ID: 381954
Sample Name:
Quotation_Request.pdf.exe
Cookbook: default.jbs
Time: 15:22:16
Date: 05/04/2021
Version: 31.0.0 Emerald

Table of Contents

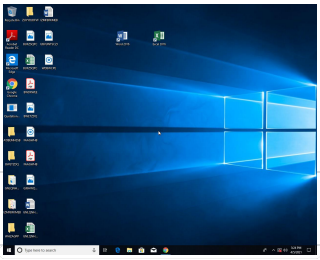
Analysis Report Quotation_Request.pdf.exe

Overview

General Information

Sample Name:	Quotation_Request.pdf.exe
Analysis ID:	381954
MD5:	79cd8383f51372c..
SHA1:	41b082acc2c972..
SHA256:	08ecce1fb89755f..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

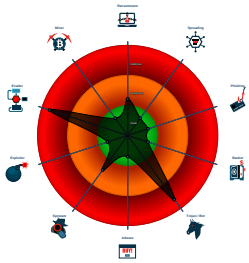
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…

Classification



Startup

- **System is w10x64**
- Quotation_Request.pdf.exe (PID: 6812 cmdline: 'C:\Users\user\Desktop\Quotation_Request.pdf.exe' MD5: 79CD8383F51372C9F0721289F6470889)
  - schtasks.exe (PID: 7156 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\mgdPGGmBTUB' /XML 'C:\Users\user\AppData\Local\Temp\tmp4108.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Quotation_Request.pdf.exe (PID: 6184 cmdline: {path} MD5: 79CD8383F51372C9F0721289F6470889)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-000c0a4c",
  "Domain1": "185.140.53.138",
  "Domain2": "wealth2021.ddns.net",
  "Port": 20221,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.915585705.000000000424 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000007.00000002.915585705.000000000424 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2f25:$a: NanoCore • 0x2f7e:$a: NanoCore • 0x2fbb:$a: NanoCore • 0x3034:$a: NanoCore • 0x166df:$a: NanoCore • 0x166f4:$a: NanoCore • 0x16729:$a: NanoCore • 0x2f1ab:$a: NanoCore • 0x2f1c0:$a: NanoCore • 0x2f1f5:$a: NanoCore • 0x2f87:$b: ClientPlugin • 0x2fc4:$b: ClientPlugin • 0x38c2:$b: ClientPlugin • 0x38cf:$b: ClientPlugin • 0x1649b:$b: ClientPlugin • 0x164b6:$b: ClientPlugin • 0x164e6:$b: ClientPlugin • 0x166fd:$b: ClientPlugin • 0x16732:$b: ClientPlugin • 0x2ef67:$b: ClientPlugin • 0x2ef82:$b: ClientPlugin
00000007.00000002.910440446.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000002.910440446.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.910440446.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.Quotation_Request.pdf.exe.5ab4629.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
7.2.Quotation_Request.pdf.exe.5ab4629.9.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
7.2.Quotation_Request.pdf.exe.5ab4629.9.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
7.2.Quotation_Request.pdf.exe.58e0000.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
7.2.Quotation_Request.pdf.exe.58e0000.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 35 entries				

Sigma Overview

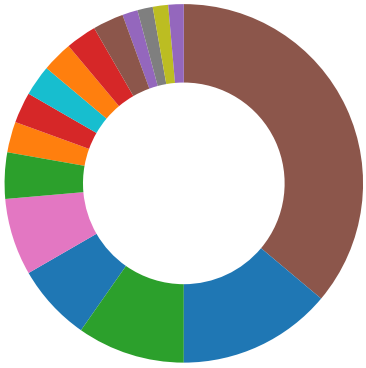
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT

Networking:

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

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

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

- Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

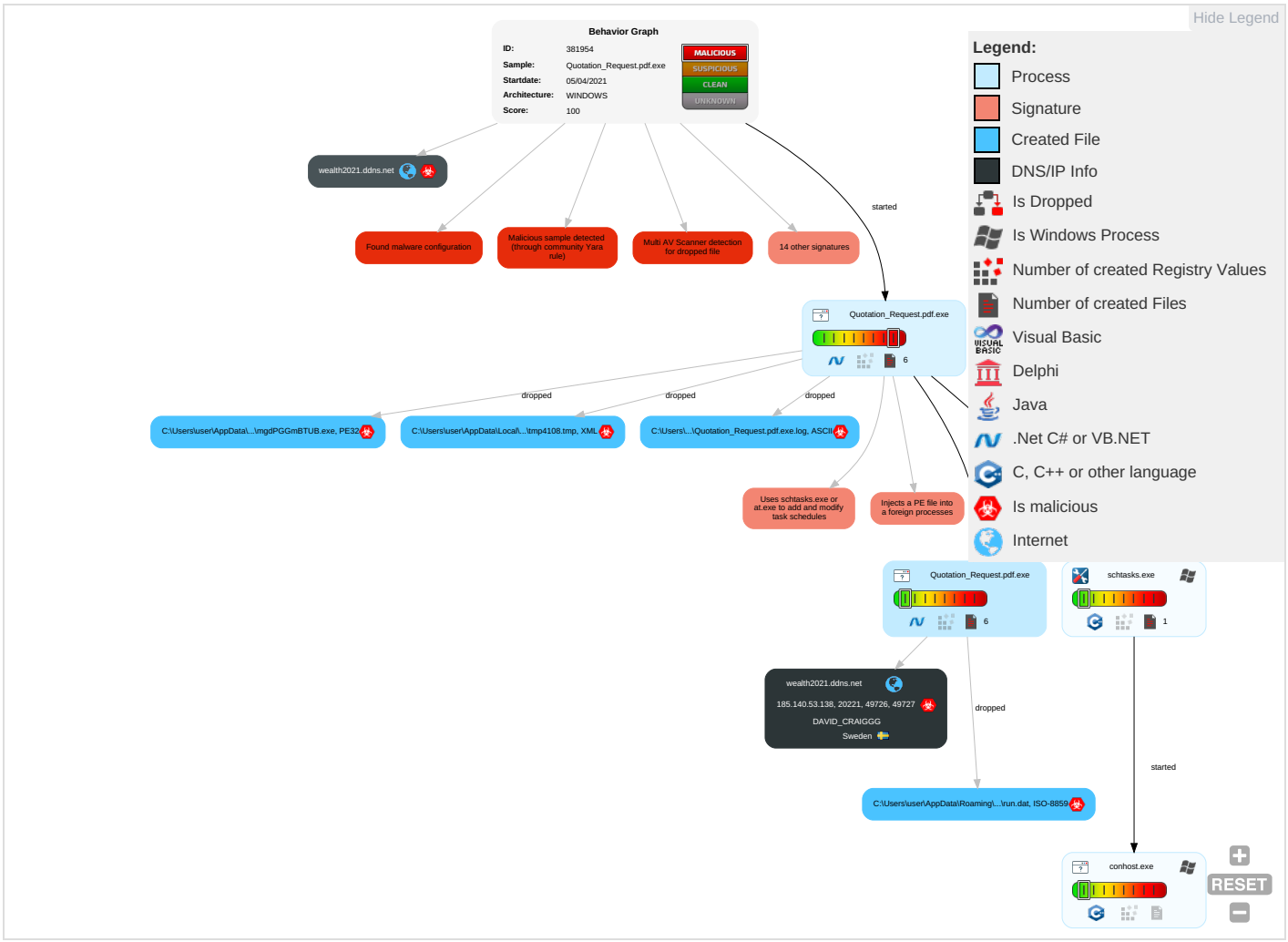
Remote Access Functionality:

- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networl Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 2	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

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
Quotation_Request.pdf.exe	30%	Virustotal		Browse
Quotation_Request.pdf.exe	24%	Metadefender		Browse
Quotation_Request.pdf.exe	58%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\mgdPGGmBTUB.exe	24%	Metadefender		Browse
C:\Users\user\AppData\Roaming\mgdPGGmBTUB.exe	58%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.Quotation_Request.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.Quotation_Request.pdf.exe.5ab0000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
wealth2021.ddns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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.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://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.coma~	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.goodfont.co.kr	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.carterandcone.coml	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.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.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.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://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://fontfabrik.com	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	
wealth2021.ddns.net	0%	Virustotal		Browse
wealth2021.ddns.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	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.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTFZ	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.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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://www.sakkal.com	0%	URL Reputation	safe	
185.140.53.138	0%	Avira URL Cloud	safe	
http://www.fontbureau.comue9	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealth2021.ddns.net	185.140.53.138	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

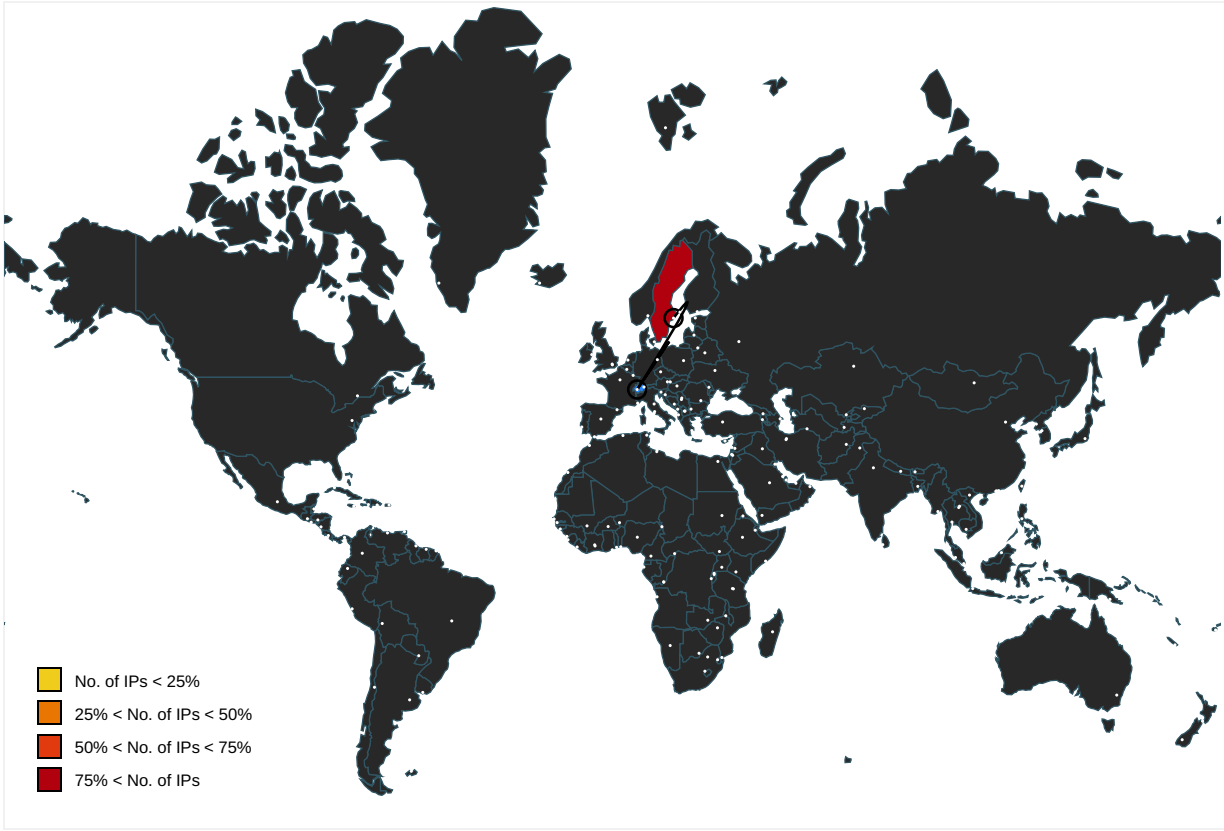
Name	Malicious	Antivirus Detection	Reputation
wealth2021.ddns.net	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
185.140.53.138	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.tiro.com	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma~	Quotation_Request.pdf.exe, 00000000.00000002.671021338.00001487000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Quotation_Request.pdf.exe, 00000000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comB.TTFZ	Quotation_Request.pdf.exe, 00000.00000002.671021338.00000001487000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Quotation_Request.pdf.exe, 00000.00000002.679777119.00000009011000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Quotation_Request.pdf.exe, 00000.00000002.678291126.00000006EC2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comue9	Quotation_Request.pdf.exe, 00000.00000002.671021338.00000001487000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.138	wealth2021.ddns.net	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	381954
Start date:	05.04.2021
Start time:	15:22:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation_Request.pdf.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:	21
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.evad.winEXE@6/4@10/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 73.2% • Quality standard deviation: 8.9%
HCA Information:	• Successful, ratio: 98% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 92.122.145.220, 104.43.139.144, 20.82.209.183, 168.61.161.212, 13.64.90.137, 92.122.213.247, 92.122.213.194, 52.155.217.156, 93.184.221.240, 20.54.26.129, 20.82.210.154 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:23:10	API Interceptor	2x Sleep call for process: Quotation_Request.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.138	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	
	1PH37n4Gva.exe	Get hash	malicious	Browse	
	35dbds3GQG.exe	Get hash	malicious	Browse	
	QXJGE2LOdP.exe	Get hash	malicious	Browse	
	O4m3hDFNbh.exe	Get hash	malicious	Browse	
	nrv_remittance#U007eorder#U007epayment.exe	Get hash	malicious	Browse	
	NEW ORDER REQUEST_EXPORT005JKL DOC.exe	Get hash	malicious	Browse	
	WIRE COPY ORDER T104484_PP.exe	Get hash	malicious	Browse	
	71AXBkD1wA.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wealth2021.ddns.net	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	FRQ_05694 revised quantity.exe	Get hash	malicious	Browse	• 185.140.53.69
	INVOICE 15112021.xlsx	Get hash	malicious	Browse	• 185.140.53.130
	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	IMG-001982-AW00173-SSE73I.exe	Get hash	malicious	Browse	• 185.140.53.230
	FYI-Orderimg.exe	Get hash	malicious	Browse	• 185.140.53.67
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	PO-94765809570-Order pdf.exe	Get hash	malicious	Browse	• 185.140.53.7
	Commercial E-invoice.exe	Get hash	malicious	Browse	• 185.140.53.137
	Order23032021.xls	Get hash	malicious	Browse	• 185.140.53.130
	ZcQwvgqtuQ.exe	Get hash	malicious	Browse	• 91.193.75.245
	lKIPqaYkKB.exe	Get hash	malicious	Browse	• 185.140.53.161
	t5R60D503x.exe	Get hash	malicious	Browse	• 185.140.53.9
	Purchase OrderDated19032021.xls	Get hash	malicious	Browse	• 185.140.53.130
	0u1JLplwRo.exe	Get hash	malicious	Browse	• 185.140.53.139
	PO-21322.xlsm	Get hash	malicious	Browse	• 185.165.153.116
	GT_0397337_03987638BNG.exe	Get hash	malicious	Browse	• 185.140.53.9
	5woB0vy0X6.exe	Get hash	malicious	Browse	• 185.140.53.139
	Doc_IMAGE-587HTY-9545-55401.exe	Get hash	malicious	Browse	• 185.140.53.230
	1PH37n4Gva.exe	Get hash	malicious	Browse	• 185.140.53.138
	malwa.exe	Get hash	malicious	Browse	• 185.140.53.9

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation_Request.pdf.exe.log

Process:	C:\Users\user\Desktop\Quotation_Request.pdf.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation_Request.pdf.exe.log	
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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

C:\Users\user\AppData\Local\Temp\tmp4108.tmp	
Process:	C:\Users\user\Desktop\Quotation_Request.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.182019841935426
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGZIHtn:cbhK79lNQR/rydbz9I3YODOLNdq3SIN
MD5:	123A817F641F0B9C918EBC19CD3D8201
SHA1:	BB9FFEE5B5B1DFD474A32613AC7E47C7CF3C7B0A
SHA-256:	9AA7AAB06FD028D56A942827538DDDA1F3F3CF38BB4629EEDCB0A614E08F53A5
SHA-512:	16C214D17BC5892D3CE2CA56127B4BE4EED9EE836E96B653482734EB5E496FE156DA9033A5F438B38D6F9395568027D212C15FD7EE92A441235CC23140C2307F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Quotation_Request.pdf.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:At:I
MD5:	9B2EC0D9440BCD7D4CD589581B957612
SHA1:	82648AF473218226F499D59C04621DD5172EC4A4
SHA-256:	7BAF6E6ED1FF241E17C44045ED4A61647BE5C6C044CFCA0074D0FA95484D600D
SHA-512:	E64DD78582CDC26433568BC11F8743C9600381D5AD4843E90FAE35E8457663716131994EBEDA99856AF587B3DE353ED05E533E957884CA88A4BEF8762681B5E2
Malicious:	**true**
Reputation:	low
Preview:	'..5..H

C:\Users\user\AppData\Roaming\mgdPGGmBTUB.exe	
Process:	C:\Users\user\Desktop\Quotation_Request.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	763392
Entropy (8bit):	7.718854206678139
Encrypted:	false
SSDEEP:	12288:M+7v0sCUuWvoXrR9yV2LNaQu4hy/f1oJ4W5erTf+uJTwtrG3:J7v0sCOvwlUV2pzvhy/fA4jSuNwtS3
MD5:	79CD8383F51372C9F0721289F6470889
SHA1:	41B082ACC2C9725DA7C20FF93DC26DF2AB06D1AA
SHA-256:	08ECCE1FB89755FA576A2C1C855BBB0F701EF20C791F56DC0C675FB2A8163691
SHA-512:	94D7101BDBA1B9A8A7D4C420B003505FBA2B731BCA7DF44B75D6A8E4E699141E76130DD2E5FB08A38D27533BAA8DEB4131EF91E59A8D94F40FDB384E408C63C
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 58%

C:\Users\user\AppData\Roaming\mgdPGGmBTUB.exe	
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....i`.....0..... .....@.. ..... ..@.....O..... ..... ..H.....text...$.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....hT..lW.....s.....0.....r...p.+..*..0.....r...p.+..*".(....*...}.....(.....(.....{....o.....*.0..D.....r...p.(.....(.....(.....(....Xs.... .... "...s....(2....*.0..+.....,..{.....+.....,..{....o.....(....*..0.....(...s!....s"...}.....s"...}.....s#...}.....s$...}.....s....}.....s#...}.....s#...}.....{....o%.....(%.....{..... .o&.....{.....A..s....o'.....{....r=..po(.....{.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.718854206678139
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Quotation_Request.pdf.exe
File size:	763392
MD5:	79cd8383f51372c9f0721289f6470889
SHA1:	41b082acc2c9725da7c20ff93dc26df2ab06d1aa
SHA256:	08ecce1fb89755fa576a2c1c855bbb0f701ef20c791f56dc0c675fb2a8163691
SHA512:	94d7101bdba1b9a8a7d4c420b003505fba2b731bca7df44b75d6a8e4e699141e76130dd2e5fb08a38d27533baa8deb4131ef91e59a8d94f40fdb384e408c636c
SSDEEP:	12288:M+7v0sCUuWvoXrR9yV2LNaQu4hy/f1oJ4W5erTf+uJTwtrG3:J7v0sCOvwlUV2pzvhy/fA4jSuNwtS3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....i`.....0..... .....@.. ..... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4bba1e
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:	0x606918F3 [Sun Apr 4 01:40:03 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbb9cc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb9a24	0xb9c00	False	0.855505551817	data	7.72629270512	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x600	0x600	False	0.446614583333	data	4.29278367861	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbc090	0x370	data		
RT_MANIFEST	0xbc410	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

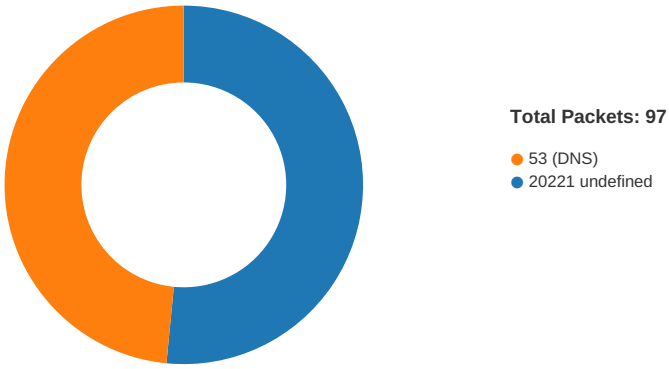
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2015 - 2021
Assembly Version	1.0.0.0
InternalName	VjmG.exe
FileVersion	1.0.0.0
CompanyName	MicroStar Ltd.
LegalTrademarks	
Comments	
ProductName	OnScreen Keyboard
ProductVersion	1.0.0.0
FileDescription	OnScreen Keyboard
OriginalFilename	VjmG.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 15:23:17.607861042 CEST	49726	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:17.653534889 CEST	20221	49726	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:18.159513950 CEST	49726	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:18.206681013 CEST	20221	49726	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:18.722078085 CEST	49726	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:18.767683029 CEST	20221	49726	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:22.912301064 CEST	49727	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:22.958090067 CEST	20221	49727	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:23.472529888 CEST	49727	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:23.518239021 CEST	20221	49727	185.140.53.138	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 15:23:24.019490957 CEST	49727	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:24.065553904 CEST	20221	49727	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:28.083786964 CEST	49728	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:28.130881071 CEST	20221	49728	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:28.644769907 CEST	49728	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:28.690340996 CEST	20221	49728	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:29.191660881 CEST	49728	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:29.237917900 CEST	20221	49728	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:34.825510979 CEST	49736	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:34.871182919 CEST	20221	49736	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:35.470364094 CEST	49736	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:35.517622948 CEST	20221	49736	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:36.098436117 CEST	49736	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:36.148466110 CEST	20221	49736	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:40.223974943 CEST	49740	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:40.269721031 CEST	20221	49740	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:40.770755053 CEST	49740	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:40.818207026 CEST	20221	49740	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:41.333318949 CEST	49740	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:41.379131079 CEST	20221	49740	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:45.444089890 CEST	49744	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:45.489789009 CEST	20221	49744	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:45.989952087 CEST	49744	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:46.035653114 CEST	20221	49744	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:46.552690983 CEST	49744	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:46.598891020 CEST	20221	49744	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:50.793452978 CEST	49745	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:50.839010000 CEST	20221	49745	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:51.349710941 CEST	49745	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:51.395467997 CEST	20221	49745	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:51.896667957 CEST	49745	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:51.942327976 CEST	20221	49745	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:56.617027998 CEST	49759	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:56.662511110 CEST	20221	49759	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:57.165913105 CEST	49759	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:57.211484909 CEST	20221	49759	185.140.53.138	192.168.2.4
Apr 5, 2021 15:23:57.725228071 CEST	49759	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:23:57.771125078 CEST	20221	49759	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:01.773710012 CEST	49766	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:01.819453955 CEST	20221	49766	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:02.335194111 CEST	49766	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:02.380965948 CEST	20221	49766	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:02.897630930 CEST	49766	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:02.943443060 CEST	20221	49766	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:07.315881968 CEST	49772	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:07.361888885 CEST	20221	49772	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:07.866709948 CEST	49772	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:07.912590027 CEST	20221	49772	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:08.413638115 CEST	49772	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:08.461688042 CEST	20221	49772	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:12.535902977 CEST	49773	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:12.581716061 CEST	20221	49773	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:13.086002111 CEST	49773	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:13.131912947 CEST	20221	49773	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:13.633065939 CEST	49773	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:13.678936005 CEST	20221	49773	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:17.761533976 CEST	49774	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:17.807049990 CEST	20221	49774	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:18.321429014 CEST	49774	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:18.367001057 CEST	20221	49774	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:18.867739916 CEST	49774	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:18.913259983 CEST	20221	49774	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:22.917108059 CEST	49775	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:22.963478088 CEST	20221	49775	185.140.53.138	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 15:24:23.477396965 CEST	49775	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:23.523214102 CEST	20221	49775	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:24.024408102 CEST	49775	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:24.070384979 CEST	20221	49775	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:28.088346004 CEST	49776	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:28.134265900 CEST	20221	49776	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:28.634102106 CEST	49776	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:28.680378914 CEST	20221	49776	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:29.180941105 CEST	49776	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:29.226833105 CEST	20221	49776	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:33.230343103 CEST	49777	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:33.276026964 CEST	20221	49777	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:33.790694952 CEST	49777	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:33.836242914 CEST	20221	49777	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:34.337629080 CEST	49777	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:34.383364916 CEST	20221	49777	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:38.723659039 CEST	49780	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:38.769186974 CEST	20221	49780	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:39.275794983 CEST	49780	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:39.321897984 CEST	20221	49780	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:39.822644949 CEST	49780	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:39.869164944 CEST	20221	49780	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:43.950467110 CEST	49781	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:43.996074915 CEST	20221	49781	185.140.53.138	192.168.2.4
Apr 5, 2021 15:24:44.510476112 CEST	49781	20221	192.168.2.4	185.140.53.138
Apr 5, 2021 15:24:44.556098938 CEST	20221	49781	185.140.53.138	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 15:22:57.076585054 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:22:57.125237942 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 5, 2021 15:22:59.392405033 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:22:59.448493004 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:03.734442949 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:03.780448914 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:29.289285898 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:29.335304022 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:29.889949083 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:29.940287113 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:30.207901001 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:30.253878117 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:31.343485117 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:31.389683008 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:32.447273970 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:32.501918077 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:33.731245995 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:33.777529955 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:34.756750107 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:34.813111067 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:35.783266068 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:35.829528093 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:37.072853088 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:37.121520042 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:38.242674112 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:38.301538944 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:40.167418957 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:40.222151041 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:40.305469036 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:40.351671934 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:41.259121895 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:41.320135117 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:42.200365067 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:42.254791975 CEST	53	56627	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 5, 2021 15:23:45.383425951 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:45.442692041 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:50.891860008 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:50.973485947 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:52.725776911 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:52.771982908 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:52.780220032 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:52.834791899 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:52.903156042 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:52.950542927 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:53.297838926 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:53.357070923 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:53.823276043 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:53.857959986 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:53.874413967 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:53.904417992 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:53.945683002 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:53.951051950 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:54.507186890 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:54.561289072 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:55.128628969 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:55.199820995 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:55.218028069 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:55.266834021 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:55.625034094 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:55.681675911 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:56.426668882 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:56.486567020 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:57.087918997 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:57.133943081 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:57.346832037 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:57.404207945 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:57.879070044 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:57.933514118 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:58.190025091 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:58.236191034 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 5, 2021 15:23:59.549933910 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:23:59.599016905 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:00.688536882 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:00.734668970 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:06.148242950 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:06.204612970 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:07.235183001 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:07.292248011 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:12.480107069 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:12.534817934 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:17.702697039 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:17.760065079 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:36.777991056 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:36.823935032 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:38.338413954 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:38.408386946 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:38.664572001 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:38.719062090 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:43.893048048 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:43.947593927 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 5, 2021 15:24:49.140777111 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:24:49.197319984 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 5, 2021 15:25:10.003813982 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 5, 2021 15:25:10.058840036 CEST	53	53418	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 5, 2021 15:23:34.756750107 CEST	192.168.2.4	8.8.8.8	0xa1cd	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:23:40.167418957 CEST	192.168.2.4	8.8.8.8	0x3454	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:23:45.383425951 CEST	192.168.2.4	8.8.8.8	0x5ef3	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:07.235183001 CEST	192.168.2.4	8.8.8.8	0x903a	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:12.480107069 CEST	192.168.2.4	8.8.8.8	0x3c89	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:17.702697039 CEST	192.168.2.4	8.8.8.8	0xeb47	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:38.664572001 CEST	192.168.2.4	8.8.8.8	0xa70b	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:43.893048048 CEST	192.168.2.4	8.8.8.8	0xa719	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:49.140777111 CEST	192.168.2.4	8.8.8.8	0x6998	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 5, 2021 15:25:10.003813982 CEST	192.168.2.4	8.8.8.8	0x22e1	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)

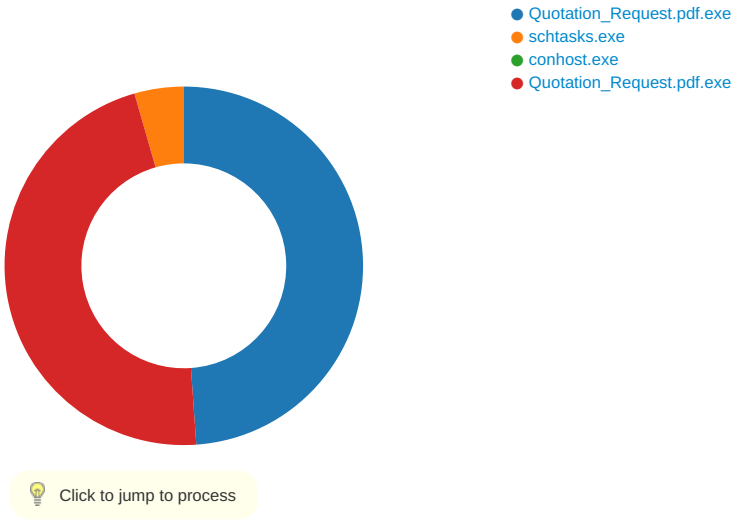
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 5, 2021 15:23:34.813111067 CEST	8.8.8.8	192.168.2.4	0xa1cd	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:23:40.222151041 CEST	8.8.8.8	192.168.2.4	0x3454	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:23:45.442692041 CEST	8.8.8.8	192.168.2.4	0x5ef3	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:07.292248011 CEST	8.8.8.8	192.168.2.4	0x903a	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:12.534817934 CEST	8.8.8.8	192.168.2.4	0x3c89	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:17.760065079 CEST	8.8.8.8	192.168.2.4	0xeb47	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:38.719062090 CEST	8.8.8.8	192.168.2.4	0xa70b	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:43.947593927 CEST	8.8.8.8	192.168.2.4	0xa719	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:24:49.197319984 CEST	8.8.8.8	192.168.2.4	0x6998	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 5, 2021 15:25:10.058840036 CEST	8.8.8.8	192.168.2.4	0x22e1	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Quotation_Request.pdf.exe PID: 6812 Parent PID: 5744

General

Start time:	15:23:02
Start date:	05/04/2021
Path:	C:\Users\user\Desktop\Quotation_Request.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation_Request.pdf.exe'
Imagebase:	0xa50000
File size:	763392 bytes
MD5 hash:	79CD8383F51372C9F0721289F6470889
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.672015342.00000000040A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.672015342.00000000040A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.672015342.00000000040A0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.671468034.0000000003DD9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.671468034.0000000003DD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.671468034.0000000003DD9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6D1CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\mgdPGGmBTUB.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp4108.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation_Request.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4108.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\mgdPGGmBTUB.exe	unknown	763392	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 f3 18 69 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 9c 0b 00 00 08 00 00 00 00 00 00 1e ba 0b 00 00 20 00 00 00 c0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....i`.......... ....0................. ....@.. ....@................	success or wait	1	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4108.tmp	unknown	1644	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation_Request.pdf.exe.log	unknown	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 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",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_v4.0.3	success or wait	1	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\Desktop\Quotation_Request.pdf.exe	unknown	763392	success or wait	1	6C011B4F	ReadFile

Analysis Process: schtasks.exe PID: 7156 Parent PID: 6812

General

Start time:	15:23:13
Start date:	05/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\mgdPGGmBTUB' /XML 'C:\Users\user\AppData\Local\Temp\tmp4108.tmp'
Imagebase:	0x830000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4108.tmp	unknown	2	success or wait	1	83AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4108.tmp	unknown	1645	success or wait	1	83ABD9	ReadFile

Analysis Process: conhost.exe PID: 7164 Parent PID: 7156

General

Start time:	15:23:13
Start date:	05/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Quotation_Request.pdf.exe PID: 6184 Parent PID: 6812

General

Start time:	15:23:14
Start date:	05/04/2021
Path:	C:\Users\user\Desktop\Quotation_Request.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe80000
File size:	763392 bytes
MD5 hash:	79CD8383F51372C9F0721289F6470889
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.915585705.0000000004249000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.915585705.0000000004249000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.910440446.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.910440446.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.910440446.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.912659858.0000000003201000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.917484017.00000000058E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.917484017.00000000058E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.917702828.0000000005AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.917702828.0000000005AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.917702828.0000000005AB0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	27 c8 af f8 35 f8 d8 48	'...5..H	success or wait	1	6C011B4F	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\Desktop\Quotation_Request.pdf.exe	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Users\user\Desktop\Quotation_Request.pdf.exe	unknown	512	success or wait	1	6D18D72F	unknown

Disassembly

Code Analysis