NOTA MAKLUMAN GCERT BIL. 1/2015
PADA 28 APRIL 2015

KETERANGAN ANCAMAN	
Nama dan Jenis Ancaman	**Ransomware Malware**
Tarikh Dikesan	**28 April 2015**
Bilangan Agensi Terlibat	**Semua**

Sistem Pengoperasian/Aplikasi Berisiko

- Semua sistem pengoperasian.

Kaedah Serangan

- *Ransomware* adalah sejenis *malware* atau virus berbahaya yang menyerang komputer dan menyekat akses kepada sistem/komputer sehingga bayaran tertentu dibuat kepada pencipta virus untuk membuka sekatan
- Aplikasi berbahaya ini cuba memaksa mangsa membayar wang tebusan dengan mengeluarkan mesej *pop-up* di atas skrin komputer
- Mesej *pop-up* ini menyatakan komputer pengguna sudah dikunci dan semua fail di dalamnya dienkrip sebelum meminta wang tebusan dibayar bagi memulihkan semula akses ke komputer mereka.

Medium Serangan

- *Ransomware* menyerang pengguna melalui emel yang tidak dikenali serta melampirkan fail berbahaya untuk dimuat turun. (Contohnya *.cab)
- *Ransomware* boleh menyerang dengan menyediakan *link* yang memohon pengguna untuk klik pada *link* tersebut dan akan membawa pengguna ke laman berbahaya.

Kesan Serangan

- Pencipta *Ransomeware* meletakkan mangsa dalam ketakutan dan panik, seterusnya mengakibatkan mangsa klik pautan ataupun membuat proses bayaran wang tebusan yang mana mengakibatkan jangkitan malware atau virus yang lain pula.
- Contoh mesej biasa dipamerkan adalah :
    - '*Your computer has been infected with a virus. Click here to resolve the issue',*
    - *'Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine'*
    - *'All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data'.*
- Sasaran *Ransomeware* merupakan pengguna di rumah, operasi perniagaan dan syarikat. *Ransomware* memberi kesan yang menyebabkan kerugian akibat pembaikian dan pemulihan sistem atau fail yang rosak serta boleh menjejaskan reputasi syarikat.

Cadangan Tindakan Pencegahan

- Kerap membuat *backup* data ke dalam *external hard disk / thumdrive* persendirian
- Jangan klik *link* dalam mana-mana emel yang tidak dikenali sama ada emel rasmi atau tidak rasmi (yahoo, gmail dan lain-lain)
- *Bookmarked* laman yang dipercayai dan selalu dilayari oleh pengguna untuk menghindari daripada memasuki ke laman yang berbahaya.
- Sahkan alamat pengirim emel yang diterima sebelum klik mana-mana *link* yang dipaparkan dalam emel tersebut atau memuat turun lampiran berkenaan.

Cadangan Tindakan Pengukuhan

- Jangan sesekali mengikut arahan bayaran wang tebusan. Membayar wang tebusan tidak menjamin fail yang dienkrip boleh diakses semula tetapi akan mengakibatkan wang dan maklumat pengguna perbankan terdedah kepada penggodam.
- Mengemaskini perisian anti-virus.
- Memastikan sistem operasi dan perisian dikemaskini dengan *patches* terkini.

Maklumat Lanjut

- US CERT: Crypto Ransomware [online], https://www.us-cert.gov/ncas/alerts/TA14-295A
- MyCERT : https://www.mycert.org.my/en/services/advisories/mycert/2014/main/detail/1010/index.html