ID: 508840
Sample Name: yRqHWQ91dT
Cookbook: default.jbs
Time: 17:05:27
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

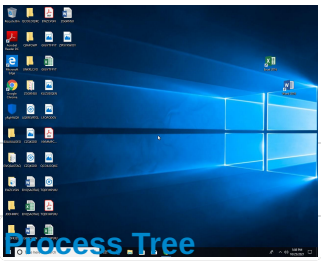
Windows Analysis Report yRqHWQ91dT

Overview

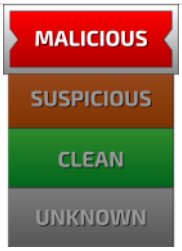
General Information

Sample Name:	yRqHWQ91dT (renamed file extension from none to exe)
Analysis ID:	508840
MD5:	b50ffa06eca2b3a..
SHA1:	4cdbdb338a22fd1.
SHA256:	a181b562122fb37.
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



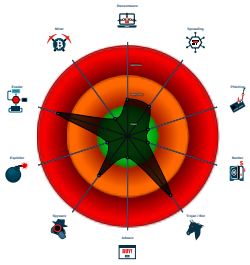
Ursnif

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Yara detected Ursnif
- Detected unpacking (changes PE se…
- PE file has a writeable .text section
- Writes or reads registry keys via WMI
- Machine Learning detection for dropp…
- Writes registry values via WMI
- Uses 32bit PE files
- Queries the volume information (nam…
- Antivirus or Machine Learning detec…

Classification



- **System is w10x64**
- yRqHWQ91dT.exe (PID: 5776 cmdline: 'C:\Users\user\Desktop\yRqHWQ91dT.exe' MD5: B50FFA06ECA2B3A4D92562561FC6B2D1)
  - msiexec.exe (PID: 3428 cmdline: msiexec /i 'C:\Users\user\AppData\Local\Temp\CssValidatorInstallerTemp\CssValidator.msi' /qn /norestart MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- msiexec.exe (PID: 2952 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 640 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 7A8FDEF089EF820D04B2E0639E42DA17 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - audiodent.exe (PID: 5656 cmdline: C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\audiodent.exe MD5: A0052D6EAC0D6D4296DE89213447416D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"GP2bItvzCMVimwFhSq2LMu3Hl69+F5VOC4HbUzLcgCFvHPQPwYycui0JiyqQuwt1jV1IDboN9TEBxLB8CQWBGqcjZkZnRvT4fL8wjq8CCeHOLprVhSXFIxyR2QXzTHDcHr2ux9/r22BaiLqlqlqcKQ1PI6I3WFn39M0K5k1WypMPthcp
EVFSO8sVBHvcqRSV",
  "c2_domain": [
    "get.updates.avast.cn",
    "huyasos.in",
    "curves.ws",
    "huyasos.in",
    "rorobrun.in",
    "huyasos.in",
    "tfslld.ws",
    "huyasos.in"
  ],
  "botnet": "2002",
  "server": "12",
  "serpent_key": "44004499FJFHGTYB",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000003.462453858.0000000008A28000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000003.462430424.0000000008A28000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000002.524066037.0000000008A28000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000003.462394649.0000000008A28000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000003.462483110.0000000008A28000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.audiodent.exe.7f70000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
9.2.audiodent.exe.83b94a0.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
9.2.audiodent.exe.83b94a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

PE file has a writeable .text section

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

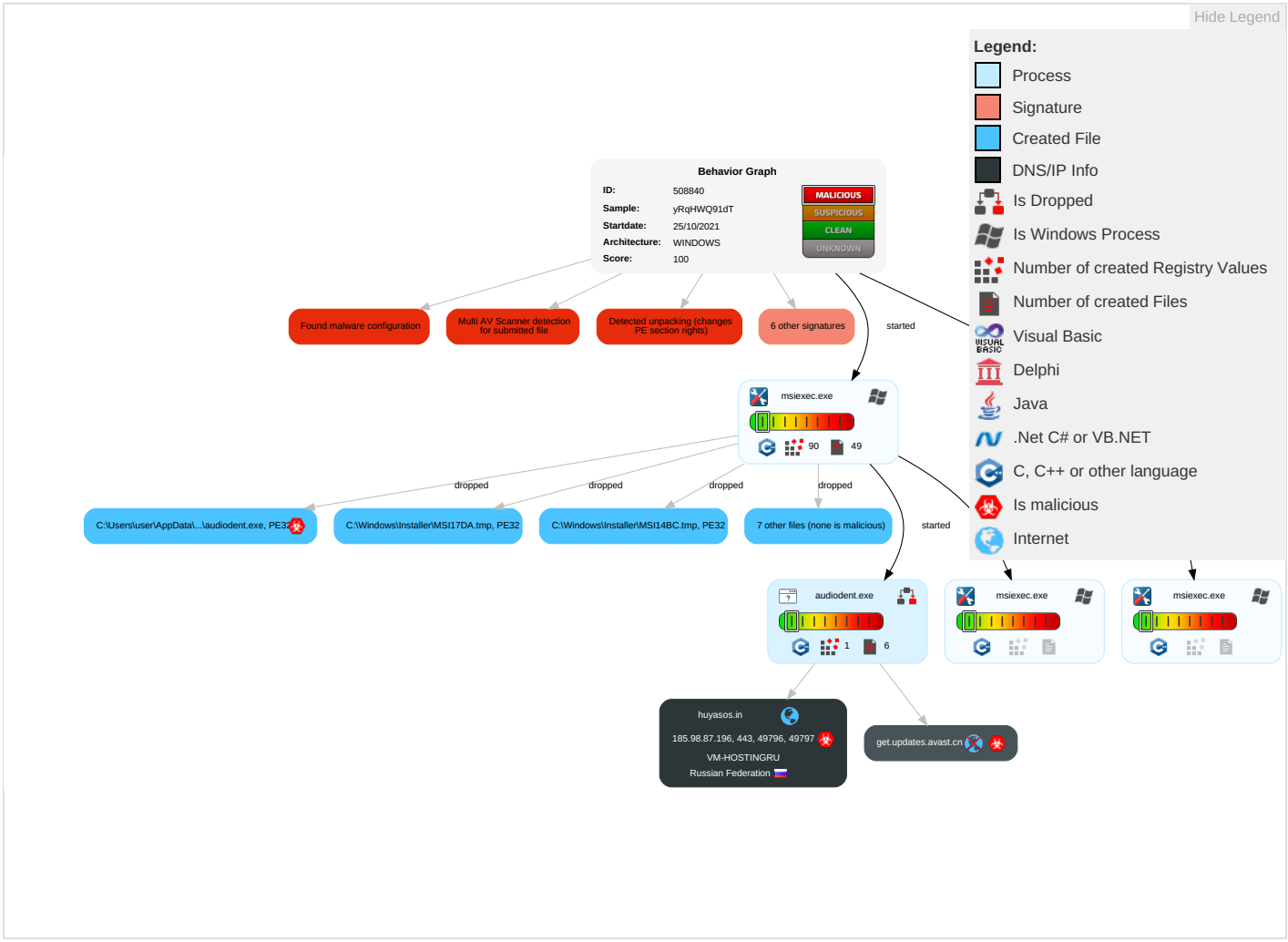
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
Replication Through Removable Media 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Obfuscated Files or Information 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non App Lay Pro
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 2	Software Packing 2 1	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	App Lay Pro
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Pro Imp
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	System Information Discovery 2 5	SSH	Keylogging	Data Transfer Size Limits	Fall Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	File Deletion 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 3 1	DCSync	Security Software Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Wel
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mai

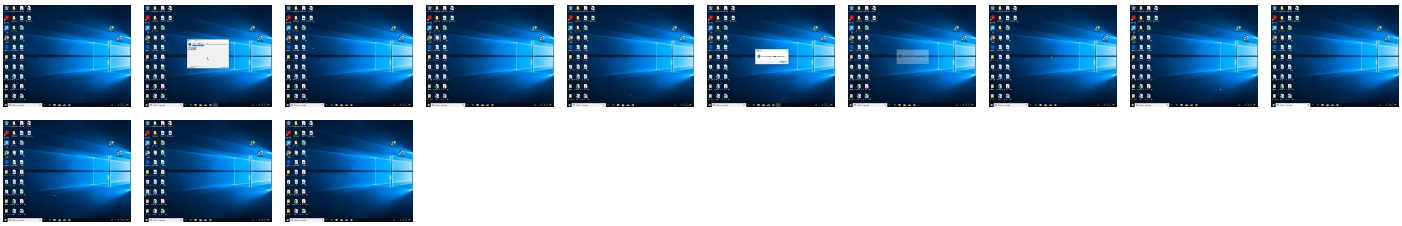
Behavior Graph



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
yRqHWQ91dT.exe	13%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\audiodent.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.batteries_v2.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.batteries_v2.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.core.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.core.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.provider.dynamic_cdecl.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.provider.dynamic_cdecl.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.provider.e_sqlcipher.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.provider.e_sqlcipher.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\Typography.GlyphLayout.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\Typography.GlyphLayout.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\libEGL.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\libEGL.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.yRqHWQ91dT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
9.2.audiodent.exe.7f70000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
1.0.yRqHWQ91dT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
9.2.audiodent.exe.980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://get.updates.avast.cn/l	0%	Avira URL Cloud	safe	
http://https://huyasos.in/sreamble/1Cy_2BOoNkPfZNI/cBFrvY8_2BuNL_2FRI/EvMKECOy8/d_2Bs3isSO64yzYzMTFW/VpmMJy	0%	Avira URL Cloud	safe	
http://www.grsoftware.net/downloads/grbackpro/grbakpro.pdf	0%	Avira URL Cloud	safe	
http://https://www.grsoftware.net	0%	Avira URL Cloud	safe	
http://https://huyasos.in/	0%	Avira URL Cloud	safe	
http://www.grsoftware.net/home/buynow.html	0%	Avira URL Cloud	safe	
http://https://huyasos.in/sreamble/1Cy_2BOoNkPfZNI/cBFrvY8_2BuNL_2FRI/EvMKECOy8/d_2Bs3isSO	0%	Avira URL Cloud	safe	
http://https://get.updates.avast.cn/	0%	Avira URL Cloud	safe	
http://https://get.updates.avast.cn/sreamble/L9cG8Vo2GQztGm0qovd/ps29AL3_2BtYxlbeUwyhe0/qJy1kBhZdmLJX/23gke	0%	Avira URL Cloud	safe	
http://www.mega-nerd.com/libsndfile/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
huyasos.in	185.98.87.196	true	true		unknown
get.updates.avast.cn	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.98.87.196	huyasos.in	Russian Federation		205840	VM-HOSTINGRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508840
Start date:	25.10.2021
Start time:	17:05:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yRqHWQ91dT (renamed file extension from none to 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:	28
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:	mal100.troj.evad.winEXE@8/22@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 38.5% (good quality ratio 37.4%) • Quality average: 80.1% • Quality standard deviation: 25.8%
HCA Information:	• Successful, ratio: 55% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:06:47	API Interceptor	2x Sleep call for process: audiodent.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
huyasos.in	OfsNSr9oYp.exe	Get hash	malicious	Browse	• 95.181.178.82
	W1qNIM5mQL.exe	Get hash	malicious	Browse	• 95.181.178.82

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VM-HOSTINGRU	installer.exe	Get hash	malicious	Browse	• 185.98.87.179
	0Xe1Rmpae5.exe	Get hash	malicious	Browse	• 185.98.87.65
	MtYLiiai45.exe	Get hash	malicious	Browse	• 185.98.87.65
	wVVTcS6zyZ.exe	Get hash	malicious	Browse	• 185.98.87.149
	_00541_Purchase Order_.xlsx	Get hash	malicious	Browse	• 185.98.87.149
	Hlxj8nfBay.exe	Get hash	malicious	Browse	• 92.242.40.244
	cpMHTTwNC1.exe	Get hash	malicious	Browse	• 92.242.40.244
	report_11.20.doc	Get hash	malicious	Browse	• 92.242.40.104
	report_11.20.doc	Get hash	malicious	Browse	• 92.242.40.104
	report_11.20.doc	Get hash	malicious	Browse	• 92.242.40.104
	New Price Quotation.exe	Get hash	malicious	Browse	• 92.242.40.195

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Canon Invoice - SG191009 & SG191008-pdf.exe	Get hash	malicious	Browse	• 92.242.40.195
	BANK_TT_PDF.exe	Get hash	malicious	Browse	• 92.242.40.195
	SWIFT MT103 MIDLGB31.exe	Get hash	malicious	Browse	• 92.242.40.195
	P117_881_pdf.exe	Get hash	malicious	Browse	• 92.242.40.195
	T8823_pdf.exe	Get hash	malicious	Browse	• 92.242.40.195
	SC-08453.exe	Get hash	malicious	Browse	• 92.242.40.195
	Revised PO 106622.exe	Get hash	malicious	Browse	• 92.242.40.195
	6FmrsohIP6g8w7i.exe	Get hash	malicious	Browse	• 92.242.40.195
	jkZKRSpFycGYr28.exe	Get hash	malicious	Browse	• 92.242.40.195

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Windows\Installer\MSI14BC.tmp	o4c8AUtX1g.exe	Get hash	malicious	Browse	
	farcry6_repack.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Config.Msi\530d7b.rbs	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	11078
Entropy (8bit):	5.746451563704331
Encrypted:	false
SSDEEP:	192:XYW1elYlxwrGBkmAnQZorAWax08RkpzTX344OL4B0eqsfn8cEYHsfn8cEY4nRS6J:XYUeljAWax08RkpzTX344OL4BnfnihfY
MD5:	1B30CF4F480C59E05A5C1540289760CA
SHA1:	37786DEA0D2A951B5DFAE6E02652EDF272AD9C19
SHA-256:	94BC18376E4915500F830DEBC436AA330A44346526D28634BA250794286B2FF3
SHA-512:	9D5D00651E068DAF9551F60BDB301C7D3A7CDFBD55574A1E81805A7CF532166CC3486623E99D789ECE10439BA72DF3B7041B4566646BF3B6A4DD742CA0638A(
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@.YS.@.....@.....@.....@.....@.....@.....&.{8C4E8105-89CF-42DC-B547-B756AB6C9EC5}..CSS Validator..CssValidator.msi.@.....@.. ..@.....@.....&.{2E68BFCA-136D-489B-99E7-02370AE416AC}.....@.....@.....@.....@.....@.....@.....@.....@.....CSS Validator.....Rollback..Rolling back action:....RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{BACEFD7C-2242-4BDA-88CA-278EA0FBAC71}&.{8C4E8105-89CF-42DC-B547-B756AB6C9EC5}.@.....&.{E1F4536E-7D2A-4F44-81EE-727B5F105E80}&.{8C4E8105-89CF-42DC-B547-B756AB6C9EC5}.@.....&.{834EA0BB-8035-4ACB-9366-174CC245FFAC}&.{8C4E8105-89CF-42DC-B547-B756AB6C9EC5}.@.....&.{F40562C3-E5CF-4975-B128-0CB43DBE0174}&.{8C4E8105-89CF-42DC-B547-B756AB6C9EC5}.@.....&.{C321E67B-035D-49DD-B4D5-4B5285D7B97D}&.{8C4E8105-89CF-42DC-B547-B756AB6C9EC5}.@.....&.{7F85F72B-E3A4-4884-A6D2-F057681DC710}&.{8C4E8105-89CF-42DC-B547-B756AB6C9EC5}.@.....&.{572BD592-23BE-4219-874A-9F3CC4AB9FEC}&.{8C4E8105-89CF-

C:\Users\user\AppData\Local\Temp\CssValidatorInstallerTemp\CssValidator.msi	
Process:	C:\Users\user\Desktop\yRqHWQ91dT.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {2E68BFCA-136D-489B-99E7-02370AE416AC}, Number of Words: 10, Subject: CSS Validator, Author: Hemoco bvba, Name of Creating Application: Advanced Installer 18.7 build 0a7fdead, Template: ;1033, Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Category:	dropped
Size (bytes):	7775232
Entropy (8bit):	7.95100555954072
Encrypted:	false
SSDEEP:	196608:rY7cfmLhGlwa2wQiXAytyTCpj59zHpmzSTnUT4R+:rY7cfmLYwMQiXAytJ55gzSTw
MD5:	4C0F425E456ED7904F1B207FAD617EBE
SHA1:	56304F5446B7DB91314E252143E59353072A6F28
SHA-256:	A14D402C30E55AC43A83596A1D2832A730A7EB3A056E9420AC725B0EF02A176A
SHA-512:	C9AD2C0B0EBF21F7D683026689429DEF5BC5AA8DE2B3778CB1B84259CF920BF8506A55080BF7B292BE9D37C0B37398802F438C183046C0ECF6CF70D3BF396D3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\CssValidatorInstallerTemp\CssValidator.msi	
Preview:	.....>.....w.....C.....~.....q..... .....;..... .....#...2..... ...!..".....$...%...&...'...(...)...*...+...0...-...../...3...1...:...>...4...5...6...7...8...9.....<.....=...f...?...@...A... B.....E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v. ..w...x...y...z...

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\LICENSE.electron.txt	
Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1060
Entropy (8bit):	5.127745905239685
Encrypted:	false
SSDEEP:	24:lDiJHxRHuyPP3GtlHw1Gg9QH+sUW8Ok4F+d1o36qjFD:lDiJzfPvGt7ICQH+sfIte36AFD
MD5:	F8436F54558748146EC7EBD61CA6AC38
SHA1:	EF226E5B023D458EFCDC59DC653694D89802F81C
SHA-256:	34F6F27C26D1BB8682EBB42AE401F558228FD608455BD7C6561D5FD500B7D05B
SHA-512:	5B310B48BBEE286F03E645E4BFAD0EC870A7C68C445D54F46F3EAAA9C427F9DE6CD0561D451838BD53C78A5289E9F0BDA19CDA4257A4657580AFA6C3579130 0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Copyright (c) 2013-2019 GitHub Inc...Permission is hereby granted, free of charge, to any person obtaining.a copy of this software and associated documentation files (the ."Software"), to deal in the Software without restriction, including.without limitation the rights to use, copy, modify, merge, publish,.distribute, sublicense, and/or sell copies of the Software, and to.permit persons to whom the Software is furnished to do so, subject to.the following conditions:..The above copyright notice and this permission no tice shall be.included in all copies or substantial portions of the Software...THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,.EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF.MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND.NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE.LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION.OF C ONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION.WITH

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\License.txt	
Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	3319
Entropy (8bit):	4.74915258074069
Encrypted:	false
SSDEEP:	96:mFc2eAg2pZGQlvzRCyLiqxt2X3I8Si0mebrSv:zfAgmrRhL4I8SiWbrSv
MD5:	CBD32695674DCFBA5C4609DEFCAFDF55
SHA1:	6F5C934CB49845AF6B59683544A95A7E4B515DCE
SHA-256:	2568688DD3418B21FD0D4CD416C1A759DE9DAE759E192BCCF834D3EC2E1E7F2C
SHA-512:	AE430B2FEE5864BB4130C44C26A90A2053B098C4E783AD0AD9C587B3E4FD1A38E7AD5D87C5AF6E598ED7D1A6A766F104B4C07599FCD282248E655FFBAC2C26 68
Malicious:	false
Reputation:	low
Preview:	END-USER LICENSE AGREEMENT FOR GRSOFTWARE SOFTWARE GRBackPro.....IMPORTANT - READ CAREFULLY: This GRSoftware End-User License Agre ement is a legal agreement between you (either an individual or a single entity) and GRSoftware for the GRSoftware product identified above, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this End-User License Agreement, do not install or use the SOFTWARE PRODUCT; you may ho wever, return it to your place of purchase for a full refund.....SOFTWARE PRODUCT LICENSE....The SOFTWARE PRODUCT is protected by copyright laws and i nternational copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold. You may not rent, lease, or lend the SOFTWARE PRODUCT. You may permanently transfer all your rights under

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\ReadMe.txt	
Process:	C:\Windows\System32\msiexec.exe
File Type:	ISO-8859 text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	20212
Entropy (8bit):	4.793794798262899
Encrypted:	false
SSDEEP:	384:DtfgszUGxVnoOxazTGExOrDDDuUMOT4SsWv:xLxVnoVzTG3kk4E
MD5:	8EB0D56C86DA3080CFE2F9BAB6D6318C
SHA1:	A63256C40D34B844D2DB2F2DFB2A6C068F2F1E19
SHA-256:	091CBA047A79B4BE6A10FF265153D44C8474CC24FBC0B9C17775F481738AE8DD
SHA-512:	12E15DE204C2EDF2AB4D57E2A35D96DC2D6296079EC1C86CEAAA7510336F9C57CC833C10EE50F592797C700DD729D3076065523FFB83B0DEBA5B872BD4EED 49
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\ReadMe.txt	
Preview:	Distribution Summary..~~~~~~~~~~~~~~~~~~~~~~~....GRBackPro: Professional backup for Windows 10/8.1/8/7/Vista/XP ans Windows Server 2019/2016/2012/2008/2003 v9.3.x..Release Date: 19 October 2021..Categories: backup utility, file utility, system utility..Supported Platforms: Win10, Win8.1, Win2019, Win2016, Win2012, Win8, Win7, Win2008, Vista, Win2003, WinXP....Description..~~~~~~~..GRBackPro is a professional Windows backup program that helps you maintain your..vital computer data. It can re-create your source folder tree onto the..destination drive (or a single compressed archive) and for every folder it can..copy your files or create a PKZIP. compatible compressed archive with long file..name support and password protection. You can run a full, incremental or..differential backup of your files. You can synchro nize your backup..files/directories with your sources. You can easily restore all or just some..files to either the original source or to a new location. You can define..multiple b

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.batteries_v2.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.288309221167179
Encrypted:	false
SSDEEP:	48:64+lYpBBasD07Nf4yBrl/KckU1N4zOuS0GiWekJWC27fSMBBhAA+vnaOLhWLsnO/:yOalx/lCcXYz1S0Gx7i7zHAA+CO/l
MD5:	E3DDBE5680FAD01D0E5B7B963181BC06
SHA1:	BECCE75CDA9222511E9F8D480B145CE6C24A6CCF
SHA-256:	07A2736DF9434B0FBBC5C441A76726CA66EB21554622B5F09D797EA01DF9F0C7
SHA-512:	055E2AE9079B2CB8DE58F01CA19C8561C21349406186A1E884765AA074C57740E7E6C4A43C3E4A939F1316F4D8114671032D76F61DEB9B0C7BEB9C1D10076579
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....f....." ..0.....)... ...@..... .....j... ..`.....)..O....@..`.....`.....\(..T..... ..... ..H.....text..... ..... ..`.rsrc...`....@.....@..@.rel oc.....`.....@..B.....)......H.....d ..x.....'.....(....*.s....(....*.BSJB.....v4.0.30319.....l.....#~..L.....#Strings.....#US... .....#GUID.....`...#Blob.....G.....3.....6.m.....m...s.Z.....q.....V.....Y.....8.1.....1.....1.....(.....1.9.....1.9..... P .....W .....T.....T.....T...).T...1.T...9.T...A.T...

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.core.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	50688
Entropy (8bit):	5.803306723899389
Encrypted:	false
SSDEEP:	768:DQPUEF4XAR8QTqUp6H1Y1wDUmydr8wqlUUUUaeoJdFUUUUUUjIM5UUUV/NLF44vQ:HXAR8QTqUpC91ydLJdr8dbhi1FLsu
MD5:	358BF09045A59A1B85ACD9BC0A592904
SHA1:	53CF59D7B192F570D528B4D5C72DFA7AC25E1D7B
SHA-256:	6BE5D612830990F4185DEA66B4BAABE191D641A3A97E081A2F62FBADF2AF5B0F
SHA-512:	8E99956FAEDD57E83FB46CC2DE6D241BE9ED6B0A6967B00F7518FF461D28DBB67A3B00CB8ED22981A635E0688B53C79A507F4D92AF88F9F290980AA0BEF5B55
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{....." ..0.....N.... ....O.....0.....T..... ....H.....text...T.... ....`.rsrc...0.....@..@.reloc..... .....@..B.....-.....H.....0@.....p.....(....*..(....*..(....*.....*Z~....,*.oA...&.....*.....*b~....-.r...ps....z~....*.(#...o7...*.0.....(#.... ..o8.....(....Q*6.(.....(%...*.0.....(#.....o9.....(....Q*R.(.....(....('...*:(#.....o>...*N.(.....(.....()...*2(#....o:...*2(#....o;...*..o....*..o....*2(#....o<...*2(#....o=...*6(#.....o....*...0.....s .....}"....{"...-...+....!...s.....(1...*6(#.....o....*6..(....(3..

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.provider.dynamic_cdecl.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	5.551074874821588
Encrypted:	false
SSDEEP:	1536:/RzZVISfvupRJ5d82N40duRlYy33r7HfrmYs0c6mRFgDJ8pYeFU6yTaM/eT72VmH:Zc5wAJlMq
MD5:	6A5E8F425D04F3BC66360F2BF07688A4
SHA1:	E7627232FD39730D90F11D979F1DAC6356A5244A
SHA-256:	2A45581E2ED65CAE497A199A56F311FA08B3D8C1B777E936F15D04D0B96923D1
SHA-512:	06FC1C49B40EDD398AB81505E906065D3C9B52782F7E310A71CB17FF27E5521249A6CA81E18E1A546186308CC872EB4A28ACB120D055A04B31850BEC1642D8E
Malicious:	false

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.provider.dynamic_cdecl.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....0....." ..0.....Z.... ... .`.....n.. ..`.....O.... .....@.....T..... ....H.....text...`.... ..... ..`.rsrc..... .....@..@.reloc.....@ .....@..B.....9.....H.....4E..$.....X.....6.....(....*.~....*F~H.....o|.....*N.....s....o...+*..0.....(.....~.....o....*.0.....(..... .~I.....o....*.0..%.....(.....(.....~J.....o....*....0..H.....(.....(.....~K....o.....(....(.....{.....o....*2~#....o....*2~"....o....*2~F....ot...*6~G....ox...*:~H.....o|...*2~ $....o....*2~%....o....*>.(.....o....*...0..N.....,.....s.....

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\SQLitePCLRaw.provider.e_sqlcipher.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	38912
Entropy (8bit):	5.68164166116722
Encrypted:	false
SSDEEP:	768:nL++D20WXYjIzkPkPhh55Rru026caYscRZyQ5yuyc8VqaVYDRY1YXojnKLkI+lIG:a+S0WXYjIzkPkPhh55Rru026caYscRZK
MD5:	B7102F54D13AF5F4B66B12692DDE2D51
SHA1:	8A5619C2AA731AACF9D83EAFF3133FE0C63659DB
SHA-256:	C6CB095CEA1A39307A0579E9EC7C7D7161D04E88A245476417FE0C7D12A9B85E
SHA-512:	3577B57CA1656D0D939BF7A03F0D7D0A86C8797B57900F42690F83704681C7FDDA0919158011C29EBEA1AA66E53A28252CEFA15C84A8E32DF9E2EC41C128C43
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...C.4....." ..0.....2.... ....`.....O.....T..... ..... ..H.....text...8.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....2...w.....0.....r...p*2...(.....*N.....s....o...+*..*..0.....(.....(....*....0.....(.....(.....(....*. ..0..>.....(.....(.....(.....(....(.....{.....o5...*..(....*..(....*..(....*"..(....*&...(....*..(....*..(....*>.(.....o....*....0..I.....,.....sl.....s.....+.....s.....(.....(.....(.....o....*....0..... .....(.....(....*2.(....(....*....0..

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\Typography.GlyphLayout.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	27648
Entropy (8bit):	5.565938052019052
Encrypted:	false
SSDEEP:	768:W8cd6x5pyqNfNbttXqLYIA69kP2ulg4Q:WAx5p7fdXqLYIv9kPK4Q
MD5:	3301FD842AC418CF18BC96FA52D2D497
SHA1:	80B32039DF1C2439046DFCB30120D7BE8FACEAAB
SHA-256:	91CA98A59CE9B3347F6F23A0C52C714C4E56AE862956D9465E12E6D07EF87CD6
SHA-512:	051F218D9120F2E3D3E19301B73BF3D4FA0582456C032D6A3C2A05435754907092C41352B3EA9B2228A599081EFD87BF7D32633D87ADFEBB197D5A1B265BC15F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`....." ..0..b..... ..... ..... ..@.....O..... ..... ..H.....text...$a... ...b..... ..`.rsrc.....d.....@..@.reloc..... .....j.....@..B.....H.....>...@.....(....*^.(.....5...%...}....*:.(.....}....*:.(.....}....*>..}.....}....*~.,..(....+..}.....(....}....*R.{....-. {.....*.*F..2.. ..../...*.*....0..L.....(....-..o.....*.o....%..(....%..(....%..(.....(.....b...b`..b`.`*.0.....(.....(...(!.....io"...*2.{....(....*2.{....(....*.o#.,..,.{....{....s~....(....*..{....o $.....}.....{....o%....{....o&...*..0..B.....{.....o'...

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\assets\goal_achieved.png	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PNG image data, 889 x 886, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	104621
Entropy (8bit):	7.961279215007163
Encrypted:	false
SSDEEP:	1536:aEdO/Zg43pJQup/9SUe/73fYcBHLV1fqlABxM2urRCGYnf0qYtWZX2ywtgV2/ug1:aEOW4jl5/7AcBHLV9qgxc3chb424H1
MD5:	A2B879334ED0DED12343695E26E30554
SHA1:	581DCF49F959F35B13A71705B917A61658BD7836
SHA-256:	ECDBDF4A3A32936E79327FD7CA276340E89960CCB6CAA665A27BBB8EA774C83D
SHA-512:	2050065D7D4EADEBD7814E76A18039FECF6C93AE5D145777761CAA452CBE3C7C4D7122EC709F60990254D2A4F4CFF3DD0774A9FDCA08C5AA8BD4C40D7A087F0
Malicious:	false

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\assets\goal_achieved.png	
Preview:	.PNG.....IHDR...y...v.....D.@.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^.w..gv.....0. '.....,w.AKz.[.kI..jW.K.....H..$9.....)..RI.I..OZ..#.....4...L.ynN.....h.. .wnx~U/ .owc.N...y..-!..B.!..B.!..B.!..B.!..B.!..B.!..B.!..B.!..B.!.e.R.!...7n.m?q..!KYY.d2Y_RR.....W....q...nA.V"..Vj...z....e...X,.~Nb...Sh..>..4..,....t.]...+`..sU.!.0...B...1...o....j;V+.lh. ..,.X..-G[.V...<.nn...?.....S.a..VLP...R"..."...X...`}..o....]v....g.Z..z.m..SW.o.p.....B.).yB.Q$@X.d._{.eh..n.9.8...4+.y.....h%..o\.A...Z.W`..v..D.B`x..`.~..... K.t.....b.m..n.B../.. <.....].q.X.l6.....m.g?...={.....B.!..u.B.Q`.....s..5h.r.:...F.....Hk@s....B.Q.....TD..#s.lc:&....%...;.D..{..,%....8.2.!..6.cX..h\g..4.....Ha..a...3X.).....&!.{..y...B.....B.<.....f$.\ 5x..W...E.S.q<..b..-.L!GqF!g..%._..]X."....3.G.g.@X,..V.c.A.M...6K../8..[F.iL.c.....0..!.e.....E.4.....E.1a..\..h~S..x..q.[.....B.....B.....N.....i.*.....).,h.p.X.

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\assets\goal_progress.png	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PNG image data, 1024 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	66444
Entropy (8bit):	7.695795199213902
Encrypted:	false
SSDEEP:	1536:/og6riWZ+mPCTR4dEWsEbr22JCzIl9fWvWBkAXQqj0DgUB62rBcUWD/:l6pHKT+Nm2kDfW0jgI08UU2ru9D/
MD5:	3559215A74E795F065A0EBA888FAB63E
SHA1:	78834C228B2BCEF9A2D22D8B407BFF1901955043
SHA-256:	8EB9852560A3E6ED0790A8B40CEDEEEFF8A39D6F2985738EC81DFE9445F61D8A
SHA-512:	9E5FD39BB5E420F2172B25E15B75ED988FBA1343925AD019D8636932DDA9B20090E2F14BA48F3E1B003EB499910E43FD5870CD122188FC8EB39684E3253A8F2B
Malicious:	false
Preview:	.PNG.....IHDR.....+... .IDATx^.....YY...Tw..Lfl....df....&..Q..l.V.....(..+.....WTT.....-...P.M...YTHv....f.d..L6..u?..YY.....Su~...'{.:.y...f..Sb. .... .@b..*./.....~S...7Q.].off..?O LL\.....+..g..s..+...'....g.....?.FU.^c.%c.....1fEU..s..W...{.....b.....Z.. ..E.^..U.. .....x...qb.L.... ...._..... .....x!...1..k.X,.....yY.h.r.???/.....MM.....o....H..E..Xo...l6...r...^[[..m..A pO>..guu5..p1.`.....@.....J%.....@.'.....^...m....p..233....\.w.">...N.^|.1..;=?..T..c..@..:.....b.8366voR.1/.. .....p.:.... .S.....Z..DQ$g..v..%q.....O.O...TU/..ic.)U=-"..s..&A. \...VO.`p..@.....`Q.....@.;..w.~bb.>.....}wd.YXXx....[.i.....c.6.\i..Z...";...'"...."..... ....v.8....@.i.#G....r.u..X,..B!..r..{.b...h.OU.D..c..V..\.w...i.!hG.c.@...\....je.....@.!.\.woQ.....m.. .....B.#r".. ...}....'h.A....hO`.{.....e...~{~..E..]....7....8...._.bC..8....@...4..... .....x..}{...\Z.4..V..._%P.....Q...[.L.... .....

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\audiodent.exe	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10532352
Entropy (8bit):	6.6035389772335265
Encrypted:	false
SSDEEP:	98304:zihKeDg7JMqrr43ls1Wcliy36CpnNZ6zk9zYAl3P43N4tGqFbd3HuLeLunGrfSTT:IRBqnE50ytnNUAl/40RHZMEfWtR
MD5:	A0052D6EAC0D6D4296DE89213447416D
SHA1:	2F3ED143855A0490D8E3EC564FE27A3F72FA4916
SHA-256:	C57A1C9570FF6CEFF0A08770A142C348B5B3E5B2C03417C03C0FBFFB7707069F
SHA-512:	0352C179F4D2F6E5CEAA116B885203E613662F6D93D9AE7B2FC8FC0FAF89DD4889A66C5D4DA9D12CC8D38D7BB4E38A116E9A0E4F629E51979D07EA7EB4996D 1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....H.....!..L.!This program cannot be run in DOS mode....$.....1:._i.._i..i..i._i&(.i._i&(.i._i..\h.._i..[h.._i..Zh.._i..^h.._ia.^h.._i..^ i.._i..Zh.._iN.Vh.._iN.Zh.._iN.[h.._iN._h.._iN..i._i...i._iN.]h.._iRich.._i....7...6...7.....7...Rich6.....PE..L...-6ua.....hl..J4.....c.....l...@..... .@.....0h.....H~...i..T.....j.....i..@.....l.....text...-fl.....hl..... ....rdata...|$...l..~$..ll.....@..@.data. ..P.....@....rsrc...0h.....j.....@..@.reloc..H~.....6.....@..B..... .....

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\libEGL.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	109056
Entropy (8bit):	6.49594862756501
Encrypted:	false
SSDEEP:	3072:cM7DNjsmbZIwfTCR7GrVXFb5Q3jaZRUjF0rQDGYoM:XX7CRwVh5QsRKDGxM
MD5:	E4B0061BFC552111AA9F6A63AC61B1B9
SHA1:	2F4F9A0E179EB17FF077C3BBA30C09E1EA0E0C0F
SHA-256:	17C8685F54EFD76AE5C3171F146910772B49A3D733CDA66E2FBC5C64CE800214
SHA-512:	978D41141967FDBD509D081F1FB107F13C61EABB4E13712D7D4FEF51997AD0273F211901AD46E0A352770FD849F15B878AFF1B02B3600880160D1213DC9B53A4
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...PC.^.....'!.....'.....@..... .....(..... .....l...~.....(.....text..... ..`.rdata...t.. ...v.....@..@.data..... .....@....00cfg.....@..@.voltbl.d.....rsrc... .....@..@.reloc..l.....@..B..... ....

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\qclp2.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4254720
Entropy (8bit):	6.929231407239177
Encrypted:	false
SSDEEP:	49152:nJ6Wv9ViKjOpvDNXbqgf5gHUkphV7DkzigZAIcn2vjkMcRc/s+kobXnz/q/xnd/s:nJ6Wv9VBS9DJxzIV7Dkms5ZVQa
MD5:	7FC7D8096392A3887F53F85A570137C6
SHA1:	18822D95CDB79D25ACFCFFED8395CC208AA03D04
SHA-256:	F6B6D5C0EA15112F428A83B923B879EC43AA54D7677AD29E763532881509DEED
SHA-512:	CAC312C0700EACFF4A2FFAAB844275AC9D0093C64AA1C74D4A94822D02117E3A55BA1310500B4D1024DCB075720B9FFB2DCD0FDBCF8748C72A4890E24D53E7C0
Malicious:	false
Preview:	MZ.....@.....H.....!..L.!This program cannot be run in DOS mode....$.....1:._i._i._i..i._i&(.i._i&(.i._i..\h._i..[h._i..Zh._i..^h._ia.^h._i..^i._i..Zh._iN.Vh._iN.Zh._iN.[h._iN._h._iN..i._i...i._iN.]h._iRich._i'y.....'y.....Rich.....PE..L...18ua.....!.....)b..... .....A.....=@...@..... .....;.H.....;.T.....>..k.....?.....p.:.....:.....:.@..... .....text..... ..`.rdata..... .....@..@.data..... <..`.... <.....@....rsrc....k....>..l...j=.....@..@.reloc.....?.....>.....@..B..... .....

C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\zmq	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PDF document, version 1.5
Category:	dropped
Size (bytes):	442111
Entropy (8bit):	**7.994446353856369**
Encrypted:	**true**
SSDEEP:	6144:aorUBWkDwzCvAmehaITUjbhl+jG8xgGS21gdljuFFuybeBq//GvucNIrbRQ873vS:ahWgFomnll+ABHILycq3GGcNIrbfev
MD5:	DCED29FE7B0769AF598BE6684DD85677
SHA1:	DF5808C075F7AD586A858D1B71449C954C648A37
SHA-256:	84855FF6E0BB4BB79E4CC13B600C26633340CAA3FDEC16504E7006777213C0F4
SHA-512:	2408B866FA00EC9342BAC2223BF3092FAFFB8481BB8B0D4BBBEF4305739497211619A01DB2E8AC18563888E4755D2E36AF208459013D6BA781F4F06C00654F6E
Malicious:	false
Preview:	%PDF-1.5.%.....1 0 obj <</Length 587 ./Filter /FlateDecode.>>.stream.x.mTM..@...+z.&...?.tBL.$..d4..*.....<.._...f..W._w..r..c;...`G.U.O.V.&.....[v...6.W.7..T..vb...uYt /N....5.....=..S.<b...G...I(vEwv+OR8$.....6mQ.oB.J)..*.....3.q..X.ysO'.H.)-."...}.....[...<V^...[I..F.x.M..(Ob..q..Z.g..Bz.....<../V.....[m..Xq.Y...g..'.R.D.....?k3.q8~.J.....#..... 8.}.RC.g..%.P...)..{.4..".a/.. .C..^.@..8Y*C..%Md_b.g..4..L.0^.O....\.....p..g...\...8~.s..3.....{M...Nq7..*j.6..f-.S.A.'..A.!.:.O...L.0...x/i.dB.n..^.ySS.W.+%={.I.b.....o..k.....c.6|f...3.4. {...p.Y.d.r...K.+H.....WA.....4nfh.i*0.Ei..ZW5v.&...@.I....6..endstream.endobj.2 0 obj <</Length 598 ./Filter /FlateDecode.>>.stream.x.mTM..@...+z.&...?.tBL.0 ..d4..*.....<..~U..f..W._u...v..c;Z.....MfG..}...I.]/....m..o.....0^'..^.x]f.kn{..EK{*..u.pg..6;..$4..;..gZ8,.....M[T.P.RJG.e.W.xm.....E.7....."/....7.....j;{Y..."1.t.m.|...o.ir...I..c..>[T.. .En.n#....b.....

C:\Windows\Installer\530d79.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {2E68BFCA-136D-489B-99E7-02370AE416AC}, Number of Words: 10, Subject: CSS Validator, Author: Hemoco bvba, Name of Creating Application: Advanced Installer 18.7 build 0a7fdead, Template: ;1033, Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Category:	dropped
Size (bytes):	7775232
Entropy (8bit):	7.95100555954072
Encrypted:	false
SSDEEP:	196608:rY7cfmLhGlwa2wQiXAytyTCpj59zHpmzSTnUT4R+:rY7cfmLYwMQiXAytJ55gzSTw
MD5:	4C0F425E456ED7904F1B207FAD617EBE
SHA1:	56304F5446B7DB91314E252143E59353072A6F28
SHA-256:	A14D402C30E55AC43A83596A1D2832A730A7EB3A056E9420AC725B0EF02A176A
SHA-512:	C9AD2C0B0EBF21F7D683026689429DEF5BC5AA8DE2B3778CB1B84259CF920BF8506A55080BF7B292BE9D37C0B37398802F438C183046C0ECF6CF70D3BF396D3
Malicious:	false
Preview:	.....>.....w.....C.....~.....q..... .....;..... .....#...2..... ...I...".....$...%...&...'...(...)...*...+...0...-...../...3...1..:...>...4...5...6...7...8...9.....<.....=...f...?...@...A... B.....E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v. ..w...x...y...z...

C:\Windows\Installer\530d7c.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {2E68BFCA-136D-489B-99E7-02370AE416AC}, Number of Words: 10, Subject: CSS Validator, Author: Hemoco bvba, Name of Creating Application: Advanced Installer 18.7 build 0a7fdead, Template: ;1033, Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Category:	dropped

C:\Windows\Installer\530d7c.msi	
Size (bytes):	7775232
Entropy (8bit):	7.95100555954072
Encrypted:	false
SSDEEP:	196608:rY7cfmLhGlwa2wQiXAytyTCpj59zHpmzSTnUT4R+:rY7cfmLYwMQiXAytJ55gzSTw
MD5:	4C0F425E456ED7904F1B207FAD617EBE
SHA1:	56304F5446B7DB91314E252143E59353072A6F28
SHA-256:	A14D402C30E55AC43A83596A1D2832A730A7EB3A056E9420AC725B0EF02A176A
SHA-512:	C9AD2C0B0EBF21F7D683026689429DEF5BC5AA8DE2B3778CB1B84259CF920BF8506A55080BF7B292BE9D37C0B37398802F438C183046C0ECF6CF70D3BF396D3
Malicious:	false
Preview:	.....>.....w.....C.....~.....q..... .....#...2..... B.....E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v. ..w...x...y...z...

C:\Windows\Installer\MSI14BC.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	402912
Entropy (8bit):	6.383799484265228
Encrypted:	false
SSDEEP:	6144:hsEQsy5dfBkvAUnBU76LNaiDWbqw0EAOqcmCIVKVPgvf:4sw6vAUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F6227BA
Malicious:	false
Joe Sandbox View:	• Filename: o4c8AUtX1g.exe, Detection: malicious, Browse • Filename: farcry6_repack.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@p..!..!..!..J..!..J...!...T..!...T..!...T...!..J..!..J..!..J..!..!... ...T...!...T..!...T. .!..!..!...T..!..Rich.!.....PE..L...".Ia....."!.....*.....6|.....P.....k.....@.....p.....D.....0.....A...8..p.....@:..... .H9..@.....$.....text...6..... ..`.rdata..8.....@..@.data.....@....rsrc...0.....@..@.reloc...A.....B... .....@..B..... .....

C:\Windows\Installer\MSI17DA.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	402912
Entropy (8bit):	6.383799484265228
Encrypted:	false
SSDEEP:	6144:hsEQsy5dfBkvAUnBU76LNaiDWbqw0EAOqcmCIVKVPgvf:4sw6vAUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F6227BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@p..!..!..!..J..!..J...!...T..!...T..!...T...!..J..!..J..!..J..!..!... ...T...!...T..!...T. .!..!..!...T..!..Rich.!.....PE..L...".Ia....."!.....*.....6|.....P.....k.....@.....p.....D.....0.....A...8..p.....@:..... .H9..@.....$.....text...6..... ..`.rdata..8.....@..@.data.....@....rsrc...0.....@..@.reloc...A.....B... .....@..B..... .....

C:\Windows\Installer\MSI1C62.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	5958
Entropy (8bit):	5.682448959061152
Encrypted:	false
SSDEEP:	96:VYW1elER4Nkqt1Cpz339yBst52zKvi2tKfrz5z5zYTO166GyD9iD04c0eXIYYXlH:VYW1elER4Nkqt1Ch39+st52WvztkD14J
MD5:	77E5D1C2DBBFE347BA7AD0E9804631A7

C:\Windows\Installer\MSI1C62.tmp	
SHA1:	C5EE351655A1F9A078EBA531A0FD492D9FC91F7A
SHA-256:	BC0A8B364763524A9FEDBDBF089D57881E0EE0DB6F3ADF132E062347B22F1C5C
SHA-512:	36A36D58A17DE1357C2D616EFF08A7C73C5B4121AC8730A37837829A080C9FA414F522BA2E2ABC5C844B777AFB35E87A9E75F41E4A10774EDE85A2DF240A2D0C
Malicious:	false
Preview:	...@IXOS.@.....@.YS.@.....@.....@.....@.....@.....@.....&.{8C4E8105-89CF-42DC-B547-B756AB6C9EC5}..CSS Validator..CssValidator.msi.@.....@.. ..@.....@.....&.{2E68BFCA-136D-489B-99E7-02370AE416AC}.....@.....@.....@.....@.....@.....@.....@.....@.....CSS Validator.....Rollback..Rolling back action:....RollbackCleanup..Removing backup files..File: [1]...@.....@.....ProcessComponents..Updating component registration...@.....@.....@.]....&.{BACEFD7C-2242-4BDA-88CA-278EA0FBAC71}:.C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\.@.....@.....@.....@.....&.{E1F4536E-7D2A-4F44-81EE-727B5F105E80}..01:\Software\Hemoco bvba\CSS Validator\Version.@.....@.....@.....@.....&.{834EA0BB-8035-4ACB-9366-174CC245FFAC}C.C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\qclp2.dll.@.....@.....@.....@.....&.{F40562C3-E5CF-4975-B128-0CB43DBE0174}G.C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\audiodent.exe.@.....@.....@.....@.....&.{C321E67B-035D-49DD-B4D5-

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	
Process:	C:\Windows\System32\msiexec.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	81287
Entropy (8bit):	5.298823419018036
Encrypted:	false
SSDEEP:	192:XL/vcrZZDZo/ZrXczaIcO/gcMH5elWSLk:XDvsDZGrkaIcO/Y5Xuk
MD5:	D3BF7F2FE7D96CF90EB3393D278780A1
SHA1:	BD85EE8A111C1314DCC2658ABCA971B037E4A016
SHA-256:	37E9A251EE2D4D666A49C8252CEFCDC9344F267463F31C1D9E8D5DBEB7912D30
SHA-512:	0040AF5B6E695D9AA089C8424728510DB1D1858DF543F802A4318422EEB6B2C29D1B1904F4B161B43EA7161EB570B4F5468CD8525C6F76B7089DFB119E6365C0
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 10:38:04.497 [4552]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.513 [4552]: ngen returning 0x00000000..07/23/2020 10:38:04.559 [4480]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Word, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.559 [4480]: ngen returning 0x00000000..07/23/2020 10:38:04.622 [4256]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Common.Implementation, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:38:04.622 [

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.979283280048606
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	yRqHWQ91dT.exe
File size:	7580858
MD5:	b50ffa06eca2b3a4d92562561fc6b2d1
SHA1:	4cdbdb338a22fd11f0fcc973598e25ba54529db3
SHA256:	a181b562122fb3752137474073f22e1b2b1b4cc82a5269e73847a0e2e212cd56
SHA512:	f96b0eb15b5d8b0162b039aa83be39059ec282d2afc11f4a4dcd0069407203a48db2438e0062c197032af3e5bd8d0694ed03d703dfb424bd145c68ccf84ebc8a
SSDEEP:	196608:r175c0ur92j0iXGqUIyBOiC5Bl7l8HiX7wTPcVW1XjYvK:r175c0ur60lGqUIyBSlBhrwTP6k
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L..."$_.....f...|.....H3.....@

File Icon

Icon Hash:	f0dcdcdcdccc7830

Static PE Info

General

Entrypoint:	0x403348
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x29b48	0x29c00	False	0.0983345808383	data	3.11769658082	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 17:07:07.918047905 CEST	192.168.2.5	8.8.8.8	0x537b	Standard query (0)	get.update s.avast.cn	A (IP address)	IN (0x0001)
Oct 25, 2021 17:08:28.162395954 CEST	192.168.2.5	8.8.8.8	0x82e5	Standard query (0)	huyasos.in	A (IP address)	IN (0x0001)
Oct 25, 2021 17:08:29.209424973 CEST	192.168.2.5	8.8.8.8	0x82e5	Standard query (0)	huyasos.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 17:07:07.969619989 CEST	8.8.8.8	192.168.2.5	0x537b	Name error (3)	get.update s.avast.cn	none	none	A (IP address)	IN (0x0001)
Oct 25, 2021 17:08:29.319314003 CEST	8.8.8.8	192.168.2.5	0x82e5	No error (0)	huyasos.in		185.98.87.196	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: yRqHWQ91dT.exe PID: 5776 Parent PID: 5984

General

Start time:	17:06:28
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\yRqHWQ91dT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yRqHWQ91dT.exe'
Imagebase:	0x400000
File size:	7580858 bytes
MD5 hash:	B50FFA06ECA2B3A4D92562561FC6B2D1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: msiexec.exe PID: 3428 Parent PID: 5776

General

Start time:	17:06:30
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	msiexec /i 'C:\Users\user\AppData\Local\Temp\CssValidatorInstallerTemp\CssValidator.msi' /qn /norestart
Imagebase:	0xdf0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: msiexec.exe PID: 2952 Parent PID: 556

General

Start time:	17:06:31
Start date:	25/10/2021
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff6e40a0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Written

File Read

Registry Activities — Show Windows behavior

Analysis Process: msiexec.exe PID: 640 Parent PID: 2952

General

Start time:	17:06:34

Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 7A8FDEF089EF820D04B2E0639E42DA17
Imagebase:	0xdf0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: audiodent.exe PID: 5656 Parent PID: 2952

General

Start time:	17:06:41
Start date:	25/10/2021
Path:	C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\audiodent.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Hemoco bvba\CSS Validator\audiodent.exe
Imagebase:	0x980000
File size:	10532352 bytes
MD5 hash:	A0052D6EAC0D6D4296DE89213447416D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.462453858.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.462430424.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000002.524066037.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.462394649.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.462483110.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000009.00000002.524018514.00000000083B9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.462302321.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.462367584.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.462337552.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.462470017.0000000008A28000.00000004.00000040.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Disassembly

Code Analysis