ID: 651268
Sample Name: RKKO3T4hSU
Cookbook: default.jbs
Time: 18:20:04
Date: 23/06/2022
Version: 35.0.0 Citrine

Table of Contents

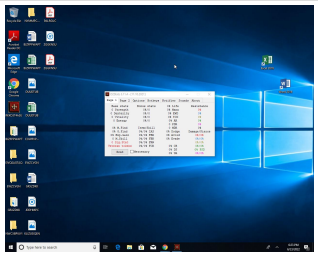
Windows Analysis Report

RKKO3T4hSU

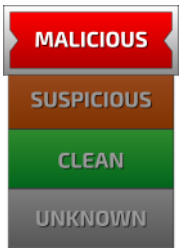
Overview

General Information

Sample Name:	RKKO3T4hSU (renamed file extension from none to exe)
Analysis ID:	651268
MD5:	df9025d622d4ac..
SHA1:	ff97781df2915d2..
SHA256:	22b2655f8d9880..
Infos:	



Detection

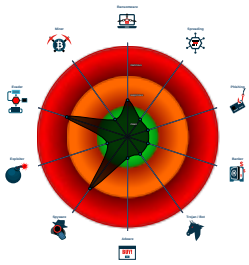


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Installs a global keyboard hook
- Binary is likely a compiled AutoIt sc…
- Uses 32bit PE files
- Found a high number of Window / U…
- Installs a raw input device (often for…
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to check if a d…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Found evasive API chain (date chec…

Classification



Process Tree

- **System is w10x64**
- RKKO3T4hSU.exe (PID: 824 cmdline: "C:\Users\user\Desktop\RKKO3T4hSU.exe" MD5: DF9025D622D4AC7B41641491C26DC146)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

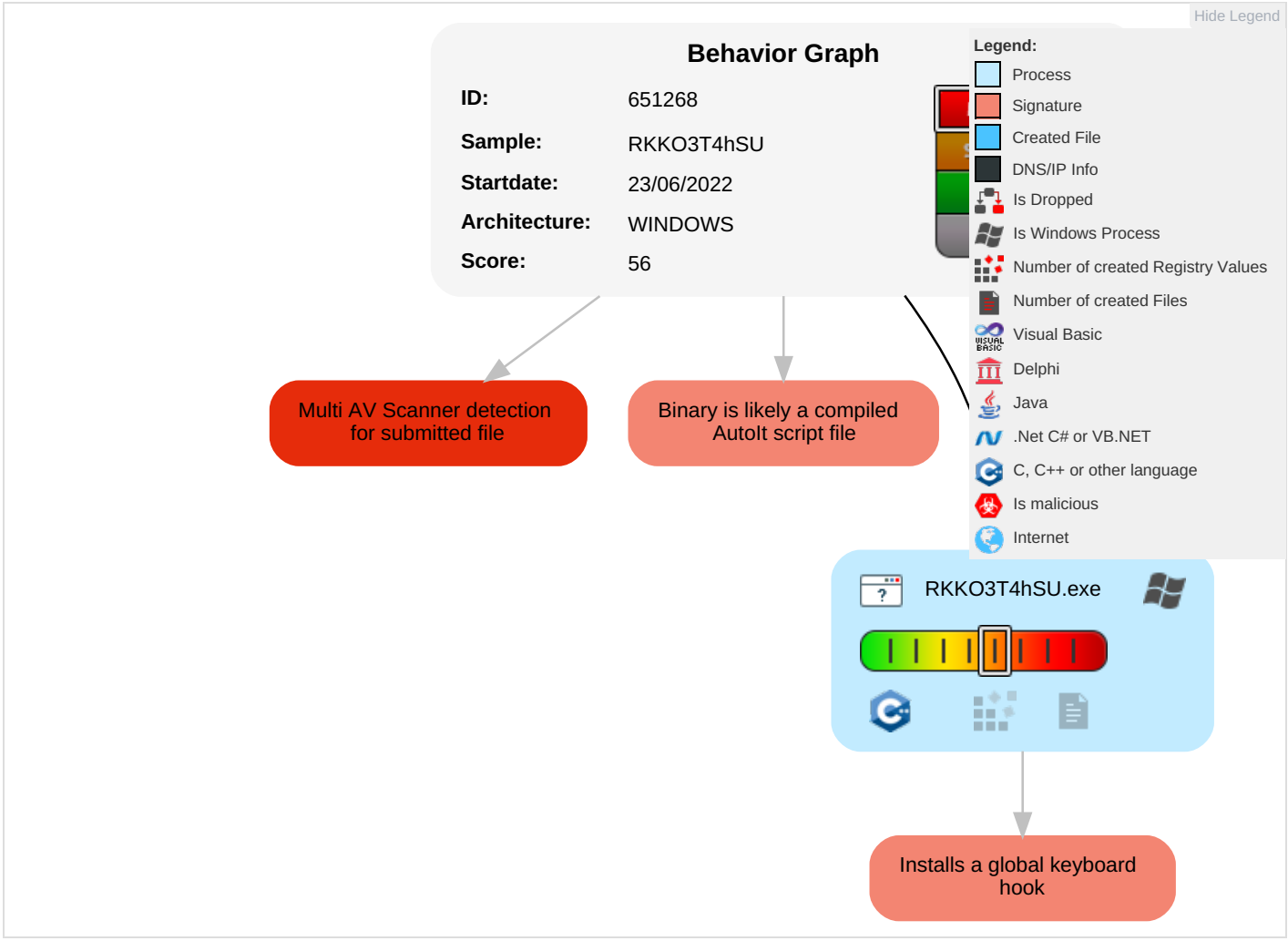
System Summary

Binary is likely a compiled AutoIt script file

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	2 Native API	Path Interception	1 Process Injection	2 Virtualization/Sandbox Evasion	1 3 1 Input Capture	1 System Time Discovery	Remote Services	1 3 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	3 Security Software Discovery	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Obfuscated Files or Information	Security Account Manager	2 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 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	Steganography	Cached Domain Credentials	2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

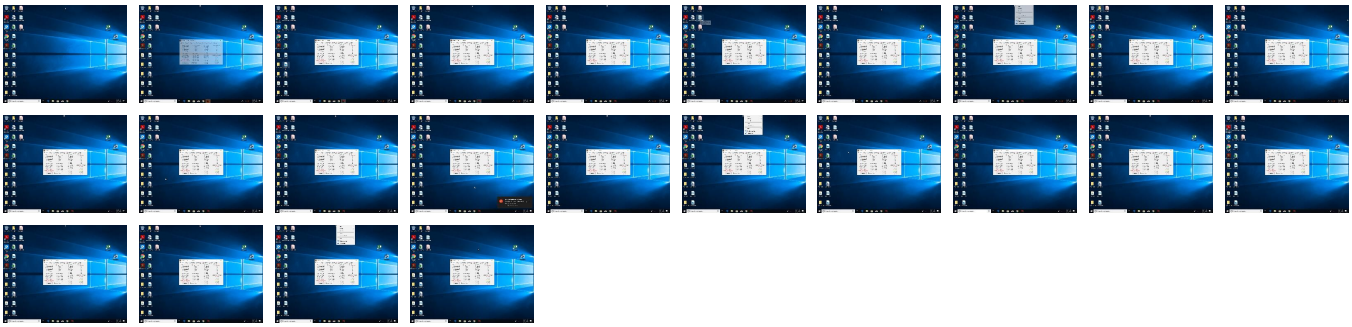
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RKKO3T4hSU.exe	12%	Virustotal		Browse
RKKO3T4hSU.exe	14%	Metadefender		Browse
RKKO3T4hSU.exe	11%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.RKKO3T4hSU.exe.a90000.0.unpack	100%	Avira	HEUR/AGEN.1215508		Download File
0.0.RKKO3T4hSU.exe.a90000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://forum.median-xl.com/viewtopic.php?f=4&t=3702	RKKO3T4hSU.exe, 00000000.00000002.681137900.0000000001033000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	651268
Start date and time: 23/06/202218:20:04	2022-06-23 18:20:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RKKO3T4hSU (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.spyw.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.7%) • Quality average: 81.4% • Quality standard deviation: 12.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
Entropy (8bit):	7.708642860790186
TrID:	• Win32 Executable (generic) a (10002005/4) 99.39% • UPX compressed Win32 Executable (30571/9) 0.30% • Win32 EXE Yoda's Crypter (26571/9) 0.26% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02%
File name:	RKKO3T4hSU.exe
File size:	800768
MD5:	df9025d622d4ac7b41641491c26dc146
SHA1:	ff97781df2915d2d8330d7641f572915da7513cd
SHA256:	22b2655f8d9880171d3caf5ccfc408b07c96d47ba0f15e1ad00df414c7494f74
SHA512:	f3ba07b7b072ccb8d73896517a3f8053e46d5706b32057c09e1e533a62bf46b67ae5ef077cf7b02ecad3df51b7ed180244afb5da446e0122180f1a641af637c8
SSDEEP:	24576:s4GHnhIzOarvotm4V1B3KTr5Lr8Cmat2:rshdarysr8C
TLSH:	F7050178DB9BE17BE26776FD899027B4FC2224D0FE3964B45DCC5110199004FBEAADA0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..R...R...R....C..P.....;.S..._@#.a..._@....._@..g...[j..[... [jo.w...R...r.....#.S..._@'.S...R.k.S.....".S...RichR..

File Icon

Icon Hash:	4994346870344d4b

Static PE Info

General

Entrypoint:	0x545ad0
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, TERMINAL_SERVER_AWARE
Time Stamp:	0x61641E2F [Mon Oct 11 11:21:19 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fc6683d30d9f25244a50fd5357825e79

Entrypoint Preview

Instruction
pushad
mov esi, 004F0000h
lea edi, dword ptr [esi-000EF000h]
push edi
jmp 00007F7864F22B7Dh
nop
mov al, byte ptr [esi]
inc esi
mov byte ptr [edi], al
inc edi
add ebx, ebx
jne 00007F7864F22B79h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F7864F22B5Fh
mov eax, 00000001h
add ebx, ebx
jne 00007F7864F22B79h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
add ebx, ebx
jnc 00007F7864F22B7Dh
jne 00007F7864F22B9Ah
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F7864F22B91h
dec eax

Instruction
add ebx, ebx
jne 00007F7864F22B79h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc eax, eax
jmp 00007F7864F22B46h
add ebx, ebx
jne 00007F7864F22B79h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
jmp 00007F7864F22BC4h
xor ecx, ecx
sub eax, 03h
jc 00007F7864F22B83h
shl eax, 08h
mov al, byte ptr [esi]
inc esi
xor eax, FFFFFFFFh
je 00007F7864F22BE7h
sar eax, 1
mov ebp, eax
jmp 00007F7864F22B7Dh
add ebx, ebx
jne 00007F7864F22B79h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F7864F22B3Eh
inc ecx
add ebx, ebx
jne 00007F7864F22B79h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jc 00007F7864F22B30h
add ebx, ebx
jne 00007F7864F22B79h
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
adc ecx, ecx
add ebx, ebx
jnc 00007F7864F22B61h
jne 00007F7864F22B7Bh
mov ebx, dword ptr [esi]
sub esi, FFFFFFFCh
adc ebx, ebx
jnc 00007F7864F22B56h
add ecx, 02h
cmp ebp, FFFFFB00h
adc ecx, 02h
lea edx, dword ptr [edi+ebp]
cmp ebp, FFFFFFFCh
jbe 00007F7864F22B80h
mov al, byte ptr [edx]

Rich Headers

Programming Language:	• [ASM] VS2013 build 21005 • [C] VS2013 build 21005 • [C++] VS2013 build 21005 • [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [ASM] VS2013 UPD5 build 40629 • [RES] VS2013 build 21005 • [LNK] VS2013 UPD5 build 40629

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1b3090	0x424	.rsrc
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x146000	0x6d090	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1b34b4	0xc	.rsrc
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	0x145cb4	0x48	UPX1
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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
UPX0	0x1000	0xef000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
UPX1	0xf0000	0x56000	0x55e00	False	0.9878491175400291	data	7.936412421761764	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x146000	0x6e000	0x6d600	False	0.7275334821428572	data	7.381009291900878	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x146594	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0x1466c0	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0x1467ec	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0x146918	0x32028	data	English	Great Britain
RT_ICON	0x178944	0xc828	data	English	Great Britain
RT_ICON	0x185170	0x3228	dBase IV DBT of \200.DBF, blocks size 0, block length 12288, next free block index 40, next free block 2002334583, next used block 863525171	English	Great Britain
RT_ICON	0x18839c	0x1ca8	data	English	Great Britain
RT_ICON	0x18a048	0xca8	dBase IV DBT of @.DBF, block length 3072, next free block index 40, next free block 1565207644, next used block 710691370	English	Great Britain
RT_ICON	0x18acf4	0x568	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_MENU	0x10c238	0x50	data	English	Great Britain
RT_DIALOG	0x10c288	0xfc	data	English	Great Britain
RT_STRING	0x10c384	0x594	data	English	Great Britain
RT_STRING	0x10c918	0x68a	data	English	Great Britain
RT_STRING	0x10cfa4	0x490	data	English	Great Britain

Name	RVA	Size	Type	Language	Country
RT_STRING	0x10d434	0x5fc	data	English	Great Britain
RT_STRING	0x10da30	0x65c	data	English	Great Britain
RT_STRING	0x10e08c	0x466	data	English	Great Britain
RT_STRING	0x10e4f4	0x158	data	English	Great Britain
RT_RCDATA	0x18b260	0x2778c	data		
RT_GROUP_ICON	0x1b29f0	0x5a	data	English	Great Britain
RT_GROUP_ICON	0x1b2a50	0x14	data	English	Great Britain
RT_GROUP_ICON	0x1b2a68	0x14	data	English	Great Britain
RT_GROUP_ICON	0x1b2a80	0x14	data	English	Great Britain
RT_VERSION	0x1b2a98	0x1f8	data	English	Great Britain
RT_MANIFEST	0x1b2c94	0x3fa	ASCII text, with CRLF line terminators	English	Great Britain

Imports

DLL	Import
KERNEL32.DLL	LoadLibraryA, GetProcAddress, VirtualProtect, VirtualAlloc, VirtualFree, ExitProcess
ADVAPI32.dll	GetAce
COMCTL32.dll	ImageList_Remove
COMDLG32.dll	GetOpenFileNameW
GDI32.dll	LineTo
IPHLPAPI.DLL	IcmpSendEcho
MPR.dll	WNetUseConnectionW
ole32.dll	CoGetObject
OLEAUT32.dll	VariantInit
PSAPI.DLL	GetProcessMemoryInfo
SHELL32.dll	DragFinish
USER32.dll	GetDC
USERENV.dll	LoadUserProfileW
UxTheme.dll	IsThemeActive
VERSION.dll	VerQueryValueW
WININET.dll	FtpOpenFileW
WINMM.dll	timeGetTime
WSOCK32.dll	connect

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	Great Britain	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: RKKO3T4hSU.exe PID: **824**, Parent PID: **408**

General	
Target ID:	0
Start time:	18:21:08
Start date:	23/06/2022
Path:	C:\Users\user\Desktop\RKKO3T4hSU.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RKKO3T4hSU.exe"
Imagebase:	0xa90000
File size:	800768 bytes
MD5 hash:	DF9025D622D4AC7B41641491C26DC146
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly