MALICIOUS

Classifications: -

Threat Names: AgentTesla.v3

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe**
ID	#4243636
MD5	d88a146f731e00b42947ec060f3d4f43
SHA1	46243e85f209fdb306affd5eefb9ffe5fa3d2614
SHA256	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51
File Size	43.00 KB
Report Created	2022-05-02 15:23 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 14 matches)

Score	Category	Operation	Count	Classification
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) msbuild.exe.			
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe modifies memory of (process #5) msbuild.exe.			
4/5	Injection	Modifies control flow of another process	1	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe alters context of (process #5) msbuild.exe.			
1/5	Hide Tracks	Creates process with hidden window	2	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe starts (process #2) cmd.exe with a hidden window. • (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe starts (process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe with a hidden window.			
1/5	Privilege Escalation	Enables process privilege	2	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe enables process privilege "SeDebugPrivilege". • (Process #5) msbuild.exe enables process privilege "SeDebugPrivilege".			
1/5	Persistence	Installs system startup script or application	1	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe adds ""C:\Users\RDhJ0CNFevzX\AppData\Roaming\OarkzIb\Puizg.exe"" to Windows startup via registry.			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe enumerates running processes.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe reads from (process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe resolves host name "cdn.discordapp.com" to IP "-".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #1) d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe opens an outgoing TCP connection to host "162.159.129.233:443".			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #5) msbuild.exe resolves 49 API functions by name.			

Mitre ATT&CK Matrix

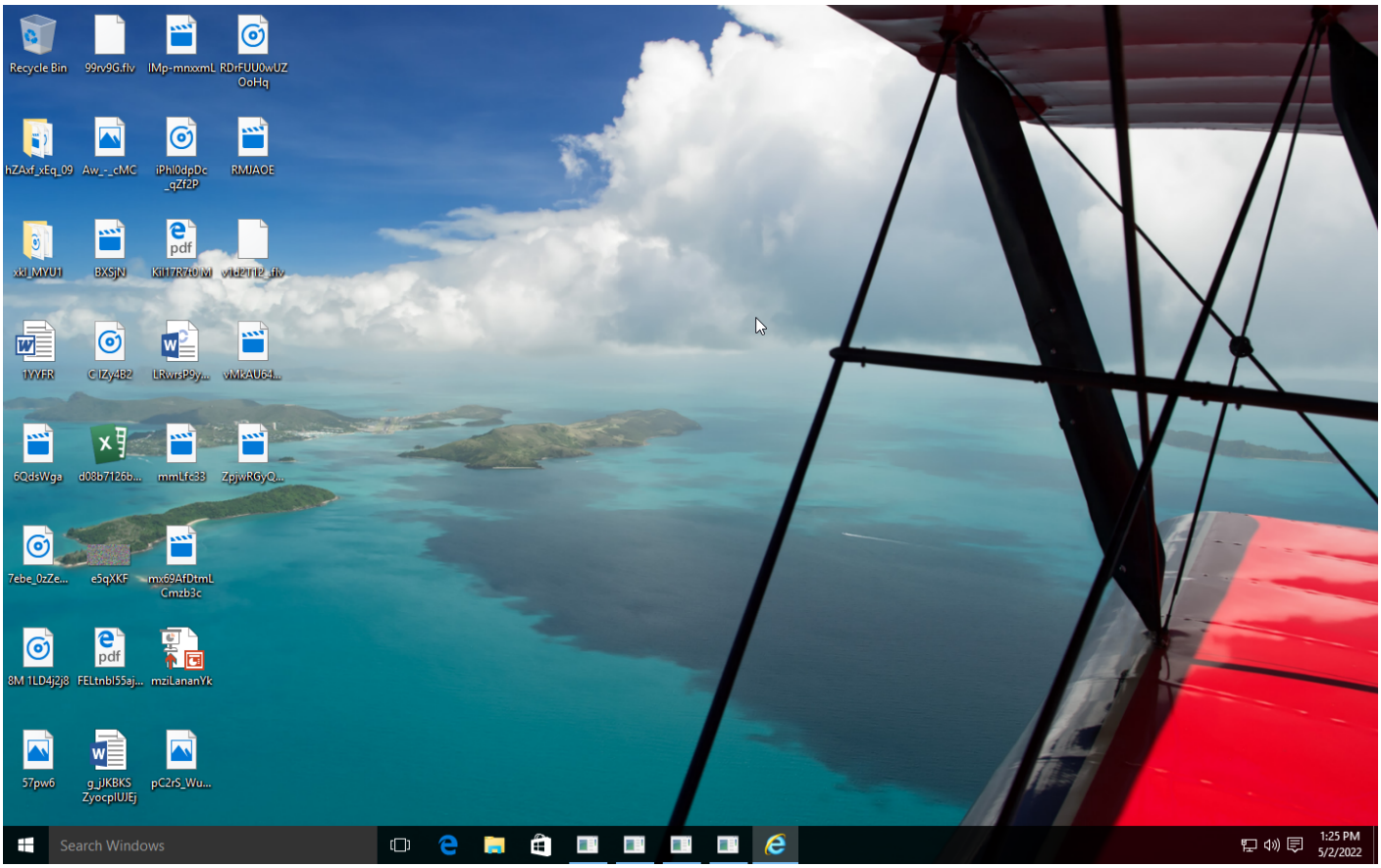
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
		#T1060 Registry Run Keys / Startup Folder		#T1143 Hidden Window		#T1057 Process Discovery					
				#T1112 Modify Registry							
				#T1045 Software Packing							

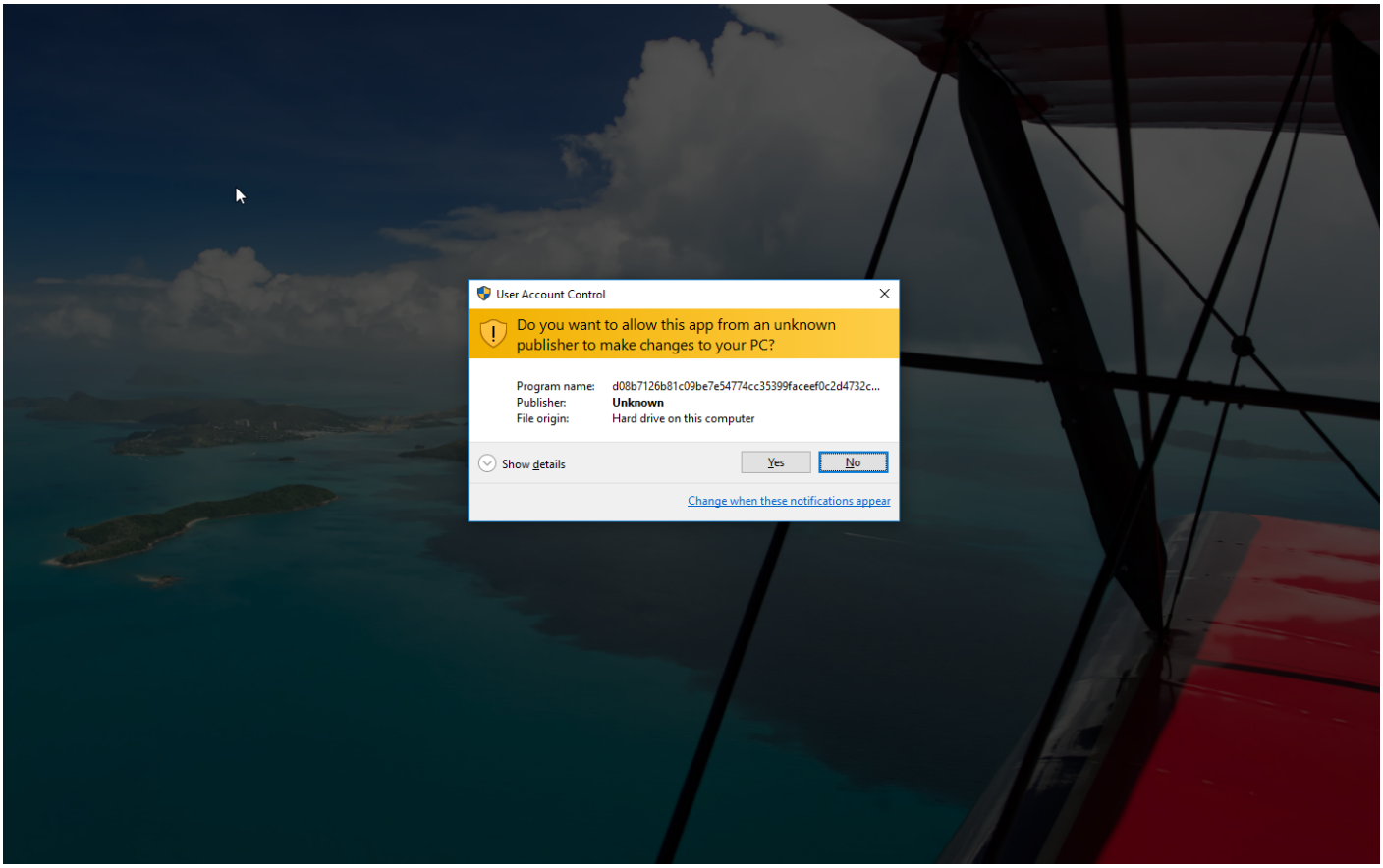
Sample Information

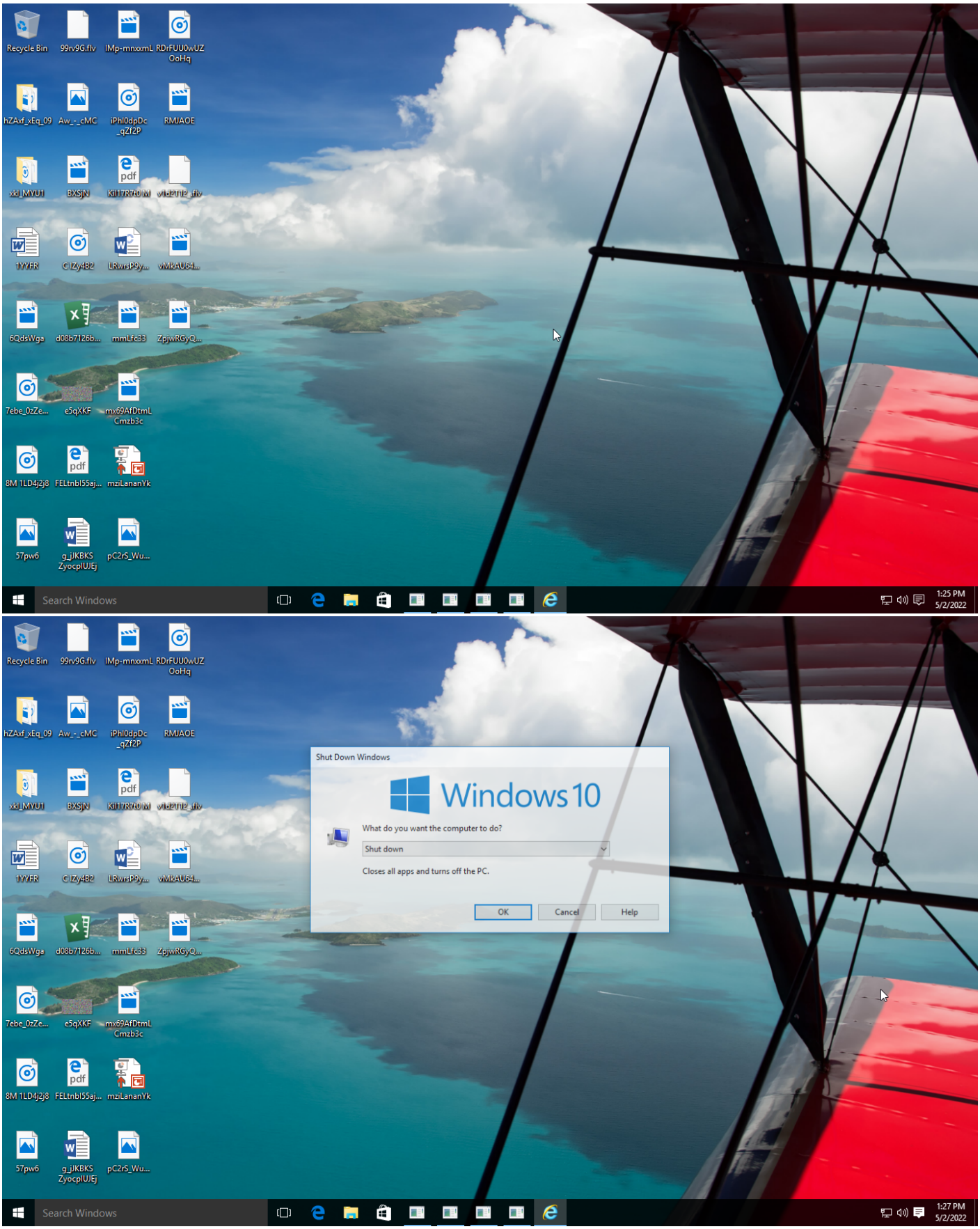
ID	#4243636
MD5	d88a146f731e00b42947ec060f3d4f43
SHA1	46243e85f209fdb306affd5eefb9ffe5fa3d2614
SHA256	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51
SSDeep	384:FHYm+Nnx5Cb+XHJynH5rHmHfffffJQaulaipMwCKzH2S3dd0hUADkadcX:FHYmyDCCXHJASGlbMwCKN3deVDwX
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe
File Size	43.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-05-02 15:23 (UTC+2)
Analysis Duration	00:03:58
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	1


Recycle Bin
99rv9G.flv
IMp-mnxmL
RDrFUU0wUZ OoHq
hZAxf_xEq_09
Aw_-_cMC
iPhl0dpDc _qZf2P
RMJAOE
xkLMYU1
BXSjN
Kil17R70.tif
vILZT12_.flv
1YYFR
C IZy4B2
LRwrsP9y...
vMkAU64...
6QdsWga
d08b7126b...
mmLfc33
ZpjwRGyQ...
7ebe_0zZe...
e5qXKF
mx69AfDtmL Cmzb3c
8M 1LD4j2j8
FELtnbl55aj...
mziLananYk
57pw6
g_jKBKS ZyocplUEj
pC2rS_Wu...
Search Windows
1:25 PM
5/2/2022


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: d08b7126b81c09be7e54774cc35399faceef0c2d4732c...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

11.88 KB total sent

1265.66 KB total received

4 ports 443, 139, 53, 445

2 contacted IP addresses

1 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

1 DNS requests for 1 domains

1 nameservers contacted

0 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

1 sessions, 0 bytes sent, 0 bytes received

HTTP Requests

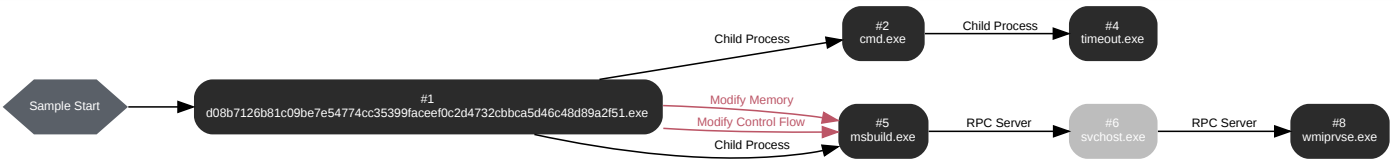
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	http://cdn.discordapp.com/attachments/968108194327052308/970585558680223784/Nqdkg_Cbadgewx.png	-	-		0 bytes	NA

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	cdn.discordapp.com	NO_ERROR			NA

BEHAVIOR

Process Graph



Process #1: d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 83959, Reason: Analysis Target
Unmonitor End Time	End Time: 221280, Reason: Terminated
Monitor duration	137.32s
Return Code	0
PID	2064
Parent PID	1932
Bitness	32 Bit

Dropped Files (1)

File Name	File Size	SHA256	YARA Match
C:\Users\RDhJ0CNFevzX\Desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	43.00 KB	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51	✖

Host Behavior

Type	Count
System	118
Process	108
Environment	8
Module	88
Window	20
File	26
-	10
Registry	30
-	3
-	7
User	2
-	1

Network Behavior

Type	Count
HTTP	1
DNS	1
TCP	2

Process #2: cmd.exe

ID	2
File Name	c:\windows\syswow64\cmd.exe
Command Line	"C:\Windows\System32\cmd.exe" /c timeout 20
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 177594, Reason: Child Process
Unmonitor End Time	End Time: 215586, Reason: Terminated
Monitor duration	37.99s
Return Code	0
PID	2344
Parent PID	2064
Bitness	32 Bit

Host Behavior

Type	Count
Environment	8
File	8
Module	1
Process	1

Process #4: timeout.exe

ID	4
File Name	c:\windows\syswow64\timeout.exe
Command Line	timeout 20
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 193527, Reason: Child Process
Unmonitor End Time	End Time: 215586, Reason: Terminated
Monitor duration	22.06s
Return Code	0
PID	1752
Parent PID	2344
Bitness	32 Bit

Host Behavior

Type	Count
File	142
System	373
Module	2

Process #5: msbuild.exe

ID	5
File Name	c:\windows\microsoft.net\framework\v4.0.30319\msbuild.exe
Command Line	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 218671, Reason: Child Process
Unmonitor End Time	End Time: 247053, Reason: Terminated
Monitor duration	28.38s
Return Code	1073807364
PID	780
Parent PID	2064
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\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	0x1210	0x400000(4194304)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	0x1210	0x402000(4202496)	0x33c00	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	0x1210	0x436000(4415488)	0x600	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	0x1210	0x438000(4423680)	0x200	✔	1
Modify Memory	#1: c:\users\rdhj0cnfevzx\desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	0x1210	0x27f008(2617352)	0x4	✔	1
Modify Control Flow	#1: c:\users\rdhj0cnfevzx\desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	0x1210 / 0xab0	0x435b8e(4414350)	-	✔	1

Host Behavior

Type	Count
File	25
Module	52
User	1
COM	12
Registry	11
-	7
System	4

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: 225453, Reason: RPC Server
Unmonitor End Time	End Time: 314566, Reason: Terminated by timeout
Monitor duration	89.11s
Return Code	Unknown
PID	868
Parent PID	780
Bitness	64 Bit

Process #8: wmiprvse.exe

ID	8
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: 225453, Reason: RPC Server
Unmonitor End Time	End Time: 314566, Reason: Terminated by timeout
Monitor duration	89.11s
Return Code	Unknown
PID	3608
Parent PID	868
Bitness	64 Bit

Host Behavior

Type	Count
System	2
Registry	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51	C:\Users\RDhJ0CNFevzX\Desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe, C:\Users\RDhJ0CNFevzX\AppData\Roaming\OarkzIb\Puizg.exe	Sample File	43.00 KB	application/vnd.microsoft.portable-executable	Access, Create, Write	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\AppData\Roaming\OarkzIb\Puizg.exe	Sample File, Dropped File, VM File, Accessed File	Access, Create, Write	MALICIOUS
C:\Users\RDhJ0CNFevzX\Desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
C:\Users\RDhJ0CNFevzX\AppData\Roaming\OarkzIb	Accessed File	Access, Create	CLEAN
System Paging File	Accessed File	Access	CLEAN
C:\Windows\SysWOW64\timeout.exe	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe.config	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\AppData\Roaming	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe.Config	Accessed File	Access, Read	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
http://cdn.discordapp.com/attachments/968108194327052308/970585558680223784/Nqdkg_Cbadgewx.png	-	162.159.134.233, 162.159.130.233, 162.159.129.233, 162.159.135.233, 162.159.133.233	-	-	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
cdn.discordapp.com	162.159.134.233, 162.159.130.233, 162.159.129.233, 162.159.135.233, 162.159.133.233	-	TCP, DNS, HTTPS	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\LegacyWPADSupport	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe, msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Impersonation Level	access, read	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting\Default Namespace	access, read	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\HWRPortReuseOnSocketBind	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe, msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Scripting	access	msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Puizg	access, write, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe, msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319	access	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe, msbuild.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319\SchUseStrongCrypto	access, read	d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe, msbuild.exe	CLEAN

Process

Process Name	Commandline	Verdict
d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe	"C:\Users\RDhJ0CNFevzX\Desktop\d08b7126b81c09be7e54774cc35399faceef0c2d4732cbbca5d46c48d89a2f51.exe"	MALICIOUS
msbuild.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe	SUSPICIOUS
cmd.exe	"C:\Windows\System32\cmd.exe" /c timeout 20	CLEAN
timeout.exe	timeout 20	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	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	4.5.0
Dynamic Engine Version	4.5.0 / 04/22/2022 19:04
Static Engine Version	4.5.0.0 / 2022-04-22 17:45:13
AV Exceptions Version	4.5.0.2 / 2022-04-03 15:57:54
Link Detonation Heuristics Version	4.5.0.19 / 2022-04-20 05:46:11
Smart Memory Dumping Rules Version	4.5.0.2 / 2022-04-03 15:57:54
Config Extractors Version	4.5.0.14 / 2022-04-07 17:00:08
Signature Trust Store Version	4.5.0.2 / 2022-04-03 15:57:54
VMRay Threat Identifiers Version	4.5.0.24 / 2022-04-26 09:10:00
YARA Built-in Ruleset Version	4.5.0.2

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	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