ID: 385478
Sample Name: Swift_Copy.exe
Cookbook: default.jbs
Time: 15:20:24
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

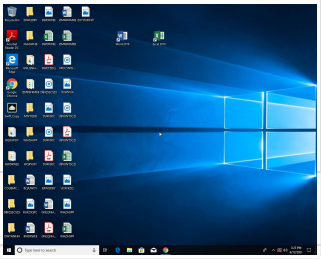
Analysis Report Swift_Copy.exe

Overview

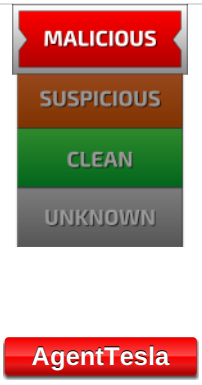
General Information

Sample Name:	Swift_Copy.exe
Analysis ID:	385478
MD5:	7c315e5221144e..
SHA1:	2d337a4c65ef709.
SHA256:	c9cf74378c0ab62..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

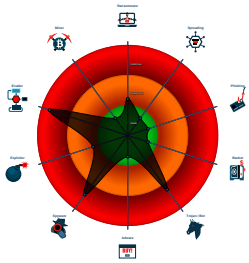


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Found evasive API chain (trying to d…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- Swift_Copy.exe (PID: 7016 cmdline: 'C:\Users\user\Desktop\Swift_Copy.exe' MD5: 7C315E5221144EBE207421FCF5578985)
  - schtasks.exe (PID: 2192 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NiUISpmncyqd' /XML 'C:\Users\user\AppData\Local\Temp\tmp6587.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Swift_Copy.exe (PID: 5952 cmdline: C:\Users\user\Desktop\Swift_Copy.exe MD5: 7C315E5221144EBE207421FCF5578985)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "result.package@yandex.ruBlessing123smtp.yandex.ru"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.673934957.000000000320 9000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000007.00000002.910330939.000000000315 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.910330939.000000000315 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000007.00000002.908724525.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.684677250.000000000A4D 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

Unpacked PEs

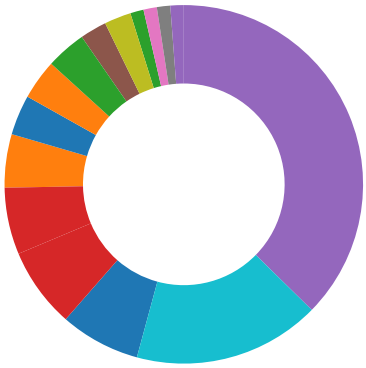
Source	Rule	Description	Author	Strings
7.2.Swift_Copy.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Swift_Copy.exe.a576e18.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Swift_Copy.exe.a576e18.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Found evasive API chain (trying to detect sleep duration tampering with parallel thread)
- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Mail credentials (via file access)

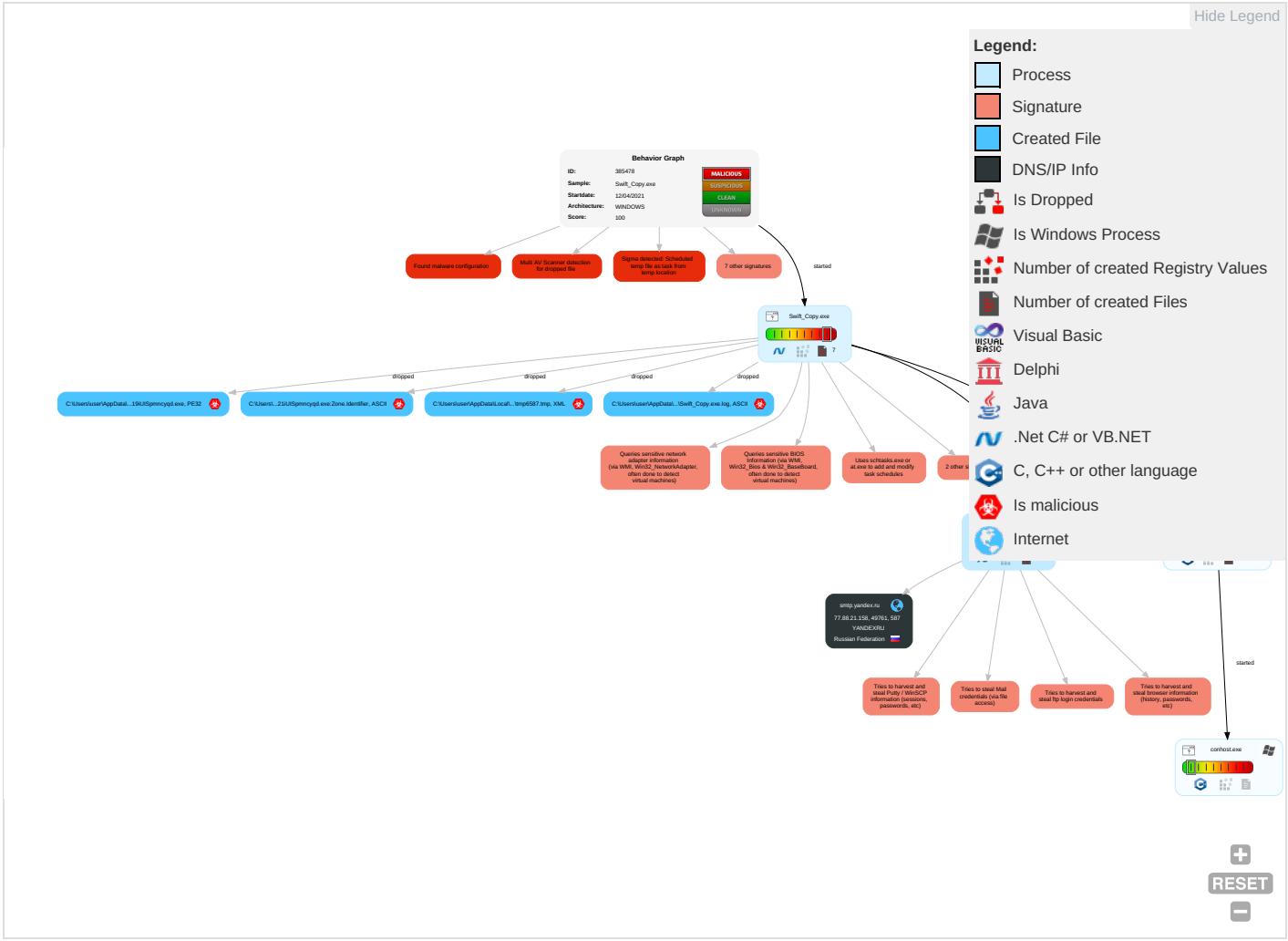
Remote Access Functionality:

- Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Swift_Copy.exe	32%	Virustotal		Browse
Swift_Copy.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Swift_Copy.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NiUISpmncyqd.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\NiUISpmncyqd.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comO=	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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://M7Hwvg39EZsNS3.net	0%	Avira URL Cloud	safe	
http://www.carterandcone.comams	0%	Avira URL Cloud	safe	
http://www.fontbureau.comituF$=	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.comlaywU	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypooo	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comak=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/TS	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypo	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnj	0%	Avira URL Cloud	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.sajatypeworks.comriwnD	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.fontbureau.comessed3=	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comd	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.sajatypeworks.comn	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comr=	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-r	0%	Avira URL Cloud	safe	
http://www.carterandcone.comfachUD	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.carterandcone.comonaEUo	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn.	0%	Avira URL Cloud	safe	
http://www.carterandcone.comint	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.yandex.ru	77.88.21.158	true	false		high

URLs from Memory and Binaries

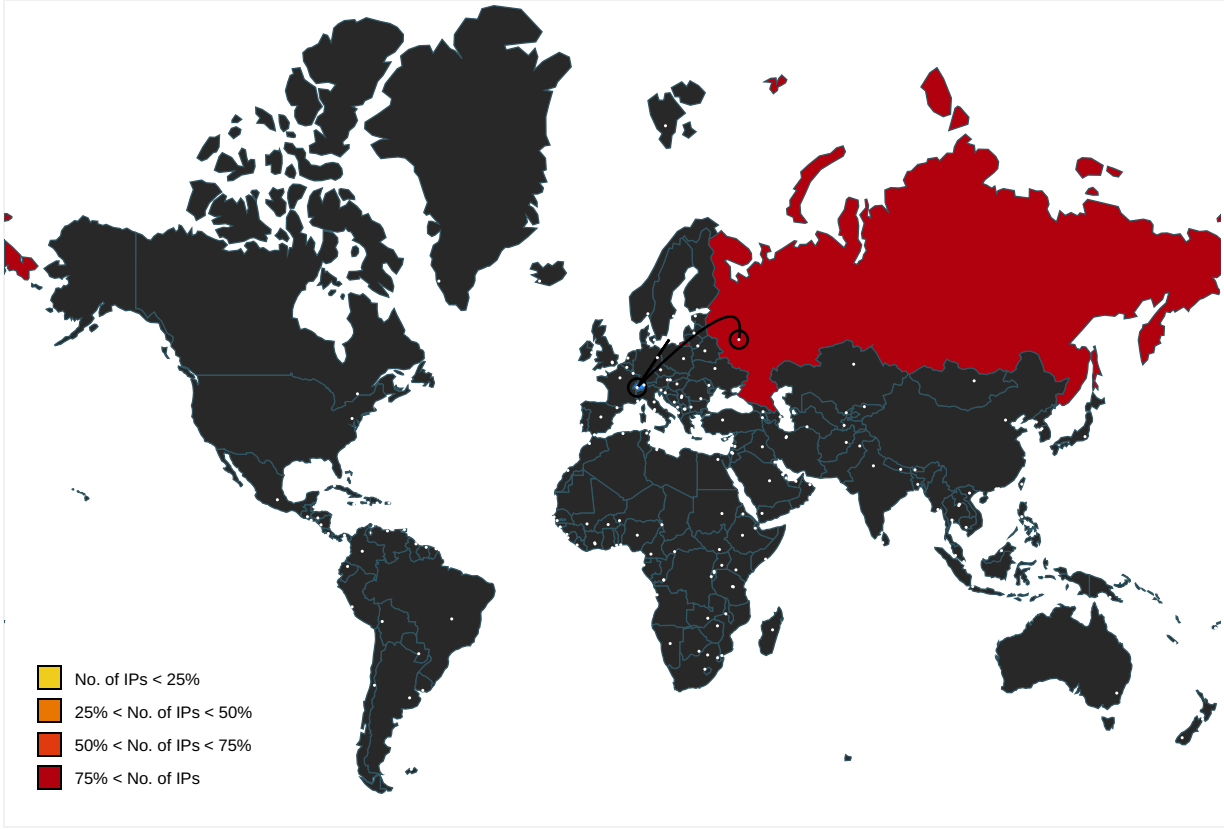
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Swift_Copy.exe, 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comO=	Swift_Copy.exe, 00000001.00000003.651955584.00000000056C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers.R	Swift_Copy.exe, 00000001.00000003.650057481.00000000056FC000.00000004.00000001.sdmp	false		high
http://M7Hwvg39EZsNS3.net	Swift_Copy.exe, 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp, Swift_Copy.exe, 00000007.00000002.910470938.000000000325E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comams	Swift_Copy.exe, 00000001.00000003.647185341.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersuR	Swift_Copy.exe, 00000001.00000003.651436325.00000000056F5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comituF$=	Swift_Copy.exe, 00000001.00000003.651955584.00000000056C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comlaywU	Swift_Copy.exe, 00000001.00000003.647185341.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Swift_Copy.exe, 00000001.00000003.656444196.00000000056F5000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comypooo	Swift_Copy.exe, 00000001.00000003.647622574.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	Swift_Copy.exe, 00000001.00000003.647260344.00000000056FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comak=	Swift_Copy.exe, 00000001.00000003.672581470.00000000056C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/TS	Swift_Copy.exe, 00000001.00000003.646684294.00000000056C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Swift_Copy.exe, 00000001.00000002.673934957.0000000003209000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comypo	Swift_Copy.exe, 00000001.00000003.647330238.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersR	Swift_Copy.exe, 00000001.00000003.651716227.00000000056F5000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnj	Swift_Copy.exe, 00000001.00000003.646509059.00000000056FD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersORe	Swift_Copy.exe, 00000001.00000003.650341989.00000000056FC000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comB.TTF	Swift_Copy.exe, 00000001.00000003.672581470.00000000056C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comriwnD	Swift_Copy.exe, 00000001.00000003.645172427.00000000056DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	Swift_Copy.exe, 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fontbureau.comessed3=	Swift_Copy.exe, 00000001.00000003.651955584.00000000056C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fonts.com	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp, Swift_Copy.exe, 00000001.00000003.646116742.00000000056C6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comd	Swift_Copy.exe, 00000001.00000003.645172427.00000000056DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersp	Swift_Copy.exe, 00000001.00000003.649972151.00000000056FC000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%	Swift_Copy.exe, 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Swift_Copy.exe, 00000001.00000002.684677250.000000000A4D5000.00000004.00000001.sdmp, Swift_Copy.exe, 00000007.00000002.908724525.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comn	Swift_Copy.exe, 00000001.00000003.645092939.00000000056DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	Swift_Copy.exe, 00000001.00000003.653279079.00000000056CD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DynDns.comDynDNS	Swift_Copy.exe, 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comr=	Swift_Copy.exe, 00000001.00000003.651955584.00000000056C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Swift_Copy.exe, 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTC	Swift_Copy.exe, 00000001.00000003.647260344.00000000056FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comn	Swift_Copy.exe, 00000001.00000003.645560443.00000000056DB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnu-r	Swift_Copy.exe, 00000001.00000003.646509059.00000000056FD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comfachUD	Swift_Copy.exe, 00000001.00000003.647008291.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	Swift_Copy.exe, 00000001.00000003.651955584.00000000056C4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comX	Swift_Copy.exe, 00000001.00000003.645259047.00000000056DB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comonaEUo	Swift_Copy.exe, 00000001.00000003.647185341.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn.	Swift_Copy.exe, 00000001.00000003.646509059.00000000056FD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comint	Swift_Copy.exe, 00000001.00000003.647185341.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Swift_Copy.exe, 00000001.00000003.646769974.00000000056CB000.00000004.00000001.sdmp, Swift_Copy.exe, 00000001.00000003.646524857.00000000056C4000.00000004.00000001.sdmp, Swift_Copy.exe, 00000001.00000003.646509059.00000000056FD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp, Swift_Copy.exe, 00000001.00000003.650731068.00000000056FC000.00000004.00000001.sdmp	false		high
http://www.fontbureau.commr=	Swift_Copy.exe, 00000001.00000003.672581470.00000000056C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comypol;	Swift_Copy.exe, 00000001.00000003.647260344.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://Mjyucn.com	Swift_Copy.exe, 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comy	Swift_Copy.exe, 00000001.00000003.647185341.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/$	Swift_Copy.exe, 00000001.00000003.646684294.00000000056C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Swift_Copy.exe, 00000001.00000002.679315929.00000000057C0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/o	Swift_Copy.exe, 00000001.00000003.649928925.00000000056FC000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comncy	Swift_Copy.exe, 00000001.00000003.647260344.00000000056FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers:	Swift_Copy.exe, 00000001.00000003.650536948.00000000056FC000.00000004.00000001.sdmp	false		high
http://www.tiro.comh	Swift_Copy.exe, 00000001.00000003.645469714.00000000056DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comE.TTF	Swift_Copy.exe, 00000001.00000003.651955584.00000000056C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385478
Start date:	12.04.2021
Start time:	15:20:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Swift_Copy.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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/4@1/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 40% • Quality standard deviation: 28.5%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 104.43.139.144, 52.147.198.201, 13.88.21.125, 168.61.161.212, 20.50.102.62, 104.43.193.48, 92.122.213.247, 92.122.213.194, 52.155.217.156, 2.20.142.209, 2.20.142.210, 20.54.26.129, 20.82.209.183, 40.88.32.150, 104.42.151.234 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
15:21:17	API Interceptor	904x Sleep call for process: Swift_Copy.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
77.88.21.158	Customer ID 2199201992001.xlsx	Get hash	malicious	Browse	
	UOB_BANK_MT104_SCAN.exe	Get hash	malicious	Browse	
	zq17jG57TX.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.36663460.22787.exe	Get hash	malicious	Browse	
	Payment_Advice.exe	Get hash	malicious	Browse	
	Swift_Copy.exe	Get hash	malicious	Browse	
	C6RET8T1Wi.exe	Get hash	malicious	Browse	
	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	
	SWIFT.exe	Get hash	malicious	Browse	
	Payment _Advice (2).exe	Get hash	malicious	Browse	
	cricket.exe	Get hash	malicious	Browse	
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	
	Shandong CIRS Form.exe	Get hash	malicious	Browse	
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	
	REQUEST QUOTATION BID..pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.yandex.ru	Customer ID 2199201992001.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	UOB_BANK_MT104_SCAN.exe	Get hash	malicious	Browse	• 77.88.21.158
	zq17jG57TX.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.GenericKD.36663460.22787.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment_Advice.exe	Get hash	malicious	Browse	• 77.88.21.158
	qINcOlwRud.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift_Copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	C6RET8T1Wi.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment _Advice (2).exe	Get hash	malicious	Browse	• 77.88.21.158
	cricket.exe	Get hash	malicious	Browse	• 77.88.21.158
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	• 77.88.21.158
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 77.88.21.158
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
YANDEXRU	Customer ID 2199201992001.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	UOB_BANK_MT104_SCAN.exe	Get hash	malicious	Browse	• 77.88.21.158
	zq17jG57TX.exe	Get hash	malicious	Browse	• 77.88.21.158
	SecuriteInfo.com.Trojan.GenericKD.36663460.22787.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment_Advice.exe	Get hash	malicious	Browse	• 77.88.21.158
	Swift_Copy.exe	Get hash	malicious	Browse	• 77.88.21.158
	C6RET8T1Wi.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ# ZAT77095_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 77.88.21.158
	SWIFT.exe	Get hash	malicious	Browse	• 77.88.21.158
	Payment _Advice (2).exe	Get hash	malicious	Browse	• 77.88.21.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	cricket.exe	Get hash	malicious	Browse	• 77.88.21.158
	SG1_000000123205044_1.pdf.gz.exe	Get hash	malicious	Browse	• 77.88.21.158
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 77.88.21.158
	_VmailMessage_Wave19922626.html	Get hash	malicious	Browse	• 77.88.21.179
	Order 01042021-V728394-H16.pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	RFQ#EX50GO_pdf.exe	Get hash	malicious	Browse	• 77.88.21.158
	TRANSACTION_INTTRANSFER_1617266945242 MEDICON_PDF.exe	Get hash	malicious	Browse	• 77.88.21.158
	Shandong CIRS Form.exe	Get hash	malicious	Browse	• 77.88.21.158
	DHL_DELIVERY_CONFIRMATION_CBJ00204202106 8506.exe	Get hash	malicious	Browse	• 77.88.21.158

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\Local\Temp\tmp6587.tmp

Process:	C:\Users\user\Desktop\Swift_Copy.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.180730639398364
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGtAtn:cbhK79lNQR/rydbz9I3YODOLNdq34W
MD5:	8D02A2C41969C722FCF30BA28EB49DA5
SHA1:	24244639536F0DCCF04E7E59F034FC026E8AC465
SHA-256:	EAE2226E24CD6342A64C4D28D5F5B7695E4B4FA26933A9B3A5D20908EFF1F565
SHA-512:	F8EA50EBB4204C3E8E5EE2D4D461EB0EC338180071B50D5170C313CC5E0EA9E4D7E64501E4B19287B3390677D343B52856B1333E8E44C5419BEB9DA50AEB32E5
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\NiUISpmncyqd.exe	
Process:	C:\Users\user\Desktop\Swift_Copy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	684544
Entropy (8bit):	7.441452446452719
Encrypted:	false
SSDEEP:	12288:i4enOh6dI9C8l7y0aTrhdgepi7xMU76P1wPGL45eYKcDQIBdHKsMjvLeh:zGE7ylrvgeFU7QSuE5ebcBdqnvLeh
MD5:	7C315E5221144EBE207421FCF5578985
SHA1:	2D337A4C65EF709607DA501C87F3127E61356E2F
SHA-256:	C9CF74378C0AB6240EF866BE3673DD54A46B36CCF58A7C9036344F96FB812AEE
SHA-512:	9E6CB34B5F61BBA7320D66B7BF9A26DC09BB577B8CD630D41242A7ED062969D45B4322F4C242567F23EBA416B46421D4529A908AD5BE16FC00ABB9948ACD9DB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 31%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....j.... ... ....@.. ..... ..@.....O.... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.reloc..... .....p.....@..B.....L.....H.....L..... H.....0.....(#...($.....(.....o%....*.....(&.....('.....((.....().....(*....*N..(....o....(+....*&..(,....*.s-.....s.....s/.....s0.....s1.....*....0.....~....o2....+..*.0.....~....o3....+..*.0.....~....o4....+..*.0.....~....o5....+..*.0.....~....o6....+..*.0..<.....~.....(7.....,!r...p.....(8...o9...s:.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\NiUISpmncyqd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Swift_Copy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
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):	7.441452446452719
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:	Swift_Copy.exe
File size:	684544
MD5:	7c315e5221144ebe207421fcf5578985
SHA1:	2d337a4c65ef709607da501c87f3127e61356e2f
SHA256:	c9cf74378c0ab6240ef866be3673dd54a46b36ccf58a7c9036344f96fb812aee
SHA512:	9e6cb34b5f61bba7320d66b7bf9a26dc09bb577b8cd630d41242a7ed062969d45b4322f4c242567f23eba416b4642d4529a908ad5be16fc00abb9948acd9ddb
SSDEEP:	12288:i4enOh6dI9C8l7y0aTrhdgepi7xMU76P1wPGL45eYKcDQIBdHKsMjvLeh:zGE7ylrvgeFU7QSuE5ebcBdqnvLeh

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P.....j.... ... .@.. .....@.....

File Icon

Icon Hash:	d28ab3b0e0ab96c4

Static PE Info

General

Entrypoint:	0x48016a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6073F386 [Mon Apr 12 07:15:18 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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]
or dword ptr [edx], ecx
or eax, 00000020h
add byte ptr [ecx+49h], cl
sub al, byte ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
dec ebp
dec ebp
add byte ptr [edx], ch
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x80118	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x82000	0x28be8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	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	0x7e188	0x7e200	False	0.882034347126	Intel 80386 COFF object file, not stripped, 8 sections, symbol offset=0x48, 327682 symbols, optional header size 57004	7.81058952683	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x28be8	0x28c00	False	0.349471577837	data	5.40668860774	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x822b0	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	0x92ad8	0x94a8	data		
RT_ICON	0x9bf80	0x5488	data		
RT_ICON	0xa1408	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	0xa5630	0x25a8	data		
RT_ICON	0xa7bd8	0x10a8	data		
RT_ICON	0xa8c80	0x988	data		
RT_ICON	0xa9608	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xa9a70	0x76	data		
RT_GROUP_ICON	0xa9ae8	0x14	data		
RT_VERSION	0xa9afc	0x3c4	data		
RT_MANIFEST	0xa9ec0	0xd25	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

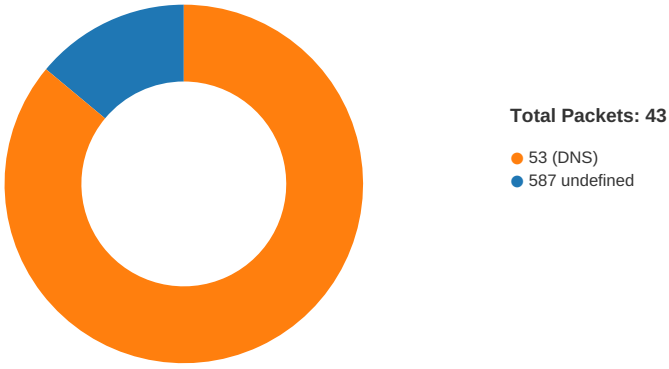
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Adobe Inc, Sel 2011 - 2021

Description	Data
Assembly Version	1.0.0.0
InternalName	SafeIsolatedStorageFileHandle.exe
FileVersion	1.0.0.0
CompanyName	Adobe Inc, Sel
LegalTrademarks	
Comments	
ProductName	Image Studio
ProductVersion	1.0.0.0
FileDescription	Image Studio
OriginalFilename	SafeIsolatedStorageFileHandle.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:22:54.346390963 CEST	49761	587	192.168.2.4	77.88.21.158
Apr 12, 2021 15:22:54.433274031 CEST	587	49761	77.88.21.158	192.168.2.4
Apr 12, 2021 15:22:54.433454990 CEST	49761	587	192.168.2.4	77.88.21.158
Apr 12, 2021 15:22:54.675438881 CEST	587	49761	77.88.21.158	192.168.2.4
Apr 12, 2021 15:22:54.675848961 CEST	49761	587	192.168.2.4	77.88.21.158
Apr 12, 2021 15:22:54.676445961 CEST	49761	587	192.168.2.4	77.88.21.158
Apr 12, 2021 15:22:54.762717009 CEST	587	49761	77.88.21.158	192.168.2.4
Apr 12, 2021 15:22:54.762747049 CEST	587	49761	77.88.21.158	192.168.2.4
Apr 12, 2021 15:22:54.763138056 CEST	587	49761	77.88.21.158	192.168.2.4
Apr 12, 2021 15:22:54.763267994 CEST	49761	587	192.168.2.4	77.88.21.158
Apr 12, 2021 15:22:54.763299942 CEST	49761	587	192.168.2.4	77.88.21.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:21:04.814481974 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:04.872620106 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:18.415958881 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:18.464657068 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:19.754889965 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:19.805573940 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:20.551693916 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:20.600583076 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:21.923937082 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:21.972752094 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:22.758521080 CEST	62389	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 15:21:22.807193041 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:24.610006094 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:24.661613941 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:26.402741909 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:26.454277992 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:30.049638033 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:30.098385096 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:37.154692888 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:37.203407049 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:38.748816967 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:38.800419092 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:42.871474981 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:42.930630922 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:48.848750114 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:48.900338888 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:50.776698112 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:50.825323105 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:58.736860991 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:58.795701981 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:59.458136082 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:59.518275023 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 12, 2021 15:21:59.769620895 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:21:59.828299046 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:00.099821091 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:00.156972885 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:00.608100891 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:00.665195942 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:00.877737045 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:00.943867922 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:01.404957056 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:01.453598976 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:02.034857988 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:02.094917059 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:02.677016020 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:02.728565931 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:03.513921976 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:03.571016073 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:04.704343081 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:04.761306047 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:05.237303019 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:05.294704914 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:14.063190937 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:14.114712000 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:15.315243006 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:15.385335922 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:44.961093903 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:45.012701988 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:46.033994913 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:46.093497038 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:46.276879072 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:46.325532913 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:47.381880045 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:47.438931942 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:48.212789059 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:48.277633905 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:53.278372049 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:53.330122948 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:54.211492062 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:54.256355047 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:54.262229919 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:54.315794945 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 12, 2021 15:22:55.307904959 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 12, 2021 15:22:55.356748104 CEST	53	59794	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 15:22:54.256355047 CEST	192.168.2.4	8.8.8.8	0x3555	Standard query (0)	smtp.yandex.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 15:22:54.315794945 CEST	8.8.8.8	192.168.2.4	0x3555	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)

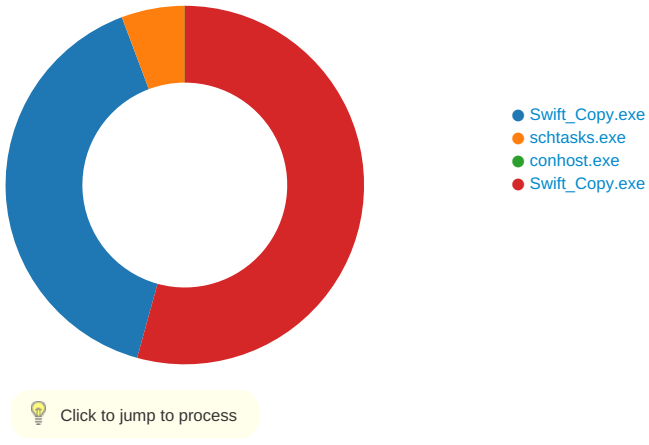
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 15:22:54.675438881 CEST	587	49761	77.88.21.158	192.168.2.4	220 vla3-23c3b031fed5.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru)
Apr 12, 2021 15:22:54.675848961 CEST	49761	587	192.168.2.4	77.88.21.158	EHLO 724471
Apr 12, 2021 15:22:54.762747049 CEST	587	49761	77.88.21.158	192.168.2.4	250-vla3-23c3b031fed5.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 42991616 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Swift_Copy.exe PID: 7016 Parent PID: 5164

General

Start time:	15:21:10
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Swift_Copy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Swift_Copy.exe'
Imagebase:	0xb40000
File size:	684544 bytes
MD5 hash:	7C315E5221144EBE207421FCF5578985
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: 00000001.00000002.673934957.0000000003209000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.684677250.000000000A4D5000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Roaming\NiUISpmncyqd.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	68518B4	CopyFileW
C:\Users\user\AppData\Roaming\NiUISpmncyqd.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	68518B4	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp6587.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13BB61C	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Swift_Copy.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6587.tmp	success or wait	1	6852622	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\NiUISpmncyqd.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 86 f3 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e2 07 00 00 8e 02 00 00 00 00 00 6a 01 08 00 00 20 00 00 00 20 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 e0 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....s`.......... ....P............j.... ... .@.. ....@................	success or wait	3	68518B4	CopyFileW
C:\Users\user\AppData\Roaming\ NiUISpmncyqd.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	68518B4	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp6587.tmp	unknown	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 37 37 31 5c 6a 6f 6e 65 73 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.microso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	68522DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Swift_Copy.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7254A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: schtasks.exe PID: 2192 Parent PID: 7016

General

Start time:	15:21:22
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NiUISpmncyqd' /XML 'C:\Users\user\AppData\Local\Temp\tmp6587.tmp'
Imagebase:	0x9b0000
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\tmp6587.tmp	unknown	2	success or wait	1	9BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6587.tmp	unknown	1646	success or wait	1	9BABD9	ReadFile

Analysis Process: conhost.exe PID: 6672 Parent PID: 2192

General

Start time:	15:21:23
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: Swift_Copy.exe PID: 5952 Parent PID: 7016

General

Start time:	15:21:23
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Swift_Copy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Swift_Copy.exe
Imagebase:	0xa90000
File size:	684544 bytes
MD5 hash:	7C315E5221144EBE207421FCF5578985
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: 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.910330939.0000000003151000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.908724525.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	unknown

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	722760AC	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	722760AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5BD105B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5BD105B	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	5BD105B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	5BD105B	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\e66a8f68-5dba-4210-8c9d-e1510d52a6b1	unknown	4096	success or wait	1	5BD105B	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	5BD105B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	5BD105B	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	5BD105B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5BD105B	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5BD105B	ReadFile

Disassembly

Code Analysis