Sehubungan dengan ancaman Malware Ransomware jenis Wannacry atau Wannacrypt yang terjadi di seluruh dunia termasuk Indonesia, kami menghimbau kepada seluruh Pegawai di Lingkungan Pemkab Klaten yang menggunakan Sistem Operasi Windows untuk melakukan hal-hal pencegahan.

Langkah-langkah yang dapat dilakukan sebagai pencegahan sebelum memulai beraktivitas menggunakan komputer :

1. Sebelum menghidupkan komputer, putuskan koneksi internet dari komputer baik kabel LAN maupun wifi.
2. Backup data-data penting ke media lain (flashdisk, harddisk ext, dll) atau ke sistem operasi lain (mac, linux)
3. Setelah data selesai dibackup, internet bisa diaktifkan.
4. Lakukan update security. patch MS17-010 dapat di download di (tutorial terlampir) https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
5. Lakukan update antivirus dan full scan PC anda
6. Nonaktifkan fungsi macros dan SMBv1 (tutorial terlampir)
7. Nonaktifkan port 139, 445, dan 3389 (tutorial terlampir)

Selain dapat menyebar melalui jaringan, malware juga dapat menyebar melalui file attachment pada email maupun link ke situs-situs yang terinfeksi Malware. Semua pegawai diharap berhati-hati dan tidak membuka file-file attachment maupun situs dengan ekstensi mencurigakan karena saat ini belum ada solusi yang paling cepat dan jitu untuk mengembalikan file-file yang sudah terinfeksi WannaCry. Salah satu cara antisipasi adalah dengan memutus sambungan internet dari komputer yang terinfeksi akan menghentikan penyebaran WannaCry ke komputer lain yang rentan.

Laporan insiden dan konsultasi dapat menghubungi Bidang Informatika Dinas Komunikasi dan Informatika Klaten di 0272 321046 eks 253

Referensi :

1. https://www.kominfo.go.id/content/detail/9636/siaran-pers-no-55hmkominfo052017-tentang-himbauan-agar-segeramelakukan-tindakan-pencegahan-terhadap-ancaman-malware-khususnya-ransomware-jenis-wannacry/0/siaran_pers
2. https://kominfo.go.id/content/detail/9637/siaran-pers-no-56hmkominfo052017-tentang-antisipasi-terhadap-ancamanmalware-ransomware-jenis-wannacry/0/siaran_pers

Tutorial versi ISACA berisi :

1. Tutorial update patch MS17-010
2. Menutup port dengan firewall (untuk semua versi Windows),
3. Update Antivirus Windows Defender (win10),
4. disable SMBv1 (win10), dapat didownload di http://klatenkab.go.id/wp-content/uploads/2017/05/Tutorial-ISACA.pdf

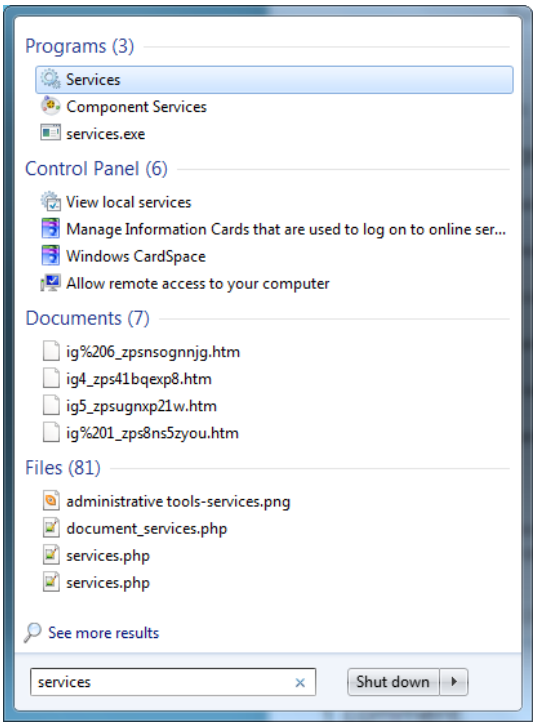
Tutorial yang ada pada dokumen ini :

1. Tutorial disable SMBv1 (windows 7, vista, xp)
2. Tutorial apabila terjadi kegagalan dalam install patch
3. Tutorial menonaktifan Fungsi Macros

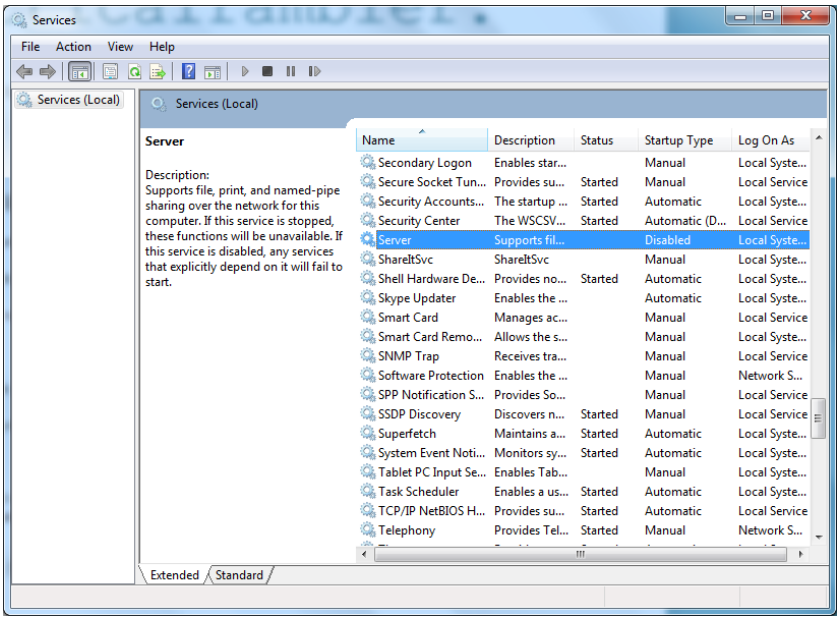
TUTORIAL MENONAKTIFKAN SMBv1 UNTUK WINDOWS7, vista, xp

Berikut adalah cara untuk menonaktifkan SMBv1:

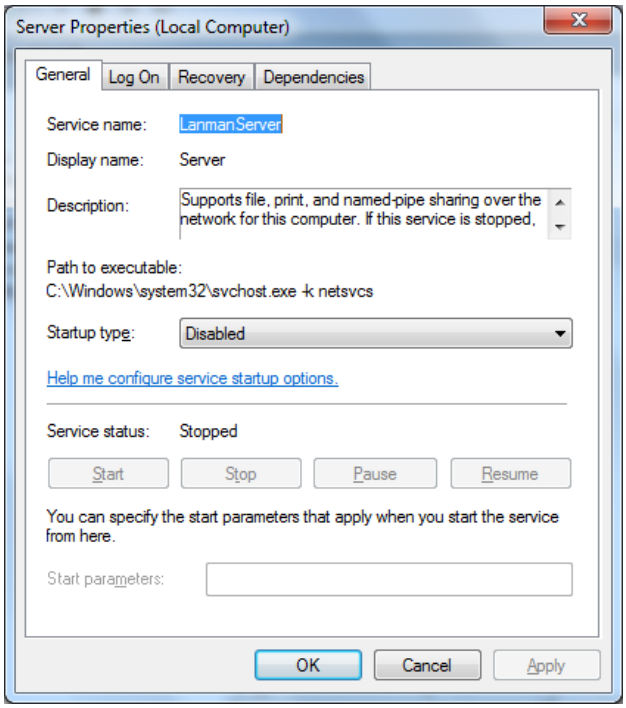
1. Ketik “services” lalu buka hasil teratas



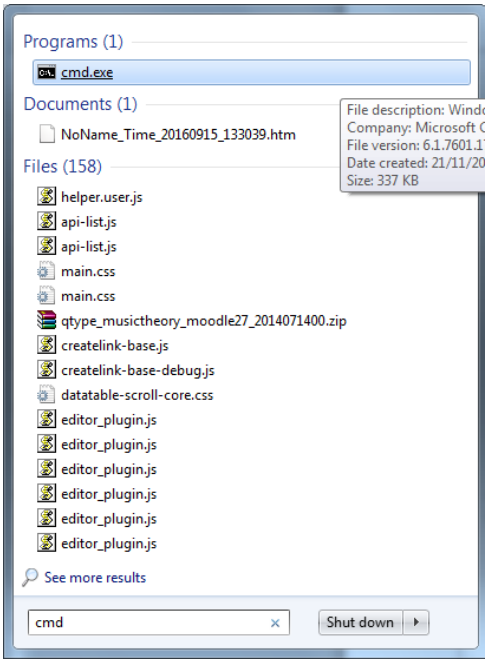
2. Cari “Server” kemudian klik kanan “Properties”



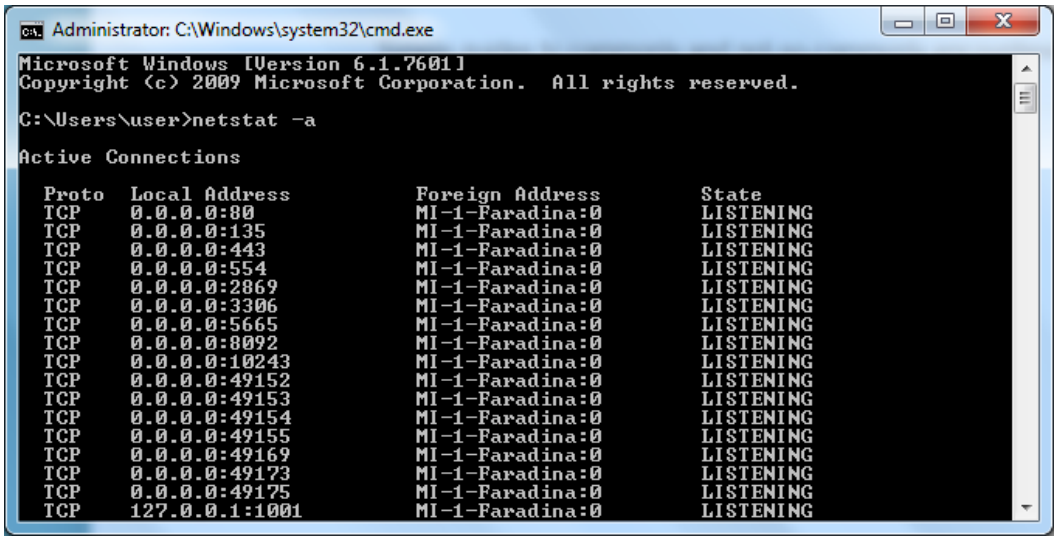
3. Klik “Stop” dan pada Startup type pilih “Disabled”



4. Restart PC
5. Ketikkan “cmd” pilih yang paling atas



6. Ketikkan “netstat –a” kemudian enter

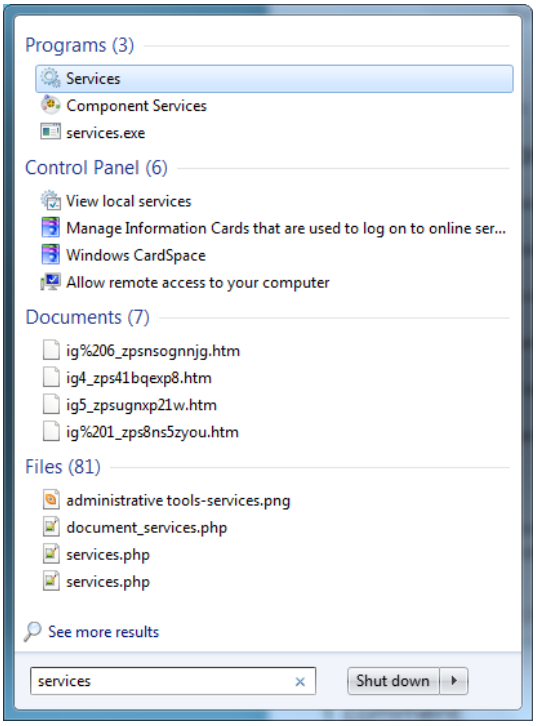


Bila dalam daftar tidak ada TCP 0.0.0.0:445, maka anda sudah berhasil menutup port SMBv1

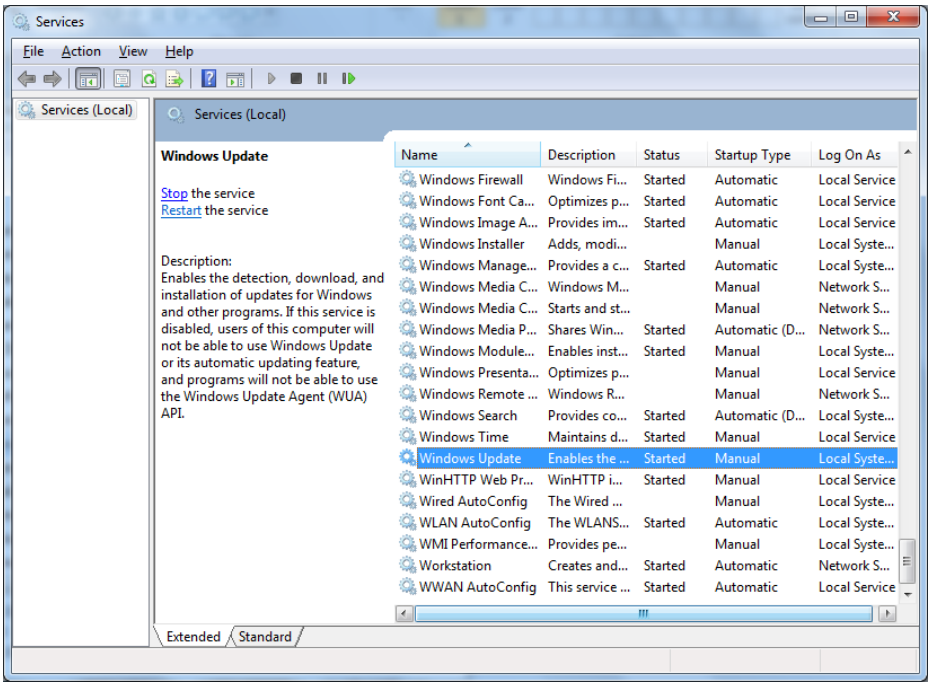
TUTORIAL BILA TERJADI GAGAL UPDATE PATCH

Bila terjadi gagal update patch, bisa mengikuti langkah2 berikut

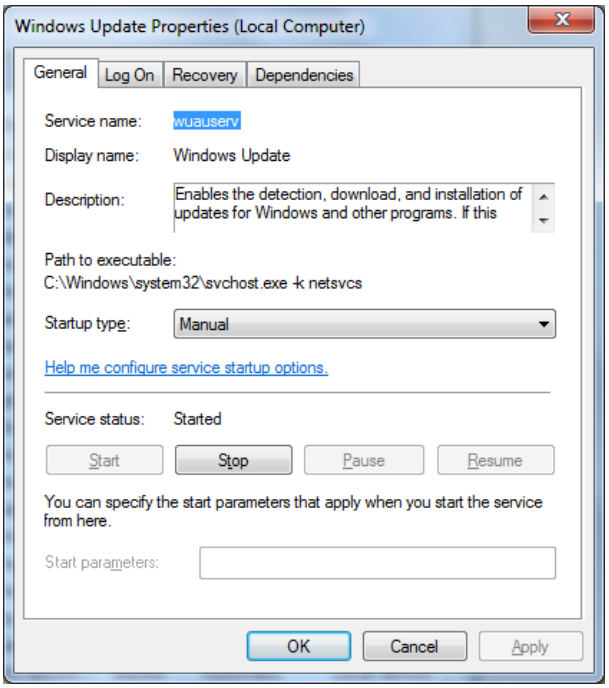
1. Ketik “services” lalu buka hasil teratas



2. Pada Windows Update klik kanan, pilih “Properties”



3. Pada startup type pilih “Manual” kemudian klik “Start”



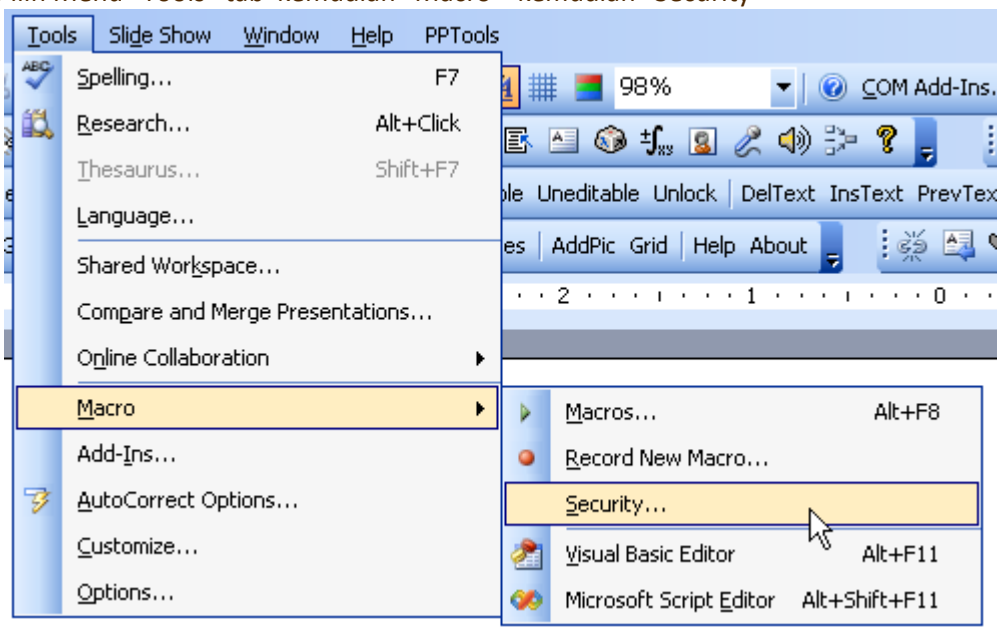
4. Restart komputer
5. Jalankan kembali patch nya.

Tutorial menonaktifkan Fungsi Macros

*lakukan hal ini untuk semua aplikasi Office (Word, Excel, PowerPoint, dll)

Untuk Mic. Office 2000 dan 2003

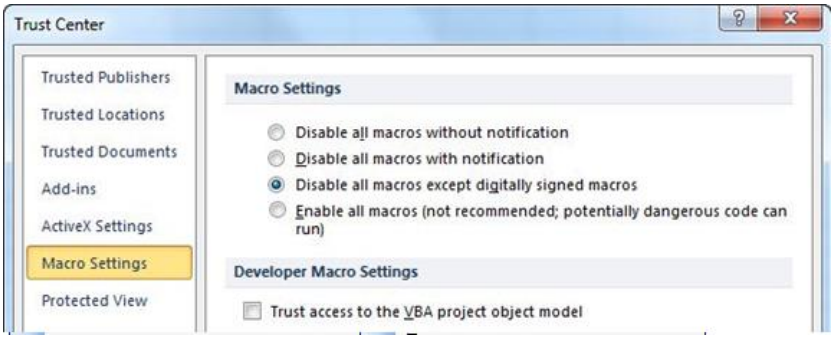
1. Pilih Menu “Tools” tab kemudian “Macro” kemudian “Security”



2. Pilih Security Level pada “Medium Security”,
   Maka setiap macro berjalan akan menanyakan Permission Setiap kali sebelum macro dijalan kan.

Untuk Mic. Office 2007

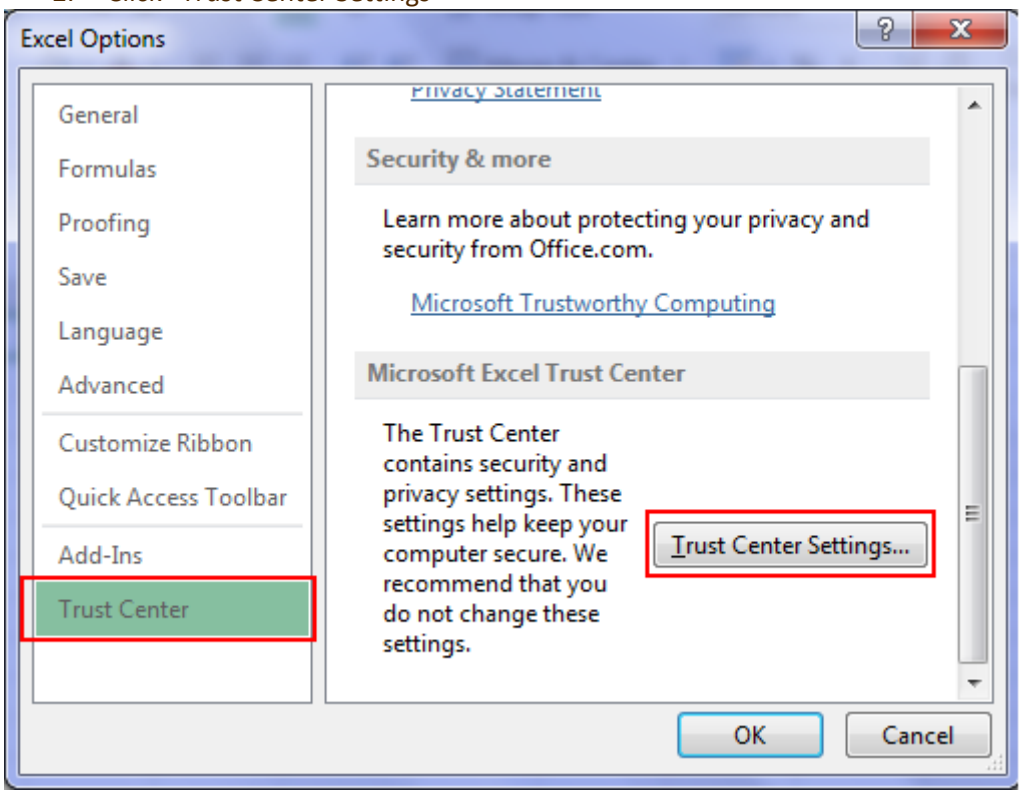
1. Click Tombol “Office”
2. Klik “Excel option” (Lokasi dibawah)
3. Pilih “Trust Center” > “Trust Center Setting”



4. Pilih macro Setting dan pilih “Disable all macros except digitally signed macros”

Untuk Mic. Office 2010

1. Pilih File => Options **=>** Trus Center
2. Click “Trust Center Settings”



3. Setelah itu pilih “Macro Setting” dan pilih Security Setting “Disable all macros except digitally signed macros”