ID: 1290344
Sample Name:
sublime.text.v4152-patch.exe
Cookbook: default.jbs
Time: 05:26:27
Date: 12/08/2023
Version: 38.0.0 Beryl

Table of Contents

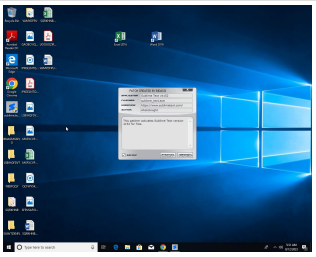
Windows Analysis Report

sublime.text.v4152-patch.exe

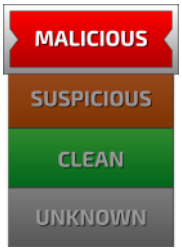
Overview

General Information

Sample Name:	sublime.text.v4152-patch.exe
Analysis ID:	1290344
MD5:	15f0f046c5a23…
SHA1:	106888897e37…
SHA256:	5ee68867759b…
Infos:	



Detection

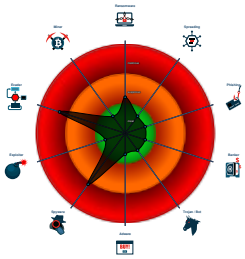


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Generic Patcher
- Found stalling execution ending in A…
- PE file has nameless sections
- PE file has a writeable .text section
- Machine Learning detection for drop…
- Machine Learning detection for sam…
- Contains functionality to modify clip…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- Found a high number of Window / U…

Classification



Process Tree

- **System is w10x64**
- sublime.text.v4152-patch.exe (PID: 5480 cmdline: C:\Users\user\Desktop\sublime.text.v4152-patch.exe MD5: 15F0F046C5A23F898A4162724A16BE09)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
sublime.text.v4152-patch.exe	CN_Honker_Acunetix_Web_Vulnerability_Scanner_8_x_Enterprise_Edition_KeyGen	Sample from CN Honker Pentest Toolset - file Acunetix_Web_Vulnerability_Scanner_8.x_Enterprise_Edition_KeyGen.exe	Florian Roth	• 0xccf59:$s0: <description>Patch</description> • 0x804:$s2: \dup2patcher.dll • 0x815:$s3: load_patcher

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\dup2patcher.dll	JoeSecurity_GenericPatcher	Yara detected Generic Patcher	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.886505239.0000000000830000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_GenericPatcher	Yara detected Generic Patcher	Joe Security	
Process Memory Space: sublime.text.v4152-patch.exe PID: 5480	JoeSecurity_GenericPatcher	Yara detected Generic Patcher	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.sublime.text.v4152-patch.exe.830000.2.raw.unpack	JoeSecurity_GenericPatcher	Yara detected Generic Patcher	Joe Security	
0.2.sublime.text.v4152-patch.exe.830000.2.unpack	JoeSecurity_GenericPatcher	Yara detected Generic Patcher	Joe Security	
0.2.sublime.text.v4152-patch.exe.6c660000.4.unpack	JoeSecurity_GenericPatcher	Yara detected Generic Patcher	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing

Contains functionality to modify clipboard data

System Summary

Malicious sample detected (through community Yara rule)

PE file has nameless sections

PE file has a writeable .text section

Malware Analysis System Evasion

Found stalling execution ending in API Sleep call

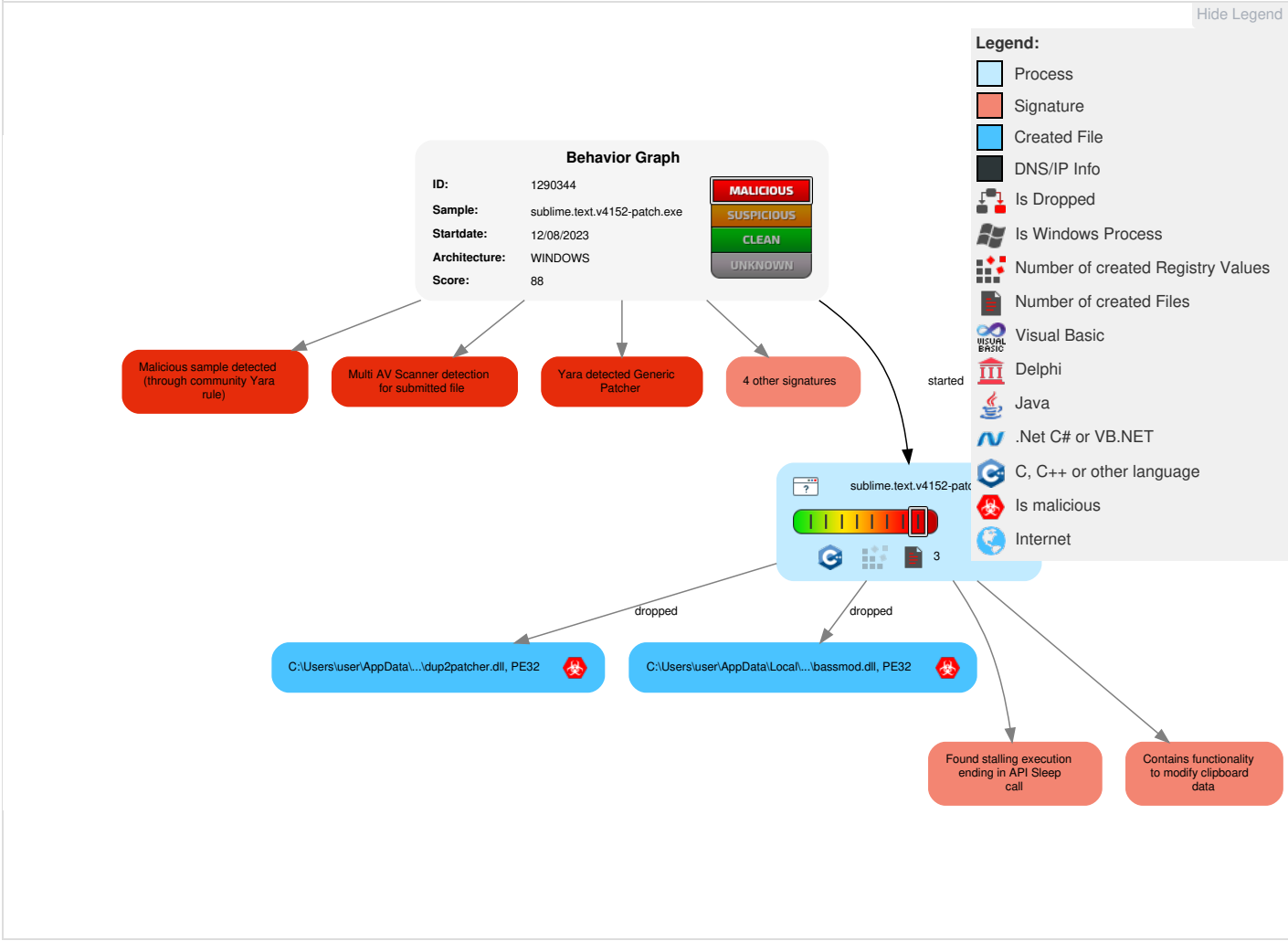
HIPS / PFW / Operating System Protection Evasion

Yara detected Generic Patcher

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	Path Interception	Path Interception	2 Virtualization/Sandbox Evasion	1 Input Capture	1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	3 Software Packing	LSASS Memory	2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	1 1 Clipboard Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

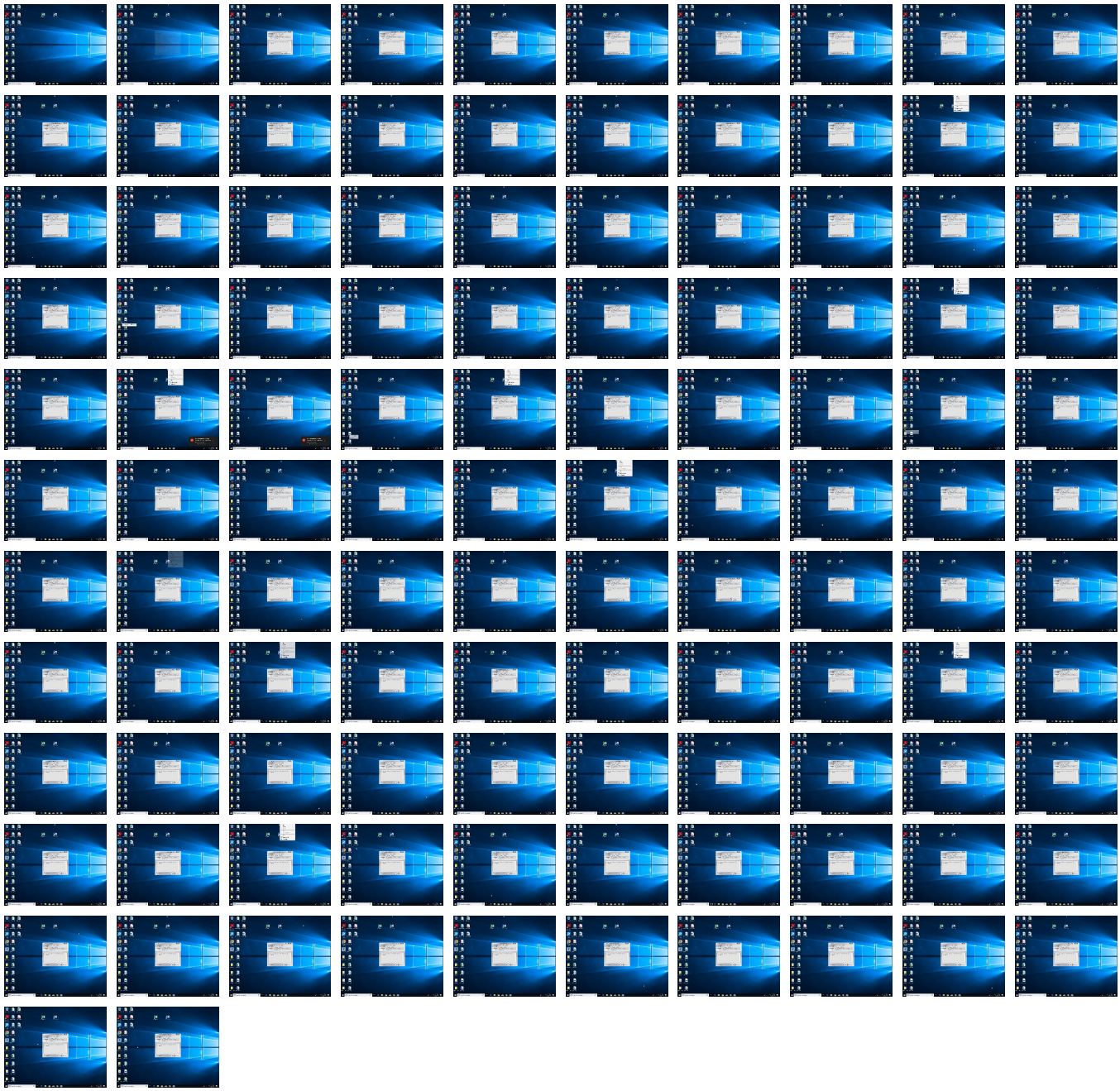
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
sublime.text.v4152-patch.exe	57%	ReversingLabs	Win32.Hacktool.Generic	
sublime.text.v4152-patch.exe	62%	Virustotal		Browse
sublime.text.v4152-patch.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\dup2patcher.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\bassmod.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\bassmod.dll	1%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://diablo2oo2.cjb.netP76y	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.sublimetext.com/ttps://www.sublimetext.com/	sublime.text.v4152-patch.exe, 00000000.00000002.886492885.00000000006FC000.00000004.00000010.00020000.00000000.sdmp	false		high
http://https://www.sublimetext.com/AholicknightAugust	sublime.text.v4152-patch.exe, 00000000.00000002.886994622.000000006C6AF000.00000080.00000001.01000000.00000004.sdmp, sublime.text.v4152-patch.exe, 00000000.00000002.886505239.0000000000867000.00000004.00001000.00020000.00000000.sdmp, dup2patcher.dll.0.dr	false		high
http://https://www.sublimetext.com/_n	sublime.text.v4152-patch.exe, 00000000.00000002.886492885.00000000006FC000.00000004.00000010.00020000.00000000.sdmp	false		high
http://https://www.sublimetext.com/	sublime.text.v4152-patch.exe, 00000000.00000002.886492885.00000000006FC000.00000004.00000010.00020000.00000000.sdmp, sublime.text.v4152-patch.exe, 00000000.00000002.886994622.000000006C6AF000.00000080.00000001.01000000.00000004.sdmp, sublime.text.v4152-patch.exe, 00000000.00000002.886505239.0000000000867000.00000004.00001000.00020000.00000000.sdmp, sublime.text.v4152-patch.exe, 00000000.00000002.886647795.00000000009B8000.00000004.00000020.00020000.00000000.sdmp, dup2patcher.dll.0.dr	false		high
http://diablo2oo2.cjb.netP76y	sublime.text.v4152-patch.exe, 00000000.00000002.886994622.000000006C6AF000.00000080.00000001.01000000.00000004.sdmp, sublime.text.v4152-patch.exe, 00000000.00000002.886505239.0000000000867000.00000004.00001000.00020000.00000000.sdmp, dup2patcher.dll.0.dr	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	38.0.0 Beryl
Analysis ID:	1290344
Start date and time:	2023-08-12 05:26:27 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	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
Sample file name:	sublime.text.v4152-patch.exe
Detection:	MAL
Classification:	mal88.spyw.evad.winEXE@1/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 33.3% (good quality ratio 31.8%) • Quality average: 81.2% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, arc.msn.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\bassmod.dll

Process:	C:\Users\user\Desktop\sublime.text.v4152-patch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	34308
Entropy (8bit):	7.892542080413996
Encrypted:	false
SSDEEP:	768:qQmS5iUgi5czW+DlrQOS1DeDdjgNtbX4O6DHix84H0:qQz5Tgof+DdpS1+djctLSHiZ0
MD5:	E4EC57E8508C5C4040383EBE6D367928
SHA1:	B22BCCE36D9FDEAE8AB7A7ECC0B01C8176648D06
SHA-256:	8AD9E47693E292F381DA42DDC13724A3063040E51C26F4CA8E1F8E2F1DDD547F
SHA-512:	77D5CF66CAF06E192E668FAE2B2594E60A498E8E0CCEF5B09B9710721A4CDB0C852D00C446FD32C5B5C85E739DE2E73CB1F1F6044879FE7D237341BBB6F2782
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 3% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....D.... ..PE..L.....@.....!.....C .....0.....#..t....!..O..... .....|.....`..... .....`.....(...Z... .....D$...*..5...j...f...PRj.....j..S.ERROR!.Corrupt Data!... ..f.`P....h.p..j..P..C.h.....<$.3f....t...;S.^.....Vj.PWj.j.Vj.PW....Y.Yf..\.....X..t...:...E.....Z...t..$.4..l$..m..J...R...z... .%XZt..).....u.....A.....r..j.3.3.0_.K~.....s.3.....s...$A.'.....lu....=.....=.....$.....u.....V+.48.^.I..... ...G...F.....^..$.....8.....[..... .....7..... .....".4"....."..

C:\Users\user\AppData\Local\Temp\dup2patcher.dll

Process:	C:\Users\user\Desktop\sublime.text.v4152-patch.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	808960
Entropy (8bit):	5.828626402420864
Encrypted:	false
SSDEEP:	12288:Wc2ldltF9jWPTePnnXSwJ0sX3cw5eD1+6QNZgYTgIQH:TmnXSwJ0s8PI6WgVI
MD5:	5B7F89778E8F916541AE3030F2330638
SHA1:	AA07437488CF42D38B75BE4D144DCFF6DCF51BE8
SHA-256:	3E56B33860EE05F5A51AE21693BE5E12349D65516A5A1E00EB3154ABD940BC65
SHA-512:	B7BB28A648CA9C0B62B8A1E6006FC1A119760053FB42919EB1EEF698FCFE84024EE598E6DC33BF757F1E0EA489EE38B2D56B0628B029050F79D773FDE6E1C03F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GenericPatcher, Description: Yara detected Generic Patcher, Source: C:\Users\user\AppData\Local\Temp\dup2patcher.dll, Author: Joe Security
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....bd.....! ....n#.....u.....u.....u.....u.....u.....Rich..... .....PE..L.....P.....!..... .....@.....p.....P.....0.....H.....D..... .....text...J..... ....rdata.....@..@.data....W.....@....rsrc.....0.....@....reloc..Z.....N.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.998608383385908
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:	sublime.text.v4152-patch.exe
File size:	840'704 bytes
MD5:	15f0f046c5a23f898a4162724a16be09
SHA1:	106888897e37c6b5fbb26fb7ed1ad2d264aa2e9e
SHA256:	5ee68867759bd9dd852bd874db2716721d9d6671586533c8b62f820b18e690c5
SHA512:	1df7f5bb90caf04d2df864ea1e4a6a1decf471957a8bf0214b346fc9e621b241d0c6204568209c34a6798a36a0147037b5a202a94b5afe019e729f600b373695
SSDEEP:	24576:qAXm+fFb4LUYEVjfFkkG9K/N088z6tsAHMU48Obds6:qAXmkb4LUvV7C9K10F6Hs2Ob
TLSH:	6C0533A045E02712F3BAC87D4FD4B6FE907D0B991D3BCC9632DA65A3D926F4C240931A

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.m.-...-...-.....,...B.....-...<...B...,...B...,...B...,...Rich-.....PE..L.....P.....+.....

File Icon

Icon Hash:	629c8e879e07e21d

Static PE Info

General

Entrypoint:	0x40102b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x50D4CDC2 [Fri Dec 21 20:59:46 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	dc73a9bd8de0fd640549c85ac4089b87

Entrypoint Preview

Instruction
call 00007F3EEC52E8CCh
push 00000000h
call 00007F3EEC52E9CAh
push ebp
mov ebp, esp
add esp, FFFFFBF4h
push esi
push edi
push ebx
push 00000000h
call 00007F3EEC52E9C9h
mov dword ptr [00403030h], eax
mov dword ptr [ebp-08h], 00000000h
push 0000000Ah
push 00403000h
push 00000000h
call 00007F3EEC52E9A3h
or eax, eax
je 00007F3EEC52E8E3h
mov dword ptr [ebp-04h], eax
push dword ptr [ebp-04h]
push 00000000h
call 00007F3EEC52E9C2h
mov dword ptr [ebp-0Ch], eax
push dword ptr [ebp-04h]
push 00000000h
call 00007F3EEC52E9A9h
or eax, eax

Instruction
je 00007F3EEC52E8C5h
mov dword ptr [ebp-08h], eax
cmp dword ptr [ebp-08h], 00000000h
je 00007F3EEC52E8F4h
push 00000004h
push 00001000h
push dword ptr [ebp-0Ch]
push 00000000h
call 00007F3EEC52E99Dh
mov edi, eax
push dword ptr [ebp-0Ch]
push dword ptr [ebp-08h]
push edi
call 00007F3EEC52E983h
mov dword ptr [ebp-08h], edi
push DEADBEEFh
push dword ptr [ebp-0Ch]
push dword ptr [ebp-08h]
call 00007F3EEC52E804h
cmp dword ptr [ebp-08h], 00000000h
je 00007F3EEC52E8F6h
lea eax, dword ptr [ebp-0000040Ch]
push eax
push 00000400h
call 00007F3EEC52E947h
push 00403004h
lea eax, dword ptr [ebp-0000040Ch]
push eax
call 00007F3EEC52E95Ah
push dword ptr [ebp-0Ch]
push dword ptr [ebp-08h]
lea eax, dword ptr [ebp+0000FBF4h]

Rich Headers

Programming Language:	• [IMP] VS2010 build 30319 • [ASM] VS2010 build 30319 • [RES] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2050	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4000	0xcc7e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd1000	0x34	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x48	.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	0x1f6	0x200	False	0.70703125	data	5.064079900511637	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0x1d8	0x200	False	0.55859375	tar archive (old), type 'P' \300 , seconds \372 , linkname !, comment: duleHandleA	4.270638734332521	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3000	0x34	0x200	False	0.078125	data	0.5689880404256953	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x4000	0xcc7e0	0xcc800	False	0.9700321859718827	data	7.999743265140669	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd1000	0x52	0x200	False	0.123046875	data	0.7360464330211749	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x4138	0x6b0d	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced			0.9986133917168399
RT_RCDATA	0xac48	0xc5800	data			0.9697240901898734
RT_GROUP_ICON	0xd0448	0x14	data			1.05
RT_MANIFEST	0xd045c	0x382	XML 1.0 document, ASCII text, with CRLF line terminators			0.45657015590200445

Imports

DLL	Import
kernel32.dll	DeleteFileA, ExitProcess, FindResourceA, FreeLibrary, GetModuleHandleA, GetProcAddress, GetTempPathA, LoadLibraryA, LoadResource, RtlMoveMemory, SizeofResource, VirtualAlloc, lstrcatA, CloseHandle, CreateFileA, FlushFileBuffers, WriteFile

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: sublime.text.v4152-patch.exe PID: 5480, Parent PID: 3524

General

Target ID:	0
Start time:	05:27:17
Start date:	12/08/2023
Path:	C:\Users\user\Desktop\sublime.text.v4152-patch.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\sublime.text.v4152-patch.exe
Imagebase:	0x1a0000
File size:	840'704 bytes
MD5 hash:	15F0F046C5A23F898A4162724A16BE09
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GenericPatcher, Description: Yara detected Generic Patcher, Source: 00000000.00000002.886505239.0000000000830000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	false

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dup2patcher.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1A11A4	CreateFileA
C:\Users\user\AppData\Local\Temp\bassmod.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C666D6C	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\dup2patcher.dll	0	808960	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 62 64 fd fd 03 0a 92 03 0a 92 03 0a fd fd 21 20 90 03 0a fd 6e 23 18 94 03 0a fd fd 75 fd 90 03 0a 92 03 0b ab 03 0a fd 1c 1c 19 fd fd 03 0a fd fd 75 fd 82 03 0a fd fd 75 fd 93 03 0a fd fd 75 fd 93 03 0a fd fd 75 fd 93 03 0a fd 52 69 63 68 fd 03 0a fd 00 00 00 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	MZ@!L!This program cannot be run in DOS mode.$bd! n#uuuuuRichPEL	success or wait	1	1A11C6	WriteFile
unknown	unknown	2			invalid handle	1	6C666D43	WriteFile
unknown	unknown	39			invalid handle	1	6C666D43	WriteFile
unknown	unknown	2			invalid handle	1	6C666D43	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bassmod.dll	0	34308	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 44 00 00 00 fd 20 00 00 50 45 00 00 4c 01 02 00 fd fd fd 40 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 fd 16 01 00 fd 16 01 00 00 00 00 00 43 20 01 00 00 10 00 00 00 fd 00 00 00 00 00 10 00 10 00 00 00 02 00 00 04 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 30 01 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 14 23 01 00 74 03 00 00 fd 21 01 00 4f 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@D PEL@!C 0#t!O	success or wait	1	6C666D8E	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly