IMBAUAN TERKAIT AKTIVITAS SIBER BERBAHAYA YANG MEMANFAATKAN SITUASI CORONA VIRUS DI WUHAN

Pendahuluan

Kelompok kriminal siber dapat memanfaatkan situasi penyebaran Virus Corona di Wuhan untuk melacarkan kegiatan serangan siber / aktivitas siber berbahaya dengan mengirimkan surel/ email atau pesan yang membujuk pengguna untuk membuka tautan atau lampiran yang telah disisipi program berbahaya dengan menawarkan informasi terkait situasi Virus Corona di Wuhan.

File berbahaya yang dilampirkan dalam email atau pesan dapat **berupa file berekstensi pdf mp4 atau docx dengan tautan atau diberi nama file yang terkait dengan situasi terkini Virus Corona di Wuhan**, seperti **cara melindungi diri dari virus, informasi terkini ancaman atau prosedur deteksi virus**. File -file tersebut dapat disisipi trojan atau *worm* yang dapat **menimbulkan risiko kerusakan, modifikasi, pencurian data dan mengganggu operasi komputer dan jaringan komputer jika pengguna meng-klik tautan atau membuka dokumen lampiran tersebut**.

Saat ini sudah dilaporkan satu kasus aktivitas siber berbahaya yang memanfaatkan situasi Virus Corona di Wuhan. **yang diidentifikasi sebagai aktivitas *"Emotet malspam"* di Jepang**. Pada kasus tersebut **penjahat siber mengirim email yang disamarkan sebagai pemberitahuan resmi dari penyedia layanan kesejahteraan penyandang cacat dan pusat kesehatan masyarakat**. Email-email ini diklaim memberikan rincian informasi tentang langkah-langkah pencegahan terhadap virus, **untuk menarik calon korban untuk membuka lampiran jahat dalam email tersebut.**

Emotet sendiri merupakan program jahat yang tergolong sebagai trojan, dan pertama kali ditemukan untuk mencuri data finansial/ perbankan, dan pada umumnya disebarkan melalui *Phishing Campaign.*

Rekomendasi Prosedur Keamanan

Untuk menghindari jatuhnya korban karena aktivitas siber berbahaya khususnya Emotet. **Pengguna disarankan untuk tidak mengklik tautan dan membuka lampiran file yang terlihat mencurigakan dan jika pengirim pesan tersebut tidak dapat diverifikasi/ dari sumber yang tidak dipercaya**. Masyarakat / pengguna dapat memanfaatkan sumber informasi yang valid untuk mengetahui perkembangan informasi terkait virus Corona dari Situs Kementerian Kesehatan RI yang dapat diakses pada tautan berikut:

http://infeksiemerging.kemkes.go.id/category/situasi-infeksi-emerging/info-corona-virus/#.XjWI3iMxXD4

Berikut beberapa rekomendasi keamanan yang dapat diterapkan oleh pengguna / organisasi untuk meningkatkan sistem proteksi serangan Emotet:

1. **Gunakan Anti-Virus.**
   Mayoritas produk anti-virus yang ada dapat mendeteksi dan mem-blok varian emotet yang diketahui berserta *malware* turunannya, seperti "Trickbot". Gunakan Antivirus dengan fitur pembaruan otomatis untuk *signature* dan program/ perangkat lunak, dan lakukan *Full Scan* secara rutin.

2. **Lakukan pembaruan perangkat lunak secara rutin.**
   Usahakan untuk memeriksa dan melakukan pembaruan versi perangkat lunak dan sistem operasi yang digunakan dengan pembaruan terbaru, terutama pembaruan keamanan untuk meminimalisir risiko infeksi program jahat atau eksploitasi kerentanan oleh penjahat siber.

3. **Aktifkan Microsoft Office Macro hanya jika benar-benar diperlukan.**
   Dalam kebanyakan kasus, infeksi awal Emotet adalah melalui macro yang disematkan di dokumen Microsoft Office atau PDF. Pengguna disarankan untuk menonaktifkan macro secara *default*, dan membatasi izin yang memungkinkan eksekusi macro untuk mengurangi kemungkinan akses awal emotet melalui metode ini.

4. **Gunakan Fitur Penyaringan/ Filter Email.**
   Pengguna disarankan untuk menerapkan filter pada *gateway email* untuk menyaring email dengan indikator *spam malware* yang dikenal, dan memblokir alamat IP yang mencurigakan pada *firewall*. Email yang tampak mencurigakan harus segera dilaporkan ke departemen TI untuk diisolasi dan diselidiki. Tinjau pengaturan akun *Outlook/ mail client* lain secara teratur yang mungkin diatur untuk meneruskan semua *email* (*auto-forward*) secara otomatis, yang dapat mengakibatkan kebocoran data jika terjadi infeksi *malware*.

5. **Non-aktifkan layanan/ *service* yang tidak diperlukan.**
   Malware Emotet sering memanfaatkan kerentanan yang ditemukan pada *background service* untuk menyebar ke komputer lain dalam jaringan. *Remote Desktop Protocol* (RDP) adalah salah satu contohnya. Pengguna disarankan untuk menonaktifkan layanan tersebut jika tidak diperlukan, untuk mencegah *malware* mengeksploitasi layanan tersebut.

6. **Memasang perangkat lunak pengontrol Aplikasi.**
   Pengguna disarankan untuk menginstal perangkat lunak kontrol aplikasi yang menyediakan layanan *whitelisting* aplikasi dan / atau direktori. Hal ini bertujuan untuk membatasi aplikasi yang berjalan dan memastikan bahwa Aplikasi yang diizinkan saja yang dapat berjalan.

7. **Lakukan pencadangan data/file secara berkala.**
   Infeksi Emotet juga memungkinkan menjadi jalan masuk awal bagi Ransomware, oleh karena itu sangat penting untuk melakukan pencadangan data secara berkala untuk dapat melakukan pemulihan data jika terjadi infeksi Emotet atau Ransomware. Pada umumya Ransomware menginfeksi perangkat penyimpanan yang terhubung, sehingga perlu dipastikan bahwa terdapat cadangan data yang disimpan secara *offline* atau terputus

secara fisik pada jaringan atau koneksi apapun saat tidak digunakan untuk menghindari penyebaran *malware* pada data yang dicadangkan.

Referensi

[1] https://www.csa.gov.sg/singcert/alerts/malicious-cyber-activities-leveraging-wuhan-coronavirus-situation
[2] https://www.csa.gov.sg/singcert/advisories/emotet-malware-campaign-2019
[3] https://www.us-cert.gov/ncas/alerts/TA18-201A
[4] https://www.cyber.gov.au/threats/advisory-2019-131a-emotet-malware-campaign

Riwayat Dokumen

Versi 1.0: Januari 2020