MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Word Document**
File Name	**ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0.doc**
ID	#3210555
MD5	7044bd240219ec2f83b01c532e2ce5ba
SHA1	745cdbc4a826c5960eef3f4a9aa307ff94e4b7fb
SHA256	ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0
File Size	77.50 KB
Report Created	2021-12-31 13:49 (UTC+1)
Target Environment	win7_64_sp1_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (9 rules, 9 matches)

Score	Category	Operation	Count	Classification
4/5	Masquerade	Creates a new process from a system binary	1	-
	• (Process #1) winword.exe creates a new explorer.exe process.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as "Mal/Generic-S".			
4/5	Heuristics	Document tries to trick users into running macros	1	-
	• Extracted text from an image embedded in C:\Users\kEecfMwgj\Desktop\ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0.doc suggests enabling macros.			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #2) explorer.exe.			
4/5	Network Connection	Attempts to connect through HTTP	1	-
	• (Process #4) mshta.exe connects to "http://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYlaSBt0KLfMB9kXwZBv6ZpTs... ...ErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcYCjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0".			
2/5	Execution	Office macro uses an execute function	1	-
	• Office macro uses the exec function.			
2/5	Execution	Executes macro on specific event	1	-
	• Executes macro automatically on target "document" and event "open".			
1/5	Heuristics	Contains suspicious meta data	1	-
	• Office document contains below average content data.			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			

Mitre ATT&CK Matrix

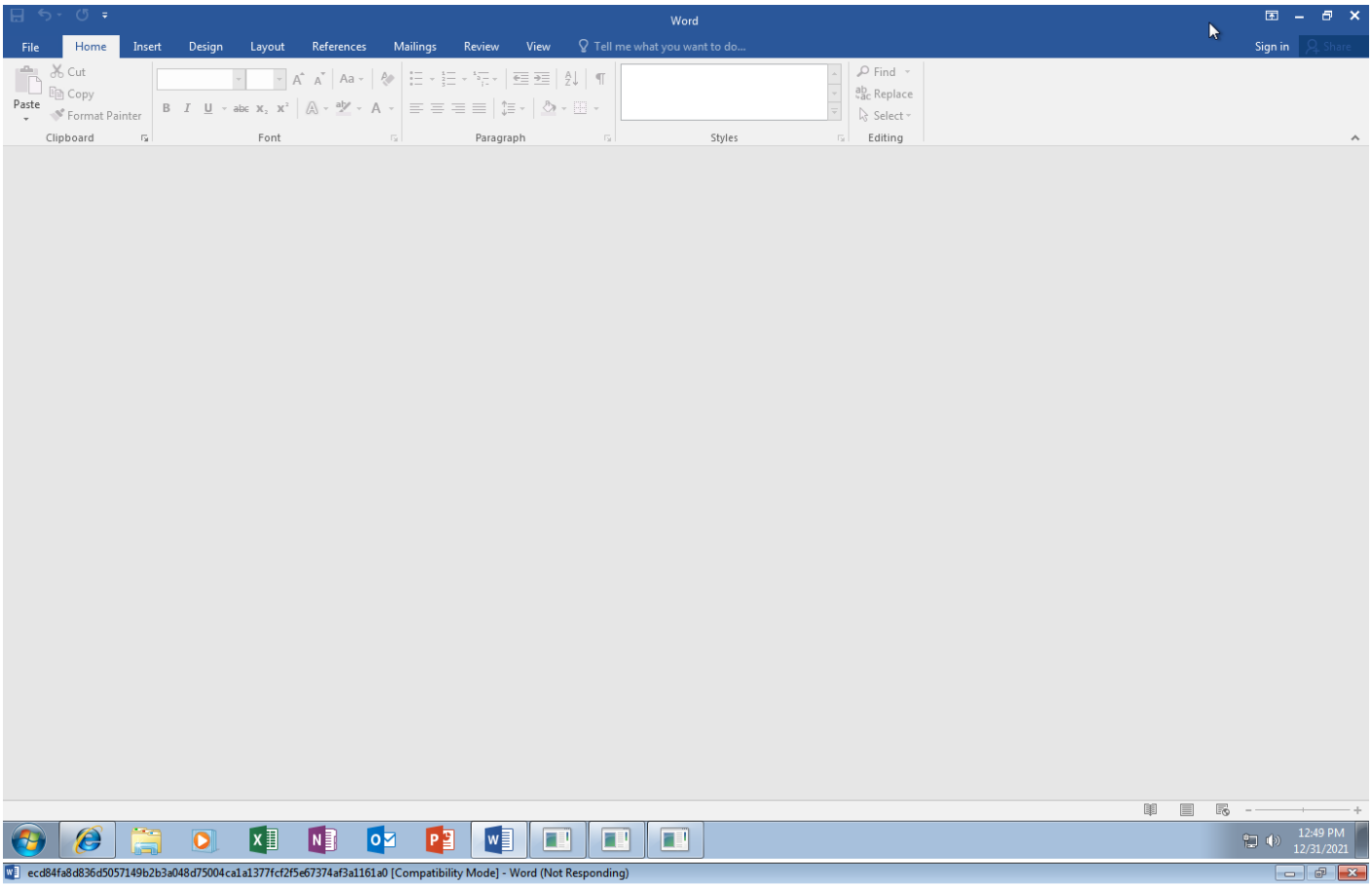
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1064 Scripting			#T1064 Scripting					#T1071 Standard Application Layer Protocol		

Sample Information

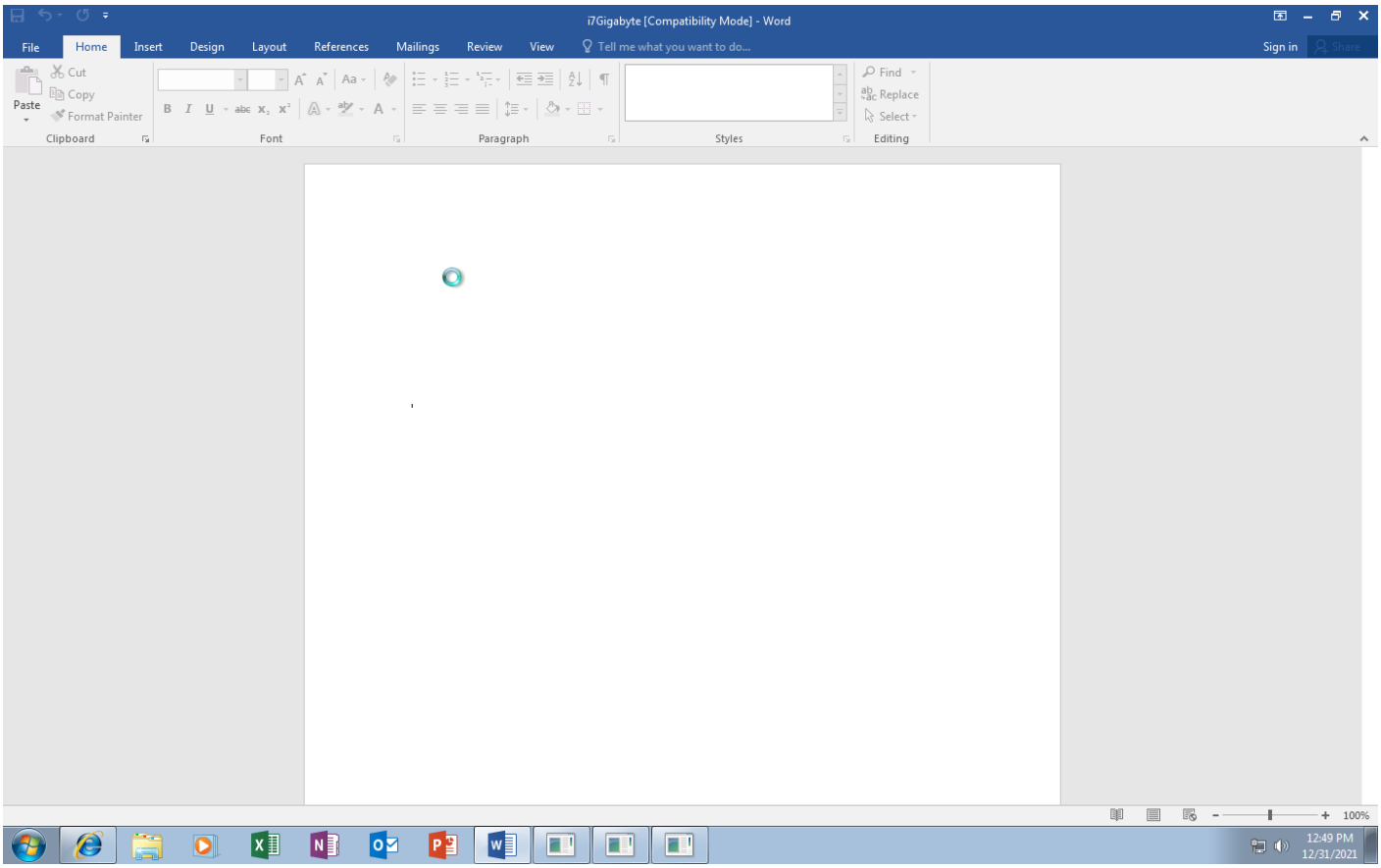
ID	#3210555
MD5	7044bd240219ec2f83b01c532e2ce5ba
SHA1	745cdbc4a826c5960eef3f4a9aa307ff94e4b7fb
SHA256	ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0
SSDeep	768:P/MMM1tMFur3Be1l3Jeq1awypEuqjuy+uqezc1GFZIdJ6jtQlQNBOTHxPlz/tZj8:Zja8ldPhW/jTEQMiebld4Kkd6t
File Name	ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0.doc
File Size	77.50 KB
Sample Type	Word Document
Has Macros	✓

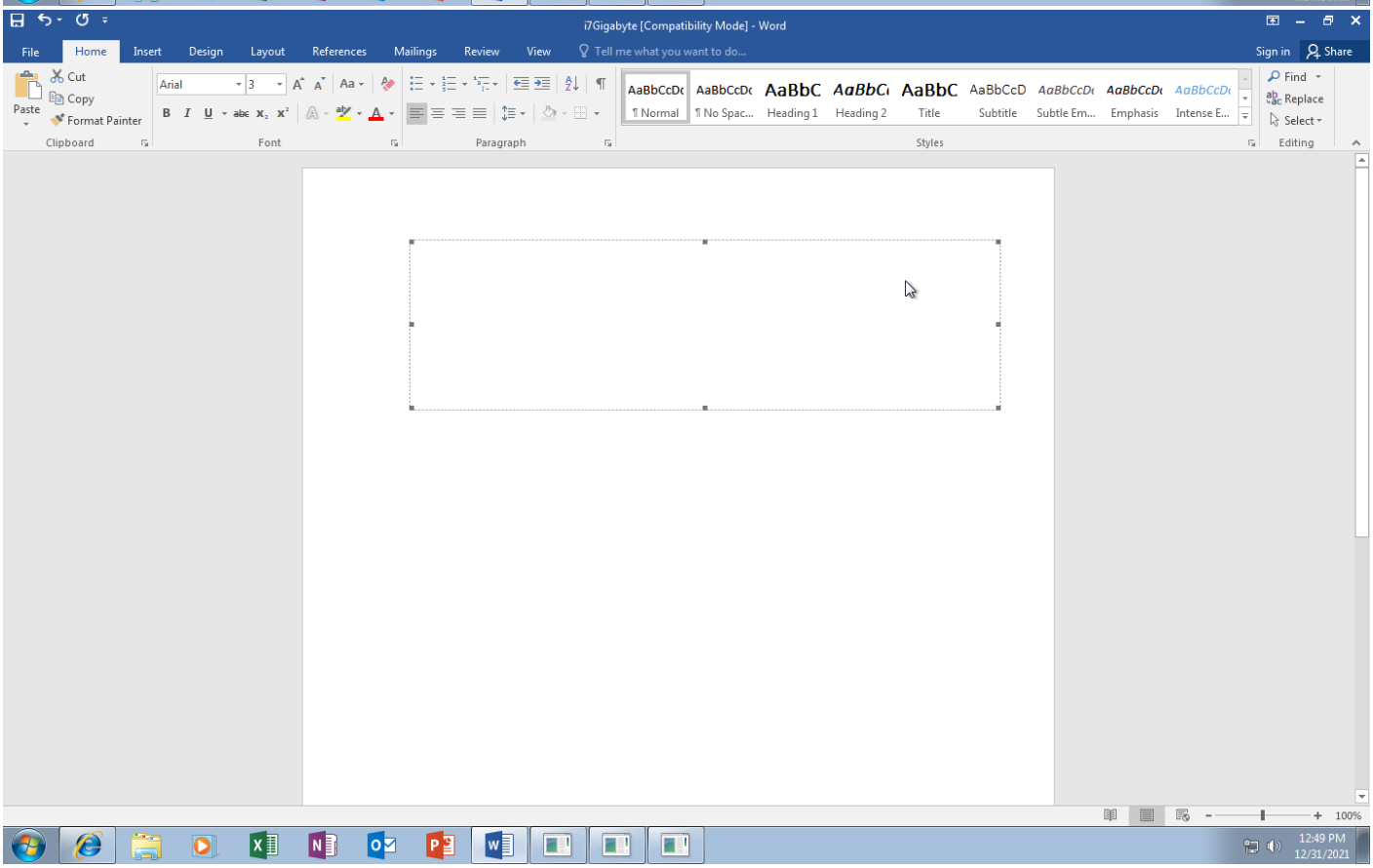
Analysis Information

Creation Time	2021-12-31 13:49 (UTC+1)
Analysis Duration	00:04:05
Termination Reason	Timeout
Number of Monitored Processes	5
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
12:49 PM
12/31/2021
ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0 [Compatibility Mode] - Word (Not Responding)


12:49 PM
12/31/2021





Screenshots truncated

NETWORK

General

841 bytes total sent

597 bytes total received

1 ports 80

1 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 841 bytes sent, 597 bytes received

HTTP Requests

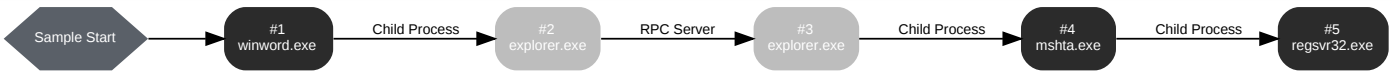
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYlaSBt0KLfMB9kXwZBv6ZpTsny6/qAhlQjrAaLKJeTLQnbCarASpMADNe9u1... ...1XErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcYCjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	patelboostg.com	NoError	45.67.229.54		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: 41053, Reason: Analysis Target
Unmonitor End Time	End Time: 231841, Reason: Terminated
Monitor duration	190.79s
Return Code	0
PID	3420
Parent PID	912
Bitness	32 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
-	3.96 KB	aec91c78c4dc06c5bcea7b5020c38b003fc120153d51a3adb4f32d8000a6326a	✗
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
-	162 bytes	33b0af3e22cc50e215f77539ac661526ea5d1a21a8db6900c4bb7c058ce296af	✗

Host Behavior

Type	Count
Keyboard	12
Module	4
COM	2
Process	1

Process #2: explorer.exe

ID	2
File Name	c:\windows\syswow64\explorer.exe
Command Line	explorer i7Gigabyte.hta
Initial Working Directory	C:\Users\kEecfMwgj\Documents\
Monitor Start Time	Start Time: 66641, Reason: Child Process
Unmonitor End Time	End Time: 82119, Reason: Terminated
Monitor duration	15.48s
Return Code	1
PID	3656
Parent PID	3420
Bitness	32 Bit

Process #3: explorer.exe

ID	3
File Name	c:\windows\explorer.exe
Command Line	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 72922, Reason: RPC Server
Unmonitor End Time	End Time: 148691, Reason: Terminated
Monitor duration	75.77s
Return Code	1
PID	3684
Parent PID	584
Bitness	64 Bit

Process #4: mshta.exe

ID	4
File Name	c:\windows\syswow64\mshta.exe
Command Line	"C:\Windows\SysWOW64\mshta.exe" "C:\Users\kEecfMwgj\Documents\i7Gigabyte.hta"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 77411, Reason: Child Process
Unmonitor End Time	End Time: 92646, Reason: Terminated
Monitor duration	15.23s
Return Code	0
PID	3712
Parent PID	3684
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
-	204 bytes	56591a120bd1c7d012554befd923d1ac7bf015a53a36c2808766f74fbfdceb64	✖

Host Behavior

Type	Count
System	48
Module	125
File	7
Environment	2
Registry	106
-	5
Keyboard	2
Mutex	1
Window	9
COM	14
-	1
Process	1

Network Behavior

Type	Count
HTTP	1
TCP	1

Process #5: regsvr32.exe

ID	5
File Name	c:\windows\syswow64\regsvr32.exe
Command Line	"C:\Windows\System32\regsvr32.exe" c:\users\public\gigabytel7.jpg
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 90918, Reason: Child Process
Unmonitor End Time	End Time: 99286, Reason: Terminated
Monitor duration	8.37s
Return Code	3
PID	3784
Parent PID	3712
Bitness	32 Bit

Host Behavior

Type	Count
System	3
Module	4
Registry	4
File	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0	C:\Users\kEecfMwgj\Desktop\ecd84fa8d836d5057149b2b3a048d75004ca1a1377fcf2f5e67374af3a1161a0.doc	Sample File	77.50 KB	application/msword	-	MALICIOUS
aec91c78c4dc06c5bcea7b5020c38b003fc120153d51a3adb4f32d8000a6326a	c:\users\keecfmwgj\documents\~wrd0000.tmp, c:\users\keecfmwgj\documents\i7gigabyte.hta	Dropped File	3.96 KB	text/html	-	CLEAN
33b0af3e22cc50e215f77539ac661526ea5d1a21a8db6900c4bb7c058ce296af	c:\users\keecfmwgj\documents\~$gigabyte.hta	Dropped File	162 bytes	application/octet-stream	-	CLEAN
56591a120bd1c7d012554befd923d1ac7bf015a53a36c2808766f74fbfdceb64	c:\users\public\gigabytel7.jpg	Downloaded File	204 bytes	text/html	Create, Write, Access, Read	CLEAN
f7f7a14d693935c6a2bcea607e802050e520ca6d12a3833f0d06731645056d92	0.PNG	Embedded File	25.82 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Windows\SysWOW64\mshta.exe	Accessed File	Access	CLEAN
Win.ini	Accessed File	Access, Read	CLEAN
C:\Windows\SysWOW64\mshtml.dll	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
c:\users\public\gigabytel7.jpg	Downloaded File	Create, Write, Access, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://patelboostg.com/frhe/L8dclCye7SQ5WTFva78FDxOjGBOF9iJro4DRgV/5inYlaSBt0KLfMB9kXwZBv6ZpTsny6/qAhlQjrAaLKJeTLQnbCarASpMADNe9u1... ... 1XErrU1F/vaci3?page=V8BBaQuem65&page=XYvyd0Dcrg6fJYLGHRVWp7s1tv&page=dvZwXcjcYCjBX8tPaALshiDAx85PEq&sid=10tOgWzOZj9xyAidNJAz3d9Ob0	-	45.67.229.54	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
patelboostg.com	45.67.229.54	-	HTTP, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
45.67.229.54	patelboostg.com	Moldova	TCP, HTTP, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Local\!PrivacIE!SharedMemory!Mutex	access	mshta.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CLASSES_ROOT\clsid\{25336920-03f9-11cf-8fd0-00aa00686f13}\InProcServer32	access, read	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CSS_DATA_RESPECTS_XSS_ZONE_SETTING_KB912120	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CSS_DATA_RESPECTS_XSS_ZONE_SETTING_KB912120	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_EXTERNAL_STYLE_SHEET_FIX_FOR_SMARTNAVIGATION_KB926131	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_EXTERNAL_STYLE_SHEET_FIX_FOR_SMARTNAVIGATION_KB926131	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ARIA_SUPPORT	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ARIA_SUPPORT	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LEGACY_DISPPARAMS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LEGACY_DISPPARAMS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PRIVATE_FONT_SETTING	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_PRIVATE_FONT_SETTING	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CSS_SHOW_HIDE_EVENTS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CSS_SHOW_HIDE_EVENTS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISPLAY_NODE_ADVISE_KB833311	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DISPLAY_NODE_ADVISE_KB833311	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_EXPANDURI_BYPASS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ALLOW_EXPANDURI_BYPASS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BODY_SIZE_IN_EDITABLE_IFRAME_KB943245	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BODY_SIZE_IN_EDITABLE_IFRAME_KB943245	access	mshta.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DATABINDING_SUPPORT	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DATABINDING_SUPPORT	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENFORCE_BSTR	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENFORCE_BSTR	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_DYNAMIC_OBJECT_CACHING	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_DYNAMIC_OBJECT_CACHING	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LEGACY_TOSTRING_IN_COMPATVIEW	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_LEGACY_TOSTRING_IN_COMPATVIEW	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_OM_SCREEN_ORIGIN_DISPLAY_PIXELS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_OM_SCREEN_ORIGIN_DISPLAY_PIXELS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_CRASH_RECOVERY_SAVE_KB978454	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_RESTRICT_CRASH_RECOVERY_SAVE_KB978454	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CLEANUP_AT_FLS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_CLEANUP_AT_FLS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFileMenu	access, read	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MANAGE_SCRIPT_CIRCULAR_REFS	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MANAGE_SCRIPT_CIRCULAR_REFS	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DOCUMENT_COMPATIBLE_MODE	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_DOCUMENT_COMPATIBLE_MODE	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_DOCUMENT_ZOOM	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_DOCUMENT_ZOOM	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PageSetup	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\PageSetup\Print_Background	access, read	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_XSSFILTER	access	mshta.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_XSSFILTER	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SHOW_FAILED_CONNECT_CONTENT_KB942615	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_SHOW_FAILED_CONNECT_CONTENT_KB942615	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_TREAT_IMAGE_AS_AUTHORITATIVE	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MIME_TREAT_IMAGE_AS_AUTHORITATIVE	access	mshta.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MSHTML_AUTOLOAD_IEFRAME	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_MSHTML_AUTOLOAD_IEFRAME	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script\Features	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3\COM+Enabled	access, read	mshta.exe	CLEAN
HKEY_CLASSES_ROOT\.jpg	access, read	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\jpegfile	access	regsvr32.exe	CLEAN
HKEY_CLASSES_ROOT\jpegfile\AutoRegister	access	regsvr32.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDITIONAL_IE8_MEMORY_CLEANUP	access	mshta.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ADDITIONAL_IE8_MEMORY_CLEANUP	access	mshta.exe	CLEAN

Process

Process Name	Commandline	Verdict
explorer.exe	explorer i7Gigabyte.hta	SUSPICIOUS
mshta.exe	"C:\Windows\SysWOW64\mshta.exe" "C:\Users\kEecfMwgj\Documents\i7Gigabyte.hta"	SUSPICIOUS
winword.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n	CLEAN
explorer.exe	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding	CLEAN
regsvr32.exe	"C:\Windows\System32\regsvr32.exe" c:\users\public\gigabytel7.jpg	CLEAN

YARA / AV

No YARA or AV matches available.

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	4.4.0
Dynamic Engine Version	4.4.0 / 12/08/2021 19:04
Static Engine Version	4.4.0.0 / 2021-12-08 18:00:20
AV Exceptions Version	4.4.1.6 / 2021-12-14 15:06:27
Link Detonation Heuristics Version	4.4.1.7 / 2021-12-15 19:11:26
Smart Memory Dumping Rules Version	4.4.0.0 / 2021-12-08 18:00:20
Signature Trust Store Version	4.4.1.6 / 2021-12-14 15:06:27
VMRay Threat Identifiers Version	4.4.1.7 / 2021-12-15 19:11:26
YARA Built-in Ruleset Version	4.4.1.7

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