MALICIOUS

Classifications: -
Threat Names: -
Verdict Reason: -

Sample Type	**Word Document**
File Name	**d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82.doc**
ID	#5129041
MD5	4f487d329bcf514575a0c8e5a4dcb53f
SHA1	52d9885233394acffdda1ea3a40989a8b47e9e34
SHA256	d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82
File Size	2261.96 KB
Report Created	2022-08-12 03:25 (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 failed to connect to http://45.8.146.139/fhfty/WM9BW2TQYMF_YV4HRQ4WA3K_5F-D0L5S/rm.			
3/5	Network Connection	All network connection attempts failed	1	-
	• Host "45.8.146.139" is unavailable.			
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

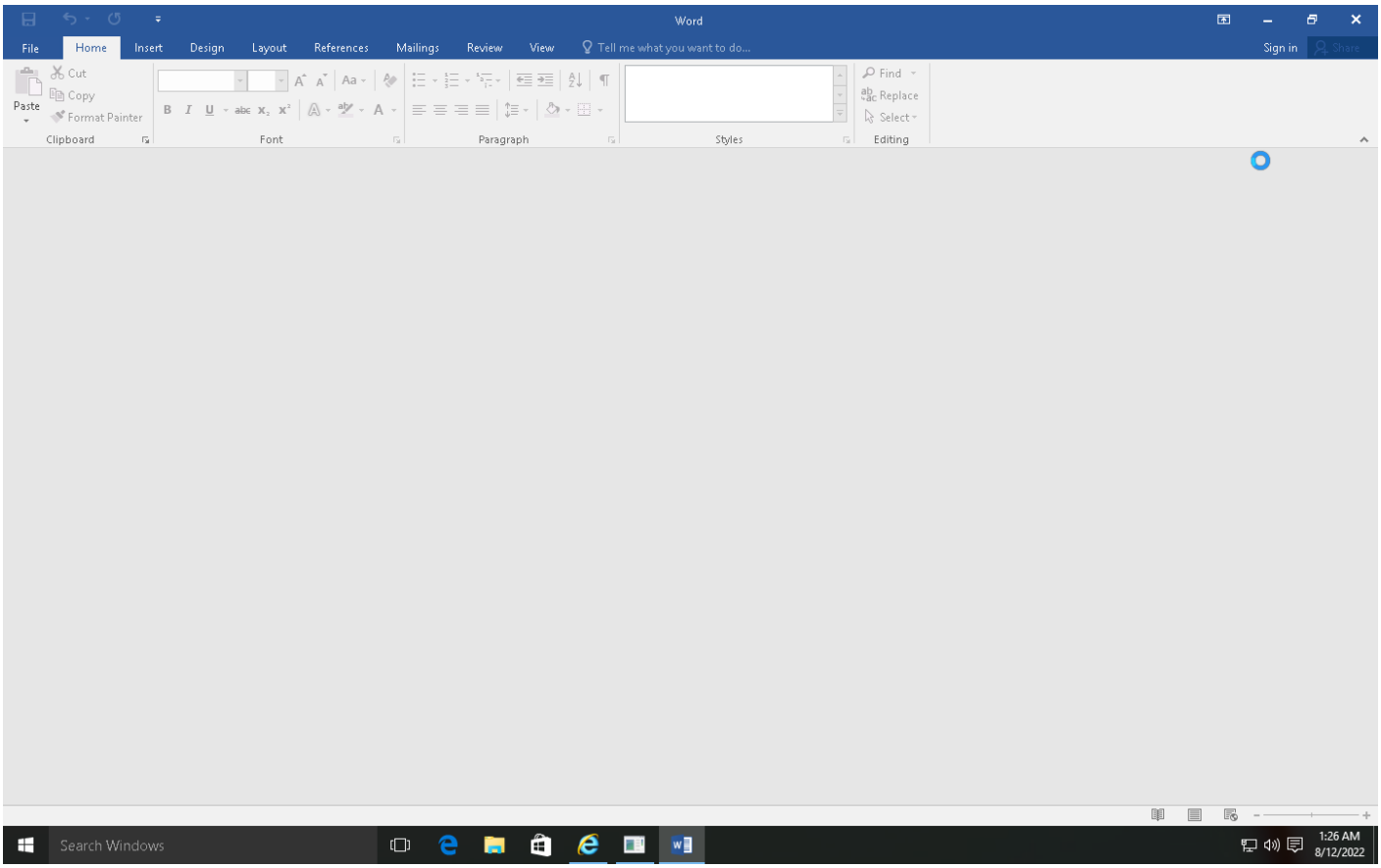
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1064 Scripting					#T1071 Standard Application Layer Protocol		

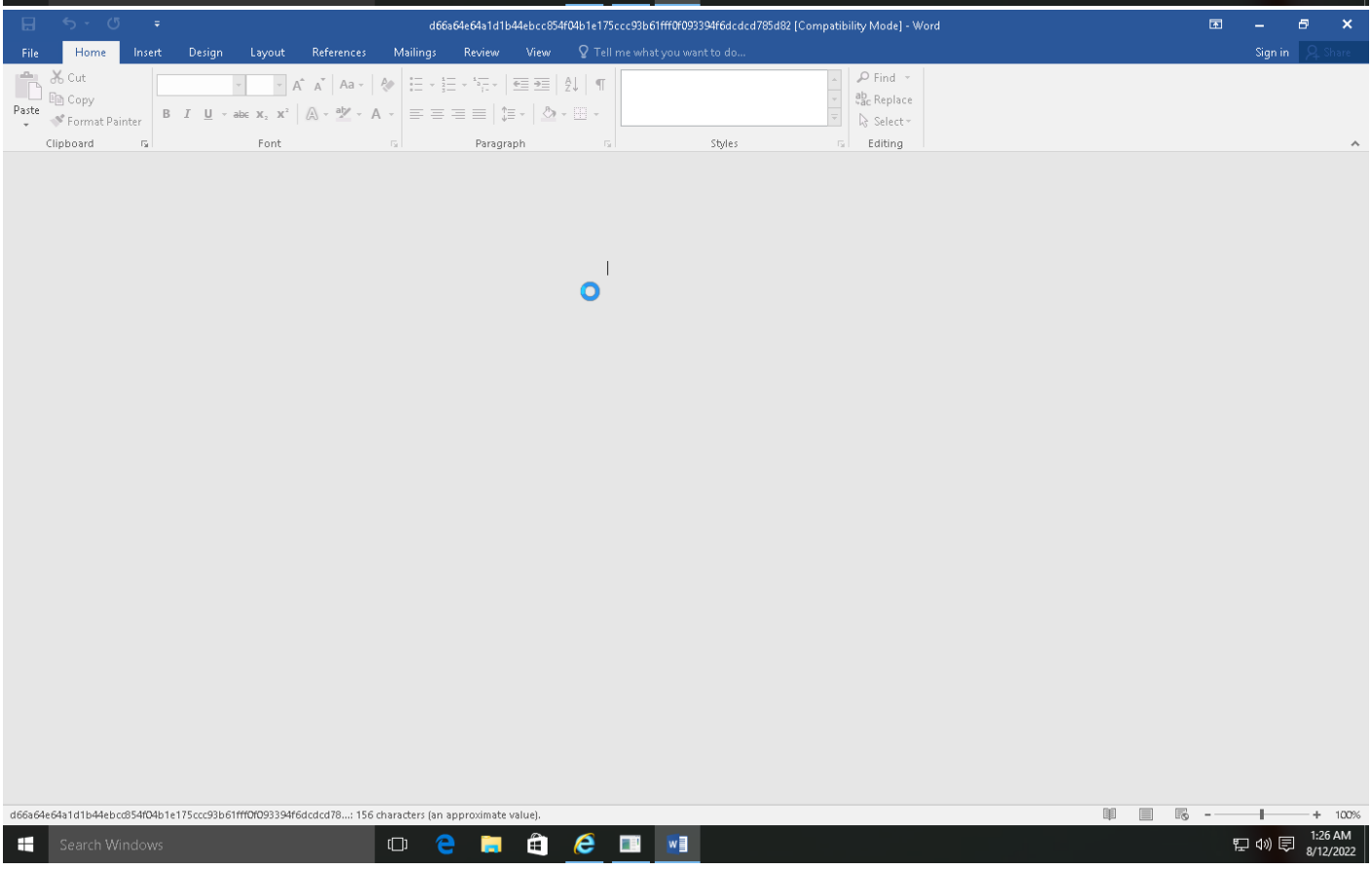
Sample Information

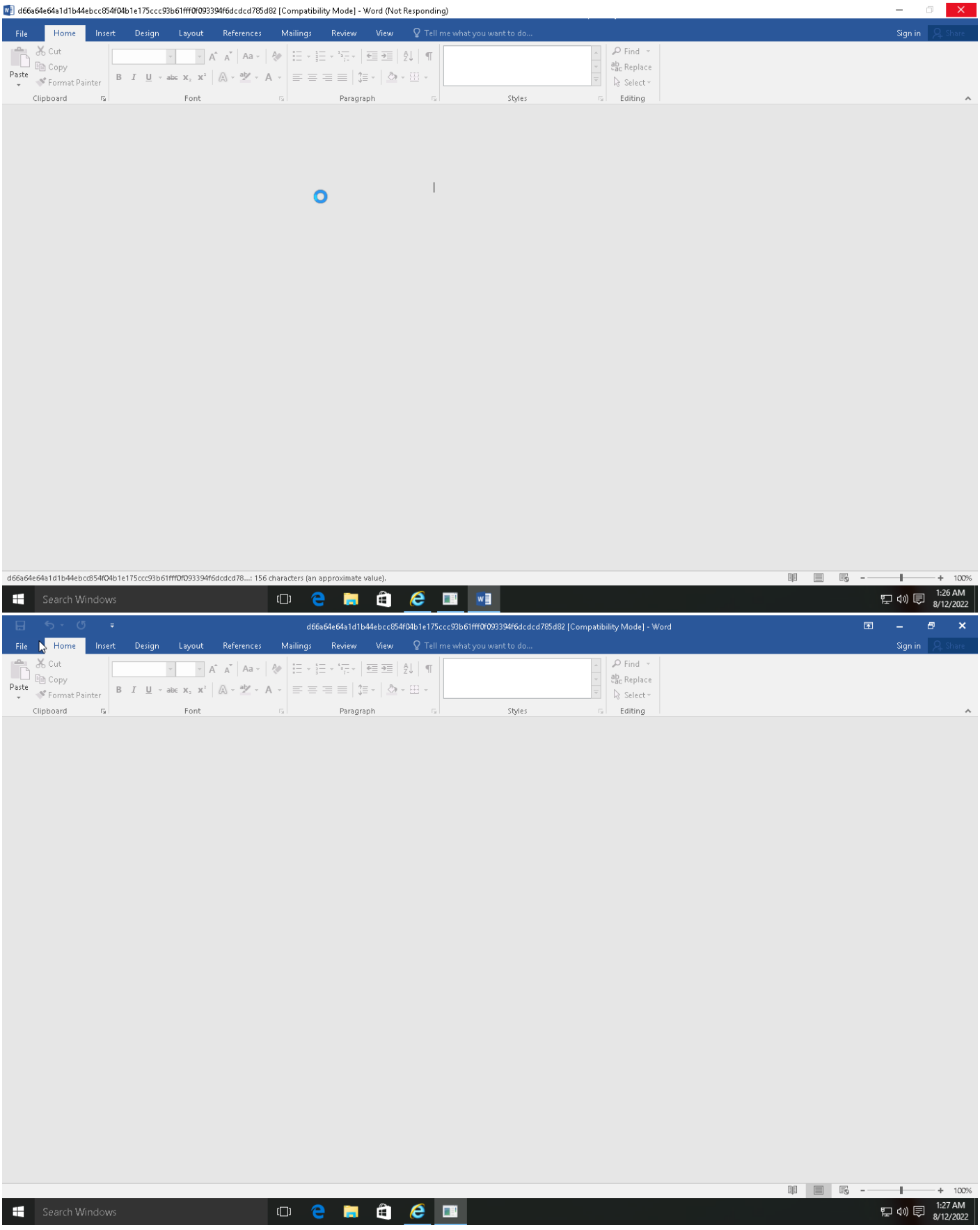
ID	#5129041
MD5	4f487d329bcf514575a0c8e5a4dcb53f
SHA1	52d9885233394acffdda1ea3a40989a8b47e9e34
SHA256	d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82
SSDeep	49152:TnxBpMvUTIyOgNz8bc10lsulzqMy44elEAU33SapcOnaT54Z1+bBOz:TxBpMavFNzUculsul+d44e1y3VIV4rY2
File Name	d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82.doc
File Size	2261.96 KB
Sample Type	Word Document
Has Macros	✔

Analysis Information

Creation Time	2022-08-12 03:25 (UTC+2)
Analysis Duration	00:04:08
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
1:26 AM
8/12/2022


d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82 [Compatibility Mode] - 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
d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd78...: 156 characters (an approximate value).
100%
Search Windows
1:26 AM
8/12/2022



Screenshots truncated

NETWORK

General

244 bytes total sent

40 bytes total received

2 ports 80, 445

2 contacted IP addresses

1 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

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://45.8.146.139/fhfty/WM9BW2TQYMF_YV4HRQ4WA3K_5F-D0L5S/rm	-	-		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: 71100, Reason: Analysis Target
Unmonitor End Time	End Time: 319678, Reason: Terminated by timeout
Monitor duration	248.58s
Return Code	Unknown
PID	4796
Parent PID	1972
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\y8DFD.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	84
Keyboard	65
System	10
File	7
Environment	1
-	4

Network Behavior

Type	Count
HTTP	1
TCP	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82	C:\Users\RDhJ0CNFevzX\Desktop\d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82.doc	Sample File	2261.96 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
c79bcf4cccfcac32f26c892f6196be3d299ceaa4dc157e633f73e470534b9f90	image2.png	Extracted File	250.21 KB	image/png	-	CLEAN
0d79507fbc5d3c1843f0584e92ffd8b8f2862b4ae569beb934963b30185e6489	image1.png	Extracted File	77.99 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\d66a64e64a1d1b44ebcc854f04b1e175ccc93b61fff0f093394f6dcdcd785d82.doc	Sample File, VM File	-	MALICIOUS
image1.png	-	-	CLEAN
ThisDocument	-	-	CLEAN
image2.png	-	-	CLEAN
c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\y8DFD.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\y8DFD.tmp.dll	Accessed File	Access, Create	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://45.8.146.139/fhfty/WM9BW2TQYMF_YV4HRQ4WA3K_5F-D0L5S/rm	-	45.8.146.139	-	-	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
45.8.146.139	-	Russia	TCP	SUSPICIOUS

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