惡意家族Korgo , Pinfi 查詢結果

1. 來源: virustotal : 以這兩者作為keyword進行查詢 , 但未有結果 -> 沒有可查詢結果回傳 ### 因為未用全小寫search
2. 來源: google:
   1. (Pinfi) Symantic: 分類為Win32.Pinfi , 此外在其他各家防毒廠的分類 : **Also Known As:**

**Win32.Parite.a [KAV],**

**W32/Pate.a [McAfee],**

**Win32.Pinfi.A [CA],**

**PE\_PARITE.A [Trend],**

**W32/Parite-A [Sophos],**

**Win32/Parite.A [RAV]**

**所有別名可參考: http://www.threatexpert.com/threats/w32-pinfi.html**

主要特徵行為: W32.Pinfi is a memory-resident polymorphic virus that will infect the .EXE and .SCR files. This virus can also spread via mapped drives and network shares

(Korgo) Symantic: 分類為 Win32.Korgo ,此外子分類包含了下列數種

W32.Korgo.A: worm that attempts to exploit the Microsoft LSASS Windows vulnerability, also listens on TCP ports 113, 2041, and 3067

W32.Korgo.F

W32.Korgo.I

W32.Korgo.L

W32.Korgo.P

W32.Korgo.R

W32.Korgo.S (N的變種): worm attempts to propagate by exploiting the Microsoft Windows LSASS Buffer Overrun Vulnerability on TCP port 445 and 113 2000 and 8192

W32.Korgo.T

W32.Korgo.U

W32.Korgo.V

W32.Korgo.Z