ID: 553301
Sample Name: KYC INQUIRY 14-01.exe
Cookbook: default.jbs
Time: 16:18:15
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report KYC INQUIRY 14-01.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 5
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 10
Public 10
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Data Directories 13
Sections 13
Resources 13
Imports 14
Version Infos 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 14
DNS Queries 14
DNS Answers 14
SMTP Packets 14
Code Manipulations 14
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: KYC INQUIRY 14-01.exe PID: 6504 Parent PID: 5176 15
General 15
File Activities 15
File Created 15
File Written 15
File Read 15

Copyright Joe Security LLC 2022

Analysis Process: KYC INQUIRY 14-01.exe PID: 5984 Parent PID: 6504 15
General 15
File Activities 16
File Created 16
File Read 16
Disassembly 16
Code Analysis 16

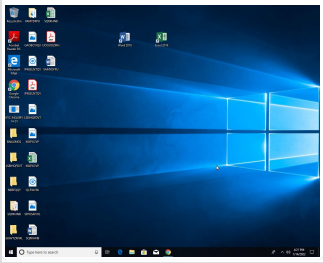
Windows Analysis Report KYC INQUIRY 14-01.exe

Overview

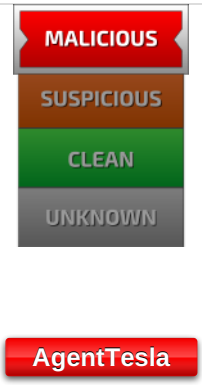
General Information

Sample Name:	KYC INQUIRY 14-01.exe
Analysis ID:	553301
MD5:	16d01fd64df5977..
SHA1:	dcfe9d148b76768.
SHA256:	77743ead6e13c0..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



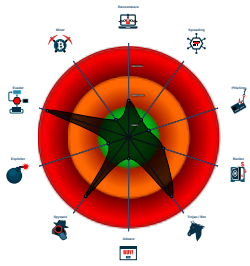
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fil…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- .NET source code contains method …
- .NET source code contains very larg…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- KYC INQUIRY 14-01.exe (PID: 6504 cmdline: "C:\Users\user\Desktop\KYC INQUIRY 14-01.exe" MD5: 16D01FD64DF59776D3454734512DED3C)
  - KYC INQUIRY 14-01.exe (PID: 5984 cmdline: C:\Users\user\Desktop\KYC INQUIRY 14-01.exe MD5: 16D01FD64DF59776D3454734512DED3C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "syed@amtartec.com",
  "Password": "Ra@454504",
  "Host": "mail.amtartec.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.688722039.000000000264A000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.928613280.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.928613280.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.685488835.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000004.00000000.685488835.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.KYC INQUIRY 14-01.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.KYC INQUIRY 14-01.exe.400000.4.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.KYC INQUIRY 14-01.exe.369a178.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.KYC INQUIRY 14-01.exe.369a178.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.0.KYC INQUIRY 14-01.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Copyright Joe Security LLC 2022

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

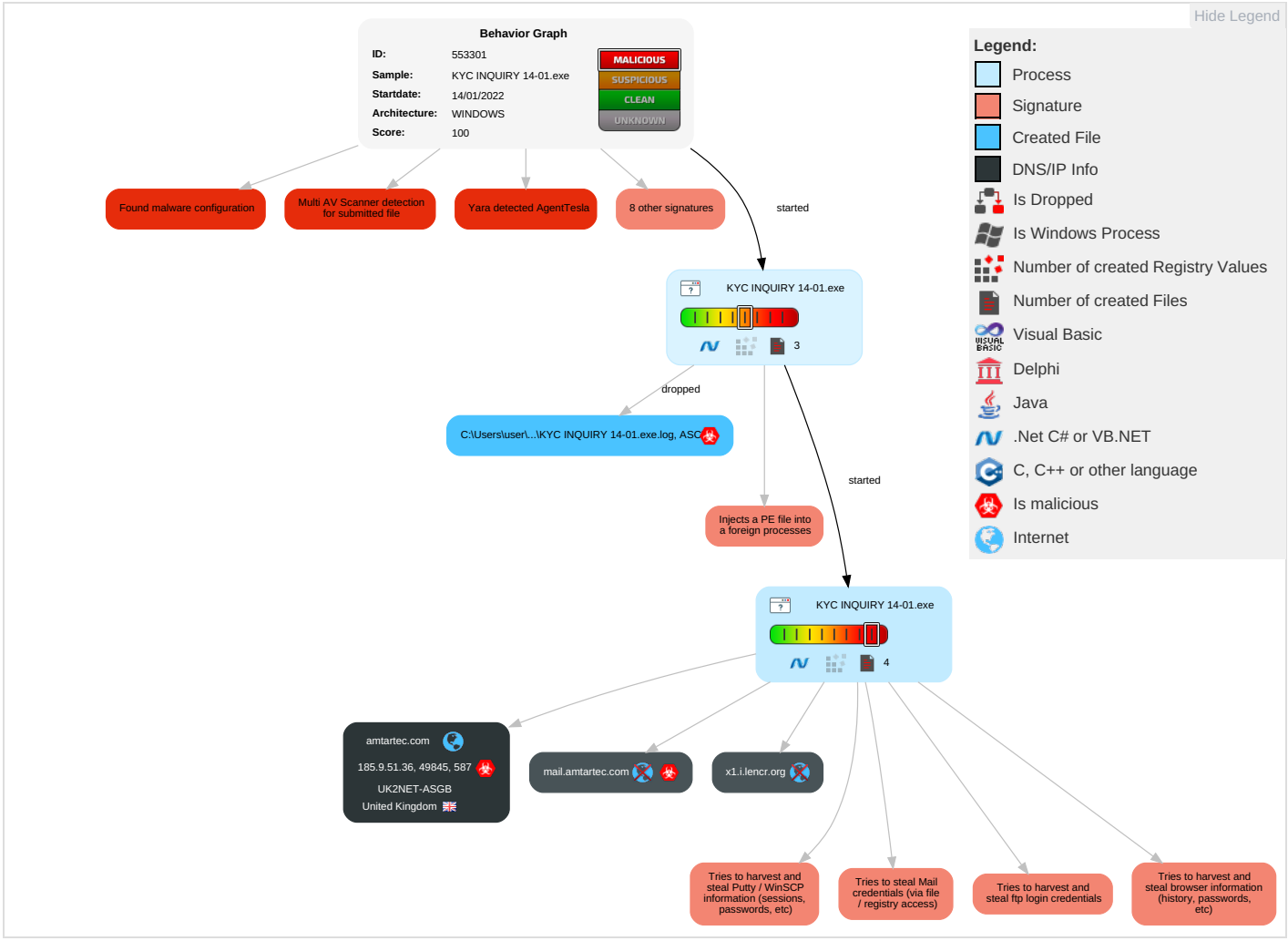
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Masquerading 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	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	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	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	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 Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

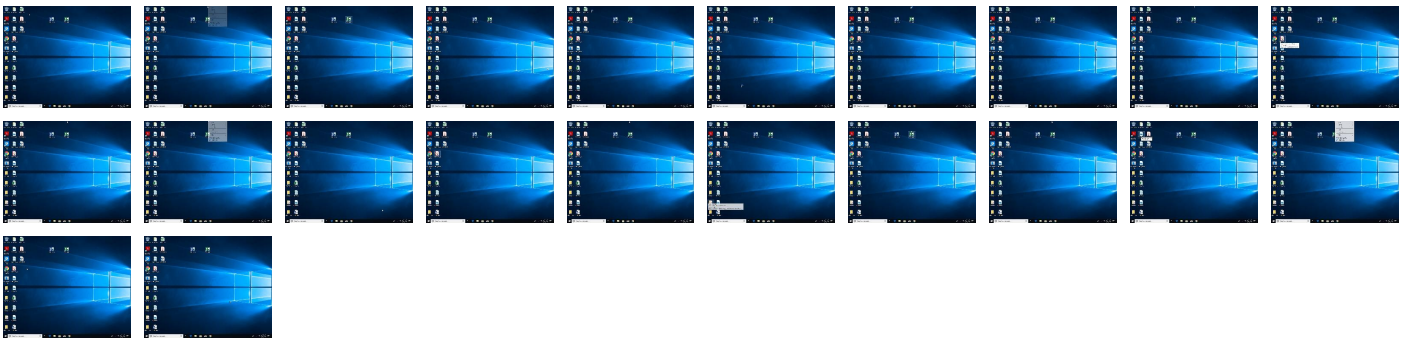
Behavior Graph



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
KYC INQUIRY 14-01.exe	32%	Virustotal		Browse
KYC INQUIRY 14-01.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.KYC INQUIRY 14-01.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.KYC INQUIRY 14-01.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.KYC INQUIRY 14-01.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.KYC INQUIRY 14-01.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.KYC INQUIRY 14-01.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.KYC INQUIRY 14-01.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
amtartec.com	2%	Virustotal		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
x1.i.lencr.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cnue	0%	URL Reputation	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.zhongyicts.com.cnt-p	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comuewaX	0%	Avira URL Cloud	safe	
http://bWuGMpUiLLMQeS0B9HKc.net	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.carterandcone.comue	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cni	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://ecvgsx.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://x1.i.lencr.org/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://amtartec.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://x1.i.lencr.org/j	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/)	0%	Avira URL Cloud	safe	
http://mail.amtartec.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
amtartec.com	185.9.51.36	true	true	• 2%, Virustotal, Browse	unknown
x1.i.lencr.org	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
mail.amtartec.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Copyright Joe Security LLC 2022

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.9.51.36	amtartec.com	United Kingdom		13213	UK2NET-ASGB	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553301
Start date:	14.01.2022
Start time:	16:18:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KYC INQUIRY 14-01.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:	16
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@3/5@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0%) • Quality average: 10% • Quality standard deviation: 22.4%
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
16:19:18	API Interceptor	733x Sleep call for process: KYC INQUIRY 14-01.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\2D85F72862B55C4EADD9E66E06947F3D	
Process:	C:\Users\user\Desktop\KYC INQUIRY 14-01.exe
File Type:	data
Category:	dropped
Size (bytes):	1391
Entropy (8bit):	7.705940075877404
Encrypted:	false
SSDEEP:	24:ooVdTH2NMU+I3E0Ulcrgdaf3sWrATrnkC4EmCUkmGMkfQo1fSZotWzD1:ooVguI3Kcx8WIzNeCUkJMmSuMX1
MD5:	0CD2F9E0DA1773E9ED864DA5E370E74E
SHA1:	CABD2A79A1076A31F21D253635CB039D4329A5E8
SHA-256:	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
SHA-512:	3B40F27E828323F5B91F8909883A78A21C86551761F27B38029FAAEC14AF5B7AA96FB9F9CC93EE201B5EB1D0FEF17B290747E8B839D2E49A8F36C5EBF3C7C910
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..k0..S.....@.YDc.c...0...*.H.....0O1.0...U....US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10...1506041104 38Z..3506041104 38Z0O1.0...U... .US1)0'..U... Internet Security Research Group1.0...U....ISRG Root X10.."0...*.H.....0.....$s..7.+W(.....8..n<.W.x.u...jn..O(..h.lD...c...k....1.!~.3<.H..y.....!.K...qiJffl.~<p. .)".....K...~....G.|.H#S.8.O.o...IW..t../.8.{.p!.u.0<.....c...O..K~.....w...{J.L.%.p..)..S$.....J.?..aQ.....cq...o[...\4ylv.;.by.../&.....6....7..6u...r.....I.....*.A..v.....5/(.I....dwn G7..Y^h..r...A)>Y>.&.$...Z.L@.F....:Qn.;.}r...xY.>Qx...../..>{J.Ks.....P.|C.t..t.....0.[q6....00\H..;..}`...).....A.....|.;F.H*..v.v..j.=...8.d..+..(.....B.".'].y...p..N..:..'Qn..d.3CO.....B0 @0...U.....0...U.....0....0...U.....y.Y.{....s.....X..n0...*.H.....U.X....P.....i ').au\.n...i/..VK..s.Y.!.~.Lq...`.9....!V..P.Y...Y.....b.E.f..|o..;....'...}~.."....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\KYC INQUIRY 14-01.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	**7.995245868798237**
Encrypted:	**true**
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvrP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEBF3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....;w.....RSNj .authroot.stl..>.(.5..CK..8T....c_.d...A.K...+.d.H..*i.RJJ.IQIR..$t)Kd.-[..T\{..ne.....<.w.....A..B.....c...wi.....D....c.0D,L.....f y....Rg...=.....i,3.3..Z....~^ve<...TF.*...f.zy.,...m.@.0.0...m.3..I(..+..v#...(.2....e...L..*y..V.....~U...."<ke.....I.X:Dt..R<7.5\A7L0=..T.V...IDr..8<....r&...I-.^..b.b.".Af....E.._.. r.>.`;,.Hob..S.....7'..\.R$.".g..+..64..@nP.....k3...B.`.G..@D.....L.....`^...#OpW.....!....`.....rf:.}.R.@....gR.#7....I..H.#...d.Qh..3..fCX....==#..M.I..~&....[.J9.\..Ww.....Tx.%....]..a4E ...q.+...#.*a..x..O..V.t..Y1!.T..`U...-...< _@...|(.....0..3.`.LU...E0.Gu.4KN....5...?.....I.p..'.....N<.d.O..dH@c1t...[w/...T....cYK.X>.0..Z.....O>..9.3.#9X.%.b...5.YK.E.V.....`./.3.._ ..nN]..=..M.o.F.._..z...._...gY..!Z..?l....vp.I.:.d.Z..W.....~...N.._.k...&.....$.....i.F.d.....D!e.....Y..,.E..m.;.1... $.F..O.F.o_}.uG....,.%.>,.Zx.....o....c./.;....g&.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D	
Process:	C:\Users\user\Desktop\KYC INQUIRY 14-01.exe

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\2D85F72862B55C4EADD9E66E06947F3D	
File Type:	data
Category:	dropped
Size (bytes):	192
Entropy (8bit):	2.8064124905820815
Encrypted:	false
SSDEEP:	3:kkFklx7pklflIXlE/zMc+kl7vNNX8RolJuRdyo1dlUKlGXJlDdt:kKKJ1bl7VNMa8Rdy+UKcXP
MD5:	4A9383DDA1B555B0482BCE39D980D801
SHA1:	32D22C955C4FC6AE9A6A5D523CC6C0162E18C2F2
SHA-256:	D80EB9F34CB71554A8E79D9411BC2AAAEBF2D3C22DD042C4D7F9D70D49080067
SHA-512:	A64B9045FA3256F6C552F6E1481B117519BADB0C094C353078DC23A92D6B3CE54C9FE9932968DA6FE43CE405A8B2A52999D13F98E659F742A309A72107F6382B
Malicious:	false
Reputation:	low
Preview:	p..... .....NF.s...(..... .....~...3.....o...h.t.t.p.:./.x.1...i...l.e.n.c.r...o.r.g./...".5.a.6.2.8.1.5.c.-.5.6.f."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\KYC INQUIRY 14-01.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.107354238829088
Encrypted:	false
SSDEEP:	6:kKHl7k8SN+SkQlPlEGYRMY9z+4KlDA3RUeYlUmlUR/t:Pl79kPlE99SNxAhUeYlUSA/t
MD5:	CD1193487E842FB09580F190E8854F43
SHA1:	9F7D85ED563298576947EAC5DC7C881B38C73B73
SHA-256:	1E6BB9B9D15DB356B93F2D11A16F4D5C1788C2C3BCAA0E2FBA122CFF34CE073A
SHA-512:	5DC850BD90754D755FB12447FD023EC1A492C617F7505C20721C667B1F44052C7A9AD99A773345BF5539B30D6F5FE764ECF80E590751717184CEF256E11364C9
Malicious:	false
Reputation:	low
Preview:	p..... .....u...(..... .....q.\].....&.....h.t.t.p.:./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.7.1.e.1.5.c.5.d.c.4.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\KYC INQUIRY 14-01.exe.log	
Process:	C:\Users\user\Desktop\KYC INQUIRY 14-01.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.226177281531698

General

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:	KYC INQUIRY 14-01.exe
File size:	590336
MD5:	16d01fd64df59776d3454734512ded3c
SHA1:	dcfe9d148b76768ae3dea9875255c0873d58d1b0
SHA256:	77743ead6e13c024db3534a837c669ee3c4fbaac2320bb937fbe5e58de4a3b3
SHA512:	cb90d72e5244c4baf5aa9ee7aad040dbdc6b47318cb3b5dbec4a6c9d1b2290d650c4c8be77255c5017af181c446d6daa70202e89002429e5c6046643c0d0d699
SSDEEP:	12288:KK777777777777N7LPJ6OISxBo/+0dxGhu2jfwr7zo:KK777777777777ILB6O/p0dlhJwjo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....g.a..... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4916de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61E1670E [Fri Jan 14 12:05:34 2022 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	0x8f6e4	0x8f800	False	0.755303040614	data	7.23594935691	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x92000	0x5f4	0x600	False	0.438802083333	data	4.189050521	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x94000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 16:21:00.951390028 CET	192.168.2.4	8.8.8.8	0x333c	Standard query (0)	mail.amtartec.com	A (IP address)	IN (0x0001)
Jan 14, 2022 16:21:01.099323034 CET	192.168.2.4	8.8.8.8	0xdbe6	Standard query (0)	mail.amtartec.com	A (IP address)	IN (0x0001)
Jan 14, 2022 16:21:03.558242083 CET	192.168.2.4	8.8.8.8	0xdca9	Standard query (0)	x1.i.lencr.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 16:21:01.072341919 CET	8.8.8.8	192.168.2.4	0x333c	No error (0)	mail.amtartec.com	amtartec.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 16:21:01.072341919 CET	8.8.8.8	192.168.2.4	0x333c	No error (0)	amtartec.com		185.9.51.36	A (IP address)	IN (0x0001)
Jan 14, 2022 16:21:01.326092005 CET	8.8.8.8	192.168.2.4	0xdbe6	No error (0)	mail.amtartec.com	amtartec.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 16:21:01.326092005 CET	8.8.8.8	192.168.2.4	0xdbe6	No error (0)	amtartec.com		185.9.51.36	A (IP address)	IN (0x0001)
Jan 14, 2022 16:21:03.580791950 CET	8.8.8.8	192.168.2.4	0xdca9	No error (0)	x1.i.lencr.org	crl.root-x1.letsencrypt.org.edgekey.net		CNAME (Canonical name)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 14, 2022 16:21:01.543900967 CET	587	49845	185.9.51.36	192.168.2.4	220-summit.nocdirect.com ESMTP Exim 4.93 #2 Fri, 14 Jan 2022 15:21:00 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 14, 2022 16:21:01.544349909 CET	49845	587	192.168.2.4	185.9.51.36	EHLO 724471
Jan 14, 2022 16:21:01.578347921 CET	587	49845	185.9.51.36	192.168.2.4	250-summit.nocdirect.com Hello 724471 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 14, 2022 16:21:01.578954935 CET	49845	587	192.168.2.4	185.9.51.36	STARTTLS
Jan 14, 2022 16:21:01.617613077 CET	587	49845	185.9.51.36	192.168.2.4	220 TLS go ahead

Code Manipulations

Copyright Joe Security LLC 2022

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: KYC INQUIRY 14-01.exe PID: 6504 Parent PID: 5176

General

Start time:	16:19:10
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\KYC INQUIRY 14-01.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\KYC INQUIRY 14-01.exe"
Imagebase:	0x280000
File size:	590336 bytes
MD5 hash:	16D01FD64DF59776D3454734512DED3C
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: 00000000.00000002.688722039.000000000264A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.688470946.0000000002601000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.689364084.0000000003609000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.689364084.0000000003609000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: KYC INQUIRY 14-01.exe PID: 5984 Parent PID: 6504

General

Start time:	16:19:19
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\KYC INQUIRY 14-01.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\KYC INQUIRY 14-01.exe
Imagebase:	0x6a0000
File size:	590336 bytes
MD5 hash:	16D01FD64DF59776D3454734512DED3C
Has elevated privileges:	true

Copyright Joe Security LLC 2022

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.928613280.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.928613280.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.685488835.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.685488835.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.684540552.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.684540552.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.685016391.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.685016391.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.685872653.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.685872653.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.930221885.00000000029C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.930221885.00000000029C1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2022