MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Word Document**
File Name	**7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027.doc**
ID	#5378872
MD5	7e8133cf5f56adcfafb9bc91390c9fe7
SHA1	2cc6471245901e51565ad69df6b8586629965cf1
SHA256	7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027
File Size	252.54 KB
Report Created	2022-09-12 18:11 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (4 rules, 12 matches)

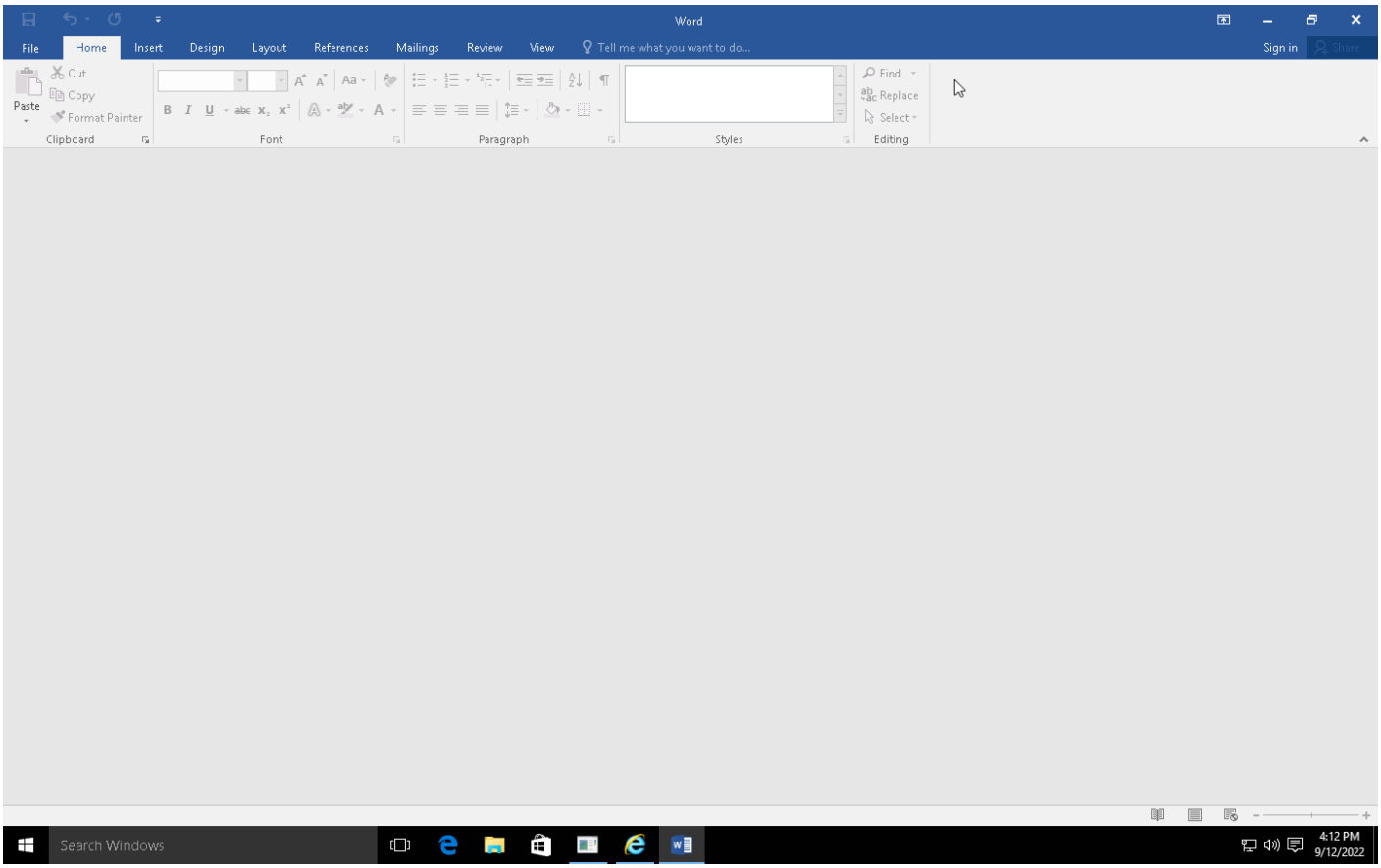
Score	Category	Operation	Count	Classification
4/5	Reputation	Known malicious file	2	-
	• Reputation analysis labels embedded file "" as Mal/Generic-S. • Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Execution	Document tries to create process	8	-
	• Document creates (process #5) javaw.exe. • Document creates (process #6) javaw.exe. • Document creates (process #7) javaw.exe. • Document creates (process #10) javaw.exe. • Document creates (process #11) javaw.exe. • Document creates (process #12) javaw.exe. • Document creates (process #3) javaw.exe. • Document creates (process #4) javaw.exe.			
1/5	Heuristics	Contains suspicious meta data	1	-
	• Office document contains below average content data.			
1/5	Heuristics	Contains known suspicious class identifier	1	-
	• Office document contains known suspicious class identifier for ActiveX object "Packager6" (CLSID {F20DA720-C02F-11CE-927B-0800095AE340}).			

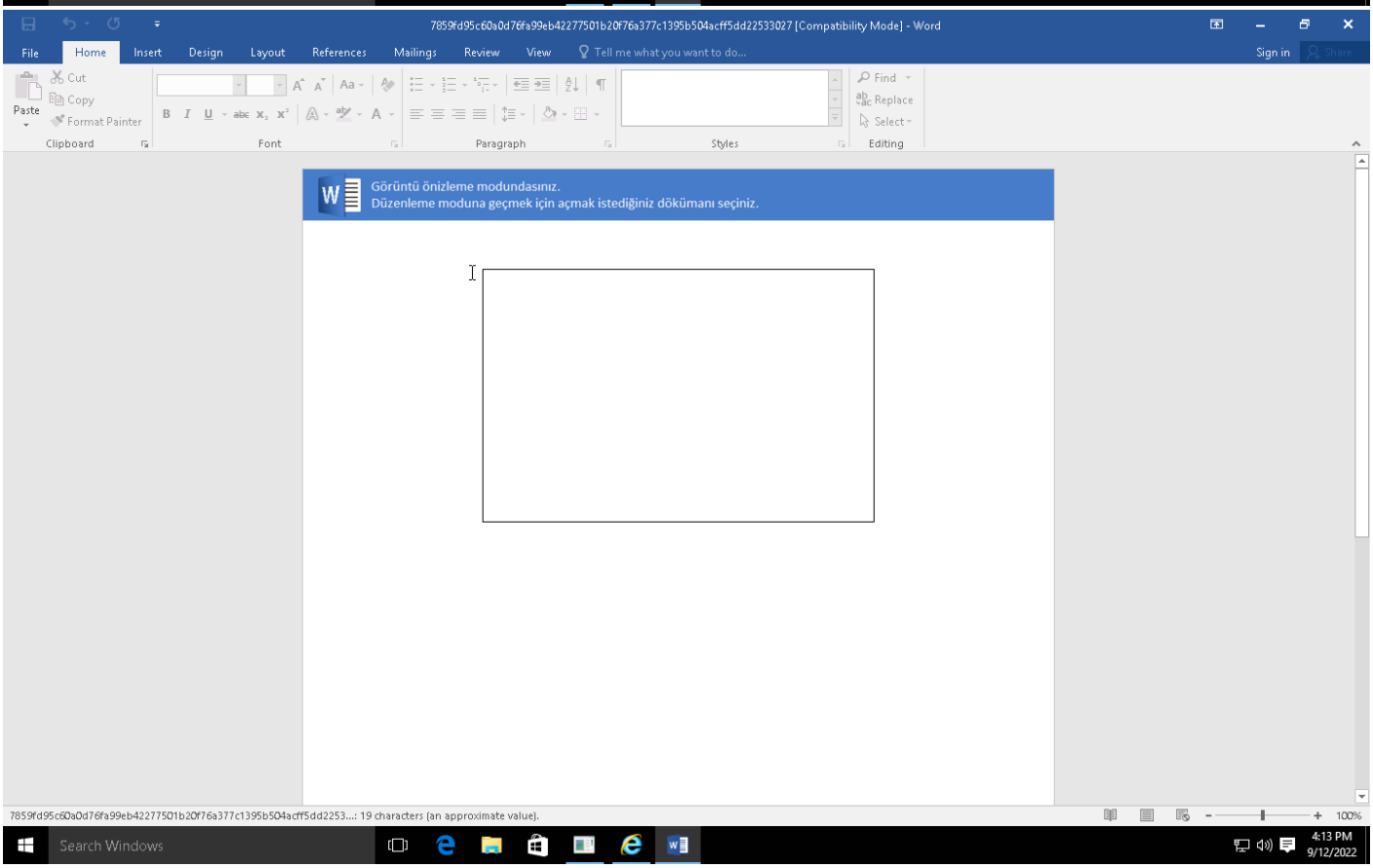
Sample Information

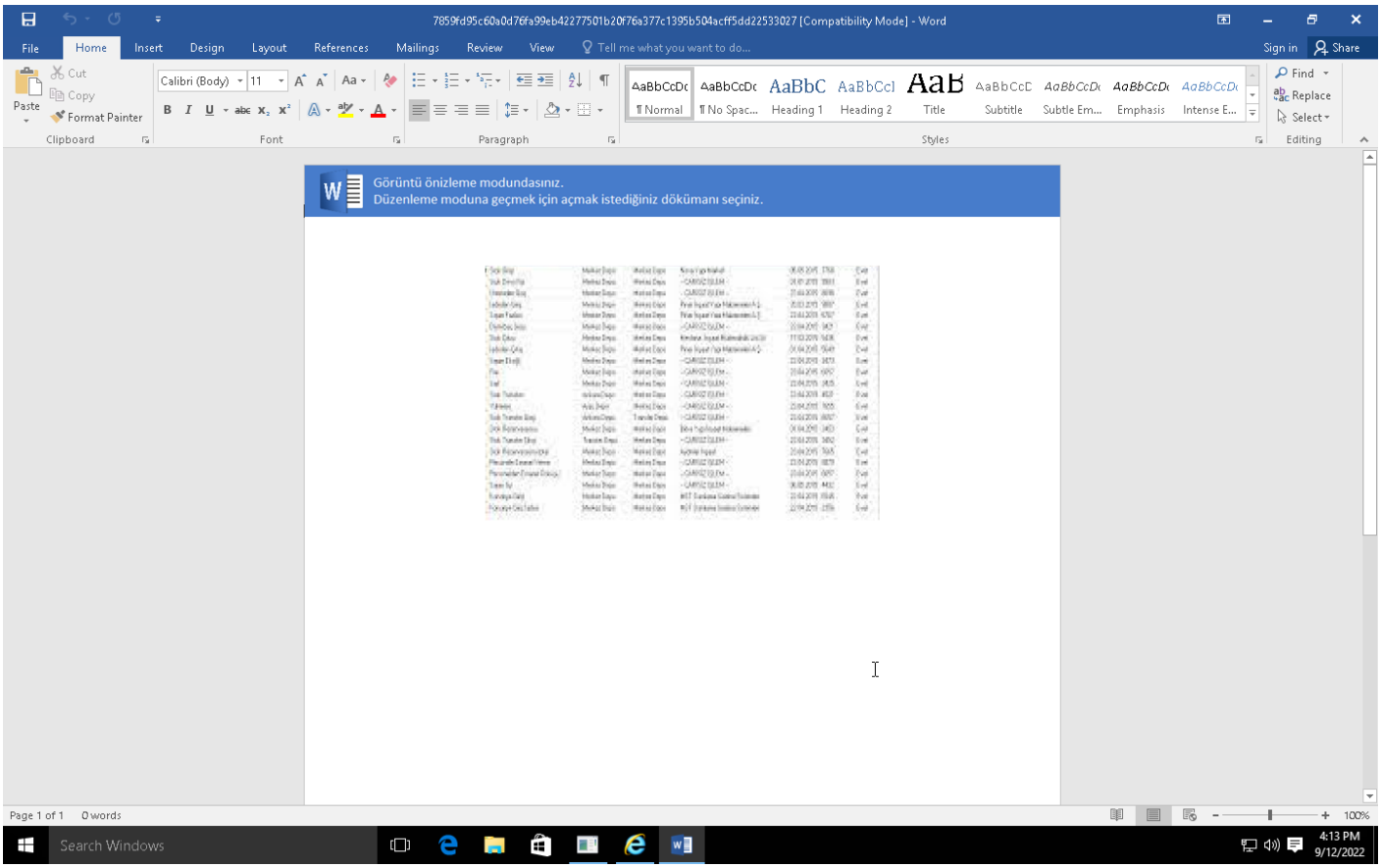
ID	#5378872
MD5	7e8133cf5f56adcfafb9bc91390c9fe7
SHA1	2cc6471245901e51565ad69df6b8586629965cf1
SHA256	7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027
SSDeep	6144:CsjU1vruW+UztmXtb2wDayQ7B4Y6/EcKbiCW:tjaumMXtb2w+yM4YhVWCW
File Name	7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027.doc
File Size	252.54 KB
Sample Type	Word Document
Has Macros	✔

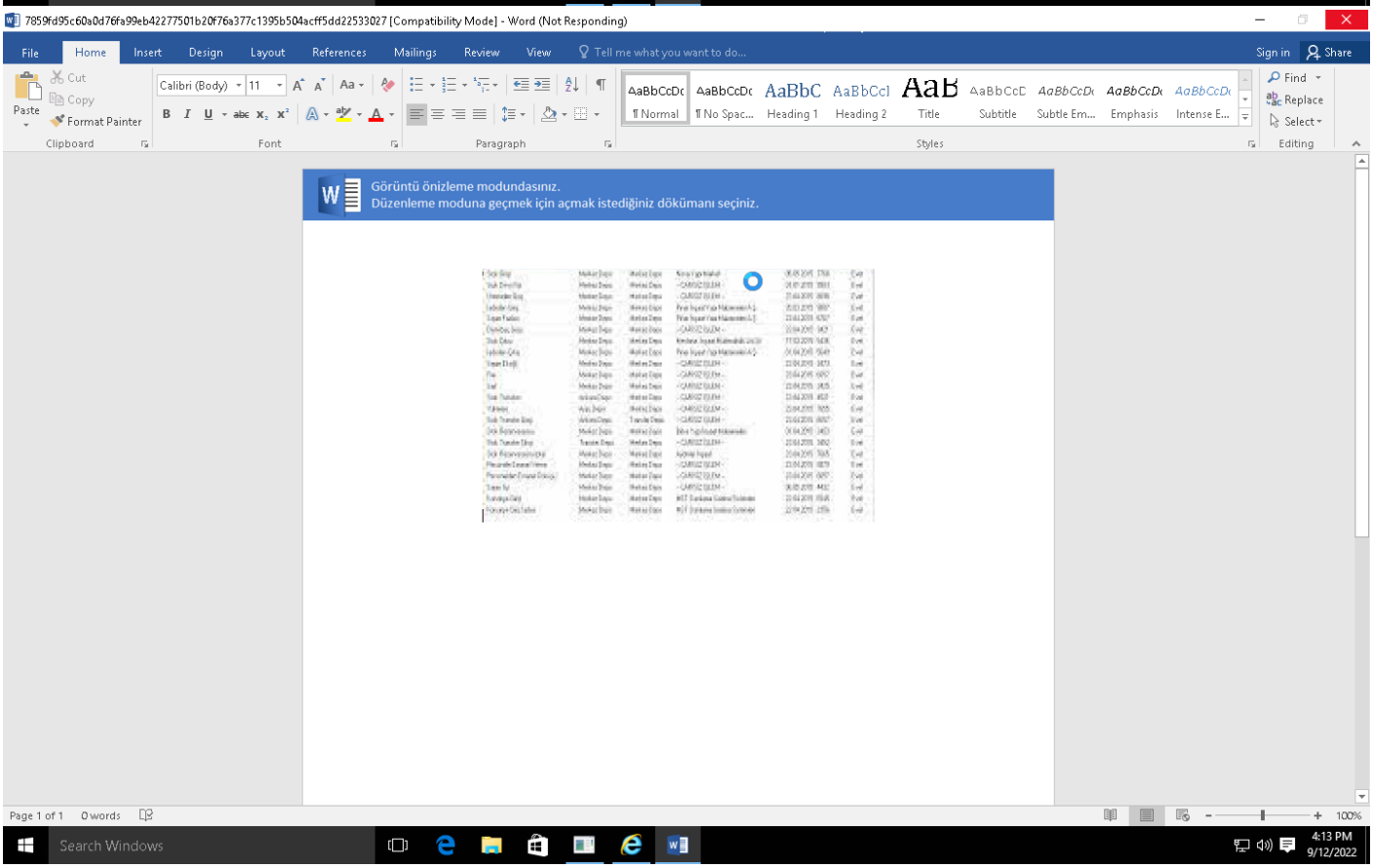
Analysis Information

Creation Time	2022-09-12 18:11 (UTC+2)
Analysis Duration	00:04:07
Termination Reason	Timeout
Number of Monitored Processes	11
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
Find
Replace
Select
Editing
Search Windows
4:12 PM
9/12/2022


7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027 [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
Görüntü önizleme modundasınız.
Düzenleme moduna geçmek için açmak istediğiniz dökümanı seçiniz.
7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd2253...: 19 characters (an approximate value).
100%
Search Windows
4:13 PM
9/12/2022





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 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

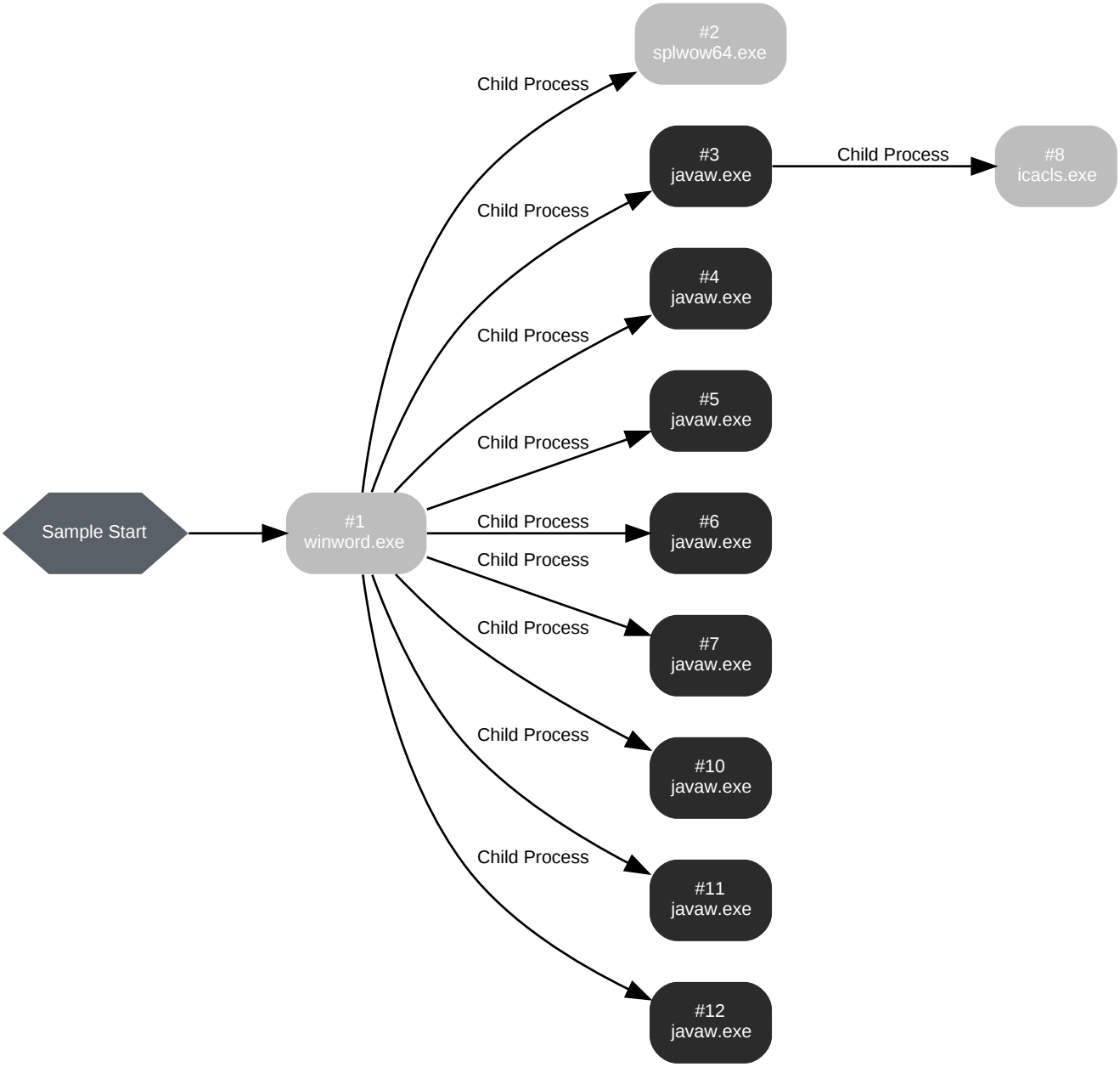
HTTP/S

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: 73067, Reason: Analysis Target
Unmonitor End Time	End Time: 292584, Reason: Terminated
Monitor duration	219.52s
Return Code	0
PID	4748
Parent PID	1648
Bitness	32 Bit

Process #2: splwow64.exe

ID	2
File Name	c:\windows\splwow64.exe
Command Line	C:\Windows\splwow64.exe 8192
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 106261, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	214.88s
Return Code	Unknown
PID	5072
Parent PID	4748
Bitness	64 Bit

Process #3: javaw.exe

ID	3
File Name	c:\program files\java\jre1.8.0_171\bin\javaw.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 135155, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	185.98s
Return Code	Unknown
PID	4108
Parent PID	4748
Bitness	64 Bit

Dropped Files (8)

File Name	File Size	SHA256	YARA Match
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	51 bytes	62739458c97ae85da3ab1ebaa2a5a933a023e4db1449721b0ddb5197b8f544d5	✖
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	51 bytes	96c04e91c9a10f7826312dacac99b06503ddd78a3d5bd3df9b1db2fa31b7efbc	✖
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	51 bytes	9a3b5534bc25907d62f2c1dda5fccb7d00b99e17e70235ebb295503247aeb064	✖
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	51 bytes	a3ef479dfa0b4bfbe9452abb54d78f793e13e763875a613f4b6feefd30030c4f	✖
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	51 bytes	f37a29162697c3d4550b44ef5f71173b0e450b72e09982f67be01e5eeb036a27	✖
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	51 bytes	8e692844e4658fb423719372ffc00068c4a93f3419606e1b5b622a741d066df7	✖
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	51 bytes	a80a1af1f1cc56a7d465109793c676bc1dac9e4f9e1024cec67b41fbcb1dd691	✖
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	51 bytes	0b17a708a9568dc454ad105a8d1a165f470215dc50320f66a8e9d0aaa514cca0	✖

Host Behavior

Type	Count
System	13
File	1786
Module	10
Environment	6
-	4
Process	1

Process #4: javaw.exe

ID	4
File Name	c:\program files\java\jre1.8.0_171\bin\javaw.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 147903, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	173.24s
Return Code	Unknown
PID	2756
Parent PID	4748
Bitness	64 Bit

Host Behavior

Type	Count
System	13
File	2035
Module	10
Environment	4

Process #5: javaw.exe

ID	5
File Name	c:\program files\java\jre1.8.0_171\bin\javaw.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 158607, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	162.53s
Return Code	Unknown
PID	3228
Parent PID	4748
Bitness	64 Bit

Host Behavior

Type	Count
System	13
File	1954
Module	8
Environment	4

Process #6: javaw.exe

ID	6
File Name	c:\program files\java\jre1.8.0_171\bin\javaw.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 168370, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	152.77s
Return Code	Unknown
PID	3164
Parent PID	4748
Bitness	64 Bit

Host Behavior

Type	Count
System	13
File	1839
Module	10
Environment	4

Process #7: javaw.exe

ID	7
File Name	c:\program files\java\jre1.8.0_171\bin\javaw.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 182289, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	138.85s
Return Code	Unknown
PID	3316
Parent PID	4748
Bitness	64 Bit

Host Behavior

Type	Count
System	13
File	1437
Module	8
Environment	4

Process #8: icacls.exe

ID	8
File Name	c:\windows\system32\icacls.exe
Command Line	C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant "everyone":(OI)(CI)M
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 192653, Reason: Child Process
Unmonitor End Time	End Time: 217658, Reason: Terminated
Monitor duration	25.00s
Return Code	0
PID	4268
Parent PID	4108
Bitness	64 Bit

Process #10: javaw.exe

ID	10
File Name	c:\program files\java\jre1.8.0_171\bin\javaw.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 194818, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	126.32s
Return Code	Unknown
PID	3084
Parent PID	4748
Bitness	64 Bit

Host Behavior

Type	Count
System	13
File	1341
Module	10
Environment	4

Process #11: javaw.exe

ID	11
File Name	c:\program files\java\jre1.8.0_171\bin\javaw.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 198565, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	122.57s
Return Code	Unknown
PID	4340
Parent PID	4748
Bitness	64 Bit

Host Behavior

Type	Count
System	13
File	1362
Module	10
Environment	4

Process #12: javaw.exe

ID	12
File Name	c:\program files\java\jre1.8.0_171\bin\javaw.exe
Command Line	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Documents\
Monitor Start Time	Start Time: 212016, Reason: Child Process
Unmonitor End Time	End Time: 321139, Reason: Terminated by timeout
Monitor duration	109.12s
Return Code	Unknown
PID	1388
Parent PID	4748
Bitness	64 Bit

Host Behavior

Type	Count
System	13
File	1266
Module	10
Environment	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
543eb377d95104a39c65e164349fc94ce5fe2cd515ff1d9a5e2e9ec4e8473348	oleObject1.bin	Extracted File	165.50 KB	application/CDFV2	-	MALICIOUS
7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027	C:\Users\RDhJ0CNFevzX\Desktop\7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027.doc	Sample File	252.54 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	MALICIOUS
62739458c97ae85da3ab1eaa2a5a933a023e4db1449721b0ddb5197b8f544d5	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File	51 bytes	text/plain	Access, Create, Write	CLEAN
96c04e91c9a10f7826312dacac99b06503ddd78a3d5bd3df9b1db2fa31b7efbc	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File	51 bytes	text/plain	Access, Create, Write	CLEAN
9a3b5534bc25907d62f2c1dda5fccb7d00b99e17e70235ebb295503247aeb064	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File	51 bytes	text/plain	Access, Create, Write	CLEAN
a3ef479dfa0b4bfbe9452abb54d78f793e13e763875a613f4b6feefd30030c4f	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File	51 bytes	text/plain	Access, Create, Write	CLEAN
f37a29162697c3d4550b44ef5f71173b0e450b72e09982f67be01e5eeb036a27	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File	51 bytes	text/plain	Access, Create, Write	CLEAN
8e692844e4658fb423719372ffc00068c4a93f3419606e1b5b622a741d066df7	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File	51 bytes	text/plain	Access, Create, Write	CLEAN
a1566d12b7bee123511040635ae34d71e23ae1f73706347eb5926a61ab72bdb7	image2.png	Extracted File	67.28 KB	image/png	-	CLEAN
a80a1af1f1cc56a7d465109793c676bc1dac9e4f9e1024cec67b41fbcb1dd691	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File	51 bytes	text/plain	Access, Create, Write	CLEAN
67ba24dd3354c3e058b032fbaf799d9f0d11fd35fa9b80a9dedaa3abffe32893	image1.PNG	Extracted File	8.77 KB	image/png	-	CLEAN
8cb74bd01205df1e777cc8c1a343aa65287909cd72aa7b8388f4c32024dce624	a0v2H8.jar	Extracted File	160.62 KB	application/java-archive	-	CLEAN
0b17a708a9568dc454ad105a8d1a165f470215dc50320f66a8e9d0aaa514cca0	C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File	51 bytes	text/plain	Access, Create, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\7859fd95c60a0d76fa99eb42277501b20f76a377c1395b504acff5dd22533027.doc	Sample File, VM File	-	MALICIOUS
C:\Program Files\Java\jre1.8.0_171\lib\meta-index	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\bin\zip.dll	Accessed File	Access	CLEAN
a0v2H8.jar	-	-	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunec.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\sunrsasign.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\zipfs.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\classes	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
oleObject1.bin	-	-	CLEAN
C:\Windows\Sun\Java\lib\ext	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\resources.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\jaccess.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunpkcs11.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\management\usagetracker.properties	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\charsets.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\dnsns.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunmscapi.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\jfxrt.jar	Accessed File	Access	CLEAN
C:\ProgramData\Oracle\Java\.oracle_jre_usage\17dfc292991c7ca0.timestamp	Dropped File, Accessed File	Access, Create, Write	CLEAN
C:\ProgramData\Oracle\Java\usagetracker.properties	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\jsse.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171	Accessed File	Access	CLEAN
C:\ProgramData\Oracle\Java\.oracle_jre_usage	Accessed File	Access, Create	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\jfr.jar	Accessed File	Access	CLEAN
C:\Windows\Sun\Java\lib\ext\meta-index	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\jce.jar	Accessed File	Access	CLEAN
image2.png	-	-	CLEAN
C:\Program Files\Java\jre1.8.0_171\meta-index	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\cldrdata.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\bin\server\jvm.dll	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\rt.jar	Accessed File	Access, Read	CLEAN
C:\Windows\system32\icacls.exe	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\meta-index	Accessed File	Access, Read	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\sunjce_provider.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\access-bridge-64.jar	Accessed File	Access	CLEAN
image1.PNG	-	-	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\nashorn.jar	Accessed File	Access	CLEAN
C:\Program Files\Java\jre1.8.0_171\lib\ext\localedata.jar	Accessed File	Access	CLEAN

Process

Process Name	Commandline	Verdict
javaw.exe	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"	CLEAN

Process Name	Commandline	Verdict
javaw.exe	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"	CLEAN
javaw.exe	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"	CLEAN
icacls.exe	C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant "everyone":(OI)(CI)M	CLEAN
javaw.exe	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"	CLEAN
javaw.exe	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"	CLEAN
javaw.exe	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"	CLEAN
winword.exe	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n	CLEAN
splwow64.exe	C:\Windows\splwow64.exe 8192	CLEAN
javaw.exe	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"	CLEAN
javaw.exe	"C:\Program Files\Java\jre1.8.0_171\bin\javaw.exe" -jar "C:\Users\RDHJ0C~1\AppData\Local\Temp\a0v2H8.jar"	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	4.6.1.22 / 2022-09-02 16:24:37
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.20 / 2022-08-26 12:47:07
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.22 / 2022-09-02 16:24:37
YARA Built-in Ruleset Version	4.6.1.20

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	8.0.1710.11

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