ID: 800703
Sample Name: ProduKey.exe
Cookbook: default.jbs
Time: 18:26:35
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

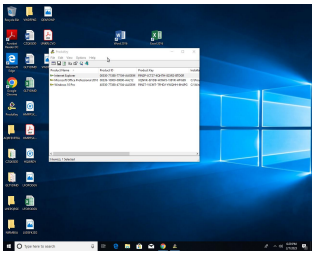
Windows Analysis Report

ProduKey.exe

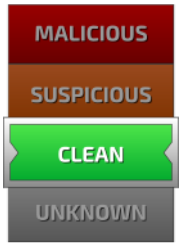
Overview

General Information

Sample Name:	ProduKey.exe
Analysis ID:	800703
MD5:	9260e593a0f2d..
SHA1:	8b3736186f996..
SHA256:	bace5e41e07d…
Infos:	



Detection

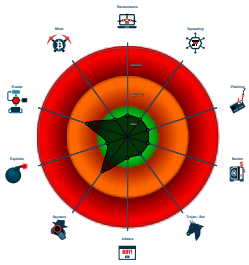


Score:	0
Range:	0 - 100
Whitelisted:	true
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Uses 32bit PE files
- Found a high number of Window / U…
- Queries the product ID of Windows
- Extensive use of GetProcAddress (…
- Uses code obfuscation techniques (…
- Queries the product ID of Microsoft …
- Contains functionality to dynamicall…
- Contains functionality for read data …

Classification



Process Tree

- **System is w10x64**
- ProduKey.exe (PID: 4460 cmdline: C:\Users\user\Desktop\ProduKey.exe MD5: 9260E593A0F2D798FDDC16A7B19AD808)
- **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

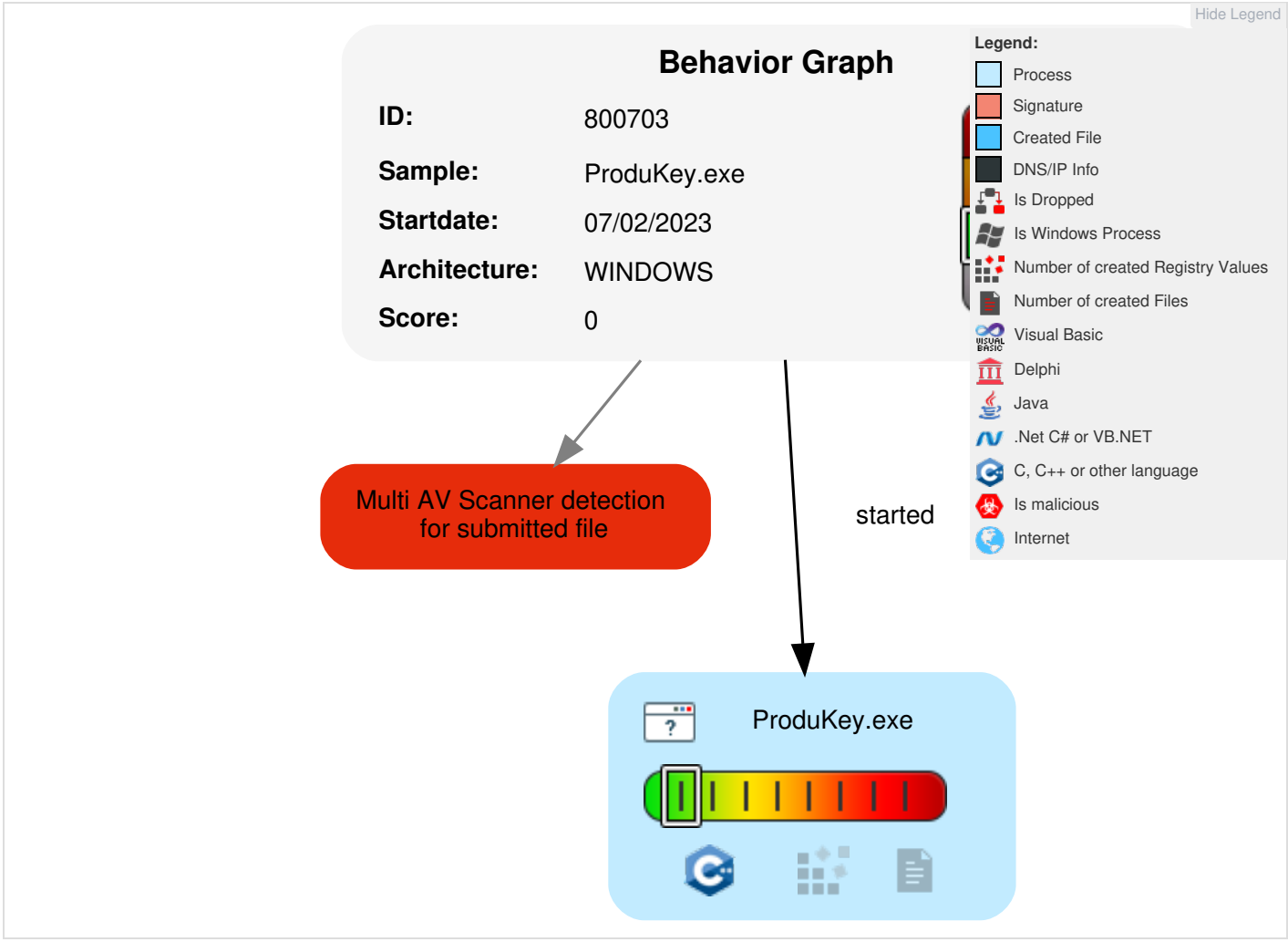
AV Detection

Multi AV Scanner detection for submitted file

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 Command and Scripting Interpreter	Path Interception	Path Interception	1 Obfuscated Files or Information	OS Credential Dumping	1 Application Window Discovery	Remote Services	1 Clipboard Data	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	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)	Obfuscated Files or Information	Security Account Manager	2 3 System Information 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

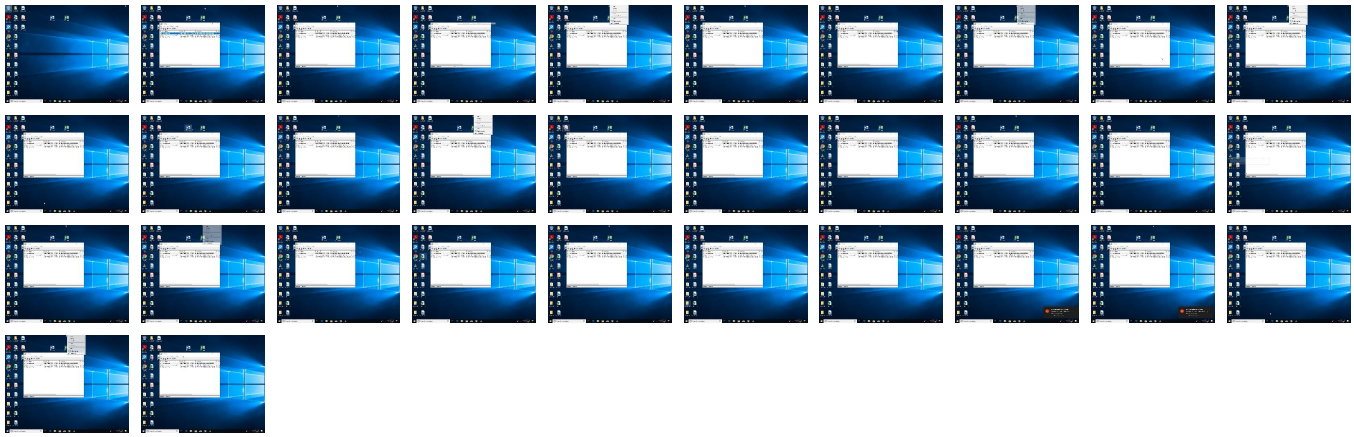
Behavior Graph



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
ProduKey.exe	55%	ReversingLabs		
ProduKey.exe	50%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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://www.nirsoft.net/utils/product_cd_key_viewer.html/stext/shtml/sverhtml/sxml/stab/scomma/stabul	ProduKey.exe	false		high
http://www.nirsoft.net/	ProduKey.exe	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.html	ProduKey.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800703
Start date and time:	2023-02-07 18:26:35 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 55s
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:	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
Sample file name:	ProduKey.exe
Detection:	CLEAN
Classification:	clean48.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.7% (good quality ratio 95.9%) • Quality average: 86.5% • Quality standard deviation: 24.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

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
Entropy (8bit):	6.479180238883247
TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	ProduKey.exe
File size:	96464
MD5:	9260e593a0f2d798fddc16a7b19ad808
SHA1:	8b3736186f9963a5cedd4a2d8dca66041799d0cd
SHA256:	bace5e41e07df9f71b07828dacfde462ce609fa1cd387c7e1cc4aacc59cf00e5
SHA512:	0f2a95f78387b6c4d0c92fd2ef09d7c54c001caed53a63e99af4a19bc92ae0f9dd7a4b655f43667221169d2151a37872ddba3166f74a446be7f06862a4fe3535
SSDEEP:	1536:QuSJT0fl+h17f8OOaC4ujuZkbqYsh/Oud84KTEAUo2Gye42sbiE2:7SJT0fEhhfQH6ZkbqYshTLTGye45R2
TLSH:	F2936B43B7E04471E6E30A712ABA97368EF57D705538C90F57505A8B6CB07C0EE2A39B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+q..J...J...J..'i_..J...i...J..'i...J...EB..J...J...K....m..J....c..J....g..J..Rich.J.....PE..L....O.X.....

File Icon

Icon Hash:	54b26869f8c8cc00

Static PE Info

General

Entrypoint:	0x4010e0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x58EB4FC1 [Mon Apr 10 09:26:25 2017 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:	db1e107cc62854bf6b319abbe0feb186

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=COMODO Code Signing CA 2, O=COMODO CA Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 9/12/2014 2:00:00 AM 9/13/2019 1:59:59 AM
Subject Chain	• CN=Nir Sofer, O=Nir Sofer, STREET=5 Hashoshanim st., L=Ramat Gan, S=Gush Dan, PostalCode=52583, C=IL
Version:	3
Thumbprint MD5:	20080320FBD46305C5578175AB0A9EAA
Thumbprint SHA-1:	A80BAEDA573DF2712F23A41857E648475EAC9BA5
Thumbprint SHA-256:	EAFCB355770E7E64E5559482605D7801F30FEE6B159BF91196D5C9DC6B2419AC
Serial:	1AF0660E837A35A2CD92EC613FC15DB8

Entrypoint Preview

Instruction
push 00000070h
push 0040F3F0h
call 00007FF59CC303F9h
xor ebx, ebx
push ebx
mov edi, dword ptr [0040F108h]
call edi
cmp word ptr [eax], 5A4Dh
jne 00007FF59CC30231h
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
cmp dword ptr [ecx], 00004550h
jne 00007FF59CC30224h
movzx eax, word ptr [ecx+18h]
cmp eax, 0000010Bh
je 00007FF59CC30231h
cmp eax, 0000020Bh
je 00007FF59CC30217h
mov dword ptr [ebp-1Ch], ebx

Instruction
jmp 00007FF59CC30239h
cmp dword ptr [ecx+00000084h], 0Eh
jbe 00007FF59CC30204h
xor eax, eax
cmp dword ptr [ecx+000000F8h], ebx
jmp 00007FF59CC30220h
cmp dword ptr [ecx+74h], 0Eh
jbe 00007FF59CC301F4h
xor eax, eax
cmp dword ptr [ecx+000000E8h], ebx
setne al
mov dword ptr [ebp-1Ch], eax
mov dword ptr [ebp-04h], ebx
push 00000002h
call dword ptr [0040F370h]
pop ecx
or dword ptr [00412EBCh], FFFFFFFFh
or dword ptr [00412EC0h], FFFFFFFFh
call dword ptr [0040F36Ch]
mov ecx, dword ptr [0041217Ch]
mov dword ptr [eax], ecx
call dword ptr [0040F368h]
mov ecx, dword ptr [00412178h]
mov dword ptr [eax], ecx
mov eax, dword ptr [0040F364h]
mov eax, dword ptr [eax]
mov dword ptr [00412EB8h], eax
call 00007FF59CC3034Fh
cmp dword ptr [00412000h], ebx
jne 00007FF59CC3021Eh
push 004012CAh
call dword ptr [0040F31Ch]
pop ecx
call 00007FF59CC30324h

Rich Headers

Programming Language:	• [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	0x10834	0xf0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x13000	0x39b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x14a00	0x2ed0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0xf3d0	0x1c	.rdata
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	0xf000	0x394	.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	0xdc3f	0xde00	False	0.5847585867117117	data	6.373935270388497	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0xf000	0x2a5e	0x2c00	False	0.46351207386363635	data	5.673793868405335	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x12000	0xec4	0x200	False	0.20703125	data	1.1949104842322338	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x13000	0x39b4	0x3a00	False	0.31654094827586204	data	4.101674932157477	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x136e8	0x134	data	English	United States
RT_BITMAP	0x1381c	0x3e8	Device independent bitmap graphic, 112 x 16 x 4, image size 896, 16 important colors	Hebrew	Israel
RT_BITMAP	0x13c04	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112, resolution 3780 x 3780 px/m	English	United States
RT_BITMAP	0x13cdc	0xd8	Device independent bitmap graphic, 14 x 14 x 4, image size 112, resolution 3780 x 3780 px/m	English	United States
RT_ICON	0x13db4	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	Hebrew	Israel
RT_ICON	0x1409c	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	Hebrew	Israel
RT_ICON	0x141c4	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	Hebrew	Israel
RT_MENU	0x142ec	0x73a	data	English	United States
RT_MENU	0x14a28	0x20c	data	English	United States
RT_DIALOG	0x14c34	0xa2	data	Hebrew	Israel
RT_DIALOG	0x14cd8	0x296	data	Hebrew	Israel
RT_DIALOG	0x14f70	0xabc	data	Hebrew	Israel
RT_DIALOG	0x15a2c	0xfa	data	Hebrew	Israel
RT_STRING	0x15b28	0x230	data	English	United States
RT_STRING	0x15d58	0x52	data	English	United States
RT_STRING	0x15dac	0x128	data	English	United States
RT_STRING	0x15ed4	0x4c	Matlab v4 mat-file (little endian) S, numeric, rows 0, columns 0	English	United States
RT_STRING	0x15f20	0x50	data	English	United States
RT_STRING	0x15f70	0xd6	Matlab v4 mat-file (little endian) P, numeric, rows 0, columns 0	English	United States
RT_STRING	0x16048	0x5a	data	English	United States
RT_STRING	0x160a4	0x42	data	English	United States
RT_STRING	0x160e8	0x6a	data	English	United States
RT_STRING	0x16154	0x78	data	English	United States
RT_STRING	0x161cc	0x6c	Matlab v4 mat-file (little endian) Q, numeric, rows 0, columns 0	English	United States
RT_STRING	0x16238	0x62	data	English	United States
RT_ACCELERATOR	0x1629c	0x70	data	Hebrew	Israel
RT_GROUP_CURSOR	0x1630c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0x16320	0x22	data	Hebrew	Israel
RT_GROUP_ICON	0x16344	0x14	data	Hebrew	Israel
RT_VERSION	0x16358	0x2dc	data	Hebrew	Israel
RT_MANIFEST	0x16634	0x380	ASCII text, with very long lines (435), with CRLF line terminators	English	United States

Imports

DLL	Import
MPR.dll	WNetOpenEnumA, WNetEnumResourceA, WNetCloseEnum
msvcrt.dll	_cexit, _XcptFilter, _exit, _c_exit, _onexit, __dllonexit, _purecall, exit, _strlwr, _itoa, strchr, strtoul, _memicmp, __setusermatherr, _initterm, __getmainargs, qsort, _acmdln, malloc, free, ???2@YAPAXI@Z, ???3@YAXPAX@Z, atof, atoi, _strnicmp, _mbsicmp, _stricmp, _strcmpi, strrchr, strncat, sprintf, _adjust_fdiv, __p__commode, __p__fmode, __set_app_type, _controlfp, _except_handler3, memset, memcpy

DLL	Import
COMCTL32.dll	CreateToolbarEx, ImageList_Create, ImageList_ReplaceIcon, ImageList_SetImageCount, ImageList_AddMasked
WS2_32.dll	gethostbyname, WSAStartup, WSACleanup, htons, WSAGetLastError, connect, WSAAsyncSelect, gethostbyaddr, closesocket, WSASetLastError
KERNEL32.dll	OpenProcess, CreateThread, ResumeThread, ReadProcessMemory, ExitProcess, CreateFileA, GetStartupInfoA, GetFileSize, GetModuleFileNameA, GetTimeFormatA, GetCurrentProcessId, SetErrorMode, DeleteFileA, GetStdHandle, EnumResourceNamesA, WritePrivateProfileStringA, GetPrivateProfileIntA, MultiByteToWideChar, GetFileAttributesA, LoadLibraryExA, GetLastError, FindNextFileA, FindFirstFileA, GetLogicalDrives, GetComputerNameA, GetDriveTypeA, WideCharToMultiByte, GetPrivateProfileStringA, Sleep, GetCurrentProcess, CompareFileTime, FileTimeToLocalFileTime, FreeLibrary, FileTimeToSystemTime, GetProcAddress, LoadLibraryA, GetModuleHandleA, FormatMessageA, GetTempFileNameA, FindClose, GetWindowsDirectoryA, ReadFile, GetDateFormatA, GetSystemDirectoryA, GetVersionExA, WriteFile, CloseHandle, GetTempPathA, GlobalAlloc, LocalFree, GlobalLock, GlobalUnlock
USER32.dll	SetTimer, PostQuitMessage, TrackPopupMenu, EndDeferWindowPos, KillTimer, GetFocus, TranslateMessage, DispatchMessageA, DestroyWindow, ModifyMenuA, CreateDialogParamA, LoadStringA, BeginDeferWindowPos, GetMessageA, IsDialogMessageA, DeferWindowPos, RegisterWindowMessageA, SetCursor, GetSysColorBrush, ChildWindowFromPoint, ShowWindow, LoadCursorA, EndDialog, GetDlgItem, CreateWindowExA, SetDlgItemInt, SendDlgItemMessageA, GetDlgItemInt, SetDlgItemTextA, GetDlgItemTextA, SetWindowTextA, RegisterClassA, UpdateWindow, GetSystemMetrics, PostMessageA, SetMenu, LoadAcceleratorsA, SetWindowPos, DefWindowProcA, TranslateAcceleratorA, MessageBoxA, GetWindowPlacement, SendMessageA, GetWindowRect, LoadImageA, LoadIconA, GetWindowLongA, SetWindowLongA, InvalidateRect, SetFocus, MapWindowPoints, GetSysColor, GetClassNameA, GetMenu, CloseClipboard, GetParent, OpenClipboard, EmptyClipboard, GetDC, GetSubMenu, EnableMenuItem, MoveWindow, ReleaseDC, CheckMenuItem, GetMenuItemCount, GetClientRect, LoadMenuA, GetMenuStringA, SetClipboardData, EnableWindow, GetCursorPos, DialogBoxParamA, GetDlgCtrlID, DestroyMenu, EnumChildWindows, GetMenuItemInfoA, GetWindowTextA
GDI32.dll	GetTextExtentPoint32A, SetBkColor, GetStockObject, GetDeviceCaps, SetTextColor, CreateFontIndirectA, SetBkMode, DeleteObject
comdlg32.dll	GetSaveFileNameA, GetOpenFileNameA, FindTextA
ADVAPI32.dll	RegUnLoadKeyA, RegConnectRegistryA, RegEnumValueA, RegDeleteValueA, RegQueryInfoKeyA, RegOpenKeyExA, RegCloseKey, RegEnumKeyExA, RegQueryValueExA, RegSetValueExA, RegDeleteKeyA, RegLoadKeyA
SHELL32.dll	ShellExecuteA, SHBrowseForFolderA, SHGetMalloc, SHGetPathFromIDListA, ShellExecuteExA
ole32.dll	CoInitialize, CoUninitialize

Possible Origin

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

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

Analysis Process: ProduKey.exe PID: **4460**, Parent PID: **3528**

General

Target ID:	0

Start time:	18:27:36
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\ProduKey.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ProduKey.exe
Imagebase:	0x400000
File size:	96464 bytes
MD5 hash:	9260E593A0F2D798FDDC16A7B19AD808
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