ID: 247495
Sample Name: iceix_1.2.0.0.vir
Cookbook: default.jbs
Time: 07:45:42
Date: 20/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

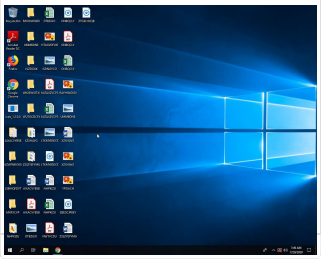
Analysis Report iceix_1.2.0.0.vir

Overview

General Information

Sample Name:	iceix_1.2.0.0.vir (renamed file extension from vir to exe)
Analysis ID:	247495
MD5:	4581c813cbc584…
SHA1:	ae17112eff30ff1d..
SHA256:	fa4bd653c43c8c9..

Most interesting Screenshot:



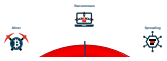
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Detected ZeusVM e-Banking Trojan
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for subm…
- Contains VNC / remote desktop func…
- Machine Learning detection for samp…
- Antivirus or Machine Learning detec…
- Contains functionality to dynamically…
- Contains functionality to enumerate …
- Contains functionality to launch a pr…
- Contains functionality to open a port…

Classification



Startup

- **System is w10x64**
- iceix_1.2.0.0.exe (PID: 1396 cmdline: 'C:\Users\user\Desktop\iceix_1.2.0.0.exe' MD5: 4581C813CBC584530B75C58C30D8B29B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

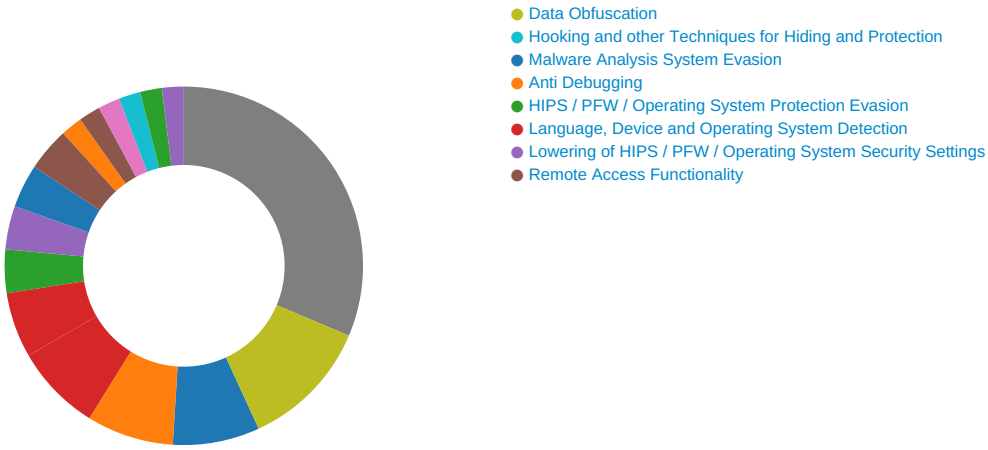
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Cryptography
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Protection of GUI
- System Summary



Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud:

Detected ZeusVM e-Banking Trojan

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Remote Access Functionality:

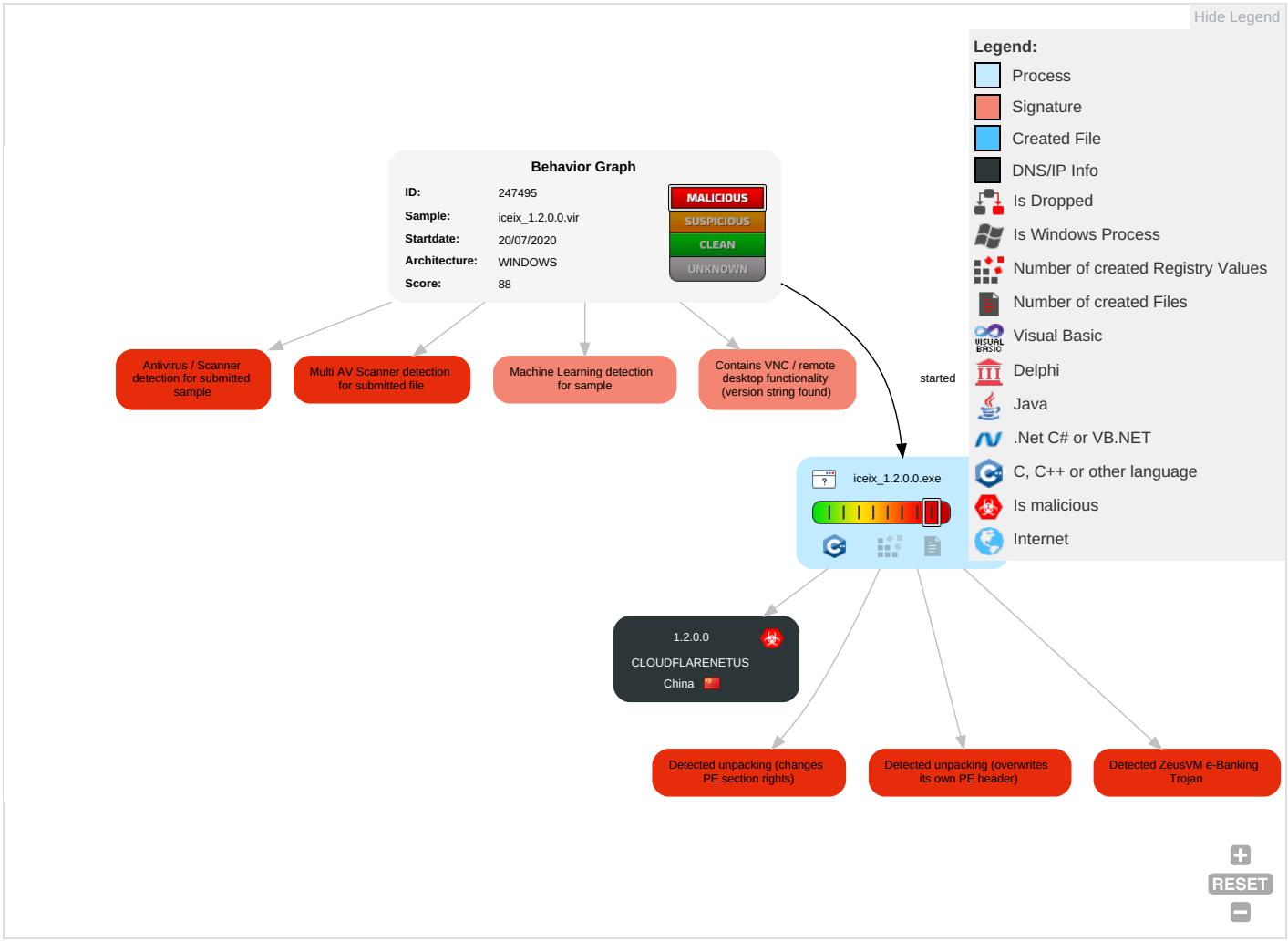
Contains VNC / remote desktop functionality (version string found)

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 1	Execution through API 1	Create Account 1	Valid Accounts 1	Software Packing 2 3	Input Capture 1 1	System Time Discovery 2	Remote File Copy 1	Input Capture 1 1	Data Encrypted 1	Commonly Used Port 1	Eavesdrop on Insecure Network Communicatio
Replication Through Removable Media	Graphical User Interface 1	Valid Accounts 1	Access Token Manipulation 1 1	Obfuscated Files or Information 2	Network Sniffing	Account Discovery 1	Remote Desktop Protocol 1	Clipboard Data 1	Exfiltration Over Other Network Medium	Remote File Copy 1	Exploit SS7 to Redirect Phon Calls/SMS
External Remote Services	Windows Management Instrumentation	Application Shimming 1	Application Shimming 1	Valid Accounts 1	Input Capture	Security Software Discovery 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Cryptographic Protocol 2	Exploit SS7 to Track Device Location
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Access Token Manipulation 1 1	Credentials in Files	File and Directory Discovery 1	Logon Scripts	Input Capture	Data Encrypted	Remote Access Tools 1	SIM Card Swap
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Install Root Certificate 1	Account Manipulation	System Information Discovery 3	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol	Manipulate Device Communicatio
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	DLL Search Order Hijacking	Brute Force	Network Share Discovery 1	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port	Jamming or Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Software Packing	Two-Factor Authentication Interception	Process Discovery 1	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port	Rogue Wi-Fi Access Points
Spearphishing via Service	Third-party Software	Logon Scripts	Process Injection	Indicator Blocking	Bash History	System Owner/User Discovery 1	Remote Desktop Protocol	Clipboard Data	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol	Downgrade to Insecure Protocols

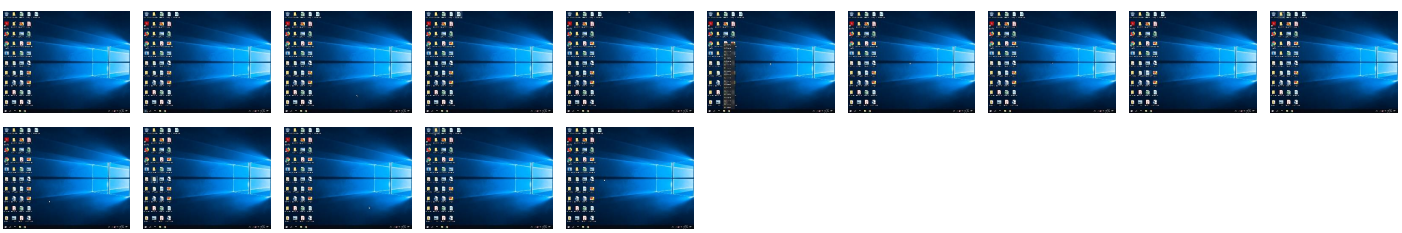
Behavior Graph



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
iceix_1.2.0.0.exe	89%	Virustotal		Browse
iceix_1.2.0.0.exe	77%	Metadefender		Browse
iceix_1.2.0.0.exe	92%	ReversingLabs	Win32.Trojan.Zbot	
iceix_1.2.0.0.exe	100%	Avira	TR/Crypt.XPACK.Gen8	
iceix_1.2.0.0.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.iceix_1.2.0.0.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.iceix_1.2.0.0.exe.21b0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
0.2.iceix_1.2.0.0.exe.400000.0.unpack	100%	Avira	TR/Spy.Zbot.aoqb.5		Download File
0.2.iceix_1.2.0.0.exe.510000.1.unpack	100%	Avira	TR/Spy.Zbot.aoqb.5		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Country	Flag	ASN	ASN Name	Malicious
1.2.0.0	China		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	247495
Start date:	20.07.2020
Start time:	07:45:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	iceix_1.2.0.0.vir (renamed file extension from vir to exe)
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	6
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:	mal88.bank.troj.evad.winEXE@1/0@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 50.3% (good quality ratio 43.4%) • Quality average: 72.4% • Quality standard deviation: 36.3%
HCA Information:	• Successful, ratio: 57% • 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, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
1.2.0.0	UICE.online.OOB.Setup_x64(Version 1.2.0.0).exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	http://app.sizeswatch.com	Get hash	malicious	Browse	• 104.16.126.175
	http://comtechadsl.com/ehepsqm.exe	Get hash	malicious	Browse	• 104.20.74.28
	http://blueeyeswebsite.com/	Get hash	malicious	Browse	• 104.24.110.109
	ATT20893.HTML	Get hash	malicious	Browse	• 104.16.133.229
	ATT84128.HTML	Get hash	malicious	Browse	• 104.16.133.229
	http://https://bit.ly/30cSl6K	Get hash	malicious	Browse	• 104.16.124.96
	http://https://jhmetalinc-my.sharepoint.com/:o:/p/office/EiJ0PCnWDtJHiWQIXRi7bWgB6cFzFQtLhcLET3v8d3NRLA?rtime=ORiHa4Eq2Eg	Get hash	malicious	Browse	• 104.16.132.229
	ATT39268.HTM	Get hash	malicious	Browse	• 104.16.133.229
	payment730.xls	Get hash	malicious	Browse	• 104.27.180.83

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://atcsagacity.com/wp-admin/MYWZIKG/eigyho/s9w0816332646203713g44z0n2u/	Get hash	malicious	Browse	• 172.67.186.191
	http://https://gogoanime1.net/.well-known/acme-challenge/bid/login.php	Get hash	malicious	Browse	• 104.16.132.229
	http://https://lroetrgpfxciziew.frb.io/?bbre=pdsi93reodfxci	Get hash	malicious	Browse	• 104.16.133.229
	http://mapfrecomercial.com/	Get hash	malicious	Browse	• 104.16.202.237
	http://https://event.on24.com/wcc/r/2462461/BB0A869CCD07459AE0E4C73F0AD810E3/1209023?partnerref=connect	Get hash	malicious	Browse	• 104.17.71.206
	http://https://u10500736.ct.sendgrid.net/ls/click?upn=GJ-2Fwg0v0GjXICnjOzCZwjhkRw9-2BbFlj0p-2BETjV5NQUzZanQeaYMDpzIDJ401Kach0E7l_YxCxpoge33FNHhRVcK23d3jJCq3cIHwc-2BD1XeO3y4vWhDSyEnUs6U-2FsQ3r28LvMmBf0-2FyPTfw7LkuX8KPrqtuiBKVLJGudFG5cgos-2FYMheOpZ3KzgDMXMKE-2BA6yiT-2Bi5BQtK80dm1zrijWZnCRa6hF0zjqp3QnkLp0NHHccLK9ZW3lYLn1ntwPI5yxeaqK-2FwMj6c4bzGzF8lmQMxhNRSLY2oartjGJW1716gR3wWT6FnAMuuMr-2BmVOWIDO3doJzx	Get hash	malicious	Browse	• 104.22.0.232
	http://youbue.com	Get hash	malicious	Browse	• 104.20.21.239
	MuMuInstaller_1.1.0.4_a2ca17_yxmrfz_zh-Hans_1573441614.exe	Get hash	malicious	Browse	• 1.1.0.4
	Invoice2867.hTMl	Get hash	malicious	Browse	• 104.27.165.84
	http://https://www.seat26.com/wp-includes/js/tinymce/plugins/colorpicker/gastblogg/warenkorb.php?street=kqh1sdty120gb0c&face=guess&window=section	Get hash	malicious	Browse	• 104.16.132.229
	http://www.hobbyfarms.com/how-to-build-a-vermin-proof-chicken-feeder/	Get hash	malicious	Browse	• 104.18.99.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.571470151920988
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:	iceix_1.2.0.0.exe
File size:	148992
MD5:	4581c813cbc584530b75c58c30d8b29b
SHA1:	ae17112eff30ff1daacac943e5551a31f7e896a6
SHA256:	fa4bd653c43c8c9ce265eba2bd425962752b062fea81327d3cd5338b545d611e
SHA512:	7272b1cc00db4355709794fd39cc1bf281d636f12dbd4538aee1b5f15eebbb7676a9297fd1e54766348865b5f5794f2dd93d10b566422702f4c6555bbb66634f
SSDEEP:	3072:RdWhDmi+cPqVNEoUdu5oF7SYYlFcTnVFptvk5C139NobE7Lq:EiiyNN+uuIYYiVFrvk5C+4

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|..s/..s/..s/.../..s/..r/..s/.../..s/.S./..s/.S./..s/.S./..s/Rich..s/.....PE..L....!.M.....h.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40ac56
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	
Time Stamp:	0x4D8C21A2 [Fri Mar 25 05:01:22 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	449e52edf16603587b7d503b65e9b7ae

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 48h
push 00000009h
push dword ptr [004361C0h]
call dword ptr [004350A8h]
push 004361D8h
push 004361C4h
call dword ptr [004350BCh]
mov eax, dword ptr [004361C0h]
mov cx, word ptr [004361CCh]
cmp word ptr [eax+08h], cx
jne 00007F9BB0CACF0Dh
mov cl, byte ptr [004361F0h]
xor eax, eax
mov dword ptr [ebp-0Ch], eax
mov dword ptr [ebp-0Ch], eax
mov dword ptr [ebp-04h], 078718C3h
cmp cl, byte ptr [004361FAh]
jne 00007F9BB0CACEF6h
and dword ptr [ebp-14h], 00000000h
jmp 00007F9BB0CACC4Eh
mov ecx, dword ptr [ebp-14h]
inc ecx
mov dword ptr [ebp-14h], ecx
cmp dword ptr [ebp-14h], 00000018h
jnc 00007F9BB0CACCA4h
cmp dword ptr [ebp-14h], 00000025h
jne 00007F9BB0CACC7Ah

Instruction
sbb ecx, 00000C8Eh
xor ecx, 00000F2Ch
mov ecx, 00000FBDh
sub ecx, 000005CDh
push 0043A285h
push 00008B65h
push 000075BAh
push dword ptr [ebp-0Ch]
push 00006970h
call dword ptr [00435058h]
jmp 00007F9BB0CACBE7h
test dword ptr [00000000h], esi

Rich Headers

Programming Language:	• [LNK] VS2010 SP1 build 40219 • [RES] VS2010 SP1 build 40219 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3a2d1	0x66	.form4
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3f000	0x64	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x40000	0x13a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x42000	0x5a8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x365e0	0x1c	.data
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	0x35000	0x100	.itext
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	0x33e60	0x1da00	False	0.92011965981	data	7.58246971662	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.itext	0x35000	0x100	0x200	False	0.302734375	data	2.36816673441	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x36000	0x64a	0x800	False	0.6083984375	data	5.27392115406	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.form1	0x37000	0x64	0x200	False	0.142578125	data	1.04618098643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.form2	0x38000	0x140	0x200	False	0.544921875	data	3.46722474739	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.form3	0x39000	0x140	0x200	False	0.345703125	data	2.73033408951	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.form4	0x3a000	0x337	0x400	False	0.578125	data	4.09203456651	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.info	0x3b000	0x3400	0x3400	False	0.632136418269	data	6.44681786234	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.idata	0x3f000	0x55a	0x600	False	0.561197916667	data	5.00605735846	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x40000	0x2000	0x1400	False	0.048828125	data	3.92863683353	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x42000	0x5b4	0x600	False	0.830729166667	data	6.33404587159	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x40100	0x65c	data	English	United States
RT_BITMAP	0x4075c	0x376	PC bitmap, Windows 3.x format, 17 x 16 x 24	English	United States
RT_BITMAP	0x40ad4	0x356	PC bitmap, Windows 3.x format, 13 x 20 x 24	English	United States
RT_BITMAP	0x40e2c	0x576	PC bitmap, Windows 3.x format, 31 x 14 x 24	English	United States

Imports

DLL	Import
GDI32.dll	GetLayout, PolyBezier, LineDDA, SetMapMode, GetMapMode, AddFontResourceW, EndDoc, StretchDIBits, OffsetRgn, TextOutA, GetTextExtentPointA, SetWindowExtEx, SaveDC
USER32.dll	KillTimer, SetPropW, GetWindowTextA, DestroyAcceleratorTable, ToUnicodeEx, InSendMessage, GetWindow, AllowSetForegroundWindow, ModifyMenuW, GetWindowLongA, EnumThreadWindows, SetDlgItemTextA, DialogBoxParamA, OemToCharBuffA, DrawMenuBar, CharUpperW, GetClassInfoExW, SetTimer, GetMenuItemInfoW, SendMessageTimeoutW, GetWindowDC, GetMenuItemID, GetClassInfoA, SetWindowTextW, HiliteMenuItem, CharToOemA, SetCursorPos, CallWindowProcA, CharLowerBuffW
msvcrt.dll	exit
KERNEL32.dll	CreateEventA, lstrcatW, CancelWaitableTimer, FindNextFileW, LoadLibraryW, VirtualQuery, GetCurrentDirectoryW, LockResource, CreateSemaphoreA, lstrcpyA, IsValidLocale, GetCurrentProcessId, FormatMessageA, ExitProcess, SetFileTime, HeapSize, IsBadWritePtr

Exports

Name	Ordinal	Address
?_xr_kmg__p_pitn_ajs_dIY@YGM_N@Z	1	0x401b24

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: iceix_1.2.0.0.exe PID: 1396 Parent PID: 3700

General

Start time:	07:47:16
Start date:	20/07/2020
Path:	C:\Users\user\Desktop\iceix_1.2.0.0.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\iceix_1.2.0.0.exe'
Imagebase:	0x400000

File size:	148992 bytes
MD5 hash:	4581C813CBC584530B75C58C30D8B29B
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis