MALICIOUS

Classifications: Downloader

Threat Names: C2/Generic-A IcedID

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll**
ID	#5129040
MD5	363777daf36e9534762d30bd4bf22c74
SHA1	ea94d9afd355dd23a069f21b3562d85a4266da4f
SHA256	8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6
File Size	352.00 KB
Report Created	2022-08-12 03:24 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (5 rules, 14 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	IcedID configuration was extracted	1	Downloader
	• A configuration for IcedID was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	2	Downloader
	• Rule "IcedID_Loader" from ruleset "Malware" has matched on a memory dump for (process #121) rzvaqzgqak.exe. • Rule "IcedID_Loader" from ruleset "Malware" has matched on a memory dump for (process #106) rzvaqzgqak.exe.			
4/5	Reputation	Contacts known malicious URL	1	-
	• Reputation analysis labels the URL "http://alexbionka.com/" which was contacted by (process #76) rzvaqzgqak.exe as C2/Generic-A.			
4/5	Reputation	Resolves known malicious domain	1	-
	• Reputation analysis labels the resolved domain "alexbionka.com" as C2/Generic-A.			
1/5	Obfuscation	Resolves API functions dynamically	9	-
	• (Process #16) rzvaqzgqak.exe resolves 52 API functions by name. • (Process #31) rzvaqzgqak.exe resolves 52 API functions by name. • (Process #46) rzvaqzgqak.exe resolves 52 API functions by name. • (Process #61) rzvaqzgqak.exe resolves 52 API functions by name. • (Process #76) rzvaqzgqak.exe resolves 52 API functions by name. • (Process #91) rzvaqzgqak.exe resolves 52 API functions by name. • (Process #106) rzvaqzgqak.exe resolves 52 API functions by name. • (Process #121) rzvaqzgqak.exe resolves 52 API functions by name. • (Process #136) rzvaqzgqak.exe resolves 52 API functions by name.			

Malware Configuration: IcedID

Metadata	Key	Extracted Value
URL	Url	alexbionka.com

Mitre ATT&CK Matrix

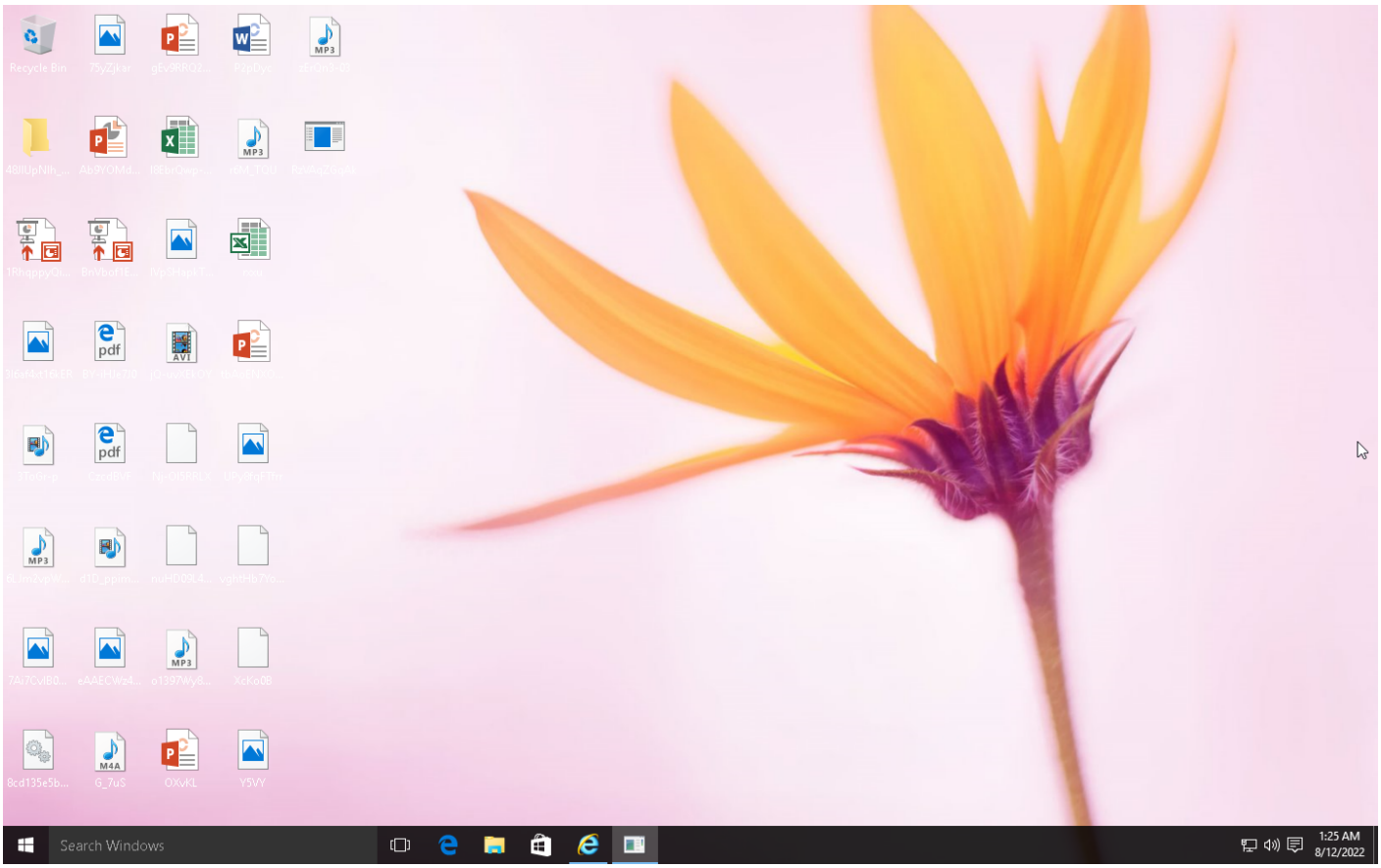
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1045 Software Packing							

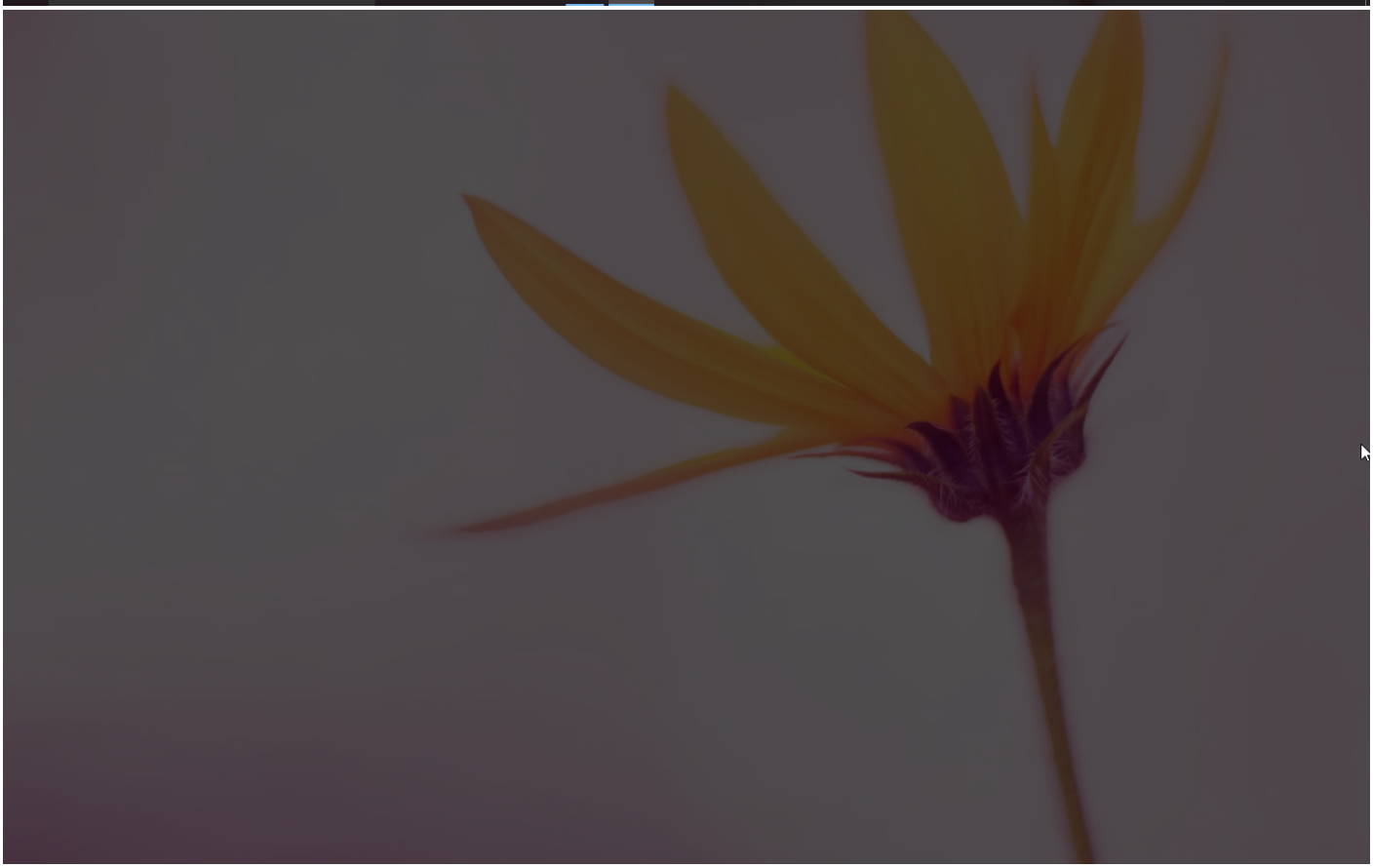
Sample Information

ID	#5129040
MD5	363777daf36e9534762d30bd4bf22c74
SHA1	ea94d9afd355dd23a069f21b3562d85a4266da4f
SHA256	8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6
SSDeep	6144:RYCYa6MfAcSIE+S0fzAMJfWpKd5WhAI7CJDZ/PeHbUhHTmGPqG7s6FmlEHKiTd:SCwMfjSIE+A4eguRJDtPZIG46FkEH9
File Name	8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll
File Size	352.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✔

Analysis Information

Creation Time	2022-08-12 03:24 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	136
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	0
YARA Enabled	✔
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	2


Search Windows
1:25 AM
8/12/2022



NETWORK

General

4.38 KB total sent

5.19 KB total received

2 ports 80, 53

2 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

9 sessions, 4.32 KB sent, 5.12 KB received

HTTP Requests

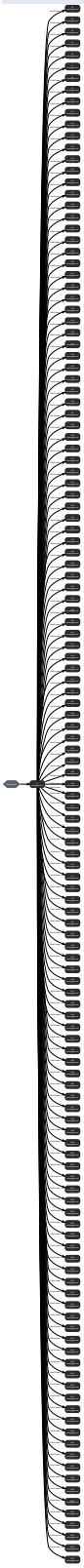
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://alexbionka.com	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	alexbionka.com	NO_ERROR	64.227.108.27		NA

BEHAVIOR

Process Graph



Process #1: rzvaqzgqak.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpmt4chc1t" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 68588, Reason: Analysis Target
Unmonitor End Time	End Time: 293022, Reason: Terminated
Monitor duration	224.43s
Return Code	0
PID	1640
Parent PID	1972
Bitness	64 Bit

Host Behavior

Type	Count
Module	19
File	8
Environment	1
Process	135

Process #2: rzvaqzgqak.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 92871, Reason: Child Process
Unmonitor End Time	End Time: 158077, Reason: Terminated
Monitor duration	65.21s
Return Code	0
PID	3320
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #3: rzvaqzgqak.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 94221, Reason: Child Process
Unmonitor End Time	End Time: 159082, Reason: Terminated
Monitor duration	64.86s
Return Code	0
PID	3244
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #4: rzvaqzgqak.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 94849, Reason: Child Process
Unmonitor End Time	End Time: 161523, Reason: Terminated
Monitor duration	66.67s
Return Code	0
PID	3216
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #5: rzvaqzgqak.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 95573, Reason: Child Process
Unmonitor End Time	End Time: 161680, Reason: Terminated
Monitor duration	66.11s
Return Code	0
PID	3132
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #6: rzvaqzgqak.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 96397, Reason: Child Process
Unmonitor End Time	End Time: 163094, Reason: Terminated
Monitor duration	66.70s
Return Code	0
PID	3108
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #7: rzvaqzgqak.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 96838, Reason: Child Process
Unmonitor End Time	End Time: 163898, Reason: Terminated
Monitor duration	67.06s
Return Code	0
PID	2940
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #8: rzvaqzgqak.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 97326, Reason: Child Process
Unmonitor End Time	End Time: 164725, Reason: Terminated
Monitor duration	67.40s
Return Code	0
PID	3000
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #9: rzvaqzgqak.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 98043, Reason: Child Process
Unmonitor End Time	End Time: 164484, Reason: Terminated
Monitor duration	66.44s
Return Code	0
PID	2800
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #10: rzvaqzgqak.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 98856, Reason: Child Process
Unmonitor End Time	End Time: 166210, Reason: Terminated
Monitor duration	67.35s
Return Code	0
PID	936
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #11: rzvaqzgqak.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 99906, Reason: Child Process
Unmonitor End Time	End Time: 168394, Reason: Terminated
Monitor duration	68.49s
Return Code	0
PID	4048
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #12: rzvaqzgqak.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100425, Reason: Child Process
Unmonitor End Time	End Time: 167769, Reason: Terminated
Monitor duration	67.34s
Return Code	0
PID	1148
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #13: rzvaqzgqak.exe

ID	13
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 100938, Reason: Child Process
Unmonitor End Time	End Time: 168566, Reason: Terminated
Monitor duration	67.63s
Return Code	0
PID	4480
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #14: rzvaqzgqak.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 101997, Reason: Child Process
Unmonitor End Time	End Time: 135621, Reason: Terminated
Monitor duration	33.62s
Return Code	0
PID	4476
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #15: rzvaqzgqak.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 102609, Reason: Child Process
Unmonitor End Time	End Time: 169503, Reason: Terminated
Monitor duration	66.89s
Return Code	0
PID	768
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #16: rzvaqzgqak.exe

ID	16
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 102983, Reason: Child Process
Unmonitor End Time	End Time: 144228, Reason: Terminated
Monitor duration	41.24s
Return Code	0
PID	4376
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	25
User	1

Network Behavior

Type	Count
HTTP	1

Process #17: rzvaqzgqak.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 103467, Reason: Child Process
Unmonitor End Time	End Time: 170254, Reason: Terminated
Monitor duration	66.79s
Return Code	0
PID	4352
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #18: rzvaqzgqak.exe

ID	18
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 104269, Reason: Child Process
Unmonitor End Time	End Time: 173795, Reason: Terminated
Monitor duration	69.53s
Return Code	0
PID	4512
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #19: rzvaqzgqak.exe

ID	19
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 105211, Reason: Child Process
Unmonitor End Time	End Time: 174357, Reason: Terminated
Monitor duration	69.15s
Return Code	0
PID	4524
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #20: rzvaqzgqak.exe

ID	20
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 106443, Reason: Child Process
Unmonitor End Time	End Time: 177715, Reason: Terminated
Monitor duration	71.27s
Return Code	0
PID	4556
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #21: rzvaqzgqak.exe

ID	21
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 108224, Reason: Child Process
Unmonitor End Time	End Time: 181611, Reason: Terminated
Monitor duration	73.39s
Return Code	0
PID	4572
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #22: rzvaqzgqak.exe

ID	22
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 109005, Reason: Child Process
Unmonitor End Time	End Time: 181610, Reason: Terminated
Monitor duration	72.61s
Return Code	0
PID	4596
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #23: rzvaqzgqak.exe

ID	23
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 110423, Reason: Child Process
Unmonitor End Time	End Time: 184175, Reason: Terminated
Monitor duration	73.75s
Return Code	0
PID	760
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #24: rzvaqzgqak.exe

ID	24
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 111562, Reason: Child Process
Unmonitor End Time	End Time: 185134, Reason: Terminated
Monitor duration	73.57s
Return Code	0
PID	4752
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #25: rzvaqzgqak.exe

ID	25
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 112307, Reason: Child Process
Unmonitor End Time	End Time: 187388, Reason: Terminated
Monitor duration	75.08s
Return Code	0
PID	4696
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #26: rzvaqzgqak.exe

ID	26
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 113435, Reason: Child Process
Unmonitor End Time	End Time: 185312, Reason: Terminated
Monitor duration	71.88s
Return Code	0
PID	4788
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #27: rzvaqzgqak.exe

ID	27
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 114572, Reason: Child Process
Unmonitor End Time	End Time: 187388, Reason: Terminated
Monitor duration	72.82s
Return Code	0
PID	4448
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #28: rzvaqzgqak.exe

ID	28
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 115809, Reason: Child Process
Unmonitor End Time	End Time: 187419, Reason: Terminated
Monitor duration	71.61s
Return Code	0
PID	4832
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #29: rzvaqzgqak.exe

ID	29
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 116619, Reason: Child Process
Unmonitor End Time	End Time: 189883, Reason: Terminated
Monitor duration	73.26s
Return Code	0
PID	4304
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #30: rzvaqzgqak.exe

ID	30
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 116796, Reason: Child Process
Unmonitor End Time	End Time: 191504, Reason: Terminated
Monitor duration	74.71s
Return Code	0
PID	1316
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #31: rzvaqzgqak.exe

ID	31
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="0"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117209, Reason: Child Process
Unmonitor End Time	End Time: 161522, Reason: Terminated
Monitor duration	44.31s
Return Code	0
PID	900
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	24
User	1

Network Behavior

Type	Count
HTTP	1

Process #32: rzvaqzgqak.exe

ID	32
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117452, Reason: Child Process
Unmonitor End Time	End Time: 192188, Reason: Terminated
Monitor duration	74.74s
Return Code	0
PID	2876
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #33: rzvaqzgqak.exe

ID	33
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 117781, Reason: Child Process
Unmonitor End Time	End Time: 192110, Reason: Terminated
Monitor duration	74.33s
Return Code	0
PID	2912
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #34: rzvaqzgqak.exe

ID	34
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 118190, Reason: Child Process
Unmonitor End Time	End Time: 189269, Reason: Terminated
Monitor duration	71.08s
Return Code	0
PID	1472
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #35: rzvaqzgqak.exe

ID	35
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 119786, Reason: Child Process
Unmonitor End Time	End Time: 191504, Reason: Terminated
Monitor duration	71.72s
Return Code	0
PID	1428
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #36: rzvaqzgqak.exe

ID	36
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 121861, Reason: Child Process
Unmonitor End Time	End Time: 191965, Reason: Terminated
Monitor duration	70.10s
Return Code	0
PID	3076
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #37: rzvaqzgqak.exe

ID	37
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 124536, Reason: Child Process
Unmonitor End Time	End Time: 193158, Reason: Terminated
Monitor duration	68.62s
Return Code	0
PID	3096
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #38: rzvaqzgqak.exe

ID	38
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 126516, Reason: Child Process
Unmonitor End Time	End Time: 195002, Reason: Terminated
Monitor duration	68.49s
Return Code	0
PID	3168
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #39: rzvaqzgqak.exe

ID	39
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 127556, Reason: Child Process
Unmonitor End Time	End Time: 165116, Reason: Terminated
Monitor duration	37.56s
Return Code	0
PID	3184
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #40: rzvaqzgqak.exe

ID	40
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 128560, Reason: Child Process
Unmonitor End Time	End Time: 196375, Reason: Terminated
Monitor duration	67.81s
Return Code	0
PID	3200
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #41: rzvaqzgqak.exe

ID	41
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 129034, Reason: Child Process
Unmonitor End Time	End Time: 197116, Reason: Terminated
Monitor duration	68.08s
Return Code	0
PID	3268
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #42: rzvaqzgqak.exe

ID	42
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 129194, Reason: Child Process
Unmonitor End Time	End Time: 196436, Reason: Terminated
Monitor duration	67.24s
Return Code	0
PID	3284
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #43: rzvaqzgqak.exe

ID	43
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 130158, Reason: Child Process
Unmonitor End Time	End Time: 198549, Reason: Terminated
Monitor duration	68.39s
Return Code	0
PID	3300
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #44: rzvaqzgqak.exe

ID	44
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 133220, Reason: Child Process
Unmonitor End Time	End Time: 202390, Reason: Terminated
Monitor duration	69.17s
Return Code	0
PID	3372
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #45: rzvaqzgqak.exe

ID	45
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 134901, Reason: Child Process
Unmonitor End Time	End Time: 174311, Reason: Terminated
Monitor duration	39.41s
Return Code	0
PID	1780
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #46: rzvaqzgqak.exe

ID	46
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 136122, Reason: Child Process
Unmonitor End Time	End Time: 204108, Reason: Terminated
Monitor duration	67.99s
Return Code	0
PID	4884
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	42
User	1

Network Behavior

Type	Count
HTTP	1

Process #47: rzvaqzgqak.exe

ID	47
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 137139, Reason: Child Process
Unmonitor End Time	End Time: 183219, Reason: Terminated
Monitor duration	46.08s
Return Code	0
PID	2952
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #48: rzvaqzgqak.exe

ID	48
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 140899, Reason: Child Process
Unmonitor End Time	End Time: 184097, Reason: Terminated
Monitor duration	43.20s
Return Code	0
PID	4864
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #49: rzvaqzgqak.exe

ID	49
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 142647, Reason: Child Process
Unmonitor End Time	End Time: 186904, Reason: Terminated
Monitor duration	44.26s
Return Code	0
PID	4904
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #50: rzvaqzgqak.exe

ID	50
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 144159, Reason: Child Process
Unmonitor End Time	End Time: 186902, Reason: Terminated
Monitor duration	42.74s
Return Code	0
PID	4912
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #51: rzvaqzgqak.exe

ID	51
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 144911, Reason: Child Process
Unmonitor End Time	End Time: 187419, Reason: Terminated
Monitor duration	42.51s
Return Code	0
PID	4952
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #52: rzvaqzgqak.exe

ID	52
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 146317, Reason: Child Process
Unmonitor End Time	End Time: 186916, Reason: Terminated
Monitor duration	40.60s
Return Code	0
PID	4052
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #53: rzvaqzgqak.exe

ID	53
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 147225, Reason: Child Process
Unmonitor End Time	End Time: 217266, Reason: Terminated
Monitor duration	70.04s
Return Code	0
PID	4140
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #54: rzvaqzgqak.exe

ID	54
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 148287, Reason: Child Process
Unmonitor End Time	End Time: 188990, Reason: Terminated
Monitor duration	40.70s
Return Code	0
PID	4180
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #55: rzvaqzgqak.exe

ID	55
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 149020, Reason: Child Process
Unmonitor End Time	End Time: 218645, Reason: Terminated
Monitor duration	69.62s
Return Code	0
PID	4860
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #56: rzvaqzgqak.exe

ID	56
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 150187, Reason: Child Process
Unmonitor End Time	End Time: 220332, Reason: Terminated
Monitor duration	70.14s
Return Code	0
PID	4688
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #57: rzvaqzgqak.exe

ID	57
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 151294, Reason: Child Process
Unmonitor End Time	End Time: 192643, Reason: Terminated
Monitor duration	41.35s
Return Code	0
PID	4680
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #58: rzvaqzgqak.exe

ID	58
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 152607, Reason: Child Process
Unmonitor End Time	End Time: 222299, Reason: Terminated
Monitor duration	69.69s
Return Code	0
PID	4872
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #59: rzvaqzgqak.exe

ID	59
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 154014, Reason: Child Process
Unmonitor End Time	End Time: 223778, Reason: Terminated
Monitor duration	69.76s
Return Code	0
PID	2588
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #60: rzvaqzgqak.exe

ID	60
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 155492, Reason: Child Process
Unmonitor End Time	End Time: 223631, Reason: Terminated
Monitor duration	68.14s
Return Code	0
PID	2720
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #61: rzvaqzgqak.exe

ID	61
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="Install"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 158079, Reason: Child Process
Unmonitor End Time	End Time: 242135, Reason: Terminated
Monitor duration	84.06s
Return Code	0
PID	5060
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	28
User	1

Network Behavior

Type	Count
HTTP	1

Process #62: rzvaqzgqak.exe

ID	62
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 163096, Reason: Child Process
Unmonitor End Time	End Time: 227502, Reason: Terminated
Monitor duration	64.41s
Return Code	0
PID	5104
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #63: rzvaqzgqak.exe

ID	63
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 164470, Reason: Child Process
Unmonitor End Time	End Time: 230926, Reason: Terminated
Monitor duration	66.46s
Return Code	0
PID	5084
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #64: rzvaqzgqak.exe

ID	64
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 164966, Reason: Child Process
Unmonitor End Time	End Time: 231691, Reason: Terminated
Monitor duration	66.72s
Return Code	0
PID	4876
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #65: rzvaqzgqak.exe

ID	65
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 165825, Reason: Child Process
Unmonitor End Time	End Time: 234129, Reason: Terminated
Monitor duration	68.30s
Return Code	0
PID	4460
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #66: rzvaqzgqak.exe

ID	66
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 166357, Reason: Child Process
Unmonitor End Time	End Time: 234615, Reason: Terminated
Monitor duration	68.26s
Return Code	0
PID	2576
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #67: rzvaqzgqak.exe

ID	67
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 166967, Reason: Child Process
Unmonitor End Time	End Time: 235160, Reason: Terminated
Monitor duration	68.19s
Return Code	0
PID	3396
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #68: rzvaqzgqak.exe

ID	68
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 167674, Reason: Child Process
Unmonitor End Time	End Time: 236513, Reason: Terminated
Monitor duration	68.84s
Return Code	0
PID	3464
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #69: rzvaqzgqak.exe

ID	69
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 169194, Reason: Child Process
Unmonitor End Time	End Time: 236527, Reason: Terminated
Monitor duration	67.33s
Return Code	0
PID	3488
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #70: rzvaqzgqak.exe

ID	70
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 169902, Reason: Child Process
Unmonitor End Time	End Time: 238298, Reason: Terminated
Monitor duration	68.40s
Return Code	0
PID	3576
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #71: rzvaqzgqak.exe

ID	71
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 181844, Reason: Child Process
Unmonitor End Time	End Time: 246943, Reason: Terminated
Monitor duration	65.10s
Return Code	0
PID	3636
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #72: rzvaqzgqak.exe

ID	72
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 185313, Reason: Child Process
Unmonitor End Time	End Time: 249454, Reason: Terminated
Monitor duration	64.14s
Return Code	0
PID	3668
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #73: rzvaqzgqak.exe

ID	73
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 185964, Reason: Child Process
Unmonitor End Time	End Time: 251568, Reason: Terminated
Monitor duration	65.60s
Return Code	0
PID	3900
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #74: rzvaqzgqak.exe

ID	74
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186904, Reason: Child Process
Unmonitor End Time	End Time: 252203, Reason: Terminated
Monitor duration	65.30s
Return Code	0
PID	3920
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #75: rzvaqzgqak.exe

ID	75
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 188991, Reason: Child Process
Unmonitor End Time	End Time: 254208, Reason: Terminated
Monitor duration	65.22s
Return Code	0
PID	3952
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #76: rzvaqzgqak.exe

ID	76
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 190755, Reason: Child Process
Unmonitor End Time	End Time: 247706, Reason: Terminated
Monitor duration	56.95s
Return Code	0
PID	3992
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	20
User	1

Network Behavior

Type	Count
HTTP	1

Process #77: rzvaqzgqak.exe

ID	77
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 192112, Reason: Child Process
Unmonitor End Time	End Time: 259778, Reason: Terminated
Monitor duration	67.67s
Return Code	0
PID	4004
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #78: rzvaqzgqak.exe

ID	78
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 193744, Reason: Child Process
Unmonitor End Time	End Time: 268050, Reason: Terminated
Monitor duration	74.31s
Return Code	0
PID	4024
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #79: rzvaqzgqak.exe

ID	79
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 194356, Reason: Child Process
Unmonitor End Time	End Time: 267988, Reason: Terminated
Monitor duration	73.63s
Return Code	0
PID	1052
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #80: rzvaqzgqak.exe

ID	80
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 195497, Reason: Child Process
Unmonitor End Time	End Time: 268956, Reason: Terminated
Monitor duration	73.46s
Return Code	0
PID	2816
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #81: rzvaqzgqak.exe

ID	81
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 196377, Reason: Child Process
Unmonitor End Time	End Time: 270910, Reason: Terminated
Monitor duration	74.53s
Return Code	0
PID	4128
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #82: rzvaqzgqak.exe

ID	82
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 198027, Reason: Child Process
Unmonitor End Time	End Time: 271474, Reason: Terminated
Monitor duration	73.45s
Return Code	0
PID	1452
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #83: rzvaqzgqak.exe

ID	83
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 199984, Reason: Child Process
Unmonitor End Time	End Time: 271474, Reason: Terminated
Monitor duration	71.49s
Return Code	0
PID	4308
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #84: rzvaqzgqak.exe

ID	84
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 203056, Reason: Child Process
Unmonitor End Time	End Time: 271936, Reason: Terminated
Monitor duration	68.88s
Return Code	0
PID	4320
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #85: rzvaqzgqak.exe

ID	85
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 205832, Reason: Child Process
Unmonitor End Time	End Time: 278379, Reason: Terminated
Monitor duration	72.55s
Return Code	0
PID	3332
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #86: rzvaqzgqak.exe

ID	86
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 206266, Reason: Child Process
Unmonitor End Time	End Time: 277934, Reason: Terminated
Monitor duration	71.67s
Return Code	0
PID	5020
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #87: rzvaqzgqak.exe

ID	87
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 206561, Reason: Child Process
Unmonitor End Time	End Time: 278379, Reason: Terminated
Monitor duration	71.82s
Return Code	0
PID	3340
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #88: rzvaqzgqak.exe

ID	88
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 206890, Reason: Child Process
Unmonitor End Time	End Time: 279753, Reason: Terminated
Monitor duration	72.86s
Return Code	0
PID	2972
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #89: rzvaqzgqak.exe

ID	89
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 207311, Reason: Child Process
Unmonitor End Time	End Time: 281226, Reason: Terminated
Monitor duration	73.92s
Return Code	0
PID	2760
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #90: rzvaqzgqak.exe

ID	90
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 207717, Reason: Child Process
Unmonitor End Time	End Time: 280707, Reason: Terminated
Monitor duration	72.99s
Return Code	0
PID	4340
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #91: rzvaqzgqak.exe

ID	91
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 208338, Reason: Child Process
Unmonitor End Time	End Time: 255084, Reason: Terminated
Monitor duration	46.75s
Return Code	0
PID	4580
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	22
User	1

Network Behavior

Type	Count
HTTP	1

Process #92: rzvaqzgqak.exe

ID	92
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 208909, Reason: Child Process
Unmonitor End Time	End Time: 281458, Reason: Terminated
Monitor duration	72.55s
Return Code	0
PID	4792
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #93: rzvaqzgqak.exe

ID	93
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 210671, Reason: Child Process
Unmonitor End Time	End Time: 284148, Reason: Terminated
Monitor duration	73.48s
Return Code	0
PID	2920
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #94: rzvaqzgqak.exe

ID	94
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 212133, Reason: Child Process
Unmonitor End Time	End Time: 284148, Reason: Terminated
Monitor duration	72.02s
Return Code	0
PID	1116
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #95: rzvaqzgqak.exe

ID	95
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 212944, Reason: Child Process
Unmonitor End Time	End Time: 284645, Reason: Terminated
Monitor duration	71.70s
Return Code	0
PID	1480
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #96: rzvaqzgqak.exe

ID	96
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 215041, Reason: Child Process
Unmonitor End Time	End Time: 284148, Reason: Terminated
Monitor duration	69.11s
Return Code	0
PID	3092
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #97: rzvaqzgqak.exe

ID	97
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 220283, Reason: Child Process
Unmonitor End Time	End Time: 285476, Reason: Terminated
Monitor duration	65.19s
Return Code	0
PID	3084
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #98: rzvaqzgqak.exe

ID	98
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 223290, Reason: Child Process
Unmonitor End Time	End Time: 287454, Reason: Terminated
Monitor duration	64.16s
Return Code	0
PID	3276
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #99: rzvaqzgqak.exe

ID	99
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 225075, Reason: Child Process
Unmonitor End Time	End Time: 289424, Reason: Terminated
Monitor duration	64.35s
Return Code	0
PID	3308
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #100: rzvaqzgqak.exe

ID	100
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 227028, Reason: Child Process
Unmonitor End Time	End Time: 291272, Reason: Terminated
Monitor duration	64.24s
Return Code	0
PID	3492
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #101: rzvaqzgqak.exe

ID	101
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 231036, Reason: Child Process
Unmonitor End Time	End Time: 296021, Reason: Terminated
Monitor duration	64.98s
Return Code	0
PID	2172
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #102: rzvaqzgqak.exe

ID	102
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 235439, Reason: Child Process
Unmonitor End Time	End Time: 297929, Reason: Terminated
Monitor duration	62.49s
Return Code	0
PID	4616
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #103: rzvaqzgqak.exe

ID	103
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 237871, Reason: Child Process
Unmonitor End Time	End Time: 278378, Reason: Terminated
Monitor duration	40.51s
Return Code	0
PID	4948
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #104: rzvaqzgqak.exe

ID	104
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 239385, Reason: Child Process
Unmonitor End Time	End Time: 279144, Reason: Terminated
Monitor duration	39.76s
Return Code	0
PID	2712
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #105: rzvaqzgqak.exe

ID	105
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 240336, Reason: Child Process
Unmonitor End Time	End Time: 302473, Reason: Terminated
Monitor duration	62.14s
Return Code	0
PID	2472
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #106: rzvaqzgqak.exe

ID	106
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="explorer.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 241390, Reason: Child Process
Unmonitor End Time	End Time: 297423, Reason: Terminated
Monitor duration	56.03s
Return Code	0
PID	5000
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	24
User	1

Network Behavior

Type	Count
HTTP	1

Process #107: rzvaqzgqak.exe

ID	107
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 242136, Reason: Child Process
Unmonitor End Time	End Time: 303721, Reason: Terminated
Monitor duration	61.59s
Return Code	0
PID	3208
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #108: rzvaqzgqak.exe

ID	108
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 242619, Reason: Child Process
Unmonitor End Time	End Time: 282082, Reason: Terminated
Monitor duration	39.46s
Return Code	0
PID	3120
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #109: rzvaqzgqak.exe

ID	109
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 243697, Reason: Child Process
Unmonitor End Time	End Time: 304710, Reason: Terminated
Monitor duration	61.01s
Return Code	0
PID	924
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #110: rzvaqzgqak.exe

ID	110
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 245183, Reason: Child Process
Unmonitor End Time	End Time: 283852, Reason: Terminated
Monitor duration	38.67s
Return Code	0
PID	5072
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #111: rzvaqzgqak.exe

ID	111
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 246632, Reason: Child Process
Unmonitor End Time	End Time: 284148, Reason: Terminated
Monitor duration	37.52s
Return Code	0
PID	3216
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	22
File	3
Environment	1

Process #112: rzvaqzgqak.exe

ID	112
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 248153, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	61.00s
Return Code	Unknown
PID	2580
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	23
File	3
Environment	1

Process #113: rzvaqzgqak.exe

ID	113
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 249668, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	59.49s
Return Code	Unknown
PID	3244
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #114: rzvaqzgqak.exe

ID	114
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 251787, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	57.37s
Return Code	Unknown
PID	5052
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	17
File	3
Environment	1

Process #115: rzvaqzgqak.exe

ID	115
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 252624, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	56.53s
Return Code	Unknown
PID	1460
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #116: rzvaqzgqak.exe

ID	116
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 252911, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	56.24s
Return Code	Unknown
PID	5068
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #117: rzvaqzgqak.exe

ID	117
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 253185, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	55.97s
Return Code	Unknown
PID	1268
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #118: rzvaqzgqak.exe

ID	118
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 253708, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	55.45s
Return Code	Unknown
PID	2732
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #119: rzvaqzgqak.exe

ID	119
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 254349, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	54.81s
Return Code	Unknown
PID	4880
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #120: rzvaqzgqak.exe

ID	120
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 255268, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	53.89s
Return Code	Unknown
PID	668
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #121: rzvaqzgqak.exe

ID	121
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 255807, Reason: Child Process
Unmonitor End Time	End Time: 302456, Reason: Terminated
Monitor duration	46.65s
Return Code	0
PID	4492
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	17
User	1

Network Behavior

Type	Count
HTTP	1

Process #122: rzvaqzgqak.exe

ID	122
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 256330, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	52.83s
Return Code	Unknown
PID	4536
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #123: rzvaqzgqak.exe

ID	123
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 256843, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	52.31s
Return Code	Unknown
PID	768
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #124: rzvaqzgqak.exe

ID	124
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 258931, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	50.23s
Return Code	Unknown
PID	4500
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #125: rzvaqzgqak.exe

ID	125
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 261625, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	47.53s
Return Code	Unknown
PID	1196
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #126: rzvaqzgqak.exe

ID	126
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 269327, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	39.83s
Return Code	Unknown
PID	4804
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	17
File	3
Environment	1

Process #127: rzvaqzgqak.exe

ID	127
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 273607, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	35.55s
Return Code	Unknown
PID	3616
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #128: rzvaqzgqak.exe

ID	128
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 279263, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	29.89s
Return Code	Unknown
PID	4556
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #129: rzvaqzgqak.exe

ID	129
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 282082, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	27.07s
Return Code	Unknown
PID	4824
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	17
File	3
Environment	1

Process #130: rzvaqzgqak.exe

ID	130
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 284199, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	24.96s
Return Code	Unknown
PID	2904
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #131: rzvaqzgqak.exe

ID	131
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 285669, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	23.49s
Return Code	Unknown
PID	568
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #132: rzvaqzgqak.exe

ID	132
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 286478, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	22.68s
Return Code	Unknown
PID	4224
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #133: rzvaqzgqak.exe

ID	133
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 288136, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	21.02s
Return Code	Unknown
PID	2952
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #134: rzvaqzgqak.exe

ID	134
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 289354, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	19.80s
Return Code	Unknown
PID	2648
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #135: rzvaqzgqak.exe

ID	135
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 289625, Reason: Child Process
Unmonitor End Time	End Time: 309156, Reason: Terminated by timeout
Monitor duration	19.53s
Return Code	Unknown
PID	4752
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	18
File	3
Environment	1

Process #136: rzvaqzgqak.exe

ID	136
File Name	c:\users\rdhj0cnfevzx\desktop\rzvaqzgqak.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 290184, Reason: Child Process
Unmonitor End Time	End Time: 304620, Reason: Terminated
Monitor duration	14.44s
Return Code	0
PID	3212
Parent PID	1640
Bitness	64 Bit

Host Behavior

Type	Count
Module	497
File	3
Environment	1
System	14
User	1

Network Behavior

Type	Count
HTTP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6	C:\Users\RDhJ0CNFevzX\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll	Sample File	352.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
92e4bcc9d85220f941eac6090cb30ebce298894f48fd1d0782ddd60211fb8d12	-	Downloaded File	268 bytes	text/html	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll	Sample File, VM File	-	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpmt4chc1t	Accessed File	Access, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://alexbionka.com	-	64.227.108.27	-	GET	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
alexbionka.com	64.227.108.27	-	HTTP, TCP, DNS	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
64.227.108.27	alexbionka.com	United States	HTTP, TCP, DNS	CLEAN
127.0.0.1	-	-	-	CLEAN

Process

Process Name	Commandline	Verdict
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="explorer.exe"	SUSPICIOUS
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpmt4chc1t" /s	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW	CLEAN

Process Name	Commandline	Verdict
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="0"	CLEAN

Process Name	Commandline	Verdict
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="0"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzIW /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="Install"	CLEAN

Process Name	Commandline	Verdict
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="Install"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="DefaultInstall"	CLEAN

Process Name	Commandline	Verdict
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="DefaultInstall"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="127.0.0.1"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="explorer.exe"	CLEAN

Process Name	Commandline	Verdict
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="explorer.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDHJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="iexplore.exe"	CLEAN

Process Name	Commandline	Verdict
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="iexplore.exe"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=JfUksQmDGYQRSQfC /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=MVeMOgOlu /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=OnqcowdLVOpj /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=aXXRQNg /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=agetCYHzlW /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=bbMIBZKkpJrSw /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=nvWxVSzNIh /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=onXyNAQeqW /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=qBYCIPM /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=raiafa /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ryiLrNIWKPUxQAhG /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=tndPRjog /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=vGGAkgKOkEwmNdGA /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=zBiUZzLtC /fn_args="%Temp%\IXP000.TMP\"	CLEAN
rzvaqzgqak.exe	"C:\Users\RDhJ0CNFevzX\Desktop\RzVAqZGqAk.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8cd135e5b49d16aceb7665b6316cd4df2e132ef503ff0af51c080bad7010efd6.exe.dll" /fn_id=ztyasufasklfmjnaks /fn_args="%Temp%\IXP000.TMP\"	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	IcedID_Loader	IcedID Initial Downloader	Memory Dump	-	Downloader	5/5
Malware	IcedID_Loader	IcedID Initial Downloader	Memory Dump	-	Downloader	5/5

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	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.16 / 2022-08-10 15:34:29
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
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