ID: 626606
Sample Name:
jc1NVSdAkP.exe
Cookbook: default.jbs
Time: 15:37:08
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

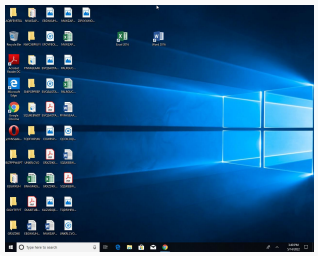
Windows Analysis Report

jc1NVSdAkP.exe

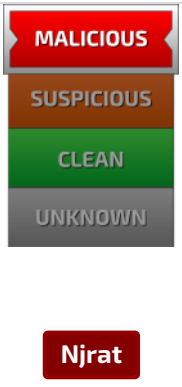
Overview

General Information

Sample Name:	jc1NVSdAkP.exe
Analysis ID:	626606
MD5:	4ae230eae2ec7b..
SHA1:	2439307f4a8b2d..
SHA256:	5f22cd86922fc0d..
Tags:	exe njrat RAT
Infos:	



Detection



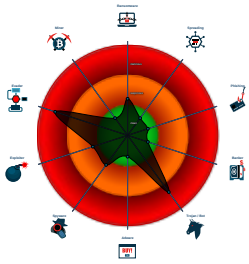
Njrat

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected Njrat
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Uses netsh to modify the Windows …

Classification



Process Tree

- **System is w10x64**
- jc1NVSdAkP.exe (PID: 6296 cmdline: "C:\Users\user\Desktop\jc1NVSdAkP.exe" MD5: 4AE230EAE2EC7BB0CFE6F9069616421E)
  - sytesnet.exe (PID: 6704 cmdline: "C:\Users\user\AppData\Roaming\sytesnet.exe" MD5: 4AE230EAE2EC7BB0CFE6F9069616421E)
    - netsh.exe (PID: 6340 cmdline: netsh firewall add allowedprogram "C:\Users\user\AppData\Roaming\sytesnet.exe" "sytesnet.exe" ENABLE MD5: 98CC37BBF363A38834253E22C80A8F32)
      - conhost.exe (PID: 5984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Njrat


```
{
  "Campaign ID": "Deep==2020",
  "Version": "0.7d",
  "Install Name": "sytesnet.exe",
  "Install Dir": "AppData",
  "Registry Value": "8336fcc4e4035f156be83ac267209dbd",
  "Host": "volkatv500.sytes.net",
  "Port": "999",
  "Network Seprator": "|'|'|",
  "Install Flag": "False"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x4d4e:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x4ea6:$s3: Executed As • 0x4e88:$s6: Download ERROR
00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NjRAT	Detects NjRAT / Bladabindi	ditekSHen	• 0x4ce0:$s1: netsh firewall delete allowedprogram • 0x4dbc:$s2: netsh firewall add allowedprogram • 0x4d4e:$s3: 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00 63 00 20 00 70 00 69 00 6E 00 67 • 0x4e64:$s4: Execute ERROR • 0x4ec0:$s4: Execute ERROR • 0x4e88:$s5: Download ERROR • 0x4fec:$s6: [kl]
00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x4dbc:$a1: netsh firewall add allowedprogram • 0x4d8c:$a2: SEE_MASK_NOZONECHECKS • 0x5036:$b1: [TAP] • 0x4d4e:$c3: cmd.exe /c ping
00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x4d8c:$reg: SEE_MASK_NOZONECHECKS • 0x4e64:$msg: Execute ERROR • 0x4ec0:$msg: Execute ERROR • 0x4d4e:$ping: cmd.exe /c ping 0 -n 2 & del
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.jc1NVSdAkP.exe.1be00000.5.raw.unpack	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x4d4e:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x4ea6:$s3: Executed As • 0x4e88:$s6: Download ERROR
0.2.jc1NVSdAkP.exe.1be00000.5.raw.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
0.2.jc1NVSdAkP.exe.1be00000.5.raw.unpack	MALWARE_Win_NjRAT	Detects NjRAT / Bladabindi	ditekSHen	• 0x4ce0:$s1: netsh firewall delete allowedprogram • 0x4dbc:$s2: netsh firewall add allowedprogram • 0x4d4e:$s3: 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00 63 00 20 00 70 00 69 00 6E 00 67 • 0x4e64:$s4: Execute ERROR • 0x4ec0:$s4: Execute ERROR • 0x4e88:$s5: Download ERROR • 0x4fec:$s6: [kl]
0.2.jc1NVSdAkP.exe.1be00000.5.raw.unpack	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x4dbc:$a1: netsh firewall add allowedprogram • 0x4d8c:$a2: SEE_MASK_NOZONECHECKS • 0x5036:$b1: [TAP] • 0x4d4e:$c3: cmd.exe /c ping
0.2.jc1NVSdAkP.exe.1be00000.5.raw.unpack	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x4d8c:$reg: SEE_MASK_NOZONECHECKS • 0x4e64:$msg: Execute ERROR • 0x4ec0:$msg: Execute ERROR • 0x4d4e:$ping: cmd.exe /c ping 0 -n 2 & del
Click to see the 14 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf) - Source IP: 192.168.2.3 - Destination IP: 41.103.180.209

Timestamp:	192.168.2.341.103.180.209497519992814856 05/14/22-15:39:01.814335
SID:	2814856
Source Port:	49751
Destination Port:	999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf) - Source IP: 192.168.2.3 - Destination IP: 41.103.180.209

Timestamp:	192.168.2.341.103.180.209497519992825563 05/14/22-15:39:01.814335

SID:	2825563
Source Port:	49751
Destination Port:	999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll) - Source IP: 192.168.2.3 - Destination IP: 41.103.180.209	−
Timestamp:	192.168.2.341.103.180.209497519992033132 05/14/22-15:39:01.539928
SID:	2033132
Source Port:	49751
Destination Port:	999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act) - Source IP: 192.168.2.3 - Destination IP: 41.103.180.209	−
Timestamp:	192.168.2.341.103.180.209497519992825564 05/14/22-15:39:06.382536
SID:	2825564
Source Port:	49751
Destination Port:	999
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN njRAT/Bladabindi CnC Callback (act) - Source IP: 192.168.2.3 - Destination IP: 41.103.180.209	−
Timestamp:	192.168.2.341.103.180.209497519992814860 05/14/22-15:39:06.382536
SID:	2814860
Source Port:	49751
Destination Port:	999
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration
Multi AV Scanner detection for submitted file
Yara detected Njrat
Antivirus / Scanner detection for submitted sample
Antivirus detection for URL or domain
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

Compliance

Detected unpacking (overwrites its own PE header)

Networking

Snort IDS alert for network traffic
C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Njrat

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

.NET source code contains potential unpacker

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

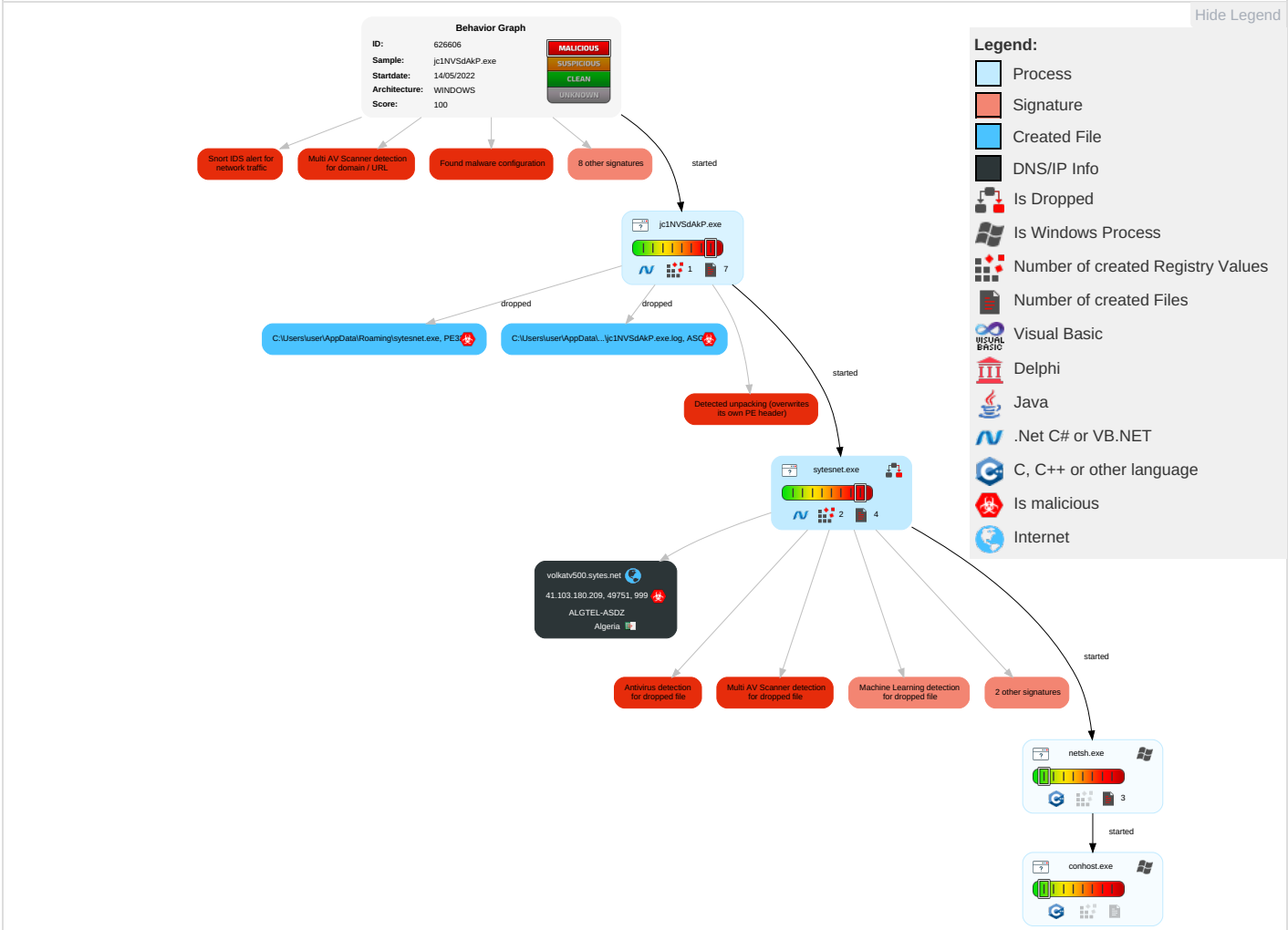
Remote Access Functionality

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 2 Process Injection	1 1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	2 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 2 Software Packing	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

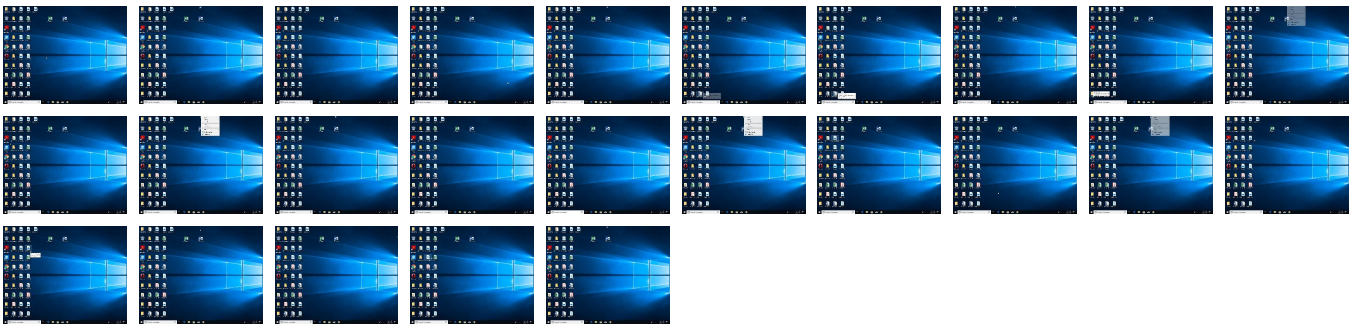
Behavior Graph



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
jc1NVSdAkP.exe	64%	Virustotal		Browse
jc1NVSdAkP.exe	26%	Metadefender		Browse
jc1NVSdAkP.exe	61%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
jc1NVSdAkP.exe	100%	Avira	TR/Dropper.Gen	
jc1NVSdAkP.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\sytesnet.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\sytesnet.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sytesnet.exe	64%	Virustotal		Browse
C:\Users\user\AppData\Roaming\sytesnet.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Roaming\sytesnet.exe	61%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.jc1NVSdAkP.exe.c80000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.sytesnet.exe.e0000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.sytesnet.exe.e0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.sytesnet.exe.e0000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
volkatv500.sytes.net	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
volkatv500.sytes.net	11%	Virustotal		Browse
volkatv500.sytes.net	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
volkatv500.sytes.net	41.103.180.209	true	true	• 11%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
volkatv500.sytes.net	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown

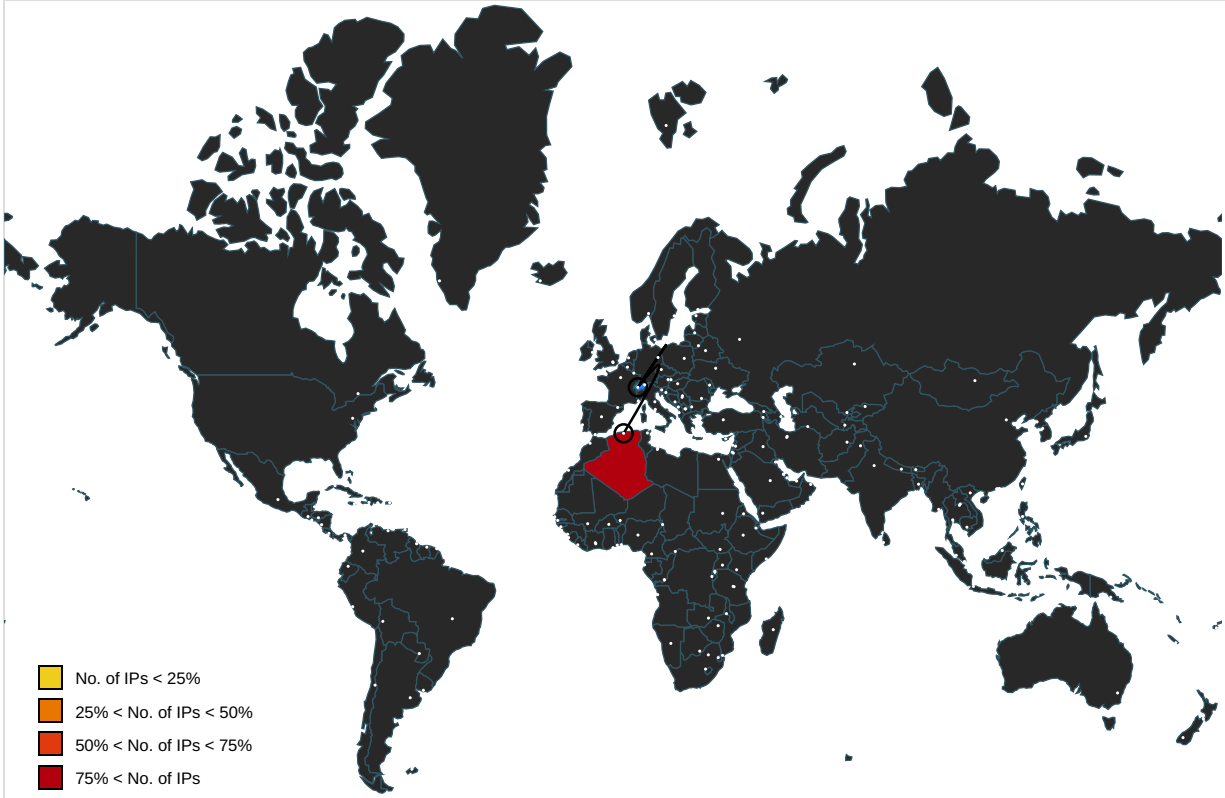
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000002.293306717.0000000001705000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	jc1NVSdAkP.exe, 00000000.00000003.256656239.000000001BF6F000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	jc1NVSdAkP.exe, 00000000.00000003.263865875.000000001BF71000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	jc1NVSdAkP.exe, 00000000.00000003.264295560.000000001BF70000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	jc1NVSdAkP.exe, 00000000.00000003.261828407.000000001BF6F000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000003.261768881.000000001BF70000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000003.261853022.000000001BF70000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	jc1NVSdAkP.exe, 00000000.00000003.262067529.000000001BF70000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000003.261981088.000000001BF71000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000003.261816363.000000001BF75000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000003.261768881.000000001BF70000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000003.261853022.000000001BF70000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000003.261933692.000000001BF6F000.00000004.00000020.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000002.298492596.000000001DDA2000.00000004.00000800.00020000.00000000.sdmp, jc1NVSdAkP.exe, 00000000.00000003.262105808.000000001BF76000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.103.180.209	volkatv500.sytes.net	Algeria		36947	ALGTEL-ASDZ	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626606
Start date and time: 14/05/202215:37:08	2022-05-14 15:37:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jc1NVSdAkP.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:	26
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.troj.evad.winEXE@6/4@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 0.8%) • Quality average: 32.8% • Quality standard deviation: 33%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target jc1NVSdAkP.exe, PID 6296 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\jc1NVSdAkP.exe.log

Process:	C:\Users\user\Desktop\jc1NVSdAkP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.280979230295524
Encrypted:	false
SSDEEP:	12:Q3LaJcP0/9UkB9t0kaHYGLi1B01kKVdisk70OAEaANv:ML2pBLaYgioQxAfA9
MD5:	4F9B2B715AECAC008745D08674616098
SHA1:	C57514C4DD41B45672DA1B05D487E72D46F000AC
SHA-256:	E3A1D0AC3EC711220FADB6166C7C40078134ED136865BCB35DF2034091CB66A9
SHA-512:	4F26878A7FF989DF363B1E55614D856408C44B7F970AA725F1B7C1431D52A7793BFAA22F53897CCF7469E52615550B06FCDBC1A6D51CC5390B2C87FD8559037E
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System\1201f26cb986c93f55044bb4fa22b294\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.VisualBas#\76002c3c0a2b9f0c8687ad35e8d9d309\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\b12bbcf27f41d96fe44360ae0b566f9b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\454c09ea87bde1d5f545d60232083b79\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Runtime.Remo#\bc6a0a01a7bd9d05ca132f229184fce6\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Roaming\sytesnet.exe

Process:	C:\Users\user\Desktop\jc1NVSdAkP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	226304
Entropy (8bit):	6.497123229913743
Encrypted:	false
SSDEEP:	3072:cLuhd/JZMeAgxbSGsbnzjQuJZQ4r0CuCilOD2Ri/xL1MrXk6kXBOSDWHubKta:TJZMerxWbnzjQRMx4HkZW10tDyt
MD5:	4AE230EAE2EC7BB0CFE6F9069616421E
SHA1:	2439307F4A8B2D0938AB5BF480A0B12DA403933B
SHA-256:	5F22CD86922FC0DFFF33F6D9906291E50D12259B86E5A8BC804B6945CA7E994E
SHA-512:	1C06F2E1BB06B68BD4D269D5016A08E83081B260497E026CA2EBAADFC489318C54F1D079BC0D40D751F9FBA0EA89FE90635F9DBC1ED34448C66401A438C3828
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 64%, Browse • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 61%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...h\|p_.....`...p.....~.. .....@.. .....@.....~..W..... .....H.....text....^... ...`..... ..`.reloc.....b.....@..B.rsrc.....d.....@..@.....~.....H.....p...$.....".(.....*....0.....s.....*.0..2.....(.....(.....o.....o.....o .....o!.....*...0..).....~..... ("....~....o#...%&~....o$...%&.....9.....E.....-.....&...~....o#...%&.....+a~.....o%...%&..o&...%&....,?.E.....,#.E.....~.....~.....o%...%&o'.....1..E.....~.....~.. ..o#...%&..o(....~....~....o#...%&o).....~.....(*...%&s+...o,.....(-.....

C:\Windows\assembly\Desktop.ini

Process:	C:\Users\user\Desktop\jc1NVSdAkP.exe
File Type:	Windows desktop.ini, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	227
Entropy (8bit):	5.2735028737400205
Encrypted:	false
SSDEEP:	6:a1eZBXVNYTF0NwoScUbtSgyAXIWv7v5PMKq:UeZBFNYTswUq1r5zq
MD5:	F7F759A5CD40BC52172E83486B6DE404
SHA1:	D74930F354A56CFD03DC91AA96D8AE9657B1EE54
SHA-256:	A709C2551B8818D7849D31A65446DC2F8C4CCA2DCBBC5385604286F49CFDAF1C
SHA-512:	A50B7826BFE72506019E4B1148A214C71C6F4743C09E809EF15CD0E0223F3078B683D203200910B07B5E1E34B94F0FE516AC53527311E2943654BFCEADE53298
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	; ==++==..; ..; Copyright (c) Microsoft Corporation. All rights reserved...; ..; ==--==..[.ShellClassInfo]..CLSID={1D2680C9-0E2A-469d-B787-065558BC7D43}..ConfirmFileOp=1..InfoTip=Contains application stability information...

\Device\ConDrv

Process:	C:\Windows\System32\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
Reputation:	high, very likely benign file
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):	6.497123229913743
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:	jc1NVSdAkP.exe
File size:	226304
MD5:	4ae230eae2ec7bb0cfe6f9069616421e
SHA1:	2439307f4a8b2d0938ab5bf480a0b12da403933b
SHA256:	5f22cd86922fc0dfff33f6d9906291e50d12259b86e5a8bc804b6945ca7e994e
SHA512:	1c06f2e1bb06b68bd4d269d5016a08e83081b260497e026ca2ebaadfc489318c54f1d079bc0d40d751f9fba0ea89fe90635f9dbc1ed34448c66401a438c382f8
SSDEEP:	3072:cLuhd/JZMeAgxbSGsbnzjQuJZQ4r0CuCilOD2Ri/xL1MrXk6kXBOSDWHubKta:TJZMerxWbnzjQRMx4HkZW10tDyt
TLSH:	2C244AAA33D86B02D45877B9458BA75053FEFA20FB02D6007E55797A3C937BB68121C3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...h|p_.....`...p.....~... .....@.. .....@.....

File Icon

Icon Hash:	e8ccc6c6cecce831

Static PE Info

General	
Entrypoint:	0x427eee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F707C68 [Sun Sep 27 11:50:00 2020 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x27e94	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2a000	0x10eec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x28000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1adb8	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x25ef4	0x26000	False	0.632606907895	data	7.0671537001	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x28000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x2a000	0x10eec	0x11000	False	0.324922449449	data	4.52018300234	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2a130	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 16777216, next used block 16777216		
RT_GROUP_ICON	0x3a958	0x14	data		
RT_VERSION	0x3a96c	0x394	data		
RT_MANIFEST	0x3ad00	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

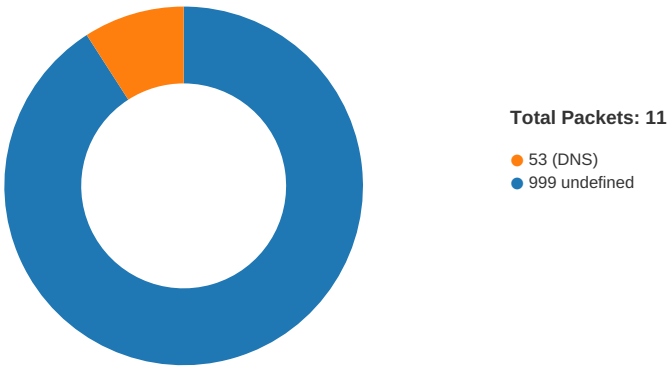
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	'
Assembly Version	0.0.0.0
InternalName	WindowsApplication14.exe
FileVersion	0.0.0.0
CompanyName	'
Comments	'
ProductName	'
ProductVersion	0.0.0.0
FileDescription	'
OriginalFilename	WindowsApplication14.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.341.103.180.209497519992814856 05/14/22-15:39:01.814335	TCP	2814856	ETPRO TROJAN njrat ver 0.7d Malware CnC Callback (inf)	49751	999	192.168.2.3	41.103.180.209
192.168.2.341.103.180.209497519992825563 05/14/22-15:39:01.814335	TCP	2825563	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (inf)	49751	999	192.168.2.3	41.103.180.209
192.168.2.341.103.180.209497519992033132 05/14/22-15:39:01.539928	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49751	999	192.168.2.3	41.103.180.209
192.168.2.341.103.180.209497519992825564 05/14/22-15:39:06.382536	TCP	2825564	ETPRO TROJAN Generic njRAT/Bladabindi CnC Activity (act)	49751	999	192.168.2.3	41.103.180.209
192.168.2.341.103.180.209497519992814860 05/14/22-15:39:06.382536	TCP	2814860	ETPRO TROJAN njRAT/Bladabindi CnC Callback (act)	49751	999	192.168.2.3	41.103.180.209

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:38:59.926131010 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:39:00.000283003 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:39:00.000499010 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:39:01.539927959 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:39:01.814233065 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:39:01.814335108 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:39:02.089317083 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:39:06.104610920 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:39:06.109133005 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:39:06.382436991 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:39:06.382535934 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:39:06.654485941 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:39:24.170299053 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:39:24.171821117 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:39:24.446300030 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:39:42.234999895 CEST	999	49751	41.103.180.209	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:39:42.240200043 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:39:42.513825893 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:40:00.298675060 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:40:00.301579952 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:40:00.570667028 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:40:18.365504980 CEST	999	49751	41.103.180.209	192.168.2.3
May 14, 2022 15:40:18.366318941 CEST	49751	999	192.168.2.3	41.103.180.209
May 14, 2022 15:40:18.640578985 CEST	999	49751	41.103.180.209	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:38:59.801275015 CEST	57421	53	192.168.2.3	8.8.8.8
May 14, 2022 15:38:59.819323063 CEST	53	57421	8.8.8.8	192.168.2.3

DNS Queries

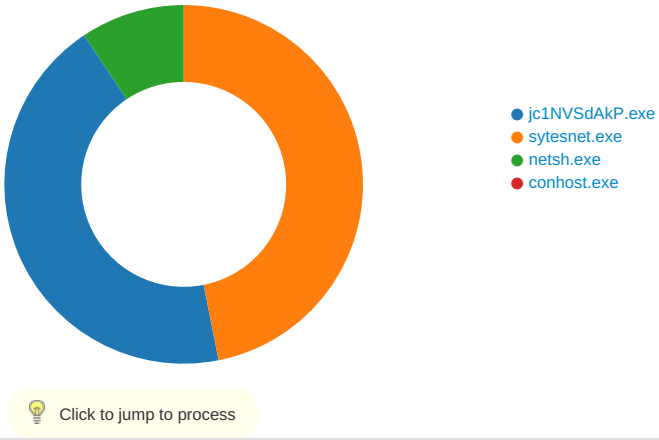
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 14, 2022 15:38:59.801275015 CEST	192.168.2.3	8.8.8.8	0x3f25	Standard query (0)	volkatv500 .sytes.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 14, 2022 15:38:59.819323063 CEST	8.8.8.8	192.168.2.3	0x3f25	No error (0)	volkatv500 .sytes.net		41.103.180.209	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: jc1NVSdAkP.exe PID: **6296**, Parent PID: **3040**

General

Target ID:	0
Start time:	15:38:08
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\jc1NVSdAkP.exe

Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\jc1NVSdAkP.exe"
Imagebase:	0xc80000
File size:	226304 bytes
MD5 hash:	4AE230EAE2EC7BB0CFE6F9069616421E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: 00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: 00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000000.00000002.297921919.000000001BE00000.00000004.08000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.293369368.00000000031E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000002.293369368.00000000031E1000.00000004.00000800.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000000.00000002.293369368.00000000031E1000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC607F8527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC607F8527	unknown
C:\Windows\assembly	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC60B59517	unknown
C:\Windows\assembly\Desktop.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC60B59517	unknown
C:\Users\user\AppData\Roaming\sytesnet.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC609B8147	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\jc1NVSdAkP.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC60B46184	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\assembly\Desktop.ini	0	227	3b 20 3d 3d 2b 2b 3d 3d 0d 0a 3b 20 0d 0a 3b 20 20 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 3b 20 0d 0a 3b 20 3d 3d 2d 2d 3d 3d 0d 0a 5b 2e 53 68 65 6c 6c 43 6c 61 73 73 49 6e 66 6f 5d 0d 0a 43 4c 53 49 44 3d 7b 31 44 32 36 38 30 43 39 2d 30 45 32 41 2d 34 36 39 64 2d 42 37 38 37 2d 30 36 35 35 35 38 42 43 37 44 34 33 7d 0d 0a 43 6f 6e 66 69 72 6d 46 69 6c 65 4f 70 3d 31 0d 0a 49 6e 66 6f 54 69 70 3d 43 6f 6e 74 61 69 6e 73 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 73 74 61 62 69 6c 69 74 79 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 0d 0a	; ==++==; ; Copyright (c) Microsoft Corporation. All rights reserved.; ; ==--==[.ShellC lassInfo]CLSID= {1D2680C9-0E2A-469d-B787-065558BC7D43}Confirm FileOp=1InfoTip=Contain s application stability information.	success or wait	1	7FFC60B59517	unknown
C:\Users\user\AppData\Roaming\sytesnet.exe	0	226304	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 68 7c 70 5f 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 0b 00 00 60 02 00 00 70 03 00 00 00 00 00 fd 7e 02 00 00 20 00 00 00 fd 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELh|p_`p~ @ @	success or wait	1	7FFC609B8147	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\jc1NVSdAkP.exe.log	0	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 36 34 5c 53 79 73 74 65 6d 5c 31 32 30 31 66 32 36 63 62 39 38 36 63 39 33 66 35 35 30 34 34 62 62 34 66 61 32 32 62 32 39 34 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 36 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e 6e	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System\1201f26cb986c93f55044bb4fa22b294\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.VisualBas#\76002c3c0a2b9f0c8687ad35e8d9d309\Microsoft.VisualBasic.n	success or wait	1	7FFC60B461CE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFC60825C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FFC60825C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFC60945AF3	ReadFile
C:\Users\user\Desktop\jc1NVSdAkP.exe	unknown	226304	success or wait	1	7FFC609B8147	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER	di	unicode	!	success or wait	1	7FFC609B8147	RegSetValueExW

Analysis Process: sytesnet.exe PID: **6704**, Parent PID: **6296**

General

Target ID:	5
Start time:	15:38:30
Start date:	14/05/2022
Path:	C:\Users\user\AppData\Roaming\sytesnet.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\sytesnet.exe"
Imagebase:	0xe0000
File size:	226304 bytes
MD5 hash:	4AE230EAE2EC7BB0CFE6F9069616421E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 64%, Virustotal, Browse • Detection: 26%, Metadefender, Browse • Detection: 61%, ReversingLabs

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC607F8527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC607F8527	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC607F8527	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFC607F8527	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFC60825C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FFC60825C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFC60945AF3	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FFC60825C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	7FFC60825C7C	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FFC609B8147	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MediaResources	success or wait	1	7FFC609B8147	unknown
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\MediaResources\msvideo	success or wait	1	7FFC609B8147	unknown
HKEY_CURRENT_USER\Software\8336fcc4e4035f156be83ac267209dbd	success or wait	1	7FFC609B8147	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Environment	SEE_MASK_NOZONECHECKS	unicode	1	success or wait	1	7FFC609B8147	RegSetValueExW
HKEY_CURRENT_USER\Software\8336fcc4e4035f156be83ac267209dbd	[kl]	unicode		success or wait	1	7FFC609B8147	RegSetValueExW

Analysis Process: netsh.exe PID: **6340**, Parent PID: **6704**

General

Target ID:	15
Start time:	15:38:49
Start date:	14/05/2022

Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh firewall add allowedprogram "C:\Users\user\AppData\Roaming\sytesnet.exe" "sytesnet.exe" ENABLE
Imagebase:	0x7ff7c7490000
File size:	92672 bytes
MD5 hash:	98CC37BBF363A38834253E22C80A8F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	306	306	4f 6b 2e 0d 0a 0d 0a	Ok.	success or wait	1	7FF7C7497C21	WriteFile
\Device\ConDrv	311	5	0d 0a		success or wait	1	7FF7C7497C21	WriteFile
\Device\ConDrv	313	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF7C7497C21	WriteFile

Analysis Process: conhost.exe PID: **5984**, Parent PID: **6340**

General

Target ID:	16
Start time:	15:38:50
Start date:	14/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly