ID: 336710
Sample Name: DES_ Holdings Ltd - products listing.exe
Cookbook: default.jbs
Time: 17:51:49
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

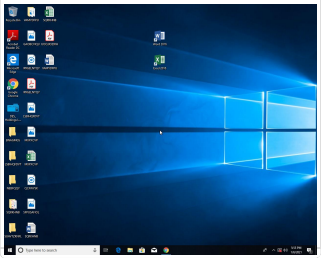
Analysis Report DES_ Holdings Ltd - products listing.exe

Overview

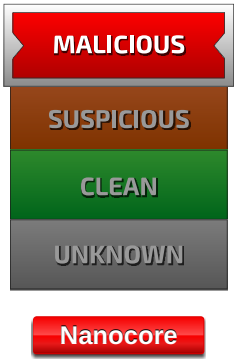
General Information

Sample Name:	DES_ Holdings Ltd - products listing.exe
Analysis ID:	336710
MD5:	f88e81d7f208b4e..
SHA1:	4da7041d786ebc..
SHA256:	9fd3eec622da853.
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

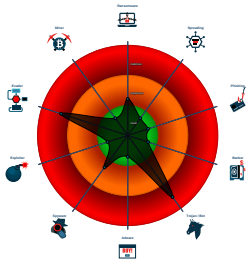


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- DES_ Holdings Ltd - products listing.exe (PID: 6520 cmdline: 'C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe' MD5: F88E81D7F208B4EBCA34AE5F1F032D0F)
  - schtasks.exe (PID: 976 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UgJYJdoaOfKgTb' /XML 'C:\Users\user\AppData\Local\Temp\tmp933B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DES_ Holdings Ltd - products listing.exe (PID: 4812 cmdline: C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe MD5: F88E81D7F208B4EBCA34AE5F1F032D0F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "C2: ": [
    "212.83.46.26"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.610060366.00000000063E0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000B.00000002.610060366.00000000063E0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000B.00000002.610060366.00000000063E0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.605354131.00000000030F1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000002.610010923.000000000634 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.DES_ Holdings Ltd - products listing.exe.6340000.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
11.2.DES_ Holdings Ltd - products listing.exe.6340000.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
11.2.DES_ Holdings Ltd - products listing.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
11.2.DES_ Holdings Ltd - products listing.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
11.2.DES_ Holdings Ltd - products listing.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 7 entries				

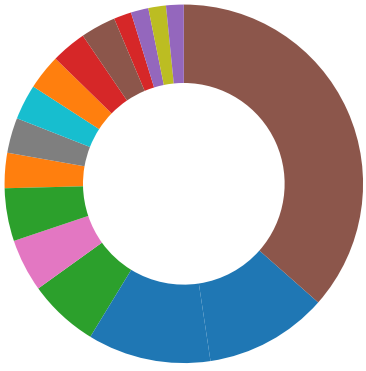
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

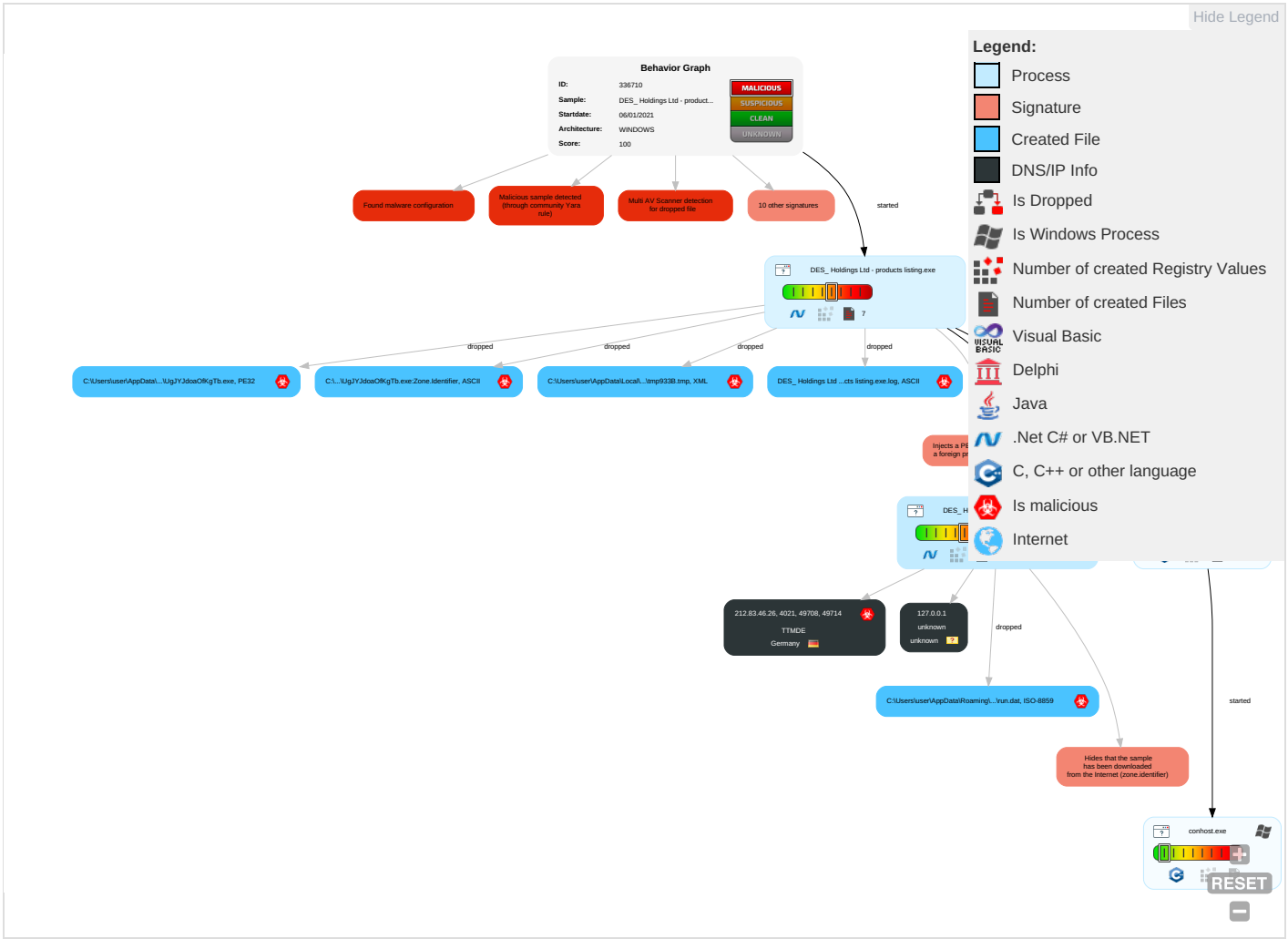
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

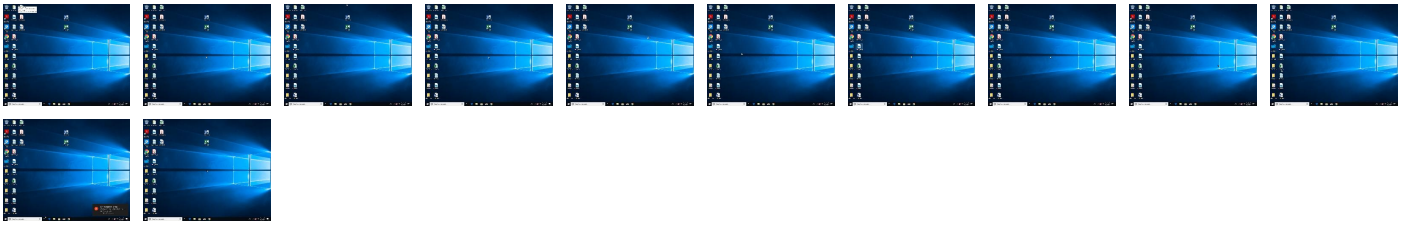
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DES_ Holdings Ltd - products listing.exe	31%	Virustotal		Browse
DES_ Holdings Ltd - products listing.exe	13%	ReversingLabs	Win32.Trojan.Wacatac	
DES_ Holdings Ltd - products listing.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UgJYJdoaOfKgTb.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\UgJYJdoaOfKgTb.exe	13%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.DES_ Holdings Ltd - products listing.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.DES_ Holdings Ltd - products listing.exe.63e0000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.83.46.26	unknown	Germany		47447	TTMDE	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336710
Start date:	06.01.2021
Start time:	17:51:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DES_ Holdings Ltd - products listing.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/5@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.4%) • Quality average: 30.8% • Quality standard deviation: 34.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • 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
17:52:58	API Interceptor	1297x Sleep call for process: DES_ Holdings Ltd - products listing.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
212.83.46.26	DES_ Holdings Ltd - products listing.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TTMDE	DES_ Holdings Ltd - products listing.exe	Get hash	malicious	Browse	• 212.83.46.26
	http://https://wearemondaymorning.com/?email=alabdullaah@qcb.gov.qa	Get hash	malicious	Browse	• 91.216.248.23
	http://https://u5827342.ct.sendgrid.net/ls/click?upn=ZYh6DIqA4xFmr84ZswpQ4c7ONXu2767hYXZwjBnWOY1JkdxAPQD-2Fy87STH2Xf5tCCv1Cfr7SK5QugA1gtf5hkg-3D-3Dr4Nw_DjWowFHgGKgaKR9KzEYTR3nC3p1AWGbaYDP6e93ZAEhNXUTlygFT7vEfeXJ-2FNinzoSEU8wjkiLZ-2Bj7exG0PiN7C92INCv5B1zQa4g83-2Ba0GFHBdwZkJ1voppTs162kZzXHlYGblxkHafYbaoPEnOE3v4nRdYqpT6uzb2BlJNElCCZ2m51yxYwgCwRvlrdJPPvzbuawtl4F-2B3DK6fR-2B-2BXI9P5zbvVuxMdWkFA2kHjw8I-3D	Get hash	malicious	Browse	• 185.88.212.176
	http://particulares-personas.casacam.net	Get hash	malicious	Browse	• 86.106.131.146
	1.12.2018.js	Get hash	malicious	Browse	• 62.113.241.182
	LAZZARO - DICHIARAZIONE NUOVO DI FABBRICA FT.610.vbs	Get hash	malicious	Browse	• 185.212.44.165
	2018-12-10-Dridex-retrieved-by-Ursnif-infected-host.exe	Get hash	malicious	Browse	• 185.158.251.55
	430#U0437.js	Get hash	malicious	Browse	• 86.105.5.133
	dropper.vbs	Get hash	malicious	Browse	• 185.212.47.162
	24Faktura-2018_10_03_PDF.exe	Get hash	malicious	Browse	• 86.105.5.133
	ttcv.exe	Get hash	malicious	Browse	• 62.113.206.33
	968.exe	Get hash	malicious	Browse	• 185.212.44.188
	bDFXsuH7Y.exe	Get hash	malicious	Browse	• 185.212.44.197
	http://demo2.aurorapro.co/Download/US_us/Invoice-for-you&data=02|01||447072d204914f25042208d6077443fb|1a407a2d76754d178692b3ac285306e4|0|0|636704593269411757&sdata=1bJ9B7e/nHSkZxTPSrTtNw1nYhl4ZkhcBHYLd4Noe44=&reserved=0	Get hash	malicious	Browse	• 62.113.194.2
	Magnoliaenergyservices_Inquiry.doc	Get hash	malicious	Browse	• 185.212.44.114
	Magnoliaenergyservices_Inquiry.doc	Get hash	malicious	Browse	• 185.212.44.114
	Don_Callahan_Statement.doc	Get hash	malicious	Browse	• 185.212.44.114
	dana.exe	Get hash	malicious	Browse	• 185.212.44.188
	Request.doc	Get hash	malicious	Browse	• 185.212.44.192
	Request.doc	Get hash	malicious	Browse	• 185.212.44.192

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DES_ Holdings Ltd - products listing.exe.log	
Process:	C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DES_ Holdings Ltd - products listing.exe.log	
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp933B.tmp	
Process:	C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1663
Entropy (8bit):	5.1803883907180115
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB2tn:cbhH7MlNQ8/rydbz9I3YODOLNdq3u
MD5:	E4794214782243EDC33DF293621136FA
SHA1:	7C776E3B82E32C04FCB5779A47A106CAFEAE92AA
SHA-256:	B5FBE1899DB293730EA34618001AEFE03ED3EE1A0503139FD16A03C2CEC619EC
SHA-512:	8B63BA348E0ECC6636475E60FFDC569A0318713A8BD9E5B1F25387C13BF0702A3F5222517818500D74238E00C05ACC726E2891C45354069A8A98C62ED5A11F42
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:NJb:Hb
MD5:	C2C6E1222E610AA323D9597E281A2D56
SHA1:	C220F2C305C40E82E42F9BC50F16272FB84E3310
SHA-256:	FAEAECD3D06E9B34911353BD30297341151A746A311795B35EC8DB1D2267D167
SHA-512:	8C6A750FF8A56055249346B73AB380E15CD7C3205C1D2C6F95BF2A25096F44FADFD848779A2743B6E20583F205D56A6D23E7DE3FFDABAD956395B9B674C2299
Malicious:	**true**
Reputation:	low
Preview:	.1.....H

C:\Users\user\AppData\Roaming\UgJYJdoaOfKgTb.exe	
Process:	C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1043968
Entropy (8bit):	7.356839656807373
Encrypted:	false
SSDEEP:	24576:SVTJysf9VhvhSCH0+W5AGl5qPim5PpmmAWB:Af31Uf5if5PXv
MD5:	F88E81D7F208B4EBCA34AE5F1F032D0F
SHA1:	4DA7041D786EBC59DFB33EEC1196C1AE2CC94F89
SHA-256:	9FD3EEC622DA8536E22C164BBD05D80DADA1003FADD07FD4800CED6C0579812C
SHA-512:	A794F4663C05A52321938EFFD29BFFF27214F400F3F838C94210D63729EE506C453C230DF0D2BDC57814EFF398049D865AE893980D9BDB070D0B608D9282FD62
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low

C:\Users\user\AppData\Roaming\UgJYJdoaOfKgTb.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e._.....P.....8..... .....@.. .....@..... ..@.....W.....6..... ....H.....text...$.... ....`.rsrc....6.....6.....@..@.reloc..... .....@..B.....H.....@.....I.....0..#.....+.&...(....(.....(.....o....*.....0.....+.&..8.....8....+5..ia.+...`a...kYE..... .....M.....+.....&...+.....+...eYE.....)...7...?...H...b...w.....+.+....+...(.....8y.....(.....8j.....(.....8\.....8T.....8K.....(....+.(....85....81.....&+..8.....8.....8....*...0.....+ .&...+C..ja.+..._a8.....jX+T.e(.....+...fYE.....O...e..

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.356839656807373
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:	DES_ Holdings Ltd - products listing.exe
File size:	1043968
MD5:	f88e81d7f208b4ebca34ae5f1f032d0f
SHA1:	4da7041d786ebc59dfb33eec1196c1ae2cc94f89
SHA256:	9fd3eec622da8536e22c164bbd05d80dada1003fadd07fd4800ced6c0579812c
SHA512:	a794f4663c05a52321938effd29bfff27214f400f3f838c94210d63729ee506c453c230df0d2bdc57814eff398049d865ae893980d9bdb070d0b608d9282fd62
SSDEEP:	24576:SVTJysf9VhvhSCH0+W5AGl5qPim5PpmmAWB:Af31Uf5if5PXv
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e._.....P.....8..... .....@.. .....@..... .....@.....

File Icon

Icon Hash:	00a275154a880000

Static PE Info

General

Entrypoint:	0x4ed31e
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FF565C2 [Wed Jan 6 07:24:50 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xed2c4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xee000	0x13600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x102000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xeb324	0xeb400	False	0.697449314227	data	7.45520893226	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xee000	0x13600	0x13600	False	0.208543346774	data	4.32755744619	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x102000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xee160	0x10828	data		
RT_ICON	0xfe988	0x25b5	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x100f40	0x22	data		
RT_VERSION	0x100f64	0x346	data		
RT_MANIFEST	0x1012ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Saga 2019 (C)
Assembly Version	4.0.31.4
InternalName	IClientChannelSink.exe
FileVersion	4.0.31.4
CompanyName	
LegalTrademarks	
Comments	
ProductName	PANCHAYAT
ProductVersion	4.0.31.4
FileDescription	PANCHAYAT
OriginalFilename	IClientChannelSink.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 17:53:10.111084938 CET	49708	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:10.151746035 CET	4021	49708	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:10.699081898 CET	49708	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:10.739984035 CET	4021	49708	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:11.409092903 CET	49708	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:11.449992895 CET	4021	49708	212.83.46.26	192.168.2.7

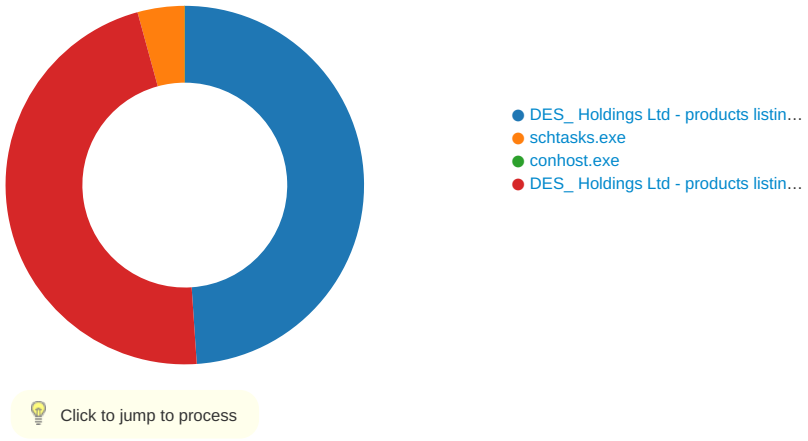
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 17:53:15.481971025 CET	49714	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:15.522370100 CET	4021	49714	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:16.074491978 CET	49714	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:16.115080118 CET	4021	49714	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:16.665894032 CET	49714	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:16.707134008 CET	4021	49714	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:20.717137098 CET	49719	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:20.757800102 CET	4021	49719	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:21.262439966 CET	49719	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:21.303704977 CET	4021	49719	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:21.809355021 CET	49719	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:21.849813938 CET	4021	49719	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:41.284243107 CET	49753	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:41.325028896 CET	4021	49753	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:41.826730967 CET	49753	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:41.867628098 CET	4021	49753	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:42.373560905 CET	49753	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:42.414251089 CET	4021	49753	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:46.454283953 CET	49755	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:49.467911005 CET	49755	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:49.508497953 CET	4021	49755	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:50.014904976 CET	49755	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:50.055160046 CET	4021	49755	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:54.063577890 CET	49756	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:54.104882002 CET	4021	49756	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:54.609143019 CET	49756	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:54.649852991 CET	4021	49756	212.83.46.26	192.168.2.7
Jan 6, 2021 17:53:55.155965090 CET	49756	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:53:55.196655035 CET	4021	49756	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:14.578449965 CET	49762	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:14.618778944 CET	4021	49762	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:15.141961098 CET	49762	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:15.182620049 CET	4021	49762	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:15.688868999 CET	49762	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:15.729763985 CET	4021	49762	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:19.800349951 CET	49763	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:19.841017008 CET	4021	49763	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:20.345871925 CET	49763	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:20.386894941 CET	4021	49763	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:20.909408092 CET	49763	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:20.950213909 CET	4021	49763	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:24.964709997 CET	49764	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:25.005273104 CET	4021	49764	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:25.517765999 CET	49764	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:25.558191061 CET	4021	49764	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:26.064696074 CET	49764	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:26.105319977 CET	4021	49764	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:45.255342007 CET	49768	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:45.296133995 CET	4021	49768	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:45.800730944 CET	49768	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:45.841567039 CET	4021	49768	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:46.347635984 CET	49768	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:46.388117075 CET	4021	49768	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:50.399077892 CET	49769	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:50.440547943 CET	4021	49769	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:50.941751957 CET	49769	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:50.982470989 CET	4021	49769	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:51.488678932 CET	49769	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:51.531482935 CET	4021	49769	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:55.537494898 CET	49770	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:55.578629017 CET	4021	49770	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:56.082842112 CET	49770	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:54:56.123642921 CET	4021	49770	212.83.46.26	192.168.2.7
Jan 6, 2021 17:54:56.629757881 CET	49770	4021	192.168.2.7	212.83.46.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 17:54:56.670499086 CET	4021	49770	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:15.890100956 CET	49774	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:15.930814981 CET	4021	49774	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:16.445079088 CET	49774	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:16.485426903 CET	4021	49774	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:16.992007971 CET	49774	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:17.032809973 CET	4021	49774	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:21.040476084 CET	49775	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:21.081031084 CET	4021	49775	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:21.586123943 CET	49775	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:21.626566887 CET	4021	49775	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:22.132986069 CET	49775	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:22.173580885 CET	4021	49775	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:26.183592081 CET	49776	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:26.224164009 CET	4021	49776	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:26.727159977 CET	49776	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:26.768723011 CET	4021	49776	212.83.46.26	192.168.2.7
Jan 6, 2021 17:55:27.274094105 CET	49776	4021	192.168.2.7	212.83.46.26
Jan 6, 2021 17:55:27.315253019 CET	4021	49776	212.83.46.26	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DES_ Holdings Ltd - products listing.exe PID: 6520 Parent PID: 5692

General

Start time:	17:52:37
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe'
Imagebase:	0x870000
File size:	1043968 bytes
MD5 hash:	F88E81D7F208B4EBCA34AE5F1F032D0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6D17CF06	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	6D17CF06	unknown
C:\Users\user\AppData\Roaming\UgJYJdoaOfKgTb.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	6C0CDD66	CopyFileW
C:\Users\user\AppData\Roaming\UgJYJdoaOfKgTb.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C0CDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp933B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C0C7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DES_ Holdings Ltd - products listing.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp933B.tmp	success or wait	1	6C0C6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UgJYJdoaOfKgTb.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c2 65 f5 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 b4 0e 00 00 38 01 00 00 00 00 00 1e d3 0e 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 10 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....e._.......... ....P......8........... ....@.. ....@ ....@................	success or wait	4	6C0CDD66	CopyFileW
C:\Users\user\AppData\Roaming\ UgJYJdoaOfKgTb.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C0CDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp933B.tmp	unknown	1663	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registrati	success or wait	1	6C0C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DES_ Holdings Ltd - products listing.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D48C907	WriteFile

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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0C1B4F	ReadFile

Analysis Process: schtasks.exe PID: 976 Parent PID: 6520

General

Start time:	17:53:04
Start date:	06/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UgJYJdoaOfKgTb' /XML 'C:\Users\user\AppData\Local\Temp\tmp933B.tmp'
Imagebase:	0xa20000
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

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\tmp933B.tmp	unknown	2	success or wait	1	A2AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp933B.tmp	unknown	1664	success or wait	1	A2ABD9	ReadFile

Analysis Process: conhost.exe PID: 4472 Parent PID: 976

General

Start time:	17:53:05
Start date:	06/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: DES_ Holdings Ltd - products listing.exe PID: 4812 Parent PID: 6520

General

Start time:	17:53:05
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe
Imagebase:	0xc40000
File size:	1043968 bytes
MD5 hash:	F88E81D7F208B4EBCA34AE5F1F032D0F
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: 0000000B.00000002.610060366.00000000063E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.610060366.00000000063E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.610060366.00000000063E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.605354131.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.610010923.0000000006340000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.610010923.0000000006340000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.602980109.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.602980109.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.602980109.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.608557876.0000000004139000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.608557876.0000000004139000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6D17CF06	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	6D17CF06	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	6C0CBEFF	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	6C0C1E60	CreateFileW
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	6C0CBEFF	CreateDirectoryW
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	6C0CBEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe:Zone.Identifier	success or wait	1	6C042935	unknown

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	unknown	8	f1 31 a3 fb ae b2 d8 48	.1.....H	success or wait	1	6C0C1B4F	WriteFile

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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0C1B4F	ReadFile
C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe	unknown	4096	success or wait	1	6D13D72F	unknown
C:\Users\user\Desktop\DES_ Holdings Ltd - products listing.exe	unknown	512	success or wait	1	6D13D72F	unknown

Disassembly

Code Analysis