ID: 778237
Sample Name: New Inquiries.exe
Cookbook: default.jbs
Time: 09:11:08
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

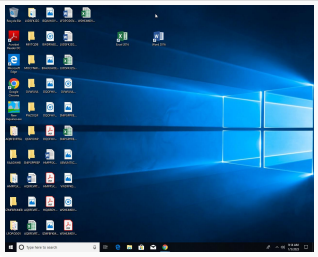
Windows Analysis Report

New Inquiries.exe

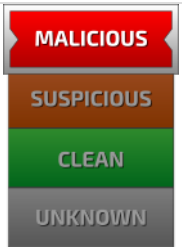
Overview

General Information

Sample Name:	New Inquiries.exe
Analysis ID:	778237
MD5:	14f34ce68a9fa22..
SHA1:	bb12303832e9d7.
SHA256:	bda00392e993ae.
Tags:	AgentTesla exe
Infos:	



Detection



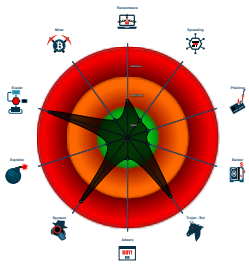
AgentTesla, zgRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected zgRAT
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Contains functionality to register a lo…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- New Inquiries.exe (PID: 3080 cmdline: C:\Users\user\Desktop\New Inquiries.exe MD5: 14F34CE68A9FA222F4890789E3B52F1A)
  - New Inquiries.exe (PID: 6128 cmdline: C:\Users\user\Desktop\New Inquiries.exe MD5: 14F34CE68A9FA222F4890789E3B52F1A)
  - New Inquiries.exe (PID: 6092 cmdline: C:\Users\user\Desktop\New Inquiries.exe MD5: 14F34CE68A9FA222F4890789E3B52F1A)
  - New Inquiries.exe (PID: 6116 cmdline: C:\Users\user\Desktop\New Inquiries.exe MD5: 14F34CE68A9FA222F4890789E3B52F1A)
  - New Inquiries.exe (PID: 5176 cmdline: C:\Users\user\Desktop\New Inquiries.exe MD5: 14F34CE68A9FA222F4890789E3B52F1A)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "smtp.yandex.com",
  "Username": "hisgraceinme@yandex.com",
  "Password": "General1248@1"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000004.00000000.275678550.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x22f9f:$a20: get_LastAccessed • 0x250dc:$a30: set_GuidMasterKey • 0x23053:$a33: get_Clipboard • 0x23061:$a34: get_Keyboard • 0x2421e:$a35: get_ShiftKeyDown • 0x2422f:$a36: get_AltKeyDown • 0x2306e:$a37: get_Password • 0x23aa4:$a38: get_PasswordHash • 0x24927:$a39: get_DefaultCredentials
00000000.00000002.284958103.0000000002D53000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.284057743.0000000002C5B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.286924185.0000000003C29000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0xa84df:$a20: get_LastAccessed • 0xd0aff:$a20: get_LastAccessed • 0x2b2e9f:$a20: get_LastAccessed • 0xaa61c:$a30: set_GuidMasterKey • 0xd2c3c:$a30: set_GuidMasterKey • 0x2b4fdc:$a30: set_GuidMasterKey • 0xa8593:$a33: get_Clipboard • 0xd0bb3:$a33: get_Clipboard • 0x2b2f53:$a33: get_Clipboard • 0xa85a1:$a34: get_Keyboard • 0xd0bc1:$a34: get_Keyboard • 0x2b2f61:$a34: get_Keyboard • 0xa975e:$a35: get_ShiftKeyDown • 0xd1d7e:$a35: get_ShiftKeyDown • 0x2b411e:$a35: get_ShiftKeyDown • 0xa976f:$a36: get_AltKeyDown • 0xd1d8f:$a36: get_AltKeyDown • 0x2b412f:$a36: get_AltKeyDown • 0xa85ae:$a37: get_Password • 0xd0bce:$a37: get_Password • 0x2b2f6e:$a37: get_Password
00000004.00000002.514770158.0000000002851000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.New Inquiries.exe.2caffbc.0.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0x39f2:$v1: SbieDll.dll • 0x3a0c:$v2: USER • 0x3a18:$v3: SANDBOX • 0x3a2a:$v4: VIRUS • 0x3a7a:$v4: VIRUS • 0x3a38:$v5: MALWARE • 0x3a4a:$v6: SCHMIDTI • 0x3a5e:$v7: CURRENTUSER
4.0.New Inquiries.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x26926:$s10: logins • 0x263b4:$s11: credential • 0x23253:$g1: get_Clipboard • 0x23261:$g2: get_Keyboard • 0x2326e:$g3: get_Password • 0x2440e:$g4: get_CtrlKeyDown • 0x2441e:$g5: get_ShiftKeyDown • 0x2442f:$g6: get_AltKeyDown
4.0.New Inquiries.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2319f:$a20: get_LastAccessed • 0x252dc:$a30: set_GuidMasterKey • 0x23253:$a33: get_Clipboard • 0x23261:$a34: get_Keyboard • 0x2441e:$a35: get_ShiftKeyDown • 0x2442f:$a36: get_AltKeyDown • 0x2326e:$a37: get_Password • 0x23ca4:$a38: get_PasswordHash • 0x24b27:$a39: get_DefaultCredentials
0.2.New Inquiries.exe.2c87698.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.New Inquiries.exe.2c87698.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0x2e116:$v1: SbieDll.dll • 0x2e130:$v2: USER • 0x2e13c:$v3: SANDBOX • 0x2e14e:$v4: VIRUS • 0x2e19e:$v4: VIRUS • 0x2e15c:$v5: MALWARE • 0x2e16e:$v6: SCHMIDTI • 0x2e182:$v7: CURRENTUSER
Click to see the 24 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

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

Stealing of Sensitive Information

Yara detected zgRAT

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

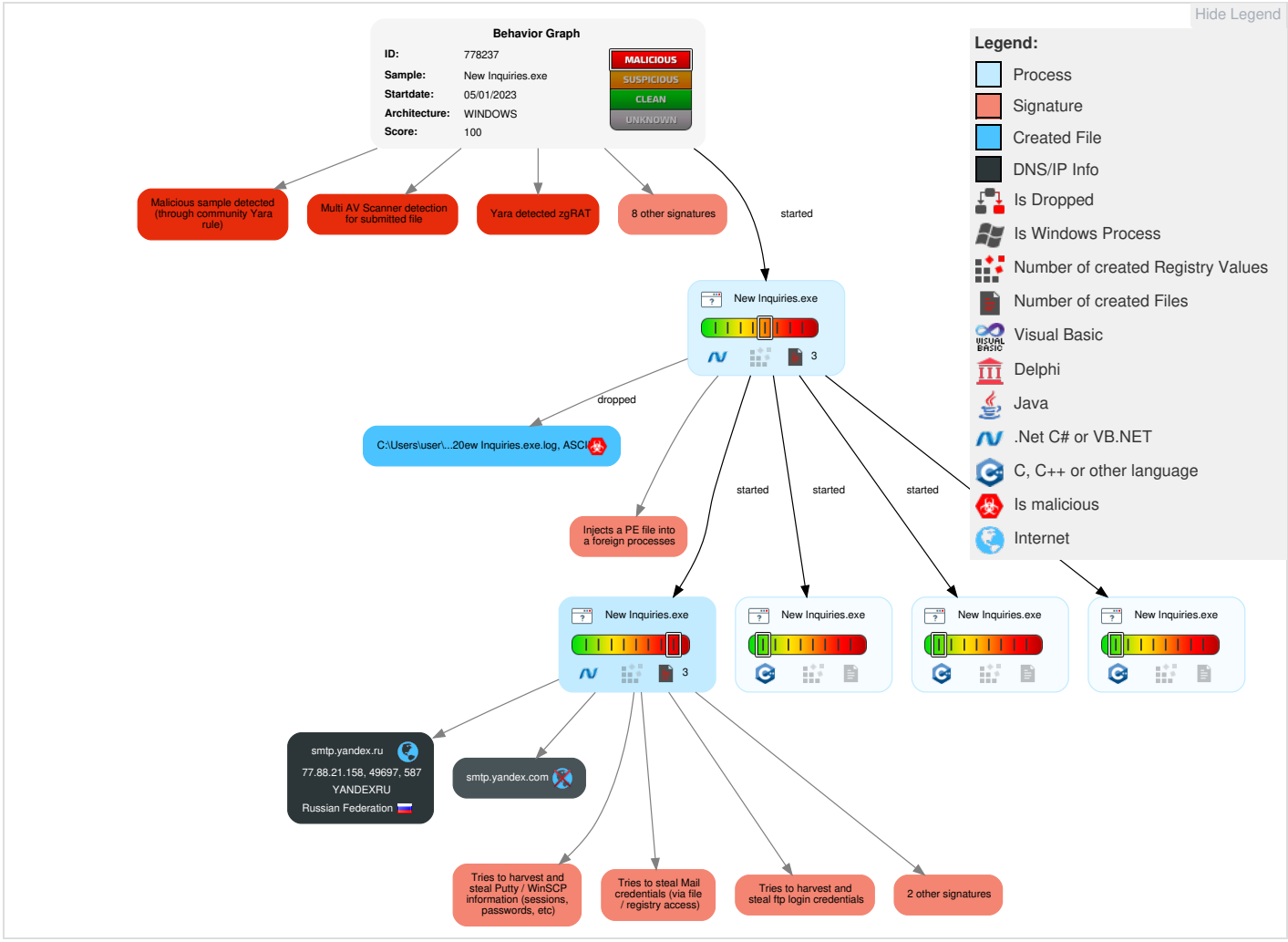
Yara detected zgRAT

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	2 1 Input Capture	1 Process Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

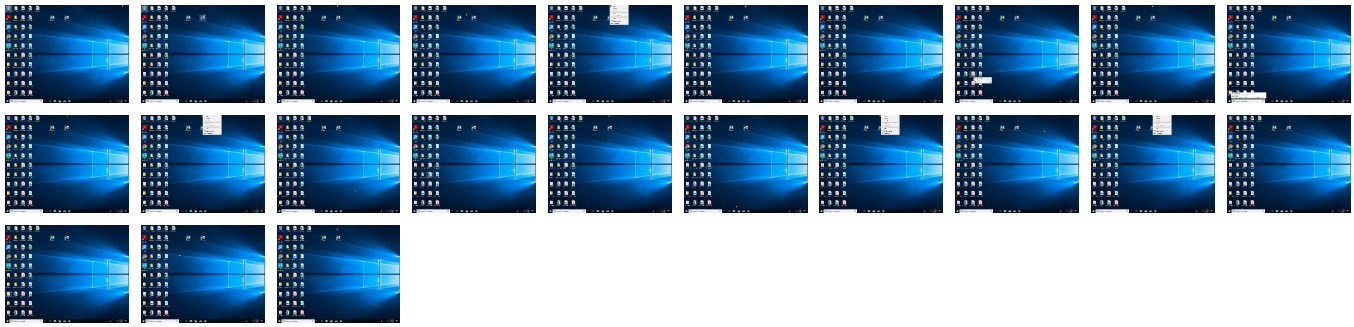
Behavior Graph



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
New Inquiries.exe	15%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
New Inquiries.exe	21%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.New Inquiries.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fssnet-n.de	0%	Avira URL Cloud	safe	
http://www-FSSNET-N.de.	0%	Avira URL Cloud	safe	
http://0kw8yxBP9SjNp6iDn.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

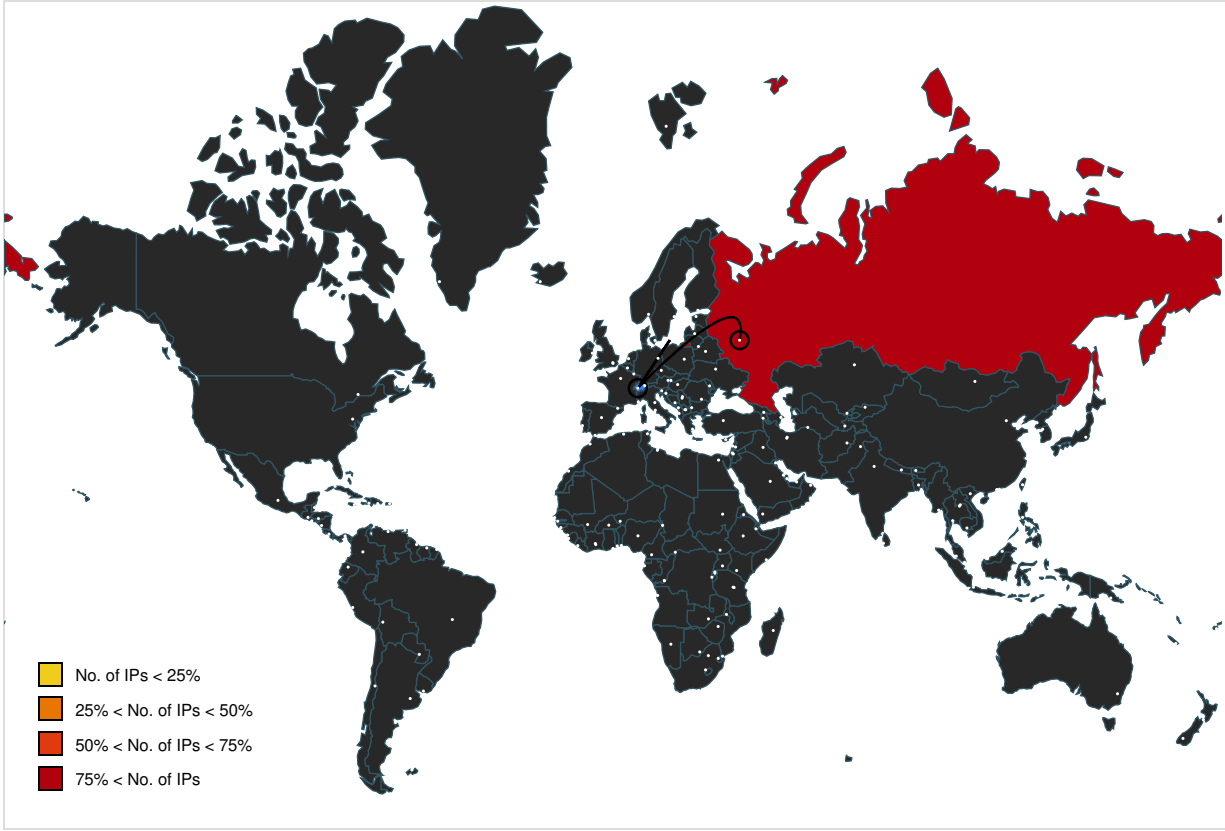
Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fssnet-n.de	New Inquiries.exe	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www-FSSNET-N.de.	New Inquiries.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://smtp.yandex.com	New Inquiries.exe, 00000004.00000002.517966891.0000000002BE9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://0kw8yxBP9SjNp6iDn.com	New Inquiries.exe, 00000004.00000002.514770158.0000000002851000.00000004.00000800.00020000.00000000.sdmp, New Inquiries.exe, 00000004.00000002.518045904.0000000002C0C000.00000004.00000800.00020000.00000000.sdmp, New Inquiries.exe, 00000004.00000002.518066878.0000000002C15000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	New Inquiries.exe, 00000004.00000002.514770158.0000000002851000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	New Inquiries.exe, 00000000.00000002.293425589.0000000006D82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778237
Start date and time:	2023-01-05 09:11:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Inquiries.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, 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@9/1@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- 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
09:12:11	API Interceptor	676x Sleep call for process: New Inquiries.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Inquiries.exe.log

Process:	C:\Users\user\Desktop\New Inquiries.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**

Reputation:	high, 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):	7.557841516680359
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 Inquiries.exe
File size:	659968
MD5:	14f34ce68a9fa222f4890789e3b52f1a
SHA1:	bb12303832e9d7f09929fdcf13d48dc5d33734c6
SHA256:	bda00392e993aec17335551aa8bbe596bf1aab747e7b41ebd65d1360ea117458
SHA512:	0b4e78bf313a9c62a10dce403583964abef5a2be7f865cf484bbcaf4d9e5f5c4a6b3705676036126f46f3e14f85972d0b918b70595c1a034ecc1991ab1e25ae8
SSDEEP:	12288:v16q9hx1HsAi3W65CCe3LB47q0nLW2Rfxj0s:B9hx3cW6oCebB47rnC4fxQs
TLSH:	1AE4CF4022E90B55F2BE9BF9283121404BB1B9D7F97EE36D8EC164EE15B1F448A14F63
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....V.c.....0.....$.....f.... ... .@.. .....@.....

File Icon

Icon Hash:	e3cfcccecca46894

Static PE Info

General

Entrypoint:	0x4a0a66
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63B656AA [Thu Jan 5 04:48:42 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa0a12	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x2064	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x9bc10	0x54	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9ea6c	0x9ec00	False	0.795095656988189	data	7.570374319797151	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x2064	0x2200	False	0.6196001838235294	data	6.4950187217885205	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa6000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

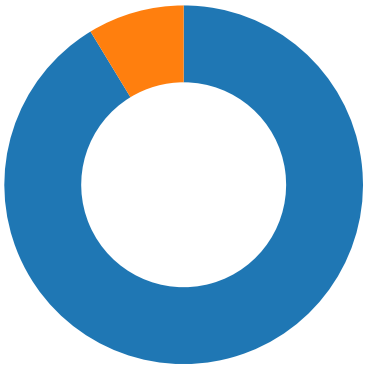
Name	RVA	Size	Type	Language	Country
RT_ICON	0xa2100	0xe72	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xa2f84	0x14	data		
RT_VERSION	0xa2fa8	0x380	data		
RT_MANIFEST	0xa3338	0xd25	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



Total Packets: 23

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:12:37.523272038 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:37.579607010 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:37.579875946 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:37.787043095 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:37.790563107 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:37.846858025 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:37.846930027 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:37.847382069 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:37.903650999 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:37.903714895 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:37.952445030 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.008886099 CET	587	49697	77.88.21.158	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:12:38.010085106 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.010139942 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.010190010 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.010230064 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.010325909 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.014235973 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.020104885 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.076680899 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.152487040 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.169496059 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.226102114 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.229351044 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.285790920 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.287503004 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.361238956 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.361780882 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.424417973 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.424849987 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.487318993 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.487910986 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.544802904 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.550384998 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.550551891 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.552134991 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.552227974 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:12:38.607623100 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.608541012 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:38.875274897 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:12:39.043133974 CET	49697	587	192.168.2.3	77.88.21.158
Jan 5, 2023 09:13:53.875366926 CET	587	49697	77.88.21.158	192.168.2.3
Jan 5, 2023 09:13:53.875534058 CET	49697	587	192.168.2.3	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 5, 2023 09:12:37.423968077 CET	62704	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:12:37.443080902 CET	53	62704	8.8.8.8	192.168.2.3
Jan 5, 2023 09:12:37.483679056 CET	49977	53	192.168.2.3	8.8.8.8
Jan 5, 2023 09:12:37.503631115 CET	53	49977	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 5, 2023 09:12:37.423968077 CET	192.168.2.3	8.8.8.8	0x3cc5	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:12:37.483679056 CET	192.168.2.3	8.8.8.8	0xf434	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:12:37.443080902 CET	8.8.8.8	192.168.2.3	0x3cc5	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)	false
Jan 5, 2023 09:12:37.443080902 CET	8.8.8.8	192.168.2.3	0x3cc5	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)	false
Jan 5, 2023 09:12:37.503631115 CET	8.8.8.8	192.168.2.3	0xf434	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)	false

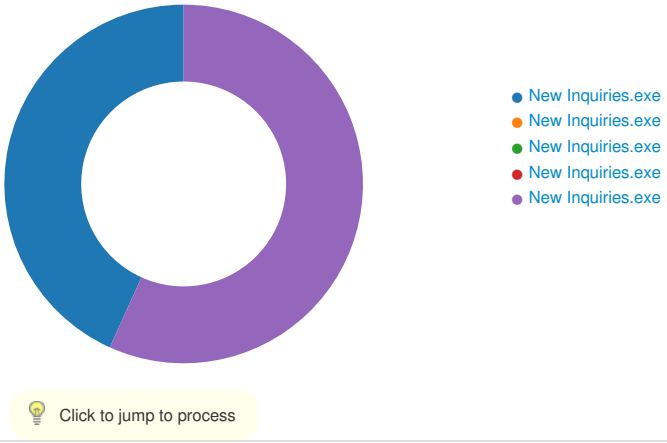
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 5, 2023 09:12:37.503631115 CET	8.8.8.8	192.168.2.3	0xf434	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 5, 2023 09:12:37.787043095 CET	587	49697	77.88.21.158	192.168.2.3	220 iva2-656890eaceb5.qloud-c.yandex.net (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru) 1672906357-bCTcGlJYMqM1
Jan 5, 2023 09:12:37.790563107 CET	49697	587	192.168.2.3	77.88.21.158	EHLO 783875
Jan 5, 2023 09:12:37.846930027 CET	587	49697	77.88.21.158	192.168.2.3	250-iva2-656890eaceb5.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 53477376 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 5, 2023 09:12:37.847382069 CET	49697	587	192.168.2.3	77.88.21.158	STARTTLS
Jan 5, 2023 09:12:37.903714895 CET	587	49697	77.88.21.158	192.168.2.3	220 Go ahead

Statistics

Behavior



System Behavior

Analysis Process: New Inquiries.exe PID: **3080**, Parent PID: **3452**

General

Target ID:	0
Start time:	09:12:00
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\New Inquiries.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New Inquiries.exe
Imagebase:	0x8b0000
File size:	659968 bytes
MD5 hash:	14F34CE68A9FA222F4890789E3B52F1A
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: 00000000.00000002.284958103.0000000002D53000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.284057743.0000000002C5B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.286924185.0000000003C29000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D37CF06	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	6D37CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New Inquiries.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D68C78D	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\New Inquiries.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D68C907	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	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2B03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1C1B4F	ReadFile

Analysis Process: New Inquiries.exe PID: **6128**, Parent PID: **3080**

General

Target ID:	1
Start time:	09:12:13
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\New Inquiries.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\New Inquiries.exe
Imagebase:	0x310000
File size:	659968 bytes
MD5 hash:	14F34CE68A9FA222F4890789E3B52F1A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: New Inquiries.exe PID: **6092**, Parent PID: **3080**

General

Target ID:	2
Start time:	09:12:13
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\New Inquiries.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\New Inquiries.exe
Imagebase:	0x110000
File size:	659968 bytes
MD5 hash:	14F34CE68A9FA222F4890789E3B52F1A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: New Inquiries.exe PID: **6116**, Parent PID: **3080**

General

Target ID:	3
Start time:	09:12:13
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\New Inquiries.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\New Inquiries.exe
Imagebase:	0x80000
File size:	659968 bytes
MD5 hash:	14F34CE68A9FA222F4890789E3B52F1A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: New Inquiries.exe PID: **5176**, Parent PID: **3080**

General

Target ID:	4
Start time:	09:12:14
Start date:	05/01/2023
Path:	C:\Users\user\Desktop\New Inquiries.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New Inquiries.exe
Imagebase:	0x500000
File size:	659968 bytes
MD5 hash:	14F34CE68A9FA222F4890789E3B52F1A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000004.00000000.275678550.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.514770158.0000000002851000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.514770158.0000000002851000.00000004.00000800.00020000.00000000.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	6D37CF06	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	6D37CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp8F47.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1C7038	GetTempFileNameW

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	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C1C1B4F	ReadFile

Disassembly

No disassembly