ID: 553248
Sample Name: 72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe
Cookbook: default.jbs
Time: 14:54:23
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

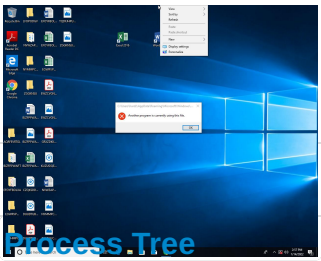
Windows Analysis Report 72CA3E2F8479A075C8E089F…

Overview

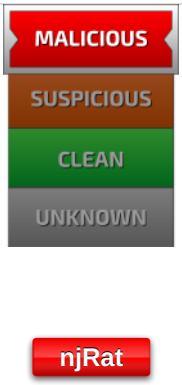
General Information

Sample Name:	72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe
Analysis ID:	553248
MD5:	70aca878bfaac1e..
SHA1:	4997c055b582c7..
SHA256:	72ca3e2f8479a07.
Tags:	exe njrat RAT
Infos:	

Most interesting Screenshot:



Detection

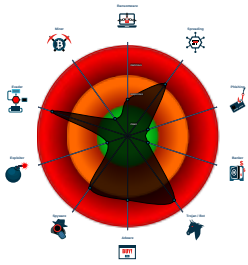


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Sigma detected: Drops fake system…
- Multi AV Scanner detection for subm…
- Detected njRat
- Malicious sample detected (through …
- Yara detected Njrat
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Uses netsh to modify the Windows n…

Classification



- **System is w10x64**
- 72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe (PID: 6756 cmdline: "C:\Users\user\Desktop\72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe" MD5: 70ACA878BFAAC1EAF7019EDDD97FC877)
  - System.exe (PID: 5628 cmdline: "C:\Users\user\AppData\Roaming\System.exe" MD5: 70ACA878BFAAC1EAF7019EDDD97FC877)
    - netsh.exe (PID: 2976 cmdline: netsh firewall add allowedprogram "C:\Users\user\AppData\Roaming\System.exe" "System.exe" ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 1876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- System.exe (PID: 6172 cmdline: "C:\Users\user\AppData\Roaming\System.exe" .. MD5: 70ACA878BFAAC1EAF7019EDDD97FC877)
- System.exe (PID: 6964 cmdline: "C:\Users\user\AppData\Roaming\System.exe" .. MD5: 70ACA878BFAAC1EAF7019EDDD97FC877)
- System.exe (PID: 5224 cmdline: "C:\Users\user\AppData\Roaming\System.exe" .. MD5: 70ACA878BFAAC1EAF7019EDDD97FC877)
- **cleanup**

Malware Configuration

Threatname: Njrat


```
{
  "Host": "System.exe",
  "Port": "13467",
  "Mutex": "9156ea52d892a71a5c604fdd4141de82",
  "Registry Value": "Software\\Microsoft\\Windows\\CurrentVersion\\Run",
  "Campaign ID": "HacKed",
  "Version": "im523",
  "Network Seprator": "|'|'|"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	

Source	Rule	Description	Author	Strings
72CA3E2F8479A075C8E089F543F79C4F1CF868D6 6D327.exe	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x80de:$a1: netsh firewall add allowedprogram • 0x82d8:$b1: [TAP] • 0x827e:$b2: & exit • 0x824a:$c1: md.exe /k ping 0 & del

Dropped Files

Source	Rule	Description	Author	Strings
C:\svchost.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
C:\svchost.exe	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x80de:$a1: netsh firewall add allowedprogram • 0x82d8:$b1: [TAP] • 0x827e:$b2: & exit • 0x824a:$c1: md.exe /k ping 0 & del
C:\Users\user\AppData\Roaming\System.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
C:\Users\user\AppData\Roaming\System.exe	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x80de:$a1: netsh firewall add allowedprogram • 0x82d8:$b1: [TAP] • 0x827e:$b2: & exit • 0x824a:$c1: md.exe /k ping 0 & del
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd 4141de82.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.318400224.0000000000C72000.00000 002.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000004.00000000.318400224.0000000000C72000.00000 002.00020000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x7ede:$a1: netsh firewall add allowedprogram • 0x80d8:$b1: [TAP] • 0x807e:$b2: & exit • 0x804a:$c1: md.exe /k ping 0 & del
0000000C.00000000.392201898.0000000000512000.00000 002.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
0000000C.00000000.392201898.0000000000512000.00000 002.00020000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x7ede:$a1: netsh firewall add allowedprogram • 0x80d8:$b1: [TAP] • 0x807e:$b2: & exit • 0x804a:$c1: md.exe /k ping 0 & del
0000000C.00000002.403902841.0000000000512000.00000 002.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.System.exe.c70000.1.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
4.0.System.exe.c70000.1.unpack	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x80de:$a1: netsh firewall add allowedprogram • 0x82d8:$b1: [TAP] • 0x827e:$b2: & exit • 0x824a:$c1: md.exe /k ping 0 & del
9.2.System.exe.f50000.0.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
9.2.System.exe.f50000.0.unpack	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x80de:$a1: netsh firewall add allowedprogram • 0x82d8:$b1: [TAP] • 0x827e:$b2: & exit • 0x824a:$c1: md.exe /k ping 0 & del
4.0.System.exe.c70000.0.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
Click to see the 21 entries				

Sigma Overview

System Summary:

Sigma detected: Netsh Port or Application Allowed

HIPS / PFW / Operating System Protection Evasion:

Sigma detected: Drops fake system file at system root drive

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected Njrat
- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for domain / URL
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Spreading:

- Creates autorun.inf (USB autostart)

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- Connects to many ports of the same IP (likely port scanning)
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:

- Yara detected Njrat

Operating System Destruction:

- Protects its processes via BreakOnTermination flag

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Persistence and Installation Behavior:

- Drops PE files with benign system names

Boot Survival:

Drops PE files to the startup folder

Creates autostart registry keys with suspicious names

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information:

Yara detected Njrat

Remote Access Functionality:

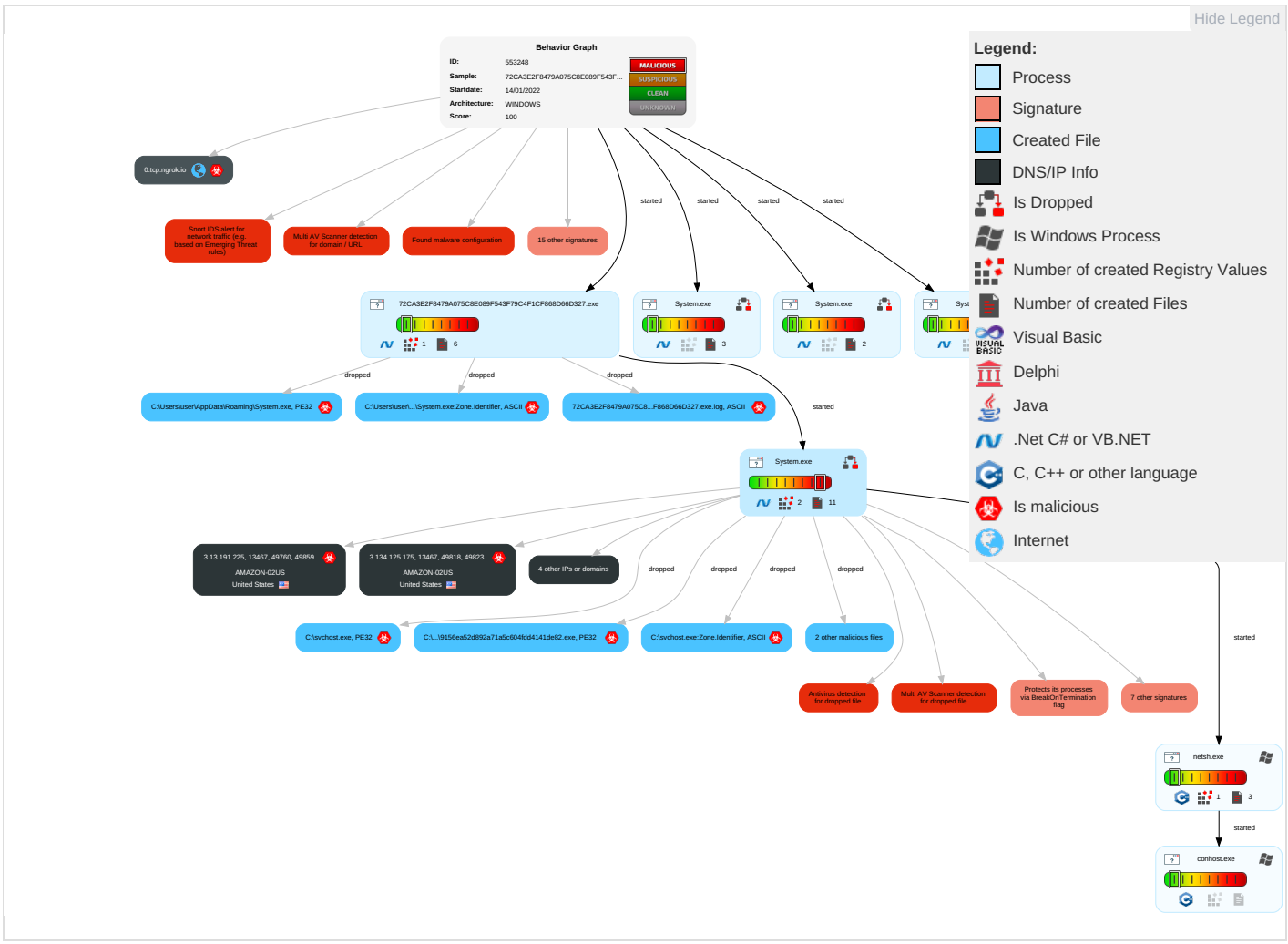
Detected njRat

Yara detected Njrat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Replication Through Removable Media 1 1	Native API 1	Registry Run Keys / Startup Folder 2 2 1	Process Injection 1 2	Masquerading 1 1	Input Capture 1 1	Security Software Discovery 1 1	Replication Through Removable Media 1 1	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 2 2 1	Disable or Modify Tools 2 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Peripheral Device Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe	77%	Virustotal		Browse
72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe	86%	Metadefender		Browse
72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe	95%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe	100%	Avira	TR/ATRAPS.Gen	
72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\System.exe	100%	Avira	TR/ATRAPS.Gen	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe	100%	Avira	TR/ATRAPS.Gen	
C:\svchost.exe	100%	Avira	TR/ATRAPS.Gen	
C:\Users\user\AppData\Roaming\System.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe	100%	Joe Sandbox ML		
C:\svchost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe	77%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe	86%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe	95%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Roaming\System.exe	77%	Virustotal		Browse
C:\Users\user\AppData\Roaming\System.exe	86%	Metadefender		Browse
C:\Users\user\AppData\Roaming\System.exe	95%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\svchost.exe	77%	Virustotal		Browse
C:\svchost.exe	86%	Metadefender		Browse
C:\svchost.exe	95%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe.840000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
9.0.System.exe.f50000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.System.exe.c70000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.2.System.exe.c70000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.System.exe.c70000.2.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.System.exe.c70000.3.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
12.0.System.exe.510000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
0.2.72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe.840000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.System.exe.c70000.1.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
11.0.System.exe.50000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
12.2.System.exe.510000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
11.2.System.exe.50000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
9.2.System.exe.f50000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
0.tcp.ngrok.io	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
System.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
0.tcp.ngrok.io	3.17.7.232	true	true	• 14%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
System.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.134.125.175	unknown	United States		16509	AMAZON-02US	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.17.7.232	0.tcp.ngrok.io	United States		16509	AMAZON-02US	true
3.22.30.40	unknown	United States		16509	AMAZON-02US	true
3.14.182.203	unknown	United States		16509	AMAZON-02US	true
3.13.191.225	unknown	United States		16509	AMAZON-02US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553248
Start date:	14.01.2022
Start time:	14:54:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.spre.troj.adwa.spyw.evad.winEXE@9/10@42/6
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 11.8% (good quality ratio 7.7%) • Quality average: 46.8% • Quality standard deviation: 38.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:55:43	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 9156ea52d892a71a5c604fdd4141de82 " C:\Users\user\AppData\Roaming\System.exe" ..
14:55:51	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run 9156ea52d892a71a5c604fdd4141de82 "C:\Users\user\AppData\Roaming\System.exe" ..
14:55:59	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 9156ea52d892a71a5c604fdd4141de82 "C:\Users\user\AppData\Roaming\System.exe" ..

Time	Type	Description
14:56:07	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe.log	
Process:	C:\Users\user\Desktop\72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk7v:MLF20NaL3z2p29hJ5g522r0
MD5:	80EFBEC081D7836D240503C4C9465FEC
SHA1:	6AF398E08A359457083727BAF296445030A55AC3
SHA-256:	C73F730EB5E05D15FAD6BE10AB51FE4D8A80B5E88B89D8BC80CC1DF09ACE1523
SHA-512:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5E
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\System.exe.log	
Process:	C:\Users\user\AppData\Roaming\System.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk7v:MLF20NaL3z2p29hJ5g522r0
MD5:	80EFBEC081D7836D240503C4C9465FEC
SHA1:	6AF398E08A359457083727BAF296445030A55AC3
SHA-256:	C73F730EB5E05D15FAD6BE10AB51FE4D8A80B5E88B89D8BC80CC1DF09ACE1523

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\System.exe.log	
SHA-512:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5E
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe	
Process:	C:\Users\user\AppData\Roaming\System.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.575659694964963
Encrypted:	false
SSDEEP:	384:3IhqBkiyrnDNGRn5IyUv6IzfDhW/6wFbbrAF+rMRTyN/0L+EcoinblneHQM3epz3:If5M5jUvPzQCw1rM+rMRa8Nu1pt
MD5:	70ACA878BFAAC1EAF7019EDDD97FC877
SHA1:	4997C055B582C71CBB3863C9523986B51A339797
SHA-256:	72CA3E2F8479A075C8E089F543F79C4F1CF868D66D3272B2E6B0F0FDED1BDB60
SHA-512:	17BEDCD516BA8F18B5E4D8A2A8C9D1B6E95BE2158D654B3B15FE2D379CDCE682C609801E1B5C01487FA732EF1591D7CDE1460448FFD4FFE8A50F6C3C82CB3C2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe, Author: Brian Wallace @botnet_hunter
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 77%, Browse • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 95%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.`..... .....@.. ..... ..@.....p...K.....@..... ..... ..H.....text..... ..... ..`.rsrc...@.....@..@.relo c.....@..B.....H.....e...E.....&.(.....**..(.....*.s.....s.....s.....s.....*.0.....~....o.....+..*.0.....~... .o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....(....(.....+..*...0.....(.....+..*.0.....(.....+..*.0.....(.....+..*.0.. .....,(...+.+.+....+...*.0..... .....**..(.....*....0..&.....~.....,(...+.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\9156ea52d892a71a5c604fdd4141de82.exe:Zone.Identifier	
Process:	C:\Users\user\AppData\Roaming\System.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\System.exe	
Process:	C:\Users\user\Desktop\72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.575659694964963
Encrypted:	false
SSDEEP:	384:3IhqBkiyrnDNGRn5IyUv6IzfDhW/6wFbbrAF+rMRTyN/0L+EcoinblneHQM3epz3:If5M5jUvPzQCw1rM+rMRa8Nu1pt
MD5:	70ACA878BFAAC1EAF7019EDDD97FC877
SHA1:	4997C055B582C71CBB3863C9523986B51A339797
SHA-256:	72CA3E2F8479A075C8E089F543F79C4F1CF868D66D3272B2E6B0F0FDED1BDB60

C:\Users\user\AppData\Roaming\System.exe	
SHA-512:	17BEDCD516BA8F18B5E4D8A2A8C9D1B6E95BE2158D654B3B15FE2D379CDCE682C609801E1B5C01487FA732EF1591D7CDE1460448FFD4FFE8A50F6C3C82CB3C2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\System.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\System.exe, Author: Brian Wallace @botnet_hunter
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 77%, Browse • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 95%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.`..... .....@.. ..... ..@.....p...K.....@..... ..... ..H.....text..... ..... ..`.rsrc...@.....@..@.relo c.....@..B.....H.....e...E.....&.(.....**..(.....*.s.....s.....s.....s.....*.0.....~....o.....+..*.0.....~... .o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....(....(.....+..*...0.....(.....+..*.0.....(.....+..*.0.....(.....+..*.0.. .....,(...+.+.+....+...*.0..... .....**..(.....*....0..&.....~.....,(...+.

C:\Users\user\AppData\Roaming\System.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\autorun.inf	
Process:	C:\Users\user\AppData\Roaming\System.exe
File Type:	Microsoft Windows Autorun file, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	50
Entropy (8bit):	4.320240000427043
Encrypted:	false
SSDEEP:	3:It1KV2LKMACovK0x:e1KzxvD
MD5:	5B0B50BADE67C5EC92D42E971287A5D9
SHA1:	90D5C99143E7A56AD6E5EE401015F8ECC093D95A
SHA-256:	04DDE2489D2D2E6846D42250D813AB90B5CA847D527F8F2C022E6C327DC6DB53
SHA-512:	C064DC3C4185A38D1CAEBD069ACB9FDBB85DFB650D6A241036E501A09BC89FD06E267BE9D400D20E6C14B4068473D1C6557962E8D82FDFD191DB7EABB6E6621
Malicious:	**true**
Preview:	[autorun]..open=C:\svchost.exe..shellexecute=C:\..

C:\svchost.exe	
Process:	C:\Users\user\AppData\Roaming\System.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.575659694964963
Encrypted:	false
SSDEEP:	384:3IhqBkiyrnDNGRn5IyUv6IzfDhW/6wFbbrAF+rMRTyN/0L+EcoinblneHQM3epz3:If5M5jUvPzQCw1rM+rMRa8Nu1pt
MD5:	70ACA878BFAAC1EAF7019EDDD97FC877
SHA1:	4997C055B582C71CBB3863C9523986B51A339797
SHA-256:	72CA3E2F8479A075C8E089F543F79C4F1CF868D66D3272B2E6B0F0FDED1BDB60
SHA-512:	17BEDCD516BA8F18B5E4D8A2A8C9D1B6E95BE2158D654B3B15FE2D379CDCE682C609801E1B5C01487FA732EF1591D7CDE1460448FFD4FFE8A50F6C3C82CB3C2
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\svchost.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\svchost.exe, Author: Brian Wallace @botnet_hunter

C:\svchost.exe	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 77%, Browse • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 95%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.`..... ..... .....@.. ..... ..@.....p...K.....@..... ..... ..H.....text..... ..... ..`.rsrc...@.....@..@.relo c.....@..B.....H.....e...E.....&.(.....**..(.....*.s.....s.....s.....s.....*.0.....~....o....+..*.0.....~... .o.....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....(....(.....+..*...0.....(.....+..*.0.....(.....+..*.0.....(.....+..*.0.. .....,.(...+.+.+....+...*.0..... .....**..(.....*....0..&.....~.....,.(...+.

C:\svchost.exe:Zone.Identifier	
Process:	C:\Users\user\AppData\Roaming\System.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\netsh.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	313
Entropy (8bit):	4.971939296804078
Encrypted:	false
SSDEEP:	6:/ojfKsUTGN8Ypox42k9L+DbGMKeQE+vigqAZs2E+AYeDPO+Yswyha:wjPIGNrkHk9iaeIM6ADDPOHyha
MD5:	689E2126A85BF55121488295EE068FA1
SHA1:	09BAAA253A49D80C18326DFBCA106551EBF22DD6
SHA-256:	D968A966EF474068E41256321F77807A042F1965744633D37A203A705662EC25
SHA-512:	C3736A8FC7E6573FA1B26FE6A901C05EE85C55A4A276F8F569D9EADC9A58BEC507D1BB90DBF9EA62AE79A6783178C69304187D6B90441D82E46F5F56172B5C5C
Malicious:	false
Preview:	..IMPORTANT: Command executed successfully...However, "netsh firewall" is deprecated;..use "netsh advfirewall firewall" instead...For more information on using "netsh advfirewall firewall" commands..instead of "netsh firewall", see KB article 947709..at https://go.microsoft.com/fwlink/?linkid=121488 .....Ok.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.575659694964963
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe
File size:	37888
MD5:	70aca878bfaac1eaf7019eddd97fc877
SHA1:	4997c055b582c71cbb3863c9523986b51a339797
SHA256:	72ca3e2f8479a075c8e089f543f79c4f1cf868d66d3272b2e6b0f0fded1bdb60

General

SHA512:	17bedcd516ba8f18b5e4d8a2a8c9d1b6e95be2158d654b3b15fe2d379cdce682c609801e1b5c01487fa732ef1591d7cde1460448ffd4ffe8a50f6c3c82cb36c2
SSDEEP:	384:3IhqBkiyrnDNGRn5IyUv6IzfDhW/6wFbbrAF+rMRTyN/0L+EcoinblneHQM3epz3:If5M5jUvPzQCw1rM+rMRa8Nu1pt
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.`..... ....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40abbe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60AB6F12 [Mon May 24 09:17:06 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x8bc4	0x8c00	False	0.463895089286	data	5.60730804361	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc000	0x240	0x400	False	0.3134765625	data	4.96877165952	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:55:46.343993	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49753	13467	192.168.2.3	3.17.7.232
01/14/22-14:55:48.595556	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60784	8.8.8.8	192.168.2.3
01/14/22-14:55:48.762801	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49754	13467	192.168.2.3	3.17.7.232
01/14/22-14:55:51.454912	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49755	13467	192.168.2.3	3.17.7.232
01/14/22-14:55:54.224128	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49758	13467	192.168.2.3	3.17.7.232
01/14/22-14:55:57.123895	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49759	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:00.006211	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49760	13467	192.168.2.3	3.13.191.225
01/14/22-14:56:03.177148	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49761	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:05.935422	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55102	8.8.8.8	192.168.2.3
01/14/22-14:56:06.098596	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49762	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:08.812231	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56236	8.8.8.8	192.168.2.3
01/14/22-14:56:08.974929	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49763	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:11.736334	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49559	8.8.8.8	192.168.2.3
01/14/22-14:56:11.904970	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49765	13467	192.168.2.3	3.22.30.40
01/14/22-14:56:14.639656	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49767	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:17.749487	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49770	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:20.375566	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49771	13467	192.168.2.3	3.17.7.232
01/14/22-14:56:23.288901	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49773	13467	192.168.2.3	3.22.30.40
01/14/22-14:56:26.086507	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49778	13467	192.168.2.3	3.17.7.232
01/14/22-14:56:28.732206	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49799	13467	192.168.2.3	3.17.7.232
01/14/22-14:56:31.478555	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49803	13467	192.168.2.3	3.22.30.40
01/14/22-14:56:34.195822	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49813	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:36.993737	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49816	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:39.740921	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49818	13467	192.168.2.3	3.134.125.175
01/14/22-14:56:42.427424	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49819	13467	192.168.2.3	3.17.7.232
01/14/22-14:56:45.091298	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49820	13467	192.168.2.3	3.17.7.232
01/14/22-14:56:47.745365	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49821	13467	192.168.2.3	3.22.30.40
01/14/22-14:56:50.337717	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50824	8.8.8.8	192.168.2.3
01/14/22-14:56:50.506419	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49822	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:53.280011	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49823	13467	192.168.2.3	3.134.125.175
01/14/22-14:56:55.918054	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62855	8.8.8.8	192.168.2.3
01/14/22-14:56:56.085319	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49825	13467	192.168.2.3	3.14.182.203
01/14/22-14:56:58.776496	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49826	13467	192.168.2.3	3.22.30.40
01/14/22-14:57:01.289281	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49290	8.8.8.8	192.168.2.3
01/14/22-14:57:01.456784	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49840	13467	192.168.2.3	3.22.30.40
01/14/22-14:57:04.185000	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49851	13467	192.168.2.3	3.14.182.203
01/14/22-14:57:06.846067	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49852	13467	192.168.2.3	3.134.125.175

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-14:57:09.672363	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49857	13467	192.168.2.3	3.22.30.40
01/14/22-14:57:12.379810	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49858	13467	192.168.2.3	3.134.125.175
01/14/22-14:57:15.052356	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49859	13467	192.168.2.3	3.13.191.225
01/14/22-14:57:17.712854	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49860	13467	192.168.2.3	3.13.191.225
01/14/22-14:57:20.383404	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49861	13467	192.168.2.3	3.134.125.175
01/14/22-14:57:23.134241	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49862	13467	192.168.2.3	3.14.182.203
01/14/22-14:57:25.811740	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49864	13467	192.168.2.3	3.134.125.175
01/14/22-14:57:28.851831	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49865	13467	192.168.2.3	3.22.30.40
01/14/22-14:57:31.155906	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49866	13467	192.168.2.3	3.22.30.40
01/14/22-14:57:33.794104	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49867	13467	192.168.2.3	3.13.191.225
01/14/22-14:57:36.531249	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49868	13467	192.168.2.3	3.13.191.225
01/14/22-14:57:39.326499	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49869	13467	192.168.2.3	3.22.30.40

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:55:45.826014996 CET	192.168.2.3	8.8.8.8	0x354d	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:48.573869944 CET	192.168.2.3	8.8.8.8	0x7217	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:51.250332117 CET	192.168.2.3	8.8.8.8	0x1e2	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:54.034359932 CET	192.168.2.3	8.8.8.8	0x5d28	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:56.930083036 CET	192.168.2.3	8.8.8.8	0xc746	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:59.640835047 CET	192.168.2.3	8.8.8.8	0x47a0	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:02.986785889 CET	192.168.2.3	8.8.8.8	0x53ee	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:05.912566900 CET	192.168.2.3	8.8.8.8	0x1b23	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:08.785914898 CET	192.168.2.3	8.8.8.8	0x7451	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:11.714885950 CET	192.168.2.3	8.8.8.8	0xa4dd	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:14.454736948 CET	192.168.2.3	8.8.8.8	0xb74	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:17.219274998 CET	192.168.2.3	8.8.8.8	0xd3e	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:20.142657042 CET	192.168.2.3	8.8.8.8	0x4e7a	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:23.108827114 CET	192.168.2.3	8.8.8.8	0x900e	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:25.848159075 CET	192.168.2.3	8.8.8.8	0xa643	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:28.549057961 CET	192.168.2.3	8.8.8.8	0x1087	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:31.243753910 CET	192.168.2.3	8.8.8.8	0x990c	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:56:33.952836037 CET	192.168.2.3	8.8.8.8	0x8d4	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:36.805179119 CET	192.168.2.3	8.8.8.8	0xf5b	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:39.552303076 CET	192.168.2.3	8.8.8.8	0x135d	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:42.237478018 CET	192.168.2.3	8.8.8.8	0x8ce5	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:44.912789106 CET	192.168.2.3	8.8.8.8	0x1565	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:47.566504002 CET	192.168.2.3	8.8.8.8	0xfe29	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:50.310465097 CET	192.168.2.3	8.8.8.8	0xecf	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:53.083189011 CET	192.168.2.3	8.8.8.8	0xa4dd	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:55.895234108 CET	192.168.2.3	8.8.8.8	0x6f54	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:58.591355085 CET	192.168.2.3	8.8.8.8	0x3abe	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:01.259596109 CET	192.168.2.3	8.8.8.8	0xa299	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:03.945168972 CET	192.168.2.3	8.8.8.8	0x5d9f	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:06.660762072 CET	192.168.2.3	8.8.8.8	0x7ff4	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:09.400335073 CET	192.168.2.3	8.8.8.8	0x296d	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:12.201404095 CET	192.168.2.3	8.8.8.8	0xcb98	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:14.870506048 CET	192.168.2.3	8.8.8.8	0x7190	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:17.534580946 CET	192.168.2.3	8.8.8.8	0x2b1b	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:20.180349112 CET	192.168.2.3	8.8.8.8	0x732d	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:22.931205988 CET	192.168.2.3	8.8.8.8	0xff31	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:25.630670071 CET	192.168.2.3	8.8.8.8	0x3ef9	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:28.312005997 CET	192.168.2.3	8.8.8.8	0x5e29	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:30.979021072 CET	192.168.2.3	8.8.8.8	0xf575	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:33.620198011 CET	192.168.2.3	8.8.8.8	0xec81	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:36.354939938 CET	192.168.2.3	8.8.8.8	0x2c4c	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:39.139276981 CET	192.168.2.3	8.8.8.8	0x4984	Standard query (0)	0.tcp.ngrok.io	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:55:45.845385075 CET	8.8.8.8	192.168.2.3	0x354d	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:48.595556021 CET	8.8.8.8	192.168.2.3	0x7217	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:51.267457962 CET	8.8.8.8	192.168.2.3	0x1e2	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:54.053494930 CET	8.8.8.8	192.168.2.3	0x5d28	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:56.949445963 CET	8.8.8.8	192.168.2.3	0xc746	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:55:59.660417080 CET	8.8.8.8	192.168.2.3	0x47a0	No error (0)	0.tcp.ngrok.io		3.13.191.225	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:03.006030083 CET	8.8.8.8	192.168.2.3	0x53ee	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:56:05.935421944 CET	8.8.8.8	192.168.2.3	0x1b23	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:08.812231064 CET	8.8.8.8	192.168.2.3	0x7451	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:11.736334085 CET	8.8.8.8	192.168.2.3	0xa4dd	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:14.474361897 CET	8.8.8.8	192.168.2.3	0xb74	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:17.238837957 CET	8.8.8.8	192.168.2.3	0xd3e	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:20.162110090 CET	8.8.8.8	192.168.2.3	0x4e7a	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:23.126688004 CET	8.8.8.8	192.168.2.3	0x900e	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:25.867337942 CET	8.8.8.8	192.168.2.3	0xa643	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:28.568577051 CET	8.8.8.8	192.168.2.3	0x1087	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:31.262999058 CET	8.8.8.8	192.168.2.3	0x990c	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:33.969996929 CET	8.8.8.8	192.168.2.3	0x8d4	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:36.825191021 CET	8.8.8.8	192.168.2.3	0xf5b	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:39.572302103 CET	8.8.8.8	192.168.2.3	0x135d	No error (0)	0.tcp.ngrok.io		3.134.125.175	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:42.254549980 CET	8.8.8.8	192.168.2.3	0x8ce5	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:44.930639029 CET	8.8.8.8	192.168.2.3	0x1565	No error (0)	0.tcp.ngrok.io		3.17.7.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:47.586004019 CET	8.8.8.8	192.168.2.3	0xfe29	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:50.337717056 CET	8.8.8.8	192.168.2.3	0xecf	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:53.101566076 CET	8.8.8.8	192.168.2.3	0xa4dd	No error (0)	0.tcp.ngrok.io		3.134.125.175	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:55.918054104 CET	8.8.8.8	192.168.2.3	0x6f54	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:56:58.608932018 CET	8.8.8.8	192.168.2.3	0x3abe	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:01.289280891 CET	8.8.8.8	192.168.2.3	0xa299	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:03.965209007 CET	8.8.8.8	192.168.2.3	0x5d9f	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:06.680274010 CET	8.8.8.8	192.168.2.3	0x7ff4	No error (0)	0.tcp.ngrok.io		3.134.125.175	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:09.419737101 CET	8.8.8.8	192.168.2.3	0x296d	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:12.220947981 CET	8.8.8.8	192.168.2.3	0xcb98	No error (0)	0.tcp.ngrok.io		3.134.125.175	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:14.890022993 CET	8.8.8.8	192.168.2.3	0x7190	No error (0)	0.tcp.ngrok.io		3.13.191.225	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:57:17.553966999 CET	8.8.8.8	192.168.2.3	0x2b1b	No error (0)	0.tcp.ngrok.io		3.13.191.225	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:20.201327085 CET	8.8.8.8	192.168.2.3	0x732d	No error (0)	0.tcp.ngrok.io		3.134.125.175	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:22.950678110 CET	8.8.8.8	192.168.2.3	0xff31	No error (0)	0.tcp.ngrok.io		3.14.182.203	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:25.649379969 CET	8.8.8.8	192.168.2.3	0x3ef9	No error (0)	0.tcp.ngrok.io		3.134.125.175	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:28.331880093 CET	8.8.8.8	192.168.2.3	0x5e29	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:30.998452902 CET	8.8.8.8	192.168.2.3	0xf575	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:33.639610052 CET	8.8.8.8	192.168.2.3	0xec81	No error (0)	0.tcp.ngrok.io		3.13.191.225	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:36.375444889 CET	8.8.8.8	192.168.2.3	0x2c4c	No error (0)	0.tcp.ngrok.io		3.13.191.225	A (IP address)	IN (0x0001)
Jan 14, 2022 14:57:39.159666061 CET	8.8.8.8	192.168.2.3	0x4984	No error (0)	0.tcp.ngrok.io		3.22.30.40	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe PID: 6756 Parent PID: 2944

General

Start time:	14:55:24
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\72CA3E2F8479A075C8E089F543F79C4F1CF868D66D327.exe"
Imagebase:	0x840000
File size:	37888 bytes
MD5 hash:	70ACA878BFAAC1EAF7019EDDD97FC877
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000000.300280402.0000000000842000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000000.300280402.0000000000842000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.319076223.0000000000842000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000002.319076223.0000000000842000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: System.exe PID: 5628 Parent PID: 6756

General

Start time:	14:55:32
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\System.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\System.exe"
Imagebase:	0xc70000
File size:	37888 bytes
MD5 hash:	70ACA878BFAAC1EAF7019EDDD97FC877
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000000.318400224.0000000000C72000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000000.318400224.0000000000C72000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000000.317417479.0000000000C72000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000000.317417479.0000000000C72000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000000.317702364.0000000000C72000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000000.317702364.0000000000C72000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000000.317974918.0000000000C72000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000000.317974918.0000000000C72000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000002.571615119.0000000000C72000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000002.571615119.0000000000C72000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\System.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\System.exe, Author: Brian Wallace @botnet_hunter
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 77%, Virustotal, Browse • Detection: 86%, Metadefender, Browse • Detection: 95%, ReversingLabs
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: netsh.exe PID: 2976 Parent PID: 5628

General

Start time:	14:55:40
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh firewall add allowedprogram "C:\Users\user\AppData\Roaming\System.exe" "System.exe" ENABLE
Imagebase:	0xe40000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Written

Registry Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 1876 Parent PID: 2976

General

Start time:	14:55:41
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: System.exe PID: 6172 Parent PID: 3352

General

Start time:	14:55:51
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\System.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\System.exe" ..
Imagebase:	0xf50000
File size:	37888 bytes
MD5 hash:	70ACA878BFAAC1EAF7019EDDD97FC877
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000009.00000000.356890184.0000000000F52000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000009.00000000.356890184.0000000000F52000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000009.00000002.370029896.0000000000F52000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000009.00000002.370029896.0000000000F52000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Analysis Process: System.exe PID: 6964 Parent PID: 3352

General

Start time:	14:55:59
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\System.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\System.exe" ..
Imagebase:	0x50000
File size:	37888 bytes
MD5 hash:	70ACA878BFAAC1EAF7019EDDD97FC877
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000B.00000002.388359726.0000000000052000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000B.00000002.388359726.0000000000052000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000B.00000000.376536403.0000000000052000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000B.00000000.376536403.0000000000052000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: System.exe PID: 5224 Parent PID: 3352

General

Start time:	14:56:07
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\System.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\System.exe" ..
Imagebase:	0x510000
File size:	37888 bytes
MD5 hash:	70ACA878BFAAC1EAF7019EDDD97FC877
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000C.00000000.392201898.0000000000512000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000C.00000000.392201898.0000000000512000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 0000000C.00000002.403902841.0000000000512000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 0000000C.00000002.403902841.0000000000512000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis