Anti Anti-VMware

written by Mert SARICA | 18 July 2010

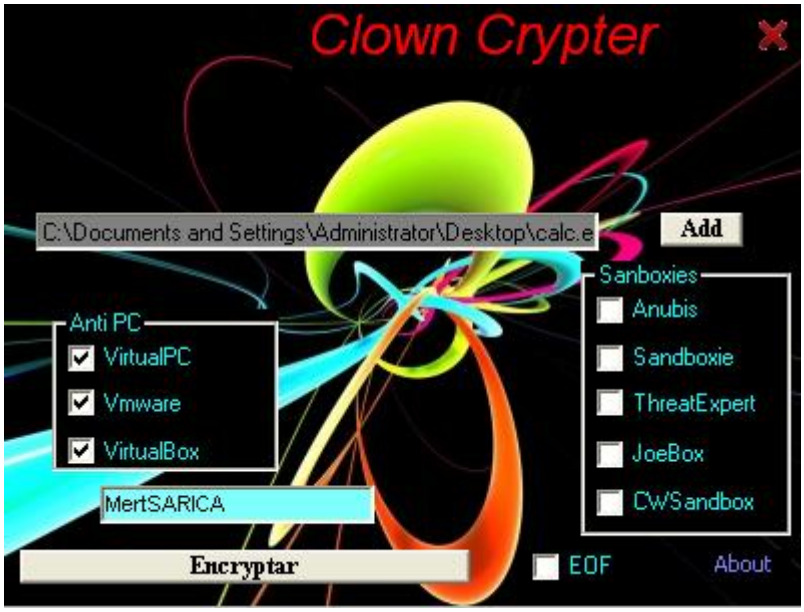
Zararlı yazılım analizi yapanlar için sanal makina yazılımları (vmware, virtualpc, virtualbox) en büyük nimettir. Hiç bir zaman işletim sistemi üzerinde çalıştırmayacağınız veya çalıştırma konusunda tereddüt ettiğiniz tehlikeli, zararlı veya şüpheli yazılımları hiç çekinmeden çalıştırarak işletim sistemi üzerinde neler olup bittiğini anlamanıza yardımcı olurlar.

Tabii bunu bilen art niyetli kişiler, işlerin bu kadar kolay olmasını hiç bir zaman istemezler bu nedenle zararlı yazılımlarının sanal makina içerisinde incelenmesini engellemek için zararlı kodlarına sanal makinayı tespit eden fonksiyonlar ekleyerek bu zararlı yazılımların işletim sistemi üzerinde çalışmasını engellerler. Tabii kod seviyesinde tersine mühendislik konusunda uzman bir analist bu engelleri kolaylıkla aşabileceği için eninde sonunda zararlı yazalımları analiz ederek mutlu sona ulaşabilecektir.

Peki ya kod seviyesinde tersine mühendislik konusunda uzman olmayan bir kişi böyle bir zararlı yazılım ile karşılaşınca ne yapabilir ? Tabiiki sistem seviyesinde tersine mühendisliğe başvurabilir.

Örnek olarak windows'un hesap makinasını internetten bulduğumuz ve sanal makina tespit etme özelliğine sahip olan herhangi bir şifreleme aracı (crypter) ile şifreleyip inceleyelim.

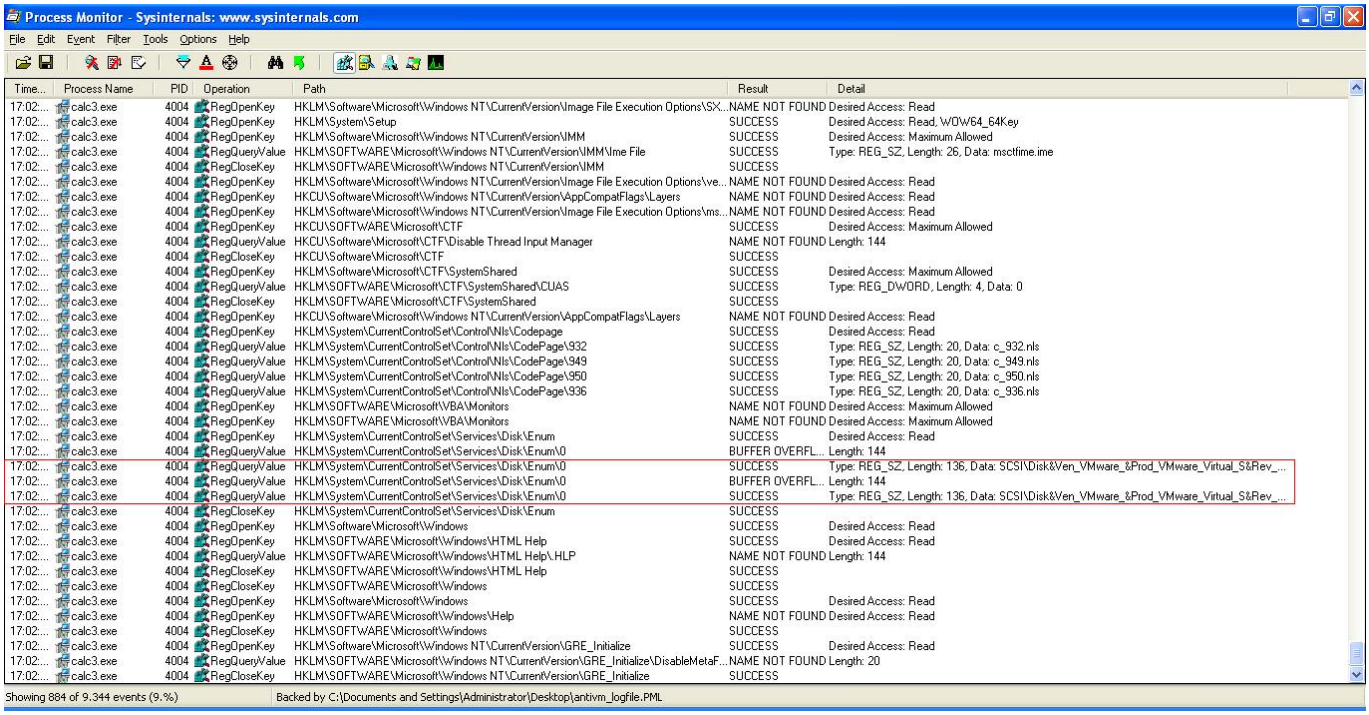
Clown Crypter adındaki şifreleme aracını indirdikten sonra çalıştırıp incelediğimizde hem sanal makina hem de sandbox tespit etme özelliklerine sahip olduğunu görebiliyoruz.



Calc.exe programını tüm sanal makina tespit etme seçeneklerini işaretleyerek şifreledikten sonra calc3.exe adı altında kayıt ederek VMWare içinde çalıştırdığımızda programın çalışmadığını görebiliyoruz. Peki teknik olarak bu tespit nasıl gerçekleştiriliyor ?

Çoğunlukla bu tür programlar arasında en çok kullanılan yöntemlerden biri kayıt defterindeki (registry) bazı değerleri kontrol etmek ve VMWare, Virtual veya VBOX anahtar kelimelerini aratmaktır. Bunu teyit etmek için Sysinternals'ın Process Monitor yazılımı ile calc3.exe programını hemen incelemeye başlayalım. Bilmeyenleriniz için kısa bir açıklama, Process Monitor yazılımı, incelenen programın dosya sistemi üzerinde gerçekleştirdiği işlemlerden, kayıt defterinde açtığı ve incelediği tüm anahtarları ve değerleri görebilmenizi sağlayan faydalı bir eserdir.

Calc3.exe programını Process Monitor ile incelediğimizde kayıt defterinde kontrol ettiği anahtar hemen dikkatimizi çekiyor.



İlgili anahtarda geçen VMWare ile Virtual anahtar kelimelerinin değiştirdiğimizde (VMWare -> MWare, Virtual -> irtual) ve programı çalıştırdığımızda programın başarıyla çalıştığını görebiliyoruz.

Yukarıdaki yöntemi kullanan örnek fonksiyon:

```
Public Function IsVirtualPCPresent() As Long
  Dim lhKey       As Long
  Dim sBuffer     As String
  Dim lLen        As Long

  If RegOpenKeyEx(&H80000002, "SYSTEM\ControlSet001\Services\Disk\Enum", _
     0, &H20019, lhKey) = 0 Then
      sBuffer = Space$(255): lLen = 255
      If RegQueryValueEx(lhKey, "0", 0, 1, ByVal sBuffer, lLen) = 0 Then
          sBuffer = UCase(Left$(sBuffer, lLen - 1))
          Select Case True
              Case sBuffer Like "*VIRTUAL*":   IsVirtualPCPresent = 1
              Case sBuffer Like "*VMWARE*":    IsVirtualPCPresent = 2
              Case sBuffer Like "*VBOX*":      IsVirtualPCPresent = 3
          End Select
      End If
      Call RegCloseKey(lhKey)
  End If
```

End Function

Art niyetli kişiler tarafından sanal makina tespiti için kullanılan diğer bir yöntem ise VMware Backdoor I/O Port. VMWare Backdoor ? Evet aynen öyle, VMWare, sanal makina ile port 0x5658 bağlantı noktasından haberleşmek için özel olarak tasarlanan bir arka kapı kullanmaktadır. Bu arka kapıda kullanılan bağlantı noktasının sahte olduğunu ayrıca belirtmek isterim.

Art niyetli kişiler tarafından kullanılan örnek fonksiyon:

```
bool IsInsideVMWare()
{
     bool rc = true;
     __try
    {
          __asm
    {
    push edx
    push ecx
    push ebx
    mov eax, 'VMXh'
    mov ebx, 0 // any value but not the MAGIC VALUE
    mov ecx, 10 // get VMWare version
    mov edx, 'VX' // port number
    in eax, dx // read port
    // on return EAX returns the VERSION
    cmp ebx, 'VMXh' // is it a reply from VMWare?
    setz [rc] // set return value
    pop ebx
    pop ecx
    pop edx
    }
}
__except(EXCEPTION_EXECUTE_HANDLER)
{
    rc = false;
}
   return rc;
}
```

Neyseki buna karşı VMWare üzerinde ufak bir konfigürasyon değişikliği yaparak VMWare'in tespit edilmesini önleyebilirsiniz. Bunun için yapmanız gereken sanal makinaya ait olan VMX dosyasına aşağıdaki parametreleri eklemek olacaktır.

- isolation.tools.getPtrLocation.disable = "TRUE"
- isolation.tools.setPtrLocation.disable = "TRUE"
- isolation.tools.setVersion.disable = "TRUE"
- isolation.tools.getVersion.disable = "TRUE"
- monitor_control.disable_directexec = "TRUE"
- monitor_control.disable_chksimd = "TRUE"
- monitor_control.disable_ntreloc = "TRUE"
- monitor_control.disable_selfmod = "TRUE"
- monitor_control.disable_reloc = "TRUE"
- monitor_control.disable_btinout = "TRUE"
- monitor_control.disable_btmemspace = "TRUE"
- monitor_control.disable_btpriv = "TRUE"
- monitor_control.disable_btseg = "TRUE"

VMWare üzerinde zararlı yazılım incelemek isteyenler için engel teşkil edebilecek bu iki yöntemi aşmanızı sağlayan bu yazı umarımki faydalı olmuştur. Sanal makina tespit töntemlerinin bu iki tanesi ile sınırlı kalmadığını hatırlatır, bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim…