

Anti Anti-VMware

written by Mert SARICA | 18 July 2010

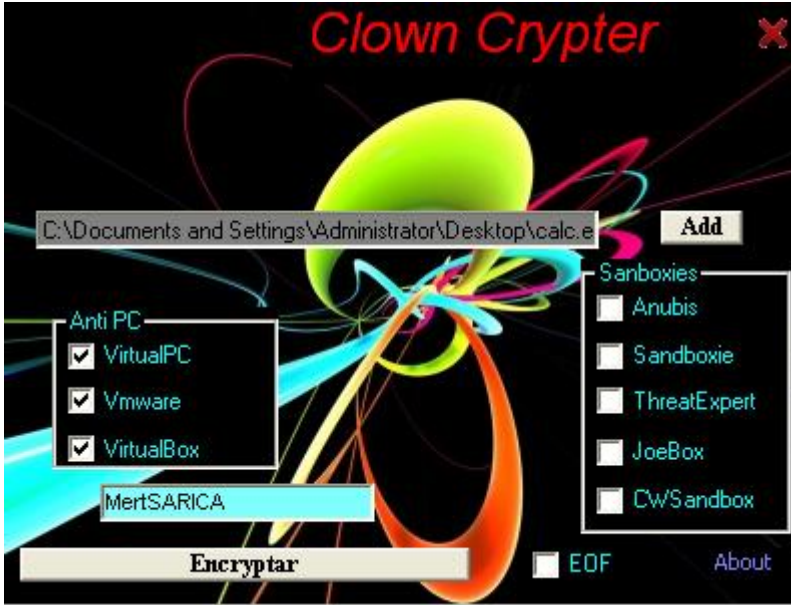
Zararlı yazılım analizi yapanlar için sanal makina yazılımları (vmware, virtualpc, virtualbox) en büyük nimettir. Hiç bir zaman işletim sistemi üzerinde çalıştırmayacağınız veya çalıştırma konusunda tereddüt ettiğiniz tehlikeli, zararlı veya şüpheli yazılımları hiç çekinmeden çalıştırarak işletim sistemi 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 yazılımları analiz ederek mutlu sona ulaşabilecektir.

Peki ya kod seviyesinde tersine mühendislik konusunda uzman olmayan bir kişi böyle bir zararlı yazılım ile karşılaşınca ne yapabilir ? Tabii ki 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.

Time...	Process Name	PID	Operation	Path	Result	Detail
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SV...	NAME NOT FOUND	Desired Access: Read
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\System\Setup	SUCCESS	Desired Access: Read, W/DW64_64Key
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\MM	SUCCESS	Desired Access: Maximum Allowed
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\MM\me File	SUCCESS	Type: REG_SZ, Length: 26, Data: mscftime.ime
17:02:...	calc3.exe	4004	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\MM	SUCCESS	
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ve...	NAME NOT FOUND	Desired Access: Read
17:02:...	calc3.exe	4004	RegOpenKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	NAME NOT FOUND	Desired Access: Read
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ms...	NAME NOT FOUND	Desired Access: Read
17:02:...	calc3.exe	4004	RegOpenKey	HKCU\SOFTWARE\Microsoft\CTF	SUCCESS	Desired Access: Maximum Allowed
17:02:...	calc3.exe	4004	RegQueryValue	HKCU\Software\Microsoft\CTF\Disable Thread Input Manager	NAME NOT FOUND	Length: 144
17:02:...	calc3.exe	4004	RegCloseKey	HKCU\Software\Microsoft\CTF	SUCCESS	
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\Software\Microsoft\CTF\SystemShared	SUCCESS	Desired Access: Maximum Allowed
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\SOFTWARE\Microsoft\CTF\SystemShared\CUAS	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
17:02:...	calc3.exe	4004	RegCloseKey	HKLM\SOFTWARE\Microsoft\CTF\SystemShared	SUCCESS	
17:02:...	calc3.exe	4004	RegOpenKey	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	NAME NOT FOUND	Desired Access: Read
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	Desired Access: Read
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\932	SUCCESS	Type: REG_SZ, Length: 20, Data: c_932.nls
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\949	SUCCESS	Type: REG_SZ, Length: 20, Data: c_949.nls
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\950	SUCCESS	Type: REG_SZ, Length: 20, Data: c_950.nls
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\936	SUCCESS	Type: REG_SZ, Length: 20, Data: c_936.nls
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\SOFTWARE\Microsoft\VBAs\Monitors	NAME NOT FOUND	Desired Access: Maximum Allowed
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\SOFTWARE\Microsoft\VBAs\Monitors	NAME NOT FOUND	Desired Access: Maximum Allowed
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\System\CurrentControlSet\Services\Disk\Enum	SUCCESS	Desired Access: Read
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\System\CurrentControlSet\Services\Disk\Enum\0	BUFFER OVERFL...	Length: 144
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\System\CurrentControlSet\Services\Disk\Enum\0	SUCCESS	Type: REG_SZ, Length: 136, Data: SCSI\Disk&Ven_VMware_&Prod_VMware_Virtual_S&Rev...
17:02:...	calc3.exe	4004	RegCloseKey	HKLM\System\CurrentControlSet\Services\Disk\Enum	SUCCESS	
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\Software\Microsoft\Windows	SUCCESS	Desired Access: Read
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\HTML Help	SUCCESS	Desired Access: Read
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows\HTML Help\HLP	NAME NOT FOUND	Length: 144
17:02:...	calc3.exe	4004	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\HTML Help	SUCCESS	
17:02:...	calc3.exe	4004	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows	SUCCESS	
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\Software\Microsoft\Windows	SUCCESS	Desired Access: Read
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\Help	NAME NOT FOUND	Desired Access: Read
17:02:...	calc3.exe	4004	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows	SUCCESS	
17:02:...	calc3.exe	4004	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: Read
17:02:...	calc3.exe	4004	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaF...	NAME NOT FOUND	Length: 20
17:02:...	calc3.exe	4004	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	

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 "*VB0X*": 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.getVersion.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 yöntemlerinin bu iki tanesi ile sınırlı kalmadığını hatırlatır, bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim...