MALICIOUS

Classifications: Spyware

Threat Names: AgentTesla.v3 Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe**
ID	#5067850
MD5	f7c9cf1410373a60a5c5a5e02aa4bd3c
SHA1	97cf7689f3b6dfd0efd37e7f16aa1bd2cfe537de
SHA256	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245
File Size	782.50 KB
Report Created	2022-08-05 15:37 (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) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.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) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe modifies memory of (process #7) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe alters context of (process #7) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\kqruryFrIFc.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\kqruryFrIFc.exe", to be triggered by REGISTRATION.			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #1) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe starts (process #3) schtasks.exe with a hidden window. • (Process #1) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe starts (process #1) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe reads from (process #1) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.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) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe enables process privilege "SeDebugPrivilege".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #7) b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe resolves 49 API functions by name.			

Malware Configuration: AgentTesla

Metadata	Key	Extracted Value
Encryption Key	Key Algorithm	qg== XOR
URL	Url Tags	https://api.telegram.org/bot5589784704:AAHKB3hx6EncDiLmSpjVqiBsp072Mevw-S8/sendDocument Telegram
Other: Telegram Chat ID	Tags Value	Telegram 1428355250

Mitre ATT&CK Matrix

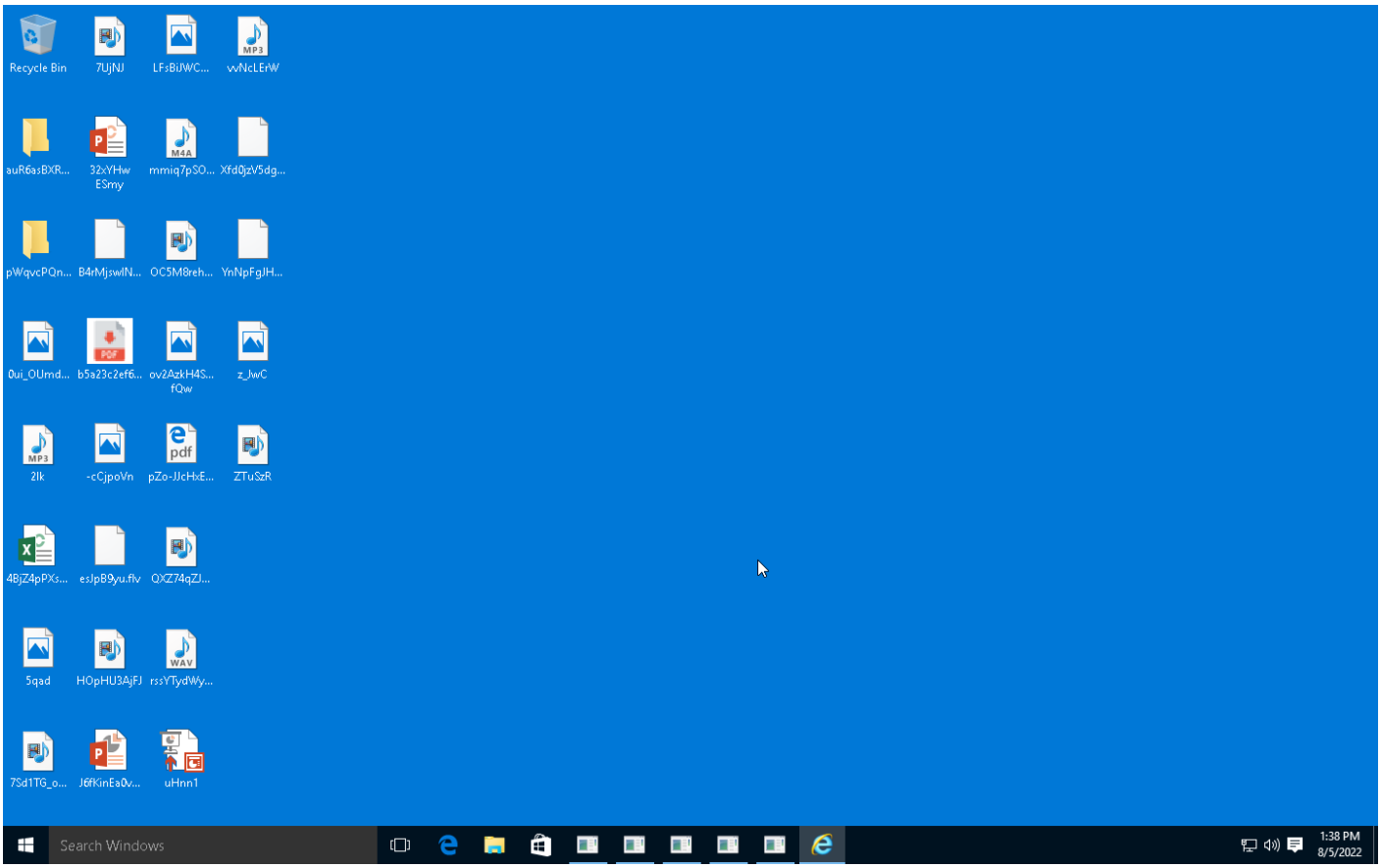
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window							
				#T1045 Software Packing							

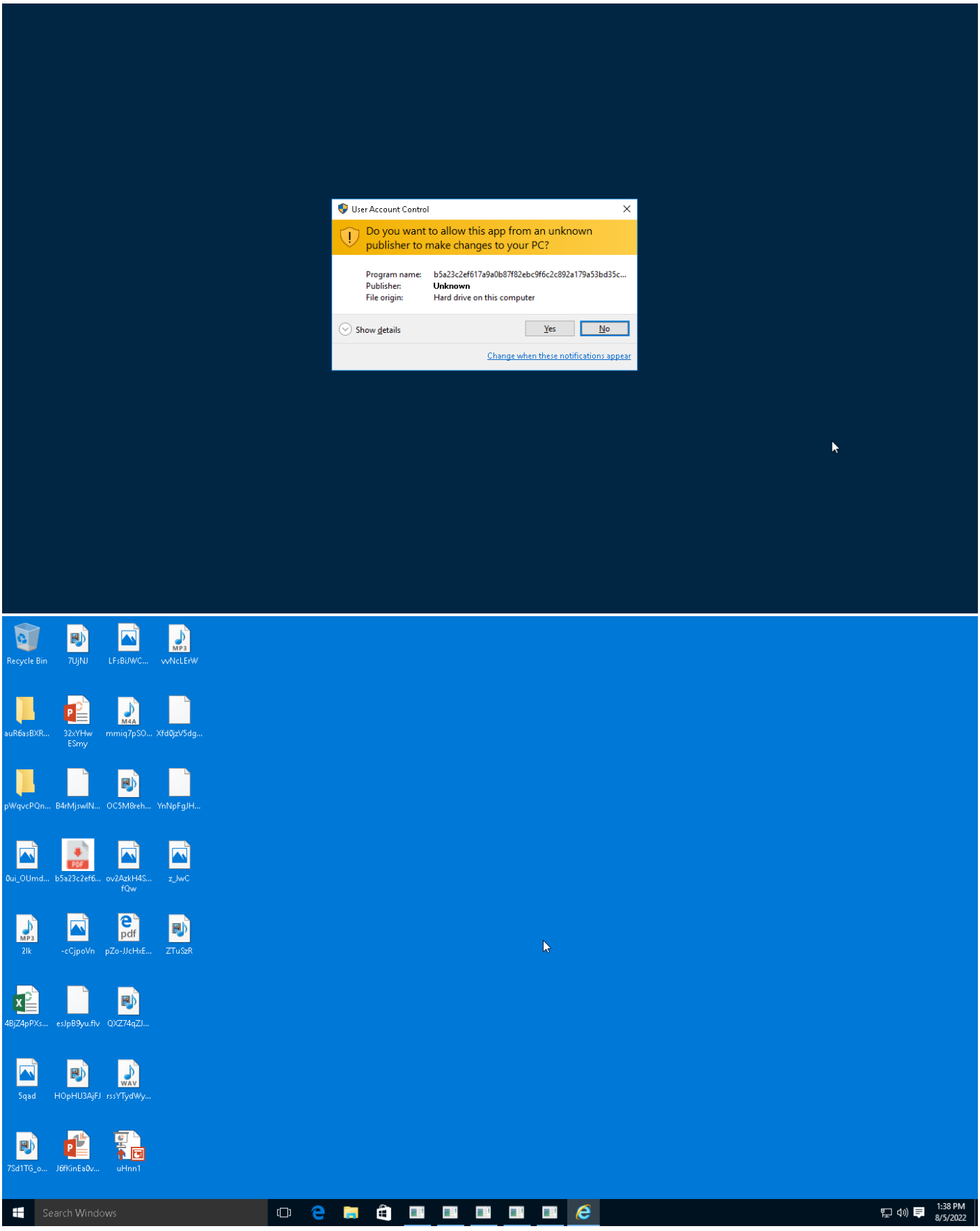
Sample Information

ID	#5067850
MD5	f7c9cf1410373a60a5c5a5e02aa4bd3c
SHA1	97cf7689f3b6dfd0efd37e7f16aa1bd2cfe537de
SHA256	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245
SSDeep	12288:hk2xg+ugGp2SrKUhxw3YjusvkRgutp43ARSepVIAnlFxCn9nLtzHeb:y2xgP01D3tRgutOzepVIAlLGnc
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe
File Size	782.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 15:37 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	8
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
7UjNJ
LFsBiJWC...
vvNcLErW
auR6asBXR...
32xYHw ESmy
mmiq7pSO...
Xfd0jzV5dg...
pWqvcPQn...
B4rMjswIN...
OC5M8reh...
YnNpFgJH...
0ui_OUmd...
b5a23c2ef6...
ov2AzkH4S... fQw
z_JwC
2lk
-cCjpoVn
pZo-JJcHxE...
ZTuSzR
4BjZ4pPXs...
esJpB9yu.flv
QXZ74qZJ...
5qad
HOpHU3AjFJ
rssYTydWy...
7Sd1TG_o...
J6fKinEa0v...
uHnn1
Search Windows
1:38 PM
8/5/2022



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

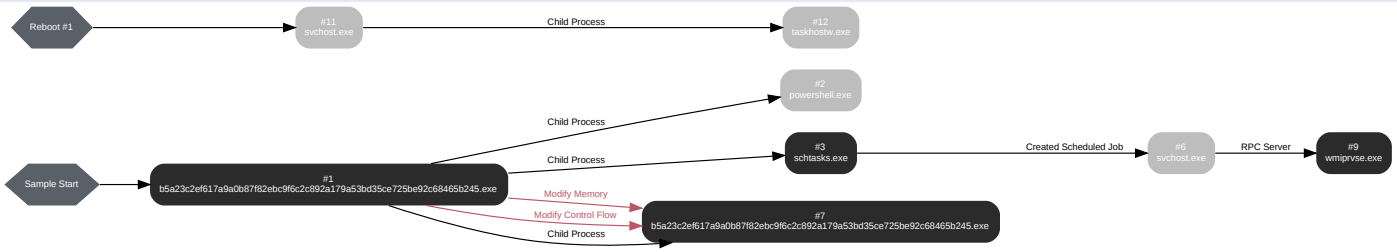
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 61268, Reason: Analysis Target
Unmonitor End Time	End Time: 208100, Reason: Terminated
Monitor duration	146.83s
Return Code	0
PID	824
Parent PID	1972
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	782.50 KB	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp621.tmp	1.56 KB	46206dae5258d36c346b9203feadd3e1e31d637c0d96f2c2a49bb2a1bbff1f73	✖

Host Behavior

Type	Count
Registry	4
Module	1070
Window	337
System	298
File	28
User	1
Process	3
-	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\RDhJ0CNFevzX\AppData\Roaming\kqruryFrIFc.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 183325, Reason: Child Process
Unmonitor End Time	End Time: 228220, Reason: Terminated
Monitor duration	44.90s
Return Code	1073807364
PID	1204
Parent PID	824
Bitness	32 Bit

Process #3: schtasks.exe

ID	3
File Name	c:\windows\syswow64\schtasks.exe
Command Line	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\kqruryFrIFc" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp621.tmp"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 183899, Reason: Child Process
Unmonitor End Time	End Time: 203540, Reason: Terminated
Monitor duration	19.64s
Return Code	0
PID	1528
Parent PID	824
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
COM	1
File	10

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: 201012, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 301372, Reason: Terminated by timeout
Monitor duration	100.36s
Return Code	Unknown
PID	864
Parent PID	1528
Bitness	64 Bit

Process #7: b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 203768, Reason: Child Process
Unmonitor End Time	End Time: 228538, Reason: Terminated
Monitor duration	24.77s
Return Code	1073807364
PID	1752
Parent PID	824
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\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	0x10b4	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	0x10b4	0x402000(4202496)	0x33e00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	0x10b4	0x436000(4415488)	0x600	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	0x10b4	0x438000(4423680)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	0x10b4	0x277008(2584584)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	0x10b4 / 0xae0	0x435cde(4414686)	-	✔	1

Host Behavior

Type	Count
-	7
Registry	17
File	19
User	1
Module	54
System	4
COM	12

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: 213853, Reason: RPC Server
Unmonitor End Time	End Time: 301372, Reason: Terminated by timeout
Monitor duration	87.52s
Return Code	Unknown
PID	4464
Parent PID	864
Bitness	64 Bit

Host Behavior

Type	Count
System	1

Process #11: svchost.exe

ID	11
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: 260432, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 301372, Reason: Terminated by timeout
Monitor duration	40.94s
Return Code	Unknown
PID	864
Parent PID	1528
Bitness	64 Bit

Process #12: taskhostw.exe

ID	12
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 295048, Reason: Child Process
Unmonitor End Time	End Time: 301372, Reason: Terminated by timeout
Monitor duration	6.32s
Return Code	Unknown
PID	1348
Parent PID	864
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245	C:\Users\RDhJ0CNFevzX\Desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\kqruryFrIFc.exe	Sample File	782.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
46206dae5258d36c346b9203feadd3e1e31d637c0d96f2c2a49bb2a1bbff1f73	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp621.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\kqruryFrIFc.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe.config	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp621.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
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

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://api.telegram.org/bot5589784704:AAHKB3hx6EncDiLmSpjVqiBsp072Mevw-S8/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\.NETFramework\DbgManagedDebugger	read, access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	read, access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	read, access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SchSendAuxRecord	access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\System.Net.ServicePointManager.SecurityProtocol	access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	read, access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchSendAuxRecord	read, access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	CLEAN

Process

Process Name	Commandline	Verdict
b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	"C:\Users\RDhJ0CNFevzX\Desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe"	MALICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\kqruryFrIFc" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp621.tmp"	SUSPICIOUS
b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe	"C:\Users\RDhJ0CNFevzX\Desktop\b5a23c2ef617a9a0b87f82ebc9f6c2c892a179a53bd35ce725be92c68465b245.exe"	SUSPICIOUS
taskhostw.exe	taskhostw.exe SYSTEM	CLEAN
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\kqruryFrIFc.exe"	CLEAN
wmiprvse.exe	C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	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	4.6.0
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