ID: 811712
Sample Name: XF-Sublime-KG.exe
Cookbook: default.jbs
Time: 22:46:49
Date: 19/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

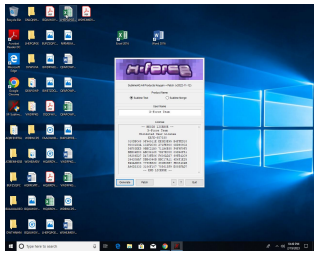
Windows Analysis Report

XF-Sublime-KG.exe

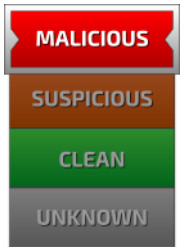
Overview

General Information

Sample Name:	XF-Sublime-KG.exe
Analysis ID:	811712
MD5:	7302bf7492812..
SHA1:	576204f2c01ca..
SHA256:	e2ee8ae987d7…
Infos:	



Detection

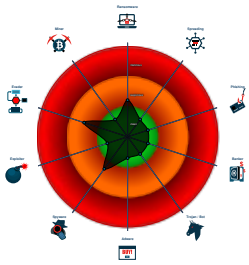


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for drop…
- PE file has nameless sections
- Machine Learning detection for sam…
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Sample file is different than original …
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- XF-Sublime-KG.exe (PID: 5156 cmdline: C:\Users\user\Desktop\XF-Sublime-KG.exe MD5: 7302BF7492812404394214BCBFB334A5A)
  - XF-Sublime-KG.exe (PID: 5128 cmdline: C:\Users\user\AppData\Local\Temp\XF-Sublime-KG.exe MD5: F6DC9BF22EC5259F4428E4B33863E270)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

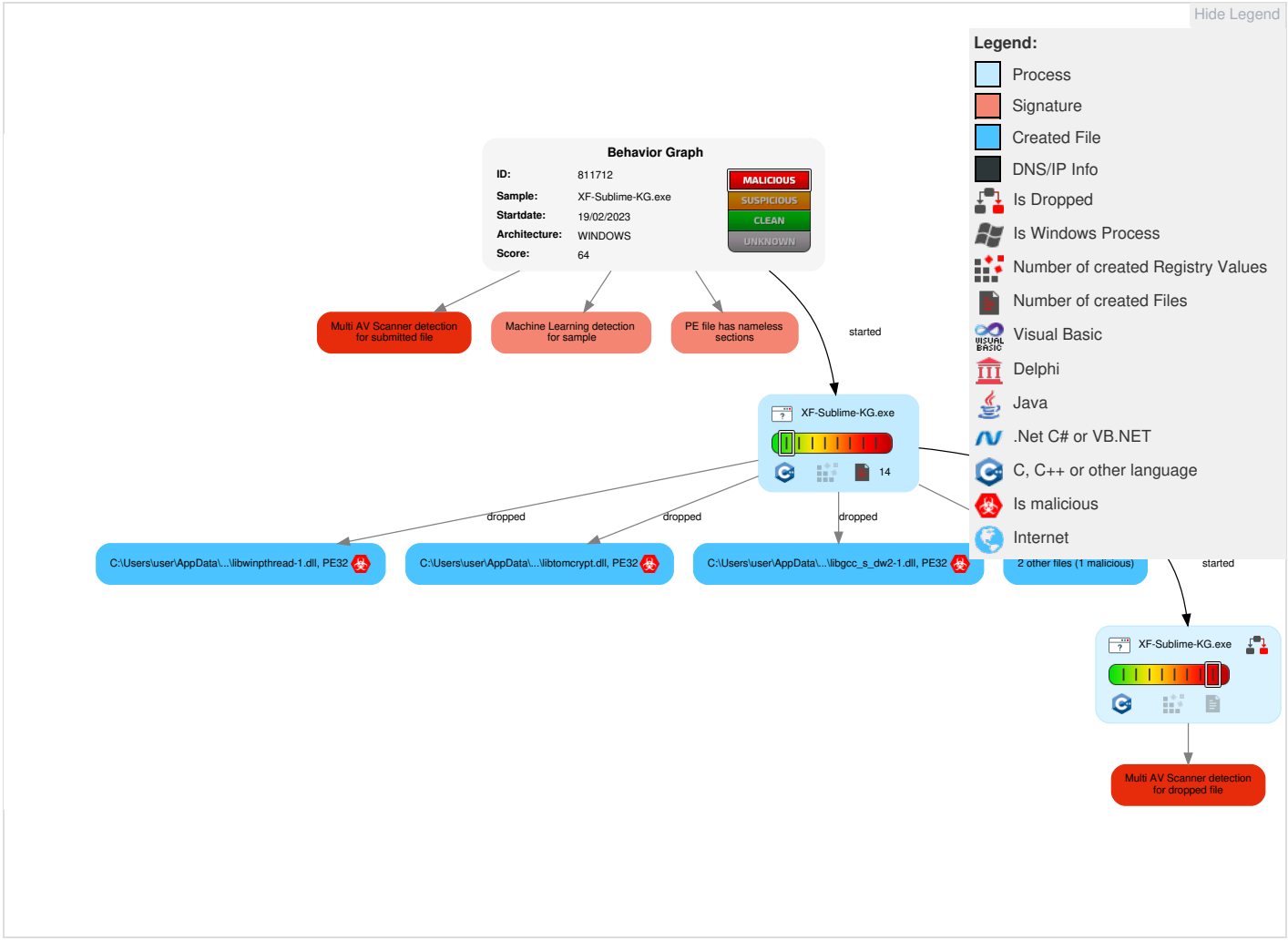
System Summary

PE file has nameless sections

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	1 Native API	Path Interception	1 Access Token Manipulation	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Process Injection	1 Access Token Manipulation	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard 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)	3 1 Software Packing	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Process Injection	NTDS	1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

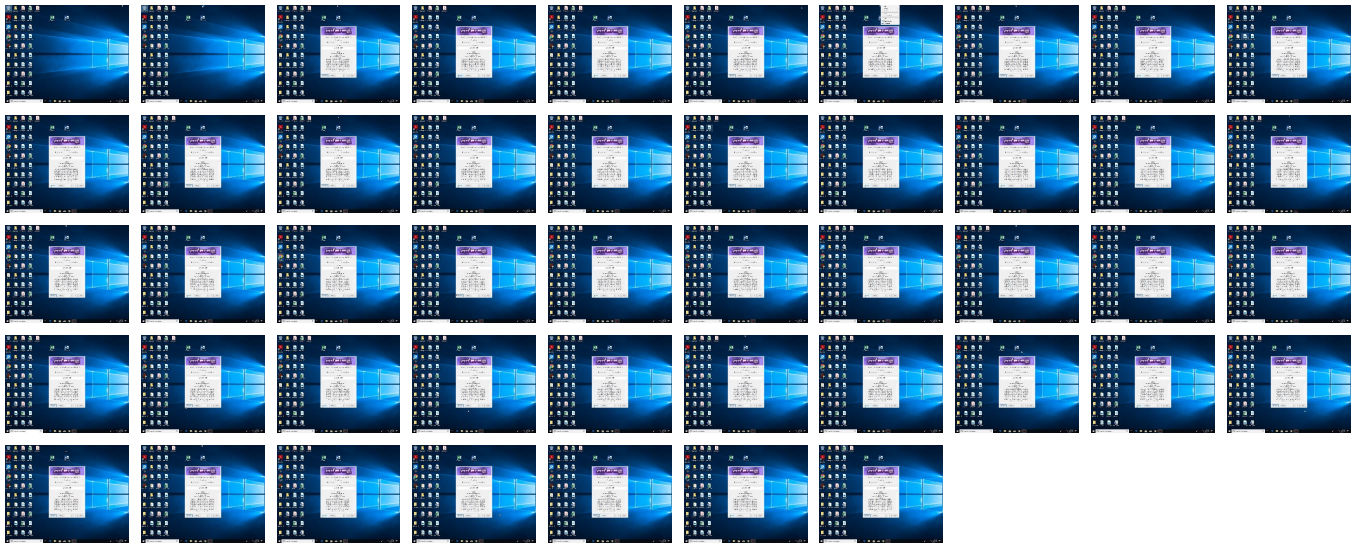
Behavior Graph



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
XF-Sublime-KG.exe	42%	ReversingLabs	Win32.Trojan.Generic	
XF-Sublime-KG.exe	36%	Virustotal		Browse
XF-Sublime-KG.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\BASSMOD.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\BASSMOD.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\XF-Sublime-KG.exe	23%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\XF-Sublime-KG.exe	19%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\libgcc_s_dw2-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libgcc_s_dw2-1.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\libtomcrypt.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libtomcrypt.dll	1%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\libwinpthread-1.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.XF-Sublime-KG.exe.286606e.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.XF-Sublime-KG.exe.6f500000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.XF-Sublime-KG.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	XF-Sublime-KG.exe	false		high
http://mingw-w64.sourceforge.net/X	XF-Sublime-KG.exe, 00000000.00000002.521940680.0000000002865000.00000004.00000020.00020000.00000000.sdmp, XF-Sublime-KG.exe, 00000001.00000002.522451285.00000000734C6000.00000008.00000001.01000000.00000005.sdmp, nst2ED8.tmp.0.dr, libwinpthread-1.dll.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	811712
Start date and time:	2023-02-19 22:46:49 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 15s
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:	14
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:	XF-Sublime-KG.exe

Detection:	MAL
Classification:	mal64.winEXE@3/6@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 13.9% (good quality ratio 11.3%) • Quality average: 55.6% • Quality standard deviation: 38.9%
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 • Changed system and user locale, location and keyboard layout to English - United States

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.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\XF-Sublime-KG.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:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • 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.^.l..... ...G...F.....^..$.....8.....[..... .....7..... .....".."4".....""..

C:\Users\user\AppData\Local\Temp\XF-Sublime-KG.exe

Process:	C:\Users\user\Desktop\XF-Sublime-KG.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	113152
Entropy (8bit):	6.869170124491304
Encrypted:	false
SSDEEP:	1536:9FagSlkXMcUcpXBOdGuyjKk54BgtztXHif73qsfiTpJKQJbPP0:eGrUcpXBqNyek54CRtHifj5fiTpQQNP
MD5:	F6DC9BF22EC5259F4428E4B33863E270
SHA1:	ED3758FCD5B85C30423B613E92F73E775AF86F50
SHA-256:	EDC3D74FA71B78C8EC482C6C36C7304F619C3CD92F90AD4E4645EEBC41524CFB
SHA-512:	833544B7B41924F454498D1F4806898C3D0DAB06EAAE0AEEDC6A99E6D1E080D042EAA86915A540579149AC7D2F9FFC8DC267808EC6DAA43D594232EB00FD3AC3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23% • Antivirus: Virustotal, Detection: 19%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....oc.....$..... .....@.....0..... ..@... ....P..`..... .....d.....".....text...t.....`.P`.data.....@.`..rdata..h..... .....@.`@.eh_fram..... .....@.0@.bss.....`..idata..... .....@.0..CRT....0....0.....@.0..tls.....@..... ..@.0..rsrc...`....P..`.....@.0..reloc..... .....@.0B.....

C:\Users\user\AppData\Local\Temp\libgcc_s_dw2-1.dll

Process:	C:\Users\user\Desktop\XF-Sublime-KG.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	125637
Entropy (8bit):	6.268647580482249
Encrypted:	false
SSDEEP:	3072:uG8lWU0dy47MlXxu3d49XrEh2AC+tUB8I3+jz6pq:58lWUP47MlXxv9XQh2ACJBujz6w
MD5:	E45E405491FE9C857E27ED81FF7CEBEA
SHA1:	994B5962E7E6910D5EE0EF1DD5316A3CA77C3F4B
SHA-256:	66AC4CCC4D40BE26842CD87665924171952511 4C3D7BFA93C64198918AF1CB27
SHA-512:	409C5FD12099770571168F54AF644B5F000CFC416EE12A76F63EBCABE9124CFD3B36AA4CEE24D66EC9D0C7762191D14F22740C2585A06EAFCBF044CBA4589C8
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....,....&#...$.d.....n.....`..... ..@... .....u.... ..x.....P..... .....text....b.....d.....`.P`.data...(.....h.....@.0..rdata...".....$...j.....@.`@/4.....4.....6.....@.0@.bss.....0..edata..u.....@.0@.idata..x.... .....@.0..CRT.....0..... .....@.0..tls.....@.....@.0..reloc.....P.....@.0B.....

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

Process:	C:\Users\user\Desktop\XF-Sublime-KG.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed

Category:	dropped
Size (bytes):	373760
Entropy (8bit):	7.891684055333905
Encrypted:	false
SSDEEP:	6144:xzHNJ6O1FEAiz0WJDD6+OM3V+O/oYDOZ2fwHExZkWYB6KbK3xy+BH/osej:xz6O3HW0uXzOM3IOAYDOZ2fw6Y3+BH/x
MD5:	77B01DD3263B26E9D85F23B0F3E669C6
SHA1:	30A9C56D53271E93E7D880B2CAED0EA771E99D6D
SHA-256:	6A011B173D149E6B667B9DA3569BB6B05E6038249AB5F020AD448086E02CEDAF
SHA-512:	1F8C5C36696536624B849161EE0777F49485C2FB01464E3D4E5EDD131527661140F6ED66AD41892E6A0D1B27B07CED738D8DAD1CE2F8BACF58A4AEF84DB62E58
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#...#.`...`..... ....Po..... ....!...Y... .....z.....8.....UPX0.....UPX1....`.....V.....@...UPX2 .....`... ...\...X.....@...3.96.UPX!.....,.p.8.g.....Q...p..&..O}.....$.....|.....&.....WVSD..D$$..ur..R...~W.....1...B.'._...({..M..a.r.....5B.(.....,.....[.....s...[^_.....T...w.. .d....=..X.1....t<..F9.....1.....f0l.5....*...K..D.Dt..T$(..... ..$.....&8.4..bsm.....f...I....~....;Q...{..0.v..'..S.A.o .....a.np.....q,....O.;YUD:.....{..UW..V.....S..R.....ui.3|k..B Hp....|4...M4$&..B-.\..r3%..)\..._\.(J.1.:....?.G...].~..Cig...m]...=Z..t.....<8...Z.....n!].v..`%.[-.

C:\Users\user\AppData\Local\Temp\libwinpthread-1.dll

Process:	C:\Users\user\Desktop\XF-Sublime-KG.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	69064
Entropy (8bit):	6.103634473024697
Encrypted:	false
SSDEEP:	768:TMPAo9wofbyiXcCo1QWb0r2jBOGL6rqEXzPm3YRiFWinrrF:wP+KPXMAqBiNPm3YdinV
MD5:	695D4B0B03267985AA0A74DCBF3E3A0E
SHA1:	2C3093161CEF7BB823804BAC7099202AAD23729D
SHA-256:	B87CEEA97753D556C4598776C0AC47E5B11797E82416406B418296BD8159E8B2
SHA-512:	EFDE8057DD2CD603970A4C5EC27E3E25A6449EB5BB66C2A8AC9DF45E65D932852F5E24584A2CA166D73E851DA0CC781B8B6A1D40D2A61BE0A1321B2D12F12EC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....V.....#...$.....d..... .@... .....0..t....`..P.....p.....1..H.....text.....`.P`.data...L.....@.0..rdat a.....@.0@/4.....|3.....4.....@.0@.bss.....0..edata.....@.0@.idata..t....0.....@.0..CRT....0....@..... .....@.0..tls.....P.....@.0..rsrc...P....`.....@.0..reloc.....p.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\nst2ED8.tmp

Process:	C:\Users\user\Desktop\XF-Sublime-KG.exe
File Type:	data
Category:	dropped
Size (bytes):	720111
Entropy (8bit):	7.480304861528708
Encrypted:	false
SSDEEP:	12288:qTgIQHB8IWUOUhOCtz6O3HW0uXzOM3IOAYDOZ2fw6Y3+BH/osOPm3Y1Ifkh:bIo8M+vAO32BzOM3DAYgAG3+BH/osOP6
MD5:	B1729793C9AA6FCDC4AB305EAC1738B8
SHA1:	828C07332696A03821FA307496059BAAAB3CD8B2
SHA-256:	6AB9E18291A65123CDB0A175184663EDFD79C58F2A2FE96CCCE05D9A067A30C6
SHA-512:	EFAADB7C043B4B115EA219572D29FEBBF7D131EA97362AA3C7D1BCE6358B2483B42B2AD1B63812F402C208582F644BADC11272A53949C735FF37E5A4FA522322
Malicious:	false
Reputation:	low
Preview:	F.....,.....,.....D.....F..... .....i..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.970357138752211
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:	XF-Sublime-KG.exe
File size:	531393
MD5:	7302bf749281240439214bcbfb334a5a
SHA1:	576204f2c01ca78370c25d3147f8cbed73b7c205
SHA256:	e2ee8ae987d783ec5cd4ee7cc8ac968f0ddd85cbd40eacce0df57dea00dc1417
SHA512:	9b333ceff330d544326dfbfc546f88823aaf4f2b9649aa3b2df5148ed5904d5437eb08470e12bbd693ac8ca80778cbd8400cfa2298afb95ae13848573051afc4
SSDEEP:	12288:nYxTGmN/OZv6l2W0DB9BQ18QtPCKxReCh18xMb9hk:nYNGm1AvaTtPCKRhWS3k
TLSH:	86B41291BAE19463FB85877169362B1FC9F87CF50991AA3B23181E8FB45D720DE0D306
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	fcdcecf0f0e4f6fa

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h

Instruction
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FF428BE4E7Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FF428BE4E4Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0x39a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.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	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0x39a0	0x3a00	False	0.2095231681034483	data	5.905827843956638	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b190	0x3228	Device independent bitmap graphic, 64 x 128 x 24, image size 12800	English	United States
RT_DIALOG	0x3e3b8	0x100	data	English	United States
RT_DIALOG	0x3e4b8	0x11c	data	English	United States
RT_DIALOG	0x3e5d8	0x60	data	English	United States
RT_GROUP_ICON	0x3e638	0x14	data	English	United States
RT_MANIFEST	0x3e650	0x349	XML 1.0 document, ASCII text, with very long lines (841), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

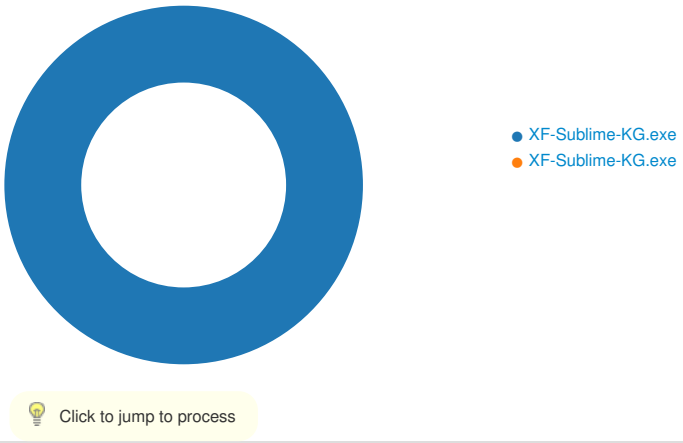
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: XF-Sublime-KG.exe PID: **5156**, Parent PID: **3452**

General

Target ID:	0
Start time:	22:47:45
Start date:	19/02/2023
Path:	C:\Users\user\Desktop\XF-Sublime-KG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\XF-Sublime-KG.exe
Imagebase:	0x400000
File size:	531393 bytes
MD5 hash:	7302BF749281240439214BCBFB334A5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: XF-Sublime-KG.exe PID: **5128**, Parent PID: **5156**

General	
Target ID:	1
Start time:	22:47:46
Start date:	19/02/2023
Path:	C:\Users\user\AppData\Local\Temp\XF-Sublime-KG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\XF-Sublime-KG.exe
Imagebase:	0xb70000
File size:	113152 bytes
MD5 hash:	F6DC9BF22EC5259F4428E4B33863E270
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 23%, ReversingLabs • Detection: 19%, Virustotal, Browse
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly