MALICIOUS

Classifications: Backdoor, Keylogger

Threat Names: njRAT, njRAT.07Green

Verdict Reason: -

Sample Type	**Windows Exe (x86-32)**
File Name	**777.exe**
ID	#10314599
MD5	5bfdd6f255b2dae01d5c4659013cf60a
SHA1	5c13ff1330c95618545e0227ee5cc63abc54abd0
SHA256	acf17b69da3e82d40c98c9cb27c04d190a694a62113e764e8ebdf8ff08da2c37
File Size	37.00 KB
Report Created	2024-04-27 09:41 (UTC)
Target Environment	windows 10 (64bit TH2 -EN- MSO_2016) | exe

OVERVIEW

VMRay Threat Identifiers (10 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	2	Backdoor
	• YARA detected "njRAT" from ruleset "RATs" in memory dump data from (process #1) 777.exe. • YARA detected "njRAT" from ruleset "RATs" in the sample file C:\Users\RDhJ0CNFevzX\Desktop\777.exe.			
4/5	Reputation	Malicious file detected via reputation	1	-
	• The sample itself is a known malicious file.			
3/5	Network Connection	Performs DNS request for known DDNS domain	1	-
	• Resolves hostname "moso9waoaooa.zapto.org" of dynamic DNS provider "noip.com".			
2/5	Defense Evasion	Modifies Windows Firewall configuration	1	-
	• (Process #1) 777.exe adds an allowed program to the Windows Firewall configuration via netsh.			
1/5	Mutex	Creates mutex	2	-
	• (Process #1) 777.exe creates mutex with name "d86a5a37535830d84862d4926a2aa55a". • (Process #1) 777.exe creates mutex with name "Global\.net clr networking".			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #1) 777.exe starts (process #2) netsh.exe with a hidden window.			
1/5	Input Capture	Monitors keyboard input	1	Keylogger
	• (Process #1) 777.exe frequently reads the state of a keyboard key by API.			
1/5	Privilege Escalation	Enables process privileges	1	-
	• (Process #1) 777.exe enables process privilege "SeDebugPrivilege".			
1/5	Network Connection	Performs DNS request	1	-
	• (Process #1) 777.exe fails to resolve hostname "moso9waoaooa.zapto.org"			

Malware Configuration: njRAT

Metadata	Key	Extracted Value
Version	Value	im523
Mission ID	Value	HacKed
Mutex	Value	d86a5a37535830d84862d4926a2aa55a
Socket	Address Port Network Protocol C2	moso9waoaooa.zapto.org 1177 tcp ✔
Other: Network Separator	Value	|'|'|

Mitre ATT&CK Matrix

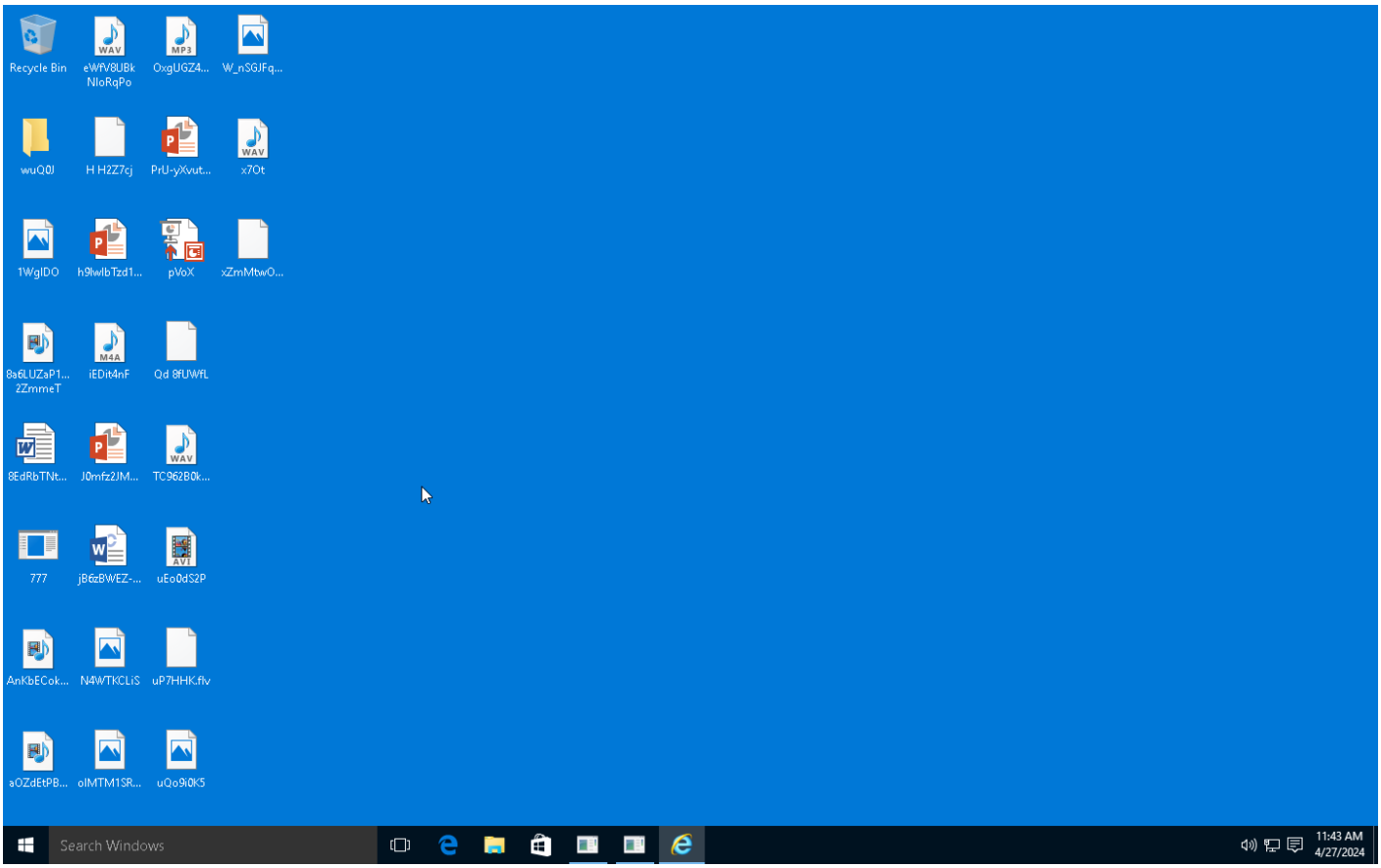
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window	#T1056 Input Capture			#T1056 Input Capture			
				#T1089 Disabling Security Tools							

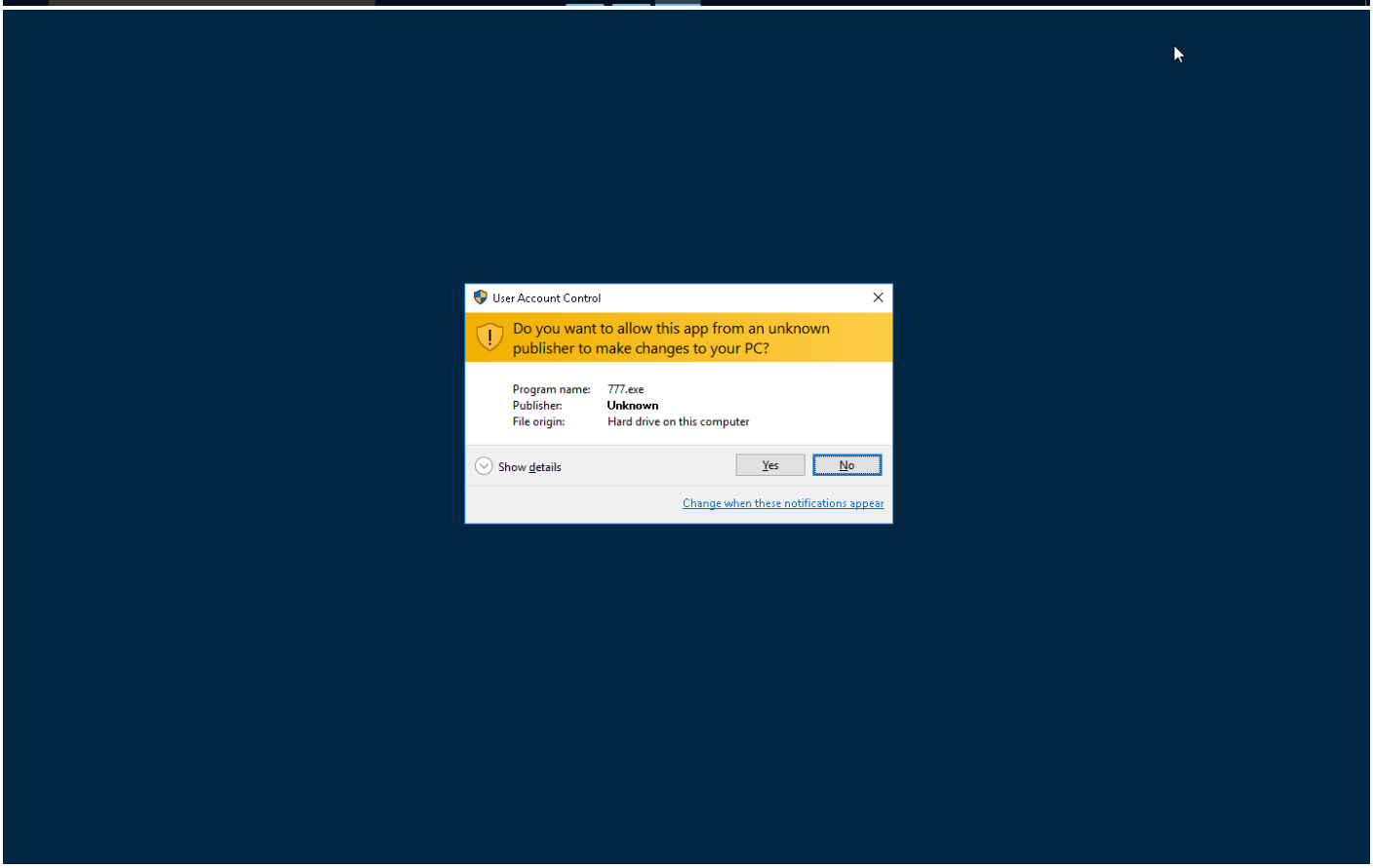
Sample Information

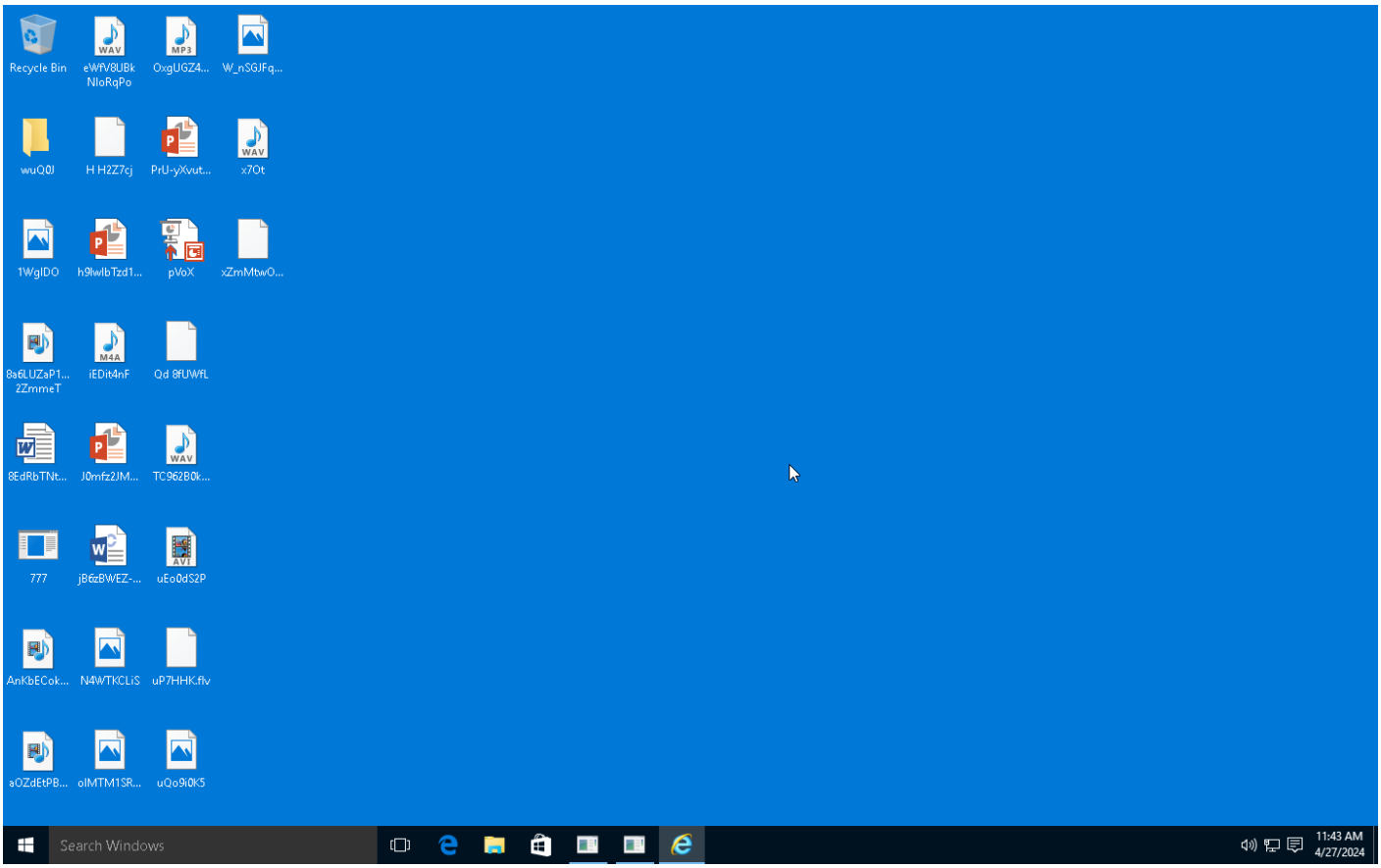
ID	#10314599
MD5	5bfdd6f255b2dae01d5c4659013cf60a
SHA1	5c13ff1330c95618545e0227ee5cc63abc54abd0
SHA256	acf17b69da3e82d40c98c9cb27c04d190a694a62113e764e8ebdf8ff08da2c37
SSDeep	384:IAG23hUidkGXR21cGMy8Pqq53tGFlymkirAF+rMRTyN/0L+EcoinblneHQM3epzl:ZG23ZLGv8Pqq58imHrM+rMRa8Nujlt
ImpHash	f34d5f2d4577ed6d9ceec516c1f5a744
File Name	777.exe
File Size	37.00 KB
Sample Type	Windows Exe (x86-32)
Has Macros	✔

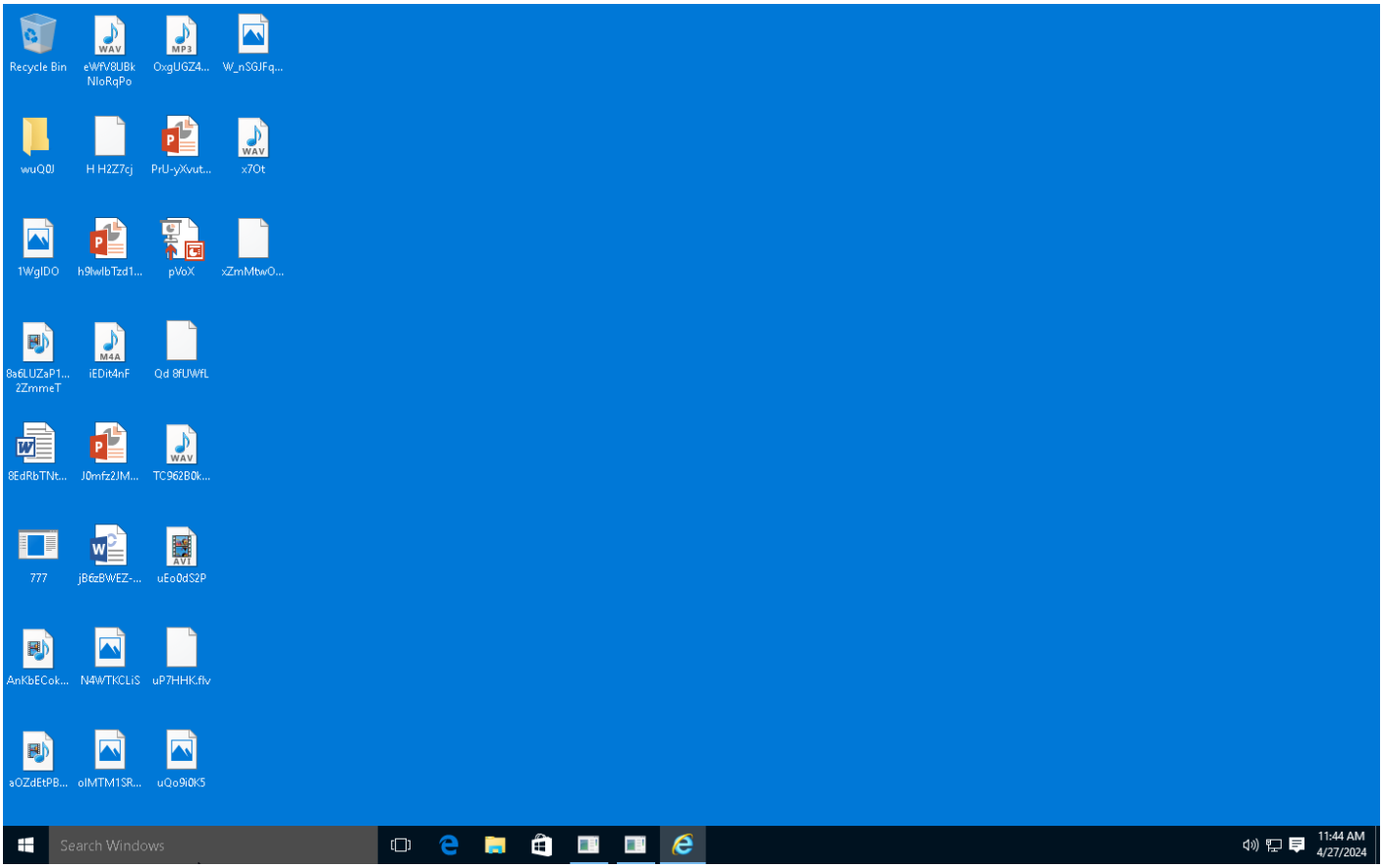
Analysis Information

Creation Time	2024-04-27 09:41 (UTC)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	2
Execution Successful	True
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
eWfV8UBk NIoRqPo
OxgUGZ4...
W_nSGJFq...
wuQ0J
H H2Z7cj
PrU-yXvut...
x7Ot
1WgIDO
h9IwlbTzd1...
pVoX
xZmMtwO...
8s6LUZaP1... 2ZmmeT
iEDit4nF
Qd 8fUWfL
8EdRbTNt...
J0mfz2JM...
TC962B0k...
777
jB6zBWEZ-...
uEo0dS2P
AnKbECok...
N4WTKCLiS
uP7HHK.flv
aOZdEtPB...
oIMTM1SR...
uQo9i0K5
Search Windows
11:43 AM
4/27/2024


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: 777.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear





Screenshots truncated

NETWORK

General

204 bytes total sent

196 bytes total received

1 ports 53

1 contacted IP addresses

0 URLs extracted

0 files downloaded

0 malicious hosts detected

DNS

3 DNS requests for 1 domains

1 nameservers contacted

1 total requests returned errors

HTTP/S

0 URLs contacted, 0 servers

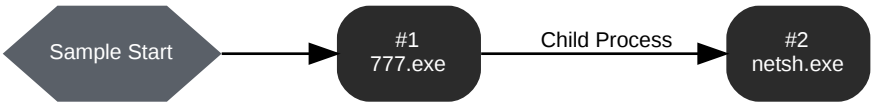
0 sessions, 0 bytes sent, 0 bytes received

DNS Requests

Type	Hostname	Response Code	Resolved IPs	CNames	Verdict
AAAA	moso9waoaooa[.]zapto[.]org	-	-	-	SUSPICIOUS

BEHAVIOR

Process Graph



Process #1: 777.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\777.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\777.exe"
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 159636, Reason: Analysis Target
Unmonitor End Time	End Time: 399652, Reason: Terminated by timeout
Monitor duration	240.02s
Return Code	Unknown
PID	2360
Parent PID	-
Bitness	32 Bit

Host Behavior

Type	Count
Module	18
System	55
Registry	23
Mutex	23
Process	1
Keyboard	3262
Window	3
File	16
User	1
-	92

Network Behavior

Type	Count
DNS	1

Process #2: netsh.exe

ID	2
File Name	c:\windows\syswow64\netsh.exe
Command Line	netsh firewall add allowedprogram "C:\Users\RDhJ0CNFevzX\Desktop\777.exe" "777.exe" ENABLE
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 175485, Reason: Child Process
Unmonitor End Time	End Time: 197595, Reason: Terminated
Monitor duration	22.11s
Return Code	0
PID	4788
Parent PID	2360
Bitness	32 Bit

Host Behavior

Type	Count
Module	41
Registry	19
System	9
File	6

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
acf17b69da3e82d40c98c9cb27c04d190a694a62113e764e8ebdf8ff08da2c37	C:\Users\RDhJ0CNFevzX\Desktop\777.exe	Sample File	37.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS
396a4debad9ef01a4c4a692e747af9708960a10ab6a353b6af09aa49ab06f9ff	-	Memory Dump	64.00 KB	application/vnd.microsoft.portable-executable	-	MALICIOUS

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\777.exe	Sample File	-	MALICIOUS
System Paging File	Accessed File	Access	CLEAN
C:\Windows\SYSTEM32\MFC42u.dll	Accessed File	Access	CLEAN
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Config\machine.config	Accessed File	Access, Read	CLEAN
C:\Users\RDhJ0CNFevzX\Desktop\777.config	Accessed File	Access	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
moso9waoaooa[.]zapto[.]org	-	-	-	SUSPICIOUS

Mutex

Name	Operations	Parent Process Name	Verdict
d86a5a37535830d84862d4926a2aa55a	access	777.exe	MALICIOUS
Global\.net clr networking	delete, access	777.exe	CLEAN

Registry

Registry Key	Operations	Parent Process Name	Verdict
HKEY_CURRENT_USER\Software\d86a5a37535830d84862d4926a2aa55a	access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NetSh	access	netsh.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework	access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgJITDebugLaunchSetting	read, access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\DbgManagedDebugger	read, access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion	access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\InstallationType	read, access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance	access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\Library	read, access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\IsMultiInstance	read, access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.NET CLR Networking\Performance\First Counter	read, access	777.exe	CLEAN

Registry Key	Operations	Parent Process Name	Verdict
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance	access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\CategoryOptions	read, access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\FileMappingSize	read, access	777.exe	CLEAN
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.net clr networking\Performance\Counter Names	read, access	777.exe	CLEAN

Process

Process Name	Commandline	Verdict
777.exe	"C:\Users\RDhJ0CNFevzX\Desktop\777.exe"	MALICIOUS
netsh.exe	netsh firewall add allowedprogram "C:\Users\RDhJ0CNFevzX\Desktop\777.exe" "777.exe" ENABLE	CLEAN

YARA / AV

YARA (2)

Ruleset Name	Rule Name	Rule Description	File Type	File Name	Classification	Verdict
RATs	njRAT	njRAT	Sample File	C:\Users\RDhJ0CNFevzX\Desktop\777.exe	Backdoor	5/5
RATs	njRAT	njRAT	Memory Dump	-	Backdoor	5/5

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	windows 10 (64bit TH2 -EN- MSO_2016)
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	2024.2.1
Dynamic Engine Version	2024.2.1 / 03/23/2024 11:02
Static Engine Version	2024.2.1.0 / 2024-03-23 09:36:38
AV Exceptions Version	2024.2.1.5 / 2024-03-22 20:39:30
Link Detonation Heuristics Version	2024.2.1.18 / 2024-04-18 14:31:08
Smart Memory Dumping Rules Version	2024.2.1.5 / 2024-03-22 20:39:30
Config Extractors Version	2024.2.1.18 / 2024-04-18 14:31:08
Signature Trust Store Version	2024.2.1.9 / 2024-03-26 09:11:11
VMRay Threat Identifiers Version	2024.2.1.23 / 2024-04-25 06:55:37
YARA Built-in Ruleset Version	2024.2.1.18

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	8.0.1710.11

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