MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Word Document**
File Name	**3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47.doc**
ID	#5127471
MD5	2b10f2617b32857999df1cf5f19f0d8d
SHA1	448e513536aa0c576b123d5b243e1bdc6d261d6f
SHA256	3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47
File Size	2244.96 KB
Report Created	2022-08-11 21:07 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (4 rules, 4 matches)

Score	Category	Operation	Count	Classification
4/5	Network Connection	Attempts to connect through HTTP	1	-
	• (Process #1) winword.exe connects to http://45.8.146.139/fhfty/A8-39SODTF9EOBD6C7Q2AKY01XKI_WQ2/loader_p3_dll_64_n3_crypt_x64_asm_clone_n129.dll.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Execution	Executes macro on specific event	1	-
	• Executes macro automatically on target "document" and event "open".			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			

Mitre ATT&CK Matrix

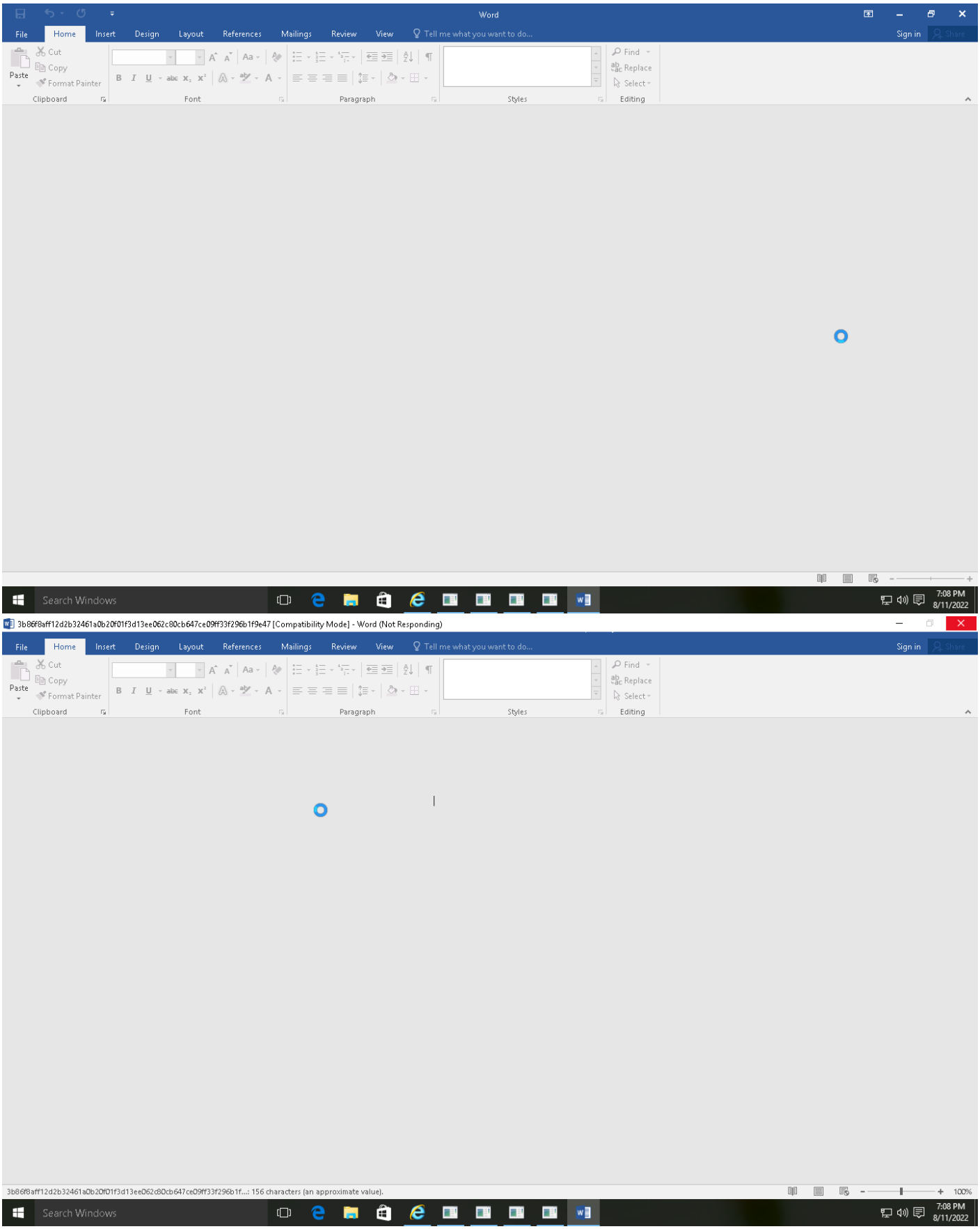
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1064 Scripting					#T1071 Standard Application Layer Protocol		

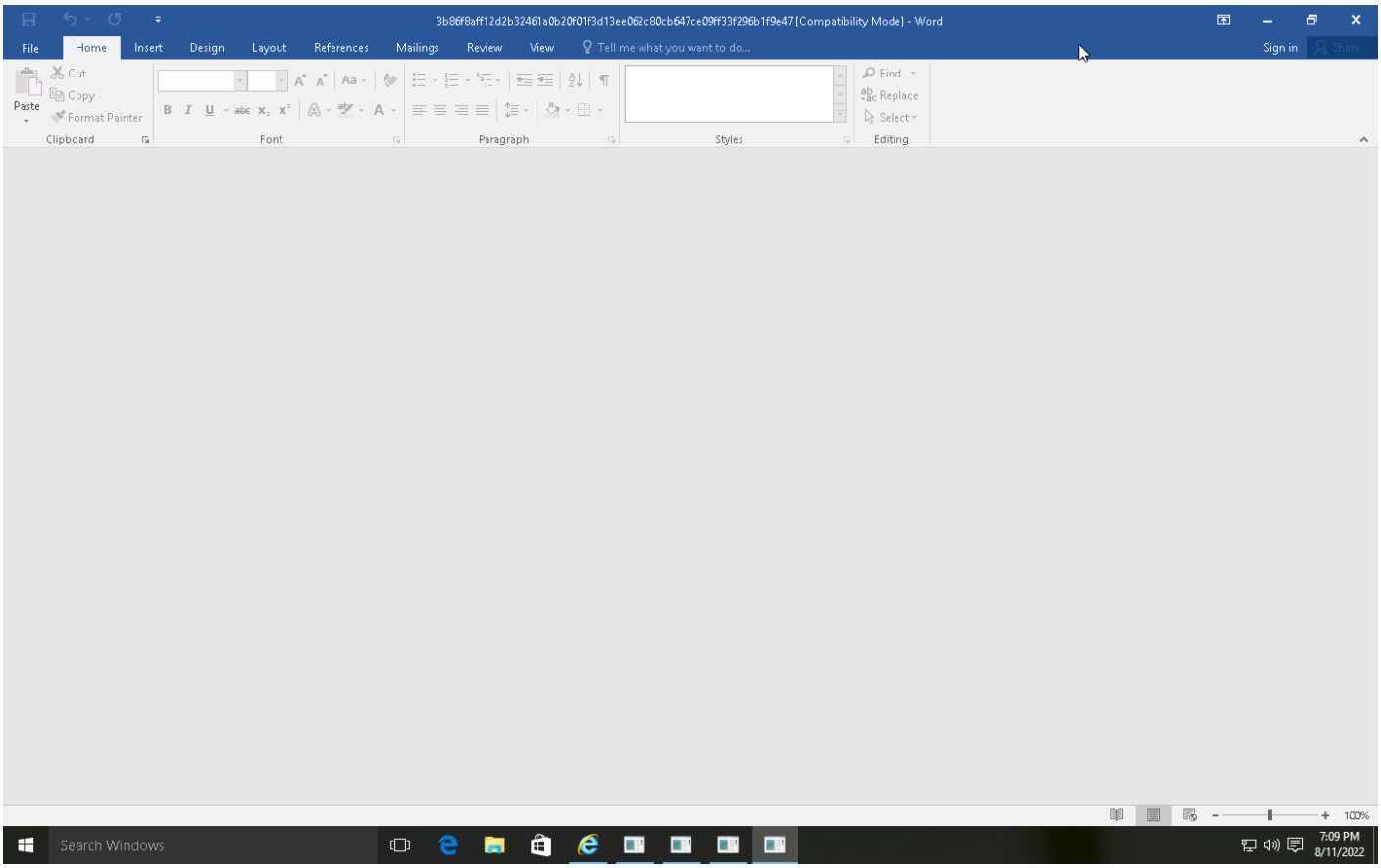
Sample Information

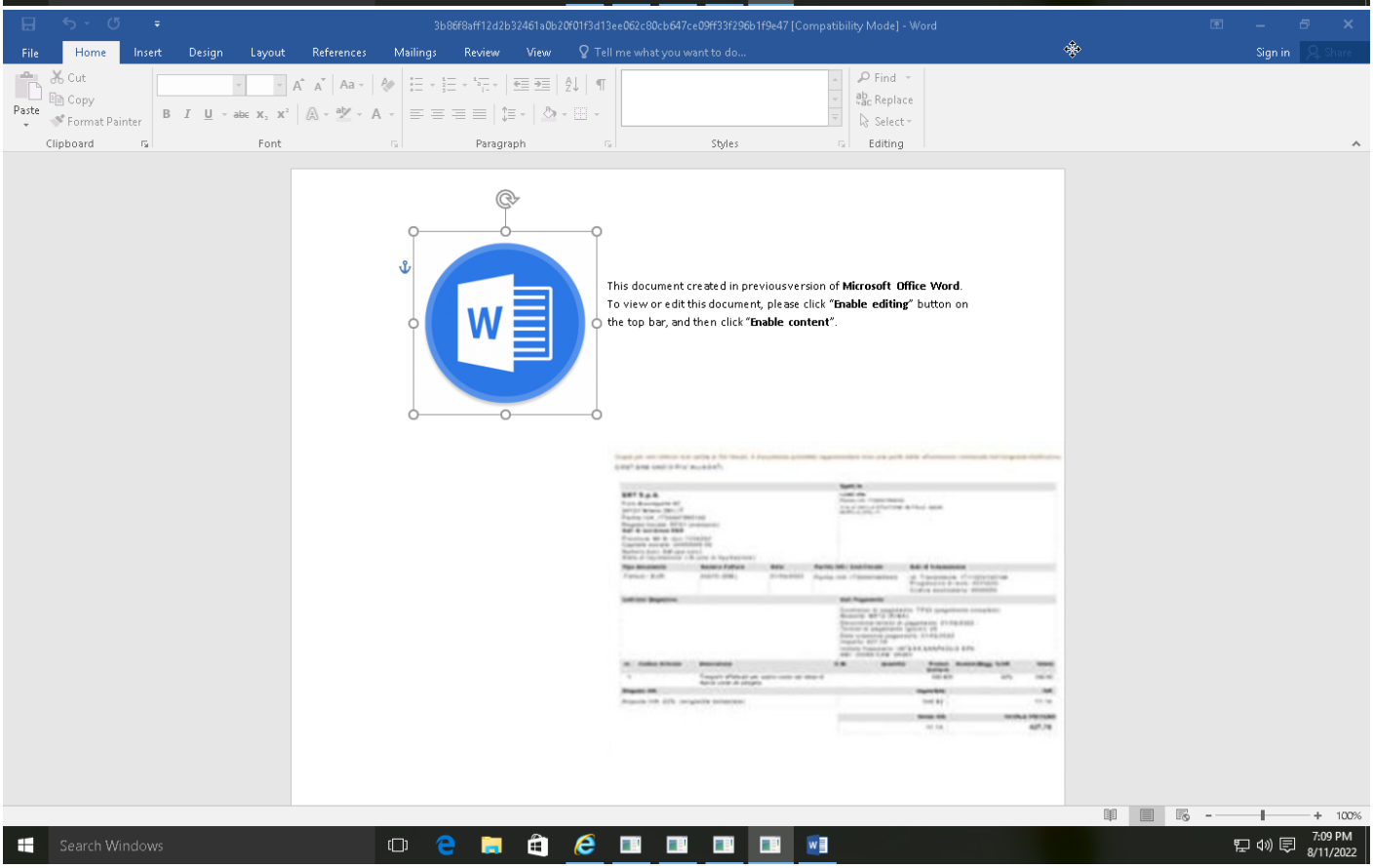
ID	#5127471
MD5	2b10f2617b32857999df1cf5f19f0d8d
SHA1	448e513536aa0c576b123d5b243e1bdc6d261d6f
SHA256	3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47
SSDeep	49152:tljQhPf8F7u26T076/JsKhCa8CCGEEt1yEU:WjufCre/1UMEEzyh
File Name	3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47.doc
File Size	2244.96 KB
Sample Type	Word Document
Has Macros	✔

Analysis Information

Creation Time	2022-08-11 21:07 (UTC+2)
Analysis Duration	00:04:09
Termination Reason	Timeout
Number of Monitored Processes	1
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	0


Word
File Home Insert Design Layout References Mailings Review View Tell me what you want to do... Sign in Share
Paste Cut Copy Format Painter
Clipboard Font Paragraph Styles Editing
Find Replace Select
Search Windows
7:08 PM 8/11/2022
3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47 [Compatibility Mode] - Word (Not Responding)
3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f...: 156 characters (an approximate value).
100%





Screenshots truncated

NETWORK

General

851 bytes total sent

680 bytes total received

1 ports 80

1 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 771 bytes sent, 680 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://45.8.146.139/fhfty/A8-39SODTF9EOBD6C7Q2AKY01XKI_WQ2/loader_p3_dll_64_n3_crypt_x64_asm_clone_n129.dll	-	-		0 bytes	NA

BEHAVIOR

Process Graph

Process #1: winword.exe

ID	1
File Name	c:\program files (x86)\microsoft office\office16\winword.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 56823, Reason: Analysis Target
Unmonitor End Time	End Time: 306467, Reason: Terminated by timeout
Monitor duration	249.64s
Return Code	Unknown
PID	4944
Parent PID	1972
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	247 bytes	c175b47463d9b491fd2c37332744f9720dcc5157e2b97ee3b3a1174499a101f6	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\yBDEB.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	82
Keyboard	61
System	9
File	12
Environment	1
-	3

Network Behavior

Type	Count
HTTP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47	C:\Users\RDhJ0CNFevzX\Desktop\3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47.doc	Sample File	2244.96 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	MALICIOUS
8cd11eb654c64c7315f7b2904d123532f7993faf2f210b250c4c4d670200ff73	image1.png	Extracted File	60.48 KB	image/png	-	CLEAN
c175b47463d9b491fd2c37332744f9720dcc5157e2b97ee3b3a1174499a101f6	C:\Users\RDHJ0C~1\AppData\Local\Temp\yBDEB.tmp.dll	Downloaded File	247 bytes	text/html	Access, Create, Read	CLEAN
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
6ad88ef0bbe4928886afcbe59b5c6af268bc8962dea7636c7bfb4a593a6fd77c	image2.png	Extracted File	250.66 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\3b86f8aff12d2b32461a0b20f01f3d13ee062c80cb647ce09ff33f296b1f9e47.doc	Sample File, VM File	-	MALICIOUS
C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\yBDEB.tmp.dll	Accessed File, Downloaded File, Extracted File	Access, Create, Read	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\l738dhgv\loader_p3_dll_64_n3_crypt_x64_asm_clone_n129[1].htm	Downloaded File, Extracted File	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
ThisDocument	-	-	CLEAN
image2.png	-	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\yBDEB.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
image1.png	-	-	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://45.8.146.139/fhfty/A8-39SODTF9EOBD6C7Q2AKY01XKI_WQ2/loader_p3_dll_64_n3_crypt_x64_asm_clone_n129.dll	-	45.8.146.139	-	GET	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
45.8.146.139	-	Russia	HTTP, TCP	CLEAN

Process

Process Name	Commandline	Verdict
winword.exe	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n	CLEAN

YARA / AV

No YARA or AV matches available.

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