



**МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ**  
**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**  
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**  
**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**

**Лабораторна робота 3**

**Динамічний аналіз шкідливого програмного забезпечення**

**Підготував:**

студент 4 курсу

групи ФІ-84

Коломієць Андрій Юрійович

**Email:** *andkol-ipt22@lil.kpi.ua*

**Викладач:**

**Київ – 2021**

## **Лабораторна робота 3**

### **Динамічний аналіз шкідливого програмного забезпечення**

#### **Мета роботи**

Отримати навички динамічного аналізу **ШПЗ** для платформ **Windows x86** та **x64**.

#### **Постановка задачі**

Дослідити методи автоматичного аналізу **ШПЗ** у пісочниці та популярних антивірусних засобах. Дослідити методи протидії динамічному аналізу в процесі доставки **ШПЗ**.

#### **Завдання**

- Протестуйте **pafish.exe** у **Cuckoo** . Порівняйте результати з прямим запуском у віртуальній машині.
- Розгорніть лабораторію антивірусами. Список антивірусів може включати, але не обмежується:

- *Windows Defender*;
- *Kaspersky Free Antivirus*;
- *Bitdefender Antivirus Free Edition*;
- *Avast Free Antivirus*;
- *Avira Free Antivirus*;
- *AVG 2020*;
- *360 Total Security*;
- *Sophos Home Free*;
- *Zillya! Антивірус Безкоштовний*.

Оновіть антивірусні бази до поточного стану.

- Дослідіть 3-5 зразків з **theZoo** у
  - *Cuckoo Sandbox*;
  - *Антивірусній лабораторії з попереднього кроку*.

При роботі дотримуйтесь техніки безпеки. У **theZoo** представлені активні зразки з функціями шифрування, знищення інформації, експлуатації вразливостей в локальній системі та мережі, автоматичного розповсюдження. Необережний запуск може призвести до зараження власної системи та втрати даних.

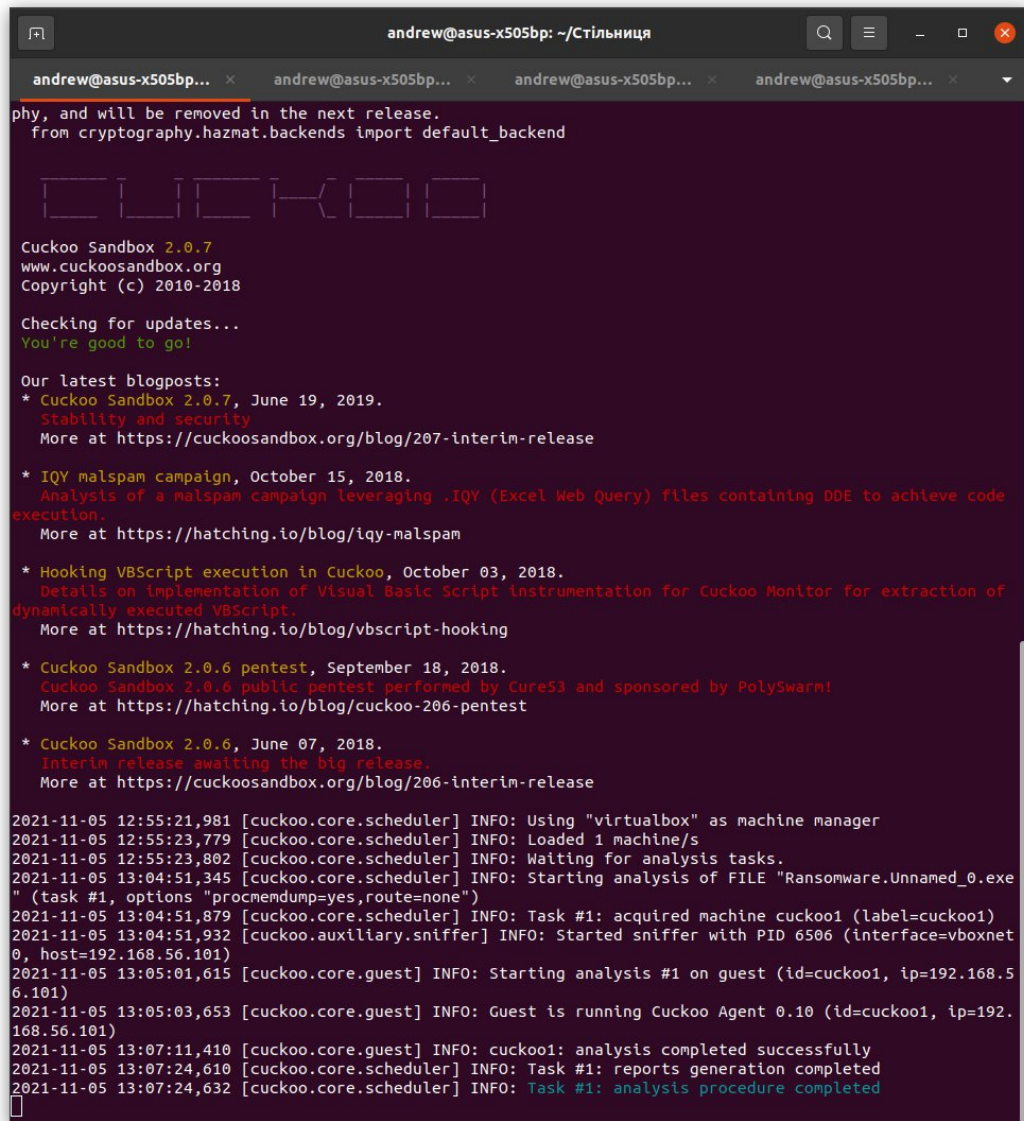
- Реалізуйте мовою **C/C++** детектування середовища аналізу – при запуску у **Cuckoo** та лабораторії з попереднього пункту програма:
  - не має ознак шкідливості у **Cuckoo** та не детектується антивірусами,
  - завершує роботу в середовищі аналізу,
  - при запуску у фізичній системі показує повідомлення користувачу

**(MessageBox “Hello kitty!”).**

- Замініть повідомлення на запуск довільного шеллкоду.
- Проаналізуйте механізм передачі керування у **LIEF** , на прикладі інструментування **PuTTY.exe** .
- Зберіть повністю зразок засобу доставки з результатів попередніх пунктів – антиемуляція, **download-execute** шеллкод, навантаження , та проаналізуйте у розгорнутих **Cuckoo** та лабораторії.
- Модифікуйте отриманий зразок для успішного проходження поведінкового аналізу та тестів антивірусними засобами.

## Зауваження

Розгортання лабораторії з *Cuckoo* мало труднощі і на жаль успішна установка була виконана після виконання лабораторної роботи. В данному протоколі наводиться онлайн версія *Cuckoo Sandbox* проте результати виконання аналогічних дій були ті ж самі.



```
andrew@asus-x505bp: ~/Стільниця
andrew@asus-x505bp... x andrew@asus-x505bp... x andrew@asus-x505bp... x andrew@asus-x505bp... x
phy, and will be removed in the next release.
from cryptography.hazmat.backends import default_backend

Cuckoo Sandbox 2.0.7
www.cuckoosandbox.org
Copyright (c) 2010-2018

Checking for updates...
You're good to go!

Our latest blogposts:
* Cuckoo Sandbox 2.0.7, June 19, 2019.
  Stability and security
  More at https://cuckoosandbox.org/blog/207-interim-release

* IQY malspam campaign, October 15, 2018.
  Analysis of a malspam campaign leveraging .IQY (Excel Web Query) files containing DDE to achieve code
  execution.
  More at https://hatching.io/blog/iqy-malspam

* Hooking VBScript execution in Cuckoo, October 03, 2018.
  Details on implementation of Visual Basic Script instrumentation for Cuckoo Monitor for extraction of
  dynamically executed VBScript.
  More at https://hatching.io/blog/vbscript-hooking

* Cuckoo Sandbox 2.0.6 pentest, September 18, 2018.
  Cuckoo Sandbox 2.0.6 public pentest performed by Cure53 and sponsored by PolySwarm!
  More at https://hatching.io/blog/cuckoo-206-pentest

* Cuckoo Sandbox 2.0.6, June 07, 2018.
  Interim release awaiting the big release.
  More at https://cuckoosandbox.org/blog/206-interim-release

2021-11-05 12:55:21,981 [cuckoo.core.scheduler] INFO: Using "virtualbox" as machine manager
2021-11-05 12:55:23,779 [cuckoo.core.scheduler] INFO: Loaded 1 machine/s
2021-11-05 12:55:23,802 [cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
2021-11-05 13:04:51,345 [cuckoo.core.scheduler] INFO: Starting analysis of FILE "Ransomware.Unnamed_0.exe
" (task #1, options "procmemdump=yes,route=none")
2021-11-05 13:04:51,879 [cuckoo.core.scheduler] INFO: Task #1: acquired machine cuckoo1 (label=cuckoo1)
2021-11-05 13:04:51,932 [cuckoo.auxiliary.sniffer] INFO: Started sniffer with PID 6506 (interface=vboxnet
0, host=192.168.56.101)
2021-11-05 13:05:01,615 [cuckoo.core.guest] INFO: Starting analysis #1 on guest (id=cuckoo1, ip=192.168.5
6.101)
2021-11-05 13:05:03,653 [cuckoo.core.guest] INFO: Guest is running Cuckoo Agent 0.10 (id=cuckoo1, ip=192.
168.56.101)
2021-11-05 13:07:11,410 [cuckoo.core.guest] INFO: cuckoo1: analysis completed successfully
2021-11-05 13:07:24,610 [cuckoo.core.scheduler] INFO: Task #1: reports generation completed
2021-11-05 13:07:24,632 [cuckoo.core.scheduler] INFO: Task #1: analysis procedure completed
```

## Виконання роботи

Протестуйте *pafish.exe* у *Cuckoo* . Порівняйте результати з прямим запуском у віртуальній машині.

### Прямий запуск в віртуальній середовищі

```
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\IEUser>CD C:/Users/IEUser/Desktop/pafish-master/pafish-master
C:\Users\IEUser\Desktop\pafish-master\pafish-master>pafish
* Pafish (Paranoid fish) *

Some anti(debugger/VM/sandbox) tricks
used by malware for the general public.

[*] Windows version: 6.1 build 7601
[*] CPU: AuthenticAMD
    Hypervisor: VBoxVBoxVBox
    CPU brand: AMD A9-9420 RADEON R5, 5 COMPUTE CORES 2C+3G

[-] Debuggers detection
[*] Using IsDebuggerPresent() ... OK

[-] CPU information based detections
[*] Checking the difference between CPU timestamp counters <rdtsc> ... OK
[*] Checking the difference between CPU timestamp counters <rdtsc> forcing VM ex
it ... traced!
[*] Checking hypervisor bit in cpuid feature bits ... traced!
[*] Checking cpuid hypervisor vendor for known VM vendors ... traced!

[-] Generic sandbox detection
[*] Using mouse activity ... OK
[*] Checking username ... OK
[*] Checking file path ... OK
[*] Checking common sample names in drives root ... OK
[*] Checking if disk size <= 60GB via DeviceIoControl() ... OK
[*] Checking if disk size <= 60GB via GetDiskFreeSpaceEx() ... traced!
[*] Checking if Sleep() is patched using GetTickCount() ... OK
[*] Checking if NumberOfProcessors is < 2 via raw access ... traced!
[*] Checking if NumberOfProcessors is < 2 via GetSystemInfo() ... traced!
[*] Checking if physical memory is < 1Gb ... traced!
[*] Checking operating system uptime using GetTickCount() ... OK
[*] Checking if operating system IsNativeUhdBoot() ... OK

[-] Hooks detection
[*] Checking function ShellExecuteExW method 1 ... OK
[*] Checking function CreateProcessA method 1 ... OK

[-] Sandboxie detection
[*] Using GetModuleHandle(sbi.dll) ... OK

[-] Wine detection
[*] Using GetProcAddress(wine_get_unix_file_name) from kernel32.dll ... OK
[*] Reg key (HKCU\SOFTWARE\Wine) ... OK

[-] VirtualBox detection
[*] Scsi port->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\HARDWARE\Description\System "SystemBiosVersion") ... traced!
[*] Reg key (HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions) ... traced!
[*] Reg key (HKLM\HARDWARE\Description\System "VideoBiosVersion") ... traced!
[*] Reg key (HKLM\HARDWARE\ACPI\BIST\UBOX) ... traced!
[*] Reg key (HKLM\HARDWARE\ACPI\FADT\UBOX) ... traced!
[*] Reg key (HKLM\HARDWARE\ACPI\BIST\UBOX) ... traced!
[*] Reg key (HKLM\SYSTEM\ControlSet001\Services\UBOX*) ... traced!
[*] Reg key (HKLM\HARDWARE\DESCRIPTION\System "SystemBiosDate") ... traced!
[*] Driver files in C:\WINDOWS\system32\drivers\UBOX* ... traced!
[*] Additional system files ... traced!
[*] Looking for a MAC address starting with 08:00:27 ... traced!
[*] Looking for pseudo devices ... traced!
[*] Looking for VBoxTray windows ... traced!
[*] Looking for VBox network share ... traced!
[*] Looking for VBox processes (vboxservice.exe, vboxtray.exe) ... traced!
[*] Looking for VBox devices using WMI ... traced!
```

```

[-] VMware detection
[*] Scsi port 0,1,2 ->bus->target id->logical unit id-> 0 identifier ... OK
[*] Reg key (HKLM\SOFTWARE\VMware, Inc.\VMware Tools) ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmmouse.sys ... OK
[*] Looking for C:\WINDOWS\system32\drivers\vmhgfs.sys ... OK
[*] Looking for a MAC address starting with 00:05:69, 00:0C:29, 00:1C:14 or 00:5
0:56 ... OK
[*] Looking for network adapter name ... OK
[*] Looking for pseudo devices ... OK
[*] Looking for VMware serial number ... OK

[-] 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

[-] Feel free to RE me, check log file for more information.

```

## Cuckoo Sandbox

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package	
2459080	30/10/2021 12:18	pafish.exe	exe	● running
Done				

### Summary

File pafish.exe

Summary		Download	Filedata sample	Download yara
Size	75,0KB			
Type	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows			
MD5	9159ed64c4421d888d88b72db23f3			
SHA1	124f462281e229888ae5e9a24d6e713639a64f9			
SHA256	2188f4a13add5e34edc16994876a9d2f5eac3fcb695db856953701bd24cd6d5			
SHA512	<a href="#">Show SHA512</a>			
CRC32	6f630481			
scodep	None			
Yara	<ul style="list-style-type: none"> <li>vmdetect - Possibly employs anti-virtualization techniques</li> <li>Check_Oemu_Description - (no description)</li> <li>Check_Oemu_DeviceMap - (no description)</li> <li>Check_VBox_Description - (no description)</li> <li>Check_VBox_DeviceMap - (no description)</li> <li>Check_VBox_Guest_Additions - (no description)</li> <li>Check_VBox_VideoDrivers - (no description)</li> <li>Check_VMware_DeviceMap - (no description)</li> <li>Check_VmTools - (no description)</li> <li>Check_Wine - (no description)</li> </ul>			

### Score

This file is **very suspicious**, with a score of 10 out of 10!

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

### Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

### Information on Execution

Analysis					
Category	Started	Completed	Duration	Routing	Logs
FILE	Oct. 30, 2021, 1:44 p.m.	Oct. 30, 2021, 1:46 p.m.	109 seconds	Internet	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

### Signatures

- Yara rules detected for file (10 events) >
- Checks if process is being debugged by a debugger (1 event) >
- Command line console output was observed (50 out of 128 events) >
- Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate) (1 event) >
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event) >





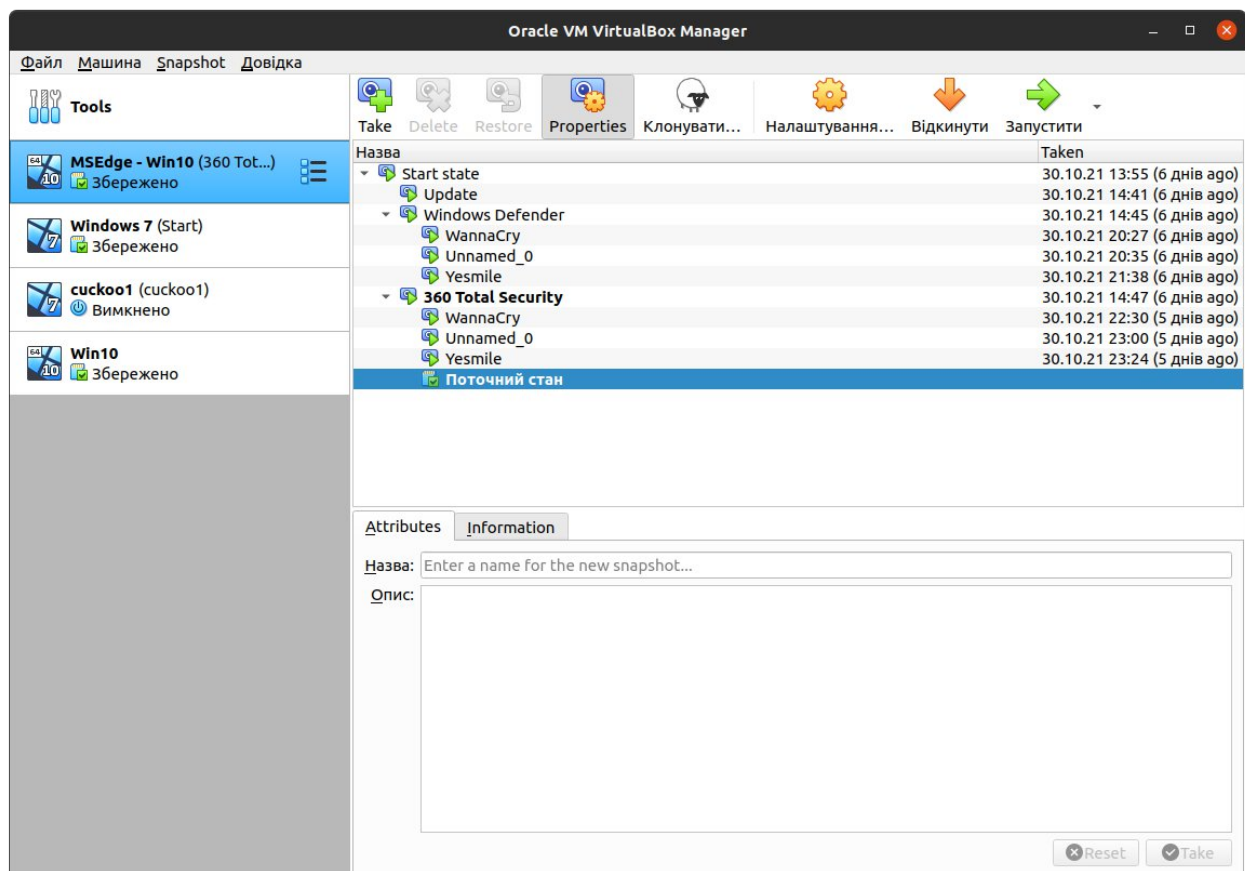
Розгорніть лабораторію з 2-3 антивірусами. Список антивірусів може включати, але не обмежується

– *Windows Defender*;

– *360 Total Security*;

Оновіть антивірусні бази до поточного стану.

### ***Розгортання лабораторії з антивірусами***





Дослідіть 3-5 зразків з **theZoo** у

– *Cuckoo Sandbox*;

– *Антивірусній лабораторії з попереднього кроку.*

При роботі дотримуйтесь техніки безпеки. У **theZoo** представлені активні зразки з функціями шифрування, знищення інформації, експлуатації вразливостей в локальній системі та мережі, автоматичного розповсюдження. Необережний запуск може призвести до зараження власної системи та втрати даних.

## Cuckoo Sandbox

## WannaCry

### Summary

File ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

Size	3.4MB
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84c82835a5d21bdcf75a61706d8ab549
SHA1	5f1f465afaabcf8015061a3ab2c2e74f3a4426467
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
SHA512	<a href="#">Show SHA512</a>
CRC32	4022FCAA
ssdeep	98304:QpPeBhz1aRxcSUDK365AEthvwa9P593R8yAVp2g3x::QpPe1Ccxk3ZAEIadzR8yc4qB
Yara	<ul style="list-style-type: none"><li>WannaDecryptor - Detection for common strings of WannaDecryptor</li><li>Wanna_Sample_84c82835a5d21bdcf75a61706d8ab549 - Specific sample match for WannaCryptor</li><li>ransom_tefefonica - Ransomware Telefonica</li><li>WannaCry_Ransomware_Generic - Detects WannaCry Ransomware on Disk and in Virtual Page</li><li>WannaCry_Ransomware - Detects WannaCry Ransomware</li><li>WannaCry_Ransomware_Dropper - WannaCry Ransomware Dropper</li><li>wannacry_static_ransom - Detects WannaCryptor spreaded during 2017-May-12th campaign and variants</li><li>win_registry - Affect system registries</li><li>win_files_operation - Affect private profile</li><li>Win32_Ransomware_WannaCry - Yara rule that detects WannaCry ransomware.</li></ul>

#### Information on Execution

Category	Started	Completed	Duration	Routing	Logs
FILE	Oct. 30, 2021, 11:52 p.m.	Oct. 30, 2021, 11:54 p.m.	124 seconds	Internet	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

#### Signatures

- Yara rules detected for file (10 events)
- Queries for the computername (2 events)
- Checks if process is being debugged by a debugger (1 event)
- Command line console output was observed (2 events)
- Uses Windows APIs to generate a cryptographic key (4 events)

### Score

This file is **very suspicious**, with a score of 10 out of 10!

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

#### Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

**Ooops, your important files are encrypted.**

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "**@WanaDecryptor@.exe**" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

## Unnamed\_0

### Summary

File Ransomware.Unnamed\_0.exe

Size	902.5KB
Type	PE32 executable (GUI) Intel 80386 Mono/Net assembly, for MS Windows
MD5	96af1c9de13c6236bc5428c339c57283
SHA1	c6bdf185419e31987f4b7291f9966a0460e4b25
SHA256	517ac596a548ba1193686766c57ad3288c2258c518894eb27361b674526cc
SHA512	<a href="#">Show SHA512</a>
CRC32	96928089
ssdeep	24576:CBPj11w1z5dyqtnhCJfmuEEOj17WpJ1WY:7Q13aZCfKOUj178rj1W
Yara	None matched

#### Information on Execution

Category	Started	Completed	Duration	Routing	Logs
FILE	Oct. 30, 2021, 11:53 p.m.	Oct. 30, 2021, 11:55 p.m.	125 seconds	Internet	<a href="#">Show Analysis Log</a> <a href="#">Show Cuckoo Log</a>

#### Signatures

- Allocates read-write-execute memory (usually to unpack itself) (22 events)
- Checks if process is being debugged by a debugger (2 events)
- Uses Windows APIs to generate a cryptographic key (9 events)
- Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)
- One or more potentially interesting buffers were extracted, these generally contain injected code, configuration data, etc.
- Creates executable files on the filesystem (1 event)
- Searches running processes potentially to identify processes for sandbox evasion, code injection or memory dumping (39 events)
- The binary likely contains encrypted or compressed data indicative of a packer (2 events)
- Checks for the Locally Unique Identifier on the system for a suspicious privilege (1 event)

### Score

This file is **very suspicious**, with a score of 18 out of 10!


Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

#### Autosubmit

2459964  
2459965

#### Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)



## Yesmile

### Summary

File YESMILE.EXE

Size	4.8KB
Type	DOS executable (COM)
MD5	b7586a154365f8131217869d528a1381
SHA1	694ee33186437a664ceb1e44263627cc2491392
SHA256	91fa185f353b798b4d7b3b468583244e4c84be8c43959b32d6821d764d5d8c41
SHA512	<a href="#">Show SHA512</a>
CRC32	9C003583
ssdeep	96:30R8/9WcWkY/BHOMBRAT0B6xhDKHSH-GaYauD:v633e90az5MJC
Yara	None matched


#### Information on Execution

Category	Started	Completed	Duration	Routing	Logs
FILE	Oct. 30, 2021, 11:54 p.m.	Oct. 30, 2021, 11:55 p.m.	53 seconds	Internet	<a href="#">Show Analysis Log</a> <a href="#">Show Cuckoo Log</a>

#### Signatures

- File has been identified by 10 AntiVirus engine on IMA as malicious (10 events)
- File has been identified by 25 AntiVirus engines on VirusTotal as malicious (25 events)

#### Screenshots



### Score


This file is **very suspicious**, with a score of 18 out of 10!

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

#### Feedback

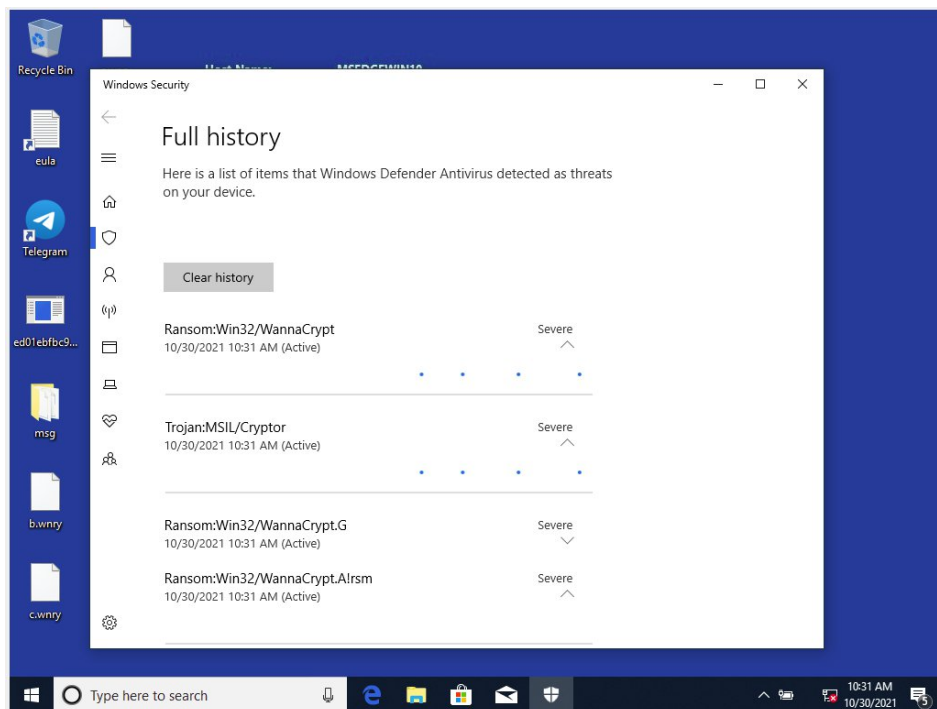
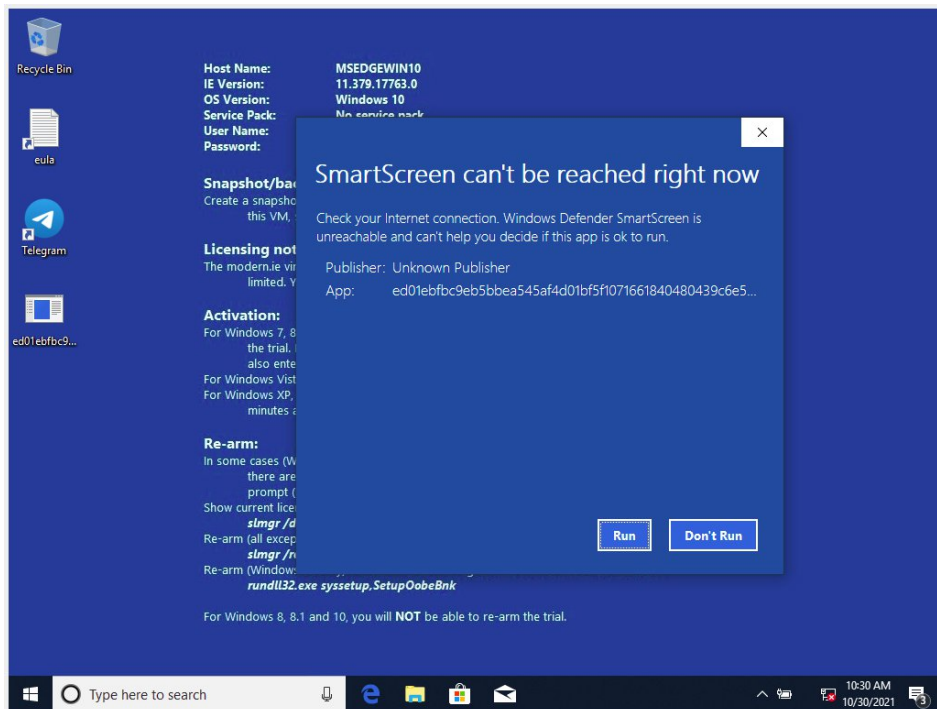
Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Name	Response	Post-Analysis Lookup	IP Address	Status	Action	VT	Location
No hosts contacted.			No hosts contacted.				

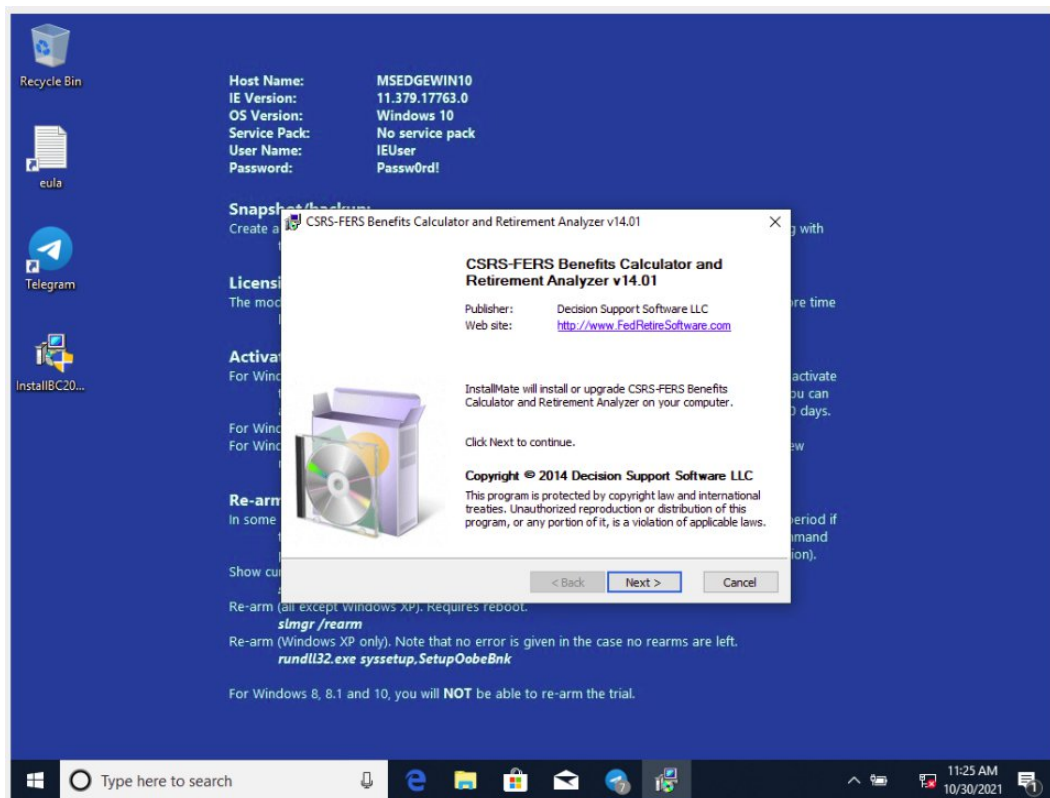
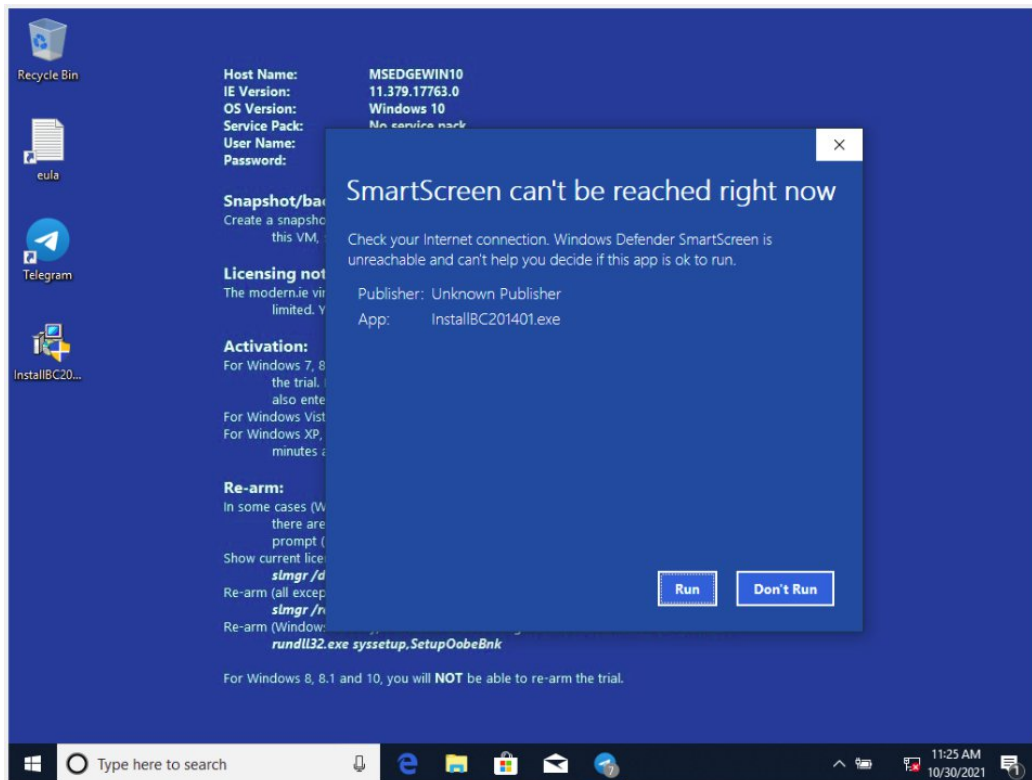


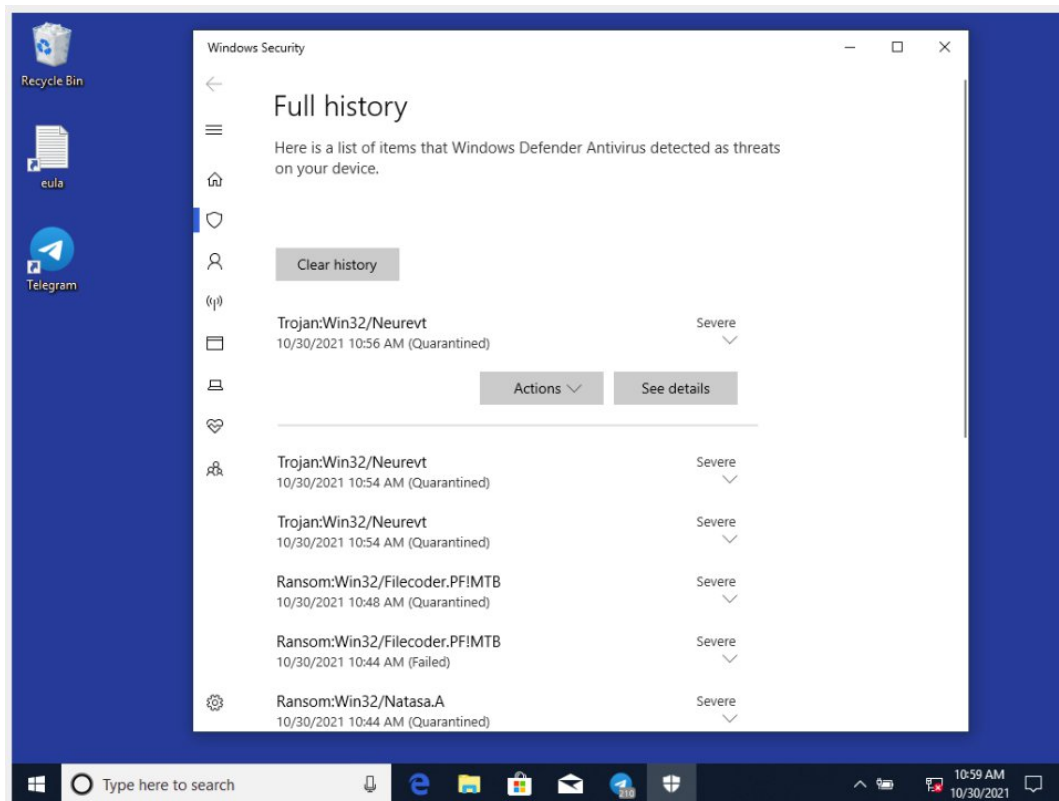
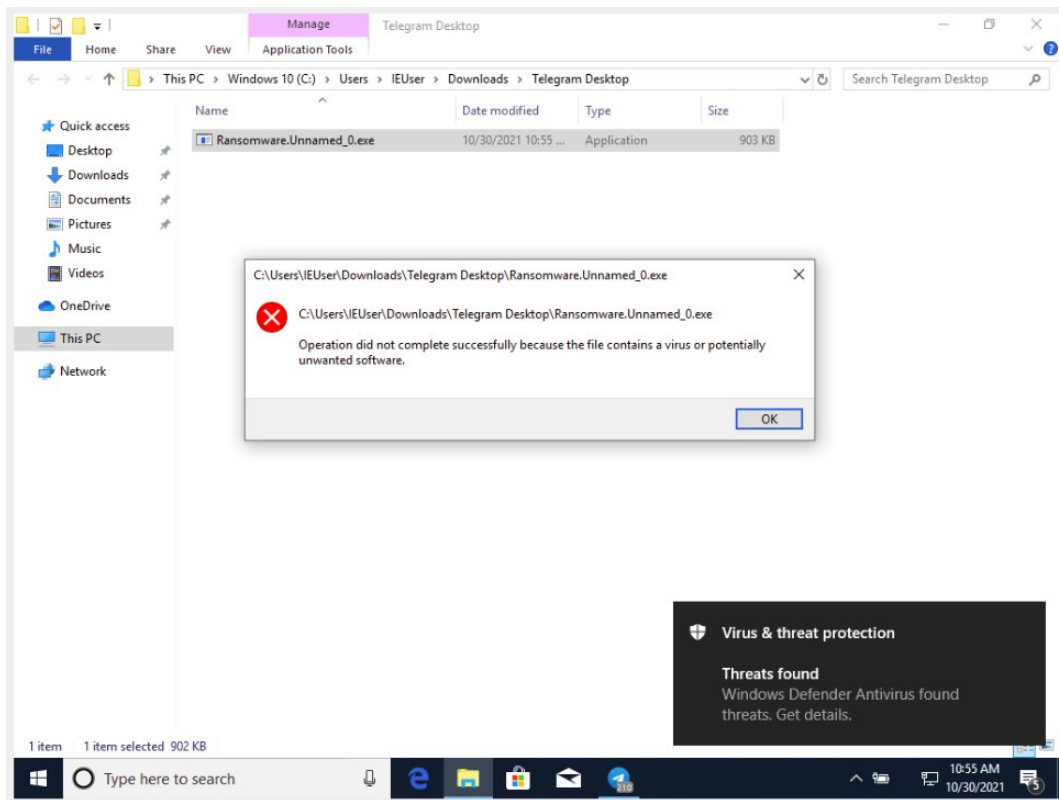
*Переходимо в VM Windows 10 та тестуємо шкідливі зразки файлів*

## WannaCry



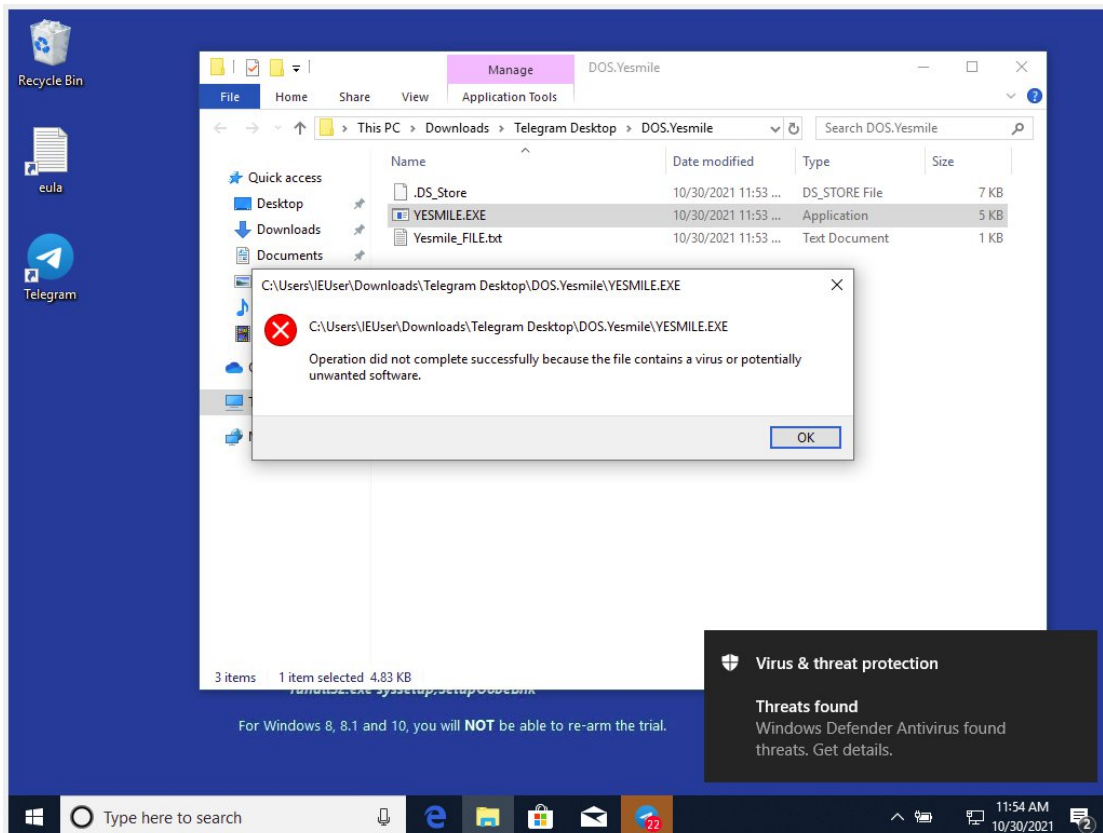
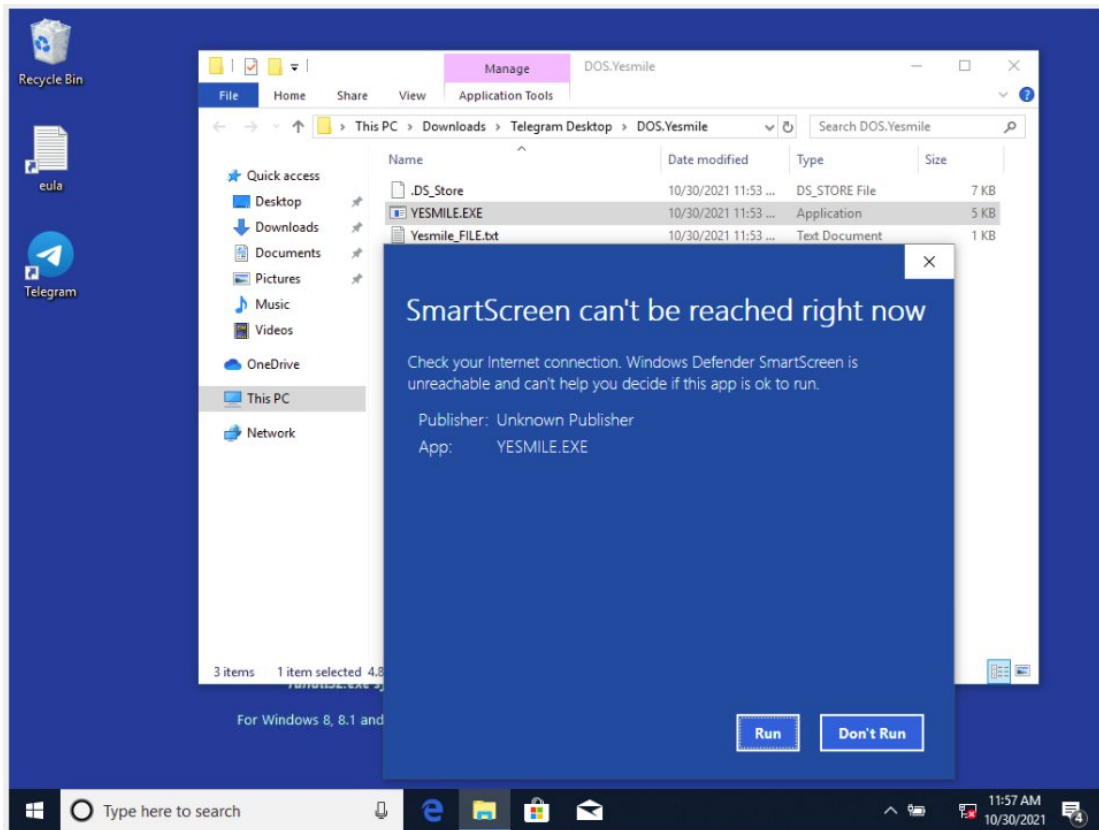
## Unnamed\_0



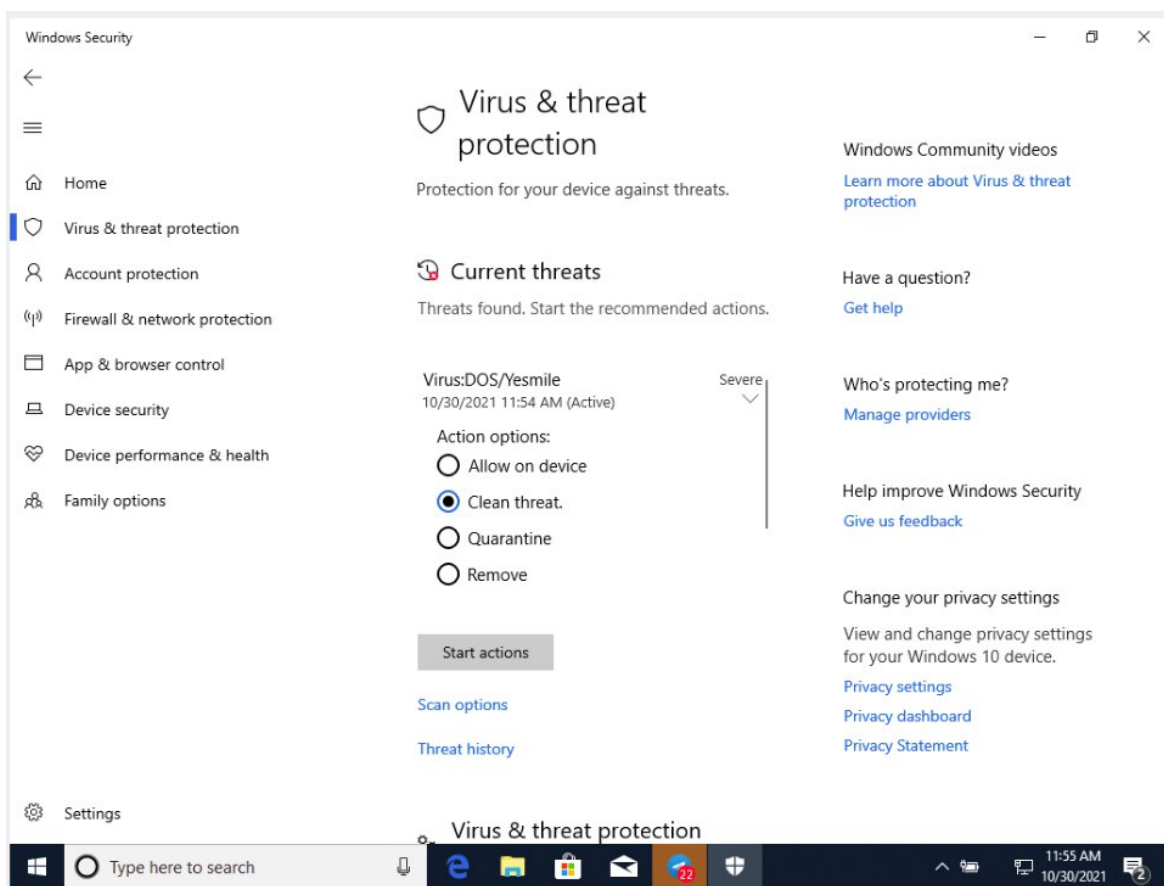




## Yesmile







***Посилання на відповідні результати для Cuckoo Sandbox:***

- WannaCry :

<https://cuckoo.cert.ee/analysis/2459960/summary/>

- Unnamed\_0 :

<https://cuckoo.cert.ee/analysis/2459961/summary/>

- Yesmile :

<https://cuckoo.cert.ee/analysis/2459963/summary/>

Реалізуйте мовою C/C++ детектування середовища аналізу – при запуску у **Cuckoo** та лабораторії з попереднього пункту програма:

- не має ознак шкідливості у **Cuckoo** та не детектується антивірусами,
- завершує роботу в середовищі аналізу,
- при запуску у фізичній системі показує повідомлення користувачу
- замініть повідомлення на запуск довільного шеллкоду .

**(MessageBox “Hello kitty!”).**

**Код, що детектує віртуальне середовище**

```
#include <iostream>
#include <vector>
#include <string>
#include <Windows.h>
#include <winbase.h>
#include <fstream>

using namespace std;

std::string execute(const std::string& command)
{
    system((command + " > temp.txt").c_str());

    ifstream ifs("temp.txt");

    string ret{ std::istreambuf_iterator<char>(ifs), std::istreambuf_iterator<char>() };

    ifs.close(); // must close the inout stream so the file can be cleaned up

    if (std::remove("temp.txt") != 0)
    {
        perror("Error deleting temporary file");
    }

    return ret;
}
```

```

bool Is_VM_system()
{

    string system_information=execute("wmic computersystem get model,manufacturer");

    if (system_information.find("Virtual") != std::string::npos || system_information.find("virtual") != std::string::npos)
    {
        cout << endl << system_information << endl;
        return true;
    }
    else
    {
        return false;
    }
}

bool IsVM_file()
{
    vector<string> file_name;

    //VMware
    {
        file_name.push_back("C:\\Windows\\System32\\drivers\\Vmmouse.sys");
        file_name.push_back("C:\\Windows\\System32\\drivers\\vm3dgl.dll");
        file_name.push_back("C:\\Windows\\System32\\drivers\\vmdum.dll");
        file_name.push_back("C:\\Windows\\System32\\drivers\\vm3dver.dll");
        file_name.push_back("C:\\Windows\\System32\\drivers\\vmtray.dll");
        file_name.push_back("C:\\Windows\\System32\\drivers\\VMToolsHook.dll");
        file_name.push_back("C:\\Windows\\System32\\drivers\\lvmmousever.dll");
        file_name.push_back("C:\\Windows\\System32\\drivers\\lvmhgfs.dll");
        file_name.push_back("C:\\Windows\\System32\\drivers\\vmGuestLib.dll");
        file_name.push_back("C:\\Windows\\System32\\drivers\\VmGuestLibJava.dll");
    }

    //VirtualBox
    {
        file_name.push_back("C:\\Windows\\System32\\drivers\\VBoxMouse.sys");
        file_name.push_back("C:\\Windows\\System32\\drivers\\VBoxGuest.sys");
        file_name.push_back("C:\\Windows\\System32\\drivers\\VBoxSF.sys");
        file_name.push_back("C:\\Windows\\System32\\drivers\\VBoxVideo.sys");
        file_name.push_back("C:\\Windows\\System32\\vboxdisp.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxhook.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxmxrnp.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxoglarrayspu.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxoglcrutil.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxoglerrorspu.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxoglfeedbackspu.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxoglpackspu.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxoglpassthroughspu.dll");
        file_name.push_back("C:\\Windows\\System32\\vboxservice.exe");
        file_name.push_back("C:\\Windows\\System32\\vboxtray.exe");
    }

    for (int i=0;i<file_name.size();i++)
    {
        string path = file_name[i];
    }
}

```

```

GetFileAttributes((LPCWSTR)path.c_str());

if (INVALID_FILE_ATTRIBUTES == GetFileAttributes((LPCWSTR)path.c_str()) && GetLastError() == ERROR_FILE_NOT_FOUND)
{
    continue;
}
else
{
    cout << path.c_str() << endl;
    return true;
}

}

return false;
}

int main()
{
    if (IsVM_file() || Is_VM_system())
    {
        cout << endl << "Virtual Machine enviroment is switch on." << endl;
    }
    else
    {
        //First verison program
        //

        HWND hWnd = GetForegroundWindow();    ShowWindow(hWnd, SW_HIDE);

        MessageBox(0, L"Hello Kitty!", L"Virtual Machine enviroment is switch off.", MB_OK);

        //Second version program
        //

        /*char buf[] = "\xcc\xcc\xcc\xcc";

        int (*func)();
        func = (int (*)(void*)) buf;
        (int)(*func)();

        Sleep(1000);

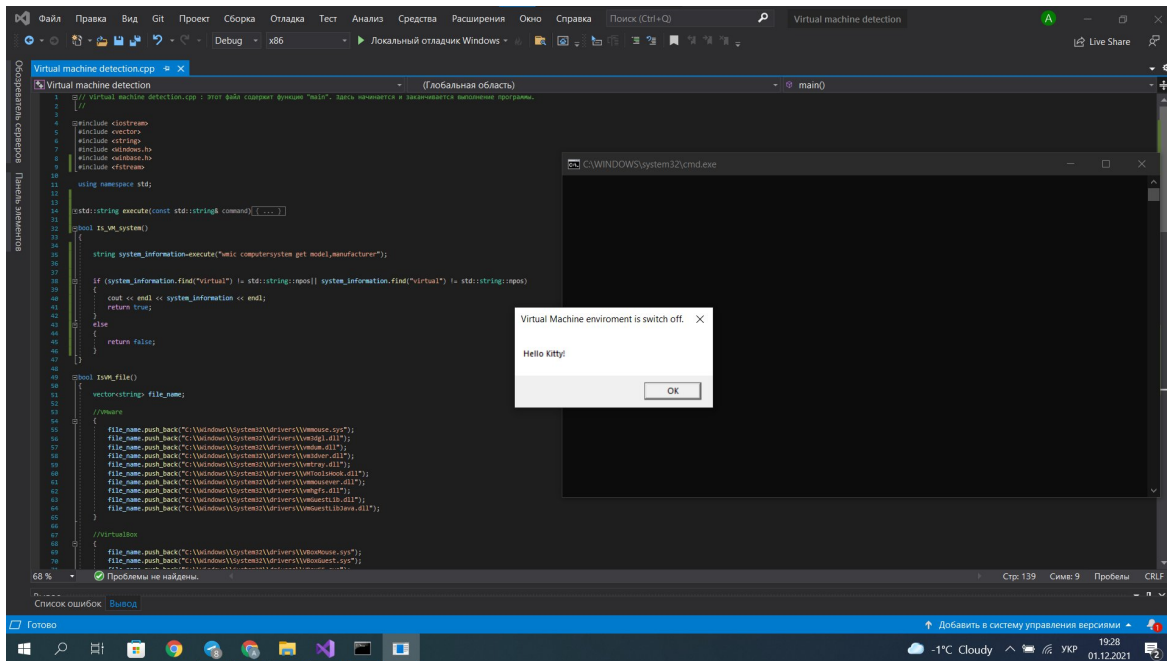
        cin.get();*/

    }

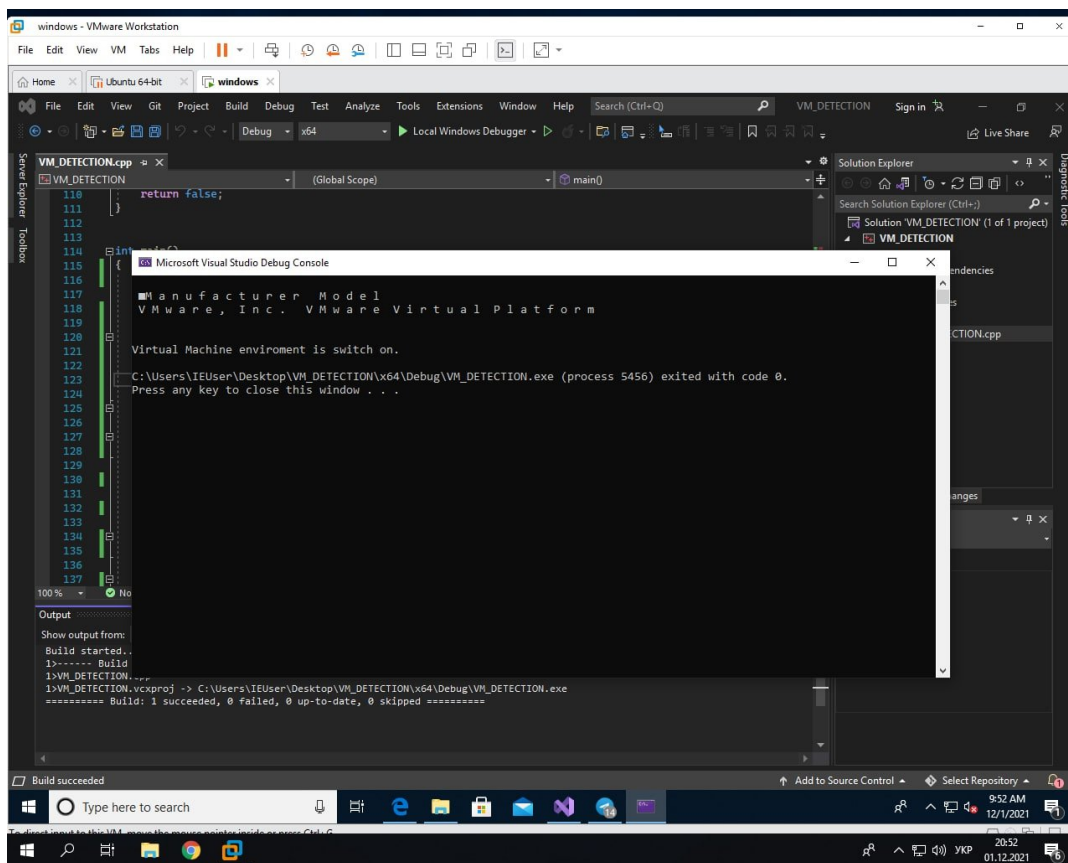
    return 0;
}

```

## Фізична машина



## Віртуальна машина



## Тестування в Cuckoo Sandbox

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package
2515126	01/12/2021 20:22	Virtual machine detection .cpp	-
Done			

Summary

File Virtual machine detection .cpp

Summary

Size: 5.6KB

Type: C++ source, UTF-8 Unicode (with BOM) text, with CRLF line terminators

MDS: d6e7ad9b5ca4b26919701fcb4a99e843

SHA1: 185c955bbaac219e8d6c26d17e4c5440131b0a97

SHA256: ae1d5f8e2e780f4db8a99c0b60e69243099f2c13b6c662800d2660b4f43162

SHA512: [Show SHA512](#)

CRC32: 7CFA8037

ssdeep: 96:3zVkgxSPf00M506EXovK257Aarz1PH1VL2Ve6LmrHwF+UF+Hw:JVpx08ZrIRzFHCw

Yara:

- vmdetect - Possibly employs anti-virtualization techniques
- antivm\_virtualbox - AntiVM checks for VirtualBox
- vmdetect\_misc - Following Rule is referenced from AlienVault's Yara rule repository. This rule contains additional processes and driver names.

Score

This file appears fairly benign with a score of 0.1 out of 10.

Please notice: The scoring system is currently still in development and should be considered an alpha feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
FILE	Dec 1, 2021, 8:22 p.m.	Dec 1, 2021, 8:26 p.m.	229 seconds	Internet	<a href="#">Show Analyzer Log</a> <a href="#">Show Cuckoo Log</a>

Signatures

Yara rules detected for file (3 events)

Screenshots

Name Response Post-Analysis Lookup

No hosts contacted.

IP Address Status Action VT Location

No hosts contacted.

Детектування в Cuckoo Sandbox відсутнє.

Посилання на **report**: <https://cuckoo.cert.ee/analysis/2515126/summary/>