

MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	Word Document
File Name	23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab.doc
ID	#5127364
MD5	ee1d6eb5b07b99e65fc0cb477193c35c
SHA1	9d4dbf701c8ede93a79036dd5a0316da988a2eeb
SHA256	23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab
File Size	2288.31 KB
Report Created	2022-08-11 20:48 (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	-
<ul style="list-style-type: none"> • (Process #1) winword.exe connects to http://45.8.146.139/fhfy/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1I/-f. 				
4/5	Reputation	Known malicious file	1	-
<ul style="list-style-type: none"> • Reputation analysis labels the sample itself as Mal/Generic-S. 				
2/5	Execution	Executes macro on specific event	1	-
<ul style="list-style-type: none"> • Executes macro automatically on target "document" and event "open". 				
1/5	Execution	Contains suspicious Office macro	1	-
<ul style="list-style-type: none"> • Office document contains a suspicious VBA macro. 				

Mitre ATT&CK Matrix

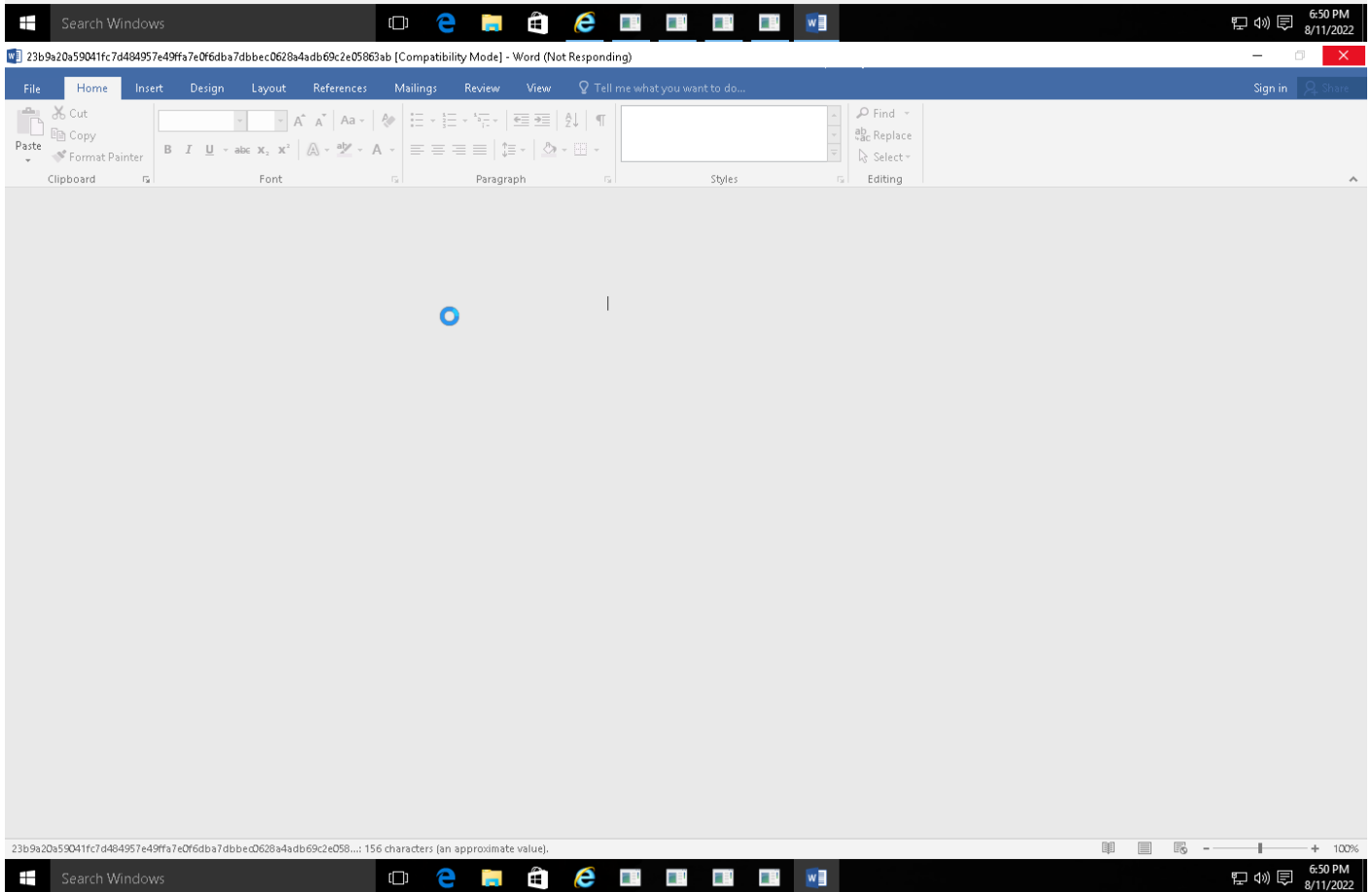
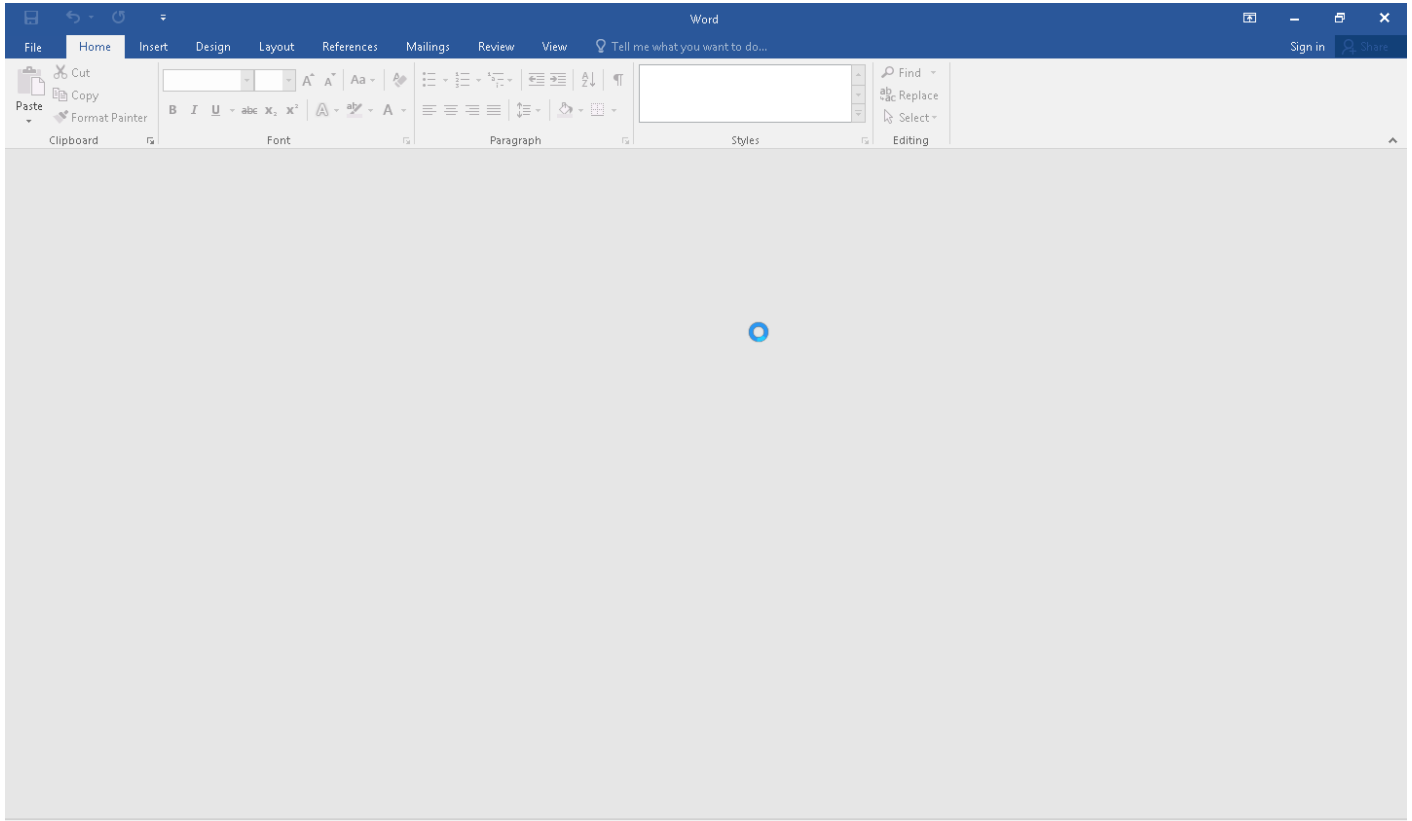
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1064 Scripting					#T1071 Standard Application Layer Protocol		

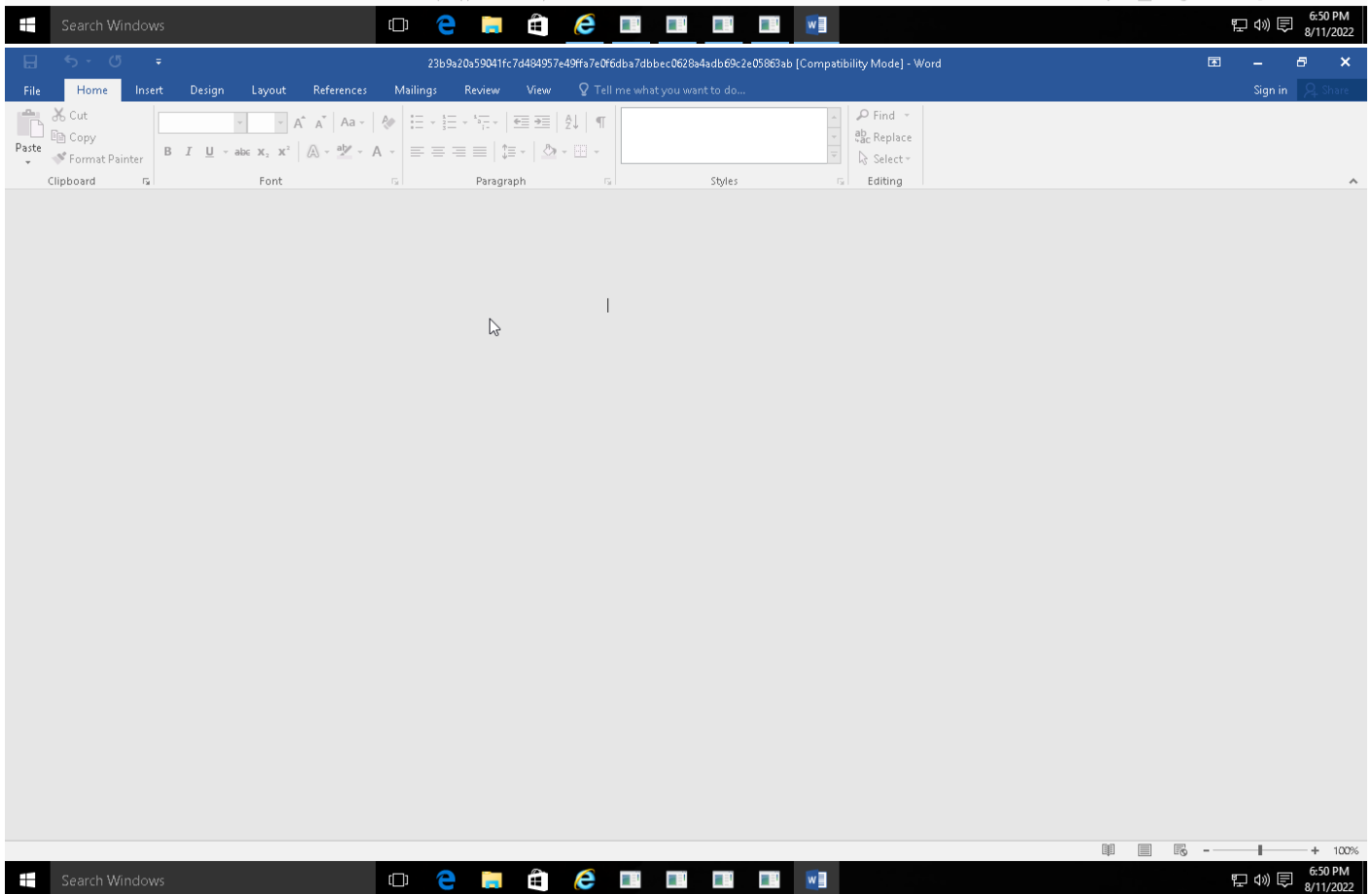
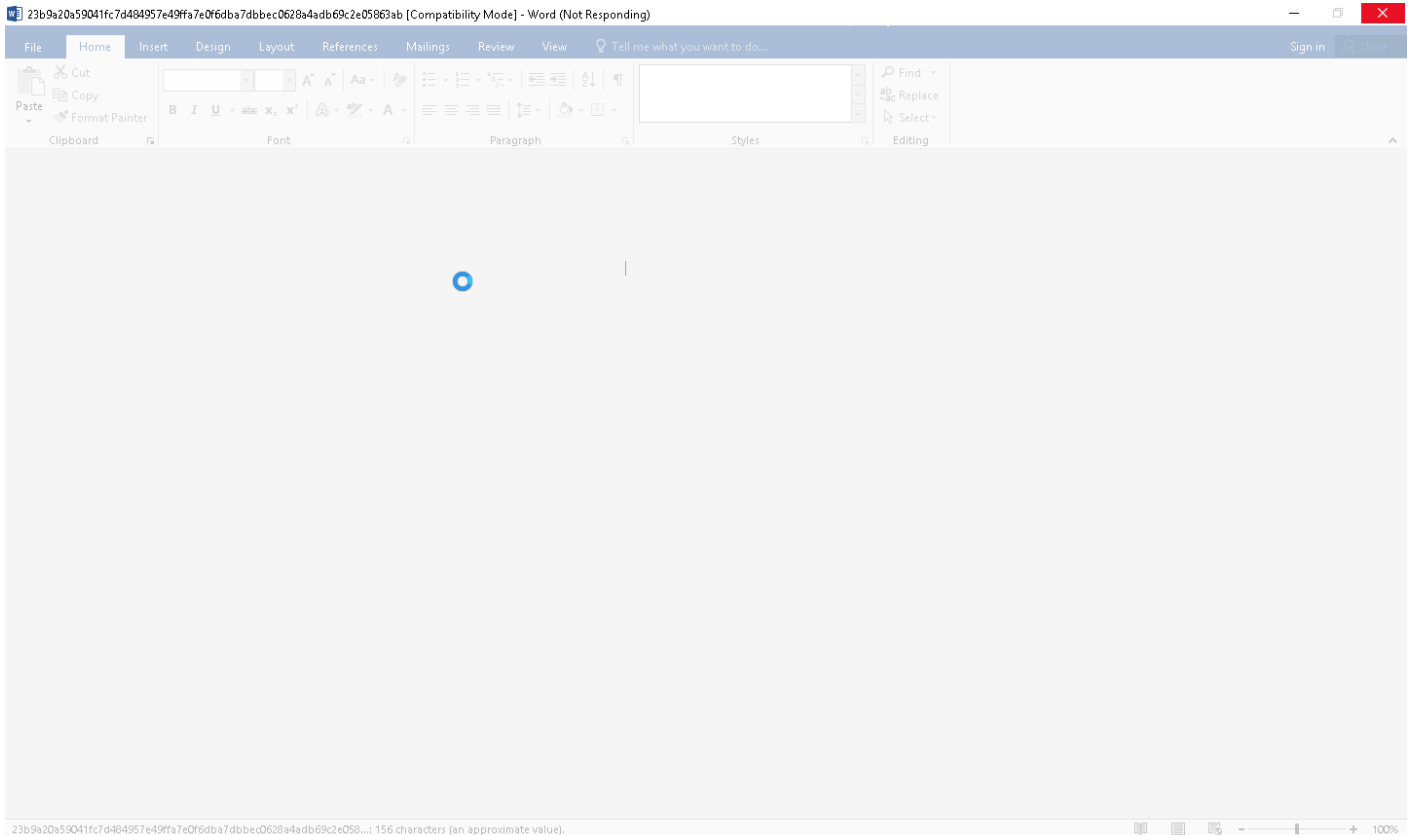
Sample Information

ID	#5127364
MD5	ee1d6eb5b07b99e65fc0cb477193c35c
SHA1	9d4dbf701c8ede93a79036dd5a0316da988a2eeb
SHA256	23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab
SSDeep	49152:xyG/bJ98ozhp4kBA4Y0bRfqmIYOxtKW72swnql:QS8otukBbRfqUjRy7T
File Name	23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab.doc
File Size	2288.31 KB
Sample Type	Word Document
Has Macros	✓

Analysis Information

Creation Time	2022-08-11 20:48 (UTC+2)
Analysis Duration	00:04:07
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





Screenshots truncated

NETWORK

General

805 bytes total sent

794 bytes total received

2 ports 80, 445

2 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, 725 bytes sent, 634 bytes received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://45.8.146.139/fhfty/NH1-X8NL7CO4_YNJ-MEFY7BW9QYIJW1i/-f	-	-		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: 67429, Reason: Analysis Target
Unmonitor End Time	End Time: 314590, Reason: Terminated by timeout
Monitor duration	247.16s
Return Code	Unknown
PID	4328
Parent PID	1972
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
-	201 bytes	469501f44d054081ad49d1d0ab0b8031ecce6986d17d346cc39dfb7bcf327f76	✘
C:\Users\RDhJ0C~1\AppData\Local\Temp\B2B4.tmp	0 bytes	e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855	✘

Host Behavior

Type	Count
Module	82
Keyboard	67
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
	23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab	C:\Users\RDHJ0CNFevz\X\Desktop\23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab.doc	Sample File	2288.31 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	MALICIOUS
	131b8a928d925e1a7eaa188384bd499856749db1523d310516079162cecd2368	image1.png	Extracted File	104.48 KB	image/png	-	CLEAN
	da16ea1eb023c9781b993946f2ecc7989eb7e698784f0db9d62cc2d1c467d43b	image2.png	Extracted File	249.95 KB	image/png	-	CLEAN
	c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	-	Modified File	128 bytes	application/octet-stream	-	CLEAN
	469501f44d054081ad49d1d0ab0b8031ecce6986d17d346cc39dfb7bcf327f76	C:\Users\RDHJ0C~1\AppData\Local\Temp\B2B4.tmp.dll	Downloaded File	201 bytes	text/html	Access, Create, Read	CLEAN

Filename	File Name	Category	Operations	Verdict
	C:\Users\RDHJ0CNFevz\X\Desktop\23b9a20a59041fc7d484957e49ffa7e0f6dba7dbbec0628a4adb69c2e05863ab.doc	Sample File, VM File	-	MALICIOUS
	C:\Users\RDHJ0C~1\AppData\Local\Temp\B2B4.tmp.dll	Accessed File, Downloaded File, Extracted File	Access, Create, Read	CLEAN
	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE	Accessed File	Access	CLEAN
	C:\Users\RDHJ0C~1\AppData\Local\Temp\B2B4.tmp	Dropped File, Accessed File, Not Extracted	Access, Create, Delete	CLEAN
	c:\users\rdhj0cnfevz\appdata\local\microsoft\windows\inetcache\ie\htx5vgwpl-f[1].htm	Downloaded File, Extracted File	-	CLEAN
	c:\users\rdhj0cnfevz\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	-	CLEAN
	image2.png	-	-	CLEAN
	ThisDocument	-	-	CLEAN
	image1.png	-	-	CLEAN

URL	URL	Category	IP Address	Country	HTTP Methods	Verdict
	http://45.8.146.139/fhfy/NH1-X8NL7CO4_YNJ-MEFY7BW9QYJW1/-f	-	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
