MALICIOUS

Classifications: Backdoor

Threat Names: Remcos

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe**
ID	#5068466
MD5	de9784a4f56eaf8affc96754a15a5cd3
SHA1	35c361a8bfdb894e80fe99728e60ad7d08745af1
SHA256	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da
File Size	928.00 KB
Report Created	2022-08-05 18:22 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (10 rules, 12 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	Remcos configuration was extracted	1	Backdoor
	• A configuration for Remcos was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	2	Backdoor
	• Rule "remcos_rat" from ruleset "RATs" has matched on a memory dump for (process #2) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe. • Rule "remcos_rat" from ruleset "RATs" has matched on a code dump for (process #1) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe.			
4/5	Reputation	Known malicious file	1	-
	• The sample itself is a known malicious file.			
2/5	Injection	Writes into the memory of a process started from a created or modified executable	1	-
	• (Process #1) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe modifies memory of (process #2) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe.			
2/5	Injection	Modifies control flow of a process started from a created or modified executable	1	-
	• (Process #1) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe alters context of (process #2) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe starts (process #1) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe with a hidden window. • (Process #2) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe starts (process #3) cmd.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe reads from (process #1) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.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 #2) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe creates mutex with name "remcos_totevzugmgbhhbj".			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #2) f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe adds ""C:\Users\RDhJ0CNFevzX\remcos\remcos.exe"" to Windows startup via registry.			

Malware Configuration: Remcos

Metadata	Key	Extracted Value
Socket	Tags Address Port C2	Domain #0 79.134.225.97 8600 ✔
Encryption Key	Key Tags Algorithm	123456 Domain #0 RC4
Version	Value	1.7 Pro
Mutex	Value	remcos_totevzugmgbhhbj
Interval	Value	5.0
Path	Name Is Dir Tags Name Is Dir Path Directory Path Name Is Dir	remcos.exe ✖ Log File logs.dat ✖ User Profile User Profile ✔
Other: Assigned Name	Value	Host
Other: Screenshot Windows	Value	

Mitre ATT&CK Matrix

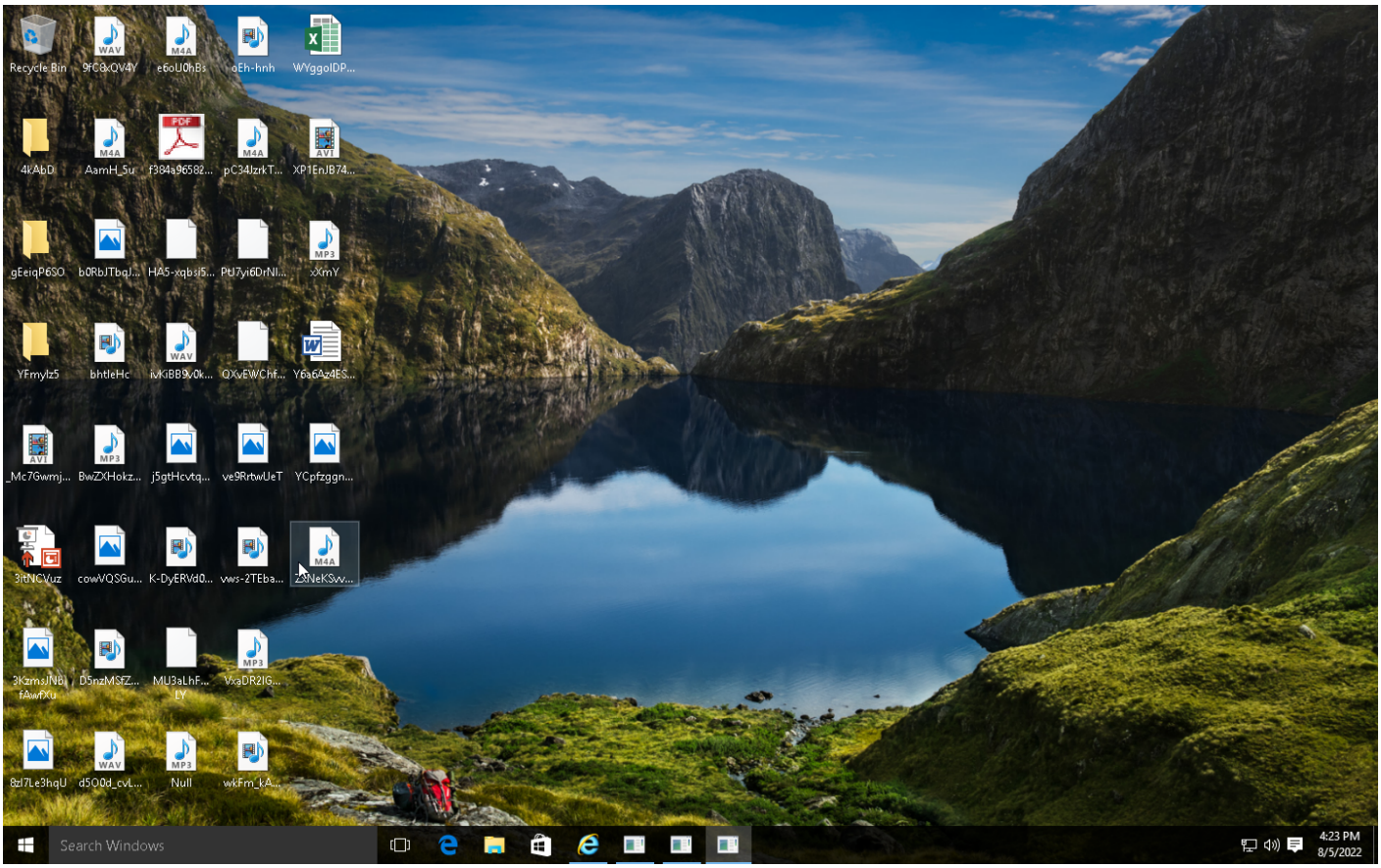
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window #T1045 Software Packing #T1112 Modify Registry							

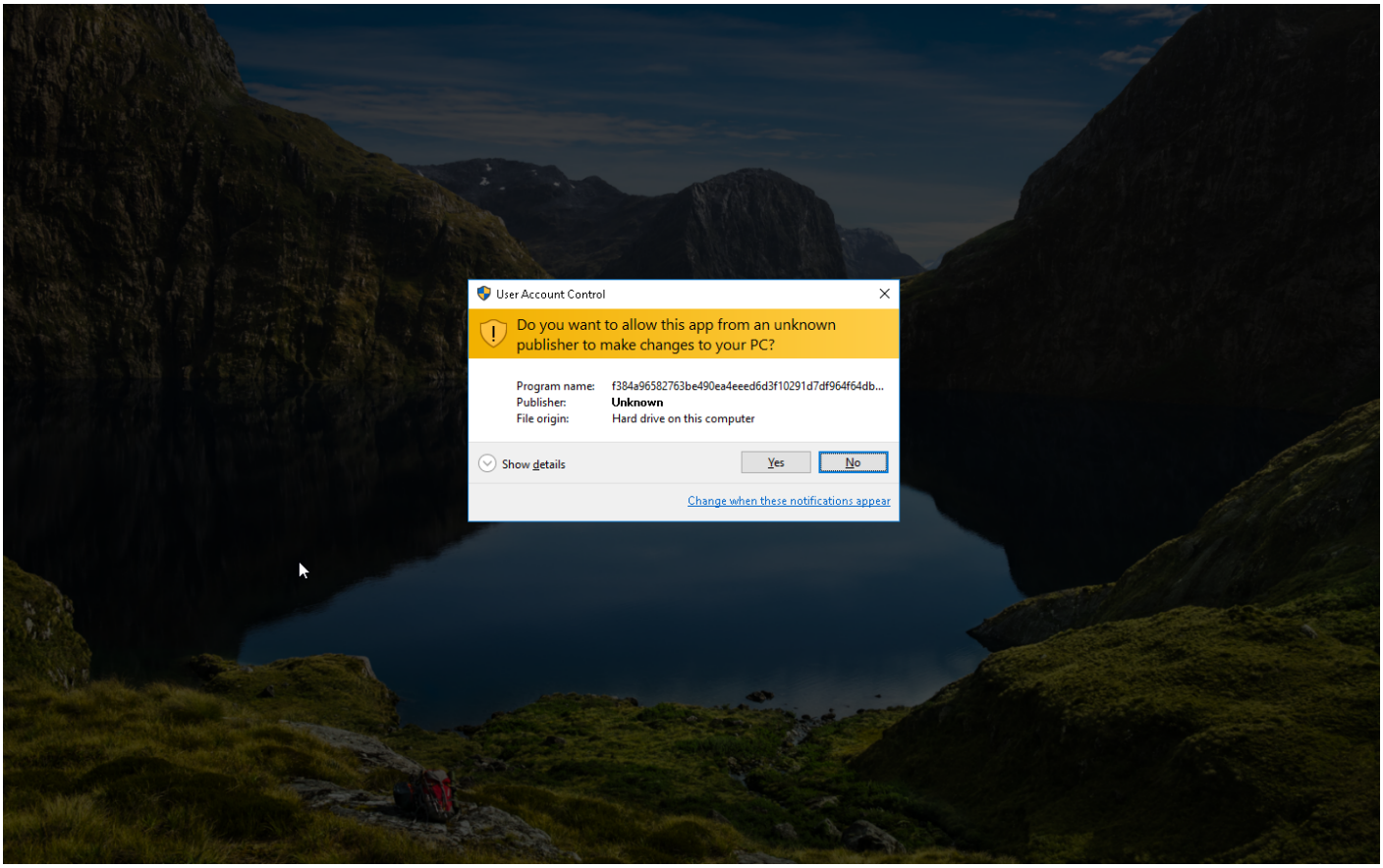
Sample Information

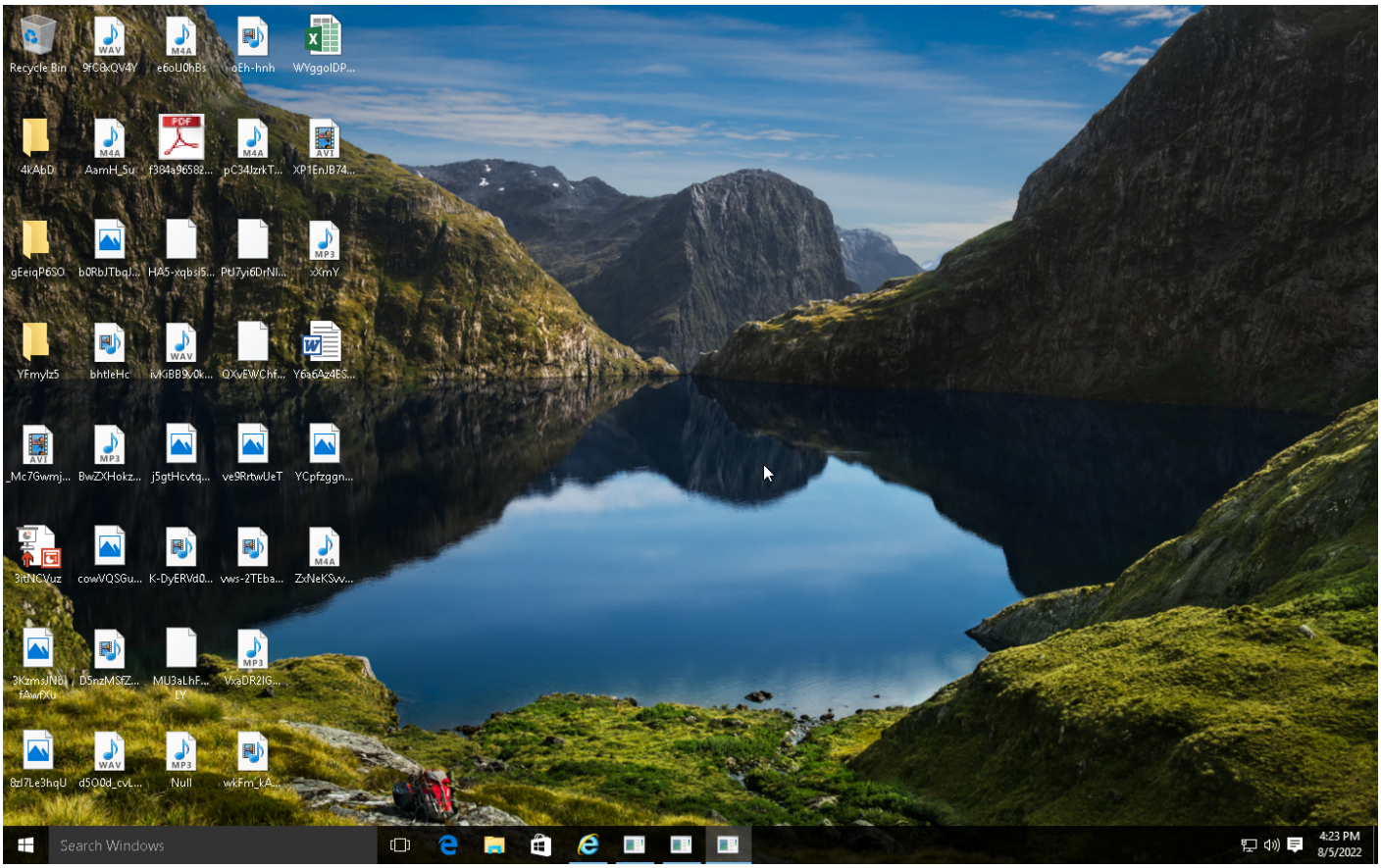
ID	#5068466
MD5	de9784a4f56eaf8affc96754a15a5cd3
SHA1	35c361a8bfdb894e80fe99728e60ad7d08745af1
SHA256	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da
SSDeep	12288:4Rb0kj3oTB2b2UVFdPBGjIKHfrLPVPf1cLlq+R3rU8weZd+ydGRuwJGdaTuM18N5:4RA0siGjIKHf/NH1eFR7U8wWkTRk
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe
File Size	928.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

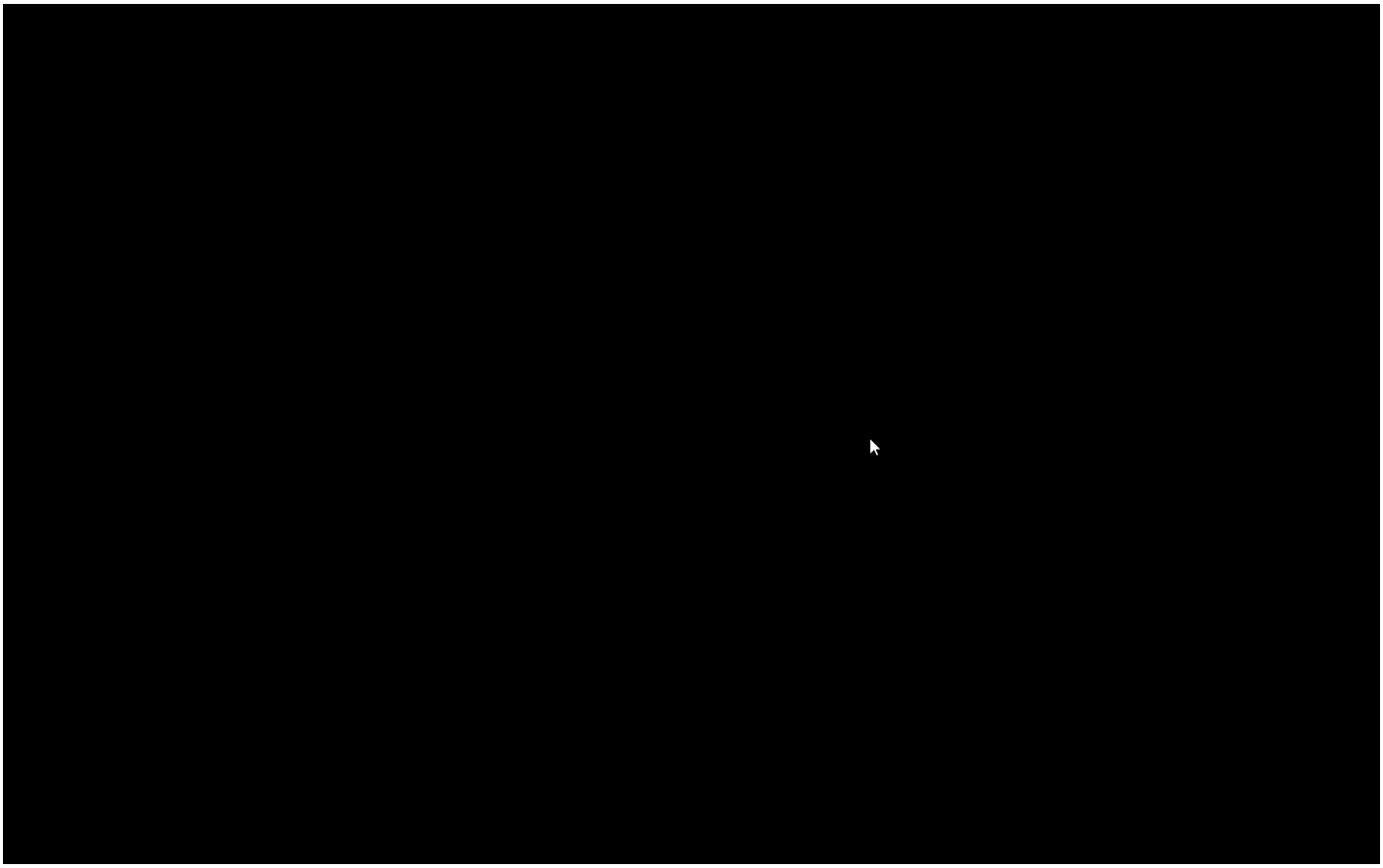
Analysis Information

Creation Time	2022-08-05 18:22 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	6
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	9


Recycle Bin
Search Windows
4:23 PM
8/5/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: f384a96582763be490ea4eeed6d3f10291d7df964f64db...
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

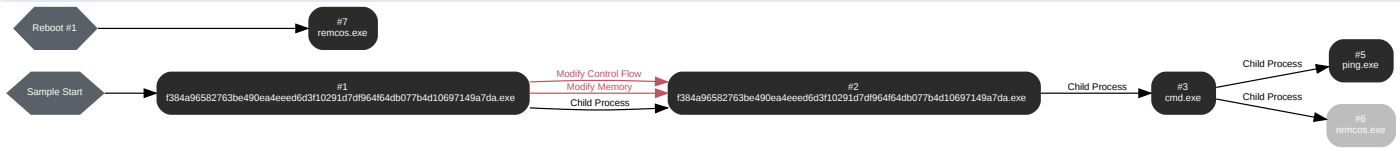
HTTP/S

0 URLs contacted, 0 servers

0 sessions, 0 bytes sent, 0 bytes received

BEHAVIOR

Process Graph



Process #1: f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 64316, Reason: Analysis Target
Unmonitor End Time	End Time: 189119, Reason: Terminated
Monitor duration	124.80s
Return Code	0
PID	4952
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
Registry	4
Module	1142
Window	22
File	20
COM	1
System	3
Process	1
-	3
-	8

Process #2: f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 183843, Reason: Child Process
Unmonitor End Time	End Time: 192397, Reason: Terminated
Monitor duration	8.55s
Return Code	0
PID	3820
Parent PID	4952
Bitness	32 Bit

Injection Information (7)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	0x135c	0x400000(4194304)	0x1000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	0x135c	0x401000(4198400)	0xf000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	0x135c	0x410000(4259840)	0x5000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	0x135c	0x415000(4280320)	0x1000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	0x135c	0x416000(4284416)	0x1000	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	0x135c	0x310008(3211272)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	0x135c / 0x11e0	0x40fd88(4259208)	-	✔	1

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	928.00 KB	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da	✖
C:\Users\RDHJ0C~1\AppData\Local\Temp\install.bat	90 bytes	7facb45b7dd680d9dd92572885114d1c21e26653a9b3db8d512b916fa40afaf7	✖

Host Behavior

Type	Count
Module	20
Mutex	2
Registry	5
File	2
Process	1

Process #3: cmd.exe

ID	3
File Name	c:\windows\syswow64\cmd.exe
Command Line	C:\Windows\system32\cmd.exe /c ""C:\Users\RDHJ0C~1\AppData\Local\Temp\install.bat" "
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 191508, Reason: Child Process
Unmonitor End Time	End Time: 219687, Reason: Terminated
Monitor duration	28.18s
Return Code	3221225786
PID	4596
Parent PID	3820
Bitness	32 Bit

Host Behavior

Type	Count
Module	8
Registry	17
File	119
Environment	25
System	1
Process	2
-	1

Process #5: ping.exe

ID	5
File Name	c:\windows\syswow64\ping.exe
Command Line	PING 127.0.0.1 -n 2
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 210034, Reason: Child Process
Unmonitor End Time	End Time: 217399, Reason: Terminated
Monitor duration	7.37s
Return Code	0
PID	4712
Parent PID	4596
Bitness	32 Bit

Host Behavior

Type	Count
Module	1
File	26
Registry	2
-	3
Environment	12
-	2
System	1

Process #6: remcos.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\remcos\remcos.exe
Command Line	"C:\Users\RDhJ0CNFevzX\remcos\remcos.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 216484, Reason: Child Process
Unmonitor End Time	End Time: 219687, Reason: Terminated
Monitor duration	3.20s
Return Code	1073807364
PID	4584
Parent PID	4596
Bitness	32 Bit

Process #7: remcos.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\remcos\remcos.exe
Command Line	"C:\Users\RDhJ0CNFevzX\remcos\remcos.exe"
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 292646, Reason: Autostart
Unmonitor End Time	End Time: 305346, Reason: Terminated by timeout
Monitor duration	12.70s
Return Code	Unknown
PID	3008
Parent PID	1656
Bitness	32 Bit

Host Behavior

Type	Count
Registry	4
Module	27
Window	4
File	1

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da	C:\Users\RDhJ0CNFevzX\Desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe, C:\Users\RDhJ0CNFevzX\remcos\remcos.exe	Sample File	928.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS
7facb45b7dd680d9dd92572885114d1c21e26653a9b3db8d512b916fa40afaf7	C:\Users\RDHJ0C~1\AppData\Local\Temp\install.bat	Dropped File	90 bytes	text/plain	Access, Read	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\remcos\remcos.exe	Dropped File, Accessed File, VM File	Access, Create, Write	MALICIOUS
C:\Windows\SYSTEM32\RichEd20.DLL	Accessed File	Access	CLEAN
"C:\Users\RDHJ0C~1\AppData\Local\Temp\install.bat"	Accessed File	Access	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\install.bat	Dropped File, Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\remcos\remcos.exe.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\remcos	Accessed File	Access, Create	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe.config	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\cmd.exe	Accessed File	Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://79.134.225.97	-	79.134.225.97	-	-	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
79.134.225.97	-	-	-	CLEAN
127.0.0.1	-	-	-	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
remcos_totevzugmgbhhbj	access	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	MALICIOUS
Remcos_Mutex_Inj	access	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck	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\DelayedExpansion	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	create, access	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	access	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	remcos.exe, f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\remcos_totevzugmgbhhbj	access	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	remcos.exe, f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName	read, access	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion	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	access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\remcos	access, write	f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	remcos.exe, f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	remcos.exe, f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	access	ping.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor	access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions	read, access	cmd.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DefaultTTL	read, access	ping.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck	read, access	cmd.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar	read, access	cmd.exe	CLEAN

Process

Process Name	Commandline	Verdict
f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	"C:\Users\RDhJ0CNFevzX\Desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe"	SUSPICIOUS
f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe	"C:\Users\RDhJ0CNFevzX\Desktop\f384a96582763be490ea4eeed6d3f10291d7df964f64db077b4d10697149a7da.exe"	SUSPICIOUS
cmd.exe	C:\Windows\system32\cmd.exe /c ""C:\Users\RDHJ0C~1\AppData\Local\Temp\install.bat" "	CLEAN
ping.exe	PING 127.0.0.1 -n 2	CLEAN
remcos.exe	"C:\Users\RDhJ0CNFevzX\remcos\remcos.exe"	CLEAN
remcos.exe	"C:\Users\RDhJ0CNFevzX\remcos\remcos.exe"	CLEAN

YARA / AV

YARA (9)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	remcos_rat	Remcos RAT	Memory Dump	-	Backdoor	5/5
RATs	remcos_rat	Remcos RAT	-	-	Backdoor	5/5
RATs	remcos_rat	Remcos RAT	Memory Dump	-	Backdoor	5/5
RATs	remcos_rat	Remcos RAT	Memory Dump	-	Backdoor	5/5
RATs	remcos_rat	Remcos RAT	Memory Dump	-	Backdoor	5/5
RATs	remcos_rat	Remcos RAT	Memory Dump	-	Backdoor	5/5
RATs	remcos_rat	Remcos RAT	Memory Dump	-	Backdoor	5/5
RATs	remcos_rat	Remcos RAT	Memory Dump	-	Backdoor	5/5
RATs	remcos_rat	Remcos RAT	Memory Dump	-	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