MALICIOUS

Classifications: Spyware

Threat Names: Trojan.GenericKDZ.76753 Gen:Variant.Mikey.113998

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll**
ID	#2782972
MD5	2955d4759afce09a41c1df5b108f0287
SHA1	11e277c3c987b4119909dd099a5f901e074698e3
SHA256	97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070
File Size	1196.00 KB
Report Created	2021-09-28 14:27 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (16 rules, 158 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	9	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\ekwn\DUI70.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\H15dP8\sqmapi.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #2) hcpmumu.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #71) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #60) hcpmumu.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #123) hcpmumu.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #232) sethc.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #237) hcpmumu.exe as "Gen:Variant.Mikey.113998".		
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #2) hcpmumu.exe alters context of (process #71) explorer.exe.			
4/5	Privilege Escalation	Creates elevated child process	1	-
	• (Process #71) explorer.exe creates (process #229) eudcedit.exe with elevated privileges.			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #71) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Hide Tracks	Deletes file after execution	2	-
	• (Process #71) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\local\ekwn\sethc.exe". • (Process #71) explorer.exe deletes executed executable "c:\windows \system32\eudcedit.exe".			
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\PrivacIE\txGHoCV75Mr\sethc.exe", to be triggered by Time. Task has been rescheduled by the analyzer.			
1/5	Discovery	Reads system data	23	-

Score	Category	Operation	Count	Classification
		• (Process #2) hcpmumu.exe reads the Windows installation date from registry. • (Process #3) hcpmumu.exe reads the Windows installation date from registry. • (Process #4) hcpmumu.exe reads the Windows installation date from registry. • (Process #6) hcpmumu.exe reads the Windows installation date from registry. • (Process #5) hcpmumu.exe reads the Windows installation date from registry. • (Process #8) hcpmumu.exe reads the Windows installation date from registry. • (Process #7) hcpmumu.exe reads the Windows installation date from registry. • (Process #11) hcpmumu.exe reads the Windows installation date from registry. • (Process #34) hcpmumu.exe reads the Windows installation date from registry. • (Process #13) hcpmumu.exe reads the Windows installation date from registry. • (Process #10) hcpmumu.exe reads the Windows installation date from registry. • (Process #33) hcpmumu.exe reads the Windows installation date from registry. • (Process #38) hcpmumu.exe reads the Windows installation date from registry. • (Process #37) hcpmumu.exe reads the Windows installation date from registry. • (Process #32) hcpmumu.exe reads the Windows installation date from registry. • (Process #42) hcpmumu.exe reads the Windows installation date from registry. • (Process #21) hcpmumu.exe reads the Windows installation date from registry. • (Process #20) hcpmumu.exe reads the Windows installation date from registry. • (Process #71) explorer.exe reads the Windows installation date from registry. • (Process #25) hcpmumu.exe reads the Windows installation date from registry. • (Process #60) hcpmumu.exe reads the Windows installation date from registry. • (Process #179) hcpmumu.exe reads the Windows installation date from registry. • (Process #110) hcpmumu.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	93	-

- (Process #2) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #3) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #4) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #2) hcpmumu.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #6) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #5) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #7) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #8) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #11) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #34) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #13) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #10) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #33) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #38) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #37) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #32) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #42) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #71) explorer.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #21) hcpmumu.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #71) explorer.exe creates mutex with name "{33ff21cb-ff8c-80f2-435a-9f14e40fde6b}".
- (Process #71) explorer.exe creates mutex with name "{ad66cb9e-7ae1-701b-6069-4a7b793507ac}".
- (Process #71) explorer.exe creates mutex with name "{6ae03f50-7a2d-c6e9-ca75-492d6e54c058}".
- (Process #71) explorer.exe creates mutex with name "{13e06e4b-2481-b368-8f42-2212f1d59822}".
- (Process #71) explorer.exe creates mutex with name "{65c8ac9c-25ba-82f3-37f2-3fe3857eeb82}".
- (Process #71) explorer.exe creates mutex with name "{858c4289-63b2-a2dd-c583-194c14978d8f}".
- (Process #71) explorer.exe creates mutex with name "{247e511c-baa2-d42e-5dea-e537316b6ab0}".
- (Process #71) explorer.exe creates mutex with name "{445e88c9-0ef7-f980-790a-73297e705b1f}".
- (Process #71) explorer.exe creates mutex with name "{0a229cb1-bb57-9bd8-01b2-31e4b7cbf515}".
- (Process #71) explorer.exe creates mutex with name "{4126ed8b-1649-b296-c1a8-6a31b31e936e}".
- (Process #71) explorer.exe creates mutex with name "{50a49a66-4b11-240c-8816-398b6bd70ed6}".
- (Process #71) explorer.exe creates mutex with name "{2d7bccd8-c070-8723-c092-31c38068d849}".
- (Process #71) explorer.exe creates mutex with name "{aa8eec2a-1624-d913-f987-9558cbeacce1}".
- (Process #71) explorer.exe creates mutex with name "{9124fc0f-aad1-69ca-f087-b6f4b4618452}".
- (Process #71) explorer.exe creates mutex with name "{3424d05e-75d9-fa9d-601e-13c62053c3c5}".
- (Process #71) explorer.exe creates mutex with name "{91af0379-7553-2b9a-1768-bb6f0281e3e9}".
- (Process #71) explorer.exe creates mutex with name "{821b3d72-6d45-a55c-2ff2-657dbbeba155}".
- (Process #71) explorer.exe creates mutex with name "{87870dec-87d4-3464-8983-690c1429eba9}".
- (Process #71) explorer.exe creates mutex with name "{9a382e7d-fa1b-dd43-a0dd-294ace4cebfc}".
- (Process #71) explorer.exe creates mutex with name "{8da6b341-b6ae-4ed6-a4db-b8d7a21d3ce2}".
- (Process #71) explorer.exe creates mutex with name "{02d851a8-f7cd-b455-df45-71a402a6edbc}".
- (Process #71) explorer.exe creates mutex with name "{6ba32bba-4e96-f5a2-050a-03757c53defe}".
- (Process #71) explorer.exe creates mutex with name "{c048b0eb-b8ca-7103-8f33-90bb9cc094e1}".
- (Process #71) explorer.exe creates mutex with name "{c7dddfcc-fb68-9c80-b7a6-092779936187}".
- (Process #71) explorer.exe creates mutex with name "{b59073af-3f1e-9c2e-af6d-076c62047c1a}".
- (Process #71) explorer.exe creates mutex with name "{7f2d86d4-0955-2066-882a-14cbed49896d}".
- (Process #71) explorer.exe creates mutex with name "{018d1282-98a9-7481-13d2-c8f764fa5048}".
- (Process #71) explorer.exe creates mutex with name "{09994fee-51eb-0a96-ec56-cae7e3daecec}".
- (Process #71) explorer.exe creates mutex with name "{29021d34-bd3b-66d0-b71b-552d729d9a4a}".
- (Process #71) explorer.exe creates mutex with name "{b407468a-fc89-c63a-2493-e889c30daef8}".
- (Process #71) explorer.exe creates mutex with name "{e4e8cfa9-4e2a-ffb0-a03d-bd662f479cc0}".
- (Process #71) explorer.exe creates mutex with name "{baf9aa31-a0c9-f808-5a2b-06d9f2a620eb}".
- (Process #71) explorer.exe creates mutex with name "{6d4ceb18-7d30-0d62-7553-417a12d1ddd9}".
- (Process #71) explorer.exe creates mutex with name "{b049459e-3c89-2588-306b-77da13f498b6}".
- (Process #71) explorer.exe creates mutex with name "{7150daae-191d-d79c-f695-5cf339e31f5f}".
- (Process #71) explorer.exe creates mutex with name "{32c5cb54-a427-4241-90fb-bc414e1c9eff}".
- (Process #71) explorer.exe creates mutex with name "{cb59f0a7-5035-4c73-c0b0-ac2839924f2a}".
- (Process #71) explorer.exe creates mutex with name "{89977e79-7c98-ab0d-42f0-94b76fc1b777}".
- (Process #71) explorer.exe creates mutex with name "{b4e9fa2e-e01d-98cf-6d18-53806885dfda}".
- (Process #71) explorer.exe creates mutex with name "{0f5fef32-f8f1-ad75-9bdb-8e355695ddde}".
- (Process #71) explorer.exe creates mutex with name "{19049204-25e8-7de2-df5-a1e7c9fdc579}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	1	-

• (Process #2) hcpmumu.exe reads from (process #71) explorer.exe.

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	9	-

• (Process #71) explorer.exe starts C:\Windows\system32\eudcedit.exe with a hidden window.
• (Process #71) explorer.exe starts (process #229) eudcedit.exe with a hidden window.
• (Process #71) explorer.exe starts C:\Windows\system32\perfmon.exe with a hidden window.
• (Process #71) explorer.exe starts C:\Windows\system32\SystemPropertiesComputerName.exe with a hidden window.
• (Process #71) explorer.exe starts (process #154) sethc.exe with a hidden window.
• (Process #71) explorer.exe starts (process #232) sethc.exe with a hidden window.
• (Process #71) explorer.exe starts (process #255) spreview.exe with a hidden window.
• (Process #71) explorer.exe starts C:\Windows\system32\rrinstaller.exe with a hidden window.
• (Process #71) explorer.exe starts C:\Windows \system32\rrinstaller.exe with a hidden window.

Score	Category	Operation	Count	Classification
1/5	System Modification	Modifies operating system directory	4	-

• (Process #71) explorer.exe creates file "\\?\C:\Windows \system32\MFC42u.dll" in the OS directory.
• (Process #71) explorer.exe creates file "\\?\C:\Windows \system32\eudcedit.exe" in the OS directory.
• (Process #71) explorer.exe creates file "\\?\C:\Windows \system32\MFPlat.DLL" in the OS directory.
• (Process #71) explorer.exe creates file "\\?\C:\Windows \system32\rrinstaller.exe" in the OS directory.

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Writes an unusually large amount of data to the registry	1	-

• (Process #71) explorer.exe hides 3600 bytes in "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder\{0CDCFD74-9368-FB31-4629-21EB5AA8E73C}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-

• (Process #71) explorer.exe resolves 26 API functions by name.

Score	Category	Operation	Count	Classification
1/5	Execution	Drops PE file	7	-

• (Process #71) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\ekwn\DUI70.dll".
• (Process #71) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\H15dP8\sqmapi.dll".
• (Process #71) explorer.exe drops file "\\?\C:\Windows \system32\MFC42u.dll".
• (Process #71) explorer.exe drops file "\\?\C:\Windows \system32\eudcedit.exe".
• (Process #71) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\ekwn\sethc.exe".
• (Process #71) explorer.exe drops file "\\?\C:\Windows \system32\MFPlat.DLL".
• (Process #71) explorer.exe drops file "\\?\C:\Windows \system32\rrinstaller.exe".

Score	Category	Operation	Count	Classification
1/5	Execution	Executes dropped PE file	3	-

• Executes dropped file "\\?\C:\Windows \system32\eudcedit.exe".
• Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\ekwn\sethc.exe".
• Executes dropped file "\\?\C:\Windows \system32\rrinstaller.exe".

Score	Category	Operation	Count	Classification
-	Trusted	Known clean file	4	-

• File "\\?\C:\Windows \system32\eudcedit.exe" is a known clean file.
• File "C:\Users\kEecfMwgj\AppData\Local\ekwn\sethc.exe" is a known clean file.
• File "\\?\C:\Windows \system32\rrinstaller.exe" is a known clean file.
• File "c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6" is a known clean file.

Mitre ATT&CK Matrix

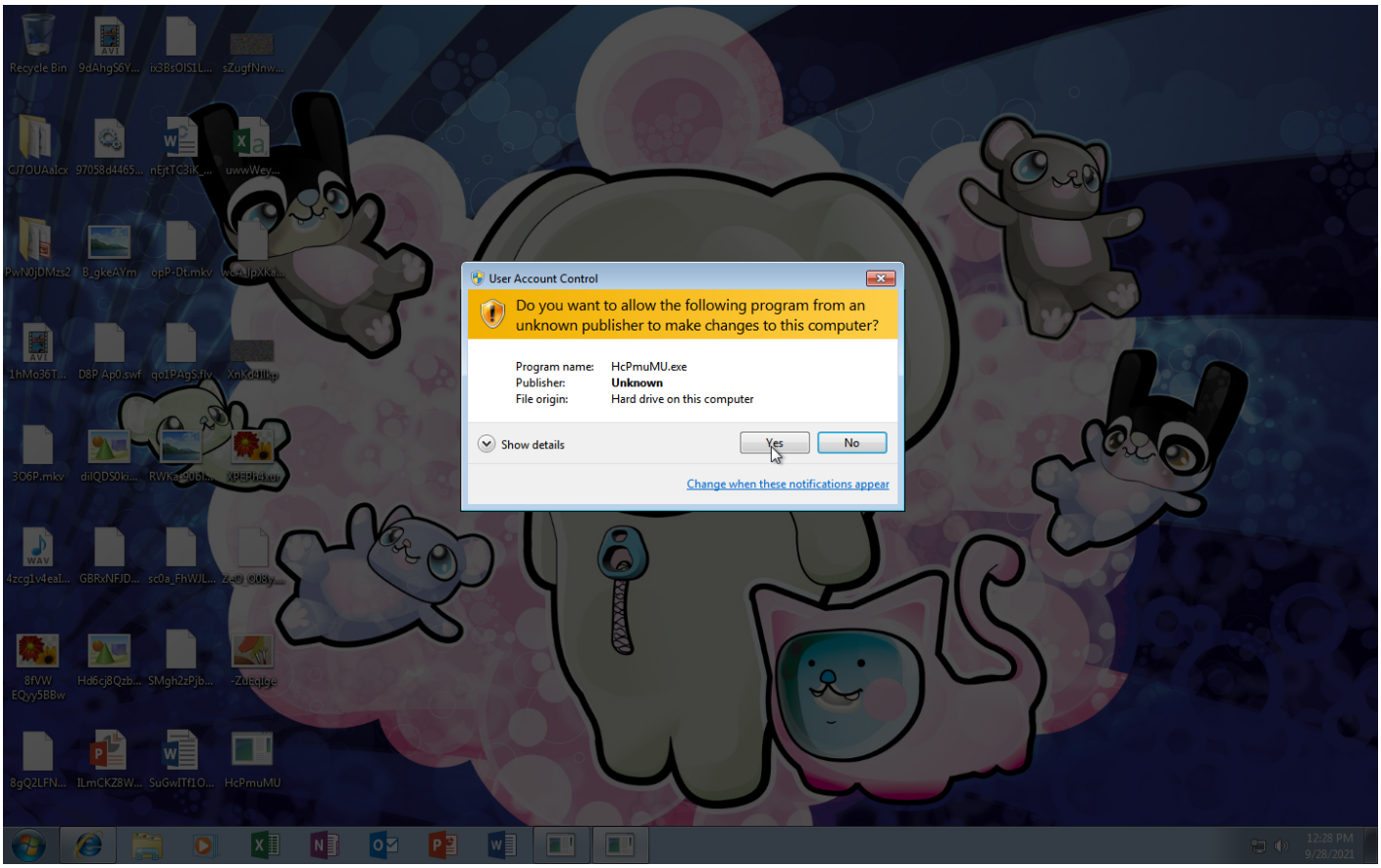
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window		#T1082 System Information Discovery					
				#T1112 Modify Registry		#T1012 Query Registry					
				#T1045 Software Packing							

Sample Information

ID	#2782972
MD5	2955d4759afce09a41c1df5b108f0287
SHA1	11e277c3c987b4119909dd099a5f901e074698e3
SHA256	97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070
SSDeep	12288:/VI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:2fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll
File Size	1196.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 14:27 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	281
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	9
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: HcPmuMU.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

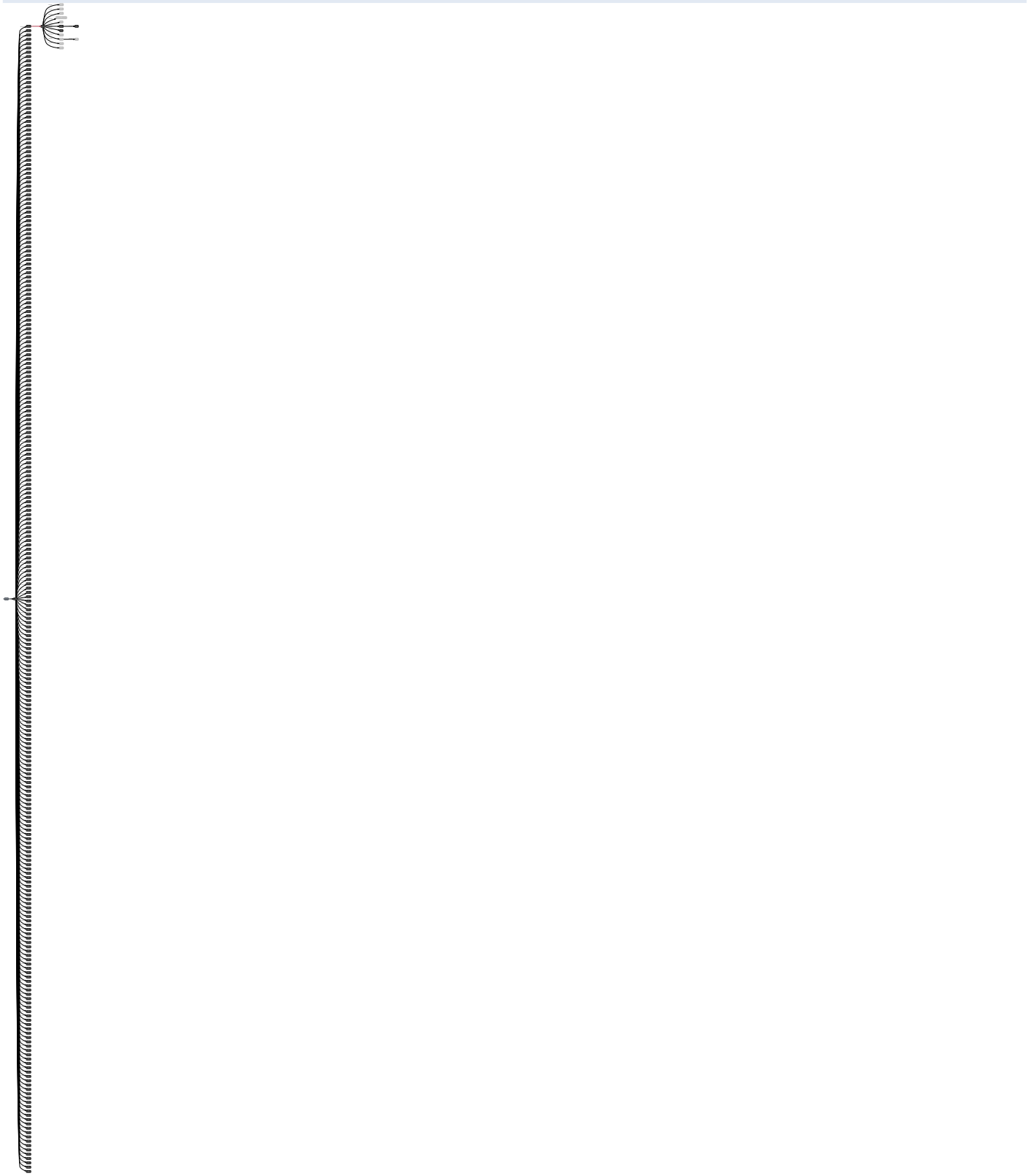
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: hcpmumu.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpw9sqrl_v" /s
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 52651, Reason: Analysis Target
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	241.93s
Return Code	Unknown
PID	3668
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	16
File	7
Environment	1
Process	267

Process #2: hcpmumu.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#1
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67858, Reason: Child Process
Unmonitor End Time	End Time: 105707, Reason: Terminated
Monitor duration	37.85s
Return Code	0
PID	3688
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	9
Module	41
File	118
Environment	2
Registry	589
Mutex	5
Process	2
-	2
-	1
-	32

Process #3: hcpmumu.exe

ID	3
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#10
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 69269, Reason: Child Process
Unmonitor End Time	End Time: 83601, Reason: Terminated
Monitor duration	14.33s
Return Code	0
PID	3700
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #4: hcpmumu.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#11
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 69383, Reason: Child Process
Unmonitor End Time	End Time: 87734, Reason: Terminated
Monitor duration	18.35s
Return Code	0
PID	3712
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	7
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #5: hcpmumu.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#13
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 69817, Reason: Child Process
Unmonitor End Time	End Time: 87606, Reason: Terminated
Monitor duration	17.79s
Return Code	0
PID	3732
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #6: hcpmumu.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#14
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 70221, Reason: Child Process
Unmonitor End Time	End Time: 86779, Reason: Terminated
Monitor duration	16.56s
Return Code	0
PID	3748
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #7: hcpmumu.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#15
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71465, Reason: Child Process
Unmonitor End Time	End Time: 86995, Reason: Terminated
Monitor duration	15.53s
Return Code	0
PID	3760
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #8: hcpmumu.exe

ID	8
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#16
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71765, Reason: Child Process
Unmonitor End Time	End Time: 87286, Reason: Terminated
Monitor duration	15.52s
Return Code	0
PID	3772
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	589
Mutex	7

Process #9: hcpmumu.exe

ID	9
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#17
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 73640, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	220.94s
Return Code	Unknown
PID	3788
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #10: hcpmumu.exe

ID	10
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#18
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 74053, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	220.53s
Return Code	Unknown
PID	3804
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #11: hcpmumu.exe

ID	11
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#19
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76223, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	218.36s
Return Code	Unknown
PID	3832
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	114
Environment	2
Registry	171
Mutex	3

Process #12: hcpmumu.exe

ID	12
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#2
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76945, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	217.64s
Return Code	Unknown
PID	3852
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #13: hcpmumu.exe

ID	13
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#20
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77118, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	217.47s
Return Code	Unknown
PID	3864
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #14: hcpmumu.exe

ID	14
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#21
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77504, Reason: Child Process
Unmonitor End Time	End Time: 265874, Reason: Terminated
Monitor duration	188.37s
Return Code	0
PID	3884
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #15: hcpmumu.exe

ID	15
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#22
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77568, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	217.01s
Return Code	Unknown
PID	3896
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #16: hcpmumu.exe

ID	16
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#23
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77661, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	216.92s
Return Code	Unknown
PID	3908
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #17: hcpmumu.exe

ID	17
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#24
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77800, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	216.78s
Return Code	Unknown
PID	3920
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #18: hcpmumu.exe

ID	18
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#25
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77867, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	216.72s
Return Code	Unknown
PID	3932
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #19: hcpmumu.exe

ID	19
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#26
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78004, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	216.58s
Return Code	Unknown
PID	3944
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #20: hcpmumu.exe

ID	20
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#27
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78083, Reason: Child Process
Unmonitor End Time	End Time: 136214, Reason: Terminated
Monitor duration	58.13s
Return Code	0
PID	3956
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #21: hcpmumu.exe

ID	21
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#28
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78215, Reason: Child Process
Unmonitor End Time	End Time: 135141, Reason: Terminated
Monitor duration	56.93s
Return Code	0
PID	3968
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	3

Process #22: hcpmumu.exe

ID	22
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#29
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78284, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	216.30s
Return Code	Unknown
PID	3980
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #23: hcpmumu.exe

ID	23
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#3
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78363, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	216.22s
Return Code	Unknown
PID	3992
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #24: hcpmumu.exe

ID	24
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#30
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78445, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	216.14s
Return Code	Unknown
PID	4004
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #25: hcpmumu.exe

ID	25
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#31
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78554, Reason: Child Process
Unmonitor End Time	End Time: 136214, Reason: Terminated
Monitor duration	57.66s
Return Code	0
PID	4016
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #26: hcpmumu.exe

ID	26
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#32
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78608, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.97s
Return Code	Unknown
PID	4028
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #27: hcpmumu.exe

ID	27
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#33
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78733, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.85s
Return Code	Unknown
PID	4040
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #28: hcpmumu.exe

ID	28
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#34
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78801, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.78s
Return Code	Unknown
PID	4052
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #29: hcpmumu.exe

ID	29
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#35
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78920, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.66s
Return Code	Unknown
PID	4064
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #30: hcpmumu.exe

ID	30
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#36
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78984, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.60s
Return Code	Unknown
PID	4076
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #31: hcpmumu.exe

ID	31
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#4
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79093, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.49s
Return Code	Unknown
PID	4088
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #32: hcpmumu.exe

ID	32
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#43
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79182, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.40s
Return Code	Unknown
PID	1092
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #33: hcpmumu.exe

ID	33
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#44
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79311, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.27s
Return Code	Unknown
PID	3092
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #34: hcpmumu.exe

ID	34
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#45
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79373, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.21s
Return Code	Unknown
PID	1356
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #35: hcpmumu.exe

ID	35
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#46
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79500, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.08s
Return Code	Unknown
PID	1060
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	19
File	112
Environment	1

Process #36: hcpmumu.exe

ID	36
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#48
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79566, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	215.02s
Return Code	Unknown
PID	1896
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #37: hcpmumu.exe

ID	37
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#49
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79706, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	214.88s
Return Code	Unknown
PID	2124
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #38: hcpmumu.exe

ID	38
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#50
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79768, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	214.81s
Return Code	Unknown
PID	3224
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #39: hcpmumu.exe

ID	39
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#60
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79908, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	214.68s
Return Code	Unknown
PID	3280
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #40: hcpmumu.exe

ID	40
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#62
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79979, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	214.60s
Return Code	Unknown
PID	3256
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #41: hcpmumu.exe

ID	41
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#63
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81102, Reason: Child Process
Unmonitor End Time	End Time: 173631, Reason: Terminated
Monitor duration	92.53s
Return Code	0
PID	3244
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #42: hcpmumu.exe

ID	42
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#64
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81237, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	213.35s
Return Code	Unknown
PID	3292
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	113
Environment	2
Registry	171
Mutex	3

Process #43: hcpmumu.exe

ID	43
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#65
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81594, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	212.99s
Return Code	Unknown
PID	3328
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #44: hcpmumu.exe

ID	44
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#66
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81689, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	212.89s
Return Code	Unknown
PID	1872
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #45: hcpmumu.exe

ID	45
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#67
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81894, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	212.69s
Return Code	Unknown
PID	3316
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #46: hcpmumu.exe

ID	46
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#68
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81955, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	212.63s
Return Code	Unknown
PID	3096
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #47: hcpmumu.exe

ID	47
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#69
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82132, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	212.45s
Return Code	Unknown
PID	1436
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #48: hcpmumu.exe

ID	48
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#7
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82214, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	212.37s
Return Code	Unknown
PID	2132
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #49: hcpmumu.exe

ID	49
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#72
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82348, Reason: Child Process
Unmonitor End Time	End Time: 233980, Reason: Terminated
Monitor duration	151.63s
Return Code	0
PID	2144
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	67

Process #50: hcpmumu.exe

ID	50
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#73
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82404, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	212.18s
Return Code	Unknown
PID	2156
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #51: hcpmumu.exe

ID	51
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#74
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82665, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	211.92s
Return Code	Unknown
PID	2168
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #52: hcpmumu.exe

ID	52
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#75
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82735, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	211.85s
Return Code	Unknown
PID	2180
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #53: hcpmumu.exe

ID	53
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#76
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82945, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	211.64s
Return Code	Unknown
PID	2192
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #54: hcpmumu.exe

ID	54
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#77
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83012, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	211.57s
Return Code	Unknown
PID	2204
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #55: hcpmumu.exe

ID	55
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#78
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83217, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	211.37s
Return Code	Unknown
PID	2540
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #56: hcpmumu.exe

ID	56
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#79
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83262, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	211.32s
Return Code	Unknown
PID	2552
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #57: hcpmumu.exe

ID	57
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#8
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83419, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	211.16s
Return Code	Unknown
PID	2564
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #58: hcpmumu.exe

ID	58
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#80
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83467, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	211.12s
Return Code	Unknown
PID	2576
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #59: hcpmumu.exe

ID	59
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#81
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83602, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.98s
Return Code	Unknown
PID	2588
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #60: hcpmumu.exe

ID	60
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#82
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83655, Reason: Child Process
Unmonitor End Time	End Time: 161680, Reason: Terminated
Monitor duration	78.03s
Return Code	0
PID	2600
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #61: hcpmumu.exe

ID	61
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#83
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83729, Reason: Child Process
Unmonitor End Time	End Time: 236328, Reason: Terminated
Monitor duration	152.60s
Return Code	0
PID	2612
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #62: hcpmumu.exe

ID	62
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#84
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83812, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.77s
Return Code	Unknown
PID	2624
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #63: hcpmumu.exe

ID	63
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#85
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83890, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.69s
Return Code	Unknown
PID	2636
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #64: hcpmumu.exe

ID	64
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#86
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84081, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.50s
Return Code	Unknown
PID	2648
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #65: hcpmumu.exe

ID	65
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#9
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84206, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.38s
Return Code	Unknown
PID	2660
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #66: hcpmumu.exe

ID	66
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BeginBufferedAnimation
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84260, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.32s
Return Code	Unknown
PID	2672
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #67: hcpmumu.exe

ID	67
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BeginBufferedPaint
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84325, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.26s
Return Code	Unknown
PID	2684
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #68: hcpmumu.exe

ID	68
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BeginPanningFeedback
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84396, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.19s
Return Code	Unknown
PID	2696
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #69: hcpmumu.exe

ID	69
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintClear
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84517, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.07s
Return Code	Unknown
PID	2708
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #70: hcpmumu.exe

ID	70
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintInit
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84576, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	210.01s
Return Code	Unknown
PID	3220
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #71: explorer.exe

ID	71
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 84697, Reason: Injection
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	209.89s
Return Code	Unknown
PID	1116
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (1)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\hcpmumu.exe	0xe6c / 0x474	0x77732ed0(2004037328)	-	✓	1

Dropped Files (11)

File Name	File Size	SHA256	YARA Match
-	50 bytes	2d970fea1e7ebc4c9bae287309fa032cb2ac90323c0cdb49ca9593dc7d074c98	✗
\\?\C:\Windows \system32\MFC42u.dll	1325.50 KB	1fcae1eeb5b5cf627c786bbe8a38f3d2af7a3f2c56ac850a830909db3aa93811	✗
\\?\C:\Windows \system32\eudcedit.exe	351.50 KB	1f64118bdc3515e8e9fce6ad182f6d0c8a6528d638fedb4901a6152cde4c7cde	✗
C:\Users\kEecfMwgj\AppData\Local\ekwn\DUI70.dll	1404.00 KB	8704f443c944264d96f3f0a6df5a0b42fc6e34720d77cdf5a10834c9af2ec891	✗
C:\Users\kEecfMwgj\AppData\Local\ekwn\sethc.exe	272.50 KB	dd94bf73f0e3652b76cfb774b419ceaa2082bc7f30cc34e28dfa51952fa9ccb5	✗
\\?\C:\Windows \system32\MFPlat.DLL	422.00 KB	fd5484565f50a094dafe9c830520f122140ee6b4bc5b1b2e325f17819d4e37f9	✗
\\?\C:\Windows \system32\rrinstaller.exe	54.50 KB	6832ffa7cd2d0a92eccbea7e90b8e344f6dc808f2c3cc0a93859a45057028937	✗
C:\Users\kEecfMwgj\AppData\Local\H15dP8\sqmapi.dll	1200.00 KB	cea138e5f0a20c09ef1ddd139147dd37e30782b40a1a823e3eac7ab6d557c5a4	✗
-	1.40 KB	f8f3f429ad8ca958bd7f06fd7c57b6c4a5a7d3f50a189c346f4dd4c2cc35e0cb	✗
-	1.40 KB	72275404c470b62a5ff49013e3f952d9480afd5c7e45b6c504235823da4894ae	✗
-	1.42 KB	c618f7e6248d9ce73071bdf26cea5e0eb7b54c778ca8be5f706b6d3fa8330f12	✗

Host Behavior

Type	Count
Module	44
File	1171
System	497
Process	29

Type	Count
Registry	33464
Environment	1
-	13
Mutex	15630
-	3
COM	2

Process #72: hcpmumu.exe

ID	72
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintRenderAnimation
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85785, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	208.80s
Return Code	Unknown
PID	784
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #73: hcpmumu.exe

ID	73
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintSetAlpha
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85971, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	208.61s
Return Code	Unknown
PID	3412
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #74: hcpmumu.exe

ID	74
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintStopAllAnimations
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 86413, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	208.17s
Return Code	Unknown
PID	3420
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #75: hcpmumu.exe

ID	75
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintUnInit
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 86706, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	207.88s
Return Code	Unknown
PID	3368
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #76: hcpmumu.exe

ID	76
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=CloseThemeData
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 86780, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	207.80s
Return Code	Unknown
PID	3448
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #77: hcpmumu.exe

ID	77
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeBackground
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 86996, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	207.59s
Return Code	Unknown
PID	3408
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #78: hcpmumu.exe

ID	78
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeBackgroundEx
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87287, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	207.30s
Return Code	Unknown
PID	3492
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #79: hcpmumu.exe

ID	79
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeEdge
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87492, Reason: Child Process
Unmonitor End Time	End Time: 248546, Reason: Terminated
Monitor duration	161.05s
Return Code	0
PID	3504
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #80: hcpmumu.exe

ID	80
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeIcon
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87615, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	206.97s
Return Code	Unknown
PID	3620
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #81: hcpmumu.exe

ID	81
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeParentBackground
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87735, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	206.85s
Return Code	Unknown
PID	3544
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #82: hcpmumu.exe

ID	82
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeParentBackgroundEx
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87820, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	206.76s
Return Code	Unknown
PID	3536
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #83: hcpmumu.exe

ID	83
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeText
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87922, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	206.66s
Return Code	Unknown
PID	3516
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #84: hcpmumu.exe

ID	84
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeTextEx
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88218, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	206.37s
Return Code	Unknown
PID	3632
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #85: hcpmumu.exe

ID	85
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EnableThemeDialogTexture
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88309, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	206.27s
Return Code	Unknown
PID	3500
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #86: hcpmumu.exe

ID	86
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EnableTheming
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88428, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	206.16s
Return Code	Unknown
PID	3708
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #87: hcpmumu.exe

ID	87
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EndBufferedAnimation
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88620, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	205.96s
Return Code	Unknown
PID	3740
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #88: hcpmumu.exe

ID	88
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EndBufferedPaint
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88703, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	205.88s
Return Code	Unknown
PID	3148
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #89: hcpmumu.exe

ID	89
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EndPanningFeedback
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88891, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	205.69s
Return Code	Unknown
PID	3200
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #90: hcpmumu.exe

ID	90
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetBufferedPaintBits
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88959, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	205.62s
Return Code	Unknown
PID	3120
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #91: hcpmumu.exe

ID	91
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetBufferedPaintDC
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89291, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	205.29s
Return Code	Unknown
PID	3508
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #92: hcpmumu.exe

ID	92
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetBufferedPaintTargetDC
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89343, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	205.24s
Return Code	Unknown
PID	3796
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #93: hcpmumu.exe

ID	93
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetBufferedPaintTargetRect
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89438, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	205.15s
Return Code	Unknown
PID	3656
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #94: hcpmumu.exe

ID	94
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetCurrentThemeName
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89621, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	204.96s
Return Code	Unknown
PID	3652
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #95: hcpmumu.exe

ID	95
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeAppProperties
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89699, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	204.88s
Return Code	Unknown
PID	3824
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #96: hcpmumu.exe

ID	96
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBackgroundContentRect
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89884, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	204.70s
Return Code	Unknown
PID	3108
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #97: hcpmumu.exe

ID	97
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBackgroundExtent
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89951, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	204.63s
Return Code	Unknown
PID	3088
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #98: hcpmumu.exe

ID	98
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBackgroundRegion
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90194, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	204.39s
Return Code	Unknown
PID	3812
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #99: hcpmumu.exe

ID	99
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBitmap
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90266, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	204.32s
Return Code	Unknown
PID	3860
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #100: hcpmumu.exe

ID	100
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBool
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90439, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	204.14s
Return Code	Unknown
PID	3904
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #101: hcpmumu.exe

ID	101
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeColor
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90498, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	204.09s
Return Code	Unknown
PID	3940
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #102: hcpmumu.exe

ID	102
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeDocumentationProperty
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90614, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	203.97s
Return Code	Unknown
PID	3976
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #103: hcpmumu.exe

ID	103
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeEnumValue
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90802, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	203.78s
Return Code	Unknown
PID	4012
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #104: hcpmumu.exe

ID	104
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeFilename
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90913, Reason: Child Process
Unmonitor End Time	End Time: 199343, Reason: Terminated
Monitor duration	108.43s
Return Code	0
PID	4048
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #105: hcpmumu.exe

ID	105
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeFont
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91091, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	203.49s
Return Code	Unknown
PID	4084
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #106: hcpmumu.exe

ID	106
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeInt
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91235, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	203.35s
Return Code	Unknown
PID	3076
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #107: hcpmumu.exe

ID	107
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeIntList
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92040, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	202.54s
Return Code	Unknown
PID	1728
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #108: hcpmumu.exe

ID	108
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeMargins
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92323, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	202.26s
Return Code	Unknown
PID	3264
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #109: hcpmumu.exe

ID	109
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeMetric
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93769, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	200.81s
Return Code	Unknown
PID	3596
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #110: hcpmumu.exe

ID	110
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemePartSize
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 94494, Reason: Child Process
Unmonitor End Time	End Time: 282956, Reason: Terminated
Monitor duration	188.46s
Return Code	0
PID	3248
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	171
Mutex	4

Process #111: hcpmumu.exe

ID	111
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemePosition
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95911, Reason: Child Process
Unmonitor End Time	End Time: 193255, Reason: Terminated
Monitor duration	97.34s
Return Code	0
PID	384
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #112: hcpmumu.exe

ID	112
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemePropertyOrigin
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96348, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	198.24s
Return Code	Unknown
PID	1580
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #113: hcpmumu.exe

ID	113
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeRect
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 98011, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	196.57s
Return Code	Unknown
PID	2164
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #114: hcpmumu.exe

ID	114
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeStream
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 99809, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	194.77s
Return Code	Unknown
PID	2188
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #115: hcpmumu.exe

ID	115
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeString
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 100164, Reason: Child Process
Unmonitor End Time	End Time: 213437, Reason: Terminated
Monitor duration	113.27s
Return Code	0
PID	2548
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #116: hcpmumu.exe

ID	116
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysBool
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 101607, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	192.98s
Return Code	Unknown
PID	2644
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #117: hcpmumu.exe

ID	117
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysColor
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 101911, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	192.67s
Return Code	Unknown
PID	2680
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #118: hcpmumu.exe

ID	118
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysColorBrush
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103439, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	191.14s
Return Code	Unknown
PID	2788
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #119: hcpmumu.exe

ID	119
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysFont
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103969, Reason: Child Process
Unmonitor End Time	End Time: 216516, Reason: Terminated
Monitor duration	112.55s
Return Code	0
PID	3752
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	66
Mutex	4

Process #120: hcpmumu.exe

ID	120
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysInt
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 104885, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	189.70s
Return Code	Unknown
PID	3736
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #121: hcpmumu.exe

ID	121
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysSize
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 105125, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	189.46s
Return Code	Unknown
PID	3764
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #122: hcpmumu.exe

ID	122
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysString
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 108303, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	186.28s
Return Code	Unknown
PID	3828
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #123: hcpmumu.exe

ID	123
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeTextExtent
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 108597, Reason: Child Process
Unmonitor End Time	End Time: 212507, Reason: Terminated
Monitor duration	103.91s
Return Code	0
PID	3404
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #124: hcpmumu.exe

ID	124
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeTextMetrics
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 121105, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	173.48s
Return Code	Unknown
PID	3728
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #125: hcpmumu.exe

ID	125
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeTransitionDuration
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133770, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	160.81s
Return Code	Unknown
PID	768
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #126: hcpmumu.exe

ID	126
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetWindowTheme
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134612, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	159.97s
Return Code	Unknown
PID	568
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #127: hcpmumu.exe

ID	127
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=HitTestThemeBackground
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134980, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	159.60s
Return Code	Unknown
PID	4000
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #128: eudcedit.exe

ID	128
File Name	c:\windows\system32\eudcedit.exe
Command Line	C:\Windows\system32\eudcedit.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 135325, Reason: Child Process
Unmonitor End Time	End Time: 138756, Reason: Terminated
Monitor duration	3.43s
Return Code	3221226540
PID	4072
Parent PID	1116
Bitness	64 Bit

Process #129: hcpmumu.exe

ID	129
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsAppThemed
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 135478, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	159.10s
Return Code	Unknown
PID	196
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #130: hcpmumu.exe

ID	130
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsCompositionActive
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 136361, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	158.22s
Return Code	Unknown
PID	1544
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #131: hcpmumu.exe

ID	131
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsThemeActive
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 137648, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	156.94s
Return Code	Unknown
PID	1268
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #132: hcpmumu.exe

ID	132
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsThemeBackgroundPartiallyTransparent
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 138243, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	156.34s
Return Code	Unknown
PID	3592
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #133: hcpmumu.exe

ID	133
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsThemeDialogTextureEnabled
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 138751, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	155.83s
Return Code	Unknown
PID	3580
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #134: hcpmumu.exe

ID	134
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsThemePartDefined
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 138951, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	155.63s
Return Code	Unknown
PID	3332
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	134

Process #135: hcpmumu.exe

ID	135
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=OpenThemeData
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 139138, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	155.44s
Return Code	Unknown
PID	3236
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #136: hcpmumu.exe

ID	136
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=OpenThemeDataEx
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 139627, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	154.96s
Return Code	Unknown
PID	916
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #137: hcpmumu.exe

ID	137
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=SetThemeAppProperties
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140139, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	154.44s
Return Code	Unknown
PID	2704
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	18
File	112
Environment	1

Process #138: hcpmumu.exe

ID	138
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=SetWindowTheme
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140454, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	154.13s
Return Code	Unknown
PID	3748
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #139: hcpmumu.exe

ID	139
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=SetWindowThemeAttribute
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140983, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	153.60s
Return Code	Unknown
PID	304
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #140: hcpmumu.exe

ID	140
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=ThemeInitApiHook
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141241, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	153.34s
Return Code	Unknown
PID	1676
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #141: hcpmumu.exe

ID	141
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=UpdatePanningFeedback
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141728, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	152.85s
Return Code	Unknown
PID	896
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #142: eudcedit.exe

ID	142
File Name	c:\windows \system32\eudcedit.exe
Command Line	"C:\Windows \system32\eudcedit.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 141786, Reason: Child Process
Unmonitor End Time	End Time: 144207, Reason: Terminated
Monitor duration	2.42s
Return Code	3221226540
PID	932
Parent PID	1116
Bitness	64 Bit

Process #143: hcpmumu.exe

ID	143
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#1 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141923, Reason: Child Process
Unmonitor End Time	End Time: 255408, Reason: Terminated
Monitor duration	113.48s
Return Code	0
PID	3136
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	66
Mutex	1

Process #144: hcpmumu.exe

ID	144
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#10 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 143035, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	151.55s
Return Code	Unknown
PID	1816
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #145: perfmon.exe

ID	145
File Name	c:\windows\system32\perfmon.exe
Command Line	C:\Windows\system32\perfmon.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 143165, Reason: Child Process
Unmonitor End Time	End Time: 146617, Reason: Terminated
Monitor duration	3.45s
Return Code	3221226540
PID	1076
Parent PID	1116
Bitness	64 Bit

Process #146: hcpmumu.exe

ID	146
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#11 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 143327, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	151.26s
Return Code	Unknown
PID	1860
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	68

Process #147: hcpmumu.exe

ID	147
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#13 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 144835, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	149.75s
Return Code	Unknown
PID	440
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #148: hcpmumu.exe

ID	148
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#14 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 145341, Reason: Child Process
Unmonitor End Time	End Time: 294583, Reason: Terminated by Timeout
Monitor duration	149.24s
Return Code	Unknown
PID	900
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #149: hcpmumu.exe

ID	149
File Name	c:\users\keecfmwgj\desktop\hcpmumu.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#15 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146018, Reason: Child Process
Unmonitor End Time	End Time: 284563, Reason: Terminated
Monitor duration	138.54s
Return Code	0
PID	672
Parent PID	3668
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	66

Process #150: systempropertiescomputername.exe

ID	150
File Name	c:\windows\system32\systempropertiescomputername.exe
Command Line	C:\Windows\system32\SystemPropertiesComputerName.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 146277, Reason: Child Process
Unmonitor End Time	End Time: 148890, Reason: Terminated
Monitor duration	2.61s
Return Code	3221226540
PID	2060
Parent PID	1116
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070	C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll, C:\Users\kEecfMwgj\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll	Sample File	1196.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
8704f443c944264d96f3f0a6df5a0b42fc6e34720d77cdf5a10834c9af2ec891	C:\Users\kEecfMwgj\AppData\Local\ekwn\DUI70.dll, C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\PrivacIE\txGHoCV75Mr\DUI70.dll	Dropped File	1404.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	MALICIOUS
cea138e5f0a20c09ef1ddd139147dd37e30782b40a1a823e3eac7ab6d557c5a4	C:\Users\kEecfMwgj\AppData\Local\H15dP8\sqmapi.dll	Dropped File	1200.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
1f64118bdc3515e8e9fce6ad182f6d0c8a6528d638fedb4901a6152cde4c7cde	\\?\C:\Windows\system32\eudcedit.exe	Dropped File	351.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	SUSPICIOUS
dd94bf73f0e3652b76cfb774b419ceaa2082bc7f30cc34e28dfa51952fa9ccb5	C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\PrivacIE\txGHoCV75Mr\sethc.exe, C:\Users\kEecfMwgj\AppData\Local\ekwn\sethc.exe	Dropped File	272.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	SUSPICIOUS
2d970fea1e7ebc4c9bae287309fa032cb2ac90323c0cdb49ca9593dc7d074c98	c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	50 bytes	application/octet-stream	-	CLEAN
1fcae1eeb5b5cf627c786bbe8a38f3d2af7a3f2c56ac850a830909db3aa93811	\\?\C:\Windows\system32\MFC42u.dll	Dropped File	1325.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	CLEAN
fd5484565f50a094dafe9c830520f122140ee6b4bc5b1b2e325f17819d4e37f9	\\?\C:\Windows\system32\MFPlat.DLL	Dropped File	422.00 KB	application/vnd.microsoft.portable-executable	-	CLEAN
6832ffa7cd2d0a92eccbea7e90b8e344f6dc808f2c3cc0a93859a45057028937	\\?\C:\Windows\system32\rrinstaller.exe	Dropped File	54.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
f8f3f429ad8ca958bd7f06fd7c57b6c4a5a7d3f50a189c346f4dd4c2cc35e0cb	c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	1.40 KB	application/octet-stream	-	CLEAN
72275404c470b62a5ff49013e3f952d9480afd5c7e45b6c504235823da4894ae	c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	1.40 KB	application/octet-stream	-	CLEAN
c618f7e6248d9ce73071bdf26cea5e0eb7b54c778ca8be5f706b6d3fa8330f12	c:\users\keecfmwgj\appdata\roaming\microsoft\crypto\rsa\s-1-5-21-4219442223-4223814209-3835049652-1000\4fe4574abf1bcb0f6ed6a78aa750fb2c_b9c8f16e-2e51-4052-9ecb-f86ae5d96ef6	Dropped File	1.42 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\tmpw9sqrl_v	Accessed File	Access, Read	CLEAN
C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN
C:\Windows\system32\netsh.exe	Accessed File	Access	CLEAN
C:\Windows\system32\diskperf.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\diskraid.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\Dism.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dispdiag.exe	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\DisplaySwitch.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\djoin.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dllhost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dllhst3g.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dnscacheugc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\doskey.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dpapimig.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\DpiScaling.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dpnsvr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\driverquery.exe	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Windows Media Player\outlook.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\drvinst.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dvdplay.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dvdupgrd.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dwm.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\DWWIN.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\dxdiag.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\Dxpserver.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\Eap3Host.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\efsui.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\EhStorAuthn.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\esentutl.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\eudcedit.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MFC42u.dll	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\PrivacIE\txGHoCV75Mr	Accessed File	Access, Create	CLEAN
\\?\C:\Windows \system32\	Accessed File	Access, Delete, Create	CLEAN
\\?\C:\Windows \	Accessed File	Access, Delete, Create	CLEAN

File Name	Category	Operations	Verdict
\\?\C:\Windows \system32\MFC42u.dll	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Windows\system32\PING.EXE	Accessed File	Access	CLEAN
C:\Windows\system32\GettingStarted.exe	Accessed File	Access	CLEAN
C:\Windows\system32\pcalua.exe	Accessed File	Access	CLEAN
\\?\C:\Windows \system32\eudcedit.exe	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Windows\system32\taskeng.exe	Accessed File	Access	CLEAN
C:\Windows\system32\tzutil.exe	Accessed File	Access	CLEAN
C:\Windows\system32\charmap.exe	Accessed File	Access	CLEAN
C:\Windows\system32\chgusr.exe	Accessed File	Access	CLEAN
C:\Windows\system32\mpnotify.exe	Accessed File	Access	CLEAN
C:\Windows\system32\poqexec.exe	Accessed File	Access	CLEAN
C:\Windows\system32\PkgMgr.exe	Accessed File	Access	CLEAN
C:\Windows\system32\wininit.exe	Accessed File	Access	CLEAN
C:\Windows\system32\SearchProtocolHost.exe	Accessed File	Access	CLEAN
C:\Windows\system32\TsWpfWrp.exe	Accessed File	Access	CLEAN
C:\Windows\system32\chglogon.exe	Accessed File	Access	CLEAN
C:\Windows\system32\perfmon.exe	Accessed File	Access	CLEAN
C:\Windows\system32\SystemPropertiesComputerName.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\shutdown.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RMActivate_ssp_isv.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wimserv.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\sethc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\DUI70.dll	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\system\msmapi\1033\msmapi32.dll	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Local\ekwn\	Accessed File	Access, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\ekwn\DUI70.dll	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\ekwn\sethc.exe	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\PrivacIE\txGHoCV75Mr\DUI70.dll	Dropped File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\PrivacIE\txGHoCV75Mr\sethc.exe	Dropped File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\MZMU	Accessed File	Access, Create	CLEAN
C:\Windows\system32\verclsid.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\Register-CimProvider.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\comp.exe	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\conhost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RegisterIEPKEYs.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\regsvr32.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\spreview.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rekeywiz.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\sqmapi.dll	Accessed File	Access, Read	CLEAN
C:\Windows\system32\relog.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RelPost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\repair-bde.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\replace.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\reset.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\resmon.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RMActivate.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RMActivate_isv.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RMActivate_ssp.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RmClient.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\Robocopy.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ROUTE.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RpcPing.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rrinstaller.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MFPlat.DLL	Accessed File	Access, Read	CLEAN
\\?\C:\Windows \system32\MFPlat.DLL	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Windows \system32\rrinstaller.exe	Dropped File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\H15dP8\	Accessed File	Access, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\H15dP8\sqmapi.dll	Accessed File	Access, Write, Create	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{bbfa96fb-03e2-244a-e13e-86541d1b182b}	access	hcpmumu.exe	CLEAN
{ba62725d-6184-50d2-b706-2d7b865dd82b}	access	hcpmumu.exe	CLEAN
{33ff21cb-ff8c-80f2-435a-9f14e40fde6b}	access	explorer.exe	CLEAN
{ad66cb9e-7ae1-701b-6069-4a7b793507ac}	access	explorer.exe	CLEAN
{6ae03f50-7a2d-c6e9-ca75-492d6e54c058}	access	explorer.exe	CLEAN
{13e06e4b-2481-b368-8f42-2212f1d59822}	access	explorer.exe	CLEAN
{65c8ac9c-25ba-82f3-37f2-3fe3857eeb82}	access	explorer.exe	CLEAN
{858c4289-63b2-a2dd-c583-194c14978d8f}	access	explorer.exe	CLEAN
{247e511c-baa2-d42e-5dea-e537316b6ab0}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{445e88c9-0ef7-f980-790a-73297e705b1f}	access	explorer.exe	CLEAN
{0a229cb1-bb57-9bd8-01b2-31e4b7cbf515}	access	explorer.exe	CLEAN
{4126ed8b-1649-b296-c1a8-6a31b31e936e}	access	explorer.exe	CLEAN
{50a49a66-4b11-240c-8816-398b6bd70ed6}	access	explorer.exe	CLEAN
{2d7bccd8-c070-8723-c092-31c38068d849}	access	explorer.exe	CLEAN
{aa8eec2a-1624-d913-f987-9558cbeacce1}	access	explorer.exe	CLEAN
{9124fc0f-aad1-69ca-f087-b6f4b4618452}	access	explorer.exe	CLEAN
{3424d05e-75d9-fa9d-601e-13c62053c3c5}	access	explorer.exe	CLEAN
{91af0379-7553-2b9a-1768-bb6f0281e3e9}	access	explorer.exe	CLEAN
{821b3d72-6d45-a55c-2ff2-657dbbeba155}	access	explorer.exe	CLEAN
{87870dec-87d4-3464-8983-690c1429eba9}	access	explorer.exe	CLEAN
{9a382e7d-fa1b-dd43-a0dd-294ace4cebfc}	access	explorer.exe	CLEAN
{8da6b341-b6ae-4ed6-a4db-b8d7a21d3ce2}	access	explorer.exe	CLEAN
{02d851a8-f7cd-b455-df45-71a402a6edbc}	access	explorer.exe	CLEAN
{6ba32bba-4e96-f5a2-050a-03757c53defe}	access	explorer.exe	CLEAN
{c048b0eb-b8ca-7103-8f33-90bb9cc094e1}	access	explorer.exe	CLEAN
{c7dddfcc-fb68-9c80-b7a6-092779936187}	access	explorer.exe	CLEAN
{b59073af-3f1e-9c2e-af6d-076c62047c1a}	access	explorer.exe	CLEAN
{7f2d86d4-0955-2066-882a-14cbed49896d}	access	explorer.exe	CLEAN
{018d1282-98a9-7481-13d2-c8f764fa5048}	access	explorer.exe	CLEAN
{09994fee-51eb-0a96-ec56-cae7e3daecec}	access	explorer.exe	CLEAN
{29021d34-bd3b-66d0-b71b-552d729d9a4a}	access	explorer.exe	CLEAN
{b407468a-fc89-c63a-2493-e889c30daef8}	access	explorer.exe	CLEAN
{e4e8cfa9-4e2a-ffb0-a03d-bd662f479cc0}	access	explorer.exe	CLEAN
{baf9aa31-a0c9-f808-5a2b-06d9f2a620eb}	access	explorer.exe	CLEAN
{6d4ceb18-7d30-0d62-7553-417a12d1ddd9}	access	explorer.exe	CLEAN
{b049459e-3c89-2588-306b-77da13f498b6}	access	explorer.exe	CLEAN
{7150daae-191d-d79c-f695-5cf339e31f5f}	access	explorer.exe	CLEAN
{32c5cb54-a427-4241-90fb-bc414e1c9eff}	access	explorer.exe	CLEAN
{cb59f0a7-5035-4c73-c0b0-ac2839924f2a}	access	explorer.exe	CLEAN
{89977e79-7c98-ab0d-42f0-94b76fc1b777}	access	explorer.exe	CLEAN
{b4e9fa2e-e01d-98cf-6d18-53806885dfda}	access	explorer.exe	CLEAN
{0f5fef32-f8f1-ad75-9bdb-8e355695ddde}	access	explorer.exe	CLEAN
{19c49204-25e6-7fde-2df5-abe7c9f8c579}	access	explorer.exe	CLEAN
{5956720b-c5d2-6758-edbe-d5ccba607a9e}	access	explorer.exe	CLEAN
{0402eb8b-f148-c7ad-ffa2-b74b9de48502}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{d3bb376e-cd4b-063e-153f-92e67d6bd5b4}	access	explorer.exe	CLEAN
{b6d3b4a4-6cfa-1231-4ff7-0ba6415393a1}	access	explorer.exe	CLEAN
{3cae724b-3276-fc13-d3ab-c6ed41b8b612}	access	explorer.exe	CLEAN
{eac231ca-bef5-dfa4-9a95-7f54db289ede}	access	explorer.exe	CLEAN
{0f9c1045-a44b-fd0b-b460-2ee3d5078a43}	access	explorer.exe	CLEAN
{9cbd6054-a191-e3b6-414b-b0e3134c7396}	access	explorer.exe	CLEAN
{e71f6f75-a4f4-9f9c-a01e-a74ad62c7006}	access	explorer.exe	CLEAN
{ab0794eb-96ed-13f3-14b9-6dcb56087a93}	access	explorer.exe	CLEAN
{6cec2c43-71e1-cfd3-97c6-43608f834a1d}	access	explorer.exe	CLEAN
{9d58babe-8b5c-503e-4f0d-14a0382ba493}	access	explorer.exe	CLEAN
{0e584ce2-6304-09b0-d7f9-30289afde72e}	access	explorer.exe	CLEAN
{30394b09-8a16-7548-c258-89a55b260289}	access	explorer.exe	CLEAN
{6361c904-b160-d26c-c724-a5012e7bf0e4}	access	explorer.exe	CLEAN
{831cdbe1-2408-1e5a-7415-c4e69eafebc3}	access	explorer.exe	CLEAN
{58686fd1-c00c-aac7-11ae-1d948bcfdeef}	access	explorer.exe	CLEAN
{226e5239-0a41-4cee-fd93-21c269356f14}	access	explorer.exe	CLEAN
{f7e425e9-2c2e-be2f-0d5b-2323085b4198}	access	explorer.exe	CLEAN
{ac2c4635-574f-aca9-e5d1-5d19d708afb3}	access	explorer.exe	CLEAN
{4b4afda5-e2b9-d796-ffdf-e673864c9758}	access	explorer.exe	CLEAN
{f19b14a2-88dd-47d7-1f4a-7d683d327e57}	access	explorer.exe	CLEAN
{981764c6-b91b-534f-d7e6-2632ffbe9834}	access	explorer.exe	CLEAN
{123791ad-06f4-9671-c776-3422a38fcfb4}	access	explorer.exe	CLEAN
{c1784757-d0b7-8962-6fc0-1b7a8cf6ca0c}	access	explorer.exe	CLEAN
{3f892d5f-8788-06ab-b7d5-7a7c5b0b83cd}	access	explorer.exe	CLEAN
{e491d418-bd3e-f65e-2664-43d1dc901091}	access	explorer.exe	CLEAN
{f27483b5-751e-0337-6b4f-204e0dbb68a4}	access	explorer.exe	CLEAN
{a85e5bb1-210f-eaa7-93a8-252b8f88d4ba}	access	explorer.exe	CLEAN
{04ca13c3-0d16-b840-15ce-c3199f6d6829}	access	explorer.exe	CLEAN
{dc18897b-2710-1798-733d-efbc6923d540}	access	explorer.exe	CLEAN
{49a07584-0681-527e-eea4-a464367a4642}	access	explorer.exe	CLEAN
{01f24027-5822-0b07-51de-a8815e01c33d}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
-	access, create	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE	access	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	hcpmumu.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	access, read	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	hcpmumu.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	hcpmumu.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	access, read	hcpmumu.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	access, read	hcpmumu.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	access, read	hcpmumu.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{79665E8E-4365-6B8F-DA00-D0B828D4FEEC}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{40B0E89D-864F-7B36-E7BA-299B4295A387}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{658B8EB4-E886-BA66-3237-86E65BEB1E60}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5F4CA0A3-A910-CB32-91E3-65C4C90E354E}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{DDF3826C-BF0E-D11A-3ABF-ED0CA6E11CF7}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{30E6C3C1-A382-20F0-0569-B60929C9A348}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A6D924EE-443F-B6B2-7A21-B2F64E00F2EC}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{961EFF9D-BB8C-3A05-CE8E-AB9FF0211A1C}\ShellFolder	access, create	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F7EBB03F-F792-B7CA-EA56-C982AFE2C903}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{09EBA979-3626-0867-E995-47290ADFECDE}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{FFF9BCDE-8935-C1CF-14B1-3FE011D23CE0}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BD5CE409-7117-60F0-7C10-5E495810A4FD}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E8C1261E-A3EA-CD08-28CD-4DBC093C573E}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{09EBA979-3626-0867-E995-47290ADFECDE}\ShellFolder\{C9CFDF7A-FD69-B9C3-1440-82584A74B213}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{961EFF9D-BB8C-3A05-CE8E-AB9FF0211A1C}\ShellFolder\{11F918D5-403B-27A8-F4C2-B74261C71AD8}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9A97E6A9-29FC-3B68-4B33-94C2960CC881}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4663F19F-2DFA-ECF3-DDFB-370E2E26C4FA}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{49E122CC-49ED-565C-A828-344EDBE840A6}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BBF565DE-9A24-D768-2CD0-543EF86AD28F}\ShellFolder	access, create	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\InstallDate	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DXM_Runtime	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40	access	explorer.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MPlayer2	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ProPlusRetail - en-us\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{16735AF7-1D8D-3681-94A5-C578A61EC832}	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{16735AF7-1D8D-3681-94A5-C578A61EC832}\DisplayName	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{16735AF7-1D8D-3681-94A5-C578A61EC832}\DisplayVersion	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{1D8E6291-B0D5-35EC-8441-6616F567A0F7}	access	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder\{0CDCFD74-9368-FB31-4629-21EB5AA8E73C}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder\InstallDate	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\InstallDate	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh	access	netsh.exe	CLEAN

Process

Process Name	Commandline	Verdict
sethc.exe	C:\Users\kEecfMwgj\AppData\Local\ekwn\sethc.exe	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpw9sqrl_v" /s	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#1	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#10	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#11	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#13	CLEAN

Process Name	Commandline	Verdict
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#14	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#15	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#16	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#17	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#18	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#19	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#2	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#20	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#21	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#22	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#23	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#24	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#25	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#26	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#27	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#28	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#29	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#3	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#30	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#31	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#32	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#33	CLEAN

Process Name	Commandline	Verdict
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#34	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#35	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#36	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#4	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#43	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#44	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#45	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#46	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#48	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#49	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#50	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#60	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#62	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#63	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#64	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#65	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#66	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#67	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#68	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#69	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#7	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#72	CLEAN

Process Name	Commandline	Verdict
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#73	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#74	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#75	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#76	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#77	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#78	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#79	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#8	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#80	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#81	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#82	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#83	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#84	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#85	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#86	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#9	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BeginBufferedAnimation	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BeginBufferedPaint	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BeginPanningFeedback	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintClear	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintInit	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintRenderAnimation	CLEAN

Process Name	Commandline	Verdict
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintSetAlpha	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintStopAllAnimations	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=BufferedPaintUnInit	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=CloseThemeData	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeBackground	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeBackgroundEx	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeEdge	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeIcon	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeParentBackground	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeParentBackgroundEx	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeText	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=DrawThemeTextEx	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EnableThemeDialogTexture	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EnableTheming	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EndBufferedAnimation	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EndBufferedPaint	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=EndPanningFeedback	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetBufferedPaintBits	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetBufferedPaintDC	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetBufferedPaintTargetDC	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetBufferedPaintTargetRect	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetCurrentThemeName	CLEAN

Process Name	Commandline	Verdict
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeAppProperties	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBackgroundContentRect	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBackgroundExtent	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBackgroundRegion	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBitmap	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeBool	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeColor	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeDocumentationProperty	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeEnumValue	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeFilename	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeFont	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeInt	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeIntList	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeMargins	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeMetric	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemePartSize	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemePosition	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemePropertyOrigin	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeRect	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeStream	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeString	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysBool	CLEAN

Process Name	Commandline	Verdict
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysColor	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysColorBrush	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysFont	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysInt	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysSize	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeSysString	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeTextExtent	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeTextMetrics	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetThemeTransitionDuration	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=GetWindowTheme	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=HitTestThemeBackground	CLEAN
eudcedit.exe	C:\Windows\system32\eudcedit.exe	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsAppThemed	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsCompositionActive	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsThemeActive	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsThemeBackgroundPartiallyTransparent	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsThemeDialogTextureEnabled	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=IsThemePartDefined	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=OpenThemeData	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=OpenThemeDataEx	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=SetThemeAppProperties	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=SetWindowTheme	CLEAN

Process Name	Commandline	Verdict
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=SetWindowThemeAttribute	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=ThemeInitApiHook	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=UpdatePanningFeedback	CLEAN
eudcedit.exe	"C:\Windows \system32\eudcedit.exe"	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#1 /fn_args="0"	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#10 /fn_args="0"	CLEAN
perfmon.exe	C:\Windows\system32\perfmon.exe	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#11 /fn_args="0"	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#13 /fn_args="0"	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#14 /fn_args="0"	CLEAN
hcpmumu.exe	"C:\Users\kEecfMwgj\Desktop\HcPmuMU.exe" /dll="C:\Users\KEECFM~1\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll" /fn_id=#15 /fn_args="0"	CLEAN

Reduced dataset

YARA / AV

Antivirus (9)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\Desktop\97058d4465daae2446886d425d9a8215df518e6845e8a4bedb30acea4e8d2070.exe.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\AppData\Local\ekwn\DUI70.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\AppData\Local\H15dP8\sqmapi.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 08:04:18+00:00
Built-in AV Database Records	10477558

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH

User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows