ID: 323892
Sample Name: Proforma Invoice with Bank Details_pdf.exe
Cookbook: default.jbs
Time: 18:48:08
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

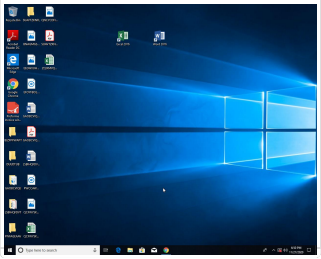
Analysis Report Proforma Invoice with Bank Details_pd…

Overview

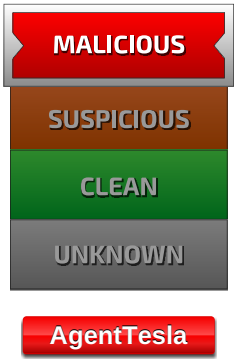
General Information

Sample Name:	Proforma Invoice with Bank Details_pdf.exe
Analysis ID:	323892
MD5:	8816ae2d440c50..
SHA1:	210289b9df203f8..
SHA256:	d2146d63100b68..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

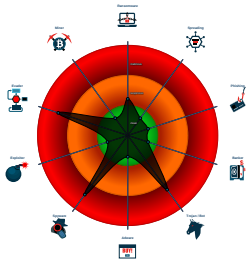


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Sigma detected: MSBuild connects …
- Yara detected AgentTesla
- .NET source code contains potentia…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- Proforma Invoice with Bank Details_pdf.exe (PID: 6672 cmdline: 'C:\Users\user\Desktop\Proforma Invoice with Bank Details_pdf.exe' MD5: 8816AE2D440C50E7EC52BE21AE6E2B22)
  - conhost.exe (PID: 6680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6736 cmdline: cmd /c schtasks /Create /TN name /XML 'C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - schtasks.exe (PID: 6756 cmdline: schtasks /Create /TN name /XML 'C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml' MD5: 15FF7D8324231381BAD48A052F85DF04)
  - MSBuild.exe (PID: 6744 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe MD5: 88BBB7610152B48C2B3879473B17857E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "umfkxJ05b",
  "URL: ": "http://AAETsHFcmz5EiUda3E.net",
  "To: ": "",
  "ByHost: ": "mail.hybridgroupco.com:587",
  "Password: ": "IvIoSkuTkG",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.473024653.0000000002C01000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.209201167.0000000000C66000.00000004.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.473614554.0000000002CCE000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.469545862.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.474100533.0000000002DA4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Unpacked PEs

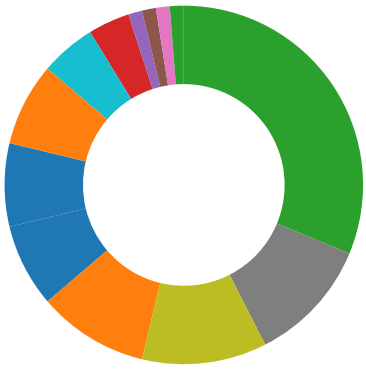
Source	Rule	Description	Author	Strings
0.2.Proforma Invoice with Bank Details_pdf.exe.c40000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: MSBuild connects to smtp port

Signature Overview



- AV Detection
- Networking
- 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 domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

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

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

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:

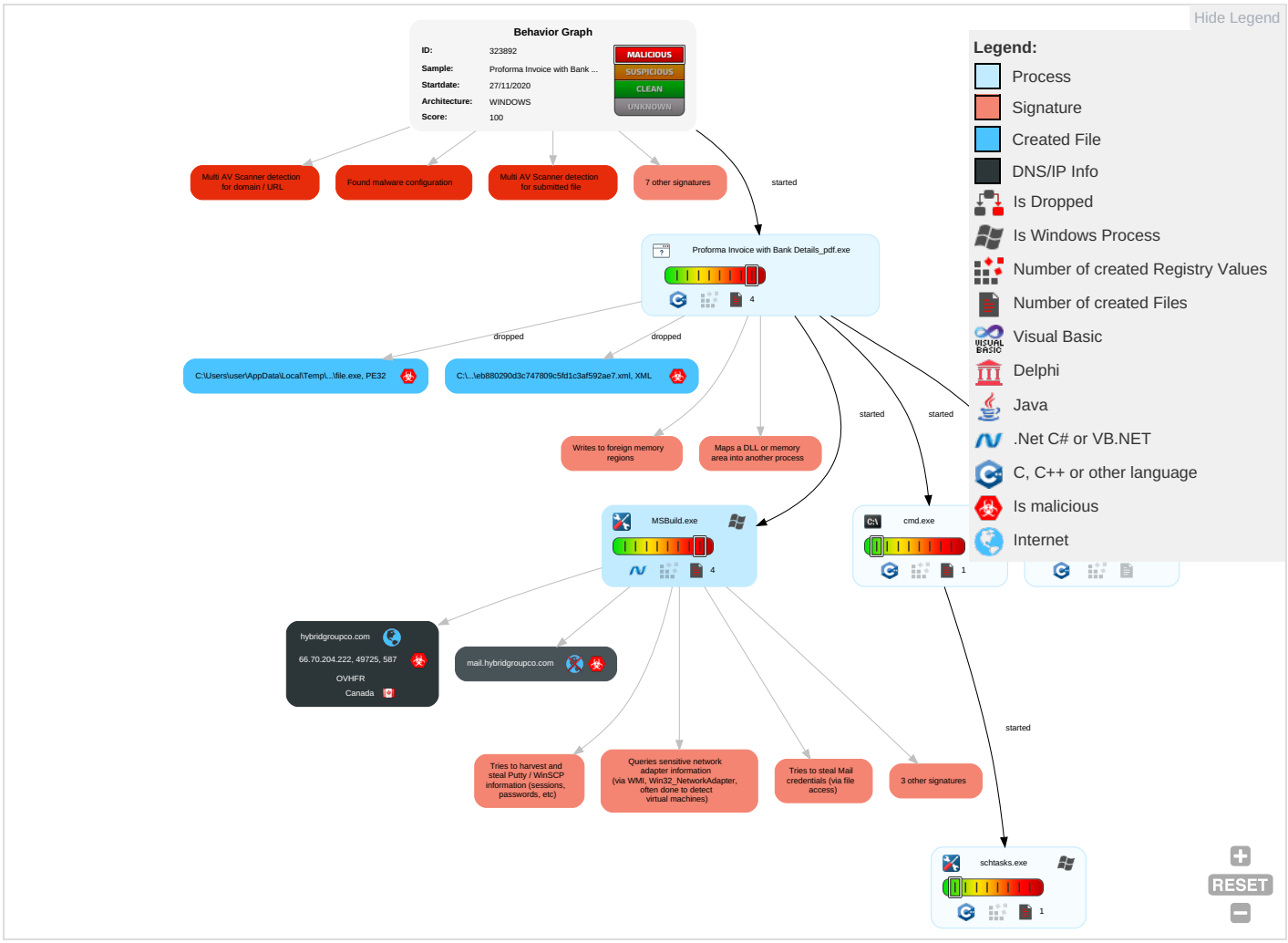
Yara detected AgentTesla

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 2 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 3 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Security Software Discovery 1 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 2 1 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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

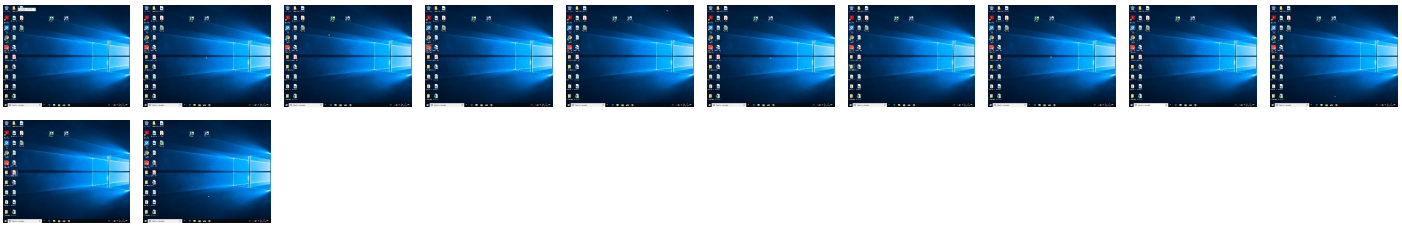
Behavior Graph



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
Proforma Invoice with Bank Details_pdf.exe	31%	Virustotal		Browse
Proforma Invoice with Bank Details_pdf.exe	27%	ReversingLabs		
Proforma Invoice with Bank Details_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\folder\file.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
hybridgroupco.com	0%	Virustotal		Browse
mail.hybridgroupco.com	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:	0%	Virustotal		Browse
http://127.0.0.1:	0%	Avira URL Cloud	safe	
http://AAETsHFcmz5EiUda3E.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	0%	URL Reputation	safe	
http://AAETsHFcmz5EiUda3E.net0	0%	Avira URL Cloud	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

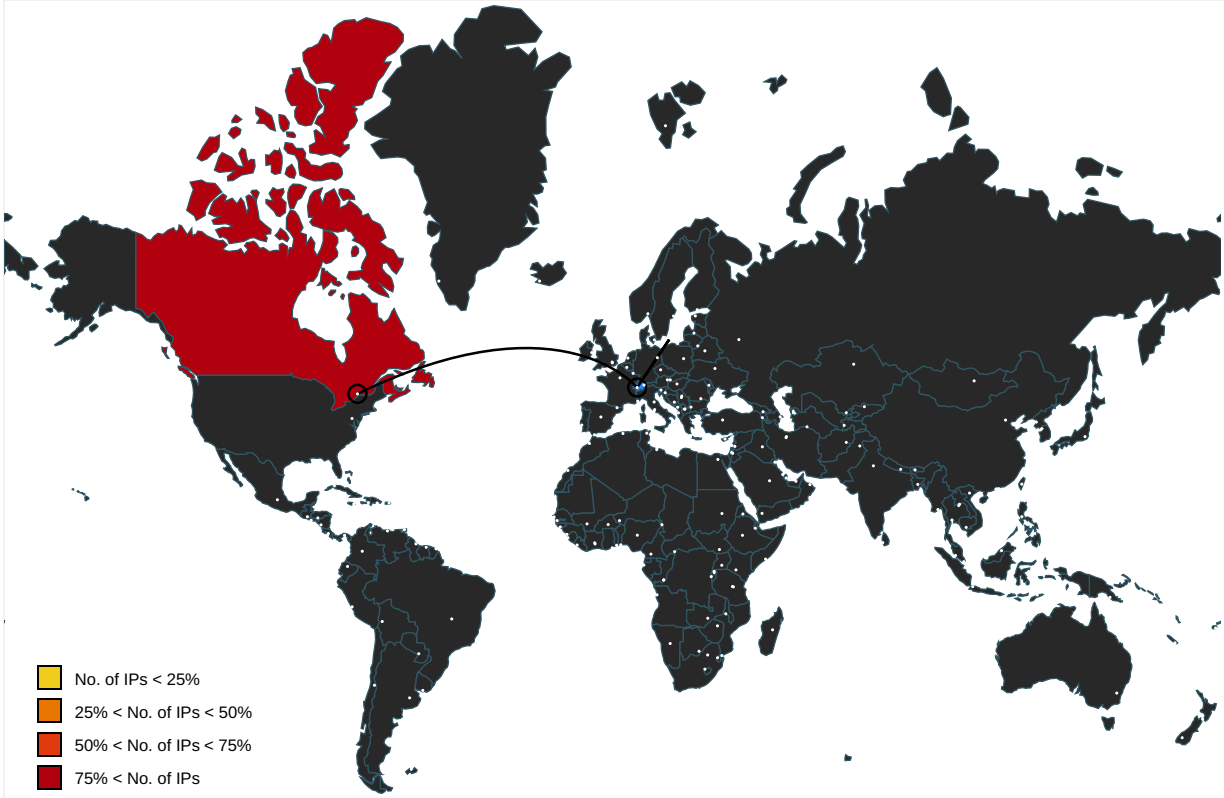
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hybridgroupco.com	66.70.204.222	true	true	• 0%, Virustotal, Browse	unknown
mail.hybridgroupco.com	unknown	unknown	true	• 10%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:	Proforma Invoice with Bank Details_pdf.exe, Proforma Invoice with Bank Details_pdf.exe, 00000000.00000002.209201167.0000000000C66000.00000004.00020000.sdmp, MSBuild.exe, 00000003.00000002.469545862.000000000402000.00000040.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://AAETsHFcmz5EiUda3E.net	MSBuild.exe, 00000003.00000002.474100533.0000000002DA4000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/	Proforma Invoice with Bank Details_pdf.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/U	Proforma Invoice with Bank Details_pdf.exe, 00000000.00000002.209201167.0000000000C66000.00000004.00020000.sdmp, MSBuild.exe, 00000003.00000002.469545862.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://AAETsHFcmz5EiUda3E.net0	MSBuild.exe, 00000003.00000002.473614554.0000000002CCE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	Proforma Invoice with Bank Details_pdf.exe, Proforma Invoice with Bank Details_pdf.exe, 00000000.00000002.209201167.0000000000C66000.00000004.00020000.sdmp, MSBuild.exe, 00000003.00000002.469545862.000000000402000.00000040.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Proforma Invoice with Bank Details_pdf.exe, MSBuild.exe, 00000003.00000002.469545862.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	unknown	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323892
Start date:	27.11.2020
Start time:	18:48:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Invoice with Bank Details_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:	25
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@8/2@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 76.1% (good quality ratio 71.3%) • Quality average: 81.5% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 82% • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.42.151.234, 51.104.139.180, 104.80.23.128, 20.54.26.129, 2.20.142.210, 2.20.142.209, 92.122.213.247, 92.122.213.194, 13.88.21.125, 51.104.144.132 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:49:14	API Interceptor	895x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	Image001.exe	Get hash	malicious	Browse	
	4nfg3g3nwg.exe	Get hash	malicious	Browse	
	DOC04121993.exe	Get hash	malicious	Browse	
	PI.exe	Get hash	malicious	Browse	
	d9f83622ec1564600202a937d2414af8.exe	Get hash	malicious	Browse	
	Image001.exe	Get hash	malicious	Browse	
	mEPbT6Dbzc.exe	Get hash	malicious	Browse	
	b32sUgpVdT.exe	Get hash	malicious	Browse	
	ZXeB2BO1Lq.exe	Get hash	malicious	Browse	
	kiGANMAmR3.exe	Get hash	malicious	Browse	
	QM34U1x8I6.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Y2UrKCOaJm.exe	Get hash	malicious	Browse	
	SJAOO8OCe3.exe	Get hash	malicious	Browse	
	zh7966Pn0l.exe	Get hash	malicious	Browse	
	o7B4zT1WNb.exe	Get hash	malicious	Browse	
	emMAbUc8Xg.exe	Get hash	malicious	Browse	
	a2onj1GOHs.exe	Get hash	malicious	Browse	
	RDp6VoVSfQ.exe	Get hash	malicious	Browse	
	DUE_INVOICE.exe	Get hash	malicious	Browse	
	2M3ZdRze7b.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.51
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 145.239.131.55
	http://https://mincast.us-south.cf.appdomain.cloud/redirect/?email=prampon@soteb.fr	Get hash	malicious	Browse	• 149.56.20.211
	Image001.exe	Get hash	malicious	Browse	• 66.70.204.222
	4nfg3g3nwg.exe	Get hash	malicious	Browse	• 66.70.204.222
	due-invoice.xlsm	Get hash	malicious	Browse	• 87.98.154.146
	SHIPPING DOCUMENT & PACKING LIST.exe	Get hash	malicious	Browse	• 51.75.130.83
	anthon.exe	Get hash	malicious	Browse	• 51.38.230.18
	ORDER-207044.xLs.exe	Get hash	malicious	Browse	• 54.37.36.116
	Bulk Order - 1017C.exe	Get hash	malicious	Browse	• 51.75.130.83
	SWIFT Transfer (103) W071323.exe	Get hash	malicious	Browse	• 51.75.130.83
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 87.98.154.146
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 51.77.152.34
	tarifvertrag_igbce_weihnachtsgeld_k#U00fcndigung.js	Get hash	malicious	Browse	• 51.77.152.34
	Invoice_Payment Form_948792.xlsm	Get hash	malicious	Browse	• 213.186.33.40
	0151-83872-976-67-83872.htm	Get hash	malicious	Browse	• 51.210.112.129
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• 92.222.121.127
	PAYMENT ADVISE.exe	Get hash	malicious	Browse	• 51.75.130.83
	http://https://eti-salat.com/x/	Get hash	malicious	Browse	• 145.239.6.126
	index.html	Get hash	malicious	Browse	• 139.99.124.57

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml

Process:	C:\Users\user\Desktop\Proforma Invoice with Bank Details_pdf.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1287
Entropy (8bit):	5.224351566085788
Encrypted:	false
SSDEEP:	24:2do4+S8TcqdqMhrKOgFwvaPIrovlgU3ODOiIQRvh7hwZgvw43aVdyL3Tbn:c+XBqMhGeaPIrovl33ODOiLdKZgfoILv
MD5:	4E45BCEC6ED11BB2765703CA8CA4A469
SHA1:	2D2060D24EAA8352FB02AD6106E782CE62E195D1
SHA-256:	381A73DEBD630FB0411220156217C871B931452D7915FE81EF73091A8B9A5214
SHA-512:	3A9DC709E42584ACAF300EB9D0985EE39CABDF06A8327A8475417A54277DCCF66AF127185374117335A11280C7C5A0281D87F708379582DF03944DB0C3ED4488
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml	
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>2015-09-27T14:27:44.8929027</Date > .<Author>142233\user</Author>.</RegistrationInfo>.<Triggers>.<LogonTrigger>.<Enabled>true</Enabled>.<UserId>142233\user</UserId>.</LogonTrigger>.<RegistrationTrigger>.<Enabled>false</Enabled>.</RegistrationTrigger>.</Triggers>.<Principals>.<Principal id="Author">.<UserId>142233\user</UserId>.<LogonType>InteractiveToken</LogonType>.<RunLevel>LeastPrivilege</RunLevel>.</Principal>.</Principals>.<Settings>.<MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.<AllowHardTerminate>false</AllowHardTerminate>.<StartWhenAvailable>true</StartWhenAvailable>.<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.<IdleSettings>.<StopOnIdleEnd>true</StopOnIdleEnd>.<RestartOnIdle>false</RestartOnIdle>.</IdleSettings>.<AllowStartOnDemand>true</AllowStartOnDemand>.<Enabled>true</Enabled>.<Hidden>fals

C:\Users\user\AppData\Local\Temp\folder\file.exe	
Process:	C:\Users\user\Desktop\Proforma Invoice with Bank Details_pdf.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	626186
Entropy (8bit):	7.525138445631881
Encrypted:	false
SSDEEP:	12288:SrRqJJ1rAfoG1WFn4LJ6zuTlq3v9+s9tlgGKwE:QRq1rAsGEzwq3v9+s9tLi
MD5:	029A3195D923405E8017102F90346E1E
SHA1:	EB670BBD759C268B547E3397A0AED30C515CCF17
SHA-256:	6713DB52BAFE0DE00F0F03ED9A1618ABE5946105DAECF10938323E12CE41FA7F
SHA-512:	4FA94F113D0F75108709F33629B6EB3BCD517762BF14CF164F7D4D0E7A71DA96F7A62F3F44DD6D101BC83E763FA9CA4BEBD9C6066A87FF8CEF30B69D8AE17CD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Km.Km.Km..>.Rm..<..m..=..m.Km..m..J.Xm.l. .Jm.l.:.Jm.Kmd.Jm.l.?.Jm.RichKm.....PE..L...G..._.....b...X.....?H.....@.....@.....h.....p.....@.....text...9a.....b..... ..`.rdata...c.....d...f.....@..@.data.....h.....@....rsrc.....2.....@..@.reloc.....p.....@..B.....

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.5252045251493005
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Proforma Invoice with Bank Details_pdf.exe
File size:	626176
MD5:	8816ae2d440c50e7ec52be21ae6e2b22
SHA1:	210289b9df203f83f263fe2530aa28c078b8d6c1
SHA256:	d2146d63100b68c87046aa63c8e5b73a8893e171f24c3500070005ccea0eaacd
SHA512:	3f0f5c577025b60e219fcc64e20d1294ed74d3fd80006130e56d30f2fbacd80e7da112649e52892db6a977d25ae5abe3f856176e226dc0f891a96deb044cc1a
SSDEEP:	12288:SrRqJJ1rAfoG1WFn4LJ6zuTlq3v9+s9tlgGKwE:QRq1rAsGEzwq3v9+s9tLi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Km..Km..Km....>.Rm....<..m....=..m..Km...m....J.Xm..l. .Jm..l.:.Jm..Kmd.Jm..l.?.Jm..RichKm.....PE..L..

File Icon

Icon Hash:	f0f06094c36ee8c2

Static PE Info

General

Entrypoint:	0x40483f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FC0D847 [Fri Nov 27 10:43:19 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	be74bcf76a56fe7a35a0a7f280acf926

Entrypoint Preview

Instruction
call 00007FD71CEDB463h
jmp 00007FD71CED3D3Ch
call 00007FD71CEDA0C7h
mov edx, eax
mov eax, dword ptr [edx+6Ch]
cmp eax, dword ptr [0041FC94h]
je 00007FD71CED3EC2h
mov ecx, dword ptr [0041FD54h]
test dword ptr [edx+70h], ecx
jne 00007FD71CED3EB7h
call 00007FD71CED9EACh
mov eax, dword ptr [eax+04h]
ret
call 00007FD71CEDA0A1h
mov edx, eax
mov eax, dword ptr [edx+6Ch]
cmp eax, dword ptr [0041FC94h]
je 00007FD71CED3EC2h
mov ecx, dword ptr [0041FD54h]
test dword ptr [edx+70h], ecx
jne 00007FD71CED3EB7h
call 00007FD71CED9E86h
add eax, 000000A0h
ret
push ebp
mov ebp, esp
sub esp, 44h
mov eax, dword ptr [0041F9B8h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
push ebx
xor ebx, ebx
push esi
mov esi, dword ptr [ebp+08h]
mov dword ptr [ebp-2Ch], ebx
mov eax, dword ptr [esi+000000A8h]
mov dword ptr [ebp-20h], ebx
mov dword ptr [ebp-24h], ebx
mov dword ptr [ebp-1Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-44h], esi

Instruction
mov dword ptr [ebp-40h], ebx
test eax, eax
je 00007FD71CED41C2h
push edi
lea edi, dword ptr [esi+04h]
cmp dword ptr [edi], ebx
jne 00007FD71CED3ECEh
push edi
push 00001004h
push eax
lea eax, dword ptr [ebp-44h]
push ebx
push eax
call 00007FD71CEDA928h
add esp, 14h
test eax, eax
jne 00007FD71CED416Ah
push 00000004h
call 00007FD71CED7295h
push 00000002h
push 00000180h
mov dword ptr [ebp-2Ch], eax

Rich Headers

Programming Language:	• [RES] VS2012 build 50727 • [LNK] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1d868	0xc8	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x89000	0xd4b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x97000	0x1484	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x1c520	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x18000	0x204	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16139	0x16200	False	0.572232521186	data	6.66933993297	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x63ba	0x6400	False	0.3630859375	data	4.86039745717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x69684	0x66800	False	0.987345179116	data	7.98736576468	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0xd4b0	0xd600	False	0.080917786215	data	3.628789833	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x97000	0x8594	0x8600	False	0.125670475746	data	1.56501104284	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x890f0	0xd228	data	English	United States
RT_GROUP_ICON	0x96318	0x14	data	English	United States
RT_MANIFEST	0x96330	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	HeapReAlloc, EnumSystemLocalesEx, IsValidLocaleName, LCMapStringEx, GetUserDefaultLocaleName, GetModuleHandleW, TerminateProcess, GetCurrentProcess, LoadLibraryExW, FlsSetValue, FlsGetValue, FlsAlloc, SetUnhandledExceptionFilter, UnhandledExceptionFilter, SetFilePointerEx, ReadFile, GetConsoleMode, GetConsoleCP, FlushFileBuffers, CloseHandle, GetOEMCP, GetACP, IsValidCodePage, FreeEnvironmentStringsW, OutputDebugStringW, LoadLibraryW, SetStdHandle, WriteConsoleW, ReadConsoleW, CreateFileW, VirtualProtect, FlsFree, GetEnvironmentStringsW, GetTickCount64, GetSystemTimeAsFileTime, QueryPerformanceCounter, GetModuleFileNameA, GetStartupInfoW, InitOnceExecuteOnce, WideCharToMultiByte, InterlockedIncrement, InterlockedDecrement, EncodePointer, DecodePointer, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSectionEx, DeleteCriticalSection, Sleep, GetLocaleInfoEx, MultiByteToWideChar, GetStringTypeW, GetLastError, HeapFree, GetCommandLineA, GetCPInfo, RaiseException, RtlUnwind, HeapAlloc, InitializeCriticalSectionAndSpinCount, IsProcessorFeaturePresent, IsDebuggerPresent, GetProcessHeap, SetLastError, GetCurrentThreadId, ExitProcess, GetModuleHandleExW, GetProcAddress, HeapSize, GetStdHandle, WriteFile, GetModuleFileNameW, GetFileType
MSWSOCK.dll	s_perror, rexec, rcmd, GetNameByTypeW, EnumProtocolsW, dn_expand
SETUPAPI.dll	SetupQueryInfFileInformationW, SetupGetInfFileListA, SetupQueueDeleteA
MPR.dll	MultinetGetConnectionPerformanceA, WNetConnectionDialog1A, WNetGetResourceParentA, MultinetGetConnectionPerformanceW, WNetGetUserW
WINMM.dll	timeEndPeriod, timeKillEvent, mmioFlush, midiStreamOut, joySetCapture, midiInStart
pdh.dll	PdhVbGetCounterPathElements, PdhRemoveCounter, PdhEnumObjectItemsW, PdhOpenQueryA, PdhVbIsGoodStatus, PdhGetLogFileSize
msi.dll	
GDI32.dll	SetMagicColors, EnumFontFamiliesExW, CreateRectRgn, RemoveFontMemResourceEx, EudcUnloadLinkW, CreateCompatibleBitmap, CreateFontIndirectA, ScaleViewportExtEx, CreatePatternBrush, CreateICW
MAPI32.dll	

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 73

- 53 (DNS)
- 80 (HTTP)
- 587 undefined
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 18:49:16.637509108 CET	49679	443	192.168.2.3	13.83.66.189

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 18:49:16.637701035 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.683197975 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.683275938 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.808008909 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.808058023 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.808098078 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.808145046 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.808186054 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.808206081 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.822509050 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.822563887 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.822581053 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.822616100 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.822652102 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.822701931 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.822729111 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.822778940 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.822802067 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.822850943 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.822865963 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.822911024 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.822930098 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.822985888 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.823029995 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.823081017 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.823107004 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.823151112 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.823170900 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.853338003 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.853439093 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.853486061 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.853533983 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.853554964 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.853593111 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.853641033 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.869080067 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869136095 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869203091 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.869235039 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869323969 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869373083 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.869437933 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869491100 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869558096 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.869591951 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869651079 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869699001 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:16.869723082 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869796038 CET	443	49679	13.83.66.189	192.168.2.3
Nov 27, 2020 18:49:16.869844913 CET	49679	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:49:35.606722116 CET	49725	587	192.168.2.3	66.70.204.222
Nov 27, 2020 18:49:35.712296009 CET	587	49725	66.70.204.222	192.168.2.3
Nov 27, 2020 18:49:35.712419987 CET	49725	587	192.168.2.3	66.70.204.222
Nov 27, 2020 18:49:35.944700003 CET	587	49725	66.70.204.222	192.168.2.3
Nov 27, 2020 18:49:35.945132971 CET	49725	587	192.168.2.3	66.70.204.222
Nov 27, 2020 18:49:36.050761938 CET	587	49725	66.70.204.222	192.168.2.3
Nov 27, 2020 18:49:36.051378012 CET	49725	587	192.168.2.3	66.70.204.222
Nov 27, 2020 18:49:36.110667944 CET	49725	587	192.168.2.3	66.70.204.222
Nov 27, 2020 18:49:36.158169031 CET	587	49725	66.70.204.222	192.168.2.3
Nov 27, 2020 18:49:36.159563065 CET	49725	587	192.168.2.3	66.70.204.222
Nov 27, 2020 18:49:36.216675043 CET	587	49725	66.70.204.222	192.168.2.3
Nov 27, 2020 18:49:36.216753006 CET	49725	587	192.168.2.3	66.70.204.222
Nov 27, 2020 18:49:36.615303993 CET	80	49689	104.108.38.112	192.168.2.3
Nov 27, 2020 18:49:36.617043018 CET	49689	80	192.168.2.3	104.108.38.112

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 18:49:36.617099047 CET	49689	80	192.168.2.3	104.108.38.112
Nov 27, 2020 18:49:36.633902073 CET	80	49689	104.108.38.112	192.168.2.3
Nov 27, 2020 18:49:38.803575993 CET	80	49680	205.185.216.10	192.168.2.3
Nov 27, 2020 18:49:38.803857088 CET	49680	80	192.168.2.3	205.185.216.10
Nov 27, 2020 18:49:40.108978033 CET	80	49683	93.184.220.29	192.168.2.3
Nov 27, 2020 18:49:40.109314919 CET	49683	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:49:40.319173098 CET	80	49684	93.184.220.29	192.168.2.3
Nov 27, 2020 18:49:40.319333076 CET	49684	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:49:40.563829899 CET	49688	443	192.168.2.3	104.108.60.202
Nov 27, 2020 18:49:40.584395885 CET	443	49688	104.108.60.202	192.168.2.3
Nov 27, 2020 18:49:40.584429026 CET	443	49688	104.108.60.202	192.168.2.3
Nov 27, 2020 18:49:40.584531069 CET	49688	443	192.168.2.3	104.108.60.202
Nov 27, 2020 18:49:40.584580898 CET	49688	443	192.168.2.3	104.108.60.202
Nov 27, 2020 18:49:40.735589981 CET	80	49687	93.184.220.29	192.168.2.3
Nov 27, 2020 18:49:40.735716105 CET	49687	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:49:41.575989962 CET	80	49682	93.184.220.29	192.168.2.3
Nov 27, 2020 18:49:41.576338053 CET	49682	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:49:41.897706985 CET	49693	443	192.168.2.3	104.80.21.45
Nov 27, 2020 18:49:41.898313999 CET	49694	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:49:43.322161913 CET	49697	443	192.168.2.3	204.79.197.200
Nov 27, 2020 18:49:43.322335005 CET	49696	443	192.168.2.3	204.79.197.200
Nov 27, 2020 18:50:29.458873987 CET	49682	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:50:29.459007025 CET	49678	443	192.168.2.3	13.83.66.189
Nov 27, 2020 18:50:29.459096909 CET	49683	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:50:29.459163904 CET	49680	80	192.168.2.3	205.185.216.10
Nov 27, 2020 18:50:29.459284067 CET	49681	80	192.168.2.3	67.27.233.126
Nov 27, 2020 18:50:29.475214005 CET	80	49682	93.184.220.29	192.168.2.3
Nov 27, 2020 18:50:29.475243092 CET	80	49683	93.184.220.29	192.168.2.3
Nov 27, 2020 18:50:29.475353956 CET	49682	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:50:29.475466013 CET	49683	80	192.168.2.3	93.184.220.29
Nov 27, 2020 18:50:29.480077982 CET	80	49681	67.27.233.126	192.168.2.3
Nov 27, 2020 18:50:29.480241060 CET	49681	80	192.168.2.3	67.27.233.126
Nov 27, 2020 18:50:29.481194973 CET	80	49680	205.185.216.10	192.168.2.3
Nov 27, 2020 18:50:29.481340885 CET	49680	80	192.168.2.3	205.185.216.10
Nov 27, 2020 18:50:29.520664930 CET	49679	443	192.168.2.3	13.83.66.189

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 18:48:50.724462986 CET	60831	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:48:50.751859903 CET	53	60831	8.8.8.8	192.168.2.3
Nov 27, 2020 18:48:51.523782969 CET	60100	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:48:51.550929070 CET	53	60100	8.8.8.8	192.168.2.3
Nov 27, 2020 18:48:52.340898037 CET	53195	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:48:52.368297100 CET	53	53195	8.8.8.8	192.168.2.3
Nov 27, 2020 18:48:53.460632086 CET	50141	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:48:53.487828970 CET	53	50141	8.8.8.8	192.168.2.3
Nov 27, 2020 18:48:54.683697939 CET	53023	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:48:54.710848093 CET	53	53023	8.8.8.8	192.168.2.3
Nov 27, 2020 18:48:55.710408926 CET	49563	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:48:55.737627983 CET	53	49563	8.8.8.8	192.168.2.3
Nov 27, 2020 18:48:56.610769987 CET	51352	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:48:56.637826920 CET	53	51352	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:17.352818966 CET	59349	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:17.380176067 CET	53	59349	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:25.267473936 CET	57084	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:25.304222107 CET	53	57084	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:28.796281099 CET	58823	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:28.823597908 CET	53	58823	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:29.572182894 CET	57568	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:29.599486113 CET	53	57568	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:30.357292891 CET	50540	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:30.384581089 CET	53	50540	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:31.431689978 CET	54366	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 18:49:31.458792925 CET	53	54366	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:31.604557991 CET	53034	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:31.648224115 CET	53	53034	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:35.526433945 CET	57762	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:35.572897911 CET	53	57762	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:40.148825884 CET	55435	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:40.186539888 CET	53	55435	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:51.248121023 CET	50713	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:51.275444031 CET	53	50713	8.8.8.8	192.168.2.3
Nov 27, 2020 18:49:54.172245026 CET	56132	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:49:54.209326982 CET	53	56132	8.8.8.8	192.168.2.3
Nov 27, 2020 18:50:04.793050051 CET	58987	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:50:04.820249081 CET	53	58987	8.8.8.8	192.168.2.3
Nov 27, 2020 18:50:25.860347986 CET	56579	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:50:25.887492895 CET	53	56579	8.8.8.8	192.168.2.3
Nov 27, 2020 18:50:27.451786041 CET	60633	53	192.168.2.3	8.8.8.8
Nov 27, 2020 18:50:27.487265110 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 18:49:35.526433945 CET	192.168.2.3	8.8.8.8	0x1fe7	Standard query (0)	mail.hybridgroupco.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 18:49:35.572897911 CET	8.8.8.8	192.168.2.3	0x1fe7	No error (0)	mail.hybridgroupco.com	hybridgroupco.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 18:49:35.572897911 CET	8.8.8.8	192.168.2.3	0x1fe7	No error (0)	hybridgroupco.com		66.70.204.222	A (IP address)	IN (0x0001)

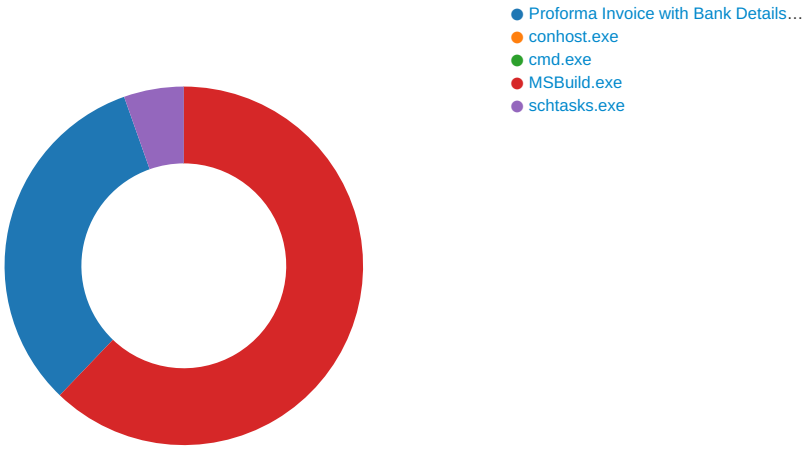
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 27, 2020 18:49:35.944700003 CET	587	49725	66.70.204.222	192.168.2.3	220-host.theserver.live ESMTP Exim 4.93 #2 Fri, 27 Nov 2020 21:49:35 +0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 18:49:35.945132971 CET	49725	587	192.168.2.3	66.70.204.222	EHLO 142233
Nov 27, 2020 18:49:36.050761938 CET	587	49725	66.70.204.222	192.168.2.3	250-host.theserver.live Hello 142233 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-STARTTLS 250 HELP
Nov 27, 2020 18:49:36.051378012 CET	49725	587	192.168.2.3	66.70.204.222	STARTTLS
Nov 27, 2020 18:49:36.158169031 CET	587	49725	66.70.204.222	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Proforma Invoice with Bank Details_pdf.exe PID: 6672 Parent PID: 5608

General

Start time:	18:48:55
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\Proforma Invoice with Bank Details_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Proforma Invoice with Bank Details_pdf.exe'
Imagebase:	0xc40000
File size:	626176 bytes
MD5 hash:	8816AE2D440C50E7EC52BE21AE6E2B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.209201167.0000000000C66000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\folder	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	C62DB0	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\folder\file.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	C62CF6	CreateFileW
C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	C65267	CreateFileW

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\Local\Temp\folder\file.exe	unknown	626186	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 f8 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 0f 0c 9d ea 4b 6d f3 b9 4b 6d f3 b9 4b 6d f3 b9 8f a8 3e b9 52 6d f3 b9 8f a8 3c b9 0a 6d f3 b9 8f a8 3d b9 fc 6d f3 b9 4b 6d f2 b9 ce 6d f3 b9 b7 1a 4a b9 58 6d f3 b9 6c ab 20 b9 4a 6d f3 b9 6c ab 3a b9 4a 6d f3 b9 4b 6d 64 b9 4a 6d f3 b9 6c ab 3f b9 4a 6d f3 b9 52 69 63 68 4b 6d f3 b9 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 50 45 00 00 4c 01 05	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $...........Km..Km..Km....>.R m.... <..m....=..m..Km...m....J. Xm..l. .Jm..l.:.Jm..Kmd.Jm..l. ?.Jm..RichKm................. ........PE..L..	success or wait	1	C62D0F	WriteFile
C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml	unknown	1287	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 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 20 3d 20 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 0a 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 3c 44 61 74 65 3e 32 30 31 35 2d 30 39 2d 32 37 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 20 3e 20 0a 3c 41 75 74 68 6f 72 3e 31 34 32 32 33 33 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 3c 54 72 69 67 67 65 72 73 3e 0a 3c 4c 6f 67 6f 6e 54	<?xml version="1.0" encoding="UTF-16"?>. <Task version = "1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>.<Date>2015-09-27T14:27:44.8929027</Date > . <Author>142233\user</Author>.</RegistrationInfo>. <Triggers>.<LogonT	success or wait	1	C65296	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Proforma Invoice with Bank Details_pdf.exe	unknown	626176	success or wait	1	C62CBC	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	C61186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	C61186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	C61186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	C61186	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	C61186	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	C61186	ReadFile

Analysis Process: conhost.exe PID: 6680 Parent PID: 6672

General

Start time:	18:48:56
Start date:	27/11/2020
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: cmd.exe PID: 6736 Parent PID: 6672

General

Start time:	18:48:56
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c schtasks /Create /TN name /XML 'C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: MSBuild.exe PID: 6744 Parent PID: 6672

General

Start time:	18:48:56
Start date:	27/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Imagebase:	0x520000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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: 00000003.00000002.473024653.0000000002C01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.473614554.0000000002CCE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.469545862.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.474100533.0000000002DA4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5870DCF	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5870DCF	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5870DCF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5870DCF	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\579e1ca5-083c-4ff8-97b5-97675c77c151	unknown	4096	success or wait	1	5870DCF	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	5870DCF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5870DCF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5870DCF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	5870DCF	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	5870DCF	ReadFile

Analysis Process: schtasks.exe PID: 6756 Parent PID: 6736

General

Start time:	18:48:57
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /Create /TN name /XML 'C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml'
Imagebase:	0xae0000
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\eb880290d3c747809c5fd1c3af592ae7.xml	unknown	2	success or wait	1	AEAB22	ReadFile
C:\Users\user\AppData\Local\Temp\eb880290d3c747809c5fd1c3af592ae7.xml	unknown	1288	success or wait	1	AEABD9	ReadFile

Disassembly

Code Analysis