إعداد/ السيد المعداوى

فيروس
W32.Mabezat.B

يفضل فحص الجهاز اكثر من مره وستلاحظ ان بعض الملفات تحذف والبقايا وهي الباك اب للفيروس ليعيد نفسه لايستطيع النوترن حذفه ويتعرف عليه باسم

W32.Mabezat.B

ولكنه موجود باسم اخر مخفي وهو مثلا

The worm may use other email attachment file names :including the following

s.rar****

office_crack.rar

serials.rar

passwords.rar

s_secrets.rar****

source.rar

imp_data.rar

documents_backup.rar

backup.rar

MyDocuments.rar

HpphmfUppmcbsOpujgjfs/fyf

GoogleToolbarNotifier.exe

PanasonicDVD_DigitalCam.exe

Antenna2Net.exe

RadioTV.exe

Microsoft MSN.exe

Sony Erikson DigitalCam.exe

IDE Conector P2P.exe

s Keys Secrets.exe****

FaxSend.exe

RecycleBinProtect.exe

Disk Defragmenter.exe

CD Burner.exe

ShowDesktop.exe

BrowseAllUsers.exe

Lock****sPartition.exe**

Win99compatibleXP.exe

MakeUrOwnFamilyTree.exe

sXp StartMenu Settings.exe****

Recycle Bin.exe

Adjust Time.exe

Microsoft ******s Network.exe

HP_LaserJetAllInOneConfig.exe

FloppyDiskPartion.exe

msjavx86.exe

AmericanOnLine.exe

Crack_GoogleEarthPro.exe

Lock Folder.exe

InstallMSN11En.exe

InstallMSN11Ar.exe

JetAudio dump.exe

KasperSky6.0 Key.doc.exe

Office2007 Serial.txt.exe

Office2007 CD-Key.doc.exe

Make ******s Original.exe

NokiaN73Tools.exe

WinrRarSerialInstall.exe

ولذلك قم بعمل سكان للجهاز واختر السكان العميق وهو FULL SCAN

وليس السكان السريع والوقت المستغرق حسب حجم الجهاز هارد ٢٥٠ جيجا ساتا SATA

اخذ تنظيفه ١٠ ساعات

وبعدها سيعطيك النوترن النتيجه بعدد الفيروسات

المحذوفه والغير محذوفه يتعرف عليها باسم وهي موجوده باسم اخر مخفي بصيغة RAR

الا انها ملفات دوس لزارعه الفايروس من جديد ولكنها نسخه خامله لاتنشط الا بفتحها ولو عن طريق الخطا

ابحث عن المسميات التاليه بجهازك من START

ومنها الى SEARCH

ومنها الى خيار البحث بالجهاز وابحث عن الملفات التاليه اواحذفها من الجهاز

s.rar****

office_crack.rar

serials.rar

passwords.rar

s_secrets.rar****

source.rar

imp_data.rar

documents_backup.rar

backup.rar

MyDocuments.rar

وقم بحذفها عن طريق CTRL+D

حددها ب CTRL+A

واحذفها عن طريق زر من الكي بورد CTRL+D

ومن ثم اختر اوكي ليتم نقلها الى سله المحذوفات

وستلاحظ جميع الملفات حجمها ٤٤ كيلو بايت وهي ملفات دوس وليس مضغوطه

والان ننتقل الى خطوة حذف الباتش من الجهاز الذي يعيده من الرجستري

قم بالبحث عن الملف بنفس الطريقه من START

ومنها الى SEARCH

وابحث عن هذا الملف بجهاز وتاكد اذا وجدته احذفه

FILE PATH

واليكم طريقه البحث والحذف بالصور

عند وجود الملفات احذفها ولااستطيع تصويرها لاني نظفت الجهاز ولكن ستلاحظ جميعها حجمها ٤٤K

إعداد/ السيد المعداوى