekat SMB (port 139 dan 445) dari akses luaran
- Menyekat akses rangkaian dalaman agensi bagi perkhidmatan perkongsian fail (port 139 dan 445) kecuali capaian terhadap server perkongsian fail yang sah sahaja
- Menghentikan/Menutup perkhidmatan SMB (port 139 dan 445) jika tidak diperlukan
- Tidak sesekali mengikut arahan bayaran wang tebusan
- Memastikan warga organisasi dimaklumkan akan ancaman ini dan sentiasa berwaspada dengan memastikan fail kepilan dan pautan yang diterima melalui emel yang diragui tidak dibuka
- Memastikan pemantauan rapi dilaksanakan dan segera melaporkan sebarang aktiviti yang dicurigai

Maklumat Lanjut

- https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- http://www.nc4.gov.my/view_alert_advisory?id=5916c82de4b0f9d70f3eae30
- http://www.catalog.update.microsoft.com/search.aspx?q=4012598
- http://www.zdnet.com/article/wannacrypt-ransomware-microsoft-issues-patch-for-windows-xp-and-other-old-systems/