MALICIOUS

Classifications: -
Threat Names: -
Verdict Reason: -

Sample Type	**RTF Document**
File Name	**New Order (MY 01-22-DTHI .doc.rtf**
ID	#5067132
MD5	ae55aaa571fd4f87839cb1ebc9706d32
SHA1	f7dab7f7f3556fe38a001dba46c9e93d4ffbf32b
SHA256	49235a707a23701651de637ce90e530247dcf6877001f416aa459a9bb0a22daa
File Size	10.94 KB
Report Created	2022-08-05 12:53 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (2 rules, 2 matches)

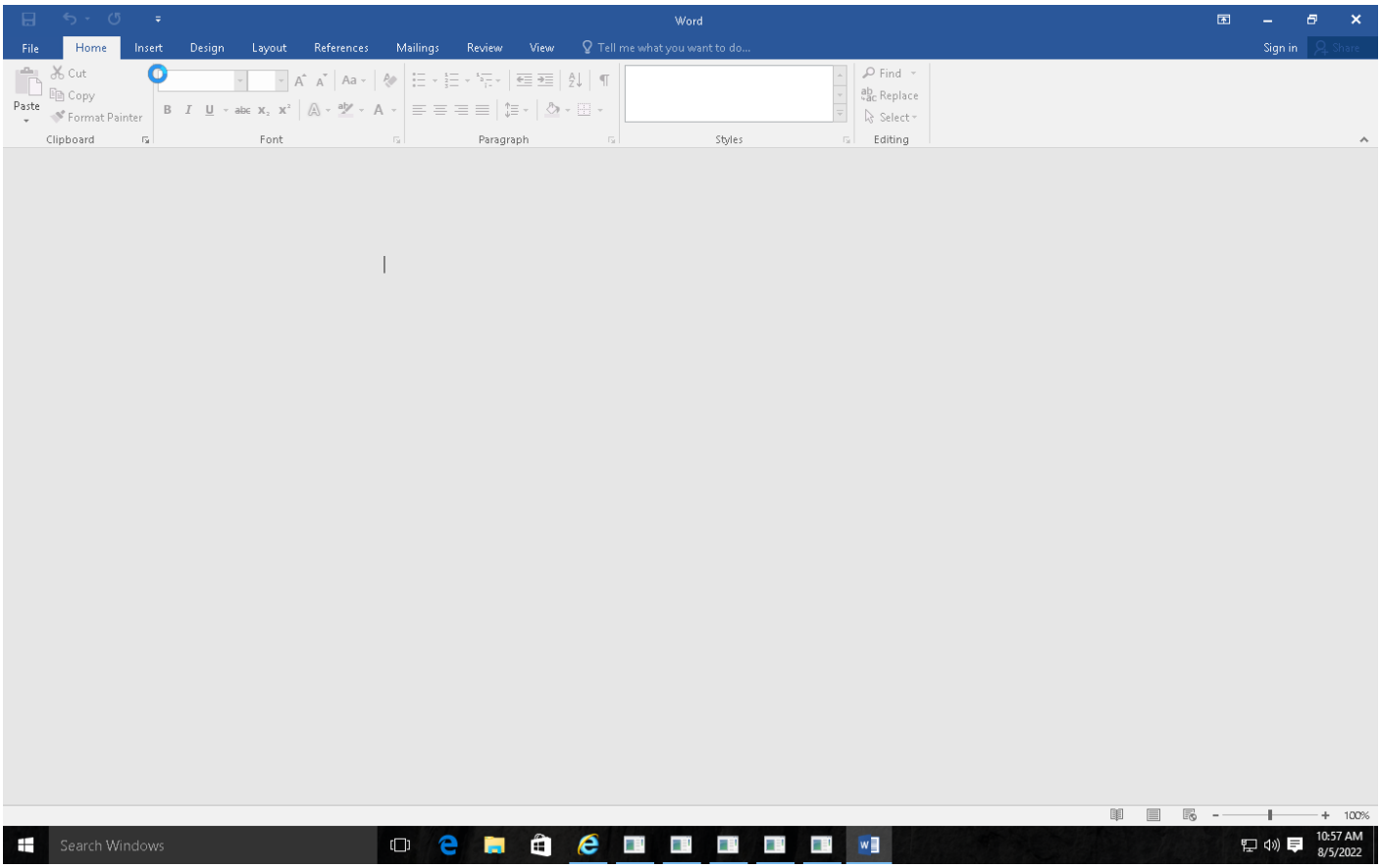
Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
4/5	YARA	Malicious content matched by YARA rules	1	-
	• Rule "RTF_Header_obfuscation" from ruleset "Malicious-Documents" has matched on the sample itself.			

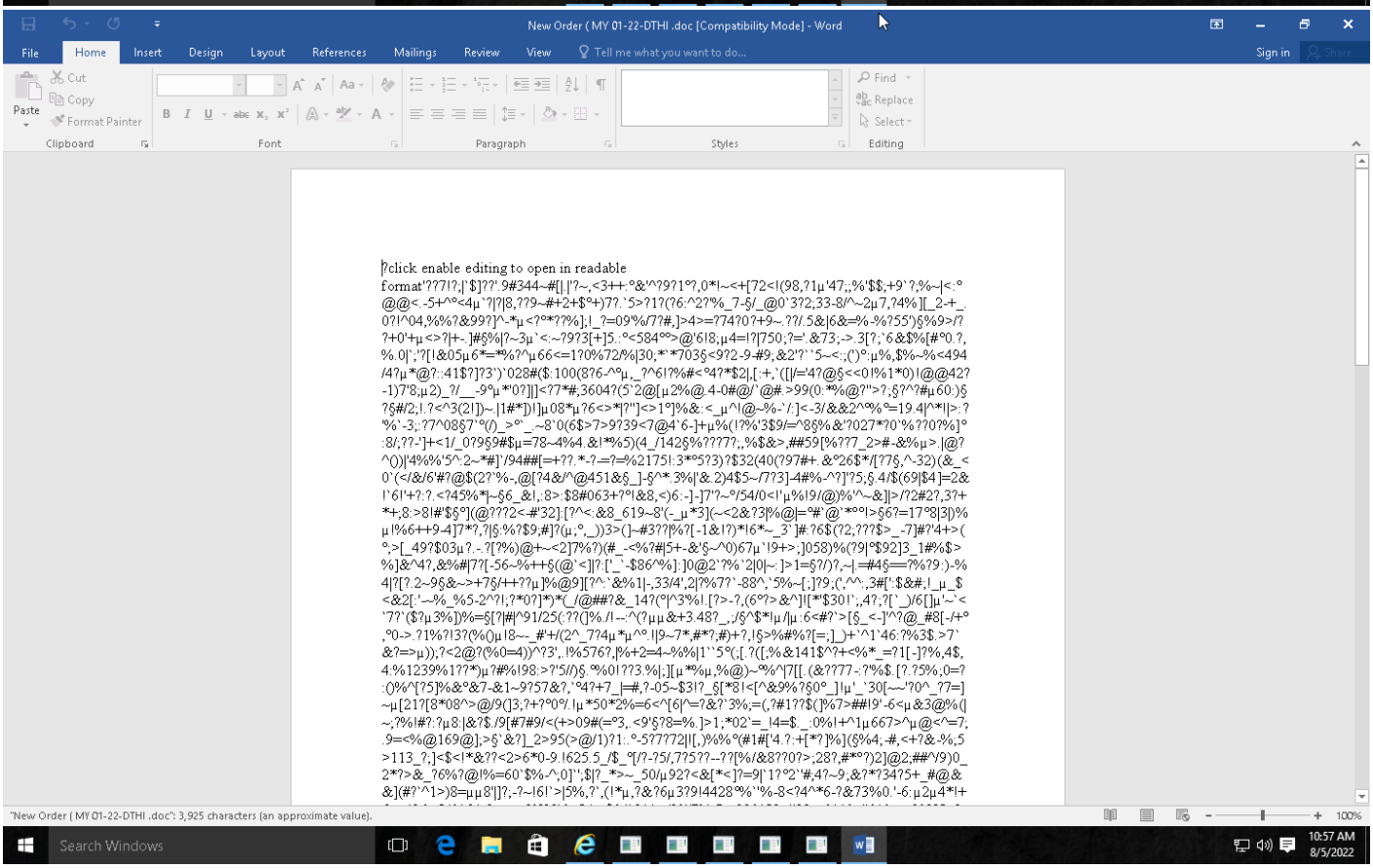
Sample Information

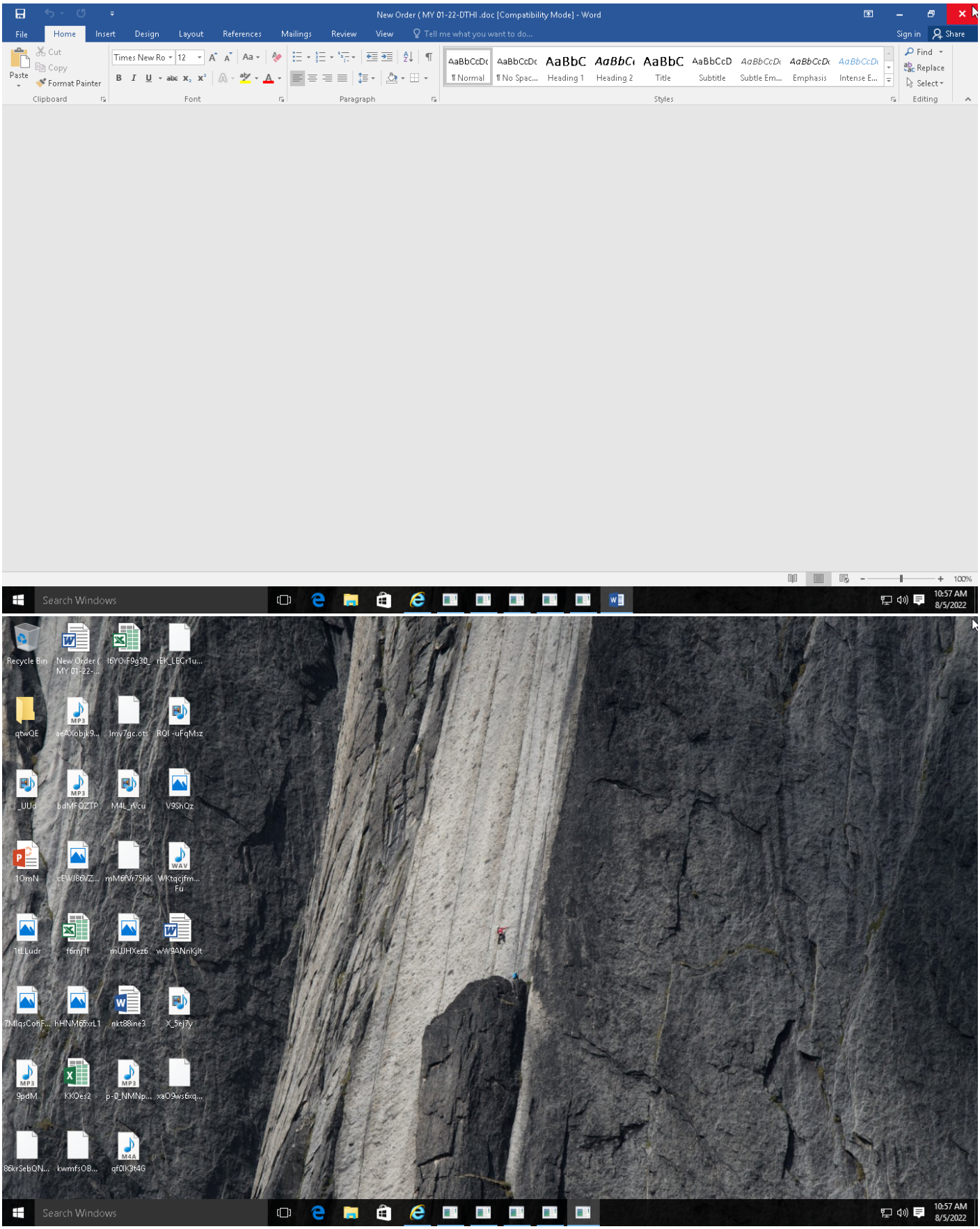
ID	#5067132
MD5	ae55aaa571fd4f87839cb1ebc9706d32
SHA1	f7dab7f7f3556fe38a001dba46c9e93d4ffbf32b
SHA256	49235a707a23701651de637ce90e530247dcf6877001f416aa459a9bb0a22daa
SSDeep	192:a6VFXWgf93ef3FZr2aZmnJfiMll+bZXe9uZwVtDvwFiNS+NS6CLcFS6s:a6VFXWgf93et0dJfVll+bZXe9uUFwEAd
File Name	New Order (MY 01-22-DTHI .doc.rtf
File Size	10.94 KB
Sample Type	RTF Document
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 12:53 (UTC+2)
Analysis Duration	00:03:37
Termination Reason	All processes terminated
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	1


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
Find
Replace
Select
Editing
Search Windows
10:57 AM
8/5/2022


New Order (MY 01-22-DTHI .doc [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
Find
Replace
Select
Editing
?click enable editing to open in readable
"New Order (MY 01-22-DTHI .doc": 3,925 characters (an approximate value).
Search Windows
10:57 AM
8/5/2022


New Order (MY 01-22-DTHI .doc [Compatibility Mode] - Word
Search Windows
Recycle Bin
Search Windows

NETWORK

General

92 bytes total sent

40 bytes total received

1 ports 445

1 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph

Process #1: 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: 59962, Reason: Analysis Target
Unmonitor End Time	End Time: 266977, Reason: Terminated
Monitor duration	207.01s
Return Code	0
PID	4564
Parent PID	1972
Bitness	32 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
49235a707a23701651de637ce90e530247dcf6877001f416aa459a9bb0a22daa	C:\Users\RDhJ0CNFevzX\Desktop\New Order (MY 01-22-DTHI .doc.rtf	Sample File	10.94 KB	text/rtf	-	MALICIOUS
3573c1372e6f6a9fe849037a393c653a5889524440839a72852825179c188e1b	UNKNOWN_1	Extracted File	1.55 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\New Order (MY 01-22-DTHI .doc.rtf	Sample File, VM File	-	MALICIOUS
UNKNOWN_1	-	-	CLEAN

Process

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

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malicious-Documents	RTF_Header_obfuscation	Malformed RTF header; commonly used to confuse analyzers	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\New Order (MY 01-22-DTHI .doc.rtf	-	4/5

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	4.6.1.14 / 2022-08-03 12:19:21
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