MALICIOUS

Classifications: -

Threat Names: AgentTesla.v3

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe**
ID	#2100004
MD5	b78eed700665bf868771e371d2622000
SHA1	48daa093155e9eaa563f6eb537a57f940f2aa6c6
SHA256	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513
File Size	698.50 KB
Report Created	2022-05-04 12:03 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (11 rules, 14 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Agent Tesla configuration was extracted	1	Spyware
	• A configuration for Agent Tesla was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Spyware
	• Rule "AgentTesla_StringDecryption_v3" from ruleset "Malware" has matched on a memory dump for (process #7) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe modifies memory of (process #7) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe alters context of (process #7) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\gfLnSNNH.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\gfLnSNNH.exe", to be triggered by REGISTRATION.			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe starts taskhostw.exe with a hidden window. • (Process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe starts (process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe reads from (process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #7) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe enables process privilege "SeDebugPrivilege".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #7) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe resolves 49 API functions by name.			
1/5	Execution	Executes itself	1	-
	• (Process #1) 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe executes a copy of the sample at C:\Users\RDhJ0CNFevzX\AppData\Roaming\gfLnSNNH.exe.			

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
Encryption Key	Key Algorithm	qg== XOR
URL	Url Tags	https://api.telegram.org/bot5187728823:AAGLMGn_JIHiLgjLPDeSA29u69fic0Upi8Y/sendDocument Telegram
Other: Telegram Chat ID	Tags Value	Telegram 5049233732

Mitre ATT&CK Matrix

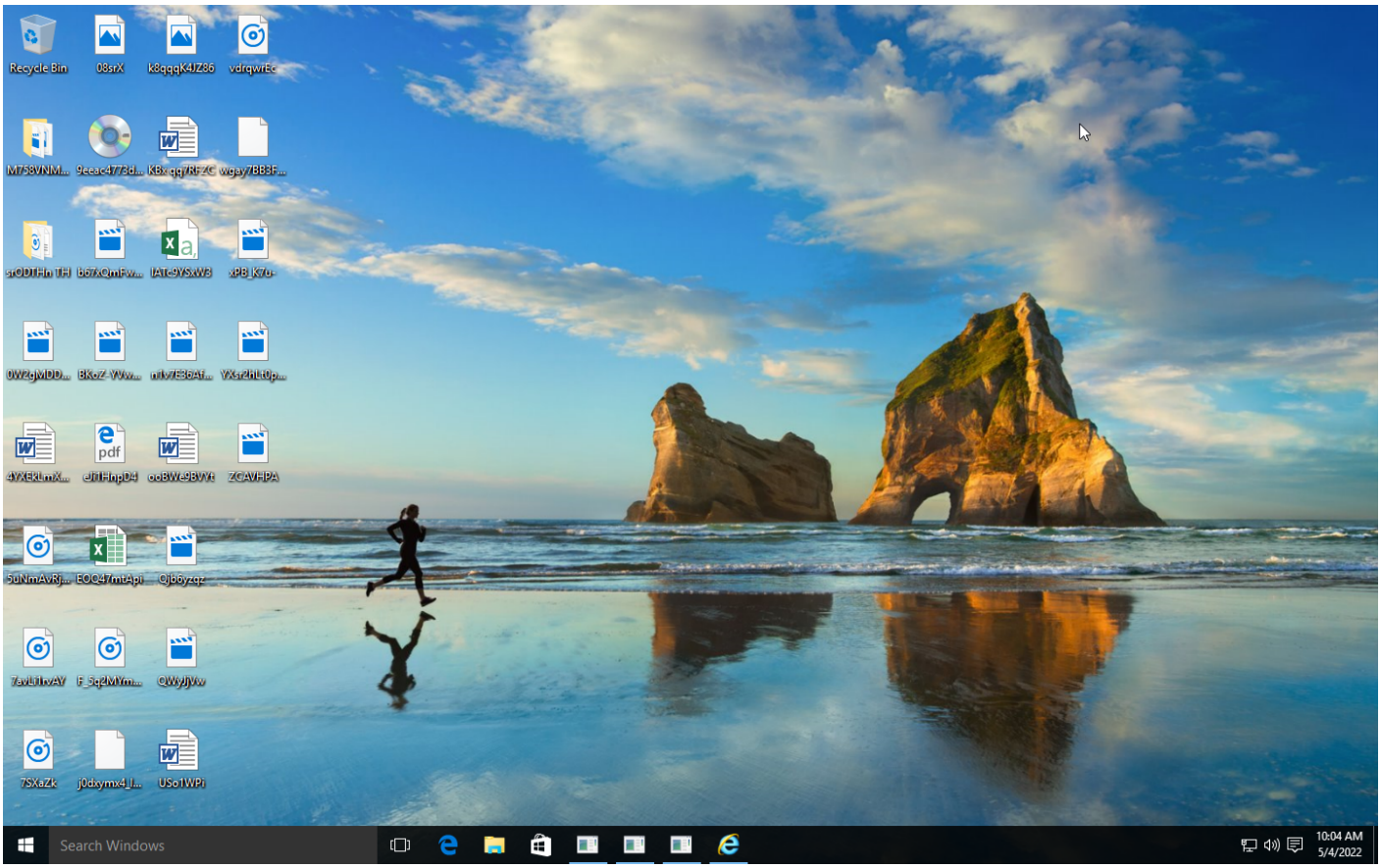
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window							
				#T1045 Software Packing							

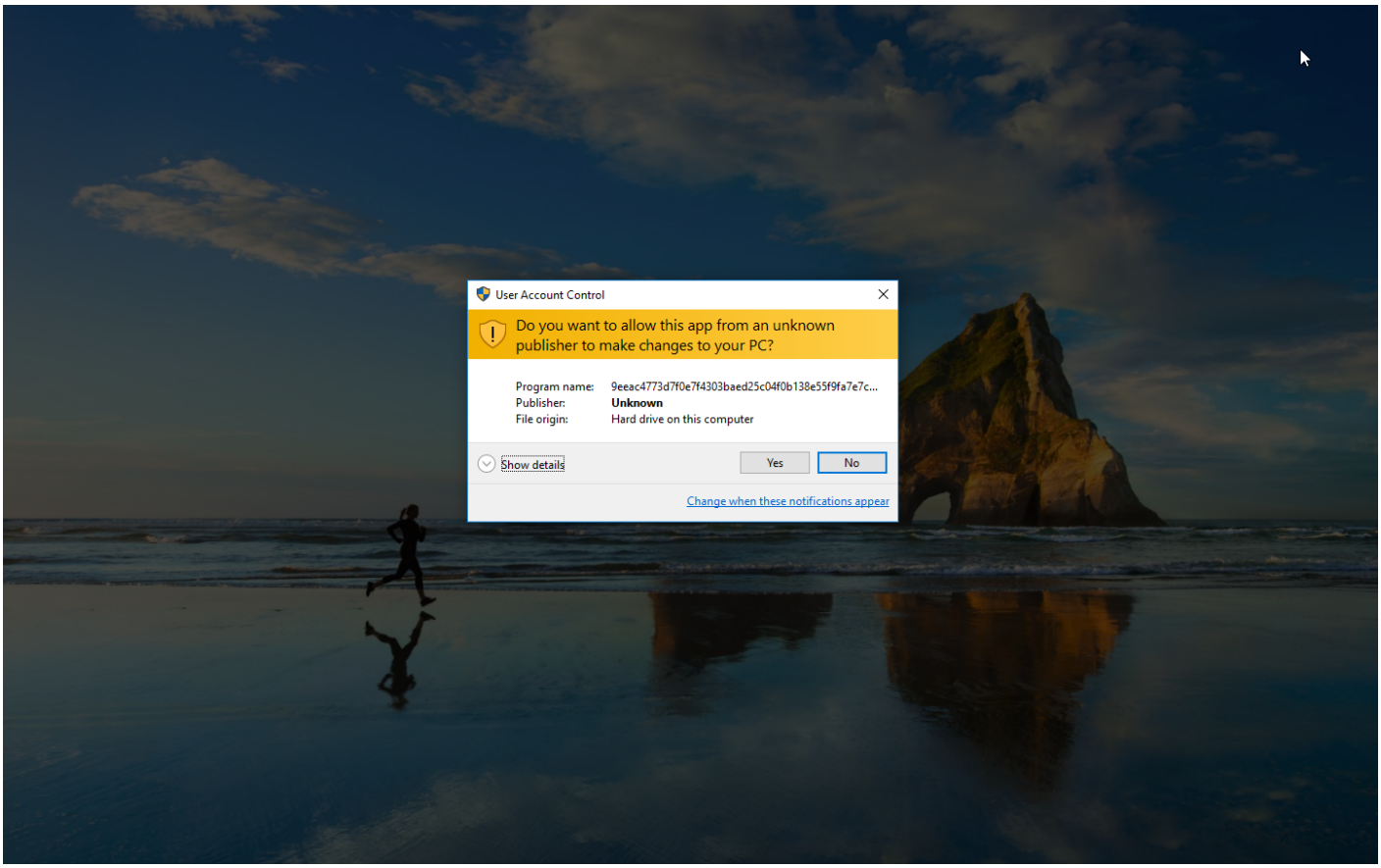
Sample Information

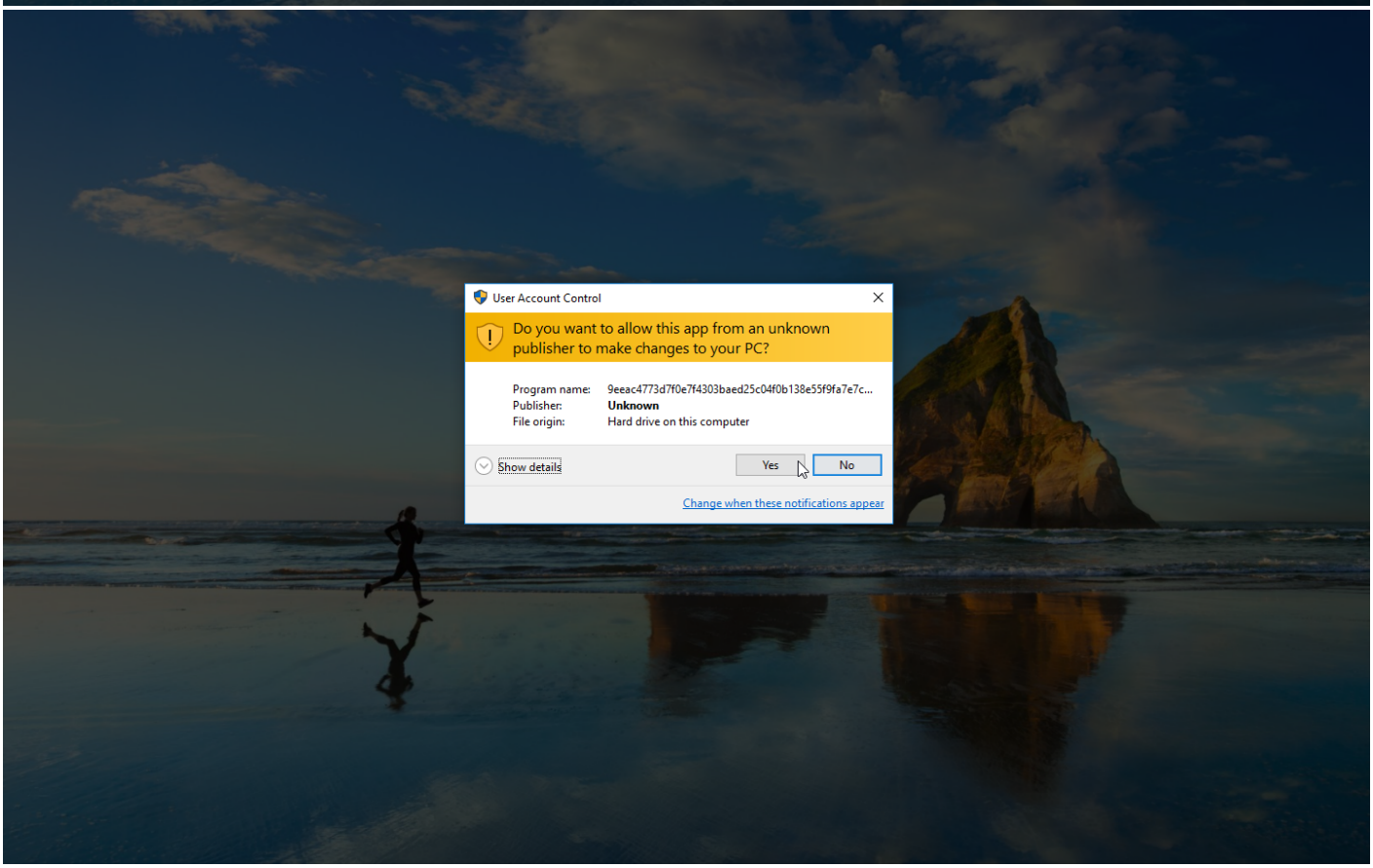
ID	#2100004
MD5	b78eed700665bf868771e371d2622000
SHA1	48daa093155e9eaa563f6eb537a57f940f2aa6c6
SHA256	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513
SSDeep	12288:+V2L2lj3hxwDvVbyP8wqEBI1sIAzYy3/w+8RqbVVte2moi2bOxNtbs5:M2p3MDvVmkwqYnlA/ltWVVtX
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe
File Size	698.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-05-04 12:03 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	11
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	1


Recycle Bin
08srX
k8qqqK4IZ86
vdrqwrEc
M758VNM...
9eeac4773d...
KBx qq7RFZC
wgay7BB3F...
sODTHn TH
b67xQmFw...
IATc9YSxW3
xPB_K7o-
0W3gWDD...
BKoZ-YVw...
mlv7E3GAf...
YXsrzhLtUp...
4YXERLmX...
eJTHnpD4
ooBWe9BWft
ZCAVHPA
5uNmAvRj...
EOQ47mtApi
Qjb0yzqz
7avLiTrvAY
F_5qdMYm...
QWyJjVw
7SXaZk
j0dxymx4_l...
USo1WPi
Search Windows
10:04 AM
5/4/2022





Screenshots truncated

NETWORK

General

0 bytes total sent

0 bytes total received

0 ports

0 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

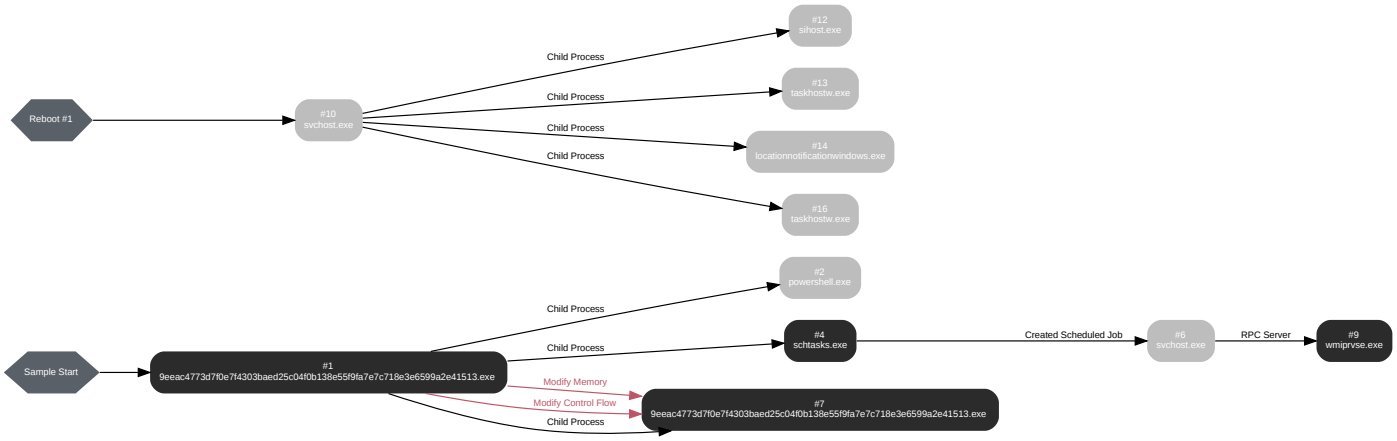
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 85365, Reason: Analysis Target
Unmonitor End Time	End Time: 202858, Reason: Terminated
Monitor duration	117.49s
Return Code	0
PID	1796
Parent PID	1864
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Roaming\gfLnSNNH.exe	698.50 KB	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpA573.tmp	1.56 KB	4d4844431fdb09c416e08786528fdc22b5e1cf105b5e26f55b99978c948deed0	✖

Host Behavior

Type	Count
Module	207
-	3
Process	3
-	7
Window	6
User	1
System	2
File	10
Registry	3

Process #2: powershell.exe

ID	2
File Name	c:\windows\syswow64\windowspowershell\v1.0\powershell.exe
Command Line	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\gfLnSNNH.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 187588, Reason: Child Process
Unmonitor End Time	End Time: 229410, Reason: Terminated
Monitor duration	41.82s
Return Code	1073807364
PID	4928
Parent PID	1796
Bitness	32 Bit

Process #4: schtasks.exe

ID	4
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gfLnSNNH" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpA573.tmp"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 188339, Reason: Child Process
Unmonitor End Time	End Time: 200561, Reason: Terminated
Monitor duration	12.22s
Return Code	0
PID	3068
Parent PID	1796
Bitness	32 Bit

Host Behavior

Type	Count
File	10
Module	3
COM	1

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: 197860, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 325448, Reason: Terminated by timeout
Monitor duration	127.59s
Return Code	Unknown
PID	864
Parent PID	3068
Bitness	64 Bit

Process #7: 9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 199999, Reason: Child Process
Unmonitor End Time	End Time: 229398, Reason: Terminated
Monitor duration	29.40s
Return Code	1073807364
PID	4520
Parent PID	1796
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	0x9e8	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	0x9e8	0x402000(4202496)	0x33c00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	0x9e8	0x436000(4415488)	0x400	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	0x9e8	0x438000(4423680)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	0x9e8	0x34a008(3448840)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	0x9e8 / 0x11b4	0x435b9e(4414366)	-	✔	1

Host Behavior

Type	Count
File	19
Module	52
COM	12
Registry	11
System	4
-	7
User	1

Process #9: wmiprvse.exe

ID	9
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: 207065, Reason: RPC Server
Unmonitor End Time	End Time: 325448, Reason: Terminated by timeout
Monitor duration	118.38s
Return Code	Unknown
PID	3828
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Registry	2

Process #10: svchost.exe

ID	10
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: 257292, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 325448, Reason: Terminated by timeout
Monitor duration	68.16s
Return Code	Unknown
PID	868
Parent PID	3068
Bitness	64 Bit

Process #12: sihost.exe

ID	12
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 283068, Reason: Child Process
Unmonitor End Time	End Time: 325448, Reason: Terminated by timeout
Monitor duration	42.38s
Return Code	Unknown
PID	1256
Parent PID	868
Bitness	64 Bit

Process #13: taskhostw.exe

ID	13
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 287894, Reason: Child Process
Unmonitor End Time	End Time: 325448, Reason: Terminated by timeout
Monitor duration	37.55s
Return Code	Unknown
PID	1316
Parent PID	868
Bitness	64 Bit

Process #14: locationnotificationwindows.exe

ID	14
File Name	c:\windows\system32\locationnotificationwindows.exe
Command Line	C:\Windows\System32\LocationNotificationWindows.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 290712, Reason: Child Process
Unmonitor End Time	End Time: 325448, Reason: Terminated by timeout
Monitor duration	34.74s
Return Code	Unknown
PID	1412
Parent PID	868
Bitness	64 Bit

Process #16: taskhostw.exe

ID	16
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 306446, Reason: Child Process
Unmonitor End Time	End Time: 325448, Reason: Terminated by timeout
Monitor duration	19.00s
Return Code	Unknown
PID	1744
Parent PID	868
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513	C:\Users\RDhJ0CNFevzX\AppData\Roaming\gfLnSNNH.exe, C:\Users\RDhJ0CNFevzX\Desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	Sample File	698.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
4d4844431fdb09c416e08786528fdc22b5e1cf105b5e26f55b99978c948deed0	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpA573.tmp	Dropped File	1.56 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\gfLnSNNH.exe	Sample File, Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe.config	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpA573.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.telegram.org/bot5187728823:AAGLMGn_JlHiLgjLPDeSA29u69fic0Upi8Y/sendDocument	-	-	-	-	MALICIOUS

Domain

Domain	IP Address	Country	Protocols	Verdict
api.telegram.org	-	-	-	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	CLEAN

Process

Process Name	Commandline	Verdict
9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe"	SUSPICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gfLnSNNH" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpA573.tmp"	SUSPICIOUS
9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9eeac4773d7f0e7f4303baed25c04f0b138e55f9fa7e7c718e3e6599a2e41513.exe"	SUSPICIOUS
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
sihost.exe	sihost.exe	CLEAN
taskhostw.exe	taskhostw.exe SYSTEM	CLEAN
locationnotificationwindows.exe	C:\Windows\System32\LocationNotificationWindows.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\gfLnSNNH.exe"	CLEAN
taskhostw.exe	taskhostw.exe	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
Malware	AgentTesla_StringDecryption_v3	Agent Tesla v3 string decryption	Memory Dump	-	Spyware	5/5

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	4.5.0
Dynamic Engine Version	4.5.0 / 04/22/2022 19:04
Static Engine Version	4.5.0.0 / 2022-04-22 17:45:13
AV Exceptions Version	4.5.0.2 / 2022-04-03 15:57:54
Link Detonation Heuristics Version	4.5.0.19 / 2022-04-20 05:46:11
Smart Memory Dumping Rules Version	4.5.0.2 / 2022-04-03 15:57:54
Config Extractors Version	4.5.0.14 / 2022-04-07 17:00:08
Signature Trust Store Version	4.5.0.2 / 2022-04-03 15:57:54
VMRay Threat Identifiers Version	4.5.0.24 / 2022-04-26 09:10:00
YARA Built-in Ruleset Version	4.5.0.2

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	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