MALICIOUS

Classifications: -
Threat Names: -
Verdict Reason: -

Sample Type	**Excel Document**
File Name	**msk.xls**
ID	#10565041
MD5	d57de46a209c32633dbb10f36eef7a06
SHA1	ebf2d3f3e47b39e8783330f1a6aa6f510e2a7a7f
SHA256	5dbcefc3f5401265b8fe4bb0c8a645914b45b850a13dfaa5ec313ec8e108b2c5
File Size	6411.29 KB
Report Created	2024-06-03 09:26 (UTC)
Target Environment	windows 7 (64bit SP1 -EN- MSO_2016) | ms_office

OVERVIEW

VMRay Threat Identifiers (22 rules, 128 matches)

Score	Category	Operation	Count	Classification
4/5	Obfuscation	Reads from memory of another process	87	-

- (Process #21) wmiprvse.exe reads from dwm.exe.
- (Process #21) wmiprvse.exe reads from taskhost.exe.
- (Process #21) wmiprvse.exe reads from explorer.exe.
- (Process #21) wmiprvse.exe reads from iexplore.exe.
- (Process #21) wmiprvse.exe reads from watchearly.exe.
- (Process #21) wmiprvse.exe reads from win.exe.
- (Process #21) wmiprvse.exe reads from future policy reality.exe.
- (Process #21) wmiprvse.exe reads from whatenergyindicate.exe.
- (Process #21) wmiprvse.exe reads from beautiful_type_interesting.exe.
- (Process #21) wmiprvse.exe reads from believewill.exe.
- (Process #21) wmiprvse.exe reads from able_paper_his.exe.
- (Process #21) wmiprvse.exe reads from systemboth.exe.
- (Process #21) wmiprvse.exe reads from traditional.exe.
- (Process #21) wmiprvse.exe reads from trial_just_role.exe.
- (Process #21) wmiprvse.exe reads from catchpastgo.exe.
- (Process #21) wmiprvse.exe reads from growth staff.exe.
- (Process #21) wmiprvse.exe reads from poorbyto.exe.
- (Process #21) wmiprvse.exe reads from great dark world.exe.
- (Process #21) wmiprvse.exe reads from regionbagraise.exe.
- (Process #21) wmiprvse.exe reads from itself.exe.
- (Process #21) wmiprvse.exe reads from purpose low shoot.exe.
- (Process #21) wmiprvse.exe reads from ncftp.exe.
- (Process #21) wmiprvse.exe reads from 3dftp.exe.
- (Process #21) wmiprvse.exe reads from absolutetelnet.exe.
- (Process #21) wmiprvse.exe reads from alftp.exe.
- (Process #21) wmiprvse.exe reads from barca.exe.
- (Process #21) wmiprvse.exe reads from bitkinex.exe.
- (Process #21) wmiprvse.exe reads from coreftp.exe.
- (Process #21) wmiprvse.exe reads from far.exe.
- (Process #21) wmiprvse.exe reads from filezilla.exe.
- (Process #21) wmiprvse.exe reads from flashfxp.exe.
- (Process #21) wmiprvse.exe reads from fling.exe.
- (Process #21) wmiprvse.exe reads from foxmailincmail.exe.
- (Process #21) wmiprvse.exe reads from gmailnotifierpro.exe.
- (Process #21) wmiprvse.exe reads from icq.exe.
- (Process #21) wmiprvse.exe reads from leechftp.exe.
- (Process #21) wmiprvse.exe reads from notepad.exe.
- (Process #21) wmiprvse.exe reads from whatsapp.exe.
- (Process #21) wmiprvse.exe reads from aldelo.exe.
- (Process #21) wmiprvse.exe reads from ccv_server.exe.
- (Process #21) wmiprvse.exe reads from centralcreditcard.exe.
- (Process #21) wmiprvse.exe reads from creditservice.exe.
- (Process #21) wmiprvse.exe reads from edcsvr.exe.
- (Process #21) wmiprvse.exe reads from fpos.exe.
- (Process #21) wmiprvse.exe reads from isspos.exe.
- (Process #21) wmiprvse.exe reads from mxslipstream.exe.
- (Process #21) wmiprvse.exe reads from omnipos.exe.
- (Process #21) wmiprvse.exe reads from spcwin.exe.
- (Process #21) wmiprvse.exe reads from spgagentservice.exe.
- (Process #21) wmiprvse.exe reads from utg2.exe.
- (Process #21) wmiprvse.exe reads from operamail.exe.
- (Process #21) wmiprvse.exe reads from outlook.exe.
- (Process #21) wmiprvse.exe reads from pidgin.exe.
- (Process #21) wmiprvse.exe reads from product.exe.
- (Process #21) wmiprvse.exe reads from walk.exe.
- (Process #21) wmiprvse.exe reads from catch.exe.
- (Process #21) wmiprvse.exe reads from periodwhich.exe.
- (Process #21) wmiprvse.exe reads from scriptftp.exe.
- (Process #21) wmiprvse.exe reads from skype.exe.
- (Process #21) wmiprvse.exe reads from smartftp.exe.

Score	Category	Operation	Count	Classification
4/5	Execution	Sends control codes to a driver	1	-
	• (Process #34) wmiprvse.exe controls driver "\\.\C:" through API DeviceIOControl.			
4/5	Network Connection	Performs DNS request	2	-
	• (Process #17) verclsid.exe resolves hostname "asper1.freeddns.org" to IP "186.48.86.162". • (Process #30) verclsid.exe resolves hostname "asper1.freeddns.org" to IP "186.48.86.162".			
4/5	Network Connection	Performs DNS request for known DDNS domain	1	-
	• (Process #17) verclsid.exe resolves hostname "asper1.freeddns.org" of dynamic DNS provider "dynu.com".			
4/5	Network Connection	Connects to remote host	2	-
	• (Process #30) verclsid.exe sends UDP message to host "186.48.86.162:57441". • (Process #17) verclsid.exe sends UDP message to host "186.48.86.162:57441".			
4/5	Network Connection	Attempts to connect through HTTPS	1	-
	• (Process #1) excel.exe connects to hxxps://picstate[.]com/file/20260941_ugxbx/B7CHZ11.png.			
4/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #17) verclsid.exe tries to connect to UDP port 57441 at 186.48.86.162.			
4/5	Execution	Document tries to create process	1	-
	• Document creates (process #2) schtasks.exe.			
4/5	Execution	Abuses verclsid to execute code	4	-
	• (Process #3) taskeng.exe abuses the system binary verclsid.exe to execute code. • (Process #16) cmd.exe abuses the system binary verclsid.exe to execute code. • (Process #25) taskeng.exe abuses the system binary verclsid.exe to execute code. • (Process #29) cmd.exe abuses the system binary verclsid.exe to execute code.			
4/5	Task Scheduling	Schedules task	3	-
	• Schedules task for command ""verclsid.exe"", to be triggered by LOGON. • Schedules task for command "schtasks.exe", to be triggered by SESSION_STATE_CHANGE. • Schedules task for command ""verclsid.exe"", to be triggered by SESSION_STATE_CHANGE.			
3/5	Discovery	Enumerates running processes	2	-
	• (Process #19) wmic.exe enumerates running processes via WMI query SELECT creationdate FROM Win32_Process WHERE name="wininit.exe". • (Process #32) wmic.exe enumerates running processes via WMI query SELECT creationdate FROM Win32_Process WHERE name="wininit.exe".			
3/5	Privilege Escalation	Enables process privileges	2	-
	• (Process #21) wmiprvse.exe enables process privilege "SeDebugPrivilege". • (Process #34) wmiprvse.exe enables process privilege "SeDebugPrivilege".			
2/5	Network Connection	Office macro uses a network function	2	-
	• Office macro uses the network function open. • Office macro uses the network function send.			
2/5	Execution	Creates suspicious COM object	2	-

Score	Category	Operation	Count	Classification
	• Office macro creates suspicious WinHTTP.WinHTTPrequest.5 COM object. • Office macro creates suspicious WinHTTP.WinHTTPrequest.5.1 COM object.			
2/5	Defense Evasion	Loads a dropped DLL	4	-
	• (Process #14) verclsid.exe loads dropped DLL b79266.dll. • (Process #17) verclsid.exe loads dropped DLL b79266.dll. • (Process #26) verclsid.exe loads dropped DLL b79266.dll. • (Process #30) verclsid.exe loads dropped DLL b79266.dll.			
2/5	Execution	Office macro uses an execute function	2	-
	• Office macro uses the shell function. • Office macro uses the run function.			
2/5	Execution	Office macro uses a file I/O function	6	-
	• Office macro uses the open function. • Office macro uses the put function. • Office macro uses the close function. • Office macro uses the freefile function. • Office macro uses the lof function. • Office macro uses the print function.			
2/5	YARA	Suspicious content matched by YARA rules	1	-
	• YARA detected "VBA_Download_Commands" from ruleset "Generic" in script.			
1/5	Defense Evasion	Accesses volumes directly	1	-
	• (Process #34) wmiprvse.exe opens a handle to directly access the volume "C".			
1/5	Obfuscation	Overwrites code	1	-
	• (Process #1) excel.exe overwrites code to possibly hide behavior.			
1/5	Execution	Contains suspicious Office macro	1	-
	• Office document contains a suspicious VBA macro.			
1/5	Execution	Executes macro on specific event	1	-
	• Executes macro on target "document" and event "close".			

Mitre ATT&CK Matrix

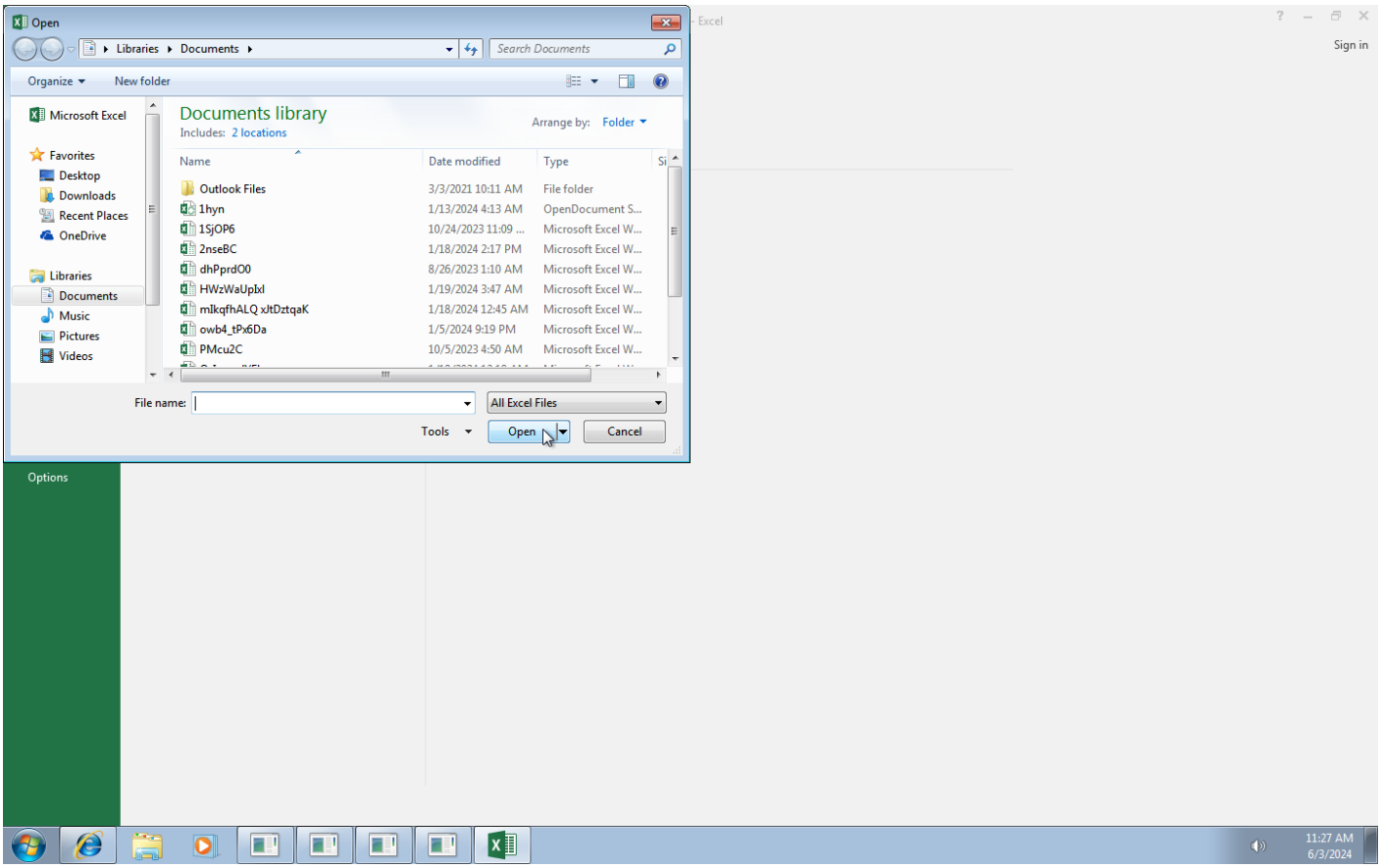
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1006 File System Logical Offsets		#T1082 System Information Discovery			#T1071 Standard Application Layer Protocol		
	#T1064 Scripting			#T1045 Software Packing					#T1032 Standard Cryptographic Protocol		
	#T1218 Signed Binary Proxy Execution			#T1064 Scripting					#T1065 Uncommonly Used Port		
	#T1053 Scheduled Task			#T1218 Signed Binary Proxy Execution							

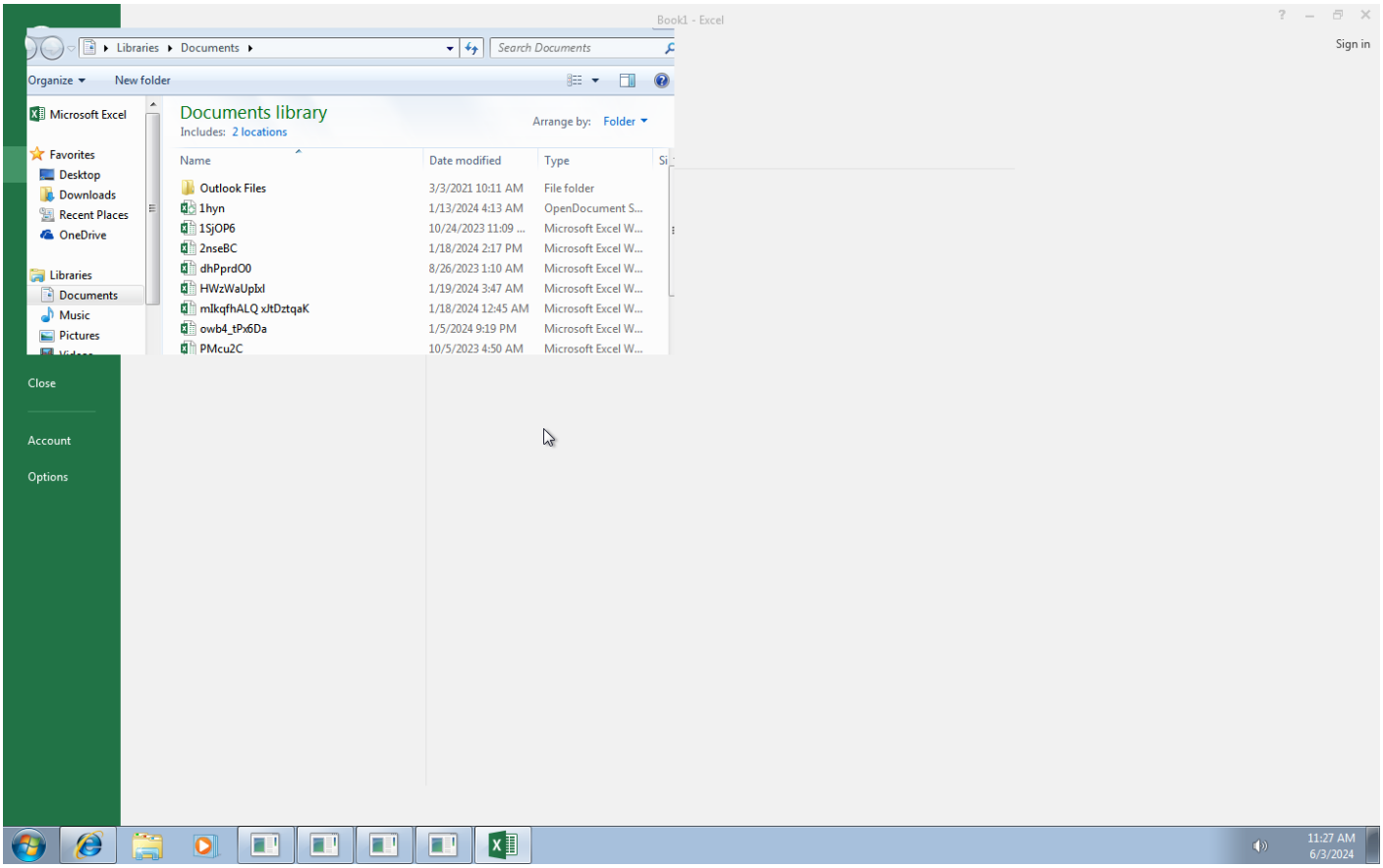
Sample Information

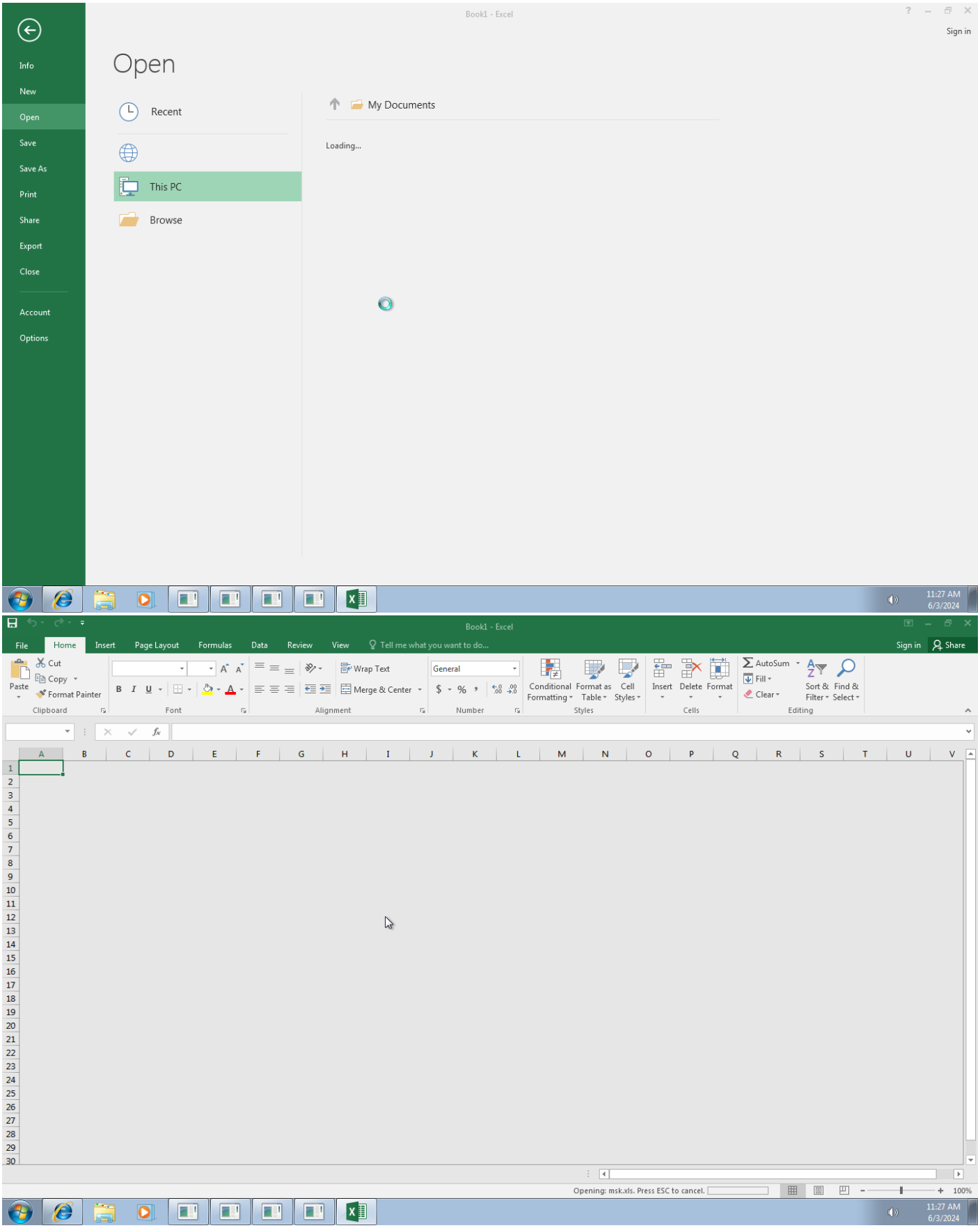
ID	#10565041
MD5	d57de46a209c32633dbb10f36eef7a06
SHA1	ebf2d3f3e47b39e8783330f1a6aa6f510e2a7a7f
SHA256	5dbcefc3f5401265b8fe4bb0c8a645914b45b850a13dfaa5ec313ec8e108b2c5
SSDeep	49152:qtl1YCAnrStN354aGlhG10h8/M4dp0btcfPYIUdLC71:zNAnc36aGlhG168/M4diuojdLC71
File Name	msk.xls
File Size	6411.29 KB
Sample Type	Excel Document
Has Macros	✔

Analysis Information

Creation Time	2024-06-03 09:26 (UTC)
Analysis Duration	00:10:03
Termination Reason	Timeout
Number of Monitored Processes	35
Execution Successful	True
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	1


Open
Libraries ▸ Documents ▸
Search Documents
Organize
New folder
Microsoft Excel
Documents library
Includes: 2 locations
Arrange by: Folder
Favorites
Desktop
Downloads
Recent Places
OneDrive
Libraries
Documents
Music
Pictures
Videos
Name
Date modified
Type
Outlook Files 3/3/2021 10:11 AM File folder
1hyn 1/13/2024 4:13 AM OpenDocument S...
1SjOP6 10/24/2023 11:09 ... Microsoft Excel W...
2nseBC 1/18/2024 2:17 PM Microsoft Excel W...
dhPprdO0 8/26/2023 1:10 AM Microsoft Excel W...
HWzWaUpbI 1/19/2024 3:47 AM Microsoft Excel W...
mIkqfhALQ xJtDztqaK 1/18/2024 12:45 AM Microsoft Excel W...
owb4_tPx6Da 1/5/2024 9:19 PM Microsoft Excel W...
PMcu2C 10/5/2023 4:50 AM Microsoft Excel W...
File name:
All Excel Files
Tools
Open
Cancel
Excel
Sign in
Options
11:27 AM
6/3/2024


Book1 - Excel
Libraries ▸ Documents ▸
Search Documents
Organize
New folder
Microsoft Excel
Documents library
Includes: 2 locations
Arrange by: Folder
Favorites
Desktop
Downloads
Recent Places
OneDrive
Libraries
Documents
Music
Pictures
Name
Date modified
Type
Outlook Files 3/3/2021 10:11 AM File folder
1hyn 1/13/2024 4:13 AM OpenDocument S...
1SjOP6 10/24/2023 11:09 ... Microsoft Excel W...
2nseBC 1/18/2024 2:17 PM Microsoft Excel W...
dhPprdO0 8/26/2023 1:10 AM Microsoft Excel W...
HWzWaUpbI 1/19/2024 3:47 AM Microsoft Excel W...
mIkqfhALQ xJtDztqaK 1/18/2024 12:45 AM Microsoft Excel W...
owb4_tPx6Da 1/5/2024 9:19 PM Microsoft Excel W...
PMcu2C 10/5/2023 4:50 AM Microsoft Excel W...
Close
Account
Options
Sign in
11:27 AM
6/3/2024



Screenshots truncated

NETWORK

General

1.75 KB total sent

233.15 KB total received

3 ports 57441, 443, 53

3 contacted IP addresses

0 URLs extracted

1 files downloaded

1 malicious hosts detected

DNS

3 DNS requests for 2 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

1 URLs contacted, 1 servers

1 sessions, 1.32 KB sent, 232.90 KB received

HTTP Requests

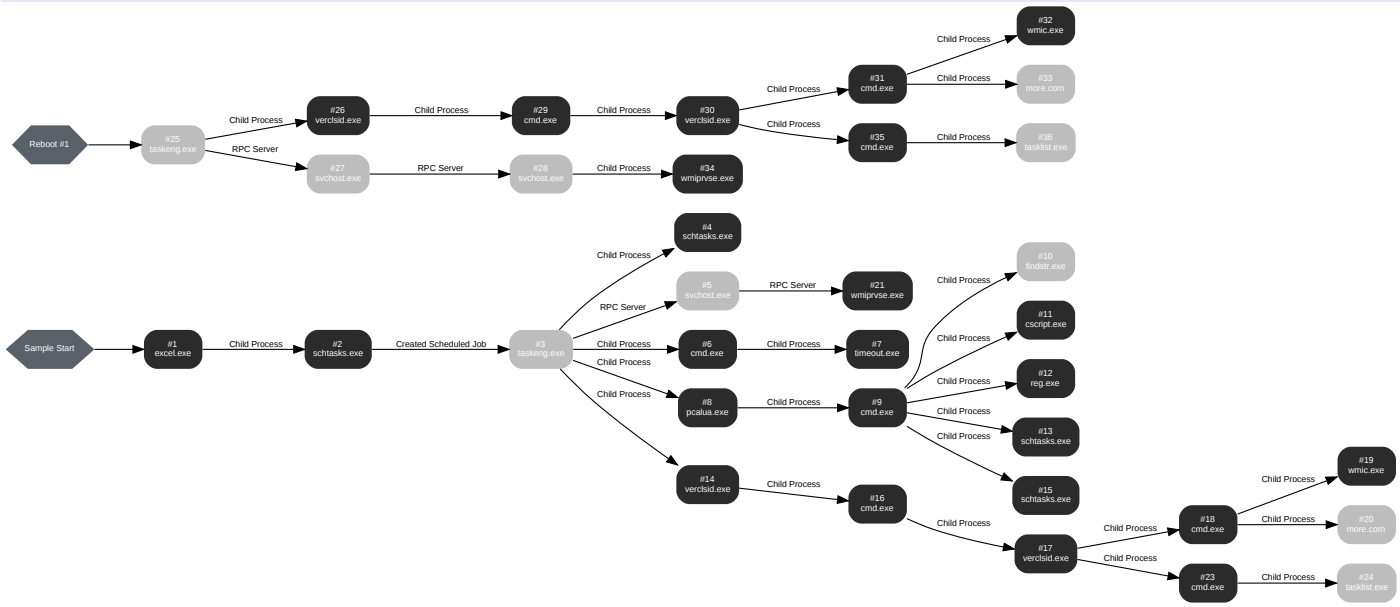
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	hxxps://picstate[.]com/file/20260941_ugxbx/B7CHZ11.png	-	-	-	0 bytes	CLEAN

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	asper1[.]freeddns[.]org	NO_ERROR	186.48.86.162	-	MALICIOUS
A	picstate[.]com	NO_ERROR	104.21.13.121, 172.67.167.243	-	CLEAN

BEHAVIOR

Process Graph



Process #1: excel.exe

ID	1
File Name	c:\program files\microsoft office\office16\excel.exe
Command Line	"C:\Program Files\Microsoft Office\Office16\EXCEL.EXE"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 78907, Reason: Analysis Target
Unmonitor End Time	End Time: 261396, Reason: Terminated
Monitor duration	182.49s
Return Code	0
PID	3652
Parent PID	-
Bitness	64 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\TTT.TMP	213.00 KB	3f2e57aa025065184ceff957838a11e342d161febd4119d89b89a98c758ad9a9	✖
C:\Users\KEECFM~1\AppData\Local\Temp\check01.txt	3.80 KB	2252c2901ef42d0aecf41e8a79022f679b624f3f484c20ed81fd7dff188e8062	✖
C:\Users\KEECFM~1\AppData\Local\Temp\Z11.xml	1.75 KB	0b3ea5dcf88f100c6e0ce2ebb2c850d6de042bf2fca9ed83c47b713530acd977	✖
C:\Users\KEECFM~1\AppData\Local\Temp\ZZ11.tmp	1.73 KB	75813ed2c7a29277e051794d633d6e9cb3501b648add1d7a20b0d6d530143ff6	✖

Host Behavior

Type	Count
Module	2
Window	1
COM	3
File	19
Process	1

Network Behavior

Type	Count
HTTPS	1

Process #2: schtasks.exe

ID	2
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks /Create /TN \Z11 /f /XML C:\Users\KEECFM~1\AppData\Local\Temp\Z11.xml
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 216275, Reason: Child Process
Unmonitor End Time	End Time: 223445, Reason: Terminated
Monitor duration	7.17s
Return Code	0
PID	484
Parent PID	3652
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	7
COM	1
File	9

Process #3: taskeng.exe

ID	3
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {33C6C6ED-05D5-479F-9912-01F9AEE1F38B} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 370173, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	313.32s
Return Code	Unknown
PID	900
Parent PID	484
Bitness	64 Bit

Process #4: schtasks.exe

ID	4
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks.exe /delete /tn "\lockw" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 370801, Reason: Child Process
Unmonitor End Time	End Time: 373109, Reason: Terminated
Monitor duration	2.31s
Return Code	1
PID	1096
Parent PID	900
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	11
-	2
COM	1
File	10

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: 370852, Reason: RPC Server
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	312.64s
Return Code	Unknown
PID	876
Parent PID	900
Bitness	64 Bit

Process #6: cmd.exe

ID	6
File Name	c:\windows\system32\cmd.exe
Command Line	cmd.exe /c "copy /y "C:\Users\KEECFM~1\AppData\Local\Temp\check01.txt" "C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat" & timeout 1"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 372085, Reason: Child Process
Unmonitor End Time	End Time: 375085, Reason: Terminated
Monitor duration	3.00s
Return Code	0
PID	2888
Parent PID	900
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat	3.80 KB	2252c2901ef42d0aecf41e8a79022f679b624f3f484c20ed81fd7dff188e8062	✖

Host Behavior

Type	Count
Module	1
File	28
Process	2
Environment	8

Process #7: timeout.exe

ID	7
File Name	c:\windows\system32\timeout.exe
Command Line	timeout 1
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 372820, Reason: Child Process
Unmonitor End Time	End Time: 374877, Reason: Terminated
Monitor duration	2.06s
Return Code	0
PID	3088
Parent PID	2888
Bitness	64 Bit

Host Behavior

Type	Count
System	12
Module	2
File	24

Process #8: pcalua.exe

ID	8
File Name	c:\windows\system32\pcalua.exe
Command Line	pcalua.exe -a "C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 373892, Reason: Child Process
Unmonitor End Time	End Time: 376692, Reason: Terminated
Monitor duration	2.80s
Return Code	0
PID	3096
Parent PID	900
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	1
Window	1

Process #9: cmd.exe

ID	9
File Name	c:\windows\system32\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ""C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat" "
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 374957, Reason: Child Process
Unmonitor End Time	End Time: 382228, Reason: Terminated
Monitor duration	7.27s
Return Code	0
PID	2868
Parent PID	3096
Bitness	64 Bit

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\a.xml	1.29 KB	c962ef38436b26bd8bd55146a90ac34bf323997fbb3686595ed35ddb4a65ac80	✖
C:\Users\KEECFM~1\AppData\Local\Temp\writebin.vbs	750 bytes	97cd69ab34502eeeb1c77414ac8cdd21c0d99e7cd7aeb30e3695b095bb33db38	✖
C:\Users\kEecfMwgj\AppData\Local\{D77D06B2-C71E-C031-9266-658FBD2652B7}\B79266.DLL	213.00 KB	ebb38b608cc64b140273b3568ba22398c7b052a3c3bfac3cc15f370a0e1764bc	✖

Host Behavior

Type	Count
Module	5
File	1600
Environment	118
Process	7

Process #10: findstr.exe

ID	10
File Name	c:\windows\system32\findstr.exe
Command Line	findstr /r "^[^a-z]*:::" "C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 375779, Reason: Child Process
Unmonitor End Time	End Time: 377055, Reason: Terminated
Monitor duration	1.28s
Return Code	0
PID	3116
Parent PID	2868
Bitness	64 Bit

Process #11: cscript.exe

ID	11
File Name	c:\windows\system32\cscript.exe
Command Line	cscript //nologo "C:\Users\KEECFM~1\AppData\Local\Temp\writebin.vbs" "4D5A50" "C:\Users\KEECFM~1\AppData\Local\Temp\MMM.TMP"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 375992, Reason: Child Process
Unmonitor End Time	End Time: 378814, Reason: Terminated
Monitor duration	2.82s
Return Code	0
PID	3128
Parent PID	2868
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\MMM.TMP	6 bytes	bd57b1dad8c2692be84de0fd2bd8795b0f7331e6b3a075a0d73f5c05710a75af	✖

Host Behavior

Type	Count
System	23
Module	18
Registry	27
-	1
Window	1
COM	5
File	7

Process #12: reg.exe

ID	12
File Name	c:\windows\system32\reg.exe
Command Line	reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{A78ED123-AB77-406B-9999-2A5D9D2F7FB7}\InprocServer32\ /t REG_SZ /d "C:\Users\kEecfMwgj\AppData\Local\{D77D06B2-C71E-C031-9266-658FBD2652B7}\B79266.DLL" /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 377371, Reason: Child Process
Unmonitor End Time	End Time: 378814, Reason: Terminated
Monitor duration	1.44s
Return Code	0
PID	3168
Parent PID	2868
Bitness	64 Bit

Host Behavior

Type	Count
System	3
Module	1
Registry	4
File	5

Process #13: schtasks.exe

ID	13
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks /Create /TN \Update_AgentConfig_kEecfMwgj /f /XML "C:\Users\KEECFM~1\AppData\Local\Temp\a.xml"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 378820, Reason: Child Process
Unmonitor End Time	End Time: 380722, Reason: Terminated
Monitor duration	1.90s
Return Code	0
PID	3240
Parent PID	2868
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	7
COM	1
File	9

Process #14: verclsid.exe

ID	14
File Name	c:\windows\system32\verclsid.exe
Command Line	verclsid.exe /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7}
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 379606, Reason: Child Process
Unmonitor End Time	End Time: 383399, Reason: Terminated
Monitor duration	3.79s
Return Code	3
PID	3336
Parent PID	900
Bitness	64 Bit

Host Behavior

Type	Count
System	4
Module	45
Window	1
File	1
Process	1

Process #15: schtasks.exe

ID	15
File Name	c:\windows\system32\schtasks.exe
Command Line	schtasks /Delete /TN \Z11 /f
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 379716, Reason: Child Process
Unmonitor End Time	End Time: 382040, Reason: Terminated
Monitor duration	2.32s
Return Code	0
PID	3300
Parent PID	2868
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Module	11
-	2
COM	1
File	5

Process #16: cmd.exe

ID	16
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c start "" verclsid.exe /M /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7} & Exit
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 382050, Reason: Child Process
Unmonitor End Time	End Time: 383554, Reason: Terminated
Monitor duration	1.50s
Return Code	0
PID	404
Parent PID	3336
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	4
Environment	2
Process	1
-	1

Process #17: verclsid.exe

ID	17
File Name	c:\windows\system32\verclsid.exe
Command Line	verclsid.exe /M /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7}
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 382489, Reason: Child Process
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	301.00s
Return Code	Unknown
PID	1060
Parent PID	404
Bitness	64 Bit

Host Behavior

Type	Count
System	20
Module	53
Window	4
File	13
Process	2
User	1
-	2

Network Behavior

Type	Count
DNS	1
UDP	1

Process #18: cmd.exe

ID	18
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c WMIC PROCESS where name="wininit.exe" get creationdate |more > %TEMP%\~dr9078
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 399750, Reason: Child Process
Unmonitor End Time	End Time: 408624, Reason: Terminated
Monitor duration	8.87s
Return Code	0
PID	3540
Parent PID	1060
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\KEECFM~1\AppData\Local\Temp\~dr9078	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Module	1
Environment	13
File	36
Process	2

Process #19: wmic.exe

ID	19
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	WMIC PROCESS where name="wininit.exe" get creationdate
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 400047, Reason: Child Process
Unmonitor End Time	End Time: 408592, Reason: Terminated
Monitor duration	8.54s
Return Code	0
PID	3564
Parent PID	3540
Bitness	64 Bit

Host Behavior

Type	Count
System	14
Module	5
COM	8
Registry	5
File	8
-	1

Process #20: more.com

ID	20
File Name	c:\windows\system32\more.com
Command Line	more
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 400130, Reason: Child Process
Unmonitor End Time	End Time: 408591, Reason: Terminated
Monitor duration	8.46s
Return Code	0
PID	3560
Parent PID	3540
Bitness	64 Bit

Process #21: wmiprvse.exe

ID	21
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 401269, Reason: RPC Server
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	282.22s
Return Code	Unknown
PID	3252
Parent PID	876
Bitness	64 Bit

Host Behavior

Type	Count
Module	16
User	2
System	222
Process	650
-	1043

Process #23: cmd.exe

ID	23
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c tasklist /fo csv >> C:\Users\KEECFM~1\AppData\Local\Temp\~dr9078
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 409846, Reason: Child Process
Unmonitor End Time	End Time: 419108, Reason: Terminated
Monitor duration	9.26s
Return Code	0
PID	3512
Parent PID	1060
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	16
Environment	8
Process	1

Process #24: tasklist.exe

ID	24
File Name	c:\windows\system32\tasklist.exe
Command Line	tasklist /fo csv
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 410234, Reason: Child Process
Unmonitor End Time	End Time: 418749, Reason: Terminated
Monitor duration	8.52s
Return Code	0
PID	3688
Parent PID	3512
Bitness	64 Bit

Process #25: taskeng.exe

ID	25
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {58CB376B-B7C1-4AA2-A22D-0FDB9D0F5A07} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 476832, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	206.66s
Return Code	Unknown
PID	1276
Parent PID	3240
Bitness	64 Bit

Process #26: verclsid.exe

ID	26
File Name	c:\windows\system32\verclsid.exe
Command Line	verclsid.exe /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7}
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 479875, Reason: Child Process
Unmonitor End Time	End Time: 550123, Reason: Terminated
Monitor duration	70.25s
Return Code	3
PID	1368
Parent PID	1276
Bitness	64 Bit

Host Behavior

Type	Count
System	4
Module	45
Window	1
File	1
Process	1

Process #27: svchost.exe

ID	27
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: 480706, Reason: RPC Server
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	202.79s
Return Code	Unknown
PID	880
Parent PID	1276
Bitness	64 Bit

Process #28: svchost.exe

ID	28
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k DcomLaunch
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 541929, Reason: RPC Server
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	141.56s
Return Code	Unknown
PID	608
Parent PID	880
Bitness	64 Bit

Process #29: cmd.exe

ID	29
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c start "" verclsid.exe /M /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7} & Exit
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 549563, Reason: Child Process
Unmonitor End Time	End Time: 551799, Reason: Terminated
Monitor duration	2.24s
Return Code	0
PID	1448
Parent PID	1368
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	4
Environment	2
Process	1
-	1

Process #30: verclsid.exe

ID	30
File Name	c:\windows\system32\verclsid.exe
Command Line	verclsid.exe /M /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7}
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 550123, Reason: Child Process
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	133.37s
Return Code	Unknown
PID	1432
Parent PID	1448
Bitness	64 Bit

Host Behavior

Type	Count
System	20
Module	53
Window	4
File	13
Process	2
User	1
-	2

Network Behavior

Type	Count
DNS	1
UDP	1

Process #31: cmd.exe

ID	31
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c WMIC PROCESS where name="wininit.exe" get creationdate |more > %TEMP%\~dr9078
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 561482, Reason: Child Process
Unmonitor End Time	End Time: 567769, Reason: Terminated
Monitor duration	6.29s
Return Code	0
PID	1856
Parent PID	1432
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
Environment	13
File	36
Process	2

Process #32: wmic.exe

ID	32
File Name	c:\windows\system32\wbem\wmic.exe
Command Line	WMIC PROCESS where name="wininit.exe" get creationdate
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 561742, Reason: Child Process
Unmonitor End Time	End Time: 567769, Reason: Terminated
Monitor duration	6.03s
Return Code	0
PID	1312
Parent PID	1856
Bitness	64 Bit

Host Behavior

Type	Count
System	14
Module	5
COM	8
Registry	5
File	8
-	1

Process #33: more.com

ID	33
File Name	c:\windows\system32\more.com
Command Line	more
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 561823, Reason: Child Process
Unmonitor End Time	End Time: 567706, Reason: Terminated
Monitor duration	5.88s
Return Code	0
PID	1244
Parent PID	1856
Bitness	64 Bit

Process #34: wmiprvse.exe

ID	34
File Name	c:\windows\system32\wbem\wmiprvse.exe
Command Line	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 563395, Reason: Child Process
Unmonitor End Time	End Time: 683492, Reason: Terminated by timeout
Monitor duration	120.10s
Return Code	Unknown
PID	2020
Parent PID	608
Bitness	64 Bit

Host Behavior

Type	Count
System	96
Mutex	1
Module	70
Registry	5
File	3
-	6
User	2
-	1
Process	106
-	119

Process #35: cmd.exe

ID	35
File Name	c:\windows\system32\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c tasklist /fo csv >> C:\Users\KEECFM~1\AppData\Local\Temp\~dr9078
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 571601, Reason: Child Process
Unmonitor End Time	End Time: 574742, Reason: Terminated
Monitor duration	3.14s
Return Code	0
PID	1016
Parent PID	1432
Bitness	64 Bit

Host Behavior

Type	Count
Module	1
File	16
Environment	8
Process	1

Process #36: tasklist.exe

ID	36
File Name	c:\windows\system32\tasklist.exe
Command Line	tasklist /fo csv
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 571883, Reason: Child Process
Unmonitor End Time	End Time: 574742, Reason: Terminated
Monitor duration	2.86s
Return Code	0
PID	156
Parent PID	1016
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
5dbcefc3f5401265b8fe4bb0c8a645914b45b850a13dfaa5ec313ec8e108b2c5	C:\Users\kEecfMwgj\Desktop\msk.xls	Sample File	6411.29 KB	application/vnd.ms-excel.sheet.macroEnabled.12	-	MALICIOUS
d0c3dc4daee29d452e10229387a5638676f07470f341fbc3e86cd722567bc8b4	Module7	Script	3.06 KB	application/x-vba-macros	-	SUSPICIOUS
780aad1fe29c120a985db2423b35ef94aaf6ab063525ddb4f7b7fea0e011185a	Módulo6	Script	111 bytes	application/x-vba-macros	-	SUSPICIOUS
ebb38b608cc64b140273b3568ba22398c7b052a3c3bfac3cc15f370a0e1764bc	C:\Users\kEecfMwgj\AppData\Local\{D77D06B2-C71E-C031-9266-658FBD2652B7}\B79266.DLL	Dropped File	213.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	SUSPICIOUS
fa09ef1b83f77ac31aaaf81d02c0143e96066ecac209c4066ef6276f61ea7bc0	image1.jpeg	Extracted File	22.35 KB	image/jpeg	-	CLEAN
e5b106d13edb2cb1711191948ba614e747fc03e236fd4c9628208231e525d1a9	-	Downloaded File	218.62 KB	image/png	-	CLEAN
75813ed2c7a29277e051794d633d6e9cb3501b648add1d7a20b0d6d530143ff6	C:\Users\KEECFM~1\AppData\Local\Temp\ZZ11.tmp	Dropped File	1.73 KB	text/xml	Access, Create, Read, Write	CLEAN
3f2e57aa025065184ceff957838a11e342d161febd4119d89b89a98c758ad9a9	C:\Users\KEECFM~1\AppData\Local\Temp\TTT.TMP, C:\Users\KEECFM~1\AppData\Local\Temp\TTT.tmp	Dropped File	213.00 KB	application/octet-stream	Access, Create, Delete, Read, Write	CLEAN
2252c2901ef42d0aecf41e8a79022f679b624f3f484c20ed81fd7dff188e8062	C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat, C:\Users\KEECFM~1\AppData\Local\Temp\check01.txt	Dropped File	3.80 KB	text/x-msdos-batch	Access, Create, Delete, Read, Write	CLEAN
0b3ea5dcf88f100c6e0ce2ebb2c850d6de042bf2fca9ed83c47b713530acd977	C:\Users\KEECFM~1\AppData\Local\Temp\Z11.xml	Dropped File	1.75 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN
97cd69ab34502eeeb1c77414ac8cdd21c0d99e7cd7aeb30e3695b095bb33db38	C:\Users\KEECFM~1\AppData\Local\Temp\writebin.vbs	Dropped File	750 bytes	text/plain	Access, Create, Delete, Write	CLEAN
bd57b1dad8c2692be84de0fd2bd8795b0f7331e6b3a075a0d73f5c05710a75af	C:\Users\KEECFM~1\AppData\Local\Temp\MMM.TMP	Dropped File	6 bytes	text/plain	Access, Create, Delete, Read, Write	CLEAN
c962ef38436b26bd8bd551465a90ac34bf323997fbb3686595ed35ddb4a65ac80	C:\Users\KEECFM~1\AppData\Local\Temp\a.xml	Dropped File	1.29 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN
5db0fb6bbc0635956653a2177aa6125ee142e657a1294cc7efd0b935c1395b3a	c:\users\keecfmwgj\appdata\local\microsoft\windows\history\history.ie5\index.dat	Modified File	64.00 KB	application/octet-stream	-	CLEAN
07e2f7c011eab3663c90fbab1e3a39eaf2915684374ed79f8e89a48c2e9414ea	c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\index.dat	Modified File	64.00 KB	application/octet-stream	-	CLEAN
0c5cceba5c416d5424387794429f89a2456b5326e2c7e5d8d2bd67f34bb616ec	c:\users\keecfmwgj\appdata\roaming\microsoft\windows\cookies\index.dat	Modified File	32.00 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\msk.xls	Sample File	-	MALICIOUS
verclsid.exe	Miscellaneous File	-	MALICIOUS
schtasks.exe	Miscellaneous File	-	MALICIOUS

File Name	Category	Operations	Verdict
image1.jpeg	Miscellaneous File	-	CLEAN
Module7	Miscellaneous File	-	CLEAN
Módulo1	Miscellaneous File	-	CLEAN
Módulo2	Miscellaneous File	-	CLEAN
Módulo3	Miscellaneous File	-	CLEAN
Módulo4	Miscellaneous File	-	CLEAN
Módulo5	Miscellaneous File	-	CLEAN
Módulo6	Miscellaneous File	-	CLEAN
UserForm1	Miscellaneous File	-	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\ZZ11.tmp	Accessed File, Dropped File	Access, Create, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\TTT.TMP	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\check01.txt	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\Z11.xml	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\writebin.vbs	Accessed File, Dropped File	Access, Create, Delete, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\MMM.TMP	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\kEecfMwgj\AppData\Local\{D77D06B2-C71E-C031-9266-658FBD2652B7}\B79266.DLL	Accessed File, Dropped File	Access, Create, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\a.xml	Accessed File, Dropped File	Access, Create, Delete, Read, Write	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp\~dr9078	Accessed File, Dropped File	Access, Create, Delete, Read	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\windows\history\history.ie5\index.dat	Modified File	-	CLEAN
c:\users\keecfmwgj\appdata\local\microsoft\windows\temporary internet files\content.ie5\index.dat	Modified File	-	CLEAN
c:\users\keecfmwgj\appdata\roaming\microsoft\windows\cookies\index.dat	Modified File	-	CLEAN
C:\Windows\system32\schtasks.exe	Accessed File	Access	CLEAN
C:\Windows\system32\timeout.exe	Accessed File	Access	CLEAN
"C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat"	Accessed File	Access	CLEAN
C:\Windows\system32\cscript.exe	Accessed File	Access	CLEAN
C:\Users\KEECFM~1\AppData\Local\Temp	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\{D77D06B2-C71E-C031-9266-658FBD2652B7}	Accessed File	Access, Create	CLEAN
nul	Accessed File	Access, Write	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Windows\system32\verclsid.exe	Accessed File	Access	CLEAN
C:\Windows\system32\wbem\XSL-Mappings.xml	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Windows\system32\wbem\\texttable.xsl	Accessed File	Access	CLEAN
C:\Windows\system32\WBEM\Logs\	Accessed File	Access	CLEAN
\\.\C:	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
hxxps://picstate[.]com/file/20260941_ugxbx/B7CHZ11.png	Contacted, Extracted	104.21.13.121, 172.67.167.243	United States	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
asper1[.]freeddns[.]org	186.48.86.162	Uruguay	DNS, UDP	MALICIOUS
picstate[.]com	104.21.13.121, 172.67.167.243	United States	DNS, TCP, HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
186.48.86.162	asper1[.]freeddns[.]org	Uruguay	DNS, UDP	MALICIOUS
::	-	-	-	CLEAN
104.21.13.121	picstate[.]com	-	DNS, TCP, HTTPS	CLEAN
172.67.167.243	picstate[.]com	United States	DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
-	access	wmiprvse.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings	create, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings	create, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\IgnoreUserSettings	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Enabled	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Enabled	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\LogSecuritySuccesses	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\TrustPolicy	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\UseWINSAFER	read, access	cscript.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\Timeout	read, access	cscript.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\Timeout	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows Script Host\Settings\DisplayLogo	read, access	cscript.exe	CLEAN
HKEY_CLASSES_ROOT\.vbs	read, access	cscript.exe	CLEAN
HKEY_CLASSES_ROOT\VBSFile\ScriptEngine	read, access	cscript.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	access	reg.exe	CLEAN
HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{A78ED123-AB77-406B-9999-2A5D9D2F7FB7}\InprocServer32	read, create, write, access	reg.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM	access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Logging Directory	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\CIMOM\Log File Max Size	read, access	wmic.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM	create, access	wmiprvse.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\WBEM\CIMOM\EnableObjectValidation	read, access	wmiprvse.exe	CLEAN

Process

Process Name	Commandline	Verdict
schtasks.exe	schtasks /Create /TN \Z11 /f /XML C:\Users\KEECFM~1\AppData\Local\Temp\Z11.xml	SUSPICIOUS
taskeng.exe	taskeng.exe {33C6C6ED-05D5-479F-9912-01F9AEE1F38B} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	SUSPICIOUS
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat" "	SUSPICIOUS
schtasks.exe	schtasks /Create /TN \Update_AgentConfig_kEecfMwgj /f /XML "C:\Users\KEECFM~1\AppData\Local\Temp\a.xml"	SUSPICIOUS
verclsid.exe	verclsid.exe /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7}	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c start "" verclsid.exe /M /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7} & Exit	SUSPICIOUS
verclsid.exe	verclsid.exe /M /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7}	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c WMIC PROCESS where name="wininit.exe" get creationdate	more > %TEMP%\~dr9078	SUSPICIOUS
wmic.exe	WMIC PROCESS where name="wininit.exe" get creationdate	SUSPICIOUS
taskeng.exe	taskeng.exe {58CB376B-B7C1-4AA2-A22D-0FDB9D0F5A07} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	SUSPICIOUS
verclsid.exe	verclsid.exe /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7}	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c start "" verclsid.exe /M /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7} & Exit	SUSPICIOUS
verclsid.exe	verclsid.exe /M /S /C {A78ED123-AB77-406B-9999-2A5D9D2F7FB7}	SUSPICIOUS
wmic.exe	WMIC PROCESS where name="wininit.exe" get creationdate	SUSPICIOUS
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c tasklist /fo csv >> C:\Users\KEECFM~1\AppData\Local\Temp\~dr9078	SUSPICIOUS

Process Name	Commandline	Verdict
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	SUSPICIOUS
excel.exe	"C:\Program Files\Microsoft Office\Office16\EXCEL.EXE"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
schtasks.exe	schtasks.exe /delete /tn "\lockw" /f	CLEAN
cmd.exe	cmd.exe /c "copy /y "C:\Users\KEECFM~1\AppData\Local\Temp\check01.txt" "C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat" & timeout 1"	CLEAN
timeout.exe	timeout 1	CLEAN
pcalua.exe	pcalua.exe -a "C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat"	CLEAN
findstr.exe	findstr /r "^[^a-z]*:::" "C:\Users\KEECFM~1\AppData\Local\Temp\check01.bat"	CLEAN
cscript.exe	cscript //nologo "C:\Users\KEECFM~1\AppData\Local\Temp\writebin.vbs" "4D5A50" "C:\Users\KEECFM~1\AppData\Local\Temp\MMM.TMP"	CLEAN
reg.exe	reg add HKEY_CURRENT_USER\SOFTWARE\Classes\CLSID\{A78ED123-AB77-406B-9999-2A5D9D2F7FB7}\InprocServer32\ /t REG_SZ /d "C:\Users\kEecfMwgj\AppData\Local\{D77D06B2-C71E-C031-9266-658FBD2652B7}\B79266.DLL" /f	CLEAN
schtasks.exe	schtasks /Delete /TN \Z11 /f	CLEAN
more.com	more	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c tasklist /fo csv >> C:\Users\KEECFM~1\AppData\Local\Temp\~dr9078	CLEAN
tasklist.exe	tasklist /fo csv	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c WMIC PROCESS where name="wininit.exe" get creationdate | more > %TEMP%\~dr9078	CLEAN
more.com	more	CLEAN
tasklist.exe	tasklist /fo csv	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Generic	VBA_Download_Commands	VBA macro may attempt to download external content; possible dropper	-	Module7	-	2/5

ENVIRONMENT

Virtual Machine Information

Name	win7_64_sp1_en_mso2016
Description	windows 7 (64bit SP1 -EN- MSO_2016)
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	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.29 / 2024-05-11 04:28:14
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.27 / 2024-05-02 14:06:04
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.31 / 2024-05-17 05:43:49
YARA Built-in Ruleset Version	2024.2.1.32

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	8.0.7601.17514
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	8.0.1710.11

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