ID: 882704
Sample Name:
Standard_Monitor_Driver_Signed_Win10_x64.exe
Cookbook: default.jbs
Time: 17:15:51
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

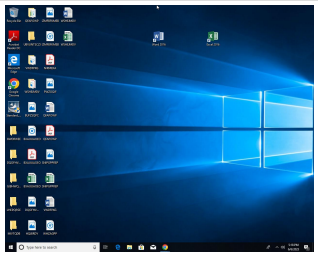
Windows Analysis Report

Standard_Monitor_Driver_Signed_Win10_x64.exe

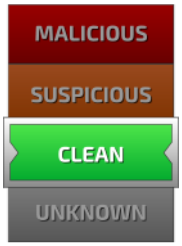
Overview

General Information

Sample Name:	Standard_Monitor_Driver_Signed_Win10_x64.exe
Analysis ID:	882704
MD5:	cf77f6850ff98d…
SHA1:	ccba9f71b67bd..
SHA256:	d81e3afb0a8a8..
Infos:	



Detection

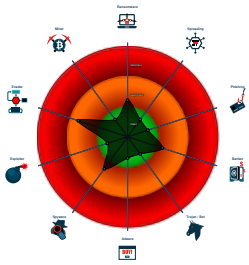


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	20%

Signatures

- Uses 32bit PE files
- Queries the volume information (nam…
- Drops certificate files (DER)
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- PE file contains sections with non-s…
- Detected potential crypto function
- Found potential string decryption / a…
- Sample execution stops while proce…
- Contains functionality to dynamicall…
- Found dropped PE file which has no…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox
Sample has a GUI, but Joe Sandbox has not found any clickable buttons, likely more UI automation may extend behavior
Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")
Sample searches for specific file, try point organization specific fake files to the analysis machine

Process Tree

- **System is w10x64**
- Standard_Monitor_Driver_Signed_Win10_x64.exe (PID: 7148 cmdline: C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe MD5: CF77F6850FF98D1B681832160F2691FE)
  - Setup.exe (PID: 7132 cmdline: C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.exe MD5: 1AEB989E361AF85F5099DE3DA25457F4)
    - IKernel.exe (PID: 5220 cmdline: "C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe" -RegServer MD5: B3FD01873BD5FD163AB465779271C58F)
- IKernel.exe (PID: 1852 cmdline: C:\PROGRA~2\COMMON~1\INSTAL~1\user\6\INTEL3~1\IKernel.exe -Embedding MD5: B3FD01873BD5FD163AB465779271C58F)
  - IKernel.exe (PID: 7140 cmdline: "C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\iKernel.exe" /REGSERVER MD5: B3FD01873BD5FD163AB465779271C58F)
  - cmd.exe (PID: 7040 cmdline: cmd.exe /c C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon find monitor* > mon.txt MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - devcon.exe (PID: 4400 cmdline: C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon find monitor* MD5: 337FF45A8FD5B7BE152508EBC2E584CA)
  - cmd.exe (PID: 7136 cmdline: cmd.exe /c C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon update MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - devcon.exe (PID: 7088 cmdline: C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon update MD5: 337FF45A8FD5B7BE152508EBC2E584CA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

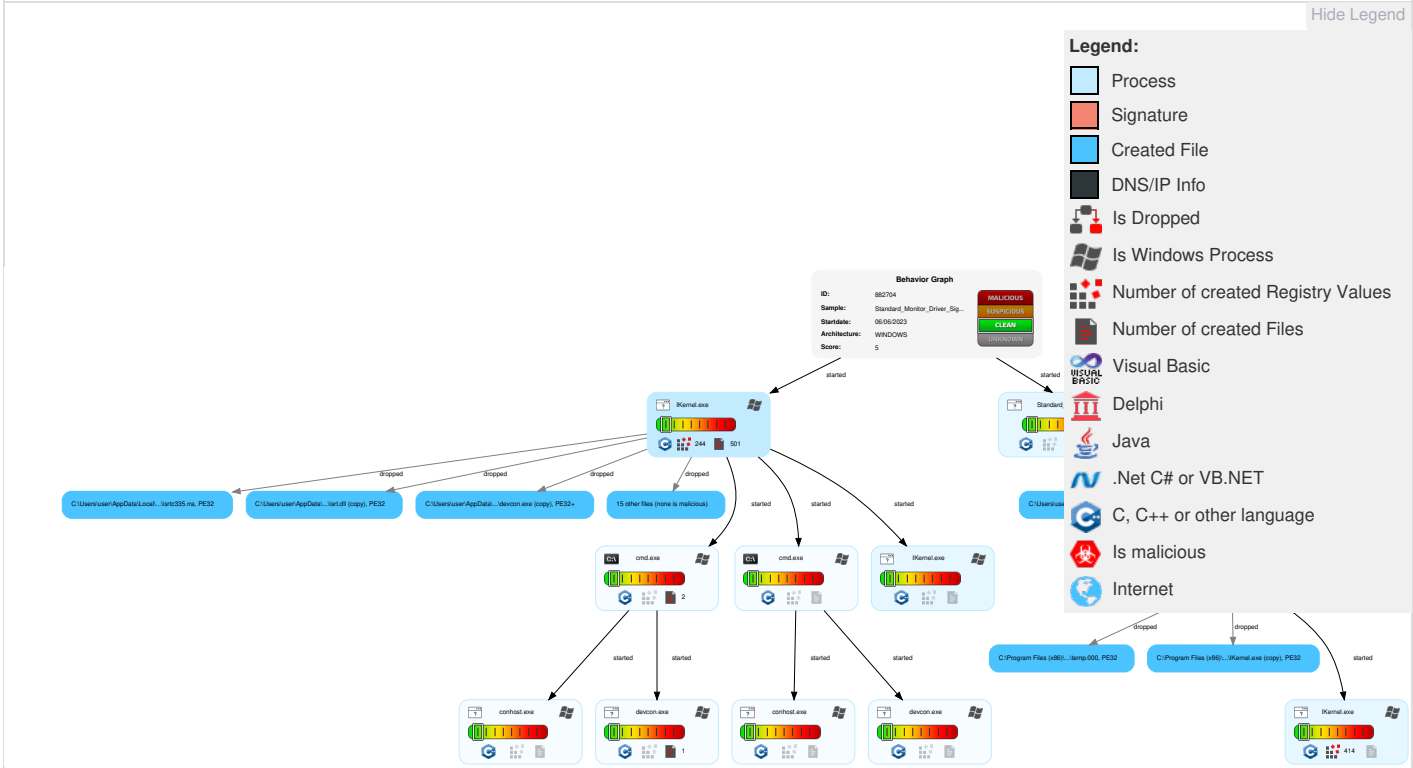
Joe Sandbox Signatures

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	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 Access Token Manipulation	2 1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 2 Process Injection	1 Access Token Manipulation	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	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 2 Process Injection	Security Account Manager	1 Process 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 Deobfuscate/Decode Files or Information	NTDS	4 File and Directory Discovery	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	2 Obfuscated Files or Information	LSA Secrets	1 5 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

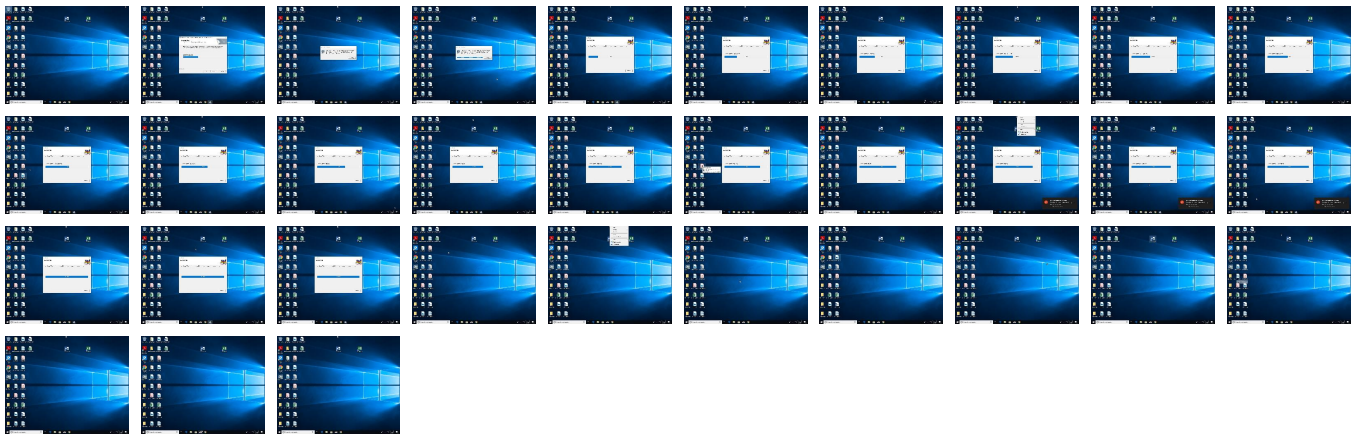
Behavior Graph



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
Standard_Monitor_Driver_Signed_Win10_x64.exe	0%	ReversingLabs		
Standard_Monitor_Driver_Signed_Win10_x64.exe	0%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe (copy)	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\ctorbcec.rra	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\iusebde6.rra	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\objebdb7.rra	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\temp.000	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\IScript\iscrbeb1.rra	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\IScript\iscript.dll (copy)	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\ctor.dll (copy)	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\iuser.dll (copy)	0%	ReversingLabs		
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\objectps.dll (copy)	0%	ReversingLabs		
C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\Setucb05.rra	0%	ReversingLabs		
C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\Setup.exe (copy)	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}_IsRc3c2.rra	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}_IsRes.dll (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}_IsUc299.rra	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}_IsUser.dll (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcc23b.rra	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon.exe (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\isrt.dll (copy)	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\isrtc335.rra	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.viewsonic.com.cndesc	0%	Avira URL Cloud	safe	
http://www.viewsonic.comXYZ	0%	Avira URL Cloud	safe	
http://www.viewsonic.com.cn	0%	Avira URL Cloud	safe	
http://www.installuser.com/user/	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://www.viewsonic.com.cn	lKernel.exe, 00000003.00000003.515919292.0000000002B1B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.viewsonic.comXYZ	lKernel.exe, 00000003.00000003.533702562.0000000002B1B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.installuser.com/user/	lKernel.exe, 00000003.00000003.581439915.0000000002AF3000.00000004.00000020.00020000.00000000.sdmp, lKernel.exe, 00000003.00000003.580553661.0000000002ADB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.viewsonic.com	lKernel.exe, 00000003.00000003.533702562.0000000002B1B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.viewsonic.com.cndesc	lKernel.exe, 00000003.00000003.519124556.0000000002B1B000.00000004.00000020.00020000.00000000.sdmp, lKernel.exe, 00000003.00000003.515919292.0000000002B1B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882704
Start date and time:	2023-06-06 17:15:51 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
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
Sample file name:	Standard_Monitor_Driver_Signed_Win10_x64.exe
Detection:	CLEAN
Classification:	clean5.winEXE@18/1146@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.9% (good quality ratio 97.4%) • Quality average: 79.3% • Quality standard deviation: 24.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe
- Created / dropped Files have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtWriteFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe (copy)

Process:	C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	614532
Entropy (8bit):	6.195803070094149
Encrypted:	false
SSDEEP:	6144:cTqa+rypBCk+Fx7/BCttXXikQklSn8nbFpBJkCcjaIJ/M6HnpJpaijgBwTFg56lX:fr/SlSBUJjnNRjpTWamB4
MD5:	B3FD01873BD5FD163AB465779271C58F
SHA1:	E1FF9981A09AB025D69AC891BFC931A776294D4D
SHA-256:	985EB55ECB750DA812876B8569D5F1999A30A24BCC54F9BAB4D3FC44DFEDB931
SHA-512:	6674AB1D65DA9892B7DD2FD37F300E087F58239262D44505B53379C676FD16DA5443D2292AEAAE01D3E6C40960B12F9CAC651418C827D2A33C29A6CDF874BE4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1"\.PL..PL..PL..L@..PL.?LB..PL.TOF..PL.TOG..PL..O_..PL..PL..PL..PM.oPL..s_..PL.CpF..PL.CpG..PL.{VJ..PL.Rich.PL.....PE..L...lh@=...../.....@.....text...Z..... ..`.rdata..`T.....`.....@..@.data...\.... ...P... .....@....rsrc.....p.....@..@.....

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\corebc8e.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	28529
Entropy (8bit):	4.000373969114487
Encrypted:	false
SSDEEP:	384:2ERJ48bJNafWlc/n++TOa2SZ4+CIPo2S4m:2ER3JNaM+MJIPo27m
MD5:	62D5F9827D867EB3E4AB9E6B338348A1
SHA1:	828E72F9C845B1C0865BADAEF40D63FB36447293
SHA-256:	5214789C08EE573E904990DCD29E9E03AAF5CF12E86FAE368005FD8F4E371BD5
SHA-512:	B38BB74DC2E528C2A58A7D14A07BD1ECAAF55168B53AFC8F4718F3BF5D6F8C8B922B98551A355EBB1009F23CFF02FD8596413468993A43756C4DE7DFED57373 2
Malicious:	false
Preview:	; Corecomp.ini..;..; This file stores information about files that InstallShield..; will install to the Windows\System folder, such as Windows..; 95 and NT 4.0 core components and DAO, ODBC, and ActiveX files...; ..; The entries have the following format, without a space before ..; or after the equal sign:..;..; <file name>=<properties>..; ..; Currently, following properties are supported:..; 0x00000000 No registry entry is created for this file. It is..; not logged for uninstallation, and is therefore ..; never removed...;..; Inappropriate modification to this file can prevent an..; application from getting Windows 95/Windows NT logo...;..; Last Updated: 12/8/1999; bn....[Win32]....12500852.CPX=0x00000000 ..12510866.CPX=0x00000000 ..12520437.cpx=0x00000000..12520850.cpx=0x00000000..12520860.CPX=0x00000000..12520861.CPX=0x00000000 ..12520863.CPX=0x00000000 ..12520865.CPX=0x00000000..82557ndi.dll=0x00000000..8514a.dll=0x00000000..95fiber.dll=0x000

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\ctorbcec.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe

File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	5.420648120129751
Encrypted:	false
SSDEEP:	768:uj5UUtenZewInMM66FwMd21I1FNVBt3NogjISsK7phsfTkF0kN1usI5FrAg1OBoM:Q5PI9F6SCdNoe57phsgW7Ag8lj
MD5:	003A6C011AAC993BCDE8C860988CE49B
SHA1:	6D39D650DFA5DED45C4E0CB17B986893061104A7
SHA-256:	590BE865DDF8C8D0431D8F92AA3948CC3C1685FD0649D607776B81CD1E267D0A
SHA-512:	032ABA4403EB45646AA1413FDC6C5D08BAAB4D0306D20B4209E70C84E47F6B72E68457BBC4331A5F1A5FA44AA776A89EB9FD29D0D956FA2FE11364C26AB09E E7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9l..}..L}..L}..L...Ly..L.-.Lx..L}..Lx..L+..Lv..L}..L=..L$..Lt..L.-.L{..L ...L|..L.-.L|..LRich}..L.....PE..L....;.....!....p.....i.....0.....@.....x.....l..... ..... 4.....text....k.....p..... ..`.rdata..'..... .....@..@.data.....@....rsrc....l.....p.....@..@.reloc..... ....@..B.. .....

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\iusebde6.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	176128
Entropy (8bit):	6.103238184891712
Encrypted:	false
SSDEEP:	3072:r+qN/OeBOZOptEHrOM/JUb1pZHYJvY6zsB7qAJy/Km1kUpbVxgr:5/bPtQxJUb1pdGQ6z73vzpbV6r
MD5:	377765FD4DE3912C0F814EE9F182FEDA
SHA1:	A0AB6A28F4BA057D5EAE5C223420EB599CD4D3B1
SHA-256:	8EFCBD8752D8BBFD7EE559502D1AA28134C9BF391BF7FC5CE6FDFD4473599AFB
SHA-512:	31BEFB11715F78043B7684287B4086CE003CB66F97C6EFF8C2B438EAE29045D8856172C6B898BE9F08C139EDC4647C2BCE000DA497AED208B7A5A69D4D90C7 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<`.]...]...]...A...]..yB...]...A...]..n}...]..yB...]...]...]...B...]...~...]...]. .D]..n}...]..V[...]..n}...]..Rich.].....PE..L....;.....!....p...@..... ..... .....@..... .....X.....text....m.....p..... ..`.rdata...>.....@.....@..@.data....-..... .....@....rsrc... .....@..@.reloc...$.....0.. .....@..B.....

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\objebdb7.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	2.240898610474827
Encrypted:	false
SSDEEP:	192:Ec9t9ShCx1JQ5BoQZgTWPLnOBog5MOSiYp7e9MCMWnaaAyqX:EAxoVgTNk9sM9pE
MD5:	8F02B204853939F8AEFE6B07B283BE9A
SHA1:	C161B9374E67D5FA3066EA03FC861CC0023EB3CC
SHA-256:	32C6AD91DC66BC12E1273B1E13EB7A15D6E8F63B93447909CA2163DD21B22998
SHA-512:	8DF23B7D80A4DD32C484CA3BD1922E11938D7ECDA9FC5FD5045EED882054EFCA7B7131EA109C4F20D8279845FFEB50EF46FB7419D190B8CF307EB00168746E 9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?..hQ..hQ..hQ.Rt_..hQ..KB..hQ..hP..hQ..H[..hQ..nW..hQ..HU..h Q.Rich.hQ.....PE..L....;.....!....0...@.....p0.....@.....H.....C..<....`.....p..h..... .....@.....orpc...p..... ..... ..`.text...B....0.....0..... ..`.rdata.....@.....@.....@..@.data...,....P.....P.....@....rsrc.....`.....`..... .....@..@.reloc.....p.....p.....@..B.....

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\temp.000

Process:	C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.exe

File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	614532
Entropy (8bit):	6.195803070094149
Encrypted:	false
SSDEEP:	6144:cTqa+rypBCk+Fx7/BCttXXikQklSn8nbFpBJkCcjaIJ/M6HnpJpaijgBwTFg56lX:fr/SlSBUJjnNRjpTWamB4
MD5:	B3FD01873BD5FD163AB465779271C58F
SHA1:	E1FF9981A09AB025D69AC891BFC931A776294D4D
SHA-256:	985EB55ECB750DA812876B8569D5F1999A30A24BCC54F9BAB4D3FC44DFEDB931
SHA-512:	6674AB1D65DA9892B7DD2FD37F300E087F58239262D44505B53379C676FD16DA5443D2292AEAAE01D3E6C40960B12F9CAC651418C827D2A33C29A6CDF874BE4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1"\.PL..PL..PL..L@..PL.?LB..PL.TOF..PL.TOG..PL..O_..PL..PL..PL..PM.oPL..s_..PL.CpF..PL.CpG..PL.{VJ..PL.Rich.PL.....PE..L...lh@=...../.....@.....text...Z..... ..`.rdata..`T.....`.....@..@.data...\.... ...P... .....@....rsrc.....p.....@..@.....

C:\Program Files (x86)\Common Files\InstallShield\IScript\iscrbeb1.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	225280
Entropy (8bit):	6.172364662668933
Encrypted:	false
SSDEEP:	6144:v4cBIsIikn+3HUYzZ2HWrXzXdgASLB2X4X:v4cBI5X+kkkqjXdpX
MD5:	B2F7E6DC7E4AAE3147FBFC74A2DDB365
SHA1:	716301112706E93F85977D79F0E8F18F17FB32A7
SHA-256:	4F77A9018B6B0D41151366E9ACAB3397416D114FC895703DEB82B20F40116AD1
SHA-512:	E6AE396BD9B4F069B5FAFE135C0F83718CC236D1CF9007DB7305BD5442C86483C0F1E0FAD9CD6D547E8715278E23E6FAFA973C63EBBE998A31A2153DBBBE7F83
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:.".~.L.~.L.~.L...@...L...B.d.L...F.-.L...G.l.L...F...L.~.L.{.L.(._.c.L.'._.u.L.~.M...L...G.q.L...J...L...H...L.Rich~.L.....PE..L....;.....!....P... .....`.....P..... .....@...1.....`..X.....text...fJ.....P..... ..`.rdata..T....`.....`.....@..@.data....!..... .....@....rsrc..... ... .@..@.reloc...=...@...@...0.....@..B.....

C:\Program Files (x86)\Common Files\InstallShield\IScript\iscript.dll (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	225280
Entropy (8bit):	6.172364662668933
Encrypted:	false
SSDEEP:	6144:v4cBIsIikn+3HUYzZ2HWrXzXdgASLB2X4X:v4cBI5X+kkkqjXdpX
MD5:	B2F7E6DC7E4AAE3147FBFC74A2DDB365
SHA1:	716301112706E93F85977D79F0E8F18F17FB32A7
SHA-256:	4F77A9018B6B0D41151366E9ACAB3397416D114FC895703DEB82B20F40116AD1
SHA-512:	E6AE396BD9B4F069B5FAFE135C0F83718CC236D1CF9007DB7305BD5442C86483C0F1E0FAD9CD6D547E8715278E23E6FAFA973C63EBBE998A31A2153DBBBE7F83
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:.".~.L.~.L.~.L...@...L...B.d.L...F.-.L...G.l.L...F...L.~.L.{.L.(._.c.L.'._.u.L.~.M...L...G.q.L...J...L...H...L.Rich~.L.....PE..L....;.....!....P... .....`.....P..... .....@...1.....`..X.....text...fJ.....P..... ..`.rdata..T....`.....`.....@..@.data....!..... .....@....rsrc..... ... .@..@.reloc...=...@...@...0.....@..B.....

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\corecomp.ini (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	ASCII text, with CRLF line terminators

Category:	dropped
Size (bytes):	28529
Entropy (8bit):	4.000373969114487
Encrypted:	false
SSDEEP:	384:2ERJ48bJNafWlc/n++TOa2SZ4+CIPo2S4m:2ER3JNaM+MJIPo27m
MD5:	62D5F9827D867EB3E4AB9E6B338348A1
SHA1:	828E72F9C845B1C0865BADAEF40D63FB36447293
SHA-256:	5214789C08EE573E904990DCD29E9E03AAF5CF12E86FAE368005FD8F4E371BD5
SHA-512:	B38BB74DC2E528C2A58A7D14A07BD1ECAAF55168B53AFC8F4718F3BF5D6F8C8B922B98551A355EBB1009F23CFF02FD8596413468993A43756C4DE7DFED57373 2
Malicious:	false
Preview:	; Corecomp.ini..;..; This file stores information about files that InstallShield..; will install to the Windows\System folder, such as Windows..; 95 and NT 4.0 core components and DAO, ODBC, and ActiveX files...; ..; The entries have the following format, without a space before ..; or after the equal sign:..;..; <file name>=<properties>..; ..; Currently, following properties are supported:..; 0x00000000 No registry entry is created for this file. It is..; not logged for uninstallation, and is therefore ..; never removed...;..; Inappropriate modification to this file can prevent an..; application from getting Windows 95/Windows NT logo...;..; Last Updated: 12/8/1999; bn....[Win32]....12500852.CPX=0x00000000 ..12510866.CPX=0x00000000 ..12520437.cpx=0x00000000..12520850.cpx=0x00000000..12520860.CPX=0x00000000..12520861.CPX=0x00000000 ..12520863.CPX=0x00000000 ..12520865.CPX=0x00000000..82557ndi.dll=0x00000000..8514a.dll=0x00000000..95fiber.dll=0x000

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\ctor.dll (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	77824
Entropy (8bit):	5.420648120129751
Encrypted:	false
SSDEEP:	768:uj5UUtenZewInMM66FwMd21I1FNVBt3NogjISsK7phsfTkF0kN1usI5FrAg1OBoM:Q5PI9F6SCdNoe57phsgW7Ag8lj
MD5:	003A6C011AAC993BCDE8C860988CE49B
SHA1:	6D39D650DFA5DED45C4E0CB17B986893061104A7
SHA-256:	590BE865DDF8C8D0431D8F92AA3948CC3C1685FD0649D607776B81CD1E267D0A
SHA-512:	032ABA4403EB45646AA1413FDC6C5D08BAAB4D0306D20B4209E70C84E47F6B72E68457BBC4331A5F1A5FA44AA776A89EB9FD29D0D956FA2FE11364C26AB09E E7
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9I..}..L}..L}..L...Ly..L.-.Lx..L}..Lx..L+..Lv..L}..L=..L$..Lt..L.-.L{..L ...L|..L.-.L|..LRich}..L.....PE..L.....;.....!.....p.....i.....0.....@.....x.....l..... ..... 4.....text....k.....p..... ..`.rdata..'..... .....@..@.data.....@....rsrc....l.....p.....@..@.reloc..... ....@..B.. .....

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\iuser.dll (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	176128
Entropy (8bit):	6.103238184891712
Encrypted:	false
SSDEEP:	3072:r+qN/OeBOZOptEHrOM/JUb1pZHYJvY6zsB7qAJy/Km1kUpbVxgr:5/bPtQxJUb1pdGQ6z73vzpbV6r
MD5:	377765FD4DE3912C0F814EE9F182FEDA
SHA1:	A0AB6A28F4BA057D5EAE5C223420EB599CD4D3B1
SHA-256:	8EFCBD8752D8BBFD7EE559502D1AA28134C9BF391BF7FC5CE6FDFD4473599AFB
SHA-512:	31BEFB11715F78043B7684287B4086CE003CB66F97C6EFF8C2B438EAE29045D8856172C6B898BE9F08C139EDC4647C2BCE000DA497AED208B7A5A69D4D90C7 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<`.]...]...]...A...]..yB...]...A...]..n}...]..yB...]...]...]...B...]...~...]...]. .D]..n}...]..V[...]..n}...]..Rich.].....PE..L.....;.....!.....p...@..... .....@..... .....X.....text....m.....p..... ..`.rdata...>.....@.....@..@.data....-..... .....@....rsrc... .....@..@.reloc...$.....0.. .....@..B.....

C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\objectps.dll (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	32768
Entropy (8bit):	2.240898610474827
Encrypted:	false
SSDEEP:	192:Ec9t9ShCx1JQ5BoQZgTWPLnOBog5MOSiYp7e9MCMWnaaAyqX:EAxoVgTNk9sM9pE
MD5:	8F02B204853939F8AEFE6B07B283BE9A
SHA1:	C161B9374E67D5FA3066EA03FC861CC0023EB3CC
SHA-256:	32C6AD91DC66BC12E1273B1E13EB7A15D6E8F63B93447909CA2163DD21B22998
SHA-512:	8DF23B7D80A4DD32C484CA3BD1922E11938D7ECDA9FC5FD5045EED882054EFCA7B7131EA109C4F20D8279845FFEB50EF46FB7419D190B8CF307EB00168746E9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?..hQ..hQ..hQ.Rt_..hQ..KB..hQ..hP..hQ..H[..hQ..nW..hQ..HU..hQ.Rich.hQ.....PE..L.....;.....!.....0...@.....p0.....@.....H.....C..<....`.....p..h.....@.....orpc...p..... ..... ..`.text...B....0.....0..... ..`.rdata.....@.....@.....@..@.data...,....P.....P.....@....rsrc.....`.....`.....@..@.reloc.....p.....p.....@..B.....

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\Setucb05.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	56320
Entropy (8bit):	6.027925766515646
Encrypted:	false
SSDEEP:	1536:ztsySvW1Xro1uNjEaJUJTmH90vK27leQE:ZMssQNxJUJTxvK27QQE
MD5:	1AEB989E361AF85F5099DE3DA25457F4
SHA1:	4F494142E3FB00C6D6845525CD4540BA3F7BE9EF
SHA-256:	AB9E0291A763EFC32E84E7117F9A0FBC99B681C96DF0BB27A66433A726667E5C
SHA-512:	0ECD71F3DEB154C8F48EC278822820F41AB15C6EFE76B00B8F6A95E28A62A97FBB8C44EB38293CAE3FE3A0FE29FEDBC660671885C4E3F7EB0016B6DBF3B4B273
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k.z..b)..b)..b)P.h)..b);.l)..b)G*h)..b)..b)..b)..q)..b)..c)..b).)q)..b)G*i)..b)..d)..b)Rich..b).....PE..L.....;.....t...d.....$.....@.....I..... .....text....r.....t..... ..`.rdata..:.....x.....@..@.data.....@....rsrc....I.....J.....@..@.....

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\Setucb34.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	data
Category:	dropped
Size (bytes):	174246
Entropy (8bit):	4.867152049703912
Encrypted:	false
SSDEEP:	1536:5zO7vcGlb5xhxrj8gDIL1nm3QzLgat1YRHU5CWb76pK/UWn9T12mrmHEhjpPWmr8:Sbh9jRRCK/Hy
MD5:	619D8A0CC00121812601D573CA1F6C95
SHA1:	CC2E25DC8D02F4ABF07B921645381D001D59B432
SHA-256:	8D0399C34F7CE6C66E6A0515A06FD893E1A2369CCE1FD3910B6EF0C312323841
SHA-512:	E0494BC16C3A5A6419525D2D2FEE81AEF99D31C926F85E4A30EAB1A47BD8B882DB406C27958662DB35B71DAED0BEE88ADE6A0E25A5B56E8832955FB8E0897EFB
Malicious:	false
Preview:	aLuZ..Copyright (c) 1990-1999 Stirling Technologies, Ltd. All Rights Reserved.....|...+.....z0..c...H.....J.....bWin95.....bWin9X.....bWin98.....bWinMe.....bSubversion_A.....bSubversion_B.....bSubversion_C.....bVersionNotFound.....bWinNT.....bWinNT4.....bWinNT351.....bWin2000.....bWinXP.....bAdmin_Logged_On.....nServicePack.....WINNT.....WIN9X.....bShellExplorer.....bAlpha.....bIntel.....nOSMajor.....nOSMinor.....nWinMajor.....nWinMinor.....int1.....int2.....dwEventType.....dwRestorePtType.....llSequenceNumber.@...szDescription.....nStatus.....llSequenceNumber.....cb.....lpReserved.....lpDesktop...lpTitle.....dwX.....dwY.....dwXSize.....dwYSize.....dwXCountChars.....dwYCountChars.....dwFillAttribute.....dwFlags.....wShowWindow.....lpReserved2.....hStdInput.....hStdOutput.....hStdError.....hProcess.....hThread.....dwProcessId.....dwThreadId.....nYearMonth.....nDay.....nHourMin.

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\Setup.exe (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	56320

Entropy (8bit):	6.027925766515646
Encrypted:	false
SSDEEP:	1536:ztsySvW1Xro1uNjEaJUJTmH90vK27leQE:ZMssQNxJUJTxvK27QQE
MD5:	1AEB989E361AF85F5099DE3DA25457F4
SHA1:	4F494142E3FB00C6D6845525CD4540BA3F7BE9EF
SHA-256:	AB9E0291A763EFC32E84E7117F9A0FBC99B681C96DF0BB27A66433A726667E5C
SHA-512:	0ECD71F3DEB154C8F48EC278822820F41AB15C6EFE76B00B8F6A95E28A62A97FBB8C44EB38293CAE3FE3A0FE29FEDBC660671885C4E3F7EB0016B6DBF3B4B273
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k.z..b)..b)..b)P.h)..b);.l)..b)G*h)..b)..b)..b)..q)..b)..c)..b).)q)..b)G*i)..b)..d)..b)Rich..b).....PE..L....;.....t...d.....$.....@.....l.....text....r.....t..... ..`.rdata..:.....x.....@..@.data.....@....rsrc....l.....J.....@..@.....

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\Setup.ini

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Generic INItialization configuration [Languages]
Category:	dropped
Size (bytes):	191
Entropy (8bit):	5.289826361205214
Encrypted:	false
SSDEEP:	3:3bhAFKLMj8v1s1tRFRLeIm1WmPQ26fSkVQVUs+GsYq/n6YfqLCYrYygZ5CcGZ:3bhdLMgm1tXRLrm1Wd0hus2YUzyLCNyD
MD5:	3B4298D8DF8C5815A673E83D7B249AED
SHA1:	553661973EB9834A71FC46C6DA8CE048EDC23AD0
SHA-256:	477DE38A2CF354C78E4FB6A5E3894E01034AA84084BC1F2EF873CCA86745637D
SHA-512:	B47C237CB1606407A1BCDFA1AC688656F38DE8734DA8B83AA100BC10C03DD92DF593980528406B02678269618FC20C85E43A7FCE9B461DDCF1B4786150303CE
Malicious:	false
Preview:	[Startup]..AppName=ViewSonic Windows 10 x64 INF Installation..ProductGUID=FC47C7A5-BE63-11D5-B7C9-005004566E4D..user=0..Copy=1..Source=0..[Languages]..Default=0x0009..count=1..key0=0x0009..

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\data1.cab (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	619311
Entropy (8bit):	**7.999107062707787**
Encrypted:	**true**
SSDEEP:	12288:K2xBihWGDfPn06MOn78KoC+1NQjn1AhO33ST6EuCWfcWeWgYwC:VxBihd46MGoCIQhmO30bWfcW2YI
MD5:	6F80DFDAB2B78973E6E009BB80AF2A21
SHA1:	C7F90BDEC8D5BEB34972688295E8AF09D98ED2E0
SHA-256:	CF06609F7F2459A8F95BF92CE5E5B8027BF33C500E270A363654D122FF308FA4
SHA-512:	2B69AD7228EBBED239FAFA233AC184E73E0FA32745EF7D59FA6D3A28398D00B803F5D1853167DD3BA7953AAF7036E90C0144FC2001AD9C8746372FE3F6094AFE
Malicious:	false
Preview:	ISc(.`.....d.....G.c.....P.VnM.....D..N..}2I]..pb.RI...b....4.1...D..?.I.....\.r"9.}....>..m....(.n.m0...8..P*. ;..%.....V...f..8..P..R...h..z..+Y.w...._~....^.^.K.....QW.'...[6..^...(.r.....K..E{..R../m....~.Q.^Q...?..A.{"|.....yo..]]\.$..K...1.....e.....T.i..G_xM..Z...f..v.;....k..^pB.^...b...=QD../..A...w.o.B.{+ +...?..|...?.w`|.:P....f.].'..pp..Q..^.wy.....-..W;...o...I.^.*..O.....^o..=...?.....>.8.Yig.$=.fQ.....U...2U....pi$^Sgz..u..iu...}.Hai.T.%...%}W~/Z...v*.$...@.....W..}.!..]....^.....z.....7}6

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\data1.hdr (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	212040
Entropy (8bit):	4.394493624236369
Encrypted:	false
SSDEEP:	1536:CsZaS0BO5FPx8Z79mQBLCSLPCr1oT/5+z5D+RNJKuYqT+tNWvB8i9z9:CsgS0Y0zBp+I5+1qv0gk8VD
MD5:	62A423044E0E00EBB13A8E52915FAFD0
SHA1:	65142C3727B4AE8FF9345EB930930452E3C62E25

SHA-256:	D3CA011D11098DB955971C307D96A612442D5D25821EB4DF5723DAD251CE4DA9
SHA-512:	CEF190CD0605B2616F602C83FF064F15053879725238B6383278AD770C5BDF18E4711F89B83D903FEE4FFCFF23482AA0A6A915C3298CCDE2E160F66404625164
Malicious:	false
Preview:	ISc(.`.....H<.....d.....G.c.....P.VnM.....D..N..}2I]..pb.RI...b....4.1...D..?.I.....[...[.....<.....Q..D...D..."E...E...E..fF...F..2G...G...G..:H...H..6I...I...J..nJ...J...J...K.."K..FK...K...K...K...L..6L..fL...L...L...M..JM..zM...M...M...N..FN ...N...N...N..fO...O...P..VP..nP..zP...P.....Q..:Q..^Q..jQ...Q...Q...Q...R..BR..ZR..~R.....R.....R...R.....R...S..>S..JS..bS...S...S.."T..FT..jT...T...T...U..NU..~U...U...U..... .....U...U.....&V..VV..zV...V...V...V...W...W...W..6X..~X...Y...Y...Z..vZ...Z...[...[

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\dataca98.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	212040
Entropy (8bit):	4.394493624236369
Encrypted:	false
SSDEEP:	1536:CsZaS0BO5FPx8Z79mQBLCSLPCr1oT/5+z5D+RNJKuYqT+tNWvB8i9z9:CsgS0Y0zBp+I5+1qv0gk8VD
MD5:	62A423044E0E00EBB13A8E52915FAFD0
SHA1:	65142C3727B4AE8FF9345EB930930452E3C62E25
SHA-256:	D3CA011D11098DB955971C307D96A612442D5D25821EB4DF5723DAD251CE4DA9
SHA-512:	CEF190CD0605B2616F602C83FF064F15053879725238B6383278AD770C5BDF18E4711F89B83D903FEE4FFCFF23482AA0A6A915C3298CCDE2E160F66404625164
Malicious:	false
Preview:	ISc(.`.....H<.....d.....G.c.....P.VnM.....D..N..}2I]..pb.RI...b....4.1...D..?.I.....[...[.....<.....Q..D...D..."E...E...E..fF...F..2G...G...G..:H...H..6I...I...J..nJ...J...J...K.."K..FK...K...K...K...L..6L..fL...L...L...M..JM..zM...M...M...N..FN ...N...N...N..fO...O...P..VP..nP..zP...P.....Q..:Q..^Q..jQ...Q...Q...Q...R..BR..ZR..~R.....R.....R...R.....R...S..>S..JS..bS...S...S.."T..FT..jT...T...T...U..NU..~U...U...U..... .....U...U.....&V..VV..zV...V...V...V...W...W...W..6X..~X...Y...Y...Z..vZ...Z...[...[

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\datacad7.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	619311
Entropy (8bit):	**7.999107062707787**
Encrypted:	**true**
SSDEEP:	12288:K2xBihWGDfPn06MOn78KoC+1NQjn1AhO33ST6EuCWfcWeWgYwC:VxBihd46MGoClQhmO30bWfcW2Yl
MD5:	6F80DFDAB2B78973E6E009BB80AF2A21
SHA1:	C7F90BDEC8D5BEB34972688295E8AF09D98ED2E0
SHA-256:	CF06609F7F2459A8F95BF92CE5E5B8027BF33C500E270A363654D122FF308FA4
SHA-512:	2B69AD7228EBBED239FAFA233AC184E73E0FA32745EF7D59FA6D3A28398D00B803F5D1853167DD3BA7953AAF7036E90C0144FC2001AD9C8746372FE3F6094AFE
Malicious:	false
Preview:	ISc(.`.....d.....G.c.....P.VnM.....D..N..}2I]..pb.RI...b....4.1...D..?.I.....\.r"9.}....>..m....(.n.m0...8..P*. ;..%.....V...f..8..P..R...h..z..+Y.w...._~....^.^.K.....QW.'...[6..^...(.r.....K..E{..R../m....~.Q.^Q...?..A.{"|.....yo..]]\.$..K...1.....e.....T.i. .G_xM..Z...f..v.;....k..^pB.^...b...=QD../..A...w.o.B.{+ +...?..|...?.w`|.:P....f.].'..pp..Q..^.wy.....-..W;...o...I.^.*..O.....^o..=...?.....>.8.Yig.$=.fQ.....U...2U....pi$^Sgz..u..iu...} .Hai.T.%...%}W~/Z...v*.$...@.....W..}.!..]....^.....z.....7}6

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\layoca69.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	data
Category:	dropped
Size (bytes):	417
Entropy (8bit):	1.9863894806793425
Encrypted:	false
SSDEEP:	3:o/BtaaRt/flIlYlF5lWllLlulllltldtflflflflflflH9El2paFgnRXnyiSTNULH:o/Bx1GYlgl5Ut13QiXnHSTNULT9Fn
MD5:	A6799E71BEA5DC7A7F16FAEE1650072B
SHA1:	38EEABCE51952914DA19BFC82647264695F8A9E4
SHA-256:	A8A15AD8D602356CACD08BA81FE1C0172CA646A7A5C26126606E6AF5ECB50DA8
SHA-512:	46EF381812357A436AA681942A582DE2E4ED3AE3061494D4A242757C9A5F1834E6CC7889BD888821ACE9C5A06D49FBC90D4B26936AE800B35C8B9CEC1239F83
Malicious:	false
Preview:	c..R.@..... ...<.....8.....X...c...m...y.....b...b...b...b...b...b...b...SETUP.INI..Setup.exe.ikernel.ex_.Setup.inx.data1.hdr.data1.cab.data2.cab.

C:\Program Files (x86)\InstallShield Installation Information\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\layout.bin (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	data
Category:	dropped
Size (bytes):	417
Entropy (8bit):	1.9863894806793425
Encrypted:	false
SSDEEP:	3:o/BtaaRt/flIlYlF5lWllLluIlltldtflflflflflflH9El2paFgnRXnyiSTNULH:o/Bx1GYlgl5Ut13QiXnHSTNULT9Fn
MD5:	A6799E71BEA5DC7A7F16FAEE1650072B
SHA1:	38EEABCE51952914DA19BFC82647264695F8A9E4
SHA-256:	A8A15AD8D602356CACD08BA81FE1C0172CA646A7A5C26126606E6AF5ECB50DA8
SHA-512:	46EF381812357A436AA681942A582DE2E4ED3AE3061494D4A242757C9A5F1834E6CC7889BD888821ACE9C5A06D49FBC90D4B26936AE800B35C8B9CEC1239F83
Malicious:	false
Preview:	c..R.@..... ....<.....8.....X...c...m...y.....b...b...b...b...b...b...SETUP.INI..Setup.exe.ikernel.ex_.Setup.inx.data1.hdr.data1.cab.data2.cab.

C:\Users\user\AppData\Local\Temp\IECB57A.tmp

Process:	C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.exe
File Type:	MS Compress archive data, SZDD variant, original size: 614532 bytes
Category:	dropped
Size (bytes):	346602
Entropy (8bit):	7.73908901473112
Encrypted:	false
SSDEEP:	6144:GnqCU025Do1BIFcsvbEfeqbnTdOJzEANIA9atuimsU7gaeaiNqltaBZv4fvxg:Aqw2qnQcs4bh+zxNeim79GqlQuK
MD5:	93B63F516482715A784BBEC3A0BF5F3A
SHA1:	2478FECA446576C33E96E708256D4C6C33E3FA68
SHA-256:	FBF95719B956B548B947436E29FEB18BB884E01F75AE31B05C030EBD76605249
SHA-512:	2C8F29DDA748E21231AB8C30C7A57735104B786120BB392EB1C20A320F2DDDDE392D136FD0C70853BB9AF851BBE47DF2955D8F9D5973B64870AC90BD12D2DD 0
Malicious:	false
Preview:	SZDD..'3A..`...MZ.....}.....@.....!..L.!T.his prog.ram cann.ot be ru.n in DOS. mode.....$...1"\..PL.t..L@.}.u.?LB..u..TOF...G.}.u..O_..u..u.M.ou..s._..u.CpF ....G..u.{V.J..u.Rich.t.....PE..L...lh@=...../...../.....p%.%...6....#.....%.M.Z.K.....).....te.xt..Z...%....l... ..`.r/data. T-.)..`"$....@..#..\.-. ....!N ~1+..rs rc..,.....pV-....-.-.-.-.-.-.-.=..=-===M=]=m=}=.=..=.=.=.=.=.=.=.M..M-M=MMM]MmM}M.M..M.M.M.M.M.M.M.]..]-]=]M]]]m}}].].].].].].].].].m..m-m=mMm]mmm}m.m..m.m. m.m.m.m.m.}..}-}=}M}]}m}}}.}..}.}.}.}.}.}.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.] .m.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.].m.}...../.F.....<SVW3.9.y..M.u...u..u.....u..].3..S..3.j.Q.PV.}..}...R.;.....W.M.j._QV.P.0.....f.}..ul8...j.@.||.E..j.P.M....". E.

C:\Users\user\AppData\Local\Temp\bb37.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	1194496
Entropy (8bit):	3.186985870848205
Encrypted:	false
SSDEEP:	6144:cFiXwzECtlythUXKeb66FJWSXmSt6uYoXU5BZn7c8l3MU6AReQlGo1/j4s+5i9Jh:Cb8
MD5:	170D479C9479066D3DD7618EE97EC879
SHA1:	C1087E3C348DEF96673186FC66CBD3C7204F7D4A
SHA-256:	E01B3D8E9C3C0B719951E43A62F24FEF18A251E4351B239D06A52D1168774A28
SHA-512:	F8F4BFE2D97EAEBDFB378A3F728419927918F35440C32104AB817441BCE8F8128461D65213961C6FD27BBA3799082025D0C2487CD7CD8A9A2EF3CB5CF9590FE
Malicious:	false
Preview:	.....>.....|.....w.....|.....}.....|..... ....."..... .....$..... ...!...#...U...%.../...&...'...(...)...*...+...,...-.....C...B...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A... X...G...D...E...F...T...W...I...J...K...L...M...N...O...P...Q...R...S.....V...B...^...b...Y...Z...[...\...]...%..._...`...a...c...e...d...x...o...g...h...i...j...k...l...m...n...5...p...q...r...|...t...u...v. ..w...x...y...z...

C:\Users\user\AppData\Local\Temp\extAF51.tmp

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	Generic INItialization configuration [Dialog1001]
Category:	dropped
Size (bytes):	5248

Entropy (8bit):	4.900585489889706
Encrypted:	false
SSDEEP:	96:Kq2orCnavjFYCgENA3jOpAWaMd1ZcMeJgocuEaegn:KopxYuU2NaM9eJ4aegn
MD5:	9EFCC61A0BAA38A6D7C67A05A97C7B87
SHA1:	72B713A72EF7E972DFD5BE5F79DA8E9AACEDB296
SHA-256:	7CCB3A50CA08C66A220E4DA614CBABA1D05157359EDD174223C788B86D929EDF
SHA-512:	AC57100B76826AF9F7650417DD765C23B522E31A1F3B44BFE9E70ED520BF6C6EB1978118A8147C99487B05A7A4C4AFC964F457B79F921FF8236E4D60561B1238
Malicious:	false
Preview:	[Dialog1000]..100=Welcome to the InstallShield Wizard for %s..101=The InstallShield Wizard(TM) will help install %s on your computer. To continue, click Next.....[Dialog1001]..0=License Agreement..1=Please read the following license agreement carefully...121=I &accept the terms in the license agreement..122=I &do not accept the terms in the license agreement....[Dialog1002]..0=Location to Save Files..1=Where would you like to save your files?..101=Please enter the folder where you want these files saved. If the folder does not exist, it will be created for you. To continue, click Next...102=&Save files in folder:..103=&Change.....[Dialog1003]..0=Password..1=This package has been password protected...106=&Password:..107=Enter the password required to run this package. Please note that passwords are case sensitive. Click Next to continue.....[Dialog1004]..0=Overwrite Protection..2=Cancel..109=&Yes..110=&No..111=Y&es to All..112=N&o to All..113=The following file is already on yo

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.exe

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	56320
Entropy (8bit):	6.027925766515646
Encrypted:	false
SSDEEP:	1536:ztsySvW1Xro1uNjEaJUJTmH90vK27leQE:ZMssQNxJUJTxvK27QQE
MD5:	1AEB989E361AF85F5099DE3DA25457F4
SHA1:	4F494142E3FB00C6D6845525CD4540BA3F7BE9EF
SHA-256:	AB9E0291A763EFC32E84E7117F9A0FBC99B681C96DF0BB27A66433A726667E5C
SHA-512:	0ECD71F3DEB154C8F48EC278822820F41AB15C6EFE76B00B8F6A95E28A62A97FBB8C44EB38293CAE3FE3A0FE29FEDBC660671885C4E3F7EB0016B6DBF3B4B273
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k.z..b)..b)..b)P.h)..b);.l)..b)G*h)..b)..b)..b)..q)..b)..c)..b).)q)..b)G*i)..b)..d)..b)Rich..b).....PE..L.....;.....t...d.....$.....@.....l.....text....r.....t..... ..`.rdata..:.....x.....@..@.data.....@....rsrc....l.....J.....@..@.....

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.ini

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	Generic INItialization configuration [Languages]
Category:	dropped
Size (bytes):	163
Entropy (8bit):	5.334857776179536
Encrypted:	false
SSDEEP:	3:3bhAFKLMj8v1s1tRFRLeIm1WmPQ26fSkVQVUs+aYrYygZ5CcGZ:3bhdLMgm1tXRLrm1Wd0husTNyW5fGZ
MD5:	FFC572385FA498C295A4AA5DAD637EB2
SHA1:	D6213B0E2A3010EEDD468613EBE277413F8249CB
SHA-256:	56BC9507F45B7C13FCBBEDCCB0FE455A0A9A5AC43432B7544FE33B8331943AF8
SHA-512:	1CCBF14C427DBD98253A8AB6C966BB9077DDA6B079AECC7974A4DD05478A717E664F81CCAEBD0D286680EEA188B220FB84FAA57868031647EB0A489FF1704152
Malicious:	false
Preview:	[Startup]..AppName=ViewSonic Windows 10 x64 INF Installation..ProductGUID=FC47C7A5-BE63-11D5-B7C9-005004566E4D..[Languages]..Default=0x0009..count=1..key0=0x0009..

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\data1.cab

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	619311
Entropy (8bit):	**7.999107062707787**
Encrypted:	**true**
SSDEEP:	12288:K2xBihWGDfPn06MOn78KoC+1NQjn1AhO33ST6EuCWfcWeWgYwC:VxBihd46MGoCIQhmO30bWfcW2YI
MD5:	6F80DFDAB2B78973E6E009BB80AF2A21

SHA1:	C7F90BDEC8D5BEB34972688295E8AF09D98ED2E0
SHA-256:	CF06609F7F2459A8F95BF92CE5E5B8027BF33C500E270A363654D122FF308FA4
SHA-512:	2B69AD7228EBBED239FAFA233AC184E73E0FA32745EF7D59FA6D3A28398D00B803F5D1853167DD3BA7953AAF7036E90C0144FC2001AD9C8746372FE3F6094AFE
Malicious:	false
Preview:	ISc(.`..... .....d.....G.c.....P.VnM.....D..N..}2I]..pb.RI...b....4.1...D..?.I..... .....\.r"9.}....>..m....(.n.m0...8..P*. ;..%.....V...f..8..P..R...h..z..+Y.w...._~....^.^.K.....QW.'...[6..^...(.r.....K..E{..R../m....~.Q.^Q...?..A.{"|.....yo..]]\.$..K...1.....e.....T.i. .G_xM..Z...f..v.;....k..^pB.^...b...=QD../..A...w.o.B.{+ +...?..\|...?.w`\|.:P....f.]."..pp..Q..^.wy.....-..W;...o...I.^.*..O.....^o..=...?.....>.8.Yig.$=.fQ.....U...2U....pi$^Sgz..u..iu...} .Hai.T.%...%}W~/Z...v*.$...@.....W..}.!..]....^.....z.....7}6

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\data1.hdr

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	212040
Entropy (8bit):	4.394493624236369
Encrypted:	false
SSDEEP:	1536:CsZaS0BO5FPx8Z79mQBLCSLPCr1oT/5+z5D+RNJKuYqT+tNWvB8i9z9:CsgS0Y0zBp+I5+1qv0gk8VD
MD5:	62A423044E0E00EBB13A8E52915FAFD0
SHA1:	65142C3727B4AE8FF9345EB930930452E3C62E25
SHA-256:	D3CA011D11098DB955971C307D96A612442D5D25821EB4DF5723DAD251CE4DA9
SHA-512:	CEF190CD0605B2616F602C83FF064F15053879725238B6383278AD770C5BDF18E4711F89B83D903FEE4FFCFF23482AA0A6A915C3298CCDE2E160F66404625164
Malicious:	false
Preview:	ISc(.`.....H<..... .....d.....G.c.....P.VnM.....D..N..}2I]..pb.RI...b....4.1...D..?.I..... .....[...[.....<.....Q..D...D.."E...E...E..fF...F..2G...G...G..:H...H..6I...I...J..nJ...J...J...K.."K..FK...K...K...K...L..6L..fL...L...L...M..JM..zM...M...M...N..FN ...N...N...N..fO...O...P..VP..nP..zP...P.....Q..:Q..^Q..jQ...Q...Q...Q...R..BR..ZR..~R.....R.....R...R.....R...S..>S..JS..bS...S...S.."T..FT..jT...T...T...U..NU..~U...U...U..... .....U...U.....&V..VV..zV...V...V...V...W...W...W..6X..~X...Y...Y...Z..vZ...Z...[...[

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\data2.cab

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	2264239
Entropy (8bit):	**7.9986584302391055**
Encrypted:	**true**
SSDEEP:	49152:OkK0D0EcTdcjtP+WR0WnMMnfWvqqzlV9tRBdBQGte/3dn:Ov0DGTdcpG60Wdn+vRXRlQTtn
MD5:	720F14DD859391C33A28544F81E708C6
SHA1:	A0BDCC249A0AB7BDD051CE38683040BBB19AE525
SHA-256:	CFA3149C9AFACE9AB316C971BB509B1A6E322B9255FFAEB94A5A154FCC6ADEB5
SHA-512:	AB5DE9105D1DF44C55E354C697A63D369F9E6D1C8366000D5014EC454CFC719979FF0DF83147EBF529C0EED0C19D6D9C582F0B07D28A9D93CCFCC297805FEF8
Malicious:	false
Preview:	ISc(.`..... .....d.....G.c.....P.VnM.....D..N..}2I]..pb.RI...b....4.1...D..?.I..... .....u..X.<T.?gf,3.5.1.....d+".D.`d0.1.6.$$.*..5...PT.%.JE%Z%$.T.A.....<..=.=.....q..bW.N..<.,....VB#@.(..p.=bW..$..r.....F.s.(.....5..scf'.A.%..^.}A3.b..f..}....$.h@...'. @..#9.". 6.A.VK.H*..".]..z.".....++jp...u".%$....$"..D.7... y,?..p.L.&.e P. ...l.!...../4.....@.@.]...l....Z.;..P.....k ...g..>..E..... .....-.....%..j.}{W...s...%+....N&...S....8.p8-L. ....H.N...c.....t.T..V.u.J..j.9a....V....77....p.8.KW..A.6.....YlP.....&..2.*.

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\ikernel.ex_

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	MS Compress archive data, SZDD variant, original size: 614532 bytes
Category:	dropped
Size (bytes):	346602
Entropy (8bit):	7.73908901473112
Encrypted:	false
SSDEEP:	6144:GnqCU025Do1BIFcsvbEfeqbnTdOJzEANlA9atuimsU7gaeaiNqltaBZv4fvxg:Aqw2qnQcs4bh+zxNeim79GqlQuK
MD5:	93B63F516482715A784BBEC3A0BF5F3A
SHA1:	2478FECA446576C33E96E708256D4C6C33E3FA68
SHA-256:	FBF95719B956B548B947436E29FEB18BB884E01F75AE31B05C030EBD76605249
SHA-512:	2C8F29DDA748E21231AB8C30C7A57735104B786120BB392EB1C20A320F2DDDDE392D136FD0C70853BB9AF851BBE47DF2955D8F9D5973B64870AC90BD12D2DD0

Malicious:	false
Preview:	SZDD..'3A..`...MZ.....}.....@.....!..L.!T.his prog.ram cann.ot be ru.n in DOS. mode.....$...1"\..PL.t..L@.}.u.?LB..u..TOF...G.}.u..O_..u..u.M.ou..s._..u.CpF ....G..u.{V.J..u.Rich.t.....PE..L....lh@=...../...../.....p%.%...6....#.....%.M.Z.K.....).....te.xt..Z...%....l... ..`.r/data. T-.)..`"$....@..#..\.-. ....!N ~1+..rs rc..,.....pV-....-.-.-.-.-.-.=..=-===M=]=m=}=.=..=.=.=.=.=.=.=.M..M-M=MMM]MmM}M.M..M.M.M.M.M.M.M.]..}-]=]M]]]m]}].].].].].].].].].m..m-m=mMm]mmm}m.m..m.m. m.m.m.m.m.}..}-}=}M}]}m}}}.}..}.}.}.}.}.}.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.].m.}.....-.=.M.].m.} .m.}.....-.=.M.].m.}.....-.=.M.].m.}...../.F.....<SVW3.9.y..M.u...u..u.....u..].3..S..3.j.Q.PV.}..}...R.;.....W.M.j._QV.P.0.....f.}..ul8...j.@.||.E..j.P.M...." . E.

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\layout.bin

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	data
Category:	dropped
Size (bytes):	417
Entropy (8bit):	1.9863894806793425
Encrypted:	false
SSDEEP:	3:o/BtaaRt/fllIYlF5lWlILlulltldtflflflflflflH9El2paFgnRXnyiSTNULH:o/Bx1GYlgl5Ut13QiXnHSTNULT9Fn
MD5:	A6799E71BEA5DC7A7F16FAEE1650072B
SHA1:	38EEABCE51952914DA19BFC82647264695F8A9E4
SHA-256:	A8A15AD8D602356CACD08BA81FE1C0172CA646A7A5C26126606E6AF5ECB50DA8
SHA-512:	46EF381812357A436AA681942A582DE2E4ED3AE3061494D4A242757C9A5F1834E6CC7889BD888821ACE9C5A06D49FBC90D4B26936AE800B35C8B9CEC1239F83
Malicious:	false
Preview:	c..R.@..... ....<.....8.....X...c...m...y.....b...b...b...b...b...b...b...SETUP.INI..Setup.exe.ikernel.ex_.Setup.inx.data1.hdr.data1.cab.data2.cab.

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\setup.inx

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	data
Category:	dropped
Size (bytes):	174246
Entropy (8bit):	4.867152049703912
Encrypted:	false
SSDEEP:	1536:5zO7vcGlb5xhxrj8gDlL1nm3QzLgat1YRHU5CWb76pK/UWn9T12mrmHEhjpPWmr8:Sbh9jRRCK/Hy
MD5:	619D8A0CC00121812601D573CA1F6C95
SHA1:	CC2E25DC8D02F4ABF07B921645381D001D59B432
SHA-256:	8D0399C34F7CE6C66E6A0515A06FD893E1A2369CCE1FD3910B6EF0C312323841
SHA-512:	E0494BC16C3A5A6419525D2D2FEE81AEF99D31C926F85E4A30EAB1A47BD8B882DB406C27958662DB35B71DAED0BEE88ADE6A0E25A5B56E8832955FB8E0897 EFB
Malicious:	false
Preview:	aLuZ..Copyright (c) 1990-1999 Stirling Technologies, Ltd. All Rights Reserved.....|...+.....z0..c...H.....J.....bWin9 5.....bWin9X.....bWin98.....bWinMe.....bSubversion_A.....bSubversion_B.....bSubversion_C.....bVersionNotFound.....bWinNT.....bWinNT4.....bWinNT351.....bWin200 0.....bWinXP.....bAdmin_Logged_On.....nServicePack.....WINNT.....WIN9X.....bShellExplorer.....bAlpha.....bIntel.....nOSMajor.....nOSMinor.....nWinMajor.....nWinMinor... ....int1.....int2.....dwEventType.....dwRestorePtType.....llSequenceNumber.@...szDescription.....nStatus.....llSequenceNumber.....cb.....lpReserved.....lpDesktop... ..lpTitle.....dwX.....dwY.....dwXSize.....dwYSize.....dwXCountChars.....dwYCountChars.....dwFillAttribute.....dwFlags.....wShowWindow.....lpReserved2.....hStdInput.....hS tdOutput.....hStdError.....hProcess.....hThread.....dwProcessId.....dwThreadId.....nYearMonth.....nDay.....nHourMin.

C:\Users\user\AppData\Local\Temp\pftB01D.tmp\pftw1.pkg

Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	Microsoft Cabinet archive data, many, 3299096 bytes, 8 files, at 0x2c +A "\Disk1\data1.cab" +A "\Disk1\data1.hdr", ID 12345, number 1, 113 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	3299096
Entropy (8bit):	**7.9994781557461**
Encrypted:	**true**
SSDEEP:	49152:wtthGt1LHQzcLx7o11qxT48S7du1Owbn0XdGtayRVIKYbCRAQIGEtmpd8OzlJQHK:wlt1BW11J8S7e0XdGgyXtH/Ivmr90gZ
MD5:	F0F65D35CB74B313777DFFD76951ACF4
SHA1:	B41BA8E2891F23585EFE2FAC65416988A16CB351
SHA-256:	BB19AE69B6A255C7467478C76E085F2985334DB57B09C479F85A009106B30E42
SHA-512:	64B3EEA03478210B80F01E9A6082963A24B238BB1FA1E0B69D0C00F09756D3FC2D36A3529EAC803DF4E3CA350C802B761D7104B1C92A160AD7B4DB6AB603431 9
Malicious:	false
Preview:	MSCF.....W2.....,.....90..7...q.../s.....V,[.\Disk1\data1.cab.H<../s.....V,[.\Disk1\data1.hdr...".w.....V0[.\Disk1\data2.cab..I..&</.....,@ .\Disk1\ikernel.ex_.....4....V0[.\Disk1\layout.bin.....4...%+." .\Disk1\Setup.exe.....c5....V)[.\Disk1\Setup.ini.....Td5....V)[.\Disk1\setup.inx.+.A.r~..CK.S.0@.%xm.m..m.m.m.m.....d.yO.s..tw..J:-.dD... ..._.....?@.....|.0.....e^...Q..b...<.....<.7Y7\.4"...ol.IR.....GQ2.....?.%.q...P.4..(C.....V.....8[}..?...I../2"(.m.I.@./8...R..K.I."...T.//L.9P_.[R..j.z..<.&.50..j~..|..zft.t..W....Z....Z../....u. w.C)&.{.*...b.?.E....+..m.*!..|..2t.R:.....o.....r.=...tt._IZ..w.....{.&v..^..L.[>o.K..G,`*...ew..4[z.M.*.\.c../.....u.*uK#..+..y.DN..W...{..^...>.....?...o.O.....s..{...L.tj..3..k..N*.u..<. ...h+s.q.....w.$.t!.r;.v>.K.t.."xW...[#{.7o.z9..4,..IxsL.>...T.@..Tj.....-Ht..<K'].N,\..~\|^$.,...H...I}.|.5.'.].FI..@.....{...}P._surG..t..f.~....<1W.....}.p..>...:..1a.F..~...^5k.<.|v.`..B..

C:\Users\user\AppData\Local\Temp\plfAF50.tmp	
Process:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
File Type:	Generic INItialization configuration [Dialog1001]
Category:	dropped
Size (bytes):	5248
Entropy (8bit):	4.900585489889706
Encrypted:	false
SSDEEP:	96:Kq2orCnavjFYCgENA3jOpAWaMd1ZcMeJgocuEaegn:KopxYuU2NaM9eJ4aegn
MD5:	9EFCC61A0BAA38A6D7C67A05A97C7B87
SHA1:	72B713A72EF7E972DFD5BE5F79DA8E9AACEDB296
SHA-256:	7CCB3A50CA08C66A220E4DA614CBABA1D05157359EDD174223C788B86D929EDF
SHA-512:	AC57100B76826AF9F7650417DD765C23B522E31A1F3B44BFE9E70ED520BF6C6EB1978118A8147C99487B05A7A4C4AFC964F457B79F921FF8236E4D60561B1238
Malicious:	false
Preview:	[Dialog1000]..100=Welcome to the InstallShield Wizard for %s..101=The InstallShield Wizard(TM) will help install %s on your computer. To continue, click Next.....[Dialo g1001]..0=License Agreement..1=Please read the following license agreement carefully...121=I &accept the terms in the license agreement..122=I &do not accept the terms in the license agreement....[Dialog1002]..0=Location to Save Files..1=Where would you like to save your files?..101=Please enter the folder where you want these f iles saved. If the folder does not exist, it will be created for you. To continue, click Next...102=&Save files in folder:..103=&Change.....[Dialog1003]..0=Password..1=This package has been password protected...106=&Password:..107=Enter the password required to run this package. Please note that passwords are case sensitive. Click Next to continue.....[Dialog1004]..0=Overwrite Protection..2=Cancel..109=&Yes..110=&No..111=Y&es to All..112=N&o to All..113=The following file is already on yo

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\VSC.BMP (copy)	
Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PC bitmap, Windows 3.x format, 75 x 60 x 24, image size 13680, resolution 3937 x 3937 px/m, cbSize 13734, bits offset 54
Category:	dropped
Size (bytes):	13734
Entropy (8bit):	5.0930553474278355
Encrypted:	false
SSDEEP:	192:PEwSSLsfyURhe6OgTc3qxczGN8NOQECU313sR5qe+uA:HSSLsfTRhzDo3qiz9e318DqaA
MD5:	45359E643F2710A8EBD29A4A34908F25
SHA1:	4AC33970E1B4C40CD21048287C9421B8D59CB927
SHA-256:	461AA9F0CDC888BCC05B1F67FCEF01149ABAAD2FC544BA599A5F7A5ACCAD5A6D
SHA-512:	AC7B6AC87886D2FA1247B9FF5D897C73C382F1716D7A1E9F3A01C2548C2A89C5F2896C3460ACD2730A3424ACB1E9F24882C957BB29DAEC8BE038B48902DCD5 A
Malicious:	false
Preview:	BM.5.....6...(...K...<.....p5..a...a..... X

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\VSCc26a.rra	
Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PC bitmap, Windows 3.x format, 75 x 60 x 24, image size 13680, resolution 3937 x 3937 px/m, cbSize 13734, bits offset 54
Category:	dropped
Size (bytes):	13734
Entropy (8bit):	5.0930553474278355
Encrypted:	false
SSDEEP:	192:PEwSSLsfyURhe6OgTc3qxczGN8NOQECU313sR5qe+uA:HSSLsfTRhzDo3qiz9e318DqaA
MD5:	45359E643F2710A8EBD29A4A34908F25
SHA1:	4AC33970E1B4C40CD21048287C9421B8D59CB927
SHA-256:	461AA9F0CDC888BCC05B1F67FCEF01149ABAAD2FC544BA599A5F7A5ACCAD5A6D
SHA-512:	AC7B6AC87886D2FA1247B9FF5D897C73C382F1716D7A1E9F3A01C2548C2A89C5F2896C3460ACD2730A3424ACB1E9F24882C957BB29DAEC8BE038B48902DCD5 A
Malicious:	false
Preview:	BM.5.....6...(...K...<.....p5..a...a..... X

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}_IsRc3c2.rra	
Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	258048
Entropy (8bit):	5.801916805215816
Encrypted:	false
SSDEEP:	3072:TXRZKyskkkkknffCp5CrRb9YfMX0E9QsJB9cWe7Ka2c2DRJMn2b:ThzskkkkknffCp5CrRKluaqL
MD5:	48EA604D4FA7D9AF5B121C04DB6A2FEC
SHA1:	DC3C04977106BC1FBF1776A6B27899D7B81FB937
SHA-256:	CBE8127704F36ADCC6ADBAB60DF55D1FF8FB7E600F1337FB9C4A59644BA7AA2B
SHA-512:	9206A1235CE6BD8CEDA0FF80FC01842E9CBBEB16267B4A875A0F1E6EA202FD4CBD1A52F8A51BED35A2B38252EB2B2CD2426DC7D24B1EA715203CC0935D612707
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...W...W...W.&.\...W.&.]...W.M.Y...W...V...W...D...W.1.]... W...Q...W.Rich..W.....PE..L.....;.....!.....0.....@.....D..(....`...w..... .....@.....text....*.....0..... ..`.rdata.....@.....@.....@..@.data.....P.....P.....@....rsrc....w...`.....`.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}_IsRes.dll (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	258048
Entropy (8bit):	5.801916805215816
Encrypted:	false
SSDEEP:	3072:TXRZKyskkkkknffCp5CrRb9YfMX0E9QsJB9cWe7Ka2c2DRJMn2b:ThzskkkkknffCp5CrRKluaqL
MD5:	48EA604D4FA7D9AF5B121C04DB6A2FEC
SHA1:	DC3C04977106BC1FBF1776A6B27899D7B81FB937
SHA-256:	CBE8127704F36ADCC6ADBAB60DF55D1FF8FB7E600F1337FB9C4A59644BA7AA2B
SHA-512:	9206A1235CE6BD8CEDA0FF80FC01842E9CBBEB16267B4A875A0F1E6EA202FD4CBD1A52F8A51BED35A2B38252EB2B2CD2426DC7D24B1EA715203CC0935D612707
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...W...W...W.&.\...W.&.]...W.M.Y...W...V...W...D...W.1.]... W...Q...W.Rich..W.....PE..L.....;.....!.....0.....@.....D..(....`...w..... .....@.....text....*.....0..... ..`.rdata.....@.....@.....@..@.data.....P.....P.....@....rsrc....w...`.....`.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}_IsUc299.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	307296
Entropy (8bit):	5.486716084490027
Encrypted:	false
SSDEEP:	3072:w7VOURxibuzR5Czbws0NwCfp/Xvb6A14WFsTtQ/NgoQcTbNY:w7VOmaucbBNCx/uR+Fa
MD5:	D80017F2B2F6EB9F0E4B86100B58639A
SHA1:	3D4383DFFBACA485D1E231CBD0C3D9CC0690A0B1
SHA-256:	765F6A8864A49A2267F2EE633642268FB46C9A9C5D7F58FBC7AA015F5BBB11C6
SHA-512:	C258BCA4980262E65A4FC6DC4EE574993322E86CBFBC86F2341E95A8977B977ACA90818513A6CE051C9FA576AC209CDE0290D6365AA177EE17062E62872108F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x-.|.~.|.~.|.~.c.~.|.~e`.~.|.~.|.~.|.~.c.~.|.~.c.~.|.~^z.~.|.~Rich.|.~ .....PE..L....h<.....!.....0.....(.....#..... .....text...pq..... ..`.rdata..w..... .....@..@.data...T?.....0.....@....idata.....@....rsrc...#.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}_IsUser.dll (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	307296
Entropy (8bit):	5.486716084490027
Encrypted:	false
SSDEEP:	3072:w7VOURxibuzR5Czbws0NwCfp/Xvb6A14WFsTtQ/NgoQcTbNY:w7VOmaucbBNCx/uR+Fa
MD5:	D80017F2B2F6EB9F0E4B86100B58639A
SHA1:	3D4383DFFBACA485D1E231CBD0C3D9CC0690A0B1
SHA-256:	765F6A8864A49A2267F2EE633642268FB46C9A9C5D7F58FBC7AA015F5BBB11C6
SHA-512:	C258BCA4980262E65A4FC6DC4EE574993322E86CBFBC86F2341E95A8977B977ACA90818513A6CE051C9FA576AC209CDE0290D6365AA177EE17062E62872108F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x-.|.~.|.~.|.~.c.~.|.~e`.~.|.~.|.~.|.~.c.~.|.~.c.~.|.~^z.~.|.~Rich.|.~ .....PE..L....h<.....!.....0.....(.....#..... .....text...pq..... ..`.rdata..w..... .....@..@.data...T?.....0.....@....idata.....@....rsrc...#.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\defac393.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	RIFF (little-endian) data, palette, 1168 bytes, data size 1028, 256 entries, extra bytes 0x6f66666c
Category:	dropped
Size (bytes):	1168
Entropy (8bit):	2.551387347019812
Encrypted:	false
SSDEEP:	12:b126a96IlDkYTYcspSuB0MRG763GDwFGrZYOFBz3WI7KEpw3f6QL7nhem:Ax96Il9T3ISMg76KJrZtT2b5X
MD5:	0ABAFE3F69D053494405061DE2629C82
SHA1:	E414B6F1E9EB416B9895012D24110B844F9F56D1
SHA-256:	8075162DB275EB52F5D691B15FC0D970CB007F5BECE33CE5DB509EDF51C1F020
SHA-512:	63448F2BEF338EA44F3BF9EF35E594EF94B4259F3B2595D77A836E872129B879CEF912E23CF48421BABF1208275E21DA1FABFDC494958BCFCD391C78308EAA27
Malicious:	false
Preview:	RIFF....PAL data.....f...3.....f...3.....f...3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3.....f...3.....f...3..... .....f..3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3.....f...3.....f...3.....f...3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3.....f...f...f ...f.f.f.3.f...f...f...f.f.f.f.3.f...f...f...f...f.i.f.3.f...ff..ff..ff..fff.ff3.ff..f3..f3..f3..f3f.f33.f3..f...f...f...f.f.f.3.f...3...3...3...3.f.3.3.3...3...3...3...3.f.3.3.3...3...3...3...3.f.3.3.3...3f..3f..3f..3ff.3f3.3f..3 3..33..33..33f.333.33..3...3...3...3.f.3.3.3.....f...3.....f...3.....f...3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3..... .....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\default.pal (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	RIFF (little-endian) data, palette, 1168 bytes, data size 1028, 256 entries, extra bytes 0x6f66666c
Category:	dropped
Size (bytes):	1168
Entropy (8bit):	2.551387347019812
Encrypted:	false
SSDEEP:	12:b126a96IlDkYTYcspSuB0MRG763GDwFGrZYOFBz3WI7KEpw3f6QL7nhem:Ax96Il9T3ISMg76KJrZtT2b5X
MD5:	0ABAFE3F69D053494405061DE2629C82
SHA1:	E414B6F1E9EB416B9895012D24110B844F9F56D1
SHA-256:	8075162DB275EB52F5D691B15FC0D970CB007F5BECE33CE5DB509EDF51C1F020
SHA-512:	63448F2BEF338EA44F3BF9EF35E594EF94B4259F3B2595D77A836E872129B879CEF912E23CF48421BABF1208275E21DA1FABFDC494958BCFCD391C78308EAA27
Malicious:	false
Preview:	RIFF....PAL data.....f...3.....f...3.....f...3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3.....f...3.....f...3..... .....f..3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3.....f...3.....f...3.....f...3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3.....f...f...f ...f.f.f.3.f...f...f...f.f.f.f.3.f...f...f...f...f.i.f.3.f...ff..ff..ff..fff.ff3.ff..f3..f3..f3..f3f.f33.f3..f...f...f...f.f.f.3.f...3...3...3...3.f.3.3.3...3...3...3...3.f.3.3.3...3...3...3...3.f.3.3.3...3f..3f..3f..3ff.3f3.3f..3 3..33..33..33f.333.33..3...3...3...3.f.3.3.3.....f...3.....f...3.....f...3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3..... .....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcc23b.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	73216
Entropy (8bit):	5.1607318530178015
Encrypted:	false

SSDEEP:	768:4bzr2eKdjkwP15JJ8F8TQ2MdKbNunu72RW2CeTxHs4gZWk:4r2eK9JJmG7Zwnu72RW2PxHeW
MD5:	337FF45A8FD5B7BE152508EBC2E584CA
SHA1:	1C158FFDD4AE0802425D6C950B5D27CE5E1D25BA
SHA-256:	E6EBF1AA7D6D26CACB3AD81507837BD99FCAE352105D8E59ADE2E030BB380F6B
SHA-512:	DB7DA02666B130703CDB128908A6DF95F979923FCD8E3E96EBC39806A7DEA158977F27F3E60A487CB75C20157138C2F0091315DB1EB230FDB571AFB8C0D15AE6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.gF.....Cr.t....Ct.}....Cd.q....C{.|....Cu.~....Cq.~...Rich.....PE..d.....B.....#.....{.....P.....*..... .....p...x.....`.....text..... ..`.data...(.....@....pdata..`.....@..@.rsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon.exe (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	73216
Entropy (8bit):	5.1607318530178015
Encrypted:	false
SSDEEP:	768:4bzr2eKdjkwP15JJ8F8TQ2MdKbNunu72RW2CeTxHs4gZWk:4r2eK9JJmG7Zwnu72RW2PxHeW
MD5:	337FF45A8FD5B7BE152508EBC2E584CA
SHA1:	1C158FFDD4AE0802425D6C950B5D27CE5E1D25BA
SHA-256:	E6EBF1AA7D6D26CACB3AD81507837BD99FCAE352105D8E59ADE2E030BB380F6B
SHA-512:	DB7DA02666B130703CDB128908A6DF95F979923FCD8E3E96EBC39806A7DEA158977F27F3E60A487CB75C20157138C2F0091315DB1EB230FDB571AFB8C0D15AE6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.gF.....Cr.t....Ct.}....Cd.q....C{.|....Cu.~....Cq.~...Rich.....PE..d.....B.....#.....{.....P.....*..... .....p...x.....`.....text..... ..`.data...(.....@....pdata..`.....@..@.rsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\isrt.dll (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	331776
Entropy (8bit):	6.377016902367252
Encrypted:	false
SSDEEP:	6144:KzbdBEFj2WevDaaf4SUANAV+sckpp/+oZO2qwZ1YN3jWo5KDjr73rgE0:oBEAH33AVnpRoO1pWK/PbgE
MD5:	61C056D2DF7AB769D6FD801869B828A9
SHA1:	4213D0395692FA4181483FFB04EEF4BDA22CCEEE
SHA-256:	148D8F53BBA9A8D5558B192FB4919A5B0D9CB7FD9F8E481660F8667DE4E89B66
SHA-512:	A2DA2558C44E80973BADC2E5F283CEC254A12DFBCC66C352C8F394E03B1E50F98551303EAB6F7995AC4AFD5A503BD29B690D778B0526233EFC781695ED9E912
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.-.osC.osC.osC..oO.lsC..oM.tsC.lI..sC.lH.}sC.SI.jsC.osC.lsC.9IP.zsC.6PP.|sC.osB.}rC.SH.CsC.uE.nsC.SG.nsC.RichosC.....PE..L...s.;.....!.....`.....0.....pd.....XM.....H:.....I.....text..... ..`.rdata.....@..@.data....J.....0.....@....rsrc.....@..@.reloc.. H.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\isrtc335.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	331776
Entropy (8bit):	6.377016902367252
Encrypted:	false

SSDEEP:	6144:KzbdBEFj2WevDaaf4SUANAV+sckpp/+oZO2qwZ1YN3jWo5KDjr73rgE0:oBEAH33AVnpRoO1pWK/PbgE
MD5:	61C056D2DF7AB769D6FD801869B828A9
SHA1:	4213D0395692FA4181483FFB04EEF4BDA22CCEEE
SHA-256:	148D8F53BBA9A8D5558B192FB4919A5B0D9CB7FD9F8E481660F8667DE4E89B66
SHA-512:	A2DA2558C44E80973BADC2E5F283CEC254A12DFBCC66C352C8F394E03B1E50F98551303EAB6F7995AC4AFD5A503BD29B690D778B0526233EFC781695ED9E912
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.-.osC.osC.osC..oO.lsC..oM.tsC.lI..sC.lH.}sC.SI.jsC.osC.lsC.9lP.zsC.6PP.|sC.osB.}rC.SH.CsC.uE.nsC.SG.nsC.RichosC.....PE..L...s.;.....!.....`.....0.....pd.....XM.....H:.....I.....text..... ..`.rdata.....@..@.data....J.....0.....@....rsrc.....@..@.reloc.. H.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\setuc20d.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	data
Category:	dropped
Size (bytes):	174246
Entropy (8bit):	4.867152049703912
Encrypted:	false
SSDEEP:	1536:5zO7vcGlb5xhxrj8gDlL1nm3QzLgat1YRHU5CWb76pK/UWn9T12mrmHEhjpPWmr8:Sbh9jRRCK/Hy
MD5:	619D8A0CC00121812601D573CA1F6C95
SHA1:	CC2E25DC8D02F4ABF07B921645381D001D59B432
SHA-256:	8D0399C34F7CE6C66E6A0515A06FD893E1A2369CCE1FD3910B6EF0C312323841
SHA-512:	E0494BC16C3A5A6419525D2D2FEE81AEF99D31C926F85E4A30EAB1A47BD8B882DB406C27958662DB35B71DAED0BEE88ADE6A0E25A5B56E8832955FB8E0897EFB
Malicious:	false
Preview:	aLuZ..Copyright (c) 1990-1999 Stirling Technologies, Ltd. All Rights Reserved.....|...+.....z0..c...H.....J.....bWin95.....bWin9X.....bWin98.....bWinMe.....bSubversion_A.....bSubversion_B.....bSubversion_C.....bVersionNotFound.....bWinNT.....bWinNT4.....bWinNT351.....bWin2000.....bWinXP.....bAdmin_Logged_On.....nServicePack.....WINNT.....WIN9X.....bShellExplorer.....bAlpha.....bIntel.....nOSMajor.....nOSMinor.....nWinMajor.....nWinMinor.....int1.....int2.....dwEventType.....dwRestorePtType.....llSequenceNumber.@...szDescription.....nStatus.....llSequenceNumber.....cb.....lpReserved.....lpDesktop...lpTitle.....dwX.....dwY.....dwXSize.....dwYSize.....dwXCountChars.....dwYCountChars.....dwFillAttribute.....dwFlags.....wShowWindow.....lpReserved2.....hStdInput.....hStdOutput.....hStdError.....hProcess.....hThread.....dwProcessId.....dwThreadId.....nYearMonth.....nDay.....nHourMin.

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\setup.inx (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	data
Category:	dropped
Size (bytes):	174246
Entropy (8bit):	4.867152049703912
Encrypted:	false
SSDEEP:	1536:5zO7vcGlb5xhxrj8gDlL1nm3QzLgat1YRHU5CWb76pK/UWn9T12mrmHEhjpPWmr8:Sbh9jRRCK/Hy
MD5:	619D8A0CC00121812601D573CA1F6C95
SHA1:	CC2E25DC8D02F4ABF07B921645381D001D59B432
SHA-256:	8D0399C34F7CE6C66E6A0515A06FD893E1A2369CCE1FD3910B6EF0C312323841
SHA-512:	E0494BC16C3A5A6419525D2D2FEE81AEF99D31C926F85E4A30EAB1A47BD8B882DB406C27958662DB35B71DAED0BEE88ADE6A0E25A5B56E8832955FB8E0897EFB
Malicious:	false
Preview:	aLuZ..Copyright (c) 1990-1999 Stirling Technologies, Ltd. All Rights Reserved.....|...+.....z0..c...H.....J.....bWin95.....bWin9X.....bWin98.....bWinMe.....bSubversion_A.....bSubversion_B.....bSubversion_C.....bVersionNotFound.....bWinNT.....bWinNT4.....bWinNT351.....bWin2000.....bWinXP.....bAdmin_Logged_On.....nServicePack.....WINNT.....WIN9X.....bShellExplorer.....bAlpha.....bIntel.....nOSMajor.....nOSMinor.....nWinMajor.....nWinMinor.....int1.....int2.....dwEventType.....dwRestorePtType.....llSequenceNumber.@...szDescription.....nStatus.....llSequenceNumber.....cb.....lpReserved.....lpDesktop...lpTitle.....dwX.....dwY.....dwXSize.....dwYSize.....dwXCountChars.....dwYCountChars.....dwFillAttribute.....dwFlags.....wShowWindow.....lpReserved2.....hStdInput.....hStdOutput.....hStdError.....hProcess.....hThread.....dwProcessId.....dwThreadId.....nYearMonth.....nDay.....nHourMin.

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\valuc307.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Generic INItialization configuration [Data]
Category:	dropped
Size (bytes):	419
Entropy (8bit):	5.366788577730877
Encrypted:	false
SSDEEP:	12:1M8UyIMLYQ9GLYQ9CuhLxqyLYQ9ysSxRfcLYQ9r:1MZQLv8Lv4uhLYyLvsltcLvJ

MD5:	B71474C793EC448635B52BAF53AEB918
SHA1:	B580F46BA5FD949EFFB61CD39C9D3D77CB8642F4
SHA-256:	15ED93F703799AE5EAA08DA849123155FCB51509F1E7B250C5C54BF7213D5757
SHA-512:	6F749943D1B9BE7AB37DB07D520762D2B8F93E533DA58B2FB5777E9AEBD2F128DAF927C87B0C8979E3A8B8247607CABA73FC78EF462B3D739EDE75919520D1C7
Malicious:	false
Preview:	[General]..Type=STRINGTABLESPECIFIC..Version=1.00.000..Language=0009....[Data]..TITLE_MAIN=ViewSonic Windows 10 64bit Signed Files..TITLE_CAPTIONBAR=ViewSonic Windows 10 64bit Signed Files..COMPANY_NAME=ViewSonic Corporation..PRODUCT_NAME=ViewSonic Windows 10 64bit Signed Files..PRODUCT_KEY=Standard_Monitor_Driver_Signed_Win10_x64.exe..PRODUCT_VERSION=1.5.0.63..FOLDER_NAME=ViewSonic Windows 10 64bit Signed Files....

C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\value.shl (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Generic INItialization configuration [Data]
Category:	dropped
Size (bytes):	419
Entropy (8bit):	5.366788577730877
Encrypted:	false
SSDEEP:	12:1M8UyIMLYQ9GLYQ9CuhLxqyLYQ9ysSxRfcLYQ9r:1MZQLv8Lv4uhLYyLvsltcLvJ
MD5:	B71474C793EC448635B52BAF53AEB918
SHA1:	B580F46BA5FD949EFFB61CD39C9D3D77CB8642F4
SHA-256:	15ED93F703799AE5EAA08DA849123155FCB51509F1E7B250C5C54BF7213D5757
SHA-512:	6F749943D1B9BE7AB37DB07D520762D2B8F93E533DA58B2FB5777E9AEBD2F128DAF927C87B0C8979E3A8B8247607CABA73FC78EF462B3D739EDE75919520D1C7
Malicious:	false
Preview:	[General]..Type=STRINGTABLESPECIFIC..Version=1.00.000..Language=0009....[Data]..TITLE_MAIN=ViewSonic Windows 10 64bit Signed Files..TITLE_CAPTIONBAR=ViewSonic Windows 10 64bit Signed Files..COMPANY_NAME=ViewSonic Corporation..PRODUCT_NAME=ViewSonic Windows 10 64bit Signed Files..PRODUCT_KEY=Standard_Monitor_Driver_Signed_Win10_x64.exe..PRODUCT_VERSION=1.5.0.63..FOLDER_NAME=ViewSonic Windows 10 64bit Signed Files....

C:\ViewSonic\ID24398e.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Microsoft color profile 2.3, type lcms, RGB/XYZ-mntr device by VSC, 824 bytes, 3-6-2021 10:52:10 "ID2456 sRGB 6500K"
Category:	dropped
Size (bytes):	824
Entropy (8bit):	3.1658424298010788
Encrypted:	false
SSDEEP:	12:HmhEDqICfNVDVFLsrGhaTlYsloBzlG/ISD37QnJGp/RtRtthKJwJU:GhqqIGjvLHhaTlYsloBzl2PKGp5XYJE
MD5:	44B99C9FC60A4BBF8D33FA8AD6CE27E0
SHA1:	1BDDD16DFCB8A20DC31BF2B696B80C6A4E28D7F5
SHA-256:	393B63D4D2E4892F8341FBEFF868B9D9ABF1A1EE94F88B3A683ACDC1FA58C729
SHA-512:	733D66E2B77EDBA1CAD951EB5EB305D04DDF2051E016F19A282D8C5EFC6D93009A9C35AC30D6803623FB0C47DC364A159B2C36B955A48ADB58037222E7FCC83
Malicious:	false
Preview:	...8lcms.0..mntrRGB XYZ .....4..acspMSFT....VSC.....-VSC.....dmnd... ...pdesc.....ldmdd.....awtpt...`....rXYZ...t....bXYZ.....gXYZ.....rTRC.....gTRC.....bTRC.....chrm.....$cprt.....bkpt...$....desc.....ViewSonic Corporation.....desc.....ID2456 sRGB 6500K.....desc.....ID2456.....XYZ .....>.....XYZ .....;.....XYZ .....$.....7XYZ .....O;.....curv.....3..curv.....3..curv.....3..chrm.....O\..I....7..&%....text....ViewSonic Corporation...XYZ .....

C:\ViewSonic\ID2439bd.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2173
Entropy (8bit):	5.57346910118799
Encrypted:	false
SSDEEP:	48:5BMMcao5ueQyA4j+jBtBwe+pVQqVWhVwFcBNC:5BMM4Ja4j+jBzFK6q0hWFH
MD5:	BA4B1FD39CF1E25122D172F283DA58B7
SHA1:	6EA8AE2BCDBF9EDC4DA6C716D5E29882336E313C
SHA-256:	5DFCC28A33526E6AF1BD2D415B6FE783D3C1E345AF6A77A9FD52AE5F30212EC9
SHA-512:	A4C953F6341E7471D5F7D9E6B18B447DA704F1C6CE865CB22ECBBC678997B3F61C8175CDCF39BACD878B292E379532D8F7B6C4770699DF4ED0E59DEB5CBB654
Malicious:	false

Preview:	;Monitor.Inf..;Copyright 2021, ViewSonic Corporation....[Version] ..CatalogFile=ID2456.cat..PnpLockdown=1 ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=06/03/2021, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..ID2456.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..ID2456.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTamd64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSCA43C....[ViewSonic.NTx86] ..%ID2456_A%=ID2456_A.Install,Monitor\VSCA43C..%ID2456_D%=ID2456_D.Install,Monitor\VSCA43C....[ViewSonic.NTamd64] ..%ID2456_A%=ID2456_A.Install,Monitor\VSCA43C..%ID2456_D%=ID2456_D.Install,Monitor\VSCA43

C:\ViewSonic\IFP2e39.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1764
Entropy (8bit):	5.551267239545935
Encrypted:	false
SSDEEP:	24:tI2Q7Jo8MMLk8rBF+0Ro51LkeLsLCHAZpnhpVVorhVNP1nD5vy+pVoCreRVkLlgr:GBMMIco5ueQSE5Dwre+pVFWV9Km
MD5:	41C7CDD21106EE1A9EEE6116EF92D85C
SHA1:	EAD77B137D1CA40214F3E2CE75857D5BFE3DEEE4
SHA-256:	733AC21AA0C98DDBB72A820345345672BCEF5032779DF967CBB5E3164AED87A8
SHA-512:	BA2B052C5B35BE24B2428760E020E4E67E821E9F8565914BD87B2DCD0685F408DFA808908607A3EC2E7E655E9120D032BC41CF907063877654D243499D1AC721
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86/x64, 8 x86/x64, 10 x86/x64..;Copyright 2018, ViewSonic Corporation....[Version] ..CatalogFile=IFP2710.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=01/15/2018, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..IFP2710.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..IFP2710.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSCA436....[ViewSonic] ..%IFP2710%=IFP2710.Install,Monitor\VSCA436 ....[ViewSonic.NTx86] ..%IFP2710%=IFP2710.Install,Monitor\VSCA436....[ViewSonic.NTAMD64] ..%IFP2710%=IFP2710.Install,Monitor\

C:\ViewSonic\PJD5132.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2337
Entropy (8bit):	5.589053536173171
Encrypted:	false
SSDEEP:	48:NBMMVEo5ueQSmzmZjD3lj4A2Q1QUjliV9R0VaEV7Q:NBMMxJ0aZjD3lj4fQ1QliN0oEBQ
MD5:	79974261CCBBF1D2143B2DEEACB4510B
SHA1:	7B28704A5844333A848166C84E7198A2987D9011
SHA-256:	0A9FC9632A5C7E3B995850F34926FC74D7D6E50AD18150CFF1FDCB77D83FA962
SHA-512:	6434347BF86BEE68000ECD3C87879F2A676334E22766FC6B7870DC1A5EEAB8508D9D0A502D0209CBB86F5A1C9258EB1A8B3278A028C3D375E56D3F70B752868
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD5132.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/03/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..PJD5132.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD5132.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC622C..ExcludeFromSelect.nt=Monitor\VSC652C....[ViewSonic] ..%PJD5132%=PJD5132.Install,Monitor\VSC622C ..%PJD5232L%=PJD5232L.Install,Monitor\VSC652C....[ViewSonic.NTx86] ..%PJD5132%=PJD5132.Install

C:\ViewSonic\PJD5134.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2953
Entropy (8bit):	5.633435889655384
Encrypted:	false
SSDEEP:	48:OeBMMV+Bo5ueQSm5mXjXNSdNSPNSc0R10R/F0RCtNEliVtNVW3VbB4VPVxq:OeBMM46J08TXNSdNSPNSc0R10R/F0R0j
MD5:	1B0B28AA5B084D8326D47F4C24312203
SHA1:	35EA558A763F85D0E95CC2B8231EC1D5C3E0145F
SHA-256:	8CBCA618501DC99C95C9CA030C5D32B11A371A5818868556E38410A9448D5038
SHA-512:	3D8FA476CBD8C7231C69FD49E23B7345385C81C9547B187A211B2654198382BB9A041408CB8AB7887BD3E3AD81350163A9E6BC59CA8F3C5037309F01836B9506
Malicious:	false

Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD5134.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/03/2013, 1.5.0.0....[DestinationDirs]..Defa ultDestDir= 12..PJD5134.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD5134.ICM=1....[Monitor_Service.Install]..DisplayName = % Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromS elect.nt=Monitor\VSC642C..ExcludeFromSelect.nt=Monitor\VSC662C..ExcludeFromSelect.nt=Monitor\VSC3929....[ViewSonic] ..%PJD5134%=PJD5134.Install,Moni tor\VSC642C ..%PJD5234L%=PJD5234L.Install,Monitor\VSC662C..%PJD5533w%=

C:\ViewSonic\PJD5134.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2953
Entropy (8bit):	5.633435889655384
Encrypted:	false
SSDEEP:	48:OeBMMV+Bo5ueQSm5mXjXNSdNSPNSc0R10R/F0RCtNEliVtNVW3VbB4VPVxq:OeBMM46J08TXNSdNSPNSc0R10R/F0R0j
MD5:	1B0B28AA5B084D8326D47F4C24312203
SHA1:	35EA558A763F85D0E95CC2B8231EC1D5C3E0145F
SHA-256:	8CBCA618501DC99C95C9CA030C5D32B11A371A5818868556E38410A9448D5038
SHA-512:	3D8FA476CBD8C7231C69FD49E23B7345385C81C9547B187A211B2654198382BB9A041408CB8AB7887BD3E3AD81350163A9E6BC59CA8F3C5037309F01836B9506
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD5134.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/03/2013, 1.5.0.0....[DestinationDirs]..Defa ultDestDir= 12..PJD5134.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD5134.ICM=1....[Monitor_Service.Install]..DisplayName = % Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromS elect.nt=Monitor\VSC642C..ExcludeFromSelect.nt=Monitor\VSC662C..ExcludeFromSelect.nt=Monitor\VSC3929....[ViewSonic] ..%PJD5134%=PJD5134.Install,Moni tor\VSC642C ..%PJD5234L%=PJD5234L.Install,Monitor\VSC662C..%PJD5533w%=

C:\ViewSonic\PJD5234.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Microsoft color profile 2.0, type appl, RGB/XYZ-mntr device, 512 bytes, 30-8-2012 11:15:35, PCS Z=0xd32c "PJD5234"
Category:	dropped
Size (bytes):	512
Entropy (8bit):	3.7351058964577124
Encrypted:	false
SSDEEP:	12:uPII7l/Cle/UD7sVWCD9AlL08wwG/atRtRtySP6/TiG:uD7INUDYVJAl7XXT6/Tz
MD5:	42D2E612E5364A133FC2F504BADC46F0
SHA1:	20F6DD1BB3F60288F86634C26FE76BDAE30570B4
SHA-256:	6DDAF5C0E7196B7FA7D9F73E272C3A03D99C5952145F27D984B3006C1CB0A819
SHA-512:	0928A87DB3586A856B73B282D3BE1D3C8B5D0FB6C1FBFA6C44FC0FD42107CC682827E736F77C3F5182EF334F77C4ABAC57D922D902A2EF03D7AC93C46E1E08 8
Malicious:	false
Preview:	....appl....mntrRGB XYZ .....#acspMSFT....NONE.....,.....desc.....0rXYZ...,....gXYZ...@....bXYZ...T....rTRC...h....gTRC...x ....bTRC.....wtpt.....cprt.....@calt.....desc.....PJD5234.....XYZ .....U...(.....XYZ .....XYZ ....<....curv.....3..curv.....3..curv.....3..XYZ .....text....Copyright . 2012 ViewSonic Corporation.....dtim.....#

C:\ViewSonic\PJD5234.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2338
Entropy (8bit):	5.601169277105082
Encrypted:	false
SSDEEP:	48:sBMMVAo5ueQSSFYgpdptmIiVkP3VWGVyc:sBMMVJc1pdp1iw3lGgc
MD5:	A047F6CF8C15AEDA86135D28CCC31CA3
SHA1:	324FE362E004FE0AF3359A357AEA2E138ECE1ACE
SHA-256:	597D3BEBAAE22E8F4C419D31E00C20AD5A3C73B181536E8F01889E0813E5013A
SHA-512:	694A70460F454834B548112A646AE96F7F047C26045148159E1FB1C14CEC4494001143F1D234261336BC150D080269E3674E7C0636D42790929BEF5034B31099
Malicious:	false

Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD5234.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/03/2013, 1.5.0.0....[DestinationDirs]..Defa ultDestDir= 12..PJD5234.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD5234.ICM=1....[Monitor_Service.Install]..DisplayName = % Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromS elect.nt=Monitor\VSC8D2C..ExcludeFromSelect.nt=Monitor\VSCFF2C....[ViewSonic] ..%PJD5234%=PJD5234.Install,Monitor\VSC8D2C ..%PJD5483s%=PJD5483s.Inst all,Monitor\VSCFF2C....[ViewSonic.NTx86] ..%PJD5234%=PJD5234.Install

C:\ViewSonic\PJD5d68f.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2337
Entropy (8bit):	5.589053536173171
Encrypted:	false
SSDEEP:	48:NBMMVEo5ueQSmzmZjD3lj4A2Q1QUjIiV9R0VaEV7Q:NBMMxJ0aZjD3lj4fQ1QliN0oEBQ
MD5:	79974261CCBBF1D2143B2DEEACB4510B
SHA1:	7B28704A5844333A848166C84E7198A2987D9011
SHA-256:	0A9FC9632A5C7E3B995850F34926FC74D7D6E50AD18150CFF1FDCB77D83FA962
SHA-512:	6434347BF86BEE68000ECD3C87879F2A676334E22766FC6B7870DC1A5EEAB8508D9D0A502D0209CBB86F5A1C9258EB1A8B3278A028C3D375E56D3F70B752868
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD5132.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/03/2013, 1.5.0.0....[DestinationDirs]..Defa ultDestDir= 12..PJD5132.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD5132.ICM=1....[Monitor_Service.Install]..DisplayName = % Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromS elect.nt=Monitor\VSC622C..ExcludeFromSelect.nt=Monitor\VSC652C....[ViewSonic] ..%PJD5132%=PJD5132.Install,Monitor\VSC622C ..%PJD5232L%=PJD5232L.Inst all,Monitor\VSC652C....[ViewSonic.NTx86] ..%PJD5132%=PJD5132.Install

C:\ViewSonic\PJD5d789.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Microsoft color profile 2.0, type appl, RGB/XYZ-mntr device, 512 bytes, 30-8-2012 11:15:35, PCS Z=0xd32c "PJD5234"
Category:	dropped
Size (bytes):	512
Entropy (8bit):	3.7351058964577124
Encrypted:	false
SSDEEP:	12:uPII7l/Cle/UD7sVWCD9AlL08wwG/atRtRtySP6/TiG:uD7INUDYVJAl7XXT6/Tz
MD5:	42D2E612E5364A133FC2F504BADC46F0
SHA1:	20F6DD1BB3F60288F86634C26FE76BDAE30570B4
SHA-256:	6DDAF5C0E7196B7FA7D9F73E272C3A03D99C5952145F27D984B3006C1CB0A819
SHA-512:	0928A87DB3586A856B73B282D3BE1D3C8B5D0FB6C1FBFA6C44FC0FD42107CC682827E736F77C3F5182EF334F77C4ABAC57D922D902A2EF03D7AC93C46E1E08 8
Malicious:	false
Preview:	....appl....mntrRGB XYZ .....#acspMSFT....NONE.....,.....desc.....0rXYZ...,....gXYZ...@....bXYZ...T....rTRC...h....gTRC...x ....bTRC.....wtpt.....cprt.....@calt.....desc.....PJD5234.....XYZ .....U...(.....XYZ .....XYZ ....<....curv.....3..curv.....3..curv.....3..XYZ .....text....Copyright . 2012 ViewSonic Corporation.....dtim.....#

C:\ViewSonic\PJD5d7b7.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2338
Entropy (8bit):	5.601169277105082
Encrypted:	false
SSDEEP:	48:sBMMVAo5ueQSSFYgpdptmIiVkP3VWGVyc:sBMMVJc1pdp1iw3lGgc
MD5:	A047F6CF8C15AEDA86135D28CCC31CA3
SHA1:	324FE362E004FE0AF3359A357AEA2E138ECE1ACE
SHA-256:	597D3BEBAAE22E8F4C419D31E00C20AD5A3C73B181536E8F01889E0813E5013A
SHA-512:	694A70460F454834B548112A646AE96F7F047C26045148159E1FB1C14CEC4494001143F1D234261336BC150D080269E3674E7C0636D42790929BEF5034B31099
Malicious:	false

Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD5234.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/03/2013, 1.5.0.0....[DestinationDirs]..Defa ultDestDir= 12..PJD5234.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD5234.ICM=1....[Monitor_Service.Install]..DisplayName = % Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromS elect.nt=Monitor\VSC8D2C..ExcludeFromSelect.nt=Monitor\VSCFF2C....[ViewSonic] ..%PJD5234%=PJD5234.Install,Monitor\VSC8D2C ..%PJD5483s%=PJD5483s.Inst all,Monitor\VSCFF2C....[ViewSonic.NTx86] ..%PJD5234%=PJD5234.Install

C:\ViewSonic\PJD5d883.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2953
Entropy (8bit):	5.633435889655384
Encrypted:	false
SSDEEP:	48:OeBMMV+Bo5ueQSm5mXjXNSdNSPNSc0R10R/F0RCtNEliVtNVW3VbB4VPVxq:OeBMM46J08TXNSdNSPNSc0R10R/F0R0j
MD5:	1B0B28AA5B084D8326D47F4C24312203
SHA1:	35EA558A763F85D0E95CC2B8231EC1D5C3E0145F
SHA-256:	8CBCA618501DC99C95C9CA030C5D32B11A371A5818868556E38410A9448D5038
SHA-512:	3D8FA476CBD8C7231C69FD49E23B7345385C81C9547B187A211B2654198382BB9A041408CB8AB7887BD3E3AD81350163A9E6BC59CA8F3C5037309F01836B9506
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD5134.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/03/2013, 1.5.0.0....[DestinationDirs]..Defa ultDestDir= 12..PJD5134.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD5134.ICM=1....[Monitor_Service.Install]..DisplayName = % Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromS elect.nt=Monitor\VSC642C..ExcludeFromSelect.nt=Monitor\VSC662C..ExcludeFromSelect.nt=Monitor\VSC3929....[ViewSonic] ..%PJD5134%=PJD5134.Install,Moni tor\VSC642C ..%PJD5234L%=PJD5234L.Install,Monitor\VSC662C..%PJD5533w%=

C:\ViewSonic\PJD6543w.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Microsoft color profile 2.0, type appl, RGB/XYZ-mntr device, 512 bytes, 25-9-2012 16:30:00, PCS Z=0xd32c "PJD6543w"
Category:	dropped
Size (bytes):	512
Entropy (8bit):	3.7439004743055793
Encrypted:	false
SSDEEP:	12:uyH7l/Cle/UD7sVWCD9Alh3YxGNRtRtyKIq/B/Zs:uyH7lNUDYVJAlS+Xiq/BRs
MD5:	78AEF7FE19722DD6974A5D51F94CE024
SHA1:	DCD6FBF06E322D2854E91D7980AAB02694D882B5
SHA-256:	AFAF6A14B766885C516DCA660A5CA66ECB2A3659F9B95E7F0D9D32D10755BB39
SHA-512:	90147CDD144CF23E7047F0C9956810780BE0FCD0D775A1DBC79CC9B651BE4DC0089428E402911454CE90B9E96151EA83B6CE130BBECB81AA89060D312AAA47 E
Malicious:	false
Preview:	....appl....mntrRGB XYZ .....acspMSFT....NONE.....,.....desc.....0rXYZ...,....gXYZ...@....bXYZ...T....rTRC...h....gTRC...x ....bTRC.....wtpt.....cprt.....@calt.....desc.....PJD6543w.....XYZ .....A..."....mXYZ .....d.../XYZ .....#.....curv.....3..curv.....3..curv.....3..XYZ .....text....Copyright . 2012 ViewSonic Corporation.....3...dtim.....

C:\ViewSonic\PJD6543w.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2570
Entropy (8bit):	5.618014851472671
Encrypted:	false
SSDEEP:	48:LBMMHcMo5ueQSmqmUmPvgthvytTvgtELVG8WG5GliVT63VPYVDG9N:LBMMHeJ0XNPvgthvytTvgtEhGdGli83V
MD5:	C9053691557F521D3B25C3CD869FD1C1
SHA1:	031C2733A89FCC91ECCE71D15CD4D421539B1E3B
SHA-256:	336D352B8C1DD13AB95902FD14DB45E21432F35B15D5A575E57B4862907B6DA2
SHA-512:	23AE1C44E0E195402A380D997ABE05C34E07E2ED19ACB6064BDDE62B237C35027105D46565D63C75E2A4CB63B7B1B7B90883BEFE16D2A1D0EEFCC24A08298F 60
Malicious:	false

Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD6543w.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/22/2013, 1.5.0.0....[DestinationDirs]..Def aultDestDir= 12..PJD6543w.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD6543w.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFr omSelect.nt=Monitor\VSC6A2C..ExcludeFromSelect.nt=Monitor\VSC672C..ExcludeFromSelect.nt=Monitor\VSC692C....[ViewSonic] ..%PJD6543w%=PJD6543w.Install ,Monitor\VSC6A2C..%PJD6235%=PJD6235.Install,Monitor\VSC672C ..%PJD6245

C:\ViewSonic\PJD6d6bd.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Microsoft color profile 2.0, type appl, RGB/XYZ-mntr device, 512 bytes, 25-9-2012 16:30:00, PCS Z=0xd32c "PJD6543w"
Category:	dropped
Size (bytes):	512
Entropy (8bit):	3.7439004743055793
Encrypted:	false
SSDEEP:	12:uyH7I/Cle/UD7sVWCD9Alh3YxGNRtRtyKIq/B/Zs:uyH7INUDYVJAlS+Xiq/BRs
MD5:	78AEF7FE19722DD6974A5D51F94CE024
SHA1:	DCD6FBF06E322D2854E91D7980AAB02694D882B5
SHA-256:	AFAF6A14B766885C516DCA660A5CA66ECB2A3659F9B95E7F0D9D32D10755BB39
SHA-512:	90147CDD144CF23E7047F0C9956810780BE0FCD0D775A1DBC79CC9B651BE4DC0089428E402911454CE90B9E96151EA83B6CE130BBECB81AA89060D312AAA47E
Malicious:	false
Preview:	....appl....mntrRGB XYZ .....acspMSFT....NONE.....,.....desc.....0rXYZ...,....gXYZ...@....bXYZ...T....rTRC...h....gTRC...x ....bTRC.....wtpt.....cprt.....@calt.....desc.....PJD6543w.....XYZ .....A..."....mXYZ .....d.../XYZ .....#.....curv.....3..curv.....3..curv.....3..XYZ .....text....Copyright . 2012 ViewSonic Corporation.....3...dtim.....

C:\ViewSonic\PJD6d6ec.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2570
Entropy (8bit):	5.618014851472671
Encrypted:	false
SSDEEP:	48:LBMMHcMo5ueQSmqmUmPvgthvytTvgtELVG8WG5GliVT63VPYVDG9N:LBMMHeJ0XNPvgthvytTvgtEhGdGli83V
MD5:	C9053691557F521D3B25C3CD869FD1C1
SHA1:	031C2733A89FCC91ECCE71D15CD4D421539B1E3B
SHA-256:	336D352B8C1DD13AB95902FD14DB45E21432F35B15D5A575E57B4862907B6DA2
SHA-512:	23AE1C44E0E195402A380D997ABE05C34E07E2ED19ACB6064BDDE62B237C35027105D46565D63C75E2A4CB63B7B1B7B90883BEFE16D2A1D0EEFCC24A08298F60
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD6543w.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/22/2013, 1.5.0.0....[DestinationDirs]..Def aultDestDir= 12..PJD6543w.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD6543w.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFr omSelect.nt=Monitor\VSC6A2C..ExcludeFromSelect.nt=Monitor\VSC672C..ExcludeFromSelect.nt=Monitor\VSC692C....[ViewSonic] ..%PJD6543w%=PJD6543w.Install ,Monitor\VSC6A2C..%PJD6235%=PJD6235.Install,Monitor\VSC672C ..%PJD6245

C:\ViewSonic\PJD7820HD.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1776
Entropy (8bit):	5.548687317017361
Encrypted:	false
SSDEEP:	24:t6QDJo8MMLr8rH+0Ro51LkeLsLCHmhXaluhX+auhXa4uhXCorBSOP1FD5vyiV5VM:vBMMPco5ueQSmhihAhehjSOIiV5aVRtJ
MD5:	8A479B8DD5C9CDA9C70BD7496ABCCC08
SHA1:	007ED4BE8DAA817C7BE7F1F7CC9A7F2154911997
SHA-256:	D9AC10AAEA519B4DD3B8943D58044DB896AB13AB8C0843579725D712C19E279A
SHA-512:	5CA67CF07D22E27CB04E8CB4104C176DCD4D4EE567B0794E633401FC2340DEA5D8BB2EE8F5D9D96835B36F8DC52821099A1912D7FB1CD8C7D5163DF200EAF4F
Malicious:	false

Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD7820HD.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=01/15/2013, 1.5.0.0....[DestinationDirs]..De faultDestDir= 12..PJD7820HD.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD7820HD.ICM=1....[Monitor_Service.Install]..Di splayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..E rrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[C ontrolFlags]..ExcludeFromSelect.nt=Monitor\VSC6D2C....[ViewSonic] ..%PJD7820HD%=PJD7820HD.Install,Monitor\VSC6D2C ....[ViewSonic.NTx86] ..%PJD7820 HD%=PJD7820HD.Install,Monitor\VSC6D2C....[ViewSonic.NTAMD64] ..%PJD7820HD%=PJD7820HD.Ins

C:\ViewSonic\PJD7d42d.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1776
Entropy (8bit):	5.548687317017361
Encrypted:	false
SSDEEP:	24:t6QDJo8MMLr8rH+0Ro51LkeLsLCHmhXaluhX+auhXa4uhXCorBSOP1FD5vyiV5VM:vBMMPco5ueQSmhihAhehjSOliV5aVRtJ
MD5:	8A479B8DD5C9CDA9C70BD7496ABCCC08
SHA1:	007ED4BE8DAA817C7BE7F1F7CC9A7F2154911997
SHA-256:	D9AC10AAEA519B4DD3B8943D58044DB896AB13AB8C0843579725D712C19E279A
SHA-512:	5CA67CF07D22E27CB04E8CB4104C176DCD4D4EE567B0794E633401FC2340DEA5D8BB2EE8F5D9D96835B36F8DC52821099A1912D7FB1CD8C7D5163DF200EAF 4F
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD7820HD.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=01/15/2013, 1.5.0.0....[DestinationDirs]..De faultDestDir= 12..PJD7820HD.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD7820HD.ICM=1....[Monitor_Service.Install]..Di splayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..E rrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[C ontrolFlags]..ExcludeFromSelect.nt=Monitor\VSC6D2C....[ViewSonic] ..%PJD7820HD%=PJD7820HD.Install,Monitor\VSC6D2C ....[ViewSonic.NTx86] ..%PJD7820 HD%=PJD7820HD.Install,Monitor\VSC6D2C....[ViewSonic.NTAMD64] ..%PJD7820HD%=PJD7820HD.Ins

C:\ViewSonic\PJD8353s.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2375
Entropy (8bit):	5.59006929235629
Encrypted:	false
SSDEEP:	48:aBMM4ceo5ueQSOUmeiHVndnt3liVO3VryVkJV4:aBMM4MJcVndn6iw3FyiJV4
MD5:	C4851815F654CCC87EF6ED15692C1785
SHA1:	DD66BDF0DB30231A240F69CD39884C50A880C361
SHA-256:	575A31630F65BA217CCF5E1E835E5A6A6264608E05A0115010A7CF3E15303CB8
SHA-512:	C643BDDF163985C61D9BB905F5FC66031F73BC8FBAC9A343B5EB10E9E7E8119EF82AE1B00A569232081A35B46D3489C8281FF22A635385886C9B2ABB3463730
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD8353s.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=03/04/2013, 1.5.0.0....[DestinationDirs]..Def aultDestDir= 12..PJD8353s.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD8353s.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFr omSelect.nt=Monitor\VSCA32C..ExcludeFromSelect.nt=Monitor\VSC802C....[ViewSonic] ..%PJD8353s%=PJD8353s.Install,Monitor\VSCA32C ..%PJD8653w s%=PJD8653ws.Install,Monitor\VSC802C....[ViewSonic.NTx86] ..%PJD8353s%=PJD8353

C:\ViewSonic\PJD8353s.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2375
Entropy (8bit):	5.59006929235629
Encrypted:	false
SSDEEP:	48:aBMM4ceo5ueQSOUmeiHVndnt3liVO3VryVkJV4:aBMM4MJcVndn6iw3FyiJV4
MD5:	C4851815F654CCC87EF6ED15692C1785
SHA1:	DD66BDF0DB30231A240F69CD39884C50A880C361
SHA-256:	575A31630F65BA217CCF5E1E835E5A6A6264608E05A0115010A7CF3E15303CB8
SHA-512:	C643BDDF163985C61D9BB905F5FC66031F73BC8FBAC9A343B5EB10E9E7E8119EF82AE1B00A569232081A35B46D3489C8281FF22A635385886C9B2ABB3463730
Malicious:	false

Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD8353s.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=03/04/2013, 1.5.0.0....[DestinationDirs]..Def aultDestDir= 12..PJD8353s.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD8353s.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFr omSelect.nt=Monitor\VSCA32C..ExcludeFromSelect.nt=Monitor\VSC802C....[ViewSonic] ..%PJD8353s%=PJD8353s.Install,Monitor\VSCA32C ..%PJD8653w s%=PJD8653ws.Install,Monitor\VSC802C....[ViewSonic.NTx86] ..%PJD8353s%=PJD8353

C:\ViewSonic\PJD8633ws.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	4906
Entropy (8bit):	5.650913728691022
Encrypted:	false
SSDEEP:	96:6BMMfJ0JM+Uw+vM+ZNDdDJD1DlDID/iV5Sr9JDnFDuSC6:6MMfJOknZ6V5Sr9JDnFDv
MD5:	28822AA2FEAF6CF81125B0AC7EE3E838
SHA1:	DF0AE3BFACD90940B2520D45DC9A7D5F5524A0A5
SHA-256:	78F1C103936C6E9E65E96F82B534F48BD2EB8FBD4D62DAF23CF9982BFCEC79C3
SHA-512:	67D1533BD6A46F4EC5E6ACECBF142E5622D78F6DD4C32E7DD9AD48BC7BFDE4C01890893F742A0466168EB4F8CA197997B2D79428C8A42255A898EFB2109A2D 22
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD8633ws.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/23/2013, 1.5.0.0....[DestinationDirs]..De faultDestDir= 12..PJD8633ws.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD8633ws.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelec t.nt=Monitor\VSC6B2C..ExcludeFromSelect.nt=Monitor\VSC8F2C..ExcludeFromSelect.nt=Monitor\VSC912C..ExcludeFromSelect.nt=Monitor\VSC782C..ExcludeFromSel ect.nt=Monitor\VSC7A2C..ExcludeFromSelect.nt=Monitor\VSC762C

C:\ViewSonic\PJD8d49b.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2375
Entropy (8bit):	5.59006929235629
Encrypted:	false
SSDEEP:	48:aBMM4ceo5ueQSOUmeiHVndnt3IiVO3VryVkJV4:aBMM4MJcVndn6iw3FyiJV4
MD5:	C4851815F654CCC87EF6ED15692C1785
SHA1:	DD66BDF0DB30231A240F69CD39884C50A880C361
SHA-256:	575A31630F65BA217CCF5E1E835E5A6A6264608E05A0115010A7CF3E15303CB8
SHA-512:	C643BDDF163985C61D9BB905F5FC66031F73BC8FBAC9A343B5EB10E9E7E8119EF82AE1B00A569232081A35B46D3489C8281FF22A635385886C9B2ABB3463730
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD8353s.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=03/04/2013, 1.5.0.0....[DestinationDirs]..Def aultDestDir= 12..PJD8353s.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD8353s.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFr omSelect.nt=Monitor\VSCA32C..ExcludeFromSelect.nt=Monitor\VSC802C....[ViewSonic] ..%PJD8353s%=PJD8353s.Install,Monitor\VSCA32C ..%PJD8653w s%=PJD8653ws.Install,Monitor\VSC802C....[ViewSonic.NTx86] ..%PJD8353s%=PJD8353

C:\ViewSonic\PJD8d815.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	4906
Entropy (8bit):	5.650913728691022
Encrypted:	false
SSDEEP:	96:6BMMfJ0JM+Uw+vM+ZNDdDJD1DlDID/iV5Sr9JDnFDuSC6:6MMfJOknZ6V5Sr9JDnFDv
MD5:	28822AA2FEAF6CF81125B0AC7EE3E838
SHA1:	DF0AE3BFACD90940B2520D45DC9A7D5F5524A0A5
SHA-256:	78F1C103936C6E9E65E96F82B534F48BD2EB8FBD4D62DAF23CF9982BFCEC79C3
SHA-512:	67D1533BD6A46F4EC5E6ACECBF142E5622D78F6DD4C32E7DD9AD48BC7BFDE4C01890893F742A0466168EB4F8CA197997B2D79428C8A42255A898EFB2109A2D 22
Malicious:	false

Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=PJD8633ws.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/23/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..PJD8633ws.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..PJD8633ws.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC6B2C..ExcludeFromSelect.nt=Monitor\VSC8F2C..ExcludeFromSelect.nt=Monitor\VSC912C..ExcludeFromSelect.nt=Monitor\VSC782C..ExcludeFromSelect.nt=Monitor\VSC7A2C..ExcludeFromSelect.nt=Monitor\VSC762C

C:\ViewSonic\Pro10100.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2364
Entropy (8bit):	5.45902819019518
Encrypted:	false
SSDEEP:	48:1BMMi0o5ueQSIqUSMo9o2/IiVBRVI6VdF:1BMM0JUo9opivRK6TF
MD5:	47257A37C7A2092E2FE6A9FBC5A881B9
SHA1:	BECF5B07FFE1AA2B9B3B44839FE9B9B190F52244
SHA-256:	5729334E527EBB8124579666A9B797F582C37C1747F4461B96E39154174010B4
SHA-512:	84ADFB8A7D4A69A2CDC76BF2451A4F1925D55C3308AC11E7AE4729215AE07E8661D1E882C98F315B8B9706B41AD9CDF480AE265C6947E821CDAF491E3E2610 6
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=Pro10100.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=05/09/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..Pro10100.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..Pro10100.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC412D..ExcludeFromSelect.nt=Monitor\VSCC92E....[ViewSonic] ..%Pro10100%=Pro10100.Install,Monitor\VSC412D ..%Pro10500w%=Pro10500w.Install,Monitor\VSCC92E....[ViewSonic.NTx86] ..%Pro10100%=Pro1010

C:\ViewSonic\Pro1db42.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2364
Entropy (8bit):	5.45902819019518
Encrypted:	false
SSDEEP:	48:1BMMi0o5ueQSIqUSMo9o2/IiVBRVI6VdF:1BMM0JUo9opivRK6TF
MD5:	47257A37C7A2092E2FE6A9FBC5A881B9
SHA1:	BECF5B07FFE1AA2B9B3B44839FE9B9B190F52244
SHA-256:	5729334E527EBB8124579666A9B797F582C37C1747F4461B96E39154174010B4
SHA-512:	84ADFB8A7D4A69A2CDC76BF2451A4F1925D55C3308AC11E7AE4729215AE07E8661D1E882C98F315B8B9706B41AD9CDF480AE265C6947E821CDAF491E3E2610 6
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=Pro10100.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=05/09/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..Pro10100.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..Pro10100.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC412D..ExcludeFromSelect.nt=Monitor\VSCC92E....[ViewSonic] ..%Pro10100%=Pro10100.Install,Monitor\VSC412D ..%Pro10500w%=Pro10500w.Install,Monitor\VSCC92E....[ViewSonic.NTx86] ..%Pro10100%=Pro1010

C:\ViewSonic\SD-T225.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1760
Entropy (8bit):	5.513589372625848
Encrypted:	false
SSDEEP:	24:t6QfIJo8MMLy8r3+0Ro51LkeLsLCH+KneMn6anW5ortV2MxP1FD5vy+pVSsHfeR7:xBMM+0o5ueQSbpbFVrl+pVSsCVr2A
MD5:	3FA0AD47328B4B138D514364BFB1E816
SHA1:	46B10145C04996733F2425703C22CB16538DB25A
SHA-256:	E17421023957447D8427BE001CC0BB9B474825465F45782F9EAB2C277B8CB277
SHA-512:	5BBC5B2B081399121D0A79C24A0087999DB047FCC987AF9D49FB10362180CEC4100CBC5B789C1D1153D47D4B6C59EB1AACE8144C5CD53EF2935419084251EF 0

Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=SD-T225.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=12/23/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..SD-T225.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..SD-T225.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC912F....[ViewSonic] ..%SD-T225%=SD-T225.Install,Monitor\VSC912F ....[ViewSonic.NTx86] ..%SD-T225%=SD-T225.Install,Monitor\VSC912F....[ViewSonic.NTAMD64] ..%SD-T225%=SD-T225.Install,Monitor\VSC91

C:\ViewSonic\SD-T225.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1760
Entropy (8bit):	5.513589372625848
Encrypted:	false
SSDEEP:	24:t6QfIJo8MMLy8r3+0Ro51LkeLsLCH+KneMn6anW5ortV2MxP1FD5vy+pVSsHfeR7:xBMM+0o5ueQSbpbFVrI+pVSsCVr2A
MD5:	3FA0AD47328B4B138D514364BFB1E816
SHA1:	46B10145C04996733F2425703C22CB16538DB25A
SHA-256:	E17421023957447D8427BE001CC0BB9B474825465F45782F9EAB2C277B8CB277
SHA-512:	5BBC5B2B081399121D0A79C24A0087999DB047FCC987AF9D49FB10362180CEC4100CBC5B789C1D1153D47D4B6C59EB1AACE8144C5CD53EF2935419084251EF0
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=SD-T225.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=12/23/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..SD-T225.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..SD-T225.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC912F....[ViewSonic] ..%SD-T225%=SD-T225.Install,Monitor\VSC912F ....[ViewSonic.NTx86] ..%SD-T225%=SD-T225.Install,Monitor\VSC912F....[ViewSonic.NTAMD64] ..%SD-T225%=SD-T225.Install,Monitor\VSC91

C:\ViewSonic\SD-T245.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1760
Entropy (8bit):	5.5318973449677316
Encrypted:	false
SSDEEP:	24:t6QfRFJo8MMLy8rf+0Ro51LkeLsLCHyK+MaamorXV2OP1FD5vy+pV8sHfeRVeioQ:TBMM+Eo5ueQSvJ7lVnI+pV8sCVtiC
MD5:	5235BC34D69032836EF121B7864BA47B
SHA1:	03E530C554C3546293BAAD487489CC3A6CCEB214
SHA-256:	A958EF2D1895A225ADF551DCD2B41251376F90298819FCC490FAACE245321804
SHA-512:	0EF45B1195A72F89F7D5DA50DF8D72996A9B4C8256AAC23F5580254CF6F9C8EC3257779C5B765A8E32D65EF151FB953D207FDFEBDF0A08A40B46FD03405D3FA0
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=SD-T245.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=12/23/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..SD-T245.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..SD-T245.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC8F2F....[ViewSonic] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F2F ....[ViewSonic.NTx86] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F2F....[ViewSonic.NTAMD64] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F

C:\ViewSonic\SD-T245.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1760
Entropy (8bit):	5.5318973449677316
Encrypted:	false
SSDEEP:	24:t6QfRFJo8MMLy8rf+0Ro51LkeLsLCHyK+MaamorXV2OP1FD5vy+pV8sHfeRVeioQ:TBMM+Eo5ueQSvJ7lVnI+pV8sCVtiC
MD5:	5235BC34D69032836EF121B7864BA47B
SHA1:	03E530C554C3546293BAAD487489CC3A6CCEB214
SHA-256:	A958EF2D1895A225ADF551DCD2B41251376F90298819FCC490FAACE245321804

SHA-512:	0EF45B1195A72F89F7D5DA50DF8D72996A9B4C8256AAC23F5580254CF6F9C8EC3257779C5B765A8E32D65EF151FB953D207FDFEBDF0A08A40B46FD03405D3FA0
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=SD-T245.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=12/23/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..SD-T245.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..SD-T245.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC8F2F....[ViewSonic] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F2F ....[ViewSonic.NTx86] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F2F....[ViewSonic.NTAMD64] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F

C:\ViewSonic\SD-Te10e.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1760
Entropy (8bit):	5.5318973449677316
Encrypted:	false
SSDEEP:	24:t6QfRFJo8MMLy8rf+0Ro51LkeLsLCHyK+MaamorXV2OP1FD5vy+pV8sHfeRVeioQ:TBMM+Eo5ueQSvJ7lVnI+pV8sCVtiC
MD5:	5235BC34D69032836EF121B7864BA47B
SHA1:	03E530C554C3546293BAAD487489CC3A6CCEB214
SHA-256:	A958EF2D1895A225ADF551DCD2B41251376F90298819FCC490FAACE245321804
SHA-512:	0EF45B1195A72F89F7D5DA50DF8D72996A9B4C8256AAC23F5580254CF6F9C8EC3257779C5B765A8E32D65EF151FB953D207FDFEBDF0A08A40B46FD03405D3FA0
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=SD-T245.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=12/23/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..SD-T245.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..SD-T245.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC8F2F....[ViewSonic] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F2F ....[ViewSonic.NTx86] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F2F....[ViewSonic.NTAMD64] ..%SD-T245%=SD-T245.Install,Monitor\VSC8F

C:\ViewSonic\SD-Te1aa.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1760
Entropy (8bit):	5.513589372625848
Encrypted:	false
SSDEEP:	24:t6QfIJo8MMLy8r3+0Ro51LkeLsLCH+KneMn6anW5ortV2MxP1FD5vy+pVSsHfeR7:xBMM+0o5ueQSbpbFVrI+pVSsCVr2A
MD5:	3FA0AD47328B4B138D514364BFB1E816
SHA1:	46B10145C04996733F2425703C22CB16538DB25A
SHA-256:	E17421023957447D8427BE001CC0BB9B474825465F45782F9EAB2C277B8CB277
SHA-512:	5BBC5B2B081399121D0A79C24A0087999DB047FCC987AF9D49FB10362180CEC4100CBC5B789C1D1153D47D4B6C59EB1AACE8144C5CD53EF2935419084251EF0
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=SD-T225.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=12/23/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..SD-T225.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..SD-T225.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC912F....[ViewSonic] ..%SD-T225%=SD-T225.Install,Monitor\VSC912F ....[ViewSonic.NTx86] ..%SD-T225%=SD-T225.Install,Monitor\VSC912F....[ViewSonic.NTAMD64] ..%SD-T225%=SD-T225.Install,Monitor\VSC91

C:\ViewSonic\SD-Z225.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1718
Entropy (8bit):	5.490121203920855
Encrypted:	false
SSDEEP:	24:tXQtyMMLkb8rGx0Ro51LkD0H0LsLmIxmzdt4Omz/BmzD5orOMV2PRxP1nD5vy+pW:myMMCYo5uE0QwAPSrMV6e+pVZsIV1lj
MD5:	174ECA9D76FD57593B14E8472FA82B80
SHA1:	926A3B521DEF46490DCAF3EBA04390AF1BFC7000

SHA-256:	2AA53D80053FEF5046A62ABEBD3FF9FF5678035E203E5A888D4A8604D5DCBCB2
SHA-512:	320EF2622F8CA92DDB83D6CD8A18A2AFD9273EC17CA0EA321D0832E9C85395E4193F2B2B08474FF04F55A10714726C235CB1348822E3DD697E9815EE5BDAFC E
Malicious:	false
Preview:	;Monitor.Inf for Windows 7/ Windows 8..;Copyright 2013, ViewSonic Corporation....[Version] ..signature="$CHICAGO$"..Class=Monitor..ClassGuid={4D36E96E-E325-11 CE-BFC1-08002BE10318}..Provider=%ViewSonic%..CatalogFile=SD-Z225.cat..DriverVer=02/01/2013, 1.5.1.0....[DestinationDirs]..DefaultDestDir= 11..SD-Z225. CopyFiles=23....[SourceDisksNames]..1=%DiskName%,,....[SourceDisksFiles]..SD-Z225.ICM=1.....[Monitor_Service.Install]..DisplayName = %Monitor.SVCD ESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERV ICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys.....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC5D2D.....[Manufacturer]..%ViewSonic%=ViewSon ic,NTia64,NTamd64....[ViewSonic] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D ....[ViewSonic.NTia64] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D .... [ViewSonic.NTamd64] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D ....[SD-Z2

C:\ViewSonic\SD-Z225.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1718
Entropy (8bit):	5.490121203920855
Encrypted:	false
SSDEEP:	24:tXQtyMMLkb8rGx0Ro51LkD0H0LsLmIxmzdt4Omz/BmzD5orOMV2PRxP1nD5vy+pW:myMMCYo5uE0QwAPSrMV6e+pVZslV1lj
MD5:	174ECA9D76FD57593B14E8472FA82B80
SHA1:	926A3B521DEF46490DCAF3EBA04390AF1BFC7000
SHA-256:	2AA53D80053FEF5046A62ABEBD3FF9FF5678035E203E5A888D4A8604D5DCBCB2
SHA-512:	320EF2622F8CA92DDB83D6CD8A18A2AFD9273EC17CA0EA321D0832E9C85395E4193F2B2B08474FF04F55A10714726C235CB1348822E3DD697E9815EE5BDAFC E
Malicious:	false
Preview:	;Monitor.Inf for Windows 7/ Windows 8..;Copyright 2013, ViewSonic Corporation....[Version] ..signature="$CHICAGO$"..Class=Monitor..ClassGuid={4D36E96E-E325-11 CE-BFC1-08002BE10318}..Provider=%ViewSonic%..CatalogFile=SD-Z225.cat..DriverVer=02/01/2013, 1.5.1.0....[DestinationDirs]..DefaultDestDir= 11..SD-Z225. CopyFiles=23....[SourceDisksNames]..1=%DiskName%,,....[SourceDisksFiles]..SD-Z225.ICM=1.....[Monitor_Service.Install]..DisplayName = %Monitor.SVCD ESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERV ICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys.....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC5D2D.....[Manufacturer]..%ViewSonic%=ViewSon ic,NTia64,NTamd64....[ViewSonic] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D ....[ViewSonic.NTia64] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D .... [ViewSonic.NTamd64] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D ....[SD-Z2

C:\ViewSonic\SD-Z246.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1828
Entropy (8bit):	5.576377001595759
Encrypted:	false
SSDEEP:	48:KUyMMQ8o5ueQuhIxO32xISc7P+pVLGfVkxWD:K3MMMJJIxO32xuTK9GfWxWD
MD5:	B4FBE86F1018E8B2C0BA3756DCA6759A
SHA1:	FB0F0BA148E09AD07E2BFC148BBBB6F7C144208E
SHA-256:	1CA6A9536376F92736BA01BC3B670EBE93002BB5140472D30C4B5D2CD485F83E
SHA-512:	F80D02BEFBB5996BEB698B26AF97EEB807E7C662622E0496F5E35156B97EC80DD64274E5A4F386A6B5CE09CCD6754D572DCB810AFA1D746D1A25F4AF8CFE9 88
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 95/98/Me/2000/XP/Server 2003/XP x64/Vista/Vista x64/Windows 7/Windows 7 x64/Windows 8/Windows 8 x64....;Copyright 2014, ViewSonic Corporation....[Version] ..signature="$CHICAGO$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..CatalogFile=S D-Z246.cat..DriverVer=06/30/2014, 1.5.1.0....[DestinationDirs]..DefaultDestDir= 11..SD-Z246.CopyFiles=23....[SourceDisksNames]..1=%DiskLabel%,,....[SourceDisksF iles]..SD-Z246.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSon ic%=ViewSonic,NTia64,NTamd64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC7C30....[ViewSonic] ..%SD-Z246%=SD-Z246.Install,Monitor\VSC7C30 .... [ViewSonic.NTia64] ..%SD-Z246%=SD-Z246.Install,Monitor\VS

C:\ViewSonic\SD-Z246.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1828
Entropy (8bit):	5.576377001595759
Encrypted:	false
SSDEEP:	48:KUyMMQ8o5ueQuhIxO32xISc7P+pVLGfVkxWD:K3MMMJJIxO32xuTK9GfWxWD
MD5:	B4FBE86F1018E8B2C0BA3756DCA6759A

SHA1:	FB0F0BA148E09AD07E2BFC148BBBB6F7C144208E
SHA-256:	1CA6A9536376F92736BA01BC3B670EBE93002BB5140472D30C4B5D2CD485F83E
SHA-512:	F80D02BEFBB5996BEB698B26AF97EEB807E7C662622E0496F5E35156B97EC80DD64274E5A4F386A6B5CE09CCD6754D572DCB810AFA1D746D1A25F4AF8CFE9088
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 95/98/Me/2000/XP/Server 2003/XP x64/Vista/Vista x64/Windows 7/Windows 7 x64/Windows 8/Windows 8 x64....;Copyright 2014, ViewSonic Corporation....[Version] ..signature="$CHICAGO$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..CatalogFile=SD-Z246.cat..DriverVer=06/30/2014, 1.5.1.0....[DestinationDirs]..DefaultDestDir= 11..SD-Z246.CopyFiles=23....[SourceDisksNames]..1=%DiskLabel%,,....[SourceDisksFiles]..SD-Z246.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTia64,NTamd64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC7C30....[ViewSonic] ..%SD-Z246%=SD-Z246.Install,Monitor\VSC7C30 ....[ViewSonic.NTia64] ..%SD-Z246%=SD-Z246.Install,Monitor\VS

C:\ViewSonic\SD-Zd3cf.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1718
Entropy (8bit):	5.490121203920855
Encrypted:	false
SSDEEP:	24:tXQtyMMLkb8rGx0Ro51LkD0H0LsLmIxmzdt4Omz/BmzD5orOMV2PRxP1nD5vy+pW:myMMCYo5uE0QwAPSrMV6e+pVZslV1lj
MD5:	174ECA9D76FD57593B14E8472FA82B80
SHA1:	926A3B521DEF46490DCAF3EBA04390AF1BFC7000
SHA-256:	2AA53D80053FEF5046A62ABEBD3FF9FF5678035E203E5A888D4A8604D5DCBCB2
SHA-512:	320EF2622F8CA92DDB83D6CD8A18A2AFD9273EC17CA0EA321D0832E9C85395E4193F2B2B08474FF04F55A10714726C235CB1348822E3DD697E9815EE5BDAFCE
Malicious:	false
Preview:	;Monitor.Inf for Windows 7/ Windows 8..;Copyright 2013, ViewSonic Corporation....[Version] ..signature="$CHICAGO$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..CatalogFile=SD-Z225.cat..DriverVer=02/01/2013, 1.5.1.0....[DestinationDirs]..DefaultDestDir= 11..SD-Z225.CopyFiles=23....[SourceDisksNames]..1=%DiskName%,,....[SourceDisksFiles]..SD-Z225.ICM=1.....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys.....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC5D2D.....[Manufacturer]..%ViewSonic%=ViewSonic,NTia64,NTamd64....[ViewSonic] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D ....[ViewSonic.NTia64] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D ....[ViewSonic.NTamd64] ..%SD-Z225%=SD-Z225.Install,Monitor\VSC5D2D ....[SD-Z2

C:\ViewSonic\SD-Ze3cd.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1828
Entropy (8bit):	5.576377001595759
Encrypted:	false
SSDEEP:	48:KUyMMQ8o5ueQuhIxO32xISc7P+pVLGfVkxWD:K3MMMJJIxO32xuTK9GfWxWD
MD5:	B4FBE86F1018E8B2C0BA3756DCA6759A
SHA1:	FB0F0BA148E09AD07E2BFC148BBBB6F7C144208E
SHA-256:	1CA6A9536376F92736BA01BC3B670EBE93002BB5140472D30C4B5D2CD485F83E
SHA-512:	F80D02BEFBB5996BEB698B26AF97EEB807E7C662622E0496F5E35156B97EC80DD64274E5A4F386A6B5CE09CCD6754D572DCB810AFA1D746D1A25F4AF8CFE9088
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 95/98/Me/2000/XP/Server 2003/XP x64/Vista/Vista x64/Windows 7/Windows 7 x64/Windows 8/Windows 8 x64....;Copyright 2014, ViewSonic Corporation....[Version] ..signature="$CHICAGO$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..CatalogFile=SD-Z246.cat..DriverVer=06/30/2014, 1.5.1.0....[DestinationDirs]..DefaultDestDir= 11..SD-Z246.CopyFiles=23....[SourceDisksNames]..1=%DiskLabel%,,....[SourceDisksFiles]..SD-Z246.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTia64,NTamd64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC7C30....[ViewSonic] ..%SD-Z246%=SD-Z246.Install,Monitor\VSC7C30 ....[ViewSonic.NTia64] ..%SD-Z246%=SD-Z246.Install,Monitor\VS

C:\ViewSonic\TD161ba6.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1679
Entropy (8bit):	5.536085399866959
Encrypted:	false
SSDEEP:	24:tIxQFJo8MMLM8rP+0Ro51LkeLsLiHoz7orFVceP1nD5vy+pVp2sreRVk/AOKahfL:tBMM4go5ueQy/V7e+pV4sWVkCFxm

MD5:	E3B19BF076EC259177AA62851F30A1AD
SHA1:	AF90E1784C05568628D2B953F1535927D69AE1C5
SHA-256:	CF1241AE2299F3C02B5616FEBB91C0C0D222FDD95EBBED6A2195182F8053EE00
SHA-512:	9036A2781497FCCFBBE97B87A0F82B0715AE4AEFE9D557D481B3E8EF85883CE6346D4068FF0BB5213BA016EEC693FBBA04C560BE591B2508BD711131D072748A
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86/x64, 8 x86/x64, 10 x86/x64..;Copyright 2019, ViewSonic Corporation....[Version] ..CatalogFile=TD1655.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=12/09/2019, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..TD1655.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..TD1655.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTamd64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSCD039....[ViewSonic.NTx86] ..%TD1655%=TD1655.Install,Monitor\VSCD039....[ViewSonic.NTamd64] ..%TD1655%=TD1655.Install,Monitor\VSCD039....[TD1655.Install] ..DelReg=DEL_CURRENT_REG ..AddReg=TD1655

C:\ViewSonic\TD16fee.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	2483
Entropy (8bit):	5.585153273475261
Encrypted:	false
SSDEEP:	48:pBMMuKo5ueQSRoOmqYWee+pVlVQAVYKm1k:pBMMmJouDKfDaKm1k
MD5:	D84CE886801EAFD4290A49301704B194
SHA1:	99BCB57B270E550ECBD4E7D1F8350A5382F01586
SHA-256:	11AA58DDFE653D8DD786A0D256621F8CA683CFAB42A232BB4FEAF2CFEF3793E6
SHA-512:	0EAEF7A65081BE12942908926E7ED9B8AE37219691E5C844E3BAEB588345A4E27BED306C2DB912EFC8D08D3FCFAB7B87A3C1CF6B3879E4DC96A656EE466C9675
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86/x64, 8 x86/x64, 10 x86/x64..;Copyright 2018, ViewSonic Corporation....[Version] ..CatalogFile=TD1630-3.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=08/03/2018, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..TD1630-3.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..TD1630-3.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSCC234....[ViewSonic] ..%TD1630-3_HDMI_14%=TD1630-3_HDMI_14.Install,Monitor\VSCC234 ..%TD1630-3_VGA%=TD1630-3_VGA.Install,Monitor\VSCC234....[ViewSonic.NTx86] ..%TD1630-3_HDMI_14%=TD1630-3_H

C:\ViewSonic\TD17b4b.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Microsoft color profile 2.3, type lcms, RGB/XYZ-mntr device by lcms, 824 bytes, 6-3-2018 10:59:55, 0x4ab64bc31deabf53 MD5 "TD1711 sRGB 6500K"
Category:	dropped
Size (bytes):	824
Entropy (8bit):	3.3320865472467602
Encrypted:	false
SSDEEP:	12:Hh1zOEICfNVDVFLsrGhaTlYslUZlNSD3innlnAhRtRtJdD6JU:B1z5IGjvLHhaTlYslUZlFeXR6
MD5:	A13005FE622320C0D5FBBD8268F1ECD5
SHA1:	30CE15FEF353247FEA62C2860138BA7A005A0B79
SHA-256:	88E81B96D884174FBF8188F823A6A4432204703F584D777CA6C11EA5142A0ABD
SHA-512:	9507FEC49216F2F29A36A650C8C5A7C89E6DB2922063E1C337DE9CA9F5BC307F6A27D1F9841D738281E6E069CE5EAF1C9726AEB551EBDFFD9A2C92746BF1D55
Malicious:	false
Preview:	...8lcms.0..mntrRGB XYZ .....;.7acspMSFT....lcms.....-lcmsJ.K...S....|.H.....dmnd... ...pdesc.....ldmdd.....awtpt...`....rXYZ...t....bXYZ.....gXYZ.....rTRC.....gTRC.....bTRC.....chrm.....$cprt.....bkpt...$....desc.....ViewSonic Corporation.....desc.....TD1711 sRGB 6500K.....desc.....TD1711.....XYZ .....>.....XYZ .....t...<...;XYZ .....%k.....XYZ .....]L.....3curv.....3..curv.....3..curv.....3..chrm.....y..T{..M....)..&f...\text....ViewSonic Corporation...XYZ .....

C:\ViewSonic\TD17b79.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1808
Entropy (8bit):	5.4989161417630354
Encrypted:	false
SSDEEP:	48:3NoMU7oIhqSQUsXNE4LPEosVfVszioWFAo5uKn:3NoMW+VXNE4L7sxeziJ9
MD5:	B3BBE8EB035C04B136DE6BEE3499075B

SHA1:	FF91CDCF2D05B4AFFE0BA7C407F2A40CA5A103DB
SHA-256:	6E1AC876885B9DCB267625115BA0B6E6715D70067D9B9628E02268071AE10910
SHA-512:	FA9D7232A622EAB599A3C26E72E38578BAB40804C5DD23D2BC685F8322A9BBF2DA196E6EDDE74E5BDF72BBFF6687C365BEDA6E3BAC2694C1C356924BCA1E9DAC
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 95/98/Me/2000/XP/Server 2003/XP x64/Vista/Vista x64/Windows 7/Windows 7 x64....;Copyright 2018, ViewSonic Corporation....[Version].. Signature = "$Windows NT$"..Class = Monitor..ClassGuid = {4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider = %ViewSonic%..CatalogFile = TD1711.cat..DriverVer = 03/06/2018, 1.0.0.0....[SourceDisksNames]..1 = %DiskName%....[SourceDisksFiles]..TD1711.icm = 1....[DestinationDirs]..DefaultDestDir = 12..TD1711.Copyfiles = 23....[ControlFlags]..ExcludeFromSelect = Monitor\VSCD336....[Manufacturer]..%ViewSonic% = ViewSonic, NTx86, NTAMD64....[ViewSonic-Mfg]..%TD1711% = TD1711.Install, Monitor\VSCD336....[ViewSonic.NTx86]..%TD1711% = TD1711.Install, Monitor\VSCD336....[ViewSonic.NTAMD64]..%TD1711% = TD1711.Install, Monitor\VSCD336....[TD1711.Install]..DelReg = DEL_CURRENT_REG..AddReg = TD1711.AddReg, 1280x1024, DPMS..CopyFiles = TD1711.CopyFiles....[DEL_CURRENT_REG]..HKR,MODES..HKR,,MaxResolution..HKR,,DPMS..HKR,

C:\ViewSonic\TD2210_Series.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Microsoft color profile 2.0, type appl, RGB/XYZ-mntr device, 512 bytes, 18-5-2016 16:24:29, PCS Z=0xd32c "TD2210 Series"
Category:	dropped
Size (bytes):	512
Entropy (8bit):	3.8039598314087915
Encrypted:	false
SSDEEP:	12:uTO/7I/Cle/UD7sVWCD9Alp14Rtaey9wRtRtyWTomOa:uTe7INUDYVJAI+XnTopa
MD5:	9DDB68E1C2E0984F97F3AB5B66FCAF93
SHA1:	C1E864C13D9D871F1B22F981AA908D918BB07D9F
SHA-256:	EBF1E60C36A7ABE865B37FE705FB6A9E0994C78DCB69CF8DC6CB297C657F9771
SHA-512:	C5BBE6CFC82AF82FE293CF15BCD3C6606BBDC21501FDCC43FAFB02B4A7316149EF45E11C1C8DB860308FFA6C743DA946FBA8DEBEC7ED9A13282EC4A36A9EF501
Malicious:	false
Preview:	....appl....mntrRGB XYZ .....acspMSFT....NONE.....desc.....0rXYZ...,....gXYZ...@....bXYZ...T....rTRC...h....gTRC...x....bTRC.....wtpt.....cprt.....@calt.....desc.....TD2210 Series.....XYZ .....ia..8+...qXYZ .....g.....XYZ .....%.....curv.....3..curv.....3..curv.....3..XYZ .....text....Copyright . 2016 ViewSonic Corporation.....x.....dtim.....

C:\ViewSonic\TD2210_Series.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1896
Entropy (8bit):	5.477648716332173
Encrypted:	false
SSDEEP:	48:nWBMMVe/o5ueQSUTtZzGVVe+pV0qCVOqD:WBMMRJXWKXCrD
MD5:	0D96890756EB6E237987D99FEC919DD2
SHA1:	F8A16BB26273BC973B66527F9FD415BB33A0127C
SHA-256:	8AD291610D4BF191AEAC885744C930350AA2F1BD4319A542389C3D1888567B61
SHA-512:	582FFC755F9B396347B3B5296011111F5FF20924B2AA6A06648EF8DE715BEF3128021A87B2B2FC2A0441EF0F151A07564AF67D90C6B9B5ABC4404E5CD2C598D2
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64, 10 x86, 10 x64....;Copyright 2016, ViewSonic Corporation....[Version] ..CatalogFile=TD2210_SERIES.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=05/18/2016, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..TD2210_SERIES.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..TD2210_SERIES.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC0833....[ViewSonic] ..%TD2210_SERIES%=TD2210_SERIES.Install,Monitor\VSC0833 ....[ViewSonic.NTx86] ..%TD2210_SERIES%=TD2210_SERIES.Install,Monitor\VSC0833....[Vie

C:\ViewSonic\TD222182.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1679
Entropy (8bit):	5.524664898257959
Encrypted:	false
SSDEEP:	48:LBMMceGzko5ueQyiCkDWkre+pVTEIVjldFXqN:LBMM+JoVKKpEIhjF2
MD5:	BB6B071369CC97E746FE5821F64A445C
SHA1:	DDC0160A6F4EB55FA7ACDAA611BDC2D11AF61046
SHA-256:	523559EFF0F8CAB7C9D5333FFC624F871C329D888C2A4887D085E920B70EBCDE

SHA-512:	9D85C7EA092131E0111FFD64FEBD6F6398A70CE86AE9DE15512A87671BAFEDD07DD1B9A97747ADFEC5670E42DACD2B163A238C3970B07A09561FE2788B76A5AA
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86/x64, 8 x86/x64, 10 x86/x64..;Copyright 2020, ViewSonic Corporation....[Version] ..CatalogFile=TD2223.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=04/15/2020, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..TD2223.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..TD2223.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTamd64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSC5D3A....[ViewSonic.NTx86] ..%TD2223%=TD2223.Install,Monitor\VSC5D3A....[ViewSonic.NTamd64] ..%TD2223%=TD2223.Install,Monitor\VSC5D3A....[TD2223.Install] ..DelReg=DEL_CURRENT_REG ..AddReg=TD2223

C:\ViewSonic\TD2230_Series.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1423
Entropy (8bit):	5.542907222520867
Encrypted:	false
SSDEEP:	24:tXPeQtyMMLP5u8r+lh25lLsL+HNiWOUt4/OUmOpMor+JZccp55vy+pVw4JfV52VJ:xyMMrcXqfQuZOV/O5OpmJZcEK+pVLd58
MD5:	4A95CD16C1FA4ACA186BDEB63A06933A
SHA1:	72C0A6C27E419FEA021D5D96B4AEAAC38CE1A487
SHA-256:	85F4217EE8C94A0583E385D4545CBFE9D0619CE5499FD89EA9021D9044BEAA06
SHA-512:	696072E1DD4EF3F5D872E916990741B9AE5C3D355CF2D9BAE64E3A2DBD082863939EC80270644A769BFD857E43158C6656C25F90B411194D2DCCA236AE4ED67B
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 95/98/Me/2000/XP/Server 2003/XP x64/Vista/Vista x64/Windows 7/Windows 7 x64....;Copyright 2016, ViewSonic Corporation....[Version] ..signature="$CHICAGO$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..CatalogFile=TD2230_Series.cat..DriverVer=01/07/2016, 1.5.1.0....[DestinationDirs]..DefaultDestDir= 11..TD2230_Series.CopyFiles=23....[SourceDisksNames]..1=%DiskLabel%,,....[SourceDisksFiles]..TD2230_Series.ICM=1....[Manufacturer]..%ViewSonic%=ViewSonic,NTia64,NTamd64....[ControlFlags]..ExcludeFromSelect.nt=*....[ViewSonic] ..%TD2230_Series%=TD2230_Series.Install,Monitor\VSC9A32 ....[ViewSonic.NTia64] ..%TD2230_Series%=TD2230_Series.Install,Monitor\VSC9A32 ....[ViewSonic.NTamd64] ..%TD2230_Series%=TD2230_Series.Install,Monitor\VSC9A32 ....[TD2230_Series.Install] ..DelReg=DEL_CURRENT_REG ..AddReg=TD2230_Series.AddReg,1920,DPMS..Copyfiles=TD2230_Series.CopyFiles....[DEL_CURRENT_REG]..HKR,MODES..HKR,,MaxResolut

C:\ViewSonic\TD2230_Series.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1423
Entropy (8bit):	5.542907222520867
Encrypted:	false
SSDEEP:	24:tXPeQtyMMLP5u8r+lh25lLsL+HNiWOUt4/OUmOpMor+JZccp55vy+pVw4JfV52VJ:xyMMrcXqfQuZOV/O5OpmJZcEK+pVLd58
MD5:	4A95CD16C1FA4ACA186BDEB63A06933A
SHA1:	72C0A6C27E419FEA021D5D96B4AEAAC38CE1A487
SHA-256:	85F4217EE8C94A0583E385D4545CBFE9D0619CE5499FD89EA9021D9044BEAA06
SHA-512:	696072E1DD4EF3F5D872E916990741B9AE5C3D355CF2D9BAE64E3A2DBD082863939EC80270644A769BFD857E43158C6656C25F90B411194D2DCCA236AE4ED67B
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 95/98/Me/2000/XP/Server 2003/XP x64/Vista/Vista x64/Windows 7/Windows 7 x64....;Copyright 2016, ViewSonic Corporation....[Version] ..signature="$CHICAGO$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..CatalogFile=TD2230_Series.cat..DriverVer=01/07/2016, 1.5.1.0....[DestinationDirs]..DefaultDestDir= 11..TD2230_Series.CopyFiles=23....[SourceDisksNames]..1=%DiskLabel%,,....[SourceDisksFiles]..TD2230_Series.ICM=1....[Manufacturer]..%ViewSonic%=ViewSonic,NTia64,NTamd64....[ControlFlags]..ExcludeFromSelect.nt=*....[ViewSonic] ..%TD2230_Series%=TD2230_Series.Install,Monitor\VSC9A32 ....[ViewSonic.NTia64] ..%TD2230_Series%=TD2230_Series.Install,Monitor\VSC9A32 ....[ViewSonic.NTamd64] ..%TD2230_Series%=TD2230_Series.Install,Monitor\VSC9A32 ....[TD2230_Series.Install] ..DelReg=DEL_CURRENT_REG ..AddReg=TD2230_Series.AddReg,1920,DPMS..Copyfiles=TD2230_Series.CopyFiles....[DEL_CURRENT_REG]..HKR,MODES..HKR,,MaxResolut

C:\ViewSonic\TD2240_Series.icm (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1880
Entropy (8bit):	5.45095066108995
Encrypted:	false
SSDEEP:	24:t6QCJo8MML38rJh+0Ro51LkeLsLCH3dUoN5or+nc6P1FD5vy+pVpwreRVhrNVKa/:mBMM7eno5ueQSNnjI+pVGWVA2
MD5:	1E9276ABE23243B1CA923DA1B481D558
SHA1:	CF785FBE2116118719E01BC0353B6E94FEBA300D

SHA-256:	799D62654B0C3C90447FBA0BFABE9D914E6628CD0A96520AAF5365A8604E614F
SHA-512:	7FAD6199F23F5C216E93627421C5E6F519A953547B2322B95E89400D8A65747D6436103C87B0EE7C7304905FA413FC3D8E44BBF173338834867308712AC41DDC1
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=TD2240_Series.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=05/28/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..TD2240_Series.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..TD2240_Series.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSCD82E....[ViewSonic] ..%TD2240_Series%=TD2240_Series.Install,Monitor\VSCD82E ....[ViewSonic.NTx86] ..%TD2240_Series%=TD2240_Series.Install,Monitor\VSCD82E....[ViewSonic.NTAMD64]

C:\ViewSonic\TD2240_Series.inf (copy)

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1880
Entropy (8bit):	5.45095066108995
Encrypted:	false
SSDEEP:	24:t6QCJo8MML38rJh+0Ro51LkeLsLCH3dUoN5or+nc6P1FD5vy+pVpwreRVhrNVKa/:mBMM7eno5ueQSNnjI+pVGWVA2
MD5:	1E9276ABE23243B1CA923DA1B481D558
SHA1:	CF785FBE2116118719E01BC0353B6E94FEBA300D
SHA-256:	799D62654B0C3C90447FBA0BFABE9D914E6628CD0A96520AAF5365A8604E614F
SHA-512:	7FAD6199F23F5C216E93627421C5E6F519A953547B2322B95E89400D8A65747D6436103C87B0EE7C7304905FA413FC3D8E44BBF173338834867308712AC41DDC1
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=TD2240_Series.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=05/28/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..TD2240_Series.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..TD2240_Series.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSCD82E....[ViewSonic] ..%TD2240_Series%=TD2240_Series.Install,Monitor\VSCD82E ....[ViewSonic.NTx86] ..%TD2240_Series%=TD2240_Series.Install,Monitor\VSCD82E....[ViewSonic.NTAMD64]

C:\ViewSonic\TD22dd93.rra

Process:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	1880
Entropy (8bit):	5.45095066108995
Encrypted:	false
SSDEEP:	24:t6QCJo8MML38rJh+0Ro51LkeLsLCH3dUoN5or+nc6P1FD5vy+pVpwreRVhrNVKa/:mBMM7eno5ueQSNnjI+pVGWVA2
MD5:	1E9276ABE23243B1CA923DA1B481D558
SHA1:	CF785FBE2116118719E01BC0353B6E94FEBA300D
SHA-256:	799D62654B0C3C90447FBA0BFABE9D914E6628CD0A96520AAF5365A8604E614F
SHA-512:	7FAD6199F23F5C216E93627421C5E6F519A953547B2322B95E89400D8A65747D6436103C87B0EE7C7304905FA413FC3D8E44BBF173338834867308712AC41DDC1
Malicious:	false
Preview:	;Monitor.Inf for Windows(R) 7 x86, 7 x64, 8 x86, 8 x64....;Copyright 2013, ViewSonic Corporation....[Version] ..CatalogFile=TD2240_Series.cat ..signature="$Windows NT$"..Class=Monitor..ClassGuid={4D36E96E-E325-11CE-BFC1-08002BE10318}..Provider=%ViewSonic%..DriverVer=05/28/2013, 1.5.0.0....[DestinationDirs]..DefaultDestDir= 12..TD2240_Series.CopyFiles=23....[SourceDisksNames]..1=%diskname%,,....[SourceDisksFiles]..TD2240_Series.ICM=1....[Monitor_Service.Install]..DisplayName = %Monitor.SVCDESC%..ServiceType = 1 ; SERVICE_KERNEL_DRIVER..StartType = 3 ; SERVICE_DEMAND_START..ErrorControl = 1 ; SERVICE_ERROR_NORMAL..ServiceBinary = %12%\monitor.sys....[Manufacturer]..%ViewSonic%=ViewSonic,NTx86,NTAMD64....[ControlFlags]..ExcludeFromSelect.nt=Monitor\VSCD82E....[ViewSonic] ..%TD2240_Series%=TD2240_Series.Install,Monitor\VSCD82E ....[ViewSonic.NTx86] ..%TD2240_Series%=TD2240_Series.Install,Monitor\VSCD82E....[ViewSonic.NTAMD64]

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, InstallShield self-extracting archive
Entropy (8bit):	7.988529444078634
TrID:	• Win32 Executable (generic) a (10002005/4) 99.53% • InstallShield setup (43055/19) 0.43% • 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:	Standard_Monitor_Driver_Signed_Win10_x64.exe

File size:	3593536
MD5:	cf77f6850ff98d1b681832160f2691fe
SHA1:	ccba9f71b67bd9582804b6a3c27fbcf89431e7be
SHA256:	d81e3afb0a8a83be2f99c5709d2b107171dc86b33405729fbef539bba4449de1
SHA512:	9ea5d40195bbd26b128865a79657e438efb7f6f0fd252a44c6c4db042df329d3e29f7702e9b788bcd7ac674e0193c8617a7a95328b0036537d8d75d2d2525c58
SSDEEP:	49152:Ha8tthGt1LHQzcLx7o11qxT48S7du1Owbn0XdGtayRVIKYbCRAQlGEtmpd8OzlJG:HxIt1BW11J8S7e0XdGgyXtH/Ivmr90g0
TLSH:	AFF523C690AA859FD6B052B03194E06791C68F4307979AFBFB0A3C54637EDF584CD2A3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...w...w...w...w...h...w..sk...w...h...w...T...w...w..Iw...W...w..7q...w..Rich.w.....PE..L....Z.;...

File Icon

Icon Hash:	89adaca1e18e0183

Static PE Info

General

Entrypoint:	0x408947
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x3B965AC1 [Wed Sep 5 17:02:57 2001 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:	5a9b89741dd0eb9be8754b41c4d30c55

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 11/6/2022 4:00:00 PM 12/8/2023 3:59:59 PM
Subject Chain	• CN=ViewSonic Corporation, O=ViewSonic Corporation, L=Brea, S=California, C=US, SERIALNUMBER=2901060, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US
Version:	3
Thumbprint MD5:	314F00D9B9CC9FD11449BEFF959410B0
Thumbprint SHA-1:	9CD028804B50B7544B252440DBD51EB0590D74F9
Thumbprint SHA-256:	10F4B784D17B2650606D9638292019B3FED3B3DF0F2447B892E561D865625504
Serial:	0ECA051B4309228B4688033D3FE5E37B

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 00413318h
push 0040BA80h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp

Instruction
sub esp, 58h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
call dword ptr [004131E8h]
xor edx, edx
mov dl, ah
mov dword ptr [0041635Ch], edx
mov ecx, eax
and ecx, 000000FFh
mov dword ptr [00416358h], ecx
shl ecx, 08h
add ecx, edx
mov dword ptr [00416354h], ecx
shr eax, 10h
mov dword ptr [00416350h], eax
xor esi, esi
push esi
call 00007F06B0733B15h
pop ecx
test eax, eax
jne 00007F06B0733A3Ah
push 0000001Ch
call 00007F06B0733AE5h
pop ecx
mov dword ptr [ebp-04h], esi
call 00007F06B0736946h
call dword ptr [004131ECh]
mov dword ptr [00418A24h], eax
call 00007F06B0736804h
mov dword ptr [00416328h], eax
call 00007F06B07365ADh
call 00007F06B07364EFh
call 00007F06B073495Eh
mov dword ptr [ebp-30h], esi
lea eax, dword ptr [ebp-5Ch]
push eax
call dword ptr [004130B8h]
call 00007F06B0736480h
mov dword ptr [ebp-64h], eax
test byte ptr [ebp-30h], 00000001h
je 00007F06B0733A38h
movzx eax, word ptr [ebp-2Ch]
jmp 00007F06B0733A35h
push 0000000Ah
pop eax
push eax
push dword ptr [ebp-64h]
push esi
push esi
call dword ptr [004130E0h]

Rich Headers	
Programming Language:	• [C++] VS98 (6.0) build 8168 • [C] VS98 (6.0) build 8168 • [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13938	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a000	0x2caa8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x36aca0	0x28a0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x13000	0x2fc	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x11b16	0x12000	False	0.600830078125	data	6.60209928895754	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x13000	0x1950	0x2000	False	0.3582763671875	data	4.782525832448763	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x15000	0x4e38	0x2000	False	0.2440185546875	data	2.421916530044494	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x1a000	0x2caa8	0x2d000	False	0.19073350694444444	data	7.0229976344770915	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x1bff8	0x25ba2	Device independent bitmap graphic, 164 x 314 x 24, image size 0, resolution 2834 x 2834 px/m	English	United States
RT_BITMAP	0x41ba0	0x38e4	Device independent bitmap graphic, 180 x 75 x 8, image size 13500, resolution 2834 x 2834 px/m, 256 important colors	English	United States
RT_ICON	0x1ad98	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	United States
RT_ICON	0x1aec0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 320	English	United States
RT_ICON	0x1b428	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_ICON	0x1b710	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1152	English	United States
RT_DIALOG	0x45488	0x19a	data	English	United States
RT_DIALOG	0x1a8d0	0x92	data	English	United States
RT_DIALOG	0x1a968	0xbe	data	English	United States
RT_DIALOG	0x1acc0	0xd6	data	English	United States
RT_DIALOG	0x1aa28	0xae	data	English	United States
RT_DIALOG	0x1a658	0x272	data	English	United States
RT_DIALOG	0x1a570	0xe2	data	English	United States
RT_DIALOG	0x1ac30	0x90	data	English	United States
RT_DIALOG	0x1aad8	0xf0	data	English	United States
RT_DIALOG	0x1abc8	0x62	data	English	United States
RT_STRING	0x45c90	0x632	data	English	United States
RT_STRING	0x462c8	0x1a8	data	English	United States
RT_STRING	0x46898	0x11a	data	English	United States
RT_STRING	0x46470	0xba	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x46530	0x366	data	English	United States
RT_STRING	0x469b8	0x98	data	English	United States
RT_STRING	0x46a50	0x58	data	English	United States
RT_GROUP_ICON	0x1bfb8	0x3e	data	English	United States
RT_VERSION	0x45628	0x668	data	English	United States

Imports

DLL	Import
KERNEL32.dll	GetProcAddress, FormatMessageA, DeleteFileA, MulDiv, IsDBCSLeadByte, GetExitCodeProcess, CreateProcessA, GetTempFileNameA, GetSystemDefaultLCID, WaitForSingleObject, CompareStringA, Sleep, SetFileTime, LocalFileTimeToFileTime, DosDateTimeToFileTime, FreeLibrary, RemoveDirectoryA, FindNextFileA, WritePrivateProfileSectionA, GetStartupInfoA, WriteFile, ReadFile, SetFileAttributesA, LocalFree, LocalAlloc, LockResource, LoadResource, FindResourceA, SizeofResource, GetModuleHandleA, GlobalFree, GlobalUnlock, GlobalLock, GlobalAlloc, MultiByteToWideChar, lstrcmpiA, GetDiskFreeSpaceA, HeapAlloc, GetProcessHeap, HeapFree, GetModuleFileNameA, ExitProcess, CreateFileA, CreateFileMappingA, MapViewOfFile, UnmapViewOfFile, lstrcpynA, SetFilePointer, GetFileSize, FindFirstFileA, CreateDirectoryA, GetLastError, GetPrivateProfileStringA, FindClose, GetFileAttributesA, lstrcatA, lstrlenA, GetWindowsDirectoryA, lstrcpyA, GetSystemDirectoryA, GetTempPathA, GetPrivateProfileSectionA, LoadLibraryA, MoveFileExA, WritePrivateProfileStringA, GetShortPathNameA, FlushFileBuffers, CloseHandle, IsBadCodePtr, IsBadReadPtr, SetStdHandle, LCMapStringW, LCMapStringA, SetUnhandledExceptionFilter, GetStdHandle, SetHandleCount, GetFileType, GetEnvironmentStrings, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsA, UnhandledExceptionFilter, FreeEnvironmentStringsW, TerminateProcess, GetStringTypeW, GetCurrentProcess, GetOEMCP, GetACP, GetStringTypeA, IsBadWritePtr, HeapReAlloc, GetCPInfo, VirtualFree, HeapCreate, VirtualAlloc, GetVersion, GetCommandLineA, HeapDestroy, RtlUnwind
USER32.dll	GetParent, GetDlgItem, SetFocus, SendDlgItemMessageA, EnableWindow, CheckRadioButton, GetWindowLongA, LoadStringA, LoadImageA, MessageBoxA, CharNextA, IsDlgButtonChecked, GetDlgItemTextA, CheckDlgButton, SetDlgItemTextA, ReleaseDC, GetDC, GetWindow, PostMessageA, SetWindowTextA, wsprintfA, GetDesktopWindow, GetWindowTextA, DestroyWindow, CreateDialogParamA, FillRect, GetSysColor, GetSysColorBrush, EndPaint, BeginPaint, DrawTextA, MoveWindow, GetClientRect, ScreenToClient, GetNextDlgTabItem, SetParent, MapDialogRect, IsWindow, GetWindowRect, CreateDialogIndirectParamA, ShowWindow, InvalidateRect, IsWindowEnabled, SetWindowPos, UpdateWindow, IsDialogMessageA, SetWindowLongA, GetActiveWindow, SetActiveWindow, LoadIconA, PeekMessageA, SendMessageA, DispatchMessageA, TranslateMessage
GDI32.dll	CreateFontIndirectA, RealizePalette, SelectPalette, CreatePalette, GetObjectA, GetStockObject, CreateDIBitmap, GetTextExtentPointA, SelectObject, EnumFontFamiliesExA, DeleteDC, BitBlt, TextOutA, SetBkMode, SetBkColor, CreateCompatibleDC, CreateSolidBrush, SetTextColor, DeleteObject, GetDeviceCaps
ADVAPI32.dll	RegCloseKey, RegQueryValueExA, RegOpenKeyExA
SHELL32.dll	ShellExecuteA, SHBrowseForFolderA, SHGetPathFromIDListA, SHGetMalloc
LZ32.dll	LZOpenFileA, LZCopy, LZClose
COMCTL32.dll	

Possible Origin

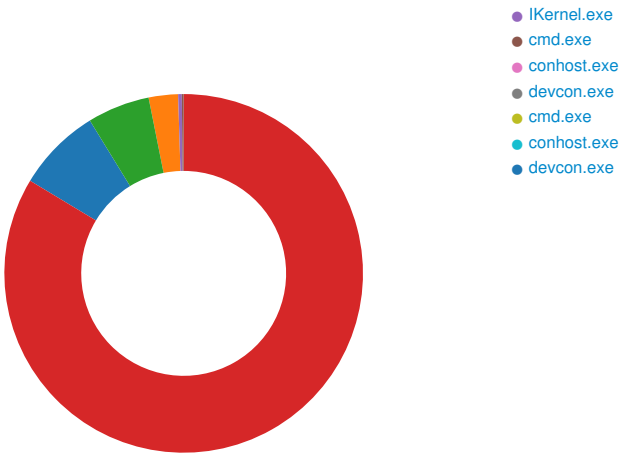
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: Standard_Monitor_Driver_Signed_Win10_x64.exe PID: 7148, Parent PID: 3452

General

Target ID:	0
Start time:	17:16:46
Start date:	06/06/2023
Path:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Standard_Monitor_Driver_Signed_Win10_x64.exe
Imagebase:	0x400000
File size:	3593536 bytes
MD5 hash:	CF77F6850FF98D1B681832160F2691FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: Setup.exe PID: 7132, Parent PID: 7148

General

Target ID:	1
Start time:	17:16:47
Start date:	06/06/2023
Path:	C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\pftB01D.tmp\Disk1\Setup.exe
Imagebase:	0x400000
File size:	56320 bytes
MD5 hash:	1AEB989E361AF85F5099DE3DA25457F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4067FD	CreateDirectoryA
C:\Program Files (x86)\Common Files\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4067FD	CreateDirectoryA
C:\Program Files (x86)\Common Files\InstallShield\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4067FD	CreateDirectoryA
C:\Program Files (x86)\Common Files\InstallShield\user\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4067FD	CreateDirectoryA
C:\Program Files (x86)\Common Files\InstallShield\user\6\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4067FD	CreateDirectoryA
C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4067FD	CreateDirectoryA
C:\Users\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4067FD	CreateDirectoryA
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	4067FD	CreateDirectoryA
C:\Users\user\AppData\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4067FD	CreateDirectoryA
C:\Users\user\AppData\Local\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4067FD	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4067FD	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\IECB57A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	404AFD	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\IECB57A.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	40418F	CopyFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IECB57A.tmp	success or wait	1	404B35	DeleteFileA
C:\Users\user\AppData\Local\Temp\IECB57A.tmp	success or wait	1	404F8E	DeleteFileA

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\IECB57A.tmp	0	131072	53 5a 44 44 fd fd 27 33 41 00 fd 60 09 00 fd 4d 5a fd 00 03 00 00 00 7d 04 fd fd fd fd 00 00 fd fd fd fd 01 01 40 01 04 0f 0d 1c 09 08 01 00 fd 00 0e 1f fd 0e 00 fd 09 fd fd 21 fd 01 4c fd 21 54 fd 68 69 73 20 70 72 6f 67 fd 72 61 6d 20 63 61 6e 6e fd 6f 74 20 62 65 20 72 75 fd 6e 20 69 6e 20 44 4f 53 fd 20 6d 6f 64 65 2e 0d 0d fd 0a 24 01 04 fd 31 22 5c fd fd 50 4c 0f 74 05 fd 4c 40 0f 7d fd 75 00 3f 4c 42 0f fd 75 00 fd 54 4f 46 0f fd 02 47 0f 7d fd 75 00 fd 4f 5f 0f fd 75 04 7b 75 02 4d 0f 6f 75 00 fd 73 fd 5f 0f fd 75 00 43 70 46 0f 74 fd 02 47 0f fd 75 00 7b 56 fd 4a 0f fd 75 00 52 69 63 68 fd 74 01 1c 0d fd 05 50 45 00 00 4c 7f 01 04 00 6c 68 40 3d fd 05 fd fd 00 2f 01 0b 01 06 00 fd 00 fd 12 10 fd fd 00 00 fd fd 2f 05 00 00 10 fd fd fd 16	SZDD'3A`MZ}@!L!This program cannot be run in DOS mode.$1"\PL tL@}u? LBuTOFG}uO_uuMous_u CpFGu {VJuRichtPELlh@=//	success or wait	3	40418F	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: IKernel.exe PID: **5220**, Parent PID: **7132**

General

Target ID:	2
Start time:	17:16:48
Start date:	06/06/2023
Path:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe" -RegServer
Imagebase:	0x400000
File size:	614532 bytes
MD5 hash:	B3FD01873BD5FD163AB465779271C58F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: IKernel.exe PID: **1852**, Parent PID: **800**

General

Target ID:	3
Start time:	17:16:49
Start date:	06/06/2023
Path:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
Wow64 process (32bit):	true
Commandline:	C:\PROGRA~2\COMMON~1\INSTAL~1\user\6\INTEL3~1\IKernel.exe -Embedding
Imagebase:	0x400000
File size:	614532 bytes
MD5 hash:	B3FD01873BD5FD163AB465779271C58F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\id2456.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\ID2456.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\ID2456.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\ifp2710.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\IFP2710.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\IFP2710.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pjd5132.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD5132.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD5132.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pjd5134.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD5134.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD5134.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pjd5232.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD5232.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD5232.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pjd5234.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD5234.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD5234.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pjd6543w.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD6543w.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD6543w.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pjd7820hd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD7820HD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD7820HD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pjd8353s.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD8353s.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD8353s.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pjd8633ws.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD8633ws.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\PJD8633ws.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\pro10100.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\Pro10100.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\Pro10100.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\sd-t225.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-T225.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-T225.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\sd-t245.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-T245.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-T245.inf	success or wait	1	31E7CFA	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\sd-z225.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-Z225.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-Z225.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\sd-z245.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-Z245.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-Z245.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\sd-z246.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-Z246.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\SD-Z246.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td1630-3.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD1630-3.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD1630-3.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td1655.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD1655.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD1655.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td1711.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD1711.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD1711.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2210_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2210_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2210_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2223.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2223.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2223.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2230_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2230_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2230_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2240_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2240_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2240_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2335_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2335_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2335_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2340_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2340_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2340_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2423.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2423.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2423.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2430 series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2430 Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2430 Series.INF	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2455.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2455.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2455.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2456.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2456.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2456.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2740_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2740_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2740_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td2760.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2760.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD2760.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\td3207.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD3207.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\TD3207.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1620_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1620_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\VA1620_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1630_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1630_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1630_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1655-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1655-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1655-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1901_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1901_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1901_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1903_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1903_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1903_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1912_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1912_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1912_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1917_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1917_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1917_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1920_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1920_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1920_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1921_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1921_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1921_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1922-a.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1922-a.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1922-a.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1923_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1923_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1923_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1925_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1925_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1925_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1938_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1938_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1938_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1939_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1939_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1939_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va1948_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1948_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA1948_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2022_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2022_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2022_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2037 series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2037 SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2037 SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2037a-led-2.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2037A-LED-2.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2037A-LED-2.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2046_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2046_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2046_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2055_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2055_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2055_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2201-fhd.cat	success or wait	1	31E7CFA	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\VA2201-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2201-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2201_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2201_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2201_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2205-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2205-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2205-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2209_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2209_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2209_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2210-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2210-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2210-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2212_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2212_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2212_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2214s_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2214s_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2214s_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2215-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2215-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2215-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2220_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2220_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2220_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2223-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2223-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2223-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2232-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2232-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2232-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2233-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2233-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2233-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2241_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2241_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2241_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2246_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2246_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2246_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2247-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2247-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2247-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2249_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2249_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2249_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2251_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2251_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2251_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2252_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2252_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2252_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2256_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2256_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2256_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2259 series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2259 Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2259 Series.inf	success or wait	1	31E7CFA	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\va2261_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2261_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2261_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2265S_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2265_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2265_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2342_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2342_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2342_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2349_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2349_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2349_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2359 series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2359 Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2359 Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2403-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2403-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2403-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2405-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2405-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2405-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2406-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2406-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2406-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2406_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2406_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2406_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2407_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2407_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2407_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2408-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2408-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2408-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2408_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2408_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2408_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2409-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2409-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2409-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2410-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2410-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2410-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2415-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2415-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2415-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2415_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2415_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2415_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2418-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2418-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2418-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2419_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2419_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2419_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2420-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2420-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2420-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2430-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2430-FHD.icm	success or wait	1	31E7CFA	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\VA2430-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2432-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2432-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2432-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2435-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2435-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2435-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2445_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2445_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2445_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2446_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2446_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2446_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2447-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2447-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2447-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2449 series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2449 Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2449 Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2451_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2451_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2451_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2452_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2452_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2452_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2455_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2455_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2455_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2456_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2456_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2456_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2459-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2459-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2459-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2459_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2459_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2459_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2465_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2465_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2465_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2710-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2710-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2710-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2715-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2715-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2715-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2715-qhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2715-QHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2715-QHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2718-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2718-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2718-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2719-2k_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2719-2K_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2719-2K_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2719_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2719_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2719_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2720-fhd.cat	success or wait	1	31E7CFA	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\VA2720-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2720-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2732-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2732-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2732-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2735-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2735-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2735-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2746_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2746_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2746_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2747-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2747-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2747-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2756_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2756_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2756_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2759 series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2759 Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2759 Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2759-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2759-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2759-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2855_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2855_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2855_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va2932_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2932_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA2932_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va3209-fhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA3209-FHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA3209-FHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va3209-qhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA3209-QHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA3209-QHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va3456-wqhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA3456-WQHD.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA3456-WQHD.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va705_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA705_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA705_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va916_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA916_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA916_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va926_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA926_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA926_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\va951s.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA951S.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VA951S.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg1655.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG1655.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG1655.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2039 SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2039 SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2039.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2233mh_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2233mh_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2233mh_Series.inf	success or wait	1	31E7CFA	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\vg2233smh_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2233Smh_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2233Smh_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2233_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2233_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2233_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2235_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2235_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2235_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2239_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2239_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2239_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2240.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2240.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2240.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2248.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2248.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2248.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2249_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2249_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2249_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2253_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2253_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2253_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2401_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2401_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2401_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2409-mhu.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2409-mhu.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2409-mhu.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2428_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2428_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2428_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2433mh_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2433mh_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2433mh_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2433smh_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2433Smh_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2433Smh_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2433_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2433_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2433_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2435_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2435_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2435_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2437.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2437_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2437_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2438_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2438_SERIES.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2438_SERIES.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2439_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2439_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2439_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2440.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2440.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2440.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2440v.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2440V.icm	success or wait	1	31E7CFA	DeleteFileA

File Path	Completion	Count	Source Address	Symbol
C:\ViewSonic\VG2440V.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2440w.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2440W.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2440W.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2448.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2448.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2448.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2448a.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2448a.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2448a.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2449_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2449_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2449_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2453_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2453_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2453_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2455-2k.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2455-2k.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2455-2K.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2455.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2455.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2455.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2456a.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2456a.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2456a.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2709-2k-mhd.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2709-2K-mhd.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2709-2K-mhd.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2709-2k-mhdu.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2709-2K-mhdu.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2709-2K-mhdu.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2709-mhu.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2709-mhu.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2709-mhu.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2719-2k.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2719-2K.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2719-2K.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2732_series.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2732_Series.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2732_Series.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2739.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2739.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2739.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2740v.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2740V.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2740V.inf	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\vg2748.cat	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2748.icm	success or wait	1	31E7CFA	DeleteFileA
C:\ViewSonic\VG2748.inf	success or wait	1	31E7CFA	DeleteFileA

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\default.pal	unknown	4	success or wait	1	32223EA	ReadFile
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\default.pal	unknown	12	success or wait	1	322242F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\mon.txt	unknown	4096	success or wait	1	3257CBB	ReadFile
C:\Windows\SysWOW64\mon.txt	unknown	4096	end of file	1	3257CBB	ReadFile
C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\VSC.BMP	unknown	13734	success or wait	1	33E2765	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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: IKernel.exe PID: **7140**, Parent PID: **1852**

General

Target ID:	4
Start time:	17:16:50
Start date:	06/06/2023
Path:	C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\IKernel.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Common Files\InstallShield\user\6\Intel 32\iKernel.exe" /REGSERVER
Imagebase:	0x400000
File size:	614532 bytes
MD5 hash:	B3FD01873BD5FD163AB465779271C58F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{91814EC0-B5F0-11D2-80B9-00104B1F6CEA}\LocalServer32	NULL	unicode	C:\PROGRA~2\COMMON~1\INSTAL~1\user\6\INTEL3~1\IKernel.exe	C:\PROGRA~2\COMMON~1\INSTAL~1\user\6\INTEL3~1\iKernel.exe	success or wait	1	431CC0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\WOW6432Node\CLSID\{22D84EC7-E201-4432-B3ED-A9DCA3604594}\LocalServer32	NULL	unicode	C:\PROGRA~2\COMMON~1\INSTAL~1\user\6\INTEL3~1\IKernel.exe	C:\PROGRA~2\COMMON~1\INSTAL~1\user\6\INTEL3~1\iKernel.exe	success or wait	1	431CC0	RegSetValueExA

Analysis Process: cmd.exe PID: **7040**, Parent PID: **1852**

General

Target ID:	5

Start time:	17:16:52
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon find monitor* > mon.txt
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\mon.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1BD194	CreateFileW

Analysis Process: conhost.exe PID: **7160**, Parent PID: **7040**

General

Target ID:	6
Start time:	17:16:52
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: devcon.exe PID: **4400**, Parent PID: **7040**

General

Target ID:	7
Start time:	17:16:53
Start date:	06/06/2023
Path:	C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon find monitor*
Imagebase:	0x100000000
File size:	73216 bytes
MD5 hash:	337FF45A8FD5B7BE152508EBC2E584CA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **7136**, Parent PID: **1852**

General	
Target ID:	10
Start time:	17:17:30
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon update
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **1772**, Parent PID: **7136**

General	
Target ID:	11
Start time:	17:17:30
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: devcon.exe PID: **7088**, Parent PID: **7136**

General	
Target ID:	12
Start time:	17:17:30
Start date:	06/06/2023
Path:	C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{FC47C7A5-BE63-11D5-B7C9-005004566E4D}\devcon update
Imagebase:	0x100000000
File size:	73216 bytes
MD5 hash:	337FF45A8FD5B7BE152508EBC2E584CA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly