MALICIOUS

Classifications: Keylogger | Backdoor

Threat Names: njRAT | njRAT.07NyanCat | Mal/Generic-S

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe**
ID	#5067209
MD5	1f85c12fcd3232c577e5e8cc07fbf1e1
SHA1	3741755f8a11638209821a3cd7c01104acac184d
SHA256	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4
File Size	754.50 KB
Report Created	2022-08-05 13:25 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (12 rules, 12 matches)

Score	Category	Operation	Count	Classification
5/5	Extracted Configuration	njRAT configuration was extracted	1	Backdoor
	• A configuration for njRAT was extracted from artifacts of the dynamic analysis.			
5/5	YARA	Malicious content matched by YARA rules	1	Backdoor
	• Rule "njRAT" from ruleset "RATs" has matched on a memory dump for (process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe.			
4/5	Reputation	Known malicious file	1	-
	• Reputation analysis labels the sample itself as Mal/Generic-S.			
2/5	Discovery	Queries OS version via WMI	1	-
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe queries OS version via WMI.			
2/5	Discovery	Executes WMI query	1	-
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe executes WMI query: select * from Win32_OperatingSystem.			
1/5	Mutex	Creates mutex	1	-
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe creates mutex with name "d84c416188f84fa099".			
1/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe frequently reads the state of a keyboard key by API.			
1/5	Privilege Escalation	Enables process privilege	1	-
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe enables process privilege "SeDebugPrivilege".			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe resolves host name "milla11.publicvm.com" to IP "91.109.186.4".			
1/5	Network Connection	Connects to remote host	1	-
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe opens an outgoing TCP connection to host "91.109.186.4:5050".			
1/5	Network Connection	Tries to connect using an uncommon port	1	-
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe tries to connect to TCP port 5050 at 91.109.186.4.			
1/5	Obfuscation	Resolves API functions dynamically	1	-
	• (Process #1) f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe resolves 49 API functions by name.			

Malware Configuration: njRAT

Metadata	Key	Extracted Value
Version	Value	0.7NC
Mission ID	Value	NYAN CAT
Mutex	Value	d84c416188f84fa099
Socket	Address Port Network Protocol C2	milla11.publicvm.com 5050 tcp ✔
Other: Network Separator	Value	@!#&^%$

Mitre ATT&CK Matrix

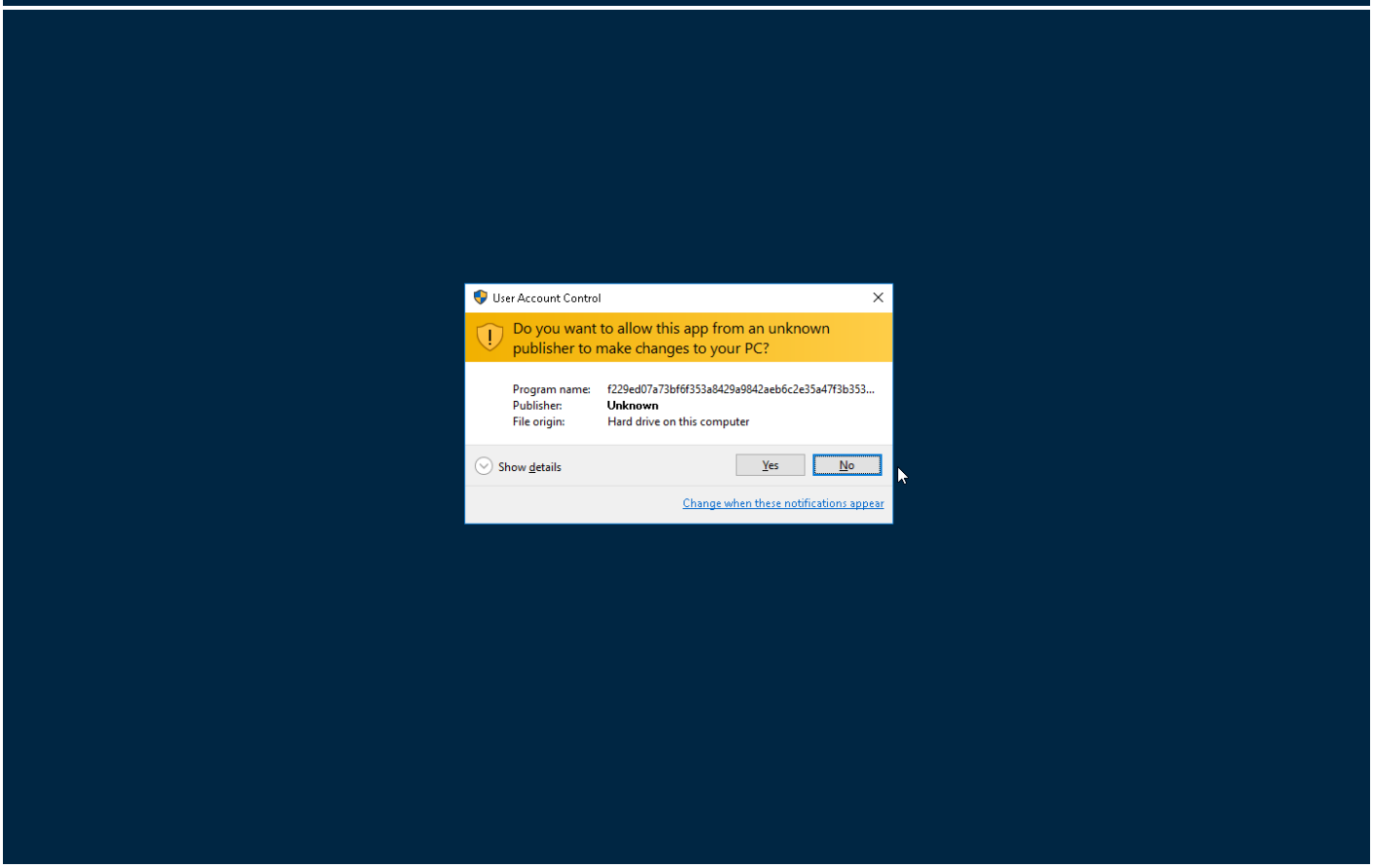
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	#T1047 Windows Management Instrumentation			#T1045 Software Packing	#T1056 Input Capture	#T1082 System Information Discovery		#T1056 Input Capture	#T1065 Uncommonly Used Port		

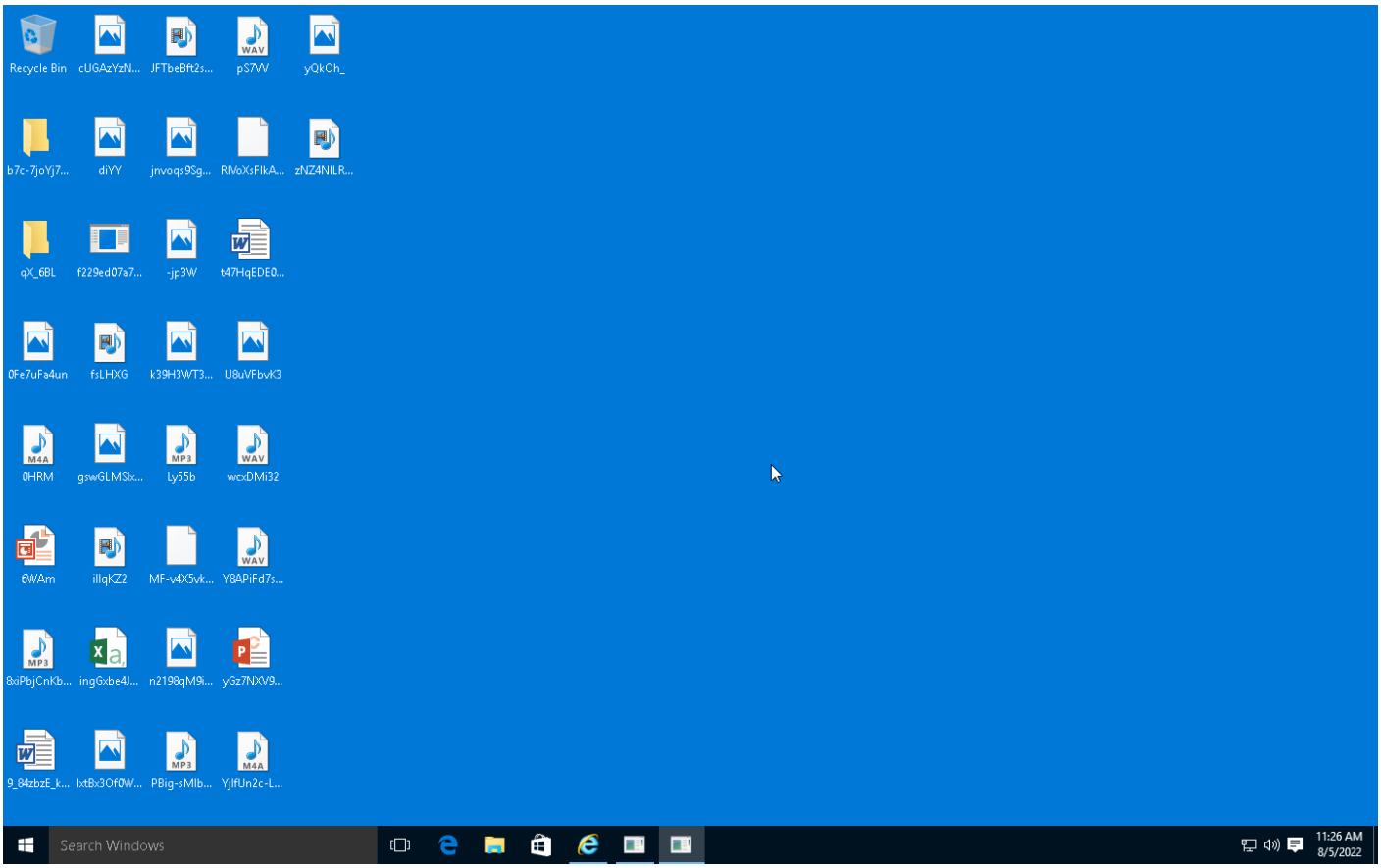
Sample Information

ID	#5067209
MD5	1f85c12fcd3232c577e5e8cc07fbf1e1
SHA1	3741755f8a11638209821a3cd7c01104acac184d
SHA256	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4
SSDeep	12288:WqShlfQIKMR4LClwugCEzE3qA2nv1gfckf:4hlYIKMCigCEzE312nKck
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe
File Size	754.50 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

Analysis Information

Creation Time	2022-08-05 13:25 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	1
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


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353...
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear


Recycle Bin
cUGAzYzN...
JFTbeBft2s...
pS7W
yQkOh_
b7c-7joYj7...
diYY
jnvoqs9Sg...
RIVoXsFIkA...
zNZ4NILR...
qX_6BL
f229ed07a7...
-jp3W
t47HqEDE0...
0Fe7uFa4un
fsLHXG
k39H3WT3...
U8uVFbvK3
0HRM
gswGLMSk...
Ly55b
wcxDMi32
6WAm
illqKZ2
MF-v4X5vk...
Y8APiFd7s...
8xiPbjCnKb...
ingGxbe4J...
n2198qM9k...
yGz7NXV9...
9_84zbzE_k...
lxtBx3Of0W...
PBig-sMlb...
YjlfUn2c-L...
Search Windows
11:26 AM
8/5/2022

NETWORK

General

2.15 KB total sent

1.62 KB total received

2 ports 5050, 53

2 contacted IP addresses

0 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

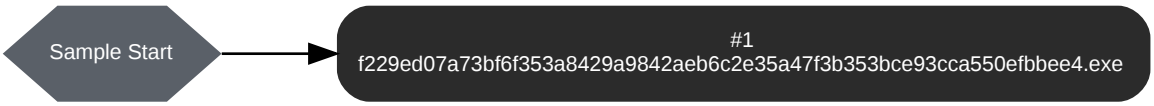
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
A	milla11.publicvm.com	NO_ERROR	91.109.186.4		NA

BEHAVIOR

Process Graph



Process #1: f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 72040, Reason: Analysis Target
Unmonitor End Time	End Time: 312048, Reason: Terminated by timeout
Monitor duration	240.01s
Return Code	Unknown
PID	3192
Parent PID	1972
Bitness	32 Bit

Host Behavior

Type	Count
Module	61
Window	3
Registry	56
Mutex	1
Keyboard	10108
File	19
-	2
User	3
Environment	2
System	50
-	1
COM	9
-	2

Network Behavior

Type	Count
DNS	1
TCP	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4	C:\Users\RDhJ0CNFevzX\Desktop\f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	Sample File	754.50 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
e2a3bd0ad84baab2d23dfbfcf8e2b6bcbf4853d9b79aa29fa778b5a523960303	-	Extracted File	12.45 KB	image/png	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	Sample File, Accessed File, VM File	Access	MALICIOUS
System Paging File	Accessed File	Access	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe.config	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	Accessed File	Access, Read	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
milla11.publicvm.com	91.109.186.4	-	TCP, DNS	MALICIOUS

IP

IP Address	Domains	Country	Protocols	Verdict
91.109.186.4	milla11.publicvm.com	France	TCP, DNS	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
d84c416188f84fa099	access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	MALICIOUS

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\AppContext	access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\Dynamic DST	access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Std	read, access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_CURRENT_USER\Software\d84c416188f84fa099\vn	read, access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_CURRENT_USER\Software\d84c416188f84fa099	create, access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Display	read, access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\MUI_Dlt	read, access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time	access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\W. Europe Standard Time\TZI	read, access	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN
HKEY_CURRENT_USER\Software\d84c416188f84fa099\[kl]	read, access, write	f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	CLEAN

Process

Process Name	Commandline	Verdict
f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe	"C:\Users\RDhJ0CNFevzX\Desktop\f229ed07a73bf6f353a8429a9842aeb6c2e35a47f3b353bce93cca550efbbee4.exe"	MALICIOUS

YARA / AV

YARA (1)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	njRAT	njRAT	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