MALICIOUS

Classifications: Backdoor

Threat Names: Mal/Generic-S | AsyncRAT.v057B | AsyncRAT | Mal/HTMLGen-A

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe**
ID	#5070161
MD5	44e407b3de4a9865ab747bdca810b0b9
SHA1	6eb199e6837432d8acb98c03b22277f340726372
SHA256	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5
File Size	606.50 KB
Report Created	2022-08-06 00:04 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (13 rules, 17 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	AsyncRAT configuration was extracted	1	Backdoor
	• A configuration for AsyncRAT was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	2	Backdoor
	• Rule "AsyncRAT" from ruleset "RATs" has matched on a memory dump for (process #7) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe. • Rule "AsyncRAT" from ruleset "RATs" has matched on a code dump for (process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
4/5	Reputation	Contacts known malicious IP address	1	-
	• Reputation analysis labels the contacted IP address 91.193.75.135 as Mal/HTMLGen-A.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe modifies memory of (process #7) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe alters context of (process #7) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe.			
2/5	Task Scheduling	Schedules task	2	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\RhFYnHFgJ.exe", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\RhFYnHFgJ.exe", to be triggered by REGISTRATION.			
1/5	Hide Tracks	Creates process with hidden window	3	-
	• (Process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe starts (process #4) schtasks.exe with a hidden window. • (Process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe starts (process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe reads from (process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Mutex	Creates mutex	1	-
	• (Process #7) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe creates mutex with name "AsyncMutex_6SI8OkPnk".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #7) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe opens an outgoing TCP connection to host "91.193.75.135:3030".			

Score	Category	Operation	Count	Classification
1/5	Network Connection	Tries to connect using an uncommon port	1	-

• (Process #7) da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe tries to connect to TCP port 3030 at 91.193.75.135.

Malware Configuration: AsyncRAT

Metadata	Key	Extracted Value
Version	Value	0.5.7B
Socket	Address Port Network Protocol C2 Listen	91.193.75.135 3030 tcp ✔ ✖
Mutex	Value	AsyncMutex_6SI8OkPnk
Interval	Tags Value	Delay 3.0
Mission ID	Value	Default
Other: Install	Value	✖
Other: Key	Tags Value	PBKDF2 Input Password 1Ba6XzwjYQzIX4shYeIo0qFnPymebjFx
Other: Salt	Value	v+seVvvNlzuyGQIkMKV4QwA9VkTSHmK51PGA5+bDOUE=
Other: Certificate	Value	MIIE8jCCAtqgAwIBAgIQAM+RaVeeMATrO06o/lu9FzANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZ…
Other: Serversignature	Value	T6Cy4F1d0H+vsuC6OwFFvzu/FhnU0g4HQz0cR8wFp4+VfIN/nUfqYFGHZHNAiLbGOQ6AJTzMIsq/evpX6xJc0Jj5xRtrDxVhn…
Other: Anti Analysis Enabled	Value	✖
Other: BDOS Enabled	Value	✖

Mitre ATT&CK Matrix

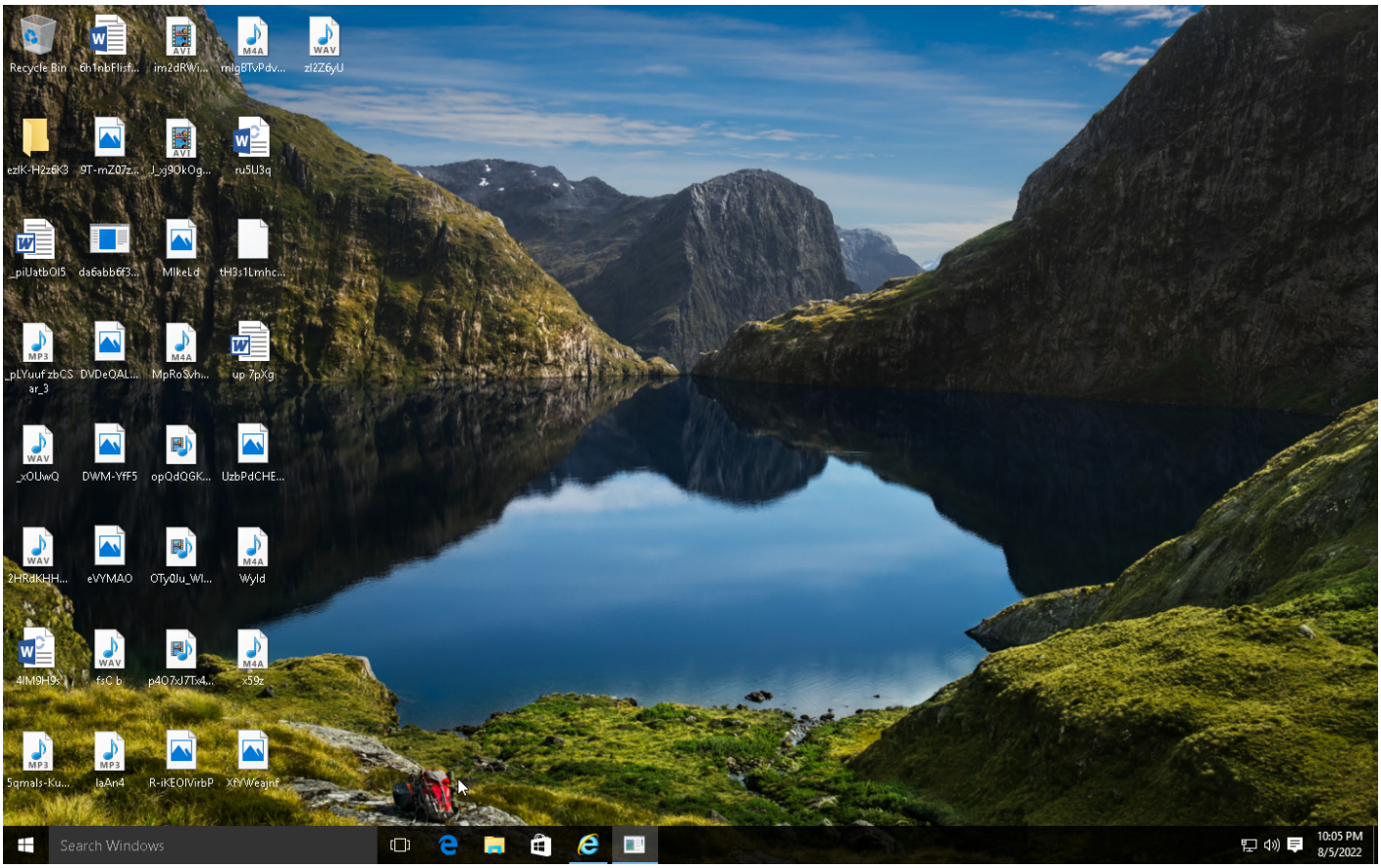
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window					#T1065 Uncommonly Used Port		
				#T1045 Software Packing							

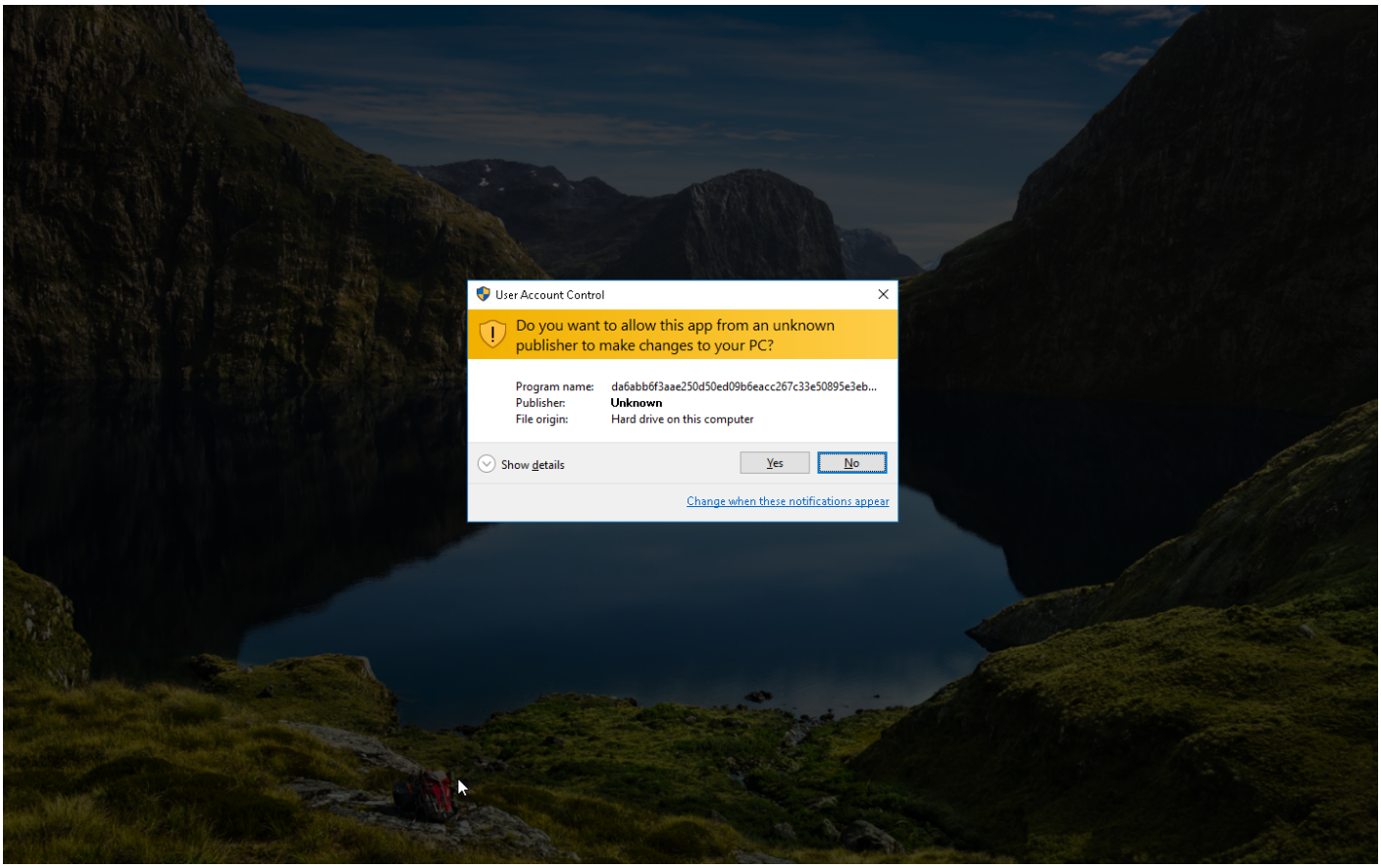
Sample Information

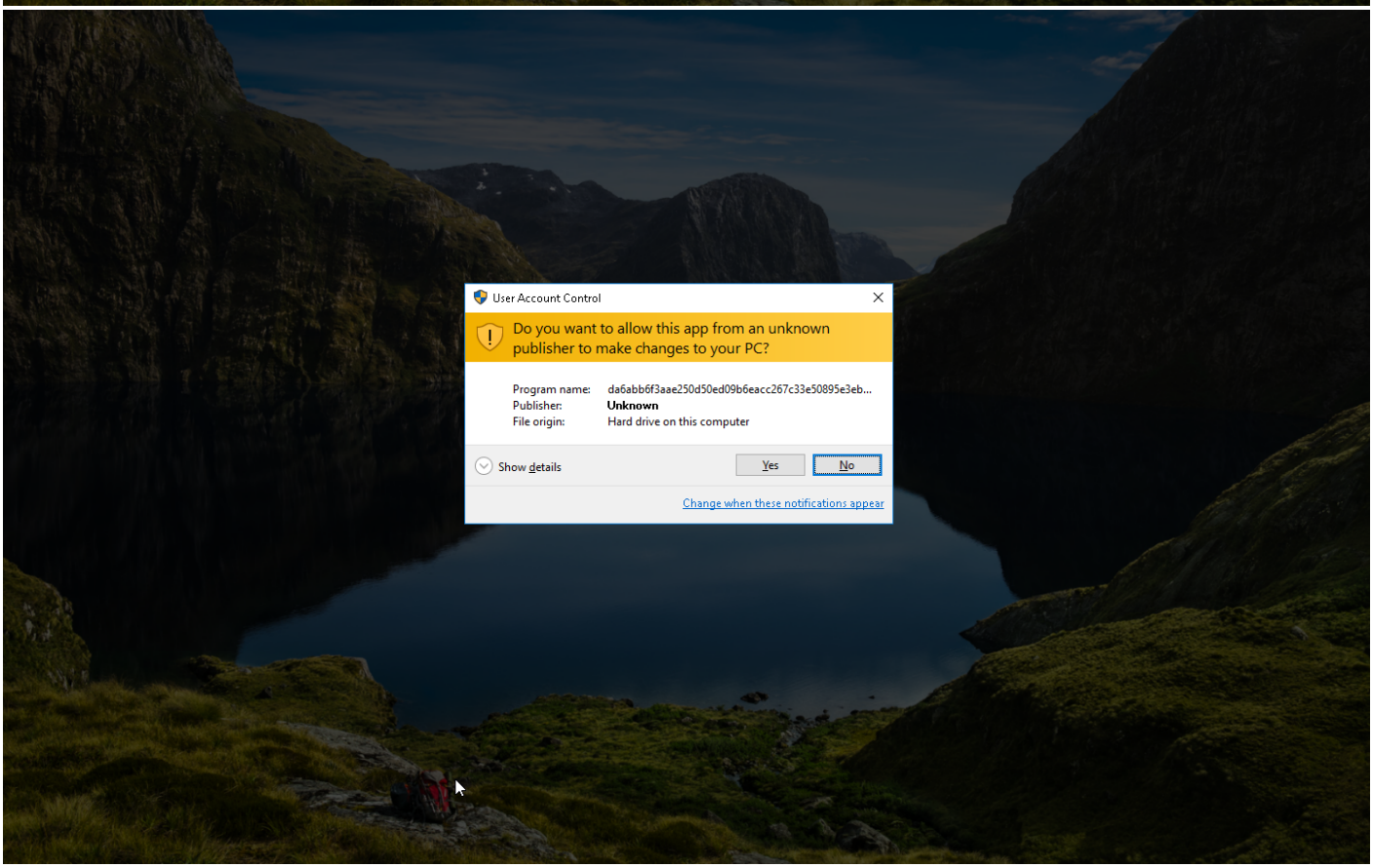
ID	#5070161
MD5	44e407b3de4a9865ab747bdca810b0b9
SHA1	6eb199e6837432d8acb98c03b22277f340726372
SHA256	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5
SSDeep	12288:4H2iNSg6SKlpxxDAE7Mn3cs9OWvHoFiPEwjlk2Y/gbb:81SLlpxx8EEc85oFaj22p
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe
File Size	606.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-06 00:04 (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	2


Recycle Bin
Search Windows
10:05 PM
8/5/2022





Screenshots truncated

NETWORK

General

304 bytes total sent

240 bytes total received

1 ports 3030

1 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

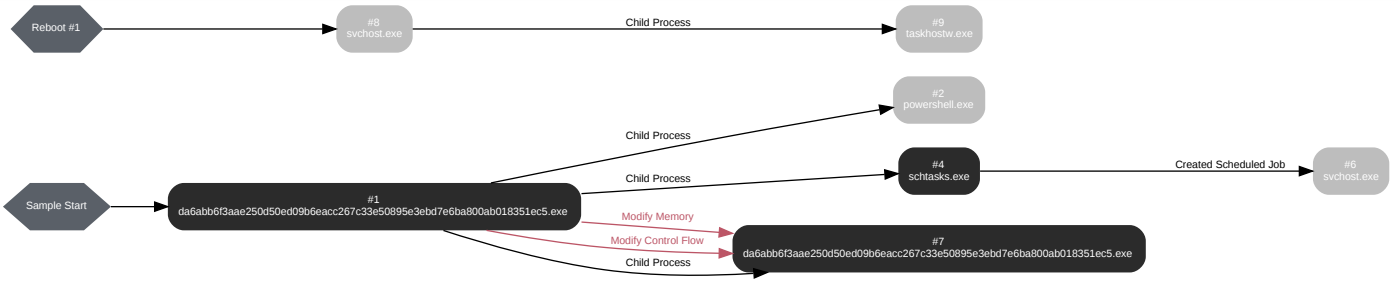
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 72649, Reason: Analysis Target
Unmonitor End Time	End Time: 209259, Reason: Terminated
Monitor duration	136.61s
Return Code	0
PID	5004
Parent PID	1972
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	606.50 KB	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpF9CA.tmp	1.56 KB	7ad7f1c3663eddd7c8ce47f00249cbd4b582d3a7b35d97f2648228370b4702c2	✖

Host Behavior

Type	Count
Registry	4
Module	83
Window	6
File	10
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\RhFYnHFgJ.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 185488, Reason: Child Process
Unmonitor End Time	End Time: 230783, Reason: Terminated
Monitor duration	45.30s
Return Code	1073807364
PID	3620
Parent PID	5004
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\RhFYnHFgJ" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpF9CA.tmp"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186095, Reason: Child Process
Unmonitor End Time	End Time: 206086, Reason: Terminated
Monitor duration	19.99s
Return Code	0
PID	3612
Parent PID	5004
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: 203693, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 312701, Reason: Terminated by timeout
Monitor duration	109.01s
Return Code	Unknown
PID	864
Parent PID	3612
Bitness	64 Bit

Process #7: da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 206002, Reason: Child Process
Unmonitor End Time	End Time: 230798, Reason: Terminated
Monitor duration	24.80s
Return Code	1073807364
PID	4252
Parent PID	5004
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\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	0x1390	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	0x1390	0x402000(4202496)	0xb200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	0x1390	0x40e000(4251648)	0x800	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	0x1390	0x410000(4259840)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	0x1390	0x39d008(3788808)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	0x1390 / 0x10c4	0x40d02e(4247598)	-	✔	1

Host Behavior

Type	Count
Registry	1
User	1
System	2
File	19
Mutex	1

Network Behavior

Type	Count
TCP	1

Process #8: svchost.exe

ID	8
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: 264206, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 312701, Reason: Terminated by timeout
Monitor duration	48.49s
Return Code	Unknown
PID	1004
Parent PID	3612
Bitness	64 Bit

Process #9: taskhostw.exe

ID	9
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe SYSTEM
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 299945, Reason: Child Process
Unmonitor End Time	End Time: 312701, Reason: Terminated by timeout
Monitor duration	12.76s
Return Code	Unknown
PID	1308
Parent PID	1004
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5	C:\Users\RDhJ0CNFevzX\Desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\RhFYnHFgJ.exe	Sample File	606.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
7ad7f1c3663eddd7c8ce47f0249cbd4b582d3a7b35d97f2648228370b4702c2	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpF9CA.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\RhFYnHFgJ.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpF9CA.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:\Users\RDhJ0CNFevzX\Desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe.config	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://91.193.75.135:3030	-	91.193.75.135	-	-	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
91.193.75.135	-	Estonia	TCP	MALICIOUS

Mutex

Name	Operations	Parent Process Name	Verdict
AsyncMutex_6SI8OkPnk	access	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	MALICIOUS

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	CLEAN

Process

Process Name	Commandline	Verdict
da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	"C:\Users\RDhJ0CNFevzX\Desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe"	MALICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\RhFYnHFgJ" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpF9CA.tmp"	SUSPICIOUS
da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe	"C:\Users\RDhJ0CNFevzX\Desktop\da6abb6f3aae250d50ed09b6eacc267c33e50895e3ebd7e6ba800ab018351ec5.exe"	SUSPICIOUS
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
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\RhFYnHFgJ.exe"	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	AsyncRAT	AsyncRAT	Memory Dump	-	Backdoor	5/5
RATs	AsyncRAT	AsyncRAT	-	-	Backdoor	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