ID: 412574
Sample Name: PURCHASE ORDER.exe
Cookbook: default.jbs
Time: 19:32:50
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

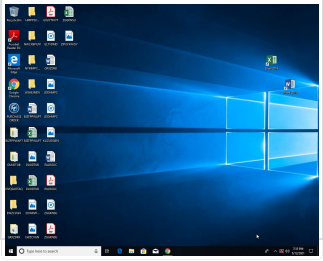
Analysis Report PURCHASE ORDER.exe

Overview

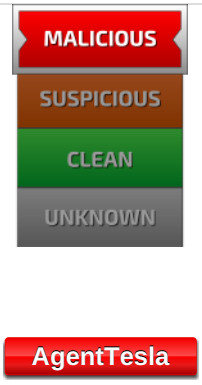
General Information

Sample Name:	PURCHASE ORDER.exe
Analysis ID:	412574
MD5:	3dbed8889c9e07..
SHA1:	55e331a1169b7f8.
SHA256:	a10213876dda12..
Infos:	

Most interesting Screenshot:



Detection



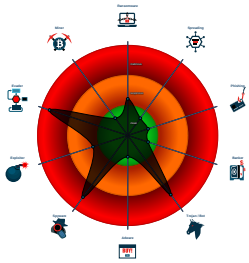
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- PURCHASE ORDER.exe (PID: 5388 cmdline: 'C:\Users\user\Desktop\PURCHASE ORDER.exe' MD5: 3DBED8889C9E0709D9D5B9DF08D5EABF)
  - schtasks.exe (PID: 396 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GNBVBDzQwHiY' /XML 'C:\Users\user\AppData\Local\Temp\tmpA9B9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PURCHASE ORDER.exe (PID: 6156 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: 3DBED8889C9E0709D9D5B9DF08D5EABF)
  - PURCHASE ORDER.exe (PID: 6172 cmdline: C:\Users\user\Desktop\PURCHASE ORDER.exe MD5: 3DBED8889C9E0709D9D5B9DF08D5EABF)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "ghulam.sarwar@dadabhoy.edu.pkDadabhoy.456mail.dadabhoy.edu.pkmarsspace454@yandex.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.238977520.000000000319B000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.503023451.000000000354 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.503023451.000000000354 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.239232235.000000000417 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.239232235.000000000417 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

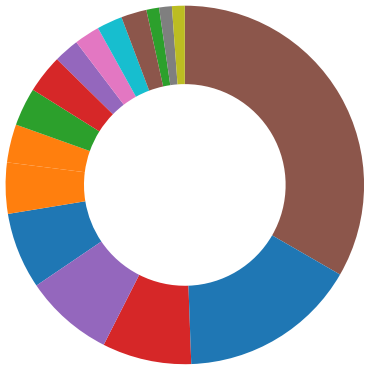
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.PURCHASE ORDER.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.PURCHASE ORDER.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PURCHASE ORDER.exe.428e9e8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PURCHASE ORDER.exe.428e9e8.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PURCHASE ORDER.exe.428e9e8.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Machine Learning detection for dropped file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Yara detected AgentTesla

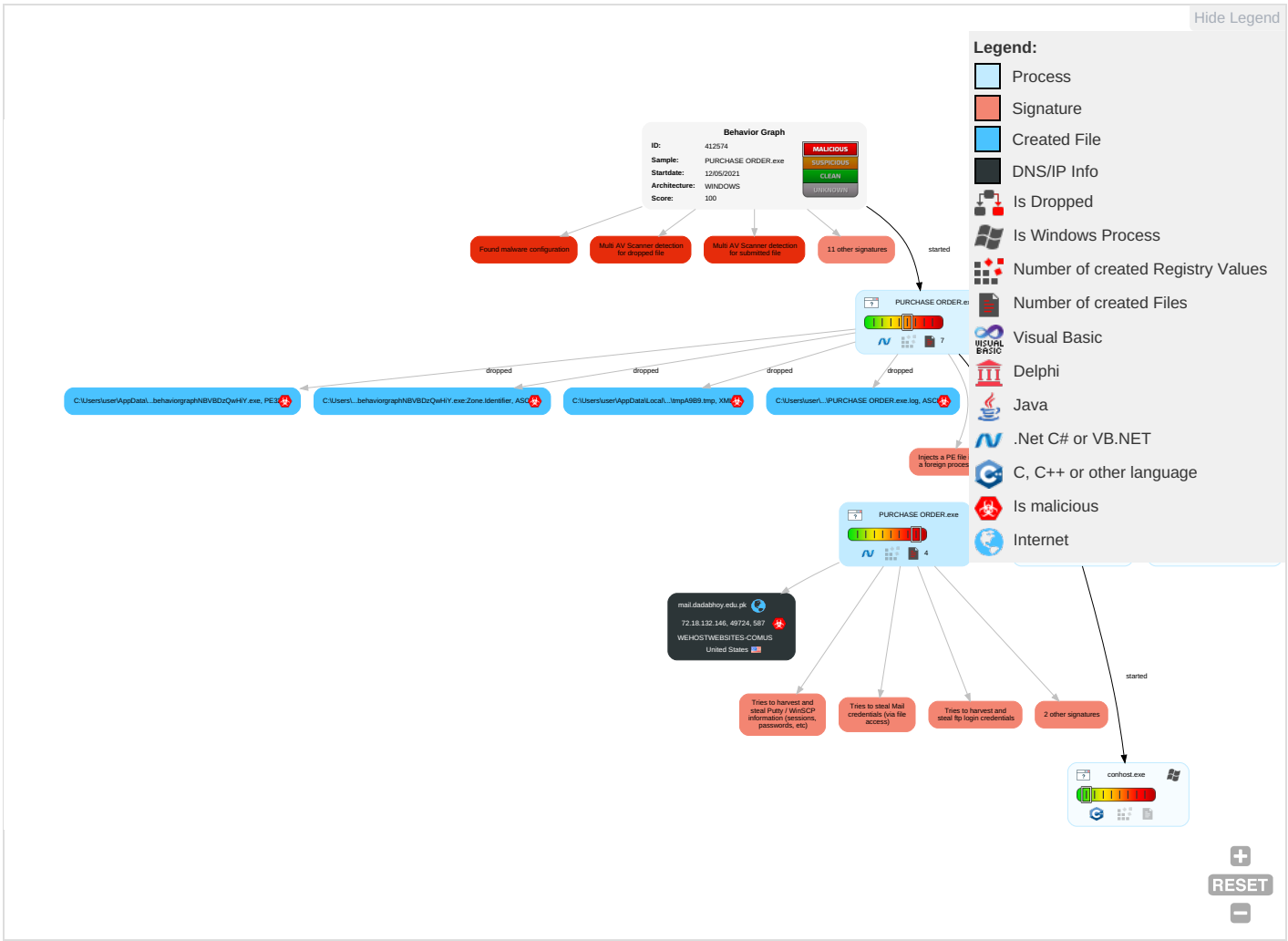
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Obfuscated Files or Information 3	Input Capture 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 3	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4 1	LSA Secrets	Security Software Discovery 3 2 1	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Virtualization/Sandbox Evasion 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol

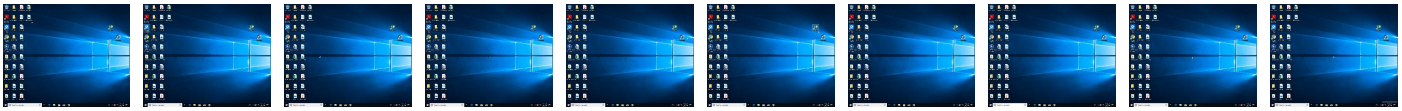
Behavior Graph

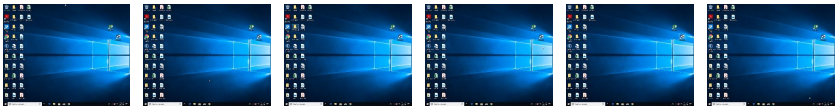


Screenshots

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
PURCHASE ORDER.exe	22%	Virustotal		Browse
PURCHASE ORDER.exe	28%	ReversingLabs	Win32.Trojan.Wacatac	
PURCHASE ORDER.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\GNBVBDzQwHiY.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\GNBVBDzQwHiY.exe	28%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.PURCHASE ORDER.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://UZkOts.com	0%	Avira URL Cloud	safe	
http://https://kMicsa3HazLTjD.net	0%	Avira URL Cloud	safe	

Domains and IPs

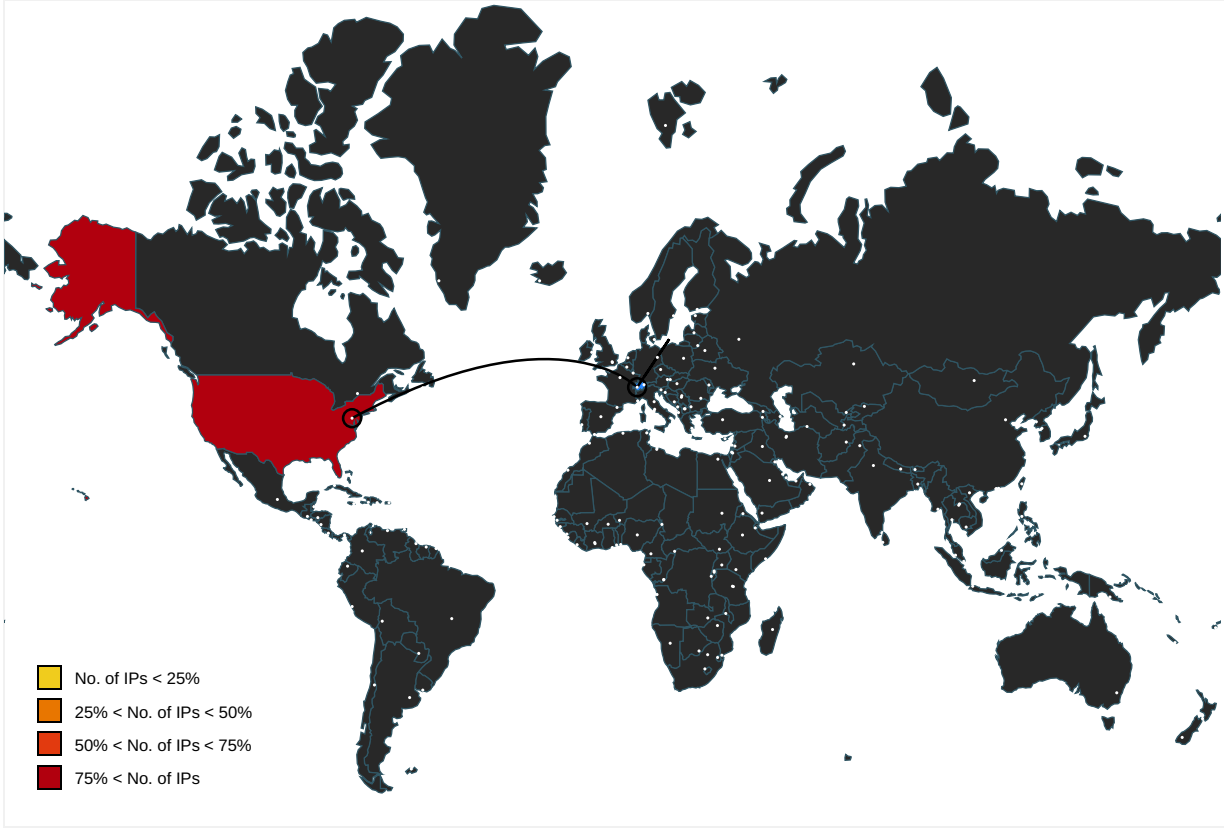
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.dadabhoy.edu.pk	72.18.132.146	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	PURCHASE ORDER.exe, 00000004.00000002.503023451.000000003541000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	PURCHASE ORDER.exe, 00000004.00000002.503023451.000000003541000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	PURCHASE ORDER.exe, 00000004.00000002.503023451.000000003541000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	PURCHASE ORDER.exe, 00000004.00000002.503023451.000000003541000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%	PURCHASE ORDER.exe, 00000004.00000002.503023451.000000003541000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PURCHASE ORDER.exe, 00000000.00000002.239232235.000000004171000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000004.00000002.498714437.000000000040200.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	PURCHASE ORDER.exe, 00000000.00000002.238977520.000000003197B000.00000004.00000001.sdmp	false		high
http://UZkOts.com	PURCHASE ORDER.exe, 00000004.00000002.503023451.000000003541000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kMicsa3HazLTjD.net	PURCHASE ORDER.exe, 00000004.00000002.503023451.000000003541000.00000004.00000001.sdmp, PURCHASE ORDER.exe, 00000004.00000002.503328534.000000000358900.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
72.18.132.146	mail.dadabhoy.edu.pk	United States		30475	WEHOSTWEBSITES-COMUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412574
Start date:	12.05.2021
Start time:	19:32:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PURCHASE ORDER.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:	29
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.spyw.evad.winEXE@8/4@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 46% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 96% • 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 • Excluded IPs from analysis (whitelisted): 93.184.220.29, 13.88.21.125, 20.82.210.154, 204.79.197.200, 13.107.21.200, 104.43.139.144, 92.122.145.220, 184.30.24.56, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • 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
19:33:42	API Interceptor	967x Sleep call for process: PURCHASE ORDER.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
72.18.132.146	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	Proforma Invoice.exe	Get hash	malicious	Browse	
	INVOICE34 56730015.exe	Get hash	malicious	Browse	
	PAYMENT COPY.exe	Get hash	malicious	Browse	
	AD1-2001028L.exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	Balance Payment.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.dadabhoy.edu.pk	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 72.18.132.146
	Proforma Invoice.exe	Get hash	malicious	Browse	• 72.18.132.146
	INVOICE34 56730015.exe	Get hash	malicious	Browse	• 72.18.132.146
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 72.18.132.146
	AD1-2001028L.exe	Get hash	malicious	Browse	• 72.18.132.146
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 72.18.132.146
	Balance Payment.exe	Get hash	malicious	Browse	• 72.18.132.146

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEHOSTWEBSITES-COMUS	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 72.18.132.146
	Proforma Invoice.exe	Get hash	malicious	Browse	• 72.18.132.146
	INVOICE34 56730015.exe	Get hash	malicious	Browse	• 72.18.132.146
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 72.18.132.146
	AD1-2001028L.exe	Get hash	malicious	Browse	• 72.18.132.146
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 72.18.132.146
	Balance Payment.exe	Get hash	malicious	Browse	• 72.18.132.146
	64.exe	Get hash	malicious	Browse	• 23.239.203.21
	Inquiry Ref DW200929-ED1.xls	Get hash	malicious	Browse	• 72.18.132.34
	VZs73znCvb.exe	Get hash	malicious	Browse	• 72.18.130.163

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\PURCHASE ORDER.exe.log	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpA9B9.tmp	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1649
Entropy (8bit):	5.189172014947723
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBtKtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3Q

C:\Users\user\AppData\Local\Temp\tmpA9B9.tmp	
MD5:	94359E9274617C25D530B2DDB63D4F90
SHA1:	6789225F844A5ECE7DDB2919F6012B4581A2448F
SHA-256:	699084A187BA33274C7CA9B84FDBABACD5BB4C3E2DDF7EB5CA2C2DC58BA12AF6
SHA-512:	B1581F1C911A6D041C5F339B5B61883637C5455846C227BCDFF2817561A9DD3FAF088E25AC8F6F8256B3F26E7704C6098A75C62FAC26FC3599617C47501E493D
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>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\GNBVBDzQwHiY.exe	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	710656
Entropy (8bit):	7.595096185086584
Encrypted:	false
SSDEEP:	12288:H6FPcIlQykx1zO9U/CyVbC4dhmYLk5wFMt01Aqb8MvOfA42MmGVH:H6FPSx1iSXFnOz+8MGN2MVH
MD5:	3DBED8889C9E0709D9D5B9DF08D5EABF
SHA1:	55E331A1169B7F8773C0A2332E85C73322477831
SHA-256:	A10213876DDA124A602A41A9B947E66ED8AD7E330B76596BDB0AB00B435AADED
SHA-512:	BFFE152DE01F9E3F73CF78AE3D38D9E6BE7FD4E924D7A629E921BF6D5466C4DF4605317E86A958669C33D67958D10366D37B1E91BE681BBE9E10A64C5CC514F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X.`.....P.....T.....v.... .....@.. .....@.....@.....$...O.....0Q..... ..... ..H.....text...|.... ..... ..`.rsrc...0Q.....R.....@..@.relo c..... .....@..B.....X.....H.....P.....0.....(....(.....(....o!....*.....("......(#.....($.....(%.....(&....*N..(....oS... ('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0..<.....~.....(3 .....,!r...p.....(4...o5...s6.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\GNBVBDzQwHiY.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PURCHASE ORDER.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):	7.595096185086584

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PURCHASE ORDER.exe
File size:	710656
MD5:	3dbed8889c9e0709d9d5b9df08d5eabf
SHA1:	55e331a1169b7f8773c0a2332e85c73322477831
SHA256:	a10213876dda124a602a41a9b947e66ed8ad7e330b765 6bdb0ab00b435aaded
SHA512:	bffe152de01f9e3f73cf78ae3d38d9e6be7fd4e924d7a629 e921bf6d5466c4df4605317e86a958669c33d67958d1036 6d37b1e91be681bbe9e10a64c5cc5146f
SSDEEP:	12288:H6FPcIlQykx1zO9U/CyVbC4dhmYLk5wFMt01A qb8MvOfA42MmGVH:H6FPSx1iSXFnOz+8MGN2MVH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X..`.....P.....T.....v.... .....@.. .....@.....@.....

File Icon

Icon Hash:	60d088f59092cc31

Static PE Info

General

Entrypoint:	0x4aa176
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609BD458 [Wed May 12 13:12:56 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xaa124	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x5130	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa817c	0xa8200	False	0.797387604554	data	7.6332778418	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x5130	0x5200	False	0.512623856707	data	5.60122084223	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	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	0xac130	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xb0358	0x14	data		
RT_VERSION	0xb036c	0x394	data		
RT_MANIFEST	0xb0700	0xa2e	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

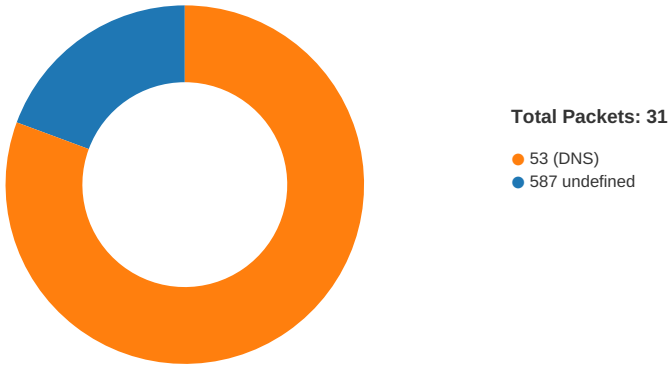
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	DefaultInterfaceAttribute.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	LibraryManagementSystem
ProductVersion	1.0.0.0
FileDescription	LibraryManagementSystem
OriginalFilename	DefaultInterfaceAttribute.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:35:15.835755110 CEST	49724	587	192.168.2.5	72.18.132.146
May 12, 2021 19:35:16.014936924 CEST	587	49724	72.18.132.146	192.168.2.5
May 12, 2021 19:35:16.015052080 CEST	49724	587	192.168.2.5	72.18.132.146
May 12, 2021 19:35:16.172660112 CEST	49724	587	192.168.2.5	72.18.132.146
May 12, 2021 19:35:16.349592924 CEST	587	49724	72.18.132.146	192.168.2.5
May 12, 2021 19:35:16.523308992 CEST	587	49724	72.18.132.146	192.168.2.5
May 12, 2021 19:35:16.523338079 CEST	587	49724	72.18.132.146	192.168.2.5
May 12, 2021 19:35:16.523467064 CEST	587	49724	72.18.132.146	192.168.2.5
May 12, 2021 19:35:16.523495913 CEST	49724	587	192.168.2.5	72.18.132.146
May 12, 2021 19:35:16.523531914 CEST	49724	587	192.168.2.5	72.18.132.146
May 12, 2021 19:35:16.523607016 CEST	49724	587	192.168.2.5	72.18.132.146

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:33:34.903877974 CEST	54302	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:34.925451994 CEST	53784	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:34.955418110 CEST	53	54302	8.8.8.8	192.168.2.5
May 12, 2021 19:33:34.975557089 CEST	53	53784	8.8.8.8	192.168.2.5
May 12, 2021 19:33:35.719926119 CEST	65307	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:35.785490036 CEST	53	65307	8.8.8.8	192.168.2.5
May 12, 2021 19:33:36.048047066 CEST	64344	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:33:36.109672070 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 19:33:36.127527952 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:36.184672117 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 19:33:37.381658077 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:37.430454016 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 19:33:38.515108109 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:38.564013958 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 19:33:39.410775900 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:39.459733963 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 19:33:39.747169018 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:39.808377028 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 19:33:40.701724052 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:40.751944065 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 19:33:41.648571968 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:41.705708027 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 19:33:42.796734095 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:42.846669912 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 19:33:45.245131969 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:45.295453072 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 19:33:46.190026999 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:46.241955996 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 19:33:47.349349976 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:47.398499012 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 19:33:48.449527025 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:48.501425028 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 19:33:58.780842066 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 19:33:58.856266975 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 19:34:11.457942963 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 19:34:11.517812014 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 19:34:18.638611078 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 19:34:18.699443102 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 19:34:46.341012001 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 19:34:46.409173965 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 19:34:54.637468100 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 19:34:54.699223042 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 19:35:09.309345961 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 19:35:09.367100954 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 19:35:15.743837118 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 19:35:15.807564020 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 19:35:20.972039938 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 19:35:21.039608955 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 19:35:25.249305010 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 19:35:25.321475983 CEST	53	54791	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 19:35:15.743837118 CEST	192.168.2.5	8.8.8.8	0x96ac	Standard query (0)	mail.dadabhoy.edu.pk	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:35:15.807564020 CEST	8.8.8.8	192.168.2.5	0x96ac	No error (0)	mail.dadabhoy.edu.pk		72.18.132.146	A (IP address)	IN (0x0001)

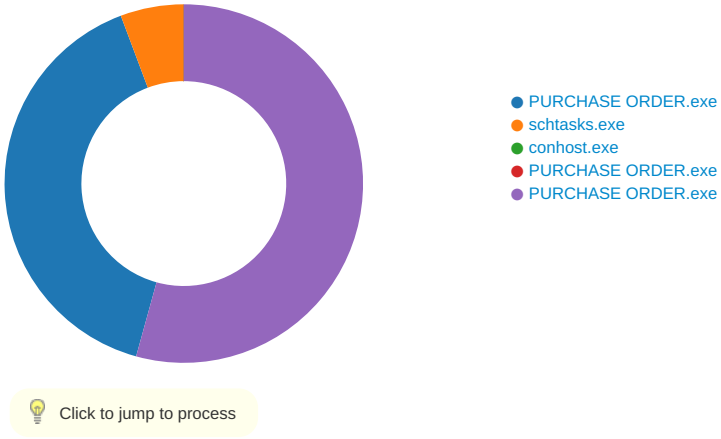
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 19:35:16.523308992 CEST	587	49724	72.18.132.146	192.168.2.5	220-vps.dadabhoy.edu.pk ESMTP Exim 4.94.2 #2 Thu, 13 May 2021 01:35:16 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 19:35:16.523338079 CEST	587	49724	72.18.132.146	192.168.2.5	421 vps.dadabhoy.edu.pk lost input connection

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PURCHASE ORDER.exe PID: 5388 Parent PID: 5580

General

Start time:	19:33:42
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PURCHASE ORDER.exe'
Imagebase:	0xab0000
File size:	710656 bytes
MD5 hash:	3DBED8889C9E0709D9D5B9DF08D5EABF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.238977520.000000000319B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.239232235.0000000004171000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.239232235.0000000004171000.00000004.00000001.sdmp, Author: Joe Security
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	72B860AC	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	72B860AC	unknown
C:\Users\user\AppData\Roaming\GNBVBDzQwHiY.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	125BF98	CopyFileW
C:\Users\user\AppData\Roaming\GNBVBDzQwHiY.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	125BF98	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA9B9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	51707F8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\PURCHASE ORDER.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA9B9.tmp	success or wait	1	5170DCA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\GNBVBDzQwHiY.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 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 58 d4 9b 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 82 0a 00 00 54 00 00 00 00 00 00 76 a1 0a 00 00 20 00 00 00 c0 0a 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 0b 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...X..`.......... ....P......T......v.... ....@.. ....@ ....@.................	success or wait	3	125BF98	CopyFileW
C:\Users\user\AppData\Roaming\GNBVBDzQwHiY.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	125BF98	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA9B9.tmp	unknown	1649	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 61 6c 66 6f 6e 73 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 6f 6e 49	<?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>.. </RegistrationI	success or wait	1	5170A87	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\PURCHASE ORDER.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: schtasks.exe PID: 396 Parent PID: 5388

General

Start time:	19:33:44
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GNBVBDzQwHiY' /XML 'C:\Users\user\AppData\Local\Temp\tmpA9B9.tmp'
Imagebase:	0x10c0000
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\tmpA9B9.tmp	unknown	2	success or wait	1	10CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA9B9.tmp	unknown	1650	success or wait	1	10CABD9	ReadFile

Analysis Process: conhost.exe PID: 3880 Parent PID: 396

General

Start time:	19:33:44
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: PURCHASE ORDER.exe PID: 6156 Parent PID: 5388

General

Start time:	19:33:45
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Imagebase:	0x390000
File size:	710656 bytes
MD5 hash:	3DBED8889C9E0709D9D5B9DF08D5EABF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: PURCHASE ORDER.exe PID: 6172 Parent PID: 5388

General

Start time:	19:33:45
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER.exe
Imagebase:	0xd80000
File size:	710656 bytes
MD5 hash:	3DBED8889C9E0709D9D5B9DF08D5EABF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.503023451.0000000003541000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.503023451.0000000003541000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.498714437.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.498714437.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
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	72B860AC	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	72B860AC	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	72B860AC	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	72B860AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5ED113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5ED113B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	5ED113B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\7242182d-e195-44e9-ada2-f6d882c49d8a	unknown	4096	success or wait	1	5ED113B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	5ED113B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5ED113B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5ED113B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5ED113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5ED113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5ED113B	ReadFile

Disassembly

Code Analysis