MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll**
ID	#969104
MD5	31058530a762dc9f9bb34d28203f5314
SHA1	28c5d0fc080868ebb37050a565796f19a48eee87
SHA256	2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991
File Size	2292.00 KB
Report Created	2021-09-28 13:29 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 82 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	7	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #6) dkfqcooedk.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #24) explorer.exe as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #31) dkfqcooedk.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #32) dkfqcooedk.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #33) dkfqcooedk.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #45) dkfqcooedk.exe as "Gen:Variant.Mikey.113998".		
4/5	Injection	Modifies control flow of another process	6	-
	• (Process #6) dkfqcooedk.exe alters context of (process #24) explorer.exe. • (Process #15) dkfqcooedk.exe alters context of (process #24) explorer.exe. • (Process #27) dkfqcooedk.exe alters context of (process #24) explorer.exe. • (Process #6) dkfqcooedk.exe alters context of (process #26) shellexperiencehost.exe. • (Process #15) dkfqcooedk.exe alters context of (process #26) shellexperiencehost.exe. • (Process #27) dkfqcooedk.exe alters context of (process #26) shellexperiencehost.exe.		
3/5	Discovery	Reads installed applications	1	Spyware
	• Reads installed programs by enumerating the SOFTWARE registry key.			
2/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #24) explorer.exe creates a new explorer.exe process.			
1/5	Discovery	Reads system data	29	-

Score	Category	Operation	Count	Classification
		• (Process #6) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #2) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #4) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #3) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #5) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #7) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #8) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #14) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #9) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #10) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #11) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #17) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #12) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #13) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #20) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #15) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #16) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #18) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #19) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #21) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #22) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #23) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #25) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #27) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #28) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #30) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #31) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #32) dkfqcooedk.exe reads the Windows installation date from registry. • (Process #34) dkfqcooedk.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	32	-

Score	Category	Operation	Count	Classification
		• (Process #6) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #2) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #4) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #3) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #6) dkfqcooedk.exe creates mutex with name "{20974a93-a551-df17-8967-748358091d34}". • (Process #5) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #7) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #8) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #14) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #9) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #10) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #11) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #17) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #12) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #13) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #20) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #15) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #16) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #18) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #19) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #15) dkfqcooedk.exe creates mutex with name "{20974a93-a551-df17-8967-748358091d34}". • (Process #21) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #22) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #23) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #25) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #27) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #28) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #27) dkfqcooedk.exe creates mutex with name "{20974a93-a551-df17-8967-748358091d34}". • (Process #30) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #31) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #32) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}". • (Process #34) dkfqcooedk.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".		
1/5	Obfuscation	Reads from memory of another process	3	-
		• (Process #6) dkfqcooedk.exe reads from (process #24) explorer.exe. • (Process #15) dkfqcooedk.exe reads from (process #24) explorer.exe. • (Process #27) dkfqcooedk.exe reads from (process #24) explorer.exe.		
1/5	Crash	A monitored process crashed	2	-
		• (Process #24) explorer.exe crashed. • (Process #15) dkfqcooedk.exe crashed.		
1/5	Obfuscation	Resolves API functions dynamically	1	-
		• (Process #24) explorer.exe resolves 25 API functions by name.		

Mitre ATT&CK Matrix

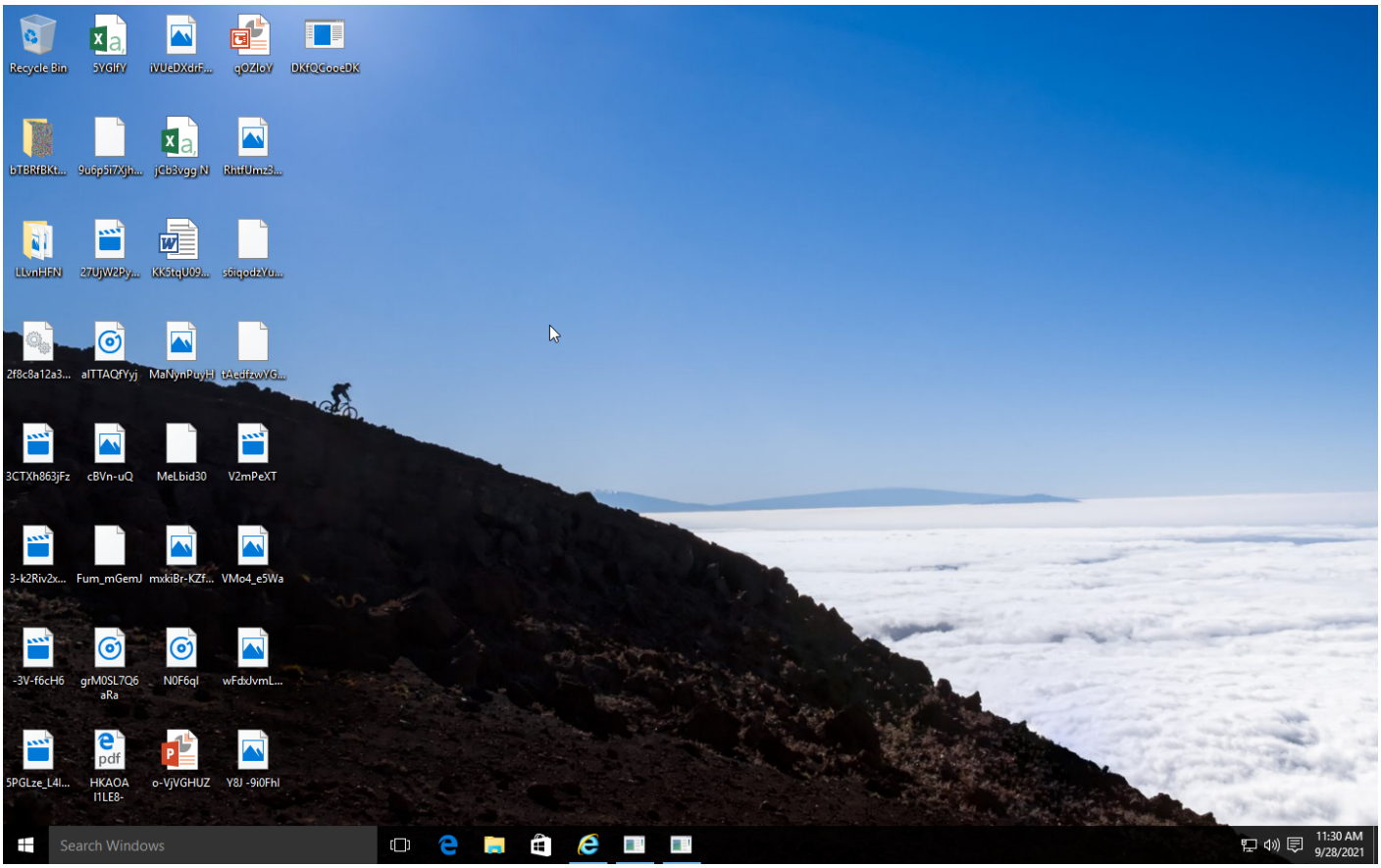
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing		#T1082 System Information Discovery					
						#T1012 Query Registry					

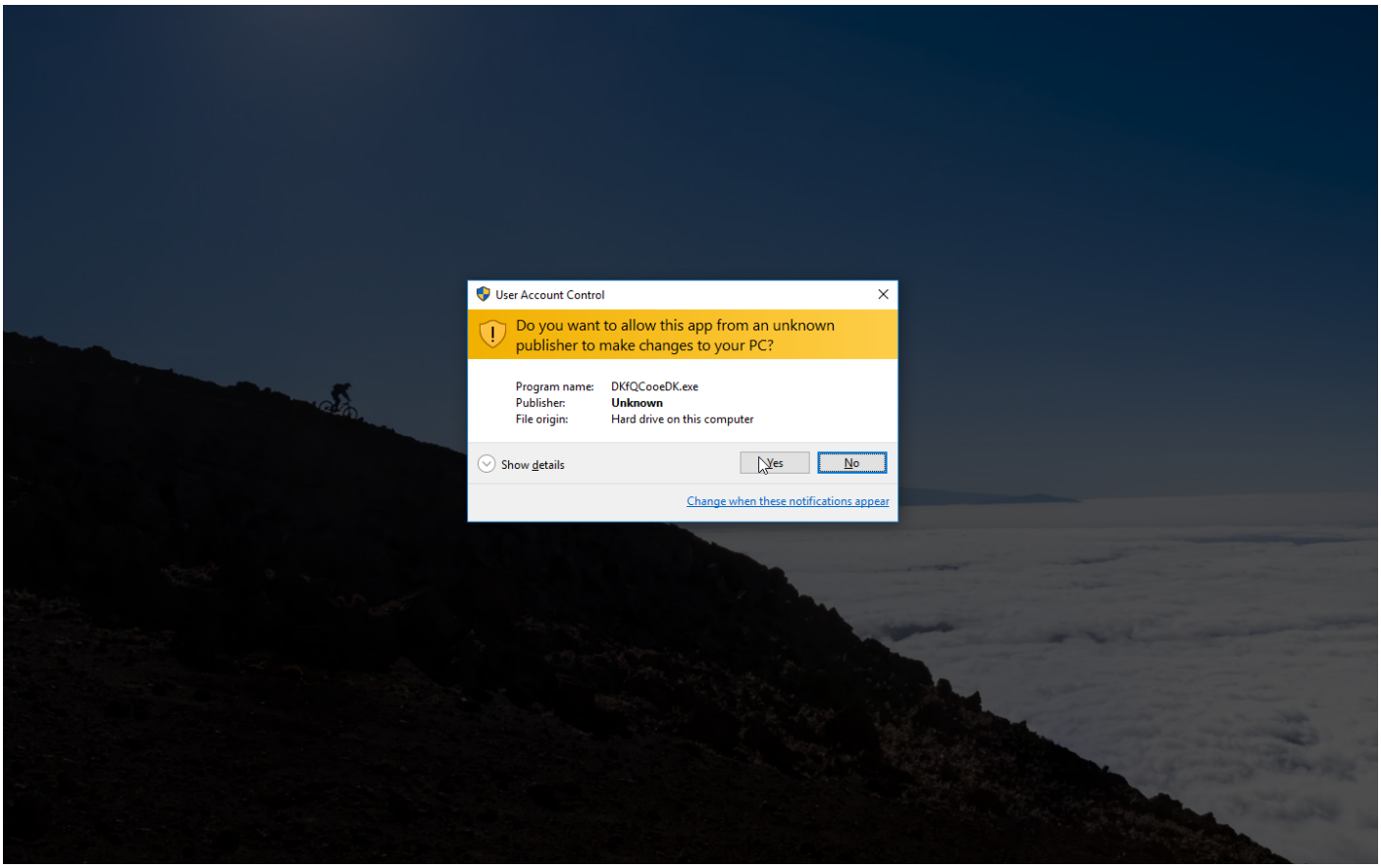
Sample Information

ID	#969104
MD5	31058530a762dc9f9bb34d28203f5314
SHA1	28c5d0fc080868ebb37050a565796f19a48eee87
SHA256	2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991
SSDeep	12288:xVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:AfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll
File Size	2292.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 13:29 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	47
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	7
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
5YGlfY
iVUeDXdrF...
qOZloY
DKfQCooeDK
bTBRfBKt...
9u6p5i7Xjh...
jCb3vgg N
RhtfUmzS...
LLvnHFN
27UjW2Py...
KK5tqU09...
s6iqodzYu...
2f8c8a12a3...
aITTAQfYyj
MaNynPuyH
tAedfzwYG...
3CTXh863jFz
cBVn-uQ
MeLbid30
V2mPeXT
3-k2Riv2x...
Fum_mGemJ
mxkiBr-KZf...
VMo4_e5Wa
-3V-f6cH6
grM0SL7Q6aRa
N0F6ql
wFdvJvmL...
5PGLze_L4l...
HKAOAI1LE8-
o-VjVGHUZ
Y8J -9i0Fhl
Search Windows
11:30 AM
9/28/2021


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

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

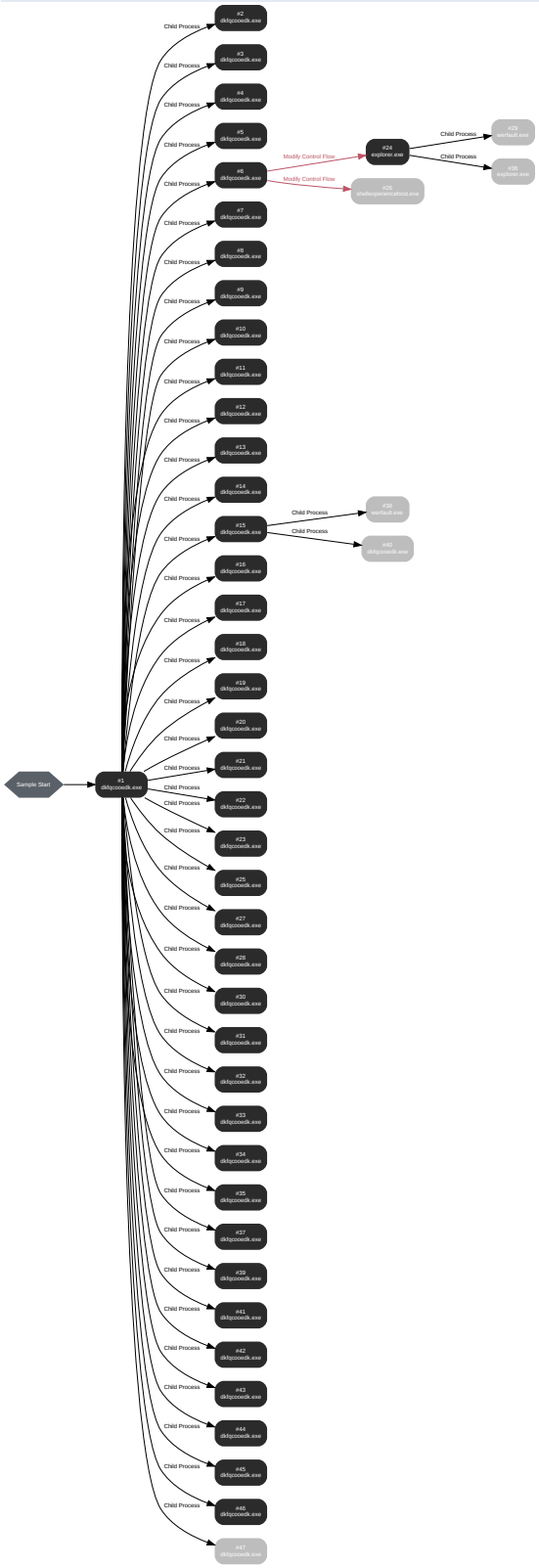
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: dkfqcooedk.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmprfp2gzup" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 68855, Reason: Analysis Target
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	248.39s
Return Code	Unknown
PID	3468
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	41

Process #2: dkfqcooedk.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 87358, Reason: Child Process
Unmonitor End Time	End Time: 140864, Reason: Terminated
Monitor duration	53.51s
Return Code	0
PID	1368
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #3: dkfqcooedk.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 88837, Reason: Child Process
Unmonitor End Time	End Time: 144213, Reason: Terminated
Monitor duration	55.38s
Return Code	0
PID	3700
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #4: dkfqcooedk.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 91816, Reason: Child Process
Unmonitor End Time	End Time: 143554, Reason: Terminated
Monitor duration	51.74s
Return Code	0
PID	1800
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	789
Mutex	7

Process #5: dkfqcooedk.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 93805, Reason: Child Process
Unmonitor End Time	End Time: 164370, Reason: Terminated
Monitor duration	70.56s
Return Code	0
PID	2688
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	7
Environment	2
Registry	789
Mutex	7

Process #6: dkfqcooedk.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingCodePage
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 96040, Reason: Child Process
Unmonitor End Time	End Time: 264338, Reason: Terminated
Monitor duration	168.30s
Return Code	0
PID	2552
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	36
Environment	2
Registry	789
Mutex	6
Process	2
-	49
-	32
-	122

Process #7: dkfqcooedk.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingName
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100855, Reason: Child Process
Unmonitor End Time	End Time: 185030, Reason: Terminated
Monitor duration	84.17s
Return Code	0
PID	2424
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	788
Mutex	7

Process #8: dkfqcooedk.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 104806, Reason: Child Process
Unmonitor End Time	End Time: 202450, Reason: Terminated
Monitor duration	97.64s
Return Code	0
PID	2064
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	787
Mutex	7

Process #9: dkfqcooedk.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 108650, Reason: Child Process
Unmonitor End Time	End Time: 219461, Reason: Terminated
Monitor duration	110.81s
Return Code	0
PID	2056
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #10: dkfqcooedk.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 118070, Reason: Child Process
Unmonitor End Time	End Time: 227177, Reason: Terminated
Monitor duration	109.11s
Return Code	0
PID	2620
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #11: dkfqcooedk.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 123711, Reason: Child Process
Unmonitor End Time	End Time: 228290, Reason: Terminated
Monitor duration	104.58s
Return Code	0
PID	1156
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #12: dkfqcooedk.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 131034, Reason: Child Process
Unmonitor End Time	End Time: 242428, Reason: Terminated
Monitor duration	111.39s
Return Code	0
PID	3868
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #13: dkfqcooedk.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 141616, Reason: Child Process
Unmonitor End Time	End Time: 247951, Reason: Terminated
Monitor duration	106.33s
Return Code	0
PID	2272
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #14: dkfqcooedk.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 148307, Reason: Child Process
Unmonitor End Time	End Time: 207561, Reason: Terminated
Monitor duration	59.25s
Return Code	0
PID	2308
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #15: dkfqcooedk.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 160271, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Crashed
Monitor duration	156.97s
Return Code	Unknown
PID	3792
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	56
-	1
-	108

Process #16: dkfqcooedk.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlReaderInputWithEncodingName /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 170621, Reason: Child Process
Unmonitor End Time	End Time: 274610, Reason: Terminated
Monitor duration	103.99s
Return Code	0
PID	2560
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #17: dkfqcooedk.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 179753, Reason: Child Process
Unmonitor End Time	End Time: 240285, Reason: Terminated
Monitor duration	60.53s
Return Code	0
PID	4312
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #18: dkfqcooedk.exe

ID	18
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186594, Reason: Child Process
Unmonitor End Time	End Time: 278362, Reason: Terminated
Monitor duration	91.77s
Return Code	0
PID	4404
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #19: dkfqcooedk.exe

ID	19
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 191947, Reason: Child Process
Unmonitor End Time	End Time: 278369, Reason: Terminated
Monitor duration	86.42s
Return Code	0
PID	4024
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #20: dkfqcooedk.exe

ID	20
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 198861, Reason: Child Process
Unmonitor End Time	End Time: 247812, Reason: Terminated
Monitor duration	48.95s
Return Code	0
PID	4748
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #21: dkfqcooedk.exe

ID	21
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 207395, Reason: Child Process
Unmonitor End Time	End Time: 281354, Reason: Terminated
Monitor duration	73.96s
Return Code	0
PID	3336
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #22: dkfqcooedk.exe

ID	22
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlReaderInputWithEncodingName /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 216202, Reason: Child Process
Unmonitor End Time	End Time: 286084, Reason: Terminated
Monitor duration	69.88s
Return Code	0
PID	96
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #23: dkfqcooedk.exe

ID	23
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 227626, Reason: Child Process
Unmonitor End Time	End Time: 290526, Reason: Terminated
Monitor duration	62.90s
Return Code	0
PID	816
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #24: explorer.exe

ID	24
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 236980, Reason: Injection
Unmonitor End Time	End Time: 317246, Reason: Crashed
Monitor duration	80.27s
Return Code	Unknown
PID	1636
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (150)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x668	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x690	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x694	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6bc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6dc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6e8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x71c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x734	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x73c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x74c	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x798	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x7a8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x7b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x7d0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x7ec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x7f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x460	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x83c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x954	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x9c0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xbec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x4c4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x4ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x8b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x984	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x97c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xa20	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xff8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x328	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xc94	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xc70	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xcdc	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0xdd0	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0xdbc	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x62c	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0xa34	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0xbe8	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x69c	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x1380	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0xc28	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5f8bb580(140721911477632)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c: \users\rdhj0cnfevzx\desktop \dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5f8bb580(140721911477632)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0x6b4	0x7ffc5ecdce60(140721899032160)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x668	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x690	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x694	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x6ac	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x6b0	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x6b4	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x6b8	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x6bc	0x7ffc5f8b4f00(140721911451392)	-	✔	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x6dc	0x7ffc5f8b4f00(140721911451392)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x6e8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x71c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x734	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x73c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x74c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x798	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x7a8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x7b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x7d0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x7ec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x7f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x460	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x83c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x954	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x9c0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xbec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x4c4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x4ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x8b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x984	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x97c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xa20	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xff8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x328	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xc94	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xc70	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xcdc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xdd0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xdbc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x62c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xa34	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xbe8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x69c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x1380	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xc28	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x12fc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x1038	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x9f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x4d0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x738	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x1310	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0x4c8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x668	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x690	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x694	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x6ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x6b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x6b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x6b8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x6bc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x6dc	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x6e8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x71c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x734	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x73c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x74c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x798	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x7a8	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x7b0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x7d0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x7ec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x7f0	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x460	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x83c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x954	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x9c0	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0xbec	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x4c4	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x4ac	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0x8b4	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Host Behavior

Type	Count
Module	38
File	109
System	1
Registry	13

Process #25: dkfqcooedk.exe

ID	25
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 238690, Reason: Child Process
Unmonitor End Time	End Time: 293325, Reason: Terminated
Monitor duration	54.63s
Return Code	0
PID	1560
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	730
Mutex	7

Process #26: shellexperiencehost.exe

ID	26
File Name	c:\windows\systemapps\shellexperiencehost_cw5n1h2txyewy\shellexperiencehost.exe
Command Line	"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
Initial Working Directory	C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\
Monitor Start Time	Start Time: 239189, Reason: Injection
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	78.06s
Return Code	Unknown
PID	2660
Parent PID	628
Bitness	64 Bit

Injection Information (9)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xa8c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xb50	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#6: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x858 / 0xa70	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xa8c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xb50	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#15: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x13b0 / 0xa70	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0xa8c	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0xb50	0x7ffc5f8b4f00(140721911451392)	-	✓	1
Modify Control Flow	#27: c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe	0x7cc / 0xa70	0x7ffc5f8b4f00(140721911451392)	-	✓	1

Process #27: dkfqcooedk.exe

ID	27
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 246105, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	71.14s
Return Code	Unknown
PID	1732
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	8
Environment	2
Registry	771
Mutex	5
Process	2
-	56
-	1
-	108

Process #28: dkfqcooedk.exe

ID	28
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 252868, Reason: Child Process
Unmonitor End Time	End Time: 301857, Reason: Terminated
Monitor duration	48.99s
Return Code	0
PID	2816
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #29: werfault.exe

ID	29
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1636 -s 5408
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 260497, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	56.75s
Return Code	Unknown
PID	1092
Parent PID	1636
Bitness	64 Bit

Process #30: dkfqcooedk.exe

ID	30
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 266453, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	50.79s
Return Code	Unknown
PID	3148
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #31: dkfqcooedk.exe

ID	31
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlReaderInputWithEncodingName /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 275771, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	41.48s
Return Code	Unknown
PID	2580
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #32: dkfqcooedk.exe

ID	32
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 279091, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	38.16s
Return Code	Unknown
PID	3288
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
Mutex	7

Process #33: dkfqcooedk.exe

ID	33
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 282041, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	35.20s
Return Code	Unknown
PID	1204
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	27
File	112
System	1
Environment	2
Registry	59

Process #34: dkfqcooedk.exe

ID	34
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 285308, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	31.94s
Return Code	Unknown
PID	4776
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	1
Environment	2
Registry	226
Mutex	3

Process #35: dkfqcooedk.exe

ID	35
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 289058, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	28.19s
Return Code	Unknown
PID	3268
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #36: explorer.exe

ID	36
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 291816, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	25.43s
Return Code	Unknown
PID	4540
Parent PID	1636
Bitness	64 Bit

Process #37: dkfqcooedk.exe

ID	37
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 292175, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	25.07s
Return Code	Unknown
PID	4056
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #38: werfault.exe

ID	38
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 3792 -s 684
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 292735, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	24.51s
Return Code	Unknown
PID	4612
Parent PID	3792
Bitness	64 Bit

Process #39: dkfqcooedk.exe

ID	39
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 292979, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	24.27s
Return Code	Unknown
PID	4648
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #40: dkfqcooedk.exe

ID	40
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 293034, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	24.21s
Return Code	Unknown
PID	4588
Parent PID	3792
Bitness	64 Bit

Process #41: dkfqcooedk.exe

ID	41
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 294007, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	23.24s
Return Code	Unknown
PID	4804
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #42: dkfqcooedk.exe

ID	42
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 295081, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	22.16s
Return Code	Unknown
PID	3432
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #43: dkfqcooedk.exe

ID	43
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 297780, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	19.47s
Return Code	Unknown
PID	1484
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #44: dkfqcooedk.exe

ID	44
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 298459, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	18.79s
Return Code	Unknown
PID	1456
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #45: dkfqcooedk.exe

ID	45
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C: \Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" / fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 301921, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	15.32s
Return Code	Unknown
PID	2624
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #46: dkfqcooedk.exe

ID	46
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 306803, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	10.44s
Return Code	Unknown
PID	3736
Parent PID	3468
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #47: dkfqcooedk.exe

ID	47
File Name	c:\users\rdhj0cnfevzx\desktop\dkfqcooedk.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 311154, Reason: Child Process
Unmonitor End Time	End Time: 317246, Reason: Terminated by Timeout
Monitor duration	6.09s
Return Code	Unknown
PID	1688
Parent PID	3468
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991	C:\Users\RDhJ0CNFevzX\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll, C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll	Sample File	2292.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmprfp2gzup	Accessed File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll	Accessed File	Read, Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\Explorer.EXE	Accessed File	Access	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
127.0.0.1	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	dkfqcooedk.exe	CLEAN
{20974a93-a551-df17-8967-748358091d34}	access	dkfqcooedk.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
-	create, access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate	read, access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	access	dkfqcooedk.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA	read, access	dkfqcooedk.exe	CLEAN

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

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmprfp2gzup" /s	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingCodePage	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingName	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="0"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="0"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="0"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="0"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="0"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="0"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="1"	CLEAN

Process Name	Commandline	Verdict
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="Install"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="Install"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="Install"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="Install"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="Install"	CLEAN
shellexperiencehost.exe	"C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="Install"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="DefaultInstall"	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1636 -s 5408	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="DefaultInstall"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="DefaultInstall"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="DefaultInstall"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="DefaultInstall"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="DefaultInstall"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="127.0.0.1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="127.0.0.1"	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 3792 -s 684	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="127.0.0.1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="127.0.0.1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingCodePage /fn_args="127.0.0.1"	CLEAN

Process Name	Commandline	Verdict
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriterOutputWithEncodingName /fn_args="127.0.0.1"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReader /fn_args="explorer.exe"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingCodePage /fn_args="explorer.exe"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlReaderInputWithEncodingName /fn_args="explorer.exe"	CLEAN
dkfqcooedk.exe	"C:\Users\RDhJ0CNFevzX\Desktop\DKfQCooeDK.exe" /dll="C:\Users\RDHJ0C~1\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll" /fn_id=CreateXmlWriter /fn_args="explorer.exe"	CLEAN

YARA / AV

Antivirus (7)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\2f8c8a12a31d244689c70b428031eb90f3b791323ab6dfa45e2a3d5921877991.exe.dll	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Trojan.GenericKDZ.76753	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS
Memory Dump	Gen:Variant.Mikey.113998	-	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
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	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB

User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows