ID: 879026
Sample Name:
BulkSMSData.scr.exe
Cookbook: default.jbs
Time: 13:04:19
Date: 31/05/2023
Version: 37.1.0 Beryl

Table of Contents

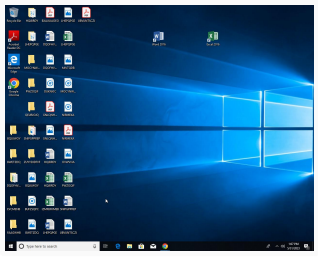
Windows Analysis Report

BulkSMSData.scr.exe

Overview

General Information

Sample Name:	BulkSMSData.scr.exe
Analysis ID:	879026
MD5:	8086b3bcc69a…
SHA1:	8aa75f5791db9..
SHA256:	6c774ebc6771…
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

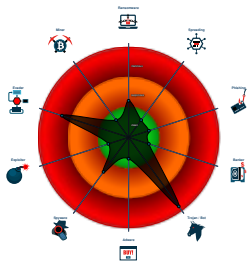
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected Nanocore RAT
- Writes to foreign memory regions
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- BulkSMSData.scr.exe (PID: 5720 cmdline: C:\Users\user\Desktop\BulkSMSData.scr.exe MD5: 8086B3BCC69AB5C969B67A4BA8104F61)
  - vbc.exe (PID: 6908 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
  - cmd.exe (PID: 6888 cmdline: cmd.exe" /C mkdir "C:\Users\user\AppData\Roaming\winpr0 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6992 cmdline: "cmd.exe" /C schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\winpr0\winpr0.exe'" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6960 cmdline: schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\winpr0\winpr0.exe'" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 7092 cmdline: cmd.exe" /C copy "C:\Users\user\Desktop\BulkSMSData.scr.exe" "C:\Users\user\AppData\Roaming\winpr0\winpr0.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5920 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: B3A917344F5610BEEC562556F11300FA)
  - conhost.exe (PID: 7040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	http://https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.morphisec.com/syk-crypter-discord	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "2774b180-050c-444b-91a0-70a89c8c",
  "Group": "DuckDNS",
  "Domain1": "iphy1.duckdns.org",
  "Domain2": "127.0.0.1",
  "Port": 54984,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.746119123.0000000000742000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.746119123.0000000000742000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.746119123.0000000000742000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000001.00000002.746119123.0000000000742000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xff8d:$a1: NanoCore.ClientPluginHost • 0xff4d:$a2: NanoCore.ClientPlugin • 0x11ea6:$b1: get_BuilderSettings • 0xfda9:$b2: ClientLoaderForm.resources • 0x115c6:$b3: PluginCommand • 0xff7e:$b4: IClientAppHost • 0x1a3fe:$b5: GetBlockHash • 0x124fe:$b6: AddHostEntry • 0x161f1:$b7: LogClientException • 0x1246b:$b8: PipeExists • 0xffb7:$b9: IClientLoggingHost
00000001.00000002.753307659.0000000009340000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.vbc.exe.95c4629.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
1.2.vbc.exe.95c4629.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
1.2.vbc.exe.95c4629.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.vbc.exe.95c4629.6.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xb14f:$x2: NanoCore.ClientPlugin • 0xb184:$x3: NanoCore.ClientPluginHost • 0xb143:$i2: IClientData • 0xb165:$i3: IClientNetwork • 0xb174:$i5: IClientDataHost • 0xb19e:$i6: IClientLoggingHost • 0xb1b1:$i7: IClientNetworkHost • 0xb1c4:$i8: IClientUIHost • 0xb1d2:$i9: IClientNameObjectCollection • 0xb1ee:$i10: IClientReadOnlyNameObjectCollection • 0xaf41:$s1: ClientPlugin • 0xb158:$s1: ClientPlugin • 0x10179:$s6: get_ClientSettings
1.2.vbc.exe.95c4629.6.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xb184:$a1: NanoCore.ClientPluginHost • 0xb14f:$a2: NanoCore.ClientPlugin • 0x100ca:$b1: get_BuilderSettings • 0x10039:$b7: LogClientException • 0xb19e:$b9: IClientLoggingHost
Click to see the 62 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Moves itself to temp directory

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

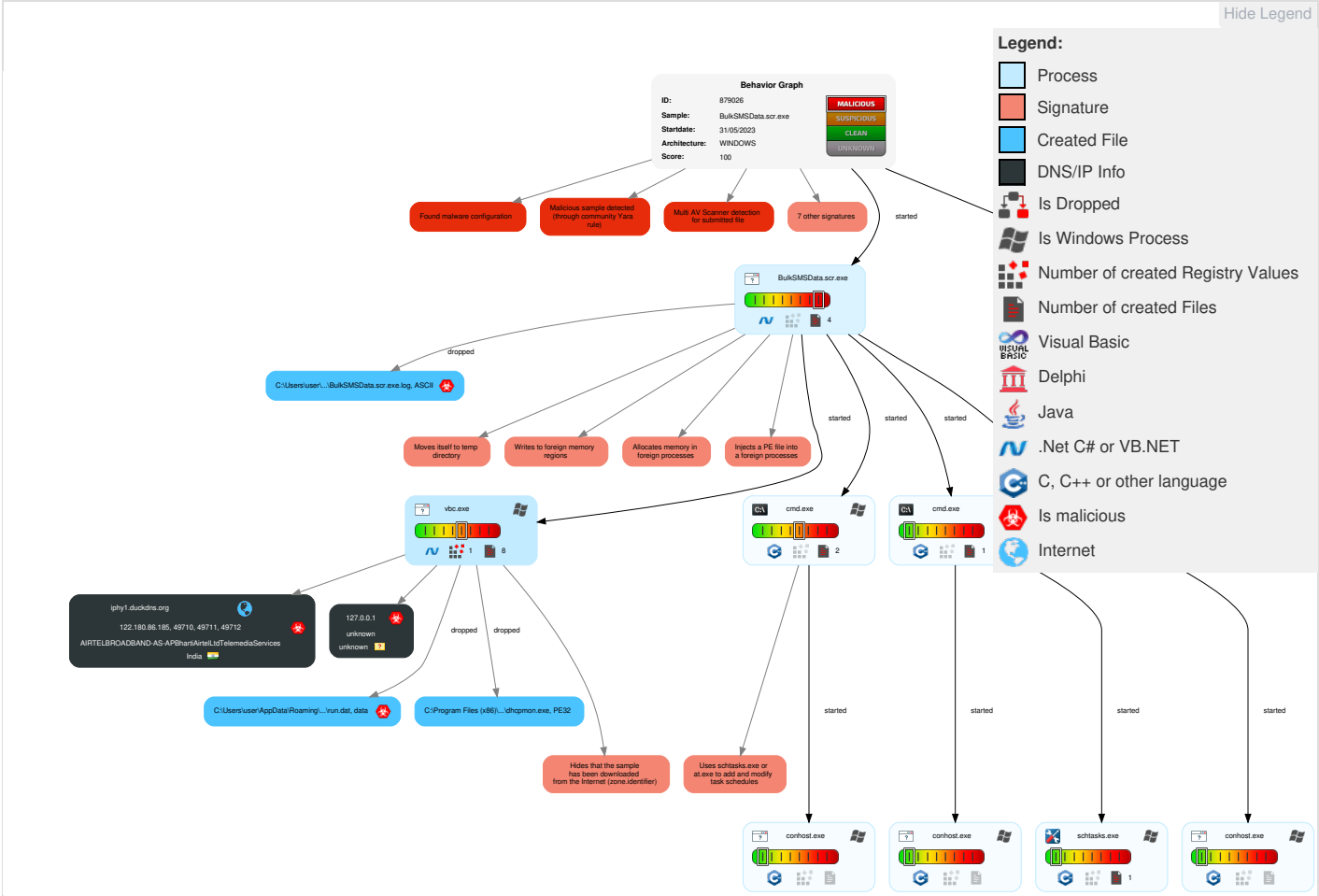
Yara detected Nanocore RAT

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
1 Valid Accounts	1 Scheduled Task/Job	1 Valid Accounts	1 Valid Accounts	1 2 Masquerading	2 1 Input Capture	1 Security Software Discovery	Remote Services	2 1 Input Capture	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	1 Scheduled Task/Job	1 Access Token Manipulation	1 Valid Accounts	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	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)	3 1 2 Process Injection	1 Access Token Manipulation	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Scheduled Task/Job	1 Disable or Modify Tools	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 1 Virtualization/Sandbox Evasion	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 1 2 Process Injection	Cached Domain Credentials	System Owner/User 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	1 Deobfuscate/Decode Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Obfuscated Files or Information	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 2 Software Packing	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

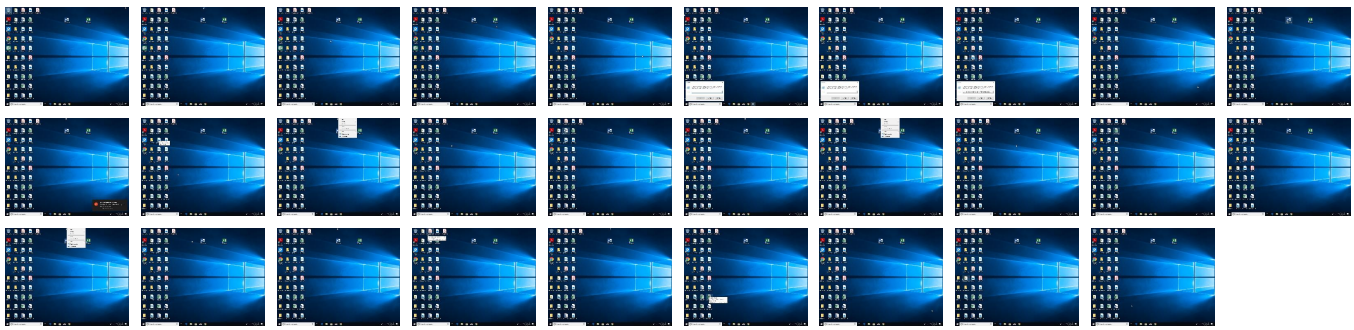
Behavior Graph



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
BulkSMSData.scr.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.Zilla	
BulkSMSData.scr.exe	56%	Virustotal		Browse
BulkSMSData.scr.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
127.0.0.1	0%	Avira URL Cloud	safe	
http://https://subf.domfagdfa6ffaffiffn.comd/objecsts.json?api_key=123R	0%	Avira URL Cloud	safe	
iphy1.duckdns.org	0%	Avira URL Cloud	safe	
http://go.microsoft	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iphy1.duckdns.org	122.180.86.185	true	true		unknown

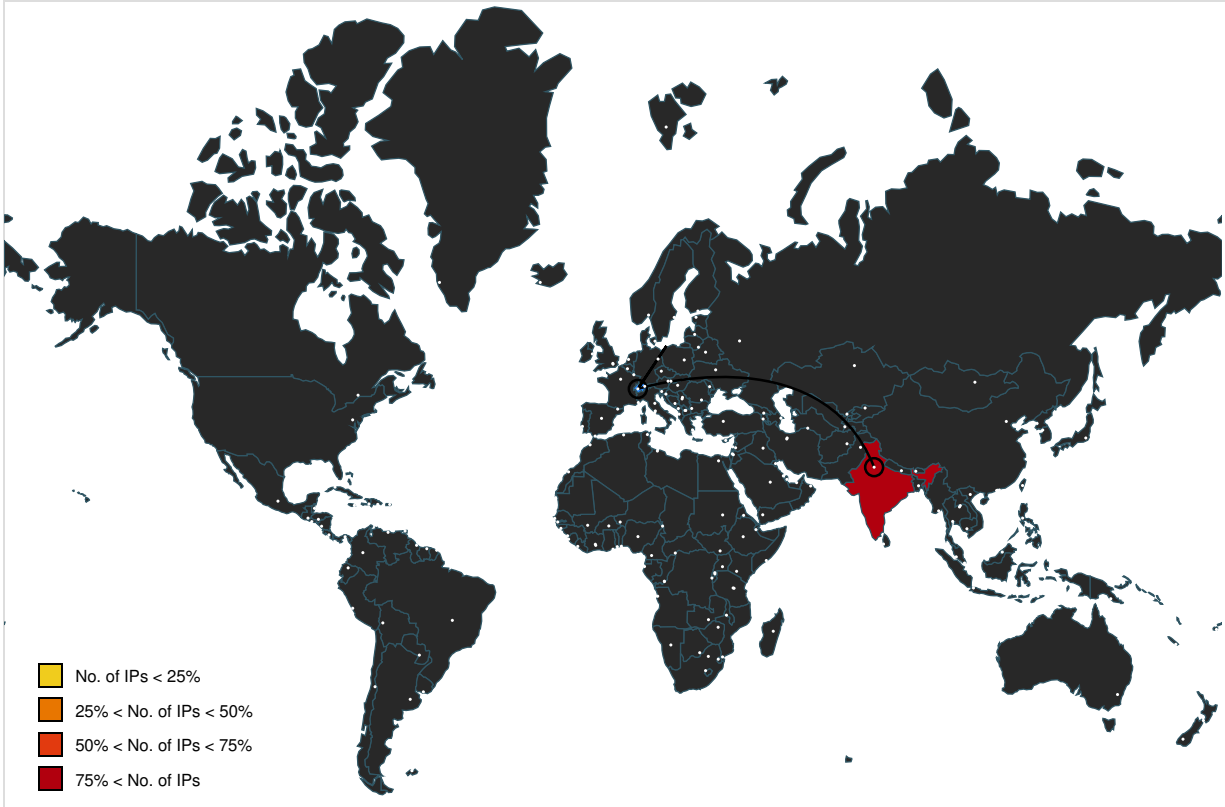
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
iphy1.duckdns.org	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://go.microsoft	dhcpmon.exe, 00000009.00000002.521116760.00000000054FA000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000001.00000002.747695002.0000000006C81000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://subf.domfagdfa6ffaffiffn.comd/objecsts.json?api_key=123R	BulkSMSData.scr.exe	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
122.180.86.185	iphy1.duckdns.org	India		24560	AIRTELBROADBAND-AS-APBhartiAirtelLtdTelemediaServices	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	879026
Start date and time:	2023-05-31 13:04:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
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
Sample file name:	BulkSMSData.scr.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@16/4@12/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): WMIADAP.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:05:28	Task Scheduler	Run new task: Nafifas path: "C:\Users\user\AppData\Roaming\winpr0\winpr0.exe"
13:05:28	API Interceptor	934x Sleep call for process: vbc.exe modified
13:05:29	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2688096
Entropy (8bit):	6.409257767499659
Encrypted:	false
SSDEEP:	49152:PAa87OQFMC/tWcHUgeRjRKW+0UpzIrFjB5u901ACUTum:PAa87zLtWI6jX+0UFIrZ//1a
MD5:	B3A917344F5610BEEC562556F11300FA
SHA1:	F7B1AC747E7705A21ACDD582B63800016BE21774
SHA-256:	7BA4838E3356B69254730E891ADD84092E3143016A515FF3E990CE19874A2459
SHA-512:	2D1515D75C3E5870F2FB57B321E02CF9611D30F3716A5670F0C32781AEB96576508B3B1C9717B2AC041B7752865842DD8AF7AF712988FF90FE3E6847821FFE60
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....d..O..O..O.....O.....O..v...O..v...O.....O.....O.....O..=:..O..=:..O..=:..O..=:..O..v...O..O...N.....O.....O.....O.....O..Rich.O.....PE..L....`.Z....."....."..8..... "...@..... )....!)...@..... .....d.".V.....#.....#.L.....(.`>....'.46....".T.....`...@.....#.....text...d."....."..... ..`.data...,....."....."..... @....idata.....#.....#.....@..@.tls.....#.....#.....@....rsrc...L.....#.....#.....@..@.reloc..46....'..8....'.....@..B.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BulkSMSData.scr.exe.log

Process:	C:\Users\user\Desktop\BulkSMSData.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	520
Entropy (8bit):	5.345981753770044
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:MLUE4K5E4Ks2wKDE4KhK3VZ9pKhk
MD5:	044A637E42FE9A819D7E43C8504CA769
SHA1:	6FCA27B1A571B73563C8424C84F4F64F3CBCBE2F
SHA-256:	E88E04654826CE00CC7A840745254164DDBD175066D6E4EA6858BF0FE463EBB4
SHA-512:	C9A74FA4154FA5E5951B0EEAC5330CA4BAC981FF9AD24C08575A76AD5D99CFB68556B9857C9C8209A1BFCB43F82E00F14962987A18A92A715F45AD0D4E4A71 C
Malicious:	**true**

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:PP3yn:X3yn
MD5:	C91D16A633B7F25569DA3A33CCAD5EF9
SHA1:	A91A73FAEDE3EC9C24413F5D7B49F18A0B37DC5C
SHA-256:	D76F97B54C8E6C520E8803FC7BB35409AF83D83D5FF3744B2DC872E3C7EAE222
SHA-512:	982309CDA931DF0DE7FBB6E4870D9E675AD4C79F2B21D9E58575BB40C0CA99758DD506B215904EFA14270F33F7B5F5617627D4444AE02B984F170F7D96019FB
Malicious:	**true**
Preview:	.!.`.b.H

\Device\ConDrv

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with very long lines (304)
Category:	dropped
Size (bytes):	6809
Entropy (8bit):	4.315685828355093
Encrypted:	false
SSDEEP:	96:zKHDGKD7zrrRYZZ/HPw4//HP/HH6K1jqQiGyGTFchzCKtihKCsO2b0N/+7vKAKPO:YrRYZXCKgQifr8sC/635P
MD5:	DA37CE62FC9ABAB3226A1797FF449487
SHA1:	18F29B4F3B1D12BA18DF2EF8964DA20107EEFFC9
SHA-256:	80EAB2A83F12150619544DBFFDD130D60B6869EE742F9000F8E3109F406FAD6E
SHA-512:	5A8BF4140440BCB218CFE90A3371AE761212BC4364DC7E7C055980D3FAB4C4E4499B1CADB13666D4D5F03B6AE835AEE4B44F78D4B2A4AA4ABDF20D8161B12F66
Malicious:	false
Preview:	Microsoft (R) Visual Basic Compiler version 14.7.3056.for Visual Basic 2012.Copyright (c) Microsoft Corporation. All rights reserved...This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to Visual Basic 2012, which is no longer the latest version. For compilers that support newer versions of the Visual Basic programming language, see http://go.microsoft.com/fwlink/?LinkID=533241.. Visual Basic Compiler Options.. - OUTPUT FILE -./out:<file> Specifies the output file name../target:exe Create a console application (default). (Short form: /t)./target:winexe Create a Windows application../target:library Create a library assembly../target:module Create a module that can be added to an assembly../target:appcontainerexe Create a Windows application that runs in AppContainer../ta

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.634585002639547
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	BulkSMSData.scr.exe
File size:	422912
MD5:	8086b3bcc69ab5c969b67a4ba8104f61
SHA1:	8aa75f5791db90006a7c5db8118ab6bcd695df2c
SHA256:	6c774ebc677180296f994563e208f0b0c09f7e7f25435999c6377668a91ba6b6
SHA512:	62b9b747fe9ac835f3a9460be1196accc56e0f38d74f98124da871b1c97586cac77cfc0625000e0d16ff99154a5d065be35182214b0a3c0323660bcd5bf90894
SSDEEP:	6144:gKH1blm9ZuDIoOX520kV0aAAkTKpVatxtMV6ksT:RfmyDI55vPaAvrxtye
TLSH:	7F949B27B2BCC5E2F95C3CF9929443244AB0ACA28239E247D85FBDD0E9773A7D1055C6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Ewd..... ... .@.. .....@.....

File Icon

	
Icon Hash:	07d8d8d4d4d85026

Static PE Info

General

Entrypoint:	0x4403d4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x647745B0 [Wed May 31 13:03:44 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x4038a	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x42000	0x28aed	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x3e3da	0x3e400	False	0.9171608308232931	data	7.852555160628475	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x42000	0x28aed	0x28c00	False	0.047695791794478526	data	2.9740933674644365	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6c000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x420ac	0xc35	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x42d05	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584		
RT_ICON	0x53551	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016		
RT_ICON	0x5ca1d	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600		
RT_ICON	0x61ec9	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896		
RT_ICON	0x66115	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600		
RT_ICON	0x686e1	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0x697ad	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400		
RT_ICON	0x6a159	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0x6a60f	0x84	data		

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x6a6cf	0x1f8	data	English	United States
RT_MANIFEST	0x6a903	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 13:05:29.495012045 CEST	49710	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:29.697541952 CEST	54984	49710	122.180.86.185	192.168.2.6
May 31, 2023 13:05:30.198441029 CEST	49710	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:30.401186943 CEST	54984	49710	122.180.86.185	192.168.2.6
May 31, 2023 13:05:30.901772976 CEST	49710	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:31.103679895 CEST	54984	49710	122.180.86.185	192.168.2.6
May 31, 2023 13:05:35.417171001 CEST	49711	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:35.587439060 CEST	54984	49711	122.180.86.185	192.168.2.6
May 31, 2023 13:05:36.089608908 CEST	49711	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:36.260035992 CEST	54984	49711	122.180.86.185	192.168.2.6
May 31, 2023 13:05:36.855357885 CEST	49711	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:37.025765896 CEST	54984	49711	122.180.86.185	192.168.2.6
May 31, 2023 13:05:41.292907000 CEST	49712	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:41.475595951 CEST	54984	49712	122.180.86.185	192.168.2.6
May 31, 2023 13:05:41.980804920 CEST	49712	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:42.163629055 CEST	54984	49712	122.180.86.185	192.168.2.6
May 31, 2023 13:05:42.668308973 CEST	49712	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:05:42.852124929 CEST	54984	49712	122.180.86.185	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 13:06:02.124450922 CEST	49716	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:02.314635038 CEST	54984	49716	122.180.86.185	192.168.2.6
May 31, 2023 13:06:02.826570988 CEST	49716	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:03.016988039 CEST	54984	49716	122.180.86.185	192.168.2.6
May 31, 2023 13:06:03.529784918 CEST	49716	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:03.720632076 CEST	54984	49716	122.180.86.185	192.168.2.6
May 31, 2023 13:06:07.786798954 CEST	49717	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:07.989407063 CEST	54984	49717	122.180.86.185	192.168.2.6
May 31, 2023 13:06:08.498656988 CEST	49717	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:08.700860023 CEST	54984	49717	122.180.86.185	192.168.2.6
May 31, 2023 13:06:09.201756954 CEST	49717	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:09.403778076 CEST	54984	49717	122.180.86.185	192.168.2.6
May 31, 2023 13:06:13.819217920 CEST	49718	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:14.005460978 CEST	54984	49718	122.180.86.185	192.168.2.6
May 31, 2023 13:06:14.514760017 CEST	49718	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:14.698142052 CEST	54984	49718	122.180.86.185	192.168.2.6
May 31, 2023 13:06:15.217943907 CEST	49718	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:15.401125908 CEST	54984	49718	122.180.86.185	192.168.2.6
May 31, 2023 13:06:34.745697021 CEST	49722	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:34.935530901 CEST	54984	49722	122.180.86.185	192.168.2.6
May 31, 2023 13:06:35.438349962 CEST	49722	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:35.628101110 CEST	54984	49722	122.180.86.185	192.168.2.6
May 31, 2023 13:06:36.141799927 CEST	49722	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:36.331302881 CEST	54984	49722	122.180.86.185	192.168.2.6
May 31, 2023 13:06:40.399135113 CEST	49723	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:40.589797974 CEST	54984	49723	122.180.86.185	192.168.2.6
May 31, 2023 13:06:41.095207930 CEST	49723	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:41.285351992 CEST	54984	49723	122.180.86.185	192.168.2.6
May 31, 2023 13:06:41.798326969 CEST	49723	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:41.988706112 CEST	54984	49723	122.180.86.185	192.168.2.6
May 31, 2023 13:06:46.137659073 CEST	49724	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:46.321229935 CEST	54984	49724	122.180.86.185	192.168.2.6
May 31, 2023 13:06:46.829929113 CEST	49724	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:47.013951063 CEST	54984	49724	122.180.86.185	192.168.2.6
May 31, 2023 13:06:47.517625093 CEST	49724	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:06:47.701272964 CEST	54984	49724	122.180.86.185	192.168.2.6
May 31, 2023 13:07:08.264868975 CEST	49728	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:08.433547020 CEST	54984	49728	122.180.86.185	192.168.2.6
May 31, 2023 13:07:08.941194057 CEST	49728	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:09.109972954 CEST	54984	49728	122.180.86.185	192.168.2.6
May 31, 2023 13:07:09.613152027 CEST	49728	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:09.781765938 CEST	54984	49728	122.180.86.185	192.168.2.6
May 31, 2023 13:07:13.977325916 CEST	49729	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:14.166018009 CEST	54984	49729	122.180.86.185	192.168.2.6
May 31, 2023 13:07:14.676089048 CEST	49729	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:14.870055914 CEST	54984	49729	122.180.86.185	192.168.2.6
May 31, 2023 13:07:15.473117113 CEST	49729	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:15.661956072 CEST	54984	49729	122.180.86.185	192.168.2.6
May 31, 2023 13:07:19.725891113 CEST	49730	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:19.904256105 CEST	54984	49730	122.180.86.185	192.168.2.6
May 31, 2023 13:07:20.410985947 CEST	49730	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:20.590341091 CEST	54984	49730	122.180.86.185	192.168.2.6
May 31, 2023 13:07:21.098493099 CEST	49730	54984	192.168.2.6	122.180.86.185
May 31, 2023 13:07:21.280308962 CEST	54984	49730	122.180.86.185	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 13:05:29.363399982 CEST	59504	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 31, 2023 13:05:29.485690117 CEST	53	59504	8.8.8.8	192.168.2.6
May 31, 2023 13:05:35.301834106 CEST	65198	53	192.168.2.6	8.8.8.8
May 31, 2023 13:05:35.415797949 CEST	53	65198	8.8.8.8	192.168.2.6
May 31, 2023 13:05:41.172956944 CEST	62910	53	192.168.2.6	8.8.8.8
May 31, 2023 13:05:41.286559105 CEST	53	62910	8.8.8.8	192.168.2.6
May 31, 2023 13:06:02.094636917 CEST	63863	53	192.168.2.6	8.8.8.8
May 31, 2023 13:06:02.123040915 CEST	53	63863	8.8.8.8	192.168.2.6
May 31, 2023 13:06:07.765028954 CEST	63229	53	192.168.2.6	8.8.8.8
May 31, 2023 13:06:07.785238028 CEST	53	63229	8.8.8.8	192.168.2.6
May 31, 2023 13:06:13.792140007 CEST	62538	53	192.168.2.6	8.8.8.8
May 31, 2023 13:06:13.812063932 CEST	53	62538	8.8.8.8	192.168.2.6
May 31, 2023 13:06:34.703680992 CEST	54903	53	192.168.2.6	8.8.8.8
May 31, 2023 13:06:34.732391119 CEST	53	54903	8.8.8.8	192.168.2.6
May 31, 2023 13:06:40.369873047 CEST	51530	53	192.168.2.6	8.8.8.8
May 31, 2023 13:06:40.393373966 CEST	53	51530	8.8.8.8	192.168.2.6
May 31, 2023 13:06:46.021251917 CEST	56122	53	192.168.2.6	8.8.8.8
May 31, 2023 13:06:46.136280060 CEST	53	56122	8.8.8.8	192.168.2.6
May 31, 2023 13:07:08.231833935 CEST	52556	53	192.168.2.6	8.8.8.8
May 31, 2023 13:07:08.261351109 CEST	53	52556	8.8.8.8	192.168.2.6
May 31, 2023 13:07:13.923969030 CEST	61609	53	192.168.2.6	8.8.8.8
May 31, 2023 13:07:13.947426081 CEST	53	61609	8.8.8.8	192.168.2.6
May 31, 2023 13:07:19.695219040 CEST	52481	53	192.168.2.6	8.8.8.8
May 31, 2023 13:07:19.723649025 CEST	53	52481	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 31, 2023 13:05:29.363399982 CEST	192.168.2.6	8.8.8.8	0x3bb1	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:05:35.301834106 CEST	192.168.2.6	8.8.8.8	0x4ff0	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:05:41.172956944 CEST	192.168.2.6	8.8.8.8	0xfa52	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:02.094636917 CEST	192.168.2.6	8.8.8.8	0x5373	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:07.765028954 CEST	192.168.2.6	8.8.8.8	0x63ab	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:13.792140007 CEST	192.168.2.6	8.8.8.8	0x1221	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:34.703680992 CEST	192.168.2.6	8.8.8.8	0xe2e3	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:40.369873047 CEST	192.168.2.6	8.8.8.8	0xfc00	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:46.021251917 CEST	192.168.2.6	8.8.8.8	0x3006	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:07:08.231833935 CEST	192.168.2.6	8.8.8.8	0x1cfa	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:07:13.923969030 CEST	192.168.2.6	8.8.8.8	0x617c	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false
May 31, 2023 13:07:19.695219040 CEST	192.168.2.6	8.8.8.8	0x3f08	Standard query (0)	iphy1.duckdns.org	A (IP address)	IN (0x0001)	false

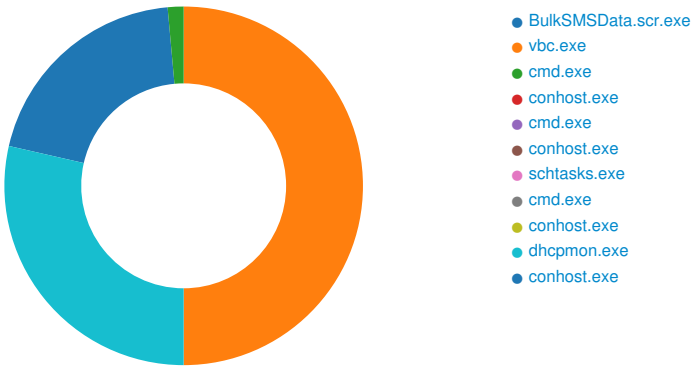
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 13:05:29.485690117 CEST	8.8.8.8	192.168.2.6	0x3bb1	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:05:35.415797949 CEST	8.8.8.8	192.168.2.6	0x4ff0	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:05:41.286559105 CEST	8.8.8.8	192.168.2.6	0xfa52	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 31, 2023 13:06:02.123040915 CEST	8.8.8.8	192.168.2.6	0x5373	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:07.785238028 CEST	8.8.8.8	192.168.2.6	0x63ab	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:13.812063932 CEST	8.8.8.8	192.168.2.6	0x1221	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:34.732391119 CEST	8.8.8.8	192.168.2.6	0xe2e3	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:40.393373966 CEST	8.8.8.8	192.168.2.6	0xfc00	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:06:46.136280060 CEST	8.8.8.8	192.168.2.6	0x3006	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:07:08.261351109 CEST	8.8.8.8	192.168.2.6	0x1cfa	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:07:13.947426081 CEST	8.8.8.8	192.168.2.6	0x617c	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false
May 31, 2023 13:07:19.723649025 CEST	8.8.8.8	192.168.2.6	0x3f08	No error (0)	iphy1.duckdns.org		122.180.86.185	A (IP address)	IN (0x0001)	false

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: BulkSMSData.scr.exe PID: 5720, Parent PID: 3452

General

Target ID:	0
Start time:	13:05:19
Start date:	31/05/2023
Path:	C:\Users\user\Desktop\BulkSMSData.scr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BulkSMSData.scr.exe
Imagebase:	0xb50000

File size:	422912 bytes
MD5 hash:	8086B3BCC69AB5C969B67A4BA8104F61
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.500524619.00000000042EA000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.500524619.00000000042EA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.500524619.00000000042EA000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.500524619.00000000042EA000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.500524619.00000000041B5000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.500524619.00000000041B5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.500524619.00000000041B5000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.500524619.00000000041B5000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: vbc.exe PID: **6908**, Parent PID: **5720**

General

Target ID:	1
Start time:	13:05:25
Start date:	31/05/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0xce0000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.746119123.0000000000742000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.746119123.0000000000742000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.746119123.0000000000742000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.746119123.0000000000742000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.753307659.0000000009340000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.753307659.0000000009340000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.753307659.0000000009340000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.753307659.0000000009340000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.752179756.0000000007C89000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.752179756.0000000007C89000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.752179756.0000000007C89000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.753460667.00000000095C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.753460667.00000000095C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.753460667.00000000095C0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.753460667.00000000095C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.753460667.00000000095C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.747695002.0000000006C81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.747695002.0000000006C81000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	high

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	72ECCF06	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	72ECCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71D1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71D11E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71D1BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71D1DD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71D1BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71D1BEFF	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 21 fd 60 12 62 fd 48	!`bH	success or wait	1	71D11B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	524288	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 28 01 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 fd 2e 64 fd fd 4f 0a fd 4f 0a fd 4f 0a fd 18 00 fd fd 4f 0a fd 18 00 fd fd 4f 0a fd 76 fd fd fd 4f 0a fd 76 fd fd fd 4f 0a fd 1d fd fd 4f 0a fd 1f fd fd fd 4f 0a fd 1d fd fd 4f 0a fd 3d 3a fd fd 4f 0a fd 3d 3a fd fd 4f 0a fd 3d 3a fd fd 4f 0a fd 3d 3a fd fd 4f 0a fd 76 fd fd fd 4f 0a fd 4f 0b fd fd 4e 0a fd 1f fd fd fd fd 4f 0a	MZ@(!L!This program cannot be run in DOS mode.$.dOOOOOvOvOOO O=:O=:O=:O=:OvOONO	success or wait	6	71D1DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	72EA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	72EA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72EA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72E003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	72EACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	72EACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72E003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72E003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72E003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72E003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72EA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71D11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71D11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4096	success or wait	1	71D11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4096	end of file	1	71D11B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72E8D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72E8D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe	unknown	4096	success or wait	1	72E8D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe	unknown	512	success or wait	1	72E8D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	4095	success or wait	1	72EA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe.config	unknown	8173	end of file	1	72EA5705	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	71D1646A	RegSetValueExW

Analysis Process: cmd.exe PID: **6888**, Parent PID: **5720**

General

Target ID:	2
Start time:	13:05:26
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe" /C mkdir "C:\Users\user\AppData\Roaming\winpr0
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\winpr0	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1BBFE7	CreateDirectoryW

Analysis Process: conhost.exe PID: **6964**, Parent PID: **6888**

General

Target ID:	3
Start time:	13:05:26
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: cmd.exe PID: **6992**, Parent PID: **5720**

General	
Target ID:	4
Start time:	13:05:26
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\winpr0\winpr0.exe'" /f
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6988**, Parent PID: **6992**

General	
Target ID:	5
Start time:	13:05:26
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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: schtasks.exe PID: **6960**, Parent PID: **6992**

General	
Target ID:	6
Start time:	13:05:27
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\winpr0\winpr0.exe'" /f
Imagebase:	0xac0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **7092**, Parent PID: **5720**

General

Target ID:	7
Start time:	13:05:27
Start date:	31/05/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe" /C copy "C:\Users\user\Desktop\BulkSMSData.scr.exe" "C:\Users\user\AppData\Roaming\winpr0\winpr0.exe
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7076**, Parent PID: **7092**

General

Target ID:	8
Start time:	13:05:27
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **5920**, Parent PID: **3452**

General

Target ID:	9
Start time:	13:05:38
Start date:	31/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xe70000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, ReversingLabs

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	76	76	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 0a 0a 54 68 69 73 20 63 6f 6d 70 69 6c 65 72 20 69 73	Copyright (c) Microsoft Corporation. All rights reserved.This compiler is	success or wait	1	EE4CE5	WriteFile
\Device\ConDrv	441	365	0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 56 69 73 75 61 6c 20 42 61 73 69 63 20 43 6f 6d 70 69 6c 65 72 20 4f 70 74 69 6f 6e 73 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2d 20 4f 55 54 50 55 54 20 46 49 4c 45 20 2d 0a 2f 6f 75 74 3a 3c 66 69 6c 65 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 70 65 63 69 66 69 65 73 20 74 68 65 20 6f 75 74 70 75 74 20 66 69 6c 65 20 6e 61 6d 65 2e 0a 2f 74 61 72 67 65 74 3a 65 78 65 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 61 20 63 6f 6e 73 6f 6c 65 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 20 28 53 68 6f 72 74 20 66 6f 72 6d 3a 20 2f 74	Visual Basic Compiler Options - OUTPUT FILE -/out:<file> Specifies the output file name./target:exe Create a console application (default). (Short form: /t	success or wait	1	EE4CE5	WriteFile
\Device\ConDrv	442	1	20		success or wait	1	EE4CE5	WriteFile
\Device\ConDrv	460	18	56 69 73 75 61 6c 20 42 61 73 69 63 20 43 6f 6d 70 69	Visual Basic Compi	success or wait	1	EE4CE5	WriteFile
\Device\ConDrv	489	29	0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20		success or wait	1	EE4CE5	WriteFile
\Device\ConDrv	490	1	0a		success or wait	1	EE4CE5	WriteFile
\Device\ConDrv	491	1	20		success or wait	1	EE4CE5	WriteFile
\Device\ConDrv	525	34	2d 20 4f 55 54 50 55 54 20 46 49 4c 45 20 2d 0a 2f 6f 75 74 3a 3c 66 69 6c 65 3e 20 20 20 20 20 20 20	- OUTPUT FILE -/out: <file>	success or wait	8	EE4CE5	WriteFile
\Device\ConDrv	540	15	0a 2f 6f 75 74 3a 3c 66 69 6c 65 3e 20 20 20	/out:<file>	success or wait	8	EE4CE5	WriteFile
\Device\ConDrv	541	1	2f	/	success or wait	8	EE4CE5	WriteFile
\Device\ConDrv	552	11	20 20 20 20 20 20 20 20 20 20 20		success or wait	46	EE4CE5	WriteFile
\Device\ConDrv	575	23	53 70 65 63 69 66 69 65 73 20 74 68 65 20 6f 75 74 70 75 74 20 66 69	Specifies the output fi	success or wait	46	EE4CE5	WriteFile
\Device\ConDrv	606	31	0a 2f 74 61 72 67 65 74 3a 65 78 65 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	/target:exe	success or wait	54	EE4CE5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	607	1	2f	/	success or wait	53	EE4CE5	WriteFile
\Device\ConDrv	618	11	20 20 20 20 20 20 20 20 20 20 20		success or wait	18	EE4CE5	WriteFile
\Device\ConDrv	641	23	43 72 65 61 74 65 20 61 20 63 6f 6e 73 6f 6c 65 20 61 70 70 6c 69 63	Create a console applic	success or wait	18	EE4CE5	WriteFile
\Device\ConDrv	697	56	0a 2f 74 61 72 67 65 74 3a 77 69 6e 65 78 65 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 61 20 57 69 6e 64 6f 77 73 20 61 70 70 6c	/target:winexe Create a Windows appl	success or wait	18	EE4CE5	WriteFile
\Device\ConDrv	698	1	2f	/	success or wait	18	EE4CE5	WriteFile
\Device\ConDrv	1222	1	20		success or wait	8	EE4CE5	WriteFile
\Device\ConDrv	1603	34	77 69 6c 64 63 61 72 64 20 73 70 65 63 69 66 69 63 61 74 69 6f 6e 73 2e 0a 2f 72 65 66 65 72 65 6e 63	wildcard specifications./referenc	success or wait	8	EE4CE5	WriteFile

Analysis Process: conhost.exe PID: **7040**, Parent PID: **5920**

General

Target ID:	10
Start time:	13:05:38
Start date:	31/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly