MALICIOUS

Classifications: Spyware

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

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll**
ID	#2782997
MD5	cbaf988697e5794257533479c39ed20a
SHA1	02d31d47c4bcb4285e847634be7483a31986b29e
SHA256	8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8
File Size	1220.00 KB
Report Created	2021-09-28 14:41 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 129 matches)

Score	Category	Operation	Count	Classification
4/5	Antivirus	Malicious content was detected by heuristic scan	6	-
	• Built-in AV detected the sample itself as "Trojan.GenericKDZ.76753". • Built-in AV detected a memory dump of (process #2) tasyggycx.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #6) tasyggycx.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 #17) tasyggycx.exe as "Gen:Variant.Mikey.113998". • Built-in AV detected a memory dump of (process #64) tasyggycx.exe as "Gen:Variant.Mikey.113998".		
4/5	Injection	Modifies control flow of another process	4	-
	• (Process #2) tasyggycx.exe alters context of (process #14) explorer.exe. • (Process #9) tasyggycx.exe alters context of (process #14) explorer.exe. • (Process #16) tasyggycx.exe alters context of (process #14) explorer.exe. • (Process #29) tasyggycx.exe alters context of (process #14) explorer.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 #14) explorer.exe creates a new explorer.exe process.		
1/5	Discovery	Reads system data	48	-

Score	Category	Operation	Count	Classification
		• (Process #2) tasyggycx.exe reads the Windows installation date from registry. • (Process #3) tasyggycx.exe reads the Windows installation date from registry. • (Process #4) tasyggycx.exe reads the Windows installation date from registry. • (Process #5) tasyggycx.exe reads the Windows installation date from registry. • (Process #6) tasyggycx.exe reads the Windows installation date from registry. • (Process #7) tasyggycx.exe reads the Windows installation date from registry. • (Process #8) tasyggycx.exe reads the Windows installation date from registry. • (Process #9) tasyggycx.exe reads the Windows installation date from registry. • (Process #10) tasyggycx.exe reads the Windows installation date from registry. • (Process #11) tasyggycx.exe reads the Windows installation date from registry. • (Process #12) tasyggycx.exe reads the Windows installation date from registry. • (Process #17) tasyggycx.exe reads the Windows installation date from registry. • (Process #13) tasyggycx.exe reads the Windows installation date from registry. • (Process #15) tasyggycx.exe reads the Windows installation date from registry. • (Process #16) tasyggycx.exe reads the Windows installation date from registry. • (Process #19) tasyggycx.exe reads the Windows installation date from registry. • (Process #20) tasyggycx.exe reads the Windows installation date from registry. • (Process #21) tasyggycx.exe reads the Windows installation date from registry. • (Process #22) tasyggycx.exe reads the Windows installation date from registry. • (Process #23) tasyggycx.exe reads the Windows installation date from registry. • (Process #24) tasyggycx.exe reads the Windows installation date from registry. • (Process #25) tasyggycx.exe reads the Windows installation date from registry. • (Process #26) tasyggycx.exe reads the Windows installation date from registry. • (Process #29) tasyggycx.exe reads the Windows installation date from registry. • (Process #31) tasyggycx.exe reads the Windows installation date from registry. • (Process #32) tasyggycx.exe reads the Windows installation date from registry. • (Process #33) tasyggycx.exe reads the Windows installation date from registry. • (Process #34) tasyggycx.exe reads the Windows installation date from registry. • (Process #35) tasyggycx.exe reads the Windows installation date from registry. • (Process #42) tasyggycx.exe reads the Windows installation date from registry. • (Process #36) tasyggycx.exe reads the Windows installation date from registry. • (Process #37) tasyggycx.exe reads the Windows installation date from registry. • (Process #38) tasyggycx.exe reads the Windows installation date from registry. • (Process #39) tasyggycx.exe reads the Windows installation date from registry. • (Process #43) tasyggycx.exe reads the Windows installation date from registry. • (Process #44) tasyggycx.exe reads the Windows installation date from registry. • (Process #45) tasyggycx.exe reads the Windows installation date from registry. • (Process #46) tasyggycx.exe reads the Windows installation date from registry. • (Process #47) tasyggycx.exe reads the Windows installation date from registry. • (Process #48) tasyggycx.exe reads the Windows installation date from registry. • (Process #52) tasyggycx.exe reads the Windows installation date from registry. • (Process #53) tasyggycx.exe reads the Windows installation date from registry. • (Process #51) tasyggycx.exe reads the Windows installation date from registry. • (Process #54) tasyggycx.exe reads the Windows installation date from registry. • (Process #55) tasyggycx.exe reads the Windows installation date from registry. • (Process #57) tasyggycx.exe reads the Windows installation date from registry. • (Process #59) tasyggycx.exe reads the Windows installation date from registry. • (Process #60) tasyggycx.exe reads the Windows installation date from registry.		
1/5	Mutex	Creates mutex	55	-

- (Process #2) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #3) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #4) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #2) tasyggycx.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #5) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #6) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #7) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #8) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #9) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #10) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #9) tasyggycx.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #11) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #12) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #17) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #13) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #15) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #16) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #19) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #16) tasyggycx.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #20) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #21) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #22) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #23) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #24) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #25) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #26) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #29) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #31) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #32) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #29) tasyggycx.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #33) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #34) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #35) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #42) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #36) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #37) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #38) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #39) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #38) tasyggycx.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #43) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #44) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #45) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #46) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #47) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #45) tasyggycx.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #48) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #51) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #52) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #53) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #54) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #55) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #57) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #55) tasyggycx.exe creates mutex with name "{54137ce8-d76d-e7fc-dec3-c85f290e5b98}".
- (Process #59) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".
- (Process #60) tasyggycx.exe creates mutex with name "{0aa26147-58aa-e888-6782-4bac88c336bd}".

Score	Category	Operation	Count	Classification
1/5	Obfuscation	Reads from memory of another process	7	-

- (Process #2) tasyggycx.exe reads from (process #14) explorer.exe.
- (Process #9) tasyggycx.exe reads from (process #14) explorer.exe.
- (Process #16) tasyggycx.exe reads from (process #14) explorer.exe.
- (Process #29) tasyggycx.exe reads from (process #14) explorer.exe.
- (Process #38) tasyggycx.exe reads from (process #14) explorer.exe.
- (Process #45) tasyggycx.exe reads from (process #14) explorer.exe.
- (Process #55) tasyggycx.exe reads from (process #14) explorer.exe.

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

- (Process #14) explorer.exe resolves 25 API functions by name.

Score	Category	Operation	Count	Classification
1/5	Crash	A monitored process crashed	6	-

- (Process #14) explorer.exe crashed.
- (Process #9) tasyggycx.exe crashed.
- (Process #16) tasyggycx.exe crashed.
- (Process #29) tasyggycx.exe crashed.
- (Process #38) tasyggycx.exe crashed.
- (Process #45) tasyggycx.exe crashed.

Mitre ATT&CK Matrix

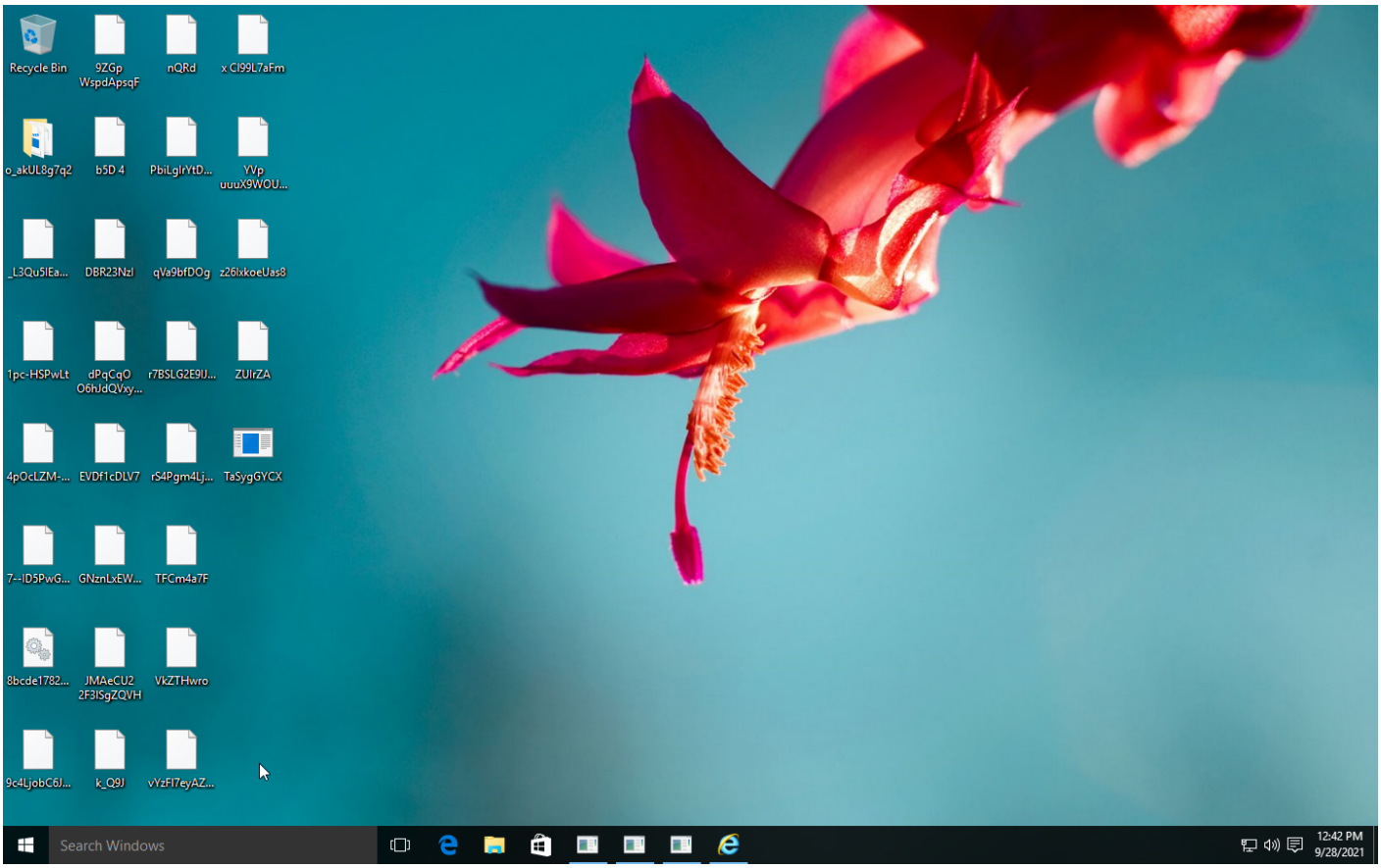
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing		#T1082 System Information Discovery					
						#T1012 Query Registry					

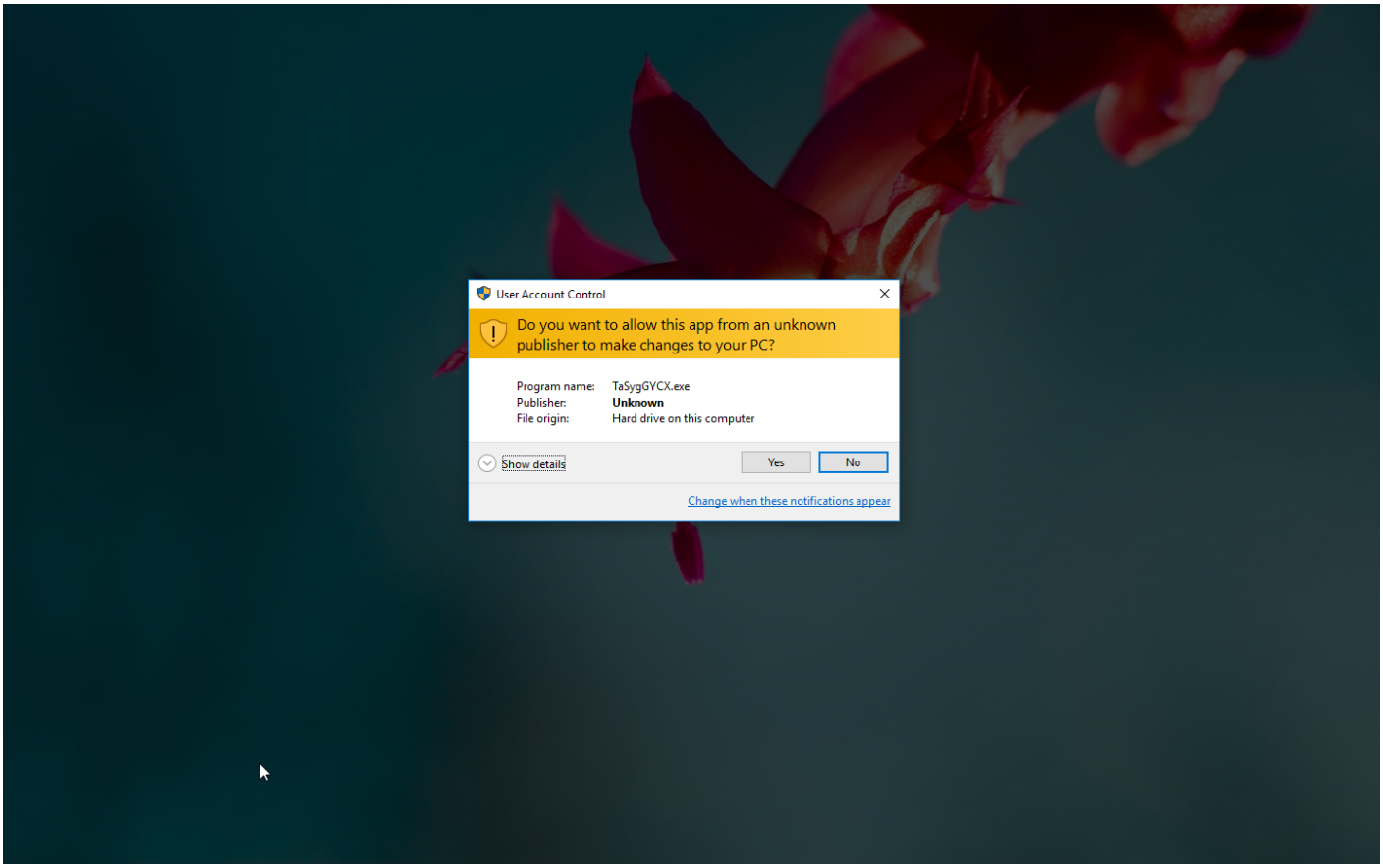
Sample Information

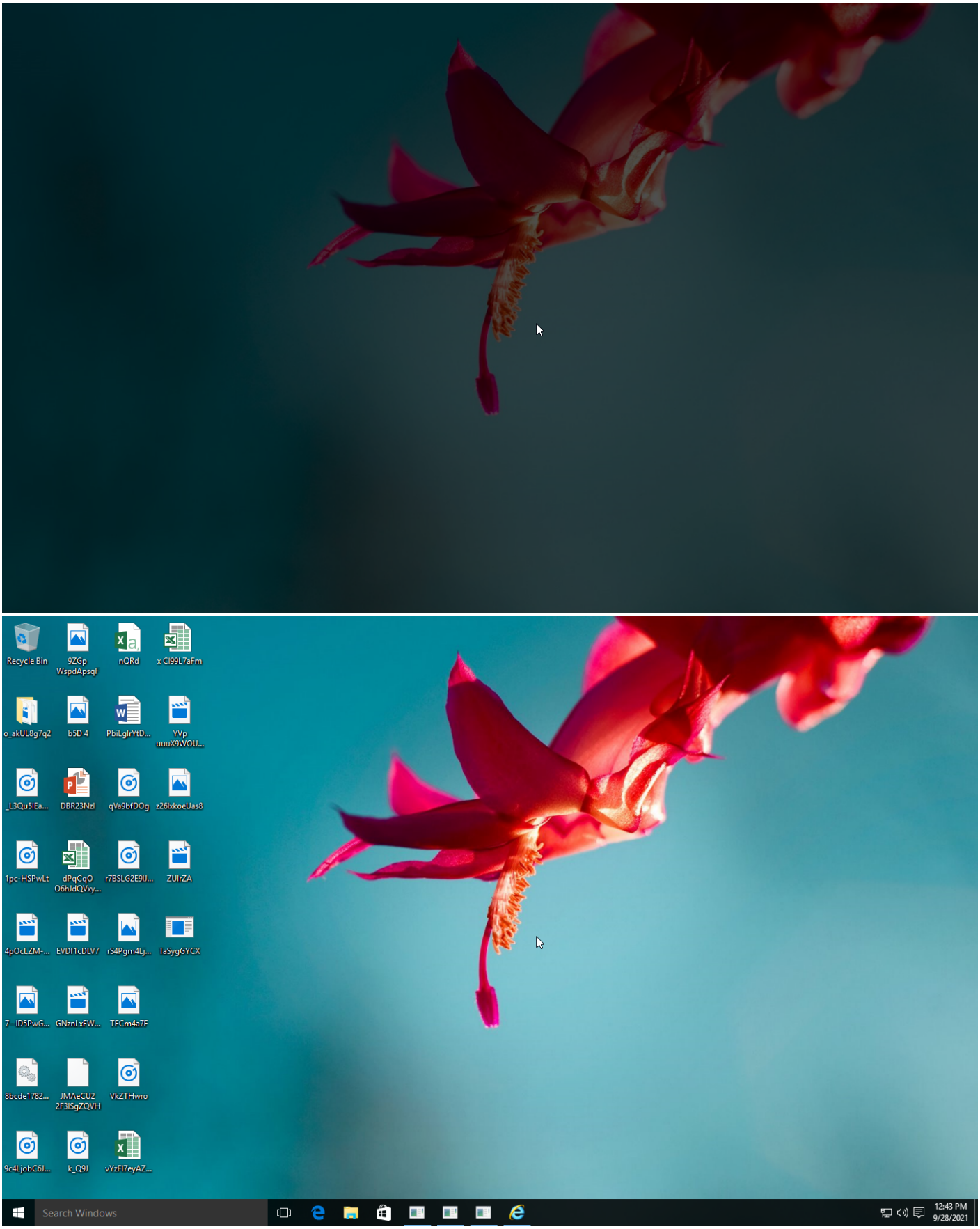
ID	#2782997
MD5	cbaf988697e5794257533479c39ed20a
SHA1	02d31d47c4bcb4285e847634be7483a31986b29e
SHA256	8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8
SSDeep	12288:qVl0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:3fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
ImpHash	6668be91e2c948b183827f040944057f
File Name	8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll
File Size	1220.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 14:41 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	67
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	6
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
9ZGp WspdApsqF
nQRd
x CI99L7aFm
o_akUL8g7q2
b5D 4
PbiLglrYtD...
YVp uuuX9WOU...
_L3Qu5lEa...
DBR23Nzl
qVa9bfDOg
z26lxkoeUas8
1pc-HSPwLt
dPqCqO O6hJdQVxy...
r7BSLG2E9U...
ZUlrZA
4pOcLZM-...
EVDf1cDLV7
rS4Pgm4Lj...
TaSygGYCX
7--ID5PwG...
GNznLxEW...
TFCm4a7F
8bcde1782...
JMAeCU2 2F3ISgZQVH
VkZTHwro
9c4LjobC6J...
k_Q9J
vYzFI7eyAZ...
Search Windows
12:42 PM
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: TaSygGYCX.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

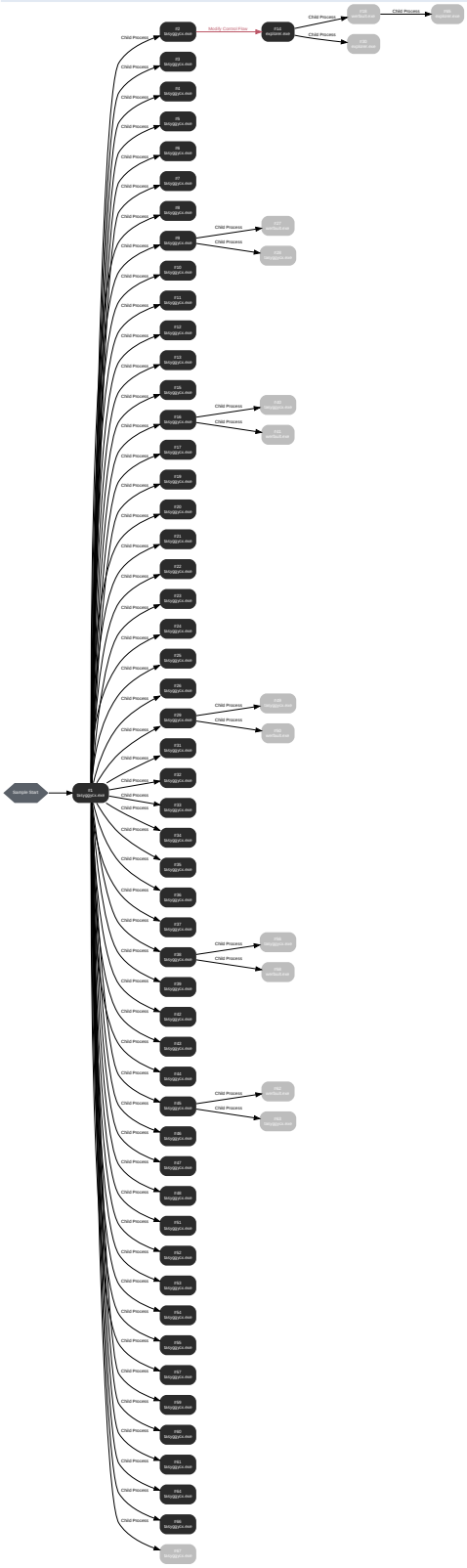
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: tasyggycx.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpo74kwsx1" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 72030, Reason: Analysis Target
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	243.31s
Return Code	Unknown
PID	3288
Parent PID	1600
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	53

Process #2: tasyggycx.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 91931, Reason: Child Process
Unmonitor End Time	End Time: 163712, Reason: Terminated
Monitor duration	71.78s
Return Code	0
PID	2708
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	36
Environment	2
Registry	789
Mutex	6
Process	2
-	42
-	32
-	108

Process #3: tasyggycx.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoByHandle
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 94395, Reason: Child Process
Unmonitor End Time	End Time: 121552, Reason: Terminated
Monitor duration	27.16s
Return Code	0
PID	2628
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #4: tasyggycx.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 95759, Reason: Child Process
Unmonitor End Time	End Time: 129521, Reason: Terminated
Monitor duration	33.76s
Return Code	0
PID	1900
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #5: tasyggycx.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 98016, Reason: Child Process
Unmonitor End Time	End Time: 138971, Reason: Terminated
Monitor duration	40.95s
Return Code	0
PID	2508
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #6: tasyggycx.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100853, Reason: Child Process
Unmonitor End Time	End Time: 148131, Reason: Terminated
Monitor duration	47.28s
Return Code	0
PID	1880
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	8
Environment	2
Registry	789
Mutex	7

Process #7: tasyggycx.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 105186, Reason: Child Process
Unmonitor End Time	End Time: 152470, Reason: Terminated
Monitor duration	47.28s
Return Code	0
PID	1904
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #8: tasyggycx.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 110453, Reason: Child Process
Unmonitor End Time	End Time: 160951, Reason: Terminated
Monitor duration	50.50s
Return Code	0
PID	1952
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #9: tasyggycx.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 115372, Reason: Child Process
Unmonitor End Time	End Time: 236182, Reason: Crashed
Monitor duration	120.81s
Return Code	1114
PID	1948
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	788
Mutex	6
Process	2
-	43
-	1
-	82
Window	1

Process #10: tasyggycx.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 119824, Reason: Child Process
Unmonitor End Time	End Time: 172432, Reason: Terminated
Monitor duration	52.61s
Return Code	0
PID	2612
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #11: tasyggycx.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 125353, Reason: Child Process
Unmonitor End Time	End Time: 178302, Reason: Terminated
Monitor duration	52.95s
Return Code	0
PID	2104
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #12: tasyggycx.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 130036, Reason: Child Process
Unmonitor End Time	End Time: 184287, Reason: Terminated
Monitor duration	54.25s
Return Code	0
PID	4756
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #13: tasyggycx.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 137040, Reason: Child Process
Unmonitor End Time	End Time: 189636, Reason: Terminated
Monitor duration	52.60s
Return Code	0
PID	4016
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	786
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: 143168, Reason: Injection
Unmonitor End Time	End Time: 315340, Reason: Crashed
Monitor duration	172.17s
Return Code	Unknown
PID	1600
Parent PID	18446744073709551615
Bitness	64 Bit

Injection Information (150)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xe34	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xe54	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xf40	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xfe0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xfe8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xce0	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x77c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x124c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x1334	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0xe58	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb28bab580(140716696843648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb28bab580(140716696843648)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#2: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x131c / 0x69c	0x7ffb2623ce60(140716653399648)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x684	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✔	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✔	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xe34	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xe54	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xf40	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xfe0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xfe8	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xce0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x77c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x124c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x1334	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0xe58	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#9: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0x978 / 0x12ec	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x684	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x688	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x68c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x69c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x6a4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x6a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x6b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x6b8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x6c8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x6d0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x6d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x6f0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x710	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x728	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x73c	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x75c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x764	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x768	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x774	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x7a8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x7b4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xa9c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xb94	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xbf8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xbfc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x8b0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x5d4	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x8bc	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x928	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xe34	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xe54	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xf40	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xfe0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xfe8	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xce0	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x77c	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x124c	0x7ffb28ba4f00(140716696817408)	-	✓	1

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x1334	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0xe58	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#16: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xd50 / 0x12ec	0x7ffb28ba4f00(140716696817408)	-	✓	1
Modify Control Flow	#29: c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe	0xf14 / 0x644	0x7ffb28ba4f00(140716696817408)	-	✓	1

Host Behavior

Type	Count
Module	37
File	109

Process #15: tasyggycx.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 147675, Reason: Child Process
Unmonitor End Time	End Time: 194067, Reason: Terminated
Monitor duration	46.39s
Return Code	0
PID	3008
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #16: tasyggycx.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 153978, Reason: Child Process
Unmonitor End Time	End Time: 274947, Reason: Crashed
Monitor duration	120.97s
Return Code	1114
PID	4784
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	43
-	1
-	82
Window	1

Process #17: tasyggycx.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 161878, Reason: Child Process
Unmonitor End Time	End Time: 188292, Reason: Terminated
Monitor duration	26.41s
Return Code	0
PID	4612
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #18: werfault.exe

ID	18
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1600 -s 4424
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 162155, Reason: Child Process
Unmonitor End Time	End Time: 312891, Reason: Terminated
Monitor duration	150.74s
Return Code	0
PID	4664
Parent PID	1600
Bitness	64 Bit

Process #19: tasyggycx.exe

ID	19
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 168259, Reason: Child Process
Unmonitor End Time	End Time: 216447, Reason: Terminated
Monitor duration	48.19s
Return Code	0
PID	1264
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #20: tasyggycx.exe

ID	20
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 171537, Reason: Child Process
Unmonitor End Time	End Time: 219130, Reason: Terminated
Monitor duration	47.59s
Return Code	0
PID	2220
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #21: tasyggycx.exe

ID	21
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 174604, Reason: Child Process
Unmonitor End Time	End Time: 226161, Reason: Terminated
Monitor duration	51.56s
Return Code	0
PID	4968
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #22: tasyggycx.exe

ID	22
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoByHandle /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 178823, Reason: Child Process
Unmonitor End Time	End Time: 225536, Reason: Terminated
Monitor duration	46.71s
Return Code	0
PID	464
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #23: tasyggycx.exe

ID	23
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 183405, Reason: Child Process
Unmonitor End Time	End Time: 232141, Reason: Terminated
Monitor duration	48.74s
Return Code	0
PID	176
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #24: tasyggycx.exe

ID	24
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 187147, Reason: Child Process
Unmonitor End Time	End Time: 237150, Reason: Terminated
Monitor duration	50.00s
Return Code	0
PID	1380
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #25: tasyggycx.exe

ID	25
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 190878, Reason: Child Process
Unmonitor End Time	End Time: 240827, Reason: Terminated
Monitor duration	49.95s
Return Code	0
PID	2684
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #26: tasyggycx.exe

ID	26
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 193771, Reason: Child Process
Unmonitor End Time	End Time: 244657, Reason: Terminated
Monitor duration	50.89s
Return Code	0
PID	5064
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #27: werfault.exe

ID	27
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1948 -s 628
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 195768, Reason: Child Process
Unmonitor End Time	End Time: 228286, Reason: Terminated
Monitor duration	32.52s
Return Code	0
PID	3272
Parent PID	1948
Bitness	64 Bit

Process #28: tasyggycx.exe

ID	28
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 195902, Reason: Child Process
Unmonitor End Time	End Time: 228357, Reason: Terminated
Monitor duration	32.45s
Return Code	259
PID	1616
Parent PID	1948
Bitness	64 Bit

Process #29: tasyggycx.exe

ID	29
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 196512, Reason: Child Process
Unmonitor End Time	End Time: 300243, Reason: Crashed
Monitor duration	103.73s
Return Code	1114
PID	3108
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	43
-	1
-	82
Window	1

Process #30: explorer.exe

ID	30
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\Explorer.EXE
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 197904, Reason: Child Process
Unmonitor End Time	End Time: 310883, Reason: Terminated
Monitor duration	112.98s
Return Code	259
PID	3976
Parent PID	1600
Bitness	64 Bit

Process #31: tasyggycx.exe

ID	31
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 200307, Reason: Child Process
Unmonitor End Time	End Time: 250241, Reason: Terminated
Monitor duration	49.93s
Return Code	0
PID	4824
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #32: tasyggycx.exe

ID	32
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 204024, Reason: Child Process
Unmonitor End Time	End Time: 255548, Reason: Terminated
Monitor duration	51.52s
Return Code	0
PID	2544
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #33: tasyggycx.exe

ID	33
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 215913, Reason: Child Process
Unmonitor End Time	End Time: 262284, Reason: Terminated
Monitor duration	46.37s
Return Code	0
PID	3348
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #34: tasyggycx.exe

ID	34
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 220721, Reason: Child Process
Unmonitor End Time	End Time: 262773, Reason: Terminated
Monitor duration	42.05s
Return Code	0
PID	900
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #35: tasyggycx.exe

ID	35
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 223958, Reason: Child Process
Unmonitor End Time	End Time: 264275, Reason: Terminated
Monitor duration	40.32s
Return Code	0
PID	4116
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #36: tasyggycx.exe

ID	36
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 230357, Reason: Child Process
Unmonitor End Time	End Time: 267346, Reason: Terminated
Monitor duration	36.99s
Return Code	0
PID	4192
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #37: tasyggycx.exe

ID	37
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 233576, Reason: Child Process
Unmonitor End Time	End Time: 269079, Reason: Terminated
Monitor duration	35.50s
Return Code	0
PID	4276
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #38: tasyggycx.exe

ID	38
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237702, Reason: Child Process
Unmonitor End Time	End Time: 313095, Reason: Crashed
Monitor duration	75.39s
Return Code	1114
PID	4324
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	43
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	43
-	1
-	82
Window	1

Process #39: tasyggycx.exe

ID	39
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 242201, Reason: Child Process
Unmonitor End Time	End Time: 277345, Reason: Terminated
Monitor duration	35.14s
Return Code	0
PID	4376
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #40: tasyggycx.exe

ID	40
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 245547, Reason: Child Process
Unmonitor End Time	End Time: 269590, Reason: Terminated
Monitor duration	24.04s
Return Code	259
PID	4428
Parent PID	4784
Bitness	64 Bit

Process #41: werfault.exe

ID	41
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4784 -s 628
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 245706, Reason: Child Process
Unmonitor End Time	End Time: 268752, Reason: Terminated
Monitor duration	23.05s
Return Code	0
PID	4440
Parent PID	4784
Bitness	64 Bit

Process #42: tasyggycx.exe

ID	42
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 247061, Reason: Child Process
Unmonitor End Time	End Time: 264917, Reason: Terminated
Monitor duration	17.86s
Return Code	0
PID	4496
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #43: tasyggycx.exe

ID	43
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 251252, Reason: Child Process
Unmonitor End Time	End Time: 283639, Reason: Terminated
Monitor duration	32.39s
Return Code	0
PID	2064
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #44: tasyggycx.exe

ID	44
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoByHandle /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 255756, Reason: Child Process
Unmonitor End Time	End Time: 290734, Reason: Terminated
Monitor duration	34.98s
Return Code	0
PID	4108
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #45: tasyggycx.exe

ID	45
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 259621, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Crashed
Monitor duration	55.72s
Return Code	Unknown
PID	1920
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	8
Environment	2
Registry	786
Mutex	6
Process	2
-	43
-	1
-	82

Process #46: tasyggycx.exe

ID	46
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 264252, Reason: Child Process
Unmonitor End Time	End Time: 299181, Reason: Terminated
Monitor duration	34.93s
Return Code	0
PID	4964
Parent PID	3288
Bitness	64 Bit

Host Behavior

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

Process #47: tasyggycx.exe

ID	47
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 267870, Reason: Child Process
Unmonitor End Time	End Time: 299185, Reason: Terminated
Monitor duration	31.32s
Return Code	0
PID	2616
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	591
Mutex	7

Process #48: tasyggycx.exe

ID	48
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 269950, Reason: Child Process
Unmonitor End Time	End Time: 299914, Reason: Terminated
Monitor duration	29.96s
Return Code	0
PID	3660
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #49: tasyggycx.exe

ID	49
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 270636, Reason: Child Process
Unmonitor End Time	End Time: 296089, Reason: Terminated
Monitor duration	25.45s
Return Code	259
PID	2936
Parent PID	3108
Bitness	64 Bit

Process #50: werfault.exe

ID	50
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 3108 -s 628
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 270761, Reason: Child Process
Unmonitor End Time	End Time: 295406, Reason: Terminated
Monitor duration	24.64s
Return Code	0
PID	1424
Parent PID	3108
Bitness	64 Bit

Process #51: tasyggycx.exe

ID	51
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 272699, Reason: Child Process
Unmonitor End Time	End Time: 302874, Reason: Terminated
Monitor duration	30.18s
Return Code	0
PID	3136
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	753
Mutex	7

Process #52: tasyggycx.exe

ID	52
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 274880, Reason: Child Process
Unmonitor End Time	End Time: 304419, Reason: Terminated
Monitor duration	29.54s
Return Code	0
PID	1752
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	621
Mutex	7

Process #53: tasyggycx.exe

ID	53
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 277524, Reason: Child Process
Unmonitor End Time	End Time: 304893, Reason: Terminated
Monitor duration	27.37s
Return Code	0
PID	2040
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #54: tasyggycx.exe

ID	54
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 279857, Reason: Child Process
Unmonitor End Time	End Time: 305731, Reason: Terminated
Monitor duration	25.87s
Return Code	0
PID	1708
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #55: tasyggycx.exe

ID	55
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 286245, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	29.09s
Return Code	Unknown
PID	1364
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	38
File	118
System	7
Environment	2
Registry	774
Mutex	5
Process	2
-	2
-	1

Process #56: tasyggycx.exe

ID	56
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 292439, Reason: Child Process
Unmonitor End Time	End Time: 308296, Reason: Terminated
Monitor duration	15.86s
Return Code	259
PID	484
Parent PID	4324
Bitness	64 Bit

Process #57: tasyggycx.exe

ID	57
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 292758, Reason: Child Process
Unmonitor End Time	End Time: 311483, Reason: Terminated
Monitor duration	18.73s
Return Code	0
PID	2852
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #58: werfault.exe

ID	58
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 4324 -s 632
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 292780, Reason: Child Process
Unmonitor End Time	End Time: 308267, Reason: Terminated
Monitor duration	15.49s
Return Code	0
PID	1288
Parent PID	4324
Bitness	64 Bit

Process #59: tasyggycx.exe

ID	59
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 296120, Reason: Child Process
Unmonitor End Time	End Time: 313349, Reason: Terminated
Monitor duration	17.23s
Return Code	0
PID	4836
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	6
Environment	2
Registry	766
Mutex	7

Process #60: tasyggycx.exe

ID	60
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 301677, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	13.66s
Return Code	Unknown
PID	4888
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	28
File	117
System	2
Environment	2
Registry	366
Mutex	3

Process #61: tasyggycx.exe

ID	61
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 305054, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	10.29s
Return Code	Unknown
PID	4772
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #62: werfault.exe

ID	62
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 1920 -s 632
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 305855, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	9.48s
Return Code	Unknown
PID	4960
Parent PID	1920
Bitness	64 Bit

Process #63: tasyggycx.exe

ID	63
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 306457, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	8.88s
Return Code	Unknown
PID	1952
Parent PID	1920
Bitness	64 Bit

Process #64: tasyggycx.exe

ID	64
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 307250, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	8.09s
Return Code	Unknown
PID	2832
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #65: explorer.exe

ID	65
File Name	c:\windows\explorer.exe
Command Line	"C:\Windows\Explorer.EXE" /LOADSAVEDWINDOWS
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 308769, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	6.57s
Return Code	Unknown
PID	5072
Parent PID	4664
Bitness	64 Bit

Process #66: tasyggycx.exe

ID	66
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 309302, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	6.04s
Return Code	Unknown
PID	5076
Parent PID	3288
Bitness	64 Bit

Host Behavior

Type	Count
Module	26
File	112
Environment	1

Process #67: tasyggycx.exe

ID	67
File Name	c:\users\rdhj0cnfevzx\desktop\tasyggycx.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoA /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 314066, Reason: Child Process
Unmonitor End Time	End Time: 315340, Reason: Terminated by Timeout
Monitor duration	1.27s
Return Code	Unknown
PID	1996
Parent PID	3288
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8	C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll, C:\Users\RDhJ0CNFevzX\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll	Sample File	1220.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpo74kwsx1	Accessed File	Access, Read	CLEAN
C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll	Accessed File	Access, Read	CLEAN
System Paging File	Accessed File	Access	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{0aa26147-58aa-e888-6782-4bac88c336bd}	access	tasyggycx.exe	CLEAN
{54137ce8-d76d-e7fc-dec3-c85f290e5b98}	access	tasyggycx.exe	CLEAN

Registry

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

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

Process

Process Name	Commandline	Verdict
explorer.exe	C:\Windows\Explorer.EXE	SUSPICIOUS
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpo74kwsx1" /s	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoA	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoByHandle	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExA	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExW	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeA	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExA	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExW	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeW	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoW	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileA	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileW	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileA	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileW	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameA	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameW	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1600 -s 4424	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueA	CLEAN

Process Name	Commandline	Verdict
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueW	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoA /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoByHandle /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExA /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExW /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeA /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExA /fn_args="0"	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1948 -s 628	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExW /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeW /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoW /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileA /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileW /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileA /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileW /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameA /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameW /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueA /fn_args="0"	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4784 -s 628	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueW /fn_args="0"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoA /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoByHandle /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExA /fn_args="1"	CLEAN

Process Name	Commandline	Verdict
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoExW /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeA /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExA /fn_args="1"	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 3108 -s 628	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeExW /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoSizeW /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoW /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileA /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerFindFileW /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileA /fn_args="1"	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 4324 -s 632	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerInstallFileW /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameA /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerLanguageNameW /fn_args="1"	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 1920 -s 632	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueA /fn_args="1"	CLEAN
explorer.exe	"C:\Windows\Explorer.EXE" /LOADSAVEDWINDOWS	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=VerQueryValueW /fn_args="1"	CLEAN
tasyggycx.exe	"C:\Users\RDhJ0CNFevzX\Desktop\TaSygGYCX.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll" /fn_id=GetFileVersionInfoA /fn_args="Install"	CLEAN

YARA / AV

Antivirus (6)

File Type	Threat Name	File Name	Verdict
Sample File	Trojan.GenericKDZ.76753	C:\Users\RDhJ0CNFevzX\Desktop\8bcde178298b0263ce7cb8e4c6a5ef4d0fcea9729a21e2cef4eaec3f2ad27bc8.exe.dll	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

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