ID: 800706
Sample Name: ProduKey.chm
Cookbook: default.jbs
Time: 18:27:23
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

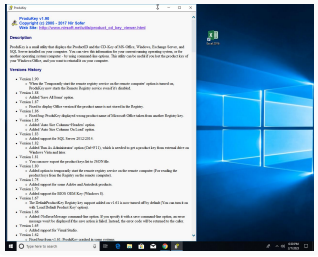
Windows Analysis Report

ProduKey.chm

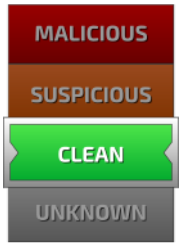
Overview

General Information

Sample Name:	ProduKey.chm
Analysis ID:	800706
MD5:	182a4559a321…
SHA1:	79615bb7a3ef4..
SHA256:	1c47f8ade1b23..



Detection

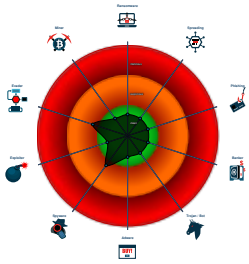


Score:	0
Range:	0 - 100
Whitelisted:	true
Confidence:	100%

Signatures

- Allocates memory with a write watch…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- hh.exe (PID: 5168 cmdline: "C:\Windows\hh.exe" C:\Users\user\Desktop\ProduKey.chm MD5: A50C9DF7603E2F1AEA6B54053794A326)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

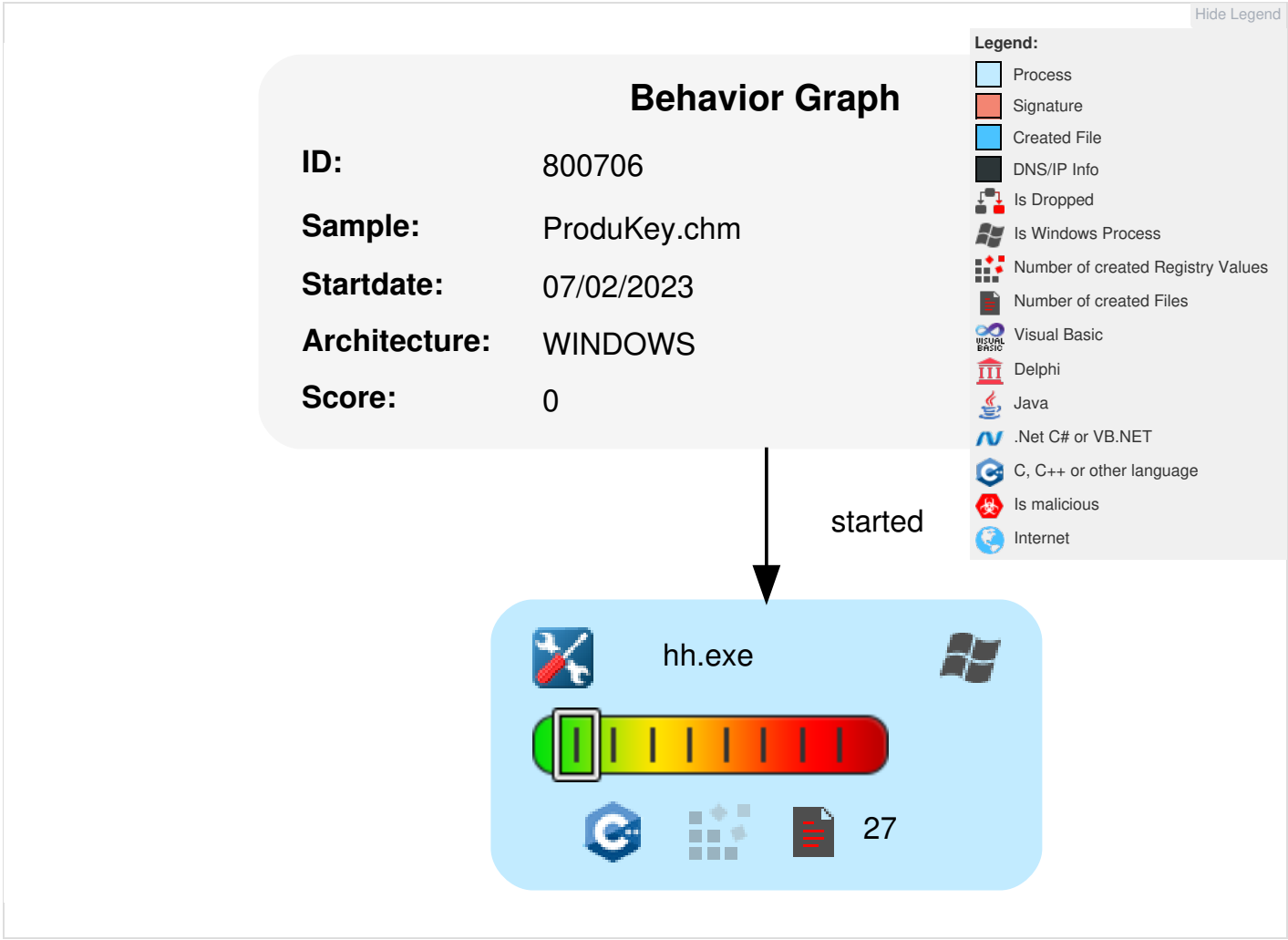
Joe Sandbox Signatures

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

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	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 Virtualization/Sandbox Evasion	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	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 Virtualization/Sandbox Evasion	LSASS Memory	1 2 System Information 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)	1 Disable or Modify Tools	Security Account Manager	Query Registry	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

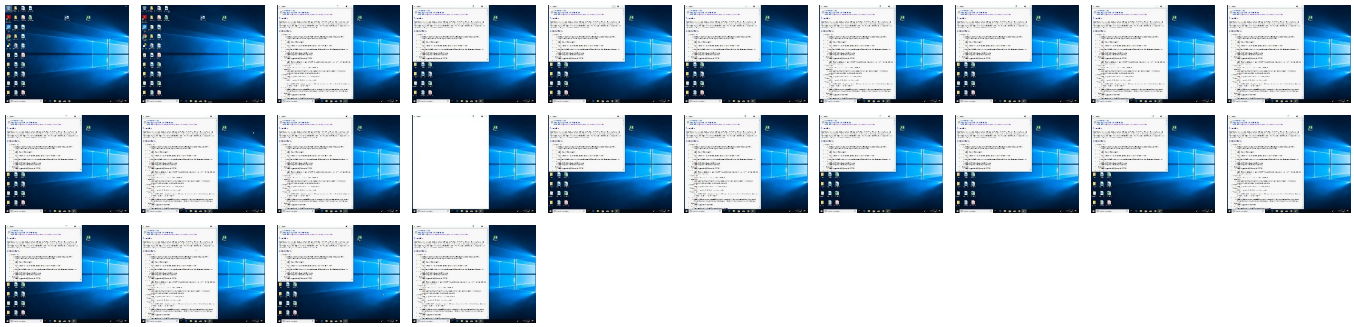
Behavior Graph

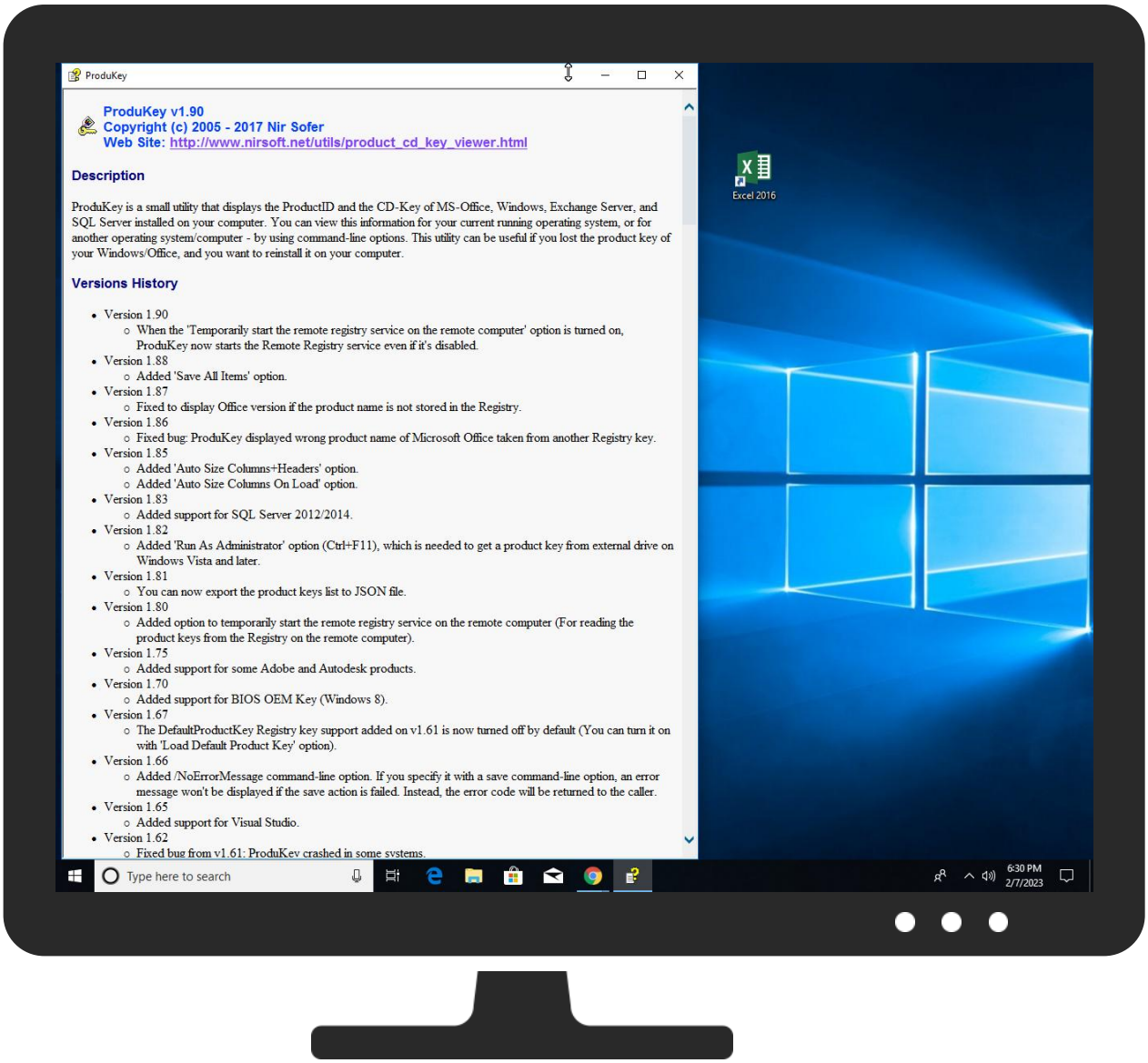


Screenshots

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.chm	0%	ReversingLabs		
ProduKey.chm	0%	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.htmlheD	hh.exe, 00000000.00000003.342372315.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp, hh.exe, 00000000.00000003 .256038817.000002977F2AA000.00000004.000 00020.00020000.00000000.sdmp, hh.exe, 00 000000.00000003.256086124.000002977F2B30 00.00000004.00000020.00020000.00000000.sdmp, hh.exe, 00000000.00000002.517359915.000002977 F2AF000.00000004.00000020.00020000.00000 000.sdmp, hh.exe, 00000000.00000003.2561 23169.000002977F2B9000.00000004.00000020 .00020000.00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.htmlF	hh.exe, 00000000.00000003.342372315.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp, hh.exe, 00000000.00000002 .517359915.000002977F2AF000.00000004.000 00020.00020000.00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.htmlf	hh.exe, 00000000.00000002.517359915.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.htmlche	hh.exe, 00000000.00000002.517359915.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp	false		high
http://blog.nirsoft.net/2009/05/17/antivirus-companies-cause-a-big-headache-to-small-developers/z	hh.exe, 00000000.00000002.516565390.0000 0297033E0000.00000004.00000020.00020000. 00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.html	hh.exe, 00000000.00000003.256073687.0000 02977F2A5000.00000004.00000020.00020000. 00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.htmlroduk ey.html9	hh.exe, 00000000.00000003.342372315.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp, hh.exe, 00000000.00000002 .517359915.000002977F2AF000.00000004.000 00020.00020000.00000000.sdmp	false		high
http://blog.nirsoft.net/2009/05/17/antivirus-companies-cause-a-big-headache-to-small-developers/	hh.exe, 00000000.00000003.256038817.0000 02977F2AA000.00000004.00000020.00020000. 00000000.sdmp, hh.exe, 00000000.00000002 .516565390.000002970341500 0.00000004.000 00020.00020000.00000000.sdmp, hh.exe, 00 000000.00000003.304733003.0000029707B740 00.00000004.00000020.00020000.00000000.sdmp, hh.exe, 00000000.00000003.256086124.000002977 F2B3000.00000004.00000020.00020000.00000 000.sdmp, hh.exe, 00000000.00000002.5173 59915.000002977F2AF000.00000004.00000020 .00020000.00000000.sdmp, hh.exe, 0000000 0.00000002.517281294.000002977F212000.00 000004.00000020.00020000.00000000.sdmp, hh.exe, 00000000.00000002.516565390.00000297033E00 00.00000004.00000020.00020000.00000000.sdmp, hh.exe, 00000000.00000003.270025264.000002970 7B75000.00000004.00000020.00020000.00000 000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.html.	hh.exe, 00000000.00000003.342372315.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp, hh.exe, 00000000.00000002 .517359915.000002977F2AF000.00000004.000 00020.00020000.00000000.sdmp	false		high
http://blog.nirsoft.net/2009/05/17/antivirus-companies-cause-a-big-headache-to-small-developers/v	hh.exe, 00000000.00000002.516565390.0000 0297033E0000.00000004.00000020.00020000. 00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.htmll	hh.exe, 00000000.00000002.517359915.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp, hh.exe, 00000000.00000002 .516565390.00000297033CA000.00000004.000 00020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nirsoft.net/utils/product_cd_key_viewer.htmlroduk ey.htmlDAT	hh.exe, 00000000.00000003.342372315.0000 02977F24C000.00000004.00000020.00020000. 00000000.sdmp, hh.exe, 00000000.00000002 .517359915.000002977F24C000.00000004.000 00020.00020000.00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.html6	hh.exe, 00000000.00000002.517359915.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.htmlv	hh.exe, 00000000.00000003.342372315.0000 02977F2AF000.00000004.00000020.00020000. 00000000.sdmp, hh.exe, 00000000.00000002 .517359915.000002977F2AF000.00000004.000 00020.00020000.00000000.sdmp	false		high
http://www.nirsoft.net/utils/product_cd_key_viewer.htmls	hh.exe, 00000000.00000003.309121391.0000 029707218000.00000004.00000800.00020000. 00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800706
Start date and time:	2023-02-07 18:27:23 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 22s
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:	10
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.chm
Detection:	CLEAN
Classification:	clean1.winCHM@1/6@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .chm

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:28:22	API Interceptor	2x Sleep call for process: hh.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\Microsoft\Windows\INetCache\IE\9QTQHWWN\produkey_icon[1].gif

Process:	C:\Windows\hh.exe
File Type:	GIF image data, version 89a, 32 x 32
Category:	dropped
Size (bytes):	1040
Entropy (8bit):	2.880106848979278
Encrypted:	false
SSDEEP:	6:NlGq9K5tqwnEIPa8lqdNQ9DPAPdYa7+xRgrXscvMS2iQ5zy+r:3GQKzqwnEQa8lqdNQ9YfYgQ3S2t5p
MD5:	AA06955654EEF849A51DF89FDC9208BC
SHA1:	23D978B8078DB5A3EE0649A6422C09A2D1B41B20
SHA-256:	AB80BF76AC30775829501AD88F1A378C08BD4B6E4CBEBA3BC2A4629E575C25AD
SHA-512:	100C2EE2E5CEE36046DE6362292A72E02C975265BC15CE7F0F7F44638673C01B7A88DC8D72F89089924362F405CD00A30097F781BAEDCF16FA2941C53D2F1E2
Malicious:	false
Reputation:	low
Preview:	GIF89a . ...!.....,..... . ...H.....*\.....R...!...(V.h.c../...Q#H."........4...E.. ...rB..o.....1.>.....#.....t.....`.j."......x.*.[G..[..T.x..j.....p...G..8i.....@.....3w.9!r....4.6n..{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\main[1].css

Process:	C:\Windows\hh.exe
File Type:	assembler source, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4325
Entropy (8bit):	5.131781973149786

Encrypted:	false
SSDEEP:	96:89g7yv0e+6zNDoBMq558yw3KiTAT/q0yHF:8iyv0MDoBz55xw6iTAbq0yl
MD5:	EA2F0A6152B6C2EF85D08F9A4411069A
SHA1:	84C0440CB77D6B7B78A71EA1DD6651C7C73AF07E
SHA-256:	9345F60F069E163F4EE0518529A0260C0715AD93C35E808E3BC39D6890E19101
SHA-512:	75A1925F36FD7A1651A3C0FE0373D0BC4A64B83F4BDFD689D8E74348078F0466484C978CD9BD681F45F36A51FB035CBBC1D8D14614586AE7E93B720786AFAD5
Malicious:	false
Reputation:	low
Preview:	BODY {background-color: #F8F8F8; color: #000000;scrollbar-face-color: #DEE3E7;scrollbar-highlight-color: #FFFFFF;scrollbar-shadow-color: #DEE3E7;scrollbar-3dlight-color: #D1D8DD;scrollbar-arrow-color: #006090;scrollbar-track-color: #EFEFEF;scrollbar-darkshadow-color: #98AAB0;}..A:LINK {color: #8040FF }..A:VISITED {color: #C020F0 }..A:HOVER {color: #FF0099 }...title1 {border-width: 2;border-style: outset ; background-color: #0000E0; color: #FFFFFF; width: 100%;font-weight:700;font-family: Arial, Helvetica, sans-serif;font-size: 13pt;}...title2 {border-width: 1;border-style: outset; background-color: #C8C8C8;color: #000080; width: 100%; font-weight:700;font-family: Arial, Helvetica, sans-serif;font-size: 13pt;}...filestable {border-width: 0; background-color: #ECECEC; color: #000000; width: 100%}...filesrow {background-color: #E6E6E6; color: #000000;}...filetitle {font-size:medium; font-weight:700; font-weight:700;font-family: Arial, Helvetica, sans-serif;font-size: 12pt;}...faquestion

C:\Users\user\AppData\Local\Temp\IMT4D03.tmp

Process:	C:\Windows\hh.exe
File Type:	data
Category:	dropped
Size (bytes):	8276
Entropy (8bit):	0.6274991512679713
Encrypted:	false
SSDEEP:	12:m0l6eohI+KKe+KjK9zh+KlE/KlEvt+KlEvdX:SQ1V2FlEClEvt1lEvdX
MD5:	943D3CE711A5EBA4A01A9B4E8EDF1388
SHA1:	E8DFD5502B1413F4996CA43E2E76E45F2A32A1D7
SHA-256:	BBB45CCB31607F92D62EE94204B0E2E4CA802EA6AE6A7B8B6AEBFE99655FA920
SHA-512:	C969D0EF61FFAC73436EC7F094F9C737AD0F26D05EAA8AA506A919F31ACF22E237CBB088F7291C1883C8BF3ABE764F9895F921B4B37EE87A0353F8E4229E68E3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	ITSP....T..... .....j..].!.....".."..T.....PMGL?...../....::DataSpace/NameList..4<(::DataSpace/Storage/MSCompressed/Content...,::DataSpace/Storage/MSCompressed/ControlData....)::DataSpace/Storage/MSCompressed/SpanInfo..../::DataSpace/Storage/MSCompressed/Transform/List..p&_::DataSpace/Storage/MSCompressed/Transform/{7FC28940-9D31-11D0-9B27-00A0C91E9C7C}/InstanceData/...i::DataSpace/Storage/MSCompressed/Transform/{7FC28940-9D31-11D0-9B27-00A0C91E9C7C}/InstanceData/ResetTable..... ....

C:\Users\user\AppData\Local\Temp\~DF5DD65DA5026806E4.TMP

Process:	C:\Windows\hh.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFD5FF97BB24F8E7A7.TMP

Process:	C:\Windows\hh.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.3613836054883338
Encrypted:	false
SSDEEP:	3:YmsaITILPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	679672A5004E0AF50529F33DB5469699

SHA1:	427A4EC3281C9C4FAEB47A22FFBE7CA3E928AFB0
SHA-256:	205D000AA762F3A96AC3AD4B25D791B5F7FC8EFB9056B78F299F671A02B9FD21
SHA-512:	F8615C5E5CF768A94E06961C7C8BEF99BEB43E004A882A4E384F5DD56E047CA59B963A59971F78DCF4C35D1BB92D3A9BC7055BFA3A0D597635DE1A9CE06A3476
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Roaming\Microsoft\HTML Help\hh.dat

Process:	C:\Windows\hh.exe
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	8590
Entropy (8bit):	0.7897229186550494
Encrypted:	false
SSDEEP:	12:1om6ysNMqiNMvyc0Ke0l6eohI+KKe+KjK9zh+KlE/KlEvt+KlEvdX:12x5yc0JQ1V2FlEClEvt1lEvdX
MD5:	9741E5E3988CBCF1C7A1F4F02FC789C0
SHA1:	C41598C950E0D47591194DF4BAAB06B4B435619E
SHA-256:	9C8FCA6A0D5767F7C889FB51F0020580DEB34A251FCE8EF72E4A877540601309
SHA-512:	0BC09FFBD6A180B1150C08739670E28B405A9AAF48763B16B8768FE9BC850E3291F6D3AFF1249E5C2685AB952C00FF0B00FB743DFA86030B5A2308924228914E
Malicious:	false
Preview:	ITSF....`.....|.{....."....|.{....."..`.....(.....:.....T .....!.....,.....j..].!....."..T.....U.n.c.o.m.p.r.e.s.s.e.d.....M.S.C.o.m.p.r.e.s.s.e.d...{.7.F.C.2.8.9.4.0.-.9.D.3.1.-.1.1.D.0.....LZXC.....ITSP....T..... .....j..].!....."..T.....PMGL?...../....::DataSpace/NameList..4<(::DataSpace/Storage/MSCompressed/Content...,::DataSpace/Storage/MSCompressed/ControlData....)::DataSpace/Storage/MSCompressed/SpanInfo..../::DataSpace/Storage/MSCompressed/Transform/List..p&_::DataSpace/Storage/MSCompressed/Transform/{7FC28940-9D31-11D0-9B27-00A0C91E9C7C}/InstanceData/...i::DataSpace/Storage/MSCompressed/Transform/{7FC28940-9D31-11D0-9B27-00A0C91E9C7C}/InstanceData/ResetTable.....

Static File Info

General

File type:	MS Windows HtmlHelp Data
Entropy (8bit):	5.4586329774402795
TrID:	• Windows HELP File (4004/1) 100.00%
File name:	ProduKey.chm
File size:	17708
MD5:	182a4559a321819cff2bc87283253d09
SHA1:	79615bb7a3ef42ca9783f0e9e58dcb21a1b180b8
SHA256:	1c47f8ade1b23861436f7e58971990d99c66fcbf9e85bdf2a2b7bdd1e8641d60
SHA512:	9859d4e00192f1d13b9f882a26ce9a5543973c8ee49c7ca5db83818e1f29dcf1ad5332497e1ea4d872aed318440a8ad457c955ba47367c819e51a6a387a42fc1
SSDEEP:	192:6tgcLqluN9rRwaLe8ofxzmxQdMCNIE0GoxH+0XyMw70PF:69L2A9rRGxzrdQzWe6yM
TLSH:	FF828DF0A7258611C864473273E0314EFA483A2789E3496565DFF39F2549D02BEB2BBD
File Content Preview:	ITSF....`.....|.{....."....|. {....."..`.....x.....T.....,E.....ITSP....T.....j..].!....."..T.....PMGL...../..../#IDXHDR...7.../#ITBITS..

File Icon

Icon Hash:	60d0c86c7c7c9c20

Static Microsoft Compiled HTML Help Info

Objects

Name	Type	Preview
$WWKeywordLinks	directory	
#URLSTR	data	.....produkey.html.
#ITBITS	empty	

Name	Type	Preview
#IDXHDR	data	T#SM..... ....
$OBJINST	X11 SNF font data, MSB first	.....$...bF.V.O.....UU..... ....
produkey.html	HTML document, ASCII text, with CRLF line terminators	<html>..<head>..<title>ProduKey</title>..<link rel="stylesheet" href="main.css">....</head>..<body>....<table border="0" class="utilcaption">..<tr><td><img src="produkey_icon.gif">.. <td>ProduKey v1.90.. ..Copyright (c) 2005 - 2017 Nir Sofer.. .
#STRINGS	data	.main.ProduKey.ProduKey.
$WWAssociativeLinks	directory	
$FIftiMain	empty	
#URLTBL	data	t.....
produkey_icon.gif	GIF image data, version 89a, 32 x 32	GIF89a . ...
#SYSTEM	data	.....OX....HHA Version 4.74.8702...$.....produkey.html.....produkey.... .main.....T#SM..... .....
#TOPICS	data	.....
main.css	assembler source, ASCII text, with CRLF line terminators	BODY {background-color: #F8F8F8; color: #000000;scrollbar-face-color: #DEE3E7;scrollbar-highlight-color: #FFFFFF;scrollbar-shadow-color: #DEE3E7;scrollbar-3dlight-color: #D1D8DD;scrollbar-arrow-color: #006090;scrollbar-track-color: #EFEFEF;scrollbar
#WINDOWS	data	....X.....0..... .....

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: hh.exe PID: **5168**, Parent PID: **3452**

General

Target ID:	0
Start time:	18:28:20
Start date:	07/02/2023
Path:	C:\Windows\hh.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\hh.exe" C:\Users\user\Desktop\ProduKey.chm
Imagebase:	0x7ff665f20000
File size:	17920 bytes
MD5 hash:	A50C9DF7603E2F1AEA6B54053794A326
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly