ID: 876179
Sample Name:
IdeaShareKeyInstaller.exe
Cookbook: default.jbs
Time: 13:03:23
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

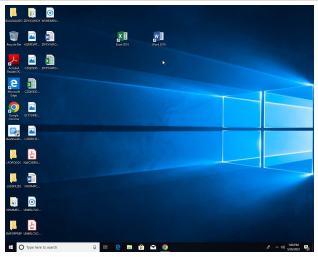
Windows Analysis Report

IdeaShareKeyInstaller.exe

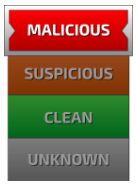
Overview

General Information

Sample Name:	IdeaShareKeyInstaller.exe
Analysis ID:	876179
MD5:	c7dfff14e88761..
SHA1:	5dc3cbf93f798...
SHA256:	d08117db56fe4..
Infos:	



Detection



Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

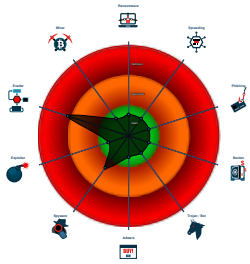
Compliance

Score:	16
Range:	0 - 100

Signatures

- DLL side loading technique detected
- Uses schtasks.exe or at.exe to add...
- Uses 32bit PE files
- Contains functionality to check if a d...
- Uses code obfuscation techniques (...
- PE file contains sections with non-s...
- Queries device information via Setu...
- Contains functionality to query CPU...
- Sample execution stops while proce...
- Contains functionality to communica...
- Contains functionality to check if a w...
- Contains functionality to dynamicall...
- Found dropped PE file which has no...

Classification



Process Tree

- **System is w10x64**
- IdeaShareKeyInstaller.exe (PID: 6132 cmdline: C:\Users\user\Desktop\IdeaShareKeyInstaller.exe MD5: C7DFFF14E887613A25CEC2E1EE87F5A9)
  - taskkill.exe (PID: 1836 cmdline: "taskkill" /F /T /IM FaultReport.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - conhost.exe (PID: 912 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - taskkill.exe (PID: 6900 cmdline: "taskkill" /F /T /IM IdeaShareKey.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - conhost.exe (PID: 6904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - taskkill.exe (PID: 5976 cmdline: taskkill" /F /IM IdeaShareService.exe /FI "STATUS eq running MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - conhost.exe (PID: 1768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - taskkill.exe (PID: 5788 cmdline: "taskkill" /F /T /IM FaultReport.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - conhost.exe (PID: 4404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - taskkill.exe (PID: 1844 cmdline: "taskkill" /F /T /IM IdeaShareKey.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
    - conhost.exe (PID: 5816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - IdeaShareService.exe (PID: 5840 cmdline: C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe MD5: 4C43F81A16703A0539A95CCCB064585F)
  - schtasks.exe (PID: 5528 cmdline: schtasks /delete /tn /f MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6912 cmdline: schtasks /create /xml C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.xml /tn IdeaShareServiceAt20230526130440 MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - IdeaShareService.exe (PID: 1836 cmdline: C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe C:\Windows\system32\config\systemprofile\AppData\Local\IdeaShareKey\IdeaShareService.exe MD5: 4C43F81A16703A0539A95CCCB064585F)
  - dllhost.exe (PID: 5788 cmdline: C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} MD5: 2528137C6745C4EADD87817A1909677E)
- IdeaShareService.exe (PID: 2348 cmdline: "C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service MD5: 4C43F81A16703A0539A95CCCB064585F)
- IdeaShareService.exe (PID: 3968 cmdline: "C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service MD5: 4C43F81A16703A0539A95CCCB064585F)
- IdeaShareService.exe (PID: 5744 cmdline: "C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service MD5: 4C43F81A16703A0539A95CCCB064585F)
- IdeaShareService.exe (PID: 2488 cmdline: "C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service MD5: 4C43F81A16703A0539A95CCCB064585F)
- **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

Compliance

Uses 32bit PE files

EXE planting / hijacking vulnerabilities found

DLL planting / hijacking vulnerabilities found

PE / OLE file has a valid certificate

Binary contains paths to debug symbols

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

HIPS / PFW / Operating System Protection Evasion

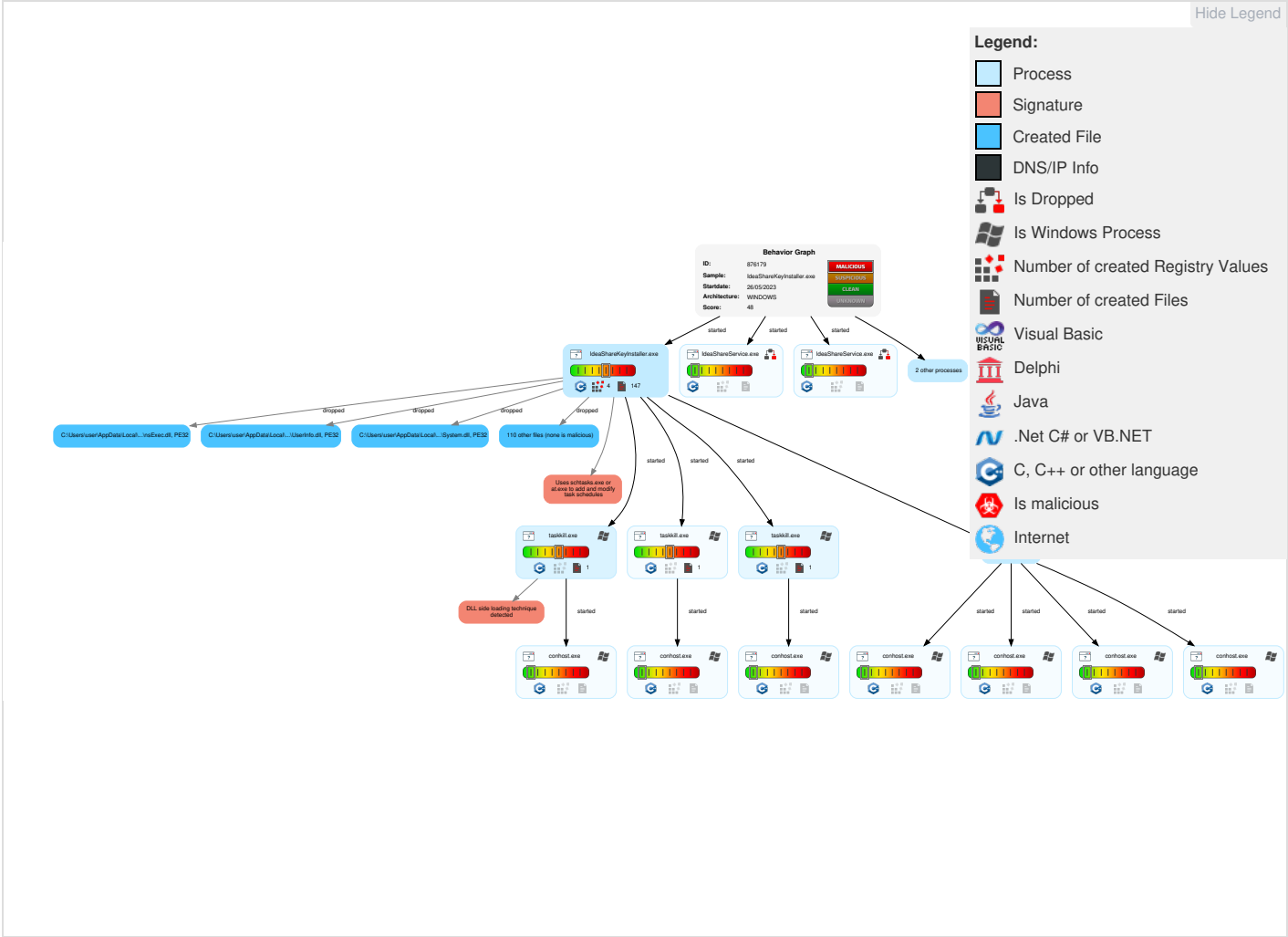
DLL side loading technique detected

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 Windows Management Instrumentation	1 Scheduled Task/Job	1 2 Process Injection	1 Masquerading	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Native API	1 DLL Side-Loading	1 Registry Run Keys / Startup Folder	1 2 Process Injection	Security Account Manager	1 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	2 DLL Search Order Hijacking	1 DLL Side-Loading	2 Obfuscated Files or Information	NTDS	3 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	2 DLL Search Order Hijacking	1 Software Packing	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Timestomp	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	2 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 DLL Search Order Hijacking	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

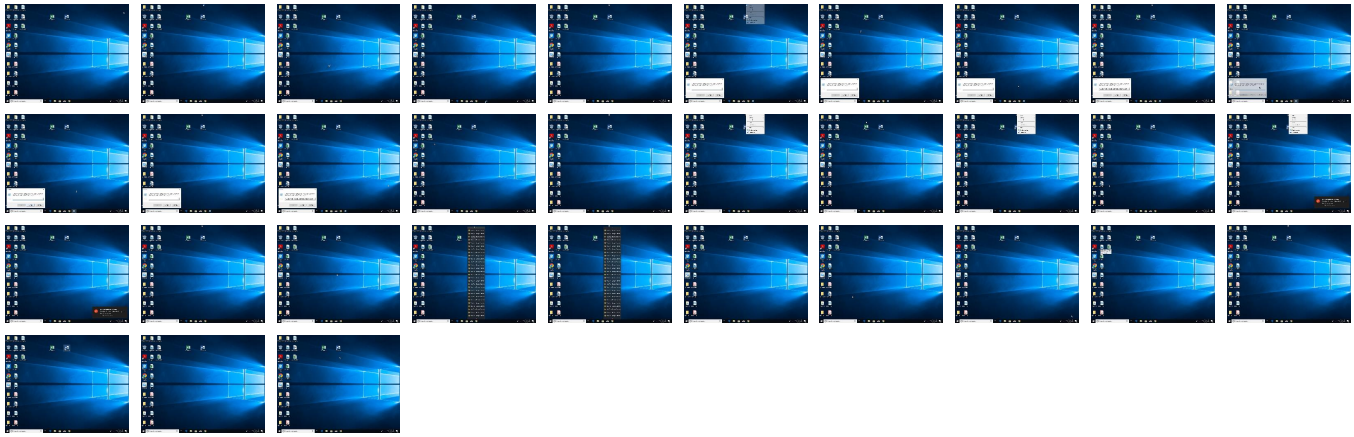
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\IdeaShareKey\FaultReport.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKey.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Core.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\Qt5Gui.dll	0%	ReversingLabs		
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\api-ms-win-core-debug-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-errorhandling-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-file-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-handle-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-interlocked-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-io-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-libraryloader-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-localization-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-localization-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-localregistry-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-memory-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-misc-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-processenvironment-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-processthreads-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-processthreads-l1-1-1.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-profile-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-rtlsupport-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-string-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-synch-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-synch-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-sysinfo-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-timezone-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-util-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-conio-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-convert-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-environment-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-filesystem-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-locale-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-math-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-multibyte-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-private-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-process-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-runtime-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-stdio-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-string-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-time-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-utility-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-downlevel-kernel32-l2-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-eventing-provider-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-security-base-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\concrt140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\dbgcore.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\IdeaShareKey\dbghelp.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\libipsi_crypto.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\libipsi_osal.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\libipsi_pse.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\libipsi_ssl.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\mfc110.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\mfc110u.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\mfc140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\mfc140u.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\mfcm140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\mfcm140u.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\msvcp110.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\msvcp140.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\msvcr100.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\msvcr110.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\platforms\qwindows.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\tup_exception.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\tup_login.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\tup_rtp.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\IdeaShareKey\ucrtbase.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)08:27	0%	URL Reputation	safe	
http://https://%s/Ws/SmcExternal2.asmx	0%	Avira URL Cloud	safe	
http://www.color.org)	0%	Avira URL Cloud	safe	
http://https://%s/getClientParam.action?client=%s®iste=%u	0%	Avira URL Cloud	safe	
http://%s/Ws/SmcExternal2.asmx	0%	Avira URL Cloud	safe	
http://https://%u.%u.%u.%u:%u%s	0%	Avira URL Cloud	safe	
http://https://curCA.zipcurCA.tgz/newCA.tgz:8544/eua/rest/cert/downloadstup_http_download_file	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)	IdeaShareKeyInstaller.exe, 00000000.00000003.363946159.00000000028D3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://bugreports.qt.io/_q_receiveReplyMicrosoft-IIS/4.Microsoft-IIS/5.Netscape-Enterprise/3.WebLogi	IdeaShareKeyInstaller.exe, 00000000.00000003.363946159.00000000028D3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.phreedom.org/md5)08:27	IdeaShareKeyInstaller.exe, 00000000.00000003.363946159.00000000028D3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.aiim.org/pdfa/ns/id/	IdeaShareKeyInstaller.exe, 00000000.00000003.362279958.0000000028D0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.openssl.org/H	IdeaShareKeyInstaller.exe, 00000000.00000003.400345936.00000000030F6000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://%s/getClientParam.action?client=%s®iste=%u	IdeaShareKeyInstaller.exe, 00000000.00000003.404028040.00000000030F2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://%s/Ws/SmcExternal2.asmx	IdeaShareKeyInstaller.exe, 00000000.00000003.404028040.00000000030F2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://nsis.sf.net/NSIS_ErrorError	IdeaShareKeyInstaller.exe, 00000000.00000003.406551623.00000000030F1000.00000004.00000020.00020000.00000000.sdmp, IdeaShareKeyInstaller.exe, 00000000.00000003.355313023.0000000000409000.00000002.00000001.01000000.00000003.sdmp, IdeaShareKeyInstaller.exe, 00000000.00000002.412809253.0000000000409000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://%s/Ws/SmcExternal2.asmx	IdeaShareKeyInstaller.exe, 00000000.00000003.404028040.00000000030F2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://%u.%u.%u.%u:%u%s	IdeaShareKeyInstaller.exe, 00000000.00000003.404028040.00000000030F2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.color.org)	IdeaShareKeyInstaller.exe, 00000000.00000003.362279958.0000000028D0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://bugreports.qt.io/	IdeaShareKeyInstaller.exe, 00000000.00000003.363946159.0000000028D3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://curCA.zipcurCA.tgz/newCA.tgz:8544/eua/rest/cert/downloadstup_http_download_file	IdeaShareKeyInstaller.exe, 00000000.00000003.397323334.00000000030FB000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://curl.haxx.se/docs/http-cookies.html	IdeaShareKeyInstaller.exe, 00000000.00000003.403541817.00000000030FC000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876179
Start date and time:	2023-05-26 13:03:23 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 35s
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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	IdeaShareKeyInstaller.exe

Detection:	MAL
Classification:	mal48.evad.winEXE@30/122@0/0
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 77.6%) • Quality average: 56.6% • Quality standard deviation: 37.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, audiodg.exe, consent.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Execution Graph export aborted for target IdeaShareKeyInstaller.exe, PID 6132 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:04:40	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run IdeaShareKey "C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service
13:04:42	Task Scheduler	Run new task: IdeaShareServiceAt20230526130440 path: %LOCALAPPDATA%\IdeaShareKey\IdeaShareService.exe
13:04:49	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run IdeaShareKey "C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service
13:04:50	API Interceptor	1x Sleep call for process: dllhost.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\ACE.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1306192
Entropy (8bit):	6.665518931955342
Encrypted:	false
SSDEEP:	24576:V+HuCXLBjKQSzYfoWHob6+/F4NrrXgUfuEPO:cHXcZbOlrXgUfzO
MD5:	1C10E6567A3157549AE19CD6067FDCD6
SHA1:	2DF2FB74221B55540E169BDC8135D3A99D9321FD
SHA-256:	CE797AECFAB749DA3E20A34AA4BA599956BD12FA642F22D461580CC97D7ECE46
SHA-512:	624DBDD3821558DBF4A6026767C12122A5D55C317BAE9A9DD5496D09CBE2CD635E98418DF6231023F06AADDEC48267CC09969425D5CB1E792E486BDF048928 4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:#..~B..~B..~B..w:..jB..,*..wB..,*..rB..,*..eB..,*..xB...$..oB..~B...C.. .+..IC...+...B...+k..B..~B...B...+...B..Rich~B.....PE..L.....]..... !.....k`.....@.....P0... .... .....p.....@...@.....text..... ..`.rdata..6.....@..@.data....L.....>.....@....rsrc.....@. .@.reloc..... .....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\APConfig.ini

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	Generic INItialization configuration [CONNECTION]
Category:	dropped
Size (bytes):	986
Entropy (8bit):	6.253157387259237
Encrypted:	false
SSDEEP:	24:+vw+s7vvh6hqsldg/dLUSvl0ZWP0EK7Fa6UKHzCahzy:+vw17vhqldg/dnvIQWP07Fa6UAWahy
MD5:	6E4E26BB0851A091106C715556648461
SHA1:	F46C4B319C33CFE21896E6AC24154FAC8F96D2EB
SHA-256:	A5E2D74BF94E9400A692EF3EB31F216263DC881FE0BD26F20E879B8C969FB13F
SHA-512:	7F28FDE9D50C6A9624FA8DD5E8393373B8FB0ECAF5BAFF751E762D369F98D686A1AA492522EC5DABB3649908A49B875095DCD20AC1D20644903FA03F3322134 0
Malicious:	false
Preview:	;.....!!!!!!!!!!!!!!!!!!..[SYSTEM]..close-button-action=0..;..... 1:..... 2.....hide-window-after-share=1..default-language=0..;.....APP.... 1:.... 0:..... defalut-codelen = 0;..;.....0:6-8. 1:14. ....0....[CONNECTION]..multicast-ip-type=0..;..ip.... 0:IPv4 1:IPv6....multicast-ipv4-address=224.8.8.1..;..ipv4.....multicast-ipv6-a ddress=ff16::1..;..ipv6.....broadcast-ip-type=0..;..ip.... 0:IPv4 1:IPv6....broadcast-ipv4-address=255.255.255.255..;..ipv4.....tcp-port=4999..;....TE....TCP.....https-port= 1444..;....TE....HTTPS.....group-port=13333..;.....search-max-terminal-num=100..;.....search-over-time=3000..;.....(....)....default-bandwidth=4096..;..... ...default-pcmute=1..;.....PC.....[EUA]..eua-address=..eua-port=....[MultiScreen]..screenchoice=0..[IdeaShareServiceTask]..TaskName=IdeaShareServiceAt2023 0526130440..

C:\Users\user\AppData\Local\IdeaShareKey\DumpTypeConfig.json

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.305255793112395
Encrypted:	false
SSDEEP:	3:3HGolnmGoERHFtRyvY:3HGo8GoeHfRJ
MD5:	7F9084CDC8D6543FB2BA540554E2DD50
SHA1:	A51FBF9A97C31AF9D7B65571F18A17556F12B968
SHA-256:	A2F48DFD7A9EC678CA0B750AA4BB939578B66427D2B866D2326A2A606092F9C2
SHA-512:	17424310D9CFECABCAD34C5DE114614E202D7B8AABA8B857BAB19C5C234F95C65AA056EA8B96EF9A9FD876FB449C3523A7DF647BBB6C9150D9F47CA49D4F0 265
Malicious:	false
Preview:	{.. "DumpType": 208,.. "DumpProcess" : true..}

C:\Users\user\AppData\Local\IdeaShareKey\EUAConfig.ini

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	Generic INItialization configuration [EUA]
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.235090828572348

Encrypted:	false
SSDEEP:	6:Br5ArDLT93AW4KROGLlARKMWaNDUmuyO5EYRXXl+dVT:hgJ3+KSsMkmuHEf0
MD5:	A07D996417082554A2802A01B6397B00
SHA1:	A628F4C21EC347B1DB52F207E28D7A131E0FD0AD
SHA-256:	74E5AB84E3CA74F707062FD8DB7AF77D1E039B0A683879D662E1566D23F07ABD
SHA-512:	3926D4ABC85FB059F7FA0B3100488B5392560B42B76BC32E77271B37794D086A638F0E36B010890160A29B7BB0AD282B7D97C7D60A8D4598F0ABF455EE9AB643
Malicious:	false
Preview:	;.....!!!!!!!!!!!!!!!!!!!..;SMC2.0 eua-version=2.0 ..SMC3.0 eua-version=3.0 / eua-version=..[SYSTEM]..upgrade-url=https://www.huaweicloud.com/product/ideahub/ideashare.html..[EUA]..eua-address=..eua-port=..eua-unicode=..eua-version=.....

C:\Users\user\AppData\Local\IdeaShareKey\FaultReport.exe

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1072720
Entropy (8bit):	6.376676027211651
Encrypted:	false
SSDEEP:	24576:gNbx+L03ycomJPzJnCdTDlFmDDr5MkIhtjd9g:g3acomJPzNllFmvr2kWp9g
MD5:	2D039B24C1F9BEBEE01BA988FC1B8BC8
SHA1:	5212C9542ADE50E8E49872410077EDC924C994E4
SHA-256:	7B0F6A3221A8071D94F1526501698352CDFF942B543561BED462A1AD4E565610
SHA-512:	0DB9689DC6C691336665E3222733DAB5504C7B0F2A6629E4BBFF089D26A09463FE230A39FBD979B39EE90B9053C2A55025B1CF42610718B17CB308A6E2866118
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.k.....h.....n.....V.....V.....~.....y.....i.....l....Rich.....PE..L.....[..... ..... D.....0....@.....p.....q<....@.....\...|.....(2.....P0.....l....9.....@.....0..t..... .....text..... ....`.rdata...8...0...:..$.....@..@.data....(...p.....^.....@....rsrc...(2.....4...r.....@..@.reloc.....@..B..... ....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4326480
Entropy (8bit):	6.375224351213715
Encrypted:	false
SSDEEP:	49152:bnBML8ymWfjTbvykohRC6+JYlkkduOZBZojQ+8XOEG63nq2eTC9OgT4yQ8y2ogKM:9MqWfzrCRF+lZ0Ro
MD5:	A67B045D2024FA2E387F5946E1D18822
SHA1:	32B8EE59C3E45D73C54B41D955F5B07E9B2C5073
SHA-256:	881CD77023E4F1435D0FC5F849786FFAC9E52CEEF5E0737CCEC6F90014EB1BE6
SHA-512:	6057495ED21952064F995D817A04978E43F353561ED1DA3DC20896183F4B2043942553F50A675125E38A2E29004012CA9EE33091CFE4CBAA7E69276111F3CF02
Malicious:	false
Preview:	MZ.....@.....`.....!..L.!This program cannot be run in DOS mode....$.....;x{.;x{.;x{... x{...x{....x{..!~.9x{...:x{..&x.%x{..&~.Nx{..&...x{...?x{.&z.9x{.&...x{...lx{.;x{.zx{..w&.9x{.T...:x{.2...8x{.;xz.$y{.....:x{.%*..:x{.&r..x{.&{.:x{.&...:x{.;x..:x{.&y.:x{.Rich;x{.....PE..L...$.Qa.....!..... #..t!.....0#.....D.....B...@.....>.D.....>.T.....B.....A.P0....B.\.....=.p.....\|.=..... .=.@.....0#.h.....text...r.#..... #..... ..`.rdata.....0#.....$#.....@..@.data.....>.....>.....@....gfids..l.....B.....?.....@..@.tls.....B.....?.....@..._RDATA..0.....B.....?.....@..@.rsrc.....B.....?.....@..@.reloc..\.....B.....?.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\HME_Video_H263D.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	216656
Entropy (8bit):	6.7506717898617925
Encrypted:	false
SSDEEP:	3072:AIUwa4EgKgsIBnbf7buNgzgR4R775rMtmlC57YmnLVrRghJwMZwkK1MYzYUVsGhG:y4EgH6ulMYlWBLVrRZ5zZb/s
MD5:	E3CEC23B09090E7F628934EB026C02DA
SHA1:	370BFA3688815281429A06F51584E14E27F015DE
SHA-256:	433D8DC7EC375FB3BD0AA325C48D7DCB377CBD1F578F3538484625309179BB33
SHA-512:	C2A1FB34771E465D99B08A52E2DA2B587B847CBAE69EBF324072F4044CA0A2B0CDB04BE5277FE07BD59766CAC41611F1DA315162CFE64ACB9CC76D08E4F1F759

Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....Y.....[.....Z.....:.....'.....'... ...".W.....?.....'.....Rich.....PE..L.....aZ.....!....Z.....u.....p.....@.....T..(....P..p.....P0...`..h.....p..... .....@.....p.....text....K.....L..... ..`.rotext.....`.....P..... ..`.rdata.....p.....^.....@..@.data...@.....@....rodata. (....0.....@..@.gfids.....@.....@..@.rsrc...p....P.....@..@.reloc..h....`.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\HME_Video_H263E.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	244816
Entropy (8bit):	6.7801240880524825
Encrypted:	false
SSDEEP:	6144:x4EgujdkrYgiZfHRomD29qz4NYhAOoly2+:x4Eg8f1Jh6kz6Yh+Ex
MD5:	503351F71198FB7337D99E41A9EC9469
SHA1:	5021CEEE10C7CAF37A66ECB31DAED28F1A102C41
SHA-256:	441B20CE4E5E703E71CF789C823D4C0374417F3CF4F9972F1CD872B8AFE1B76C
SHA-512:	AEEE0D5D78236CDA456E0B43BC31A020491A0F2FC5BDD0E909F44B36A1B91366D8031518B2A4C5A6D14F97D3BF67CC396868F44294E856CF76E5BB2385AD78A 3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{..,?..?..?...EB.....E@.K...EA.%.....~-.....~).....~0..6. .<..?..k..?..8 .....~".....~>....L.>..?.$.>.....~>..Rich?.....PE..L...`.aZ.....!.....Y<....@..... o.....o..(.....p.....P0.....0g..p..... .....g..@.....text... ..... ..`.rdata.....@..@.data...h.....d.....@....gfids.....p.....@..@ .rsrc...p.....r.....@..@.reloc.....x.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\HME_Video_H264D.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	339536
Entropy (8bit):	6.837077073322368
Encrypted:	false
SSDEEP:	6144:T4YD/qJsJrmEaJEr0LkooGDcO3+5150dXNw:sYD/qJsJSyr0IooGb32CdXS
MD5:	98D0A3067F1460C1F6CE16BFEAC119EE
SHA1:	819B46AC818070516160ABB8081338FEE83EC5CD
SHA-256:	9DDAD8EB9E1F2AEA03E97CAA9624D043645197794F90DDEA028931AEFDCB1135
SHA-512:	88D55A57EB6ECD832EF4FFB8A2EB3E80CC61F7EC6C86F3346413CD48ECA1F0C47025F22EE42F5F15E6067B71005CA8EBCB2751341C1D95B83E2A38F96DDF1E 69
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....w.!...r...r...rh..r...rh..r...rh..r...r.H.s...r.H.s...r.H.s...r.nor...r...r...r.. .r...rKH.s...rKH.s...rNH.r...r..kr...rKH.s...rRich...r.....PE..L...s,.[.....!.....*..... .....`.....@.....@.....H...(....0..x..... ....P0...@.....0...p.....@..... .....text..... ..`.rdata..".... .....@..@.data...X.....@....rodata.x..... .....@..@.gfids..... .....@..@.rsrc...x....0.....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\HME_Video_H264E.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	572496
Entropy (8bit):	6.813870196889395
Encrypted:	false
SSDEEP:	6144:pBEAOOeOOkf5/eb2Dkj8/GHo1jfS6z6vgrTdfEu7A+v+6NXKzf1rhAOpdYiivYUe:Jf5/Oyt/GHo1jfS6ZxxUbDZrhjdYzYf
MD5:	33153833517326E90F122E8187A1783D
SHA1:	4F193D9B0B031D6187209F6EB1379DFBF8F7B098
SHA-256:	ACED84436E2DDBF8AF9A6B5DBE87FE12BD521147383A16644E78E5416BED6EB0
SHA-512:	9539B6E81A75C679ED734254EAEA734220DC8CA67E7A9185230C6F68076D87D617E3F9EB25A0F6EC83420E19CF63EBB56E370095449F68927DC9A78FB9BCFBB 3
Malicious:	false

Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....d.]. .3. .3. .3..K.1.3..K..V.3..K..:.3...0.3.3...6.6.3...7./.3.)...#.3. .2.}.3. .3.4.3...;...3...3.!.3....!.3. ..!.3...1.!.3.Rich .3.....PE..L....).[.....!.....8...h.....R.....P.....@.....X..P...@Z..(.....p..... .P0.....*...Q..p.....pQ..@.....P..$.....text...`..... ..`.rodata..... ...0..... ..`.rdata.....P.....<.....@..@.data.... ...p... ....N.....@....gfids.....X.....@..@.rsrc...p.....Z.....@..@.reloc...*.....,..`.....@..B..... .....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	110672
Entropy (8bit):	6.1350045814779826
Encrypted:	false
SSDEEP:	1536:dp9S0SXWxThxm4Dii/vLUn/qf6kaMqqU+NV26sDjkZ4eDgVBr8:P9MW1hYiXLUnSYMqqDLSjkZ4esVe
MD5:	5FF5C83B14F5A889BADA319A5BB358C9
SHA1:	01D16B137BF5C2F7CCD6A9A3081B193C4E5C0112
SHA-256:	7EDBE4A8B56DC93AEF55E6FC7773A7969891FB7AE5C7E2B58E912AD6E7F79460
SHA-512:	247AF0225333BFE5495C153E962EFB060C89C1808C980606AFC22830324188C6ADE711F1C1F30AEFE946494F4CE0345D8CFFE4E7138D0AAA7B98E87377723923
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h{.n,..=,..=,..=%b{= ..=.D.<...=.D.</..=.D.<'..=.D.<'..=..#=)..=,..=...= .D.<?..=.D.<-..=.D.=-..=.D.<-..=Rich,..=.....PE..L...<.J`.....!.....s.....@.....p`.....L.....<.....P0.....p....U..8..... .....V..@.....L.....text...>..... ..`.rdata...^.....`.....@..@.data...P....p.....\.....@....idata.....^.....@..@.gfi ds..%.....j.....@..@.00cfg.....I.....@..@.rsrc...<.....n.....@..@.reloc..M.....t.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\HW_H265dec_Win32D.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	425040
Entropy (8bit):	6.780509562078731
Encrypted:	false
SSDEEP:	6144:cc7XlftWAILyubX2T0Kmd/xaksZCJtidQjdQjaYTG46Uo9HuPbE5uW6ES:BjWAIt2Tgx3YTGzOPbE5uW6v
MD5:	12ADB346824A97E1A36E4C679F8BEC68
SHA1:	14948C5065F48041F47E943A653EA2BF69BF5EE3
SHA-256:	66F2636A7D5CE1302F946B3B22C9ADB14EDFFF0AA1DF5A74E7366D738B5AFB47
SHA-512:	8147BF9A4053BDF2D6C39EBBF677BBC3770CE0C107296F396536E29203D3035277A3B631AA084480F21DA43A6175AC59054DB60FCB0A85ACE07A436574A4E95
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....v.Z.....?.b.....?.`.....?.a.....I.....I.....I.....V.X.....I.. .....I.....ll.....I.....Rich.....PE..L....\.\.....!.....$...0.....@.....@.....(.....)..(....p.....L..P0.....!..p..... .....p!..@.....@..$.....text...7#.....$..... ..`.rdata..&....@.....(.....@..@.data.....@.....@....gfids.....`.....$..... .@..@.rsrc.....p.....&.....@..@.reloc..... ...,.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKey.exe

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2133352
Entropy (8bit):	6.05899363891946
Encrypted:	false
SSDEEP:	12288:wHqmIYaT78j5ybM8vSagD6en57GGLGWV9LaDKSSsJ8JTgGL2tSMH77YQaJ3QZixq:bsD6IZfLibWJTgXt97IJgUq
MD5:	30B853E3808705B98AE4C7F92670DA58
SHA1:	9B94C1D8F9BAEA96AEC0B65BE8803DE1F5BE9B34
SHA-256:	F2D6AA073D9A05843D7AAEDAE9BE83E737836E0A781439015E70B458F321B4DC
SHA-512:	83B1552CA2B90F7D00D8B0386E45C334E7070FF486D97B3666E26FF62B7DC33A6E1EA27C0C0F89FD543F162435BC0C260F242863AE20D65A60E68AB044558627
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....6B..W,_.W,_.W,_./._.W,_.?(^.W,_.?/^.W,_.?)^.W,_.?-^.W,_.<+^.W ,_z>)^.W,_w>-^.W,_A>-^.W,_z>-^.W,_.<-^.W,_.W-_.T,_w>)^.W,_w>._.W,_.W._.W,_w>.^.W,_Rich.W,_.....PE..L.....a.....$...T.....r.....@....@..... .....*. ...@.....|.....v .h..... ... ...8.....X...@.....|.....text...&".....$..... ..`.rdata..<r...@...t...(..... .@..@.data.....@....idata..H.....@..@.tls.....@....00cfg.....@..@.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	467304
Entropy (8bit):	2.6884804650060365
Encrypted:	false
SSDEEP:	3072:Yj+K5m4AWLJppB08rbggromrWrxYMyf+Rr:YaKLLimrCxYMHr
MD5:	4C43F81A16703A0539A95CCCB064585F
SHA1:	C19E07D0CBB8BA66E4DD86010B42A55338100B24
SHA-256:	17F9772138062770DE8BF6F22270A2B9E63AC4BB83369AAC40BC391447FC2EEF
SHA-512:	0B45DD3A2AA3EE53922C3A02D45B4AD83D9EC4208F908B455F989F9247F9E61292E328EF1E0869FFF6967B31858EA2CEA11AB12BDA5AA70D52A7B3A8F6198D7 F
Malicious:	false
Preview:	MZ......................@.................................. ....!..L.!This program cannot be run in DOS mode....$.....................6.../.......................Z.....2....... ...Rich...................PE..L...2&Sa.....................N...................@..........................0.......v....@............................ ... .@..................h.... ....T...........................x...@........ ....0............................text.............................. ..`.rdata..@W.......X.................@..@.data........0.....................@....rsrc........@....... ....@..@.reloc....... ....@..B... ....

C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.xml

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	2752
Entropy (8bit):	3.5425978089708146
Encrypted:	false
SSDEEP:	48:yei1q9eQn1ab9f9V9Lvara+iniudupRCRfMufAuRa7T5XHPsV8iRrp+++:tpnkpBGdinigVMll7dHFA+
MD5:	59A14E32BD5B5C0FB0FD95D259C8B290
SHA1:	86D422B0CD2AAFE63C09C54063B739EE57DDA49E
SHA-256:	8193F1847C8849A5FB567F74CFAA8EAAA5418B99132465F2B6E65DF56B3BFA09
SHA-512:	9CF9FF9A3DDE24085937ABAAD7F75BA8CD5C6A6F6D2C31C1EE0DBA0E5C940A005F404B8EE4C9DE5CE38B969ECDD107E6E98CA0E29039053DC54D024A7F00 B451
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.T.a.s.k. .v.e.r.s.i.o.n.=.".1...2.". .x.m.l.n.s.=.".h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n.d.o.w.s./.2.0.0.4./.0.2./.m.i.t./.t.a.s.k.".>..... . .<.R.e.g.i.s.t.r.a.t.i.o.n.I.n.f.o.>. . . . .<.U.R.I.>.\.I.d.e.a.S.h.a.r.e.S.e.r.v.i.c.e.<./.U.R.I.>..... . .<./.R.e.g.i.s.t.r.a.t.i.o.n.I.n.f.o.>..... . .<.T.r.i.g.g.e.r.s.>..... . . . .<.L.o.g.o.n.T.r.i.g.g.e.r.>..... . . . . . .<.E.n.a.b.l.e.d.>.t.r.u.e.<./.E.n.a.b.l.e.d.>..... . . . .<./.L.o.g.o.n.T.r.i.g.g.e.r.>..... . .<./.T.r.i.g.g.e.r.s.>..... . .<.P.r.i.n.c.i.p.a.l.s.>..... . . . .<.P.r.i.n.c.i.p.a.l. .i.d.=.".A.u.t.h.o.r.".>. . . . .<.R.u.n.L.e.v.e.l.>.H.i.g.h.e.s.t.A.v.a.i.l.a.b.l.e.<./.R.u.n.L.e.v.e.l.>..... . . . .<./.P.r.i.n.c.i.p.a.l.>..... . .<./.P.r.i.n.c.i.p.a.l.s.>..... . .<.S.e.t.t.i.n.g.s.>..... . . . .<.M.u.l.t.i.p.l.e.I.n.s.t.a.n.c.e.s.P.o.l.i.c.y.>.I.g.n.o.r.e.N.e.w.<./.M.u.l.t.i.p.

C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log

Process:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	1534
Entropy (8bit):	3.1885529270410067
Encrypted:	false
SSDEEP:	24:Q+Md0I+d8ortdGDd6DAsAI+dF44O4odFWdF6oqd7I+dLIt:rMz+aort8Dk+PPFoPWP6oqq+Kt
MD5:	88C284B7CF3256E6964D8326563C920A
SHA1:	10427ACBA1747AE26FBDE7AED3EF1ABC0BA318A5
SHA-256:	EDC0C98E73A5BAB7154878A6D33E261CEE8B94EEE2326502CBA373F14C6A0093
SHA-512:	0DFE4220F75C8280922BAD7FA852DE7BB981740441C3D95D3F63CFF27A985ED70BE199A164ACFE4AE9F6062F951597A47E19937620ADB6E8D777C20556CDF21 B
Malicious:	false
Preview:	..[.2.0.2.3.-. .5.-.2.6.].-.[.1.3.:. .4.:.4.0.:.2.1.1.].I.n.f.o.:.*.I.d.e.a.S.h.a.r.e.S.e.r.v.i.c.e. .S.t.a.r.t.!.!.!.*.......[.2.0.2.3.-. .5.-.2.6.].-.[.1.3.:. .4.:.4.0.:.2.5.8.].I.n.f.o.:.*.D.i.a.l.o.g. .I.n.i.t. .S.t.a.r.t.*.......[.2.0.2.3.-. .5.-.2.6.].-.[.1.3.:. .4.:.4.0.:.2.5.8.].I.n.f.o.:.C.h.e.c.k. .I.d.e.a.S.h.a.r.e.K.e.y. .D.e.v.i.c.e.......[.2.0.2.3.-. .5.-.2.6.].-.[.1.3.:. .4.:.4.2.:.9.4.0.].I.n.f.o.:.*.I.d.e.a.S.h.a.r.e.S.e.r.v.i.c.e. .S.t.a.r.t.!.!.!.*.......[.2.0.2.3.-. .5.-.2.6.].-.[.1.3.:. .4.:.4.5.:.6.1.7.].W.a.r.n.:.n.o.t. .G.e.t. .L.o.g.i.c.a.l. .D.r.i.v.e.s.......[.2.0.2.3.-. .5.-.2.6.].-.[.1.3.:. .4.:.4.5.:.6.1.7.].I.n.f.o.:.N.o.t. .f.o.u.n.d. .D.e.v.i.c.e.......[.2.0.2.3.-. .5.-.2.6.].-.[.1.3.:. .4.:.4.5.:.6.1.7.].I.n.f.o.

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.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%
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\IdeaShareKeyInstaller.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:	1AE4580ECEE6E992501C963B9406A2A0A927CA48AB0A3E7B8FDC247EC21AA74EDA9818224D72C3088893418FE8E5044E857B347D056B77DC5D4F73F5BF0EAC DA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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\IdeaShareKeyInstaller.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:	A2AF4D9ACE035C51E5CF846DB3955895422E65AE6A6D7D523493AC3AE6BC28ABA87A272BB50B16FC5FFF438723A911E31DED0EEFBDB4EFF7416D7C5E121C6 4CA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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\IdeaShareKeyInstaller.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%
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\IdeaShareKeyInstaller.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:	1280CCF34D6B31CAAC2D5F5EAEEDB45E8D8F364E378EC79CCF63072CC40D5ADBB38016D934C8A193606FA6D00F7A7CC4C844DE4E94B06203DA6F954A190763 9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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\api-ms-win-core-debug-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552
Entropy (8bit):	6.807322537395992
Encrypted:	false
SSDEEP:	192:43W1hWJn744tk0icWU9F6MZVGl4ogvekMEbceCayowG:UW1hWF/u2WuFRZk4VvDMCYa0G
MD5:	86AD4CED5FA23308A3F1F2864DC46A0C
SHA1:	8F83EABAC8720C741A1FE826A5444C20C4F2BF97
SHA-256:	A17BE9DFB1193EC6E03F86FAC682F845AC4B7318E7F2AB26FAB81F7BFD0704B7
SHA-512:	8E24C32C1237EB52FEBA46071ADAB77D943C590C466410CB26645744524C73CD3D666DC844A149CFA096F5780E7227B47602E1C04E99B272E8F2C2B0D9CF23E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ...~.....!..... .....0.....E....@..... .....h.....T.....text..... ..... .`.rsrc..... .....@..@.....~.....9...T...T.....~.....d.....~.....RSDS..' .I_^..IR..I....api-ms-win-core-debug-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....~.....P.....(...8...H...|.....q.....api-ms-win-core-debug-l1-1-0.dll .DebugBreak.kernel32.DebugBreak.IsDebuggerPresent.kernel32.IsDebuggerPresent.OutputDebugStringA.kernel32.OutputDebugStri

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-errorhandling-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped

Size (bytes):	8552
Entropy (8bit):	6.887791584852844
Encrypted:	false
SSDEEP:	192:OnmxD3jW1hWJw744tk0icWU9F6MZVGl4ogvekMEbceC4WXqxixB:On4W1hW6/u2WuFRZk4VvDMCY4WXqixB
MD5:	461ECB89ACC6B7AFB8CD3C7A531279EE
SHA1:	2E9409369E14D747D4D5027B1B6CCDC46B009B65
SHA-256:	8BCBB0599A08986D8A6B91AC6504AA7E1CADFA800E543199896358E5936117D1
SHA-512:	84FDA003E18F640548BECBD024A0FF30E90AE7BC39F523EABB33EB05A7E75FEA6F38E53E919D8C3B147A1D377E1E4693B84DD696BC39815104F0B5D0A2068BC3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L....<b.....!..... ....0.....[....@..... .....h.....T..... .....text..... ....`.rsrc..... .....@..@.....<b.....A...T...T.....<b.....d.....<b.....RSDS....>....j..C.....api-ms-win-core-errorhandling-l1-1-0.pdb .....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....<b.....n.....(...D...`.....4...f.....'...J.....api-ms-win-core-errorhandling-l1-1-0.dll.GetErrorMode.kernel32.GetErrorMode.GetLastError.kernel32.GetLastError.RaiseExcept

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-file-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12136
Entropy (8bit):	6.669096938301602
Encrypted:	false
SSDEEP:	192:2d5RDYPvVX8rFTsxW1hWJM744tk0icWU9F6MZVGl4ogvekMEbceCKmi:66PvVX7W1hW6/u2WuFRZk4VvDMCYKmi
MD5:	F2902CBE3338B160EAA9EC197C85D3F4
SHA1:	933B6D48897043B7C17039DFE1F25577A67500E5
SHA-256:	206A6B4A28643F29A04FE8726CFD28949652C1FEDB7BE817C2D2339DBC7BB6B5
SHA-512:	BC0099CC0BE317047DF5ADBAF2B25561B10C8A9514DDDEF1B0A648274357F32FF2EC328ABA8290E91706BE02CC245662859CA6B4FE4B3C9F1093DE315FED03A3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L...s.(.....!.....0.....@.....X.....@.....0.....h.....T.....text..... ....`.rsrc.....0.....@..@....s.(.....8...T...T.....s.(.....d.....s.(.....RSDS..c."....]3.9.O.....api-ms-win-core-file-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....s.(.....K...K.....D...p...6...`.....?...l.....A.....6..._.....:...e..... ....l...n.....-...d.....*...g.....*...U.....M...

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-file-l1-2-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552
Entropy (8bit):	6.848685532385122
Encrypted:	false
SSDEEP:	192:Z1WIghWGwnY744tk0icWU9F6MZVGl4ogvekMEbceCVO:XWPhWs/u2WuFRZk4VvDMCYVO
MD5:	43ECE6A90EDAADD2FF48AB8C8C6774D4
SHA1:	5D36019F3A938E7EB8C346A663353FAA5B1F4C0F
SHA-256:	7D977159F753E6B4FE7A82D2DDFC83BF58659E0E24E460977C6FEFB872DFDAF0
SHA-512:	32D8C2321C8C1925FB3055536F273ADD085385343288A038FF6D66C80F25FF5D7A0C4373D53729DB0D7ABEA56445545F201DA6D6D3DCAA88362754D0B30AB39
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.....!..... ....0.....M.....@.....L..... .....h.....T.....text...<..... ....`.rsrc..... .....@..@.....L.....8...T...T.....L.....d.....L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T.....rdata$zzzdbg.....L....edata... ..`....rsrc$01....` .....rsrc$02.....L....@.....(...8...l.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kernel32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-file-l2-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552

Entropy (8bit):	6.984013967829882
Encrypted:	false
SSDEEP:	192:1ZwWIghWGwk744tk0icWU9F6MZVGl4ogvekMEbceCdS6qd:IWPhWI/u2WuFRZk4VvDMCYdRqd
MD5:	5DD19F00D3DBFE2A6E951D02DA187E57
SHA1:	06A9C8A9AE826950814E86812C1B9FB42D7C7382
SHA-256:	57E1AB78D04F211A130934903C3D1309AC2AC6FD12CF027D70E5A041319F02C8
SHA-512:	5F30BE97126DA6174730650177D3431D244F8E720F61056D58A2CC3004AF9014C95702C4DDC8296AEFB001F5F426C583B2FBCFE71925EC875C80217373AD6402
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..\|.... .....!..... ....0.....@..... .....h.....T.....text...}..... ....`.rsrc..... .....@..@....4..\|.....8...T...T.....4..\|.....d.....4..\|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata. .T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....4..|.....D...p.....#...P.....;...g.....<...m.....%...Z..... .api-ms-win-core-file-l2-1-0.dll.CopyFile2.kernel32.CopyFile2.CopyFileExW.kernel32.CopyFileExW.Crea

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-handle-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552
Entropy (8bit):	6.837987798459471
Encrypted:	false
SSDEEP:	192:TW1hWJZ744tk0icWU9F6MZVGl4ogvekMEbceCGyDap0YZ/cGC:TW1hWD/u2WuFRZk4VvDMCYGRVUGC
MD5:	D6B1A1E8D8B199A853F1FD76B54670C4
SHA1:	22DE0F484DA80675E4C28F2678B034F5230240EB
SHA-256:	0DDDC1FADEB2BC447314D0EDFE4E5C091F246497229EDD66BEE096EF062620A2
SHA-512:	9618A224ED5B05348898C9F1E8AEBC27BDED6256A4BF7EDA9CD2651B68D3B198218A72F42D2B5AB9AE60C94D7068BC7A82DD9F4D2C113CED7D91220F37F5C 9C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ..c..c.....!..... ....0.....@..... _..... .....h.....T.....text..._..... ....`.rsrc..... .....@..@....c..c.....:...T...T.....c..c.....d.....c..c.....RSDS..:..z][....08d.....api-ms-win-core-handle-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....c..c....Z.....(...<...P.....A...|.....,.....api-ms-win-core-handle-l1-1- 0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-heap-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552
Entropy (8bit):	7.018650924251849
Encrypted:	false
SSDEEP:	192:FEleW1hWJSB744tk0icWU9F6MZVGl4ogvekMEbceCllDQj:FEleW1hWwR/u2WuFRZk4VvDMCYllMj
MD5:	2BE904BCB606F729840BE69EE40E44B2
SHA1:	A904312EF84915BBBA051EF40A09887FD706CEE0
SHA-256:	0DB2FC25B2879C11E19C69759C25FB1775AB696789A7A5B3552AC9DF7F7FA904
SHA-512:	404791D83EB7E725D385B2DC6FFD768AED9634F3B4549CF38D5FBDC37997FFABF75F24BC49E474C1DDE5B60BD0658ED86D5C1B814C10449B9B95E9AB7FC33 26
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ..l7.....!..... ....0.....a.....@..... .....h.....T.....text..... ....`.rsrc..... .....@..@....l7.....8...T...T.....l7.....d.....l7.....RSDS..3.+.!u..m.m.....api-ms-win-core-heap-l1-1-0.pdb..... T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....l7.....X.....2...Q...q.....C...h.....(...E...f..... .....0..._...z.....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-interlocked-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9064
Entropy (8bit):	6.797947539384126

Encrypted:	false
SSDEEP:	192:p5iYsFqW1hWJw744tk0icWU9F6MZVGl4ogvekMEbceCkOr:p5iYsFqW1hWW/u2WuFRZk4VvDMCYk0
MD5:	4C2142996B21E2644879E5203624EC59
SHA1:	B38B0719A3CF609855072FF422C5F96C2282BD00
SHA-256:	13A8C7CF80A6B8DFE4E90095EE836E5AAA632DE2213A499A39FC46C31BD698FB
SHA-512:	B9D59FCB4AE261F3BC856E8726F7A5044CC4F5BDDDD8FFC7BF5A92983871BC49771F06AFE2D9821CD538376DC13E6C7C2A74B029709B8E570BC14AFE32095A19
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ..`H.....!..... ..... .....0.....@..... .....h.....T.....text..... ..... ..`.rsrc..... .....@..@....`H.....?...T...T.....`H.....d.....`H.....RSDSR..*: H..*.2\.....api-ms-win-core-interlocked-l1-1-0.pdb.. .....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....`H.....(...T.....L.....!..U.....1.....p.....@...s..... .....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-io-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9064
Entropy (8bit):	6.659206533560419
Encrypted:	false
SSDEEP:	192:wWBhWzH744tk0icWU9F6MZVGl4ogvekMEbceC5U0Gt:wWBhWP/u2WuFRZk4VvDMCY5Ul
MD5:	2B3B17466A3E0E028093835CF6757986
SHA1:	563755352589B2EE15F7DBD920E93846A4F9671D
SHA-256:	FF711920AAC91746EE6241D3CC6466D213ACC1AFE31F89409C02228E125BF66E
SHA-512:	5941877A6B006884F5DB5A57D69394AE17A936D75037ABD661F9CA48EE6D0729AA37C8868460B30C1601B826F9097790D139F21932697A3665994CA14BE543DC
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3...w.w.w..._.v...C.u...\.v...A.v.Richw.....PE..L....K.T.....!..... ....0.....:....@..... .....h.....8.....text..... ..`.rsrc. ....@..@..... .....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-libraryloader-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9576
Entropy (8bit):	6.765413150281784
Encrypted:	false
SSDEEP:	192:dvmgdKvuBL3BZL8W1hWJMy744tk0icWU9F6MZVGl4ogvekMEbceCajNer3:d+g4vuBL3BmW1hW1/u2WuFRZk4VvDMC6
MD5:	06007617BEB4F1690309E88F7E0735FB
SHA1:	38B7BC000A138D611FD61191BEDDC42D46138D70
SHA-256:	648D13605052E86F9D580FC02F51CF71922F9E86ED994454666F5E7916FABBB6
SHA-512:	416F3735611DFFB144E124EB8AC4112A99823A18B49D28A8B4FB0E07CB58C6B6F665BC4AE28BBD6853A6568B14A884BD105C6B52905ED8BAD465B17D6F24120E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ...A.....!..... ....0.....c4....@..... .....h.....T.....text..... ....`.rsrc..... .....@..@.....A.....A...T...T.....A.....d.....A.....RSDS6..7....].8D.....api-ms-win-core-libraryloader-l1-1-0.pdb..... ..T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....A.....(.....G...z.....-...\.....=...j.....(...l...k..... 7...`.....O...r.....*...Y.....=...^.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-localization-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10088
Entropy (8bit):	6.6051372332267775
Encrypted:	false
SSDEEP:	192:zIgZaSs8zF3xd3nHM0uWohWPM744tk0icWU9F6MZVGl4ogvekMEbceC1y0:zIDSsYF3xd3nHM0uWohWc/u2WuFRZk4i

MD5:	F190B9E47B75AB76C211F9AA2B977760
SHA1:	701AA08D014DFF8991B753D30C10A03C8604F510
SHA-256:	FA691EB187ABA98605765E79D5A61ABA568F8B4E3018D4398A148517DC4A315C
SHA-512:	719C0432144D81124BDD9A920880BE0A33CE19648D79D44C96DCB0A694C0E6ADE43D7E9841A34B542ED5A4C4BE4BEBEB562BA97DCEAA73DF15278A3B513D4A3B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...{..{..{..r._.z..r.N.y..r.Y.z..r.\.z..Rich{.....PE..L..... .Q.....!..... ....@.....0.....@.....u..... .....h.....text...e... ....`.rsrc..... .....@..@..... .....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-localization-l1-2-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11112
Entropy (8bit):	6.827717959439512
Encrypted:	false
SSDEEP:	192:DuZOMw3zdp3bwjGjue9/0jCRrndbVWIghWGwO744tk0icWU9F6MZVGl4ogvekME4:4OMw3zdp3bwjGjue9/0jCRrndbVWPhW3
MD5:	46D931081C0627A149943DC3C8E1FFE7
SHA1:	F4846083ABD9F37E25B731C65AC177D4AE4E2DB3
SHA-256:	EE8B5A0881DFBB72E8C63A3FFD30D3E62D1467F9693AB743D117612B2B11AB02
SHA-512:	6ED4BE78F479C36DF0B75BFF7CC243AFAD4B61790DAC4D39EEEE1FBB34F4EC7B1E5D8F8D02C2966579B76157A62DFC5440FC331E1D14DF70ABE72A5E472C877B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... .....!..... .....0.....]....@..... .....h.....T.....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....;...;...(.....<...f.....5...]....!...l...q..... N...../...j...../...^...../...\.....8...`.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-localregistry-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10088
Entropy (8bit):	6.494013779954252
Encrypted:	false
SSDEEP:	192:ct6SHWohWXg744tk0icWU9F6MZVGl4ogvekMEbceC0qH5:3SHWohW4/u2WuFRZk4VvDMCY0qH5
MD5:	AE360771ADA3A11A2BA30AB4FEEBF76F
SHA1:	88A4E2F97536C9A0247B875EDC17C1A689BD6A71
SHA-256:	4F630CABF2E601AE368A694C47057C5A4A9A809E7C155745193FC93883F1D4D9
SHA-512:	11262BC5B5C6EC888E3E71EF633B4707F30B211632073B2BC9B2A837A56D11B675EBCA510878BA6FF0D7C2F16C13498AAE8D8C16F23BD9D63C70655FB5E20F50
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...{..{..{..r._.z..r.N.y..r.Y.z..r.\.z..Rich{.....PE..L..... .Q.....!..... .....@.....@.....[..... .....h....0.....text...K.... ....`.rsrc..... .....@..@.reloc.....0.....@..B..... ....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-memory-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9064
Entropy (8bit):	6.828381437265535
Encrypted:	false
SSDEEP:	192:/btW1hWJU744tk0icWU9F6MZVGl4ogvekMEbceCqgbU:/btW1hWi/u2WuFRZk4VvDMCYqgbU
MD5:	F1F85A25C7ABC45D24B64B891815B510

SHA1:	5D467A2EF9F05FE140910EF304EA211B71FC58D3
SHA-256:	96292248376742BECFA5130C07F81CCCED8B75291CE55CA8C56AFC3967021ADC
SHA-512:	EEE46B07F9F7B582D29DE29618A2159F8F12F2B303722C74A395F8C6EC7DC303568F4F3B28636AB4DE4818748A9D73A68442CDD7D46B67F3497E10C20A3AB3F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ....@p...........!........................ ....0......."....@............................l............ ....h..............T...text...l......... ....`.rsrc........ ......................@..@......@p........:...T...T.........@p........d.................@p....................RSDS..?O.....Z..n....api-ms-win-core-memory-l1-1-0.pdb.......... .T....rdata..T........rdata$zzzdbg.......l....edata... ..`....rsrc$01....` ....rsrc$02......................@p....................(...h...........)...P...w..................C...g..................%...P...........B.. .g...................4...[...|...................=...................................api-ms-win-core-memory-l1-1-0.dl

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-misc-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10088
Entropy (8bit):	6.350968002370562
Encrypted:	false
SSDEEP:	192:4s0D2rWohWXe744tk0icWU9F6MZVGl4ogvekMEbceCRHdG2W:PWohWC/u2WuFRZk4VvDMCYRHsP
MD5:	59E238940F143B1519F9FD4F873A8D23
SHA1:	28B6B3F7ED3551F27F4735BE612A0E26CBECB318
SHA-256:	E258403032B863626B8979DD5CE87BD6D84C61D8F0796457CE9FB83026E5BE80
SHA-512:	B674D66BF4B3E6978611EAC978C91A8113BD4B4407C5EEDFCA80AE3637D2B87B51702F5C0D36FB0A3052F7627DBDE7B2562794E7C4208165F25B48196B8917E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......?...{..{..{..r._.z..r.N.y..r.Y.z..r.\.z..Rich{..........................PE..L..... .Q...........!........................ ....@...........@............................n............ ....h....0...text....... ....`.rsrc........ ....@..@.reloc.......0......................@..B.. ....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-processenvironment-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9576
Entropy (8bit):	6.7750746850469294
Encrypted:	false
SSDEEP:	192:vHW1hWJa744tk0icWU9F6MZVGl4ogvekMEbceC/PJy:vHW1hWo/u2WuFRZk4VvDMCY/PJy
MD5:	338D8312971776E15DBEAE1DD411379E
SHA1:	A56972C6AD98D91AF383D450EAA39FC3DC96CA3B
SHA-256:	827C37AD66CEE66564E09915183BF28B394A82408577CD95DA0AD28B9A80CD38
SHA-512:	6FAB24A333C8709D969C16F6A8B937439E9B633357D1D62C08BDB4D2037A384B54267502E19E4CA62538B96C238885A981EDA0CA24DE82E94337AAF034587899
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ....!........................ ....0............@............................G............ ....h...............T..text...G......... ....`.rsrc........ ......................@..@................F...T...T...................d.......................................RSDSW.........$.~).....api-ms-win-core-processenvironment-l1-1-0 .pdb...........T....rdata..T........rdata$zzzdbg.......G....edata... ..`....rsrc$01....` ....rsrc$02................................(...\|.......B...............$...M...{...............P...................6...k........ ..../...(...e...............=...f...............8...q...............!...T............... ....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-processthreads-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10600
Entropy (8bit):	6.839787316810637
Encrypted:	false
SSDEEP:	192:ZLfk1JzX9cKSIdW1hWJv744tk0icWU9F6MZVGl4ogvekMEbceCuKR5o:pfk1JzNcKSIdW1hWR/u2WuFRZk4VvDMU
MD5:	8376C584A28430235AF597B4CA3CA0DE
SHA1:	65AE54E058DC79EB11B47F67E226783CE1B36CE1
SHA-256:	5AF602F4DD90F4C6EDA49EE73E0D33D002A696FA7550C67117F962E02F9B061A

SHA-512:	118D608CFA7AC6FE1E70E2144B02F7782ED387E5560F490603C386A1BE777C0C112E8C2BEF5E699DA35529F1E140D79BA25CE36E8216EFD1E2D09DE5DFB794(5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ...P.....I..... ....0.....@..... ....h.....T.....text..... ....`.rsrc..... .....@..@.....P.....B...T...T.....P.....d.....P.....RSDS...&^Z.....5.n~.....api-ms-win-core-processthreads-l1-1-0.pd b.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....P.....1...1...(.....K...x.....,...`.....C...q.....'...N...y..... ....."...I...{.....B...p.....,...c.....H...x.....9...S...p.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-processthreads-l1-1-1.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9064
Entropy (8bit):	6.874778036355501
Encrypted:	false
SSDEEP:	192:0NADfIeRWIghWGw7744tk0icWU9F6MZVGl4ogvekMEbceCIv525:0NADfIeRWPhWr/u2WuFRZk4VvDMCYIvu
MD5:	10BF9BA5ED56387B19BAC5828372FEE7
SHA1:	48A6CB59F92788CB779DA29154ED6A61DC04A8EA
SHA-256:	78321B589DE714CE936A056279778BB02AD3008D48E91F597B8906F85197AF92
SHA-512:	BC634453E954F968C6FBBAB05161906107454DCAA9FA541D9888381D56D581FC16E5D10E871E3C815455237B052F14B88E7A4695F1F76B70C5E0BF9723456277
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....9..... .....!..... ....0.....w....@..... ....h.....T.....text..... ....`.rsrc..... .....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&.n....5..l....)....api-ms-win-core-processthreads-l1-1-1.pdb..... ..T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....9.....(...`.....-...l.....".."...W.....N.....P.....F...q..... .....3...r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-profile-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8040
Entropy (8bit):	7.047105665145192
Encrypted:	false
SSDEEP:	192:xiW1hWJli744tk0icWU9F6MZVGl4ogvekMEbceC6pwfb+q:xiW1hWR/u2WuFRZk4VvDMCY6Xq
MD5:	045D0A8EC27B42B52CCC4468B3DD9896
SHA1:	B9DC492BE2DA2F7F582696CFEA2958C6B4995B33
SHA-256:	9A5BA3BC8FE04C0D69E29D3F0F63271CD82D4991CF6EA7B956E266A175530C30
SHA-512:	6A3D14AE4EFFC490343B1ED92432021D289B7D48CEBCC4492CAE495414E55F1869C3A09B95D4B6B1BEFE990B232266C2314B93DD98184D7B8A0B2A4CDC939A 9D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L....- .....!..... ....0.....@..... ....h.....T.....text..... ....`.rsrc..... .....@..@.....-.....;...T...T.....-.....d.....-.....RSDS....M.h=.N...`....api-ms-win-core-profile-l1-1-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....-.....<.....(...0...8...w....._.....api-ms-win-core-profile-l1-1-0.dll.QueryPerf ormanceCounter.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-rtlsupport-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8040
Entropy (8bit):	7.047594552109745
Encrypted:	false
SSDEEP:	192:Q6uGZW1hWJO744tk0icWU9F6MZVGl4ogvekMEbceCCsDW:Q6uGZW1hW8/u2WuFRZk4VvDMCYCEW
MD5:	C41A2341F5D3570636268E0757FA34C8
SHA1:	EEF3D2D3DBD5F2F5765CD5BDAEAD24D8595A7B63
SHA-256:	275FB34B1ECF18E9177FDC257785E9F251F65C3E5118232B2FA241460AF1F052
SHA-512:	C6490062944F7A973958ED0E89D82592F0AA73200C3108AB21713639B292FFEEED960F867D272CAE7DBCA174885FF7B6CD1FF596805A453356B062BB61E0831A

Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ....?.....!..... ....0.....@..... .....h.....T.....text..... ....`.rsrc..... .....@..@.....?.....>...T...T.....?.....d.....?.....RSDSMmC{Sj.6..m.....api-ms-win-core-rtlsupport-l1-1-0.pdb... .....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....?.....F.....(...4...@...~.....l.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlCaptureContext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-string-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552
Entropy (8bit):	6.909683481057144
Encrypted:	false
SSDEEP:	192:syMvlW1hWJ8744tk0icWU9F6MZVGl4ogvekMEbceCRuil:syMvlW1hWe/u2WuFRZk4VvDMCYRuil
MD5:	037780DA6EA1272C1E6F0BB6E9C79277
SHA1:	AA31CF5CA1EF374EA60B92126283F96D65825F95
SHA-256:	3F9F4C5901196CD60F38F794AC3CC4AC999B6A208FD81CA927F102710D135A0D
SHA-512:	1AED234EBFAD3F88D942B37C15C71322B98D3137DB451B283F13AFAFA328FE5B056FD82983A513BCAC44B0495F157015928796574C9ECFAE63759DD2D8D18A73
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L...?%.....!..... ....0.....@..... .....h.....T.....text..... ....`.rsrc..... .....@..@....?%.....:...T...T.....?%.....d.....?%.....RSDSv..v0.M..-.~UP....api-ms-win-core-string-l1-1-0.pdb..... ..T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....?%.....x.....(...H...h.....)...O...x.....>...i..... .....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-synch-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10600
Entropy (8bit):	6.72682923520993
Encrypted:	false
SSDEEP:	192:6dv3V0dfpkXc2MAvVaoK5W1hWJ9f744tk0icWU9F6MZVGl4ogvekMEbceCMaZag3:6dv3V0dfpkXc0vVa7W1hW7T/u2WuFRZs
MD5:	05004028CC37056DD1494845DB22A7B7
SHA1:	2466C474B8958BD21670518AD1C96FB7A8008075
SHA-256:	432985B0FFC5DB8180F7E33EA2362244424622AFC24A924A3E9E851F5A993FF5
SHA-512:	A0FAF124F4657D255764BF99AACC47CDE4B54FF0A9583953D805BDC16CC15D1870F7BBDCE3A9AC3FB47A76FD2A44BCE69A39FFFCC044E9F5F5D2C12683168FE
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ....^P.....!..... ....0.....u....@.....V..... .....h.....T.....text... V..... ..`.rsrc..... .....@..@.....^P.....9...T...T.....^P.....d.....^P.....RSDSu.J@z..Hd/..!+.d....api-ms-win-core-synch-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....^P.....)...)...(.....p.....1...c.....!...F...m.....$...X..... .....$...[.....@...i.....!...Q.....[.....7.....O.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-synch-l1-2-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9064
Entropy (8bit):	6.929250597299494
Encrypted:	false
SSDEEP:	192:Cu+ANY2tZ3gWIghWGwd744tk0icWU9F6MZVGl4ogvekMEbceCcEICn:ntZ3gWPhWp/u2WuFRZk4VvDMCYcE9n
MD5:	531B792880D9F8961EF9AF63D2BE6FE1
SHA1:	789F8FB5E2F6C0400B9A3EE5F17D1F3E95D17D7A
SHA-256:	AD310E1633B908D62F1F8AAE92E2AFB9A86C5A71AA6FABF306CDAA2DC78E0989
SHA-512:	6D8B8DE046865889AAF723359F94D8F65EE175196D2E47A3BAC9EDCB1AEF5E63F19972B794A0AFCFACA288B57BF712337D29CC77513DA8B3D5C1C718C1CA9ICD

Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... ....0.....@.....v..... .....h.....T.....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rdata..T.....rdata$zzzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...l.....R.....W.....&...b.....$...W.....6...w..... .....;...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-sysinfo-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9576
Entropy (8bit):	6.78780327042544
Encrypted:	false
SSDEEP:	192:OrLv12KIMFAW1hWJE744tk0icWU9F6MZVGl4ogvekMEbceCNYnP:OrLN2NW1hWu/u2WuFRZk4VvDMCYNC
MD5:	F2D73704D46DE29BE97CF3717C441F50
SHA1:	BCC0A82C4D46F5731C5C574C981D9F2C18565628
SHA-256:	77043C1A00F4B5D4F5C62B54B47AE19B1C34AC90BBAFA8C209219791A83C4152
SHA-512:	975AAD9289A540D194AE5FB4919050C5F5624C65CC0F0208770F7F39DE085AE2819952C0F7CE6DCDAC84CED9A3593813AFC9285D3B4A84A093A89E01F86F808
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L...k-.\.....!..... ....0.....@.....E..... .....h.....T.....text...E..... ....`.rsrc..... .....@..@....k-.\.....;...T...T.....k-.\.....d.....k-.\.....RSDSo.....j..f....B....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....k-.\.....(.....:...i.....N.....7...s.....+...M...r...../...'...V.....:...k.....X..... ...?...d.....".....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-timezone-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552
Entropy (8bit):	7.016631615696383
Encrypted:	false
SSDEEP:	192:rWIghWGwD744tk0icWU9F6MZVGl4ogvekMEbceC58uTkhp:rWPhWz/u2WuFRZk4VvDMCY59kX
MD5:	348CD4903DC8EF567FEC88B5F8B77F0E
SHA1:	8E880F38A6CDC36694DC757B53725BA643A17DE0
SHA-256:	0E1A391AE36D0D1F7E8C930A48AC8F6EA3350DF6CDA0E54E37FE6BB98D8D3BFE
SHA-512:	25F071AF12A04FE85EA158A460FBD2F3E19AEB191523142F78A3C02AA5B099373BF4FB86F2F6C892B259D607599BDAEBBDBCA278E2BD616750BD6A75B7DBDE45
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... .....!..... ....0.....".....@..... .....h.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....Y.x.....(...L...p.....5...s.....+...i.....U.....I.....api-ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-core-util-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552
Entropy (8bit):	6.82220257938724
Encrypted:	false
SSDEEP:	192:EnjW1hWJU744tk0icWU9F6MZVGl4ogvekMEbceC29A:EjW1hWS/u2WuFRZk4VvDMCY2K
MD5:	21EC3DB15B7A90E6072D04F9956BA31C
SHA1:	2FF9553CBE3827CCF5E8D8EFF0E0EDC09FCE0D16
SHA-256:	A926890895E5380809ACA6EAC88EEC1E8D90D827B6BA4BD17FEBEA9FDDC4AE69
SHA-512:	876E2B91365E1E6E48A41C046FCE89AAEF7453DD6C9A1C1FB84E8DF1B35E64EFA6B0CDCC2E69DB71AA231BE9F0CB3D154E18EA9B193F40A7EC28D6A78442CE30
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. .....!..... .....0.....;....@.....9..... .....h.....T.....text...)..... .....`.rsrc..... .....@..@.....8...T...T.....d.....RSDS..k...5...U.\|O5....api-ms-win-core-util-l1-1-0.pdb.....T....rdata. .T.....rdata$zzzdbg.....9....edata... ..`....rsrc$01....` .....rsrc$02.....J.....@...o.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.ke rnel32.Beep.DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-conio-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9576
Entropy (8bit):	6.82292361499687
Encrypted:	false
SSDEEP:	192:JWIghWGwx744tk0icWU9F6MZVGl4ogvekMEbceC9aJIaE:JWPhWF/u2WuFRZk4VvDMCY9a0
MD5:	28C9BEE76895EFCD300F752CD777FEA0
SHA1:	DDFEA66D097B70339E1D378C615AE06C093468AB
SHA-256:	D0FC3756D3B2A3E304991582EEABE30C7068C30D5B2E924FD0518ED86397D19E
SHA-512:	299AA4902CECCF650BAD00CC2F294C81B5A137439E3D9558AB008A6505CA217E5EB56BD27CFFFC6C28F87CAB0F6A4D250298245AF4EF2A327B2A76A2EFF0A4 F2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... .....0.....B=....@..... .....h.....T.....text..... .. `.rsrc..... .....@..@v.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-convert-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12648
Entropy (8bit):	6.511977985882006
Encrypted:	false
SSDEEP:	192:wpdkKBcydWIghWGwf744tk0icWU9F6MZVGl4ogvekMEbceCzo:0uydWPhWv/u2WuFRZk4VvDMCYzo
MD5:	674E89541C1CC113261C3BFE845ED41F
SHA1:	DB7E92E7AD166001658B4624B7B2817ADC97CCCD
SHA-256:	79C102CEDAF63CB7915CE88CDD0819267E759B97C20A62089B92AA1573CA1FC7
SHA-512:	78BEA075F23361FA5A22B75CF63C9AE54612EAFCDABBBAFD0357A238E5AB4358F20F38AA667E0401A0BCAF0A48E642698CB2B6334DDC10B3660C1DC88222E8 EC
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....A....@.....0.....h.....T.....text..... .... `.rsrc.....0.....@..@v.....NE.....:...d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1-0.pdb.....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....NE.....z...z...8... .....(...C...^...y.....1...N...k..... .....*...E...`...y.....5...R...o.....,...M...n.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-environment-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9064
Entropy (8bit):	6.779909769465169
Encrypted:	false
SSDEEP:	192:EWIghWGwV744tk0icWU9F6MZVGl4ogvekMEbceCS0dCm:EWPhWZ/u2WuFRZk4VvDMCYS0db
MD5:	9F1C384F335A302418710DBB8FF9195F
SHA1:	BED8F65BB984750C378505254A3A99EF9763C3E2
SHA-256:	C6594CD39B96390EB97860B8715E0B2248578C59938A2BD89A1BE118F564B312
SHA-512:	AEDC5A64152F7669C3602B5B543687263FAF7D56BE0FC8C7DD9D7E48917B6573AF4DF74B31D5F9FF7EF1515813DC0B1D04A76292994BFFA09ECA378195B402E 3
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....jU..... .....!..... ....0.....^C....@..... "..... .....h.....T..... .....text...2..... ....`.rsrc..... .....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N....R.s,"\....api-ms-win-crt-environment-l1-1-0. pdb.....d....rdata..d.....rdata$zzzdbg....."....edata... ..`....rsrc$01....` .....rsrc$02.....jU.....8.....C...d.....3...O...l..... ..... 5...Z...w.....)...F...a.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-filesystem-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10600
Entropy (8bit):	6.815260948052972
Encrypted:	false
SSDEEP:	192:F77q6nWlC0i5C1WIghWGwr744tk0icWU9F6MZVGl4ogvekMEbceCUkJTXJ:pq6nWm5C1WPhWL/u2WuFRZk4VvDMCYU4
MD5:	FD26D001F789C73280DB0B43EBE5B296
SHA1:	CF3B87A3CB94CD59D0E30CC62584A3240B410581
SHA-256:	26923E3E205E9E88587EBF1880D96CE55BD1090DB7FAA3BAB7A80C1D9C87E6CE
SHA-512:	6FD4846078D5D340017C9943FFEE94477097F4AE129F3D580678316881DDA55535927D259CC31BBD4C192DA03B97D8DC94519C81BF87FF9A1BA4935C88CC708
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....h.... .....!..... ....0.....n.....@..... ....h.....T..... .....text..... ....`.rsrc..... .....@..@v.....h.....=...d...d.....h.....d.....h.....RSDS.....a.'..G...A.....api-ms-win-crt-filesystem-l1-1-0.pdb..... ....d....rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....h.....A...A...8...<...@.....$...=...V...q.....)...M...q...../... O...o.....7...X...v.....6...U...r.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-heap-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9576
Entropy (8bit):	6.734341451717679
Encrypted:	false
SSDEEP:	192:bY3vY17aFBR4WIghWGwX744tk0icWU9F6MZVGl4ogvekMEbceCLDq/+kh:bY3e9WPhW//u2WuFRZk4VvDMCYLDS+S
MD5:	2D6AA88CD42D4CF28D20F8143874E6ED
SHA1:	F36B4CCB1A08AEB1B601022D3157C93E7B81C038
SHA-256:	AA14E72891F972DF15948A9CE975C392BF4964687778E032AC9ABBD519C8493F
SHA-512:	2D5A3FD637B46194FCC04608CC55A9A8DB44C8AA9BF84B34B8E155F0BCEED5209853CB573B548603D72F328E8285C9088F416C162ED83365F0D1EDF6F107E03
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....!..... ....0.....q.....@..... ....h.....T..... .....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....J.o ....6.....(.....c.....S.....1...V...y.....<...c..... .....U...z.....:...u.....&...E...p.....,..U...

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-locale-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9064
Entropy (8bit):	6.912452724430786
Encrypted:	false
SSDEEP:	192:cWIghWGwry744tk0icWU9F6MZVGl4ogvekMEbceCkPTRdm:cWPhW/m/u2WuFRZk4VvDMCYkPT6
MD5:	B171DED7253FE180A4B314E343E63697
SHA1:	190AEFF916C3A76501418077A0236CFBC4ADB039
SHA-256:	9652A74DDF2EB9F4E9A8EAE6A54FDD6282FADEE165D150AA182ADAD1BE1C6489
SHA-512:	5C426FF1F92B9BDC81C827CB25F78C75FA9ECA62B1A640EA1D8ECF9DDF42D70C9F2E203863D8A5F891A528E76427704997DDDE0E95F2A6CBB2C4847D992797 D4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... .....!..... ....0.....+....@..... .....e..... .....h.....T.....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$k....api-ms-win-crt-locale-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....e....edata... ..`....rsrc$01....` .....rsrc$02.....|..O.....8.....5...h.....E.....$...N...t.....$...D...b ...!...R..... ...s.....:...k.....9...X.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-math-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19304
Entropy (8bit):	6.1800293377315
Encrypted:	false
SSDEEP:	384:eOTEmbM4Oe5grykfIgTmLyWPhWT/u2WuFRZk4VvDMCYbC:uEMq5grxfInb12Tg4tDF
MD5:	34EC21AC35C664E6D5BCAE0B79767368
SHA1:	410FE5FDFA108DE013090F85EC86A5A9452BBDB3
SHA-256:	B9788E4060C80A1CE3AE845D3443A38B155A42E650AFF42AF98B2E93362EA5EB
SHA-512:	D6E29CA8DA1D70CD03F3B959C8EDB4ECE1ADD53B12D62E21CD8C4D86A2A6C03DBD2781F0B6E74FE1813DBBFEC58A7A546FDAC3A5A9B0A8A6EBF025A0F77 2A6A4
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....n.....@.....+.....@.....4..h.....T.....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,...api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-multibyte-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16744
Entropy (8bit):	6.171874624951984
Encrypted:	false
SSDEEP:	384:kXy+Kr6aLPmIHJI6/CpG3t2G3t4odXL5WPhWB/u2WuFRZk4VvDMCYRgMVCV3:kXZKrZPmIHJI64z2Tg4tDdB
MD5:	EEA50F530D1ED619D47A67B729581412
SHA1:	C73628A3DDED87F6C1DF6283EC2F5AD2D9FD54AF
SHA-256:	12EB7C4AC34E3BD0D0B0933A51AA08ECB3664EC05B5AC1BD1EFA7A89DECA07B4
SHA-512:	0EEA221B5F5A00FCE7AF7EF77CDAFCB73207D34C6831B84D7F8A84C2CB532E5E48890BC18186419658DBF6D79AE3EAE682ACB67C977536A10179B72AFBE3A0 43
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'..... .....!.....$.....@.....P.....@..... .....@.....*..h.....T.....text...."..... $ ....`.rsrc.....@.....&.....@..@v.....u'.....<...d...d.....u'.....d.....u'.....RSDS7.%..5..+...+.....api-ms-win-crt-multibyte-l1-1- 0.pdb.....d....rdata..d.....rdata$zzzdbg..... ...edata...@..`....rsrc$01....`@.....rsrc$02.....u'.....8...X...x...;..`.....1...T...w.....'. ..L...q.....B...e.....7...Z...}.....+...L...m.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-private-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	63336
Entropy (8bit):	5.455178439951802
Encrypted:	false
SSDEEP:	1536:J0DjXDe5c4bFE2Jy2cvxXWpD9d3334BkZnVPLXBuL:YjDe5c4bFE2Jy2cvxXWpD9d3334BkZn8
MD5:	E681A50108F93C915D3A7F06341E8E05
SHA1:	4145037385733133733D0ABBA1737DBBCE293F054
SHA-256:	5B698E14AE0FD5C1FB56125EF0E23F59C8C8A50565F75A67E541E67B9EA1826E
SHA-512:	B7805800A69B33CB40AE1965E39734B280E9FC9779496CF57261BB743B80BBB0F7D2F5261F568DF6AE30E98E6430ECF84C932BDF301A92A89698FE3B0F3A524D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3A..w e.w e.w e..De.v e..Da.u e..D..v e..Dg.v e.Richw e.PE..L. ..2.....!.....4;...@.....h.....T.....text..... ....`.rsrc.....@..@v.....2.....:...d...d.....2.....d.....2.....RSDSTrXT..{...b.....api-ms-win-crt-private-l1-1-0.pdb. .....d....rdata..d.....rdata$zzzdbg.....edata.....`....rsrc$01....`.....rsrc$02.....2.....>.....8...d#...5...>...?..-?..U?...?...?...?...@..L@...@...@...@ ..!A..RA...A...A...A...B..BB...B...B...C..>C..vC...C...C...C...D..>D..wD...D...E..[E...E...E...E..'F..]F...F...F...F..8G..kG...G..

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-process-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9576
Entropy (8bit):	6.7618528259191235
Encrypted:	false
SSDEEP:	192:YRQqjd7dWIghWGw6744tk0icWU9F6MZVGl4ogvekMEbceCJKbC:YKcWPhWi/u2WuFRZk4VvDMCYJyC
MD5:	6E9BEEADB1C3F03648829974CC884509
SHA1:	2E61B3EB58373CF904A8F7BCC049345A6E1AC9E6
SHA-256:	0E95DA4D92C0F2E59733FF5B3679DE5BCDB9824E9111608E4D6DD2312AD9B65A
SHA-512:	F325676631373ADBE1036F997A2DB3607FD17154A014CF5619523AE908F54C43DCD57FC265A555764ADB6ED508012EC8932E961359150C9CD7BF39539DAEEED
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...l.h..... .....!..... ....0.....@.....x..... .....h.....T.....text..... ....`.rsrc..... .....@..@v.....l.h.....:...d...d.....l.h.....d.....l.h.....RSDSZ\.qM..I....3.....api-ms-win-crt-process-l1-1-0.pdb.....d. ...rdata..d.....rdata$zzzdbg.....x....edata... ..`....rsrc$01....` .....rsrc$02.....l.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z..... .....!...<...V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-runtime-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13160
Entropy (8bit):	6.551362181960196
Encrypted:	false
SSDEEP:	192:70CjfhrpIhhf4AN5/jijWIghWGwA744tk0icWU9F6MZVGl4ogvekMEbceCt3/i:7b7hrKwWPhWc/u2WuFRZk4VvDMCYt3/i
MD5:	381BE5F54D942EA3A6C0F4BCA1C1E3F4
SHA1:	8E0005A94AA0BB0719859F3637C7225DA582A653
SHA-256:	9D938D92C42B5FAEA799659417E859473C64C45059283140A0117EC556830A60
SHA-512:	E44EDD2B1F0718ED7D5F0454D2B3298D9C2F938DB6607F8240416899A9F963F38A5955E34D2C065EAF1A66A5CB75337D54A47210F13B9CC8B50AF8322E255A2(
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....L..... .....!.....0.....@.....t....@.....0.....h.....T.....text..... ....`.rsrc.....0.....@..@v.....L.....:...d...d.....L.....d.....L.....RSDS6..>[d.=. ....C....api-ms-win-crt-runtime-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....L.....f.....k...k...8.....4...S...s.....E...g..... ...)...N...n.....&...E...f.....'...D...j.....>.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-stdio-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14696
Entropy (8bit):	6.442308517376209
Encrypted:	false
SSDEEP:	192:tPnLpHquWYFxEpahjWIghWGwN744tk0icWU9F6MZVGl4ogvekMEbceC6nhP/6j:FZpFVhjWPhWJ/u2WuFRZk4VvDMCY6nhw
MD5:	19B9EF6B90166C2A0FE5E5D18EFC2119
SHA1:	C2D714A1A16B81584CBB9011AF0A731266041EE5
SHA-256:	362B0783E622AFAA36403CF0EEFB9D3BA8C73AA3193D4D13075682FB778C35C2
SHA-512:	94E9D9A4618AA0328132278A92CED8500597DEC3958A37CC00610551A1B0F61BDBD641CD103962ADEDC7F2BAD5EDEBDB7D14653CB837DF79937F7333E99B4D 34
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....0.....@.....P....@.....a.....0.....".h.....T.....text...a..... ....`.rsrc.....0.....@..@v.....8...d...d.....d.....RSDS...iS#.hg.....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....^.....(..... .....<...y.....)...h..... ...].....H.....)...D...^...v..... .....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-string-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14696
Entropy (8bit):	6.413223558342021
Encrypted:	false
SSDEEP:	384:diFMx0C5yguNvZ5VQgx3SbwA7yMVIkFGlnWPhWi/u2WuFRZk4VvDMCYt8Po:d6S5yguNvZ5VQgx3SbwA71IkFvY2Tg4E
MD5:	8946CB2F22ADCDD09155C8EECE321037
SHA1:	6DB949F83FB9461063C018E857589BFF7BD75453
SHA-256:	38E0B9D51BB87378DBCE522EB7810B94E4DB463A88DDEA0D16C57B611848E60F
SHA-512:	90930BD6BCC8E34A519D9070EE6F7E34F533D640DA0EA39C5834928D32491059471E8FB7E841411B873A96483D6A687A50A1EA544836012C187D012786CA0491
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.... .....!.....0.....@.....@.....0.....".h.....T.....text..... ....`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....$[~f..5....api-ms-win-crt-string-l1-1-0.pdb... .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....S....8.....W...s.....#...B...a.....<... [...z.....;...[...{..... ...A...b.....<...X...r.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-time-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11112
Entropy (8bit):	6.672983574571931
Encrypted:	false
SSDEEP:	192:8QSWb6VJDyWIghWGwn744tk0icWU9F6MZVGl4ogvekMEbceCNEgM:8QSWWVgWPhWP/u2WuFRZk4VvDMCYNQ
MD5:	ED4919904759439B646E1E03AF262EAC
SHA1:	C90BA976D78F866908AF778FFC7AE25FF9425C75
SHA-256:	51110EC0761B641E75F1E29C24B3689DA363C10C28ED2FC81852DD94165A4376
SHA-512:	7848183288E7BB0309D74241E595D4D90E9300DF95ADBEA6B183F1C15A3D5EC8020B750B5B90B142A704A3E49CC56445CE38562942D0BA3737EE478CD5E7BED 8
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... .....!..... ....0.....+....@..... .....h.....T.....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb..... ..d....rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....OI.....H...H...(...H...h... ...=...\...z.....8...V...s.....&...D...a...~..... .....?...b.....!...F...k.....0...N...k.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-crt-utility-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	9064
Entropy (8bit):	6.898154682787428
Encrypted:	false
SSDEEP:	192:cfHQdu3WIghWGwl2744tk0icWU9F6MZVGl4ogvekMEbceC1PNH4Z:cfBWPhW5q/u2WuFRZk4VvDMCY1PR4Z
MD5:	1F2DD1CC0E87A404590DACC38218161D
SHA1:	D16E2DB04E7EDF80FEEA8A12BEFB43C9ABB2146D
SHA-256:	986D7F0685F2D74CB4F698F17824AF2AF8A7E68AAE64489E5CC12A1D806E8979
SHA-512:	3970E007E7528FF6354F07C73EC69F865FCE781AEE9D3FF3C0430C3D9B22D4DF1EC00A3C14A9DB0C1A7C7416ABADBED1808CED72E0D667D8C96B03EB5C5B7 BE5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!5..... .....!..... ....0.....@.....^..... .....h.....T.....text...n..... ....`.rsrc..... .....@..@v.....!5.....:...d...d.....!5.....d.....!5.....RSDS.....k.....api-ms-win-crt-utility-l1-1-0.pdb.....d. ...rdata..d.....rdata$zzzdbg.....^....edata... ..`....rsrc$01....` .....rsrc$02.....!5.....d.....8.....(.....#...<...U...l.....+...@...[...r..... .....4...I..._.....3...N...e...|.....

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-downlevel-kernel32-l2-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11624
Entropy (8bit):	6.629669041618242
Encrypted:	false
SSDEEP:	192:LEnLL1CbqHCJFY4bmWphWDH744tk0icWU9F6MZVGl4ogvekMEbceCU4:LEL8qHCJkWphWP/u2WuFRZk4VvDMCYU4
MD5:	D907B13A13DB8B6F58EB4716171D0A3E
SHA1:	3372265606E2902274D20AE4BA6A8FAF1233E938
SHA-256:	04540FC89D6C3EA557D6DC52A9EE39903EEF24C00CAD93382312A8AD40673EEC
SHA-512:	E1CA900C97DFE5AF8236A5FCF85D9B50A265C0E29353BF58D77F45AC3B9DCC71A49787A073A13546499E4047A099BFA03B864F6824CF5D5098FFCA44C33EFD B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....be..be..be...e..be...a..be.....be...g..be.Rich.be.PE..L.....A..... .....!..... ....0.....>....@.....p..... .....h.....T.....text...x..... ....`.rsrc..... .....@..@.....A.....A...T...T.....A.....x.....A.....$.....RSDS..I1./'....NM.....api-ms-win-downlevel-kernel32-l2-1-0.pdb..... .T....rdata..T.....rdata$zzzdbg...4...<....text$mn....p.....edata... ..`....rsrc$01....` .....rsrc$02.... .....I1./'....NM....Z..n/6A.t...A.3....3....3....3..3....3..(.3....3.. .....3....3..... ....A.....R.....y...y.....|...`...4...4...9...9...>...C...4...>...>...>...F...K...P...U...P...4...Z...>...>...]...

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-eventing-provider-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	8552
Entropy (8bit):	6.985297852249055
Encrypted:	false
SSDEEP:	192:S/k+sF1SGs/nWphWDR744tk0icWU9F6MZVGl4ogvekMEbceC5v/:SM++CWphWd/u2WuFRZk4VvDMCY5v/
MD5:	E7D33C7B62DB5C9605354A83A12CD40E
SHA1:	23A67338E62A48D68DC98D8104478284996BEBDC
SHA-256:	50041495891624CFE7237AF6BA7F4A4DFC3AEE665F7295362DBE45AEBCBBA546
SHA-512:	109053C7E8188FBD2AD5E12DBBF3CFB26400C4E2AC5454FD240456B85765824A82F8A20AABD88FF08D507E8177379D7E65D87B90B88BF786074FE012E1A1A24
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....be..be..be...e..be...a..be.....be...g..be.Rich.be.PE..L...px..... .....!..... ....0.....c.....@..... ...\..... .....h.....T.....text...\|..... ....`.rsrc..... .....@..@....px.....@...T...T.....px.....d.....px.....$.....RSDS.V....].S&....\j....API-MS-Win-Eventing-Provider-L1-1-0.pdb.....T. ...rdata..T.....rdata$zzzdbg... ...\....edata... ..`....rsrc$01....` .....rsrc$02.... ....V....].S&....\j.T..k.s.5...px.....px.....H...p.....C...o.....3...`..... ..a....."...M.....api-ms-win-eventing-provider-l1-1-0.dll.EventActivityIdContr

C:\Users\user\AppData\Local\IdeaShareKey\api-ms-win-security-base-l1-1-0.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	14184
Entropy (8bit):	6.614988974610919
Encrypted:	false
SSDEEP:	384:PgegRaB87W74EsL10c5VG5xWphW9/u2WuFRZk4VvDMCYmhI:PgeMa4W74Es5FGuD2Tg4tDxI
MD5:	B779CF7DE36CE3403C2DB3ECDDA04AD9
SHA1:	A22A15F074ECF866FE506D7409D2F7E52235CDA2
SHA-256:	1279A054A4379822A00C01E3F73E8C2D49C56BC281BF0D4E41755F509847AB70
SHA-512:	B2D8C09A0B30F1178694F6CC74C169646D0810264851453A8B603DD426DB539FB7C2200E20EC95EDCD0009059FF4EAF2A8AA32B77ED9771B4C70944CE8061E0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....be..be..be...e..be...a..be.....be...g..be.Rich.be.PE..L..... .....!.....0.....@.....@..... ....`.rsrc.....0.....@..@.....<...T...T.....d.....$.....RSDS.Jn...`.....api-ms-win-security-base-l1-1-0.pdb.....T....rdata..T.... ....rdata$zzzdbg... ...I....edata...0..`....rsrc$01....`0.....rsrc$02.... ....Jn...`.....<....*,.....a...a...H.....P...B...q.....&...}.....)...\.....3...\...~..... .....>...o.....M.....1...t..... ...R...x...../...V...w.....

C:\Users\user\AppData\Local\IdeaShareKey\concrt140.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	233320
Entropy (8bit):	6.639971066679949
Encrypted:	false
SSDEEP:	6144:uVtg4bkcTc3uYSw5ejegvGw9xEPOL8an39bkH1r12z/WK398:uI4xL+wsQ8anK1Azrq
MD5:	C1C5248B307B81997DDB3DE51A033FCA
SHA1:	7F015DB75334C0593AD4AEECE466C5492994D7B0
SHA-256:	E608C7BE5C061E053CAD7B695D50990982FDB0EFB53460262DFF0D6520398323
SHA-512:	F2BBA261A23890EBA4FA636415F513202BDE2135F91F857B35655B7813FEDBAE9F436FE6571A7F470A66721E906B2BC878EBBB10458085B78B6AAB79FBC7AF6B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...]..,.],.,B.I,.],.%.,.]..,.],.,z..-.],.z..-.],.z..-.],.z..-.],.z..-.],.z.}, .],.z..-.],.Rich.],.....PE..L.....U.....!.....p.....0..... .....@A.....K..0R.....p.....x..h.....)...'..8.....((..@ .....P..,.....text...L..... ..`.data..... ...,.....@....idata..`....P.....8.....@..@.rsrc.....p.....J.....@..@.reloc...).....*...N..... .....@..B.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	763472
Entropy (8bit):	6.488661421415057
Encrypted:	false
SSDEEP:	12288:bg0t134n44iXmBllcSc9a0qu95z40HE3cGex:bg0t134n4vslIcScU0dFkN0
MD5:	633CAA1C300A2801DF64CC8E0C78FA42
SHA1:	69E04EAC22EF1B51C297D90FAE38E14A6F4AE6E6
SHA-256:	1A22302646545AC053431BC0609068CB9ACF90DEA82D7495C037F29F92B12BD3
SHA-512:	942E9A37F15938295F0022D3169DBF4A07359618CDF22C559289A8828A66195DB56316BCC73036D8AEAD4B454DF6FB296DAA2D1D1FAF29BB7D494940533198A/
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... K..d*..d*..d*..mR*.p*...L..l*..6B..o*..6B..h*..6B..s*..6B..b*...C..g*.. d*..Y+...C..Z*...C..e*...CF.e*...C..e*..Richd*.....PE..L....._a.....!.....j.....".....@.....5.....|.... .....v..P0...0.....0...T... .....(.....@.....<.....text...gi.....j..... ..`.rdata...u.....v...n.....@..@.data.....@....rsrc..... .....@. .@.reloc.....0.....@..B.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144232
Entropy (8bit):	6.539247038216602
Encrypted:	false
SSDEEP:	3072:MmaQASh0NdONoQOxTcdmz3QCAalrN3qnKs31pD4AlR3AqXDzePXsE03:jASh0NdO3CA6Z3qKw12AlR3AqXG903
MD5:	DAA2CF898745C0A54AEACAA009F80CB5
SHA1:	F8E8C9A8396532ABCA2C7006001B76C41BD67E8A
SHA-256:	C190B37B14959861D71089D796AB30B6832B41F2202C5A38BD9AD596128025DC
SHA-512:	D215FF830EB8CA733BA08B7B53E25A7480CE3C6C86A259EB8E42977BEAF7F70B19B94173F6EEC0094CD14624D02119BA4F6D95D9F8BC3DB4F0EAB474133E4B27
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....rIf.!If.!If.!].. Kf.!@.j!If.!If.!.b.!].. Nf.!].. Bf.!].. Hf.!].. Yf.!].. Yf.!]..!Hf.!]..! Hf.!].. Hf.!RichIf.!.....PE..L...W.RS.....!.....F.....`.....@A.....q.....0.....h....@..$...0[..T..... ....8...@.....text..... ..`.data.....@....idata..b.....@..@.mrdata.<.....@..@.rsrc.....0.... .....@..@.reloc..$....@.....@..B..... .....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1506152
Entropy (8bit):	6.561928277157185
Encrypted:	false
SSDEEP:	24576:rmRJbFmBRDhOQnPR20KEpbhnO0At4lukzUdyqkvOz/D4/2Up+gM0OtA3+CpIc2Io:CdF1QnPU0Ke/M7+2kjGttCpHGyr3Fcac
MD5:	558CDAEDB9A620804713A012BAB53925
SHA1:	8D711E9A2BDB8F782E1D5BD788F07877A05C976B
SHA-256:	28C1A16629F4BED8C9CB49C1903D6631B0B904757CE82333F5A149765B8A088A
SHA-512:	90F3FAE26640E0EF284E57B5D375E2A8C7966C63936312DDC8670BF1E8CB373DB887AF5CE16EFD5116B9A56B0EC0E2E93E27EDE3B8E8283127BDE2EFE0724EA9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3.t.`.t.`.t.`[..a.t.`[..a.t.`...a.t.`...`.t.`.t.`.p.`...a.t.`...a.t.`...a.t.`...a.t.`..q` .t.`...a.t.`..s`.t.`...a.t.`Rich.t.`.....PE..L.....~.....!.....*.....\.....@.....-.....@A.....".....4..X.....H.....h.....f..T..... .....@.....0.....!..`.....text....-..... ..`.data.....@...x...2.....@....idata..l....0... .....@..@.didat.....P.....@....mrdata.\....`..... .....@..@.rsrc...H.....@..@.reloc.....@..B..... .....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	84560
Entropy (8bit):	6.756069673594986
Encrypted:	false
SSDEEP:	1536:2fYVoVbSXVp6cfP4M6LxvsTlnNf3frk3z5Q88MNiCjKjVBT:2DVmpcRsGBkDaSNFjKjVp
MD5:	24625FE7D79F640B268929328CB3715D
SHA1:	92212AD81710C1FA663668B771A74C1C6A3998FF
SHA-256:	643629F241EE37BDC885AA7B601C652ABEA9E5FC66432C2B56BBD38BADC64C3B
SHA-512:	55038FBC382CDD148A2D2C313D1E03BF5EE4D46C97B9974E101EA1A566F94B92FFA1079385EA5A177FB1DDA31978B6AF14860D5A6E8C7E42A0AFFA39EF42C62C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h.,...,...,...%.a.>...~...(...~... ...~...4...~...*.....*...../.....9..... &.....*.....-.....-.....-...Rich,.....PE..L...._a.....!.....r.....P.....@.....L...<...,....0.....P0...@..... p..... .....@.....text..... ..`.rdata..>W.....X.....@..@.data..... .....@....rsrc.....0..... ..@..@.reloc.....@.....@..B..... .....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	116304
Entropy (8bit):	6.677438670861377
Encrypted:	false
SSDEEP:	1536:sLgeURS91XzZBGtkzo7oQVtbRfL84mg8H0O4J6C8o7STmrjrVBO:svn/cj84mg8+R7STmrjrVE
MD5:	B866257E2D5AC2B1AF5AAC737FFF3BDF
SHA1:	BB78BF3DEC6BCB47EAF11FDC61F29C3B932611FA
SHA-256:	63AC2564C376298FD3A5852BF85962A9DF20CB8D1EEBA786A77CA613696161F8
SHA-512:	4EBE9CCC98C3CCF6681FD2AF1327F5796A68875BA1DE9FDFC8DDE9A8F2B8317E24F8F371232C66EC67F190F40A436D8298505B5A19EEE9E827A9FEAF744E9A22
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o.....S...S...S.v)S...S.f.R...S.f.R...S.f.R...S.f.R...S.n.R...S/g.R...S/g.R...S...SA..S/g.R...S/g.R...S/gES...S/g.R...SRich...S.....PE..L...!._a.....!.....i....@.....`....M..(e.....P0.....p.....`...@.....text..... ..`.rdata.....@..@.data...t.....t.....@....rsrc.....~.....@..@.reloc.....@..B.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	118352
Entropy (8bit):	6.652855823872858
Encrypted:	false
SSDEEP:	1536:/1/6e0/vlJao/YUy4KBxL1eyGsu1yg2dXUbVi1IZ5/5Xn8E1U1eD+fWcgm/VBN:Y2lxLIL1idXdar/5XE1eMWcH/Vr
MD5:	86902F7D1B0A075961FAF817E5A1F323
SHA1:	7C89796A026657F3F88CACEB34D840ADD7BD2941
SHA-256:	35D2AF9060C9440359995E542AEECB97F20D5EEC3AF1627E0BA0AD33AAEAF82E
SHA-512:	D2F89710C44832E41FFCFD2C47138105812C5B4A17A108793FC0D86DA428BB8156C9CDDEA53C70431473EB071EA475B736C1F8DCC63FE1725763597889A67BD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`6...e...e...e..e...e...d...e...d...e...d...e...d...e...d...eH..d...eE..d...e...e...eE..d...eE..d...eE..e...eE...d...eRich...e.....PE..L... ._a.....!.....Z.....j....@.....J.....a.....P0.....P....".T.....".....X"..@.....text..... ..`.rdata..V.....@..@.data.....|.....@....rsrc.....@..@.reloc..P.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\fr_config.ini

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	Generic INItialization configuration [CONFIGPATH]
Category:	dropped
Size (bytes):	3670
Entropy (8bit):	6.120070866180341
Encrypted:	false
SSDEEP:	96:/HrPqr0lHrerb7Po9KOgR7vipdG+fGplNQ0CftHA72e:WA2fydffGpDVitg7n
MD5:	62CCCFC9B665A7349615B3BE5A985383
SHA1:	19459D13B355A39B80D7C3A2F249C696FB14E25C
SHA-256:	F7BC365261E75E964F376DFD5B8C5CEF2AF59E45C94B2179B135622048A55193
SHA-512:	B08A6DD5785C90B7BF1E8BDEDDE31F9FBE9EF7AC9ECBCEA642CCCF4512E09ECDFA3735272DF633E7FB40B4FCEAAE3D54F568DF6FB6F685C807FEE6BECCD7F613
Malicious:	false
Preview:	..;----------.....Section----------..[LOGPATH]..; .....; .... FR.EXE .....; .....%windir%.....+.....; .....path = MyTest\..; .....%windir%\Zapotec.log..path=fr_exception\fr_fun.log..path=fr_exception\fr_trace.log..path=log\..; .....[CONFIGPATH]..; .... FR.EXE .....; .....%windir%.....+.....; .....%userprofile%..%windir%....; .....%windir%\XDICT.INI....; .....path = MyTest\..;path=%windir%\win.ini..; .....;----------.....Section----------..; ....Section.....0.....1.....;----------

C:\Users\user\AppData\Local\IdeaShareKey\fr_lang.ini

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	12142
Entropy (8bit):	6.107666131324222
Encrypted:	false
SSDEEP:	192:g4XYpRWgUw+gaNgCVb/8vXGBTjexxPi5r8iY5lwQ6la5aWMYdj9PjeiU9ICLn:GpRWgU3b/vrYOQ6MaWdj9P6iU9IT
MD5:	6D8FB45D8B1E43FA53CEE2EEDECCFB05
SHA1:	FB163C949A73B646D3785E6C815C1AF6779A159E
SHA-256:	8E0C60E4991482F7EB53DD19F07D8CFF725354E2E9DCCC62B4D02D8F56A4B8D1
SHA-512:	E1E0B5E74162E42E7EA835E78D80CDEFF9811511D887D0119C8A90B29EA4D317CA684197505F54E4645D49C9CEF6FCDBC908E26A6AE21497495F7A1B46C3557A
Malicious:	false

Preview:	[zh_CN]..; Audio.....IDS_AUDIO_ADAPTER_OPEN=.....IDS_AUDIO_ADAPTER_CLOSE=.....IDS_AUDIO_DEVICE_INFO=/********** ..... ********** ********/..IDS_AUDIO_DEVICE_NAME=.....:..IDS_AUDIO_DEVICE_MANUFACTURER=.....:..IDS_AUDIO_DRIVER_VERSION = ...:..IDS_AUDIO_DEVICE_SITUATION=.....:..IDS_AUDIO_VOLUM=.....:..IDS_AUDIO_VOLUM_ZERO=.....:..IDS_YES=....IDS_NO=....IDS_AUDIO_MICROPHONE_VOLUM=.....:..IDS_AUDIO_MICROPHONE_VOLUM_ZERO=.....:....; Network.....IDS_NETWORK_TCP_PORT_ZERO=.....TCP.....IDS_NETWORK_UDP_PORT_ZERO=.....UDP.....IDS_NETWORK_PROTOCAL_TYPE=.....IDS_NETWORK_LOCAL_ADDR=.....IDS_NETWORK_REMOT_ADDR=.....IDS_NETWORK_PORT_STATUS=.....IDS_NETWORK_INFORMATION=/********** ..... **********/..IDS_NETWORK_INTERFACE_DESC=.....:..IDS_NETWORK_MAC_ADDR=MAC ...:..IDS_NETWORK_DNS_NAME=DNS.....:

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	380496
Entropy (8bit):	6.273969763669411
Encrypted:	false
SSDEEP:	6144:cbEYPX45mcXvAm72tcCtYlzEbzNS/gBlOtDodcNay+j7F:8BQYcfAm72tcCtYm8/g7ceZ
MD5:	B421A76547807ACC79ED2C2615791BDD
SHA1:	822E285C02D5A4AE60A09D40D382DA5236A192CE
SHA-256:	E600A65EEB937576E37F5849299E64C4D5A96C10583544C9898423D944FB8569
SHA-512:	20F0132FA4A9BA295D2E5D4105BA70B1982F10E408AD98E00A0599F0ACE2E94C0B8AC447C0C3C2589F0AD46DD97FCCFD40D40AFB24684E56C4C4720365F304E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&..H...H...H.-....H.....H.....H..d%...H.....H..d3...H...I..H.....H.....H.....H.....H.Rich..H.....PE..L...w.[.....!.....}H.....Y....@...../..S...H.....P.. =.....P0.....@.. .....@.....L.....text...I..... ..`.rdata..S_.....`.....@..@.data.....0.....@....rsrc... =...P...>.....@..@.reloc...D.....F...X.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\h265EncDll.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1782352
Entropy (8bit):	6.5353249142156855
Encrypted:	false
SSDEEP:	49152:E6+a83O6BDUpEeMTB4aX8cfZMPaJxV6bD9ibaTHpzHvxwuY8DGPKDEed384YN7aJ:4Lcauiyqu0+9lwHu
MD5:	A2499C31A3CE2201F93E5FE20135C4BA
SHA1:	9B4F1504DE1ED84EA23E8D8D6F80BD0FB1FA5586
SHA-256:	C4F5D764C44095F9AEE5B92C156B9F50DF788635259B00ADE026507F14503514
SHA-512:	CFFDB8898306B14DE0F9A509DD77F5CA59E890A5F54FA9D3C2CA0CE22BCB965EC38B97BF1C53BAE4676AFB1A20CEACFBB36E273B069743CB65FC2AC574A8EE25
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|..8..Q8..Q8..Q1.TQ2..Q...P:..Q...P2..Q...P3..Q...P3..Q...P;..Q8..Q}..Q8..Q/..Q...P...Q...P9..Q..8Q9..Q...P9..QRich8..Q.....PE..L....O.]..... .....!....P.....m^.....p.....@.....P..... .....P0...0..`i.....p.....p...@.....p.....rodata..... ..`.text..... ..`.rdata..~)...p...*...T.....@..@.data...pa.....~.....@..._RDATA.....@..@.rsrc..... .....@..@.reloc..`i...0...j.....@..B.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	649808
Entropy (8bit):	6.687571741025146
Encrypted:	false
SSDEEP:	6144:gqZS7KSZyKhuJn88RXENedMEZbMbJsTdlVcBE8/ShewrGFXJNPo9Y4FJlk1Xjs45:g5/juWNy2rVYLFOk1Xw47r+4qOQZvQX
MD5:	4DD63FC0B8C7E122AE6F8B21490BD92B
SHA1:	0EFCA41C7F87AD201F147DCD26459198A3C8B233
SHA-256:	DD097AF4B9A33B3B4E8C8A4EBC25CF344A62CCBDB55AA7C4999AF0ACB840D61A
SHA-512:	112AB5C40375D87F4C84003303C8BB894AF3F8E5F7DEC3640F274634DF63D8890748310E112845CDB725862C4DAB8F9FE05633B99CF1E9EFBBB7F1C8D000362
Malicious:	false

Preview:	MZ.....@.....@.....!..L.!This program cannot be run in DOS mode....$.....R7&.3Yu.3Yu.3Yu.K.u.3Yu.U^t.3Yu.[Xt.3Yua..u.3Yu.[\t.3Yu.[]t.3Yu.[Zt.3YuhZQt.3YuhmXt.3YueZXt.3YuhZXt.3Yu.UXt.3Yu.3Xu.1YuhZ]t.3YuhZ\t.3YuhZYt.3YuhZ.u.3YuhZ[t.3YuRich.3Yu.....PE..L.....a.....!.....$.....<.....r....@.....>..H'..He..D....@.....P0...P..... x..T.....y.....xx..@.....text.....`.rdata..j.....@..@.data....b.....L.....@....rsrc.....@.....@..@.reloc.....P.....@..B.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	479312
Entropy (8bit):	5.755790119297246
Encrypted:	false
SSDEEP:	6144:k27h53VAW4c4FhGw8l6HkbcpetYZPFvUGj7spG/H:9hNVAW4hMaazqGP
MD5:	6FDF57E2FE8CE3DA29B172A51F97A79E
SHA1:	4E565830C405DE1418EF8D3B31C59252AF9680C6
SHA-256:	BD7472BF1666750F9313200933E38134A1AC5B89FEAC91DB9E595D03751B4B27
SHA-512:	706C88C1B83182E115ABCADA60765545D53FF615B1CF26CE52626A837914084B2705055D186F685B2E595083427A135FF792D3E35FAAAAEF553B9FE5DC8B670C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1.t.Ps'.Ps'.Ps'.(.'.Ps'.8p&.Ps'.8w&.Ps'.8v&.Ps'.8r&.Ps'.;r&.Ps'"9r&.Ps'/9r&.Ps'.Pr'.Qs'/9v&.Ps'/9s&.Ps'/9.'.Ps'/9q&.Ps'Rich.Ps'.....PE..L...D._a.....!.....R.....#.....J<....@.....P...~...T..... ..<..... ..P0...0...F...e..8.....j.....f..@.....T.....text..... ..`.rdata...:.....<.....@..@.data...Lr...0...`.....@....idata...E.....F...~.....@..@.tls.....@....00cfg.....@..@.rsrc...<.... .....@..@.reloc...O...0...P.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\language.txt

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:MWWn:MWWn
MD5:	E17184BCB70DCF3942C54E0B537FFC6D
SHA1:	E0F05ED4FD4FFB1AF17B55948173BFE2900CEFB4
SHA-256:	F8B7291025863577C250B562E8AA0D7A70387BC67029915CD5C2DFDA40A9E055
SHA-512:	7CDF804C2F5BCA9F9A2E44408B5FC1EF7CCBEF9D8B929AA38958B0E3673B8AD1C5EC3F8600EA81003C54071E1316FF13C091A6D1D05B7C121C72B01E2DAF8869
Malicious:	false
Preview:	1033

C:\Users\user\AppData\Local\IdeaShareKey\libcrypto-1_1.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2118736
Entropy (8bit):	6.163592861974243
Encrypted:	false
SSDEEP:	49152:O9ZoCGzGFxHGwvtWU89su1CPwDv3uFh+qi+:IZ/9mAWU8l1CPwDv3uFh+2
MD5:	BAD35B9E18ADEB8E7ACEE0B2F7884F9A
SHA1:	1879856BA7F3B2F7342E94DFFC292255E5BD9EDD
SHA-256:	DCEC8FDCF2DE254BB77D3704CCE25B9571618AD9E274B34CB4E293815ED51CA3
SHA-512:	4591E1626DA0E4D117F43A4AB0769BE5ED03D335D3D6DB2DBEA67CBFECECC6FC7A6BE3F3B3E6A720D999C2B9B817012610FBBA1B04FF7761F0DBEC05F9FD662D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a.#j%.M9%.M9%.M9,..91.M9..L8'.M9..N8/.M9..H8/.M9..I8..M9.H.9..M9%.L9..M9..I8Z.M9..M8$.M9..9$.M9..O8$.M9Rich%.M9.....PE..L...}.E`.....!.....h..... .....@!...@.....hg...u..T.....|.....$ .P0.....`...8.....@.....p.....text..... ..`.rdata..H.....@..@.data....Y.....@....idata..J....p.....@..@.gfids..%.....,.....@..@.00cfg.....@..@.rsrc...|.....0.....@..@.reloc.....8.....@..B.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	686440
Entropy (8bit):	6.381411525632177
Encrypted:	false
SSDEEP:	12288:vGrf/vB5Xp3OmO7wXbU3Z+W0CF1MV+Qt+BR+:vWvBzzO7wSEQUr4B8
MD5:	BFA6205254C112F6F3389FD1F697119D
SHA1:	86FCAFA2C100297298FC3DC3AB04CC898B4D2C1F
SHA-256:	E582B9FF37724709AC198B6CAEDF8AEF835C2E2FCCBE75EFC2196C014FC5A9FC
SHA-512:	9DB55BE85E643A421804220DC24ADB525DCECA146CB04C3B20A9A9820EB14C94595A6D103D374AA8ABDF5ED4B8A5403662628291349C86BDA224B4D27CA829 4B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p.+..sx..sx..sx.i.x..sxOqry..sxOqpy..sxOqvy..sxOqwy..sx..x..s xgpry..sx..rx..sxgp{y..sxgpsy..sxgp.x..sxgpqy..sxRich..sx.....PE..L....%%\.....!.....|.....@.....i...6.....@.....b.. h....P..8T...f.....f..@.....text..... ..`.rdata.....@..@.data.....v.....@....rsrc.....@..... .....@..@.reloc..8T...P...V.....@..B..... .....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	31080
Entropy (8bit):	6.522300868283526
Encrypted:	false
SSDEEP:	768:r+NncKII7m+L9pcMfxzJgV+hDXMtLmYHaGe0Os2Tg4tDgU9:SNpOcFBm0
MD5:	FFF865474DE0E8CDBA1F951A8EE28789
SHA1:	57853D2CAF1EC578F4D832A7CC395B2CA0EDE2F6
SHA-256:	C289468DB334C8772D7B6EBF379964B26357712DB487E202927BA0604FFC898D
SHA-512:	039E6FB42029D82790D582EFC7A683060435A37BE0119B36FD188BB37D39F5A166841F887723324F9E4A301A60899DE46983D7610233BA771A8C0478DBEEB503
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i..:..:..:..:..:..r..;..:r..;..:r..;..:r..;..:r..;..:<d.:..:..:...:Z..;..:Z..;..:Z..:...:Z..;..: Rich..:.....PE..L....%%\.....!....8...(.....=.....P.....K.....@.....V..d....c.....b..h.....0S..... .PS..@.....P.....text...#7.....8..... ..`.rdata.....P.....<.....@..@.data.....p.....Z.....@....rsrc.....\.....@..@.reloc..... ^.....@..B..... .....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	885096
Entropy (8bit):	6.497572549746118
Encrypted:	false
SSDEEP:	12288:pqKHhbgTEO93++OEzbb7Lwk0rotwCud4FZADxj1oGbXBMi/XJ5bF7eSdRh9V7nfN:R1Zc+KbAkERoGBnfXPHSDrWkGOQGlrkD
MD5:	E1C5D9A4A651291FA30684A7ADD22579
SHA1:	945AB0106B22A36A7ABE1647CE4F3F7F05795F34
SHA-256:	F291C7BC848ADB4A30CE990D9539A41D845E45421AA709F01CEF63B898FAF209
SHA-512:	B828C23CF47D3BACC6E2093735033DA7A0C4F3C628A7798C8BF4EB175D93383F1A29BA5010A72446311D5361A34A5C256F07A691CA93EC323531509F80A6593F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....SZ._24._24._24.VJ..Y24..R5.]24..R7.]24..R1.U24..R0.T24.....]2 4..S5.X24._25..24..S0..24..S4.^24..S.^24..S6.^24.Rich_24.....PE..L....%%\.....!.....r.....8....@.....H.....j.. h.... ..(x..P.....p...@.....text..... ..`.rdata.....@..@.data...t>.....<.....@....rsrc..... .....@..@.reloc..(x... ...z.....@..B..... .....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Category:	dropped
Size (bytes):	704872
Entropy (8bit):	6.47289040454708
Encrypted:	false
SSDEEP:	12288:EVxeUqzjoyrJ4y2YVuq7sn98U4JNCikALSUXdyWqSRAVgBsVEXXcUyoa6U:EndwBJ/2YVKn90zX5e5QcUCL
MD5:	8DE46DDC209F8965A085AD2AF78DD559
SHA1:	ED4F5FC7AD5D5B25BD03B2A8854F5B028A7F5C08
SHA-256:	217EFF2DF882B76239BDD12C3AB69044AEF884186348F206F53719092CD929D8
SHA-512:	1BC7DC2E14C6C0E234451BB5F265F48B06C153AA520D9591AE7F6280BEA1B9A523FFD6553DA95DBE961C3440E14E26671152E2AA78F49001BEEA918A5B9DB13 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*...D...D...D.....D..E...D."5....D..G...D..A...D..@...D.m.E...D...E. ..D.m.@..D.m.D...D.m.....D.m.F...D.Rich..D.....PE..L....h.\.....!.....H...x.....8P.....`.....L....@.....0s...2..... ...h.....`Z...o.....p..@.....`.....text....F.....H..... ..`.rdata..\`...`...b...L.....@..@.data.....@....gfids..... .....J.....@..@.rsrc.....L.....@..@.reloc..`Z.....\...N.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\libssl-1_1.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	506960
Entropy (8bit):	5.818853596983871
Encrypted:	false
SSDEEP:	12288:8jt6zvCJGO1phi2h6wbAbWWz5rruaqeol2JeL0xU2lvzZe9P:8ja2snjqhixU2lvzZe9P
MD5:	E3F5AC6D77CCAD6AA833A9E94A839EDE
SHA1:	CCB4B8AAB190D47F3BBE3621B6ABE503BB3021E0
SHA-256:	79A162A034010A7A473F988EC051F4AF7399920C43130D27DBE7DCEFB51CB1CA
SHA-512:	3111C76721E59881A96C42067BC577B48146D2A42B730706A35409DEEA03D35AACC6A05E8291AFCB8E3540182B272AFA243C4FC412B3D7835F964134F71155D6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0...c...c...c..1c...c..b...cS.ic...c..b...c..b...c..b...c..b...c...cl..c..b...c ..b...c..]c...c..b...cRich...c.....PE..L.....E`.....!....`.....p.....@.....N...*.....s.....P0.....3...z..8..... .....z..@..... .....text...o_.....`..... ..`.rdata...f...p...h...d.....@..@.data....;.....6.....@....idata..3A... ...B.....@.. @.gfids..%....p.....D.....@..@.00cfg.....F.....@..@.rsrc...s.....H.....@..@.reloc...:.....<...P.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\log_config.ini

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	356
Entropy (8bit):	3.468942392814782
Encrypted:	false
SSDEEP:	6:QrFS8UdP8l9m4ml9xWMAhAAl9PTQ2l9t9il9vmSdP8l9PsfHDNrA2TQ11lgrA2Tw:Qgv09mh9QMAhv9Pn9tg9vld89PsPhrmb
MD5:	68B28B4DE497B213619D7854E89E9497
SHA1:	CCAFDC0515A83C0E27B216712BD05AF6E8F4A6AC
SHA-256:	1BC5B7EC18DBB36933B12F1AD86D97F49E19DF468C561091253AB3DFB86D5FA8
SHA-512:	A88281D1BBBD90E1CB95FC0998AB2364AE12BC90633C6725B3F2863BFE727E1DB5BA47938914C84C08E20806479874953BAE94DDB703A34520B7FA0A498FF73 C
Malicious:	false
Preview:	..;..e._.~+R....;.A.L.E.R.T. . .=. .1.0.0.,.....;.C.R.I.T. . . .=. .2.0.0.,.....;.E.R.R.O.R. . .=. .3.0.0.,. .....;.W.A.R.N. . . .=. .4.0.0.,.....;.N.O.T.I.C.E. .=. .5.0.0.,.....;.I.N.F.O. . . .=. .6. 0.0.,.....;.D.E.B.U.G. . .=. .7.0.0.,.....;.N.O.T.S.E.T. .=. .8.0.0.....[.S.e.r.v.i.c.e.]...l.o.g.l.e.v.e.l.=.6.0.0...[.G.U.I.]...l.o.g.l.e.v.e.l.=.6.0.0...

C:\Users\user\AppData\Local\IdeaShareKey\mfc110.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4411240
Entropy (8bit):	7.065642613116238
Encrypted:	false
SSDEEP:	98304:311W/N/BknZf4OJX9t+NaeR2dURRUyFLOAkGkzdnEVomFHKnP+g9:3ucyFLOyomFHKnPh

MD5:	DFE37438750449245F558144974EDE06
SHA1:	CFFAF042F43E96923B5FA4EFB88DAAB8E83393E9
SHA-256:	9C43F3F4156B90BAE1597A6A249B4EDEB629482F910038FD2172125BC1745AAF
SHA-512:	D8382D86A919BF57D4CE185330ACA5804E882785F8567F961E5AD054A92F72592EF0026A90DDE113DA320B2E1192CAE696E990619A15F157787C960CBBDF7DC
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uv..1..1..1...`w.0...`u.3...`t.9...`v.<.....3.....;.....<.....?..1..1...`s.".. .....0.....0.....0..Rich1.....PE..L.....Q....."!.....6)..T.....$.....P).....C.....|C...@.....@g(.[....P*.....*.....8C.h....P@.h..... .....@.....|^*.....X(.....text....5).....6)..... ..`.data.....P).....:).....@....idata..~Q...P*..R....).....@..@.rsrc.....*.....2*.....@.. @.reloc...I...P@..n....?.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\mfc110u.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4446568
Entropy (8bit):	7.070043206175241
Encrypted:	false
SSDEEP:	98304:Dra1QTpsfQ//4/IzLPQ6EOmh0U+0d7fFLOAkGkzdnEVomFHKnPQg+P:D50j+0hFLOyomFHKnPQg+P
MD5:	BD56515BE170D64B880F2DF6D4CEF453
SHA1:	A505B7AE8E788C9C4821995E1BE80642F7E3C422
SHA-256:	986BB4ABBA3F7CBE3439D1332572AC8FAA17B2F3EEDF7B7C50023137382CC7EA
SHA-512:	FA86D19A220C52D62108FDB9E902FC6B1B26305F982529C36E9DFA91C575A46B9C95A1CFAFFC88AC464EC257B03F4DDEEA63D9D253EA7D5C38E43170F01513 5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uv..1...1...1....`t.0....`v.3....`w.9....`u.<.....3.....;.....<.....?...1. .....`p."..... .....0.....0.....0...Rich1.....PE..L...(..Q....."!.....).....@.....).....C.....\_D...@.....X.*.....@+.....C.h.....@.....d. ).8.....@.....*.X.....).....text.....).....)..... ..`.data.....*.....).....@....idata...O....*..P....*.....@....rsrc.....@+.....".+..... ....@..@.reloc.....@.....@.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\mfc140.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4746600
Entropy (8bit):	7.054863961502151
Encrypted:	false
SSDEEP:	98304:+0BSmTN0O3xKBHfR2NJU0Fri7YZ2FLOAkGkzdnEVomFHKnPzkT:dlA5RaU0Fri7YZ2FLOyomFHKnPzkT
MD5:	670E529FE7DA60D01F3A8800A280C6A6
SHA1:	5FAF707A8F36CBF3A76E5EFECA521C753A0AA180
SHA-256:	0B81C2C57A18E56DF5CCB1EEA07E62C13152816B495F2AA7AEFEC037FA195C4C
SHA-512:	19A213369A875BDE35919A09FD3783EB6F0FE819F6F6A81A8F2B5FF16ACB3E2FC6D1D36EC3104CC035E0D464D3728EA764B8F1391198383ADD4DB0476EFF894 6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c..c..c..4...c..4.y.c..4.x.c.....c.....c.....c.....c.....c..4.c.c..c..g.... ...b.....c....s.c.....c..Rich.c.....PE..L.....0].....\"!.....6...X.....0.*.....P.....H.....I.H...@A.....Pc-.....=/...../.....VH.h....@E.....@ @..8.....@4..@.....0/.....T-.....text...C5.....6..... ..`.data.....P.....:.....@....idata..vT...0/..V.....@..@.didat...../.....2/..... .....@....rsrc...../.....6/.....@..@.reloc.....@E.....D.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\mfc140u.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5041512
Entropy (8bit):	6.868096553287344
Encrypted:	false
SSDEEP:	98304:H4iE2PQUbOxTla877f2EYmPCHLy1ZqLEFwaBS5z6IFLOAkGkzdnEVomFHKnPv1aI:YF2oUyxo8nxCHLLE7BS5zfFLOyomFHKX
MD5:	C88EE0ACFC089ED05A822361A8DF55EA

SHA1:	A83E311015EB8D0CB28A3B82B01B4A3E0FBAFAA7
SHA-256:	CC83D44EE23F5F44429A2B523DF6505432F6AE79A3233ADEBE234A3FB7B1BB8A
SHA-512:	43F06AE3B0008115A92F6271B21F2BC69900771B6DDAFC8A8DD76CB70494C0D8A6002F9314841701253526F793D99AA7011B3188305D9A8349CA6EC23D809F22
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c..c..c..<.w.c..<.q.c..<.p.c.....c.....c.....c.....c.....c.....c..<.k.c..c..{`... ....b.....c....{.c.....c..Rich.c.....PE..L.....0]....."!....z2..^.....d..... M.....M...@A.....L...|.3.....3.....L.h.....I.....2.8..... ....ha..@.....3.x...Xz2.....text...tx2.....z2..... ..`.data...@.....2.....~2.....@....idata...S....3..T...Z3.....@..@.didat.....3.....3.....@....rsrc... .....3.....3.....@..@.reloc.....I.....JI.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\mfcm140.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	82280
Entropy (8bit):	6.3353023306928895
Encrypted:	false
SSDEEP:	1536:ZJLMNkxLIY4XSeko0OIvoNXb5zLxK9nhhsZG5n0S9MhAb7IBN:ZJXLl5Se+kNXb5zLxK9nhhss0qMm7IX
MD5:	E9B833A49608F17E628DA7916EDE6A3C
SHA1:	58F67085899A3032A5CC3C4EE066E270E0EDACEA
SHA-256:	4DAD4B14FED7DB1F5652E8C7448AA5128987FAD3AEFC8333FEDAB2F650FCF3EB
SHA-512:	782A12AA0CF07F82B959808E6412B24B50B5D6A4A1B15A4FDBF1FA99F4F2173F8F88A8C00490161046EA5E72C9F8B4E5F164EE0689992D0C46257988725B9B68
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q..E.....o.....e.....G.....G.....G.....e.....o.....G. ..6...G.....G.....G.....Rich.....PE..L.....0]......"!....B.....RP.....`.....p.....k....@.....,.....@-.....P.....*..h....`..8... .e..8..... e..@.....`..$.....c..H.....text....@.....B..... ..`.rdata..r....`.....F.....@..@.data...\....@.....@....rsrc.....P..... ..... .....@..@.reloc..8....`.....$.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\mfcm140u.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	82280
Entropy (8bit):	6.336819654689569
Encrypted:	false
SSDEEP:	1536:ZIHM1IsY9Y4XSmbhvoteMhf8G3DTzLxK9nhhsZGQv4gE+ubh3Bna:ZIOY95SmVQtekr3DTzLxK9nhhsf4gE3q
MD5:	6294658E01A8CDB666C25F944F3AB309
SHA1:	EF0E6EDEDE7701678070D1482D34DABBED562B3D
SHA-256:	BAE2E69AACE99768E160A5EFD5438C13CC2F751BAEB34A5E8DCF5917D77B33C4
SHA-512:	16FE56645A49FF63F59DAA58BFA3C9EBA28D746144A0D20100090F19576AC96B0AA9EBF704534568B011CD9F3238E8103E2CA4616E7F912A797DEA03E51E8B91
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q..E.....o.....e.....G.....G.....G.....e.....o.....G. ..6...G.....G.....G.....Rich.....PE..L.....0]......"!....B.....RP.....`.....p.....'6....@.....,.....@-.....P.....*..h....`..8... .e..8..... e..@.....`..$.....c..H.....text....@.....B..... ..`.rdata..r....`.....F.....@..@.data...\....@.....@....rsrc.....P..... ..... .....@..@.reloc..8....`.....$.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\msvcp110.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	525160
Entropy (8bit):	6.028639794493234
Encrypted:	false
SSDEEP:	12288:7qULlc5nb9rywgfyhUgiW6QR7t5sA3Ooc8sHkC2eRxU/:1LHnhryLfBA3Ooc8sHkC2eRxU/
MD5:	C05390EDA8A91A5620B690C87CD38C51
SHA1:	F9F4B60E5E7322E5AC4AC1ED494619B7ACDF9780
SHA-256:	9E6040347E946DCDC4C514B7DC54DA71D8EF3F2068F50FC743BC84937B879CF2

SHA-512:	0709EC82D06C26CFBA68DC3B607E1E7F5634DEF55CB744663C602B811FE32585905C875DBAF29ECE600498BCF3D5602EA9A8637622BD0BE270BE65CE075310
F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7.>.....:.L....:.J....:.H.....:.I.....:.T...:.M....:.N....:.K. ...Rich.....PE..L.....P......"!.....0.....P.....@.....`N..$.....<.....h.....D.....K..@.....D. .....text..... ..`.data....`...0...2.....@....idata.....N.....@..@.rsrc.....j.....@..@.reloc...}.....~...n.....@..B.... .....

C:\Users\user\AppData\Local\IdeaShareKey\msvcp140.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	429416
Entropy (8bit):	6.615729295233097
Encrypted:	false
SSDEEP:	12288:iAoA7hbarg71r4RzfxjJhUgiW6QR7t5s03Ooc8dHkC2esq0JY:iAoAN3r0Bm03Ooc8dHkC2eT0JY
MD5:	195BB153285AC6C01A8EA97046E9C741
SHA1:	E672E7E33FE94D07B14E203C468E634FE21CC7FC
SHA-256:	02BB7B7482F186E4AB29BB3482FC64DF1CFD77BF2113A4230912A2439FCFFF76
SHA-512:	E8797B9A202C8C80EB1FE49DC12D251DE18E2DF874E45EBA3B5E1589C86D610E2E1ACAB76F1BED959FBB858D3EE62A2715E903B90EB40D4BFBED2C17CAA1
B395
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U.C.4...4...4..t.I..4...L...4..Lm...4...4...4..Lm...4..Lm...4..Lm...4.. Lm...4..Lm...4..Lm}..4..Lm...4..Rich.4.....PE..L.....U....."!..... ....F.....@A.....A.....R.....v..h.....:. .0g..8.....)..@.....P.....P>..@.....text..."..... ..`.data....'... .....@....idata..2....P.....@..@.didat..4....p.....4..... .....@....rsrc.....6.....@..@.reloc...:.....<...:.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\msvcr100.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	770408
Entropy (8bit):	6.909293518342905
Encrypted:	false
SSDEEP:	12288:nQmCy3NeRjkpQmj3oaMtQqjoygfXq3kon9IlbgaOxQdVJJ6j5EBKX8hP:QmCy3VQs9MtLjTgfa3kon9FaOdEh
MD5:	003953639FF3E89D449CD3ACA162D977
SHA1:	DF17A51E5C676532AF6A8C2A18447232F0507D01
SHA-256:	6FAD45A23BE054A89F95203D1A61BCE1B191F386CDA8E4A7477B8ED0AC211D6C
SHA-512:	E46D39073C32315C425908842568C3B9D6116C36DADBB5CDBA07251FC77999B59F85920D9ED059D7B50129166F062A31F8DFD6CB307819F1E49BA7D531151E5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... R.HA<.HA<.HA<.A9..KA<.HA=..A<.'7..@<.'7...A<.'7..|A<.'7...A< .'7..IA<.'7..IA<.'7..IA<.RichHA<.....PE..L.....K....."!..... ....x.....@.....I.....D...(.....h..... L..h...8..... .....pE..@.....text..... ..`.data...|Z... ...N.....@....rsrc.....X.....@..@.reloc.. L.....N...\.....@..B..... .....

C:\Users\user\AppData\Local\IdeaShareKey\msvcr110.dll

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	865640
Entropy (8bit):	6.907564550247982
Encrypted:	false
SSDEEP:	12288:FmCyHcMpK7QdgD+9Tr8r3FmJciMgLFWkA8qTWu+FVlofpJCjNdr12iqwZeQ:FmCyHNlQdTryVmCiplkqTWu+FN
MD5:	AA55CAC7DEA173F3588A5C1A45FA34E3
SHA1:	2AE69D1B660E4C6E10C0E9EC7D56B58D6894EB23
SHA-256:	F03CCC107E4D9CF9B6BFD34CF53B1FE6686FF4C7ADC283377CB878C8A6191611

SHA-512:	B0C4D3CECDABF8ECF8EE5D6E89C0F5D58089C96AC4B3358B8B5405A022816AD46403E0FCEF2381C67027DBB430A0827AD5BC72828B97F19C9663C88E025E42F9
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x._'<.1t<.1t<.1t<.0t..1t...t?.1t.+.t..1t.+.t].1t.+.t..1t.+.t..1t.+.t=.1t .+.t=.1t.+.t=.1tRich<.1t.....PE..L.....P......"!....`.....<.....@.....`.....@.....`.....(.....h.....S..0n..8.....0...@.....text....^.....`..... ..`.data....\...p...N...d.....@....idata.....@....rsrc.....@..@.reloc...S.....T.....@..B.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.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:	32D64143CEE92FE6CAB366493DDFFB034EA71DF2B7CE584238DEB56E54886083676A50C6FBF28E871F926081E8C8AFD72B7FEB8EF24C50E16A4C034939D5433E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	107600
Entropy (8bit):	6.714402999473523
Encrypted:	false
SSDEEP:	1536:TfpY458f9IIbr1DIutsJxvOm2fo5AtqN52UgB3ATF3pkbueRKEtgVBJ:rpYM8f9XPSDxvmQ52UI3cfgKcgV3
MD5:	D60080362C25CC73DC5D260D2DA61F4F
SHA1:	F4F50A38C2E038F6FBA9109E99CEE19C98981187
SHA-256:	06ABAD066B4CADD68827FDC4CADE48DEED161C8F9EEC5BA870B2E1AAF927B1B9
SHA-512:	B42031F7937702A239F3BEBD4462F62F35F39918FE7DAFC84ED2D06BFF34B6A12DB352E3C50D8B6C938EF8F2B27180D4E996AB19E871A8DC13ED06C3FB938199
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.)B..G...G...G.....G.B.F...G.B.B...G.B.C...G.B.D...G.u.F... G...F...G...F...G...F.@.G...C...G...G...G.....G...E...G.Rich..G.....PE..L....`8a.....!.....&...j.....q&.....@.....@.....a.....(o. .....t..P0.....P]..T.....]..@.....@..d.....text...8$.....&..... ..`.rdata..T8...@...:...*.....@..@.data....!.....d..... ...@....rsrc.....f.....@..@.reloc.....h.....@..B.....

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

Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	160336
Entropy (8bit):	6.692815830319358
Encrypted:	false
SSDEEP:	3072:JBufNHLZ8pmgFUEBkZNWUV9Ynb2N/ktIUxs3aO0Pjy6VK:7+j8HyEBkXWUV9YnypkKNR2K
MD5:	0E8DF991E24520405B0CF1266B3128B7
SHA1:	75EF94E3B5B2C0F4617090B4AB3689081B8109DD
SHA-256:	0DA66721A1DD63F12A8DC8DE833DAB54C767610F3D86D99441875168229 30AC3
SHA-512:	728669D250E503F1C88776F50E4D7DF9BC4AD926C2E90A1CCCA0494C126FD1D5E3F8DD82B53D2A685C207C8AE313CF7C182A0198FDAF3DA26CFF121D91B1D37

Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I."...LS..LS..LS.Z.S..LS.Z.Sq.LS.Z.S..LS6.OR..LS6.IR..LS6.HR..LS...S..LS..MS[.LS..DR*.LS..LR..LS...S..LS...S..LS..NR..LSRich..LS.....PE..L....N.\.....!.....m....@.....".."..$...4%..(....`.....B..P0...p..H...p...p.....@.....text..... ..`.rdata..2k.....I.....@..@.data.....0.....@..gfids.....P.....&.....@..@.rsrc.....`.....(.....@..@.reloc..H....p.....@..B.....

C:\Users\user\AppData\Local\IdeaShareKey\tup_air_client.dll	
Process:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	468560
Entropy (8bit):	6.76603570394093
Encrypted:	false
SSDEEP:	6144:/uAv9WWpduh5Xwp4TSSOm1vOMghyOqbaJ989nLgMB041048OyaJxDBzW:GQ9m5XhZ1rbsYgMB041jHq
MD5:	6BA9EB5A513291388F0901F50F1EED8C
SHA1:	1438DA149C7F4827674E3A31B03AF66095C129B3
SHA-256:	4CCD623C590554573DE6C5B06F7019ABEA8DE0795FEEE80145ADB6702532225E
SHA-512:	8B127A019AE8BE066E0A49DE8819CFDC475F1ABAF381A6E609A49A54578BC780962A40A144BCD456C62CB9F617B895FA8ACAA322EA6849932577385ABC39816C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k.,/.BP/.BP/.BP..AQ*.BP..FQ#.BP..CQ+.BP..GQ6.BP&..P?.BP..CQ;.BP..CQ,.BP/.CPc.BP..GQ5.BP..BQ..BP...P..BP..@Q..BPRich/.BP.....PE..L...b.Qa.....!.....x.....H.....T.....@.....L.....S.....P0... ...w.....T.....d.....@.....text...z..... ..`.rdata.....@..@.data....j.....f.....@....gfids..H.....x.....@..@.tls.....z.....@....rsrc.....|.....@..@.reloc...w... ...x...~.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.999876539921463
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:	IdeaShareKeyInstaller.exe
File size:	23716040
MD5:	c7dfff14e887613a25cec2e1ee87f5a9
SHA1:	5dc3cbf93f7981ab7198e6769749f021cd01c062
SHA256:	d08117db56fe4550a2c35a3ab3140a515e2a2e9ebbfc2ab8b89d2ab12e0a5786
SHA512:	f7f4b01e111247240bd8a36108ebdd0a0ba02398ee444de62e121ac9ef32217edded348e5747d6d2d46b27eae8c85e9d42a2d8d3709d65361cdf8d920ec69983
SSDEEP:	393216:4k/9WC05CN0YZqFhXeeYc7R/ASRObUdUzdXVQkdnhN1rmL2Q4Lbcq81xxrsT69z:J/9WJ5CN1iBej+tUUdAfQkBhzmL2/blw
TLSH:	C73733C589FD80A9DA29817082E014F2E68E3D341D07EB1CB135FA15563B6BA7DB4B8D
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:	0109999d9d0d8901

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
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 00007F230865D550h
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

Instruction
push 0046BDC0h
call 00007F230865D232h
call dword ptr [004090B0h]
push eax
mov edi, 004C40A0h
push edi
call 00007F230865D220h
push ebx
call dword ptr [00409158h]
cmp word ptr [004C40A0h], 0022h
mov dword ptr [00473DD8h], eax
mov eax, edi
jne 00007F230865AB2Ah
push 00000022h
pop esi
mov eax, 004C40A2h
push esi
push eax
call 00007F230865CEF8h
push eax
call dword ptr [00409270h]
mov esi, eax
mov dword ptr [esp+20h], esi
jmp 00007F230865ABB1h
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
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x101000	0x4bb0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x169b078	0x3050	
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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	0x8d000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x101000	0x4bb0	0x4c00	False	0.2041529605263158	data	3.382324314575568	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1011d8	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_DIALOG	0x105400	0x100	data	English	United States
RT_DIALOG	0x105500	0x11c	data	English	United States
RT_DIALOG	0x105620	0x60	data	English	United States
RT_GROUP_ICON	0x105680	0x14	data	English	United States
RT_VERSION	0x105698	0x238	data		
RT_MANIFEST	0x1058d0	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
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

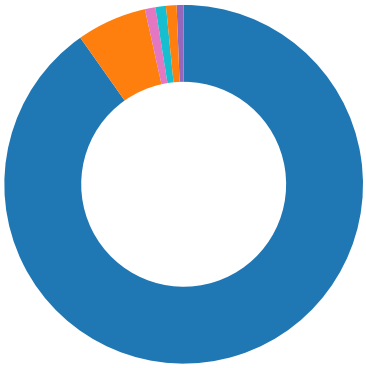
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- IdeaShareKeyInstaller.exe
- taskkill.exe
- conhost.exe
- taskkill.exe
- conhost.exe
- taskkill.exe
- conhost.exe
- taskkill.exe
- conhost.exe
- taskkill.exe
- conhost.exe
- IdeaShareService.exe
- schtasks.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- IdeaShareService.exe
- IdeaShareService.exe
- dllhost.exe
- IdeaShareService.exe
- IdeaShareService.exe
- IdeaShareService.exe

Click to jump to process

System Behavior

Analysis Process: IdeaShareKeyInstaller.exe PID: **6132**, Parent PID: **3452**

General

Target ID:	0
Start time:	13:04:14
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\IdeaShareKeyInstaller.exe
Imagebase:	0x400000
File size:	23716040 bytes
MD5 hash:	C7DFFF14E887613A25CEC2E1EE87F5A9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	success or wait	1	4028FB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\IdeaShareKey	success or wait	1	4028FB	RegCreateKeyExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\IdeaShareKey\IdeaShareKey	success or wait	1	4028FB	RegCreateKeyExW
HKEY_CURRENT_USER\Software\IdeaShareKey	success or wait	1	4028FB	RegCreateKeyExW
HKEY_CURRENT_USER\Software\IdeaShareKey\IdeaShareKey	success or wait	1	4028FB	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareKey.exe	unicode	RUNASUSER HIGHDPIAWARE	success or wait	1	4029D7	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\IdeaShareKey\IdeaShareKey	Installer Language	unicode	1033	success or wait	1	4029D7	RegSetValueExW
HKEY_CURRENT_USER\Software\IdeaShareKey\IdeaShareKey	Installer Language	unicode	1033	success or wait	1	4029D7	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	IdeaShareKey	unicode	"C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service	success or wait	1	4029D7	RegSetValueExW

Analysis Process: taskkill.exe PID: **1836**, Parent PID: **6132**

General

Target ID:	1
Start time:	13:04:15
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	"taskkill" /F /T /IM FaultReport.exe
Imagebase:	0xb60000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **912**, Parent PID: **1836**

General

Target ID:	2
Start time:	13:04:15
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: **6900**, Parent PID: **6132**

General

Target ID:	3
Start time:	13:04:15
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	"taskkill" /F /T /IM IdeaShareKey.exe
Imagebase:	0xb60000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6904**, Parent PID: **6900**

General

Target ID:	4
Start time:	13:04:15
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: **5976**, Parent PID: **6132**

General

Target ID:	5
Start time:	13:04:38
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\taskkill.exe

Wow64 process (32bit):	true
Commandline:	taskkill" /F /IM IdeaShareService.exe /FI "STATUS eq running
Imagebase:	0xb60000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 1768, Parent PID: 5976

General

Target ID:	6
Start time:	13:04:38
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: 5788, Parent PID: 6132

General

Target ID:	7
Start time:	13:04:38
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	"taskkill" /F /T /IM FaultReport.exe
Imagebase:	0x7ff745070000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4404, Parent PID: 5788

General	
Target ID:	8
Start time:	13:04:38
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: **1844**, Parent PID: **6132**

General	
Target ID:	9
Start time:	13:04:39
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	"taskkill" /F /T /IM IdeaShareKey.exe
Imagebase:	0xb60000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5816**, Parent PID: **1844**

General	
Target ID:	10
Start time:	13:04:39
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: IdeaShareService.exe PID: **5840**, Parent PID: **6132**

General

Target ID:	11
Start time:	13:04:40
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe
Imagebase:	0x11c0000
File size:	467304 bytes
MD5 hash:	4C43F81A16703A0539A95CCCB064585F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	11C8778	CreateDirectoryW
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CA1909F	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	0	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	2	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 34 00 30 00 3a 00 32 00 31 00 31 00 5d 00 49 00 6e 00 66 00 6f 00 3a 00	[2023- 5-26]-[13: 4:40:211]Info:	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	66	134	2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 49 00 64 00 65 00 61 00 53 00 68 00 61 00 72 00 65 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 53 00 74 00 61 00 72 00 74 00 21 00 21 00 21 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 0d 00 0a 00	**********IdeaShareService Start!!!**********	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	200	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	202	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 34 00 30 00 3a 00 32 00 35 00 38 00 5d 00 49 00 6e 00 66 00 6f 00 3a 00	[2023- 5-26]-[13: 4:40:258]Info:	success or wait	1	6C80AC2A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	266	134	2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 44 00 69 00 61 00 6c 00 6f 00 67 00 20 00 49 00 6e 00 69 00 74 00 20 00 53 00 74 00 61 00 72 00 74 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 0d 00 0a 00	************************Dialog Init Start************************	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	400	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	402	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 34 00 30 00 3a 00 32 00 35 00 38 00 5d 00 49 00 6e 00 66 00 6f 00 3a 00	[2023- 5-26]-[13: 4:40:258]Info:	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	466	54	43 00 68 00 65 00 63 00 6b 00 20 00 49 00 64 00 65 00 61 00 53 00 68 00 61 00 72 00 65 00 4b 00 65 00 79 00 20 00 44 00 65 00 76 00 69 00 63 00 65 00 0d 00 0a 00	Check IdeaShareKey Device	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	720	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	722	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 34 00 35 00 3a 00 36 00 31 00 37 00 5d 00 57 00 61 00 72 00 6e 00 3a 00	[2023- 5-26]-[13: 4:45:617]Warn:	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	786	48	6e 00 6f 00 74 00 20 00 47 00 65 00 74 00 20 00 4c 00 6f 00 67 00 69 00 63 00 61 00 6c 00 20 00 44 00 72 00 69 00 76 00 65 00 73 00 0d 00 0a 00	not Get Logical Drives	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	834	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	836	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 34 00 35 00 3a 00 36 00 31 00 37 00 5d 00 49 00 6e 00 66 00 6f 00 3a 00	[2023- 5-26]-[13: 4:45:617]Info:	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	900	36	4e 00 6f 00 74 00 20 00 66 00 6f 00 75 00 6e 00 64 00 20 00 44 00 65 00 76 00 69 00 63 00 65 00 0d 00 0a 00	Not found Device	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	936	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	938	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 34 00 35 00 3a 00 36 00 31 00 37 00 5d 00 49 00 6e 00 66 00 6f 00 3a 00	[2023- 5-26]-[13: 4:45:617]Info:	success or wait	1	6C80AC2A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	1002	132	2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 44 00 69 00 61 00 6c 00 6f 00 67 00 20 00 49 00 6e 00 69 00 74 00 20 00 46 00 69 00 6e 00 69 00 73 00 68 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 0d 00 0a 00	***********************Dialog Init Finish***********************	success or wait	1	6C80AC2A	WriteFile

Analysis Process: schtasks.exe PID: **5528**, Parent PID: **6132**

General

Target ID:	12
Start time:	13:04:40
Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /delete /tn /f
Imagebase:	0xa90000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1840**, Parent PID: **5528**

General

Target ID:	13
Start time:	13:04:40
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6912**, Parent PID: **6132**

General

Target ID:	14
Start time:	13:04:40

Start date:	26/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /xml C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.xml /tn IdeaShareServiceAt20230526130440
Imagebase:	0xa90000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.xml	unknown	2	success or wait	1	A9AB22	ReadFile
C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.xml	unknown	2752	success or wait	1	A9AB73	ReadFile

Analysis Process: conhost.exe PID: **5324**, Parent PID: **6912**

General

Target ID:	15
Start time:	13:04:41
Start date:	26/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: IdeaShareService.exe PID: **1836**, Parent PID: **1080**

General

Target ID:	18
Start time:	13:04:42
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe C:\Windows\system32\config\systemprofile\AppData\Local\IdeaShareKey\IdeaShareService.exe
Imagebase:	0x11c0000
File size:	467304 bytes
MD5 hash:	4C43F81A16703A0539A95CCCB064585F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	520	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	522	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 34 00 32 00 3a 00 39 00 34 00 30 00 5d 00 49 00 6e 00 66 00 6f 00 3a 00	[2023- 5-26]-[13: 4:42:940]Info:	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	586	134	2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 49 00 64 00 65 00 61 00 53 00 68 00 61 00 72 00 65 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 53 00 74 00 61 00 72 00 74 00 21 00 21 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 0d 00 0a 00	**********IdeaShareService Start!!!**********	success or wait	1	6C80AC2A	WriteFile

Analysis Process: IdeaShareService.exe PID: **2348**, Parent PID: **3452**

General	
Target ID:	19
Start time:	13:04:48
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service
Imagebase:	0x11c0000
File size:	467304 bytes
MD5 hash:	4C43F81A16703A0539A95CCCB064585F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: dllhost.exe PID: **5788**, Parent PID: **800**

General	
Target ID:	21
Start time:	13:04:50
Start date:	26/05/2023
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
Imagebase:	0x7ff769260000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: IdeaShareService.exe PID: **3968**, Parent PID: **3452**

General	
Target ID:	24
Start time:	13:04:50
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service
Imagebase:	0x11c0000
File size:	467304 bytes
MD5 hash:	4C43F81A16703A0539A95CCCB064585F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	1134	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	1136	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 35 00 30 00 3a 00 38 00 33 00 37 00 5d 00 49 00 6e 00 66 00 6f 00 3a 00	[2023- 5-26]-[13: 4:50:837]Info:	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	1200	134	2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 49 00 64 00 65 00 61 00 53 00 68 00 61 00 72 00 65 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 53 00 74 00 61 00 72 00 74 00 21 00 21 00 21 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 0d 00 0a 00	**********IdeaShareService Start!!!**********	success or wait	1	6C80AC2A	WriteFile

Analysis Process: IdeaShareService.exe PID: **5744**, Parent PID: **3452**

General	
Target ID:	25
Start time:	13:04:57
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service
Imagebase:	0x11c0000
File size:	467304 bytes
MD5 hash:	4C43F81A16703A0539A95CCCB064585F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: IdeaShareService.exe PID: **2488**, Parent PID: **3452**

General	
Target ID:	29
Start time:	13:04:58
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\IdeaShareKey\IdeaShareService.exe" service
Imagebase:	0x11c0000
File size:	467304 bytes
MD5 hash:	4C43F81A16703A0539A95CCCB064585F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	1334	2	fd fd		success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	1336	64	5b 00 32 00 30 00 32 00 33 00 2d 00 20 00 35 00 2d 00 32 00 36 00 5d 00 2d 00 5b 00 31 00 33 00 3a 00 20 00 34 00 3a 00 35 00 39 00 3a 00 20 00 34 00 39 00 5d 00 49 00 6e 00 66 00 6f 00 3a 00	[2023- 5-26]-[13: 4:59: 49]Info:	success or wait	1	6C80AC2A	WriteFile
C:\Users\user\AppData\Local\IdeaShareKey\Log\IdeaShareService.log	1400	134	2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 49 00 64 00 65 00 61 00 53 00 68 00 61 00 72 00 65 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 53 00 74 00 61 00 72 00 74 00 21 00 21 00 21 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 2a 00 0d 00 0a 00	********************IdeaShareService Start!!!********************	success or wait	1	6C80AC2A	WriteFile

Disassembly

No disassembly