ID: 433269
Sample Name: NEW URGENT ENQUIRY.exe
Cookbook: default.jbs
Time: 15:02:22
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

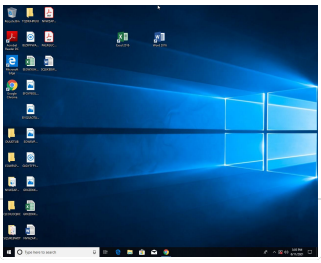
Analysis Report NEW URGENT ENQUIRY.exe

Overview

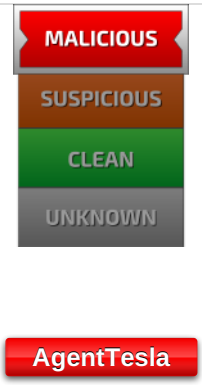
General Information

Sample Name:	NEW URGENT ENQUIRY.exe
Analysis ID:	433269
MD5:	151ec82864cc85…
SHA1:	b93f14d8b0eb8e0.
SHA256:	1d5221667b8424..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

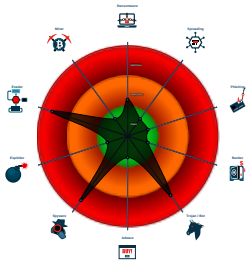


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- 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 register a lo…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Moves itself to temp directory

Classification



Process Tree

- **System is w10x64**
- NEW URGENT ENQUIRY.exe (PID: 6068 cmdline: 'C:\Users\user\Desktop\NEW URGENT ENQUIRY.exe' MD5: 151EC82864CC859F03BE0CB572F30357)
  - NEW URGENT ENQUIRY.exe (PID: 996 cmdline: C:\Users\user\Desktop\NEW URGENT ENQUIRY.exe MD5: 151EC82864CC859F03BE0CB572F30357)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "staffs@globaloffs-site.com",
  "Password": "yLxCDRZ2",
  "Host": "smtp.globaloffs-site.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.480352639.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.480352639.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000002.00000002.485743997.0000000002C11000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000002.00000000.248827227.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000000.248827227.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Copyright Joe Security LLC 2021

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.NEW URGENT ENQUIRY.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.NEW URGENT ENQUIRY.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
2.0.NEW URGENT ENQUIRY.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.0.NEW URGENT ENQUIRY.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.NEW URGENT ENQUIRY.exe.3e911b0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

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

Initial sample is a PE file and has a suspicious name

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)

Copyright Joe Security LLC 2021

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

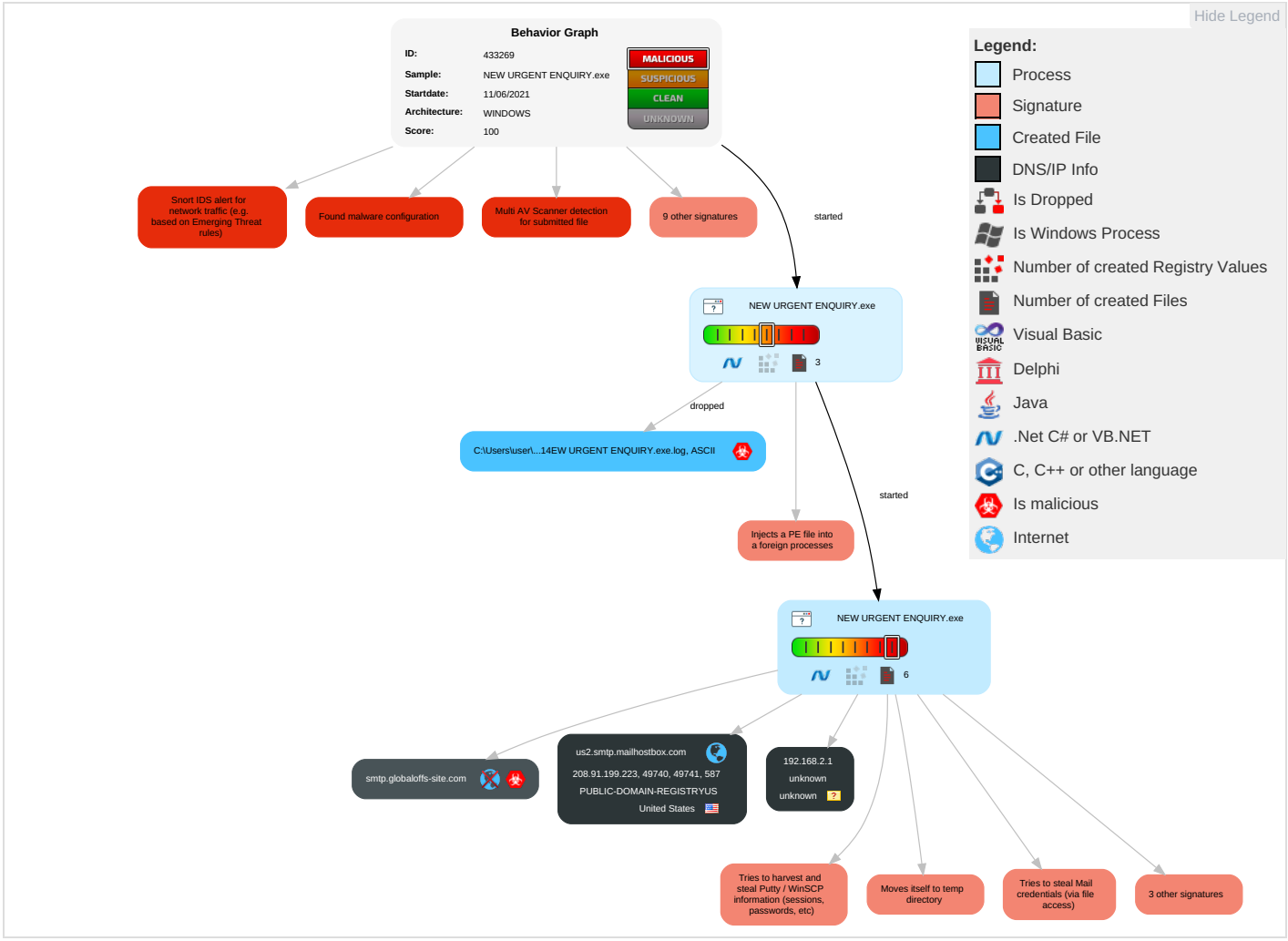
Yara detected AgentTesla

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	Masquerading 1 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standa Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Credentials in Registry 1	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Behavior Graph

Copyright Joe Security LLC 2021



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
NEW URGENT ENQUIRY.exe	17%	Virustotal		Browse
NEW URGENT ENQUIRY.exe	15%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.NEW URGENT ENQUIRY.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
2.2.NEW URGENT ENQUIRY.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
smtp.globaloffs-site.com	1%	Virustotal		Browse

URLs

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnO	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://wEpeG8K7Dd1RoPgNaN.net	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comC	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.como.y	0%	Avira URL Cloud	safe	
http://www.fontbureau.comepkove	0%	Avira URL Cloud	safe	
http://www.sakkal.comx	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.founder.com.cn/cnC	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.sajatypeworks.comQ	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.goodfont.co.krk	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://NDGIhc.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	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://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	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://www.tiro.compe	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cna	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnobtGd	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comlvfet	0%	URL Reputation	safe	
http://www.fontbureau.comlvfet	0%	URL Reputation	safe	
http://www.fontbureau.comlvfet	0%	URL Reputation	safe	
http://smtp.globaloffs-site.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
smtp.globaloffs-site.com	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433269
Start date:	11.06.2021
Start time:	15:02:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW URGENT ENQUIRY.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:	23
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@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 45.2% • Quality standard deviation: 37%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:03:19	API Interceptor	790x Sleep call for process: NEW URGENT ENQUIRY.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	KC8ZMn81JC.exe	Get hash	malicious	Browse	
	Factura PO 1541973.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	
	order 4806125050.xlsx	Get hash	malicious	Browse	
	BP4w3lADAPfOKml.exe	Get hash	malicious	Browse	
	PO -TXGU5022187.xlsx	Get hash	malicious	Browse	
	FXDmHliz25.exe	Get hash	malicious	Browse	
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	
	003BC09180600189.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Scr.Malcodegdn30.30554.exe	Get hash	malicious	Browse	
	MOQ FOB ORDER_____.exe	Get hash	malicious	Browse	
	YR1eBxhF96.exe	Get hash	malicious	Browse	
	Quote SEQTE00311701.xlsx	Get hash	malicious	Browse	
	sqQyO37l3c.exe	Get hash	malicious	Browse	
	Urgent RFQ_AP65425652_032421,pdf.exe	Get hash	malicious	Browse	
	INVOICE FOR PAYMENT_pdf_____ _____.exe	Get hash	malicious	Browse	
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	Recibo de banco.exe	Get hash	malicious	Browse	• 208.91.198.143
	KC8ZMn81JC.exe	Get hash	malicious	Browse	• 208.91.199.224
	Factura PO 1541973.exe	Get hash	malicious	Browse	• 208.91.199.223
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	• 208.91.199.224
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	• 208.91.199.223
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225
	JK6Ul6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	• 208.91.198.143
	order 4806125050.xlsx	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Trojan.PackedNET.831.28325.exe	Get hash	malicious	Browse	• 208.91.199.225
	G8mumaTxk5kFdBG.exe	Get hash	malicious	Browse	• 208.91.198.143
	Trial order 20210609.exe	Get hash	malicious	Browse	• 208.91.199.224
	BP4w3lADAPfOKml.exe	Get hash	malicious	Browse	• 208.91.199.223
	4It7P3KCyYHUWHU.exe	Get hash	malicious	Browse	• 208.91.199.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Recibo de banco.exe	Get hash	malicious	Browse	• 208.91.198.143
	KC8ZMn81JC.exe	Get hash	malicious	Browse	• 208.91.199.224
	audit-1133808478.xlsb	Get hash	malicious	Browse	• 43.225.55.182
	Factura PO 1541973.exe	Get hash	malicious	Browse	• 208.91.199.223
	Urgent Contract Order GH7856648,pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	NEW ORDER 112888#.exe	Get hash	malicious	Browse	• 208.91.199.224
	oRSxZhDFLi.exe	Get hash	malicious	Browse	• 208.91.199.225
	SAUDI ARAMCO Tender Documents - BOQ and ITB.exe	Get hash	malicious	Browse	• 208.91.199.223
	0PyeqVfoHGFVl2r.exe	Get hash	malicious	Browse	• 208.91.199.223
	#U260e#Ufe0f Zeppelin.com AudioMessage_259-55.HTM	Get hash	malicious	Browse	• 207.174.212.247
	SecuriteInfo.com.MachineLearning.Anomalous.97.15449.exe	Get hash	malicious	Browse	• 208.91.198.143
	lFccIK78FD.exe	Get hash	malicious	Browse	• 208.91.198.143
	Order10 06 2021.doc	Get hash	malicious	Browse	• 162.215.241.145
	PO187439.exe	Get hash	malicious	Browse	• 119.18.54.126
	Urgent Contract Order GH78566484,pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	MOQ FOB ORDER.exe	Get hash	malicious	Browse	• 208.91.199.225

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JK6UI6IKioPWJ6Y.exe	Get hash	malicious	Browse	• 208.91.198.143
	ekrrUChjXvng9Vr.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.832.15445.exe	Get hash	malicious	Browse	• 208.91.198.143
	order 4806125050.xlsx	Get hash	malicious	Browse	• 208.91.199.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW URGENT ENQUIRY.exe.log	
Process:	C:\Users\user\Desktop\NEW URGENT ENQUIRY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEg:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHV
MD5:	394E646B019FF472CE37EE76A647A27F
SHA1:	BD5872D88EE9CD2299B5F0E462C53D9E7040D6DA
SHA-256:	2295A0B1F6ACD75FB5D038ADE65725EDF3DDF076107AEA93E4A864E35974AE2A
SHA-512:	7E95510C85262998AECC9A06A73A5BF6352304AF6EE143EC7E48A17473773F33A96A2F4146446444789B8BCC9B83372A227DC89C3D326A2E142BCA1E1A9B4809
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\3d4kzwat.thm\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\NEW URGENT ENQUIRY.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, 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):	7.306874188608789
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	NEW URGENT ENQUIRY.exe
File size:	1549824
MD5:	151ec82864cc859f03be0cb572f30357
SHA1:	b93f14d8b0eb8e0c12da8e8d4afcd9048a8228a2
SHA256:	1d5221667b8424ccbc7ecc85a7067dc264ac31ff97dfee76a080b7280b60d1e2
SHA512:	e44b05ec9123ee154f442c99701d5f782e41fac6761d8f3342d93303c325bbf56ef8c2c1437d6f187b2c7e1f92a71da1072d204b018f91abf8f780134b575a14
SSDEEP:	24576:+fuNeBUdtwsEgwsAe/z8YEoqSg5LIJfHKdofUA125kuV3MM1zMIDsxTt8gYcL:yuwBUwsEgwsAe5U/BldqdosA125BIYcL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....<... ...@....@.. .....@.....

File Icon

Icon Hash:	e0c6a169f4bed870

Static PE Info

General

Entrypoint:	0x553cba
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:	0x60C3192E [Fri Jun 11 08:05:02 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x151cc0	0x151e00	False	0.698621179014	data	7.39671386262	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x154000	0x2837c	0x28400	False	0.599864130435	data	6.35305378662	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2021

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x17e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/11/21-15:05:19.130058	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49740	587	192.168.2.3	208.91.199.223
06/11/21-15:05:22.400224	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49741	587	192.168.2.3	208.91.199.223

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 15:05:16.249649048 CEST	192.168.2.3	8.8.8.8	0xb219	Standard query (0)	smtp.globaloffs-site.com	A (IP address)	IN (0x0001)
Jun 11, 2021 15:05:16.539876938 CEST	192.168.2.3	8.8.8.8	0xb60a	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
Jun 11, 2021 15:05:16.455562115 CEST	8.8.8.8	192.168.2.3	0xb219	No error (0)	smtp.globaloffs-site.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:05:16.455562115 CEST	8.8.8.8	192.168.2.3	0xb219	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 11, 2021 15:05:16.455562115 CEST	8.8.8.8	192.168.2.3	0xb219	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 11, 2021 15:05:16.455562115 CEST	8.8.8.8	192.168.2.3	0xb219	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jun 11, 2021 15:05:16.455562115 CEST	8.8.8.8	192.168.2.3	0xb219	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jun 11, 2021 15:05:16.598628998 CEST	8.8.8.8	192.168.2.3	0xb60a	No error (0)	smtp.globaloffs-site.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 15:05:16.598628998 CEST	8.8.8.8	192.168.2.3	0xb60a	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jun 11, 2021 15:05:16.598628998 CEST	8.8.8.8	192.168.2.3	0xb60a	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jun 11, 2021 15:05:16.598628998 CEST	8.8.8.8	192.168.2.3	0xb60a	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 15:05:16.598628998 CEST	8.8.8.8	192.168.2.3	0xb60a	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 15:05:17.407032013 CEST	587	49740	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jun 11, 2021 15:05:17.576631069 CEST	49740	587	192.168.2.3	208.91.199.223	EHLO 878164
Jun 11, 2021 15:05:17.753143072 CEST	587	49740	208.91.199.223	192.168.2.3	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
Jun 11, 2021 15:05:17.756095886 CEST	49740	587	192.168.2.3	208.91.199.223	AUTH login c3RhZmZzQGdsb2JhbG9mZnMtc2l0ZS5jb20=
Jun 11, 2021 15:05:17.933439970 CEST	587	49740	208.91.199.223	192.168.2.3	334 UGFzc3dvcmQ6
Jun 11, 2021 15:05:18.113620043 CEST	587	49740	208.91.199.223	192.168.2.3	235 2.7.0 Authentication successful
Jun 11, 2021 15:05:18.125082016 CEST	49740	587	192.168.2.3	208.91.199.223	MAIL FROM:<staffs@globaloffs-site.com>
Jun 11, 2021 15:05:18.304600954 CEST	587	49740	208.91.199.223	192.168.2.3	250 2.1.0 Ok
Jun 11, 2021 15:05:18.759105921 CEST	49740	587	192.168.2.3	208.91.199.223	RCPT TO:<staffs@globaloffs-site.com>
Jun 11, 2021 15:05:18.949807882 CEST	587	49740	208.91.199.223	192.168.2.3	250 2.1.5 Ok
Jun 11, 2021 15:05:18.950215101 CEST	49740	587	192.168.2.3	208.91.199.223	DATA
Jun 11, 2021 15:05:19.126883030 CEST	587	49740	208.91.199.223	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Jun 11, 2021 15:05:19.130342007 CEST	49740	587	192.168.2.3	208.91.199.223	.
Jun 11, 2021 15:05:19.406755924 CEST	587	49740	208.91.199.223	192.168.2.3	250 2.0.0 Ok: queued as D3BED18547D
Jun 11, 2021 15:05:20.774704933 CEST	49740	587	192.168.2.3	208.91.199.223	QUIT
Jun 11, 2021 15:05:20.953493118 CEST	587	49740	208.91.199.223	192.168.2.3	221 2.0.0 Bye
Jun 11, 2021 15:05:21.310415030 CEST	587	49741	208.91.199.223	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jun 11, 2021 15:05:21.314012051 CEST	49741	587	192.168.2.3	208.91.199.223	EHLO 878164
Jun 11, 2021 15:05:21.490082026 CEST	587	49741	208.91.199.223	192.168.2.3	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
Jun 11, 2021 15:05:21.491157055 CEST	49741	587	192.168.2.3	208.91.199.223	AUTH login c3RhZmZzQGdsb2JhbG9mZnMtc2l0ZS5jb20=
Jun 11, 2021 15:05:21.667876959 CEST	587	49741	208.91.199.223	192.168.2.3	334 UGFzc3dvcmQ6
Jun 11, 2021 15:05:21.847563982 CEST	587	49741	208.91.199.223	192.168.2.3	235 2.7.0 Authentication successful
Jun 11, 2021 15:05:21.848362923 CEST	49741	587	192.168.2.3	208.91.199.223	MAIL FROM:<staffs@globaloffs-site.com>
Jun 11, 2021 15:05:22.027477026 CEST	587	49741	208.91.199.223	192.168.2.3	250 2.1.0 Ok
Jun 11, 2021 15:05:22.030374050 CEST	49741	587	192.168.2.3	208.91.199.223	RCPT TO:<staffs@globaloffs-site.com>
Jun 11, 2021 15:05:22.221380949 CEST	587	49741	208.91.199.223	192.168.2.3	250 2.1.5 Ok
Jun 11, 2021 15:05:22.222388029 CEST	49741	587	192.168.2.3	208.91.199.223	DATA
Jun 11, 2021 15:05:22.398606062 CEST	587	49741	208.91.199.223	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Jun 11, 2021 15:05:22.400413990 CEST	49741	587	192.168.2.3	208.91.199.223	.
Jun 11, 2021 15:05:22.676768064 CEST	587	49741	208.91.199.223	192.168.2.3	250 2.0.0 Ok: queued as 21A4A185763

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: NEW URGENT ENQUIRY.exe PID: 6068 Parent PID: 5664

General

Start time:	15:03:17
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\NEW URGENT ENQUIRY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEW URGENT ENQUIRY.exe'
Imagebase:	0x960000
File size:	1549824 bytes
MD5 hash:	151EC82864CC859F03BE0CB572F30357
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: 00000000.00000002.256781458.0000000003DE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.256781458.0000000003DE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.256294425.0000000002E30000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: NEW URGENT ENQUIRY.exe PID: 996 Parent PID: 6068

General

Start time:	15:03:32
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\NEW URGENT ENQUIRY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NEW URGENT ENQUIRY.exe
Imagebase:	0x700000
File size:	1549824 bytes
MD5 hash:	151EC82864CC859F03BE0CB572F30357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.480352639.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000002.480352639.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.485743997.0000000002C11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000000.248827227.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000002.00000000.248827227.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021