MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll**
ID	#2782917
MD5	a75be08d11b5028b6e0fa8be59676599
SHA1	c47a48e04dc10641df07dba7dbbb73602e6615aa
SHA256	7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a
File Size	2056.00 KB
Report Created	2021-09-28 14:12 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (17 rules, 161 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	14	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\fg0b\VERSION.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\dOFgn\VERSION.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\VERSION.dll as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #2) roprri.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #14) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #24) roprri.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #19) roprri.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #33) roprri.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #51) roprri.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #14) explorer.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #135) spreview.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #30) roprri.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #112) roprri.exe as "Gen:Variant.Mikey.113998".		
4/5	Injection	Modifies control flow of another process	2	-
	• (Process #2) roprri.exe alters context of (process #14) explorer.exe. • (Process #11) roprri.exe alters context of (process #14) explorer.exe.			
4/5	Privilege Escalation	Creates elevated child process	1	-
	• (Process #14) explorer.exe creates (process #152) windowsanytimeupgrade.exe with elevated privileges.			
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Data Collection	Reads sensitive mail data	1	-
	• (Process #14) explorer.exe tries to read sensitive data of mail application "The Bat!" by file.			
2/5	Data Collection	Reads sensitive browser data	1	-
	• (Process #14) explorer.exe tries to read sensitive data of web browser "Internet Explorer / Edge" by file.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #14) explorer.exe has a thread which sleeps more than 5 minutes.			
2/5	Hide Tracks	Deletes file after execution	4	-
	• (Process #14) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\local\fg0b\spreview.exe". • (Process #14) explorer.exe deletes executed executable "c:\windows \system32\windowsanytimeupgrade.exe". • (Process #14) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\local\dofgn\cmstp.exe". • (Process #14) explorer.exe deletes executed executable "c:\users\keecfmwgj\appdata\local\ctp9rydd\ui0detect.exe".			
1/5	Discovery	Reads system data	14	-

Score	Category	Operation	Count	Classification
		• (Process #2) roprri.exe reads the Windows installation date from registry. • (Process #4) roprri.exe reads the Windows installation date from registry. • (Process #3) roprri.exe reads the Windows installation date from registry. • (Process #7) roprri.exe reads the Windows installation date from registry. • (Process #6) roprri.exe reads the Windows installation date from registry. • (Process #9) roprri.exe reads the Windows installation date from registry. • (Process #5) roprri.exe reads the Windows installation date from registry. • (Process #8) roprri.exe reads the Windows installation date from registry. • (Process #10) roprri.exe reads the Windows installation date from registry. • (Process #11) roprri.exe reads the Windows installation date from registry. • (Process #12) roprri.exe reads the Windows installation date from registry. • (Process #13) roprri.exe reads the Windows installation date from registry. • (Process #14) explorer.exe reads the Windows installation date from registry. • (Process #16) roprri.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	84	-

- (Process #2) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #4) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #2) roprri.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #3) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #7) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #6) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #5) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #8) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #9) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #10) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #11) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #12) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #13) roprri.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #14) explorer.exe creates mutex with name "{bbfa96fb-03e2-244a-e13e-86541d1b182b}".
- (Process #11) roprri.exe creates mutex with name "{ba62725d-6184-50d2-b706-2d7b865dd82b}".
- (Process #14) explorer.exe creates mutex with name "{33ff21cb-ff8c-80f2-435a-9f14e40fde6b}".
- (Process #14) explorer.exe creates mutex with name "{ad66cb9e-7ae1-701b-6069-4a7b793507ac}".
- (Process #14) explorer.exe creates mutex with name "{6ae03f50-7a2d-c6e9-ca75-492d6e54c058}".
- (Process #14) explorer.exe creates mutex with name "{13e06e4b-2481-b368-8f42-2212f1d59822}".
- (Process #14) explorer.exe creates mutex with name "{65c8ac9c-25ba-82f3-37f2-3fe3857eeb82}".
- (Process #14) explorer.exe creates mutex with name "{2abfad8b-306f-ae21-21b6-6871f4adee91}".
- (Process #14) explorer.exe creates mutex with name "{0f9efc60-2714-9348-bba5-dc278ba33013}".
- (Process #14) explorer.exe creates mutex with name "{0fbd56d3-f3b8-edce-f394-613d71047fdd}".
- (Process #14) explorer.exe creates mutex with name "{58078409-4d48-58c2-bbac-98f6809a0389}".
- (Process #14) explorer.exe creates mutex with name "{6deb4144-d426-afcd-96ba-1febb5348581}".
- (Process #14) explorer.exe creates mutex with name "{14a53b80-b6de-81e7-ed6c-2690e7bf017c}".
- (Process #14) explorer.exe creates mutex with name "{93f0b9bd-750b-91aa-43ce-42ee557a016a}".
- (Process #14) explorer.exe creates mutex with name "{0a229cb1-bb57-9bd8-01b2-31e4b7cbf515}".
- (Process #14) explorer.exe creates mutex with name "{4126ed8b-1649-b296-c1a8-6a31b31e936e}".
- (Process #14) explorer.exe creates mutex with name "{50a49a66-4b11-240c-8816-398b6bd70ed6}".
- (Process #14) explorer.exe creates mutex with name "{2d7bccd8-c070-8723-c092-31c38068d849}".
- (Process #14) explorer.exe creates mutex with name "{0de8b163-06f9-25fe-23a3-578eb97d6c5c}".
- (Process #14) explorer.exe creates mutex with name "{821b3d72-6d45-a55c-2ff2-657dbbeba155}".
- (Process #14) explorer.exe creates mutex with name "{1a7a0e3d-e642-9ee8-a175-339463130825}".
- (Process #14) explorer.exe creates mutex with name "{8da6b341-b6ae-4ed6-a4db-b8d7a21d3ce2}".
- (Process #14) explorer.exe creates mutex with name "{6bc7ca6d-1ff4-948e-acb8-8ace0ff7d262}".
- (Process #14) explorer.exe creates mutex with name "{c048b0eb-b8ca-7103-8f33-90bb9cc094e1}".
- (Process #14) explorer.exe creates mutex with name "{b5d19349-ced1-2973-477a-88f731ebad8b}".
- (Process #14) explorer.exe creates mutex with name "{f6765311-c624-7d20-c394-3057b2a6af46}".
- (Process #14) explorer.exe creates mutex with name "{61445a9f-32ce-1160-e05e-43b687216a6f}".
- (Process #14) explorer.exe creates mutex with name "{89b9ed65-9a3a-f1c2-7aff-062779231709}".
- (Process #14) explorer.exe creates mutex with name "{73aa5908-f17f-645c-b343-cc90c97db734}".
- (Process #14) explorer.exe creates mutex with name "{144d5a95-7221-f17b-879b-9aacc036a420}".
- (Process #14) explorer.exe creates mutex with name "{c84b0bc4-1cbf-767a-1a31-e366c8be89ca}".
- (Process #14) explorer.exe creates mutex with name "{95f84887-1d41-9061-e67e-0279b6af17cd}".
- (Process #14) explorer.exe creates mutex with name "{de76bbb7-2e89-6a07-4cb0-73d47f8864dc}".
- (Process #14) explorer.exe creates mutex with name "{d435791e-8be2-87e1-800b-5c696b52a8f2}".
- (Process #14) explorer.exe creates mutex with name "{8e35622f-5b01-99f1-24ca-7e2c1a23249b}".
- (Process #14) explorer.exe creates mutex with name "{80663b84-20b8-3de1-5999-140e58d67c60}".
- (Process #14) explorer.exe creates mutex with name "{d2e7374a-940d-481d-c27a-a6169257d900}".
- (Process #14) explorer.exe creates mutex with name "{8dcd38ec-186f-5df8-2880-e7d897695e42}".
- (Process #14) explorer.exe creates mutex with name "{dbf760ba-fee3-a258-2c95-0bf2ae6f687c}".
- (Process #14) explorer.exe creates mutex with name "{d8e8ed8e-ed18-d8b2-20c5-9722faa1d0a2}".
- (Process #14) explorer.exe creates mutex with name "{7150daae-191d-d79c-f695-5cf339e31f5f}".
- (Process #14) explorer.exe creates mutex with name "{32c5cb54-a427-4241-90fb-bc414e1c9eff}".
- (Process #14) explorer.exe creates mutex with name "{cb59f0a7-5035-4c73-c0b0-ac2839924f2a}".
- (Process #14) explorer.exe creates mutex with name "{89977e79-7c98-ab0d-42f0-94b76fc1b777}".
- (Process #14) explorer.exe creates mutex with name "{b4e9fa2e-e01d-98cf-6d18-53806885dfda}".
- (Process #14) explorer.exe creates mutex with name "{0f5fef32-f8f1-ad75-9bdb-8e355695ddde}".
- (Process #14) explorer.exe creates mutex with name "{19049204-25e8-7fe2-df5-abe7c9fdc579}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	2	-

- (Process #2) roprri.exe reads from (process #14) explorer.exe.
- (Process #11) roprri.exe reads from (process #14) explorer.exe.

Score	Category	Operation	Count	Classification
1/5	Hide Tracks	Creates process with hidden window	15	-

- (Process #14) explorer.exe starts C:\Windows\system32\WindowsAnytimeUpgrade.exe with a hidden window.
- (Process #14) explorer.exe starts (process #120) spreview.exe with a hidden window.
- (Process #14) explorer.exe starts (process #152) windowsanytimeupgrade.exe with a hidden window.
- (Process #14) explorer.exe starts (process #135) spreview.exe with a hidden window.
- (Process #14) explorer.exe starts C:\Windows\system32\rstrui.exe with a hidden window.
- (Process #14) explorer.exe starts (process #145) cmstp.exe with a hidden window.
- (Process #14) explorer.exe starts (process #161) cmstp.exe with a hidden window.
- (Process #14) explorer.exe starts C:\Windows\system32\SystemPropertiesAdvanced.exe with a hidden window.
- (Process #14) explorer.exe starts C:\Windows\system32\ocsetup.exe with a hidden window.
- (Process #14) explorer.exe starts C:\Windows\system32\odbcad32.exe with a hidden window.
- (Process #14) explorer.exe starts (process #173) ui0detect.exe with a hidden window.
- (Process #14) explorer.exe starts C:\Windows\system32\recdisc.exe with a hidden window.
- (Process #14) explorer.exe starts C:\Windows \system32\recdisc.exe with a hidden window.
- (Process #14) explorer.exe starts (process #189) ui0detect.exe with a hidden window.
- (Process #14) explorer.exe starts (process #194) devicepairingwizard.exe with a hidden window.

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

- (Process #14) explorer.exe creates file "\\?\C:\Windows \system32\slc.dll" in the OS directory.
- (Process #14) explorer.exe creates file "\\?\C:\Windows \system32\WindowsAnytimeUpgrade.exe" in the OS directory.
- (Process #14) explorer.exe creates file "\\?\C:\Windows \system32\ReAgent.dll" in the OS directory.
- (Process #14) explorer.exe creates file "\\?\C:\Windows \system32\recdisc.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 #14) explorer.exe hides 3600 bytes in "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder\{82DD4CB4-45C1-3A12-16A7-34583B57EDDA}".

Score	Category	Operation	Count	Classification
1/5	Execution	Drops PE file	10	-

- (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\fg0b\VERSION.dll".
- (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\dOFgn\VERSION.dll".
- (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\VERSION.dll".
- (Process #14) explorer.exe drops file "\\?\C:\Windows \system32\slc.dll".
- (Process #14) explorer.exe drops file "\\?\C:\Windows \system32\WindowsAnytimeUpgrade.exe".
- (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\fg0b\spreview.exe".
- (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\dOFgn\cmstp.exe".
- (Process #14) explorer.exe drops file "\\?\C:\Windows \system32\ReAgent.dll".
- (Process #14) explorer.exe drops file "\\?\C:\Windows \system32\recdisc.exe".
- (Process #14) explorer.exe drops file "C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\UI0Detect.exe".

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

- Executes dropped file "\\?\C:\Windows \system32\WindowsAnytimeUpgrade.exe".
- Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\fg0b\spreview.exe".
- Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\dOFgn\cmstp.exe".
- Executes dropped file "\\?\C:\Windows \system32\recdisc.exe".
- Executes dropped file "C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\UI0Detect.exe".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #14) explorer.exe resolves 27 API functions by name.			
-	Trusted	Known clean file	6	-
	• File "\\?\C:\Windows \system32\WindowsAnytimeUpgrade.exe" is a known clean file. • File "C:\Users\kEecfMwgj\AppData\Local\fg0b\spreview.exe" is a known clean file. • File "C:\Users\kEecfMwgj\AppData\Local\dOFgn\cmstp.exe" is a known clean file. • File "\\?\C:\Windows \system32\recdisc.exe" is a known clean file. • File "C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\UI0Detect.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

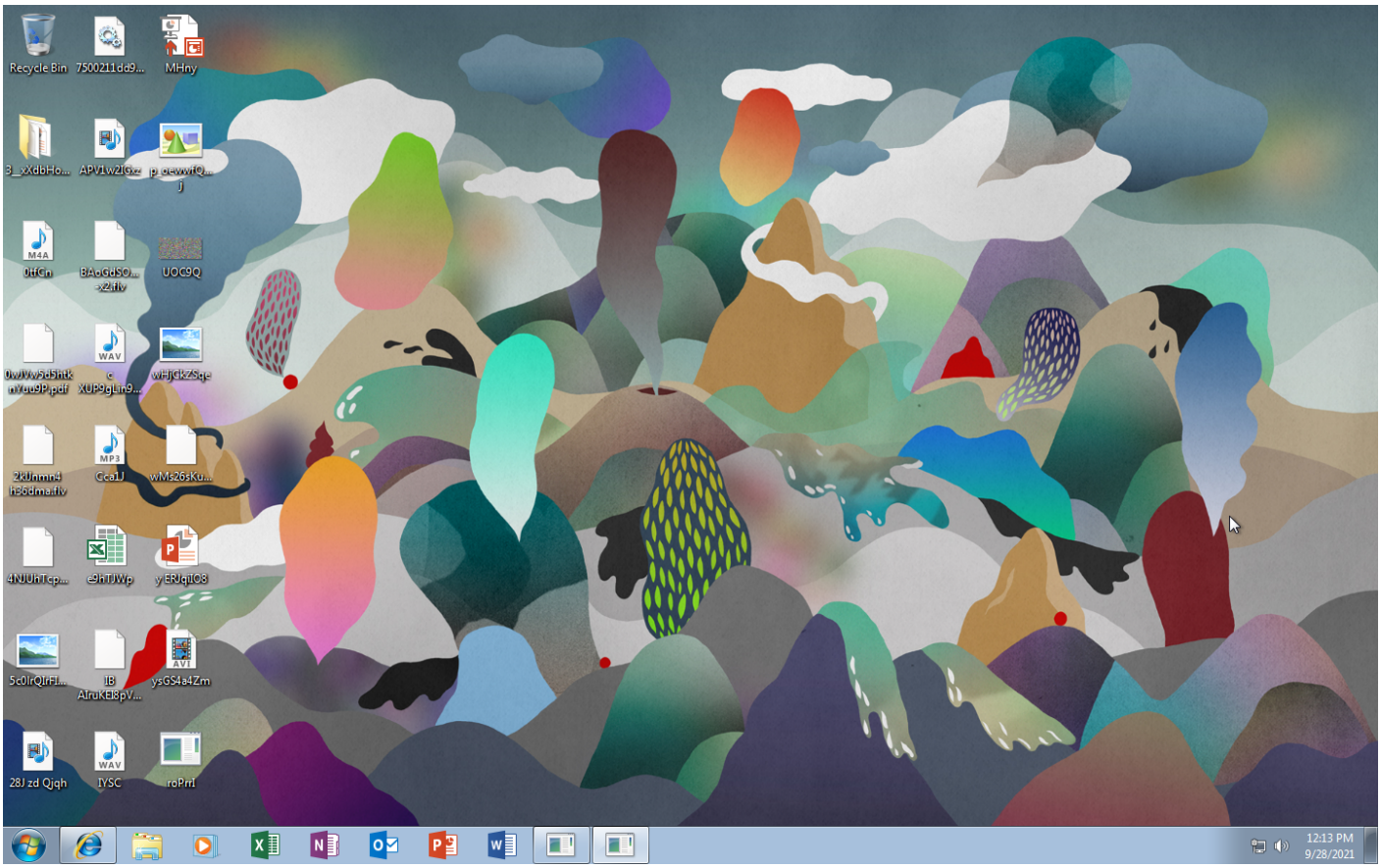
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1081 Credentials in Files	#T1082 System Information Discovery		#T1119 Automated Collection			
				#T1112 Modify Registry		#T1012 Query Registry		#T1005 Data from Local System			
				#T1045 Software Packing		#T1083 File and Directory Discovery					

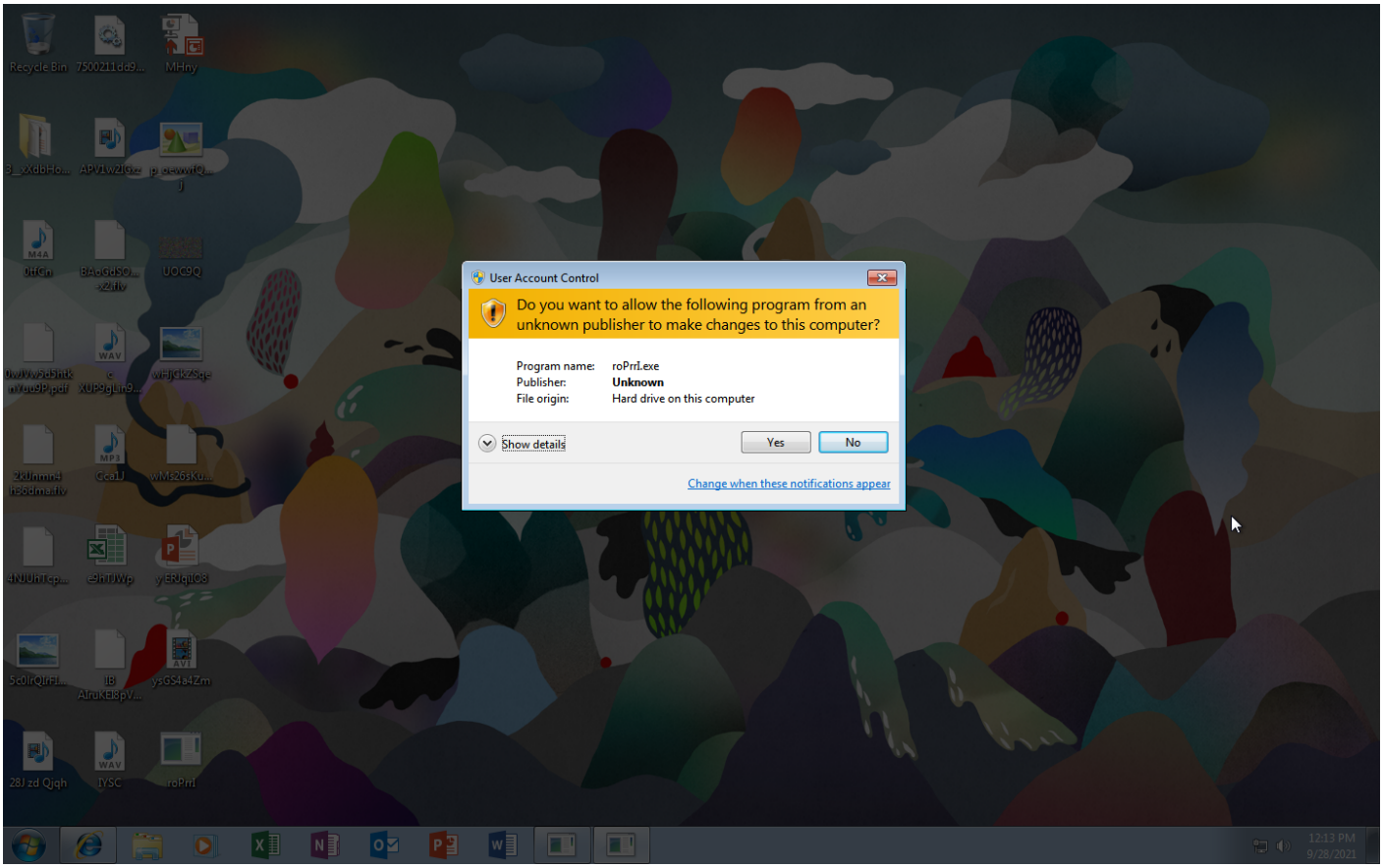
Sample Information

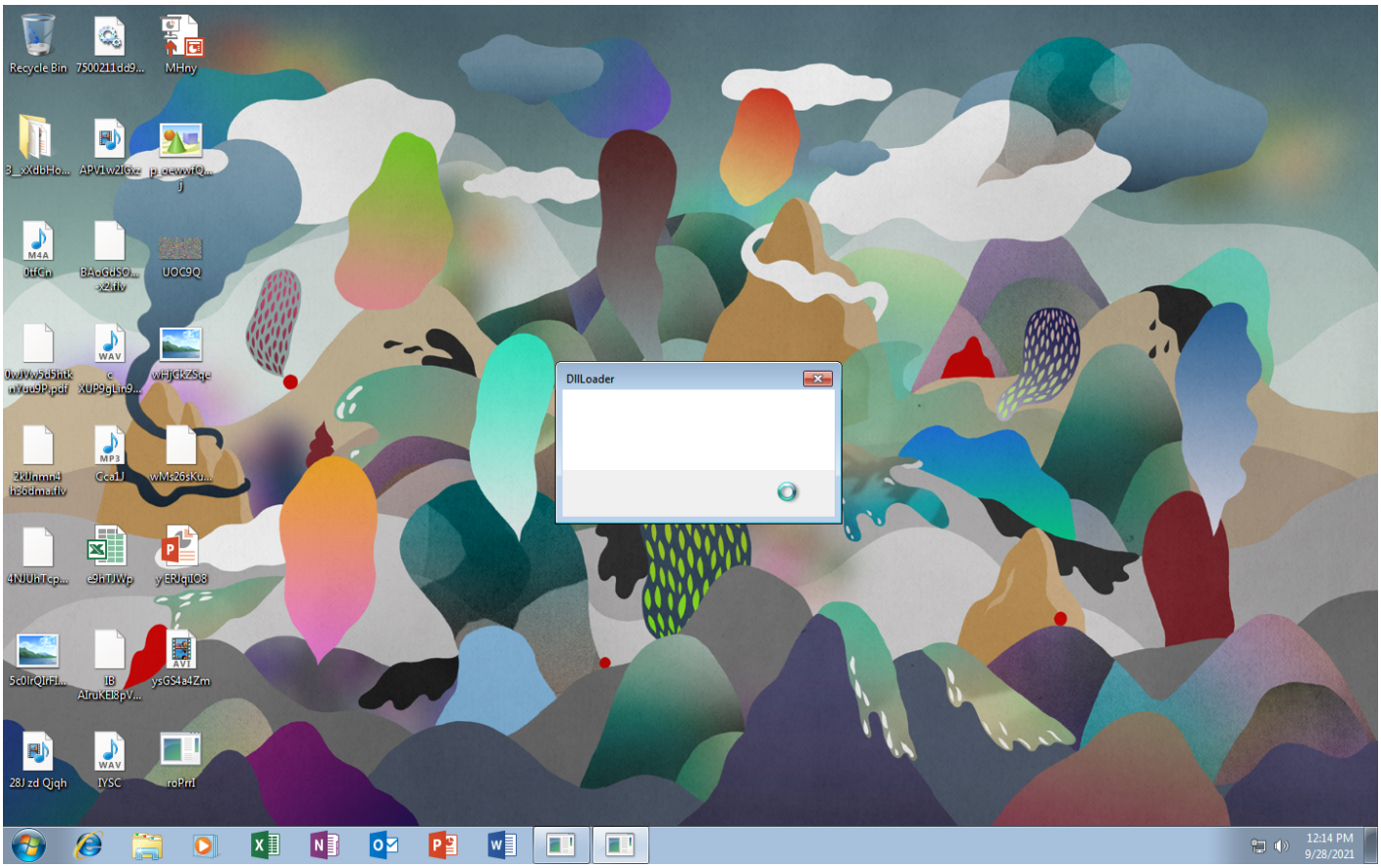
ID	#2782917
MD5	a75be08d11b5028b6e0fa8be59676599
SHA1	c47a48e04dc10641df07dba7dbbb73602e6615aa
SHA256	7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a
SSDeep	12288:LVl0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:KfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll
File Size	2056.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

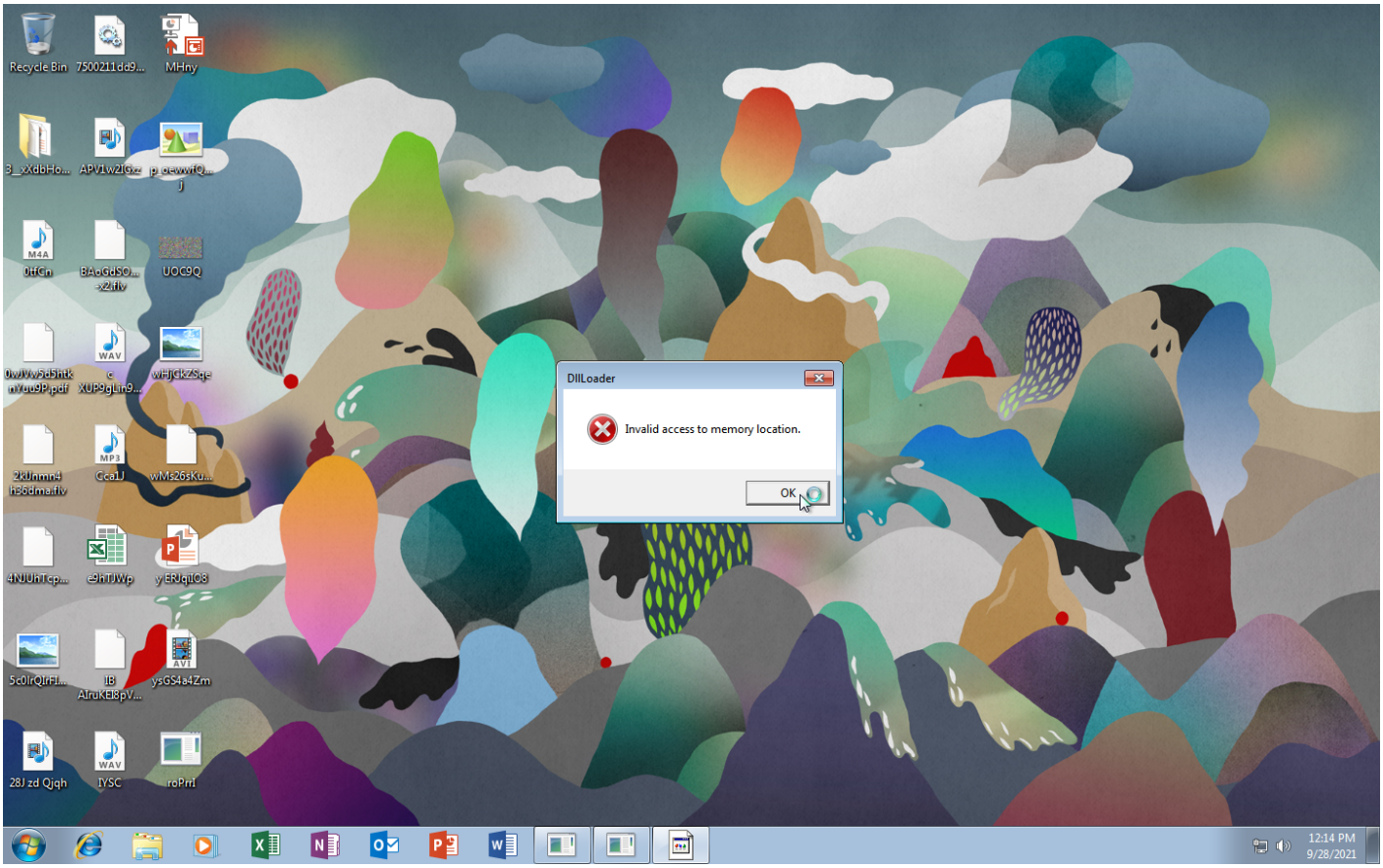
Analysis Information

Creation Time	2021-09-28 14:12 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	195
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	16
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: roPrrI.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

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

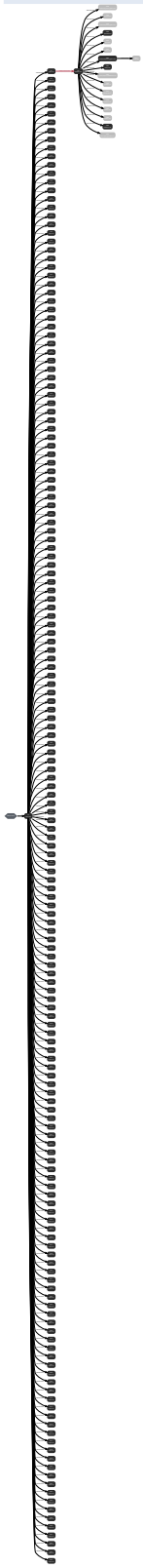
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: roprri.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpg5eszf6e" /s
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 46107, Reason: Analysis Target
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	248.15s
Return Code	Unknown
PID	3844
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	16
File	6
Environment	1
Process	177

Process #2: roprri.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#1
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 57969, Reason: Child Process
Unmonitor End Time	End Time: 90426, Reason: Terminated
Monitor duration	32.46s
Return Code	0
PID	3872
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	41
Module	41
File	118
Environment	2
Registry	589
Mutex	6
Process	2
-	34
-	36
-	96

Process #3: roprri.exe

ID	3
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#10
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 59356, Reason: Child Process
Unmonitor End Time	End Time: 71921, Reason: Terminated
Monitor duration	12.56s
Return Code	0
PID	3884
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	343
Mutex	7

Process #4: roprri.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#11
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 59452, Reason: Child Process
Unmonitor End Time	End Time: 68913, Reason: Terminated
Monitor duration	9.46s
Return Code	0
PID	3896
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	7
Module	31
File	117
Environment	2
Registry	514
Mutex	6

Process #5: roprri.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#13
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 60123, Reason: Child Process
Unmonitor End Time	End Time: 81305, Reason: Terminated
Monitor duration	21.18s
Return Code	0
PID	3912
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	527
Mutex	7

Process #6: roprri.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#14
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 60305, Reason: Child Process
Unmonitor End Time	End Time: 74147, Reason: Terminated
Monitor duration	13.84s
Return Code	0
PID	3924
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	289
Mutex	7

Process #7: roprri.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#15
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 61539, Reason: Child Process
Unmonitor End Time	End Time: 73500, Reason: Terminated
Monitor duration	11.96s
Return Code	0
PID	3940
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	351
Mutex	7

Process #8: roprri.exe

ID	8
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#16
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 62599, Reason: Child Process
Unmonitor End Time	End Time: 76141, Reason: Terminated
Monitor duration	13.54s
Return Code	0
PID	3952
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	8
Module	31
File	117
Environment	2
Registry	527
Mutex	7

Process #9: roprri.exe

ID	9
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#17
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 62952, Reason: Child Process
Unmonitor End Time	End Time: 80467, Reason: Terminated
Monitor duration	17.52s
Return Code	0
PID	3964
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #10: roprri.exe

ID	10
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#18
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 64825, Reason: Child Process
Unmonitor End Time	End Time: 80792, Reason: Terminated
Monitor duration	15.97s
Return Code	0
PID	3988
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #11: roprri.exe

ID	11
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#19
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65224, Reason: Child Process
Unmonitor End Time	End Time: 149893, Reason: Terminated
Monitor duration	84.67s
Return Code	0
PID	4000
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	54
Module	40
File	118
Environment	2
Registry	350
Mutex	6
Process	2
-	2
-	50

Process #12: roprri.exe

ID	12
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#2
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 67857, Reason: Child Process
Unmonitor End Time	End Time: 90333, Reason: Terminated
Monitor duration	22.48s
Return Code	0
PID	4024
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #13: roprri.exe

ID	13
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#20
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 69939, Reason: Child Process
Unmonitor End Time	End Time: 90332, Reason: Terminated
Monitor duration	20.39s
Return Code	0
PID	4044
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #14: explorer.exe

ID	14
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 71030, Reason: Injection
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	223.23s
Return Code	Unknown
PID	1116
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (65)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x460	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x474	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x4b8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x4bc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x4cc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x4d4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x52c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x534	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x540	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x5d8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x478	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x510	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x514	0x777313f0(2004030448)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x51c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x53c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x350	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x354	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x5a4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x7b0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x59c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x2f8	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x5cc	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x694	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x4b0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0xa14	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0xae0	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0xca4	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0xd58	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0xd5c	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0xd68	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0xe24	0x777313f0(2004030448)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77732ed0(2004037328)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✓	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77732ed0(2004037328)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c:\users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c: \users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c: \users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c: \users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c: \users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c: \users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a30(2001889840)	-	✔	1
Modify Control Flow	#2: c: \users\keecfmwgj\desktop\roprri.exe	0xf24 / 0x50c	0x77526a60(2001889888)	-	✔	1
Modify Control Flow	#11: c: \users\keecfmwgj\desktop\roprri.exe	0xfa4 / 0x474	0xf0000(983040)	-	✔	1

Dropped Files (14)

File Name	File Size	SHA256	YARA Match
-	50 bytes	2d970fea1e7ebc4c9bae287309fa032cb2ac90323c0cdb49ca9593dc7d074c98	✘
\\?\C:\Windows \system32\slc.dll	30.00 KB	ecfd25bf4e556beb43cac72ec30a7b3de318dc950994bd5480514605f31b2ef2	✘
\\?\C:\Windows \system32\WindowsAnytimeUpgrade.exe	251.50 KB	1018c9e81abe5a4a5eada97fc92a6561e3be13bf5a8eaa1be6d7226cbc9e9f7e	✘
C:\Users\kEecfMwgj\AppData\Local\fg0b\VERSION.dll	2060.00 KB	9f2e7cb50c729b34f490422bbadfbd10487505abc90a124221dfe34e9727c628	✘
C:\Users\kEecfMwgj\AppData\Local\fg0b\spreview.exe	294.50 KB	4307f21d3ec3b51cba6a905a80045314ffccb4c60c11d99a3d77cc8103014208	✘
C:\Users\kEecfMwgj\AppData\Local\dOFgn\VERSION.dll	2060.00 KB	6747894733b6d3a4ba11585dc5c7b14fec22babd70dea0d19124a6c2210a6a8f	✘
C:\Users\kEecfMwgj\AppData\Local\dOFgn\cmstp.exe	90.00 KB	51d298b1a8a2d00d5c608c52dba0655565d021e9798ee171d7fa92cc0de729a6	✘
\\?\C:\Windows \system32\ReAgent.dll	306.50 KB	e2b09cfdead0313843c3dbf5233833c1d9c80a33078bf4739760b64fb1fd524a	✘
\\?\C:\Windows \system32\recdisc.exe	232.50 KB	dcaeb590394b42d180e23e3cef4dd135513395b026e0ed489aec49848b85b8f0	✘
C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\VERSION.dll	2060.00 KB	6db6518c8bddc3986a8d19aadfa6594239f5a332d7405802a7a77afb9844b56c	✘
C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\UI0Detect.exe	40.00 KB	b8dab8aa804fc23021bfebd7ae4d40fbe648d6c6ba21cc008e26d1c084972f9b	✘
-	1.40 KB	64c30ee40b2e18bf9bb8e389a20668dc5e24ce51ff2ca38d5cdf6c8a2719056f	✘
-	1.40 KB	72275404c470b62a5ff49013e3f952d9480afd5c7e45b6c504235823da4894ae	✘
-	1.42 KB	cad9b90b73aef995edf234d8d02852519dc40d938f9fcf75d664ca69c19826fb	✘

Host Behavior

Type	Count
Module	84
File	1765
System	346
Process	32

Type	Count
Registry	37592
Environment	3
-	13
Mutex	19911
-	3

Process #15: roprri.exe

ID	15
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#21
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 73648, Reason: Child Process
Unmonitor End Time	End Time: 117116, Reason: Terminated
Monitor duration	43.47s
Return Code	0
PID	4064
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	91
Mutex	4

Process #16: roprri.exe

ID	16
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#22
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 75588, Reason: Child Process
Unmonitor End Time	End Time: 118354, Reason: Terminated
Monitor duration	42.77s
Return Code	0
PID	4084
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	93
Mutex	4

Process #17: roprri.exe

ID	17
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#23
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76279, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	217.98s
Return Code	Unknown
PID	2792
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #18: roprri.exe

ID	18
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#24
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76419, Reason: Child Process
Unmonitor End Time	End Time: 130820, Reason: Terminated
Monitor duration	54.40s
Return Code	0
PID	2768
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	91
Mutex	4

Process #19: roprri.exe

ID	19
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#25
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76680, Reason: Child Process
Unmonitor End Time	End Time: 156648, Reason: Terminated
Monitor duration	79.97s
Return Code	0
PID	2744
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #20: roprri.exe

ID	20
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#26
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76742, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	217.52s
Return Code	Unknown
PID	2728
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #21: roprri.exe

ID	21
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#27
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76850, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	217.41s
Return Code	Unknown
PID	2712
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #22: roprri.exe

ID	22
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#28
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76933, Reason: Child Process
Unmonitor End Time	End Time: 153536, Reason: Terminated
Monitor duration	76.60s
Return Code	0
PID	2700
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #23: roprri.exe

ID	23
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#29
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77092, Reason: Child Process
Unmonitor End Time	End Time: 132828, Reason: Terminated
Monitor duration	55.74s
Return Code	0
PID	2688
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	70
Mutex	4

Process #24: roprri.exe

ID	24
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#3
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77183, Reason: Child Process
Unmonitor End Time	End Time: 158676, Reason: Terminated
Monitor duration	81.49s
Return Code	0
PID	2676
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #25: roprri.exe

ID	25
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#30
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77281, Reason: Child Process
Unmonitor End Time	End Time: 232307, Reason: Terminated
Monitor duration	155.03s
Return Code	0
PID	2664
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #26: roprri.exe

ID	26
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#31
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77428, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	216.83s
Return Code	Unknown
PID	2652
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #27: roprri.exe

ID	27
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#32
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77570, Reason: Child Process
Unmonitor End Time	End Time: 196583, Reason: Terminated
Monitor duration	119.01s
Return Code	0
PID	2640
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #28: roprri.exe

ID	28
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#33
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77658, Reason: Child Process
Unmonitor End Time	End Time: 247717, Reason: Terminated
Monitor duration	170.06s
Return Code	0
PID	2632
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #29: roprri.exe

ID	29
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#34
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77729, Reason: Child Process
Unmonitor End Time	End Time: 246581, Reason: Terminated
Monitor duration	168.85s
Return Code	0
PID	2620
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #30: roprri.exe

ID	30
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#35
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77879, Reason: Child Process
Unmonitor End Time	End Time: 217041, Reason: Terminated
Monitor duration	139.16s
Return Code	0
PID	2608
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #31: roprri.exe

ID	31
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#36
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 77954, Reason: Child Process
Unmonitor End Time	End Time: 223653, Reason: Terminated
Monitor duration	145.70s
Return Code	0
PID	2788
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #32: roprri.exe

ID	32
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#4
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78123, Reason: Child Process
Unmonitor End Time	End Time: 286926, Reason: Terminated
Monitor duration	208.80s
Return Code	0
PID	3168
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #33: roprri.exe

ID	33
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#43
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78203, Reason: Child Process
Unmonitor End Time	End Time: 178893, Reason: Terminated
Monitor duration	100.69s
Return Code	0
PID	3108
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #34: roprri.exe

ID	34
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#44
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78346, Reason: Child Process
Unmonitor End Time	End Time: 184298, Reason: Terminated
Monitor duration	105.95s
Return Code	0
PID	1392
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #35: roprri.exe

ID	35
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#45
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78414, Reason: Child Process
Unmonitor End Time	End Time: 190546, Reason: Terminated
Monitor duration	112.13s
Return Code	0
PID	1916
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #36: roprri.exe

ID	36
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#46
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78547, Reason: Child Process
Unmonitor End Time	End Time: 169814, Reason: Terminated
Monitor duration	91.27s
Return Code	0
PID	1872
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #37: roprri.exe

ID	37
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#48
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78610, Reason: Child Process
Unmonitor End Time	End Time: 195975, Reason: Terminated
Monitor duration	117.36s
Return Code	0
PID	1032
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #38: roprri.exe

ID	38
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#49
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78741, Reason: Child Process
Unmonitor End Time	End Time: 212908, Reason: Terminated
Monitor duration	134.17s
Return Code	0
PID	948
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #39: roprri.exe

ID	39
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#50
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78816, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	215.44s
Return Code	Unknown
PID	3328
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #40: roprri.exe

ID	40
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#60
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78950, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	215.31s
Return Code	Unknown
PID	3228
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #41: roprri.exe

ID	41
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#62
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79004, Reason: Child Process
Unmonitor End Time	End Time: 273413, Reason: Terminated
Monitor duration	194.41s
Return Code	0
PID	3212
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #42: roprri.exe

ID	42
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#63
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79116, Reason: Child Process
Unmonitor End Time	End Time: 169314, Reason: Terminated
Monitor duration	90.20s
Return Code	998
PID	3120
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	33
File	112
Environment	2
Window	1

Process #43: roprri.exe

ID	43
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#64
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79216, Reason: Child Process
Unmonitor End Time	End Time: 155291, Reason: Terminated
Monitor duration	76.08s
Return Code	0
PID	3376
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	70
Mutex	4

Process #44: roprri.exe

ID	44
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#65
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79240, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	215.02s
Return Code	Unknown
PID	3352
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #45: roprri.exe

ID	45
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#66
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79270, Reason: Child Process
Unmonitor End Time	End Time: 193853, Reason: Terminated
Monitor duration	114.58s
Return Code	0
PID	3344
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #46: roprri.exe

ID	46
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#67
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79298, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	214.96s
Return Code	Unknown
PID	3384
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #47: roprri.exe

ID	47
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#68
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79326, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	214.93s
Return Code	Unknown
PID	3436
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #48: roprri.exe

ID	48
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#69
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79357, Reason: Child Process
Unmonitor End Time	End Time: 210647, Reason: Terminated
Monitor duration	131.29s
Return Code	0
PID	1036
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #49: roprri.exe

ID	49
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#7
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79381, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	214.88s
Return Code	Unknown
PID	3392
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #50: roprri.exe

ID	50
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#72
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79442, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	214.82s
Return Code	Unknown
PID	3532
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #51: roprri.exe

ID	51
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#73
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79583, Reason: Child Process
Unmonitor End Time	End Time: 192871, Reason: Terminated
Monitor duration	113.29s
Return Code	0
PID	3540
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #52: roprri.exe

ID	52
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#74
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79643, Reason: Child Process
Unmonitor End Time	End Time: 173350, Reason: Terminated
Monitor duration	93.71s
Return Code	0
PID	3528
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #53: roprri.exe

ID	53
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#75
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79790, Reason: Child Process
Unmonitor End Time	End Time: 230834, Reason: Terminated
Monitor duration	151.04s
Return Code	0
PID	3592
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #54: roprri.exe

ID	54
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#76
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 79869, Reason: Child Process
Unmonitor End Time	End Time: 173233, Reason: Terminated
Monitor duration	93.36s
Return Code	0
PID	824
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #55: roprri.exe

ID	55
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#77
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 80032, Reason: Child Process
Unmonitor End Time	End Time: 180085, Reason: Terminated
Monitor duration	100.05s
Return Code	0
PID	2140
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #56: roprri.exe

ID	56
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#78
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 80117, Reason: Child Process
Unmonitor End Time	End Time: 162399, Reason: Terminated
Monitor duration	82.28s
Return Code	0
PID	2152
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #57: roprri.exe

ID	57
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#79
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 80468, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	213.79s
Return Code	Unknown
PID	2164
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #58: roprri.exe

ID	58
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#8
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 80566, Reason: Child Process
Unmonitor End Time	End Time: 160910, Reason: Terminated
Monitor duration	80.34s
Return Code	0
PID	2208
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #59: roprri.exe

ID	59
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#80
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 80717, Reason: Child Process
Unmonitor End Time	End Time: 259676, Reason: Terminated
Monitor duration	178.96s
Return Code	0
PID	2220
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #60: roprri.exe

ID	60
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#81
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 80792, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	213.47s
Return Code	Unknown
PID	2436
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #61: roprri.exe

ID	61
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#82
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81276, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	212.98s
Return Code	Unknown
PID	2448
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #62: roprri.exe

ID	62
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#83
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81378, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	212.88s
Return Code	Unknown
PID	2460
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #63: roprri.exe

ID	63
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#84
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81449, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	212.81s
Return Code	Unknown
PID	2472
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #64: roprri.exe

ID	64
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#85
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81624, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	212.63s
Return Code	Unknown
PID	2484
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #65: roprri.exe

ID	65
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#86
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81683, Reason: Child Process
Unmonitor End Time	End Time: 195974, Reason: Terminated
Monitor duration	114.29s
Return Code	0
PID	2496
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #66: roprri.exe

ID	66
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#9
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81762, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	212.50s
Return Code	Unknown
PID	2508
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #67: roprri.exe

ID	67
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BeginBufferedAnimation
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81856, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	212.40s
Return Code	Unknown
PID	2520
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #68: roprri.exe

ID	68
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BeginBufferedPaint
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81950, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	212.31s
Return Code	Unknown
PID	2532
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #69: roprri.exe

ID	69
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BeginPanningFeedback
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82208, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	212.05s
Return Code	Unknown
PID	2544
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #70: roprri.exe

ID	70
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintClear
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82269, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	211.99s
Return Code	Unknown
PID	2556
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #71: roprri.exe

ID	71
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintInit
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82535, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	211.72s
Return Code	Unknown
PID	2568
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #72: roprri.exe

ID	72
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintRenderAnimation
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82601, Reason: Child Process
Unmonitor End Time	End Time: 253850, Reason: Terminated
Monitor duration	171.25s
Return Code	0
PID	2584
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #73: roprri.exe

ID	73
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintSetAlpha
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82778, Reason: Child Process
Unmonitor End Time	End Time: 219130, Reason: Terminated
Monitor duration	136.35s
Return Code	0
PID	2596
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #74: roprri.exe

ID	74
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintStopAllAnimations
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82844, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	211.41s
Return Code	Unknown
PID	2780
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #75: roprri.exe

ID	75
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintUnInit
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 82923, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	211.34s
Return Code	Unknown
PID	3124
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #76: roprri.exe

ID	76
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=CloseThemeData
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83012, Reason: Child Process
Unmonitor End Time	End Time: 227538, Reason: Terminated
Monitor duration	144.53s
Return Code	0
PID	1884
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	106

Process #77: roprri.exe

ID	77
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeBackground
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83200, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	211.06s
Return Code	Unknown
PID	3604
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #78: roprri.exe

ID	78
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeBackgroundEx
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83270, Reason: Child Process
Unmonitor End Time	End Time: 252420, Reason: Terminated
Monitor duration	169.15s
Return Code	0
PID	3492
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #79: roprri.exe

ID	79
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeEdge
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83439, Reason: Child Process
Unmonitor End Time	End Time: 254864, Reason: Terminated
Monitor duration	171.43s
Return Code	0
PID	3488
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #80: roprri.exe

ID	80
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeIcon
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83521, Reason: Child Process
Unmonitor End Time	End Time: 229701, Reason: Terminated
Monitor duration	146.18s
Return Code	0
PID	3484
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #81: roprri.exe

ID	81
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeParentBackground
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83604, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	210.66s
Return Code	Unknown
PID	3732
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #82: roprri.exe

ID	82
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeParentBackgroundEx
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83696, Reason: Child Process
Unmonitor End Time	End Time: 217877, Reason: Terminated
Monitor duration	134.18s
Return Code	0
PID	3772
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #83: roprri.exe

ID	83
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeText
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83798, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	210.46s
Return Code	Unknown
PID	3744
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #84: roprri.exe

ID	84
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeTextEx
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 83900, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	210.36s
Return Code	Unknown
PID	3764
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #85: roprri.exe

ID	85
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EnableThemeDialogTexture
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84627, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	209.63s
Return Code	Unknown
PID	3672
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #86: roprri.exe

ID	86
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EnableTheming
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 84926, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	209.33s
Return Code	Unknown
PID	3688
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #87: roprri.exe

ID	87
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EndBufferedAnimation
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85035, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	209.22s
Return Code	Unknown
PID	3680
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #88: roprri.exe

ID	88
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EndBufferedPaint
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85107, Reason: Child Process
Unmonitor End Time	End Time: 258339, Reason: Terminated
Monitor duration	173.23s
Return Code	0
PID	3840
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #89: roprri.exe

ID	89
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EndPanningFeedback
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85260, Reason: Child Process
Unmonitor End Time	End Time: 229659, Reason: Terminated
Monitor duration	144.40s
Return Code	0
PID	3300
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #90: roprri.exe

ID	90
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetBufferedPaintBits
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85309, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	208.95s
Return Code	Unknown
PID	3856
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #91: roprri.exe

ID	91
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetBufferedPaintDC
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85457, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	208.80s
Return Code	Unknown
PID	3880
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #92: roprri.exe

ID	92
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetBufferedPaintTargetDC
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85510, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	208.75s
Return Code	Unknown
PID	3920
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #93: roprri.exe

ID	93
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetBufferedPaintTargetRect
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85633, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	208.63s
Return Code	Unknown
PID	3504
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #94: roprri.exe

ID	94
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetCurrentThemeName
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85692, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	208.57s
Return Code	Unknown
PID	3948
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #95: roprri.exe

ID	95
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeAppProperties
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85791, Reason: Child Process
Unmonitor End Time	End Time: 189892, Reason: Terminated
Monitor duration	104.10s
Return Code	0
PID	3500
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #96: roprri.exe

ID	96
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBackgroundContentRect
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85940, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	208.32s
Return Code	Unknown
PID	3652
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #97: roprri.exe

ID	97
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBackgroundExtent
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 86513, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	207.75s
Return Code	Unknown
PID	3980
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #98: roprri.exe

ID	98
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBackgroundRegion
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 86622, Reason: Child Process
Unmonitor End Time	End Time: 188279, Reason: Terminated
Monitor duration	101.66s
Return Code	0
PID	3824
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #99: roprri.exe

ID	99
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBitmap
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87058, Reason: Child Process
Unmonitor End Time	End Time: 283338, Reason: Terminated
Monitor duration	196.28s
Return Code	0
PID	3812
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #100: roprri.exe

ID	100
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBool
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87182, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	207.08s
Return Code	Unknown
PID	3800
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #101: roprri.exe

ID	101
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeColor
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 87334, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	206.93s
Return Code	Unknown
PID	4016
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #102: roprri.exe

ID	102
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeDocumentationProperty
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88544, Reason: Child Process
Unmonitor End Time	End Time: 276692, Reason: Terminated
Monitor duration	188.15s
Return Code	0
PID	3900
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #103: roprri.exe

ID	103
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeEnumValue
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89037, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	205.22s
Return Code	Unknown
PID	1372
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #104: roprri.exe

ID	104
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeFilename
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89175, Reason: Child Process
Unmonitor End Time	End Time: 191608, Reason: Terminated
Monitor duration	102.43s
Return Code	0
PID	3888
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #105: roprri.exe

ID	105
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeFont
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 90939, Reason: Child Process
Unmonitor End Time	End Time: 217039, Reason: Terminated
Monitor duration	126.10s
Return Code	0
PID	3940
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #106: roprri.exe

ID	106
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeInt
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91033, Reason: Child Process
Unmonitor End Time	End Time: 193213, Reason: Terminated
Monitor duration	102.18s
Return Code	0
PID	3792
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #107: roprri.exe

ID	107
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeIntList
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91239, Reason: Child Process
Unmonitor End Time	End Time: 193432, Reason: Terminated
Monitor duration	102.19s
Return Code	0
PID	4036
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #108: roprri.exe

ID	108
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeMargins
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91830, Reason: Child Process
Unmonitor End Time	End Time: 267342, Reason: Terminated
Monitor duration	175.51s
Return Code	0
PID	3924
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #109: roprri.exe

ID	109
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeMetric
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91981, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	202.28s
Return Code	Unknown
PID	3952
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #110: roprri.exe

ID	110
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemePartSize
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92740, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	201.52s
Return Code	Unknown
PID	2756
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	18
File	112
Environment	1

Process #111: roprri.exe

ID	111
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemePosition
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92891, Reason: Child Process
Unmonitor End Time	End Time: 197623, Reason: Terminated
Monitor duration	104.73s
Return Code	0
PID	2704
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #112: roprri.exe

ID	112
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemePropertyOrigin
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93670, Reason: Child Process
Unmonitor End Time	End Time: 231152, Reason: Terminated
Monitor duration	137.48s
Return Code	0
PID	2668
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #113: roprri.exe

ID	113
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeRect
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 93907, Reason: Child Process
Unmonitor End Time	End Time: 186318, Reason: Terminated
Monitor duration	92.41s
Return Code	0
PID	2636
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #114: roprri.exe

ID	114
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeStream
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 95833, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	198.43s
Return Code	Unknown
PID	3316
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #115: roprri.exe

ID	115
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeString
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 96154, Reason: Child Process
Unmonitor End Time	End Time: 233091, Reason: Terminated
Monitor duration	136.94s
Return Code	0
PID	3364
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #116: roprri.exe

ID	116
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysBool
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103328, Reason: Child Process
Unmonitor End Time	End Time: 188901, Reason: Terminated
Monitor duration	85.57s
Return Code	0
PID	3348
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #117: roprri.exe

ID	117
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysColor
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114644, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	179.62s
Return Code	Unknown
PID	912
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #118: windowsanytimeupgrade.exe

ID	118
File Name	c:\windows\system32\windowsanytimeupgrade.exe
Command Line	C:\Windows\system32\WindowsAnytimeUpgrade.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 117117, Reason: Child Process
Unmonitor End Time	End Time: 123046, Reason: Terminated
Monitor duration	5.93s
Return Code	3221226540
PID	4040
Parent PID	1116
Bitness	64 Bit

Process #119: roprri.exe

ID	119
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysColorBrush
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 118355, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	175.90s
Return Code	Unknown
PID	4076
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #120: spreview.exe

ID	120
File Name	c:\windows\system32\spreview.exe
Command Line	C:\Windows\system32\spreview.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 120274, Reason: Child Process
Unmonitor End Time	End Time: 124762, Reason: Terminated
Monitor duration	4.49s
Return Code	0
PID	2160
Parent PID	1116
Bitness	64 Bit

Process #121: roprri.exe

ID	121
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysFont
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 123859, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	170.40s
Return Code	Unknown
PID	2216
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #122: roprri.exe

ID	122
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysInt
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 124195, Reason: Child Process
Unmonitor End Time	End Time: 235879, Reason: Terminated
Monitor duration	111.68s
Return Code	0
PID	2468
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #123: windowsanytimeupgrade.exe

ID	123
File Name	c:\windows \system32\windowsanytimeupgrade.exe
Command Line	"C:\Windows \system32\WindowsAnytimeUpgrade.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 125297, Reason: Child Process
Unmonitor End Time	End Time: 126805, Reason: Terminated
Monitor duration	1.51s
Return Code	3221226540
PID	2504
Parent PID	1116
Bitness	64 Bit

Process #124: roprri.exe

ID	124
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysSize
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 125318, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	168.94s
Return Code	Unknown
PID	2528
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #125: roprri.exe

ID	125
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysString
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 125664, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	168.59s
Return Code	Unknown
PID	3476
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #126: roprri.exe

ID	126
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeTextExtent
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 127900, Reason: Child Process
Unmonitor End Time	End Time: 277859, Reason: Terminated
Monitor duration	149.96s
Return Code	0
PID	2592
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	30
File	112
Environment	2
Registry	91
Mutex	4

Process #127: roprri.exe

ID	127
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeTextMetrics
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 129552, Reason: Child Process
Unmonitor End Time	End Time: 270593, Reason: Terminated
Monitor duration	141.04s
Return Code	0
PID	1336
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #128: roprri.exe

ID	128
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeTransitionDuration
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 132548, Reason: Child Process
Unmonitor End Time	End Time: 253443, Reason: Terminated
Monitor duration	120.89s
Return Code	0
PID	3644
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #129: roprri.exe

ID	129
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetWindowTheme
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 133819, Reason: Child Process
Unmonitor End Time	End Time: 267341, Reason: Terminated
Monitor duration	133.52s
Return Code	0
PID	3668
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #130: roprri.exe

ID	130
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=HitTestThemeBackground
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134478, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	159.78s
Return Code	Unknown
PID	3296
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #131: roprri.exe

ID	131
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsAppThemed
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 137625, Reason: Child Process
Unmonitor End Time	End Time: 252306, Reason: Terminated
Monitor duration	114.68s
Return Code	0
PID	3440
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #132: roprri.exe

ID	132
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsCompositionActive
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 139132, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	155.13s
Return Code	Unknown
PID	1928
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #133: roprri.exe

ID	133
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsThemeActive
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 141603, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	152.66s
Return Code	Unknown
PID	3984
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #134: roprri.exe

ID	134
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsThemeBackgroundPartiallyTransparent
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 146679, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	147.58s
Return Code	Unknown
PID	3876
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #135: spreview.exe

ID	135
File Name	c:\users\keecfmwgj\appdata\local\fg0b\spreview.exe
Command Line	C:\Users\kEecfMwgj\AppData\Local\fg0b\spreview.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 148864, Reason: Child Process
Unmonitor End Time	End Time: 163649, Reason: Terminated
Monitor duration	14.79s
Return Code	0
PID	560
Parent PID	1116
Bitness	64 Bit

Host Behavior

Type	Count
File	109
Module	11

Process #136: roprri.exe

ID	136
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsThemeDialogTextureEnabled
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148908, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	145.35s
Return Code	Unknown
PID	1920
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #137: roprri.exe

ID	137
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsThemePartDefined
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 154470, Reason: Child Process
Unmonitor End Time	End Time: 273772, Reason: Terminated
Monitor duration	119.30s
Return Code	0
PID	3956
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #138: roprri.exe

ID	138
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=OpenThemeData
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 157996, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	136.26s
Return Code	Unknown
PID	1956
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	28
File	112
Environment	1

Process #139: roprri.exe

ID	139
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=OpenThemeDataEx
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 161193, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	133.07s
Return Code	Unknown
PID	476
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #140: roprri.exe

ID	140
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=SetThemeAppProperties
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 162765, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	131.49s
Return Code	Unknown
PID	676
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	109

Process #141: rstrui.exe

ID	141
File Name	c:\windows\system32\rstrui.exe
Command Line	C:\Windows\system32\rstrui.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 165053, Reason: Child Process
Unmonitor End Time	End Time: 170968, Reason: Terminated
Monitor duration	5.92s
Return Code	3221226540
PID	1960
Parent PID	1116
Bitness	64 Bit

Process #142: roprri.exe

ID	142
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=SetWindowTheme
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 170379, Reason: Child Process
Unmonitor End Time	End Time: 290791, Reason: Terminated
Monitor duration	120.41s
Return Code	0
PID	896
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	29
File	112
Environment	2
Registry	141

Process #143: roprri.exe

ID	143
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=SetWindowThemeAttribute
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 171043, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	123.22s
Return Code	Unknown
PID	856
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #144: roprri.exe

ID	144
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=ThemeInitApiHook
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 173234, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	121.03s
Return Code	Unknown
PID	100
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #145: cmstp.exe

ID	145
File Name	c:\windows\system32\cmstp.exe
Command Line	C:\Windows\system32\cmstp.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 173525, Reason: Child Process
Unmonitor End Time	End Time: 176299, Reason: Terminated
Monitor duration	2.77s
Return Code	0
PID	1876
Parent PID	1116
Bitness	64 Bit

Process #146: roprri.exe

ID	146
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=UpdatePanningFeedback
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 176732, Reason: Child Process
Unmonitor End Time	End Time: 265143, Reason: Terminated
Monitor duration	88.41s
Return Code	0
PID	1356
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #147: roprri.exe

ID	147
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#1 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 178025, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	116.23s
Return Code	Unknown
PID	3220
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #148: roprri.exe

ID	148
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#10 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 178952, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	115.31s
Return Code	Unknown
PID	2056
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	17
File	3
Environment	1

Process #149: roprri.exe

ID	149
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#11 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 184438, Reason: Child Process
Unmonitor End Time	End Time: 288657, Reason: Terminated
Monitor duration	104.22s
Return Code	0
PID	2084
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

Process #150: roprri.exe

ID	150
File Name	c:\users\keecfmwgj\desktop\roprri.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#13 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 187548, Reason: Child Process
Unmonitor End Time	End Time: 294259, Reason: Terminated by Timeout
Monitor duration	106.71s
Return Code	Unknown
PID	1640
Parent PID	3844
Bitness	64 Bit

Host Behavior

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

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a	C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll, C:\Users\kEecfMwgj\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll	Sample File	2056.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
9f2e7cb50c729b34f490422bbadfbd10487505abc90a124221dfe34e9727c628	C:\Users\kEecfMwgj\AppData\Local\fg0b\VERSION.dll	Dropped File	2060.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	MALICIOUS
6747894733b6d3a4ba11585dc5c7b14fec22babd70dea0d19124a6c2210a6a8f	C:\Users\kEecfMwgj\AppData\Local\dOFgn\VERSION.dll	Dropped File	2060.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	MALICIOUS
6db6518c8bddc3986a8d19aadfa6594239f5a332d7405802a7a77afb9844b56c	C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\VERSION.dll	Dropped File	2060.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	MALICIOUS
1018c9e81abe5a4a5eada97fc92a6561e3be13bf5a8eaa1be6d7226cbc9e9f7e	\\?\C:\Windows\system32\WindowsAnytimeUpgrade.exe	Dropped File	251.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	SUSPICIOUS
4307f21d3ec3b51cba6a905a80045314ffccb4c60c11d99a3d77cc8103014208	C:\Users\kEecfMwgj\AppData\Local\fg0b\spreview.exe	Dropped File	294.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	SUSPICIOUS
51d298b1a8a2d00d5c608c52dba0655565d021e9798ee171d7fa92cc0de729a6	C:\Users\kEecfMwgj\AppData\Local\dOFgn\cmstp.exe	Dropped File	90.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	SUSPICIOUS
b8dab8aa804fc23021bfebd7ae4d40fbe648d6c6ba21cc008e26d1c084972f9b	C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\UI0Detect.exe	Dropped File	40.00 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
ecfd25bf4e556beb43cac72ec30a7b3de318dc950994bd5480514605f31b2ef2	\\?\C:\Windows \system32\slc.dll	Dropped File	30.00 KB	application/vnd.microsoft.portable-executable	Access, Write, Delete, Create	CLEAN
e2b09cfdead0313843c3dbf5233833c1d9c80a33078bf4739760b64fb1fd524a	\\?\C:\Windows \system32\ReAgent.dll	Dropped File	306.50 KB	application/vnd.microsoft.portable-executable	-	CLEAN
dcaeb590394b42d180e23e3cef4dd135513395b026e0ed489aec49848b85b8f0	\\?\C:\Windows \system32\recdisc.exe	Dropped File	232.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Create	CLEAN
64c30ee40b2e18bf9bb8e389a20668dc5e24ce51ff2ca38d5cdf6c8a2719056f	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
cad9b90b73aef995edf234d8d02852519dc40d938f9fcf75d664ca69c19826fb	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\roPrrI.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Users\KEECFM~1\AppData\Local\Temp\tmpg5eszf6e	Accessed File	Access, Read	CLEAN
C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll	Accessed File	Access, Read	CLEAN
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\verclsid.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\verifier.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\vmicsvc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\vssadmin.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\VSSVC.exe	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\Internet Explorer\iexplore.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\w32tm.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\waitfor.exe	Accessed File	Access, Read	CLEAN
C:\Program Files\MSBuild\outlook.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wbadmin.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wbengine.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wecutil.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WerFault.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WerFaultSecure.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wermgr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wevtutil.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wextract.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WFS.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\where.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\whoami.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wiaacmgr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wiawow64.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\wimserv.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsAnytimeUpgrade.exe	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\Microsoft\UProof\jzo	Accessed File	Access, Create	CLEAN
C:\Windows\system32\SyncHost.exe	Accessed File	Access	CLEAN
C:\Windows\system32\WSManHTTPConfig.exe	Accessed File	Access	CLEAN
C:\Windows\system32\mobsync.exe	Accessed File	Access	CLEAN
C:\Windows\system32\mtstocom.exe	Accessed File	Access	CLEAN
C:\Windows\system32\tracerpt.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\dxdiag.exe	Accessed File	Access	CLEAN
C:\Windows\system32\attrib.exe	Accessed File	Access	CLEAN
C:\Windows\system32\spreview.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\slc.dll	Accessed File	Access, Read	CLEAN
\\?\C:\Windows \system32\	Accessed File	Access, Delete, Create	CLEAN
\\?\C:\Windows \	Accessed File	Access, Delete, Create	CLEAN
C:\Windows\system32\VERSION.dll	Accessed File	Access, Read	CLEAN
\\?\C:\Windows \system32\slc.dll	Dropped File	Access, Write, Delete, Create	CLEAN
\\?\C:\Windows \system32\WindowsAnytimeUpgrade.exe	Dropped File	Access, Write, Delete, Create	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\fg0b\	Accessed File	Access, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\fg0b\VERSION.dll	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\fg0b\spreview.exe	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Windows\system32\rstrui.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ROUTE.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\msiexec.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\cmstp.exe	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Local\dOFgn\	Accessed File	Access, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\dOFgn\VERSION.dll	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\dOFgn\cmstp.exe	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Windows\system32\chkntfs.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\mcbuilder.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\diskpart.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\bcdboot.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\chkdsk.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\appidpolicyconverter.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\SystemPropertiesAdvanced.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ocsetup.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ktmutil.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RMActivate_ssp.exe	Accessed File	Access	CLEAN
C:\Windows\system32\AtBroker.exe	Accessed File	Access	CLEAN
C:\Windows\system32\clip.exe	Accessed File	Access	CLEAN
C:\Windows\system32\CompMgmtLauncher.exe	Accessed File	Access	CLEAN
C:\Windows\system32\replace.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\charmap.exe	Accessed File	Access	CLEAN
C:\Windows\system32\ftp.exe	Accessed File	Access	CLEAN
C:\Windows\system32\PkgMgr.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RunLegacyCPLElevated.exe	Accessed File	Access	CLEAN
C:\Windows\system32\odbcad32.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PnPutil.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\RMActivate_ssp_isv.exe	Accessed File	Access	CLEAN
C:\Windows\system32\logoff.exe	Accessed File	Access	CLEAN
C:\Windows\system32\plasrv.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ctfmon.exe	Accessed File	Access	CLEAN
C:\Windows\system32\Defrag.exe	Accessed File	Access	CLEAN
C:\Windows\system32\UI0Detect.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\odbcconf.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\openfiles.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\OptionalFeatures.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\osk.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\p2phost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PATHPING.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\pcalua.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\pcaui.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\pcawrk.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\pcwrun.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PING.EXE	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PnPUnattend.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\poqexec.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\powercfg.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PresentationHost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PresentationSettings.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\prevhost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\print.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PrintBrmUi.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\printfilterpipelinesvc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\PrintIsolationHost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\printui.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\proquota.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\psr.exe	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\PushPrinterConnections.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\qappsrv.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\qprocess.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\query.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\quser.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\qwinsta.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rasautou.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rasdial.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\raserver.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rasphone.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rdpclip.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\rdrleakdiag.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ReAgentc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\recdisc.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\ReAgent.dll	Accessed File	Access, Read	CLEAN
\\?\C:\Windows \system32\ReAgent.dll	Accessed File	Access, Write, Create	CLEAN
\\?\C:\Windows \system32\recdisc.exe	Dropped File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\	Accessed File	Access, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\VERSION.dll	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\UI0Detect.exe	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Windows\system32\SearchFilterHost.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\fsutil.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\logagent.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\DevicePairingWizard.exe	Accessed File	Access, Read	CLEAN
C:\Windows\system32\MFC42u.dll	Accessed File	Access, Read	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{bbfa96fb-03e2-244a-e13e-86541d1b182b}	access	roprri.exe	CLEAN
{ba62725d-6184-50d2-b706-2d7b865dd82b}	access	roprri.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
{2abfad8b-306f-ae21-21b6-6871f4adee91}	access	explorer.exe	CLEAN

Name	Operations	Parent Process Name	Verdict
{0f9efc60-2714-9348-bba5-dc278ba33013}	access	explorer.exe	CLEAN
{0fbd56d3-f3b8-edce-f394-613d71047fdd}	access	explorer.exe	CLEAN
{58078409-4d48-58c2-bbac-98f6809a0389}	access	explorer.exe	CLEAN
{6deb4144-d426-afcd-96ba-1febb5348581}	access	explorer.exe	CLEAN
{14a53b80-b6de-81e7-ed6c-2690e7bf017c}	access	explorer.exe	CLEAN
{93f0b9bd-750b-91aa-43ce-42ee557a016a}	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
{0de8b163-06f9-25fe-23a3-578eb97d6c5c}	access	explorer.exe	CLEAN
{821b3d72-6d45-a55c-2ff2-657dbbeba155}	access	explorer.exe	CLEAN
{1a7a0e3d-e642-9ee8-a175-339463130825}	access	explorer.exe	CLEAN
{8da6b341-b6ae-4ed6-a4db-b8d7a21d3ce2}	access	explorer.exe	CLEAN
{6bc7ca6d-1ff4-948e-acb8-8ace0ff7d262}	access	explorer.exe	CLEAN
{c048b0eb-b8ca-7103-8f33-90bb9cc094e1}	access	explorer.exe	CLEAN
{b5d19349-ced1-2973-477a-88f731ebad8b}	access	explorer.exe	CLEAN
{f6765311-c624-7d20-c394-3057b2a6af46}	access	explorer.exe	CLEAN
{61445a9f-32ce-1160-e05e-43b687216a6f}	access	explorer.exe	CLEAN
{89b9ed65-9a3a-f1c2-7aff-062779231709}	access	explorer.exe	CLEAN
{73aa5908-f17f-645c-b343-cc90c97db734}	access	explorer.exe	CLEAN
{144d5a95-7221-f17b-879b-9aacc036a420}	access	explorer.exe	CLEAN
{c84b0bc4-1cbf-767a-1a31-e366c8be89ca}	access	explorer.exe	CLEAN
{95f84887-1d41-9061-e67e-0279b6af17cd}	access	explorer.exe	CLEAN
{de76bbb7-2e89-6a07-4cb0-73d47f8864dc}	access	explorer.exe	CLEAN
{d435791e-8be2-87e1-800b-5c696b52a8f2}	access	explorer.exe	CLEAN
{8e35622f-5b01-99f1-24ca-7e2c1a23249b}	access	explorer.exe	CLEAN
{80663b84-20b8-3de1-5999-140e58d67c60}	access	explorer.exe	CLEAN
{d2e7374a-940d-481d-c27a-a6169257d900}	access	explorer.exe	CLEAN
{8dcd38ec-186f-5df8-2880-e7d897695e42}	access	explorer.exe	CLEAN
{dbf760ba-fee3-a258-2c95-0bf2ae6f687c}	access	explorer.exe	CLEAN
{d8e8ed8e-ed18-d8b2-20c5-9722faa1d0a2}	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

Name	Operations	Parent Process Name	Verdict
{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
{d3bb376e-cd4b-063e-153f-92e67d6bd5b4}	access	explorer.exe	CLEAN
{b6d3b4a4-6cfa-1231-4ff7-0ba6415393a1}	access	explorer.exe	CLEAN
{4ca4e63e-905e-107f-374f-1750e8740450}	access	explorer.exe	CLEAN
{e3da75c1-eb4d-4447-0f9d-3fa8c289e7a1}	access	explorer.exe	CLEAN
{de3f70ba-8476-26f1-9ee5-6932102a553e}	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
{49069b1e-63fa-179e-2a14-7912540c6c1f}	access	explorer.exe	CLEAN
{9f2637b5-de2f-b5e7-8510-77a247b76e7b}	access	explorer.exe	CLEAN
{5e610f68-9ac3-bcea-ac24-0b922ef757c5}	access	explorer.exe	CLEAN
{9bc542f4-d905-5d00-1c6b-cf1215fa0d5f}	access	explorer.exe	CLEAN
{d492c145-d614-09d7-9444-3394dde6cb98}	access	explorer.exe	CLEAN
{03ebac9a-7cb3-376a-2aba-295e5c829591}	access	explorer.exe	CLEAN
{5373e284-644b-01f2-8622-c8162783e2f3}	access	explorer.exe	CLEAN
{4b4afda5-e2b9-d796-ffdf-e673864c9758}	access	explorer.exe	CLEAN
{47b2fdeb-d3e8-4c0e-719e-412fa7dba8f3}	access	explorer.exe	CLEAN
{0664d2e9-8581-4188-4e98-08a66db38b34}	access	explorer.exe	CLEAN
{f026885f-91f2-ff2b-7bb4-4684c02ff166}	access	explorer.exe	CLEAN
{f5c7d9ea-5ce2-927d-e473-9ca230a5db3b}	access	explorer.exe	CLEAN
{7e336941-b8af-f8b8-8f2d-9baec07649fc}	access	explorer.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
-	access, create	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE	access	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	roprri.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	access, read	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	roprri.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	access, read	roprri.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin	access, read	roprri.exe, explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\PromptOnSecureDesktop	access, read	roprri.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
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

Registry Key	Operations	Parent Process Name	Verdict
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\{242596E0-609C-5095-99B4-19AC518EE9DA}	access, write	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{961EFF9D-BB8C-3A05-CE8E-AB9FF0211A1C}\ShellFolder\{9C723621-3B4C-B0E2-AED6-4F622B256BC7}	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\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 NT\InstallDate	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail	access, read	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook	access	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Clients\Mail\Microsoft Outlook\DllPathEx	access, read	explorer.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{71BC1377-8B48-A04B-D279-F048DCF94E7E}\ShellFolder\{82DD4CB4-45C1-3A12-16A7-34583B57EDDA}	access, write	explorer.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InstallDate	access, read	explorer.exe	CLEAN

Process

Process Name	Commandline	Verdict
spreview.exe	C:\Users\kEecfMwgj\AppData\Local\fg0b\spreview.exe	MALICIOUS
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpg5eszf6e" /s	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#1	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#10	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#11	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#13	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#14	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#15	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#16	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#17	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#18	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#19	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#2	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#20	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#21	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#22	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#23	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#24	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#25	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#26	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#27	CLEAN

Process Name	Commandline	Verdict
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#28	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#29	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#3	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#30	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#31	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#32	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#33	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#34	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#35	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#36	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#4	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#43	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#44	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#45	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#46	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#48	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#49	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#50	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#60	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#62	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#63	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#64	CLEAN

Process Name	Commandline	Verdict
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#65	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#66	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#67	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#68	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#69	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#7	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#72	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#73	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#74	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#75	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#76	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#77	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#78	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#79	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#8	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#80	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#81	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#82	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#83	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#84	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#85	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#86	CLEAN

Process Name	Commandline	Verdict
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#9	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BeginBufferedAnimation	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BeginBufferedPaint	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BeginPanningFeedback	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintClear	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintInit	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintRenderAnimation	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintSetAlpha	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintStopAllAnimations	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=BufferedPaintUnInit	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=CloseThemeData	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeBackground	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeBackgroundEx	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeEdge	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeIcon	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeParentBackground	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeParentBackgroundEx	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeText	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=DrawThemeTextEx	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EnableThemeDialogTexture	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EnableTheming	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EndBufferedAnimation	CLEAN

Process Name	Commandline	Verdict
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EndBufferedPaint	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=EndPanningFeedback	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetBufferedPaintBits	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetBufferedPaintDC	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetBufferedPaintTargetDC	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetBufferedPaintTargetRect	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetCurrentThemeName	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeAppProperties	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBackgroundContentRect	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBackgroundExtent	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBackgroundRegion	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBitmap	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeBool	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeColor	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeDocumentationProperty	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeEnumValue	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeFilename	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeFont	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeInt	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeIntList	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeMargins	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeMetric	CLEAN

Process Name	Commandline	Verdict
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemePartSize	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemePosition	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemePropertyOrigin	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeRect	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeStream	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeString	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysBool	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysColor	CLEAN
windowsanytimeupgrade.exe	C:\Windows\system32\WindowsAnytimeUpgrade.exe	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysColorBrush	CLEAN
spreview.exe	C:\Windows\system32\spreview.exe	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysFont	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysInt	CLEAN
windowsanytimeupgrade.exe	"C:\Windows \system32\WindowsAnytimeUpgrade.exe"	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysSize	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeSysString	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeTextExtent	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeTextMetrics	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetThemeTransitionDuration	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=GetWindowTheme	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=HitTestThemeBackground	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsAppThemed	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsCompositionActive	CLEAN

Process Name	Commandline	Verdict
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsThemeActive	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsThemeBackgroundPartiallyTransparent	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsThemeDialogTextureEnabled	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=IsThemePartDefined	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=OpenThemeData	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=OpenThemeDataEx	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=SetThemeAppProperties	CLEAN
rstrui.exe	C:\Windows\system32\rstrui.exe	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=SetWindowTheme	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=SetWindowThemeAttribute	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=ThemeInitApiHook	CLEAN
cmstp.exe	C:\Windows\system32\cmstp.exe	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=UpdatePanningFeedback	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#1 /fn_args="0"	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#10 /fn_args="0"	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#11 /fn_args="0"	CLEAN
roprri.exe	"C:\Users\kEecfMwgj\Desktop\roPrrI.exe" /dll="C:\Users\KEECFM~1\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll" /fn_id=#13 /fn_args="0"	CLEAN

Reduced dataset

YARA / AV

Antivirus (16)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\Desktop\7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a.exe.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\AppData\Local\fg0b\VERSION.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\AppData\Local\dOFgn\VERSION.dll	MALICIOUS
Dropped File	Trojan.GenericKDZ.76753	C:\Users\kEecfMwgj\AppData\Local\CtP9RYDd\VERSION.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
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
Memory Dump	Trojan.GenericKDZ.76753	-	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