MALICIOUS

Classifications: Backdoor

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

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe**
ID	#5070061
MD5	d4278af4c129db3ea1c48d890304abd1
SHA1	b6ca93a2c12c164a73339020070662b618723744
SHA256	9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc
File Size	616.50 KB
Report Created	2022-08-05 23:57 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (14 rules, 21 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) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe. • Rule "AsyncRAT" from ruleset "RATs" has matched on a code dump for (process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.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) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe modifies memory of (process #7) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe alters context of (process #7) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe.			
2/5	Task Scheduling	Schedules task	3	-
	• Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\ZgolgcKGNozdg.exe", to be triggered by LOGON. • Schedules task for command ""C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe"", to be triggered by LOGON. • Schedules task for command "C:\Users\RDhJ0CNFevzX\AppData\Roaming\ZgolgcKGNozdg.exe", to be triggered by REGISTRATION.			
2/5	Task Scheduling	Schedules task via schtasks	1	-
	• Schedules task "" via the schtasks command line utility.			
1/5	Hide Tracks	Creates process with hidden window	5	-
	• (Process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe starts (process #2) powershell.exe with a hidden window. • (Process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe starts (process #4) schtasks.exe with a hidden window. • (Process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe starts (process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe with a hidden window. • (Process #7) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe starts (process #8) cmd.exe with a hidden window. • (Process #7) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe starts (process #7) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe reads from (process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.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) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe creates mutex with name "AsyncMutex_6SI8OkPnk".			

Score	Category	Operation	Count	Classification
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #7) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe enables process privilege "SeDebugPrivilege".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #7) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe enumerates running processes.			
1/5	Discovery	Possibly does reconnaissance	1	-
	• (Process #7) 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe tries to gather information about application "Mozilla Firefox" by file.			

Malware Configuration: AsyncRAT

Metadata	Key	Extracted Value
Version	Value	0.5.7B
Socket	Address Port Network Protocol C2 Listen	37.0.14.198 6161 tcp ✔ ✖
Path	Path Directory Path Name Is Dir	%AppData%\.exe %AppData% .exe ✖
Mutex	Value	AsyncMutex_6SI8OkPnk
Interval	Tags Value	Delay 3.0
Mission ID	Value	Default
Other: Install	Value	✔
Other: Key	Tags Value	PBKDF2 Input Password 7cZb2K9l1fVDH41Tzlj0nQ0y6RuWOolR
Other: Salt	Value	v+seVvvNlzuyGQIkMKV4QwA9VkTSHmK51PGA5+bDOUE=
Other: Certificate	Value	MIIE8jCCAtqgAwIBAgIQALbPNt6guR+VUEjOEcEL1zANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZ…
Other: Serversignature	Value	b1jv8C01WVgi46QdR+OigHxE2+T1AJEbA0fIK5fUIviOfntIO9aDPp+8SKtBQcB3TvesBYaVVj4TxX/ZjmuYsjU+K6vM+mBrBUA…
Other: Anti Analysis Enabled	Value	✖
Other: BDOS Enabled	Value	✖

Mitre ATT&CK Matrix

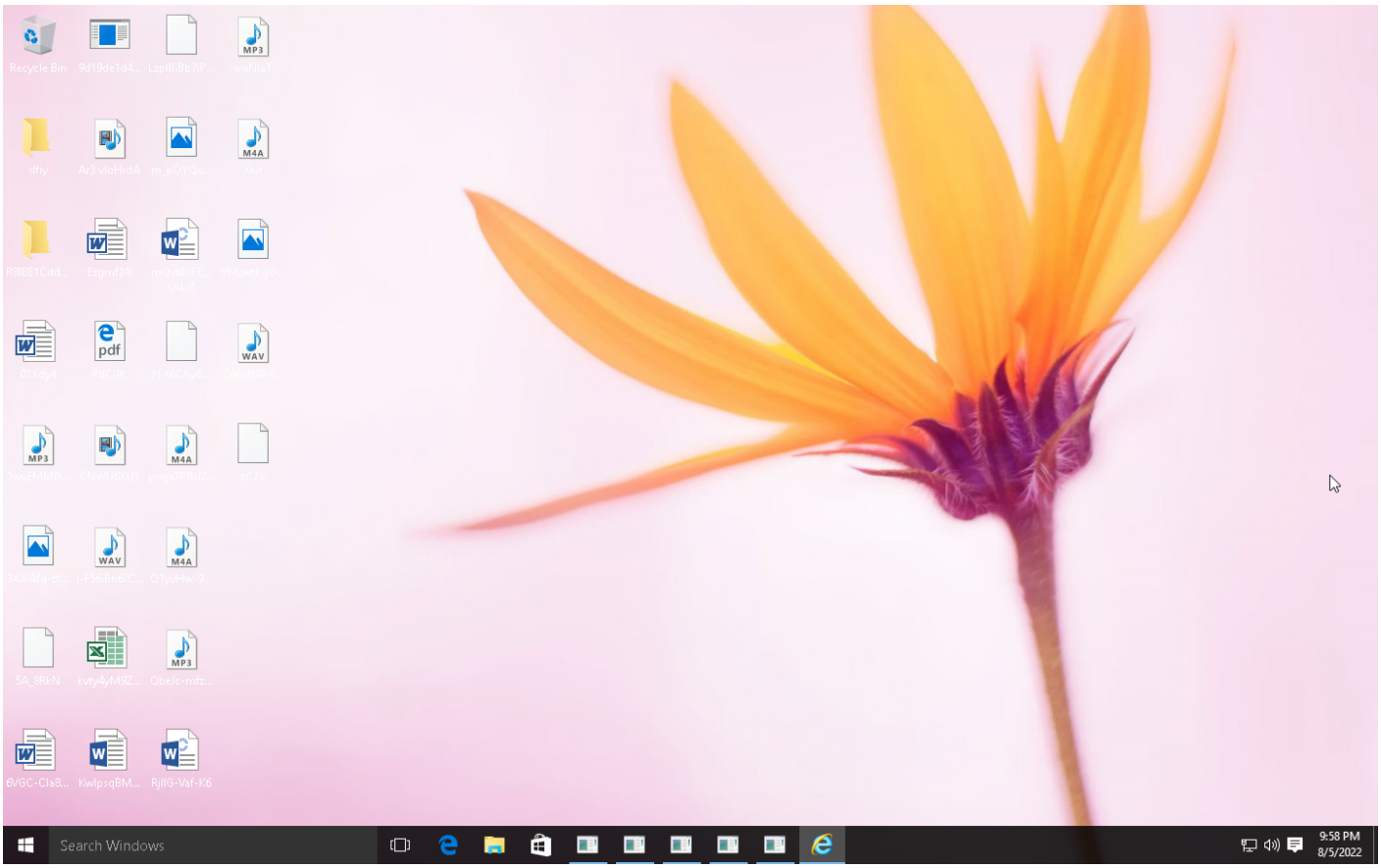
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1053 Scheduled Task	#T1143 Hidden Window		#T1057 Process Discovery					
				#T1045 Software Packing		#T1083 File and Directory Discovery					

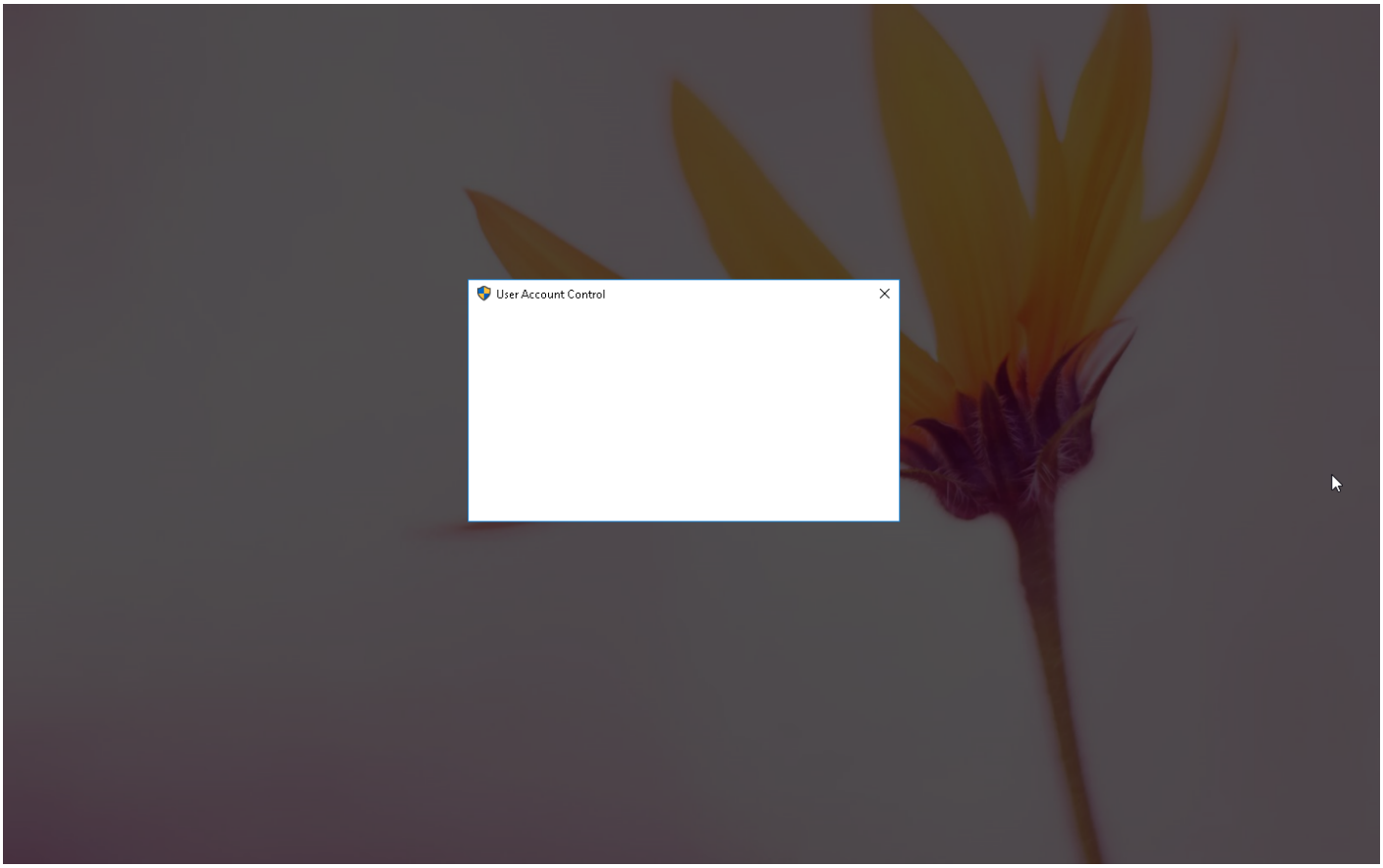
Sample Information

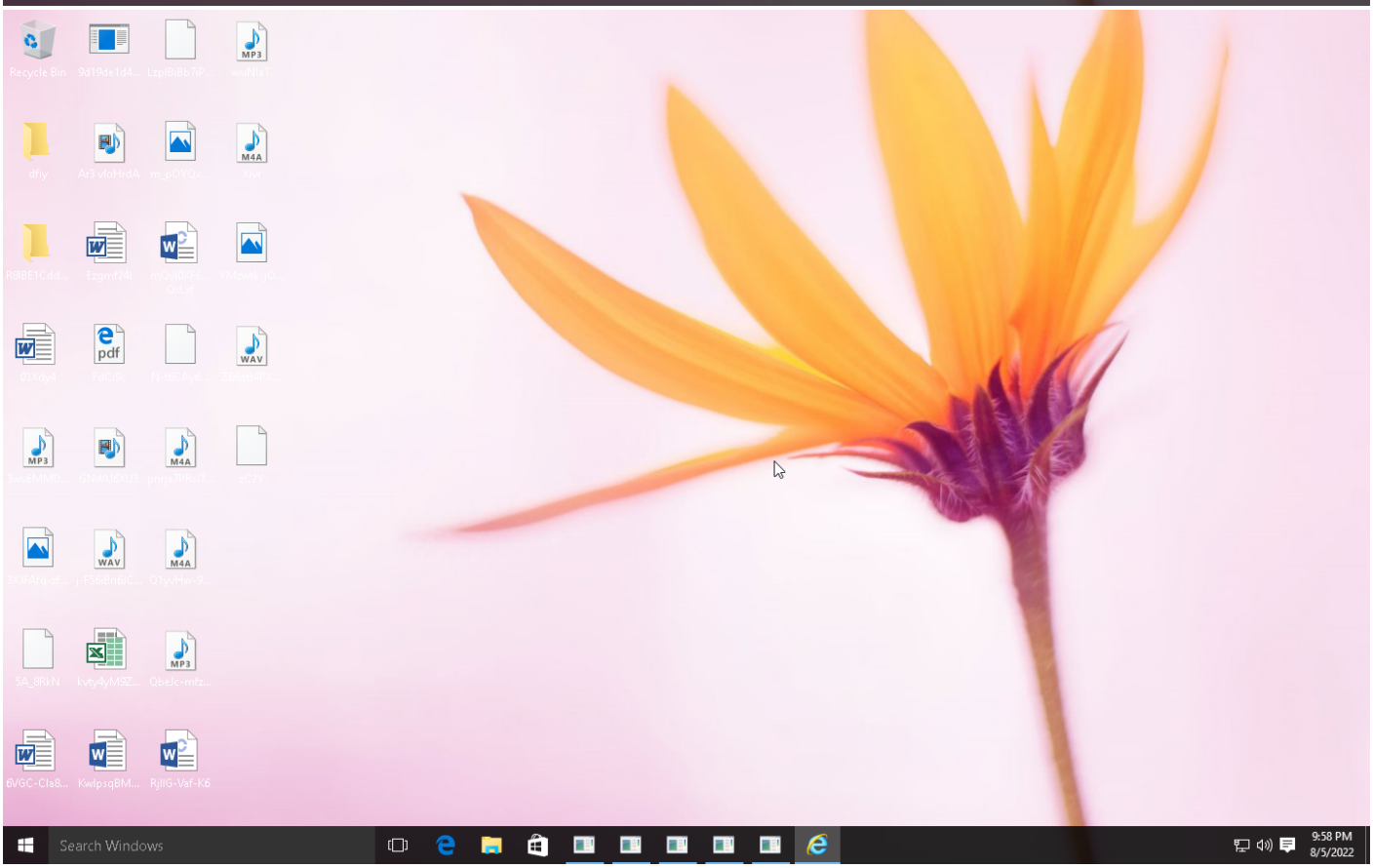
ID	#5070061
MD5	d4278af4c129db3ea1c48d890304abd1
SHA1	b6ca93a2c12c164a73339020070662b618723744
SHA256	9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc
SSDeep	12288:AzTgQCM0ei0Hth5PSQ7OBOXhsAOf9vHg6SKlpx:tTAhPSkOBOPOf9vJLlpx
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe
File Size	616.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 23:57 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	14
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


Search Windows
9:58 PM
8/5/2022


User Account Control



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

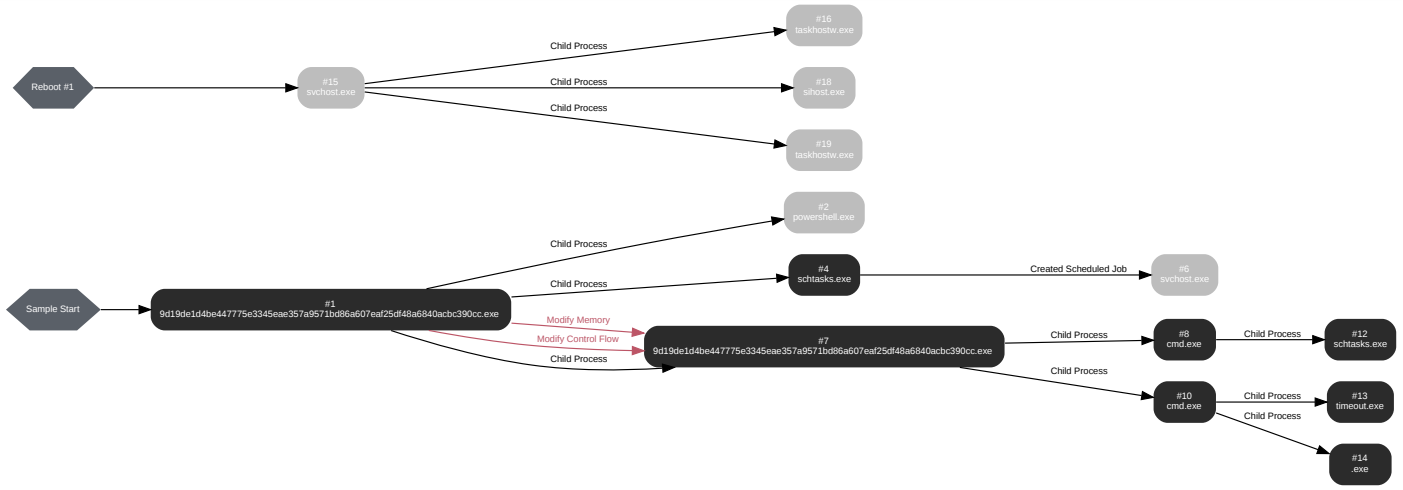
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 65441, Reason: Analysis Target
Unmonitor End Time	End Time: 191163, Reason: Terminated
Monitor duration	125.72s
Return Code	0
PID	3112
Parent PID	1972
Bitness	32 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp95DB.tmp	1.56 KB	0e7126bff40cd57601121dc11ec5f2db9c88bb6b68b0aab3cf3e15e1782124ea	✖
C:\Users\RDhJ0CNFevzX\AppData\Roaming\ZgolgcKGNozdg.exe	616.50 KB	9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc	✖

Host Behavior

Type	Count
Registry	4
Module	108
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\ZgolgcKGNozdg.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 169896, Reason: Child Process
Unmonitor End Time	End Time: 230164, Reason: Terminated
Monitor duration	60.27s
Return Code	1073807364
PID	4908
Parent PID	3112
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\ZgolgcKGNozdg" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp95DB.tmp"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 170624, Reason: Child Process
Unmonitor End Time	End Time: 188513, Reason: Terminated
Monitor duration	17.89s
Return Code	0
PID	4892
Parent PID	3112
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: 186349, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 305693, Reason: Terminated by timeout
Monitor duration	119.34s
Return Code	Unknown
PID	864
Parent PID	4892
Bitness	64 Bit

Process #7: 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 188376, Reason: Child Process
Unmonitor End Time	End Time: 203510, Reason: Terminated
Monitor duration	15.13s
Return Code	0
PID	2896
Parent PID	3112
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\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	0xaf0	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	0xaf0	0x402000(4202496)	0xb200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	0xaf0	0x40e000(4251648)	0x800	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	0xaf0	0x410000(4259840)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	0xaf0	0x322008(3285000)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	0xaf0 / 0xa88	0x40d08e(4247694)	-	✔	1

Dropped Files (3)

File Name	File Size	SHA256	YARA Match
\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp.bat	157 bytes	a1f8c3d64e72fb887033132465cde2da3a2a7d6c86b55d296e92babfdf4d8933	✖
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe	616.50 KB	9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc	✖
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✖

Host Behavior

Type	Count
Registry	1
User	2

Type	Count
System	3
File	16
Mutex	1
Module	67
Process	105

Process #8: cmd.exe

ID	8
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "" /tr '"C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe"' & exit
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 200421, Reason: Child Process
Unmonitor End Time	End Time: 207349, Reason: Terminated
Monitor duration	6.93s
Return Code	0
PID	2908
Parent PID	2896
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
Environment	8
File	4
Process	1

Process #10: cmd.exe

ID	10
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ""C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp.bat""
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 201193, Reason: Child Process
Unmonitor End Time	End Time: 216803, Reason: Terminated
Monitor duration	15.61s
Return Code	1
PID	800
Parent PID	2896
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	102
Environment	25
System	1
Process	2
-	1

Process #12: schtasks.exe

ID	12
File Name	c:\windows\syswow64\schtasks.exe
Command Line	schtasks /create /f /sc onlogon /rl highest /tn "" /tr '"C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe"'
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 203521, Reason: Child Process
Unmonitor End Time	End Time: 206526, Reason: Terminated
Monitor duration	3.00s
Return Code	0
PID	1284
Parent PID	2908
Bitness	32 Bit

Host Behavior

Type	Count
Module	3
System	3
COM	1
File	6

Process #13: timeout.exe

ID	13
File Name	c:\windows\syswow64\timeout.exe
Command Line	timeout 3
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 204825, Reason: Child Process
Unmonitor End Time	End Time: 211508, Reason: Terminated
Monitor duration	6.68s
Return Code	0
PID	1980
Parent PID	800
Bitness	32 Bit

Host Behavior

Type	Count
Module	2
System	19
File	34

Process #14: .exe

ID	14
File Name	c:\users\rdhj0cnfevzx\appdata\roaming\.exe
Command Line	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 210469, Reason: Child Process
Unmonitor End Time	End Time: 233584, Reason: Terminated
Monitor duration	23.11s
Return Code	1073807364
PID	2788
Parent PID	800
Bitness	32 Bit

Host Behavior

Type	Count
Registry	4
Module	81
Window	4
File	1

Process #15: svchost.exe

ID	15
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: 258829, Reason: Created Scheduled Job
Unmonitor End Time	End Time: 305693, Reason: Terminated by timeout
Monitor duration	46.86s
Return Code	Unknown
PID	96
Parent PID	1284
Bitness	64 Bit

Process #16: taskhostw.exe

ID	16
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe TpmTasks
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 289693, Reason: Child Process
Unmonitor End Time	End Time: 305693, Reason: Terminated by timeout
Monitor duration	16.00s
Return Code	Unknown
PID	1396
Parent PID	96
Bitness	64 Bit

Process #18: sihost.exe

ID	18
File Name	c:\windows\system32\sihost.exe
Command Line	sihost.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 293895, Reason: Child Process
Unmonitor End Time	End Time: 305693, Reason: Terminated by timeout
Monitor duration	11.80s
Return Code	Unknown
PID	1452
Parent PID	96
Bitness	64 Bit

Process #19: taskhostw.exe

ID	19
File Name	c:\windows\system32\taskhostw.exe
Command Line	taskhostw.exe
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 301784, Reason: Child Process
Unmonitor End Time	End Time: 305693, Reason: Terminated by timeout
Monitor duration	3.91s
Return Code	Unknown
PID	1548
Parent PID	96
Bitness	64 Bit

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc	C:\Users\RDhJ0CNFevzX\AppData\Roaming\ZgolgcKGNozdg.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe, C:\Users\RDhJ0CNFevzX\Desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	Sample File	616.50 KB	application/vnd.microsoft.portable-executable	Access, Create, Read, Write	MALICIOUS
a1f8c3d64e72fb887033132465cde2da3a2a7d6c86b55d296e92babfdf4d8933	\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp.bat, tmpDAB.tmp.bat, C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp.bat	Dropped File	157 bytes	text/x-msdos-batch	Access, Create, Read, Write	CLEAN
0e7126bff40cd57601121dc11ec5f2db9c88bb6b68b0aab3cf3e15e1782124ea	C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp95DB.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\.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	Sample File, Accessed File, VM File	Access, Read	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\ZgolgcKGNozdg.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Program Files\Windows Portable Devices\alftp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Media Player\fling.exe	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\bitkinex.exe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\thunderbird.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\hard.exe	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Defender\minute-bed.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Multimedia Platform\3dftp.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Sidebar\coreftp.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe.config	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Defender\icq.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\centralcreditcard.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\trillian.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\webdrive.exe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\spgagentservice.exe	Accessed File	Access	CLEAN
C:\Program Files\WindowsPowerShell\far.exe	Accessed File	Access	CLEAN
\??\C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp.bat	Dropped File, Accessed File	Access, Create, Read, Write	CLEAN
C:\Program Files\Windows Journal\winscp.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Internet Explorer\republican-opportunity.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\thank.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp	Dropped File, Accessed File, Not Extracted	Access, Create	CLEAN
C:\Program Files (x86)\Microsoft Analysis Services\operamail.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\outlook.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp95DB.tmp	Dropped File, Accessed File	Access, Create, Delete, Read, Write	CLEAN
C:\Program Files\WindowsPowerShell\edcsvr.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Multimedia Platform\aldelo.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Mail\other.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe.config	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\thing_really.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE	Accessed File	Access	CLEAN
C:\Program Files\Common Files\pidgin.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\thesepolice.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Common Files\whatsapp.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Journal\active-charge.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Photo Viewer\notepad.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\creditservice.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Photo Viewer\office.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\foxmailincmail.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender\isspos.exe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\allow_note.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Defender\scriptftp.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Journal\leechftp.exe	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\yahoomessenger.exe	Accessed File	Access	CLEAN
C:\Program Files\Common Files\oh represent.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\schtasks.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft Office\top.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\timeout.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Sidebar\flashfxp.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\fpos.exe	Accessed File	Access	CLEAN
C:\Program Files\MSBuild\film.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Journal\mxslipstream.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows Portable Devices\skype.exe	Accessed File	Access	CLEAN

File Name	Category	Operations	Verdict
C:\Program Files\Microsoft Office\smartftp.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Media Player\utg2.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\WindowsPowerShell\involve_off.exe	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Program Files\Windows Media Player\certainlyifmaterial.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows NT\budget senior.exe	Accessed File	Access	CLEAN
C:\Program Files\Microsoft Office\protect.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft SQL Server\spcwin.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Windows NT\filezilla.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Portable Devices\approach-time.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft SQL Server\accupos.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Reference Assemblies\ncftp.exe	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN
NUL	Accessed File	Access, Create	CLEAN
C:\Program Files (x86)\Windows Defender\afr38.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows NT\talk.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft SQL Server\omnipos.exe	Accessed File	Access	CLEAN
"C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp.bat"	Accessed File	Access	CLEAN
C:\Program Files\Windows Sidebar\any contain meet.exe	Accessed File	Access	CLEAN
C:\Program Files\Internet Explorer\gmailnotifierpro.exe	Accessed File	Access	CLEAN
C:\Program Files\Windows Mail\barca.exe	Accessed File	Access	CLEAN
C:\Program Files\Reference Assemblies\officer water student.exe	Accessed File	Access	CLEAN
C:\Program Files (x86)\Microsoft SQL Server\ccv_server.exe	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Local\Temp	Accessed File	Access	CLEAN
C:\Program Files (x86)\Mozilla Firefox\absolutetelnet.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://37.0.14.198:6161	-	37.0.14.198	-	-	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
37.0.14.198	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
AsyncMutex_6SI8OkPnk	access	9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	MALICIOUS

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	.exe, 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	.exe, 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	.exe, 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	.exe, 9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe"	MALICIOUS
schtasks.exe	"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ZgolgcKGNozdg" /XML "C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmp95DB.tmp"	SUSPICIOUS
9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe	"C:\Users\RDhJ0CNFevzX\Desktop\9d19de1d4be447775e3345eae357a9571bd86a607eaf25df48a6840acbc390cc.exe"	SUSPICIOUS
schtasks.exe	schtasks /create /f /sc onlogon /rl highest /tn "" /tr '"C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe"'	SUSPICIOUS

Process Name	Commandline	Verdict
powershell.exe	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\RDhJ0CNFevzX\AppData\Roaming\ZgolgcKGNozdg.exe"	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	CLEAN
cmd.exe	"C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "" /tr '"C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe"' & exit	CLEAN
taskhostw.exe	taskhostw.exe TpmTasks	CLEAN
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\RDhJ0CNFevzX\AppData\Local\Temp\tmpDAB.tmp.bat""	CLEAN
sihost.exe	sihost.exe	CLEAN
timeout.exe	timeout 3	CLEAN
.exe	"C:\Users\RDhJ0CNFevzX\AppData\Roaming\.exe"	CLEAN
taskhostw.exe	taskhostw.exe	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k netsvcs	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