ID: 413056
Sample Name: SophosSetup (9).exe
Cookbook: default.jbs
Time: 07:25:49
Date: 13/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

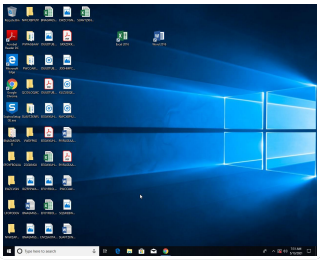
Analysis Report SophosSetup (9).exe

Overview

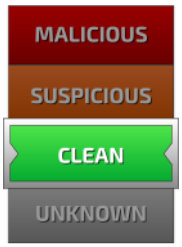
General Information

Sample Name:	SophosSetup (9).exe
Analysis ID:	413056
MD5:	070002b28e379e..
SHA1:	db19c547d72313..
SHA256:	c92892ee1c9a44..
Infos:	

Most interesting Screenshot:



Detection

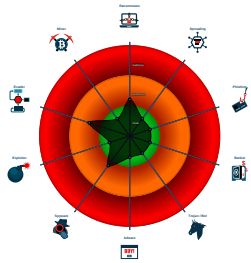


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Contains functionality to check if a d…
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Contains functionality which may be…
- Detected potential crypto function
- Drops PE files
- Found potential string decryption / a…
- PE file contains an invalid checksum
- PE file contains executable resource…
- PE file contains strange resources
- Sample file is different than original …
- Uses 32bit PE files
- Uses Microsoft's Enhanced Cryptog…

Classification



Startup

- **System is w10x64**
- SophosSetup (9).exe (PID: 4064 cmdline: 'C:\Users\user\Desktop\SophosSetup (9).exe' -install MD5: 070002B28E379E0C362F0E69ECD6D60B)
  - Setup.exe (PID: 6052 cmdline: 'C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe' -install MD5: 2FBBB26E1892185D13E4CD39FABD24EA)
- SophosSetup (9).exe (PID: 5912 cmdline: 'C:\Users\user\Desktop\SophosSetup (9).exe' /install MD5: 070002B28E379E0C362F0E69ECD6D60B)
  - Setup.exe (PID: 996 cmdline: 'C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe' /install MD5: 2FBBB26E1892185D13E4CD39FABD24EA)
- SophosSetup (9).exe (PID: 3888 cmdline: 'C:\Users\user\Desktop\SophosSetup (9).exe' /load MD5: 070002B28E379E0C362F0E69ECD6D60B)
  - Setup.exe (PID: 5872 cmdline: 'C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe' /load MD5: 2FBBB26E1892185D13E4CD39FABD24EA)
- **cleanup**

Malware Configuration

No configs have been found

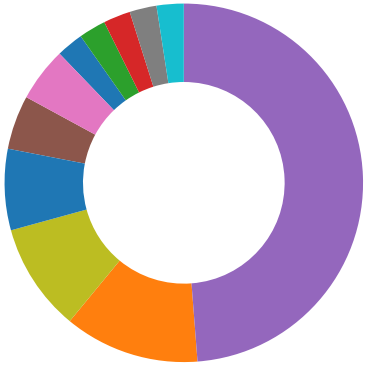
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



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

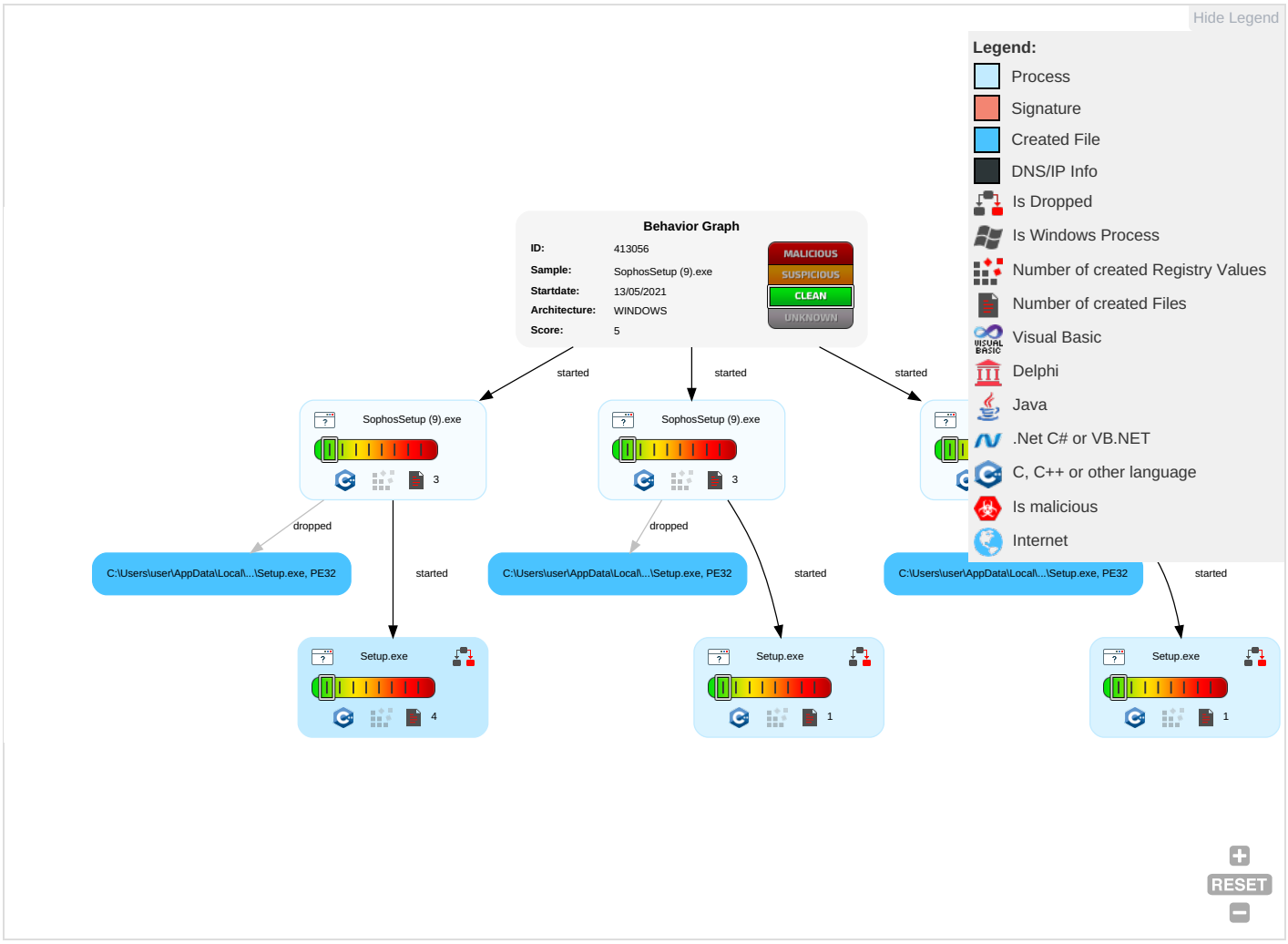
Click to jump to signature section

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 1	Process Injection 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Devic Without Authorizatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizatic
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

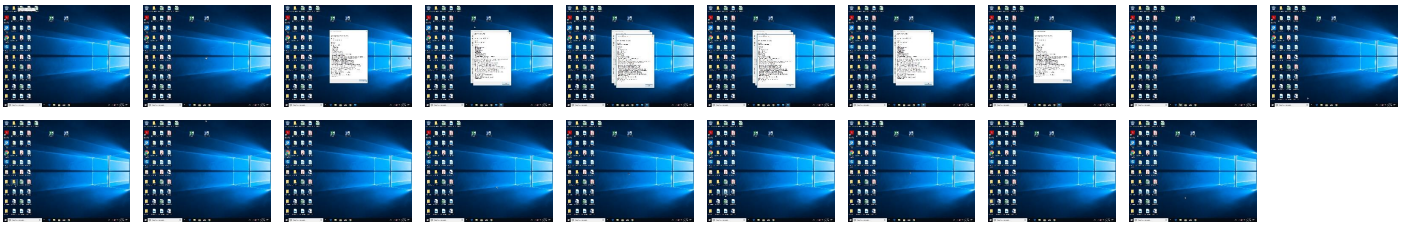
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SophosSetup (9).exe	3%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.digicert.c#	0%	Avira URL Cloud	safe	
http://ocsp.dig	0%	Avira URL Cloud	safe	
http://www.emtype.nethttp://www.emtype.net/emtype_eula.phpSophos	0%	Avira URL Cloud	safe	
http://crl4.digicert.	0%	Avira URL Cloud	safe	
http://ocsp.digy	0%	Avira URL Cloud	safe	
http://cacerts.d_	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.sophos.com/ja-jp/legal.aspx	SophosSetup (9).exe	false		high
http://ocsp.digicert.c#	Setup.exe, 00000003.00000002.246648079.0000000002F86000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.dig	Setup.exe, 00000003.00000002.247044892.0000000004BE2000.00000004.00000001.sdmp, Setup.exe, 00000008.00000002.230087964.0000000004AB2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.sophos.com/fr-fr/legal.aspx	SophosSetup (9).exe	false		high
http://https://www.sophos.com/es-es/legal.aspx	SophosSetup (9).exe	false		high
http://https://www.sophos.com/it-it/legal.aspx	SophosSetup (9).exe	false		high
http://www.emtype.nethttp://www.emtype.net/emtype_eula.phpSophos	SophosSetup (9).exe	false	• Avira URL Cloud: safe	unknown
http://crl4.digicert.	Setup.exe, 00000006.00000002.238159203.0000000000AE6000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.digy	Setup.exe, 00000006.00000002.242624835.0000000004AA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.sophos.com/zh-cn/legal.aspx	SophosSetup (9).exe	false		high
http://https://www.sophos.com/de-de/legal.aspx	SophosSetup (9).exe	false		high
http://cacerts.d_	Setup.exe, 00000003.00000002.246648079.0000000002F86000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.sophos.com/en-us/legal.aspx	SophosSetup (9).exe	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413056
Start date:	13.05.2021
Start time:	07:25:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SophosSetup (9).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
Run name:	Cmdline fuzzy
Number of analysed new started processes analysed:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean5.winEXE@9/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 59% (good quality ratio 57.3%) • Quality average: 79.3% • Quality standard deviation: 24.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory 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

No context

Created / dropped Files

C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142940.log	
Process:	C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	4.94342683088856
Encrypted:	false
SSDEEP:	3:tUI6IaGRVLSsWKgKSxyIAlcWHYiRgmv:maaCzWSR/hqmv
MD5:	87C7FC884DAD3948EADEA2CBBF398A47
SHA1:	3D10E3816AACB746A37823999684770BA3ABDC24
SHA-256:	8CFFFD1DE93C2E312655CF5D90407AEB281226176496ABCEF38BC90C07C5E1B7
SHA-512:	F81E8238AF335469ED927013045DDBB5E41091377937A4A979D2E1E7D8CB03239DB88458AB0C984D8F16023D6082BDAE087074ED95F10ABA15FF5DEB376EFB6
Malicious:	false
Reputation:	low
Preview:	2021-05-13T14:29:40.7267937Z ERROR : Unknown argument passed: install..

C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142943.log	
Process:	C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	132
Entropy (8bit):	5.260325582657426
Encrypted:	false
SSDEEP:	3:j1RPWXp5cViE2J5xAIWHRHX60lcoQIaGRWklNjVRKLIKVXZWJkmv:jTPWXp+N23f0Hq0lLda6hRKLIKVXZVmv
MD5:	164F558F9715C2D6B8035D652A83E502
SHA1:	715570F5612385415CD9BF7E34FA2E18242327A7
SHA-256:	FE4B897063DE1FFFE50323DB77739DB6D37D8B2D0998A882C84BD2AFB5C19A9B
SHA-512:	422DF9A4E838EFEF63E1F781CAA0B1982BC43923F1DA79F078C4A0F645D5B23F015BD5A9242F4C55DC211C95633E310D4D5FA6A4BF9A2A6C9308315FE399739
Malicious:	false
Reputation:	low
Preview:	Started C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe..2021-05-13T14:29:43.8361591Z ERROR : Non-option passed: /install..

C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142946.log	
Process:	C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	129
Entropy (8bit):	5.233658121631069
Encrypted:	false
SSDEEP:	3:j1RPWXp5cViE2J5xAISHDlo0lcoQIaGRTLWVQk32RKLIKVXZWJEoyn:jTPWXp+N23f6K0lLdaECf2RKLIKVXZtl
MD5:	71529C39A8CD9E6BCD85802F721D1E36
SHA1:	0C1C6D18153F3C4B2CC49D4ED4F8D1F7A266BC41
SHA-256:	E7EB7538D62ACBE072379AEC20594FA9E97DB302832251EAAEC359A8F053D35B
SHA-512:	D99BEA7D9657DA2385C10E6F8EB46FF3965163DB2B2CE8E0F620FF0CC1652A233ECE577B5603143E0AEA306C1706C7C34970A6870BD8E1F1D45BC342358A6D3C
Malicious:	false
Reputation:	low
Preview:	Started C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe..2021-05-13T14:29:46.3361535Z ERROR : Non-option passed: /load..

C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe	
Process:	C:\Users\user\Desktop\SophosSetup (9).exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1450448
Entropy (8bit):	6.9423549894664385
Encrypted:	false
SSDEEP:	24576:IB1wuKbfsIGVx5ysPwvX66x06qYaFKtyWGzM5N4iDTxA2M1QnDc5GQKGEDtV/5CT:5uKYbjyslvK6OPFky1w5N4iDTW2aQnD+
MD5:	2FBBB26E1892185D13E4CD39FABD24EA
SHA1:	84980D34A9BC41276B15DB0903C24A4FD51B76FB
SHA-256:	FB982FCB69A5EB6C2DFF43A2029F3BAB7EA0DCD57A71FCF13E94E7D9DAD84578

C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe	
SHA-512:	18F9A40F707E8692BDEDCEAEB4C7E2B1B43104CAFA5D9AEE26218DF7281D9C6EA105A147F9FDE2FA0716C64D41FD51F0F04BD83C49B75D89666267561378D2E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....eyT..*T..*T..*@..+C..*@..+...*...+@..*...+L..*@..+O..*@..+U. .*@..+C..*T..*...*...+...*..+"..*..*U..*T.*P..*..+U..*RichT..*.....PE..L...(..._.....`.....`&.....p....@.....@.....O.. .`.....`...T.....p.....@.....p.....text...._.....`..... ..`.rdata..8....p.....d.....@..@.data..... .....@....rsrc..... ...@..@.reloc.....`.....*.....@..B.....

C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\scf.dat	
Process:	C:\Users\user\Desktop\SophosSetup (9).exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2873
Entropy (8bit):	5.942974396829338
Encrypted:	false
SSDEEP:	48:DchSbUVcaa17kq/4tNMqW/rs7kQNxUdHQcvR02T7Wk6DfA0S7P+Qkb6ciSRKentY:DchNVcaOp/4ujs7kldHQc3j+A0SDvkbS
MD5:	7F6178CAE7007FCCA6EFBCB98767322B
SHA1:	C7395EA2486AA7C4CDA3C254CDF9B2E6983F4089
SHA-256:	FEAF3F01B4747CA6DC834A70434A619AA943722F292D05C9A26FFDCE6E953B76
SHA-512:	3506FBDC55FF0D742C31FEF63179017F49EC691B9A770B5670C0562469D452019E1C48792A5E3EF9595D944B6F3B31BBAD6C9302BFEA2B63C96253361D418D4F
Malicious:	false
Reputation:	low
Preview:	"setup.exe" 1450448 2fbbb26e1892185d13e4cd39fabd24ea.-----BEGIN SIGNATURE-----.Qzeu9kPq6h0vRVw6nNfMvyN1EWkkmlboVUbHLg8xPsQfSG6xIlQPoL1P4UWjJa/n.So1ZLGjKFa+Dg4wVdB1DoPjwCvJtKBvdUcsrXn5GbRje3b1SHDVwjKdewoWWJN6H.aUAU7W8U4AiMrQNHH1sBDEDYtTdD9k5jT+Ngt9Vv9Zu5Br9tEv891x78yDM/u8U+.Axg5f2SnCfi8Nz7oWMguJQ==.-----END SIGNATURE-----.-----BEGIN CERTIFICATE-----.MIIDUjCCAjqgAwIBAgIBGDANBgkqhkiG9w0BAQUFADCBnDEiMCAGA1UEAxMZU29w.aG9zSW50ZXJtZWRpYXRlRXhwMjAyNDEiMCAGCSqGSIb3DQEJARYTc29waG9zY2FA.c29waG9zLmNvbTEUMBIGA1UECBMLT3hmb3Jkc2hpcmUxCzAJBgNVBAYTAlVLMRMw.EQYDVQQKEwpTb3Bob3MgTHRkMRowGAYDVQQLExFTb3Bob3NTZWN1cmVCdWlsZDAe.Fw0wODEyMDEwMDAwMDBaFw0yNDAxMjgwMDAwMDBaMIGQMRYwFAYDVQQDFA1CdWls.ZF9FeHAyMDI0MSIwIAYJKoZIhvcNAQkBFhNzb3Bob3NjYUBzb3Bob3MuY29tMRQw.EgYDVQQIEwtPeGZvcmRzaGlyZTELMAkGA1UEBhMCVUsxEzARBgNVBAoTClNvcGhv.cyBMdGQxGjAYBgNVBAsTEVNvcGhvc1NlY3VyZUJ1aWxkMIG/MA0GCSqGSIb3DQEB.AQUAA4GtADCBqQKBoQDW9BwTyF312Yil5uWabaEUioILML4G/aBPWpxYW/2t65rh.Ziydvjl71N9NBiydBPPIaWv/vV2IYqhTG6j9hOqNuaVYK1hMokZoDZ5wkXmpOZua

C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe	
Process:	C:\Users\user\Desktop\SophosSetup (9).exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1450448
Entropy (8bit):	6.9423549894664385
Encrypted:	false
SSDEEP:	24576:IB1wuKbfsIGVx5ysPwvX66x06qYaFKtyWGzM5N4iDTxA2M1QnDc5GQKGEDtV/5CT:5uKYbjysIvK6OPFky1w5N4iDTW2aQnD+
MD5:	2FBBB26E1892185D13E4CD39FABD24EA
SHA1:	84980D34A9BC41276B15DB0903C24A4FD51B76FB
SHA-256:	FB982FCB69A5EB6C2DFF43A2029F3BAB7EA0DCD57A71FCF13E94E7D9DAD84578
SHA-512:	18F9A40F707E8692BDEDCEAEB4C7E2B1B43104CAFA5D9AEE26218DF7281D9C6EA105A147F9FDE2FA0716C64D41FD51F0F04BD83C49B75D89666267561378D2E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....eyT..*T..*T..*@..+C..*@..+...*...+@..*...+L..*@..+O..*@..+U. .*@..+C..*T..*...*...+...*..+"..*..*U..*T.*P..*..+U..*RichT..*.....PE..L...(..._.....`.....`&.....p....@.....@.....O.. .`.....`...T.....p.....@.....p.....text...._.....`..... ..`.rdata..8....p.....d.....@..@.data..... .....@....rsrc..... ...@..@.reloc.....`.....*.....@..B.....

C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\scf.dat	
Process:	C:\Users\user\Desktop\SophosSetup (9).exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2873
Entropy (8bit):	5.942974396829338
Encrypted:	false
SSDEEP:	48:DchSbUVcaa17kq/4tNMqW/rs7kQNxUdHQcvR02T7Wk6DfA0S7P+Qkb6ciSRKentY:DchNVcaOp/4ujs7kldHQc3j+A0SDvkbS
MD5:	7F6178CAE7007FCCA6EFBCB98767322B
SHA1:	C7395EA2486AA7C4CDA3C254CDF9B2E6983F4089

C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\scf.dat	
SHA-256:	FEAF3F01B4747CA6DC834A70434A619AA943722F292D05C9A26FFDCE6E953B76
SHA-512:	3506FBDC55FF0D742C31FEF63179017F49EC691B9A770B5670C0562469D452019E1C48792A5E3EF9595D944B6F3B31BBAD6C9302BFEA2B63C96253361D418D4F
Malicious:	false
Preview:	"setup.exe" 1450448 2fbbb26e1892185d13e4cd39fabd24ea.-----BEGIN SIGNATURE-----.Qzeu9kPq6h0vRVw6nNfMvyN1EWkkmlboVUbHLg8xPsQfSG6xIlQPoL1P4UWjJa/n.So1ZLGjKFa+Dg4wVdB1DoPjwCvJtKBvdUcsrXn5GbRje3b1SHDVwjKdewoWWJN6H.aUAU7W8U4AiMrQNHH1sBDEDYtTdD9k5jT+Ngt9Vv9Zu5Br9tEv891x78yDM/u8U+.Axg5f2SnCfi8Nz7oWMguJQ==.-----END SIGNATURE-----.-----BEGIN CERTIFICATE-----.MIIDUjCCAjqgAwIBAgIBGDANBgkqhkiG9w0BAQUFADCBnDEiMCAGA1UEAxMZU29w.aG9zSW50ZXJtZWRpYXRlRXhwMjAyNDEiMCAGCSqGSIb3DQEJARYTc29waG9zY2FA.c29waG9zLmNvbTEUMBIGA1UECBMLT3hmb3Jkc2hpcmUxCzAJBgNVBAYTAlVLMRMw.EQYDVQQKEwpTb3Bob3MgTHRkMRowGAYDVQQLExFTb3Bob3NTZWN1cmVCdWlsZDAe.Fw0wODEyMDEwMDAwMDBaFw0yNDAxMjgwMDAwMDBaMIGQMRYwFAYDVQQDFA1CdWls.ZF9FeHAyMDI0MSlwIAYJKoZIhvcNAQkBFhNzb3Bob3NjYUBzb3Bob3MuY29tMRQw.EgYDVQQIEwtPeGZvcmRzaGlyZTELMAkGA1UEBhMCVUsxEzARBgNVBAoTClNvcGhv.cyBMdGQxGjAYBgNVBAsTEVNvcGhvc1NlY3VyZUJ1aWxkMIG/MA0GCSqGSIb3DQEB.AQUAA4GtADCBqQKBoQDW9BwTyF312Yil5uWabaEUioILML4G/aBPWpxYW/2t65rh.ZiydvjI71N9NBiydBPPIaWv/vV2IYqhTG6j9hOqNuaVYK1hMokZoDZ5wkXmpOZua

C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe	
Process:	C:\Users\user\Desktop\SophosSetup (9).exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1450448
Entropy (8bit):	6.9423549894664385
Encrypted:	false
SSDEEP:	24576:IB1wuKbfsIGVx5ysPwvX66x06qYaFKtyWGzM5N4iDTxA2M1QnDc5GQKGEDtV/5CT:5uKYbjysIvK6OPFky1w5N4iDTW2aQnD+
MD5:	2FBBB26E1892185D13E4CD39FABD24EA
SHA1:	84980D34A9BC41276B15DB0903C24A4FD51B76FB
SHA-256:	FB982FCB69A5EB6C2DFF43A2029F3BAB7EA0DCD57A71FCF13E94E7D9DAD84578
SHA-512:	18F9A40F707E8692BDEDCEAEB4C7E2B1B43104CAFA5D9AEE26218DF7281D9C6EA105A147F9FDE2FA0716C64D41FD51F0F04BD83C49B75D89666267561378D2E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....eyT..*T..*T..*@..+C..*@..+...*...+@..*...+L..*@..+O..*@..+U..*@..+C..*T..*...*...+...*..+"..*..*U..*T.*P..*..+U..*RichT..*.....PE..L...(..._.....`.....`&.....p....@.....@.....O.....`.....`...T.....p.....@.....p.....text...._.....`..... ..`.rdata..8....p.....d.....@..@.data..... .....@....rsrc.....@..@.reloc.....`.....*.....@..B.....

C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\scf.dat	
Process:	C:\Users\user\Desktop\SophosSetup (9).exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	2873
Entropy (8bit):	5.942974396829338
Encrypted:	false
SSDEEP:	48:DchSbUVcaa17kq/4tNMqW/rs7kQNxUdHQcvR02T7Wk6DfA0S7P+Qkb6ciSRKentY:DchNVcaOp/4ujs7kldHQc3j+A0SDvkbS
MD5:	7F6178CAE7007FCCA6EFBCB98767322B
SHA1:	C7395EA2486AA7C4CDA3C254CDF9B2E6983F4089
SHA-256:	FEAF3F01B4747CA6DC834A70434A619AA943722F292D05C9A26FFDCE6E953B76
SHA-512:	3506FBDC55FF0D742C31FEF63179017F49EC691B9A770B5670C0562469D452019E1C48792A5E3EF9595D944B6F3B31BBAD6C9302BFEA2B63C96253361D418D4F
Malicious:	false
Preview:	"setup.exe" 1450448 2fbbb26e1892185d13e4cd39fabd24ea.-----BEGIN SIGNATURE-----.Qzeu9kPq6h0vRVw6nNfMvyN1EWkkmlboVUbHLg8xPsQfSG6xIlQPoL1P4UWjJa/n.So1ZLGjKFa+Dg4wVdB1DoPjwCvJtKBvdUcsrXn5GbRje3b1SHDVwjKdewoWWJN6H.aUAU7W8U4AiMrQNHH1sBDEDYtTdD9k5jT+Ngt9Vv9Zu5Br9tEv891x78yDM/u8U+.Axg5f2SnCfi8Nz7oWMguJQ==.-----END SIGNATURE-----.-----BEGIN CERTIFICATE-----.MIIDUjCCAjqgAwIBAgIBGDANBgkqhkiG9w0BAQUFADCBnDEiMCAGA1UEAxMZU29w.aG9zSW50ZXJtZWRpYXRlRXhwMjAyNDEiMCAGCSqGSIb3DQEJARYTc29waG9zY2FA.c29waG9zLmNvbTEUMBIGA1UECBMLT3hmb3Jkc2hpcmUxCzAJBgNVBAYTAlVLMRMw.EQYDVQQKEwpTb3Bob3MgTHRkMRowGAYDVQQLExFTb3Bob3NTZWN1cmVCdWlsZDAe.Fw0wODEyMDEwMDAwMDBaFw0yNDAxMjgwMDAwMDBaMIGQMRYwFAYDVQQDFA1CdWls.ZF9FeHAyMDI0MSlwIAYJKoZIhvcNAQkBFhNzb3Bob3NjYUBzb3Bob3MuY29tMRQw.EgYDVQQIEwtPeGZvcmRzaGlyZTELMAkGA1UEBhMCVUsxEzARBgNVBAoTClNvcGhv.cyBMdGQxGjAYBgNVBAsTEVNvcGhvc1NlY3VyZUJ1aWxkMIG/MA0GCSqGSIb3DQEB.AQUAA4GtADCBqQKBoQDW9BwTyF312Yil5uWabaEUioILML4G/aBPWpxYW/2t65rh.ZiydvjI71N9NBiydBPPIaWv/vV2IYqhTG6j9hOqNuaVYK1hMokZoDZ5wkXmpOZua

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.992564322628606

General

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:	SophosSetup (9).exe
File size:	1565616
MD5:	070002b28e379e0c362f0e69ecd6d60b
SHA1:	db19c547d7231362040c8ff10c92451e059c3ef2
SHA256:	c92892ee1c9a44469650f5575e64c11fa08f44bcdf61c49e19a2714e2b6a7f5b
SHA512:	f863ffad6ce6e67380698ef8b12aca5f7256c52f84847d7f120b5c7d56838e6b264436cdd5ab72e52055d99998455ca7ce053fcfeb9c63e32ddb0d6d08643c52
SSDEEP:	24576:c/5CxBMhB1wuKbfsIGVx5ysPwvX66x06qYaFKtyWGzM5N4iDTxA2M1QnDc5GQKG3:c/5CxBMKuKYbjysIvK6OPFky1w5N4iDA
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.r.g...g...g...s...b...g...B.....f.....e.....f...g...e.....f...Richg.....PE..L...}.._.....p.....

File Icon

Icon Hash:	72697c6949f0cc70

Static PE Info

General

Entrypoint:	0x402210
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F928E7D [Fri Oct 23 08:04:13 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	dbe2d93d7fa7dad8827b11304f9692c2

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert EV Code Signing CA (SHA2), OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 11/6/2018 4:00:00 PM 2/4/2022 4:00:00 AM
Subject Chain	• CN=Sophos Ltd, OU=Endpoint Security Group, O=Sophos Ltd, L=Abingdon, C=GB, SERIALNUMBER=02096520, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=GB
Version:	3
Thumbprint MD5:	424FF48C1975D5FD2134CBF70558A678
Thumbprint SHA-1:	80ABFE016005D804CCC344600C2207AFCF212A7B
Thumbprint SHA-256:	44E319D9E913676A311E521A671D687C16846A291BD86A83900FD425C77ACA0F
Serial:	0995B7452559F652761AF8868F44D950

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 30h
push ebx
push esi
push edi
call 00007FAA34C85B27h
test al, al
jne 00007FAA34C86D3Ch
push 00403858h
call 00007FAA34C868E9h
lea eax, dword ptr [ebp-04h]
mov dword ptr [ebp-04h], 00000000h
push eax
push 00000000h
push 00000000h
push 00000000h
push 00000000h
push 00000000h
push 00000000h
push 00000220h
push 00000020h
push 00000002h
lea eax, dword ptr [ebp-18h]
mov dword ptr [ebp-18h], 00000000h
push eax
mov word ptr [ebp-14h], 0500h
call dword ptr [00403004h]
test eax, eax
jne 00007FAA34C86D3Ch
push 004033F8h
call 00007FAA34C868A4h
lea eax, dword ptr [ebp-0Ch]
mov dword ptr [ebp-0Ch], 00000000h
push eax
push dword ptr [ebp-04h]
push 00000000h
call dword ptr [00403000h]
test eax, eax
jne 00007FAA34C86D3Ch
push 00403450h
call 00007FAA34C86880h
cmp dword ptr [ebp-0Ch], 00000000h
mov eax, dword ptr [ebp-04h]
setne bl
test eax, eax
je 00007FAA34C86D39h
push eax
call dword ptr [0040300Ch]
test bl, bl
jne 00007FAA34C86D3Ch
push 00403888h
call 00007FAA34C8685Dh
call dword ptr [00403088h]
mov dword ptr [00404000h], eax
lea eax, dword ptr [ebp-30h]
push eax
call 00007FAA34C86249h
add esp, 04h
mov esi, 00000020h
call dword ptr [0000301Ch]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3bc8	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x35000	0x175a8c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x178c00	0x57b0	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1ab000	0x210	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3a38	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3000	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x165c	0x1800	False	0.474772135417	data	5.67619442195	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0xf80	0x1000	False	0.415771484375	data	4.25404794293	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x30008	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x35000	0x175a8c	0x175c00	False	0.538502038043	data	6.98801421001	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1ab000	0x210	0x400	False	0.505859375	data	4.16615383322	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x35288	0x528	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0x357b0	0x1428	dBase IV DBT of @.DBF, block length 5120, next free block index 40, next free block 0, next used block 0	English	Great Britain
RT_ICON	0x36bd8	0x2d28	data	English	Great Britain
RT_ICON	0x39900	0xd819	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	Great Britain
RT_RCDATA	0x4711c	0x1621d0	PE32 executable (GUI) Intel 80386, for MS Windows		
RT_RCDATA	0x1a92ec	0xb39	ASCII text		
RT_GROUP_ICON	0x1a9e28	0x3e	data	English	Great Britain
RT_VERSION	0x1a9e68	0x390	data	English	United States
RT_VERSION	0x1aa1f8	0x390	data	English	United States
RT_MANIFEST	0x1aa588	0x501	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetProcAddress, SetDllDirectoryW, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, CreateDirectoryW, CreateFileW, DeleteFileW, RemoveDirectoryW, WriteFile, GetTempPathW, CloseHandle, HeapAlloc, GetModuleHandleW, HeapFree, WaitForSingleObject, ExitProcess, GetExitCodeProcess, CreateProcessW, GetStartupInfoW, GetTickCount, GetSystemDirectoryW, GetModuleFileNameW, LoadResource, LockResource, SizeofResource, FindResourceW, LocalFree, HeapSetInformation, GetProcessHeap, GetLastError, HeapReAlloc, SetEnvironmentVariableW
ADVAPI32.dll	CheckTokenMembership, AllocateAndInitializeSid, ConvertStringSecurityDescriptorToSecurityDescriptorW, FreeSid

Version Infos

Description	Data
LegalCopyright	Copyright 1989-2020 Sophos Limited.
InternalName	SophosSetup.exe
FileVersion	1.10.305.0
CompanyName	Sophos Limited

Description	Data
Comments	20201023075653-695d849e00c621938906f733ffb9051614277482-FnyoEp
ProductName	Sophos Setup
ProductVersion	1.10
FileDescription	Sophos Setup
OriginalFilename	SophosSetup.exe
Translation	0x0809 0x04b0

Possible Origin

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

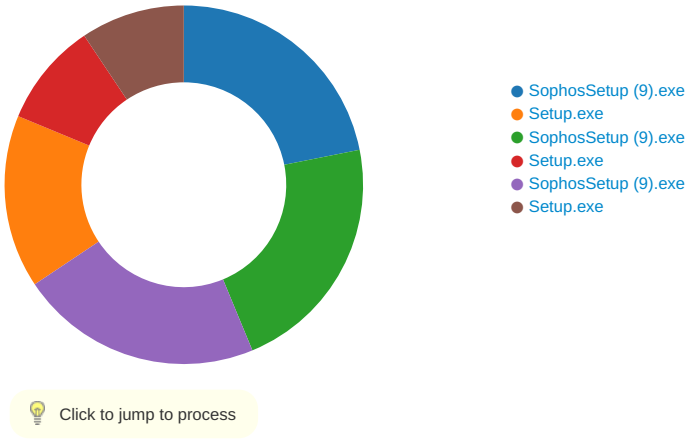
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SophosSetup (9).exe PID: 4064 Parent PID: 5604

General

Start time:	07:29:39
Start date:	13/05/2021
Path:	C:\Users\user\Desktop\SophosSetup (9).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SophosSetup (9).exe' -install
Imagebase:	0x1f0000
File size:	1565616 bytes
MD5 hash:	070002B28E379E0C362F0E69ECD6D60B
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\sfl-9a9a6400	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1F1CD6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1F136A	CreateFileW
C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\scf.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1F136A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe	success or wait	1	1F177C	DeleteFileW
C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\scf.dat	success or wait	1	1F17A0	DeleteFileW

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\sfl-9a9a6400\Setup.exe	unknown	1450448	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 00 00 00 00 00 00 00 00 00 00 08 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 10 85 65 79 54 e4 0b 2a 54 e4 0b 2a 54 e4 0b 2a 40 8f 08 2b 43 e4 0b 2a 40 8f 0e 2b ea e4 0b 2a 9f 8b 0f 2b 40 e4 0b 2a 9f 8b 08 2b 4c e4 0b 2a 40 8f 0f 2b 4f e4 0b 2a 40 8f 0d 2b 55 e4 0b 2a 40 8f 0a 2b 43 e4 0b 2a 54 e4 0a 2a 1d e5 0b 2a 9f 8b 0e 2b c2 e4 0b 2a d2 94 02 2b 22 e4 0b 2a d2 94 f4 2a 55 e4 0b 2a 54 e4 9c 2a 50 e4 0b 2a d2 94 09 2b 55 e4 0b 2a 52 69 63 68 54 e4 0b	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....eyT..*T..*T..*@..+C. .*@..+...*...+@..*...+L..*@.. + O..*@..+U..*@..+C..*T..*... *...+...*...+"..*...*U..*T..*P..* ...+U..*RichT..	success or wait	1	1F138B	WriteFile
C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\scf.dat	unknown	2873	22 73 65 74 75 70 2e 65 78 65 22 20 31 34 35 30 34 34 38 20 32 66 62 62 62 32 36 65 31 38 39 32 31 38 35 64 31 33 65 34 63 64 33 39 66 61 62 64 32 34 65 61 0a 2d 2d 2d 2d 2d 42 45 47 49 4e 20 53 49 47 4e 41 54 55 52 45 2d 2d 2d 2d 2d 0a 51 7a 65 75 39 6b 50 71 36 68 30 76 52 56 77 36 6e 4e 66 4d 76 79 4e 31 45 57 6b 6b 6d 6c 62 6f 56 55 62 48 4c 67 38 78 50 73 51 66 53 47 36 78 49 6c 51 50 6f 4c 31 50 34 55 57 6a 4a 61 2f 6e 0a 53 6f 31 5a 4c 47 6a 4b 46 61 2b 44 67 34 77 56 64 42 31 44 6f 50 6a 77 43 76 4a 74 4b 42 76 64 55 63 73 72 58 6e 35 47 62 52 6a 65 33 62 31 53 48 44 56 77 6a 4b 64 65 77 6f 57 57 4a 4e 36 48 0a 61 55 41 55 37 57 38 55 34 41 69 4d 72 51 4e 48 48 31 73 42 44 45 44 59 74 54 64 44 39 6b 35 6a 54 2b 4e 67 74 39 56 76 39 5a 75 35 42 72	"setup.exe" 1450448 2fbbb26e18 92185d13e4cd39fabd24ea. -----BEGIN SIGNATURE---- -.Qzeu9kPq6h0 vRVw6nNfMvyN1EWkkml boVUbHLg8xP sQfSG6xIlQPoL1P4UWjJa /n.So1ZLG jKFa+Dg4wVdB1DoPjwCv JtKBvdUcsr Xn5GbRje3b1SHDVwjKde woWWJN6H.a UAU7W8U4AiMrQNHH1sB DEDYtTdD9k5 jT+Ngt9Vv9Zu5Br	success or wait	1	1F138B	WriteFile

Analysis Process: Setup.exe PID: 6052 Parent PID: 4064

General

Start time:	07:29:39
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sfl-9a9a6400\Setup.exe' -install
Imagebase:	0x990000
File size:	1450448 bytes
MD5 hash:	2FBBB26E1892185D13E4CD39FABD24EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Sophos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	9EFF12	CreateDirectoryW
C:\ProgramData\Sophos\CloudInstaller	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	9EFF12	CreateDirectoryW
C:\ProgramData\Sophos\CloudInstaller\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	9EFF12	CreateDirectoryW
C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142940.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	A28A23	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142940.log	unknown	71	32 30 32 31 2d 30 35 2d 31 33 54 31 34 3a 32 39 3a 34 30 2e 37 32 36 37 39 33 37 5a 20 45 52 52 4f 52 20 3a 20 55 6e 6b 6e 6f 77 6e 20 61 72 67 75 6d 65 6e 74 20 70 61 73 73 65 64 3a 20 69 6e 73 74 61 6c 6c 0d 0a	2021-05-13T14:29:40.7267937Z ERROR : Unknown argument passed: install..	success or wait	1	A1C712	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: SophosSetup (9).exe PID: 5912 Parent PID: 5604

General

Start time:	07:29:41
Start date:	13/05/2021
Path:	C:\Users\user\Desktop\SophosSetup (9).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SophosSetup (9).exe' /install
Imagebase:	0x1f0000
File size:	1565616 bytes
MD5 hash:	070002B28E379E0C362F0E69ECD6D60B

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\sfl-5b4b6400	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1F1CD6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1F136A	CreateFileW
C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\scf.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1F136A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe	success or wait	1	1F177C	DeleteFileW
C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\scf.dat	success or wait	1	1F17A0	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe	unknown	1450448	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 08 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 10 85 65 79 54 e4 0b 2a 54 e4 0b 2a 54 e4 0b 2a 40 8f 08 2b 43 e4 0b 2a 40 8f 0e 2b ea e4 0b 2a 9f 8b 0f 2b 40 e4 0b 2a 9f 8b 08 2b 4c e4 0b 2a 40 8f 0f 2b 4f e4 0b 2a 40 8f 0d 2b 55 e4 0b 2a 40 8f 0a 2b 43 e4 0b 2a 54 e4 0a 2a 1d e5 0b 2a 9f 8b 0e 2b c2 e4 0b 2a d2 94 02 2b 22 e4 0b 2a d2 94 f4 2a 55 e4 0b 2a 54 e4 9c 2a 50 e4 0b 2a d2 94 09 2b 55 e4 0b 2a 52 69 63 68 54 e4 0b	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........eyT..*T..*T..*@..+C. .*@..+...*...+@..*...+L..*@.. + O..*@..+U..*@..+C..*T..*... *...+...*...+"..*...*U..*T..*P..* ...+U..*RichT..	success or wait	1	1F138B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\scf.dat	unknown	2873	22 73 65 74 75 70 2e 65 78 65 22 20 31 34 35 30 34 34 38 20 32 66 62 62 62 32 36 65 31 38 39 32 31 38 35 64 31 33 65 34 63 64 33 39 66 61 62 64 32 34 65 61 0a 2d 2d 2d 2d 2d 42 45 47 49 4e 20 53 49 47 4e 41 54 55 52 45 2d 2d 2d 2d 2d 0a 51 7a 65 75 39 6b 50 71 36 68 30 76 52 56 77 36 6e 4e 66 4d 76 79 4e 31 45 57 6b 6b 6d 6c 62 6f 56 55 62 48 4c 67 38 78 50 73 51 66 53 47 36 78 49 6c 51 50 6f 4c 31 50 34 55 57 6a 4a 61 2f 6e 0a 53 6f 31 5a 4c 47 6a 4b 46 61 2b 44 67 34 77 56 64 42 31 44 6f 50 6a 77 43 76 4a 74 4b 42 76 64 55 63 73 72 58 6e 35 47 62 52 6a 65 33 62 31 53 48 44 56 77 6a 4b 64 65 77 6f 57 57 4a 4e 36 48 0a 61 55 41 55 37 57 38 55 34 41 69 4d 72 51 4e 48 48 31 73 42 42 44 59 74 54 64 44 39 6b 35 6a 54 2b 4e 67 74 39 56 76 39 5a 75 35 42 72	"setup.exe" 1450448 2fbbb26e18 92185d13e4cd39fabd24ea. -----BEGIN SIGNATURE---- -.Qzeu9kPq6h0 vRVw6nNfMvyN1EWkkml boVUbHLg8xP sQfSG6xIlQPoL1P4UWjJa /n.So1ZLG jKFa+Dg4wVdB1DoPjwCv JtKBvdUcsr Xn5GbRje3b1SHDVwjKde woWWJN6H.a UAU7W8U4AiMrQNHH1sB DEDYtTdD9k5 jT+Ngt9Vv9Zu5Br	success or wait	1	1F138B	WriteFile

Analysis Process: Setup.exe PID: 996 Parent PID: 5912

General

Start time:	07:29:42
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe' /install
Imagebase:	0xaf0000
File size:	1450448 bytes
MD5 hash:	2FBBB26E1892185D13E4CD39FABD24EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142943.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	B88A23	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:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142943.log	unknown	66	53 74 61 72 74 65 64 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 73 66 6c 2d 35 62 34 62 36 34 30 30 5c 53 65 74 75 70 2e 65 78 65 0d 0a	Started C:\Users\user\AppData\Local\Temp\sfl-5b4b6400\Setup.exe..	success or wait	1	B7C712	WriteFile
C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142943.log	unknown	66	32 30 32 31 2d 30 35 2d 31 33 54 31 34 3a 32 39 3a 34 33 2e 38 33 36 31 35 39 31 5a 20 45 52 52 4f 52 20 3a 20 4e 6f 6e 2d 6f 70 74 69 6f 6e 20 70 61 73 73 65 64 3a 20 2f 69 6e 73 74 61 6c 6c 0d 0a	2021-05-13T14:29:43.8361591Z ERROR : Non-option passed: /install..	success or wait	1	B7C712	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: SophosSetup (9).exe PID: 3888 Parent PID: 5604

General

Start time:	07:29:44
Start date:	13/05/2021
Path:	C:\Users\user\Desktop\SophosSetup (9).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SophosSetup (9).exe' /load
Imagebase:	0x1f0000
File size:	1565616 bytes
MD5 hash:	070002B28E379E0C362F0E69ECD6D60B
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\sfl-1bfb6400	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1F1CD6	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1F136A	CreateFileW
C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\scf.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1F136A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe	success or wait	1	1F177C	DeleteFileW
C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\scf.dat	success or wait	1	1F17A0	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe	unknown	1450448	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 08 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 10 85 65 79 54 e4 0b 2a 54 e4 0b 2a 54 e4 0b 2a 40 8f 08 2b 43 e4 0b 2a 40 8f 0e 2b ea e4 0b 2a 9f 8b 0f 2b 40 e4 0b 2a 9f 8b 08 2b 4c e4 0b 2a 40 8f 0f 2b 4f e4 0b 2a 40 8f 0d 2b 55 e4 0b 2a 40 8f 0a 2b 43 e4 0b 2a 54 e4 0a 2a 1d e5 0b 2a 9f 8b 0e 2b c2 e4 0b 2a d2 94 02 2b 22 e4 0b 2a d2 94 f4 2a 55 e4 0b 2a 54 e4 9c 2a 50 e4 0b 2a d2 94 09 2b 55 e4 0b 2a 52 69 63 68 54 e4 0b	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........eyT..*T..*T..*@..+C. .*@..+...*...+@..*...+L..*@.. + O..*@..+U..*@..+C..*T..*... *...+...*...+"..*...*U..*T..*P..* ...+U..*RichT..	success or wait	1	1F138B	WriteFile
C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\scf.dat	unknown	2873	22 73 65 74 75 70 2e 65 78 65 22 20 31 34 35 30 34 34 38 20 32 66 62 62 62 32 36 65 31 38 39 32 31 38 35 64 31 33 65 34 63 64 33 39 66 61 62 64 32 34 65 61 0a 2d 2d 2d 2d 2d 42 45 47 49 4e 20 53 49 47 4e 41 54 55 52 45 2d 2d 2d 2d 2d 0a 51 7a 65 75 39 6b 50 71 36 68 30 76 52 56 77 36 6e 4e 66 4d 76 79 4e 31 45 57 6b 6b 6d 6c 62 6f 56 55 62 48 4c 67 38 78 50 73 51 66 53 47 36 78 49 6c 51 50 6f 4c 31 50 34 55 57 6a 4a 61 2f 6e 0a 53 6f 31 5a 4c 47 6a 4b 46 61 2b 44 67 34 77 56 64 42 31 44 6f 50 6a 77 43 76 4a 74 4b 42 76 64 55 63 73 72 58 6e 35 47 62 52 6a 65 33 62 31 53 48 44 56 77 6a 4b 64 65 77 6f 57 57 4a 4e 36 48 0a 61 55 41 55 37 57 38 55 34 41 69 4d 72 51 4e 48 48 31 73 42 44 45 44 59 74 54 64 44 39 6b 35 6a 54 2b 4e 67 74 39 56 76 39 5a 75 35 42 72	"setup.exe" 1450448 2fbbb26e18 92185d13e4cd39fabd24ea. -----BEGIN SIGNATURE---- -.Qzeu9kPq6h0 vRVw6nNfMvyN1EWkkml boVUbHLg8xP sQfSG6xIlQPoL1P4UWjJa /n.So1ZLG jKFa+Dg4wVdB1DoPjwCv JtKBvdUcsr Xn5GbRje3b1SHDVwjKde woWWJN6H.a UAU7W8U4AiMrQNHH1sB DEDYtTdD9k5 jT+Ngt9Vv9Zu5Br	success or wait	1	1F138B	WriteFile

Analysis Process: Setup.exe PID: 5872 Parent PID: 3888

General

Start time:	07:29:45
Start date:	13/05/2021
Path:	C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe' /load
Imagebase:	0xef0000
File size:	1450448 bytes
MD5 hash:	2FBBB26E1892185D13E4CD39FABD24EA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142946.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	F88A23	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142946.log	unknown	66	53 74 61 72 74 65 64 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 73 66 6c 2d 31 62 66 62 36 34 30 30 5c 53 65 74 75 70 2e 65 78 65 0d 0a	Started C:\Users\user\AppData\Local\Temp\sfl-1bfb6400\Setup.exe..	success or wait	1	F7C712	WriteFile
C:\ProgramData\Sophos\CloudInstaller\Logs\SophosCloudInstaller_20210513_142946.log	unknown	63	32 30 32 31 2d 30 35 2d 31 33 54 31 34 3a 32 39 3a 34 36 2e 33 33 36 31 35 33 35 5a 20 45 52 52 4f 52 20 3a 20 4e 6f 6e 2d 6f 70 74 69 6f 6e 20 70 61 73 73 65 64 3a 20 2f 6c 6f 61 64 0d 0a	2021-05-13T14:29:46.3361535Z ERROR : Non-option passed: /load..	success or wait	1	F7C712	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis