MALICIOUS

Classifications: Downloader

Threat Names: BumbleBee

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll**
ID	#6849654
MD5	a740177df6f2918373d4e6f482b8c2e3
SHA1	4501edd7904033cfdee783c03af2df0db935be30
SHA256	51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656
File Size	903.00 KB
Report Created	2023-02-03 20:26 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (10 rules, 104 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	BumbleBee configuration was extracted	1	Downloader
	• A configuration for BumbleBee was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	8	Downloader
	• Rule "BumbleBee_v3" from ruleset "Malware" has matched on a memory dump for (process #2) mrnqsjgq.exe. • Rule "BumbleBee_v3" from ruleset "Malware" has matched on a memory dump for (process #12) mrnqsjgq.exe. • Rule "BumbleBee_v3" from ruleset "Malware" has matched on a memory dump for (process #7) mrnqsjgq.exe. • Rule "BumbleBee_v3" from ruleset "Malware" has matched on a memory dump for (process #35) mrnqsjgq.exe. • Rule "BumbleBee_v3" from ruleset "Malware" has matched on a memory dump for (process #40) mrnqsjgq.exe. • Rule "BumbleBee_v3" from ruleset "Malware" has matched on a memory dump for (process #22) mrnqsjgq.exe. • Rule "BumbleBee_v3" from ruleset "Malware" has matched on a memory dump for (process #45) mrnqsjgq.exe. • Rule "BumbleBee_v3" from ruleset "Malware" has matched on a memory dump for (process #17) mrnqsjgq.exe.			
3/5	Anti Analysis	Modifies native system functions	3	-
	• (Process #45) mrnqsjgq.exe modifies native system functions, possibly to evade hooking. • (Process #7) mrnqsjgq.exe modifies native system functions, possibly to evade hooking. • (Process #12) mrnqsjgq.exe modifies native system functions, possibly to evade hooking.			
2/5	Discovery	Executes WMI query	20	-
	• (Process #2) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #2) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct. • (Process #7) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #7) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct. • (Process #2) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_OperatingSystem . • (Process #12) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #2) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem . • (Process #12) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct. • (Process #17) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #17) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct. • (Process #22) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #22) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct. • (Process #27) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #27) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct. • (Process #35) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #35) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct. • (Process #40) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #40) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct. • (Process #45) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystem. • (Process #45) mrnqsjgq.exe executes WMI query: SELECT * FROM Win32_ComputerSystemProduct.			
2/5	Discovery	Collects hardware properties	9	-

Score	Category	Operation	Count	Classification
		• (Process #2) mrnqsjgq.exe queries hardware properties via WMI. • (Process #7) mrnqsjgq.exe queries hardware properties via WMI. • (Process #12) mrnqsjgq.exe queries hardware properties via WMI. • (Process #17) mrnqsjgq.exe queries hardware properties via WMI. • (Process #22) mrnqsjgq.exe queries hardware properties via WMI. • (Process #27) mrnqsjgq.exe queries hardware properties via WMI. • (Process #35) mrnqsjgq.exe queries hardware properties via WMI. • (Process #40) mrnqsjgq.exe queries hardware properties via WMI. • (Process #45) mrnqsjgq.exe queries hardware properties via WMI.		
2/5	Discovery	Queries OS version via WMI	1	-
		• (Process #2) mrnqsjgq.exe queries OS version via WMI.		
1/5	Network Connection	Connects to remote host	9	-
		• (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "223.135.6.77:148". • (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "156.216.108.127:166". • (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "95.75.67.119:378". • (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "102.140.73.149:203". • (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "205.29.103.127:281". • (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "19.145.84.7:406". • (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "67.170.228.186:485". • (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "68.14.122.249:399". • (Process #2) mrnqsjgq.exe opens an outgoing TCP connection to host "131.0.32.0:278".		
1/5	Network Connection	Tries to connect using an uncommon port	9	-
		• (Process #2) mrnqsjgq.exe tries to connect to TCP port 148 at 223.135.6.77. • (Process #2) mrnqsjgq.exe tries to connect to TCP port 399 at 68.14.122.249. • (Process #2) mrnqsjgq.exe tries to connect to TCP port 166 at 156.216.108.127. • (Process #2) mrnqsjgq.exe tries to connect to TCP port 378 at 95.75.67.119. • (Process #2) mrnqsjgq.exe tries to connect to TCP port 203 at 102.140.73.149. • (Process #2) mrnqsjgq.exe tries to connect to TCP port 281 at 205.29.103.127. • (Process #2) mrnqsjgq.exe tries to connect to TCP port 406 at 19.145.84.7. • (Process #2) mrnqsjgq.exe tries to connect to TCP port 278 at 131.0.32.0. • (Process #2) mrnqsjgq.exe tries to connect to TCP port 485 at 67.170.228.186.		
1/5	Crash	A monitored process crashed	35	-

Score	Category	Operation	Count	Classification
		• (Process #3) mrnqsjgq.exe crashed. • (Process #4) mrnqsjgq.exe crashed. • (Process #5) mrnqsjgq.exe crashed. • (Process #6) mrnqsjgq.exe crashed. • (Process #8) mrnqsjgq.exe crashed. • (Process #10) mrnqsjgq.exe crashed. • (Process #11) mrnqsjgq.exe crashed. • (Process #13) mrnqsjgq.exe crashed. • (Process #14) mrnqsjgq.exe crashed. • (Process #15) mrnqsjgq.exe crashed. • (Process #16) mrnqsjgq.exe crashed. • (Process #18) mrnqsjgq.exe crashed. • (Process #19) mrnqsjgq.exe crashed. • (Process #20) mrnqsjgq.exe crashed. • (Process #21) mrnqsjgq.exe crashed. • (Process #23) mrnqsjgq.exe crashed. • (Process #24) mrnqsjgq.exe crashed. • (Process #25) mrnqsjgq.exe crashed. • (Process #26) mrnqsjgq.exe crashed. • (Process #28) mrnqsjgq.exe crashed. • (Process #29) mrnqsjgq.exe crashed. • (Process #33) mrnqsjgq.exe crashed. • (Process #34) mrnqsjgq.exe crashed. • (Process #36) mrnqsjgq.exe crashed. • (Process #37) mrnqsjgq.exe crashed. • (Process #38) mrnqsjgq.exe crashed. • (Process #39) mrnqsjgq.exe crashed. • (Process #41) mrnqsjgq.exe crashed. • (Process #42) mrnqsjgq.exe crashed. • (Process #43) mrnqsjgq.exe crashed. • (Process #44) mrnqsjgq.exe crashed. • (Process #46) mrnqsjgq.exe crashed. • (Process #47) mrnqsjgq.exe crashed. • (Process #48) mrnqsjgq.exe crashed. • (Process #49) mrnqsjgq.exe crashed.		
1/5	Obfuscation	Resolves API functions dynamically	9	-
		• (Process #2) mrnqsjgq.exe resolves 65 API functions by name. • (Process #7) mrnqsjgq.exe resolves 65 API functions by name. • (Process #12) mrnqsjgq.exe resolves 65 API functions by name. • (Process #17) mrnqsjgq.exe resolves 65 API functions by name. • (Process #22) mrnqsjgq.exe resolves 65 API functions by name. • (Process #27) mrnqsjgq.exe resolves 65 API functions by name. • (Process #35) mrnqsjgq.exe resolves 65 API functions by name. • (Process #40) mrnqsjgq.exe resolves 65 API functions by name. • (Process #45) mrnqsjgq.exe resolves 65 API functions by name.		

Malware Configuration: BumbleBee

Metadata	Key	Extracted Value
Mission ID	Value	tokdll
Encryption Key	Key Algorithm	SHN5SXNIc21RdQ== RC4

Address	54.160.255.91
Port	451
Network Protocol	tcp
C2	✔
Address	19.145.84.7
Port	406
Network Protocol	tcp
C2	✔
Address	156.216.108.127
Port	166
Network Protocol	tcp
C2	✔
Address	125.244.223.72
Port	490
Network Protocol	tcp
C2	✔
Address	224.92.39.198
Port	215
Network Protocol	tcp
C2	✔
Address	192.111.146.189
Port	443
Network Protocol	tcp
C2	✔
Address	195.20.17.233
Port	443
Network Protocol	tcp
C2	✔
Address	234.127.218.210
Port	313
Network Protocol	tcp
C2	✔
Address	162.245.164.97
Port	137
Network Protocol	tcp
C2	✔
Address	37.174.161.230
Port	189
Network Protocol	tcp
C2	✔
Address	70.32.201.190
Port	205
Network Protocol	tcp
C2	✔
Address	110.116.102.14
Port	316
Network Protocol	tcp
C2	✔
Address	131.0.32.0
Port	278
Network Protocol	tcp
C2	✔
Address	67.170.228.186
Port	485
Network Protocol	tcp
C2	✔
Address	87.187.206.121
Port	253
Network Protocol	tcp
C2	✔
Address	145.182.157.176
Port	119
Network Protocol	tcp
C2	✔
Address	213.2.161.94
Port	366
Network Protocol	tcp
C2	✔
Address	84.67.118.184
Port	380
Network Protocol	tcp
C2	✔
Address	177.98.252.9
Port	392
Network Protocol	tcp
C2	✔
Address	68.14.122.249
Port	399
Network Protocol	tcp
C2	✔
Address	62.113.238.73
Port	443
Network Protocol	tcp
C2	✔
Address	46.161.160.60
Port	264
Network Protocol	tcp
C2	✔
Address	178.222.244.255
Port	172
Network Protocol	tcp
C2	✔

Socket

Metadata	Key	Extracted Value
Other: Identifier	Value	443

Mitre ATT&CK Matrix

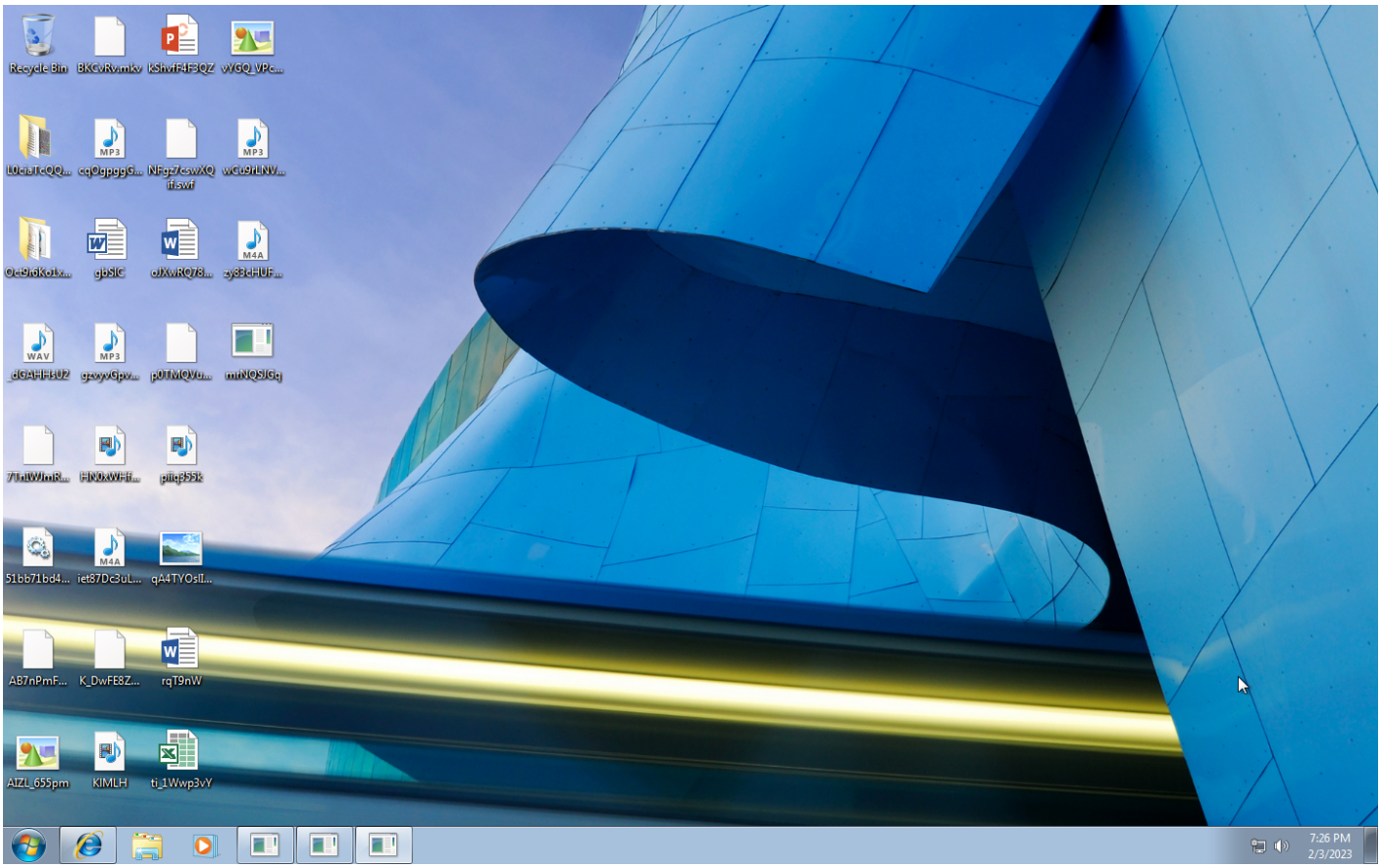
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1045 Software Packing		#T1082 System Information Discovery			#T1065 Uncommonly Used Port		

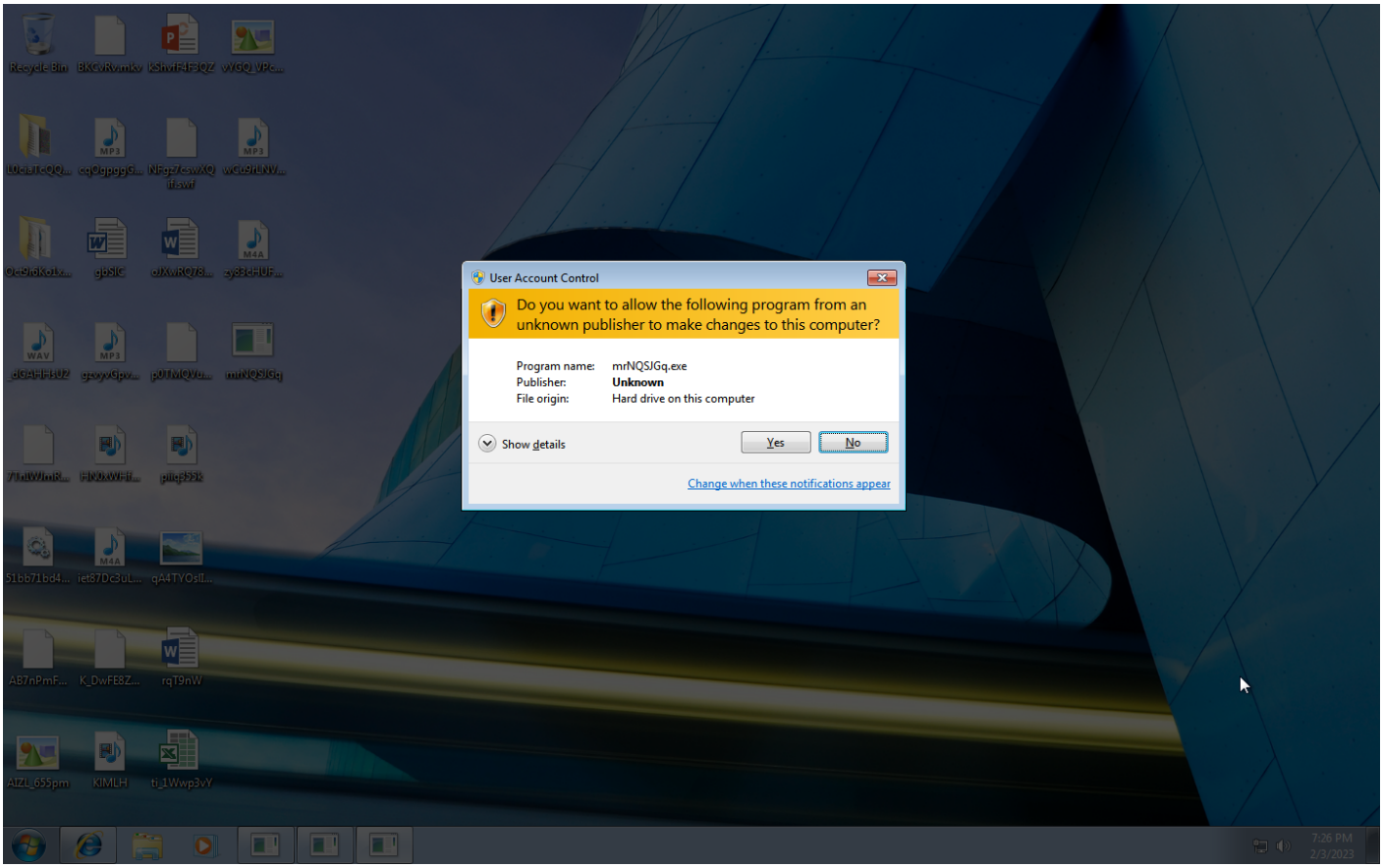
Sample Information

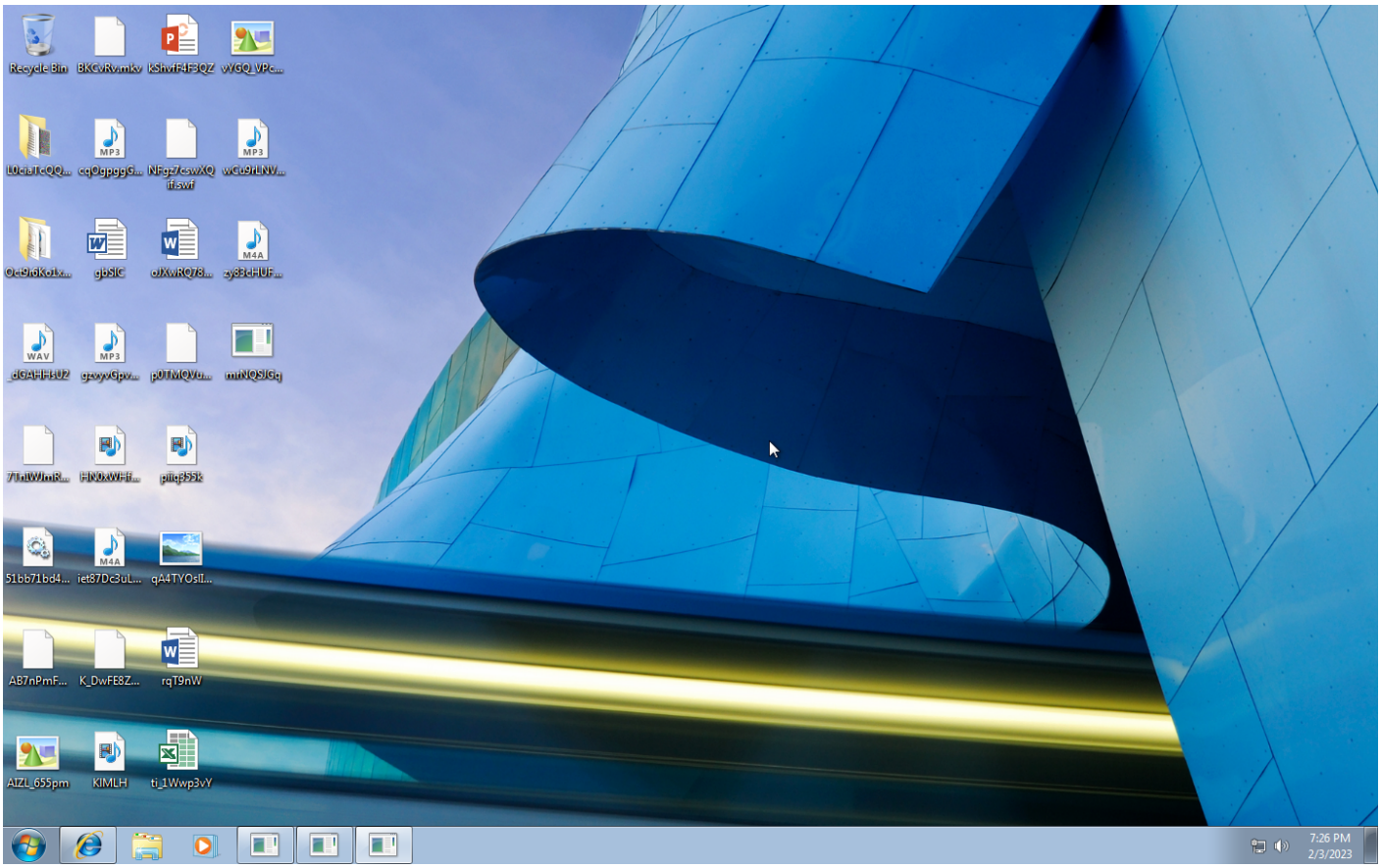
ID	#6849654
MD5	a740177df6f2918373d4e6f482b8c2e3
SHA1	4501edd7904033cfdee783c03af2df0db935be30
SHA256	51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656
SSDeep	24576:gYfSxQ6Gjq/v/PQ7fV+Hz9PuYWp9ToAbXjTA+JxN9QS:/fSqovPQ7Cs9FbTTAAbx
ImpHash	5b5de5739f4fcbaa215d9c878921b5a7
File Name	51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll
File Size	903.00 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✔

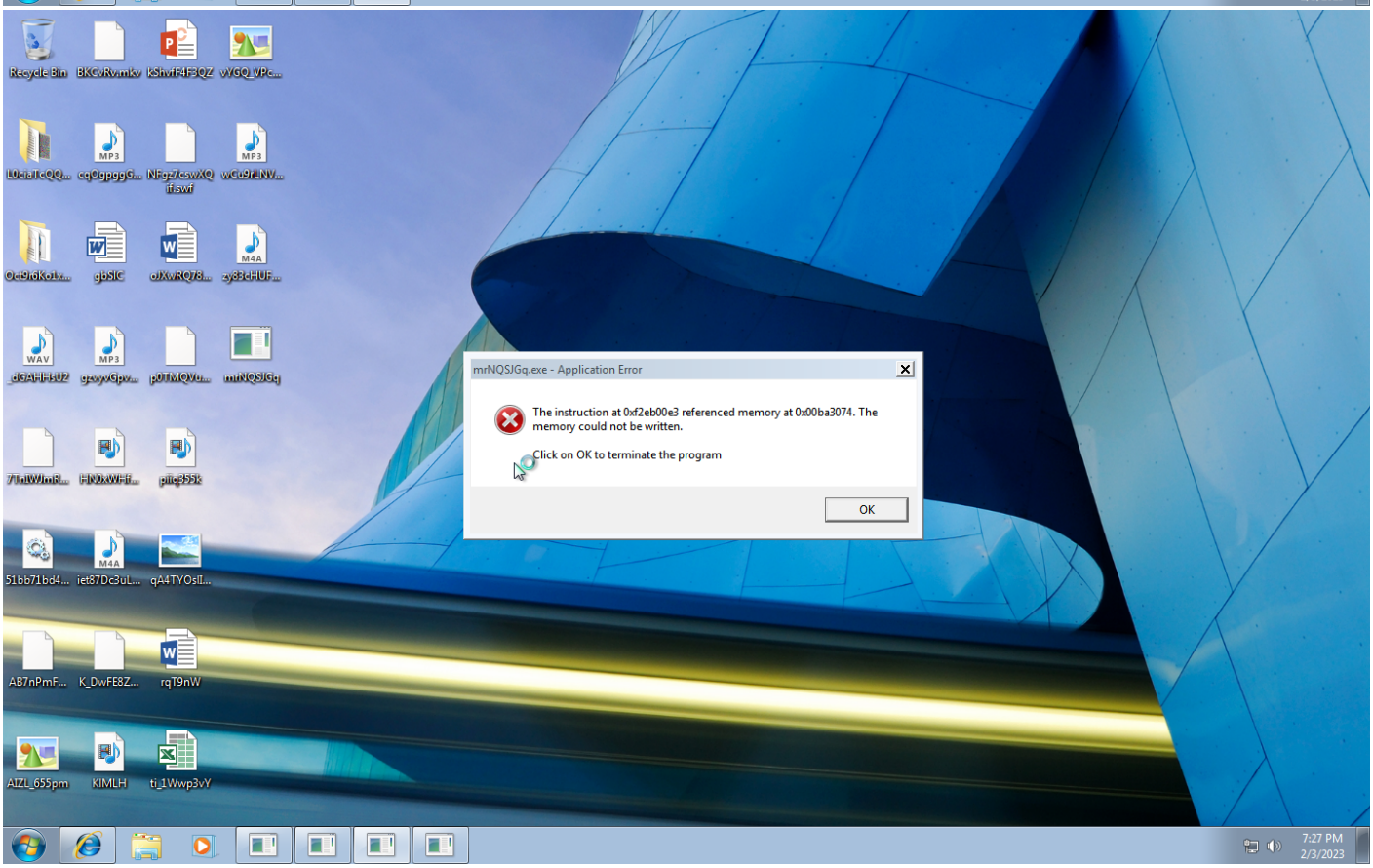
Analysis Information

Creation Time	2023-02-03 20:26 (UTC+1)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	48
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	51




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





Screenshots truncated

NETWORK

General

1.34 KB total sent

120 bytes total received

9 ports 485, 166, 203, 399, 148, 406, 278, 281, 378

9 contacted IP addresses

33 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

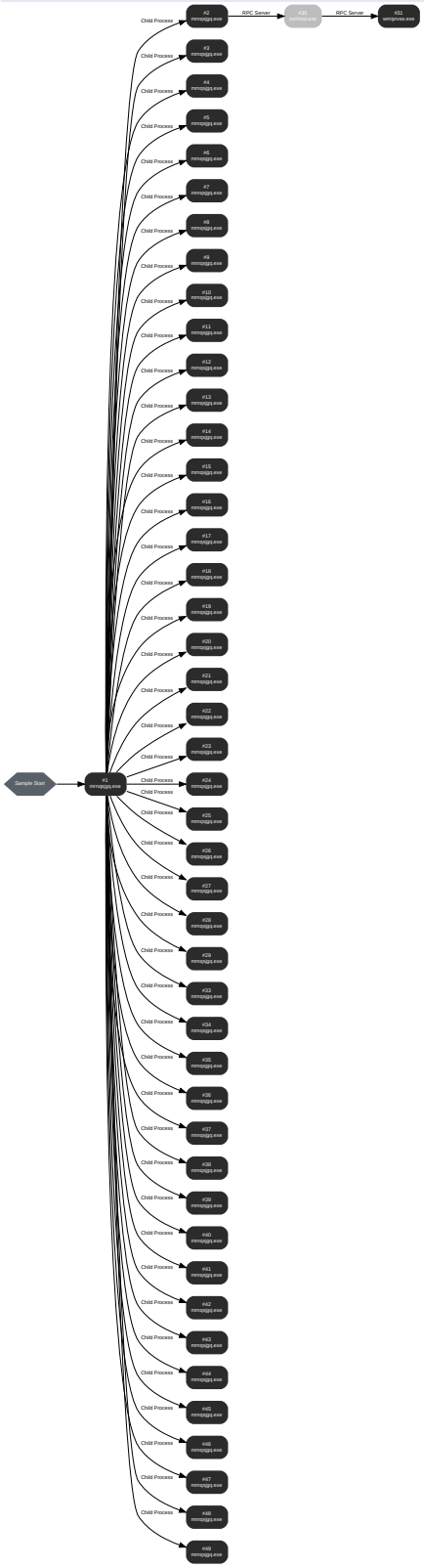
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: mrnqsjgq.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpacqpvsqb" /s
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 45299, Reason: Analysis Target
Unmonitor End Time	End Time: 152420, Reason: Terminated
Monitor duration	107.12s
Return Code	0
PID	4036
Parent PID	1888
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	7
Environment	1
Process	45

Process #2: mrnqsjgq.exe

ID	2
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 48136, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Terminated by timeout
Monitor duration	248.07s
Return Code	Unknown
PID	4056
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	6
Module	118
File	8
Environment	2
-	4
-	1
COM	4
-	4
-	15

Network Behavior

Type	Count
TCP	9

Process #3: mrnqsjgq.exe

ID	3
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 48261, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	247.95s
Return Code	Unknown
PID	4068
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #4: mrnqsjgq.exe

ID	4
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 48469, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	247.74s
Return Code	Unknown
PID	4084
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #5: mrnqsjgq.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 48741, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	247.47s
Return Code	Unknown
PID	2972
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #6: mrnqsjgq.exe

ID	6
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49050, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	247.16s
Return Code	Unknown
PID	2984
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #7: mrnqsjgq.exe

ID	7
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49271, Reason: Child Process
Unmonitor End Time	End Time: 118515, Reason: Terminated
Monitor duration	69.24s
Return Code	0
PID	2996
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	116
File	8
Environment	2
-	2
-	1
COM	3
-	2

Process #8: mrnqsjgq.exe

ID	8
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 49938, Reason: Child Process
Unmonitor End Time	End Time: 145401, Reason: Crashed
Monitor duration	95.46s
Return Code	3221225477
PID	2960
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #9: mrnqsjgq.exe

ID	9
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 50097, Reason: Child Process
Unmonitor End Time	End Time: 65704, Reason: Terminated
Monitor duration	15.61s
Return Code	3221225477
PID	3036
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #10: mrnqsjgq.exe

ID	10
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 51204, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	245.00s
Return Code	Unknown
PID	3056
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #11: mrnqsjgq.exe

ID	11
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt /fn_args="0"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 51372, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	244.84s
Return Code	Unknown
PID	1856
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #12: mrnqsjgq.exe

ID	12
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 52638, Reason: Child Process
Unmonitor End Time	End Time: 120834, Reason: Terminated
Monitor duration	68.20s
Return Code	0
PID	812
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	116
File	8
Environment	2
-	2
-	1
COM	2
-	2

Process #13: mrnqsjgq.exe

ID	13
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 53814, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	242.39s
Return Code	Unknown
PID	2360
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #14: mrnqsjgq.exe

ID	14
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 54598, Reason: Child Process
Unmonitor End Time	End Time: 65712, Reason: Crashed
Monitor duration	11.11s
Return Code	3221225477
PID	1560
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #15: mrnqsjgq.exe

ID	15
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 56218, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	239.99s
Return Code	Unknown
PID	2424
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #16: mrnqsjgq.exe

ID	16
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt /fn_args="1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 57759, Reason: Child Process
Unmonitor End Time	End Time: 135534, Reason: Crashed
Monitor duration	77.78s
Return Code	3221225477
PID	3528
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #17: mrnqsjgq.exe

ID	17
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 59091, Reason: Child Process
Unmonitor End Time	End Time: 123784, Reason: Terminated
Monitor duration	64.69s
Return Code	0
PID	3568
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	117
File	8
Environment	2
-	2
-	1
COM	2
-	3

Process #18: mrnqsjgq.exe

ID	18
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 59314, Reason: Child Process
Unmonitor End Time	End Time: 129873, Reason: Crashed
Monitor duration	70.56s
Return Code	3221225477
PID	3584
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #19: mrnqsjgq.exe

ID	19
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 60423, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	235.78s
Return Code	Unknown
PID	3656
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #20: mrnqsjgq.exe

ID	20
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 63229, Reason: Child Process
Unmonitor End Time	End Time: 83192, Reason: Crashed
Monitor duration	19.96s
Return Code	3221225477
PID	3732
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #21: mrnqsjgq.exe

ID	21
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt /fn_args="Install"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 65775, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	230.43s
Return Code	Unknown
PID	3704
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #22: mrnqsjgq.exe

ID	22
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 66088, Reason: Child Process
Unmonitor End Time	End Time: 132599, Reason: Terminated
Monitor duration	66.51s
Return Code	0
PID	3724
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	116
File	8
Environment	2
-	2
-	1
COM	2
-	2

Process #23: mrnqsjgq.exe

ID	23
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 69137, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	227.07s
Return Code	Unknown
PID	3764
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #24: mrnqsjgq.exe

ID	24
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 70896, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	225.31s
Return Code	Unknown
PID	3812
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #25: mrnqsjgq.exe

ID	25
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 71311, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	224.90s
Return Code	Unknown
PID	3796
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #26: mrnqsjgq.exe

ID	26
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt /fn_args="DefaultInstall"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76075, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	220.13s
Return Code	Unknown
PID	2472
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #27: mrnqsjgq.exe

ID	27
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78813, Reason: Child Process
Unmonitor End Time	End Time: 136270, Reason: Terminated
Monitor duration	57.46s
Return Code	0
PID	2776
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	116
File	8
Environment	2
-	2
-	1
COM	2
-	2

Process #28: mrnqsjgq.exe

ID	28
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 81178, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	215.03s
Return Code	Unknown
PID	2836
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #29: mrnqsjgq.exe

ID	29
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 85278, Reason: Child Process
Unmonitor End Time	End Time: 118131, Reason: Crashed
Monitor duration	32.85s
Return Code	3221225477
PID	2876
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #30: svchost.exe

ID	30
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 90672, Reason: RPC Server
Unmonitor End Time	End Time: 296208, Reason: Terminated by timeout
Monitor duration	205.54s
Return Code	Unknown
PID	872
Parent PID	4056
Bitness	64 Bit

Process #31: wmiprvse.exe

ID	31
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 90672, Reason: RPC Server
Unmonitor End Time	End Time: 296208, Reason: Terminated by timeout
Monitor duration	205.54s
Return Code	Unknown
PID	3424
Parent PID	872
Bitness	64 Bit

Process #33: mrnqsjgq.exe

ID	33
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 91910, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	204.30s
Return Code	Unknown
PID	2944
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #34: mrnqsjgq.exe

ID	34
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt /fn_args="127.0.0.1"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 92870, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	203.34s
Return Code	Unknown
PID	3884
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #35: mrnqsjgq.exe

ID	35
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 98514, Reason: Child Process
Unmonitor End Time	End Time: 140220, Reason: Terminated
Monitor duration	41.71s
Return Code	0
PID	3064
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	116
File	8
Environment	2
-	2
-	1
COM	2
-	2

Process #36: mrnqsjgq.exe

ID	36
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 103856, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	192.35s
Return Code	Unknown
PID	4024
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #37: mrnqsjgq.exe

ID	37
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 106373, Reason: Child Process
Unmonitor End Time	End Time: 149464, Reason: Crashed
Monitor duration	43.09s
Return Code	3221225477
PID	2016
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #38: mrnqsjgq.exe

ID	38
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 108992, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	187.22s
Return Code	Unknown
PID	3516
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #39: mrnqsjgq.exe

ID	39
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt /fn_args="explorer.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 114931, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	181.28s
Return Code	Unknown
PID	3740
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #40: mrnqsjgq.exe

ID	40
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 120835, Reason: Child Process
Unmonitor End Time	End Time: 140611, Reason: Terminated
Monitor duration	19.78s
Return Code	0
PID	3808
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	116
File	8
Environment	2
-	2
-	1
COM	2
-	2

Process #41: mrnqsjgq.exe

ID	41
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 128902, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	167.31s
Return Code	Unknown
PID	1564
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #42: mrnqsjgq.exe

ID	42
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 134958, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	161.25s
Return Code	Unknown
PID	1212
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #43: mrnqsjgq.exe

ID	43
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 137438, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	158.77s
Return Code	Unknown
PID	956
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #44: mrnqsjgq.exe

ID	44
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt /fn_args="iexplore.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 139454, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	156.75s
Return Code	Unknown
PID	2936
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #45: mrnqsjgq.exe

ID	45
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140227, Reason: Child Process
Unmonitor End Time	End Time: 154028, Reason: Terminated
Monitor duration	13.80s
Return Code	0
PID	2796
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	5
Module	116
File	8
Environment	2
-	2
-	1
COM	2
-	2

Process #46: mrnqsjgq.exe

ID	46
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 140612, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	155.60s
Return Code	Unknown
PID	1544
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #47: mrnqsjgq.exe

ID	47
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 145094, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	151.11s
Return Code	Unknown
PID	2188
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #48: mrnqsjgq.exe

ID	48
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 148844, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	147.36s
Return Code	Unknown
PID	3248
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

Process #49: mrnqsjgq.exe

ID	49
File Name	c:\users\keecfmwgj\desktop\mrnqsjgq.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMlFUh3Tzt /fn_args="%Temp%\IXP000.TMP\"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150545, Reason: Child Process
Unmonitor End Time	End Time: 296208, Reason: Crashed
Monitor duration	145.66s
Return Code	Unknown
PID	3300
Parent PID	4036
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	20
File	3
Environment	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656	C:\Users\kEecfMwgj\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll, C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll	Sample File	903.00 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll	Accessed File, Sample File	Access	MALICIOUS
\??\C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\tmpacqpvsqb	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe	Accessed File	Access	CLEAN
\??\C:\Windows\WinSxS\amd64_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_2b24536c71ed437a\gdiplus.dll	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://131[.]0[.]32[.]0:278	Extracted	131.0.32.0	Brazil	-	MALICIOUS
hxxp://238[.]54[.]240[.]219:153	Extracted	238.54.240.219	-	-	MALICIOUS
hxxp://54[.]160[.]255[.]91:451	Extracted	54.160.255.91	-	-	MALICIOUS
hxxp://145[.]182[.]157[.]176:119	Extracted	145.182.157.176	-	-	MALICIOUS
hxxp://19[.]145[.]84[.]7:406	Extracted	19.145.84.7	United States	-	MALICIOUS
hxxp://177[.]98[.]252[.]9:392	Extracted	177.98.252.9	-	-	MALICIOUS
hxxp://62[.]113[.]238[.]73:443	Extracted	62.113.238.73	-	-	MALICIOUS
hxxp://110[.]116[.]102[.]14:316	Extracted	110.116.102.14	-	-	MALICIOUS
hxxp://67[.]170[.]228[.]186:485	Extracted	67.170.228.186	United States	-	MALICIOUS
hxxp://126[.]240[.]38[.]176:121	Extracted	126.240.38.176	-	-	MALICIOUS
hxxp://178[.]222[.]244[.]255:172	Extracted	178.222.244.255	-	-	MALICIOUS
hxxp://61[.]82[.]172[.]52:112	Extracted	61.82.172.52	-	-	MALICIOUS
hxxp://84[.]67[.]118[.]184:380	Extracted	84.67.118.184	-	-	MALICIOUS
hxxp://55[.]176[.]184[.]70:338	Extracted	55.176.184.70	-	-	MALICIOUS
hxxp://37[.]174[.]161[.]230:189	Extracted	37.174.161.230	-	-	MALICIOUS
hxxp://192[.]111[.]146[.]189:443	Extracted	192.111.146.189	-	-	MALICIOUS
hxxp://70[.]32[.]201[.]190:205	Extracted	70.32.201.190	-	-	MALICIOUS
hxxp://213[.]2[.]161[.]94:366	Extracted	213.2.161.94	-	-	MALICIOUS
hxxp://156[.]216[.]108[.]127:166	Extracted	156.216.108.127	Egypt	-	MALICIOUS

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxp://125[.]244[.]223[.]72:490	Extracted	125.244.223.72	-	-	MALICIOUS
hxxp://224[.]92[.]39[.]198:215	Extracted	224.92.39.198	-	-	MALICIOUS
hxxp://205[.]29[.]103[.]127:281	Extracted	205.29.103.127	United States	-	MALICIOUS
hxxp://68[.]14[.]122[.]249:399	Extracted	68.14.122.249	United States	-	MALICIOUS
hxxp://102[.]140[.]73[.]149:203	Extracted	102.140.73.149	South Africa	-	MALICIOUS
hxxp://223[.]135[.]6[.]77:148	Extracted	223.135.6.77	Japan	-	MALICIOUS
hxxp://46[.]161[.]160[.]60:264	Extracted	46.161.160.60	-	-	MALICIOUS
hxxp://87[.]187[.]206[.]121:253	Extracted	87.187.206.121	-	-	MALICIOUS
hxxp://95[.]75[.]67[.]119:378	Extracted	95.75.67.119	Italy	-	MALICIOUS
hxxp://50[.]34[.]114[.]59:137	Extracted	50.34.114.59	-	-	MALICIOUS
hxxp://244[.]65[.]94[.]203:282	Extracted	244.65.94.203	-	-	MALICIOUS
hxxp://234[.]127[.]218[.]210:313	Extracted	234.127.218.210	-	-	MALICIOUS
hxxp://162[.]245[.]164[.]97:137	Extracted	162.245.164.97	-	-	MALICIOUS
hxxp://195[.]20[.]17[.]233:443	Extracted	195.20.17.233	-	-	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
68.14.122.249	-	United States	TCP	CLEAN
162.245.164.97	-	-	-	CLEAN
62.113.238.73	-	-	-	CLEAN
126.240.38.176	-	-	-	CLEAN
70.32.201.190	-	-	-	CLEAN
127.0.0.1	-	-	-	CLEAN
55.176.184.70	-	-	-	CLEAN
178.222.244.255	-	-	-	CLEAN
54.160.255.91	-	-	-	CLEAN
223.135.6.77	-	Japan	TCP	CLEAN
125.244.223.72	-	-	-	CLEAN
19.145.84.7	-	United States	TCP	CLEAN
61.82.172.52	-	-	-	CLEAN
177.98.252.9	-	-	-	CLEAN
131.0.32.0	-	Brazil	TCP	CLEAN
156.216.108.127	-	Egypt	TCP	CLEAN
67.170.228.186	-	United States	TCP	CLEAN
205.29.103.127	-	United States	TCP	CLEAN
224.92.39.198	-	-	-	CLEAN
238.54.240.219	-	-	-	CLEAN

IP Address	Domains	Country	Protocols	Verdict
110.116.102.14	-	-	-	CLEAN
46.161.160.60	-	-	-	CLEAN
84.67.118.184	-	-	-	CLEAN
87.187.206.121	-	-	-	CLEAN
192.111.146.189	-	-	-	CLEAN
244.65.94.203	-	-	-	CLEAN
195.20.17.233	-	-	-	CLEAN
95.75.67.119	-	Italy	TCP	CLEAN
234.127.218.210	-	-	-	CLEAN
37.174.161.230	-	-	-	CLEAN
50.34.114.59	-	-	-	CLEAN
213.2.161.94	-	-	-	CLEAN
145.182.157.176	-	-	-	CLEAN
102.140.73.149	-	South Africa	TCP	CLEAN

Process

Process Name	Commandline	Verdict
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc	SUSPICIOUS
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fel="C:\Users\KEECFM~1\AppData\Local\Temp\tmpacqpvsqb" /s	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=Cpurthnvlc /fn_args="0"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="0"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="0"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="0"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt /fn_args="0"	CLEAN

Process Name	Commandline	Verdict
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=CpurthnvIc /fn_args="1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt /fn_args="1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=CpurthnvIc /fn_args="Install"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="Install"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="Install"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="Install"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt /fn_args="Install"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=CpurthnvIc /fn_args="DefaultInstall"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="DefaultInstall"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="DefaultInstall"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="DefaultInstall"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt /fn_args="DefaultInstall"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=CpurthnvIc /fn_args="127.0.0.1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="127.0.0.1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="127.0.0.1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="127.0.0.1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt /fn_args="127.0.0.1"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=CpurthnvIc /fn_args="explorer.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="explorer.exe"	CLEAN

Process Name	Commandline	Verdict
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="explorer.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="explorer.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt /fn_args="explorer.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=CpurthnvIc /fn_args="iexplore.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="iexplore.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="iexplore.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="iexplore.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt /fn_args="iexplore.exe"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=CpurthnvIc /fn_args="%Temp%\IXP000.TMP\"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=FPH732n7 /fn_args="%Temp%\IXP000.TMP\"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=KlXWgB9j /fn_args="%Temp%\IXP000.TMP\"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=LKKIJ77 /fn_args="%Temp%\IXP000.TMP\"	CLEAN
mrnqsjgq.exe	"C:\Users\kEecfMwgj\Desktop\mrNQSJGq.exe" /dll="C:\Users\KEECFM~1\Desktop\51bb71bd446bd7fc03cc1234fcc3f489f10db44e312c9ce619b937fad6912656.exe.dll" /fn_id=MMIFUh3Tzt /fn_args="%Temp%\IXP000.TMP\"	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

YARA (51)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5
Malware	BumbleBee_v3	BumbleBee	Memory Dump	-	Downloader	5/5

ENVIRONMENT

Virtual Machine Information

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

Platform Information

Platform Version	2023.1.0
Dynamic Engine Version	2023.1.0 / 01/31/2023 04:27
Static Engine Version	2023.1.0.0 / 2023-01-31 03:00:19
AV Exceptions Version	2023.1.0.1 / 2023-01-16 12:28:15
Link Detonation Heuristics Version	2023.1.0.3 / 2023-01-26 15:34:20
Smart Memory Dumping Rules Version	2023.1.0.1 / 2023-01-16 12:28:15
Config Extractors Version	2023.1.0.3 / 2023-01-26 15:34:20
Signature Trust Store Version	2023.1.0.3 / 2023-01-26 15:34:20
VMRay Threat Identifiers Version	2023.1.0.5 / 2023-02-02 10:39:37
YARA Built-in Ruleset Version	2023.1.0.3

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	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp

System Root	C:\Windows