ID: 365501
Sample Name: IcTy2OaX9w
Cookbook: default.jbs
Time: 16:31:40
Date: 09/03/2021
Version: 31.0.0 Emerald

Table of Contents

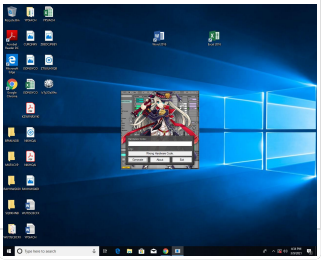
Analysis Report IcTy2OaX9w

Overview

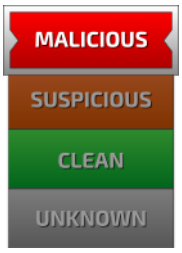
General Information

Sample Name:	IcTy2OaX9w (renamed file extension from none to exe)
Analysis ID:	365501
MD5:	5137f6c1b6fec54..
SHA1:	2acfa6961576086.
SHA256:	72c96f7e2f4823b..
Infos:	

Most interesting Screenshot:



Detection

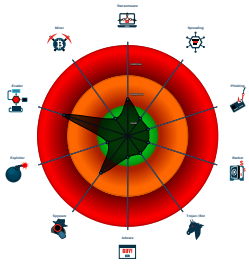


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Contains functionality to detect slee…
- Creates files with lurking names (e.g…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- PE file has nameless sections
- Antivirus or Machine Learning detec…
- Contains capabilities to detect virtua…
- Contains functionality for read data f…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale

Classification



Startup

- **System is w10x64**
- IcTy2OaX9w.exe (PID: 6944 cmdline: 'C:\Users\user\Desktop\IcTy2OaX9w.exe' MD5: 5137F6C1B6FEC54E3C4FCE6261905DD6)
  - keygen.exe (PID: 7020 cmdline: C:\Users\user\AppData\Local\Temp\keygen.exe MD5: 88FB2EFAEF130C7256BF703580A414A7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

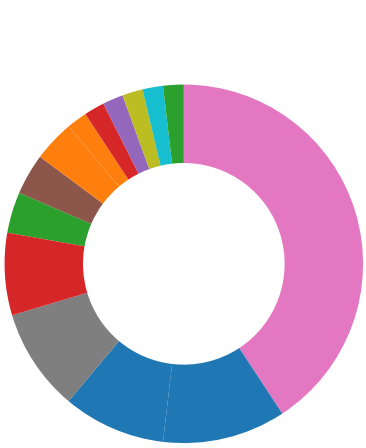
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading
- Networking



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

Creates files with lurking names (e.g. Crack.exe)

PE file has nameless sections

Malware Analysis System Evasion:

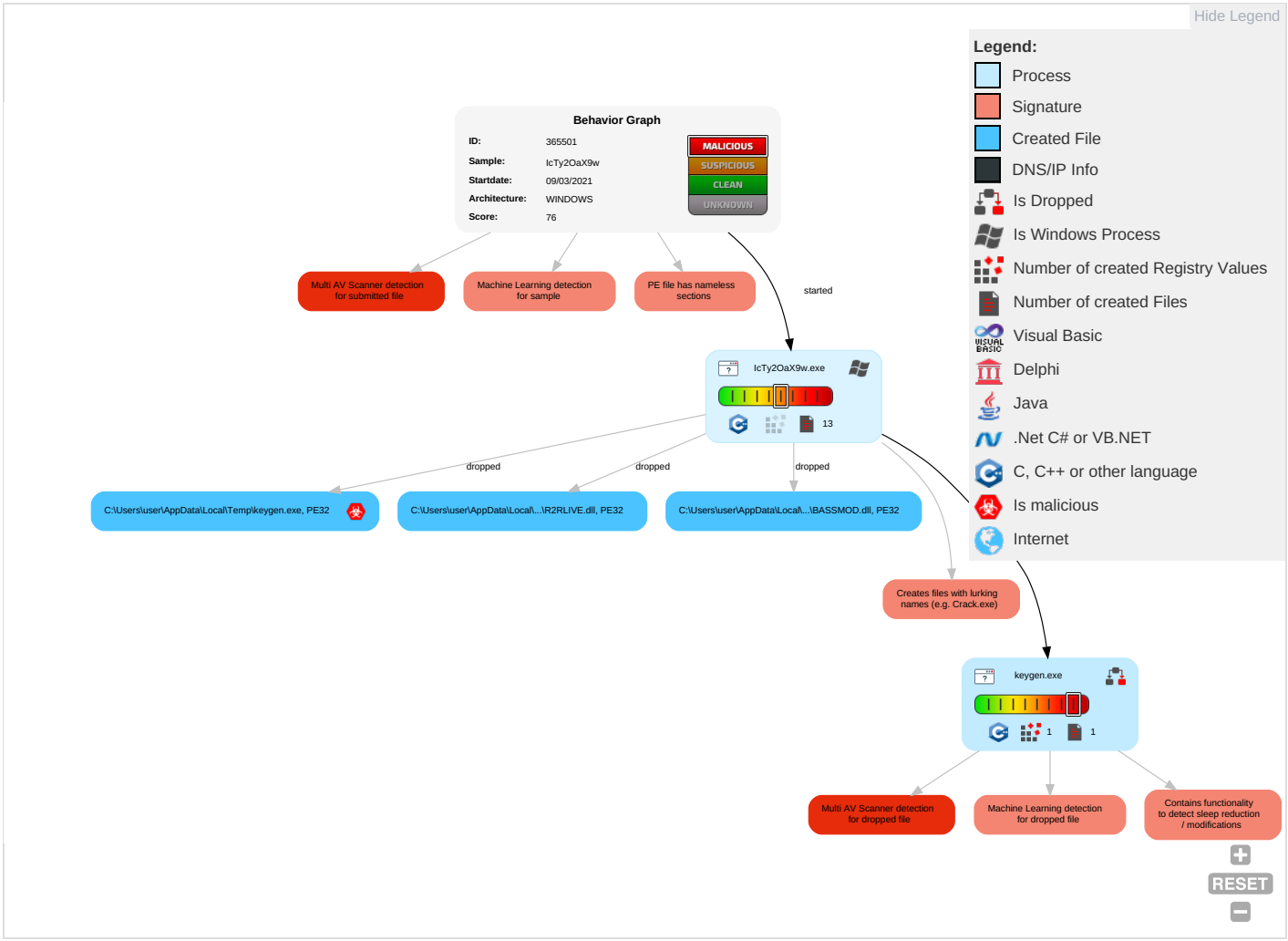
Contains functionality to detect sleep reduction / modifications

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Access Token Manipulation 1	Masquerading 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS Redirect Pl Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 2 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po

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
IcTy2OaX9w.exe	22%	Metadefender		Browse
IcTy2OaX9w.exe	68%	ReversingLabs	Win32.PUA.Generic	
IcTy2OaX9w.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\keygen.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\BASSMOD.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\BASSMOD.dll	3%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\R2RLIVE.dll	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\R2RLIVE.dll	2%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\keygen.exe	30%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\keygen.exe	54%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.IcTy2OaX9w.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.0.IcTy2OaX9w.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.IcTy2OaX9w.exe.28b3edd.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.keygen.exe.10000000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.1.keygen.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
3.1.keygen.exe.10000000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.IcTy2OaX9w.exe.27a1982.4.unpack	100%	Avira	TR/Patched.Ren.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_Error	IcTy2OaX9w.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	IcTy2OaX9w.exe	false		high
http://www.openssl.org/support/faq.html	R2RLIVE.dll.1.dr	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	365501
Start date:	09.03.2021
Start time:	16:31:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IcTy2OaX9w (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
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:	MAL
Classification:	mal76.evad.winEXE@3/5@0/0

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 29.5% (good quality ratio 27.9%) • Quality average: 80.8% • Quality standard deviation: 28%
HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/365501/sample/IcTy2OaX9w.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\BASSMOD.dll	Patch.exe	Get hash	malicious	Browse	
	(32-Bit) 4K Video Downloader v4.12.0.3570 Patch.exe	Get hash	malicious	Browse	
	accd.5.0.x-patch.exe	Get hash	malicious	Browse	
	accd.5.0.x-patch.exe	Get hash	malicious	Browse	
	Patch-iMazing.2.x.exe	Get hash	malicious	Browse	
	taxvxw5BSp.exe	Get hash	malicious	Browse	
	sandboxie.memory.leak.x86-x64-patch.exe	Get hash	malicious	Browse	
	Patch-WinNc.8.x.exe	Get hash	malicious	Browse	
	Patch-WinNc.8.x.exe	Get hash	malicious	Browse	
	testing.exe	Get hash	malicious	Browse	
	test.exe	Get hash	malicious	Browse	
	twk-winupdatepatch.exe	Get hash	malicious	Browse	
	snip (10.exe	Get hash	malicious	Browse	
	Patch.exe	Get hash	malicious	Browse	
	Patch-Movavi.Video.Suite.18.x.exe	Get hash	malicious	Browse	
	Patch.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\BASSMOD.dll	
Process:	C:\Users\user\Desktop\IcTy2OaX9w.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: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Joe Sandbox View:	• Filename: Patch.exe, Detection: malicious, Browse • Filename: (32-Bit) 4K Video Downloader v4.12.0.3570 Patch.exe, Detection: malicious, Browse • Filename: accd.5.0.x-patch.exe, Detection: malicious, Browse • Filename: accd.5.0.x-patch.exe, Detection: malicious, Browse • Filename: Patch-iMazing.2.x.exe, Detection: malicious, Browse • Filename: taxvxw5BSp.exe, Detection: malicious, Browse • Filename: sandboxie.memory.leak.x86-x64-patch.exe, Detection: malicious, Browse • Filename: Patch-WinNc.8.x.exe, Detection: malicious, Browse • Filename: Patch-WinNc.8.x.exe, Detection: malicious, Browse • Filename: testing.exe, Detection: malicious, Browse • Filename: test.exe, Detection: malicious, Browse • Filename: twk-winupdatepatch.exe, Detection: malicious, Browse • Filename: snip (10.exe, Detection: malicious, Browse • Filename: Patch.exe, Detection: malicious, Browse • Filename: Patch-Movavi.Video.Suite.18.x.exe, Detection: malicious, Browse • Filename: Patch.exe, Detection: malicious, 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\R2RLIVE.dll	
Process:	C:\Users\user\Desktop\IcTy2OaX9w.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	717824
Entropy (8bit):	6.647670632746934
Encrypted:	false
SSDEEP:	12288:0UEARqlP7Vu7N8Oe/6Wi4MhgmIk2xxaoy9kFDH+AYrdshhunRgyGN/o9aWEnLiiG:0U9AlP7Qp8t/6WnCgTwrlRg1vLy2C
MD5:	4CE264468BE29F6504EB745D11AA1D5C
SHA1:	072B84CBBDFA4EE945319DD338E171C2078DF455
SHA-256:	33339FD831B14D39514593CF7494BA1985DF6E32DBEF166B70D94EBAAD78CD3B
SHA-512:	E85885BE024B39C6EBB1BC041FCCE8545F6266FC26EBB1D2890E3C3A94D987397D67230634C3B973ED9E097ED591BA6577BB7F1CCA50FFCD73564DB04E3C1D BD
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.....X.....I.....I.....I.....L.....a.....a.....a.. ....Rich.....PE..L.....5`.....!.....t.....P.....@.....P.....P.....Dc...y.....y..@.....\..... .....text...!..... ..`.rdata.....@..@.data....B.....v.....@....reloc..Dc.....d.....@..B.....

C:\Users\user\AppData\Local\Temp\bgm.xm	
Process:	C:\Users\user\Desktop\IcTy2OaX9w.exe
File Type:	"Marble \032FastTracker v2.00 \004\001\024\001"
Category:	dropped

C:\Users\user\AppData\Local\Temp\bgm.xm	
Size (bytes):	1089359
Entropy (8bit):	4.519076933548576
Encrypted:	false
SSDEEP:	24576:njg85PbKWstZdIzNIPRnuEHDGLG5nyQweozKajh/q0nqVVjAsOktahU5F+eOohVz:njgcPuWs6zNIeLG5nyQweozKa1/q0nqH
MD5:	EAC249A6CBD92E5A744F1921261B4134
SHA1:	3C1BE061F209BF9CEF151399F896A1E7927BB2CB
SHA-256:	9AE311E672F224A27350DD37CCE871187377531741DF048082B9CB680CD12882
SHA-512:	3CDB465C746C816B5F9BADBE10020A636ACA694C1992E076CB251F81BA9CCA158BA5455587D0BB966743B943CE88AD0C99C74D39664C55723E169D070A79945
Malicious:	false
Reputation:	low
Preview:	Extended Module: Marble .FastTracker v2.00 .....0.....#.X.....!"...."..... .....%.IP...a.IP..a..... ....a.DP..aDP.....

C:\Users\user\AppData\Local\Temp\keygen.exe	
Process:	C:\Users\user\Desktop\IcTy2OaX9w.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	480775
Entropy (8bit):	6.016763038477501
Encrypted:	false
SSDEEP:	6144:tPA4GcGvY6Q4rOQonRBVSszRNAOlsR1GGoIbqUJX8xrW3P0++:tpGVQ4KQonRBVrzRNC1v6kc++
MD5:	88FB2EFAEF130C7256BF703580A414A7
SHA1:	E45068C6282EA2B279767BE11DFE35767EC2F9F9
SHA-256:	2EF24CB81741BCDCCE8FDAE0812ECB86A334B0A98160B4C068D2B59913C3896D
SHA-512:	33B5740B568A0C986CA15F6ADC08A73E92269225F976776CF424D0E3CCEAC1EB89E0E26E58FBD3D25BAC4AE31F4BC8B9D5A20C9C7C2808C2C24807120C62EE42
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 30%, Browse • Antivirus: ReversingLabs, Detection: 54%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1Gy.u&..u&..u&...1..h&....H.t&..f.J.w&....J.{&.....p&..u&...&...1H..&.. .1w._&...-I.t&...1M.t&..Richu&.....PE..L....<.Y..... .....0....@.....;.....(..... ...@.....text.... ....`.rdata...p...0...h.. .....@....data....@.....@..... ....

C:\Users\user\AppData\Local\Temp\nsk94DF.tmp	
Process:	C:\Users\user\Desktop\IcTy2OaX9w.exe
File Type:	data
Category:	dropped
Size (bytes):	2324680
Entropy (8bit):	6.125528514521051
Encrypted:	false
SSDEEP:	49152:KIGjgcPuWs6zNIeLG5nyQweozKa1/q0nqVVjAsOktahU5F+eOohVOq8Vnk8ZnAkA:fG8cPuW9zNIeLG5nyQweozKapq0nqVVK
MD5:	56B5212CA326AC64C540DB0555DC47D2
SHA1:	57BA15AB1EF80F4E97668A36A3ECBF368AD9DD83
SHA-256:	C76CFBE65020F08CA4E860F0BC7F387539E49B7B63B0A04C05575B62EDA7939D
SHA-512:	321F0B81D7E5942E43FD412E3796D4D0A58651A9B61A17F5234CAB37FB6F4D547712206FE0308FD5FE2483A522F91D2B085B046D851412240197C7AF8E52F762
Malicious:	false
Reputation:	low
Preview:	Z.....,.....,.....D.....x.....Z..... .....0..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

General

Entropy (8bit):	7.876265415322576
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:	IcTy2OaX9w.exe
File size:	1159926
MD5:	5137f6c1b6fec54e3c4fce6261905dd6
SHA1:	2acfa6961576086cb34376222cca49027b77871d
SHA256:	72c96f7e2f4823bb9f28944c96aa1b737be20edd52ca97b699085d3498e4ab74
SHA512:	762ccc51cb1f361ec9d44971015bfeef346f5dc0162d241f6e052bcd4ddb201655342fc21a3e8fe12243e678638e086f0c403eb01a6e52530f89f08f29e3e4a4
SSDEEP:	24576:scLyLVBj7bonifxHi8nnM6+uRCy/4cZTKRZiKx9j1zp9KtyUHW:sAOsif1TMC1wcZTK+KZzxUHW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L...2.oZ.....b.....

File Icon

Icon Hash:	29e8f0f0eaec6882

Static PE Info

General

Entrypoint:	0x403328
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5A6FED32 [Tue Jan 30 03:57:38 2018 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:	57e98d9a5a72c8d7ad8fb7a6a58b3daf

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh

Instruction
cmp ax, 00000006h
mov dword ptr [0042472Ch], eax
je 00007FD8BC8CC553h
push ebx
call 00007FD8BC8CF642h
cmp eax, ebx
je 00007FD8BC8CC549h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007FD8BC8CF5BEh
push esi
call dword ptr [004080A0h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007FD8BC8CC52Dh
push 0000000Ah
call 00007FD8BC8CF616h
push 00000008h
call 00007FD8BC8CF60Fh
push 00000006h
mov dword ptr [00424724h], eax
call 00007FD8BC8CF603h
cmp eax, ebx
je 00007FD8BC8CC551h
push 0000001Eh
call eax
test eax, eax
je 00007FD8BC8CC549h
or byte ptr [0042472Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [00408288h]
mov dword ptr [004247F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FCF0h
call dword ptr [00408178h]
push 0040A1ECh

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	0x8428	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0x22910	.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	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x298	.rdata

Name	Virtual Address	Virtual Size	Is in Section
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	0x6077	0x6200	False	0.659598214286	data	6.40397102665	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1248	0x1400	False	0.4287109375	data	5.04426133984	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a838	0x400	False	0.646484375	data	5.22445131085	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0x22910	0x22a00	False	0.598636337996	data	6.06462205727	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d280	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x3daa8	0xd3f8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x4aea0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x4d448	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x4e4f0	0x988	data	English	United States
RT_ICON	0x4ee78	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x4f2e0	0x100	data	English	United States
RT_DIALOG	0x4f3e0	0x11c	data	English	United States
RT_DIALOG	0x4f500	0x60	data	English	United States
RT_GROUP_ICON	0x4f560	0x5a	data	English	United States
RT_MANIFEST	0x4f5c0	0x349	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, CreateFileA, GetFileSize, GetModuleFileNameA, ReadFile, GetCurrentProcess, CopyFileA, Sleep, GetTickCount, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, ExitProcess, SetCurrentDirectoryA, GlobalLock, CreateThread, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, GetExitCodeProcess, WaitForSingleObject, CompareFileTime, SetFileAttributesA, GetFileAttributesA, GetShortPathNameA, MoveFileA, GetFullPathNameA, SetFileTime, SearchPathA, CloseHandle, lstrcmpiA, GlobalUnlock, GetDiskFreeSpaceA, lstrcmpA, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GlobalAlloc, GlobalFree, ExpandEnvironmentStringsA
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, ShellExecuteExA, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, SHFileOperationA
ADVAPI32.dll	AdjustTokenPrivileges, RegCreateKeyExA, RegOpenKeyExA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, RegEnumValueA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

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

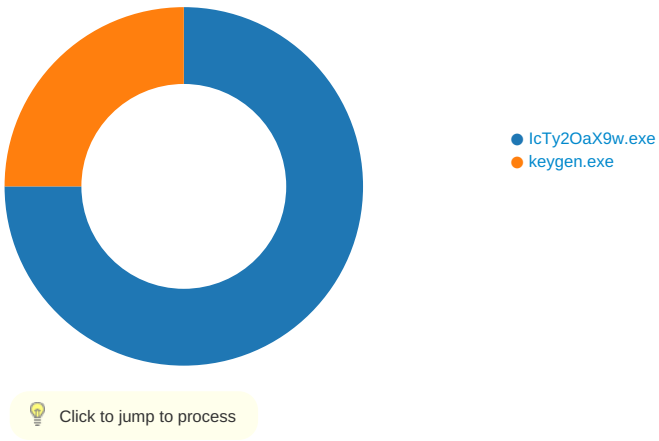
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: IcTy2OaX9w.exe PID: 6944 Parent PID: 5624

General

Start time:	16:32:27
Start date:	09/03/2021
Path:	C:\Users\user\Desktop\IcTy2OaX9w.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\IcTy2OaX9w.exe'
Imagebase:	0x400000
File size:	1159926 bytes
MD5 hash:	5137F6C1B6FEC54E3C4FCE6261905DD6
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\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsp94AF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsk94DF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CD0	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40574A	CreateDirectoryA
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	405C99	CreateFileA
C:\Users\user\AppData\Local\Temp\bgm.xm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Temp\keygen.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA
C:\Users\user\AppData\Local\Temp\R2RLIVE.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405C99	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsp94AF.tmp	success or wait	1	40359F	DeleteFileA

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\nsk94DF.tmp	unknown	19614	5a 09 00 00 88 00 00 2c 01 00 00 00 00 00 00 2c 01 00 00 01 00 00 00 44 05 00 00 0b 00 00 00 78 06 00 00 00 00 00 00 b8 08 00 00 01 00 00 00 5a 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 a2 00 00 00 f1 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Z.......,.......,.......D..... ..x...............Z...........	success or wait	104	405D2E	WriteFile
C:\Users\user\AppData\Local\Temp\BASSMOD.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 44 00 00 00 cd 20 00 00 50 45 00 00 4c 01 02 00 f5 88 d5 40 00 00 00 00 00 00 00 00 e0 00 0e 21 0b 01 06 00 88 16 01 00 88 16 01 00 00 00 00 00 43 20 01 00 00 10 00 00 00 d0 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 00 10 00 00 00 14 23 01 00 74 03 00 00 c4 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 00 f0 8b 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.... ..PE..L......@.......... .!................C ....0 ....#..t....!..O.........	success or wait	3	405D2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bgm.xm	unknown	16384	45 78 74 65 6e 64 65 64 20 4d 6f 64 75 6c 65 3a 20 4d 61 72 62 6c 65 20 20 20 20 20 20 20 20 20 20 20 20 20 20 1a 46 61 73 74 54 72 61 63 6b 65 72 20 76 32 2e 30 30 20 20 20 04 01 14 01 00 00 30 00 00 00 10 00 23 00 58 00 01 00 05 00 8e 00 00 00 01 01 04 02 11 03 05 06 07 21 22 09 08 09 0a 22 09 0b 0c 0b 0c 0d 0f 0e 10 10 12 13 14 15 16 17 18 17 1a 19 19 1b 19 1c 18 1d 16 1e 20 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Extended Module: Marble .FastTracker v2.00 .. ....0.....#.X................ .!"...."...........................	success or wait	67	405D2E	WriteFile
C:\Users\user\AppData\Local\Temp\keygen.exe	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 47 79 a6 75 26 17 f5 75 26 17 f5 75 26 17 f5 fb 31 18 f5 68 26 17 f5 f6 2e 48 f5 74 26 17 f5 66 2e 4a f5 77 26 17 f5 f6 2e 4a f5 7b 26 17 f5 8f 05 0e f5 70 26 17 f5 75 26 16 f5 ce 26 17 f5 fb 31 48 f5 03 26 17 f5 fb 31 77 f5 5f 26 17 f5 99 2d 49 f5 74 26 17 f5 fb 31 4d f5 74 26 17 f5 52 69 63 68 75 26 17 f5 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e3 3c d2 59 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......1Gy.u&..u&..u&...1..h &.....H.t&..f.J.w&.....J.{&...... p&..u&...&...1H..&...1w._&.. .- I.t&...1M.t&..Richu&.......... PE..L....<.Y...	success or wait	30	405D2E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\R2RLIVE.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 b3 8e f6 5a f7 ef 98 09 f7 ef 98 09 f7 ef 98 09 92 89 9b 08 fb ef 98 09 92 89 9d 08 58 ef 98 09 92 89 9c 08 e5 ef 98 09 49 9e 9d 08 ea ef 98 09 49 9e 9c 08 e7 ef 98 09 49 9e 9b 08 ef ef 98 09 4c 8e 9c 08 bf ee 98 09 92 89 99 08 fe ef 98 09 f7 ef 99 09 9f ef 98 09 61 9d 9c 08 f6 ef 98 09 61 9d 98 08 f6 ef 98 09 61 9d 9a 08 f6 ef 98 09 52 69 63 68 f7 ef 98 09 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....Z..... ......X.....I.....I... ....I.....L..... ......a.....a.....a..... Rich.....	success or wait	44	405D2E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IcTy2OaX9w.exe	unknown	512	success or wait	373	405CFF	ReadFile
C:\Users\user\Desktop\IcTy2OaX9w.exe	unknown	16384	success or wait	61	405CFF	ReadFile
C:\Users\user\AppData\Local\Temp\nsk94DF.tmp	unknown	4	success or wait	1	405CFF	ReadFile
C:\Users\user\AppData\Local\Temp\nsk94DF.tmp	unknown	2394	success or wait	1	403147	ReadFile
C:\Users\user\AppData\Local\Temp\nsk94DF.tmp	unknown	4	success or wait	4	405CFF	ReadFile
C:\Users\user\AppData\Local\Temp\nsk94DF.tmp	unknown	16384	success or wait	144	405CFF	ReadFile

Analysis Process: keygen.exe PID: 7020 Parent PID: 6944

General

Start time:	16:32:28
Start date:	09/03/2021
Path:	C:\Users\user\AppData\Local\Temp\keygen.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\keygen.exe
Imagebase:	0x400000
File size:	480775 bytes
MD5 hash:	88FB2EFAEF130C7256BF703580A414A7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, Metadefender, Browse • Detection: 54%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\keygen.exe	unknown	4096	success or wait	1	418E5B	ReadFile
C:\Users\user\AppData\Local\Temp\keygen.exe	unknown	4096	success or wait	1	418E5B	ReadFile
C:\Users\user\AppData\Local\Temp\keygen.exe	unknown	4096	success or wait	76	418E5B	ReadFile
C:\Users\user\AppData\Local\Temp\keygen.exe	unknown	4096	end of file	1	418E5B	ReadFile
C:\Users\user\AppData\Local\Temp\keygen.exe	unknown	4096	success or wait	2	418E5B	ReadFile
C:\Users\user\AppData\Local\Temp\bgm.xm	unknown	4096	success or wait	2	1000C19D	fread
C:\Users\user\AppData\Local\Temp\bgm.xm	unknown	1081344	success or wait	1	1000C19D	fread
C:\Users\user\AppData\Local\Temp\keygen.exe	unknown	307200	success or wait	1	418E5B	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis