ID: 384939
Sample Name:
URGENTPURCHASEORDER.pdf.exe
Cookbook: default.jbs
Time: 13:21:11
Date: 10/04/2021
Version: 31.0.0 Emerald

Table of Contents

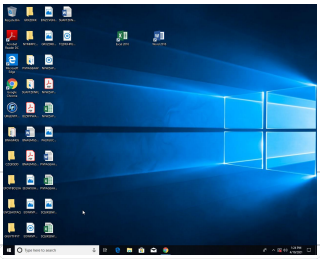
Analysis Report URGENTPURCHASEORDER.pdf.exe

Overview

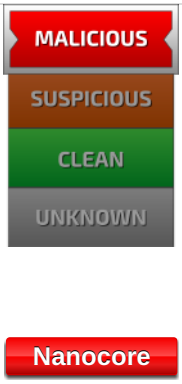
General Information

Sample Name:	URGENTPURCHASEORDER.pdf.exe
Analysis ID:	384939
MD5:	5bee945f3539cde.
SHA1:	5387b06c509be7..
SHA256:	d060635884dda2..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



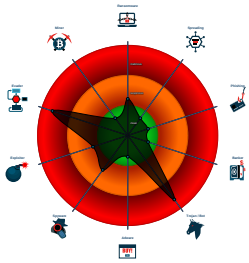
Nanocore

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 subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- URGENTPURCHASEORDER.pdf.exe (PID: 5596 cmdline: 'C:\Users\user\Desktop\URGENTPURCHASEORDER.pdf.exe' MD5: 5BEE945F3539CDE8AB9B042587AA2055)
  - schtasks.exe (PID: 2792 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ewIkYvfY' /XML 'C:\Users\user\AppData\Local\Temp\tmpD681.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6036 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **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
00000004.00000002.481258599.000000000532 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000004.00000002.481258599.000000000532 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000000.00000002.244200976.000000000332 D000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.472813842.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000002.472813842.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.5320000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
4.2.RegSvcs.exe.5320000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
4.2.RegSvcs.exe.3ebb146.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d0af:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d0dc:$x2: IClientNetworkHost
4.2.RegSvcs.exe.3ebb146.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d0af:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e18a:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d0c9:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.3ebb146.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 32 entries				

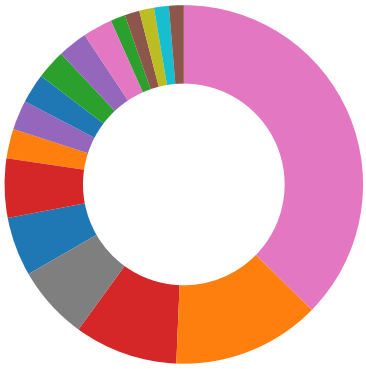
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- 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 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 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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

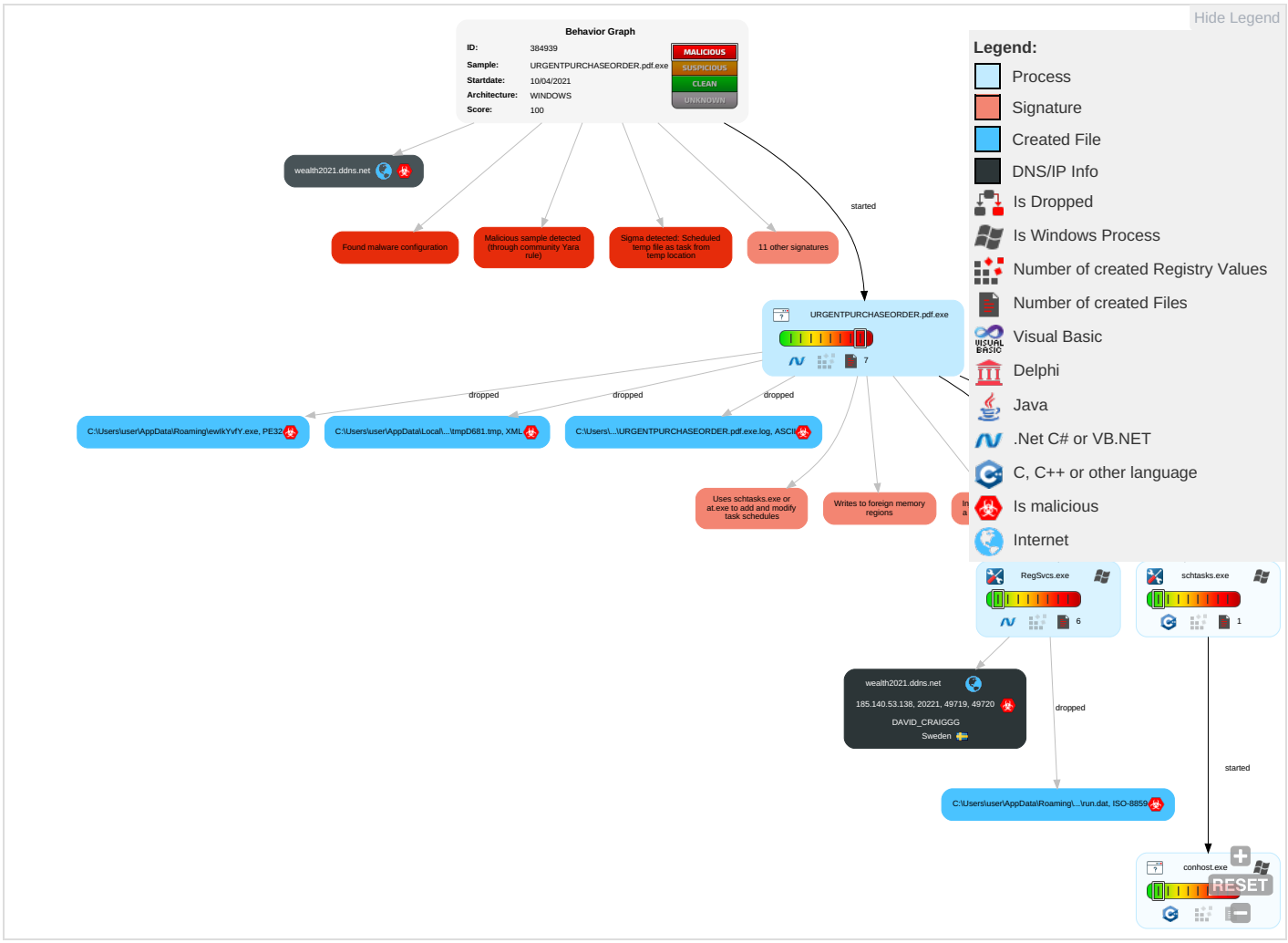
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 2 1 2	Masquerading 1 1	Input Capture 2 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
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	Exploi Redire Calls/S
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	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C 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	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 3	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

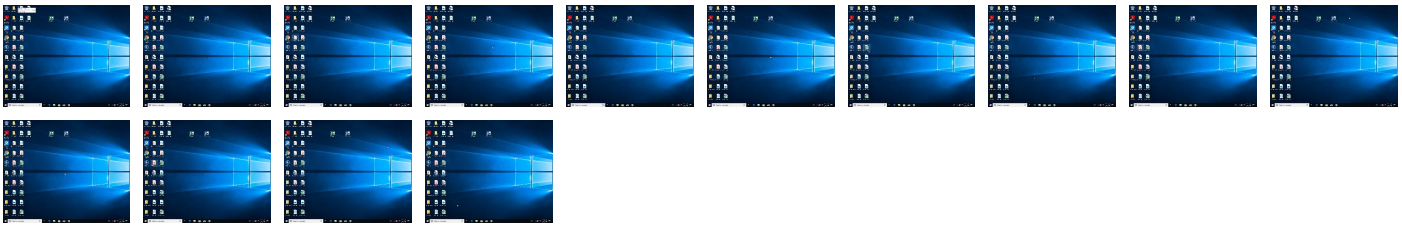
Behavior Graph



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
URGENTPURCHASEORDER.pdf.exe	26%	Virustotal		Browse
URGENTPURCHASEORDER.pdf.exe	14%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ewIkYvfY.exe	14%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.RegSvcs.exe.5330000.8.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.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://discord.gg/uMe7S9Q	0%	Avira URL Cloud	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	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.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.tiro.comlic	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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.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.founder.com.cn/cny	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	

Source	Detection	Scanner	Label	Link
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.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	
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	

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

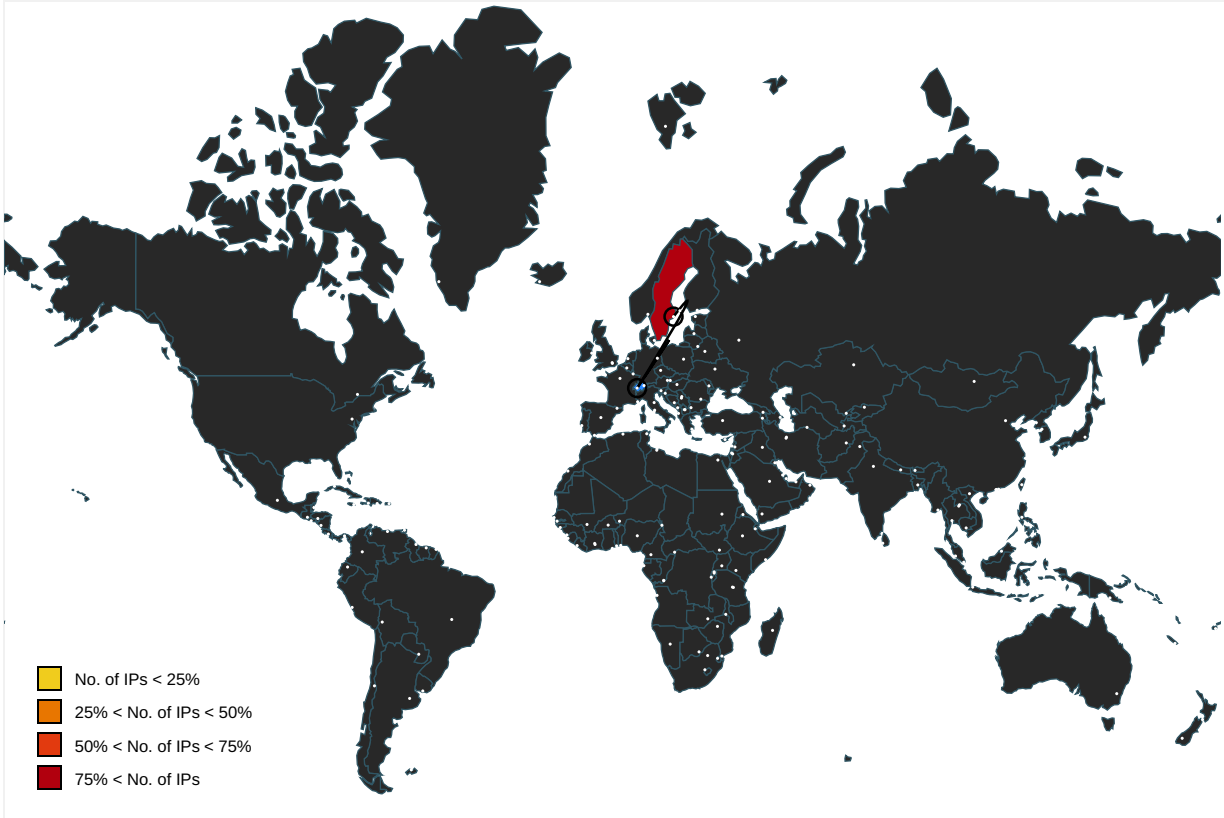
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high
http://www.fonts.comc	URGENTPURCHASEORDER.pdf.exe, 00000000.00000003.207205164.000000629B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://discord.gg/uMe7S9Q	URGENTPURCHASEORDER.pdf.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high
http://www.tiro.comn	URGENTPURCHASEORDER.pdf.exe, 00000000.00000003.208137460.000000629B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/owhenky/IViewBasic5https://discord.gg/uMe7S9QU495374727563747572616C436F6D7061726	URGENTPURCHASEORDER.pdf.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.244242727.0000003378000.00000004.00000001.sdmp	false		high
http://www.tiro.com	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comlic	URGENTPURCHASEORDER.pdf.exe, 00000000.00000003.207529567.000000629B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.243967401.0000001917000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.244200976.000000332D000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp, URGENTPURCHASEORDER.pdf.exe, 00000000.00000003.207529567.000000000629B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cny	URGENTPURCHASEORDER.pdf.exe, 00000000.00000003.209079914.000000628C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false		high
http://www.fonts.com	URGENTPURCHASEORDER.pdf.exe, 00000000.00000003.207232444.000000629B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.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	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.244242727.0000003378000.00000004.00000001.sdmp, URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.244148891.00000000032C1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	URGENTPURCHASEORDER.pdf.exe, 00000000.00000002.251443190.0000007492000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/owhenky/IViewBasic	URGENTPURCHASEORDER.pdf.exe	false		high

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:	384939
Start date:	10.04.2021
Start time:	13:21:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	URGENTPURCHASEORDER.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/5@10/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 45.5% • Quality standard deviation: 45.5%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • 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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 168.61.161.212, 104.43.139.144, 92.122.144.200, 20.82.209.183, 52.255.188.83, 23.10.249.43, 23.10.249.26, 20.54.26.129, 104.83.87.75, 104.83.127.80, 52.147.198.201 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, cdn.onenote.net.edgekey.net, skypedataprdcoleus15.cloudapp.net, wildcard.weather.microsoft.com.edgekey.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, cdn.onenote.net, fs.microsoft.com, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.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
13:22:06	API Interceptor	1x Sleep call for process: URGENTPURCHASEORDER.pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.138	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	
	Quotation_Request.pdf.exe	Get hash	malicious	Browse	
	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	Quotation_Request.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	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	TRACKING UPDATE.exe	Get hash	malicious	Browse	• 185.140.53.10
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	samples ordered 024791.exe	Get hash	malicious	Browse	• 185.140.53.69
	PO.20210704_quick shipment.exe	Get hash	malicious	Browse	• 185.140.53.69
	ANS_309487487_#049844874.exe	Get hash	malicious	Browse	• 185.140.53.9
	tmp2.exe	Get hash	malicious	Browse	• 185.140.53.71
	tmp.exe	Get hash	malicious	Browse	• 185.140.53.71
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	Doc_58YJ54-521DERG701-55YH701.exe	Get hash	malicious	Browse	• 185.140.53.230
	Quotation_Request.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\URGENTPURCHASEORDER.pdf.exe.log	
Process:	C:\Users\user\Desktop\URGENTPURCHASEORDER.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\URGENTPURCHASEORDER.pdf.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpD681.tmp	
Process:	C:\Users\user\Desktop\URGENTPURCHASEORDER.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.189890199243021
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBcYtn:cbh47TlNQ//rydbz9I3YODOLNdq3R
MD5:	12B6114F2BF336F51EE0112E9965540D
SHA1:	F9AABA57DB158925CA36F78C1A0AED4BE36B53B6
SHA-256:	E665058AB5A063BE4A15325C11BD0BCCEE9DDFF7002194F98F79107E06BEA164
SHA-512:	350017E010C9451F94912CEE68146592E259342C0FCBD121515325DA71C95EE3C35781C70703E3A1BB624E42AC3FB0ECD41701C48DF23FA6E3AE65591C13F05A
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:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:4Z9t:UP
MD5:	47BCB235EEA97B8D197D5C4357FC443C
SHA1:	F9720AD5BF18734D11FCEDA8BC5DB233529FB217
SHA-256:	AEDC8DB6758A4EC72C18605F7E428E40E119CCC0E2498FD8384CD7F348B6DF17
SHA-512:	D8CADE74EC2EE405ECA8C47CB67B240BEA2D61EC64C6DAFDBD3A0761CD9BA905649B7DA9F9D52FE33C6B1FE36F04C4A714C79A6CE361DE5A827443CBA5B2E5A
Malicious:	**true**
Reputation:	low
Preview:	..!X^..H

C:\Users\user\AppData\Roaming\ewIkYvfY.exe	
Process:	C:\Users\user\Desktop\URGENTPURCHASEORDER.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	567296
Entropy (8bit):	7.795819523197301
Encrypted:	false
SSDEEP:	12288:0vXIPuU4iLCfVBfMog/U3Ku75fKo11D7wEb3vnKC+nx/sAUF:04o4CfVBf3DV1YETK1n6
MD5:	5BEE945F3539CDE8AB9B042587AA2055
SHA1:	5387B06C509BE731CE77ECAB9719B68A8DE1ACF5
SHA-256:	D060635884DDA22139A083DA8E1CAFF1C05F41F3B3CA36D901894C839E22243D
SHA-512:	4F2E4C621BD0B14F4E86CD6E400A46B9A35ADFB2036D6320EE7959B274B45E7D96C4AFEE5168F13DB6BFE62FEF1A3C5CA1163404C6B90A1B8188E40DA5618B9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 14%
Reputation:	low

C:\Users\user\AppData\Roaming\ewlkYvfY.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.....P..Z...L.....rx... .....@.. ....@..... x..O.....H.....x..... ....H.....text...xX... ...Z..... ..`.rsrc....H.....J...\.....@..@.rel oc.....@..B.....Tx.....H..... .....v..8.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(....o.... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~.....(1.....,!r...p.....(2...o3...s4.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\ewlkYvfY.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\URGENTPURCHASEORDER.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.795819523197301
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:	URGENTPURCHASEORDER.pdf.exe
File size:	567296
MD5:	5bee945f3539cde8ab9b042587aa2055
SHA1:	5387b06c509be731ce77ecab9719b68a8de1acf5
SHA256:	d060635884dda22139a083da8e1caff1c05f41f3b3ca36d901894c839e22243d
SHA512:	4f2e4c621bd0b14f4e86cd6e400a46b9a35adfb2036d6320ee7959b274b45e7d96c4afee5168f13db6bfe62fef1a3c5ca1163404c6b90a1b8188e40da5618b89
SSDEEP:	12288:0vXIPuU4iLCfVBfMog/U3Ku75fKo11D7wEb3vnKC+nx/sAUF:04o4CfVBf3DV1YETK1n6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../.....P..Z...L.....rx... .....@.. ....@.....

File Icon

Icon Hash:	60d088f59092cc31

Static PE Info

General

Entrypoint:	0x487872
Entrypoint Section:	.text
Digitally signed:	false

General

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:	0xEDF3B22F [Tue Jul 3 16:24:15 2096 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x87820	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x88000	0x48fc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x87804	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x85878	0x85a00	False	0.898795603368	data	7.84426548095	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x48fc	0x4a00	False	0.524229307432	data	5.3654546561	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	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_ICON	0x88130	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x8c358	0x14	data		
RT_VERSION	0x8c36c	0x3a4	data		
RT_MANIFEST	0x8c710	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 2019
Assembly Version	1.0.0.0
InternalName	IVectorViewToIBindableVectorViewAdapter.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Image Viewer
ProductVersion	1.0.0.0
FileDescription	Image Viewer
OriginalFilename	IVectorViewToIBindableVectorViewAdapter.exe

Network Behavior

Network Port Distribution

Total Packets: 88

- 53 (DNS)
- 20221 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 13:22:22.287288904 CEST	49719	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:22.308971882 CEST	20221	49719	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:22.820666075 CEST	49719	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:22.843116999 CEST	20221	49719	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:23.343919992 CEST	49719	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:23.365442038 CEST	20221	49719	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:27.464068890 CEST	49720	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:27.485547066 CEST	20221	49720	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:27.993031025 CEST	49720	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:28.014736891 CEST	20221	49720	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:28.524358034 CEST	49720	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:28.545357943 CEST	20221	49720	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:32.557280064 CEST	49728	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:32.578928947 CEST	20221	49728	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:33.087095976 CEST	49728	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:33.108875990 CEST	20221	49728	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:33.622298002 CEST	49728	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:33.645001888 CEST	20221	49728	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:37.795810938 CEST	49732	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:37.817807913 CEST	20221	49732	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:38.509537935 CEST	49732	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:38.530989885 CEST	20221	49732	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:39.197052002 CEST	49732	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:39.218286991 CEST	20221	49732	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:43.254087925 CEST	49733	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:43.275274992 CEST	20221	49733	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:43.806822062 CEST	49733	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:43.828934908 CEST	20221	49733	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:44.509994984 CEST	49733	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:44.531290054 CEST	20221	49733	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:48.558897018 CEST	49734	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:48.579993010 CEST	20221	49734	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:49.197880030 CEST	49734	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:49.220746994 CEST	20221	49734	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:49.807328939 CEST	49734	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:49.828644991 CEST	20221	49734	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:54.730881929 CEST	49736	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:54.752170086 CEST	20221	49736	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:55.307725906 CEST	49736	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:55.328707933 CEST	20221	49736	185.140.53.138	192.168.2.3
Apr 10, 2021 13:22:56.010915995 CEST	49736	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:22:56.032346010 CEST	20221	49736	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:00.044962883 CEST	49738	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:00.065983057 CEST	20221	49738	185.140.53.138	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 13:23:00.573813915 CEST	49738	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:00.594989061 CEST	20221	49738	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:01.105101109 CEST	49738	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:01.126172066 CEST	20221	49738	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:05.139595985 CEST	49739	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:05.160883904 CEST	20221	49739	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:05.668185949 CEST	49739	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:05.689872980 CEST	20221	49739	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:06.199460983 CEST	49739	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:06.220621109 CEST	20221	49739	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:10.290072918 CEST	49741	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:10.311222076 CEST	20221	49741	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:10.824913979 CEST	49741	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:10.845984936 CEST	20221	49741	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:11.356008053 CEST	49741	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:11.376995087 CEST	20221	49741	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:15.455238104 CEST	49749	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:15.477463007 CEST	20221	49749	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:15.981379032 CEST	49749	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:16.002779961 CEST	20221	49749	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:16.512638092 CEST	49749	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:16.533919096 CEST	20221	49749	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:20.637798071 CEST	49755	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:20.659238100 CEST	20221	49755	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:21.169378996 CEST	49755	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:21.190633059 CEST	20221	49755	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:21.700553894 CEST	49755	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:21.721812010 CEST	20221	49755	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:25.736346006 CEST	49756	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:25.759175062 CEST	20221	49756	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:26.263613939 CEST	49756	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:26.284928083 CEST	20221	49756	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:26.794728994 CEST	49756	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:26.815633059 CEST	20221	49756	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:30.844152927 CEST	49757	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:30.865502119 CEST	20221	49757	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:31.373395920 CEST	49757	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:31.395292044 CEST	20221	49757	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:31.904576063 CEST	49757	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:31.927583933 CEST	20221	49757	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:35.938903093 CEST	49758	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:35.961844921 CEST	20221	49758	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:36.467547894 CEST	49758	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:36.488888979 CEST	20221	49758	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:36.998689890 CEST	49758	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:37.019943953 CEST	20221	49758	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:41.084667921 CEST	49759	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:41.105856895 CEST	20221	49759	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:41.608500004 CEST	49759	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:41.630117893 CEST	20221	49759	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:42.139764071 CEST	49759	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:42.160918951 CEST	20221	49759	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:46.200344086 CEST	49760	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:46.221507072 CEST	20221	49760	185.140.53.138	192.168.2.3
Apr 10, 2021 13:23:46.733905077 CEST	49760	20221	192.168.2.3	185.140.53.138
Apr 10, 2021 13:23:46.754827976 CEST	20221	49760	185.140.53.138	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 13:21:53.500550032 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:21:53.513597965 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 10, 2021 13:21:54.275424004 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:21:54.288847923 CEST	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 13:21:54.944519997 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:21:54.957844019 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 10, 2021 13:21:56.026130915 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:21:56.039885998 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 10, 2021 13:21:56.771668911 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:21:56.787292957 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 10, 2021 13:21:57.509826899 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:21:57.522052050 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 10, 2021 13:21:58.361676931 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:21:58.375561953 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 10, 2021 13:21:59.223104000 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:21:59.236020088 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:00.034452915 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:00.047821045 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:00.735707045 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:00.748488903 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:01.573005915 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:01.586170912 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:30.413235903 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:30.440238953 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:31.558715105 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:31.571634054 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:32.466567039 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:32.481575966 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:34.474006891 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:34.486565113 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:36.277395964 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:36.290640116 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:37.038639069 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:37.050949097 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:37.773684025 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:37.793812037 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:43.232366085 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:43.252691984 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:48.545027971 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:48.557930946 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:48.800945044 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:48.820245028 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 10, 2021 13:22:59.667120934 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:22:59.693808079 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:08.325223923 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:08.337743044 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:10.266738892 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:10.286132097 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:10.366518974 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:10.376585007 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:10.384871006 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:10.395803928 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:10.719083071 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:10.731772900 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:11.349730968 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:11.362250090 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:12.461837053 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:12.474558115 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:15.402087927 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:15.415385962 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:16.398881912 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:16.417119026 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:20.551948071 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:20.564553022 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:41.069704056 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:41.082732916 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:46.179269075 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:46.198777914 CEST	53	56338	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 13:23:48.412775040 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:48.424988985 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:50.471694946 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:50.504117012 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 10, 2021 13:23:51.332163095 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:23:51.345220089 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 10, 2021 13:24:11.721404076 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 10, 2021 13:24:11.733901978 CEST	53	62938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 10, 2021 13:22:37.773684025 CEST	192.168.2.3	8.8.8.8	0xcc44	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:22:43.232366085 CEST	192.168.2.3	8.8.8.8	0x9f91	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:22:48.545027971 CEST	192.168.2.3	8.8.8.8	0x686c	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:10.266738892 CEST	192.168.2.3	8.8.8.8	0xd838	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:15.402087927 CEST	192.168.2.3	8.8.8.8	0xee14	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:20.551948071 CEST	192.168.2.3	8.8.8.8	0x1cc4	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:41.069704056 CEST	192.168.2.3	8.8.8.8	0xc65a	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:46.179269075 CEST	192.168.2.3	8.8.8.8	0xd121	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:51.332163095 CEST	192.168.2.3	8.8.8.8	0xa7be	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)
Apr 10, 2021 13:24:11.721404076 CEST	192.168.2.3	8.8.8.8	0xac05	Standard query (0)	wealth2021 .ddns.net	A (IP address)	IN (0x0001)

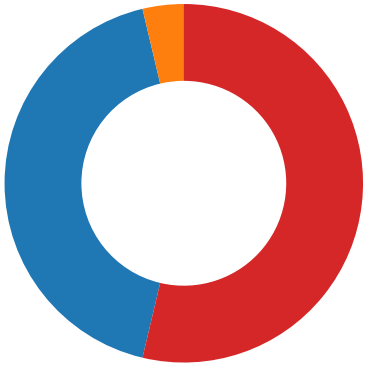
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 10, 2021 13:22:37.793812037 CEST	8.8.8.8	192.168.2.3	0xcc44	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:22:43.252691984 CEST	8.8.8.8	192.168.2.3	0x9f91	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:22:48.557930946 CEST	8.8.8.8	192.168.2.3	0x686c	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:10.286132097 CEST	8.8.8.8	192.168.2.3	0xd838	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:15.415385962 CEST	8.8.8.8	192.168.2.3	0xee14	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:20.564553022 CEST	8.8.8.8	192.168.2.3	0x1cc4	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:41.082732916 CEST	8.8.8.8	192.168.2.3	0xc65a	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:46.198777914 CEST	8.8.8.8	192.168.2.3	0xd121	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:23:51.345220089 CEST	8.8.8.8	192.168.2.3	0xa7be	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Apr 10, 2021 13:24:11.733901978 CEST	8.8.8.8	192.168.2.3	0xac05	No error (0)	wealth2021 .ddns.net		185.140.53.138	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: URGENTPURCHASEORDER.pdf.exe PID: 5596 Parent PID: 5716

General

Start time:	13:22:01
Start date:	10/04/2021
Path:	C:\Users\user\Desktop\URGENTPURCHASEORDER.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\URGENTPURCHASEORDER.pdf.exe'
Imagebase:	0xeb0000
File size:	567296 bytes
MD5 hash:	5BEE945F3539CDE8AB9B042587AA2055
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: 00000000.00000002.244200976.000000000332D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.244541522.00000000042CC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.244541522.00000000042CC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.244541522.00000000042CC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming\ewIkYvfY.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\ewIkYvfY.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF4DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD681.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF47038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\URGENTPURCHASEORDER.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD681.tmp	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ewIkYvfY.exe	0	262144	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 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 2f b2 f3 ed 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 5a 08 00 00 4c 00 00 00 00 00 00 72 78 08 00 00 20 00 00 00 80 08 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 09 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.../............ ....P..Z...L......rx... ....@.. ....@.................	success or wait	3	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\ewIkYvfY.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CF4DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD681.tmp	unknown	1641	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 68 61 72 64 7a 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	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\URGENTPURCHASEORDER.pdf.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: schtasks.exe PID: 2792 Parent PID: 5596

General

Start time:	13:22:16
Start date:	10/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ewIkYvfY' /XML 'C:\Users \user\AppData\Local\Temp\tmpD681.tmp'
Imagebase:	0x3e0000
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\tmpD681.tmp	unknown	2	success or wait	1	3EAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD681.tmp	unknown	1642	success or wait	1	3EABD9	ReadFile

Analysis Process: conhost.exe PID: 1724 Parent PID: 2792

General

Start time:	13:22:18
Start date:	10/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: RegSvcs.exe PID: 6036 Parent PID: 5596

General

Start time:	13:22:18
Start date:	10/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xa00000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000004.00000002.481258599.0000000005320000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.481258599.0000000005320000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.472813842.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.472813842.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.472813842.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.476797525.0000000002E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.480543359.0000000003EAC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.480543359.0000000003EAC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.481272072.0000000005330000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.481272072.0000000005330000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.481272072.0000000005330000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

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	6E0FCF06	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	6E0FCF06	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	6CF4BEFF	CreateDirectoryW
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	6CF41E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CF4BEFF	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	6CF4BEFF	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	d6 0c 21 58 5e fc d8 48	..!X^..H	success or wait	1	6CF41B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	4096	success or wait	1	6E0BD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	512	success or wait	1	6E0BD72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6E0D5705	unknown

Disassembly

Code Analysis