ID: 679101
Sample Name:
DCwTjs2dTP.exe
Cookbook: default.jbs
Time: 09:15:11
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report DCwTjs2dTP.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: AsyncRAT 4
Yara Signatures 5
PCAP (Network Traffic) 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Key, Mouse, Clipboard, Microphone and Screen Capturing 6
System Summary 6
Boot Survival 6
Malware Analysis System Evasion 7
Lowering of HIPS / PFW / Operating System Security Settings 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 11
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506 12
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506 12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DCwTjs2dTP.exe.log 13
C:\Users\user\AppData\Local\Temp\tmp53F0.tmp.bat 13
C:\Users\user\AppData\Roaming\sihost.exe 13
\Device\Null 14
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 15
Data Directories 16
Sections 17
Resources 17
Imports 17
Network Behavior 17
Snort IDS Alerts 17
Network Port Distribution 17
TCP Packets 18
UDP Packets 20

DNS Queries 20
DNS Answers 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: DCwTjs2dTP.exePID: 5664, Parent PID: 5308 20
General 20
File Activities 21
Analysis Process: cmd.exePID: 2612, Parent PID: 5664 21
General 21
File Activities 21
Analysis Process: conhost.exePID: 5256, Parent PID: 2612 21
General 21
Analysis Process: cmd.exePID: 6128, Parent PID: 5664 21
General 21
File Activities 22
File Read 22
Analysis Process: schtasks.exePID: 5128, Parent PID: 2612 22
General 22
File Activities 22
Analysis Process: conhost.exePID: 3404, Parent PID: 6128 22
General 22
Analysis Process: timeout.exePID: 5344, Parent PID: 6128 23
General 23
File Activities 23
File Written 23
Analysis Process: sihost.exePID: 5352, Parent PID: 6128 23
General 23
File Activities 24
File Created 24
File Read 24
Registry Activities 25
Key Created 25
Key Value Created 25
Disassembly 29

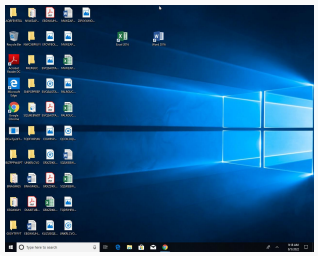
Windows Analysis Report

DCwTjs2dTP.exe

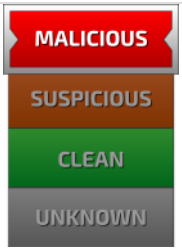
Overview

General Information

Sample Name:	DCwTjs2dTP.exe
Analysis ID:	679101
MD5:	2ed2a1d6604afe..
SHA1:	6134d837220afe..
SHA256:	2a48fa5118bf1c9..
Tags:	DCRat exe RAT
Infos:	



Detection



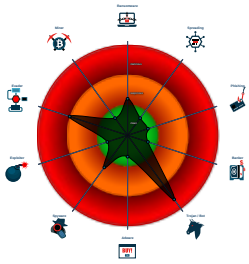
AsyncRAT, DcRat

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Yara detected DcRat
- Yara detected AsyncRAT
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Machine Learning detection for sam…
- Yara detected Generic Downloader
- Machine Learning detection for drop…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- DCwTjs2dTP.exe (PID: 5664 cmdline: "C:\Users\user\Desktop\DCwTjs2dTP.exe" MD5: 2ED2A1D6604AFEAA681F4C66DCD84194)
  - cmd.exe (PID: 2612 cmdline: "C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "sihost" /tr "'C:\Users\user\AppData\Roaming\sihost.exe'" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5128 cmdline: schtasks /create /f /sc onlogon /rl highest /tn "sihost" /tr "'C:\Users\user\AppData\Roaming\sihost.exe'" MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 6128 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\tmp53F0.tmp.bat"" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 5344 cmdline: timeout 3 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - sihost.exe (PID: 5352 cmdline: "C:\Users\user\AppData\Roaming\sihost.exe" MD5: 2ED2A1D6604AFEAA681F4C66DCD84194)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

```
{
  "Server": "techandro.giize.com,hsolic.duckdns.org",
  "Ports": "6906,6907",
  "Version": " 1.0.7",
  "Autorun": "true",
  "Install_Folder": "%AppData%",
  "Install_File": "sihost.exe",
  "AES_key": "w28XgttPSPRfTrqDPtKQKIftMUNaIi1O",
  "Mutex": "DcRatMutex_qwqdanchun",
  "Certificate":
"MIICKzCCACSgAwIBAgIVANmCJqwMXdgA6yyfZkFj0aZTsu+7MA0GCSqGSIb3DQEBDQUAMF8xEDAOBgNVBAMMB2Rldk5vZGUxEzARBgNVBAsMCnF3cWRhbmNodW4xHDAaBgNVBAoME0RjUmF0IEJ5IHF3cWRhbmNodW4xCzAJBgNVBAcMAlNIMQswCQYDVQQGEwJDTjAeFw0yMTEwMjAwODIxNThaFw0zMjA3MjkwODIxNThaMBAxDjAMBgNVBAMMBURjUmF0MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCoRh2gPhcjrCexqYsTMZyZzR9nvXDArts2Pxe7vU8QXZ/2N2LtomHs8oIRK8BSNIq8pybY9t19WGwPVl1goSW14d1Gku1DmuB7h/osKUvia9151iX4HtEJzVUZ21JY54BTSNkrB7mO9MIt+NPmW+T434g9pwjXeLqwPn9vNMjlDwIDAQABozIwMDAdBgNVHQ4EFgQUAiSCu6ZEkdGGrjqlINwtfX5B6ncwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQ0FAAOBgQCYJ/7raO8AXKrzJF9npX6m1mUuFIiPNrmznT/3GogAp/JEDW8keA7Mq+IuMV5zjeQ6jrHVToqCFDUPGd3/yMbwmDlQMYjuj+bNl5f5m2pjHKTX1B/QuUUUPLJ/kXiGOb2zml6uK4n5siqJB5Dhza1QKxnOe0RDyLEnlkVondXy6A==",
  "ServerSignature":
"ZbnE26z/kUoafAYsNOaYAdifPsyY0NUimw56hYN83bmpUDLwVLP2BeWbnk3Mb+RyC7+/9H+auM6ptQK6ib0j+DbOdeQNsf+okOIez8zETDI0UKu51c+FUimCHgyZK+I5Z5tXrRFLS4JhVTH6rhdkluo83hNFkwm6R8TV62hDMtE=",
  "External_config_on_Pastebin": "null",
  "BDOS": "false",
  "Startup_Delay": "1",
  "Group": "Default",
  "AntiProcess": "false",
  "AntiVM": "false"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	Windows_Trojan_DCRat_1aeea1ac	unknown	unknown	• 0x115fbc:$b2: DcRat By qwqdanchun1

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.522471112.0000000000EC9000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_DCRat_1aeea1ac	unknown	unknown	• 0x111f7:$b2: DcRat By qwqdanchun1 • 0x20733:$b2: DcRat By qwqdanchun1 • 0x20977:$b2: DcRat By qwqdanchun1 • 0x24e4b:$b2: DcRat By qwqdanchun1
0000000A.00000002.543917229.00000000054D0000.00000004.08000000.00040000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_B64_Artifacts	Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc.	ditekSHen	• 0x3175d:$s1: U09GVFdBUkVcTWljcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnNpb25cUnVuXA • 0x316ac:$s2: L2Mgc2NodGFza3MgL2
0000000A.00000002.531729380.0000000002D39000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DcRat_2	Yara detected DcRat	Joe Security	
0000000A.00000002.531729380.0000000002D39000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_DCRat_1aeea1ac	unknown	unknown	• 0x28bb:$b2: DcRat By qwqdanchun1 • 0x8cf3:$b2: DcRat By qwqdanchun1 • 0x8f2f:$b2: DcRat By qwqdanchun1
00000000.00000002.542742208.000000000ABB0000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DCwTjs2dTP.exe.abb0000.4.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.2.DCwTjs2dTP.exe.abb0000.4.unpack	INDICATOR_SUSPICIOUS_EXE_WMI_EnumerateVideoDevice	Detects executables attemping to enumerate video devices using WMI	ditekSHen	• 0xb33e:$q1: Select * from Win32_CacheMemory • 0xb37e:$d1: {860BB310-5D01-11d0-BD3B-00A0C911CE86} • 0xb3cc:$d2: {62BE5D10-60EB-11d0-BD3B-00A0C911CE86} • 0xb41a:$d3: {55272A00-42CB-11CE-8135-00AA004BB851}
0.2.DCwTjs2dTP.exe.abb0000.4.unpack	INDICATOR_SUSPICIOUS_EXE_DcRatBy	Detects executables containing the string DcRatBy	ditekSHen	• 0xb97a:$s1: DcRatBy
0.2.DCwTjs2dTP.exe.abb0000.4.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.DCwTjs2dTP.exe.abb0000.4.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
Click to see the 6 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Observed Malicious SSL Cert (AsyncRAT Variant) - Source IP: 182.186.88.126 - Destination IP: 192.168.2.3

Timestamp:	182.186.88.126192.168.2.36906497402848152 08/05/22-09:16:42.961653
SID:	2848152
Source Port:	6906
Destination Port:	49740
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected AsyncRAT

System Summary

Malicious sample detected (through community Yara rule)

Boot Survival

Yara detected AsyncRAT

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

Malware Analysis System Evasion

Yara detected AsyncRAT

Lowering of HIPS / PFW / Operating System Security Settings

Yara detected AsyncRAT

Stealing of Sensitive Information

Yara detected DcRat

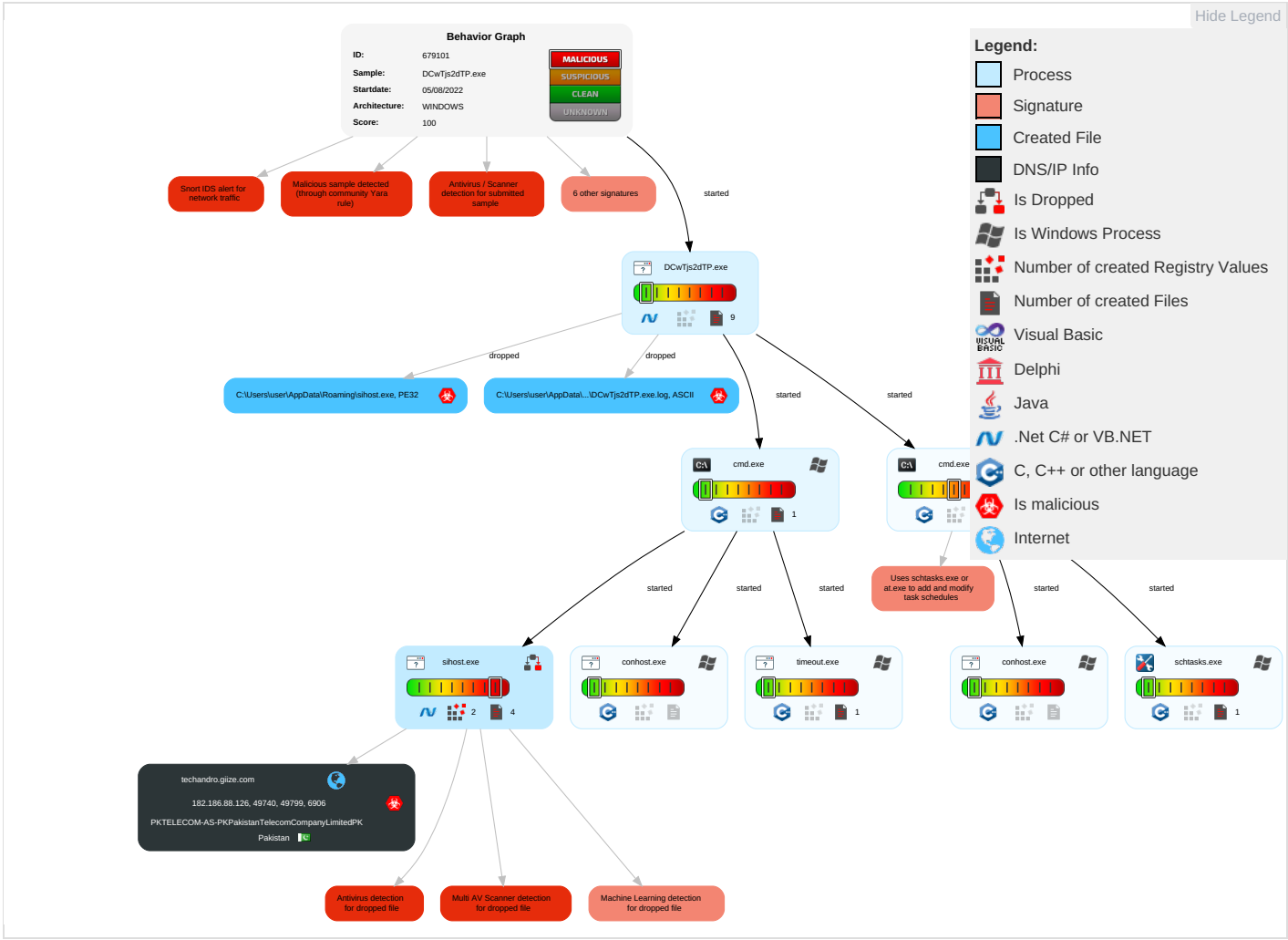
Remote Access Functionality

Yara detected DcRat

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	1 Windows Management Instrumentation	2 Scheduled Task/Job	1 2 Process Injection	1 Masquerading	1 Input Capture	1 Query Registry	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Scheduled Task/Job	Boot or Logon Initialization Scripts	2 Scheduled Task/Job	1 Modify Registry	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	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	1 Scripting	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	2 Process Discovery	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)	2 1 Virtualization/Sandbox Evasion	NTDS	2 1 Virtualization/Sandbox Evasion	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	1 2 Process Injection	LSA Secrets	1 Application Window 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	1 Scripting	Cached Domain Credentials	1 Remote System 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 2 Obfuscated Files or Information	DCSync	1 File and Directory Discovery	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	3 Software Packing	Proc Filesystem	1 3 System Information Discovery	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 Timestomp	/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

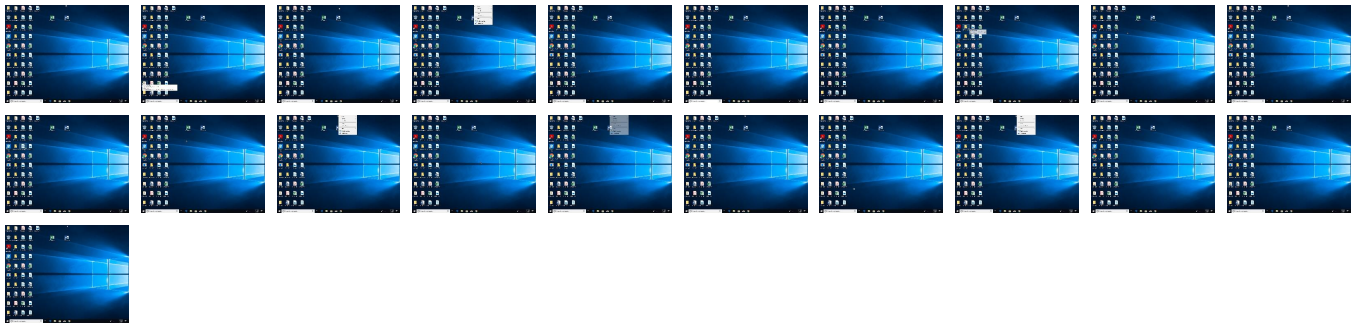
Behavior Graph



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
DCwTjs2dTP.exe	50%	ReversingLabs	ByteCode-MSIL.Backdoor.Crysan	
DCwTjs2dTP.exe	100%	Avira	TR/Dropper.MSIL.Gen	
DCwTjs2dTP.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\sihost.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Roaming\sihost.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sihost.exe	50%	ReversingLabs	ByteCode-MSIL.Backdoor.Crysan	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.DCwTjs2dTP.exe.b10000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
hsolic.duckdns.org	0%	Avira URL Cloud	safe	
techandro.giize.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
techandro.giize.com	182.186.88.126	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
hsolic.duckdns.org	true	• Avira URL Cloud: safe	unknown
techandro.giize.com	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DCwTjs2dTP.exe, 00000000.00000002.533258191.0000000003196000.00000004.00000800.00020000.00000000.sdmp, sihost.exe, 0000000A.00000002.526339237.0000000002ACF000.00000004.00000800.00020000.00000000.sdmp, sihost.exe, 0000000A.00000002.531132514.0000000002CEE000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
182.186.88.126	techandro.giize.com	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679101
Start date and time: 05/08/202209:15:11	2022-08-05 09:15:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DCwTjs2dTP.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:	35
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.winEXE@14/6@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 5.7% (good quality ratio 4.1%) • Quality average: 53.9% • Quality standard deviation: 40%
HCA Information:	• Successful, ratio: 94% • 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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, Conhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 173.222.108.226, 20.189.173.21
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, onedsblobprdwus16.westus.cloudapp.azure.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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 NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:16:25	Task Scheduler	Run new task: sihost path: "C:\Users\user\AppData\Roaming\sihost.exe"
09:16:44	API Interceptor	1x Sleep call for process: sihost.exe modified

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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\AppData\Roaming\sihost.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E94155B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....y.....Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C.....`h!0.I.(C..1Q*L.p.."s..B.....H.....fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<.....3....s.T...._.'...%{v...s.....KgV.0..X=.A.9w9.Ea.x.....\.=.e.C2.....9.....`.o... .....@pm.. a.....-M.....{...s.mW.....;.+...A.....0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt.....h4.iQ?....[.K.....uI.....}.....d....M.....6q.Q~.0.\.'U^)`..u.....-.....d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.....B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,.u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\AppData\Roaming\sihost.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.1358915940078615
Encrypted:	false

SSDEEP:	6:kKku+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:rNkPlE99SNxAhUeE1
MD5:	CCCAC476B9113FEE393FAAE046C51F0B
SHA1:	C234350AFAE80DA95858F154CF4839421C1C2C62
SHA-256:	EE0601D893B6A6978040DCA0C315C7855E278DD1264DE7AF85B91CB2B4C33882
SHA-512:	81A9355BE6696ECBEAFD7ADA021F83E105AA42B61F981BCB597B6874C67847456CC7FD975348BC15E58DDDBAB64091E3DF0FE620FDCCB870FCC28C758E1CA B78
Malicious:	false
Reputation:	low
Preview:	p..... .....(..... .....L.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DCwTjs2dTP.exe.log

Process:	C:\Users\user\Desktop\DCwTjs2dTP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.340009400190196
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhav:ML9E4Ks2wKDE4KhK3VZ9pKhk
MD5:	CC144808DBAF00E03294347EADC8E779
SHA1:	A3434FC71BA82B7512C813840427C687ADDB5AEA
SHA-256:	3FC7B9771439E777A8F8B8579DD499F3EB90859AD30EFD8A765F341403FC7101
SHA-512:	A4F9EB98200BCAF388F89AABAF7EA57661473687265597B13192C24F06638C6339A3BD581DF4E002F26EE1BA09410F6A2BBDB4DA0CD40B59D63A09BAA1AADD 3D
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp53F0.tmp.bat

Process:	C:\Users\user\Desktop\DCwTjs2dTP.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	150
Entropy (8bit):	5.092134229634079
Encrypted:	false
SSDEEP:	3:mKDDCMNqTtvL5oWXp5cViEaKC5UWvSmqRDWXp5cViE2J5xAlnTRI6WcZPy:hWKqTtT6WXp+NaZ5UWKmq1WXp+N23fTg
MD5:	F02730A3503455275DA10EFB33B82C09
SHA1:	76322B42303DBB065740A423FB414CEF653671E5
SHA-256:	09BE09339F9A333B4BA5580D3F6F6E9E928A5A13A1C6448631FAFB1AB0332D6D
SHA-512:	FE402C93721D335BFD90E8D1C2760D0BE95BA95F32FF7675F3B3A465192B5F766ECE30E472D91DAB5F262A4BDB2892854CB1C01E2BC84C6E20CB34EBBFEC9 F4
Malicious:	false
Preview:	@echo off..timeout 3 > NUL..START "" "C:\Users\user\AppData\Roaming\sihost.exe"..CD C:\Users\user\AppData\Local\Temp\..DEL "tmp53F0.tmp.bat" /f /q..

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

Process:	C:\Users\user\Desktop\DCwTjs2dTP.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	144384
Entropy (8bit):	7.592025541663874
Encrypted:	false
SSDEEP:	1536:kbe1mZ5AK6G/WV+22ihLk3jb6B4LGt/XzNNu0oTj7A64MWy/ASOlvL4h59MfoZ+G:ZiLe+22iUXlGlXRN+zA6cQAp+ofoZ+G
MD5:	2ED2A1D6604AFEAA681F4C66DCD84194
SHA1:	6134D837220AFE9377CD78950C8ACA43DDE08D8C
SHA-256:	2A48FA5118BF1C97DE6A6B7B0A45BCC95BD678D54F31E2F2D003E5F3EA49C780
SHA-512:	B6DC02F1974D0D90B171432156B85044AB67B51C00C9A6F2CE98562342DD2AFB64AC36AE57E291D37DA0DB564C719156718391797145596 9D9EB930C920E897
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 50%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...k.....".....0..*.....I.. ...`....@.. ..... ..`.....H..W...`.....  .....  ..H.....text....)... ...*.....  ..`.rsrc.....`.....,.....@..@.reloc..... .....2.....@..B.....H.....H.....$I.....:.....i,.7.=.v.":.....`.t.....>D.5./dos..D+..w..5...<Dp..=?.{....3eKn...f.Q....y.....,.>\..8..R:+^H. .6..I..H.W"..Y...TVf./...,w..p.!.....S.....x&.1...f.V...u..3O.....X.6xmb.....x.T..IwEY.t.%5..5....1Ca....|1.Z1.gW..sa..E..+.w..x7=..N...8QY5.y.H....L..OJ...2.....<=..=cx.M....s..F...^.. ..S...5.....O.....?S.AU.s.....:.....@..(=.Nt...q.4!..I.....j.R|..t.b...GA.{.7..i(.I.G2..z.u..y.6

\Device\Null	
Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.41440934524794
Encrypted:	false
SSDEEP:	3:hYFqdLGAR+mQRKVxLZXt0sn:hYFqGaNZKsn
MD5:	3DD7DD37C304E70A7316FE43B69F421F
SHA1:	A3754CFC33E9CA729444A95E95BCB53384CB51E4
SHA-256:	4FA27CE1D904EA973430ADC99062DCF4BAB386A19AB0F8D9A4185FA99067F3AA
SHA-512:	713533E973CF0FD359AC7DB22B1399392C86D9FD1E715248F5724AAFBBF0EEB5EAC0289A0E892167EB559BE976C2AD0A0A0D8EFC407FFAF5B3C3A32AA9A0AAA4
Malicious:	false
Preview:	..Waiting for 3 seconds, press a key to continue ....2.1.0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.592025541663874
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:	DCwTjs2dTP.exe
File size:	144384
MD5:	2ed2a1d6604afeaa681f4c66dcd84194
SHA1:	6134d837220afe9377cd78950c8aca43dde08d8c
SHA256:	2a48fa5118bf1c97de6a6b7b0a45bcc95bd678d54f31e2f2d003e5f3ea49c780
SHA512:	b6dc02f1974d0d90b171432156b85044ab67b51c00c9a6f2ce98562342dd2afb64ac36ae57e291d37da0db564c7191567183917971455969d9eb930c920e8979
SSDEEP:	1536:kbe1mZ5AK6G/WV+22ihLk3jb6B4LGt/XzNNu0oTj7A64MWy/ASOlvL4h59MfoZ+G:ZiLe+22iUXlGlXRN+zA6cQAp+ofoZ+G
TLSH:	D4E36B9D366036DFC867C872CAA82CA8AA50747B471BD203A45715EEDE4D99BCF050F3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...k.....".....0..*.....I.. ...`....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x42490e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xF60FB06B [Tue Oct 26 08:42:19 2100 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x248b4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x26000	0x596	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x28000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
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	0x22914	0x22a00	False	0.8304095216606499	SysEx File - Victor	7.625943654905051	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x596	0x600	False	0.412109375	data	4.024186334587364	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x28000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x260a0	0x30c	data		
RT_MANIFEST	0x263ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

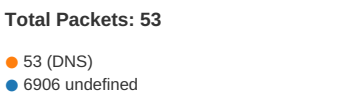
DLL	Import
mscoree.dll	_CorExeMain

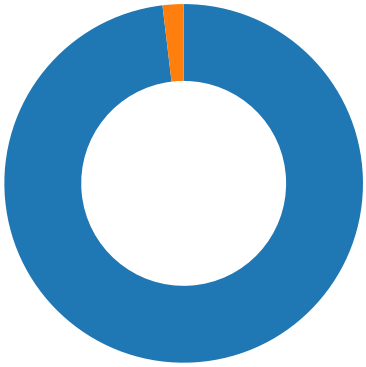
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
182.186.88.126192.168.2.36906497402848152 08/05/22-09:16:42.961653	TCP	2848152	ETPRO TROJAN Observed Malicious SSL Cert (AsyncRAT Variant)	6906	49740	182.186.88.126	192.168.2.3

Network Port Distribution





TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:16:42.343604088 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:42.507725000 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:42.507963896 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:42.793518066 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:42.961652994 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:42.980221033 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:43.147313118 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:43.202167988 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:46.467544079 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:46.836049080 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:46.836447001 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:47.193211079 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:58.082192898 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:58.449898958 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:58.450030088 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:58.612859011 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:58.734793901 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:58.906966925 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:58.953510046 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:59.070375919 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:59.440320969 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:16:59.441751003 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:16:59.811695099 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:05.920444012 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:05.969835997 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:06.131196976 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:06.173055887 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:10.167838097 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:10.545608044 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:10.545766115 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:10.730561972 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:10.782721996 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:10.952214003 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:11.004468918 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:11.991069078 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:12.361207008 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:12.361320972 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:12.723164082 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:21.618616104 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:21.978775024 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:21.979440928 CEST	49740	6906	192.168.2.3	182.186.88.126

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:17:22.142467022 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:22.189888000 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:22.352082014 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:22.379858017 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:22.742747068 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:22.743539095 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:23.120084047 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:33.216279030 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:33.586165905 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:33.586325884 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:33.750921965 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:33.878433943 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:34.040781975 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:34.080080032 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:34.441732883 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:34.442347050 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:34.888081074 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:35.953671932 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:36.003654957 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:36.184784889 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:36.237941027 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:44.886441946 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:45.245990038 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:45.247559071 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:45.411969900 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:45.504420042 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:45.665941000 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:45.682383060 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:46.049994946 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:46.050144911 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:46.436414957 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:56.406936884 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:56.767236948 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:56.767338991 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:56.949023008 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:57.146131992 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:57.307141066 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:57.372817039 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:57.735706091 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:17:57.735805988 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:17:58.094325066 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:05.973809958 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:06.146740913 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:06.311863899 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:06.443659067 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:08.011923075 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:08.389894009 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:08.390151978 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:08.563564062 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:08.740721941 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:08.901375055 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:08.914977074 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:09.280356884 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:09.280605078 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:09.526557922 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:09.647113085 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:09.808506966 CEST	6906	49740	182.186.88.126	192.168.2.3
Aug 5, 2022 09:18:09.869719028 CEST	49740	6906	192.168.2.3	182.186.88.126
Aug 5, 2022 09:18:10.230223894 CEST	6906	49740	182.186.88.126	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 09:16:42.094877958 CEST	49316	53	192.168.2.3	8.8.8.8
Aug 5, 2022 09:16:42.273111105 CEST	53	49316	8.8.8.8	192.168.2.3

DNS Queries

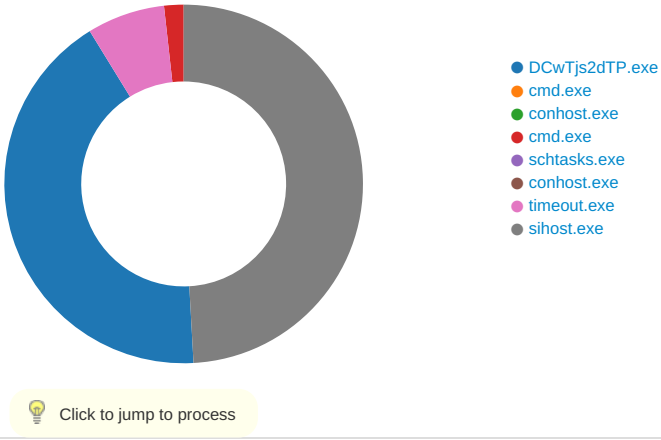
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 09:16:42.094877958 CEST	192.168.2.3	8.8.8.8	0xf053	Standard query (0)	techandro.giize.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 09:16:42.273111105 CEST	8.8.8.8	192.168.2.3	0xf053	No error (0)	techandro.giize.com		182.186.88.126	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: DCwTjs2dTP.exe PID: **5664**, Parent PID: **5308**

General

Target ID:	0
Start time:	09:16:16
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\DCwTjs2dTP.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DCwTjs2dTP.exe"
Imagebase:	0xb10000
File size:	144384 bytes
MD5 hash:	2ED2A1D6604AFEAA681F4C66DCD84194
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.542742208.000000000ABB0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.542742208.000000000ABB0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 00000000.00000002.525348826.0000000002EB0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: INDICATOR_SUSPICIOUS_EXE_WMI_EnumerateVideoDevice, Description: Detects executables attemping to enumerate video devices using WMI, Source: 00000000.00000002.542742208.000000000ABB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: INDICATOR_SUSPICIOUS_EXE_DcRatBy, Description: Detects executables containing the string DcRatBy, Source: 00000000.00000002.542742208.000000000ABB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Donutloader_f40e3759, Description: unknown, Source: 00000000.00000002.540094195.000000000478F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 00000000.00000002.526006194.0000000002F00000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 00000000.00000002.521245478.00000000011CF000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: **2612**, Parent PID: **5664**

General

Target ID:	2
Start time:	09:16:24
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c schtasks /create /f /sc onlogon /rl highest /tn "sihost" /tr "'C:\Users\user\AppData\Roaming\sihost.exe'" & exit
Imagebase:	0xc20000
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: **5256**, Parent PID: **2612**

General

Target ID:	3
Start time:	09:16:24
Start date:	05/08/2022
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

Analysis Process: cmd.exe PID: **6128**, Parent PID: **5664**

General

Target ID:	4
Start time:	09:16:24
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\AppData\Local\Temp\tmp53F0.tmp.bat""
Imagebase:	0xc20000
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 Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp53F0.tmp.bat	unknown	8191	success or wait	5	C2FB07	ReadFile

Analysis Process: schtasks.exe PID: **5128**, Parent PID: **2612**

General

Target ID:	5
Start time:	09:16:25
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn "sihost" /tr '"C:\Users\user\AppData\Roaming\sihost.exe"'
Imagebase:	0x920000
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: conhost.exe PID: **3404**, Parent PID: **6128**

General

Target ID:	7
Start time:	09:16:25
Start date:	05/08/2022
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

Analysis Process: timeout.exe PID: **5344**, Parent PID: **6128**

General

Target ID:	8
Start time:	09:16:26
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 3
Imagebase:	0x1360000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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\Null	15	15	20 73 65 63 6f 6e 64 73 2c 20 70 72 65 73 73	seconds, press	success or wait	1	1362DA7	fprintf
\Device\Null	52	37	08 32 08 31 08 30 0d 0a	210	success or wait	1	1362DA7	fprintf
\Device\Null	54	2	08 31	1	success or wait	3	1362DA7	fprintf
\Device\Null	60	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	1362DA7	fprintf

Analysis Process: sihost.exe PID: **5352**, Parent PID: **6128**

General

Target ID:	10
Start time:	09:16:29
Start date:	05/08/2022
Path:	C:\Users\user\AppData\Roaming\sihost.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\sihost.exe"
Imagebase:	0x7a0000
File size:	144384 bytes
MD5 hash:	2ED2A1D6604AFEAA681F4C66DCD84194
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 0000000A.00000002.522471112.0000000000EC9000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: INDICATOR_SUSPICIOUS_EXE_B64_Artifacts, Description: Detects executables embedding bas64-encoded APIs, command lines, registry keys, etc., Source: 0000000A.00000002.543917229.00000000054D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_DcRat_2, Description: Yara detected DcRat, Source: 0000000A.00000002.531729380.0000000002D39000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 0000000A.00000002.531729380.0000000002D39000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_DcRat_2, Description: Yara detected DcRat, Source: 0000000A.00000002.526339237.0000000002ACF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 0000000A.00000002.526339237.0000000002ACF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 0000000A.00000002.546757964.000000000A90A000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 0000000A.00000002.527734779.0000000002B49000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 0000000A.00000003.516805151.000000000A8F3000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 0000000A.00000002.523503805.0000000000F10000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_DCRat_1aeea1ac, Description: unknown, Source: 0000000A.00000003.516841569.000000000A90B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 50%, 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	6CDFCF06	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	6CDFCF06	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	6CDFCF06	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	6CDFCF06	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ActiveMovie	success or wait	1	6CCD40CE	unknown
HKEY_CURRENT_USER\Software\Microsoft\ActiveMovie\devenum	success or wait	1	6CCD40CE	unknown
HKEY_CURRENT_USER\Software\C4D93783EC1A25CC28F9	success or wait	1	6BC45F3C	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\ActiveMovie\devenum	Version	dword	7	success or wait	1	6CCD40CE	unknown
HKEY_CURRENT_USER\Software\C4D93783EC1A25CC28F9	94E168CABBEA0702E60265D1291BE8FE7C37724D89001E7AE9A73817F84114EF	binary	00 EA 05 00 1F 8B 08 00 00 00 00 00 04 00 BC BD 07 7C 1C C5 F5 07 BE B7 7B B7 7B BA 93 64 9D 74 BE 93 25 D9 92 8B E4 F5 B9 20 0B 6C 54 5C E4 46 31 25 B6 31 C6 86 D0 C1 60 03 5E FB CE 26 04 21 C5 98 4E 8C 69 86 D0 21 06 93 46 80 D0 03 84 5E 13 8A 71 48 A8 0A 84 00 01 42 7A 42 08 49 C4 7F BE EF CD EC EC 15 D9 4E FE BF FF DF 1F EB 76 76 E6 CD 9B 37 33 6F DE BC 79 F3 66 F6 80 43 2F 31 2C C3 30 C2 E2 EF CB 2F 0D E3 01 83 FF 75 1B 3B FF B7 5E FC 55 36 3E 58 69 DC 53 F6 E2 C8 07 42 FB BF 38 72 F1 89 2B 72 4D AB B3 DE 09 D9 A3 4F 69 3A F6 E8 55 AB BC B5 4D C7 1C DF 94 5D B7 AA 69 C5 AA A6 B9 5F 39 A8 E9 14 EF B8 E3 27 55 54 C4 C6 48 1C 0B E6 19 C6 FE 21 CB F8 FD C6 DF 1E A3 F0 BE 6B 98 4D F1 50 D4 30 DE 8B 18 86 CD 71 37 20 D0 24 02 4D 36 53 87 B0 C9 74 1B 86 7E 1A 47 D9 14 8F 7F 96 D1 7D 8E 61 54 D1 7F FD F4 1F 5C BE C0 BB BF C1 78 27 58 25 2A D9 6D 1B E5 BB D0 16 85 FF 6E 13 78 A3 C1 08 41 EF 3E 81 D7 49 6B 8F 3F 6D AD 78 DE F3 6E 84 EB 82 BA 9A F9 38 44 F4 51 93 B2 B9 EC B1 22 4C B4 A1 EE A8 E8 FB 91 7C 12 C5 FF 49 D9 E3 4F F6 04 60 B9 A4 99 70 7D 54 04 37 BB 90 4E D0 64 1A 11 E3 9E C9 A6 71 DD 4B 96 11 92 F1 0F D7 99 C6 E7 A9 5D AF 6F 5D 9F C8 19 CE 18 23 CC F5 14 A8 EB 33 D5 BB C9 EF 96 7A B7 F8 3D AC DE C3 FC 1E 51 EF 11 7E B7 D5 BB CD EF 8E 7A 77 F8 3D AA DE A3 FC 5E 46 EF 75 7D 31 15 4F 81 FA D6 26 E3 07 82 22 F1 3F 91 EB 2C 33 EC 98 6D F6 7E 62 1A E1 DA 74 43 4E 44 C6 9A 9B 8C E7 0C C3 33 75 50 D0 17 73 C5 BB ED 8A 74 BB AF 42 A0 F1 04 8D 31 4F 10 16 4B 5F 24 C8 09 35 A7 1A 3B AF F7 44 28 96 BA 59 90 13 DA 09 50 9A 80 5C 07 E9 51 60 07 62 4F 10 1C EB F8 97 68 BB B4 5B A5 4A 4B E7 62 40 9A 1C B0 87 8A B7 5C 5C BC E4 CA 91 23 0C 08 4B 81 ED 8C 9E 64 D3 63 02 6F CA 13 64 C5 EA 56 BA 31 E4 13 C5 D9 AF 5E 14 07 21 82 06 3B B5 D2 15 88 6D 51 D2 30 94 54 29 20 93 B9 21 E2 B7 E9 AA 4E C1 69 AD EB 44 4B 54 A1 F8 52 71 09 90 54 E9 93 E4 00	success or wait	1	6BC4DE2E	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			1F FD 6E 5A 21 10 A6 81 B0 1A 08 BD 1A F1 DB 62 0F D8 5D A2 E5 73 49 64 1D 8A AC 82 B1 62 ED 18 C8 29 AA 7A 3F B8 B6 45 86 C1 4D 19 63 56 03 F3 95 A8 81 71 A9 A8 F2 0D 21 E6 6D 81 30 D4 E6 42 2E 58 9E 28 27 96 11 71 F5 AD 11 63 99 E4 43 46 E2 8A 6C 76 73 27 4A 68 69 C7 20 70 6B 51 AC 55 18 3B 4C 75 46 5E 6C 1D 62 EB C5 4F 3F 45 4A 8A 44 C1 52 70 2C 5A 64 D8 A0 A3 BE 35 6E 3C 18 A2 A1 96 08 74 69 0C 38 44 AB D9 9D 71 5D C3 2B 44 3A 95 6F 7A A2 66 B1 98 9D 9A 71 12 A2 04 88 6D AF 5C 4A 7D 41 5D 64 AF 5C A6 FB AB D3 04 0C 37 EF 70 91 2D D0 95 A9 95 33 9E 00 FA 95 3A 6B A0 77 DB 8F 34 64 79 94 9B 8A 59 41 40 2B BC 11 02 51 DC 49 4D 0F 50 F7 0F 43 92 E2 04 49 71 82 A4 A4 56 4E 0B 64 78 06 19 38 BA F5 2A D1 E5 23 D1 E5 8D E8 DF 26 34 1E CA F4 46 82 1D 99 BC 41 78 B0 BD 13 92 63 87 FC D9 9E D6 25 05 09 98 37 68 FD 4A 30 E0 8E 59 CD E7 35 FC FB 61 88 FF 14 AF D5 B7 56 1A 7F 35 30 97 88 3E 16 6C 6F C7 52 71 BB 3A E4 8E 42 35 D1 C9 1D C0 6D 76 82 71 FA 5F 44 70 D3 0A 77 B4 48 2C 27 8E 18 9A F6 C6 80 02 22 35 9A 8A 6E 5A E1 35 8B 77 01 D4 D4 3D 7B 88 31 E3 38 E4 C8 B5 88 A8 8A 54 4D B8 2C B5 D2 1B 8B E1 B6 E0 49 C3 A0 A6 A8 89 B4 83 B8 62 5C 89 48 2A 11 26 5C 65 08 46 36 71 BF 36 D7 84 53 AD AF F4 0B 84 46 19 51 56 E6 B9 22 FA 6D 66 BD 94 29 CB A7 57 6F 1C 58 7C 58 A0 3D 30 D8 1C CA 66 BB 19 64 CB 88 CE 00 7F 1F 61 2C B8 9D 86 A2 81 D9 F3 F9 37 8C 72 B4 8D 29 66 B8 FE 0F 38 FE FB B9 8D 18 46 59 41 E8 6A EF 6B 22 98 4D 20 74 36 CA 39 13 F8 6A F1 53 4F 23 76 52 6E BC 78 AE 2F 63 F9 1C 31 8E 93 6D DF 27 88 08 BB 13 30 86 86 A0 D2 0D 68 5E 1A 91 8D C8 3C 5C C9 9B E0 60 F5 26 96 1C C2 93 50 35 20 F1 76 43 FA 28 BF B7 D5 18 5E BC D8 18 22 10 86 96 B8 AD E0 DA C9 68 F5 26 31 90 BD 36 16 2A AB FA 84 78 0B 77 00 9A 42 DE EE 60 A7 F5 08 66 FA 76 4C A8 A8 93 65 D4 2B 79 94 4A B9 4D AA 6D 5B 9A 6E 3A 37 64 B8 7B 88 8C E3 FF 96 F1 E5 49 45 85 51 C1 BC D6 64 DC 13 A6 29 3E 41 CD 29 E6 AA B5 A2 6A F5 5E 1F 04 83 6E 5B EF 2C F1 13 77 DC FD C4 A3 3C DA F4 D5 09 1B CF 9A 7D 91 40 14 6D 1A DD F5 B3 B1 B3 67 51 F0 E3 03 3E AE 9F 5D 4F C1 25 FB 7F 5C D7 35 29 A4 62 BB DA 45 B0 BD 23 8C F7 F5 D1 7B 9A BB 3E F6 F3 76 5D 8B A4 11 94 74 F9 B8 C5 27 49 04 5F 6C DA B8 B4 EB D1 90 8A ED FA 2B A0 3E B7 F0 7E F3 9D 47 9C D6 F5 39 25 81 8E AE DB 91 D4 4F 49 EF FF FA D4 E7 25 31 35 4F 7D 72 B1 C4 F5 6A EF 6B 17 77 5D 1F 52 B1 5D 98 A9 DA 6F A3 0C 4D 55 7F BA A2 6B 8D A1 F2 76 FD 13 49 97 52 52 F5 7D D5 FF 90 08 AE BE E7 88 57 BA 86 87 54 6C D7 F7 00 75 12 41 8D 9C EC 7D DE 75 3B 41 9D DD 66 FE AB EB EB 14 FC 34 71 DD 40 D7 6B 80 9A 27 A0 9C AC E8 A4 D5 EE 14 D1 09 9D 07 83 D8 56 8A 1C EB 47 2E 40 64 3D 45 76 F9 91 FB 21 D2 A6 C8 85 7E E4 5E 88 FC B3 89 C8 13 FC C8 59 88 7C 9B 22 CF F1 23 A7 22 F2 59 8A FC 81 1F 39 05 91 77 51 E4 8B 7E 64 06 91 D7 53 E4 C7 7E 64 23 22 CF A7 C8 B2 90 8A 4C 22 32 47 91 43 FD C8 21 88 3C 82 22 9B FD C8 9F 23 72 5F 8A EC F0 23 9F 47 E4 1E 14 79 80 1F F9 32 22 1B 29 F2 58 3F F2 69 44 C6 28 F2 4C 3F F2 67 88 FC 7B 08 91 D7 FA 91 4F 20 F2 5D F1 93 9B 2B 58 B3 05 F3 BC DD BE 0D EF F3 F4 FB 63 78 DF 5B BF DF 89 F7 7D F5 FB 4D 98 F3 A6 22 74 25 42 ED 98 07 37 FA 71 1B 10				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			DA 13 A1 D3 10 EA 42 68 15 42 D3 10 3A 0E A1 7A 9A 2F A7 42 C7 58 AC DE 91 25 96 FD 21 28 6D 87 B4 2D CB 75 88 47 4D 38 11 CE DE 2F 22 3D 31 13 C5 44 F8 67 81 F0 EF 00 DC 05 45 6B 1A 7E A6 03 81 90 79 AB DD 19 78 95 40 11 44 CC 84 8C 69 0F C4 56 88 D8 32 B7 1B 39 86 E5 E5 20 99 94 08 77 38 F4 60 D9 9C 9B 05 C1 5D E6 CD C6 23 ED CD C1 23 E5 CD E5 C7 3C 8E DC 0B 25 EC 0D E9 2F 2B D6 23 10 E4 E6 A3 D1 DA 57 43 5E 67 C7 99 41 E1 90 9B 49 49 07 03 6A 0E 05 E7 43 92 89 59 2D AC E4 64 07 E4 D5 3E C0 B5 1B 10 E4 BA 09 6C B4 A1 1A 2C BF E6 C9 64 DA DD 1D 10 5C 7E 49 D9 3A 6B 0F 5E 76 9C 28 86 09 D6 36 6F 8B E7 10 23 FF DF 2D 61 FE 43 3C E4 6F 8D D0 A1 A6 CA B4 A2 29 64 4F 53 4E 21 CD 1C FC 1A E9 4F F9 73 8A 90 D5 21 81 AF A6 35 6C 9C A0 F0 4C 13 DA 66 73 65 B8 F7 77 42 CF AF 8C 90 D0 AE B4 D7 0F C1 C3 59 0F D9 5D 19 5D 2F A6 A7 B0 B5 1E 7A 7B D8 15 0D 62 47 5C 21 82 85 A6 3A BD 84 A6 0A 8D AE E9 23 51 1B 12 DD 34 ED 4F FC 63 86 CA 1D 61 BA 98 CC 32 EA F9 60 9F 40 13 EE 14 73 B1 91 9D 23 68 DE 86 A5 98 BB 2F 9A 71 3E 90 EE 87 99 0F 20 04 87 F5 4A 52 AD 57 92 3C 1F 96 19 13 65 3D 06 EB 82 92 8D 6F 68 FD 74 F8 70 9E DB 6A 5A 6D E3 41 F1 2E 66 A6 44 2A D6 B7 3F F4 BE A1 E5 F4 84 B6 D1 27 A6 FE 70 2A 5D 6D 55 87 DD C9 98 C1 A0 33 6E 6B 0A 49 7A DD 03 30 40 22 65 35 76 AA C6 69 9F 0E 86 B5 03 A9 07 8A 9F AD 78 AD 89 26 84 36 E2 7E 05 D0 76 22 DA D3 62 89 FA 63 E9 2B C2 63 44 B8 3C E1 A4 97 D6 38 09 27 11 6E FB 49 74 28 D6 A6 86 BB 1B CD 5C 42 8F 6A 45 C1 D0 F1 9C 14 11 56 9B A6 86 B4 63 0E E6 70 BB 45 F5 6F 7D 6B C2 68 C2 34 2F F0 12 60 AC 3A 34 30 74 84 28 BF DA 1C 18 DA 20 9E 5C AF EA D0 B6 11 79 35 E8 1D 22 68 A8 36 DC 36 A5 90 67 7B 44 B7 E4 16 88 A4 D3 9B 30 D5 46 3A A9 7B 31 53 B4 83 7B 1B AB 8E AA 09 57 87 22 34 4C 52 98 2A 8D FA 13 7B EB 81 25 94 FD 58 E4 ED 4D 20 6C 09 11 33 C1 C7 59 66 29 9C B6 69 11 25 F4 23 74 B4 32 91 AD DA 84 3A 65 13 57 B8 0B A9 59 B3 BD 22 47 75 C4 5D A4 44 07 E7 96 A9 FD 7B 92 0E 46 2D 50 46 98 DC 83 A0 6D 40 6C 94 B9 13 11 1D ED 71 04 19 0C 12 ED B1 FD F0 DB 69 D2 71 4C A3 CD B8 F7 B7 06 F0 F8 3C 3A 89 30 AD 1F C6 7C 96 35 32 82 31 1C E8 B5 C4 67 8B 21 AD A2 61 29 20 63 24 D4 B2 D5 78 3F 18 8C 23 2A 9F C2 CB 12 3F FA 10 11 B2 DD A5 A4 EB 92 06 74 9D 68 3E 77 19 E8 BC 4C 84 B2 75 02 48 A6 47 73 87 A2 73 0A 18 BA CC 3B 0C 35 FB 2A 72 DC 8F A6 39 9C 44 72 4A 28 BD 7B 90 7C 4C 44 6E 1E 0B 3E B6 13 76 51 AE 29 AA 3D 44 DA 11 90 BA 11 C1 65 91 44 24 11 DE B4 A2 ED 29 2A DC 3D D2 90 CB 31 7E 3D 0A A4 CF 55 09 DC 71 F4 7A 34 04 6B A1 A8 9F EB 93 9F 76 8F 41 07 1D 8B A4 E3 54 52 F6 54 F1 E3 1D 0F 59 88 75 58 0B B5 57 5E 75 6B 9C 02 94 09 27 50 E1 53 F2 2B DC 9D 57 E1 68 22 5A 9C 4D D7 38 4A 35 0E AC 4E F3 2A FF 40 41 B1 51 A6 BF 3F 45 64 E6 A7 95 53 76 FA C9 BD 17 16 52 D3 AB 8A 88 C5 6D 59 A2 CC 5B 62 19 76 5F 3D 54 DF 6B 45 48 45 D4 21 E2 5B 22 94 FB 1D 00 63 89 98 BB 1C 95 88 57 C7 B3 17 A2 2D 4F 00 A9 27 02 FF 9E 02 20 11 F3 F6 10 8F D1 2C 98 92 DD EE 0A A4 BC 1C 21 84 8B 2C 02 10 23 6C 7C 8B 78 3D 44 BC A6 BC 47 B9 30 BC A4 BD 5F EA 97 94 B7 3D F8 22 C1 0E 14 8F 68 F6 2E 51 70 32 57 6F 8A 79 C1 04 32 EF CF A2 2A				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			7D 42 04 86 05 C8 B5 61 CC 6B 13 69 68 D7 B9 27 17 F5 52 79 61 2F 95 EF 6A 2F 55 24 2A 8A B3 E9 5E AA F8 9F 7A E9 3B 83 30 53 65 21 99 95 BB 4A E6 90 C4 90 E2 6C 9A CC 21 FF 13 99 85 1C 53 95 A8 2A E4 98 AA 92 1C 93 48 24 76 CC 31 89 41 39 A6 8A 39 26 21 39 A6 2A C8 0A 55 41 8E A9 0A 72 4C 01 D8 8E 38 A6 01 1C 53 C5 1C 33 C8 24 3B EB 36 26 EC 72 41 83 58 3F 1B 0F F3 9C 44 B6 02 C4 CF 13 BF B7 8A A7 50 1E 8D 54 20 5E 88 4D E3 0F E2 6F AE 78 7B 22 10 DF 61 31 9E 63 AC 7C 3C EF CA F8 B2 70 7E BC 98 80 8C EF 8A 27 56 45 DF 09 C4 E3 5F 5D 84 FF 94 6E 05 FB 14 74 A2 28 D6 93 E8 AB 98 AD EB 99 F2 2E 0E CB 65 29 DB 30 6C A9 8D 02 30 EE E8 21 14 00 64 DB 80 C3 80 A5 1B 88 ED 05 B6 91 6A 60 BB 80 69 EC 66 A4 E6 29 DB 81 61 1C 72 08 EB 26 F5 AD E5 46 1F EA 57 8A B6 DC 29 E8 F3 AB C4 AB 27 E6 7E 9B F8 34 1D EF 5F 40 54 FA 84 0D 02 05 4D A8 B8 5A A9 78 7F 22 8F 5E 11 01 7A 1C E8 17 0D 4C F3 C2 43 34 9D 27 9D 64 24 40 A7 9A 3B 6F CD 8A 95 F9 EA F5 60 E6 EC 13 08 81 CF B3 9F 23 04 8A B3 6E 44 84 86 93 2A 27 74 95 7A E3 08 D8 96 07 9B 5B F3 E4 50 BC 60 84 39 72 84 B9 05 82 60 30 38 50 CB F3 EF B9 18 93 B3 48 66 64 8F 11 F4 D0 8A 22 DA 70 91 43 16 62 77 15 88 58 29 E2 5D 0F 38 C4 B2 21 B6 A5 39 4D 4B 9A 2D CD B5 05 D8 DD 35 94 3C 2C FB F7 08 92 EB 9C 2D CD F5 59 C7 16 61 37 0B 98 1C C9 02 5A 97 44 79 CD 12 E5 F5 49 BB 10 48 46 DF 5A A0 A0 02 EB ED 60 81 B5 DE 3A 03 AB AF 52 A5 11 25 4E 60 89 75 2A AA 87 1E C9 33 65 E5 1B 65 67 ED CF FD 25 94 75 1A 2F 33 D0 1A 72 5C 40 E4 A7 44 3F EC 26 C7 A5 DF B9 8A 17 43 FC 67 FB E3 A5 DA B8 5A 84 E3 05 3C 59 8A D8 C1 86 CF 4E 6A 1E 2F D4 09 08 19 16 36 B1 5D 1D 61 86 3F C6 9A C7 AB 31 B6 D4 68 FC 9A AE DE 05 17 A8 31 56 6D DC 65 90 2D 73 A7 F5 D1 83 29 5E 5C 29 27 30 C0 CA FB 8F FE 5F 3B D8 3B 4D FC 24 07 AC F2 FE 11 85 9D 1A 18 97 AC 92 44 33 BA 9E 99 56 55 4F CF 18 7D 99 AE E7 8D 37 E6 8F D1 1A 31 EE FE 21 D3 38 CA 0A 58 46 46 8A 58 2B 7B 83 AD DE 17 D2 FB 9D FE FB 99 68 5D 5A FA E6 BE 2E DE 9B 79 59 AE 07 52 73 F6 11 01 4B 8C 2F 17 E4 72 B1 EE 9D 8E 9F 1E 30 FF 8E F3 FF E1 FF 65 FE 11 CE 4E F3 FB 6B 25 83 F9 3D A1 DA 21 DF 3C 10 B3 B3 B3 1D 55 71 C8 45 3B 3B DF 7F FF 21 B1 99 69 B9 82 00 BB 71 44 BC 7D 83 21 B5 8B F2 54 45 3B 7A 3F 5A C6 9A 45 38 11 F6 CE 40 C7 F5 22 DF 1C 34 7B CF 08 CC A1 1C 0D B3 65 6C C0 FE 06 D8 6B BD C1 56 E7 F1 1D B0 67 3B 8D 23 66 24 31 3A E3 66 10 D6 15 F5 B4 CB D2 4B 2B CA A2 42 F5 B8 5A AC 1B E3 7A D9 DD 17 87 22 21 68 89 75 78 5F 7E F9 65 FF 48 12 03 30 09 52 4A 9E F9 17 66 0D 32 26 49 7B 6F 87 B1 F5 57 BC 67 53 D3 3A D4 B8 45 C4 54 62 1D 59 32 5F 4E 34 50 6C 3D 92 8A EC 11 8B 9D 22 93 B6 99 13 EF B1 5E D4 DA CA AE 76 82 8D 4C 55 4A 4B E9 9B 3D 43 A4 6D 49 79 E7 40 FE A7 E2 ED C3 D1 E8 0E 6D D6 95 73 A3 45 BD 73 D1 0E E7 91 68 5F 1A 77 6C D1 04 FD 19 B6 6D EC C0 46 02 8B 9C B4 91 AC 57 C5 5B A5 6D 24 F5 AD 23 0D 98 CF 86 F8 7C 91 67 10 2A 68 01 24 B5 4F 84 6D 8E 76 00 9F 12 33 75 D3 D2 7A B9 03 C8 86 90 F3 41 F0 05 A8 91 58 60 5F 58 14 F3 4D E0 DA C8 52 EF 22 B0 4F 6E 13 64 43 34 05 A3 78 1E E4 C5 78 B9 04 35 6F 02 E3 D2 4F 9F 60 17 41 1B 6C 03 2D 7D 63 45 78 C0 EE 86 6D E6 52 70 FE 7A 24 D2				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			52 D6 BB 0C EF 65 EE E5 08 6F 96 25 E6 B5 D0 01 BA 85 36 A9 16 72 AB D1 40 1C 79 95 8A 2C F3 AE 00 92 35 79 6D E7 5D 59 7A 16 42 4C 94 62 A2 4A 48 02 92 F7 84 20 B8 A9 6D 99 5F 1F 1C 10 FC CA D3 16 35 72 8A FB 04 73 17 E6 28 D8 F2 E0 77 B1 7B 60 8E 42 BC 90 A4 C6 B6 12 73 17 30 AD 16 71 A7 06 74 CF 7A C1 D7 E7 E5 C9 3E D6 09 42 34 98 07 93 28 B7 38 C5 26 CE C7 1C 35 FF 06 45 4D 76 3B 5A E9 5B 1C 33 2F 5F EA 04 0C AE 79 93 33 8F BD 6A 63 D5 7A B5 5F 9A 32 2E 1D 94 46 9A 52 B2 BF 42 31 57 51 89 9F 89 60 36 1C 2D A6 D0 8D 06 35 04 EF 6A 74 3A 55 D0 BB 06 C9 ED 51 55 3F 7E 5F 14 95 62 73 C7 D4 1A 3E BD A7 5D A8 E8 AD 32 BE 6D 90 BF 48 62 10 7A 9B B3 4F 45 25 C1 2D 1C 4E 7B D7 A2 50 2C 30 0A E8 D6 D4 36 8E 21 FD 2F DB 50 A6 34 42 AA A7 4D E1 94 BB 17 DB 59 31 C4 02 56 C7 00 D9 3B B4 FF 55 1B DF B8 54 CF FF 58 23 24 76 44 FF A1 65 9A 7E 84 99 FE E6 41 2B 90 7D 50 00 51 6A 71 7D DE 2C 5D 9F 7D 74 7D 76 5A 0B 55 87 73 BE A5 EA D0 62 DC 15 42 8C 2F B3 12 FE E6 DB 25 86 54 7D 3B 27 29 9D 24 1B 8B 19 AB 6B BD EB 80 76 30 4D AB FD 00 43 2A CA 79 83 61 79 AC A8 C6 5A 2F 2D 1E 11 3C F9 B2 D2 1B 60 24 49 C6 16 4D 06 89 9A EB F3 D9				

Disassembly

No disassembly