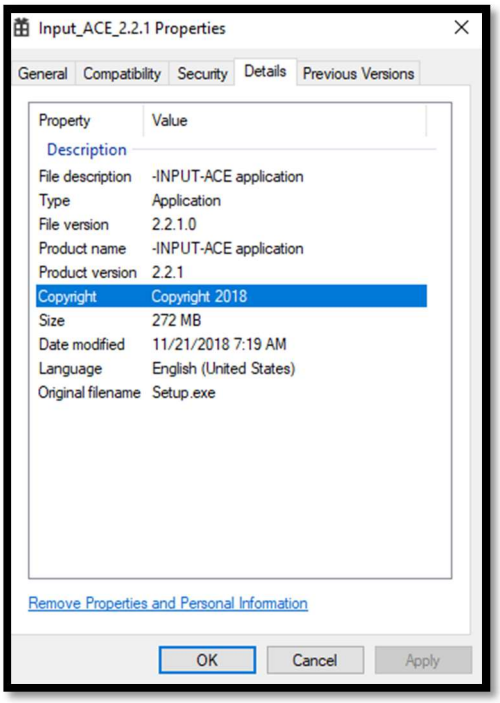
-INPUT-ACE Version 2.2.1

February 4th, 2019.

Description: This is an assessment of the –INPUT-ACE version 2.2.1. An evaluation of this software found vulnerabilities related to a possible buffer overflow[1] and denial-of-service (DoS) using a User Datagram Protocol (UDP) flood attack[2]. The main components verified include a dynamic link library (urlmon.dll) and an executable file (AviSynth_260.exe).

1. File identification:



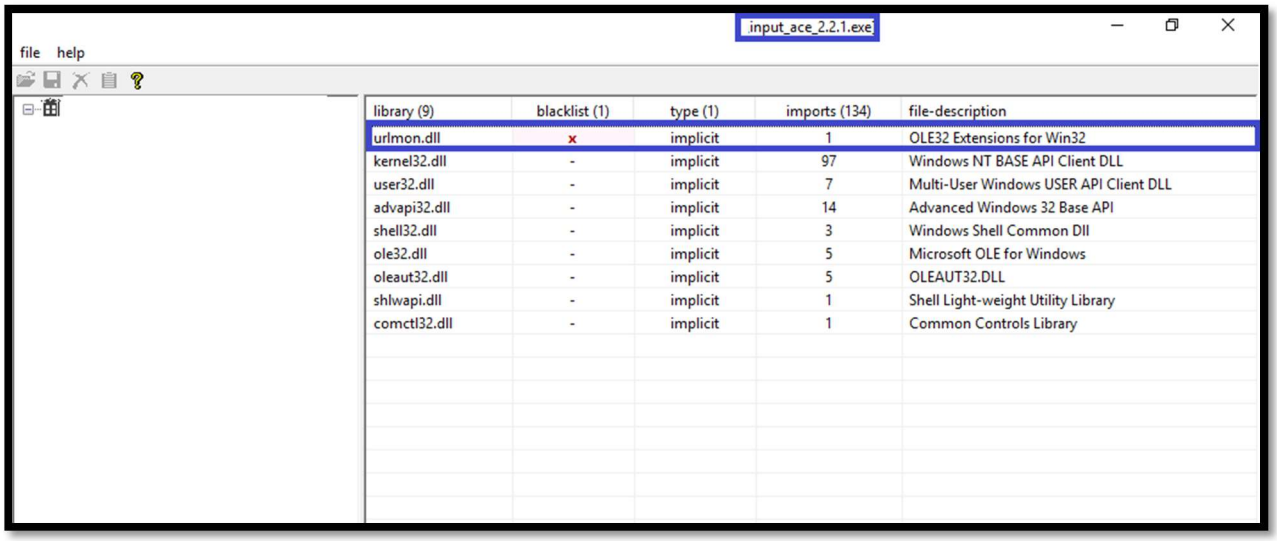
[1] https://security.radware.com/ddos-knowledge-center/ddospedia/buffer-overflow-attack/
[2] https://en.wikipedia.org/wiki/UDP_flood_attack

property	value
md5	103C00A3979359D321798AF5E8BFFD2B
sha1	FD6DE2777A6CD034D3A9131A2D56F27822D97054
sha256	A948054E81FB45B3694E5668BCEC783535203091700265A1AF8ACBADCEC0C3E8
file-type	**executable**
date	empty
language	English United States
code-page	Unicode UTF-16, little endian
FileDescription	-INPUT-ACE application
FileVersion	2.2.1
InternalName	Setup.exe
LegalCopyright	Copyright 2018
OriginalFilename	Setup.exe
ProductName	-INPUT-ACE application
ProductVersion	2.2.1
SquirrelAwareVersion	n/a
CompanyName	Occam Video Solutions

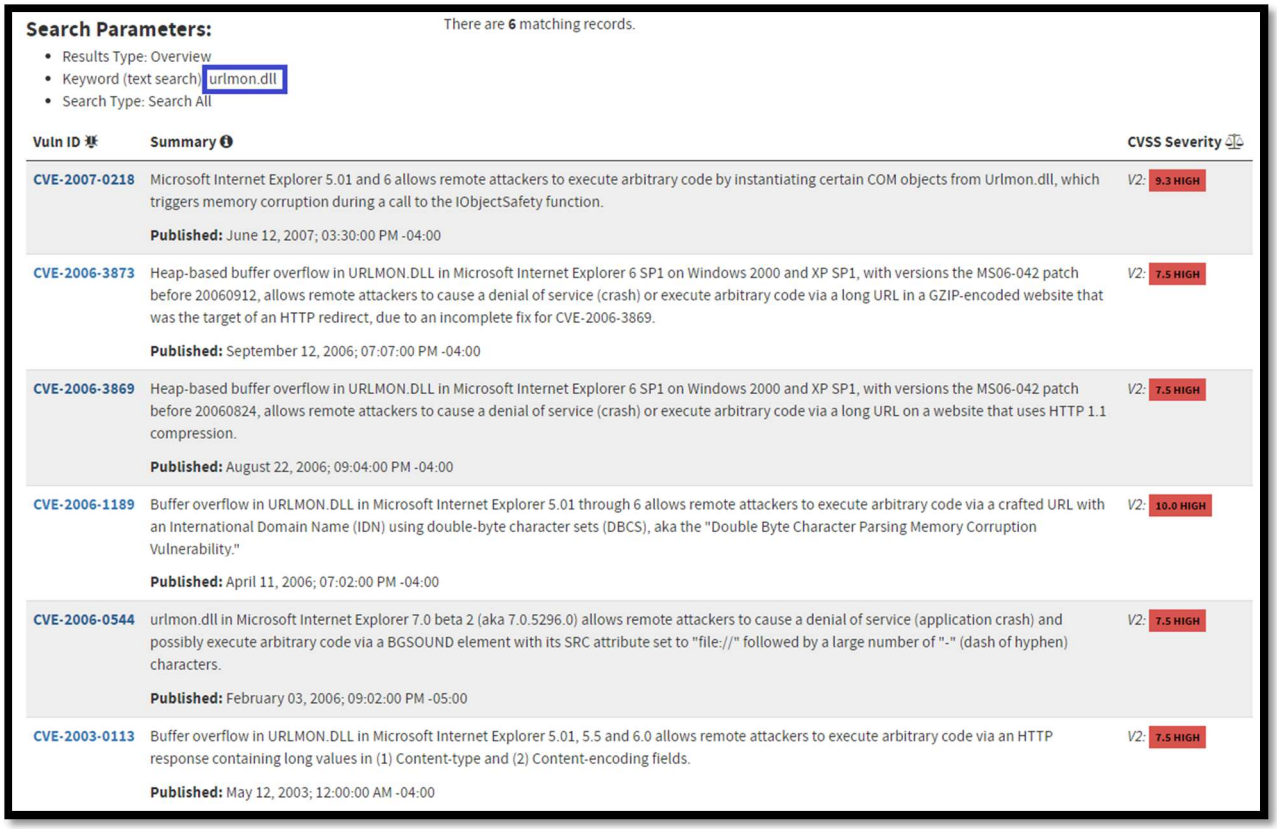
2. General security indicators:

The dos-stub message is missing
The size of the resource (DATA.131) is bigger than the max (512000 bytes) threshold
The size of the resource (DATA.131) is bigger than the max (512000 bytes) threshold
The file contains another file (type: PKZIP, location: resources, file-offset: 0x0002B310)
The file references (1) blacklisted library
The file references (1) Windows built-in privilege(s)
The size (285944320 bytes) of the file is suspicious
The online scoring service is not reachable
The signature of the resource (FLAGS:132) is unknown
The file-ratio (99%) of the resources is suspicious
The file imports (5) anonymous function(s)
The file imports (34) blacklisted function(s)
The file opts for Data Execution Prevention (DEP)
The file references a debug symbols file (path:"c:\users\paulb\code\squirrel\squirrel.windows\src\setup\bin\release\setup.pdb")
The file signature is 'Microsoft Visual C++ 8'
The file references (4) blacklisted string(s)
The file opts for Address Space Layout Randomization (ASLR)
The file opts for cookies on the stack (GS)
The file does not contain a digital Certificate
The file ignores Code Integrity

3. A suspicious urlmon.dll[3] was identified.



library (9)	blacklist (1)	type (1)	imports (134)	file-description
urlmon.dll	x	implicit	1	OLE32 Extensions for Win32
kernel32.dll	-	implicit	97	Windows NT BASE API Client DLL
user32.dll	-	implicit	7	Multi-User Windows USER API Client DLL
advapi32.dll	-	implicit	14	Advanced Windows 32 Base API
shell32.dll	-	implicit	3	Windows Shell Common Dll
ole32.dll	-	implicit	5	Microsoft OLE for Windows
oleaut32.dll	-	implicit	5	OLEAUT32.DLL
shlwapi.dll	-	implicit	1	Shell Light-weight Utility Library
comctl32.dll	-	implicit	1	Common Controls Library



Search Parameters:

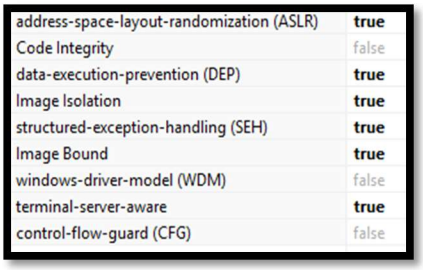
There are **6** matching records.

- Results Type: Overview
- Keyword (text search): urlmon.dll
- Search Type: Search All

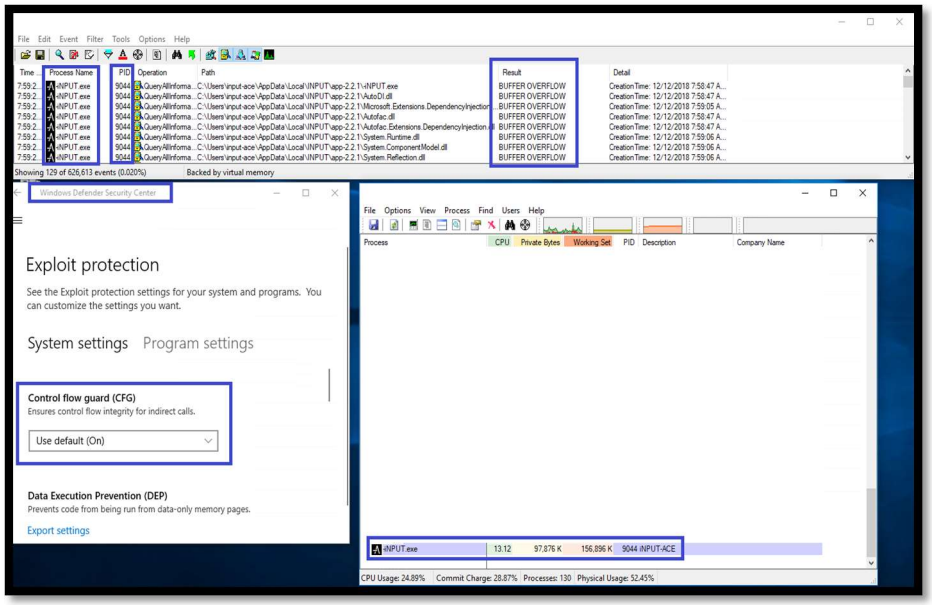
Vuln ID	Summary	CVSS Severity
CVE-2007-0218	Microsoft Internet Explorer 5.01 and 6 allows remote attackers to execute arbitrary code by instantiating certain COM objects from Urlmon.dll, which triggers memory corruption during a call to the IObjectSafety function. **Published:** June 12, 2007; 03:30:00 PM -04:00	V2: 9.3 HIGH
CVE-2006-3873	Heap-based buffer overflow in URLMON.DLL in Microsoft Internet Explorer 6 SP1 on Windows 2000 and XP SP1, with versions the MS06-042 patch before 20060912, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URL in a GZIP-encoded website that was the target of an HTTP redirect, due to an incomplete fix for CVE-2006-3869. **Published:** September 12, 2006; 07:07:00 PM -04:00	V2: 7.5 HIGH
CVE-2006-3869	Heap-based buffer overflow in URLMON.DLL in Microsoft Internet Explorer 6 SP1 on Windows 2000 and XP SP1, with versions the MS06-042 patch before 20060824, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long URL on a website that uses HTTP 1.1 compression. **Published:** August 22, 2006; 09:04:00 PM -04:00	V2: 7.5 HIGH
CVE-2006-1189	Buffer overflow in URLMON.DLL in Microsoft Internet Explorer 5.01 through 6 allows remote attackers to execute arbitrary code via a crafted URL with an International Domain Name (IDN) using double-byte character sets (DBCS), aka the "Double Byte Character Parsing Memory Corruption Vulnerability." **Published:** April 11, 2006; 07:02:00 PM -04:00	V2: 10.0 HIGH
CVE-2006-0544	urlmon.dll in Microsoft Internet Explorer 7.0 beta 2 (aka 7.0.5296.0) allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a BGSOUND element with its SRC attribute set to "file://" followed by a large number of "-" (dash of hyphen) characters. **Published:** February 03, 2006; 09:02:00 PM -05:00	V2: 7.5 HIGH
CVE-2003-0113	Buffer overflow in URLMON.DLL in Microsoft Internet Explorer 5.01, 5.5 and 6.0 allows remote attackers to execute arbitrary code via an HTTP response containing long values in (1) Content-type and (2) Content-encoding fields. **Published:** May 12, 2003; 12:00:00 AM -04:00	V2: 7.5 HIGH

[3] https://www.kb.cert.org/vuls/id/169753/

3.1 Headers shows that the ASLR[4] and DEP[5] are enabled, however the CFG is disabled[6].



Events of buffer overflow were observed even with the CFG enabled.



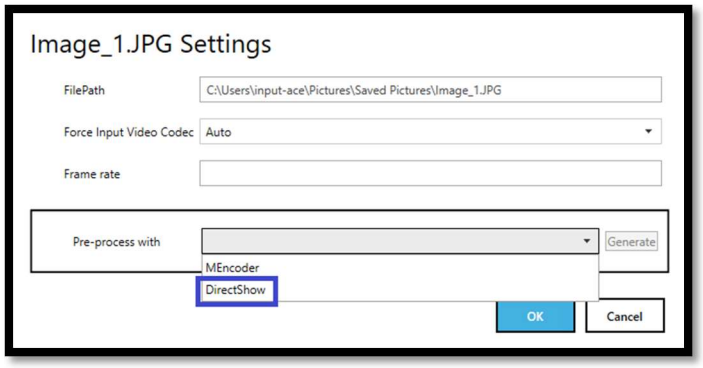
[4] https://en.wikipedia.org/wiki/Address_space_layout_randomization

[5] https://support.microsoft.com/en-ca/help/875352/a-detailed-description-of-the-data-execution-prevention-dep-feature-in

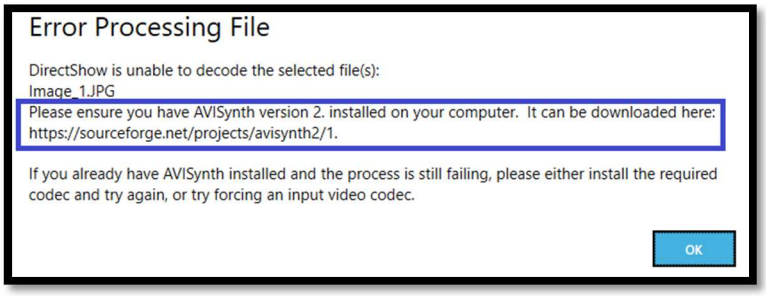
[6] https://docs.microsoft.com/en-us/windows/desktop/secbp/control-flow-guard

4. In addition, the software installation relies in the use of other components (DirectShow) in which users are suggested to install AVISynth[7].

   One of the process in editing and documenting the workflow requires the use of DirectShow.

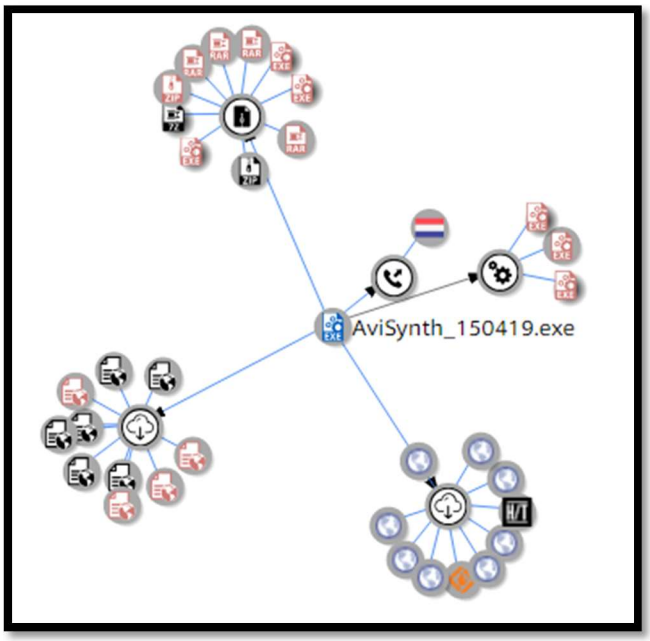


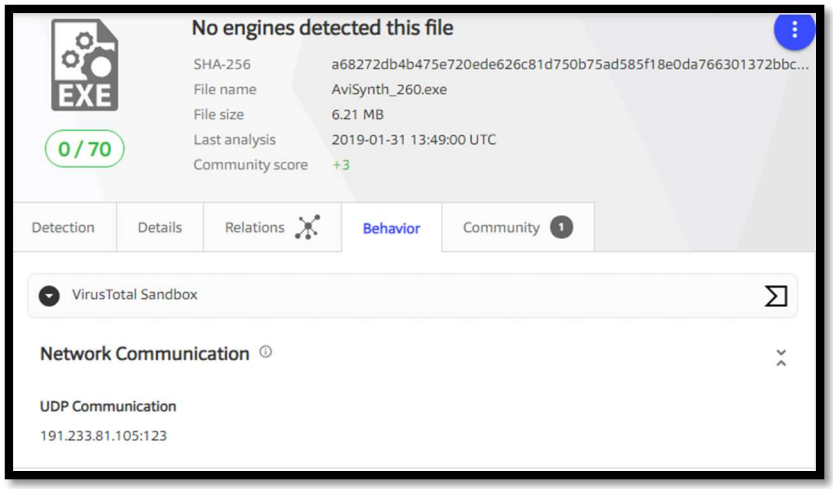
   And once the DirectShow is not installed an error message followed by the source to proceed this installation is provided:

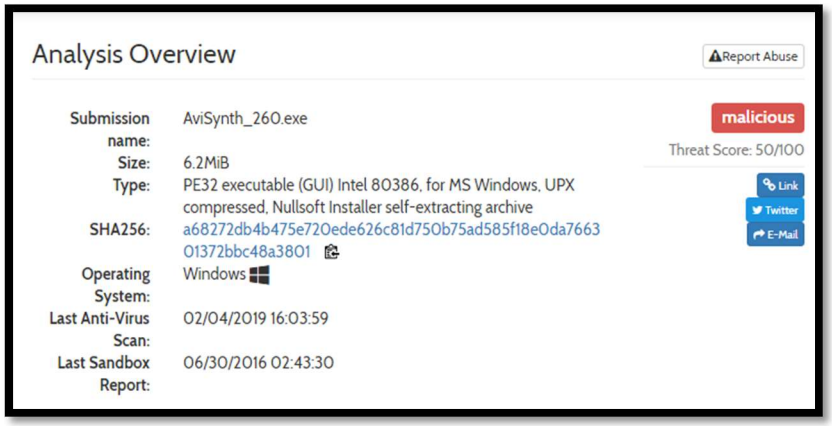


5. The user may decide if they want to install this component or not, but eventually this could impact some functionalities of the software. Unfortunately this component[8] could open access to several suspicious files using an UDP port[9]:

[7] https://sourceforge.net/projects/avisynth2/files/latest/download
[8] https://www.hybrid-analysis.com/sample/a68272db4b475e720ede626c81d750b75ad585f18e0da766301372bbc48a3801/562e93de0e316d875b8720a3
[9] https://www.virustotal.com/#/file/a68272db4b475e720ede626c81d750b75ad585f18e0da766301372bbc48a3801/behavior

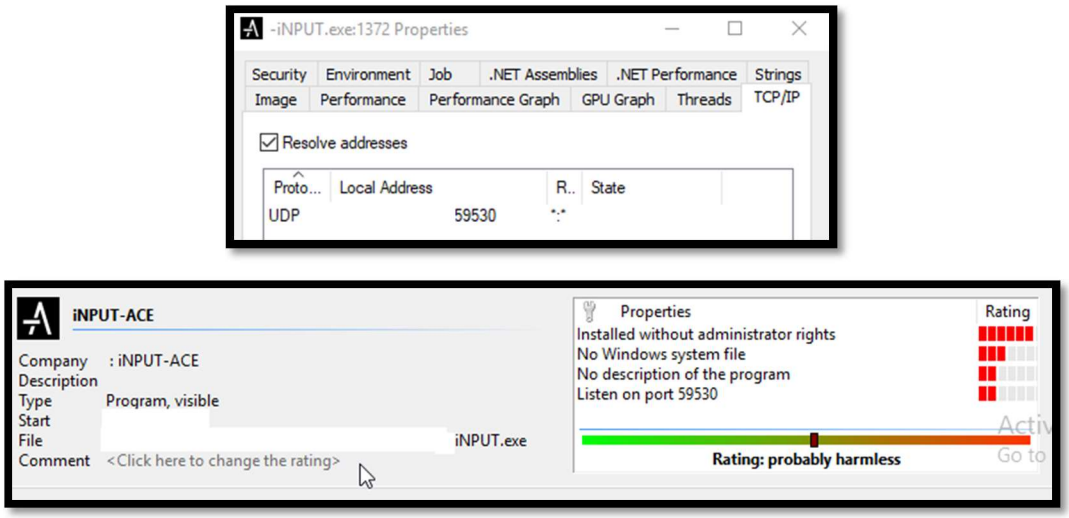

AviSynth_150419.exe


No engines detected this file
SHA-256 a68272db4b475e720ede626c81d750b75ad585f18e0da766301372bbc...
File name AviSynth_260.exe
File size 6.21 MB
Last analysis 2019-01-31 13:49:00 UTC
Community score +3
0 / 70
Detection
Details
Relations
Behavior
Community 1
VirusTotal Sandbox
Network Communication
UDP Communication
191.233.81.105:123


Analysis Overview
Report Abuse
Submission name: AviSynth_260.exe
Size: 6.2MiB
Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed, Nullsoft Installer self-extracting archive
SHA256: a68272db4b475e720ede626c81d750b75ad585f18e0da766301372bbc48a3801
Operating System: Windows
Last Anti-Virus Scan: 02/04/2019 16:03:59
Last Sandbox Report: 06/30/2016 02:43:30
malicious
Threat Score: 50/100
Link
Twitter
E-Mail

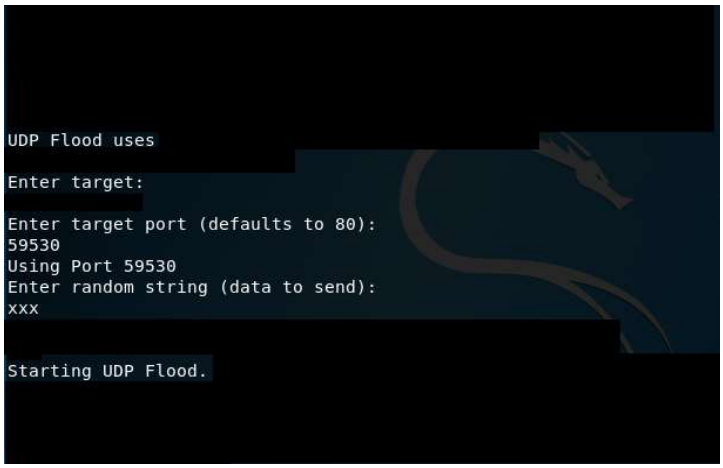
6. UDP Flood Attack

6.1 The software relies in the use of an UDP port:

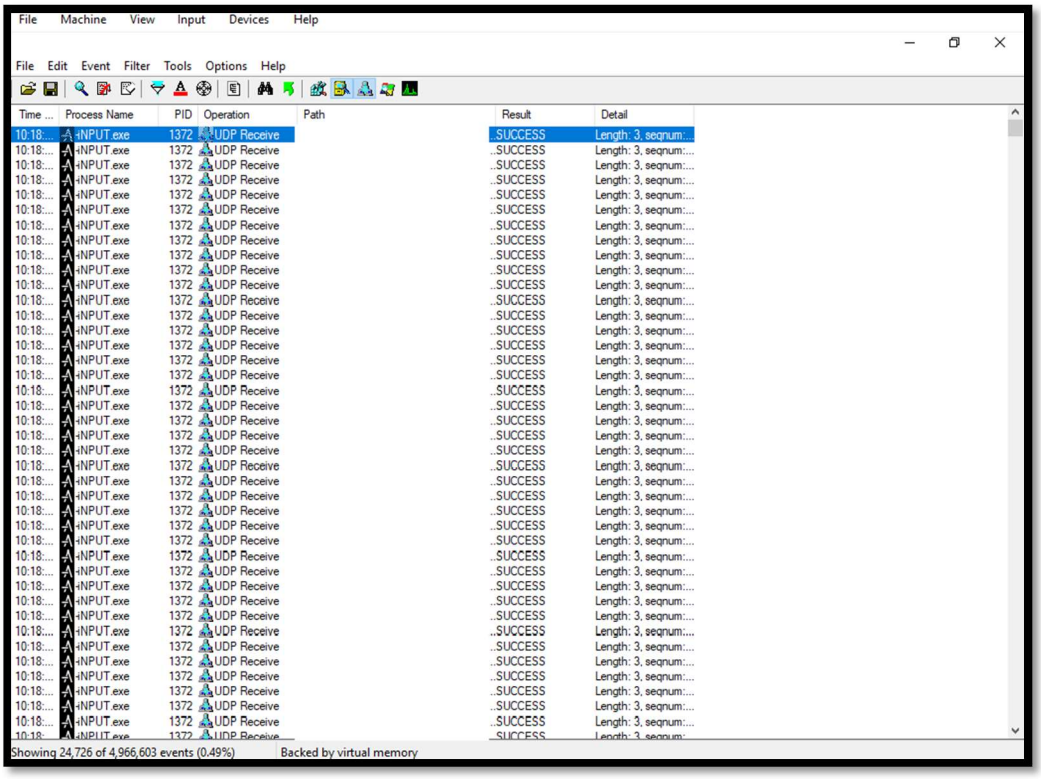


6.2 The port has an open status:

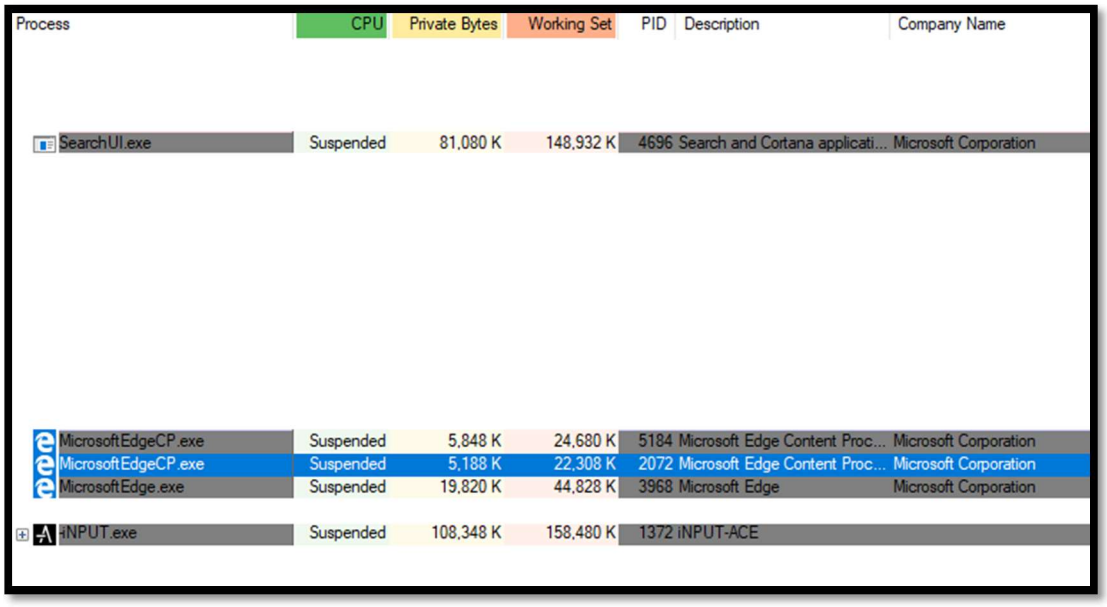
6.3 Then it is possible to send packages to this port:



6.4 Confirm the flood in the victim machine



6.5 To finally, suspend the software process and others (e.g. Microsoft Edge) under execution in the victim machine.



6.6 There is the possibility also to replicate the attack over a Transmission Control Protocol (TCP) as well by using the Remote Address and Remote Port information.