ID: 377536
Sample Name:
SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
Cookbook: default.jbs
Time: 18:07:26
Date: 29/03/2021
Version: 31.0.0 Emerald

Table of Contents

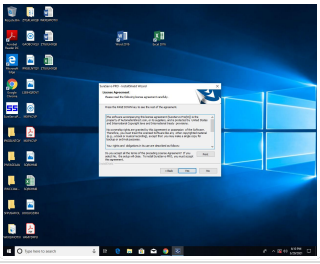
Analysis Report SureServoPROInstall_V4_1_0_5_DB2_0…

Overview

General Information

Sample Name:	SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
Analysis ID:	377536
MD5:	e1c700344a31ae..
SHA1:	e1ca62a65559a0..
SHA256:	fa07eeabe6dc625.
Infos:	

Most interesting Screenshot:



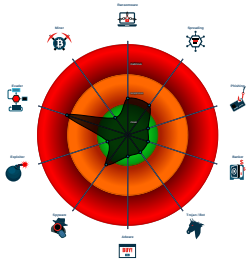
Detection

Score:	32
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- PE file has a writeable .text section
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query locale…
- Contains functionality to shutdown / …
- Contains functionality which may be…
- Detected potential crypto function
- Drops PE files
- Entry point lies outside standard sec…
- Extensive use of GetProcAddress (o…
- Found dropped PE file which has no…
- Found evasive API chain (may stop…

Classification



Analysis Advice

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

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

Startup

- **System is w10x64**
- SureServoPROInstall_V4_1_0_5_DB2_0_8.exe (PID: 6312 cmdline: 'C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe' MD5: E1C700344A31AEE275B86A0CC5FE707B)
  - setup.exe (PID: 6356 cmdline: C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe -package:'C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe' -no_selfdeleter -IS_temp -media_path:'C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\' -tempdisk1folder:'C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\' -IS_OriginalLauncher:'C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe' MD5: 88340D6E1DE3ED49364A64B3D8796AF6)
    - ISBEW64.exe (PID: 6544 cmdline: C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{B8FD074B-9EF5-416D-A3EE-6D8FB115C83F} MD5: 8A1E5A6B1C4E0C7D706EB2B36FA6C8EA)
    - ISBEW64.exe (PID: 6584 cmdline: C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{3BED6DCE-3BD7-42E3-BF6F-81E3F37201FD} MD5: 8A1E5A6B1C4E0C7D706EB2B36FA6C8EA)
    - ISBEW64.exe (PID: 6624 cmdline: C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{30C7FFBC-292B-4310-AFE7-0365F4C35832} MD5: 8A1E5A6B1C4E0C7D706EB2B36FA6C8EA)
    - ISBEW64.exe (PID: 6656 cmdline: C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{C15C7E7D-7890-420A-86BA-7E9024358B47} MD5: 8A1E5A6B1C4E0C7D706EB2B36FA6C8EA)
    - ISBEW64.exe (PID: 6696 cmdline: C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{6332241F-264C-4388-88EB-7A98CF4DBA83} MD5: 8A1E5A6B1C4E0C7D706EB2B36FA6C8EA)
    - ISBEW64.exe (PID: 6744 cmdline: C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{D1BE9E7C-E67D-4CF9-BA65-428ACD016A71} MD5: 8A1E5A6B1C4E0C7D706EB2B36FA6C8EA)
    - ISBEW64.exe (PID: 6784 cmdline: C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{176CEB1A-A045-48A9-ADF5-06CDBA606E31} MD5: 8A1E5A6B1C4E0C7D706EB2B36FA6C8EA)
- **cleanup**

Malware Configuration

No configs have been found

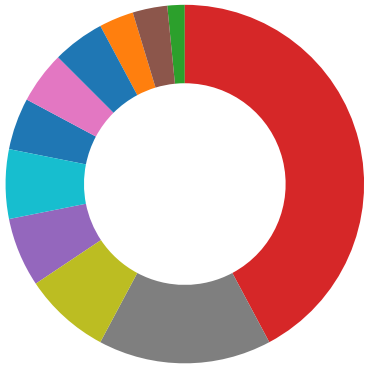
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Spreading
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

System Summary:

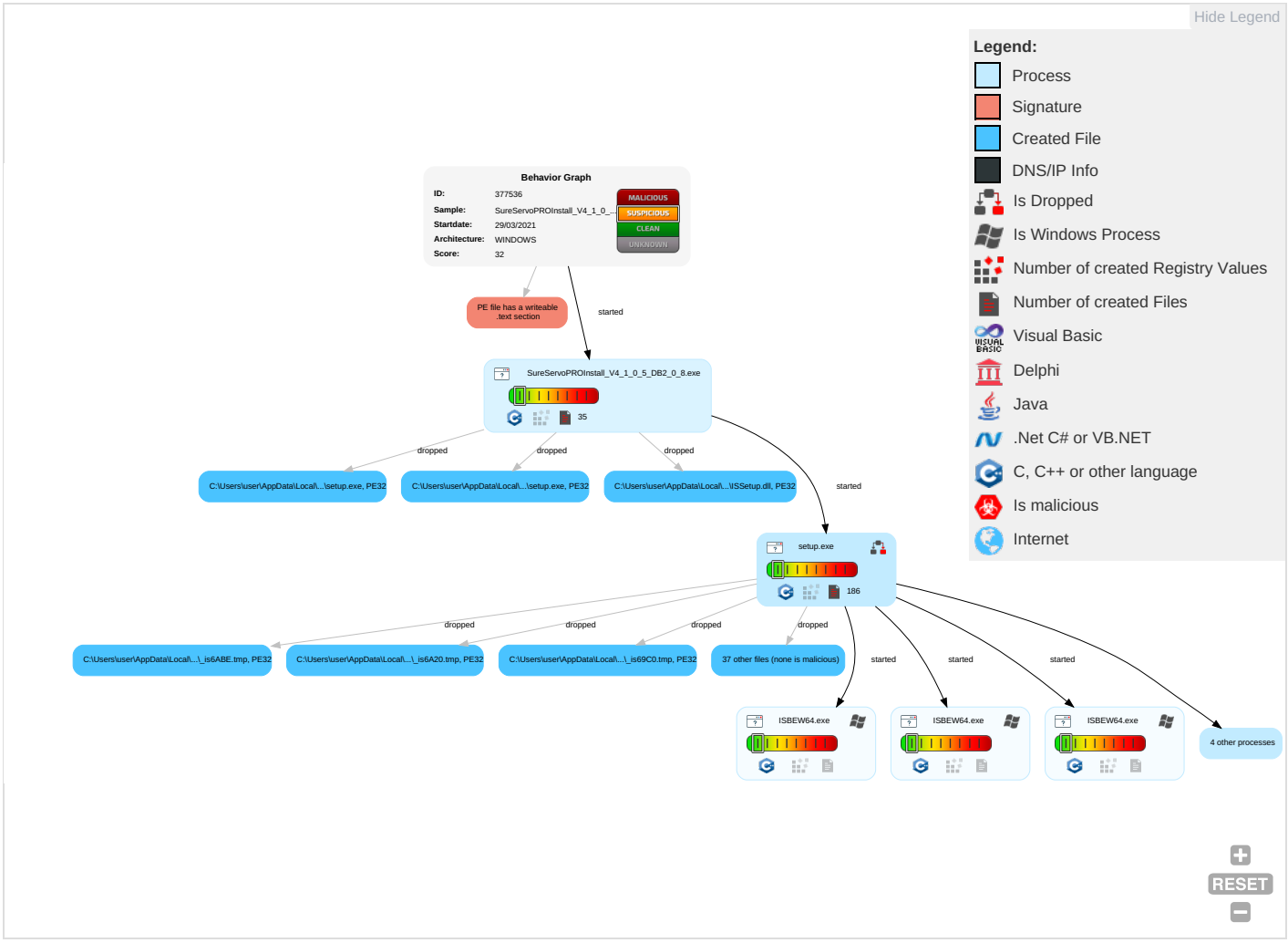
PE file has a writeable .text section

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Ren Ser Effe
Replication Through Removable Media 1	Command and Scripting Interpreter 1	Application Shimming 1	Access Token Manipulation 1	Access Token Manipulation 1	OS Credential Dumping	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Ren Trac With Auth
Default Accounts	Native API 3	Boot or Logon Initialization Scripts	Process Injection 2	Process Injection 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Ren Wip With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obt Dev Clou Bac
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Peripheral Device Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Ren Ser Effe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 2 6	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

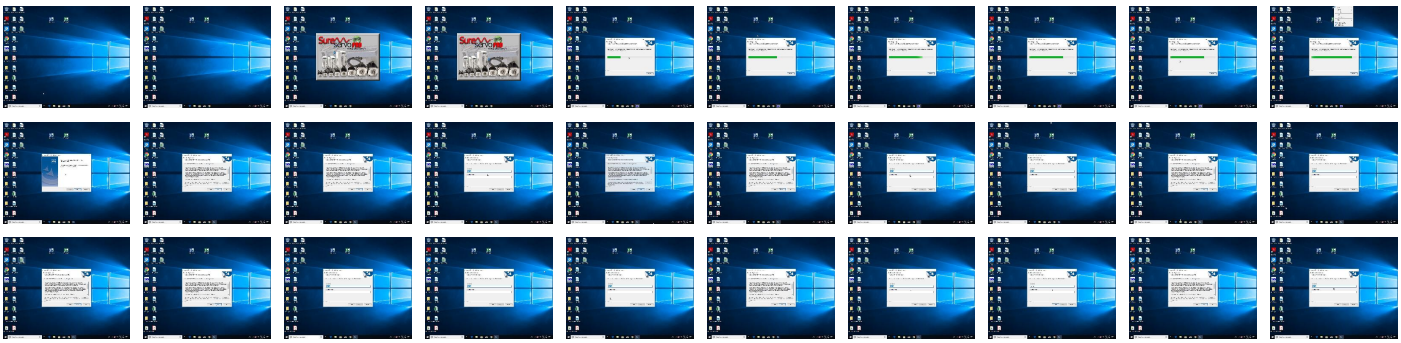
Behavior Graph

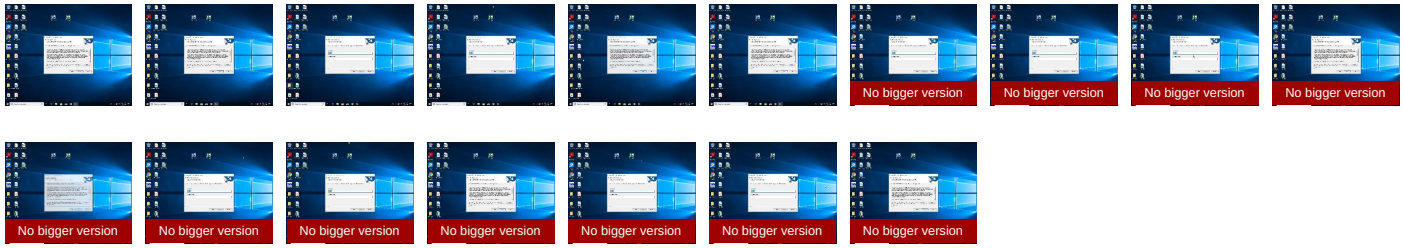


Screenshots

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
SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	0%	Virustotal		Browse
SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	3%	Metadefender		Browse
SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	0%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\ISSetup.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe	2%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542C.tmp	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_is5463.tmp	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Isr5530.tmp	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\MMO6B1E.tmp	3%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://=0x%04x.iniMS	0%	Avira URL Cloud	safe	
http://support.automationdirect.com8	0%	Avira URL Cloud	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://www.flexerasoftware.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://deviis4.installshield.com/NetNirvana/	setup.exe, 00000001.00000002.934145303.0000000000917000.00000004.00000020.sdmp	false		high
http://deviis4.installshield.com/NetNirvana/data2.cabDisk1	SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	false		high
http://=0x%04x.iniMS	SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	false	• Avira URL Cloud: safe	low
http://support.automationdirect.com8	setup.exe, 00000001.00000002.934145303.0000000000917000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.installshield.com/isetup/ProErrorCentral.asp?ErrorCode=%d	SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	setup.exe, 00000001.00000003.691546035.0000000000975000.00000004.00000001.sdmp, _is5560.tmp.1.dr	false		high
http://support.automationdirect.com	SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	false		high
http://www.flexerasoftware.com0	setup.exe, 00000001.00000002.948173876.00000000101BB000.00000040.00020000.sdmp, _is5560.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.symauth.com/cps0(	setup.exe, 00000001.00000002.948173876.00000000101BB000.00000040.00020000.sdmp, _is5560.tmp.1.dr	false		high
http://www.symauth.com/rpa00	setup.exe, 00000001.00000002.948173876.00000000101BB000.00000040.00020000.sdmp, _is5560.tmp.1.dr	false		high
http://ocsp.thawte.com0	setup.exe, 00000001.00000003.691546035.0000000000975000.00000004.00000001.sdmp, _is5560.tmp.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	377536
Start date:	29.03.2021
Start time:	18:07:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	SUS
Classification:	sus32.evad.winEXE@17/97@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.4% (good quality ratio 18.4%) • Quality average: 58.5% • Quality standard deviation: 37%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe • 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 NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	http://https://www.thepaynegroup.com/downloads/metadata/clients/blakecassels/ma5enterprise64.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	http://https://www.thepaynegroup.com/downloads/metadata/clients/blakecassels/ma5enterprise64.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	22490
Entropy (8bit):	3.484827950705229
Encrypted:	false
SSDEEP:	384:CTmyuV//BiTbh/Y4AwC2WrP2DBWa/Oa0Mhs+XVgv:CT6V//BiXh/N/lWr0aa0Mhs+XVgv
MD5:	8586214463BD73E1C2716113E5BD3E13
SHA1:	F02E3A76FD177964A846D4AA0A23F738178DB2BE
SHA-256:	089D3068E42958DD2C0AEC668E5B7E57B7584ACA5C77132B1BCBE3A1DA33EF54
SHA-512:	309200F38D0E29C9AAA99BB6D95F4347F8A8C320EB65742E7C539246AD9B759608BD5151D1C5D1D05888979DAA38F2B6C3BF492588B212B583B8ADBE81FA161
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..[.0.x.0.4.0.9.].....1.1.0.0.=.S.e.t.u.p. .I.n.i.t.i.a.l.i.z.a.t.i.o.n. .E.r.r.o.r.....1.1.0.1.=.%.s.....1.1.0.2.=.%.1. .S.e.t.u.p. .i.s. .p.r.e.p.a.r.i.n.g. .t.h.e. .%.2.,. .w.h.i.c.h. .w.i.l.l. .g.u.i.d.e. .y.o.u. .t.h.r.o.u.g.h. .t.h.e. .p.r.o.g.r.a.m. .s.e.t.u.p. .p.r.o.c.e.s.s... . .P.l.e.a.s.e. .w.a.i.t.....1.1.0.3.=.C.h.e.c.k.i.n.g. .O.p.e.r.a.t.i.n.g. .S.y.s.t.e.m. .V.e.r.s.i.o.n.....1.1.0.4.=.C.h.e.c.k.i.n.g. .W.i.n.d.o.w.s.(.R.). .I.n.s.t.a.l.l.e.r. .V.e.r.s.i.o.n.....1.1.0.5.=.C.o.n.f.i.g.u.r.i.n.g. .W.i.n.d.o.w.s. .I.n.s.t.a.l.l.e.r.....1.1.0.6.=.C.o.n.f.i.g.u.r.i.n.g. .%.s.....1.1.0.7.=.S.e.t.u.p. .h.a.s. .c.o.m.p.l.e.t.e.d. .c.o.n.f.i.g.u.r.i.n.g. .t.h.e. .W.i.n.d.o.w.s. .I.n.s.t.a.l.l.e.r. .o.n. .y.o.u.r. .s.y.s.t.e.m... .T.h.e. .s.y.s.t.e.m. .n.e.e.d.s. .t.o. .b.e. .r.e.s.t.a.r.t.e.d. .i.n. .o.r.d.e.r. .t.o. .c.o.n.t.i.n.u.e. .w.i.t.h. .t.h.e. .i.n.s.t.a.l.l.a.t.i.o.n... .P.l.e.a.s.e. .c.l.i.c.k. .R.e.s.t.a.r.t. .t.o. .r.e.b.o.o.t. .t.h.e. .s.y.s.t.e.m.....1.1.0.8.

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\0x0409.ini	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	22490
Entropy (8bit):	3.484827950705229
Encrypted:	false
SSDEEP:	384:CTmyuV//BiTbh/Y4AwC2WrP2DBWa/Oa0Mhs+XVgv:CT6V//BiXh/N/lWr0aa0Mhs+XVgv
MD5:	8586214463BD73E1C2716113E5BD3E13
SHA1:	F02E3A76FD177964A846D4AA0A23F738178DB2BE
SHA-256:	089D3068E42958DD2C0AEC668E5B7E57B7584ACA5C77132B1BCBE3A1DA33EF54
SHA-512:	309200F38D0E29C9AAA99BB6D95F4347F8A8C320EB65742E7C539246AD9B759608BD5151D1C5D1D05888979DAA38F2B6C3BF492588B212B583B8ADBE81FA161
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..[.0.x.0.4.0.9.].....1.1.0.0.=.S.e.t.u.p. .I.n.i.t.i.a.l.i.z.a.t.i.o.n. .E.r.r.o.r.....1.1.0.1.=.%.s.....1.1.0.2.=.%.1. .S.e.t.u.p. .i.s. .p.r.e.p.a.r.i.n.g. .t.h.e. .%.2.,. .w.h.i.c.h. .w.i.l.l. .g.u.i.d.e. .y.o.u. .t.h.r.o.u.g.h. .t.h.e. .p.r.o.g.r.a.m. .s.e.t.u.p. .p.r.o.c.e.s.s... . .P.l.e.a.s.e. .w.a.i.t.....1.1.0.3.=.C.h.e.c.k.i.n.g. .O.p.e.r.a.t.i.n.g. .S.y.s.t.e.m. .V.e.r.s.i.o.n.....1.1.0.4.=.C.h.e.c.k.i.n.g. .W.i.n.d.o.w.s.(.R.). .I.n.s.t.a.l.l.e.r. .V.e.r.s.i.o.n.....1.1.0.5.=.C.o.n.f.i.g.u.r.i.n.g. .W.i.n.d.o.w.s. .I.n.s.t.a.l.l.e.r.....1.1.0.6.=.C.o.n.f.i.g.u.r.i.n.g. .%.s.....1.1.0.7.=. S.e.t.u.p. .h.a.s. .c.o.m.p.l.e.t.e.d. .c.o.n.f.i.g.u.r.i.n.g. .t.h.e. .W.i.n.d.o.w.s. .I.n.s.t.a.l.l.e.r. .o.n. .y.o.u.r. .s.y.s.t.e.m... .T.h.e. .s.y.s.t.e.m. .n.e.e.d.s. .t.o. .b.e. .r.e.s.t.a.r.t.e.d. .i.n. .o.r.d.e.r. .t.o. .c.o.n.t.i.n.u.e. .w.i.t.h. .t.h.e. .i.n.s.t.a.l.l.a.t.i.o.n... .P.l.e.a.s.e. .c.l.i.c.k. .R.e.s.t.a.r.t. .t.o. .r.e.b.o.o.t. .t.h.e. .s.y.s.t.e.m.....1.1.0.8.

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\ISSetup.dll	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, PECompact2 compressed
Category:	dropped
Size (bytes):	807696
Entropy (8bit):	7.773931629042238
Encrypted:	false
SSDEEP:	12288:DIGz7ovgUHjhKtYCdP2q4/8mnL2YCTdSxZa65jcttUO+UC1nHZc:DIGz8IUDP0OqGL2YCsxZa6RuUO+UCd5c
MD5:	05E267CD74E51EFC3A9422AF3F85F6CD
SHA1:	B369F04872D31DB0D34D96014BB57BD2776AD84B
SHA-256:	0C98534B5A70E6CFA28D22BF71CE0C3F099B8F29BDD08DC39738C7D3179B22D2
SHA-512:	33BCA3B5ADE3C8A6065E470F4AAA4A2019C1B2C3324D84F71C45A5136CC8A8944EC73A1970F45D53569784B5DE624093EB08CA943A4CEBD6BD0237E5DBE50D 58
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....l.j.(...(...(.....).....1.....c...../.....)...(...4}.....=.....#...../.....S. .....)...)...(...).....)...Rich(.....PE..L.....yY.....!.....(...*.....E.%.....P.....%.....M.....8.%.G....%.....#.0.....6.....%.....`X..8.. .....k.....text.....#.....".....PEC2MO..... ....rsrc.....#.....&..... ....reloc.....%.....4.....@..... ....

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\autorun.inf	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	Microsoft Windows Autorun file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	43
Entropy (8bit):	3.9336877903443295
Encrypted:	false
SSDEEP:	3:It1KVm0QVkT2Vk9:e1K/AkTyk9
MD5:	01992077575FE1FEFE6C7CD35DE9C143
SHA1:	019D2DF4F51DC46552AF7B147678104F9CA71B2B
SHA-256:	31A7E507A8C26F4D4DA0A7B8CE59EC9AF65959E4332A6B6115C1968D9D4D15A2
SHA-512:	3B662A894E0418A4B1C6D6AA29E41CE1081048D19FDCF702833B520B22A9D29C5DC8340FBAB3BE31687719D7B4963541E5603A5C429DC945FB4478B0E3358A6
Malicious:	false
Preview:	[autorun]..open=Setup.exe..icon=Setup.exe..

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	7306253
Entropy (8bit):	**7.99568327602191**
Encrypted:	**true**
SSDEEP:	196608:hvKkS/vK+2IzIg/Os3VSCyZ6a4oo/OGHWDgSgWd/bJcbiHQ6nZk:hikS/i+psg/Os3VSCyZ6a4oo/OGHWDgf
MD5:	E147FF02C54D48B2A41DE1F3A1106324

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	
SHA1:	8F47CB86B69E311345C191959230D5344B7CD9F7
SHA-256:	FE29FAE444C13656AB226FBDA2A19275467DDA8E93A60D3A5D2698FB3D5BCA8E
SHA-512:	53E44B91E3AC481695D2A48D06218D88F03460929119B20930AB50B0424E96661F4C516DB4BE011BB49EA7EE500C340AF891B2875BB2E259DDF5DB49507BDC38
Malicious:	false
Preview:	ISc(.....V..... .....Y.b...I.....Q.....tgB.].EQ.sh...S..6F.&....Jm`.D...dF.c,Z.{o$..... .....mS.n.0....?.....}.z.....A..r...DX..K...CZ..#...93;3..tLQ.t0.d..!.?9.R.\..Y../.2...-..u/...H.rI.&.PP..i"i.nL2....t.6U.^.(..).!.5...:.AM@qM....u.L.X .>...gz..0.k.D.9|.H..>...E..+... g!9xL.\."..:.j.<...;... 1r.2....3.n:VnDyE..4.1.....@.;...N.P..0..1V.....Vd.=@.Y<.K...Z...Y.y.f.g...,O....8..m..!+....C*..d|..MF=W.FI..kK.../...- C.....{9..DG./...f..Z...7s..{C..... F.$~.2...h>K.c.>...>p.'..J..bnW\v...)...;..~]..G/...]3..S.!/F..=...=...~o.....lg|.}

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.hdr	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	InstallShield CAB
Category:	dropped
Size (bytes):	34512
Entropy (8bit):	3.564088931334005
Encrypted:	false
SSDEEP:	768:glvtFvfaIZjgIO6SaJvr5gp8XA/lINy+7IjrwsfW5D:glvDvvPxljrjqD
MD5:	BC250A5D0A3A07926924129D9C8089A7
SHA1:	671765ED01DDC6A97C5E74C042FF74A4252443B8
SHA-256:	2DBDD9CECDB45CC415278FF48FBB91EC4C8CA7D30B103E111DEB6CEDB1E44098
SHA-512:	CED97FD79F9D91370AA9855D72927ED1B1C3FD2FD65DBC6CCD10B091E7F48CDC33FB6BD0EA736BF0A802D90C84ED88C4CB0B5C44F5731F797AF769DD22AEA2C
Malicious:	false
Preview:	ISc(.....N.....B~..... .....Y.b...I.....Q.....tgB.].EQ.sh...S..6F.&....Jm`.D...dF.c,Z.{o$..... .....=.....N.....6...6.....u.....+.....1.....I...U.....a...m...y..... ..! ..- ..9 ....E .....Q .....] ..i .....u ... ...!.....!.....)!.....5!

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\layout.bin	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	data
Category:	dropped
Size (bytes):	610
Entropy (8bit):	2.0732183138745826
Encrypted:	false
SSDEEP:	6:oMaqUlfMEl/qDjO2CbwkR5aSelhCnXl8JDWLNglETl127W7Jtn:o5flftaO2tk/aSakQyBTj
MD5:	C9D89E0C09500FBEE7C9E8916ABA26AC
SHA1:	2D8D315437E2055F3C5D4ADE094AC3FB01E54B0A
SHA-256:	8F794018826D9A76DF0897244E0EC6E9B68F57F2FF940B08AA573F53B8CBB34B
SHA-512:	DBA7D1454F7695FADC2C8D7B3E08746F195781CC1E2166DAEC3AC506E60BDB82C9C2BD03981C7C099BF69026AFBF0E15262A1A51B0078827103BB8260670397
Malicious:	false
Preview:	c..S.@..b.....@.(..... ....L.....%.....x.....$...8...N.....s.e.t.u.p...i.n.i.....a.u.t.o.r.u.n...i.n.f...s.e.t.u.p...b.m.p...s.e.t.u.p...i.n.x...I.S.S.e.t.u.p...d.l.l...0.x. 0.4.0.9...i.n.i...d.a.t.a.1...h.d.r...d.a.t.a.1...c.a.b...d.a.t.a.2...c.a.b...l.a.y.o.u.t...b.i.n...s.e.t.u.p...e.x.e...

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.bmp	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	PC bitmap, Windows 3.x format, 640 x 480 x 8
Category:	dropped
Size (bytes):	308278
Entropy (8bit):	5.797980736269797
Encrypted:	false
SSDEEP:	3072:JtDZFgZ72kTNsyfMXT9J2UUrDQjJk0YE4wg:MZ72kTaXT9QdYt5M
MD5:	F194EA7CDAF317D96FE18D056B45D481
SHA1:	A71E90D631BF9ECD2D68E5620C23E704B1B6364C
SHA-256:	22B6525B8F0825AFD510ED60D0EAD259576DE32F38B4C501EA13BB49006D2218
SHA-512:	777038F077C772BF002AE1FBC26D5FD9E7FA741B87CFC907574A7537DC4B97B3893DDA4178E8D1412D260CBAF065A2A0B3AC136ABEA3D5919BE62F5B6DF119D
Malicious:	false
Preview:	BM6.....6...(.....".....".."..#!....". .#..#(.%&*.1+-.(3,.33-.*+2.1-3.,26.112.A<=.3H8.IL7.Td3../E.7;C...r..*i.--r.A>B .@?r.:DK.;iI.8Ok.:ps.EFI.RKL.GTL.VSL.HKS.RNR.JSX.VVY.a]\.GsS.kmE.juH.pxM.cb].ksY.uyX.FJd.SMb.KWc.Y\c.FFx.UJx.N_s.VXt.a^b.b]x.Zdj.ggi.rll.irl.stk.hls.qnr.jsx.wwx ..u>..vX..xN..oh..sn..|c..|{..~H.j.=.>.R.I.[.x.J.Q.f.t.z.Z.v.b.|...V...V...[...v...m...r...~..V..k..w.....!....(..*(..... ....&..,+..E?..A=..4C..;~../S..ON..b\..Os..gh..kw..w|..jk..xn..m~.. ux..MM..eZ..sr.....!....)../..... ....&../-..C<..@>..%@..<k..?K..LL..a^..oo..ON..`_..ts...~..;...O...h...{...g...x...n...z...l...|...^...g...z...y...o..|.....~..... .....

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1201936
Entropy (8bit):	6.693264418797218
Encrypted:	false
SSDEEP:	24576:SGjk6PMUtgtIKIch5+915zApy/MrllllVrGifVOCWCp:Tjk6PMUtgtJphMDw3llllVrGSVs+
MD5:	88340D6E1DE3ED49364A64B3D8796AF6
SHA1:	AB49D8F6556A2F5BA46857FBE82252D1BE3B67BD
SHA-256:	4026CFDBC97F2DF519BA28353057D8BC7CFFA7A4BCCD3F84239E28CEB7B1B50F
SHA-512:	DF1094BA3A47E0E2FE58DB48151FCB78922EF258353F951F7A89C12CA350ADE18F79C912A302EB8F606840A9BB3585F61E62CCF0CCC8127C89B751A80F3DFE6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^y....s...s...s.....s.....s.....s....s....Z.s..o....s...r...s..o....s...7.s..... s.....s.....s.Rich..s.....PE..L...d.yY.....r.....@.....Z.....B.....:.....8.....x4 ..@.....t...H:.. .....text..... ..`.rdata.....@..@.data...$L...p...&...N.....@....rsrc.....t.....@..@..... ....

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.ini	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	2424
Entropy (8bit):	3.6681367627408417
Encrypted:	false
SSDEEP:	48:rsAMoOOqqX1M74mcPTmscu/+S8gvn6CJkkY09TzcqYtxkYOvl5ZAMXvrcOyb0pn:rsAM3OGdcrmqrvnp6kY05w7tCYOvlnAM
MD5:	EE5F7E849785DA28D45BFCA84922B060
SHA1:	A417AD5C622C639C768E8861F2F23CE3AEE468AA
SHA-256:	A2F559B772F12833B7873116A4A5FC4BA2ACBA26A0B4A2E4ADB6E4BE61FD6876
SHA-512:	F080B8DA812AD255C689B9FE2A6EDA9908B363BB28AD34CD8BE58D717A8616DD006F601E3CAA7D95B3E251437EE714B43C5E859CA17AE9E8BB0BA4F53EC4FAE7
Malicious:	false
Preview:	..[.S.t.a.r.t.u.p.].....P.r.o.d.u.c.t.=.S.u.r.e.S.e.r.v.o. .P.R.O.....P.r.o.d.u.c.t.G.U.I.D.=.6.2.E.0.5.9.2.E.-.B.1.C.0.-.4.9.9.B.-.8.3.F.6.-.8.2.9.7.8.9.B.D.B.D.5.1.....C.o.m.p.a.n.y.N.a.m.e.=.A.u.t.o.m.a.t.i.o.n. .D.i.r.e.c.t.....C.o.m.p.a.n.y.U.R.L.=.w.w.w...a.u.t.o.m.a.t.i.o.n.d.i.r.e.c.t...c.o.m.....E.r.r.o.r.R.e.p.o.r.t.U.R.L.=.h.t.t.p.:././.w.w.w...i.n.s.t.a.l.l.s.h.i.e.l.d...c.o.m./.i.s.e.t.u.p./.P.r.o.E.r.r.o.r.C.e.n.t.r.a.l...a.s.p.?.E.r.r.o.r.C.o.d.e.=.%.d. .:. .0.x.%.x.&.E.r.r.o.r.I.n.f.o.=.%.s.....M.e.d.i.a.F.o.r.m.a.t.=.1.....L.o.g.M.o.d.e.=.1.....S.m.a.l.l.P.r.o.g.r.e.s.s.=.N.....S.p.l.a.s.h.T.i.m.e.=.....C.h.e.c.k.M.D.5.=.Y.....C.m.d.L.i.n.e.=.....S.h.o.w.P.a.s.s.w.o.r.d.D.i.a.l.o.g.=.N.....S.c.r.i.p.t.D.r.i.v.e.n.=.4.....[.L.a.n.g.u.a.g.e.s.].....D.e.f.a.u.l.t.=.0.x.0.4.0.9.....S.u.p.p.o.r.t.e.d.=.0.x.0.4.0.9.....R.e.q.u.i.r.e.E.x.a.c.t.L.a.n.g.M.a.t.c.h.=.0.x.0.4.0.4.,.0.x.0.8.0.4.....R.T.L.L.a.n.g.s.=.0.x.0.4.0.1.,.0.x.0.4.0.d.....[.0.x.0.4.0.9.].....0.x.0.4.

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.inx	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	data
Category:	dropped
Size (bytes):	259601
Entropy (8bit):	7.387400499116719
Encrypted:	false
SSDEEP:	3072:jAztrbh/sEXeBISOBQmRbXSP8A1ML1S4g4SNeJSfThMdU/L7Frt6Rec3pj3tCNMa:jAz5bl9xSEqNeJqOOxMecFtVkibw
MD5:	A7AEF385AB56FF232696DAB3C7D74C6D
SHA1:	48654BBB0FF5F14CDA79390D8438297440005220
SHA-256:	AB12A8B1F80818796EF14608323C809EB59875DC760BF4C685597952C8EAE545
SHA-512:	CACAB8F2B32CC48D992400D17FB83E7667C03C7922C9D43C1CDE4BFBFC16AB981941788F912C2E3833A259B5CBAA212805EE3FB51C03D5D9D48E2734902854D
Malicious:	false
Preview:	t.,....(... <$.M. .=.....l.....o.c...gWSl..SW..WS[//d.d l$.XX%.....q.y}a.=mQ.Y]A..M1..)!.).....}...m..q]}}aMm.U=].E-M.5.=.%.-.....].....a..(..H....YQQEY.0.o=55.={.gC[..W.....O.So##` .....,..x8.....X.....]..H.....5MM.5s..gW.CKgCC.....;..TDh..8P@.....8.....p.e..Q...| h.....%]1II.1....S[wSS.[.G.W .o....L.`H ..D.. .....t...L.....ayyIa.....s..w!99.!....Gs[K[.....T,.0,,.....|(.....l...P...yyy!a.....w.o.....W.;o?g..+O.....4.,$\.@....<.....l.....}uuI}.4..@....!99.!..s.w..3{.SGk.....0.D4\.... H.....4...Ye}!e. ..D....c.w.....w3.;#.#C.[.THl....(.<,4p,.$.....a..t...8..L..YQQ=Y...w.{o..`.--..S.w3.7+kk .....$..H8@.X,0...y.....x...H...1miMQ.c4....{%9-%%.-c.sO.. ...'7?..... @\D.....H.....iuUaaUi...MEE%M..gk.....?.7wK.....@.\$d8.....$.<.....e}}Qe...I]1II.1.W.[.c_.;[s.....g..W..L<l...

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, PECompact2 compressed
Category:	dropped
Size (bytes):	807696
Entropy (8bit):	7.773931629042238

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	
Encrypted:	false
SSDEEP:	12288:DIGz7ovgUHjhKtYCdP2q4/8mnL2YCTdSxZa65jcttUO+UC1nHZc:DIGz8IUDP0OqGL2YCsxZa6RuUO+UCd5c
MD5:	05E267CD74E51EFC3A9422AF3F85F6CD
SHA1:	B369F04872D31DB0D34D96014BB57BD2776AD84B
SHA-256:	0C98534B5A70E6CFA28D22BF71CE0C3F099B8F29BDD08DC39738C7D3179B22D2
SHA-512:	33BCA3B5ADE3C8A6065E470F4AAA4A2019C1B2C3324D84F71C45A5136CC8A8944EC73A1970F45D53569784B5DE624093EB08CA943A4CEBD6BD0237E5DBE50D58
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....I.j.(...(...(.....).....1.....c...../.....)...(...4}.....=.....#...../.....S. .....).....)...(...).....)...Rich(.....PE..L.....yY.....!.....(...*.....E.%.....P.....%.....M.....8.%.G....%.....#.0.....6.....%.....`X..8.. .....k.....text....#.....".....PEC2MO..... ....rsrc.....#.....&..... ....reloc.....%.....4.....@..... ....

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\MsiStub\{1F57C7D2-0C2E-406D-90F1-7C57BC934AB8}\SureServo PRO.msi	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	{96BB593B-34E7-4635-BEC7-ABBCC2C5C462}
Category:	dropped
Size (bytes):	5015552
Entropy (8bit):	7.968982080291819
Encrypted:	false
SSDEEP:	98304:gYyGExkMt19Xu6A/9DrrAAiVOJkgdsxMdTVmTyWEnzJ0KI3IleiDgtYu:/23t18//9DrrWVO3sS+GWEzJ0KI3Yeq+
MD5:	4705CFEB3D11C8E8BD63B664D822AF60
SHA1:	FE74B4D8BAF12129263EA0B6B9B0F37528D37DFC
SHA-256:	29AC0E87874DA09500145636EEC4FAEDA41359AC848768F7967422341853037F
SHA-512:	3456E8EE0735873BE13A08A2BF263521E8F31AF24DC5E12791B034ADA7CD710055DB42A5FBB9F4EA2ED63CD8CF7BAE7E609FCB1E0DF5B1F61F0604934A4EBB60
Malicious:	false
Preview:	.....>.....M.....8.....z.....o..... ...!..."...#...$...%...&...'...(...)...*...+....,-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M..... .....^..... ...!..."...#...$...%...&...'...(...)...*...+....,-...../...0...1...2...3...4...5...6...7... E...e...:...;...<...=...>...?...@...A...B...C...D...Y...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Z...]...[...\...`..._...d...c...a...b.....f...h.....g...i...n...j...m..... .....o.....p...y...r...s...t...u...v...w...x...k.....

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1201936
Entropy (8bit):	6.693264418797218
Encrypted:	false
SSDEEP:	24576:SGjk6PMUtgtIKIch5+915zApy/MrllllVrGifVOCWCp:Tjk6PMUtgtJphMDw3llllVrGSVs+
MD5:	88340D6E1DE3ED49364A64B3D8796AF6
SHA1:	AB49D8F6556A2F5BA46857FBE82252D1BE3B67BD
SHA-256:	4026CFDBC97F2DF519BA28353057D8BC7CFFA7A4BCCD3F84239E28CEB7B1B50F
SHA-512:	DF1094BA3A47E0E2FE58DB48151FCB78922EF258353F951F7A89C12CA350ADE18F79C912A302EB8F606840A9BB3585F61E62CCF0CCC8127C89B751A80F3DFE6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^y....s...s...s.....s.....s.....s.....s....Z.s..o....s...r...s..o....s...7.s..... s.....s.....s.Rich..s.....PE..L...d.yY.....r.....@.....Z.....B.....:.....8.....x4 ..@.....t...H:.. .....text..... ..`.rdata.....@..@.data...$L...p...&...N.....@....rsrc.....t.....@..@..... ....

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	
Process:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	2424
Entropy (8bit):	3.6681367627408417
Encrypted:	false
SSDEEP:	48:rsAMoOOqqX1M74mcPTmscu/+S8gvn6CJkkY09TzcqYtxkYOvl5ZAMXvrcOyb0pn:rsAM3OGdcrmqrvnp6kY05w7tCYOvlnAM
MD5:	EE5F7E849785DA28D45BFCA84922B060
SHA1:	A417AD5C622C639C768E8861F2F23CE3AEE468AA

C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	
SHA-256:	A2F559B772F12833B7873116A4A5FC4BA2ACBA26A0B4A2E4ADB6E4BE61FD6876
SHA-512:	F080B8DA812AD255C689B9FE2A6EDA9908B363BB28AD34CD8BE58D717A8616DD006F601E3CAA7D95B3E251437EE714B43C5E859CA17AE9E8BB0BA4F53EC4FAE7
Malicious:	false
Preview:	..[.S.t.a.r.t.u.p.].....P.r.o.d.u.c.t.=.S.u.r.e.S.e.r.v.o. .P.R.O.....P.r.o.d.u.c.t.G.U.I.D.=.6.2.E.0.5.9.2.E.-.B.1.C.0.-.4.9.9.B.-.8.3.F.6.-.8.2.9.7.8.9.B.D.B.D.5.1.....C.o.m.p.a.n.y.N.a.m.e.=.A.u.t.o.m.a.t.i.o.n. .D.i.r.e.c.t.....C.o.m.p.a.n.y.U.R.L.=.w.w.w...a.u.t.o.m.a.t.i.o.n.d.i.r.e.c.t...c.o.m.....E.r.r.o.r.R.e.p.o.r.t.U.R.L.=.h.t.t.p.:.//.w.w.w...i.n.s.t.a.l.l.s.h.i.e.l.d...c.o.m./.i.s.e.t.u.p./.P.r.o.E.r.r.o.r.C.e.n.t.r.a.l...a.s.p.?.E.r.r.o.r.C.o.d.e.=.%.d. .:. .0.x.%.x.&.E.r.r.o.r.I.n.f.o.=.%.s.....M.e.d.i.a.F.o.r.m.a.t.=.1.....L.o.g.M.o.d.e.=.1.....S.m.a.l.l.P.r.o.g.r.e.s.s.=.N.....S.p.l.a.s.h.T.i.m.e.=.....C.h.e.c.k.M.D.5.=.Y.....C.m.d.L.i.n.e.=.....S.h.o.w.P.a.s.s.w.o.r.d.D.i.a.l.o.g.=.N.....S.c.r.i.p.t.D.r.i.v.e.n.=.4.....[.L.a.n.g.u.a.g.e.s.].....D.e.f.a.u.l.t.=.0.x.0.4.0.9.....S.u.p.p.o.r.t.e.d.=.0.x.0.4.0.9.....R.e.q.u.i.r.e.E.x.a.c.t.L.a.n.g.M.a.t.c.h.=.0.x.0.4.0.4.,.0.x.0.8.0.4.....R.T.L.L.a.n.g.s.=.0.x.0.4.0.1.,.0.x.0.4.0.d.....[.0.x.0.4.0.9.].....0.x.0.4.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	182008
Entropy (8bit):	5.745001134941054
Encrypted:	false
SSDEEP:	3072:CIFNKUw8ALJ+C2T0FSmmiYQT4nF2E+JYVdeZ2bgA/qrXo:2Un0mT8Sc/T4F1bnxg85
MD5:	8A1E5A6B1C4E0C7D706EB2B36FA6C8EA
SHA1:	49199A62DE0EDA485B5287BAD469F92AD8EBD407
SHA-256:	4104FDE5404BFB3C5347B8ECDAEC89A2E746B1162DC75186BC79738805818C0A
SHA-512:	1393BD6C06C30DF7414494E5B06242445EB8AFDF5467C6A5E875F2C63506B0B581322B6444C6D8F06B39AA5B04D1C55A631CCF932DC6D5043296DD3ED3CD9F(
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: , Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.*.!.D.!.D.!.D../..D.D../..(.D./....D.... .D.!.E.[.D.....D.....%.D..... .D.!.. .D..... .D.Rich!.D.....PE..d...6.yY.....".....X...v.....@.....`.....J.....$.....`t..8..... .....p.....p.....text....W.....X..... ..`.rdata.....p.....\.....@..@.data... B...`.....D.....@....pdata..$.....`.....@..@.rs rc.....v.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\cor542B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	65503
Entropy (8bit):	3.783333450686201
Encrypted:	false
SSDEEP:	1536:biZVg/LPnypGccYM3MFe/Xvv+JcvpqLm416lt91FHWEi7I8qQdeVH3+HF2FnlP5r:gW/LPni+3MFe/XycRj4slt9HHWEi7I8M
MD5:	09D38CECA6A012F4CE5B54F03DB9B21A
SHA1:	01FCB72F22205E406FF9A48C5B98D7B7457D7D98
SHA-256:	F6D7BC8CA6550662166F34407968C7D3669613E50E98A4E40BEC1589E74FF5D1
SHA-512:	8C73CA3AF53A9BAF1B9801F87A8FF759DA9B40637A86567C6CC10AB491ACCB446B40C8966807BD06D52EB57384E2D6A4886510DE338019CFD7EF966B45315BA
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: 2/27/2002; rs....[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..6to4svc.dll=0x00000000..82557ndi.dll=0x00000000..8514a.dll=0x000

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23816
Entropy (8bit):	4.157035386837471
Encrypted:	false
SSDEEP:	192:YEm805ZvWFXfXDuQkC2+Z4nYe+PjPrSBO3SwVEnujexYi:q8SZvWFSQzHOnYPLWhjei
MD5:	A6CBAC7CEF4B03FCB1A9D65A5337B46C
SHA1:	DEC659C2ADEEA0B8E6C40DB8290F5855D652D7F4
SHA-256:	46AD0972344B2C71B560DAEB90075FDC5BD80F5D3AF33F1FD8B4C2D3A09FF978
SHA-512:	E8EBB5150274882E53AE7CC2BA21B01F2A7270D0FF7E979C8163EBB7600A8245D7ADEC5AAABE705EF03B5F16987649B21D6ABEBCB438935919D7403F8B25D05A

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542C.tmp	
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....yY..... .....*... ...@..... ....@.....*..K....@..x.....@.....`..... ..... ..H.....text..... ..... ..`.rsrc...x....@..... .....@..@.reloc.....`.....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542D.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	146
Entropy (8bit):	4.677494553177857
Encrypted:	false
SSDEEP:	3:cTIMOoIRuQVK/FNURAmIRMNHNQAolFNURAmIRMNHjKbo5KWREBAW4QIMOn:8IffVKNC7VNQAofC7V2bopuAW4QIT
MD5:	DB722945AB9C024CE55E469644393824
SHA1:	191782B3B4C7BD21FABB3D5B655B7F2DEC2F4F56
SHA-256:	C7E5BDC4B79F7F8C68C5F09C0C055E97FB8C62FE1B5D469B3527AB6B767C8DF2
SHA-512:	40503C28296CEB68428E327AC79326579C067511638263A477534B8E33341F24E2944077ACCDABB947981980F91604B71B6715A1488181B9C48515AB81271ED8
Malicious:	false
Preview:	<configuration>.. <startup>.. <supportedRuntime version="v2.0.50727"/>.. <supportedRuntime version="v4.0"/>.. </startup>..</configuration>

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\DIF542A.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	84
Entropy (8bit):	4.638552692098388
Encrypted:	false
SSDEEP:	3:m1eAsIdWVVVWhs6E2QVVK2Whsyor3Vg2Wn:mdv0am2QVVgQ3Van
MD5:	1EB6253DEE328C2063CA12CF657BE560
SHA1:	46E01BCBB287873CF59C57B616189505D2BB1607
SHA-256:	6BC8B890884278599E4C0CA4095CEFDF0F5394C5796012D169CC0933E03267A1
SHA-512:	7C573896ABC86D899AFBCE720690454C06DBFAFA97B69BC49B8E0DDEC5590CE16F3CC1A30408314DB7C4206AA95F5C684A6587EA2DA033AECC4F70720FC619E
Malicious:	false
Preview:	[<Properties>]..DIFx32Supported=No..DIFxIntel64Supported=No..DIFxAMD64Supported=No..

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Fon53FA.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.175273297885966
Encrypted:	false
SSDEEP:	3:m1eAsCMWRXBQYrD:mdjXIYf
MD5:	8CE28395A49EB4ADA962F828ECA2F130
SHA1:	270730E2969B8B03DB2A08BA93DFE60CBFB36C5F
SHA-256:	A7E91B042CE33490353C00244C0420C383A837E73E6006837A60D3C174102932
SHA-512:	BB712043CDDBE62B5BFDD79796299B0C4DE0883A39F79CD006D3B04A1A2BED74B477DF985F7A89B653E20CB719B94FA255FDAA0819A8C6180C338C01F39B832
Malicious:	false
Preview:	[<Properties>]..FontRegistration=No..

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Str542F.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3854
Entropy (8bit):	3.6972649326169598
Encrypted:	false
SSDEEP:	96:rsp62ISQHQmyrUeAL3TcnQcKH9tQDrKQNja1jiKWwNLNMuD7NkK/EVG64XzHjP:wKfLjpTdtmeYja1jxW45MsJkKmoP

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Str542F.tmp	
MD5:	7A3335A87C9357BE6F4B779EF83569C9
SHA1:	8E5800D3031ACD076BD3796A978646A51737978E
SHA-256:	32B99F413297053477458C4458F142074D30622C38D8232A0618A03CD534D0D3
SHA-512:	AFE8B91776C77BEA90676ECA6F576B7BC31BEF8F08D8CFC407CBFF4D108AAE908FD07054BDC3E6B13076D1E2FEAD142BB9F8062426EFD93D55D4A370B34CCA7B
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.9.].....F.O.L.D.E.R._.N.A.M.E.=.S.u.r.e.S.e.r.v.o. .P.R.O.....I.D.P.R.O.P._.S.E.T.U.P.T.Y.P.E._.C.O.M.P.L.E.T.E.=.C.o.m.p.l.e.t.e.....I.D.P.R.O.P._.S.E.T.U.P.T.Y.P.E._.C.O.M.P.L.E.T.E._.D.E.S.C.=.C.o.m.p.l.e.t.e.....I.D.P.R.O.P._.S.E.T.U.P.T.Y.P.E._.C.U.S.T.O.M.=.C.u.s.t.o.m.....I.D.P.R.O.P._.S.E.T.U.P.T.Y.P.E._.C.U.S.T.O.M._.D.E.S.C._.P.R.O.=.C.u.s.t.o.m.....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.U.n.k.n.o.w.n. .e.r.r.o.r. .r.e.t.u.r.n.e.d. .f.r.o.m. .N.e.t.A.P.I... .S.y.s.t.e.m. .e.r.r.o.r.:. .[.2.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.p.e.n. .[.P.r.o.d.u.c.t.N.a.m.e.].'.s. .o.r.i.g.i.n.a.l. .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.T.h.i.s. .e.x.e.c.u.t.a.b.l.e. .f.i.l.e. .d.o.e.s. .n.o.t. .a.p.p.e.a.r. .t.o. .b.e. .t.h.e. .o.r.i.g.i.n.a.l. .e.x.e.c.u.t.a.b.l.e. .f.i.l.e. .f.o.r. .[.P.r.o.d.u.c.t.N.a.m.e.]... .W.i.t.h.o.u.t. .u.s.i.n.g. .t.h.e. .o.r.i.g.i.n.a.l. .[.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_is5463.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1863024
Entropy (8bit):	5.6880358236693995
Encrypted:	false
SSDEEP:	12288:es4d9dfaOdWUIhpJCPtjvntnSb8COevQonCLPub+7iqV:ghrWVhDCPtjvntnSb8COevQonCfrV
MD5:	A05838872C391E729B414D2B15083983
SHA1:	027038259B7C4BFE0066B6F5635E416EFBD84157
SHA-256:	A7C7DB8CE84441DF150EE880E5BDE9C17BC7C85DC87A61B1760738ECEB61AD52
SHA-512:	0B13D56945A381DCFD453E9D21D62B030007D24B89FA6F7EAF75D62CA80F7C7FE1842A44D9DEB25E286AC8FB1FE7C3567666C1E116C96DFD641B56E9926212
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^..(...{...{...{...{...{J..{...{P..{..{...{...{...{..{...{Rich...{.....PE..L...[.yY.....!.....p.....@..(....P..V.....pP.....@.....A.....text. ..@..... ..`.rdata..... .....@..@.data....f.....P.....@....idata.....@..... .....@....rsrc...V....P.....0.....@..@.reloc...)...@...0... ....@..B..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\def5462.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	RIFF (little-endian) data, palette, version 1028, 0 entries
Category:	dropped
Size (bytes):	1168
Entropy (8bit):	2.551387347019812
Encrypted:	false
SSDEEP:	12:b126a96IlDkYTYcspSuB0MRG763GDwFGrZYOFBz3WI7KEpw3f6QL7nhem:Ax96Il9T3ISMg76KJrZtT2b5X
MD5:	0ABAFE3F69D053494405061DE2629C82
SHA1:	E414B6F1E9EB416B9895012D24110B844F9F56D1
SHA-256:	8075162DB275EB52F5D691B15FC0D970CB007F5BECE33CE5DB509EDF51C1F020
SHA-512:	63448F2BEF338EA44F3BF9EF35E594EF94B4259F3B2595D77A836E872129B879CEF912E23CF48421BABF1208275E21DA1FABFDC494958BCFCD391C78308EAA2
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...3.....f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3.....f...f...f...f...f...f...f...ff..f3..f...3...3...3...3f..33..3.....f...3.....f...f...f...f...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..33..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\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, PECompact2 compressed
Category:	dropped
Size (bytes):	432880
Entropy (8bit):	7.972245581674079
Encrypted:	false
SSDEEP:	12288:bQaI0sMvcMcl2xwNKASn+T3BKrJ1qhfcL1B:bK0s6cMcXAAQ+1w1qAn
MD5:	67B3328F3CC34596EC941DDA8574F606
SHA1:	219A67104A18F71C0CCB7B9D73F435D76E44F584
SHA-256:	CB80BFDD8263BB9AFF04BDC7D6BE71AD09800895B616223D8F97048AA0A506F7
SHA-512:	5E81FAC5A4E48353BDD0A60E8882B4B51A79298124D9FE8235940643BF2E4BFB13A881841A69DC479E1658CD42C6772C76A761CC2BE8342122E53460357C5091
Malicious:	false

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: , Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I..{'T.{'T.{'T...T.{'Tr..T.{'T!..T.{'Tr..T.{'Tr..T.{'T...T.{'T...T.{'T.{&Twz'T...T.{'T!..T.{'T!..T.{'T!..T.{'T.{.T.{'T!..T.{'TRich.{'T.....PE..L.....yY.....!.....b...6..... .....C.....S...T..... ...~.....8.....=..@.....text.....D.....PEC2MO..... ....rsrc....@.....4...H..... ....reloc.....|.....@..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\lic53F9.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1033
Entropy (8bit):	4.4792827760384135
Encrypted:	false
SSDEEP:	24:+y+y5wYN7mHxrvV3ttJZlAWDwz50m/F3MDGuBKN:+y+8wYNmHxrN3t7ZmWDe50mt8FA
MD5:	6093A0F7560DE0D93A0AE3C55EC18571
SHA1:	C0CDC3AC02D454CCD54D3871F4B68DB8E3141CF9
SHA-256:	393D6905E5CCAA672A03E3C35EE2FDD3E662D27C64D22759DEC04ACA2F84B1E8
SHA-512:	F167C407E42912D7F8EE17C6D56940F08BED2286E2A6F240A0CA5AC900967D0A66C9F0C0CDB54508A85DB8F7B3AC24C119C41D38BD309F41D2AD77CDC8A709 5
Malicious:	false
Preview:	The software accompanying this license agreement (SureServo Pro(tm)) is the property of AutomationDirect.com, or its suppliers, and is protected by United States and International Copyright laws and International treaty provisions. ....No ownership rights are granted by this Agreement or possession of the Software. Therefore, you mu st treat the Licensed Software like any other copyrighted material (e.g., a book or musical recording), except that you may make a single copy for backup or archival pu rposes. ....Your rights and obligations in its use are described as follows: ....1. You may use and display this software on a SINGLE COMPUTER. ....2. You may make one copy of the software for archival purposes or you may copy the software onto your hard disk and hold the original for archival purposes. ....3. You may not modify or attempt to reverse engineer the software, or make any attempt to change or even examine the source code of the software. ....4. You may transfer

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\set53F8.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	data
Category:	dropped
Size (bytes):	259601
Entropy (8bit):	7.387400499116719
Encrypted:	false
SSDEEP:	3072:jAztrbh/sEXeBISOBQmRbXSP8A1ML1S4g4SNeJSfThMdU/L7Frt6Rec3pj3tCNMa:jAz5bl9xSEqNeJqOOxMecFtVkibw
MD5:	A7AEF385AB56FF232696DAB3C7D74C6D
SHA1:	48654BBB0FF5F14CDA79390D8438297440005220
SHA-256:	AB12A8B1F80818796EF14608323C809EB59875DC760BF4C685597952C8EAE545
SHA-512:	CACAB8F2B32CC48D992400D17FB83E7667C03C7922C9D43C1CDE4BFBFC16AB981941788F912C2E3833A259B5CBAA212805EE3FB51C03D5D9D48E2734902854 D
Malicious:	false
Preview:	t.,....(... <$.M. .=.....l.....o.c...gWSl..SW..WS[//d.d l$.XX%.....q.y}a.=mQ.Y]A..M1..)!.).....}...m..q]}}aMm.U=].E-M.5.=.%.-..... .....].....a..(..H....YQQEY.0.o=55.={.gC[..W.....O.So##` .....,..x8.....X.....]..H.....5MM.5s..gW.CKgCC.....;..TDh..8P@.....8.....p.e..Q...| h.....%]1II.1....S[wSS.[.G.W .o....L.`H ..D.. .....t....L.....ayyIa.....s..w!99.!....Gs[K[.....T,.0,,.....|.....l...P...yyy!a.....w.o.....W.;o?g..+O.....4.,$\.@....<.....l.....}uuI}.4..@....!99.!..s.w..3{.SGk.....0. D4\.... H.....4...Ye}!e. ..D....c.w.....w3.;#.#C.[.THl....(.<,4p,.$.....a..t...8..L..YQQ=Y...w.{o..`.--..S.w3.7+kk .....$..H8@.X,0...y.....x...H...1miMQ.c4....{%9-%%.-c.sO.. ...'7?..... @\D.....H.....iuUaaUi...MEE%M..gk.....?.7wK.....@.\$d8.....$.<.....e}}Qe...I]1II.1.W.[.c_.;[s.....g..W..L<l...

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5461.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	RIFF (little-endian) data, palette, version 1028, 0 entries
Category:	dropped
Size (bytes):	1168
Entropy (8bit):	2.551387347019812
Encrypted:	false
SSDEEP:	12:b126a96llDkYTYcspSuB0MRG763GDwFGrZYOFBz3WI7KEpw3f6QL7nhem:Ax96Il9T3ISMg76KJrZtT2b5X
MD5:	0ABAFE3F69D053494405061DE2629C82
SHA1:	E414B6F1E9EB416B9895012D24110B844F9F56D1
SHA-256:	8075162DB275EB52F5D691B15FC0D970CB007F5BECE33CE5DB509EDF51C1F020
SHA-512:	63448F2BEF338EA44F3BF9EF35E594EF94B4259F3B2595D77A836E872129B879CEF912E23CF48421BABF1208275E21DA1FABFDC494958BCFCD391C78308EAA1
Malicious:	false

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5461.tmp	
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...3.f.3.3.3.3...3...3...3...3.f.3.3.3.3...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\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\lsr5530.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, PECompact2 compressed
Category:	dropped
Size (bytes):	432880
Entropy (8bit):	7.972254690191593
Encrypted:	false
SSDEEP:	12288:eQaI0sMvcMcl2xwNKASn+T3BKrJ1qhfcL1F:eK0s6cMcXAAQ+1w1qAr
MD5:	AD2580D26A6785877D6CF9F6341D016D
SHA1:	BD2E72709F28F29A06000AAEBD13C502ED17F35C
SHA-256:	1ED4BFBEF0555A5791BBF29710DBA6D1AB45741CD5149C6C5E3E2D805142601D
SHA-512:	8A6385ABDC0A00499D972DA8107C3EDBA7CECF6D31A3C6A3D497FCB2756BA7BD2EEB454597C18ECDAA2A52B73F12E1D22B142916D6E598908D1BE28B526376B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I..{'T.{'T.{'T...T.{'Tr..T.{'T!..T.{'Tr..T.{'Tr..T.{'T...T.{'T...T.{'T. {&Twz'T...T.{'T!..T.{'T!..T.{'T!..T.{'T.{.T.{'T!..T.{'TRich.{'T.....PE..L.....yY.....!.....b...6..... .....m.....S...T..... ...~.....8.....=..@.....text.....D.....PEC2MO..... ....rsrc....@.....4...H..... ....reloc.....|.....@..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\MMO6B1E.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	56576
Entropy (8bit):	4.564991825048028
Encrypted:	false
SSDEEP:	768:KbY9TtgL/031AnweYAXp8XHgKLOznUctiNxNk:aY9TtHMHXul6UcQZk
MD5:	E319496C8AE18C9323195906503295BE
SHA1:	87ACB69AAAF0C2579CB3178016EA3F98A8EAC7D9
SHA-256:	AB57D1D9E08357DC26421B82FBB7C4E3915B5E576434EE0663D75963EF288E25
SHA-512:	26436DBD83526CBA3581FCBAC363FFDF92544CEF269AE6BD6FF852F4E24E06714970CD0C649AB78ED41C764D3A28FBB39B776F7E604CE7D620EF3C499F495157
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....12.....H.....u(.....M.....Rich..... .PE..L...J.yY.....!.....P...p.....!.....`..... k..r...$f..P.....@.....`.....t ext....B.....P..... ..`.rdata.....`.....`.....@..@.data...@2...p...0...p.....@....rsrc.....@..@.reloc..(.....@..B..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Set5500.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	data
Category:	dropped
Size (bytes):	193294
Entropy (8bit):	7.395763852924137
Encrypted:	false
SSDEEP:	3072:j5YQKYcqV9W14Ih0ArHFgTosvd0WGYXa0ZQ62ecPvzXDzWt98pEycwP:j5tfTWfcdq0ZYecP1hco
MD5:	623F4E1640E711CB64FFE4D662190B89
SHA1:	013AFFDD85CE346DACB84B9F73D64C51FF0B9F6B
SHA-256:	41C8EC4BAEAEE9412A164E8B6BD9D08ED28D69101BFFB066913A229F62A447E4
SHA-512:	D93B4B311455A1724BF5E5257119D9417F1D049D6D68DBD28977F8A6432D170956FB336B842D650FC7CE8EFEBA24FAFCDA4963585659D9E294004C2BD38F2988
Malicious:	false
Preview:	t.,....(... <$.M. .=.....l.....o.c...gWSl..SW..WS[//d.d l$.XX%.....q.y}a.=mQ.Y]A. M1"a%!o).....}...m..q]}}aMm.U=].E-M.5.=.%.-..... .....A.....a..(..H....YQQEY.0.o=55.={.gC[..W.....O.So##` .....,..x8.....X.....]..H.....5MM.5s..gW.CKgCC.....;..TDh..8P@.....8.....p.e..Q...| h.....%]1II.1....S[wSS. [.G.W.o....L.`H ..D.. .....t....L.....ayyIa.....s..w!99.!....Gs[K[.....T,.0,,.....|(.....l...P...yyy!a.....w.o.....W.;o?g..+O.....4.,$\.@....<.....l.....}uul}.4..@....!99.!..s.w..3{.SGk. .....0.D4\.... H.....4...Ye}!e. ..D....c.w.....w3.;#.#C.[.THl....(.<,4p,.$.....a..t...8..L..YQQ=Y...w.{o..`.--..S.w3.7+kk .....$..H8@.X,0...y.....x...H...1miMQ.c4....{%9-%%.- c.sO....'7?..... @\D.....H.....iuUaaUi...MEE%M..gk.....?.7wK.....@.\|$d8.....$.<.....e}}Qe...I]1II.1.W.[.c_.;[s.....g..W..L<l...

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str55CE.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4336
Entropy (8bit):	3.7067941889247735
Encrypted:	false
SSDEEP:	96:rsfGRXOJABay9AIRp+tQDrKQNwNLNMuD7NK/EVGGZFLFrs1FWnDseQrlU72:wuBOOBzmtmeY45MsJKaZxRecseSlUC
MD5:	DC44BD4F445EC0FBFCDE6B81B69341FB
SHA1:	924A596D813D65C3D3D6C16057D8DA5ABF2FBAB4
SHA-256:	0A26A322483AE1A87D9B0CB50AAE05DCC97496066E0665509966A0E40ED78FDD
SHA-512:	529703FA3B856FF8A1ECA48EAD716F78A5CADA948D0BFF0D31126C9A0ED588409F44AF763774EE14360C89BF4AD1F568DDE903FF085F5D8F45C4601F9DB4146
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.c.0.c.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.U.n.e. .e.r.r.e.u.r. .i.n.c.o.n.n.u.e. .a. ...t... .r.e.n.v.o.y...e. .p.a.r. .N.e.t.A.P.I...E.r.r.e.u.r. .s.y.s.t... m.e...:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.u.v.r.i.r. .l.e. .f.i.c.h.i.e.r. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .d.e...:. .[. P.r.o.d.u.c.t.N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.C.e. .f.i.c.h.i.e.r. .e.x...c.u.t.a.b.l.e. .n.. e.s.t. .p.a.s. .l.. o.r.i.g.i.n.a.l. .e.x.i.g... .p.a.r. . [.P.r.o.d.u.c.t.N.a.m.e.]... .S.i. .v.o.u.s. .n.. u.t.i.l.i.s.e.z. .p.a.s...l.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .p.o.u.r. .i.n.s.t.a.l.l.e.r. .l.e.s. .d...p.e.n.d.a.n.c.e.s. .c.o.m.p.l. ..m.e.n.t.a.i.r.e.s.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5757.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4088
Entropy (8bit):	4.206486866324962
Encrypted:	false
SSDEEP:	96:rsDoJLpzMytQDrKQNwNLNMuD7NK/EVGj+fsFFLFrs1FWnDseQrlU72:wsJLpzMytmeY45MsJKXusFxRecseSlUC
MD5:	B0E5311CE9DB3F68DE549E6D7ADC4767
SHA1:	151C59A13B810070A466EFFF3F4370D2D87DB21C
SHA-256:	BB81906F08B9DF1ABEC43320935266505897E5E41ED2AAD84AC119F714DCA203
SHA-512:	AD84526CECBAA344FA07C7FBD640D041AB77E6C4EE28D26DE5065E7BADD8D714C63866736DB2D5535D9E7635996023BB3D54E2D92BA368ED3A2790EEE81EF 9F
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.c.1.a.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=...5.?.>.7.=.0.B.0. .3.@.5.H.:.0. .2.@.0.[.5.=.0. .>.4. .N.e.t.A.P.I... .!.8.A.B.5.<.A.:.0. .3.@.5.H.:.0.:. . [.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g. i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=...B.2.>.@.8.B.5. .[.P.r.o.d.u.c.t.N.a.m.e.]. .>.@.8.3.8.=.0.;. .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._. P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=...2.0. .8.7.2.@.H.=.0. .4.0.B.>.B.5.:.0. .=.8.X.5. .>.@.8.3.8.=.0.;.=.0. .8.7.2.@.H.=.0. .4.0.B.>.B.5.:.0. .7.0. .[.P.r.o.d.u. c.t.N.a.m.e.]... ...5.7. .:.>.@.8.H.[.5.Z.0. .>.@.8.3.8.=.0.;.0. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .7.0. .8.=.A.B.0.;.0.F.8.X.C. .4.>.4.0.B.=.8.E. .<.5.R.C.7.0.2.8.A.=.>.A.B.8.,. .[.P. r.o.d.u.c.t.N.a.m.e.]. .<.>.6.4.0. .=.5.[.5. .?.@.0.2.8.;.=.>. .@.0.4.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str57C6.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4114
Entropy (8bit):	3.6816229115047094
Encrypted:	false
SSDEEP:	96:rsNxLWZkPRmH+tQDrKQNwNLNMuD7NK/EVG+EFLFrs1FWnDseQrlU72:wXPtmeY45MsJK5xRecseSlUC
MD5:	5EB4E4FE0C7C8D6B332DD02D7215DE76
SHA1:	110B934D6953FFF5EA26709A4CF4DE79D75CDD82
SHA-256:	D8ADBA9B80D06B53ABA45D7B70FA8B9746D055EE346EAB30361843741D600B9D
SHA-512:	8EA24252FE85D86DFDDDC1A3DA3E3696D0A71585D7231BF45ACD473605A758BE4DDCCE22DE853A40EF31772F1002859EDF54BAECF7BF46735DD3346737A295 B
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.a.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.S.e. .h.a. .r.e.c.i.b.i.d.o. .u.n. .e.r.r.o.r. .d.e.s.c.o.n.o.c.i.d.o. .d.e. .N.e.t.A.P.I... .E.r.r.o.r. .d.e.l. .s. i.s.t.e.m.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. . 2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.A.b.r.i.r. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .d.e. .[.P.r.o.d.u.c.t.N.a.m.e.]. .....I. D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.E.s.t.e. .a.r.c.h.i.v.o. .e.j.e.c.u.t.a.b.l.e. .n.o. .p.a.r.e.c.e. .s.e.r. .e.l. .a.r.c.h.i.v.o. .e.j.e.c.u.t.a.b.l.e. .o.r.i.g.i.n.a.l. .d.e. .[.P.r.o.d.u.c.t.N.a.m.e.]... .S.i. .n.o. .s.e. .u.t.i.l.i.z.a. .e.l. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .p.a.r.a. .i.n.s.t.a.l.a.r. .l.a.s. .d.e.p.e.n.d.e.n.c.i.a.s. .a.d.i.c.i.o.n.a. l.e.s.,. .

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5826.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4050
Entropy (8bit):	3.7085218919932363

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5826.tmp	
Encrypted:	false
SSDEEP:	96:rsIwirf8tQDrKQNwNLNMuD7NK/EVGIFLFrs1FWnDseQrlU72:wIbrf8tmeY45MsJK0xRecseSlUC
MD5:	13F0A201CC47A57F915C49326741E5FA
SHA1:	A78D2B6062343F469E6F4FB544FAE54166079692
SHA-256:	A3E67EDB4A26F6E6326190DC115598AA594BF1FE34737E43AB65AD505ABD3931
SHA-512:	708C7414FC91D16626EE45ADE6BD52F630920381C59F0EE67C36F18E11F150E7C18D3C46B0C62E1F0E14B96D04C3D6998AE1996B68DA3DCCE6917129AAAB269D
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.b.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .p.a.l.a.u.t.t.i. .t.u.n.t.e.m.a.t.t.o.m.a.n. .v.i.r.h.e.e.n... .J...r.j.e.s.t.e.l.m...v.i.r.h.e.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. . E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.A.v.a.a. .t.u.o.t.t.e.e.n. .[.P.r.o.d.u.c.t.N.a.m.e.]. .a.l.k.u.p.e.r...i.n.e.n. .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.T...m... .t.i.e.d.o.s.t.o. .e.i. .n...y.t... .o.l.e.v.a.n. .t.u.o.t.t.e.e.n. .[.P.r.o.d.u.c.t.N.a.m.e.]. .a.l.k. u.p.e.r...i.n.e.n. .s.u.o.r.i.t.u.s.t.i.e.d.o.s.t.o... .J.o.s. .a.l.k.u.p.e.r...i.s.t... .t.i.e.d.o.s.t.o.a. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .e.i. .k...y.t.e.t... .l.i.s...r.i.i.p.p.u.v.u.u.k.s.i.e.n. . a.s.e.n.t.a.m.i.s.e.e.n.,. .[.P.r.o.d.u.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5895.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4284
Entropy (8bit):	3.7127159133841943
Encrypted:	false
SSDEEP:	96:rs9QuRXEJABayGVIRC7tQDrKQNwNLNMuD7NK/EVGfUFLFrs1FWnDseQrlU72:w9VBEOBzGtmeY45MsJKQxRecseSlUC
MD5:	49B60BC07EF4BB0349AB0E230A33EF0F
SHA1:	29682B4B4BBD569AF3259BA9E5ADF8CBE2A8421A
SHA-256:	AC9AA7CAD76A8C62C955225C216105DB89BF5070681A67E1C533F30EBBB99E8F
SHA-512:	8FF0BCD3168414F90B2B343FCCFA5CEB6C9E0BDDCC5E2559D8FCD3EF7F075690ADC4606C85A2BEBFCCD1DCD23263D6E38396DA3D0F9C9665D88018A6CE414CC
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.c.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.U.n.e. .e.r.r.e.u.r. .i.n.c.o.n.n.u.e. .a. ...t... .r.e.n.v.o.y...e. .p.a.r. .N.e.t.A.P.I... .E.r.r.e.u.r. .s.y.s.t. ..m.e...:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.u.v.r.i.r. .I.e. .f.i.c.h.i.e.r. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .d.e...:. .[.P.r.o.d.u.c.t.N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.C.e.t. .e.x.e. .n.. e.s.t. .p.a.s. .l.. o.r.i.g.i.n.a.l. .e.x.i.g... .p.a.r. .[.P.r.o.d.u.c.t.N.a.m.e.]... .S.i. .v.o.u.s. .n.. u.t.i.l.i.s.e.z. .p.a.s...l.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .p.o.u.r. .i.n.s.t.a.l.l.e.r. .l.e.s. .d...p.e.n.d.a.n.c.e.s. .c.o.m.p.l...m.e.n.t.a.i.r.e.s.,. .[.P.r.o.d.u. c.t.N.a.m.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str58F5.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3966
Entropy (8bit):	3.782323551356388
Encrypted:	false
SSDEEP:	96:rsGkNUxaRz+ZhtQDrKQNwNLNMuD7NK/EVG3FLFrs1FWnDseQrlU72:wGkNyaRz+ZhtmeY45MsJK7xRecseSlUC
MD5:	9FEBCB92E2796E3DB643A98CD6A8048F
SHA1:	91A8AD2D11594DC64FA5F79473CBE7E56418E0EF
SHA-256:	6C365B18AA0936AF8CAD22CB59574728A84C406FCC272E15597C5AD4DD786365
SHA-512:	3B3F25C2E49136739EB27F6E172D7D006D2B36F542E4C45DA8DF2BE1B806A422066A03293AABD44D5F5CB9A01803DC1186330AD4AEEBCE249947E91A70BF81A2
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.e.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.I.s.m.e.r.e.t.l.e.n. .h.i.b.a. .a. .N.e.t.A.P.I.-.r...l... .R.e.n.d.s.z.e.r.h.i.b.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.[.P.r.o.d.u.c.t.N.a.m.e.].e.r.e.d.e.t.i.j...n.e.k. .m.e.g.n.y.i.t...s.a. .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.E.z. .a. .v...g.r.e.h.a.j.t.h.a.t... .f...j.l. .n.e.m. .t.q.n.i.k. .a.(.z.). .[.P.r.o.d.u.c.t.N.a.m.e.]. .e.r.e.d.e.t.i. .v...g.r.e.h.a.j.t.h.a.t... .f...j.l.j...n.a.k... .H.a. .n.e.m. .t.e.l.e.p...t.i. .a. .t.o.v...b.b.i. .f...g.g.Q.s...g.e.k.e.t. .a.z. .e.r.e.d.e.t.i. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .h.a.s.z.n...l.a.t...v.a.l.,. .a.(.z.). .[.P.r.o.d.u.c.t.N.a.m.e.]. .e.s.e.t.l.e.g. .

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5993.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4144
Entropy (8bit):	3.737287689507876
Encrypted:	false
SSDEEP:	96:rsetyRnR5tNtQDrKQNwNLNMuD7NK/EVGYj46FLFrs1FWnDseQrlU72:wJppNtmeY45MsJKk86xRecseSlUC
MD5:	610E8CBF4583A43517CD4A454633EA14
SHA1:	F078248D8C2C2E0B5B30466886F1712C4ACC7EC3

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5993.tmp	
SHA-256:	87E995BD1EDF944B94E9965165D3E771098300980C5611B0E074F5F872DAA132
SHA-512:	5C6376125F9BC524508D3BC94979AFE29F3FFE97A38AF45772C901D340808FF083C26D7A5907CEEE3050D7B776C3C7D00FFD512D3CEFCAF438B245F95FFA585
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.a.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .j.a.v.l.j.a. .n.e.p.o.z.n.a.t.u. .g.r.e.a.k.u... .G.r.e.a.k.a. .s.u.s.t.a.v.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.o.t.v.a.r.a. .o.r.i.g.i.n.a.l.n.u. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .d.a.t.o.t.e.k.u. .z.a. .[.P.r.o.d.u.c.t.N.a.m.e.]. ....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.O.v.a. .d.a.t.o.t.e.k.a. .n.i.j.e. .o.r.i.g.i.n.a.l.n.a. .i.z.v.r.a.n.a. .d.a.t.o.t.e.k.a. .z.a. .[.P.r.o.d.u.c.t.N.a.m.e.]... .B.e.z. .u.p.o.t.r.e.b.e. .o.r.i.g.i.n.a.l.n.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .d.a.t.o.t.e.k.e. .z.a. .i.n.s.t.a.l.a.c.i.j.u. .d.o.d.a.t.n.i.h. .k.o.m.p.o.n.e.n.t.i.,. .[.P.r.o.d.u.c.t.N.a.m.e.]. . m.o.~.d.a. .n.e...e. .i.s.p.r.a.v.n.o. .

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str59F3.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4208
Entropy (8bit):	3.785870569518222
Encrypted:	false
SSDEEP:	96:rs7g7GdktQDrKQNwNLNMuD7NK/EVG49FLFrs1FW6DseQrlU72:w7GtmeY45MsJKYxRedseSlUC
MD5:	BD9F3AC351222469ED8737D18DC8BE9E
SHA1:	3D8C753C4205A9EBB94DEBE85790F551CDA2F58F
SHA-256:	DDB2AE8E37DDBDEB975A81FC2A2530128394ED7B575326DA333D3DD1A86951E8
SHA-512:	4D2108CB733C313CA718C4C9F306A7A215A0004F940E991592895B2699BE16124C88319C53161A416F5687F4977E3CBB12B50E1E6111C0F75E278CE28DE12515
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.b.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.Z. .N.e.t.A.P.I. .s.a. .v.r...t.i.l.a. .n.e.z.n...m.a. .c.h.y.b.a... .S.y.s.t...m.o.v... .c.h.y.b.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.t.v.o.r.i.e. .p...v.o.d.n... .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .[.P.r.o.d.u.c.t.N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.Z.d... .s.a.,. .~.e. .t.e.n.t.o. .s.p.u.s.t.i.t.e.>.n... .s...b.o.r. .n.i.e. .j.e. .s.p.u.s.t.i.t.e.>.n...m. .s...b.o.r.o.m. .p.r.e. .[.P.r.o.d.u.c.t.N.a.m.e.]... .B.e.z. .p.o.u.~.i.t.i.a. .p...v.o.d.n...h.o. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .p.r.e. .i.n.a.t.a.l...c.i.u. .d.o.d.a.t.o...n...c.h. .p.r...d.a.v.k.o.v.,. .n.e.m.u.s... .[.P.r.o.d.u.c.t.N.a.m.e.]. .f.u.n.g.o.v.a.e. .s.p.r...

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5B8B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4224
Entropy (8bit):	3.6902536137170823
Encrypted:	false
SSDEEP:	96:rsTYmGdUHkl8skHHFHiKFHFtQDrKQNwNLNMuD7NK/EVGDMFLFrs1FWnDseQrlU72:wTLkl16HtiKtFtmeY45MsJK3MxRecsei
MD5:	D7CE1D1C15336CA221C3582B75B612E8
SHA1:	169A027F3FD01E4791176D5DDE9CB82467026B35
SHA-256:	CE46FD9F9A892311F1A088B351B12299DCED570E6D29B60BA289129E049D4265
SHA-512:	B6DA4AC4C21D397B9D2682C8C59FFF48CE9332135CFBA875486747020598AEADD2F5F398649B5207CB564637A1F6AF06F7DBF688A6CBE948ECC255CF6B95448
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.d.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.E.t.t. .o.k...n.t. .f.e.l. .r.e.t.u.r.n.e.r.a.d.e.s. .f.r...n. .N.e.t.A.P.I... .S.y.s.t.e.m.f.e.l.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=...p.p.n.a. .d.e.n. .u.r.s.p.r.u.n.g.l.i.g.a. .v.e.r.s.i.o.n.e.n. .a.v. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .f...r. .[.P.r.o.d.u.c.t.N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.D.e.n. .h...r. .k...r.b.a.r.a. .f.i.l.e.n. .v.e.r.k.a.r. .i.n.t.e. .v.a.r.a. .d.e.n. .u.r.s.p.r.u.n.g.l.i.g.a. .k...r.b.a.r.a. .f.i.l.e.n. .f...r. .[.P.r.o.d.u.c.t.N.a.m.e.]... .O.m. .d.u. .i.n.t.e. .a.n.v...n.d.e.r. .d.e.n. .u.r.s.p.r.u.n.g.l.i.g.a. .v.e.r.s.i.o.n.e.n. .a.v. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .f...r. .a.t.t. .i.n.s.t.a.l.l.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C1A.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4084
Entropy (8bit):	4.354359322633157
Encrypted:	false
SSDEEP:	96:rsM/X0Uo/EtQDrKQNwNLNMuD7NK/EVGY1FLFrs1FWnDseQrlU72:wM/kUaEtmeY45MsJK+xRecseSlUC
MD5:	4B75B170BD6D4A8BC9A00C24F1E69370
SHA1:	F8A437C31F4BD8773BE70AC1F0C4F74E14182D0D
SHA-256:	88E3C5A90EF88A9E56CBAD049E1C301BB0591CBF110D1E72E2FF2A22AEB30826
SHA-512:	B8397DA1296531B50F3473A5861706ECB2F032E74610A28D2BD5E4702D8DF2E8CC79FEB9D37B50D7FC60FED61B265460F8C0BB3C6E1A2E42851F9C65E10116F
Malicious:	false

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C1A.tmp	
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.e.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.!.5...I.-...4.....%.2.....5.H.D.!.H...2.....4.....9...*.H.....%.1.....2... .N.e.t.A.P.I. ...I.-...4.....%.2...#.0.....: .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.C.+.I.@...4... .[.S.E.T.U.P.E.X.E.N.A.M.E.]. ...1.I...@...4.!...-... .[.P.r.o.d.u.c.t.N.a.m.e.]..... I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.D...%.L.....4...1...4...2.#...5.I...9.@.+.!.7.-...'.H.2.D.!.H.C...H.D...%.L.....4...1...4...2.#...1.I...@...4.!.*.3.+.#.1... .[.P.r.o.d.u.c.t.N.a.m.e.]. .@.!.7.H.-.D.!.H.C...I. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. ...1.I...@...4.!.C.....2.#...4.....1.I...*.H.'.....#.0...-.....5.H.*.1.!...1.....L...1...@...4.H.!.@...4.!. .[.P.r.o.d.u.c.t.N.a.m.e.]. .-.2.....3...2.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C89.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3970
Entropy (8bit):	3.811792594718289
Encrypted:	false
SSDEEP:	96:rsW6WHitQDrKQNwNLNMuD7NK/EVGlxqFLFrs1FWnDseQrlU72:wW6EitmeY45MsJKDqxRecseSlUC
MD5:	9913E3283688E61025D3804C56C451B1
SHA1:	C70C6CBA4DF874D9CE1AA032BB34AA09DFDAC8FE
SHA-256:	2CAD6DCED29395AC2ED56696C03B0B3580ADE1B59AB21CEF8B3583E89347EB67
SHA-512:	C623A43059B06B1755AA20F0131F56AC42975D729F8668C1018FE9F490FC5ACB185D1FD1EC319F6C68AA2EFB30670F90C2CD871719E75275F12CE917A06BBA63
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.f.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I.. d.e.n. .b.i.l.i.n.m.e.y.e.n. .h.a.t.a. .d...n.d...r...l.d..... .S.i.s.t.e.m. .h.a.t.a.s.1.:. .[.2.]... ..I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.[.P.r.o.d.u.c.t.N.a.m.e.]. .i...i.n. ...z.g...n. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .a.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.B.u. .y...r...t...l.e.b.i.l.i.r. .d.o.s.y.a.,.[.P.r.o.d.u.c.t.N.a.m.e.]. .i...i.n. ...z.g...n. .y...r...t...l.e.b.i.l.i.r. .d.o.s.y.a. .g.i.b.i. .g...r... n.m...y.o.r... .E.k. .b.a...1.m.l.1.l.1.k.l.a.r.1. .y...k.l.e.m.e.k. .i...i.n. ...z.g...n. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .k.u.l.l.a.n.m.a.d.a.n.,. .[.P.r.o.d.u.c.t.N.a.m.e.]. .d...z.g...n. ...a.l.1._. m.a.y.a.b.i.l.i.r... ...z.g...

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5CE9.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4116
Entropy (8bit):	3.7030824451271673
Encrypted:	false
SSDEEP:	96:rsXEPXlr76nxtQDrKQNwNLNMuD7NK/EVG5NFLFrs1FWnDseQrlU72:wXEPXlr76nxtmeY45MsJKPxRecseSlUC
MD5:	15F6DDD3D701DCC9BC3D8D0DC972338E
SHA1:	48D60B3EEFC2841E41983DD46CEB052D67896734
SHA-256:	6BC7FF846AEA9D6F6BA446FEB0B01AD84CC53CD575705EED754389FB6B60BD2F
SHA-512:	B6617E4476940B4EE7DC775CD0DE66043F83509D44C7FC4EA8B46925804B0FC0AF734DD38BCA64FDCF974D64646DBEAE08204CF9EFDB97BAEC32F91880EF26A0
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.2.d.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.E.r.r.o.r.e. .e.z.e.z.a.g.u.n.a. .i.t.z.u.l.i. .d.a. .N.e.t.A.P.I.-.t.i.k... .S.i.s.t.e.m.a.-.e.r.r.o.r.e.a.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.Z.a.b.a.l.d.u. .[.P.r.o.d.u.c.t.N.a.m.e.].-.r.e.n. .j.a.t.o.r.r.i.z.k.o. .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.E.z. .d.i.r.u.d.i. .f.i.t.x.a.t.e.g.i. .e.x.e.k.u.t.a.g.a.r.r.i. .h.a.u. .[.P.r.o.d.u.c.t.N.a.m.e.]. .j.a.t.o.r.r.i.z.k.o. .f.i.t.x.a.t.e.g.i. .e.x.e.k.u.t.a.g.a.r.r.i.a. .d.e.n.i.k... .M.e.n.d.e.k.o.t.a.s.u.n. .o.s.a.g.a.r.r.i.a.k. .i.n.s.t.a.l.a.t.z.e.k.o.,. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .j.a.t.o.r.r.i.z.k.o.a. .e.r.a.b.i.l.i. .e.z.e.a.n.,. .b.a.l.i.t.e.k.e.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5D49.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4066
Entropy (8bit):	4.188023453000621
Encrypted:	false
SSDEEP:	96:rsC+QA1Rky91RkstQDrKQNwNLNMuD7NK/EVGAjnFLFrsIkFWnDseQrlU72:wC+QA1Rky91RkstmeY45MsJKyxRIcsei
MD5:	E249C8AF20C688C103414DB347AC22E2
SHA1:	9428DBC7E2ED5F934B94597A50FF4EE01E11F1AF
SHA-256:	2CC62AEAA5A549DD4EE54D260828007D7C5FF7CD9C8D47C92225DF2501D5ECA0
SHA-512:	3AB9976FF39093DEC6430691E6BF5D0DCB7C2A2F697A0265156F2779DEAFAD2E97734AE10FDDA7F8DA0198863CA4035F50F3AA81BEDB64AA21B68953916E9B7
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.2.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=...B. .N.e.t.A.P.I. .5. .2.J.@.=.0.B.0. .=.5.8.7.2.5.A.B.=.0. .3.@.5.H.:.0... .!.8.A.B.5.<.=.0. .3.@.5.H.:.0.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=...B.2.>.@.5.B.5. .>.@.8.3.8.=.0.;.=.8.O. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .=.0. .[.P.r.o.d.u.c.t.N.a.m.e.]. .....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=...:.0.7.2.0. .A.5.,. .G.5. .B.>.7.8. .8.7.?.J.;.=.O.2.0.I. .D.0.9.;. .=.5. .5. .>.@.8.3.8.=.0.;.=.8.O. .7.0. .[.P.r.o.d.u.c.t.N.a.m.e.]... ...5.7. .?.>.<.>.I.B.0. .=.0. .>.@.8.3.8.=.0.;.=.8.O. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .7.0. .8.=.A.B.0.;.8.@.0.=.5. .=.0. .4.>.?.J.;.=.8.B.5.;.=.8. .7.0.2.8.A.8.<.>.A.B.8. .[.P.r.o.d.u.c.t.N.a.m.e.]. .<.>.6.5. .4.0. .=.5.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5DE7.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4178
Entropy (8bit):	3.69229861554142
Encrypted:	false
SSDEEP:	96:rst8bA3/j3cmZYMdW+tQDrKQNwNLNMuD7NK/EVG2X8AxpFLFrsIkFWnDseQrlU72:wmA3/j3btmeY45MsJKMfxRIcseSlUC
MD5:	E24CAD8451A5F6911B0E31D0E0C9F9EF
SHA1:	9F58E9B57BAC5BC8FFBC16591C2F1133FD0084AA
SHA-256:	33964E48ED968D8EB3B7AAA3FC4A1818DB43AD1469253AC5E7A6F71F9BB8D5BD
SHA-512:	E933B1ABDF24D92072DDD1DA03BE40CACC7241957DB4B260B4A428D60D3262357BD3896599450A3C61B1CF4D1AB0F85C60509797270893266A66472DC84B5D7
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.3.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .h.a. .r.e.t.o.r.n.a.t. .u.n. .e.r.r.o.r. .d.e.s.c.o.n.e.g.u.t.. .E.r.r.o.r. .d.e.l. .s.i.s.t.e.m.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.b.r.i.r. .e.l. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .d.e. .[.P.r.o.d.u.c.t.N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.A.q.u.e.s.t. .f.i.t.x.e.r. .e.x.e.c.u.t.a.b.l.e. .n.o. .s.e.m.b.l.a. .s.e.r. .e.l. .f.i.t.x.e.r. .e.x.e.c.u.t.a.b.l.e. .o.r.i.g.i.n.a.l. .p.e.r. .a. .[.P.r.o.d.u.c.t.N.a.m.e.]... .S.i. .n.o. .e.s. .f.a. .s.e.r.v.i.r. .e.l. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .p.e.r. .i.n.s.t.a.l...l.a.r. .l.e.s. .d.e.p.e.n.d...n.c.i.e.s. .a.d.d.i.c.i.o.n.a.l.s.,.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str61D1.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3418
Entropy (8bit):	4.169474695508292
Encrypted:	false
SSDEEP:	96:rsoNigLsAs3tQDrKQNwNLNMuD7NK/EVGAFLFrsIkFWnDseQrlU72:woNdLsAs3tmeY45MsJK8xRIcseSlUC
MD5:	238F3F00D54860840F513F485F9779AB
SHA1:	FC1CDBF3DBBABAA98653F47D31A78F9666404BBC
SHA-256:	A920114F4BE44709D686A71C4020638F24662EC50FD847990B02356C29DF1E35
SHA-512:	1297AD815E3FBE023EBF5F25F6D45D3FB9007D9CED2B19E8F0D8F6B3AE5D9D00C533C9B797DB89B958F2E5AC9997E5CDE87E327B10A70F3B2E15FBC14C8DAC74
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.4.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. ..P.V.N.P/.....S.V.N.f.0 ..|q}/...U. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=..._U .[.P.r.o.d.u.c.t.N.a.m.e.]. ..S.O.v .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.dk.WL..j}Y.P.N/f .[.P.r.o.d.u.c.t.N.a.m.e.]. ..S.O.v.WL..j.0 ...N(u.S.O.v .[.S.E.T.U.P.E.X.E.N.A.M.E.]. ..[.vQ.N.v.....[.P.r.o.d.u.c.t.N.a.m.e.]. ..S...g.Q.sOUL..0 ./f&T.\~b.S.O.v .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.S.E.A.R.C.H.=.,g!k.[..S.....O(uvQ.N.v....0 ..l.g...N.v.....[.P.r.o.d.u.c.t.N.a.m.e.]. ..S...g.Q.sOUL..0 ./f&T.\~b.S.O.v .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.O.G.M.S.G.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str626F.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4002
Entropy (8bit):	3.789808526965293
Encrypted:	false
SSDEEP:	96:rsC0FXh4n4tQDrKQNwNLNMuD7NK/EVG2HVFLFrsIkFWnDseQrlU72:w1Qn4tmeY45MsJKUxRIcseSlUC
MD5:	92ED43C2549B222BCD1FA7173458C264
SHA1:	7C82E9DA06A608A40DAB266B7CA0C06F7D4452E6
SHA-256:	05A5FA308678F8E86E519B3D99E3D6A07A210D608587B3448468308958C8C8AE
SHA-512:	33D22C5DFAA70D73D70E845E3AB5EF66ADC83958C9D6C713E78C9BFEC4577A84583BC1D53819FE7271A990E27768124DC904CBDA6D641216FD808DD64CACA79
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.5.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.R.o.z.h.r.a.n... .N.e.t.A.P.I. .v.r...t.i.l.o. .n.e.z.n...m.o.u. .c.h.y.b.u... .S.y.s.t...m.o.v... .c.h.y.b.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.t.e.v.Y...t. .p.o.v.o.d.n... .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .p.r.o.d.u.k.t.u. .[.P.r.o.d.u.c.t.N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.T.e.n.t.o. .s.p.u.s.t.i.t.e.l.n... .s.o.u.b.o.r. .s.e. .n.e.j.e.v... .j.a.k.o. .p.o.v.o.d.n... .s.p.u.s.t.i.t.e.l.n... .s.o.u.b.o.r. .p.r.o.d.u.k.t.u. .[.P.r.o.d.u.c.t.N.a.m.e.]... .B.e.z. .p.o.u.~.i.t... .p.o.v.o.d.n...h.o. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .k...i.n.s.t.a.l.a.c.i. .d.a.l.a...c.h. .z...v.i.s.l.o.s.t... .n.e.m.u.s... .[.P.r.o.d.u.c.t.N.a.m.e.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str62FE.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4078
Entropy (8bit):	3.693427637312151

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str62FE.tmp	
Encrypted:	false
SSDEEP:	96:rs4+G3TINFd/5FrtQDrKQNwNLNMuD7NK/EVGEFLFrsIkFWnDseQrlU72:wIM5rtmeY45MsJKoxRIcseSlUC
MD5:	B55E97DF4BC6CF5A58E6358FCC17174C
SHA1:	4BE6387473039A0D6185CEE6C833EAE883FC56B3
SHA-256:	905A175B585C6129B4A4318C51BC9799FE7E36307C920DBEE5C2940D5EDE363C
SHA-512:	39CA41DED43D7BF49FEA84943F0F8E10F462AF2F71445401731E87E3D33DC5AD0EF97760B8649C9947E6EDC75EDCF88E801172B61FCEF0A4353C6FD6B212149
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.6.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.U.k.e.n.d.t. .f.e.j.l. .r.e.t.u.r.n.e.r.e.t. .f.r.a. .N.e.t.A.P.I... .S.y.s.t.e.m.f.e.j.l.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=...b.n. .[.P.r.o.d.u.c.t.N.a.m.e.].s. .o.r.i.g.i.n.a.l.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.D.e.n.n.e. .e.k.s.e.k.v.e.r.b.a.r.e. .f.i.l. .s.e.r. .i.k.k.e. .u.d. .t.i.l. .a.t. .v...r.e. .d.e.n. .o.r.i.g.i.n.a.l.e. .e.k.s.e.k.v.e.r.b.a.r.e. .f.i.l. .t.i.l. .[.P.r.o.d.u.c.t.N.a.m.e.]... .H.v.i.s. .d.e.n. .o.r.i.g.i.n.a.l.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .i.k.k.e. .b.r.u.g.e.s. .t.i.l. .a.t. .i.n.s.t.a.l.l.e.r.e. .y.d.e.r.l.i.g.e.r.e. .a.f.h...n.g.i.g.h.e.d.e.r.,. .v.i.l. .[.P.r.o.d.u.c.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str636D.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4716
Entropy (8bit):	3.719544510550221
Encrypted:	false
SSDEEP:	96:rs0/zz+XzU8tQDrKQNwNLNMuD7NK/EVGzIBP/s8FLFrsIkFWnDseQrlU72:w0H+XTtmeY45MsJK/IBPnxRIcseSlUC
MD5:	9907D0B6FEAD612C422EE16E058624D0
SHA1:	7D0EF7DB3DD310AE5DB589D5DAF7A741DA269470
SHA-256:	236807D734A07ADE78940742DFE6D4F30B108D39BC119ADD685DC551A9D21B3D
SHA-512:	933818568C16E7359289A0C1F55BB2AC378EFC29B39A38188FEA2C4AF0E711B8445659DAB6A0D4DDA90C3899F4F461F66726ABA49C356D0CD7062C153CAAC1C
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.7.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .h.a.t. .e.i.n.e.n. .u.n.b.e.k.a.n.n.t.e.n. .F.e.h.l.e.r. .z.u.r...c.k.g.e.g.e.b.e.n... .S.y.s.t.e.m.f.e.h.l.e.r.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.r.i.g.i.n.a.l.d.a.t.e.i. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .v.o.n. .[.P.r.o.d.u.c.t.N.a.m.e.]. ...f.f.n.e.n.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.D.i.e.s.e. .a.u.s.f...h.r.b.a.r.e. .D.a.t.e.i. .i.s.t. .o.f.f.e.n.b.a.r. .n.i.c.h.t. .d.i.e. .a.u.s.f...h.r.b.a.r.e. .O.r.i.g.i.n.a.l.d.a.t.e.i. .f...r. .[.P.r.o.d.u.c.t.N.a.m.e.]... .W.e.n.n. .z.u.s...t.z.l.i.c.h.e. .A.b.h...n.g.i.g.k.e.i.t.e.n. .n.i.c.h.t. .m.i.t.h.i.l.f.e. .d.e.r. .O.r.i.g.i.n.a.l.d.a.t.e.i. .[.S.E.T.U.P.E.X.E.N.A.M.E.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str63FC.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4136
Entropy (8bit):	4.3186474621982365
Encrypted:	false
SSDEEP:	96:rs8d9AWOMprEtQDrKQNwNLNMuD7NK/EVGEhgWFLFrsIkFWnDseQrlU72:wYA6rEtmeY45MsJK4vxRIcseSlUC
MD5:	E08B34A09F134746811B216923BC461C
SHA1:	6DA2D5E79D416C7F869A80315B61F939BC2FE0CC
SHA-256:	8195CBE20C627D18F5E3942D0F29387F5ED5C38622E47DCC8AEBEA681F1ED957
SHA-512:	29D2896EB948097A48DC37015F36A3A30BC95AF265FDAAE9AD2521E3830E9548BC06C8A3168535D5633717C3F7A6215207AEC1B7BFE3324B5C09566769A283EA
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.8.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=..... .... .N.e.t.A.P.I... ....:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=..... ..... .[.P.r.o.d.u.c.t.N.a.m.e.].[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=..... ....[.P.r.o.d.u.c.t.N.a.m.e.]... ....[.S.E.T.U.P.E.X.E.N.A.M.E.]. .... ,..... .[.P.r.o.d.u.c.t.N.a.m.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str646B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4868
Entropy (8bit):	3.7114248634864744
Encrypted:	false
SSDEEP:	96:rs+yrUeAL3TcnQcKH9tQDrKQNwNLNMuD7NK/EVGzIBP/s6gFLFrs1FWnDseQrlUC:wsfLjpTdtmeY45MsJK/IBPpgxRecseSH
MD5:	9D8B071E65631600CB38B2BA79B5500C
SHA1:	F5DD23DBE257C59CD4F4980111AC5F55FEE16EB1
SHA-256:	7DD513653C65DBD891DCE0D9055B1EA47A6BCFD9A4FBE7AB7FB7655FCC1317C1
SHA-512:	969CB16A7045776C36F610E548BCBBDB1C30D2685F11BCB1CBA3E668D7D6587C451461FC795A2F7725A514A066E6A855003BAE27C7E18B16DB64C5013B55159

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str646B.tmp	
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.9.].....I.D.S._.E.R.R.O.R._.1.2.8.=.T.h.e. .W.i.n.d.o.w.s. .I.n.s.t.a.l.l.e.r. .s.e.r.v.i.c.e. .c.a.n.n.o.t. .u.p.d.a.t.e. .o.n.e. .o.r. .m.o.r.e. .p.r.o.t.e.c.t.e.d. .W.i.n.d.o.w.s. .f.i.l.e.s... .S.F.P. .E.r.r.o.r.:. .[.2.]... .L.i.s.t. .o.f. .p.r.o.t.e.c.t.e.d. .f.i.l.e.s.:. .[.3.].....I.D.S._.E.R.R.O.R._.1.2.9.=.U.s.e.r. .i.n.s.t.a.l.l.a.t.i.o.n.s. .a.r.e. .d.i.s.a.b.l.e.d. .v.i.a. .p.o.l.i.c.y. .o.n. .t.h.e. .m.a.c.h.i.n.e.....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.U.n.k.n.o.w.n. .e.r.r.o.r. .r.e.t.u.r.n.e.d. .f.r.o.m. .N.e.t.A.P.I... .S.y.s.t.e.m. .e.r.r.o.r.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.p.e.n. .[.P.r.o.d.u.c.t.N.a.m.e.].'.s. .o.r.i.g.i.n.a.l. .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str64CB.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4230
Entropy (8bit):	3.6763122905328247
Encrypted:	false
SSDEEP:	96:rsd3MeOitQDrKQNwNLNMuD7NK/EVGo1AFnZFLFrs1FWnDseQrlU72:wdceVtmeY45MsJKD1ZxRecseSlUC
MD5:	1BAD0A57D67D1F217EA2C07D5C6D39E1
SHA1:	BC25266746CC79C93AF7001AE0AAEA02DEAF3515
SHA-256:	2F09E90F440931737AC030D24FA8D0EED3A803074B83F8C20BC59A3A6FDBAB37
SHA-512:	970AAB1840DE73EF703F1A3C01646259428B7B6D8A5CB63CBB4CA6D88F6C8DFFABD02D6E0B4FACC378AC5563920669877926CC7A0A2B7DCA9ACF673D68ABD F43
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.0.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .h.a. .r.e.s.t.i.t.u.i.t.o. .u.n. .e.r.r.o.r.e. .s.c.o.n.o.s.c.i.u.t.o... .E.r.r.o.r.e. .d.i. .s.i.s.t.e.m.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.A.p.r.i.r.e. .i.l. .f.i.l.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l.e. .d.i. .[.P.r.o.d.u.c.t.N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.Q.u.e.s.t.o. .n.o.n. .s.e.m.b.r.a. .e.s.s.e.r.e. .i.l. .f.i.l.e. .e.s.e.g.u.i.b.i.l.e. .o.r.i.g.i.n.a.l.e. .d.i. .[.P.r.o.d.u.c.t.N.a.m.e.]... .S.e. .n.o.n. .s.i. .u.s.a. .l.a. .v.e.r.s.i.o.n.e. .o.r.i.g.i.n.a.l.e. .d.i. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .p.e.r. .i.n.s.t.a.l.l.a.r.e. .l.e. .d.i.p.e.n.d.e.n.z.e. .a.g.g.i.u.n.t.i.v.e.,. .[.P.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str652B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3996
Entropy (8bit):	4.205781947317776
Encrypted:	false
SSDEEP:	96:rsZBatQDrKQNwNLNMuD7NK/EVGzIBP/s+FLFrs1FWnDseQrlU72:wratmeY45MsJK/IBP5xRecseSlUC
MD5:	9D5F4B531FD698C68DFE9CB1690EB081
SHA1:	02CBF48ADC016DC97CDB35D8AFB151B903EBF9DC
SHA-256:	76379950A4C30BCE217F7E285077E5599C294E7F09AA6F6A0C7D6CD706DD4053
SHA-512:	0E56F4A5D4CFA184E2002EF3F0D0B118DE5BF7A97C5F86821C3731FA24AE31BEECF4CBC5B2F36CD9B71DEB635BF69613AD64804E152021F8B31D25B7803724F 5
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.1.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .K0.0.N.fj0.0.0.0L0.U0.0~0W0_0.0 ..0.0.0.0 ..0.0.0:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.[.P.r.o.d.u.c.t.N.a.m.e.]. .n0CQn0 .[.S.E.T.U.P.E.X.E.N.A.M.E.]. ..0..O0....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.S0n0.[L..S...0.0.0.0o0.0[.P.r.o.d.u.c.t.N.a.m.e.]. .n0CQn0.[L..S...0.0.0.0g0o0j0D0.0F0g0Y0.0 .CQn0 .[.S.E.T.U.P.E.X.E.N.A.M.E.]. ..0.O(u[0Z0k0...Rn0.OX[...O.0.0.0.0.0.0.0Y0.0h0.0[.P.r.o.d.u.c.t.N.a.m.e.]. .L0i..Rk0.R\OW0j0D0.S..`L0B0.0~0Y0.0 .CQn0 .[.S.E.T.U.P.E.X.E.N.A.M.E.]. ..0.i"}W0~0Y0K0?.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.S.E.A.R.C.H.=.S0n0.0.0.0.0.0.0o0.0...Rn0.OX[...O.0._..h0Y0.0.S..`L0B0.0~0Y0.0 ..OX[...Oj0

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str65C9.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3618
Entropy (8bit):	4.277404242152466
Encrypted:	false
SSDEEP:	96:rs9/Mnr8Nz0tQDrKQNwNLNMuD7NK/EVGDFLFrs1FWnDseQrlU72:w9/MnrNtmeY45MsJKfxRecseSlUC
MD5:	7AE0E03B82A1CB6F2500B2E2CD59A486
SHA1:	E2E3334CF2FF7E7FBC22AFC62A10A3A9FACECFDB
SHA-256:	446EC42E3842AAC9CEAB953FF46A208B492451646097B746C33134874EEBE5FB
SHA-512:	B3F2720EB9D59F0391192B945DBA71A41BF625BA5B480CBE9BB36545795E1BE171E1D611E35FDC078690F8054375FE17D248B99BE06EA8933B09AFFDB056BD9
Malicious:	false

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str65C9.tmp	
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.2.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I.\...0. .L. ... .$.X... ...X..... ....\. .$.X.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I .1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U .I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.[.P.r.o.d.u.c.t.N.a.m.e.].X. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. ....0.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.t. .. ..|.@. .[.P.r.o.d.u.c.t.N.a.m.e.].X. ....|.t. .D..... .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .....D. .....X... .J.. .... .m..D. .$.X.X.t. .[.P.r.o.d.u.c.t.N.a.m.e.].t.(...). .....\. ....X... .J.D. ... .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .....D. .>.<.....L.?.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.S.E.A.R.C.H.=.t. .$.X.|. ...t. .... .m..t. .D..`. ... .\. ...

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6667.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4174
Entropy (8bit):	3.690995189213825
Encrypted:	false
SSDEEP:	96:rsCy244ZOx1GOYtQDrKQNwNLNMuD7NK/EVGWFLFrs1FWnDseQrlU72:w+HtmeY45MsJK6xRecseSlUC
MD5:	FA85564A755F5D03455FFB6FD9243C56
SHA1:	33A9A3D215D58E5284DE6F5CCAE646E69438D614
SHA-256:	5C3EE71A61110C293061B6C2C3A42BE8669675674B72BA7F25E36934AD85CAA2
SHA-512:	8A2767B14F2CCE4ED65FB65C55410BE998742842670AF9CDEBC2D9218DCFDACD90729EE636AEBDBB141E6C191EDB3001161EB7FCCF879653E9BAB8FA67B0C BB8
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.3.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.O.n.b.e.k.e.n.d.e. .f.o.u.t. .g.e.r.e.t.o.u.r.n.e.e.r.d. .v.a.n. .N.e.t.A.P.I... .S.y.s.t.e.e.m.f.o.u.t.:. . [.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g. i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.r.i.g.i.n.e.l.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .v.a.n. .[.P.r.o.d.u.c.t.N.a.m.e.]. .o.p.e.n.e.n. ..... I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.D.i.t. .u.i.t.v.o.e.r.i.n.g.s.b.e.s.t.a.n.d. .i.s. .s.c.h.i.j.n.b.a.a.r. .n.i.e.t. .h.e.t. .o.r.i.g.i.n.e.l.e. .u.i.t.v.o.e.r.i. n.g.s.b.e.s.t.a.n.d. .v.o.o.r. .[.P.r.o.d.u.c.t.N.a.m.e.]... .Z.o.n.d.e.r. .g.e.b.r.u.i.k. .v.a.n. .d.e. .o.r.i.g.i.n.e.l.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .v.o.o.r. .h.e.t. .i.n.s.t.a.l.l.e.r.e.n. .v. a.n. .d.e. .e.x.t.r.a. .a.f.h.a.n.k.e.l.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str66C7.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4122
Entropy (8bit):	3.690315951986377
Encrypted:	false
SSDEEP:	96:rsU0mxCEJ0ikSvLJ0i/Ym5tQDrKQNwNLNMuD7NK/EVGfUFLFrs1FWnDseQrlU72:wXmwjNSvO6Ym5tmeY45MsJK7UxRecsei
MD5:	050779396F7FC99FFC5B81AD6254D25D
SHA1:	892CC925EF1C760A8B2177CCDC293B0CE08C2D18
SHA-256:	1DC65B0E43A63EF06611D093133A61BAE13D6CAE234B3A6442DDAABB1373F5B4
SHA-512:	ABB18375BB5FDB0560AD1F3EC772A9B524B5312C4E1E4DF5259F5347AF7E3C1602EF092EB25BE229AFCAF6870B961A6B63B77C2016D6C37486425E08D0C4EA2 F
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.4.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .r.e.t.u.r.n.e.r.t.e. .u.k.j.e.n.t. .f.e.i.l... .S.y.s.t.e.m.f.e.i.l.:. .[.2.]....I.D.S._.I.N.S.T.A.L. L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S. _.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=...p.n.e. .[.P.r.o.d.u.c.t.N.a.m.e.].s. .o.p.p.r.i.n.n.e.l.i.g.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I. T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.D.e.n.n.e. .k.j...r.b.a.r.e. .f.i.l.e.n. .e.r. .i.k.k.e. .d.e.n. .o.p.p.r.i.n.n.e.l.i.g.e. .k.j...r.b.a.r.e. .f.i.l.e.n. .f.o.r. .[.P.r.o.d.u.c.t.N.a.m.e.]... .D.e.t. .e.r. .m.u.l.i.g. .a.t. .[.P.r.o.d.u.c.t.N.a.m.e.]. .i.k.k.e. .f.u.n.g.e.r.e.r. .s.o.m. .d.e.t. .s.k.a.l. .u.t.e.n. ... .b.r.u.k.e. .d.e.t. .o.p.p.r.i.n.n.e.l.i.g.e. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .f.o.r. ... .i.n.s.t.a.l.l.e.r.e.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6765.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4276
Entropy (8bit):	3.8059353573148105
Encrypted:	false
SSDEEP:	96:rsb85Wd53tQHrKQlwlLl0uH7lK/EVG0FLFrs1FWnDseQrlU72:wbMo3t6ewQh0UxK4xRecseSlUC
MD5:	6971EE08A8BC5C8E4836D03EDFBC566D
SHA1:	E132BB2ACC742511C40AFE904DC387C34C10E80C
SHA-256:	44D69276FDA8862CDC529C8F4CD2830E2B583A327B7ABC738EC5D6AF8ABD252C
SHA-512:	2634235FBB253839835498F4FA25F55120412FC7BACFF1DA593B86820391F32C57E84A9462159EBA13C0E44B52657892301DEE4ED9EC49C925816A4D3EB554E4
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.5.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.I.n.t.e.r.f.e.j.s. .N.e.t.A.P.I. .z.w.r...c.i.B. .n.i.e.z.n.a.n.y. .b.B...d... .B.B...d. .s.y.s.t.e.m.o.w.y.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e. .....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.t.w...r.z. .o.r.y.g.i.n.a.l.n.y. .p.l.i.k. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .p.r.o.d.u.k.t.u. .[.P.r.o.d.u.c.t. N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.T.e.n. .p.l.i.k. .w.y.k.o.n.y.w.a.l.n.y. .p.r.a.w.d.o.p.o.d.o.b.n.i.e. .n.i.e. .j.e.s.t. .o.r.y.g.i.n.a.l.n.y.m. . p.l.i.k.i.e.m. . .[.P.r.o.d.u.c.t.N.a.m.e.]... .B.e.z. .z.a.i.n.s.t.a.l.o.w.a.n.i.a. .d.o.d.a.t.k.o.w.y.c.h. .w.y.m.a.g.a.n.y.c.h. .e.l.e.m.e.n.t...w. .z.a. .p.o.m.o.c... .o.r.y.g.i.n.a.l.n.e.g.o. .p.l.i.k.u. .[.S.E.T.U.P.E.X.E.N.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6823.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4094
Entropy (8bit):	3.696909822919476
Encrypted:	false
SSDEEP:	96:rsDGJ0NpGMS9aQS9+tQDrKQNwNLNMuD7NK/EVGQZFLFrs1FWnDseQrlU72:woo6tmeY45MsJKKxRecseSlUC
MD5:	1543BD3E0859BF4D1BED934250048EF2
SHA1:	E540507993A87BBFDEFBCB225DDCDA186DE928F0
SHA-256:	D3C5DAEE54797B805F4E10D6017CE72CAB413677393C38CF8998543052AF5441
SHA-512:	B7651DE2A540F70E0EC4F24C68F122C2D9EE6440A00605160C2BAD15C6E199F286134838113327CC972EA82AF9B502FEB8764AF69B5026650FB717082C4BD9F8
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.6.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .r.e.t.o.r.n.o.u. .u.m. .e.r.r.o. .d.e.s.c.o.n.h.e.c.i.d.o... .E.r.r.o. .d.o. .s.i.s.t.e.m.a.:. .[.2.]. ....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n. g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.A.b.r.i.r. .o. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .d.o. .[.P.r.o.d.u.c.t.N.a.m.e.].....I. D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.E.s.t.e. .a.r.q.u.i.v.o. .e.x.e.c.u.t...v.e.l. .n...o. .p.a.r.e.c.e. .s.e.r. .o. .a.r.q.u.i.v.o. .e.x.e.c.u.t...v.e.l. .o.r.i.g.i.n.a.l. .d.o. .[.P.r.o.d.u.c.t.N.a.m.e.]... .S.e.m. .u.s.a.r. .o. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .p.a.r.a. .i.n.s.t.a.l.a.r. .a.s. .d.e.p.e.n.d...n.c.i.a.s. .a.d.i.c.i.o.n.a.i.s.,. .o. .[.P.r.o. d.u.c.t.N.a.m.e.]. .t.a.l.v.e.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6892.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with very long lines, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4326
Entropy (8bit):	3.742736488733376
Encrypted:	false
SSDEEP:	96:rs0bm4iNhU443044+tQDrKQNwNLNMuD7NK/EVG0FLFrs1FWnDseQrlU72:w0BP6wtmeY45MsJKwxRecseSlUC
MD5:	CE0F6EDB4A13A61C274F84C14904E4D0
SHA1:	4EA7758EF297D0200C15DDFA15057B9072D01627
SHA-256:	9AFC89E8F72AB0F39C3C1BC239AEF2704290F661FB46C85803176AF737CB2CCA
SHA-512:	30D3387EC76822BA6D753D1B9EED11F414EB3398B35D6205AA5BF9BFEAC2295EE08864FDD2F718F588B2C84D47A04FC1FE921E7FF1CC4C2DC25CDB0B02FAF 90
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.8.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.E.r.o.a.r.e. .n.e.c.u.n.o.s.c.u.t... .r.e.t.u.r.n.a.t... .d.e. .N.e.t.A.P.I... .E.r.o.a.r.e. .d.e. .s.i.s.t.e.m.:. . [.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.D.e.s.c.h.i.d.e.c.i. .f.i._.i.e.r.u.l. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .c.o.r.e.s.p.u.n.z. ..t.o.r. .[.P.r.o.d.u.c.t.N.a.m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.A.c.e.s.t. .f.i._.i.e.r. .e.x.e.c.u.t.a.b.i.l. .n.u. .p.a.r.e. .a. .f.i. .f.i._.i.e.r.u.l. .e.x.e. c.u.t.a.b.i.l. .o.r.i.g.i.n.a.l. .p.e.n.t.r.u. .[.P.r.o.d.u.c.t.N.a.m.e.]... .D.a.c... .l.a. .i.n.s.t.a.l.a.r.e.a. .d.e.p.e.n.d.e.n.c.e.l.o.r. .s.u.p.l.i.m.e.n.t.a.r.e. .n.u. .s.e. .u.t.i.l.i.z.e.a.z... .f.i._. i.e.r.u.l.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6921.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4044
Entropy (8bit):	4.21849362276469
Encrypted:	false
SSDEEP:	96:rsCHsLlyhC19OtQDrKQNwNLNMuD7NK/EVGiFLFrs1FWnDseQrlU72:wiyyhC19OtmeY45MsJKexRecseSlUC
MD5:	E69CB7D48EA9CF5AB3821E5A83AF8E42
SHA1:	95A7A4AB79C880DE1C87BA8BD8C045A6FDC67743
SHA-256:	4C23AC79366731B8E032131C7F8EF2B476655AB90431B5A282A4DB78578325D4
SHA-512:	8C6F6939B9AC32B21BED59C87371CEE4DE26888874332B09FAB48ECC78DB1A988CD5641BF95FFD3C965B22BA3485DA71E5B2BDCF2F5E903D93AE8EB3F53ED DA
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.9.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=...5.8.7.2.5.A.B.=.0.O. .>.H.8.1.:.0.,. .2.K.4.0.=.=.0.O. .N.e.t.A.P.I... .!.8.A.B.5.<.=.0.O. .>.H.8.1.:.0. :. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n. g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=...B.:.@.K.B.L. .>.@.8.3.8.=.0.;.L.=.K.9. .D.0.9.;. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .[.P.r.o.d.u.c.t.N.a. m.e.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=...>.E.>.6.5. .8.A.?.>.;.=.O.5.<.K.9. .D.0.9.;. .=.5. .O.2.;.O.5.B.A.O. .>.@.8.3.8.=.0.;.L.=.K.<. .8.A.?.>.;. =.O.5.<.K.<. .D.0.9.;.>.<. .4.;.O. .[.P.r.o.d.u.c.t.N.a.m.e.]... ...A.;.8. .=.5. .8.A.?.>.;.L.7.>.2.0.B.L. .>.@.8.3.8.=.0.;.L.=.K.9. .D.0.9.;. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .4.;.O. .C.A.B.0.=.>.2.:.8. .4.>.?.>.;.=.8.B.5.;.L.=.K.E. .7.0.2.8.A.8.<.>.A.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str69BF.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4106
Entropy (8bit):	3.693476713395635

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str69BF.tmp	
Encrypted:	false
SSDEEP:	96:rs4uqh8NoqHecStV5DtQDrKQNwNLNMuD7NK/EVGQFFLFrs1FWnDseQrlU72:wxTePtmeY45MsJKExRecseSlUC
MD5:	67432E541206A23E5C96E74EA6D2FEA1
SHA1:	89EC40E0DC1BCA402D4D5B3F2B499CC85BAA4560
SHA-256:	9E0A28EB77E264E84093BA81F8044CB299C586AEA1E81801782E18BFC8425A9D
SHA-512:	E4232746B289793938FC9936180FB03CE7A7009AD1F8A49FCEE152C5ABA43649ED3717BD54E9274A4D8C11F3FB237E98A3B2B5F92B76C1F106CAB613E264C1B
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.2.1.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.K.e.s.a.l.a.h.a.n. .t.a.k. .d.i.k.e.n.a.l. .d.i.k.e.m.b.a.l.i.k.a.n. .d.a.r.i. .N.e.t.A.P.I... .K.e.s.a.l.a.h.a.n. .s.i.s.t.e.m.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.B.u.k.a. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .a.s.l.i. .u.n.t.u.k. .[.P.r.o.d.u.c.t.N.a.m.e.]. .....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.F.i.l.e. .e.x.e.c.u.t.a.b.l.e. .i.n.i. .t.a.m.p.a.k.n.y.a. .b.u.k.a.n. .f.i.l.e. .e.x.e.c.u.t.a.b.l.e. .a.s.l.i. .u.n.t.u.k. .[.P.r.o.d.u.c.t.N.a.m.e.]... .T.a.n.p.a. .m.e.n.g.g.u.n.a.k.a.n. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .a.s.l.i. .u.n.t.u.k. .m.e.n.g.i.n.s.t.a.l. .d.e.p.e.n.d.e.n.s.i. .t.a.m.b.a.h.a.n.,. .[.P.r.o.d.u.c.t.N.a.m.e.]. .t.i.d.a.k. .d.a.p.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A1F.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4066
Entropy (8bit):	3.7080241126917253
Encrypted:	false
SSDEEP:	96:rs4/ZulXtQDrKQNwNLNMuD7NK/EVG2fFLFrs1FWnDseQrlU72:w4/c5tmeY45MsJKcxRecseSlUC
MD5:	27F54FD5C0B794C5AFBAF65CB9F560BF
SHA1:	515DF34E99932A1D4348B02DE102B267069CD7AE
SHA-256:	0EBEC6EDC28341F56705DD91A70E99499C24177A8CCDF8B5F16086EE04D03630
SHA-512:	31714B56E53CCE7A2D9070D572AEFFE35C5D584AD009F61A179FC463F8960DC139AC58B1E60C2C5F88F29A374015BCCD298D29E887C543E0ECCEA7F93AA33F2
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.2.4.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .j.e. .v.r.n.i.l. .n.e.z.n.a.n.o. .n.a.p.a.k.o... .S.i.s.t.e.m.s.k.a. .n.a.p.a.k.a.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.O.d.p.r.i. .o.r.i.g.i.n.a.l.n.i. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .p.r.o.g.r.a.m.a. .[.P.r.o.d.u.c.t.N.a.m.e.]....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.N.i. .v.i.d.e.t.i.,. .d.a. .b.i. .b.i.l.a. .t.a. .i.z.v.r.a.l.j.i.v.a. .d.a.t.o.t.e.k.a. .o.r.i.g.i.n.a.l.n.a. .i.z.v.r.a.l.j.i.v.a. .d.a.t.o.t.e.k.a. .z.a. .[.P.r.o.d.u.c.t.N.a.m.e.]... ...e. .p.r.i. .n.a.m.e.s.t.i.t.v.i. .d.o.d.a.t.n.i.h. .o.d.v.i.s.n.o.s.t.i. .n.e. .u.p.o.r.a.b.l.j.a.t.e. .o.r.i.g.i.n.a.l.n.i.[.S.E.T.U.P.E.X.E.N.A.M.E.].,. .[.P.r.o.d.u.c.t.N.a.m.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A8E.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	3428
Entropy (8bit):	4.162682161486157
Encrypted:	false
SSDEEP:	96:rsEXRtQDrKQNwNLNMuD7NK/EVGEFLFrs1FWnDseQrlU72:wEXRtmeY45MsJKIxRecseSlUC
MD5:	747F4E546F471E9FB4A2A998A9937060
SHA1:	00FF0CFD40DFA3A72AAEB9BE641A11CA44BF7900
SHA-256:	13C438785ED135355515619E4FD39DF8BFD037A6DF0F3D0A2D8685CBCB33C702
SHA-512:	20F1F703F57C5E3B5B729EB6760F5648A6C533D5843FB0A137336829D53CA48C9AAB28E37383B9742213D9FEF058E8164F3711CD11C4BF83F21795D5361F713F
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.8.0.4.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. ...V.N*N.....S.V.N..0 ..|.~...U. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.Sb._ .[.P.r.o.d.u.c.t.N.a.m.e.]. ..SHr .[.S.E.T.U.P.E.X.E.N.A.M.E.]....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=...N.SgbL.. e.N}Ya..N/f .[.P.r.o.d.u.c.t.N.a.m.e.]. ..SHr.v.SgbL..e.N.0 ...N(u.SHr.v .[.S.E.T.U.P.E.X.E.N.A.M.E.]. ..[.vQ.N.vsQo..N..[.P.r.o.d.u.c.t.N.a.m.e.]. ..S...O.Q.s...0 ./f&T.[~b.SHr.v . [.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.S.E.A.R.C.H.=.,g!k.[..S.....O(uvQ.N.vsQo..N.0 ..l.g..N.vsQo..N..[.P.r.o.d.u.c.t.N.a.m.e.]. ..S...O.Q.s...0 ./f&T.[~b.Seg.v .[.S.E.T.U.P.E.X.E.N.A.M.E.].....I.D.S._.P.R.O.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6B1D.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4062
Entropy (8bit):	3.700139722926891
Encrypted:	false
SSDEEP:	96:rsiQvGJS0BGE9a49+tQDrKQNwNLNMuD7NK/EVGNEFLFrs1FWnDseQrlU72:w2SRtmeY45MsJKCxRecseSlUC
MD5:	1806AF207B3B3554176BE2DE76068302
SHA1:	908E69CD833D1259E7826D6272BFE7B30E4F43B0
SHA-256:	5692791A3D2B35EA82E334BB5E80C1701A8D9B1CC9E87A152659383888E6EE08
SHA-512:	CF8B3BE17BFBFB0B384418E1E3E5D2724C428B98F288FCD79645B83FA8A436BFDB4B3A4AC3298E1484361A3A0347B48412CBBC727F8A8C1135F644387C3B801

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6B1D.tmp	
Malicious:	false
Preview:	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.8.1.6.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.E.r.r.o. .d.e.s.c.o.n.h.e.c.i.d.o. .i.n.f.o.r.m.a.d.o. .p.o.r. .N.e.t.A.P.I... .E.r.r.o. .d.e. .s.i.s.t.e.m.a.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e.....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.2.0.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .2...0. .E.n.g.i.n.e.....I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.B.R.O.W.S.E.=.A.b.r.i.r. .o. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .d.o. .[.P.r.o.d.u.c.t.N.a.m.e.]... ..I.D.S._.P.R.E.R.E.Q.U.I.S.I.T.E._.S.E.T.U.P._.I.N.V.A.L.I.D.=.E.s.t.e. .f.i.c.h.e.i.r.o. .e.x.e.c.u.t...v.e.l. .n...o. .p.a.r.e.c.e. .s.e.r. .o. .o.r.i.g.i.n.a.l. .p.a.r.a. .[.P.r.o.d.u.c.t.N.a.m.e.]... .S.e. .n...o. .s.e. .u.s.a.r. .o. .[.S.E.T.U.P.E.X.E.N.A.M.E.]. .o.r.i.g.i.n.a.l. .p.a.r.a. .i.n.s.t.a.l.a.r. .d.e.p.e.n.d...n.c.i.a.s. .a.d.i.c.i.o.n.a.i.s.,. .o. .[.P.r.o.d.u.c.t.N.a.m.e.]. .p.o.d.e. .n...o. .f.u.n.c.i.o.n.

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5560.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1432832
Entropy (8bit):	6.450183155296358
Encrypted:	false
SSDEEP:	12288:DyIspJCPtjvntnSb8COevQonCLPubu76R7:DLsDCPtjvntnSb8COevQonC3+R7
MD5:	CD76B0EE50AD6DCE22DC8D788F5E1766
SHA1:	4E41CE3DE7FED1EE21E7D7075ADE58B2C41EE798
SHA-256:	32C91742D14671451B165B00D85D9BCCEA7A37EA138EA2550F1E4543906944E6
SHA-512:	1C5903D2B21061E0651475B62219AE3164428D77A348E51E4B04328E8683E7CA36D6BB39F758B41A1DBDF0477508E96349374AAB6D8B5B1B0A9307F8AE480B68
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@.....P.....;^.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is55FE.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.560293282221256
Encrypted:	false
SSDEEP:	12288:xyIapJCPtjvntnSb8COevQonCLPubu791:xLaDCPtjvntnSb8COevQonC3h1
MD5:	721FB29713080245684C8D5F7EB3ED21
SHA1:	E9404840900044E2124882008F48C5CD12951DE6
SHA-256:	DB11F22F90110D5610434739DA084BA377BEE08566BFCD0C5C186C8A01F8CCBC
SHA-512:	81DC39DAF4C0FED935542E415F80F9012008A73024A0EFE0BD39934C837EB5789BB5970A0D3780BA9D67152087AFB0735292F3683D65FB8A788991F2FD0C80DD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@...P.....P.....Z.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... ...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5758.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1432832
Entropy (8bit):	6.44446385785103
Encrypted:	false
SSDEEP:	12288:LyI5pJCPtjvntnSb8COevQonCLPubu7YL:LL5DCPtjvntnSb8COevQonC3EL
MD5:	C9F769E50CFD7FA59C1010D1124CF664
SHA1:	02398AFEDFC4824D97B263EB8FC7DDD8A52DE22F
SHA-256:	4F741EF0EB097DF3719431C016DED31B499F71E61FA9E45234FDB23C4BCC56BC
SHA-512:	0FA3CEC0C93DD0CE0BDFFD388205B8FE7E1B162DEB029D9865D415AD1130A2E60B3A20C9D7055FD52E94FD17D4F2AFA413DD9C75827FA991367BBE89DBBBC 959
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L...r.yY.....!.....@.....P.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is57C7.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1416448
Entropy (8bit):	6.464456578512818
Encrypted:	false
SSDEEP:	12288:6yIWpJCPtjvntnSb8COevQonCLPubu79+rpdT:6LWDCPtjvntnSb8COevQonC3Z+rpdT
MD5:	D9C32D0F07E68B978E9C589945001A16
SHA1:	2325889A15F38A6665F7EDA61A6E881B6A11F132
SHA-256:	B4159D9D8B3B144E3F262B2C93E2D2BFEA95B2C4BDD52DA13A0BA002B6B9C26B
SHA-512:	E814234F9EEC63F9B8E2C4E0E740F9F1EF2BD21B521967AFD4D7789196736CBD1C97587CF0AFB18F227B8613A71AD06378B0917F2792EB2FB503AA1BEDA99BD8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L...u.yY.....!.....@...@.....P.....V..(.....p.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc.....p... ...`.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5827.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1432832
Entropy (8bit):	6.449034862379667
Encrypted:	false
SSDEEP:	12288:IyIKpJCPtjvntnSb8COevQonCLPubu7gDx:ILKDCPtjvntnSb8COevQonC3UDx
MD5:	81530086EA62B38C00AD0AD1BB608F88
SHA1:	9EFCBC817DA901D39030893B9F5524FAB1A4F3CC
SHA-256:	BA803C78AC63A2353DE986AEB528CC2AC251712C3B3826B5A892A2400078B863
SHA-512:	60CF62AFC7324774A8E8FACAF935B0FB0CD621821AAFF1403C90515EBC818CCC63999736339CBE4AB40A97ACE61254C8B875F11B6EEA2242EF5CAE536298770
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@.....P.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5896.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.471998519259824
Encrypted:	false
SSDEEP:	12288:YyIFpJCPtjvntnSb8COevQonCLPubu7aN:YLFDCPtjvntnSb8COevQonC3+N
MD5:	570B0E3A2C9CA9497843E22CF4F281DC
SHA1:	79CE61360451547B3B42B0558151D4996D5BBE72
SHA-256:	788AD433D6DA5C6218C7079D58AD7BC818F43463FF6ADC8AF119A2E21DB3AF5B
SHA-512:	4C3D82592992B201F4D5840947293B01B3ABAB5C0FC36470BC35D12F591D3E5F02EBF12772D9E8268F17D4B9C9EC69AED45207283DE06383C38FC3F8F57C1F3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L...y.yY.....!.....@...P.....P.....V..(.....x.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...x.....@..@.reloc..... ...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is58F6.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.46137601862
Encrypted:	false
SSDEEP:	12288:zyIoLpJCPtjvntnSb8COevQonCLPubu7mq:zLoLDCPtjvntnSb8COevQonC36q

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is58F6.tmp	
MD5:	14934B54E6DD7AE9F7C9AC006305671A
SHA1:	C6C3CFE0AA036E32626CD802EE402F459C1FF2F2
SHA-256:	2DA5CD58D3B4701EBC73C987C1E87DB111DC9F40C833B586CBF01D0D0243ACF3
SHA-512:	2F3E20D9E0DD422BC05ADA557FAF6A63D32F965F5D4C23766CE8BCD0A7A6E900422D899B62EE76853A76334B27BC6D081AE0E358814C952C1E0012EBBB048C1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@...P.....P.....W.....V..(.....P.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...P.....@..@.reloc..... ...p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5994.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.467479267856592
Encrypted:	false
SSDEEP:	12288:3yIEpJCPtjvntnSb8COevQonCLPubu7Rh:3LEDCPtjvntnSb8COevQonC3lh
MD5:	1D3FD400FA8F1F9818EB71870AF6B2FD
SHA1:	DEA1FA580E28427CBB9B8F0E45AA025760C76D45
SHA-256:	695E55D535BC96C72D6929EAC47386743468D756D72CFB58093FB29DC6481E73
SHA-512:	089FC766506D5F06842068AED3EAF7DAC2FEC4859A5EE0F6D5B490F5B969DF56FE0893850D07EC19B53A30AD7F2BB1B6A376EBEF037C3061CC33CBD54F893A1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@...P.....P.....V..(..... .....P..... .text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc... .....@..@.reloc..... ...p.....@..B..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is59F4.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1416448
Entropy (8bit):	6.465632629662606
Encrypted:	false
SSDEEP:	12288:2yIZpJCPtjvntnSb8COevQonCLPubu74t:2LZDCPtjvntnSb8COevQonC3st
MD5:	DA9F99CA15A1EA4498971E75A471C5B4
SHA1:	A74A240EB87C49FD92CE6889429C1EF21A15F1BD
SHA-256:	83371792C3FCA7461CD48AA90B86EC52B4F43F44B99CA6B870796C71DE32C30E
SHA-512:	DD23DB976B9589F2A5449B68D327DBE0BF2911A1F125E3242AC9F9B97841CE1024D2FF072E970100C6D1869C4F784AFC8E98F977C105DDB41DABDBEFA2C427D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@...@.....P.....:.....V..(.....p.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc.....p... ...`.....@..B..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5B8C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1416448
Entropy (8bit):	6.585466383792146
Encrypted:	false
SSDEEP:	12288:GyIupJCPtjvntnSb8COevQonCLPubu7BWs:GLuDCPtjvntnSb8COevQonC3VWs
MD5:	60FB86CF64CEA5D9D0B24111E352941A
SHA1:	1D4F5B0CB55B6BEBCD1CA86E8FF1364F41137993
SHA-256:	FAEF7ABAF313762324909FF104DF9F54CA3CA03E365B6F5592A662B8FBC50294
SHA-512:	56906F6157D1EEAF7E91C6320DB35E48583E8E5CB7370F723B51DBBE498BFDA5E912C86FE88F684EBBA945195968513A97D385DCA46712AFAA33D3ED9EF5D530
Malicious:	false

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5B8C.tmp	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5.....7...Rich6..... ...PE..L.....yY.....!.....@...@.....P.....V..(.....p.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc.....p... ...`.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C1B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1416448
Entropy (8bit):	6.475657915504315
Encrypted:	false
SSDEEP:	12288:9yIapJCPtjvntnSb8COevQonCLPubu7Vyv0k:9LaDCPtjvntnSb8COevQonC3Hk
MD5:	4840C2447975B7BF9EA3A422C83491BB
SHA1:	8035BC050A0F168654578F8A772FBA8B872C4CFB
SHA-256:	40DA10E2A79F7B8FDA6AB8D54D626555EF9C3592428ED9C5C687ED09AD630466
SHA-512:	9CCDE09598FC95E55B165E502A3CFAAC78DFECE727F90E63583A0FFDECE669065DF30878CE21F635B1B48CD318EEF809DB2FB9638F5A654878E20617298755C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5.....7...Rich6..... ...PE..L.....yY.....!.....@...@.....P.....V..(.....P.....p.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...P.....@..@.reloc.....p... ...`.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C8A.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.460063429651935
Encrypted:	false
SSDEEP:	12288:UyITpJCPtjvntnSb8COevQonCLPubu7C7:ULTDCPtjvntnSb8COevQonC3G7
MD5:	D4C06AD994D95F4EF4D6D6470A1651ED
SHA1:	6ACBBF16499E6DB0793854C1B99D04EEC582CD29
SHA-256:	B1F411B68CBE57EBBCC223017249AC4623F00CF19DE4294EF4E5D7DC657F7CC4
SHA-512:	92678F30A723F158AF852C56CA7747F84F506FAA33E31713C144BC9884C2BE56936F9B54726780D96A4E0C77BD043859D9E9395977BDF046AD412447B5214166
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5.....7...Rich6..... ...PE..L.....yY.....!.....@...P.....P.....V..(.....x.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...x.....@..@.reloc..... ...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5CEA.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1424640
Entropy (8bit):	6.564955152994468
Encrypted:	false
SSDEEP:	12288:9yIspJCPtjvntnSb8COevQonCLPubu7MY:9LsDCPtjvntnSb8COevQonC3gY
MD5:	745EE4446117B55785F92E972E552A2E
SHA1:	16014E4691C2E7EB2454F323B72B2CDD0D36D6B0
SHA-256:	FFA7CF1E056B0F9F881BF5AA035B2E6F241E9A6E5BE3B2807AB458EF061D7E30
SHA-512:	4C32CF81D0B5466B652EC03D68CA0CA8C7019A741958C474E76C75CE5DECFA9114522CB10B8BA8F5A840156AAE65D7E197B56AC772E9759C088FF7628BC271A 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5.....7...Rich6..... ...PE..L.....yY.....!.....@..`.....P.....R.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5D4A.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5D4A.tmp	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1428736
Entropy (8bit):	6.451397234248691
Encrypted:	false
SSDEEP:	12288:ayIIpJCPtjvntnSb8COevQonCLPubu7T0:aLIDCPtjvntnSb8COevQonC3P0
MD5:	BB0D273CA35C9011A7E10E1B5EDCE27F
SHA1:	96E684B6790E9977CB76D7CE8F50EA65F14E4FDF
SHA-256:	9BEC0617B1DD5088DE564234A1AFD28D0B5F2CD0577627A1FC9AB40CED323D45
SHA-512:	D160D95325D382F7F8D1C33B0589C90E1CD42E2A3416DE1F76CD4BDE51C8AD2C66ACB7D2217B7B546AA73B22E4485CCD36DB88523576D53206E22BB59D3BA 7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L...`.yY.....!.....@...p.....P.....fq.....V..(.....X.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...X.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5DE8.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1367296
Entropy (8bit):	6.559069593802875
Encrypted:	false
SSDEEP:	12288:VyIEpJCPtjvntnSb8COevQonCLPubu74dhxk:VLEDCPtjvntnSb8COevQonC3Ok
MD5:	030F8C1384243570A67F72E644703049
SHA1:	6CD81F58E773560CEE31D10699BAFACD10B97896
SHA-256:	38443E36A9AFEA135C2501653DD599248DF8D7433EC5DE52A2A505AD5E983560
SHA-512:	CD3276A3A1ACFBFE98DB697ED583F0661BB78D36D1D615E145A498C637F1C5090A126267789E80D21B508873BAE332277AA152993B60142E04E588F86F4BCB53
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L....yY.....!.....@.....P.....S.....V..(.....8.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...8.....@..@.reloc..p..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is61D2.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1416448
Entropy (8bit):	6.475370549575337
Encrypted:	false
SSDEEP:	12288:AyIPpJCPtjvntnSb8COevQonCLPubu7hp4h:ALPDCPtjvntnSb8COevQonC3gh
MD5:	06C64C6119B5D8C81F1A70FDA9F3C4F7
SHA1:	0C0A76A48EAAB2466357651E601F871C8BBD7830
SHA-256:	ACC5EFAAD2EEE18DEA7F1AA130E198564860E9D89AD69E6FDF7BC40A61C49E42
SHA-512:	6FBC0129B74A2F25A012643FF40B9A0D02973D6B0AC03AAF201393505D6A6665A3280851EEBC3C318E8C7DB25E396A2025FBBBFBE7BC18709F1037D7BB0EED8 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L...a.yY.....!.....@...@.....P.....@.....V..(.....p.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc.....p... ...`.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6270.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.4604608790360265
Encrypted:	false
SSDEEP:	12288:NyIcpJCPtjvntnSb8COevQonCLPubu7hV:NLcDCPtjvntnSb8COevQonC3VV
MD5:	21A509036A1F5F9DA32824A72BC21523

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6270.tmp	
SHA1:	0568D0625DF21B50A958BFF26BAA187E35F95DA6
SHA-256:	61B09BE71B66D53A372A5C7E3F405FEDEFE5ED754916C811D699FF3D72AD7DB6
SHA-512:	892BE8E5D4BC16481D18C62728CA8B4865A972C5EE3D6A7DA6B1C28561820F515A0F1546D7323F4A701FFBD3EA7D03B443989046FED4DCCFA07183AF29A5DF 2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L...f.yY.....!.....@...P.....P.....".....V..(.....`.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...`.....@..@.reloc..... ...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is632E.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1432832
Entropy (8bit):	6.443315775449897
Encrypted:	false
SSDEEP:	12288:CyIXpJCPtjvntnSb8COevQonCLPubu7q64:CLXDCPtjvntnSb8COevQonC3e64
MD5:	701432D28B4BF6997365480461BD694F
SHA1:	52487E31E0BE8041D9E745BA991CC6648BC4B301
SHA-256:	58FE405AF724A2A24969AD68517B01FEEA45E7012345438C24421C6CBF4AC110
SHA-512:	5C579E93F11E2BB0C2744761FE7DE172CE3452C52A25125803E6489D2F9EAFCD0EDA9EA373621565589B6B5742F388667FA5A2451AFE9C0756A50768EB7E8F52
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L...l.yY.....!.....@.....P.....4A.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is636E.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1432832
Entropy (8bit):	6.545845810539532
Encrypted:	false
SSDEEP:	12288:iyIVpJCPtjvntnSb8COevQonCLPubu79d:iLVDCPtjvntnSb8COevQonC3Zd
MD5:	6FC83CCDC28F4ED74FA61CA181DCE654
SHA1:	3C08CBDD5827BEE4D21AACDB3AA5F9BACE06F260
SHA-256:	8E519077CC53112B80799A85DF185564905A1D0A3CD69CFD2E1D45832F326994
SHA-512:	9F73CED928492DEFCEF4BFCBA98E2AF8615DE42EED467A3154E859B167AE2D193E2C095A5B677333B25365AABE937825E418B4CCDD62819A74AA9FA949CF63 22
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L...p.yY.....!.....@.....P...../D.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is63FD.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1863024
Entropy (8bit):	5.68804336966568
Encrypted:	false
SSDEEP:	12288:zs4d9dfaOdWUIhpJCPtjvntnSb8COevQonCLPub+7iqm:ThrWVhDCPtjvntnSb8COevQonCfrm
MD5:	D9C3BC738104B03B367E2C6ACF8FAFBF
SHA1:	EB7197EB446A5831F99661E021921896B98DC2E2
SHA-256:	F5FD2D49A163D35E4D8FB90C5BCD59CD4BF19B77B5A6F0C36580B7A25A9E75FE
SHA-512:	93F7B899DB22023049E028ABDAE3CD2FB9067E0A9F4EF28E82DE90CA573B85B7B42F1303515E6563C2CB48860F1F282EE108B43612E12221F4EF16AB29FE2437
Malicious:	false

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is63FD.tmp	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^..(...{...{...{...{...{...{J..{...{P..{...{...{...{...{...{Rich...{.....PE..L... [.yY.....!.....p.....O.....@..(....P..V.....pP.....@.....A.....text. ..@..... ..`.rdata..... .....@..@.data....f.....P.....@....idata.....@..... .....@....rsrc...V....P.....0.....@..@.reloc...)...@...0.. ....@..B.....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is646C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1424640
Entropy (8bit):	6.458123690535173
Encrypted:	false
SSDEEP:	12288:ByIrpJCPtjvntnSb8COevQonCLPubu7A5k:BLrDCPtjvntnSb8COevQonC3k5k
MD5:	BB84615532980AD38E781744D6AD4215
SHA1:	A29A71F1BA7F470933F4EAFACFDD11924B636213
SHA-256:	4309C1A2181081DE7113F2956D038043F99C25C05573686243F0D5A9C4BDA8A4
SHA-512:	D6DDA0FCA6EDD0D3CF10FFB1167E523019D9DE40066987B99D031E06B8DE92571CEE9F898BC86E748BF3C989CF6EDB39934D7E3EBF0A161EE3E4BBB168C55 1D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@...`.....P.....y.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is64CC.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1387776
Entropy (8bit):	6.557180411066131
Encrypted:	false
SSDEEP:	12288:myI3pJCPtjvntnSb8COevQonCLPubu7Gg:mL3DCPtjvntnSb8COevQonC3Sg
MD5:	0F14422D86948CC1F7434A678221005D
SHA1:	E3E057850E3EE2D3AA57B6DA7CD9B3C149E5E4CC
SHA-256:	E4902E52BD344150622B6F50AD2EF0C58BD3A86476325E1D9244204D02C7191F
SHA-512:	FA53F58DFFB69A0A876C299D255E4BFA029A04E3A1BF1DCC2EF8A3FE51EFD073981D62058EC57D1BD9B011EFD545639F4ADB8FCB5165E02399852CCA9024FB D4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@.....P..... .....V..(.....pU.....P..... .text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...pU.....`.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is656A.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1379584
Entropy (8bit):	6.572389836216373
Encrypted:	false
SSDEEP:	12288:KyIOpJCPtjvntnSb8COevQonCLPubu7Ed:KLODCPtjvntnSb8COevQonC3gd
MD5:	F267C3DCD41D4B7969E8E5B422CBF206
SHA1:	951474BEDF04961934722997F10D1770D9D567AB
SHA-256:	0DE20F94CE658FDFD4F4C808D821A7ADC58BB1CC471A36E311D7FD1231A3584D
SHA-512:	C8E206CA6D8B8285BBCD17827E35453640ECEDD3E1F05D0AE22F097FE3E561DC04DD675DE9CE0AECF3007DD8C62DDC23C31E4B1CE0080996D7CAA2125937 3AE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@.....P.....V..(.....<.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc....<.....@.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is65CA.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1424640
Entropy (8bit):	6.456823380709671
Encrypted:	false
SSDEEP:	12288:oyIDpJCPtjvntnSb8COevQonCLPubu78C:oLDDCPtjvntnSb8COevQonC3AC
MD5:	C2E3F6A7F78B7AF7D83A49C8DE07FE02
SHA1:	1E8755A5E4CB433A874E1159ECCEFE99E5F78E76
SHA-256:	AD24853D5F2D5C88777F955FD84BE0F8F76D5369972DBD7EF23B21BCA176D266
SHA-512:	DCD9DE3272C74EEC64C5C3D8EA4238A1E66EB0CAC0A5A7EF85003FC9C3C479E8CEB3856587A23888746CADDF260111227D64E8958B08D3E29CE134279E494C 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..... .6...w.....5.....5....7...Rich6..... ...PE..L....yY.....!.....@...`.....P...../.....V..(.....H.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...H.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6668.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.458365440906146
Encrypted:	false
SSDEEP:	12288:cyIWpJCPtjvntnSb8COevQonCLPubu7Bj3:cLWDCPtjvntnSb8COevQonC3d3
MD5:	35AE94CD1BF2864C640176A6046A5C0C
SHA1:	16009CCC8F3F8F3D1879F8373AFE93C1AF5DA629
SHA-256:	DD92BF15CD0229EAC0E938EDB0CD0D1F15B517BC1E1179F5047A7EA87975BE6D
SHA-512:	6E0E3856AD9E20DAD413653AF9A578E17B37C0610D10E93B39B1FA658ECAFA7FF830930CD5D8361C81D66205B771F21880483254ECF9EF74CE230C281FABD08
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..... .6...w.....5.....5....7...Rich6..... ...PE..L....yY.....!.....@...P.....P.....V..(.....P.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc...P.....@..@.reloc..... ...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is66F7.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1424640
Entropy (8bit):	6.459431156458696
Encrypted:	false
SSDEEP:	12288:JyIcpJCPtjvntnSb8COevQonCLPubu7r0:JLcDCPtjvntnSb8COevQonC3P0
MD5:	0131ED35F5C407F5E5A6F5318DAF61DC
SHA1:	7F17C8345942B466E504490975E5EF019DEEBEDB
SHA-256:	E4E9876D9B1E9FF8E86A56FC5AAB3CDE617F7054DA7E667E2753F66271664717
SHA-512:	48026E421AD93E190FA6376CA2BE2C424C55BC8977B7814313B944532BF0B33A289C6A0746435BD151A09940C9C49FD93DEC4290EDD85ABC1271E715538DFDD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..... .6...w.....5.....5....7...Rich6..... ...PE..L....yY.....!.....@...`.....P.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6766.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1424640
Entropy (8bit):	6.4540275232225355
Encrypted:	false
SSDEEP:	12288:/yIKpJCPtjvntnSb8COevQonCLPub+7Aw:/LKDCPtjvntnSb8COevQonCfkw
MD5:	223F0CDA7C6BE8F0E861000D9BEB032E

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6766.tmp	
SHA1:	589DBA0092F732A4427389B8ACB0C2B7D9F6E301
SHA-256:	3281FD0BF396B4B12E91EA19764CD1042A1947A0EFC72C753A962E461FCFBBC0
SHA-512:	7BA24EE4A40B657C8E2FE93385140443FA049E36B3CD7CC422ED42D6CEAB3AB533353B0F27C234B5819755E65D1E068D45999448A9B83D6F43A2A2C379289591
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@...`.....P.....^.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6824.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1428736
Entropy (8bit):	6.447744240413919
Encrypted:	false
SSDEEP:	12288:cyIgpJCPtjvntnSb8COevQonCLPubu7z7:cLgDCPtjvntnSb8COevQonC3f7
MD5:	9FDFCCAC597E3AC1AFE41871614FD479
SHA1:	AB6B0ED43A70959B956038841A41A1B0DE578B16
SHA-256:	092C70260132E7F4411F0874D910CB44DE8B930205FD1670E83B54D107EBB462
SHA-512:	2DF9BB7D2F45495BF92D145C4DF6E0C87FC592B2DF432E5D2F50CD6993BE9D844B081279675102FE4A3DB1ED9A8AA9C74095E05FF8E882DAB30A87D5D2B2BF 0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@...p.....P.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6893.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.566543446724177
Encrypted:	false
SSDEEP:	12288:SyIIpJCPtjvntnSb8COevQonCLPubu7Q+:SLIDCPtjvntnSb8COevQonC3s+
MD5:	1485AB9FE9CED95744AA0E53E00EA61B
SHA1:	62FFC621F13EA08468553365705AC945863233BD
SHA-256:	89441DC6F4528B9454F3913FAA9802307AA8093A11A0A97ECC656FADEC2A6E86
SHA-512:	75E715A6204641D477B73A8A306B2C929886CF3B1F6119B9B76F13678CEB9D7FF704BD24B9F480551EC200C7CAF7F50F98DDE57DC3B02F7B09DEADCA47D843A B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6.....".....6...w.....5.....5....7...Rich6..... ...PE..L.....yY.....!.....@...P.....P.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... ...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6922.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.460642297632325
Encrypted:	false
SSDEEP:	12288:oyIVpJCPtjvntnSb8COevQonCLPubu7MJ:oLVDCPtjvntnSb8COevQonC3lJ
MD5:	B96E8269F6840266DD1D616A895979BA
SHA1:	614439FB7E9DAE3DBA8A789833A40CDF27623101
SHA-256:	C1DE28ECA51C2274334435E7B114EB597CB368233B39E92FDC87BA7F27705325
SHA-512:	C4EF55CCFFD4573CF18F4B003105E76E63592B49DE50098EB963E672E196606C8BB3927B5D26F122BC88EFBD65A500F302AAC7246E9B01636247C158F7783618
Malicious:	false

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6922.tmp	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5.....7...Rich6..... ...PE..L.....yY.....!.....@...P.....P.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... ...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is69C0.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1420544
Entropy (8bit):	6.465918679261405
Encrypted:	false
SSDEEP:	12288:kyI2pJCPtjvntnSb8COevQonCLPubu7Vkj:kL2DCPtjvntnSb8COevQonC3Cj
MD5:	CA1D993432BF00141FEB87D459679FC1
SHA1:	109C9A324600DE88B9B517BEC62175BCC97307E7
SHA-256:	53CB769D6612161634C08A8D1CAB58489CE3FA1219EE7198F3857B7FAF224385
SHA-512:	1A33F4EE2DA274E794DA553EA72F61A96534B35E683099FDE0AC84F97E54BEBCF84851ED78F99460817946617656A8751C6C0F9714855C1FD37C09D8DB5CBC1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5.....7...Rich6..... ...PE..L.....yY.....!.....@...P.....P.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... ...p.....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6A20.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1367296
Entropy (8bit):	6.556230678083565
Encrypted:	false
SSDEEP:	12288:QyIlpJCPtjvntnSb8COevQonCLPubu7xhCoM:QLlDCPtjvntnSb8COevQonC3NhCoM
MD5:	10DE879EA38823729653D91907F4DF49
SHA1:	443F8C90BD04B749A1B358C5DBF097560FAFBE15
SHA-256:	61C7CCCB9E343A7ADF0E93A556068B1DBAECB7202B9403425100DF3E996F1FCA
SHA-512:	20DB9942D7BDFB70455D866C79B14D6CF705FA421F27FC24CD946D33EF1C36910BE3C913D6B611C4DCBDF0F1216A143B2C3B37E4BCFC506EEE2F9CBCD448A D6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5.....7...Rich6..... ...PE..L.....yY.....!.....@.....P.....'.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..p..... .....@..B..... ....

C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6ABE.tmp	
Process:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1428736
Entropy (8bit):	6.456695021897723
Encrypted:	false
SSDEEP:	12288:VyILpJCPtjvntnSb8COevQonCLPub+7Ml:VLLDCPtjvntnSb8COevQonCfwl
MD5:	E4D7DD41D2F3FA29A82660A3A6F89190
SHA1:	584E0B8FD1EFB2A22FCE28D02F3B835C9F223E97
SHA-256:	EAEDEC4D9F0769765D24D84945C948CA468813414B4A4811C50F28380392FB2A
SHA-512:	C647919B1FCBDEEC5ACC25724694414A930EEB9EAF599319B8DD8ABA4DF3DCE999537660EFB34E433E5EF0B40416F79BFF79DD1EEB90838348490B154554BA B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...6...6...6....."..........6...w.....5.....5.....7...Rich6..... ...PE..L.....yY.....!.....@...p.....P.....V..(.....P..... ..text...Z?.....@..... ..`.rdata.....P.....P.....@..@.data... 1...`...0...`.....@....rsrc.....@..@.reloc..... .....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.955804644263245
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
File size:	26675560
MD5:	e1c700344a31aee275b86a0cc5fe707b
SHA1:	e1ca62a65559a00eac9096f7b1e0de69d82fd0c8
SHA256:	fa07eeabe6dc625c92894a62137f8c2cfb445b8e3daddd19ee3c44c00a84a708
SHA512:	2868da24290c51bfdfabce9c7523e6c5d717d387d21b5e71ccc6b2695f897a0e0b7227abb2b82625258fb8e521381ab57182e4e40a6ba5aa240842658f1a8b78
SSDEEP:	786432:ak/XpsaOs3VSCyZ6a4oo/OGHRSgWd/tOiHQ6nZWsnTrcfZ+iFpMwHw/J6:ak/XpsaOs3VSCyZ6a4oo/OGHRSgG/tOR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^y....s...s...s.....s.....s.....s.....s.....Z.s..o....s...r...s..o....s.....7.s.....s.....s.....s.Rich..s.....

File Icon

Icon Hash:	0063551165753100

Static PE Info

General

Entrypoint:	0x45e61f
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5979D664 [Thu Jul 27 12:02:44 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	952608687d343553fa2ebbe1a801044c

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=Symantec Class 3 SHA256 Code Signing CA, OU=Symantec Trust Network, O=Symantec Corporation, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 6/22/2016 2:00:00 AM 7/23/2019 1:59:59 AM
Subject Chain	• CN=Automationdirect.com, O=Automationdirect.com, L=Cumming, S=Georgia, C=US
Version:	3
Thumbprint MD5:	F4F931C45F2EB68904EC3E0CA08B9567
Thumbprint SHA-1:	3B2E79F2DA570A8C20BB6E30B31E2EFBCB588D1B
Thumbprint SHA-256:	4EFA0B423F04D38D58D3E46D4A6CDB5D9C92027E4EC89B8F5C82D9A8AE4D3FBA

Serial:	6872DC611BBCFB37A8E37BA86F3198B2

Entrypoint Preview

Instruction
call 00007F6D30A3877Fh
jmp 00007F6D30A2AB6Eh
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+14h]
push esi
test eax, eax
je 00007F6D30A2AD6Eh
cmp dword ptr [ebp+08h], 00000000h
jne 00007F6D30A2AD45h
call 00007F6D30A29BFCh
push 00000016h
pop esi
mov dword ptr [eax], esi
call 00007F6D30A317C2h
mov eax, esi
jmp 00007F6D30A2AD57h
cmp dword ptr [ebp+10h], 00000000h
je 00007F6D30A2AD19h
cmp dword ptr [ebp+0Ch], eax
jnc 00007F6D30A2AD3Bh
call 00007F6D30A29BDEh
push 00000022h
jmp 00007F6D30A2AD12h
push eax
push dword ptr [ebp+10h]
push dword ptr [ebp+08h]
call 00007F6D30A27658h
add esp, 0Ch
xor eax, eax
pop esi
pop ebp
ret
push ebp
mov ebp, esp
xor edx, edx
mov eax, edx
cmp dword ptr [ebp+0Ch], eax
jbe 00007F6D30A2AD43h
mov ecx, dword ptr [ebp+08h]
cmp word ptr [ecx], dx
je 00007F6D30A2AD3Bh
inc eax
add ecx, 02h
cmp eax, dword ptr [ebp+0Ch]
jc 00007F6D30A2AD24h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
mov ecx, dword ptr [esp+0Ch]
push edi
test ecx, ecx
je 00007F6D30A2ADC8h
push esi
push ebx
mov ebx, ecx
mov esi, dword ptr [esp+14h]
test esi, 00000003h
mov edi, dword ptr [esp+10h]
jne 00007F6D30A2AD3Dh
shr ecx, 02h
jne 00007F6D30A2ADBBh
jmp 00007F6D30A2AD59h
mov al, byte ptr [esi]
add esi, 01h
mov byte ptr [edi], al
add edi, 01h
sub ecx, 01h
je 00007F6D30A2AD5Dh
test al, al
je 00007F6D30A2AD61h
test esi, 00000003h
jne 00007F6D30A2AD17h

Rich Headers

Programming Language:	• [RES] VS2012 UPD1 build 51106 • [C++] VS2012 UPD1 build 51106 • [C] VS2012 UPD1 build 51106 • [LNK] VS2012 UPD1 build 51106

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd420c	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xdc000	0x4c600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x196ec58	0x1d10	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0xae700	0x38	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xc3478	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xae000	0x674	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xd3a48	0x120	.rdata
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	0xac3bb	0xac400	False	0.471233218433	data	6.54203736845	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xae000	0x2850e	0x28600	False	0.424596071981	data	5.1940985024	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xd7000	0x4c24	0x2600	False	0.292249177632	PGP symmetric key encrypted data - Plaintext or unencrypted data	4.51395817046	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xdc000	0x4c600	0x4c600	False	0.359125664894	data	6.52947632143	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
GIF	0xdcf04	0x339f	GIF image data, version 89a, 350 x 624	English	United States
PNG	0xe02a4	0x39ed	PNG image data, 360 x 150, 8-bit/color RGBA, non-interlaced		
PNG	0xe3c94	0x2fc9	PNG image data, 240 x 227, 8-bit/color RGBA, non-interlaced		
RT_BITMAP	0xe6c60	0x14220	data		
RT_BITMAP	0xfae80	0x1b5c	data		
RT_BITMAP	0xfc9dc	0x38e4	data		
RT_BITMAP	0x1002c0	0x1238	data		
RT_BITMAP	0x1014f8	0x6588	data		
RT_BITMAP	0x107a80	0x11f88	data		
RT_ICON	0x119a08	0x668	data		
RT_ICON	0x11a070	0x2e8	data		
RT_ICON	0x11a358	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x11a480	0xea8	data		
RT_ICON	0x11b328	0x8a8	data		
RT_ICON	0x11bbd0	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x11c138	0x25a8	data		
RT_ICON	0x11e6e0	0x10a8	data		
RT_ICON	0x11f788	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x11fbf0	0x2e8	data		
RT_ICON	0x11fed8	0x2e8	data		
RT_ICON	0x1201c0	0x2e8	data		
RT_DIALOG	0x1204a8	0x1ce	data		
RT_DIALOG	0x120678	0x266	data		
RT_DIALOG	0x1208e0	0x2b0	data		
RT_DIALOG	0x120b90	0x54	data		
RT_DIALOG	0x120be4	0x34	data		
RT_DIALOG	0x120c18	0xd6	data		
RT_DIALOG	0x120cf0	0x114	data		
RT_DIALOG	0x120e04	0xd6	data		
RT_DIALOG	0x120edc	0x246	data		
RT_DIALOG	0x121124	0x3c8	data		
RT_DIALOG	0x1214ec	0x14e	data		
RT_DIALOG	0x12163c	0x1e8	data		
RT_DIALOG	0x121824	0x1c6	data		
RT_DIALOG	0x1219ec	0x1ee	data		
RT_DIALOG	0x121bdc	0x7c	data		
RT_DIALOG	0x121c58	0x3bc	data		
RT_DIALOG	0x122014	0x158	data		
RT_DIALOG	0x12216c	0x1da	data		
RT_DIALOG	0x122348	0x10a	data		
RT_DIALOG	0x122454	0xde	data		
RT_DIALOG	0x122534	0x1d4	data		
RT_DIALOG	0x122708	0x1dc	data		
RT_DIALOG	0x1228e4	0x294	data		
RT_STRING	0x122b78	0x160	data	English	United States
RT_STRING	0x122cd8	0x23e	data	English	United States
RT_STRING	0x122f18	0x378	data	English	United States
RT_STRING	0x123290	0x252	data	English	United States
RT_STRING	0x1234e4	0x1f4	data	English	United States
RT_STRING	0x1236d8	0x66a	data	English	United States
RT_STRING	0x123d44	0x366	data	English	United States
RT_STRING	0x1240ac	0x27e	data	English	United States
RT_STRING	0x12432c	0x518	data	English	United States
RT_STRING	0x124844	0x882	data	English	United States
RT_STRING	0x1250c8	0x23e	data	English	United States
RT_STRING	0x125308	0x3ba	data	English	United States
RT_STRING	0x1256c4	0x12c	data	English	United States
RT_STRING	0x1257f0	0x4a	data	English	United States
RT_STRING	0x12583c	0xda	data	English	United States
RT_STRING	0x125918	0x110	data	English	United States
RT_STRING	0x125a28	0x20a	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x125c34	0xba	data	English	United States
RT_STRING	0x125cf0	0xa8	data	English	United States
RT_STRING	0x125d98	0x12a	data	English	United States
RT_STRING	0x125ec4	0x422	data	English	United States
RT_STRING	0x1262e8	0x5c2	data	English	United States
RT_STRING	0x1268ac	0x40	data	English	United States
RT_STRING	0x1268ec	0xcaa	data	English	United States
RT_STRING	0x127598	0x284	data	English	United States
RT_GROUP_ICON	0x12781c	0x14	data		
RT_GROUP_ICON	0x127830	0x14	data		
RT_GROUP_ICON	0x127844	0x14	data		
RT_VERSION	0x127858	0x45c	data		
RT_MANIFEST	0x127cb4	0x626	XML 1.0 document, ASCII text, with CRLF line terminators		
RT_MANIFEST	0x1282dc	0x323	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

DLL	Import
COMCTL32.dll	
KERNEL32.dll	IsBadReadPtr, CompareStringW, CompareStringA, GetSystemDefaultLangID, GetUserDefaultLangID, ExpandEnvironmentStringsW, GetCurrentDirectoryW, FileTimeToLocalFileTime, GetFileTime, SetFileAttributesW, HeapAlloc, HeapFree, GetProcessHeap, CopyFileW, GetWindowsDirectoryW, InterlockedDecrement, InterlockedIncrement, GetTempPathW, CreateFileW, LoadLibraryA, GetSystemDirectoryA, FindResourceW, GlobalFree, GlobalUnlock, GlobalLock, GlobalAlloc, GetPrivateProfileIntW, LockResource, LoadResource, MultiByteToWideChar, MoveFileExW, WriteProcessMemory, VirtualProtectEx, GetSystemDirectoryW, FlushInstructionCache, SetThreadContext, GetThreadContext, ResumeThread, TerminateProcess, ExitProcess, LoadLibraryW, lstrcatW, lstrcpynW, lstrcmpiW, LoadLibraryExW, FreeLibrary, FindResourceExW, UnmapViewOfFile, MapViewOfFile, CreateFileMappingW, VirtualQuery, GetSystemInfo, GetSystemTimeAsFileTime, CreateEventW, CreateMutexW, ReleaseMutex, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, QueryPerformanceFrequency, SetErrorMode, RaiseException, FreeResource, GetPrivateProfileSectionNamesA, GetPrivateProfileStringA, GetPrivateProfileIntA, lstrcatA, lstrcmpiA, MulDiv, FlushFileBuffers, WriteConsoleW, SetStdHandle, OutputDebugStringW, SetConsoleCtrlHandler, SetFilePointerEx, GetConsoleMode, WriteFile, SetFilePointer, GetFileSize, GetFileAttributesW, GetDiskFreeSpaceExW, GetDiskFreeSpaceW, FindFirstFileW, FindClose, CreateDirectoryW, VerLanguageNameW, IsValidLocale, GetLocaleInfoW, WideCharToMultiByte, lstrcpyA, GetTickCount, ExitThread, CreateThread, GetExitCodeProcess, ReadFile, GetCommandLineW, FormatMessageW, LocalFree, SizeofResource, GetVersionExW, GetCurrentProcess, WaitForSingleObject, SetLastError, GetLastError, DuplicateHandle, RemoveDirectoryW, DeleteFileW, SetCurrentDirectoryW, lstrlenW, lstrcpyW, GetProcAddress, GetModuleHandleW, GetModuleFileNameW, CreateProcessW, Sleep, CloseHandle, GetSystemDefaultUILanguage, ReadConsoleW, GetConsoleCP, EnumSystemLocalesW, GetUserDefaultLCID, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetFileType, HeapReAlloc, GetStdHandle, HeapSize, AreFileApisANSI, GetModuleHandleExW, GetStringTypeW, GetCurrentThreadId, GetCPInfo, GetOEMCP, IsValidCodePage, CreateSemaphoreW, GetStartupInfoW, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, SetUnhandledExceptionFilter, UnhandledExceptionFilter, FatalAppExitA, GetACP, IsProcessorFeaturePresent, IsDebuggerPresent, RtlUnwind, lstrcpynA, LocalAlloc, FindNextFileW, WritePrivateProfileSectionW, GetPrivateProfileSectionW, lstrcmpW, GetShortPathNameW, GetCurrentThread, QueryPerformanceCounter, lstrcmpA, SystemTimeToFileTime, ResetEvent, SetEvent, Process32NextW, Process32FirstW, CreateToolhelp32Snapshot, GetDateFormatW, GetTimeFormatW, GetTempFileNameW, GetEnvironmentVariableW, CompareFileTime, InterlockedExchange, LoadLibraryExA, EnterCriticalSection, LeaveCriticalSection, EncodePointer, DecodePointer, LCMapStringW, GetVersion, GetCurrentProcessId, GetLocalTime, lstrlenA, GetProcessTimes, OpenProcess, SetFileTime
USER32.dll	DialogBoxIndirectParamW, MoveWindow, SendMessageW, CharUpperBuffW, WaitForInputIdle, wsprintfW, GetDlgItem, SetDlgItemTextW, SetActiveWindow, SetForegroundWindow, SetWindowTextW, GetWindowRect, MessageBoxW, GetWindowLongW, SetWindowLongW, LoadIconW, TranslateMessage, DispatchMessageW, PeekMessageW, EndDialog, SystemParametersInfoW, GetWindow, FillRect, GetSysColor, MapWindowPoints, RemovePropW, GetPropW, SetPropW, EndPaint, BeginPaint, EnableMenuItem, GetSystemMetrics, SetFocus, ExitWindowsEx, CharUpperW, wsprintfA, CallWindowProcW, CreateWindowExW, DrawIcon, DrawTextW, UpdateWindow, GetWindowDC, InvalidateRect, DrawFocusRect, CopyRect, InflateRect, EnumChildWindows, GetClassNameW, MapDialogRect, RegisterClassExW, GetDlgItemTextW, IntersectRect, MonitorFromPoint, DefWindowProcW, GetMessageW, LoadStringW, LoadImageW, ReleaseDC, GetDC, CreateDialogParamW, GetParent, GetWindowTextW, CharNextW, GetDesktopWindow, GetClientRect, IsWindowEnabled, CreateDialogIndirectParamW, IsWindowVisible, IsDialogMessageW, FindWindowExW, ScreenToClient, EnableWindow, MsgWaitForMultipleObjects, SendDlgItemMessageW, SetWindowPos, ShowWindow, DestroyWindow, IsWindow, PostMessageW
GDI32.dll	SetTextColor, SetBkMode, SetBkColor, SaveDC, RestoreDC, CreateSolidBrush, UnrealizeObject, CreateHalftonePalette, GetDIBColorTable, SelectPalette, SelectObject, RealizePalette, GetSystemPaletteEntries, GetDeviceCaps, DeleteDC, CreatePalette, CreateCompatibleDC, BitBlt, GetObjectW, TranslateCharsetInfo, DeleteObject, CreateFontIndirectW, CreateCompatibleBitmap, CreateDCW, CreatePatternBrush, GetStockObject, GetTextExtentPoint32W, DeleteMetaFile, CreateDIBitmap, CreateBitmap, CreateRectRgn, PatBlt, PlayMetaFile, SelectClipRgn, SetMapMode, SetMetaFileBitsEx, SetPixel, StretchBlt, SetStretchBltMode, SetViewportExtEx, SetViewportOrgEx, SetWindowExtEx, SetWindowOrgEx, TextOutW
ADVAPI32.dll	CryptSignHashW, RegEnumValueW, RegQueryValueExW, SetEntriesInAclW, RegQueryInfoKeyW, RegEnumKeyExW, RegDeleteValueW, RegDeleteKeyW, SetSecurityDescriptorOwner, SetSecurityDescriptorGroup, SetSecurityDescriptorDacl, InitializeSecurityDescriptor, CreateWellKnownSid, RegSetValueExW, RegOpenKeyExW, RegCreateKeyExW, RegCloseKey, RegOpenKeyW, OpenProcessToken, AdjustTokenPrivileges, AllocateAndInitializeSid, FreeSid, LookupPrivilegeValueW, RegOverridePredefKey, RegCreateKeyW, RegEnumKeyW, OpenThreadToken, GetTokenInformation, EqualSid, CryptAcquireContextW, CryptReleaseContext, CryptDeriveKey, CryptDestroyKey, CryptSetHashParam, CryptGetHashParam, CryptExportKey, CryptImportKey, CryptCreateHash, CryptHashData, CryptDestroyHash, CryptVerifySignatureW
SHELL32.dll	SHGetPathFromIDListW, SHGetSpecialFolderLocation, SHGetMalloc, ShellExecuteExW

DLL	Import
ole32.dll	CoTaskMemFree, CoTaskMemRealloc, CoTaskMemAlloc, CoCreateInstance, CoInitializeSecurity, ProgIDFromCLSID, CreateStreamOnHGlobal, CoInitializeEx, CoUninitialize, GetRunningObjectTable, CreateItemMoniker, CoLoadLibrary, CoCreateGuid, StringFromGUID2
OLEAUT32.dll	VariantChangeType, VarBstrCmp, CreateErrorInfo, SetErrorInfo, UnRegisterTypeLib, RegisterTypeLib, LoadTypeLib, VariantInit, VariantClear, VarUI4FromStr, SysAllocString, SysFreeString, SysStringLen, SysAllocStringLen, SysReAllocStringLen, GetErrorInfo, SysStringByteLen, VarBstrCat, SysAllocStringByteLen
RPCRT4.dll	UuidCreate, RpcStringFreeW, UuidFromStringW, UuidToStringW
gdiplus.dll	GdipFree, GdipDrawImageRectI, GdipSetInterpolationMode, GdipDeleteGraphics, GdipCreateFromHDC, GdipCreateBitmapFromResource, GdipCreateBitmapFromFileICM, GdipCreateBitmapFromStreamICM, GdipCreateBitmapFromFile, GdipCreateBitmapFromStream, GdipDisposeImage, GdipCloneImage, GdiplusStartup, GdipGetImageWidth, GdipGetImageHeight, GdipAlloc

Version Infos

Description	Data
LegalCopyright	Copyright (c) 2015 Flexera Software LLC. All Rights Reserved.
ISInternalVersion	22.0.401
InternalName	Setup
FileVersion	4.1.0.5
CompanyName	Automation Direct
Internal Build Number	176888
ProductName	SureServo PRO
ProductVersion	4.1.0.5
FileDescription	InstallScript Setup Launcher Unicode
ISInternalDescription	InstallScript Setup Launcher Unicode
OriginalFilename	InstallShield Setup.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

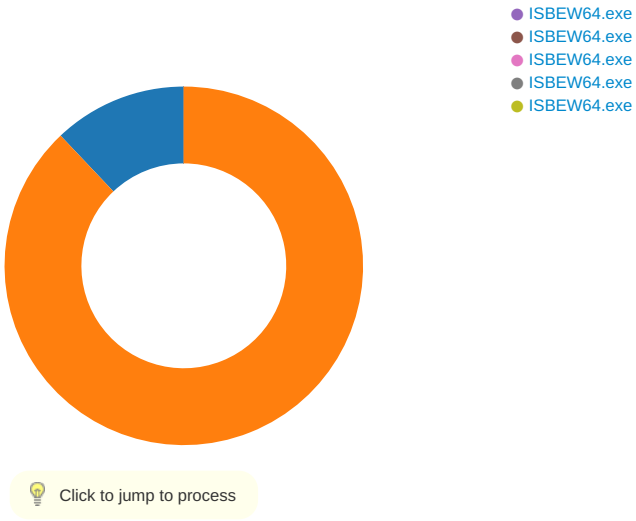
No network behavior found

Code Manipulations

Statistics

Behavior

- SureServoPROInstall_V4_1_0_5_D..
- setup.exe
- ISBEW64.exe
- ISBEW64.exe



System Behavior

Analysis Process: SureServoPROInstall_V4_1_0_5_DB2_0_8.exe PID: 6312 Parent PID: 5872

General

Start time:	18:08:23
Start date:	29/03/2021
Path:	C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe'
Imagebase:	0x400000
File size:	26675560 bytes
MD5 hash:	E1C700344A31AEE275B86A0CC5FE707B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	441B41	CreateDirectoryW
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	2	41CEEF	CreateDirectoryW
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	2	41CEEF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2	41CEEF	CreateDirectoryW
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	2	41CEEF	CreateDirectoryW
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	2	41CEEF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	41CEEF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	41CEEF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\0x0409.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\autorun.inf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.hdr	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\ISSetup.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\layout.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.inx	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\MsiStub\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	41CEEF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\MsiStub\{1F57C7D2-0C2E-406D-90F1-7C57BC934AB8}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	41CEEF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\MsiStub\{1F57C7D2-0C2E-406D-90F1-7C57BC934AB8}\SureServo PRO.msi	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	424884	CreateFileW
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	441B41	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	441B41	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	441BC0	CreateFileW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	441B41	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	441BC0	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\0x0409.ini	unknown	16384	ff fe 5b 00 30 00 78 00 30 00 34 00 30 00 39 00 5d 00 0d 00 0a 00 31 00 31 00 30 00 30 00 3d 00 53 00 65 00 74 00 75 00 70 00 20 00 49 00 6e 00 69 00 74 00 69 00 61 00 6c 00 69 00 7a 00 61 00 74 00 69 00 6f 00 6e 00 20 00 45 00 72 00 72 00 6f 00 72 00 0d 00 0a 00 31 00 31 00 30 00 31 00 3d 00 25 00 73 00 0d 00 0a 00 31 00 31 00 30 00 32 00 3d 00 25 00 31 00 20 00 53 00 65 00 74 00 75 00 70 00 20 00 69 00 73 00 20 00 70 00 72 00 65 00 70 00 61 00 72 00 69 00 6e 00 67 00 20 00 74 00 68 00 65 00 20 00 25 00 32 00 2c 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 77 00 69 00 6c 00 6c 00 20 00 67 00 75 00 69 00 64 00 65 00 20 00 79 00 6f 00 75 00 20 00 74 00 68 00 72 00 6f 00 75 00 67 00 68 00 20 00 74 00 68 00 65 00 20 00 70 00 72 00 6f 00 67 00 72 00 61 00 6d	..[.0.x.0.4.0.9.].....1.1.0.0. =.S.e.t.u.p. .I.n.i.t.i.a.l.i. z.a.t.i.o.n. .E.r.r.o.r.....1. 1.0.1.=.%.s.....1.1.0.2.=.%. 1. .S.e.t.u.p. .i.s. .p.r.e.p.a. r.i.n.g. .t.h.e. .%.2.,. .w.h. i.c.h. .w.i.l.l. .g.u.i.d.e. . y.o.u. .t.h.r.o.u.g.h. .t.h.e. .p.r.o.g.r.a.m	success or wait	1	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\0x0409.ini	unknown	6106	72 00 72 00 6f 00 72 00 20 00 43 00 6f 00 64 00 65 00 3a 00 0d 00 0a 00 32 00 30 00 30 00 33 00 3d 00 45 00 72 00 72 00 6f 00 72 00 20 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3a 00 0d 00 0a 00 32 00 30 00 30 00 34 00 3d 00 41 00 6e 00 20 00 65 00 72 00 72 00 6f 00 72 00 20 00 28 00 25 00 73 00 29 00 20 00 68 00 61 00 73 00 20 00 6f 00 63 00 63 00 75 00 72 00 72 00 65 00 64 00 20 00 77 00 68 00 69 00 6c 00 65 00 20 00 72 00 75 00 6e 00 6e 00 69 00 6e 00 67 00 20 00 74 00 68 00 65 00 20 00 73 00 65 00 74 00 75 00 70 00 2e 00 0d 00 0a 00 32 00 30 00 30 00 35 00 3d 00 50 00 6c 00 65 00 61 00 73 00 65 00 20 00 6d 00 61 00 6b 00 65 00 20 00 73 00 75 00 72 00 65 00 20 00 79 00 6f 00 75 00 20 00 68 00 61 00 76 00 65 00 20 00 66 00 69	r.r.o.r. .C.o.d.e.:.....2.0.0. 3.=.E.r.r.o.r. .I.n.f.o.r.m.a. t.i.o.n.:.....2.0.0.4.=.A.n. . e.r.r.o.r. .(.%.s.). .h.a.s. . o.c.c.u.r.r.e.d. .w.h.i.l.e. . r.u.n.n.i.n.g. .t.h.e. .s.e.t. u.p.....2.0.0.5.=.P.l.e.a.s. e. .m.a.k.e. .s.u.r.e. .y.o.u. .h.a.v.e. .f.i	success or wait	1	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\autorun.inf	unknown	43	5b 61 75 74 6f 72 75 6e 5d 0d 0a 6f 70 65 6e 3d 53 65 74 75 70 2e 65 78 65 0d 0a 69 63 6f 6e 3d 53 65 74 75 70 2e 65 78 65 0d 0a	[autorun]..open=Setup.exe ..icon=Setup.exe..	success or wait	1	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	unknown	16384	49 53 63 28 98 08 00 04 00 00 00 00 00 02 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ISc(.......................... ..V...........................	success or wait	445	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	unknown	15373	30 d5 62 a3 c4 d7 d8 05 81 22 9d b6 7d d5 99 0e 5c b1 f5 ec 48 15 4b 22 81 6f 6d 06 04 66 2f d2 b1 db 7a b6 ff c3 e1 68 c9 a2 b8 37 55 d8 36 87 18 be 39 42 fb 83 30 64 7b e2 ce 3d a3 ed ab 5c fb 90 49 19 97 7a e9 40 2d 94 7d a5 1f e2 3f fd 69 e9 3e 6c d1 4f 95 75 40 60 97 4a 99 da 57 82 e4 c4 6e 8d 43 c6 9e 8d c6 9d ff bc 5b fe 0e 6a 00 82 2b 2c 45 9a ca 04 7e 0e 42 0a 58 47 4a cf 3f ff bc 92 c2 67 cf 05 8d 01 23 5b fe 01 da 84 2f e3 9e ed 09 34 af de 50 a1 53 1e c1 dd 3e 9e e3 c1 0c c1 33 44 7e 0e c1 e6 c3 c3 9c b9 27 0e c3 c8 a8 3a e7 39 72 92 79 f5 da c4 9f 90 c4 08 67 22 96 c6 68 0e a1 74 c7 73 30 c4 d8 5b 79 99 66 a7 f0 72 32 6b cc 27 f7 38 07 69 1a 10 0e 4e 22 9f 34 83 9f 13 31 ec 1d 95 38 74 5f b4 01 44 3e fb b0 49 a4 95 d0 9e 72 cd 9c 4d 8d 43 65	0.b......"..}...\...H.K".om..f /...z....h...7U.6...9B..0d{..= ...\..I..z.@-.}...?.i.>l.O.u@` .J..W...n.C.......[..j..+,E... ~.B.XGJ.?....g....#[..../....4 ..P.S...>.....3D~.......'....: .9r.y.......g"..h..t.s0..[y.f. .r2k.'.8.i...N".4...1...8t_..D >..I....r..M.Ce	success or wait	1	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.hdr	unknown	16384	49 53 63 28 98 08 00 04 00 00 00 00 00 02 00 00 17 4e 00 00 d0 86 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d4 1d 8c d9 8f 00 b2 04 e9 80 09 98 ec f8 42 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	ISc(............N............ ....B~....................	success or wait	2	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.hdr	unknown	1744	5f 00 30 00 78 00 30 00 34 00 31 00 31 00 2e 00 64 00 6c 00 6c 00 00 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 5f 00 30 00 78 00 30 00 34 00 31 00 31 00 2e 00 69 00 70 00 73 00 00 00 5f 00 69 00 73 00 72 00 65 00 73 00 5f 00 30 00 78 00 30 00 34 00 31 00 32 00 2e 00 64 00 6c 00 6c 00 00 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 5f 00 30 00 78 00 30 00 34 00 31 00 32 00 2e 00 69 00 70 00 73 00 00 00 5f 00 69 00 73 00 72 00 65 00 73 00 5f 00 30 00 78 00 30 00 34 00 31 00 33 00 2e 00 64 00 6c 00 6c 00 00 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 5f 00 30 00 78 00 30 00 34 00 31 00 33 00 2e 00 69 00 70 00 73 00 00 00 5f 00 69 00 73 00 72 00 65 00 73 00 5f 00 30 00 78 00 30 00 34	_.0.x.0.4.1.1...d.l.l...S.t.r.i.n.g.T.a.b.l.e._.0.x.0.4.1.1...i.p.s..._.i.s.r.e.s._.0.x.0.4.1.2...d.l.l...S.t.r.i.n.g.T.a.b.l.e._.0.x.0.4.1.2...i.p.s..._.i.s.r.e.s._.0.x.0.4.1.3...d.l.l...S.t.r.i.n.g.T.a.b.l.e._.0.x.0.4.1.3...i.p.s..._.i.s.r.e.s._.0.x.0.4	success or wait	1	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\ISSetup.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6c 1e 6a f3 28 7f 04 a0 28 7f 04 a0 28 7f 04 a0 b6 df c3 a0 29 7f 04 a0 d9 b9 c9 a0 31 7f 04 a0 d9 b9 ca a0 a2 7f 04 a0 d9 b9 cb a0 63 7f 04 a0 d4 08 b8 a0 2f 7f 04 a0 d4 08 ba a0 29 7f 04 a0 28 7f 05 a0 34 7d 04 a0 d4 08 bd a0 3d 7f 04 a0 8a b8 d7 a0 23 7f 04 a0 8a b8 ca a0 2f 7f 04 a0 8a b8 cb a0 53 7f 04 a0 8a b8 ce a0 29 7f 04 a0 8a b8 cd a0 29 7f 04 a0 28 7f 93 a0 29 7f 04	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......l.j.(...(... (.......).......1...............c....... /.......)...(...4}......=..... ..#......./.......S.......).......)... (...)..	success or wait	49	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\ISSetup.dll	unknown	4880	30 43 06 03 55 04 03 13 3c 56 65 72 69 53 69 67 6e 20 43 6c 61 73 73 20 33 20 50 75 62 6c 69 63 20 50 72 69 6d 61 72 79 20 43 65 72 74 69 66 69 63 61 74 69 6f 6e 20 41 75 74 68 6f 72 69 74 79 20 2d 20 47 35 30 1e 17 0d 30 36 31 31 30 38 30 30 30 30 30 30 5a 17 0d 33 36 30 37 31 36 32 33 35 39 35 39 5a 30 81 ca 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 17 30 15 06 03 55 04 0a 13 0e 56 65 72 69 53 69 67 6e 2c 20 49 6e 63 2e 31 1f 30 1d 06 03 55 04 0b 13 16 56 65 72 69 53 69 67 6e 20 54 72 75 73 74 20 4e 65 74 77 6f 72 6b 31 3a 30 38 06 03 55 04 0b 13 31 28 63 29 20 32 30 30 36 20 56 65 72 69 53 69 67 6e 2c 20 49 6e 63 2e 20 2d 20 46 6f 72 20 61 75 74 68 6f 72 69 7a 65 64 20 75 73 65 20 6f 6e 6c 79 31 45 30 43 06 03 55 04 03 13 3c 56 65 72 69 53 69 67 6e 20	0C..U...<VeriSign Class 3 Public Primary Certification Authority - G50...061108000000Z..36 0716235959Z0..1.0...U.... US1.0...U....VeriSign, Inc.1.0...U....VeriSign Trust Network1:08..U...1(c) 2006 VeriSign, Inc. - For authorized use only1E0C. .U...<VeriSign	success or wait	1	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\layout.bin	unknown	610	63 07 00 53 00 40 00 00 62 01 00 00 00 01 00 00 06 00 00 40 a6 28 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	c..S.@..b..........@.(........	success or wait	1	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.bmp	unknown	16384	42 4d 36 b4 04 00 00 00 00 00 36 04 00 00 28 00 00 00 80 02 00 00 e0 01 00 00 01 00 08 00 00 00 00 00 00 b0 04 00 13 0b 00 00 13 0b 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 c0 dc c0 00 f0 ca a6 00 04 04 04 00 14 08 0a 00 0c 11 0d 00 17 14 0c 00 0c 0c 12 00 15 0a 15 00 0d 12 15 00 16 17 19 00 22 17 19 00 19 22 1b 00 23 21 1c 00 1a 1c 22 00 20 1e 23 00 1c 23 28 00 25 26 2a 00 31 2b 2d 00 28 33 2c 00 33 33 2d 00 2a 2b 32 00 31 2d 33 00 2c 32 36 00 31 31 32 00 41 3c 3d 00 33 48 38 00 49 4c 37 00 54 64 33 00 1d 2f 45 00 37 3b 43 00 1d 1d 72 00 1b 2a 69 00 2d 2d 72 00 41 3e 42 00 40 3f 72 00 3a 44 4b 00 3b 69 49 00 38 4f 6b 00 3a 70 73 00 45 46 49 00 52 4b 4c 00 47 54 4c 00 56	BM6.......6...(............... ...."....."..#!....". .#..#(. %&*.1+-.(3,.33-.*+2.1- 3.,26.11 2.A<=.3H8.IL7.Td3../E.7;C ...r..*i.--r.A>B.@? r.:DK.;iI.8Ok.:p s.EFI.RKL.GTL.V	success or wait	18	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.bmp	unknown	13366	b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b3 b3 b1 b3 b3 b3 b1 b3 b3 b1	....	success or wait	1	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e 79 1d 81 1a 18 73 d2 1a 18 73 d2 1a 18 73 d2 b8 df a0 d2 1b 18 73 d2 eb de be d2 03 18 73 d2 eb de bd d2 9f 18 73 d2 b8 df bd d2 18 18 73 d2 eb de bc d2 5a 18 73 d2 e6 6f cf d2 1e 18 73 d2 1a 18 72 d2 d4 19 73 d2 e6 6f ca d2 0f 18 73 d2 b8 df bc d2 37 18 73 d2 b8 df ba d2 1b 18 73 d2 1a 18 e4 d2 1b 18 73 d2 b8 df bf d2 1b 18 73 d2 52 69 63 68 1a 18 73 d2 00 00 00 00 00 00 00	MZ......................@...................................!..L.!This program cannot be run in DOS mode....$.......^y....s...s...s.......s.......s.......s.......s.....Z.s..o....s...r...s..o....s.....7.s.......s.......s.......s.Rich..s........	success or wait	73	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	unknown	5904	96 96 d9 be 61 79 0b 5b c9 4c 86 76 e5 e0 43 4b 22 95 ee c2 2b 43 c1 9f d8 68 b4 8e 40 4f ee 85 38 b9 11 c5 23 f2 64 58 f0 15 32 6f 4e 57 a1 ae 88 a4 02 d7 2a 1e cd 4b e1 dd 63 d5 17 89 32 5b b0 5e 99 5a a8 9d 28 50 0e 17 ee 96 db 61 3b 45 51 1d cf 12 56 0b 92 47 fc ab ae f6 66 3d 47 ac 70 72 e7 92 e7 5f cd 10 b9 c4 83 64 94 19 bd 25 80 e1 e8 d2 22 a5 d0 ba 02 7a a1 77 93 5b 65 c3 ee 17 74 bc 41 86 2a dc 08 4c 8c 92 8c 91 2d 9e 77 44 1f 68 d6 a8 74 77 db 0e 5b 32 8b 56 8b 33 bd d9 63 c8 49 9d 3a c5 c5 ea 33 0b d2 f1 a3 1b f4 8b be d9 b3 57 8b 3b de 04 a7 7a 22 b2 24 ae 2e c7 70 c5 be 4e 83 26 08 fb 0b bd a9 4f 99 08 e1 10 28 72 aa cd 02 03 01 00 01 a3 82 01 57 30 82 01 53 30 0c 06 03 55 1d 13 01 01 ff 04 02 30 00 30 16 06 03 55 1d 25 01 01 ff 04 0c 30 0a	....ay. [.L.v..CK"...+C...h..@O ..8...#.dX..2oNW.....*..K..c. ..2[.^.Z..(P.....a;EQ...V..G.. ..f=G.pr..._.....d...%...."... .z.w.[e...t.A.*..L.....-.wD.h.. tw..[2.V.3..c.I.:...3..... .W.;...z".$...p..N.&.....O.... (r.....W0..S0...U.....0 .0...U.%.....0.	success or wait	1	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.ini	unknown	2424	ff fe 5b 00 53 00 74 00 61 00 72 00 74 00 75 00 70 00 5d 00 0d 00 0a 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3d 00 53 00 75 00 72 00 65 00 53 00 65 00 72 00 76 00 6f 00 20 00 50 00 52 00 4f 00 0d 00 0a 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 47 00 55 00 49 00 44 00 3d 00 36 00 32 00 45 00 30 00 35 00 39 00 32 00 45 00 2d 00 42 00 31 00 43 00 30 00 2d 00 34 00 39 00 39 00 42 00 2d 00 38 00 33 00 46 00 36 00 2d 00 38 00 32 00 39 00 37 00 38 00 39 00 42 00 44 00 42 00 44 00 35 00 31 00 0d 00 0a 00 43 00 6f 00 6d 00 70 00 61 00 6e 00 79 00 4e 00 61 00 6d 00 65 00 3d 00 41 00 75 00 74 00 6f 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 20 00 44 00 69 00 72 00 65 00 63 00 74 00 0d 00 0a 00 43 00 6f 00 6d 00 70 00 61 00 6e 00 79 00 55 00 52 00 4c 00 3d 00 77	..[.S.t.a.r.t.u.p.].....P.r.o. d.u.c.t.=.S.u.r.e.S.e.r.v.o. . P.R.O.....P.r.o.d.u.c.t.G.U.I .D.=.6.2.E.0.5.9.2.E.- .B.1.C.0.-.4.9.9.B.- .8.3.F.6.-.8.2.9.7. 8.9.B.D.B.D.5.1.....C.o.m.p .a. n.y.N.a.m.e.=.A.u.t.o.m.a.t. i.o.n. .D.i.r.e.c.t.....C.o.m.p. a.n.y.U.R.L.=.w	success or wait	1	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.inx	unknown	16384	74 c4 2c 84 e1 e5 d4 28 10 fb 00 20 3c 24 fb 4d 11 20 1d 3d e4 c8 cc ec e4 dc d8 dc c8 05 6c c7 bf a7 ff cf b3 10 cb b3 c7 a7 cb dc 0c 83 a3 7f 6f bb 63 93 a0 10 67 57 53 6c 98 00 53 57 88 b7 57 53 5b 2f 2f 64 93 64 20 6c 24 18 58 58 25 d1 d5 d9 dd c1 c5 c9 cd b1 b5 b9 bd a1 a5 a9 ad 91 95 99 9d 81 85 89 8d 71 87 79 7d 61 f6 3d 6d 51 b5 59 5d 41 03 f3 4d 31 c1 ed 29 21 0b 29 cc 11 15 19 19 1d 05 09 09 0d d8 f8 f8 fc c8 e8 0e f1 dd fd fd e1 cd ed ed d1 bd dd dd c1 ad cd cd b1 9d bd bd a1 8d ad ad 91 7d 9d 9d 81 6d 8d 8d 71 5d 7d 7d 61 4d 6d 1d 55 3d 5d 01 45 2d 4d 1d 35 1d 3d e8 25 0d 2d d4 15 fc 1d dc 05 ec 0d c0 f4 dc fc 94 e4 cc f1 91 f9 c1 e1 c9 e9 b1 d1 bd d9 d3 c1 c9 c9 05 b1 96 b9 5d a1 95 a9 9d 95 95 61 9d db 28 ff f3 bb 48 b7 b7 93 c7 59 51 51 45	t.,....(... <$.M. .=..... l.....o.c...gWSl.. SW..WS[//d.d l$.XX%..... .....q.y}a.=mQ.Y]A..M 1..)!.)..... .....}...m..q]}}a Mm.U=].E-M.5.=.%.- .....]......a ..(...H....YQQE	success or wait	15	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.inx	unknown	13841	5d 89 f4 71 75 79 59 62 65 69 6d d4 55 ee 45 45 45 39 da 4d 9c 39 25 21 15 b6 29 09 19 19 2c f8 05 f0 0d e4 82 f4 dc e0 e4 a0 f1 e1 f9 d1 87 e1 dd 7b ed b1 d5 d9 dd c1 b9 cd b9 b5 95 a1 a1 a5 a9 81 37 91 1d 9d 27 8d 75 8d 61 03 75 55 65 65 60 41 fe 51 31 5d 49 45 3d d6 4d 15 39 3d f8 25 15 2d 05 ba 15 f0 aa 01 e4 09 0d f0 f4 ec e0 ec e8 ed f9 f9 fd e1 d9 8f e9 cd d5 c5 dd b5 6b c5 a1 5f b1 95 a1 a1 a5 a9 69 91 81 99 71 23 81 7d 17 8d 69 07 79 3d 65 55 6d 45 f6 55 31 e2 41 25 31 31 35 39 80 21 15 29 1d be 11 09 aa 1d f8 ae 09 e4 96 f4 e8 e0 40 e8 f1 f5 65 fd e5 e5 c5 ed d1 d5 d9 35 c1 c5 c9 bd b1 b5 b9 a1 a1 a5 a9 85 91 1d 99 9d 81 61 c4 8d 71 75 d4 7d 61 65 e8 6d 95 5d 49 5d 35 80 49 3d de 31 2d ca 3d 19 b2 29 09 15 01 1d f4 aa 05 ec f0 f4 64 fc e4 e4 dc	]..quyYbeim.U.EEE9.M.9% !..)...,.....{..... .....7...'.u.a.uUee`A.Q1]lE= .M.9=.%.-..... .....k.._.....i...q#.}..i.y= eUmE.U1.A%1159.!.)..... .....@...e.....5..... ...a..qu.}ae.m.]l]5.l=.1-.=..) .....d....	success or wait	1	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\MsiStub\{1F57C7D2-0C2E-406D-90F1-7C57BC934AB8}\SureServo PRO.msi	unknown	16384	d0 cf 11 e0 a1 b1 1a e1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 3e 00 03 00 fe ff 09 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 4d 00 00 00 01 00 00 00 00 00 00 00 00 00 10 00 00 38 00 00 00 04 00 00 00 fe ff ff ff 00 00 00 00 00 00 00 00 7a 00 00 00 00 01 00 00 03 00 00 00 f6 01 00 00 6f 02 00 00 c8 02 00 00 08 03 00 00 09 03 00 00 0a 03 00 00 0b 03 00 00 0c 03 00 00 0d 03 00 00 0e 03 00 00 0f 03 00 00 10 03 00 00 11 03 00 00 12 03 00 00 13 03 00 00 14 03 00 00 15 03 00 00 16 03 00 00 17 03 00 00 18 03 00 00 19 03 00 00 1a 03 00 00 1b 03 00 00 1c 03 00 00 1d 03 00 00 1e 03 00 00 1f 03 00 00 20 03 00 00 21 03 00 00 22 03 00 00 23 03 00 00 24 03 00 00 25 03 00 00 26 03 00 00 27 03 00 00 28 03 00 00 29 03 00 00 2a 03 00 00 2b 03 00 00 2c 03 00 00 2d 03 00	.....>..... .....M..... 8.....z..... ......o..... ....!...". ..#...$...%...&...'...(...)... *...+...,...-..	success or wait	306	425FA8	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\MsiStub\{1F57C7D2-0C2E-406D-90F1-7C57BC934AB8}\SureServo PRO.msi	unknown	2048	98 7a 47 3b 36 69 c3 0e 33 35 84 a5 2b e6 c8 4f eb 45 e8 bc 3c 6e 7d cf 04 d5 69 b5 2e 53 33 66 5e 16 50 54 5a 2d e6 24 20 e8 0d 73 f1 c8 3c b4 98 88 0e f3 30 87 9f 6b 67 8f 39 4b 5f dd a8 29 df 6b 4f 75 98 86 03 37 77 18 70 50 bf 42 e6 b5 85 6a 6e 1d 66 8e a0 e4 a7 b6 4e c0 24 8c 87 05 17 e1 63 c5 b4 60 62 d7 bc c3 c5 09 1c dc d3 3c 17 e9 28 34 fc 93 b2 d0 6f 48 ce d2 3e ab 74 10 ee c5 49 3a 07 fb aa 70 af 89 d5 be 91 f5 94 a4 57 dc 66 3e ac 35 41 d2 79 98 57 c6 51 5b 24 dd c5 4b 47 b0 6e 0d e7 02 6a a2 71 af 70 92 f5 98 a4 57 de 96 ac 83 d9 10 64 cb d3 67 77 90 ad 86 6f 76 21 da 10 c7 fc 50 af 0c 61 94 09 7c f2 16 7f ac 41 b3 d6 55 fb 6a 80 29 7e 5c 2d 70 c4 ed 55 98 c4 ed 6b 8f c4 4b 5f 99 f7 30 be f9 f5 0a c7 d3 bf 29 2b fe 90 9f c1 7c 41 98 65 e0 55	.zG;6i..35..+..O.E..<n}...i..S 3f^.PTZ-.$ ..s.. <.....0..kg.9K _..).kOu...7w.pP.B...jn.f..... N.$.....c..`b.....<..(4.... oH..>.t...I:...p.....W.f>.5 A.y.W.Q[$..KG.n...j.q.p.... W.....d..gw...ov!....P..a..|.... A..U.j.)~\-p..U...k..K_..0.... ...)+....|A.e.U	success or wait	1	425FA8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	unknown	2424	ff fe 5b 00 53 00 74 00 61 00 72 00 74 00 75 00 70 00 5d 00 0d 00 0a 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3d 00 53 00 75 00 72 00 65 00 53 00 65 00 72 00 76 00 6f 00 20 00 50 00 52 00 4f 00 0d 00 0a 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 47 00 55 00 49 00 44 00 3d 00 36 00 32 00 45 00 30 00 35 00 39 00 32 00 45 00 2d 00 42 00 31 00 43 00 30 00 2d 00 34 00 39 00 39 00 42 00 2d 00 38 00 33 00 46 00 36 00 2d 00 38 00 32 00 39 00 37 00 38 00 39 00 42 00 44 00 42 00 44 00 35 00 31 00 0d 00 0a 00 43 00 6f 00 6d 00 70 00 61 00 6e 00 79 00 4e 00 61 00 6d 00 65 00 3d 00 41 00 75 00 74 00 6f 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 20 00 44 00 69 00 72 00 65 00 63 00 74 00 0d 00 0a 00 43 00 6f 00 6d 00 70 00 61 00 6e 00 79 00 55 00 52 00 4c 00 3d 00 77	..[.S.t.a.r.t.u.p.].....P.r.o. d.u.c.t.=.S.u.r.e.S.e.r.v.o. . P.R.O.....P.r.o.d.u.c.t.G.U.I .D.=.6.2.E.0.5.9.2.E.- .B.1.C.0.-.4.9.9.B.- .8.3.F.6.-.8.2.9.7. 8.9.B.D.B.D.5.1.....C.o.m.p .a. n.y.N.a.m.e.=.A.u.t.o.m.a.t. i.o.n. .D.i.r.e.c.t.....C.o.m.p. a.n.y.U.R.L.=.w	success or wait	1	43AF74	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e 79 1d 81 1a 18 73 d2 1a 18 73 d2 1a 18 73 d2 b8 df a0 d2 1b 18 73 d2 eb de be d2 03 18 73 d2 eb de bd d2 9f 18 73 d2 b8 df bd d2 18 18 73 d2 eb de bc d2 5a 18 73 d2 e6 6f cf d2 1e 18 73 d2 1a 18 72 d2 d4 19 73 d2 e6 6f ca d2 0f 18 73 d2 b8 df bc d2 37 18 73 d2 b8 df ba d2 1b 18 73 d2 1a 18 e4 d2 1b 18 73 d2 b8 df bf d2 1b 18 73 d2 52 69 63 68 1a 18 73 d2 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......^y....s...s...s....... s.......s.......s.......s..... Z.s..o....s...r...s..o....s... ..7.s.......s.......s.......s. Rich..s........	success or wait	37	43AF74	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	unknown	3	success or wait	1	4155E1	ReadFile
C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	unknown	4	success or wait	1	4250AD	ReadFile
C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe	unknown	16384	success or wait	909	4250AD	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.ini	unknown	2	success or wait	1	4155E1	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.ini	unknown	32768	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.ini	unknown	32768	end of file	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	unknown	2424	success or wait	1	42ABB2	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	unknown	3	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe	unknown	32768	end of file	1	4155E1	ReadFile

Analysis Process: setup.exe PID: 6356 Parent PID: 6312

General

Start time:	18:08:24
Start date:	29/03/2021
Path:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe -package:'C:\Users\user\Desktop\SureServoPROInstall_V4_1_0_5_DB2_0_8.exe' -no_selfdeleter -IS_temp -media_path:'C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\' -tempdisk1folder:'C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\' -IS_OriginalLauncher:'C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.exe'
Imagebase:	0x400000
File size:	1201936 bytes
MD5 hash:	88340D6E1DE3ED49364A64B3D8796AF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 2%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	441B41	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	441BC0	CreateFileW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
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	441B41	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	441B41	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	441BC0	CreateFileW
C:\Users\user\AppData\Local\Temp\{B2849AD0-7C5E-4373-B0F4-BA2817BE4589}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100BF85A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{9D17587E-2827-4CD6-8FFD-A078748F26FA}	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	100BF85A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\538A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1003D151	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1003D151	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\set53F8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\set53F8.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\lic53F9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\lic53F9.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Fon53FA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Fon53FA.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\DIF542A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\DIF542A.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\cor542B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\cor542B.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542C.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542D.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Str542F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Str542F.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1003D151	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5461.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5461.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\def5462.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\def5462.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_is5463.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_is5463.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Set5500.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Set5500.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\lsr5530.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\lsr5530.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5560.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5560.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str55CE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str55CE.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is55FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is55FE.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5757.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5757.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5758.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5758.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str57C6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str57C6.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is57C7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is57C7.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5826.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5826.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5827.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5827.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5895.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5895.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5896.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5896.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str58F5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str58F5.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is58F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is58F6.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5993.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5993.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5994.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5994.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str59F3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str59F3.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is59F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is59F4.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5B8B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5B8B.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5B8C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5B8C.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C1A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C1A.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C1B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C1B.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C89.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C89.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C8A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C8A.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5CE9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5CE9.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5CEA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5CEA.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5D49.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5D49.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5D4A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5D4A.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5DE7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5DE7.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5DE8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5DE8.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str61D1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str61D1.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is61D2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is61D2.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str626F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str626F.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6270.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6270.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str62FE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str62FE.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is632E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is632E.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str636D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str636D.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is636E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is636E.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str63FC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str63FC.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is63FD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is63FD.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str646B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str646B.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is646C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is646C.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str64CB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str64CB.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is64CC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is64CC.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str652B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str652B.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is656A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is656A.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str65C9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str65C9.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is65CA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is65CA.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6667.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6667.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6668.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6668.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str66C7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str66C7.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is66F7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is66F7.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6765.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6765.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6766.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6766.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6823.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6823.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6824.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6824.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6892.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6892.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6893.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6893.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6921.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6921.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6922.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6922.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str69BF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str69BF.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is69C0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is69C0.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A1F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A1F.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6A20.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6A20.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A8E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A8E.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6ABE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6ABE.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6B1D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6B1D.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\MMO6B1E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	10047279	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\MMO6B1E.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	100E1834	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\538A.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\set53F8.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\lic53F9.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Fon53FA.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\DIF542A.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\cor542B.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542C.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542D.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Str542F.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5461.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\def5462.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_is5463.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Set5500.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Isr5530.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5560.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str55CE.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is55FE.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5757.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5758.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str57C6.tmp	success or wait	1	100472D0	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is57C7.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5826.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5827.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5895.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5896.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str58F5.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is58F6.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5993.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5994.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str59F3.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is59F4.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5B8B.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5B8C.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C1A.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C1B.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C89.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C8A.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5CE9.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5CEA.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5D49.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5D4A.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5DE7.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5DE8.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str61D1.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is61D2.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str626F.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6270.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str62FE.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is632E.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str636D.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is636E.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str63FC.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is63FD.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str646B.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is646C.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str64CB.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is64CC.tmp	success or wait	1	100472D0	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str652B.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is656A.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str65C9.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is65CA.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6667.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6668.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str66C7.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is66F7.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6765.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6766.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6823.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6824.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6892.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6893.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6921.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6922.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str69BF.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is69C0.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A1F.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6A20.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A8E.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6ABE.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6B1D.tmp	success or wait	1	100472D0	DeleteFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\MMO6B1E.tmp	success or wait	1	100472D0	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\set53F8.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\setup.inx	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\lic53F9.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\license.txt	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Fon53FA.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\FontData.ini	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\DIF542A.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\DIFxData.ini	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\cor542B.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\corecomp.ini	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542C.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dotnetinstaller.exe	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542D.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dotnetinstaller.exe.config	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe	success or wait	1	1007AC85	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Str542F.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\StringTable_0x0409.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isrt.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5461.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\def5462.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\default.pal	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_is5463.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_isres_0x0409.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Set5500.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Setup.inx	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Isr5530.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Isrt.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Default.pal	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5560.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0c0c.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str55CE.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0c0c.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is55FE.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0c1a.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5757.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0c1a.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5758.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x040a.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str57C6.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x040a.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is57C7.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x040b.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5826.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x040b.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5827.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x040c.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5895.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x040c.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5896.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x040e.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str58F5.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x040e.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is58F6.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x041a.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5993.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x041a.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5994.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x041b.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str59F3.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x041b.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is59F4.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x041d.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5B8B.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x041d.ips	success or wait	1	1007AC85	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5B8C.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x041e.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C1A.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x041e.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C1B.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x041f.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C89.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x041f.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C8A.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x042d.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5CE9.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x042d.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5CEA.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0402.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5D49.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0402.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5D4A.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0403.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5DE7.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0403.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5DE8.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0404.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str61D1.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0404.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is61D2.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0405.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str626F.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0405.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6270.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0406.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str62FE.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0406.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is632E.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0407.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str636D.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0407.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is636E.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0408.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str63FC.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0408.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is63FD.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0409.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str646B.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0409.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is646C.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0410.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str64CB.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0410.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is64CC.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0411.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str652B.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0411.ips	success or wait	1	1007AC85	MoveFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is656A.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0412.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str65C9.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0412.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is65CA.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0413.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6667.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0413.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6668.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0414.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str66C7.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0414.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is66F7.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0415.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6765.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0415.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6766.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0416.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6823.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0416.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6824.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0418.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6892.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0418.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6893.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0419.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6921.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0419.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6922.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0421.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str69BF.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0421.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is69C0.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0424.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A1F.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0424.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6A20.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0804.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A8E.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0804.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6ABE.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0816.dll	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6B1D.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0816.ips	success or wait	1	1007AC85	MoveFileW
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\MMO6B1E.tmp	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\MMObjHelper.dll	success or wait	1	1007AC85	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	22490	ff fe 5b 00 30 00 78 00 30 00 34 00 30 00 39 00 5d 00 0d 00 0a 00 31 00 31 00 30 00 30 00 3d 00 53 00 65 00 74 00 75 00 70 00 20 00 49 00 6e 00 69 00 74 00 69 00 61 00 6c 00 69 00 7a 00 61 00 74 00 69 00 6f 00 6e 00 20 00 45 00 72 00 72 00 6f 00 72 00 0d 00 0a 00 31 00 31 00 30 00 31 00 3d 00 25 00 73 00 0d 00 0a 00 31 00 31 00 30 00 32 00 3d 00 25 00 31 00 20 00 53 00 65 00 74 00 75 00 70 00 20 00 69 00 73 00 20 00 70 00 72 00 65 00 70 00 61 00 72 00 69 00 6e 00 67 00 20 00 74 00 68 00 65 00 20 00 25 00 32 00 2c 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 77 00 69 00 6c 00 6c 00 20 00 67 00 75 00 69 00 64 00 65 00 20 00 79 00 6f 00 75 00 20 00 74 00 68 00 72 00 6f 00 75 00 67 00 68 00 20 00 74 00 68 00 65 00 20 00 70 00 72 00 6f 00 67 00 72 00 61 00 6d	..[.0.x.0.4.0.9.].....1.1.0.0.=.S.e.t.u.p. .I.n.i.t.i.a.l.i.z.a.t.i.o.n. .E.r.r.o.r.....1.1.0.1.=.%.s.....1.1.0.2.=.%.1. .S.e.t.u.p. .i.s. .p.r.e.p.a.r.i.n.g. .t.h.e. .%.2.,. .w.h.i.c.h. .w.i.l.l. .g.u.i.d.e. .y.o.u. .t.h.r.o.u.g.h. .t.h.e. .p.r.o.g.r.a.m	success or wait	1	43AF74	WriteFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	unknown	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6c 1e 6a f3 28 7f 04 a0 28 7f 04 a0 28 7f 04 a0 b6 df c3 a0 29 7f 04 a0 d9 b9 c9 a0 31 7f 04 a0 d9 b9 ca a0 a2 7f 04 a0 d9 b9 cb a0 63 7f 04 a0 d4 08 b8 a0 2f 7f 04 a0 d4 08 ba a0 29 7f 04 a0 28 7f 05 a0 34 7d 04 a0 d4 08 bd a0 3d 7f 04 a0 8a b8 d7 a0 23 7f 04 a0 8a b8 ca a0 2f 7f 04 a0 8a b8 cb a0 53 7f 04 a0 8a b8 ce a0 29 7f 04 a0 8a b8 cd a0 29 7f 04 a0 28 7f 93 a0 29 7f 04	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.......l.j.(...(...(.......).......1...............c......./.......)...(...4}......=.......#......./.......S.......).......)...(...)..	success or wait	25	43AF74	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\set53F8.tmp	unknown	32768	74 c4 2c 84 e1 e5 d4 28 10 fb 00 20 3c 24 fb 4d 11 20 1d 3d e4 c8 cc ec e4 dc d8 dc c8 05 6c c7 bf a7 ff cf b3 10 cb b3 c7 a7 cb dc 0c 83 a3 7f 6f bb 63 93 a0 10 67 57 53 6c 98 00 53 57 88 b7 57 53 5b 2f 2f 64 93 64 20 6c 24 18 58 58 25 d1 d5 d9 dd c1 c5 c9 cd b1 b5 b9 bd a1 a5 a9 ad 91 95 99 9d 81 85 89 8d 71 87 79 7d 61 f6 3d 6d 51 b5 59 5d 41 03 f3 4d 31 c1 ed 29 21 0b 29 cc 11 15 19 19 1d 05 09 09 0d d8 f8 f8 fc c8 e8 0e f1 dd fd fd e1 cd ed ed d1 bd dd dd c1 ad cd cd b1 9d bd bd a1 8d ad ad 91 7d 9d 9d 81 6d 8d 8d 71 5d 7d 7d 61 4d 6d 1d 55 3d 5d 01 45 2d 4d 1d 35 1d 3d e8 25 0d 2d d4 15 fc 1d dc 05 ec 0d c0 f4 dc fc 94 e4 cc f1 91 f9 c1 e1 c9 e9 b1 d1 bd d9 d3 c1 c9 c9 05 b1 96 b9 5d a1 95 a9 9d 95 95 61 9d db 28 ff f3 bb 48 b7 b7 93 c7 59 51 51 45	t.,....(... <$.M. .=..... l.....o.c...gWSl.. SW..WS[//d.d l$.XX%..... .....q.y}a.=mQ.Y]A..M 1..)!.)..... .....}...m..q]}}a Mm.U=].E-M.5.=.%.- .....]......a ..(...H....YQQE	success or wait	8	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\lic53F9.tmp	unknown	1033	54 68 65 20 73 6f 66 74 77 61 72 65 20 61 63 63 6f 6d 70 61 6e 79 69 6e 67 20 74 68 69 73 20 6c 69 63 65 6e 73 65 20 61 67 72 65 65 6d 65 6e 74 20 28 53 75 72 65 53 65 72 76 6f 20 50 72 6f 28 74 6d 29 29 20 69 73 20 74 68 65 20 20 70 72 6f 70 65 72 74 79 20 6f 66 20 41 75 74 6f 6d 61 74 69 6f 6e 44 69 72 65 63 74 2e 63 6f 6d 2c 20 6f 72 20 69 74 73 20 73 75 70 70 6c 69 65 72 73 2c 20 61 6e 64 20 69 73 20 70 72 6f 74 65 63 74 65 64 20 62 79 20 20 55 6e 69 74 65 64 20 53 74 61 74 65 73 20 61 6e 64 20 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 20 43 6f 70 79 72 69 67 68 74 20 6c 61 77 73 20 61 6e 64 20 49 6e 74 65 72 6e 61 74 69 6f 6e 61 6c 20 74 72 65 61 74 79 20 20 70 72 6f 76 69 73 69 6f 6e 73 2e 20 20 0d 0a 0d 0a 4e 6f 20 6f 77 6e 65 72 73 68 69 70 20 72 69	The software accompanying this license agreement (SureServo Pro(tm)) is the property of AutomationDirect.com, or its suppliers, and is protected by United States and International Copyright laws and International treaty provisions. ....No ownership ri	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Fon53FA.tmp	unknown	37	5b 3c 50 72 6f 70 65 72 74 69 65 73 3e 5d 0d 0a 46 6f 6e 74 52 65 67 69 73 74 72 61 74 69 6f 6e 3d 4e 6f 0d 0a	[<Properties>]..FontRegistration=No..	success or wait	1	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\DIF542A.tmp	unknown	84	5b 3c 50 72 6f 70 65 72 74 69 65 73 3e 5d 0d 0a 44 49 46 78 33 32 53 75 70 70 6f 72 74 65 64 3d 4e 6f 0d 0a 44 49 46 78 49 6e 74 65 6c 36 34 53 75 70 70 6f 72 74 65 64 3d 4e 6f 0d 0a 44 49 46 78 41 4d 44 36 34 53 75 70 70 6f 72 74 65 64 3d 4e 6f 0d 0a	[<Properties>]..DIFx32Supported=No..DIFxIntel64Supported=No..DIFxAMD64Supported=No..	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\cor542B.tmp	unknown	32766	3b 20 43 6f 72 65 63 6f 6d 70 2e 69 6e 69 0d 0a 3b 0d 0a 3b 20 54 68 69 73 20 66 69 6c 65 20 73 74 6f 72 65 73 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 61 62 6f 75 74 20 66 69 6c 65 73 20 74 68 61 74 20 49 6e 73 74 61 6c 6c 53 68 69 65 6c 64 0d 0a 3b 20 77 69 6c 6c 20 69 6e 73 74 61 6c 6c 20 74 6f 20 74 68 65 20 57 69 6e 64 6f 77 73 5c 53 79 73 74 65 6d 20 66 6f 6c 64 65 72 2c 20 73 75 63 68 20 61 73 20 57 69 6e 64 6f 77 73 0d 0a 3b 20 39 35 20 61 6e 64 20 4e 54 20 34 2e 30 20 63 6f 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 61 6e 64 20 44 41 4f 2c 20 4f 44 42 43 2c 20 61 6e 64 20 41 63 74 69 76 65 58 20 66 69 6c 65 73 2e 0d 0a 3b 20 0d 0a 3b 20 54 68 65 20 65 6e 74 72 69 65 73 20 68 61 76 65 20 74 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 66 6f 72 6d 61 74 2c	; 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,	success or wait	3	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542C.tmp	unknown	23816	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1f d5 79 59 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 10 00 00 00 20 00 00 00 00 00 00 de 2a 00 00 00 20 00 00 00 40 00 00 00 00 00 11 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 00 00 00 10 00 00 13 e4 00 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@....................................!..L.!This program cannot be run in DOS mode....$.......PE..L.....yY.................. ....*... ...@...............................@...............................	success or wait	1	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\dot542D.tmp	unknown	146	3c 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e 0d 0a 20 20 3c 73 74 61 72 74 75 70 3e 0d 0a 20 20 20 20 3c 73 75 70 70 6f 72 74 65 64 52 75 6e 74 69 6d 65 20 76 65 72 73 69 6f 6e 3d 22 76 32 2e 30 2e 35 30 37 32 37 22 2f 3e 0d 0a 20 20 20 20 3c 73 75 70 70 6f 72 74 65 64 52 75 6e 74 69 6d 65 20 76 65 72 73 69 6f 6e 3d 22 76 34 2e 30 22 2f 3e 0d 0a 20 20 3c 2f 73 74 61 72 74 75 70 3e 0d 0a 3c 2f 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 3e	<configuration>.. <startup>.. <supportedRuntime version="v2.0.50727"/>.. <supportedRuntime version="v4.0"/>.. </startup>..</configuration>	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISB542E.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 65 88 2a d6 21 e9 44 85 21 e9 44 85 21 e9 44 85 d0 2f 8a 85 44 e9 44 85 d0 2f 89 85 28 e9 44 85 d0 2f 8b 85 16 e9 44 85 dd 9e f8 85 20 e9 44 85 21 e9 45 85 5b e9 44 85 dd 9e fd 85 2e e9 44 85 83 2e 97 85 25 e9 44 85 83 2e 8d 85 20 e9 44 85 21 e9 d3 85 20 e9 44 85 83 2e 88 85 20 e9 44 85 52 69 63 68 21 e9 44 85 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......e.*.!.D.!.D.!.D../..D. D../..(.D../....D..... .D.!.E. [.D.......D.....%.D..... .D.!... .D..... .D.Rich!.D.........	success or wait	11	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\Str542F.tmp	unknown	3854	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 39 00 5d 00 0d 00 0a 00 46 00 4f 00 4c 00 44 00 45 00 52 00 5f 00 4e 00 41 00 4d 00 45 00 3d 00 53 00 75 00 72 00 65 00 53 00 65 00 72 00 76 00 6f 00 20 00 50 00 52 00 4f 00 0d 00 0a 00 49 00 44 00 50 00 52 00 4f 00 50 00 5f 00 53 00 45 00 54 00 55 00 50 00 54 00 59 00 50 00 45 00 5f 00 43 00 4f 00 4d 00 50 00 4c 00 45 00 54 00 45 00 3d 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 65 00 0d 00 0a 00 49 00 44 00 50 00 52 00 4f 00 50 00 5f 00 53 00 45 00 54 00 55 00 50 00 54 00 59 00 50 00 45 00 5f 00 43 00 4f 00 4d 00 50 00 4c 00 45 00 54 00 45 00 5f 00 44 00 45 00 53 00 43 00 3d 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 65	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.9.].....F.O.L.D.E.R._.N.A.M.E.=.S.u.r.e.S.e.r.v.o. .P.R.O.....I.D.P.R.O.P._.S.E.T.U.P.T.Y.P.E._.C.O.M.P.L.E.T.E.=.C.o.m.p.l.e.t.e.....I.D.P.R.O.P._.S.E.T.U.P.T.Y.P.E._.C.O.M.P.L.E.T.E._.D.E.S.C.=.C.o.m.p.l.e.t.e	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isr5430.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c7 1a 49 07 83 7b 27 54 83 7b 27 54 83 7b 27 54 a4 bd e9 54 85 7b 27 54 72 bd ea 54 98 7b 27 54 21 bc e9 54 80 7b 27 54 72 bd e9 54 09 7b 27 54 72 bd e8 54 c9 7b 27 54 7f 0c 99 54 82 7b 27 54 7f 0c 9b 54 87 7b 27 54 83 7b 26 54 77 7a 27 54 7f 0c 9e 54 94 7b 27 54 21 bc e8 54 c8 7b 27 54 21 bc ed 54 82 7b 27 54 21 bc ee 54 82 7b 27 54 83 7b b0 54 82 7b 27 54 21 bc eb 54 82 7b 27	MZ......................@...!..L.!This program cannot be run in DOS mode....$.........I..{'T.{'T.{'T...T.{'Tr..T.{'T!..T.{'Tr..T.{'Tr..T.{'T...T.{'T...T.{'T.{&Twz'T...T.{'T!..T.{'T!..T.{'T!..T.{'T.{.T.{'T!..T.{'	success or wait	27	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5461.tmp	unknown	1168	52 49 46 46 88 04 00 00 50 41 4c 20 64 61 74 61 04 04 00 00 00 03 00 01 00 00 00 00 80 00 00 00 00 80 00 00 80 80 00 00 00 00 80 00 80 00 80 00 00 80 80 00 c0 c0 c0 00 c0 dc c0 00 a6 ca f0 00 ff ff cc 00 ff ff 99 00 ff ff 66 00 ff ff 33 00 ff cc ff 00 ff cc cc 00 ff cc 99 00 ff cc 66 00 ff cc 33 00 ff cc 00 00 ff 99 ff 00 ff 99 cc 00 ff 99 99 00 ff 99 66 00 ff 99 33 00 ff 99 00 00 ff 66 ff 00 ff 66 cc 00 ff 66 99 00 ff 66 66 00 ff 66 33 00 ff 66 00 00 ff 33 ff 00 ff 33 cc 00 ff 33 99 00 ff 33 66 00 ff 33 33 00 ff 33 00 00 ff 00 cc 00 ff 00 99 00 ff 00 66 00 ff 00 33 00 cc ff ff 00 cc ff cc 00 cc ff 99 00 cc ff 66 00 cc ff 33 00 cc ff 00 00 cc cc ff 00 cc cc cc 00 cc cc 99 00 cc cc 66 00 cc cc 33 00 cc cc 00 00 cc 99 ff 00 cc 99 cc 00 cc 99 99 00 cc 99 66	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	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\def5462.tmp	unknown	1168	52 49 46 46 88 04 00 00 50 41 4c 20 64 61 74 61 04 04 00 00 00 03 00 01 00 00 00 00 80 00 00 00 00 80 00 00 80 80 00 00 00 00 80 00 80 00 80 00 00 80 80 00 c0 c0 c0 00 c0 dc c0 00 a6 ca f0 00 ff ff cc 00 ff ff 99 00 ff ff 66 00 ff ff 33 00 ff cc ff 00 ff cc cc 00 ff cc 99 00 ff cc 66 00 ff cc 33 00 ff cc 00 00 ff 99 ff 00 ff 99 cc 00 ff 99 99 00 ff 99 66 00 ff 99 33 00 ff 99 00 00 ff 66 ff 00 ff 66 cc 00 ff 66 99 00 ff 66 66 00 ff 66 33 00 ff 66 00 00 ff 33 ff 00 ff 33 cc 00 ff 33 99 00 ff 33 66 00 ff 33 33 00 ff 33 00 00 ff 00 cc 00 ff 00 99 00 ff 00 66 00 ff 00 33 00 cc ff ff 00 cc ff cc 00 cc ff 99 00 cc ff 66 00 cc ff 33 00 cc ff 00 00 cc cc ff 00 cc cc cc 00 cc cc 99 00 cc cc 66 00 cc cc 33 00 cc cc 00 00 cc 99 ff 00 cc 99 cc 00 cc 99 99 00 cc 99 66	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	success or wait	1	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_is5463.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e f5 8d 28 1a 94 e3 7b 1a 94 e3 7b 1a 94 e3 7b 99 88 ed 7b 0e 94 e3 7b 2c b2 e9 7b 4a 94 e3 7b 1a 94 e2 7b 50 94 e3 7b e0 b7 fa 7b 19 94 e3 7b 2c b2 e8 7b 19 94 e3 7b dd 92 e5 7b 1b 94 e3 7b 52 69 63 68 1a 94 e3 7b 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 5b f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 a0 02 00 00 c0 19 00 00 00 00 00 80 11 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......^..(...{...{...{... {...{,..{J..{...{P..{...{...{,..{... {...{...{Rich...{........PE..L... [.yY...........!........................	success or wait	113	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Set5500.tmp	unknown	32766	74 c4 2c 84 e1 e5 d4 28 10 fb 00 20 3c 24 fb 4d 11 20 1d 3d e4 c8 cc ec e4 dc d8 dc c8 05 6c c7 bf a7 ff cf b3 10 cb b3 c7 a7 cb dc 0c 83 a3 7f 6f bb 63 93 a0 10 67 57 53 6c 98 00 53 57 88 b7 57 53 5b 2f 2f 64 93 64 20 6c 24 18 58 58 25 d1 d5 d9 dd c1 c5 c9 cd b1 b5 b9 bd a1 a5 a9 ad 91 95 99 9d 81 85 89 8d 71 87 79 7d 61 85 3d 6d 51 b5 59 5d 41 d3 20 4d 31 22 61 25 21 6f 29 b0 11 15 19 19 1d 05 09 09 0d d8 f8 f8 fc c8 e8 0e f1 dd fd fd e1 cd ed ed d1 bd dd dd c1 ad cd cd b1 9d bd bd a1 8d ad ad 91 7d 9d 9d 81 6d 8d 8d 71 5d 7d 7d 61 4d 6d 1d 55 3d 5d 01 45 2d 4d 1d 35 1d 3d e8 25 0d 2d d4 15 fc 1d dc 05 ec 0d c0 f4 dc fc 94 e4 cc f1 ad f9 c1 e1 85 e9 b1 d1 b9 d9 a1 c1 ad c9 04 b1 b5 b9 41 a1 95 a9 9d 95 95 61 9d db 28 ff f3 bb 48 b7 b7 93 c7 59 51 51 45	t.,....(... <$.M. .=.......... l.................o.c...gWSl.. SW..WS[//d.d l$.XX%........... ....q.y}a.=mQ.Y]A. M1"a%!o)........................ ....}...m..q]}}a Mm.U=].E-M.5.=.%.- ....A......a.. (...H....YQQE	success or wait	11	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Isr5530.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c7 1a 49 07 83 7b 27 54 83 7b 27 54 83 7b 27 54 a4 bd e9 54 85 7b 27 54 72 bd ea 54 98 7b 27 54 21 bc e9 54 80 7b 27 54 72 bd e9 54 09 7b 27 54 72 bd e8 54 c9 7b 27 54 7f 0c 99 54 82 7b 27 54 7f 0c 9b 54 87 7b 27 54 83 7b 26 54 77 7a 27 54 7f 0c 9e 54 94 7b 27 54 21 bc e8 54 c8 7b 27 54 21 bc ed 54 82 7b 27 54 21 bc ee 54 82 7b 27 54 83 7b b0 54 82 7b 27 54 21 bc eb 54 82 7b 27	MZ......................@...... ....!..L.!This program cannot be run in DOS mode....$.........I..{'T.{'T. {'T...T.{'Tr..T.{'T!..T.{'Tr..T. {'Tr..T.{'T...T.{'T...T.{'T. {&Twz'T...T.{'T!..T.{'T!..T. {'T!..T.{'T.{.T.{'T!..T.{'	success or wait	27	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5560.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d5 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 80 15 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@.........	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str55CE.tmp	unknown	4336	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 63 00 30 00 63 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 55 00 6e 00 65 00 20 00 65 00 72 00 72 00 65 00 75 00 72 00 20 00 69 00 6e 00 63 00 6f 00 6e 00 6e 00 75 00 65 00 20 00 61 00 20 00 e9 00 74 00 e9 00 20 00 72 00 65 00 6e 00 76 00 6f 00 79 00 e9 00 65 00 20 00 70 00 61 00 72 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 45 00 72 00 72 00 65 00 75 00 72 00 20 00 73 00 79 00 73 00 74 00 e8 00 6d 00 65 00 a0 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49	..[.S.t.r.i.n.g.T.a.b.l.e.:.D. a.t.a.:.0.c.0.c.].....I.D.S._. E.R.R.O.R._.2.7.5.3.0.=.U. n.e. .e.r.r.e.u.r. .i.n.c.o.n.n.u.e. .a. ...t... .r.e.n.v.o.y...e. .p.a.r. .N.e.t.A.P.I...E.r.r.e.u.r. .s.y.s.t...m.e...:. . [.2.].....I.D.S._.I.N.S.T.A.L. L.I.N.G._.M.S.I	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is55FE.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c0 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5757.tmp	unknown	4088	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 63 00 31 00 61 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 1d 04 35 04 3f 04 3e 04 37 04 3d 04 30 04 42 04 30 04 20 00 33 04 40 04 35 04 48 04 3a 04 30 04 20 00 32 04 40 04 30 04 5b 04 35 04 3d 04 30 04 20 00 3e 04 34 04 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 21 04 38 04 41 04 42 04 35 04 3c 04 41 04 3a 04 30 04 20 00 33 04 40 04 35 04 48 04 3a 04 30 04 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.c.1.a.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=...5.?.>.7.=.0.B.0..3.@.5.H.:.0. .2.@.0.[.5.=.0. .>.4. .N.e.t.A.P.I....!.8.A.B.5.<.A.:.0. .3.@.5.H.:.0.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5758.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 72 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 80 15 00 00 00 00	MZ......................@...................................!..L.!This program cannot be run in DOS mode....$.......r...6...6...6.......".........6...w.......5.......5.......7...Rich6..................PE..L...r.yY...........!.....@.........	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str57C6.tmp	unknown	4114	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 61 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 53 00 65 00 20 00 68 00 61 00 20 00 72 00 65 00 63 00 69 00 62 00 69 00 64 00 6f 00 20 00 75 00 6e 00 20 00 65 00 72 00 72 00 6f 00 72 00 20 00 64 00 65 00 73 00 63 00 6f 00 6e 00 6f 00 63 00 69 00 64 00 6f 00 20 00 64 00 65 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 45 00 72 00 72 00 6f 00 72 00 20 00 64 00 65 00 6c 00 20 00 73 00 69 00 73 00 74 00 65 00 6d 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.a.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.S.e. .h.a. .r.e.c.i.b.i.d.o. .u.n. .e.r.r.o.r. .d.e.s.c.o.n.o.c.i.d.o. .d.e. .N.e.t.A.P.I... .E.r.r.o.r. .d.e.l. .s.i.s.t.e.m.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is57C7.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 75 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 40 15 00 00 00 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......r...6...6...6.......".........6...w.......5.......5.......7...Rich6..................PE..L...u.yY...........!.....@...@.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5826.tmp	unknown	4050	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 62 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 70 00 61 00 6c 00 61 00 75 00 74 00 74 00 69 00 20 00 74 00 75 00 6e 00 74 00 65 00 6d 00 61 00 74 00 74 00 6f 00 6d 00 61 00 6e 00 20 00 76 00 69 00 72 00 68 00 65 00 65 00 6e 00 2e 00 20 00 4a 00 e4 00 72 00 6a 00 65 00 73 00 74 00 65 00 6c 00 6d 00 e4 00 76 00 69 00 72 00 68 00 65 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.b.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .p.a.l.a.u.t.t.i. .t.u.n.t.e.m.a.t.t.o.m.a.n. .v.i.r.h.e.e.n... .J...r.j.e.s.t.e.l.m...v.i.r.h.e.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5827.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c9 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 80 15 00 00 00 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......r...6...6...6.......".........6...w.......5.......5.......7...Rich6...................PE..L.....yY...........!.....@.........	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5895.tmp	unknown	4284	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 63 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 55 00 6e 00 65 00 20 00 65 00 72 00 72 00 65 00 75 00 72 00 20 00 69 00 6e 00 63 00 6f 00 6e 00 6e 00 75 00 65 00 20 00 61 00 20 00 e9 00 74 00 e9 00 20 00 72 00 65 00 6e 00 76 00 6f 00 79 00 e9 00 65 00 20 00 70 00 61 00 72 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 45 00 72 00 72 00 65 00 75 00 72 00 20 00 73 00 79 00 73 00 74 00 e8 00 6d 00 65 00 a0 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.c.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.U.n.e. .e.r.r.e.u.r. .i.n.c.o.n.n.u.e. .a. ...t... .r.e.n.v.o.y...e. .p.a.r. .N.e.t.A.P.I... .E.r.r.e.u.r. .s.y.s.t...m.e...:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5896.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 79 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L...y.yY...........! .....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str58F5.tmp	unknown	3966	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 65 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 49 00 73 00 6d 00 65 00 72 00 65 00 74 00 6c 00 65 00 6e 00 20 00 68 00 69 00 62 00 61 00 20 00 61 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2d 00 72 00 f3 00 6c 00 2e 00 20 00 52 00 65 00 6e 00 64 00 73 00 7a 00 65 00 72 00 68 00 69 00 62 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20 00 4d 00 73 00 69 00 20 00 31	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.e.]....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.I.s.m.e.r.e.t.l.e.n. .h.i.b.a. .a. .N.e.t.A.P.I.-.r...l... .R.e.n.d.s.z.e.r.h.i.b.a.:. .[.2.]....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is58F6.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 98 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@...................................!..L.!This program cannot be run in DOS mode....$.......r...6...6...6.......".........6...w.......5.......5.......7...Rich6..................PE..L.....yY...........!.....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5993.tmp	unknown	4144	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 61 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 6a 00 61 00 76 00 6c 00 6a 00 61 00 20 00 6e 00 65 00 70 00 6f 00 7a 00 6e 00 61 00 74 00 75 00 20 00 67 00 72 00 65 00 61 01 6b 00 75 00 2e 00 20 00 47 00 72 00 65 00 61 01 6b 00 61 00 20 00 73 00 75 00 73 00 74 00 61 00 76 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20 00 4d	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.a.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .j.a.v.l.j.a. .n.e.p.o.z.n.a.t.u. .g.r.e.a.k.u... .G.r.e.a.k.a. .s.u.s.t.a.v.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5994.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9c f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str59F3.tmp	unknown	4208	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 62 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 5a 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 73 00 61 00 20 00 76 00 72 00 e1 00 74 00 69 00 6c 00 61 00 20 00 6e 00 65 00 7a 00 6e 00 e1 00 6d 00 61 00 20 00 63 00 68 00 79 00 62 00 61 00 2e 00 20 00 53 00 79 00 73 00 74 00 e9 00 6d 00 6f 00 76 00 e1 00 20 00 63 00 68 00 79 00 62 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.b.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.Z. .N.e.t.A.P.I. .s.a. .v.r...t.i.l.a. .n.e.z.n...m.a. .c.h.y.b.a... .S.y.s.t...m.o.v... .c.h.y.b.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is59F4.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 9e f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 40 15 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...@.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5B8B.tmp	unknown	4224	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 64 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 45 00 74 00 74 00 20 00 6f 00 6b 00 e4 00 6e 00 74 00 20 00 66 00 65 00 6c 00 20 00 72 00 65 00 74 00 75 00 72 00 6e 00 65 00 72 00 61 00 64 00 65 00 73 00 20 00 66 00 72 00 e5 00 6e 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 53 00 79 00 73 00 74 00 65 00 6d 00 66 00 65 00 6c 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.d.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.E.t.t. .o.k...n.t. .f.e.l. .r.e.t.u.r.n.e.r.a.d.e.s. .f.r...n. .N.e.t.A.P.I... .S.y.s.t.e.m.f.e.l.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5B8C.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a5 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 40 15 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...@.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C1A.tmp	unknown	4084	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 65 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 21 0e 35 0e 02 0e 49 0e 2d 0e 1c 0e 34 0e 14 0e 1e 0e 25 0e 32 0e 14 0e 17 0e 35 0e 48 0e 44 0e 21 0e 48 0e 04 0e 32 0e 14 0e 04 0e 34 0e 14 0e 16 0e 39 0e 01 0e 2a 0e 48 0e 07 0e 01 0e 25 0e 31 0e 1a 0e 08 0e 32 0e 01 0e 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 02 0e 49 0e 2d 0e 1c 0e 34 0e 14 0e 1e 0e 25 0e 32 0e 14 0e 23 0e 30 0e 1a 0e 1a 0e 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.e.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.!.5...I.-...4.....%.2.....5.H.D.!.H...2.....4.....9...*.H.....%.1.....2... .N.e.t.A.P.I. ...I.-...4.....%.2...#.0.....:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C1B.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 aa f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 40 15 00 00 00 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......r...6...6...6.......".........6...w.......5.......5.......7...Rich6..................PE..L.....yY...........!.....@...@.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5C89.tmp	unknown	3970	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 66 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 19 20 64 00 65 00 6e 00 20 00 62 00 69 00 6c 00 69 00 6e 00 6d 00 65 00 79 00 65 00 6e 00 20 00 68 00 61 00 74 00 61 00 20 00 64 00 f6 00 6e 00 64 00 fc 00 72 00 fc 00 6c 00 64 00 fc 00 2e 00 20 00 53 00 69 00 73 00 74 00 65 00 6d 00 20 00 68 00 61 00 74 00 61 00 73 00 31 01 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.f.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I.. d.e.n. .b.i.l.i.n.m.e.y.e.n. .h.a.t.a. .d...n.d...r...l.d..... .S.i.s.t.e.m. .h.a.t.a.s.1.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5C8A.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 b5 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5CE9.tmp	unknown	4116	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 32 00 64 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 45 00 72 00 72 00 6f 00 72 00 65 00 20 00 65 00 7a 00 65 00 7a 00 61 00 67 00 75 00 6e 00 61 00 20 00 69 00 74 00 7a 00 75 00 6c 00 69 00 20 00 64 00 61 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2d 00 74 00 69 00 6b 00 2e 00 20 00 53 00 69 00 73 00 74 00 65 00 6d 00 61 00 2d 00 65 00 72 00 72 00 6f 00 72 00 65 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74	..[.S.t.r.i.n.g.T.a.b.l.e.:.D. a.t.a.:.0.4.2.d.].....I.D.S._. E.R.R.O.R._.2.7.5.3.0.=.E. r.r.o.r.e. .e.z.e.z.a.g.u.n.a. .i.t.z.u.l.i. .d.a. .N.e.t.A.P.I.- .t.i.k... .S.i.s.t.e.m.a.-.e. r.r.o.r.e.a.:. .[.2.].....I.D. S._.I.N.S.T.A.L.L.I.N.G._. M.S.I.1.2.=.I.n.s.t	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5CEA.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 b7 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 60 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...`.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5D49.tmp	unknown	4066	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 1e 04 42 04 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 35 04 20 00 32 04 4a 04 40 04 3d 04 30 04 42 04 30 04 20 00 3d 04 35 04 38 04 37 04 32 04 35 04 41 04 42 04 3d 04 30 04 20 00 33 04 40 04 35 04 48 04 3a 04 30 04 2e 00 20 00 21 04 38 04 41 04 42 04 35 04 3c 04 3d 04 30 04 20 00 33 04 40 04 35 04 48 04 3a 04 30 04 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74	..[.S.t.r.i.n.g.T.a.b.l.e.:.D. a.t.a.:.0.4.0.2.].....I.D.S._. E.R.R.O.R._.2.7.5.3.0.=... B. .N.e.t.A.P.I. .5. .2.J.@.=.0.B.0. .=.5.8.7.2.5.A.B.=.0. .3.@. 5.H.:.0... .!.8.A.B.5.<.=.0. . 3.@.5.H.:.0.:. .[.2.].....I.D. S._.I.N.S.T.A.L.L.I.N.G._. M.S.I.1.2.=.I.n.s.t	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5D4A.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 60 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 70 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L...`.yY...........! .....@...p.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str5DE7.tmp	unknown	4178	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 33 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 68 00 61 00 20 00 72 00 65 00 74 00 6f 00 72 00 6e 00 61 00 74 00 20 00 75 00 6e 00 20 00 65 00 72 00 72 00 6f 00 72 00 20 00 64 00 65 00 73 00 63 00 6f 00 6e 00 65 00 67 00 75 00 74 00 2e 00 20 00 45 00 72 00 72 00 6f 00 72 00 20 00 64 00 65 00 6c 00 20 00 73 00 69 00 73 00 74 00 65 00 6d 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.3.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .h.a. .r.e.t.o.r.n.a.t. .u.n. .e.r.r.o.r. .d.e.s.c.o.n.e.g.u.t... .E.r.r.o.r. .d.e.l. .s.i.s.t.e.m.a.:. .[.2.]... ..I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is5DE8.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c3 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 80 14 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@.........	success or wait	83	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str61D1.tmp	unknown	3418	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 34 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 b3 50 de 56 00 4e 0b 50 2f 93 a4 8a 0c ff 9f 53 e0 56 0d 4e 0e 66 02 30 20 00 fb 7c 71 7d 2f 93 a4 8a 55 fe 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20 00 4d 00 73 00 69 00 20 00 31 00 2e 00 32 00 20 00 45 00 6e 00 67 00 69 00 6e 00 65 00 2e 00 2e 00 2e 00 0d 00 0a 00 49 00 44 00 53 00 5f	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.4.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. ..P.V.N.P/......S.V.N.f.0 ..|q}/...U. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e... ........I.D.S._	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is61D2.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 61 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 40 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L...a.yY...........! .....@...@.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str626F.tmp	unknown	4002	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 35 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 52 00 6f 00 7a 00 68 00 72 00 61 00 6e 00 ed 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 76 00 72 00 e1 00 74 00 69 00 6c 00 6f 00 20 00 6e 00 65 00 7a 00 6e 00 e1 00 6d 00 6f 00 75 00 20 00 63 00 68 00 79 00 62 00 75 00 2e 00 20 00 53 00 79 00 73 00 74 00 e9 00 6d 00 6f 00 76 00 e1 00 20 00 63 00 68 00 79 00 62 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.5.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.R.o.z.h.r.a.n... .N.e.t.A.P.I. .v.r...t.i.l.o. .n.e.z.n...m.o.u. .c.h.y.b.u... .S.y.s.t...m.o.v... .c.h.y.b.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6270.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 66 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L...f.yY...........! .....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str62FE.tmp	unknown	4078	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 36 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 55 00 6b 00 65 00 6e 00 64 00 74 00 20 00 66 00 65 00 6a 00 6c 00 20 00 72 00 65 00 74 00 75 00 72 00 6e 00 65 00 72 00 65 00 74 00 20 00 66 00 72 00 61 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 53 00 79 00 73 00 74 00 65 00 6d 00 66 00 65 00 6a 00 6c 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20 00 4d 00 73	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.6.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.U.k.e.n.d.t. .f.e.j.l. .r.e.t.u.r.n.e.r.e.t. .f.r.a. .N.e.t.A.P.I... .S.y.s.t.e.m.f.e.j.l.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is632E.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 6c f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 80 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L...l.yY...........! .....@.........	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str636D.tmp	unknown	4716	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 37 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 68 00 61 00 74 00 20 00 65 00 69 00 6e 00 65 00 6e 00 20 00 75 00 6e 00 62 00 65 00 6b 00 61 00 6e 00 6e 00 74 00 65 00 6e 00 20 00 46 00 65 00 68 00 6c 00 65 00 72 00 20 00 7a 00 75 00 72 00 fc 00 63 00 6b 00 67 00 65 00 67 00 65 00 62 00 65 00 6e 00 2e 00 20 00 53 00 79 00 73 00 74 00 65 00 6d 00 66 00 65 00 68 00 6c 00 65 00 72 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.7.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .h.a.t. .e.i.n.e.n. .u.n.b.e.k.a.n.n.t.e.n. .F.e.h.l.e.r. .z.u.r...c.k.g.e.g.e.b.e.n... .S.y.s.t.e.m.f.e.h.l.e.r.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is636E.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 70 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 80 15 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L...p.yY...........! .....@.........	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str63FC.tmp	unknown	4136	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 38 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 86 03 b3 03 bd 03 c9 03 c3 03 c4 03 bf 03 20 00 c3 03 c6 03 ac 03 bb 03 bc 03 b1 03 20 00 b1 03 c0 03 cc 03 20 00 c4 03 bf 03 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 a3 03 c6 03 ac 03 bb 03 bc 03 b1 03 20 00 c3 03 c5 03 c3 03 c4 03 ae 03 bc 03 b1 03 c4 03 bf 03 c2 03 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.8.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=............... ....N.e.t.A.P.I... ....:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g.	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is63FD.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e f5 8d 28 1a 94 e3 7b 1a 94 e3 7b 1a 94 e3 7b 99 88 ed 7b 0e 94 e3 7b 2c b2 e9 7b 4a 94 e3 7b 1a 94 e2 7b 50 94 e3 7b e0 b7 fa 7b 19 94 e3 7b 2c b2 e8 7b 19 94 e3 7b dd 92 e5 7b 1b 94 e3 7b 52 69 63 68 1a 94 e3 7b 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 5b f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 a0 02 00 00 c0 19 00 00 00 00 00 80 11 00 00 00 10 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......^..(...{...{...{...{...{,..{J..{...{P..{...{...{,..{...{...{...{Rich...{........PE..L...[.yY...........!.......................	success or wait	113	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str646B.tmp	unknown	4868	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 30 00 39 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 31 00 32 00 38 00 3d 00 54 00 68 00 65 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 65 00 72 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 63 00 61 00 6e 00 6e 00 6f 00 74 00 20 00 75 00 70 00 64 00 61 00 74 00 65 00 20 00 6f 00 6e 00 65 00 20 00 6f 00 72 00 20 00 6d 00 6f 00 72 00 65 00 20 00 70 00 72 00 6f 00 74 00 65 00 63 00 74 00 65 00 64 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 66 00 69 00 6c 00 65 00 73 00 2e 00 20 00 53 00 46 00 50 00 20 00 45 00 72 00 72	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.0.9.].....I.D.S._.E.R.R.O.R._.1.2.8.=.T.h.e. .W.i.n.d.o.w.s. .I.n.s.t.a.l.l.e.r. .s.e.r.v.i.c.e. .c.a.n.n.o.t. .u.p.d.a.t.e. .o.n.e. .o.r. .m.o.r.e. .p.r.o.t.e.c.t.e.d. .W.i.n.d.o.w.s. .f.i.l.e.s... .S.F.P. .E.r.r	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is646C.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7f f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 60 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...`.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str64CB.tmp	unknown	4230	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 30 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 68 00 61 00 20 00 72 00 65 00 73 00 74 00 69 00 74 00 75 00 69 00 74 00 6f 00 20 00 75 00 6e 00 20 00 65 00 72 00 72 00 6f 00 72 00 65 00 20 00 73 00 63 00 6f 00 6e 00 6f 00 73 00 63 00 69 00 75 00 74 00 6f 00 2e 00 20 00 45 00 72 00 72 00 6f 00 72 00 65 00 20 00 64 00 69 00 20 00 73 00 69 00 73 00 74 00 65 00 6d 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.0.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .h.a. .r.e.s.t.i.t.u.i.t.o. .u.n. .e.r.r.o.r.e. .s.c.o.n.o.s.c.i.u.t.o... .E.r.r.o.r.e. .d.i. .s.i.s.t.e.m.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is64CC.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 82 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 d0 14 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@.........	success or wait	85	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str652B.tmp	unknown	3996	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 31 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 4b 30 89 30 0d 4e 0e 66 6a 30 a8 30 e9 30 fc 30 4c 30 d4 8f 55 30 8c 30 7e 30 57 30 5f 30 02 30 20 00 b7 30 b9 30 c6 30 e0 30 20 00 a8 30 e9 30 fc 30 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20 00 4d 00 73 00 69 00 20 00 31 00 2e 00 32 00 20 00 45 00 6e 00 67 00 69 00 6e 00 65 00 2e	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.1.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .K0.0.N.fj0.0.0.0L0..U0 .0~0W0_0.0 ..0.0.0.0 ..0.0.0:. . [.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e..	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is656A.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 84 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 b0 14 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@.........	success or wait	85	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str65C9.tmp	unknown	3618	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 5c b8 80 bd 30 d1 20 00 4c c5 20 00 18 c2 20 00 c6 c5 94 b2 20 00 24 c6 58 b9 00 ac 20 00 18 bc 58 d6 18 b4 c8 c5 b5 c2 c8 b2 e4 b2 2e 00 20 00 dc c2 a4 c2 5c d1 20 00 24 c6 58 b9 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20 00 4d 00 73 00 69 00 20 00 31 00 2e 00 32 00 20 00 45 00 6e 00 67	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.2.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I.\...0. .L. ... .$.X... ...X............ .....\. .$.X.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is65CA.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 8a f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 60 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...`.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6667.tmp	unknown	4174	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 33 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4f 00 6e 00 62 00 65 00 6b 00 65 00 6e 00 64 00 65 00 20 00 66 00 6f 00 75 00 74 00 20 00 67 00 65 00 72 00 65 00 74 00 6f 00 75 00 72 00 6e 00 65 00 65 00 72 00 64 00 20 00 76 00 61 00 6e 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 53 00 79 00 73 00 74 00 65 00 65 00 6d 00 66 00 6f 00 75 00 74 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.3.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.O.n.b.e.k.e.n.d.e. .f.o.u.t. .g.e.r.e.t.o.u.r.n.e.e.r.d. .v.a.n. .N.e.t.A.P.I... .S.y.s.t.e.e.m.f.o.u.t.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6668.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 8d f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str66C7.tmp	unknown	4122	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 34 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 72 00 65 00 74 00 75 00 72 00 6e 00 65 00 72 00 74 00 65 00 20 00 75 00 6b 00 6a 00 65 00 6e 00 74 00 20 00 66 00 65 00 69 00 6c 00 2e 00 20 00 53 00 79 00 73 00 74 00 65 00 6d 00 66 00 65 00 69 00 6c 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20 00 4d 00 73 00 69 00 20 00 31 00 2e	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.4.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .r.e.t.u.r.n.e.r.t.e. .u.k.j.e.n.t. .f.e.i.l... .S.y.s.t.e.m.f.e.i.l.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1..	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is66F7.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 8f f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 60 15 00 00 00 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......r...6...6...6.......".........6...w.......5.......5.......7...Rich6..................PE..L.....yY...........!.....@...`.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6765.tmp	unknown	4276	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 35 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 49 00 6e 00 74 00 65 00 72 00 66 00 65 00 6a 00 73 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 7a 00 77 00 72 00 f3 00 63 00 69 00 42 01 20 00 6e 00 69 00 65 00 7a 00 6e 00 61 00 6e 00 79 00 20 00 62 00 42 01 05 01 64 00 2e 00 20 00 42 00 42 01 05 01 64 00 20 00 73 00 79 00 73 00 74 00 65 00 6d 00 6f 00 77 00 79 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74	..[.S.t.r.i.n.g.T.a.b.l.e.:.D. a.t.a.:.0.4.1.5.].....I.D.S._. E.R.R.O.R._.2.7.5.3.0.=.I.n .t.e.r.f.e.j.s. .N.e.t.A.P.I. .z. w.r...c.i.B. .n.i.e.z.n.a.n.y. .b.B...d... .B.B...d. .s.y.s. t.e.m.o.w.y.:. .[.2.].....I.D. S._.I.N.S.T.A.L.L.I.N.G._. M.S.I.1.2.=.I.n.s.t	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6766.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 cc f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 60 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...`.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6823.tmp	unknown	4094	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 36 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 72 00 65 00 74 00 6f 00 72 00 6e 00 6f 00 75 00 20 00 75 00 6d 00 20 00 65 00 72 00 72 00 6f 00 20 00 64 00 65 00 73 00 63 00 6f 00 6e 00 68 00 65 00 63 00 69 00 64 00 6f 00 2e 00 20 00 45 00 72 00 72 00 6f 00 20 00 64 00 6f 00 20 00 73 00 69 00 73 00 74 00 65 00 6d 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.6.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .r.e.t.o.r.n.o.u. .u.m. .e.r.r.o. .d.e.s.c.o.n.h.e.c.i.d.o... .E.r.r.o. .d.o. .s.i.s.t.e.m.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6824.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 bc f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 70 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...p.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6892.tmp	unknown	4326	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 38 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 45 00 72 00 6f 00 61 00 72 00 65 00 20 00 6e 00 65 00 63 00 75 00 6e 00 6f 00 73 00 63 00 75 00 74 00 03 01 20 00 72 00 65 00 74 00 75 00 72 00 6e 00 61 00 74 00 03 01 20 00 64 00 65 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 45 00 72 00 6f 00 61 00 72 00 65 00 20 00 64 00 65 00 20 00 73 00 69 00 73 00 74 00 65 00 6d 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.8.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.E.r.o.a.r.e. .n.e.c.u.n.o.s.c.u.t... .r.e.t.u.r.n.a.t... .d.e. .N.e.t.A.P.I... .E.r.o.a.r.e. .d.e. .s.i.s.t.e.m.:. .[.2.]..... I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6893.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 94 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6921.tmp	unknown	4044	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 31 00 39 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 1d 04 35 04 38 04 37 04 32 04 35 04 41 04 42 04 3d 04 30 04 4f 04 20 00 3e 04 48 04 38 04 31 04 3a 04 30 04 2c 00 20 00 32 04 4b 04 34 04 30 04 3d 04 3d 04 30 04 4f 04 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 21 04 38 04 41 04 42 04 35 04 3c 04 3d 04 30 04 4f 04 20 00 3e 04 48 04 38 04 31 04 3a 04 30 04 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 61	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.1.9.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=...5.8.7.2.5.A.B.=.0.O..>.H.8.1.:.0.,..2.K.4.0.=.=.0.O. .N.e.t.A.P.I... .!.8.A.B.5.<.=.0.O. .>.H.8.1.:.0.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6922.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ae f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......r...6...6...6.......".........6...w.......5.......5.......7...Rich6..................PE..L.....yY...........!.....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str69BF.tmp	unknown	4106	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 32 00 31 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4b 00 65 00 73 00 61 00 6c 00 61 00 68 00 61 00 6e 00 20 00 74 00 61 00 6b 00 20 00 64 00 69 00 6b 00 65 00 6e 00 61 00 6c 00 20 00 64 00 69 00 6b 00 65 00 6d 00 62 00 61 00 6c 00 69 00 6b 00 61 00 6e 00 20 00 64 00 61 00 72 00 69 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 4b 00 65 00 73 00 61 00 6c 00 61 00 68 00 61 00 6e 00 20 00 73 00 69 00 73 00 74 00 65 00 6d 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.2.1.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.K.e.s.a.l.a.h.a.n. .t.a.k. .d.i.k.e.n.a.l. .d.i.k.e.m.b.a.l.i.k.a.n. .d.a.r.i. .N.e.t.A.P.I... .K.e.s.a.l.a.h.a.n. .s.i.s.t.e.m.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is69C0.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 b1 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 50 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@...P.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A1F.tmp	unknown	4066	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 34 00 32 00 34 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 6a 00 65 00 20 00 76 00 72 00 6e 00 69 00 6c 00 20 00 6e 00 65 00 7a 00 6e 00 61 00 6e 00 6f 00 20 00 6e 00 61 00 70 00 61 00 6b 00 6f 00 2e 00 20 00 53 00 69 00 73 00 74 00 65 00 6d 00 73 00 6b 00 61 00 20 00 6e 00 61 00 70 00 61 00 6b 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.4.2.4.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. .j.e. .v.r.n.i.l. .n.e.z.n.a.n.o. .n.a.p.a.k.o... .S.i.s.t.e.m.s.k.a. .n.a.p.a.k.a.:. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6A20.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d0 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 80 14 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............. ......PE..L.....yY...........! .....@.........	success or wait	83	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6A8E.tmp	unknown	3428	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 38 00 30 00 34 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 4e 00 65 00 74 00 41 00 50 00 49 00 20 00 d4 8f de 56 00 4e 2a 4e 19 95 ef 8b 0c ff 9f 53 e0 56 0d 4e e6 8b 02 30 20 00 fb 7c df 7e 19 95 ef 8b 55 fe 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 69 00 6e 00 67 00 20 00 4d 00 73 00 69 00 20 00 31 00 2e 00 32 00 20 00 45 00 6e 00 67 00 69 00 6e 00 65 00 2e 00 2e 00 2e 00 0d 00 0a 00 49 00 44 00 53 00 5f	..[.S.t.r.i.n.g.T.a.b.l.e.:.D.a.t.a.:.0.8.0.4.].....I.D.S._.E.R.R.O.R._.2.7.5.3.0.=.N.e.t.A.P.I. ....V.N*N.......S.V.N...0 ..|.~....U. .[.2.].....I.D.S._.I.N.S.T.A.L.L.I.N.G._.M.S.I.1.2.=.I.n.s.t.a.l.l.i.n.g. .M.s.i. .1...2. .E.n.g.i.n.e... ........I.D.S._	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_is6ABE.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 72 ff c1 d4 36 9e af 87 36 9e af 87 36 9e af 87 b5 82 a1 87 22 9e af 87 00 b8 a5 87 0e 9e af 87 36 9e ae 87 77 9e af 87 cc bd b6 87 35 9e af 87 00 b8 a4 87 35 9e af 87 f1 98 a9 87 37 9e af 87 52 69 63 68 36 9e af 87 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 d1 f3 79 59 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 00 40 00 00 00 70 15 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......r...6...6...6.......". ....6...w.......5....... 5.......7...Rich6............ ......PE..L.....yY...........! .....@...p.....	success or wait	87	1003BA34	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Str6B1D.tmp	unknown	4062	ff fe 5b 00 53 00 74 00 72 00 69 00 6e 00 67 00 54 00 61 00 62 00 6c 00 65 00 3a 00 44 00 61 00 74 00 61 00 3a 00 30 00 38 00 31 00 36 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 45 00 52 00 52 00 4f 00 52 00 5f 00 32 00 37 00 35 00 33 00 30 00 3d 00 45 00 72 00 72 00 6f 00 20 00 64 00 65 00 73 00 63 00 6f 00 6e 00 68 00 65 00 63 00 69 00 64 00 6f 00 20 00 69 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 64 00 6f 00 20 00 70 00 6f 00 72 00 20 00 4e 00 65 00 74 00 41 00 50 00 49 00 2e 00 20 00 45 00 72 00 72 00 6f 00 20 00 64 00 65 00 20 00 73 00 69 00 73 00 74 00 65 00 6d 00 61 00 3a 00 20 00 5b 00 32 00 5d 00 0d 00 0a 00 49 00 44 00 53 00 5f 00 49 00 4e 00 53 00 54 00 41 00 4c 00 4c 00 49 00 4e 00 47 00 5f 00 4d 00 53 00 49 00 31 00 32 00 3d 00 49 00 6e 00 73	..[.S.t.r.i.n.g.T.a.b.l.e.:.D. a.t.a.:.0.8.1.6.].....I.D.S._. E.R.R.O.R._.2.7.5.3.0.=.E. r.r.o. .d.e.s.c.o.n.h.e.c.i.d.o. . i.n.f.o.r.m.a.d.o. .p.o.r. .N. e.t.A.P.I... .E.r.r.o. .d.e. . s.i.s.t.e.m.a.:. .[.2.].....I. D.S._.I.N.S.T.A.L.L.I.N.G._ .M.S.I.1.2.=.I.n.s	success or wait	1	1003BA34	WriteFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\MMO6B1E.tmp	unknown	32766	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 f6 4f fc 9a b2 2e 92 c9 b2 2e 92 c9 b2 2e 92 c9 31 32 9c c9 a6 2e 92 c9 84 08 98 c9 8b 2e 92 c9 48 0d 8b c9 b5 2e 92 c9 b2 2e 93 c9 f4 2e 92 c9 84 08 99 c9 b0 2e 92 c9 75 28 94 c9 b3 2e 92 c9 4d 0e 96 c9 b3 2e 92 c9 52 69 63 68 b2 2e 92 c9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 4a f5 79 59 00 00 00 00 00 00 00 00 e0 00 0e	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........O..............12.... ....H.................. ....u(......M.......Rich...... ......................PE..L... J.yY...........	success or wait	3	1003BA34	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe	unknown	3	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	unknown	2424	success or wait	1	42ABB2	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.exe	unknown	2	success or wait	1	4155E1	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\0x0409.ini	unknown	32768	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\0x0409.ini	unknown	32768	end of file	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\ISSetup.dll	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\ISSetup.dll	unknown	3	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\ISSetup.dll	unknown	32768	end of file	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	22490	success or wait	1	42ABB2	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	unknown	46	success or wait	1	100B8373	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	unknown	46	end of file	1	100B83E7	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	unknown	46	success or wait	1	100B8373	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\ISSetup.dll	unknown	46	end of file	1	100B83E7	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\setup.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\0x0409.ini	unknown	2	success or wait	1	4155E1	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.hdr	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.hdr	unknown	3	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\layout.bin	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\layout.bin	unknown	3	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\layout.bin	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.hdr	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	unknown	3	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.inx	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.inx	unknown	3	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\setup.inx	unknown	32768	success or wait	8	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	unknown	2	success or wait	10	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	unknown	3	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	unknown	1168	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{13FF6051-2C7F-44D5-BA42-894B5CE410C5}\Disk1\data1.cab	unknown	2	success or wait	69	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	unknown	2	access denied	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Def5460.tmp	unknown	3	access denied	1	1003B9AA	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Setup.inx	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\Setup.inx	unknown	3	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\lsrt.dll	unknown	512	success or wait	846	10042C7E	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}_isres_0x0409.dll	unknown	512	success or wait	3639	10042C7E	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0409.ips	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{8DA8AB7C-68BD-40BE-B843-21CE4CD3DBA4}\StringTable_0x0409.ips	unknown	4868	success or wait	1	10056ADC	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\setup.inx	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\setup.inx	unknown	3	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isrt.dll	unknown	512	success or wait	846	10042C7E	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_isres_0x0409.dll	unknown	512	success or wait	3639	10042C7E	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\StringTable_0x0409.ips	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\StringTable_0x0409.ips	unknown	3854	success or wait	1	10056ADC	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\corecomp.ini	unknown	65503	success or wait	1	1007298C	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\setup.inx	unknown	2	success or wait	1	1003B9AA	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}\isrt.dll	unknown	512	success or wait	846	10042C7E	ReadFile
C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\{62E0592E-B1C0-499B-83F6-829789BDBD51}_isres_0x0409.dll	unknown	512	success or wait	3639	10042C7E	ReadFile

Analysis Process: ISBEW64.exe PID: 6544 Parent PID: 6356

General

Start time:	18:08:38
Start date:	29/03/2021
Path:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{B8FD074B-9EF5-416D-A3EE-6D8FB115C83F}
Imagebase:	0x7ff7f3980000
File size:	182008 bytes
MD5 hash:	8A1E5A6B1C4E0C7D706EB2B36FA6C8EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ISBEW64.exe PID: 6584 Parent PID: 6356

General

Start time:	18:08:39
Start date:	29/03/2021
Path:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{3BED6DCE-3BD7-42E3-BF6F-81E3F37201FD}
Imagebase:	0x7ff7f3980000

File size:	182008 bytes
MD5 hash:	8A1E5A6B1C4E0C7D706EB2B36FA6C8EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ISBEW64.exe PID: 6624 Parent PID: 6356

General

Start time:	18:08:39
Start date:	29/03/2021
Path:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{30C7FFBC-292B-4310-AFE7-0365F4C35832}
Imagebase:	0x7ff7f3980000
File size:	182008 bytes
MD5 hash:	8A1E5A6B1C4E0C7D706EB2B36FA6C8EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ISBEW64.exe PID: 6656 Parent PID: 6356

General

Start time:	18:08:39
Start date:	29/03/2021
Path:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{C15C7E7D-7890-420A-86BA-7E9024358B47}
Imagebase:	0x7ff7f3980000
File size:	182008 bytes
MD5 hash:	8A1E5A6B1C4E0C7D706EB2B36FA6C8EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ISBEW64.exe PID: 6696 Parent PID: 6356

General

Start time:	18:08:40
Start date:	29/03/2021
Path:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{6332241F-264C-4388-88EB-7A98CF4DBA83}
Imagebase:	0x7ff7f3980000
File size:	182008 bytes
MD5 hash:	8A1E5A6B1C4E0C7D706EB2B36FA6C8EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ISBEW64.exe PID: 6744 Parent PID: 6356

General

Start time:	18:08:41
Start date:	29/03/2021
Path:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{D1BE9E7C-E67D-4CF9-BA65-428ACD016A71}
Imagebase:	0x7ff7f3980000
File size:	182008 bytes
MD5 hash:	8A1E5A6B1C4E0C7D706EB2B36FA6C8EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ISBEW64.exe PID: 6784 Parent PID: 6356

General

Start time:	18:08:42
Start date:	29/03/2021
Path:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\{5A5FC2C6-9262-4BBA-8AD9-F7AEF29201FF}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}:{176CEB1A-A045-48A9-ADF5-06CDBA606E31}
Imagebase:	0x7ff7f3980000
File size:	182008 bytes
MD5 hash:	8A1E5A6B1C4E0C7D706EB2B36FA6C8EA
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis