[INFO] Ancaman Ransomware "Trigona”

2022-12-12 - Agent 174 - Comments (0) - General

Yth:

1. **Sekretaris Ditjen Perbendaharaan**
2. **Para Direktur Lingkup Kantor Pusat Ditjen Perbendaharaan**
3. **Tenaga Pengkaji Bidang Perbendaharaan**
4. **Para Direktur Utama Badan Layanan Umum**
5. **Para Kepala Kanwil Ditjen Perbendaharaan di Seluruh Indonesia**
6. **Para Kepala KPPN di Seluruh Indonesia**

Sehubungan dengan adanya ancaman malware khususnya ransomware dengan jenis varian baru yaitu "Trigona” untuk dapat memperhatikan beberapa hal sebagai antisipasi pencegahan dan penanganan terhadap ancaman ransomware Trigona agar tidak mengganggu kinerja dan layanan Kementerian Keuangan.

Ransomware jenis "**Trigona**" menyerang perangkat pengguna yaitu Personal Computer (PC)/Laptop yang menggunakan sistem operasi Windows dengan cara mengunci atau meng-enkripsi semua file/data didalamnya, sehingga tidak dapat diakses, dengan ciri-ciri ekstention file berubah menjadi ***._locked**. dan menampilkan permintaan tebusan sejumlah uang Cryptocurrency Monero.

Ransomware jenis "Trigona" ini menyebar dengan memanfaatkan kelemahan pada layanan Server Message Blok (SMB) atau yang biasa disebut sharing folder pada PC/laptop.

Langkah-langkah yang perlu dilakukan sebagai tindakan antisipasi pencegahan dan penangganan ancaman ransomware jenis "Trigona" atas arahan dari Tim OKI Kemenkeu adalah sebagai berikut:

1. Memastikan PC/Laptop terinstall **antivirus yang terupdate**, untuk perangkat kedinasan bisa menggunakan antivirus Mcafee atau Windows Defender dengan Signature terupdate.
2. Memastikan sistem operasi Windows PC/Laptop terinstall **Patch terupdate**.
3. Melakukan **disable port 445 (SMB)** pada OS Windows dan Firewall local Windows di PC/Laptop.
4. Melakukan backup data/file secara rutin dengan **memanfaatkan layanan Onedrive pada office 365**.

5. Apabila PC/Laptop ditemukan file/data dengan extention *._locked. agar segera melakukan tindakan :

- Mematikan atau melakukan isolasi jaringan PC/Laptop dengan mencabut koneksi kabel jaringan, dan
- Melaporkan pada Direktorat SITP c.q. Subdit Pengelolaan Data, Infrastruktur dan Keamanan Informasi, atau menghubungi Services Desk Pusintek pada semua channel.

Terima Kasih

#Salam_Sinergi

#Kemenkeu_Satu

#DJPb_Handal

#TIK_Aman