ID: 876178
Sample Name: IdeaShare Key.exe
Cookbook: default.jbs
Time: 13:01:46
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

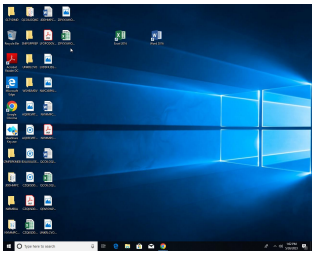
Windows Analysis Report

IdeaShare Key.exe

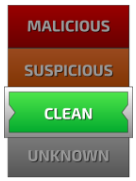
Overview

General Information

Sample Name:	IdeaShare Key.exe
Analysis ID:	876178
MD5:	e6d42ac43333…
SHA1:	ea9fc583c7bd2..
SHA256:	5faa9cd735d49..
Infos:	



Detection



Score:	9
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

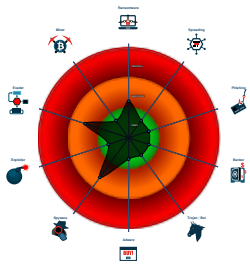
Compliance

Score:	16
Range:	0 - 100

Signatures

- Creates a DirectInput object (often f…
- EXE planting / hijacking vulnerabiliti…
- Uses 32bit PE files
- Queries the volume information (nam…
- DLL planting / hijacking vulnerabilitie…
- Sample file is different than original …
- Drops PE files
- Contains functionality to check if a d…
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function
- Contains functionality to query CPU…

Classification



Process Tree

- **System is w10x64**
- IdeaShare Key.exe (PID: 5976 cmdline: C:\Users\user\Desktop\IdeaShare Key.exe MD5: E6D42AC433331124C62460CFCCED76A1)
  - IdeaShareKeyForm.exe (PID: 5948 cmdline: C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKeyForm.exe MD5: 1A8C471F9AF78F640DC43C6C2FB533C2)
- **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

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

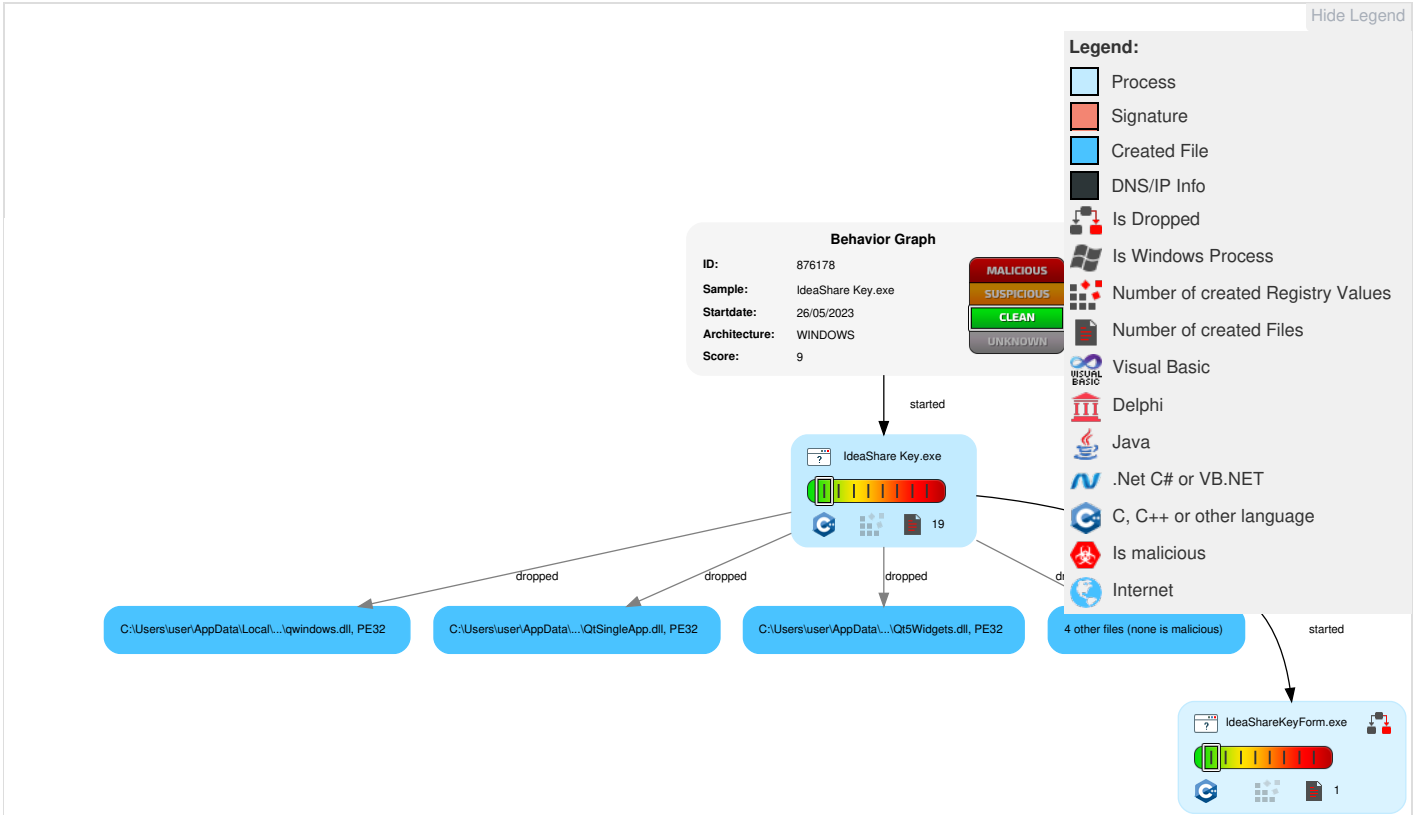
Compliance

EXE planting / hijacking vulnerabilities found
Uses 32bit PE files
DLL planting / hijacking vulnerabilities found
PE / OLE file has a valid certificate
Binary contains paths to debug symbols

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	2 DLL Search Order Hijacking	1 Process Injection	1 Masquerading	2 1 Input Capture	1 System Time Discovery	Remote Services	2 1 Input Capture	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	2 DLL Search Order Hijacking	1 Process Injection	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 System Network Configuration Discovery	SMB/Windows Admin Shares	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)	2 Obfuscated Files or Information	NTDS	2 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	2 DLL Search Order Hijacking	LSA Secrets	2 5 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

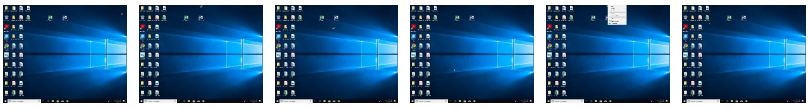
Behavior Graph



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
IdeaShare Key.exe	2%	ReversingLabs		
IdeaShare Key.exe	1%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKeyForm.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKeyForm.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Core.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Core.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Gui.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Gui.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Network.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Widgets.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\QtSingleApp.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\platforms\qwindows.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.phreedom.org/md5)	0%	URL Reputation	safe	
http://www.phreedom.org/md5)	0%	URL Reputation	safe	
http://www.phreedom.org/md5)08:27	0%	URL Reputation	safe	
http://www.color.org)	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://www.phreedom.org/md5)	IdeaShare Key.exe, 00000000.00000003.355179944.0000000002922000.00000004.00000020.00020000.00000000.sdmp, IdeaShareKeyForm.exe, 00000001.00000002.361582478.000000006BCCE000.00000002.00000001.01000000.0000000A.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://bugreports.qt.io/_q_receiveReplyMicrosoft-IIS/4.Microsoft-IIS/5.Netscape-Enterprise/3.WebLogi	IdeaShare Key.exe, 00000000.00000003.355179944.0000000002922000.00000004.00000020.00020000.00000000.sdmp, IdeaShareKeyForm.exe, 00000001.00000002.361582478.000000006BCCE000.00000002.00000001.01000000.0000000A.sdmp	false		high
http://www.phreedom.org/md5)08:27	IdeaShare Key.exe, 00000000.00000003.355179944.0000000002922000.00000004.00000020.00020000.00000000.sdmp, IdeaShareKeyForm.exe, 00000001.00000002.361582478.000000006BCCE000.00000002.00000001.01000000.0000000A.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	IdeaShare Key.exe	false		high
http://www.aiim.org/pdfa/ns/id/	IdeaShare Key.exe, 00000000.00000003.354243430.0000000002921000.00000004.00000020.00020000.00000000.sdmp, IdeaShareKeyForm.exe, 00000001.00000002.363086921.000000006C5E4000.00000002.00000001.01000000.00000008.sdmp	false		high
http://www.color.org)	IdeaShare Key.exe, 00000000.00000003.354243430.0000000002921000.00000004.00000020.00020000.00000000.sdmp, IdeaShareKeyForm.exe, 00000001.00000002.363086921.000000006C5E4000.00000002.00000001.01000000.00000008.sdmp	false	• Avira URL Cloud: safe	low
http://bugreports.qt.io/	IdeaShare Key.exe, 00000000.00000003.355179944.0000000002922000.00000004.00000020.00020000.00000000.sdmp, IdeaShareKeyForm.exe, 00000001.00000002.361582478.000000006BCCE000.00000002.00000001.01000000.0000000A.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876178
Start date and time:	2023-05-26 13:01:46 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s

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:	2
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:	IdeaShare Key.exe
Detection:	CLEAN
Classification:	clean9.winEXE@3/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 52.6%) • Quality average: 39.5% • Quality standard deviation: 42.7%
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 • Stop behavior analysis, all processes terminated

Simulations

Behavior and APIs

Time	Type	Description
13:02:40	API Interceptor	1x Sleep call for process: IdeaShareKeyForm.exe modified

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\IdeaShareKey\IdeaShareKeyForm.exe

Process:	C:\Users\user\Desktop\IdeaShare Key.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320872
Entropy (8bit):	4.939208143331431
Encrypted:	false
SSDEEP:	6144:wGXX45Tx+DPeuqD4K3FN3EiCXibivN/DHCfMiKu:HuSBMMil
MD5:	1A8C471F9AF78F640DC43C6C2FB533C2
SHA1:	8CEEC8B336A55EC150607E69F620F4EF8E009AE1
SHA-256:	284CC22997B0E20D8F30F5C7F8B2256D9756E5AFA54FE9F2C4C70485CDB4A7C3
SHA-512:	80DC736CDB80CDA2544D402627DA04E1768737D4EB682FEBBFC64B498EEAF64E110FDCF23898B08786B00A7183B1E62E460623E74BEF2D2836EFF09BADA183E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.D. .*. .*. .*.)...*.*.r.+.".*.r./.:.*.r...,*.r.).!.*.E.+.$.*./.!.*.+.&.*.+.#.*. .+..*./.%.*...!.*. ..!.*.(.!.*.Rich .*.....PE..L...d8Ca.....@.....v.....@.....].....h.....8..... .....@.....text...\..... ..`.rdata.....@..@.data...\.....@....idata..FX.....Z.....@..@.00cfg .....p.....P.....@..@.rsrc....].....^...R.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\Qt5Core.dll

Process:	C:\Users\user\Desktop\IdeaShare Key.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5298536
Entropy (8bit):	6.852481117447856
Encrypted:	false
SSDEEP:	98304:p3QkIHj14FdDhqJsv6tWKFdu9CjzHveRnZyxEdm0:pgdnJsv6tWKFdu9CjzHeb
MD5:	4BB1FC81E4B6149749B6E84EF12712D6
SHA1:	FB0143E6EA6128D7FA7B2E1731D0232D6A40689F
SHA-256:	19BE47FA14A6F1B103171FB2B9B830F631215BB522A8803795DBB72C9E8E4A8F
SHA-512:	9505ED82E68C37717C2EA4E2107ECDED41004946ABD562A03FB92F187E4855D86CF3A319FC323492865C4D0EA8A9A5110737CB662266F360FEC7993CA84C876
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....V..8].8].8]...].8]..9\.8]A".].8]..=\.8]..<\.8]..;\.8]..<\.8]..>\.8]..9\.8].9]..8]E.<\.8]E.=\$.8]E.8\.8]E..].8]..].8]E.:\.8]Rich.8].....PE..L...2.}^.....!.....'..").....%.....(....g.....PQ.....dQ...@.....G.@...0.N.....O.....P.h..... O.....PE.T.....QE.....QE.@.....(.X.....text....'.....'..... ..`.rdata....&...(...&...'.....@..@.data...|....O..J....N.....@....rsrc..... O.....8O.....@..@.reloc.....O.....>O.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\Qt5Gui.dll

Process:	C:\Users\user\Desktop\IdeaShare Key.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5978984
Entropy (8bit):	6.780270903027489
Encrypted:	false
SSDEEP:	98304:f8oNJzx4w24LwWotu+PNlwL9PmEZ23Cex:pBbUuCPwNj2C0
MD5:	D8B7393009A6743FFCFB9D3A138FC114
SHA1:	5467D025F650D80949393DAF58601B47D41A25FA
SHA-256:	48846110574CFA870918E08471A180981D934DB1AAA92B4832CC567D0630A28E
SHA-512:	1AE4580ECEE6E992501C963B9406A2A0A927CA48AB0A3E7B8FDC247EC21AA74EDA9818224D72C3088893418FE8E5044E857B347D056B77DC5D4F73F5BF0EACDA
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....?.f.{...{...{...r...m...)...q...)...w...)...c...).....y... ...z... ...v...{...<.....k. .....z.....z...{..z.....z...Rich{.....PE..L.....}^.....!.....''7..d$.....b.7.....@7.....[.....[...@.....n=.....V.h....Y.....$[.h....Y.....<.T.....<.....8.<.@.....@7.....text.... 7.....''7..... ..`.rdata...O ..@7..P ..&7.....@..@.data....c....W.....vW.....@....rsrc..... Y.....tX.....@..@.reloc.....Y.....zX.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\Qt5Network.dll

Process:	C:\Users\user\Desktop\IdeaShare Key.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1115496
Entropy (8bit):	6.66916261306281
Encrypted:	false
SSDEEP:	24576:ZNfY4/b8d22Gmou3ZjRkjZgUPiV69DrOMxpqDc0EGQVzKa4:xAd22GrziVaSDckZ
MD5:	80D7021426B78E3E7527265841FC22A7
SHA1:	2E81B7E0F3D717F80284E3A43038997D66616042
SHA-256:	169BE38BE0BC90018DFF8EF05FE004DD04A6D0B3ABE294FC67B42466E5F2E6DD
SHA-512:	A2AF4D9ACE035C51E5CF846DB3955895422E65AE6A6D7D523493AC3AE6BC28ABA87A272BB50B16FC5FFF438723A911E31DED0EEFBDB4EFF7416D7C5E121C64CA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....U.}...}...}....E..}.....}.....}.....}.....}.....}.....}..+....}...}..M~..+... 7}..+....}..+.)..}...}A..}..+....}..Rich.}.....PE..L.....}^.....!.....>.....d.....@.....s%....@.....Ta...=..@....0.....h....@ ..|.....T.....H...@.....text...?..... ..`.rdata.....@..@.data....9.....@....rsrc.....0..... @..@.reloc..|....@.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\Qt5Widgets.dll

Process:	C:\Users\user\Desktop\IdeaShare Key.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4596072
Entropy (8bit):	6.819919859208047
Encrypted:	false
SSDEEP:	98304:O1CmFlF05UMNO1ulAjhDfTbz7quDp+bXa6gYzdkSPD1UZlH6uV75uDdHBclxooG0:Yf59iJ5i
MD5:	2EBDB8799EB13D879A57CC20894EFDFF
SHA1:	8D54AC978DBBCA41742DADFD29DE360EC7E60450
SHA-256:	0CC9C3B945B35EFAB0DBB5706ED285B0C5233E6D36B2261AAA2FB7BFCBA0CD4E
SHA-512:	E580DBFF9CA35A1DDCFD879C35229212732D4E912D0F47430DB7F7C0166FBDDA895170ADF89F4EA2D81F393A71BDB4681E812B8F7B3636C7C8A3357927AEF39
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....l|.....eK.....u....._u....._u....._u.....Vu.....Vu.....t..... .;...t....t.....t'.....O.....t.....Rich.....PE..L...;.}^.....!....&,.....',.....@,...e.....PF.....G...@.....0.7..#..4.?.@.....B.....F.h. ....B..z....6.T.....6.....6.@.....@,..4.....text....$,.....&,..... ..`.rdata..d....@,.....*,.....@..@.data.....@B..h... B.....@....rsrc..... ....B.....B.....@..@.reloc...z....B..|....B.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\QtSingleApp.dll

Process:	C:\Users\user\Desktop\IdeaShare Key.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	6.1073547240575285
Encrypted:	false
SSDEEP:	768:RJiXhlJ0/q2aqiquV3aHaxGtpA510VxjqjCij9yKqTws:RJivOC9FxG4rsxjq3j9yKqss
MD5:	ABA7C077EFE89A0006FCD643A2C5EC62
SHA1:	531EB0A0941A19159921909BFE20FA47F34C0457

SHA-256:	B214C4FD356E0699900C40EBE22A757E6C6334E8C96F72791ACD27545FFC45A8
SHA-512:	1280CCF34D6B31CAAC2D5F5EAEEDB45E8D8F364E378EC79CCF63072CC40D5ADBB38016D934C8A193606FA6D00F7A7CC4C844DE4E94B06203DA6F954A19076 39
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.f.T.f.T.f.]...P.f...g.V.f...c.F.f...b.^.f...e.U.f.@.g.V.f...g.S.f.T.g..f...c .W.f...f.U.f....U.f...d.U.f.RichT.f.....PE..L.....O`.....!.....D...N.....?.....`.....@.....w.....|.....0....j..T..... .....hj..@.....`.....text....C.....D..... ..`.rdata...:...`...<...H.....@..@.data...|.....@....rsrc.....@..@.reloc..0. .....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\log\insit.log

Process:	C:\Users\user\Desktop\IdeaShare Key.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.065774219659049
Encrypted:	false
SSDEEP:	3:QvWizYQPc2XIvfYQPctTXvA:6WiRXSsTXvA
MD5:	8E2CD044125E0C173B3AAC9D12C190BB
SHA1:	1DD4E9AF27BC8DE55E1E537AFD3DEAAF4A118163
SHA-256:	CF663FEEB3397611B70272AD2D6969D1464D2E3437F371254144F6EF850FCECB
SHA-512:	F94D23D1766DD7BCBC4F55F081A717597FC607F938DF59B37A84DCB5C639871953A7B7200E8A6B2B1C14C6D85B5E08AD9A203A59731B073E25B5D3457659312
Malicious:	false
Reputation:	low
Preview:	copy dll.start IdeaShareKeyForm.start IdeaShareKeyInstaller.end.

C:\Users\user\AppData\Local\IdeaShareKey\platforms\qwindows.dll

Process:	C:\Users\user\Desktop\IdeaShare Key.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1221992
Entropy (8bit):	6.832955399743319
Encrypted:	false
SSDEEP:	12288:1YCQWyni5LoUmhY4or3D8kSqjPfmK7UpOVpYAlCRegIe5ZpzNAoKu15XSxDyfEWu:SniF3z39xPePpOkaXze5ZtN4bZa0n
MD5:	2F98DC4484F115FE227246844464CD04
SHA1:	0A49DA60F63FB476B2A3CAED2A5B7BA686A7D2FA
SHA-256:	31BF06D063B23A0AD606354D7D77416AF5713CE877F6A7E7BC658DD09DB02BB2
SHA-512:	32D64143CEE92FE6CAB366493DDFFB034EA71DF2B7CE584238DEB56E54886083676A50C6FBF28E871F926081E8C8AFD72B7FEB8EF24C50E16A4C034939D5433 E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....8..k..k..k..Ak...k...j...k...j..k...j..k...j..k...j..k...j..kN..j..kN..j..k...j. ..k..kg..kN..j...kN..j..kN.-k..kN..j..kRich..k.....PE..L.....}^.....!.....\...j.....[.....p.....@.....w..x...(x..... ..H.....h....0..<.... 9..T.....:.....H:..@.....p.....text....Z.....\..... ..`.rdata...?...p...@...`.....@..@.data....X.....@....qtmetad..... .....@..P.rsrc...H.... .....@..@.reloc..<....0.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.999391627012608
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:	IdeaShare Key.exe
File size:	6338072

MD5:	e6d42ac433331124c62460cfcced76a1
SHA1:	ea9fc583c7bd2054a8d51e61d6b1cbeee800d344
SHA256:	5faa9cd735d499eb4fbcb08a252d53020629a7418c9b6c30b00c5d2d7cc7fe25
SHA512:	cfad934f060f13b9e44934a793b1d73d4e3fbcd265050bce69481f1328bc8bc170b24ae826288b0f0b708a1bf5a4ba4df36ab7988c4a0ac96e18388ecdc9d2a8
SSDEEP:	196608:8y7Weg+i1XWsTrXmiq8mC7h0YPvw8qGqhXvmhwupR+:xk/9WC05CN0YZqFhXeeY
TLSH:	0256338092EC8466FF8A057066F075A195FEBD6D0663EB0D72368905FD2A3F45F68F04
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mu]..&]..&]..&..\&_..&..^&J..&]..&...&z\n&P..&z\.&\..&z\ {&\..&Rich]..&.....PE..L...,..R.....x.

File Icon

Icon Hash:	181b214161331b18

Static PE Info

General

Entrypoint:	0x4038a8
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x52AFF32C [Tue Dec 17 06:46:04 2013 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:	a73b2531bfc838dc3d19df5285b8d0fd

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=GlobalSign GCC R45 CodeSigning CA 2020, O=GlobalSign nv-sa, C=BE
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 6/2/2021 12:37:54 AM 6/3/2022 12:37:54 AM
Subject Chain	• CN=\u8f6f\u901a\u52a8\u529b\u4fe1\u606f\u6280\u672f\uff08\u96c6\u56e2\uff09\u80a1\u4efd\u6709\u9650\u516c\u53f8, O=\u8f6f\u901a\u52a8\u529b\u4fe1\u606f\u6280\u672f\uff08\u96c6\u56e2\uff09\u80a1\u4efd\u6709\u9650\u516c\u53f8, L=\u5317\u4eac\u5e02, S=\u5317\u4eac\u5e02, C=CN
Version:	3
Thumbprint MD5:	302F9D7469F8C3413FEEC8D8C9B808F8
Thumbprint SHA-1:	C2455B5BB7938677784BFE593CCE0E218E2AB68D
Thumbprint SHA-256:	F44AEB9493563C34D85C329C38D892C77DCC768C831AF7FB48DE773837E32AB6
Serial:	249A5D0D48B5FBE5F0138D14

Entrypoint Preview

Instruction
sub esp, 000002D8h
push ebx
push ebp
push esi
push edi
push 00000020h
xor ebx, ebx
pop esi

Instruction
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A2D0h
mov dword ptr [esp+14h], ebx
call dword ptr [00409090h]
mov dword ptr [esp+1Ch], eax
call dword ptr [00409034h]
push 00008001h
call dword ptr [004090B4h]
push ebx
call dword ptr [00409330h]
push 00000008h
mov dword ptr [00473EB8h], eax
call 00007F52B8CFD530h
push ebx
push 000002B4h
mov dword ptr [00473DD0h], eax
lea eax, dword ptr [esp+3Ch]
push eax
push ebx
push 0040A2CCh
call dword ptr [004091A4h]
push 0040A2B4h
push 0046BDC0h
call 00007F52B8CFD212h
call dword ptr [004090B0h]
push eax
mov edi, 004C40A0h
push edi
call 00007F52B8CFD200h
push ebx
call dword ptr [00409158h]
cmp word ptr [004C40A0h], 0022h
mov dword ptr [00473DD8h], eax
mov eax, edi
jne 00007F52B8CFAB0Ah
push 00000022h
pop esi
mov eax, 004C40A2h
push esi
push eax
call 00007F52B8CFCED8h
push eax
call dword ptr [00409270h]
mov esi, eax
mov dword ptr [esp+20h], esi
jmp 00007F52B8CFAB91h
push 00000020h
pop ebp
cmp ax, word ptr [eax]

Rich Headers

Programming Language:	• [C] VS2005 build 50727 • [RES] VS2005 build 50727 • [LNK] VS2005 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xada4	0xf0	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf9000	0x38f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x607050	0x45c8	
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	0x9000	0x338	.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	0x7788	0x7800	False	0.6550455729166667	data	6.509642546823201	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x2f64	0x3000	False	0.3724772135416667	data	4.571600211578863	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0x67ebc	0x200	False	0.21875	data	1.5987280494305565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x74000	0x85000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xf9000	0x38f8	0x3a00	False	0.8774245689655172	data	7.598885730468926	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf91d8	0x2fa3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_DIALOG	0xfc180	0x100	data	English	United States
RT_DIALOG	0xfc280	0x11c	data	English	United States
RT_DIALOG	0xfc3a0	0x60	data	English	United States
RT_GROUP_ICON	0xfc400	0x14	data	English	United States
RT_VERSION	0xfc418	0x1fc	data		
RT_MANIFEST	0xfc618	0x2dd	XML 1.0 document, ASCII text, with very long lines (733), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileTime, CompareFileTime, SearchPathW, GetShortPathNameW, GetFullPathNameW, MoveFileW, SetCurrentDirectoryW, GetFileAttributesW, GetLastError, CreateDirectoryW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, ExitProcess, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, SetErrorMode, lstrcpynA, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, GlobalUnlock, CloseHandle, CreateThread, LoadLibraryW, CreateProcessW, lstrcmpiA, CreateFileW, GetTempFileNameW, lstrcatW, GetProcAddress, LoadLibraryA, GetModuleHandleA, OpenProcess, lstrcpyW, GetVersionExW, GetSystemDirectoryW, GetVersion, lstrcpyA, RemoveDirectoryW, lstrcmpA, GlobalHandle, GlobalReAlloc, GetSystemDefaultLCID, GetVolumeInformationA, QueryPerformanceFrequency, GlobalMemoryStatusEx, GetSystemInfo, GetModuleFileNameA, lstrcatA, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GlobalFree, GetModuleHandleW, LoadLibraryExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, WideCharToMultiByte, lstrlenA, WriteFile, ReadFile, MultiByteToWideChar, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW, GlobalLock, MulDiv

DLL	Import
USER32.dll	GetMessagePos, CallWindowProcW, IsWindowVisible, LoadBitmapW, CloseClipboard, SetClipboardData, EmptyClipboard, OpenClipboard, TrackPopupMenu, GetWindowRect, AppendMenuW, CreatePopupMenu, GetSystemMetrics, EndDialog, EnableMenuItem, GetSystemMenu, SetClassLongW, IsWindowEnabled, SetWindowPos, DialogBoxParamW, GetClassInfoW, CreateWindowExW, SystemParametersInfoW, RegisterClassW, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharNextA, CharUpperW, CharPrevW, wvsprintfW, DispatchMessageW, PeekMessageW, wsprintfA, ScreenToClient, IsDlgButtonChecked, GetAsyncKeyState, CheckDlgButton, LoadCursorW, SetCursor, GetWindowLongW, GetSysColor, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, LoadImageW, GetDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, EndPaint, SetWindowLongW
GDI32.dll	CreateBrushIndirect, DeleteObject, GetDeviceCaps, SetBkColor, SelectObject, CreateFontIndirectW, SetBkMode, SetTextColor
SHELL32.dll	SHFileOperationW, SHGetFileInfoW, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetSpecialFolderLocation, ShellExecuteW
ADVAPI32.dll	RegQueryValueExW, RegCreateKeyExW, RegSetValueExW, RegEnumValueW, RegDeleteKeyW, RegCloseKey, RegEnumKeyW, RegOpenKeyExW, RegDeleteValueW
COMCTL32.dll	ImageList_Destroy, ImageList_AddMasked, ImageList_Create
ole32.dll	OleUninitialize, CoCreateInstance, CoTaskMemFree, OleInitialize
VERSION.dll	GetFileVersionInfoSizeW, GetFileVersionInfoSizeA, VerQueryValueW, GetFileVersionInfoW, VerQueryValueA, GetFileVersionInfoA
WININET.dll	InternetReadFile, InternetConnectA, InternetOpenA, InternetCloseHandle, HttpOpenRequestA, HttpQueryInfoA, HttpSendRequestA, InternetSetOptionA
SHLWAPI.dll	PathFindFileNameA, StrStrIA
iphlpapi.dll	GetAdaptersInfo

Possible Origin

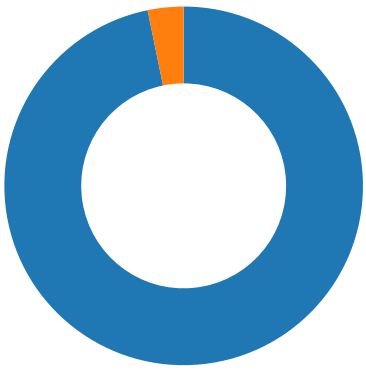
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: IdeaShare Key.exe PID: **5976**, Parent PID: **3452**

General

Target ID:	0
Start time:	13:02:36
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\IdeaShare Key.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\IdeaShare Key.exe
Imagebase:	0x400000
File size:	6338072 bytes
MD5 hash:	E6D42AC433331124C62460CFCCED76A1
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	40381A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsk3518.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405EE5	GetTempFileNameW
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	3	4017ED	CreateDirectoryW
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	3	4017ED	CreateDirectoryW
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	3	4017ED	CreateDirectoryW
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	3	4017ED	CreateDirectoryW
C:\Users\user\AppData\Local\IdeaShareKey	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4017ED	CreateDirectoryW
C:\Users\user\AppData\Local\IdeaShareKey\log	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4017ED	CreateDirectoryW
C:\Users\user\AppData\Local\IdeaShareKey\log\insit.log	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA3	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	4017ED	CreateDirectoryW
C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKeyForm.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA3	CreateFileW
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Core.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA3	CreateFileW
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Gui.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA3	CreateFileW
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Network.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA3	CreateFileW
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Widgets.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA3	CreateFileW
C:\Users\user\AppData\Local\IdeaShareKey\QtSingleApp.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA3	CreateFileW
C:\Users\user\AppData\Local\IdeaShareKey\platforms	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4017ED	CreateDirectoryW
C:\Users\user\AppData\Local\IdeaShareKey\platforms\qwindows.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EA3	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsk3518.tmp	success or wait	1	403A6B	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\log\insit.log	0	8	63 6f 70 79 20 64 6c 6c	copy dll	success or wait	8	402BA3	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKeyForm.exe	0	32768	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 18 01 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 64 fd 44 fd 20 fd 2a fd 20 fd 2a fd 20 fd 2a fd 29 fd fd fd 2a fd 2a fd 72 fd 2b fd 22 fd 2a fd 72 fd 2f fd 3a fd 2a fd 72 fd 2e fd 2c fd 2a fd 72 fd 29 fd 21 fd 2a fd 45 fd 2b fd 24 fd 2a a1 2f fd 21 fd 2a a1 2b fd 26 fd 2a 61 2b fd 23 fd 2a fd 20 fd 2b fd fd 2a 61 2f fd 25 fd 2a 61 fd fd 21 fd 2a fd 20 3d fd 21 fd 2a 61 28 fd 21 fd 2a	MZ@!L!This program cannot be run in DOS mode.$dD * * *)**r+" *r/:*r.,*r)!*E+$*/!*+&*+#* +*/%*!* !*(!*	success or wait	13	403500	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Core.dll	0	32768	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 20 01 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 fd 56 0e c2 38 5d c2 38 5d c2 38 5d fd fd fd 5d c2 38 5d fd fd 39 5c c2 38 5d 41 22 fd 5d c2 38 5d fd fd 3d 5c c2 38 5d fd fd 3c 5c 42 38 5d fd fd 3b 5c 82 38 5d fd fd 3c 5c 42 38 5d fd fd 3e 5c 82 38 5d fd fd 39 5c 02 38 5d c2 39 5d fd fd 38 5d 45 fd 3c 5c fd 38 5d 45 fd 3d 5c 24 fd 38 5d 45 fd 38 5c 82 38 5d 45 fd fd 5d 82 38	MZ@ !L!This program cannot be run in DOS mode.$V8]8]8]]8]9\8]A"]8]=\8]<\8];\8] <\8]>\8]9\8] 9]8]E<\8]E=\$8]E8\8]E]8	success or wait	229	403500	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Gui.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 3f fd 66 fd 7b fd 08 fd 7b fd 08 fd 7b fd 08 fd 72 fd fd fd 6d fd 08 fd 29 fd 0c fd 71 fd 08 fd 29 fd 0b fd 77 fd 08 fd 29 fd 0d fd 63 fd 08 fd 29 fd 09 fd 7f fd 08 fd fd 09 fd 79 fd 08 fd 20 fd 0d fd 7a fd 08 fd 20 fd 09 fd 76 fd 08 fd 7b fd 09 fd 3c fd 08 fd fd 0c fd 6b fd 08 fd fd 0d fd 12 fd 08 fd fd 08 fd 7a fd 08 fd fd fd fd 7a fd 08 fd 7b 5f fd 7a fd 08	MZ@(!L!This program cannot be run in DOS mode.$?f{{{rm)q)w)c)y z v{<kzz{z	success or wait	244	403500	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Network.dll	0	32768	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 20 01 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 1c fd 55 fd 7d fd 06 fd 7d fd 06 fd 7d fd 06 fd 05 45 06 fd 7d fd 06 fd 15 fd 07 fd 7d fd 06 fd 15 fd 07 fd 7d fd 06 fd 15 fd 07 fd 7d fd 06 fd 15 fd 07 fd 7d fd 06 fd 15 fd 07 fd 7d fd 06 15 fd 07 fd 7d fd 06 2b 14 fd 07 fd 7d fd 06 fd 7d fd 06 4d 7e fd 06 2b 14 fd 07 37 7d fd 06 2b 14 fd 07 fd 7d fd 06 2b 14 29 06 fd 7d fd 06 fd 7d 41 06 fd 7d fd 06 2b 14 fd 07 fd 7d fd	MZ@ !L!This program cannot be run in DOS mode.$U}}}E}}}}}}}+ }}M~+7}+}+)}}A}+}	success or wait	48	403500	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Widgets.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 49 7c fd fd 0d 1d fd fd 0d 1d fd fd 0d 1d fd fd 04 65 4b fd 05 1d fd fd 5f 75 fd fd 07 1d fd fd 5f 75 fd fd 04 1d fd fd 5f 75 fd fd 15 1d fd fd 5f 75 fd fd 09 1d fd fd 56 75 fd fd 0c 1d fd fd 56 75 fd fd 03 1d fd fd 74 fd fd 08 1d fd fd 0d 1d fd fd 3b 10 fd fd 74 fd fd 1d fd fd 74 fd fd 0c 1d fd fd 74 27 fd 0c 1d fd fd 0d 1d 4f fd 0c 1d fd fd 74 fd fd 0c 1d fd	MZ@ !L!This program cannot be run in DOS mode.$I|eK_u_u_u_uVuVut;ttt'Ot	success or wait	193	403500	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\QtSingleApp.dll	0	32768	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 08 01 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 10 fd 08 fd 54 fd 66 fd 54 fd 66 fd 54 fd 66 fd 5d fd fd fd 50 fd 66 fd 06 fd 67 fd 56 fd 66 fd 06 fd 63 fd 46 fd 66 fd 06 fd 62 fd 5e fd 66 fd 06 fd 65 fd 55 fd 66 fd 40 fd 67 fd 56 fd 66 fd fd fd 67 fd 53 fd 66 fd 54 fd 67 fd fd 66 fd fd fd 63 fd 57 fd 66 fd fd fd 66 fd 55 fd 66 fd fd 99 fd 55 fd 66 fd fd fd 64 fd 55 fd 66 fd 52 69 63 68 54 fd 66 fd 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$TfTfTf]PfgVfcF fb^feUf@gVfgSfTgcWffU fUfdUfRichTf	success or wait	2	403500	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\platforms\qwindows.dll	0	32768	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 20 01 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 7c 38 34 fd 6b 34 fd 6b 34 fd 6b fd fd 41 6b fd fd fd 6b fd fd fd 6a fd fd fd 6b fd fd fd 6a b4 fd 6b fd fd fd 6a 34 fd 6b fd fd fd 6a 34 fd 6b fd fd fd 6a f4 fd 6b fd fd fd 6a 74 fd 6b 4e fd fd 6a 34 fd 6b 4e fd fd 6a fd fd 6b fd fd fd 6a fd fd fd 6b 34 fd 6b 67 fd fd 6b 4e fd fd 6a fd fd fd 6b 4e fd fd 6a 74 fd 6b 4e fd 2d 6b 74 fd	MZ@ !L!This program cannot be run in DOS mode.$8kkkAkkjkjkjk jkjkjkNjkNjkjkkgkNjkNjkN-k	success or wait	58	403500	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\IdeaShare Key.exe	unknown	512	success or wait	309	40337A	ReadFile
C:\Users\user\Desktop\IdeaShare Key.exe	unknown	4	success or wait	1	40337A	ReadFile
C:\Users\user\Desktop\IdeaShare Key.exe	unknown	4	success or wait	7	40337A	ReadFile

Analysis Process: IdeaShareKeyForm.exe PID: **5948**, Parent PID: **5976**

General

Target ID:	1
Start time:	13:02:40
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKeyForm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKeyForm.exe
Imagebase:	0x11c0000

File size:	320872 bytes
MD5 hash:	1A8C471F9AF78F640DC43C6C2FB533C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs • Detection: 0%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\qtsingleapp-ideash-193a-1-lockfile	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6BE86F31	CreateFileW

Disassembly

No disassembly