ID: 358289
Sample Name: invoicepdf.exe
Cookbook: default.jbs
Time: 11:41:09
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

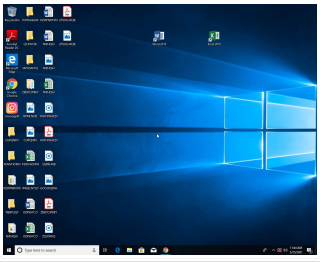
Analysis Report invoicepdf.exe

Overview

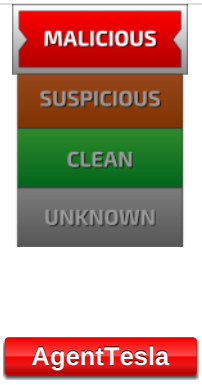
General Information

Sample Name:	invoicepdf.exe
Analysis ID:	358289
MD5:	6f98206e6905f1f…
SHA1:	71f6208364a668e.
SHA256:	97069c864ebe6a..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

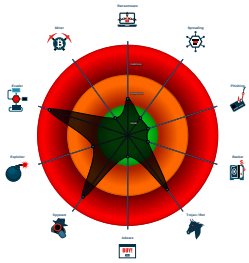


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- Found evasive API chain (trying to d…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- invoicepdf.exe (PID: 6812 cmdline: 'C:\Users\user\Desktop\invoicepdf.exe' MD5: 6F98206E6905F1F727E255D114D3C0AC)
  - schtasks.exe (PID: 6932 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\EuegmryBXVkd' /XML 'C:\Users\user\AppData\Local\Temp\tmp5A9C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - invoicepdf.exe (PID: 7052 cmdline: C:\Users\user\Desktop\invoicepdf.exe MD5: 6F98206E6905F1F727E255D114D3C0AC)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "nasir@com-cept.comkhan@980.pkmail.com-cept.comlight@redwevamaldives.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.594160867.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.337569981.0000000002AB1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.337682468.0000000002ADC000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.598124128.0000000002D9F000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.338574835.0000000003B5E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 6 entries				

Unpacked PEs

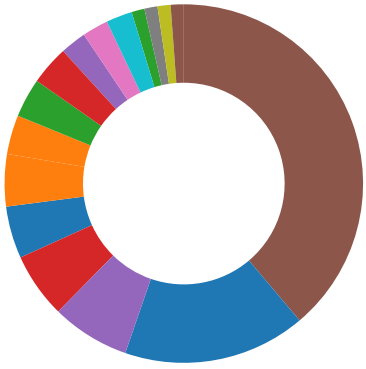
Source	Rule	Description	Author	Strings
5.2.invoicepdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.invoicepdf.exe.2ac5f2c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.invoicepdf.exe.3d71aa0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.invoicepdf.exe.3d71aa0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.invoicepdf.exe.3c743f0.3.raw.unpack	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:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

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

Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large strings

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

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

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:

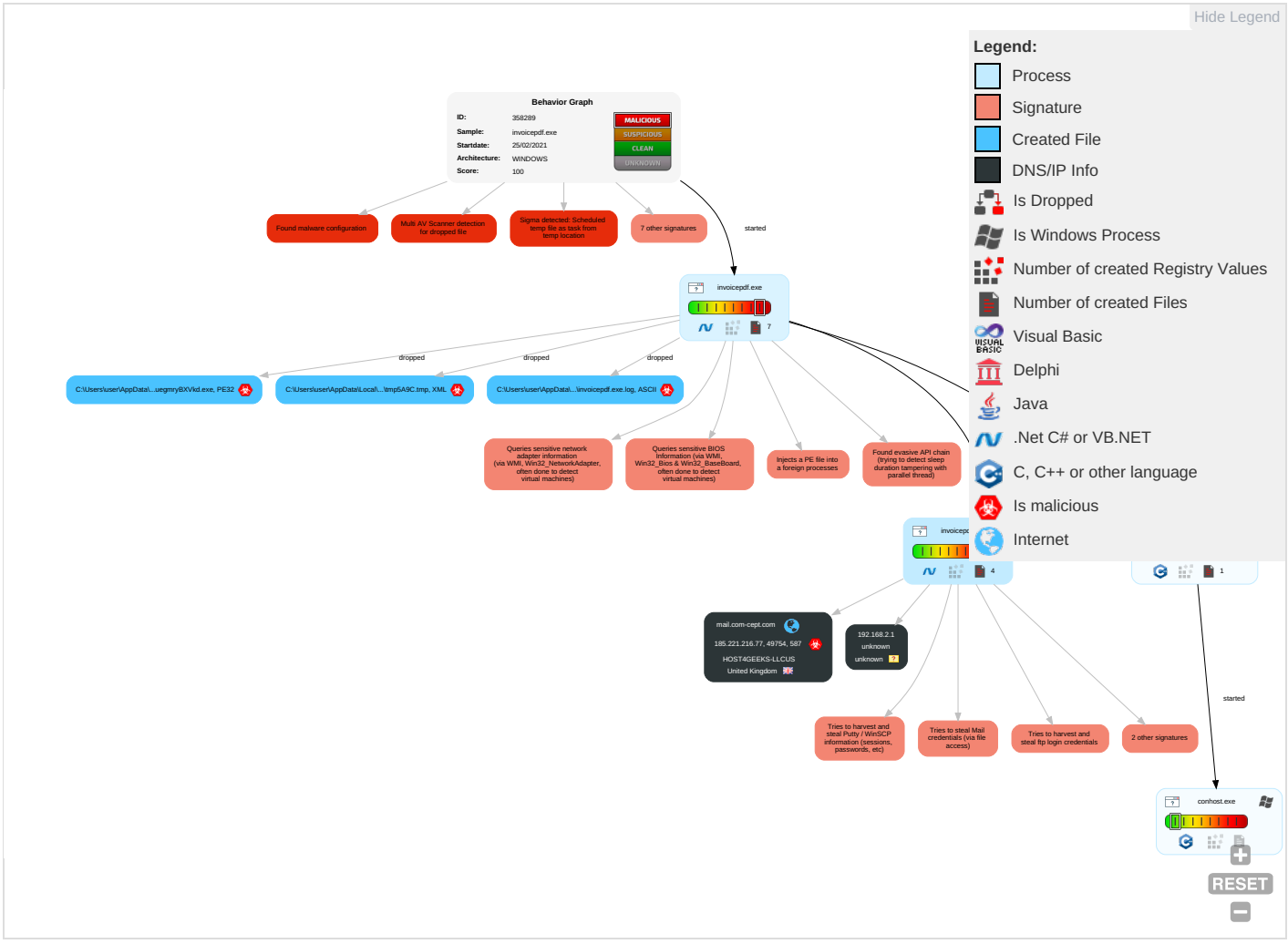
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Scheduled Task/Job 1	Access Token Manipulation 1	Obfuscated Files or Information 3 1	Input Capture 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Process Injection 1 1 2	Software Packing 2	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 1	DLL Side-Loading 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 2 1	SSH	Clipboard Data 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 5	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol

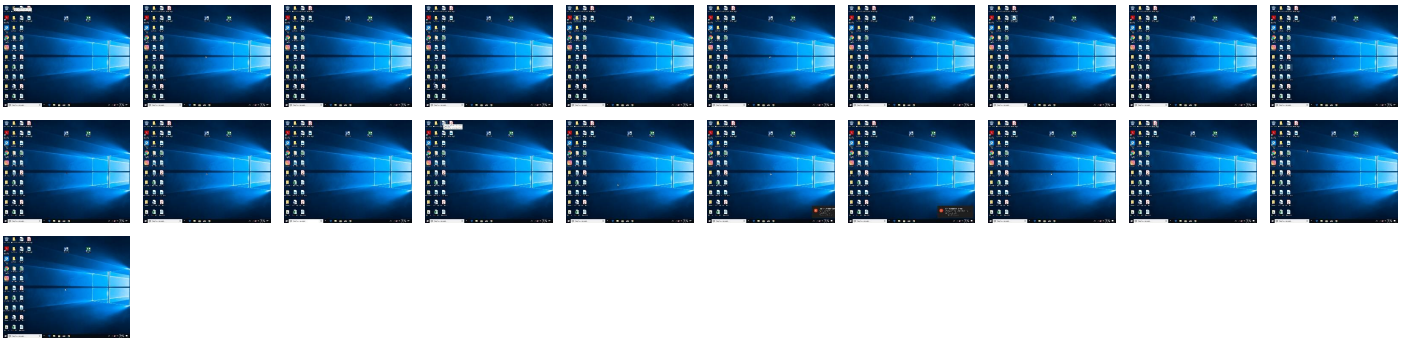
Behavior Graph



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
invoicepdf.exe	17%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\EuegmryBXVkd.exe	10%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://x4UtAvxhwOMMhTg.org	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	
http://HtsCZk.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.com-cept.com	185.221.216.77	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	invoicepdf.exe, 00000005.00000002.597890821.0000000002D11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	invoicepdf.exe, 00000005.00000002.597890821.0000000002D11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	invoicepdf.exe, 00000005.00000002.597890821.0000000002D11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://x4UtAvxhwOMMhTg.org	invoicepdf.exe, 00000005.00000002.598124128.0000000002D9F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	invoicepdf.exe, 00000005.00000002.597890821.0000000002D11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%	invoicepdf.exe, 00000005.00000002.597890821.0000000002D11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	invoicepdf.exe, 00000000.00000002.338574835.0000000003B5E000.00000004.00000001.sdmp, invoicepdf.exe, 00000005.00000002.594160867.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://HtsCZk.com	invoicepdf.exe, 00000005.00000002.597890821.0000000002D11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	invoicepdf.exe, 00000000.00000002.337569981.0000000002AB1000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.221.216.77	unknown	United Kingdom		393960	HOST4GEEKS-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358289
Start date:	25.02.2021
Start time:	11:41:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoicepdf.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:	26
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@6/4@1/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.6% (good quality ratio 3.2%) • Quality average: 56.4% • Quality standard deviation: 42.1%
HCA Information:	• Successful, ratio: 91% • 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, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 131.253.33.200, 13.107.22.200, 23.211.6.115, 52.147.198.201, 51.104.139.180, 2.20.142.209, 2.20.142.210, 67.26.73.254, 8.248.143.254, 8.253.95.249, 8.253.95.120, 67.26.83.254, 51.103.5.159, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 184.30.20.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many 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
11:41:59	API Interceptor	946x Sleep call for process: invoicepdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.221.216.77	invoice.pdf.exe	Get hash	malicious	Browse	
	invoice copys.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.com-cept.com	invoice.pdf.exe	Get hash	malicious	Browse	• 185.221.216.77
	invoice copys.exe	Get hash	malicious	Browse	• 185.221.216.77

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOST4GEEKS-LLCUS	invoice.pdf.exe	Get hash	malicious	Browse	• 185.221.216.77
	synchronossTicket#513473.htm	Get hash	malicious	Browse	• 185.221.216.34
	invoice copys.exe	Get hash	malicious	Browse	• 185.221.216.77
	55-2912.doc	Get hash	malicious	Browse	• 66.85.46.76
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 66.85.46.76
	DAT_G_0259067.doc	Get hash	malicious	Browse	• 66.85.46.76
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 66.85.46.76
	5349 TED_04235524.doc	Get hash	malicious	Browse	• 66.85.46.76
	FILE_122020_VVY_591928.doc	Get hash	malicious	Browse	• 66.85.46.76
	Archivo_29_48214503.doc	Get hash	malicious	Browse	• 66.85.46.76
	Adjunto 29 886_473411.doc	Get hash	malicious	Browse	• 66.85.46.76
	Informacion_29.doc	Get hash	malicious	Browse	• 66.85.46.76
	Informacion_29.doc	Get hash	malicious	Browse	• 66.85.46.76
	Informacion_122020_EUH-4262717.doc	Get hash	malicious	Browse	• 66.85.46.76
	1923620_YY-5094713.doc	Get hash	malicious	Browse	• 66.85.46.76
	Doc 2912 75513.doc	Get hash	malicious	Browse	• 66.85.46.76
	DAT.doc	Get hash	malicious	Browse	• 66.85.46.76
	ARCHIVOFile_762-36284.doc	Get hash	malicious	Browse	• 66.85.46.76
	4640-2912-122020.doc	Get hash	malicious	Browse	• 66.85.46.76
	MENSAJE_29_2020.doc	Get hash	malicious	Browse	• 66.85.46.76

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoicepdf.exe.log

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoicepdf.exe.log	
Process:	C:\Users\user\Desktop\invoicepdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp5A9C.tmp	
Process:	C:\Users\user\Desktop\invoicepdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	5.161993843403802
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3stn:cbha7JlNQV/rydbz9I3YODOLNdq3s
MD5:	9149142410DC43256D3D9AF56DBDEEAA
SHA1:	3A42048F278DEF0A3CA6033B90E5BF6ABF15480B
SHA-256:	8E67B925715A8CD51CAC18764A72B58A3547345A896B05AF84EA811FBF3DEBBC
SHA-512:	B0AF46671E2D5EC56FF9038E7E3F5F394BF4D14D0120244B623A13FA0786C91EE81464F66F6023617E7A66B4E1B81E90D0B6782CA2E8455E406B099E97ECAFF1
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>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\EuegmryBXVkd.exe	
Process:	C:\Users\user\Desktop\invoicepdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	788992
Entropy (8bit):	7.074594045321417
Encrypted:	false
SSDEEP:	12288:ZSprUPZb4NuAvlTwvtonQkJzUOBjgQQiq62fo1:ZEU4NuA9QkyO2im2
MD5:	6F98206E6905F1F727E255D114D3C0AC
SHA1:	71F6208364A668E72F8109A373C6C83C90B7999F
SHA-256:	97069C864EBE6A1A3E6E85BD1FF54351810CC32DE3CDFE34F7FEF15F04DA0B87
SHA-512:	53E6E020FD5DF48E7909C42C01E1FD565FE0107C0248C359B22394F67C0F3E8A67C1C7A59C70D9C964AD3D44963735505C69B7D242C3E688C9DB4758DB40770
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 10%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....t7`.....P.....N.....r.... .....@.. .....`..... ..@..... ...O.....LK.....@..... ....H.....text...x.... ....`.rsrc...LK.....L.....@..@.reloc.....@.....@..B.....T.....H.....TO.....0.....0.....(....(.....(.....o.....*.....(.....(.....(!.....("....(#....*N..(....oL...($....*&..(%....*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0..<.....~.....(0.....,!r...p.....(1...o2...s3.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\EuegmryBXVkd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\invoicepdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Roaming\EuegmryBXVkd.exe:Zone.Identifier

Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.074594045321417
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	invoicepdf.exe
File size:	788992
MD5:	6f98206e6905f1f727e255d114d3c0ac
SHA1:	71f6208364a668e72f8109a373c6c83c90b7999f
SHA256:	97069c864ebe6a1a3e6e85bd1ff54351810cc32de3cdfe34f7fef15f04da0b87
SHA512:	53e6e020fd5df48e7909c42c01e1fd565fe0107c0248c359b22394f67c0f3e8a67c1c7a59c70d9c964ad3d44963735505c69b7d242c3e688c9db4758db407703
SSDEEP:	12288:ZSprUPZb4NuAvlTwvtonQkJzUOBjgQQiq62fo1:ZEU4NuA9QkyO2im2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....t7`.....P.....N.....r.... .....@.. .....`.....@.....

File Icon

Icon Hash:	f8c492aaaa92dcfe

Static PE Info

General

Entrypoint:	0x4bd872
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6037748A [Thu Feb 25 09:57:30 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General	
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbd820	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x4b4c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbb878	0xbba00	False	0.608667138574	data	7.06854919564	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x4b4c	0x4c00	False	0.487201891447	data	5.74193482381	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbe1c0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xbe628	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4275388049, next used block 4258479509		
RT_ICON	0xbf6d0	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 3771611807, next used block 3167566498		
RT_GROUP_ICON	0xc1c78	0x30	data		
RT_GROUP_ICON	0xc1ca8	0x14	data		
RT_VERSION	0xc1cbc	0x378	data		
RT_MANIFEST	0xc2034	0xb15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

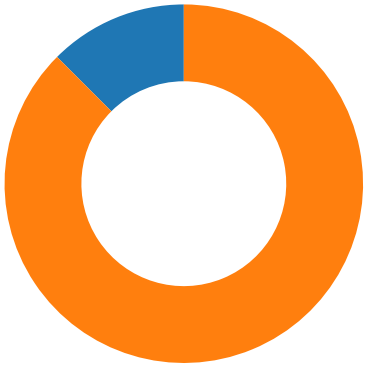
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	3.0.0.0
InternalName	SubcategoryMembershipEntry.exe
FileVersion	3.0.0.0
CompanyName	KTV
LegalTrademarks	
Comments	
ProductName	KTVManagement
ProductVersion	3.0.0.0
FileDescription	KTVManagement
OriginalFilename	SubcategoryMembershipEntry.exe

Network Behavior

Network Port Distribution



Total Packets: 48

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:43:31.370840073 CET	49754	587	192.168.2.6	185.221.216.77
Feb 25, 2021 11:43:31.428172112 CET	587	49754	185.221.216.77	192.168.2.6
Feb 25, 2021 11:43:31.429424047 CET	49754	587	192.168.2.6	185.221.216.77
Feb 25, 2021 11:43:31.562700033 CET	587	49754	185.221.216.77	192.168.2.6
Feb 25, 2021 11:43:31.565654993 CET	49754	587	192.168.2.6	185.221.216.77
Feb 25, 2021 11:43:31.623167992 CET	587	49754	185.221.216.77	192.168.2.6
Feb 25, 2021 11:43:31.624363899 CET	49754	587	192.168.2.6	185.221.216.77
Feb 25, 2021 11:43:31.683339119 CET	587	49754	185.221.216.77	192.168.2.6
Feb 25, 2021 11:43:31.715395927 CET	49754	587	192.168.2.6	185.221.216.77
Feb 25, 2021 11:43:31.773184061 CET	587	49754	185.221.216.77	192.168.2.6
Feb 25, 2021 11:43:31.773322105 CET	49754	587	192.168.2.6	185.221.216.77

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:41:49.699194908 CET	54513	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:49.734250069 CET	62044	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:49.747864962 CET	53	54513	8.8.8.8	192.168.2.6
Feb 25, 2021 11:41:49.785949945 CET	53	62044	8.8.8.8	192.168.2.6
Feb 25, 2021 11:41:51.229141951 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:51.281054974 CET	53	63791	8.8.8.8	192.168.2.6
Feb 25, 2021 11:41:51.926170111 CET	64267	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:51.985377073 CET	53	64267	8.8.8.8	192.168.2.6
Feb 25, 2021 11:41:52.386835098 CET	49448	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:52.449146986 CET	53	49448	8.8.8.8	192.168.2.6
Feb 25, 2021 11:41:53.526319027 CET	60342	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:53.575036049 CET	53	60342	8.8.8.8	192.168.2.6
Feb 25, 2021 11:41:54.992599964 CET	61346	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:55.043550968 CET	53	61346	8.8.8.8	192.168.2.6
Feb 25, 2021 11:41:55.847457886 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:56.861562967 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:57.876817942 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:57.928577900 CET	53	51774	8.8.8.8	192.168.2.6
Feb 25, 2021 11:41:59.229866028 CET	56023	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:41:59.278750896 CET	53	56023	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:01.666904926 CET	58384	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:01.715954065 CET	53	58384	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:02.539083958 CET	60261	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:02.588154078 CET	53	60261	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:03.722847939 CET	56061	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:03.774718046 CET	53	56061	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:05.102363110 CET	58336	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:05.161025047 CET	53	58336	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:06.278151989 CET	53781	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:06.327392101 CET	53	53781	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:07.443907022 CET	54064	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:07.493066072 CET	53	54064	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:08.589304924 CET	52811	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:08.639059067 CET	53	52811	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:09.869546890 CET	55299	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:09.921233892 CET	53	55299	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:11.277381897 CET	63745	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:11.326066971 CET	53	63745	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:12.736093998 CET	50055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:12.784821987 CET	53	50055	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:15.552386999 CET	61374	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:15.601363897 CET	53	61374	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:25.583460093 CET	50339	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:25.632186890 CET	53	50339	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:45.148912907 CET	63307	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:45.210259914 CET	53	63307	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:45.310525894 CET	49694	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:42:45.361241102 CET	53	49694	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:47.312665939 CET	54982	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:47.364840984 CET	53	54982	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:47.882683039 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:47.967247009 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:48.884064913 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:48.944849014 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:49.664988995 CET	62116	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:49.730720043 CET	53	62116	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:50.479805946 CET	63816	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:50.539237022 CET	53	63816	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:51.013923883 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:51.071263075 CET	53	55014	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:52.064951897 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:52.129256010 CET	53	62208	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:53.159595013 CET	57574	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:53.228266954 CET	53	57574	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:54.146301985 CET	51818	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:54.218048096 CET	53	51818	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:54.380764008 CET	56628	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:54.440798044 CET	53	56628	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:56.036001921 CET	60778	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:56.087968111 CET	53	60778	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:56.758483887 CET	53799	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:56.815855980 CET	53	53799	8.8.8.8	192.168.2.6
Feb 25, 2021 11:42:59.353415966 CET	54683	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:42:59.414673090 CET	53	54683	8.8.8.8	192.168.2.6
Feb 25, 2021 11:43:30.139228106 CET	59329	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:43:30.187971115 CET	53	59329	8.8.8.8	192.168.2.6
Feb 25, 2021 11:43:30.871164083 CET	64021	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:43:30.939100981 CET	53	64021	8.8.8.8	192.168.2.6
Feb 25, 2021 11:43:31.287022114 CET	56129	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:43:31.352623940 CET	53	56129	8.8.8.8	192.168.2.6
Feb 25, 2021 11:43:32.426588058 CET	58177	53	192.168.2.6	8.8.8.8
Feb 25, 2021 11:43:32.491616964 CET	53	58177	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 11:43:31.287022114 CET	192.168.2.6	8.8.8.8	0x73d0	Standard query (0)	mail.com-cept.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:43:31.352623940 CET	8.8.8.8	192.168.2.6	0x73d0	No error (0)	mail.com-cept.com		185.221.216.77	A (IP address)	IN (0x0001)

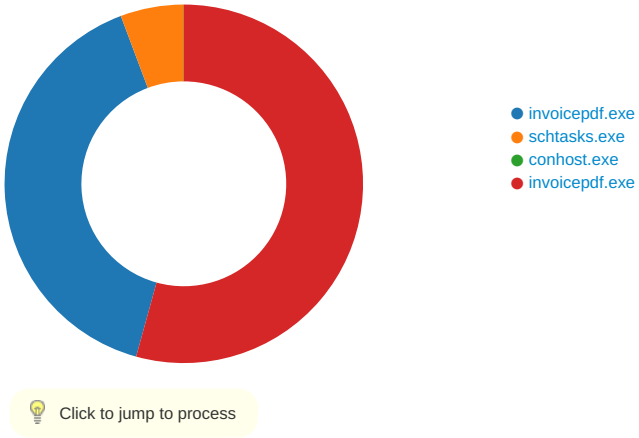
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 11:43:31.562700033 CET	587	49754	185.221.216.77	192.168.2.6	220-uksrv3.websiteserverbox.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 05:43:30 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 11:43:31.565654993 CET	49754	587	192.168.2.6	185.221.216.77	EHLO 123716
Feb 25, 2021 11:43:31.623167992 CET	587	49754	185.221.216.77	192.168.2.6	250-uksrv3.websiteserverbox.com Hello 123716 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 11:43:31.624363899 CET	49754	587	192.168.2.6	185.221.216.77	STARTTLS
Feb 25, 2021 11:43:31.683339119 CET	587	49754	185.221.216.77	192.168.2.6	220 TLS go ahead

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: invoicepdf.exe PID: 6812 Parent PID: 5916

General

Start time:	11:41:58
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\invoicepdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\invoicepdf.exe'
Imagebase:	0x2c0000
File size:	788992 bytes
MD5 hash:	6F98206E6905F1F727E255D114D3C0AC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.337569981.0000000002AB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.337682468.0000000002ADC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.338574835.0000000003B5E000.00000004.00000001.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	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\AppData\Roaming\EuegmryBXVkd.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	B5BEE8	CopyFileW
C:\Users\user\AppData\Roaming\EuegmryBXVkd.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	B5BEE8	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5A9C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	51E07D8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoicepdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5A9C.tmp	success or wait	1	51E0DAA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EuegmryBXVkd.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 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 8a 74 37 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 ba 0b 00 00 4e 00 00 00 00 00 00 72 d8 0b 00 00 20 00 00 00 e0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....t7`.......... ....P......N......r.... ........@.. ......................` ....@................	success or wait	4	B5BEE8	CopyFileW
C:\Users\user\AppData\Roaming\EuegmryBXVkd.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	B5BEE8	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5A9C.tmp	unknown	1657	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 65 6e 67 69 6e 65 65 72 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	<?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>.. </Registratio	success or wait	1	51E0A67	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\invoicepdf.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

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

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	72FE8738	ReadFile

Analysis Process: schtasks.exe PID: 6932 Parent PID: 6812

General

Start time:	11:42:01
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\EuegmryBXVkd' /XML 'C:\Users\user\AppData\Local\Temp\tmp5A9C.tmp'
Imagebase:	0x1120000
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\tmp5A9C.tmp	unknown	2	success or wait	1	112AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5A9C.tmp	unknown	1658	success or wait	1	112ABD9	ReadFile

Analysis Process: conhost.exe PID: 6984 Parent PID: 6932

General

Start time:	11:42:02
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: invoicepdf.exe PID: 7052 Parent PID: 6812

General

Start time:	11:42:02
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\invoicepdf.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\invoicepdf.exe
Imagebase:	0x480000
File size:	788992 bytes
MD5 hash:	6F98206E6905F1F727E255D114D3C0AC
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: 00000005.00000002.594160867.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.598124128.0000000002D9F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.597890821.0000000002D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.597890821.0000000002D11000.00000004.00000001.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	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\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:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	55E113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	55E113B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	55E113B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\409be960-fc65-4002-a209-7238342f2640	unknown	4096	success or wait	1	55E113B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	55E113B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	55E113B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	55E113B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	55E113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	55E113B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	55E113B	ReadFile

Disassembly

Code Analysis