

Abhishek Honmute  
111803055  
Div 1 Batch B2  
Cyber Security  
Assignment 3

## Malware Reverse Engineering And Malware Analysis

**Malware : Dropped:Trojan.Dropper.Agent.VOE**

Link to download malware: [Click here](#)

The image shows a VirusShare analysis page for a file with SHA-256 hash 91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754a0c. The file is named WEXTRACT.EXE, is 420.00 KB in size, and was uploaded on 2021-04-29 13:53:03 UTC. It has a community score of 59/170 and is flagged as malicious by 69 security vendors and 2 sandboxes. The file is categorized as 'executes-dropped-file' and 'peexe'.

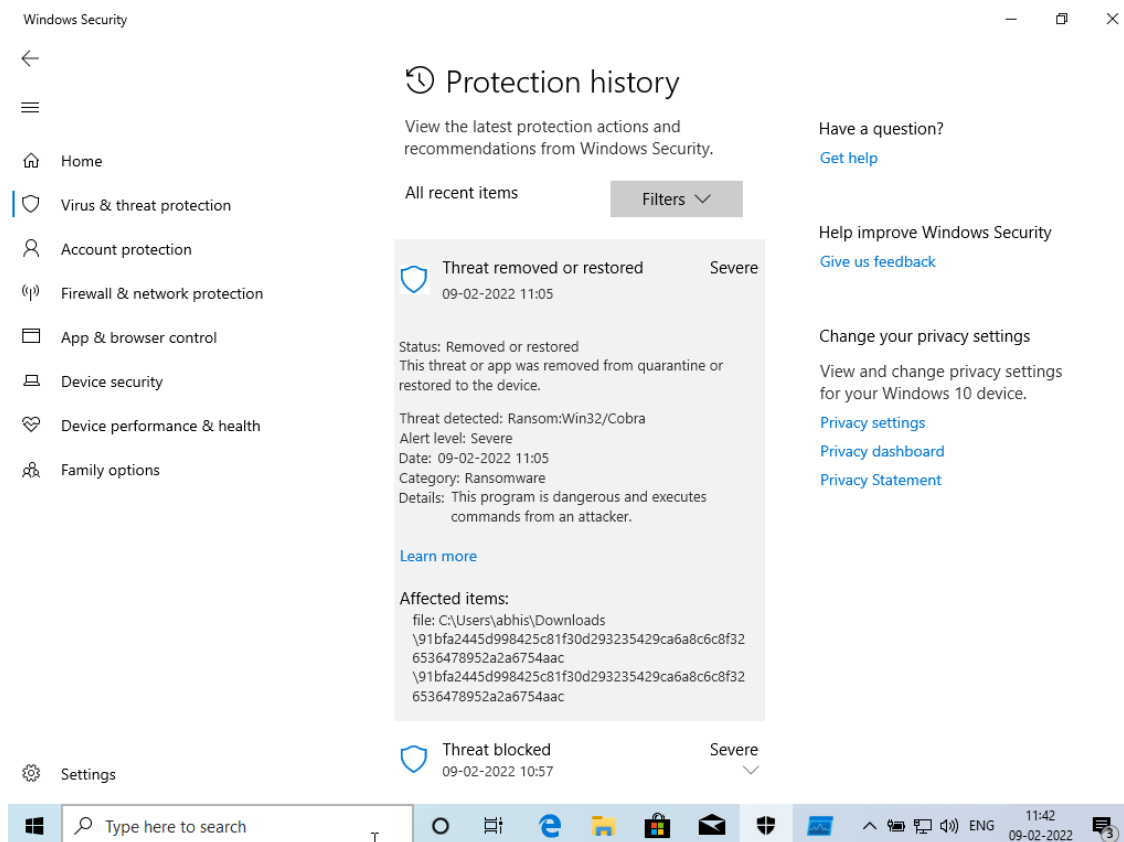
DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	① Dropped:Trojan.Dropper.Agent.VOE	AegisLab	① Trojan.Win32.Generic.I71Z	
AhnLab-V3	① Trojan/Win32.Moseran.C1294902	Alibaba	① Trojan/Win32/Yakes.cc069b2f	
ALYac	① Dropped:Trojan.Dropper.Agent.VOE	Avast	① Win32:Malware-gen	
AVG	① Win32:Malware-gen	Avira (no cloud)	① TR/Injector.juol	
BitDefender	① Dropped:Trojan.Dropper.Agent.VOE	BitDefender Theta	① AI:Packers.FBEDFA5623	
CAT-QuickHeal	① Trojan.Generic	ClamAV	① Win.Malware.Yakes-6895521-0	
Comodo	① Malware/@#3mzsbgcd97m1q	CrowdStrike Falcon	① Win/malicious_confidence_100% (W)	

This malware is a subset of the "Agent" family, which groups together a wide variety of malware that do not fit into any other known families. The Agent family includes trojans, worms, viruses, backdoors and other types of malicious programs.

A Trojan dropper, or simply a dropper, is a malicious program designed to deliver other malware to a victim's computer or phone. Droppers are most frequently Trojan programs that appear to be or include an application that is valuable to the user.

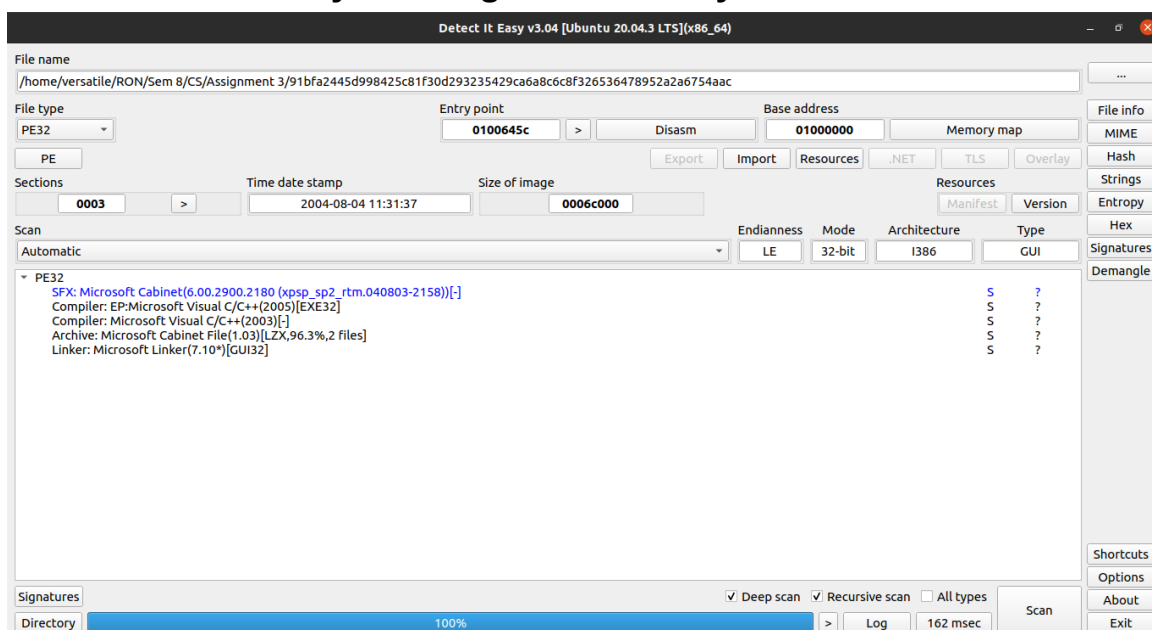
## Adding Malware in a windows machine:

Download malware file from given link. Unzip the folder using password "infected". Windows defender immediately detected the file as malware.



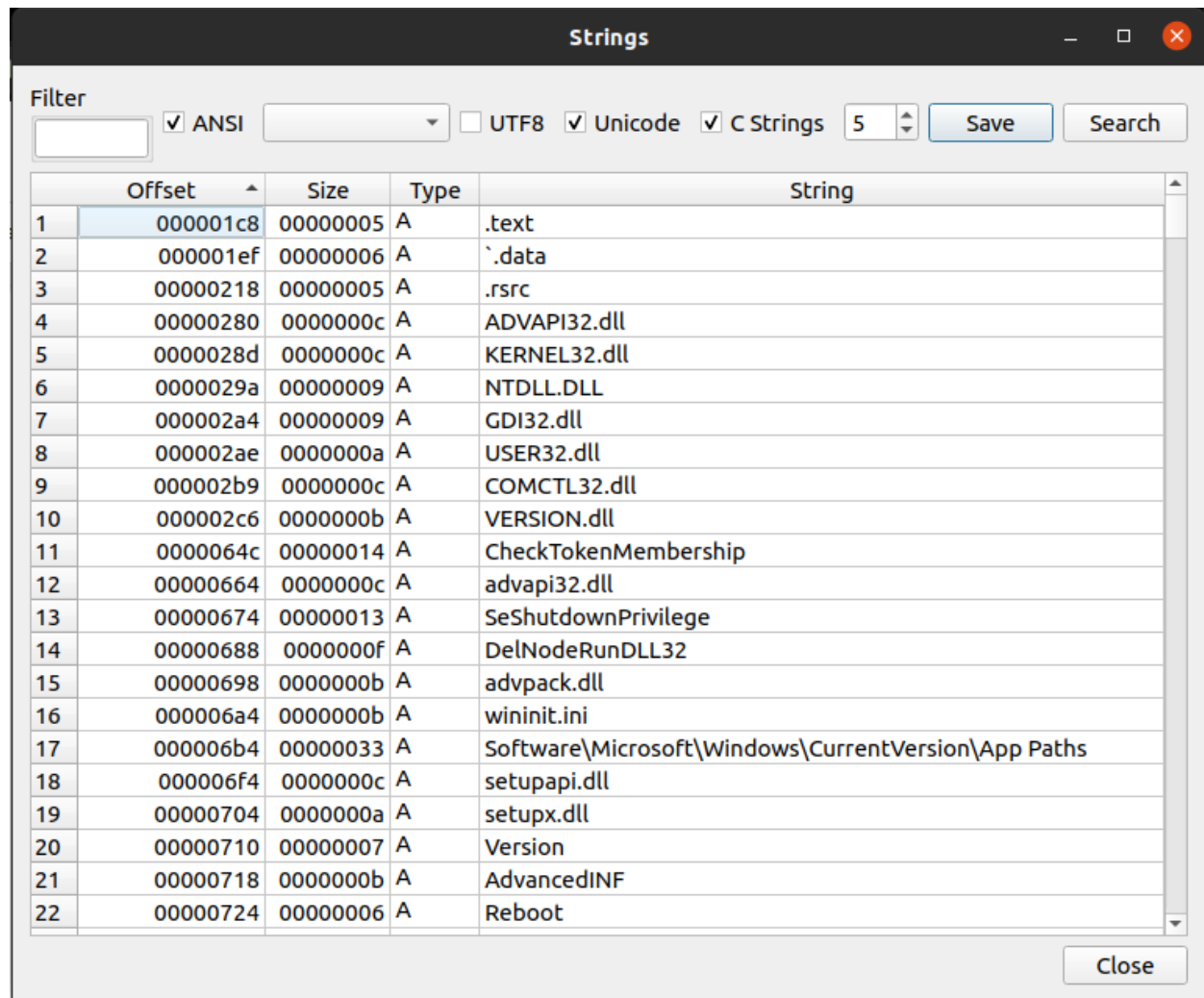
Give access to malware to study it further.

## Static Malware Analysis using Detect it easy:



File type of given malware is PE32 executable file.

To examine the malware we can extract strings from the binary malware file.



	Offset	Size	Type	String
1	000001c8	00000005	A	.text
2	000001ef	00000006	A	`.data
3	00000218	00000005	A	.rsrc
4	00000280	0000000c	A	ADVAPI32.dll
5	0000028d	0000000c	A	KERNEL32.dll
6	0000029a	00000009	A	NTDLL.DLL
7	000002a4	00000009	A	GDI32.dll
8	000002ae	0000000a	A	USER32.dll
9	000002b9	0000000c	A	COMCTL32.dll
10	000002c6	0000000b	A	VERSION.dll
11	0000064c	00000014	A	CheckTokenMembership
12	00000664	0000000c	A	advapi32.dll
13	00000674	00000013	A	SeShutdownPrivilege
14	00000688	0000000f	A	DelNodeRunDLL32
15	00000698	0000000b	A	advpack.dll
16	000006a4	0000000b	A	wininit.ini
17	000006b4	00000033	A	Software\Microsoft\Windows\CurrentVersion\App Paths
18	000006f4	0000000c	A	setupapi.dll
19	00000704	0000000a	A	setupx.dll
20	00000710	00000007	A	Version
21	00000718	0000000b	A	AdvancedINF
22	00000724	00000006	A	Reboot

After extracting the strings we can observe all the used libraries and system calls used by the malware. From observation we can see that malware is using some of the kernel libraries and doing some suspicious activities.

4	00000280	0000000c	A	ADVAPI32.dll
5	0000028d	0000000c	A	KERNEL32.dll
6	0000029a	00000009	A	NTDLL.DLL
7	000002a4	00000009	A	GDI32.dll
8	000002ae	0000000a	A	USER32.dll
9	000002b9	0000000c	A	COMCTL32.dll
10	000002c6	0000000b	A	VERSION.dll

99	000096d2	0000000d	A	FindNextFileA
100	000096e2	0000000b	A	DeleteFileA
101	000096f0	00000012	A	SetFileAttributesA
119	00009826	0000000b	A	CreateFileA
120	00009834	0000000e	A	LoadLibraryExA
121	00009846	00000009	A	lstrcpynA
122	00009852	00000015	A	GetVolumeInformationA
123	0000986a	0000000e	A	FormatMessageA
124	0000987c	00000014	A	GetCurrentDirectoryA
298	000143ae	0000005b	U	8Unable to retrieve operating system version information.!...
299	00014468	00000024	U	#Unable to create extraction thread.
300	0001454c	00000100	U	Setup could not find a drive with %s KB free disk space to ...
301	0001474e	000000c3	U	der with fully qualified pathname or choose Cancel.!Could no...
302	00014d3e	0000001e	U	Do you still want to continue?
303	00014d80	00000020	U	□Error retrieving Windows folder
304	00014dc8	00000100	U	\$NT Shutdown: OpenProcessToken error.)NT Shutdown: ...
305	00015044	000000f2	U	System message: %s.xSetup could not find a drive with %s KB...
306	0001550c	00000029	U	Do you want to restart your computer now?
307	00015560	00000083	U	eAnother copy of the '%s' package is already running on your...
308	0001568c	00000093	U	You do not have administrator privileges on this machine. So...

## Some important information from VirusTotal scan:

### Behavior Tags ⓘ

executes-dropped-file

### Network Communication ⓘ

#### DNS Resolutions

- + qualitytrade12.hopto.org
- + dns.msftncsi.com

#### Files Dropped

- + %LOCALAPPDATA%\csidl\_
- + %LOCALAPPDATA%\csidl\_x
- + %TEMP%\ixp000.tmp\1.xy\_
- + %TEMP%\ixp000.tmp\1.xyz
- + %APPDATA%\install\excel.ex\_
- + %APPDATA%\install\excel.exe
- + %APPDATA%\microsoft\windows\start menu\programs\startup\lx.vbs

### File System Actions ⓘ

#### Files Opened

<SYSTEM32>\ntdll.dll  
 %WINDIR%\syswow64\ntdll.dll  
 %TEMP%\ixp000.tmp\1.xy\_  
 %TEMP%\ixp000.tmp\1.xyz  
 %WINDIR%\syswow64\cmd.exe  
 %LOCALAPPDATA%\csidl\_x  
 %APPDATA%\install\excel.exe  
 %LOCALAPPDATA%\csidl\_  
 %WINDIR%\syswow64\net.exe  
 %WINDIR%\syswow64\net1.exe

### Files Deleted

%TEMP%\ixp000.tmp\1.xy\_  
 %TEMP%\ixp000.tmp\1.xyz  
 %LOCALAPPDATA%\csidl\_x

### Files With Modified Attributes

%TEMP%\ixp000.tmp\1.xyz  
 %TEMP%\ixp000.tmp\1.xy\_  
 %LOCALAPPDATA%\csidl\_  
 %LOCALAPPDATA%\csidl\_x  
 %APPDATA%\install\excel.ex\_  
 %APPDATA%\install\excel.exe

## Registry Actions ⓘ

### Registry Keys Opened

<HKLM>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce  
<HKCU>\software\Local AppWizard-Generated Applications  
<HKCU>\software\Local AppWizard-Generated Applications\????  
<HKCU>\software\Local AppWizard-Generated Applications\????\Recent File List  
<HKCU>\software\Local AppWizard-Generated Applications\????\Settings

### Registry Keys Deleted

<HKLM>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\wextract\_cleanup0

## Process And Service Actions ⓘ

### Processes Created

<PATH\_SAMPLE.EXE>  
%TEMP%\ixp000.tmp\1.xyz  
%WINDIR%\syswow64\cmd.exe  
<SYSTEM32>\conhost.exe  
%APPDATA%\install\excel.exe  
%WINDIR%\syswow64\net.exe  
%WINDIR%\syswow64\net1.exe

### Processes Injected

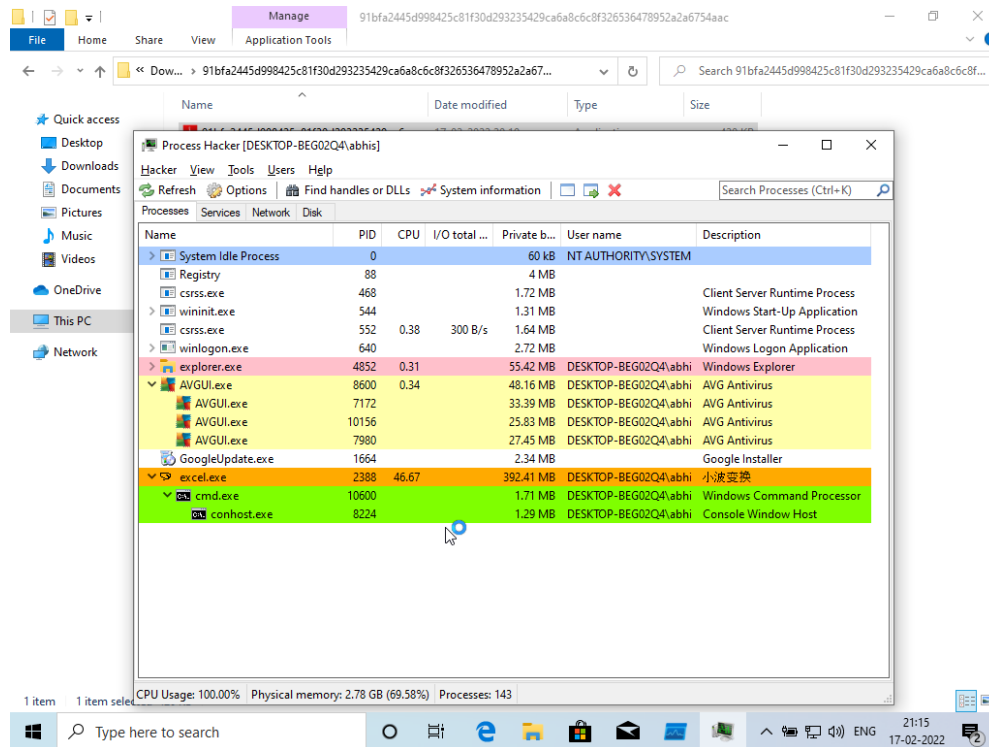
%TEMP%\ixp000.tmp\1.xyz  
%APPDATA%\install\excel.exe

### Processes Terminated

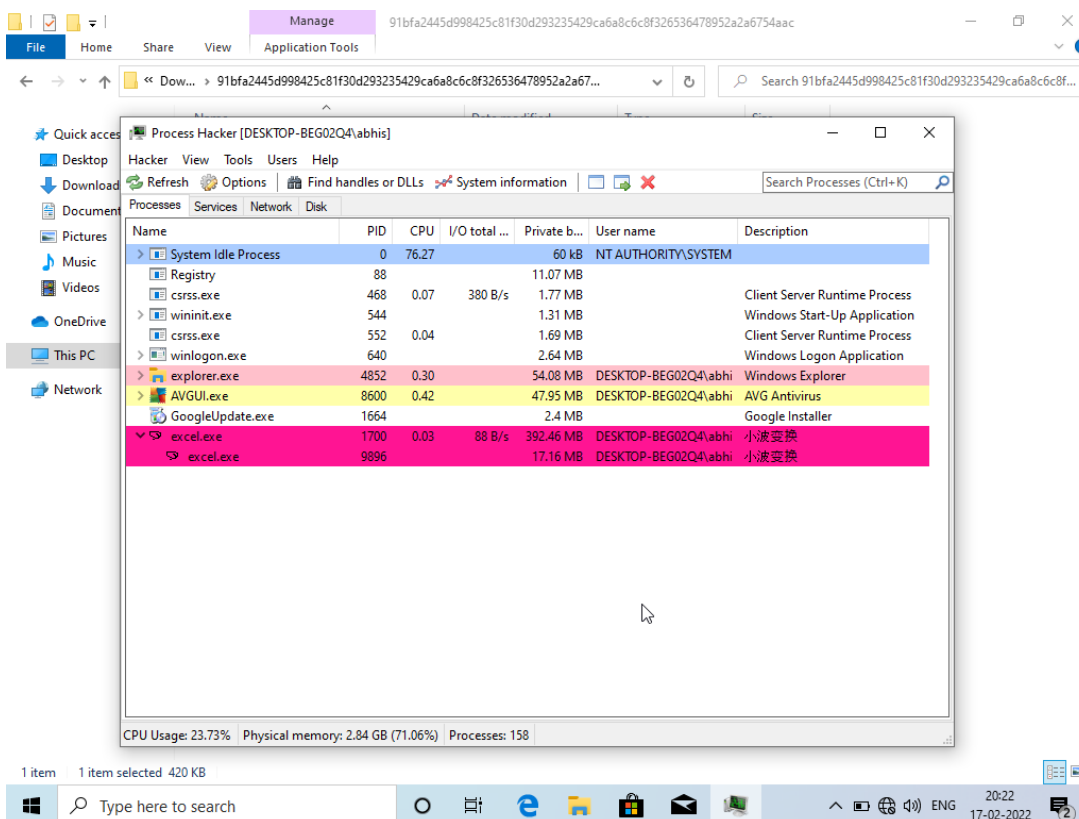
%TEMP%\ixp000.tmp\1.xyz  
%WINDIR%\syswow64\net1.exe  
%WINDIR%\syswow64\net.exe  
%WINDIR%\syswow64\cmd.exe  
<PATH\_SAMPLE.EXE>

# Dynamic Malware Analysis using Process Monitor:

1. On starting the malware, it opened the cmd.exe and ran the conhost.exe application.

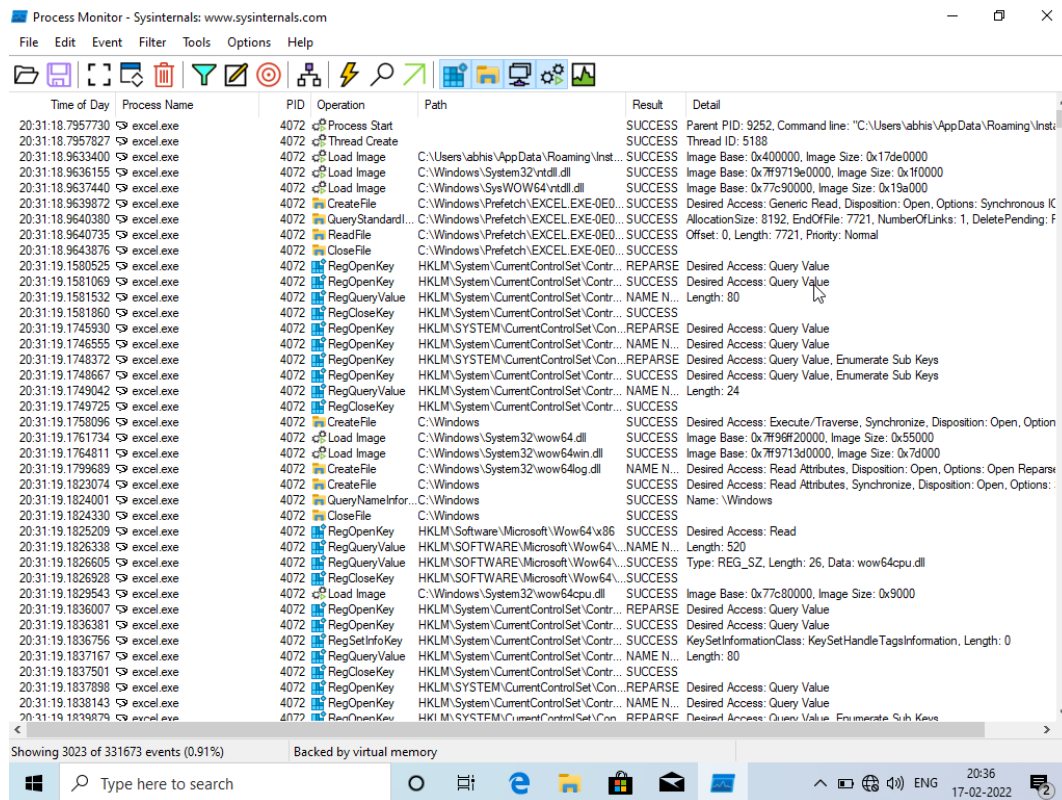


2. Then the process hacker classified it as a dangerous process by giving it a reddish color.

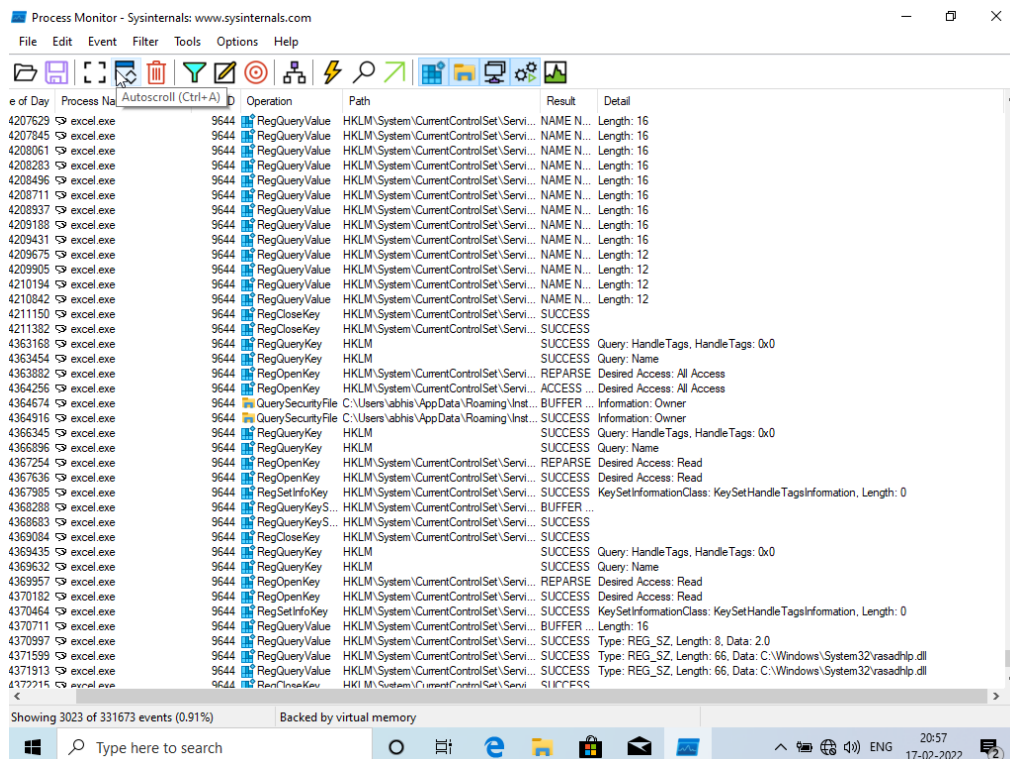




3. After some time, the excel.exe process started playing with lots of registry keys. Malware was modified to make sure it can launch itself after a reboot, to better hide, or to integrate with an existing legitimate process.

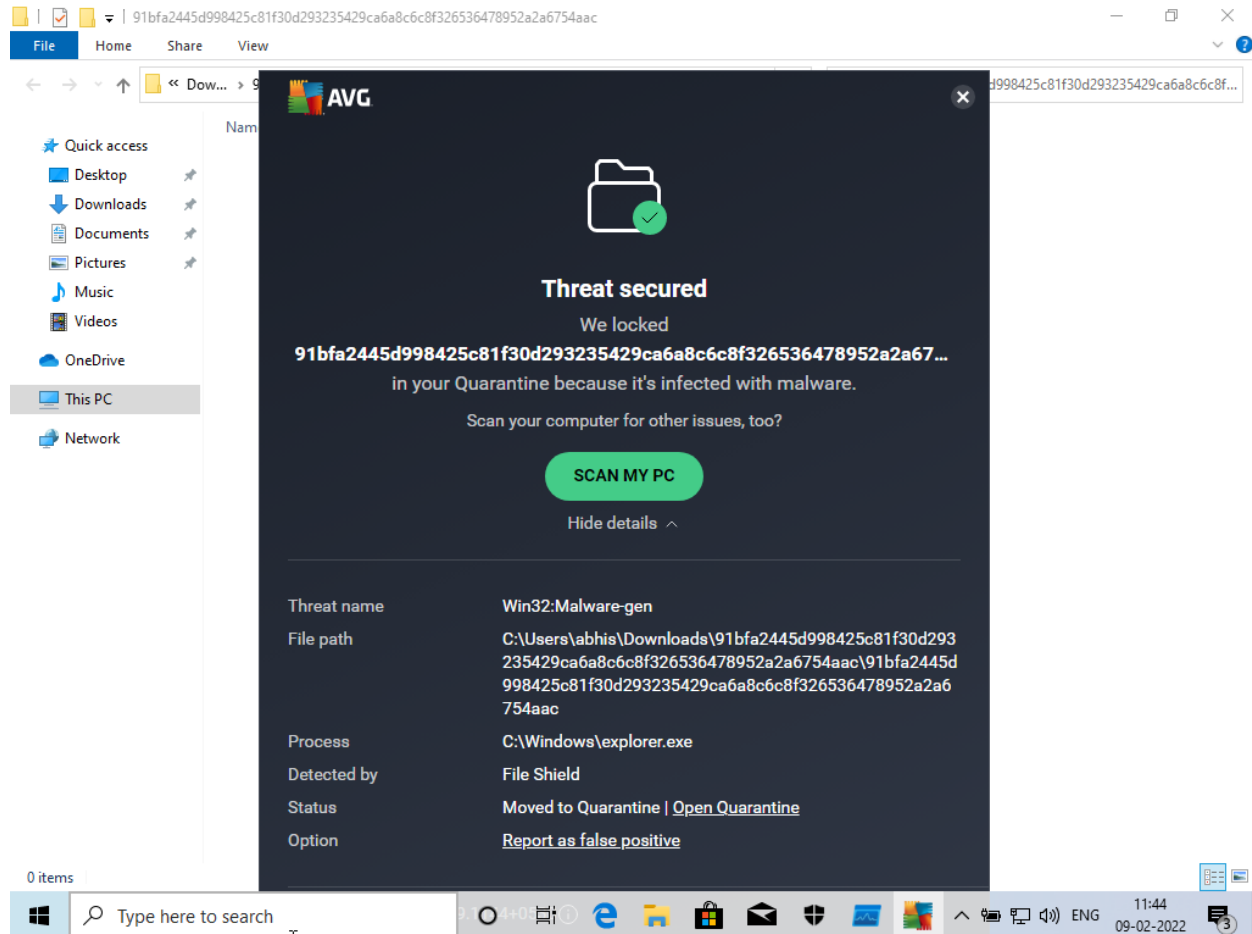


4. It was observed that malware was acquiring all the access from modifying the registry.



## Using AVG antivirus software to remove the malware:

AVG antivirus software detected the malware successfully and transferred the file to quarantine to make the computer safe.



SubInACL from Microsoft's Website can be used to repair the registry entries.

## Conclusion:

1. I installed the malware on the Windows machine.
2. Then I applied some Static Malware reverse engineering techniques to analyze the malware using the Detect It Easy tool.
3. Then I performed Dynamic Malware reverse engineering techniques to monitor the malware process using process monitor like tools.
4. I proved that Dropped:Trojan.Dropper.Agent.VOE is using some system level libraries and doing some suspicious work.
5. Then I used AVG antivirus software to detect and remove the malware file successfully.