

ID: 502664
Sample Name: CTS Graphic module for CID-Pro measurement files.msi
Cookbook: default.jbs
Time: 08:36:49
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report CTS Graphic module for CID-Pro measurement files.msi 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Analysis Advice 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 7
Contacted IPs 7
General Information 7
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASN 8
JA3 Fingerprints 8
Dropped Files 8
Created / dropped Files 8
Static File Info 13
General 13
File Icon 13
Static OLE Info 14
General 14
OLE File "CTS Graphic module for CID-Pro measurement files.msi" 14
Indicators 14
Summary 14
Streams 14
Network Behavior 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 15
Analysis Process: msiexec.exe PID: 4752 Parent PID: 1560 15
General 15
File Activities 15
Analysis Process: msiexec.exe PID: 2500 Parent PID: 556 15
General 15
File Activities 15
File Written 15
File Read 15
Registry Activities 15
Analysis Process: msiexec.exe PID: 6056 Parent PID: 2500 15
General 15
Analysis Process: msiexec.exe PID: 6300 Parent PID: 2500 16
General 16
Disassembly 16
Code Analysis 16

Copyright Joe Security LLC 2021

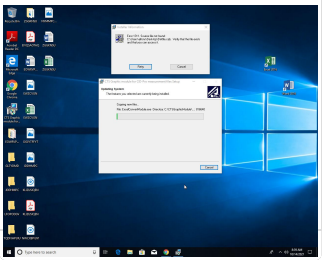
Windows Analysis Report CTS Graphic module for CID-…

Overview

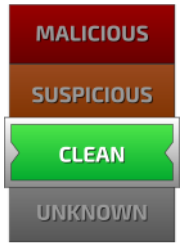
General Information

Sample Name:	CTS Graphic module for CID-Pro measurement files.msi
Analysis ID:	502664
MD5:	9d1d12f42aa3de0.
SHA1:	0a5bbbd604a5ae..
SHA256:	98d412acbb77f1f..
Infos:	

Most interesting Screenshot:



Detection

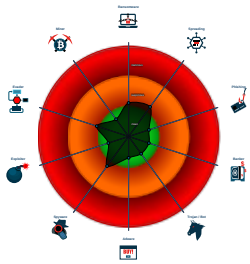


Score:	3
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Queries the volume information (nam…
- Monitors certain registry keys / valu…
- Sample file is different than original …
- Checks for available system drives …
- Found dropped PE file which has no…
- Drops PE files
- Tries to load missing DLLs
- Deletes files inside the Windows fold…
- Drops PE files to the windows direct…
- Creates files inside the system direc…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox

Sample is looking for USB drives. Launch the sample with the USB Fake Disk cookbook

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Process Tree

- **System is w10x64**
- msiexec.exe (PID: 4752 cmdline: 'C:\Windows\System32\msiexec.exe' /i 'C:\Users\user\Desktop\CTS Graphic module for CID-Pro measurement files.msi' MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 2500 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 6056 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 92B7A03B753DE557328F7B181D3A0B3D C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - msiexec.exe (PID: 6300 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding B258116E8C98C69587BFD784FAB73825 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Jbx Signature Overview

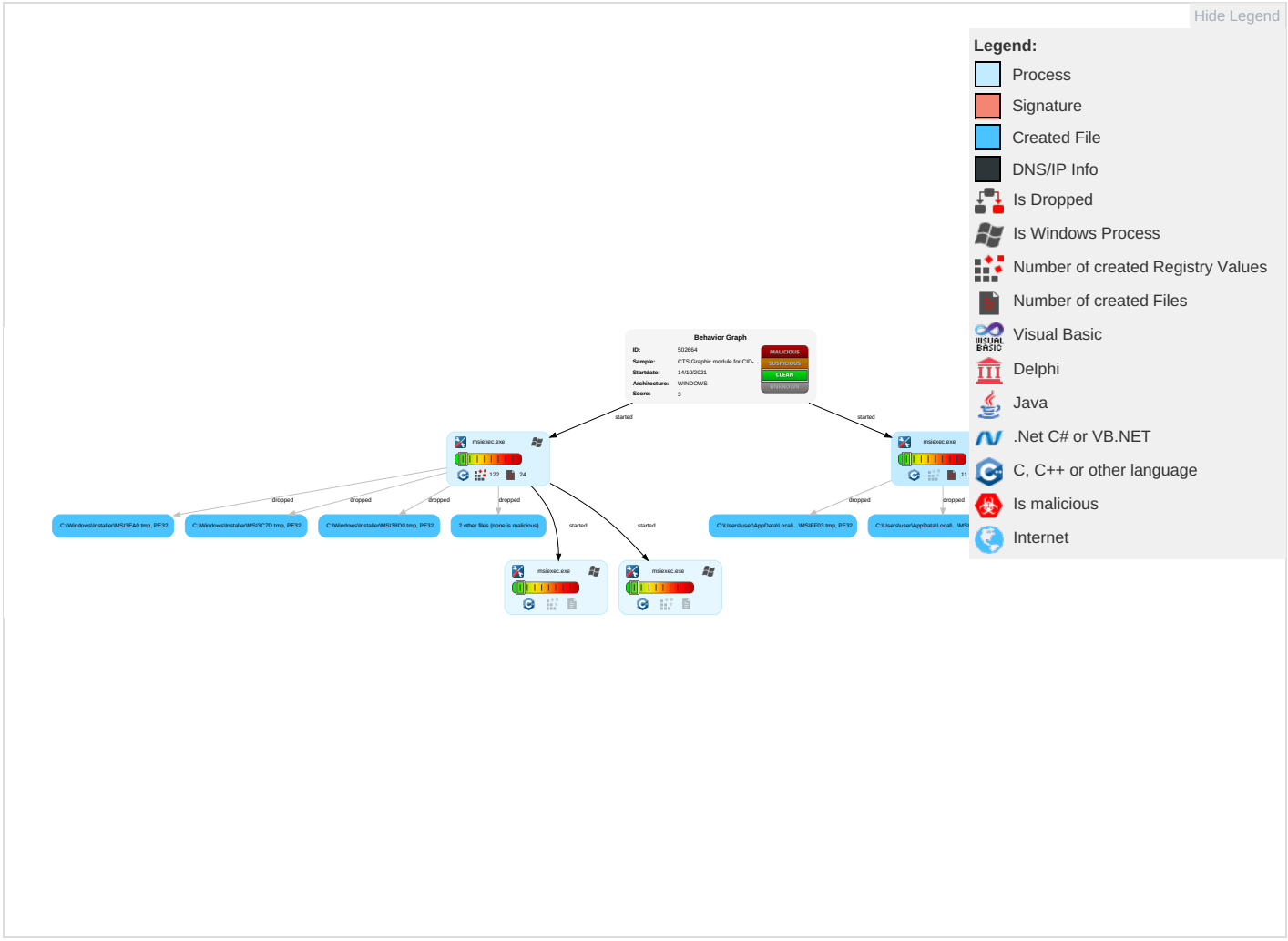
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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
Replication Through Removable Media 1	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Masquerading 2	OS Credential Dumping	Query Registry 1	Replication Through Removable Media 1	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Devic Without Authorizatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizatic
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 1	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	File Deletion 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

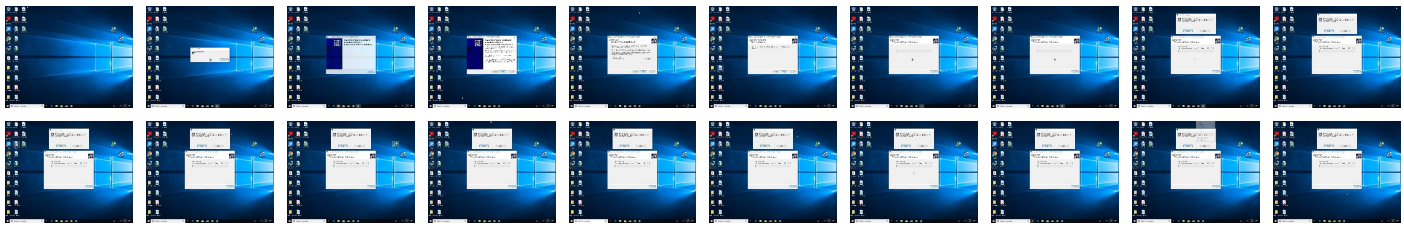
Behavior Graph

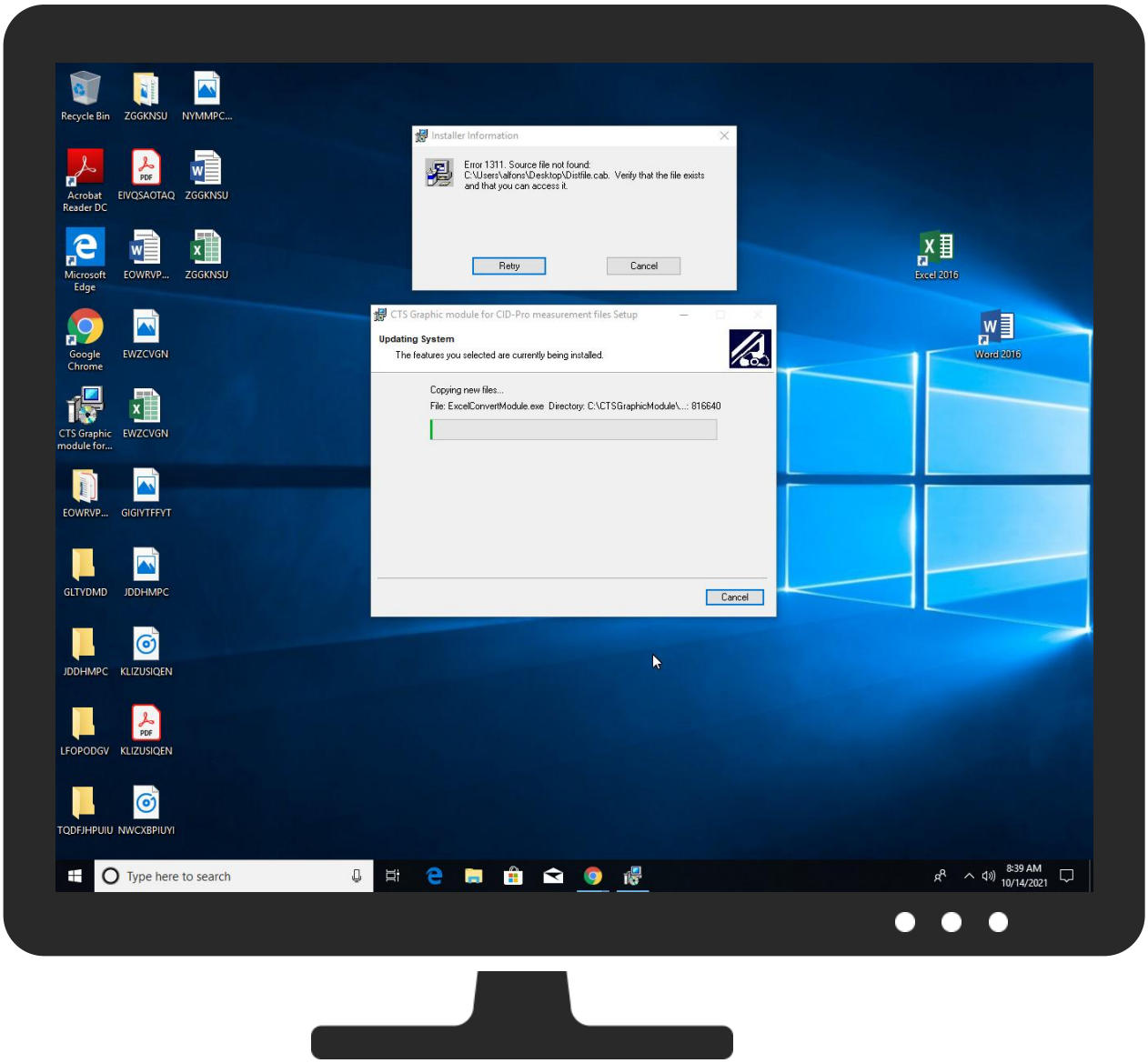


Screenshots

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
CTS Graphic module for CID-Pro measurement files.msi	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MSI195.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI195.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI5C.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI5C.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIF925.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIF925.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIFDD9.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIFDD9.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIFF03.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIFF03.tmp	0%	ReversingLabs		
C:\Windows\Installer\MSI2E3F.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSI2E3F.tmp	2%	ReversingLabs		
C:\Windows\Installer\MSI37D5.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSI37D5.tmp	2%	ReversingLabs		
C:\Windows\Installer\MSI38D0.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSI38D0.tmp	0%	ReversingLabs		

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\Windows\Installer\MSI3C7D.tmp	0%	Metadefender		Browse
C:\Windows\Installer\MSI3C7D.tmp	2%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.cts-umweltsimulation.de	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://https://www.cts-umweltsimulation.de%	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502664
Start date:	14.10.2021
Start time:	08:36:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CTS Graphic module for CID-Pro measurement files.msi
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:	CLEAN

Copyright Joe Security LLC 2021

Classification:	clean3.winMSI@6/15@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .msi
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Config.Msi\4629bc.rbs	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	12266
Entropy (8bit):	5.007776556313955
Encrypted:	false
SSDEEP:	192:RvSxQntLWvZW3fpiYmY2BIi1BClmDacA/O1hhhhj:R6xQntLWhWPgRBIi7ClmucA/w
MD5:	BB7FD55E83D560A2582510B25F862B00
SHA1:	D19CD3B9BB969738F2BEDDBE2D84D49E94DDD732
SHA-256:	04C43C0A5DD03C48B7981B782EAD83991829B5085EACB7B5C7D6C86C7661D2F7
SHA-512:	AF2954A597366B07C2BAA0877E92D696DC2FC28CFF79FDFAB1D78DFBA29C9277D3D88722D05E37CB95252E3CA14E804FF49A79233FAC68ADB985398070320BA F
Malicious:	false
Reputation:	low

C:\Config.Msi\4629bc.rbs	
Preview:	...@IXOS.@.....@.DNS.@.....@.....@.....@.....@.....@.....&.{DE800F69-955C-4883-BAFF-CB2110B8D24E}0.CTS Graphic module for CID-Pro measurement files4.CTS Graphic module for CID-Pro measurement files.msi.@.....@.....@.....@.....@.....&.{20A29E39-AE61-4E1D-8B05-2B53D975F455}.....@.....@.....@.....@.....@.....@.....@.....@.....@....0.CTS Graphic module for CID-Pro measurement files.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files.....File: [1]....ProcessComponents".Updating component registration.....&.{4CFD70BB-BCEE-4D6A-8FE0-3623C008CCE6}&.{DE800F69-955C-4883-BAFF-CB2110B8D24E}.@.....&.{50861030-DAC5-46F4-9701-8F52634854BD}&.{DE800F69-955C-4883-BAFF-CB2110B8D24E}.@.....&.{C05F4450-0A87-450B-87D5-2BB1C0EF5D1B}&.{DE800F69-955C-4883-BAFF-CB2110B8D24E}.@.....&.{08EF03B2-6164-47CA-B1C1-FDA8498EEE7E}&.{DE800F69-955C-4883-BAFF-CB2110B8D24E}.@.....&.{C0519341-0995-4225-81F9-4D502FC84490}&.{DE800F69-955C-4883-BAFF-CB2110B8D24E}.@.....&.{49066991-6467-4D74-B757-D37

C:\Users\user\AppData\Local\Temp\MSI195.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604608
Entropy (8bit):	6.120901544049748
Encrypted:	false
SSDEEP:	12288:sjso0X+9aNVnZy3aDczIh0eBqmOInKiGc/wRBUXUiqGqIZ:O0nMKbVOIKRswRiXUiqGqIZ
MD5:	7B2E16B40253B3664BD209416E40D832
SHA1:	0B8F4C27D7C366E19EBDFA6DCC4540EF46F76F26
SHA-256:	5479A842EDE9595A950BBC70A1FA52622F64FC80971AEF689C22701FFC506C9A
SHA-512:	425D57105DC80008F06C96AF06726B470D753F32F5159706A20579FBAFA1465055C2605DA754B51644E0171A6BE1FE374C0003D507C8827515341C1628EEA94D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....y.]....%.....d.....~.....h.....n.....k.....Rich..... ..PE..L...i..Y.....!.....H.....`.....p.....`..... .....h.....?.....O.....[..@.....`..... text...JG.....H..... ..`.rdata..3....`.....L.....@..@.data.....@....rsrc.....@..@.reloc.....x.....@..B..... ....

C:\Users\user\AppData\Local\Temp\MSI5C.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604608
Entropy (8bit):	6.120901544049748
Encrypted:	false
SSDEEP:	12288:sjso0X+9aNVnZy3aDczIh0eBqmOInKiGc/wRBUXUiqGqIZ:O0nMKbVOIKRswRiXUiqGqIZ
MD5:	7B2E16B40253B3664BD209416E40D832
SHA1:	0B8F4C27D7C366E19EBDFA6DCC4540EF46F76F26
SHA-256:	5479A842EDE9595A950BBC70A1FA52622F64FC80971AEF689C22701FFC506C9A
SHA-512:	425D57105DC80008F06C96AF06726B470D753F32F5159706A20579FBAFA1465055C2605DA754B51644E0171A6BE1FE374C0003D507C8827515341C1628EEA94D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....y.]....%.....d.....~.....h.....n.....k.....Rich..... ..PE..L...i..Y.....!.....H.....`.....p.....`..... .....h.....?.....O.....[..@.....`..... text...JG.....H..... ..`.rdata..3....`.....L.....@..@.data.....@....rsrc.....@..@.reloc.....x.....@..B..... ....

C:\Users\user\AppData\Local\Temp\MSI602bb.LOG	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Temp\MSI602bb.LOG	
Preview:	..

C:\Users\user\AppData\Local\Temp\MSIF925.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604608
Entropy (8bit):	6.120901544049748
Encrypted:	false
SSDEEP:	12288:sjso0X+9aNVnZy3aDczIh0eBqmOInKiGc/wRBUXUiqGqIZ:O0nMKbVOIKRswRiXUiqGqIZ
MD5:	7B2E16B40253B3664BD209416E40D832
SHA1:	0B8F4C27D7C366E19EBDFA6DCC4540EF46F76F26
SHA-256:	5479A842EDE9595A950BBC70A1FA52622F64FC80971AEF689C22701FFC506C9A
SHA-512:	425D57105DC80008F06C96AF06726B470D753F32F5159706A20579FBAFA1465055C2605DA754B51644E0171A6BE1FE374C0003D507C8827515341C1628EEA94D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....y.]....%.....d.....~.....h.....n.....k.....Rich..... ..PE..L...i..Y.....!.....H.....`.....p.....`..... .....h.....?.....O.....[..@.....`..... text...JG.....H..... ..`.rdata..3...`.....L.....@..@.data.....@....rsrc.....@..@.reloc.....x.....@..B..... ....

C:\Users\user\AppData\Local\Temp\MSIFDD9.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604608
Entropy (8bit):	6.120901544049748
Encrypted:	false
SSDEEP:	12288:sjso0X+9aNVnZy3aDczIh0eBqmOInKiGc/wRBUXUiqGqIZ:O0nMKbVOIKRswRiXUiqGqIZ
MD5:	7B2E16B40253B3664BD209416E40D832
SHA1:	0B8F4C27D7C366E19EBDFA6DCC4540EF46F76F26
SHA-256:	5479A842EDE9595A950BBC70A1FA52622F64FC80971AEF689C22701FFC506C9A
SHA-512:	425D57105DC80008F06C96AF06726B470D753F32F5159706A20579FBAFA1465055C2605DA754B51644E0171A6BE1FE374C0003D507C8827515341C1628EEA94D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....y.]....%.....d.....~.....h.....n.....k.....Rich..... ..PE..L...i..Y.....!.....H.....`.....p.....`..... .....h.....?.....O.....[..@.....`..... text...JG.....H..... ..`.rdata..3...`.....L.....@..@.data.....@....rsrc.....@..@.reloc.....x.....@..B..... ....

C:\Users\user\AppData\Local\Temp\MSIFF03.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	69120
Entropy (8bit):	6.280368727841982
Encrypted:	false
SSDEEP:	1536:T5NvYhdShE4p6sBSa/GrTywTwJe1gvxxTtO7m2Uod:TTvwdS6+c8M1gvxdtO7m2X
MD5:	5E71204F63B88FA31CC06D04141198BE
SHA1:	69CEB4C33B98C0D0583224DE9A5DADE8A3903992
SHA-256:	774B7B8BF714746E62A096AEEBAFEADF37E168D978764F14136ED96A85692326
SHA-512:	9E0665EDB50CECC01382A991C36FF2AC045B5E25E917FC08D8A8748077B39BB14192027A303052733F896B308C74ED5B7B76A7E9770C9064B4AD0E52F7B1BC42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2..a..a..a..a..a...a..a...a..aH..a..a...a..a..a..a...a..a...a'..a. .a...a..aRich..a.....PE..L.....DJ.....!.....1J.....U...\...d....P..h.....`..l...p.....(...H..... ....l.....text..... ..`.rdata...3.....4.....@..@.data....L.....@....rsrc...h....P.....@..@.reloc..x....`.....@. .B..... .....

C:\Windows\Installer\4629bb.msi	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, MSI Installer, Code page: 0, Number of Characters: 0, Number of Pages: 200, Templa te: ;9, Number of Words: 0, Revision Number: {20A29E39-AE61-4E1D-8B05-2B53D975F455}, Security: 0, Last Printed: Tue Oct 5 09:00:44 2021, Create Time/Date: Tue Oct 5 09:00:44 2021, Last Saved Time/Date: Tue Oct 5 09:00:44 2021
Category:	dropped
Size (bytes):	1644032
Entropy (8bit):	6.375958109922464
Encrypted:	false
SSDEEP:	24576:wv8/R6wC9Ab7MX/Z9cSqGqIqo/2m3F3d0nMKbVOIKRswRiXUiqGqIFj:wv8okwvkq/WOI3vXz
MD5:	9D1D12F42AA3DE041DDA288F87CED756
SHA1:	0A5BBBD604A5AE6845C4A389EF1F85708D3C679F
SHA-256:	98D412ACBB77F1FD865E17F16C62AE1E53FE3E19A183B3BA2D89C4FC3BD43FD1
SHA-512:	9CE4D8EE73792878FD625D58757F2C91710D319C2A2DC9FF18CE87BD39222E67C1B94FC0CFC3E20259FE99D1B098659E90F2A492B911CA8FEBFAB822B6444A9
Malicious:	false
Preview:	.....>.....o..... ....!...".#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...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...[...\...]...^..._...`...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\MSI2E3F.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604608
Entropy (8bit):	6.120901544049748
Encrypted:	false
SSDEEP:	12288:sjso0X+9aNVnZy3aDczIh0eBqmOInKiGc/wRBUXUiqGqIZ:O0nMKbVOIKRswRiXUiqGqIZ
MD5:	7B2E16B40253B3664BD209416E40D832
SHA1:	0B8F4C27D7C366E19EBDFA6DCC4540EF46F76F26
SHA-256:	5479A842EDE9595A950BBC70A1FA52622F64FC80971AEF689C22701FFC506C9A
SHA-512:	425D57105DC80008F06C96AF06726B470D753F32F5159706A20579FBAFA1465055C2605DA754B51644E0171A6BE1FE374C0003D507C8827515341C1628EEA94D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....y.]....%.....d.....~.....h.....n.....k.....Rich..... ..PE..L...i..Y.....!.....H.....`.....p.....`..... .....h.....?.....O.....[..@.....`..... text...JG.....H..... ..`.rdata..3....`.....L.....@..@.data.....@....rsrc.....@..@.reloc.....x.....@..B..... ....

C:\Windows\Installer\MSI37D5.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604608
Entropy (8bit):	6.120901544049748
Encrypted:	false
SSDEEP:	12288:sjso0X+9aNVnZy3aDczIh0eBqmOInKiGc/wRBUXUiqGqIZ:O0nMKbVOIKRswRiXUiqGqIZ
MD5:	7B2E16B40253B3664BD209416E40D832
SHA1:	0B8F4C27D7C366E19EBDFA6DCC4540EF46F76F26
SHA-256:	5479A842EDE9595A950BBC70A1FA52622F64FC80971AEF689C22701FFC506C9A
SHA-512:	425D57105DC80008F06C96AF06726B470D753F32F5159706A20579FBAFA1465055C2605DA754B51644E0171A6BE1FE374C0003D507C8827515341C1628EEA94D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....y.]....%.....d.....~.....h.....n.....k.....Rich..... ..PE..L...i..Y.....!.....H.....`.....p.....`..... .....h.....?.....O.....[..@.....`..... text...JG.....H..... ..`.rdata..3....`.....L.....@..@.data.....@....rsrc.....@..@.reloc.....x.....@..B..... ....

C:\Windows\Installer\MSI38D0.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	69120

C:\Windows\Installer\MSI38D0.tmp	
Entropy (8bit):	6.280368727841982
Encrypted:	false
SSDEEP:	1536:T5NvYhdShE4p6sBSa/GrTywTwJe1gvxxTtO7m2Uod:TTvwdS6+c8M1gvxdtO7m2X
MD5:	5E71204F63B88FA31CC06D04141198BE
SHA1:	69CEB4C33B98C0D0583224DE9A5DADE8A3903992
SHA-256:	774B7B8BF714746E62A096AEEBAFEADF37E168D978764F14136ED96A85692326
SHA-512:	9E0665EDB50CECC01382A991C36FF2AC045B5E25E917FC08D8A8748077B39BB14192027A303052733F896B308C74ED5B7B76A7E9770C9064B4AD0E52F7B1BC42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2..a..a..a..a..a..a..a..aH..a..a...a..a..a..a..a..a..a'..a. .a...a..aRich..a.....PE..L.....DJ.....!.....1J.....U...\...d....P..h.....`.l...p.....(...H..... ....I.....text..... ..`.rdata...3.....4.....@..@.data....L.....@....rsrc...h....P.....@..@.reloc..x...`.....@. .B..... .....

C:\Windows\Installer\MSI3C7D.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604608
Entropy (8bit):	6.120901544049748
Encrypted:	false
SSDEEP:	12288:sjso0X+9aNVnZy3aDczIh0eBqmOInKiGc/wRBUXUiqGqIZ:O0nMKbVOIKRswRiXUiqGqIZ
MD5:	7B2E16B40253B3664BD209416E40D832
SHA1:	0B8F4C27D7C366E19EBDFA6DCC4540EF46F76F26
SHA-256:	5479A842EDE9595A950BBC70A1FA52622F64FC80971AEF689C22701FFC506C9A
SHA-512:	425D57105DC80008F06C96AF06726B470D753F32F5159706A20579FBAFA1465055C2605DA754B51644E0171A6BE1FE374C0003D507C8827515341C1628EEA94D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....y.]....%.....d.....~.....h.....n.....k.....Rich..... ..PE..L...i..Y.....!.....H.....`.....p.....`..... .....h.....?.....O.....[..@.....`..... text...JG.....H..... ..`.rdata..3....`.....L.....@..@.data.....@....rsrc.....@..@.reloc.....x.....@..B..... ....

C:\Windows\Installer\MSI3EA0.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	604608
Entropy (8bit):	6.120901544049748
Encrypted:	false
SSDEEP:	12288:sjso0X+9aNVnZy3aDczIh0eBqmOInKiGc/wRBUXUiqGqIZ:O0nMKbVOIKRswRiXUiqGqIZ
MD5:	7B2E16B40253B3664BD209416E40D832
SHA1:	0B8F4C27D7C366E19EBDFA6DCC4540EF46F76F26
SHA-256:	5479A842EDE9595A950BBC70A1FA52622F64FC80971AEF689C22701FFC506C9A
SHA-512:	425D57105DC80008F06C96AF06726B470D753F32F5159706A20579FBAFA1465055C2605DA754B51644E0171A6BE1FE374C0003D507C8827515341C1628EEA94D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....y.]....%.....d.....~.....h.....n.....k.....Rich..... ..PE..L...i..Y.....!.....H.....`.....p.....`..... .....h.....?.....O.....[..@.....`..... text...JG.....H..... ..`.rdata..3....`.....L.....@..@.data.....@....rsrc.....@..@.reloc.....x.....@..B..... ....

C:\Windows\Installer\MSI4009.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	33204
Entropy (8bit):	5.781528710286994
Encrypted:	false
SSDEEP:	768:ARn1Quy6ZHvuY+G/Zac42/BXwZImqtJuaWSu3VadWxXaHb9UlwLWV:j6ZHvSTIHtJuaWSu3nxXaHbKSLm
MD5:	4361606AADC73C549CD272AAC37450F1
SHA1:	E0BAEA354D4E46480D70937FD8E822DBBFFC6BE6

C:\Windows\Installer\MSI4009.tmp	
SHA-256:	0486BD89E1670D82D920D0CFC68F285C0832257D20156C51E64B8017F7DDA572
SHA-512:	864CC4F79AE2210058620E24CB3163CA296385102C00A20CEC5AE20381230D7A47D7DA87F114D6483062BD8F4BBA135A2705858F7588310A92135C02D421DB19
Malicious:	false
Preview:	...@IXOS.@.....@.DNS.@.....@.....@.....@.....@.....@.....&.{DE800F69-955C-4883-BAFF-CB2110B8D24E}0.CTS Graphic module for CID-Pro measurement files4.CTS Graphic module for CID-Pro measurement files.msi.@.....@.....@.....@.....@.....&.{20A29E39-AE61-4E1D-8B05-2B53D975F455}.....@.....@.....@.....@.....@.....@.....@.....@.....@....0.CTS Graphic module for CID-Pro measurement files.....Rollback..Rolling back action:..[1]..RollbackCleanup..Removing backup files.....File: [1]...@.....@.....@.....ProcessComponents".Updating component registration.....@o....@.....@.]....&.{4CFD70BB-BCEE-4D6A-8FE0-3623C008CCE6}*.C:\CTSGraphicModule\ExcelConvert Module.exe.@.....@.....@.....@.....&.{50861030-DAC5-46F4-9701-8F52634854BD}..C:\CTSGraphicModule\mesa.dll.@.....@.....@.....@.....&.{C05F4450-0A87-450B-87D5-2BB1C0EF5D1B}0.C:\CTSGraphicModule\manual\CID500_manual_eng.pdf.@.....@.....@.....@.....&.{08EF03B2-6164-47CA-B1C1-FDA8498EEE7E}0.C:\CTSGraphicModule\manual\CID500_manual_deu.pdf.@.....@.....@

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):	5.29872828603926
Encrypted:	false
SSDEEP:	192:XL/vcrZZDZo/ZrXczaIcO/gcMH5elWSLc:XDvsDZGrkaIcO/Y5Xuc
MD5:	A08D323CCBCCD65F1E7803A241663B5B
SHA1:	AEEDBBCD6F99F32FA8DC22178D86B0AADD3C7048
SHA-256:	D59464B087080FBEFC1390989BAB8DC2B1A455C196825E8AF14FF98C6A456367
SHA-512:	0D75E874965D28FCD2450898010946A23D39CA21951E2789A140C2F42978DCEBF7D021E08B609A4E1F86DF24CE17164553DC2A561E7E3D6B7B8CAAD9FF0A8E7
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:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, MSI Installer, Code page: 0, Number of Characters: 0, Number of Pages: 200, Template: ;9, Number of Words: 0, Revision Number: {20A29E39-AE61-4E1D-8B05-2B53D975F455}, Security: 0, Last Printed: Tue Oct 5 09:00:44 2021, Create Time/Date: Tue Oct 5 09:00:44 2021, Last Saved Time/Date: Tue Oct 5 09:00:44 2021
Entropy (8bit):	6.375958109922464
TrID:	• Microsoft Windows Installer (77509/1) 52.18% • Windows SDK Setup Transform Script (63028/2) 42.43% • Generic OLE2 / Multistream Compound File (8008/1) 5.39%
File name:	CTS Graphic module for CID-Pro measurement files.msi
File size:	1644032
MD5:	9d1d12f42aa3de041dda288f87ced756
SHA1:	0a5bbbd604a5ae6845c4a389ef1f85708d3c679f
SHA256:	98d412acbb77f1fd865e17f16c62ae1e53fe3e19a183b3ba2d89c4fc3bd43fd1
SHA512:	9ce4d8ee73792878fd625d58757f2c91710d319c2a2dc9ff18ce87bd39222e67c1b94fc0cfc3e20259fe99d1b098659e90f2a492b911ca8febfab822b6444a91
SSDEEP:	24576:wv8/R6wC9Ab7MX/Z9cSqGqIqo/2m3F3d0nMKbVOIKRswRiXUiqGqIFj:wv8okwvkq/WOI3vXz
File Content Preview:	.....>..... .....o..... .....

File Icon



Icon Hash:	a2a0b496b2caca72

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "CTS Graphic module for CID-Pro measurement files.msi"

Indicators

Has Summary Info:	True
Application Name:	
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Code Page:	0
Title:	
Subject:	
Author:	
Keywords:	
Comments:	
Template:	;9
Last Saved By:	
Revion Number:	{20A29E39-AE61-4E1D-8B05-2B53D975F455}
Last Printed:	2021-10-05 08:00:44.006472
Create Time:	2021-10-05 08:00:44.006472
Last Saved Time:	2021-10-05 08:00:44.006472
Number of Pages:	200
Number of Words:	0
Number of Characters:	0
Creating Application:	
Security:	0

Streams

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: msiexec.exe PID: 4752 Parent PID: 1560

General

Start time:	08:37:50
Start date:	14/10/2021
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\msiexec.exe' /i 'C:\Users\user\Desktop\CTS Graphic module for CID-Pro measurement files.msi'
Imagebase:	0x7ff69b980000
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

Analysis Process: msiexec.exe PID: 2500 Parent PID: 556

General

Start time:	08:37:51
Start date:	14/10/2021
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff69b980000
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: 6056 Parent PID: 2500

General

Start time:	08:37:52
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\msiexec.exe

Copyright Joe Security LLC 2021

Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 92B7A03B753DE557328F7B181D3A0B3DC
Imagebase:	0x10000
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: msiexec.exe PID: 6300 Parent PID: 2500

General

Start time:	08:38:06
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding B258116E8C98C69587BFD784FAB73825
Imagebase:	0x10000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021