MALICIOUS

Classifications: Spyware

Threat Names: AgentTesla.v3 Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe**
ID	#4988022
MD5	24b0be710ed42b1ec10224db8db55bf6
SHA1	597bce6e93351125632e9b92fb2ca35fca8bc75d
SHA256	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316
File Size	744.50 KB
Report Created	2022-07-25 14:21 (UTC+2)
Target Environment	win7_64_sp1_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 17 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 #5) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe modifies memory of (process #5) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe alters context of (process #5) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe", to be triggered by REGISTRATION.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe creates mutex with name "egucnpqep".			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe enables process privilege "SeDebugPrivilege". • (Process #5) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe enables process privilege "SeDebugPrivilege".			
1/5	Hide Tracks	Creates process with hidden window	4	-
	• (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe starts (process #3) powershell.exe with a hidden window. • (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe starts (process #4) schtasks.exe with a hidden window. • (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe starts (process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe with a hidden window.		
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe reads from (process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Obfuscation	Resolves API functions dynamically	1	-

Score	Category	Operation	Count	Classification
		• (Process #5) 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe resolves 51 API functions by name.		

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
Encryption Key	Key Algorithm	qg== XOR
URL	Url Tags	https://api.telegram.org/bot5573921253:AAHXKq7IrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocument Telegram
Other: Telegram Chat ID	Tags Value	Telegram 5359531870

Mitre ATT&CK Matrix

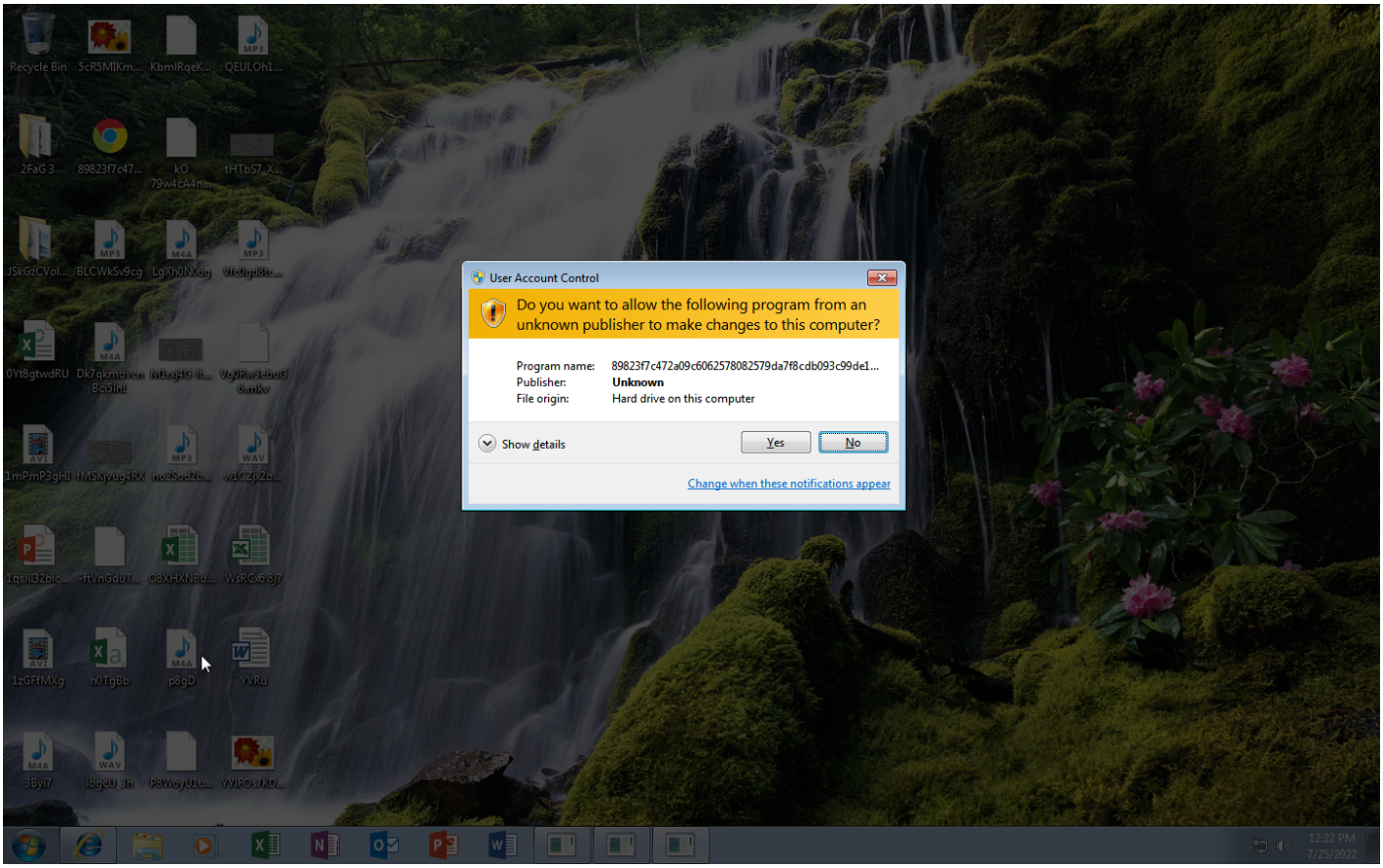
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window							
				#T1045 Software Packing							

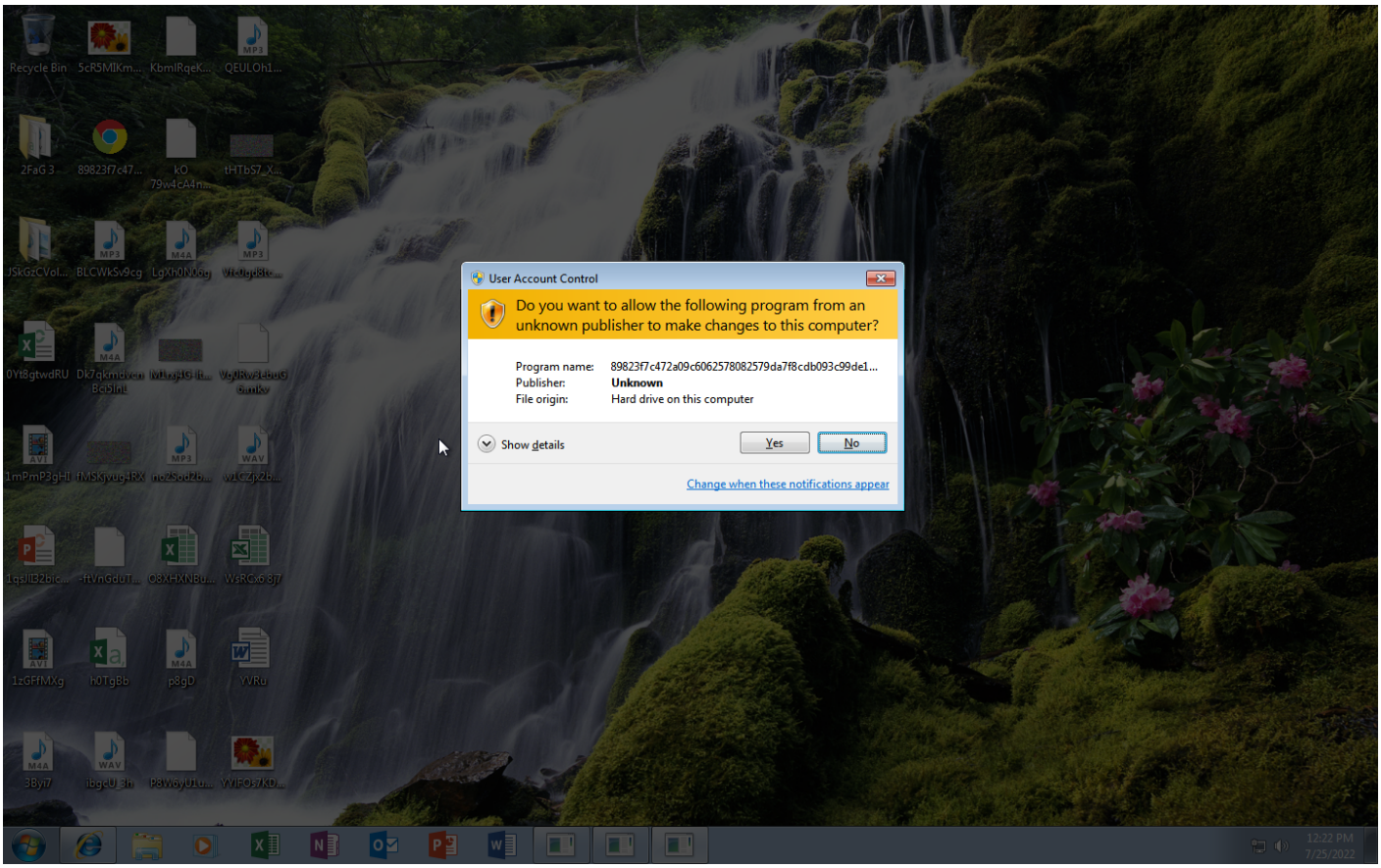
Sample Information

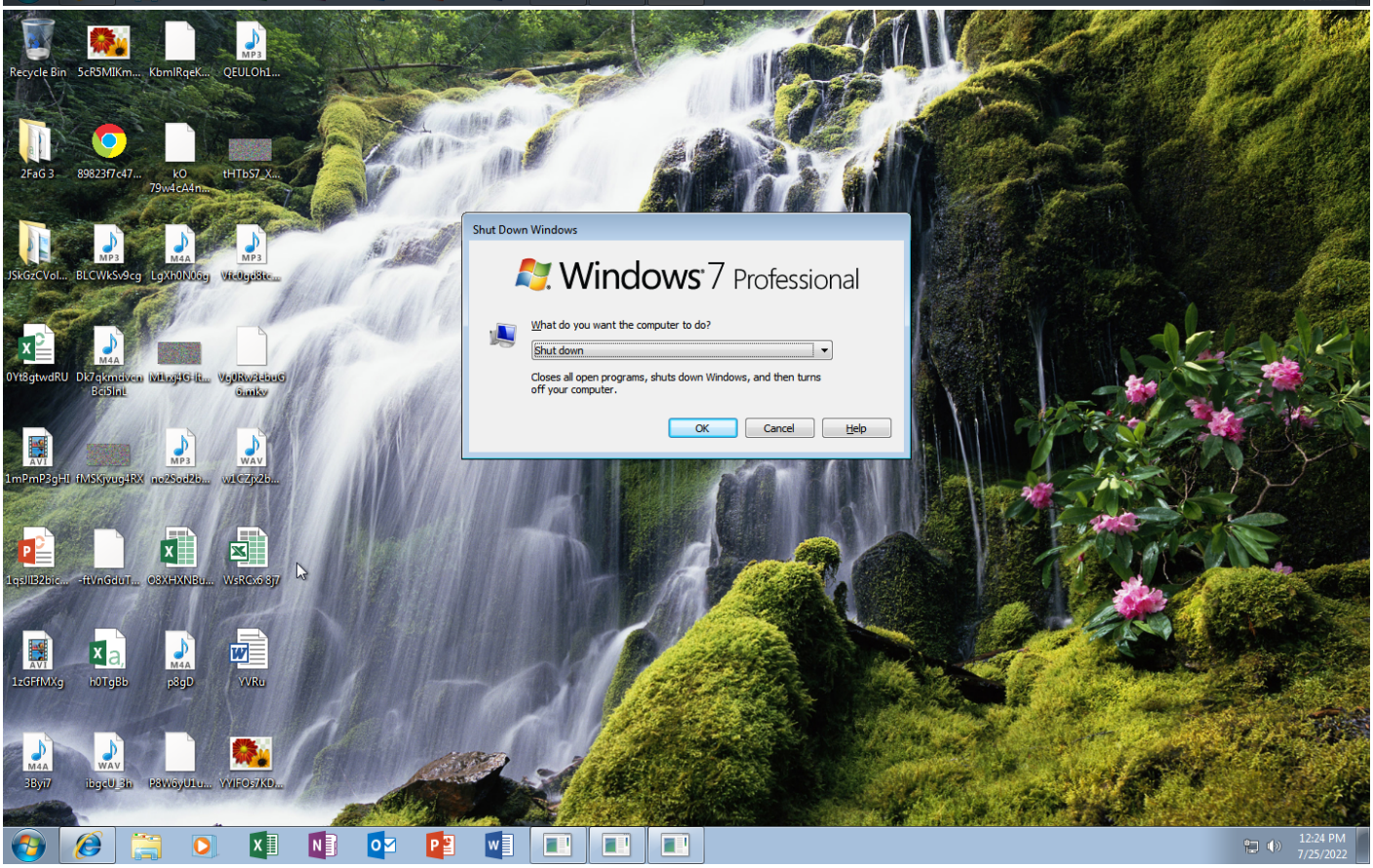
ID	#4988022
MD5	24b0be710ed42b1ec10224db8db55bf6
SHA1	597bce6e93351125632e9b92fb2ca35fca8bc75d
SHA256	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316
SSDeep	12288:AiekMj/31humhJGu/8k9kKuB/04ZZmz3Cr/KNdS2iyNAlCj+:Fcnumiu5kKMc4Lu3rNYwSlCS
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe
File Size	744.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-07-25 14:21 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	9
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


User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: 89823f7c472a09c6062578082579da7f8cdb093c99de1...
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

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

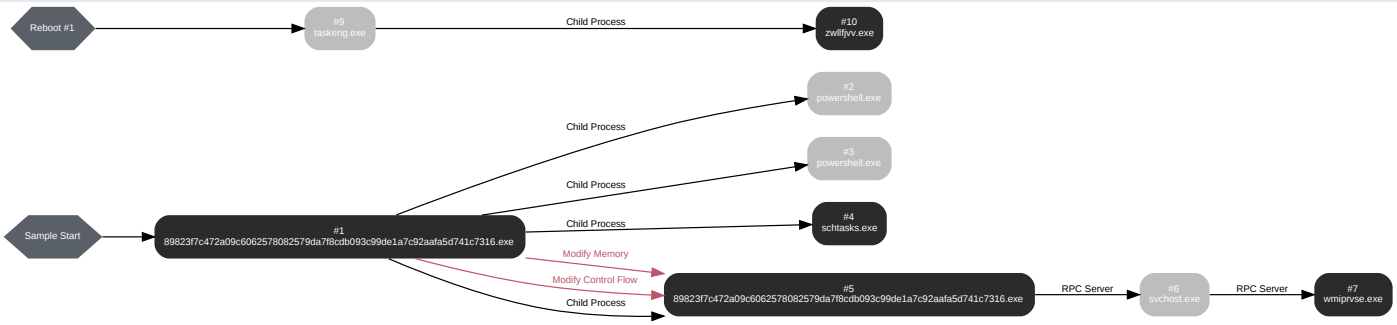
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe

ID	1
File Name	c:\users\keecfmwgj\desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 46778, Reason: Analysis Target
Unmonitor End Time	End Time: 157522, Reason: Terminated
Monitor duration	110.74s
Return Code	0
PID	2512
Parent PID	1928
Bitness	32 Bit

Dropped Files (4)

File Name	File Size	SHA256	YARA Match
-	108.45 KB	8186ee97b83e9ebaaad411ee91050beb5ecdafc34fd88f0d4e0b318d6654bcb6	✖
-	8.03 KB	790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	✖
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9370.tmp	1.56 KB	f76019ef7e45f262e57b72ba801065cb11d5f64896056c84d309296f03e96c51	✖
C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	744.50 KB	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316	✖

Host Behavior

Type	Count
Registry	4
File	29
Module	37
Window	6
Mutex	2
User	2
System	4
Process	4
-	3
-	7

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\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 149059, Reason: Child Process
Unmonitor End Time	End Time: 180422, Reason: Terminated
Monitor duration	31.36s
Return Code	1073807364
PID	2744
Parent PID	2512
Bitness	32 Bit

Process #3: powershell.exe

ID	3
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\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150213, Reason: Child Process
Unmonitor End Time	End Time: 179949, Reason: Terminated
Monitor duration	29.74s
Return Code	1073807364
PID	2916
Parent PID	2512
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\zwLLFjVv" /XML "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9370.tmp"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 150356, Reason: Child Process
Unmonitor End Time	End Time: 155214, Reason: Terminated
Monitor duration	4.86s
Return Code	0
PID	1464
Parent PID	2512
Bitness	32 Bit

Host Behavior

Type	Count
System	2
Module	7
COM	1
File	9

Process #5: 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe

ID	5
File Name	c:\users\keecfmwgj\desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe
Command Line	"C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe"
Initial Working Directory	C:\Users\kEecfMwgj\Desktop\
Monitor Start Time	Start Time: 154709, Reason: Child Process
Unmonitor End Time	End Time: 179881, Reason: Terminated
Monitor duration	25.17s
Return Code	1073807364
PID	2232
Parent PID	2512
Bitness	32 Bit

Injection Information (6)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\keecfmwgj\desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	0x9d4	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	0x9d4	0x402000(4202496)	0x33e00	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	0x9d4	0x436000(4415488)	0x600	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	0x9d4	0x438000(4423680)	0x200	✔	1
Modify Memory	#1: c:\users\keecfmwgj\desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	0x9d4	0x7efde008(2130567176)	0x4	✔	1
Modify Control Flow	#1: c:\users\keecfmwgj\desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	0x9d4 / 0xa20	0x435cce(4414670)	-	✔	1

Host Behavior

Type	Count
-	7
Registry	41
File	19
User	1
Module	62
System	4
COM	12

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: 161683, Reason: RPC Server
Unmonitor End Time	End Time: 286896, Reason: Terminated by timeout
Monitor duration	125.21s
Return Code	Unknown
PID	864
Parent PID	2232
Bitness	64 Bit

Process #7: wmiprvse.exe

ID	7
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: 161683, Reason: RPC Server
Unmonitor End Time	End Time: 286896, Reason: Terminated by timeout
Monitor duration	125.21s
Return Code	Unknown
PID	2540
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	1

Process #9: taskeng.exe

ID	9
File Name	c:\windows\system32\taskeng.exe
Command Line	taskeng.exe {2B54E3AB-81FE-4D04-A684-ECB55DA39E7A} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 249971, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 286896, Reason: Terminated by timeout
Monitor duration	36.92s
Return Code	Unknown
PID	1288
Parent PID	1464
Bitness	64 Bit

Process #10: zwllfjvv.exe

ID	10
File Name	c:\users\keecfmwgj\appdata\roaming\zwllfjvv.exe
Command Line	C:\Users\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 252432, Reason: Child Process
Unmonitor End Time	End Time: 286896, Reason: Terminated by timeout
Monitor duration	34.46s
Return Code	Unknown
PID	1372
Parent PID	1288
Bitness	32 Bit

Host Behavior

Type	Count
Registry	4
File	20
Module	11
Window	4

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316	C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe, C:\Users\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe	Sample File	744.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
8186ee97b83e9ebaaad411ee91050beb5ecdafc34fd88f0d4e0b318d6654bcb6	-	Dropped File	108.45 KB	application/octet-stream	-	CLEAN
790a6af00576b6ee07663cf571a92e5b72379c9d24f3599af1fa9fec8aeb168a	-	Dropped File	8.03 KB	application/octet-stream	-	CLEAN
f76019ef7e45f262e57b72ba801065cb11d5f64896056c84d309296f03e96c51	C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9370.tmp	Dropped File	1.56 KB	text/xml	Access, Create, Delete, Read, Write	CLEAN
b5a21327195e386b76f3b3342150cd99ce579fa406e733e2a4952a61eabc5330	-	Extracted File	7.59 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
System Paging File	Accessed File	Access	CLEAN
c:\users\keecfmwgj\appdata\local\gdipfontcachev1.dat	Dropped File	-	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe.config	Accessed File	Access	CLEAN
C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9370.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.telegram.org/bot5573921253:AAHXKq7lrmioCzUGP-9p7lopfbVX0A_ZdQA/sendDocument	-	-	-	-	MALICIOUS

Domain

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

Mutex

Name	Operations	Parent Process Name	Verdict
egucnpqep	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseHttpPipeliningAndBufferPooling	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowAllUriEncodingExpansion	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseSafeSynchronousClose	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseHttpPipeliningAndBufferPooling	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.AllowDangerousUnicodeDecompositions	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	zwllfjvv.exe, 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SystemDefaultTlsVersions	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictRfcInterimResponseHandling	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseSafeSynchronousClose	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	zwllfjvv.exe, 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.RequireCertificateEKUs	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowDangerousUnicodeDecompositions	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Uri.UseStrictIPv6AddressParsing	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\UseStrictIPv6AddressParsing	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	zwllfjvv.exe, 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\WMIDisableCOMSecurity	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\RequireCertificateEKUs	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\AllowAllUriEncodingExpansion	read, access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.UseStrictRfcInterimResponseHandling	access	89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	zwllfjvv.exe, 89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	CLEAN

Process

Process Name	Commandline	Verdict
89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	"C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe"	MALICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\zwLLFjVv" /XML "C:\Users\kEecfMwgj\AppData\Local\Temp\tmp9370.tmp"	SUSPICIOUS
89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe	"C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe"	SUSPICIOUS
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\kEecfMwgj\Desktop\89823f7c472a09c6062578082579da7f8cdb093c99de1a7c92aafa5d741c7316.exe"	CLEAN
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe"	CLEAN
taskeng.exe	taskeng.exe {2B54E3AB-81FE-4D04-A684-ECB55DA39E7A} S-1-5-21-4219442223-4223814209-3835049652-1000:Q9IATRKPRH\kEecfMwgj:Interactive:LUA[1]	CLEAN
zwllfjvv.exe	C:\Users\kEecfMwgj\AppData\Roaming\zwLLFjVv.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	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	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	VPN DE starvpn
Network Config Name	VPN DE starvpn

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	4.6.0.1 / 2022-07-04 05:54:12
Link Detonation Heuristics Version	4.6.0.3 / 2022-07-11 12:34:44
Smart Memory Dumping Rules Version	4.6.0.1 / 2022-07-04 05:54:12
Config Extractors Version	4.6.0.5 / 2022-07-18 16:31:08
Signature Trust Store Version	4.6.0.1 / 2022-07-04 05:54:12
VMRay Threat Identifiers Version	4.6.0.5 / 2022-07-18 16:31:08
YARA Built-in Ruleset Version	4.6.0.5

Software Information

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

System Information

Sample Directory	C:\Users\kEecfMwgj\Desktop
Computer Name	Q9IATRKPRH
User Domain	Q9IATRKPRH
User Name	kEecfMwgj
User Profile	C:\Users\kEecfMwgj
Temp Directory	C:\Users\KEECFM~1\AppData\Local\Temp

System Root	C:\Windows