Dr.WEB®
с 1992 года

Методы противодействия техникам детектирования песочниц на примере Doctor Web vxCube

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Докладчик

- Игорь Здобнов
- Руководитель антивирусной лаборатории Dr.Web

Что такое sandbox ?

- Изолированная среда
- Средство анализа подозрительных файлов
- Защита от 0-day угроз и таргетированных атак

Зачем защищать sandbox

- Современные угрозы все чаще детектируют песочницы
  - GootKit
  - ZeuS Panda
  - GravityRAT
- Недостаточно защищенная песочница может быть поэксплуатирована
  - Zero-Day Exploit Published for VM Escape Flaw in VirtualBox
  - 10 new VM escape vulnerabilities discovered in VirtualBox
  - VirtualBox E1000 Guest-to-Host Escape

Как устроен sandbox

- Виртуальная машина (VirtualBox, VMware, QEMU, XEN/KVM, etc)
- Регистратор событий операционной системы
  - Агент
  - Гипервизор
  - Агент скрытый гипервизором

Как устроен sandbox

- Плюсы и минусы каждого из подходов
  - Агент
  - Гипервизор
  - Агент скрытый гипервизором

Как устроен sandbox: Агент

- Драйвер операционной системы
  - Легко обнаружить
  - Снять перехваты или выгрузить драйвер
  - Агент может “утечь”

Как устроен sandbox: Гипервизор

- Гипервизор
  - Сложен в разработке
  - Ничего не знает о внутренностях операционной системы

Векторы атаки на sandbox

- Анализ программного окружения
- Детектирование пользовательской активности
- Детектирование виртуальной среды
  - Проверка артефактов гипервизора
  - Проверка оборудования
  - Атаки по времени

Анализ программного окружения

- Проверка загруженных библиотек в процесс
- Проверка отладчика
- Проверка мьютексов
- Проверка окон

Анализ программного окружения

```
int sboxie_detect_sbiedll() {
        if (GetModuleHandle("sbiedll.dll") != NULL) {
                return TRUE;
        }
        else {
                return FALSE;
        }
}
```

Анализ программного окружения

```
/*-----------------------------------------------Sunbelt sanbox detect-----------
/****
 * Query loaded sunbelt modules
 *
 * return: TRUE - if detected, FALSE - otherwise
 */

int sunbelt_sandbox_modules()
{
        if (GetModuleHandle("api_log.dll") != NULL) {
                return TRUE;
        }
        if (GetModuleHandle("dir_watch.dll") != NULL) {
                return TRUE;
        }
        if (GetModuleHandle("pstorec.dll") != NULL) {
                return TRUE;
        }

        return FALSE;
}
```

Анализ программного окружения

```
        {"^TCPViewClass$", ".*"},
        {".*", "^TCPView - Sysinternals.*$"},
        {"^API_TRACE_MAIN$", ".*"},
        {".*", "^C:\\\\Program Files\\\\Wireshark.*$"},
        {".*", "^C:\\\\wireshark.*$"},
        {".*", "^C:\\\\SandCastle\\\\tools\\\\FakeServer\\.exe$"},
        {".*", "^Fortinet Sunbox$"},
        {"^SmartSniff$", ".*"},
        {".*", "^Fiddler - .*$"},
        {".*", "^Jing$"},
        {".*", "^Wget.*$"},
        {".*", "^start\\.bat - C:\\\\Manual\\\\auto.bat$"},
        {".*", "^Total Commander 7\\.0 - Ahnlab Inc\\.$"},
        {".*", "^Total Commander 6\\.53 - GRISOFT, s\\.r\\.o\\.$"},
        {".*", "^Total Commander 7\\.56a - Avira Soft$"},
        {".*", "^Total Commander 7\\.56a - ROKURA SRL$"},
        {"^gdkWindowToplevel&$", "^Wireshark.*"},
        {".*", "^C:\\\\Python27\\\\Python\\.exe$"},
        {".*", "^C:\\\\strawberry\\\\perl\\\\bin\\\\perl\\.exe$"},
        {"^ThunderRT6FormDC$", "^SysAnalyzer&$"},
        {"^TfrmMain$", "^All-Seeing Eye$"},
        {"^Afx:400000:b:10011:6:350167$", "^Malicious Code Monitor.*$"},
        {"^TApplication$", "^Mouse Move.*$"},
        {"^SmartSniff$", "^SmartSniff$"},
        {"^ConsoleWindowClass$", "^VxStream Kernel Service Manager$"}
};
```

Анализ программного окружения

```
int check_dll_hook(int writelogs){
        const char * blacklist[] = {
                "avcuf32.dll",
                "BgAgent.dll",
                "guard32.dll",
                "wl_hook.dll",
                "QOEHook.dll",
                "a2hooks32.dll",
                "dir_watch.dll",
                "tracer.dll",
                "SbieDll.dll",
                "APIOverride.dll",
                "NtHookEngine.dll",
                "api_log.dll",
                "LOG_API.DLL",
                "LOG_API32.DLL"
        };
```

Анализ программного окружения

```
int check_kernel_driver(int writelogs){
        const char * blacklist[] = {
                "taskrun\\bruta\\kbruta.sys",
                "taskrun\\bruta\\TBM.sys",
                "vmx_svga.sys",
                "vmmouse.sys",
                "xennet.sys",
                "CaptureProcessMonitor.sys",
                "CaptureRegistryMonitor.sys",
                "CaptureFileMonitor.sys",
                "CWSandboxWatchdogDri (sic)",
                "VBoxVideo.sys",
                "bdsnm.sys",
                "bdsflt.sys",
                "ggc.sys",
                "catflt.sys",
                "wsnf.sys",
                "llio.sys",
                "mscank.sys",
                "EMLTDI.SYS",
                "vsdatant.sys",
                "360Box.sys",
                "360Box64.sys",
                "360Camera.sys",
                "360Camera64.sys",
                "360SelfProtection.sys",
                "360AntiHacker.sys",
                "360AntiHacker64.sys",
                "360AvFlt.sys",
                "pctNdis.sys",
                "pctNdisLW64.sys",
```

Детектирование пользовательской активности

- Проверка движения мыши
- Наличие последних редактируемых файлов
- Время с момента старта операционной системы
- Запущенные пользовательские программы
- Проверка имени пользователя и принадлежность к домену

Детектирование пользовательской активности

```
Public Sub checkUsername()

    printMsg "[*] Checking Win32_ComputerSystem.Username ..."
    badUsername = False
    badUsernames = Array("admin", "malfind", "sandbox", "test")

    Set objWMIService = GetObject("winmgmts:\\.\root\cimv2")
    Set colItems = objWMIService.ExecQuery("Select * from Win32_ComputerSystem", , 48)

    For Each objItem In colItems

        For Each badName In badUsernames
            If InStr(LCase(objItem.UserName), badName) > 0 Then
                badUsername = True
            End If
        Next

    Next

    If badUsername Then
        printMsg "DETECTED"
    Else
        printMsg "OK"
    End If

End Sub
```

Проверка артефактов гипервизора

- Ветки реестра, файлы драйверов, имена устройств

```
/*-----------------------------------VMWare additional detect-----------------

/** check if there are Vmware string in "SYSTEM\ControlSet001\services\Disk\Enum\0"

        return: TRUE - if detected, FALSE - otherwise
*/

int vmware_folders(int writelogs){
        const char* blacklist[] = {
                "C:\\Program Files\\VMware\\VMware Tools",
                "C:\\Program Files (x86)\\VMware\\VMware Tools"
        };
```

Проверка артефактов гипервизора

- https://kb.vmware.com/s/article/1009458

Mechanisms to determine if software is running in a VMware virtual machine (1009458)

Last Updated: 05.01.2015 **Categories:** Best Practices 7 **Language:** English subscribe

Details

This KB article documents the mechanisms that programs should use to determine if software is running in a VMware virtual machine.

Solution

Detecting when software is running in a VMware virtual machine relies on two mechanisms:

- Testing the CPUID hypervisor present bit
- Testing the virtual BIOS DMI information and the hypervisor port

Проверка оборудования

- Проверка оборудования через WMI

```
SELECT * FROM Win32_Bios
SELECT * FROM Win32_NetworkAdapterConfiguration
SELECT * FROM Win32_Processor
SELECT * FROM Win32_LogicalDisk
SELECT * FROM Win32_Computer
SELECT * FROM MSAcpi_ThermalZoneTemperature CurrentTemperature)
SELECT * FROM Win32_Fan
```

Проверка оборудования

```
Public Sub checkBios()

    printMsg "[*] Checking Win32_Bios.SMBIOSBIOSVersion & SerialNumber ..."

    badBios = False
    badBiosNames = Array("virtualbox", "vmware", "kvm")

    Set objWMIService = GetObject("winmgmts:\\.\root\cimv2")
    Set colItems = objWMIService.ExecQuery("Select * from Win32_Bios", , 48)

    For Each objItem In colItems

        For Each badName In badBiosNames
            If InStr(LCase(objItem.SMBIOSBIOSVersion), badName) > 0 Then
                badBios = True
            End If
            If InStr(LCase(objItem.SerialNumber), badName) > 0 Then
                badBios = True
            End If
        Next

    Next
    If badBios Then
        printMsg "DETECTED"
    Else
        printMsg "OK"
    End If

End Sub
```

Атаки по времени

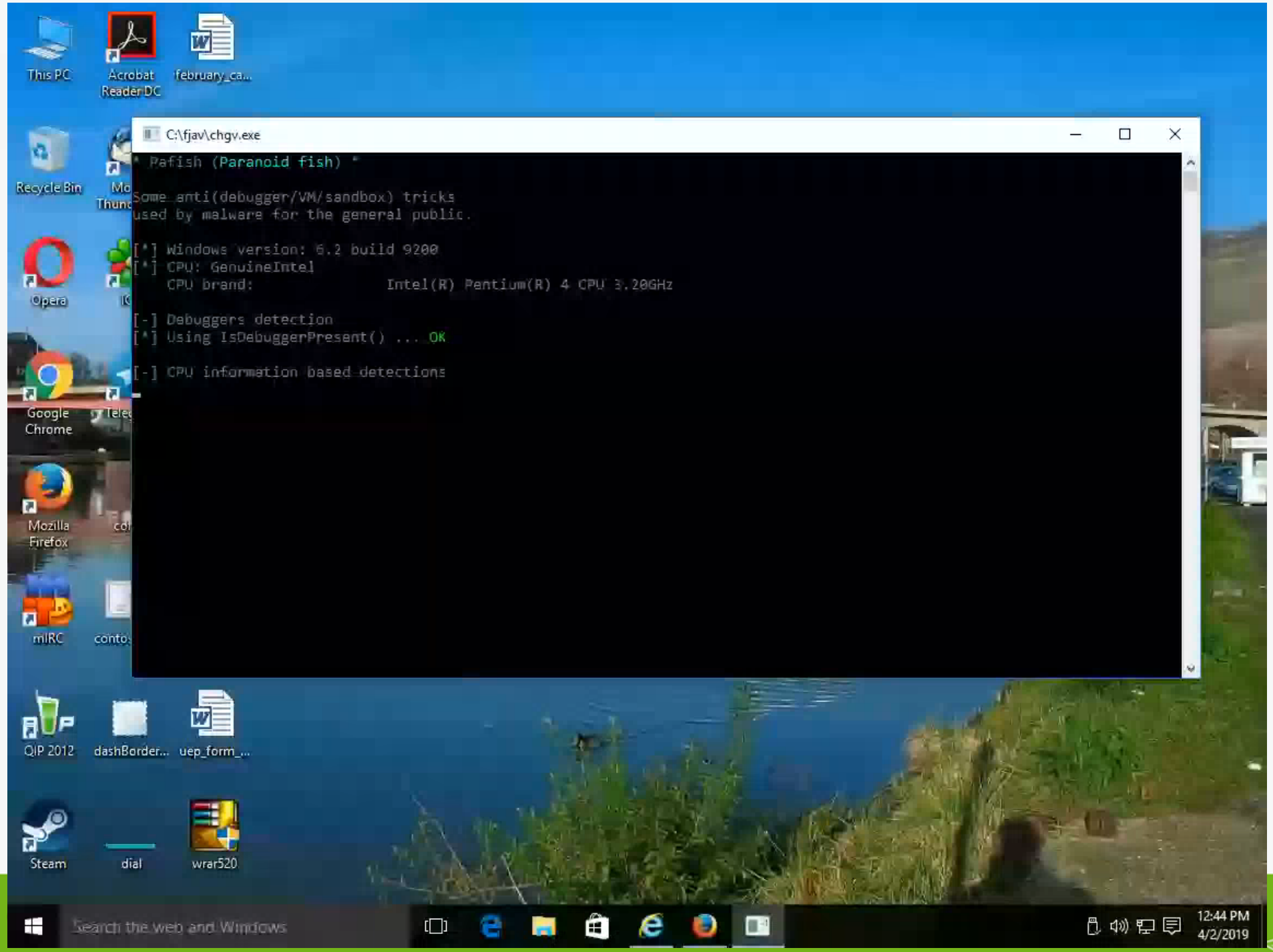
- Временные задержки внутри программы
- Анализ времени исполнения инструкций

```
static inline unsigned long long rdtsc_diff_vmexit() {
        unsigned ret;
        __asm__ volatile(
                "rdtscp\n\t"
                "mov %%eax, %%esi\n\t"
                "mov $0x70000001, %%eax\n\t"
                "cpuid\n\t"
                "rdtscp\n\t"
                "sub %%esi, %%eax\n\t"
                "mov %%eax, %0\n\t" :
                "=r" (ret)
        );
        return (unsigned long long)ret;
}

static inline unsigned long long rdtsc_diff_vmexit4() {
        unsigned ret;
        __asm__ volatile(
                "rdtscp\n\t"
                "mov %%eax, %%esi\n\t"
                "mov $0x70000001, %%eax\n\t"
                "cpuid\n\t"
                "mov $0x70000002, %%eax\n\t"
                "cpuid\n\t"
                "mov $0x70000003, %%eax\n\t"
                "cpuid\n\t"
                "mov $0x70000004, %%eax\n\t"
                "cpuid\n\t"
                "rdtscp\n\t"
                "sub %%esi, %%eax\n\t"
                "mov %%eax, %0\n\t" :
                "=r" (ret)
        );
        return (unsigned long long)ret;
}
```

Pafish

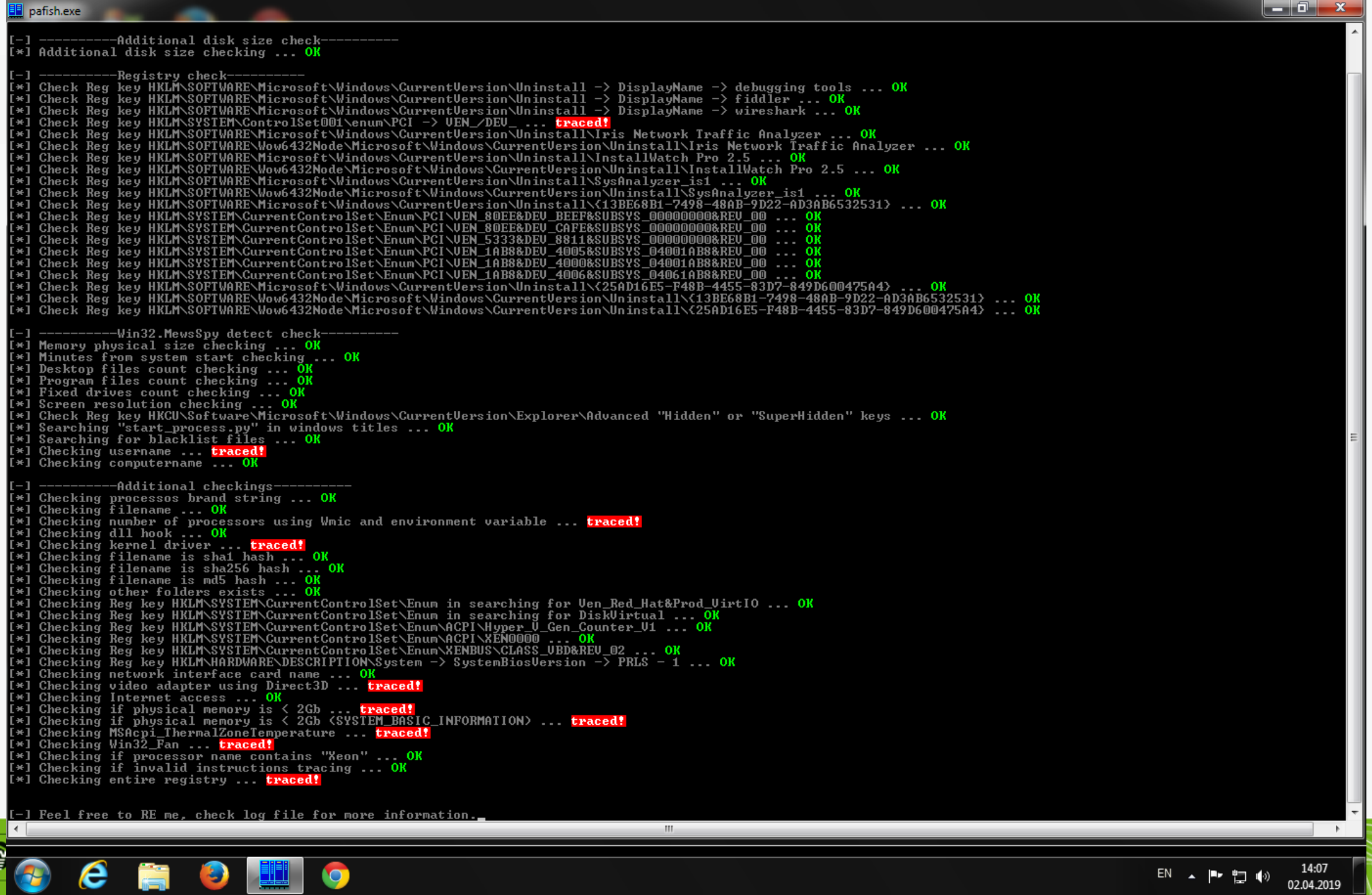
- Для проверки защищенности sandbox существует pafish (но он не обновлялся с 2016 ☺) По этому мы сделали свой pafish
- pafish drweb edition – объединяет в себе самые последние методы детектирования песочний используемые в современных угрозах


This PC
Acrobat Reader DC
february_ca...
Recycle Bin
Opera
Google Chrome
Mozilla Firefox
mIRC
QIP 2012
dashBorder...
uep_form_...
Steam
dial
wrar520
C:\fjav\chgv.exe
* Pafish (Paranoid fish) *
Some anti(debugger/VM/sandbox) tricks
used by malware for the general public.
[*] Windows version: 6.2 build 9200
[*] CPU: GenuineIntel
CPU brand: Intel(R) Pentium(R) 4 CPU 3.20GHz
[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[-] CPU information based detections
Search the web and Windows
12:44 PM
4/2/2019


C:\pbpl\vmuhvry.exe
* Pafish (Paranoid fish) *
Some anti(debugger/VM/sandbox) tricks
used by malware for the general public.
[*] Windows version: 6.1 build 7601
[*] CPU: GenuineIntel
CPU brand: Intel(R) Pentium(R) CPU B960 @ 2.20GHz
[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[-] CPU information based detections
Computer
Steam
ICQ
toolbar
Recycle Bin
Winamp
Acrobat Reader DC
dashBorder..
Google Chrome
dashBorder...
mIRC
delete
Mozilla Firefox
hadac_new...
SDKSample...
Mozilla Thunderbird
hanni_uma...
Telegram
Opera
holycrossc...
TestCertific...
12:28 PM
4/1/2019


pafish.exe
C:\111>pafish.exe
* Pafish (Paranoid fish) *
Some anti(debugger/VM/sandbox) tricks
used by malware for the general public.
[*] Windows version: 6.1 build 7601
[*] CPU: GenuineIntel
Hypervisor: VMwareVMware
CPU brand: Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz
[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK
[-] CPU information based detections
[*] Checking the difference between CPU timestamp counters (rdtsc) ... traced!
[*] Checking the difference between CPU timestamp counters (rdtsc) forcing VM exit ... traced!
[*] Checking the difference between CPU timestamp counters (rdtsc) forcing VM exit for 4 instructions cpuid ... OK
[*] Checking hypervisor bit in cpuid feature bits ... traced!
[*] Checking cpuid hypervisor vendor for known VM vendors ... traced!
[-] Generic sandbox detection
EN
14:06
02.04.2019


pafish.exe
[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK
[*] Reg key (HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions) ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "VideoBiosVersion") ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\DSDT\VBOX__) ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\FADT\VBOX__) ... OK
[*] Reg key (HKLM\HARDWARE\ACPI\RSDT\VBOX__) ... OK
[*] Reg key (HKLM\SYSTEM\ControlSet001\Services\VBox*) ... OK
[*] Reg key (HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDate") ... OK
[*] Driver files in C:\WINDOWS\system32\drivers\VBox* ... OK
[*] Additional system files ... OK
[*] Looking for a MAC address starting with 08:00:27 ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VBoxTray windows ... OK
[*] Looking for VBox network share ... OK
[*] Looking for VBox processes (vboxservice.exe, vboxtray.exe) ... OK
[*] Looking for VBox devices using WMI ... OK
[-] VMware detection
[*] Scsi port 0,1,2 ->bus->target id->logical unit id-> 0 identifier ... traced!
[*] Reg key (HKLM\SOFTWARE\VMware, Inc.\VMware Tools) ... traced!
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... traced!
[*] Looking for C:\WINDOWS\system32\drivers\vmhgfs.sys ... traced!
[*] Looking for a MAC address starting with 00:05:69, 00:0C:29, 00:1C:14 or 00:50:56 ... traced!
[*] Looking for network adapter name ... OK
[*] Looking for pseudo devices ... traced!
[*] Looking for VMware serial number ... traced!
[-] Qemu detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK
[*] cpuid CPU brand string 'QEMU Virtual CPU' ... OK
[-] Bochs detection
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... OK
[*] cpuid AMD wrong value for processor name ... OK
[*] cpuid Intel wrong value for processor name ... OK
[-] Cuckoo detection
[*] Looking in the TLS for the hooks information structure ... OK
[-] ----------DRWEB detection----------
[-] ----------Emulator detection----------
[*] Checking cpuid vendor for known VM vendors ... OK
[*] Check Reg key HKLM\SYSTEM\ControlSet001\services\disk\enum -> sandbox ... OK
[*] Check Reg key HKLM\SYSTEM\ControlSet001\Control\SystemInformation -> sandbox ... OK
[*] Looking for Sandbox file C:\sandbox\starter.exe ... OK
[*] Looking for Sandbox file c:\ipf\BDCore_U.dll ... OK
[*] Looking for Sandbox file c:\cwsandbox_manager ... OK
[*] Looking for Sandbox file C:\cwsandbox ... OK
[*] Looking for Sandbox file C:\gfisandbox ... OK
[*] Looking for Sandbox file d:\sandbox_svc.exe ... OK
[-] ----------VirtualBox detection----------
[*] Check Reg key HKLM\SYSTEM\ControlSet001\services\Disk\Enum "0" -> VBOX ... OK
[*] Check Reg key HKLM\SYSTEM\ControlSet001\Enum\IDE\CdRomVBOX_CD-ROM_____1.0____ ... OK
[*] Oracle mac address prefix starting with 00:03:BA, 00:07:82, 00:0F:4B, 00:10:4F, 00:10:E0, 00:14:4F, 00:20:F2, 00:21:28, 00:21:F6, 08:00:20 ... OK
[*] Executing driverquery command ... OK
[*] VirtualBox video adapter name ... OK
[*] [*] VirtualBox motherboard product ... OK
[*] VirtualBox disk info from setup API ... OK
[*] Searching VirtualBox device VBoxGuest in system objects ... OK
[*] Searching VirtualBox device VBoxMiniRdr in system objects ... OK
[*] Searching VirtualBox driver VBoxVideo in system objects ...
EN
14:05
02.04.2019


pafish.exe
[-] ----------Additional disk size check----------
[*] Additional disk size checking ... OK
[-] ----------Registry check----------
[*] Check Reg key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall -> DisplayName -> debugging tools ... OK
[*] Check Reg key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall -> DisplayName -> fiddler ... OK
[*] Check Reg key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall -> DisplayName -> wireshark ... OK
[*] Check Reg key HKLM\SYSTEM\ControlSet001\enum\PCI -> VEN_/DEV_ ... traced!
[*] Check Reg key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Iris Network Traffic Analyzer ... OK
[*] Check Reg key HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Iris Network Traffic Analyzer ... OK
[*] Check Reg key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\InstallWatch Pro 2.5 ... OK
[*] Check Reg key HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\InstallWatch Pro 2.5 ... OK
[*] Check Reg key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SysAnalyzer_is1 ... OK
[*] Check Reg key HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\SysAnalyzer_is1 ... OK
[*] Check Reg key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13BE68B1-7498-48AB-9D22-AD3AB6532531} ... OK
[*] Check Reg key HKLM\SYSTEM\CurrentControlSet\Enum\PCI\VEN_80EE&DEV_BEEF&SUBSYS_00000000&REV_00 ... OK
[*] Check Reg key HKLM\SYSTEM\CurrentControlSet\Enum\PCI\VEN_80EE&DEV_CAFE&SUBSYS_00000000&REV_00 ... OK
[*] Check Reg key HKLM\SYSTEM\CurrentControlSet\Enum\PCI\VEN_5333&DEV_8811&SUBSYS_00000000&REV_00 ... OK
[*] Check Reg key HKLM\SYSTEM\CurrentControlSet\Enum\PCI\VEN_1AB8&DEV_4005&SUBSYS_04001AB8&REV_00 ... OK
[*] Check Reg key HKLM\SYSTEM\CurrentControlSet\Enum\PCI\VEN_1AB8&DEV_4000&SUBSYS_04001AB8&REV_00 ... OK
[*] Check Reg key HKLM\SYSTEM\CurrentControlSet\Enum\PCI\VEN_1AB8&DEV_4006&SUBSYS_04061AB8&REV_00 ... OK
[*] Check Reg key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{25AD16E5-F48B-4455-83D7-849D600475A4} ... OK
[*] Check Reg key HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{13BE68B1-7498-48AB-9D22-AD3AB6532531} ... OK
[*] Check Reg key HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{25AD16E5-F48B-4455-83D7-849D600475A4} ... OK
[-] ----------Win32.MewsSpy detect check----------
[*] Memory physical size checking ... OK
[*] Minutes from system start checking ... OK
[*] Desktop files count checking ... OK
[*] Program files count checking ... OK
[*] Fixed drives count checking ... OK
[*] Screen resolution checking ... OK
[*] Check Reg key HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced "Hidden" or "SuperHidden" keys ... OK
[*] Searching "start_process.py" in windows titles ... OK
[*] Searching for blacklist files ... OK
[*] Checking username ... traced!
[*] Checking computername ... OK
[-] ----------Additional checkings----------
[*] Checking processos brand string ... OK
[*] Checking filename ... OK
[*] Checking number of processors using Wmic and environment variable ... traced!
[*] Checking dll hook ... OK
[*] Checking kernel driver ... traced!
[*] Checking filename is sha1 hash ... OK
[*] Checking filename is sha256 hash ... OK
[*] Checking filename is md5 hash ... OK
[*] Checking other folders exists ... OK
[*] Checking Reg key HKLM\SYSTEM\CurrentControlSet\Enum in searching for Ven_Red_Hat&Prod_VirtIO ... OK
[*] Checking Reg key HKLM\SYSTEM\CurrentControlSet\Enum in searching for DiskVirtual ... OK
[*] Checking Reg key HKLM\SYSTEM\CurrentControlSet\Enum\ACPI\Hyper_V_Gen_Counter_V1 ... OK
[*] Checking Reg key HKLM\SYSTEM\CurrentControlSet\Enum\ACPI\XEN0000 ... OK
[*] Checking Reg key HKLM\SYSTEM\CurrentControlSet\Enum\XENBUS\CLASS_VBD&REV_02 ... OK
[*] Checking Reg key HKLM\HARDWARE\DESCRIPTION\System -> SystemBiosVersion -> PRLS - 1 ... OK
[*] Checking network interface card name ... OK
[*] Checking video adapter using Direct3D ... traced!
[*] Checking Internet access ... OK
[*] Checking if physical memory is < 2Gb ... traced!
[*] Checking if physical memory is < 2Gb (SYSTEM_BASIC_INFORMATION) ... traced!
[*] Checking MSAcpi_ThermalZoneTemperature ... traced!
[*] Checking Win32_Fan ... traced!
[*] Checking if processor name contains "Xeon" ... OK
[*] Checking if invalid instructions tracing ... OK
[*] Checking entire registry ... traced!
[-] Feel free to RE me, check log file for more information._
EN
14:07
02.04.2019

```
C:\111>dir
 Volume in drive C has no label.
 Volume Serial Number is A416-BD00

 Directory of C:\111

02.04.2019  14:06    <DIR>          .
02.04.2019  14:06    <DIR>          ..
02.04.2019  14:06                 0 hi_av_and_tools_detect
02.04.2019  14:06                 0 hi_bad_kernel_driver
02.04.2019  14:06                 0 hi_bad_number_of_processors
02.04.2019  14:06                 0 hi_bad_registry
02.04.2019  14:06                 0 hi_bad_video_adapter
02.04.2019  14:06                 0 hi_CPU_VM_hv_vendor_name
02.04.2019  14:06                 0 hi_CPU_VM_hypervisor_bit
02.04.2019  14:06                 0 hi_CPU_VM_rdtsc
02.04.2019  14:06                 0 hi_CPU_VM_rdtsc_force_vm_exit
02.04.2019  14:06                 0 hi_hypervisor
02.04.2019  14:06                 0 hi_microsoft_virtual_pc
02.04.2019  14:06                 0 hi_MSAcpi_ThermalZoneTemperature
02.04.2019  14:06                 0 hi_physicalmemory_less_2Gb
02.04.2019  14:06                 0 hi_sandbox
02.04.2019  14:06                 0 hi_sandbox_drive_size2
02.04.2019  14:06                 0 hi_sandbox_mouse_act
02.04.2019  14:06                 0 hi_sandbox_NumberOfProcessors_less_2_GetSystemInfo
02.04.2019  14:06                 0 hi_sandbox_NumberOfProcessors_less_2_raw
02.04.2019  14:06                 0 hi_vmware
02.04.2019  14:06                 0 hi_Win32_Fan
02.04.2019  14:06                 0 hi_win32_mewsspy
28.11.2018  13:20         1 157 120 pafish.exe
02.04.2019  14:06           159 882 pafish.log
              23 File(s)      1 317 002 bytes
               2 Dir(s)   7 947 661 312 bytes free
```

detection method	vxCube	A	B	C	D	E	F
hi_CPU_VM_rdtsc	+	+	+	-	+	+	+
hi_CPU_VM_rdtsc_force_vm_exit	+	-	-	-	+	-	-
hi_CPU_VM_rdtsc_force_vm_exit1000	+	+	+	+	+	-	-
hi_MSAcpi_ThermalZoneTemperature	+	-	-	+	+	-	-
hi_Trap_Flag	+	+	-	+	-	+	+
hi_Win32_Fan	+	-	-	+	-	-	+
hi_Xeon_Processor	+	+	-	+	+	-	-
hi_bad_internet_access	+	+	-	-	+	+	+
hi_bad_kernel_driver	+	+	+	-	+	+	+
hi_bad_number_of_processors	+	- (!2)	-	+	-	-	+
hi_bad_registry_key	+	- (qemu)	+	-	+	+	+
hi_bad_video_adapter	+	+	+	-	+	+	-
hi_physicalmemory_less_2Gb	+	+	+	-	-	+	-
hi_sandbox	+	- (uptime)	-	-	+	+	-
hi_sandbox_mouse_act	+	-	-	+	+	+	+
hi_virtualbox	+	+	-	-	+	-	-
hi_win32_mewsspy	- (user)	-	-	-	+	-	-
hi_qemu	+	- (mac, reg)	+	+	+	+	+
hi_av_and_tools_detect	+	+	+	+	+	-	+

Вопросы?

Dr.Web vxCube на 30 дней для проверки 100 файлов

https://drw.sh/gift