ID: 568663
Sample Name: snd.exe
Cookbook: default.jbs
Time: 17:23:19
Date: 08/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

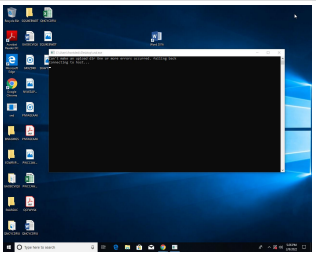
Windows Analysis Report

snd.exe

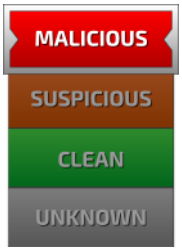
Overview

General Information

Sample Name:	snd.exe
Analysis ID:	568663
MD5:	0a76e0e59456d3.
SHA1:	1b6df9f456fbb2f…
SHA256:	886cb22ffe43a38..
Infos:	



Detection

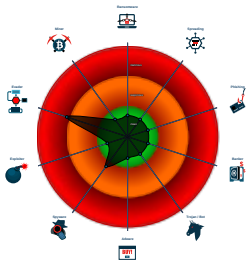


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Found potential dummy code loops …
- Machine Learning detection for sam…
- Uses 32bit PE files
- Found a high number of Window / U…
- Queries the volume information (nam…
- Yara signature match
- Sample file is different than original …
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Sample execution stops while proce…

Classification



Process Tree

- **System is w10x64**
- snd.exe (PID: 5692 cmdline: "C:\Users\user\Desktop\snd.exe" MD5: 0A76E0E59456D310419266270C410936)
  - conhost.exe (PID: 5516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
snd.exe	MALWARE_Win_ExMatter	Detects BlackMatter data exfiltration tool	ditekSHen	0xf63a1:$s1: Renci.SshNet. 0xf6ce2:$s1: Renci.SshNet. 0xf6da5:$s1: Renci.SshNet. 0xf6e2b:$s1: Renci.SshNet. 0xf7b60:$s1: Renci.SshNet. 0xf7ba6:$s1: Renci.SshNet. 0xf7bf6:$s1: Renci.SshNet. 0xf7e44:$s1: Renci.SshNet. 0xf8298:$s1: Renci.SshNet. 0xf82c0:$s1: Renci.SshNet. 0xf83bd:$s1: Renci.SshNet. 0xfb414:$s1: Renci.SshNet. 0xfb437:$s1: Renci.SshNet. 0xfb605:$s1: Renci.SshNet. 0xfb97f:$s1: Renci.SshNet. 0xfb9a8:$s1: Renci.SshNet. 0xfb9db:$s1: Renci.SshNet. 0xfba06:$s1: Renci.SshNet. 0xfba35:$s1: Renci.SshNet. 0xfba67:$s1: Renci.SshNet. 0xfba89:$s1: Renci.SshNet.

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.snd.exe.d30000.0.unpack	MALWARE_Win_ExMatter	Detects BlackMatter data exfiltration tool	ditekSHen	0xf63a1:$s1: Renci.SshNet. 0xf6ce2:$s1: Renci.SshNet. 0xf6da5:$s1: Renci.SshNet. 0xf6e2b:$s1: Renci.SshNet. 0xf7b60:$s1: Renci.SshNet. 0xf7ba6:$s1: Renci.SshNet. 0xf7bf6:$s1: Renci.SshNet. 0xf7e44:$s1: Renci.SshNet. 0xf8298:$s1: Renci.SshNet. 0xf82c0:$s1: Renci.SshNet. 0xf83bd:$s1: Renci.SshNet. 0xfb414:$s1: Renci.SshNet. 0xfb437:$s1: Renci.SshNet. 0xfb605:$s1: Renci.SshNet. 0xfb97f:$s1: Renci.SshNet. 0xfb9a8:$s1: Renci.SshNet. 0xfb9db:$s1: Renci.SshNet. 0xfba06:$s1: Renci.SshNet. 0xfba35:$s1: Renci.SshNet. 0xfba67:$s1: Renci.SshNet. 0xfba89:$s1: Renci.SshNet.
0.0.snd.exe.d30000.0.unpack	MALWARE_Win_ExMatter	Detects BlackMatter data exfiltration tool	ditekSHen	0xf63a1:$s1: Renci.SshNet. 0xf6ce2:$s1: Renci.SshNet. 0xf6da5:$s1: Renci.SshNet. 0xf6e2b:$s1: Renci.SshNet. 0xf7b60:$s1: Renci.SshNet. 0xf7ba6:$s1: Renci.SshNet. 0xf7bf6:$s1: Renci.SshNet. 0xf7e44:$s1: Renci.SshNet. 0xf8298:$s1: Renci.SshNet. 0xf82c0:$s1: Renci.SshNet. 0xf83bd:$s1: Renci.SshNet. 0xfb414:$s1: Renci.SshNet. 0xfb437:$s1: Renci.SshNet. 0xfb605:$s1: Renci.SshNet. 0xfb97f:$s1: Renci.SshNet. 0xfb9a8:$s1: Renci.SshNet. 0xfb9db:$s1: Renci.SshNet. 0xfba06:$s1: Renci.SshNet. 0xfba35:$s1: Renci.SshNet. 0xfba67:$s1: Renci.SshNet. 0xfba89:$s1: Renci.SshNet.

Sigma Signatures

No Sigma rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

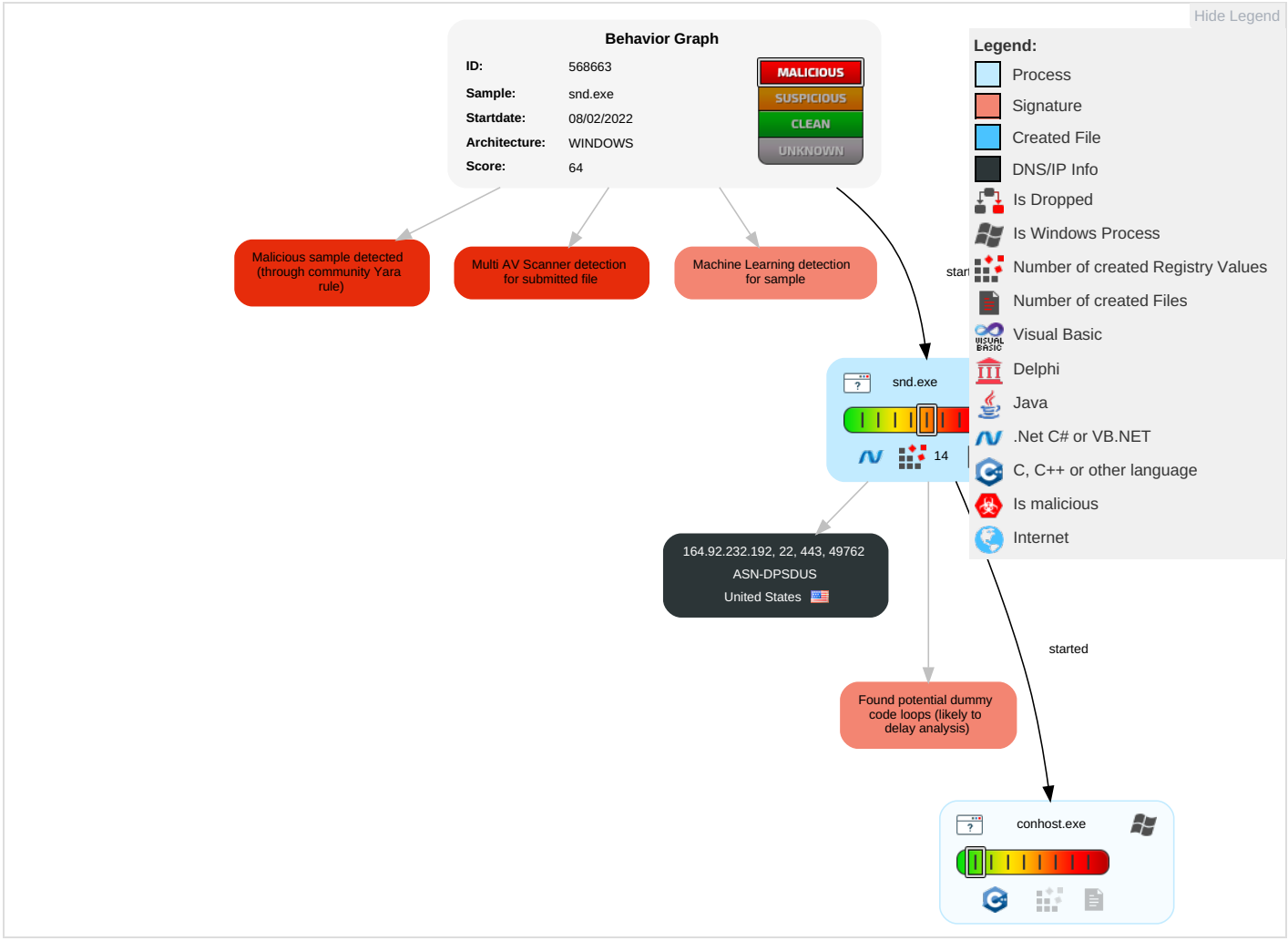
Anti Debugging

Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 2 2 Virtualization/Sandbox Evasion	LSASS Memory	1 Query Registry	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 2 2 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

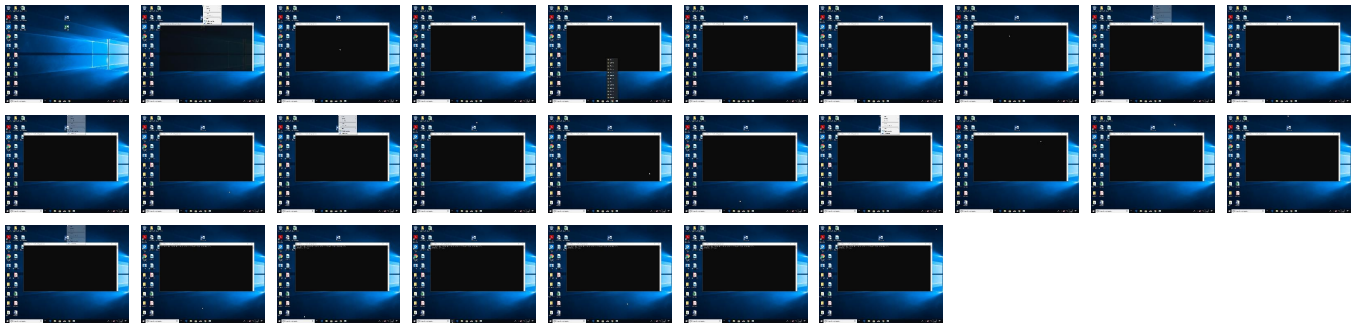
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
snd.exe	53%	Virustotal		Browse
snd.exe	61%	ReversingLabs	ByteCode-MSIL.Trojan.ExMatter	
snd.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://164.92.232.192/data/x	0%	Avira URL Cloud	safe	
http://https://164.92.232.192/data/3Can	0%	Avira URL Cloud	safe	
http://https://164.92.232.192/data/WORKGROUP.813848/	0%	Avira URL Cloud	safe	
http://https://duckduckgo.comqThere	0%	Avira URL Cloud	safe	
http://https://164.92.232.192x	0%	Avira URL Cloud	safe	
http://https://164.92.232.192/data/	0%	Avira URL Cloud	safe	
http://https://164.92H	0%	Avira URL Cloud	safe	

Domains and IPs

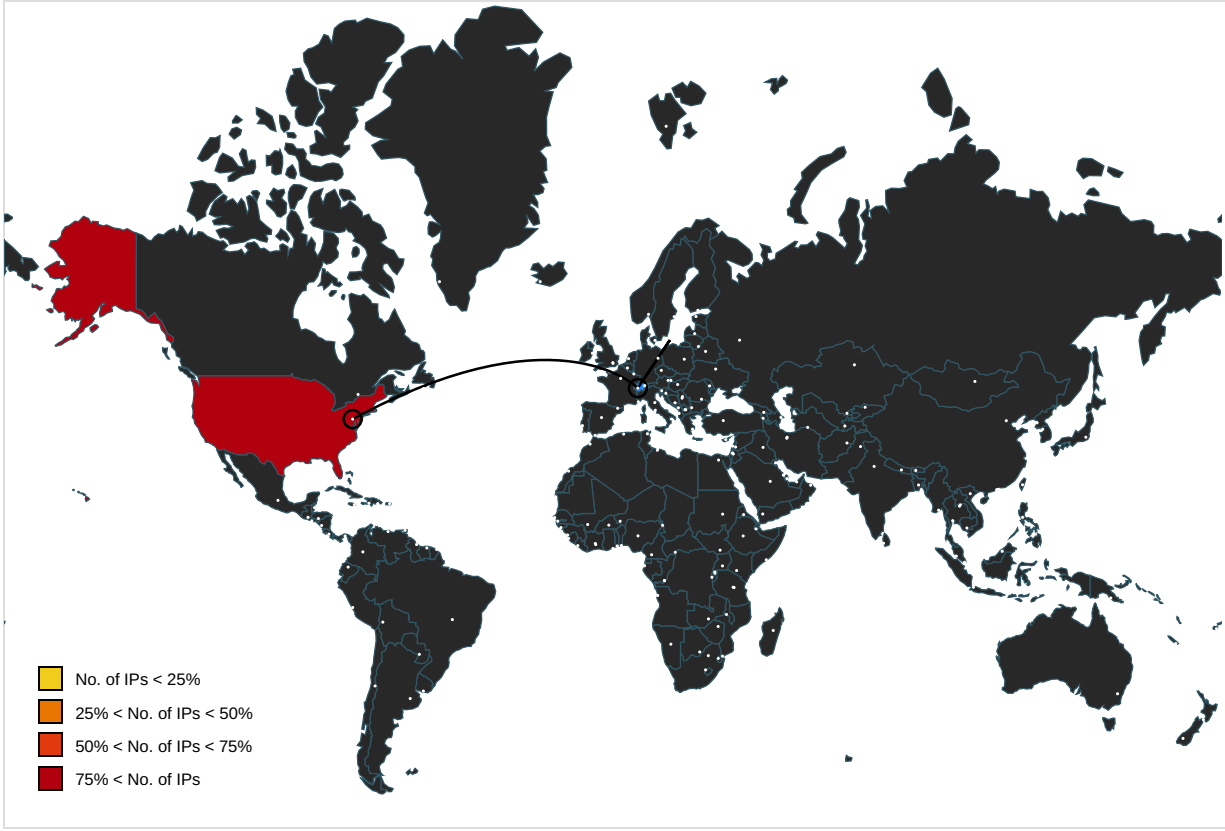
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://164.92.232.192/data/x	snd.exe, 00000000.00000002.519526709.000 00000031C1000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://164.92.232.192/data/3Can	snd.exe	false	• Avira URL Cloud: safe	unknown
http:// https://164.92.232.192/data/WORKGROUP.813848/	snd.exe, 00000000.00000002.519526709.000 00000031C1000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tools.ietf.org/html/rfc4253#section-4.2	snd.exe	false		high
http://https://duckduckgo.comqThere	snd.exe	false	• Avira URL Cloud: safe	unknown
http://https://164.92.232.192x	snd.exe, 00000000.00000002.519526709.000 00000031C1000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	low
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/name	snd.exe, 00000000.00000002.519526709.000 00000031C1000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://https://164.92.232.192/data/	snd.exe	false	• Avira URL Cloud: safe	unknown
http://https://tools.ietf.org/html/rfc4253#sec	snd.exe	false		high
http://https://164.92H	snd.exe, 00000000.00000002.519656216.000 000000327C000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://tools.ietf.org/html/rfc4253#section-4.	snd.exe	false		high
http://https://duckduckgo.com	snd.exe	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
164.92.232.192	unknown	United States		46930	ASN-DPSDUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	568663
Start date:	08.02.2022
Start time:	17:23:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	snd.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.evad.winEXE@2/1@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7.1% (good quality ratio 5.6%) • Quality average: 55.7% • Quality standard deviation: 36.8%

HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target snd.exe, PID 5692 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:24:49	API Interceptor	963x Sleep call for process: snd.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

\Device\ConDrv

Process:	C:\Users\user\Desktop\snd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	91
Entropy (8bit):	4.298548340139557
Encrypted:	false
SSDEEP:	3:ccFJfwV3XA8nwGA9KYoNRgLcv:FFOjwj9dauLe
MD5:	87449663D541AE83DCD4BDF9CBE96D0F
SHA1:	A1419597141B07ACEBDE8683C16C6D6EB92FA0B8

SHA-256:	803117358C99A080AB7B481E412993F2A9EF6A6128E1BE390A038A249650AC6F
SHA-512:	D7A73F4E32F15A6BC9C5C23B49623C183B7E7F0A76744067FD07561851815078BFF865B2C41276BF0C1C62F7B3E33BB2C2F4AD6D46E0D3DF99F095EACF7F1C0 7
Malicious:	false
Reputation:	low
Preview:	Can't make an upload dir One or more errors occurred. falling back..Connecting to host.....

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.04960117701529
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	snd.exe
File size:	1355264
MD5:	0a76e0e59456d310419266270c410936
SHA1:	1b6df9f456fbb2f793d8402d78c3338355ed98be
SHA256:	886cb22ffe43a3838ef152ef57bbfa66f52b71c534bfe3d8af3d29ea973daadf
SHA512:	bc32f32dbabf995a9971b7f34a433f93cd5ef634aa1bc91402b9474b957d115f493f93ca8d738080f2e3bdfd5d5430d694706a1cc6a42e9743edc87c064336ac
SSDEEP:	24576:Jmh0AMeTP7tpKY3sN1XUNPZKoN2ALtSax+:cFBThpKTXUNPZK2jf
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...%..a..... .....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x54c29e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61FB1625 [Wed Feb 2 23:39:17 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14c250	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14e000	0x596	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x150000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x14c1e0	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x14a2a4	0x14a400	False	0.377296880914	data	6.05319018352	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x14e000	0x596	0x600	False	0.412760416667	data	4.03797800026	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x150000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x14e0a0	0x30c	data		
RT_MANIFEST	0x14e3ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

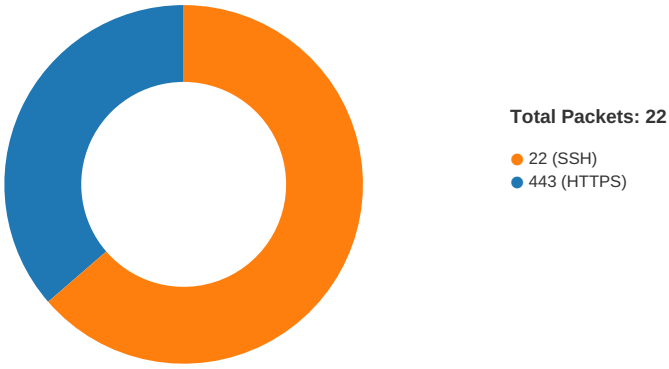
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	sender2.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	sender2
ProductVersion	1.0.0.0
FileDescription	sender2
OriginalFilename	sender2.exe

Network Behavior

Network Port Distribution



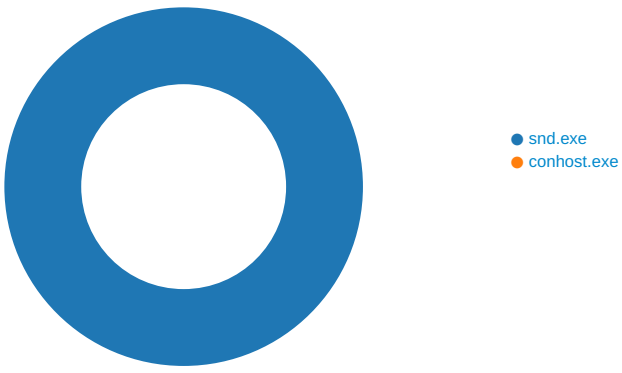
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2022 17:24:23.024465084 CET	49762	443	192.168.2.7	164.92.232.192

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 8, 2022 17:24:23.024528027 CET	443	49762	164.92.232.192	192.168.2.7
Feb 8, 2022 17:24:23.024657965 CET	49762	443	192.168.2.7	164.92.232.192
Feb 8, 2022 17:24:23.287492037 CET	49762	443	192.168.2.7	164.92.232.192
Feb 8, 2022 17:24:23.287561893 CET	443	49762	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:02.606378078 CET	49762	443	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:02.653862953 CET	443	49762	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:03.405878067 CET	49849	443	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:03.405937910 CET	443	49849	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:03.406033039 CET	49849	443	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:03.461317062 CET	49849	443	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:03.461361885 CET	443	49849	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:06.693900108 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:06.724852085 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:06.724984884 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:06.749135971 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:06.764698982 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:06.816354990 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:07.017211914 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:07.046648979 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:07.047993898 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:07.097641945 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:12.561610937 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:12.590997934 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:14.518470049 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:14.547741890 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:14.555624962 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:14.723253965 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:22.299853086 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:22.328149080 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:22.329166889 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:22.358473063 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:22.358499050 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:22.370834112 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:22.409041882 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:22.421771049 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:22.453186989 CET	22	49853	164.92.232.192	192.168.2.7
Feb 8, 2022 17:26:22.453304052 CET	49853	22	192.168.2.7	164.92.232.192
Feb 8, 2022 17:26:26.199938059 CET	49849	443	192.168.2.7	164.92.232.192

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: snd.exe PID: **5692**, Parent PID: **660**

General

Target ID:	0
Start time:	17:24:45
Start date:	08/02/2022
Path:	C:\Users\user\Desktop\snd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\snd.exe"
Imagebase:	0xd30000
File size:	1355264 bytes
MD5 hash:	0A76E0E59456D3104192662 70C410936
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF8F8FF1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFF8F8FF1E9	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFF89F4B526	WriteFile
\Device\ConDrv	68	68	43 6f 6e 6e 65 63 74 69 6e 67 20 74 6f 20 68 6f 73 74 2e 2e 2e 0d 0a	Connecting to host...	success or wait	2	7FFF89F4B526	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF8F7CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF8F7CB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF8F8A12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF8F7D2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF8F8A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF8F8A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Net.Http\a0f6e3585453700574fc42ba3653c021\System.Net.Http.ni.dll.aux	unknown	536	success or wait	1	7FFF8F8A12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF8F8A12E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF8F8A12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF8F7CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF8F7CB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF89F4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF89F4B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml.Linq\8e40b70389a56f1a2e084a433266fe7e\System.Xml.Linq.ni.dll.aux	unknown	872	success or wait	1	7FFF8F8A12E7	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5516**, Parent PID: **5692**

General

Target ID:	1
Start time:	17:24:45
Start date:	08/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly