MALICIOUS

Classifications: Spyware

Threat Names: VBS.Heur.ObfDldr.30.6277A94D.Gen

Verdict Reason: -

Sample Type	**Word Document**
File Name	**Miembros de la UNAB para arrestar.docx**
ID	#664619
MD5	f6e2c8a84bf778c239df19c3bc9d479c
SHA1	9d029b7e83026ae8cedbf68f92b7717eeec05a27
SHA256	c3e56af0c0a13e8ab4e6f2269d1c15586e72f9b7a90c22980f976e6786388a03
File Size	38.93 KB
Report Created	2021-06-24 02:24 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | ms_office

OVERVIEW

VMRay Threat Identifiers (10 rules, 14 matches)

Score	Category	Operation	Count	Classification
5/5	Input Capture	Captures clipboard data	1	Spyware
	• (Process #1) winword.exe reads data from clipboard.			
4/5	Discovery	Executes WMI query	3	-
	• (Process #7) wscript.exe executes WMI query: SELECT UUID FROM Win32_ComputerSystemProduct. • (Process #7) wscript.exe executes WMI query: SELECT Name FROM Win32_OperatingSystem. • (Process #7) wscript.exe executes WMI query: Select * from AntiVirusProduct.			
4/5	Discovery	Queries OS version via WMI	1	-
	• (Process #7) wscript.exe queries OS version via WMI.			
4/5	Defense Evasion	Tries to detect the presence of antivirus software	1	-
	• (Process #7) wscript.exe tries to detect antivirus software via WMI query: "Select * from AntiVirusProduct".			
4/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDriveUpdate.vbs", to be triggered by Time. Task has been rescheduled by the analyzer.			
4/5	Antivirus	Malicious content was detected by heuristic scan	2	-
	• Built-in AV detected the dropped file C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDriveUpdate.vbs as "VBS.Heur.ObfDldr.30.6277A94D.Gen". • Built-in AV detected a memory dump of (process #7) wscript.exe as "VBS.Heur.ObfDldr.30.6277A94D.Gen".			
4/5	Network Connection	Tries to connect using an uncommon port	1	-
	• Tries to connect to TCP port 44567 at 185.233.202.230.			
2/5	Heuristics	Possible phishing document	2	-
	• Document "C:\Users\kEecfMwgj\Desktop\Miembros de la UNAB para arrestar.docx" is unusually short and contains a URL https://templateworkshop.site:44567/template_storage/normal_template/template48.dot. • Document "c:\users\keecfmwgj\desktop\~wrd0000.tmp" is unusually short and contains a URL https://templateworkshop.site:44567/template_storage/normal_template/template48.dot.			
2/5	Network Connection	Embedded URL does not use standard port	1	-
	• Embedded HTTPS URL "https://templateworkshop.site:44567/template_storage/normal_template/template48.dot" does not use port 443.			
1/5	Heuristics	Contains suspicious meta data	1	-
	• Office document contains below average content data.			
-	Trusted	Known clean file	1	-
	• A file which was only downloaded to memory is a known clean file.			

Mitre ATT&CK Matrix

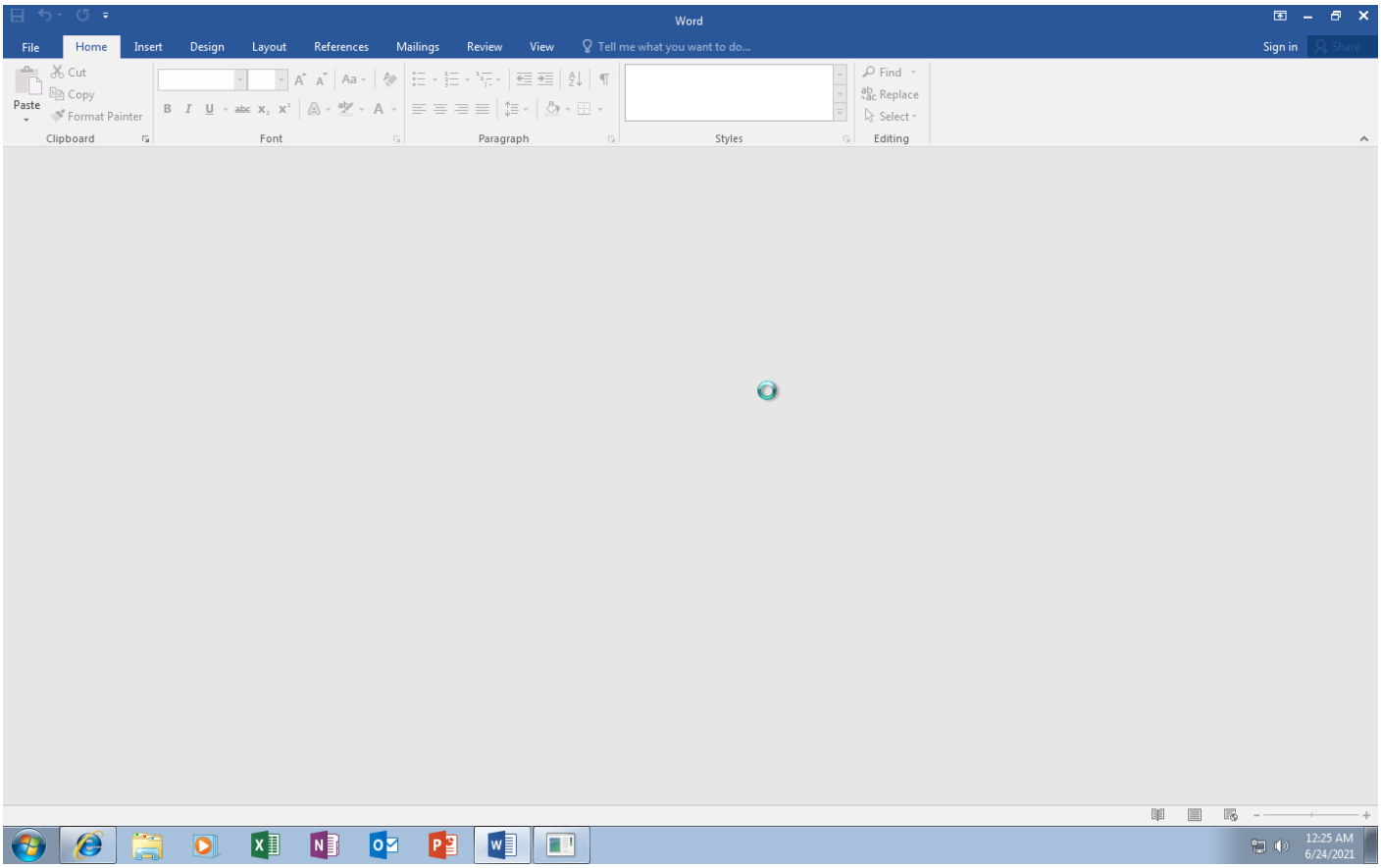
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
#T1193 Spearphishing Attachment	#T1047 Windows Management Instrumentation	#T1053 Scheduled Task	#T1053 Scheduled Task			#T1082 System Information Discovery		#T1115 Clipboard Data	#T1065 Uncommonly Used Port		
	#T1053 Scheduled Task					#T1063 Security Software Discovery					

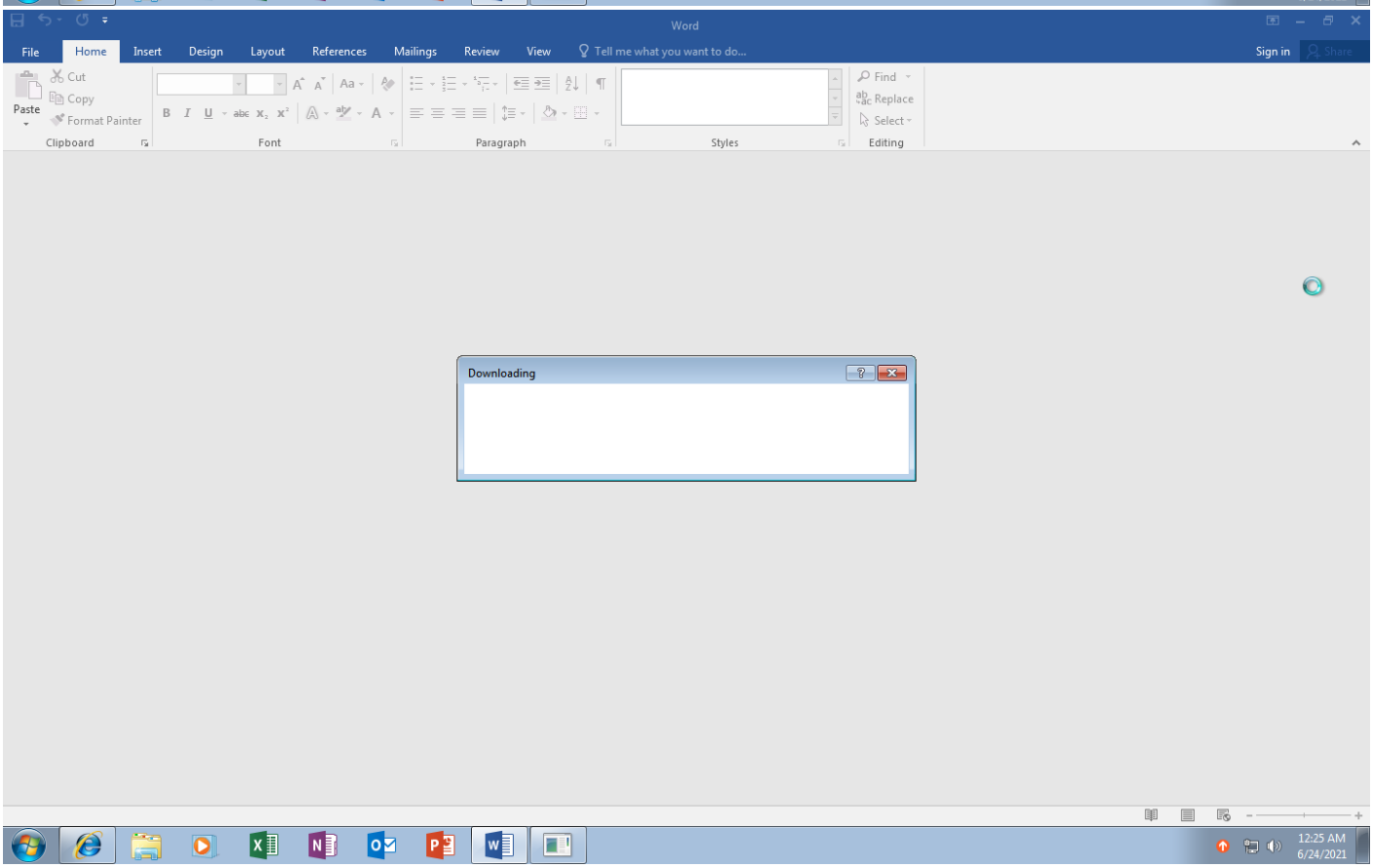
Sample Information

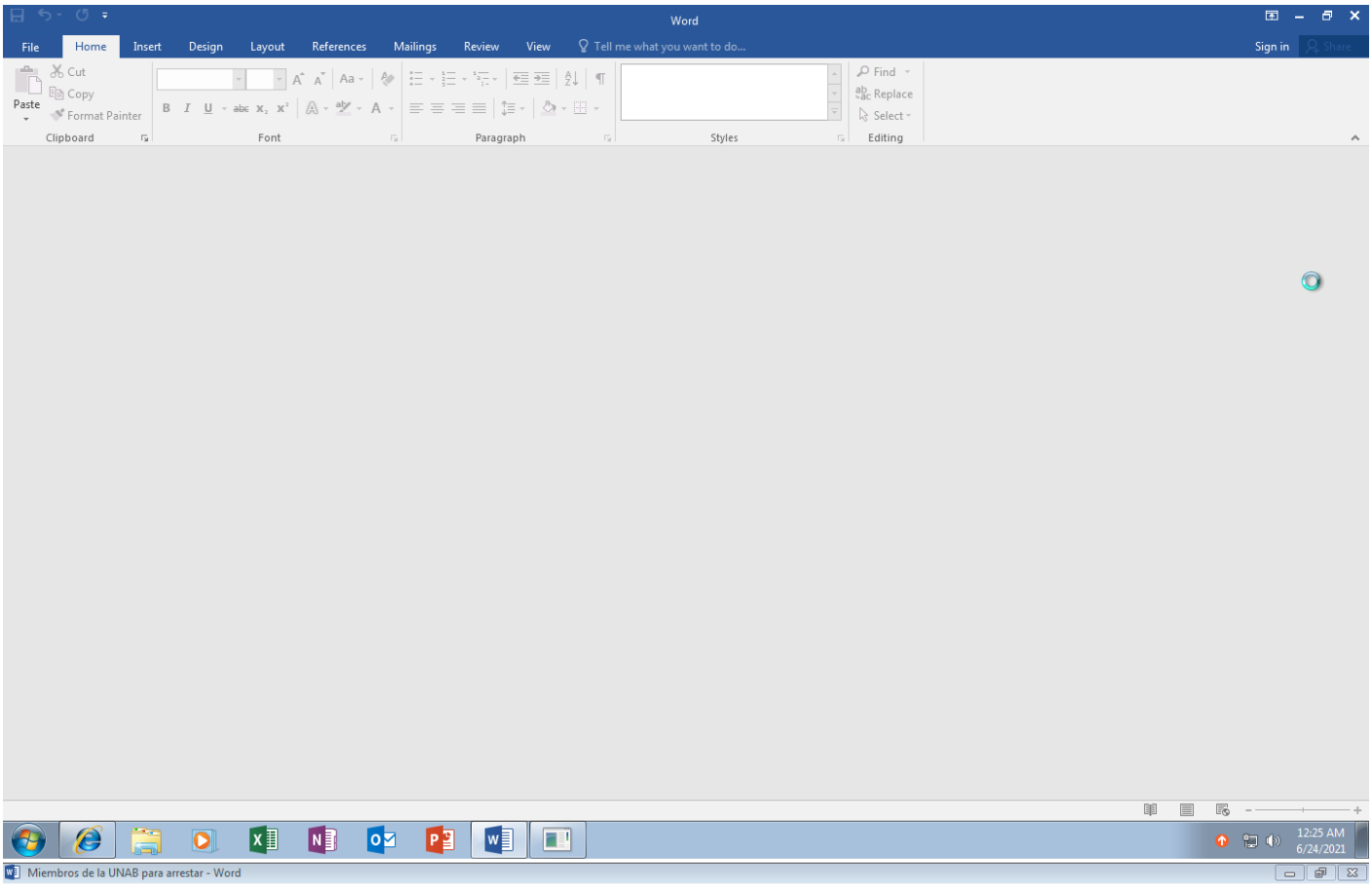
ID	#664619
MD5	f6e2c8a84bf778c239df19c3bc9d479c
SHA1	9d029b7e83026ae8cedbf68f92b7717eeec05a27
SHA256	c3e56af0c0a13e8ab4e6f2269d1c15586e72f9b7a90c22980f976e6786388a03
SSDeep	768:I/V0eQ94LHTKkDMCS6LsGov5UODZ7ewDgxHPldQ0JN9/5NE7099992qyo8ek:chFjTKuQGeU+789dQaNx5N/99992Tp
File Name	Miembros de la UNAB para arrestar.docx
File Size	38.93 KB
Sample Type	Word Document
Has Macros	✓

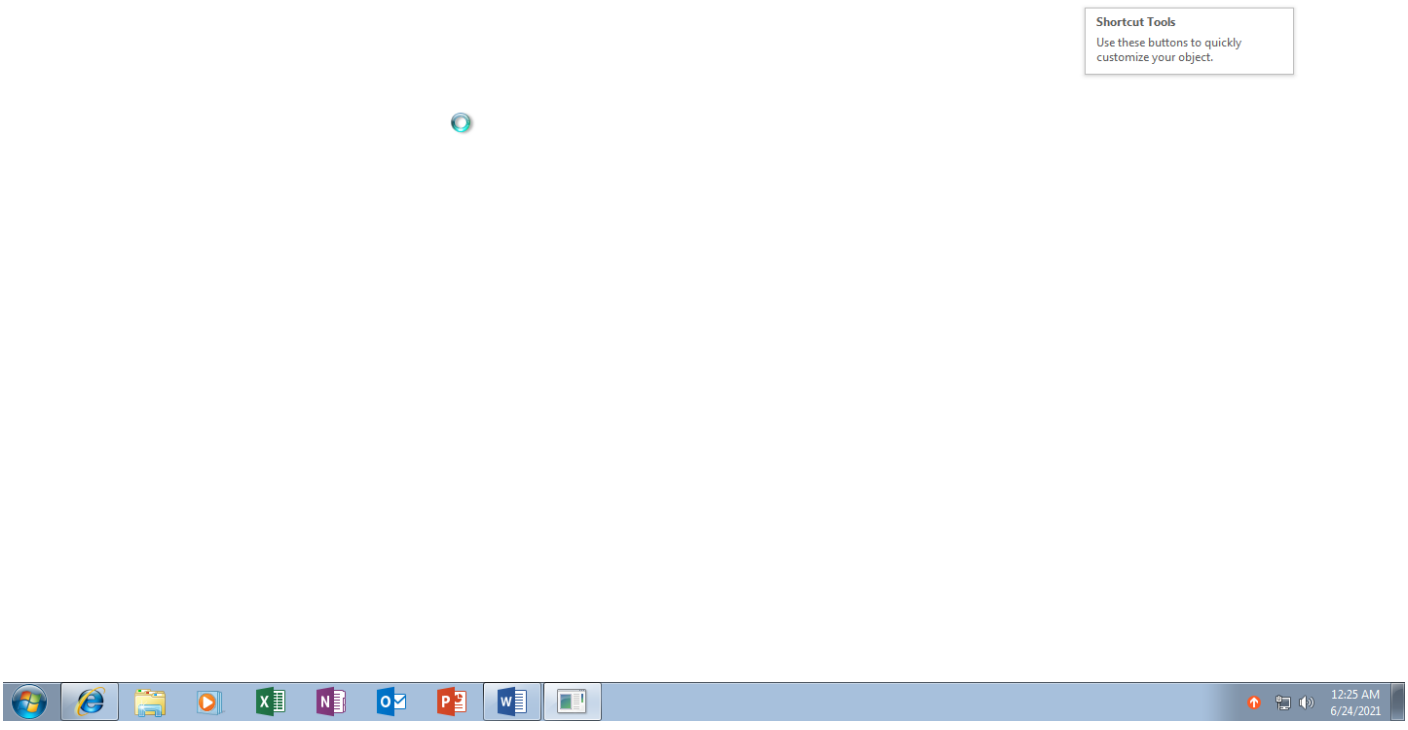
Analysis Information

Creation Time	2021-06-24 02:24 (UTC+2)
Analysis Duration	00:04:05
Termination Reason	Timeout
Number of Monitored Processes	6
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	2
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
12:25 AM
6/24/2021


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
Downloading
12:25 AM
6/24/2021





Screenshots truncated

NETWORK

General

14.17 KB total sent

732.91 KB total received

2 ports 80, 44567

2 contacted IP addresses

1 URLs extracted

2 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

7 sessions, 14.17 KB sent, 732.91 KB received

HTTP Requests

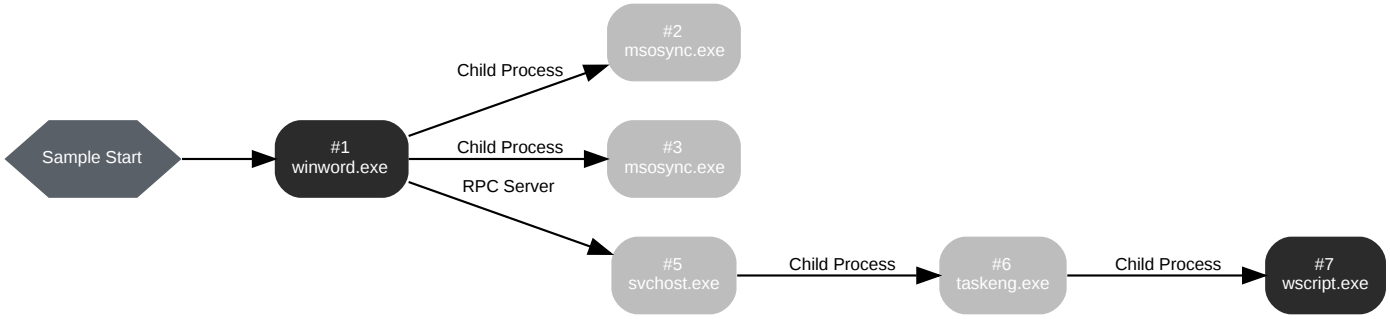
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
POST	http://185.233.202.60/cuamtwwzcmiglgydesed_irwlsnbwuexnmxoikdgx_ouruovwekqcvmdciutmd_bgpidjxpqasasebcptfi_interaction_bot	-	-		0 bytes	NA
GET	https://templateworkshop.site:44567/template_storage/normal_template/template48.dot	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	templateworkshop.site	NoError	185.233.202.230		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: 40442, Reason: Analysis Target
Unmonitor End Time	End Time: 285578, Reason: Terminated by Timeout
Monitor duration	245.14s
Return Code	Unknown
PID	3396
Parent PID	1124
Bitness	32 Bit

Dropped Files (6)

File Name	File Size	SHA256	YARA Match
-	38.93 KB	c3e56af0c0a13e8ab4e6f2269d1c15586e72f9b7a90c22980f976e6786388a03	✗
C:\Users\KEECFM~1\AppData\Local\Temp\nohitatusbkwu.tmp	55.96 KB	c1f383fd6b36cee26c861b3d8c253308bb8d8cdb1869c27e2008bf1daf1031ce	✗
-	68.13 KB	781f2723cbf154805d650a9fbe57f4e7a8de4875b022763991a89a3f9274b733	✗
-	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDriveUpdate.vbs	11.51 KB	2aa7cfcdef49150b32da1c3202ec115601a45ac10cbe7ab12f95ce839506e359	✗
-	1150.08 KB	9c3fee047908bf9fa622081ac1ca885bc38ecc5e664986c17c900716dd237b36	✗

Host Behavior

Type	Count
Module	52
Keyboard	39
COM	4
File	4
System	3

Process #2: msosync.exe

ID	2
File Name	c:\program files (x86)\microsoft office\root\office16\msosync.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\Office16\MsoSync.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Documents\
Monitor Start Time	Start Time: 59891, Reason: Child Process
Unmonitor End Time	End Time: 285578, Reason: Terminated by Timeout
Monitor duration	225.69s
Return Code	Unknown
PID	3568
Parent PID	3396
Bitness	32 Bit

Process #3: msosync.exe

ID	3
File Name	c:\program files (x86)\microsoft office\root\office16\msosync.exe
Command Line	"C:\Program Files (x86)\Microsoft Office\Root\Office16\MsoSync.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Documents\
Monitor Start Time	Start Time: 60442, Reason: Child Process
Unmonitor End Time	End Time: 69071, Reason: Terminated
Monitor duration	8.63s
Return Code	0
PID	3584
Parent PID	3396
Bitness	32 Bit

Process #5: svchost.exe

ID	5
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k netsvcs
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 71272, Reason: RPC Server
Unmonitor End Time	End Time: 285578, Reason: Terminated by Timeout
Monitor duration	214.31s
Return Code	Unknown
PID	816
Parent PID	464
Bitness	64 Bit

Process #6: taskeng.exe

ID	6
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {85A9294A-3A50-46E7-BF46-60F6008500EA} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 116230, Reason: Child Process
Unmonitor End Time	End Time: 285578, Reason: Terminated by Timeout
Monitor duration	169.35s
Return Code	Unknown
PID	3844
Parent PID	816
Bitness	64 Bit

Process #7: wscript.exe

ID	7
File Name	c:\windows\system32\wscript.exe
Command Line	C:\Windows\System32\WScript.exe "C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDriveUpdate.vbs"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 118039, Reason: Child Process
Unmonitor End Time	End Time: 128787, Reason: Terminated
Monitor duration	10.75s
Return Code	0
PID	3880
Parent PID	3844
Bitness	64 Bit

Host Behavior

Type	Count
System	32
Module	28
Registry	29
-	1
Window	1
COM	45
File	4
-	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
2aa7cfcdef49150b32da1c3202ec115601a45ac10cbe7ab12f95ce839506e359	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDriveUpdate.vbs	Dropped File	11.51 KB	text/plain	Create, Access	MALICIOUS
c3e56af0c0a13e8ab4e6f2269d1c15586e72f9b7a90c22980f976e6786388a03	C:\Users\kEecfMwgj\Desktop\Miembros de la UNAB para arrestar.docx	Sample File	38.93 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	MALICIOUS
eb910ff216b08c85661b22c8a540746dbc67aed19b6b5fa1381af8d50ef2717d	c:\users\keecfmwgj\appdata\local\microsoft\office\16.0\officefilecache\centraltable.laccdb	Modified File	128 bytes	application/octet-stream	-	CLEAN
781f2723cbf154805d650a9fbe57f4e7a8de4875b022763991a89a3f9274b733	c:\users\keecfmwgj\desktop\~wrd0000.tmp, c:\users\keecfmwgj\desktop\miembros de la unab para arrestar.docx	Dropped File	68.13 KB	application/vnd.openxmlformats-officedocument.wordprocessingml.document	-	CLEAN
9c3fee047908bf9fa622081ac1ca885bc38ecc5e664986c17c900716dd237b36	c:\users\keecfmwgj\appdata\local\temp\tryrthhfghfhgffgg.tmp	Dropped File	1150.08 KB	application/octet-stream	-	CLEAN
c1f383fd6b36cee26c861b3d8c253308bb8d8cdb1869c27e2008bf1daf1031ce	C:\Users\KEECFM~1\AppData\Local\Temp\nohitatusbkwu.tmp	Dropped File	55.96 KB	image/jpeg	Access, Write	CLEAN
e2387990169884493955e1588f65a75c996efb887d5395f5807527910239e7416	-	Downloaded File	480 bytes	text/plain	-	CLEAN
74188468490e859f321fa79343591c6c0a4880d3f77a5cab99298d5e2d6c2c42	-	Downloaded File	77 bytes	text/plain	-	CLEAN
efc63bd01240449348a3ceefb00f047101db509e35c7b80572a97b76b24a79a8	image1.png	Embedded File	29.96 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDriveUpdate.vbs	Dropped File	Create, Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\nohitatusbkwu.tmp	Dropped File	Delete, Access, Write	CLEAN
C:\Windows\System32\WScript.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://templateworkshop.site:44567/template_storage/normal_template/template48.dot	-	-	-	GET	SUSPICIOUS
http://185.233.202.60/cuamtwwzcmiglgydesed_irwlsnbwuexnmxoikdgx_ouruovwekqcvmdciutmd_bgpidjxpqasasebcptfi_interaction_bot	-	185.233.202.60	-	POST	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
templateworkshop.site	185.233.202.230	-	HTTPS, DNS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
185.233.202.230	templateworkshop.site	Russia	TLS, TCP, DNS	MALICIOUS
185.233.202.60	-	Russia	HTTP, TCP	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings	create, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings	create, access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\IgnoreUserSettings	access, read	wscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled	access, read	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled	access, read	wscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	access, read	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	access, read	wscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	access, read	wscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	access, read	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	access, read	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	access, read	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Timeout	access, read	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	access, read	wscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Timeout	access, read	wscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	access, read	wscript.exe	CLEAN
HKEY_CLASSES_ROOT\.vbs	access, read	wscript.exe	CLEAN
HKEY_CLASSES_ROOT\VBSFile\ScriptEngine	access, read	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	wscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	access, read	wscript.exe	CLEAN

Process

Process Name	Commandline	Verdict
wscript.exe	C:\Windows\System32\WScript.exe "C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDriveUpdate.vbs"	SUSPICIOUS
winword.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE" /n	CLEAN
msosync.exe	"C:\Program Files (x86)\Microsoft Office\Root\Office16\MsoSync.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskeng.exe	taskeng.exe {85A9294A-3A50-46E7-BF46-60F6008500EA} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN

YARA / AV

Antivirus (2)

File Type	Threat Name	File Name	Verdict
Dropped File	VBS.Heur.ObfDldr.30.6277A94D.Gen	C:\Users\kEecfMwgj\AppData\Local\Microsoft\OneDriveUpdate.vbs	MALICIOUS
Memory Dump	VBS.Heur.ObfDldr.30.6277A94D.Gen	-	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

Analyzer Information

Analyzer Version	4.2.2
Dynamic Engine Version	4.2.2 / 06/07/2021 03:43
Static Engine Version	4.2.2.0
Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-06-23 21:18:57+00:00
AV Exceptions Version	4.2.2.13 / 2021-06-02 18:07:39
VTI Ruleset Version	4.2.2.21 / 2021-06-16 07:30:46
YARA Built-in Ruleset Version	4.2.2.18
Link Detonation Heuristics Version	-
Signature Trust Store Version	4.2.2.13 / 2021-06-02 18:07:39
Analysis Report Layout Version	10

Software Information

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