ID: 755998
Sample Name: payment swift.exe
Cookbook: default.jbs
Time: 13:26:11
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

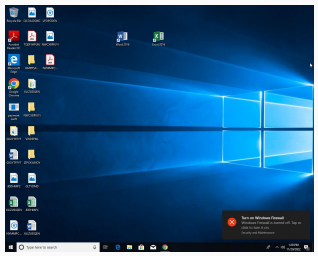
Windows Analysis Report

payment swift.exe

Overview

General Information

Sample Name:	payment swift.exe
Analysis ID:	755998
MD5:	0eb99950c8a30f..
SHA1:	54557815e576ac..
SHA256:	469dae2eed97bb.
Tags:	exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

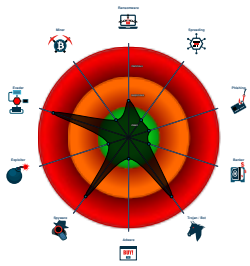
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- 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…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains very larg…

Classification



Process Tree

- **System is w10x64**
- payment swift.exe (PID: 3100 cmdline: C:\Users\user\Desktop\payment swift.exe MD5: 0EB99950C8A30FEE01EBFDAA33498B22)
  - payment swift.exe (PID: 4460 cmdline: C:\Users\user\Desktop\payment swift.exe MD5: 0EB99950C8A30FEE01EBFDAA33498B22)
- WdFVsOe.exe (PID: 2460 cmdline: "C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe" MD5: 0EB99950C8A30FEE01EBFDAA33498B22)
  - WdFVsOe.exe (PID: 4768 cmdline: C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe MD5: 0EB99950C8A30FEE01EBFDAA33498B22)
- WdFVsOe.exe (PID: 5992 cmdline: "C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe" MD5: 0EB99950C8A30FEE01EBFDAA33498B22)
  - WdFVsOe.exe (PID: 972 cmdline: C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe MD5: 0EB99950C8A30FEE01EBFDAA33498B22)
  - WdFVsOe.exe (PID: 1276 cmdline: C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe MD5: 0EB99950C8A30FEE01EBFDAA33498B22)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Host": "host39.registrar-servers.com",
  "Username": "dickson@potashin.us",
  "Password": "*r4} Du LH  n87G"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.313645910.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000000.313645910.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000000.313645910.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31d17:$a13: get_DnsResolver • 0x30424:$a20: get_LastAccessed • 0x32745:$a27: set_InternalServerPort • 0x32a7a:$a30: set_GuidMasterKey • 0x30536:$a33: get_Clipboard • 0x30544:$a34: get_Keyboard • 0x31911:$a35: get_ShiftKeyDown • 0x31922:$a36: get_AltKeyDown • 0x30551:$a37: get_Password • 0x3106c:$a38: get_PasswordHash • 0x32179:$a39: get_DefaultCredentials
00000000.00000002.315807649.00000000030D5000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.360649511.0000000002655000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.WdFVsOe.exe.25e063c.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
2.2.WdFVsOe.exe.25e063c.1.raw.unpack	INDICATOR_SUSPICIOUS_EXE_Anti_OldCopyPaste	Detects executables potentially checking for WinJail sandbox window	ditekSHen	• 0xcfea:$v1: SbieDll.dll • 0xd004:$v2: USER • 0xd010:$v3: SANDBOX • 0xd022:$v4: VIRUS • 0xd072:$v4: VIRUS • 0xd030:$v5: MALWARE • 0xd042:$v6: SCHMIDTI • 0xd056:$v7: CURRENTUSER
0.2.payment swift.exe.4392240.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.payment swift.exe.4392240.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.payment swift.exe.4392240.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32c56:$s10: logins • 0x326d0:$s11: credential • 0x2e936:$g1: get_Clipboard • 0x2e944:$g2: get_Keyboard • 0x2e951:$g3: get_Password • 0x2fd01:$g4: get_CtrlKeyDown • 0x2fd11:$g5: get_ShiftKeyDown • 0x2fd22:$g6: get_AltKeyDown
Click to see the 25 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

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

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

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)

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

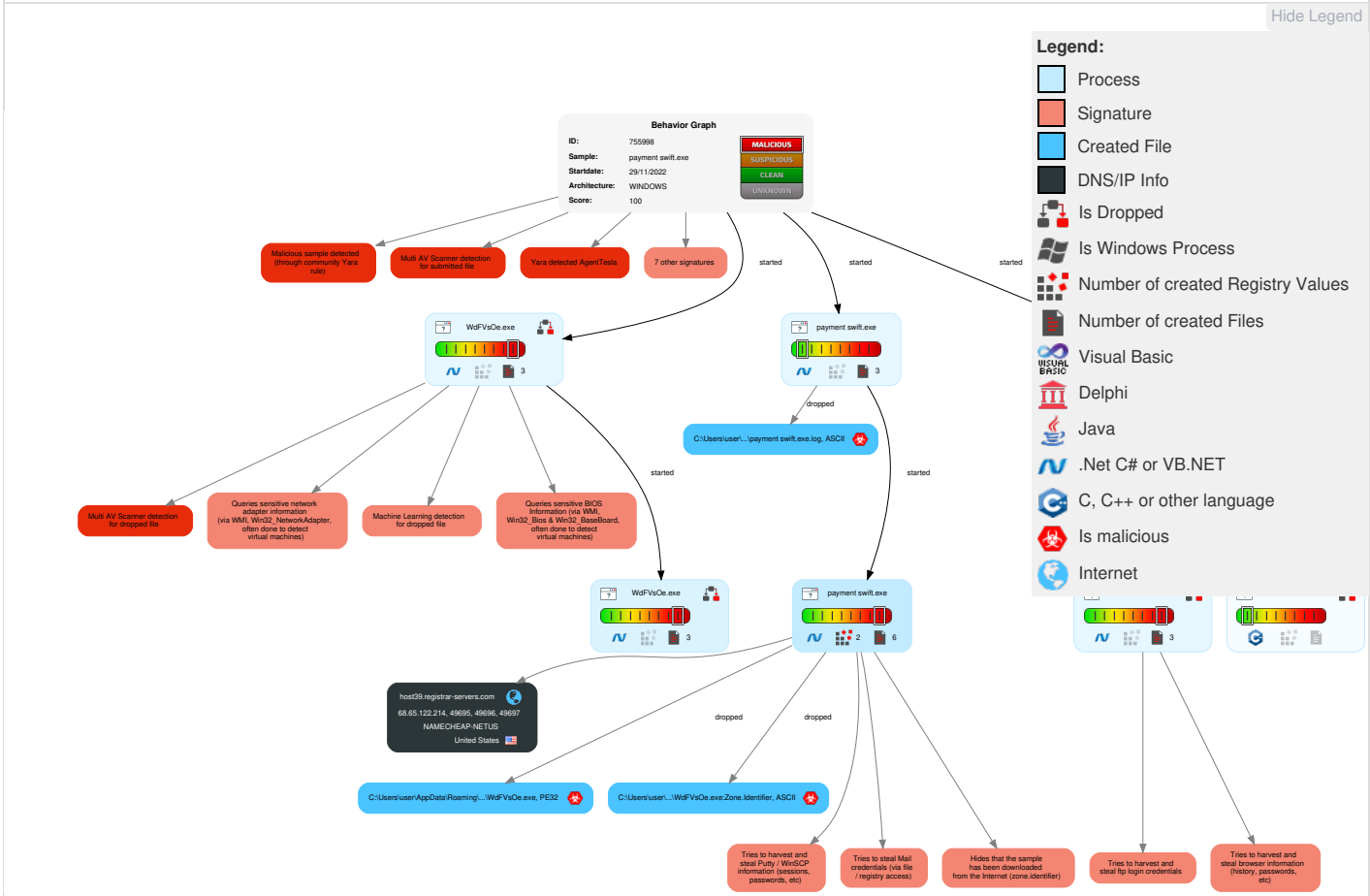
Yara detected AgentTesla

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 Registry Run Keys / Startup Folder	1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 1 4 System Information 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	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Input Capture	3 1 1 Security Software 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)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	1 Process Discovery	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)	3 Software Packing	NTDS	1 3 1 Virtualization/Sandbox Evasion	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	1 Masquerading	LSA Secrets	1 Application Window 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 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Remote System Discovery	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 1 Process Injection	DCSync	Network Sniffing	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 Hidden Files and Directories	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

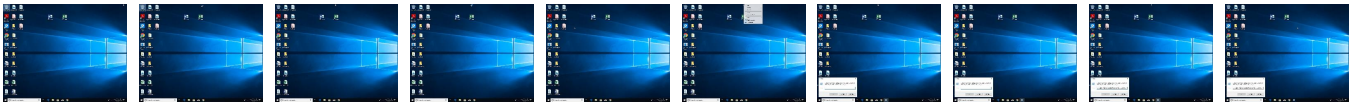
Behavior Graph

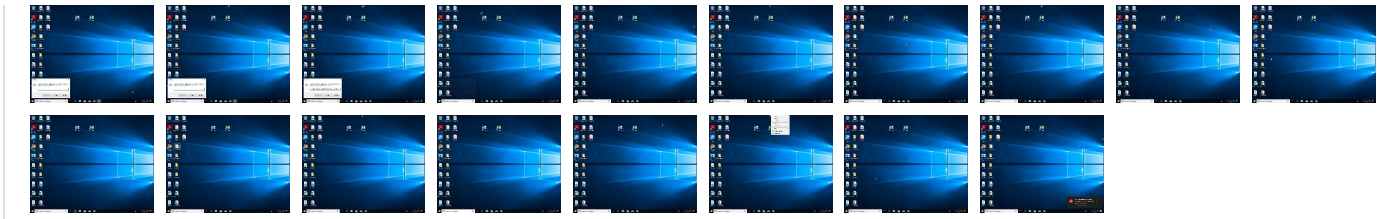


Screenshots

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
payment swift.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
payment swift.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.payment swift.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
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/bThe	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.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	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://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://D16a0atI7uWaj.comX	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com09	0%	Avira URL Cloud	safe	
http://kjkcOA.com	0%	Avira URL Cloud	safe	
http://https://D16a0atI7uWaj.com	0%	Avira URL Cloud	safe	
http://crl.comor	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host39.registrar-servers.com	68.65.122.214	true	false		high

URLs from Memory and Binaries

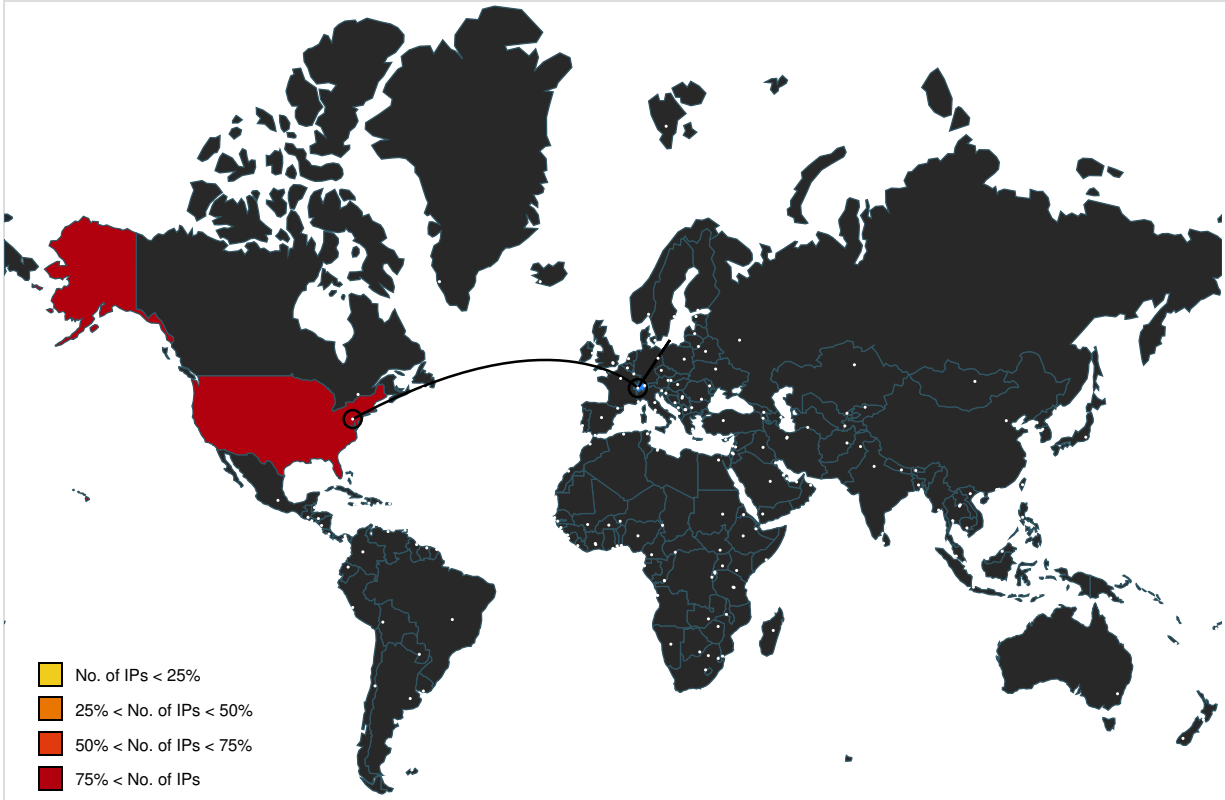
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	payment swift.exe, 00000001.00000002.568239695.0000000000C61000.00000004.00000020.00020000.00000000.sdmp, payment swift.exe, 00000001.00000002.568309572.0000000000C69000.00000004.00000020.00020000.00000000.sdmp, payment swift.exe, 00000001.00000002.578503982.0000000002E6F000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.578453028.0000000002BC4000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.587147691.0000000006360000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000006.00000002.579742937.0000000002EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	payment swift.exe, 00000001.00000002.570872866.0000000002B41000.00000004.00000080.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.569999847.0000000002841000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000006.00000002.571356587.0000000002B2C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000080.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000080.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000080.00020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	payment swift.exe, 00000001.00000002.568239695.0000000000C61000.00000004.00000020.00020000.00000000.sdmp, payment swift.exe, 00000001.00000002.568309572.0000000000C69000.00000004.00000020.00020000.00000000.sdmp, payment swift.exe, 00000001.00000002.578503982.0000000002E6F000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.578453028.0000000002BC4000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.587147691.0000000006360000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000006.00000002.579742937.0000000002EA2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000080.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000080.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com09	payment swift.exe, 00000001.00000002.568239695.0000000000C61000.00000004.00000020.00020000.00000000.sdmp, payment swift.exe, 00000001.00000002.568309572.0000000000C69000.00000004.00000020.00020000.00000000.sdmp, payment swift.exe, 00000001.00000002.578503982.0000000002E6F000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.578453028.0000000002BC4000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.587147691.0000000006360000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000006.00000002.579742937.0000000002EA2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000080.00020000.00000000.sdmp	false		high
http://host39.registrar-servers.com	payment swift.exe, 00000001.00000002.578503982.0000000002E6F000.00000004.00000080.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.578453028.0000000002BC4000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000006.00000002.579742937.0000000002EA2000.00000004.00000800.00020000.00000000.sdmp	false		high

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	payment swift.exe, 00000001.00000002.570872866.0000000002B41000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000003.00000002.569999847.0000000002841000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000006.00000002.571356587.0000000002B2C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://D16a0atI7uWaj.comX	WdFVsOe.exe, 00000003.00000002.577583432.0000000002B6F000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000006.00000002.578885319.0000000002E4C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://kjkcOA.com	WdFVsOe.exe, 00000006.00000002.571356587.0000000002B2C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	WdFVsOe.exe, 00000006.00000002.571356587.0000000002B2C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://D16a0atI7uWaj.com	WdFVsOe.exe, 00000006.00000002.578885319.0000000002E4C000.00000004.00000800.00020000.00000000.sdmp, WdFVsOe.exe, 00000006.00000002.579991612.0000000002EC5000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	payment swift.exe, 00000000.00000002.319963745.0000000006F82000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.comor	WdFVsOe.exe, 00000003.00000002.587147691.0000000006360000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
68.65.122.214	host39.registrar-servers.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755998
Start date and time:	2022-11-29 13:26:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment swift.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/4@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- 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
13:27:09	API Interceptor	694x Sleep call for process: payment swift.exe modified
13:27:19	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run WdFVsOe C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
13:27:27	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run WdFVsOe C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
13:27:29	API Interceptor	947x Sleep call for process: WdFVsOe.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\WdFVsOe.exe.log

Process:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
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, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\Desktop\payment swift.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
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..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\Desktop\payment swift.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	945664
Entropy (8bit):	7.6581864683594505
Encrypted:	false
SSDEEP:	12288:3COqU+QmQCIcQNPy74FM33rWkwxrjbd9IWKRnyZ1V+Db6H6mXH7iODdzoa1cfN:SWmhQNzFM33KrNnO+V+Db6HNiODdEPf
MD5:	0EB99950C8A30FEE01EBFDAA33498B22
SHA1:	54557815E576AC70FCBCDFCB6765F3D2A2DFF507
SHA-256:	469DAE2EED97BBFE08AE548308E77AEDCD0795FB4B2B1ABCDD1A0315FE1FF216
SHA-512:	7641E3432CDEC9CCE11E474713DB3363403F85745F7AE8D92F576D5F4F1901E90C997BF11D3DC65F906B344F8D1FF6E28DE330C674623F9C9B251BE8E1342E2

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0..f..... .....@.. ..... .@.....X...O..... ....H.....text....e... ...f..... ..`.rsrc.....h.....@..@.reloc..... .....I.....@..B.....H.....<.....I...8u.. .....^..}.....(.....(.....*.0.....s.....o.....(.....*...0.....s.....o.....(.....*...0.....s.....o.....(..... *...0.....s.....o.....(.....*...0..+.....,..{.....+.....{....o.....(.....*..0..r.....(....s.....s....}.....s....}.....s....}.....s....}.....(.....{....(....o.....{.....o.....{.....o .....{....r...p"..@A...s!. ..o".....{....(#...o$.....{.... .... ..

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

Process:	C:\Users\user\Desktop\payment swift.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**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6581864683594505
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	payment swift.exe
File size:	945664
MD5:	0eb99950c8a30fee01ebfdaa33498b22
SHA1:	54557815e576ac70fcbcdfcb6765f3d2a2dff507
SHA256:	469dae2eed97bbfe08ae548308e77aedcd0795fb4b2b1abcdd1a0315fe1ff216
SHA512:	7641e3432cdec9cce11e474713db3363403f85745f7ae8d92f576d5f4f1901e90c997bf11d3dc65f906b344f8d1ff6e28de330c674623f9c9b251be8e1342e2d
SSDEEP:	12288:3COqU+QmQCIcQNPy74FM33rWkwxrjbd9IWKRnyZ1V+Db6H6mXH7iODdzoa1cfN:SWmhQNzFM33KrNnO+V+Db6HNiODdEPf
TLSH:	1E15D08033A2AF71F5296BF67821900827763C5EA5F1D2286EDDF0DE2676B5049F0B17
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0..f..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e85aa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000

Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385B3CD [Tue Nov 29 07:25:01 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe8558	0x4f	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xea000	0x388	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xec000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe65b0	0xe6600	False	0.8272061940450353	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.664774300353232	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xea000	0x388	0x400	False	0.3720703125	data	2.8564669469222315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xec000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

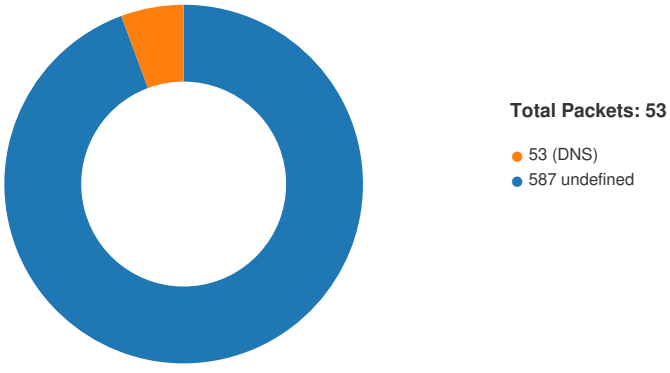
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xea058	0x32c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:27:27.737919092 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:27.906387091 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:27.906543970 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:28.230930090 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:28.231297016 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:28.411633015 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:28.412159920 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:28.582920074 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:28.630537987 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:28.641078949 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:28.827491999 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:28.827521086 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:28.827538013 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:28.827548981 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:28.827672005 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:28.834069014 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:28.880552053 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:28.943869114 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:29.123837948 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:29.177495003 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:29.207124949 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:29.378030062 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:29.382957935 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:29.555260897 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:29.556241035 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:29.744044065 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:29.745124102 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:29.913490057 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:29.914035082 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:30.116836071 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:30.117255926 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:30.285303116 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:30.313560963 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:30.314049006 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:30.314532042 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:30.314614058 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:30.481308937 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:30.481446028 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:30.482685089 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:30.493328094 CET	587	49695	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:30.537200928 CET	49695	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:52.961391926 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:53.131294012 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.139246941 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:53.371095896 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.375797987 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:53.545335054 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.545738935 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:53.718911886 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.743896008 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:53.930495024 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.930560112 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.930602074 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.930634022 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.930641890 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:53.930711985 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:53.933422089 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:53.976525068 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:54.141011953 CET	49696	587	192.168.2.4	68.65.122.214

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:27:54.312279940 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:54.351562977 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:54.413350105 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:54.582950115 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:54.583501101 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:54.753087997 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:54.788609982 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:54.966085911 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:55.007924080 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:55.286735058 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:55.456346035 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:55.490048885 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:55.664738894 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:55.710999966 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:55.712172985 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:55.881733894 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:56.117333889 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:56.262183905 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:56.262289047 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:56.262352943 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:56.262420893 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:27:56.431560993 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:56.431605101 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:56.431633949 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:56.431664944 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:56.436434984 CET	587	49696	68.65.122.214	192.168.2.4
Nov 29, 2022 13:27:56.617333889 CET	49696	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:28:05.598038912 CET	49697	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:28:05.764733076 CET	587	49697	68.65.122.214	192.168.2.4
Nov 29, 2022 13:28:05.764971972 CET	49697	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:28:06.114202976 CET	587	49697	68.65.122.214	192.168.2.4
Nov 29, 2022 13:28:06.114742041 CET	49697	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:28:06.282293081 CET	587	49697	68.65.122.214	192.168.2.4
Nov 29, 2022 13:28:06.288638115 CET	49697	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:28:06.459296942 CET	587	49697	68.65.122.214	192.168.2.4
Nov 29, 2022 13:28:06.486413956 CET	49697	587	192.168.2.4	68.65.122.214
Nov 29, 2022 13:28:06.701844931 CET	587	49697	68.65.122.214	192.168.2.4
Nov 29, 2022 13:28:06.710268021 CET	587	49697	68.65.122.214	192.168.2.4
Nov 29, 2022 13:28:06.710328102 CET	587	49697	68.65.122.214	192.168.2.4
Nov 29, 2022 13:28:06.710361004 CET	587	49697	68.65.122.214	192.168.2.4
Nov 29, 2022 13:28:06.710397005 CET	587	49697	68.65.122.214	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 13:27:27.661490917 CET	56572	53	192.168.2.4	8.8.8.8
Nov 29, 2022 13:27:27.680375099 CET	53	56572	8.8.8.8	192.168.2.4
Nov 29, 2022 13:27:52.909621000 CET	50911	53	192.168.2.4	8.8.8.8
Nov 29, 2022 13:27:52.929089069 CET	53	50911	8.8.8.8	192.168.2.4
Nov 29, 2022 13:28:05.553168058 CET	59683	53	192.168.2.4	8.8.8.8
Nov 29, 2022 13:28:05.574378014 CET	53	59683	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 13:27:27.661490917 CET	192.168.2.4	8.8.8.8	0x201d	Standard query (0)	host39.registrar-servers.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:27:52.909621000 CET	192.168.2.4	8.8.8.8	0xe05d	Standard query (0)	host39.registrar-servers.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 13:28:05.553168058 CET	192.168.2.4	8.8.8.8	0x22fd	Standard query (0)	host39.registrar-servers.com	A (IP address)	IN (0x0001)	false

DNS Answers

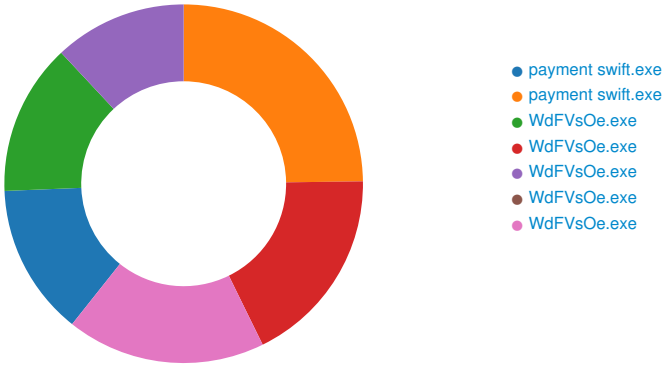
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 13:27:27.680375099 CET	8.8.8.8	192.168.2.4	0x201d	No error (0)	host39.registrar-servers.com		68.65.122.214	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:27:52.929089069 CET	8.8.8.8	192.168.2.4	0xe05d	No error (0)	host39.registrar-servers.com		68.65.122.214	A (IP address)	IN (0x0001)	false
Nov 29, 2022 13:28:05.574378014 CET	8.8.8.8	192.168.2.4	0x22fd	No error (0)	host39.registrar-servers.com		68.65.122.214	A (IP address)	IN (0x0001)	false

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 29, 2022 13:27:28.230930090 CET	587	49695	68.65.122.214	192.168.2.4	220-host39.registrar-servers.com ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 07:27:28 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 13:27:28.231297016 CET	49695	587	192.168.2.4	68.65.122.214	EHLO 767668
Nov 29, 2022 13:27:28.411633015 CET	587	49695	68.65.122.214	192.168.2.4	250-host39.registrar-servers.com Hello 767668 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 13:27:28.412159920 CET	49695	587	192.168.2.4	68.65.122.214	STARTTLS
Nov 29, 2022 13:27:28.582920074 CET	587	49695	68.65.122.214	192.168.2.4	220 TLS go ahead
Nov 29, 2022 13:27:53.371095896 CET	587	49696	68.65.122.214	192.168.2.4	220-host39.registrar-servers.com ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 07:27:53 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 13:27:53.375797987 CET	49696	587	192.168.2.4	68.65.122.214	EHLO 767668
Nov 29, 2022 13:27:53.545335054 CET	587	49696	68.65.122.214	192.168.2.4	250-host39.registrar-servers.com Hello 767668 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 13:27:53.545738935 CET	49696	587	192.168.2.4	68.65.122.214	STARTTLS
Nov 29, 2022 13:27:53.718911886 CET	587	49696	68.65.122.214	192.168.2.4	220 TLS go ahead
Nov 29, 2022 13:28:06.114202976 CET	587	49697	68.65.122.214	192.168.2.4	220-host39.registrar-servers.com ESMTP Exim 4.95 #2 Tue, 29 Nov 2022 07:28:06 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 29, 2022 13:28:06.114742041 CET	49697	587	192.168.2.4	68.65.122.214	EHLO 767668
Nov 29, 2022 13:28:06.282293081 CET	587	49697	68.65.122.214	192.168.2.4	250-host39.registrar-servers.com Hello 767668 [102.129.143.49] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 29, 2022 13:28:06.288638115 CET	49697	587	192.168.2.4	68.65.122.214	STARTTLS
Nov 29, 2022 13:28:06.459296942 CET	587	49697	68.65.122.214	192.168.2.4	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: payment swift.exe PID: **3100**, Parent PID: **3528**

General

Target ID:	0
Start time:	13:27:03
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\payment swift.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\payment swift.exe
Imagebase:	0xa80000
File size:	945664 bytes
MD5 hash:	0EB99950C8A30FEE01EBFDAA33498B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.315807649.00000000030D5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.318247702.000000000427E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.318247702.000000000427E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.318247702.000000000427E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.315641125.0000000003021000.00000004.00000800.00020000.00000000.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	6D61CF06	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	6D61CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment swift.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D92C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment swift.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	6D92C907	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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile

Analysis Process: payment swift.exe PID: **4460**, Parent PID: **3100**

General

Target ID:	1
Start time:	13:27:11
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\payment swift.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\payment swift.exe
Imagebase:	0x6d0000

File size:	945664 bytes
MD5 hash:	0EB99950C8A30FEE01EBFDAA33498B22
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: 00000001.00000000.313645910.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.313645910.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000000.313645910.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.570872866.0000000002B41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.570872866.0000000002B41000.00000004.00000800.00020000.00000000.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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Roaming\WdFVsOe	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C46BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.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	6C46DD66	CopyFileW
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C46DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp13F9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe:Zone.Identifier	success or wait	1	5C6733A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.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 73 fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 66 0e 00 00 06 00 00 00 00 00 00 fd fd 0e 00 00 20 00 00 00 fd 0e 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 0e 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.$PELc0f @ @	success or wait	4	6C46DD66	CopyFileW
C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.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	6C46DD66	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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ca8b3b75-86f2-4edb-b016-ef7ebe8beb9b	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C461B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	WdFVsOe	unicode	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe	success or wait	1	6C46646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	WdFVsOe	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C46DE2E	RegSetValueExW

Analysis Process: WdFVsOe.exe PID: **2460**, Parent PID: **3528**

General

Target ID:	2
Start time:	13:27:27
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe"
Imagebase:	0x1f0000
File size:	945664 bytes
MD5 hash:	0EB99950C8A30FEE01EBFDAA33498B22
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.360649511.0000000002655000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.360150897.00000000025A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, 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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WdFVsOe.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D92C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WdFVsOe.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	6D92C907	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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile

Analysis Process: WdFVsOe.exe PID: **4768**, Parent PID: **2460**

General

Target ID:	3
Start time:	13:27:31
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Imagebase:	0x4c0000
File size:	945664 bytes
MD5 hash:	0EB99950C8A30FEE01EBFDAA33498B22
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: 00000003.00000002.569999847.0000000002841000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.569999847.0000000002841000.00000004.00000800.00020000.00000000.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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp7023.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW

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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ca8b3b75-86f2-4edb-b016-ef7ebe8beb9b	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C461B4F	ReadFile

Analysis Process: WdFVsOe.exe PID: **5992**, Parent PID: **3528**

General

Target ID:	4
Start time:	13:27:35
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe"
Imagebase:	0x400000
File size:	945664 bytes

MD5 hash:	0EB99950C8A30FEE01EBFDAA33498B22
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D61CF06	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	6D61CF06	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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile

Analysis Process: WdFVsOe.exe PID: **972**, Parent PID: **5992**

General

Target ID:	5
Start time:	13:27:43
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Imagebase:	0xf0000
File size:	945664 bytes
MD5 hash:	0EB99950C8A30FEE01EBFDAA33498B22
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: WdFVsOe.exe PID: **1276**, Parent PID: **5992**

General

Target ID:	6
Start time:	13:27:43
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\WdFVsOe\WdFVsOe.exe
Imagebase:	0x650000
File size:	945664 bytes
MD5 hash:	0EB99950C8A30FEE01EBFDAA33498B22
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: 00000006.00000002.571356587.0000000002B2C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.571356587.0000000002B2C000.00000004.00000800.00020000.00000000.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	6D61CF06	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	6D61CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpA4BF.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C467038	GetTempFileNameW

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	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\ca8b3b75-86f2-4edb-b016-ef7ebe8beb9b	unknown	4096	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C461B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C461B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C461B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C461B4F	ReadFile

Disassembly

No disassembly