Sandbox Detection

written by Mert SARICA | 2 December 2019 In my blog posts that I wrote 8-9 years ago (Anti Analiz, Anti Anti-VMWare), I mentioned that malicious individuals who develop malware use various methods to make it difficult for security researchers or systems to analyze their malware on virtual systems.

Nowadays, with the widespread use of Virtual Desktop Infrastructure (VDI) technologies in corporate environments, virtual systems are no longer primarily used by servers or malware analysts, security researchers. As a result, malware developers, and also red team members who perform ethical hacking, aim to design and develop tools that can operate on virtual systems but are not detectable by virtual analysis systems. Knowing that it is impossible to develop a tool that does not work on virtual analysis systems with a realistic approach, malware developers are searching for their malware's hash values on VirusTotal at certain intervals to understand if they have been detected and to stop their operations. Similarly, red team members who do not want to be caught, use projects like RedELK to ensure the sustainability of their operations.

I have decided to research and share with you how easy or difficult it is to detect these trusted sandbox systems, such as VirusTotal, Any.Run, Hybrid Analysis, Lastline Analyst, VMRay Analyzer, etc. which are commonly used by end-users and security experts to upload files suspected of being malicious.

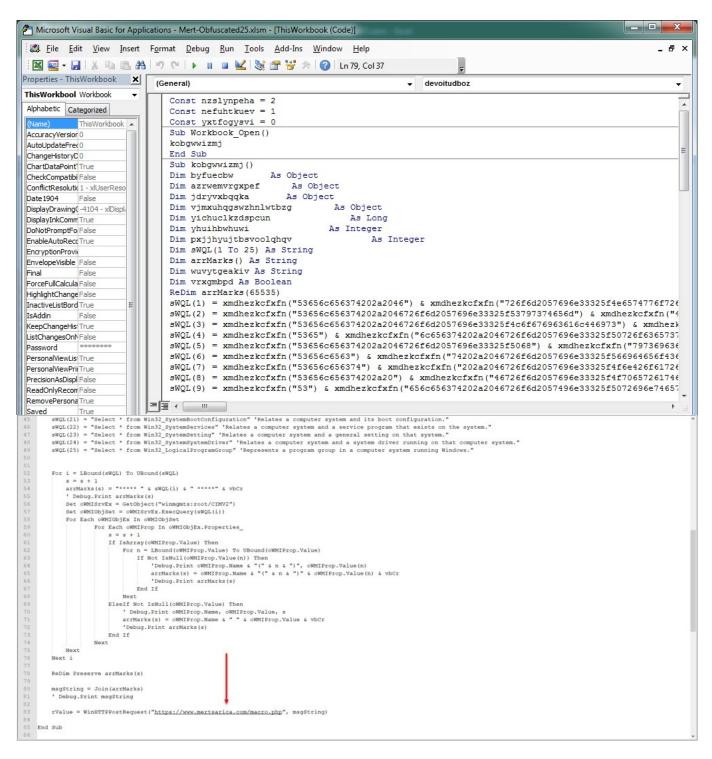
To do this, I first needed to gather information (reconnaissance) about the sandbox systems. When a software is uploaded to a sandbox system, it is monitored and recorded by the system when it communicates with a target system (C&C) during dynamic analysis. In short, these systems are allowed to have internet connections on them. So, I decided to prepare a Microsoft Office macro that collects information about the target operating system. The easiest way to do this with the macro is to take advantage of the Windows Management Instrumentation (WMI) which is commonly used for lateral movement in targeted attacks (APT). If you do a small research on Microsoft's website about WMI, you can see that you can collect a lot of information about the target operating system using the Win32 Provider.

To avoid reinventing the wheel, I did a quick search on Google and came across a simple script that collects information via WMI using VBA. After

adding 25 classes that are specific to the operating system on Microsoft's page to this script file, I made it send the information to https://www.mertsarica.com/macro.php. To make sure it cannot be easily detected by antivirus software, I also used the macro_pack tool to hide the macro (obfuscation).

📝 C:\U	sers\Mert\Desktop\Mert-Obfusca	ated25.txt - Notepad	++							
File E	dit Search View Encoding	Language Setting	s Tools Macro Run Plugins Window ?							
6		() 2 c # ¹	* < < I II							
🔚 Mert-	-Obfuscated25.txt 🔀	<pre>by the force of the set of t</pre>								
1	' Author: Mert SARICA	- https://www	w.mertsarica.com - mert.sarica[@]gmail.com							
2	' For Security Research Purposes Only									
3	' Credit: https://sit	es.google.com/	/site/beyondexcel/project-updates/exposingsystemsecretswithvbaandwmiapi							
4										
5		Open()								
6	WMI End Sub		i i i i i i i i i i i i i i i i i i i							
8	End Sub									
9	Sub WMI()									
10	Sub WHI()									
11	Dim oWMISrvEx	As Object	SWbemServicesEx							
12	Dim oWMIObjSet									
13	Dim oWMIObjEx									
14	Dim oWMIProp	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		-								
21	Dim rValue As Boo	lean								
22										
23	ReDim arrMarks(65	535)								
24										
25		-								
26	~									
27 28	~ ` '									
29	~	_								
30										
31										
32										
33										
34	~									
35										
36										
37										
00	-		Commissed (Dervessents - services on - services suster winning Windows II							
Normal	text file	length :	6.277 lines : 128 Ln : 13 Col : 51 Sel : 0 0 Windows (CR LF) UTF-8 INS							

_ 🗆 🗙 C:\Windows\system32\cmd.exe . E Malicious Office, UBS, and other retro formats for pentests and redteam - Ver ion:1.6 Release:Community le 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... VBA names obfuscation ... -] Repame functions [+1]h(Γ. Rename functions... Rename variables... Rename numeric constants... Rename API imports... OK! at VBA strings obfuscation ...] Split strings... Encode strings... OK! T+ VBA 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 VBA... 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!



After uploading the Mert-Obfuscated25.xlsm file to Any.Run and VirusTotal, I saw requests coming to https://www.mertsarica.com/macro.php after a short time. When I looked at the incoming requests, I saw that there was quite a bit of information for me to analyze regarding the systems that perform sandbox analysis. :)

While looking at this information, my attention was first caught by the LastBootUpTime value that appeared in the output of the Select * From Win32_OperatingSystem WMI request. This value indicates the date and time when the operating system was last started. Sandbox systems restart the

operating system from scratch, in its clean state, before analyzing the malware, so there is a maximum time difference of 30 minutes between the date and time of the operating system's reboot (LastBootUpTime) and the date and time of the analysis (LocalDateTime). Based on this information, it is possible to assume that the software was analyzed in the sandbox.



As I continued to look at the information I had collected, I came across an output where I noticed a difference of 4 months between LastBootUpTime and LocalDateTime. This raised suspicion since a user system (Windows 7) that hasn't been restarted for 4 months is quite unusual, so I began to investigate this information more closely. As it is known, most security researchers, malware analysts have an isolated, virtual analysis system. To save time, this analysis system is not restarted each time, but instead, is returned from an instant image (snapshot). An operating system returned from an instant image, LastBootUpTime gradually becomes older, and the time difference between LocalDateTime and it can sometimes be months when a malware is being analyzed. In light of this information, I also checked the WMI section where I suspected that this output had collected information on program groups in the Windows operating system, Win32_LogicalProgramGroup, and this time I saw that the system had tools such as Immunity Debugger, Process Hacker, which are frequently used by security researchers, malware analysts. This gave me the information that my Office file was analyzed by a threat hunter. :)

217.86.43	7.86.42.248.brt 🖾	
		^
	, , ,	
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	
	FreeSpaceInPagingFiles 1791456	
	DE Cullians Hen	> [Management.ManagementDateTimeConverter]::ToDateTime("20190329103419.697000+060") #LocalDateTime
	TrotallDate 20160410151054 0000004120	
310	Zy Mart 7819 Cur	a 12:34:19
		> [Management.ManagementDateTimeConverter]::ToDateTime("201811113103206.500000+060") #LastBootUpTime
	1 3 c l Josef 3 free	/ Instruction and a second se Second second sec
		11 12:32:06
		ition?
318		
15750	16.42.245 M CI	
15751		c- cstart Menu\\Programs\\Games*
15753	Setting \\MARYHILL-PC\root\cinv2:Win32_LogicalProgramGroup.Name="Public	c:Start Menu\\Programs\\HxD Hex Editor*
15753 15754	Setting \\MARYHILL-DC\root\cimv2:Win32_LogicalProgramGroup.Name="Public Element \\MARYHILL-DC\root\cimv2:Win32_ComputerSystem.Name="MARYHILL-FC	csStart Nenu\\Programs\\HxD Hex Editor" c=
15753 15754 15755 15756	Setting \\MARYHIL-PC\root\cinv2:Nin32_LogicalProgramGroup.Name=*Publi Element \\MARYHIL-PC\root\cinv2:Nin32_Computer3ystem.Name=*Publi Setting \\MARYHIL-PC\root\cinv2:Nin32_Computer3ystem.Name=*Publi Element \\MARYHIL-PC\root\cinv2:Nin32_Computer3ystem.Name=*Publi	c:Start Menu\\Programs\\HmD Hex Editor" C" C:Start Menu\\Programs\\Immunity Inc" C"
15753 15754 15755 15756 15757	Setting \UMARYHIL-EC\root\cimy2Hin32_LogicalFogramicroup.Names*tubil Element \UMARYHIL-EC\root\cimy2Hin32_LogicalFogramicroup.Names*Tubil Satting \UMARYHIL-EC\root\cimy2Hin32_ComputerBystem.Names*Tubil Bienent \UMARYHIL-EC\root\cimy2Hin32_ComputerBystem.Names*Tubil Satting \UMARYHIL-EC\root\cimy2Hin32_ComputerBystem.Names*Tubil Satting \UMARYHIL-EC\root\cimy2Hin32_ComputerBystem.Names*Tubil Satting \UMARYHIL-EC\root\cimy2Hin32_ComputerBystem.Names*Tubil Satting \UMARYHIL-EC\root\cimy2Hin32_ComputerBystem.Names*Tubil	c:Bfart Nenu\\Programs\\HKD Hex Editor" :Sfart Menu\\Programs\\Immunity Inc" :Sfart Menu\\Programs\\Immunity Inc\\Immunity Debugger"
15753 15754 15755 15756 15757 15758	Setting \\MARYHILL-PC\root\cimv2:Win32_LogicalProgramGroup.Hame="Publi Blement \\MARYHIL-PC\root\cimv2:Win32_ComputerSystem.Hame="Publi Sating \\MARYHIL-PC\root\cimv2:Win32_ComputerSystem.Hame="Publi Blement \\MARYHIL-PC\root\cimv2:Win32_ComputerSystem.Hame="Publi Blement \\MARYHIL-PC\root\cimv2:Win32_ComputerSystem.Hame="Publi Blement \\MARYHIL-PC\root\cimv2:Win32_ComputerSystem.Name="Publi Blement \\MARYHIL-PC\root\cimv2:Win32_ComputerSystem.Name="Publi Blement \\MARYHIL-PC\root\cimv2:Win32_ComputerSystem.Name="Publi Blement \\MARYHIL-PC\root\cimv2:Win32_ComputerSystem.Name="Publi	c:Start Menu\\Programs\\HmD Hex Editor" c" c:Start Menu\\Programs\\Immunity Inc" c:Start Menu\\Programs\\Immunity Inc\\Immunity Debugger" c"
15753 15754 15755 15756 15757 15758 15759 15760	38 Betting \UMARYHIL-PC\root\cimy2:Win32_LogicalFyogramCroup.Namas*full 8 Riement \UMARYHIL-PC\root\cimy2:Win32_LogicalFyogramCroup.Namas*full 5 Steing \UMARYHIL-PC\root\cimy2:Win32_LogicalFyogramCroup.Namas*full 6 Riement \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full 7 Betting \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full 8 Riement \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full 8 Betting \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full 58 Biting \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full 58 Betting \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full 58 Biting \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full 59 Betting \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full 50 Riement \UMARYHIL-PC\root\cimy2:Win32_ComputerSystem.Namas*full	c:Bfart Menu\\Programs\\HxD Hex Editor" c:sfart Menu\\Programs\\Immunity Inc" c:sfart Menu\\Programs\\Immunity Inc\\Immunity Debugger" c: c:sfart Menu\\Programs\\Java"
15753 15754 15755 15756 15757 15758 15759 15760 15761	Betting \UMANYHIL-PC\root\cim2:Hin32_LogicalFrogramCroup.Hames*tubil Slement \UMANYHIL-PC\root\cim2:Hin32_ComputerSystem.Hames*MaNYHIL- Setting \UMANYHIL-PC\root\cim2:Hin32_ComputerSystem.Hames*MaNYHIL- Setting \UMANYHIL-PC\root\cim2:Hin32_ComputerSystem.Hames*AdvintLe- Blament \UMANYHIL-PC\root\cim2:Hin32_ComputerSystem.Hames*Fubil Batting \UMANYHIL-PC\root\cim2:Hin32_ComputerSystem.Hames*Fubil Batting \UMANYHIL-PC\root\cim2:Hin32_ComputerSystem.Hames*Fubil Blament \UMANYHIL-PC\root\cim2:Hin32_ComputerSystem.Hames*Fubil Batting \UMANYHIL-PC\root\cim2:Hin32_ComputerSystem.Hames*Fubil	c:Start Menu\\Programs\\HmD Hex Editor" c" c:Start Menu\\Programs\\Immunity Inc" c:Start Menu\\Programs\\Immunity Inc\\Immunity Debugger" c"
15753 15754 15755 15756 15757 15758 15759 15760 15761 15762	Setting \UMAYHIL-PC\root\cim22Hin32_LogicalFpogramCroup.Names*bull Betenent \UMAYHIL-PC\root\cim22Hin32_LogicalFpogramCroup.Names*Publi Satting \UMAYHIL-PC\root\cim22Hin32_ComputerSystem.Names*PAUHI Betenent \UMAYHIL-PC\root\cim22Hin32_ComputerSystem.Names*Publi Betenent \UMAYHIL-PC\root\cim22Hin32_ComputerSystem.Names*Publi Betenent \UMAYHIL-PC\root\cim22Hin32_ComputerSystem.Names*Publi Betenent \UMAYHIL-PC\root\cim22Hin32_ComputerSystem.Names*Publi Betenent \UMAYHIL-PC\root\cim22Hin32_ComputerSystem.Names*Publi Betenent \UMAYHIL-PC\root\cim22Hin32_ComputerSystem.Names*Publi Betenent \UMAYHIL-PC\root\cim22Hin32_LogicalFrogramCroup.Names*Publi Betenent \UMAYHIL-PC\root\cim2	C:Start Nenu\\Programs\\Immunity Inc" C:Start Menu\\Programs\\Immunity Inc" C:Start Menu\\Programs\\Immunity Inc\\Immunity Debugger" C:Start Menu\\Programs\\Java" C:Start Menu\\Programs\\Java"
15753 15754 15755 15755 15756 15759 15760 15761 15762 15763 15764	31 Betting \UMARYHIL-PC\root\cimy2:Hin32_LogicalFrogramCroup.Names*Publi 21 Betting \UMARYHIL-PC\root\cimy2:Hin32_LogicalFrogramCroup.Names*Publi 25 Betting \UMARYHIL-PC\root\cimy2:Hin32_ComputerSystem.Names*Publi 26 Blament \UMARYHIL-PC\root\cimy2:Hin32_ComputerSystem.Names*Publi 27 Betting \UMARYHIL-PC\root\cimy2:Hin32_ComputerSystem.Names*Publi 28 Betting \UMARYHIL-PC\root\cimy2:Hin32_ComputerSystem.Names*Publi 38 Hin3 Betting \UMARYHIL-PC\root\cimy2:Hin32_ComputerSystem.Names*Publi 38 Betting \UMARYHIL-PC\root\cimy2:Hin32_ComputerSystem.Names*Publi Betting \UMARYHIL-PC\root\cimy2:Hin32_Compical*FogramCroup.Names*	c:Start Nenu\\Programs\\Hmunity Inc" CSStart Menu\\Programs\\Immunity Inc" CSStart Menu\\Programs\\Immunity Inc\\Immunity Debugger" CSStart Menu\\Programs\\Java" SSStart Menu\\Programs\\Haintenance" SSStart Menu\\Programs\\Haintenance" CSStart Menu\\Programs\\Hidrosoft Office 2016 %ools" C*
15753 15754 15755 15756 15757 15750 15760 15761 15762 15763 15764 15765	33 Betting \UMARYHIL-PC\root\cim2?Hin32_LogicalProgramCroup.Name="Hub11 44 Element \UMARYHIL-PC\root\cim2?Hin32_LogicalProgramCroup.Name="Publ13 55 Satting \UMARYHIL-PC\root\cim2?Hin32_ComputerBytem.Name="Publ13 56 Element \UMARYHIL-PC\root\cim2?Hin32_ComputerBytem.Name="Publ13 57 Batting \UMARYHIL-PC\root\cim2?Hin32_ComputerBytem.Name="Publ13 58 Batting \UMARYHIL-PC\root\cim2?Hin32_ComputerBytem.Name="Publ14 58 Batting \UMARYHIL-PC\root\cim2?Hin32_ComputerBytem.Name="Publ14 58 Batting \UMARYHIL-PC\root\cim2?Hin32_LogicalProgramCroup.Name="Fubl14 58 Batting \UMARYHIL-PC\root\cim2?Hin32_LogicalProgramCroup.Name="Fubl14	c:Btart Menu\\Programs\\Had Hex Editor" CStart Menu\\Programs\\Immunity Inc* CStart Menu\\Programs\\Immunity Inc\\Immunity Debugger" CStart Menu\\Programs\\Java" Fort Menu\\Programs\\Maintenance" SStart Menu\\Programs\\Maintenance" SStart Menu\\Programs\\Midrowoft Office 2016 Tools" CStart Menu\\Programs\\Programs\\Midrowoft Office 2016 Tools" SStart Menu\\Programs\Programs\\Programs\\Programs\Programs\Programs\Programs\\Programs\Progr
15753 15754 15755 15755 15756 15759 15760 15761 15762 15763 15764	Setting \UMAYHILL-PC\root\cim2:Hin32_LogicalFrogramCroup.Names*tubli Blemant \UMAYHILL-PC\root\cim2:Hin32_LogicalFrogramCroup.Names*tubli Blemant \UMAYHILL-PC\root\cim2:Hin32_ComputerBystem.Name*Tubli Blemant \UMAYHILL-PC\root\cim2:Hin32_ComputerBystem.Name* Blemant \UMAYHILL-PC\root\cim2:Hin32_ComputerBystem.Name* Blemant \UMAYHILL-PC\root\cim2:Hin32_ComputerBystem.Name* Blemant \UMAYHILL-PC\root\cim2:Hin32_ComputerBystem.Name* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomp.Hame* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomp.Hame* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomp.Hame* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomp.Hame* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomp.Hame* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomp.Hame* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomp.Hame* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomp.Hame* Blemant \UMAYHILL-PC\root\cim2:Hin32_DogicalProgramScomPC Blemant \UMAYHILHANTANTANTANTANTANTANTANTANTANTANTANTANTA	c:Start Nenu\\Programs\\HxD Hex Editor" CStart Nenu\\Programs\\Immunity Inc" CStart Nenu\\Programs\\Immunity Inc\\Immunity Debugger" CStart Nenu\\Programs\\Java" CStart Nenu\\Programs\\Maintenance" CStart Nenu\\Programs\\Hidrowoft Office 2016 Tools" CStart Nenu\\Programs\Programs\
15753 15754 15755 15756 15759 15760 15761 15762 15763 15764 15765 15765 15766 15767	31 Betting \\UARYHILL-DC\root\cim2:Hin32_LogicalProgramicroup.Name="bublic 51 Betting \\UARYHILL-DC\root\cim2:Hin32_LogicalProgramicroup.Name="bublic 55 Betting \\UARYHILL-DC\root\cim2:Hin32_LogicalProgramicroup.Name="bublic 56 Riament \UARYHILL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 57 Betting \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 58 Biament \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 58 Betting \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 52 Biament \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 53 Betting \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 54 Betting \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 55 Betting \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 56 Betting \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 56 Betting \UMARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="bublic 56 <th>C:Btart Nenu\\Programs\\HmuD Hex Editor" C:Start Menu\\Programs\\Immunity Inc" C:Start Menu\\Programs\\Immunity Inc\\Immunity Debugger" C:Start Menu\\Programs\\Java" C:Start Menu\\Programs\\Midromoft Office 2016 Tools" C:Start Menu\\Programs\\Process Hacker 2" C:Start Menu\\Programs\\Process Hacker 2\\Help and Bupport" C:Start Menu\\Programs\\Process Hacker 2\\Help Acker 2\\Help Acker 2\\Fello Acker 2\\</th>	C:Btart Nenu\\Programs\\HmuD Hex Editor" C:Start Menu\\Programs\\Immunity Inc" C:Start Menu\\Programs\\Immunity Inc\\Immunity Debugger" C:Start Menu\\Programs\\Java" C:Start Menu\\Programs\\Midromoft Office 2016 Tools" C:Start Menu\\Programs\\Process Hacker 2" C:Start Menu\\Programs\\Process Hacker 2\\Help and Bupport" C:Start Menu\\Programs\\Process Hacker 2\\Help Acker 2\\Help Acker 2\\Fello Acker 2\\
15753 15754 15755 15756 15759 15760 15761 15762 15765 15765 15765 15766 15766 15768 15769	33 Betting \UMARYHIL-PC\root\cim22Hin32_LogicalFogramCroup.Names*Publi 21 Betting \UMARYHIL-PC\root\cim22Hin32_ComputerSystem.Name*PARYHIL- 25 Betting \UMARYHIL-PC\root\cim22Hin32_ComputerSystem.Name*PARYHIL- 26 Blement \UMARYHIL-PC\root\cim22Hin32_ComputerSystem.Name*PARYHIL- 27 Betting \UMARYHIL-PC\root\cim22Hin32_ComputerSystem.Name*PARYHIL- 28 Betting \UMARYHIL-PC\root\cim22Hin32_LogicalForgramCroup.Name*PARYHIL- 28 Blement \UMARYHIL-PC\root\cim22Hin32_LogicalForgramCroup.Name*PARYHIL- 28 Blement \UMARYHIL-PC\root\cim22Hin32_LogicalForgramCroup.Name*PARYHIL- 28 Blement \UMARYHIL-PC\root\cim24Hin32_LogicalForgramCroup.Name*PARYHIL- 29 Batting \UMARYHIL-PC\root\cim24Hin32_LogicalForgramCroup.Name*PARYHIL- 20 Satting \UMARYHIL-PC\root\cim24Hin32_LogicalForgramCroup.Name*PARYHIL- 20 Satting \UMARYHIL-PC\root\cim24Hin32_LogicalForgramAry <tr< th=""><th>C:Start Menu\\Programs\\HmuD Hex Editor" CStart Menu\\Programs\\Immunity Inc" CStart Menu\\Programs\\Immunity Inc\\Immunity Debugger" CStart Menu\\Programs\\Java" CStart Menu\\Programs\\Hdiresoft Office 2016 Tools" CS CStart Menu\\Programs\\Hidrosoft Office 2016 Tools" CS CStart Menu\\Programs\\Process Hacker 2" CS CStart Menu\\Programs\\Process Hacker 2" CS CSTart Menu\\Programs\\Process Hacker 2\\Help and Support" CSTART Menu\\Programs\\Process Macker 2\\Help and Support" CSTART Menu\\Programs\\Process Macker 2\\Help Acker 2\\He</th></tr<>	C:Start Menu\\Programs\\HmuD Hex Editor" CStart Menu\\Programs\\Immunity Inc" CStart Menu\\Programs\\Immunity Inc\\Immunity Debugger" CStart Menu\\Programs\\Java" CStart Menu\\Programs\\Hdiresoft Office 2016 Tools" CS CStart Menu\\Programs\\Hidrosoft Office 2016 Tools" CS CStart Menu\\Programs\\Process Hacker 2" CS CStart Menu\\Programs\\Process Hacker 2" CS CSTart Menu\\Programs\\Process Hacker 2\\Help and Support" CSTART Menu\\Programs\\Process Macker 2\\Help and Support" CSTART Menu\\Programs\\Process Macker 2\\Help Acker 2\\He
15753 15754 15755 15756 15759 15760 15761 15762 15763 15764 15765 15765 15766 15767	33 Betting \UMAYHILL-PC\root\cim22Hin32_LogicalProgramCroup.Hams=*Ruh11 51 Betting \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*MaYHILL- 55 Setting \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*MaYHIL- 56 Betting \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*MaYHIL- 57 Betting \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*MaYHIL- 58 Betting \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*AuXHILL- 58 Bissing \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*AuXHILL- 56 Bissing \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*AuXHILL- 56 Bissing \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*Bissing AuXHILL- 56 Bissing \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*Bissing AuXHILL- 56 Bissing \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*Bissing AuXHILL- 56 Bissing \UMAYHILL-PC\root\cim22Hin32_ComputerSystem.Hams=*Bissing AuXH	C:BEart Menul\Programs\\HmuD Hex Editor" C:Start Menul\Programs\\Immunity Inc" C:Start Menul\Programs\\Immunity Inc\\Immunity Debugger" C:Start Menul\Programs\\Maintenance" C:Start Menul\Programs\\Hicrosoft Office 2016 Tools" C:Start Menul\Programs\\Process Hacker 2" C:Start Menul\Programs\Process Hacker 2\Help and Support" C:Start Menul\Programs\Process Hacker 2.\Help Acker 2.\
15753 15754 15755 15755 15759 15760 15761 15762 15764 15765 15766 15766 15769 15770 15770	Betting \UMANYHIL-PC\root\cim2:Hin32_LogicalProgramCroup.Hames="Rubil Blement \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Betting \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Blement \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Betting \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Betting \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Betting \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Batting \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Batting \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Batting \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames="Rubil Batting \UMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Hames Batting	C:Btart Menu\\Programs\\HmuD Hex Editor" C* C:Etart Menu\\Programs\\Immunity Inc* C* C:Etart Menu\\Programs\\Java* C* C:Etart Menu\\Programs\\Maintemance* C* C:Etart Menu\\Programs\\Microsoft Office 2016 Tools* C* C:Etart Menu\\Programs\\Process Hacker 2* C* C:Etart Menu\\Programs\\Process Hacker 2\\Help and Support* C* C* C* C* C* C* C* C* C* C
15753 15754 15755 15755 15759 15761 15762 15763 15764 15765 15766 15766 15765 15766 15767 15770 15771 15772 15773	38 Betting \\UARYHILL-BC\root\cim2:Hin32_LogicalFogramCroup.Name="hulli 58 Betting \\UARYHILL-BC\root\cim2:Hin32_ComputerBystem.Name="hulli 58 Biting \\UARYHILL-PC\root\cim2:Hin32_ComputerBystem.Name="hulli 58 Biting \\UARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="hulli 52 Element \\UARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="hulli 52 Element \\UARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="hulli 54 Satting \UARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="hulli 55 Biting \UARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="hulli 56 Batting \UARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="hulli 57 Batting \UARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="hulli 56 Batting \UARYHIL-PC\root\cim2:Hi	Cliftart Menul\Programs\\HmuD Hex Editor" Cliftart Menul\Programs\\Immunity Inc" Cliftart Menul\Programs\\Java" Cliftart Menul\Programs\\Haintenance" Cliftart Menul\Programs\\Haintenance" Cliftart Menul\Programs\\Hidrosoft Office 2016 Tools" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2.\Help and Support" Cliftart Menul\Programs\\Hidrosoft Office 2.7" Cliftart Menul\Programs\\Bittartup" Cliftart Menul\Programs\\Hidrosoft Office 2.7" Cliftart Menul\Programs\\Hidrosoft Menul\Programs\\Hidrosoft Office 2.7" Cliftart Menul\Programs\\Bittartup" Cliftart Menul\Programs\\Hidrosoft Office 2.7" Cliftart Menul\Programs\\Bittartup" Cliftart Menul\Programs\\Bittartup" Cliftart Menul\Programs\\Bittartup" Cliftart Menul\Programs\\Bittartup" Cliftart Menul\Programs\\Bittartup" Cliftart Menul\Programs\\Bittartup" Cliftart Menul\Programs\\Bittartup" Cliftart Menul
15753 15754 15755 15755 15759 15760 15761 15762 15764 15765 15766 15766 15769 15770 15770	Betting \UMAYHILL=PC\root\cim21Hin32_LogicalProgramCroup.Hames="Hub11 Blement \UMAYHILL=PC\root\cim21Hin32_ComputerBystem.Hames="Hub11 Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames="Hub11 Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames="Hub11 Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames="Hub11 Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames="Hub11 Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames Betting \UMAYHILL=PC\root\cim22Hin32_ComputerBystem.Hames Betting \UMAYHILL=PC\root\cim2Hin32_Hin32_ComputerBystem.Hames Betting \UMAYHILL=PC\root\cim2Hin32_Hin32_Hin32_Hin32_Hin32_Hin32_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34_Hin34	C:Btart Menul\Programs\\HmtD Hex Editor" C* C:Etart Menul\Programs\\Immunity Inc\\Immunity Debugger" C* C:Etart Menul\Programs\\Java" C* C:Etart Menul\Programs\\Mintemance" C* C:Etart Menul\Programs\\Process Hacker 2* C* C:Etart Menul\Programs\\Process Hacker 2* C* C:Etart Menul\Programs\\Process Hacker 2\\Help and Bupport" C* C:Etart Menul\Programs\\Startup" C* C* C* C* C* C* C* C* C* C
15753 15755 15755 15755 15759 15760 15761 15762 15763 15765 15766 15766 15766 15769 15770 15772 15772 15773	Betting \VMANYHIL-PC\root\cim22Hin32_LogicalProgramCroup.Hams=*Huh1 Blement \VMANYHIL-PC\root\cim22Hin32_ComputerBystem.Nams=*MANYHIL- Betting \VMANYHIL-PC\root\cim22Hin32_ComputerBystem.Nams=*MANYHIL- Betting \VMANYHIL-PC\root\cim22Hin32_ComputerBystem.Nams=*Auh1 Betting \VMANYHIL-PC\root\cim2Hin32_ComputerBystem.Nams=*Auh1 Betting \VMANYHIL-PC\root\cim2Hin32_LogicalProgram1	C:Btart Menul/Programs/lmmunity Inc" C:Btart Menul/Programs/lmmunity Inc/lmmunity Debugger" C:Btart Menul/Programs/lmmunity Inc/lmmunity Debugger" C:Btart Menul/Programs/lgrows" C:Btart Menul/Programs/lgrows: MacKer 2016 Tools" C:Btart Menul/Programs/lprocess HacKer 2 C:Btart Menul/Programs/lprocess HacKer 2/Help and Support" C:Btart Menul/Programs/lprocess HacKer 2/Help and Support AcKer 2/Help and Suppor
15753 15755 15755 15759 15759 15760 15760 15763 15763 15765 15766 15766 15769 15776 15775 15777 15777 15777	Betting \\WARYHILL-BC\root\cim2:Hin32_LogicalProgramCroup.Hams=*bub1 Slement \\WARYHILL-BC\root\cim2:Hin32_LogicalProgramCroup.Hams=*MAYHILL- Betting \\WARYHILL-BC\root\cim2:Hin32_LogicalProgramCroup.Hams=*MAYHIL- Batting \\WARYHILL-PC\root\cim2:Hin32_ComputerBystem.Nams=*MAYHIL- Batting \\WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=*MAYHIL- Batting \\WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=* Batting \\WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=* Batting \WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=* Batting \WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=* Batting \WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=* Batting \WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=* Batting \WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=* Batting \WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Nams=* Batting \WARYHIL-PC\root\cim2:Hin32_Hin32_Hin32_Hin32_Hin32_	<pre>cldtart Menu\\Programs\\Immunity Inc" cldtart Menu\\Programs\\Immunity Inc" cldtart Menu\\Programs\\Immunity Inc\\Immunity Debugger" cldtart Menu\\Programs\\Java" cldtart Menu\\Programs\\Midrosoft Office 2016 Tools" cldtart Menu\\Programs\\Midrosoft Office 2016 Tools" cldtart Menu\\Programs\\Midrosoft Office 2016 Tools" cldtart Menu\\Programs\\Process Hacker 2" cldtart Menu\\Programs\\Process Hacker</pre>
15753 15755 15755 15755 15759 15760 15761 15762 15763 15765 15766 15766 15766 15769 15770 15772 15772 15773	33 Betting \UMARYHIL-PC\root\cim22Hin32_LogicalProgramCroup.Name="Publi 34 Betting \UMARYHIL-PC\root\cim22Hin32_ComputerBystem.Name="Publi 35 Betting \UMARYHIL-PC\root\cim22Hin32_ComputerBystem.Name="Publi 36 Bitting \UMARYHIL-PC\root\cim22Hin32_ComputerBystem.Name="Publi 37 Betting \UMARYHIL-PC\root\cim22Hin32_ComputerBystem.Name="Publi 38 Bitting \UMARYHIL-PC\root\cim22Hin32_ComputerBystem.Name="Advintion" 38 Bitting \UMARYHIL-PC\root\cim22Hin32_LogicalProgramCoup.Name="Fubli 38 Bitting \UMARYHIL-PC\root\cim22Hin32_LogicalProgramCoup.Name="Fubli 38 Bitting \UMARYHIL-PC\root\cim22Hin32_LogicalProgramCoup.Name="Fubli 38 Bitting \UMARYHIL-PC\root\cim22Hin32_LogicalProgramCoup.Name="Fubli 38 Bitting \UMARYHIL-PC\root\cim24Hin32_LogicalProgram Mam="Fubli 38<	<pre>cldtart Menu\\Programs\\Immunity Inc" cldtart Menu\\Programs\\Immunity Inc" cldtart Menu\\Programs\\Immunity Inc\\Immunity Debugger" cldtart Menu\\Programs\\Java" cldtart Menu\\Programs\\Midrosoft Office 2016 Tools" cldtart Menu\\Programs\\Midrosoft Office 2016 Tools" cldtart Menu\\Programs\\Midrosoft Office 2016 Tools" cldtart Menu\\Programs\\Process Hacker 2" cldtart Menu\\Programs\\Process Hacker</pre>
15753 15755 15755 15756 15756 15759 15760 15761 15763 15764 15765 15766 15766 15766 15766 15770 15770 15772 15773 15773 15773 15775 15776 15776	33 Betting \\WARYHIL-BC\root\cim2:Hin32_LogicalProgramCroup.Name="Publi 34 Betting \\WARYHIL-BC\root\cim2:Hin32_ComputerBystem.Name="ANDHILL 35 Betting \\WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="ANDHILL 36 Bitting \\WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="ANDHILL 37 Betting \\WARYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="ANDHILL 38 Bitting \\WARYHIL-PC\root\cim2:Hin32_LogicalProgramCroup.Name="Hub11" 38 Bitting \\WARYHILL-PC\root\cim2:Hin32_LogicalProgramCroup.Name="Hub11" 38 Bitting \\WARYHIL-PC\root\cim2:Hin32_LogicalProgramCroup.Name="Hub11" 38 Bitting \\WARYHIL-PC\root\cim2:Hin32_LogicalProgramCroup.Name="Hub11" 38 Bitting \\WARYHIL-PC\root\cim2:Hin32_LogicalProgramCroup.Name="Hub11"	Cliftart Nenul\Programs\\Immunity Inc" Cliftart Nenul\Programs\\Immunity Inc" Cliftart Nenul\Programs\\Immunity Inc\\Immunity Debugger" Cliftart Nenul\Programs\\Maintenance" Cliftart Menul\Programs\\Maintenance" Cliftart Menul\Programs\\Midrosoft Office 2016 Tools" Cliftart Menul\Programs\\Midrosoft Office 2016 Tools" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2\Help and Support" Cliftart Menul\Programs\\BinPcap" Cliftart Menul\Programs\BinPcap" Cliftart Menul\Programs\\BinPcap"
15753 15755 15756 15756 15759 15759 15761 15761 15762 15762 15765 15766 15769 15770 15771 15772 15776 15776 15776 15776 15776 15779 15779	Betting \VMANVHIL-PC\root\cim21Hin3_LogicalProgramCroup.Hames*Publi Blement \VMANVHIL-PC\root\cim21Hin3_ComputerBystem.Hames*MANVHIL- Betting \VMANVHIL-PC\root\cim21Hin3_ComputerBystem.Hames*MANVHIL- Betting \VMANVHIL-PC\root\cim21Hin3_ComputerBystem.Hames*Publi Betting \VMANVHIL-PC\root\cim21Hin3_ComputerBystem.Hames*Publi Betting \VMANVHIL-PC\root\cim21Hin3_ComputerBystem.Hames*Publi Betting \VMANVHIL-PC\root\cim21Hin3_ComputerBystem.Hames*Publi Betting \VMANVHIL-PC\root\cim21Hin3_ComputerBystem.Hames*Publi Betting \VMANVHIL-PC\root\cim21Hin3_ComputerBystem.Hames*Publi Batting \VMANVHIL-PC\root\cim22Hin3_ComputerBystem.Hames*Publi Batting \VMANVHIL-PC\root\cim24Hin3_ComputerBystem.Hames*Publi Batting \VMANVHIL-PC\root\cim24Hin3_ComputerBystem.Hames*Publi Batting \VMANVHIL-PC\root\cim24Hin3_ComputerBystem.Hames*Publi Batting \VMANVHIL-PC\root\cim24Hin3_ComputerBystem.Hames*Publi Batting \VMANVHIL-PC\root\cim24Hin3_ComputerBystem.Hames*Publi </th <th>Clfart NenullProgramsllmmunity Inc" C C C C C C C C C C C C C C C C C C C</th>	Clfart NenullProgramsllmmunity Inc" C C C C C C C C C C C C C C C C C C C
15753 15755 15755 15756 15756 15750 15750 15760 15761 15763 15764 15765 15766 15766 15766 15770 15770 15770 15777 15773 15773 15777 15777 15777 15776	Betting \UMARYHILL=BC\root\cim2:Hin32_LogicalFogramCroup.Hams="Hull= Blament \UMARYHILL=PC\root\cim2:Hin32_ComputerBystem.Nams="MARYHILL= Batting \UMARYHILE=PC\root\cim2:Hin32_ComputerBystem.Nams="MARYHILE= Batting \UMARYHILE=PC\root\cim2:Hin32_ComputerBystem.Nams="AMAYHILE= Batting \UMARYHILE=PC\root\cim2:Hin32_Comp	Cliftart Nenul\Programs\\ImmUnity Inc" Cliftart Nenul\Programs\\ImmUnity Inc" Cliftart Menul\Programs\\ImmUnity Inc\\ImmUnity Debugger" Cliftart Menul\Programs\\Java" Cliftart Menul\Programs\\Microsoft Office 2016 Wools" Cliftart Menul\Programs\\Microsoft Office 2016 Wools" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2\\Help and Support" Cliftart Menul\Programs\\Process Hacker 2" Cliftart Menul\Programs\\Process Hacker 2\\Help and Support" Cliftart Menul\Programs\\Help Cliftart Menul\Programs\\Liftart Menul\Programs\\Help Cliftart Menu\\Programs\\Help Cliftart Menul\Programs\\Help Cliftart Menu\\Programs\\Help Cliftart Menu\\Programs\\Help Cliftart Menu\\Programs\\Help Cliftart Menu\\Programs\\Help Cliftart Menu\\Programs\\Help Cliftart Menu\\Programs\\Accessories" Cliftart Menu\\Programs\\Accessories\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessibility" Cliftart Menu\\Programs\\Accessories\\Accessibility" Cliftart Me
1373.1 13735 13735 13735 13735 13735 13750 13740 137700 13770 13770 137700 137700 17770 17770 17770 17770 17770 17	Betting \WARVHILL=BC\root\cim2:Hin32_LogicalProgramCroup.Hames="Aubil Blament \WARVHILL=BC\root\cim2:Hin32_ComputerBystem.Name="MARVHILL= Betting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name="MARVHILL= Betting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name="MARVHILL= Betting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name="MARVHILL= Batting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name="MARVHILL= Batting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name="MARVHILL= Batting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name="MARVHILL= Batting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name="MARVHILE Batting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name="MARVHILE Batting \WARVHILL=PC\root\cim2:Hin32_ComputerBystem.Name	Clistert Menul/Programs/lmmunity Inc" Clistert Menul/Programs/lmmunity Inc/lmmunity Debugger" Clistert Menul/Programs/lmmunity Inc/lmmunity Debugger" Clistert Menul/Programs/lyava" Clistert Menul/Programs/lkintenance" Clistert Menul/Programs/lkintenance" Clistert Menul/Programs/lkintenance" Clistert Menul/Programs/lyrocess Hacker 2" Clistert Menul/Programs/lyrocess Hacker 2" Clistert Menul/Programs/lyrocess Hacker 2\lHelp and Support" Clistert Menul/Programs/lyrocess Hacker 2\lHelp and Support 3 Clistert Menul/Programs/lyrocess Hacker 2 Clistert Menul/Programs/lyrocess Hacker 2 Clistert Menul/Programs/lyrocess Hacker 2 Clistert Menul/Programs/lyrocess 4 Clistert Menul/Programs/lyrocess 4 Clistert Menul/Programs/lyrocess 4 Clistert Menul/Programs/lyrocess 4 Clistert Menul/Progra
13753 13754 13755 13755 13755 13755 13755 13755 13755 13762 13763 13763 13763 13763 13763 13765 13766 13765 13776 13776 13776 13777 13777 13777 13777 13777 13777 13777 13777 13777 137787 13778 13778 13778 13778 13778 13778 13778 13778 13778 13778	Betting \VMANVIIL-PC\root\cim21Hin3_LogicalProgramCroup.Hames*tub1 Blement \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Betting \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Betting \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Betting \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Betting \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Betting \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Batting \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Batting \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Batting \VMANVIIL-PC\root\cim21Hin3_ComputerBytem.Hames*TMANVIIL- Batting \VMANVIIL-PC\root\cim22Hin3_ComputerBytem.Hames*TMANVIIL- Batting \VMANV	Cliftert Menul/Programs//Immunity Inc" CT
1373.1 13735 13735 13735 13735 13735 13750 13740 137700 13770 13770 137700 137700 17770 17770 17770 17770 17770 17	Betting \VMANVHIL-BC\root\cim22Hin32_LogicalProgramCroup.Hams=*MaNVHIL- Slement \VMANVHIL-BC\root\cim22Hin32_ComputerBystem.Nams=*MANVHIL- Betting \VMANVHIL-PC\root\cim22Hin32_ComputerBystem.Nams=*MANVHIL- Batting \VMANVHIL-PC\root\cim22Hin32_ComputerBystem.Nams=*MANVHIL- Nams=*Naty Batting \VMANVHIL-PC\root\cim22Hin32_ComputerBystem.Nams=*MANVHIL- Nams=*Naty Batting \VMANVHIL-PC\root\cim22Hin32_ComputerBystem.Nams=*MANVHIL- Nams=*Naty Batting \VMANVHIL-PC\root\cim22Hin32_ComputerBystem.Nams=*MANVHIL- Nams=*Naty Batting \VMA	Didart Nenu\\Programs\\ImmUnity Inc" Didart Menu\\Programs\\ImmUnity Inc" Didtart Menu\\Programs\\ImmUnity Inc\\ImmUnity Debugger" Didtart Menu\\Programs\\Maintenance" Didtart Menu\\Programs\\Maintenance" Didtart Menu\\Programs\\Microsoft Office 2016 Wools" Didtart Menu\\Programs\\Process Hacker 2" Didtart Menu\\Programs\\Process Hacker 2 Didtart Menu\\Programs\\Process Hacker 2 Didtart Menu\\Programs\\Process Hacker 2 Didtart Menu\\Programs\\Process Hacker 2 Didtart Menu\\Programs\\Startup" Didtart Menu\\Programs\\Miccessories" Didtart Menu\\Programs\\Addinistrative Tools" Didtart Menu\Programs\\Addinistrative Tools" Didtart Menu\\Programs\\Addinistrative Tools"
137334 137534 137535 137354 137535 137350 137530 137530 137530 137531 13764 137744 137744 137744 137744 137744 137744 137744 137744 137744 137744 137745 13774 137775 137770 137701 137775 137770 137703 137704 137780 135780 155780 155780 155780 155780 155780 155780 155780 155780 155780 1557	Ava çıkmış tehdit avcısı:)	Cliftert Menul/Programs/lmmunity Inc" Cliftert Menul/Programs/lmmunity Inc" Cliftert Menul/Programs/lmmunity Inc/lmmunity Debugger" Cliftert Menul/Programs/lminterance" Cliftert Menul/Programs/lMicrosoft Office 2016 Tools" Cliftert Menul/Programs/lFrocess Hacker 2" Cliftert Menul/Programs/lFrocess Hacker 2" Cliftert Menul/Programs/lFrocess Hacker 2" Cliftert Menul/Programs/lFrocess Hacker 2./Help and Support" Cliftert Menul/Programs/lfrocessories" Cliftert Menul/Programs/lfrocessories" Cliftert Menul/Programs/lfrocessories/lfrocessories" Cliftert Mary Hill:Start Menul/Programs/lfrocessories/lfrocessories" Cliftert Mary Hill:Start Menul/Programs/lfrocessories" Cliftert Mary Hill:Start Menul/Programs/Mainistrative Tools" Cliftert Mary Hill:Start Menul/Programs/Mainistrative Tools" Cliftert Mary Hill:Start Menul/Programs/Mainistrative Tools" Cliftert Mary Hill:Start Menul/Programs/Mainistrative Tools"
1373.3 1373.5 1373.5 1373.5 1373.5 1373.5 1373.5 1373.5 1374.0 13777.0 137777.0 13777.0 13777.0 13777.0 13777.0 1377	Betting \VMANYHIL-PC\root\cim21Hin32_LogicalProgramCroup.Hams="Hub11 Bismont \VMANYHIL-PC\root\cim21Hin32_ComputerBystem.Nams="HAWHIL- Betting \VMANYHIL-PC\root\cim21Hin32_ComputerBystem.Nams="Hub11 Betting \VMANYHIL-PC\root\cim22Hin32_ComputerBystem.Nams="Hub11 Betting \VMANYHIL-PC\root\cim22Hin32_ComputerBystem.Nams="Hub11 Betting \VMANYHIL-PC\root\cim22Hin32_ComputerBystem.Nams="Hub11 Betting \VMANYHIL-PC\root\cim22Hin32_ComputerBystem.Nams="Hub111 Betting \VMANYHIL-PC\root\cim22Hin32_Compu	Context Nemu\\Programs\\Imp Hex Editor" Context Nemu\\Programs\\Immunity Inc" Context Memu\\Programs\\Immunity Inc\\Immunity Debugger" Context Nemu\\Programs\\Java" Context Nemu\\Programs\\Mintemance" Context Nemu\\Programs\\Mintemance" Context Nemu\\Programs\\Process Hacker 2" Context Nemu\\Programs\\Process Hacker 2" Context Nemu\\Programs\\Process Hacker 2\Help and Support" Context Nemu\\Programs\\Process Hacker 2\Help and Support" Context Nemu\\Programs\\Bintegr Context Nemu\\Programs\\Administrative Tools" Context Nemu\\Programs\\Administrative Tools" Context Nemu\\Programs\\Bintegr Context Nemu\\Programs\\Programs\\Bintegr Context Nemu\\Programs\\Administrative Tools" Context Nemu\\Programs\\Startup" Context Nemu\\Programs\\Startup* Context Nemu\\Programs\\Startup* Context Nemu\\Programs\\Startup* Context Nemu\\Programs\\Startup
13753 13754 13755 13755 13755 13759 13770 13770 13770 13770 13770 13770 13770 13770 13770 13776 13776 13776 13777 13777 13777 13777 13777 13777 13777 13777 13777 13777 1377700 1377700 137770000000000	Betting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="ManyHill- Siement \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="ManyHill- Setting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="ManyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="ManyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32_ComputerBystem.Name="AnyHill- Batting \VMANYHIL-PC\root\cim2:Hin32	<pre>clitert Menu\\Programs\\Imumity Ind" clitert Menu\\Programs\\Imumity Ind" clitert Menu\\Programs\\Imumity Ind\\Immunity Debugger" clitert Menu\\Programs\\Maintenance" clitert Menu\\Programs\\Microsoft Office 2016 Tools" clitert Menu\\Programs\\Accessories\\Accessories" clitert Menu\\Programs\\Accessories\\System Tools" clitert Menu\\Programs\\Accessories\\System Tools" clitert\Mary Hill:Start Menu\\Programs\\Accessories\\System Tools" clitert\Mary Hill:Start Menu\\Programs\\Accessories\\Mintenance" clitert\Mary Hill:Start Menu\\Programs\\Mintenance" clitert\Mary Hill:Start Menu\\Programs\\Microsoft clitert\Mary</pre>

Lastly, my attention was also caught by the output of the Select * from Win32_SystemBIOS WMI request. When I looked at the information coming from the sandboxes, I saw that one of them was running on the BOCHS emulator and another one was running on the QEMU emulator. Therefore, I understood that these two systems belong to the sandbox system.

171 ReleaseDate 2013102900000.000000+000 172 SMBIOSBIOSVersion A04			
172 SHEIOSNAJORVEISION AGA 173 SMEIOSMAJORVERSION 2	Books is a portable IA-32 and v86 64 IBM DC		
174 SMBIOSMinorVersion 0	Bochs is a portable IA-32 and x86-64 IBM PC		
175 SMBIOSPresent True	compatible emulator and debugger mostly		
176 SoftwareElementID Intel IGD BDSM enabled at 0x%08x, size %11dMB, dev 00:02.0	written in C++ and distributed as free		
177 SoftwareElementState 3 178 Status OK	software under the GNU Lesser General		
179 SystemBiosMajorVersion 0	Public License. It supports emulation of the		
180 SystemBiosMinorVersion 0	processor, memory, disks, display, Ethernet,		
181 TargetOperatingSystem 0	BIOS and common hardware peripherals of		
182 Version BOCHS - 1 183 ***** Select * from Win32 SystemBIOS *****	PCs		
<pre>103 Select * From win52_SystemBIOS ***** 104 GroupComponent \\DESKTOP-HRW10\root\cimv2:Win32_ComputerSystem.Name="DESKTOP-HRW10"</pre>			
PartComponent \\DESKTOP-HRW10\root\cimv2:Win32_BIOS.Name="Intel IGD BDSM enabled at 0, size %11dMB,	dev 00:02.0",SortwareElementID="Intel IGD BDSM enabled at 0x%00x, size		
<pre>%11dMB, dev 00:02.0",SoftwareElementState=3,TargetOperatingSystem=0,Version="BOCHS - 1"</pre>			
186 ***** Select * from Win32_Desktop *****			
187 CursorBlinkRate 500 188 DragFullWindows True			
189 IconTitleFaceName MS Shell Dlg			
190 IconTitleSize 8			
191 IconTitleWrap True			
192 Name NT AUTHORITY\SYSTEM			
:\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)INTED IGD BDSM ENAbled at 0x%08x, size %]	dev 00:02.0		
13880 Manufacturer SeaBIOS			
13884 SMBIOSBIOSVersion rel-1.11.0-0-g63451fcal3-prebuilt.gemu-pro 13892 Version _ASUS 1	oject.org		
	em.Name="PC-4A095E27CB"		
13895 PartComponent \\PC-4A095E27CB\root\cimv2:Win32_BIOS me="Int	tel 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 QEMU is a free and			
13918			
13919 open-source emulator			
13920 that performs hardware			
13923 VIRTUALIZATION. QEMU IS a			
13924 hosted virtual machine			
monitor: it emulates the			
13928 machine's processor			
13929			
13930 through dynamic binary			
13931 13932			
13933			
13934			
13935 ICONTILIEWRAP True			
13935 ICONTITIEWRAP TRUE 13936 Name PC-4A095E27CB\STRAZNJICA.GRUBUTT			
13935 ICONTITIEWRAP TRUE 13936 Name PC-4A095E27CB\STRAZNJICA.GRUBUTT 13937 Pattern (None)			
13935 ICONTILleWrap True 13936 Name PC-4A095E27CB\STRAZNJICA.GRUBUTT 13937 Pattern (None) 13938 ScreenSaverActive False			
13935 ICONTITIEWRAP TRUE 13936 Name PC-4A095E27CB\STRAZNJICA.GRUBUTT 13937 Pattern (None)			
13935 ICONTITIEWrap True 13936 Name PC-4A095E27CB\STRAZNJICA.GRUBUTT 13937 Pattern (None) 13938 ScreenSaverActive False 13939 ScreenSaverSecure False	>		
13935 ICONTITIEWRAP TRUE 13936 Name PC-4A095E27CB\STRAZNJICA.GRUBUTT 13937 Pattern (None) 13938 ScreenSaverActive False 13939 ScreenSaverSecure False 13940 ScreenSaverTimeout 60 <	> 15,377 lines INS Read-only Edit Pluq-in Newer 500.2 KB #		

Based on the IP addresses that made requests to the macro.php file during the period of time up until October, I can say that these are most likely from VMRay, Lastline, Any.RUN, VirusTotal sandbox systems and a threat hunter's

IP	Domain	Country	Region	City	ISP	ASN N
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	dslb-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	Tettnang Castle	Deutsche Telekom AG	3320
54.233.172.230	google-proxy-64-233-172- 230.google.com	United States			Google LLC	15169
36.102.6.213	google-proxy-66-102-6- 213.google.com	Inited States			Google LLC	15169
66.249.88.41	google-proxy-66-249-88- 41.google.com	States	California	Mountain View	Google LLC	15169
36.249.88.60	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	Inited States	Georgia	Atlanta	Comcast Cable Communications, LLC	7922
72.12.209.146		Inited States	Indiana	Lafayette	Wintek Corporation	11114
35.203.44.80		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

In conclusion, it does not seem difficult in practice to understand that a developed software, code is running on a sandbox system using the information obtained through WMI, therefore it is important to remember that it is possible for a malicious person or a member of a red team to benefit from this information and the IP addresses, IP blocks of sandbox systems to bypass sandbox analysis.

Hope to see you in the following articles.

Note: Those who are interested can download my presentation file titled "Sandbox Detection" which I discussed this topic in, from the following link, which was presented on November 22nd at the NOPcon International Hacker Conference.