MALICIOUS

Classifications: -

Threat Names: Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe**
ID	#5068021
MD5	1fb5d967f92174e0bbb15262f8cd209f
SHA1	76fbd5b88154976887b5099c21666ca3be2cd76e
SHA256	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024
File Size	6026.50 KB
Report Created	2022-08-05 16:16 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (8 rules, 9 matches)

Score	Category	Operation	Count	Classification
4/5	Defense Evasion	Obscures a file's origin	1	-
	• (Process #1) 740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe tries to delete zone identifier of file "C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe".		
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Task Scheduling	Schedules task	1	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe", to be triggered by LOGON.			
2/5	Task Scheduling	Schedules task via schtasks	1	-
	• Schedules task "Google Update" via the schtasks command line utility.			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) 740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe enables process privilege "SeDebugPrivilege". • (Process #6) svchost.exe enables process privilege "SeDebugPrivilege".			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe creates mutex with name "Local\a65c20d9-cf82-4bb4-8f7e-e90aff87b9b5".			
1/5	System Modification	Modifies operating system directory	1	-
	• (Process #1) 740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe creates file "C:\Windows\system32\Windows\RuntimeBroker.exe" in the OS directory.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe starts (process #1) 740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe with a hidden window.			

Mitre ATT&CK Matrix

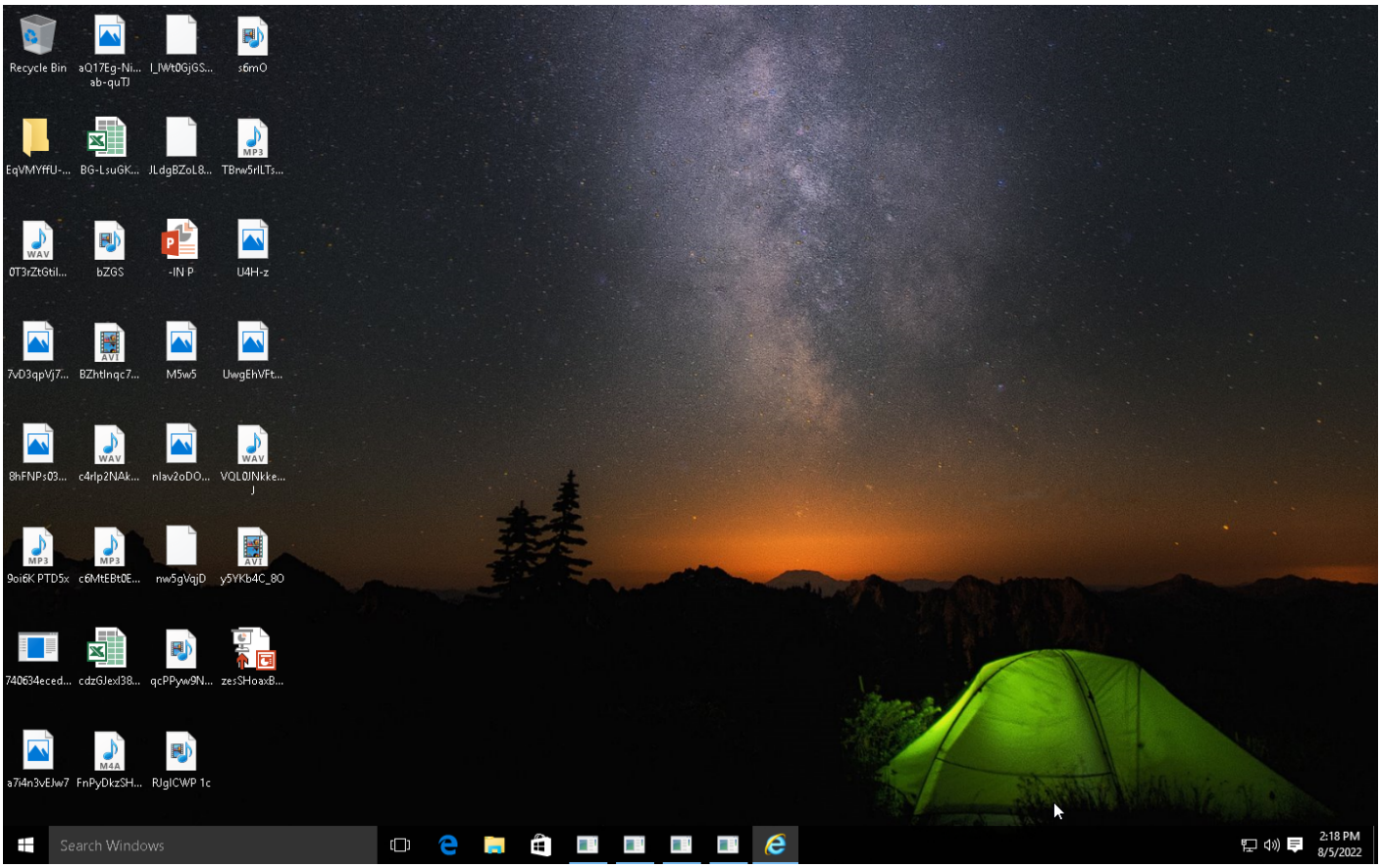
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1096 NTFS File Attributes							
				#T1143 Hidden Window							

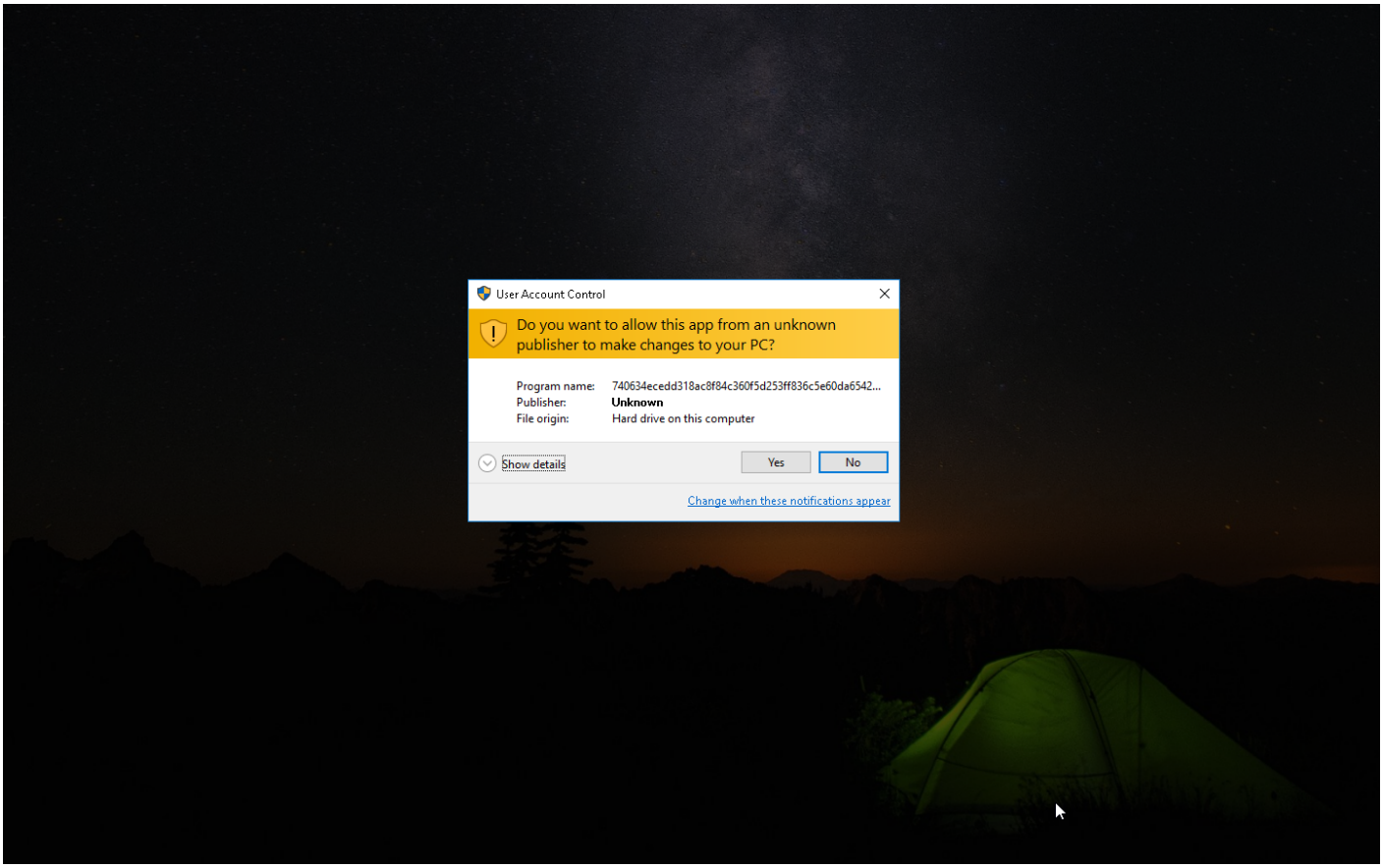
Sample Information

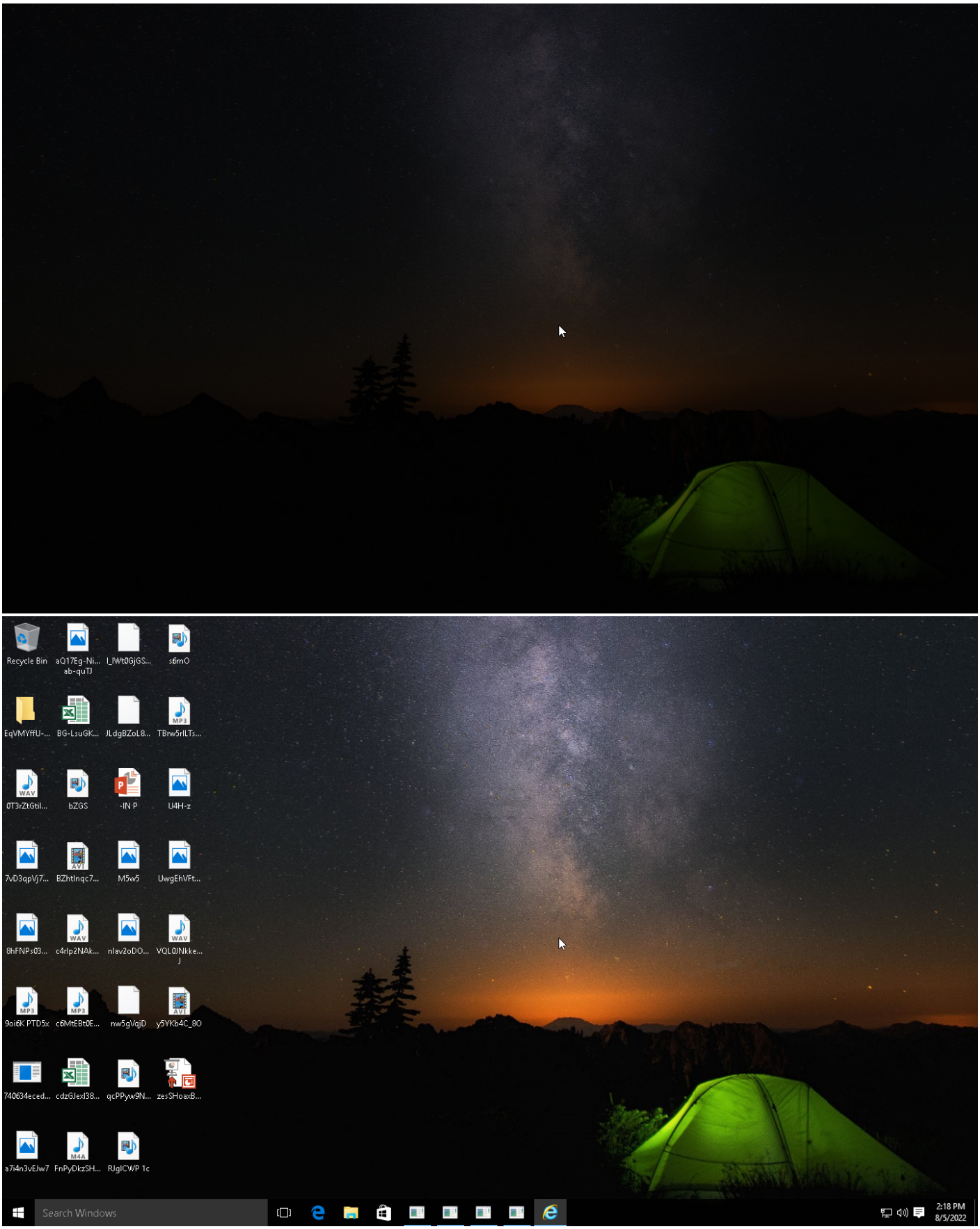
ID	#5068021
MD5	1fb5d967f92174e0bbb15262f8cd209f
SHA1	76fbd5b88154976887b5099c21666ca3be2cd76e
SHA256	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024
SSDeep	98304:5Po4eyejblyJFeBLgYcNBUsBtzOevoMIda05+8pbVTnVp8DW1db7LAm0xVHzd6Wy:640sHwwakZpX1aYGHMaBq9DR5y03HQiB
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe
File Size	6026.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 16:16 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	7
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


Recycle Bin
Search Windows
2:18 PM
8/5/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 740634ecedd318ac8f84c360f5d253ff836c5e60da6542...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

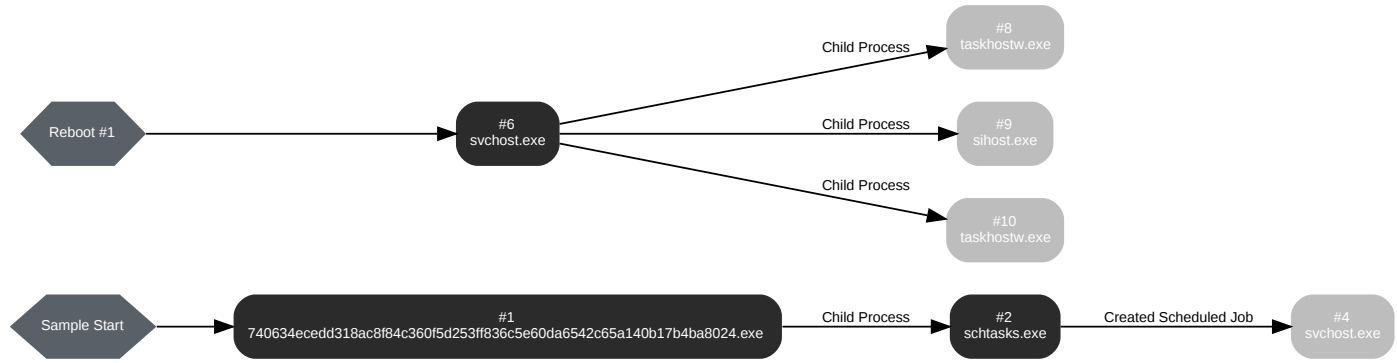
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 81709, Reason: Analysis Target
Unmonitor End Time	End Time: 161616, Reason: Terminated
Monitor duration	79.91s
Return Code	1073807364
PID	3076
Parent PID	1972
Bitness	64 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Windows\system32\Windows\RuntimeBroker.exe	6026.50 KB	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024	✖

Host Behavior

Type	Count
Registry	12
File	27
Module	22
Environment	4
-	2
User	3
Window	5
System	6
Mutex	1
Process	1

Process #2: schtasks.exe

ID	2
File Name	c:\windows\system32\schtasks.exe
Command Line	"schtasks" /create /tn "Google Update" /sc ONLOGON /tr "C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe" /rl HIGHEST /f
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 131015, Reason: Child Process
Unmonitor End Time	End Time: 136872, Reason: Terminated
Monitor duration	5.86s
Return Code	0
PID	1656
Parent PID	3076
Bitness	64 Bit

Host Behavior

Type	Count
Module	3
System	3
COM	1
File	6

Process #4: svchost.exe

ID	4
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: 134351, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 321721, Reason: Terminated by timeout
Monitor duration	187.37s
Return Code	Unknown
PID	864
Parent PID	1656
Bitness	64 Bit

Process #6: svchost.exe

ID	6
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: 208096, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 321721, Reason: Terminated by timeout
Monitor duration	113.62s
Return Code	Unknown
PID	1008
Parent PID	1656
Bitness	64 Bit

Host Behavior

Type	Count
-	4
COM	2

Process #8: taskhostw.exe

ID	8
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 241233, Reason: Child Process
Unmonitor End Time	End Time: 321721, Reason: Terminated by timeout
Monitor duration	80.49s
Return Code	Unknown
PID	1408
Parent PID	1008
Bitness	64 Bit

Process #9: sihost.exe

ID	9
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 257292, Reason: Child Process
Unmonitor End Time	End Time: 321721, Reason: Terminated by timeout
Monitor duration	64.43s
Return Code	Unknown
PID	1572
Parent PID	1008
Bitness	64 Bit

Process #10: taskhostw.exe

ID	10
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 287662, Reason: Child Process
Unmonitor End Time	End Time: 321721, Reason: Terminated by timeout
Monitor duration	34.06s
Return Code	Unknown
PID	764
Parent PID	1008
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024	C:\Windows\system32\Windows\RuntimeBroker.exe, C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	Sample File	6026.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Windows\system32\Windows\RuntimeBroker.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Windows\SYSTEM32\schtasks.exe	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\system32\Windows	Accessed File	Access, Create	CLEAN
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe:Zone.Identifier	Accessed File	Access, Delete	CLEAN
C:\Windows\system32	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe.config	Accessed File	Access	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
Local\a65c20d9-cf82-4bb4-8f7e-e90aff87b9b5	access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	CLEAN

Process

Process Name	Commandline	Verdict
740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe	"C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe"	MALICIOUS
schtasks.exe	"schtasks" /create /tn "Google Update" /sc ONLOGON /tr "C:\Users\RDhJ0CNFevzX\Desktop\740634ecedd318ac8f84c360f5d253ff836c5e60da6542c65a140b17b4ba8024.exe" /rl HIGHEST /f	SUSPICIOUS
taskhostw.exe	taskhostw.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
taskhostw.exe	taskhostw.exe SYSTEM	CLEAN
sihost.exe	sihost.exe	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.6.0
Dynamic Engine Version	4.6.0 / 07/08/2022 04:26
Static Engine Version	4.6.0.0 / 2022-07-08 03:00:22
AV Exceptions Version	4.6.1.9 / 2022-07-29 14:01:00
Link Detonation Heuristics Version	4.6.1.9 / 2022-07-29 14:01:00
Smart Memory Dumping Rules Version	4.6.1.9 / 2022-07-29 14:01:00
Config Extractors Version	4.6.1.12 / 2022-08-02 11:53:09
Signature Trust Store Version	4.6.1.9 / 2022-07-29 14:01:00
VMRay Threat Identifiers Version	4.6.1.14 / 2022-08-03 12:19:21
YARA Built-in Ruleset Version	4.6.1.10

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1001
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB
User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp

System Root	C:\Windows